

Curriculum Vitae

Yvo Desmedt

1 Personal Details

Name: Yvo Desmedt
Present appointment: Chair of Information Communication Technology
Computer Science, University College London, UK
Date of appointment: August 2004

2 Education

Dates	Detail of degree; diploma; other qualification	Institution
1979	Masters in Electrical Engineering (cum Laude)	Katholieke Universiteit Leuven (Belgium)
1984	PhD in Applied Science (Summa cum Laude)	Katholieke Universiteit Leuven (Belgium)

3 Professional History (in chronological order)

Dates	Detail of position held	Institution
August 1979–November 1980	Research Assistant, Electrical Engineering Dept.	Katholieke Universiteit Leuven, Belgium
December 1983–December 1984	Research Assistant, Electrical Engineering Dept.	Katholieke Universiteit Leuven, Belgium
January 1985–May 1985	Visiting Assistant Professor, Computer Science	University of New Mexico, U.S.A.
June 1985–September 1985	Research Assistant, Electrical Engineering Dept.	Katholieke Universiteit Leuven, Belgium
October 1985–August 1986	Post-doctoral NFWO (National Science Foundation Belgium) researcher	Katholieke Universiteit Leuven, Belgium
September 1986–May 1987	Visiting Professor, Dépt. I.R.O.	Université de Montréal, Canada
June 1987–August 1987	Assistant Professor, Dépt. I.R.O.	Université de Montréal, Canada
September 1987–August 1991	Assistant Professor, Electrical Engineering and Computer Science	University of Wisconsin — Milwaukee, U.S.A.
September 1991–August 1995	Associate Professor, Electrical Engineering and Computer Science	University of Wisconsin — Milwaukee, U.S.A.

PROFESSIONAL HISTORY

September 1995–August 1999	Professor, Department of Electrical Engineering and Computer Science	University of Wisconsin — Milwaukee, U.S.A.
August 1999–August 2004	Professor, Department of Computer Science	Florida State University, U.S.A.
August 2004–August 2009	BT-Chair of Information Security	University College London, U.K.

4 Other Appointments and Affiliations

Dates	Detail of position held	Institution
June 1989–July 1989	Visiting Professor, Fakultät für Informatik	University of Karlsruhe, West-Germany
July 1991–September 1991	Visiting Fellow, Department of Computer Science	University of New South Wales, ADFA, Canberra, Australia
October 1993–January 1994	Visiting Associate Professor, Computer Science Department	Technion, Israel
February 1994–April 1994	Sabbatical at the Dept. of Combinatorics and Optimization	University of Waterloo, Canada
May 1994–July 1994	Sabbatical at the Dipartimento di Informatica ed Applicazioni	Università di Salerno, Italy
August 1996–July 1997	Founding Director of the Center for Cryptography, Computer and Network Security, College of Engineering and Applied Science	University of Wisconsin — Milwaukee, U.S.A.
June 1997–July 1997	Professorial Fellow, Department of Computer Science	University of Wollongong, New South Wales, Australia
December 1999	Visiting Professor	Tokyo Institute of Technology, Japan
August 1999–August 2000	Adjunct Professor, Department of Electrical Engineering and Computer Science	University of Wisconsin — Milwaukee, U.S.A.
June–July 2002	Visiting Professor, Department of Electrical Engineering	Université Catholique de Louvain, Belgium
November 2003–January 2004	JSPS Fellow	Ibaraki University, Japan
August 1997–July 2004	Visiting Professor of Information Security, Department of Mathematics	Royal Holloway, U.K.
January 2000–June 2004	Director of the Laboratory of Security and Assurance in Information Technology, NSA Center of Excellence	Florida State University, U.S.A.
March–April 2005	Visiting Professor in Computing	Macquarie University, Australia
June–August 2005	QUT Visiting Fellow	Queensland University of Technology, Australia
November 2008–January 2009 since August 2004	JSPS Fellow Courtesy Professor, Department of Computer Science	Ibaraki University, Japan Florida State University, U.S.A.

OTHER APPOINTMENTS AND AFFILIATIONS

November 2009–October 2010 Invited Senior Research Scientist

Research Center for Information Security, AIST, Japan

5 Prizes, Awards and other Honours:

Dates	Detail of prize, award or honour	Electing body
1983	100 Year Bell Telephone Belgium Prize	
1985	IBM Belgium Prize for best PhD in Computer Science	NFWO, Belgium
1985	S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunication) Prize	
1992	Graduate School/University of Wisconsin — Milwaukee Foundation Research Award	Graduate School
2000	Center of Excellence in Information Security Education at Florida State University	NSA
2010	International Association of Cryptologic Research Fellow	IACR Fellows Committee

6 Grants

- [1] Grant for research in cryptography December 1980–November 1983, received from IWONL, Belgium (Institute for Scientific Research for the Industry and Agriculture), \$60,000 (net).
- [2] Post-doctoral grant for research in cryptography October 1985–August 1986, received from NFWO (National Foundation for Scientific Research), Belgium, \$40,000.
- [3] National Science Foundation: Networking and Communications Research: NCR-9004879: “Covert-Free and Subliminal-Free Channels” \$140,391, August 1, 1990 – January 31, 1994. No co-investigators.
- [4] National Science Foundation: Networking and Communications Research: NCR-9106327: “Multi-Sender and Multi-Receiver Network Security” \$118,140, September 1, 1991 – August 31, 1994 No co-investigators.
- [5] National Science Foundation: INT-9123464: “U.S.–U.K. Cooperative Research: Multi-User Network Security and Subliminal-Free Channels” July 1, 1992– December 31, 1994: \$10,000. European co-investigators: Mike Burmester and Fred Piper, Department of Mathematics, Royal Holloway, University of London.
- [6] Visiting Fellowship Research grant to visit Prof. Piper (Royal Holloway, University of London, Great Britain) May 1995–July 1995, received from Science and Engineering Research Council, \$5,440.
- [7] National Science Foundation: Networking and Communications Research: NCR-9508528: “Multi-Sender and Multi-Receiver Network Security” \$275,240, September 1, 1995 – August 31, 1999. No co-investigators.
- [8] Defense Advanced Research Program Agency: F30602-97-1-0205: “Critical Analysis of the Use of Redundancy to Achieve Survivability in the Presence of Malicious Attacks” \$217,122, April 14, 1997 – May 23, 1999. No co-investigators.
- [9] National Science Foundation: Networking and Communications Research: NCR-9729238: “Connection to the vBNS for the University of Wisconsin-Milwaukee” \$407,600, March 1, 1998 – February 29, 2000 Co-investigator: Jim Lowe.
- [10] National Science Foundation: Computer-Communications Research: CCR-9903216: “Information Hiding, Tracing and Watermarking” \$164,997, September 1, 1999 – August 31, 2003. No co-investigators.
- [11] National Science Foundation: Communications Research: CCR-0109425: “Cryptanalytic study of the AES finalist and its variants” \$49,974, April 1, 2001 – March 31, 2003. No co-investigators.

GRANTS

- [12] National Science Foundation: Networking Research: ANI-0087641: “Anonymity” \$299,930, September 1, 2001 – August 31, 2006. No co-investigators.
- [13] National Science Foundation: Trusted Computing: CCR-0209092: “Models for Trusted Systems” \$149,899, August 1, 2002 – July 31, 2005. Co-investigator: Mike Burmester.
- [14] National Security Agency: MDA 904-02-1-0217: “Scholarships for Security and Assurance in Information Technology at FSU” \$379,414, August 16, 2002 – August 15, 2003. Principal Investigator: Mike Burmester and Co-investigator: Alec Yasinsac.
- [15] National Science Foundation: Networking Research: DUE-0243117: “Cyber Training and Education at Florida State University” \$1,150,787 and a supplement of \$85,828, January 1, 2003 – December 31, 2006. Co-investigators: Alec Yasinsac and Mike Burmester.
- [16] National Security Agency: MDA 904-03-1-0205: “Scholarships for Security and Assurance in Information Technology at FSU” \$264,814 August 23, 2003 – August 24, 2004. Principal Investigator: Mike Burmester and Co-investigator: Alec Yasinsac.
- [17] Japan Society for the Promotion of Science (JSPS) fellow, nominated by the National Science Foundation, Japan Program, \$16,883, November 22, 2003 – January 6, 2004, Host: Kaoru Kurosawa.
- [18] EPSRC: EP/C538285/1, BT Professor in Information Security, £500,000, matched by British Telecommunications (£500,000) August 9, 2004 – August 8, 2009.
- [19] ARC DP0665035: AUS\$ 390,000, “Secure Multi-Party Computation”, jointly with Dr. H. Wang, Prof. J. R. Seberry, Assoc. Prof. C. Xing, 2006–2008.
- [20] EPSRC 06000399: Industrial Case, co-funded by BT-1080050886, “Modelling & Simulation of Security Properties of Large Scale Networks”, 2007-2010.
- [21] 2007CB807902: “Cryptography”, Ministry of Science and Technology of China, jointly with Prof. X. Wang and Prof. A. Yao, 2007-2009.
- [22] Japan Society for the Promotion of Science (JSPS) fellow, November 13, 2008 – January 10, 2009, Host: Kaoru Kurosawa.
- [23] 2007CB807901: “Cryptography”, Ministry of Science and Technology of China, jointly with Prof. A. Yao and Prof. X. Wang, 2009-2011.

In preparation

Secure Internet Voting, EPSRC, 36 months, to be submitted.

7 Academic supervision

Date	Details
1988–1989	MSc. advisor of Y. Frankel
Spring 1989	Independent study advisor of: Y. Frankel, B. Quandt
Fall 1989	Independent study advisor of: K. Sechtig
Fall 1989–Fall 1992	PhD advisor of Y. Frankel
1993–1994	MSc. advisor of K. McMillan
Spring 1995–Spring 1997	MSc. advisor of V. Vaidhyanathan
Fall 1997–Spring 1998	MSc. advisor of S. Hou
Fall 1997–Fall 1998	Postdoctoral advisor of Dr. Y. Wang

ACADEMIC SUPERVISION

Fall 1997–Spring 2000	PhD advisor of B. King
Spring 1998–Summer 1999	MSc. advisor of T. V. Le
Fall 1998–Spring 2000	MSc. advisor of R. B. Harrison
Fall 1999–Spring 2004	PhD advisor of T. V. Le
Fall 2000–Fall 2002	MSc. advisor of T. Hlavka
Fall 2000–Spring 2003	MSc. advisor of M. Patel
Spring 2001	Master project advisor of M. Khatib
Spring 2001–Spring 2003	MSc. advisor of R. Punyayutthakarn
Fall 2001–Spring 2006	PhD advisor of G. Jakimoski
Fall 2002–Spring 2004	Master project advisor of V. Adityan
2005–2006	MSc. advisor of A. Alfaraj, M. Issa; Post-doctoral advisor of H. Phan
2006–2007	MSc. advisor of A. Bitsios, M. A. Khan, C. Scordellis, A. Tillirides, Q. Yang
2007–2008	Phd Advisor of S. Erotokritou, J. McLaughlin, Q. Yang,
2008–2009	PhD Advisor of S. Erotokritou, S. Mahmood, Q. Yang; MSc advisor of S. Estehghari; Post-doctoral advisor of Y. Lu
2009–2010	PhD Advisor of S. Erotokritou, S. Mahmood and Q. Yang; MSc advisor of J. Cheney; Post-doctoral advisor of Y. Lu
current	PhD Advisor of S. Erotokritou, S. Mahmood and Q. Yang; Post-doctoral advisor of Y. Lu

8 Research

Citations: 5433 (Google Scholar).

8.1 Selected Publications

- [1] M. Davio, Y. Desmedt, M. Fosseprez, R. Govaerts, J. Hulsbosch, P. Neutjens, P. Piret, J.-J. Quisquater, J. Vandewalle, and P. Wouters. Analytical characteristics of the DES. In D. Chaum, editor, *Advances in Cryptology. Proc. Crypto 83*, pp. 171–202. Plenum Press, 1984. Santa Barbara, California, U.S.A., August 22–24. (Cited: Google Scholar: 42)
- [2] Y. Desmedt, J. Vandewalle, and R. Govaerts. A critical analysis of the security of knapsack public key algorithms. *IEEE Transaction on Information Theory*, IT-30(4), pp. 601–611, July 1984. (Cited: ISI: 7, Google Scholar: 28)
- [3] M. Davio, Y. Desmedt, J. Goubert, F. Hoornaert, and J.-J. Quisquater. Efficient hardware and software implementations for the DES. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology. Proc. of Crypto 84 (Lecture Notes in Computer Science 196)*, pp. 144–146. Springer-Verlag, 1985. Santa Barbara, California, U.S.A., August 19–22. (Cited: Google Scholar: 25)
- [4] Y. Desmedt, J.-J. Quisquater, and M. Davio. Dependence of output on input in DES : Small avalanche characteristics. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology. Proc. of Crypto 84 (Lecture Notes in Computer Science 196)*, pp. 359–376. Springer-Verlag, 1985. (Google Scholar:24)

- [5] P. Delsarte, Y. Desmedt, A. Odlyzko, and P. Piret. Fast cryptanalysis of the Matsumoto-Imai public key scheme. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology. Proc. of Eurocrypt 84 (Lecture Notes in Computer Science 209)*, pp. 142–149. Springer-Verlag, Berlin, 1985. (Cited: ISI: 10, Google Scholar: 10)
- [6] Y. Desmedt and A. Odlyzko. A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes. In Hugh C. Williams, editor, *Advances in Cryptology: Crypto '85, Proceedings (Lecture Notes in Computer Science 218)*, pp. 516–522. Springer-Verlag, 1986. (Cited: ISI: 4, Google Scholar: 48)
- [7] Y. Desmedt. What happened with knapsack cryptographic schemes. In J. K. Skwirzynski, editor, *Performance Limits in Communication, Theory and Practice, NATO ASI Series E: Applied Sciences — Vol. 142*, pp. 113–134. Kluwer Academic Publishers, 1988. Proceedings of the NATO Advanced Study Institute Il Ciocco, Castelvechchio Pascoli, Tuscany, Italy, July 7–19, 1986. (Cited: Google Scholar: 26)
- [8] Y. Desmedt and J.-J. Quisquater. Public key systems based on the difficulty of tampering (Is there a difference between DES and RSA?). In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto '86 (Lecture Notes in Computer Science 263)*, pp. 111–117. Springer-Verlag, 1987. (Cited: ISI: 9, Google Scholar: 57)
- [9] Y. Desmedt, C. Goutier, and S. Bengio. Special uses and abuses of the Fiat-Shamir passport protocol. In C. Pomerance, editor, *Advances in Cryptology, Proc. of Crypto '87 (Lecture Notes in Computer Science 293)*, pp. 21–39. Springer-Verlag, 1988. (Cited: ISI: 31, Google Scholar: 107)
- [10] Y. Desmedt. Society and group oriented cryptography : a new concept. In C. Pomerance, editor, *Advances in Cryptology, Proc. of Crypto '87 (Lecture Notes in Computer Science 293)*, pp. 120–127. Springer-Verlag, 1988. (Cited: ISI: 65, Google Scholar: 311)
- [11] Y. Desmedt. Subliminal-free authentication and signature. In C. G. Günther, editor, *Advances in Cryptology, Proc. of Eurocrypt '88 (Lecture Notes in Computer Science 330)*, pp. 23–33. Springer-Verlag, May 1988. Davos, Switzerland. (Cited: ISI: 11, Google Scholar: 36)
- [12] G. Davida and Y. Desmedt. Passports and visas versus IDs. In C. G. Günther, editor, *Advances in Cryptology, Proc. of Eurocrypt '88 (Lecture Notes in Computer Science 330)*, pp. 183–188. Springer-Verlag, May 1988. Davos, Switzerland. (Cited: ISI: 2, Google Scholar: 7)
- [13] Y. Desmedt. Abuses in cryptography and how to fight them. In S. Goldwasser, editor, *Advances in Cryptology — Crypto '88, Proceedings (Lecture Notes in Computer Science 403)*, pp. 375–389. Springer-Verlag, 1990. (Cited: ISI: 8, Google Scholar: 44)
- [14] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In G. Brassard, editor, *Advances in Cryptology — Crypto '89, Proceedings (Lecture Notes in Computer Science 435)*, pp. 307–315. Springer-Verlag, 1990. (Cited: ISI: 158, Google Scholar: 822)
- [15] Y. Desmedt and M. Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks. In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology — Crypto '90, Proceedings (Lecture Notes in Computer Science 537)*, pp. 177–188. Springer-Verlag, 1991. (Cited: ISI: 6, Google Scholar: 28)
- [16] M. V. D. Burmester and Y. Desmedt. All languages in NP have divertible zero-knowledge proofs and arguments under cryptographic assumptions. In I. Damgård, editor, *Advances in Cryptology, Proc. of Eurocrypt '90 (Lecture Notes in Computer Science 473)*, pp. 1–10. Springer-Verlag, 1991. Århus, Denmark, May 21–24 (**51% acceptance rate**). (Cited: ISI: 2, Google Scholar: 18)
- [17] T. Beth and Y. Desmedt. Identification tokens — or: Solving the chess grandmaster problem. In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology — Crypto '90, Proceedings (Lecture Notes in Computer Science 537)*, pp. 169–176. Springer-Verlag, 1991. (Cited: ISI: 15, Google Scholar: 54)
- [18] S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier, and J.-J. Quisquater. Secure implementations of identification systems. *Journal of Cryptology*, 4(3), pp. 175–183, 1991. (Cited: Google Scholar: 53)

