# Michael Steiner

1701 SW Columbia Street, #405
Portland, OR 97201, USA

email: *steiner@acm.org* www: http://vcard.acm.org/~steiner/


## Areas of Interest

- Computer Security: network security, cryptographic protocols, multi-party security and security engineering.
- Distributed Systems: middle-ware, information-retrieval, networking, mobile systems, cloud.

## Education

- Doktor der Ingenieurwissenschaften (Dr. Ing.) der Naturwissenschaftlich-Technischen Fakultät der Universität des Saarlandes, March, 2002.
  Title: "Secure Group Key Agreement".
  Advisors: Prof. Dr. B. Pfitzmann, Prof. Dr. G. Tsudik (University of California, Irvine).
  Grade: Summa cum laude / Mit Auszeichnung
- Diplom Informatik-Ingenieur, Eidgenössische Technische Hochschule (ETH) Zürich, November 1992.
  Title: "TCP/IP on the Ceres: Design and Implementation of a Communication Stack"
  Advisor: Prof. Dr. Beverly Sanders.
- Matura Typus B. Gymnasium Laufental-Thierstein, Laufen, September 1986.

## Employment History

- November 2015 - present
  Research Scientist, Intel Labs, Hillsboro, OR, USA; Member of the Security and Privacy Research Department. Research in multi-party security relying on hardware security, e.g., TEEs such as SGX, and/or cryptography, e.g., fully-homomorphic encryption.
- December 2013 - November 2015
  Research Scientist, IBM Research - India, Bangalore, KA, India. Research focusing on security challenges in BOYD devices and privacy-preserving and scalable information retrieval. Exploring new security challenges and opportunities in GMU.
- November 2002 - November 2015
  Research Scientist, IBM T.J Watson Research Laboratory, Hawthorne, NY, USA; since December 2013, on temporary assignment with IBM Research - India, Bangalore, KA, India. Member of the Secure Software and Services Department[1]. Research in intrusion response,

risk management, middle ware security and cryptographic protocols. Most recently, work with US government on making privacy-preserving yet scalable data-query systems practical, advancing the state-of-the-art in terms of scale by several orders of magnitude. Previously, development of novel security analysis and management techniques for clouds of virtual systems. Prior work focused on tackling security challenges in cyber-physical systems, in particular Smart Grids, and security aspects in Web 2.0 – dealing with issues such as end-to-end authentication and mashup isolation, e.g., contributing influently to the OpenAjax Secure Component model. Instrumental in the development of a Network Admission Control-based Tivoli Compliance and Remediation Management solution and in the security design and implementation of a large software-as-a-service infrastructure for IGS (IBM Global Services).

- October 2001 - June 2002
  Head of the cryptography and security group[2] (Lehrstuhlvertretung/Acting Professor), Universität des Saarlandes, Saarbrücken. Group leader of the EU ITS project MAFTIA[3] working on the formal modeling of dependable cryptographic systems. Teaching course on cryptographic protocols.

- April 1999 - September 2001
  Research Scientist, Universität des Saarlandes, Saarbrücken. Member of the cryptography and security group[4]. Research in formal models/proofs for secure group key agreements, protocols for password-based authentication and number-theoretic cryptographic assumptions.

- January 1993 - December 2001
  Research Scientist, IBM Research Laboratory, Rüschlikon, Switzerland. Member of the security group[5]. Participation in the EU RACE project SAMSON and in several projects in the area of secure electronic commerce: Design of the *i*KP payment protocol family[6], micro-payment extensions, and the core of the SET Secure Electronic Transactions Protocol, a standization effort performed with EuroPay, MasterCard and Visa. Technical co-leader of the EU ACTS project SEMPER[7] working on the architecture of a secure e-commerce platform and the design of a generic and modular payment framework.

- January 1990 - December 1992
  System administrator, ETH Zürich, Switzerland. Management of network of MacIntosh Computers running MacOS and A/UX. (Part time work).

- June 1990 - October 1990
  Software Engineer, S.A. GEOLINK, Paris, France. Work within a EU RACE project on data retrieval / compression for a distributed database.

- March 1989 - December 1989
  Hard- and software consultant, METTLER Instrumente AG, Greifensee, Switzerland (part time work).

