Curriculum Vitae of Gregory Neven

IBM Research – Zurich
Säumerstrasse 4
8803 Rüschlikon
Switzerland

Work phone: +41-44-724 82 62
Fax: +41-44-724 89 53
Email: nev@zurich.ibm.com
Web page : http://www.neven.org

Research Interests

- Cryptography and information security in general
- Provably secure cryptography
- Policy languages for access control and privacy

Education

- Ph.D. in Applied Sciences, option Computer Science
  Katholieke Universiteit Leuven, May 2004
  Thesis: Provably Secure Identity-Based Identification Schemes and Transitive Signatures
  Advisors: Frank Piessens and Bart De Decker
- Burgerlijk Ingenieur in de Computerwetenschappen (cfr. MSE in Computer Science), summa cum laude
  Katholieke Universiteit Leuven, July 2000
  Thesis: Secure Distributed Computing
  Advisor: Frank Piessens

Work Experience

- April 2008 – present: Research Staff Member at IBM Zurich Research Laboratory, engaged in several EU projects including PrimeLife, ABC4Trust, FI-WARE, FutureID
- October 2005 – March 2008: Postdoctoral Fellow of the Research Foundation – Flanders (F.W.O.-Vlaanderen) at SCD-COSIC, Department of Electrical Engineering, Katholieke Universiteit Leuven
- October 2005 – September 2006: Visiting postdoctoral researcher at Ecole Normale Supérieure (ENS), Paris
- October 2004 – September 2005: Postdoctoral researcher at SCD-COSIC, Department of Electrical Engineering, Katholieke Universiteit Leuven
- October 2000 – September 2004: Research Assistant of the Fund for Scientific Research – Flanders, Belgium (F.W.O.-Vlaanderen) at Distrinet group, Department of Computer Science, Katholieke Universiteit Leuven
- July 2004 – September 2004: Visiting scholar at University of California at San Diego (UCSD), working with Mihir Bellare and Chong Zhang on accurate metering schemes
- July 2003 – October 2003: Visiting scholar at University of California at San Diego (UCSD), working with Mihir Bellare and Chanathip Namprempre on identity-based identification and signature schemes
- January 2002 – September 2002: Visiting scholar at University of California at San Diego (UCSD), working with Mihir Bellare on transitive signatures
- April 2000 – December 2002: Co-founder and part-time software engineer at Business Integration Company nv (BICO, later called QMedit), a startup focused on business application integration for the healthcare sector.

Professional Activities

- Author of over 50 scientific publications, four book chapters, one book, and seven patents in the fields of cryptography and privacy policy languages. (Total of 1650 citations with h-index 19 on Google Scholar).
- Keynote speaker at IFIP Summer School on Privacy 2011, PQCrypto 2010, Digital Identity Management 2010, PrimeLife Summer School 2010, IFIP Summer School 2011.
- Program Chair of LatinCrypt 2012
- Program committee member of PETS 2011 and 2012, SCN 2012, ESORICS 2011, Eurocrypt 2008, ESORICS 2011, Provsec 2010, Pairing 2009, WPES 2009, PrimeLife Summer School 2010 and 2011, Indocrypt 2006, International Conference on Security of Information and Networks (SIN) 2007, Information Security Conference (ISC) 2007 and 2009, MyCrypt 2005, and WISA 2005.
- Member of editorial board of IOS Press Series on Advances in Cryptology and Information Security (ACIS)
- Member of the OASIS SAML and XACML technical committees.

Personal Information

- Born in Maasmechelen, Belgium, on January 28, 1978
- Citizen of Belgium
- Spoken languages: Dutch (native), English (fluent), French (fluent), German (fluent), Swiss-German (fluent), and Spanish (notion)

