Jaarverslag en onderzoeksrapportage 2009

Dit is het tweede volle jaar dat Ei/Ψ actief is. We zijn er trots op dat twee gezamenlijke onderzoeksvoorstellen door STW gehonoreerd zijn.
De eerste verjaardag van Ei/Ψ is gevierd met een symposium waar 86 mensen aan deelnamen.

Wetenschappelijke activiteiten in 2009

EiPSI Seminar

4 maart Patrick Hof, *Practical Security and Crypto: Why Mallory Sometimes Doesn't Care*
18 maart Gaetan Bisson, *Computing endomorphism rings of ordinary elliptic curves over finite fields*
1 april Christiane Peters, *Explicit Bounds for Generic Decoding Algorithms for Code-Based Cryptography*
15 april José Villegas Bautista, *On Secure Integer Comparison*
13 mei Simona Orzan, *Titel onbekend*
10 juni Jiqiang Lu, *Security of AES against Differential Power Analysis*
24 juni Fred Spiessens & Daniel Trivellato, *Protecting Information with Polipo Security Policies*
16 sept. Boris Škorić, *Quantum Readout of Physical Unclonable Functions*
4 nov. Bárbara Vieira, *Correctness with respect to reference implementations*
18 nov. Boris Škorić & Fred Spiessens, *Reputations in Polipo*

TU/e-Philips Colloquium

2 juli Bart van Rijnsoever, *Overview activities Research Group Information & System Security*
23 sept. Boris Škorić, *Quantum Readout of Physical Unclonable Functions*
3 dec. Emile Kelkboom, *An Analysis of the Relationship between Privacy, Security and Convenience of a Template Protection System*

Cryptography Working Group

20 febr. Lejla Batina, *Recent Developments in Side-Channel Attacks*
José Villegas Bautista, *Verifiable Rotators of Homomorphic Encryptions*
Balazs Dosa, *Traitor Tracing in Broadcast Networks*
Christiane Peters, *Advances in Information-Set Decoding*

2 okt. Cees Jansen, *Towards Mickey's LEB*
Jurjen Bos, *Leakage-Resilient Storage*

Michael Naehrig, *Efficient computation of pairings on elliptic curves*
Ruden Teuben, *Related-Key attacks on AES*

4 dec. Jeroen Doumen, *Recent attacks on AES: should we be worried?*
Peter Schwabe, *Implementing Wagner's generalized birthday attack*
Lejla Batina, *Differential cluster analysis*
Dan Bernstein, *Breaking ECC2K-130*

First Anniversary of EiPSI

24 april Andy Clark, *Security Delusions and the Madness of Crowds*
Boris Škorić, *Security with noisy data*
Benne de Weger, *MD5 considered harmful today*
David Naccache, *Defensive Finite-State Automata*

Workshops

- SPEED-CC -- Software Performance Enhancement for Encryption and Decryption and Cryptographic Compilers, Oktober 12-13, 2009, Berlijn
- WISSEC 2009: 4th Benelux Workshop on Information and System Security November 19-20, 2009, Louvain-la-Neuve

Personele activiteiten in 2009

- Aanstelling van Milan Petkovic als deeltijdhoogleraar in de SEC groep.
- Werving van de Ph.D. studenten Dion Boesten en Jan Jaap Oosterwijk voor het CREST project.
- Werving van de Ph.D. student Meilof Veeningen voor het "Identity Management for Mobile Devices" project.
- Werving van de Ph.D. student Antonino Simone voor het "Collusion Resistant Watermarking Codes" project.
- Werving van de Ph.D. studente Xiaoping Liang voor het TAS3 project.
- Werving van de Ph.D. studente Mayla Brusò voor het PEARL project.
- Afscheid van Fred Spiessen.

