References

[1] Mihir Bellare, Oded Goldreich, and Shafi Goldwasser. Incremental cryptography: The case of hashing and signing. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 216–233. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[2] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of cipher block chaining. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 341–358. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[3] Th. Beth, D.E. Lazic, and A. Mathias. Cryptanalysis of cryptosystems based on remote chaos replication. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 318–331. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[4] Ingrid Biehl, Johannes Buchmann, and Christoph Thiel. Cryptographic protocols based on discrete logarithms in real-quadratic orders. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 56–60. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[5] Jürgen Bierbrauer, K. Gopalakrishnan, and D.R. Stinson. Bounds for resilient functions and orthogonal arrays. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 247–256. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[6] Daniel Bleichenbacher and Ueli M. Maurer. Directed acyclic graphs, one-way functions and digital signatures. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 75–82. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[7] Carlo Blundo, Alfredo De Santis, Giovanni Di Crescenzo, Antonio Giorgio Gaggia, and Ugo Vaccaro. Multi-secret sharing schemes. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 150–163. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[8] Mike Burmester. On the risk of opening distributed keys. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 308–317. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[9] Ran Canetti and Amir Herzberg. Maintaining security in the presence of transient faults. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 425–438. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[10] Jinhui Chao, Kazuo Tanada, and Shigeo Tsujii. Design of elliptic curves with controllable lower boundary of extension degree for reduction attacks. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 50–55. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[11] Benny Chor, Amos Fiat, and Moni Naor. Tracing traitors. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Confer-*

ence on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994), volume 839 of *LNCS*, pages 257–270. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[12] Don Coppersmith. Attack on the cryptographic scheme niks-tas. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 294–307. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[13] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 174–187. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[14] Don Davis, Ross Ihaka, and Philip Fenstermacher. Cryptographic randomness from air turbulence in disk drives. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 114–120. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[15] Olivier Delos and Jean-Jacques Quisquater. An identity-based signature scheme with bounded life-span. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 83–94. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[16] Cynthia Dwork and Moni Naor. An efficient existentially unforgeable signature scheme and its applications. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, Au-*

gust 21-25, 1994), volume 839 of *LNCS*, pages 234–246. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[17] Christian Gehrmann. Cryptanalysis of the gemmell and naor multiround authentication protocol. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 121–128. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[18] Henri Gilbert and Pascal Chauvaud. A chosen plaintext attack of the 16-round khufu cryptosystem. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 359–368. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[19] Marc Girault and Jacques Stern. On the length of cryptographic hash-values used in identification schemes. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 202–215. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[20] Tamás Horváth, Spyros S. Magliveras, and Tran van Trung. A parallel permutation multiplier for a pgm crypto-chip. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 108–113. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[21] Toshiya Itoh, Yuji Ohta, and Hiroki Shizuya. Language dependent secure bit commitment. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 188–201. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[22] Jr. Kaliski, Burton S. and M.J.B. Robshaw. Linear cryptanalysis using multiple approximations. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 26–39. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[23] Hugo Krawczyk. Lfsr-based hashing and authentication. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 129–139. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[24] Kaoru Kurosawa. New bound on authentication code with arbitration. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 140–149. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[25] Eyal Kushilevitz and Adi Rosén. A randomness-rounds tradeoff in private computation. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 397–410. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[26] Susan K. Langford and Martin E. Hellman. Differential-linear cryptanalysis. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 17–25. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[27] Chae Hoon Lim and Pil Joong Lee. More flexible exponentiation with precomputation. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*,

pages 95–107. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[28] James L. Massey and Shirlei Serconek. A fourier transform approach to the linear complexity of nonlinearly filtered sequences. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 332–340. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[29] Mitsuru Matsui. The first experimental cryptanalysis of the data encryption standard. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 1–11. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[30] Ueli M. Maurer. Towards the equivalence of breaking the diffie-hellman protocol and computing discrete logarithms. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 271–281. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[31] Preda Mihailescu. Fast generation of provable primes using search in arithmetic progressions. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 282–293. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[32] Kazuo Ohta and Kazumaro Aoki. Linearcryptanalysis of the fast data encipherment algorithm. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 12–16. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[33] Tatsuaki Okamoto. Designated confirmer signatures and public-key encryption are equivalent. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 61–74. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[34] Kazue Sako and Joe Kilian. Secure voting using partially compatible homomorphisms. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 411–424. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[35] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Pitfalls in designing substitution boxes. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 383–396. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[36] Jacques Stern. Designing identification schemes with keys of short size. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 164–173. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[37] Jean-Pierre Tillich and Gilles Zémor. Hashing with sl_2. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Barbara, California, August 21-25, 1994)*, volume 839 of *LNCS*, pages 40–49. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[38] Yukiyasu Tsunoo, Eiji Okamoto, and Tomohiko Uyematsu. Ciphertext only attack for one-way function of the map using one ciphertext. In Yvo G. Desmedt, editor, *Proceedings of the 14th Annual International Conference on Advances in Cryptology, CRYPTO'94 (Santa Bar-*

bara, California, August 21-25, 1994), volume 839 of *LNCS*, pages 369–382. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.