- [19] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In J. Feigenbaum, editor, *Advances in Cryptology — Crypto '91, Proceedings (Lecture Notes in Computer Science 576)*, pp. 457–469. Springer-Verlag, 1992. (Cited: ISI: 65, Google Scholar: 385)
- [20] Y. Desmedt and M. Yung. Weaknesses of undeniable signature schemes. In D. W. Davies, editor, *Advances in Cryptology, Proc. of Eurocrypt '91 (Lecture Notes in Computer Science 547)*, pp. 205–220. Springer-Verlag, April 1991. Brighton, U.K. (Cited: ISI: 12, Google Scholar: 59)
- [21] Y. Frankel and Y. Desmedt. Parallel reliable threshold multisignature. Tech. Report TR-92-04-02, Dept. of EE & CS, Univ. of Wisconsin — Milwaukee, April 1992. ftp://ftp.cs.uwm.edu/pub/tech_reports/desmedt-rsa-threshold_92.ps. (Cited: ISI: 1, Google Scholar: 73)
- [22] Y. Desmedt, Y. Frankel, and M. Yung. Multi-receiver / multi-sender network security: efficient authenticated multicast/ feedback. In *IEEE INFOCOM '92, Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies*, pp. 2045–2054, Florence, Italy, May 4–8, 1992. (Cited: ISI: 23, Google Scholar: 97)
- [23] Y. Desmedt and M. Burmester. Towards practical ‘proven secure’ authenticated key distribution. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 228–231, November 3–5, 1993. Fairfax, Virginia, U.S.A. (**37% acceptance rate**). (Cited: Google Scholar: 18)
- [24] A. De Santis, Y. Desmedt, Y. Frankel, and M. Yung. How to share a function securely. In *Proceedings of the twenty-sixth annual ACM Symp. Theory of Computing (STOC)*, pp. 522–533, May 23–25, 1994. (Cited: Google Scholar: 249)
- [25] M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. In A. De Santis, editor, *Advances in Cryptology — Eurocrypt '94, Proceedings (Lecture Notes in Computer Science 950)*, pp. 275–286. Springer-Verlag, 1995. (Cited: ISI: 44, Google Scholar: 617)
- [26] Y. G. Desmedt. Threshold cryptography. *European Trans. on Telecommunications*, 5(4), pp. 449–457, July–August 1994. **Invited paper**. (Cited: ISI: 85, Google Scholar: 296)
- [27] Y. Desmedt, G. Di Crescenzo, and M. Burmester. Multiplicative non-abelian sharing schemes and their application to threshold cryptography. In J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology — Asiacrypt '94, Proceedings (Lecture Notes in Computer Science 917)*, pp. 21–32. Springer-Verlag, 1995. (Cited: ISI: 15, Google Scholar: 34)
- [28] Y. G. Desmedt and Y. Frankel. Homomorphic zero-knowledge threshold schemes over any finite abelian group. *SIAM Journal on Discrete Mathematics*, 7(4), pp. 667–679, November 1994. (Cited: ISI: 37, Google Scholar: 73)
- [29] Y. Desmedt. Securing traceability of ciphertexts — towards a secure software key escrow system. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology — Eurocrypt '95, Proceedings (Lecture Notes in Computer Science 921)*, pp. 147–157. Springer-Verlag, 1995. (Cited: ISI: 14, Google Scholar: 36)
- [30] S. R. Blackburn, M. Burmester, Y. Desmedt, and P. R. Wild. Efficient multiplicative sharing schemes. In U. Maurer, editor, *Advances in Cryptology — Eurocrypt '96, Proceedings (Lecture Notes in Computer Science 1070)*, pp. 107–118. Springer-Verlag, 1996. Zaragoza, Spain, May 12–16 (**27% acceptance rate**). (Cited: ISI: 28, Google Scholar: 38)
- [31] M. Burmester and Y. Desmedt. Efficient and secure conference key distribution. In M. Lomas, editor, *Security Protocols (Lecture Notes in Computer Science 1189)*, pp. 119–130. Springer-Verlag, 1997. (Cited: ISI: 2, Google Scholar: 78)
- [32] M. Burmester, Y. G. Desmedt, T. Itoh, K. Sakurai, H. Shizuya, and M. Yung. A progress report on subliminal-free channels. In R. Anderson, editor, *Information Hiding, First International Workshop, Proceedings (Lecture Notes in Computer Science 1174)*, pp. 159–168. Springer-Verlag, 1996. Cambridge, U.K., May 30–June 1. (Cited: Google Scholar: 18)

- [33] Y. Desmedt. Simmons' protocol is not free of subliminal channels. In *Proceedings: 9th IEEE Computer Security Foundations Workshop*, pp. 170–175, Kenmare, Ireland, June 10–12, 1996. (Cited: ISI: 6, Google Scholar: 17)
- [34] Y. Desmedt and S. Jajodia. Redistributing secret shares to new access structures and its applications. Tech. Report ISSE-TR-97-01, George Mason University, July 1997. ftp://isse.gmu.edu/pub/techrep/97_01_jajodia.ps.gz. (Cited: ISI: 7, Google Scholar: 121)
- [35] M. V. D. Burmester, Y. G. Desmedt, F. Piper, and M. Walker. A general zero-knowledge scheme. *Designs, Codes and Cryptography*, 12(1), pp. 13–37, September 1997. (Cited: Google Scholar: 17)
- [36] Y. Desmedt. Some recent research aspects of threshold cryptography. In E. Okamoto, G. Davida, and M. Mambo, editors, *Information Security, Proceedings (Lecture Notes in Computer Science 1396)*, pp. 158–173. Springer-Verlag, 1997. Invited lecture, September 17–19, 1997, Tatsunokuchi, Ishikawa, Japan, Springer-Verlag. (Cited: Google Scholar: 120)
- [37] K. Kurosawa and Y. Desmedt. Optimum traitor tracing and asymmetric schemes. In K. Nyberg, editor, *Advances in Cryptology — Eurocrypt '98, Proceedings (Lecture Notes in Computer Science 1403)*, pp. 145–157. Springer-Verlag, 1998. (Cited: ISI: 58, Google Scholar: 161)
- [38] K. Kurosawa, T. Yoshida, Y. Desmedt, and M. Burmester. Some bounds and a construction for secure broadcast encryption. In K. Ohta and D. Pei, editors, *Advances in Cryptology — Asiacrypt '98, Proceedings (Lecture Notes in Computer Science 1514)*, pp. 420–433. Springer-Verlag, October, 18–22 1998. Beijing, China (**27% acceptance rate**). (Cited: ISI: 15, Google Scholar: 19)
- [39] M. Burmester, Y. Desmedt, and J. Seberry. Equitable key escrow with limited time span. In K. Ohta and D. Pei, editors, *Advances in Cryptology — Asiacrypt '98, Proceedings (Lecture Notes in Computer Science 1514)*, pp. 380–391. Springer-Verlag, October, 18–22 1998. (Cited: ISI: 11, Google Scholar: 28)
- [40] M. Burmester and Y. Desmedt. Secure communication in an unknown network using certificates. In K. Y. Lam, E. Okamoto, and C. Xing, editors, *Advances in Cryptology — Asiacrypt '99, Proceedings (Lecture Notes in Computer Science 1716)*, pp. 274–287. Springer-Verlag, November, 14–18 1999. Singapore (**32% acceptance rate**). (Cited: ISI: 14, Google Scholar: 25)
- [41] M. Burmester, Y. Desmedt, H. Doi, M. Mambo, E. Okamoto, M. Tada, and Y. Yoshifuji. A structured ElGamal-type multisignature scheme. In H. Imai and Y. Zheng, editors, *Public Key Cryptography*, volume 1751 of *Lecture Notes in Computer Science*, pp. 466–483. Springer, 2000. (Cited: ISI: 18, Google Scholar: 51)
- [42] A. Beimel, M. Burmester, Y. Desmedt, and E. Kushilevitz. Computing functions of a shared secret. *SIAM Journal on Discrete Mathematics*, 13(3), pp. 324–345, 2000. (Cited: ISI: 2, Google Scholar: 9)
- [43] Y. Desmedt and K. Kurosawa. How to break a practical MIX and design a new one. In B. Preneel, editor, *Advances in Cryptology — Eurocrypt 2000, Proceedings (Lecture Notes in Computer Science 1807)*, pp. 557–572. Springer-Verlag, 2000. (Cited: ISI: 30, Google Scholar: 100)
- [44] Y. Wang and Y. Desmedt. Secure communication in broadcast channels. *Journal of Cryptology*, 14(2), pp. 121–135, 2001. (Cited: ISI: 15, Google Scholar: 33)
- [45] Y. Desmedt, R. Safavi-Naini, H. Wang, L. Batten, C. Charnes, and J. Pieprzyk. Broadcast anti-jamming systems. *Computer Networks*, 35(2–3), pp. 223–236, February 2001. (Cited: ISI: 6, Google Scholar: 25)
- [46] Y. Desmedt and Y. Wang. Perfectly secure message transmission revisited. In L. Knudsen, editor, *Advances in Cryptology — Eurocrypt 2002, Proceedings (Lecture Notes in Computer Science 2332)*, pp. 502–517. Springer-Verlag, 2002. (Cited: ISI: 31, Google Scholar: 79)
- [47] G. Jakimoski and Y. Desmedt. Related-key differential cryptanalysis of 192-bit key AES variants. In M. Matsui and R. J. Zuccherato, editors, *Selected Areas in Cryptography*, volume 3006 of *Lecture Notes in Computer Science*, pp. 208–221. Springer, 2004. 10th Annual International Workshop, SAC 2003, August 14–15, 2003, Ottawa, Ontario, Canada. (Cited: ISI: 28, Google Scholar: 53)

RESEARCH

- [48] M. Burmester, Y. Desmedt, R. Wright, and A. Yasinsac. Accountable privacy. In B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, editors, *Security Protocols Workshop, 12th International Workshop, 2004 (Lecture Notes in Computer Science, 3957)*, pp. 83–95. Springer-Verlag, 2006. Cambridge, United Kingdom April 26–28. (Cited: ISI: 2, Google Scholar: 14)
- [49] K. Kurosawa and Y. Desmedt. A new paradigm of hybrid encryption scheme. In M. Franklin, editor, *Advances in Cryptology — Crypto 2004, Proceedings (Lecture Notes in Computer Science 3152)*, pp. 426–442. Springer-Verlag, 2004. (Cited: ISI: 67, Google Scholar: 150)
- [50] M. Burmester and Y. G. Desmedt. Is hierarchical public-key certification the next target for hackers? *Communications of the ACM*, 47(8), pp. 68–74, August 2004. (Cited: ISI: 7, Google Scholar: 30)
- [51] M. Burmester and Y. Desmedt. A secure and scalable group key exchange system. *Information Processing Letters*, 94(3), pp. 137–143, May 2005. (Cited: ISI: 27, Google Scholar: 51)
- [52] Y. Desmedt, Y. Wang, and M. Burmester. A complete characterization of tolerable adversary structures for secure point-to-point transmissions without feedback. In X. Deng and D. Du, editors, *Algorithms and Computation, 16th Annual International Conference, ISAAC 2005, (Lecture Notes in Computer Science 3827)*, pp. 277–287, 2005. December 19 - 21, 2005, Sanya, Hainan, China (**20% acceptance**). (Cited: ISI: 5, Google Scholar: 16)
- [53] Y. Desmedt, J. Pieprzyk, R. Steinfeld, and H. Wang. A non-malleable group key exchange protocol robust against active insiders. In S. K. Katsikas, J. Lopez, M. Backes, S. Gritzalis, and B. Preneel, editors, *Information Security Conference, ISC 2006 (Lecture Notes in Computer Science 4176)*, pp. 459–475, August 30 - September 2, 2006. Samos Island, Greece. (Cited: ISI: 11, Google Scholar: 17)
- [54] Y. Wang and Y. Desmedt. Perfectly secure message transmission revisited. *IEEE Transactions on Information Theory*, 54(6), pp. 2582–2595, 2008. (Cited: ISI: 3, Google Scholar: 18)

Other Publications (no overlap)

8.2 Books and proceedings

- [55] Y. Desmedt. Instelbare scramblers. Master’s thesis, Katholieke Universiteit Leuven, Belgium, July 1979. In Dutch.
- [56] Y. Desmedt. *Analysis of the Security and New Algorithms for Modern Industrial Cryptography*. PhD thesis, K.U. Leuven, Leuven, Belgium, October 1984.
- [57] Y. G. Desmedt, editor. *Advances in Cryptology — Crypto ’94, Proceedings (Lecture Notes in Computer Science 839)*, New York, August 1994. Springer-Verlag.
- [58] Y. G. Desmedt, editor. *Public Key Cryptography — PKC 2003, 6th International Workshop on Practice and Theory in Public Key Cryptography, Proceedings (Lecture Notes in Computer Science 2567)*, New York, January 2003. Springer-Verlag.
- [59] Y. G. Desmedt, H. Wang, Y. Mu, and Y. Li, editors. *Cryptology and Network Security, 4th International Conference, CANS 2005, Xiamen, China, December 14–16, 2005 Proceedings*, volume 3810 of *Lecture Notes in Computer Science*, New York, 2005. Springer-Verlag.
- [60] Y. Desmedt, editor. *Information Theoretic Security, Second International Conference, ICITS 2007, (Lecture Notes in Computer Science 4883)*, New York, 2009. Springer-Verlag.

8.3 In books

- [61] G. I. Davida and Y. Desmedt. Cryptography based data security. In M. C. Yovits, editor, *Advances in Computers*, pp. 171–222. Academic Press, 1990. Volume 30.
- [62] G. I. Davida, Y. G. Desmedt, and B. J. Matt. Defending systems against viruses through cryptographic authentication. In L. J. Hoffman, editor, *Rogue Programs: Viruses, Worms and Trojan Horses*, pp. 261–272. Van Nostrand Reinhold, New York, 1990.
- [63] Y. Desmedt. *Breaking One Million DES keys*, chapter 9. O’Reilly, Sebastol, California, 1998.

8.4 Journal publications

- [64] Y. Desmedt, J. Vandewalle, and R. Govaerts. Cryptografie : Een veiligheidsaspect in de informatie. *Computer Org. Inform., (Belgium)*, pp. 17–19, June 1982. In Dutch.
- [65] Y. Desmedt, J. Vandewalle, and R. Govaerts. How iterative transformations can help to crack the Merkle-Hellman cryptographic scheme. *Electronics Letters*, 18(21), pp. 910–911, October 14, 1982.
- [66] Y. Desmedt, J. Vandewalle, and R. Govaerts. Industriële cryptografie : Noodzakelijke bescherming van informatie tegen misbruik en vervalsing. *Het Ingenieursblad (KVIV, Belgium)*, 32(1), pp. 17–23, January 1983. In Dutch.
- [67] Y. Desmedt, J. Vandewalle, and R. Govaerts. Linear algebra and extended mappings generalize public key cryptographic knapsack algorithms. *Electronics Letters*, 19(10), pp. 379–381, May 12, 1983.
- [68] R. Govaerts, J. Vandewalle, and Y. Desmedt. Industriële cryptografie. *Technivisie (Belgium)*, 1(15), pp. 10–12, November 2, 1983. In Dutch.
- [69] R. Govaerts, J. Vandewalle, and Y. Desmedt. Computerfraude en informatiebeveiliging: een risico en een uitdaging. *Economisch en Sociaal Tijdschrift*, 39(6), pp. 665–680, December 1985. In Dutch.
- [70] Y. G. Desmedt. The ideal world of computer security. *International Security Review*, pp. 29–32, January/February 1990. (**Invited paper**).
- [71] M. V. D. Burmester and Y. G. Desmedt. Remarks on the soundness of proofs. *Electronics Letters*, 25(22), pp. 1509–1511, October 26, 1989.
- [72] J.-J. Quisquater and Y. G. Desmedt. Chinese lotto as an exhaustive code-breaking machine. *Computer*, 24(11), pp. 14–22, November 1991.
- [73] Y. G. Desmedt. The “A” cipher does not necessarily strengthen security. *Cryptologia*, 15(3), pp. 203–206, July 1991.
- [74] Y. G. Desmedt. Cryptanalysis of conventional and public key cryptosystems. *Note Recensioni Notizie*, 39(3), pp. 87–96, 1990.
- [75] G. I. Davida and Y. G. Desmedt. Passports and visas versus IDs. *Computers & Security*, 11(3), pp. 253–258, May 1992.
- [76] M. Burmester, Y. Desmedt, and T. Beth. Efficient zero-knowledge identification schemes for smart cards. *The Computer Journal*, 35(1), pp. 21–29, February 1992. Special issue on Safety and Security.
- [77] M. Burmester, Y. Desmedt, and M. Yung. Canali “subliminal-free”: Una soluzione verso canali “covert-free”. *Rivista di Informatica*, XXIII(1), pp. 5–14, gennaio-marzo 1993. In Italian.
- [78] M. Burmester, Y. G. Desmedt, T. Itoh, K. Sakurai, and H. Shizuya. Divertible and subliminal-free zero-knowledge proofs of languages. *Journal of Cryptology*, 12(3), pp. 197–223, 1999.
- [79] A. Beimel, M. Burmester, Y. Desmedt, and E. Kushilevitz. Computing functions of a shared secret. *SIAM Journal on Discrete Mathematics*, 13(3), pp. 324–345, 2000.

