References

1. AACS Specifications, 2006. http://www.aacsla.com/specifications/.
2. M. Abdalla, D. Pointcheval, P.-A. Fouque, and D. Vergnaud, editors. *Applied Cryptography and Network Security, 7th International Conference, ACNS 2009, Paris-Rocquencourt, France, June 2-5, 2009. Proceedings*, volume 5536 of *Lecture Notes in Computer Science*, 2009.
3. M. Abdalla, Y. Shavitt, and A. Wool. Key management for restricted multicast using broadcast encryption. *IEEE/ACM Trans. Netw.*, 8(4):443–454, 2000.
4. W. Aiello, S. Lodha, and R. Ostrovsky. Fast digital identity revocation (extended abstract). In H. Krawczyk, editor, *CRYPTO*, volume 1462 of *Lecture Notes in Computer Science*, pages 137–152. Springer, 1998.
5. M. Ak, K. Kaya, and A. A. Selcuk. Optimal subset-difference broadcast encryption with free riders. *Information Sciences*, 2009.
6. N. Attrapadung and H. Imai. Graph-decomposition-based frameworks for subset-cover broadcast encryption and efficient instantiations. In B. K. Roy, editor, *ASIACRYPT*, volume 3788 of *Lecture Notes in Computer Science*, pages 100–120. Springer, 2005.
7. L. M. Batten and X. Yi. Efficient broadcast key distribution with dynamic revocation. *Security and Communication Networks*, 1(4):351–362, 2008.
8. M. Bellare, editor. *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, volume 1880 of *Lecture Notes in Computer Science*. Springer, 2000.
9. O. Berkman, M. Parnas, and J. Sgall. Efficient dynamic traitor tracing. In *SODA*, pages 586–595, 2000.
10. S. Berkovits. How to broadcast a secret. In *EUROCRYPT*, pages 535–541, 1991.
11. E. R. Berlekamp and L. Welch. Error correction of algebraic block codes. U.S. Patent, Number 4,633,470, 1986.
12. I. Biehl and B. Meyer. Protocols for collusion-secure asymmetric fingerprinting (extended abstract). In R. Reischuk and M. Morvan, editors, *STACS*, volume 1200 of *Lecture Notes in Computer Science*, pages 399–412. Springer, 1997.
13. O. Billet and D. H. Phan. Efficient traitor tracing from collusion secure codes. In R. Safavi-Naini, editor, *ICITS*, volume 5155 of *Lecture Notes in Computer Science*, pages 171–182. Springer, 2008.

14. O. Billet and D. H. Phan. Traitors collaborating in public: Pirates 2.0. In A. Joux, editor, *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 189–205. Springer, 2009.
15. G. R. Blakley, C. Meadows, and G. B. Purdy. Fingerprinting long forgiving messages. In H. C. Williams, editor, *CRYPTO*, volume 218 of *Lecture Notes in Computer Science*, pages 180–189. Springer, 1985.
16. D. Boneh and M. K. Franklin. An efficient public key traitor tracing scheme. In Wiener [124], pages 338–353.
17. D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In J. Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.
18. D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Shoup [109], pages 258–275.
19. D. Boneh and M. Hamburg. Generalized identity based and broadcast encryption schemes. In J. Pieprzyk, editor, *ASIACRYPT*, volume 5350 of *Lecture Notes in Computer Science*, pages 455–470. Springer, 2008.
20. D. Boneh, A. Kiayias, and H. W. Montgomery. Robust fingerprinting codes : a near optimal construction. In *ACM Workshop on Digital Rights Management*, 2010.
21. D. Boneh and M. Naor. Traitor tracing with constant size ciphertext. In P. Ning, P. F. Syverson, and S. Jha, editors, *ACM Conference on Computer and Communications Security*, pages 501–510. ACM, 2008.
22. D. Boneh, A. Sahai, and B. Waters. Fully collusion resistant traitor tracing with short ciphertexts and private keys. In S. Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 573–592. Springer, 2006.
23. D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data (extended abstract). In D. Coppersmith, editor, *CRYPTO*, volume 963 of *Lecture Notes in Computer Science*, pages 452–465. Springer, 1995.
24. D. Boneh and B. Waters. A fully collusion resistant broadcast, trace, and revoke system. In A. Juels, R. N. Wright, and S. D. C. di Vimercati, editors, *ACM Conference on Computer and Communications Security*, pages 211–220. ACM, 2006.
25. R. Canetti, J. A. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas. Multicast security: A taxonomy and some efficient constructions. In *INFOCOM*, pages 708–716, 1999.
26. R. Canetti, T. Malkin, and K. Nissim. Efficient communication-storage tradeoffs for multicast encryption. In *EUROCRYPT*, pages 459–474, 1999.
27. H. Chabanne, D. H. Phan, and D. Pointcheval. Public traceability in traitor tracing schemes. In Cramer [31], pages 542–558.
28. B. Chor, A. Fiat, and M. Naor. Tracing traitors. In Y. Desmedt, editor, *CRYPTO*, volume 839 of *Lecture Notes in Computer Science*, pages 257–270. Springer, 1994.
29. B. Chor, A. Fiat, M. Naor, and B. Pinkas. Tracing traitors. *IEEE Transactions on Information Theory*, 46(3):893–910, 2000.
30. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, 1997.