Publications

- Articles in international reviewed journals:
    - Gregory Neven. Efficient sequential aggregate signed data. IEEE Transactions on Information Theory, 57(3), pages 1803-1815, 2011.
    - Michel Abdalla, James Birkett, Dario Catalano, Alexander W. Dent, John Malone-Lee, Gregory Neven, Jacob C. N. Schuldt, and Nigel P. Smart. Wildcarded identity-based encryption. Journal of Cryptology 24(1), pages 42-82, 2011.
    - Claudio A. Ardagna, Jan Camenisch, Markulf Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer, and Mario Verdicchio. Exploiting cryptography for privacy-enhanced access control. Journal of Computer Security 18(1), pages 123-160, 2010.
    - Gregory Neven, Nigel Smart, and Bogdan Warinschi. Hash function requirements for Schnorr signatures. Journal of Mathematical Cryptology 3(1), pages 69-87, 2009.
    - Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security proofs for identity-based identification and signature schemes. Journal of Cryptology 22(1), pages 1-61, 2009.
    - Michel Abdalla, Eike Kiltz, and Gregory Neven. Generalized key delegation for hierarchical identity-based encryption. IET Information Security 2(3), pages 67-78, 2008.
    - Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions. Journal of Cryptology 21(3), pages 350-391, 2008.
    - Gregory Neven. A simple transitive signature scheme for directed trees. Theoretical Computer Science 396(1-3), pages 277-282, 2008.
    - Zekeriya Erkin, Alessandro Piva, Stefan Katzenbeisser, Reginald L. Lagendijk, Jamshid Shokrollahi, Gregory Neven and Mauro Barni. Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing. EURASIP Journal on Information Security, vol. 2007, article ID 78943, 20 pages, 2007.
    - Chanathip Namprempre, Gregory Neven and Michel Abdalla. A study of blind message authentication codes. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E-90A(1), pages 75-82, January 2007.
    - M. Bellare and G. Neven. *Transitive Signatures: New Schemes and Proofs*. IEEE Transactions on Information Theory, 51(6), June 2005, pp. 2133-2151.
    - G. Neven, E. Van Hoeymissen, B. De Decker and F. Piessens. *Enabling Secure Distributed Computations: Semi-trusted Hosts and Mobile Agents*. In Networking and Information Systems Journal 3 (2000), Hermes Science Publications, pp. 1-18.
- Contributions at international congresses and symposia, completely published in proceedings:
    - Jan Camenisch, Maria Dubovitskaya, Gregory Neven, and Gregory M. Zaverucha. Oblivious transfer with hidden access control policies. In D. Catalano, N. Fazio, R. Gennaro and A. Nicolosi, editors, Public Key Cryptography - PKC 2011, volume 6571 of Lecture Notes in Computer Science, pages 192-209. Springer, 2011.
    - Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Sara Foresti, Gregory Neven, Stefano Paraboschi, Franz-Stefan Preiss, Pierangela Samarati, and Mario Verdicchio. Fine-grained disclosure of access policies. In M. Soriano, S. Qing, J. López, editors, 12th International Conference on Information and Communications Security - ICICS 2010, volume 6476 of Lecture Notes in Computer Science, pages 16-30. Springer, 2010.
    - Patrik Bichsel, Jan Camenisch, Gregory Neven, Nigel P. Smart, and Bogdan Warinschi. Get Shorty via group signatures without encryption. In J. Garay and R. De Prisco, editors, 7th International Conference on Security and Cryptography for

Networks - SCN 2010, volume 6280 of Lecture Notes in Computer Science, pages 381-398. Springer, 2010.