## Publications

- **Thesis**


[1] Michael Steiner. *Secure Group Key Agreement*. Dissertation, Naturwissenschaftlich-Technische Fakultät der Universität des Saarlandes, Saarbrücken, March 2002.

[2] Michael Steiner. TCP/IP on the Ceres: Design and implementation of a communication stack. Diplomarbeit, Eidgenössische Technische Hochschule (ETH), Zürich, November 1992.


- **Books (Editor) and Book chapters**


[1] Somnath Chakrabarti, Thomas Knauth, Dmitrii Kuvaiskii, Michael Steiner, and Mona Vij. Trusted execution environment with Intel SGX. In Xiaoqian Jiang and Haixu Tang, editors, *Responsible Genomic Data Sharing — Challenges and Approaches*, pages 161–190. Elsevier Science Publishers B.V., 2020.

[2] Gérard Lacoste, Birgit Pfitzmann, Michael Steiner, and Michael Waidner, editors. *SEMPER — Secure Electronic Marketplace for Europe*, volume 1854 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin Germany, August 2000.

[3] Birgit Baum-Waidner, Gérard Lacoste, Birgit Pfitzmann, Michael Steiner, Michael Waidner, and Arnd Weber. Part I: The vision of SEMPER. In Lacoste et al. [2], pages 1–37.

[4] N. Asokan, Birgit Baum-Waidner, Torben P. Pedersen, Birgit Pfitzmann, Matthias Schunter, Michael Steiner, and Michael Waidner. Architecture. In Lacoste et al. [2], pages 45–64.

[5] N. Asokan and Michael Steiner. The payment framework. In Lacoste et al. [2], pages 187–214.

[6] N. Asokan, Phil Janson, Michael Steiner, and Michael Waidner. State of the art in electronic payment systems. In Marvin V. Zelkowitz, editor, *Advances in Computers*, volume 43, pages 425–449. Academic Press, March 2000.


- **Journals**


[1] Michael Backes, Birgit Pfitzmann, Michael Steiner, and Michael Waidner. Polynomial liveness. *Journal of Computer Security*, 12(3/4):589–618, 2004.

[2] Chun-Li Lin, Hung-Min Sun, Michael Steiner, and Tzonelih Hwan. Three-party encrypted key exchange without server public-keys. *IEEE Communications Letters*, 5(12):497–499, December 2001.

[3] Michael Steiner, Peter Buhler, Thomas Eirich, and Michael Waidner. Secure password-based cipher suite for TLS. *ACM Transactions on Information and System Security*, 4(2):134–157, May 2001.

[4] Michael Steiner, Gene Tsudik, and Michael Waidner. Key agreement in dynamic peer groups. *IEEE Transactions on Parallel and Distributed Systems*, 11(8):769–780, August 2000.

[5] Mihir Bellare, Juan Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Els Van Herreweghen, and Michael Waidner. Design, implementation and deployment of the *i*KP secure electronic payment system. *IEEE Journal on Selected Areas in Communications*, 18(4):611–627, April 2000.

[6] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. New multiparty authentication services and key agreement protocols. *IEEE Journal on Selected Areas in Communications*, 18(4):628–639, April 2000.

[7] N. Asokan, Hervé Debar, Michael Steiner, and Michael Waidner. Authenticating public terminals. *Computer Networks*, 31(8):861–870, May 1999.

[8] Jose L. Abad-Peiro, N. Asokan, Michael Steiner, and Michael Waidner. Designing a generic payment service. *IBM Systems Journal*, 37(1):72–88, January 1998.

[9] Michael Steiner, Günter Karjoth, and Ralf Hauser. Management von Sicherheitsdiensten in verteilten Systemen. *Datenschutz und Datensicherheit DuD, Verlag Friedrich Vieweg & Sohn, Wiesbaden*, 19(3):150–155, March 1995.

- **Conferences and Workshops (refereed)**

[1] Fan Sang, Jaehyuk Lee, Xiaokuan Zhang, Meng Xu, Scott Constable, Yuan Xiao, Michael Steiner, Mona Vij, and Taesoo Kim. SENSE: Enhancing microarchitectural awareness for TEEs via subscription-based notification. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2024)*, San Diego, CA, February 2024. Internet Society.