- [80] M. Burmester and Y. G. Desmedt. Secure communication in an unknown network with Byzantine faults. *Electronics Letters*, 34(8), pp. 741–742, April 16, 1998.
- [81] Y. G. Desmedt and K. Kurosawa. Practical and proven zero-knowledge constant round variants of GQ and Schnorr. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E82-A(1), pp. 69–76, January 1999. Special Section on Cryptography and Information Security.
- [82] Y. Wang, Y. Desmedt, and M. Burmester. Models for dependable computation with multiple inputs and some hardness results. *Fundamenta Informaticae*, 42(1), pp. 61–73, March 2000.
- [83] Y. Desmedt. Re: Lack of anonymity in microsoft word. *Forum On Risks To The Public In Computers And Related Systems*, 20(24), March 11, 1999. See also <http://catless.ncl.ac.uk/Risks/20.24.html#subj16>.
- [84] N. Alexandris, M. Burmester, V. Chrissikopoulos, and Y. Desmedt. Secure linking of customers, merchants and banks in electronic commerce. *Future Generation Computer Systems*, 16(4), pp. 393–401, February 2000.
- [85] Y. Desmedt. Is there a need for survivable computation in critical infrastructures? *Information Security Technical Report*, 7(2), pp. 11–21, 2002.
- [86] Y. Desmedt and Y. Wang. Analyzing vulnerabilities of critical infrastructures using flows and critical vertices in and/or graphs. *International Journal of Foundations of Computer Science*, 15(1), pp. 107–125, February 2004.
- [87] J.-S. Coron, Y. Desmedt, D. Naccache, A. Odlyzko, and J. P. Stern. Index calculation attacks on rsa signature and encryption. *Des. Codes Cryptography*, 38(1), pp. 41–53, 2006.
- [88] Y. Desmedt. Análisis científico del ciberterrorismo. *Novática*, (172), pp. 33–37, noviembre-diciembre 2004.
- [89] Y. Desmedt. Towards a scientific analysis of robust critical infrastructures. *UPGRADE*, V(6), pp. 36–41, December 2004.
- [90] Y. Desmedt. A high availability internetwork capable of accommodating compromised routers. *BT Technology Journal*, 24(3), pp. 77–83, 2006.
- [91] Y. Desmedt, R. Gennaro, K. Kurosawa, and V. Shoup. A new and improved paradigm for hybrid encryption secure against chosen-ciphertext attack. *Journal of Cryptology*, 23(1), pp. 91–120, 2010.

8.5 Conference publications (refereed)

- [92] Y. Desmedt, J. Vandewalle, and R. Govaerts. A high speed parallel discrete source coder. In *Picture Coding Symposium*, pp. 58–59, Montréal, Canada, June 3–5, 1981.
- [93] Y. Desmedt, J. Vandewalle, and R. Govaerts. The use of knapsacks in public key systems. In *Groupes de Contact F.N.R.S. - Contactgroepen N.F.W.O. : Sciences Mathématiques - Wiskundige Wetenschappen*, pp. 190–211, Mons, Belgium, February 26, 1982.
- [94] Y. Desmedt, J. Vandewalle, and R. Govaerts. The influence of parallel coders in the encoding of a discrete source. In *Derde Symposium over Informatietheorie in de Benelux*, pp. 13–17, Zoetermeer, The Netherlands, May 13–14, 1982.
- [95] Y. Desmedt, J. Vandewalle, and R. Govaerts. Critical analysis of the security of knapsack public key algorithm. In *Derde Symposium over Informatietheorie in de Benelux*, pp. 19–27, Zoetermeer, The Netherlands, May 13–14, 1982.
- [96] Y. Desmedt, J. Vandewalle, and R. Govaerts. The influence of parallel coders in the encoding of a discrete source. In *International Symposium on Information Theory*, p. 14, Les Arcs, France, June 21–25, 1982. IEEE. Abstracts of papers.

RESEARCH

- [97] Y. Desmedt, J. Vandewalle, and R. Govaerts. Critical analysis of the security of knapsack public key algorithms. In *International Symposium on Information Theory*, pp. 115–116, Les Arcs, France, June 21–25, 1982. IEEE. Abstracts of papers.
- [98] Y. Desmedt, J. Vandewalle, and R. Govaerts. A combination of the public key knapsack and the RSA algorithm. In *International Symposium on Information Theory*, p. 116, Les Arcs, France, June 21–25, 1982. IEEE. Abstracts of papers.
- [99] Y. Desmedt, J. Vandewalle, and R. Govaerts. A highly secure cryptographic algorithm for high speed transmission. In *Globecom '82*, pp. 180–184, Miami, Florida, U.S.A., November 29–December 2, 1982. IEEE.
- [100] Y. Desmedt, J. Vandewalle, and R. Govaerts. A general public key cryptographic knapsack algorithm based on linear algebra. In *4th Symposium on Information Theory in the Benelux*, pp. 55–62. ISBN 90-334-0690-X, May 26–27, 1983. Haasrode, Belgium.
- [101] Y. Desmedt, J. Vandewalle, and R. Govaerts. The mathematical relation between the economic, cryptographic and information theoretical aspects of authentication. In *4th Symposium on Information Theory in the Benelux*, pp. 63–65. ISBN 90-334-0690-X, May 26–27, 1983. Haasrode, Belgium.
- [102] Y. Desmedt, J. Vandewalle, and R. Govaerts. A general public key cryptographic knapsack algorithm based on linear algebra. In *Intern. Symp. Inform. Theory*, pp. 129–130, St. Jovite, Quebec, Canada, September 26–30, 1983. IEEE. Abstracts of papers.
- [103] Y. Desmedt, J. Vandewalle, and R. Govaerts. The mathematical relation between the economic, cryptographic and information theoretical aspects of authentication. In *Intern. Symp. Inform. Theory*, p. 93, St. Jovite, Québec, Canada, September 26–30, 1983. IEEE. Abstracts of papers.
- [104] Y. Desmedt, J. Vandewalle, and R. Govaerts. Does public key cryptography provide adequate communication security. In *E.N.S.E.C. Conf.*, pp. 52–59, September 27–29, 1983. Brussels, Belgium.
- [105] Y. Desmedt, J. Vandewalle, and R. Govaerts. Does public key cryptography provide a practical and secure protection of data storage and transmission. In *Proc. Intern. Carnahan Conference on Security Technology*, pp. 133–139, Zürich, Switzerland, October 4–6, 1983. IEEE.
- [106] Y. Desmedt, J. Vandewalle, and R. Govaerts. Cryptography protects information against several frauds. In *Proc. Intern. Carnahan Conference on Security Technology*, pp. 255–259, Zürich, Switzerland, October 4–6, 1983. IEEE.
- [107] Y. Desmedt, J. Vandewalle, and R. Govaerts. Can public key cryptography provide fast practical and secure schemes against eavesdropping and fraud in modern communication networks? In *Telecom '83 - Proc. 4th World Telecommunication Forum*, pp. 1.2.6.1.–1.2.6.7., Geneva, Switzerland, October 29–November 1, 1983.
- [108] Y. Desmedt, J. Vandewalle, and R. Govaerts. Noiseless source coding of images and texts becomes practical using a parallelisation and bit encoder. In *Proc. 2nd. Int. Conf. on New Systems and Services in Telecommunications*, Liège, Belgium, November 16–18, 1983.
- [109] Y. Desmedt, J. Vandewalle, and R. Govaerts. Fast authentication using public key schemes. In *1984 International Zürich Seminar on Digital Communications*, pp. 191–197, Zürich, Switzerland, March 6–8, 1984. IEEE Catalog No. 84CH1998–4.
- [110] M. Davio, Y. Desmedt, and J.-J. Quisquater. Propagation characteristics of the DES. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology. Proc. of Eurocrypt 84 (Lecture Notes in Computer Science 209)*, pp. 62–73. Springer-Verlag, Berlin, 1985. Paris, France, April 9–11, 1984.
- [111] R. Govaerts, Y. Desmedt, and J. Vandewalle. Cryptography : How to attack, what to protect? In *ICC 84*, pp. 175–178, Amsterdam, The Netherlands, May 16–18, 1984. IEEE.

- [112] Y. Desmedt, J. Vandewalle, and R. Govaerts. The most general cryptographic knapsack scheme. In *Proc. International Carnahan Conference on Security Technology*, pp. 115–120, Lexington, Kentucky, U.S.A., May 16–18, 1984. IEEE.
- [113] F. Hoornaert, J. Goubert, and Y. Desmedt. Efficient hardware implementation of the DES. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology. Proc. of Crypto 84 (Lecture Notes in Computer Science 196)*, pp. 147–173. Springer-Verlag, 1985. Santa Barbara, California, U.S.A., August 19–22.
- [114] J. Peperstraete, R. Govaerts, J. Vandewalle, and Y. Desmedt. Is the protection of data security and privacy an unattainable dream? In *Proc. Eurocon 84*, Brighton, United Kingdom, September 26–28, 1984.
- [115] Y. Desmedt. Unconditionally secure authentication schemes and practical and theoretical consequences. In Hugh C. Williams, editor, *Advances in Cryptology: Crypto '85, Proceedings (Lecture Notes in Computer Science 218)*, pp. 42–55. Springer-Verlag, 1986. Santa Barbara, California, U.S.A., August 18–20.
- [116] J.-J. Quisquater, Y. Desmedt, and M. Davio. The importance of ‘good’ key scheduling schemes (how to make a secure DES scheme with ≤ 48 bit keys?). In Hugh C. Williams, editor, *Advances in Cryptology: Crypto '85, Proceedings (Lecture Notes in Computer Science 218)*, pp. 537–542. Springer-Verlag, 1986. Santa Barbara, California, U.S.A., August 18–20.
- [117] Y. Desmedt, F. Hoornaert, and J.-J. Quisquater. Several exhaustive key search machines and DES. In *Eurocrypt 86 (Abstract of papers)*, pp. 2.2A.–2.2B., Linköping, Sweden, May 20–22, 1986. IACR. ISBN 91-7870-077-9.
- [118] H. Cloetens, Y. Desmedt, L. Bierens, J. Vandewalle, and R. Govaerts. Additional properties in the S-boxes of the DES. In *Eurocrypt 86 (Abstract of papers)*, p. 2.3., Linköping, Sweden, May 20–22, 1986. IACR. ISBN 91-7870-077-9.
- [119] Y. Desmedt. Is there an ultimate use of cryptography? In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto '86 (Lecture Notes in Computer Science 263)*, pp. 459–463. Springer-Verlag, 1987. Santa Barbara, California, U.S.A., August 11–15.
- [120] Y. Desmedt. Major security problems with the “unforgeable” (Feige-)Fiat-Shamir proofs of identity and how to overcome them. In *Securicom 88, 6th worldwide congress on computer and communications security and protection*, pp. 147–159. SEDEP Paris France, March 15–17, 1988.
- [121] Y. Desmedt. Protecting against abuses of cryptosystems in particular in the context of verification of peace treaties. In R. M. Capocelli, editor, *Sequences (Combinatorics, Compression, Security, and Transmission)*, pp. 394–405. Springer-Verlag, 1990. Positano, Italy, June, 1988.
- [122] Y. Desmedt. Abuses in cryptography and how to fight them. In S. Goldwasser, editor, *Advances in Cryptology — Crypto '88, Proceedings (Lecture Notes in Computer Science 403)*, pp. 375–389. Springer-Verlag, 1990. Santa Barbara, California, U.S.A., August 21–25 (**57% acceptance rate**).
- [123] M. V. D. Burmester, Y. Desmedt, F. Piper, and M. Walker. A general zero-knowledge scheme. In J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology, Proc. of Eurocrypt '89 (Lecture Notes in Computer Science 434)*, pp. 122–133. Springer-Verlag, 1990. Houthalen, Belgium, April 10–13.
- [124] G. Davida, Y. Desmedt, and R. Peralta. A key distribution based on any one-way function. In J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology, Proc. of Eurocrypt '89 (Lecture Notes in Computer Science 434)*, pp. 75–79. Springer-Verlag, 1990. Houthalen, Belgium, April 10–13.
- [125] G. I. Davida, Y. G. Desmedt, and B. J. Matt. Defending systems against viruses through cryptographic authentication. In *Proceedings 1989 IEEE Symposium on Security and Privacy*, pp. 312–318, May 1989. Oakland, California.
- [126] Y. Desmedt. Making conditionally secure cryptosystems unconditionally abuse-free in a general context. In G. Brassard, editor, *Advances in Cryptology — Crypto '89, Proceedings (Lecture Notes in Computer*

- Science 435*), pp. 6–16. Springer-Verlag, 1990. Santa Barbara, California, U.S.A., August 20–24 (**48% acceptance rate**).
- [127] Y. Desmedt. Cryptanalysis of conventional and public key cryptosystems. In *Secondo Simposio su Stato e Prospettive della Ricerca crittografica in Italia*, pp. 22–41, November 23–24, 1989. Invited paper at the 2nd National Symposium on Cryptography Roma, Italy.
- [128] Y. Desmedt. An introduction to zero-knowledge proofs. In A. Klar, editor, *Mathematical Concepts of Dependable Systems*, p. 6, Oberwolfach, Germany, April 15–21, 1990. Mathematisches Forschungsinstitut Oberwolfach. Tagungsbericht 17/1990.
- [129] Y. Desmedt. System security of identification. In A. Klar, editor, *Mathematical Concepts of Dependable Systems*, p. 15, Oberwolfach, Germany, April 15–21, 1990. Mathematisches Forschungsinstitut Oberwolfach. Tagungsbericht 17/1990.
- [130] Y. Desmedt, C. Jahl, C. Landwehr, and H. Strack. Defining primitives for dependable communication. In A. Klar, editor, *Mathematical Concepts of Dependable Systems*, pp. 16–18, Oberwolfach, Germany, April 15–21, 1990. Mathematisches Forschungsinstitut Oberwolfach. Tagungsbericht 17/1990.
- [131] G. Davida, Y. Desmedt, and R. Peralta. On the importance of memory resources in the security of key exchange protocols. In I. Damgård, editor, *Advances in Cryptology, Proc. of Eurocrypt '90 (Lecture Notes in Computer Science 473)*, pp. 11–15. Springer-Verlag, 1991. Århus, Denmark, May 21–24 (**51% acceptance rate**).
- [132] Y. Desmedt. Computer-life: the next generation of computer viruses. In *Symposium on Computer Security, Threats and Countermeasures*, pp. 77–86, 1991. Roma, Italy, November 22–23, 1990.
- [133] M. Burmester, Y. Desmedt, and M. Yung. Subliminal-free channels: a solution towards covert-free channels. In *Symposium on Computer Security, Threats and Countermeasures*, pp. 188–197, 1991. Roma, Italy, November 22–23, 1990.
- [134] M. V. D. Burmester and Y. Desmedt. Broadcast interactive proofs. In D. W. Davies, editor, *Advances in Cryptology, Proc. of Eurocrypt '91 (Lecture Notes in Computer Science 547)*, pp. 81–95. Springer-Verlag, April 1991. Brighton, U.K.
- [135] Y. Desmedt. The next generation of computer threats. In D. Lefkon, editor, *Safe Computing, Proceedings: Fourth Annual Computer Virus & Security Conference*, pp. 596–607. DPMA and ACM-SIGSAC and IEEE-CS, March 14–15, 1991.
- [136] Y. Desmedt and M. Yung. Unconditional subliminal-freeness in unconditional authentication systems. In *Proceedings 1991 IEEE International Symposium on Information Theory*, p. 176, Budapest, Hungary, June 24–28, 1991. Full paper in preparation.
- [137] Y. Desmedt and M. Burmester. An efficient zero-knowledge scheme for the discrete logarithm based on smooth numbers. In H. Imai, R. L. Rivest, and T. Matsumoto, editors, *Advances in Cryptology — Asiacrypt '91, Proceedings (Lecture Notes in Computer Science 739)*, pp. 360–367. Springer-Verlag, 1993. Fujiyoshida, Japan, November, 1991 (**39% acceptance rate**).
- [138] Y. Desmedt and Y. Frankel. Perfect zero-knowledge sharing schemes over any finite Abelian group. In R. Capocelli, A. De Santis, and U. Vaccaro, editors, *Sequences II (Methods in Communication, Security, and Computer Science)*, pp. 369–378. Springer-Verlag, 1993. Positano, Italy, June 17–21, 1991.
- [139] Y. Desmedt. Alternative approach to cryptanalysis. In M. Frisch, editor, *E.I.S.S.-Workshop, Public-Key Cryptography: State of the Art and Future Direction*, p. 11, Oberwolfach, Germany, July 3–6, 1991. Mathematisches Forschungsinstitut Oberwolfach. Tagungsbericht 28a/1991.
- [140] Y. Frankel and Y. Desmedt. Multisignatures for virus protection. In D. Lefkon, editor, *Secure Networks, Proceedings: Fifth International Computer Virus & Security Conference*, pp. 641–649. DPMA and ACM-SIGSAC and IEEE-CS, March 12–13, 1992.

