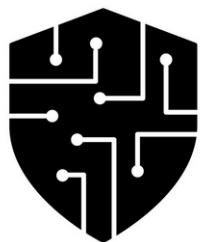


Google v. Security First Innovations



Security First Innovations

February 27, 2025

IPR2024-00212, -00214, -00215
U.S. Patent Nos. 11,178,116; 11,068,609; 10,452,854

Sullivan & Cromwell LLP
Andrei Iancu
Stephen Elliott
Haley Sanders

Lowenstein & Weatherwax LLP
Nathan Lowenstein

Exhibit 2048

Petitioner Had Obligation To Make Its Case In The Petition



“the expedited nature of IPRs bring with it **an obligation for petitioners to make their case in their petition to institute.**”

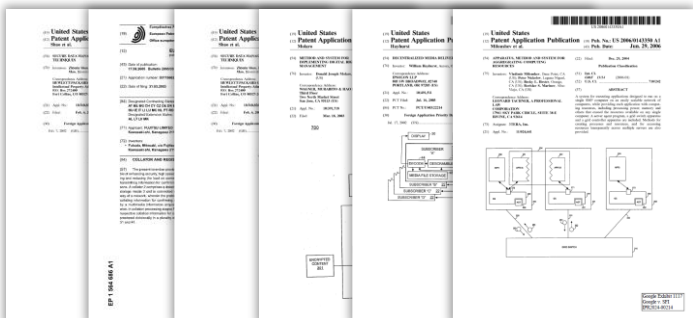
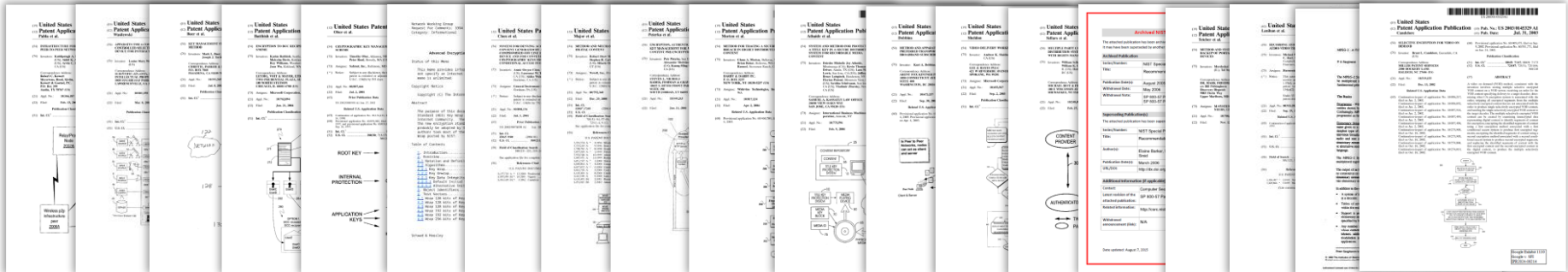
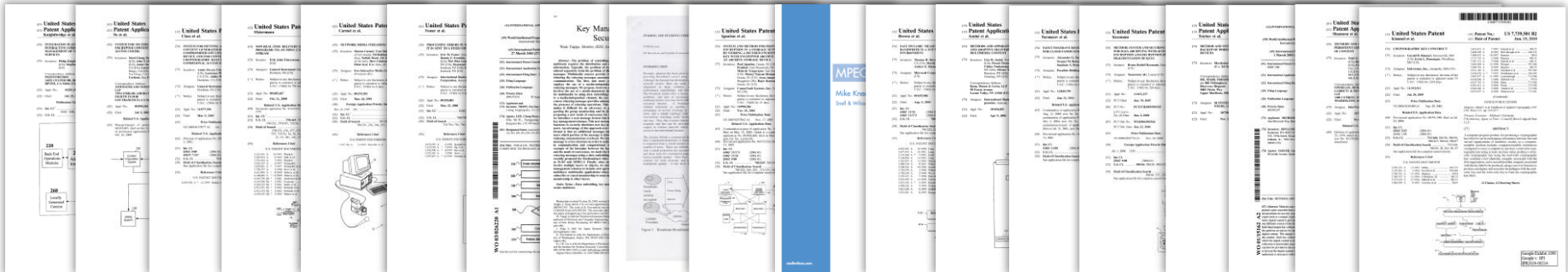
Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd., 821 F.3d 1359, 1369 (Fed. Cir. 2016)



“Petitioner **may not submit new** evidence or **argument** in reply that it could have presented earlier, e.g. **to make out a prima facie case of unpatentability.**”

Consolidated Trial Practice Guide, 73 (Nov. 2019)

Petitioner Failed To Make Its Case: Over Forty New Exhibits To Support Replies In Each Case



Petitioner Failed To Make Its Case: 118 To 136-Page, ~25,000 To 29,000-Word Reply Declarations

Petition



Reply Declaration



Petitioner's Unexplained Citations To The Reply Declarations And New Exhibits Should Be Disregarded



“Arguments must not be incorporated by reference from one document into another document. **Combined...replies...are not permitted.”**

37 C.F.R. § 42.6(a)(3)

“[T]he Petition includes citations to the Declaration to support conclusory statements for which the Petition **does not otherwise provide an argument or explanation** ... This practice ... **amounts to incorporation by reference** ... [and] serves to **circumvent the page limits** ... while imposing on our time by **asking us to sift through** ... [the] Declaration ... **to locate the specific arguments corresponding to the numerous paragraphs cited** to support Petitioner’s assertions.”

Cisco Sys., Inc. v. C-Cation Techs., LLC, IPR2014-00454, Paper 12, 9-10 (Aug. 29, 2014)
(Informative)

Petitioner Improperly Incorporates The Reply Declarations By Reference

E.g., -00215 Reply at 18 Cites 22 Paragraphs Of Reply Decl., ¶¶157-179, But Does Not Discuss Any Of It

134. Similarly, EX1084 at 10(2) mentions that an “OTP packet” can be “A check or series of multiple data as one over IP network.” Thus, EX1084 contemplates SFT’s argument that something called a “packet” cannot also be “data or series of data.”

135. In another example, EX1081 (at 4.7.2) describes a system that “transmitting a set into a plurality of data blocks, including one or more of the data blocks into 1. data checks,” where “[a] set of each data check can correspond to a packet” (i.e., “a set is only one check per packet”). Thus, EX1081 contemplates SFT’s argument that something called a “packet” cannot also be “data check,” if a data set or a packet is only divisible into data checks rather than itself being the data check.

136. Thus, the above references contradict any argument that SFT is incorrect in its argument that the POAs would understand that packets cannot be clearly, purely between packets, could a user transmit, also be “divided data data checks” (008, 078). The above references demonstrate that POAs would disagree, as do I.

III. MY REPLY TO SFT REGARDING GROUND 1 IS STILL MY OPINION THAT I CHALLENGED CLAIMS WOULD HAVE BEEN OBVIOUS TO OVERGROUND.

137. For Ground 1, the above references, SFT only disputes whether China discloses, as an obvious disclosure of China would have performed.

-83-

138. In my First Declaration, I discussed several alternative arguments demonstrating that China had anticipated and/or understood obvious (i.e., including limitation [C]) based on disclosures in China, POAs’ understanding thereof, and/or use of conventional, well-known encryption techniques (all of which I substantiated with multiple prior art references). First Declaration, ¶¶107-114. In my opinion, these opinions are still correct in SFT’s 008 and Dr. Rubin’s declaration that the disclosures that [C] and/or other references of the challenged claims were not disclosed and rendered obvious over China.

139. For Ground 1, I have been asked to focus the Reply Declaration on one of my alternative opinions for Ground 1. Specifically, I have been asked to focus on my opinion on the obviousness of my argument that POAs had access to encrypt China’s disclosures with their encryption key (“KEY”). As I discussed in my First Declaration, POAs had access to the data to understand the data keys, thus, in multiple conventional references (and documented use, a well-known, conventional technique in the prior art. First Declaration, ¶¶111-114) using conventional disclosed data before, (EIA, A) SFT does not appear to dispute that encrypting encryption keys with KEAs, was known.

-84-

or that encrypting China’s data keys with a KEA means [C] under SFT’s contention.”

140. In my First Declaration, ¶¶114-115, I also discussed (EIA, A) disclosures regarding public key encryption, (i.e., Chinese before (EIA, A), the reasoning behind my opinion that it would have been obvious to POAs to use a conventional KEA to encrypt China’s data key was fundamentally different from, and not dependent on, technology regarding China’s disclosure of using public key encryption. Instead, my alternative opinions were not as presented as POAs’ background knowledge and prior art references that explicitly provided POAs with sufficient to encrypt China’s data key and a reasonable expectation of success in doing so. This alternative opinion was independent of China’s disclosures involving public key encryption. In other words, even if China and nothing of all other public key encryption (which China does not use to encrypt data keys), it is not and will not any argument that POAs would have had access to, and a reasonable expectation of success in doing so, encrypt China’s data keys with a conventional key encryption key (KEA), for its well-known technique that I documented with conventional in the prior art. The disclosure that I documented with conventional in the prior art.

141. I have offered alternative opinions to both China, and Poas, and/or to make obvious [C] under a proper claim scope. See First Declaration, ¶¶104-114.

-85-

142. In my First Declaration, ¶¶114-115, I also discussed (EIA, A) disclosures regarding public key encryption, (i.e., Chinese before (EIA, A), the reasoning behind my opinion that it would have been obvious to POAs to use a conventional KEA to encrypt China’s data key was fundamentally different from, and not dependent on, technology regarding China’s disclosure of using public key encryption. Instead, my alternative opinions were not as presented as POAs’ background knowledge and prior art references that explicitly provided POAs with sufficient to encrypt China’s data key and a reasonable expectation of success in doing so. This alternative opinion was independent of China’s disclosures involving public key encryption. In other words, even if China and nothing of all other public key encryption (which China does not use to encrypt data keys), it is not and will not any argument that POAs would have had access to, and a reasonable expectation of success in doing so, encrypt China’s data keys with a conventional key encryption key (KEA), for its well-known technique that I documented with conventional in the prior art. The disclosure that I documented with conventional in the prior art.

143. I have offered alternative opinions to both China, and Poas, and/or to make obvious [C] under a proper claim scope. See First Declaration, ¶¶104-114.

-86-

using KEAs were well-known.” And China itself discloses the device is provided different levels of access to various data in different groups of people. First Declaration, ¶¶114-115.

144. SFT argues that Dr. Rubin’s declaration that the encryption method described in reference to China’s Figure 7 is not the encrypted data of that being stored with a data-encryption key that is itself not encrypted (i.e., a plaintext key is stored with an encrypted data). First Declaration, ¶¶114-115. SFT and Dr. Rubin do not dispute that such encrypted data key as China that is stored with an encrypted data is not the key to which that data (e.g., China’s publications per Figure 7). (See [009] (009, 078, 079, 080, 081, 082, 083, 084, 085, 086, 087, 088, 089, 090, 091, 092, 093, 094, 095, 096, 097, 098, 099, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000).

145. Even with China’s disclosure, my SFT still recognizes that an attack could be made “insecure” (China’s) if encrypted data of the attack.

146. China discloses implementing protection for the watchdogs. See China, [009] (009, 078, 079, 080, 081, 082, 083, 084, 085, 086, 087, 088, 089, 090, 091, 092, 093, 094, 095, 096, 097, 098, 099, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000).

147. China discloses implementing protection for the watchdogs. See China, [009] (009, 078, 079, 080, 081, 082, 083, 084, 085, 086, 087, 088, 089, 090, 091, 092, 093, 094, 095, 096, 097, 098, 099, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 35

Petitioner Improperly Incorporates New Evidence By Reference

E.g., -00214 Reply at 9 Cites Seven New Exhibits,
But Does Not Discuss Any Of It

United States
Patent Application Publication
Pub. No. US 2002/00249 A1
Pub. Date: Jan. 23, 2002

ABSTRACT

A method of determining whether a user is a user of a system or a user of a system is disclosed. The method includes receiving a request from a user to determine whether the user is a user of a system or a user of a system. The method also includes determining whether the user is a user of a system or a user of a system based on the request. The method further includes providing a response to the user based on the determination.

FIG. 1

Google Exhibit 1071
Google = 1071
IPR-1071-00114

United States Patent
Patent No. US 6,252,227 B1
Date of Patent: Aug. 14, 2001

ABSTRACT

A method of determining whether a user is a user of a system or a user of a system is disclosed. The method includes receiving a request from a user to determine whether the user is a user of a system or a user of a system. The method also includes determining whether the user is a user of a system or a user of a system based on the request. The method further includes providing a response to the user based on the determination.

FIG. 1

Google Exhibit 1071
Google = 1071
IPR-1071-00114

United States Patent
Patent No. US 6,717,677 B1
Date of Patent: Aug. 5, 2006

ABSTRACT

A method of determining whether a user is a user of a system or a user of a system is disclosed. The method includes receiving a request from a user to determine whether the user is a user of a system or a user of a system. The method also includes determining whether the user is a user of a system or a user of a system based on the request. The method further includes providing a response to the user based on the determination.

FIG. 1

Google Exhibit 1071
Google = 1071
IPR-1071-00114

United States Patent
Patent No. US 6,205,675 B1
Date of Patent: Nov. 13, 2000

ABSTRACT

A method of determining whether a user is a user of a system or a user of a system is disclosed. The method includes receiving a request from a user to determine whether the user is a user of a system or a user of a system. The method also includes determining whether the user is a user of a system or a user of a system based on the request. The method further includes providing a response to the user based on the determination.

FIG. 1

Google Exhibit 1071
Google = 1071
IPR-1071-00114

United States Patent
Patent No. US 6,682,329 B1
Date of Patent: Dec. 9, 2000

ABSTRACT

A method of determining whether a user is a user of a system or a user of a system is disclosed. The method includes receiving a request from a user to determine whether the user is a user of a system or a user of a system. The method also includes determining whether the user is a user of a system or a user of a system based on the request. The method further includes providing a response to the user based on the determination.

FIG. 1

Google Exhibit 1071
Google = 1071
IPR-1071-00114

United States Patent Application Publication
Pub. No. US 2002/00249 A1
Pub. Date: Jan. 23, 2002

ABSTRACT

A method of determining whether a user is a user of a system or a user of a system is disclosed. The method includes receiving a request from a user to determine whether the user is a user of a system or a user of a system. The method also includes determining whether the user is a user of a system or a user of a system based on the request. The method further includes providing a response to the user based on the determination.

FIG. 1

Google Exhibit 1071
Google = 1071
IPR-1071-00114

United States Patent Application Publication
Pub. No. US 2002/00249 A1
Pub. Date: Jan. 23, 2002

ABSTRACT

A method of determining whether a user is a user of a system or a user of a system is disclosed. The method includes receiving a request from a user to determine whether the user is a user of a system or a user of a system. The method also includes determining whether the user is a user of a system or a user of a system based on the request. The method further includes providing a response to the user based on the determination.

FIG. 1

Google Exhibit 1071
Google = 1071
IPR-1071-00114

United States Patent Application Publication
Pub. No. US 2002/00249 A1
Pub. Date: Jan. 23, 2002

ABSTRACT

A method of determining whether a user is a user of a system or a user of a system is disclosed. The method includes receiving a request from a user to determine whether the user is a user of a system or a user of a system. The method also includes determining whether the user is a user of a system or a user of a system based on the request. The method further includes providing a response to the user based on the determination.

FIG. 1

Google Exhibit 1071
Google = 1071
IPR-1071-00114

Demonstrative Exhibit – Not Evidence

-00212 Sur-Reply, 1-2; -00214 Sur-Reply, 1-2; -00215 Sur-Reply, 1-2

7

Petitioner's Grounds

1. Foster Grounds

a) Foster and Hayhurst (IPR2024-00212/215)

b) Foster Alone (IPR2024-00214)

2. Orsini Grounds (IPR2024-00214/215)

3. Tajima Grounds (IPR2024-00212)

Petitioner Raises Foster-Hayhurst Ground In IPR2024-00212, -00215

Case No. IPR2024-00212
Patent No. 11,178,116

Ground Number and Reference(s)		Claims	Basis
1	Tajima (EX1005)	1, 5-8	§§102/103
2	Tajima, Foster (EX1006)	1-2, 9, 11-14	§103
3	Tajima, Rivest (EX1034)	9-14	§103
4	Tajima, Rivest, Shyu (EX1016)	1-3, 6	§103
5	Foster, Hayhurst (EX1007)	1-2, 5, 9, 11	§103

Case No. IPR2024-00215
Patent No. 10,452,854

Ground Number and Reference(s)		Claims	Basis
1	Orsini (EX1005)	1-10	§§102/103
2	Foster (EX1006), Hayhurst (EX1007)	1-10	§103

The -00212/-00214 Foster-Hayhurst Arguments Are Substantively Identical

Case IPR2024-00215 Patent 10,452,854

III. THE FOSTER-HAYHURST GROUND FAILS (ALL CLAIMS, GROUND 2).	32
A. Petitioner Fails To Demonstrate That Hayhurst Is Analogous Art.	32
1. Hayhurst And The '854 Patent Do Not Share The Same Field Of Endeavor.	33
2. Hayhurst Is Not Reasonably Pertinent To The Problem The Inventors Of The '854 Patent Were Addressing.	38
B. Petitioner Fails To Demonstrate That A POSITA Would Be Motivated To Combine Foster And Hayhurst (All Claims, Ground 2).	41
1. Foster Provides Synchronized Transmission To Avoid Delays.	42
2. Hayhurst's System Does Not Allow For Real-Time Streaming Because Its System Requires Delays.	47
3. Petitioner's Combination Involves Storing And Distributing All Of Foster's Content Units Per Hayhurst's Methodology Which Precludes Real-Time Streaming.	49
4. A POSITA Would Not Be Motivated To Combine Foster And Hayhurst As Proposed.	51

Case IPR2024-00212 Patent 11,178,116

IV. THE FOSTER-HAYHURST GROUND FAILS (GROUND 5, CLAIMS 1-2, 5, 9 AND 11).	38
A. Petitioner Fails To Demonstrate That Hayhurst Is Analogous Art.	38
1. Hayhurst And The '116 Patent Do Not Share The Same Field Of Endeavor.	39
2. Hayhurst Is Not Reasonably Pertinent to the Problem the Inventors of the '116 Patent Were Addressing.	44
B. Petitioner Fails To Demonstrate That A POSITA Would Be Motivated To Combine Foster And Hayhurst.	47
1. Foster Provides Synchronized Transmission To Avoid Delays.	48
2. Hayhurst's Goal Is Directed to Reducing the Bandwidth Requirements for the Provision of Content Where Immediate, Random Access Is Not Required.	53
3. Petitioner's Combination Involves Storing and Distributing All of Foster's Content Units per Hayhurst's Method.	55
4. A POSITA Would Not Be Motivated To Combine Foster And Hayhurst As Proposed.	56

Foster-Hayhurst Fails (IPR2024-00212, -00215)

➤ Hayhurst Is Not Analogous Art (IPR2024-00212, -00215)

- ❑ No Motivation To Combine Foster-Hayhurst Shown (IPR2024-00212, -00215)
- ❑ Foster's Packets/Payloads Are Not Shares/Chunks (IPR2024-00214, -00215)

Petitioner Has Burden To Prove Hayhurst Is Analogous



“A reference **qualifies as prior art** for an obviousness determination under § 103 **only when it is analogous** to the claimed invention.”

In re Klein, 647 F.3d 1343, 1348 (Fed. Cir. 2011)

“We agree with Sanofi that **[Petitioner] did not carry its burden** to argue that de Gennes is analogous to the '614 patent.”

Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.,
66 F.4th 1373, 1377 (Fed. Cir. 2023)

Petition Did Not Argue Hayhurst Is Analogous Art



Two Analogous Art Tests



“Two criteria have evolved for determining whether prior art is analogous:

- (1) whether the art is from the **same field of endeavor**, regardless of the problem addressed, and
- (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is **reasonably pertinent to the particular problem with which the inventor is involved.**”

In re Clay, 966 F.2d 656, 658-59 (Fed. Cir. 1992)
(modified formatting)

Clay: Field Of Endeavor Test Is Strictly Applied



“Clay’s field of endeavor is the **storage of refined liquid hydrocarbons**. The field of endeavor of Sydansk’s invention, on the other hand, is the **extraction of crude petroleum**. The Board clearly erred in considering Sydansk to be within the same field of endeavor as Clay’s.”

In re Clay, 966 F.2d 656, 659 (Fed. Cir. 1992)



Oil storage

Different Fields



Oil extraction

Clay is the leading analogous art case, cited 46x by CAFC

Wang: FOE Test Is Strictly Applied



“The Allen-Bradley art is not in the same field of endeavor as the claimed subject matter merely because it relates to memories. It involves memory circuits in which modules of varying sizes may be added or replaced; in contrast, the subject patents teach compact modular memories.”

Wang Labs., Inc. v. Toshiba Corp.,
993 F.2d 858, 864 (Fed. Cir. 1993)

SIMMs for Industrial Machines



Different Fields

SIMMs for PCs



Petitioner/Dr. Bhattacharjee Recognized The '854 And Hayhurst Have Different Fields

DECLARATION OF AVIEL D. RUBIN, PH.D.



100. As an initial matter, I note that Petitioner and Dr. Bhattacharjee admit that '854 and Hayhurst have different fields. According to Petitioner and Dr. Bhattacharjee, the '854's field is securing data while Hayhurst's is decentralized electronic media delivery. Pet., 4 (“[t]he '854 patent relates to techniques for securing electronic data from unauthorized access.”); Ex. 1003 [Bhattacharjee-Decl.] ¶ 33 (same); Pet., 59 (“Hayhurst concerns ‘*electronic media delivery, such as video-on-demand*’”); Ex. 1003 [Bhattacharjee-Decl.] ¶ 178 (same); Ex. 2034 [Bhattacharjee-Depo.] 101:19-25. I agree that the '854 and Hayhurst have different fields.

Reply: Petitioner Still Does Not Identify The '854's Field

PETITIONER'S REPLY TO PATENT OWNER RESPONSE

SFI argues “the '854's field is securing data,” including securely storing and communicating data. POR, 33-35. Hayhurst is in that field.

REPLY DECLARATION OF SAMRAT BHATTACHARJEE, PH.D.

11. SFI argues “the '854's field is securing data,” including securely storing and communicating the secured data. POR, 33-35. I have not been asked to opine on whether SFI has identified the correct field of endeavor for the '854 patent. That is not necessary to my opinion because, for the reasons I discuss below, it is my opinion Hayhurst is (at least) in the same field of endeavor that SFI has identified for the '854 patent.



Traditional Sources For Discerning Field Of Endeavor

- “The Board looked to the **written description** and **claims** ... to determine the field of endeavor for each reference. ... The Board also cited the **title** of the ’752 patent” *Airbus S.A.S. v. Firepass Corp.*, 941 F.3d 1374, 1380-81 (Fed. Cir. 2019)
- “[T]he **specification** of each reference includes a ‘**Field of the Invention**’ section that distinctly describes each applicable field of endeavor.” *Airbus*, 941 F.3d at 1381 n.8
- “Elson discloses a ‘system for sensing a characteristic of fluid flowing’ ... Elson **abstract**, 1:56-2:2. Barker is directed to a fluid temperature sensor, having a through lumen for conducting fluid. Barker **abstract**, 1:64-66.” *Kamstrup A/S v. Axioma Metering UAB*, 43 F.4th 1374, 1384 (Fed. Cir. 2022)
- “The Board ... correctly set the field ... by consulting the **structure and function of the claimed invention** ...” *In re Bigio*, 381 F.3d 1320, 1326 (Fed. Cir. 2004)
- “Tellingly, the ’649 patent itself refers to ‘the prior art padlock’ in the **background of the invention**.” *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1237-38 (Fed. Cir. 2010)



Traditional Sources: '854's Field Is "Securing Data"

(54) **SECURE DATA PARSER METHOD AND SYSTEM**

(57) **ABSTRACT**
A secure data parser is provided that may be integrated into any suitable system for securely storing and communicating data. The secure data parser parses data and then splits the data into multiple portions that are stored or communicated distinctly. Encryption of the original data, the portions of data, or both may be employed for additional security. The secure data parser may be used to protect data in motion by splitting original data into portions of data, that may be communicated using multiple communications paths.

FIELD OF THE INVENTION
The present invention relates in general to a system for securing data from unauthorized access or use.

BACKGROUND OF THE INVENTION
In today's society, individuals and businesses conduct an ever-increasing amount of activities on and over computer systems. These computer systems, including proprietary and non-proprietary computer networks, are often storing, archiving, and transmitting all types of sensitive information. Thus, an ever-increasing need exists for ensuring data stored and transmitted over these systems cannot be read or otherwise compromised.

SUMMARY OF THE INVENTION
Based on the foregoing, a need exists to provide a cryptographic system whose security is user-independent while still supporting mobile users. Accordingly, one aspect of the present invention is to provide a method for securing virtually any type of data from unauthorized access or use. The method comprises one

DECLARATION OF AVIEL D. RUBIN, PH.D.

The '854's Field Is "Securing Data"	
Title	"secure data parser and network"
Abstract	"secure data parser for "securely storing and communicating data"
Field of Invention	"securing data from unauthorized access or use." Ex. 1001 ['854] 1:25-26.
Background of the Invention	focuses on the need "for ensuring data stored and transmitted ... cannot be read or otherwise compromised" and seeks "to provide a cryptographic system whose security is user-independent ..." <i>Id.</i> , 1:35-37, 2:42-44.
Summary of the Invention	"one aspect of the present invention is to provide a method for securing virtually any type of data from unauthorized access or use." <i>Id.</i> , 2:45-47.
Claims	each claim concerns "securely storing a data set" or "securing a data set"

1. A method for securely storing a data set, the method comprising:



Traditional Sources: Hayhurst's Field Is "Decentralized Media Delivery"

(54) DECENTRALIZED MEDIA DELIVERY

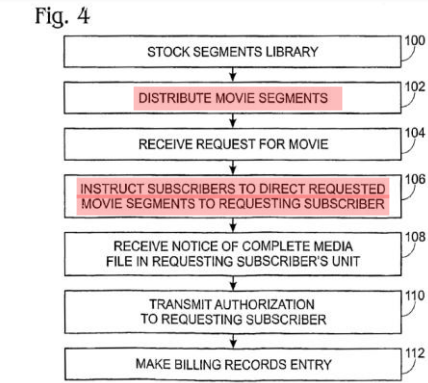
(57) **ABSTRACT**

A decentralized approach to delivering a media file to a requesting subscriber in a network of subscribers comprises the steps of segmenting the media file into a plurality of segments and distributing the segments of the media file

TECHNICAL FIELD

[0002] This application relates to the field of electronic media delivery, such as video-on-demand, including the secure handling and storage of such media.

[0015] FIG. 4 is a flow diagram showing how the decentralized media file delivery of the present invention is carried out.



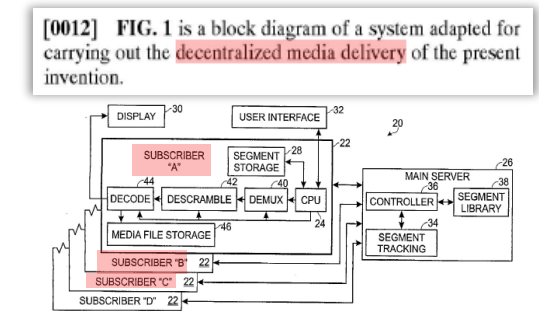
BACKGROUND

[0003] Current options for viewing a movie at home include traveling to a movie rental store to obtain a videotape or DVD copy of the movie. The copy must be returned a few days later. Another option is to select from the limited number of choices that are offered from sources that provide what is known as pay-per-view movies. Cable or broadcast movie channels provide a limited number of selections of movies for display a predetermined times.

[0004] It is usually not economically feasible for the operator of, for example, a cable television (CATV) system (or other content provider) to provide for delivery-on-demand a large number of movie selections to subscribers because such a system requires a extensive amount of bandwidth between the content provider and each of the subscriber units (televisions or other display devices) of the network.

SUMMARY OF THE INVENTION

[0005] The present invention addresses the problem of prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files. In short, there is provided a system that shifts the bandwidth requirements away from the content provider and to the network of subscriber units.



DECLARATION OF AVIEL D. RUBIN, PH.D.

Hayhurst's Field Is "Decentralized Media Delivery"	
Title	"Decentralized Media Delivery"
Abstract	"A decentralized approach to delivering a media file ..."
Technical Field	"This application relates to the field of electronic media delivery ..." <i>Id.</i> , [0002].
Background of the Invention	Focuses entirely upon delivering movie files. <i>Id.</i> , [0003]-[0004].
Summary of the Invention	"The present invention addresses the problem of prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files." <i>Id.</i> , [0005].
Specification/Figures	"FIG. 1 is a block diagram of a system adapted for carrying out the decentralized media delivery of the present invention." <i>Id.</i> , [0012] "FIG. 4 is a flow diagram showing how the decentralized media file delivery of the present invention is carried out." [0015]
Claims	each claim concerns decentralized media delivery

1. A method of delivering a media file that is requested by a requesting subscriber of a network of subscribers, comprising the steps of:

- segmenting the media file into a plurality of segments;
- distributing the segments of the media file among the network of subscribers for storage on respective units of the subscribers; and
- responding to a request from the requesting subscriber by directing to that requesting subscriber all of the plurality of segments of the media file.



The '854 And Hayhurst Have Different Fields

DECLARATION OF AVIEL D. RUBIN, PH.D.

The '854's Field Is "Securing Data"	
Title	" secure data parser and network"
Abstract	" secure data parser for " securely storing and communicating data "
Field of Invention	" securing data from unauthorized access or use." Ex. 1001 ['854] 1:25-26.
Background of the Invention	focuses on the need "for ensuring data stored and transmitted ... cannot be read or otherwise compromised " and seeks "to provide a cryptographic system whose security is user-independent ..." <i>Id.</i> , 1:35-37, 2:42-44.
Summary of the Invention	"one aspect of the present invention is to provide a method for securing virtually any type of data from unauthorized access or use." <i>Id.</i> , 2:45-47.
Claims	each claim concerns "securely storing a data set" or "securing a data set"

Hayhurst's Field Is "Decentralized Media Delivery"	
Title	"Decentralized Media Delivery"
Abstract	"A decentralized approach to delivering a media file ..."
Technical Field	"This application relates to the field of electronic media delivery ..." <i>Id.</i> , [0002].
Background of the Invention	Focuses entirely upon delivering movie files. <i>Id.</i> , [0003]-[0004].
Summary of the Invention	"The present invention addresses the problem of prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files ." <i>Id.</i> , [0005].
Specification/Figures	"FIG. 1 is a block diagram of a system adapted for carrying out the decentralized media delivery of the present invention." <i>Id.</i> , [0012] "FIG. 4 is a flow diagram showing how the decentralized media file delivery of the present invention is carried out." [0015]
Claims	each claim concerns decentralized media delivery

Petitioner: Hayhurst Is In The Field Of “Securing Data”

PETITIONER’S REPLY TO PATENT OWNER RESPONSE

Hayhurst’s “**Technical Field**” is “the field of electronic media delivery...including the **secure handling and storage** of such media.” Hayhurst, [0002]. That alone should be dispositive that Hayhurst is analogous art. *In re Wood*, 599 F.2d 1032, 1036 (C.C.P.A. 1979). EX1111 (“Bhattacharjee-Reply”), ¶¶4-12.

Petitioner Myopically Focuses On One Clause And Ignores The Rest Of Hayhurst

(54) **DECENTRALIZED MEDIA DELIVERY**

SUMMARY OF THE INVENTION

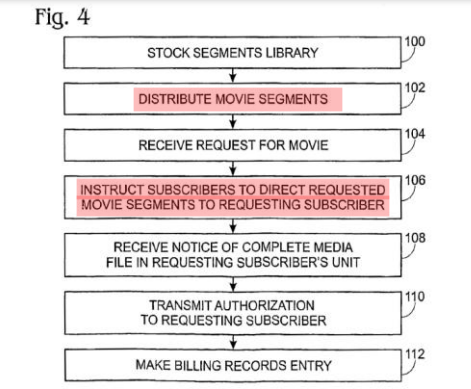
[0005] The present invention addresses the problem of prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files. In short, there is provided a system that shifts the bandwidth requirements away from the content provider and to the network of subscriber units.

TECHNICAL FIELD

[0002] This application relates to the field of electronic media delivery, such as video-on-demand, including the secure handling and storage of such media.

[0012] FIG. 1 is a block diagram of a system adapted for carrying out the decentralized media delivery of the present invention.

[0015] FIG. 4 is a flow diagram showing how the decentralized media file delivery of the present invention is carried out.



