

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC.; INSTAGRAM, INC.; WHATSAPP LLC; META
PLATFORMS TECHNOLOGIES, LLC; AND GIPHY, INC.

Petitioners

v.

VL COLLECTIVE IP LLC

Patent Owner

U.S. Patent No. 7,266,682

Case IPR2023-00923

**DECLARATION OF SYLVIA D. HALL-ELLIS, Ph.D.
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 7,266,682**

I, Sylvia D. Hall-Ellis, declare as follows:

I. INTRODUCTION

1. My name is Sylvia D. Hall-Ellis. I have been retained as an expert by Petitioners Meta Platforms, Inc., Instagram, Inc., WhatsApp LLC, Meta Platforms Technologies LLC, and GIPHY, Inc. (“Petitioners”) in this proceeding before the the United States Patent and Trademark Office (“USPTO”).

2. I have written this declaration at the request of the Petitioners to provide my expert opinion regarding the authenticity and public availability of a publication. My declaration sets forth my opinions in detail and provides the basis for my opinions regarding the authenticity and public availability of this publication. If called to testify in the above-captioned proceeding, I will testify regarding the opinions and bases set forth below.

3. I reserve the right to supplement or amend my opinions, and bases for them, in response to any additional evidence, testimony, discovery, argument, and/or other additional information that may be provided to me after the date of this declaration.

4. I am being compensated for my time spent working on this matter at my normal consulting rate of \$350 per hour, plus reimbursement for any additional reasonable expenses. My compensation is not in any way tied to the content of this

declaration, the substance of my opinions, or the outcome of this proceeding. I have no other interests in this proceeding or with any of the parties.

5. All the materials that I considered and relied upon are discussed explicitly in this declaration.

II. QUALIFICATIONS

6. I am currently an Adjunct Professor in the School of Information at San José State University in San José, California. I obtained a Master of Library Science from the University of North Texas in 1972 and a Ph.D. in Library Science from the University of Pittsburgh in 1985. Over the last fifty years, I have held various positions in the field of library and information resources. I was first employed as a librarian in 1966 and have been involved in the field of library sciences since, holding numerous positions.

7. I am a member of the American Library Association (ALA) and its Association for Library Collections & Technical Services (ALCTS) Division, and I served on the Committee on Cataloging: Resource and Description (which wrote the new cataloging rules) and as the chair of the Committee for Education and Training of Catalogers and the Competencies and Education for a Career in Cataloging Interest Group. I also served as the founding Chair of the ALCTS Division's Task Force on Competencies and Education for a Career in Cataloging. Additionally, I have served as the Chair for the ALA Office of Diversity's

Committee on Diversity, as a member of the REFORMA National Board of Directors, as a member of the Editorial Board for the ALCTS premier cataloging journal, *Library Resources and Technical Services*, and as a Co-Chair of the Membership Committee for the Library Research Round Table (LRRT) of the American Library Association. Currently I serve as a member of the LRRT Nominating Committee.

8. I have also given over one hundred presentations in the field, including several on library cataloging systems and Machine-Readable Cataloging (“MARC”) standards. My current research interests include library cataloging systems, metadata, and organization of electronic resources.

9. I have been deposed twenty-seven times: (1) *Symantec Corp. v. Finjan, Inc.*, Petition for *Inter Partes Review* of U.S. Patent No. 7,613,926, May 26, 2016, on behalf of Symantec Corp.; (2) *Symantec Corp. v. Finjan, Inc.*, 14-cv-299-HSG (N.D. Cal.), on behalf of Symantec Corp., September 14, 2017; (3) one deposition for ten matters: *Intellectual Ventures I LLC v. AT&T Mobility LLC*; *AT&T Mobility II LLC*, New Cingular Wireless Services, Inc., SBC Internet Services, Inc., Wayport, Inc., and Cricket Wireless LLC, C.A. No. 12-193 (LPS); *Intellectual Ventures II LLC v. AT&T Mobility LLC*; *AT&T Mobility II LLC*, New Cingular Wireless Services, Inc., SBC Internet Services, Inc., Wayport, Inc., and Cricket Wireless LLC, C.A. No. 13-1631 (LPS); *Intellectual Ventures I*

LLC v. T-Mobile USA, Inc. and T-Mobile US, Inc., C.A. No. 13-1632 (LPS); *Intellectual Ventures II LLC v. T-Mobile USA, Inc. and T-Mobile US, Inc.*, C.A. No. 13-1633 (LPS); *Intellectual Ventures I LLC, v. Nextel Operations, Inc., Sprint Spectrum L.P., Boost Mobile, LLC and Virgin Mobile USA, L.P.*, C.A. No. 13-1634 (LPS); *Intellectual Ventures II LLC v. Nextel Operations, Inc., Sprint Spectrum L.P., Boost Mobile, LLC and Virgin Mobile USA, L.P.*, C.A. No. 13-1635 (LPS); *Intellectual Ventures I LLC, v. United States Cellular Corporation*, C.A. No. 13-1636 (LPS); *Intellectual Ventures I LLC v. United States Cellular Corporation*, C.A. No. 13-1637 (LPS); *Intellectual Ventures II LLC v. AT&T Mobility LLC, AT&T Mobility II LLC, New Cingular Wireless Services, Inc.*, C.A. No. 15-799 (LPS); *Intellectual Ventures I LLC v. T-Mobile USA, Inc. and T-Mobile US, Inc.*, C.A. No. 15-800 (LPS), on behalf of AT&T Mobility LLC; AT&T Mobility II LLC, Boost Mobile, LLC Cricket Wireless LLC, Nextel Operations, Inc., New Cingular Wireless Services, Inc., SBC Internet Services, Inc., Sprint Spectrum L.P., T-Mobile USA, Inc., T-Mobile US, Inc., United States Cellular Corporation Virgin Mobile USA, L.P., and Wayport, Inc., November 15, 2016; (4) *Hitachi Maxell, LTD., v. Top Victory Electronics (Taiwan) Co. Ltd., et al.*, 2:14-cv-1121 JRG-RSP (E.D. Texas), on behalf of Top Victory Electronics (Taiwan) Co. LTD, *et al.*, January 20, 2016; (5) *Sprint Spectrum, L.P. v. General Access Solutions, Ltd.*, Petition for *Inter Partes Review* of U.S. Patent No. 7,173,916, on behalf of

Sprint Spectrum L.P., July 13, 2018; (6) *Nichia Corporation v. Vizio, Inc.*, 8:16-cv-00545; on behalf of Vizio, Inc., October 12, 2018; (7) *Intellectual Ventures I LLC, v. T-Mobile USA, Inc., T-Mobile US, Inc., Ericsson Inc., and Telefonaktiebolaget LM Ericsson*, 2:17-cv-00557 (JRG), on behalf of T-Mobile USA, Inc., T-Mobile US, Inc., Ericsson Inc., and Telefonaktiebolaget LM Ericsson, October 19, 2018; (8) *Pfizer, Inc. v. Biogen, Inc.*, Petition for *Inter Partes Review* of U.S. Patent No. 8,821,873, on behalf of Pfizer, November 3, 2018; (9) *Finjan, Inc. v. ESET, LLC and ESET SPOL. S.R.O.*, 3:17-cv-00183-CAB-BGS, on behalf of ESET, January 15, 2019; (10) *Finjan, Inc. v. Cisco Systems, Inc.*, 5:17-cv-00072-BLF-SVK, on behalf of Cisco Systems, Inc., September 6, 2019; (11) *Facebook, Inc., Instagram, LLC and Whatsapp Inc. v. Blackberry Limited*, Petition for *Inter Partes Review* of U.S. Patent No. 9,349,120 B2, on behalf of Facebook, Inc., Instagram, LLC and Whatsapp Inc. December 20, 2019; (12) *3Shape A/S and 3Shape Inc. v. Align Technology, Inc.*, Petition for *Inter Partes Review* of U.S. Patent No. 7,156,661, IPR 2020-00222 and IPR 2020-00223, August 10, 2020, on behalf of 3Shape A/S and 3Shape Inc.; (13) *Finjan Inc. v. Rapid7, Inc. and Rapid7 LLC*, Northern District of Delaware; 1:18-cv-01519-MN, September 15, 2020; (14) *VLSI Technology LLC v. Intel Corporation*, Western District of Texas, 6:19-cv-00254, 6:19-cv-00255, 6:19-cv-00256, on behalf of Intel Corporation, September 23, 2020; (15) *Finjan Inc. v.*

Sonicwall, Inc., Northern District of California, 5:17-cv-04467-BLF-HRL, on behalf of Sonicwall, Inc., October 27, 2020; (16) *VLSI Technology, LLC v. Intel Corporation*, District of Delaware, 1:18-cv-00966-CFC-CJB, February 5, 2021, on behalf of the Intel Corporation; (17) *Unified Patents, LLC v. Good Kaisha IP Bridge I*, Petition for *Inter Partes Review* of U. S. Patent 7,817,868, February 11, 2021, on behalf of Unified Patents; (18) *Finjan, Inc. v. Qualsys, Inc.*, Northern District of California, 4:18-cv-07229-YGR, March 1, 2021, on behalf of Qualsys, Inc.; (19) *Qualcomm, Inc. v. Monterey Research LLC*, Petition for *Inter Partes Review* of U. S. Patent 6,534,805, May 6, 2021, on behalf of Qualcomm, Inc.; (20) *Hulu, LLC v. Sound View Innovations, LLC*, Petition for *Inter Partes Review* of U. S. Patent 5,806,062, May 14, 2021, on behalf of Hulu, LLC; (21) *VLSI Technology LLC v. Intel Corporation*, Western District of Texas, 6:19-cv-00254, 6:19-cv-00255 and 6:19-cv-00256, August 3, 2021, on behalf of Intel Corporation; (22) *Liquidia Technologies, Inc. v. United Therapeutics Corporation*, Petition for *Inter Partes Review* of U. S. Patent 10,716,793 B2, October 20, 2021, on behalf of Liquidia Technologies, Inc.; (23) *EcoFactor, Inc. v. Google, Inc.*, Western District of Texas, 6:20-cv-00075 (ADA), 6:20-0078-ADA, and 6:20-cv-00080 ADA, October 27, 2021, on behalf of Google, Inc.; (24) *Liquidia Technologies, Inc. v. United Therapeutics Corporation*, Petition for *Inter Partes Review* of U. S. Patent

10,716,793 B2, March 11, 2022, on behalf of Liquidia Technologies, Inc.; (25) *Juniper Networks, Inc. v. Swarm Technology LLC*, Petition for *Inter Partes Review* of U. S. Patent 9,852,004, May 5, 2022, on behalf of Juniper Networks, Inc.; (26) *ParkerVision, Inc. v. Intel Corporation*, Western District of Texas, 6:20-cv-108 (ADA), October 26, 2022, on behalf of the Intel Corporation; and, (27) *CommScope v. TQ Delta*, Petition for *Inter Partes Review* of U. S. Patents 9,094,348 and 10,833,809, February 16, 2023, on behalf of CommScope.

10. My full curriculum vitae is attached as Appendix 1.

III. PRELIMINARIES

A. Scope of Declaration and Legal Standards

11. I am not an attorney and will not offer opinions on the law. I am, however, rendering my expert opinion on the authenticity of the documents referenced herein and on when and how each of these documents was disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising ordinary diligence, could have located the documents by January 18, 2000.

12. I am informed by counsel that a printed publication qualifies as publicly accessible as of the date it was disseminated or otherwise made available such that a person interested in and ordinarily skilled in the relevant subject matter

could locate it through the exercise of ordinary diligence.

13. While I understand that the determination of public accessibility under the foregoing standard rests on a case-by-case analysis of the facts particular to an individual publication, I also understand that a printed publication is rendered “publicly accessible” if it is cataloged and indexed by a library such that a person interested in the relevant subject matter could locate it (*i.e.*, I understand that cataloging and indexing by a library is sufficient, though there are other ways that a printed publication may qualify as publicly accessible). One manner of sufficient indexing is indexing according to subject matter category. I understand that the cataloging and indexing by a single library of a single instance of a particular printed publication is sufficient, even if the single library is in a foreign country. I understand that, even if access to a library is restricted, a printed publication that has been cataloged and indexed therein is publicly accessible so long as a presumption is raised that the portion of the public concerned with the relevant subject matter would know of the printed publication. I also understand that the cataloging and indexing of information that would guide a person interested in the relevant subject matter to the printed publication, such as the cataloging and indexing of an abstract for the printed publication, is sufficient to render the printed publication publicly accessible.

14. I understand that routine business practices, such as general library

cataloging and indexing practices, can be used to establish an approximate date on which a printed publication became publicly accessible.

B. Persons of ordinary skill in the art.

15. I am told by counsel that the subject matter of this proceeding relates to data transmission, and specifically, a method and system for transmitting data from a transmitter to a receiver.

16. I have been informed by counsel that a “person of ordinary skill in the art at the time of the invention” (“POSITA”) is a hypothetical person who is presumed to be familiar with the relevant field and its literature at the time of the inventions. This hypothetical person is also a person of ordinary creativity, capable of understanding the scientific principles applicable to the pertinent field.

17. I have been informed by counsel that Petitioners contend that persons of ordinary skill in this subject matter or art would have had a Bachelor’s degree in computer science, electrical engineering, or a related field, and two years of experience; or by obtaining a Master’s degree in electrical engineering or a related field, but having only one to two years of experience; or by having no formal education but experience in network data transmission and computer networking of at least eight years. Additional education might compensate for less experience, and vice-versa.

18. Regardless of whether Petitioner’s or Patent Owner’s definition of a

person of ordinary skill in the art is used, it is my opinion that such a person would have been engaged in research, learning, study, and practice in the field, and formal instruction so that bibliographic resources relevant to his or her research would be familiar. Before January 18, 2000, such a person would have had access to a vast array of long-established print resources in data transmission and computer networking as well as to a rich set of online resources providing indexing information, abstracts, and full text services.

IV. LIBRARY PROFESSIONAL PRACTICES

19. In preparing this declaration, I used authoritative databases, such as the OCLC bibliographic database, the Library of Congress Online Catalog, and the Library of Congress Subject Authorities, to confirm citation details of the various publications discussed. Unless I note otherwise below in reference to a specific serial publication, it is my expert opinion that this standard protocol was followed for the serial publication discussed below.

20. *Indexing.* A researcher may discover material relevant to his or her topic in a variety of ways. One common means of discovery is to search for relevant information in an index of periodicals and other publications. Having found relevant material, the researcher will then normally obtain it online, look for it in libraries, or purchase it from the publisher, a bookstore, a document delivery service, or other provider. Sometimes, the date of a document's public accessibility

will involve both indexing and library date information. However, date information for indexing entries is often unavailable. This is especially true for online indices.

21. Indexing services use a wide variety of controlled vocabularies to provide subject access and other means of discovering the content of documents. The Library of Congress Subject Authorities includes standard forms of terms and cross references that are included in bibliographic records. Subject headings are terms that an individual seeking a document regardless of format can enter in the search bar of the online catalog. Subjects also connect an authenticated term (one included in the Library of Congress subject headings list) with related, broader, and narrower terms. The formats in which these access terms are presented vary from service to service.

22. Online indexing services commonly provide bibliographic information, abstracts, and full-text copies of the indexed publications, along with a list of the documents cited in the indexed publication. These services also often provide lists of publications that cite a given document. A citation of a document is evidence that the document was publicly available and in use by researchers no later than the publication date of the citing document. Prominent indexing services include *Scopus*, the *IEEE Xplore* database, the *ACM Digital Library*, *Google Scholar*, and the *Internet Archive*.

V. ONLINE CATALOGS AND MARC RECORDS

23. MARC is a framework into which descriptive bibliographic data are transcribed to interact with the software in online library catalogs to provide access to books, journals, and other resources in the collection. The bibliographic data provide points of access and can be searched by a POSITA to identify and obtain resources in the library collection. An information seeker (or POSITA) can search a local online library catalog or the holdings of a group of libraries in a state or region or in the global catalog WorldCat.

24. MARC records are not designed for public viewing. Although a significant number of libraries provide access to the MARC version of a bibliographic record, the public display is designed to show information in a succinct manner that is quickly understood and useful to the information seeker. Libraries determine the default search for the online catalog to make the entry of search terms efficient and result in a successful search. Information seekers can enter a keyword, title, author, or standard number for the item. Libraries may also provide a search capability called “Summon” that allows the information seeker to enter known information about the item to conduct a search.

25. Learning to use an online library catalog begins in elementary school and continues through high school and post-secondary studies. Undergraduate students further develop their skills to use the online catalog at the academic

institution where they are studying through information literacy instruction which is provided by professional reference and user experience librarians. The skills required to search, identify, and obtain the resources identified in this declaration/report are fundamental to using the online catalogs in libraries and information centers. Therefore, a POSITA who has attained the undergraduate and/or graduate educational levels described above (see paragraph 17) possesses the searching and retrieval skills needed to search library catalogs.

26. Professional catalog and metadata librarians prepare and enhance MARC records to provide points of access for each item in the library collection. Using a set of internationally adopted guidelines, rules for the assignment of classification numbers, and the assignment of subject headings from standardized lists, taxonomies, folksonomies, locally developed lists. An information seeker (including POSITAs) can search the online library catalog in a number of ways to identify a specific item or resources on a defined topic.

27. The continued development of the software that supports integrated online library catalogs resulted in the potential to search by an individual creator or author, title proper or variant title, a series that contains the desired item, subjects, corporate bodies responsible in part for the creation of an item, or standard identification numbers associated with the item (e.g., International Standard Book Numbers (ISBN), International Standard Serial Numbers (ISSN), and Publisher's

Numbers). Each of these data elements appears in a prescribed location within the MARC framework so that the software can parse, index, and display data elements resulting from a user-initiated search.

28. Examining the MARC records for a specific item reveals the comprehensive data transcribed about a particular item at the time that cataloging and classification occurred. In addition to the creator, title, subjects, and standard numbers, additional information may provide additional and relevant data depending on the type of resource. Understanding the full extent of bibliographic data for an item and the points of access associated with it provide essential information that can be used to determine the indexing and public availability for documents described in this declaration/report.

VI. LIBRARY CATALOGING PRACTICES

29. I am fully familiar with the library cataloging standard known as the MARC standard, which is an industry-wide standard method of storing and organizing library catalog information.¹ MARC was first developed in the 1960's by the Library of Congress. A MARC-compatible library is one that has a catalog consisting of individual MARC records for each of its items. Today, MARC is the primary communications protocol for the transfer and storage of bibliographic

¹ The full text of the standard is available from the Library of Congress at <http://www.loc.gov/marc/bibliographic/> (last visited April 20, 2023).

metadata in libraries.²

30. Since at least the early 1970s and continuing to the present day, MARC has been the primary communications protocol for the transfer and storage of bibliographic metadata in libraries.³ As explained by the Library of Congress:

You could devise your own method of organizing the bibliographic information, but you would be isolating your library, limiting its options, and creating much more work for yourself. Using the MARC standard prevents duplication of work and allows libraries to better share bibliographic resources. Choosing to use MARC enables libraries to acquire cataloging data that is predictable and reliable. If a library were to develop a “home-grown” system that did not use MARC records, it would not be taking advantage of an industry-wide standard whose primary purpose is to foster communication of information.

Using the MARC standard also enables libraries to make use of commercially available library automation systems to manage library operations. Many systems are available for libraries of all sizes and

² Almost every major library in the world is MARC-compatible. See, e.g., *MARC Frequently Asked Questions (FAQ)*, Library of Congress, <https://www.loc.gov/marc/faq.html> (last visited April 20, 2023) (“MARC is the acronym for Machine-Readable Cataloging. It defines a data format that emerged from a Library of Congress-led initiative that began nearly fifty years ago. It provides the mechanism by which computers exchange, use, and interpret bibliographic information, and its data elements make up the foundation of most library catalogs used today.”). MARC is the ANSI/NISO Z39.2-1994 (reaffirmed 2016) standard for Information Interchange Format.

³ A complete history of the development of MARC can be found in *MARC: Its History and Implications* by Henrietta D. Avram (Washington, DC: Library of Congress, 1975) and available online from the Hathi Trust (<https://babel.hathitrust.org/cgi/pt?id=mdp.39015034388556;view=1up;seq=1>; last visited April 20, 2023).

are designed to work with the MARC format. Systems are maintained and improved by the vendor so that libraries can benefit from the latest advances in computer technology. The MARC standard also allows libraries to replace one system with another with the assurance that their data will still be compatible.

Why Is a MARC Record Necessary? LIBRARY OF CONGRESS.⁴

31. Thus, almost every major library in the world is MARC-compatible. See, e.g., *MARC Frequently Asked Questions (FAQ)*, LIBRARY OF CONGRESS.⁵ (“MARC is the acronym for MACHine-Readable Cataloging. It defines a data format that emerged from a Library of Congress-led initiative that began fifty years ago. It provides the mechanism by which computers exchange, use, and interpret bibliographic information, and its data elements make up the foundation of most library catalogs used today.”). MARC is the ANSI/NISO Z39.2-1994 standard (reaffirmed in 2016) for Information Interchange Format. The full text of the standard is available from the Library of Congress.⁶

32. A MARC record comprises several fields, each of which contains specific data about the work. Each field is identified by a standardized, unique, three-digit code corresponding to the type of data that follow. For example, a

⁴ <http://www.loc.gov/marc/umb/um01to06.html#part2>

⁵ <https://www.loc.gov/marc/faq.html>

⁶ <http://www.loc.gov/marc/bibliographic/>

work's title is recorded in Field 245; the primary author of the work is transcribed in Field 100; an item's International Standard Book Number ("ISBN") consisting of ten or thirteen digits is transcribed in Field 020; an item's International Standard Serial Number ("ISSN") is transcribed in Field 022; the Library of Congress classification notation is recorded in Field 050; and the publication date is recorded in Field 260 under the subfield "c." If a work is a periodical, then its publication frequency is recorded in Field 310, and the publication dates (e.g., the first and last publication) are recorded in Field 362, which is also referred to as the enumeration/chronology field.⁷

33. The library that created the record is recorded in Field 040 in subfield "a" with a unique library code. When viewing the MARC record online via Online Computer Library Center's ("OCLC") bibliographic database, hovering over this code with the mouse reveals the full name of the library. I used this method of "mousing over" the library codes in the OCLC database to identify the originating library for the MARC records discussed in this declaration. Where this "mouse over" option was not available, I consulted the Directory of OCLC Libraries to identify the institution that created the MARC record.⁸

34. MARC records also include several fields that include subject matter

⁷ <http://www.loc.gov/marc/bibliographic/bd3xx.html>

⁸ <https://www.oclc.org/en/contacts/libraries.html>

classification information. An overview of MARC record fields is available through the Library of Congress.⁹ For example, 6XX fields are termed “Subject Access Fields.”¹⁰ Among these, for example, is the 650 field; this is the “Subject Added Entry – Topical Term” field.¹¹ The 650 field is a “[s]ubject added entry in which the entry element is a topical term.” These entries “are assigned to a bibliographic record to provide access according to generally accepted thesaurus-building rules (e.g., *Library of Congress Subject Headings* (LCSH), *Medical Subject Headings* (MeSH)).” *Id.* Further, MARC records include call numbers, which themselves include a classification number. For example, the 050 field is the “Library of Congress Call Number.”¹² A defined portion of the Library of Congress Call (LCC) Number is the classification number, and “source of the classification number is *Library of Congress Classification* and the *LC Classification-Additions and Changes*.” Thus, included in the 050 field is a subject matter classification. Further, the 082 field is the “Dewey Decimal Call Number.”¹³ A defined portion of the Dewey Decimal Call (DDC) Number is the classification number, and “source of the classification number is the *Dewey Decimal*

⁹ <http://www.loc.gov/marc/bibliographic/>

¹⁰ <http://www.loc.gov/marc/bibliographic/bd6xx.html>

¹¹ <http://www.loc.gov/marc/bibliographic/bd650.html>

¹² <http://www.loc.gov/marc/bibliographic/bd050.html>

¹³ <http://www.loc.gov/marc/bibliographic/bd082.html>

Classification and Relative Index.” Thus, included in the 082 field is a subject matter classification. Each item in a library has a single classification number. A library selects a classification scheme (*e.g.*, the Library of Congress classification scheme just described or a similar scheme such as the Dewey Decimal classification scheme) and uses it consistently. When the Library of Congress assigns the LCC classification number, it appears as part of the 050 field. When the Library of Congress assigns the DDC classification number, it appears as part of the 082 field. If a local library assigns the classification number, it appears in a 090 field. In either scenario, the MARC record includes a classification number that represents a subject matter classification.

35. The OCLC was created “to establish, maintain and operate a computerized library network and to promote the evolution of library use, of libraries themselves, and of librarianship, and to provide processes and products for the benefit of library users and libraries, including such objectives as increasing availability of library resources to individual library patrons and reducing the rate of rise of library per-unit costs, all for the fundamental public purpose of furthering ease of access to and use of the ever-expanding body of worldwide scientific,

literary and educational knowledge and information.”¹⁴ Among other services, OCLC and its members are responsible for maintaining the WorldCat database (<http://www.worldcat.org/>), used by independent and institutional libraries throughout the world.

36. OCLC also provides its members online access to MARC records through its OCLC bibliographic database. When an OCLC member institution acquires a work, it creates a MARC record for this work in its computer catalog system in the ordinary course of its business. MARC records created at the Library of Congress are tape-loaded into the OCLC database through a subscription to MARC Distribution Services daily or weekly. Once the MARC record is created by a cataloger at an OCLC member institution or is tape-loaded from the Library of Congress, the MARC record is then made available to any other OCLC members online, and therefore made available to the public. Accordingly, once the MARC record is created by a cataloger at an OCLC member institution or is tape-loaded from the Library of Congress or another library anywhere in the world, any publication corresponding to the MARC record has been cataloged and indexed according to its subject matter such that a person interested in that subject matter could, with reasonable diligence, locate and access the publication through any

¹⁴ Third Article, Amended Articles of Incorporation of OCLC Online Computer Library Center, Incorporated (available at <https://www.oclc.org/content/dam/oclc/membership/articles-of-incorporation.pdf>).

library with access to the OCLC bibliographic database or through the Library of Congress.

37. When an OCLC member institution creates a new MARC record, OCLC automatically supplies the date of creation for that record. The date of creation for the MARC record appears in the fixed Field (008), characters 00 through 05. The MARC record creation date reflects the date on which the item was first acquired or cataloged. Initially, Field 005 of the MARC record is automatically populated with the date the MARC record was created in year, month, day format (YYYYMMDD) (some of the newer library catalog systems also include hour, minute, second (HHMMSS)). Thereafter, the library's computer system may automatically update the date in Field 005 every time the library updates the MARC record (*e.g.*, to reflect that an item has been moved to a different shelving location within the library). Field 005 is visible when viewing a MARC record via an appropriate computerized interface, but when a MARC record is printed to hardcopy, no "005" label appears. The initial Field 005 date (*i.e.*, the date the MARC record was created) does appear, however, next to the label "Entered."¹⁵ The date upon which the most recent update to Field 005 occurred also appears, next to the label "Replaced." Thus, when an item's MARC

¹⁵ Field 005 is visible when viewing a MARC record via an appropriate computerized interface. But when a MARC record is printed directly to hardcopy from the OCLC database, the "005" label is not shown. The date in the 005 field instead appears next to the label "Replaced."

record has been printed to hardcopy—as is the case with the exhibits to this declaration—the date reflected next to the label “Entered” is necessarily on or after the date the library first cataloged and indexed the underlying item.

38. Once one library has cataloged and indexed a publication by creating a MARC record for that publication, other libraries that receive the publication do not create additional MARC records—the other libraries instead rely on the original MARC record. They may update or revise the MARC record to ensure accuracy, but they do not replace or duplicate it. This practice does more than save libraries from duplicating labor. It also enhances the accuracy of MARC records. Further, it allows librarians around the world to know that a particular MARC record is authoritative (in contrast, a hypothetical system wherein duplicative records were created would result in confusion as to which record is authoritative).

39. Catalogers can create MARC records for all types of print, online, and digital resources. The date of creation of the MARC record by a cataloger at an OCLC member institution reflects when the underlying item is accessible to the public. Upwards of two-thirds to three-quarters of book sales to libraries come from a jobber or wholesaler for online and print resources. These resellers make it their business to provide books to their customers as fast as possible, often providing turnaround times of only a single day after publication. Libraries purchase a significant portion of the balance of their books directly from publishers

themselves, which provide delivery on a similarly expedited schedule. In general, libraries make these purchases throughout the year as the books are published and shelve the books as soon thereafter as possible to make the books available to their patrons. Thus, books are generally available at libraries across the country within just a few days of publication.

VII. PUBLICATION 1: *Secure Transport Protocols for High-Speed Networks* by Erol Basturk, Mihir Bellare, Chee-Seng Chow, and Roch Guerin. Exhibit A (“Basturk”)

40. Exhibit A is a copy of the cover, title page, abstract, and the text of a technical report titled *Secure Transport Protocols for High-Speed Networks* by Erol Basturk, Mihir Bellare, Chee-Seng Chow, and Roch Guerin (hereafter “Basturk”) prepared for and issued by the Advanced Networking Laboratory at the IBM T. J. Watson Research Center (Yorktown Heights, New York) and dated January 31, 1994. On the last page of Exhibit A, a notice appears that reads as follows: “Copies may be requested from IBM Thomas J. Watson Research Center, Publications office 16-220, P. O. Box 218, Yorktown Heights, NY 10598.” I obtained Exhibit A from counsel. Exhibit A is complete; no pages are missing, and the text on each page appears to flow seamlessly from one page to the next; further, there are no visible alterations to the document. Exhibit A is a true and correct copy in a condition that creates no suspicion about its authenticity.

41. **University of Alabama – Birmingham.** Attachment 1A is a true and

correct copy of the MARC record for this technical report from the online catalog in the Mervyn H. Sterne Library at the University of Alabama – Birmingham (UAB). Library ownership is indicated by the presence of the library code (ABC) in field 049. According to the metadata in Attachment 1A, the Basturk technical report was cataloged on September 1, 1995 (as recorded in field 008 “950901”) and was based on OCLC record number 33074839 (see first field 035). The Basturk technical report is identified as part of the Research Report series prepared by staff in the IBM Research Division as document number RC 19981 (see field 490). A cataloger prepared basic information about the technical report which included the title (field 245), publisher (field 260), extent of the item (field 300), series (fields 490 and 830), subject headings (fields 650 and 653), author/creator (field 700), contributing authors/creators (field 500), and locally assigned Library of Congress classification number (field 090).

42. In response to a request, cataloguing librarians at UAB reported that the “x” after the date is not an official Library of Congress symbol, but simply means that was catalogued locally. They cannot provide further information about the publication date or the receipt date. Typically, a cataloger will handwrite the call number on the item before a more permanent spine label is affixed.

43. The library continues to update and enhance the MARC record to meet current cataloging rules. The most recent enhancement to this MARC record

occurred on March 2, 2023, as shown in the field 005 (“20230302”) of Attachment 1A. I personally identified and retrieved the library catalog records which is Attachment 1A.

44. Based on finding a print copy of the technical report titled *Secure Transport Protocols for High-Speed Networks* in the Mervyn H. Sterne Library at the University of Alabama – Birmingham and MARC record in its online library catalog attached as Attachment 1A, it is my opinion that the Basturk technical report was publicly available by at least September 1, 1995.

45. Attachment 1A further includes an entry in field 090 (“TK5105.59 \$b .S4435x”) as described above, this includes a subject matter classification number consistent with the Library of Congress classification system (analogous to the Dewey Decimal classification system). Attachment 1A further includes two descriptor terms reading “Computer networks \$x Security measures \$x Computer programs” (see Attachment 1B, Library of Congress subject heading sh94001277 and Attachment 1C, Library of Congress subject heading sh85029524) and “Computer network protocols” (see Attachment 1D, Library of Congress subject heading sh85029512) in the 650 fields. Thus, as of its cataloging, the publication corresponding to the MARC record attached hereto as Attachment 1A was indexed according to its subject matter by virtue of at least two independently sufficient classifications: the field 090 entry and the field 650 entries. Further, as of

September 1, 1995, the MARC record attached hereto as Attachment 1A was accessible through any library with access to the OCLC bibliographic database or the online catalog at a library that added this technical report to its collection, which means that the corresponding publication was publicly available on or before that same date through any library with access to the OCLC bibliographic database or through an individual library.

46. Stanford University Libraries. Attachment 1E is a true and correct copy of the MARC record for this technical report from the online catalog in the Stanford University Libraries (Palo Alto, California). Library ownership is indicated by the presence of the library code (STF) in field 049. According to the metadata in Attachment 1E, the Basturk technical report was cataloged on July 20, 1995 (as recorded in field 916 “19950720”) and was based on OCLC record number 33074839 (see first field 035). The Basturk technical report is identified as part of the Research Report series prepared by staff in the IBM Research Division as document number RC 19981 (see field 490). A cataloger prepared basic information about the technical report which included the title (field 245), publisher (field 260), extent of the item (field 300), series (fields 490 and 830), subject headings (fields 650 and 653), author/creator (field 700), contributing authors/creators (field 500), and locally assigned Library of Congress classification number (field 090).

47. The library continues to update and enhance the MARC record to meet current cataloging rules. The most recent enhancement to this MARC record occurred on March 2, 2023, as shown in the field 005 (“20230302”) of Attachment 1E. I personally identified and retrieved the library catalog records which is Attachment 1E.

48. Based on finding a print copy of the technical report titled *Secure Transport Protocols for High-Speed Networks* in the Stanford University Libraries and MARC record in its online library catalog attached as Attachment 1E, it is my opinion that the Basturk technical report was publicly available by at least September 1, 1995.

49. Attachment 1E further includes an entry in field 090 (“TK5105.59 \$b .S4435x”) as described above, this includes a subject matter classification number consistent with the Library of Congress classification system (analogous to the Dewey Decimal classification system). Attachment 1E further includes two descriptor terms reading “Computer networks \$x Security measures \$x Computer programs” (see Attachment 1B, Library of Congress subject heading sh94001277 and Attachment 1C, Library of Congress subject heading sh85029524) and “Computer network protocols” (see Attachment 1D, Library of Congress subject heading sh85029512) in the 650 fields. Thus, as of its cataloging, the publication corresponding to the MARC record attached hereto as Attachment 1E was indexed

according to its subject matter by virtue of at least two independently sufficient classifications: the field 050 entry and the field 650 entries. Further, as of September 1, 1995, the MARC record attached hereto as Attachment 1E was accessible through any library with access to the OCLC bibliographic database or the online catalog at a library that added this technical report to its collection, which means that the corresponding publication was publicly available on or before that same date through any library with access to the OCLC bibliographic database or through an individual library.

50. Carnegie Mellon University. Attachment 1F is a true and correct copy of the MARC record for this technical report from the online catalog in the Hunt Library at Carnegie Mellon University (Pittsburgh, Pennsylvania). Library ownership is indicated by the presence of the library code (PMC) in field 049. According to the metadata in Attachment 1F, the Basturk technical report was received in the cataloging department on August 22, 1995 (see field 910) and was cataloged on September 1, 1995 (as recorded in the “Entered” field, “19950901”). A cataloger in the Hunt Library at Carnegie Mellon University prepared basic information about the technical report which included the title (field 245), publisher (field 260), extent of the item (field 300), series (field 490), subject heading (field 650), author/creator (field 700), and locally assigned Library of Congress classification number (field 099). The cataloger contributed the MARC

record to the OCLC bibliographic database as OCLC record number 33074839 (see field 903). The Basturk technical report is identified as part of the Research Report series prepared by staff in the IBM Research Division as document number RC 19981 (see field 810). I personally identified and retrieved the library catalog records which is Attachment 1F.

51. Based on finding a print copy of the technical report titled *Secure Transport Protocols for High-Speed Networks* in the Hunt Library at Carnegie Mellon University and MARC record in its online library catalog attached as Attachment 1F, it is my opinion that the Basturk technical report was publicly available by at least September 1, 1995.

52. Attachment 1F further includes a descriptor term reading “Computer network protocols” (see Attachment 1D, Library of Congress subject heading sh85029512) in the 650 field. Further, as of September 1, 1995, the MARC record attached hereto as Attachment 1F was accessible through any library with access to the OCLC bibliographic database or the online catalog at a library that added this technical report to its collection, which means that the corresponding publication was publicly available on or before that same date through any library with access to the OCLC bibliographic database or through an individual library.

53. OCLC bibliographic database and WorldCat. Based on finding a print copy of the technical report titled *Secure Transport Protocols for High-Speed*

Networks in the Hunt Library at Carnegie Mellon University and MARC record in its online library catalog that as contributed to the OCLC bibliographic database and its publicly available database WorldCat (see Attachment 1G), it is my opinion that the Basturk technical report was publicly available by at least September 1, 1995, as shown in the “Entered” field (“19950901”). The IBM report number on Exhibit A (RC 19981) matches the metadata in field 088 of Attachment 1G. Therefore, Exhibit A is the same technical report as the one that the cataloger in the Hunt Library at Carnegie Mellon University used to create the MARC record that is Attachment 1G.

54. Attachment 1G further includes a descriptor term reading “Computer network protocols” (see Attachment 1D, Library of Congress subject heading sh85029512) in the 650 field. Further, as of September 1, 1995, the MARC record attached hereto as Attachment 1G was accessible through any library with access to the OCLC bibliographic database or the online catalog at a library that added this technical report to its collection, which means that the corresponding publication was publicly available on or before that same date through any library with access to the OCLC bibliographic database or through an individual library.

55. Attachment 1G indicates that the technical report titled *Secure Transport Protocols for High-Speed Networks* as cataloged in the Hunt Library at Carnegie Mellon University is currently available from 3 libraries. In view of

above, the technical report titled *Secure Transport Protocols for High-Speed Networks* was publicly available on September 1, 1995, because by that date it had been received, cataloged, and indexed in the Hunt Library at Carnegie Mellon University and made part of the OCLC bibliographic database. For these reasons, it is my opinion that Exhibit A was published and accessible to the public on September 1, 1995.

56. **IBM Libraries.** The public availability of the Basturk technical report is further confirmed by Julia O’Keeffe, Global Librarian and Publications Catalog Manager at the IBM T. J. Watson Research Center. I’ve reviewed communications from Julia O’Keeffe in which she stated that IBM Research Reports were publicly available but that there was not a formal distribution system. At that time, the reports were available upon request from IBM (see ¶ 34). Typically, a researcher would see a citation to a report in another work, and then request a copy of the report.

57. Further, Ms. O’Keeffe said that there was not an internal system to track subsequent publications of specific reports in an IBM journal or in an outside journal. However, Ms. O’Keeffe indicated that it was unlikely that a report was later published in an IBM-sponsored journal if it did not appear in either the *IBM Systems Journal* (1962-2008) or the *IBM Journal of Research and Development* (1957-2020). Archives of both journals have been transferred to the Institute of

Electrical and Electronic Engineers (IEEE) for inclusion in the *IEEE Xplore* database.

58. In the past, IBM had a larger library system of private, corporate libraries with several locations that were not open to the public. Ms. O’Keeffe noted that she is currently the only librarian at IBM. She joined IBM in 2018 and does not have any institutional knowledge from the 1990s, nor is there anyone left to ask. She stated that there are no available records from the 1990s, nor is there a method of tracking the public availability of a particular report. If a report were classified as confidential, it would have been marked on the report. Further, IBM did not publicize the availability of research reports.

59. **Citations of the Basturk technical report.** Ms. O’Keeffe is not able to identify the way in which researchers or members of the public would have found out about the Basturk report. She said that a researcher would have obtained a copy of the document from another author or someone the author knew at IBM. Therefore, in view of the above, the Basturk technical report was publicly available by September 1, 1995, because by then it had been cataloged and indexed, made part of the OCLC bibliographic database, and received in at least one library. This is further confirmed by the bibliographic citations of the Basturk technical paper that appeared in a conference paper and on lists of resources related to the topic.

60. A conference paper titled “Digital Signcryption or How to Achieve $\text{Cost}(\text{Signature} \ \& \ \text{Encryption}) \ll \text{Cost}(\text{Signature}) + \text{Cost}(\text{Encryption})$ ” by Yuliang Zheng (hereafter “Zheng”) was published in the a book titled *Advances in Cryptology -- CRYPTO '97* on pages 156-179. The CRYPTO '97 conference was held on August 17-21, 1997, in Santa Barbra, California. Zheng cited the Basturk technical report in his paper as the first reference on page 178 (see Attachment 1H, page 14). The Zheng conference paper is also available from the publisher, Springer,¹⁶ and is cited in the ACM Digital Library,¹⁷ the digital repository *Semantic Scholar*,¹⁸ and the International Association for Cryptologic Research website.¹⁹ The publisher’s website indicates that the conference proceedings volume was publicly available online by January 1, 1006. Specifically, the text is complete; no pages are missing, and the text on each page appears to flow seamlessly from one page to the next; further, there are no visible alterations to the document. Attachment 1H can be found within the custody of a library – a place where, if authentic, a copy of this conference proceedings volume would likely be. Attachment 1H is a true and correct copy in a condition that creates no suspicion

¹⁶ <https://link.springer.com/chapter/10.1007/BFb0052234>

¹⁷ <https://dl.acm.org/doi/10.5555/646762.706181>

¹⁸ <https://www.semanticscholar.org/paper/Digital-Signcryption-or-How-to-Achieve-%26-%3C%3C-%2B-Zheng/072e8123e534331625f52111cb5b7c0441bee8aa>

¹⁹ <https://www.iacr.org/cryptodb/data/paper.php?pubkey=1857>

about authenticity.

