Curriculum Vitae

Yvo Desmedt

1 Personal Details

Name:	Yvo Desmedt
h-index:	47
Erdös number:	2
Present appointment:	Jonsson Distinguished Professor Department of Computer Science The University of Texas at Dallas, USA Date of appointment: August 2012

First Cryptographer with a Wikipedia page in Texas, i.e., since 2010

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-July 2009	BT-Chair of Information Security	University College London, U.K.
August 2009-March 2017	Chair of Information Communication Technology	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.
December 1996–January 1997	Consultant for Trusted Information Systems	Maryland, USA (5 days total)
June 1997–July 1997	Professorial Fellow, Department of Computer Science	University of Wollongong, New South Wales, Australia
June 1997–November 1997	Consultant for Trusted Information Systems	Maryland, USA (3 days total)
March 1998–July 1999	Consultant for Trusted Information Systems	Maryland, USA (19 days total)
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.
August 2000	Consultant for the State of Florida	(2 days)
May–June, 2002	Consultant for George Mason University	(15 days total)
June–July 2002	Visiting Professor, Department of Electrical Engineering	Université Catholique de Louvain, Belgium

OTHER APPOINTMENTS AND AFFILIATIONS

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	JSPS Fellow	Ibaraki University, Japan
since August 2004	Courtesy Professor, Department of Computer Science	Florida State University, U.S.A.
November 2009–October 2010	Invited Senior Research Scientist	Research Center for Information Security, AIST, Japan
July 2013	Consultant for EpicOne	Houston, Texas, USA (10 hours total)
February 2014–March 2014	Consultant for Noumena Research Ventures Ltd.	Croydon, UK (4 days total)
May 2015–July 2015	Consultant for Zendo	Prague, Czech Republic (9 hours total)
April 2017–March 2022	Honorary Professor of Computer Science	University College London, UK
June 2020–July 2021	Consultant for Cryptoquant	Dallas, USA (6 hours total)

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
2016	Member of Royal Flemish Academy of Belgium for Science and the Arts	Current members

6 Professional memberships

Organization	Beginning Date	End Date
International Association of Cryptologic Research	1984	today
IEEE	2015	today
ACM	2016	today

7 Publications

7.1 Books

[1] Y. Desmedt. Instelbare scramblers. Master's thesis, Katholieke Universiteit Leuven, Belgium, July 1979. In Dutch.

[2] Y. Desmedt. *Analysis of the Security and New Algorithms for Modern Industrial Cryptography.* PhD thesis, K.U. Leuven, Leuven, Belgium, October 1984.

7.2 Books edited

[1] Y. G. Desmedt, editor. *Advances in Cryptology — Crypto '94, Proceedings (Lecture Notes in Computer Science 839)*, New York, August 1994. Springer-Verlag.

[2] 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.

[3] 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.

[4] Y. Desmedt, editor. *Information Theoretic Security, Second International Conference, ICITS 2007, (Lecture Notes in Computer Science 4883)*, New York, 2009. Springer-Verlag.

[5] Y. Desmedt, editor. *Information Security, 16th International Conference, ISC 2013, Dallas, Texas, USA, November 13-15, 2013, Proceedings*, volume 7807 of *Lecture Notes in Computer Science*. Springer, 2015.

7.3 Refereed journals

[1] Y. Desmedt, J. Vandewalle, and R. Govaerts. Cryptografie : Een veiligheidsaspect in de informatie. *Computer Org. Inform., (Belgium)*, pp. 17–19, June 1982. In Dutch.

[2] 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.

[3] Y. Desmedt, J. Vandewalle, and R. Govaerts. Industriele cryptografie : Noodzakelijke bescherming van informatie tegen misbruik en vervalsing. *Het Ingenieursblad (KVIV, Belgium)*, 32(1), pp. 17–23, January 1983. In Dutch.

[4] 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.

[5] R. Govaerts, J. Vandewalle, and Y. Desmedt. Industriele cryptografie. *Technivisie (Belgium)*, 1(15), pp. 10–12, November 2, 1983. In Dutch.

[6] 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.

[7] 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.

[8] M. V. D. Burmester and Y. G. Desmedt. Remarks on the soundness of proofs. *Electronics Letters*, 25(22), pp. 1509–1511, October 26, 1989.

[9] Y. G. Desmedt. The ideal world of computer security. *International Security Review*, pp. 29–32, January/February 1990. (Invited paper).

[10] Y. G. Desmedt. Cryptanalysis of conventional and public key cryptosystems. *Note Recensioni Notizie*, 39(3), pp. 87–96, 1990.

[11] 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.

[12] Y. G. Desmedt. The "A" cipher does not necessarily strengthen security. *Cryptologia*, 15(3), pp. 203–206, July 1991.

[13] J.-J. Quisquater and Y. G. Desmedt. Chinese lotto as an exhaustive code-breaking machine. *Computer*, 24(11), pp. 14–22, November 1991.

[14] 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.

[15] G. I. Davida and Y. G. Desmedt. Passports and visas versus IDs. *Computers & Security*, 11(3), pp. 253–258, May 1992.

[16] 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.

[17] Y. G. Desmedt. Threshold cryptography. *European Trans. on Telecommunications*, 5(4), pp. 449–457, July-August 1994. (Invited paper).

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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`.

[24] 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.

[25] 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.

[26] 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.

[27] Y. Wang and Y. Desmedt. Secure communication in multicast channels. *Journal of Cryptology*, 14(2), pp. 121–135, 2001.

[28] 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.

[29] Y. Desmedt. Is there a need for survivable computation in critical infrastructures? *Information Security Technical Report*, 7(2), pp. 11–21, 2002.

[30] 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.

[31] 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.

[32] Y. Desmedt. Análisis científico del ciberterrorismo. *Novática*, (172), pp. 33–37, noviembre-diciembre 2004.

[33] Y. Desmedt. Towards a scientific analysis of robust critical infrastructures. *UPGRADE*, V(6), pp. 36–41, December 2004.

[34] M. Burmester and Y. Desmedt. A secure and scalable group key exchange system. *Information Processing Letters*, 94(3), pp. 137–143, May 2005.

[35] 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.

[36] Y. Desmedt. A high availability internetwork capable of accommodating compromised routers. *BT Technology Journal*, 24(3), pp. 77–83, 2006.

[37] Y. Wang and Y. Desmedt. Perfectly secure message transmission revisited. *IEEE Transactions on Information Theory*, 54(6), pp. 2582–2595, 2008.

[38] 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.

[39] Y. Wang and Y. Desmedt. Edge-colored graphs with applications to homogeneous faults. *Information Processing Letters*, 111(13), pp. 634–641, July 2011.

[40] Y. Desmedt, J. Pieprzyk, R. Steinfeld, X. Sun, C. Tartary, H. Wang, and A. C.-C. Yao. Graph coloring applied to secure computation in non-abelian groups. *Journal of Cryptology*, 25(4), pp. 557–600, 2012.

[41] S. Mahmood and Y. Desmedt. Two new economic models for privacy. *SIGMETRICS Performance Evaluation Review*, 40(4), pp. 84–89, 2013.

[42] H. J. Asghar, Y. Desmedt, J. Pieprzyk, and R. Steinfeld. A subexponential construction of graph coloring for multiparty computation. *J. Mathematical Cryptology*, 8(4), pp. 363–403, 2014.

[43] Y. Lu and Y. Desmedt. Walsh transforms and cryptographic applications in bias computing. *Cryptography and Communications*, 8(3), pp. 435–453, 2016.

[44] Y. Desmedt and F. Piper. Perfect anonymity. *IEEE Trans. Information Theory*, 65(6), pp. 3990–3997, 2019.

[45] Y. Desmedt, S. Mo, and A. M. Slinko. Framing in secret sharing. *IEEE Trans. Inf. Forensics Secur.*, 16, pp. 2836–2842, 2021.

[46] V. S. Sehrawat, F. Y. Yeo, and Y. Desmedt. Extremal set theory and LWE based access structure hiding verifiable secret sharing with malicious-majority and free verification. *Theor. Comput. Sci.*, 886, pp. 106–138, 2021.

7.4 Chapters in edited volumes

[1] 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.

[2] 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.

[3] Y. Desmedt. *Breaking One Million DES keys*, chapter 9. O'Reilly, Sebastol, California, 1998.

[4] Y. Desmedt. A brief survey of research jointly with Jean-Jacques Quisquater. In D. Naccache, editor, *Cryptography and Security*, volume 6805 of *Lecture Notes in Computer Science*, pp. 8–12. Springer, 2012.

[5] Y. Desmedt. What is the future of cryptography? In P. Y. A. Ryan, D. Naccache, and J.-J. Quisquater, editors, *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, volume 9100 of *Lecture Notes in Computer Science*, pp. 109–122. Springer, 2016.

[6] Y. Desmedt and A. Shaghaghi. Function-based access control (FBAC): towards preventing insider threats in organizations. In *From Database to Cyber Security — Essays Dedicated to Sushil Jajodia on the Occasion of His 70th Birthday*, volume 11170 of *Lecture Notes in Computer Science*, pp. 143–165. Springer, 2018. Invited paper.

7.5 Refereed conference publications

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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, Switserland, October 29–November 1, 1983.

[18] Y. Desmedt, J. Vandewalle, and R. Govaerts. Noiseless source coding of images and texts becomes practical using a parallellisation and bit encoder. In *Proc. 2nd. Int. Conf. on New Systems and Services in Telecommunications*, Liège, Belgium, November 16–18, 1983.

[19] 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.

[20] 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.