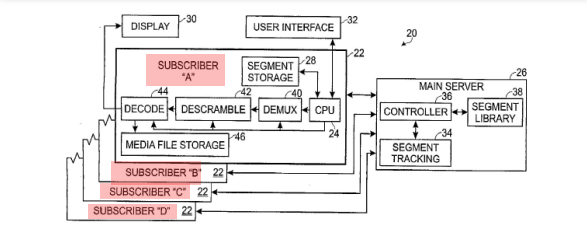
(57) **ABSTRACT**

A decentralized approach to delivering a media file to a requesting subscriber in a network of subscribers comprises the steps of segmenting the media file into a plurality of segments and distributing the segments of the media file among the network of subscribers, and responding to a request from the requesting subscriber by directing to that requesting subscriber all of the plurality of segments of the media file. All of segments are assembled into the media file and displayed or stored by the requesting subscriber.

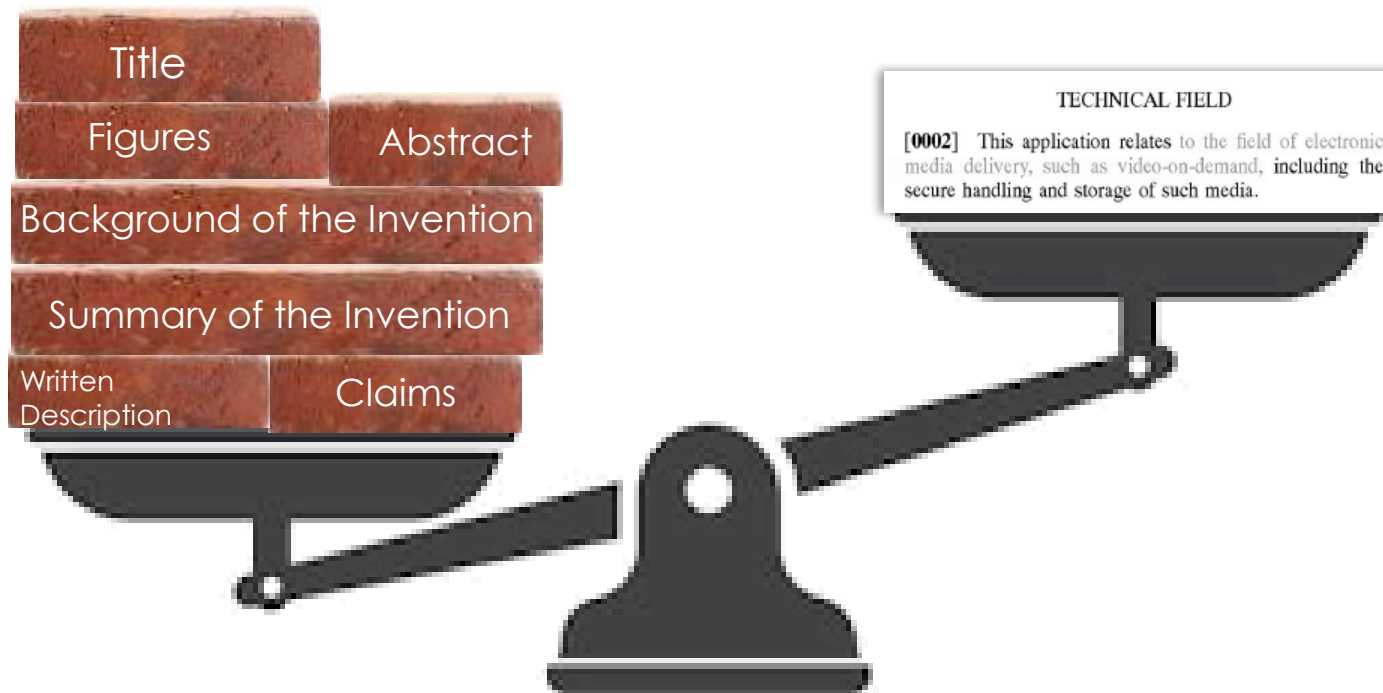
BACKGROUND

[0003] Current options for viewing a movie at home include traveling to a movie rental store to obtain a videotape or DVD copy of the movie. The copy must be returned a few days later. Another option is to select from the limited number of choices that are offered from sources that provide what is known as pay-per-view movies. Cable or broadcast movie channels provide a limited number of selections of movies for display a predetermined times.

[0004] It is usually not economically feasible for the operator of, for example, a cable television (CATV) system (or other content provider) to provide for delivery-on-demand a large number of movie selections to subscribers because such a system requires a extensive amount of bandwidth between the content provider and each of the subscriber units (televisions or other display devices) of the network.



The Weight Of The Evidence Confirms Hayhurst's Field Is Decentralized Media Delivery



Hayhurst: Segmented Storage Tangentially Results In Security

(12) Patent Application Publication Hayhurst

SUMMARY OF THE INVENTION

[0005] The present invention addresses the problem of prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files. In short, there is provided a system that shifts the bandwidth requirements away from the content provider and to the network of subscriber units.

[0006] In one embodiment, a media file representing, for example, a movie is segmented. These segments are distributed among the network of subscriber units. Any one of the subscribers may submit a request to view a movie. In response to such a request, the other subscriber units direct to the requesting subscriber all of the segments, which are then assembled into the complete media file (movie) for display, or stored for later display, on the requesting subscriber's unit.

[0008] The segmented and distributed storage of the media file provides a high level of security and a deterrence to piracy. No single subscriber unit has more than a segment of a media file, which segment, by itself, has little value.

- Addressing limited bandwidth
- Distributes movie segments across subscribers
- Security is an ancillary benefit

Dr. Rubin: Hayhurst's Security Is A By-Product Of Decentralized Media Delivery And Was Not Needed In The Prior Art

DECLARATION OF AVIEL D. RUBIN, PH.D.



104. I note that Petitioner argues that “Hayhurst concerns ‘electronic media delivery, such as video-on-demand’ and how the data is ‘secure[ly] handl[ed] and stor[ed].’” Pet., 59 (citing Ex. 1007 [Hayhurst] [0002]). While Hayhurst does include disclosures about the security of the electronic media files it delivers, in my opinion, that is not Hayhurst’s field of endeavor as established by the traditional sources I discussed above. Rather, security only tangentially relates to Hayhurst’s field of decentralized electronic media delivery. Hayhurst does not teach, for example, that prior art systems did not adequately secure media files, or that its invention addresses a need for more security. Ex. 1007 [Hayhurst] [0003]-[0005]. The mere mention of “secure handling and storage” of the media files does not change or expand Hayhurst’s field from decentralized electronic media delivery to also somehow encompass the ’854’s field.

Two Analogous Art Tests



“Two criteria have evolved for determining whether prior art is analogous:

- (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and
- (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is **reasonably pertinent to the particular problem with which the inventor is involved.**”

In re Clay, 966 F.2d 656, 658-59 (Fed. Cir. 1992)
(modified formatting)

Even Technologically Similar References May Not Be Reasonably Pertinent



“A person having ordinary skill in the art would not reasonably have expected to solve **the problem of dead volume in tanks for storing refined petroleum** by considering a reference **dealing with plugging underground formation anomalies**. The Board’s finding to the contrary is clearly erroneous.”

In re Clay, 966 F.2d 656, 660 (Fed. Cir. 1992)

“Wang’s SIMMs were designed to provide **compact computer memory with minimum size, low cost, easy repairability, and easy expandability**. ... In contrast, the Allen-Bradley patent relates to a **memory circuit for a larger, more costly industrial controller**. ... [T]he Allen-Bradley prior art is not reasonably pertinent and is not analogous.”

Wang Labs., Inc. v. Toshiba Corp., 993 F.2d 858, 864-65 (Fed. Cir. 1993)

Hayhurst's Problem Must Be Identified And Compared To The '854's Problem



“when addressing whether a reference is analogous art with respect to a claimed invention under a reasonable-pertinence theory, **the problems to which both relate must be identified and compared.**”

Donner Tech., LLC v. Pro Stage Gear, LLC, 979 F.3d 1353, 1359 (Fed. Cir. 2020)



Petitioner And Dr. Bhattacharjee Do Not Identify Hayhurst's Problem Let Alone Compare It To The '854's Problem



Undisputed: '854 Addresses Problem Of User-Independent Security For Cryptographic System While Supporting Mobile Users

(10) **Patent No.:** US 10,452,854 B2

Unfortunately, even the foregoing typical public-key cryptographic systems are still highly reliant on the user for security. For example, cryptographic systems issue the pri-

The foregoing mobile biometric cryptographic system still suffers from a variety of drawbacks. For example, the mobile user may lose or break the smartcard or portable computing device, thereby having his or her access to potentially important data entirely cut-off. Alternatively, a



DECLARATION OF AVIEL D. RUBIN, PH.D.

106. The '854 is directed towards creating a cryptographic system whose security is user independent, while still supporting mobile users. Ex. 1001 ['854]

Based on the foregoing, a need exists to provide a cryptographic system whose security is user-independent while still supporting mobile users.

Ex. 1001 ['854] 1:30-37, 1:46-2:14, 2:15-38, 2:42-44



Undisputed: Hayhurst's Problem Is Limited Bandwidth For Video-On-Demand

(12) Patent Application Publication Hayhurst

[0004] It is usually not economically feasible for the operator of, for example, a cable television (CATV) system (or other content provider) to provide for delivery-on-demand a large number of movie selections to subscribers because such a system requires a extensive amount of bandwidth between the content provider and each of the subscriber units (televisions or other display devices) of the network.

SUMMARY OF THE INVENTION

[0005] The present invention addresses the problem of prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files. In short, there is provided a system that shifts the bandwidth requirements away from the content provider and to the network of subscriber units.

DECLARATION OF AVIEL D. RUBIN, PH.D.

107. By contrast, Hayhurst is directed towards “address[ing] the prohibitive bandwidth requirements for a content provider associated with delivering video-on-demand other large media files.” Ex. 1007 [Hayhurst] [0005].

DECLARATION OF SAMRAT BHATTACHARJEE, PH.D.

Hayhurst, [0002]. Hayhurst says then-existing systems for “delivery-on-demand” of media content “require[d] an extensive amount of bandwidth.” Hayhurst (EX1007), [0004]. To address that problem and provide other advantages, Hayhurst’s media files are segmented and “distributed among a network of subscriber units,” which store media-file segments so individual subscribers can



Dr. Rubin: Hayhurst And The '854 Address Different Problems

DECLARATION OF AVIEL D. RUBIN, PH.D.



108. The '854, again, addresses eliminating user vulnerabilities in storing sensitive information. Hayhurst, by contrast, addresses the prohibitive bandwidth requirements for video-on-demand from the perspective of the content provider. Ex. 1007 [Hayhurst] [0003]-[0005].

110. A POSITA looking to solve a problem with securing data sets in a user-independent fashion would not have looked to a reference directed to reducing the bandwidth required to transmit video-on-demand. Thus, in my opinion, Hayhurst is not reasonably pertinent to the '854 because they are directed to different problems, and Petitioner and Dr. Bhattacharjee fail to demonstrate that Hayhurst is analogous art to the '854 patent.

Dr. Rubin: Hayhurst's Teachings Are Not Relevant To the '854's Problem

DECLARATION OF AVIEL D. RUBIN, PH.D.



109. Security from piracy is merely an ancillary benefit to Hayhurst's solution of decentralizing content delivery. And, what little Hayhurst has to say about encryption does not suggest that it is directed towards securing data in a manner that is "user-independent." Rather, in Hayhurst's system, a subscriber requests both an encrypted movie and an encryption key. Ex. 1007 [Hayhurst] [0028], [0030]. While the movie is originally dispersed amongst thousands of subscribers, it is reassembled, along with the key, by a single user. Thus, the security of the data (the movie) is user-dependent.

Foster-Hayhurst Fails (IPR2024-00212, -00215)

- ❑ Hayhurst Is Not Analogous Art (IPR2024-00212, -00215)

- **No Motivation To Combine Foster-Hayhurst Shown (IPR2024-00212, -00215)**

- ❑ Foster's Packets/Payloads Are Not Shares/Chunks (IPR2024-00214, -00215)

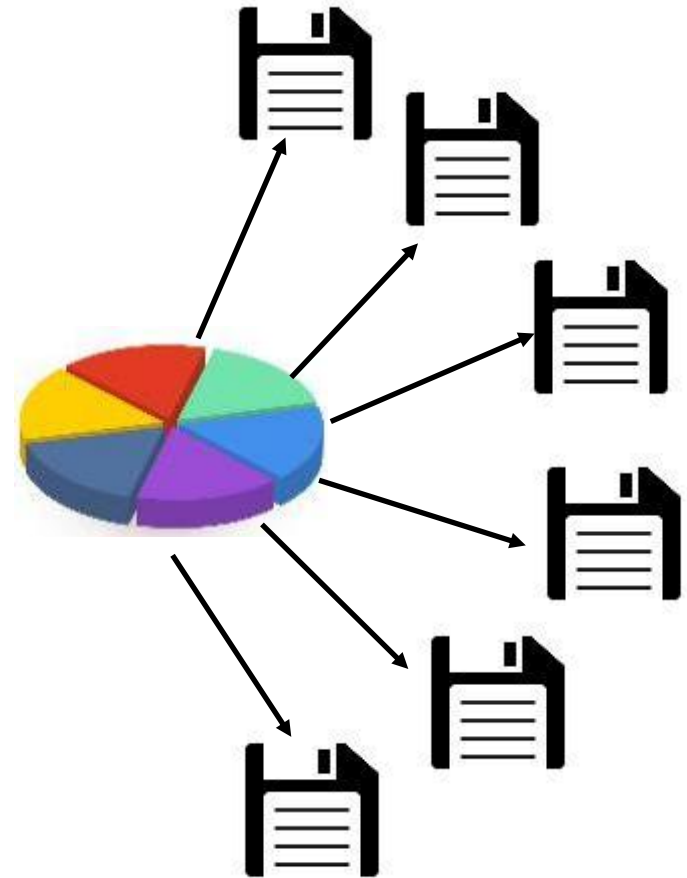
'854/'116 Claims: Require Storing Data Chunks On A “Plurality Of Different Storage Devices”

(10) Patent No.: US 10,452,854 B2

storing with the plurality of data chunks data indicative of at least one of the distinct encryption keys on a plurality of different storage devices.

(10) Patent No.: US 11,178,116 B2

separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys on a plurality of different storage devices.



Undisputed: Foster Does Not Store Data Chunks On A “Plurality Of Different Storage Devices”

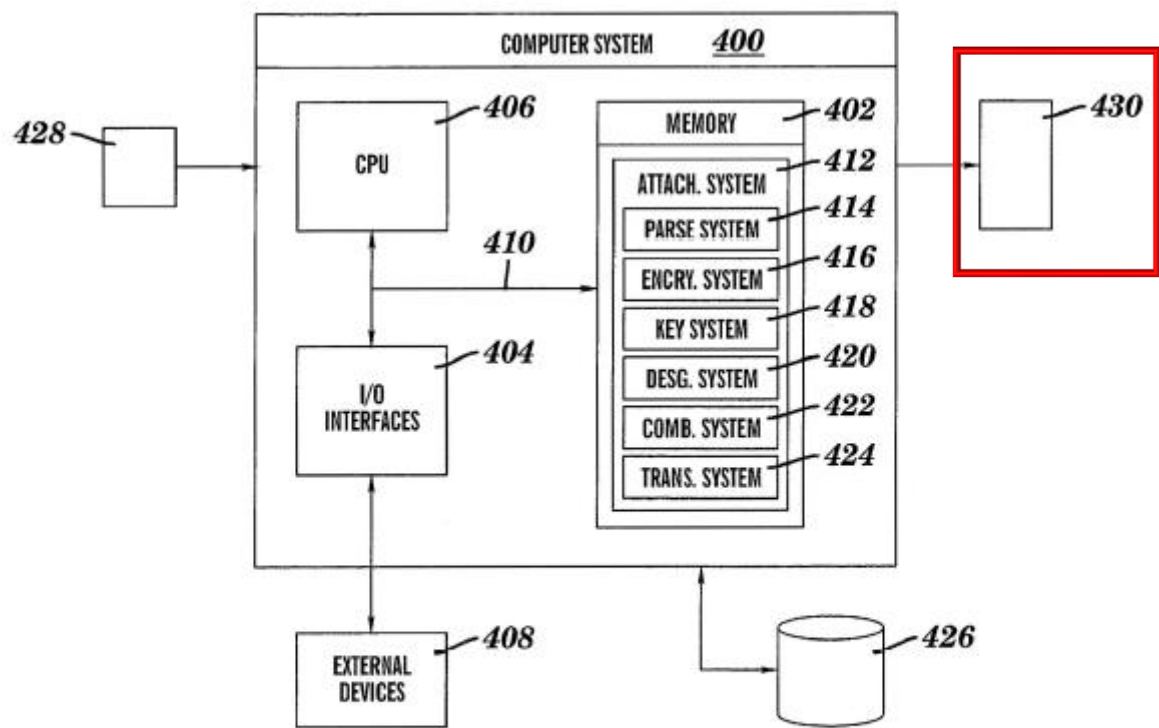
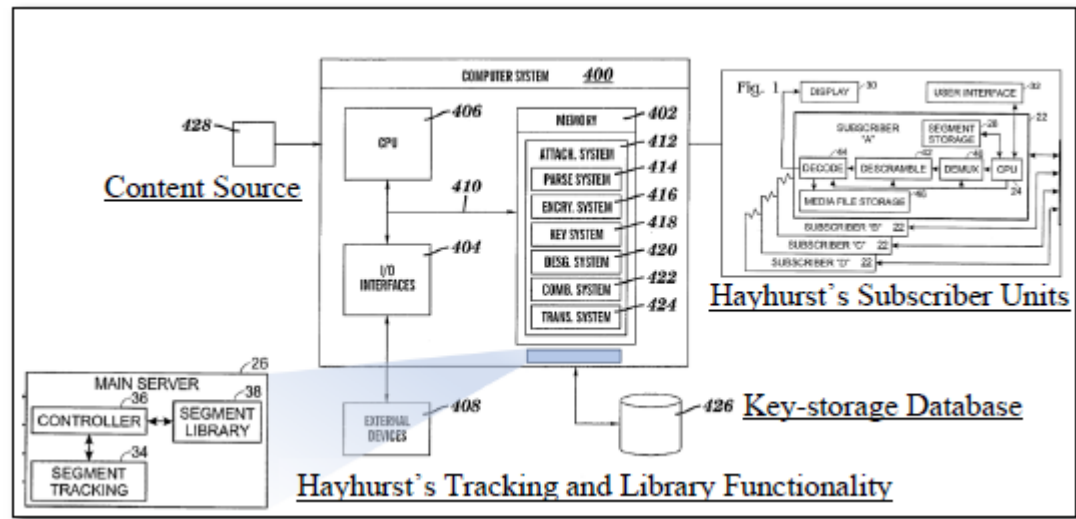


FIG. 16

Petition Combines Foster's Data Encryption Technique With Hayhurst's Distributed Storage

PETITION FOR INTER PARTES REVIEW
UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §42.1 et seq



The Foster-Hayhurst combination would have used Foster's technique of encrypting portions of a data set with respective encryption keys that are themselves encrypted with a KEK that is stored in a key-storage system, and Hayhurst's technique of storing the encrypted data on different storage devices. Bhattacharjee,

Petition's Combination: All Of Foster's Content Units Are Distributed Per Hayhurst's Method

PETITION FOR INTER PARTES REVIEW UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §42.1 et seq

POSAs had reason to store Foster's encrypted content units on multiple storage devices (*e.g.*, consumer set-top boxes like Hayhurst's subscriber units and Foster's recipients 430) based on Hayhurst's techniques for storing and distributing encrypted data segments. Bhattacharjee, ¶182.

POSAs would have recognized several benefits in storing Foster's encrypted content units distributed on different storage devices as Hayhurst teaches. Foster's

to known encryption and data-storage methods, to yield the predictable result of Foster's encrypted content units being stored on and retrievable from distributed storage devices as taught in Hayhurst. *KSR*, 550 U.S. at 416; Bhattacharjee, ¶185.

“segment tracking” functionality of Hayhurst's main server 26 so it can control distribution of and access to Foster's encrypted content portions on the “subscriber units.” Hayhurst, [0017], [0023]-[0024], [0026], FIGS. 1, 4; Foster, [0040]-[0041],

No Motivation To Render Reference “Inoperable For Its Intended Purpose” Or Change Its “Principle Of Operation”



POSITA would not be motivated to render reference “**inoperable for its intended purpose**” or “**change [its] principle of operation.**”

Plas-Pak Indus., Inc. v. Sulzer Mixpac AG, 600 Fed. Appx. 755, 759 (Fed. Cir. 2015)

“This suggested combination ... would require a substantial reconstruction and redesign of the elements shown ... as well as **a change in the basic principles under which the Chinnery et al. construction was designed to operate.**”

In re Ratti, 270 F.2d 810, 813 (C.C.P.A. 1959)

Foster's Purpose Is To Synchronize Transmission Of Encrypted Content Units And Encryption Keys

(54) METHOD, SYSTEM AND PROGRAM PRODUCT FOR ATTACHING A TITLE KEY TO ENCRYPTED CONTENT FOR SYNCHRONIZED TRANSMISSION TO A RECIPIENT

(57) ABSTRACT

A method and system for attaching a title key to encrypted content for synchronized transmission to, or storage by, a recipient is provided. Specifically, under the present invention, an elementary media stream is parceled into content units that each include a content packet and a header. The content packets are encrypted with one or more title keys. Once the content packets have been encrypted, the title keys are themselves encrypted with a key encrypting key. The encrypted title keys are then attached to the corresponding encrypted content packets for synchronized transmission to a recipient.

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention generally relates to a method, system and program product for attaching a title key to encrypted content for synchronized transmission to a recipient. Specifically, a title key used to encrypt content is itself encrypted, and attached to the encrypted content so that both can be synchronously transmitted to a recipient.

SUMMARY OF THE INVENTION

[0008] In general, the present invention provides a method, system and program product for attaching a title key to encrypted content for synchronized transmission to a recipient. Specifically, under the present invention, a content

DECLARATION OF AVIEL D. RUBIN, PH.D.

114. As can be seen throughout Foster's disclosure, Foster's fundamental goal is to synchronize the transmission of encrypted content packets with the keys used to encrypt those packets. Doing so allows each packet to be viewed as soon

SAMRAT BHATTACHARJEE

Q. Why does synchronous transmission to a receiver foster random access to content?

A. That is sort of the whole invention in Foster.



Foster: Prior Art Systems Without Synchronization Had Undesirable Delays

Foster et al.

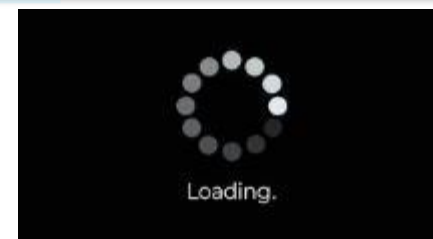
being used, a new key pair can be sent to the receiver. In sending separate key sets to the receiver in this manner, however, loss of synchronization between the content and the keys is risked. Moreover, both DRMS and CAS can have inherent latencies in providing random access of protected content.

use the key to decrypt the content. Similar to the DRMS, the CAS fails to provide synchronized delivery of a key with encrypted content. Moreover, because delivery of keys and protected content are non-synchronized in a CAS, certain latencies such as delays are inherent in attempting to gain random access to the content.

[0051] As indicated above, the DRMS fails to provide synchronized delivery of the content with the keys used to encrypt the content. That is, license server 16 must be separately accessed. When providing the keys in such a manner, there exists a likelihood that either the appropriate keys will not be matched with the encrypted content, or a single key will be used, weakening the security. Furthermore, providing keys from license server 16 requires a back channel.

random access of content. As indicated above, both DRMS and CAS have inherent latencies (e.g., delays) in providing random access of content. Specifically, because each content packet transmitted under the present invention is “packaged” with the title key that was used to encrypt it, a recipient can access and decrypt the content stream at any packet.

[0056] As indicated above, because the KMB is necessary to access encrypted content, the KMB should be delivered synchronously with, or prior to, the encrypted content. When this condition is not met, a delay could be incurred between when encrypted content is received and when it accessed (e.g., between when a channel is changed and when an image is displayed).



Foster: Synchronizes Transmission To Avoid Delays

(12) **Patent Application Publication**
Foster et al.

content unit 116 can then be transmitted to a recipient. That is, the encrypted content unit, the header and the header extension (including the encrypted title key) will be delivered to, or stored by, a recipient as a single, integral data stream. Thus, a recipient will receive or store encrypted content along with all information necessary to decrypt the content. This not only prevents the synchronization problems associated with previous systems, but also provides random access of content. As indicated above, both DRMS and CAS have inherent latencies (e.g., delays) in providing random access of content. Specifically, because each content packet transmitted under the present invention is “packaged” with the title key that was used to encrypt it, a recipient can access and decrypt the content stream at any packet.

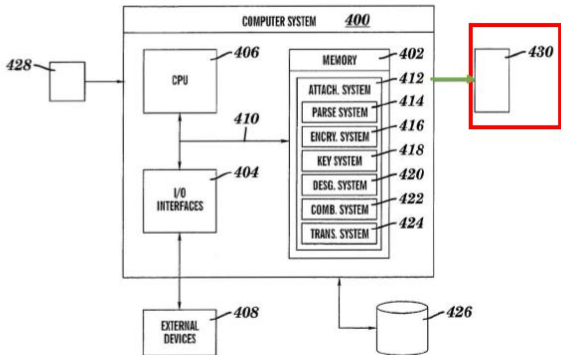


FIG. 16

DECLARATION OF AVIEL D. RUBIN, PH.D.

Ex. 1006 [Foster] Fig. 16 (annotated); [0078] (“computer system 400 ... process[es] content units ... and transmit[s] the processed content units to a recipient 430.”). Because each content unit contains both the content and the key, each content unit may be encrypted and transmitted by the source as it is generated, and then decrypted and viewed without the delay found in prior art systems wherein the key had to be separately attained. *Id.*, [0064].



Foster Is Directed Towards Cable Television

(12) Patent Application Publication Foster et al.

[0039] Content Service Provider—an entity, such as a cable service provider, that provides the “pipeline” through which content is delivered from a content owner to a consumer.

[0040] Receiver—a consumer device, such as a set-top box, a DVD player, etc., that receives content directly from a content owner, from a content service or from another receiver within a consumer home network.

[0006] In a television-based CAS, the content and keys are prepared at a head-end server based on the appropriate subscriber information. The encrypted content and keys are

[0052] Referring now to FIG. 2, a Conditional Access System (CAS), such as a cable or satellite television system, is shown in greater detail. In a CAS, two entitlement

DECLARATION OF AVIEL D. RUBIN, PH.D.

119. Importantly, Foster contemplates using its invention in the cable television context. Foster teaches that its system processes and transmits content units between a “Content Service Provider” “such as a cable service provider” (*id.*, [0039]) and a “Receiver” “such as a set-top box” (*id.*, [0040]). *Id.*, Fig. 16, [0078]. It seeks to improve upon prior art cable systems providing real-time television. *Id.*, [0052] (Foster is directed towards “Conditional Access System[s] (CAS),” which are “cable or satellite television system[s]”); [0006].



Foster's Invention Facilitates Real-Time Television/Streaming

(12) **Patent Application Publication**
Foster et al.

DECLARATION OF AVIEL D. RUBIN, PH.D.

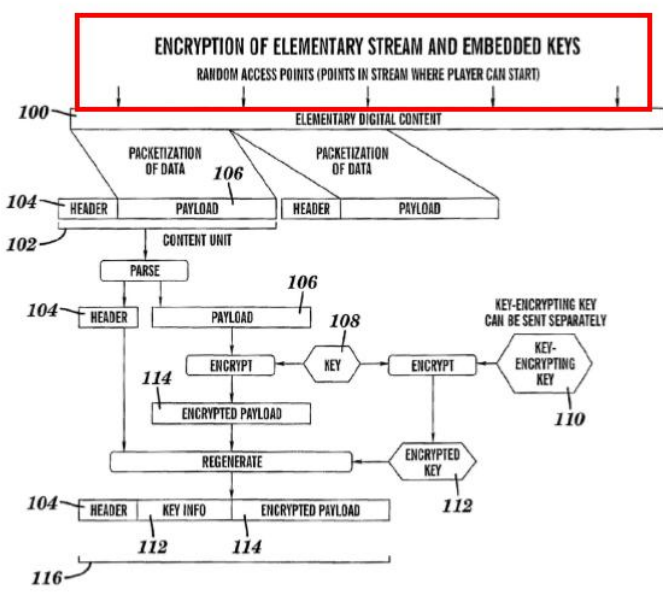


FIG. 8

[0056] As indicated above, because the KMB is necessary to access encrypted content, the KMB should be delivered synchronously with, or prior to, the encrypted content. When this condition is not met, a delay could be incurred between when encrypted content is received and when it accessed (e.g., between when a channel is changed and when an image is displayed).

120. Foster's teachings of synchronized transmission to reduce delays/latencies are particularly significant in a streaming context contemplated by Foster's Figure 8, which Petitioner relies upon (e.g., Pet., 56, 65-66). "In streaming, multimedia data is transferred in a stream of packets that are interpreted and rendered in real time by a software application, as the packets arrive in the user's terminal." Ex. 2035 [Patrikakis] 220. Because packets are transmitted as a stream and rendered in real-time, any delays have an especially noticeable impact. When watching, e.g., a live sporting event, any delay in receiving, decrypting and/or rendering each content unit in a stream would be a significant drawback.



Foster And Hayhurst Have Conflicting Goals

Foster et al.



Hayhurst



Hayhurst Is Focused On Bandwidth Issues For Video-On-Demand

(12) Patent Application Publication Hayhurst

BACKGROUND

[0003] Current options for viewing a movie at home include traveling to a movie rental store to obtain a videotape or DVD copy of the movie. The copy must be returned a few days later. Another option is to select from the limited number of choices that are offered from sources that provide what is known as pay-per-view movies. Cable or broadcast movie channels provide a limited number of selections of movies for display a predetermined times.

[0004] It is usually not economically feasible for the operator of, for example, a cable television (CATV) system (or other content provider) to provide for delivery-on-demand a large number of movie selections to subscribers because such a system requires a extensive amount of bandwidth between the content provider and each of the subscriber units (televisions or other display devices) of the network.

SUMMARY OF THE INVENTION

[0005] The present invention addresses the problem of prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files. In short, there is provided a system that shifts the bandwidth requirements away from the content provider and to the network of subscriber units.



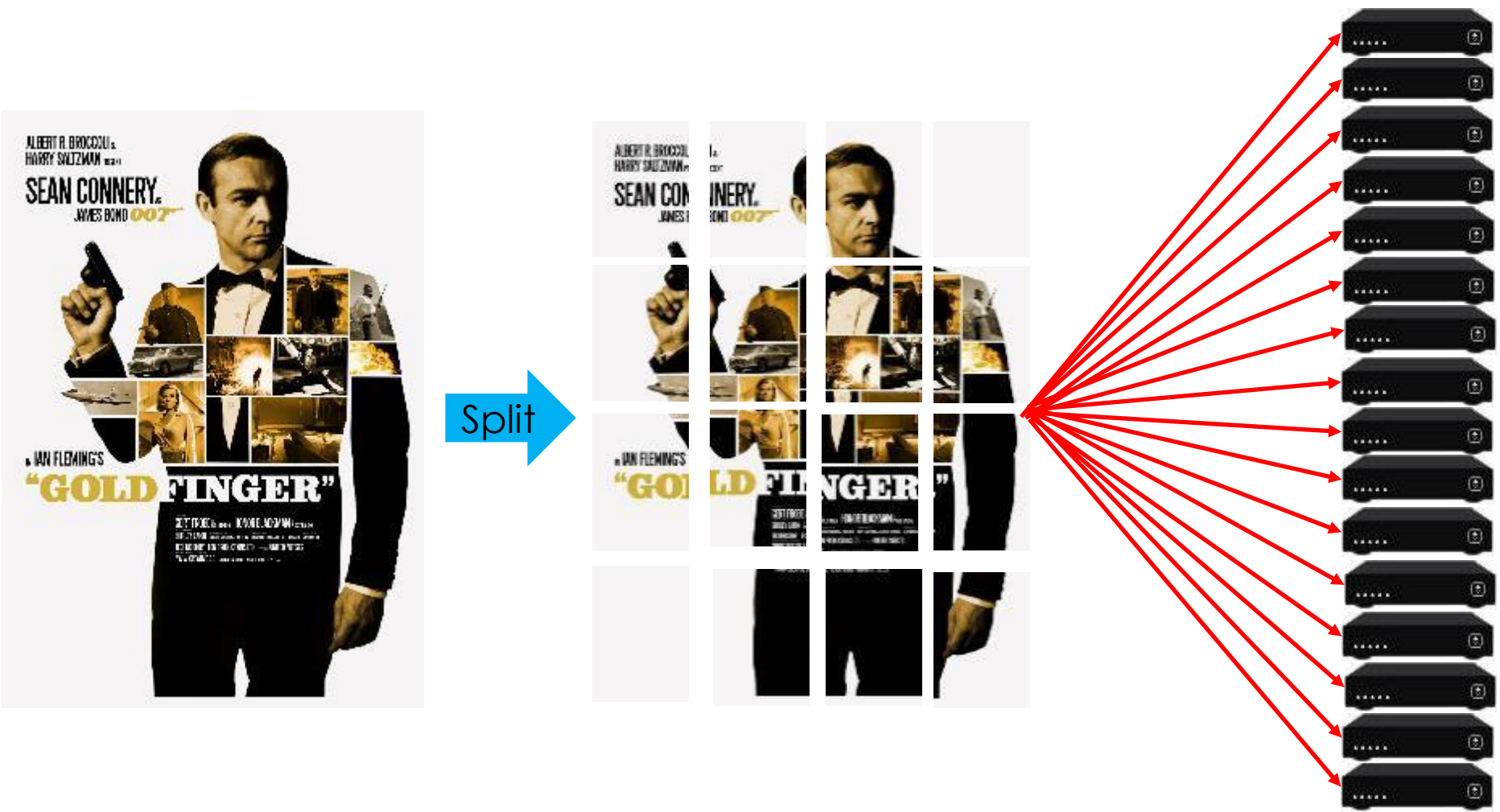
Undisputed: Hayhurst Is Not Concerned With Synchronous Transmission, Avoiding Delays, Or Real-Time Streaming

DECLARATION OF AVIEL D. RUBIN, PH.D.