[2] Chris Wilkerson, Sachin Taneja, Raghavan Kumar, Sanu Mathew, Jeremy Casas, Jin Yang, Michael Steiner, Huijing Gong, Duhyeong Kim Wen Wang and, Ro Cammarota, Poornima Lalwaney, Adish Vartak, Vasantha Srirambhatla, Sandeep Jain, and AppaRao Ch. Intel HERACLES homomorphic encryption revolutionary accelerator with correctness for learning-oriented end-to-end solutions. In *Proceedings of the Government Microcircuit Applications & Critical Technology Conference (GOMAC Tech)*, March 2023.

[3] Fan Sang, Ming-Wei Shih, Sangho Lee, Xiaokuan Zhang, Michael Steiner, Mona Vij, and Taesoo Kim. PRIDWEN: Universally hardening SGX programs via load-time synthesis. In *Proceedings of the USENIX Annual Technical Conference (USENIX'22)*, June 2022.

[4] Fritz Alder, N. Asokan, Arseny Kurnikov, Andrew Paverd, and Michael Steiner. S-FaaS: Trustworthy and accountable function-as-a-service using Intel SGX. In *Proceedings of the 2019 ACM Workshop on Cloud Computing Security (CCSW)*, November 2019.

[5] Ivan De Oliveira Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, Michael Steiner, and Gene Tsudik. VRASED: A verified hardware/software co-design for remote attestation. In *Proceedings of the 28th USENIX Security Symposium*. USENIX, August 2019.

[6] Sky Faber, Stanislaw Jarecki, Hugo Krawczyk, Quan Nguyen, Marcel Rosu, and Michael Steiner. Rich queries on encrypted data: Beyond exact matches. In Günther Pernul, Peter Ryan, and Edgar Weippl, editors, *Proceedings of the Twentieth European Symposium on Research in Computer Security (ESORICS)*, volume 9327 of *Lecture Notes in Computer Science*, pages 123–145. Springer-Verlag, Berlin Germany, 2015.

[7] David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel Rosu, and Michael Steiner. Dynamic searchable encryption in very-large databases: Data structures and implementation. In *Proceedings of the Symposium on Network and*

*Distributed Systems Security (NDSS 2014)*, San Diego, CA, February 2014. Internet Society.

[8] Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel C. Rosu, and Michael Steiner. Outsourced symmetric private information retrieval. In *Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS)*, Berlin, Germany, November 2013. ACM Press.

[9] David Cash, Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel Rosu, and Michael Steiner. Highly-scalable searchable symmetric encryption with support for boolean queries. In *Advances in Cryptology – CRYPTO '2013*, volume 8042 of *Lecture Notes in Computer Science*. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 2013.

[10] Ran Canetti, Suresh Chari, Shai Halevi, Birgit Pfitzmann, Arnab Roy, Michael Steiner, and Wietse Venema. Composable security analysis of OS services. In *Proceedings of the 9th Conference on Applied Cryptography and Network Security (ANCS)*, volume 6715 of *Lecture Notes in Computer Science*, pages 431–448, 2011.

[11] Suresh N. Chari, Vincenzo V. Diluoffo, Paul A. Karger, Elaine R. Palmer, Tal Rabin, Josyula R. Rao, Pankaj Rohotgi, Helmut Scherzer, Michael Steiner, and David C. Toll. Designing a side channel resistant random number generator. In *Proceedings of the Ninth Smart Card Research and Advanced Application Conference (CARDIS)*, volume 6035 of *Lecture Notes in Computer Science*, pages 49–64. Springer-Verlag, Berlin Germany, 2010.

[12] Sebastian Gajek, Jörg Schwenk, Michael Steiner, and Chen Xuan. Risks of the CardSpace protocol. In *12th International Conference on Information Security (ISC)*, volume 5735 of *Lecture Notes in Computer Science*, pages 278–293. Springer-Verlag, Berlin Germany, 2009.

[13] Paula Austel, Sumeer Bhola, Suresh Chari, Larry Koved, Michael McIntosh, Michael Steiner, and Samuel Weber. Secure delegation for Web 2.0 and mashups. In *Web 2.0 Security & Privacy Workshop*. IEEE Computer Society, Technical Committee on Security and Privacy, 2008.