61. I downloaded the Zheng conference paper from the publisher's website. The Basturk citation on the publisher's website links to Google Scholar.²⁰ However, the document that appears is titled *Secure Transport Protocols for High-Speed Networks* and is dated March 1994 (Attachment 1I). The document is hosted on the Department of Computer Science & Engineering in the Jacobs School of Engineering at University of California – San Diego (UCSD) website.²¹ The UCSD website includes the Zheng conference paper ("srtp.pdf") in a bibliography that was last updated on August 2, 2021.²² Therefore, the version of the Basturk technical report is different than Exhibit A.

62. A technical report titled *Secure Transport Protocols for High-Speed Networks* appears on a bibliography maintained by Be Hubbard and Ronald L. Rivest.²³ The website is part of the Theory of Computation (TOC) which is part of the Computer Science and Artificial Intelligence Laboratory (CSAIL) at the Massachusetts Institute of Technology (MIT)²⁴ The Hubbard and Rivest bibliography was last updated on April 2, 1995. The technical report titled *Secure*

²⁰ <https://cseweb.ucsd.edu/~mihir/papers/srtp.pdf>

²¹ <https://cseweb.ucsd.edu/>

²² <https://cseweb.ucsd.edu/~mihir/papers/>

²³ <https://web.mit.edu/~bjaspan/lib/tex/bibtex/bib/rivest-crypto.bib>

²⁴ <https://toc.csail.mit.edu/>

Transport Protocols for High-Speed Networks lists the authors as Mihir Bellare, Erol Basturk, Chee-Seng Chow, and Roch Guerin and a January 1994 date. The technical report cannot be downloaded from the web page.

63. The Basturk technical report titled *Secure Transport Protocols for High-Speed Networks* appears in the Technical Paper Archive – Research Reports maintained by IBM.²⁵ The Basturk technical report is listed as document 69. Clicking on the technical report title results in the display of the abstract and the limited distribution notice that appear on pages 4 and 3 of Exhibit A. The document is identified as RC 19981 with a 1994 date. The technical report cannot be downloaded from the web page.

VIII. SUMMARY OF OPINIONS

64. In view of the foregoing, it is my opinion that the publications described above were publicly available no later than the corresponding date listed in the table below:

Exhibit	Publication	Publicly Available No Later Than
A	Basturk, Erol, Mihir Bellare, Chee-Seng Chow, and Roch Guerin. <i>Secure Transport Protocols for High-Speed Networks</i> . Research report RC 19981. Yorktown Heights, NY: IBM T. J. Watson Research Center, 1994.	September 1, 1995

65. I declare that all statements made herein of my knowledge are true,

²⁵ <https://dominoweb.draco.res.ibm.com/>

and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: May 23, 2023

By: 
Sylvia D. Hall-Ellis, Ph.D.

EXHIBIT A

TK
5105.59
S4435
1994x

SECURE TRANSPORT PROTOCOLS
FOR HIGH-SPEED NETWORKS



The University of Alabama at Birmingham

**Mervyn H. Sterne
Library**

917 13th Street South
Birmingham, Alabama 35294

TK
5705.59
S4435
1994x

Research Report

Secure Transport Protocols for High-Speed Networks

E. Basturk, M. Bellare, C.-S. Chow and R. Guérin

IBM Research Division
T. J. Watson Research Center
Yorktown Heights, NY 10598

LIBRARY
UNIVERSITY OF ALABAMA
LIBRARY

LIMITED DISTRIBUTION NOTICE

This report has been submitted for publication outside of IBM and will probably be copyrighted if accepted for publication. It has been issued as a Research Report for early dissemination of its contents and will be distributed outside of IBM up to one year after the date indicated at the top of this page. In view of the transfer of copyright to the outside publisher, its distribution outside of IBM prior to publication should be limited to peer communications and specific requests. After outside publication, requests should be filled only by reprints or legally obtained copies of the article (e.g., payment of royalties).

IBM Research Division
Almaden • T.J. Watson • Tokyo • Zurich

INFORMATION SCIENCES
INSTITUTE LIBRARY

Secure Transport Protocols for High-Speed Networks

EROL BASTURK* MIHIR BELLARE† CHEE-SENG CHOW‡ ROCH GUÉRIN§

Advanced Networking Laboratory
IBM T.J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598, USA.

January 31, 1994

Abstract

We argue that the increasingly widespread use of networks is leading to new security concerns such as *secure delivery* which are most naturally associated with the *transport level* and best addressed by the design of *secure transport protocols*. We present *general methods* for such a design which are directed at optimizing performance on a *high speed network*. Our work reflects the experience gained in designing and implementing a particular *secure transport protocol*.

* e-mail: basturk@watson.ibm.com.

† e-mail: mihir@watson.ibm.com.

‡ email: cschow@watson.ibm.com.

§ email: guerin@watson.ibm.com.

1. Introduction

The purpose of this paper is to provide a comprehensive overview of the current state of research in the field of artificial intelligence (AI). The paper will focus on the recent developments in machine learning, natural language processing, and computer vision. The first section will discuss the challenges and opportunities in AI research. The second section will review the state-of-the-art in machine learning, including supervised, unsupervised, and reinforcement learning. The third section will discuss the recent advances in natural language processing, such as sequence-to-sequence models and attention mechanisms. The fourth section will review the state-of-the-art in computer vision, including convolutional neural networks and generative models. The paper will conclude with a discussion of the future directions of AI research.

The paper is organized as follows. Section 2 discusses the challenges and opportunities in AI research. Section 3 reviews the state-of-the-art in machine learning. Section 4 discusses the recent advances in natural language processing. Section 5 reviews the state-of-the-art in computer vision. Section 6 concludes with a discussion of the future directions of AI research.

Artificial intelligence (AI) is a branch of computer science that aims to create machines that can perform tasks that require human intelligence. The field of AI has a long history, dating back to the 1950s. In the early days, AI was primarily concerned with the development of algorithms that could solve specific problems, such as playing chess or solving puzzles. However, in recent years, AI has made significant progress in many areas, including machine learning, natural language processing, and computer vision. This progress has been driven by a combination of factors, including the availability of large amounts of data, the development of powerful algorithms, and the increasing computational power of modern computers. In this paper, we will provide a comprehensive overview of the current state of research in AI, focusing on the recent developments in machine learning, natural language processing, and computer vision.

Machine learning is a subset of AI that focuses on the development of algorithms that can learn from data. There are three main types of machine learning: supervised learning, unsupervised learning, and reinforcement learning. Supervised learning involves training a model on a dataset of labeled examples, so that it can learn to map new inputs to the correct output. Unsupervised learning involves training a model on a dataset of unlabeled examples, so that it can learn to find patterns in the data. Reinforcement learning involves training a model to learn how to take actions in an environment to maximize a reward. Machine learning has many applications, including image recognition, speech recognition, and recommendation systems.

Natural language processing (NLP) is a branch of AI that focuses on the development of algorithms that can understand and generate human language. NLP has many applications, including machine translation, sentiment analysis, and text summarization. In recent years, NLP has made significant progress, particularly in the area of sequence-to-sequence models, which are used for tasks such as machine translation and text generation. Attention mechanisms have also been developed, which allow models to focus on specific parts of the input when generating output. These advances have led to significant improvements in the performance of NLP systems.

1 Introduction

As we entrust more and more of our communication to networks, the concern with security increases. This paper begins by arguing that the *nature* of the security guarantees which users will need and expect is changing. In particular, new requirements, like *secure delivery*, are emerging. In contrast to traditional security features which tend to be purely application level, the new ones are most naturally identified with the transport level. We suggest the design of *secure transport protocols* as the most effective way of filling all needs, and present a general method to transform a given transport protocol into a secure one. The design puts particular emphasis on maintaining the level of performance of the original transport protocol, particularly in a high speed environment. Our work reflects the experience gained in the design and implementation of a specific secure high-speed transport protocol.

1.1 Security requirements and their placement

Two parties, denoted A and B , communicate over a network. We will naturally view the parties as applications who use a common transport protocol. An adversary E monitors the parties' communications, and is even capable of injecting or removing messages from the lines. Nonetheless, the parties wish to be able to communicate "securely." Their advantage over E is to possess a random, shared secret key a (eg. a DES key) which E doesn't know.^{1,2}

Our discussion of security features which follows takes the perspective of a designer and architect of a secure communications medium. It reflects the need to add security functionality in a way which is consistent with, and best matches, the existing communication structure. To this end, we distinguish security features according to the layer of the communication structure to which they are most naturally associated. We found that the traditional features are mostly application level, while the new ones we deem necessary are transport level.

APPLICATION LEVEL SECURITY FEATURES: INTEGRITY AND CONFIDENTIALITY. *Integrity* and *confidentiality* are the two traditional, and important, security features. The first means that it isn't possible for E to modify the contents of transmitted data. The second means that E cannot figure out the content of the transmission but the receiver can recover it. Note they are requirements

¹ How they come into possession of such a key is not our concern here. Rather, the problem is how to use the key to communicate securely.

² For simplicity we stick to this symmetric case. Our methods can be modified to work in the public key scenario as well.

on the *data* transmitted by the application. This is the reason we view them as application level security features, a view which is reflected in the traditional method of providing these features, which we discuss next.

APPLICATION LEVEL SECURITY. Application level security features are easily (and usually) provided by *application level security*. Here the sender applies appropriate cryptographic functions to his data *before* passing it to the transport for conveyance. This is the approach of Kerberos [5] and KryptoKnight [3]. Integrity is usually guaranteed by *signing* the data before passing it to the transport level. Confidentiality is usually guaranteed by having *A encrypt* the data before passing it to the transport level, and having *B decrypt* the ciphertext which is received by his transport module and passed up to him.

TRANSPORT LEVEL SECURITY FEATURES: SECURE DELIVERY. Secure delivery, roughly speaking, is a guarantee to the sender *A* that his message was received by *B* and not intercepted and destroyed by the adversary. It is essentially an extension of the standard transport level *reliability* feature to the more adversarial setting we are discussing, which is why it seems most natural to view it as a transport level feature.

Note that the presence of the application level security features does not necessarily imply the **security of delivery**. The adversary can easily make a sending application believe that whatever it **transmitted** has been received by the receiving application, even if the data are signed or encrypted by the upper layer. How? Suppose *A* sends some data to *B* which *E* would prefer never reaches *B* (we will see later examples of why *E* might like to do this). *E* stops the data from reaching *B* (remember, all communication goes through her and she has the power to do this). Then, she sends a transport level acknowledgement of received data to the sending port. This acknowledgement is a transport level flow. Not being generated by an application, it is not signed. The transport protocol at the sending end will believe the acknowledgment, and tell the sender that its data has been received!³

Is the lack of secure delivery a serious security problem? Yes. Here are two examples that help see **why**. The first is the example that lead us to pinpoint the problem. It is the problem of securing control flows in a network. We have a number of (trusted) network *control points* linked by a **spanning tree**. At any time, one control point is the root of the tree. Suppose *A* wishes to pass

³ An implicit assumption is that the application is not performing its own acknowledgments and retransmission, but, more naturally, relying on the transport for these features. Indeed, asking the application to duplicate these transport functions is usually poor design in that it belies the layered communication structure, and would also adversely affect performance.

its root position to B . It sends a (application level signed) messages saying so, and, assuming the message arrived, relinquishes the root position itself. Without secure delivery, we don't know B got the message, and now the tree has no root.

Suppose B is a broker, and A and (the adversary) E both want to buy a certain stock. E prevents A 's purchase requests from reaching B so that she can buy the stock herself.

Actually secure delivery is only one example of a transport level security feature that is desirable. In Appendix A we will discuss things more formally and point to a mathematical notion of security which we believe captures the actual requirement, and includes secure delivery, integrity (and, optionally, confidentiality) as special cases. Roughly, we will ask that either the flows between the parties maintain, in the presence of E , the "relative ordering" as well as content that they would have if E were not present, or the parties detect the presence of E .

TRANSPORT LEVEL SECURITY. In this design, the application passes its key a to the transport module, and leaves to the latter the task of applying any cryptographic functions or taking other security steps. The advantage is that the transport module can compute a signature which covers not only the data but also (relevant parts of) the transport header which it creates, particularly the byte sequence numbers. It can also sign the acknowledgments messages which exist only at the transport level. As we will see, these possibilities are key to the provision of secure delivery.

1.2 The design of efficient and secure transport protocols

We specify a method to transform any transport protocol into a "secure" version, equipped not only with the new security features discussed above, but providing, at least as options, the standard application level security features. Below we discuss the elements of the solution followed by some of its features.

ELEMENTS OF THE SOLUTION. The design will be specified in full in the body of the paper, but here is a brief sketch. The secure transport protocol has two phases, the *initialization* phase and the *steady state*. In the former, an *entity authentication and key exchange* protocol is executed. This authenticates the parties and yields them a *session key* α . In the steady state, if the integrity option is selected, both data integrity and secure delivery are provided by attaching to each packet a signature, computed under key α , and taken over some portions of the header and the data payload. Note that acknowledgments, which have no data, are also signed. If confidentiality is desired, the data is encrypted, also under α . See the rest of the paper for more details on which parts of the header must be signed and which left in the clear; why the design guarantees secure

delivery; and also for explanations on why a session key is needed when the parties already share the long lived key a .

COMPATIBILITY. Usually, applications are written on top of an existing transport protocol before any security is included in it. We want to assure *compatibility* of a secure version of this protocol with the regular non-secure version. The secure transport protocol then becomes a superset of the regular transport protocol. Applications using the regular transport protocol should not have to be modified at all.

PERFORMANCE. We take into account various *efficiency* requirements for the secure version of a transport protocol. Certain functions should be designed so that they can readily be off-loaded to hardware without impacting the original flow and processing of messages. Specifically, encryption and decryption may initially be performed in software, but, as speed increases, dedicated hardware components will almost certainly be required. For example, software encryption and decryption for secure video conferences may be feasible at low resolution. However, the provision of high resolution secure video conferences is likely to require hardware support. Our protocol should be able to operate in both environments. There are many other design aspects that need to reflect this requirement. For example, it may be worthwhile to factor into the design the eventual parallelization of certain processes, to define "intelligent" packet format for faster parsing, to allow rapid context retrieval based on simple connection-based information – all these things should be considered in order to provide greater efficiency.

In addition, the design should seek to minimize the performance degradation resulting from the provision of security. Obviously, performance degradations cannot be avoided altogether as security typically involves additional flows and/or processing. The goal, though, is to limit such degradations by restricting the number of new flows needed to support security functions, and by remaining as true as possible to the design philosophy of the original transport protocol. For example, latency can be reduced if the same flows used to authenticate the two parties wishing to communicate, also serve as the vehicle for distributing the session key they will use. Similarly, further reduction can be achieved by including user data in the initial authentication flows, so that under the optimistic (but generally true) assumption that authentication will succeed, data transmission is not unnecessarily delayed. Whenever possible, security segments are "piggybacked" on, or combined with, existing flows.

PROOFS. We mentioned above that we have a mathematical definition of the security properties our protocol should satisfy. Correspondingly, we have proofs that if certain cryptographic functions,

such as the DES, are suitably hard, then our design meets the definition.

IMPLEMENTATION. Section 3 briefly describes an implementation in which we added security features to an existing high-speed transport protocol. The implementation embodies the design principles outlined above as well as functions and techniques discussed in the rest of the paper.

2 Design of a secure transport protocol

An understanding of our design choices is facilitated by first explaining the performance issues which influence them. Following this explanation we specify the user interface of the secure transport protocol and a high level sketch of the design. Then we go deeper into the components.

2.1 Performance Issues

While previous sections motivated the need for security at the transport layer, they also mentioned a number of performance considerations that are of importance when designing an efficient secure transport protocol. Here we review these performance issues and describe how they influence the design. Details specific to individual components are provided in subsequent sections.

The provision of security is bound to somewhat degrade performance, but the goal is to keep this impact at a minimum. A first generic step towards minimizing the perceived performance impact of security is to provide a range of security “options” to users. Each option corresponds to a different trade-off between the level of security it affords and its cost in terms of performance. For example, users with different requirements may want to choose between encryption algorithms of different complexity and strength. It is, therefore, important to incorporate the flexibility of such choices when designing a secure transport protocol. Accordingly, our design provides a wide range of security options which are further detailed later.

There are, however, performance issues that are common to any security option, and their impact should also be minimized. Performance degradations caused by the provision of security have two major causes: additional flows and increased processing. Additional flows are typically required for authentication purposes during the initial phases of a connection. Increased processing is the result of the computational requirements of security functions such as signature generation and verification, and encryption/decryption. We now review the design implications of both, and identify the components they impact most.

ADDITIONAL FLOWS. As mentioned above, security typically requires additional flows during the initial (setup) phase of a connection. This translates in an increased overhead and a greater latency

before data transmissions can start. This can be particularly significant for short connections. There are, however, several rules that can/should be followed to limit this.

A first and obvious one is to restrict the number of additional flows needed, i.e., provide as many security functions as possible in each flow. For example (see below), key distribution can be carried out jointly with the first authentication flow rather than through a separate one. Another simple rule is to combine security flows, whenever possible, with existing protocol flows. For example, initial authentication flows can be piggybacked onto the connection establishment procedures (if authentication fails, the connection is aborted). This allows the parallelization of authentication and connection handshakes and limits, therefore, any increase in latency. Finally, a last step to minimize latency is to allow data transmission to start even before the authentication (or connection establishment, for that matter) phase has completed. This can be achieved by allowing the inclusion of user data in the initial authentication/connection flows (again, the data are discarded if the authentication fails).

To summarize, the three design rules that should be followed in order to limit the performance impact of security flows are as follows:

- (1) Minimize the number of additional flows;
- (2) Piggyback security flows on existing protocol flows;
- (3) Allow early data transmission (during initialization phase).

The design we describe below follows these design rules.

INCREASED PROCESSING. The other aspect of security that has the potential to degrade performance is the additional processing required by security functions. This is most significant for long connections as it applies to all steady state transmissions. There are, however, again some rules that can be followed to limit this impact.

The main one is that all computations should be performed in the most timely fashion possible. In other words, while an increase in the amount of computation is unavoidable, it is important to ensure that nothing slows down or delays this additional processing. In all instances we would like all computations to be carried out "on-the-fly" as data is being transmitted or received. This minimizes latency.

When applied to security functions such as signature generation and verification or encryption/decryption, the requirement of on-the-fly processing has several implications. For example, we would like decryption of a received packet to proceed independently of that of any other packet (note that this also allows parallelization) as packets may be received out of order.

Computation of cryptographic functions can be greatly speeded up by use of dedicated hardware. Our design does not require such hardware to be available, but adopts various design principles that would allow this hardware, if available, to be exploited in the best possible way. On-the-fly processing is important in this regard as it facilitates the eventual off-loading to the hardware. Both signature computation and encryption/decryption rely on the use of secret information (key) shared by the two communicating parties. Retrieval of this information is, therefore, necessary for such processing. While one can assume its immediate availability when transmitting data, it must typically be retrieved upon receipt of a packet and this context retrieval step can introduce latency. It is, therefore, useful to design security functions, in particular signature computation, which allow processing to start immediately upon arrival of data, without waiting for the associated context retrieval to complete.

To summarize, our requirement for timely and on-the-fly security computations translates into three specific design rules:

- (1) Signature computation starts before the retrieval of connection context;
- (2) Packets are independently encrypted;
- (3) Hardware utilization is facilitated wherever possible.

2.2 The user interface

STARTUP INFORMATION. Each potential user (application) A of the secure transport protocol has a table T_A whose entries are pairs: $T_A = (A_1, a_1), \dots, (A_N, a_N)$ for some N . Each A_i is the identity of another user, and a_i is the key shared by A and A_i (but not known to any other user or the adversary). Henceforth this key will be referred to as the *long lived* key (LL-key).

CONNECTION INITIATOR INTERFACE. Now suppose A wishes to initiate a connection with B , with whom it shares LL-key a . It interfaces with a local piece of software to which it passes the identity B and the key a . It can also control the nature and strength of the security to be provided by specifying some options which will be discussed below. This software creates for her an entity we call her *secure transport machine* and denote by M_A . Once initialized, A can send (and receive) data via the secure transport machine just as it would via the original (insecure) version. That is, when it wants to send a message m , it passes it to the secure transport machine, and the latter is responsible for relaying the message, applying any necessary cryptographic functions to it, taking care of retransmission, and in general providing all transport facilities.

RESPONDER INTERFACE. At the receiving end, party B has also initialized a secure transport

machine M_B . This machine has access to the table T_B of identities and associated keys. An incoming packet identifies the identity of the (claimed) sender, and the receiving machine then uses the table to get the associated key. With this key it can now verify signatures or perform any other necessary cryptography.

SUMMARY. In summary, we view A as having a secure machine M_A with which it interfaces. Similarly, B interfaces with its secure machine M_B . The cross network communication is performed by the two machines, who send each other packets across the network and are responsible for the secure transport mechanism.

OPTIONS. The options amongst which the initiator can select are the following.

- (1) *Authentication and session key exchange (AKE) protocol specification.* The application chooses one out of a set of four possible authentication and session key exchange (AKE) protocols to be executed at the beginning of the interaction. The choices are described in Section 2.4.
- (2) *Integrity option.* If this option is selected then data integrity and secure delivery are provided. Otherwise they are not provided.
- (3) *Confidentiality option.* If this option is selected then data confidentiality is provided by encryption. Otherwise, the data will be in the clear.
- (4) *Basic cryptographic primitive specification.* The protocol lists a set of cryptographic primitives such as MD5 (Message Digest number 5), SHA (Secure Hash Algorithm), DES (Data Encryption Standard) and double DES, which it will use to provide both integrity and confidentiality. The application chooses which one to use.

As discussed in Section 2.1, the purpose of providing options is to allow the user to trade security for performance. We now see how this is reflected in the last three options listed above. The discussion on AKE selection is in Section 2.4.

An application which wants, say, only integrity, should not be unnecessarily burdened with the performance cost inherent in providing encryption. Similarly an application wanting only confidentiality should not be burdened with the cost of signing inherent in providing integrity. So integrity and confidentiality are better made (orthogonal) options.

Cryptographic primitives exhibit a trade-off between strength and speed: more secure primitives take more time to compute. An application which needs a high level of security must be willing to pay for it in performance, and can choose a primitive which is very strong but adds to the

performance cost. An application which needs just a little security can specify a weaker but faster primitive and get better performance.

2.3 Overview of design

We divide the design into the following components:

- (1) *Initialization: Authentication and session key exchange.* When A initializes M_A (by passing it B 's identity and the shared key a) the machine initiates and executes an authentication and key exchange protocol with M_B . Specifically, the protocol used is the one chosen by the initiator in the options specified above. This protocol results in the distribution of a new (fresh) *session key* α while making sure that this key is authentic (ie. known only to M_A and M_B).
- (2) *Steady state:* Initialization completed, M_A is ready to receive data from the application A and send it to B ; similarly, M_B is ready to receive data from M_A and pass it to B .
 - (2.1) *Integrity via signing.* If the integrity option is selected then data is *signed* by M_A under the session key α (a signature is also called a MAC, or message authentication code). The signature covers not only the data payload but also the transport header (as explained later). On receiving a signed packet, M_B uses α to verify the signature.
 - (2.2) *Confidentiality via encryption.* If the confidentiality option is selected then the data payload is encrypted by M_A under the session key α . On receiving a packet, M_B uses α to decrypt the payload and then passes the plaintext to B .

The following sections explain the components indicated above.

2.4 Authentication and session key exchange

As discussed above, the secure session begins with an authentication and key exchange protocol which yields to the parties a session key α to be used (to sign and encrypt) in the rest of the session. The first thing that needs to be explained is: Since the parties already share a key (namely the LL-key a) why get another one? The use of a session key has several motivations. First, it helps avoid cross session attacks in which data from one session are replayed in another. Second, it minimizes exposure of the long lived key. It is a standard technique in cryptographic practice. Notice that only the transport machines M_A and M_B know about the session key. A and B never see it.

There are many AKE protocols reflecting, as usual, a trade-off between performance and security. Following our principle of allowing the application the option of choosing its level of trade-off we will specify several options of AKE protocols. To discuss them let's begin by looking at the issues. There are three basic kinds of authentication. *Initiator* authentication leaves the responder convinced of the identity of the initiator, but not necessarily vice versa. *Responder* authentication leaves the initiator convinced of the identity of the responder, but not necessarily vice versa. *Mutual* authentication leaves each party convinced of the identity of the other.

AKE protocols typically use either *timestamps* or *nonces* to ensure "freshness" of a party's flows. (A nonce as used here is a random number). Nonce based methods require more flows (or "passes" as they are called in this area) than timestamp ones and thus adversely affect performance. On the other hand, timestamps require some degree of clock synchronization, with decreasing security as one allows a greater margin of error in this synchronization.

Potentially we thus have six options: three kinds of authentication, and either timestamps or nonces in each case. When one examines the basic flow structure in each case, however (cf. [1]) it is easy to eliminate two of them.⁴ This leaves the following options.

- (1) *Initiator authentication with time stamp, one pass.* Initiator authenticates himself to responder in a single flow. Useful for secure datagrams.
- (2) *Responder authentication with nonces, two pass.* Responder authenticates himself to initiator. Protocol has the following basic form: initiator issues a nonce serving as a challenge, and responder answers. Two flows.
- (3) *Mutual authentication with time stamps, two passes.* The above protocols are combined. The initiator authenticates himself with a timestamped flow while simultaneously issuing a challenge, and the responder answers.
- (4) *Mutual authentication with nonces, three passes.* Each party authenticates the other with nonces. Three flows.

Our protocols are inspired by the AKE protocols of [1] but have been modified to increase efficiency. We briefly review the performance considerations which motivated these modifications, and identify the resulting design guidelines.

⁴ An initiator nonce based protocol would need three flows within which we can do mutual nonce based anyway; similarly a responder time stamped protocol would need two flows within which we can do responder nonce based anyway.

A first step towards minimizing the overhead imposed by security on connection setup is to embed session key distribution in the *first* authentication flow. That is, the receipt of the first flow suffices to recover the session key. Moreover, use of the long-lived key is eliminated after the first flow and only the session key is used. If hardware is being used for signing then this minimizes the key switching time for the initiator, since he can switch to the session key as soon as the first flow is dispatched.

User data are included in the authentication flows to reduce latency. These user data are then retained by the receiver and delivered only after the successful completion of the authentication process. In case the authentication fails, all previously received data are discarded, and the upper layer is notified of the authentication failure. Piggybacking control (connection) information in the initial authentication flows can also help lower the overhead imposed by security on connection setup.

Error rates are low in high-speed networks and authentication should succeed most of the time. Transmitting user data during the authentication process can, therefore, reduce latency without impacting security. More generally, the protocol will allow transmission of user data not only in the authentication flows themselves, but also in any “initial transmission window” which may be allocated to the transmitter.⁵

Note that data packets in the authentication flows are signed using the *session* key which is another reason to switch as soon as possible to using it instead of the long-lived key.

The AKE protocols use signatures, and some of the choices in their design reflect performance issues arising from signature consideration. These issues are a part of the next section.

2.5 Integrity and signatures

Signatures are used in the AKE protocols and also, if the integrity option is selected, in the steady state. In the latter, their use will guarantee a broad set of properties including protection of the data against modification, secure delivery, and protection against replay attacks. Let's begin by describing the mechanisms and see why they yield the above mentioned properties in the steady state. Then we will look at design choices which are motivated by performance issues and which apply to the use of signatures in both the AKE protocols and the steady state.

We denote by MAC_α a message authentication code under α . It has, roughly speaking, the following property. If an adversary sees a sequence $(m_1, \text{MAC}_\alpha(m_1)), \dots, (m_k, \text{MAC}_\alpha(m_k))$ of messages

⁵ An initial transmission window may be allocated by the transport protocol to minimize connection setup latency.

together with their MACs (or signatures), then it is infeasible for this adversary to produce a pair of the form $(m, \text{MAC}_\alpha(m))$ in which $m \notin \{m_1, \dots, m_k\}$.

In the steady state (integrity option assumed selected) the sender attaches to each packet p the value $\text{MAC}_\alpha(\bar{p})$ where $\bar{p}$ is the subset of p which includes the transport header, the full data payload, and the trailer of the packet p . We will see that of particular importance is the fact that the transport header includes the sequence number of the packet which is thereby covered by the MAC. We assume that all packets in each direction, even those which are purely transport level acknowledgements (ACKs), can be differentiated. A simple solution is to include in each packet a large enough (to avoid wrap-around) signature counter. We also assume that the transport header contains information which identifies the sender so that the identity of the sender is covered by the MAC as well. On receiving p, τ the receiver checks that $\tau = \text{MAC}_\alpha(\bar{p})$ and rejects the packet unless this is true.

The signature prevents the adversary from making the receiver accept packets which were not in fact produced by the sender. The signature by itself does not, however, prevent a *replay attack*. In this attack the adversary simply resends a packet which was previously sent by the sender, so that its signature is legitimate and will be accepted by the receiver.⁶ This attack fails because the signature also covers the (signature) sequence number of the packet, and the receiver does not accept packets out of order. Indeed, as part of the normal transport level checking, out of order packets will be discarded.

The manner in which security against replay is guaranteed illustrates well an advantage of security at the transport level. Sequencing is a standard and already present transport function. We simply exploit its presence. Had we wanted to prevent replay at the application level we would have had to implement sequencing with transport level counters and provide for our own checking and retransmission, thereby not only making implementation significantly harder but duplicating the transport functionality and degrading performance.

Secure delivery is guaranteed because the ACKs include sequence numbers and are signed. Note that the signature also provides error detection, so that no CRC or error detection code is required. *Replaying* of packets from one session into another is not possible because each session has a different session key.

We now turn to design issues motivated by performance. Let us recall some of the issues identified

⁶ To see the importance of preventing such attacks, take the following example. The adversary collects one genuine ACK. Now, when the sender sends any flow, she can prevent secure delivery. She kills the sender's flow but replays to him the ACK she has from before. The sender accepts the ACK and believes his data has reached the receiver.

in Section 2.1. It is essential that the steady state overhead involved in computing and checking signatures and counters be kept to a minimum. Ideally, we want signatures to be computed and verified on-the-fly; i.e., MAC generation (verification) should be carried out as data transmissions (receptions) proceeds rather than before (after) these operations have completed. The goal is to avoid slowing down the regular flow of data, and allow the possible off-load of signature computations and verifications to dedicated hardware. The ability to achieve such on-the-fly processing depends on two major components. The first is the latency in retrieving the information needed to perform the necessary computations. The second is the nature of the computations themselves. The first component is most relevant at the receiver, while the second is equally important at both the transmitter and the receiver.

The main source of latency when receiving a new packet is the time needed to recover the associated connection context. The context contains information such as the shared session key, the counter value of the last accepted packet, the type of cryptographic function used, etc., which are central to the verification of a packet integrity. Some delay is obviously unavoidable when retrieving this information, but it should be made as small as possible and its impact on the packet verification process should be kept to a minimum. A first step in achieving this is to allow context retrieval to be performed as quickly as possible by specifying early on in the packet all the required information. While rapid context retrieval certainly helps it does not eliminate all initial latency, and it is therefore still important to allow computations to start even before the full context has been retrieved. Finally, latency can also be kept small by ensuring that computations are of minimal complexity while meeting our security requirements.

These different requirements have been incorporated in our design, where the goal of minimal latency is reflected in the following two rules.

First, all data used to generate the signature is present in the packet. Let's illustrate with an example from the AKE protocols. In such challenge response protocols, it is common that one party (say B) proves his identity by signing a challenge R_A sent by A . In such a case, rather than returning $\langle R_A, \sigma \rangle$ with $\sigma = \text{MAC}_\alpha(R_A)$, party B could return just the short tag σ ; after all, A already knows R_A (it is in A 's context) so why waste bandwidth sending it? The reason for preferring to send the full $\langle R_A, \sigma \rangle$ is that signature verification can begin without waiting for the outcome of context retrieval. On the other hand, the cost of resending R_A is minimal since bandwidth is not that expensive at these speeds. In general, this translates into the following packet format: a signed packet will be of the form $\langle D, \sigma \rangle$ where σ is a signature of packet D under key α .

Note that we cannot prevent context retrieval of R_A in the above example since A must definitely check that what is received is the signature of the right challenge (namely the challenge A just sent). But putting the information in the flow decouples the signature checking from this context retrieval.

Second, MAC computations are kept simple and can start prior to context retrieval. In particular, we rely on MAC implementations of the form $\text{MAC}_\alpha(m) = f_\alpha(h(m))$, where h is a (hash) function depending neither on α nor on the cryptographic primitive chosen in the initial options. The use of such an implementation will enhance performance in our setting as MAC computation does not have to wait for α and the cryptographic function to be retrieved from the context; we can begin computing $h(m)$ straight away. By the time we need to compute f_α the key α and cryptographic function will have been retrieved. In addition, since h can be chosen to be a standard hash function and only f_{α} needs to involve more computationally intensive cryptographic functions, the overall cost of signature generation/verification can be kept low.

The authentication protocols and packet formats of our implementation guarantee minimal latency by following the above two rules.

2.6 Confidentiality via encryption

Confidentiality means user data should not be readable by the adversary. The secure transport protocol will encrypt user data, under the session key, and use the ciphertexts as the actual payload. As encryption is done prior to packetization, the signature (if present) of an outgoing packet is computed *after* data encryption and the signature of an incoming packet is computed *before* decryption. This complies with the requirement of a signature computed “on the fly”. If the signature checking at reception fails, it means the packet is corrupted, and the packet is simply dropped: decryption is avoided.

Note that only user data are encrypted. One might, in principle, consider encrypting also certain parts of the transport headers. (We cannot, of course, encrypt the *entire* transport header: at a minimum the connection identifier must be in the clear to allow the receiver to know under which key it should decrypt!) Although encryption of parts of the transport headers might be argued to provide a higher degree of privacy, we believe the gain is marginal compared to the loss in performance. Encryption is a costly operation, and keeping it to a minimum is required. This also translates into a number of additional design rules.

In our design, we don’t want to reencrypt the data each time it must be retransmitted. Therefore, we make sure the ciphertexts (as opposed to the plaintexts) are available for retransmission. This

is achieved by requiring that a ciphertext $E(x)$ of plaintext x is of the same length of x , and simply replacing the input plaintext buffer with the corresponding ciphertext.

Next, we also want to minimize the processing associated with decryption so that it can always proceed with minimum latency, even in cases of errors and/or packet losses. Minimizing the associated processing means, among other things, that we would like to decrypt each packet only once. However, the ability to ensure this strongly depends on the retransmission policy used by the transport protocol. In particular, while selective retransmission readily allows only one decryption per packet, this is not necessarily true with go-back- n . In order to ensure, that under a go-back- n retransmission scheme decryption is performed only once for each packet, we must either stop decrypting as soon as a gap is detected (as it triggers a retransmission from the sender), or continue decrypting subsequent received packets but keep track of the associated spans. The first alternative introduces significant additional latency in the decryption process, while the second essentially amounts to implementing selective retransmission. Because of the inherent inefficiency of go-back- n during decryption, we recommend that selective retransmission be used when confidentiality is requested.

The requirement that decryption be able to proceed with minimum latency even in case of packet losses or errors, also introduces requirements on the encryption scheme itself. In general, an encryption scheme is said to have a *history of length i* if the ability to decrypt a ciphertext block is conditional on already being in possession of the decryptions of the i previous ciphertext blocks. Schemes with large history will not be acceptable, because the loss of a single block affects the ability to decrypt i blocks. This effectively prevents the decryption of several subsequent blocks, and translates into increased latency. The most commonly used encryption scheme, namely cipher block chaining, has a history of two; although this is low enough to be tolerable, we prefer to avoid it. Instead, we have designed encryption schemes with history 0, so that the decryption of any packet can proceed independently of the reception of others. In addition, the scheme is such that both the encryption and the decryption procedures are parallelizable. This is in line with our design requirement to maintain the ability to use hardware support.

Another important design consideration in selecting an encryption/decryption scheme is its impact on error propagation. Lines usually have some degree of noise, so that a bit can be flipped now and then. Encryption, however, can effectively amplify the channel noise. Suppose a bit is flipped in $X = E(x)$, the encryption of x , and the receiver gets X' . In many encryption schemes, the decryption $D(X')$ differs from x in more than one bit, i.e., a single bit error has propagated to multiple bits. For example, in cipher block chaining it could differ in up to half the bits. This

can translate in significant performance degradations for certain applications, whose data is either robust to limited errors (redundant information) or protected by some form of error correcting code. (Note that we assume here that data integrity is not selected as it would immediately result in the discarding of any packet in error, irrespective of the number of errors).

To avoid this problem, we use encryption schemes in which bit errors don't propagate. Specifically, our encryptions have the property that $d_H(E(x), E(y)) = d_H(x, y)$ for all x, y , where d_H is the Hamming distance. So error correcting on the plaintext is not affected. One might argue that the problem could have been solved in other ways. For example, put the ciphertext in error correcting form. This is bad for performance as well as inflexible. First, an application should have its choice of error correcting code and not have this dictated by the transport. Second, applications might be error correcting plaintext already, so that coding would be done twice.

To conclude, we stress that the extra features of our encryption schemes described above are obtained without any loss of security. Our encryption is DES based, and secure as long as DES behaves like a pseudorandom function. It even has security properties lacking in CBC-DES.

3 Implementation Overview

In this last section we briefly outline the structure of our implementation of a secure transport protocol based on a version of an existing, high-speed optimistic transport protocol similar to XTP [6, 4]. The implementation is in C and has been developed on an RS6000 workstation. All the features introduced in the previous sections (authentication, confidentiality, integrity, choice of the level of security) have been incorporated and tested.

An application which wants to use the transport protocol has to link with the transport machine object code (see Section 2.2). The code basically consists of an interface with the application and of two threads, one for transmission and one for reception of packets. The interface requests and responses are communicated to the threads through message queues.

To add security to the non-secure version of the protocol, four parts of the protocol have to be modified: the interface, the connection resources (contexts), the state machine and the format of the packets.

The application communicates with the RTP machine through the interface by using structures called *verbs* which contain data specific to particular actions of the protocol: OPEN, CONNECT, LISTEN, SEND, RECEIVE, DISCONNECT, CLOSE. Typically, OPEN allocates local resources, CONNECT allows the setting of the address to be called, SEND gives some buffers of data to

be sent on a specific connection, etc. These verbs can be chained together and passed in one call to the RTP machine, which will then process them. For example, OPEN and the chained verbs CONNECT-SEND allows to specify a recipient and the content of a message. The transport machine will then packetize the message and send it over the network to the specified recipient. Once the message has been delivered, the application is notified. The connection can then be closed and resources freed by issuing a CLOSE verb. Verbs, besides their chaining capability, have the advantage that they can easily be extended.

The interface to this protocol has been extended while remaining compatible with the previous non-secure version. Beyond simple compatibility advantages, this also greatly eases the work of "securing" existing applications built on top of this protocol. When security is provided, the CONNECT and LISTEN verbs have dedicated fields for security options, such as a long-lived key and bits to select the cryptographic function and whether integrity and/or confidentiality must be provided.

The protocol associates to each connection a resource called its *context*, which contains all the information necessary to provide the required transport services, such as states, pending data, timers, etc. Information relative to the security options and cryptographic keys is also stored in the context which, along with the RTP state machine, has also been expanded to include states relative to the authentication process.

A transport packet consists of a header followed by data, if any. The format of the packets has been designed to be extensible. Most transport control functions are present in optional fields called segments which are part of the transport header. A security segment has been added to include information needed for authentication and confidentiality. Following data, a trailer has been added that contains the packet signature.

A library of fast implementation of cryptographic functions has been used in order to implement the encryption algorithm and the signature scheme. Currently, MD5, SHA, DES, Double DES are the functions the upper layer can choose from.

To test the secure protocol, a secure file transfer application has been created from an existing non-secure version. The user only specifies once at the beginning of the transfer the type of security he wants to select for this transfer: integrity, confidentiality, etc. Then both the origin (client) and the destination (server) of the transfer have to agree on a long-lived key and a cryptographic function. The presence of an enemy has been simulated by performing different actions on transmitted packets, namely, bit flipping, packet delay, misordering or loss, and replay. As expected, the protocol ensured that under all possible (tested) attack scenarios, the presence of the enemy translated in

either complete interruption of transmission (as if the link was cut...) or eventual successful transfer of the file. The protocol was, therefore, successful at preventing the enemy from taking any active action during the transfer.

4 Conclusions

We have presented the design of a secure transport protocol with the requirements of compatibility, efficiency and security strength. A brief description of an existing implementation of secure transport protocol running over a high-speed network has also been given.

References

- [1] M. BELLARE AND P. ROGAWAY. Entity authentication and key distribution. *Advances in Cryptology – Crypto'93 Proceedings*.
- [2] O. GOLDBREICH, S. GOLDWASSER AND S. MICALI. How To Construct Random Functions. *Journal of the Association for Computing Machinery* **33**(4), 792-807 (October 1986).
- [3] R. MOLVA, G. TSUDIK, E. VAN HERREWEGHEN AND S. ZATTI. *Kryptoknight* authentication and key distribution system. ESORICS 92, Toulouse, France, November 1992.
- [4] R. M. SANDERS, A.C. WEAVER. The Xpress Transfer Protocol (XTP): A Tutorial. *Computer Communication Review (USA)* Vol. 20, No. 5, Oct. 1990, pp 67-80.
- [5] J. STEINER, C. NEUMAN, J. SCHILLER. Kerberos: An Authentication Service for Open Network Systems. *USENIX Winter Conference*, Dallas, Texas, February 1988.
- [6] A.C. WEAVER. The Xpress Transfer Protocol. *Proceedings International Workshop on Advanced Communications and Applications for High Speed Networks*, Munich, Germany 16-19 March 1992.