[21] 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. Paris, France, April 9–11, 1984.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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. Santa Barbara, California, U.S.A., August 19–22.

[27] 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.

[28] 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.

[29] 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. Santa Barbara, California, U.S.A., August 18–20.

[30] 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.

[31] 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.

[32] 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.

[33] 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, Castelvecchio Pascoli, Tuscany, Italy, July 7–19, 1986.

[34] 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. Santa Barbara, California, U.S.A., August 11–15.

[35] 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.

[36] 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. Santa Barbara, California, U.S.A., August 16–20.

[37] 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. Santa Barbara, California, U.S.A., August 16–20.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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. Santa Barbara, California, U.S.A., August 20–24.

[48] 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.

[49] 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 Forschungsintitut Oberwolfach. Tagungbericht 17/1990.

[50] Y. Desmedt. System security of identification. In A. Klar, editor, *Mathematical Concepts of Dependable Systems*, p. 15, Oberwolfach, Germany, April 15–21, 1990. Mathematisches Forschungsintitut Oberwolfach. Tagungbericht 17/1990.

[51] 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 Forschungsintitut Oberwolfach. Tagungbericht 17/1990.

[52] 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. Åarhus, Denmark, May 21–24.

[53] 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. Åarhus, Denmark, May 21–24.

[54] 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. Santa Barbara, California, U.S.A., August 11–15.

[55] 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. Santa Barbara, California, U.S.A., August 11–15.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

[60] 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.

[61] 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.

[62] 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. Santa Barbara, California, U.S.A., August 12–15.

[63] 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.

[64] 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.

[65] 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 Forschungsintitut Oberwolfach. Tagungbericht 28a/1991.

[66] 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. .

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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.

[73] 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.

[74] 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.

[75] 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.

[76] 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.

[77] 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.

[78] 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.

[79] 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..

[80] S. G. Barwick, Y. Desmedt, and P. Wild. Homomorphic threshold schemes, k-arcs and Lenstra's constant. In P. G. Farrell, editor, *Codes and cyphers*, pp. 95–102. Formora Ltd., Essex, 1995. Royal Agricultural College, Cirencester, December, 1993.

[81] 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. Montréal, Québec, Canada.

[82] M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. In *Preproceedings of Eurocrypt '94*, pp. 279–290. Scuola Superiore Guglielmo Reiss Romoli (SSGRR), 1994. Perugia, Italy, May 9–12.

[83] 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.

[84] 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.

[85] Y. Desmedt. Subliminal-free sharing schemes. In *Proceedings 1994 IEEE International Symposium on Information Theory*, p. 490, Trondheim, Norway, June 27–July 1, 1994.

[86] 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. Wollongong, Australia, November/December, 1994.

[87] 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. Saint-Malo, France, May 21–25.

[88] 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.

[89] 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.

[90] 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. Cambridge, United Kingdom April 10-12, 1996.

[91] 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.

[92] 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.

[93] 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.

[94] 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.

[95] 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.

[96] 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. Espoo, Finland, May 31–June 4.

[97] 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.

[98] 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.

[99] 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.

[100] 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.

[101] 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.

[102] 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. Beijing, China.

[103] 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.

[104] 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.

[105] 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.

[106] 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.

[107] 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.

[108] 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.

[109] 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.

[110] Y. Desmedt. A too limited list of infrastructures identified as critical. In *Protecting NATO Information Systems in the* 21^{st} *Century*, pp. 3–1–3–9, May 2000. Washington DC, U.S.A., October 25–27, 1999.

[111] 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.

[112] 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.

[113] 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.

[114] 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.

[115] 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. Bruges, Belgium, May 14-18.

[116] 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.

[117] 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.

[118] 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.

[119] 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.

[120] 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.

[121] 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.

[122] 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.

[123] 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.

[124] 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.

[125] 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.

[126] 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. Amsterdam, The Netherlands, April 28–May 2.

[127] 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.

[128] 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.

[129] Y. Desmedt and B. King. Verifiable democracy a protocol to secure an electronic legislature. In R. Traunmüller 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.

[130] 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.

[131] 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.

[132] 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.

[133] 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.

[134] 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.

[135] 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.

[136] 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.

[137] 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.

[138] 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.

[139] 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. Santa Barbara, California, USA, August 15-19.

[140] 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.

[141] 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.

[142] 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.

[143] 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.

[144] 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.

[145] 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.

[146] 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.

[147] 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.

[148] 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.

[149] 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.

[150] 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).

[151] 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.

[152] 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.

[153] 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.

[154] 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.

[155] 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.

[156] 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.

[157] 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.

[158] 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.

[159] 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.

[160] 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.

[161] 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.

[162] 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.

[163] 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.

[164] 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.

[165] 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.

[166] 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.

[167] 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.

[168] 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.

[169] 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.

[170] 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.

[171] 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.

[172] 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.

[173] Y. Lu and Y. Desmedt. Improved distinguishing attack on rabbit. In M. Burmester, G. Tsudik, S. Magliveras, and I. Ilić, editors, *Information Security Conference (ISC 2010)*, volume 6531 of *Lecture Notes in Computer Science*, pp. 17–23. Springer, 2011.

[174] K. Jia, Y. Desmedt, L. Han, and X. Wang. Pseudo-cryptanalysis of luffa. In *Inscrypt 2010*, 2010. To appear in the proceedings, LNCS.

[175] Y. Desmedt and A. Miyaji. Redesigning group key exchange protocol based on bilinear pairing suitable for various environments. In *Inscrypt 2010*, 2010. To appear in the proceedings, LNCS.

[176] Q. Yang and Y. Desmedt. General perfectly secure message transmission using linear codes. In M. Abe, editor, *Asiacrypt 2010*, volume 6477 of *Lecture Notes in Computer Science*, pp. 448–465. Springer, 2010.

[177] 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.

[178] Y. Wang and Y. Desmedt. Homogeneous faults, colored edge graphs, and cover free families. In S. Fehr, editor, *Information Theoretic Security, 5th International Conference, ICITS*, volume 6673 of *Lecture Notes in Computer Science*, pp. 58–72. Springer, May 2011.

[179] S. Mahmood and Y. Desmedt. Poster: Preliminary analysis of Google+'s privacy. In *18th ACM Conference on Computer and Communications Security*, October 17–21, 2011.

[180] Y. Desmedt. Secret sharing and reliable cloud computing. In *Cryptography for Emerging Technologies and Applications Workshop, National Institute of Standards and Technology (NIST), Gaithersburg, Maryland*, November 7–8, 2011.

[181] Q. Yang and Y. Desmedt. Secure communication in multicast graphs. In S. H. Lee and X. Wang, editors, *Asiacrypt 2011*, volume 7073 of *Lecture Notes in Computer Science*, pp. 538–555. Springer, 2011.

[182] S. Mahmood and Y. Desmedt. Your facebook deactivated friend or a cloaked spy. In *PerCom Workshops*, pp. 367–373. IEEE, 2012.

[183] S. Mahmood and Y. Desmedt. Online social networks, a criminals multipurpose toolbox (poster abstract). In D. Balzarotti, S. J. Stolfo, and M. Cova, editors, *RAID*, volume 7462 of *Lecture Notes in Computer Science*, pp. 374–375. Springer, 2012.

[184] S. Mahmood and Y. Desmedt. Usable privacy by visual and interactive control of information flow. In B. Christianson, J. A. Malcolm, F. Stajano, and J. Anderson, editors, *Security Protocols Workshop*, volume 7622 of *Lecture Notes in Computer Science*, pp. 181–188. Springer-Verlag, 2012.

[185] Y. Desmedt, J. Pieprzyk, and R. Steinfeld. Active security in multiparty computation over black-box groups. In I. Visconti and R. De Prisco, editors, *SCN*, volume 7485 of *Lecture Notes in Computer Science*, pp. 503–521. Springer, 2012.

[186] Y. Desmedt and P. Chaidos. Applying divertibility to blind ballot copying in the Helios Internet voting system. In S. Foresti, M. Yung, and F. Martinelli, editors, *ESORICS*, volume 7459 of *Lecture Notes in Computer Science*, pp. 433–450. Springer, 2012.

[187] S. Erotokritou and Y. Desmedt. Human perfectly secure message transmission protocols and their applications. In I. Visconti and R. De Prisco, editors, *SCN*, volume 7485 of *Lecture Notes in Computer Science*, pp. 540–558. Springer, 2012.

[188] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis. How to attack two-factor authentication internet banking. In A.-R. Sadeghi, editor, *Financial Cryptography and Data Security, 17th International Conference, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers*, volume 7859 of *Lecture Notes in Computer Science*, pp. 322–328. Springer, 2013.

[189] Y. Wang and Y. Desmedt. Efficient secret sharing schemes achieving optimal information rate. In *2014 IEEE Information Theory Workshop, ITW 2014*, pp. 516–520. IEEE, 2014.

[190] Y. Desmedt. On the key role intelligence agencies can play to restore our democratic institutions. In B. Christianson, J/ A. Malcolm, V. Matyás, P. Svenda, F. Stajano, and J. Anderson, editors, *Security Protocols XXII*, volume 8809 of *Lecture Notes in Computer Science*, pp. 276–285 and 286–299. Springer, 2014.

[191] Y. Desmedt and K. Morozov. Parity check based redistribution of secret shares. In *Proceedings IEEE International Symposium on Information Theory*, pp. 959–963, Hong-Kong, June 14–19, 2015.