[14] Frederik De Keukelaere, Sumeer Bhola, Michael Steiner, Suresh Chari, and Sachiko Yoshihama. SMash: Secure cross-domain mashups on unmodified browsers. In *Proceedings of the 17th International Conference on the World-Wide Web*, pages 535–544. ACM Press, 2008.

[15] K. Vikram and Michael Steiner. Mashup component isolation via server-side analysis and instrumentation. In *Web 2.0 Security & Privacy Workshop*. IEEE Computer Society, Technical Committee on Security and Privacy, 2007.

[16] Sumeer Bhola, Suresh Chari, and Michael Steiner. Security for web2.0 application scenarios: Exposures, issues and challenges. In *Web 2.0 Security & Privacy Workshop*. IEEE Computer Society, Technical Committee on Security and Privacy, 2007.

[17] Ran Canetti, Shai Halevi, and Michael Steiner. Mitigating dictionary attacks on password-protected local storage. In *Advances in Cryptology – CRYPTO '2006*, Lecture Notes in Computer Science, pages 160–179. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 2006.

[18] Liqun Chen, Matthias Enzmann, Ahmad-Reza Sadeghi, Markus Schneider, and Michael Steiner. A privacy-protecting coupon system. In *Proceedings of the Nineth Conference on Financial Cryptography (FC '05)*, volume 3570 of *Lecture Notes in Computer Science*,

pages 93–108, Roseau, The Commonwealth Of Dominica, 2005. International Financial Cryptography Association (IFCA), Springer-Verlag, Berlin Germany.

[19] Ran Canetti, Shai Halevi, and Michael Steiner. Hardness amplification of weakly verifiable puzzles. In *Theory of Cryptography Conference*, Lecture Notes in Computer Science, pages 17–33. Springer-Verlag, Berlin Germany, 2005.

[20] Naga Ayachitula, Suresh Chari, Josyula R. Rao, Michael Steiner, and Maheswaran Surendra. Autonomic enterprise security through orchestration. In *4th Annual Conference on Emerging Information Technology*, Princeton, NJ, USA, Oct 2004.

[21] Michael Backes, Birgit Pfitzmann, Michael Steiner, and Michael Waidner. Polynomial fairness and liveness. In *Proceedings of the 15th IEEE Computer Security Foundations Workshop*, pages 160–174. IEEE Computer Society Press, June 2002.

[22] Ahmad-Reza Sadeghi and Michael Steiner. Assumptions related to discrete logarithms: Why subtleties make a real difference. In Birgit Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT '2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 243–260, Innsbruck, Austria, 2001. Springer-Verlag, Berlin Germany.

[23] Peter Buhler, Thomas Eirich, Michael Steiner, and Michael Waidner. Secure password-based cipher suite for TLS. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '00)*, pages 129–142, San Diego, CA, February 2000. Internet Society.

[24] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. Authenticated group key agreement and friends. In *Proceedings of the 5th ACM Conference on Computer and Communications Security (CCS)*, pages 17–26, San Francisco, California, November 1998. ACM Press.

[25] N. Asokan, Els Van Herreweghen, and Michael Steiner. Towards a framework for handling disputes in payment systems. In *Proceedings of the 3rd USENIX Workshop on Electronic Commerce*, pages 187–202, Boston, Mass., September 1998. USENIX.

[26] Michael Steiner, Gene Tsudik, and Michael Waidner. CLIQUES: A new approach to group key agreement. In *Proceedings of the 18th International Conference on Distributed Computing Systems (ICDCS)*, pages 380–387, Amsterdam, May 1998. IEEE Computer Society Press.

[27] N. Asokan, Phil Janson, Michael Steiner, and Michael Waidner. Electronic payment systems. In *Public-Key Solutions 96*, September 1996.

[28] Ralf Hauser, Michael Steiner, and Michael Waidner. Micro-payments based on iKP. In *14th Worldwide Congress on Computer and Communications Security Protection*, pages 67–82, C.N.I.T Paris-La Defense, France, June 1996.

[29] Michael Steiner, Gene Tsudik, and Michael Waidner. Diffie-Hellman key distribution extended to groups. In Clifford Neuman, editor, *Proceedings of the 3rd ACM Conference on Computer and Communications Security (CCS)*, pages 31–37, New Delhi, India, March 1996. ACM Press.

