UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.;
SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

NETWORK-1 TECHNOLOGIES, INC.,
Patent Owner.

IPR2026-00114
Patent 11,233,780

DECLARATION OF DR. KARTHIKEYAN SUNDARESAN IN SUPPORT OF PATENT OWNER NETWORK-1'S PRELIMINARY RESPONSES

TABLE OF CONTENTS

I. Introduction 1

II. Professional Background and Qualifications 2

III. Relevant Time 4

IV. Level of Ordinary Skill in the Art 4

V. Materials Considered 5

VI. Claim Construction 6

VII. My Opinions Regarding Selected Issues 6

A. The Patents At Issue [EX1001] 6

B. The Prosecution Histories For The Patents At Issue [EX1004] 15

1. '893 Prosecution History 15

2. '780 Prosecution History 17

3. '094 Prosecution History 20

C. Petitioner's References and Grounds 22

1. Park [EX1005] 24

2. GlobalPlatform [EX1006] 26

3. AbiChar [EX1007] 29

4. X9.63-Overview [EX1008] 31

5. Nix175 [EX1016] 32

6. Petitioner's Other References (Haggerty [EX1012], Pierce [EX1013], Konstantinou [EX1014], and Weiss [EX1009]) 35

D. The Patent Office Allowed The Challenged Independent Claims After Considering All Of Petitioner's References And Petitioner Has Not Showed How The Office Erred 35

E. Petitioner's References Do Not Teach Or Suggest "Receiv[ing] … A Symmetric Key" And Deriving A Profile Key (All Patents) 37

F. Petitioner's References Do Not Teach Or Suggest "Decrypting … Using The Symmetric Key … The Subscriber Identity" ('893 Only) 42

G. A POSITA Would Not Combine The Park and GlobalPlatform References As The Petition Proposes (All Patents) 45

H. The Patents At Issue Are Entitled To Their Priority Dates (All Patents) ... 51

VIII. Declaration 54

APPENDIX A (RESUME) 56

EXHIBIT LIST

Exhibit	Description
EX2001	Complaint for Patent Infringement, *Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd., et al.*, EDTX-2-25-cv-00667, Dkt. 1 (June 27, 2025)
EX2002	Docket Control Order, *Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd., et al.*, EDTX-2-25-cv-00667, Dkt. 26 (Oct. 10, 2025)
EX2003	U.S. Patent No. 11,606,204
EX2004	U.S. Patent No. 11,973,864
EX2005	U.S. Patent No. 12,166,869
EX2006	U.S. Patent No. 11,233,780
EX2007	U.S. Patent No. 12,207,094
EX2008	U.S. Patent No. 11,916,893
EX2009	Google Patents Page for U.S. Patent No. 11,606,204, https://patents.google.com/patent/US11606204B2/en?oq=11606204 (accessed Jan. 13, 2026)
EX2010	Google Patents Page for U.S. Patent No. 11,233,780, https://patents.google.com/patent/US11233780B2/en?oq=11%2c233%2c780 (accessed Jan. 13, 2026)
EX2011	September 2, 2016 Rejection of Samsung Patent Application No. 14/803,946
EX2012	U.S. Patent Publication No. 2015/0163056
EX2013	U.S. Patent Publication No. 2015/0121066
EX2014	September 6, 2018 Notice of Allowance and Notice of References Cited for Samsung Patent Application No. 15/350,963
EX2015	U.S. Patent Publication No. 2015/0143125
EX2016	Defendants' Patent Local Rule 3-3 Disclosure of Invalidity Contentions, *Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd., et al.*, EDTX-2-25-cv-00667 (December 9, 2025)
EX2017	U.S. Patent No. 8,761,390

Exhibit	Description
EX2018	Declaration of Eric J. Enger in Support of Patent Owner's Discretionary Denial Brief
EX2019	Declaration of John Nix in Support of Patent Owner's Discretionary Denial Brief
EX2020	Email chain dated September 27, 2016, produced with Bates Nos. NWO_SAM_00013288–90
EX2021	Email chain dated December 21, 2016, produced with Bates No. NWO_SAM_00013295
EX2022	"Patent Portfolio for 'Embedded SIMs' and the 'Internet of Things,'" produced with Bates Nos. NWO_SAM_00013436–37
EX2023	Email chain dated January 3, 2017, produced with Bates Nos. NWO_SAM_00013296–97
EX2024	U.S. Patent Application No. 14/099,329
EX2025	U.S. Patent Publication No. 2014/0237101
EX2026	U.S. Patent Publication No. 2014/0219447
EX2027	3GPP TS 33.102 "3G security; security architecture," v10.0.0 (May 2011)
EX2028	3GPP TS 33.401 "Security architecture," v10.0.0 (March 2011)
EX2029	Declaration of Dr. Karthikeyan Sundaresan In Support of Patent Owner's Preliminary Responses
EX2030	U.S. Patent Application No. 14/084,141

I. Introduction

¶1. My name is Dr. Karthikeyan Sundaresan. I have been retained by Network-1 Technologies Inc. ("Patent Owner" or "Network-1") to provide my expert assessment and technical opinions in connection with the above captioned inter partes reviews of U.S. Patent Nos. 11,233,780 ("the '780 Patent"), 11,916,893 ("the '893 Patent"), and 12,207,094 ("the '094 Patent"). All three of those patents are related and share a common specification, and all three of the IPRs generally apply the same references in the same manner, so I have combined my opinions about those three patents into one declaration for submission in all three IPRs.

¶2. Specifically, I have been asked to provide my opinions regarding specific aspects of how a person of ordinary skill in the art ("POSITA") would understand certain teachings and aspects of the references Petitioners put forth vis-à-vis the three related patents at issue.

¶3. This declaration is based on information currently available to me. I reserve the right to expand, modify, or supplement my opinions if I become aware of evidence or information that was not available for review at the time I drafted this declaration.

¶4. Network-1 is paying me at a rate of $600 per hour plus expenses for my study and testimony in this case. This compensation is not contingent upon my

performance, the outcome of these IPRs, or any issues involved in or related to these IPRs.

II. Professional Background and Qualifications

¶5. I have attached my curriculum vitae ("CV") as Appendix A to this declaration. My CV includes a list of publications on which I am an author. It contains further details regarding my experience, education, and other qualifications. Nonetheless, I now expound upon my qualifications and professional background related to the field of wireless communications and related security protocols.

¶6. I am a Professor in the School of ECE, Georgia Tech. Prior to that, I spent fifteen years in wireless and telecom research at NEC Labs America, Princeton.

¶7. My research interests are broadly in wireless networking and mobile computing, and span both algorithm design as well as system prototyping. A good part of my research targets mobile cellular networks, starting with 4G and currently expanding into 6G, in which security of mobile networks and data sessions has been a topic of investigation.

¶8. I am the recipient of ACM Sigmobile's Rockstar award (2016) for my contributions to mobile computing and wireless networking. I have also received several best paper awards at prestigious ACM and IEEE conferences. I also received

a business contribution award for bringing research technology to commercialization at NEC.

¶9. I led the spin-out efforts of two innovative research technologies (NavigateIO Inc. and Wirinos Inc.) for infrastructure-free tracking of first responders in GPS-denied environments and sustainable product tracking in supply chains.

¶10. I have participated in various organizational and editorial roles for IEEE and ACM conferences and journals, and served as the program committee co-chair for ACM MobiCom'16. I am a Fellow of the National Academy of Inventors, Fellow of the IEEE, and an ACM distinguished member.

¶11. I am listed as an inventor/co-inventor on many patents and patent applications, as well as an author on numerous peer-reviewed conferences and journals in top-tier IEEE and ACM publications. The following list reflects some that are related to wireless communications and security:

Patent/Pub No.	**Title**	**Filed/Published**
10,296,394	Consistent Hashing	November 28, 2016
10,298,671	Design of Randomization Function and its Application in Load Balancing	November 1, 2016
10,331,493	Systems and Methods for Distributed Assignment of Task Identifiers	November 1, 2016
IEEE ICDCS	Securing Wireless Data Networks against Eavesdropping using Smart Antennas	June, 2008

III. Relevant Time

¶12. The three patents-at-issue in these IPRs each have an effective priority date of December 6, 2013 ("Effective Priority Date"). I am aware that the Petitioner has argued that each of these three patents are not entitled to that December 6, 2013 effective priority date, but rather has argued that: (a) the '780 Patent is only entitled to a June 26, 2019 priority date ('780 Pet. at 10); (b) the '893 Patent is only entitled to a December 10, 2021 filing date ('893 Pet. at 9); and (c) the '094 Patent is only entitled to a December 10, 2021 filing date ('094 Pet. at 10). I disagree for the reasons set forth below. Notwithstanding, only my opinions involving Nix175 would be affected based on the patents at issue having a later effective date; my opinions as to all other grounds and references would remain unchanged even if the patents at issue have a later effective date.

¶13. To the extent that I cite to exhibits created or published after the Effective Priority Date, I consider that the reference is still relevant to what a POSITA would have understood the point for which I cite the reference at or around the time of the invention.

IV. Level of Ordinary Skill in the Art

¶14. I understand that Petitioners have proposed that a person of ordinary skill in the art ("POSITA") for each of the three patents at issue "would have had at least a bachelor's degree in electrical engineering, computer engineering, computer

science, or a similar field, and 2-3 years of experience with cellular/WLAN security and mobile devices." '780 Pet. at 9; '893 Pet. at 9; '094 Pet. at 9. I understand that Patent Owner has not taken a position as to whether that level of ordinary skill is correct, but has reserved the right to propose its own definition in the future (if necessary).

¶15. It is my opinion that I would qualify as at least a person of ordinary skill in the art at the relevant time under Petitioners' description of a POSITA (and any other reasonable description), and that I exceed this level of knowledge, experience, and education so that I am qualified to provide an expert opinion in this proceeding.

¶16. I have approached my analysis from the perspective of a POSITA as of the Effective Priority Date. To the extent that I cite documents that were created after the Effective Priority Date, I have considered that their teachings are still instructive.

V. Materials Considered

¶17. In forming my opinions expressed herein, I have considered all the exhibits from each of the three IPRs, as well as my own education and experience. This includes the items listed in the exhibit list at the beginning of this declaration (Patent Owner's exhibits), as well as those listed in the exhibit list at the beginning of each Petition (Petitioner's exhibits).

VI. Claim Construction

¶18. I understand that claims are construed as per the understanding of a person of ordinary skill at the time of the invention after having read the patent specification and file history.

¶19. For purposes of these IPRs, I understand Petitioner has not asked for any claim term to be expressly construed (while reserving the right to seek different or narrower constructions in the parallel litigation). '780 Pet. at 11; '893 Pet. at 10; '094 Pet. at 10. So in my analysis, I did not expressly construe any claim term either. Rather, in my analysis, I have applied the plain and ordinary meaning of the claim terms. My opinions would not change under any reasonable claim construction of any claim term.

VII. My Opinions Regarding Selected Issues

¶20. I have been asked to provide opinions regarding a narrow range of issues in support of Patent Owner's Preliminary Responses, which I have been informed is limited to setting forth the reasons why no *inter partes* review should be instituted. If *inter partes* review is instituted, I may provide additional opinions and analysis regarding validity of the patents at issue.

A. The Patents At Issue [EX1001]

¶21. Each of the three patents at issue relate to provisioning and authenticating mobile devices that have an embedded subscriber identity module

("eSIM"). An eSIM may also be referred to as an embedded universal integrated circuit card ("eUICC"). *E.g.*, '893[1] at 19:31-33.

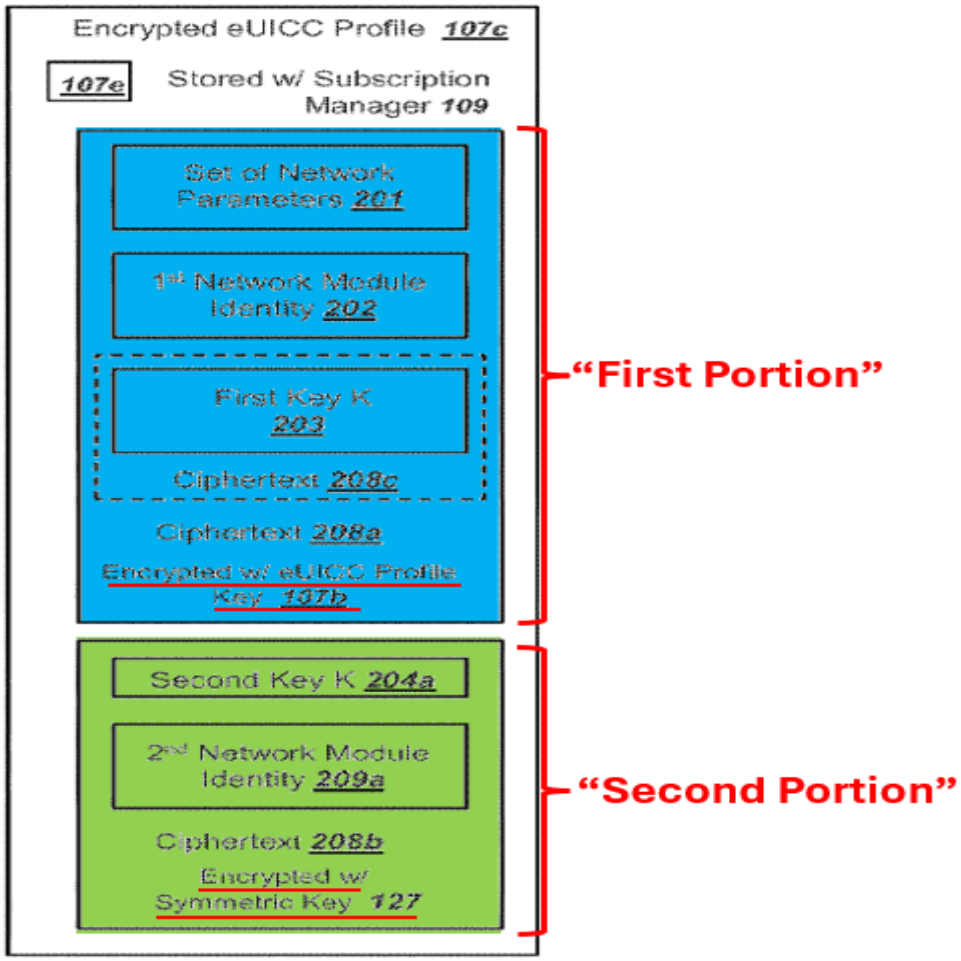
¶22. Before the patents at issue, mobile devices used a traditional SIM card, *i.e.*, a plastic-encased chip that was physically inserted into the mobile device and could be removed and replaced. '893 at 2:38-44. These traditional SIM cards were pre-loaded with various subscriber information for provisioning and authenticating the mobile device, including a set of parameters identifying the mobile device, information about the network that the mobile device should connect to, and a pre-shared secret key K. *Id.* at 2:45-55. But due to their physical nature, traditional SIM cards had many disadvantages that made them (1) unsuitable for devices in remote locations, (2) less convenient, (3) more costly, and (4) less secure. *Id.* at 2:64-3:15.

¶23. Due to the drawbacks with physical SIM cards, the industry began considering replacing them with eSIMs. '893 at 3:16-20. With eSIMs, the authentication hardware is permanently embedded within the mobile device and cannot be removed. However, eSIMs are not typically pre-loaded with the subscriber information for provisioning and authenticating the mobile device; rather, that profile information for the subscriber is electronically transferred to the eSIM. *See id.* at 3:34-4:41. The patents at issue provide a framework for securing that profile

[1] All the patents at issue share a common specification with the same text and figures. So while I typically cite to the '893 Patent, the citations apply equally to the corresponding portions of the '780 and '094 Patents.

information—especially in the context of a distributed network controlled by multiple different parties. *See id.* at 4:45-8:44.

¶24. The annotated excerpt from Figure 2a (below) illustrates the contents of the exemplary profile information—or encrypted eUICC Profile 107c—that is secured in the eSIM per the patents at issue. The encrypted eUICC profile includes two distinct portions: (1) a first portion (blue); and a second portion (green). '893 at 30:35-40. Importantly, as indicated by the red underlining below, the first portion is encrypted with an eUICC profile key 107b, while the second portion is encrypted with a different symmetric key 127. *Id.* at 11:52-56, 32:46-49. Thus, the first and second portions of the eUICC profile are encrypted differently, so that discovery of one of the keys does not yield the entirety of the profile information.



¶25. To decrypt the first portion, the eSIM derives the eUICC profile key 107b (using, *e.g.*, an Elliptic Curve Diffie-Hellman key exchange with a subscription manager), and then uses that eUICC profile key 107(b) with a deciphering algorithm on the first portion. '893 at 38:23-29, 34:42-57. To decrypt the second portion, the eSIM receives a separate symmetric key 127 and then uses it with a deciphering algorithm on the second portion to identify the network module identity 209a and the key K 204a. *Id.* at 36:56-58. At that point, the mobile device is provisioned and can successfully authenticate itself with the network. *Id.* at 36:58-60. This

approach—which uses *two different keys*, obtained in *two different ways*, to decrypt *two different portions* of the profile—increases security for both the user of the mobile device and the network operator. *Id.* at 35:35-38.

¶26. The independent claims of the patents at issue typify the approach discussed above. For example, '893 claim 1 recites a "mobile device" comprising an "eUICC" or eSIM. '893 at 80:22, 80:37. The eUICC is configured to receive an "eUICC profile" comprising a distinct "first portion" and a distinct "second portion." *Id.* at 80:42, 80:46, 80:48-49. To decrypt the first portion, the eUICC "derive[s] a profile key using an elliptic curve Diffie Hellman (ECDH) key exchange" and then uses it to decipher the first portion. *Id.* at 80:39-43. To decrypt the second portion, the eUICC "receive[s] the symmetric key" and then uses it to decipher the "key K and the subscriber identity" within that second portion. *Id.* at 80:44-48. Finally, the eUICC "generate[s] a response value for authentication of the mobile device with the wireless network using the key K." *Id.* at 80:50-52.