[192] Y. Desmedt and S. Erotokritou. Making code voting secure against insider threats using unconditionally secure MIX schemes and human PSMT protocols. In *Vote ID*, volume 9269 of *Lecture Notes in Computer Science*. Springer, 2015.

[193] Y. Desmedt and A. Shaghaghi. Function-based access control (FBAC): From access control matrix to access control tensor. In *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, pp. 89–92. ACM, 2016.

[194] P. D'Arco, R. De Prisco, and Y. Desmedt. Private visual share-homomorphic computation and randomness reduction in visual cryptography. In A. C. A. Nascimento and P. S. L. M. Barreto, editors, *Information Theoretic Security - 9th International Conference, ICITS 2016, Revised Selected Papers*, volume 10015 of *Lecture Notes in Computer Science*, pp. 95–113, 2016.

[195] V. S. Sehrawat and Y. Desmedt. Strengthening software diversity through targeted diversification. In *SECURWARE 2016*, 2016.

[196] Y. Desmedt, V. Iovino, G. Persiano, and I. Visconti. Controlled homomorphic encryption: Definition and construction. In M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. A. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, and M. Jakobsson, editors, *Financial Cryptography and Data Security - FC 2017, Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Revised Selected Papers*, Lecture Notes in Computer Science, pp. 107–129. Springer, 2017.

[197] M. Punekar, Q. M. Malluhi, Y. Wang, and Y. Desmedt. Candidate MDS array codes for tolerating three disk failures in RAID-7 architectures. In A. Anjum, A. Sill, X. Zhao, M. M. Farid, S. Pallickara, and J. Cao, editors, *Proceedings of the Fourth IEEE/ACM International Conference on Big Data Computing, Applications and Technologies, BDCAT 2017, Austin, TX, USA, December 05 - 08, 2017*, pp. 33–42. ACM, 2017.

[198] Y. Desmedt. "Need to know" to defend one's home, or should one buy a wifi enabled thermostat? In H. Hamdan, D. E. Boubiche, H. Toral-Cruz, S. Akleylek, and H. Mcheick, editors, *Proceedings of the Second International Conference on Internet of things and Cloud Computing, ICC 2017, Cambridge, United Kingdom, March 22-23, 2017*, pp. 201:1–201:4. ACM, 2017.

[199] R. Safavi-Naini, V. Lisý, and Y. Desmedt. Economically optimal variable tag length message authentication. In A. Kiayias, editor, *Financial Cryptography and Data Security - 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers*, volume 10322 of *Lecture Notes in Computer Science*, pp. 204–223. Springer, 2017.

[200] M. Punekar, Q. M. Malluhi, Y. Desmedt, and Y. Wang. Computational aspects of ideal (t, n)-threshold scheme of Chen, Laing, and Martin. In *CANS 2017*, volume 11261 of *Lecture Notes in Computer Science*, pp. 470–481. Springer, 2018.

[201] Y. Desmedt and K. Morozov. VSS made simpler. In N. Attrapadung and T. Yagi, editors, *IWSEC 2019, Proceedings*, volume 11689 of *Lecture Notes in Computer Science*, pp. 329–342. Springer, 2019.

[202] Y. Desmedt and A. Slinko. Realistic versus rational secret sharing. In T. Alpcan, Y. Vorobeychik, J. S. Baras, and G. Dán, editors, *Decision and Game Theory for Security - 10th International Conference, GameSec 2019, Proceedings*, volume 11836 of *Lecture Notes in Computer Science*, pp. 152–163. Springer, 2019.

[203] Y. Desmedt, S. Dutta, and K. Morozov. Evolving perfect hash families: A combinatorial viewpoint of evolving secret sharing. In Y. Mu, R. H. Deng, and X. Huang, editors, *Cryptology and Network Security - 18th International Conference, CANS*, volume 11829 of *Lecture Notes in Computer Science*, pp. 291–307. Springer, 2019.

[204] V. S. Sehrawat and Y. Desmedt. Bi-homomorphic lattice-based PRFs and unidirectional updatable encryption. In Y. Mu, R. H. Deng, and X. Huang, editors, *Cryptology and Network Security - 18th International Conference, CANS*, volume 11829 of *Lecture Notes in Computer Science*, pp. 3–23. Springer, 2019.

[205] V. S. Sehrawat and Y. Desmedt. Access structure hiding secret sharing from novel set systems and vector families. In D. Kim, R. N. Uma, Z. Cai, and D. H. Lee, editors, *Computing and Combinatorics - 26th International Conference, COCOON Proceedings*, volume 12273 of *Lecture Notes in Computer Science*, pp. 246–261. Springer, 2020.

[206] Y. Desmedt. Are clouds making our research irrelevant and who is at fault? (position paper). In S. De Capitani di Vimercati and P. Samarati, editors, *Proceedings of the 19th International Conference on Security and Cryptography, SECRYPT 2022, Lisbon, Portugal, July 11-13, 2022*, pp. 436–442. SCITEPRESS, 2022.

[207] Y. Desmedt. Cryptologists should not ignore the history of Al-Andalusia. In S. El Hajji, S. Mesnager, and E. M. Souidi, editors, *Codes, Cryptology and Information Security - 4th International Conference, C2SI 2023, Rabat, Morocco, May 29-31, 2023, Proceedings*, volume 13874 of *Lecture Notes in Computer Science*, pp. 3–9. Springer, 2023. Invited paper.

[208] Yvo Desmedt, Alireza Kavousi, and Aydin Abadi. Poster: Byzantine discrepancy attacks against calendar, set-intersection and nations. In Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie, editors, *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS 2024, Salt Lake City, UT, USA, October 14-18, 2024*, pp. 5057–5059. ACM, 2024.

7.6 Unrefereed publications

7.6.1 Techreports and archives

[1] 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.

[2] 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.

[3] G. Davida and Y. Desmedt. "Complete" identification systems. Tech. Report TR-CS-88-15, Dept. of EE & CS, Univ. of Wisconsin–Milwaukee, May 1988.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] Y. Desmedt. A cryptanalytic study of cascade ciphers. Tech. Report TR–91–6–01, Dept. of EE & CS, Univ. of Wisconsin–Milwaukee, June 1991.

[13] 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.

[14] 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.

[15] 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.

[16] Y. Desmedt. Practical interactive proven secure authentication scheme. Tech. Report TR–94–02–02, Dept. of EE & CS, Univ. of Wisconsin–Milwaukee, February 1994.

[17] Y. Berbers, W. Debeuckelaere, P. De Hert, Y. Desmedt, F. De Smet, M. Hildebrandt, K. Poels, J, Pierson, B. Preneel, and J. Vandewalle. Privacy in tijden van internet, sociale netwerken en big data (in Dutch, i.e., privacy in the age of the internet, social networks and big data). Report, the Royal Flemish Academy of Belgium for Science and the Arts, 2017.

[18] V. S. Sehrawat and Y. Desmedt. Access structure hiding secret sharing from novel set systems and vector families. *CoRR*, abs/2008.07969, 2020.

[19] V. S. Sehrawat, F. Y. Yeo, and Y. Desmedt. Extremal set theory and LWE based access structure hiding verifiable secret sharing with malicious majority and free verification. *CoRR*, abs/2011.14804, 2020.

[20] Aydin Abadi and Yvo Desmedt. Supersonic OT: fast unconditionally secure oblivious transfer. *IACR Cryptol. ePrint Arch.*, p. 1012, 2024.

[21] Aydin Abadi and Yvo Desmedt. Supersonic OT: fast unconditionally secure oblivious transfer. *CoRR*, abs/2406.15529, 2024.

[22] Yvo Desmedt and Aydin Abadi. Delegated-query oblivious transfer and its practical applications. *IACR Cryptol. ePrint Arch.*, p. 1006, 2024.

[23] Yvo Desmedt and Aydin Abadi. Delegated-query oblivious transfer and its practical applications. *CoRR*, abs/2406.15063, 2024.

[24] Aydin Abadi and Yvo Desmedt. Scalable post-quantum oblivious transfers for resource-constrained receivers. *IACR Cryptol. ePrint Arch.*, p. 36, 2025.

7.6.2 Contributions to scientific and technical encyclopedia

[1] 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.

[2] Y. Desmedt. Cryptographic foundations. In M. Atallah, editor, *Handbook of Algorithms and Theory of Computation*, chapter 38. CRC, Boca Raton, 1998.

[3] Y. Desmedt. Encryption schemes. In M. Atallah, editor, *Handbook of Algorithms and Theory of Computation*, chapter 39. CRC, Boca Raton, 1998.

[4] Y. Desmedt. Elgamal public key encryption. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 183. Springer, 2005.

[5] 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.

[6] 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.

[7] Y. Desmedt. Access structure. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 7. Springer, 2005.

[8] Y. Desmedt. Covert channels. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, pp. 106–107. Springer, 2005.

[9] Y. Desmedt. Deniable encryption. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, pp. 142–143. Springer, 2005.

[10] Y. Desmedt. Knapsack cryptographic schemes. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, pp. 333–342. Springer, 2005.

[11] Y. Desmedt. Man-in-the-middle attack. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 368. Springer, 2005.

[12] Y. Desmedt. Relay attack. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 519. Springer, 2005.

[13] Y. Desmedt. Station-to-station protocol. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, p. 596. Springer, 2005.

[14] Y. Desmedt. Threshold cryptography. In H. C. A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, pp. 606–611. Springer, 2005.

[15] Y. Desmedt. Cryptographic foundations. In M. Atallah and M. Blanton, editors, *Handbook of Algorithms and Theory of Computation: special topics and techniques*, chapter 9. CRC, Boca Raton, 2nd edition, 2010.