- [141] Y. Frankel and Y. Desmedt. Classification of ideal homomorphic threshold schemes over finite Abelian groups. In R. A. Rueppel, editor, *Advances in Cryptology — Eurocrypt '92, Proceedings (Lecture Notes in Computer Science 658)*, pp. 25–34. Springer-Verlag, 1993. Balatonfüred, Hungary, May, 1992 (**40% acceptance rate**).
- [142] Y. Desmedt. The Eurocrypt'92 controversial issue — trapdoor primes and moduli. In R. A. Rueppel, editor, *Advances in Cryptology — Eurocrypt '92, Proceedings (Lecture Notes in Computer Science 658)*, p. 198. Springer-Verlag, 1993. Panel, Balatonfüred, Hungary, May, 1992.
- [143] Y. Frankel, Y. Desmedt, and M. Burmester. Non-existence of homomorphic general sharing schemes for some key spaces. In E. F. Brickell, editor, *Advances in Cryptology — Crypto '92, Proceedings (Lecture Notes in Computer Science 740)*, pp. 549–557. Springer-Verlag, 1993. Santa Barbara, California, U.S.A., August 16–20 (**28% acceptance rate**).
- [144] M. V. D. Burmester and Y. Desmedt. Zero-knowledge based identification: from a theoretical concept towards a practical token. In R. M. Aiken, editor, *Education and Society, Information Processing 92, Volume II, Proceedings of the IFIP 12th World Computer Congress*, pp. 479–485, Madrid, Spain, September 7–11, 1992. North Holland.
- [145] Y. Desmedt. Breaking the traditional computer security research barriers. In Y. Deswarte, G. Eizenberg, and J.-J. Quisquater, editors, *Computer Security—ESORICS 92 (Lecture Notes in Computer Science 648)*, pp. 125–138. Springer-Verlag, Toulouse, France, November 23–25, 1992. Invited paper.
- [146] Y. Desmedt. Threshold cryptosystems. In J. Seberry and Y. Zheng, editors, *Advances in Cryptology — Auscrypt '92, Proceedings (Lecture Notes in Computer Science 718)*, pp. 3–14. Springer-Verlag, 1993. Gold Coast, Queensland, Australia, December, 1992, invited paper.
- [147] Y. Desmedt and J. Seberry. Practical proven secure authentication with arbitration. In J. Seberry and Y. Zheng, editors, *Advances in Cryptology — Auscrypt '92, Proceedings (Lecture Notes in Computer Science 718)*, pp. 27–32. Springer-Verlag, 1993. Gold Coast, Queensland, Australia, December, 1992 (**71% acceptance rate**).
- [148] Y. Desmedt. Threshold cryptography. In W. Wolfowicz, editor, *Proceedings of the 3rd Symposium on: State and Progress of Research in Cryptography*, pp. 110–122, February 15–16, 1993. Rome, Italy, invited paper.
- [149] N. Alexandris, M. Burmester, V. Chrissikopoulos, and Y. Desmedt. A secure key distribution system. In W. Wolfowicz, editor, *Proceedings of the 3rd Symposium on: State and Progress of Research in Cryptography*, pp. 30–34, February 15–16, 1993. Rome, Italy.
- [150] Y. Desmedt and M. Yung. Unconditionally secure broadcast authentication. In W. Wolfowicz, editor, *Proceedings of the 3rd Symposium on: State and Progress of Research in Cryptography*, pp. 106–109, February 15–16, 1993. Rome, Italy.
- [151] Y. Desmedt. Computer security by redefining what a computer is. In J. B. Michael, V. Ashby, and C. Meadows, editors, *Proceedings New Security Paradigms II Workshop*, pp. 160–166. ACM-SIGSAC, IEEE Computer Society Press, 1992–1993. Little Compton, Rhode Island, U.S.A.
- [152] S. G. Barwick, Y. Desmedt, and P. Wild. Homomorphic threshold schemes, k-arcs and Lenstra's constant. In P. G. Farrell, editor, *Codes and ciphers*, pp. 95–102. Formora Ltd., Essex, 1995. Royal Agricultural College, Cirencester, December, 1993.
- [153] M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. In A. De Santis, editor, *Advances in Cryptology — Eurocrypt '94, Proceedings (Lecture Notes in Computer Science 950)*, pp. 275–286. Springer-Verlag, 1995. Perugia, Italy, May 9–12 (**26% acceptance rate**).
- [154] Y. Desmedt and M. Yung. Minimal cryptosystems and defining subliminal-freeness. In *Proceedings 1994 IEEE International Symposium on Information Theory*, p. 347, Trondheim, Norway, June 27–July 1, 1994.

- [155] Y. Desmedt. Subliminal-free sharing schemes. In *Proceedings 1994 IEEE International Symposium on Information Theory*, p. 490, Trondheim, Norway, June 27–July 1, 1994.
- [156] Y. Desmedt. Extending Reed-Solomon codes to modules. In *Proceedings 1995 IEEE International Symposium on Information Theory*, p. 498, Whistler, BC, Canada, September 17–22, 1995.
- [157] Y. Desmedt. Establishing Big Brother using covert channels and other covert techniques. In R. Anderson, editor, *Information Hiding, First International Workshop, Proceedings (Lecture Notes in Computer Science 1174)*, pp. 65–71. Springer-Verlag, 1996. Cambridge, U.K., May 30–June 1.
- [158] M. Burmester, Y. Desmedt, and G. Kabatianskii. Trust and security: A new look at the Byzantine generals problem. In R. N. Wright and P. G. Neumann, editors, *Network Threats, DIMACS, Series in Discrete Mathematics and Theoretical Computer Science, December 2–4, 1996, vol. 38*. AMS, 1998.
- [159] Y. G. Desmedt, S. Hou, and J.-J. Quisquater. Cerebral cryptography. In D. Aucsmith, editor, *Information Hiding, Second International Workshop, Proceedings (Lecture Notes in Computer Science 1525)*, pp. 62–72. Springer-Verlag, 1998. Portland, Oregon, April 15–17 (**61% acceptance rate**).
- [160] Y. Desmedt, B. King, W. Kishimoto, and K. Kurosawa. A comment on the efficiency of secret sharing scheme over any finite abelian group. In C. Boyd and E. Dawson, editors, *Information Security and Privacy, ACISP'98, Proceedings (Lecture Notes in Computer Science 1438)*, pp. 391–402. Springer-Verlag, July 13–15, 1998. Brisbane, Australia (**53% acceptance rate**).
- [161] Y. Desmedt. Information-theoretic secure identification. In *Proceedings IEEE International Symposium on Information Theory*, p. 296, Cambridge, Massachusetts, August 16–21, 1998. <http://www.ee.princeton.edu/~isitrecv/p172.ps>.
- [162] Y. Desmedt and V. Viswanathan. Unconditionally secure dynamic conference key distribution. In *Proceedings IEEE International Symposium on Information Theory*, p. 383, Cambridge, Massachusetts, August 16–21, 1998. <http://www.ee.princeton.edu/~isitrecv/p171.ps>.
- [163] Y. Desmedt, S. Hou, and J.-J. Quisquater. Audio and optical cryptography. In K. Ohta and D. Pei, editors, *Advances in Cryptology — Asiacrypt '98, Proceedings (Lecture Notes in Computer Science 1514)*, pp. 392–404. Springer-Verlag, October, 18–22 1998. Beijing, China (**27% acceptance rate**).
- [164] M. Burmester, Y. Desmedt, and Y. Wang. Using approximation hardness to achieve dependable computation. In M. Luby, J. Rolim, and M. Serna, editors, *Randomization and Approximation Techniques in Computer Science, Proceedings (Lecture Notes in Computer Science 1518)*, pp. 172–186. Springer-Verlag, October, 8–10 1998. Barcelona, Spain.
- [165] Y. Wang and Y. Desmedt. Secure communication in broadcast channels. In J. Stern, editor, *Advances in Cryptology — Eurocrypt '99, Proceedings (Lecture Notes in Computer Science 1592)*, pp. 446–458. Springer-Verlag, 1999. Prague, Czech Republic, May 2–6 (**27% acceptance rate**).
- [166] Y. Desmedt. Viewpoint on research and development needed to achieve survivability of the critical information infrastructure. In *Position papers for the 1998 Information Survivability Workshop, participants' edition*, pp. 57–61. IEEE Computer Society, October 28–30, 1998. Orlando, Florida.
- [167] Y. Desmedt and Y. Wang. Maximum flows & critical vertices in AND/OR graphs. In *INFORMS (INstitute For Operations Research and the Management Sciences)*, p. 8, Baltimore, Maryland, May 2–5, 1999. INFORMS. <http://www.informs.org/Conf/Cincinnati99//TALKS/SA34.html> Cincinnati, Ohio.
- [168] Y. Desmedt and B. King. Verifiable democracy. In B. Preneel, editor, *Secure Information Networks, IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99)*, pp. 53–70. Kluwer Academic Publishers, September, 20–21 1999. Leuven, Belgium (**70% acceptance rate**).
- [169] Y. Desmedt, T. V. Le, and J.-J. Quisquater. Nonbinary audio cryptography. In A. Pfitzmann, editor, *Information Hiding, Third International Workshop, Proceedings (Lecture Notes in Computer Science*

- 1768), pp. 478–489. Springer-Verlag, 2000. Dresden, Germany, September 29–October 1, 1999 (**49% acceptance rate**).
- [170] Y. Desmedt. A too limited list of infrastructures identified as critical. In *Protecting NATO Information Systems in the 21st Century*, pp. 3–1–3–9, May 2000. Washington DC, U.S.A., October 25–27, 1999.
- [171] Y. Desmedt and Y. Wang. Approximation hardness and secure communication in broadcast channels. In K. Y. Lam, E. Okamoto, and C. Xing, editors, *Advances in Cryptology — Asiacrypt '99, Proceedings (Lecture Notes in Computer Science 1716)*, pp. 247–257. Springer-Verlag, November, 14–18 1999. Singapore (**32% acceptance rate**).
- [172] N. Alexandris, M. Burmester, V. Chrissikopoulos, and Y. Desmedt. Designated 2-verifier proofs and their application to electronic commerce. In K.-Y. Lam, I. E. Shparlinski, H. Wang, and C. Xing, editors, *Proceedings Workshop on Cryptography and Computational Number Theory (CCNT'99)*, pp. 149–163. Birkhäuser, 2001. Singapore, November 22-26, 1999.
- [173] X. Wang, Y. Huang, Y. Desmedt, and D. Rine. Enabling secure on-line DNS dynamic update. In *Proceedings of the Sixteenth Annual Computer Security Applications Conference (ACSAC'00)*, pp. 52–58, December 11-15, 2000. New Orleans, Louisiana.
- [174] Y. Desmedt. A definition of cryptography. In *Proceedings of the Tenth National Conference on Information Security*, pp. I–VII, 2000. Invited lecture, May 5-6, 2000, Hualien, Taiwan.
- [175] K. Kurosawa, T. Yoshida, and Y. Desmedt. Inherently large traceability of broadcast encryption scheme. In *Proceedings IEEE International Symposium on Information Theory*, p. 464, Sorrento, Italy, June 25-30, 2000. <http://www.dia.unisa.it/isit2000/lavori/634.ps>.
- [176] Y. Desmedt. Statement on issues in high performance computing security. In *Proceedings of the 23rd National Information Systems Security Conference*, p. 660, Baltimore, Maryland, October 16–19, 2000.
- [177] C. Adams, M. Burmester, Y. Desmedt (moderator), M. Reiter, and P. Zimmermann. Which PKI (Public Key Infrastructure) is the right one? (panel). In *Proceedings of the 7th ACM Conference on Computer and Communications Security*, pp. 98–101, November 1–4, 2000. Athens, Greece.
- [178] Y. Desmedt and T. V. Le. Moiré cryptography. In *Proceedings of the 7th ACM Conference on Computer and Communications Security*, pp. 116–124, November 1–4, 2000. Athens, Greece (**21% acceptance rate**).
- [179] Y. Desmedt, M. Burmester, and J. Seberry. Equitability in retroactive data confiscation versus proactive key escrow. In K. Kim, editor, *Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2001, proceedings (Lecture Notes in Computer Science 1992)*, pp. 277–286. Springer-Verlag, February 13–15, 2001. Cheju Island, Korea (**45% acceptance rate**).
- [180] Y. Desmedt, M. Burmester, R. Safavi-Naini, and H. Wang. Threshold things that think (T^4): security requirements to cope with theft of handheld/handless internet devices. CD-ROM. Presented at the Symposium on Requirements Engineering for Information Security, Indianapolis, Indiana, USA, March 5-6, 2001.
- [181] M. Burmester and Y. Desmedt. Hierarchical public-key certification: The next target for hackers? In *The First International Workshop for Asian Public Key Infrastructure (IWAP 2001), proceedings*, pp. 77–92, 2001. Deajeon (Korea), October 19 - 20.
- [182] Y. Desmedt, M. Burmester, and Y. Wang. Are we on the right track to achieve survivable computer network systems. Accepted at the Fourth Information Survivability Workshop (ISW-2001), March 18–20.
- [183] M. Burmester, Y. Desmedt, M. Mambo, and E. Okamoto. Formal modes and concrete examples of ordered multi-party cryptography. In *Proceedings of ISEC*. IEICE, 2001. Tokyo, Japan, December 17, 2001.

- [184] Y. Desmedt (moderator). Towards a funded research agenda. Fourth Information Survivability Workshop, Vancouver, Canada, March 18-20, 2002, <http://www.cert.org/research/isw/isw2001/slides/summary-work-group-2.pdf>.
- [185] Y. Desmedt, R. Safavi-Naini, and H. Wang. Redistribution of mechanical secret shares. In M. Blaze, editor, *Financial Cryptography, 6th International Conference, Proceedings (Lecture Notes in Computer Science 2357)*, pp. 238–252. Springer-Verlag, 2003. Southhampton, Bermuda, March 11-14, 2002 (**26% acceptance rate**).
- [186] Y. Desmedt, M. Burmester, and Y. Wang. Using economics to model threats and security in distributed computing. Workshop on Economics and Information Security, Berkeley, May 16-17, 2002, <http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/33.ps>.
- [187] Y. Desmedt, M. Burmester, and K. Kurosawa. On perfect traitor tracing. In *Proceedings IEEE International Symposium on Information Theory*, p. 439, Lausanne, Switzerland, June 30–July 5, 2002.
- [188] Y. Desmedt and Y. Wang. Maximum flows and critical vertices in and/or graphs. In O. H. Ibarra and L. Zhang, editors, *Computing and Combinatorics, 8th Annual International Conference, COCOON 2002 (Lecture Notes in Computer Science 2387)*, pp. 238–248. Springer-Verlag, 2002. Singapore, August 15-17 (**57% acceptance rate**).
- [189] Y. Desmedt and B. King. Verifiable democracy a protocol to secure an electronic legislature. In R. Traummüller and K. Lenk, editors, *Electronic Government, First International Conference, EGOV 2002 (Lecture Notes in Computer Science 2456)*, pp. 460–463. Springer-Verlag, 2002. Aix-en-Provence, France, September 2-5.
- [190] Y. Desmedt and Y. Wang. Efficient zero-knowledge protocols for some practical graph problems. In *Third Conference on Security in Communication Networks '02 (Lecture Notes in Computer Science 2576)*, pp. 296–308. Springer-Verlag, 2003. Amalfi, Italy, September 12-13, 2002.
- [191] T. V. Le and Y. Desmedt. Cryptanalysis of UCLA watermarking schemes for intellectual property protection. In F.A.P. Petitcolas, editor, *Information Hiding, 5th International Workshop IH 2002 (Lecture Notes in Computer Science 2578)*, pp. 213–225. Springer-Verlag, 2002. Noordwijkerhout, The Netherlands, October 7-9 (**35% acceptance rate**).
- [192] Y. Desmedt. Security problems with on-line revocation. In *The Second International Workshop for Asian Public Key Infrastructure, Proceedings*, p. 66, 2002. Invited lecture, October 30 - November 1, 2002, Taipei, Taiwan.
- [193] Y. Desmedt, K. Kurosawa, and T. V. Le. Error correcting and complexity aspects of linear secret sharing schemes. In C. Boyd and W. Mao, editors, *Information Security, 6th International Conference, ISC 2003, (Lecture Notes in Computer Science 2851)*, pp. 396–407. Springer-Verlag, 2003. Bristol, UK, October 1-3 (**23% acceptance rate**).
- [194] Y. Desmedt. Broader privacy issues. RFID Privacy Workshop, MIT, Boston, November 11, 2003, <http://rfidprivacy.ex.com/papers/desmedt.pdf>.
- [195] M. Burmester, Y. Desmedt, and Y. Wang. A critical analysis of models for fault-tolerant and secure computation. In *Proceedings of the IASTED Communication, Network, and Information Security (CNIS) 2003*, pp. 147–152, 2003.
- [196] T. V. Le, R. Sparr, R. Wernsdorf, and Y. Desmedt. Complementation-like and cyclic properties of aes round functions. In *Fourth Conference on the Advanced Encryption Standard (AES): AES - State of the Crypto Analysis (Lecture Notes in Computer Science 3373)*. Springer-Verlag, 2005. Bonn, Germany, May 10–12, 2004.
- [197] Y. Desmedt and M. K. Patel. A modernized version of visual cryptography. In *Applied Cryptography and Network Security, Second International Conference, ACNS: Technical Track*, 2004. Yellow Mountain, China, June 8-11.