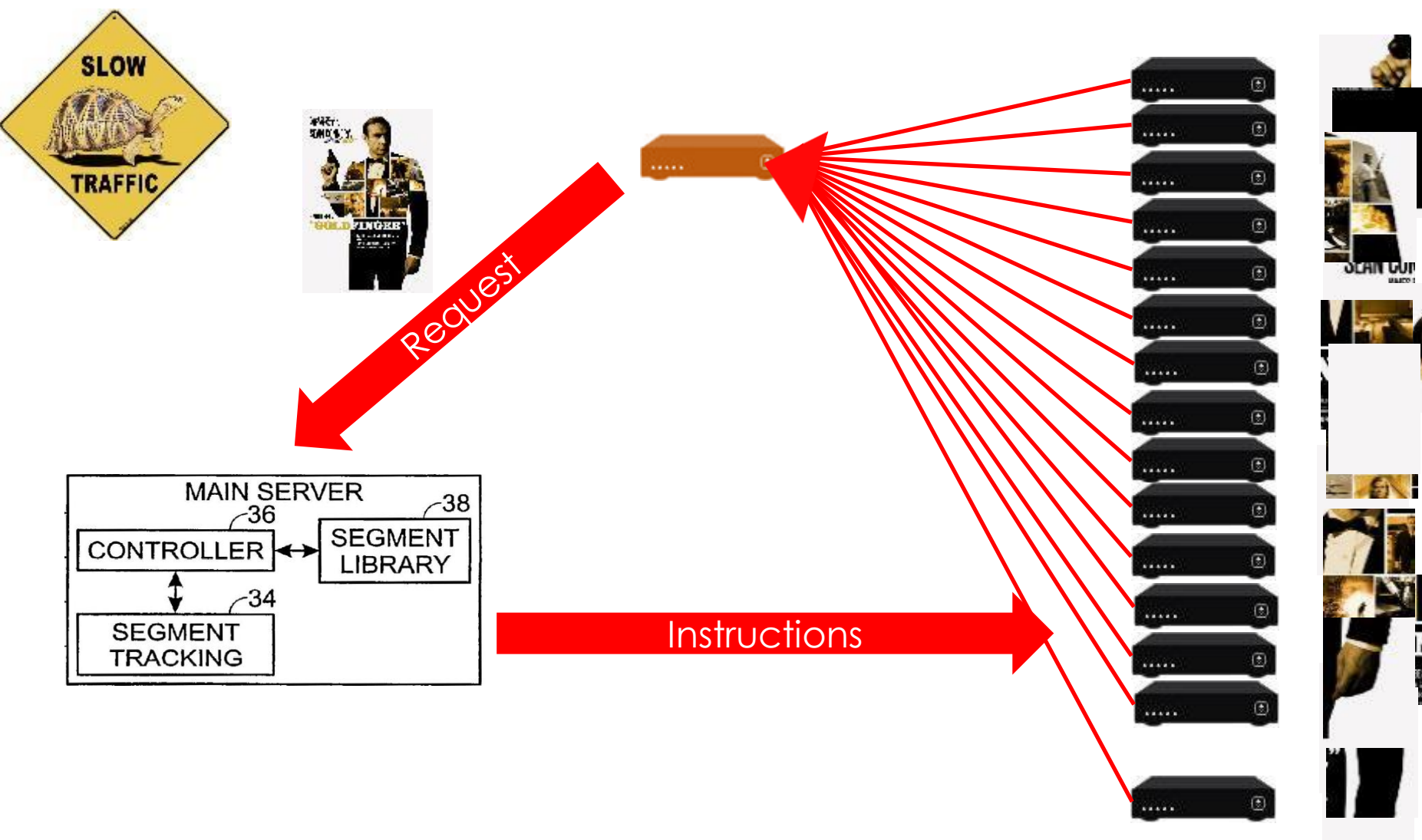


122. Unlike Foster, Hayhurst is not concerned with synchronous transmission, avoiding delays, or facilitating real-time streaming. Indeed, Hayhurst purports to facilitate the transmission and playback of content files rather than content streams. As I previously explained in Section VI.B.1(b), Hayhurst aims to overcome “prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files” to a subscriber network. Ex. 1007 [Hayhurst] [0005]. Hayhurst teaches that, in light of the size of these

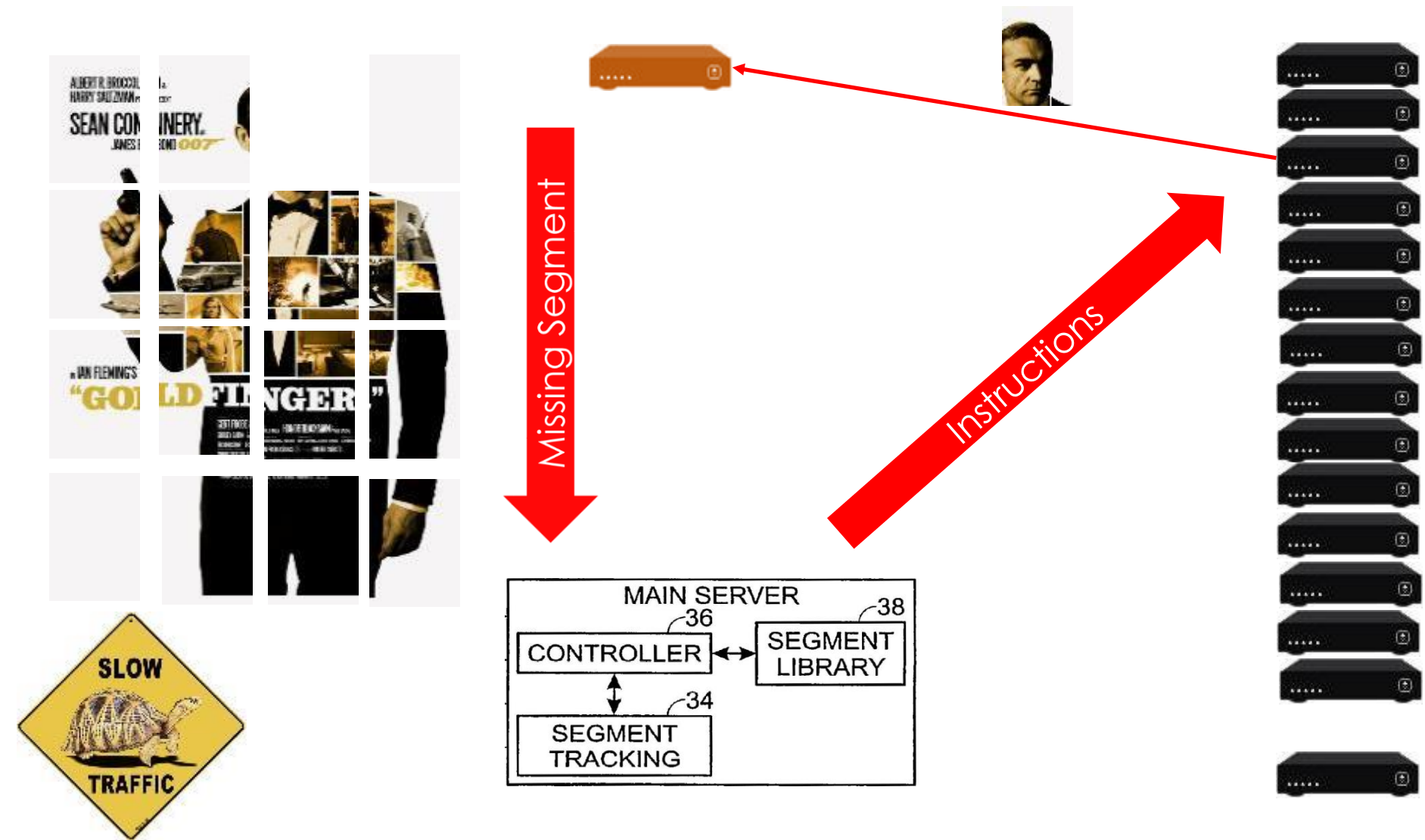
Hayhurst's Method Of Decentralized Distribution



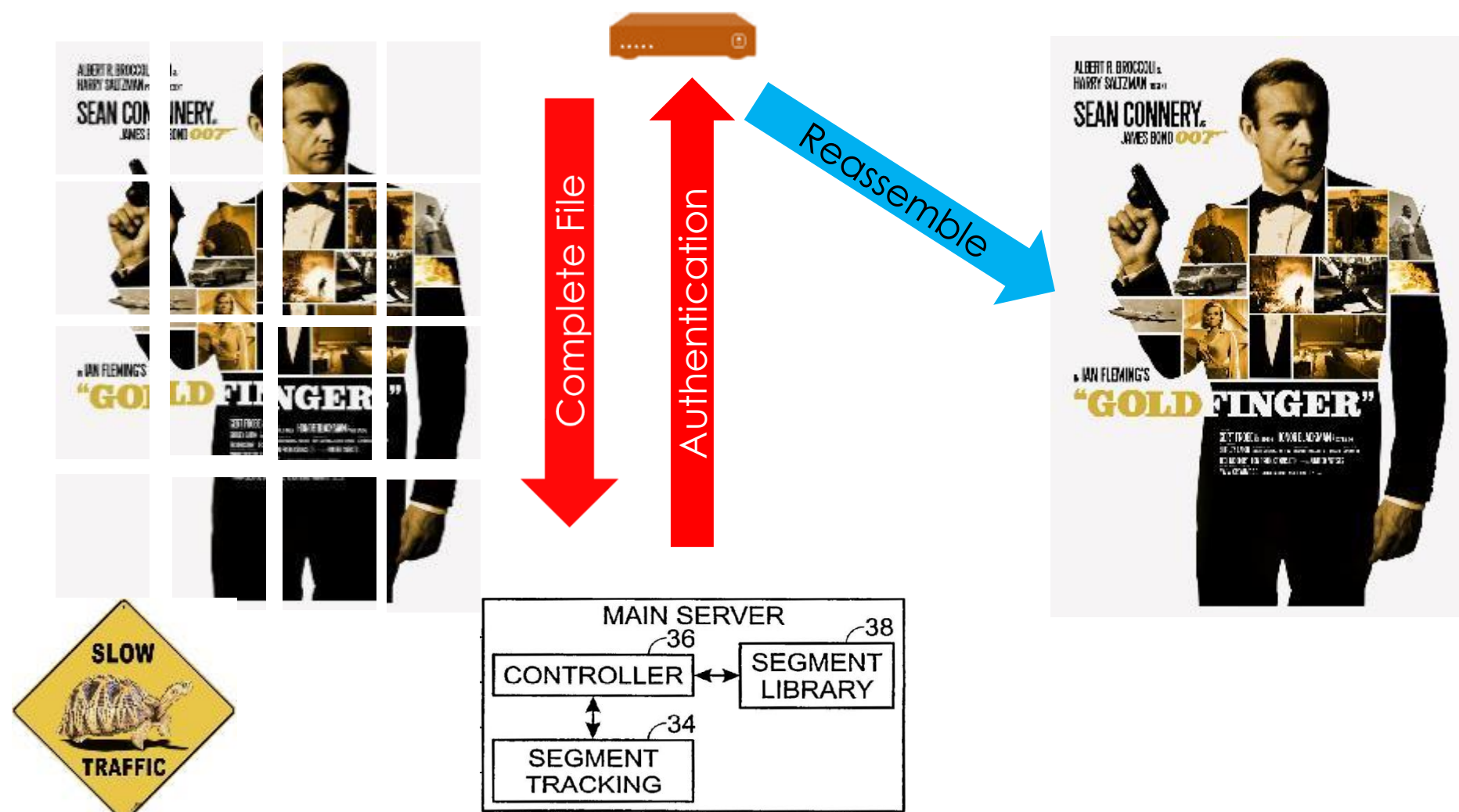
Requesting STB Requests Movie From Main Server Which Instructs Other STBs To Send Movie Segments



Missing Segments Must Be Sought From Other STBs



Once All Segments Are Received, Authentication Is Sought And The Movie Is Processed And Reassembled



Undisputed: Hayhurst Distributed Method Incompatible With Live Television

Foster



Hayhurst



DECLARATION OF AVIEL D. RUBIN, PH.D.

124. Hayhurst's methodology is not compatible with real-time streaming or random-access viewing of live television. Hayhurst requires that an entire movie file be segmented, and the segments transmitted to, and stored among, the members of a subscriber network before the movie can even be requested for viewing by any individual subscriber. Beyond that, because the segments are not stored in or received in any particular order, the movie cannot be viewed at all until (i) *all* segments are received from the subscriber network by the subscriber, (ii) the requesting unit obtains authorization, and (iii) the packets are descrambled and then reassembled into the complete movie file. Ex. 1007 [Hayhurst] [0029]; [0030]; Ex. 2034 [Bhattacharjee-Depo.] 101:19-25. Thus, Hayhurst's system requires all segments to be received and for the entire file to be reassembled the system can play the movie, thus, "excluding the use for covering live events." Ex. 2035 [Patrikakis] 219.

Undisputed: Hayhurst's Method Would Preclude Foster From Real-Time Television And Streaming



DECLARATION OF AVIEL D. RUBIN, PH.D.

134. In the Foster/Hayhurst combination, a set-top box requesting cable television content would have to wait to receive all of the packets sent from the set-top boxes of a multitude of other subscribers before seeking and obtaining authorization and before reassembling and processing the entire content file. This wait-and-see approach would not work when trying to watch live television. Ex. 1006 [Foster] [0063].

Foster-Hayhurst Is Less Secure Than Foster Alone



DECLARATION OF AVIEL D. RUBIN, PH.D.

by Hayhurst's video-on-demand system. Foster's system, moreover, has sufficient security at the source, security which would be undermined in the combination, as



Foster: KEK Can Be Easily Changed If Compromised

(12) **Patent Application Publication**
Foster et al.

DECLARATION OF AVIEL D. RUBIN, PH.D.

[0054] FIG. 4 demonstrates that an encrypted title key 30 can be re-encrypted with a different key encrypting key 32 without having to re-encrypt the encrypted content 26. As shown, encrypted key 30 is received and decrypted with key encrypting key 28. Title key 24 is then re-encrypted with a new key encrypting key 32. The re-encrypted title key 34 is then transmitted along with the undisturbed encrypted content 26. By re-encrypting title key 24, the protection on the content can be varied without having to re-encrypt the content itself, which could be significantly more time-consuming and/or consume more resources than re-encrypting title key 24.

135. In Foster, should a key-encrypting-key be compromised or “protection on the content [need] to be varied,” “an encrypted title key 30 can be re-encrypted with a different key encrypting key 32 without having to re-encrypt the encrypted content 26.” Ex. 1006 [Foster] [0054].

Id., Fig. 4. Thus, Foster contemplates seamlessly switching the KEK for security purposes without re-encrypting the underlying content. Thus, if a key-encrypting-key is compromised, or a switch is otherwise desirable, a new KEK may be utilized going forward.

RE-ENCRYPTED KEY ENCRYPTION

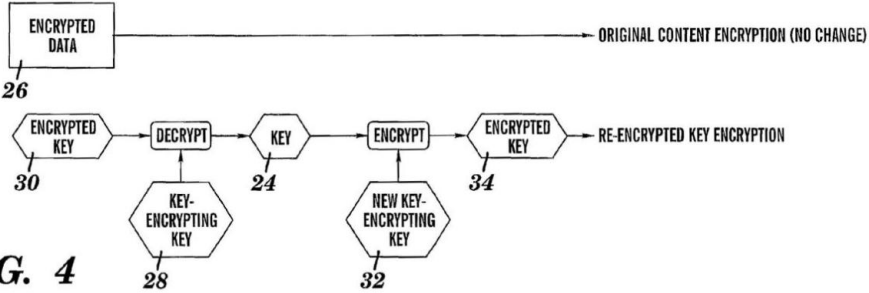
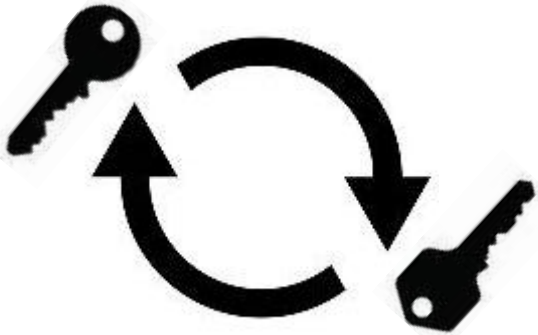


FIG. 4



Dr. Rubin: Foster Allows A KEK To Be Unique To Each Recipient, Increasing Security

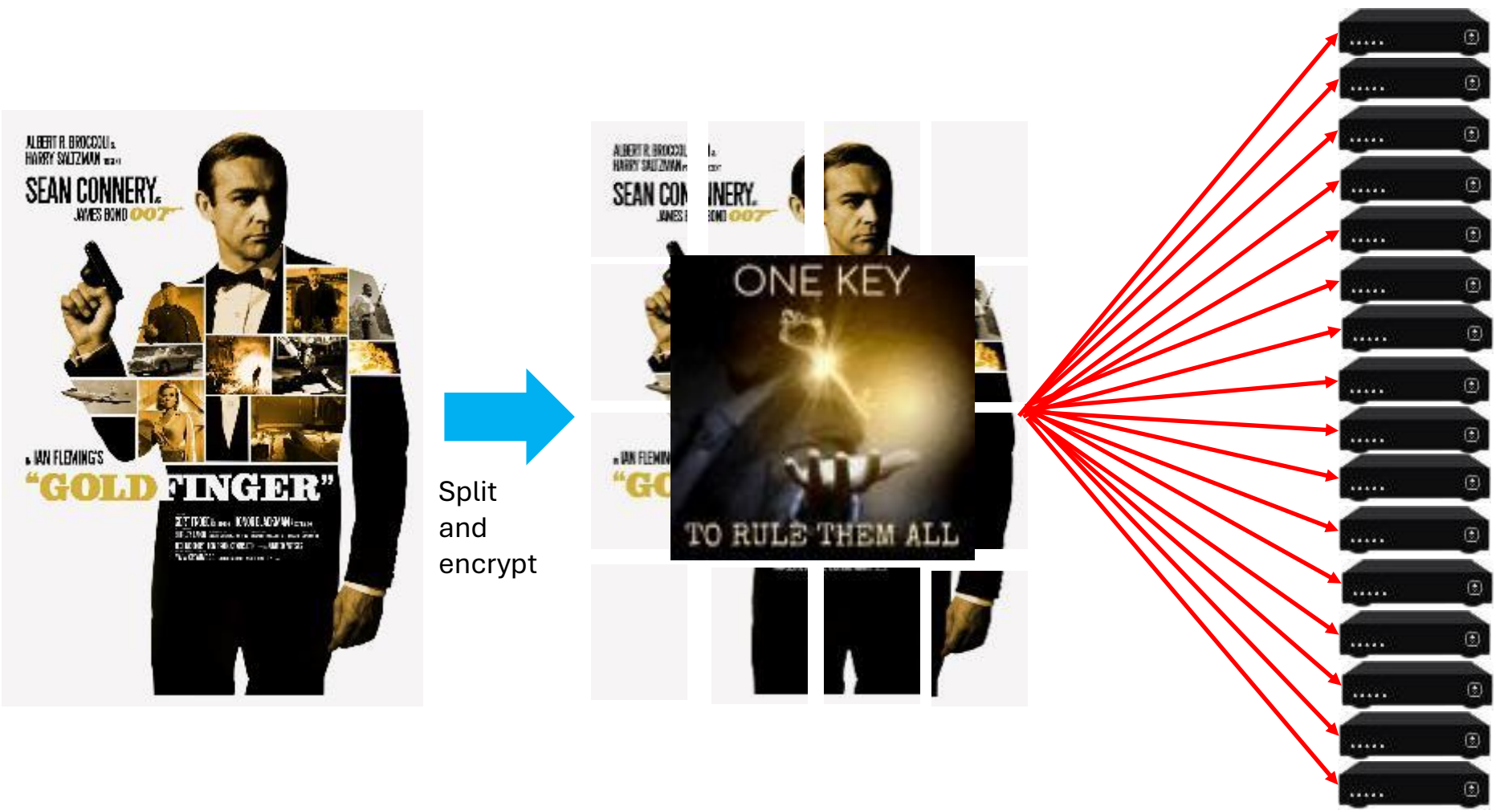
DECLARATION OF AVIEL D. RUBIN, PH.D.



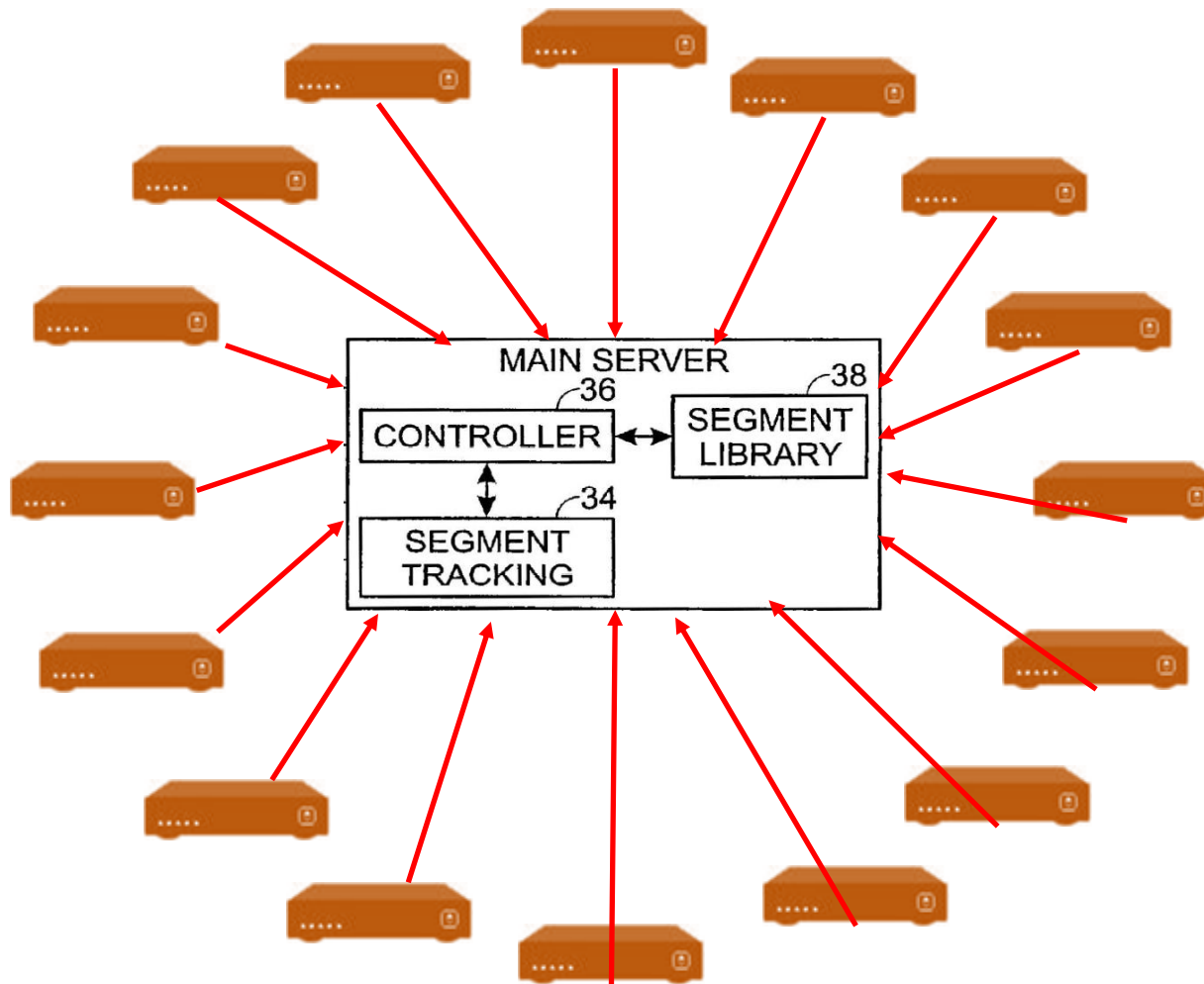
136. Moreover, Foster allows for a key-encrypting-key to be unique to each recipient. Foster teaches that “key encrypting key 28 is generally determined based on a key management block (KMB), which is typically delivered to a recipient concurrently with or prior to the delivery of encrypted content 26.” *Id.*, [0054]. Because each recipient receives a KMB from which a key-encrypting-key can be determined, that key-encrypting-key can be unique to each recipient. This further increases the security of Foster’s content as the damage from any compromise of a recipient’s key-encrypting-key can be limited to that recipient and further prevented by simply changing that recipient’s key-encrypting-key.



Foster-Hayhurst: Movie Is Pre-encrypted And Distributed Among Subscribers



Foster-Hayhurst: Because Any Subscriber Can Request Pre-encrypted Movie, KEKs Cannot Be Unique To Each Subscriber



Undisputed: In Foster-Hayhurst, KEKs Can At Most Be Unique To A Movie

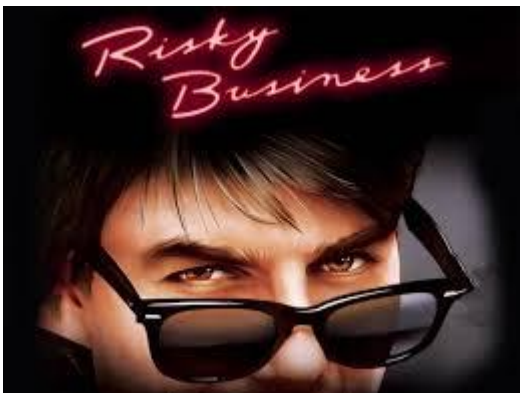


DECLARATION OF AVIEL D. RUBIN, PH.D.

137. Foster/Hayhurst uses Hayhurst's method of storing and distributing content. Consequently, any subscriber (of thousands) is able to request content that has been divided into segments across thousands of subscribers. Because any one of Hayhurst's subscribers can request the content, which has already been segmented and divided in advance, in any combination, Foster's content units would all have to be secured using the same KEK(s), regardless of which subscriber will eventually request the content.

Undisputed: Having KEKs Unique To A Movie Is Less Secure Than To Each User

DECLARATION OF AVIEL D. RUBIN, PH.D.



138. This, however, makes the combined system less secure for two reasons. First, it makes the KEKs more vulnerable. Because the KEK(s) is/are distributed amongst thousands of subscribers, there are thousands of potential points of failure. And, if one set-top-box (of thousands) with the KEK(s) gets compromised, all of the content is compromised because all of the content is encrypted using the same KEK(s) and title keys. Second, it would be more complicated to switch KEKs than in Foster alone as all of the content units are distributed across the subscribers instead of streamed in real time as in Foster. Thus, adding Hayhurst's methods to Foster's system would make Foster's system less secure in contravention of Foster's aims. Ex. 1006 [Foster] [0004] ("In transmitting such content, however, the security thereof must be ensured.").

Reply Theory That Foster Recognizes Re-encrypting Content As An Alternative Is Contrary To Foster's Teachings

Reply

Foster

“Foster does not require changing the KEK. **Rather, Foster recognizes ‘re-encrypting the content itself,’ rather than changing the KEK, is an alternative.**”

Reply, 11.

[0054] FIG. 4 demonstrates that an encrypted title key 30 can be re-encrypted with a different key encrypting key 32 without having to re-encrypt the encrypted content 26. As shown, encrypted key 30 is received and decrypted with key encrypting key 28. Title key 24 is then re-encrypted with a new key encrypting key 32. The re-encrypted title key 34 is then transmitted along with the undisturbed encrypted content 26. By re-encrypting title key 24, the protection on the content can be varied without having to re-encrypt the content itself, which could be significantly more time-consuming and/or consume more resources than re-encrypting title key 24.



Don't Do That!

Petitioner Fails To Demonstrate “POSAs Knew How To Change/Replace KEKs Across Many Devices/Users”

PETITIONER’S REPLY

used for multiple segments. Furthermore, POSAs knew how to change/replace KEKs across many devices/users. Bhattacharjee-Reply, ¶¶104-105, ¶¶110-115 (citing EX1078, 4:5-28; EX1079, 544-546; EX1080, 2-7).

Peer-to-peer
information
delivery, not
KEKs

Replacing
session keys,
not KEKs

Replacing traffic
encryption keys,
not KEKs

Petitioner Failed To Consider Significant Drawbacks Of Using Hayhurst's Distribution With Foster's System



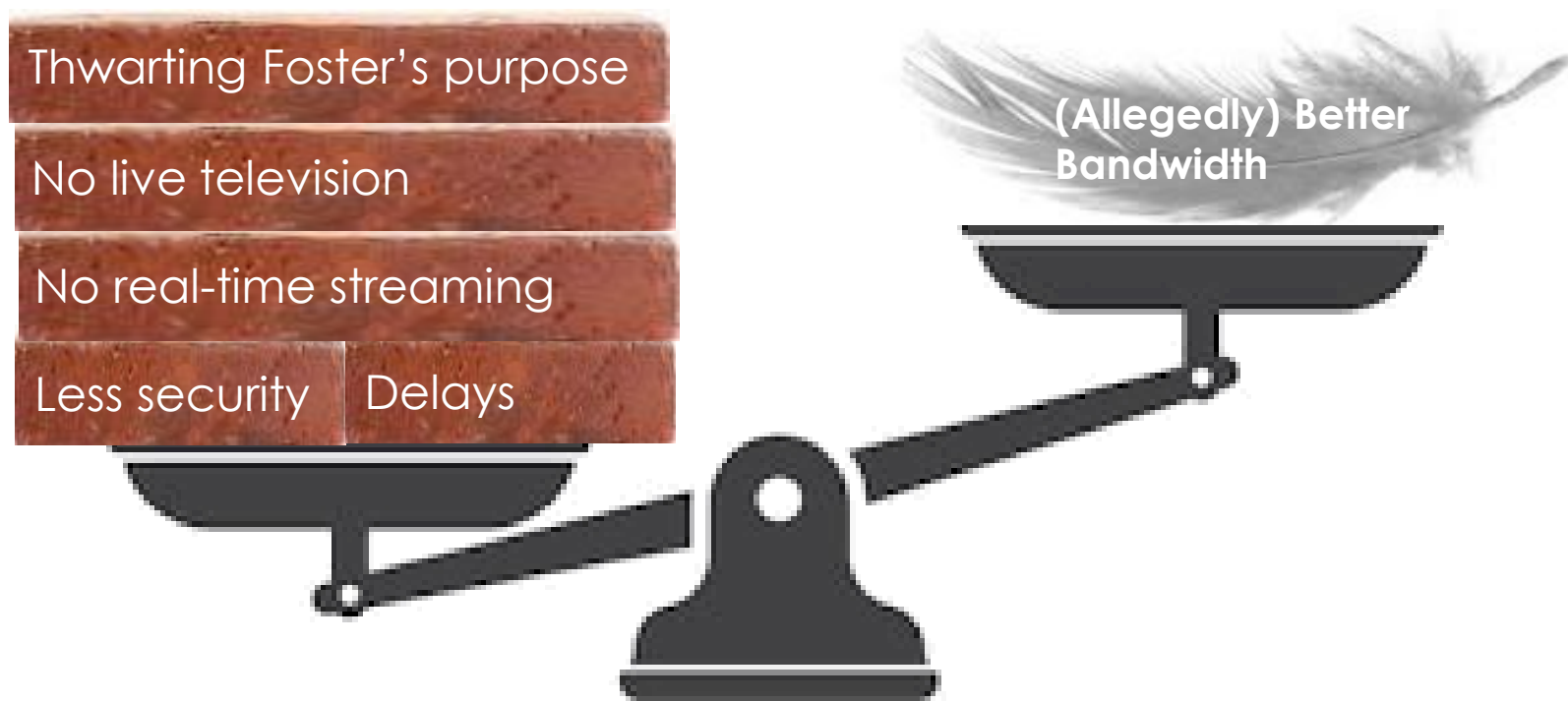
“[t]he Board must **weigh the benefits and drawbacks** of the modification against each other, to determine whether there would be a motivation to combine.”