[16] Y. Desmedt. Encryption schemes. In M. Atallah and M. Blanton, editors, *Handbook of Algorithms and Theory of Computation: special topics and techniques*, chapter 10. CRC, Boca Raton, 2nd edition, 2010.

[17] Y. Desmedt. Elgamal public key encryption. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, p. 396. Springer, 2nd edition, 2011.

[18] Y. Desmedt. Fiat-Shamir identification protocol and the Fiat-Shamir signature scheme. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, pp. 457–458. Springer, 2nd edition, 2011.

[19] Y. Desmedt. Trojan horses, computer viruses and worms. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, pp. 1319–1320. Springer, 2nd edition, 2011.

[20] Y. Desmedt. Access structure. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, p. 20. Springer, 2nd edition, 2011.

[21] Y. Desmedt. Covert channels. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, pp. 265–266. Springer, 2nd edition, 2011.

[22] Y. Desmedt. Deniable encryption. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, pp. 322–323. Springer, 2nd edition, 2011.

[23] Y. Desmedt. Knapsack cryptographic schemes. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, pp. 695–704. Springer, 2nd edition, 2011.

[24] Y. Desmedt. Man-in-the-middle attack. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, p. 759. Springer, 2nd edition, 2011.

[25] Y. Desmedt. Relay attack. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, p. 1042. Springer, 2nd edition, 2011.

[26] Y. Desmedt. Station-to-station protocol. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, p. 1256. Springer, 2nd edition, 2011.

[27] Y. Desmedt. Threshold cryptography. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, pp. 1288–1293. Springer, 2nd edition, 2011.

[28] Y. Desmedt and Goce Jakimoski. Broadcast authentication from an information theoretic perspective. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, pp. 170–171. Springer, 2nd edition, 2011.

[29] Y. Desmedt and Goce Jakimoski. Stream and multicast authentication. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, pp. 1260–1263. Springer, 2nd edition, 2011.

[30] Yvo Desmedt. Trojan horses, computer viruses, and worms. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–2. Springer, 3rd edition, March 2024.

[31] Yvo Desmedt. Assumptions. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–2. Springer, 3rd edition, March 2024.

[32] Yvo Desmedt and Qiushi Yang. Perfectly secure message transmission. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–4. Springer, 3rd edition, March 2024.

[33] Yvo Desmedt. The fiat-shamir identification protocol and the feige-fiat-shamir signature scheme. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–2. Springer, 3rd edition, March 2024.

[34] Yvo Desmedt. Elgamal public key encryption. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–2. Springer, 3rd edition, March 2024.

[35] Yvo Desmedt. Secret sharing and shamir threshold scheme. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–5. Springer, 3rd edition, March 2024.

[36] Yvo Desmedt. Covert channels. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–2. Springer, 3rd edition, March 2024.

[37] Yvo Desmedt. Threshold cryptography. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–8. Springer, 3rd edition, March 2024.

[38] Yvo Desmedt. Station-to-station protocol. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–2. Springer, 3rd edition, March 2024.

[39] Yvo Desmedt. Man-in-the-middle and relay attack. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–2. Springer, 3rd edition, March 2024.

[40] Yvo Desmedt. Access and adversary structure. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–2. Springer, 3rd edition, March 2024.

[41] Yvo Desmedt. Knapsack cryptographic schemes. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–13. Springer, 3rd edition, March 2024.

[42] Yvo Desmedt. Deniable encryption. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–2. Springer, 3rd edition, March 2024.

[43] Yvo Desmedt and Goce Jakimoski. Broadcast authentication from an information theoretic perspective. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–3. Springer, 3rd edition, August 2024.

[44] Goce Jakimoski and Yvo Desmedt. Stream and multicast authentication. In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography and Security*, pp. 1–5. Springer, 3rd edition, March 2024.

7.7 Submitted

[1] A. Abadi and Y. Desmedt. Oblivis: An oblivious transfer framework for efficient and delegated query access. Submitted to SIGMoD 2026 on July 18, 2025.

[2] A. Abadi, Y. Desmedt, and A. Shaghaghi. Exposure by default: How Microsoft Teams, Outlook, and Calendar endanger (organizational) privacy. Submitted on July 23, 2025 to Communications of the ACM.

[3] A. Abadi and Y. Desmedt. Scalable information-theoretic oblivious transfers for resource-constrained receivers. Submitted to Network and Distributed System Security (NDSS) Symposium 2026 on August 2, 2025.

7.8 Invited presentations

7.8.1 At distinguished seminar series

Date	Details
October 17, 2018	Distinguished Department Lecture, Electrical Engineering and Computer Science, Oregon State University, Corvalis, Oregon, *The fundamental reasons information technological systems are insecure*
October 22, 2018	Distinguished Speaker at the Department of Computer Science and Engineering, University of North Texas, Denton, Texas, *The fundamental reasons information technological systems are insecure*
November 20, 2018	Dean Seminar, Faculty of Information Technology, Monash University, Melbourne, Australia *The fundamental reasons information technological systems are insecure*

7.8.2 At conferences and workshops

Date	Details
May 16–18, 1984	ICC 84, IEEE, Amsterdam, The Netherlands: *Cryptography : How to attack, what to protect?*
October 15–21, 1989	the "Monte Verita Seminar: Future Directions in Cryptography", Ascona, Switzerland: • *"Subliminal-free authentication in an international environment"* • *"Practical applications of zero-knowledge"*
November 23–24, 1989	Secondo Simposio su Stato e Prospettive della Ricerca crittografica in Italia: *Cryptanalysis of conventional and public key cryptosystems*
April 15–21, 1990	Mathematical Concepts of Dependable Systems, Oberwolfach, Germany: • *An introduction to zero-knowledge proofs* • *Defining primitives for dependable communication* • *System security of identification*
July 3–6, 1991	E.I.S.S.-Workshop, Public-Key Cryptography: State of the Art and Future Direction, Oberwolfach, Germany: *Alternative approach to cryptanalysis*
November 23–25, 1992	ESORICS 92, Toulouse, France: *Breaking the traditional computer security research barriers*
December 13–16, 1992	Auscrypt '92, Gold Coast, Australia: *Threshold cryptosystems*
February 15–16, 1993	3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy: *Threshold cryptography*
June 22–24, 1994	the "Workshop on Key Escrow", Karlruhe, Germany: • *"Threshold Decryption"* • *"Securing Traceability of Ciphertexts"* • *"What we Really Need"*
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*

INVITED PRESENTATIONS

July 6–18, 1998	the "Coding and Cryptography" workshop, IMA (Institute for Mathematics and its Applicants), 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*
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*

INVITED PRESENTATIONS

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*
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*

INVITED PRESENTATIONS

November 26, 2010	"Jean-Jacques Quisquater Emeritus day" Université Catholique de Louvain, Belgium: *A survey of almost 30 years of joint research with Prof. Quisquater*
June 7, 2011	"Workshop "Secret Sharing and Cloud Computing," Institute of Mathematics for Industry, Kyushu University, Japan: *Secure Multiparty Computation to Protect Cloud Computing*
June 28–30, 2011	"The 8th IEEE/FTRA International Conference on Secure and Trust Computing, Data Management, and Applications," Loutraki, Greece: *30 Years Computer Hacking: Can we achieve Secure and Trusted Computing?*
July 11–15, 2011	"International Workshop on Network Topologies," Brussels, Belgium: *A Survey of Generalized Connectivity and its Applications in Security*
September 7–9, 2011	"Seventh International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2011)," London, UK: *Why Security Engineering Fails*
September 25–30, 2011	Public-Key Cryptography, Dagstuhl, Germany: *Active Security in General Secure Multi-Party Computation via Black-Box Groups*
December 15, 2011	"Symposium on Mathematical Theory in Cryptologic Research," Chinese Association for Cryptologic Research, Beijing, China: *A Survey of Generalized Connectivity and its Applications in Security*
October 5, 2012	workshop on "Cryptographic Technologies suitable for Cloud Computing," Kyushu University, Fukuoka, Japan: *Secure Multiparty Computation almost without Verifiable Secret Sharing*
October 26-27, 2012	Workshop - Online Security and Civil Rights: A Fine Ethical Balance, Hertfordshire, UK: *On the Key Role Intelligence Agencies can play to Restore our Democratic Institutions*
December 6-7, 2012	Keynote lecture at the workshop on the International View of Cryptography and Security and Their Use in Practice: Focus on Mobile and Embedded Computing, Beijing, China: *Deployment issues related to cryptography in cloud computing and social networks*
May 21-25, 2013	the Mathematics of Information-Theoretic Cryptography Workshop, Leiden, the Netherlands: *Functional Secret Sharing*
May 31, 2013	the International State of the Art Cryptography Workshop, Athens, Greece: *The bumpy road to deployment: mislabeling practical and theoretical research*
September 3-4, 2013	Variety of Algebraic, Nonlinear and Dynamical Equations With Applications in Learning, Life Sciences and Esecurity, Katholieke Universiteit Leuven, Leuven, Belgium: *From Public Key Infrastructures to Secure Multiparty Computation.*
September 5-6, 2013	keynote speaker at Secure Digital Ecosystems conference, September 5-6, 2013, Leuven, Belgium: *An academic vision on cyber security in the future.*
April 3-4, 2014	the Cloud Computing Security and Identity Workshop, The National Museum of Computing, Bletchley Park Milton Keynes: *Clouds: A point of no return?*
May 16, 2014	the International State of the Art Cryptography Workshop, Copenhagen, Denmark, with lecture: *A proposal for personal clouds*
October 29, 2014	cataCRYPT, San Fransisco, California: *From Cryptology to Cryptonomy, or Are we putting all our Crypto Eggs in a Single Basket?*