¶27. Here is '893 claim 1, highlighted to show (1) the first portion of the profile is decrypted using the *derived* profile key (blue) and (2) the second portion of the profile is decrypted using the *received* symmetric key (green):

> 1. A mobile device for communicating with a wireless network, the mobile device comprising:
> a first memory configured to store an embedded universal integrated circuit card (eUICC) identity;

a random number generator operably connected to a processor connected to a second memory configured to generate a random number for an eUICC private key corresponding to an eUICC public key;

a radio including one or more transmit antennas and one or more receiving antennas configured to:

a. transmit, to a subscription manager, the eUICC identity and the eUICC public key; and

b. ***receive***, from the subscription manager, i) an eUICC profile comprising network parameters, a key K, and a subscriber identity and ii) a symmetric key; and

an eUICC associated with the eUICC identity and configured to:

a. ***derive*** a profile key using an elliptic curve Diffie Hellman (ECDH) key exchange with the eUICC private key and a subscription manager public key;

b. decrypt a first portion of the eUICC profile using the profile key;

c. receive the symmetric key from a network application operating in the mobile device;

d. decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising the key K and the subscriber identity, wherein the first portion and the second portion are distinct; and

e. generate a response value for authentication of the mobile device with the wireless network using the key K.

'893 at 80:22-52 (emphasis and highlighting added).

¶28. The independent claims of the '780 and '094 Patents are virtually identical to one another (the '780 has apparatus claims, while the '094 has method claims), and they are both very similar to '893 independent claim 1. For example, I've highlighted '780 claim 1 to show (1) the first portion of the profile is decrypted using the *derived* profile key (blue) and (2) the second portion of the profile is decrypted using the *received* symmetric key (green):

> 1. An embedded universal integrated circuit card (eUICC) comprising:
> one or more processors; and
> a non-transitory computer-readable memory operatively connected to the one or more processors, the non-transitory computer-readable memory having stored thereon machine readable instructions that, when executed by the one or more processors cause the one or more processors to perform steps of:
> (a) generating a first message comprising:
> (1) an identity of the embedded universal integrated circuit card;
> (2) a nonce; and
> (3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key;
> (b) sending the first message via a network application to a subscription manager system;
> (c) deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms;

(d) storing a subscription manager public key which corresponds to a subscription manager private key;

(e) ***deriving*** a profile key using a key exchange algorithm based on at least:

(i) the second eUICC private key, and

(ii) the stored subscription manager public key,

wherein the profile key can also be derived at the subscription manager system based at least on:

(iii) the second eUICC public key, and

(iv) the subscription manager private key;

(f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;

(g) ***receiving*** the symmetric key;

(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;

(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and

(j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.

'780 at 80:18-62 (emphasis and highlighting added).

¶29. Likewise, I've highlighted '094 claim 1 to show (1) the first portion of the profile is decrypted using the *derived* profile key (blue) and (2) the second portion of the profile is decrypted using the *received* symmetric key (green):

1. A method comprising:

(a) generating a first message comprising:

(1) an identity of an embedded universal integrated circuit card (eUICC);

(2) a nonce; and

(3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key;

(b) sending the first message via a network application to a subscription manager system;

(c) deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms;

(d) storing a subscription manager public key which corresponds to a subscription manager private key;

(e) ***deriving*** a profile key using a key exchange algorithm based on at least:

(i) the second eUICC private key, and

(ii) the stored subscription manager public key, wherein the profile key can also be derived at the subscription manager system based at least on: the second eUICC public key, and the subscription manager private key;

(f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;

(g) ***receiving*** the symmetric key;

(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;

(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and

(j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.

'094 at 80:31-67 (emphasis and highlighting added).

B. The Prosecution Histories For The Patents At Issue [EX1004]

1. '893 Prosecution History

¶30. The application that resulted in the '893 Patent was filed on December 10, 2021; however, that application claimed priority to a string of other related applications dating back to December 6, 2013. '893 FH at 361-515. The '893 application had fifteen initial claims. *Id.* at 487-489.

¶31. On January 20, 2022, shortly after filing the '893 application, the applicant disclosed a number of references to the examiner, including all five of the references used by the Petition against '893 independent claim 1. '893 FH at 214-351. More specifically, at the very onset of prosecution, the applicant disclosed each of Park (*id.* at 341), GlobalPlatform (*id.* at 339), AbiChar (*id.* at 340), X9.63-Overview (*id.* at 350), and Nix175 (*id.* at 275). The examiner explicitly considered each of those five references. *Id.* at 169 (Park), *id.* at 167 (GlobalPlatform), *id.* at 168 (AbiChar), *id.* at 178 (X9.63-Overview), and *id.* at 148 (Nix175).

¶32. On March 27, 2023, the examiner rejected independent claim 1 under 35 U.S.C. §112, but did not issue any §§102(a)-(b) rejections for novelty or obviousness in light of the considered prior art. '893 FH at 117-123.

¶33. On September 19, 2023, the applicant and the examiner had an interview, during which they agreed on minor claim amendments (*e.g.*, explicitly adding a processor, memory, and transceiver) to overcome that §112 rejection. '893 FH at 113-116. A few days later, on September 27, 2023, the applicant amended independent claim 1 as agreed during the interview. *Id.* at 95. The applicant also added new dependent claims 16-17. *Id.* at 98.

¶34. The examiner allowed all the pending claims on October 18, 2023. '893 FH at 75-79. He stated that the '893 claims were allowable "since the prior arts taken individually or in combination fails to particularly disclose" all the claim limitations. *Id.* at 76.

¶35. In the reasons for allowance, the examiner specifically noted differences between the allowed claims and one prior art reference, U.S. Printed Patent Application No. 2014/0237101 to Park, which he referred to as a "Primary Reference." '893 FH at 77. Remarkably, the inventor of that "Primary Reference" patent application is the same person that authored the primary reference used in Samsung's petitions—Jaemin Park. *Compare* EX2025 at 1 *with* EX1005 at 1. But that is not where the similarities end; both Park references have similar disclosures.

That Park patent application teaches "securely provisioning various profiles" for an eUICC (EX2025 at [0085]), while the Park paper teaches a "secure profile provisioning architecture for eUICCs" (EX1005 at 1). And the examiner explicitly recognized that teaching from that Park patent application, noting it "discloses a method for managing a profile in an embedded UICC." '893 FH at 77.

¶36. Importantly, the examiner explained in the reasons for allowance that that Park patent application did not disclose a number of limitations from '893 claim 1, including: (1) "receiv[ing], from the subscription manager, … a symmetric key"; and (2) "decrypt[ing] … using the symmetric key … the subscriber identity." '893 FH at 77. As explained below, the Petition's references similarly fail to teach or suggest those same two claim limitations.

¶37. The '893 Patent issued on February 27, 2024. *See* '893 FH at 63.

2. '780 Prosecution History

¶38. The application that resulted in the '780 Patent was filed on June 26, 2019; however, that application claimed priority to a string of other related applications dating back to December 6, 2013. '780 FH at 3532-3688. The '780 application had twenty-two initial claims. *Id.* at 3658-3662.

¶39. On July 25, 2019, shortly after filing the '780 application, the applicant disclosed a number of references to the examiner, including *all five of the references used by the Petition against '780 independent claim 1*. '780 FH at 3475-3523. More

specifically, at the very onset of prosecution, the applicant disclosed each of Park (*id.* at 3520), GlobalPlatform (*id.* at 3485), AbiChar (*id.* at 3485), X9.63-Overview (*id.* at 3375), and Nix175 (*id.* at 3476). The examiner explicitly considered each of those five references. *Id.* at 3448 (Park), *id.* at 3469 (GlobalPlatform), *id.* at 3468 (AbiChar), *id.* at 3331 (X9.63-Overview), and *id.* at 3459 (Nix175).

¶40. On January 15, 2021, the examiner rejected all the claims for double patenting, as well as dependent claims 14 and 17 under 35 U.S.C. §112. '780 FH at 3406-3417. However, the examiner did not issue any §§102(a)-(b) rejections for novelty or obviousness in light of the considered prior art. *Id.* To the contrary, the examiner allowed independent claim 1 over the prior art of record. *Id.* at 3412.

¶41. In the reasons for allowance, the examiner specifically noted differences between the allowed claims and one prior art reference, U.S. Printed Patent Application No. 2014/0219447 to Park. '780 FH at 3412, 3414-3416. The inventor of that patent application is the same person that authored the primary reference used in Samsung's petitions—Jaemin Park. *Compare* EX2026 at 1 *with* EX1005 at 1. And both Park references have somewhat similar disclosures. That Park patent application teaches "securely provisioning various profiles" for an eUICC (EX2026 at [0011]), while the Park paper teaches a "secure profile provisioning architecture for eUICCs" (EX1005 at 1). And the examiner explicitly recognized that teaching from that Park patent application, noting it "discloses a

method wherein an [mobile network operator] receives a secret key allocated to a corresponding embedded UICC (eUICC) through SM-SR (secure routing) in an environment where [the subscription manager] is divided and implemented as SM-SR and SM-DP (data preparation)." '780 FH at 3414.

¶42. On March 18, 2021, the applicant submitted a terminal disclaimer to overcome the double patenting rejection and cancelled dependent claims 14 and 17 to overcome the §112 rejection. '780 FH at 3393-3403.

¶43. On June 29, 2021, the examiner issued a formal notice of allowance. '780 FH at 3311-3318. In that notice, the examiner incorporated the prior reasons for allowance from the January 15, 2021 office action. *Id.* at 3317.

¶44. On August 5, 2021, the applicant disclosed additional references, including numerous patents and co-pending applications filed by the inventor, John Nix. In light of these disclosures, the applicant requested continued examination. '780 FH at 96-3310.

¶45. On August 20, 2021, after considering those additional references, the examiner issued another formal notice of allowance that, again, incorporated the prior reasons for allowance from the earlier office action. '780 FH at 56-59.

¶46. On August 25, the applicant disclosed a final reference and requested continued examination. '780 FH at 38-49.

¶47. Finally, on September 14, 2021, after considering that final reference, the examiner issued yet another formal notice of allowance that, once again, incorporated the prior reasons for allowance from the earlier office action. '780 FH at 12-15.

¶48. The '780 Patent issued on January 25, 2022. '780 FH at 1.

3. '094 Prosecution History

¶49. The application that resulted in the '094 Patent was filed on January 18, 2024; however, that application claimed priority to a string of other related applications dating back to December 6, 2013. '094 FH at 491-630. The '780 application had twenty-two initial claims. *Id.* at 620-623.

¶50. On April 9, 2024, shortly after filing the '094 application, the applicant disclosed a number of references to the examiner, including *all five of the references used by the Petition against '094 independent claim 1*. '094 FH at 241-318. More specifically, at the very onset of prosecution, the applicant disclosed each of Park (*id.* at 292), GlobalPlatform (*id.* at 290), AbiChar (*id.* at 291), X9.63-Overview (*id.* at 310), and Nix175 (*id.* at 252). The examiner explicitly considered each of those five references. *Id.* at 202 (Park), *id.* at 200 (GlobalPlatform), *id.* at 201 (AbiChar), *id.* at 229 (X9.63-Overview), and *id.* at 174 (Nix175).

¶51. On September 18, 2024, the examiner rejected all the claims for double patenting and under 35 U.S.C. §112 (for failing to explicitly define "eUICC"). '094

FH at 130-140. However, the examiner did not issue any §§102(a)-(b) rejections for novelty or obviousness in light of the considered prior art. *Id.* To the contrary, the examiner allowed independent claim 1 over the prior art of record. *Id.* at 135.

¶52. In the reasons for allowance, the examiner specifically noted differences between the allowed claims and one prior art reference, U.S. Printed Patent Application No. 2014/0219447 to Park. '094 FH at 135, 137-139. The inventor of that patent application is the same person that authored the primary reference used in Samsung's petitions—Jaemin Park. *Compare* EX2026 at 1 *with* EX1005 at 1. And both Park references have somewhat similar disclosures. That Park patent application teaches "securely provisioning various profiles" for an eUICC (EX2026 at [0011]), while the Park paper teaches a "secure profile provisioning architecture for eUICCs" (EX1005 at 1). And the examiner explicitly recognized that teaching from that Park patent application, noting it "discloses a method wherein an [mobile network operator] receives a secret key allocated to a corresponding embedded UICC (eUICC) through SM-SR (secure routing) in an environment where [the subscription manager] is divided and implemented as SM-SR and SM-DP (data preparation)." '094 FH at 137.

¶53. On November 4, 2024, the applicant submitted a terminal disclaimer to overcome the double patenting rejection and amended claim 1 to define "eUICC" and overcome the §112 rejection. '094 FH at 110-120.

¶54. On December 3, 2024, the examiner issued a formal notice of allowance. '094 FH at 74-77. In that notice, the examiner incorporated the prior reasons for allowance from the September 18, 2024 office action. *Id.* at 76.

¶55. The '094 Patent issued on January 21, 2025. '094 FH at 63.

C. Petitioner's References and Grounds

¶56. The three petitions assert numerous grounds of invalidity based on combinations of various references. However, with respect to the independent claims of the patents at issue (*i.e.*, '893 claim 1, '780 claim 1, and '094 claim 1), each of the three petitions apply the same five references: (1) Park; (2) GlobalPlatform; (3) AbiChar; (4) X9.63-Overview; and (5) Nix175. The petitions further apply additional references for some of the dependent claims. For completeness, I list below all the grounds in each of the three petitions.

¶57. This table summarizes the grounds asserted against the '893 Patent:

Ground	**Claims**	**Statute**	**References**
1	1, 3, 6-11, 13-17	§103	Park + GlobalPlatform + AbiChar
2	1, 3, 6-11, 13-17	§103	Park + GlobalPlatform + X9.63-Overview
3	2, 12	§103	Park + GlobalPlatform + AbiChar + Haggerty <u>OR</u> Park + GlobalPlatform + X9.63-Overview + Haggerty
4	4-5	§103	Park + GlobalPlatform + AbiChar + Pierce <u>OR</u>

			Park + GlobalPlatform + X9.63-Overview + Pierce
5	10-11	§103	Park + GlobalPlatform + AbiChar + Konstantinou OR Park + GlobalPlatform + X9.63-Overview + Konstantinou
6	1-17	§103	Nix175 + Park + GlobalPlatform

'893 Pet. at 3. None of those references, either alone or in combination, teach or suggest all the elements of challenged '893 independent claim 1.

¶58. This table summarizes the grounds asserted against the '780 Patent:

Ground	Claims	Statute	References
1	1-15, 17-20	§103	Park + GlobalPlatform + AbiChar
2	1-15, 17-20	§103	Park + GlobalPlatform + X9.63-Overview
3	16	§103	Park + GlobalPlatform + AbiChar + Weiss
4	16	§103	Park + GlobalPlatform + X9.63-Overview + Weiss
5	1-20	§103	Nix175 + Park + GlobalPlatform

'780 Pet. at 3. None of those references, either alone or in combination, teach or suggest all the elements of challenged '780 independent claim 1.

¶59. This table summarizes the grounds asserted against the '094 Patent:

Ground	Claims	Statute	References
1	1-17, 19-22	§103	Park + GlobalPlatform + AbiChar
2	1-17, 19-22	§103	Park + GlobalPlatform + X9.63-Overview
3	18	§103	Park + GlobalPlatform + AbiChar + Weiss

4	18	§103	Park + GlobalPlatform + X9.63-Overview + Weiss
5	1-22	§103	Nix175 + Park + GlobalPlatform

'094 Pet. at 3. None of those references, either alone or in combination, teach or suggest all the elements of challenged '094 independent claim 1.