[30] Mihir Bellare, Juan Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, and Michael Waidner. iKP – A family of secure electronic payment protocols. In *Proceedings of the First USENIX Workshop on Electronic Commerce*, pages 89–106, New York, July 1995. USENIX.

[31] Ralf Hauser and Michael Steiner. Generic extensions of WWW browsers. In *Proceedings of the First USENIX Workshop on Electronic Commerce*, pages 147–154, New York, July 1995. USENIX.

[32] Ralf Hauser, Günter Karjoth, and Michael Steiner. Management von sicherheitsdiensten in verteilten systemen. In Prof. Dr. Kurt Bauknecht and Dr. Stephanie Teufel, editors, *Sicherheit in Informationssystemen SIS'94*, Proceedings der Fachtagung SIS '94, Universität Zürich-Irchel, Institut für Informatik, pages 7–21. vdf Verlag der Fachvereine Zürich, March 1994.

- **Magazines**

[1] Sachiko Yoshihama, Frederik De Keukelaere, Michael Steiner, and Naohiko Uramoto. Overcome security threats for AJAX applications. *IBM developerWorks*, June 2007.

[2] Gérard Lacoste and Michael Steiner. SEMPER: A security framework for the global electronic marketplace. *comtec – the magazine for telecommunications technology*, 77(9):56–63, September 1999.

[3] N. Asokan, Phil Janson, Michael Steiner, and Michael Waidner. State of the art in electronic payment systems. *IEEE Computer*, 30(9):28–35, September 1997.

- **Unrefereed**

[1] Michael Steiner, Gene Tsudik, and Michael Waidner. Refinement and extension of Encrypted Key Exchange. *ACM Operating Systems Review*, 29(3):22–30, July 1995.

- **Project Deliverables (Editor)**

[1] Crypographic semantics for algebraic model. Deliverable D08, EU Project IST-1999-11583 Malicious- and Accidental-Fault Tolerance for Internet Applications (MAFTIA), February 2002.

[2] SEMPER Consortium. Final report. Public deliverable D13, ACTS Project AC026, 2000.

[3] SEMPER Consortium. Architecture, services and protocols. Deliverable D10, public specification, ACTS Project AC026, January 1999.

- **Technical Reports**

[1] Karim Eldefrawy, Ivan O. Nunes, Norrathep Rattanavipanon, Michael Steiner, and Gene Tsudik. Formally verified hardware/software co-design for remote attestation. Technical Report arXiv:1811.00175v1 [cs.CR], arXiv.org, November 2018.

[2] Mic Bowman, Andrea Miele, Michael Steiner, and Bruno Vavala. Private data objects: an overview. Technical Report arXiv:1807.05686v1 [cs.CR], arXiv.org, July 2018.

[3] Thomas Knauth, Michael Steiner, Somnath Chakrabarti, Li Lei, Cedric Xing, and Mona Vij. Integrating Remote Attestation with Transport Layer Security. Technical Report arXiv:1801.05863v1 [cs.CR], arXiv.org, 2018.

[4] Sky Faber, Stanislaw Jarecki, Hugo Krawczyk, Quan Nguyen, Marcel Rosu, and Michael Steiner. Rich queries on encrypted data: Beyond exact matches. Report 2015/927, Cryptology ePrint Archive, September 2015.

[5] David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel Rosu, and Michael Steiner. Dynamic searchable encryption in very-large databases: Data structures and implementation. Report 2014/853, Cryptology ePrint Archive, October 2014.

[6] Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel C. Rosu, and Michael Steiner. Outsourced symmetric private information retrieval. 2013/720, Cryptology ePrint Archive, November 2013.

[7] David Cash, Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel Rosu, and Michael Steiner. Highly-scalable searchable symmetric encryption with support for boolean queries. Report 2013/169, Cryptology ePrint Archive, March, revised in August 2013.

[8] Frederik De Keukelaere, Sumeer Bhola, Michael Steiner, Suresh Chari, and Sachiko Yoshihama. SMash: Secure cross-domain mashups on unmodified browsers. Technical Report RT0742, IBM Research, June 2007.