INVITED PRESENTATIONS

December 11, 2014,	Keynote speaker at Conference on Cyber Security & Privacy, Rome, Italy: *Can we maintain Human Rights in Our Cyber Empire?* (also interviewed, see: `https://www.youtube.com/watch?v=S3_pN4UI1Fg`)
May 1, 2015	the International State of the Art Cryptography Workshop, Sofia, Bulgaria: *From Cryptology to Cryptonomy, or Are we putting all our Crypto Eggs in a Single Basket?*
September 25, 2015,	Keynote speaker at Free and Safe in Cyberspace, Brussels, Belgium *Threshold Cryptography and Redistribution of Secret Shares as Tools to increase Privacy and Functionality of Escrow Systems.*
September 30, 2015	cataCRYPT, Florence, Italy: *Are we Learning from Information Security Catastrophes?*
May 13, 2016	the International State of the Art Cryptography Workshop, Vienna, Austria: *Should we ban encryption? The world is not black and white.*
May 31, 2016	invited speaker at the workshop on Theory and Practice of Secure Multiparty Computation 2016, Aarhus, Denmark: *Optimal round VSS with a non-interactive Dealer: VSS as a special case of VSR,*
September 5, 2016	keynote speaker at the workshop on Secret Sharing for Dependability, Usability and Security of Network Storage and Its Mathematical Modeling, Kyushu University, Fukuoka, Japan: *Applications of Secret Sharing: Beyond Storage*
May 5, 2017	the International State of the Art Cryptography Workshop, Paris, France: *A Summary of CATAcrypt*
June 12, 2017	keynote speaker at the workshop on "Cryptographic Technologies for Securing Network Storage and Their Mathematical Modeling," Kyushu University, Fukuoka, Japan: *Human Recomputable Secret Shares and their Applications in E-Voting*
December 8, 2017	invited speaker at the International State of the Art Cryptography Workshop, Hong Kong: *Internet Voting on Insecure Platforms*
February 23, 2018	invited speaker at the International Workshop on Secret Sharing and Security, Department of Mathematics, University of Auckland, New Zealand: *From Secret Sharing to Protecting Critical Infrastructures*
July 11, 2018	invited speaker at Blockchain Research and Applications, IEEE World Congress on Computational Intelligence, Rio de Janeiro, Brazil, *Blockchain: A Cautionary Viewpoint.*
October 25, 2019	keynote speaker at the 18th International Conference on Cryptology and Network Security (CANS), Fuzhou, China, *Can we trust our security primitives?*
March 23, 2023	invited video speaker at the INSEC WORLD conference, Beijing, China, *Cryptography: A Cautionary Viewpoint.*
June 30–July 4, 2025	Journées Arithmétiques (Number Theory Workshop), University of Luxembourg, Luxembourg, *Could factoring of integers be in polynomial time on a classical computer?*
July 10, 2025	invited speaker at the Anderson's celebration workshop, Institut Henri Poincaré, Amphithéâtre Charles Hermite, Paris, *Computations with Weyl Algebra*

7.8.3 At seminar series

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

INVITED PRESENTATIONS

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 fur 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,"*
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"*.

INVITED PRESENTATIONS

November 15, 1991	Mitsubishi Electric Corporation, Computer & Information Systems Lab., Kamakura, Kanagawa, Japan: *"Reliable Parallel Multisignatures"*.
January 7, 1992	the Univerité 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"*.
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,"* .

INVITED PRESENTATIONS

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"*.
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"*.

INVITED PRESENTATIONS

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"*.
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,"*

INVITED PRESENTATIONS

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 Electricsal 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".*
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".*

INVITED PRESENTATIONS

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, 2001	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"*.
November 8 & 15, 2002	University of North Carolina at Charlotte, Department of Software and Information Systems, U.S.A., : • *"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,"*

INVITED PRESENTATIONS

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"*.
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"*
May 26, 2005	BT, Martlesham, UK: *"The Future of Cryptography for the Next 25 Years,"*

INVITED PRESENTATIONS

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,"*
February 7, 2006	BT, Martlesham, UK: *"Protecting against Denial of Service in Computer Networks,"*
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 PRESENTATIONS

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,"*
February 20, 2007	BT, Martlesham, UK: *"Non-Degrading Erasure-Tolerant Information Authentication with an Application to Multicast Stream Authentication over Lossy Channels,"*
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 1, 2007	BT, Martlesham, UK: *Applying Recreational Mathematics to Secure Multiparty Computation."*
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."*

INVITED PRESENTATIONS

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,"*
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"*

INVITED PRESENTATIONS

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"*
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, Virginia: *"Challenging Issues for Privacy and Cryptography"*
September 17, 2010	BT, Adastral Park, UK: *"Challenging Issues for Privacy and Cryptography in Europe"*
January 5, 2011	Macquarie University, Department of Computing, Australia: *"E-voting: what cryptographers overlooked for 20 years"*
February 14, 2011	Virginia Tech, Department of Computer Science, U.S.A.: *"Towards Secure Internet Voting"*
February 15, 2011	Virginia Tech, National Capital Region, U.S.A.: *"Towards Secure Internet Voting"*
April 26, 2011	Nanjing University, Department of Computer Science & Technology, China: *"After 30 years computer hacking how can we secure the internet?"*
April 27, 2011	Yangzhou University, Computer Science and Engineering, China: *"Revisiting pairing based group key exchange"*
May 9, 2011	Maryland Cybersecurity Center, University of Maryland, U.S.A.: *"Cyber Security: a Contradiction or a Paradox"*
August 25, 2011	AT&T Labs, San Ramon, California, U.S.A.: *"30 Years Computer Hacking: is Cloud Computing a Solution?"*
November 9, 2011	NIST (National Institute of Standards and Technology), Gaithersburg, Maryland, U.S.A.: *"Towards Secure Internet Voting: Taking Hacking into Account"*
December 8, 2011	Tsinghua University, Beijing: *"Secure Computing using a Hacked Terminal: e-voting as an example"*
April 27, 2012	CISE, University of Florida, Gainesville: *"Protecting against Insider Threats"*
May 10, 2012	Department of Computer Science, University of Calgary: • *Active Security in General Secure Multi-Party Computation via Black-Box Groups* • *Why Security Engineering Fails*
September 2, 2012	Telecom Italia, Turin, Italy: *Secure Multiparty Computation for Cloud Security*
September 21, 2012	University of North-Carolina Charlotte: *Secure Multiparty Computation for Cloud Security*
October 12, 2012	Nippon Telegraph and Telephone Corp., Musashino Research and Development Center, Japan: *Secure Multiparty Computation: an alternative approach*

INVITED PRESENTATIONS

October 15, 2012	National Institute of Information and Communications Technology, Koganei (Tokyo): • *Secure Multiparty Computation for Cloud Security* • *New Models for Privacy and Privacy in Social Networks* • *Two Problems with the Internet Helios System*
December 18, 2012	Department of Electrical Engineering, Université Catholique de Louvain, Belgium: *New Models for Privacy and Privacy in Social Networks*
April 8, 2013	Nippon Telegraph and Telephone Corp., Musashino Research and Development Center, Japan: *Divertible Proofs and Weaknesses of Internet Voting*
June 10, 2013	Kyushu University, Fukuoka, Japan: *Functional Secret Sharing.*
June 21, 2013	Department of Electrical Engineering, Université Catholique de Louvain, Belgium: *Functional Secret Sharing.*
August 7, 2013	Department of Computer Science, University of Calgary, Canada: *Functional Secret Sharing*
August 9, 2013	Department of Computer Science, University of Calgary, Canada: *Human Perfectly Secure Message Transmission Protocols and their Applications*
August 13, 2013	Department of Computer Science, Stanford University: *Functional Secret Sharing*
September 13, 2013	Microsoft Research, Cambridge, UK: *Is The Rise of Cloud Storage, Cloud Computing and Social Networks a Consequence of a Failed OS (Operating System) Design?*
November 27, 2013	Nanyang Technological University, School of Physical & Mathematical Sciences, Singapore: *Perfectly Secure Message Transmission using Covering Designs*
January 10, 2014	School of Computer Science and Software Engineering, The University of Wollongong, Australia: *Functional Secret Sharing*
February 19, 2014	CSE Colloquium, South Methodist University, Dallas, Texas: *Macro-Economic Study of Critical Infrastructures,*
March 17, 2014	Dipartimento di Informatica, Università degli Studi di Salerno, Italy: *From Public Key Infrastructures to Secure Multiparty Computation*
June 30, 2014	Horst Görtz Institut für IT-Sicherheit, Ruhr University, Germany *From Public Key Infrastructures to Secure Multiparty Computation*
August 14, 2014	Department of Computer Science, University of Calgary, Canada: *On the Key Role Intelligence Agencies can play to Restore our Democratic Institutions*
October 17, 2014	Seminars of the Cyber Security Centre, Oxford University, UK: *On the Key Role Intelligence Agencies can play to Restore our Democratic Institutions*
November 24, 2014	Department of Mathematics, University of North Texas, Denton. *A survey of the tools used in modern cryptology*
December 22, 2014	Kyushu University, Fukuoka, Japan: *Using Secure Multiparty Computation to Secure Outsourcing of Computation: What Theoreticians Missed,*
June 5, 2015	Chinese University of Hong Kong: *Distributed Cryptographic Security using Advanced Algebra*
June 12, 2015	Kyushu University, Fukuoka, Japan: *VSS with a Non-Interactive Dealer using Optimal Randomness and Optimal Number of Rounds.*