Blijken van externe waardering

Peter Birkner

Sandro Etalle

Tanja Lange
Lid van buitenlandse promotiecommissie:
Invited speaker at:

Christiane Peters

Ruud Pellikaan

Lid van buitenlandse promotiecommissie

Berry Schoenmakers

Betrokkenheid bij organisatie van symposia, conferenties, e.d.

Sandro Etalle

Co-PC-Chair of
PC Member of

- The 3rd IFIP International Conference on Trust Management (TM'09). June 15-19, 2009 Purdue University, West Lafayette, USA. Deadline: January 12th. PC member.
- Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security Affiliated with ETAPS 2009 York, UK March 28 (Sat) and 29 (Sun), 2009. PC Member.
- 2009 IEEE International Conference on Information Privacy Security, Risk and Trust, August 29-31, Vancouver, CA. (PC member)
- Selfstrus'09, Athens/Glyfada, Greece, November 15-20
- BDIM '09, New York, USA, June 1
- WITS '09, York, UK, March 28-29

Jerry den Hartog

PC Member of

- Workshop on Foundations of Computer Security (FCS 2009), Los Angeles USA, August 10th
- Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'09), York UK, March 28-29

Tanja Lange

Main organizer and PC Chair of
PC member of:

-

Member of steering committees:

Jiqiang Lu

PC member of

- The 7th IEEE International Conference on e-Business Engineering (ICEBE '10), 20-22 October 2010, Shanghai, China.
- The Second International ICST Conference on Security and Privacy in Mobile Information and Communication Systems(Mobisec '10), 26-28 May 2010, Catania, Italy.
- The 5th International Conference on Future Information Technology (FutureTech '10), 21-23 May 2010, Busan, Korea.
- The 6th IEEE International Conference on e-Business Engineering (ICEBE '09), 21-23 October 2009, Macau, China.

Ruud Pellikaan

Invited lectures

Berry Schoenmakers

Co-chair of

PC member of

Henk van Tilborg

Organizer of the

- Cryptography Working Group meetings
- Ei/Ψ's e .

PC lid van

- Program Committee Member of WCC2009, Ullensvang, Norway, May 10-15, 2009.
- Program Committee Member of YACC 2010, Porquerolles Island, France, October 4-8, 2010.

Benne de Weger

Nicola Zannone

PC member of

- **Fourth International Workshop on Data Privacy Management (DPM 2009), September 24, 2009, Saint Malo, France.**
- **International Workshop on Security Measurements and Metrics (MetriSec 2009), October 14, 2009, Lake Buena Vista, Florida, USA.**
- **12th International Conference on Network-Based Information Systems (NBiS 2009), August 19-21, 2009, Indianapolis, USA.**
- **International Conference on Security and Cryptography (SECRYPT 2009), 7-10 July 7-10, 2009, Milan, Italy.**
- **3rd International Conference on Network and System Security (NSS 2009), 19-21 October, 2009, Gold Coast, Australia.**
- **2nd International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ 2009), July 19-24, 2009, Colmar, France.**
- **Program committee member, 4th International Conference on Availability, Reliability and Security (ARES 2009), 16-19 March, 2009, Fukuoka, Japan.**

Publication chair of

- **International Symposium on Engineering Secure Software and Systems (ESSoS 2009), 4-6 February, 2009, Leuven, Belgium.**

Editorial werk

Andries Brouwer

- Journal of Algebraic Combinatorics
- European Journal of Combinatorics

Sandro Etalle

Jerry den Hartog

- Coeditor Special Issue of the Journal of Automated Reasoning on Computer Security: Foundations and Automated Reasoning (JAR-CS'09)

Tanja Lange

- Editor of Journal of Applicable Algebra in Engineering, Applicable Algebra in Engineering (AAECC)
- Editor of Advances In Mathematics of Communications.