[9] Suresh Chari, Sudhakar Govindavajhala, Daisuke Nojiri, Josyula R. Rao, and Michael Steiner. Elix0r: Cost-effective incident response. Research Report RC 23765, IBM Research Division, Thomas J.Watson Research Center, Yorktown Heights, NY 10598, May 2004.

[10] Ahmad-Reza Sadeghi and Michael Steiner. Assumptions related to discrete logarithms: Why subtleties make a real difference. Report 2002/126, Cryptology ePrint Archive, August 2002.

[11] Final report on verification and assessment. Deliverable D22, EU Project IST-1999-11583 Malicious- and Accidental-Fault Tolerance for Internet Applications (MAFTIA), January 2003.

[12] Birgit Pfitzmann, Michael Steiner, and Michael Waidner. A formal model for multi-party group key agreement. Technical Report RZ 3383 (# 93419), IBM Research, 2002.

[13] Mihir Bellare, Juan Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Els Van Herreweghen, and Michael Waidner. Design, implementation and deployment of a secure account-based electronic payment system. Research Report RZ 3137, IBM Research Division, June 1999.

[14] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. New multi-party authentication services and key agreement protocols. Research Report RZ 3115 (# 93161), IBM Research, March 1999.

[15] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. Authenticated group key agreement and friends. Research Report RZ 3063 (#93109), IBM Research, October 1998.

[16] N. Asokan, Els Van Herreweghen, and Michael Steiner. Towards a framework for handling disputes in payment systems. Research Report RZ 2996, IBM Research, March 1998.

[17] Michael Steiner, Gene Tsudik, and Michael Waidner. CLIQUES: A new approach to group key agreement. Research Report RZ 2984 (# 93030), IBM Research, December 1997.

[18] Jose L. Abad-Peiro, N. Asokan, Michael Steiner, and Michael Waidner. Designing a generic payment service. Research Report RZ 2891 (# 90839), IBM Research, December 1996.

[19] N. Asokan, Phil Janson, Michael Steiner, and Michael Waidner. Electronic payment systems. Research Report RZ 2890 (# 90838), IBM Research, December 1996.

[20] Ralf Hauser, Michael Steiner, and Michael Waidner. Micro-payments based on iKP. Research Report 2791 (# 89269), IBM Research, February 1996.

Many of above publications can be found in electronic form on the Internet[8] .

## Lectures and Talks

- Invited tutorial on secure electronic commerce and participation at panel at COMDEX Internet, Frankfurt, October 1997.
- Invited lecture on security in electronic commerce as part of the Postgraduate Course in Computer Science "Distributed Systems", École Polytechnique Fédérale de Lausanne (EPFL), May, 1999.
- Keynote talks: "Searchable Encryption for the Real World: Theory and Practice" IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, September 2014;
- Conference talks (see section on publications for more details): EITC, Princeton, October, 2004; NDSS, San Diego, February 2000; SecuriCom, Paris, June 1996; 3rd ACM CCS, New Delhi, March 1996; SIS, Zurich, March 1994.
- Invited seminar talks: "Searchable Encryption for the Real World: Theory and Practice" Technische Universität Darmstadt, September 2014; "Secure Password-Based Cipher Suite for TLS", Johns Hopkins University, June 2000; "Secure password-based cipher suite for TLS: The importance of end-to-end security", University of Helsinki, November 2000; "Fairness in Electronic Commerce", Technische Universität Darmstadt, July 1998; "SEMPER", ISACA Internet Seminar, Zurich, August 1997.
- Further Presentations: "Architecture of SEMPER", 2nd Public SEMPER Workshop, Zurich, November 1998; "Secure Electronic Marketplace for Europe", ICX Workshop, London, February 1998; Various presentations at IBM-wide Technical Symposia in 1995, 1996 & 1997.

## Teaching

- Course on advanced cryptographic protocols, Winter 2001/2002.
- Seminar Internet security, Winter 2001/2002 (with A. Feldman, S. Steinbrecher & R. Sommer).
- Seminar cryptographic protocols, Sommer 2000 (with M. Schunter & T. Beiler).
- One semester introductory course in programming for secondary school teachers, 1985.