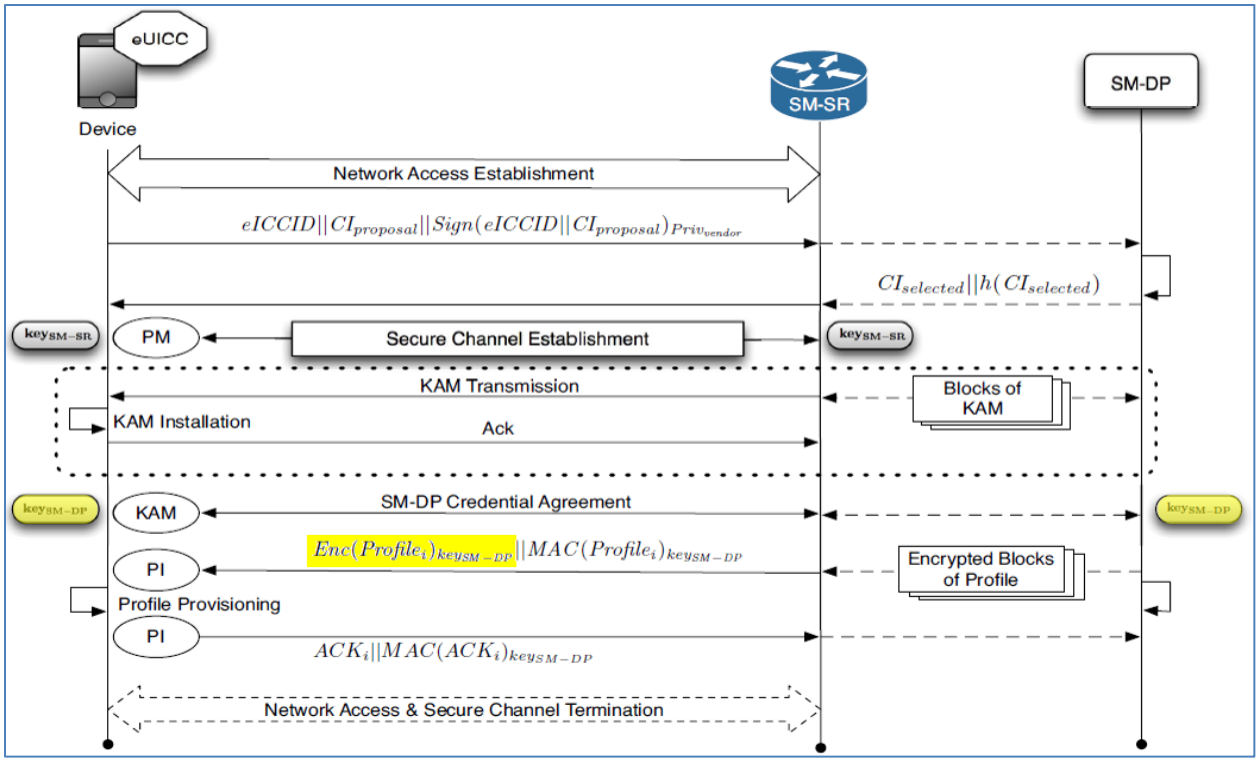
1. Park [EX1005]

¶60. Park, EX1005 (in all three petitions), is a paper titled "Secure Profile Provisioning Architecture for Embedded UICC" authored in 2013 by Jaemin Park *et al*. EX1005 at 1. Park addresses the security challenges of remotely provisioning profiles onto eUICCs. *Id.* According to Park, because no single mobile network operator ("MNO") controlled an eUICC, a new component called the Subscription Manager ("SM") was introduced, divided into two entities: (1) a data preparation entity ("SM-DP") that generates profiles; and (2) a secure routing entity ("SM-SR") that transports profiles to the eUICC. *Id.* However, since profiles often contain sensitive information, this new ecosystem raised security concerns. *Id.*

¶61. To combat those security concerns, Park proposes a Secure Profile Provisioning Architecture ("SPA") that has two phases. EX1005 at 3. In the first pre-provisioning phase, the eUICC vendor installs SM-SR credentials into the eUICC and registers the eUICC's capability information (*e.g.*, supported cryptographic algorithms, key agreement protocols) with a certification center. *Id.* In the second

secure profile provisioning phase, the eUICC connects to SM-SR and sends its ID and capability information signed by the eUICC vendor's key. *Id.* at 4. The SM-DP verifies this signature using the eUICC vendor's certificate obtained from the eUICC Certification Center. *Id.* The SM-DP then selects appropriate cryptographic protocols based on the eUICC's reported capabilities and communicates the selected parameters back to the eUICC. *Id.* A new internal eUICC module called the Key Agreement Module ("KAM") dynamically performs a key agreement with SM-DP to generate fresh SM-DP credentials on demand. *Id.* SM-DP then encrypts the entire profile using those credentials and transmits them through SM-SR's secure channel to the eUICC. *Id.* Finally, the eUICC's profile installer decrypts, verifies, and installs the profile, and then sends acknowledgments back to the SM-DP. *Id.*

¶62. Figure 4 illustrates Park's profile provisioning procedure, discussed above. Notably, as illustrated by the yellow highlighting, Park teaches for both the mobile device and the SM-DP to separately <u>*derive*</u> the profile key, $key_{SM\text{-}DP}$, and then use it to encrypt/decrypt the <u>*entirety*</u> of the profile, $Enc(Profile_i)key_{SM\text{-}DP}$:



EX1005 at 4-5 (highlighting added).

¶63. Notably, Park is silent about key aspects of the independent claims from the three patents at issue, including: (1) a profile with two distinct portions, each of which is decrypted using a different key obtained in a different way; (2) using an elliptic curve Diffie Hellman key exchange to derive a profile key; (3) decrypting the subscriber identity from within the second portion using the received symmetric key; and (4) generating a first message comprising a nonce.

2. GlobalPlatform [EX1006]

¶64. GlobalPlatform, EX1006 (in all three petitions), is document titled "Card Specification, version 2.2.1" issued by the GlobalPlatform standards

organization and dated January 2011. EX1006 at 1.[2] GlobalPlatform defines a standardized architecture for smart card security, including secure channel protocols designed to protect communications between a card and an off-card entity. *Id.* at 39-40, 48, 132. One of those secure channel protocols is called "SCP10." *See id.* at 254.

¶65. For confidentiality, GlobalPlatform mostly relies on use of a secure channel encryption key ("C-ENC") to encrypt message data transmitted to and from the card. EX1006 at 278-279. In addition, SCP10 also imposes an additional level of protection for particularly sensitive data (*i.e.*, keys) transmitted to the card; the sensitive key data can be first encrypted with a symmetric Data Encryption Key ("DEK") and then the entire message—including the already-encrypted sensitive key data—is further encrypted using the C-ENC key. *See id.* at 284. Thus, SCP10 utilizes two-levels of nested encryption for particularly sensitive key data included within the message data.

¶66. GlobalPlatform's SCP10 teaches two alternative and mutually-exclusive methods by which the card can obtain these keys: (1) the key agreement method; and (2) the key transport method. EX1006 at 255. With (1) the key agreement method, the card and the off-card entity initially exchange secret values

[2] Citations in EX1006 are to the bates numbering (bottom right) and not to the internal page numbering (top right) as in the Petition.

and then subsequently use those secrets to compute and *derive* the keys. *Id.* With (2) the key transport method, the card *receives* the keys from the off-card entity and does not have to compute them. *Id.* To select which of the two methods will be used for the session, GlobalPlatform teaches to set the first bit, b1, of a parameter in the card recognition data to "1" if the key agreement method will be used and "0" if the key transport method will be used. *Id.* at 255, 300-302. Thus, it is impossible within a given session for a card to both derive one key (*e.g.*, C-ENC) and receive another key (*e.g.*, DEK). Table F-1 and its corresponding text confirm as much:

Key transport and key agreement relate to the process of establishing session keys for the Secure Channel Session.

- With **key agreement** the Security Domain and the Off-Card Entity exchange secret values when the Secure Channel is being initiated, and session keys are then derived from those secrets using an algorithm known to both the Off-Card Entity and the Security Domain;
- With **key transport** the Security Domain receives session keys to be used for the Secure Channel Session from the Off-Card Entity during Secure Channel initiation.

b8	b7	b6	b5	b4	b3	b2	b1	Description
Not available	0	0	0	0	0	-	0	Key Transport
Not available	0	0	0	0	0	-	1	Key Agreement
Not available	0	0	0	0	0	0	-	Signature with message recovery
Not available	0	0	0	0	0	1	-	Signature without message recovery

Table F-1: Values of Parameter "i"

Id. at 255 (highlighting added).

¶67. GlobalPlatform fails to teach key parts of the independent claims from the patents at issue, including: (1) both deriving a profile key *and* receiving a symmetric key at the mobile device/eUICC; (2) decrypting a subscriber identity

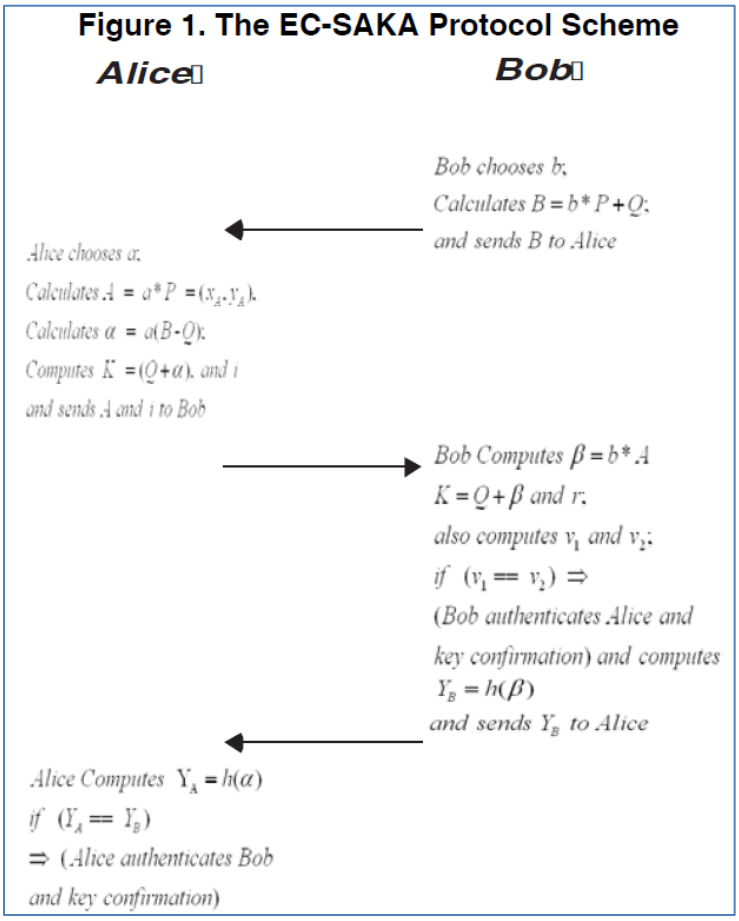
using the symmetric key; and (3) using an elliptic curve Diffie Hellman key exchange to derive a profile key with a subscription manager.

3. AbiChar [EX1007]

¶68. AbiChar, EX1007 (in all three petitions), is a paper titled "A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications" authored in 2007 by Pierre Abi-Char *et al*. EX1007 at 1. To provide secure communication for mobile devices, AbiChar presents "a fast and secure authenticated key agreement protocol based on elliptic curve cryptography" called "EC-SAKA." *Id.* EC-SAKA is a three-pass authenticated key establishment protocol designed for low-power mobile wireless devices. *Id.*

¶69. Figure 1 (below) illustrates the EC-SAKA protocol scheme. As can be seen, the EC-SAKA protocol consists of three message flows between a client (Alice) and a server (Bob). EX1007 at 3. In the setup phase, Alice selects an elliptic curve $E(Z_p)$, chooses a random base point P of prime order n, and derives a public parameter $Q = h(pw) * P$ from her password pw, then transfers the parameters (E, Q, P, n) to Bob securely. *Id.* In the first flow, Bob chooses a random challenge b and sends $B = b * P + Q$ to Alice. *Id.* In the second flow, Alice chooses a random challenge a, computes $A = a * P$, derives a shared value $\alpha = a(B - Q)$, computes the shared key $K = Q + \alpha$, and generates an ElGamal signature (A, i) which she sends to Bob. *Id.* And in the third flow, Bob verifies Alice's signature and computes $\beta = b *$

A, deriving the same shared key $K = Q + \beta$. *Id.* Upon verification, both parties derive the final session key $K_s = h(ID(Alice) \| ID(Bob) \| K)$. *Id.* at 3-4.

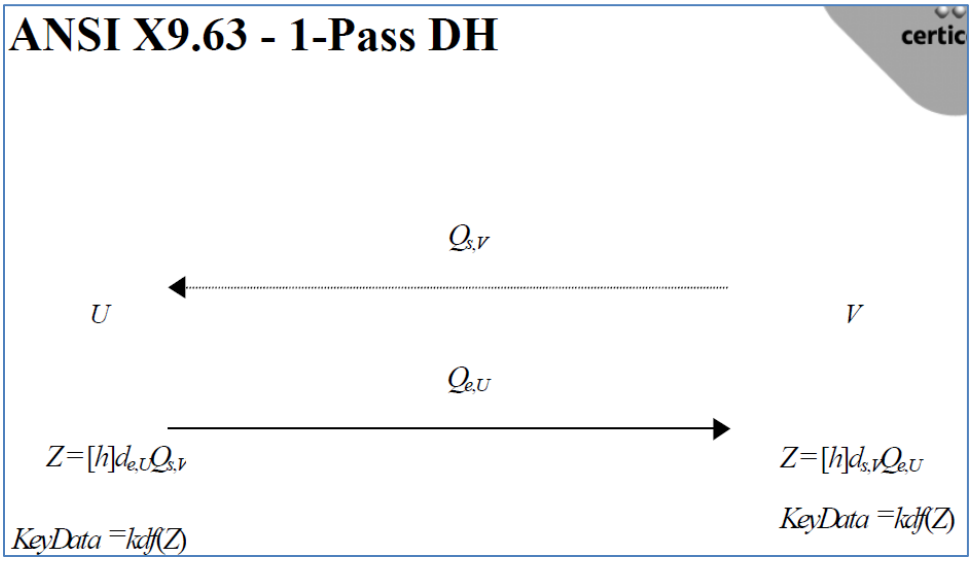


AbiChar fails to teach many components of the independent claims of the patents at issue, including: (1) a profile with two distinct portions, each of which is decrypted using a different key obtained in a different way; (2) receiving the symmetric key at the mobile device/eUICC; (3) decrypting a subscriber identity using the symmetric key; and generating a first message comprising a nonce.

4. X9.63-Overview [EX1008]

¶70. X9.63-Overview, EX1008 (in all three petitions), is a presentation titled "ANSI X9.63 Overview: Key Agreement and Key Transport Using Elliptic Curve Cryptography" authored in 2007 by Simon Blake-Wilson. EX1008 at 1. It provides a summary of the ANSI X9.63 standard then being developed by the ANSI X9F1 committee. *Id.* at 3. It "specifies key agreement and key transport schemes using elliptic curve cryptography." *Id.*

¶71. One of those schemes is the one-pass Diffie-Hellman scheme, which AbiChar refers to as "1-Pass DH":



EX1008 at 12. In the one-pass Diffie Hellman scheme, an entity randomly generates an ephemeral private key, computes a corresponding public key, and transmits that public key to a remote party so that both sides can derive a shared symmetric key. *Id.* at 7, 12. More specifically, one entity (*U*) generates a fresh ephemeral key pair

by randomly selecting an ephemeral private key ($d_{e,U}$) and computing a corresponding ephemeral public key ($Q_{e,U}$). *Id.* at 7, 12. Entity *U* sends its ephemeral public key to the other party (*V*), and both entities compute a shared secret (*Z*) using their respective private keys and the public key received from the other party. *Id.* at 12. That shared secret is then passed through the key derivation function (*kdf*) to produce shared keying material (*KeyData*). *Id.*

¶72. X9.63-Overview fails to teach many key components of the independent claims of the patents at issue, including: (1) a profile with two distinct portions, each of which is decrypted using a different key obtained in a different way; (2) receiving the symmetric key at the mobile device/eUICC; (3) decrypting a subscriber identity using the symmetric key; and generating a first message comprising a nonce.

5. Nix175 [EX1016]

¶73. Nix175, EX1016 (in all three petitions), is a U.S. Patent titled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication" filed on December 6, 2013 by John Nix. EX1016 at 1. Each of the three patents at issue are continuations of Nix175; they all share the same specification and each of the patents at issue claims priority to Nix175. *Compare* '893 Patent, '780 Patent, and '094 Patent *with* EX1016. Nix175 is not prior art to any of the patents at issue, as explained below.

¶74. For various reasons, Samsung concedes that Nix175 is only prior art if the three patents at issue are not entitled to their priority claims. '893 Pet. at 19; '780 Pet. at 18; '094 Pet. at 18.

¶75. First, with respect to the '893 Patent, the '780 Patent, and the '094 Patent, Samsung alleges that none of those three patents are entitled to claim priority to Nix175 because those patents either: (a) explicitly claim "receiv[ing] from the subscription manager, … a symmetric key" ('893 Pet. at 9-10); or (b) place no limit on the source of the claimed "symmetric key" so the claims are broad enough to cover receiving the symmetric key from the subscription manager ('780 Pet. at 9-10, '094 Pet. at 9-10), which Nix175 allegedly does not support. However, Nix175 explicitly discloses receiving the symmetric key 127 from mobile network operator 104. EX1016 at 57:56-61, Fig 3 at step 309. And Nix175 also teaches that the "mobile network operator 104 could operate the eUICC subscription manager 109." *Id.* at 11:1-3; *see also id.* at 36:33-34 ("the MNO 104 could also function as a eUICC subscription manager 109"). Thus, because Nix175 teaches the mobile network operator and the subscription manager can be the same, Nix175 also discloses receiving a symmetric key from a subscription manager—thereby providing written description support for the claims of the patents at issue.

¶76. Second, with respect to the '780 Patent and the '094 Patent (but not the '893 Patent), Samsung alleges that neither of those two patents are entitled to claim

priority to Nix175 because those patents claim both a "first eUICC public key" and a "second eUICC public key," but Nix175 allegedly only discloses one eUICC private/public key pair. '780 Pet. at 9, '094 Pet. at 9. This is wrong. Nix175 teaches two key pairs: (i) one pair for generating a digital signature used in authenticating; and (ii) another pair for deriving a profile key used in decryption. Nix175 describes the first key pair at, *e.g.*, 47:17, 54-55 (a first instance of eUICC private key 215 is stored on module 101 within the mobile device and a first instance of eUICC public key 214 is stored on subscription manager 109). This first key pair is used to generate a digital signature that is sent in a first message from the eUICC to the subscription manager. Nix175 at 48:65-49:6. The subscription manager then uses this digital signature to authenticate the eUICC. *Id.* at 49:15-19. Nix175 describes the second key pair at, *e.g.*, 51:65-52:2 (a second instance of eUICC public key 214 and eUICC private key 215). This second key pair is derived using Elliptic Curve Cryptography (ECC) algorithms and a random number generator. *Id.* Then this second key pair is subsequently used with other information to derive a profile key used to decrypt a portion of the eUICC profile. *Id.* at 52:24-32. Thus, because Nix175 teaches two eUICC public/private key pairs, Nix175 provides written description support for the '780 and '094 patent claims.

¶77. In sum, each of the patents at issue are entitled to their earliest December 6, 2013 priority date, and Nix175 is not prior art.

6. Petitioner's Other References (Haggerty [EX1012], Pierce [EX1013], Konstantinou [EX1014], and Weiss [EX1009])

The petitions cumulatively rely on four other references—Haggerty (EX1012), Pierce (EX1013), Konstantinou (EX1014), and Weiss (EX1009)—just to invalidate certain dependent claims. But since I only address the independent claims of the patents at issue in this declaration, I reserve the right to explain those four references in the future (if necessary).

D. The Patent Office Allowed The Challenged Independent Claims After Considering All Of Petitioner's References And Petitioner Has Not Showed How The Office Erred

¶78. With respect to the independent claims of the patents at issue, Samsung asserts combinations of five references—*all of which were considered during prosecution of the respective patents*. As explained above in §VII(B), the applicant disclosed and the examiner explicitly contemplated each of Park, GlobalPlatform, AbiChar, X9.63-Overview, and Nix175. Yet even after considering each of those references, the examiner determined that the independent claims were allowable.