- Laurent Bussard, Gregory Neven, and Franz-Stefan Preiss. Downstream usage control. In IEEE International Symposium on Policies for Distributed Systems and Networks - POLICY 2010, pages 22-29. IEEE Computer Society, 2010.
- Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Gregory Neven, Stefano Paraboschi, Franz-Stefan Preiss, Pierangela Samarati, and Mario Verdicchio. Enabling privacy-preserving credential-based access control with XACML and SAML. In 10th IEEE International Conference on Computer and Information Technology - CIT 2010, pages 1090-1095. IEEE Computer Society, 2010.
- Jan Camenisch, Sebastian Mödersheim, Gregory Neven, Franz-Stefan Preiss, and Dieter Sommer. A card requirements language enabling privacy-preserving access control. In J. Joshi and B. Carminati, editors, 15th ACM Symposium on Access Control Models and Technologies - SACMAT 2010, pages 119-128. ACM, 2010.
- Jan Camenisch, Maria Dubovitskaya, and Gregory Neven. Unlinkable priced oblivious transfer with rechargeable wallets. In R. Sion, editor, 14th International Conference on Financial Cryptography and Data Security - FC 2010, volume 6052 of Lecture Notes in Computer Science, pages 66-81. Springer, 2010.
- Jan Camenisch and Gregory Neven. Saving on-line privacy. In M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, and G. Zhang, editors, Privacy and Identity Management for Life, volume 320 of IFIP Advances in Information and Communication Technology, pages 34-47. Springer, 2010.
- Michel Abdalla, Mihir Bellare, and Gregory Neven. Robust encryption. In D. Micciancio, editor, 7th Theory of Cryptography Conference - TCC 2010, volume 5978 of Lecture Notes in Computer Science, pages 480-497. Springer, 2010.
- Jan Camenisch, Maria Dubovitskaya and Gregory Neven. Oblivious transfer with access control. In E. Al-Shaer, S. Jha, and A. Keromytis, editors, Proceedings of the 2009 ACM Conference on Computer and Communications Security, pages 131-140. ACM Press, 2009.
- Gregory Neven. Efficient sequential aggregate signed data. In N. Smart, editor, Advances in Cryptology - EUROCRYPT 2008, volume 4965 of Lecture Notes in Computer Science, pages 52–69. Springer, 2008.
- Elena Andreeva, Gregory Neven, Bart Preneel and Thomas Shrimpton. Seven-Property-Preserving Iterated Hashing: ROX. In K. Kurosawa, editor, Advances in Cryptology - ASIACRYPT 2007, volume 4833 of Lecture Notes in Computer Science, pages 130-146. Springer, 2007.
- Michel Abdalla, Eike Kiltz and Gregory Neven. Generalized key delegation for hierarchical identity-based encryption. In J. Biskup, and J. Lopez, editors, Computer Security - ESORICS 2007, volume 4734 of Lecture Notes in Computer Science, pages 139-154. Springer, 2007.
- Mihir Bellare, Chanathip Namprempre and Gregory Neven. Unrestricted aggregate signatures. In L. Arge, C. Cachin, T. Jurdzinski, and A. Tarlecki, editors, 34th International Colloquium on Automata, Languages and Programming - ICALP 2007, volume 4596 of Lecture Notes in Computer Science, pages 411-422. Springer, 2007.
- James Birkett, Alexander W. Dent, Gregory Neven and Jacob C. N. Schuldt. Efficient chosen-ciphertext secure identity-based encryption with wildcards. In J. Pieprzyk, H. Ghodosi, and E. Dawson, editors, 12th Australasian Conference on Information Security and Privacy - ACISP 2007, volume 4586 of Lecture Notes in Computer Science, pages 274-292. Springer, 2007.

- Jan Camenisch, Gregory Neven and abhi shelat. Simulatable adaptive oblivious transfer. In M. Naor, editor, Advances in Cryptology - EUROCRYPT 2007, volume 4515 of Lecture Notes in Computer Science, pages 573-590. Springer, 2007.
- Elena Andreeva, Gregory Neven, Bart Preneel and Thomas Shrimpton. Three-property preserving iterations of keyless compression functions. ECRYPT Workshop on Hash Functions 2007, electronically available from http://events.iaik.tugraz.at/HashWorkshop07/.
- Michel Abdalla, Alexander W. Dent, John Malone-Lee, Gregory Neven, Duong Hieu Phan and Nigel P. Smart. Identity-based traitor tracing. In T. Okamoto and X. Wang, editors, Public Key Cryptography - PKC 2007, volume 4450 of Lecture Notes in Computer Science, pages 458-476. Springer, 2007.
- M. Bellare and G. Neven. Identity-based multi-signatures from RSA. To appear in M. Abe, ed., Topics in Cryptology – CT-RSA 2007, volume ? of Lecture Notes in Computer Science, pages ?-?. Springer-Verlag, 2007.
- M. Bellare and G. Neven. Multi-signatures in the plain public-key model and a general forking lemma. In R. N. Wright, S. De Capitani di Vimercati, and V. Shmatikov, editors, Proceedings of the 13th ACM Conference on Computer and Communications Security, pages 390-399. ACM Press, 2006.
- M. Abdalla, D. Catalano, A. W. Dent, J. Malone-Lee, G. Neven and N. Smart. Identity-based encryption gone wild. To appear in B. Preneel, ed., ICALP 2006, volume ???? of Lecture Notes in Computer Science, pages 1-12. Springer-Verlag, 2006.
- K. Kursawe, G. Neven and P. Tuyls. Private policy negotiation. To appear in G. Di Crescenzo and A. Rubin, eds., Financial Cryptography 2006, volume ???? of Lecture Notes in Computer Science, pages 1-15. Springer-Verlag, 2006.
- M. Abdalla, C. Namprempre and G. Neven. On the (im)possibility of blind message authentication codes. In D. Pointcheval, ed, Topics in Cryptology - CT-RSA 2006, volume 3860 of Lecture Notes in Computer Science, pages 262-279. Springer-Verlag, 2006.
- M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier and H. Shi. *Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions.* In Advances in Cryptology – CRYPTO 2005, V. Shoup ed., Lecture Notes in Computer Science, vol. 3621, Springer-Verlag, 2005, pp. 205-222.
- M. Bellare, C. Namprempre and G. Neven. *Security Proofs for Identity-Based Identification and Signature Schemes.* In Advances in Cryptology – EUROCRYPT 2004, C. Cachin and J. Camenisch eds., Lecture Notes in Computer Science, vol. 3027, Springer-Verlag, 2004, pp. 468-486.
- M. Bellare and G. Neven. *Transitive Signatures based on Factoring and RSA*. In Advances in Cryptology – ASIACRYPT 2002, Y. Zheng ed., Lecture Notes in Computer Science, vol. 2501, Springer-Verlag, 2002, pp. 397-414.
- B. De Decker, G. Neven and F. Piessens. *Secure Vickrey Auctions without a Trusted Third Party.* In Security and Privacy in the Age of Uncertainty, IFIP TC11 18th International Conference on Information Security (SEC2003), D. Gritzalis, S. de Capitani di Vimercati, P. Samarati and S. Katsikas eds., IFIP Conference Proceedings 250, Kluwer Academic Publishers, 2003, pp. 337-348.
- B. De Decker, G. Neven, F. Piessens and E. Van Hoeymissen. *Second Price Auctions: a Case Study of Secure Distributed Computing.* In New Developments in Distributed Applications and Interoperable Systems, K. Zielinski, K. Geihs and A. Laurentowski eds., Kluwer Academic Publishers, 2001, pp. 217-228.
- T. Herlea, J. Claessens, G. Neven, F. Piessens, B. Preneel and B. De Decker. *On Securely Scheduling a Meeting.* In Trusted Information - The New Decade