## Service

- Program Committee Member:
  - 7th ACM Conference on Computer and Communication Security, Nov. 2000, Athens;
  - 8th ACM Conference on Computer and Communication Security, Nov. 2001, Philadelphia;
  - 7th European Symposium on Research in Computer Science (ESORICS), Oct. 2002, Zurich.
  - 8th European Symposium on Research in Computer Science (ESORICS), Oct. 2003, Gjovik.
  - 9th European Symposium on Research in Computer Science (ESORICS), Oct. 2004, Nice.
  - Symposium on Research in Security and Privacy, May 2004, Oakland.
  - Symposium on Research in Security and Privacy, May 2007, Oakland.
  - ACM Symposium on Information, Computer and Communications Security (AsiaCCS), March 2006, Taipei, Taiwan.
  - 10th Information Security Conference (ISC'07), October 2007, Valparaiso, Chile.
  - 1st International Workshop on Group-Oriented Cryptographic Protocols (GOCP 2007), July 2007, Wroclaw, Poland. (held in conjunction with the 34th International Colloquium on Automata, Languages and Programming – ICALP 2007.)
  - 17th International World Wide Web Conference, Security & Privacy Track, Bejing, China, April 2008.
  - 18th International World Wide Web Conference, Security & Privacy Track, Madrid, Spain, April 2009.
  - 12th International Workshop on Practice and Theory in Public Key Cryptography (PKC), March 18-20, 2009, Irvine, CA, USA.
  - 12th Information Security Conference (ISC'09), September 2009, Pisa, Italy.
  - 4th ACM Conference on Wireless Network Security (WiSec'11), June 2011, Hamburg, Germany.
  - 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'12), April 2012, Tuscon, AZ, USA.
  - 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'13), April 2013, Budapest, Hungary.
  - 13th International Conference on Applied Cryptography and Network Security (ACNS 2015), June 2015, New York, USA.

  (Invitation to join the PC of the 9th ACM Conference on Computer and Communication Security, 2002 declined for time reasons).

- Reviewer: ACM Transactions on Information and System Security, IEEE Transactions on Computers, IEEE Personal Communications, IEEE Internet Computing, Computer Communication Review, Computer Networks and ISDN Systems, Information Processing Letters, IBM Journal of Research and Development, IBM System Journal, Springer Journal of Digital Libraries, Acta Cybernetica, ETRI Journal, Eurocrypt, NDSS, PERVASIV.

- Invited to evaluate project proposals for the EU IST Priority Call 1, the Research Council of Norway and the ETH, Zurich.
- Invited participant in workshop "Trust & Confidence in electronic commerce". Preparation of the strategic content for the 5th Framework of european RTD projects, March 1998.
- Member of the personal commission in the IBM Research Laboratory from 1997 - 1999

## Miscellaneous

- Awards
  - IBM Outstanding Technical Achievement Awards, August 1996 and December 2005.
  - IBM Research Division Awards, December 1995, December 1998 and June 2007.
  - IBM Invention Achievement Awards, November 1999 (First Plateau), June 2005 (Second Plateau), December 2006 (Third Plateau) and June 2009 (Fourth Plateau).
  - ISOC Best Paper Award, NDSS'2000, February, 2000.
  - IBM Personal Systems Institute Award for Prize Winning Design in the Advanced PC Device Contest, October, 2000.
- Grants: Graduiertenkolleg "Effizienz und Komplexität von Algorithmen und Rechenanlagen", Deutsche Forschungsgesellschaft, April 1999 - September 2000.
- Patents: Seventeen patents granted and several patent applications under evaluation.
- Membership: Senior Member of the ACM (SIGSAC & SIGOPS), Member of the IEEE Computer Society.

## Personal

- Citizenship: Switzerland / USA.
- Languages: german(mother tongue), english(fluent), french(good).
- Hobbies: cycling, soaring and skiing. Likes contemporary literature, music and playing violoncello.

## References

- *Available on on request*

### Notes

[1] http://domino.research.ibm.com/comm/research_teams.nsf/pages/sss-dept.index.html

[2] http://krypt.cs.uni-sb.de/index_eng.html

[3] http://www.maftia.org/

[4] http://krypt.cs.uni-sb.de/index_eng.html

[5] http://www.zurich.ibm.com/security/

[6] http://www.zurich.ibm.com/security/past-projects/ecommerce/iKP.html

[7] http://www.semper.org

[8] http://www.semper.org/sirene/lit/sirene.lit.html