¶79. The examiner specifically noted differences between the independent claims of the patents at issue and two patent applications: (1) U.S. Printed Patent Application No. 2014/0237101 to Park (in the '893 prosecution); and (2) U.S. Printed Patent Application No. 2014/0219447 to Park (in the '780 and '094 prosecutions). *See supra* at §VII(B). Those Park patent applications from the prosecution histories, EX2025 and EX2026, have the same inventor and a similar

disclosure to Samsung's primary Park paper from the Petitions, EX1005. *Compare* EX2025 *and* EX2026 *with* EX1005. For example, the Park patent applications teach "securely provisioning various profiles" for an eUICC (EX2025 at [0085], EX2026 at [0011]), while the Park paper teaches a "secure profile provisioning architecture for eUICCs" (EX1005 at 1). And the examiner appreciated those teachings from the Park patent applications, stating in the '893 prosecution that one "discloses a method for managing a profile in an embedded UICC, and more particularly, to a method for managing a profile in an embedded UICC that enables management information on the profile provided within the embedded UICC to play an essential role for providing communication and additional services, to be provided to a device existing outside the embedded UICC." '893 FH at 77. And in the '780 and '094 prosecutions, the examiner stated that another Park patent application "discloses a method wherein an [mobile network operator] receives a secret key allocated to a corresponding embedded UICC (eUICC) through SM-SR (secure routing) in an environment where [the subscription manager] is divided and implemented as SM-SR and SM-DP (data preparation)." '780 FH at 3414; '094 FH at 137.

¶80. Notwithstanding the above, none of the three Petitions explain how the Patent Office erred in applying that considered prior art and allowing the independent claims of the patents at issue.

E. Petitioner's References Do Not Teach Or Suggest "Receiv[ing] … A Symmetric Key" And Deriving A Profile Key (All Patents)

¶81. The independent claims of the patents at issue all require both "receiving" a "symmetric key" and "deriving" a "profile key." '893 at 80:30-41; '780 at 80:42-43, 53; '094 at 80:47, 58. That aspect of the independent claims is not satisfied—or even suggested—by the combination of Park, GlobalPlatform and AbiChar or the combination of Park, GlobalPlatform and X9.63-Overview. None of those references, alone or in combination, discloses or suggests *receiving* a symmetric key and also *deriving* a profile key.

(a) The Patents At Issue Require Both Receiving A Symmetric Key <u>And</u> Deriving A Profile Key.

¶82. The plain language of the various independent claim 1s is clear that two different keys must be obtained using two different methods. First, the devices must *receive*—as an incoming transmission from an external entity—a symmetric key. '893 at 80:30-36; '780 at 80:53; '094 at 80:58. This is not a key that is locally derived or computed amongst two parties through a mutual protocol. Rather, it is a key that one party sends and the other party *receives*.

¶83. Second, the various claim 1's also separately require *deriving* a profile key using a key exchange algorithm (such as elliptic curve Diffie Hellman). '893 at 80:39-41; '780 at 80:42-43; '094 at 80:47-48. This profile key is obtained very differently than the symmetric key discussed above; the various independent claims

are clear that the profile key is *derived* (*i.e.*, calculated from various information), and not simply received like the symmetric key.

¶84. The patent specifications also confirm there is a difference in how the two claimed keys are obtained. The symmetric key is one that originates externally and is *received* by the mobile device. *See e.g.*, '893 at 36:56-58 ("the module can receive a symmetric key 127 to decrypt the second key K 204a"); *see also id*. at 6:38-40. On the other hand, the profile key is one that is *derived* using other information according to, *e.g.*, an elliptic curve Diffie Hellman key exchange. *Id.* at 53:27-60.

¶85. Thus, one important aspect of the challenged independent claims is that the symmetric key and the profile key are obtained via different methods to increase security. One of those keys (the symmetric key) is received by the mobile device as part of an encrypted communication, while the other key (the profile key) is derived at the mobile device using ECDH cryptographic parameters and algorithms.

(b) Park Does Not Teach Transmission of Any Symmetric Key To A Mobile Device.

¶86. Park's Secure Profile Provisioning Architecture ("SPA") does not disclose a subscription manager that transmits a symmetric key to the eUICC. Rather, Park describes a two-entity Subscription Manager architecture—SM-SR (Secure Routing) for transporting the encrypted profile, and SM-DP (Data Preparation) for generating and encrypting it. EX1005 at 1-2. And in Park's key agreement framework, the SM-DP and the eUICC establish a shared session key—

Park's *keySM-DP*—through an asymmetric key agreement protocol housed in the eUICC's Key Agreement Module ("KAM"). *Id.* at 4-5. The result is that each side independently derives *keySM-DP* through the key exchange; neither side transmits *keySM-DP* to the other. *Id.* at 4. By design, *keySM-DP* is a mutually derived key, not a received one.

¶87. Park teaches no additional, separate symmetric key that is generated by the SM-DP and then transmitted to the eUICC. And while Park's profile is encrypted with *keySM-DP* and that profile is subsequently sent over the secure channel—the *keySM-DP* itself is never transmitted; it is independently computed at each endpoint. EX1005 at 4-7. There is no step in Park's protocol in which the subscription manager transmits a symmetric key to the eUICC, where it is received.

(c) GlobalPlatform Teaches Two Mutually-Exclusive Methods For Obtaining Session Keys; It Does Not Teach Mixing Those Methods Within a Session.

¶88. Recognizing the deficiencies in Park, Samsung alleges that GlobalPlatform's Data Encryption Key ("DEK") is the claimed "symmetric key" that is received using GlobalPlatform's key transport option. '893 Pet. at 40, 57; '780 Pet. at 41-42, 59-60; '094. Pet at 41-42, 60. However, Samsung fails to note that the key transport option is just one of two mutually-exclusive ways by which the card can obtain session keys. *Id.* More specifically, GlobalPlatform teaches using either (1) a key transport option, where the card <u>*receives*</u> session keys from an off-

card entity or (2) a key agreement option, where the card and the off-card entity exchange secret values and then *derive* the session keys using an algorithm. EX1006 at 255.

¶89. Importantly, the two options cannot be used together; rather, for any given session, either the key transport option is used OR the key agreement option is used (but not both). EX1006 at 255. This is clear because GlobalPlatform teaches that the choice to use either the key transport option or the key agreement option is recorded as a single bit in a parameter within the card recognition and security domain management data. *Id.* If the key transport option is selected, then the first bit is a "0." Alternatively, if the key agreement option is selected, then the first bit is a "1." *Id.* Table F1 illustrates this protocol:

b8	b7	b6	b5	b4	b3	b2	b1	Description
Not available	0	0	0	0	0	-	0	Key Transport
Not available	0	0	0	0	0	-	1	Key Agreement
Not available	0	0	0	0	0	0	-	Signature with message recovery
Not available	0	0	0	0	0	1	-	Signature without message recovery

Table F-1: Values of Parameter "i"

Id. (highlighting added); *see also id.* at 301-302.

¶90. This is significant because, for purposes of the claimed "deriv[ing] a profile key" limitation, Samsung alleges the eUICC would derive the session key using its private key and the subscription manager public key (*i.e.*, the key agreement option is selected). *See* '893 Pet. at 42; '780 Pet. at 37-38; '094 Pet. at 37-38. But

that necessarily means that the GlobalPlatform's key transport option cannot be selected. *See supra.*

¶91. Thus, GlobalPlatform cannot teach or suggest the claimed "receiv[ing] a symmetric key" and deriving a profile key.

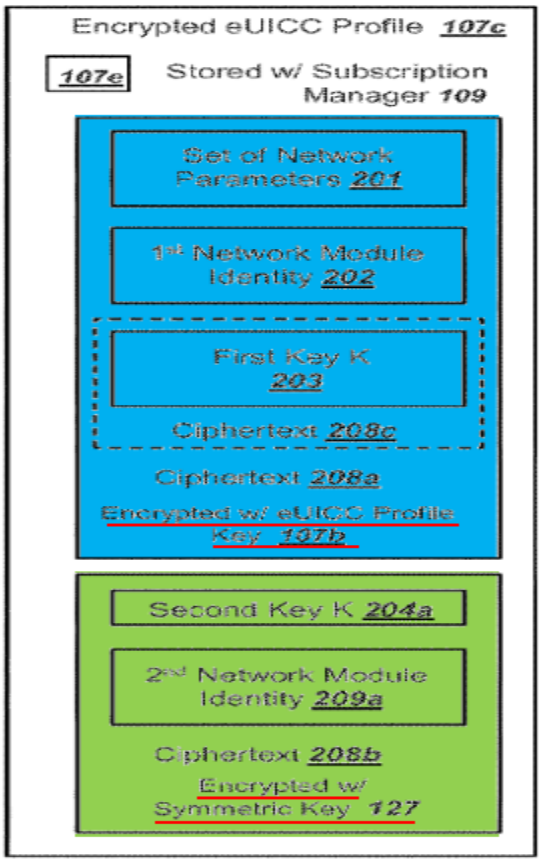
(d) AbiChar and X9.63-Overview Do Not Cure These Deficiencies

¶92. Lastly, neither AbiChar (Ground 1) nor X9.63-Overview (Ground 2) fills the gaps left by Park and GlobalPlatform. Both references merely describe ECDH and elliptic curve key exchange protocols. EX1007, EX1008. And as Petitioner's own mapping confirms, these references are relied upon only to supply the ECDH algorithm used to <u>*derive*</u> Park's *keySM-DP* (*i.e.*, the claimed "profile key" in claim 1). '893 Pet. at 41–45, 57–61; '780 Pet. at 35-38, 60-64; '094 Pet. at 34-38, 60-64. Neither AbiChar nor X9.63-Overview teaches or suggests a mobile device receiving a symmetric key from another entity, as claimed. Rather, Abi-Char's and X9.63-Overview's ECDH key exchange, by its very nature, produces a shared key through mutual derivation without transmitting the key itself. The ECDH-derived session key is <u>*not*</u> a symmetric key that is <u>*received*</u> from another party; it is one that each party independently computes. AbiChar and X9.63-Overview thus directly reinforce the opposite of what the independent claims of the patents at issue require.

F. Petitioner's References Do Not Teach Or Suggest "Decrypting … Using The Symmetric Key … The Subscriber Identity" ('893 Only)

¶93. Claim 1 of the '893 Patent also requires that the eUICC within the mobile device be configured to "decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising [] the subscriber identity." '893 at 80:46-48.

¶94. The '893 specification (including annotated Figure 2a below) similarly explains that the eUICC profile contains a second portion 208b (green) that includes a second network module identity 209a. EX1001 at 32:44-46. And the eUICC can decrypt the second network module identity 209 using the symmetric key. *Id.* at 60:38-43.



Id. at Fig. 2a (highlighting and red underlining added).

¶95. As an initial matter, for the reasons described above, none of the references teach or suggest to "receive [] a symmetric key." *See supra* at §VII(E). So it necessarily follows that none of those references can teach or suggest to use that non-existent received symmetric key to decrypt anything—including a "subscriber identity."

¶96. Notwithstanding, Petitioner alleges that Park's International Mobile Subscriber Identity ("IMSI") is the claimed "subscriber identity" and that it would be decrypted (and encrypted) using GlobalPlatform's DEK "symmetric key." '893 Pet. at 45-46, 57. But GlobalPlatform never teaches to encrypt/decrypt the IMSI

using the DEK. At most, GlobalPlatform teaches to "use[] the relevant data encryption session key (DEK) for *sensitive data* in command messages or for *sensitive data* in response messages." EX1006 at 284 (emphasis added). And according to GlobalPlatform, such sensitive data includes "all *keys* transmitted to a card." *Id.* (emphasis added). Thus, GlobalPlatform only teaches to encrypt/decrypt any sensitive key data sent to the card. *Id.*

¶97. Unlike key data, the IMSI is not the sort of sensitive data that GlobalPlatform teaches must be encrypted. Rather, in the 3G and 4G networks that were available in 2011 when GlobalPlatform was released, the IMSI was transmitted in plain text over the air during initial network attachment. For example, in 3G networks, when the user registers for the first time in a serving network, that network requests the user to send its permanent entity and "the user's response contains the IMSI in cleartext." EX2027 at 19. And the same is true in 4G networks. EX2028 at 21 (disclosing a mechanism where the 4G MME requests the user to send its permanent identity and "the user's response contains the IMSI in cleartext.")

¶98. Thus, a POSITA would not have understood GlobalPlatform as teaching to encrypt the IMSI using the DEK symmetric key. And the Petitioner does not rely on any other reference for this claim element. '893 Pet. at 45-46, 57. Thus, none of Petitioner's references—whether alone or in combination—teach or suggest

"decrypt[ing] … using the symmetric key … the subscriber identity," as per '893 claim 1.

G. A POSITA Would Not Combine The Park and GlobalPlatform References As The Petition Proposes (All Patents)

¶99. Samsung's theory depends upon a person of skill choosing to layer GlobalPlatform's DEK mechanism into Park's SPA in a particular way that does not appear in either reference. That choice is guided entirely by the hindsight knowledge of the claim limitation itself. Park already provides adequate security with full profile encryption using $key_{SM\text{-}DP}$; there is no articulated need within Park's architecture for an additional symmetric layer providing more security.

¶100. If a POSITA were to combine Park and GlobalPlatform, he/she would have looked to GlobalPlatform for implementation details of the smart card protocol to aid in realizing Park's scheme. Indeed, this is precisely what Park teaches: "consider the way to apply the de-facto standard for profile provisioning, [GlobalPlatform], to the eUICC provisioning ecosystem" in Park. EX1005 at 2. However, that POSITA would have been aware of Park's teaching that a direct application of GlobalPlatform's smart card protocol to Park's profile provision scheme faces numerous drawbacks affecting security and efficiency, particularly using two SCP sessions (Fig 2 in Park). EX1005 at 2-3 ("applying the [GlobalPlatform smart card protocol] into [Park's] eUICC provisioning ecosystem has several drawbacks with respect to scalability, efficiency, security, and

flexibility"). So that POSITA would have looked to retain the core principle of a single SCP session taught by Park's application of GlobalPlatform's SCP (Fig. 4 in Park) and carefully weighed the effects to security and efficiency when making any modifications to Park.

¶101. For example, a POSITA would have understood that Park's provisioning ecosystem already provides for adequate security. In Park's provisioning ecosystem, the SM-DP subscription manager locally derives its SM-DP key, $key_{SM\text{-}DP}$, and then uses it to encrypt the entire profile in a single SCP session. EX1005 at 4 (the eUICC and SM-DP "dynamically [] generate the SM-DP Credentials ($key_{SM\text{-}DP}$) [and then] SM-DP encrypts each block of [the] profile ($Profile_i$) [before] send[ing] the protected profile blocks to the eUICC"). In other words, for security reasons, the SM-DP and eUICC do not transport the SM-DP key, $key_{SM\text{-}DP}$, but rather locally derive it. *Id.* This avoids the need to transport the SM-DP key and expose it to other entities, potentially weakening the overall security. *Id.* Thus, when combining Park and GlobalPlatform, a POSITA would have similarly recognized the need to avoid exposing any session keys to other entities.

¶102. Accordingly, to retain the security advantage of Park's proposed design and implementation with a single SCP session, a POSITA would have used GlobalPlatform's key agreement option to derive the session keys—in much the same manner as Park derives the SM-DP key. More specifically, a POSITA would

have set the first bit in parameter *i* in card recognition or SD management data to "1" to utilize the key agreement option (rather than to "0" to utilize the key transport option):

b8	b7	b6	b5	b4	b3	b2	b1	Description
Not available	0	0	0	0	0	-	0	Key Transport
Not available	0	0	0	0	0	-	1	Key Agreement
Not available	0	0	0	0	0	0	-	Signature with message recovery
Not available	0	0	0	0	0	1	-	Signature without message recovery

Table F-1: Values of Parameter "i"

EX1006 at 255 (highlighting added).

¶103. Because of this binary choice, and to maintain consistency with Park's choice of key agreement for its SM-DP key, this would result in all of GlobalPlatform's session keys being derived—including the C-ENC key (equivalent of Park's SM-DP key) used to encrypt the entire profile and the DEK key used to encrypt the sensitive key data. *Id.* Thus, Park implicitly teaches to use GlobalPlatform's key agreement option to securely derive keys—and not the key transport option that could expose keys to security issues. In this manner, the properly-combined system retains Park's security advantages.