Berry Schoenmakers

- Editor of International Journal of Applied Cryptography (IJACT)

Henk van Tilborg

- Associate Editor of *Designs, Codes and Cryptography*.
- Associate Editor of the *Journal of Combinatorics, Information & System Sciences*.
- Advisory Editor of *Advances In Mathematics Of Communications*.
- Editor of *Asian-European Journal of Mathematics*.
- Associate editor for *Journal of the Indonesian Mathematical Society*.

Advies commissies

Lopende en gehonoreerde projecten (zie http://www.win.tue.nl/sec/research.html of http://www.win.tue.nl/dw/cc/)

- TAS^3 IP/Trust Management (EU Integrated Project), 2008-2012.
- CACE - Computer Aided Cryptography Engineering (EU-project, FP7); drie jaar, aanvang 1-1-2008.
- SecureSCM –Secure Supply Chain Management (EU-project, FP7); drie jaar, aanvang 1-2-2008.
- ECRYPT II - Network of Excellence in Cryptography (EU-project, FP7); vier jaar, aanvang in de zomer van 2008.
- Pearl – Privacy Enhanced security Architecture for RFID labels (STW/Sentinels project), 2007-2010.
- S-Mobile - Security of Software and Services for Mobile Systems (STW/Sentinels project), 2007-2011.
- PINPASJC - Program Inferred Power Analysis in Software -- JavaCard (STW/Sentinels project), 2005-2008.

- SEDAN - SEarchable DAta eNcryption (STW/Sentinels project), 2007 -2011.
- PASC - Practical Aspects of Secure Computation, (STW/Sentinels project), 2006 – 2009
- PRIAM – Privacy Issues and Ambient intelligence (INRIA), 2007-2008.
- POSEIDON - System Evolvability and Reliability of Systems of Systems (ESI/Thales), 2007-2011.
- CREST – Collusion Resistant Tracing (STW/Sentinels project), 2009 -2013
- Identity Management for Mobile Devices, 2009-2013.
- "Toegepaste Cryptografie" - langdurig lopende WBSO subsidie.
- Philips NatLab adviseurschap (Schoenmakers)
- DIAMANT (Cryptologie hoogleraar), 2006-2011.
- CEDICT (Embedded System Security hoogleraar) 2007-2012.
- ASCA (Kenniswerkersregeling) 2009-2010.

Nieuwe projectaanvragen (zie voor samenvatting Bijlage 2)

Onderwijs

De groepsleden verzorgen het volgende security-gerelateerd onderwijs.
- 2IC95 Seminar security
- 2IC99 Capita selecta security
- 2IF02/2IS35 Verification of security protocols
- 2IF03/2IC95 Seminar Information Security Technology
- 2IF11/2IS25 Distributed trust management
- 2IM23 Minor project
- 2IS05 Security
- 2WC09 Coding & Crypto 1
- 2WC10 Cryptographic Protocols
- 2WC11 Coding & Crypto 2
- 2WC12 Cryptography 1
- 2WC13 Cryptography 2
- 2WC14 Linux kernel and hacker's hut
- 2WC16 Linux kernel and OS security

Additioneel beschikbaar via het Kerckhoffs Institute zijn:
- 2IF02 Verification of security protocols
- 2IF03 Seminar Information Security Technology
- 2IF05 Introduction to computer security (UT)
- 2IF06 Software security (RU)
- 2IF07 Security in organizations (UT)
- 2IF08 Network security (UT)
- 2IF09 Biometric Recognition
- 2IF11 Distributed Trust Management

- 2IF12 Law in Cyberspace
- 2IF14 Hardware and operating system security (RU)
- 2IF15 Secure Data Management
- 2IF16 Security of Information Services

Mastermath
- Cryptology course, with other lecturers from CWI.
- Coding theory
- Number Theory and Cryptology

We zullen voorstellen doen om Security, i.h.b. cryptologie, beter zichtbaar te doen zijn in de bachelors fase van wiskunde en in de master fase van informatica.