31. R. Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005.
32. J. Daemen and V. Rijmen. *The Design of Rijndael: AES- The Advanced Encryption Standard*. Springer, New York, 2002.
33. C. Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys. In *ASIACRYPT*, pages 200–215, 2007.
34. C. Delerablée, P. Paillier, and D. Pointcheval. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, editors, *Pairing*, volume 4575 of *Lecture Notes in Computer Science*, pages 39–59. Springer, 2007.
35. Y. Dodis and N. Fazio. Public key broadcast encryption for stateless receivers. In Feigenbaum [41], pages 61–80.
36. Y. Dodis and N. Fazio. Public key trace and revoke scheme secure against adaptive chosen ciphertext attack. In Y. Desmedt, editor, *Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 100–115. Springer, 2003.
37. Y. Dodis, N. Fazio, A. Kiayias, and M. Yung. Scalable public-key tracing and revoking. In *PODC*, pages 190–199, 2003.
38. C. Dwork, M. Naor, O. Reingold, G. N. Rothblum, and S. P. Vadhan. On the complexity of differentially private data release: efficient algorithms and hardness results. In M. Mitzenmacher, editor, *STOC*, pages 381–390. ACM, 2009.
39. N. Fazio, A. Nicolosi, and D. H. Phan. Traitor tracing with optimal transmission rate. In J. A. Garay, A. K. Lenstra, M. Mambo, and R. Peralta, editors, *ISC*, volume 4779 of *Lecture Notes in Computer Science*, pages 71–88. Springer, 2007.
40. U. Feige, P. Raghavan, D. Peleg, and E. Upfal. Computing with noisy information. *SIAM J. Comput.*, 23(5):1001–1018, 1994.
41. J. Feigenbaum, editor. *Security and Privacy in Digital Rights Management, ACM CCS-9 Workshop, DRM 2002, Washington, DC, USA, November 18, 2002, Revised Papers*, volume 2696 of *Lecture Notes in Computer Science*. Springer, 2003.
42. A. Fiat and M. Naor. Broadcast encryption. In Stinson [112], pages 480–491.
43. A. Fiat and T. Tassa. Dynamic traitor training. In Wiener [124], pages 354–371.
44. J. Furukawa and N. Attrapadung. Fully collusion resistant black-box traitor revocable broadcast encryption with short private keys. In L. Arge, C. Cachin, T. Jurdzinski, and A. Tarlecki, editors, *ICALP*, volume 4596 of *Lecture Notes in Computer Science*, pages 496–508. Springer, 2007.
45. E. Gafni, J. Staddon, and Y. L. Yin. Efficient methods for integrating traceability and broadcast encryption. In Wiener [124], pages 372–387.
46. S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008.
47. J. A. Garay, J. Staddon, and A. Wool. Long-lived broadcast encryption. In Bellare [8], pages 333–352.
48. M. R. Garey, D. S. Johnson, and L. J. Stockmeyer. Some simplified np-complete problems. In *STOC*, pages 47–63, 1974.