A Towards a formal definition of security

The introduction gave an intuitive indication of the security features we achieve. Informal security is, however, an approach often leading to incorrect and, therefore, insecure protocols. So it is important to be able to state precisely what is the problem being solved, and show that we do solve it. Accordingly, we are able to formally define the goal we achieve. This formal definition is

in the model of [1]. Based on it, we are also able to prove that our protocols are secure as long as standard cryptographic primitives (such as DES) obey some standard well defined properties (eg. behaving like a “pseudorandom function” [2]). This section sketches the model and definition. In the formal model [1] all communication between A and B is via the adversary E . That is, any message is actually sent to the adversary. She decides whether she wants to relay it, modify it, destroy it, make copies of it, etc. At any time she may send party A (resp. B) a message purporting to be from B (resp. A). Moreover, she may start up multiple *sessions* between A and B , and try cross session attacks.

We consider two “experiments.” The first imagines the adversary to be benign, **only** relaying messages like a good channel. The second considers an adversary misbehaving **arbitrarily**, but assumed to have neither the secret key a nor the power to break DES. Our definition says that a protocol is secure if, except with small probability, the protocol flows either “look the same” in the two experiments or the parties “detect” the adversary. More precisely, one of the following is true in the second experiment: (1) the parties reject the connection altogether (2) every flow sent (except perhaps the last) is faithfully relayed to the recipient, with relative ordering of flows maintained. Condition (2) simply states that the protocol is capable of recreating the appearance of a good channel despite the presence of the adversary. This statement can be formalized using the notion of “matching conversations” of [1]. (Of course, to preserve meaningfulness, we also add that when the adversary is benign, all flows are correctly delivered and the connection is not terminated; otherwise, our definition as given above could be satisfied by always having the parties reject the connection!)

36339 11 420 039 7

[illegible]

Meta 1010

ATTACHMENT 1A

001 999944343503176
 005 20230302121503.0
 008 950901s1994 cau b 000 0 eng d
 035 ##\$a(OCOLC)ocm33074839
 035 ##\$a(ABAU)994434-uabdb-Voyager
 040 ##\$aPMC \$cPMC \$dOCLCQ \$dABC
 049 ##\$aABCC
 090 ##\$aTK5105.59 \$b.S4435 1994x
 245 00\$aSecure transport protocols for high-speed networks /
 \$cErol Basturk ... [et al.].
 260 ##\$a[San Jose, Calif.] : \$bIBM Research Division, Almaden ;
 \$aYorktown Heights, NY : \$bIBM Thomas J. Watson Research Center,
 Publications Office [distributor, \$c1994]
 300 ##\$a21 p. ; \$c28 cm.
 490 1#\$aResearch report / IBM Research Division ; \$vRC 19981
 (84561)
 500 ##\$aCover title.
 500 ##\$a"3/8/94."
 500 ##\$a"January 31, 1994"--P. 1.
 500 ##\$aAdditional authors: M. Bellare, C.-S. Chow, and R.
 Guérin.
 504 ##\$aIncludes bibliographical references (p. 20).
 650 #0\$aComputer networks \$xSecurity measures \$xComputer
 programs.
 650 #0\$aComputer network protocols.
 700 1#\$aBasturk, Erol.
 830 #0\$aResearch report (IBM Research) ; \$vRC 19981.
 910 ##\$a@1998 mono c1 T
 994 ##\$aC0 \$bABC

ATTACHMENT 1B

[The Library of Congress](#)>> [Go to Library of Congress Online Catalog](#)

LIBRARY OF CONGRESS AUTHORITIES

[Help](#)[New Search](#)[Search History](#)[Headings List](#)[Start Over](#)< [Previous](#)[Next](#) >[MARC Display](#)[Labelled Display](#)**LC control no.:** sh 94001277**LCCN Permalink:** <https://lccn.loc.gov/sh94001277>**HEADING:** Computer networks Security measures

000 01070cz a2200277n 450

001 4857583

005 20120330081238.0

008 940217i| anannbabn |a ana

010 __ |a sh 94001277

035 __ |a (DLC)sh 94001277

035 __ |a (DLC)204268

040 __ |a DLC |c DLC |d DLC

053 _0 |a TK5105.59

150 __ |a Computer networks |x Security measures

360 __ |i subdivision |a Computer networks--Security measures |i under subjects

450 __ |a Computer network security

450 __ |a Network security, Computer

450 __ |a Security of computer networks

550 __ |w g |a Computer security

670 __ |a Work cat.: 94-1841: Lowe, S.J. Enterprisewide network security, c1994.

670 __ |a Engr. index: |b v. 89, pt. VI, p. 2276, under Computer network security (Computer networks--Security systems)

670 __ |a LC database, 2/3/94 |b (Computer network security; Computer and network security; Security mechanisms for computer networks)

675 __ |a ASTI; |a Web. 3

906 __ |t 9601 |u te05 |v 1

952 __ |a Made for existing bibliographic records

953 __ |a jf08 |b ta21

< [Previous](#)[Next](#) >**Save, Print or Email Records (View [Help](#))**Select Download Format: [Text \(Labelled Display\)](#)[Press to SAVE or PRINT](#)

Email Text (Labelled Display) to:

Press to SEND EMAIL

[Help](#) - [Search](#) - [Search History](#) - [Headings List](#) - [Start Over](#)



Library of Congress

URL: <https://www.loc.gov/>

Mailing Address:

101 Independence Ave,
S.E.
Washington, DC 20540

Library of Congress Authorities

URL: <http://authorities.loc.gov/>

Library of Congress Online Catalog

URL: <https://catalog.loc.gov/>

Questions, comments, error reports: [Contact Us](#)

ATTACHMENT 1C

[The Library of Congress](#)>> [Go to Library of Congress Online Catalog](#)

LIBRARY OF CONGRESS AUTHORITIES

[Help](#)[New Search](#)[Search History](#)[Headings List](#)[Start Over](#)< [Previous](#)[Next](#) >[MARC Display](#)[Labelled Display](#)

LC control no.: sh 85029524

LCCN Permalink: <https://lcn.loc.gov/sh85029524>

HEADING: Computer programs

000 00962cz a2200253n 450

001 4681797

005 20120323071049.0

008 860227|| anannbabn |a ana

010 __ |a sh 85029524

035 __ |a (DLC)sh 85029524

035 __ |a (DLC)28482

040 __ |a DLC |c DLC |d DLC

150 __ |a Computer programs

360 __ |i subdivision |a Computer programs |i under topical headings; and uniform titles of individual computer programs

450 __ |a Computer program files

450 __ |a Files, Computer program

450 __ |a Program files, Computer

450 __ |a Programs, Computer

550 __ |w g |a Computer files

550 __ |w g |a Computer software

680 __ |i Here are entered works limited to computer programs. General works on computer programs accompanied by documentation such as manuals, diagrams and operating instructions, etc. are entered under |a Computer software.

681 __ |i Note under |a Computer software

906 __ |t 9524 |u te03 |v 0

953 __ |a xx00 |b te03

< [Previous](#)[Next](#) >**Save, Print or Email Records (View [Help](#))**Select Download Format: [Press to SAVE or PRINT](#)

Email Text (Labelled Display) to:

[Press to SEND EMAIL](#)

Meta 1010

[Help](#) - [Search](#) - [Search History](#) - [Headings List](#) - [Start Over](#)

**Library of Congress**

URL: <https://www.loc.gov/>

Mailing Address:

101 Independence Ave,
S.E.
Washington, DC 20540

Library of Congress Authorities

URL: <http://authorities.loc.gov/>

Library of Congress Online Catalog

URL: <https://catalog.loc.gov/>

Questions, comments, error reports: [Contact Us](#)

ATTACHMENT 1D

[The Library of Congress](#)>> [Go to Library of Congress Online Catalog](#)

LIBRARY OF CONGRESS AUTHORITIES

[Help](#)[New Search](#)[Search History](#)[Headings List](#)[Start Over](#)< [Previous](#)[Next](#) >[MARC Display](#)[Labelled Display](#)

LC control no.: sh 85029512

LCCN Permalink: <https://lcn.loc.gov/sh85029512>

HEADING: Computer network protocols

000 00454cz a2200181n 450

001 4681786

005 20120323071047.0

008 860211i| anannbabn |b ana

010 __ |a sh 85029512

035 __ |a (DLC)sh 85029512

035 __ |a (DLC)28471

040 __ |a DLC |c DLC |d DLC

053 _0 |a TK5105.55

150 __ |a Computer network protocols

450 __ |a Protocols, Computer network

550 __ |w g |a Computer networks

906 __ |t 9723 |u te07 |v 0

953 __ |a xx00 |b jg12

< [Previous](#)[Next](#) >**Save, Print or Email Records (View [Help](#))**Select Download Format: [Text \(Labelled Display\)](#)[Press to SAVE or PRINT](#)

Email Text (Labelled Display) to:

[Press to SEND EMAIL](#)[Help](#) - [Search](#) - [Search History](#) - [Headings List](#) - [Start Over](#)**Library of Congress**URL: <https://www.loc.gov/>

Mailing Address:

101 Independence Ave,

S.E.

Washington, DC 20540

Library of Congress AuthoritiesURL: <http://authorities.loc.gov/>**Library of Congress Online Catalog**URL: <https://catalog.loc.gov/>Questions, comments, error reports: [Contact Us](#)**Meta 1010**

ATTACHMENT 1E

001 a4639201
003 SIRSI
005 20230408050003.0
008 950720|||||||xx ||||||||||||eng||
027 1 a| Research report RC 19981
035 a| (OCoLC-M)33074839
035 a| (OCoLC-I)275541436
110 20 a| Thomas J. Watson IBM Research Center n| RC 19981. =| ^A464814
245 10 a| Secure transport protocols for high-speed networks.
260 1 c| 1994.
596 a| 31
700 1 a| Basturk, E. ?| UNAUTHORIZED
700 1 a| Bellare, M. ?| UNAUTHORIZED
700 1 a| Chow, C.-S. ?| UNAUTHORIZED
700 1 a| Guerin, R. ?| UNAUTHORIZED
916 a| DATE CATALOGED b| 19950720
999 a| 130310 w| ALPHANUM c| 1 i| 36105046094145 d| 3/22/2023 e| 3/22/2023 k| CHECKEDOUT l| STACK
S m| SAL3 n| 2 r| M s| Y t| STKS-MONO u| 7/28/2001 z| TAX=8.25

ATTACHMENT 1F

001 991001791619704436
 005 19950901125255.0
 008 950901s1994 nyu tb 000 0 eng d
 035 ##\$a450351-o1cmu_inst
 035 ##\$a(OCOLC)450351 \$9ExL
 040 ##\$aPMC \$cPMC
 049 ##\$aPMCC
 088 ##\$aRC 19981 (84561)
 099 ##\$aIBMC 19981
 245 00\$aSecure transport protocols for high-speed networks /
 \$cErol Basturk ... [et al.].
 260 ##\$aYorktown Heights, N.Y. : \$bIBM T.J. Watson Research
 Center, \$c[1994].
 300 ##\$a21 p. ; \$c28 cm.
 490 1#\$aResearch report RC. International Business Machines
 Corporation. Research Division ; \$v19981
 500 ##\$a"January 31, 1994."
 504 ##\$aIncludes bibliographical references.
 520 ##\$aAbstract: "We argue that the increasingly widespread use
 of networks is leading to new security concerns such as secure
 delivery which are most naturally associated with the transport
 level and best addressed by the design of secure transport
 protocols. We present general methods for such a design which are
 directed at optimizing performance on a high speed network. Our
 work reflects the experience gained in designing and implementing a
 particular secure transport protocol."
 596 ##\$a9
 650 #0\$aComputer network protocols.
 700 1#\$aBasturk, Erol.
 810 2#\$aInternational Business Machines Corporation. \$bResearch
 Division. \$tResearch report ; \$vRC 19981.
 901 ##\$aocm33074839
 902 ##\$a450351
 903 ##\$ao33074839
 910 ##\$ajh/dw 8-22-95
 916 ##\$a19950901
 917 ##\$a19950901
 918 ##\$aJH8I
 919 ##\$a0
 920 ##\$a
 945 ##\$he&s-tech rept \$i38482007033885
 999 ##\$aIBMC 19981 \$wALPHANUM \$c1 \$i38482007033885 \$d9/1/1995
 \$lBY-REQUEST \$mOFFSITE \$rY \$sY \$tTECH-RPT \$u9/1/1995 FORM=MARC

ATTACHMENT 1G

<u>OCLC</u>		33074839		No holdings in XXX - 3 other holdings	
Books				Re 199 En 509 Re 2022082	
				Stat 01 tere 01 place 0194115	
<u>Type</u>	a	<u>ELvl</u>		<u>Src</u>	d
<u>BLvl</u>	m	<u>Form</u>		<u>Audn</u>	
		<u>Cont</u>	bt	<u>Ctrl</u>	
<u>Desc</u>	a	<u>GPub</u>		<u>Lang</u>	eng
		<u>LitF</u>	0	<u>MRec</u>	
		<u>DtSt</u>	s	<u>Indx</u>	0
		<u>Fest</u>	0	<u>Dates</u>	1994
				<u>Ctry</u>	nyu

ATTACHMENT 1H

Digital Signcryption or How to Achieve $\text{Cost}(\text{Signature \& Encryption}) << \\ \text{Cost}(\text{Signature}) + \text{Cost}(\text{Encryption})$ *

Yuliang Zheng

Monash University, McMahon's Road, Frankston, Melbourne, VIC 3199, Australia
Email: yuliang@mars.fcit.monash.edu.au

Abstract. Secure and authenticated message delivery/storage is one of the major aims of computer and communication security research. The current standard method to achieve this aim is “(digital) signature followed by encryption”. In this paper, we address a question on the cost of secure and authenticated message delivery/storage, namely, *whether it is possible to transport/store messages of varying length in a secure and authenticated way with an expense less than that required by “signature followed by encryption”*. This question seems to have never been addressed in the literature since the invention of public key cryptography. We then present a positive answer to the question. In particular, we discover a new cryptographic primitive termed as “signcryption” which *simultaneously* fulfills both the functions of digital signature and public key encryption in a logically single step, and with a cost *significantly* lower than that required by “signature followed by encryption”. For typical security parameters for high level security applications (size of public moduli = 1536 bits), signcryption costs 50% (31%, respectively) less in computation time and 85% (91%, respectively) less in message expansion than does “signature followed by encryption” based on the discrete logarithm problem (factorization problem, respectively).

Keywords

Authentication, Digital Signature, Encryption, Key Distribution, Secure Message Delivery/Storage, Public Key Cryptography, Security, Signcryption.

1 Introduction

To avoid forgery and ensure confidentiality of the contents of a letter, for centuries it has been a common practice for the originator of the letter to sign his/her name on it and then seal it in an envelope, before handing it over to a deliverer.

* Patent pending (PO3234/96, filed on October 25, 1996). The full version of this paper can be obtained from <http://www-pscit.fcit.monash.edu.au/~yuliang/>

Public key cryptography discovered nearly two decades ago [7] has revolutionized the way for people to conduct secure and authenticated communications. It is now possible for people who have never met before to communicate with one another in a secure and authenticated way over an open and insecure network such as Internet. In doing so the same two-step approach has been followed. Namely before a message is sent out, the sender of the message would sign it using a digital signature scheme, and then encrypt the message (and the signature) using a private key encryption algorithm under a randomly chosen message encryption key. The random message encryption key would then be encrypted using the recipient's public key. We call this two-step approach signature-then-encryption.

Signature generation and encryption consume machine cycles, and also introduce "expanded" bits to an original message. Hence the cost of a cryptographic operation on a message is typically measured in the message expansion rate and the computational time invested by both the sender and the recipient. With the current standard signature-then-encryption, the cost for delivering a message in a secure and authenticated way is essentially the sum of the cost for digital signature and that for encryption.

In this paper, we address a question on the cost of secure and authenticated message delivery, namely, *whether it is possible to transfer a message of arbitrary length in a secure and authenticated way with an expense less than that required by signature-then-encryption*. This question seems to have never been addressed in the literature since the invention of public key cryptography. We then present a positive answer to the question. In particular, we discover a new cryptographic primitive termed as "signcryption" which *simultaneously* fulfills both the functions of digital signature and public key encryption in a logically single step, and with a cost *significantly* smaller than that required by signature-then-encryption. The saving in cost grows proportionally to the size of security parameters. Hence it will be more significant in the future when larger parameters are required to compensate theoretical and technological advances in cryptanalysis.

2 The Traditional Signature-Then-Encryption Approach

As we mentioned earlier, public key cryptography invented by Diffie and Hellman [7] makes it a reality for one (1) to digitally sign a message, and (2) to send a message securely to another person with whom no common encryption key has been shared. Currently, the standard approach for a user, say Alice, to send a secure and authenticated message to another user Bob is signature-then-encryption. The best example that follows the two-step approach is PEM, a standard for secure e-mail on Internet [15].

To compare the efficiency of two different methods for secure and authenticated message delivery, we examine two types of "cost" involved: (1) computational cost, and (2) communication overhead (or storage overhead for stored messages). The *computational cost* indicates how much computational effort has to be invested both by the sender and the recipient of a message. We estimate

the computational cost by counting the number of dominant operations involved. Typically these operations include private key encryption and decryption, hashing, modulo addition, multiplication, division (inversion), and more importantly, exponentiation. In addition to computational cost, digital signature and encryption based on public key cryptography also require extra bits to be appended to a message. We call these extra “redundant” bits the *communication overhead* involved. We say that a message delivery method is superior to another if (the aggregated value of) the computational cost and communication overhead required by the former is less than that by the latter.

The first part of Table 2 indicates the computational cost and communication overhead of “Schnorr signature-then-ElGamal encryption” against that of “DSS-then-ElGamal encryption” and “RSA signature-then-RSA encryption”. Note that, although not shown in the table, other combinations such as “Schnorr signature-then-RSA encryption” and “RSA signature-then-ElGamal encryption” may also be used in practice. As discussed in [21], with the current state of the art, computing discrete logarithm on $GF(p)$ and factoring a composite n of the same size are equally difficult. This simplifies our comparison of the efficiency of a cryptographic scheme based on RSA against that based on discrete logarithm, as we can assume that the moduli n and p are of the same size.

We close this section by examining the increasingly disproportionate cost for secure and authenticated message delivery in the currently standard signature-then-encryption approach, with an example text of 10000 bits (which corresponds roughly to a 15-line email message). For current and low security level applications, when RSA is used, the computational cost is centered around the execution of four (4) exponentiations modulo 512-bit integers, and the communication overhead is 1024 bits. When Schnorr signature and ElGamal encryption are used, the computational cost consists mainly of six (6) exponentiations modulo 512-bit integers, and the communication overhead is about 750 bits.

However, if the contents of the text are highly sensitive, or a text of the same length will be transmitted in 2010, then very large moduli, say of 5120 bits, might have to be employed. In such a situation, if RSA is used, four (4) exponentiations modulo (very large!) 5120-bit integers have to be invested in computation ², and the communication overhead is 10240 bits, which is now longer than the original 10000-bit text! If, instead, Schnorr signature and ElGamal encryption is used, then the computational cost is six (6) exponentiations modulo (again very large!) 5120-bit integers, and the communication overhead of about 5560 bits is more than half of the length of the original message. From this example, one can see that in the signature-then-encryption approach, the cost, especially communication overhead, for secure and authenticated message delivery, is becoming disproportionately large for future, or current but high-level security, applications. This observation serves as further justification on the necessity of inventing a new and more economical method for secure and authenticated message delivery.

² The number of bit operations required by exponentiation modulo an integer is a cubic function of the size of the modulo.

3 Digital Signcryption — A More Economical Approach

Over the past two decades since public key cryptography was invented, signature-then-encryption has been a standard method for one to deliver a secure and authenticated message of arbitrary length, and no one seems to have ever questioned whether it is absolutely necessary for one to use the sum of the cost for signature and the cost for encryption to achieve both contents confidentiality and origin authenticity.

Having posed a question that is of fundamental importance both from a theoretical and a practical point of view, we now proceed to tackle it. We will show how the question can be answered positively by the use of a new cryptographic primitive called “signcryption” whose definition follows.

Intuitively, a digital *signcryption* scheme is a cryptographic method that fulfills both the functions of secure encryption and digital signature, but *with a cost smaller than that required by signature-then-encryption*. Using the (informal) terminology in cryptography, it consists of a pair of (polynomial time) algorithms (S, U) , where S is called the *signcryption algorithm*, while U the *unsigncryption algorithm*. S in general is probabilistic, but U is most likely to be deterministic. (S, U) satisfy the following conditions:

1. *Unique unsigncryptability* — Given a message m , the algorithm S *signcrypts* m and outputs a *signcryptured text* c . On input c , the algorithm U *unsigncrypts* c and recovers the original message un-ambiguously.
2. *Security* — (S, U) fulfill, simultaneously, the properties of a secure encryption scheme and those of a secure digital signature scheme. These properties mainly include: confidentiality of message contents, unforgeability, and non-repudiation.
3. *Efficiency* — The computational cost, which includes the computational time involved both in signcryption and unsigncryption, and the communication overhead or added redundant bits, of the scheme is *smaller* than that required by the best currently known signature-then-encryption scheme with comparable parameters.

A direct consequence of having to satisfy both the second and third requirements is that “signcryption $\neq$ signature-then-encryption”. These two requirements also justify our decision to introduce the new word *signcryption* which clearly indicates the ability for the new approach to achieve both the functions of digital signature and secure encryption in a logically single operation.

The rest of this section is devoted to seeking for concrete implementations of signcryption. We first identify two (types of) efficient ElGamal-based signature schemes. Then we show how to use a common property of these schemes to construct signcryption schemes.

3.1 Shortening ElGamal-Based Signatures

ElGamal digital signature scheme [9] involves two parameters public to all users: (1) p — a large prime, and (2) g — an integer in $[1, \dots, p-1]$ with order

$p - 1$ modulo p . User Alice's secret key is an integer x_a chosen randomly from $[1, \dots, p - 1]$ with $x_a \nmid (p - 1)$ (i.e., x_a does not divide $p - 1$), and her public key is $y_a = g^{x_a} \bmod p$.

Alice's signature on a message m is composed of two numbers r and s :

$$\begin{aligned} r &= g^x \bmod p \\ s &= (\text{hash}(m) - x_a \cdot r) / x \bmod (p - 1) \end{aligned}$$

where hash is a one-way hash function, and x is chosen independently at random from $[1, \dots, p - 1]$ with $x \nmid (p - 1)$ every time a message is to be signed by Alice. Given (m, r, s) , one can verify whether (r, s) is Alice's signature on m by checking whether $g^{\text{hash}(m)} = y_a^r \cdot r^s \bmod p$ is satisfied.

Since its publication in 1985, ElGamal signature has received extensive scrutiny by the research community. In addition, it has been generalized and adapted to numerous different forms (see for instance [23, 4, 18, 20] and especially [11] where an exhaustive survey of some 13000 ElGamal based signatures has been carried out.) Two notable variants of ElGamal signature are Schnorr signature [23] and DSS or Digital Signature Standard [18]. With DSS, g is an integer in $[1, \dots, p - 1]$ with order q modulo p , where q is a large prime factor of $p - 1$. Alice's signature on a message m is composed of two numbers r and s which are defined as

$$\begin{aligned} r &= (g^x \bmod p) \bmod q \\ s &= (\text{hash}(m) + x_a \cdot r) / x \bmod q \end{aligned}$$

where x is a random number chosen from $[1, \dots, q - 1]$. Given (m, r, s) , one accepts (r, s) as Alice's valid signature on m if $(g^{\text{hash}(m)/s} \cdot y_a^{r/s} \bmod p) \bmod q = r$ is satisfied.

For most ElGamal based schemes, the size of the signature (r, s) on a message is $2|p|$, $|q| + |p|$ or $2|q|$, where p is a large prime and q is a prime factor of $p - 1$. The size of an ElGamal based signature, however, can be reduced by using a modified "seventh generalization" method discussed in [11]. In particular, we can change the calculations of r and s as follows:

1. Calculation of r — Set $r = \text{hash}(k, m)$, where $k = g^x \bmod q$ ($k = g^x \bmod (p - 1)$ if the original r is calculated modulo $(p - 1)$), x is a random number from $[1, \dots, q]$ (or from $[1, \dots, p - 1]$ with $x \nmid (p - 1)$), and hash is a one-way hash function such as Secure Hash Standard or SHS [19].
2. Calculation of s — For an *efficient* ElGamal based signature scheme, the calculation of (the original) s from x_a , x , r and optionally, $\text{hash}(m)$ involves only simple arithmetic operations, including modulo addition, subtraction, multiplication and division. Here we assume that x_a is the secret key of Alice the message originator. Her matching public key is $y_a = g^{x_a} \bmod p$. We can modify the calculation of s in the following way:
 - (a) If $\text{hash}(m)$ is involved in the original s , we replace $\text{hash}(m)$ with a number 1, but leave r intact. The other way may also be used, namely we change r to 1 and then replace $\text{hash}(m)$ with r .

- (b) If s has the form of $s = (\dots)/x$, then changing it to $s = x/(\dots)$ does not add additional computational cost to signature generation, but may reduce the cost for signature verification.

To verify whether (r, s) is Alice's signature on m , we recover $k = g^x \bmod p$ from r, s, g, p and y_a and then check whether $\text{hash}(k, m)$ is identical to r .

To illustrate how to shorten ElGamal based signatures, now we consider DSS. It should be stressed that many other ElGamal based signature schemes, in particular those defined on a sub-group of order q (see for example [11, 20]), can be shortened in the same way and are all equally good candidates for signcryption. Table 1 shows two shortened versions of DSS, which are denoted by SDSS1 and SDSS2 respectively. Here are a few remarks on the table: (1) the first letter "S" in the name of a scheme stands for "shortened", (2) the parameters p, q and g are the same as those for DSS, (3) x is a random number from $[1, \dots, q]$, x_a is Alice's secret key and $y_a = g^{x_a} \bmod p$ is her matching public key, (4) $|t|$ denotes the size or length (in bits) of t , (5) the schemes have the same signature size of $|\text{hash}(\cdot)| + |q|$, (6) SDSS1 is slightly more efficient than SDSS2 in signature generation, as the latter involves an extra modulo multiplication.

Recently Pointcheval and Stern [22] have proven that Schnorr signature is unforgeable by any adaptive attacker who is allowed to query Alice's signature generation algorithm with messages of his choice [10], in a model where the one-way hash function used in the signature scheme is assumed to behave like a random function (the random oracle model). The core idea behind the unforgeability proof by Pointcheval and Stern is based on an observation that the signature has been converted from a 3-move zero-knowledge protocol (for proof of knowledge) with respect to a honest verifier. With such a signature scheme, unforgeability against a non-adaptive attacker who is not allowed to possess valid message-signature pairs follows from the soundness of the original protocol. Furthermore, as the protocol is zero-knowledge with respect to a honest verifier, the signature scheme converted from it can be efficiently simulated in the random oracle model. This implies that an adaptive attacker is not more powerful than a non-adaptive attacker in the random oracle model.

Turning our attention to SDSS1 and SDSS2, both can be viewed as being converted from a 3-move zero-knowledge protocol (for proof of knowledge) with respect to a honest verifier. Thus Pointcheval and Stern's technique is applicable also to SDSS1 and SDSS2. Summarizing the above discussions, both SDSS1 and SDSS2 are unforgeable by adaptive attackers, under the assumptions that discrete logarithm is hard and that the one-way hash function behaves like a random function.

3.2 Implementing Signcryption with Shortened Signature

An interesting characteristic of a shortened ElGamal based signature scheme obtained in the method described above is that although $g^x \bmod p$ is not explicitly contained in a signature (r, s) , it can be recovered from r, s and other public parameters. This motivates us to construct a signcryption from a shortened signature scheme.

Shortened schemes	Signature (r, s) on a message m	Recovery of $k = g^x \bmod p$	Length of signature
SDSS1	$r = \text{hash}(g^x \bmod p, m)$ $s = x/(r + x_a) \bmod q$	$k = (y_a \cdot g^r)^s \bmod p$	$ \text{hash}(\cdot) + q $
SDSS2	$r = \text{hash}(g^x \bmod p, m)$ $s = x/(1 + x_a \cdot r) \bmod q$	$k = (g \cdot y_a^r)^s \bmod p$	$ \text{hash}(\cdot) + q $

p : a large prime (public to all),
 q : a large prime factor of $p - 1$ (public to all),
 g : a (random) integer in $[1, \dots, p - 1]$ with order q modulo p (public to all),
 hash : a one-way hash function (public to all),
 x_a : Alice's secret key,
 y_a : Alice's public key ($y_a = g^{x_a} \bmod p$).

Table 1. Examples of Shortened and Efficient Signature Schemes

We exemplify our construction method using the two shortened signatures in Table 1. The same construction method is applicable to other shortened signature schemes based on ElGamal. As a side note, Schnorr's signature scheme, without being further shortened, can be used to construct a signcryption scheme which is slightly more advantageous in computation than other signcryption schemes from the view point of a message originator.

In describing our method, we will use E and D to denote the encryption and decryption algorithms of a private key cipher such as DES [17] and SPEED [25]. Encrypting a message m with a key k , typically in the cipher block chaining or CBC mode, is indicated by $E_k(m)$, while decrypting a ciphertext c with k is denoted by $D_k(c)$. In addition we use $KH_k(m)$ to denote hashing a message m with a key-ed hash algorithm KH under a key k . An important property of a key-ed hash function is that, just like a one-way hash function, it is computationally infeasible to find a pair of messages that are hashed to the same value (or collide with each other). This implies a weaker property that is sufficient for signcryption: given a message m_1 , it is computationally intractable to find another message m_2 that collides with m_1 . In [2] two methods for constructing a cryptographically strong key-ed hash algorithm from a one-way hash algorithm have been demonstrated. For most practical applications, it suffices to define $KH_k(m) = \text{hash}(k, m)$, where hash is a one-way hash algorithm.

Assume that Alice also has chosen a secret key x_a from $[1, \dots, q]$, and made public her matching public key $y_a = g^{x_a} \bmod p$. Similarly, Bob's secret key is x_b and his matching public key is $y_b = g^{x_b} \bmod p$.

The signcryption and unsigncryption algorithms constructed from a shortened signature are remarkably simple. For Alice to signcrypt a message m for Bob, she carries out the following:

Signcryption by Alice the Sender

1. Pick x randomly from $[1, \dots, q]$, and let $k = y_b^x \bmod p$. Split k into k_1 and k_2 of appropriate length. (Note: one-way hashing, or even simple folding, may be applied to k prior splitting, if k_1 or k_2 is too long to fit in E or KH , or one wishes k_1 and k_2 to be dependent on all bits in k .)
2. $r = KH_{k_2}(m)$.
3. $s = x/(r + x_a) \bmod q$ if SDSS1 is used, or
 $s = x/(1 + x_a \cdot r) \bmod q$ if SDSS2 is used instead.
4. $c = E_{k_1}(m)$.
5. Send to Bob the signcrypted text (c, r, s) .

The unsigncryption algorithm works by taking advantages of the property that $g^x \bmod p$ can be recovered from r, s, g, p and y_a by Bob. On receiving (c, r, s) from Alice, Bob unsigncrypts it as follows:

Unsigncryption by Bob the Recipient

1. Recover k from r, s, g, p, y_a and x_b :
 $k = (y_a \cdot g^r)^{s \cdot x_b} \bmod p$ if SDSS1 is used, or
 $k = (g \cdot y_a^r)^{s \cdot x_b} \bmod p$ if SDSS2 is used.
2. Split k into k_1 and k_2 .
3. $m = D_{k_1}(c)$.
4. accept m as a valid message originated from Alice only if $KH_{k_2}(m)$ is identical to r .

In the following, the two examples of signcryption schemes will be denoted by SCS1 and SCS2 respectively. For the purpose of a detailed comparison, the cost of these signcryption schemes has been analyzed and listed, along with other signature-then encryption schemes, in Table 2.

Finally two remarks follow: (1) signcryption schemes can also be derived from shortened signature schemes based on the discrete logarithm problem on elliptic curves [13]. (2) the functions, especially non-repudiation and unforgeability, of signcryption may not be fully implemented by the use of a shared key between Alice and Bob, such as $g^{z_a \cdot x_b} \bmod p$ or a key obtained via a Key Pre-distribution Scheme [16], unless tamper-resistant devices and/or trusted third parties are involved.

3.3 Working with Signature-Only and Encryption-Only Modes

Not all messages require both confidentiality and integrity. Some messages may need to be signed only, while others may need to be encrypted only. For the two digital signcryption schemes SCS1 and SCS2, when a message is sent in clear, they degenerate to signature schemes with verifiability by the recipient

only. As will be argued in Section 6, limiting verifiability to the recipient only still preserves non-repudiation, and may represent an advantage for some applications where the mere fact that a message is originated from Alice needs to be kept secret. Furthermore, if Alice uses g instead of Bob's public key y_b in the calculation of k , the schemes becomes corresponding shortened ElGamal based signature schemes with universal verifiability.

To work with the encryption-only mode, one may simply switch to the ElGamal encryption, or any other public key encryption scheme.

Various schemes	Computational cost	Communication overhead (in bits)
signature-then-encryption based on RSA	EXP=2, HASH=1, ENC=1 [EXP=2, HASH=1, DEC=1]	$ n_a + n_b $
signature-then-encryption based on DSS + ElGamal encryption	EXP=3, MUL=1, DIV=1 ADD=1, HASH=1, ENC=1 [EXP=3, MUL=1, DIV=2 ADD=0, HASH=1, DEC=1]	$2 q + p $
signature-then-encryption based on Schnorr signature + ElGamal encryption	EXP=3, MUL=1, DIV=0 ADD=1, HASH=1, ENC=1 [EXP=3, MUL=1, DIV=0 ADD=0, HASH=1, DEC=1]	$ KH(\cdot) + q + p $
signcryption SCS1	EXP=1, MUL=0, DIV=1 ADD=1, HASH=1, ENC=1 [EXP=2, MUL=2, DIV=0 ADD=0, HASH=1, DEC=1]	$ KH(\cdot) + q $
signcryption SCS2	EXP=1, MUL=1, DIV=1 ADD=1, HASH=1, ENC=1 [EXP=2, MUL=2, DIV=0 ADD=0, HASH=1, DEC=1]	$ KH(\cdot) + q $

where

EXP = the number of modulo exponentiations,
MUL = the number of modulo multiplications,
DIV = the number of modulo division (inversion),
ADD = the number of modulo addition or subtraction,
HASH = the number of one-way or key-ed hash operations,
ENC = the number of encryptions using a private key cipher,
DEC = the number of decryptions using a private key cipher,
Parameters in the brackets indicate the number of operations involved in "decryption-then-verification" or "unsigncryption".

Table 2. Cost of Signature-Then-Encryption v.s. Cost of Signcryption

4 Cost of Signcryption v.s. Cost of Signature-Then-Encryption

The most significant advantage of signcryption over signature-then-encryption lies in the dramatic reduction of computational cost and communication overhead which can be symbolized by the following inequality:

$$\text{Cost}(\text{signcryption}) < \text{Cost}(\text{signature}) + \text{Cost}(\text{encryption}).$$

With SCS1 and SCS2, this advantage is shown in Tables 3 and 4.

Note that when comparing with RSA based signature-then-encryption, we have assumed that a relatively small public exponent e is employed for encryption or signature verification, although cautions should be taken in light of recent progress in cryptanalysis against RSA with an small exponent (see for example [6]). Therefore the main computational cost for RSA based signature-then-encryption is in decryption or signature generation which generally involves a modulo exponentiation with a *full size* exponent d . We have further assumed that the Chinese Remainder Theorem is used, so that the computational expense for RSA decryption can be reduced, theoretically, to a quarter of the expense with a full size exponent.

security parameters $ p , q , KH(\cdot) (= hash(\cdot))$	saving in comp. cost	saving in comm. overhead
768, 152, 80	50%	76.8%
1024, 160, 80	50%	81.0%
2048, 192, 96	50%	87.7%
4096, 256, 128	50%	91.0%
8192, 320, 160	50%	94.0%
10240, 320, 160	50%	96.0%

$$\text{saving in comp. cost} = \frac{3 \text{ modulo exponentiations}}{6 \text{ modulo exponentiations}} = 50\%$$

$$\text{saving in comm. cost} = \frac{|hash(\cdot)| + |q| + |p| - (|KH(\cdot)| + |q|)}{|hash(\cdot)| + |q| + |p|}$$

Table 3. Saving of Signcryption over Signature-Then-Encryption Using Schnorr Signature and ElGamal Encryption

4.1 How the Parameters are Chosen

Advances in fast computers help an attacker in increasing his capability to break a cryptosystem. To compensate this, larger security parameters, including $|n_a|$, $|n_b|$, $|p|$, $|q|$ and $|KH(\cdot)|$ must be used in the future. From an analysis by Odlyzko [21] on the hardness of discrete logarithm, one can see that unless there is an algorithmic breakthrough in solving the factorization or discrete logarithm

security parameters $ p (= n_a = n_b), q , KH(\cdot) $	advantage in comp. cost	advantage in comm. overhead
768, 152, 80	0%	84.9%
1024, 160, 80	6.25%	88.3%
2048, 192, 96	43.8%	93.0%
4096, 256, 128	62.0%	95.0%
8192, 320, 160	77.0%	97.0%
10240, 320, 160	81.0%	98.0%

$$\text{advantage in comp. cost} = \frac{0.375(|n_a|+|n_b|)-4.5|q|}{0.375(|n_a|+|n_b|)}$$

$$\text{advantage in comm. cost} = \frac{|n_a|+|n_b|-(|KH(\cdot)|+|q|)}{|n_a|+|n_b|}$$

Table 4. Advantage of Signcryption over RSA based Signature-Then-Encryption with *Small Public Exponents*

problem, $|q|$ and $|KH(\cdot)|$ can be increased at a smaller pace than can $|n_a|$, $|n_b|$ and $|p|$. Thus, as shown in Tables 3 and 4, the saving or advantage in computational cost and communication overhead by signcryption will be more significant in the future when larger parameters must be used.

The selection of security parameters $|p|$, $|q|$, $|n_a|$ and $|n_b|$ in Tables 3 and 4, has been partially based on recommendations made in [21]. The parameter values in the tables, however, are indicative only, and can be determined flexibly in practice. We also note that choosing $|KH(\cdot)| \approx |q|/2$ is due to the fact that using Shank's baby-step-giant-step or Pollard's rho method, the complexity of computing discrete logarithms in a sub-group of order q is $O(\sqrt{q})$ (see [14]). Hence choosing $|KH(\cdot)| \approx |q|/2$ will minimize the communication overhead of the signcryption schemes SCS1 and SCS2. Alternatively, one may decide to choose $KH(\cdot) \in [1, \dots, q]$ which can be achieved by setting $|KH(\cdot)| = |q| - 1$. This will not affect the computational advantage of the signcryption schemes, but slightly increase their communication overhead.

5 Applications of Signcryption

As discussed in the introduction, a major motivation of this work is to search for a more economical method for secure and authenticated transactions/message delivery. If digital signcryptions are applied in this area, the resulting benefits are potentially significant: for every single secure and authenticated electronic transaction, we may save 50% in computational cost and 85% in communication overhead.

The proposed signcryption schemes are compact and particularly suitable for smart card based applications. We envisage that they will find innovative applications in many areas including digital cash payment systems, EDI and personal health cards. Of particular importance is the fact that signcryption

may be used to design more efficient digital cash transaction protocols that are often required to provide with both the functionality of digital signature and encryption.

In the full paper we also show how to adapt a signcryption scheme into one for broadcast communication which involves multiple recipients. Such an adapted scheme shares a comparable computational cost with a broadcast scheme proposed in RFC1421. The communication overhead required by the scheme based on signcryption, however, is multiple times lower than that required the scheme in RFC1421.

Another surprising property of the proposed signcryption schemes is that it enables us to carry out fast, secure, unforgeable and non-repudiable key transport *in a single block whose size is smaller than $|p|$* . In particular, using either of the two signcryption schemes, we can transport highly secure and authenticated keys in a single ATM cell (48 byte payload + 5 byte header). A possible combination of parameters is $|p| \geq 512$, $|q| = 160$, and $|KH(\cdot)| = 80$, which would allow the transport of an unforgeable and non-repudiable key of up to 144 bits. Advantages of such a key transport scheme over interactive key exchange protocols such as those proposed in [8] are obvious, both in terms of computational efficiency and compactness of messages. Compared with previous attempts for secure, but un-authenticated, key transport based on RSA (see for example [1, 12]), our key transport scheme has a further advantage in that it offers both unforgeability and non-repudiation. In a similar way, a multi-recipient signcryption scheme can be used as a very economical method for generating conference keys among a group of users.

6 Unforgeability, Non-repudiation and Confidentiality of Signcryption

Like any cryptosystem, security of signcryption in general has to address two aspects: (1) to protect what, and (2) against whom. With the first aspect, we wish to prevent the contents of a signcrypted message from being disclosed to a third party other than Alice, the sender, and Bob, the recipient. At the same time, we also wish to prevent Alice, the sender, from being masquerade by other parties, including Bob. With the second aspect, we consider the most powerful attackers one would be able to imagine in practice, namely adaptive attackers who are allowed to have access to Alice's signcryption algorithm and Bob's unsigncryption algorithm.

We say that a signcryption scheme is secure if the following conditions are satisfied:

1. Unforgeability — it is computationally infeasible for an adaptive attacker (who may be a dishonest Bob) to masquerade Alice in creating a signcrypted text.
2. Non-repudiation — it is computationally feasible for a third party to settle a dispute between Alice and Bob in an event where Alice denies the fact that she is the originator of a signcrypted text with Bob as its recipient.

3. Confidentiality — it is computationally infeasible for an adaptive attacker (who may be any party other than Alice and Bob) to gain any partial information on the contents of a signcrypted text.