Scientific output 2009
Zie Bijlage 3

Personele samenstelling van EiPSI

Coding & Crypto

Vaste staf
Brouwer, Andries
Lange, Tanja
Pellikaan, Ruud
Schoenmakers, Berry
Tilborg, Henk van
Weger, Benne de

Gast
Bernstein, Daniel

Postdoc
Ignatenko, Tanya (deeltijd met Elektro)
Toft, Tomas (tot 1 oktober)

Ph.D. students
Birkner, Peter (tot 1 oktober)
Bisson, Gaetan
Hoogh, Sebastiaan
Liesdonk, Peter van
Naehrig, Michael
Peters, Christiane
Relinde Jurrius
Schwabe, Peter
Villegas Bautista, José

Ondersteunend
Klooster, Anita (secretaresse CC en Ei/Ψ)
Kortsmit, Wil (IT specialist)

Security

Vaste staf

Etalle, Sandro
Hartog, Jerry den
Škorić, Boris

Deeltijd

Petkovic, Milan

Postdoc

Chatzikokolakis, Kostas
Lu, Jiqiang
Spiessens, Fred (tot 1 december)
Zannone, Nicola

Ph.D. student

Boesten, Dion (vanaf 1 december)
Bruso, Mayla (vanaf 15 februari)
Pan, Jing
Pontes Soares Rocha, Bruno
Simone, Antonino (vanaf 15 februari)
Trivellato, Daniel

Ondersteunend

Kortsmit, Wil (IT specialist)
Matthijsse-van Geenen, Jolande (secretaresse SEC)

Media

15 januari 2009	artikel in "Cursor", Benne de Weger *Team met TU/e'er legt zwakke plek in internetbeveiliging bloot*
9 februari 2009	artikel in "Newsweek", Benne de Weger *Attack of the Vigilante Cryptos*
21 maart 2009	artikel in "Volkskrant", TU Eindhoven *Kinderporno laat verdachte vingerafdrukken achter*
14 mei 2009	radio-interview met Sandro Etalle bij "Omroep Brabant"
24 september 2009	interview in Cursor 3 Boris Skoric, rubriek Vox Academici *"Bij beveiligingskwesties kun je niet paranoïde genoeg zijn"*

Start digitale colleges
http://web.tue.nl/cursor/internet/jaargang52/cursor03/nieuws/index.php?page=n5
Artikeltje of verzekering - backup service...
http://web.tue.nl/cursor/internet/jaargang52/cursor01/opinie/opinie.php?page=op4

Dissertations

- P. Birkner, *Efficient Arithmetic on Low-Genus Curves*, TU/e, 16 februari.
- M. Naehrig, *Constructive and Computational Aspects of Cryptographic Pairings*, TU/e, 7 mei.

Gasten

Daniel Bernstein	bijna continu
Christine Swart	17-25 januari

Gerhard Frey	16 februari
Steven Galbraith	16-17 februari
Yvo Desmedt	26 maart – 10 april
Chen-Mou Cheng	22-24 april
Bo-Yin Yang	22-24 april
David Naccache	23-26 april
Andy Clark	23-25 april
M. Scott	7-8 mei
Seda Guerses	22-23 april
Gabor Tardos	5-7 oktober

OVERIG

11 mei

Anita Borg Scholarship voor Christiane Peters

juni

Toekenning "CRYPTO 2009 best-paper award" voor het artikel *Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate* van Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik en . Benne de Weger

Bijlage 1 Nieuwe projectaanvragen in 2009

Seflex	**????**
Stamina	**niet geaccepteerd**
TrustSTS	**niet geaccepteerd**

Bijlage 2 Pers

Press release October 24, 2008
Cryptographers crack 30-year-old code

Press release: December 30, 2008
Experts uncover weakness in Internet security

Bijlage 3 Wetenschappelijke output

Journal article

Bulygin, S. & Pellikaan, G.R. (2009). Bounded distance decoding of linear error-correcting codes with Gröbner bases. *Journal of Symbolic Computation, 44*(12), 1626-1643.

