Gregory Neven

Katholieke Universiteit Leuven
Departement Computerwetenschappen
Celestijnenlaan 200A
B-3001 Heverlee-Leuven
Belgium

Work phone: +32-16-32 78 36
Mobile: +32-486-44 44 23
Fax: +32-16-32 79 96
Gregory.Neven@cs.kuleuven.ac.be
http://www.cs.kuleuven.ac.be/~gregory

Research Interests

- Cryptography and information security in general
- Provably secure public-key cryptography in particular

Education

- Ph.D. in Applied Sciences, option Computer Science.
  Katholieke Universiteit Leuven, May 2004
  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
  Thesis advisor: Frank Piessens

Work Experience

- October 2000 – Present: Research Assistant of the Fund for Scientific Research – Flanders, Belgium (F.W.O.-Vlaanderen)
- 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 schemes
- January 2002 – September 2002: Visiting scholar at University of California at San Diego (UCSD), working with Mihir Bellare on transitive signatures

Teaching Experience

- Guidance of the following Master Theses at K.U.Leuven:
  - Group-oriented digital signatures, by Kristof Verslype, 2003-2004
  - Anonymous broadcast and multicast, by Jo De Muynck, 2003-2004
  - Advanced signature primitives, by Liesje Demuynck, 2002-2003
  - A secure Vickrey auction without trusted third party, by Johan Daems, 2001-2002
  - Security in XML documents, by Gwyn Nuyts and Sven Van den Eynde, 2001-2002
- Teaching Assistant for the course on Secure Software Engineering taught by Frank Piessens at K.U.Leuven during academic years 2000-2001, 2001-2002, 2002-2003 and 2003-2004
- Teaching Assistant for the course on Operating Systems taught by Bart De Decker at K.U.Leuven during academic years 2000-2001 and 2003-2004
- An introduction to XML, tutorial at ADA Europe 2001 Conference
- Co-teaching of KVIV course module on Secure Software Engineering at K.U.Leuven, October 2000 (KVIV is the professional association of Flemish engineers)

Awards

- Winner of the IBM Belgium Awards for Informatics, 2001
- Laureate of the KVIV Thesis Award, 2000
- Third prize in Krypton Thesis Award, 2000

Professional Activities

- Invited talks:
  - Security proofs for identity-based identification and signature schemes, at IBM Zurich Research Laboratory, February 16th 2004, at the invitation of Christian Cachin
  - Transitive signatures based on factoring and RSA, at Université Catholique de Louvain-la-Neuve, May 27th 2003, at the inivation of Jean-Jacques Quisquater
  - Transitive signatures based on factoring and RSA, at University of California at San Diego, September 29th 2002, at the invitation of Mihir Bellare
  - Secure function evaluation using quadratic residuosity, at K.U.Leuven Department of Mathematics, April 25th 2001, at the invitation of Jan Denef
- External reviewer for the following conferences and journals:
  - Applied Cryptography and Network Security (ACNS) 2004
  - IFIP International Information Security Conference (SEC) 2004
  - Information Processing Letters (IPL)
  - First Theory of Cryptography Conference (TCC) 2004
  - Conference on Communications and Multimedia Security (CMS) 2003
  - Information Security Conference (ISC) 2003
  - International Conference on Information Security and Cryptology (ICISC) 2003
  - IFIP Working Conference on Network Security (I-NetSec) 2001

Publications

- Articles in international reviewed journals:
  - 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:
  - 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.

Personal Information

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

References

- **Prof. Mihir Bellare**
  Department of Computer Science & Engineering, University of California at San Diego
  9500 Gilman Drive
  La Jolla, CA 92093-0114, USA
  Phone: +1-858-534-4544
  Email: mihir@cs.ucsd.edu

- **Prof. Frank Piessens**
  Departement Computerwetenschappen, Katholieke Universiteit Leuven
  Celestijnenlaan 200A
  B-3001 Heverlee-Leuven, Belgium
  Phone: +32-16-32 76 03
  Email: Frank.Piessens@cs.kuleuven.ac.be

- **Prof. Bart Preneel**
  ESAT-COSIC, Katholieke Universiteit Leuven
  Kasteelpark Arenberg 10
  B-3001 Heverlee-Leuven, Belgium
  Phone: +32-16-32 11 48
  Email: Bart.Preneel@esat.kuleuven.ac.be