¶104. In stark contrast to the straightforward combination discussed above, Samsung proposes a combined Park-GlobalPlatform system that is not taught by either reference and is improperly motivated by hindsight. In Samsung's combination (which I do not agree with), the key K and IMSI are considered to be

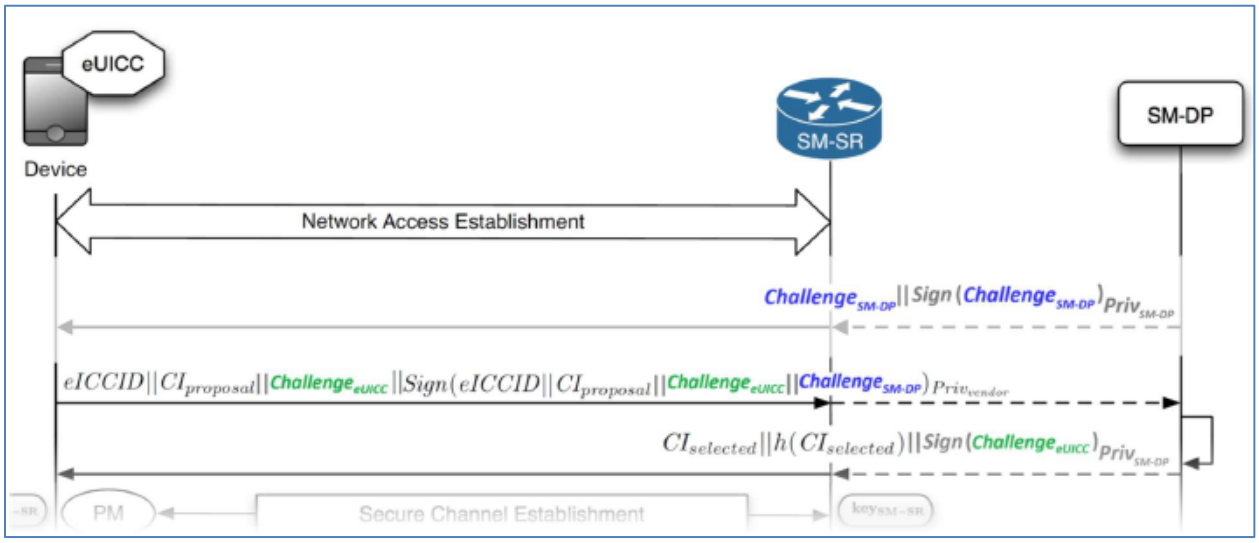
sensitive data that is encrypted by GlobalPlatform's DEK key, and then the entirety of the profile is further encrypted by another session key (*e.g.*, Park's SM-DP key or GlobalPlatform's C-ENC key). *See* '893 Pet. at 20-23; '780 Pet. at 19-20, 22-25; '094 Pet. at 19-20, 22-25. But Park does not teach a second layer of encryption. And while GlobalPlatform provides an option for a second layer of encryption for sensitive key data, it never teaches including the module identity (IMSI) as part of the second layer of encryption.

¶105. Further, in Samsung's combination, the DEK key is sent using GlobalPlatform's key transport option, while the other session keys are derived using GlobalPlatform's key agreement option. *See* '893 Pet. at 21-23; '780 Pet. at 22-25; '094 Pet. at 22-25. But GlobalPlatform never teaches to use both options simultaneously to obtain different keys. More specifically, GlobalPlatform does not teach using (1) the key transport option for DEK <u>and</u> (2) the key agreement option for other session keys (like the Command Encryption session key, C-ENC, which Samsung says serves the same function as Park's $key_{SM\text{-}DP}$). *See* '893 Pet. at 21; '780 Pet. at 22; '094 Pet. at 22. Instead, GlobalPlatform specifically states that the card recognition or SD management data will contain a parameter *i* whose first bit *b1* determines whether <u>*all*</u> the session keys are obtained using either (1) the key transport option (*b1*=0) or (2) the key agreement option (*b1*=1). EX1006 at 255. Thus, Samsung's combination is illogical and goes against the references' teachings.

¶106. Next, when combining Park with GlobalPlatform, a POSITA would not have been motivated to obtain just the DEK using the key transport option, while obtaining the other session keys via a different key agreement option, as these would require two separate sessions, thereby teaching away from Park that advocates for a single session. Instead, a POSITA would have viewed using two methods of obtaining session keys (as opposed to one) as inefficient and increasing overhead, as articulated by Park. In short, a POSITA would not have been motivated to build the combined Park-GlobalPlatform system in the manner set forth in the Petition, absent adopting the inventive insight disclosed only in the patents at issue.

¶107. Finally, with respect to the '780 and '094 Patents, Samsung argues that a POSITA would have modified Park Figure 4 to include GlobalPlatform's PKI authentication scheme such that the eUICC would generate a message with two nonces. '780 Pet. at 31-33; '094 Pet. at 30-32. This was done in hindsight to recreate the claimed "first message comprising … a nonce." '780 at 80:27-30; '094 at 80:32-35. But a person of skill would not have combined Park and GlobalPlatform as Samsung suggests. Park's PKI authentication scheme is not nonce-based. EX1005 at 4-5. And in light of Park's pre-existing deterministic data authentication, a POSITA would not have been motivated to include an additional layer of nonce-based authentication (like in GlobalPlatform) that compounds overhead without providing additional utility.

¶108. More specifically, Samsung modifies Park Figure 4 to include the blue and green "challenges"—neither of which appear in actual Park Figure 4:



'780 Pet. at 32; '094 Pet. at 31. The above portion of Park Figure 4 illustrates part of the initial capability negotiation between the device and SM-DP. Samsung argues that a POSITA would have made this modification to allow for PKI-based authentication between the two entities. *Id.* However, the existing negotiation exchange in Park already teaches that both entities use PKI; that is, their private keys include and sign deterministic pieces of information (*eICCID*, $CI_{proposed}$, $CI_{selected}$) for various reasons, including to enable authentication. In light of Park's pre-existing PKI based authentication, a POSITA would not have been motivated to include an additional, redundant layer of signing/authentication that adds to the overhead of authentication, without providing additional utility.

H. The Patents At Issue Are Entitled To Their Priority Dates (All Patents)

¶109. First, with respect to the '893 Patent, the '780 Patent, and the '094 Patent, Samsung alleges that none of those three patents are entitled to claim priority to their earliest priority dates because those patents either: (a) explicitly claim "receiv[ing] from the subscription manager, … a symmetric key" ('893 Pet. at 9-10); or (b) place no limit on the source of the claimed "symmetric key" so the claims are broad enough to cover receiving the symmetric key from the subscription manager ('780 Pet. at 9-10, '094 Pet. at 9-10), which the earliest Nix patent application allegedly does not support. And, according to the Petitions, if the patents at issue are not entitled to their earliest priority dates, then the inventor's own earlier patent, Nix175, allegedly becomes prior art. *Id.*

¶110. However, the earliest priority Nix patent application (and all subsequent applications in the chain) teach that the "mobile network operator 104 could operate the eUICC subscription manager 109." EX2024 at 25 (20:5); *see also id.* at 65 (60:7-8) ("the MNO 104 could also function as a eUICC subscription manager 109"). Thus, because the earliest priority application teaches the mobile network operator and the subscription manager can be the same, there is ample written description for receiving a symmetric key from a subscription manager. Hence, the patents at issue are entitled to their earliest December 6, 2013 priority date, and Nix175 is not prior art.

¶111. Second, with respect to the '780 Patent and the '094 Patent (but not the '893 Patent), Samsung alleges that neither of those two patents are entitled to claim priority to their earliest priority dates because those patents claim both a "first eUICC public key" and a "second eUICC public key," but the earliest Nix patent application only discloses one eUICC private/public key pair. '780 Pet. at 9, '094 Pet. at 9. However, the earliest priority Nix patent application (and all subsequent applications in the chain including the '780 and '094 applications) teaches two key pairs: (i) one pair for generating a digital signature used in authenticating; and (ii) another pair for deriving a profile key used in decryption.

¶112. The earliest Nix patent application describes the first key pair at, *e.g.*, EX2024 at 82 (77:13) and 83 (78:9) (a first instance of eUICC private key 215 is stored on module 101 within the mobile device and a first instance of eUICC public key 214 is stored on subscription manager 109). This first key pair is used to generate a digital signature that is sent in a first message from the eUICC to the subscription manager. *Id.* at 85 (80:5-10). The subscription manager then uses this digital signature to authenticate the eUICC. *Id.* (80:16-18).

¶113. The earliest Nix patent application describes the second key pair at, *e.g.*, EX2024 at 89 (84:25-27) (a second instance of eUICC public key 214 and eUICC private key 215). This second key pair is derived using Elliptic Curve Cryptography (ECC) algorithms and a random number generator. *Id.* at 89-90 (84:25-85:3). Then

this second key pair is subsequently used with other information to derive a profile key used to decrypt a portion of the eUICC profile. *Id.* at 90 (85:15-20). Thus, because the Nix priority applications teach two eUICC public/private key pairs, there is ample written description support for the claims of the '780 and '094 Patents at issue.

¶114. Another Nix patent application no. 14/084,141, which the '780 and '094 Patents explicitly incorporate by reference ('780 at 1:25-30, '094 at 1:33-38), explicitly discloses both a "first module private key" and a derived "second module private key":

> In exemplary embodiments, a module can use a *first module private key* and a server can use a *first module public key* to establish communication between the two nodes. The server can belong to a mobile network operator and be associated with a wireless network. The server can securely send the module a set of cryptographic parameters, where the set of cryptographic parameters includes values to define an equation for an elliptic curve. The values could comprise constants and variables such that the module can calculate an elliptic curve, and the elliptic curve can be different than standard, published curves. The set of cryptographic parameters could be sent from the server to the module in a server encrypted data, where the server encrypted data is decrypted by the module using any of (i) *the first module private key*, (ii) a symmetric key, and (iii) a shared secret key. The module can use the set of cryptographic parameters, a random number generator, and a key pair generation algorithm within a set of

> cryptographic algorithms in order to generate a *new, second module key pair, which could comprise a second module public key and a second module private key*. The module can securely and/or authoritatively send the *second module public key* to the server, where the steps to implement security for sending the *second module public key* can include using of the *first module public key* and/or the shared secret key.

EX2030 at 12:30-13:11 (emphasis added). And the patents at issue explicitly teach that a module public/private key can be the same as an eUICC public/private key. '780 at 43:62-44:3; '094 at 44:5-14. This provides further written description supporting two eUICC public/private key pairs.

VIII. Declaration

¶115. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross examination on the subject matter of this declaration. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

¶116. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true. Further, these statements are made with the knowledge that willful false statements

are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and may jeopardize the validity of the Patent-at-Issue.

Executed on March 3, 2026, at Atlanta, Georgia.

Dr. Karthikeyan Sundaresan

APPENDIX A (RESUME)

KARTHIKEYAN (KARTHIK) SUNDARESAN

5152 Centergy One
75 5th St NW, Atlanta GA 30308
Ph: 404.894.5141

karthik@ece.gatech.edu
https://karthik.ece.gatech.edu
https://marga.ece.gatech.edu

Education

- Georgia Institute of Technology, USA - Ph.D (ECE), 2006; M.S (ECE), 2003
- Anna University, India - B.S. (Electronics and Communications), 2001

Professional Experience

Professor — Oct 2021 – Present
School of ECE (Adjunct, CS) , Georgia Tech, Atlanta, USA
Director, MARGA (Mobile Advanced Research@GT)

Visiting Chair Professor — June 2025-June 2027
Computer Science, Indian Institute of Technology, Chennai, IN

Co-founder, CTO — Jun 2023 – Present
Wirinos Inc.

Co-founder, Technical Advisor — Apr 2022 – Present
NavigateIO Inc.

Senior Researcher — Aug 2006 – Sep 2021
NEC Labs America, Princeton NJ, USA

Research Assistant — Aug 2001 – July 2006
Georgia Tech, Atlanta, USA

Research Intern — Jan 2006 – Mar 2006
Intel Research, Cambridge, UK

Research Intern — May 2005 – Aug 2005
Los Alamos National Lab, Los Alamos, USA

Research Fellow — May 2001 – Jul 2001
AU-KBC Research Center, Chennai, India

Awards/Honors

Professional/Academic

- NAI (National Academy of Inventors) Fellow, 2023 for creating outstanding inventions with a tangible impact on the quality of life, economic development, and welfare of society.
- IEEE Fellow, 2020 for contributions to algorithms for mobile networking and computing
- ACM Distinguished Member, 2018 for outstanding scientific contributions to computing.
- Association for Computing Machinery (ACM) SIGMOBILE Rockstar Award, 2016 – for early-career contributions to mobile connectivity (Citation).
- Business Contribution Award for LTE Small-cell Technology Commercialization, NEC 2015.

- University Gold Medal; ranking FIRST in academic performance, School of ECE, Anna University, 2001.
- Ramanujan Centennial Gold Medal; ranking FIRST overall in all Mathematics courses across all disciplines in B.E., Anna University, 2001.
- Alumni Association's Best Outgoing Student Award, School of ECE, Anna University, Aug 2001.

Research

- Best Paper Runner-up Award: "Enabling Acoustic IoT through Composable Distributed Beamforming Tags", ACM International Conference on Information Processing in Sensor Networks (IPSN), May 2024.
- Best Paper Finalist: "Scalable Network Tomography for Dynamic Spectrum Access", IEEE International Conference on Computer Communications (INFOCOM), May 2024.
- Best Paper Award: "Is WiFi 802.11mc FTM Ready for Prime-time Deployment?", ACM Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization, Oct 2022.
- Best Paper Award: "SkyCore: Moving Core to the Edge for Untethered and Reliable UAV-based LTE Networks", ACM International Conference on Mobile Networking and Computing (MobiCom), Oct 2018.
- Best Paper Finalist: "BLU: Blue-printing Interference for Robust LTE Access in Unlicensed Spectrum", ACM International Conference on Emerging Networking Experiments and Technologies (CoNEXT), Dec 2017.
- Best Paper Award: "MIDAS: Empowering 802.11ac Networks through Multiple-input Distributed Antenna Systems", ACM International Conference on Emerging Networking Experiments and Technologies (CoNEXT), Dec 2014.
- Best Paper Award: "On Exploiting Diversity and Spatial Reuse in Relay-enabled Wireless Networks", in ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), May 2008.
- Best Paper Award: "Routing in Ad-Hoc Networks with MIMO Links", in IEEE International Conference on Network Protocols (ICNP), Nov 2005.
- Best Paper Award: "Practical Limits on Achievable Energy Improvements and Useable Delay Tolerance in Correlation Aware Data Gathering in Wireless Sensor Networks", in IEEE International Conference on Sensing, Communication and Networking (SECON), Sept. 2005.

Dissertations

- Sigma Xi Best Doctoral Thesis Award, Georgia Institute of Technology, USA, Apr. 2007. Thesis title: "Network Protocols for Ad-hoc Networks with Smart Antennas"
- Sigma Xi Best Master's Thesis Award, Georgia Institute of Technology, USA, Apr. 2004. Thesis title: "MAC Protocols for Ad-hoc Networks with Switched Beam Antennas"
- Alumni Association's Best Undergraduate Thesis Award, Anna University, INDIA, Aug. 2001. Thesis title: "Energy Allocation and Multiple Access for Multi-carrier Communication"

Commercialization/ Start-up

My work has also focused on translating research to high impact commercialization, technology transfer and start-up activities.

- Wirinos Inc.: Ultra-low power sustainable wireless tags for identification and high accuracy tracking in large scale supply chain and IoT applications
  Led its innovative design and productization through GT's Create-X start-up incubator program in 2023. Engaged in proof-of-concept trials for tracking personnel and medical devices/assets with healthcare providers; co-founder and chief technical advisor for Wirinos Inc.

- NavigateIO Inc.: Infrastructure-free Tracking of First Responders in Dynamic GPS-denied Indoor Environments
  Led its productization through NECx and Alchemist start-up accelerator programs. Successfully raised seed funding; ran numerous proof-of-concept trials with first responders since 2019; co-founder and chief technical advisor of NavigateIO Inc.

- FERMI: Self-Organizing Network Solution for Interference Management in Heterogeneous LTE Networks
  Technology-transferred to NEC business units for commercialization through LTE small cell base stations, 2015. Received business award for commercialization.

Technical/Industry Experience

- Leading end-to-end R&D visions and groups targeting challenging problems in the wireless (networking, sensing, embedded and autonomous systems) space: identifying the key problems, coming up with technically (algorithmically) sound solutions, translating solutions to real-world systems
- Leading and mentoring a team of Ph.D researchers in accomplishing challenging R&D projects, as well as numerous Ph.D students and contributing to their thesis
- Translating research ideas to commercialization: deploying research prototypes in real-world, continuous iteration of solution (towards productization) based on user feedback
- Taking research solutions through start-up incubation and accelerator programs

Work Experience

Professor, School of ECE, CS, Georgia Tech, Atlanta GA — Oct 2021 - Present

Director, MARGA (Mobile Advanced Research Lab at Georgia Tech) Lab

Leading a highly motivated group of graduate students on cutting-edge research problems in mobile and wireless networks, sensing and computing in various exciting verticals spanning immersive experience, wireless health, aerial connectivity, etc.

PI on grant proposals (awarded):

- "ARMIN: Autonomous, Resilient Mobility Inverted Networks", OUSD, Co-PI.
- "Adaptive 5G Core Network", Strategic Initiative Proposal, Georgia Tech Research Institute (GTRI), Co-PI.
- "Seamless Coexistence of Positioning and Communications in 5G and Beyond Wireless Systems", Single PI, NSF.
- "A New Paradigm of Scalable Acoustic IoT through Composable, Distributed Beamforming", Single PI, NSF.

Co-founder and Chief Technology Officer, Wirinos Inc. — 2023 - Present

Co-Inventor of an ultra-low power, high-accuracy wireless tracking solution for large scale supply chain and IoT applications. Developed the research solution with post-doc

at MARGA, GT and incubated through GT's Create-X accelerator program; co-founded the start-up in 2023. Engaged in successful PoCs with healthcare facilities.

Co-founder and Chief Technology Advisor, NavigateIO Inc. — 2022 - Present

Inventor of an infrastructure-free, real-time, wireless tracking solution for challenging, GPS-denied indoor environments. Led the research solution from NEC labs through start-up incubation and co-founded the start-up. Numerous successful PoCs with first responder departments across the country, and federal grant recipient for the same.

Senior Researcher, NEC Labs America, Princeton NJ — 2006 - 2021

Led several challenging research projects in the Mobile Communications and Networking department. Research thrusts targeted three directions: (1) Confluence of 5G Networks and Autonomous Systems — exploring an alternate, paradigm of rapidly-deployable, on-demand, self-configurable mobile networks that can be hosted and driven by future, pervasive autonomous platforms (UAVs and AGVs). (2) Ultra Low Power Sensing — aims to remove several of the critical barriers in enabling future on-body healthcare applications, by leveraging wireless backscattering to design novel, ultra low power (micro-W) wireless tags with significantly enhanced deployment, communication and sensing capabilities. (3) Tracking in Resource-constrained Environments — rethinking wireless localization and tracking solutions for practical applications like first responder (zero infrastructure support) situations, or massive scale (low-cost, low-power beacons) inventory tracking in warehouses that inherently operate in resource-constrained regimes.