Arctic Cat Inc. v. Polaris Indus., 795 Fed. App'x. 827, 833 (Fed. Cir. 2019)

“Coupled with testimony confirming the **potential problems** of automatic throttle reapplication and suggesting **an alternative approach might reduce those same problems**, J.A. 2230-32, a jury could find **a skilled artisan would not have been motivated to combine ...**”

Arctic Cat Inc. v. Bombardier Rec. Prods., 876 F.3d 1350, 1363 (Fed. Cir. 2017)

The Drawbacks Outweigh The Benefits



Petitioner May Not Change Its Theory In Reply



“Petitioner **may not submit new** evidence or **argument** in reply that it could have presented earlier, e.g. **to make out a prima facie case of unpatentability.**”

Consolidated Trial Practice Guide, 73 (Nov. 2019)



“the expedited nature of IPRs bring with it **an obligation for petitioners to make their case in their petition to institute.**”

Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd., 821 F.3d 1359, 1369 (Fed. Cir. 2016)

“We see no error in the Board’s rejection of Ariosa’s reliance, in its Reply submissions, **on previously unidentified portions of a prior art reference to make a meaningfully distinct contention.**”

Ariosa Diagnostics v. Verinata Health, Inc., 805 F.3d 1359, 1368 (Fed. Cir. 2015)

Petitioner Shifts Its Theory In Reply From Reliance Upon Hayhurst's Storage Devices To "Foster's Storage Context"

PETITION FOR INTER PARTES REVIEW UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §42.1 et seq

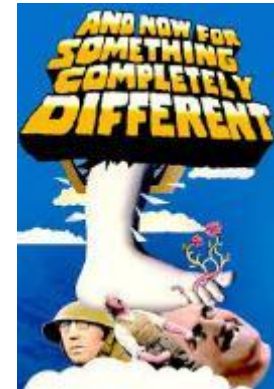
POSAs had reason to store Foster's encrypted content units on multiple storage devices (*e.g.*, consumer set-top boxes like Hayhurst's subscriber units and Foster's recipients 430) based on Hayhurst's techniques for storing and distributing encrypted data segments. Bhattacharjee, ¶182.

POSAs would have recognized several benefits in storing Foster's encrypted content units distributed on different storage devices as Hayhurst teaches. Foster's



PETITIONER'S REPLY TO PATENT OWNER RESPONSE

1322, 1331 (Fed. Cir. 2012). Foster's teachings are not limited to live-streaming, as Foster teaches **storing** encrypting content for and by recipient(s) (*e.g.*, video-on-demand). Foster, [0064]. In (at least) Foster's storage context—relied upon in the Petition (65, 80-82)—POSAs would have recognized the benefits of combining Foster with Hayhurst. Bhattacharjee-Reply, ¶¶48-57.



Petition Relied Upon Hayhurst's Storage Method, Not Foster's

PETITION FOR INTER PARTES REVIEW UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §42.1 et seq

The Foster-Hayhurst combination would have used Foster's technique of encrypting portions of a data set with respective encryption keys that are themselves encrypted with a KEK that is stored in a key-storage system, and Hayhurst's technique of storing the encrypted data on different storage devices. Bhattacharjee,

device)); also the combination's recipients are implemented with the functionality of Hayhurst's subscriber units, including their storage devices. §VII.C;

No Mention Of "Foster's Storage Context"

Reply: Petitioner Relies Upon “Foster’s DRMS” For The First Time

Petition

- No mention of DRMS
- Alleged “storage device” is a set-top box, not a personal computer

Reply

“In **Foster’s DRMS**, ‘content is packaged and loaded [i.e., stored] onto a web server’ and subsequently ‘downloaded to [i.e., stored to a] **personal computer**’ for on-demand access (i.e., viewing stored content whenever the user wants to).”

Reply, 8.



Reply: Petitioner Relies Upon Foster's "Program Stream" For The First Time

Petition



Reply

“Foster discloses processing datasets for an **MPEG ‘program stream,’** which Foster says (and POSAs knew) is intended for storing ‘in fixed storage.’” Reply, 9.



Even If Considered, New Reply Theories Fail



Reply: “Foster’s DRMS” Is Evidence Of Foster’s “Storage Context”

PETITIONER’S REPLY TO PATENT OWNER RESPONSE

Foster recognizes that synchronization reduces latency for storage-based purposes, like for Digital Rights Management Systems (“DRMSs”). Foster, [0064] (“[A] recipient will receive or **store** encrypted content...”). Rubin-Depo., 83-85, 96-99. In Foster’s DRMS, “content is packaged and **loaded** [i.e., stored] onto a web server” and subsequently “**downloaded to** [i.e., stored to a] personal computer” for on-demand access (i.e., viewing stored content whenever the user wants to). Foster, [0005], [0049] (users access “content on [the] media server”); FIG. 1 (content is “stream[ed] or **stored**”); EX2039, 6-10 (DRMS “safeguards **content** when **at rest** [i.e., stored],” and when “**stored** on a receiving device”). Foster’s synchronization

DRMS Is Background Art Foster's Invention Replaces

(12) Patent Application Publication Foster et al.

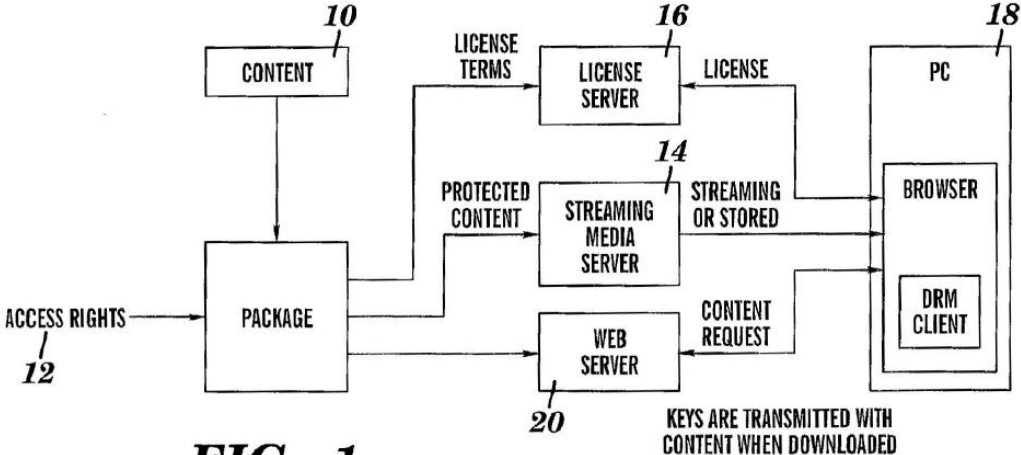


FIG. 1

Prior Art

[0003] 2. Background Art

[0005] Current technologies that utilize key-based security practices include a personal computer-based Digital Rights Management System (DRMS) and a Conditional Access System (CAS). In the case of the former, content is packaged

the keys is risked. Moreover, both DRMS and CAS can have inherent latencies in providing random access of protected content.

[0007] In view of the foregoing, there exists a need for a method, system and program product for attaching a key to encrypted content for synchronized transmission to, or storage by, a receiver. That is, a need exists for a key used to

[0049] Referring now to FIG. 1, a depiction of a Digital Rights Management System (DRMS) is shown. As depicted,

[0051] As indicated above, the DRMS fails to provide synchronized delivery of the content with the keys used to encrypt the content. That is, license server 16 must be separately accessed. When providing the keys in such a manner, there exists a likelihood that either the appropriate keys will not be matched with the encrypted content, or a single key will be used, weakening the security. Furthermore, providing keys from license server 16 requires a back channel.

Figure 1's DRMS Does Not Include Foster's Invention

(12) Patent Application Publication
Foster et al.

[0049] Referring now to **FIG. 1**, a depiction of a Digital Rights Management System (DRMS) is shown. As depicted,

[0051] As indicated above, the DRMS fails to provide synchronized delivery of the content with the keys used to encrypt the content. That is, license server 16 must be separately accessed. When providing the keys in such a manner, there exists a likelihood that either the appropriate keys will not be matched with the encrypted content, or a single key will be used, weakening the security. Furthermore, providing keys from license server 16 requires a back channel.

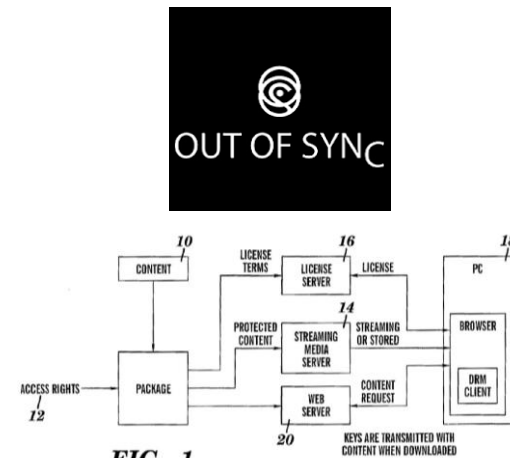


FIG. 1

SAMRAT BHATTACHARJEE

Q. Why does synchronous transmission to a receiver foster random access to content?

A That is sort of the whole invention in Foster.

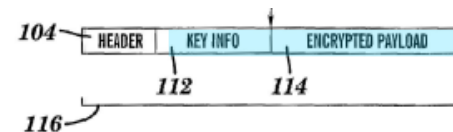


FIG. 8

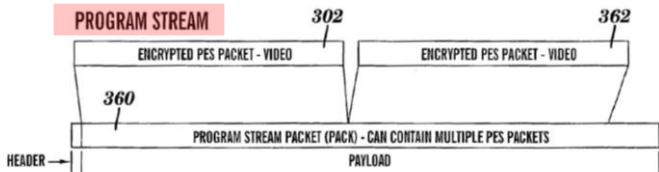
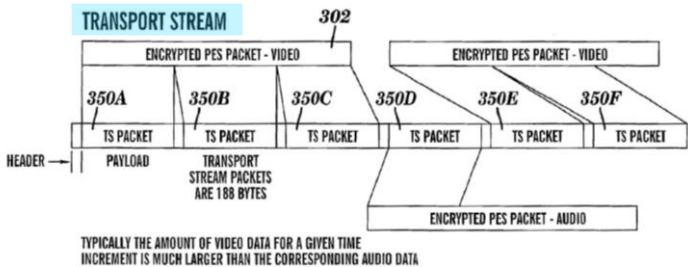
Reply: Foster's Program Stream Is For "Fixed Storage"

PETITIONER'S REPLY

Consistent with its DRMS disclosures, Foster discloses processing datasets for an MPEG "program stream," which Foster says (and POSAs knew) is intended for storing "**in fixed storage.**" Foster, [0073]; *see also* EX2014, 1 ("[p]rogram streams are **designed for...storage**"); EX1108, 1:65-2:31; EX1109, 1-9, 13);

Petitioner's Combination Would Use A Transport Stream (For, e.g., Cable TV), Not A Program Stream (e.g., for DVDs)

(12) Patent Application Publication Foster et al.



[0073] Once the encrypted key (and any optional identifier information and/or verifier) has been attached to PES packet 306, the resulting PES unit 302 can then be multiplexed in two different system options. The first is shown in FIG. 14 and is known as a transport stream. A transport stream is typically used in error-prone broadcast environments such as digital television. As depicted, transport stream packets 350A-F are relatively small, and it generally takes multiple transport stream packets 350A-C to contain a single video PES unit 302. The second option is a program stream, which is shown in FIG. 15. A program stream is generally used in more reliable transmissions such as those with error correcting codes or in fixed storage. Unlike transport stream packets, however, a single program stream packet 360 can hold multiple video PES units 302 and 362.

(12) Patent Application Publication Hayhurst

[0016] With reference to FIG. 1, a preferred embodiment of the present invention includes a network 20 of electronically connected subscribers A, B, C, and D. The small number of subscribers depicted here is intended to be representative of, for example, the thousands of subscribers that may be part of a typical cable television (CATV) network. Alternatively, the network can be any other communications network of users or subscribers, such as those linked by a local area network (LAN) or a wide area network (WAN).



Foster-Hayhurst Fails (IPR2024-00212, -00215)

- ❑ Hayhurst Is Not Analogous Art (IPR2024-00212, -00215)
- ❑ No Motivation To Combine Foster-Hayhurst Shown (IPR2024-00212, -00215)
- **Foster's Packets/Payloads Are Not Shares/Chunks (IPR2024-00214, -00215)**

'854/'609 Claims Require "Generating A Plurality Of Data Chunks"

US 10,452,854 B2

1. A method for securely storing a data set, the method comprising:
receiving an external key from an external storage system,
generating a plurality of data chunks based on the data set,
such that the data set can be reconstructed using at least
a minimum number of the plurality of data chunks,
wherein generating the data chunks comprises:
distributing the data set into a plurality of shares,
wherein each of the shares comprises less than all of
the data set,

US 11,068,609 B2

1. A method for securing data, the method comprising:
executing code by a processor to perform:
receiving a first key from a storage system;
generating a plurality of data chunks based on a data
set, wherein each data chunk of the plurality of data
chunks comprises less than an entirety of data of the
data set, and wherein the data set can be recon-
structed using at least a minimum number of the
plurality of chunks;

Petitioner: Foster's Packets/Payloads Are Chunks/Shares

PETITION FOR INTER PARTES REVIEW
UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §42.1 et seq

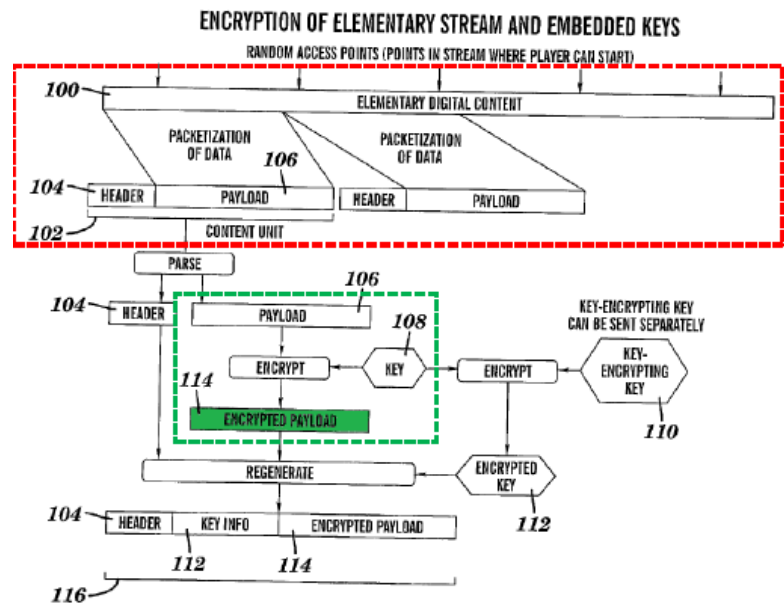


FIG. 8

illustrated in Foster's Figure 8 (red-box annotation below), Foster generates a plurality of "payloads" by "parcel[ing]" the elementary content stream (the claimed "data set," §VII.D.2 [1A]). Foster, [0064]; Bhattacharjee, ¶¶201-02.

As discussed further below (§VII.D.4 [1B1], §VII.D.6 [1B3]) and illustrated in Figure 8 (green-box above), the payloads ([1B1]'s "shares") are encrypted to generate encrypted payloads, which are "a plurality of data chunks based on the data set," as claimed. POSAs thus understood Foster to meet SFI's construction of

Undisputed: The Petition Did Not Explain Why Foster's Payloads Are Shares/Chunks

PETITION FOR INTER PARTES REVIEW UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §42.1 et seq



illustrated in Foster's Figure 8 (red-box annotation below), Foster generates a plurality of "payloads" by "parcel[ing]" the elementary content stream (the claimed "*data set*," §VII.D.2 [1A]). Foster, [0064]; Bhattacharjee, ¶¶201-02.

As discussed further below (§VII.D.4 [1B1], §VII.D.6 [1B3]) and illustrated in Figure 8 (green-box above), the payloads ([1B1]'s "*shares*") are encrypted to generate encrypted payloads, which are "*a plurality of data chunks based on the data set*," as claimed. POSAs thus understood Foster to meet SFI's construction of

Undisputed: Foster's Packets/Payloads Are Data Packets That Are Part Of The MPEG Protocol

Foster et al.

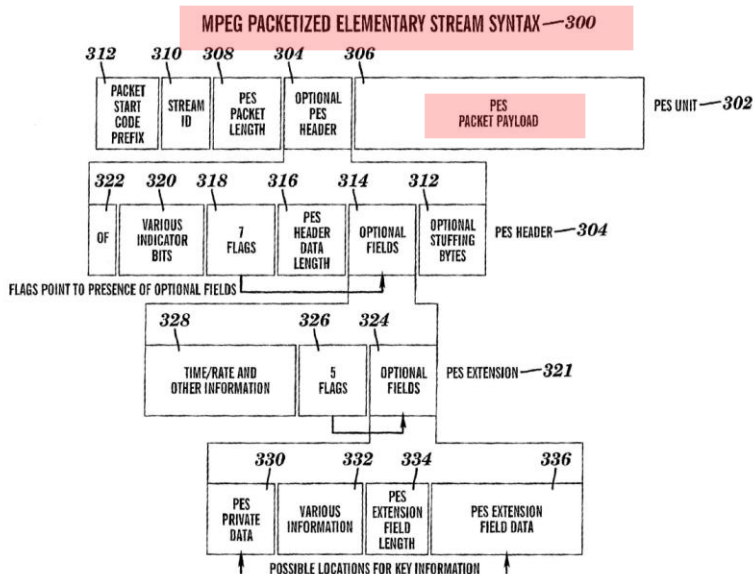


FIG. 13

[0072] Referring now to FIG. 13, an exemplary MPEG embodiment of the present invention is depicted. As shown, a MPEG packetized elementary stream 300 is parceled into PES (packet) units 302 (only one shown for clarity purposes). PES unit 302 includes packetized elementary stream (PES) packet payload 306, optional PES header 304, packet length 308, stream identification 310 and start code prefix 312. PES packet payload 306 will be encrypted with a title key, which will then be encrypted with a key encrypting key and embedded in PES unit 302 as header extension 321. As

DECLARATION OF AVIEL D. RUBIN, PH.D.

Pet., 72-74. Foster teaches that these “payloads” refer to the payloads of MPEG Packetized Elementary Stream (PES) packets (also referred to in Foster as “units”), as illustrated below in Figure 13:

Ex. 1006 [Foster] Fig. 13, [0072] (“a MPEG packetized elementary stream 300 is parceled into PES (packet) units 302 PES unit 302 includes packetized elementary stream (PES) packet payload 306” which “will be encrypted with a title key”). Foster’s PES packets are also referred to as “data packets.” See Ex. 2011 [Tsai] [0001], cl. 1. Consequently, Petitioner and Dr. Bhattacharjee map the

Undisputed: Specification Identifies A Data Packet/Payload As The Dataset To Be Divided Into Shares

(10) **Patent No.:** US 10,452,854 B2

At step 4106, the data packet or data block may then be partitioned into two or more data shares using one of the data splitting algorithms described above in accordance with the present invention. In some embodiments, the data packet or

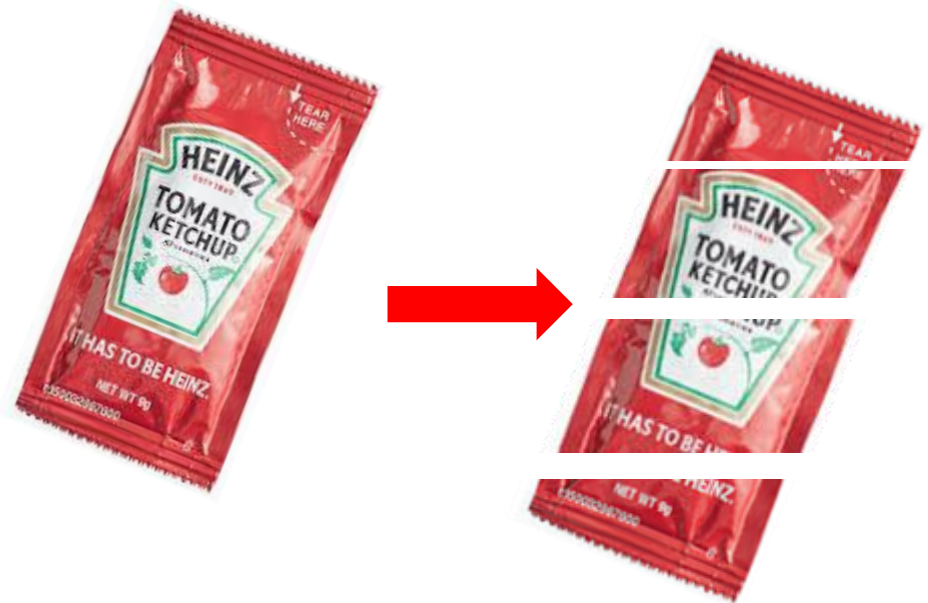
'854, 82:21-24

a predetermined number of shares. Packets of data (e.g., network packets) may also be efficiently split and restored

'854, 81:36-37

and a data partitioning phase. Simplified header generation process 4000 and simplified data partitioning process 4010 are shown in FIGS. 40A and 40B, respectively. One or both of these processes may be performed on network packets, file system blocks, or any other suitable information.

'854, 81:54-58



“each node sends out **3 shares in a single packet**”

“These services allow **breaking down packet payloads into smaller units (called chunks)** ...” Ex. 2037 [Li-I] 1

“We break [data packet] D into n shares ...” Ex. 2043 [Mao] 9532

“A packet consists of multiple chunks...”

“to consistently **divide ... packet payloads into multiple byte sequences, called chunks.**” Ex. 2036 [Hur] 1202

“the **payload could be divided into multiple equal-sized chunks ...**” Ex. 2041 [Li-III] 7

Dr. Rubin: Patents' Shares/Chunks Generated To Secure Data While Foster's Packets/Payloads Part Of MPEG Standard

(10) Patent No.: US 10,452,854 B2

Traditional encryption technologies known in the art rely on one or more key used to encrypt the data and render it unusable without the key. The data, however, remains whole and intact and subject to attack. The secure data parser of the present invention, in one embodiment, addresses this problem by performing a cryptographic parsing and splitting of the encrypted file into two or more portions or shares, and in another embodiment, preferably four or more shares, adding another layer of encryption to each share of the data, then storing the shares in different physical and/or logical locations. When one or more data shares are physically

'854, 56:47-51

(12) Patent Application Publication Foster et al.

[0072] Referring now to FIG. 13, an exemplary MPEG embodiment of the present invention is depicted. As shown, a MPEG packetized elementary stream 300 is parceled into PES (packet) units 302 (only one shown for clarity purposes). PES unit 302 includes packetized elementary stream (PES) packet payload 306, optional PES header 304, packet length 308, stream identification 310 and start code prefix 312. PES packet payload 306 will be encrypted with a title key, which will then be encrypted with a key encrypting key and embedded in PES unit 302 as header extension 321. As

Ex. 1006, [0072]

DECLARATION OF AVIEL D. RUBIN, PH.D.

149. Nor does the '854's discussion of shares suggest that a packet payload would be deemed a "data share" or a "data chunk" when encrypted. As the '854 explains, partitioning the data set into chunks increases security because when "data ... remains whole and intact," it is "subject to attack." The '854 addresses this concern, in part, by "performing a cryptographic parsing and splitting of the encrypted file." Ex. 1001 ['854] 56:47-61. Thus, the '854 teaches that splitting the data set into shares helps secure the data.

150. A packet payload (as in Foster as well as Hayhurst), however, does not exist to protect the data. Rather it exists by virtue of the MPEG packetized elementary stream standard. Ex. 1006 [Foster] [0072]-[0073]; Ex. 2014 [Overview-of-MPEG-2-Systems] ("An elementary stream is broken up into packets, forming a *packetized elementary stream* (PES)."). These packets allow for transmission of the content. See Ex. 2015 [Newton's-Telecom-Dictionary] 626

Petitioner Fails To Provide Any Evidence Showing That Packets/Payloads Refer To Chunks/Shares



Petitioner's Straw Man Argument: "SFI Suggests A Share Must Be 'Cryptographically Generated'"

PETITIONER'S REPLY

SFI suggests a *share* must be "cryptographically generated" so the splitting of the *data set* by itself makes it less susceptible to "attack." POR, 68-69. But the



PATENT OWNER'S SUR-REPLY

Petitioner ignores these portions and alleges that "SFI suggests a share must be 'cryptographically generated' so the splitting of the data set by itself makes it less susceptible to 'attack.'" *Id.*, 15. But, as seen above, this is not and has never been Patent Owner's position. Rather, the '854's specification gives several examples of how a dataset may be split and is clear that a packet or its payload is itself a dataset that is split into shares or chunks, regardless of whether the split is performed cryptographically. Ex. 1001 ['854] 82:21-24, 81:36-37, 81:54-58.

Petitioner's Grounds

1. Foster Grounds

a) Foster and Hayhurst (IPR2024-00212/215)

b) Foster Alone (IPR2024-00214)

2. Orsini Grounds (IPR2024-00214/215)

3. Tajima Grounds (IPR2024-00212)

Petitioner Relies On Foster Alone in -00214 IPR

Case No. IPR2024-00214
Patent No. 11,068,609

Ground Number and Reference		Claims	Basis
1	Orsini (EX1005)	1-10	§§102/103
2	Foster (EX1006)	1-3, 7-8	§§102/103
		4-6, 9-10	§103

Foster Fails (IPR2024-00214)

- **Foster's CPU Does Not "Execut[e] Code" "To Perform" "Storing ... At Least One Data Chunk"**
- ❑ Foster's CPU Is Not "Coupled To" A "Memory" On Foster's Receiver/Recipient
- ❑ No Motivation To Modify Foster As Proposed

Petitioner's Anticipation Argument: Foster's CPU Is The "Processor" And "Recipient 430" Is The Storage Device

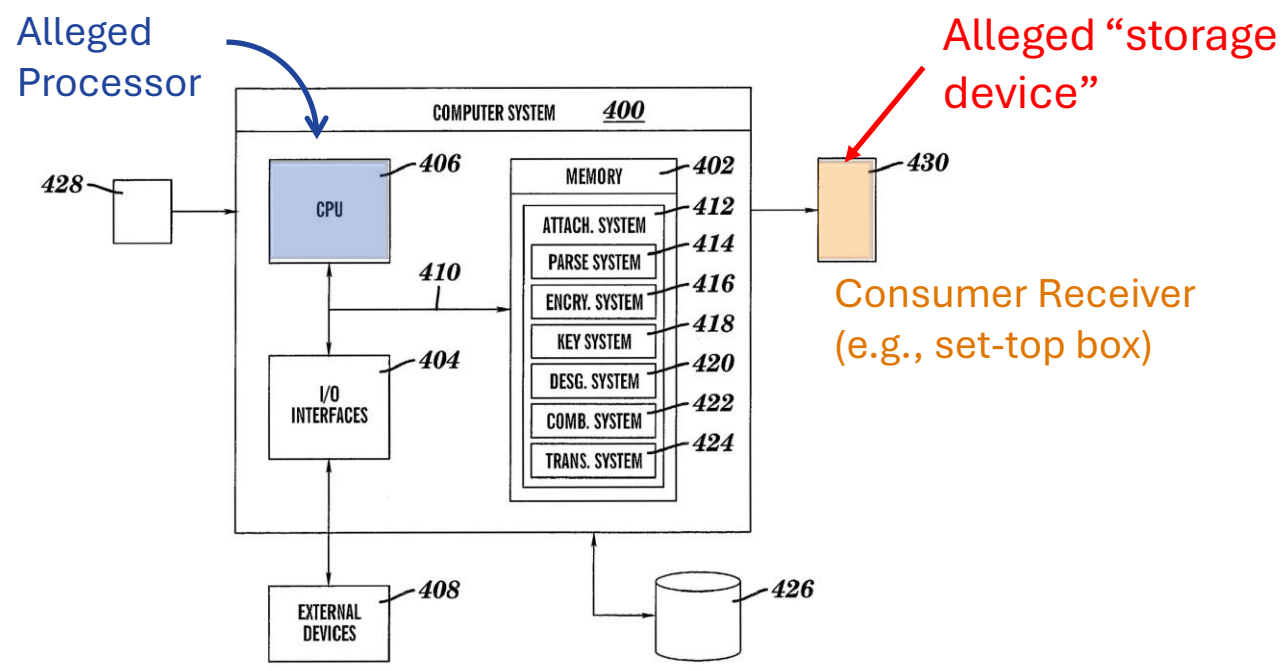


FIG. 16

No showing that Foster's CPU "executes code" to "perform storing" on STB

The Recipient Is Not A Part Of Foster's Computer System

DECLARATION OF AVIEL D. RUBIN, PH.D.



110. As can be seen in Foster's Figure 16 below, Foster's **recipient 430** is not part of the **computer system 400** which contains **CPU 406**:

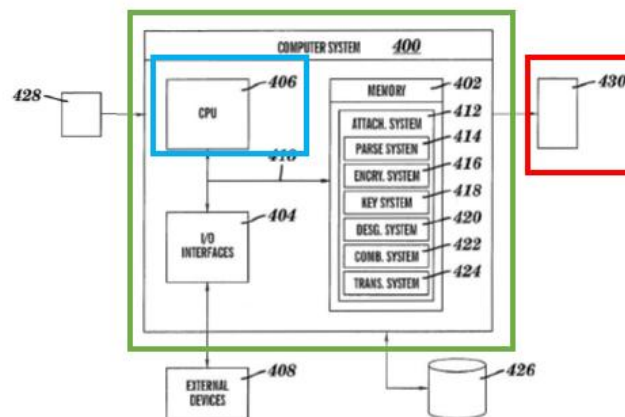


FIG. 16

Ex. 1006 [Foster] Fig. 16, [0075] (listing what “computer system 400 generally comprises,” not including recipient 430). Consequently, for Foster’s CPU 406 to “execute code ... to perform” “storing ... at least one data chunk,” Foster’s CPU 406 must at least instruct recipient 430 to store or perform some action related to storing a content unit.

Petitioner's Explanation As To How Foster's CPU Executes Code To Store Content On Recipient?



Undisputed: Foster's CPU Transmits Content And Is Agnostic As To What Receiver Does With It

DECLARATION OF AVIEL D. RUBIN, PH.D.



111. Foster, however, teaches that its computer system 400 merely

“transmit[s] the processed content units to [the] recipient 430.” *Id.*, [0078]. Once

instructing recipient 430 to store the content. Fundamentally, in Foster's system,

computer system 400 is agnostic as to what the recipients do with the content units,

(12) Patent Application Publication Foster et al.

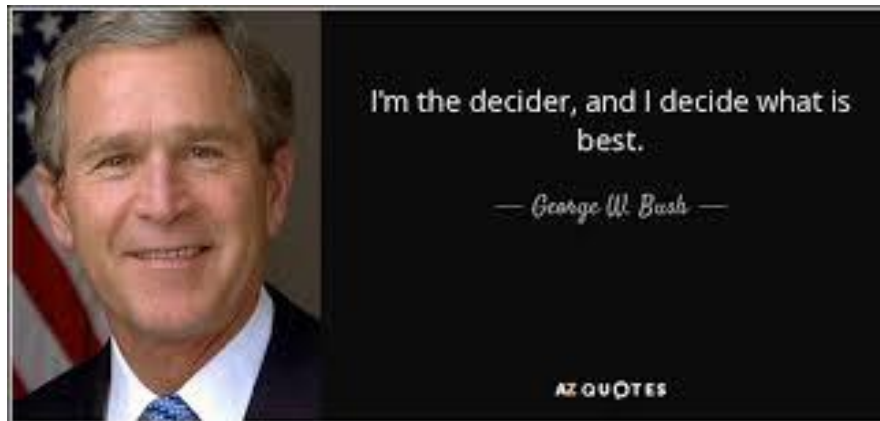
[0078] It should be understood that computer system 400 is intended to be representative of any system capable of processing content units of an elementary content stream received from source 428, and transmitting the processed content units to a recipient 430. Stored in memory 402 is attachment system 412, which includes parsing system 414, encryption system 416, key system 418, designation system 420, combination system 422 and transmission system 424.