- [198] Y. Desmedt and M. Burmester. Identity-based key infrastructures (IKIs). In Y. Deswarte, F. Cuppens, S. Jajodia, and L. Wang, editors, *19th IFIP International Information Security Conference (SEC 2004)*, pp. 167–176. Kluwer, August, 23–26 2004. Toulouse, France.
- [199] B. King and Y. Desmedt. Securing abstention in an electronic legislature. In Jr. R. H. Sprague, editor, *Hawaii International Conference on System Sciences*. IEEE Computer Society, January, 3 - 6 2005. CD ROM, Big Island of Hawaii, USA.
- [200] Y. Desmedt. Understanding why some network protocols are user-unfriendly. In B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, editors, *Security Protocols Workshop, 13th International Workshop, 2005 (Lecture Notes in Computer Science 4631)*, pp. 215–227. Springer-Verlag, 2007. Cambridge, United Kingdom April 20-22.
- [201] Y. Desmedt and Y. Wang. Survey of models for critical infrastructures and methods to measure robustness. In *First CRIS International Workshop on Critical Information Infrastructures, Proceedings*. IEEE, Computer Society Press, May, 17-18 2005. Linköping, Sweden.
- [202] Y. Desmedt. Potential impacts of a growing gap between theory and practice in information security. In C. Boyd and J. M. González Nieto, editors, *Information Security and Privacy, ACISP 2005, Proceedings (Lecture Notes in Computer Science 3574)*, pp. 532–536. Springer-Verlag, July 4–6, 2005. Brisbane, Australia, invited talk.
- [203] Y. Desmedt. Robust operations. In L.-Y. Wu X.S. Zhang, D.-G. Liu, editor, *Operations Research and its Applications, Fifth International Symposium, ISORA '05*, Lecture Notes in Operations Research, pp. 267–275, Beijing, China, August, 8–13 2005. World Publishing Corporation. Tibet, China.
- [204] Y. Desmedt and K. Kurosawa. Electronic voting: starting over? In J. Zhou, J. Lopez, R. H. Deng, and F. Bao, editors, *Information Security, 8th International Conference, ISC 2005, (Lecture Notes in Computer Science 3650)*, pp. 329–343. Springer-Verlag, 2005. Singapore, September 20-23 (**14% acceptance rate**).
- [205] Y. Desmedt. Towards a formal definition of cryptography. 2004. Security In Information Systems WOSIS-2004, Porto, Portugal, April 13, invited presentation.
- [206] Y. Desmedt, Y. Wang, R. Safavi-Naini, and H. Wang. Radio networks with reliable communication. In L. Wang, editor, *Computing and Combinatorics, 11th Annual International Conference, COCOON, Proceedings (Lecture Notes in Computer Science 3595)*, pp. 156–166, 2005. Kunming, Yunnan China, August 16-19, 2005 (**27% acceptance**).
- [207] Y. Desmedt and Y. Wang. Identifying which infrastructures are critical. In *The IEE seminar on Signal Processing Solutions For Homeland Security*, pp. 2/1–2/19, 2005. October 11, 2005, London, UK.
- [208] Y. Desmedt. Security when routers are taken over by the adversary. In E. Kranakis, E. Haroutunian, and E. Shahbazian, editors, *Aspects of Network Security and Information Security*, volume 17 of *NATO Science for Peace and Security Issues, D: Information and Communication Security*, pp. 10–18. IOS Press, 2008. October 1 - October 12, 2005, Yerevan, Armenia (Invited Speaker).
- [209] Y. Desmedt. Unconditionally private and reliable communication in an untrusted network. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, Proceedings*, pp. 38–41, October 16–19, 2005. Awaji Island, Japan.
- [210] Y. Desmedt and T. Lange. Pairing based threshold cryptography improving on Libert-Quisquater and Baek-Zheng. In G. Di Crescenzo and A. D. Rubin, editors, *Financial Cryptography*, volume 4107 of *Lecture Notes in Computer Science*. Springer, 2006.
- [211] K. Peng, J. M. González Nieto, Y. Desmedt, and E. Dawson. Klein bottle routing: An alternative to onion routing and mix network. In *Information Security and Cryptology - ICISC 2006 (Lecture Notes in Computer Science 4296)*, pp. 296–309, 2006.

- [212] Y. Desmedt, Y. Wang, and M. Burmester. Revisiting colored networks and privacy preserving censorship. In Javier López, editor, *Critical Information Infrastructures Security, First International Workshop, CRITIS 2006, Samos, Greece, August 31 - September 1, 2006*, volume 4347 of *Lecture Notes in Computer Science*, pp. 140–150. Springer, 2006.
- [213] Y. Desmedt, T. Lange, and M. Burmester. Scalable authenticated tree based group key exchange for ad-hoc groups. In S. Dietrich and R. Dhamija, editors, *Financial Cryptography*, volume 4886 of *Lecture Notes in Computer Science*, pp. 104–118. Springer, 2007.
- [214] Y. Desmedt. Position statement in RFID s&p panel: from relative security to perceived secure. In S. Dietrich and R. Dhamija, editors, *Financial Cryptography*, volume 4886 of *Lecture Notes in Computer Science*, pp. 53–56. Springer, 2007. Invited panel.
- [215] Y. Desmedt and G. Jakimoski. Non-degrading erasure-tolerant information authentication with an application to multicast stream authentication over lossy channels. In M. Abe, editor, *CT-RSA 2007*, volume 4377 of *Lecture Notes in Computer Science*, pp. 324–338. Springer, 2007.
- [216] R. Safavi-Naini, S. Wang, and Y. Desmedt. Unconditionally secure ring authentication. In F. Bao and S. Miller, editors, *ACM Symposium on Information, Computer and Communications Security, ASIACCS 2007*, pp. 173–181, 2007.
- [217] Y. Desmedt, J. Pieprzyk, R. Steinfeld, and H. Wang. On secure multi-party computation in black-box groups. In *Advances in Cryptology — Crypto 2007, Proceedings (Lecture Notes in Computer Science 4622)*, pp. 591–612, 2007.
- [218] Y. Desmedt and K. Kurosawa. A generalization and a variant of two threshold cryptosystems based on factoring. In J. A. Garay, A. K. Lenstra, M. Mambo, and R. Peralta, editors, *Information Security Conference (ISC)*, volume 4779 of *Lecture Notes in Computer Science*, pp. 351–361. Springer, 2007.
- [219] I. Damgård, Y. Desmedt, M. Fitzi, and J. B. Nielsen. Secure protocols with asymmetric trust. In K. Kurosawa, editor, *Advances in Cryptology - ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pp. 357–375. Springer, 2007.
- [220] Y. Desmedt and T. Lange. Revisiting pairing based group key exchange. In G. Tsudik, editor, *Financial Cryptography and Data Security, 12th International Conference, Cozumel, Mexico, January 28-31, 2008*, volume 5143 of *Lecture Notes in Computer Science*, pp. 53–68. Springer, 2008.
- [221] J. Callas, Y. Desmedt, D. Nagy, A. Otsuka, J.-J. Quisquater, and Moti Yung. Real electronic cash versus academic electronic cash versus paper cash (panel report). In G. Tsudik, editor, *Financial Cryptography and Data Security, 12th International Conference, Cozumel, Mexico, January 28-31, 2008*, volume 5143 of *Lecture Notes in Computer Science*, pp. 307–313. Springer, 2008.
- [222] Y. Desmedt and D. H. Phan. A CCA secure hybrid Damgård’s ElGamal encryption. In J. Baek, F. Bao, K. Chen, and X. Lai, editors, *Provable Security, Second International Conference, ProvSec Shanghai, China, October 30 - November 1, 2008*, volume 5324 of *Lecture Notes in Computer Science*, pp. 68–82. Springer, 2008.
- [223] Y. Desmedt, H. Lipmaa, and D. H. Phan. Hybrid Damgård is CCA1-secure under the DDH assumption. In M. K. Franklin, L. C. K. Hui, and D. S. Wong, editors, *Cryptology and Network Security, 7th International Conference, CANS, Hong-Kong, China, December 2-4, 2008*, volume 5339 of *Lecture Notes in Computer Science*, pp. 18–30. Springer, 2008.
- [224] Y. Desmedt, B. King, and B. Schoenmakers. Revisiting the Karnin, Greene and Hellman bounds. In R. Safavi-Naini, editor, *Information Theoretic Security, Third International Conference, ICITS, Calgary, Canada, August 10-13, 2008*, volume 5155 of *Lecture Notes in Computer Science*, pp. 183–198. Springer, 2008.

- [225] D. Tonien, R. Safavi-Naini, P. Nickolas, and Y. Desmedt. Unconditionally secure approximate message authentication. In Y. M. Chee, C. Li, S. Ling, H. Wang, and C. Xing, editors, *Coding and Cryptology, Second International Workshop, IWCC 2009, Zhangjiajie, China, June 1-5, 2009. Proceedings*, volume 5557 of *Lecture Notes in Computer Science*, pp. 233–247. Springer, 2009.
- [226] Q. Yang and Y. Desmedt. Cryptanalysis of secure message transmission protocols with feedback. In K. Kurosawa, editor, *Information Theoretic Security, 4th International Conference, ICITS, Revised Selected Papers*, volume 5973 of *Lecture Notes in Computer Science*, pp. 159–176. Springer, 2009.
- [227] Y. Desmedt, S. Erotokritou, and R. Safavi-Naini. Simple and communication complexity efficient almost secure and perfectly secure message transmission schemes. In D. Bernstein and T. Lange, editors, *Africacrypt, May 3-6, South Africa, Proceedings*, volume 6055 of *Lecture Notes in Computer Science*, pp. 166–183. Springer, 2010.
- [228] Y. Desmedt and E. Elkind. Equilibria of plurality voting with abstentions. In D. C. Parkes, C. Dellarocas, and M. Tennenholtz, editors, *ACM conference on Electronic Commerce*, pp. 347–356, 2010.
- [229] S. Estehghari and Y. Desmedt. Exploiting the client vulnerabilities in internet e-voting systems: Hacking Helios 2.0 as an example. In *2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '10), August 9–10, 2010*, 2010.
- [230] K. Jia, Y. Desmedt, L. Han, and X. Wang. Pseudo-cryptanalysis of luffa. In *Inscrypt 2010*, 2010. To appear in the proceedings, LNCS.
- [231] A. Miyaji and Y. Desmedt. Redesigning group key exchange protocol based on bilinear pairing suitable for various environments. In *Inscrypt 2010*, 2010. To appear in the proceedings, LNCS.
- [232] Y. Lu and Y. Desmedt. Improved distinguishing attack on rabbit. In *Information Security Conference (ISC)*, October 2010. To appear in the proceedings, LNCS.
- [233] Y. Lu and Y. Desmedt. Bias analysis of a certain problem with applications to E0 and Shannon cipher. In *Information Security and Cryptology - ICISC 2010*, December 2010. To appear in the proceedings, LNCS.
- [234] Q. Yang and Y. Desmedt. General perfectly secure message transmission using linear codes. In *Asiacrypt 2010*, 2010. To appear in the proceedings, LNCS.

8.6 Techreport

- [235] Y. Desmedt, J. Vandewalle, and R. Govaerts. Critical analysis of the security of knapsack public key algorithms. Internal report, ESAT K. U. Leuven Belgium, Leuven Belgium, October 1981. Presented at IEEE ISIT 1982 and also in IEEE Transaction on Information Theory 1984.
- [236] S. Bengio, G. Brassard, Y. Desmedt, C. Goutier, and J.-J. Quisquater. Aspects and importance of secure implementations of identification systems. Manuscript M209, Philips Research Laboratory, 1987. Appeared partially in Journal of Cryptology.
- [237] G. Davida and Y. Desmedt. “Complete” identification systems. Tech. Report TR-CS-88-15, Dept. of EE & CS, Univ. of Wisconsin–Milwaukee, May 1988.
- [238] M. V. D. Burmester, Y. G. Desmedt, F. Piper, and M. Walker. A general zero-knowledge scheme. Tech. Report TR-CS-89-1, Dept. of EE & CS, Univ. of Wisconsin–Milwaukee, March 1989. Published in Proc. of Eurocrypt '89.
- [239] M. V. D. Burmester, Y. G. Desmedt, F. Piper, and M. Walker. A meta zero-knowledge scheme. Report 89/13, European Institute for System Security, Universität of Karlsruhe, Germany, 1989. Presented at CO89 Combinatorial Optimization Conference.

- [240] T. Beth and Y. Desmedt. Identification tokens — or: Solving the chess grandmaster problem. Report 90/1, European Institute for System Security, Universität of Karlsruhe, Germany, 1990. Published in the Proc. of Crypto '90.
- [241] M. V. D. Burmester and Y. Desmedt. All languages in NP have divertable zero-knowledge proofs and arguments under cryptographic assumptions. Report 90/2, European Institute for System Security, Universität of Karlsruhe, Germany, 1990. Published in Proc. Eurocrypt '90.
- [242] Y. Desmedt and M. Burmester. An efficient zero-knowledge scheme for the discrete logarithm based on smooth numbers. Tech. Report TR-91-5-01, Dept. of EE & CS, Univ. of Wisconsin-Milwaukee, May 1991. Presented at Asiacrypt'91.
- [243] Y. Desmedt. Computer-life: the next generation of computer viruses. Report 91/8, European Institute for System Security, Universität of Karlsruhe, Germany, 1991. Published in Proc. Symposium on Computer Security, Threats and Countermeasures, Roma, Italy, 1990.
- [244] J.-J. Quisquater and Y. Desmedt. A lotto as an exhaustive code-breaking machine. Report 91/9, European Institute for System Security, Universität of Karlsruhe, Germany, 1991. Published in Computer (IEEE), November 1991.
- [245] M. Burmester, Y. Desmedt, and T. Beth. Efficient zero-knowledge identification schemes for smart cards based on Abelian groups. Report 91/10, European Institute for System Security, Universität of Karlsruhe, Germany, 1991. Published in the special issue on Safety and Security, The Computer Journal, February 1992.
- [246] Y. Desmedt. A cryptanalytic study of cascade ciphers. Tech. Report TR-91-6-01, Dept. of EE & CS, Univ. of Wisconsin-Milwaukee, June 1991.
- [247] Y. Desmedt and Y. Frankel. Perfect zero-knowledge sharing schemes over any finite Abelian group. Tech. Report TR-91-6-02, Dept. of EE & CS, Univ. of Wisconsin-Milwaukee, June 1991. Presented at Sequences '91, Revised version, "Homomorphic zero-knowledge threshold schemes over any finite Abelian group", February 1992.
- [248] Y. Frankel and Y. Desmedt. Classification of ideal homomorphic threshold schemes over finite Abelian groups. Tech. Report TR-92-2-01, Dept. of EE & CS, Univ. of Wisconsin-Milwaukee, February 1992. Presented at Eurocrypt '92.
- [249] Y. Frankel, Y. Desmedt, and M. Burmester. Non-existence of homomorphic general sharing schemes for some key spaces. Tech. Report TR-92-05-03, Dept. of EE & CS, Univ. of Wisconsin-Milwaukee, May 1992. Presented at Crypto '92.
- [250] Y. Desmedt. Practical interactive proven secure authentication scheme. Tech. Report TR-94-02-02, Dept. of EE & CS, Univ. of Wisconsin-Milwaukee, February 1994.

9 Knowledge transfer

Research successfully and sustainably commercialised

- Threshold Cryptography, commercialised by, e.g., IBM. Moreover, the technology is under consideration to be adapted by the DNSSEC-Deployment Group and used in the financial sector.
- Co-inventor of electronic passports and electronic visas (1988).
- Recruited in 1995 for the post of Vice-President of Citibank (New York) to implement cryptographically secure e-commerce (declined)
- Cited in several IETF RFC, such as RFC 2313, RFC 3447, RFC 3607

KNOWLEDGE TRANSFER

- Cited 10 times by different authors in “Contemporary Cryptology,” Editor: G. J. Simmons (Fellow of Cambridge), IEEE Press, 1992.
- Cited 21 times in the textbook “Applied Cryptography” by Bruce Schneier, 1996
- Cited 12 times in the “Handbook of Applied Cryptography,” by A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, CRC, 1996

Contributions to scientific and technical encyclopedia:

- [251] Y. G. Desmedt. Cryptography. In J. G. Webster, editor, *Wiley Encyclopedia of Electrical and Electronics Engineering*, volume 4, pp. 425–432. John Wiley & Sons, New York, 1999. (**Invited paper**).
- [252] Y. Desmedt. Cryptographic foundations. In M. Atallah, editor, *Handbook of Algorithms and Theory of Computation*, chapter 38. CRC, Boca Raton, 1998.
- [253] Y. Desmedt. Encryption schemes. In M. Atallah, editor, *Handbook of Algorithms and Theory of Computation*, chapter 39. CRC, Boca Raton, 1998.
- [254] Y. Desmedt. *Breaking One Million DES keys*, chapter 9. O’Reilly, Sebastol, California, 1998.
- [255] Y. Desmedt. Elgamal public key encryption. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 183. Springer, 2005.
- [256] Y. Desmedt. Fiat-shamir identification protocol and the fiat-shamir signature scheme. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 222. Springer, 2005.
- [257] Y. Desmedt. Trojan horses, computer viruses and worms. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, pp. 627–628. Springer, 2005.
- [258] Y. Desmedt. Access structure. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 7. Springer, 2005.
- [259] Y. Desmedt. Covert channels. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, pp. 106–107. Springer, 2005.
- [260] Y. Desmedt. Deniable encryption. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, pp. 142–143. Springer, 2005.
- [261] Y. Desmedt. Knapsack cryptographic schemes. In H. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, pp. 333–342. Springer, 2005.
- [262] Y. Desmedt. Man-in-the-middle attack. In H. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 368. Springer, 2005.
- [263] Y. Desmedt. Relay attack. In H. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 519. Springer, 2005.
- [264] Y. Desmedt. Station-to-station protocol. In H. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 596. Springer, 2005.
- [265] Y. Desmedt. Threshold cryptography. In H. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, pp. 606–611. Springer, 2005.
- [266] Y. Desmedt. Cryptographic foundations. In M. Atallah, editor, *Handbook of Algorithms and Theory of Computation*, chapter 38. CRC, Boca Raton, 2nd edition, To appear.
- [267] Y. Desmedt. Encryption schemes. In M. Atallah, editor, *Handbook of Algorithms and Theory of Computation*, chapter 39. CRC, Boca Raton, 2nd edition, To appear.

Other applicable contributions:

- consultant for TIS, Network Associates, and George Mason University.
- member of the advisory board of the Kluwer Encyclopedia on Cryptography (2002–2004, 2009–).

10 Teaching

Teaching to international audiences

- Invited speaker at the post-graduate course on cryptology, CWI, Amsterdam, The Netherlands, October 14–25, 1985: “*DES*”.
- Invited (sole) lecturer at ETH, Zürich, Switzerland, April 23–24, 1990: *Tutorial on Zero-knowledge*.
- Invited lecturer at the ICU (Information and Communications University), Taejon, South Korea, February 16–17, 2001: *Tutorial on Zero-Knowledge and its Applications*.
- Invited lecturer at the “Mathematics of Cryptology” (Mathematical Society of the Flemish community), Brussels, Belgium, May 9, 2003: *Different Aspects of Secret Sharing*.
- Invited at the “Digital Rights Management” (DRM) postgraduate course, Université Catholique de Louvain, Louvain-la-Neuve, Belgium, May 17–19, 2005:
 - *Panel on research for the future DRM systems* (May 19),
 - *Traitor Tracing* (May 19),
 - *Digital Steganography: an Introduction* (May 19).
- Sole lecturer on “Threshold Cryptography,” Universidad Carlos III de Madrid, Spain, June 7–10, 2005.
- Invited at the “11th Estonian Winter School in Computer Science” (EWSCS), Palmse, Estonia, March 4–12, 2006:
 - Robust Operations Research I: Introduction & Communication Networks
 - Robust Operations Research II: Production Networks
 - Robust Operations Research III: Operations
- Invited at the “Ecole de printemps ”cryptographie et securite informatique,” France, April 28, 2006: “Deni de Service et Securite des Reseaux de Telecommunication.”
- Invited at CALIT: Center of Advanced Learning in Information Technologies “Symposium on Systems Security and Privacy,” Diegem, Belgium, October 19–20, 2006: “From Relative Security to Perceived Security.”
- Sole lecturer on “Threshold Cryptography,” Dalian University of Technology, China, September 10–14, 2007.