Prior to these, earlier research thrusts had targeted: (i) wireless connectivity: pushed the performance envelope across multiple dimensions (capacity, latency, density, heterogeneity, user experience, availability) through novel network-level as well cross-layer (PHY+MAC) solutions. (ii) software-defined mobile computing: bringing software-defined computing and mobile connectivity together to enable demanding future applications ranging from massive scale Internet of Things (IoT) to high-bandwidth, low-latency Continuous Mobile Vision (eg. augmented/virtual reality), over mobile networks.

In addition to numerous publications and patents, work has received recognition through numerous awards both from company (for commercialization, startup incubation), as well as the broader research community (IEEE Fellow, ACM distinguished member, ACM early career award, and numerous best paper awards).

More information available at: https://sites.google.com/view/karthik-s/home/research-latest; some demos at: https://sites.google.com/view/karthik-s/home/research/demos.

Research Assistant, Georgia Tech, Atlanta GA — 2001 - 2006

Graduate research in the GNAN research group: focused on designing efficient network protocols for wireless networks that leveraged various forms of smart antennas. While advanced antenna technologies like MIMO were becoming popular at the physical layer (on isolated links), it was unclear how they can be effectively leveraged at higher layers of the protocol stack to deliver value to the network as a whole and to end applications. My thesis pushed the boundaries in this direction, and made significant advances in the design of algorithmically-sound solutions for leveraging such smart antennas in the network. My masters and doctoral theses received the best thesis awards at GaTech.

Research Intern, Intel Research, Cambridge UK, Jan – Mar 2006

Designed and implemented algorithms for self-organizing wireless LANs. The algorithms leveraged several cross layer parameters such as load, average contention duration, etc. that were measured at the firmware and instrumented for access at the driver. The algorithms were implemented in the device driver and tested in Intel's wireless LAN access points & client devices. This work was published in ACM IMC 2006.

Research Intern, Los Alamos National Lab, Los Alamos NM, May - Aug 2005

Investigated the problem of communication in multi-hop wireless networks with smart antennas from a combinatorial perspective in the discrete simulation science division. This involved the design of efficient centralized as well as purely localized algorithms with performance guarantees to help nodes determine the optimal usage of available degrees of freedom to improve network utilization; and resulted in a publication in ACM MobiHoc 2006. I also designed and implemented MAC protocols for wireline networks as part of a highly scalable network simulator.

Research Fellow, AU-KBC Research Center, Chennai India, May - Aug 2001

Designed a novel, adaptive allocation algorithm for multi-user OFDM communication systems that minimizes the total transmit power by optimally allocating OFDM sub-carriers and data bits based on instantaneous channel information. This work was later published in Wireless Personal Communications Journal, (Kluwer) Apr 2003.

Research Contributions

- 60+ awarded patents (Appendix A)
- 100+ research papers in top-tier IEEE and ACM conferences and journals, and book chapter (Appendix B)
- Several invited talks, tutorials, seminars, keynotes and panels (Appendix C)

Professional Activities

- Several leadership (technical and organizational) roles in top tier conferences; service on numerous international-level research review panels, committees and editorial boards (Appendix D)

Patents (Appendix A)

Technical Expert for Patent Litigation

- Network1 vs. Samsung (HPC LLP), 2025-Present; US Patents #11,233,780, #12,207,094, #11,916,893
- Daingean vs. T-Mobile (HPC LLP), 2023-2025; US Patent #8,576,803
- Daingean vs. AT&T, (HPC LLP), 2023-2025; US Patents #8,576,803, #10,484,976, #10,841,958
- XiFi vs. Samsung (Robins Kaplan LLP), 7 patents, 2024.
- Geoscope Tech. vs. Apple Inc. (Fish and Richardson), 2023-2024; US Patents #8,400,358, #8,786,494, #8,406,753, #7,561,104
- Broadcom vs. Netflix (Adsero IP), 2022; US Patents #7,103,794, #8,646,014

Provisional Patents (Co-Inventor)

1. A Spectrally-efficient wake-up radio control plane for WiFi, Application # 63/877,623, Sep 2025.
2. Collaborative 5G positioning for 2D and 3D location services, Application # 63/676050, July 2024.
3. System, Method and Apparatus for Distributed Acoustic Beamforming for Practical IoT Applications, Application # 63/469855, May 2023.
4. RF Systems, Methods and Apparatus for High Accuracy Tracking with Ultra Low Power Wireless Tags, Application # 63/422522, Nov 2022.
5. Device tracking with Radio ranging and sensor functions, Provisional # 17/722,721, Oct 2022.
6. Lidar-driven mmWave beam management, Provisional # 17/575,193, Jul 2022.
7. Near real-time reconstruction using drones, Provisional # 17/220,046, Oct 2021.
8. Infrastructure-free tracking and response, Provisional # 17/214,188, Sep 2021.
9. Reading passive wireless tags using commodity devices, Provisional # 17/202,854, Sep 2021.
10. Locating objects in indoor spaces using radio frequency backscatter tags, Provisional # 17/157,194, Jul 2021.

Awarded Patents (Co-Inventor)

11. Infrastructure-free RF Tracking in Dynamic Indoor Environments, US patent # 11,388,564, Jul 2022.
12. Un-manned Aerial Vehicle Network, US patent # 11,356,172, Jun 2022.
13. Tracking Indoor Objects with Inertial Sensor Measurements, US patent # 11,169,518, Nov 2021.
14. Tracking Indoor Objects from an Unmanned Aerial Vehicle, US patent # 11,089,432, Aug 2021.
15. Self-configuring Long Term Evolution Radio Access Network on Unmanned Autonomous Vehicles, US patent # 11,054,843, Jul 2021.
16. Backscatter-aided Navigation System, US patent # 10,852,415, Dec 2020.
17. In-home Inventory and Location System, US patent # 10,852,414, Dec 2020.
18. Tagging Objects in Indoor Spaces using Ambient, Distributed Backscatter, US patent # 10,852,413, Dec 2020.
19. In-store Interaction and Location System for Interfacing Users with Products, US patent # 10,852,416, Dec 2020.
20. Signaling for Coordinated Multi-point Transmission and Reception, US patent # 10,616,880, Apr 2020.
21. Speculative Scheduling in Wireless Networks, US patent # 10,582,529, Mar 2020.
22. Interference Topology Inference to Enhance Performance of LTE Unlicensed Networks, US patent # 10,574,535, Feb 2020.
23. Implementing Wireless Communication Networks using Unmanned Aerial Vehicles, US patent # 10,470,243, Nov 2019.
24. System and Method for Enabling Interference Awareness for LTE Operation in Unlicensed Spectrum, US patent # 10,469,188, Nov 2019.
25. Product Checkout and Interest Detection in Retail Environment using Radio Frequency Identification, US patent # 10,410,025, Sept 2019.
26. Distributed Architecture for Implementing Wireless Communication Networks, US patent # 10,405,373, Sept 2019.
27. Blue-printing Interference for LTE Access In Unlicensed Spectrum, US patent # 10,405,209, Sept 2019.
28. Battery-free Touch-aware User Input using RFID Tags, US patent # 10,346,655, July 2019.

29. Systems and Methods for Distributed Assignment of Task Identifiers, US patent # 10,331,493, June 2019.
30. Design of Randomization Function and its Application in Load Balancing, US patent # 10,298,671, May 2019.
31. Consistent Hashing, US patent # 10,296,394, May 2019.
32. Enabling Technologies for LTE on Unlicensed Spectrum, US patent # 10,292,054, May 2019.
33. Enabling High-bandwidth Responsive Mobile Applications in LTE Networks, US patent # 10,122,547, Nov 2018.
34. Interference Alignment in a Network with Asymmetrical Channel Dimensions, US patent # 10,110,293, Oct 2018.
35. Asynchronous Access and Synchronous Transmission for Coexistence of Wireless Standards, US patent # 10,091,114, Oct 2018.
36. Software-driven Long-Term Evolution Core Network for Mobile Access, US patent # 10,021,172, July 2018
37. Efficient Network-wide Broadcasting over LTE Networks, US patent # 9,967,860, May 2018.
38. Enabling Long Term Evolution/WiFi Coexistence, US patent # 9,936,414, Apr 2018.
39. System and method for dynamic provisioning of Wi-Fi capacity in large venues using a C-RAN architecture, US patent # 9,813,944, Nov 2017.
40. Scaling Wireless Full-Duplex in Multi-Cell Networks, US patent # 9,722,720, Aug 2017.
41. Intelligent WiFi-offloading for Next-generation Mobile Networks, US patent # 9,723,532, Aug 2017.
42. Degrees of Freedom in Multi-cell Wireless Systems with Full-duplex Base Stations using Interference Alignment, US patent # 9,736,785, Aug 2017.
43. Method and Apparatus for Powerline Communication and Networking in Multi-flow Environments, US patent # 9,654,174, May 2017.
44. Efficient Large Scale Multiple Input Multiple Output Communications, US patent # 9,413,474, Sept 2016.
45. Multi-user Multiple Input Multiple Output (MIMO) Communication with Distributed Antenna Systems in Wireless Networks, US patent # 9,450,654, Sept 2016.
46. Carrier Aggregation, US patent # 9,337,966, May 2016.
47. Multiple-Input Multiple-Output Wireless Communications With Full-Duplex Radios, US patent # 9,137,788, Sept 2015.
48. A Cloud Based Radio Access Network for Small Cells, US patent # 9,125,047, Sept 2015.
49. Tailoring Wireless Transmission Strategies to User Profiles in Cloud Based Radio Access Networks, US patent # 9,066,351, Jun 2015.
50. Methods and Apparatus for Integrating Batch Scheduling with External Beamforming, US patent # 8,976,696, Mar 2015.
51. Scalable Network MIMO for Wireless Networks, US patent # 8,923,907, Dec 2014.
52. CoordinatedMulti-PointTransmission, US patent # 8,891,604, Nov 2014.
53. Method for a Canceling Self Interference Signal Using Active Noise Cancellation for Full- Duplex Simultaneous (in time) and overlapping (in space) Wireless Transmission and Reception on the Same Frequency Band, US patent # 8,879,433, Nov 2014.
54. Method for a Canceling Self Interference Signal Using Passive Noise Cancellation for Full- Duplex Simultaneous (in time) and overlapping (in space) Wireless Transmission and Reception on the Same Frequency Band, US patent # 8,837,332, Sep 2014.

55. Femtocell Resource Management for Interference Mitigation, US patent # 8,767,580, July 2014.
56. Methods and Systems for Allocation of Macro Cell Resources in a Distributed Femtocell Network and a Distributed Relay Station Network, US patent # 8,780,849, July 2014.
57. High Performance and Low Complexity Scheduling Method for Resource Usage in OFDMA Wireless Relay Networks, US patent # 8,660,030, Feb 2014.
58. Channel Estimation Methods and Systems Based on Power Measurement at Receivers, US patent # 8,537,928, Sep 2013.
59. Video Multicast Scheduling, US patent # 8,537,738, Sep 2013.
60. Multicast Scheduling Systems and Methods for Leveraging Cooperation Gains in Relay Networks, US patent # 8,537,693, Sep 2013.
61. Link Layer Multicasting Systems and Methods, US patent # 8,520,764, Aug 2013.
62. Wireless Multicasting with Beamforming Antennas, US patent # 8,519,888, Aug 2013.
63. Beamforming methods and systems employing measured power at a receiver to perform channel estimation, US patent # 8,380,133, Feb 2013.
64. Methods and systems for location-based allocation of macro cell resources, US patent # 8,374,135, Feb 2013.
65. Systems and methods for adaptive beamforming in indoor wireless networks, US patent # 8,340,584, Dec 2012.
66. Methods and systems for allocation of macro cell resources in a distributed femto cell network and a distributed relay station network, US patent # 8,311,005, Nov 2012.
67. Optimal beam scheduling for multicasting in wireless networks, US patent # 8,310,975, Nov 2012.
68. Systems and methods for leveraging spatial reuse in OFDMA relay networks, US patent # 8,218,472, Jul 2012.
69. High performance scheduling methods and apparatus for leveraging diversity in relay- enabled wireless networks, US patent # 8,170,031, May 2012.
70. System and Method for Scheduling in Relay-assisted Wireless Networks, US patent # 8,134,946, Mar 2012.
71. Integrated scheduling of unicast and multicast traffic in relay-enabled wireless networks, US patent # 8,098,609, Dec 2012.
72. Method for scheduling heterogeneous traffic in B3G/4G cellular networks with multiple channels, US patent # 7,856,004, Jan 2010.

Publications (Appendix B)

Conference

73. N. Matson, Y-T. Lin, K. Sundaresan, "A Holistic Approach to Non-Terrestrial 5G Networking with LEO Satellites: Algorithms, Experiments and Insights", ACM International Conference on emerging Networking EXperiments and Technologies (CONEXT), Dec 2025.

74. A. Madnaik, K. Sundaresan, "Practical Design and Orchestration of Frequency-Shifting RIS for NLoS mmWave Sensing", ACM International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing" (MobiHoc), Oct 2025.

75. S. Venkateswaran, H-C. Lin, K. Sundaresan, R. Sivakumar, "AuraWake: A Spectrally-Efficient Wake-up Radio Control Plane for Wi-Fi", International Conference on

Modeling, Analysis and Simulation of Wireless and Mobile Systems" (MSWiM), Oct 2025.

76. H. Mii, K. Sundaresan, "Towards a Privacy-preserving Approach for Seated Posture Monitoring using mmWave Radar and CNNs", ACM UbiSense (Ubiquitous Sensing) Workshop, co-located with ACM UbiComp, Oct 2025.

77. Y. Li, R. Sheshadri, K. Sundaresan, E. Chai, Y. Zeng, J. Raghuram, S. Banerjee, "Medusa: Scalable Multi-View Biometric Sensing in the Wild with Distributed MIMO Radars", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Oct 2025.

78. N. Garg, I. Shahid, R. Seshadri, K. Sundaresan, and N. Roy, "Large-scale UWB Localization: Algorithms and Implementation", To Appear in Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI), Apr 2025.

79. Y-T. Lin, N. Matson and K. Sundaresan, "Bringing Collaborative Positioning to Native 5G Systems for Enhanced 2D and 3D Location Services", To appear in ACM International Conference on emerging Networking EXperiments and Technologies (CONEXT), Dec 2024.

80. A. Liu, Y-T. Lin, and K. Sundaresan, "View-agnostic Human Exercise Cataloging with Single MmWave Radar", ACM Joint International Conference on Pervasive and Ubiquitous Computing (UbiComp), Aug 2024.

81. M. Rostami, A. Liu, K. Sundaresan, "Enabling Acoustic IoT through Composable Distributed Beamforming Tags", ACM International Conference on Information Processing in Sensor Networks (IPSN), **Best Paper Runner-up Award,** May 2024.

82. N. C. Matson, K. Sundaresan, "Online Radio Environment Map Creation via UAV Vision for Aerial Networks", IEEE International Conference on Computer Communications (INFOCOM), May 2024.

83. A. Madnaik, N. C. Matson, K. Sundaresan, "Scalable Network Tomography for Dynamic Spectrum Access", IEEE International Conference on Computer Communications (INFOCOM), **Best Paper Finalist,** May 2024.

84. Y-T. Lin, K. Sundaresan, "A New Paradigm of Communication-aware Collaborative Positioning for FutureG Wireless Systems", ACM International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing" (MobiHoc), Oct 2023.

85. F. Ahmad, C. Shin, E. Chair, K. Sundaresan, R. Govindan, "AeroTraj: Trajectory Planning for Fast, and Accurate 3D Reconstruction using a Drone-based LiDAR". Proceedings of ACM Joint International Conference on Pervasive and Ubiquitous Computing (UbiComp), Oct 2023.

86. M. Dasari, R. Seshadri, K. Sundaresan, S. Das, "RoVaR: Robust Multi-agent Tracking through Dual-layer Diversity in Visual and RF Sensing", Proceedings of ACM Joint International Conference on Pervasive and Ubiquitous Computing (UbiComp), Oct 2023.

87. M. Rostami, K. Sundaresan, "Enabling High Accuracy Pervasive Tracking with Ultra Low Power UWB Tracking Tags", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Oct 2022.

88. S. Aggarwal, R. Seshadri, K. Sundaresan, D. Koutsonikolas, "Is WiFi 802.11mc FTM Ready for Prime-time Deployment", Proceedings of ACM Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization, **Best Paper Award**, Oct 2022.

89. T. Woodford, X. Zhang, E. Chai and K. Sundaresan, "FishEye: Leveraging Diverse Reflector Geometries for Omni-directional Around-corner Automotive Radar", Proceedings of ACM International Conference on Mobile Systems, Applications and Services (MOBISYS), June 2022.

90. M. Rostami, X. Chen. Y. Feng, K. Sundaresan, D. Ganesan, "MIXIQ: Re-thinking Ultra Low Power Receiver Design for Next-generation On-body Applications", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Oct 2021.

91. R. Seshadri, E. Chai, K. Sundaresan, S. Rangarajan, "SkyHaul" A Self-Organizing Gigabit Network in the Sky", Proceedings of ACM International Symposium on Theory, Algorithmic Foundations and Protocol Design for Mobile Networks and Mobile Computing (MOBIHOC), July 2021.

92. T. Woodford, X. Zhang, E. Chai and K. Sundaresan, "SpaceBeam: Lidar-driven One-Shot mmWave Beam Management", Proceedings of ACM International Conference on Mobile Systems, Applications and Services (MOBISYS), June 2021.

93. H. Alhulayyil, K. Apicharttrisorn, J. Chen, K. Sundaresan, S. Oymak and S. Krishnamurthy, "WOLT: Auto-configuration of Integrated Enterprise PLC-WiFi Networks", Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS), Nov 2020.

94. M. Rostami, K. Sundaresan, E. Chai, S. Rangarajan, and D. Ganesan, "Redefining Passive in Backscattering with Commodity Devices", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Oct 2020.