Undisputed: Foster's Recipient 430 Decides Whether To Store Or Instantly Display Content

DECLARATION OF AVIEL D. RUBIN, PH.D.

111. Foster, however, teaches that its computer system 400 merely “transmit[s] the processed content units to [the] recipient 430.” *Id.*, [0078]. Once the recipient 430 receives the content unit, the “recipient 430 *can*,” if it so chooses “then synchronously store the encrypted content and attached title key.” *Id.*, [0079]. Significantly, Foster teaches that recipient 430 can also instantly display the content units rather than storing them, which would be the typical usage in the television context Foster contemplates. *See id.*, [0008] (content unit processed “for



Undisputed: Foster's Content Units Contain No Instructions

(12) **Patent Application Publication**
Foster et al.

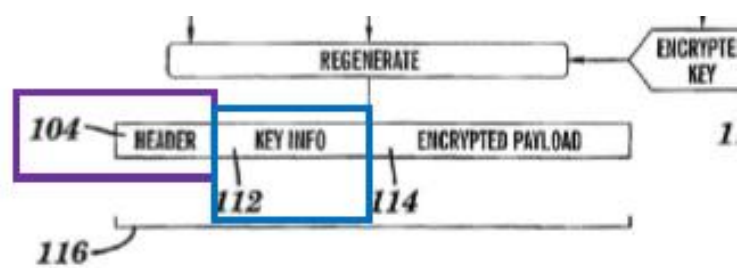


FIG. 8

a header 104 and a content packet 106. Header 104 includes information helpful in identifying the content such as a time stamp, type of content: video, audio or other. Header 104 is especially useful, for example, in synchronizing sound data with video data. Once parceled, header 104 of each content

[0066] Referring now to FIG. 9, header extension 118 is shown in greater detail. As depicted, header extension 118 includes encrypted title key 112, optional identifier information 120 and optional verifier 122. Identifier information 120 is clear text information such as a fixed value indicating encrypted content, a version number and/or mask values used to avoid aliasing of reserved bit patterns. The mask values are used to prevent key information or other data in a header extension from aliasing a known code. Specifically, the mask values indicate to modify (e.g., invert) part or all of the key information so as to distinguish it from a known code that may have a specialized purpose. This avoids a possible erroneous code detection. Verifier 122, if used, is a value that allows a recipient to verify that the correct title key has been recovered.

DECLARATION OF AVIEL D. RUBIN, PH.D.

Indeed, Foster only teaches sending a header and a header extension with key information along with the encrypted payload:

Ex. 1006 [Foster] Fig. 8, [0064] (“the encrypted content unit, the header and the header extension (including the encrypted title key) will be delivered to, or stored by, a recipient as a single, integral data stream.”); Ex. 2034 [Bhattacharjee-Depo.] 55:15-18. The header “includes information helpful in identifying the content such as a time stamp, type of content: video, audio or other” and “is especially useful, for example, in synchronizing sound data with video data.” Ex. 1006 [Foster] [0064]. The header extension “includes encrypted title key 112, optional identifier information 120 and optional verifier 122.” *Id.*, [0066]. Notably, Foster does not teach that the header or the header extension contains instructions on what the receiver should do with the content units upon receipt. Consequently, the decision

Instructions not INCLUDED

Reply Incorrectly Contends POR Offers New Construction

PETITIONER'S REPLY

SFI argues Foster's processor is "agnostic as to what the recipient does with" content and fails to "instruct the recipient to store or perform some action related to storing." POR, 43-44. This is a new construction (EX1060) and SFI identifies no intrinsic evidence requiring the processor to instruct a storage device. *Wasica*



The Plain Language Requires The Processor To Execute Code To Perform Storing

1. A method for securing data, the method comprising:
executing code by a processor to perform:

receiving a first key from a storage system;
generating a plurality of data chunks based on a data set, wherein each data chunk of the plurality of data chunks comprises less than an entirety of data of the data set, and wherein the data set can be reconstructed using at least a minimum number of the plurality of chunks;

encrypting each respective data chunk of the plurality of data chunks with a respective second key, wherein each of the respective second keys are distinct from each other;

performing a cryptographic operation based on the first key to further secure the plurality of data chunks; and
storing, in a memory coupled to the processor, at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys on at least one storage device.



Reply: Petitioner Still Does Not Identify Code To Perform Storing

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

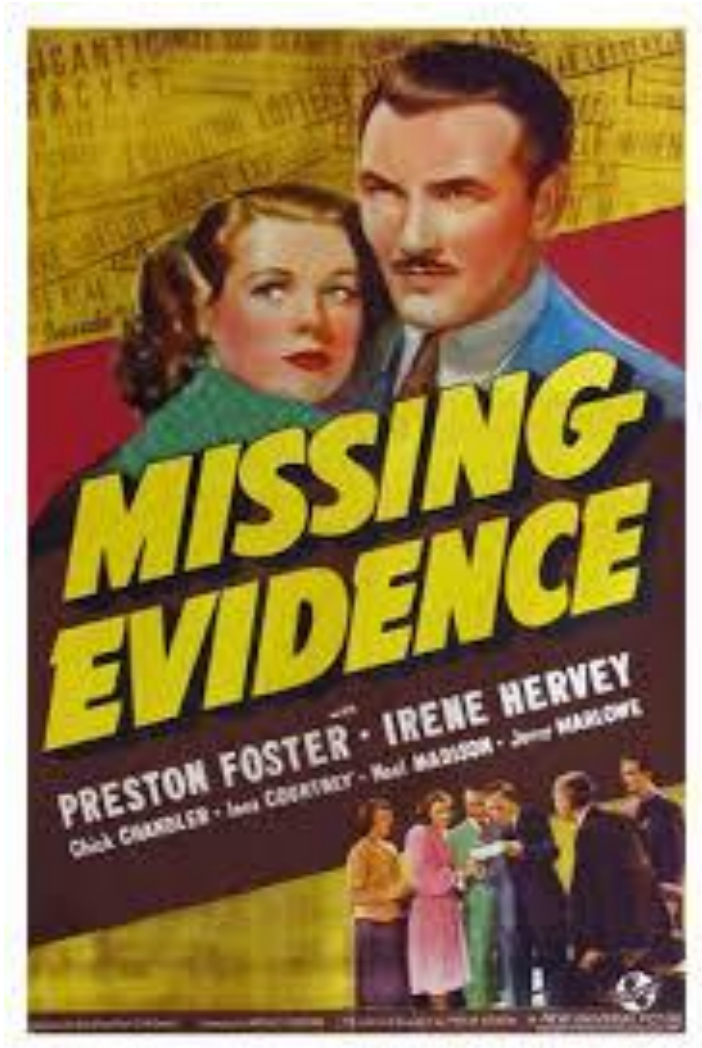
GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC
Patent Owner.

Case No. IPR2024-00214
Patent No. 11,068,609

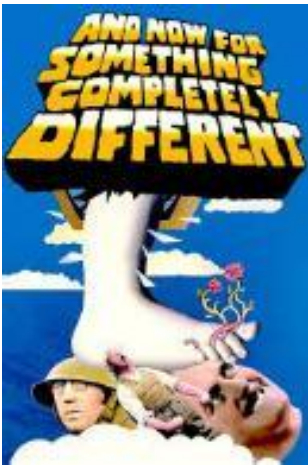
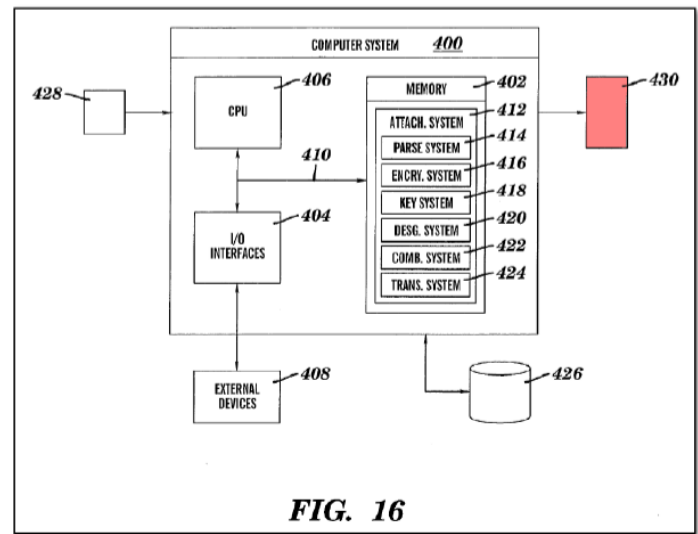
PETITIONER’S REPLY TO PATENT OWNER RESPONSE



Rather, Petitioner Shifts Its Theory To Foster's Memory 402 Instead Of Recipient 430

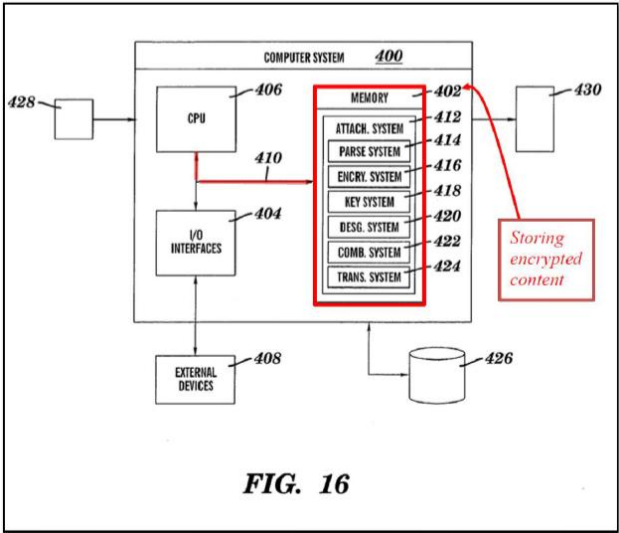
Petition

“Each content unit 116 discussed above is stored on receiver at ‘**receipt 430**’; that receiver is a ‘storage device’ (e.g., consumer set-top box)” Pet., 75.



Reply

“Foster’s processor executes code that encrypts and stores data on **storage-device memory (RAM)** directly coupled to it.” Reply, 7-8.



Petitioner's New Theory Is Untimely



“Petitioner **may not submit new** evidence or **argument** in reply that it could have presented earlier, e.g. **to make out a prima facie case of unpatentability.**”

Consolidated Trial Practice Guide, 73 (Nov. 2019)

“the expedited nature of IPRs bring with it **an obligation for petitioners to make their case in their petition to institute.**”

Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd., 821 F.3d 1359, 1369 (Fed. Cir. 2016)

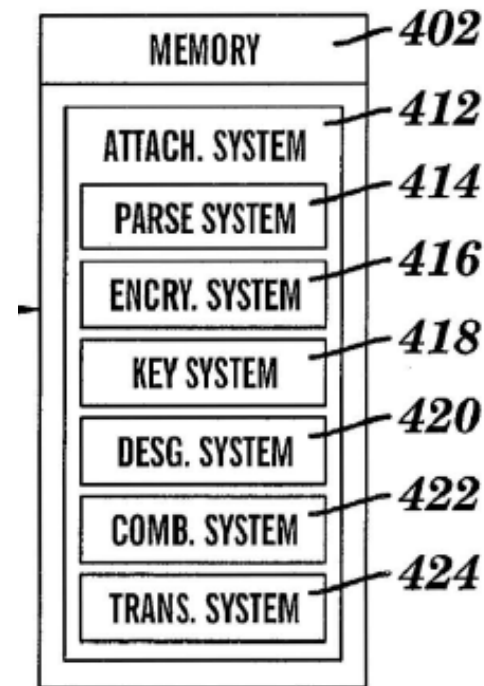
“We see no error in the Board’s rejection of Ariosa’s reliance, in its Reply submissions, **on previously unidentified portions of a prior art reference to make a meaningfully distinct contention.**”

Ariosa Diagnostics v. Verinata Health, Inc., 805 F.3d 1359, 1368 (Fed. Cir. 2015)

Foster's Memory 402 Does Not Store Content Or Content Units

(12) Patent Application Publication Foster et al.

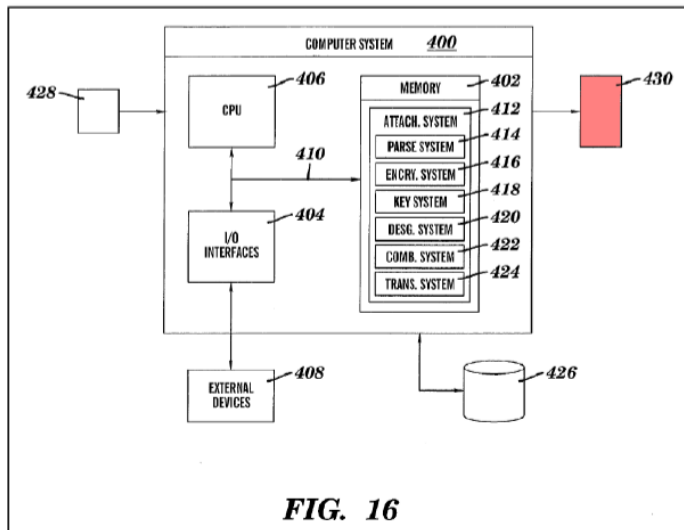
[0078] It should be understood that computer system 400 is intended to be representative of any system capable of processing content units of an elementary content stream received from source 428, and transmitting the processed content units to a recipient 430. Stored in memory 402 is attachment system 412, which includes parsing system 414, encryption system 416, key system 418, designation system 420, combination system 422 and transmission system 424.



Reply: Petitioner Also Shifts To Relying Upon “Foster’s DRMS”

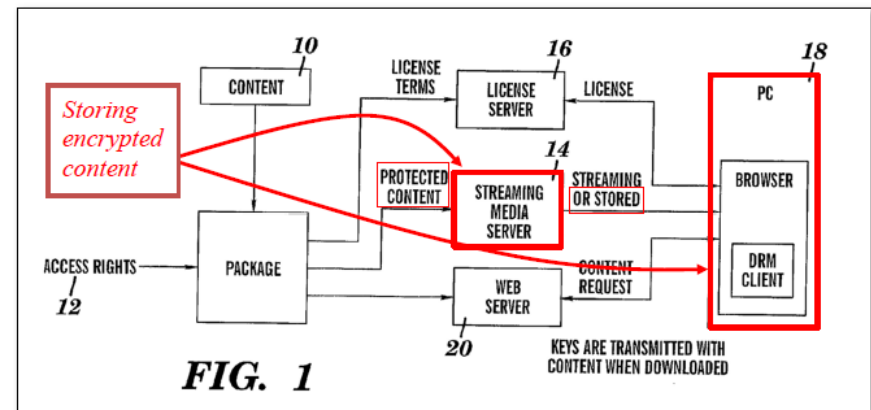
Petition

“Each content unit 116 discussed above is stored on receiver at ‘**receipt 430**’ [sic]; that receiver is a ‘storage device’ (e.g., **consumer set-top box**)” Pet., 75.



Reply

“Foster’s processor executes code to ‘package[...and load[encrypted data] onto **media server 14**,’ which is later ‘downloaded to **PC 18**.’” Reply, 9.



DRMS Is Background Art Foster's Invention Replaces

(12) **Patent Application Publication**
Foster et al.

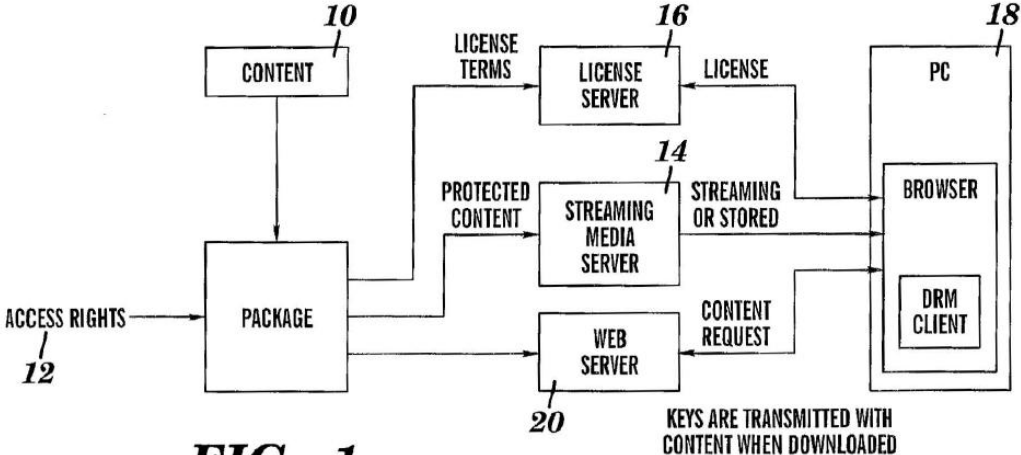


FIG. 1

Prior Art

[0003] 2. Background Art

[0005] Current technologies that utilize key-based security practices include a personal computer-based Digital Rights Management System (DRMS) and a Conditional Access System (CAS). In the case of the former, content is packaged

the keys is risked. Moreover, both DRMS and CAS can have inherent latencies in providing random access of protected content.

[0007] In view of the foregoing, there exists a need for a method, system and program product for attaching a key to encrypted content for synchronized transmission to, or storage by, a receiver. That is, a need exists for a key used to

[0049] Referring now to FIG. 1, a depiction of a Digital Rights Management System (DRMS) is shown. As depicted,

[0051] As indicated above, the DRMS fails to provide synchronized delivery of the content with the keys used to encrypt the content. That is, license server 16 must be separately accessed. When providing the keys in such a manner, there exists a likelihood that either the appropriate keys will not be matched with the encrypted content, or a single key will be used, weakening the security. Furthermore, providing keys from license server 16 requires a back channel.

Petitioner Does Not Explain Why A POSITA Would Be Motivated To Combine Foster's Invention With Criticized Prior Art



“[I]t is not enough that the prior art reference ... includes multiple, distinct teachings that the artisan might somehow combine to achieve the claimed invention’ to show anticipation.”

BlephEx, LLC v. Myco Indus., 24 F.4th 1391, 1400 (Fed. Cir. 2022)

when “combining multiple embodiments from a single reference, or selecting from large lists of elements in a single reference, **there must be a motivation to make the combination ...**”

In re Stepan Co., 868 F.3d 1342, 1346 n.1 (Fed. Cir. Aug. 2017)

Reply: Petitioner Also Newly Argues Foster Encodes Content As A “Program Stream” For “Fixed Storage”

Petition



Reply

Foster’s processor **executes code to encrypt content for ... [a] ‘program stream’**.... Foster explicitly says the program stream ‘is generally used in more reliable transmissions such as those...in fixed storage.’” Reply, 10.



Encoding A Program Stream Is Not “Executing Code ... To Perform” “Storing”

(12) Patent Application Publication Foster et al.

[0073] Once the encrypted key (and any optional identifier information and/or verifier) has been attached to PES packet 306, the resulting PES unit 302 can then be multiplexed in two different system options. The first is shown in FIG. 14 and is known as a transport stream. A transport stream is typically used in error-prone broadcast environments such as digital television. As depicted, transport stream packets 350A-F are relatively small, and it generally takes multiple transport stream packets 350A-C to contain a single video PES unit 302. The second option is a program stream, which is shown in FIG. 15. A program stream is generally used in more reliable transmissions such as those with error correcting codes or in fixed storage. Unlike transport stream packets, however, a single program stream packet 360 can hold multiple video PES units 302 and 362.

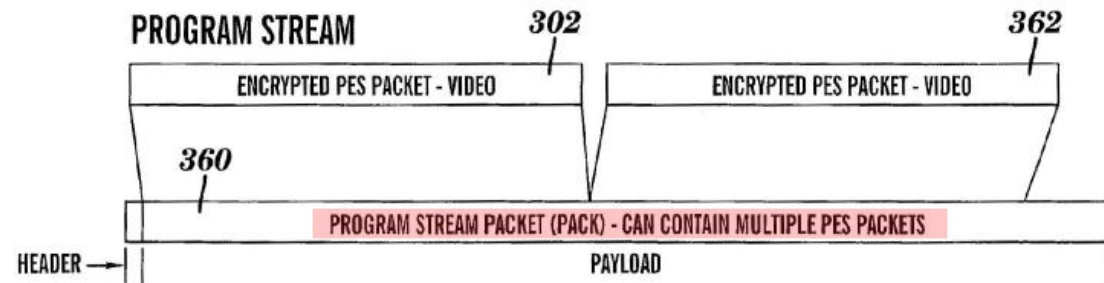


FIG. 15

No “Storing” “Perform[ed]”

Foster Fails (IPR2024-00214)

- ❑ Foster's CPU Does Not "Execut[e] Code" "To Perform" "Storing ... At Least One Data Chunk"
- **Foster's CPU Is Not "Coupled To" A "Memory" On Foster's Receiver/Recipient**
- ❑ No Motivation To Modify Foster As Proposed

Anticipation Theory: Receiver's Hard Drive Is Coupled To CPU Via Bus 410 And Transmission System 424

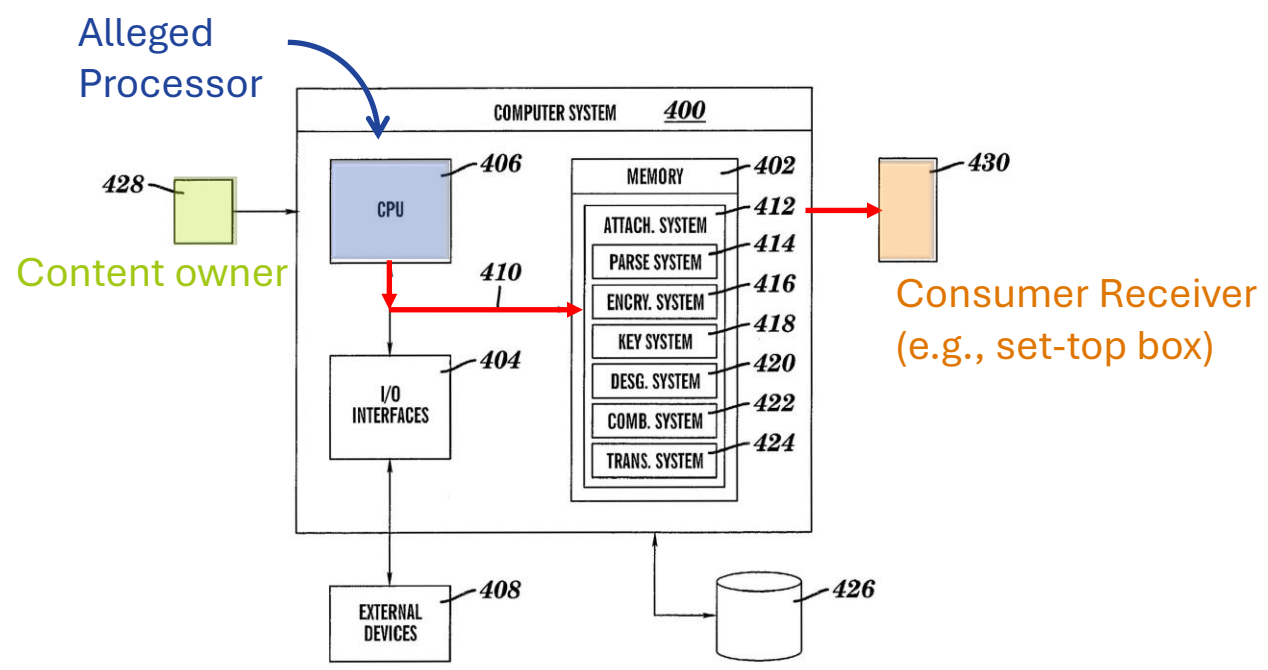


FIG. 16

But, Foster's CPU Is, At Most, Coupled To The Receiver, Not Any Hard Drive On The Receiver

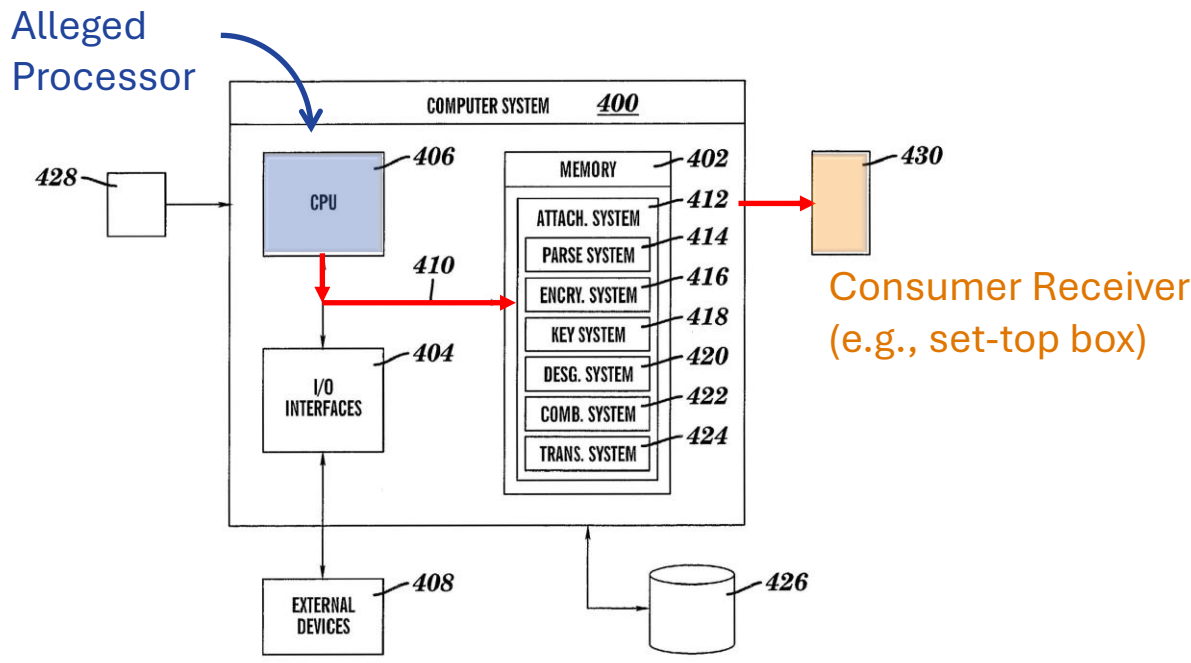


FIG. 16

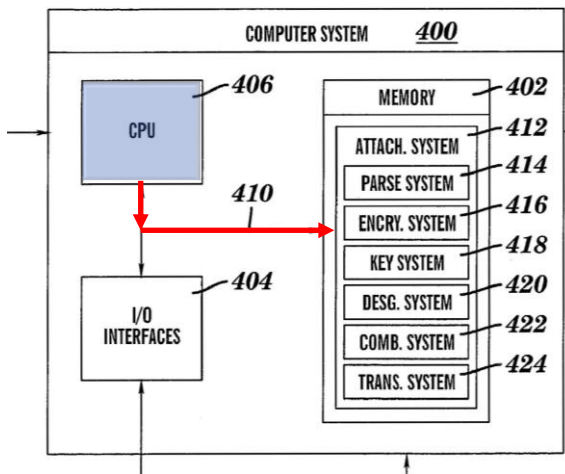
Dr. Rubin: Bus 410 Is A Communication Link For Components In Computer System 400

(12) **Patent Application Publication**
Foster et al.

output system, printer, monitor, facsimile, pager, etc. Bus 410 provides a communication link between each of the components in the computer system 400 and likewise may

DECLARATION OF AVIEL D. RUBIN, PH.D.

121. Certainly, nothing in Foster’s disclosure suggests that the CPU is “coupled to” the alleged “hard drive” on the recipient. Notably, Foster does not mention any “hard drive” on the recipient’s system. Certainly, there is no teaching that Foster’s CPU is coupled to any memory on the recipient. Petitioner points to Foster’s “bus 410” but bus 410 is a “communication link” for the components in Foster’s computer system 400; it does not connote a communication link to the recipient, much less the recipient’s alleged hard drive. Ex. 1006 [Foster] [0076] (“Bus 410 provides a communication link *between each of the components in the computer system 400.*”). Similarly, Foster’s transmission system 424 is described



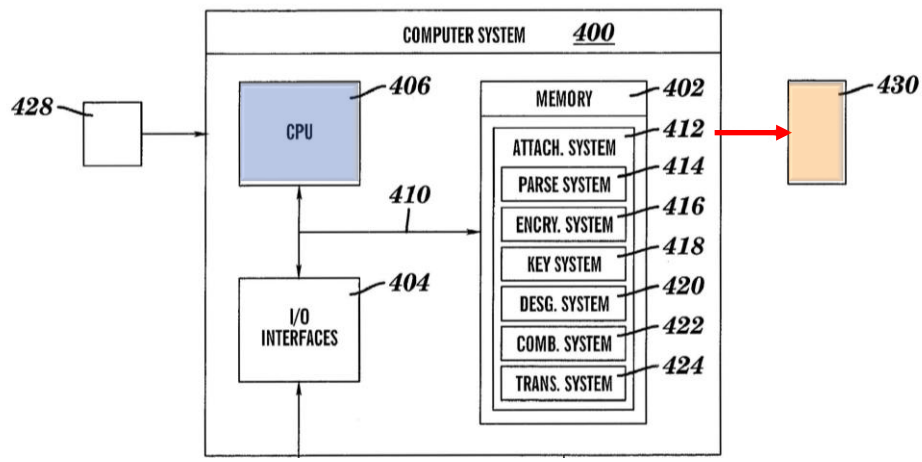
424 Transmits To Recipient, Not The Recipient's Hard Drive

(12) Patent Application Publication Foster et al.

combination system 422. In any event, the encrypted content packet, the header and the header extension will be combined into a single processed content unit by combination system 422 and synchronously transmitted to recipient 430 via transmission system 424. Once received, recipient 430

DECLARATION OF AVIEL D. RUBIN, PH.D.

computer system 400.”). Similarly, Foster’s transmission system 424 is described as transmitting information to recipient 430. See Ex. 1006 [Foster] [0079] (“In any event, the encrypted content packet, the header and the header extension will be combined into a single processed content unit by combination system 422 and synchronously transmitted to recipient 430 via transmission system 424.”). In



Again: Foster's CPU Is Agnostic As To What Receiver Does With Content

DECLARATION OF AVIEL D. RUBIN, PH.D.



111. Foster, however, teaches that its computer system 400 merely

“transmit[s] the processed content units to [the] recipient 430.” *Id.*, [0078]. Once

instructing recipient 430 to store the content. Fundamentally, in Foster's system,

computer system 400 is agnostic as to what the recipients do with the content units,

(12) Patent Application Publication Foster et al.

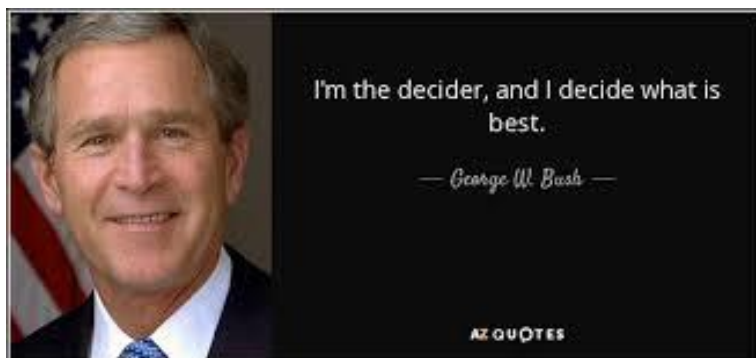
[0078] It should be understood that computer system 400 is intended to be representative of any system capable of processing content units of an elementary content stream received from source 428, and transmitting the processed content units to a recipient 430. Stored in memory 402 is attachment system 412, which includes parsing system 414, encryption system 416, key system 418, designation system 420, combination system 422 and transmission system 424.



No Indication That Foster's CPU And The Recipient's Hard Drive Are "Coupled" Because The Recipient Decides Whether To Store The Data

DECLARATION OF AVIEL D. RUBIN, PH.D.

synchronously transmitted to recipient 430 via transmission system 424.”). In Foster, it is the recipient’s system alone that decides whether to store the information. *Id.* (“Once received, recipient 430 can then synchronously store the encrypted content and attached title key.”). Thus, at most, Foster discloses sending content units from Foster’s system to the recipient. Foster discloses that it is solely the recipient that decides whether to store that information. The independent decision at the recipient to store the transmitted information (or not store it) does not disclose or suggest that any alleged hard drive on the recipient is “coupled to” Foster’s CPU 406.