Challenge, Michel Dupuy and Pierre Paradinas (eds.), IFIP Conference Proceedings 193, Kluwer Academic Publishers, 2001, pp. 183-198.

- B. De Decker, F. Piessens, E. Van Hoeymissen and G. Neven. *Semi-trusted Hosts and Mobile Agents: Enabling Secure Distributed Computations.* In Mobile Agents for Telecommunications Applications, E. Horlait (ed.), Lecture Notes in Computer Science, vol. 1931, Springer, 2000, pp. 219-232.
- G. Neven, F. Piessens and B. De Decker. *On the Practical Feasibility of Secure Distributed Computing: a Case Study.* In Information Security for Global Information Infrastructures, S. Qing and J. Eloff (eds.), Kluwer Academic Publishers, 2000, pp. 361-370.

- Contributions at international congresses and symposia, only abstract published:
  - S. Van den Enden, E. Van Hoeymissen, G. Neven and P. Verbaeten. *A Case Study in Application Integration.* In OOPSLA Business Objects and Components Design and Implementation Workshop VI: Enterprise Application Integration, October 2000, Minneapolis, Minnesota (USA).
  - F. Piessens, B. De Decker, E. Van Hoeymissen and G. Neven. *On the Trade-Off between Communication and Trust in Secure Computations*. In ECOOP Workshop on Mobile Object Systems, Cannes, France, June 13, 2000.
- Books
  - Marc Joye and Gregory Neven, editors. Identity-based cryptography. Volume 2 of Cryptology and Information Security Series. IOS Press, 2008.
- Book chapters
  - Laurent Bussard, Gregory Neven, and Franz-Stefan Preiss. Matching privacy policies and preferences: access control, obligations, authorisations, and downstream usage. In J. Camenisch, S. Fischer-Hübner, and K. Rannenberg, editors, Privacy and identity management for life, pages 313-326. Springer, 2011.
  - Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Gregory Neven, Stefano Paraboschi, Eros Pedrini, Franz-Stefan Preiss, Pierangela Samarati, and Mario Verdicchio. Advances in access control policies. In J. Camenisch, S. Fischer-Hübner, and K. Rannenberg, editors, Privacy and identity management for life, pages 327-342. Springer, 2011.
  - Jan Camenisch, Maria Dubovitskaya, Markulf Kohlweiss, Jorn Lapon, and Gregory Neven. Cryptographic mechanisms for privacy. In J. Camenisch, S. Fischer-Hübner, and K. Rannenberg, editors, Privacy and identity management for life, pages 117-134. Springer, 2011.
  - Eike Kiltz and Gregory Neven. Identity-based signatures. In M. Joye and G. Neven, editors, Identity-based cryptography, volume 2 of Cryptology and Information Security Series, pages 31-44. IOS Press, 2008.