INVITED PRESENTATIONS

June 25, 2015	University of New South-Wales, Sydney, Australia: *What if NSA could break all "conditional" cryptosystems?*
August 13, 2015	Department of Computer Science, University of Calgary, Canada: *Using Secure Multiparty Computation to Secure Outsourcing of Computation: What Theoreticians Missed,*
September 9, 2015	École polytechnique fédérale de Lausanne, Switzerland: *Using Secure Multiparty Computation to Secure Outsourcing of Computation: What Theoreticians Missed,*
January 21, 2016	Royal Flemish Academy of Belgium for Science and the Arts, Brussels, Belgium, Installation lecture *De fundamentele oorzaken van onveilige informatie systemen.* (The fundamental reasons information technological systems are insecure),
January 22, 2016	Department of Electrical Engineering, Katholieke Universiteit Leuven (Belgium): *Towards Cloud-Friendly Secure Multiparty Computation*,
May 5, 2016	Dépt. I.R.O., Université de Montréal, Canada: *On the Key Role Intelligence Agencies can play to Restore our Democratic Institutions*,
May 25, 2016	Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, Tokyo, Japan: *Internet Voting on Insecure Platforms*,
June 9, 2016	Department of Computer Science, Birmingham University, UK: • *Should we ban encryption? The world is not black and white.* • *Internet Voting on Insecure Platforms*,
June 16, 2016	Department of Electrical Engineering, Université Catholique de Louvain, Belgium: *Internet Voting on Insecure Platforms*,
July 14, 2016	Department of Computer Science, University College London: *Internet Voting on Insecure Platforms*,
November 17, 2016	Faculty of Informatics, Università della Svizzera italiana, Lugano, Switzerland: *On the Key Role Intelligence Agencies can play to Restore our Democratic Institutions*,
November 24, 2016	University of Qatar, Doha, Qatar: *Cryptography: an Introduction*,
May 26, 2017	Nippon Telegraph and Telephone Corp., Musashino Research and Development Center, Japan: *Internet Voting on Insecure Platforms*,
June 1, 2017	Department of Information and Communications Technology, Osaka University, Osaka, Japan: *Parity Check based Redistribution of Secret Shares*,
June 19, 2017	Department of Informatics and Telecommunications, University of Athens, Greece: *Internet Voting on Insecure Platforms*,
June 22, 2017	Faculté des Sciences, de la Technologie et de la Communication, University of Luxembourg, Luxembourg: *Internet Voting on Insecure Platforms*,
July 24, 2017	School of Informatics, The University of Edinburgh, Edinburgh, UK: *Internet Voting on Insecure Platforms*,
July 25, 2017	School of Computing Science, Newcastle University, UK: *Internet Voting on Insecure Platforms*,
March 14, 2018	Commonwealth Scientific and Industrial Research Organisation, Sydney, Australia, *Orthogonal Cryptanalysis*,
June 18, 2018	Department of Computer and Information Science, Linköping University, Sweden, *Survivable Engineering: Can we learn from history?*

INVITED PRESENTATIONS

June 20, 2018	Department of Informatics, The University of Bergen, Norway, *Using Secure Multiparty Computation to Secure Outsourcing of Computation: What Theoreticians Missed*,
June 21, 2018	Department of Informatics, University of Oslo, Norway, *The fundamental reasons information technological systems are insecure*,
June 25, 2018	Department of Computer Science, Helsinki University of Technology - Aalto University, Finland, *Using Secure Multiparty Computation to Secure Outsourcing of Computation: What Theoreticians Missed*,
November 13, 2018	Faculty of Information Technology, Monash University, Melbourne, Australia *Towards a Secure OS and Secure Apps using MPC*,
December 4, 2018	Cambridge Computer Laboratory, Cambridge University, Cambridge, UK, *Function-Based Access Control (FBAC)*,
December 10, 2018	Department of Electrical Engineering, the University of Leuven, Belgium, *Towards a Secure OS and Secure Apps using MPC*,
March 8, 2019	Department of Mathematics, Canterbury University, Christchurch, New Zealand, *A survey of the tools used in modern cryptology*,
April 10, 2019	Tsinghua University, Beijing, China, *Secure Multiparty Computation versus Secure Outsourcing*,
April 13, 2019	Key Laboratory of Cryptologic Technology and Information Security, Shandong University, Jinan, China, *2000 years of cryptology: a struggle towards science*,
April 20, 2019	University of Electronic Technology, Guilin, China, *2000 years of cryptology: a struggle towards science*,
April 22, 2019	Jinan University, Guangzhou, China, *Secure Multiparty Computation versus Secure Outsourcing*,
April 26, 2019	Chinese University of Hong Kong, Hong Kong, China, *Secure Multiparty Computation versus Secure Outsourcing*,
July 1, 2019	Politecnico di Torino, Turin, Italy, *Private and Reliable Communication with Untrusted Components*,
November 8, 2019	Dept. of Computer Science, University of Texas at Dallas, USA, *Could Anonymity be a Myth?*,
February 17, 2020	School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore: *Perfect Anonymity: Could Anonymity be a Myth?*,
February 21, 2020	Vietnam Institute for Advanced Study in Mathematics, Hanoi, Vietnam, *Some applications of Graph Theory in Cryptography and Reliability*,
February 25, 2020	School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore: *Secure Multiparty Computation versus Secure Outsourcing*,
December 14, 2021	Department of Computer Science, Telecom University, Paris, France, *Perfect Anonymity: Could Anonymity be a Myth?*,
June 23, 2022	Information Security Group, Department of Computer Science, University College London, UK, *Framing and Realistic Secret Sharing*,
July 27, 2022	School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore, *Framing and Realistic Secret Sharing*,
December 20, 2022	Faculty of Information Technology, Monash University, Melbourne, Australia, *Framing and Realistic Secret Sharing*,

INVITED PRESENTATIONS

March 9, 2023	Kyushu University, Fukuoka, Japan, *Perfect Anonymity: Could Anonymity be a Myth?*,
March 10, 2023	Department of Information and Communications Technology, Osaka University, Osaka, Japan, *Framing and Realistic Secret Sharing*,
March 17, 2023	Research Center for Information Security, AIST, Japan *Framing and Realistic Secret Sharing*,
December 14, 2023	Faculty of Informatics, Università della Svizzera italiana, Lugano, Switzerland, *Are Clouds making our Research Irrelevant and Who is at Fault?*
December 18, 2023	École polytechnique fédérale de Lausanne, Switzerland, *Perfect Anonymity: Could Anonymity be a Myth?*,
May 21, 2024	University of New South-Wales, Sydney, Australia *Are Clouds making our Research Irrelevant and Who is at Fault?*
May 22, 2024	CSIRO, Sydney, Australia, *Secure Outsourcing and Secure Globalization*,
May 23, 2024	Macquarie University, Department of Computing, Australia, *Perfect Anonymity: Could Anonymity be a Myth?*,
June 20, 2025	Department of Information and Communications Technology, Osaka University, Osaka, Japan, *Should Distributed Systems be a Required Course and Where/What Crypto is used in Practical Voting Systems?*

7.9 Submitted presentations (accepted)

May 19, 2020	IEEE Symposium on Security and Privacy (short presentation, virtual), *Security versus Privacy in the Age of COVID-19* (submitted on April 24, 2020)
August 18, 2020	Crypto 2020 (rump session, virtual), *40 years Advances in Cryptology: How Will History Judge Us?* (submitted on August 17, 2020)
May 2, 2022	Financial Cryptography 2022 (poster presentation), *Is voting via the cloud so far from the state of the art, that we should not trust it?* (submitted on November 25, 2021)

7.10 Other

February 14, 2020	4th Workshop on Trusted Smart Contracts In Association with Financial Cryptography 2020, *Smart Contracts: Critical Viewpoints* (poster, jointly with S. Chow),
December 2, 2022	Texas Crypto Day, Texas A&M, College Station, USA, *The Impact of Outdated Crypto Books on Research: Anonymity Revisited*,
April 14, 2023	Texas Crypto Day, University of Texas, Austin, USA, *Forencics Aspects of Secret Sharing*,

GRANTS

September 23, 2024	Workshop on Vehicle Theft and Thwarting Relay Attacks, University College London, UK: • Zero-Knowledge based Identification • Early Research on the Relay Attack (replacing J.-J. Quisquater) • Beth-Desmedt protocols,
December 13, 2024	Texas Crypto Day, Rice University, Houston, USA, *Should Distributed Systems be a Required Course and Where/What Crypto is used in Practical Voting Systems?*

8 Grants

8.1 Proposals in preparation

- **Grant preparation:** proposal to be submitted to NSF 25-515 with title "Integrity in deep learning/neural network models." PI Brian King (Purdue University), with UTD as subcontract.

8.2 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.

GRANTS

[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.

[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, Asoc. Prof. C. Xing, 2006–2008.

[20] EJAM: Industrial Case, co-funded by BT-1080050886, "Modelling & Simulation of Security Properties of Large Scale Networks", 2007-2010, £60,864, Funded as part of EPSRC GR/T11364/01, "Collaborative Training Account: University College London," PI S. Caddick, Co-PIs B. F. Buxton and J. A. Parkinson.

[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.

[24] Security Science Doctoral Training Centre, £ 7,446,274, 01 October 2009 – 31 March 2018, contributed to UCL's proposal, principal investigator Prof. Tilley.