49. C. Gentry, Z. Ramzan, and D. P. Woodruff. Explicit exclusive set systems with applications to broadcast encryption. In *FOCS*, pages 27–38. IEEE Computer Society, 2006.
50. M. T. Goodrich, J. Z. Sun, and R. Tamassia. Efficient tree-based revocation in groups of low-state devices. In M. K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 511–527. Springer, 2004.
51. V. Guruswami and M. Sudan. Improved decoding of reed-solomon and algebraic-geometric codes. In *FOCS*, pages 28–39, 1998.
52. H.-J. Guth and B. Pfitzmann. Error- and collusion-secure fingerprinting for digital data. In A. Pfitzmann, editor, *Information Hiding*, volume 1768 of *Lecture Notes in Computer Science*, pages 134–145. Springer, 1999.
53. D. Halevy and A. Shamir. The lsd broadcast encryption scheme. In M. Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 47–60. Springer, 2002.
54. H. D. L. Hollmann, J. H. van Lint, J.-P. M. G. Linnartz, and L. M. G. M. Tolhuizen. On codes with the identifiable parent property. *J. Comb. Theory, Ser. A*, 82(2):121–133, 1998.
55. J. Y. Hwang, D. H. Lee, and J. Lim. Generic transformation for scalable broadcast encryption schemes. In Shoup [109], pages 276–292.
56. Y. H. Hwang and P. J. Lee. Efficient broadcast encryption scheme with log-key storage. In G. D. Crescenzo and A. D. Rubin, editors, *Financial Cryptography*, volume 4107 of *Lecture Notes in Computer Science*, pages 281–295. Springer, 2006.
57. N.-S. Jho, J. Y. Hwang, J. H. Cheon, M.-H. Kim, D. H. Lee, and E. S. Yoo. One-way chain based broadcast encryption schemes. In Cramer [31], pages 559–574.
58. H. Jin and J. Lotspiech. Renewable traitor tracing: A trace-revoke-trace system for anonymous attack. In J. Biskup and J. Lopez, editors, *ESORICS*, volume 4734 of *Lecture Notes in Computer Science*, pages 563–577. Springer, 2007.
59. H. Jin and J. B. Lotspiech. Defending against the pirate evolution attack. In F. Bao, H. Li, and G. Wang, editors, *ISPEC*, volume 5451 of *Lecture Notes in Computer Science*, pages 147–158. Springer, 2009.
60. H. Jin and S. Pehlivanoglu. Traitor tracing without a priori bound on the coalition size. In P. Samarati, M. Yung, F. Martinelli, and C. A. Ardagna, editors, *ISC*, volume 5735 of *Lecture Notes in Computer Science*, pages 234–241. Springer, 2009.
61. P. Junod, A. Karlov, and A. K. Lenstra. Improving the boneh-franklin traitor tracing scheme. In S. Jarecki and G. Tsudik, editors, *Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 88–104. Springer, 2009.
62. A. Kiayias and S. Pehlivanoglu. Pirate evolution: How to make the most of your traitor keys. In A. Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 448–465. Springer, 2007.
63. A. Kiayias and S. Pehlivanoglu. On the security of a public-key traitor tracing scheme with sublinear ciphertext size. In E. Al-Shaer, H. Jin, and G. L. Heileman, editors, *Digital Rights Management Workshop*, pages 1–10. ACM, 2009.
64. A. Kiayias and S. Pehlivanoglu. Tracing and revoking pirate rebroadcasts. In Abdalla et al. [2], pages 253–271.