A detailed description of the proofs/arguments of the security of the signcryption schemes SCS1 and SCS2 can be found in the full paper. Here are the key ideas used in the proofs/arguments:

1. Unforgeability — this can be done using the technique of Pointcheval and Stern [22].
2. Non-repudiation — A dispute between Alice and Bob can be settled by a trusted third party (say a judge), by the use of a zero-knowledge proof protocol between the judge and Bob. In particular, they can use a very simple 4-move zero-knowledge interactive proof protocol proposed by Chaum in [5].
3. Confidentiality — We achieve our goal by reduction: we will reduce the confidentiality of another encryption scheme called C_{kh} , whose confidentiality is relatively well-understood, to the confidentiality of a signcryption scheme (say SCS1). With the encryption scheme C_{kh} , the ciphertext of a message m is defined as $(u = g^x \bmod p, c = E_{k_1}(m), r = KH_{k_2}(m))$ where k_1 and k_2 are defined in the same way as in SCS1. C_{kh} is a slightly modified version of a scheme that has received special attention in [24, 3] (see also earlier work [26].)

Now assume that there is an attacker for SCS1. Call this attacker A_{SCS1} . We show how A_{SCS1} can be translated into one for C_{kh} , called $A_{C_{kh}}$. Note that for a message m , the input to A_{SCS1} includes $q, p, g, y_a = g^{x_a} \bmod p, y_b = g^{x_b} \bmod p, u = g^x \bmod p, c = E_{k_1}(m), r = KH_{k_2}(m)$. With the attacker $A_{C_{kh}}$ for C_{kh} , however, its input includes: $q, p, g, y_b = g^{x_b} \bmod p, u = g^x \bmod p, c = E_{k_1}(m)$, and $r = KH_{k_2}(m)$. One immediately identifies that two numbers that correspond to y_a and s which are needed by A_{SCS1} as part of its input are currently missing from the input to $A_{C_{kh}}$. Thus, in order for $A_{C_{kh}}$ to “call” the attacker A_{SCS1} “as a sub-routine”, $A_{C_{kh}}$ has to create two numbers corresponding to y_a and s in the input to A_{SCS1} . Call these two yet-to-be-created numbers y'_a and s' . y'_a and s' have to have the right form so that $A_{C_{kh}}$ can “fool” A_{SCS1} . It turns out that such y'_a and s' can be easily created by $A_{C_{kh}}$ as follows: (1) pick a random number s' from $[1, \dots, q]$. (2) let $y'_a = u^{1/s'} \cdot g^{-r} \bmod p$.

A final note on signcryption follows. Unlike signature-then-encryption, the verifiability of a signcryption is in normal situations limited to Bob the recipient, as his secret key is required for unsigncryption. At the first sight, the limited verifiability of a signcryption, namely the direct verifiability by the sender only (and indirect verifiability by a judge with the cooperation of Bob), may be seen as a drawback of signcryption. Here we argue that the limited direct verifiability will not pose any problem in practice and hence should not be an obstacle to practical applications of signcryption. In the real life, a message sent to Bob in a secure and authenticated way is meant to be readable by Bob only. Thus if there is no dispute between Alice and Bob, direct verifiability by Bob only is

precisely what the two users want. In other words, in normal situations where no disputes between Alice and Bob occur, the full power of universal verifiability provided by digital signature is never needed. (For a similar reason, traditionally one uses signature-then-encryption, rather than encryption-then-signature !) In a situation where repudiation does occur, interactions between Bob and a judge would follow. This is very similar to a dispute on repudiation in the real world, say between a complainant (Bob) and a defendant (Alice), where the process for a judge to resolve the dispute requires in general interactions between the judge and the complainant, and furthermore between the judge and an expert in hand-written signature identification, as the former may rely on advice from the latter in correctly deciding the origin of a message.

7 Conclusion

We have introduced a new cryptographic primitive called signcryption for secure and authenticated message delivery, which fulfills all the functions of digital signature and encryption, but with a far smaller cost than that required by the current standard signature-then-encryption methods. Security of the signcryption schemes has been proven, and extensions of the schemes to multiple recipients has been carried out. We believe that the new primitive will open up a number of avenues for future research into more efficient security solutions.

The signcryption schemes proposed in this paper have been based on ElGamal signature and encryption. We have not been successful in searching for a signcryption scheme employing RSA or other public key cryptosystems. Therefore it remains a challenging open problem to design signcryption schemes based factorization or other computationally hard problems.

References

1. Basturk, E., Bellare, M., Chow, C.-S., Guerin, R.: Secure transport protocols for high-speed networks. IBM Research Report Report RC 19981 IBM T. J. Watson Research Center Yorktown Heights, NY 10598 1994.
2. Bellare, M., Canetti, R., Krawczyk, H.: Keying hash functions for message authentication. In *Advances in Cryptology - CRYPTO'96* (Berlin, New York, Tokyo, 1996) vol. 1109 of *Lecture Notes in Computer Science* Springer-Verlag pp. 1–15.
3. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the First ACM Conference on Computer and Communications Security* (New York, November 1993) *The Association for Computing Machinery* pp. 62–73.
4. Brickell, E., McCurley, K.: Interactive identification and digital signatures. *AT&T Technical Journal* (1991) 73–86.
5. Chaum, D.: Zero-knowledge undeniable signatures. In *Advances in Cryptology - EUROCRYPT'90* (Berlin, New York, Tokyo, 1990) vol. 473 of *Lecture Notes in Computer Science* Springer-Verlag pp. 458–464.
6. Coppersmith, D., Franklin, M., Patarin, J., Reiter, M.: Low-exponent RSA with related messages. In *Advances in Cryptology - EUROCRYPT'96* (Berlin, 1996) vol. 1070 of *Lecture Notes in Computer Science* Springer-Verlag pp. 1–9.

7. Diffie, W., Hellman, M.: New directions in cryptography. *IEEE Transactions on Information Theory* **IT-22** (1976) 472–492.
8. Diffie, W., Oorschot, P. V., Wiener, M.: Authentication and authenticated key exchange. *Designs, Codes and Cryptography* **2** (1992) 107–125.
9. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory* **IT-31** (1985) 469–472.
10. Goldwasser, S., Micali, S., Rivest, R.: A digital signature scheme secure against adaptively chosen message attacks. *SIAM J. on Computing* **17** (1988) 281–308.
11. Horster, P., Michels, M., Petersen, H.: Meta-ElGamal signature schemes. In *Proceedings of the second ACM Conference on Computer and Communications Security* (New York, November 1994) ACM pp. 96–107.
12. Johnson, D., Matyas, S.: Asymmetric encryption: Evolution and enhancements. *CryptoBytes* **2** (1996) 1–6.
13. Koblitz, N.: Elliptic curve cryptosystems. *Mathematics of Computation* **48** (1987) 203–209.
14. Lenstra, A. K., Lenstra, H. W.: *Algorithms in Number Theory* vol. A of *Handbook in Theoretical Computer Science*. Elsevier and the MIT Press 1990.
15. Linn, J.: Privacy enhancement for internet electronic mail: Part I: Message encryption and authentication procedures. Request for Comments RFC 1421 IAB IRTF PSRG, IETF PEM WG 1993.
16. Matsumoto, T., Imai, H.: On the key predistribution systems: A practical solution to the key distribution problem. In *Advances in Cryptology - CRYPTO'87* (Berlin, New York, Tokyo, 1987) vol. 239 of *Lecture Notes in Computer Science* Springer-Verlag pp. 185–193.
17. National Bureau of Standards: Data encryption standard. FIPS PUB 46 U.S. Department of Commerce January 1977.
18. National Institute of Standards and Technology: Digital signature standard (DSS). FIPS PUB 186 U.S. Department of Commerce May 1994.
19. National Institute of Standards and Technology: Secure hash standard. FIPS PUB 180-1 U.S. Department of Commerce April 1995.
20. Nyberg, K., Rueppel, R.: Message recovery for signature schemes based on the discrete logarithm problem. *Designs, Codes and Cryptography* **7** (1996) 61–81.
21. Odlyzko, A.: The future of integer factorization. *CryptoBytes* **1** (1995) 5–12.
22. Pointcheval, D., Stern, J.: Security proofs for signature schemes. In *Advances in Cryptology - EUROCRYPT'96* (Berlin, New York, Tokyo, 1996) vol. 1070 of *Lecture Notes in Computer Science* Springer-Verlag pp. 387–398.
23. Schnorr, C. P.: Efficient identification and signatures for smart cards. In *Advances in Cryptology - CRYPTO'89* (Berlin, New York, Tokyo, 1990) vol. 435 of *Lecture Notes in Computer Science* Springer-Verlag pp. 239–251.
24. Zheng, Y.: Improved public key cryptosystems secure against chosen ciphertext attacks. Technical Report 94-1 University of Wollongong Australia January 1994.
25. Zheng, Y.: The SPEED cipher. In *Proceedings of Financial Cryptography'97* (Berlin, New York, Tokyo, 1997) *Lecture Notes in Computer Science* Springer-Verlag.
26. Zheng, Y., Seberry, J.: Immunizing public key cryptosystems against chosen ciphertext attacks. *IEEE Journal on Selected Areas in Communications* **11** (1993) 715–724.

ATTACHMENT 1I

Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

EROL BASTURK* MIHIR BELLARE† CHEE-SENG CHOW‡ ROCH GUÉRIN§

March 1994

Abstract

We argue that the increasingly widespread use of networks is leading to new security concerns such as *secure delivery* which are most naturally associated with the transport level and best addressed by the design of *secure transport protocols*. We present general methods for such a design which are directed at optimizing performance on a *high speed* network. Our work reflects the experience gained in designing and implementing a particular secure transport protocol.

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.

†Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.

‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.

§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

1 Introduction

As we entrust more and more of our communication to networks, the concern with security increases. This paper begins by arguing that the *nature* of the security guarantees which users will need and expect is changing. In particular, new requirements, like *secure delivery*, are emerging. In contrast to traditional security features which tend to be purely application level, the new ones are most naturally identified with the transport level. We suggest the design of *secure transport protocols* as the most effective way of filling all needs, and present a general method to transform a given transport protocol into a secure one. The design puts particular emphasis on maintaining the level of performance of the original transport protocol, particularly in a high speed environment. Our work reflects the experience gained in the design and implementation of a specific secure high-speed transport protocol.

1.1 Security requirements and their placement

Two parties, denoted A and B , communicate over a network. We will naturally view the parties as applications who use a common transport protocol. An adversary E monitors the parties' communications, and is even capable of injecting or removing messages from the lines. Nonetheless, the parties wish to be able to communicate "securely." Their advantage over E is to possess a random, shared secret key a (eg. a DES key) which E doesn't know.^{1,2}

Our discussion of security features which follows takes the perspective of a designer and architect of a secure communications medium. It reflects the need to add security functionality in a way which is consistent with, and best matches, the existing communication structure. To this end, we distinguish security features according to the layer of the communication structure to which they are most naturally associated. We found that the traditional features are mostly application level, while the new ones we deem necessary are transport level.

APPLICATION LEVEL SECURITY FEATURES: INTEGRITY AND CONFIDENTIALITY. *Integrity* and *confidentiality* are the two traditional, and important, security features. The first means that it isn't possible for E to modify the contents of transmitted data. The second means that E cannot figure out the content of the transmission but the receiver can recover it. Note they are requirements on the *data* transmitted by the application. This is the reason we view them as application level security features, a view which is reflected in the traditional method of providing these features, which we discuss next.

APPLICATION LEVEL SECURITY. Application level security features are easily (and usually) provided by *application level security*. Here the sender applies appropriate cryptographic functions to his data *before* passing it to the transport for conveyance. This is the approach of Kerberos [5] and KryptoKnight [3]. Integrity is usually guaranteed by *signing* the data before passing it to the

¹ How they come into possession of such a key is not our concern here. Rather, the problem is how to use the key to communicate securely.

² For simplicity we stick to this symmetric case. Our methods can be modified to work in the public key scenario as well.

transport level. Confidentiality is usually guaranteed by having A *encrypt* the data before passing it to the transport level, and having B *decrypt* the ciphertext which is received by his transport module and passed up to him.

TRANSPORT LEVEL SECURITY FEATURES: SECURE DELIVERY. Secure delivery, roughly speaking, is a guarantee to the sender A that his message was received by B and not intercepted and destroyed by the adversary. It is essentially an extension of the standard transport level *reliability* feature to the more adversarial setting we are discussing, which is why it seems most natural to view it as a transport level feature.

Note that the presence of the application level security features does not necessarily imply the security of delivery. The adversary can easily make a sending application believe that whatever it transmitted has been received by the receiving application, even if the data are signed or encrypted by the upper layer. How? Suppose A sends some data to B which E would prefer never reaches B (we will see later examples of why E might like to do this). E stops the data from reaching B (remember, all communication goes through her and she has the power to do this). Then, she sends a transport level acknowledgement of received data to the sending port. This acknowledgement is a transport level flow. Not being generated by an application, it is not signed. The transport protocol at the sending end will believe the acknowledgment, and tell the sender that its data has been received!³

Is the lack of secure delivery a serious security problem? Yes. Here are two examples that help see why. The first is the example that lead us to pinpoint the problem. It is the problem of securing control flows in a network. We have a number of (trusted) network *control points* linked by a spanning tree. At any time, one control point is the root of the tree. Suppose A wishes to pass its root position to B . It sends a (application level signed) messages saying so, and, assuming the message arrived, relinquishes the root position itself. Without secure delivery, we don't know B got the message, and now the tree has no root.

Suppose B is a broker, and A and (the adversary) E both want to buy a certain stock. E prevents A 's purchase requests from reaching B so that she can buy the stock herself.

Actually secure delivery is only one example of a transport level security feature that is desirable. In Appendix A we will discuss things more formally and point to a mathematical notion of security which we believe captures the actual requirement, and includes secure delivery, integrity (and, optionally, confidentiality) as special cases. Roughly, we will ask that either the flows between the parties maintain, in the presence of E , the "relative ordering" as well as content that they would have if E were not present, or the parties detect the presence of E .

TRANSPORT LEVEL SECURITY. In this design, the application passes its key a to the transport module, and leaves to the latter the task of applying any cryptographic functions or taking other security steps. The advantage is that the transport module can compute a signature which covers

³ An implicit assumption is that the application is not performing its own acknowledgments and retransmission, but, more naturally, relying on the transport for these features. Indeed, asking the application to duplicate these transport functions is usually poor design in that it belies the layered communication structure, and would also adversely affect performance.

not only the data but also (relevant parts of) the transport header which it creates, particularly the byte sequence numbers. It can also sign the acknowledgments messages which exist only at the transport level. As we will see, these possibilities are key to the provision of secure delivery.

1.2 The design of efficient and secure transport protocols

We specify a method to transform any transport protocol into a “secure” version, equipped not only with the new security features discussed above, but providing, at least as options, the standard application level security features. Below we discuss the elements of the solution followed by some of its features.

ELEMENTS OF THE SOLUTION. The design will be specified in full in the body of the paper, but here is a brief sketch. The secure transport protocol has two phases, the *initialization* phase and the *steady state*. In the former, an *entity authentication and key exchange* protocol is executed. This authenticates the parties and yields them a *session key* α . In the steady state, if the integrity option is selected, both data integrity and secure delivery are provided by attaching to each packet a signature, computed under key α , and taken over some portions of the header and the data payload. Note that acknowledgments, which have no data, are also signed. If confidentiality is desired, the data is encrypted, also under α . See the rest of the paper for more details on which parts of the header must be signed and which left in the clear; why the design guarantees secure delivery; and also for explanations on why a session key is needed when the parties already share the long lived key a .

COMPATIBILITY. Usually, applications are written on top of an existing transport protocol before any security is included in it. We want to assure *compatibility* of a secure version of this protocol with the regular non-secure version. The secure transport protocol then becomes a superset of the regular transport protocol. Applications using the regular transport protocol should not have to be modified at all.

PERFORMANCE. We take into account various *efficiency* requirements for the secure version of a transport protocol. Certain functions should be designed so that they can readily be off-loaded to hardware without impacting the original flow and processing of messages. Specifically, encryption and decryption may initially be performed in software, but, as speed increases, dedicated hardware components will almost certainly be required. For example, software encryption and decryption for secure video conferences may be feasible at low resolution. However, the provision of high resolution secure video conferences is likely to require hardware support. Our protocol should be able to operate in both environments. There are many other design aspects that need to reflect this requirement. For example, it may be worthwhile to factor into the design the eventual parallelization of certain processes, to define “intelligent” packet format for faster parsing, to allow rapid context retrieval based on simple connection-based information – all these things should be considered in order to provide greater efficiency.

In addition, the design should seek to minimize the performance degradation resulting from the provision of security. Obviously, performance degradations cannot be avoided altogether as

security typically involves additional flows and/or processing. The goal, though, is to limit such degradations by restricting the number of new flows needed to support security functions, and by remaining as true as possible to the design philosophy of the original transport protocol. For example, latency can be reduced if the same flows used to authenticate the two parties wishing to communicate, also serve as the vehicle for distributing the session key they will use. Similarly, further reduction can be achieved by including user data in the initial authentication flows, so that under the optimistic (but generally true) assumption that authentication will succeed, data transmission is not unnecessarily delayed. Whenever possible, security segments are “piggybacked” on, or combined with, existing flows.

PROOFS. We mentioned above that we have a mathematical definition of the security properties our protocol should satisfy. Correspondingly, we have proofs that if certain cryptographic functions, such as the DES, are suitably hard, then our design meets the definition.

IMPLEMENTATION. Section 3 briefly describes an implementation in which we added security features to an existing high-speed transport protocol. The implementation embodies the design principles outlined above as well as functions and techniques discussed in the rest of the paper.

2 Design of a secure transport protocol

An understanding of our design choices is facilitated by first explaining the performance issues which influence them. Following this explanation we specify the user interface of the secure transport protocol and a high level sketch of the design. Then we go deeper into the components.

2.1 Performance Issues

While previous sections motivated the need for security at the transport layer, they also mentioned a number of performance considerations that are of importance when designing an efficient secure transport protocol. Here we review these performance issues and describe how they influence the design. Details specific to individual components are provided in subsequent sections.

The provision of security is bound to somewhat degrade performance, but the goal is to keep this impact at a minimum. A first generic step towards minimizing the perceived performance impact of security is to provide a range of security “options” to users. Each option corresponds to a different trade-off between the level of security it affords and its cost in terms of performance. For example, users with different requirements may want to choose between encryption algorithms of different complexity and strength. It is, therefore, important to incorporate the flexibility of such choices when designing a secure transport protocol. Accordingly, our design provides a wide range of security options which are further detailed later.

There are, however, performance issues that are common to any security option, and their impact should also be minimized. Performance degradations caused by the provision of security have two major causes: additional flows and increased processing. Additional flows are typically required for authentication purposes during the initial phases of a connection. Increased processing is the result of the computational requirements of security functions such as signature generation

and verification, and encryption/decryption. We now review the design implications of both, and identify the components they impact most.

ADDITIONAL FLOWS. As mentioned above, security typically requires additional flows during the initial (setup) phase of a connection. This translates in an increased overhead and a greater latency before data transmissions can start. This can be particularly significant for short connections. There are, however, several rules that can/should be followed to limit this.

A first and obvious one is to restrict the number of additional flows needed, i.e., provide as many security functions as possible in each flow. For example (see below), key distribution can be carried out jointly with the first authentication flow rather than through a separate one. Another simple rule is to combine security flows, whenever possible, with existing protocol flows. For example, initial authentication flows can be piggybacked onto the connection establishment procedures (if authentication fails, the connection is aborted). This allows the parallelization of authentication and connection handshakes and limits, therefore, any increase in latency. Finally, a last step to minimize latency is to allow data transmission to start even before the authentication (or connection establishment, for that matter) phase has completed. This can be achieved by allowing the inclusion of user data in the initial authentication/connection flows (again, the data are discarded if the authentication fails).

To summarize, the three design rules that should be followed in order to limit the performance impact of security flows are as follows:

- (1) Minimize the number of additional flows;
- (2) Piggyback security flows on existing protocol flows;
- (3) Allow early data transmission (during initialization phase).

The design we describe below follows these design rules.

INCREASED PROCESSING. The other aspect of security that has the potential to degrade performance is the additional processing required by security functions. This is most significant for long connections as it applies to all steady state transmissions. There are, however, again some rules that can be followed to limit this impact.

The main one is that all computations should be performed in the most timely fashion possible. In other words, while an increase in the amount of computation is unavoidable, it is important to ensure that nothing slows down or delays this additional processing. In all instances we would like all computations to be carried out “on-the-fly” as data is being transmitted or received. This minimizes latency.

When applied to security functions such as signature generation and verification or encryption/decryption, the requirement of on-the-fly processing has several implications. For example, we would like decryption of a received packet to proceed independently of that of any other packet (note that this also allows parallelization) as packets may be received out of order.

Computation of cryptographic functions can be greatly speeded up by use of dedicated hardware. Our design does not require such hardware to be available, but adopts various design principles that would allow this hardware, if available, to be exploited in the best possible way. On-the-fly processing is important in this regard as it facilitates the eventual off-loading to the hardware.

Both signature computation and encryption/decryption rely on the use of secret information (key) shared by the two communicating parties. Retrieval of this information is, therefore, necessary for such processing. While one can assume its immediate availability when transmitting data, it must typically be retrieved upon receipt of a packet and this context retrieval step can introduce latency. It is, therefore, useful to design security functions, in particular signature computation, which allow processing to start immediately upon arrival of data, without waiting for the associated context retrieval to complete.

To summarize, our requirement for timely and on-the-fly security computations translates into three specific design rules:

- (1) Signature computation starts before the retrieval of connection context;
- (2) Packets are independently encrypted;
- (3) Hardware utilization is facilitated wherever possible.

2.2 The user interface

STARTUP INFORMATION. Each potential user (application) A of the secure transport protocol has a table T_A whose entries are pairs: $T_A = (A_1, a_1), \dots, (A_N, a_N)$ for some N . Each A_i is the identity of another user, and a_i is the key shared by A and A_i (but not known to any other user or the adversary). Henceforth this key will be referred to as the *long lived* key (LL-key).

CONNECTION INITIATOR INTERFACE. Now suppose A wishes to initiate a connection with B , with whom it shares LL-key a . It interfaces with a local piece of software to which it passes the identity B and the key a . It can also control the nature and strength of the security to be provided by specifying some options which will be discussed below. This software creates for her an entity we call her *secure transport machine* and denote by M_A . Once initialized, A can send (and receive) data via the secure transport machine just as it would via the original (insecure) version. That is, when it wants to send a message m , it passes it to the secure transport machine, and the latter is responsible for relaying the message, applying any necessary cryptographic functions to it, taking care of retransmission, and in general providing all transport facilities.

RESPONDER INTERFACE. At the receiving end, party B has also initialized a secure transport machine M_B . This machine has access to the table T_B of identities and associated keys. An incoming packet identifies the identity of the (claimed) sender, and the receiving machine then uses the table to get the associated key. With this key it can now verify signatures or perform any other necessary cryptography.

SUMMARY. In summary, we view A as having a secure machine M_A with which it interfaces. Similarly, B interfaces with its secure machine M_B . The cross network communication is performed by the two machines, who send each other packets across the network and are responsible for the secure transport mechanism.

OPTIONS. The options amongst which the initiator can select are the following.

- (1) *Authentication and session key exchange (AKE) protocol specification.* The application chooses one out of a set of four possible authentication and session key exchange (AKE)

protocols to be executed at the beginning of the interaction. The choices are described in Section 2.4.

- (2) *Integrity option.* If this option is selected then data integrity and secure delivery are provided. Otherwise they are not provided.
- (3) *Confidentiality option.* If this option is selected then data confidentiality is provided by encryption. Otherwise, the data will be in the clear.
- (4) *Basic cryptographic primitive specification.* The protocol lists a set of cryptographic primitives such as MD5 (Message Digest number 5), SHA (Secure Hash Algorithm), DES (Data Encryption Standard) and double DES, which it will use to provide both integrity and confidentiality. The application chooses which one to use.

As discussed in Section 2.1, the purpose of providing options is to allow the user to trade security for performance. We now see how this is reflected in the last three options listed above. The discussion on AKE selection is in Section 2.4.

An application which wants, say, only integrity, should not be unnecessarily burdened with the performance cost inherent in providing encryption. Similarly an application wanting only confidentiality should not be burdened with the cost of signing inherent in providing integrity. So integrity and confidentiality are better made (orthogonal) options.

Cryptographic primitives exhibit a trade-off between strength and speed: more secure primitives take more time to compute. An application which needs a high level of security must be willing to pay for it in performance, and can choose a primitive which is very strong but adds to the performance cost. An application which needs just a little security can specify a weaker but faster primitive and get better performance.

2.3 Overview of design

We divide the design into the following components:

- (1) *Initialization: Authentication and session key exchange.* When A initializes M_A (by passing it B 's identity and the shared key a) the machine initiates and executes an authentication and key exchange protocol with M_B . Specifically, the protocol used is the one chosen by the initiator in the options specified above. This protocol results in the distribution of a new (fresh) *session key* α while making sure that this key is authentic (ie. known only to M_A and M_B).
- (2) *Steady state:* Initialization completed, M_A is ready to receive data from the application A and send it to B ; similarly, M_B is ready to receive data from M_A and pass it to B .
 - (2.1) *Integrity via signing.* If the integrity option is selected then data is *signed* by M_A under the session key α (a signature is also called a MAC, or message authentication code). The signature covers not only the data payload but also the transport header (as explained later). On receiving a signed packet, M_B uses α to verify the signature.

- (2.2) *Confidentiality via encryption.* If the confidentiality option is selected then the data payload is encrypted by M_A under the session key α . On receiving a packet, M_B uses α to decrypt the payload and then passes the plaintext to B .

The following sections explain the components indicated above.

2.4 Authentication and session key exchange

As discussed above, the secure session begins with an authentication and key exchange protocol which yields to the parties a session key α to be used (to sign and encrypt) in the rest of the session. The first thing that needs to be explained is: Since the parties already share a key (namely the LL-key a) why get another one? The use of a session key has several motivations. First, it helps avoid cross session attacks in which data from one session are replayed in another. Second, it minimizes exposure of the long lived key. It is a standard technique in cryptographic practice.

Notice that only the transport machines M_A and M_B know about the session key. A and B never see it.

There are many AKE protocols reflecting, as usual, a trade-off between performance and security. Following our principle of allowing the application the option of choosing its level of trade-off we will specify several options of AKE protocols. To discuss them let's begin by looking at the issues.

There are three basic kinds of authentication. *Initiator* authentication leaves the responder convinced of the identity of the initiator, but not necessarily vice versa. *Responder* authentication leaves the initiator convinced of the identity of the responder, but not necessarily vice versa. *Mutual* authentication leaves each party convinced of the identity of the other.

AKE protocols typically use either *timestamps* or *nonces* to ensure “freshness” of a party's flows. (A nonce as used here is a random number). Nonce based methods require more flows (or “passes” as they are called in this area) than timestamp ones and thus adversely affect performance. On the other hand, timestamps require some degree of clock synchronization, with decreasing security as one allows a greater margin of error in this synchronization.

Potentially we thus have six options: three kinds of authentication, and either timestamps or nonces in each case. When one examines the basic flow structure in each case, however (cf. [1]) it is easy to eliminate two of them.⁴ This leaves the following options.

- (1) *Initiator authentication with time stamp, one pass.* Initiator authenticates himself to responder in a single flow. Useful for secure datagrams.
- (2) *Responder authentication with nonces, two pass.* Responder authenticates himself to initiator. Protocol has the following basic form: initiator issues a nonce serving as a challenge, and responder answers. Two flows.

⁴ An initiator nonce based protocol would need three flows within which we can do mutual nonce based anyway; similarly a responder time stamped protocol would need two flows within which we can do responder nonce based anyway.

- (3) *Mutual authentication with time stamps, two passes.* The above protocols are combined. The initiator authenticates himself with a timestamped flow while simultaneously issuing a challenge, and the responder answers.
- (4) *Mutual authentication with nonces, three passes.* Each party authenticates the other with nonces. Three flows.

Our protocols are inspired by the AKE protocols of [1] but have been modified to increase efficiency. We briefly review the performance considerations which motivated these modifications, and identify the resulting design guidelines.

A first step towards minimizing the overhead imposed by security on connection setup is to embed session key distribution in the *first* authentication flow. That is, the receipt of the first flow suffices to recover the session key. Moreover, use of the long-lived key is eliminated after the first flow and only the session key is used. If hardware is being used for signing then this minimizes the key switching time for the initiator, since he can switch to the session key as soon as the first flow is dispatched.

User data are included in the authentication flows to reduce latency. These user data are then retained by the receiver and delivered only after the successful completion of the authentication process. In case the authentication fails, all previously received data are discarded, and the upper layer is notified of the authentication failure. Piggybacking control (connection) information in the initial authentication flows can also help lower the overhead imposed by security on connection setup.

Error rates are low in high-speed networks and authentication should succeed most of the time. Transmitting user data during the authentication process can, therefore, reduce latency without impacting security. More generally, the protocol will allow transmission of user data not only in the authentication flows themselves, but also in any “initial transmission window” which may be allocated to the transmitter.⁵

Note that data packets in the authentication flows are signed using the *session* key which is another reason to switch as soon as possible to using it instead of the long-lived key.

The AKE protocols use signatures, and some of the choices in their design reflect performance issues arising from signature consideration. These issues are a part of the next section.

2.5 Integrity and signatures

Signatures are used in the AKE protocols and also, if the integrity option is selected, in the steady state. In the latter, their use will guarantee a broad set of properties including protection of the data against modification, secure delivery, and protection against replay attacks. Let’s begin by describing the mechanisms and see why they yield the above mentioned properties in the steady state. Then we will look at design choices which are motivated by performance issues and which apply to the use of signatures in both the AKE protocols and the steady state.

We denote by MAC_α a message authentication code under α . It has, roughly speaking, the

⁵ An initial transmission window may be allocated by the transport protocol to minimize connection setup latency.

following property. If an adversary sees a sequence $(m_1, \text{MAC}_\alpha(m_1)), \dots, (m_k, \text{MAC}_\alpha(m_k))$ of messages together with their MACs (or signatures), then it is infeasible for this adversary to produce a pair of the form $(m, \text{MAC}_\alpha(m))$ in which $m \notin \{m_1, \dots, m_k\}$.

In the steady state (integrity option assumed selected) the sender attaches to each packet p the value $\text{MAC}_\alpha(\bar{p})$ where $\bar{p}$ is the subset of p which includes the transport header, the full data payload, and the trailer of the packet p . We will see that of particular importance is the fact that the transport header includes the sequence number of the packet which is thereby covered by the MAC. We assume that all packets in each direction, even those which are purely transport level acknowledgements (ACKs), can be differentiated. A simple solution is to include in each packet a large enough (to avoid wrap-around) *signature* counter. We also assume that the transport header contains information which identifies the sender so that the identity of the sender is covered by the MAC as well. On receiving p, τ the receiver checks that $\tau = \text{MAC}_\alpha(\bar{p})$ and rejects the packet unless this is true.

The signature prevents the adversary from making the receiver accept packets which were not in fact produced by the sender. The signature by itself does not, however, prevent a *replay attack*. In this attack the adversary simply resends a packet which was previously sent by the sender, so that its signature is legitimate and will be accepted by the receiver.⁶ This attack fails because the signature also covers the (signature) sequence number of the packet, and the receiver does not accept packets out of order. Indeed, as part of the normal transport level checking, out of order packets will be discarded.

The manner in which security against replay is guaranteed illustrates well an advantage of security at the transport level. Sequencing is a standard and already present transport function. We simply exploit its presence. Had we wanted to prevent replay at the application level we would have had to implement sequencing with transport level counters and provide for our own checking and retransmission, thereby not only making implementation significantly harder but duplicating the transport functionality and degrading performance.

Secure delivery is guaranteed because the ACKs include sequence numbers and are signed. Note that the signature also provides error detection, so that no CRC or error detection code is required. Replaying of packets from one session into another is not possible because each session has a different session key.

We now turn to design issues motivated by performance. Let us recall some of the issues identified in Section 2.1. It is essential that the steady state overhead involved in computing and checking signatures and counters be kept to a minimum. Ideally, we want signatures to be computed and verified on-the-fly; i.e., MAC generation (verification) should be carried out as data transmissions (receptions) proceeds rather than before (after) these operations have completed. The goal is to avoid slowing down the regular flow of data, and allow the possible off-load of signature computations and verifications to dedicated hardware. The ability to achieve such on-the-fly processing depends on two major components. The first is the latency in retrieving the information needed

⁶ To see the importance of preventing such attacks, take the following example. The adversary collects one genuine ACK. Now, when the sender sends any flow, she can prevent secure delivery. She kills the sender's flow but replays to him the ACK she has from before. The sender accepts the ACK and believes his data has reached the receiver.

to perform the necessary computations. The second is the nature of the computations themselves. The first component is most relevant at the receiver, while the second is equally important at both the transmitter and the receiver.

The main source of latency when receiving a new packet is the time needed to recover the associated connection context. The context contains information such as the shared session key, the counter value of the last accepted packet, the type of cryptographic function used, etc., which are central to the verification of a packet integrity. Some delay is obviously unavoidable when retrieving this information, but it should be made as small as possible and its impact on the packet verification process should be kept to a minimum. A first step in achieving this is to allow context retrieval to be performed as quickly as possible by specifying early on in the packet all the required information. While rapid context retrieval certainly helps it does not eliminate all initial latency, and it is therefore still important to allow computations to start even before the full context has been retrieved. Finally, latency can also be kept small by ensuring that computations are of minimal complexity while meeting our security requirements.

These different requirements have been incorporated in our design, where the goal of minimal latency is reflected in the following two rules.

First, all data used to generate the signature is present in the packet. Let's illustrate with an example from the AKE protocols. In such challenge response protocols, it is common that one party (say B) proves his identity by signing a challenge R_A sent by A . In such a case, rather than returning $\langle R_A, \sigma \rangle$ with $\sigma = \text{MAC}_\alpha(R_A)$, party B could return just the short tag σ ; after all, A already knows R_A (it is in A 's context) so why waste bandwidth sending it? The reason for preferring to send the full $\langle R_A, \sigma \rangle$ is that signature verification can begin without waiting for the outcome of context retrieval. On the other hand, the cost of resending R_A is minimal since bandwidth is not that expensive at these speeds. In general, this translates into the following packet format: a signed packet will be of the form $\langle D, \sigma \rangle$ where σ is a signature of packet D under key α .

Note that we cannot prevent context retrieval of R_A in the above example since A must definitely check that what is received is the signature of the right challenge (namely the challenge A just sent). But putting the information in the flow decouples the signature checking from this context retrieval.

Second, MAC computations are kept simple and can start prior to context retrieval. In particular, we rely on MAC implementations of the form $\text{MAC}_\alpha(m) = f_\alpha(h(m))$, where h is a (hash) function depending neither on α nor on the cryptographic primitive chosen in the initial options. The use of such an implementation will enhance performance in our setting as MAC computation does not have to wait for α and the cryptographic function to be retrieved from the context; we can begin computing $h(m)$ straight away. By the time we need to compute f_α the key α and cryptographic function will have been retrieved. In addition, since h can be chosen to be a standard hash function and only f_{α} needs to involve more computationally intensive cryptographic functions, the overall cost of signature generation/verification can be kept low.

The authentication protocols and packet formats of our implementation guarantee minimal latency by following the above two rules.

2.6 Confidentiality via encryption

Confidentiality means user data should not be readable by the adversary. The secure transport protocol will encrypt user data, under the session key, and use the ciphertexts as the actual payload. As encryption is done prior to packetization, the signature (if present) of an outgoing packet is computed *after* data encryption and the signature of an incoming packet is computed *before* decryption. This complies with the requirement of a signature computed “on the fly”. If the signature checking at reception fails, it means the the packet is corrupted, and the packet is simply dropped: decryption is avoided.

Note that only user data are encrypted. One might, in principle, consider encrypting also certain parts of the transport headers. (We cannot, of course, encrypt the *entire* transport header: at a minimum the connection identifier must be in the clear to allow the receiver to know under which key it should decrypt!) Although encryption of parts of the transport headers might be argued to provide a higher degree of privacy, we believe the gain is marginal compared to the loss in performance. Encryption is a costly operation, and keeping it to a minimum is required. This also translates into a number of additional design rules.

In our design, we don’t want to reencrypt the data each time it must be retransmitted. Therefore, we make sure the ciphertexts (as opposed to the plaintexts) are available for retransmission. This is achieved by requiring that a ciphertext $E(x)$ of plaintext x is of the same length of x , and simply replacing the input plaintext buffer with the corresponding ciphertext.

Next, we also want to minimize the processing associated with decryption so that it can always proceed with minimum latency, even in cases or errors and/or packet losses. Minimizing the associated processing means, among other things, that we would like to decrypt each packet only once. However, the ability to ensure this strongly depends on the retransmission policy used by the transport protocol. In particular, while selective retransmission readily allows only one decryption per packet, this is not necessarily true with go-back- n . In order to ensure, that under a go-back- n retransmission scheme decryption is performed only once for each packet, we must either stop decrypting as soon as a gap is detected (as it triggers a retransmission from the sender), or continue decrypting subsequent received packets but keep track of the associated spans. The first alternative introduces significant additional latency in the decryption process, while the second essentially amounts to to implementing selective retransmission. Because of the inherent inefficiency of go-back- n during decryption, we recommend that selective retransmission be used when confidentiality is requested.

The requirement that decryption be able to proceed with minimum latency even in case of packet losses or errors, also introduces requirements on the encryption scheme itself. In general, an encryption scheme is said to have a *history of length i* if the ability to decrypt a ciphertext block is conditional on already being in possession of the decryptions of the i previous ciphertext blocks. Schemes with large history will not be acceptable, because the loss of a single block affects the ability to decrypt i blocks. This effectively prevents the decryption of several subsequent blocks, and translates into increased latency. The most commonly used encryption scheme, namely cipher block chaining, has a history of two; although this is low enough to be tolerable, we prefer to

avoid it. Instead, we have designed encryption schemes with history 0, so that the decryption of any packet can proceed independently of the reception of others. In addition, the scheme is such that both the encryption and the decryption procedures are parallelizable. This is in line with our design requirement to maintain the ability to use hardware support.

Another important design consideration in selecting an encryption/decryption scheme is its impact on error propagation. Lines usually have some degree of noise, so that a bit can be flipped now and then. Encryption, however, can effectively amplify the channel noise. Suppose a bit is flipped in $X = E(x)$, the encryption of x , and the receiver gets X' . In many encryption schemes, the decryption $D(X')$ differs from x in more than one bit, i.e., a single bit error has propagated to multiple bits. For example, in cipher block chaining it could differ in up to half the bits. This can translate in significant performance degradations for certain applications, whose data is either robust to limited errors (redundant information) or protected by some form of error correcting code. (Note that we assume here that data integrity is not selected as it would immediately result in the discarding of any packet in error, irrespective of the number of errors).

To avoid this problem, we use encryption schemes in which bit errors don't propagate. Specifically, our encryptions have the property that $d_H(E(x), E(y)) = d_H(x, y)$ for all x, y , where d_H is the Hamming distance. So error correcting on the plaintext is not affected. One might argue that the problem could have been solved in other ways. For example, put the ciphertext in error correcting form. This is bad for performance as well as inflexible. First, an application should have its choice of error correcting code and not have this dictated by the transport. Second, applications might be error correcting plaintext already, so that coding would be done twice.

To conclude, we stress that the extra features of our encryption schemes described above are obtained without any loss of security. Our encryption is DES based, and secure as long as DES behaves like a pseudorandom function. It even has security properties lacking in CBC-DES.

3 Implementation Overview

In this last section we briefly outline the structure of our implementation of a secure transport protocol based on a version of an existing, high-speed optimistic transport protocol similar to XTP [6, 4]. The implementation is in C and has been developed on an RS6000 workstation. All the features introduced in the previous sections (authentication, confidentiality, integrity, choice of the level of security) have been incorporated and tested.

An application which wants to use the transport protocol has to link with the transport machine object code (see Section 2.2). The code basically consists of an interface with the application and of two threads, one for transmission and one for reception of packets. The interface requests and responses are communicated to the threads through message queues.

To add security to the non-secure version of the protocol, four parts of the protocol have to be modified: the interface, the connection resources (contexts), the state machine and the format of the packets.

The application communicates with the RTP machine through the interface by using structures called *verbs* which contain data specific to particular actions of the protocol: OPEN, CONNECT,

LISTEN, SEND, RECEIVE, DISCONNECT, CLOSE. Typically, OPEN allocates local resources, CONNECT allows the setting of the address to be called, SEND gives some buffers of data to be sent on a specific connection, etc. These verbs can be chained together and passed in one call to the RTP machine, which will then process them. For example, OPEN and the chained verbs CONNECT-SEND allows to specify a recipient and the content of a message. The transport machine will then packetize the message and send it over the network to the specified recipient. Once the message has been delivered, the application is notified. The connection can then be closed and resources freed by issuing a CLOSE verb. Verbs, besides their chaining capability, have the advantage that they can easily be extended.

The interface to this protocol has been extended while remaining compatible with the previous non-secure version. Beyond simple compatibility advantages, this also greatly eases the work of “securing” existing applications built on top of this protocol. When security is provided, the CONNECT and LISTEN verbs have dedicated fields for security options, such as a long-lived key and bits to select the cryptographic function and whether integrity and/or confidentiality must be provided.

The protocol associates to each connection a resource called its *context*, which contains all the information necessary to provide the required transport services, such as states, pending data, timers, etc. Information relative to the security options and cryptographic keys is also stored in the context which, along with the RTP state machine, has also been expanded to include states relative to the authentication process.