[25] Faculty Science and Technology Acquisition and Retention (STARs) Grant, The University of Texas System, $500,000, September 1, 2012 – August 31, 2015.

[26] NPRP No.: NPRP8-2158-1-423: "Efficiently Reliable and Privacy Preserving Cloud Data Storage," Funded by Qatar Foundation, principal investigator Prof. Malluhi, Qatar University, subcontract $121,803, December 1, 2015 – (extended date) July 14, 2020.

[27] ARC DP180102199: "Privacy-preserving Data Processing on the Cloud," AUS $413,043, 2018-2024, (PI: Dr. Ron Steinfeld).

9 Teaching

9.1 Advisement

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
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
2010–2011	PhD Advisor of S. Erotokritou, S. Mahmood and Q. Yang (graduated November, 2011); MSc advisor of M. Adham, A. Azodi, I. Karaolis, C. Pavlos, S. Van Roosmalen; Post-doctoral advisor of Y. Lu
2011-Summer 2012:	PhD Advisor of Pavlos Chaidos, S. Erotokritou, and S. Mahmood; MSc advisor of A. Shaghaghi.
Fall 2012-2013:	PhD Advisor of S. Erotokritou (University College London)
2014-Spring 2016:	PhD Advisor of V. S. Sehrawat (University of Texas at Dallas) and S. Erotokritou (Graduated, University College London)
Fall 2015:	Independent study advisor of N. Charlton and D. Partha
Fall 2016-Fall 2017:	PhD Advisor of V. S. Sehrawat
Spring 2018-Spring 2019:	PhD Advisor of V. S. Sehrawat and MSc Advisor of S. Dasgupta

Summer 2019 - Fall 2019:	PhD Advisor of V. S. Sehrawat (graduated)
Spring 2023:	PhD Advisor of Kolbe Surran

9.2 Classroom teaching:

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)
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

TEACHING

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
Term 2, 2010–2011: COMPGA02, Computer Security II and COMPGA04 Advanced Cryptography
Term 2, 2011–2012: COMPGA02, Computer Security II and COMPGA04 Advanced Cryptography
Fall semester 2012 7301.001, Information Theoretical Cryptography
Spring semester 2013 6377.001.13S, Introduction to Cryptography
Fall semester 2013 5333.002.13F, Discrete Structures
Spring semester 2014 CS5333.001.14S, Discrete Structures and CS6377.001.14S Introduction to Cryptography
Fall semester 2014 CS5333.002.14F, Discrete Structures and CS6377.001.14S Introduction to Cryptography
Spring semester 2015 CS7301.005.15S, Advanced Cryptography
Fall semester 2015 CS5333.002.15F Discrete Structures and CS6377.001.15F Introduction to Cryptography
Spring semester 2016 CS4V95.001, Undergraduate Course on Introduction to Cryptography
Fall semester 2016 CS5333.002.16F Discrete Structures and CS6377.001.16F Introduction to Cryptography
Spring semester 2017 CS 7301.009/SE 7301.009 Advanced Cryptography
Fall semester 2017 CS5333.002.17F Discrete Structures and CS6377.001.17F Introduction to Cryptography
Spring semester 2018 CS4301.004 Undergraduate Course on Introduction to Cryptography
Fall semester 2019 CS5333.002.19F Discrete Structures and CS6377.001.19F Introduction to Cryptography
Spring semester 2020 CS 4301.003 Undergraduate Course on Concepts of Cryptography
Fall semester 2020 CS 2305 hn1 Discrete Mathematics for Computing I (Honors Class) and CS6377.001.20F Introduction to Cryptography
Spring semester 2021 CS 4301.0w1 Undergraduate Course on Concepts of Cryptography
Fall semester 2021 CS5333.002-203 Discrete Structures and CS6377.001 Introduction to Cryptography
Spring semester 2022 CS5333.001 Discrete Structures
Fall semester 2022 CS5333.002 Discrete Structures and CS6377.001 Introduction to Cryptography
Spring semester 2023 CS 4301.001 Undergraduate Course Concepts of Cryptography
Fall semester 2023 CS5333.002 Discrete Structures and CS6377.001 Introduction to Cryptography
Spring semester 2024 CS 3305.006 Discrete Mathematics for Computing II and CS 4301.003 Undergraduate Course Concepts of Cryptography
Fall semester 2024 CS5333.002 Discrete Structures and CS6377.001 Introduction to Cryptography
Spring semester 2025 CS 2340.004 Computer Architecture and CS 3345.001 Data Structures and Introduction to Algorithmic Analysis
Fall semester 2025 CS 3345.005 Data Structures and Foundations of Algorithmic Analysis and CS6377.001 Introduction to Cryptography

9.3 Other

9.3.1 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," Sorèze, 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.
- Sole lecturer on "The Challenges of Access Control and Cryptography for Communications," SDR Europe, Amsterdam Airport, the Netherlands, October 26, 2011.
- Invited at Defence IT on "Private and Secure Communication with an Adversarial Insider," Brussels, Belgium, June 18-19, 2013.
- Invited Summer School lecturer on "Secret Sharing, Anonymization, and Practical Homomorphic Encryption," at Security and Privacy in Digital Life, EIT ICT Labs, University of Trento, Trento, July 28th till August 8th, 2014.
- Invited Winter School lecturer on "Secret Sharing and its Applications," CyberSecurity and Privacy (CySeP) Winter School, KTH Royal Institute of Technology, Stockholm, Sweden, October 27, 2014.
- Invited Summer School lecturer on "Secret Sharing, Homomorphic Encryption, and Threshold Cryptography," at Security and Privacy in Digital Life, EIT ICT Labs, University of Trento, Trento, July 2nd till 10th, 2015.
- Invited Summer School lecturer on "Secret Sharing, Homomorphic Encryption, and Threshold Cryptography," at Security and Privacy in Digital Life, EIT ICT Labs, University of Trento, Trento, June 26nd till July 8th, 2016.

- Invited Summer School lecturer on:
  - Secure Multiparty Computation
  - Secret Sharing

  at Security and Privacy in Digital Life, EIT ICT Labs, University of Trento, Trento, July 2nd till July 14th, 2017.
- Keynote Invited Summer School lecturer on: "The fundamental reasons information technological systems are insecure," at "Cybersecurity and Privacy (CySeP) Summer School", Stockholm, Sweden, June 11-15, 2018.
- Invited Summer School lecturer on:
  - Secure Multiparty Computation
  - Secret Sharing

  at Security and Privacy in Digital Life, EIT ICT Labs, University of Trento, Trento, July 1-13, 2018.
- Invited Summer School lecturer (13 hours) on: "Public Key Cryptography and Quantum Cryptography," at "Research Workshop on Cryptography, Cryptanalysis and Network Security: Current Challenges and Future Directions", Manipal Institute of Technology, MAHE, Manipal, India, September 17-18, 2018.
- Invited Summer School lecturer on:
  - "Information Security: Back to the Essentials," June 12, 2019, and
  - "2000 Years of Cryptology: a Struggle Towards Science." June 13, 2019,

  at the "Cybersecurity and Privacy (CySeP) Summer School", Stockholm, Sweden, June 10-14, 2019.
- Invited Summer School lecturer on: "Cryptography: A Cautionary Viewpoint," June 14, 2024, at the "Cybersecurity and Privacy (CySeP) Summer School", Stockholm, Sweden, June 10-14, 2024.

9.3.2 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,
- 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

9.3.3 Other teaching

- Replacement class:
  - for Prof. Colin Boyd (QUT, Australia) on "Security Goals in Cryptography," July 25, 2005.
  - for Prof. Andy Yao (Tsinghua University, China) on "The use of polynomials in cryptography," April 10, 2007, April 23, 2010 and April 8, 2011.
  - for Dr. Kirill Morozov (Kyushu University, Japan) on "Verifiable Secret Sharing and Secure Multiparty Computation," June 8, 2011.
- "Computer Security" classes as part of the University College London's (Department of Electronic & Electrical Engineering) BT MSc Module 21 "Security in a Networked World," April 2 and 15, 2008 and April 22, 2009.
- "Computer Security" classes as part of University College London's (Jill Dando Institute of Crime Science) course PUBLGC50 "Principles of Information Security," October 30 and November 2, 2009; January 24 and 31, 2011; January 23 and 30, 2012.
- "Summary of Cryptography," as part of: CS 4301, (3 hours) October 12, 2018.

10 Service

10.1 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 (2006–2018),
- Member of the Steering Committee of the International Workshop on Practice and Theory in Public Key Cryptography, PKC, (2000–).
- Member of the Board of Directors of International Financial Cryptography Association, Elected, 2013-2016,
- Member of the Steering Committee of cataCRYPT (2014–),
- Member of the Steering Committee of IEEE Science and Information Conference (2015–2017),
- Chair of the Steering Committee of the Workshop Vehicle Theft and Thwarting Relay Attacks (2024–).