Development of curriculum, etc.

At the University of Wisconsin — Milwaukee: Developed the syllabus of the course:

- 469 Introduction to Computer Security: Undergraduate/Graduate

At Florida State University:

- technical leader of its NSA (National Security Agency) Center of Excellence in Information Security Education, from May 2000 on (only 14 universities and military academies had received this recognition in May 2000).
- Developed the syllabi of the courses on:
 - CIS 5371 Cryptography
 - EN4540 Computer Security
 - GS5891: Introduction to Computer Security

At University College London:

the MSc on Information Security:

- MSc on Information Security co-director from 2005–2007,

TEACHING

- Developed the course layout, i.e., requirements, electives and the tracks in: Computer Security, Cryptography, and Digital Rights Management,
- In 2004, developed the syllabi of the courses:
 - COMPGA01 Computer Security I,
 - COMPGA02 Computer Security II,
 - COMPGA03 Cryptography I (now called: Introduction to Cryptography),
 - COMPGA04 Cryptography II (now called: Advanced Cryptography),
 - COMPGA06 Network Security

the MSc on Information Security Management:

- In 2008, developed the course layout (i.e., requirements and electives),
- Developed the course: Information Security Management

Courses taught

Spring semester 1985 CS 154 Foundations of Computing Science and CS 431 Cryptology in Computing (University of New Mexico)

Fall semester 1986 IFT 6180 Cryptologie: Theorie et Applications (Cryptology: Theory and Applications) (Université de Montréal)

Spring semester 1987 IFT 1020 Programmation 2 (Programming) (Université de Montréal)

Fall semester 1987 262–535 Data Structures

Spring semester 1988 262–535 Data Structures and 262–657 – 004 Topics in Cryptology

Fall semester 1988 262–317 Discrete Information Structures and 262–351 Intermediate Programming

Spring semester 1989 262–351 Intermediate Programming and 262–759 Data Security

Fall semester 1989 262–704 Analysis of Algorithms

Spring semester 1990 262–315 Introduction to Computer Organization and Assembly Language Programming and 262–351 Intermediate Programming

Fall semester 1990 262–252 Computer Programming II and 262–790 – 001 Advanced Topics in Cryptography

Spring semester 1991 262–217 Discrete Information Structures and 262–252 Computer Programming II

Fall semester 1991 262–755 Information and Coding Theory

Spring semester 1992 262–252 Computer Programming II

Fall semester 1992 262–252 Computer Programming II

Spring semester 1993 262–790 Advanced Cryptography

Fall semester 1993 236350 Computer Security (Technion, Israel)

Fall semester 1994 262–217 Discrete Information Structures and 262–759 Data Security

Spring semester 1995 262–217 Discrete Information Structures and 262–790 – 004 Advanced Cryptography

Fall semester 1995 262–755 Information and Coding Theory

Spring semester 1996 262–620 Computer Networks

Fall semester 1996 262–217 Discrete Information Structures and 262–759 Data Security.

Spring semester 1997 262–790 – 002 Advanced Cryptography

Fall semester 1997 262–790 – 001 Internet and Network Security/Insecurity

Spring semester 1998 262–759 Data Security

Fall semester 1998 262–217 Discrete Information Structures and 262–790 – 001 Advanced Cryptography

Spring semester 1999 262–469 Introduction to Computer Security and 262–620 Computer Networks

Fall semester 1999 CIS 4930 and CIS 5930 Special Topics in Computer Science (Cryptography)

Spring semester 2000 CIS 4930 and CIS 5930 Special Topics in Computer Science (Computer Security)

TEACHING

Fall semester 2000 CIS 4930 and CIS 5930 Special Topics in Computer Science (Cryptography)

Fall semester 2001 CIS 4930 and CIS 5930 Special Topics in Computer Science (Cryptography)

Spring semester 2001 CEN4540 Computer Security and CGS5891 Introduction to Computer Security and CIS 4930 Special Topics in Computer Science (Ada)

Spring semester 2002 CEN4540 Computer Security and CGS5891 Introduction to Computer Security and CIS5920 Colloquium

Spring semester 2003 COP3502, Sections 05 - 08, Introduction to Computer Science

Spring semester 2004 CIS5930 Section 1 Applied Security

Term 2, 2005–2006: COMPGA02, Computer Security II

Term 2, 2006–2007: COMPGA02, Computer Security II

Term 2, 2007–2008: COMPGA02, Computer Security II

Term 2, 2008–2009: COMPGA02, Computer Security II and COMPGA04 Advanced Cryptography

Term 2, 2009–2010: COMPGA02, Computer Security II and COMPGA04 Advanced Cryptography

11 Enabling

11.1 Offices held in professional organizations

- Committee Chair: Antivirus Methods Congress: University members: 1991–1992,
- President of the IACR 2002 Election Committee,
- Member of the IACR 1992 and 2001 Nomination Committee,
- returning officer of the IACR 2001 elections,
- Director (elected) of the International Association of Cryptologic Research (IACR, which organizes Crypto, Eurocrypt, and Asiacrypt) terms 1992–1993, 2001–2003, and 2006–2008,
- Chair of the 2008 IACR BOD Subcommittee to recommend a list of candidates for the new Editor in Chief of the Journal of Cryptology,
- Chair of the Steering Committee of the:
 - International Conference on Cryptology and Network Security (2005–),
 - International Conference on Information Theoretic Security (2006–),
- Member of the Steering Committee of the International Workshop on Practice and Theory in Public Key Cryptography ,PKC, (2000–).

11.2 Editing and reviewing

Date	Details
1988–1991 and 1996–1998	Reviewer for Mathematical Reviews (American Mathematical Society)
1993–1995	Contributing editor for Computer & Communications Security Reviews
since January 2001	editor of The Journal of Computer Security
since July 2001	editor of Information Processing Letters
since May 2005	Editor-in-chief of the IEE Proceedings, Information Security (now called: IET Information Security)

ENABLING

since 2006
since 2010

editor of *Advanced Mathematics of Communications*
editor of *Computers & Security*

11.3 Conferences

- Program Chair of:
 - Crypto '94,
 - the ACM workshop on Scientific Aspects of Cyber Terrorism (SACT) 2002
 - the IACR International Workshop on Practice and Theory in Public Key Cryptography (PKC) 2003,
 - Co-Program Chair of the 4th International Conference on Cryptology and Network Security (CANS) 2005, and
 - the International Conference on Information Theoretic Security (ICITS) 2007.
- Member of the Program Committee of:

Eurocrypt '89, Crypto '90, Asiacrypt'91, Eurocrypt '92, ESORICS 92, Auscrypt'92, Eurocrypt '93, Eurocrypt '94, Asiacrypt '94, 1996 International Conference on Cryptology & Information Security, Eurocrypt '98, Public Key Cryptography '99, 1999 International Conference on Information and Communications Security (ICICS'99), Public Key Cryptography 2000, Asiacrypt 2000, Public Key Cryptography 2001, 6th Australasian Conference on Information Security and Privacy (ACISP) 2001, the 8th ACM Communications and Computer Security (CCS) Conference in 2001, RSA conference 2002 (Cryptographers Track), International Workshop on Practice and Theory in Public Key Cryptography (PKC) 2002, the 3rd International Workshop for Asian Public Key Infrastructure IWAP 2003, IEEE Globecom 2003 Communications Security Symposium, Indocrypt 2003, the IACR International Workshop on Practice and Theory in Public Key Cryptography (PKC) 2004, 9th Australasian Conference on Information Security and Privacy (ACISP) 2004, 4th Conference on Security in Communication Networks, SCN 2004, 7th International Information Security Conference, ISC 2004, 2004 International Conference on Information and Communications Security (ICICS'04), the IACR International Workshop on Practice and Theory in Public Key Cryptography (PKC) 2005, Financial Cryptography 2005, 10th Australasian Conference on Information Security and Privacy (ACISP) 2005, Malaysia Cryptography (MyCrypt) 2005, 2005 International Conference on Information and Communications Security (ICICS'05), RSA conference 2006 (Cryptographers Track), ACM Symposium on Information, Computer and Communications Security, 2006 (ASIACCS 2006), Critical Information Infrastructures Security, 2006, International Conference on Information and Communications Security (ICICS'06), Fifth International Workshop on Applied PKC (IWAP'06), Asiacrypt 2006, Indocrypt 2006, Australasian Information Security Workshop 2007, Financial Cryptography 2007, Public Key Cryptology 2007, 12th Australasian Conference on Information Security and Privacy (ACISP) 2007, Africacrypt 2010, 15th Australasian Conference on Information Security and Privacy (ACISP 2010), 12th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2011), Chinacrypt 2011.
- Tutorial Chair of the 9th ACM Conference on Computer and Communications Security, 2002.
- Publicity Chair of:
 - New Security Paradigms Workshop '96.
 - New Security Paradigms Workshop '97,
- NSF Research Panels (several times).

ENABLING

- Panel member of the:
 - Eurocrypt '92 panel: Trapdoor Primes and Moduli.
 - ESORICS 92 panel: Availability and Integrity (replacing T. Beth),
 - SPRC '93 panel: Block Ciphers vs. Stream Ciphers,
 - NCSC '93 panel: Summary of New Security Paradigms Workshop,
 - Crypto '94 panel (moderator): Securing an Electronic World: Are We Ready?
 - 9th IEEE Computer Security Foundations Workshop, 1996: Panel 3: What is an attack on a cryptographic protocol?
 - DIMACS Workshop on Design and Formal Verification of Security Protocols panel, 1997 (moderator): Design Versus Verification: is verification the wrong approach? (Submitted panel.) <http://dimacs.rutgers.edu/Workshops/Security/program2/yvo-panel.htm>
 - 23rd National Information Systems Security Conference, 2000: Issues in High Performance Computing Security – A Panel Discussion,
 - the 7th ACM Conference on Computer and Communications Security, 2000 (moderator): Which PKI (Public Key Infrastructure) is the right one? (Submitted panel.)
 - RFID panel at Financial Crypto 2007.
 - the Financial Crypto 2008 Panel (Moderator) on Real Electronic Cash versus Academic Electronic Cash versus Paper Cash (submitted panel)
- Session Chair at:

Crypto '87 (the informal session). Eurocrypt '88, Crypto '90, Asiacrypt'91, Eurocrypt '92, Auscrypt '92, SPRC '93, Eurocrypt '93, Eurocrypt '94, Workshop on Key Escrow (Karlsruhe, Germany, 1994), ISIT'94, New Security Paradigms Workshop '95, New Security Paradigms Workshop '96, Public Key Cryptography '99, Communications and Multimedia Security '99 (IFIP), Cryptography and Computational Number Theory Workshop (1999), 5th Australasian Conference on Information Security and Privacy 2000, Public Key Cryptography 2001, Workshop on Cryptographic Protocols, Monte Verita, Ascona (2001), 8th ACM Conference on Computer and Communications Security 2001, PKC 2002, RSA 2002 (Crypto Track), Crypto 2002, PKC 2003, ICEIS 2004, ACISP 2004, Cryptography Workshop (Luminy, 2004), PKC 2005, Financial Cryptography 2005, ACISP 2005, ISC 2005, CANS 2005, CRITIS 2006, Asiacrypt 2006, CANS 2006, Financial Cryptography 2007, Public Key Cryptography 2007, International Workshop on Coding and Cryptology 2007, ICITS 2007, Asiacrypt 2007, CANS 2007, Financial Cryptography 2008, ICITS 2008, CANS 2008, ICITS 2009, CANS 2009, Africacrypt 2010, Inscrypt 2010, ISC 2010.

11.4 Refereeing journal papers, conferences:

Crypto 83, The Twentieth Annual International Symposium on Fault-Tolerant Computing 1990, IEEE Transactions on Software Engineering (1991), IEEE Journal on Selected Areas in Communication (1988 and 1992), Australian Research Council (1992), 1st ACM Conference on Computer and Communications Security (1993), Journal of Computer Security (1992 – 1993), IEEE Transactions on Networking (1994), Electronics Letters (1990–1994), Computers & Mathematics with applications (1993 – 1994), Designs, Codes and Cryptography (1995), Information Processing Letters (1993 – 1995), Journal of Cryptology (1987–1996), 1997 International Symposium on Information Theory, Journal of the ACM (1997), Theoretical Computer Science (1997), John Wiley (preliminary book proposal review, 1998), 2000 International Symposium on Information Theory, IEEE

ENABLING

Transactions on Computers (1995 and 2001), The International Conference on Dependable Systems and Networks (DSN) 2002, IEEE Tr. Information Theory, (1983 – 1987, 2005), NSF (1991–2005), EPSRC (since 2007).

11.5 Other

- Application Leader of I2 (Internet 2) January–August 1997.
- Member of the Internet2 Security Working Group (2000–2004).
- Member of the Ecrypt Strategic Committee 2006–2007 and 2009–2011.

12 Invited talks

At conferences and workshops:

Date	Details
May 16–18, 1984	ICC 84, IEEE, Amsterdam, The Netherlands: <i>Cryptography : How to attack, what to protect?</i>
October 15–21, 1989	the “Monte Verita Seminar: Future Directions in Cryptography”, Ascona, Switzerland: <ul style="list-style-type: none">• “<i>Subliminal-free authentication in an international environment</i>”• “<i>Practical applications of zero-knowledge</i>”
November 23–24, 1989	Secondo Simposio su Stato e Prospettive della Ricerca crittografica in Italia: <i>Cryptanalysis of conventional and public key cryptosystems</i>
April 15–21, 1990	Mathematical Concepts of Dependable Systems, Oberwolfach, Germany: <ul style="list-style-type: none">• <i>An introduction to zero-knowledge proofs</i>• <i>Defining primitives for dependable communication</i>• <i>System security of identification</i>
July 3–6, 1991	E.I.S.S.-Workshop, Public-Key Cryptography: State of the Art and Future Direction, Oberwolfach, Germany: <i>Alternative approach to cryptanalysis</i>
November 23–25, 1992	ESORICS 92, Toulouse, France: <i>Breaking the traditional computer security research barriers</i>
December 13–16, 1992	Auscrypt '92, Gold Coast, Australia: <i>Threshold cryptosystems</i>
February 15–16, 1993	3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy: <i>Threshold cryptography</i>
June 22–24, 1994	the “Workshop on Key Escrow”, Karlsruhe, Germany: <ul style="list-style-type: none">• “<i>Threshold Decryption</i>”• “<i>Securing Traceability of Ciphertexts</i>”• “<i>What we Really Need</i>”

INVITED TALKS

- September 24–29, 1995 the “Cryptography Workshop 95”, Luminy, France:
- “Zero-Knowledge Secret Sharing, Reed-Solomon Codes and its Applications”
 - “Reliable Private Digital Libraries”
 - “Unconditionally Secure Identifications”
- August 11 - 13, 1997 the DARPA PI meeting on Wrappers & Composition, Lake Tahoe, California: *Critical Analysis of the Use of Redundancy to Achieve Survivability in the Presence of Malicious Attacks*
- September 17–19, 1997 Information Security, Tatsunokuchi, Japan: *Some recent research aspects of threshold cryptography*
- September 21–26, 1997 “Cryptography” workshop, Dagstuhl, Germany: *Generalizing proactive secret sharing*
- March 8–13, 1998 the “International Workshop on Cryptographic Protocols,” Monte Verita, Ascona, Switzerland: *New approaches to asymmetric traitor tracing*
- July 6–18, 1998 the “Coding and Cryptography” workshop, IMA (Institute for Mathematics and its Applications), University of Minnesota, : *Computational complexity and covert aspects of secret sharing and their applications*
- March 1–3 , 1999 the second International Workshop on Practice and Theory in Public Key Cryptography, Kamakura, Japan: *A Research Agenda for Public Key Cryptography for the Next Century*
- June 20–25, 1999 the 1999 IEEE Information Theory Workshop”, Kruger National Park, South Africa: *The Use of Coding and Information Theory in Threshold Cryptography*
- September 26 – October 1, 1999 the “Cryptography” workshop, Luminy, France: *Using Artificial Intelligence and Computational Complexity to study Secure Distributed Systems*
- November 22–26, 1999 the “Cryptography and Computational Number Theory” workshop, Singapore:
- Democratic Threshold Cryptography,
 - Asymmetric Multi-Party Cryptography.
- May 5–6, 2000 Tenth National Conference on Information Security, Hualien, Taiwan: *A definition of cryptography*
- March 18 - 23, 2001 the “Workshop on Cryptographic Protocols”, Monte Verita, Ascona, Switzerland: *Back to the Future in Information Security (Part II)*
- October 24–25, 2001 the “ARO Invitational Workshop on Information Assurance” George Mason University, Fairfax, Virginia: *Where are the weakest links and what is the best strategy to protect?*
- November 2–4, 2001 (feature speaker) at the 3rd Midwest Arithmetical Geometry in Cryptography Workshop, University of Illinois, Urbana-Champaign, Illinois,
- *Vector Spaces and Secure Authentication*
 - *From Vector Spaces and Modules to E-Commerce with Untrusted Insiders*
 - *Applications of Combinatorial Geometry to Practical Cryptography*
- September 22–27, 2002 “Cryptography”, Dagstuhl, Germany: *Efficient Proven Secure Steganography*
- October 30 - November 1, 2002 The Second International Workshop for Asian Public Key Infrastructure, Taipei, Taiwan: *Security problems with on-line revocation*