A transport packet consists of a header followed by data, if any. The format of the packets has been designed to be extensible. Most transport control functions are present in optional fields called segments which are part of the transport header. A security segment has been added to include information needed for authentication and confidentiality. Following data, a trailer has been added that contains the packet signature.

A library of fast implementation of cryptographic functions has been used in order to implement the encryption algorithm and the signature scheme. Currently, MD5, SHA, DES, Double DES are the functions the upper layer can choose from.

To test the secure protocol, a secure file transfer application has been created from an existing non-secure version. The user only specifies once at the beginning of the transfer the type of security he wants to select for this transfer: integrity, confidentiality, etc. Then both the origin (client) and the destination (server) of the transfer have to agree on a long-lived key and a cryptographic function. The presence of an enemy has been simulated by performing different actions on transmitted packets, namely, bit flipping, packet delay, misordering or loss, and replay. As expected, the protocol ensured that under all possible (tested) attack scenarios, the presence of the enemy translated in either complete interruption of transmission (as if the link was cut...) or eventual successful transfer of the file. The protocol was, therefore, successful at preventing the enemy from taking any active action during the transfer.

4 Conclusions

We have presented the design of a secure transport protocol with the requirements of compatibility, efficiency and security strength. A brief description of an existing implementation of secure transport protocol running over a high-speed network has also been given.

Acknowledgments

Work done while the second author was at the IBM T.J. Watson Research Center, New York.

References

- [1] M. BELLARE AND P. ROGAWAY. Entity authentication and key distribution. *Advances in Cryptology – Crypto’93 Proceedings*.
- [2] O. GOLDREICH, S. GOLDWASSER AND S. MICALI. How To Construct Random Functions. *Journal of the Association for Computing Machinery* **33**(4), 792-807 (October 1986).
- [3] R. MOLVA, G. TSUDIK, E. VAN HERREWEGHEN AND S. ZATTI. *Kryptoknight* authentication and key distribution system. ESORICS 92, Toulouse, France, November 1992.
- [4] R. M. SANDERS, A.C. WEAVER. The Xpress Transfer Protocol (XTP): A Tutorial. *Computer Communication Review (USA)* Vol. 20, No. 5, Oct. 1990, pp 67-80.
- [5] J. STEINER, C. NEUMAN, J. SCHILLER. Kerberos: An Authentication Service for Open Network Systems. *USENIX Winter Conference*, Dallas, Texas, February 1988.
- [6] A.C. WEAVER. The Xpress Transfer Protocol. *Proceedings International Workshop on Advanced Communications and Applications for High Speed Networks*, Munich, Germany 16-19 March 1992.

A Towards a formal definition of security

The introduction gave an intuitive indication of the security features we achieve. Informal security is, however, an approach often leading to incorrect and, therefore, insecure protocols. So it is important to be able to state precisely what is the problem being solved, and show that we do solve it. Accordingly, we are able to formally define the goal we achieve. This formal definition is in the model of [1]. Based on it, we are also able to prove that our protocols are secure as long as standard cryptographic primitives (such as DES) obey some standard well defined properties (eg. behaving like a “pseudorandom function” [2]). This section sketches the model and definition.

In the formal model [1] all communication between A and B is via the adversary E . That is, any message is actually sent to the adversary. She decides whether she wants to relay it, modify it, destroy it, make copies of it, etc. At any time she may send party A (resp. B) a message purporting

to be from B (resp. A). Moreover, she may start up multiple *sessions* between A and B , and try cross session attacks.

We consider two “experiments.” The first imagines the adversary to be benign, only relaying messages like a good channel. The second considers an adversary misbehaving arbitrarily, but assumed to have neither the secret key a nor the power to break DES. Our definition says that a protocol is secure if, except with small probability, the protocol flows either “look the same” in the two experiments or the parties “detect” the adversary. More precisely, one of the following is true in the second experiment: (1) the parties reject the connection altogether (2) every flow sent (except perhaps the last) is faithfully relayed to the recipient, with relative ordering of flows maintained. Condition (2) simply states that the protocol is capable of recreating the appearance of a good channel despite the presence of the adversary. This statement can be formalized using the notion of “matching conversations” of [1]. (Of course, to preserve meaningfulness, we also add that when the adversary is benign, all flows are correctly delivered and the connection is not terminated; otherwise, our definition as given above could be satisfied by always having the parties reject the connection!)

APPENDIX 1

CURRICULUM VITAE SYLVIA D. HALL-ELLIS

EDUCATION

Ph.D., University of Pittsburgh, Pittsburgh, Pennsylvania, 1985
 M.P.S., University of Denver, Denver, Colorado, 2014
 Post Graduate Studies, University of Texas – San Antonio, Texas, 1975-1976
 M.L.S., University of North Texas, Denton, Texas, 1972
 B.A., Rockford University, Rockford, Illinois, 1971

PROFESSIONAL EXPERIENCE

- 1981- Consultant for higher education, non-profit organizations, and corporations.**
- 2002- Adjunct Professor, School of Information, San José State University, San José, California.** Serve as part-time faculty member teaching graduate students in technical services (cataloging, bibliographic control, classification), “core courses,” and special topics.
- 2014-2016 Director, Grants and Resource Development, Colorado Community College System.** Provided leadership and vision to foster the continued growth of rigorous scholarship, innovative projects, and creative work for statewide system, 13 campuses, and 50 teaching sites serving 155,000 students. Responsible for leadership and ensured efficient functioning of contract and grants in compliance with state & federal requirements and successful implementation and management. Served as a subject matter expert and liaison for college Grant Directors for all issues relating to grants and subcontracts.
- 2010-2014 Senior Grant Administrator, Morgridge College of Education, University of Denver (Colorado).** Provided leadership and vision to foster continued growth of rigorous scholarship, innovative research, and creative work in the Morgridge College of Education. Ensure that contract and grants processes function effectively and efficiently for 60 faculty and researchers with a focus on the successful progression and efficient management of grants totaling \$13M. Worked effectively and collegially with Department Chairs and Program Coordinators on operational grant-related management activities and with a broad range of internal and external constituencies. Supported the dissemination and promotion of faculty research and scholarship to outside constituents at conferences and through publications. Assisted Principal Investigators and grant project teams by coaching, mentoring, and financial management.
- 2011-2013 Interim Director & Assistant Dean, Westminster Law Library, Sturm College of Law, University of Denver.** Planned, organized, and directed all administrative activities for the library serving students, faculty, and alumni; oversaw the employment, retention, promotion, transfer and termination of library personnel; represented the library at professional conferences and public meetings; created and promoted a climate and culture of acceptance for new programs and services, a positive high-quality image of the law library, and that reflect the organization’s values, encourage excellent performance, and reward high productivity and innovation; provided leadership and set strategic direction of the organization; ensured that the library provided excellent customer service through solution-oriented staff response to patron needs and by responsiveness and continuous improvement of the organization; promoted, developed, and maintained positive working relationships with colleagues and customers including key stakeholders and groups, higher education institutions, the legal community, other regional libraries and districts statewide, and national library organizations.
- 2007-2014 Associate Professor, Library & Information Science, Morgridge College of Education, University of Denver (Colorado).** Served in leadership role and worked collaboratively in

program, college, campus and community environments. Advised and supervised students, taught core and specialized courses at the graduate level in an integrative, student-centered learning environment. Served on LIS, College, and University committees, and maintained working relationships with colleagues in other academic units and information professionals in the Rocky Mountain region and beyond. Served on and chair doctoral student dissertation committees. Oversaw and facilitated the College and LIS graduate student association.

- 2002-2007** **Assistant Professor, Library & Information Science, College of Education, University of Denver (Colorado).** Served as tenure-track faculty member teaching graduate students in “core courses,” resource description and access, service learning, and independent studies. Advised graduate students, participate on LIS and College committees, and serve on doctoral student dissertation committees. Oversaw and facilitated the LIS graduate student association and alumni association.
- 2000-2002** **Affiliate Faculty, Library & Information Science, College of Education, University of Denver (Colorado).** Served as part-time faculty member teaching graduate students in technical services (cataloging, bibliographic control, classification), “core courses,” and special topics. Oversaw and facilitated the LIS graduate student association and alumni association.
- 2000-2001** **Special Assistant to the Secretary’s Regional Representative, U.S. Department of Education, Region VIII, Denver, Colorado.** Served as the principal advisor and representative of the U. S. Secretary of Education’s Regional Representative (SRR). Ensured the implementation of major goals of the SRR and the Secretary. Provided leadership on behalf of the SRR in contacts with high-level officials in Region VIII requiring sensitive policy interpretation in communication with senior Department officials to solve problems and resolve issues raised by State and local education officials. Served as the primary contact for School-to-Work/Career, Children’s Health Insurance Program, and Safe and Drug-Free Schools. Delivered technical assistance to local education agencies and institutions of higher education in technology, professional development, and school construction.
- 1999-2000** **Catalog Librarian, Jefferson County Public Library, Lakewood, Colorado.** Performed original, copy cataloging and classification of library materials (English and Spanish) using standard library protocols; completed original descriptive cataloging and subject analysis; enhanced brief catalog and authority records in III.
- 1997-1999** **Development Officer, McREL International, Aurora, Colorado.** Served as senior member of corporate management team in strategic planning, development of proposals and contracts, implementation, and evaluation of new services, products, and programs for educational agencies. Provided creative leadership to corporate committees to solicit ideas, identify goals and objectives, plan, develop, present, and evaluate professional development opportunities.
- 1995-1997** **Education Specialist, Education Service Center, Region One, Edinburg, Texas.** Served as member of Administrative Cabinet team in strategic planning, development of proposals and contracts, implementation, and evaluation of telecommunications capabilities, services, products, and programs for 40 school districts serving 283,000 students in 7 counties. Provided creative leadership to regional and state committees to solicit ideas, identify strategic goals and objectives, plan, develop, present, and evaluate funding opportunities and professional development for 400 librarians.
- 1993-1996** **Assistant Professor of Library Science, Sam Houston State University, Huntsville, Texas.** Served a faculty member teaching 400 graduate students in technical services (cataloging,

bibliographic control, classification), automation, and networking. Participated in distance education program and coordinated annual conference. Conducted university and Texas Library Association-funded field research focused on library collection development and academic achievement.

- 1992-1993** **Head Librarian, Rocky Mountain College of Art & Design, Denver, Colorado.**
Responsible for the daily operation, selection and acquisition of materials, formulation of policies for library operations, media center, and photography/slides archives. Designed and implemented library automation and delivery of electronic resources to college community.
- 1981-1985** **Development Officer, PRLC, Inc., Pittsburgh, Pennsylvania.** Served as senior member of corporate management team in strategic planning, development of proposals and contracts, implementation, and evaluation of new services, products, and programs for 100 institutional member organizations. Coordinated the development of proposals and contracts totaling \$4,000,000 annually. Provided creative leadership to corporate committees to solicit ideas, identify goals and objectives, plan, develop, present, and evaluate professional development opportunities.
- 1981** **Director of Library Development, Pennsylvania Department of Education, Harrisburg, Pennsylvania.** Responsible for statewide development, technical assistance, professional development, resource sharing, children's services, institutional library services, networking, and state aid program for all libraries throughout the Commonwealth. Functioned as liaison to Governor's Advisory Council, LSCA Advisory Council, District Administrators, private colleges, universities, consortia managers, and network directors. Supervised \$14,000,000 formula-based state aid program and \$3,000,000 grant awards to individual libraries, consortia, and networks.
- 1978-1981** **Assistant Director, Southern Tier Library System, Corning, New York.** Coordinated operation of system-wide programs (technical assistance, professional development, resource sharing, technical services, outreach) to 40 public libraries in 5 counties serving 500,000 residents. Solicited ideas, identified goals, sponsored, and evaluated professional development opportunities and technical assistance sessions.
- 1976-1978** **Division Librarian for Technical Services, Corpus Christi Public Libraries, Corpus Christi, Texas.** Provided leadership in acquisitions, cataloging, serials control, and processing for main library and 4 branches serving 250,000 residents. Participated as senior member of library management team. Compiled and prepared technical evaluations, reports, and statistical analyses of Division operations to measure the achievement and cost of annual goals, objectives, and staff performance.
- 1975-1976** **System Coordinator, San Antonio Major Resource Center, San Antonio, Texas.** Served as senior member of the management team for District X Office, charged to provide technical assistance, resource sharing, media services, and professional development to librarians and staff representing 30 public library jurisdictions in 21 counties serving 1,500,000 residents. Functioned as liaison to System Director, staff, and members of governing bodies with the System Board of Directors and the Texas State Library and Historical Commission. Prepared LSCA grant applications and monitored awards totaling \$1,100,000 annually.
- 1973-1975** **Bilingual Branch Librarian, San Antonio Public Library, San Antonio, Texas.** Worked as librarian providing reference, information, and readers' advisory services in branch serving 50,000 Spanish-speaking residents in southwest San Antonio. Participated in collection development and resource acquisition activities, specializing in children's work, Spanish language resources, and multicultural studies.

1972-1973 **Librarian, Holding Institute, Laredo, Texas.** Worked as high school librarian serving 500 boarding students in Spanish-speaking environment of private school. Provided reference, research assistance, and library instruction to students and 35 faculty members.

1966-1971 **Rockford Public Library, Rockford, Illinois.** Worked in branches as part-time as a Library Assistant, Clerk, and Page in city library serving 150,000 residents.

PUBLICATIONS

Editor-reviewed Monographs (Completed and in Progress)

- Hall-Ellis, Sylvia D., and Mary Beth Weber. *Contemporary Cataloging in an RDA Environment: A Handbook for Students and Practitioners*. Chicago, IL: American Library Association. Under contract & In development.
- RDA Testing: Lessons Learned and Challenges Revealed*. Sylvia D. Hall-Ellis and Robert O. Ellett, Jr., eds. Binghamton, N.Y.: Haworth, 2012. 128 p.
- Hall-Ellis, Sylvia D., Stacey L. Bowers, Christopher D. Hudson, and M. Claire Williamson. *Librarian's Handbook for Seeking, Writing, and Managing Grants*. Santa Barbara, Calif.: Libraries Unlimited, 2011. 315 p.
- Hall-Ellis, Sylvia D., with Ann Jerabek, and Merrie W. Valliant. *Contemporary Cataloging: A Handbook for Practitioners and Students*. Open access text. Athens, GA: University of Georgia System Regents, 2011. 767 p.
- Grealy, Deborah S. and Sylvia D. Hall-Ellis. *From Research to Practice: The Scholarship of Teaching and Learning in LIS Education*. Westport, Conn.: Libraries Unlimited, 2009. 175 p.
- Hall-Ellis, Sylvia D. with J. Ann Jerabek. *Grants for School Libraries*. Westport, Conn.: Libraries Unlimited, 2003. 197 p.
- Hall-Ellis, Sylvia D., Doris Meyer, Frank W. Hoffmann, with J. Ann Jerabek. *Grant Writing for Small Libraries and School Library Media Centers*. Boulder, Colo.: NetLibrary, 2001. 173 p.
- Hall-Ellis, Sylvia D., Doris Meyer, Frank W. Hoffmann, with J. Ann Jerabek. *Grant Writing for Small Libraries and School Library Media Centers*. Englewood, Colo.: Libraries Unlimited, 2000. 173 p.

Editor-reviewed Chapters (Completed and In Progress)

- Hall-Ellis, Sylvia D. "Prepared to Lead: Talent, Skills, and Competencies." In *Telling the Technical Services Story*. Chicago, IL: American Library Association, 2020. Program Presentation for Re-Accreditation by the American Library Association, School of Information, San Jose State University, 2022.
- Hall-Ellis, Sylvia D. "Grant Writing and Sponsored Research Funding for Academic Librarians." In *The New Librarianship*. Vol. 4. Bradford Lee Eden, ed. New York: Scarecrow Press, 2015. (pp. 163-174)
- Hall-Ellis, Sylvia D. "Organizing Information: Technical Services." In *Information Services Today: An Introduction*. Sandra Hirsch, ed. Lanham, Md.: Rowman and Littlefield, 2015. (pp. 139-148)
- Hall-Ellis, Sylvia D. "Metadata, MARC, and More." In *Rethinking Technical Services, Considering Our Profession and Ourselves: What's the Future of Our Profession?* Mary Beth Weber, ed. Lanham, Md.: Rowman and Littlefield, 2015. (pp. 29-55)
- Hall-Ellis, Sylvia D., ed. "Contingent Faculty: Non-Tenure Track Faculty Series." In the *Faculty Personnel Guidelines Relating to Appointment, Promotion, and Tenure*. November 2011. Denver, Colo.: University of Denver, 2011. 42 p.
- Hall-Ellis, Sylvia D., ed. "Standard VII: Information Resources." In the *Sturm College of Law Self-Study Presentation for Accreditation by the American Bar Association*. Denver, Colo.: University of Denver, Sturm College of Law, 2011. 20 p.

Hall-Ellis, Sylvia D. "Applying for Grants from Foundations, Corporations, or Government." In *The Volunteers' Guide to Fundraising: Raise Money for Your School Team, Library or Community Group*. 1st ed. Ilona M. Bray, ed. Berkeley, Calif.: Nolo, 2011. (pp. 1-38 on accompanying disc)

Hall-Ellis, Sylvia D., ed. "Standard III: The Faculty." In the *Library and Information Science Program Self-Study Document for Accreditation by the American Library Association*. Denver, Colo.: University of Denver, Morgridge College of Education, 2010. 22 p.

Hall-Ellis, Sylvia D. "Library and Information Science Programs and Education for Catalogers and Metadata Specialists: Challenges for the Twenty-first Century." In *Conversations with Catalogers in the Twenty-First Century*. Elaine R. Sanchez, ed. Santa Barbara, Calif.: ABC-CLIO, 2010. (pp. 226-254)

Hall-Ellis, Sylvia D., ed. "Standard III: The Faculty." In the *Library and Information Science Program Self-Study Document for Accreditation by the American Library Association*. Denver, Colo.: University of Denver, College of Education, 2003. 15 p.

Lesesne, Teri S. and Sylvia D. Hall-Ellis. "The Selection, Evaluation, and Integration of Culturally Authentic Texts: A Case for Making the Online Catalog Reflect Parallel Cultures." In *Literacy: Traditional, Cultural, Technological*. Pittsburgh, Pa.: International Association of School Librarianship, 1995. (pp. 110-113)

Lesesne, Teri S. and Sylvia D. Hall-Ellis. *The Selection, Evaluation, and Integration of Culturally Authentic Texts: A Case for Making the Online Catalog Reflect Parallel Cultures*. In *Conference Proceedings of the 23rd Annual International Association of School Librarianship*, Pittsburgh, Pennsylvania, July 17-22, 1994. ERIC Document ED374816. 17 p.

Hall-Ellis, Sylvia D. "Curriculum Folio for School Library Media Specialist Programs." In the *National Council for Accreditation of Teacher Education Self-Study for Sam Houston State University*. Huntsville, Tex.: Sam Houston State University, College of Education and Applied Science, 1994. 25 p.

Bruntjen, Scott and Sylvia D. Hall. "Attempting to Automate: Lessons Learned Over Five Years." In *Advances in Library Administration*. Volume 4. Weston, Conn.: JAI Press, 1985. (pp. 177-192)

Peer-Reviewed Journal Articles (Completed and In Progress)

Hall-Ellis-Sylvia D. "Job Design for Cataloging and Metadata Librarians." Submitted to *Journal of Library Administration*. In progress.

Hall-Ellis, Sylvia D. "The Relationship of Situational Leadership and the Dreyfus Model of Skill Acquisition for Supervisors in Cataloging and Metadata Services." To be submitted to *Library Resources and Technical Services*. In progress.

Hall-Ellis, Sylvia D. *The Relationship of Core Competencies on Learning Outcomes and Employers' Expectations for Catalog Librarians and Metadata Specialists*. To be submitted to the *Journal of Education for Library and Information Science*. In progress.

Hall-Ellis, Sylvia D. "Building Cataloger Competencies: The Dreyfus Model as a Prototype for the Education and Professional Development of Catalog Librarians and Metadata Specialists in Bibliographic Control." To be submitted to the *Cataloging & Classification Quarterly*. In progress.

Hall-Ellis, Sylvia D. "Descriptive Impressions of Entry-Level Cataloger and Metadata Specialists Positions, 2000-2016: Reflections and Trends." To be submitted to *Library Resources and Technical Services*. In progress.

- Hall-Ellis, Sylvia D. "Competencies for Metadata and Cataloging Leaders: What Employers Expect as Reflected in Position Descriptions, 2000-2016." *Cataloging & Classification Quarterly*. In progress.
- Hall-Ellis, Sylvia D. "Stackable Micro-credentials – A Framework for the Future." *The Bottom Line* 29, no. 4 (April 2016), <http://www.emeraldinsight.com/doi/pdfplus/10.1108/BL-02-2016-0006>
- Ellis, Sylvia D. "Succession Planning and Staff Development – A Winning Combination." *The Bottom Line*, 28 no. 3 (May 2015): 95-98.
- Hall-Ellis, Sylvia D. "Succession Planning and Staff Development – A Winning Combination." *The Informed Librarian Online* (September 2015), http://www.informedlibrarian.com/featuredArticle.cfm?FILE=succession_1509.pdf
- Hall-Ellis, Sylvia D. "Nudges and Decision Making: A Winning Combination." *The Bottom Line* 28, no. 4 (July 2015): 133-136.
- Hall-Ellis, Sylvia D. "Succession Planning and Staff Development – A Winning Combination." *The Bottom Line* 28, no. 3 (May 2015): 95-98.
- Hall-Ellis, Sylvia D. "Metadata Competencies for Entry-Level Positions: What Employers Expect as Reflected in Position Descriptions, 2000-2013." *Journal of Library Metadata* 15, no. 2 (June 2015): 102-134.
- Hall-Ellis, Sylvia D. "Onboarding to Improve Library Retention and Productivity." *The Bottom Line* 27, no. 4 (October 2014).
- Hall-Ellis, Sylvia D. "Accept, Coach, and Inspire: A Formula for Success." *The Bottom Line* 27, no. 3 (July 2014): 103-106.
- Hall-Ellis, Sylvia D. *Reward Systems for Staff in Higher Education Institutions: Case Studies of 15 Higher Education Institutions in Colorado*. Capstone Thesis. Denver, Colo.: University of Denver, University College, 2014.
- Hall-Ellis, Sylvia D. "Reward Systems Promote High-Performance Work Teams Achieving Library Mission." *The Bottom Line* 27, no. 2 (April 2014): 66-69.
- Hall-Ellis, Sylvia D. "Investment in Staff Development for Seeking External Grant Funds." *The Bottom Line* 27, no. 1 (January 2014): 22-25.
- Hall-Ellis, Sylvia D. "Staff Investments for High Performance Teams." *The Bottom Line* 26, no. 4 (October 2013): 149-152.
- Hall-Ellis, Sylvia D. and Deborah S. Greal. "Service Learning in LIS Education: A Case for Holistic Assessment." *Catholic Library World* 82, no. 3 (March 2012): 178-187.
- Hall-Ellis, Sylvia D., and Deborah S. Greal. "The Dreyfus Model of Skill Acquisition: A Career Development Framework for Succession Planning and Management in Academic Libraries." *College and Research Libraries* (June 2012). <http://crl.acrl.org/content/early/2012/06/19/crl12-349.full.pdf+html>
- Hall-Ellis, Sylvia D. "Cataloger Competencies...What Do Employers Require?" *Cataloging & Classification Quarterly* 46, no. 3 (2008): 305-330. <http://ccq.haworthpress.com/doi:10.1080/01639370802034565>

Hall-Ellis, Sylvia D. "Subject Access for Readers' Advisory Services: Their Impact on Contemporary Spanish Fiction in Selected Public Library Collections." *Public Library Quarterly* 27, no.1 (2007): 1-18.

<http://plq.haworthpress.com/doi:10.1080/01616840802122377>

Hall-Ellis, Sylvia D. "Language Proficiencies among Catalogers and Technical Services Librarians." *Technical Services Quarterly* 25, no. 2 (2007) 31-47. http://tsq.haworthpress.com/doi:10.1300/J124v25n02_03

Hall-Ellis, Sylvia D. "Cataloging Electronic Resources & Metadata: Employers' Expectations as Reflected in *American Libraries* and *AutoCAT*, 2000-2005." *Journal of Education for Library and Information Science* 47, no. 1 (2006): 38-51.

Hall-Ellis, Sylvia D. "Descriptive Impressions of Managerial & Supervisory Cataloger Positions as Reflected in *American Libraries*, *AutoCAT*, and the *Colorado State Library Jobline*, 2000-2004: A Content Analysis of Education, Competencies, and Experience." *Cataloging & Classification Quarterly* 42, no. 1 (2006): 55-88.

Hall-Ellis, Sylvia D. "Descriptive Cataloging Proficiencies among Beginning Students: A Comparison among Traditional and Virtual Class Students." *Journal of Library & Information Services in Distance Education* 2, no. 2 (2005): 13-44.

Hall-Ellis, Sylvia D. "Descriptive Impressions of Entry-Level Cataloger Positions as Reflected in *American Libraries*, *AutoCAT*, and the *Colorado State Library Jobline*, 2000-2003." *Cataloging & Classification Quarterly* 40, no. 2 (2005): 33-72.

Hall-Ellis, Sylvia D. and Mary Ann Berry. "The Impact of Library Resource Centers on Academic Achievement in Selected Public Schools in South Texas: Preliminary Findings." *Texas Library Journal* 71, no. 2 (Summer 1995): 94-97.

Hall-Ellis, Sylvia D. "Visual Arts as Foundation for Successful Library Automation: The Rocky Mountain College of Art & Design Experience." *Art Reference Serials Quarterly* 4 (1994): 43-54.

Hall, Sylvia D. *High School Databases: An Examination of Bibliographic Data Elements*. Dissertation. Pittsburgh, Pa.: University of Pittsburgh, School of Library and Information Science, 1985.

Technical Reports

Hall-Ellis, Sylvia D. *Preparing Catalogers and Metadata Specialists Through Competency-Based Education: The San José State University iSchool Experience*. Report for the 2021 Re-Accreditation Program Presentation to the American Library Association. San José, Calif.: San José State University iSchool, 2020.

Hall-Ellis, Sylvia D. *Colorado Community College System Grant Handbook*. Denver, Colo.: Colorado Community College System, 2015.

Faculty Voices: Testimonials from the Frontiers of a Development Education Redesign. Elaine DeLott Baker, Marilyn Smith, and Sylvia D. Hall-Ellis, eds. Denver, Colo.: Colorado Community College System, 2014.

Lewis, Melanie, Jamie M. Van Leeuwen, and Sylvia D. Hall-Ellis. *Project Homeless Connect 7 Event Evaluation*. Denver, Colo.: University of Colorado Denver, 2009.

Hall-Ellis, Sylvia D. *Grant Writing Tips and Resources*. Denver, Colo.: University of Denver, 2008-2014. <http://portfolio.du.edu/grants>

- Hall-Ellis, Sylvia D. and Duan Zhang. *Project Homeless Connect 6 Event Evaluation*. Denver, Colo.: Center for Community Engagement and Service Learning, 2008.
- Hall-Ellis, Sylvia D. *Strategic Plan for Denver Medical Library System: Final Report*. Denver, Colo.: HealthONE and Denver Medical Library, 2008.
- Hall-Ellis, Sylvia D. and Duan Zhang. *Project Homeless Connect 5 Event Evaluation*. Denver, Colo.: Center for Community Engagement and Service Learning, 2008.
- Hall-Ellis, Sylvia D. *Strategic Plan for Denver Medical Library System: Phase Two Report*. Denver, Colo.: HealthONE and Denver Medical Library, 2007.
- Hall-Ellis, Sylvia D. and Duan Zhang. *Project Homeless Connect 4 Event Evaluation*. Denver, Colo.: Center for Community Engagement and Service Learning, 2007.
- Hall-Ellis, Sylvia D. *Strategic Plan for Denver Medical Library System: Phase One Report*. Denver, Colo.: HealthONE and Denver Medical Library, 2007.
- Hall-Ellis, Sylvia D. *Denver Public Library: Opportunities for Change*. Denver, Colo.: University of Denver, Colorado Community-Based Research Network & Metropolitan Organization of People, 2005.
- Hall-Ellis, Sylvia D. *Resources in Grant Writing for Colorado Schools and Libraries*. Sponsored by the Colorado Department of Education, Educational Telecommunications Unit, 1999. Revised September 2000.
- Hall-Ellis, Sylvia D. *Lewis & Clark Fellows Concept Paper for the Bicentennial Commemoration*. Vancouver, Wash.: Lewis and Clark Bicentennial Council, 1998.
- Hall-Ellis, Sylvia D. and Mary Ann Berry. *The Impact of Library Resource Centers on Academic Achievement in Public Schools in Texas: The Final Report*. Prepared under the sponsorship of the Research Enhancement Fund award from Sam Houston State University, the Texas Association of School Librarians, the Children's Services Round Table, and the Young Adults' Services Round Table. Huntsville, Tex.: Sam Houston State University, College of Education and Applied Science, 1997.
- Hall-Ellis, Sylvia D. *The Impact of Library Resource Centers on Academic Achievement in Selected Public Schools in Texas*. Huntsville, Tex.: Sam Houston State University, College of Education and Applied Science, 1997.
- Hall-Ellis, Sylvia D. *Planning for Educational Technology: the Distance Education Implementation Phase: An Investigation of Technology and Telecommunication Needs for Region One Education Service Center, South Texas Community College, TCI Cablevision of South Texas, Inc., Tech Prep of the Rio Grande Valley, Inc., Texas State Technical College, Centro Cultural en el Valle de Texas, McAllen Independent School District, Harlingen Consolidated Independent School District, Donna Independent School District, Edinburg Consolidated Independent School District, La Joya Independent School District, Mercedes Independent School District, Pharr-San Juan-Alamo Independent School District, Sharyland Independent School District, Easter Seal Society of the Rio Grande Valley, Inc., and McAllen Memorial Library*. Harlingen, Tex.: Tech Prep of the Rio Grande Valley, 1996.
- Hall-Ellis, Sylvia D. "Barcodes for the Texas Library Connection." Prepared under the sponsorship of the Office of Technology Services, Texas Education Agency. Austin, Tex.: TENET News and Conferences, March 1995.
- Hall-Ellis, Sylvia D. [et. al.] *Planning for Educational Technology: A Study of Future Technology Needs for the Donna Independent School District, Region One Education Region Service Center, Tech Prep of the Rio Grande Valley, Inc. South Texas Community College, and the Department of Library Science, Sam Houston State*

University. Research team: Sylvia D. Hall-Ellis, Ruth Ann Riggins, Noe Torres, Patricia G. Bubbs, and Michael D. Bell. Harlingen, Tex.: Tech Prep of the Rio Grande Valley, 1994. Funded through a grant award from the Texas Education Agency.

Hall-Ellis, Sylvia D. and Mary Ann Berry. *The Impact of Library Resource Centers on Academic Achievement in Selected Public Schools in South Texas*. Huntsville, Tex.: Sam Houston State University, College of Education and Applied Science, 1993. Funded through a grant award from the Sam Houston State University Research Enhancement Fund.

Hall-Ellis, Sylvia D., Alice Krueger, and Linda Brannan. *Thesaurus Development for National Curriculum Materials Database at the Eisenhower National Clearinghouse for Mathematics and Science Education, Columbus, Ohio*. Developed under the sponsorship of Mid-Continent Regional Educational Laboratory Corporate Library, Aurora, Colo. Washington, D.C.: National Science Foundation; Columbus, Ohio: ERIC Clearinghouse for Mathematics and Science Education, 1993.

Hall-Ellis, Sylvia D. and Clarence L. Coffindaffer. *Partners in Progress: The 1992 Montana Library Federation Study Final Report*. Helena, Mont: Montana State Library and The Blue Bear Group, Inc., 1992.

Hall-Ellis, Sylvia D. and Clarence L. Coffindaffer. *Montana Federation Study Identification Paper*. Denver, Colo.: The Blue Bear Group, Inc., 1992.

Bruntjen, Scott and Sylvia D. Hall. *Recommendations on the Development of System-Wide Efforts of the Northern Waters Library Service*. Ashland, Wisc.: Northern Waters Library Service and The Blue Bear Group, Inc., 1989.

Hall, Sylvia D. *The Iowa Union List of Serials as A Part of The Iowa Locator: Planning Document*. Des Moines, Ia.: State Library of Iowa, 1988.

Hall, Sylvia D. *Iowa Computer-Assisted Network (ICAN Users' Manual. IBM Compatible Edition: Version 7.0*. Des Moines, Ia.: State Library of Iowa, 1988.

Hall, Sylvia D. *Iowa Computer-Assisted Network (ICAN Users' Manual. IBM Compatible Edition: Version 5.0*. Des Moines, Ia.: State Library of Iowa, 1986.

Hall, Sylvia D. *Iowa Computer-Assisted Network (ICAN Users' Manual. Apple MacIntosh Edition: Version 5.0*. Des Moines, Ia.: State Library of Iowa, 1986.

Bruntjen, Scott and Sylvia D. Hall. *The District of Columbia Public Library Planning for Retrospective Conversion of Bibliographic Records and Automation Issues for the 1990's: Final Report*. Central City, Colo.: The Blue Bear Group, Inc., 1986.

Bruntjen, Scott and Sylvia D. Hall. *The Iowa Locator: Final Report*. Central City, Colo.: The Blue Bear Group, Inc., 1986.

Bruntjen, Scott and Sylvia D. Hall. *Discovering Resource Sharing Treasures: Accessing Pennsylvania's High School Library Collections*. Harrisburg, Pa.: State Library of Pennsylvania, Bureau of School Library Media Resources, 1985.

Hall, Sylvia D. *Retrospective Conversion and the Completeness of Cataloging in Pennsylvania High School Libraries*. Pittsburgh, Pa.: PRLC, Inc., 1985.

Bruntjen, Scott and Sylvia D. Hall. *The Iowa Locator*. Des Moines, Ia.: State Library of Iowa, 1985-
<http://www.statelibraryofiowa.org/ld/silo/locator>

Bruntjen, Scott and Sylvia D. Hall. *ICAN Analysis*. Des Moines, Ia.: State Library of Iowa, 1985.

Bruntjen, Scott and Sylvia D. Hall. *Zebras: Bar Codes, Standards, and Library Automation*. Central City, Colo.: The Blue Bear Group, Inc., 1985.

Hall, Sylvia D. and Scott Bruntjen. *Access Pennsylvania*. Harrisburg, Pa.: State Library of Pennsylvania, 1984-
<http://www.accesspa.org>

Hall, Sylvia D. *Reconfiguration of the ITAC Cataloging Data Base to Machine Readable (MARC) Format*. Classified Document. Arlington, Va.: U. S. Army Intelligence and Threat Analysis Center, 1984.

Bruntjen, Scott and Sylvia D. Hall. *South Dakota Library Automation Plan: Final Report*. Pittsburgh, Pa.: PRLC, Inc., 1982. Reprinted by the South Dakota State Library, 1983.

Bruntjen, Scott and Sylvia D. Hall. *Altoona Automation Plan: Final Report prepared for the Altoona Area Public Library and the Altoona District Library Center*. Pittsburgh, Pa.: PRLC, 1983.

Bruntjen, Scott, Sylvia D. Hall and Paul J. Pugliese. *College Space Utilization Study*. Pittsburgh, Pa.: PRLC, Inc., 1983.

Hall, Sylvia D. *Pennsylvania Public Library Film Center Union Catalog Cataloging and Technical Services Procedures Manual*. Pittsburgh, Pa.: PRLC, Inc., 1982.

Hall, Sylvia D. *History of Library Development in Pennsylvania: A Review and Content Analysis of the Plans, 1955-1980*. Pittsburgh, Pa.: PRLC, Inc., 1982.

Hall, Sylvia D. *Newspapers on Microfilm: A Listing of Newspapers in Allegheny, Chemung, Schuylers, Steuben, and Yates Counties*. Ithaca, N.Y.: South Central Reference and Research Council, 1981.

Hall, Sylvia D. *OCLC/ILL Subsystem at Southern Tier Library System*. Albany, N.Y.: SUNY/OCLC Network, 1980.

Hall, Sylvia D. *Retrospective Conversion for Major Public Libraries in South Central New York State: A Technical Report*. 2 vols. Corning, N.Y.: Southern Tier Library System, 1979-1980.

Hall, Sylvia D. *The Librarian and the Mexican-American Patron in Texas*. Austin, Tex.: Texas State Library, 1978.

Other Publications

Hall-Ellis, Sylvia D., ed. *Library and Information Science Program Self-Study Document for Accreditation by the American Library Association*. St. Paul, MN: St. Catherine University, 2017. 255 p.

Hall-Ellis, Sylvia D., and Robert O. Ellett, Jr., guest editors. *RDA Testing: Lessons Learned and Challenges Revealed: A Special Issue of Cataloging & Classification Quarterly* 49, no. 7-8 (November 2011).

Hall-Ellis, Sylvia D. and Robert O. Ellett, Jr. *Fundamentals of Cataloging I: An Online ALCTS Course*. Chicago, Ill.: American Library Association, 2009.

Hall-Ellis, Sylvia D., Angela J. Kinney and Martha Ann Bace, editors. *Best Practices in Cataloging Education Identified at the 2007 ALCTS Pre-conference: A Special Issue of the Journal for Library and Information Science Education* 49, no. 2 (Spring 2008).

Hall-Ellis, Sylvia D. *Cataloging Education: A New Emphasis for the Library and Information Science Curriculum*. Presentation delivered to the ALCTS Pre-conference, 132nd Annual Conference, American Library Association, Washington, D.C., June 22, 2007. <http://www.loc.gov/aba/professional/>

Hall-Ellis, Sylvia D. "Cataloger Competencies: Do the Employers Require What the Professors Teach?" Presentation delivered to the ALCTS CCS Heads of Cataloging Discussion Group, 131st Annual Conference, American Library Association, New Orleans, Louisiana, June 26, 2006. <http://dlist.sir.arizona.edu/>

Hall-Ellis, Sylvia D., guest editor, with Deborah S. Grealy, Clara L. Sitter, and Tassos Petrou. *Library Students' Voices in Colorado: An Issue of Colorado Libraries* 31:1 (Spring 2005).

Hall-Ellis, Sylvia D., ed. *Library and Information Science Program Self-Study Document for Accreditation by the American Library Association*. Denver, Colo.: University of Denver, College of Education, 2003. 125 p. with CD-ROM.

Hall-Ellis, Sylvia D. and Deborah S. Grealy, guest editors. *Library Education in Colorado: An Issue of Colorado Libraries* 29, no. 2 (Summer 2003).

Hall-Ellis, Sylvia D., ed. *Library and Information Science Program Self-Study Document for Accreditation by the American Library Association*. Denver, Colo.: University of Denver, College of Education, 2003.

Hall-Ellis, Sylvia D. "Adaptive Furniture for the ADA-Qualified: An Investigative Study." 2001. Unpublished manuscript.

Hall-Ellis, Sylvia D. "Cataloging Electronic Serials: A Study in User Access and Article Delivery." 2001. Unpublished manuscript.

Hall-Ellis, Sylvia D. "E-books: Acquisition and Circulation Issues in Public Libraries." 2001. Unpublished manuscript.

Hall-Ellis, Sylvia D. "Authority Control and Its Importance in School Library Media Online Catalogs." 1999. Unpublished manuscript.

Hall, Sylvia D. "Cooperation Improving Service in San Antonio System." *Texas Libraries* XXXVII (Spring 1976): 27-29.

Hall, Sylvia D. "Summer is Sea Monstrously Fun!" *Texas Library Journal* L (December 1974): 224-226.

Hall, Sylvia D. "A Brief Annotated Bibliography of Non-book Materials on the Mexican American." *Texas Library Journal* XLVIII (October 1972): 213-232.