Reply: CAFC Has Held “Coupled To” To Mean “Connected To”

PETITIONER’S REPLY

The Federal Circuit has “several times held variants of ‘coupled to’...mean simply ‘connected to.’” *Promptu Sys. Corp. v. Comcast Corp.*, 92 F.4th 1372, 1381 (Fed. Cir. 2024) (citations omitted). SFI’s expert similarly testified that “*coupled*

Petitioner's Explanation Of How Foster's CPU And The Recipient's Hard Drive Are Connected?



Foster Fails (IPR2024-00214)

- ❑ Foster's CPU Does Not "Execut[e] Code" "To Perform" "Storing ... At Least One Data Chunk"
- ❑ Foster's CPU Is Not "Coupled To" A "Memory" On Foster's Receiver/Recipient

➤ **No Motivation To Modify Foster As Proposed**

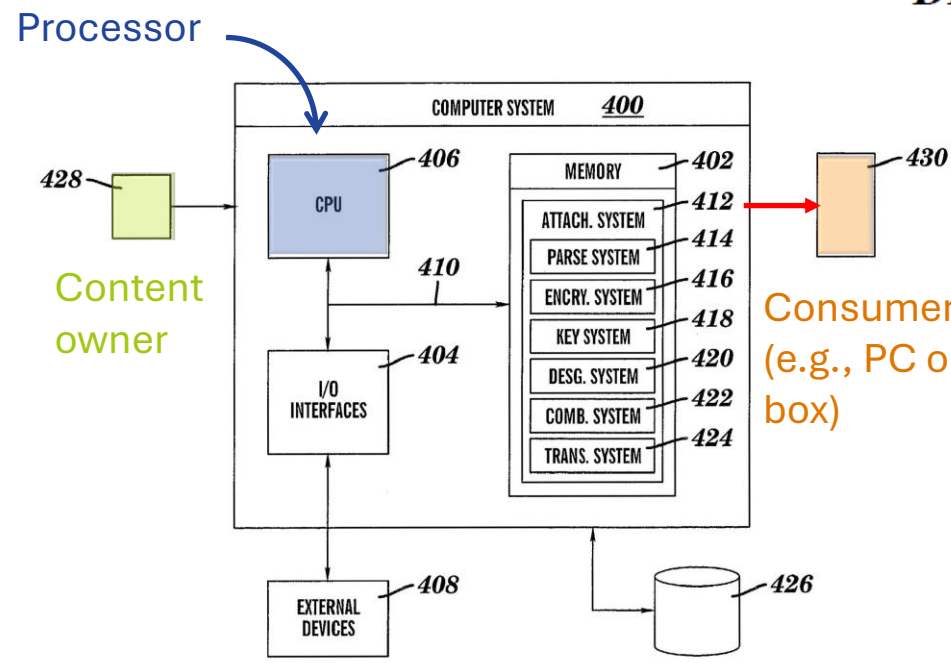
Petitioner's Obviousness Argument: Modify Foster To Store Content At Its Computer System

PETITION FOR INTER PARTES REVIEW UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §42.1 et seq

Alternatively, POSAs also had reason to store Foster's encrypted content in the memory of storage devices coupled to the processor (*e.g.*, through a bus, direct wired/wireless connection, and/or a network-based connection). As discussed above (§VII.A), Foster's system 400 is (or can be part of) a content service provider. As illustrated in Figure 16 (above), Foster's system 400 includes memory 402, which comprises "any known type of data storage," including "one or more types of data storage" or "distributed [storage] across a plurality of physical systems." Foster,

Foster Encrypts Streamed Content From Content Owner For Transmission To Receiver/Recipient

DECLARATION OF AVIEL D. RUBIN, PH.D.

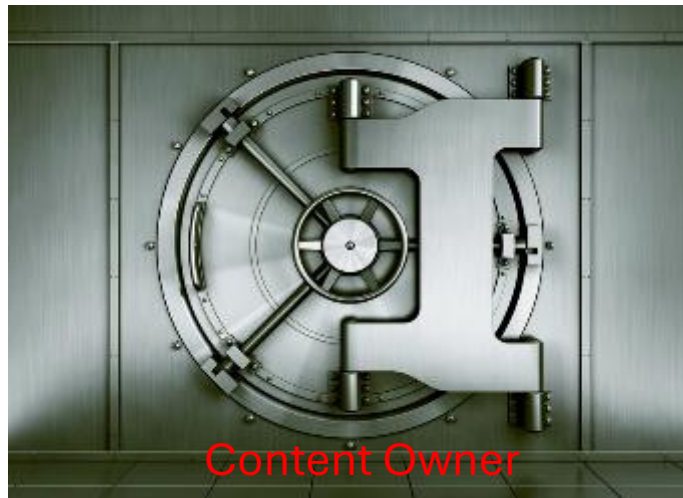


Foster's system is meant merely to act as a middleman for encryption and synchronized transmission of content (e.g., a movie) from **content sources** to **consumer recipients**, as can be seen in Figure 16 below.

FIG. 16



Foster Already Teaches Storing Content At The Content Owner (e.g., A Movie Studio) Which Already Provides The Alleged Benefits



DECLARATION OF AVIEL D. RUBIN, PH.D.

124. Foster further teaches that the content “source” or “owner” is an entity that owns and provides the content. *Id.*, [0038], [0042]. A POSITA would thus recognize that storage for “(1) backup, (2) video-on-demand distribution, and/or (3) distribution to later-identified recipients” is already provided by the content source/owner. Indeed, none of the references Petitioner cites as alleged

Modifying Foster's System Has Numerous Drawbacks That Petitioner Fails To Weigh



Modified Foster

DECLARATION OF AVIEL D. RUBIN, PH.D.

it ensures the content is secure. By contrast, if Foster's system were altered so that the content were stored in Foster's system, that would create a significant security risk as Foster's system would be hacked and an adversary would only have to target the key management block on a single consumer receiver to compromise all of the stored pre-encrypted content. There is simply no reason why a POSITA would be motivated to do this as it would surely frustrate Foster's purpose of securing the content (vis-à-vis encryption) and transmitting it to the receiver without exposing the content to further risk. As discussed, a POSITA would recognize that content is already securely stored in Foster's content sources/owners. A POSITA—and, more importantly, the content owners—would not be motivated to expose the content to potential theft unnecessarily. Moreover, if Foster's system were modified to store pre-encrypted content, significantly more storage would have to be added and that additional storage would have to be as secure as the storage at the content provider/owner. Otherwise, content provider/owners would never trust a third-party system to store its content. Indeed,

Reply: Correctly States That Content-Service Providers Store Content

PETITIONER'S REPLY

service providers (“CSPs”) storing Foster-encrypted content. POSAs knew CSPs (e.g., cable-TV companies) often purchased/licensed content from content owners and then securely stored it before delivering to recipients. Rubin-Depo., 84-94. CSPs typically and beneficially encrypted and stored that content for repeated use (e.g., downloads by different customers) – rather than repeatedly encrypting it on-the-fly – and for backup purposes. Petition, 77-78 (citing EX1045, EX1050,

But, Foster's System Is Not A CSP; It Receives Content From CSPs

(12) Patent Application Publication Foster et al.

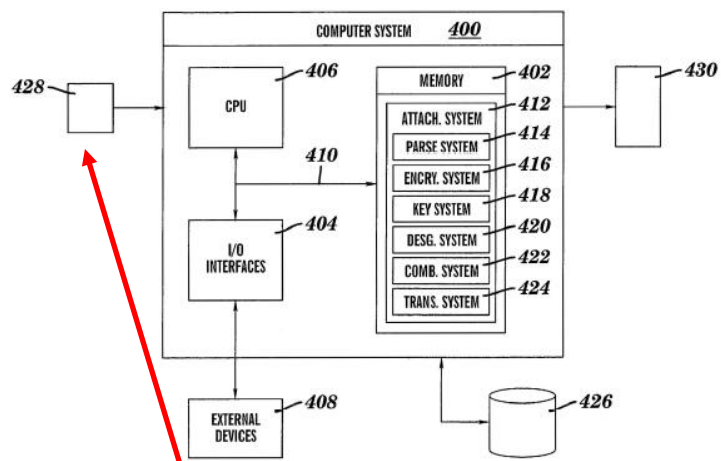


FIG. 16

[0039] Content Service Provider—an entity, such as a cable service provider, that provides the “pipeline” through which content is delivered from a content owner to a consumer.

[0078] It should be understood that computer system 400 is intended to be representative of any system capable of processing content units of an elementary content stream received from source 428, and transmitting the processed content units to a recipient 430. Stored in memory 402 is attachment system 412, which includes parsing system 414, encryption system 416, key system 418, designation system 420, combination system 422 and transmission system 424.

[0042] Source—any entity, such as a content owner, a content service provider or a receiver (in a consumer home network), capable of sending transmissions.

Separating Storage Servers And Encryption Systems Allows Each To “Focus On What They Were Good At”

REMOTE VIDEOCONFERENCE DEPOSITION OF
AVIEL D. RUBIN, Ph.D.

Q. But you said -- but Akamai, using a content distribution intermediary, would allow for like more intelligence of how you distribute the content; is that correct?

ATTORNEY LOWENSTEIN: Objection, form, scope.

A. I mean, basically they allowed AT&T to focus on what they were good at and Disney to focus on what they were good at and Akamai to focus on what they were good at.

Storage



Encryption and Synchronized Transmission

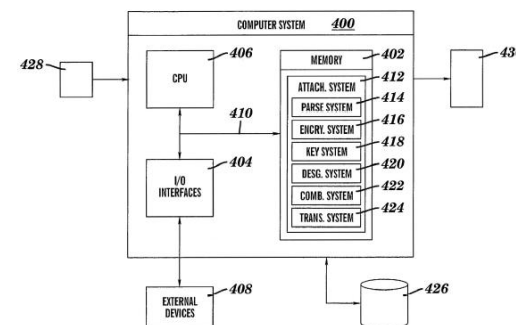
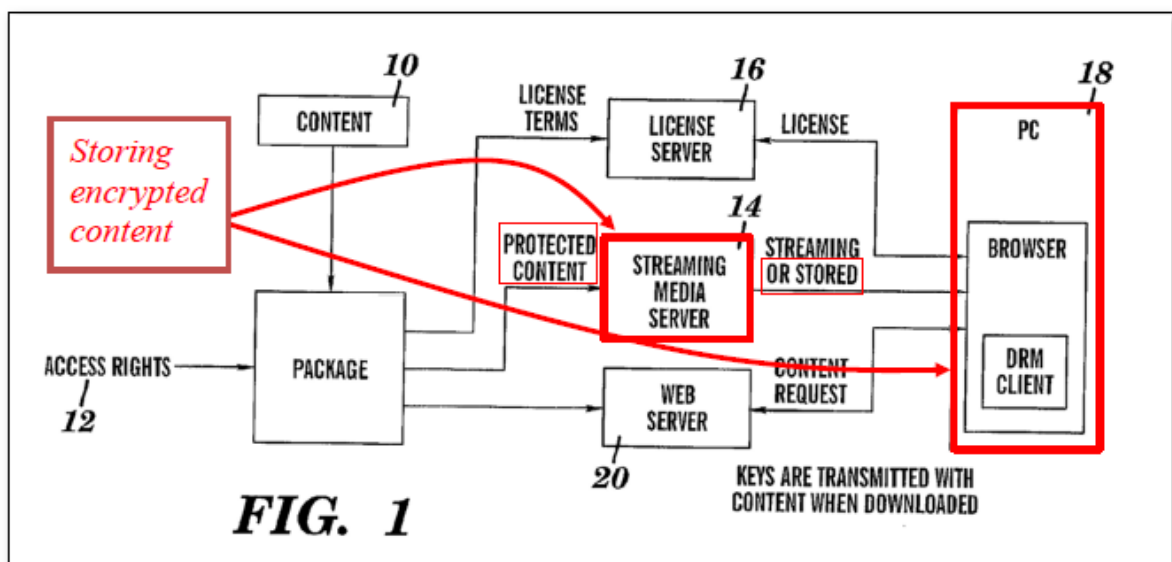


FIG. 16

Reply: Foster's Figure 1 Suggests Modifying Foster To Include Storage Servers

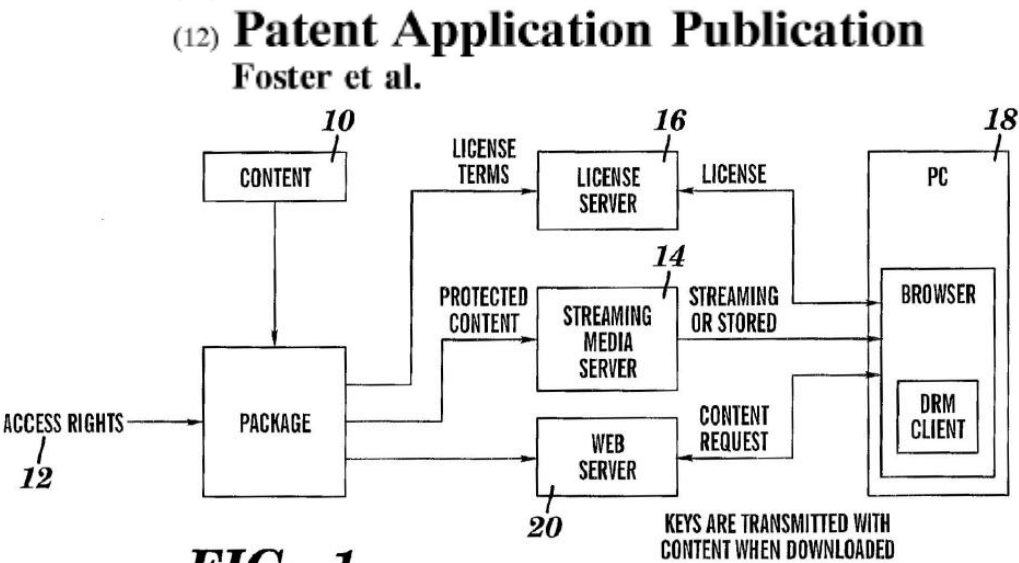
PETITIONER'S REPLY

Foster, [0049], FIG. 1 (annotated below).



Thus, Foster itself is (at least) suggesting/motivating having its processor execute code for storing on storage devices *coupled to* Foster's processor, to support content-on-demand (like VOD) and/or backup, as the Petition identified. Petition, 76-77.

Figure 1 Is Criticized Background Art



[0003] 2. Background Art

[0005] Current technologies that utilize key-based security practices include a personal computer-based Digital Rights Management System (DRMS) and a Conditional Access System (CAS). In the case of the former, content is packaged

the keys is risked. Moreover, both DRMS and CAS can have inherent latencies in providing random access of protected content.

[0007] In view of the foregoing, there exists a need for a method, system and program product for attaching a key to encrypted content for synchronized transmission to, or storage by, a receiver. That is, a need exists for a key used to

[0049] Referring now to FIG. 1, a depiction of a Digital Rights Management System (DRMS) is shown. As depicted,

[0051] As indicated above, the DRMS fails to provide synchronized delivery of the content with the keys used to encrypt the content. That is, license server 16 must be separately accessed. When providing the keys in such a manner, there exists a likelihood that either the appropriate keys will not be matched with the encrypted content, or a single key will be used, weakening the security. Furthermore, providing keys from license server 16 requires a back channel.

Petitioner's Grounds

1. Foster Grounds

- a) Foster and Hayhurst (IPR2024-00212/215)
- b) Foster Alone (IPR2024-00214)

2. Orsini Grounds (IPR2024-00214/215)

3. Tajima Grounds (IPR2024-00212)

214/215 IPRs: Orsini (Single-Reference Obviousness)

Case No. IPR2024-00214
Patent No. 11,068,609

Ground Number and Reference		Claims	Basis
1	Orsini (EX1005)	1-10	§§ ~~102~~ /103
2	Foster (EX1006)	1-3, 7-8	§§ 102/103
		4-6, 9-10	§ 103

Case No. IPR2024-00215
Patent No. 10,452,854

Ground Number and Reference(s)		Claims	Basis
1	Orsini (EX1005)	1-10	§§ ~~102~~ /103
2	Foster (EX1006), Hayhurst (EX1007)	1-10	§ 103

'854: Requires “performing a [cryptographic/encryption] operation based on the [first/external] key”

1. A method for securely storing a data set, the method comprising:

receiving an external key from an external storage system,
generating a plurality of data chunks based on the data set,
such that the data set can be reconstructed using at least
a minimum number of the plurality of data chunks,
wherein generating the data chunks comprises:

distributing the data set into a plurality of shares,
wherein each of the shares comprises less than all of
the data set,

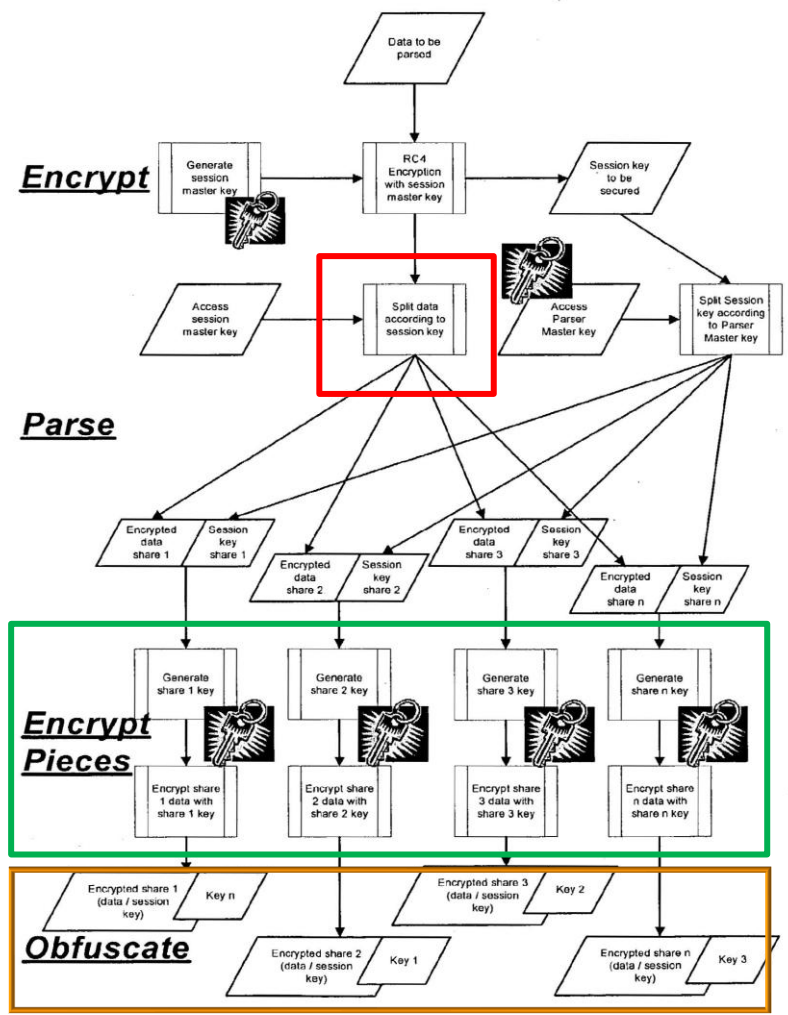
accessing a plurality of distinct encryption keys,
encrypting each of the shares with a respective one of
the plurality of distinct encryption keys,

performing an encryption operation based on the external
key to further secure the plurality of data chunks; and
storing with the plurality of data chunks data indicative of
at least one of the distinct encryption keys on a plurality
of different storage devices.

- Split data set
- Encrypt each share with distinct encryption key
- Perform encryption operation based on external key to further secure the chunks

Orsini Does Not “Perform[] An Encryption Operation Based On The External Key To Further Secure The Plurality Of Shares”

Figure 21



- Splits dataset into shares
- Encrypts each share with different share key
- Non-cryptographically stores share key with share it was not used to encrypt

Board: Orsini Ground Did Not Have Reasonable Likelihood Of Prevailing

Trials@uspto.gov
571-272-7822

Paper 15
Entered: May 23, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

IPR2024-00215
Patent 10,452,854 B2

Before THOMAS L. GIANNETTI, JASON M. REPKO, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

REPKO, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314



For all the reasons discussed above, Petitioner has not shown a reasonable likelihood of prevailing as to the unpatentability of claim 1 under its challenge based on Orsini.

Reply: Petitioner Abandons Anticipation Arguments And Most Obviousness Arguments

Filed on behalf of Google LLC by
Elisabeth H. Hunt, Reg. No. 1000000000000000
Gregory S. Nieberg, Reg. No. 1000000000000000
Nathan R. Speed (admitted to practice in the U.S.)
WOLF, GREENFIELD & SEARS, P.A.
600 Atlantic Avenue
Boston, MA 02210
(617) 646-8000 Phone
(617) 646-8646 Fax

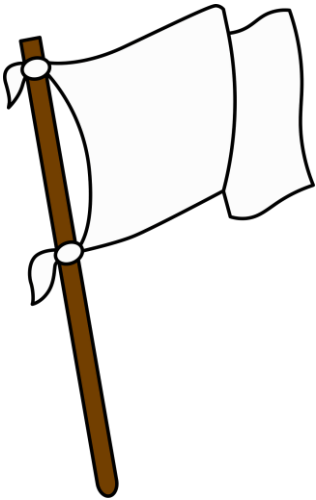
UNITED STATES PATENT AND
TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND
APPEALS BOARD

SECURITY FIRST INNOVATIONS, LLC
Patent Owner.

Case No. IPR2024-00215
Patent No. 10,452,854

PETITIONER'S REPLY TO PATENT OWNER RESPONSE

While Petitioner believes its arguments have merit, Petitioner below focuses on one obviousness argument to simplify the trial. Specifically, Petitioner's argument that POSAs would have encrypted Orsini's share keys with a key-encryption-key ("KEK") to safeguard the share keys from detection, a technique that multiple corroborating references demonstrate was known and desirable in the art. Petition, 43-45 (citing corroboration).



The Board Correctly Rejected This Argument In The ID As “Deficient”

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

discussed in § II.E.2.a.iii, Petitioner’s arguments about the public-key encryption key are deficient. In particular, Orsini does not show a public key in Figure 21. *See* Prelim. Resp. 19–20. Petitioner’s argument about the public-key encryption key is based on the features from multiple embodiments. *See* Pet. 38–39. Yet Petitioner does not provide a sufficient rationale for combining these multiple embodiments. *See id.*

Ex. 1005 ¶ 172). Thus, Petitioner has not shown a reasonable likelihood in demonstrating that claim 1 would have been obvious under its rationale about encrypting the distinct encryption keys with an externally stored KEK. *See* § II.E.2.a.iii *supra*.

Reply Does Not Cure The Petition's Deficiencies



Most Of Orsini Included In ‘609/’854 Patents

(12) United States Patent O'Hare et al.		(10) Patent No.: US 10,452,854 B2
		(45) Date of Patent: Oct. 22, 2019
(54) SECURE DATA PARSER METHOD AND SYSTEM		(58) Field of Classification Search None See application file for complete search history.
(71) Applicant:	Security First Corp. , Rancho Santa Margarita, CA (US)	(56) References Cited U.S. PATENT DOCUMENTS 5,150,407 A 9/1992 Chan 5,239,659 A 8/1993 Rudesael et al. (Continued)
(72) Inventors:	Mark S. O'Hare , Coto De Caza, CA (US); Rick L. Orsini , Flower Mound, TX (US); Roger S. Davenport , Campbell, TX (US); Steven Winick , Roslyn Heights, NY (US)	
(73) Assignee:	Security First Corp. , Ladera Ranch, CA (US)	FOREIGN PATENT DOCUMENTS AU 2004/248616 12/2004 EP 0851629 A2 7/1998 (Continued)
(*) Notice:	Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.	
(21) Appl. No.:	16/127,077	
(22) Filed:	Sep. 10, 2018	
(65)	Prior Publication Data US 2019/0197248 A1 Jun. 27, 2019	
	Related U.S. Application Data	
(63)	Continuation of application No. 14/546,887, filed on Nov. 18, 2014, now Pat. No. 10,108,807, which is a (Continued)	
(51) Int. Cl.	G06F 21/62 (2013.01) H04L 9/32 (2006.01) (Continued)	
(52) U.S. Cl.	CPC G06F 21/62 (2013.01); H04L 9/085 (2013.01); H04L 9/3231 (2013.01); (Continued)	
		20 Claims, 42 Drawing Sheets

(19) United States		(10) Pub. No.: US 2004/0049687 A1
(12) Patent Application Publication Orsini et al.		(43) Pub. Date: Mar. 11, 2004
(54) SECURE DATA PARSER METHOD AND SYSTEM	(60) Provisional application No. 60/154,734, filed on Sep. 20, 1999. Provisional application No. 60/200,396, filed on Apr. 27, 2000.	
(76) Inventors: Rick L. Orsini , Flower Mound, TX (US); John VanZandt , Mission Viejo, CA (US); Mark S. O'Hare , Coto de Caza, CA (US); Roger S. Davenport , Campbell, TX (US)	Publication Classification	
Correspondence Address: John W. Wallen, III Preston Gates & Ellis, LLP Suite 500 1735 New York Avenue, N.W. Washington, DC 20006-5209 (US)		(51) Int. Cl. 7 H04L 9/00
		(52) U.S. Cl. 713/189
(21) Appl. No.: 10/458,928	(57) ABSTRACT The present invention provides a method and system for securing sensitive data from unauthorized access or use. The method and system of the present invention is useful in a wide variety of settings, including commercial settings generally available to the public which may be extremely large or small with respect to the number of users. The method and system of the present invention is also useful in a more private setting, such as with a corporation or governmental agency, as well as between corporation, governmental agencies or any other entity.	
(22) Filed: Jun. 11, 2003	Related U.S. Application Data	
(63) Continuation-in-part of application No. 09/666,519, filed on Sep. 20, 2000.		

But, '609/'854 Add 17 New Figures And 18 New Columns To Orsini

US 11,068,609 B2

65

to a smaller workgroup, the data securing methods described herein are used to share files within groups of users.

In the example shown in FIG. 25 and described below, there are six users defined along with their role or role within the organization. The side bar represents five possible groups that the users can belong to according to their role. The arrow represents membership by the user in one or more of the groups.

When configuring the secure data parser for use in this example, the system administrator accesses the user and group information from the operating system by a maintenance program. This maintenance program generates and assigns Parser Group Master Keys to users based on their membership in groups.

In this example, there are three members in the Senior Staff group. For this group, the actions would be:

1. Access Parser Group Master Key for the Senior Staff group (generate a key if not available).
2. Generate a digital certificate associating CEO with the Senior Staff group.
3. Generate a digital certificate associating CTO with the Senior Staff group.
4. Generate a digital certificate associating Vice President, Marketing with the Senior Staff group.

The same set of actions would be done for each group, and each member within each group. When the maintenance program is complete, the Parser Group Master Key becomes a shared credential for each member of the group. Revocation of the assigned digital certificate may be done automatically when a user is removed from a group through the maintenance program without affecting the remaining members of the group.

Once the shared credentials have been defined, the parsing and splitting process remains the same. When a file, document or data element is to be secured, the user is prompted for the target group to be used when securing the data. The resulting secured data is only accessible by other members of the target group. This functionality of the methods and systems of the present invention may be used with any other computer system or software platform, any may be, for example, integrated into existing application programs or used standalone for file security.

It is readily apparent to those of ordinary skill in the art that any one or combination of encryption algorithms are suitable for use in the methods and systems of the present invention. For example, the encryption steps may, in one embodiment, be repeated to produce a multi-layered encryption scheme. In addition, a different encryption algorithm, or combination of encryption algorithms, may be used to repeat encryption steps such that different encryption algorithms are applied to the different layers of the multi-layered encryption scheme. As such, the encryption scheme itself may become a component of the methods of the present invention for securing sensitive data from unauthorized use or access.

The secure data parser may include as an internal component, as an external component, or as both an error checking component. For example, in one suitable approach, as portions of data are created using the secure data parser in accordance with the present invention, to ensure the integrity of the data within a portion, a hash value is taken at preset intervals within the portion and is appended to the end of the interval. The hash value is a predictable and reproducible numeric representation of the data. If any bit within the data changes, the hash value would be different. A scanning module (either as a stand-alone component external to the secure data parser or as an internal component) may then scan the portions of data generated by the secure data parser. Each portion of data (or alternatively, less than all portions of data according to some interval or by a random or pseudo-random sampling) is compared to the appended hash value or values and an action may be taken. This action may include a report of values that match and do not match, an alert for values that do not match, or invoking of some external or internal program to trigger a recovery of the data. For example, recovery of the data could be performed by invoking a recovery module based on the concept that fewer than all portions may be needed to generate original data in accordance with the present invention.

Any other suitable integrity checking may be implemented using any suitable integrity information appended anywhere in all or a subset of data portions. Integrity information may include any suitable information that may be used to determine the integrity of data portions. Examples of integrity information may include hash values computed based on any suitable parameter (e.g., based on respective data portions), digital signature information, message authentication code (MAC) information, any other suitable information, or any combination thereof.

The secure data parser of the present invention may be used in any suitable application. Namely, the secure data parser described herein has a variety of applications in different areas of computing and technology. Several such areas are discussed below. It will be understood that these are merely illustrative in nature and that any other suitable applications may make use of the secure data parser. It will further be understood that the examples described are merely illustrative embodiments that may be modified in any suitable way in order to satisfy any suitable desires. For example, parsing and splitting may be based on any suitable units, such as by bits, by bytes, by kilobytes, by megabytes, by any combination thereof, or by any other suitable unit.

The secure data parser of the present invention may be used to implement secure physical tokens, whereby data stored in a physical token may be required in order to access additional data stored in another storage area. In one suitable approach, a physical token, such as a compact USB flash drive, a floppy disk, an optical disk, a smart card, or any other suitable physical token, may be used to store one of at least two portions of parsed data in accordance with the present invention. In order to access the original data, the USB flash drive would need to be accessed. Thus, a personal computer holding one portion of parsed data would need to have the USB flash drive, having the other portion of parsed data, attached before the original data can be accessed. FIG. 26 illustrates this application. Storage area 2500 includes a portion of parsed data 2502. Physical token 2504, having a portion of parsed data 2506, would need to be coupled to storage area 2500 using any suitable communications interface 2508 (e.g., USB, serial, parallel, Bluetooth, IR, IEEE 1394, Ethernet, or any other suitable communications interface) in order to access the original data. This is useful in a situation where, for example, sensitive data on a computer is left alone and subject to unauthorized access attempts. By removing the physical token (e.g., the USB flash drive), the sensitive data is inaccessible. It will be understood that any other suitable approach for using physical tokens may be used.

The secure data parser of the present invention may be used to implement a secure authentication system whereby user enrollment data (e.g., passwords, private encryption keys, fingerprint templates, biometric data or any other suitable user enrollment data) is parsed and split using the secure data parser. The user enrollment data may be parsed

FIG. 39

Orsini Does Not Disclose “Workgroup Key,” Which Is Only In The '609 And '854

(12) **United States Patent**
O'Hare et al.

(10) Patent No.: **US 10,452,854 B2**
(45) Date of Patent: **Oct. 22, 2019**

The workgroup key concept allows for enhanced protection of information assets by encrypting key information stored within the shares. Once this operation is performed, even if all required shares and external keys are discovered, an attacker has no hope of recreating the information without access to the workgroup key.

performing an encryption operation based on the external key to further secure the plurality of data chunks; and

'854, cl. 1

'609, 79:46-65;
'854, 79:52-80:4



Single-Reference Obviousness Over Orsini Faces A High Bar



“In cases in which ‘common sense’ is used to supply a missing limitation, as distinct from a motivation to combine, moreover, **our search for a reasoned basis for resort to common sense must be searching.** And, this is particularly true where the missing limitation **goes to the heart of an invention.**”

-Arendi S.A.R.L. v. Apple Inc., 832 F.3d 1355, 1363 (Fed. Cir. 2016)

“we have invoked common sense to fill in a missing limitation **only when ‘the limitation in question was unusually simple and the technology particularly straightforward.’**”

-DSS Tech. Mgm’t v. Apple Inc., 885 F.3d 1367, 1374-75 (Fed. Cir. 2018)

Undisputed: Limitation Goes To “The Heart Of The Invention”

DECLARATION OF AVIEL D. RUBIN, PH.D.