10.2 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
2001-2013	editor of The Journal of Computer Security
July 2001-July 2011	editor of Information Processing Letters
since May 2005	Editor-in-chief of the IEE Proceedings, Information Security (now called: IET Information Security)
2006-2012	editor of Advanced Mathematics of Communications
2010–2011	editor of Computers & Security

10.3 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.
  - Program Chair of the Information Security Conference (ISC) 2013
- 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), Track on "Cryptography, Security and Trust" at 37th International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM 2011), 16th Australasian Conference on Information Security and Privacy (ACISP 2011), VOTEID2011, 12th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2011), Indocrypt 2011, 17th Australasian Conference on Information Security and Privacy (ACISP 2012), RSA conference 2013 (Cryptographers Track), Conference on Communications and Multimedia Security 2013, Emerging Ubiquitous Systems and Pervasive Networks 2014, ProvSec 2015, International Information Security Conference (ISC 2015), the IACR International Workshop on Practice and Theory in Public Key Cryptography (PKC) 2016, Systems Security and Privacy Track of ANT 2016, International Conference on Information and Communications Security 2016, International Information Security Conference (ISC 2016), International Conference on Cryptology and Network Security 2016, 23th Australasian Conference on Information Security and Privacy (ACISP 2018), IFIP 36th International on ICT Systems Security and Privacy Protection (IFIP SEC 2021), IFIP 37th International on ICT Systems Security and Privacy Protection (IFIP SEC 2022), 27th European Symposium on Research in Computer Security (ESORICS 2022), IFIP 38th International on ICT Systems Security and Privacy Protection (IFIP SEC 2023), The 5th International Conference on Science of Cyber Security (SciSec 2023), 21st IEEE Annual International Conference on Privacy, Security & Trust (PST 2024).

- 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).
- 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)
  - the Financial Crypto 2013 Panel (Member) on Security of Online Banking
  - the Annual Conference (Human After All: Innovation, Disruption, Society) organized by "The Institute for New Economic Thinking," Toronto, Canada on Cyber War, Cyber Space: National Security and Privacy in the Global Economy, (also interviewed, see `https://www.youtube.com/watch?v=dnk1S0pgVJ0`)
  - Free and Safe in Cyberspace, September 24-25, 2015, Brussels, Belgium
  - CataCRYPT 2017, Paris, France (Moderator) on How to Promote Funding for Cryptanalysis? (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, ICISC 2010, CANS 2010, ICITS 2011, CANS 2011, SCN 2012, Financial Cryptography 2013, ISC 2013, CANS 2013, ICITS 2013, CANS 2014, CANS 2015, Financial Cryptography 2016, SECURCOMM 2016, ICITS 2016, CANS 2017, 16th IMA International Conference on Cryptography and Coding, CANS 2018, CANS 2019, Financial Cryptography 2022, SECRYPT 2022, Texas Crypto Day 2022, CANS 2023, CANS 2024.

10.4 Refereeing journal papers, conferences (external), grant proposals:

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 Counsil (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 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, 2018), EPSRC (2007-2013), Royal Society (2011), FWF Austrian Science Fund (2011), Asiacrypt 2011, ERC (2014), SODA 2016.

10.5 External academic service

External member of the PhD jury of:

- Thomas Johansson, Dept. of Info. Theory, Lund University, Sweden, 1994 (present at the defense).
- David Naccache, Ecole Nationale Supérieure des Télécommunications, Paris, France, 1995 (present at the defense),
- Raphael Phan, Multimedia University, Malaysia, 2005,
- Michelangelo Giansiracusa, Queensland University of Technology, Brisbane, Australia, 2005

10.6 Internal academic service: university level

- Member of the Faculty and Staff Rewards and Incentives Committee September 1998–May 1999 (University of Wisconsin–Milwaukee).
- Member of the Executive Committee of the Division of Natural Sciences, September 1995–July 1999 (University of Wisconsin–Milwaukee).
- Member of the CIRC Security Committee (January 2000–April 2004) (Florida State University).
- Suggested Univ. of Texas at Dallas joins Eduroam (made on August 10, 2016)
- Member of the Committee on Academic Integrity 2016-2017 and 2017-2018 (University of Texas at Dallas).
- External Member of the Promotion Committee of Associate Professor Matt Brown (2019)
- Chair of the Promotion Committee of Associate Professor Tien Nguyen (2019)
- Member of the Mid-probationary Review Committee of Wei Yang (2020)
- International Oversight Committee (2021-2023)
- Chair of the Mid-probationary Review Committee of Kangkook Jee (2022).
- Chair of the Promotion Committee of Associate Professor Feng Chen (2025)
- Chair of the Tenure and Promotion Committee of Assistant Professor Kangkook Jee (2025)

10.7 Internal academic service: college level

- Member of the Computer Science Curriculum Committee between 1988 and 1990 (University of Wisconsin–Milwaukee).
- Member of the Total Quality Management (TQM) Research and Scholarship committee (College), 1992–1993 and 1996–1997 (University of Wisconsin–Milwaukee).
- Member of the Task Force For Promoting Research in the College of Engineering and Applied Science, September 1997–July 1999 (University of Wisconsin–Milwaukee).
- Member of the Graduate Program Subcommittee (College) between 1991 and 1993 (University of Wisconsin–Milwaukee).
- External Chair of the PhD thesis of Mohsen Jafarzadeh (Fall 2019).
- External Chair of the PhD thesis of Shenggang Dong (Spring 2021).
- External Chair of the PhD thesis of Yujie Zhang (Fall 2024).

10.8 Internal academic service: department level

- Syllabus and course development: see Teaching
- Member of:
  - the master thesis exam committee of: Valois Denis (Université de Montréal), Dancs Frank (University of Wisconsin–Milwaukee), Sam Thao (University of Wisconsin–Milwaukee), Larry Rodrigues (University of Wisconsin–Milwaukee), Lisa Eng (University of Wisconsin–Milwaukee) and Doan An Hai (University of Wisconsin–Milwaukee).
  - undergraduate honors thesis exam committee of Yanet Manzano (Florida State University, Spring 2000).
- Chair of the Computer Science curriculum subcommittee on Mathematics Requirements and Theory Courses, 1995–1996 (University of Wisconsin–Milwaukee).
- Representative for the library 1987–1996 (University of Wisconsin–Milwaukee).
- Member of the Computer Science Graduate Curriculum Committee December 1998–July 1999 (University of Wisconsin–Milwaukee).
- Coordinator for the letters of evaluation for possible promotion of Dr. McRoy in 1998–1999 (University of Wisconsin–Milwaukee).
- Member of the Infrastructure Proposal Committee of the Department of Computer Science, Fall 2000 (Florida State University).
- Member of the Faculty Evaluation Committee of the Department of Computer Science academic year 2000–2001 (Florida State University).
- Chair of the Computer Security Curriculum Subcommittee of the Department of Computer Science since Fall 1999–Spring 2002 (Florida State University).
- Chair of the Equipment Committee of the Department of Computer Science during the academic year 2000–2001 (Florida State University) and member Fall 2000–Spring 2002 and from Fall 2003 on.
- Chair of the InfoSec Subcommittee of the Department of Computer Science Fall 2000–Spring 2002 (Florida State University).
- Member of the Faculty Recruitment Committee of the Department of Computer Science from 1999–2001 (Florida State University) and 2002–2003.
- Member of the PhD Portfolio Evaluation Committee, from Spring 2003- Spring 2004 (Florida State University)
- Organizer of the 2004-2005 Adastral Seminar Series, invited speakers included: Gilles Brassard, Jean Camp, Craig Gentry, Sushil Jajodia, Xiaoyun Wang and Brent Waters.
- Member of the Adastral Academic Staff Recruitment Committee (University College London, 2004-2009)
- Member of the PhD Committee from Fall 2016- Spring 2018 (University of Texas at Dallas).
- Member of the Faculty Search Committee (Spring 2024–).

10.9 Community and Outreach

Examples:

- Public Lecture for TV: "Authentication in local and international environments", Center for Continuing Education, November 1988.
- Member of the FBI Milwaukee Infragard Chapter in 1998–1999.

SERVICE

- Lectured for the State of Florida Chief Information Officers' Council on "FSU's Efforts to Address Information Security and Assurance in Florida" (jointly with Ted Baker) on January 19, 2000.
- Attended the White House Reception for the NSA Center on May 25 2000 and May 24, 2001, Washington, D.C.
- Organized two lectures on "Electronic Voting Using Cryptography", presented by Dr. Kazue Sako (NEC Corporation, Japan) on February 22 and 23, 2001 at Florida State University. The event was attended by people from State as well as Florida State University faculty and students. An interview was broadcasted on TV.
- Interviewed by the newspaper Tallahassee Democrat for their September 19, 2001 front page article the "Common flaw in security exploited."
- Interviewed about the Nimda worm on ABC, Channel 27, Tallahassee, on September 18 and September 19, 2001.
- Interviewed by Florida State University "Research – In Review", Winter 2002, "Digital Deception," pp. 39–41.
- Attended the NSA (National Security Agency) Center of Excellence in Information Security Education Meeting at NSA, Maryland, USA, November 19, 2002 and also on September 11, 2001 and October 19 and 20, 2000.
- Seminar lecture, Florida A&M University, Computer and Information Sciences, "Information Security Research and Education," February 11, 2003, Tallahassee, FL.
- Lectured for the Faculty and Friends Club of Florida State University "Protecting against Computer Threats," February 23, 2003, Tallahassee, FL.
- Main organizer of and speaker at the "Summer School on Information Security", May 15-23, 2003, Florida State University, Tallahassee, Florida, USA,
- Meeting with the Review Panel of the Australian High Tech Crime Centre, May 23, 2006, Gold Coast, Australia.
- Interviewed about LulzSec's hacking by Sky News, London, UK, June 25, 2011.
- News articles mentioning Mahmood-Desmedt's work on Google+'s privacy weaknesses in ZDNet Australia, Zeit Online (German), Handelsblatt (German), Let's Talk (BT Blog), Security Lab for Positive Securities (Russian), Americas Review, etc. November 28–29, 2011.
- Eastfield-College, Mesquite, Texas, lecture on *Cryptography*, April 9, 2015.

10.10 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 2009-2012.