INVITED TALKS

- 9–11 July, 2003 8th Australasian Conference on Information Security and Privacy (ACISP), Wollongong, Australia: *On-Line Revocation and PKI*.
- April 13, 2004 (keynote speaker) the 2nd Workshop On Security In Information Systems (WOSIS), Porto, Portugal: *Towards a formal definition of cryptography*
- May 10–12, 2004 Fourth Conference on the Advanced Encryption Standard (AES), Bonn, Germany: *Complementation-like and cyclic properties of AES round functions*
- September 22–24, 2004 (keynote speaker) the Spanish bi-annual meeting in Computer Security & Cryptology (RECSI), Madrid: *Scientific Analysis of Cyber Terrorism*
- November 8–12, 2004 “Cryptography”, Luminy, France: *Towards a formal definition of cryptography*.
- July 4–6, 2005 ACISP 2005, Brisbane, Australia: *Potential impacts of a growing gap between theory and practice in information security*
- July 7, 2005 invited address at “RNSA Networks Workshop on Research Challenges in Information Security”, Brisbane, Australia: *Research challenges in network security beyond cryptography*
- October 2–5, 2005 “Symposium in honor of Jack van Lint”, Eindhoven, the Netherlands: *Beyond Error-Correcting Codes*.
- October 1 - October 12, 2005 NATO ASI, Yerevan, Armenia: *Security when routers are taken over by the adversary*
- October 16–19, 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, Awaji Island, Japan: *Unconditionally private and reliable communication in an untrusted network*
- November 29, 2005 “Quantum Optics,” Tokyo, Japan: *Perfect Privacy with Perfect Decryptability over a Wiretap Channel*
- December 1, 2005 “IPA Day on Cryptography” Tokyo, Japan: *Perfect Privacy with Perfect Decryptability over a Wiretap Channel*
- January 17, 2006 (keynote speaker) at the Australasian Information Security Workshop - Network Security, 2006, Hobart, Australia: *A Secure Internet with Hacked Routers in an Untrusted Network*
- May 21–26, 2006 AusCERT’s annual Asia-Pacific IT Security Conference, Gold Coast, Australia: *Academia vs. Business vs. Hackers in Information Security: the Case of Identity Theft*
- July 10, 2006 Combinatorics for Cryptography special session at the 31st Australasian Conference on Combinatorial Mathematics & Combinatorial Computing, Alice Springs, Australia: *Using combinatorics to achieve anonymity, reliability and privacy in networks*
- September 10–15, 2006 “From Security to Dependability” Dagstuhl, Germany: *Combining reliability and privacy in networks in general: a survey*
- October 9 - 13, 2006 “Number Theory and Cryptography - Open Problems” IPAM, UCLA, Los Angeles: *Trapdoor-Free RSA Like Assumption*
- March 4–9, 2007 “Cryptographic Protocols” Bertinoro, Italy: *The Need for Automated Design of Cryptographic Protocols*
- June 8–13, 2007 “International Workshop on Coding and Cryptology” Wuyishan, China: *Perfect Privacy with Perfect Decryptability over a Wiretap Channel*

INVITED TALKS

- September 16–21, 2007 “Cryptography” Dagstuhl, Germany: *Applying Recreational Mathematics to Secure Multiparty Computation*
- November 13, 2008 “IPA Day on Cryptography” Tokyo, Japan: *Applying Recreational Mathematics to Secure Multiparty Computation*
- December 12–14, 2008 “NTU-Tsinghua Workshop on Discrete Mathematics & Theoretical Computer Science 2008” Singapore: *Modern Cryptography: The State of the Art*
- May 24–29, 2009 “2009 Workshop on Cryptographic Protocols and Public-Key Cryptography” Bertinoro, Italy: 60 years of scientific research in cryptography: a reflection
- July 26–31, 2009 “Classical and Quantum Information Assurance Foundations and Practice” Dagstuhl, Germany: Towards Post-Quantum Key Exchange and Public Key Encryption Schemes using Non-Abelian Groups
- June 28-30, 2011 The 8th IEEE/FTRA International Conference on Secure and Trust Computing, data management, and Applications: Title TBA

At seminar series:

Date	Details
September 13–15, 1983	IBM Yorktown Heights, New York, U.S.A.: “ <i>Analytic characteristics of DES</i> ”.
September 16, 1983	Bell Labs, Murray Hill, New Jersey, U.S.A.: “ <i>Analytic characteristics of DES</i> ”.
September 17–25, 1983	the Univerité de Montréal, Québec, Canada from : “ <i>Analytic characteristics of DES</i> ”.
August 27–29, 1984	the NBS (National Bureau of Standards), Department of Commerce, Gaithersburg, Maryland, U.S.A., from : “ <i>Cryptography in Belgium</i> ”.
June 13–14, 1985	the “CWI”, Amsterdam, The Netherlands: “ <i>DES</i> ”.
July 9, 1985	“Philips Usfa”, Eindhoven, The Netherlands: “ <i>Over de veiligheid van de data encryption standard</i> ” (“ <i>About the security of the data encryption standard</i> ”).
June 13, 1986	the “CWI”, Amsterdam, The Netherlands: “ <i>Additional properties on the S-boxes of the DES</i> ”.
October 30, 1986	the University of Waterloo, Dept. of Electrical Engineering, Waterloo, Ontario, Canada, ,: “ <i>The data encryption standard</i> ”.
February 4–6, 1987	the University of Western Ontario, Dept. of Computer Science, London, Ontario, Canada: “ <i>DES</i> ”.
April 1, 1987	Queen’s University, Dept. of Electrical Engineering, Kingston, Ontario, Canada: “ <i>Special uses and abuses of the Fiat–Shamir Identification Protocol</i> ”.
June 3, 1987	the NBS (National Bureau of Standards), Department of Commerce, Gaithersburg, Maryland, U.S.A.: “ <i>Special uses and abuses of the Fiat–Shamir Passport Protocol</i> ”.
June 13–14, 1988	the University of Karlsruhe, Fakultät für Informatik, Karlsruhe, Germany: “ <i>Protecting against Abuses of Cryptosystems</i> ”.
June 21, 1988	Philips Research Laboratory, Brussels, Belgium: “ <i>Protecting against Abuses of Cryptosystems</i> ”.

INVITED TALKS

- June 26–July 25, 1988 University of London, Department of Mathematics, Royal Holloway and Bedford New College, Great Britain:
- “*An introduction to zero-knowledge*”
 - “*Zero-knowledge and identification*”
 - “*Zero-knowledge and subliminal-freeness*”.
- June 28, 1988 Oxford University, Merton College and Mathematical Institute, Oxford, Great Britain: “*Protecting against Abuses of Crypto-systems*”.
- July 1, 1988 University College Cardiff, Dept. of Computing Mathematics, Great Britain:
- “*Security Problems with the Unforgeable (Feige–)Fiat–Shamir Proofs of Identity and How to Overcome Them*”
 - “*Subliminal-free Authentication and Signature*”.
- July 4–8, 1988 CWI (Centre for Mathematics and Computer Science), Amsterdam, The Netherlands:
- “*Security Problems with the Unforgeable (Feige–)Fiat–Shamir Proofs of Identity and How to Overcome Them*”
 - “*Protecting against Abuses of Crypto-systems*”.
- July 20, 1988 Hewlett Packard, Bristol, Great Britain: “*DES and block ciphers*”.
- July 21, 1988 GE (General Electric) Information Services, GEISCO limited, London, Great Britain: “*Security Problems with the Unforgeable (Feige–)Fiat–Shamir Proofs of Identity and How to Overcome Them*”.
- June 23, 1989 University of Karlsruhe, Fakultät für Informatik, Karlsruhe, West-Germany, “*Viruses in the Computer World,*”
- July 3, 1989 the Institut für Signal- und Informationsverarbeitung, ETH-Zentrum, Zürich, Switzerland: “*Subliminal-free Authentication*”.
- July 7, 1989 University of Karlsruhe, Fakultät für Informatik, Karlsruhe, West-Germany, “*Key Management in a Group Oriented Society,*” .
- June 10, 1991 Philips Research Laboratory, Louvain-la-Neuve, Belgium, , at the Université Catholique de Louvain, “*The Deep Aspect of Deep Coin Tosses in Zero-Knowledge*”.
- June 14, 1991 the Fondazione Ugo Bordoni, Rome, Italy: “*The Deep Aspect of Deep Coin Tosses in Zero-Knowledge*”.
- July 2, 1991 the Fakultät für Informatik, University of Karlsruhe, Germany: “*Unconditional Subliminal-Freeness in Unconditional Authentication Systems,*” .
- July 18, 22, & 29, 1991 University of New South Wales, ADFA, Department of Computer Science, Canberra, Australia:
- “*Unconditional Subliminal-Freeness in Unconditional Authentication Systems,*”
 - “*Perfect Zero-Knowledge Sharing Schemes over any Finite Abelian Group,*”
 - “*Electronic Public Notary: An Overview,*”

INVITED TALKS

- August 14–16, 1991 the University of New England, Armidale, Australia:
- “*Unconditional Subliminal-Freeness in Unconditional Authentication Systems*,”
 - “*Perfect Zero-Knowledge Sharing Schemes over any Finite Abelian Group*,”
 - “*An Efficient Zero-Knowledge Scheme for the Discrete Logarithm based on Smooth Numbers*,”
- August 29, 1991 University of New South Wales, ADFA, Department of Computer Science, Canberra, Australia: “*An Efficient Zero-Knowledge Scheme for the Discrete Logarithm based on Smooth Numbers*,”
- October 4, 1991 University of Wisconsin—Milwaukee, Fall Computer Science Seminars, “*Unconditional Subliminal-Freeness in Unconditional Authentication Systems*,” .
- November 15, 1991 NTT Communications and Information Processing Lab., Nippon Telegraph and Telephone Corp., Yokosuka–Shi, Kanagawa, Japan: “*Perfect Zero-Knowledge Sharing Schemes*”.
- November 15, 1991 Mitsubishi Electric Corporation, Computer & Information Systems Lab., Kamakura, Kanagawa, Japan: “*Reliable Parallel Multisignatures*”.
- January 7, 1992 the Université de Montréal, Québec, Canada: “*Unconditional Subliminal-Freeness in Unconditional Authentication Systems*,” .
- April 27, 1992 Department of Computer Science and Engineering, University of Nebraska – Lincoln: “*Unconditional Subliminal-Freeness in Unconditional Authentication Systems*,” .
- May 4, 1992 the Fondazione Ugo Bordoni, Rome, Italy: “*Threshold Signatures as Secure as RSA*”.
- May 20, 1992 the Fakultät für Informatik, University of Karlsruhe, Germany: “*Threshold Signatures as Secure as RSA, or the Difficulty in Combining Two Security Primitives*,” .
- June 25, 1992 University of London, Department of Mathematics, Royal Holloway and Bedford New College, Great Britain: “*Threshold Signatures as Secure as RSA, or the Difficulty in Combining Two Security Primitives*,” .
- July 10, 1992 University of Cambridge, Computer Laboratory, Great Britain: “*Unconditional Subliminal-Freeness in Unconditional Authentication Systems*”.
- November 27, 1992 LAAS, Toulouse, France: “*Distributed Reliable Threshold Multisignatures*”.
- December 18, 1992 University of Wollongong, Wollongong, New South Wales: “*Towards computer security by redefining what a computer is*,” .
- January 14, 1993 University of Cambridge, Computer Laboratory, Great Britain: “*Threshold Cryptosystems*”.
- April 12, 1993 University of Wisconsin – Madison, U.S.A., , at the Graduate/Faculty Colloquium of the Department of Electrical Engineering and Computer Engineering: “*Computer Viruses and Computer Security*”.
- June 7, 1993 Delab, University of Trondheim, Norway, ;: “*Threshold Cryptosystems*”.
- June 24, 1993 University of London, Department of Mathematics, Royal Holloway, Great Britain: “*Unconditionally secure threshold authentication*,” .
- July 8, 1993 University of Cambridge, Computer Laboratory, Great Britain: “*Towards Practical Proven Secure Authenticated Key Distribution*”.

INVITED TALKS

- August 18, 1993 Stanford University, Information Systems Laboratory, California: *“Threshold Decryption: an Alternative to the Clipper Chip”*.
- September 24, 1993 NIST (National Institute of Standards and Technology), Department of Commerce, Gaithersburg, Maryland, U.S.A.: *“Threshold Decryption: an Alternative to the Clipper Chip”*.
- November 16, 1993 Technion, Computer Science Department, Israel: *“Zero-knowledge sharing and its applications,”* .
- April 29, 1994 Dept. of Combinatorics and Optimization, University of Waterloo, Canada: *“Zero-knowledge sharing and its applications,”* .
- June 2, 1994 Dipartimento di Informatica ed Applicazioni, Università di Salerno, Italy, *“Threshold decryption: an alternative to the Clipper Chip,”* .
- December 6, 1994 the Department of Informatics, University of Bergen, Bergen, Norway, ,:
 - *“Zero-knowledge secret sharing, Reed-Solomon codes and its applications,”*
 - *“Securing Traceability of Ciphertexts — Towards a Secure Software Key Escrow System,”*
- December 8, 1994 the Department of Information Theory, Lund University, Lund, Sweden: *“Zero-knowledge secret sharing, Reed-Solomon codes and its applications,”*
- January 5, 1995 the Laboratoire d’informatique, École Normale Supérieure, Paris, France: *“Zero-knowledge secret sharing, Reed-Solomon codes and its applications”*.
- January 13, 1995 Université Catholique de Louvain, Louvain-la-Neuve, Belgium, *“Authentication with arbitration and its generalizations,”* .
- June 6, 15 & 20, 1995 University of London, Department of Mathematics, Royal Holloway, Great Britain,
 - *“Zero-knowledge secret sharing, Reed-Solomon codes and applications,”*
 - *“Securing Traceability of Ciphertexts — Towards a Secure Software Key Escrow System,”*
 - *“Multiplicative non-abelian sharing schemes and their applications to threshold cryptography,”*
- June 23, 1995 University of Cambridge, Computer Laboratory, Great Britain: *“Securing Traceability of Ciphertexts — Towards a Secure Software Key Escrow System”*.
- June 4, 1996 University of Cambridge, Isaac Newton Institute on Computer Security, Cryptology and Coding Theory, *“Reliable Private Digital Libraries,”* .
- June 20, 1996 Université Catholique de Louvain, Louvain-la-Neuve, Belgium, *“Securing Law Enforcement and Civil Trust”*.
- July 23 & 30 1996 Royal Holloway, Department of Mathematics, Great Britain, ,
 - *“Securing Law Enforcement and Civil Trust,”*
 - *“Reliable Private Digital Libraries,”*
- May 22, 1997 University of Piraeus, Greece: *“Democracy and Cryptography,”*
- June 3, 1997 Japan Advanced Institute of Science and Technology, Nomi-gun, Ishikawa, Japan: *“Using Algebra and Combinatorics to Achieve Co-Signing and Co-Decryption, Called Threshold Cryptography.,”*
- June 12, 1997 Telecommunications Advancement Organization of Japan, Tokyo, Japan: *“Threshold Cryptography: a survey”*.

INVITED TALKS

- June 26, July 1, 21 & 23, 1997 University of Wollongong, CRYPT research group, ,
- “*Technical Aspects of Threshold Cryptography,*”
 - “*Conference Key Distribution,*”
 - “*Unconditionally Secure Identification,*”
- June 24, 1997 University of Wollongong, Computer Science, Australia, “*Threshold Cryptography,*”
- July 24, 1997 University of Western Sydney at Penrith, Australia: “*Using Algebra and Combinatorics to Achieve Co-Signing and Co-Decryption, Called Threshold Cryptography.*”
- August 8, 1997 Queensland University of Technology, Information Security Research Centre, Australia:
- “*Some Aspects of Threshold Cryptography,*”
 - “*Philosophical, Political, and Technical Aspects of Key Escrow and its Alternatives,*”
- October 24, 1997 Purdue University, Department of Computer Sciences, West Lafayette, Indiana: “*The Need to License and Restrict the Users of General Purpose Computers.*”
- December 15, 1997 Hewlett Packard, Bristol, Great Britain, , at the HP Security and Crypto Workshop: “*A Research Agenda on Cryptography for the Next Century.*”
- April 24, 1998 University of Illinois at Chicago, Department of Electrical Engineering and Computer Science: “*Society oriented cryptography.*”
- May 12, 1998 UCLA (University of California Los Angeles), Computer Science Department: “*Society oriented cryptography.*”
- May 23–26, 1998 the Fakultät für Informatik, University of Karlsruhe: “*Society oriented cryptography.*”
- June 18, 1998 the University of London, Department of Mathematics, Royal Holloway, Great Britain: “*Audio, cerebral and optical cryptography,*”
- October 23 & 24, 1998 the State Key Laboratory of Information Security, Graduate School of the University of Science and Technology of China, Beijing:
- “*Society oriented cryptography,*”
 - “*Generalizing proactive secret sharing,*”
- December 22, 1998 Japan Advanced Institute of Science and Technology, Nomi-gun, Ishikawa, Japan: “*An alternative model to secure distributed computation and its implications,*”
- January 7, 1999 Telecommunications Advancement Organization of Japan, Tokyo, Japan, ,: “*A new model for secure reliable multiparty computation and its implications.*”
- January 8, 1999 Tokyo Institute of Technology, Tokyo, ,: “*Equitable key escrow with limited time span,*”
- January 14, 1999 Japan Advanced Institute of Science and Technology, Nomi-gun, Ishikawa, Japan, “*Information-theoretic secure identification,*”
- March 12, 1999 NTT Communications and Information Processing Lab., Nippon Telegraph and Telephone Corp., Yokosuka–Shi, Kanagawa, Japan:
- “*Society oriented cryptography,*”
 - “*Audio and optical cryptography,*”
 - “*Unconditionally secure identification.*”

INVITED TALKS

- July 5, 1999 the University of London, Department of Mathematics, Royal Holloway, Great Britain:
• “*On Cyber Terrorism and Information Warfare against Civilian Targets,*”
• “*Unconditional Security Without Secret Keys,*”
- September 22, 1999 Université Catholique de Louvain, Microelectronics Laboratory, Louvain-la-Neuve, Belgium:
• “*Audio and Optical Cryptography,*”
• “*Unconditionally Secure Identification*”.
- October 22, 1999 AT&T Shannon Research Lab, Florham Park, New Jersey: “*Using Artificial Intelligence and Computational Complexity to study Secure Distributed Systems,*”
- October 27, 1999 George Mason University, Information and Software Engineering Department, Fairfax, Virginia: “*Society Oriented Cryptography and Electronic Commerce*”.
- November 5, 1999 University of Wisconsin – Milwaukee, Department of Electrical Engineering and Computer Science, ,: “*Using Artificial Intelligence and Computational Complexity to study Secure Distributed Computation*”
- November 19, 1999 National University of Singapore, School of Computing, Singapore:
• “*Using Artificial Intelligence and Computational Complexity to study Secure Distributed Systems,*”
• “*Unconditionally Secure Identification*”.
- December 20, 1999 Tokyo Institute of Technology, Department of Electrical and Electronic Engineering, Tokyo, Japan: “*Democratic Threshold Cryptography,*”
- May 4, 2000 National Dong Hwa University, Department of Electrical Engineering, Hualien, Taiwan, ,:
• “*Society Oriented Cryptography and Electronic Commerce,*”
• “*Democratic Threshold Cryptography,*”
• “*Using Artificial Intelligence and Computational Complexity to study Secure Distributed Systems.*”
- June 1, 2000 the University of London, Department of Mathematics, Royal Holloway, Great Britain: “*How to break Jakobsson’s practical Eurocrypt ’98 MIX and design a new one,*”
- June 9, 16 & 23, 2000 the University of Wollongong, Computer Science, Australia:
• “*How to break Jakobsson’s practical Eurocrypt ’98 MIX and design a new one,*”
• “*Democratic threshold cryptography,*”
• “*Using artificial intelligence and computational complexity to study secure distributed systems,*”
- June 19, 2000 the Laboratory for Information and Network Security, School of Network Computing, Monash University, Melbourne, Australia, ,: “*Society oriented cryptography and electronic commerce*”.