Book Reviews

ALA Book of Library Grant Money. Ann Kepler, ed. 8th ed. Chicago, IL: American Library Association, 2011. 978-0-8389-1058-0, \$175.00 [*Colorado Libraries*, June 2012]

Developing a Compensation Plan for Your Library. Paula M. Singer and Laura L. Francisco, comps. 2nd ed. Chicago, IL: American Library Association, 2009. 978-0-8389-0985-0, \$57.00 [*Colorado Libraries*, March 2012]

Frugal Librarian. Carol Smallwood, ed. Chicago, IL: American Library Association, 2011. 978-0-83891-075-7, \$42.00 [*Colorado Libraries*, February 2012]

Dowlin, Ken. *Getting the Money: How to Succeed in Fundraising for Public and Nonprofit Libraries*. Westport, Conn.: Libraries Unlimited, 2008. 978-1-59158-597-X, \$50.00 [*Colorado Libraries*, February 2009]

Lundahl, Mats. *Bebo de Cuba; Bebo Valdés y Su Mundo*, by Mats Lundahl. Traducción de Linda Oakeshott Dragó. Barcelona: RBA Libros, 2008. 978-849-86-7259-6, \$33.99 [*Críticas*, November 2008]

- Bonelli, Florencia. *Marlene*, by Florencia Bonelli. Buenos Aires: Aguilar, Altea, Taurus, Alfaguara, 2008. 978-987-04-0995-3, \$24.95 [*Críticas*, October 2008]
- Keret, Etgar. Traducción de Ana María Bejarano. *Pizzería Kamikaze y Otras Relatos*. México, D.F.: Editorial Sexto Piso, 2008. 968-5679-29-0, no price given [*Críticas*, September 2008]
- Littauer, Marita, and Florence Littauer. *Enriquece tu Comunicación*. Miami, Fla.: Editorial Unilit, 2008. 978-0-7899-1521-4, \$11.99 [*Críticas*, August 2008]
- Martínez, Guillermo. *La Muerte Lenta de Luciana B.* New York: Rayo Planeta, 2008. 978-0-06-156551-9, \$14.95 [*Críticas*, May 2008]
- Matthews, Joseph R. *The Evaluation and Measurement of Library Services*. Westport, Conn.: Libraries Unlimited, 2007. 978-1-59158-532-9, \$50.00 [*Colorado Libraries*, April 2008]
- Gómez-Jurado, Juan. *A Masacre de Virginia Tech: Anatomía de una Mente Torturada*. Barcelona: Ediciones El Andén, 2007. 978-84-935789-4-7, €16.50 [*Críticas*, February, 2008]
- Matthews, Joseph R. *Library Assessment in Higher Education*. Westport, Conn.: Libraries Unlimited, 2007. 978-1-59158-531-2, \$45.00 [*Colorado Libraries*, February 2008]
- Chacón, Inma. *La Princesa India: Cuando el Viento Azul*. México: Alfaguara, 2006. 970-770398-9, \$19.95 [*Críticas*, June 2006]
- Vargas Llosa, Mario. *Israel/Palestina: Paz o Guerra Santa*. fotogs. by Morgana Vargas Llosa. Spain/U.S.: Aguilar: Santillana, 2006. 84-03-09691-7, paper, \$19.95 [*Críticas*, May 2006]
- Findlay, Diane. *Digging into Dewey*. Fort Atkinson, Wisc.: Upstart Books, 2005. 978-1-932146-18-9, \$16.95 [*Colorado Libraries*, May 2006]
- Pequeñas Resistencias 4: Antología del Nuevo Cuento Norteamericano y Caribeño*. Menéndez, Ronaldo, Ignacio Padilla & Enrique del Risco, eds. Madrid: Páginas de Espuma, 2005. 84-95642-59-X, paper, \$36.95 [*Críticas*, April 2006]
- Rueda, André. *Vengo a Salvar a España: Biografía de Un Franco Desconocido*. Madrid: Nowtilus (Investigación Abierta), 2005. photogs., bibliog. 84-9763-202-8, paper, \$23.95 [*Críticas*, March 2006]
- Becerra, Ángela. *El Penúltimo Sueño*. 1st ed. Barcelona: Planeta, 2005. 84-08-05795-2, \$25.95. [*Críticas*, January 2006]
- Aguilar Camín, Héctor. *La Conspiración de la Fortuna*. 1st ed. México: Planeta, 2005. 970-37-0368-2, \$19.95 [*Críticas*, October 2005]
- México en Sus Libros*. Enrique Florescano with Pablo Mijangos, editors & compilers. 1st ed. México, D.F.: Taurus Aguilar, 2004. 968-19-0783-3, \$16.95 [*Críticas*, September 2005]
- Historia Económica de México*. Coordinator, Enrique Semo. México: Universidad Nacional Autónoma de México, Editorial Oceano de México, 2004. 13 vols. 970-32-0805+3 (obra completa), \$9.25 each [*Críticas*, August 2005]

- Czarnowsky, Christyne A. and Michael H. Williams. *Managing Your Wired Workforce: A Practical Guide*. Denver, Colo.: Bradford Pub., 2003. 1-883726-79-4, \$24.95 [*Colorado Libraries*, 2004]
- Abraham Lincoln*. Colección Grandes Biografías. Madrid: Edimat Libros, 2003. 84-8403-858-0, €4.95 [*Críticas*, 2004]
- Alponte, Juan María. *Colón: el Hombre, el Navegante, la Leyenda*. México, D.F.: Aguilar, 2003. 968-19-1260-8, \$16.95 [*Críticas*, 2004]
- Olcese Salvatecci, Alfieri. *Cómo Estudiar con Éxito: Técnicas y Hábitos Para Aprender Mejor*. México, D.F.: Alfaomega Grupo Editor, 2002. 970-15-0764-9 [*Críticas*, 2003]
- Mujeres Como Islas: Antología de Narradoras Cubanas, Dominicanas, Puertorriqueñas*. Edición: Olga Marta Pérez, Thelma Jiménez, Andrés Blanco D., eds. Santo Domingo, República Dominicana: Ediciones Ferilibro, 2002. 959-209-419-5 [*Críticas*, 2003]
- Tibol, Raquel. *Los Murales de Diego Rivera: Universidad Autónoma Chapingo*. México, D.F.: Editorial RM, Universidad Autónoma Chapingo, 2002. 968-5208-08-5 [*Críticas*, 2003]
- Lindsay-Poland, John. *Emperors in the Jungle: the Hidden History of the U.S. in Panama*. Durham, N.C.: Duke University Press, 2003. 0-8223-3098-9, \$18.95 [*Críticas*, 2003]
- Kaplan, Allison G. and Ann Marlowe Riedling. *Catalog It! A Guide to Cataloging School Library Materials*. Worthington, Ohio: Linworth Pub., 2002. 1-58683-014-7, \$44.95 [*Colorado Libraries*, 2002]
- Bardach, Ann Louise. *Cuba Confidential: Love and Vengeance in Miami and Havana*. New York: Random, 2002. 0-375-50489-3, \$25.95 [*Library Journal*, 2002]
- Swan, James. *Fundraising for Libraries: 25 Proven Ways to Get More Money for Your Library*. New York: Neal Schuman, 2002. 1-55570-433-6, \$69.95 [*Colorado Libraries*, 2002]
- Puig de Lange, Victoria. *Sol Con Agua*. Nashville, Tenn.: Editorial Vistazo/Ediciones Reio Negro, 2002. 0-9724506-0-2, \$17.75 [*Críticas*, 2002]
- The Encyclopedia of Latin American Politics*. Edited by Diana Kapiszewski; assistant editor, Alexander Kazan. Westport, Conn.: Oryx Press, 2002. 1-57356-306-4, \$74.95 [*Library Journal*, 2002]
- Vargas Lizano, Isabel. *Y Si Quieres Saber de Mi Pasado*. Con la colaboración de J.C. Vales. Madrid: Santillana Ediciones Generales, S.L., 2002. 84-03-09278-4, \$18.95 [*Críticas*, 2002]
- Ruy Sánchez, Alberto. *Los Jardines Secretos de Mogador: Voces de Tierra*. México, D.F.: Alfaguara, S.A., 2001. 968-19-0879-1, \$16.95 [*Críticas*, 2002]
- Chávez, Ricardo and Celso Santajuliana. *El Final de las Nubes*. Barcelona: RBA Libros, S.A., 2001. 84-7901-760-0, \$11.95 [*Críticas*, 2002]
- The Power of Language / El Poder de la Palabra: Selected Papers from the Second REFORMA National Conference*. Edited by Lillian Castillo-Speed and the REFORMA National Conference Publications Committee. Englewood, Colo.: Libraries Unlimited, 2001. 1-563089459, \$35.00 [*Colorado Libraries*, 2001]
- Martínez, Rubén. *Crossing Over: A Mexican Family on the Migrant Trail*. Metropolitan: Holt, 2001. 0-8050-4908-8, \$26.00 [*Library Journal*, 2001]

Guevara, Ernesto "Che." *The African Dream: the Diaries of the Revolutionary War in the Congo*. Translated from the Spanish by Patrick Camiller. With an introduction by Richard Gott and a foreword by Aleida Guevara March. New York: Grove Press, 2001. 0-8021-3834-9, \$13.00 [*Library Journal*, 2001]

Cooper, Gail and Garry Cooper. *New Virtual Field Trips*. Englewood, Colo.: Libraries Unlimited, 2001. 1-56308-887-8, \$27.50 [*Colorado Libraries*, 2001]

NATIONAL SERVICE & PROFESSIONAL AFFILIATIONS

American Library Association, Life Member

Association for Library Collections & Technical Services (now CORE)

Cataloging, Classification, and Metadata Section

ALCTS Editorial Board, Member, 2015-2019

Committee on Cataloging: Description and Access, Member, 2008-2012

Test Site for RDA, Manager, 2009-2011

Nominating Committee, Member, 2007-2008

Committee for Education and Training of Catalogers, Chair, 2006-2007, Member, 2003-2007

Competencies & Education for a Career in Cataloging Interest Group, Chair, 2010-2012; Member, 2010-

President's Program Committee, 2015-2016

Education Committee, Member, 2005-2007

Task Force on Competencies and Education for a Career in Cataloging, Chair, 2007-2009

2007 Annual Meeting Pre-conference, "What They Don't Teach in Library School: Competencies,

Education and Employer Expectations for a Career in Cataloging," Steering Committee Chair

Fundraising Committee, Member, 2004-2006

Office of Diversity

Committee on Diversity, Chair, 2010-2011

Diversity Research Advisory Committee, Member, 2009-2010

Spectrum Scholar Mentor, 2009

Diversity Grants Review Committee, Member, 2007, 2010, 2012

Office of Statistics and Research

Research and Statistics Committee, Member, 2005-2007; Intern, 2003-2005

Library Research Round Table

Nominating Committee, 2022-2023

Membership Committee, 2019-2021

Board of Directors, Member At-Large, 2009-2012

Office of Accreditation

Accreditation Panel Member (training completed 2004)

Accreditation Review Panel Member (training completed 2004)

REFORMA, Life Member

National Board of Directors, 2005-2013

National Fundraising Chair, 2005-2013

National Recruiting and Mentoring Committee, 2008-2010

Colorado Chapter, Secretary, 2004-2005

Colorado Chapter Liaison to National Board of Directors, 2004-2013

American Association of Law Libraries (AALL), Life Member Online Audiovisual Catalogers Association (OLAC) Colorado Association of Law Librarians (CoALL)

American Association of University Women Association for Library and Information Science Education (ALISE)

University of Denver ALISE Representative, 2003-2008; 2010-2011

Membership Advisory Committee, 2007-2010

Technical Services Education Special Interest Group, 2003-

Garfield Doctoral Dissertation Award Reviewer, 2012

Garfield Doctoral Dissertation Scholarship Reviewer, 2014

American Association of University Professors (AAUP), 2006-

American Grant Writers Association, 2014- Grant Professionals Institute, 2016- National Grants Management Association, 2014-

Grant Reviewer (National and Regional Team Leader), U.S. Department of Education, 1998- Grant Reviewer, Broadband Technologies Opportunity Program, U.S. Department of Commerce, 2009
Grant Reviewer, Institute of Museum and Library Services, 1998-2000
Grant Reviewer, Colorado Department of Education, 2014-
Grant Reviewer, Colorado State Library, 1998-
Grant Reviewer, American Association of Community Colleges *Working Connections* program, 1999
Peer Reviewer, *Journal for Library and Information Science Education*, 2005-
Peer Reviewer, *Journal of Library Metadata*, 2009
Peer Reviewer, *International Journal of Library and Information Science*, 2011
Regular Columnist, *The Bottom Line*, 2013-2016
Book Reviewer, *Library Journal*, 2001
Book Reviewer, *Criticas*, 2002-2009
Book Reviewer, *Colorado Libraries*, 2000-2012

REGIONAL SERVICE & PROFESSIONAL AFFILIATIONS

Mountain Plains Library Association

Professional Development Grants Committee, Member, 2005-2006
Professional Development Policy and Guidelines Sub-committee Chair, 2006

Colorado Association of Libraries

“Student Voices” Column Editor, *Colorado Libraries*, 2005-2006
Conference Planning Committee, Member, 2002
Technical Services and Automation Division, Chair, 2002-2003; Member, 2000-
Academic Libraries Division, Peer Review Conference Papers Committee, Member, 2007-2009
Education Committee, Member, 1988-1993
Diverse Populations Committee, Member, 2009-2013

SERVICE TO THE UNIVERSITY OF DENVER

Center for Teaching and Learning Faculty Advisory Board, 2007-2008; 2010-2012
Center for Community Engagement and Service Learning Advisory Board, 2007-2012
Faculty Senate
Executive Committee, 2008-2013
Nominations, Rules & Credentials Committee, Chair, 2008-2013; Member 2007-2013
Appointment, Promotion, and Tenure Revision Committee, 2010-2012
Grievance Policy Committee Member, 2007-2010
Law Library Director Search Committee Chair, 2012-2013
PROF Grant Review, College Representative to the University Review Team, 2006, 2008
Project Homeless Connect Evaluations, Principal Investigator, 2006-2009
University Technology Council, 2007-2009
University of Denver Hyde Interviews for Incoming Freshmen, 2003-2012

SERVICE TO THE MORGRIDGE COLLEGE OF EDUCATION

Appointment, Tenure & Review Committee
Member, voting, 2003-2005; 2007- 2009
Chair, Clinical Faculty Promotion & Tenure Policy Subcommittee, 2008-2009
Member, Community Engagement Subcommittee, 2007-2009
Member, Tenure Review Panel, 2003
Advancement and Alumni Relations Committee, Chair, 2003-2007; Member, 2002-2007
College Building Committee Member, 2004-2010

College of Education Student Association, Faculty Advisor, 2004-2007; 2009-2010
 Faculty Senator, 2007-2013
 Research and Scholarship Committee, Chair, 2008-2009; Member, 2002-2003, 2008-2009
 Research and Grant Mentoring Committee, Chair, 2009-2010
 Research Task Force Member, 2010-2012
 Search Committee Member, Assistant Professor for Curriculum & Instruction, 2010-2011
 Workload Task Force Member, 2010-2011

SERVICE TO THE LIBRARY & INFORMATION SCIENCE PROGRAM

Library and Information Science Student and Alumni Association, Faculty Advisor, 2002-2008
 ALA Student Chapter, Faculty Advisor, 2005-2008
 Beta Phi Mu Phi Chapter, Faculty Advisor, 2004-2014
 Steering Committee Member, Accreditation by the American Library Association, 2001-2004
 Search Committee Member, Associate Professor for LIS, 2006
 Search Committee Chair, Assistant Professors for LIS, 2003, 2005, 2006, 2007
 Search Committee Ex-Officio Member, Director for LIS, 2004

SERVICE TO SAM HOUSTON STATE UNIVERSITY

Rio Roundup: South Texas Literature Conference, Conference Coordinator, 1993
 External Relations, Fund Raising, Grants Committee, Chair, 1993-1995
 Advisory Council Committee, Chair, 1993-1995
 Students, Admissions, and Advisement Committee, Chair, 1994
 Institutional Effectiveness Committee, Member, 1993-1995

SERVICE TO THE COLLEGE OF EDUCATION AND APPLIED SCIENCE

Faculty Affairs Committee, Member, 1993-1995
 Curriculum Committee, Member, 1993-1995
 Continuing Education Committee, Member, 1993-1995

SERVICE TO THE COMMUNITY

French Teacher & Student Exchange with Laon, France, Monarch High School, Boulder Valley School District
 (Boulder, Colorado), 2017-
 Denver/Boulder Games 2022, Board of Directors, Secretary-Treasurer, 2015-2018
 United Way Campaign Committee, College of Education, 2006
 Arapahoe County, Election Judge for the County Clerk and Recorder, 2000-2005
 Arthritis Foundation, Rocky Mountain Chapter, Certified Educator & Trainer, 1999-2008
 Bonfils Blood Center, Silver Level Donor, 2000-2016
 Denver Museum of Natural History, Docent, 1992
 Tech Prep of the Lower Rio Grande Valley, Inc. (Harlingen, Texas) Board of Directors, 1995-1997
 Executive Committee, 1996-1997; Chair, Development Committee, 1995-1997; Chair, Fiscal Agency
 Committee, 1995-1996; Chair, Colleges and Universities Committee, 1996-1997
 Gilpin County (Colorado) Public Library Board of Trustees, 1986-1989; Vice President, 1987-1989
 City of Central (Colorado) Economic Development Committee, 1987-1989
 Columbine Family Health Centers, Inc. (Nederland and Black Hawk, Colorado) Board of Directors, 1988-1989

CERTIFICATION

Permanent Public Librarian Certificate - Pennsylvania, New York, Texas
 Westlaw Expert Witness, 2008-
 Certified Grant Writer®, 2016-

AWARDS AND HONORS

Advanced Practitioner for Service Learning and Community Engagement, University of Denver, 2011

Platinum Star Alumnae, College of Information, Library Science & Technologies, University of North Texas, 2009
 Commendation for Integration of Technologies in Teaching & Learning Environment, University of Denver, 2006
 Outstanding Adjunct Faculty Member Award, College of Education, University of Denver, 2002
 Beta Phi Mu, Pi, University of Pittsburgh, 1985
 Alpha Lambda Sigma, University of North Texas, 1972
Albert Nelson Marquis Lifetime Achievement Award, Who's Who in America
Who's Who in American Women
Who's Who of Women Executives
Dictionary of International Biography
Who's Who in the East
Who's Who in the South and Southwest
Who's Who in the World
Who's Who of Online Professionals
Who's Who in Library and Information Science
2,000 Notable Women
Who's Who of Emerging Leaders
Who's Who in Professional and Executive Women
Who's Who in American Education
International Who's Who of Professional and Business Women
International Leaders in Achievement
International Educator of the Year
Who's Who in Finance and Industry
Who's Who in Finance and Business

Invited International and National Conference Presentations

- Driscoll, Margaret, Christy Confetti Higgins, Scott Brown, and Sylvia D. Hall-Ellis. *A View from Within: Open House Tour of Three Canvas Core Courses*. Presentation to be delivered at the School of Information, San José State University Professional Development Seminar, San José, California, October 17, 2019.
- Hall-Ellis, Sylvia D. *Invest in Me -- I'm Your Future: Succession Planning for Libraries*. Keynote presentation delivered at the ALCTS President's Symposium, Boston, Mass., January 8, 2016.
- Seidel, Kent E. and Sylvia D. Hall-Ellis. *Making Grants Work for You: Strategies for Doctoral Students and Early Career Scholars*. Presentation delivered at the University Council for Educational Administration, Early Career Scholars Session, Indianapolis, Ind., November 9, 2013.
- Hall-Ellis, Sylvia D. *So You Want to be a Manager; Leadership Skills and Competencies for Technical Services Managers and Administrators*. Presentation delivered at the 138th Annual Conference, American Library Association, Chicago, Ill., June 29, 2013.
- Seidel, Kent E., Karen S. Riley, Lyndsay Agans, Susan Korach, and Sylvia D. Hall-Ellis. *Making Grants Work for You (Instead of Just Working for Grants)*. A panel discussion delivered at the University Council for Educational Administration, Early Career Scholars Session, Denver, Colo., November 17, 2012.
- Hall-Ellis, Sylvia D. *After the Great TS Reorganization: The Westminster Law Library*. Presentation delivered at the 137th Annual Conference, American Library Association, Anaheim, Calif., June 23, 2012.
- Hall-Ellis, Sylvia D. *Conversations with Catalogers in the 21st Century*. A panel discussion sponsored by the ALCTS Competencies for a Career in Cataloging Interest Group, delivered at the 137th Annual Conference, American Library Association, Anaheim, Calif., June 22, 2012.

- Hall-Ellis, Sylvia D., moderator. *Mid-Career Leaders Program*. A panel discussion sponsored by the ALA Committee on Diversity delivered at the 136th Annual Conference, American Library Association, New Orleans, La., June 26, 2011.
- Hall-Ellis, Sylvia D., moderator. *Diversity Town Hall*. A community conversation sponsored by the ALA Committee on Diversity delivered at the 136th Annual Conference, American Library Association, New Orleans, La., June 24, 2011.
- LaBarre, Kathryn, Sylvia D. Hall-Ellis, Karen Anderson, Rick Hasenyager, Christopher Cronin, and Penny Baker. *Briefings from RDA Test Participants*. A panel discussion delivered at the Midwinter Conference, American Library Association, San Diego, Calif., January 7, 2011.
- Miksa, Shawne, Marjorie Bloss, and Sylvia D. Hall-Ellis. *Educating the Next Generation of Catalogers: Teaching RDA*. A panel discussion delivered at the 97th Annual Conference, Association for Library and Information Science Education, San Diego, Calif., January 7, 2011.
- Hall-Ellis, Sylvia D., Robert Maxwell, John Hostage, and George Prager. *RDA Panel: What Cataloging Managers Need to Know*. Presentation delivered at the 103rd Annual Conference, American Association of Law Librarians, Denver, Colo., July 12, 2010.
- Hall-Ellis, Sylvia D. and Stacey L. Bowers. *Catalogers in the RDA Environment: Skill Sets, Expectations and Challenges*. Presentation delivered at the 103rd Annual Conference, American Association of Law Librarians, Denver, Colo., July 11, 2010.
- Hall-Ellis, Sylvia D. *Comfortable in Your Cataloging and Metadata Specialist Skin? Or, So You Want to Hire a Cataloger*. Presentation delivered to the ALCTS Research Group at the 134th Annual Conference, American Library Association, Chicago, Ill., July 11, 2009.
- Perez, Megan, Sylvia D. Hall-Ellis, and Denise Anthony. *From Novice to Expert: Collaboration for Succession Planning*. A “hot topic” presentation delivered at the 14th ACRL Conference, Seattle, Wash., March 13, 2009.
- Hall-Ellis, Sylvia D. *Cataloging in the RDA Environment: Skill Sets, Expectations and Challenges*. Presentation delivered to the ALCTS Research and Publications Committee at the Midwinter Conference, American Library Association, Denver, Colo., January 24, 2009.
- Hall-Ellis, Sylvia D. *LIS Cataloging Education for the 21st Century: Expectations and Challenges*. A panel discussion held at the 95th Annual Conference, Association for Library and Information Science Education, Denver, Colo., January 23, 2009.
- Chu, Clara, Sylvia D. Hall-Ellis, and Mark Winston. *The Doctoral Degree & Building a Career*. A panel discussion delivered at the ALA Office of Diversity Spectrum Doctoral Fellows E.J. Josey Leadership Institute, Midwinter Conference, American Library Association, Denver, Colo., January 20, 2009.
- Hall-Ellis, Sylvia D. and Robert O. Ellett, Jr. *Fundamentals of Cataloging Course: An Overview of the ALCTS Online Course*. Presentation delivered to the ALCTS Big Heads Group, 133rd Annual Conference, American Library Association, Anaheim, Calif., June 30, 2008.
- Hall-Ellis, Sylvia D. *Employers’ Expectations for Technical Services Librarians: What We Don’t Know*. Presentation delivered to the ALCTS Research and Publications Committee Program, 133rd Annual Conference, American Library Association, Anaheim, Calif., June 28, 2008.

Hall-Ellis, Sylvia D., Virginia R. Maloney, and Mary Stansbury. *Institutional Responses to Engaged Scholarship: The Carnegie Foundation Engaged University Classification at Two Universities*. Presentation delivered to the 94th Annual Conference, Association for Library and Information Science Education, Philadelphia, Pa., January 11, 2008.

Hall-Ellis, Sylvia D. *Puzzles, Problems, and Predicaments*. Presentation delivered to the ALCTS Research Discussion Group, 132nd Annual Conference, American Library Association, Washington, D.C., June 23, 2007.

Hall-Ellis, Sylvia D. *Cataloging Education: A New Emphasis for the Library and Information Science Curriculum*. Presentation delivered to the ALCTS Pre-conference, 132nd Annual Conference, American Library Association, Washington, D.C., June 22, 2007. <http://www.loc.gov/catdir/cpsocareercat.html>

Ellett, Jr., Robert O. and Sylvia D. Hall-Ellis. *Copy Cataloging Done Smarter*. Presentation delivered to the International Conference on Interdisciplinary Information Sciences and Technologies (InSciT2006), October 25-28, 2006.

Hall-Ellis, Sylvia D. and Robert O. Ellett, Jr. *Cooperative Cataloging: Challenges and Opportunities for Defense Libraries*. Presentation delivered to the 1st Annual Conference of Defense Libraries, Spanish Ministry of Defense, Madrid, Spain, July 7, 2006.

Hall-Ellis, Sylvia D. *Cataloger Competencies: Do the Employers Require What the Professors Teach?* Presentation delivered to the ALCTS CCS Heads of Cataloging Discussion Group, 131st Annual Conference, American Library Association, New Orleans, La., June 26, 2006.

Grealy, Deborah S. and Sylvia D. Hall-Ellis. *From Research to Practice: The Scholarship of Teaching and Learning in LIS Education*. Presentation delivered to the at the 92nd Annual Conference, Association for Library and Information Science Education, San Antonio, Tex., January 18, 2006.

Hall-Ellis, Sylvia D. *Employers' Expectations for Entry-Level Catalogers: What Position Announcement Data Indicate*. Research paper delivered to the Technical Services Special Interests Group, 91st Annual Conference, Association for Library and Information Science Education, Boston, Mass., January 12, 2005.
<http://dlist.sir.arizona.edu/>

Hall-Ellis, Sylvia D. *Common Errors in MARC Records Prepared by LIS Students: What Does It Mean?* Research paper delivered to the ALCTS CCS Cataloging Norms Discussion Group, Mid-Winter Conference, 90th American Library Association, San Diego, Calif., January 10, 2004.

Hall-Ellis, Sylvia D. *Visual Arts as Foundation for Successful Library Automation: The Rocky Mountain College of Art & Design Experience*. Paper delivered at the 6th Annual Conference of Higher Education, Charleston, S. C., 1993.

Hall, Sylvia D. *Design Elements for Bibliographic Databases: An Overview*. Paper delivered at the 14th Online National Conference, New York, 1983.

Invited Regional Conference Presentations

Hall-Ellis, Sylvia D., Hudson, Christopher D., Brittany Cronin, and Kathryn Michaels. "The Colorado Law Project: Meeting the Public's Need for Legal Information." Panel discussion delivered at the Mountain Plains Library Association Conference, Billings, Mont., April 9, 2011.

Grealy, Deborah S. and Sylvia D. Hall-Ellis. *Education for Information Professionals in New Mexico: Library & Information Science Graduate Education at the University of Denver*. Presentation delivered at the New Mexico Library Education Summit, Las Vegas, N.M., September 26, 2005.

Hall-Ellis, Sylvia D. *Public Library-School Library Partnerships*. Presentation delivered at the 3rd Annual Colorado Association of Libraries Conference with the Mountain Plains Library Association, Denver, Colo., October 22, 2004.

Hall-Ellis, Sylvia D. *Learn All You Can – Educational Partnership Opportunities for the Lewis and Clark Bicentennial Commemoration*. Paper delivered at the 3rd Annual Lewis and Clark Bicentennial Council National Planning Conference, Bismarck, N.D., April 26, 1998.

Invited State Conference Presentations

Grealy, Deborah S. and Sylvia D. Hall-Ellis. *Academic Library Leadership Changes: Using Succession Planning and Mentoring*. Presentation delivered at the Minnesota Library Education Conference, St. Cloud, Minn., October 10, 2013.

Hall-Ellis, Sylvia D., Merrie Valliant, and Melissa Powell. *RDA: What Is It and What Do You Need To Do With It At Your Library?* Presentation delivered at the Colorado Library Consortium Spring Conference, Ft. Morgan, Colo., April 26, 2013.

Hall-Ellis, Sylvia D. *Service Learning and the Library & Information Science Graduate Education at the University of Denver*. Presentation delivered at the 4th LEADS Scholars Orientation, Denver, Colo., August 5, 2009.

Hall-Ellis, Sylvia D. *Service Learning: Enhancement to Library & Information Science Graduate Education at the University of Denver*. Presentation delivered at the 3rd LEADS Scholars Orientation, Denver, Colo., June 2008.

Hall-Ellis, Sylvia D. *Law Librarianship: A Community Conversation*. Sponsored by the Colorado Association of Law Libraries. Paper delivered at the Colorado Supreme Court Library, Denver, Colo., May 14, 2008.

Hall-Ellis, Sylvia D. *Opportunities and Challenges in Law Librarianship: A Community Conversation*. Presentation delivered at the Sturm College of Law, Denver, Colo., November 7, 2007.

Ellis, Sylvia D. *Grant Writing Resources for Nursing Professionals*. Presentation delivered at the Presbyterian / St. Luke's Health One Medical Center 1st Annual Research Symposium, Denver, Colo., October 17, 2007.

Hall-Ellis, Sylvia D. *Project Homeless Connect 4 Event Evaluation – Insights and Lessons Learned*. Presentation delivered at the Homelessness Research Symposium: What is DU Doing about Homelessness in Denver, Denver, Colo., September 14, 2007.

Hall-Ellis, Sylvia D. *Service Learning and the Library & Information Science Graduate Education at the University of Denver*. Presentation delivered at the 2nd LEADS Scholars Orientation, Denver, Colo., August 10, 2007.

Hall-Ellis, Sylvia D. *Education for Information Professionals in a Digital Environment: Library & Information Science Graduate Education at the University of Denver*. Presentation delivered at the 15th Spring Mountains and Plains Paraprofessionals Conference, Denver, Colo., February 24, 2007.

Hall-Ellis, Sylvia D. *Public Library Service to Spanish-Speaking and Latino Residents in Denver: A Case Study*. Presentation delivered at the 4th Annual Colorado Association of Libraries Conference, Denver, Colo., November 10, 2005.

- Hall-Ellis, Sylvia D. *Education for Information Professionals in a Digital Environment: Library & Information Science Graduate Education at the University of Denver*. Presentation delivered at the 14th Annual Mountains and Plains Parapros Conference, Aurora, Colo., July 29, 2005.
- Hall-Ellis, Sylvia D. *Educational Opportunities: Library & Information Science Graduate Education at the University of Denver*. Presentation delivered at the 13th Annual Mountains and Plains Parapros Conference, Centennial, Colo., August 6, 2004.
- Hall-Ellis, Sylvia D. *Library Education & Training: Focus on the West: An LIS Faculty Member's Personal Response*. Presentation delivered at the 1st Annual Colorado Association of Libraries Conference, Keystone, Colo., October 18, 2002.
- Hall-Ellis, Sylvia D. *Grant Writing for School Librarians*. Presentation delivered at the 2002 Annual Colorado Education Media Association Conference, Colorado Springs, Colo., February 15, 2002.
- Hall-Ellis, Sylvia D. *Grants – Opportunities for the Future*. Paper delivered at the Southeast Regional Accountability Annual Conference, Lamar, Colo., November 12, 1998.
- Hall-Ellis, Sylvia D. *The Texas Library Connection and Interlibrary Loan: An Experiment in Resource Sharing*. Paper delivered at the Texas Computer Educators' Association Annual Conference, Austin, Tex., February 6, 1997.
- Hall-Ellis, Sylvia D. *Finding Grant Sources on the Internet: A Guide for Librarians*. Paper delivered at the 2nd Annual Institute for School Library Personnel, Pharr-San Juan-Alamo North High School, Pharr, Tex., July 29, 1996.
- Hall-Ellis, Sylvia D. *Mathematical and Logical Thinking: A Critical Intelligence*. Paper delivered at the 3rd Annual Paraprofessional Conference at the University of Texas - Pan American, Edinburg, Tex., March 8, 1996.
- Hall-Ellis, Sylvia D. *Cataloging Trends and Issues: Update Session*. Paper delivered at the 1st Annual Institute for School Library Personnel, South Texas Community College, McAllen, Tex., July 19, 1995.
- Hall-Ellis, Sylvia D. *Grant Writing: Tips and Encouragement for School Librarians*. Paper delivered at the 1st Annual Institute for School Library Personnel, South Texas Community College, McAllen, Tex., July 18 and 19, 1995.
- Hall-Ellis, Sylvia D. *How to Become an Expert Grant Writer*. Paper delivered at the 3rd Annual High School Principals' Academy, South Padre Island, Port Isabel, Tex., June 19, 1995.
- Texas Library Study: Results from Regions I and II*. Paper delivered at the 3rd Annual Technology Conference, Texas A&M University, College Station, Tex., November 18, 1994.
- Hall-Ellis, Sylvia D. *Academic Achievement and Middle School Students*. Paper delivered at the 8th Annual Young Adult Conference, Sam Houston State University, Huntsville, Tex., November 5, 1994.
- Hall-Ellis, Sylvia D. *Multimedia Resources for Library Leaders*. Paper delivered at the Institute for Librarians in A Multicultural Environment, Sam Houston State University, Huntsville, Tex., June 10, 1994.
- Hall-Ellis, Sylvia D. *Finding the Resource: Empowering the User, or, the Case for Curriculum Based Subject Access to Learning Resource Center Collections*. Paper delivered at the 81st Annual Texas Library Association Conference, Corpus Christi, Tex., April 12-16, 1994.
- Hall-Ellis, Sylvia D. and William H. Pichette. *Sam Houston State University Makes Use of OCLC/AMIGOS Collection Analysis CD*. Paper delivered at the 81st Annual Texas Library Association Conference, Corpus Christi, Tex., April 12-16, 1994.

Hall, Sylvia D. *Funding and Library Development in Pennsylvania: A Symbiotic Relationship*. Paper delivered at the Annual Graduate Student Colloquia, University of Pittsburgh, School of Library and Information Science, 1982.

Hall, Sylvia D. *Leadership for Public Library Trustees*. Paper delivered for the Trustees Division, Pennsylvania Library Association Annual Conference, Lancaster, Penn., 1981.

Seminar and Professional Development Presentations

Taylor, Meredith, and Sylvia D. Hall-Ellis. *Talent Management and Succession Planning*. ALCTS eForum, held March 22, 2017.

Hirsh, Sandra, Heather O'Brien, Michelle Holschuh Simmons, Michael Krasulski, and Sylvia D. Hall-Ellis. *Information Services Today: An Introduction. Part 3: Information Services: Roles in the Digital Age*. Rowan and Littlefield in partnership with Library Journal webinar, recorded February 5, 2015.

Hall-Ellis, Sylvia D. and Jennifer Sweda. *Copy Cataloging in an RDA Environment*. ALCTS eForum, held May 14 and 15, 2013.

Hall-Ellis, Sylvia D. *Law Librarianship: A Community Conversation*. Sponsored by the Colorado Association of Law Libraries, presented at the Colorado Supreme Court Library, Denver, Colo., May 14, 2008.

Hall-Ellis, Sylvia D. and Beatrice Z. Gerrish. *Reading and Libraries: Recent Research in Reading*. Presentation at the Ricks Center for Gifted Education, Denver, Colo., March 4, 2008.

Hall-Ellis, Sylvia D. *Cataloger Competencies: Do the Employers Require What the Professors Teach?* Presentation for the School of Library and Information Science, San José State University, February 12, 2008.

Hall-Ellis, Sylvia D. and Robert O. Ellett, Jr. *Cooperative Cataloging: Rules, Tools, and Conventions for Building a Multi-institutional Catalog*. Sponsored for the Spanish Ministry of Defense, Madrid, Spain, July 10, 2006.

Hall-Ellis, Sylvia D. *Cash for Kids: Grant Writing Opportunities for Youth Services Librarians*. Sponsored by the Colorado Young Adult Librarians; presented at Bemis Memorial Library, Littleton, Colo., November 13, 2002.

Hall-Ellis, Sylvia D. *MARC Records and Authority Control: Planning for Bibliographic Database Migration*. Sponsored and held at the Douglas County Public Library, Castle Rock, Colo., May 28, 2002.

Grant Writing: A Refresher for Librarians. Sponsored by Library and Information Science Program, College of Education, University of Denver; presented at University Center at Chaparral, August 12, 2000.

Hall-Ellis, Sylvia D. *Shaking the Money Tree – Basic Grant Writing for Colorado Educators*. Sponsored by the Office of Educational Telecommunications of the Colorado Department of Education.

Pikes Peak Community College, Colorado Springs, Colo., November 16, 1998.

Pueblo School District 60, Pueblo, Colo., November 12, 1998.

University of Northern Colorado, Greeley, Colo., November 10, 1998.

United Technology Educational Partnership, Grand Junction, Colo., November 9, 1998.

Hall-Ellis, Sylvia D. *Cataloging Multimedia, Kits, Globes and Map Materials in USMARC*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., April 24, 1997 and December 12, 1996.

Hall-Ellis, Sylvia D. *New Standards for School Library Media Centers*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., April 15, 1997.

- Hall-Ellis, Sylvia D. *The School Library Media Specialist in the 21st Century: Visions for the Future*. Sponsored and hosted by Pharr-San Juan-Alamo Independent School District, Pharr, Tex., April 4, 1997.
- Hall-Ellis, Sylvia D. *Cataloging Sound Recordings and Audio Materials in USMARC*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., March 20, 1997 and November 21, 1996.
- Hall-Ellis, Sylvia D. *Evaluating and Selecting CD-ROMS for School Library Media Collections*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., March 18, 1997.
- Hall-Ellis, Sylvia D. *Cataloging Audiovisual Materials in USMARC*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., February 27, 1997, November 7, 1996 and October 24, 1996.
- Hall-Ellis, Sylvia D. *Introduction to Dialog: Basic Searching Strategies*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., February 14, 1997.
- Hall-Ellis, Sylvia D. *Cataloging Books in USMARC*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., January 30, 1997, October 10, 1996, September 26, 1996 and August 8, 1996.
- Hall-Ellis, Sylvia D. *Advanced Internet Searching Techniques for Librarians*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., January 21, 1997.
- Hall-Ellis, Sylvia D. *Texas Library Connection Full-Text Searching*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., December 13, 1996 and October 25, 1996.
- Hall-Ellis, Sylvia D. *Developing Evaluation Strategies for Grants and Proposals*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., December 10, 1996.
- Hall-Ellis, Sylvia D. *Developing Needs Assessment for Grants and Proposals*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., November 12, 1996.
- Hall-Ellis, Sylvia D. *Texas Library Connection Union Catalog Searching*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., November 8, 1996 and September 6, 1996.
- Hall-Ellis, Sylvia D. *Grant Resources on the Internet*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., October 23, 1996.
- Hall-Ellis, Sylvia D. *Preparing a Response to the Telecommunications Infrastructure Fund Board: Needs Assessment, Professional Development Framework, and Evaluation Strategies*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., October 16, 1996.
- Hall-Ellis, Sylvia D. *Texas Library Connection: Building the Districtwide Bibliographic Database*. Sponsored and hosted by Mercedes Independent School District, Mercedes, Tex., September 13, 1996 and August 8, 1996. Sponsored and hosted by Los Fresnos Consolidated Independent School District, Los Fresnos, Tex., August 12, 1996.
- Hall-Ellis, Sylvia D. *School-to-Work and Special Education: An Inclusive Partnership for Success*. Sponsored and hosted by the Office of Special Education, Region One Education Service Center, Edinburg, Tex., September 11, 1996.
- Hall-Ellis, Sylvia D. *Telecommunications Infrastructure Fund Board: An Overview of Funding for Secondary Schools*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., August 31, 1996.
- Hall-Ellis, Sylvia D. *Cataloging Books, Multimedia, and Realia in USMARC*. Sponsored and hosted by Edinburg Consolidated Independent School District, Edinburg, Tex., August 6, 1996.

Hall-Ellis, Sylvia D. *Internet Resources for Grant Writers*. Sponsored and hosted by Region One Education Service Center, Edinburg, Tex., April 20, 1996.

Hall-Ellis, Sylvia D. *Enhanced Grant Writing Skills for Mathematics Educators: Writing Skills for Campus Teams*. Sponsored and hosted by the Office of General Education, Region One Education Service Center, Edinburg, Tex., March 22, 1996.

Hall-Ellis, Sylvia D. *Internet Resources for Grant Writers*. Sponsored and hosted by the College of Education and Applied Science, Sam Houston State University, Huntsville, Tex., March 9, 1996.

Hall-Ellis, Sylvia D. *Grant Writing for Mathematics Educators: A Development Process for Campus Teams*. Sponsored and hosted by the Office of General Education, Region One Education Service Center, Edinburg, Tex., March 4, 1996.

Hall-Ellis, Sylvia D. *Shaking the Money Tree: Preparing Successful Technology Grant Applications*. Sponsored and hosted by the Office of Technology and Media Services, Region One Education Service Center, Edinburg, Tex., February 29, 1996 and April 29, 1996.

Hall-Ellis, Sylvia D. *District-wide Technology Planning: Technical Assistance for the Texas Education Agency Initiative*. Sponsored and hosted by the Office of Technology and Media, Region One Education Service Center, Edinburg, Tex., February 2, 1996.

Hall-Ellis, Sylvia D. *Enhanced Grant Writing Skills*. Sponsored and hosted by Pharr-San Juan-Alamo Independent School District, Pharr, Tex., January 27, 1996.

Hall-Ellis, Sylvia D. *United States Copyright Act of 1976, Video Transmissions, Computer Software and the Internet*. Sponsored and hosted by the Office of Technology and Media, Region One Education Service Center, Edinburg, Tex., January 24, 1996.

Hall-Ellis, Sylvia D. *The Grant Writing Development Process*. Sponsored and hosted by Pharr-San Juan-Alamo Independent School District, Pharr, Tex., January 20, 1996.

Hall-Ellis, Sylvia D. *MARC Cataloging of Materials for Library Media Centers*. Sponsored and hosted by the Office of Media Services, Region One Education Service Center for the Donna Independent School District, Donna, Tex., August 17, 1995.

Hall-Ellis, Sylvia D. *Classification*. Sponsored by AJ Seminars, Rockville, Maryland; presented at University Hilton Hotel, Houston, Tex., May 10, 1995.

Hall-Ellis, Sylvia D. *Library Technical Services*. Sponsored by AJ Seminars, Rockville, Maryland; presented at University Hilton Hotel, Houston, Tex., April 26, 1995.

Hall-Ellis, Sylvia D. *Grant Writing: An Introduction for Public School Administrators*. Sponsored and hosted by the Office of Administrative Services, Region One Education Service Center, Edinburg, Tex., April 19, 1995.

Hall-Ellis, Sylvia D. *The School Library Media Specialist in the 21st Century: Visions for the Future*. Sponsored and hosted by the United Independent School District, Laredo, Tex., March 31, 1995.

Hall-Ellis, Sylvia D. *Using USMARC*. Sponsored by AJ Seminars, Rockville, Maryland; presented at University Hilton Hotel, Houston, Tex., March 29, 1995.