95. A. Dhekne, A. Chakraborty, K. Sundaresan, S. Rangarajan, "TrackIO: Tracking First Responders Inside Out", USENIX Symposium on Networked Systems Design and Implementation (NSDI), Feb 2019.

96. A. Chakraborty, E. Chai, K. Sundaresan, A. Khojastepour, S. Rangarajan, "SkyRAN: A Self- Organizing LTE RAN in the Sky", ACM International Conference on emerging Networking EXperiments and Technologies (CONEXT), Dec 2018.

97. M. Moradi, K. Sundaresan, E. Chai, S. Rangarajan, "SkyCore: Moving Core to the Edge for Un-tethered and Reliable UAV-based LTE Networks", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), **Best Paper Award**, Oct 2018.

98. R. Sheshadri, K. Sundaresan, E. Chai, S. Rangarajan, "ELI: Empowering LTE with Interference Awareness in Unlicensed Spectrum", IEEE International Conference on Network Protocols (ICNP), July 2018.

99. R. Sheshadri, K. Sundaresan, E. Chai, S. Rangarajan and D. Koutsonikolas, "BLU: Blue- printing Interference for Robust LTE Access in Unlicensed Spectrum", ACM International Conference on emerging Networking EXperiments and Technologies (CONEXT), **Best Paper Finalist**, Dec 2017.

100. S. Pradhan, E. Chai, K. Sundaresan, S. Rangarajan, L. Qiu, "RIO: A Pervasive RFID-based Touch Gesture Interface", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Oct 2017.

101. R. Sivaraj, M. Arslan, K. Sundaresan, S. Rangarajan, P. Mohapatra, "BoLTE: Efficient Network-wide LTE Broadcasting", Proceedings of IEEE International Conference onNetwork Protocols (ICNP), Oct 2017.

102. A. Banerjee, R. Mahindra, K. Sundaresan, S. Rangarajan, S. Kasera, K. V-D. Merwe, "Orchestrating the Data Plane of Virtual LTE Core Networks", Proceedings of IEEE International Conference on Sensing, Communication and Networking (SECON), June 2017.

103. S. Pradhan, E. Chai, K. Sunadresan, S. Rangarajan, L. Qiu, "Konark: A RFID-based System for Enhancing In-Store Shopping Experience", Workshop on Physical Analytics, Co-located with ACM MobiSys, June 2017.

104. K. Apichattrisorn, A. Fatya, J. Chen, K. Sundaresan, S. Krishnamurthy, "Enhancing WiFi Throughput with PLC Extenders", Passive and Active Measurements Conference (PAM), Mar 2017.

105. J. Cho, K. Sundaresan, R. Mahindra, S. Rangarajan, J. V-d. Merwe, "ACACIA: Context-aware Edge Computing over Mobile Networks", ACM International Conference on emerging Networking EXperiments and Technologies (CONEXT), Dec 2016.

106. R. Seshadri, M. Arslan, K. Sundaresan, S. Rangarajan, D. Koutsonikolas, "AmorFi: Amorphous WiFi Networks for High Density Deployments", ACM International Conference on emerging Networking EXperiments and Technologies (CONEXT), Dec 2016.

107. E. Chai, K. Sundaresan, M. Khojastepour, S. Rangarajan, "LTE in Un-licensed Spectrum: Are We There Yet?", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Oct 2016.

108. A. Atya, K. Sundaresan, S. Krishnamurthy, M. Khojastepour, S. Rangarajan, "BOLT: Enabling High-Throughput Powerline Communication Networks", ACM International Conference on emerging Networking EXperiments and Technologies (CONEXT), Dec 2015.

109. A. Banerjee, R. Mahindra, K. Sundaresan, S. Kasera, J. Van Der Merwe, S. Rangarajan, "SCALE: Scaling the LTE Control Plane for Future Wireless Access", ACM International Conference on emerging Networking EXperiments and Technologies (CONEXT), Dec 2015.

110. J. Xiong, K. Sundaresan, K. Jamieson, "ToneTrack: Leveraging Frequency-agile Radios for Time-based Indoor Wireless Localization", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Sept 2015.

111. X. Xie, E. Chai, X. Zhang, K. Sundaresan, M. Khojastepour, S. Rangarajan, "Hekaton: Efficient and Practical Large-Scale MIMO", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Sept 2015.

112. S. Singh, K. Sundaresan, S. Krishnamurthy, X. Zhang, M. Khojastepour, S. Rangarajan, "Trinity: A Practical Transmitter Cooperation Framework to Handle Heterogeneous User Profiles in Wireless Networks", Proceedings of ACM International Conference on Mobile Ad Hoc Networking and Computing (MOBIHOC), July 2015.

113. M. Lotfi, K. Sundaresan, M. Khojastepour, S. Rangarajan, "The Economics of Quality-Sponsored Data in Wireless Networks", International Symposium on Modeling and Optimization in Mobile, Ad-hoc and Wireless Networks (WiOPT), May 2015.

114. M. Khojastepour, K. Sundaresan, S. Rangarajan, "Scaling Wireless Full-duplex to Multi-cell Networks", IEEE International Conference on Computer Communications (INFOCOM), Apr 2015.

115. J. Xiong, K. Sundaresan, K. Jamieson, M. Khojastepour, S. Rangarajan, "MIDAS: Empowering 802.11ac Networks with Multiple-input Distributed Antenna Systems", **Best Paper Award**, ACM International Conference on emerging Networking EXperiments and Technologies (CONEXT), Dec 2014.

116. K. Sundaresan, M. Khojastepour, E. Chai, S. Rangarajan, "Full-duplex without Strings: Enabling Full-duplex with Half-duplex Clients", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Sept 2014.

117. R. Mahindra, H. Viswanathan, K. Sundaresan, M. Arslan, S. Rangarajan, "A Practical Traffic Management System for Integrated LTE-WiFi Networks", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Sept 2014.

118. J. Xiong, K. Jamieson, K. Sundaresan, "Synchronicity: Pushing the Envelope of Fine-grained Localization with Distributed MIMO", ACM Workshop on Hot Topics in Wireless, Sept 2014.

119. M. A. Khojastepour, E. Aryafar, K. Sundaresan, S. Rangarajan, "Exploring the Potential of Full-Duplex in Legacy LTE Systems", Proceedings of IEEE International Conference on Sensing, Communication and Networking (SECON), June 2014.

120. M. Khojastepour, K. Sundaresan, M. Farajzadeh-Tehrani, S. Rangarajan, "Degrees of Freedom per Communication Node", International Symposium on Modeling and Optimization in Mobile, Ad-hoc and Wireless Networks (WiOPT), May 2014.

121. T. Bansal, K. Sundaresan, S. Rangarajan, P. Sinha, "R2D2: Embracing Device-Device Communication in Next Generation Cellular Networks", IEEE International Conference on Computer Communications (INFOCOM), Apr 2014.

122. K. Sundaresan, M. Arslan, S. Singh, S. Rangarajan, S. Krishnamurthy, "FluidNet: A Flexible Cloud-based Radio Access Network for Small Cells", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Miami, Oct 2013.

123. X. Zhang, K. Sundaresan, A. Khojastepour, S. Rangarajan, K. Shin, "NEMOx: Scalable Network MIMO for Wireless Networks", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Miami, Oct 2013.

124. X. Xie, X. Zhang, K. Sundaresan, "Adaptive Feedback Compression for MIMO Networks", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Miami, Oct 2013.

125. K. Sundaresan, S. Rangarajan, "Energy-efficient Carrier Aggregation Algorithms for Next Generation Cellular Networks", Proceedings of IEEE International Conference on Network Protocols (ICNP), Oct 2013.

126. A. Atya, A. Aqil, S. Singh, I. Broustis, K. Sundaresan, S. Krishnamurthy, "Mitigating Malicious Interference Via Subcarrier-level Radio Agility in Wireless Networks", Proceedings of IEEE International Conference on Network Protocols (ICNP), Oct 2013.

127. J. Yoon, K. Sundaresan, A. Khojastepour, S. Rangarajan, S. Banerjee, "ProBeam: A Practical Multi-cell Beamforming System for OFDMA Small Cells", Proceedings of ACM International Conference on Mobile Ad Hoc Networking and Computing (MOBIHOC), Jul 2013.

128. C. Liu, K. Sundaresan, M. Jiang, S. Rangarajan, G.K. Chang, "The Case for Re-configurable Backhaul for Cloud-RAN based Small Cell Networks", IEEE International Conference on Computer Communications (INFOCOM), Apr 2013.

129. M. Arslan, I. Singh, S. Singh, H. Madhyastha, K. Sundaresan, S. Krishnamurthy, "Computing while Charging: Building a Distributed Computing Infrastructure with Smartphones", ACM International Conference on emerging Networking Experiments and Technologies (CONEXT), Dec 2012.

130. S. Singh, K. Sundaresan, A. Khojastepour, S. Rangarajan, S. Krishnamurthy, "One Strategy Does not Serve All: Tailoring Wireless Transmission Strategies to User Profiles", Proceedings of ACM Workshop on Hot Topics in Networks (Hotnets), Nov 2012.

131. E. Aryafar, M. Khojastepour, K. Sundaresan, S. Rangarajan and M. Chiang, "MIDU: Enabling MIMO Full Duplex", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Istanbul, Turkey, Aug 2012.

132. M. Arslan, K. Sundaresan, S. Krishnamurthy, S. Rangarajan, "Design and Implementation of an Integrated Beamformer and Uplink Scheduler for OFDMA Femtocells", Proceedings of ACM International Conference on Mobile Ad Hoc Networking and Computing (MOBIHOC), Jun 2012.

133. J. Yoon, M. Arslan, K. Sundaresan, S. Krishnamurthy, S. Banerjee, "A Distributed Resource Management Framework for Interference Mitigation in OFDMA Femtocell Networks", Proceedings of ACM International Conference on Mobile Ad Hoc Networking and Computing (MOBIHOC), Jun 2012.

134. S. Singh, M. Shahbazi, K. Pelechrinis, K. Sundaresan, S. Krishnamurthy, S. Addepalli, "A Case for Adaptive Sub-carrier Level Power Allocation in OFDMA Networks", Proc. of ACM International Conf. on Mobile Ad Hoc Networking and Computing (MOBIHOC), Jun 2012.

135. X. Zhang, M.A. Khojastepour, K. Sundaresan, S. Rangarajan, K. Shin, "Exploiting Interference Locality in Coordinated Multi-Point Transmission Systems", IEEE International Conference on Communications (ICC), June 2012.

136. S. Barghi, M. Khojastepour, K. Sundaresan, S. Rangarajan, "Characterizing the Throughput Gain of Single Cell MIMO Wireless Systems with Full Duplex Radios", International Symposium of Modeling and Optimization of Mobile, Ad Hoc, and Wireless Networks (WIOPT), May 2012.

137. K. Sundaresan and S. Rangarajan, "Adaptive Resource Scheduling in Wireless OFDMA Relay Networks", in IEEE International Conference on Computer Communications (INFOCOM), Mar 2012.

138. E. Aryafar, A. Khojastepour, K. Sundaresan, E. Knightly, S. Rangarajan, "ADAM: An Adaptive Beamforming System for Multicasting in Wireless LANs", in IEEE International Conference on Computer Communications (INFOCOM), Mar 2012.

139. M. Arslan, J. Yoon, K. Sundaresan, S. Krishnamurthy, S. Banerjee, "Characterization of Interference in OFDMA Femtocell Networks", in IEEE International Conference on Computer Communications (INFOCOM) Mini-Conf, Mar 2012.

140. A. Khojastepour, K. Sundaresan, S. Rangarajan, X. Zhang, S. Barghi, "The Case for Antenna Cancellation for Scalable Full Duplex Communications", Proceedings of ACM Workshop on Hot Topics in Networks (HotNets), Cambridge, Nov 2011.

141. M. Arslan, J. Yoon, K. Sundaresan, S. Krishnamurthy and S. Banerjee, "FERMI: A Femtocell Resource Management System for Interference Mitigation in OFDMA Networks", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Las Vegas, Sept 2011.

142. M. Khojastepour, A. Khajehnejad, K. Sundaresan, S. Rangarajan, "Adaptive Beamforming Algorithms for Wireless Link Layer Multicasting", Proceedings of IEEE Personal Indoor Mobile Radio Communications (PIMRC), Toronto, Sept 2011.

143. K. Sundaresan and S. Rangarajan, "Scheduling Algorithms for Video Multicasting with Channel Diversity in Wireless OFDMA Networks", Proceedings of ACM International Conference on Mobile Ad Hoc Networking and Computing (MOBIHOC), Paris, May 2011.

144. H. Zhang, Y. Jiang, K. Sundaresan, and S. Rangarajan, "Wireless Data Multicasting with Switched Beamforming Antennas", Proceedings of IEEE International Conference on Computer Communications (INFOCOM), Mini-Conf, Shanghai, China, April 2011.

145. S. Lakshmanan, K. Sundaresan, A. Khojastepour and S. Rangarajan, "Practical Multi-link Spatial Reuse in Wireless LANs", Proc. of IEEE International Conference on Broadband Communications, Networks, and Systems (BROADNETS), Athens, Greece, Oct 2010.

146. K. Sundaresan and S. Rangarajan, "Cooperation vs. Multiplexing: Multicast Scheduling Algorithms for OFDMA Relay Networks", Proceedings of ACM International Conference on Mobile Ad Hoc Networking and Computing (MOBIHOC), Chicago, Sept 2010.

147. S. Lakshmanan, K. Sundaresan, S. Rangarajan and R. Sivakumar, "The Myth of Spatial Reuse with Directional Antennas in Indoor Wireless Networks", Proceedings of Passive and Active Measurements Conference (PAM), Zurich, Switzerland, Apr 2010.

148. S. Lakshmanan, K. Sundaresan, S. Rangarajan and R. Sivakumar, "Practical Beamforming based on RSSI Measurements using Off-the-Shelf Wireless Clients", Proceedings of ACM SIGCOMM Internet Measurement Conference (IMC), Chicago, Nov 2009.

149. K. Sundaresan, K. Ramachandran, and S. Rangarajan, "Optimal Beam Scheduling for Multicasting in Wireless Networks", Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Beijing, China, Sept 2009.

150. K. Ramachandran, R. Kokku, K. Sundaresan, M. Gruteser and S. Rangarajan, "R2D2: Regulating Beam Shape and Rate as Directionality meets Diversity", Proceedings of ACM International Conference on Mobile Systems, Applications and Services (MOBISYS), Krakow, Poland, June 2009.

151. K. Sundaresan and S. Rangarajan, "Efficient Resource Management in OFDMA Femto Cells", Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), New Orleans, May 2009.

152. K. Sundaresan, and S. Rangarajan, "Efficient Algorithms for Leveraging Spatial Reuse in OFDMA Relay Networks", Proceedings of IEEE International Conference on Computer Communications (INFOCOM), Rio De Janeiro, Brazil, April 2009.

153. S. Lakshmanan, K. Sundaresan, R. Kokku, M. Khojastepour and S. Rangarajan, "Towards Adaptive Beamforming in Indoor Wireless Networks: An Experimental Approach", Proceedings of IEEE International Conference on Computer Communications (INFOCOM), Mini-Conf, Rio De Janeiro, Brazil, April 2009.

154. K. Sundaresan. X. Wang and M. Madihian, "Low Overhead Scheduling Algorithms for OFDMA Relay Networks", Proceedings of International Wireless Internet Conference (WICON), Maui, HI Nov 2008.

155. K. Sundaresan and S. Rangarajan, "On Coexistence of Unicast and Multicast Traffic in Relay- enabled Wireless Networks", Proceedings of IEEE International Conference on Broadband Communications, Networks, and Systems (BROADNETS), London, UK Sept 2008.

156. R. Kokku, K. Sundaresan, and G. Jiang, "Enabling Location-specific Real-time Mobile Applications", International Workshop on Mobility in the Evolving Internet Architecture (MobiArch), Seattle WA, USA, Aug 2008.

157. S. Lakshmanan, C.-L. Tsao, R. Sivakumar, and K. Sundaresan, "Securing Wireless Data Networks against Eavesdropping using Smart Antennas", in International Conference on Distributed Computing Systems (ICDCS), Beijing, China, June 2008.

158. K. Sundaresan and S. Rangarajan, "On Exploiting Diversity and Spatial Reuse in Relay- enabled Wireless Networks", Best Paper Award, Proc. of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Hong Kong, May 2008.

159. M. Blanco, R. Kokku, K. Ramachandran, S. Rangarajan, and K. Sundaresan, "On the Effectiveness of Switched Beam Antennas in Indoor Wireless Environments", Proceedings of Passive and Active Measurement Conference (PAM), Cleveland OH, USA, Apr 2008.

160. K. Sundaresan, X. Wang, and M. Madihian, "Scheduler Design for Heterogeneous Traffic in Cellular Networks with Multiple Channels", Proceedings of International Wireless Internet Conference (WICON), Austin TX, USA, Oct 2007.

161. K. Sundaresan, and R. Sivakumar, "Cooperating with Smartness: Using Heterogeneous Smart Antennas in Ad-Hoc Networks", Proceedings of IEEE International Conference on Computer Communications (INFOCOM), Anchorage, Alaska, May 2007.

162. K. Sundaresan, and K. Papagiannaki, "The Need for Cross-Layer Information in Access Point Selection", Proce. of Internet Measurement Conference (IMC), Rio De Janeiro, Oct 2006.

163. K. Sundaresan, S. Lakshmanan and R. Sivakumar, "On the Use of Smart Antennas in Multi- Hop Wireless Networks", Proceedings of International Conference on Broadband Communications, Networks, and Systems (BROADNETS), San Jose, USA, Oct 2006.

164. S. Lakshmanan, K. Sundaresan, and R. Sivakumar, "On Multi-Gateway Association in Wireless Mesh Networks", IEEE Workshop on Wireless Mesh Networks (WiMesh), Reston, VA, USA, September 2006.

165. K. Sundaresan, W. Wang and S. Eidenbenz, "Algorithmic Aspects of Communication in Ad- hoc Networks with Smart Antennas", Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Florence, Italy, May 2006.