65. A. Kiayias and S. Pehlivanoglu. Detecting and revoking pirate redistribution of content. U.S. Patent, Publication Number 2010/0043081, 2010.
66. A. Kiayias and S. Pehlivanoglu. Improving the round complexity of traitor tracing schemes. In J. Zhou and M. Yung, editors, *ACNS*, Lecture Notes in Computer Science, 2010.
67. A. Kiayias and M. Yung. On crafty pirates and foxy tracers. In Sander [104], pages 22–39.
68. A. Kiayias and M. Yung. Self protecting pirates and black-box traitor tracing. In Kilian [72], pages 63–79.
69. A. Kiayias and M. Yung. Breaking and repairing asymmetric public-key traitor tracing. In Feigenbaum [41], pages 32–50.
70. A. Kiayias and M. Yung. Traitor tracing with constant transmission rate. In L. R. Knudsen, editor, *EUROCRYPT*, volume 2332 of *Lecture Notes in Computer Science*, pages 450–465. Springer, 2002.
71. A. Kiayias and M. Yung. Public-key traitor tracing from efficient decoding and unbounded enrollment: extended abstract. In G. L. Heileman and M. Joye, editors, *Digital Rights Management Workshop*, pages 9–18. ACM, 2008.
72. J. Kilian, editor. *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*. Springer, 2001.
73. D. Kirovski and F. A. P. Petitcolas. Replacement attack on arbitrary watermarking systems. In Feigenbaum [41], pages 177–189.
74. N. Kogan, Y. Shavitt, and A. Wool. A practical revocation scheme for broadcast encryption using smart cards. In *IEEE Symposium on Security and Privacy*, pages 225–235. IEEE Computer Society, 2003.
75. H. Komaki, Y. Watanabe, G. Hanaoka, and H. Imai. Efficient asymmetric self-enforcement scheme with public traceability. In K. Kim, editor, *Public Key Cryptography*, volume 1992 of *Lecture Notes in Computer Science*, pages 225–239. Springer, 2001.
76. R. Kumar, S. Rajagopalan, and A. Sahai. Coding constructions for blacklisting problems without computational assumptions. In M. J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 609–623. Springer, 1999.
77. R. Kumar and A. Russell. A note on the set systems used for broadcast encryption. In *SODA*, pages 470–471, 2003.
78. K. Kurosawa and Y. Desmedt. Optimum traitor tracing and asymmetric schemes. In *EUROCRYPT*, pages 145–157, 1998.
79. K. Kurosawa and T. Yoshida. Linear code implies public-key traitor tracing. In D. Naccache and P. Paillier, editors, *Public Key Cryptography*, volume 2274 of *Lecture Notes in Computer Science*, pages 172–187. Springer, 2002.
80. M. Lee, D. Ma, and M. Seo. Breaking two k-resilient traitor tracing schemes with sublinear ciphertext size. In Abdalla et al. [2], pages 238–252.
81. T. Lindkvist. *Fingerprinting Digital Documents*. PhD thesis, Linkoping Studies in Science and Technology, 1999.
82. D. Liu, P. Ning, and K. Sun. Efficient self-healing group key distribution with revocation capability. In S. Jajodia, V. Atluri, and T. Jaeger, editors, *ACM Conference on Computer and Communications Security*, pages 231–240. ACM, 2003.

83. M. Luby and J. Staddon. Combinatorial bounds for broadcast encryption. In *EUROCRYPT*, pages 512–526, 1998.
84. T. Matsushita and H. Imai. A public-key black-box traitor tracing scheme with sublinear ciphertext size against self-defensive pirates. In P. J. Lee, editor, *ASIACRYPT*, volume 3329 of *Lecture Notes in Computer Science*, pages 260–275. Springer, 2004.
85. M. Mitzenmacher and E. Upfal. *Probability and Computing: randomized algorithms and probabilistic analysis*. Cambridge University Press, London, 2005.
86. D. Naccache, editor. *Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings*, volume 2020 of *Lecture Notes in Computer Science*. Springer, 2001.
87. D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In Kilian [72], pages 41–62.
88. D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. *Electronic Colloquium on Computational Complexity (ECCC)*, (043), 2002.
89. M. Naor and B. Pinkas. Threshold traitor tracing. In H. Krawczyk, editor, *CRYPTO*, volume 1462 of *Lecture Notes in Computer Science*, pages 502–517. Springer, 1998.
90. M. Naor and B. Pinkas. Efficient trace and revoke schemes. In Y. Frankel, editor, *Financial Cryptography*, volume 1962 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2000.
91. M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *STOC*, pages 427–437. ACM, 1990.
92. K. Nuida, M. Hagiwara, H. Watanabe, and H. Imai. Optimization of tardos's fingerprinting codes in a viewpoint of memory amount. In T. Furon, F. Cayre, G. J. Doërr, and P. Bas, editors, *Information Hiding*, volume 4567 of *Lecture Notes in Computer Science*, pages 279–293. Springer, 2007.
93. C. Peikert, A. Shelat, and A. Smith. Lower bounds for collusion-secure fingerprinting. In *SODA*, pages 472–479, 2003.
94. B. Pfitzmann. Trials of traced traitors. In R. J. Anderson, editor, *Information Hiding*, volume 1174 of *Lecture Notes in Computer Science*, pages 49–64. Springer, 1996.
95. B. Pfitzmann and M. Schunter. Asymmetric fingerprinting (extended abstract). In *EUROCRYPT*, pages 84–95, 1996.
96. B. Pfitzmann and M. Waidner. Asymmetric fingerprinting for larger collusions. In *ACM Conference on Computer and Communications Security*, pages 151–160, 1997.
97. Z. Ramzan and D. P. Woodruff. Fast algorithms for the free riders problem in broadcast encryption. In C. Dwork, editor, *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 308–325. Springer, 2006.
98. R. L. Rivest. All-or-nothing encryption and the package transform. In E. Biham, editor, *FSE*, volume 1267 of *Lecture Notes in Computer Science*, pages 210–218. Springer, 1997.
99. R. Safavi-Naini and Y. Wang. Sequential traitor tracing. In Bellare [8], pages 316–332.
100. R. Safavi-Naini and Y. Wang. New results on frame-proof codes and traceability schemes. *IEEE Transactions on Information Theory*, 47(7):3029–3033, 2001.