INVITED TALKS

- July 18 & 21, 2000 Queensland University of Technology, Information Security Research Centre, Brisbane, Australia:
- “*On a definition of cryptography,*”
 - “*Binary and Non-Binary Audio Cryptography,*”
- September 15, 2000 Mathematics Colloquium lecture at the Department of Mathematics, Florida State University: “*Using mathematics to achieve a reliable internet secure against conspiring insiders*”.
- January 5, 2001 Certicom, Mississauga, Ontario, Canada: “*Defending PKI against hackers,*”
- March 7, 2001 Purdue University, Department of Computer Sciences, West Lafayette, Indiana: “*Back to the Future in Information Security*”.
- March 13, 2001 John Hopkins University, Department of Computer Science, Baltimore, Maryland: “*The Importance of Appropriate Models to Information Security*”.
- May 2, 2001 Université Catholique de Louvain, Microelectronics Laboratory, Louvain-la-Neuve, Belgium: “*Anonymity in a non-broadcast environment*”.
- December 7, 2002 Ibaraki University, Department of Computer and Information Sciences, Hitachi, Ibaraki, Japan, ,: “*Anonymity in a non-broadcast environment,*”
- February 1, 2002 Katholieke Universiteit Leuven, Department of Electrical Engineering, Belgium: “*The next 25 years in cryptography*”.
- February 8, 2002 ETH, Computer Science, Zürich, Switzerland, ,: “*Scientific Issues of Cyber Terrorism*”.
- May 6, 2002 Université Catholique de Louvain, Microelectronics Laboratory, Louvain-la-Neuve, Belgium: “*Perfectly Secure Message Transmission Revisited*”.
- May 8, 2002 Universität Essen, Institut für Experimentelle Mathematik, Essen, Germany: “*Perfectly Secure Message Transmission Revisited*”.
- May 14, 2002 Stanford University, Security Laboratory (Department of Computer Science), Stanford, California, ,: “*Using economics and artificial intelligence to model threats and security in distributed computing*” at the Stanford Security Seminar.
- June 27, 2002 Université Catholique de Louvain, Microelectronics Laboratory, Louvain-la-Neuve, Belgium: “*Using economics and artificial intelligence to model threats and security in distributed environments,*”
- August 16, 2002 the Laboratories for Information Technology, Singapore: “*Perfectly Secure Message Transmission Revisited*”.
- September 10, 2002 Gemplus, Rome, Italy: “*Verifiable Democracy—a protocol to secure an electronic legislature*”.
- October 1, 2002 University of Cambridge, Computer Laboratory, Great Britain: “*Verifiable Democracy*”.
- September 30, 2002 Microsoft Research, Cambridge, Great Britain “*Efficient Proven Secure Steganography,*”
- October 4, 2002 the University of London, Department of Mathematics, Royal Holloway, Great Britain: “*Efficient Proven Secure Steganography,*”
- October 11, 2002 Université Catholique de Louvain, Microelectronics Laboratory, Louvain-la-Neuve, Belgium: “*Cryptanalysis of the CMU “Proven Secure Steganography” and Efficient Proven Secure Schemes*”.

INVITED TALKS

- November 8 & 15, 2002 University of North Carolina at Charlotte, Department of Software and Information Systems, USA, :
- “*Redistribution of mechanical secret shares,*”
 - “*Using economics and artificial intelligence to identify critical infrastructures,*”
- June 27, 2003 the University of Wollongong, Computer Science, Australia, “*Using economics and artificial intelligence to identify critical infrastructures,*”
- July 18, 2003 Macquarie University, Department of Computing, Australia, “*Using economics and artificial intelligence to identify critical infrastructures,*”
- August 5, 2003 Queensland University of Technology, Information Security Research Centre, Brisbane, Australia, “*Using economics and artificial intelligence to identify critical infrastructures,*”
- October 10, 2003 Université Catholique de Louvain, Microelectronics Laboratory, Louvain-la-Neuve, Belgium: “*Verifiable Democracy — a protocol to secure a virtual legislature*”.
- November 6, 2003 Universität Essen, Institut für Experimentelle Mathematik, Essen, Germany, ,: “*Robust and Secure Communications and its Impact on PKI*”.
- October 20 & November 10, 2003 Ruhr-Universität Bochum, Institute for Information Security and Cryptography, Bochum, Germany:
- “*Using economics and artificial intelligence to identify critical infrastructures,*”
 - “*Cryptanalysis of Several of the UCLA Watermarking Schemes for Intellectual Property Protection of Digital Circuits/Designs,*”
- December 5, 2003 Tokyo Institute of Technology, Department of Communications and Integrated Systems, Tokyo, Japan: “*Efficient Perfect Digital Steganography*”.
- December 19, 2003 NTT Communications and Information Processing Lab., Nippon Telegraph and Telephone Corp., Yokosuka-Shi, Kanagawa, Japan: “*Efficient Perfect Digital Steganography*”.
- December 26, 2003 University of Tokyo, Institute of Industrial Science, Tokyo, Japan: “*Efficient Perfect Digital Steganography*”.
- December 11, 2003 Ibaraki University, Department of Computer and Information Sciences, Hitachi, Ibaraki, Japan: “*Using economics and artificial intelligence to identify critical infrastructures,*”
- June 21 & June 30, 2004 the University of Wollongong, Computer Science, Australia:
- “*Towards a Formal Definition of Cryptography,*”
 - “*Escrowed Anonymity,*”
- August 8, 2004 Macquarie University, Department of Computing, Australia, “*Towards a Formal Definition of Cryptography*” .
- August 12, 2004 UCLA (University of California Los Angeles), Electrical Engineering Department: “*Identifying Critical Infrastructures*”
- November 23, 2004 University of Cambridge, Computer Laboratory, Great Britain, : “*Questioning the Usefulness of Identity-based Key Cryptography*”.
- November 25, 2004 the Département d’informatique, École Normale Supérieure, Paris, France: “*Escrowable Anonymity*”.

INVITED TALKS

- December 1, 2004 the Department of Mathematics, University College London, UK: *“An Introduction to Threshold Cryptography”*.
- March 16, 2005 British Telecom, Ipswich, UK: *“Modeling Critical Infrastructures”*.
- April 15, 2005 Macquarie University, Department of Computing, Australia, *“Efficient Perfect Digital Steganography”*
- June 8, 2005 Universidad Rey Juan Carlos, Applied Computational Mathematics and Engineering, Madrid, Spain: *“Models for Critical Infrastructures and Methods to Measure their Robustness”*.
- June 17, 2005 the University of Wollongong, Telecommunication and Information Technology Research Institute, Wollongong, Australia: *“The Future of Cryptography for the Next 25 Years,”*
- June 29 & August 2, 2005 Queensland University of Technology, Information Security Institute, Brisbane, Australia:
 - *“Robustness in Security: the case of networks and operations,”*
 - *“The future of cryptography for the next 25 years,”*
- November 28, 2005 University of Tokyo, Institute of Industrial Science, Tokyo, Japan: *“Escrowed Anonymity,”* .
- November 30, 2005 Tokyo Institute of Technology, Department of Communications and Integrated Systems, Tokyo, Japan: *“Denial of Service and Security in Computer Networks: the partial broadcast case.”*
- December 7, 2005 Ibaraki University, Department of Computer and Information Sciences, Hitachi, Japan: *“Denial of Service and Security in Computer Networks: the point-to-point case”*,
- December 31, 2005 Tsinghua University, Department of Computer Science, Beijing China: with lecture *“Denial of Service and Security in Computer Networks: the point-to-point case,”*
- January 3, 2006 Shandong University, Department of Mathematics, Jinan, China: *“E-voting without revealing the number of votes,”*
- June 22, 2006 the Département d’informatique, École Normale Supérieure, Paris, France: *“Pairing Based Threshold Cryptography Improving on Libert-Quisquater and Baek-Zheng”*.
- July 26, 2006 University of Wollongong, Telecommunication and Information Technology Research Institute, Wollongong, Australia: *“How to censor Big Brother?,”*
- July 14 & 21, 2006 Macquarie University, Department of Computing, Australia,
 - *“Electronic voting: starting over?”*
 - *“How to censor Big Brother?”*
- November 27, 2006 Tokyo Institute of Technology, Department of Communications and Integrated Systems, Tokyo, Japan: *“Pairing Based Threshold Cryptography Improving on Libert-Quisquater and Baek-Zheng.”*
- November 24, 2006 National Institute of Advanced Industrial Science and Technology, Research Center for Information Security, Tokyo, Japan: *“Pairing Based Threshold Cryptography Improving on Libert-Quisquater and Baek-Zheng.”*
- November 28, 2006 Ibaraki University, Department of Computer and Information Sciences, Hitachi, Japan, *“Privacy Preserving Censorship,”*

INVITED TALKS

- January 2, 2007 University of Wollongong, Telecommunication and Information Technology Research Institute, Wollongong, Australia, : *"Non-Degrading Erasure-Tolerant Information Authentication with an Application to Multicast Stream Authentication over Lossy Channels."*
- January 5, 2007 Macquarie University, Department of Computing, Australia, *"Non-Degrading Erasure-Tolerant Information Authentication with an Application to Multicast Stream Authentication over Lossy Channels,"*
- January 23, 2007 University of Cambridge, Computer Laboratory, Great Britain: *"Privacy Preserving Censorship."*
- March 19, 2007 University of La Laguna, Department of Statistics, Operations Research and Computing, Tenerife, Spain, *"Cryptography, Graph Theory and Reliable Communications,"*
- March 22, 2007 Université de Caen, Département d'informatique, Caen, France: *"Privacy Preserving Censorship."*
- April 13, 2007 Shandong University, Department of Mathematics, Jinan, China, lecture: *"Non-Degrading Erasure-Tolerant Information Authentication with an Application to Multicast Stream Authentication over Lossy Channels,"*
- March 28, 2007 Tsinghua University, Department of Computer Science, Beijing, China, *"Two zero-knowledge interactive proofs for problems in graph theory with applications in cryptography,"*
- May 3, 2007 Nanyang Technological University, School of Physical & Mathematical Sciences, Singapore, *"10 Years of the Efficient BD-II Group Key Exchange Protocol,"*
- July 13, 2007 Macquarie University, Department of Computing, Australia, *"10 Years of the Efficient BD-II Group Key Exchange Protocol,"*
- August 29, 2007 University of Illinois at Chicago, Department of Computer Science and RITES, Chicago, Illinois, *"From Relative Security to Perceived Security,"*
- September 5, 2007 Purdue University, Department of Computer Sciences, West Lafayette, Indiana: *"Applying Recreational Mathematics to Cryptography."*
- October 5, 2007 Center For Mathematical Modeling, Universidad de Chile, Santiago: *"Applying Recreational Mathematics to Secure Multiparty Computation"*
- November 9, 2007 Nanyang Technological University, School of Physical & Mathematical Sciences, Singapore, Singapore, *"Pairing Based Threshold Cryptography Improving on Libert-Quisquater and Baek-Zheng,"*
- November 16, 2007 Japan Advanced Institute of Science and Technology, Nomi-gun, Ishikawa, Japan: *"Applying Recreational Mathematics to Secure Multiparty Computation."*
- November 19, 2007 National Institute of Advanced Industrial Science and Technology, Research Center for Information Security, Tokyo, Japan: *"Applying Recreational Mathematics to Secure Multiparty Computation."*
- November 21 & 28, 2007 Ibaraki University, Department of Computer and Information Sciences, Hitachi, Japan:
 - *"10 Years of the Efficient BD-II Group Key Exchange Protocol,"*
 - *"Applying Recreational Mathematics to Secure Multiparty Computation,"*

INVITED TALKS

- March 14, 2008 Tokyo Institute of Technology, Department of Communications and Integrated Systems, Tokyo, Japan: “*Non-Degrading Erasure-Tolerant Information Authentication with an Application to Multicast Stream Authentication over Lossy Channels,*”
- March 20, 2008 Japan Advanced Institute of Science and Technology, Nomi-gun, Ishikawa, Japan: “*Revisiting pairing based group key exchange,*”
- March 20, 2008 National Institute of Informatics, Tokyo, Japan: “*Research on combining privacy and survivability in abstract data networks,*”
- April 9, 2008 Technical University Eindhoven, Eindhoven, the Netherlands, Department of Mathematics and Computing Science: “*Applying Recreational Mathematics to Secure Multiparty Computation,*”
- May 16, 2008 University of Calgary, Department of Computer Science: “*Applying Recreational Mathematics to Secure Multiparty Computation.*”
- June 5, 2008 University of Paris 8, Department of Mathematics, France: “*Applying Recreational Mathematics to Secure Multiparty Computation.*”
- July 11, 2008 ETH, Department of Computer Science: “*Applying Recreational Mathematics to Secure Multiparty Computation.*”
- September 5, 2008 Nanyang Technological University, School of Physical & Mathematical Sciences, Singapore, Singapore: *Revisiting the Karnin, Greene and Hellman Bounds.*”
- September 19, 2008 Nanyang Technological University, School of Physical & Mathematical Sciences, Singapore, Singapore: “*Non-Degrading Erasure-Tolerant Information Authentication with an Application to Multicast Stream Authentication over Lossy Channels,*”
- October 3, 2008 Macquarie University, Department of Computing, Australia, “*Applying Recreational Mathematics to Secure Multiparty Computation.*”
- November 4, 2008 University of Bristol, Department of Computer Science, UK, “*Applying Recreational Mathematics to Secure Multiparty Computation.*”
- November 10, 2008 University College London, Adastral Park Seminar Series, UK, “*Applying Recreational Mathematics to Secure Multiparty Computation.*”
- November 14, 2008 National Institute of Advanced Industrial Science and Technology, Research Center for Information Security, Tokyo, Japan: “*Revisiting pairing based group key exchange.*”
- December 17, 2008 Ibaraki University, Department of Computer and Information Sciences, Hitachi, Japan: “*The Future of Cryptography is Bright, isn't It?.*”
- December 22, 2008 NTT Musashino Research and Development Center, Japan:
 - A CCA Secure Hybrid Damgård’s ElGamal Encryption
 - Revisiting pairing based group key exchange
- March 10, 2009 the University of London, Department of Mathematics, Royal Holloway, Great Britain: “*Applying Recreational Mathematics to Secure Multiparty Computation*”
- October 22, 2009 NetentSec, Beijing, China: “*Is Our IT Society Getting Less Secure?*”
- April 7, 2010 University-Purdue University Indianapolis, Department of Electrical & Computer Engineering: “*60 years of scientific research in cryptography: a reflection*”
- April 7, 2010 Purdue University, Department of Computer Sciences, West Lafayette, Indiana: “*60 years of scientific research in cryptography: a reflection*”

INVITED TALKS

- April 22, 2010 Tsinghua University, Beijing, China, Institute for Theoretical Computer Science:
“60 years of scientific research in cryptography: a reflection”
- June 17, 2010 Ibaraki University, Department of Computer and Information Sciences, Hitachi,
Japan: *“Simple and Communication Complexity Efficient Almost Secure and
Perfectly Secure Message Transmission Schemes”*
- August 12, 2010 George Mason University, Center for Secure Information Systems, Fairfax, Vir-
ginia: *“Challenging Issues for Privacy and Cryptography”*
- September 17, 2010 BT, Adastral Park, UK: *“Challenging Issues for Privacy and Cryptography in
Europe”*