166. K. Sundaresan and R. Sivakumar, "Routing in Ad-Hoc Networks with MIMO Links", Best Paper Award, Proceedings of IEEE International Conference on Network Protocols (ICNP), Boston, Nov 2005.

167. H. Shekhar, K. Sundaresan and M. A. Ingram, "Linear and non-linear receiver processing for MIMO ad-hoc wireless networks", Proceedings of IEEE International Symposium on Wireless Personal Multimedia Communications (WPMC), Aalborg, Denmark, Sept 2005.

168. Y. Zhu, K. Sundaresan and R. Sivakumar, "Practical Limits on Achievable Energy Improvements and Useable Delay Tolerance in Correlation Aware Data Gathering in Wireless Sensor Networks", Best Paper Award, Proceedings of IEEE International Conf. on Sensor and Ad Hoc Communications and Networks (SECON), Sept 2005.

169. A. Velayutham, K. Sundaresan , and R. Sivakumar, "Non-pipelined Relay Increases Throughput Capacity of Wireless Ad-hoc Networks", Proceedings of IEEE Intl. Conference on Computer Communications (INFOCOM), Mar. 2005.

170. K. Sundaresan , and R. Sivakumar, "A Unified MAC Framework for Ad-hoc Networks with Smart Antennas", Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Tokyo, Japan, May 2004.

171. K. Sundaresan, R. Sivakumar, and M. A. Ingram, "A Fair Medium Access Control Protocol for Ad-hoc Networks with MIMO Links", Proceedings of IEEE International Conference on Computer Communications (INFOCOM), Honk Kong, Mar 2004.

172. K. Sundaresan, V. Anantharaman, H.-Y. Hsieh, and R. Sivakumar, "ATP: A Reliable Transport Protocol for Ad-hoc Networks", Proceedings of ACM International

Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Annapolis, MD USA, June 2003.

173. V. Rajendran, K. Sundaresan , and S. Subramanian, "A Power Efficient Resource Allocation Scheme for Multi-user OFDM", Proceedings of IEEE International Conference on Personal Wireless Communications (ICPWC), New Delhi, India, December 2002.

174. A. Pachai, V. Rajendran, K. Sundaresan, and S. Subramanian, "Multiple Access Schemes for OFDM based Indoor Wireless Systems", Proceedings of The 8th National Conference on Communications (NCC), 2002, Mumbai, India.

Journals

175. Y-T. Lin, N. Matson and K. Sundaresan, "Bringing Collaborative Positioning to Native 5G Systems for Enhanced 2D and 3D Location Services", To appear in Proceedings of the ACM on Networking (PACM), Dec 2024.

176. A. Liu, Y-T. Lin, and K. Sundaresan, "View-agnostic Human Exercise Cataloging with Single MmWave Radar", Proceedings of ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp), Aug 2024.

177. H. A. Alhulayyil, J. Chen, K. Sundaresan, and Srikanth V. Krishnamurthy, "Priza: Throughput-efficient DAS Clustering of WiFi-PLC Extenders in Enterprises", IEEE Transactions on Wireless Communications, Aug 2024.

178. F. Ahmad, C. Shin, E. Chair, K. Sundaresan, R. Govindan, "AeroTraj: Trajectory Planning for Fast, and Accurate 3D Reconstruction using a Drone-based LiDAR". Proceedings of ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp), Oct 2023.

179. M. Dasari, R. Seshadri, K. Sundaresan, S. Das, "RoVaR: Robust Multi-agent Tracking through Dual-layer Diversity in Visual and RF Sensing", Proceedings of ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/ UbiComp), Oct 2023.

180. M. Moradi, K. Sundaresan, E. Chai, S. Rangarajan, "SkyCore: Moving Core to the Edge for Un-tethered and Reliable UAV-based LTE Networks", Communications of the ACM, Research Highlights, Jan 2021.

181. M. Moradi, K. Sundaresan, E. Chai, S. Rangarajan, "SkyCore: Moving Core to the Edge for Un-tethered and Reliable UAV-based LTE Networks", ACM Sigmobile, GetMobile Magazine, Research Highlights, 2019.

182. J. Yoon, M. Arslan, K. Sundaresan, S. Krishnamurthy, S. Bannerjee, "Characterization of Interference in OFDMA Small-cell Networks", IEEE Transactions on Vehicular Technology, Sept 2018.

183. M. Lotfi, K. Sundaresan, M. Khojastepour, S. Sarkar, S. Rangarajan, "Economics of Quality- Sponsored Data in Non-Neutral Networks", IEEE/ACM Transactions on Networking, 2017.

184. S. Singh, K. Sundaresan, S. Krishnamurthy, X. Zhang, M. Khojastepour, "Trinity: Tailoring Wireless Transmission Strategies to User Profiles in Enterprise Wireless Networks", in IEEE/ACM Transactions on Networking, 2017.

185. J. Yoon, K. Sundaresan, M. Khojastepour, S. Rangarajan, S. Banerjee, "Joint Multi-cell Beamforming and Client Association in OFDMA Small-cell Networks", in IEEE Transactions on Mobile Computing, 2016.

186. K. Sundaresan, M. Arslan, S. Singh, S. Rangarajan, S. Krishnamurthy, "FluidNet: A Flexible Cloud-based Radio Access Network for Small Cells", in IEEE/ACM Transactions onNetworking, 2016.

187. M. Arslan, K. Sundaresan, S. Krishnamurthy, S. Rangarajan, "iBUS: An Integrated Beamformer and Uplink Scheduler for OFDMA Femtocells", in IEEE/ACM Transactions on Networking, 2016.

188. M. Arslan, K. Sundaresan, S. Rangarajan, "Software-defined Networking in Cellular Radio Access Networks: Potential and Challenges", IEEE Communications Magazine, Special Issue on Extremely Dense Wireless Networks, Jan 2015.

189. J. Yoon, M. Arslan, K. Sundaresan, S. Krishnamurthy, S. Banerjee, "Self-Organizing Resource Management Framework in OFDMA Femtocells", IEEE Transactions on Mobile Computing, 2015.

190. M. Arslan, I. Singh, S. Singh, H. Madhyastha, K. Sundaresan, S. Krishnamurthy, "CWC: A Distributed Computing Infrastructure using Smartphones", in IEEE Transactions on Mobile Computing, 2015.

191. S. Singh, M. Shahbazi, K. Pelechrinis, K. Sundaresan, S. Krishnamurthy, K. Satish, "Adaptive Sub-carrier Level Power Allocation in OFDMA Networks", IEEE Transactions on Mobile Computing, 2015.

192. A. Atya, S. Singh, I. Broustis, K. Sundaresan, S. Krishnamurthy, "Exploiting Subcarrier Agility to Alleviate Active Jamming Attacks in Wireless Networks", in IEEE Transactions on Mobile Computing, 2015.

193. K. Sundaresan, S. Rangarajan, "Video Multicasting with Channel Diversity in Wireless OFDMA Networks", in IEEE Transactions on Mobile Computing, 2014.

194. K. Sundaresan, S. Rangarajan, "Cooperation vs. Multiplexing: Multicast Scheduling Algorithms for OFDMA Relay Networks", in IEEE/ACM Transactions on Networking, 2014.

195. E. Aryafar, M. Khojastepour, K. Sundaresan, S. Rangarajan, M. Chiang, "ADAM: An Adaptive Beamforming System for Multicasting in Wireless LANs", in IEEE/ACM Transactions on Networking, 2013.

196. M. Arslan, J. Yoon, K. Sundaresan, S. Rangarajan, S. Krishnamurthy, "A Resource Management System for Interference Mitigation in Enterprise OFDMA Femtocells", in IEEE/ACM Transactions on Networking, 2013.

197. H. Zhang, J. Tanis, K. Sundaresan, S. Rangarajan and B. Zhao, "Wireless Multicast Scheduling with Switched Beamforming Antennas", in IEEE/ACM Transactions on Networking, 2012.

198. K. Sundaresan and R. Sivakumar, "Cooperating with Smartness: Using Heterogeneous Smart Antennas in Multi-hop Wireless Networks", in IEEE Transactions on Mobile Computing, Dec 2011.

199. S. Lakshmanan, K. Sundaresan and R. Sivakumar, "Multi-gateway Association in Wireless Mesh Networks", in Ad-Hoc Networks Journal, Elsevier, May 2009.

200. K. Sundaresan, and R. Sivakumar, "Routing in Ad-hoc Networks with MIMO Links: Optimization Considerations and Protocols", in Computer Networks Journal, Elsevier, 2008.

201. K. Sundaresan and R. Sivakumar, "A Unified MAC Framework for Ad-hoc Networks with Smart Antennas", in IEEE/ACM Transactions on Networking, 2007.

202. K. Sundaresan, and R. Sivakumar, "Ad-hoc Networks with Heterogeneous Smart Antennas: Performance Analysis and Protocols", in Wireless Communication and Mobile Computing Journal, Special Issue on Wireless Ad-hoc Networks: Technologies and Challenges, 2006.

203. K. Sundaresan, V. Anantharaman, H-Y. Hsieh and R. Sivakumar, "ATP: A Reliable Transport Protocol for Ad-hoc Networks", in IEEE Transactions on Mobile Computing, Nov-Dec 2005.

204. K. Sundaresan, R. Sivakumar, M. A. Ingram and T-Y. Chang, "Medium Access Control in Ad- hoc Networks with MIMO Links: Optimization Considerations and Algorithms", in IEEE Transactions on Mobile Computing, Oct-Nov 2004.

205. K. Sundaresan, H.-Y. Hsieh, and R. Sivakumar, "IEEE 802.11 over Multi-hop Wireless Networks: Problems and New Perspectives", in Ad-hoc Networks Journal, Elsevier, Feb 2004. WCMC

206. V. Anantharaman, S.-J. Park, K. Sundaresan, and R. Sivakumar, "TCP Performance over Mobile Ad-hoc Networks: A Quantitative Study", In Wireless Communications and Mobile Computing Journal (WCMC), Special Issue on Performance Evaluation of Wireless Networks, Mar 2004.

207. V. Rajendran, K. Sundaresan and S. Subramanian, "Performance of an OFDM Based Downlink Multiple Access System for Indoor Wireless Communications", in Wireless Personal Communications, Kluwer Academic Publishers, April 2003.

Book Chapters

208. K. Sundaresan, S-J. Park, and R. Sivakumar, "Transport Layer Solutions for Ad-hoc Networks", in Ad-hoc Networks: Technologies and Protocols, Kluwer, 2005.

Posters/Demos

209. J. Cho, K. Sundaresan, R. Mahindra, S. Rangarajan, J. V-d. Merwe, "ACACIA: Context-aware Edge Computing over Mobile Networks", Demo, Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), Oct 2016.

210. K. Sundaresan and R. Sivakumar, "Rate vs. Range vs. Reliability: How to Best Exploit MIMO in Ad-hoc Networks", Poster, Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Illinois, May 2005.

211. Y. Zhu, K. Sundaresan and R. Sivakumar, "Exposing Two Critical Myths About Correlation- Aware Data Aggregation", Poster, Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Illinois, May 2005.

212. K. Sundaresan and R. Sivakumar, "On the Medium Access Control Problem in Ad-hoc Networks with Smart Antennas", Poster, Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), MD USA, June 2003.

Talks (Appendix C)

Tutorials and Keynotes

- "Collaborative Positioning: From Theory To Practice", Keynote at ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization (WiNTECH), co-located with ACM MobiCom, Nov 2025.
- "Digital 1 Spectrum Twins: The `Seen' and the `Unseen'", Keynote at IEEE International Conference on Digital Twins and Parallel Intelligence, Apr 2025.
- "Architecting Networks in the Sky", Keynote at ACM Workshop on Micro Aerial Vehicle Networks, Systems, and Applications (DroNet), Co-located with ACM MobiSys, July 2022.
- "Networks in the Sky: Potential and Challenges", Tutorial at IEEE-sponsored COMSNETS, India, Jan 2022.
- "Architecting Networks in the Sky", Keynote talk at ACM DroneNet workshop on Micro Aerial Vehicle Networks, Systems, and Applications, co-located with ACM Mobisys, June 2022.
- "5G: An Evolution towards a Revolution", Tutorial at ACM MobiCom, India, Oct 2018.
- "Making Mobile Networks Fly", Keynote talk at ACM S3 workshop, co-located with ACM MobiCom, Oct 2018.
- "5G: An Evolution towards a Revolution", Tutorial at Signal Processing and Communications Conference (SPCOM), IISC, Bengaluru, India, July 2018.
- "Evolving Shades of Wireless Access Research", ACM Sigmobile Rockstar Award (Plenary) talk, ACM MobiCom, Oct 2016.
- "Cloud-driven Architectures for Next Generation Small Cell Networks", Keynote at ACM MobiArch workshop, co-located with ACM MobiCom, 2013.

Invited Panels and Talks

- "Networks in the Sky: Enabling Ubiquitous Connectivity and Sensing", Seminar talk at Georgia Tech, School of ECE, Feb 2021.
- "Untethering 5G for Ubiquitous Connectivity", Invited talk at Comsnets, Jan 2021.
- "Making Mobile Networks Fly", Seminar talk (Leaders and Innovators Series), at Texas A&M University, Nov 2019.
- "Triple Play: The Confluence of Connectivity, Computing and User Experience in Mobile Networks", School of Computer Science, University of California, Santa Barbara, Apr 2017.
- "Connectivity meets Computing: A Wireless Networking Perspective", School of Electrical Engineering, University of Washington, Seattle, Feb 2017.
- "Converged Wireless Access: The New Normal", Talk at Wireless Co-existence Workshop, Univ. of Washington, June 2016.
- "Blurred Boundaries in Future Wireless Access", Talk at 5G Forum, UCSD, May 2016.
- "Connectivity meets Computing: A Wireless Networking Perspective", School of Computer Science, University of Utah, Apr 2016.
- "Blurred Boundaries in Future Wireless Access", Talk at ACM Wireless Networking Industry Day, Mar 2016.
- "Blurred Boundaries in Future Wireless Access", Talk at ACM HotWireless Workshop, Sept 2015.
- "Connectivity meets Computing in the Path to 5G", Talk at Telecom ParisTech Workshop on 5G, Sept 2015.
- "Connectivity meets Computing: A Wireless Networking Perspective", School of ECE, UCSD, Feb 2015.
- "Cloud-driven Architectures for Next Generation Small Cell Networks", Talk at University of Delaware, CS seminar, 2013.
- "Realizing the Potential of Small Cells: An Experimental Approach", Talk at Columbia University, EE seminar, 2012.
- MIMO in Sensor and Ad Hoc Networks: Challenges and Opportunities" Panel at IEEE SECON 2008.

Professional Activities (Appendix D)

Editorial Board

Associate Editor, IEEE Transactions on Mobile Computing, Associate Editor, 2012-2018.

Conference/Workshop Organization

- Tutorial/Workshop Co-chair, ACM MobiCom 2025.
- Area Chair for IEEE ICNP, 2020.
- Track Chair for IEEE ICDCS 2017, "Mobile and Wireless Network Computing" Track.
- Program Co-Chair for ACM MobiCom 2016.
- Program Co-Chair for IEEE ICC Workshop on "LTE in Unlicensed Bands: Potential and Challenges", June 2015.
- Program Co-chair for IEEE SECON 2013.
- Poster Chair for ACM MobiHoc 2012.
- Publicity Chair for ACM MobiCom 2010.
- Publicity Chair for ACM MobiHoc 2010.
- Poster and Demo Chair for IEEE SECON 2010.
- Program Co-chair for IEEE Workshop on Wireless Mesh Networks (WiMesh) 2009; co- located with IEEE SECON 2009.
- Publications Chair for ACM Workshop on Dependability Issues in Wireless Ad-hoc and Sensor Networks (DIWANS) 2006; co-located with ACM MOBICOM 2006.

Award Committees

- ACM Sigmobile Test of Time Awards, 2023
- ACM Sigmobile Rockstar Award, 2017-2019

Technical Program Committee Memberships

- ACM MOBICOM 2008, 2011, 2012, 2014 - 2024.
- ACM SIGCOMM 2009.
- IEEE INFOCOM 2012, 2013, 2014, 2015 (advisory TPC), 2016, 2017.
- IEEE SECON 2009, 2012.
- IFIP Networking 2007, 2008.
- IEEE ICC 2010, 2012.
- IEEE MASS 2009.
- IEEE WoWMoM 2010.
- IEEE WiMesh 2009, 2010.

Referee/Panelist for Journals, Conferences and Review Panels

- Journals: IEEE/ACM — Transactions on Networking, Mobile Computing, Wireless Communications, Journal on Selected Areas in Communications, Mobile Computing and Communications Review
- Conferences: ACM — MobiCom, SIGCOMM, CONEXT, IEEE — INFOCOM, ICNP
- Evaluation committee of "MIMONet" project - a 3 year project on MIMO networks funded by Italian National Research Council, along with Dr. Robert Heath; Jan 2012.
- NSF Panelist for CISE, Network Technology and Systems 2012, 2013, 2014, 2017, 2019, 2023.

Ph.D. Dissertation Committees

- Nathan Blinn, School of ECE, Georgia Tech, Atlanta, 2025.
- Haige Chen, School of CS, Georgia Tech, Atlanta, 2025.
- Jingyuan Zhang, School of ECE, Georgia Tech, Atlanta, 2025.
- Ang Deng, School of ECE, Georgia Tech, Atlanta, 2024.
- Mohammad Saad Zia, School of ECE, Georgia Tech, Atlanta, 2023.
- Shruti Lall, School of ECE, Georgia Tech, Atlanta, 2022.
- Yuchen Liu, School of ECE, Georgia Tech, Atlanta, 2022.
- Mallesham Dasari, Computer Science, Stony Brook University, New York, 2021.
- Mohammad Rostami, Computer Science, Univ. of Massachusetts, Amherst, 2021.
- Swadhin Pradhan, Computer Science, University of Texas, Austin, 2020.
- Ashutosh Dhekne, School of ECE, UIUC, 2019.