- Hall-Ellis, Sylvia D. *Library Media Center Policies and Guidelines: How to Prepare for School Board Adoption*. Sponsored and hosted by the Office of Technology and Media Services, La Joya Independent School District, La Joya, Tex., March 10, 1995.
- Hall-Ellis, Sylvia D. *Developing District-wide Policies and Guidelines for Library Media Centers*. Sponsored and hosted by the Office of Technology and Media Services, La Joya Independent School District, La Joya, Tex., January 10, 1995.
- Hall-Ellis, Sylvia D. *MARC Cataloging of Audiovisual Materials for Library Media Centers*. Sponsored and hosted by the Office of Library Media and Technology Services, Cypress-Fairbanks Independent School District, Houston, Tex., December 1, 1994.
- Hall-Ellis, Sylvia D. *The School Library Media Specialist in the 21st Century: Visions for the Future*. Sponsored and hosted by United Independent School District, Laredo, Tex., October 14, 1994.
- Hall-Ellis, Sylvia D. *The School Library Media Specialist in the 21st Century: Visions for the Future*. Sponsored and hosted by the Laredo Independent School District, Laredo, Tex., October 7, 1994.
- Hall-Ellis, Sylvia D. *MARC Cataloging for Library Media Centers*. Sponsored by the Office of Library Media and Technology Services, Cypress-Fairbanks Independent School District, Houston, Tex., October 5, 1994.
- Hall-Ellis, Sylvia D. *Jump to the Head of the Class: Undergraduate Library Resources Available at Sam Houston State University*. Sponsored by the Office of the Associate Vice President for Student Services, Sam Houston State University, Huntsville, Tex., October 4, 1994.
- Hall-Ellis, Sylvia D. *CD-ROMs - 1994's Newest and the Best for Secondary Level Media Centers*. Sponsored and hosted by Clear Lake Independent School District, Houston, Tex., June 3, 1994.
- Hall-Ellis, Sylvia D. *Introduction to Classification*. Sponsored by AJ Seminars, Rockville, Maryland; presented at Holiday Inn, Market Center, Dallas, Tex., May 18, 1994.
- Hall-Ellis, Sylvia D. *Basic Descriptive Cataloging*. Sponsored by AJ Seminars, Rockville, Maryland; presented at University Hilton Hotel, Houston, Tex., May 4, 1994.
- Hall-Ellis, Sylvia D. *Shaking the Money Tree - Part II: Writing Successful Grant Applications*. Sponsored by Donna Independent School District, Donna, Texas, and Region One Education Service Center Edinburg, Texas; presented at South Texas Community College Library, McAllen, Tex., April 29, 1994.
- Hall-Ellis, Sylvia D. *Using MARC*. Sponsored by AJ Seminars, Rockville, Maryland; presented at Holiday Inn, Market Center, Dallas, Tex., April 6, 1994.
- Hall-Ellis, Sylvia D. *Automated Authority Control*. Sponsored by AJ Seminars, Rockville, Maryland; presented at University Hilton Hotel, Houston, Tex., March 23, 1994.
- Hall-Ellis, Sylvia D. *Automating the District School Library Media Centers: Choices and Opportunities*. Sponsored and hosted by the Office of Technology and Library Media Services, Fort Bend Independent School District, Sugar Land, Tex., March 4, 1994.
- Hall-Ellis, Sylvia D. *Shaking the Money Tree - Part I: Preparing Successful Grant Applications*. Sponsored and hosted by the Office of Library Media Services, Donna Independent School District, Donna, Tex., February 4, 1994.

GRADUATE COURSES TAUGHT

San José State University, School of Library and Information Science

INFO 249 – Advanced Cataloging and Classification (Fall 2015, 2016; Summer 2016)
INFO 287 – Special Topics in Cataloging and Classification (Spring 2017, 2018, 2019, 2020, 2021, 2022, 2023; Fall 2020, 2021, 2022, 2023)
LIBR 248 – Beginning Cataloging and Classification (Summer 2002, 2003, 2004, 2005, 2006)
LIBR 249 – Advanced Cataloging and Classification (Summer 2003; Fall 2014; Summer 2015)

University of Denver, University College

Grant Writing Certificate Seminar for Non-Profit Organizations (Fall 2020, 2021; Spring 2021)

University of Denver, Morgridge College of Education HED

5991 – Grant Writing in Higher Education (Spring 2011)
LIS 4010 – Organization of Information (Fall 2002-2009; Winter 2005; Spring 2004-2006)
LIS 4020 – Professional Principles and Ethics (Summer 2000)
LIS 4040 – Management of Libraries and Information Centers (Fall 2010; Spring 2003, 2009 (DS); Winter 2005)
LIS 4070 – Cataloging and Classification (Winter 2008, 2009, 2010, 2011, 2012; Fall 2009 (DS)) LIS
4321 – Collection Management (Spring 2005)
LIS 4326 – LIS Research (Winter 2009 (DS); Spring 2009 (DS))
LIS 4350 – Adult Materials and Services (Summer 2006, 2009)
LIS 4379 – Social Sciences Resources (Spring 2009)
LIS 4400 – Cataloging and Classification (Spring 2000, 2001; Winter 2002-2009; Summer 2005, 2006 – course renumbered LIS 4070, September 2007)
LIS 4401 – Descriptive Cataloging (Winter 2001; Spring 2002, 2003, 2006-2009; Summer 2005)
LIS 4402 – Subject Cataloging (Spring 2001, 2009; Summer 2005, 2006, 2007, 2008)
LIS 4403 – Classification Schemes (Fall 2007, 2008, 2009 (DS)) LIS
LIS 4405 – Authority Control (Winter 2009)
LIS 4510 – Materials and Services for Children (Winter 2004; Summer 2005)
LIS 4620 – Grant Writing and Fundraising (Summer 2000, 2002, 2004, 2010; Winter 2006; Fall 2006-2009)
LIS 4700 – Seminar in Technical Services (Fall 2001)
LIS 4700 – Seminar in Public Libraries (Summer 2002)
LIS 4804 – Management of Electronic Records (Spring 2004; Fall 2005)
LIS 4902 – Capstone Projects (Winter 2003, Spring 2008, 2009, 2011)
LIS 4910 – Independent Study (every quarter Winter 2000 through Spring 2011)
LIS 4920 – Service Learning (every quarter Summer 2004 through Spring 2011)
RMS 4954 – Grant Writing (Summer 2013, 2014)
RMS 4959 – Content Analysis Methodology (Spring 2015)
QRM 4978 – Grant Writing (Summer 2011, 2012)

Rutgers University, School of Communication and Information

SC&I 522 – Cataloging and Classification (Summer 2013)

University of Arizona, College of Behavioral and Social Sciences

LIS 602 – Cataloging and Classification (Summer 1995)
LIS 612 – Advanced Online Search and Retrieval (Summer 1995)

Sam Houston State University, College of Education & Applied Science

LIS 532 - Cataloging and Classification (Fall 1993, 1994, 1995)
LIS 563 - Advanced Cataloging and Classification (Summer 1994)
LIS 567 - Research Methods (Spring 1994, Spring 1995)
LIS 591 - Educational Technology (Spring 1994, 1995)
LIS 596 - Networking and Computer Technologies in Education (Fall 1993, Summer 1994, Fall 1995)

Dissertations at the University of Denver

Bowers, Stacey L. *Library Anxiety of Law School Students: A Study Utilizing the Multidimensional Library Anxiety Scale*. Chair, May 5, 2010.

Fattor, Melissa M. *Student Engagement Differences by Ethnicity and Scale for Ninth Grade Students*. Chair, November 1, 2010.

Fulton, Roseanne. *A Case Study of Culturally Responsive Teaching in Middle School Mathematics*. Kent Seidel, Chair, June 18, 2009, Outside Chair.

Grealy, Deborah S. *Tribes and Territories in Library and Information Studies Education*. Bruce Uhrmacher, Chair, June 10, 2008, Committee Member.

McCord, J. Michael. *Developing a Standard of Care for Educational Malpractice*. Chair, April 15, 2011.

Priebe, Sarah J. *Distinguishing Effects of Domain and General Knowledge on Passage Fluency and Comprehension*. Jan Keenan, Chair. July 21, 2011, Outside Chair.

Snyder-Mondragon, Sandra M. *Institutional Factors that Impact the Retention of Graduate Students of Color in Schools of Library and Information Science: A Metaregression of Accredited Library School Statistics on Student Retention and Graduation Rates*. Kathy Green, Chair, July 24, 2009, Committee Member.

Taylor, Karen Pickles. *Effective Teaching*. Elinor Katz, Chair, July 15, 2009, Outside Chair.

Thompson, Jennifer. *Distinguishing a Western Women's College: A History of the Curriculum and Student Experience at Colorado Women's College*. Edith W. King, Chair, July 16, 2010, Committee Member.

Walker, Emelda. *Influence of Organizational Factors on Job Satisfaction of Disability Service Providers at Postsecondary Institutions*. Chair, April 29, 2010.

Dissertation Proposals at the University of Denver

Bowers, Stacey L. *Library Anxiety of Law School Students: A Study Utilizing the Multidimensional Library Anxiety Scale*. Chair, November 5, 2009.

McCord, J. Michael. *Developing a Standard of Care for Educational Malpractice*. Edith W. King, Chair. April 23, 2010.

Thompson, Jennifer. *History of Colorado Women's College*. Edith W. King, Chair, October 30, 2008. Committee Member.

Walker, Emelda. *Influence of Organizational Factors on Job Satisfaction of Disability Service Providers at Postsecondary Institutions*. Chair, July 21, 2009.

Dissertations at Other Institutions

Rodríguez-Mori, Howard. *The Information Behavior of Puerto Rican Immigrants to Central Florida, 2003-2009: Grounded Analysis of Six Case Studies Use of Social Networks during the Migration Process*. Kathleen Burnett, Chair, April 10, 2009, Florida State University, Committee Member.

Schwartz, Brian *More than a Look-up Skill: Medical Information Literacy Education in Osteopathic Medical Schools*. D. Mirah Dow, Chair, July 18, 2017. Emporia State University, Committee Member.

Snow, Karen. *A Study of the Perception of Cataloging Quality among Catalogers*. Shawne D. Miksa, Chair, August 1, 2011. University of North Texas, Committee Member.

Dissertation Proposals at Other Institutions

Schwartz, Brian *More than a Look-up Skill: Medical Information Literacy Education in Osteopathic Medical Schools*. D. Mirah Dow, Chair, December 4, 2015. Emporia State University, Committee Member.

Snow, Karen. *A Study of the Perception of Cataloging Quality among Catalogers*. Shawne D. Miksa, Chair, May 11, 2010. University of North Texas, Committee Member.

Master's Thesis at the University of Denver

Hemingson, Jeff. *Recital Paper*. Lamont School of Music, February 2010, Outside Chair.

Capstones at the University of Denver

Anthony, Alisa. *Correlation of Library and Information Science Program outcomes and Vacant Position Qualifications Listed on the Colorado State Library Jobline by Employers During the Period September 1, 2000 through August 31, 2002*. Chair, Winter Quarter, 2003.

Borden, Donna M. *Improving Emergency Communications Systems: Is a Radio Communications Network the Answer?* Fall Quarter, 2014.

Bowden, Heather L.M. *Exploring Biological Models for Long-term Data Preservation*. Chair, Spring Quarter, 2008.

Casenada, Cassandra Y. *Challenges to the Recruitment, Education, and Retention of Librarians of Color*. Chair, Spring Quarter, 2008.

Chang, Jennifer C. *Legal Research Practice and Preference: A Law Firm Perspective*. Chair, Spring Quarter 2011.

Ellis, Megan S. Fitzgerald. *Design of a Public Library Adult Volunteer Recruitment Program and Training Curriculum*. Chair, Winter Quarter, 2003.

Kircher, Kathy. *Development of a Library Pathfinder for Exobiology and Posting it on the Internet*. Chair, Winter Quarter, 2003.

Melhado, Loretta. *Design of St. John's Episcopal Church Library*. Chair, Spring Quarter, 2008.

Radcliff, Kathy. *Original Cataloging of Archival materials in the HERS Collection in Penrose Library*. Chair, Winter Quarter, 2003.

Sass, Carol Ann. *ACT Periodical Index: Access to Catholic Thinking Periodical Index: Web Index to Select Catholic Periodicals*. Spring Quarter 2000.

Stone, Sergio D. *Conducting Community Analysis for the Bemis Public Library (Littleton, Colorado) Using 2002 U.S. Census Data and the Online Outcome-Based Evaluation Toolkit*. Chair, Winter Quarter, 2003.

Tureson, Tamara. *Design and Use of an Information Audit Tool for Use in a Law Library*. Chair, Winter Quarter, 2003.

Tweed, Beth. *Evaluation of Email Reference Service in a Consumer Health Library Environment*. Chair, Winter Quarter, 2003.

GRANTS AND CONTRACTS

Student Learning in Agriculture STEM through Teacher Professional Development. Research team: Stanton Gartin (PI) and Cyndi Hofmeister, Northeast Junior College; Jeff Cash, Cheryl Sánchez, Anne-Marie Crampton, Lamar Community College; Suzanna Spears, Morgan Community College; Jack Wiley, Kerry Gabrielson, Trinidad State Junior College; Michael J. Miller, Colorado State University; Michael Womochil (Co-PI), Casey Sacks, and Sylvia D. Hall-Ellis, Colorado Community College System. U.S. Department of Agriculture, Agriculture and Food Research Initiative, Food, Agriculture, Natural Resources and Human Sciences Education and Literacy Initiative, \$404,460 (2017-2020)

Leading and Achieving: the Colorado Agriculture Regional Consortium. Research team: Jack Wiley (PI), Kerry Gabrielson, Trinidad State Junior College; Jeff Cash (PI), Cheryl Sánchez, Anne-Marie Crampton, Lamar Community College; Suzanna Spears, Morgan Community College; Cyndi Hofmeister, Northeast Junior College; Michael Womochil (Co-PI), Casey Sacks, and Sylvia D. Hall-Ellis, Colorado Community College System. U.S. Department of Agriculture, Hispanic Serving Institutions Education Grants Program, \$504,414 (2017-2020)

Cyber Prep Program Planning Grant. Research team: Debbie Sagen (PI), Brenda Lauer, Pikes Peak Community College; Gretchen Martin, Koiosa Insights; and, Sylvia D. Hall-Ellis, Colorado Community College System. U.S. Department of Commerce, Regional Alliances and Multi-stakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development, \$199,681 (2016-2018)

Career and Technical Education in Colorado: Pathways to Education and Employment. Research team: Heather McKay (PI), Rutgers University; Sarah Heath, Casey Sacks, Sylvia D. Hall-Ellis, Colorado Community College System. U.S. Department of Education, Institute of Education Sciences, \$1,400,000 (2017-2021)

Pre-Alliance Planning Grant Colorado Community College Alliance. Research team: Victor Vialpondo (PI) and Janel Highfill, Community College of Aurora; Heidi Loshbaugh (Co-PI), Community College of Denver; Rick Reeves, Bill McGreevy, Liz Cox, and Kristin Aslin, Red Rocks Community College; Cathy Pellish, Front Range Community College; Samuel DeVries, Arapahoe Community College; Sylvia D. Hall-Ellis, Colorado Community College System. National Science Foundation, Louis Stokes Alliance for Minority Participation (LSAMP), \$86,817 (2016-2017)

Towards Scalable Differentiated Instruction Using Technology-enabled, Competency-based, Dynamic Scaffolding. Research team: Karen Wilcox (PI) and Vijay Kumar, Center for Computational Engineering, Massachusetts Institute of Technology; Flora McMartin, Broad-based Knowledge; Quinsigamond Community College; and, Casey Sacks, and Sylvia D. Hall-Ellis, Colorado Community College System. U.S. Department of Education, First in the World Developmental Grant, \$2,891,882 (2015-2019)

Colorado Strategic Partnerships Emergency Grant. Research team: Elise Lowe-Vaughn (PI), Amy Hodson, Celia Hardin, Barbara McBride, James Newby, Christopher Dewhurst, Nina Holland, Kate Anderson, MaryAnn Roe, Chrystalynn Chrystalynn, Elaine Edon, Mona Barnes, Tom Morgan, Rob Hanni, and Marie Valenzuela, Colorado Department of Labor and Employment; Steve Anton, Joelle Brouner, and, Katie Griego, Colorado Department of Human Services; Rebecca Holmes, Judith Martinez, and Jennifer Jirous, Colorado Department of Education; Emily Templin Lesh, Colorado Workforce Development Council; Cory Everett, Colorado Department of Regulatory Agencies; and, Casey Sacks and Sylvia D. Hall-Ellis, Colorado Community College System. U.S. Department of Labor, Strategic Partnerships Emergency Grant, \$5,000,000 (2015-2017)

CAEL Jump Start Program: Competency-Based Education. Research team: Jerry Migler (PI), Casey Sacks, Debra Cohn, Thomas Hartman, and Sylvia D. Hall-Ellis, Colorado Community College System; Matt Jamison, Front Range Community College; Mike Coste, Red Rocks Community College; Amanda Corum, Pueblo Community College; Janet Colvin, Pikes Peak Community College; and, MaryAnn Matheny, Community College of Denver. Council for Adult and Experiential Learning, \$15,000 (2015)

Summit on the Redesign of Developmental Education. Research team: Jerry Migler (PI), Casey Sacks, and Sylvia D. Hall-Ellis, Colorado Community College System; Chip Nava, Pueblo Community College; Kim Moultny, Arapahoe Community College; Debbie Ulibarri, Trinidad State Junior College; and, Kris Bernard, Front Range Community College. American Association of Community Colleges, \$15,000 (2015-2016)

Equity in Excellence at Colorado Community Colleges. Research team: Keith Howard (PI) and Sylvia D. Hall-Ellis, Colorado Community College System; Estela Mata Bensimon, Center for Urban Education, University of Southern California; and Kerry Gabrielson, Trinidad State Junior College. Colorado Department of Higher Education, Colorado Opportunity Scholarship Program, \$150,000 (2015-2016)

MBA High School of Business in Colorado. Research team: Laurie Urich (PI) and Sylvia D. Hall-Ellis, Colorado Community College System; Rudolph Sumpter and Beatrice Gerrish, Boulder Valley Schools; Keith Curry Lance, RSL Research Group. Colorado Department of Higher Education, Colorado Opportunity Scholarship Program, \$501,295 (2015-2016)

Fullbridge Program in Colorado. Research team: Keith Howard (PI) and Sylvia D. Hall-Ellis, Colorado Community College System; Suzanna Spears, Fort Morgan Community College; and, Cheryl Sánchez and Anne-Marie Compton, Lamar Community College. Colorado Department of Higher Education, Colorado Opportunity Scholarship Program, \$300,000 (2015-2017)

Colorado Community College System Alternative Credit Program. Research team: Jerry Migler (PI), Keith Howard, and Sylvia D. Hall-Ellis, Colorado Community College System. American Council on Education, \$13,000 (2015)

Internationalization in Higher Education. Researcher: Samuel D. Museus. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Internationalization, \$8,000 (2014-2015)

International Perspectives on Bilingual Education. Researcher: Sharolyn Pollard-Durodola. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Internationalization, \$3,700 (2014-2015)

Cultivating Culturally Relevant and Responsive Curriculum and Pedagogy in College. Researcher: Samuel Museus. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, iRise Grant, \$5,000 (2014-2015)

Project EMERGE (Educational Model for Evaluation and Replicability in Gifted Environments). Research team: Norma Hafenstein (PI) and Bruce Uhrmacher. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Lynde and Harry Bradley Foundation, \$235,000 (2014-2015)

Collecting Asian American Refugee Stories. Researcher: Samuel Museus. Technical reviewer for MCE: Sylvia D. Hall-Ellis. American Educational Research Association, Research Grant, \$5,000 (2014-2015)

Developing Expertise in Teaching K-5 Mathematics. Research team: Julie Sarama (PI) and Douglas H. Clements (Co-PI), in partnership with the School of Education at the University of Michigan. Technical reviewer for MCE: Sylvia D. Hall-Ellis. National Science Foundation, \$130,344 (2013-2015)

Investigation of the Long-Term Outcomes for Special Education Students. Researcher: Antonio Olmos-Gallos. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Jefferson County School District, Office of Assessment, \$40,000 (2014)

Refugee Community Collaboration. Researcher: Vicki Tomlin (PI) in partnership with the African Community Center and Jewish Family Service. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Center for Community Engagement and Service Learning, \$14,854 (2014-2015)

Access to Mathematics for All. Research team: Richard S. Kitchen (PI), Nicole M. Russell (Co-PI), and Terrence Blackman (Co-PI), Curriculum Studies and Teaching Program, Morgridge College of Education; Álvaro Árias (Co-PI, Department of Mathematics); and, James Gray (Co-PI), Department of Mathematics, Community College of Aurora. Technical reviewer for MCE: Sylvia D. Hall-Ellis. National Science Foundation, The Robert Noyce Scholarship Program, Capacity Building Project, \$349,926 (2014-2016)

Cognitive Test Battery for Intellectual Disabilities. Research team: Karen Riley (PI), Lyndsay Agans, Jessica Lerner, and Karin Dittrick-Nathan in partnership with David Hessel (PI), The MIND Institute at the University of California – Davis, and Elizabeth Berry-Kravis, Rush University Medical Center. Technical reviewer for MCE: Sylvia D. Hall-Ellis. National Institutes of Health, Outcome Measures for Use in Treatment Trials for Individuals with Intellectual and Developmental Disabilities (R01), \$2,499,996 (\$588,672 at DU) (2014- 2019)

Broadening Participation in Engineering among Women and Latino/as: A Longitudinal, Multi-Site Study. Researcher: Patton Garriott (PI) in partnership with the University of North Dakota and the University of Missouri. Technical reviewer for MCE: Sylvia D. Hall-Ellis. National Science Foundation, HER Core Research, \$677,390 (\$69,992 at DU) (2014-2019)

Designing a Teacher Evaluation System to Improve Teacher Effectiveness for Culturally and Linguistically Diverse Learners. Research team: María del Carmen Salazar (PI), Jessica Lerner, and Kathy Green. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Professional Research Opportunities for Faculty, \$29,988 (2014-2016)

Developing a College-Going Culture in Latina/O Families: Exploring the Influence of Funds of Knowledge on Family Outreach Programs. Researcher: Judy Marquez Kiyama. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Professional Research Opportunities for Faculty, \$18,720 (2014-2016)

Assessment of Quality of Life in Neural Implantation Surgery for the Treatment of Parkinson's Disease. Researcher: Cynthia McRae. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Internationalization, \$3,967 (2014-2015)

Pura Vida: Cloud Forest, Curriculum and Cross-Cultural Study. Research team: Norma Hafenstein (PI) and Bruce Uhrmacher (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Internationalization, \$8,000 (2014-2015)

Online Course Development for Curriculum and Instruction. Researcher: Ruth Chao. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Teaching and Learning, \$3,000 (2014)

Online Course Development for Curriculum and Instruction. Researcher: María del Carmen Salazar. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Teaching and Learning, \$3,000 (2014)

Online Course Development for Curriculum and Instruction. Researcher: Jessica Lerner. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Teaching and Learning, \$3,000 (2014)

Online Course Development for Curriculum and Instruction. Researcher: Duan Zhang. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Teaching and Learning, \$3,000 (2014)

The Mathematics Education of African Americans, 1866 – 1954. Researcher: Nicole M. Russell. Technical reviewer for MCE: Sylvia D. Hall-Ellis. National Academy of Education, Spencer Foundation Postdoctoral Fellowship, \$55,000 (2014-2016)

Early Childhood Care and Education Study. Research team: Carrie Germeroth (PI), Melissa Mincic, and Douglas H. Clements. Technical reviewer for MCE: Sylvia D. Hall-Ellis. State of North Dakota, Department of Public Instruction, \$73,500 (2013-2014)

Graduate Level Specialty in Addiction Counselor Training with Emphasis on Integration of Native American Specific Content. Research team: Ruth Chao (PI) and Michael J. Faragher (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. The Galena Foundation, \$289,732 (2013-2016)

The Collecting Asian American and Pacific Islander Refugee Stories (CARS) Project. Researcher: Samuel Museus. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Center for Community Engagement and Service Learning, \$15,000 (2014)

Parents in Transition: A Multiple Case Study of Parent and Family Orientation Programs. Researcher: Judy Marquéz Kiyama. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Faculty Research Fund, \$1,500 (2014-2015)

The Sistah Network: Black Women Graduate Students Supporting and Retaining Each Other. Researcher: Nicole M. Russell. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Faculty Research Fund, \$2,708 (2014-2015)

Evaluation of the Northeast Denver Babies Ready for College Program. Research team: Carrie Germeroth (PI), Melissa Mincic, and Douglas H. Clements. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Mile High Montessori, \$9,922 (2013-2014)

Developing Teaching Expertise in K-5 Mathematics. Research team: Julie Sarama (PI) and Douglas Clements (University of Denver), in partnership with Timothy Boerst (PI), Meghan Shaughnessy, Deborah Ball, Hyman Bass (School of Education at the University of Michigan). Technical reviewer for MCE: Sylvia D. Hall-Ellis. National Science Foundation, \$449,827 (\$130,344 at the University of Denver) (2013-2015)

Early Learning Care and Education Study Program Grant for the State of North Dakota. Research team: Carrie Germeroth (PI), Melissa Mincic, and Sheridan Green. Technical reviewer for MCE: Sylvia D. Hall-Ellis. State of North Dakota Department of Public Instruction, \$73,500 (2013-2014)

Local Professional Learning Community for School Leaders. Research team: Susan Korach (PI), Kristina Hesbol, and Rebecca McClure. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Education Development Center, \$10,950 (2013)

Healthy Eaters, Lifelong Movers 2: Implementing Evidence-Based School Environment, Policy, and Curricular Changes to Increase Opportunities for Healthy Eating and Physical Activity in Low Income, Rural Colorado. Research team: Elaine Berlansky, University of Colorado at Denver (PI), Nicholas Cutforth, University of Denver (Co-PI), and Allison Reeds. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Colorado Health Foundation, \$3,103,108 (2013-2017)

Hughes Rare Books Library Room Renovation in the Sturm College of Law. Project team: Patti H. Marks, Sylvia D. Hall-Ellis, and Leigh Elliott. Mabel T. Hughes Charitable Trust, \$34,000 (2013-2014)

The Promise Center Partnership with the Marsico Institute for Early Learning and Literacy and the City and County of Denver. Research team: Karen Riley (PI), Douglas H. Clements (Co-PI), and Sheridan Green. Technical reviewer for MCE: Sylvia D. Hall-Ellis. The Piton Foundation, \$223,468 (2013-2014)

Center of Excellence for Problem Gambling. Research team: Ruth Chao (PI) and J. Mike Faragher. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Colorado Department of Behavioral Health, \$68,021 (2012-2013)

United Way Implementation and Validation Review. Research team: Douglas H. Clements (PI), Amanda Moreno, and Sheridan Green. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Mile High United Way, \$19,737 (2013)

Math/Science Partnership in Rural Districts. Research team: Kristen Bunn (PI, Eagle County Schools), Paul Michalec (Co-PI), and Alegra Reiber. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Colorado Department of Education, Colorado's Mathematics and Science Partnership Program, \$750,000 (2013-2014)

Mathematics and Science Education of African Americans. Research team: Nicole Russell (PI), Sylvia D. Hall-Ellis, Steve Fisher (Penrose Library). Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Professional Research Opportunities for Faculty, \$29,994 (2013-2015)

Online Course Development for Curriculum and Instruction. Researcher: Nicole Russell. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Teaching and Learning, \$3,000 (2013)

Discourse and Opportunity: Undocumented Students and Higher Education Policy. Researcher: Ryan Gildersleeve. Technical reviewer for MCE: Sylvia D. Hall-Ellis. National Academy of Education, Spencer Foundation Postdoctoral Fellowship, \$55,000 (2012-2014)

An Anthropological Study of the Latino Graduation Ceremony. Researcher: Ryan Gildersleeve. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Spencer Foundation, \$39,900 (2012-2013)

Fragile-X and Pharmaceutical Company: Clinical Trial of AFQ056. University of California – Davis Children's Hospital MIND Institute (Sacramento), Children's Hospital Denver, and Rush Children's Hospital at Rush University Medical Center (Chicago). Karen Riley, PI. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Novartis Pharmaceuticals Corporation, \$394,206 (2012-2014)

Project Engage, Phase 2, a DAPRA Grant in partnership with Total Immersion Systems, Inc., and Texas A&M University. Research team: Karen Riley (PI) and Lyndsay Agans (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. U.S. Department of Defense, \$60,000 (2011-2013)

International School Psychology Practicum Exchange. Researcher: Gloria L. Miller. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Center for Community Engagement and Service Learning, \$14,951 (2012-2013)

Online Course Development for Curriculum and Instruction. Research team: Bruce Uhrmacher (PI) and Norma Hafenstein (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Teaching and Learning, \$18,193 (2012-2014)

Writers in the Schools. Research team: Karen Riley (PI) and Amanda Moreno (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. Colorado Humanities, \$4,965 (2012-2013)

Learning Ecosystem Validation Grant. Research team: Karen Riley (PI), Lyndsay Agans, Kent Seidel, and Shimelis Assefa. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Bill & Melinda Gates Foundation, \$315,000 (2012-2013)

Project Words of Oral Reading and Language Development (WORLD). Research team: Jorge E. Gonzalez (PI), Texas A&M University; Laura Saenz (Co-PI), University of Texas – Pan American; and, Sharolyn Pollard-Durodola (Co-PI), University of Denver. Technical reviewer for MCE: Sylvia D. Hall-Ellis. U.S. Department of Education, Institute of Education Sciences, \$53,354 (2012-2015); award \$640,718, transfer from Texas A&M University

Increasing the Efficacy of an Early Mathematics Curriculum with Scaffolding Designed to Promote Self-Regulation. Research team: Douglas H. Clements (PI) and Julie Sarama (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. U.S. Department of Education, Institute of Education Sciences, \$1,445,315 (2008-2014); award \$4,541,975, transfer from University at Buffalo, The State University of New York

Using Rule Space and Poset-based Adaptive Testing Methodologies to Identify Ability Patterns in Early Mathematics and Create a Comprehensive Mathematics Ability Test. Research team: Douglas H. Clements (PI) and Julie Sarama (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. National Science Foundation, \$323,791 (2010-2014); award \$1,194,944, transfer from University at Buffalo, The State University of New York

Comprehensive Postdoctoral Training in Scientific Education Research. Researcher: Julie Sarama (PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. U.S. Department of Education, Institute of Education Sciences, \$133,458 (2010-2014); award \$613,353, transfer from University at Buffalo, The State University of New York

Longitudinal Study of a Successful Scaling Up Project: Extending TRIAD. Research team: Douglas H. Clements (PI), Julie Sarama (Co-PI), and Abt Associates (Carolyn Layzer, Fatih Unlu, Laurie Bozzi, Lily Fesler, Alina Martinez, Cristofer Price, James van Orden). Technical reviewer for MCE: Sylvia D. Hall-Ellis. Institute of Education Sciences, \$384,940 (2011-2015; award \$1,250,286, transfer from University at Buffalo, The State University of New York

Early Childhood Education in the Context of Mathematics, Science, and Literacy. Research team: Julie Sarama (PI), Douglas H. Clements (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. National Science Foundation, \$990,020 (2010-2014; award \$2,285,228, transfer from University at Buffalo, The State University of New York

Early Childhood Clearinghouse Information Center Redesign. Research team: Karen Riley (PI) and Amanda Moreno (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. Office of the Lt. Governor of Colorado, \$12,000 (2012-2013)

Morgridge Rural Educational Leadership Initiative. Research team: Lyndsay Agans (PI), Linda Brookhart (Co-PI), Susan Korach, and Rebecca McClure. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Morgridge Family Foundation, \$100,000 (2012-2014)

Center of Excellence for Problem Gambling. Research team: Patrick Sherry (PI) and J. Mike Faragher. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Colorado Department of Behavioral Health, \$55,000 (2012-2013)

Intermodal Transportation Institute Research Initiatives. Researcher: Patrick Sherry. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University Transportation Centers Program, Research and Innovative Technology Administration, U.S. Department of Transportation. \$600,000 (2012-2014)

Mile High United Way Social Innovation Fund Early Literacy Initiative. Gloria L. Miller, PI, Amanda Moreano, Kim Hartnett-Edwards, and Sheridan Green. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Mile High United Way, \$89,992 (2012-2013)

International School Psychology Practicum Exchange. Researcher: Gloria L. Miller. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Center for Community Engagement and Service Learning, \$1,000 (2012-2013)

Refugee Student Art Outreach. Researcher: Karin Ditttrick-Nathan. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Faculty Research Fund, \$3,000 (2012-2013)

Resistance, Resilience, and Reciprocity: Centering the Voices of Black Doctoral Women with Faculty Aspirations. Researcher: Nicole M. Russell. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Faculty Research Fund, \$2,965 (2012-2013)

- Assessing Learning through Student Notebooks*. Research team: Keith Miller, Nancy Sasaki, and Kathy Green. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Professional Research Opportunities for Faculty, \$30,000 (2012-2014)
- International School Psychology Practicum Exchange*. Researcher: Gloria L. Miller. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Internationalization, \$2,000 (2012-2013)
- ELO in Colorado*. Research team: Cynthia Hazel and Duan Zhang. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Colorado Legacy Foundation, \$150,000 (2012-2013)
- Creating Online LIS Courses*. Research team: Mary C. Stansbury (PI), Shimelis Assefa, Denise Anthony, Xiao Hu, and Krystyna Matusiak. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Center for Teaching and Learning, \$15,000 (2011-2013)
- Maritime Piracy Seminar*. Researcher: Ved Nanda, The Nanda Center, Sturm College of Law. Technical reviewer for Sturm College of Law: Sylvia D. Hall-Ellis. Arsenault Family Foundation, \$15,000 (2012-2013).
- Early Childhood Librarianship: An Interdisciplinary, Experiential Learning MLIS*. Researcher: Mary C. Stansbury (PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. Laura Bush's 21st Century Librarians Program, Institute for Museums and Library Services, \$249,066 (2012-2014)
- Learning Ecosystem Planning Grant*. Research team: Karen Riley (PI), Lyndsay Agans, Kent Seidel, and Shimelis Assefa. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Bill & Melinda Gates Foundation, \$281,217 (2011-2012)
- Advanced Service Learning Practitioner Faculty Grant*, Sylvia D. Hall-Ellis, University of Denver, Center for Community Engagement and Service Learning, \$400 (2011)
- Evaluating and Enhancing the EspeciallyMe Program*. Research team: Lori D. Patton and Nicole Russell. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Center for Community Engagement and Service Learning, Public Good Fellowship Grant, \$24,780 (2012)
- Choosing Excellence: Let Every Child Bloom*. Research team: Shimelis Assefa (PI) and Mary C. Stansbury (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Center for Community Engagement and Service Learning, Public Good Grant, \$7,657 (2012)
- K-8 STEM Content Specific Professional Development to Improve Elementary Student Achievement*. Research team: Kent Seidel (PI), Nicole Russell (Co-PI), Kimberly Hartnett-Edwards, Paul Michalec, Jeff Farmer, Keith Miller, Alegra Reiber, and Nancy Sasaki. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Colorado Department of Education, Improving Teacher Quality Grant, (Title II ESEA), \$307,299 (2011-2012)
- Building a Better Principal Pipeline to Boost Student Achievement*. Researcher: Susan Korach. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Denver Public Schools; a subcontract from the Wallace Foundation Grant, \$170,000 (2011-2017)
- Center of Excellence for Problem Gambling*. Research team: J. Mike Faragher (Co-PI) and Bobbie Vollmer (PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. Colorado Department of Behavioral Health, \$79,999 (2011-2012)
- An Exploration of Novice Teachers' Core Competencies: Impacts on Student Achievement, and Effectiveness of Preparation*. Research team: Kent Seidel (PI), Kathy Green (Co-PI), Kimberly Hartnett-Edwards, and Duan Zhang. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Institute of Education Sciences, Effective Teachers and Effective Teaching, \$990,987 (2012-2015)

Project Engage, a DAPRA Grant in partnership with Total Immersion Systems, Inc., and Texas A&M University.

Research team: Karen Riley (PI) and Lyndsay Agans (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. U.S. Department of Defense, \$49,964 (2011-2014)

User-centered Evaluation of Music Search Engines. Researcher: Xiao Hu. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Faculty Research Fund, \$2,931 (2011-2012)

Educational Practicum in Vietnam and China to Promote the Inclusion of Young Children with Disabilities.

Researcher: Gloria L. Miller. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Office of Internationalization, \$5,000 (2011-2012)

Evaluation of Colorado's Enhancing Quality in Infant-Toddler (EQIT) Initiative. Research team: Virginia R.

Maloney and Amanda Moreno. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Buell Foundation, \$395,884 (2011-2013)

Creating Engaging Environments to Teach Pre-Algebra Mathematics to Elementary Students. Research team:

Álvaro Arias, Mario López, María del Carmen Salazar, and Lyndsay Agans. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver Interdisciplinary Grant, \$60,000 (2011-2012)

Morgridge Education Technology Accessible (META) Resource Project. Research team: Lyndsay Agans (PI) and

Shimelis Assefa (Co-PI). Technical reviewer for MCE: Sylvia D. Hall-Ellis. Morgridge Family Foundation, \$36,000 (2011)

MCE Connect: A 21st Century Framework for Faculty Development. Research team: Bruce Uhrmacher (PI),

Shimelis Assefa (Co-PI), Lyndsay Agans (Co-PI), Kimberly Hartnett-Edwards, Norma Hafenstein, Xiao Hu, Paul Michalec (Co-PI), María del Carmen Salazar (Co-PI), and Sandra Snyder-Mondragon. Technical reviewer for MCE: Sylvia D. Hall-Ellis. University of Denver, Center for Teaching and Learning, \$22,355 (2011-2012)

Parent Education and Parent Leadership and Advocacy. Research team: Virginia Maloney (PI) and Amanda

Moreno, Marsico Institute for Early Learning and Literacy. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Colorado Health Foundation, \$27,358 (2010-2011)

Intentional School Culture. Researcher: Cynthia Hazel. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Denver Public Schools, \$38,040 (2010-2011)

Healthy Eaters, Lifelong Movers: Implementing Evidence-Based School Environment, Policy, and Curricular Changes to Increase Opportunities for Healthy Eating and Physical Activity in Low Income, Rural Colorado.

Research team: Elaine Berlansky, University of Colorado at Denver (PI), Nicholas Cutforth, University of Denver (Co-PI), and Allison Reeds. Technical reviewer for MCE: Sylvia D. Hall-Ellis. Colorado Health Foundation, \$1,683,277 (2011-2014)

Second Life Learning Community. Research team: Don McCubbrey (PI), Sylvia D. Hall-Ellis (Co-PI), Walter

LaMendola, and Paul Novak. University of Denver, Center for Teaching and Learning, \$13,000 (2010-2011)

Reintroducing the Value of Law Librarians to Academic and Public Librarians in Colorado through the

Identification and Use of Emerging Technologies. Research team: Sylvia D. Hall-Ellis (Co-PI), Stacey L.