“external key” of claim 1—a technique not disclosed in Orsini. The workgroup key provides “enhanced protection of information assets by encrypting key information stored within the shares” (Ex. 1001 [’854] 79:66-80:1) adding “an extra level of security to a secured data set” (*id.*, 77:22-23). As the ’854 explains “even if all required shares and external keys are discovered, an attacker has no hope of recreating the information without access to the workgroup key.” *Id.*, 80:1-4. Thus, this limitation goes to the heart of the invention. Moreover, given



Undisputed: Cryptography Is A Particularly Complicated Technical Field

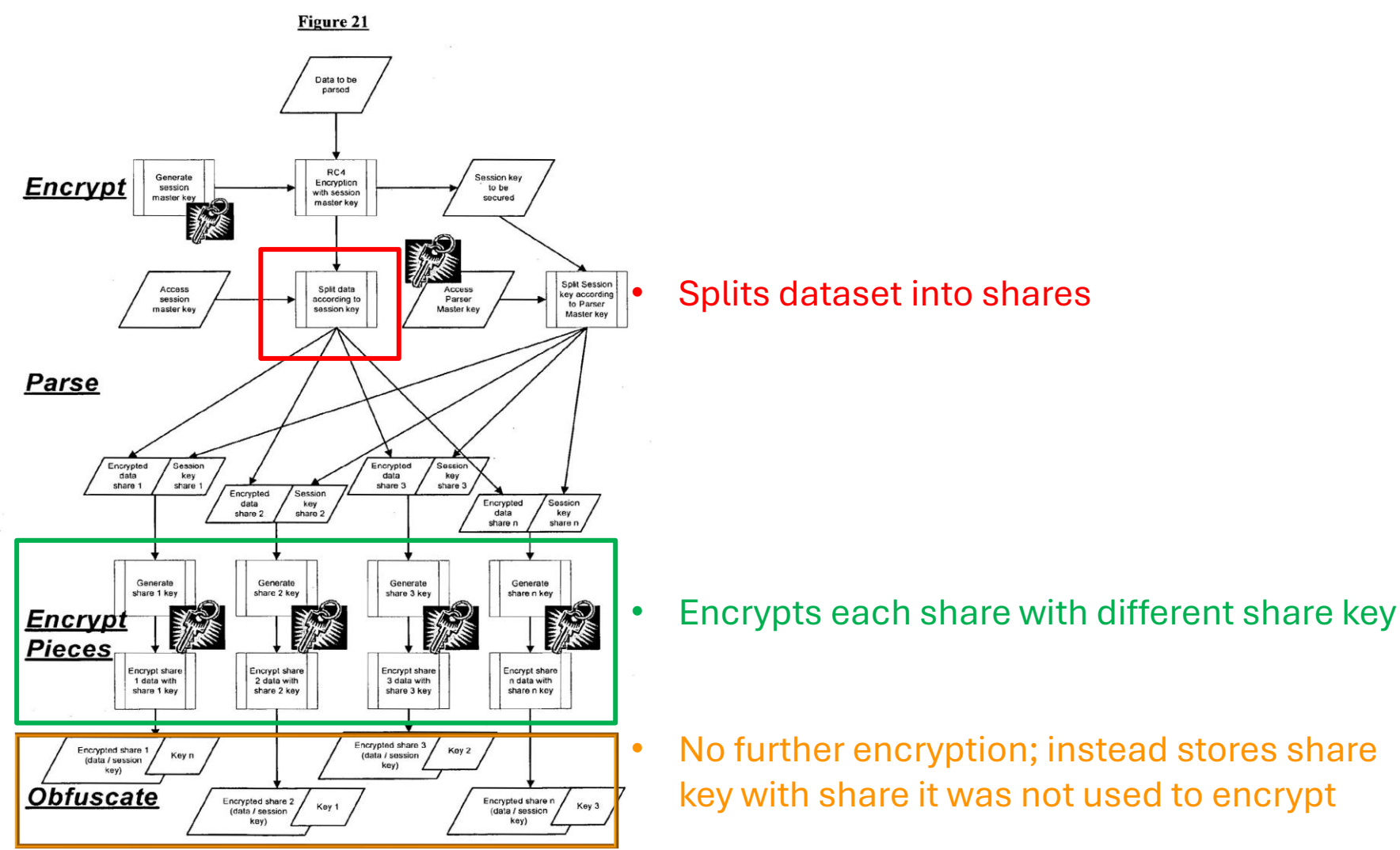


DECLARATION OF AVIEL D. RUBIN, PH.D.

66. The inventions-at-issue concern cryptography, which is a technologically-involved and complex field involving incredibly high stakes and safeguarding against a wide variety of highly sophisticated and ever-evolving cybersecurity attacks. As internationally-renowned cryptologist Bruce Schneier (Ex. 2005 [Schneier-CV]) has observed “[f]ew can do the science [of cryptography] properly” and “[g]ood cryptographers know that nothing substitutes for extensive peer review and years of analysis.” Ex. 2006 [Schneier-Why-Cryptography-Is-Harder-Than-It-Looks] 3.

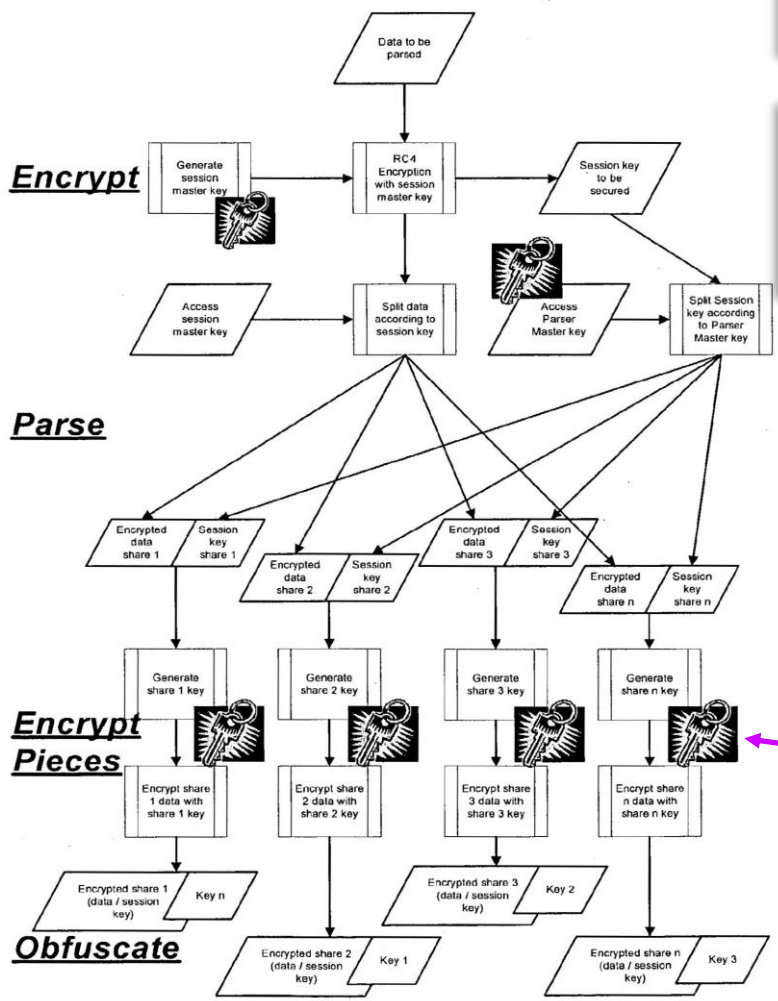


Orsini's Figure 21: No Further Encryption Operation



Petitioner: Modify Figure 21 To Encrypt Share Keys With KEK To Avoid “Potential Security Risk”

Figure 21



**PETITION FOR INTER PARTES REVIEW
UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §42.1 et seq**

to avoid a potential security risk in storing [1B3]’s encryption keys in clear (unencrypted) form on storage devices (especially those accessible from the public Internet), POSAs had reason to encrypt [1B3]’s keys with a KEK. Bhattacharjee,

Proposed modification:
encrypt share keys with KEK

Orsini Provides “Comprehensive Package For Data Security”



DECLARATION OF AVIEL D. RUBIN, PH.D.

69. Orsini already teaches hiding the encryption key used to encrypt each data chunk with a different chunk through a **non-cryptographic process**,

with a share it did not encrypt. Indeed, I note that Orsini teaches that its method provides a “comprehensive package for data security.” Ex. 1005 [Orsini] [0380] (“The data shares are then encrypted individually and the keys are stored safely with different encrypted shares. When combined, the entire process for securing data according to the methods disclosed herein becomes a comprehensive package for data security.”).

A graphic with the text “EVERYTHING YOU NEED” in large, bold, white capital letters. The background is a dark, starry night sky with a faint horizon line.

Petitioner's Arguments Amount To Impermissible Hindsight



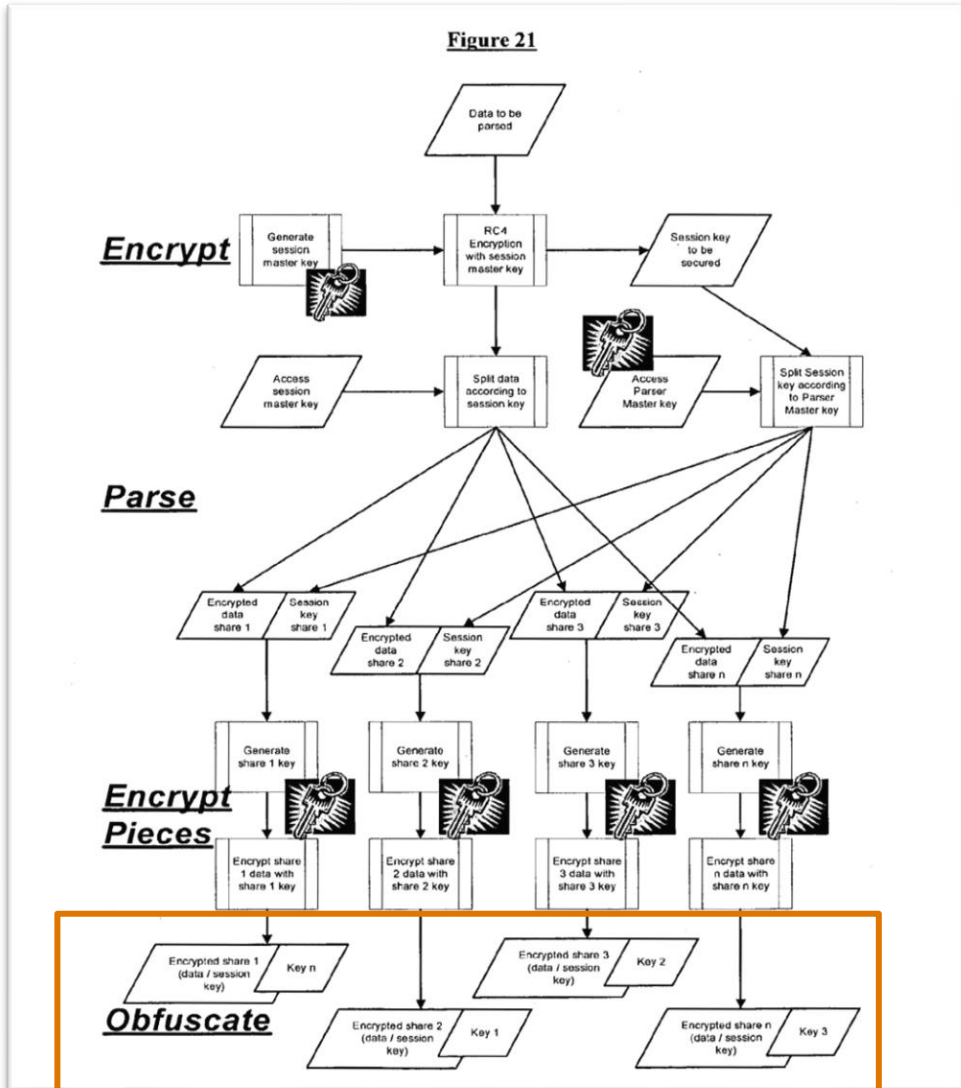
“an obviousness assessment might break an invention into its component parts ... **This form of hindsight reasoning, using the invention as a roadmap to find its prior art components, would discount the value of combining various existing features or principles in a new way to achieve a new result - often the very definition of invention.**”

Ruiz v. A.B. Chance Co., 357 F.3d 1270, 1275 (Fed. Cir. 2004)

“In attempting to support the Board’s findings, Clear-Vu argues that support can be found in the ’706 patent itself. ... **But ‘[t]he inventor’s own path itself never leads to a conclusion of obviousness; that is hindsight.’**”

Univ. of Strathclyde v. Clear-Vu Lighting LLC, 17 F.4th 155, 165 (Fed. Cir. 2021)

Petitioner Ignores Figure 21's "Obfuscate" Step: Keys Are Not Stored With The Data They Encrypt



(12) Patent Application Publication Orsini et al.

[0353] In one embodiment, it may not be desired to have any one depository contain enough information to decrypt the information held there, so the key required to decrypt the share is stored in a different data depository:

POSITA Not Motivated To Add Redundant Features



**“the AAPA already discloses an RF network ...
Thus, adding an RF network ... would render the
RF network connecting the portable PCs ...
superfluous.”**

In re NTP, Inc., 654 F.3d 1279, 1299 (Fed. Cir. 2011)



**“Petitioner ... fails to provide a specific
explanation why Hall did not already
accomplish [the asserted benefits] by itself.”**

Apple Inc. v. Cellular Comm’ns Equipment, LLC, IPR2015-00576, Paper 7, 12 (June 12, 2015)

Petitioner: Obfuscate Offers “Negligible Security”

Orsini: A “Comprehensive Package For Data Security”

PETITIONER’S REPLY TO PATENT OWNER RESPONSE

(12) Patent Application Publication Orsini et al.

POSAs, therefore, would have recognized that Orsini’s obfuscation provides (negligible) non-cryptographic security that depended heavily on the attacker not possessing the shares. Conversely, POSAs would have recognized that encrypting

Reply, 18



[0380] Another advantage provided by the methods and system of the present invention is the combination of the steps of the method of the present invention for securing data to provide a comprehensive process of maintaining security of sensitive data. The data is encrypted with a secure key and split into one or more shares, and in one embodiment, four shares, according to the secure key. The secure key is stored safely with a reference pointer which is secured into four shares according to a secure key. The data shares are then encrypted individually and the keys are stored safely with different encrypted shares. When combined, the entire process for securing data according to the methods disclosed herein becomes a comprehensive package for data security.

The Reply Fails To Consider Orsini As A Whole

PETITIONER'S REPLY TO PATENT OWNER RESPONSE

SFI does not dispute that encrypting encryption keys with KEKs was known or that encrypting Orsini's share keys with a KEK meets [1C] under SFI's claim constructions. POSAs would have used that known technique in Orsini because, as even SFI's expert admits, POSAs would "not put [] security in anything other than the keys" and the way Orsini allegedly protects its share keys – by obfuscating which data chunk each key is stored with – "is not putting the protection in the keys, so...this **does not on its own provide security.**" Rubin-Depo., 155. The expert's candid admission is consistent with the Petition's prior-art evidence explaining that "[s]ecurity' comes from 'encrypt[ing] the encryption keys themselves' with 'a key encryption key.'" Petition, 43 (quoting EX1036). On the fully developed record, [1C] is plainly obvious over Orsini.



Petitioner Ignores That Orsini Stores Shares In Different Locations From The Keys AND On Different Storage Devices

(12) Patent Application Publication Orsini et al.

[0299] 5. Encrypting each share, then store the encryption keys in different locations from the encrypted data portions or shares: Share 1 gets Key 4, Share 2 gets Key 1, Share 3 gets Key 2, Share 4 gets Key 3.

[0353] In one embodiment, it may not be desired to have any one depository contain enough information to decrypt the information held there, so the key required to decrypt the share is stored in a different data depository:

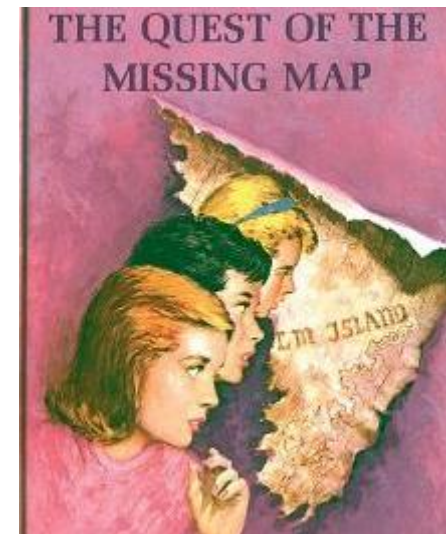
[0354] Depository 1: SD1, Kn

[0355] Depository 2: SD2, K1

[0356] Depository 3: SD3, K2

[0357] Depository n: SDn, K3.

[0379] There are major advantages provided by the data security methods and computer systems of the present invention over traditional encryption methods. One advantage is the security gained from moving shares of the data to different locations on one or more data depositories or storage devices, that may be in different logical, physical or geographical locations. When the shares of data are split physically and under the control of different personnel, for example, the possibility of compromising the data is greatly reduced.



Experts Agree: Storing Chunks Separately Adds A High Level Of Security

Dr. Bhattacharjee

Dr. Rubin

DEPOSITION OF SAMRAT BHATTACHARJEE, PH.D.

23 Now, from a network attacker's point of
24 view, if you were to put a piece of data on a USB
25 drive, remove it from the original computer that's
1 connected to the network, it's nearly perfect
2 security. Because no matter how much computation
3 they have, they're not going to be able to get to
4 it. So it's a very secure method. It is offline
5 storage, it's usually called.

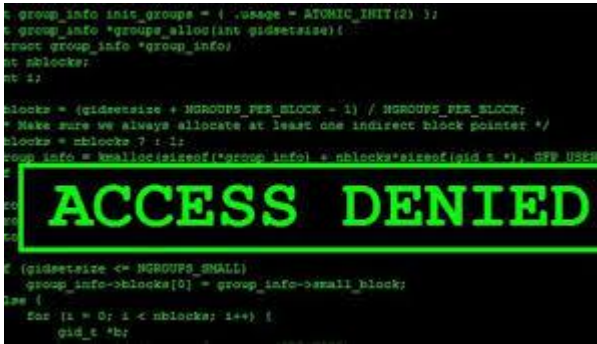


REMOTE VIDEOCONFERENCE DEPOSITION OF
AVIEL D. RUBIN, Ph.D.

Q. And that provides security by having one piece in
one location and the other piece in the other
location; is that right?

ATTORNEY LOWENSTEIN: Objection, form.

A. That makes it harder for an attacker to get the
data.



Orsini Confirms: Storing Chunks Separately Adds A High Level Of Security

(12) **Patent Application Publication** **Orsini et al.**

[0379] There are major advantages provided by the data security methods and computer systems of the present invention over traditional encryption methods. One advantage is the security gained from moving shares of the data to different locations on one or more data depositories or storage devices, that may be in different logical, physical or geographical locations. When the shares of data are split physically and under the control of different personnel, for example, the possibility of compromising the data is greatly reduced.

Petitioner's Hayhurst Reference: Storing Chunks Separately Adds "A High Level Of Security"

(12) **Patent Application Publication** **Hayhurst**

[0008] The segmented and distributed storage of the media file provides a high level of security and a deterrence to piracy. No single subscriber unit has more than a segment of a media file, which segment, by itself, has little value.

Experts Agree: Attacker Cannot Use Key Stored With Chunk

Dr. Bhattacharjee

DEPOSITION OF SAMRAT BHATTACHARJEE, PH.D.

Q: “What capabilities would that attacker need to decrypt encrypted share 2 with key 1?”

A: **“It’s not clear to me that key 1 would necessarily be useful to decrypt encrypted share 2.”**

Dr. Rubin

DECLARATION OF AVIEL D. RUBIN, PH.D.

“Orsini teaches that [Figure 21’s step] is sufficient because an attacker would not have ‘enough information to decrypt the’ data chunk stored in each data depository. ... Notably, in Figure 21’s data-securing method, the session master key, data chunks, and session keys are all either encrypted, parsed, and/or hidden, and thus each potentially vulnerable part of the encryption method is secured.”

Reply: Attacker Only Has To Try 24 Chunk-Key Pairings

PETITIONER'S REPLY TO PATENT OWNER RESPONSE

Orsini's Figure 21 divides data into four shares/chunks and stores share keys with those shares/chunks. Orsini, [0298]-[0301]. That allows (at most) twenty-four different chunk-key pairings. Rubin-Depo., 25. POSAs understood that computers could easily overcome Orsini's obfuscation by trying all twenty-four possibilities until identifying the correct one. Bhattacharjee-Reply, ¶¶223-225; Rubin-Depo., 22-



Orsini: The Dataset Is Divided Into Four Or More Shares

(12) **Patent Application Publication** **Orsini et al.**

remains whole and intact and subject to attack. The parser software suite of the present invention, in one embodiment, addresses this problem by performing a cryptographic split or parsing of the encrypted file into two or more portions or shares, and in another embodiment, preferably four or more shares, adding another layer of encryption to each share of the data, then storing the shares in different physical and/or logical locations. When one or more data shares are physically removed from the system, either by using a removable device, such as a data storage device, or by placing the share under another party's control, any possibility of compromise of secured data is effectively removed.

1!=1
2!=2
3!=6
4!=24
5!=120
6!=720
7!=5040
8!=40320
9!=362880
10!=3628800
11!=39916800
12!=479001600
13!=6227020800
14!=87178291200
15!=1307674368000
16!=20922789888000
17!=355687428096000
18!=6402373705728000
19!=121645100408832000
20!=2432902008176640000

Orsini's Method Is Not Limited To Four Shares

Petitioner's Motivation To Avoid “A Potential Security Risk” Is Insufficiently Generic

PETITION FOR INTER PARTES REVIEW
UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §42.1 et seq

“Thus, **to avoid a potential security risk** ...POSAs had reason to encrypt [1B3]’s keys with a KEK.”

-00215 Pet., 43



Motivation to “build something better,” “more efficient, cheaper” etc. was “**insufficient**”

ActiveVideo Networks Inc. v. Verizon Comms., Inc.,
694 F.3d 1312, 1327(Fed. Cir. 2012)



“[S]tatements of increased utility and minimal modifications **are generic**, and fail to provide necessary factual support”

Samsung Austin Semi., LLC v. Red Rock Analytics, LLC,
IPR2018-00556, Paper 18, 22 (Aug. 20, 2018)

Petitioner Failed To Consider Drawbacks Of Adding KEKs



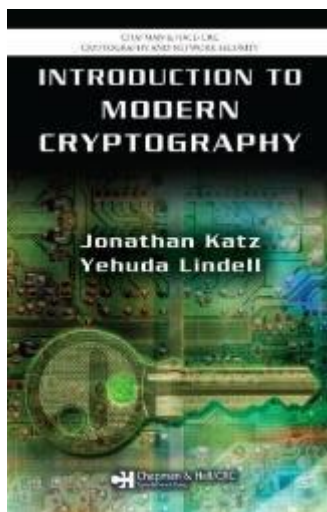
"[t]he Board must **weigh the benefits and drawbacks** of the modification against each other, to determine whether there would be a motivation to combine."

Arctic Cat Inc. v. Polaris Indus., 795 Fed. App'x. 827, 833 (Fed. Cir. 2019)

"Coupled with testimony confirming the **potential problems** of automatic throttle reapplication and suggesting **an alternative approach might reduce those same problems**, J.A. 2230-32, a jury could find **a skilled artisan would not have been motivated to combine ...**"

Arctic Cat Inc. v. Bombardier Rec. Prods., 876 F.3d 1350, 1363 (Fed. Cir. 2017)

Cryptography Is Very Complex And Seemingly “Simple” Solutions May Compromise Security



“As an example, an encryption scheme that has been proven secure ... might be implemented on a smart-card. **It may then be possible for an adversary to monitor the power usage of the smartcard** (e.g. how this power usage fluctuates over time) **and use this information to determine the key.**”

Ex. 2007 [Katz] 4

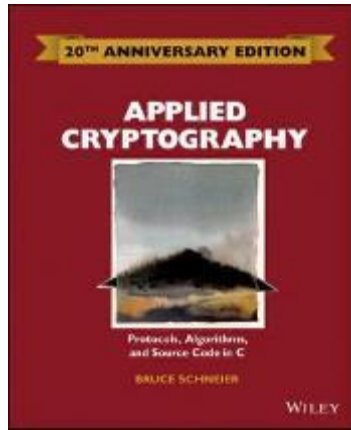


Bruce Schneier

“And just as it’s possible to build a weak structure using strong materials, **it’s possible to build a weak cryptographic system using strong algorithms and protocols.**”

Ex. 2008 [Schneier-Security-Pitfalls-In-Cryptography] 2

Key-Management Is Especially Important And Difficult



“In the real world, key management is the hardest part of cryptography. Designing secure cryptographic algorithms and protocols isn’t easy, but you can rely on a large body of academic research. **Keeping the keys secret is much harder.”**

Ex. 2010 [Schneier-Applied-Cryptography] 169



Petitioner's Proposed Solution To Key Management: Use "Session Key Management" For KEKs

PETITION FOR INTER PARTES REVIEW UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §42.1 et seq

First, as discussed, Orsini provides “external session key management” and discloses “multiple cryptographic engines” having a “single point of...key management.” [0180], [0176]-[0179], [0293], [0381]-[0386], [0412]; Bhattacharjee, ¶89; EX1015, [0044]. POSAs would have recognized several benefits to implementing such a single point of external key management for multiple cryptographic engines by centrally generating Orsini’s session master keys (and any of the conventional encryption keys discussed §VI.B.7.b *infra*) and storing them separately from data chunks in a centralized storage system built specifically for storing encryption keys, so that those keys could be centrally generated, stored, and then distributed to (received by) Orsini’s multiple cryptographic engines. Bhattacharjee, ¶89.

Dr. Rubin: Session Key Management Is Very Different From KEK Management



DECLARATION OF AVIEL D. RUBIN, PH.D.

[0386], [0412]). But **session** key management is very different than key management for longer-lived keys such as the other “conventional encryption keys” Petitioner relies upon, especially as Figure 21’s session keys (the session master key and share keys) are stored alongside the encrypted data. For example, “session keys should be changed at least daily” if not for each “particular communications session” while “key-encryption keys don’t have to be replaced as frequently,” perhaps “once a year.” Ex. 2010 [Schneier-Applied-Cryptography] 184, 47; *see also id.*, 184 (“Encryption keys used to encrypt data files for storage cannot be changed often.”).



VS



Orsini Figure 21's Session Key-Management Is To Store The Session Keys With The Data

(12) **Patent Application Publication** **Orsini et al.**

[0297] 3. In this embodiment of the method, the session master key will be stored along with the secured data shares in a data depository. Separating the session master key according to the pattern of the Parser Master Key and append the key data to the encrypted parsed data.

[0298] 4. The resulting four shares of data will contain encrypted portions of the original data and portions of the session master key. Generate a stream cipher key for each of the four data shares.

[0299] 5. Encrypting each share, then store the encryption keys in different locations from the encrypted data portions or shares: Share 1 gets Key 4, Share 2 gets Key 1, Share 3 gets Key 2, Share 4 gets Key 3.



Dr. Rubin: Figure 21's Session-Key Management Is Not Appropriate For KEKs



DECLARATION OF AVIEL D. RUBIN, PH.D.

80. Moreover, key management for a “group key,” “encryption key,” or “key-encryption key” would necessarily be different than for key management for the “session” keys in Figure 21. In Figure 21, the session master key used to encrypt the dataset is parsed within the data shares (Ex. 1005 [Orsini] [0297]) and the session share keys are stored along with the data shares (*id.*, [0299]). Therefore, so long as the party reconstructing the dataset possesses the shares, he or she also possesses the session keys necessary to decrypt the data. By contrast, the “group key,” “encryption key,” or “key-encryption key” would not be stored alongside the data but would rather need to be distributed out-of-band to the decrypting party. Consequently, those keys would need to be maintained and



Petitioner's Reply: Orsini Teaches KEK Management In Other Embodiments

Orsini **already** taught techniques for managing and securing other KEKs, or (at least) could have been modified in a simple, straightforward way to use conventional techniques for doing so. As discussed below (§II.B), Orsini supports prior art “Triple DES and AES” (Orsini, [0378]), which used and managed KEKs. Bhattacharjee-Reply, ¶¶230-232. Orsini also supports “a wide number of alternative key management systems.” Orsini, [0107].

-00215 Reply, 25-26;

-00214 Reply, 27

Even If Orsini Teaches KEK-Management, Petitioner Fails To Provide A Motivation To Combine The Different Embodiments



when “combining multiple embodiments from a single reference, or selecting from large lists of elements in a single reference, **there must be a motivation to make the combination** ... otherwise a skilled artisan would not arrive at the claimed combination.”

In re Stepan Co., 868 F.3d 1342, 1346 n.1 (Fed. Cir. Aug. 2017)

Petitioner’s Proffered
Motivation:



The Reply's New Proposed Modifications Does Not Cure The Petition's Hindsight



“The Board did not err in discounting modifications not presented in Medtronic’s petition as indicative of hindsight. It was within the Board’s discretion not to consider these untimely raised modifications.”

Medtronic, Inc. v. Teleflex Innovations S.A.R.L., 70 F.4th 1331, 1347 (Fed. Cir. 2023)

Petitioner's Grounds

1. Foster Grounds

- a) Foster and Hayhurst (IPR2024-00212/215)
- b) Foster Alone (IPR2024-00214)

2. Orsini Grounds (IPR2024-00214/215)

3. **Tajima Grounds (IPR2024-00212)**

212 IPR: Tajima, Foster, Rivest, & Shyu

PETITION FOR INTER PARTES REVIEW

IPR2024-00212
Patent 11,178,116 B2

Claims Challenged	Pre-AIA ² 35 U.S.C. §	Reference(s)/Basis
1, 5–8	102/103	Tajima
1, 2, 9, 11–14	103	Tajima, Foster
9–14	103	Tajima, Rivest
1–3, 6	103	Tajima, Rivest, Shyu
1, 2, 5, 9, 11	103	Foster, Hayhurst

The Board Should Disregard the Improperly Incorporated-By-Reference Reply Declaration and New Exhibits

Petitioner's Reply Cites 42 Paragraphs Of Reply Declaration and 42 New Exhibits, But Provides No Meaningful Discussion or Explanation



PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

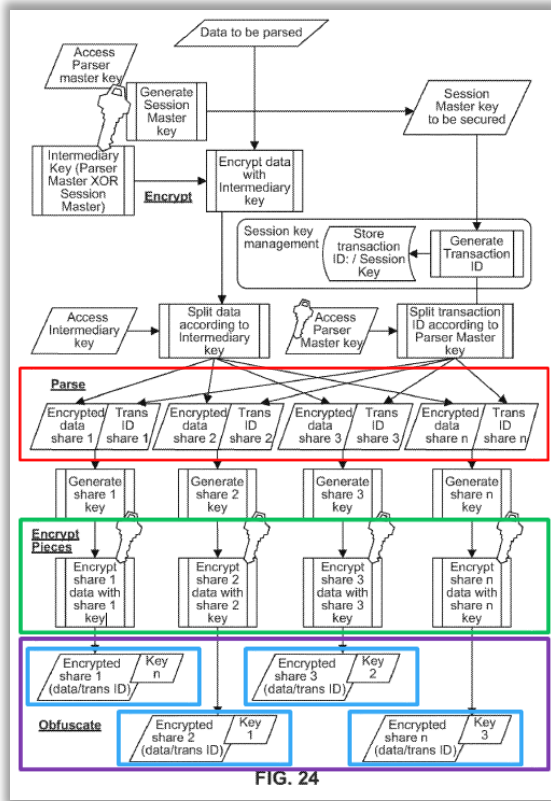
and Hayhurst describe overlapping techniques for securing data. Hayhurst *expressly* says its Technical Field “relates to” the “secure handling and storage” of data ([0002]) and uses a technique the ’116 patent itself says secures data (distributed data storage). Bhattacharjee-Reply, ¶¶65-80.

limited to streaming “live” broadcasts. POSAs knew CAS is used in video-on-demand (VOD) systems, where “content *is stored pre-encrypted* on hard drives in the VOD server” (EX1110, [0007]) and stored in “*storage media*” (EX1072, [0043]); Bhattacharjee-Reply, ¶¶128-142 (citing also EX1073, [0001]-[0004], [0043]; EX1097, 2:32-52; EX1075, 1:51-67; EX1076, 9:53-10:5; EX1077, 1:48-65, 3:56-5:8). Rubin-Depo., 85-94.

“Arguments must not be incorporated by reference from one document into another document. Combined motions, oppositions, replies, or other combined documents are not permitted.”