101. R. Safavi-Naini and Y. Wang. Traitor tracing for shortened and corrupted fingerprints. In Feigenbaum [41], pages 81–100.
102. R. Safavi-Naini and Y. Wang. Sequential traitor tracing. *IEEE Transactions on Information Theory*, 49(5):1319–1326, 2003.
103. R. Sakara and J. Furukawa. Identity-based broadcast encryption, 2007. Available at the IACR Crypto Archive http://eprint.iacr.org.
104. T. Sander, editor. *Security and Privacy in Digital Rights Management, ACM CCS-8 Workshop DRM 2001, Philadelphia, PA, USA, November 5, 2001, Revised Papers*, volume 2320 of *Lecture Notes in Computer Science*. Springer, 2002.
105. B. S. W. Schroder. *Ordered Sets: An Introduction*. Birkhauser, Boston, 2003.
106. A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pages 47–53, 1984.
107. A. T. Sherman and D. A. McGrew. Key establishment in large dynamic groups using one-way function trees. *IEEE Trans. Software Eng.*, 29(5):444–458, 2003.
108. V. Shoup. A proposal for an iso standard for public key encryption (version 1.1), 2001.
109. V. Shoup, editor. *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*. Springer, 2005.
110. A. Silverberg, J. Staddon, and J. L. Walker. Efficient traitor tracing algorithms using list decoding. In C. Boyd, editor, *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 175–192. Springer, 2001.
111. J. Staddon, D. R. Stinson, and R. Wei. Combinatorial properties of frameproof and traceability codes. *IEEE Transactions on Information Theory*, 47(3):1042–1049, 2001.
112. D. R. Stinson, editor. *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, volume 773 of *Lecture Notes in Computer Science*. Springer, 1994.
113. D. R. Stinson and R. Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM J. Discrete Math.*, 11(1):41–53, 1998.
114. D. R. Stinson and R. Wei. Key preassigned traceability schemes for broadcast encryption. In S. E. Tavares and H. Meijer, editors, *Selected Areas in Cryptography*, volume 1556 of *Lecture Notes in Computer Science*, pages 144–156. Springer, 1998.
115. G. Tardos. Optimal probabilistic fingerprint codes. In *STOC*, pages 116–125. ACM, 2003.
116. G. Tardos. Optimal probabilistic fingerprint codes. *J. ACM*, 55(2), 2008.
117. O. Telelis and V. Zissimopoulos. Absolute o(log m) error in approximating random set covering: an average case analysis. *Inf. Process. Lett.*, 94(4):171–177, 2005.
118. V. D. Tô and R. Safavi-Naini. Linear code implies public-key traitor tracing with revocation. In H. Wang, J. Pieprzyk, and V. Varadharajan, editors, *ACISP*, volume 3108 of *Lecture Notes in Computer Science*, pages 24–35. Springer, 2004.

119. D. Tonien and R. Safavi-Naini. An efficient single-key pirates tracing scheme using cover-free families. In J. Zhou, M. Yung, and F. Bao, editors, *ACNS*, volume 3989 of *Lecture Notes in Computer Science*, pages 82–97, 2006.
120. N. R. Wagner. Fingerprinting. In *IEEE Symposium on Security and Privacy*, pages 18–22, 1983.
121. D. M. Wallner, E. J. Harder, and R. C. Agee. Key management for multicast: issues and architectures, 1999. Internet Draft.
122. P. Wang, P. Ning, and D. S. Reeves. Storage-efficient stateless group key revocation. In K. Zhang and Y. Zheng, editors, *ISC*, volume 3225 of *Lecture Notes in Computer Science*, pages 25–38. Springer, 2004.
123. Y. Watanabe, G. Hanaoka, and H. Imai. Efficient asymmetric public-key traitor tracing without trusted agents. In Naccache [86], pages 392–407.
124. M. J. Wiener, editor. *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*. Springer, 1999.
125. C. K. Wong, M. G. Gouda, and S. S. Lam. Secure group communications using key graphs. In *SIGCOMM*, pages 68–79, 1998.
126. Y. Yacobi. Improved boneh-shaw content fingerprinting. In Naccache [86], pages 378–391.

Index