Bowers (PI), and Christopher Hudson, in partnership with Denver Public Library, Arapahoe Library District, and the Colorado State Supreme Court Library. University of Denver, Center for Community Engagement and Service Learning, \$5,773 (2010-11)

Reintroducing the Value of Law Librarians to Public Librarians through the Identification and Use of Emerging

Technologies and Resources. Research team: Stacey Bowers (PI) and Sylvia D. Hall-Ellis (Co-PI). American Association of Libraries, Wolters Kluwer Law & Business Grant Program, \$2,725 (2010-2011)

Faculty Service Learning Pod. Research team: María del Carmen Salazar and Nicholas Cutforth (Curriculum and Instruction Program), Frank Tuitt (Higher Education Program), Cynthia Hazel and Gloria Miller (Child, Family, and School Psychology Program), and Sylvia D. Hall-Ellis (Library and Information Science Program). University of Denver, Center for Community Engagement and Service Learning, \$8,000 (2010-2011)

Lincoln Collaborative. Research team: Antonio Esquibel (Principal, Lincoln High School), María del Carmen Salazar (Curriculum and Instruction Program), and Sylvia D. Hall-Ellis. School Improvement Grant, Denver Public Schools, \$375,000 (2010-2012)

Future LEADers of America: Leaders III. Research team: Denver Public Library (Kristen Svendsen, PI), the University of Denver (Sylvia D. Hall-Ellis), the Colorado Chapter of REFORMA (Orlando Archibeque), and the Colorado Association of Libraries (Martin Garner). Laura Bush's Recruiting Librarians for the 21st Century Program, Institute for Museums and Library Services, \$988,366 (2009-2012)

Teaching for Success in the Library Environment: LIS 4030 in Library 2.0. Research team: Deborah S. Greal (PI) and Sylvia D. Hall-Ellis (Co-PI). University of Denver, Center for Teaching and Learning, \$ 9,350 (2009-10)

Writing Group Faculty Grant, Sylvia D. Hall-Ellis, University of Denver, Center for Community Engagement and Service Learning, \$750 (2008-2009)

Collaborative Learning Faculty Grant, Sylvia D. Hall-Ellis, University of Denver, Center for Teaching and Learning, \$1,500 (2008)

Connecting Information Literacy to Learning. Research team: Lori Micho, Merrie Valliant, Amanda Samland, and Sylvia D. Hall-Ellis. Colorado State Library, LSTA Discretionary Grant Program, \$19,548 (2008-2009)

Law Librarianship Fellows Program. Research team: Sylvia D. Hall-Ellis (PI), Stacey Bowers (Co-PI), and Christopher Hudson, Westminster Law Library. Laura Bush's 21st Century Librarians Program, Institute for Museums and Library Services, \$999,370 (2008-2012)

Grant Writing in a Cooperative Learning Environment. Sylvia D. Hall-Ellis. University of Denver, Center for Teaching and Learning, \$2,000 (2008-2009)

Project Homeless Connect 6 Event Evaluation. Research team: Sylvia D. Hall-Ellis and Duan Zhang. University of Denver Center for Community Engagement and Service Learning, \$9,785 (2008)

Project Ecuador: International Learning Service Libraries – A Faculty Development Experience in Ecuador. Sylvia D. Hall-Ellis, Office of Internationalization, University of Denver, \$600 (2007)

Project Ecuador: International Learning Service Libraries – A Faculty Development Experience in Ecuador. Sylvia D. Hall-Ellis, International Service Learning Office, University of Denver, \$400 (2007)

Project Homeless Connect 5 Event Evaluation. Research team: Sylvia D. Hall-Ellis and Duan Zhang. University of Denver Center for Community Engagement and Service Learning, \$1,000 (2007)

Project Homeless Connect 4 Event Evaluation. Research team: Sylvia D. Hall-Ellis and Duan Zhang. University of Denver Center for Community Engagement and Service Learning, \$4,595 (2007)

Future LEADers of America: Leaders II. Research team: Denver Public Library (Kristen Svendsen, PI), the University of Denver (Sylvia D. Hall-Ellis), and the Colorado Chapter of REFORMA (Orlando Archibeque). Laura Bush's Recruiting Librarians for the 21st Century Program, Institute for Museums and Library Services, \$988,518 (2007-2010)

Strategic Planning Assistance for the Denver Medical Library. Sylvia D. Hall-Ellis. Denver Medical Library, Inc., \$30,000 (2006-2007)

Destiny Software for JMAC Student Lab. Sylvia D. Hall-Ellis, gift from the Sagebrush Corporation, Minneapolis, Minnesota, \$10,000 (2006)

Libraries: Tools for Education and Development Worldwide: A Faculty Development Experience in France. Sylvia D. Hall-Ellis, Office of Internationalization, University of Denver, \$800 (2005)

Denver Public Library: Opportunities for Change. Sylvia D. Hall-Ellis, Colorado Community Based Research Network, \$2,000 (2005)

Future LEADers of America. Research team: Denver Public Library (Letty Icolari and Steve Taylor, PIs), Emporia State University (Jim Agee), and the University of Denver (Sylvia D. Hall-Ellis). Recruiting Librarians for the 21st Century Program, Institute for Museums and Library Services, \$670,315 (2005-2008)

American Association of University Professors Summer Institute Professional Development Grant. Sylvia D. Hall-Ellis, American Association of University Professors, \$300 (2005)

Beta Phi Mu Alumni Tea. Sylvia D. Hall-Ellis, gift from the Office of Alumni and Parent and Relations, University of Denver, \$2,000 (2005)

Spectrum Software for LIS Student Lab. Sylvia D. Hall-Ellis, gift from the Sagebrush Corporation, Minneapolis, Minnesota, \$5,000 (2005)

Developing Research Capacity in Community Organizations and Residents through Training and Technical Assistance. Nicholas J. Cutforth (PI) and Sylvia D. Hall-Ellis. Piton Foundation, \$25,000 (2005-2006)

Libraries: Tools for Education and Development Worldwide: A Faculty Development Experience in Argentina. Sylvia D. Hall-Ellis, Office of Internationalization, University of Denver, \$500 (2004)

Developing Research Capacity in Community Organizations and Residents through Training and Technical Assistance. Research team: Nicholas J. Cutforth (PI), Gary Lichtenstein and Sylvia D. Hall-Ellis, Piton Foundation, \$25,000 (2003-2004)

Increasing Spanish-Speaking and Hispanic Diversity among Library and Information Science Students at the University of Denver: Development of a Student Recruitment Model. Researcher: Sylvia D. Hall-Ellis (PI), Office of Multicultural Excellence, University of Denver, \$2,750 (2003-2004)

Collection Development Enrichment to Support the Cataloging & Classification Specialization and School Librarianship within the Library & Information Science Program at the University of Denver. Research team: Sylvia D. Hall-Ellis (PI) and Deborah S. Grealy. Women's Library Association, University of Denver, \$4,000 (2003)

Collection Development Enrichment to Support the Library & Information Science Program at the University of Denver. Research team: Deborah S. Grealy (PI) and Sylvia D. Hall-Ellis. Women's Library Association, University of Denver, \$4,000 (2001)

Wireless LAN for Library Education. Research team: Deborah S. Grealy (PI) and Sylvia Hall-Ellis. University of Denver, Center for Teaching and Learning, \$24,000 (2001-2002)

Upward Bound – A Program for South Texas Youth. Research team: Monte Churchill, Executive Director of Community Relations; Gary R. Saucedo, Outreach Coordinator; Raymond Hernandez, (PI) Associate Dean for Student Success; and Sylvia D. Hall-Ellis, South Texas Community College (McAllen, Texas). U.S. Department of Education, Office of Postsecondary Education, \$2,672,003 (1999-2003)

Write Now! Improving Elementary Students' Writing Skills. Research team: Caryl G. Thomason, Assistant Superintendent (PI); Karen Tankersley, Principal; and, Hal Anderson, Director of Technology, Cheyenne Mountain School District 12 (Colorado Springs, Colorado); and Sylvia D. Hall-Ellis. Colorado Department of Education, Educational Telecommunications Unit, \$189,453 (1999-2001)

Operation Quick Start -- Distance Learning in Rural Colorado. Research team: Randal Weigum, Technology Coordinator (PI); Bonnie Barns, Director of Federal Programs and Staff Development; and, Adam "Joe" Raskop, Executive Director, Southeastern Board of Cooperative Educational Services (Lamar, Colorado); and Sylvia D. Hall-Ellis. Colorado Department of Education, Educational Telecommunications Unit, \$400,000 (1999-2001)

Advanced Technological Training for Information Professionals for the 21st Century. Research team: Mario Reyna, Division of Business Director (PI) and Sylvia D. Hall-Ellis, South Texas Community College (McAllen, Texas). Phi Delta Kappa and the National Science Foundation, \$250,000 (1999-2001)

Working Connections – Training Information Technologies Professionals for the 21st Century. Research team: Mario Reyna, Division of Business Director (PI) and Sylvia D. Hall-Ellis, South Texas Community College (McAllen, Texas). Microsoft Corporation and the American Association of Community Colleges, \$1,147,775 (1999-2001)

The ROAD (Research Oriented Amplification of Development to Literacy) Program. Research team: Deborah J. Leong (PI), Metropolitan State University; Elena Bodrova, Metropolitan State University; Dmitri Semenov, Robert J. Marzano, and Sylvia D. Hall-Ellis, Mid-continent Regional Educational Laboratory (Aurora, Colorado). Hewlett-Packard Foundation, \$25,000 (1998-1999)

Press to Literacy. Research team: Deborah J. Leong (PI), Metropolitan State University; Elena Bodrova, Metropolitan State University; Dmitri Semenov, Robert J. Marzano, and Sylvia D. Hall-Ellis, Mid-continent Regional Educational Laboratory (Aurora, Colorado). The Denver Post and the Robert S. McCormick Foundation, \$49,818 (1998-1999)

International Telementor Center. Research team: David Neils, David B. Frost (PI), and Sylvia D. Hall-Ellis, Mid-continent Regional Educational Laboratory (Aurora, Colorado). Hewlett-Packard Philanthropy, \$100,000 (1998-1999)

America Reads: Providing Tutor Training for the America Reads Challenge. Research team: Louis F. Cicchinelli (PI) and Sylvia D. Hall-Ellis, Mid-continent Regional Educational Laboratory (Aurora, Colorado). U.S. Department of Education, Office of Educational Research and Improvement, \$306,000 (1998-1999)

Comprehensive School Reform. Research team: Louis F. Cicchinelli (PI), J. Timothy Waters, and Sylvia D. Hall-Ellis, Mid-continent Regional Educational Laboratory (Aurora, Colorado). U.S. Department of Education, Office of Educational Research and Improvement, \$285,000 (1998-1999)

Sustainable Energy Education (SEE) Program for Grades 4-8: Preparing Today's Youth for Lifelong Learning and Responsible Actions in Energy Conservation. Research team: Mary Gromko, Colorado Department of Education; Gene McCarthy, Rocky Flats Field Office, U.S. Department of Energy; Gina Kissell, National Renewable Energy Laboratory; and Barbara L. McCombs (PI), Janet L. Bishop, and Sylvia D. Hall-Ellis, Mid-continent Regional Educational Laboratory (Aurora, Colorado). State of Colorado Governor's Office for Energy Conservation, \$499,936 (1997-1999)

Review of Kansas Curriculum Standards in Mathematics and Language Arts. Research team: Robert J. Marzano

(PI), John S. Kendall, David B. Frost, and Sylvia D. Hall-Ellis, Mid-continent Regional Educational Laboratory (Aurora, Colorado). Submitted to the Kansas State Department of Education, \$25,903 (1998)

International Telementor Center. Research team: David Neils, John Kuglin, Chris Rapp, David B. Frost (PI), and Sylvia D. Hall-Ellis, Mid-continent Regional Educational Laboratory (Aurora, Colorado). Hewlett-Packard Company, \$54,752 (1998)

Genesis Mission: Education Public Outreach. Developed in partnership by the Jet Propulsion Laboratory, California Institute of Technology, Los Alamos National Laboratory, Lockheed Martin Astronautics, and the Mid-continent Regional Educational Laboratory (Aurora, Colorado). Research team: John T. Sutton (PI), Alice Krueger, Martha Henry, Greg Rawls, Shae Isaacs, Jeff Johnson, Deb Jordan, Arlene Mitchell, David B. Frost, Jana Caldwell, J. Timothy Waters, and Sylvia D. Hall-Ellis. National Aeronautics and Space Administration, \$139,700,000; subcontract award, \$4,750,000 (1997-2007)

North Dakota Mathematics Assessment Project. Developed in partnership by the North Dakota Department of Education and Mid-continent Regional Educational Laboratory (Mid-continent Regional Educational Laboratory). Research team: Ann Clapper, Clarence Bina, Greg Gallagher, North Dakota Department of Education; Don Burger (PI), Hillary Michaels, and Sylvia D. Hall-Ellis, Mid-continent Regional Educational Laboratory (Aurora, Colorado). U.S. Office of Education, \$1,618,214; subcontract award, \$389,076 (1997-2001)

Pacific Resources for Education and Learning Distance Education: Project Evaluation. Developed in partnership by the Pacific Educational Community, the Pacific Resources for Education and Learning (PREL), and Mid-continent Regional Educational Laboratory (McREL). Research team: John W. Kofel (PI), Executive Director, PREL; J. Timothy Waters, Executive Director; Joan Buttram, Robert Keller, and Sylvia D. Hall-Ellis, Mid-continent Regional Educational Laboratory (Aurora, Colorado). U.S. Office of Education, Star Schools Program, \$10,000,000; subcontract award, \$500,000 (1997-2002)

Identification of Bilingual Gifted and Talented Children: A Comprehensive School Grants for Bilingual Education. Developed in partnership by Hidalgo (Texas) ISD, Los Fresnos (Texas) CISD, Progreso (Texas) ISD, University of Texas – Pan American (Edinburg, Texas), and Education Service Center, Region One (Edinburg, Texas). Research team: Hilda Medrano, Dean, College of Education, University of Texas – Pan American; Linda Phemister (PI), Janie Navarro, and Sylvia D. Hall-Ellis, Education Service Center, Region One. U.S. Department of Education, Office of Bilingual Education and Minority Languages Affairs, \$1,670,633 (1997-2002)

Academics 2000: First Things First -- The Texas Goals 2000. Developed for Jim Hogg (Hebbronville, Texas) County ISD, Mirando City (Texas) ISD, and San Isidro (Texas) ISD. Research team: Hilda Medrano, Dean, College of Education, University of Texas - Pan American (Edinburg, Texas); Angie Lehmann, Amy Mares, Ellen Gonzalez (PI), and Sylvia D. Hall-Ellis, Education Service Center, Region One (Edinburg, Texas). Texas Education Agency, \$339,987 (1997-2000)

Southwestern Bell's Learning Communities Initiative. Developed for Tech Prep of the Rio Grande Valley, Inc. (Harlingen, Texas); the Center for Professional Teacher Development, University of Texas – Brownsville; Teach for America – Rio Grande Valley (McAllen, Texas); and Education Service Center, Region One (Edinburg, Texas). Research team: Patricia G. Bubb, Executive Director (PI), Tech Prep of the Rio Grande Valley; Martin Winchester, Executive Director, Teach for America – Rio Grande Valley; Aileen Johnson, Director, School of Education, University of Texas – Brownsville; and Sylvia D. Hall-Ellis. Southwestern Bell Foundation, \$100,000 (1997-1998)

Texas School to Work: Regional Implementation. Developed for Tech Prep of the Rio Grande Valley, Inc. (Harlingen), South Texas Community College (McAllen), Texas State Technical College (Harlingen), Texas Southmost College (Brownsville), Empowerment Zone of the Rio Grande Valley (Mercedes), Project VIDA (Weslaco), Youth Fair Chance (McAllen), and Education Service Center, Region One (Edinburg). Research team: Patricia G. Bubb (PI), Tech Prep of the Rio Grande Valley; Stephen Vassberg, Texas State Technical College; Ellen Trevino, Youth Fair Chance; Wanda Garza, Project VIDA; Leonardo Olivares, University of

Texas – Pan American; Michael Bell, South Texas Community College; and Sylvia D. Hall-Ellis. Texas Workforce Commission, \$4,250,000 (1997-2002).

Comprehensive Bilingual Education Grant for Hidalgo ISD and Roma ISD. Developed for Hidalgo (Texas) ISD, Roma (Texas) ISD, College of Education, University of Texas – Pan American (Edinburg, Texas), and Education Service Center, Region One (Edinburg, Texas). Research team: Tomas Thomas (PI), Director, Office of Bilingual Education and Sylvia D. Hall-Ellis. U.S. Department of Education, Office of Bilingual Education and Minority Languages Affairs, \$1,531,361 (1997-2002)

Lopez High School, Porter High School, Rivera High School, Central Middle School, and Perkins Middle School, Brownsville (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$1,473,611 (1997-1998)

Donna High School, Todd Middle School, and Solis Middle School, Donna (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$704,052 (1997-1998)

Memorial Middle School and Nellie Schunior Middle School, La Joya Independent School District (Texas). Telecommunications Infrastructure Fund Board, \$293,641 (1997-1998)

Martin High School, Christen Middle School, Cigarroa Middle School, Lamar Middle School, Laredo (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$1,200,000 (1997-1998).

Lasara Middle School, Lasara (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$246,210 (1997-1998)

Los Fresnos High School and Resaca Middle School, Los Fresnos (Texas) Consolidated Independent School District. Telecommunications Infrastructure Fund Board, \$500,000 (1997-1998)

Lyford Junior High School, Lyford (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$354,997 (1997-1998)

Travis Middle School, McAllen (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$269,139 (1997-1998)

Mission High School, Mission (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$297,010 (1997-1998)

Progreso High School, Progreso (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$300,000 (1997-1998)

San Perlita High School, San Perlita (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$293,490 (1997-1998)

Myra Green Junior High School, Raymondville (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$225,000 (1997-1998)

Rio Grande City High School, Ringgold Middle School, Gruella Middle School, Rio Grande City (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$809,934 (1997-1998)

Rio Hondo Junior High School, Rio Hondo (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$297,024 (1997-1998)

Roma High School, Roma (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$333,178 (1997-1998)

San Benito High School, Miller Jordan Junior High School, San Benito (Texas) Consolidated Independent School District. Telecommunications Infrastructure Fund Board, \$547,000 (1997-1998)

Santa Maria High School and Santa Maria Middle School, Santa Maria (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$400,000 (1997-1998)

Salvador High School, United Independent School District (Laredo, Texas). Telecommunications Infrastructure Fund Board, \$250,879 (1997-1998)

Weslaco High School, Cabaza Middle School, Cuellar Middle School, Weslaco (Texas) Independent School District. Telecommunications Infrastructure Fund Board, \$874,242 (1997-1998)

Principals' Assessment and Training Center. Developed for Education Service Center, Region One (Edinburg, Texas). Research team: Roberto Zamora, Leonel Barrera, William H. Parry, and Sylvia D. Hall-Ellis. Texas Principals' Leadership Initiative, Texas Association of Secondary School Principals, Texas Association of Elementary School Principals, and the Sid Richardson Foundation. \$461,439 (1996-1998)

The Texas Library Connection -- Integrating and Sharing Resources. Developed for Hidalgo County Library System (McAllen), Cameron County Library System (Brownsville), South Texas Community College (McAllen), the University of Texas - Pan American (Edinburg), University of Texas – Brownsville, and Education Service Center, Region One (Edinburg). Research team: William R. McGee, Coordinator, Hidalgo County Library System; Joe Garcia, Director, Cameron County Library System; Michael D. Bell, Library Director, South Texas Community College; Eleanor Folger Foster, University Library, University of Texas - Pan American; Jaime Vela (PI), Director of Instructional Technology and Media Services, Ron Pontius, Instructional Technology, and Fabiola Fuentes, Media Services, Education Service Center, Region One; and Sylvia D. Hall-Ellis. Office of Library Media Services, Technology Services, Texas Education Agency. \$8,000 (1996-1997)

Developing Leadership Communities for Improving Algebra I for All Students. Developed for a partnership of the Region One Statewide Systemic Initiative Team. Research team: Noel Villarreal (PI), Eduardo Cancino, and Sylvia D. Hall-Ellis, Education Service Center, Region One (Edinburg). Texas Statewide Systemic Initiative for Reform in Mathematics, Science and Technology Education to The Charles A. Dana Center for Mathematics and Science Education, The University of Texas at Austin. \$25,000 (1996-1997)

Academics 2000: First Things First -- The Texas Goals 2000. Developed for Edinburg (Texas) CISD. Research team: Hilda Medrano, Dean, College of Education, University of Texas - Pan American (Edinburg); Helen Jones, Director (PI), Gifted and Talented Education, Edinburg CISD; and Sylvia D. Hall-Ellis, Education Service Center, Region One (Edinburg). Texas Education Agency, \$750,000 (1996-2001)

Texas Teachers Empowered for Achievement in Mathematics (TEXTEAM) Institute for Algebra I. Developed for Hidalgo ISD, Jim Hogg (Hebbronville) County ISD, La Joya ISD, La Villa ISD, Lyford ISD, Mission CISD, Pharr-San Juan-Alamo ISD, Rio Hondo ISD, San Isidro ISD, San Perlita ISD, Santa Maria ISD, Santa Rosa, Sharyland ISD, Valley View ISD, Webb (Laredo) CISD, Weslaco ISD, and Zapata County (Zapata) ISD. Research team: Noel Villarreal (PI), Chuck McInteer, Ellen M. Gonzalez, Education Service Center, Region One (Edinburg); and Sylvia D. Hall-Ellis. Charles A. Dana Center for Mathematics and Science Education, University of Texas - Austin, \$15,975 (1996)

Community Learning Center for La Villa, Texas. Developed for Edcouch-Elsa Independent School District. Research team: Noe Gonzalez (PI), Assistant Superintendent, Edcouch-Elsa Independent School District, and Sylvia D. Hall-Ellis. Delta Region Subzone, Rio Grande Valley (Texas) Rural Empowerment Zone, \$325,000 (1996-1997)

Monte Alto (Texas) Community Learning Center. Developed for Monte Alto Independent School District. Research team: Homero A. Diaz (PI), Superintendent, Monte Alto Independent School District, and Sylvia D. Hall-Ellis. Delta Region Subzone, Rio Grande Valley (Texas) Rural Empowerment Zone, \$300,000 (1996-1997)

Community Learning Center for La Villa, Texas. Developed for La Villa Independent School District. Research team: Sam Gonzalez (PI), Assistant Superintendent, La Villa Independent School District; and Sylvia D. Hall-Ellis. Delta Region Subzone, Rio Grande Valley (Texas) Rural Empowerment Zone, \$325,000 (1996-1997)

Building Project for Taylor Elementary. Developed for Mercedes (Texas) Independent School District. Research team: Mrs. Denise Rivera, Librarian, and Eduardo Infante, Principal, Taylor Elementary School; Ismael S. Cantu (PI), Federal Programs Director, Mercedes Independent School District; and Sylvia D. Hall-Ellis. Delta Region Subzone, Rio Grande Valley (Texas) Rural Empowerment Zone, \$375,000 (1996-1997)

Border Education Network (BEN) - Distance Education through Cable Television. Developed for Edinburg (Texas) Consolidated Independent School District. Research team: Noe Torres (PI), Library Media Specialist, Magdalena Rosas, Library Media and Technology Coordinator, Edinburg Consolidated Independent School District; and Sylvia D. Hall-Ellis, Education Service Center, Region One (Edinburg). Edinburg (Texas) Consolidated School District, \$250,000 (1996-1997)

Multiservice One-Stop Open Enrollment Charter School. Developed for the Information Referral Resource Assistance, Inc. (McAllen, Texas). Research team: Pablo Perez and Aguié Pena (PI), Executive Director, Information Referral Resource Assistance, Inc.; Roberto Zamora and Sylvia D. Hall-Ellis, Education Service Center, Region One (Edinburg). Texas Education Agency, \$3,066,000 (1996-2001)

Project OK: A Community Youth Opportunities Grant for Summer, 1996. Developed for McAllen (Texas) Independent School District, St. Joseph the Worker Catholic Church, and the Office of Adult Education, Education Service Center, Region One. Research team: Father Bart Flatt, St. Joseph the Worker Catholic Church; Noe Calvillo (PI), Office of Adult Education; Maria Louisa Garcia, McAllen Independent School District; and Sylvia D. Hall-Ellis, Education Service Center, Region One (Edinburg). Texas Protective and Regulatory Agency through the Office of the Mayor, City of McAllen, \$350,000 (1996-2001).

Early Childhood: a Time of Discovery. Developed for a partnership of Lasara ISD, Rio Hondo ISD, San Perlita ISD, the School of Education, University of Texas - Brownsville, and Education Service Center, Region One (Edinburg). Research team: Hugo Rodriguez, Dean, School of Education, University of Texas - Pan American; Leonel Barrera and Jack Damron, Field Service Agents, Ellen M. Gonzalez (PI), Administrator for Student Instructional Services, Ruth Solis, Education Specialist in Special Education, and Sylvia D. Hall-Ellis, Education Service Center, Region One (Edinburg). Texas Education Agency, \$722,090 (1996-2001)

Innovative Gifted and Talented Programs for Early Childhood and Elementary Education Students. Developed for a partnership of Edinburg (Texas) CISD, the School of Education, University of Texas - Pan American (Edinburg), and Education Service Center, Region One (Edinburg). Research team: Hilda Medrano, Dean, School of Education, University of Texas - Pan American; Helen de la Garza (PI), Director of Elementary Curriculum and Instruction, Edinburg CISD; and Sylvia D. Hall-Ellis. Texas Education Agency, \$750,000 (1996-2001)

Reading Recovery in Early Elementary Grades. Developed for a partnership of La Villa (Texas) ISD the School of Education, University of Texas - Pan American (Edinburg), and Education Service Center, Region One (Edinburg). Research team: Hilda Medrano, Dean, School of Education, University of Texas - Pan American; Marcario Salinas (PI), Supervisor of Elementary Curriculum and Instruction, La Villa ISD; and Sylvia D. Hall-Ellis, Education Service Center, Region One. Texas Education Agency, \$750,000 (1996-2001)

Connected Mathematics Project for Middle and Junior High Students. Developed for a partnership of Michigan State University, The Charles A. Dana Center for Mathematics and Science Education, The University of Texas at Austin and Region One Statewide Systemic Initiative Team. Research team: Jack Damron, Chuck McInteer, Noel Villarreal (PI), and Sylvia D. Hall-Ellis, Education Service Center, Region One (Edinburg). National Science Foundation through Michigan State University to the Charles A. Dana Center at the University of Texas - Austin, \$539,610 (1996-1999)

Sharing Resources: Testing the Interlibrary Loan Potential of the Texas Library Connection -- Integrating Media Resources. Developed under the sponsorship of the Hidalgo County Library System (McAllen) and Education Service Center, Region One (Edinburg). Research team: William H. McGee, Hidalgo County System Coordinator; Fabiola Fuentes, Library Media; Ronald Pontius (PI), Instructional Technology, Education Service Center, Region One; and Sylvia D. Hall-Ellis. Library Media Services Program, Office of Technology Services, Texas Education Agency, \$25,000 (1996-1997)

State and Federal Adult Education JOBS Program. Developed for Education Service Center, Region One (Edinburg). Research team: Noe Calvillo (PI), Director, Adult Education Program, and Sylvia D. Hall-Ellis. Adult Education Program, Texas Education Agency, \$532,846 (1995-1996)

Creating Safe and Drug-Free Schools and Communities. Developed for a partnership of the Region One Consortium for Safe and Drug-Free Education Environments. Research team: Clara Contreras (PI), Health Specialist, and Sylvia D. Hall-Ellis, Education Service Center, Region One (Edinburg). Texas Education Agency, \$150,000 (1995-1996)

Developing Leadership Communities for Improving Mathematics Performance for All Students on Title I Campuses. Developed for a partnership of the Region One Statewide Systemic Initiative Team. Research team: Jack Damron, Chuck McInteer, Noel Villarreal (PI), and Sylvia D. Hall-Ellis, Education Service Center, Region One (Edinburg). Texas Statewide Systemic Initiative for Reform in Mathematics, Science and Technology Education to The Charles A. Dana Center for Mathematics and Science Education, The University of Texas at Austin, \$50,669 (1995-1996)

The Impact of Library Resource Centers on Academic Achievement in Selected Public Schools in South Texas. Sylvia D. Hall-Ellis (PI). Developed under the sponsorship of the Department of Library Science, College of Education and Applied Science, Sam Houston State University (Huntsville). Texas Association of School Librarians, Children's Services Round Table, and Young Adults Round Table (Austin, Texas), \$2,500 (1995)

School Library Media Specialists Fellowship Program. Sylvia D. Hall-Ellis (PI). Developed under the sponsorship of the Department of Library Science, College of Education and Applied Science, Sam Houston State University (Huntsville, Texas). U.S. Department of Education, HEA Title II-B, Library Education and Human Resource Development Program, \$44,000 (1995-1996)

Planning for Educational Technology. Research team: Ruth Ann Riggins (PI), Director of Library Media and Technology Services, Donna (Texas) Independent School District; Noe Torres, Education Service Center, Region One; Patricia G. Bubb, Tech Prep of the Rio Grande Valley, Inc; Michael D. Bell, South Texas Community College; and Sylvia D. Hall-Ellis, Sam Houston State University. Developed under the sponsorship of Donna (Texas) Independent School District, Education Service Center, Region One (Edinburg), Tech Prep of the Rio Grande Valley, Inc. (Harlingen), South Texas Community College (McAllen), and the Department of Library Science, Sam Houston State University (Huntsville). Funded through Infusion of Educational Technology Planning Grant Program (H.B. 18: Models). Texas Education Agency, \$18,000 (1993-1994)

The Impact of Library Resource Centers on Academic Achievement in Selected Public Schools in South Texas.

Sylvia D. Hall-Ellis (PI) and Mary Ann Berry. Developed under the sponsorship of the Department of Library Science, College of Education and Applied Science, Sam Houston State University (Huntsville). Sam Houston State University Research Enhancement Fund, \$7,500 (1993-1994)

Electronic Mail Resource Sharing System: Management and Operation of the Iowa Computer-Assisted Network.

State Library of Iowa, \$294,000 (1986-1993)

The Iowa Locator: A CD-ROM Resource Sharing Tool. State Library of Iowa, \$567,000 (1986-1992)

Statewide Database Development: An OCLC Tape Analysis To Determine Feasibility. State Library of South Dakota, \$15,000 (1987)

The Iowa Locator: A Feasibility Study. State Library of Iowa, \$50,000 (1986)

Electronic Mail Resource Sharing System: A Feasibility Study for Libraries in the State of Iowa. State Library of Iowa, \$5,000 (1985)

Access Pennsylvania: A Feasibility Study. State Library of Pennsylvania, \$50,000 (1984)

Automating Library Administrative and Management Tasks: Procurement and Distribution of Microcomputer Systems for District Library Centers in the Commonwealth of Pennsylvania. State Library of Pennsylvania, \$495,000 (1982)

Sharing Serial Titles Resources: Procurement and Distribution of Microfiche Readers for 550 Libraries in the Commonwealth of Pennsylvania. State Library of Pennsylvania, \$500,000 (1982)

Electronic Mail System: A Pilot Project for Libraries throughout the Commonwealth of Pennsylvania. State Library of Pennsylvania, \$125,000 (1982)

Literacy Program for Adults in Rural Upstate New York State: Program Outreach and Evaluation - Phase 3. Appalachian Regional Commission, \$50,000 (1981)

Database Building: A Cooperative Project of the Finger Lakes Library System (Ithaca), Four County Library System (Binghamton), and the Southern Tier Library System (Corning). New York State Library, \$450,000 (1980-1985)

Faces of the Southern Tier: A Professional Photographer-in-Residence. New York State National Endowment for the Humanities, \$25,000 (1980)

Literacy Program for Adults in Rural Upstate New York State: Program Implementation - Phase 2. Appalachian Regional Commission, \$50,000 (1980)

Small Business Resources Center: A Pilot Project for Rural Public Libraries. New York State Library, \$50,000 (1980)

Media Programming: A Professional Development Program for Public Librarians in Upstate New York: A Program in Allegheny, Chemung, Schuylers, Steuben, and Yates Counties. New York State Library, \$35,000 (1979)

Information and Library Resources for Inmates and Prisoners in Selected Upstate New York Facilities: A Cooperative Program in Allegheny, Chemung, Schuylers, Steuben, and Yates Counties. New York State Library, \$25,000 (1979)

Library Resources for Homebound Adults in Upstate New York: An Outreach Program in Allegheny, Chemung, Schuyler, Steuben, and Yates Counties. New York State Library, \$40,000 (1979)

Literacy Program for Adults in Rural Upstate New York State: Program Initiation and Establishment - Phase 1. Funded by the Appalachian Regional Commission. Awarded to the Corning (New York) Public Library, \$50,000 (1979)

Information Reference Services to Homebound Adults. New York State Library, \$31,000 (1978)

Books-By-Mail Services to Homebound Adults. New York State Library, \$31,000 (1978)

System Headquarters Services and Programs for Public Libraries in District 10. Funded through Library Services and Construction Act Title I. Texas State Library and Historical Commission, \$880,000 (1976)

County Library Development Grant for Atascosita County. Funded through Library Services and Construction Act Title I. Texas State Library and Historical Commission, \$15,000 (1976)

Spanish Language Materials Collection Development Program. Texas State Library and Historical Commission, \$40,000 (1975)

Establishment of System Headquarters for Alamo Regional Library System (District 10) Headquartered at the San Antonio (Texas) Public Library. Texas State Library and Historical Commission, \$800,000 (1975)

SELECTED CONSULTANTSHIPS

Project Strategic Planning & Funding Proposal Development

Walden University, 2015.

Pikes Peak Library District, 2014.

Douglas County Public Libraries, 2011-2012.

Denver School for Science and Technology, 2008-2011.

Johnson & Wales University, Denver Campus, 2007-2009.

Challenges, Choices, and Images K-12 Charter School, Denver Public Schools, 2007.

Denver Medical Library, Inc., 2006-2010.

Bemis Public Library (Littleton), Ergonomic Design and Facilities Enhancement Consultant, 2003.

Curtis Park Community Center (Denver), Community Technology Center Evaluation and Proposal Development Consultant, 2003.

Colorado Community Based Research Network (Denver), Funding Research Associate, 2002.

Our Lady of the Rosary Academy (Edgewater), Learning Resource Center Development Project Consultant, 2001-2003

University of Southern Colorado (Pueblo). Technology Integration and Curriculum Enhancement into Higher Education Learning Environment. Proposal Development Consultant, 2000.

Jefferson County Library System (Lakewood), 1999-2000.

Southeastern BOCES (Lamar, CO). Distance Learning Curriculum Content Development Project. Proposal Development Consultant, 1998-2004.

Cheyenne Mountain School District 12 (Colorado Springs, CO). Technology Integration into Elementary Writing Curriculum Project. Proposal Development Consultant, 1998.

Telecommunications Infrastructure Fund Board Round #2 Application, 1997. Technical assistance to the following: La Villa (Texas) Independent School District; Mirando City (Texas) Independent School District; Monte Alto (Texas) Independent School District; San Isidro (Texas) Independent School District.

Telecommunications Infrastructure Fund Board Round #1, 1996. Technical assistance to the following: Brownsville (Texas) Independent School District; Donna (Texas) Independent School District; Edinburg (Texas) Consolidated Independent School District; Harlingen (Texas) Consolidated Independent School District; Jim Hogg County Independent School District (Hebbronville, Texas); La Feria (Texas) Independent School District;

La Joya (Texas) Independent School District; La Villa (Texas) Independent School District; Los Fresnos (Texas) Consolidated Independent School District; Progreso (Texas) Independent School District; Raymondville (Texas) Independent School District; Rio Hondo (Texas) Independent School District; San Benito (Texas) Independent School District; Sharyland Independent School District (Mission, Texas); Weslaco (Texas) Independent School District; Zapata (Texas) County Independent School District.

South Texas Community College (McAllen). Strategy Development to Meet the Technology Instructional Needs for Vocational, School-To-Work and Academic Programs, 1994-2000. Development Consultant.

Donna (Texas) Independent School District. Planning for the Infusion of Technology in Middle Schools Serving High At-Risk Students, 1994-1995. Research Associate.

Pettus (Texas) Independent School District. Planning for District-wide Automation in School Library Media Centers: Preparation of Data, and CD-ROM Hardware/Software Configuration Evaluation, 1994. Principal Investigator.

Fort Bend Independent School District (Sugar Land, TX). Planning for District-wide Automation in School Library Media Centers, Preparation of Data, and CD-ROM Hardware/Software Configuration Evaluation, 1994-1995. Principal Investigator.

Northern Waters Library Services (Ashland, WI). Professional Consulting Services to Make Recommendations on the Development of System-Wide Efforts of the Northern Waters Library Service, 1988-1989. Research Associate.

State Library of Iowa (Des Moines). The Iowa Locator Compact Disc to Support Multi-Type Libraries Resource Sharing including Database Design, Building, Production, and Distribution, 1986-1991. Project Director.

State Library of Iowa (Des Moines). Iowa Computer-Assisted Network Development, Enhancement, and Operation, 1985-1992. Technical Director.

State Library of South Dakota (Pierre). Statistical Sampling and Analysis of Multi-Institutional OCLC Archive Tape for Statewide Online Database Building, 1985-1986. Research Associate.

District of Columbia Public Library (Washington, DC). Planning Document for the Retrospective Conversion of Bibliographic Records and Automation Issues in the 1990's, 1984-1985. Research Associate.

State Library of Pennsylvania (Harrisburg). Database Development for High School Libraries, 1984-1985. Research Associate.

MINITEX (Minneapolis, MN). Workshops for Retrospective Conversion, Bar Coding, Library Statistics, and OCLC Serials Format, 1985. Presenter and Research Associate.

ABC Film Consortium (Altoona, Bellefonte, Johnstown, PA). Database Building, System Design, and Implementation of Online Film Booking System, 1983-1985. Database Manager.

Library Automation -- System Design & Implementation

Douglas County Library District (Castle Rock, CO). Library Automation Technical and System Performance Specifications, 2001.

Pharr-San Juan-Alamo Independent School District (Pharr, TX). Library Automation Technical and System Performance Specifications, 1997. Project Development Consultant.

Harlingen (Texas) Independent School District. Planning for District-wide Automation in Junior High School Library Media Centers: Preparation of Data, and CD-ROM Hardware/Software Configuration Evaluation, 1996. Principal Investigator.

Sharyland (Texas) Independent School District. Design and Construction of New Elementary School Library and Technology Resources Center, 1995-1996. Principal Investigator.

South Texas Independent School District (Mercedes, TX). Design and Construction of a New High School Library and Technology Resources Center, 1995-1996. Principal Investigator.

Citizens' Library (Washington, PA). Online Community Resources Files: Design and Implementation, 1984. Research Associate.

Altoona (Pennsylvania) Hospital. Integrated Online System Upgrade Study, 1984. Research Associate.

State Library of South Dakota (Pierre). Automation Plan and State Database Development, 1982-1983. Principal Investigator.

State Library of Pennsylvania (Harrisburg). COM Production and Preparation of the Technical Specifications Document, Procurement, and Distribution of Microcomputers in the Commonwealth of Pennsylvania, 1983-1984. Research Associate.

Altoona (Pennsylvania) Area Public Library. Integrated System (Circulation/Online Catalog) Study, 1982-1983. Principal Investigator.

COPSCAULD (Council of Pennsylvania State College and University Library Directors, Edinboro, PA). Design of Online Media Catalog, 1982. Principal Investigator.

Erie (Pennsylvania) County Library System. Operations Research and Design for Automated Circulation, Hardware Upgrade and Re-Retrospective Conversion, 1982. Research Associate.

Michigan Library Consortium (Lansing, MI). Tape Management System Design and Implementation, 1982-1984. Research Associate.

State Library of Pennsylvania (Harrisburg). Preparation of the Technical Specifications Document, Procurement and Distribution of Microfiche Readers in the Commonwealth of Pennsylvania, 1982. Research Associate.

Community College of Allegheny County, Allegheny Campus (Pittsburgh, PA). Integrated Systems Study, 1981. Principal Investigator.

Community College of Allegheny County, South Campus (West Mifflin, PA). Retrospective Conversion Training Program for Handicapped Students, 1981. Technical Director.

Southern Tier Library System (Corning, NY). OCLC Acquisitions Subsystem Evaluation, 1981. Principal Investigator.

South Central Reference and Research Council (Ithaca, NY). South Central Regional Delivery System, 1980. Principal Investigator.

Southern Tier Library System (Corning, NY). Newspapers on Microfilm in the Chemung-Southern Tier Library System, 1979-1981. Principal Investigator.

Cataloging & Bibliographic Database Building

Challenges, Choices, and Images K-12 Charter School, Denver Public Schools, 2007.

Denver Medical Library, Inc., 2006-2010.

Ricks Gifted and Talented School Library, 2005-

American Humane Society (Englewood), 2004-2006.

Fisher Early Learning Center Library, 2004-

Colorado Community Based Research Network (Denver), 2004-

Boulder Valley School District (Boulder), 2002-2003.

Douglas Public Library District (Castle Rock), 2001-2002.

Bibliographic Center for Research, Inc. (Denver). Original Cataloging, 2001-2003 & 1992-1993. Professional Cataloger. Libraries include Arapahoe Library District (Centennial); Clarke College (Clarke, IA); Kaiser Permanente Center for Health Research (Portland, KS); Douglas County Library System (Carson City, NV); Grinnell College (Grinnell, IA); Kansas State University (Manhattan, KS); Kansas State Library (Topeka, KS); McPherson College (McPherson, KS); Newman University (Wichita, KS); Montana Technical University (Helena, MT); Montana State Library (Helena, MT); University of Texas Southwest Medical Center Library (Dallas, TX); Community College of Southern Nevada (Las Vegas, NV); Pikes Peak Library District (Colorado Springs); Mesa Community College (Grand Junction); Coe College (Cedar Rapids, IA); Briar Cliff College (Sioux City, IA); Tri-Care Health Systems (Aurora); The Penrose-St. Francis Healthcare System (Colorado Springs); Westminster Public Library (Westminster); Lutheran Medical Center Medical Library (Wheat Ridge); American Heritage Center, University of Wyoming (Laramie, WY); National Wildlife Research Center Library (Lakewood); University of Colorado Health Sciences Center, Denison Memorial Library (Denver); Water Resources Library, Denver District Office, Bureau of Land Management (Lakewood); Mesa State Community College Learning Resources Center (Pueblo); Front Range Community College Learning Resources Center (Westminster).

Colorado Historical Society Library (Denver). Original Cataloging of Serials for Multi-Institutional Union Listing Project, 1993. Technical Services Associate. Institutional partners: Denver Art Museum, Denver Museum of Natural History Library, and Denver Botanical Gardens Library.

Arapahoe Library District (Centennial). Original Cataloging of Major Media, 1991.

Original Cataloging Projects: Davis and Elkins College (Elkins, WV), 1989-1990; Waldorf College (Forest City, IA), 1989-1990; Kennametal Corporation (Latrobe, PA), 1984-1985; Pennsylvania Public Libraries Film Center (Harrisburg), 1982-1985.

Retrospective Conversion Projects: North Central Regional Library Service (Mason City, IA), 1987-1988; Southeastern Library Services (Davenport, IA), 1986-1987; Virginia Theological Seminary (Alexandria), 1984-1985; California University of Pennsylvania (California, PA), 1984-1985; Kennametal Corporation (Latrobe, PA), 1984-1985; West Virginia University (Morgantown), 1983-1985; Altoona Area Public Library (Altoona, PA), 1983-1984; George Washington University (Washington, DC), 1983-1984; Indiana University of Pennsylvania (Indiana, PA), 1983-1985; Health Education Center (Pittsburgh), 1983-1984; Central Pennsylvania District Library Center (Bellefonte, PA), 1982-1985; Duquesne University Law School Library (Pittsburgh), 1982-1983; Allegheny County Law Library (Pittsburgh), 1982-1984; Calgon Technical Information Center (Pittsburgh), 1982; Dow Corning Corporation, Technical Information Center (Midland, MI), 1982-1983; Tri-System Public Library Retrospective Conversion Project (Binghamton, Corning, and Ithaca, NY), 1978-1981, Technical Project Director.

Updated December 2022