37 C.F.R. § 42.6(a)(3)

'116 Patent, Cl. 1: Requires Chunking, Encrypting, And Obfuscating The Encryption Keys



Split data set into chunks

Encrypt each chunk with distinct encryption key

Obfuscate each of the distinct encryption keys

Separately store each chunk with a different obfuscated key

1. A method for securing a data set, the method comprising:

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypting each of the data chunks with a respective one of a plurality of encryption keys;

obfuscating each of the plurality of different encryption keys; and

separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys on a plurality of different storage devices.

Claim 9 Of The '116 Patent Requires Transforming, Rather Than Obfuscating The Encryption Keys

9. A method for securing a data set, the method comprising:

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypting each of the data chunks with a respective one of a plurality of encryption keys;

transforming each of the plurality of different encryption keys; and

separately storing each data chunk of the plurality of data chunks together with one of the plurality of transformed different encryption keys on a plurality of different storage devices.

Split data set into chunks

Encrypt each chunk with distinct encryption key

Transform each of the distinct encryption keys

Separately store each chunk with a different transformed key

In one embodiment of the present invention, encryption keys, splitting keys, or both as used in accordance with the present invention may be further encrypted using, for example, a workgroup key in order to provide an extra level of security to a secured data set.

'116 Patent Col. 77:43-47

According to one embodiment of the present invention, an All or Nothing Transform (AoNT), such as a Full Package Transform, may be used to further secure data by transforming splitting keys, encryption keys, any other suitable data elements, or any combination thereof. For example, an

'116 Patent Col. 77:13-17

Petitioner's Ground 2: Tajima-Foster

Claims Challenged	Pre-AIA ² 35 U.S.C. §	Reference(s)/Basis
1, 5–8	102/103	Tajima
1, 2, 9, 11–14	103	Tajima, Foster
9–14	103	Tajima, Rivest
1–3, 6	103	Tajima, Rivest, Shyu
1, 2, 5, 9, 11	103	Foster, Hayhurst

A POSITA Would Not Be Motivated To Combine Tajima With Foster

- 1. Tajima and Foster solve different problems in different fields**
- 2. Tajima and Foster are fundamentally incompatible**
- 3. Petitioner's combination is redundant because Tajima already solves the problem proposed to address by adding Foster**

Petitioner Must Show A POSITA Would Have Combined Tajima-Foster In The Normal Course Of Research And Development



Obviousness requires a showing that a POSITA
“**would have selected and combined [the] prior art elements in the normal course of research and development to yield the claimed invention.**”

Unigene Labs., Inc. v. Apotex, Inc.,
655 F.3d 1352, 1360 (Fed. Cir. 2011).

1. Tajima-Foster: Different Problems, Different Fields

Tajima Improves The Security of Personal Information

[0044] It is an object of the present invention to provide a personal information management system, a personal information management method, and a server that can improve the security of personal information that is registered with areas that are connectible to the Internet.

Ex., 1005, [0044]

DECLARATION OF AVIEL D. RUBIN, PH.D.

54. It is my opinion that Tajima and Foster are directed to entirely different fields and different problems. Tajima “relates to a personal information management system” and improves upon a prior art “online shopping system” and prior art “public key cryptosystem” with a certificate authority. See EX1005, [0001], [0004]-[0007], [0025], [0042]. Thus, Tajima teaches that “an object of’ its invention is to “improve the security of personal information.” *Id.*, 44. More specifically,

Foster Improves Random Access to Streamed & Encrypted Media Packets

[0002] The present invention generally relates to a method, system and program product for attaching a title key to encrypted content for synchronized transmission to a recipient. Specifically, a title key used to encrypt content is itself encrypted, and attached to the encrypted content so that both can be synchronously transmitted to a recipient.

Ex., 1006, [0002]

Moreover, synchronized transmission and delivery of title keys with encrypted content allows random access of the content.

Ex., 1006, [0071]

1. Tajima-Foster: Different Problems, Different Fields

Tajima prior art: Key information and encrypted content stored together

[0042] However, if the above-described personal information relating to a user is registered with one area that is connectible to the Internet, there is the danger that, because the information registered with one area as a contiguous data file, this information may be viewed by unauthorized access from the outside through a security hole or by unauthorized access by someone inside the system, even though the information is registered with an area that is closed to the outside by means of the access control function of a server or a firewall.

Ex., 1005, [0042]

Tajima's solution: Key information and data it encrypts are stored separately

certificate authority 40b. Information regarding the key that was used for the encryption of data fragment Y is attached to encrypted data fragment X, and information regarding the key that was used in the encryption of data fragment X is attached to encrypted data fragment Y.

Ex., 1005, [0111]

Foster prior art: Key and encrypted content transmitted separately

to a recipient. Similar to the DRMS and CAS shown in FIGS. 1 and 2, however, the protected content is transmitted separately from the objects (i.e., key values) used to encrypt the content. Under such a scenario, errors and/or delays in decrypting content blocks 56A-C can occur. Moreover, when separately transmitting key values 55A-C, random access of content is not possible. Specifically, it is not possible to access a content stream from any content block.

Ex., 1006, [0063]

Foster's solution: Key and encrypted content transmitted together

content unit 116 can then be transmitted to a recipient. That is, the encrypted content unit, the header and the header extension (including the encrypted title key) will be delivered to, or stored by, a recipient as a single, integral data stream.

Ex., 1006, [0064]

2. Tajima Is Fundamentally Incompatible With Foster

Foster's "whole invention" is synchronized transmission: Keeping the key with the data it encrypts

DEPOSITION OF SAMRAT BHATTACHARJEE, PH.D.

Q. Why does synchronous transmission to a receiver foster random access to content?

A. That is sort of the whole invention in Foster.

DECLARATION OF AVIEL D. RUBIN, PH.D.

78. Foster, by contrast, discloses a system in which "[t]he encrypted title key [is] attached to the content packet and the header for synchronized transmission to, or storage by a receiver. *Id.*, [0008] In fact, attaching the key to content it can decrypt for synchronized transmission of the two together is essential to Foster's system—it is "the whole invention," as Dr. Bhattacharjee opined at his deposition. EX2034, 32:20-23.

2. Tajima is Fundamentally Incompatible with Foster

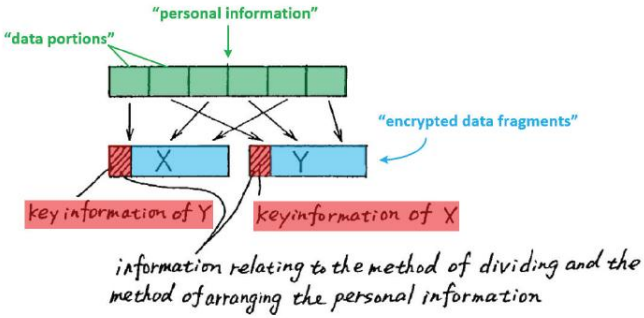
The “key” to Tajima’s invention is keeping key information separate from data chunk it encrypts

DECLARATION OF AVIEL D. RUBIN, PH.D.

data fragment X is attached to encrypted data fragment Y.” In other words, each chunk is attached to, and stored with, information about a key that is not the one used to encrypt it. Tajima EX1005, [0111]-[0114]. This means that by design Tajima’s system cannot perform synchronized transmission.

DECLARATION OF SAMRAT BHATTACHARJEE, PH.D.

Fig. 12

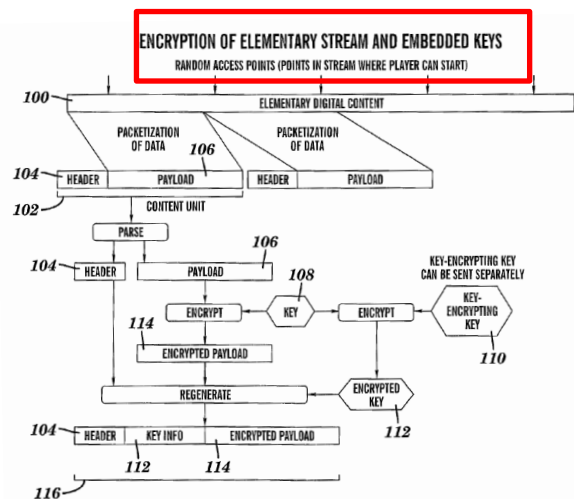


70. Next, “[d]ata fragments X and Y are then each encrypted” with a respective key (encrypted data fragments highlighted blue), key information of fragment Y is attached to encrypted data fragment X, and key information for fragment X is attached to encrypted data fragment Y (as highlighted red). *Id.*

2. Foster Discourages Combination With Tajima

DECLARATION OF AVIEL D. RUBIN, PH.D.

not be decrypted.” EX1006, [0007]. As explained in Foster’s specification, Foster’s invention solved this problem because “by transmitting the encrypted key as an integral part of the encrypted content, a receiver would receive the encrypted content as well as all information necessary to decrypt the content in a single stream.” *Id.*



Foster Teaches that Key Information/Keys Must Be Kept With Data Packet

[0009] According to a first aspect of the present invention, a method for attaching a title key to encrypted content for synchronized transmission to a recipient is provided. The method comprises the steps of: (1) encrypting content with a title key; (2) encrypting the title key with a key encrypting key; and (3) attaching the encrypted title key to the encrypted content for synchronized transmission to a recipient.

decrypting content blocks 56A-C can occur. Moreover, when separately transmitting key values 55A-C, random access of content is not possible. Specifically, it is not possible to access a content stream from any content block.

2. Tajima Discourages Combination With Foster

Tajima is an alternative to be used where key encryption, like that in Foster, is not secure

For information stored in locations connected to the internet, encryption may not provide security. Tajima explains:

[0043] Alternatively, a method may be employed in which personal information relating to a user is registered with an encrypted state. In such cases, however, the danger still remains that, even though the content of the registered personal information is encrypted and thus cannot be viewed even when stolen, given enough time, a high-speed computer may be used to decrypt the encrypted personal information.

[0044] It is an object of the present invention to provide a personal information management system, a personal information management method, and a server that can improve the security of personal information that is registered with areas that are connectible to the Internet.

A POSITA Would Not Combine Foster With Tajima



Obviousness requires a showing that a POSITA “**would have selected and combined [the] prior art elements in the normal course of research and development to yield the claimed invention.**”

Unigene Lab'ys, Inc. v. Apotex, Inc.,
655 F.3d 1352, 1360 (Fed. Cir. 2011).

DECLARATION OF AVIEL D. RUBIN, PH.D.

62. In my opinion, Tajima and Foster are far afield of one another, arise in manifestly different environments and confront quite different problems. I do not believe a POSITA would have naturally combined Tajima and Foster in the normal course of research and development.

Tajima

Foster

Focus	Context	Data Type	Location of Key Information	Securing Key Information/Encryption Keys
Security	E-commerce	Personal Data	<u>Cannot</u> be kept with Data Portion	Secures key information by storing with data it cannot decrypt
Reducing Latencies	Streaming Video	MPEG Packets	<u>Must</u> be kept with Packet	Secures keys by transmitting keys with data

3. Combination Is Redundant Because Tajima Already Addresses Petitioner's Proposed Motivation To Combine

Petitioner Only offers a single reason for combining Foster with Tajima: Foster's key encryption provides an "increased level of security" where an attacker recovers all of Tajima's data fragments

Single Motivation:

Ground 2 applies "Foster's key-encryption technique to encrypt Tajima's key[s]...to benefit from the **increased level of security**" of storing encrypted rather than plaintext keys. Petition, 37.

Reply, 12

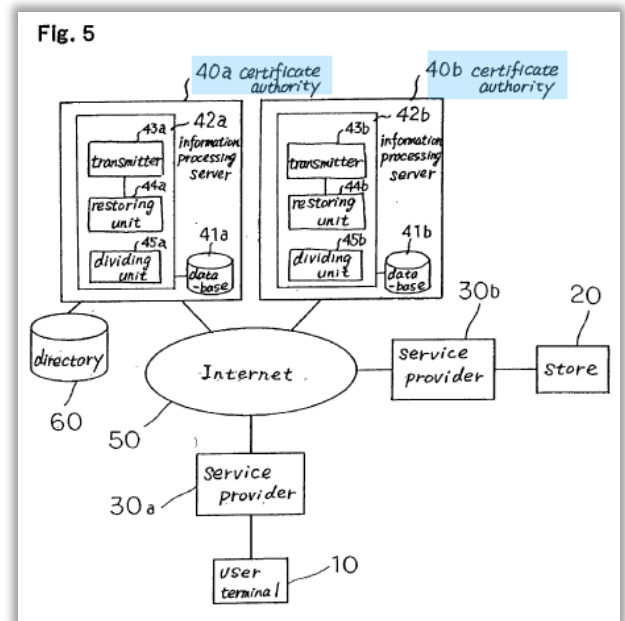
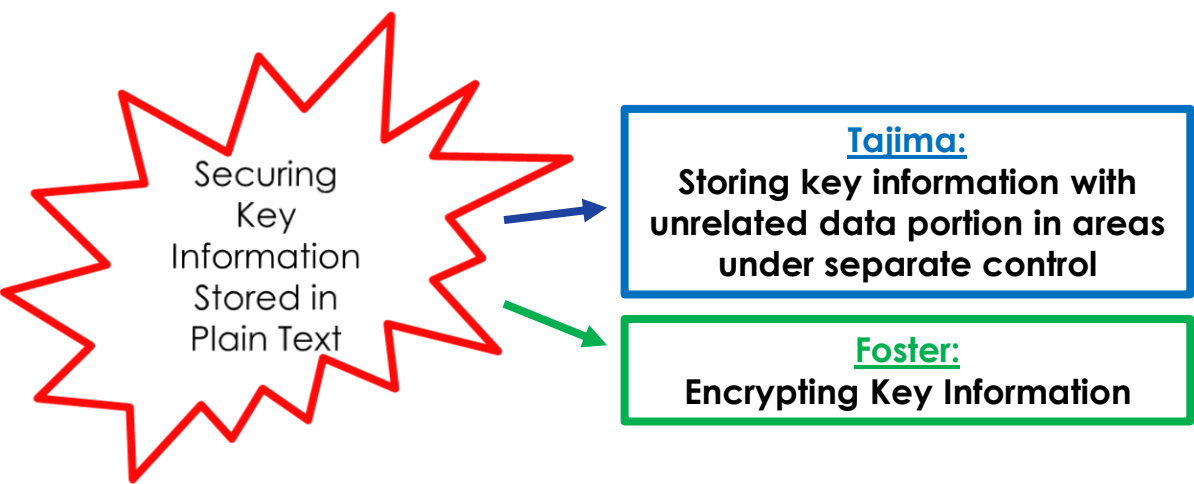
Single Context:

"Instead, Tajima-Foster **improves Tajima's** security, furthering Tajima's objective of preventing unauthorized access to personal information...[t]hat Tajima-Foster improves security of Tajima's data fragments **should an attacker successfully acquire all of them** is undisputed."

Reply, 18

But Tajima already solves this problem.

3. Petitioner's Combination Is Redundant Because Tajima Already Solves The Issue of Securing Plain-Text Key Information



Ex., 1005, Fig. 5

3. Tajima Protects Key Information By Storing The Key Information In Different Locations, Each “Under Separate Control”

[0048] Thus, because personal information that is registered with areas that are connectible to the Internet is divided into a plurality of data portions and then registered with areas that are each under separate control, the personal information cannot be viewed unless all of the areas in which data are registered are exposed, and an improvement can therefore be obtained in the security of personal information that is registered with areas that are connectible to the Internet.

Fig. 12

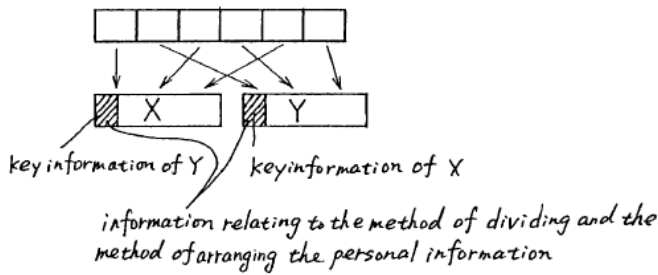
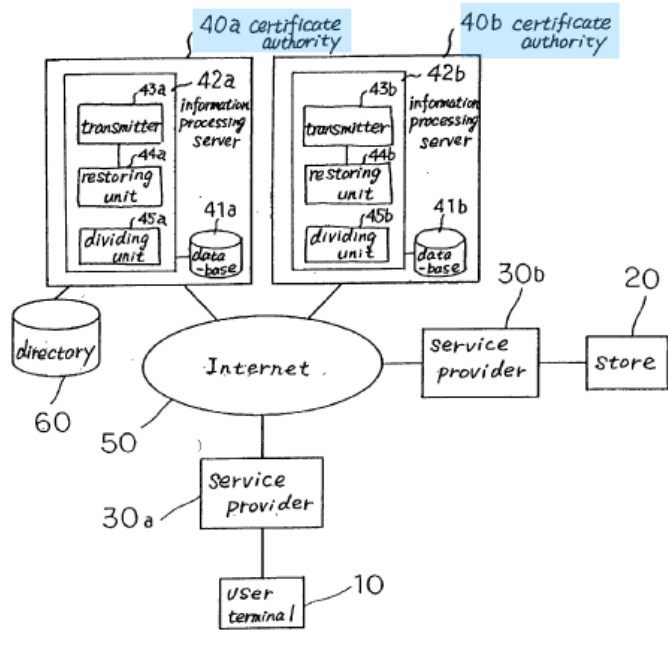
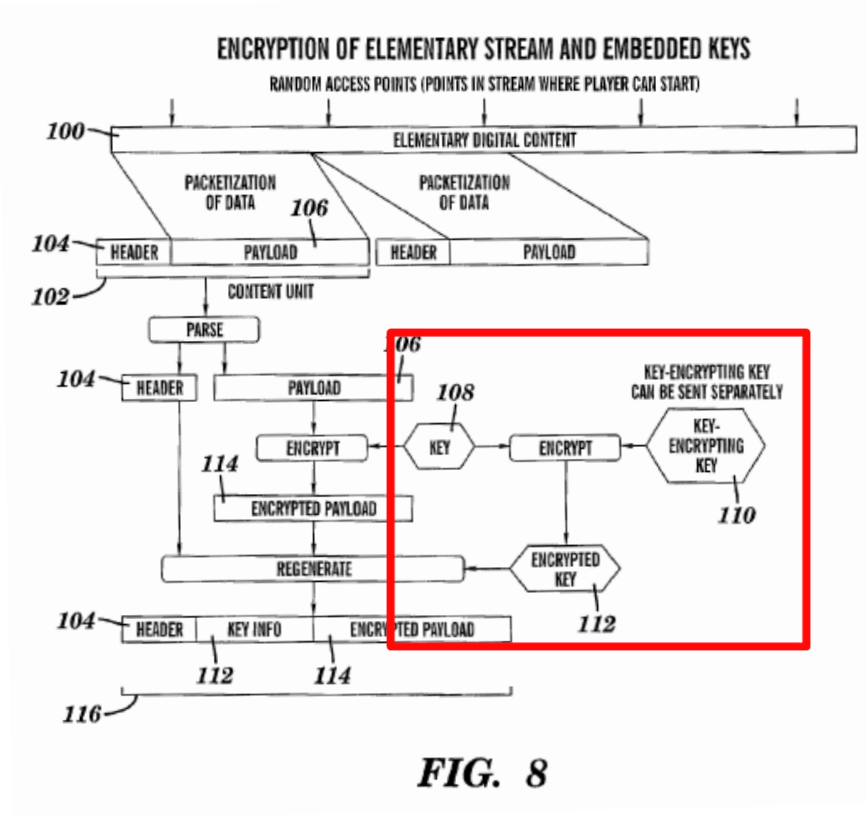


Fig. 5



3. Foster Secures The Key Information By Encrypting The Packet Encryption Keys

[0008] In general, the present invention provides a method, system and program product for attaching a title key to encrypted content for synchronized transmission to a recipient. Specifically, under the present invention, a content unit including a content packet and a header is received and parsed. A title key is then used to encrypt the content packet. Once the content packet is encrypted, the title key is itself encrypted with a key encrypting key. The encrypted title key



3. Tajima Protects Key Information By Storing It In Different Locations, Each “Under Separate Control;” An Attacker Cannot Get All Data Portions

**Tajima *Recognized* The Issue
Addressed in Foster**



[0042] However, if the above-described personal information relating to a user is registered with one area that is connectible to the Internet, there is the danger that, because the information registered with one area as a contiguous data file, this information may be viewed by unauthorized access from the outside through a security hole or by unauthorized access by someone inside the system, even though the information is registered with an area that is closed to the outside by means of the access control function of a server or a firewall.

**Foster Is Redundant Because
Tajima *Solved* The Issue Addressed
By Foster Without Key Encryption**



[0048] Thus, because personal information that is registered with areas that are connectible to the Internet is divided into a plurality of data portions and then registered with areas that are each under separate control, the personal information cannot be viewed unless all of the areas in which data are registered are exposed, and an improvement can therefore be obtained in the security of personal information that is registered with areas that are connectible to the Internet.

3. As Petitioner's Expert Admits, Tajima Already Avoids The Only Vulnerability That Motivates The Proposed Combination



Denying institution where “**Petitioner ... fails to provide a specific explanation why [the primary reference] did not already accomplish [the asserted benefits] by itself.**”

Apple Inc. v. Cellular Comm'ns Equipment, LLC,
IPR2015-00576, Paper 7, 12 (June 12, 2015)

DECLARATION OF SAMRAT BHATTACHARJEE, PH.D.

62. To address this vulnerability, Tajima's system (1) divides personal information into data fragments “such that each data fragment is completely unintelligible when taken independently” (Tajima, [0072], [0122]) and (2) stores (i.e., “registers”) each data fragment in “areas that are each under separate control” (Tajima, [0048])—i.e., different databases belonging to separate service sites connected to the Internet—so a security breach at any one area is insufficient to recover a user's personal information. That is, an attacker that successfully gained unauthorized access to a service site could procure only a single “unintelligible” data fragment and the attacker would not be able to recover the user's personal information. Tajima, [0042], [0046]-[0048], [0067], [0118], [0152].

3. Experts Agree: Combining Foster's Key Encryption With Tajima's Storage is Redundant

Dr. Bhattacharjee

Placing key information in separately controlled locations as in Tajima is a "perfect" alternative to key encryption

DEPOSITION OF SAMRAT BHATTACHARJEE, PH.D.

23 Now, from a network attacker's point of
24 view, if you were to put a piece of data on a USB
25 drive, remove it from the original computer that's
1 connected to the network, it's nearly perfect
2 security. Because no matter how much computation
3 they have, they're not going to be able to get to
4 it. So it's a very secure method. It is offline
5 storage, it's usually called.

Dr. Rubin

DECLARATION OF AVIEL D. RUBIN, PH.D.

Foster acknowledges that its "title key is encrypted with the key encrypting key" precisely so that it "can then be transmitted along with the encrypted content." EX1006, [0053]. By this suggestion, Foster ties the benefits of its KEK method to the need to secure the keys that encrypt the packets themselves (by encryption with a KEK) so that the keys can be transmitted together with the packets.

* * *

Tajima, in contrast, has no need to further secure its key information by encryption because it already secures that information by hiding it with a data fragment it cannot decrypt.

Petitioner's Ground 3: Tajima-Rivest

Claims Challenged	Pre-AIA ² 35 U.S.C. §	Reference(s)/Basis
1, 5–8	102/103	Tajima
1, 2, 9, 11–14	103	Tajima, Foster
9–14	103	Tajima, Rivest
1–3, 6	103	Tajima, Rivest, Shyu
1, 2, 5, 9, 11	103	Foster, Hayhurst

A POSITA Would Not Be Motivated To Combine Tajima With Rivest

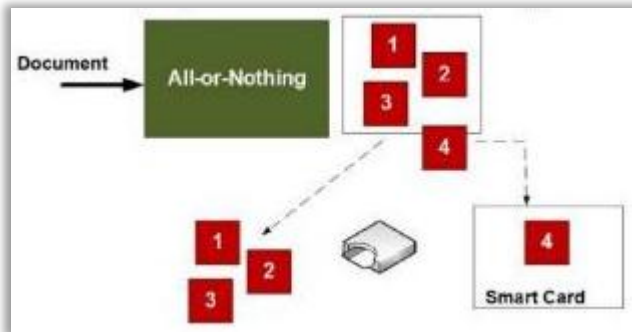
- 1. Petitioner's Tajima-Rivest Combination Is Redundant**
- 2. Rivest's AoNT Does Not Provide Additional Security & Violates Kerckhoffs' Principle**
- 3. Petitioner's Combination Creates Data Integrity Issues**

Rivest Is A Pre-Processing Step That Can Be Reversed By Anyone That Knows The Number Used To Perform The Transformation (the “AoNT Number”)

All-or-Nothing Encryption and the Package Transform

Ronald L. Rivest

Abstract. We present a new mode of encryption for block ciphers, which we call *all-or-nothing encryption*. This mode has the interesting defining property that one must decrypt the entire ciphertext before one can determine even one message block. This means that brute-force searches against all-or-nothing encryption are slowed down by a factor equal to the number of blocks in the ciphertext. We give a specific way of implementing all-or-nothing encryption using a “package transform” as a pre-processing step to an ordinary encryption mode. A package trans-



DECLARATION OF AVIEL D. RUBIN, PH.D.

Rivest discloses that the AoNT is merely a “pre-processing” step “that has certain interesting properties,” but by itself does not provide adequate protection to a dataset (such as the key information of Tajima). 1034 [Rivest] 212.

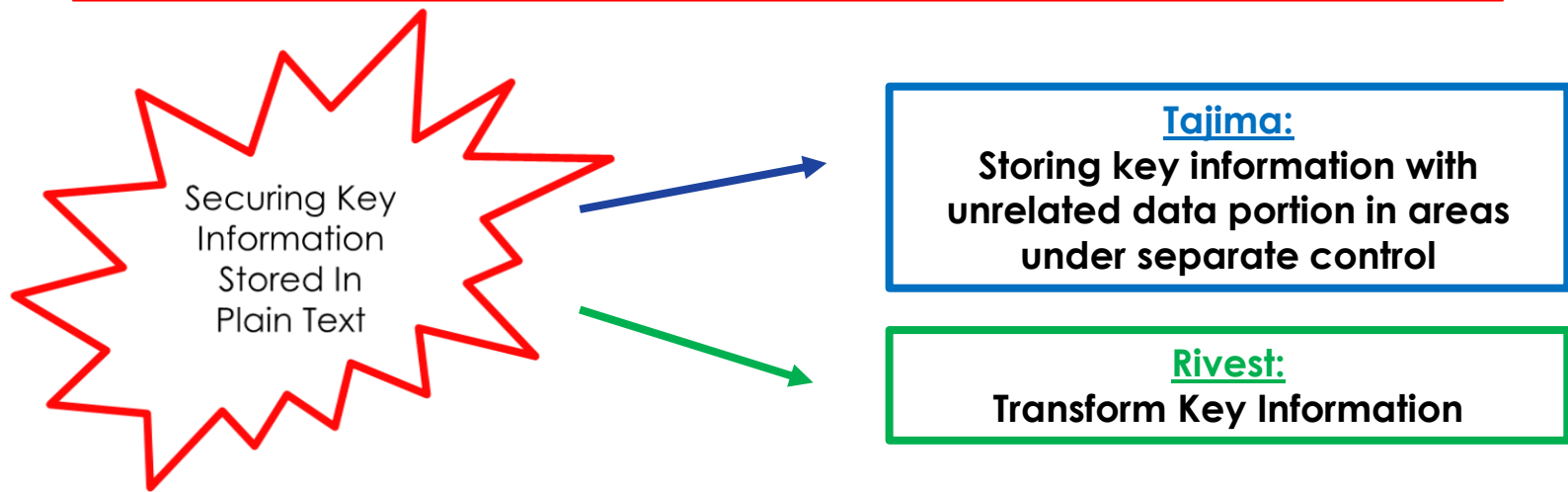
However, if the data set has merely been transformed using the AoNT, without further encryption or splitting, “anyone” who knows the random number on which the transformation is based can “invert” it to obtain the original dataset.

1. A POSITA Would Not Be Motivated To Combine Tajima & Rivest Because Tajima-Rivest Is Redundant

PETITION FOR INTER PARTES REVIEW

A POSA would have recognized the benefit of applying Rivest's "all-or-nothing" transforms (AoNT) to Tajima's key information to protect Tajima's plaintext keys (see §§VI.A-VI.B *supra*) without needing to maintain secret keys.

But Tajima already solves the problem of securing plain text key information:



2. Petitioner Proposes To Use A Public Key As The AoNT Number, But A Known AoNT Number Cannot Provide Security

Petitioner's Proposed Combination:

PETITION FOR INTER PARTES REVIEW

“Tajima-Rivest applies Rivest’s AoNT using the user’s **public** key provided to Tajima’s service sites...and thus beneficially avoids using secret keys.”

Public keys are not kept secret:
They are known to the **public**.

Rivest provides no protection if the AoNT Number is known:

DECLARATION OF AVIEL D. RUBIN, PH.D.

84. In my opinion, a POSITA would not be motivated to apply Rivest’s AoNT using the user’s public key as Petitioner suggests. Rivest says nothing about the use of public keys and is not designed to be used with public keys.

85. A POSITA would understand that without and a secret key, Rivest’s AoNT provides no security. EX1034, 212. Rather, the AoNT is used because it adds a property to a data set that can be useful for some applications.

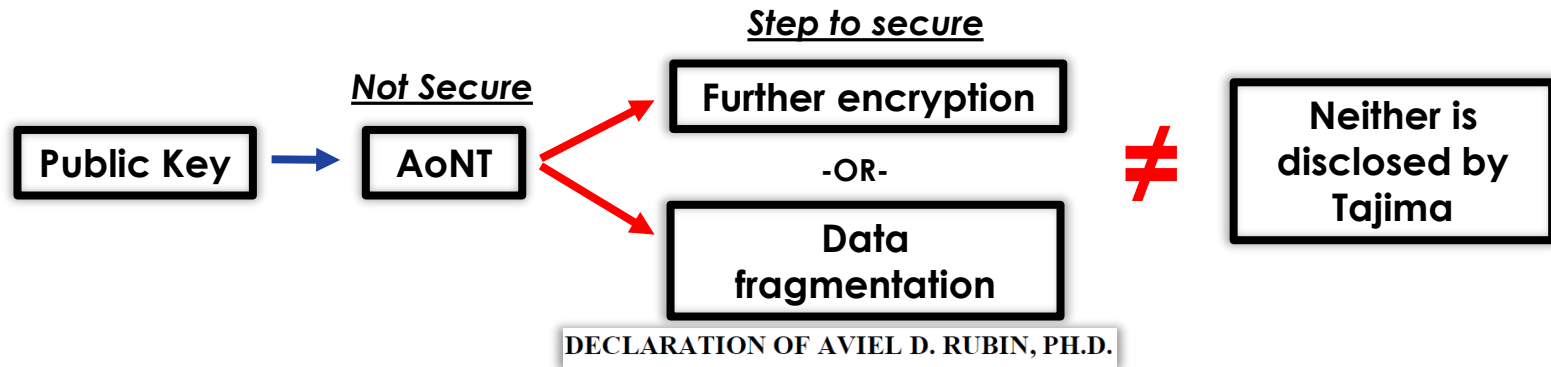
2. Tajima-Rivest Violates Kerckhoffs' Principle By Using A Known Public Key



Auguste Kerckhoffs

Kerckhoffs' principle, a fundamental rule of cryptography, requires that security of encrypted content
"rely solely on the secrecy of the key"

2. Petitioner's Combination Would Require Further, Undisclosed Steps To Secure Tajima's Key Information



without the need to maintain secret keys.” The AoNT transformation of Rivest cannot secure a key without a further encryption step or fragmentation step that would have to be added to Tajima. See EX1001, 77:5-47. If further encryption is used, that would require the system to use and maintain another secret key. Fragmenting the key and storing the pieces in different locations would be another way of securing the transformed title key, but that also is a step that would have to be added to Tajima that would require maintaining information about the locations of the pieces of the fragmented key.

3. A POSITA Would Not Be Motivated To Combine Rivest With Tajima Because Of The Risk of Data Loss

All-or-Nothing Encryption and the Package Transform

Ronald L. Rivest

[A]ll-or-nothing encryption has **terrible** error-propagation properties: if **any** ciphertext block is damaged, it is likely that **every** message block will be damaged. Thus, ciphertext should be transported with **reliable transmission means**.

Ex. 1034, 216

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

Petitioner claims its combination only stores Tajima-Rivest's transformed keys with the data fragments, but in its Reply admits that "individual transformed message blocks are kept **and transmitted** together."

Reply, 20



"[t]he Board must **weigh the benefits and drawbacks** of the modification against each other, to determine whether there would be a motivation to combine."

Arctic Cat Inc. v. Polaris Indus.,
795 Fed. App'x. 827, 833 (Fed. Cir. 2019)