Compagna, L., El Khoury, P., Krausová, A., Massacci, F., Zannone, N. (2009). How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. *Artificial Intelligence and Law*, *17*(1), 1-30.

Desmedt, Y., Duif, N., Tilborg, H.C.A. van & Wang, H. (2009). Bounds and constructions for key distribution schemes. *Advances in Mathematics of Communications, 3*(3), 273-293.

Etalle, S. & Winsborough, W.H. (2009). Maintaining control while delegating trust: Integrity constraints in trust management. *ACM Transactions on Information and System Security, 13*(1), 5-1/27.

Guajardo, J., Skoric, B., Tuyls, P.T., Kumar, S.S., Bel, T., Blom, A.H.M. & Schrijen, G.J. (2009). Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions. *Information Systems Frontiers, 11*(1), 19-41.

Guarda, P., Zannone, N. (2009). Towards the development of privacy-aware systems. *Information and Software Technology*, *51*(2), 337-350.

Lu, J. (2009). Related-key rectangle attack on 36 rounds of the XTEA block cipher. *International Journal of Information Security*, *8*(1), 1-11.

Lu, J., Ren, K., Chen, X. & Kim, K. (2009). The ring authenticated encryption scheme: How to provide a clue wisely. *Information Sciences, 179*(1-2), 161-168.

Petkovic, M., Jonker, W. (2009). Preface (Special issue on Secure data management). *Journal of Computer Security*, *17*(1), 1-3.

Schouten, B. & Jacobs, B.P.F. (2009). Biometrics and their use in e-passports. *Image and Vision Computing, 27*(3), 305-312.

Zannone, N. (2009). The SI* Modeling Framework: metamodel and applications. *International Journal of Software Engineering and Knowledge Engineering, 19*(5), 727-746.

Book - Monograph

Zannone, N. (2009). *Security Agent-Oriented Requirements Engineering: the SI**

Modeling Language and the Secure Tropos Methodology. Saarbrücken: VDM Verlag.

Book chapter

Benschop, N.F., Kleihorst, Richard, Vleuten, R.J. van der, Muurling, G. & Simonis, J. (2009). Fault Tolerant Logic by Error Correcting Codes. In N.F. Benschop (Ed.), *Associative Digital Network Theory - An Associative Algebra Approach to Logic, Arithmetic and State Machines* (pp. 83-96). Springer-Verlag.

Bulygin, S. & Pellikaan, G.R. (2009). Decoding linear error-correcting codes up to half the minimum distance with Gröbner bases. In M. Sala, T. Mora, L. Perret, S. Sakata & C. Traverso (Eds.), *Gröbner Bases, Coding, and Cryptography* (Texts and Monographs in Symbolic Computation) (pp. 361-365). Berlin: Springer.

Schoenmakers, B. (2009). Voting schemes (Chapter 15). In M.J. Atallah & M. Blanton (Eds.), *Algorithms and Theory of Computation Handbook (2nd ed, volume 2: Special topics and techniques)* (pp. 15/1-21). Boca Raton FL: CRC Press.

Tilborg, H.C.A. van (2009). Authentication codes from error-correcting codes; an overview. In B. Preneel, S. Dodunekov, V. Rijmen & S. Nikova (Eds.), *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes* (NATO Science for Peace and Security Series - D: Information and Communication Security, 23) (pp. 3-16). Amsterdam: IOS Press.

Conference proceeding

Bailey, D.V., Baldwin, B., Batina, L., Bernstein, D.J., Birkner, P., Bos, J.W., Damme, G. van, De Meulenaer, G., Fan, J., Güneysu, T., Gurkaynak, F., Kleinjung, T., Lange, T., Mentens, N., Paar, C., Regazzoni, F., Schwabe, P. & Uhsadel, L. (2009). The Certicom challenges ECC2-X. In *SHARCS'09 Workshop Record (Proceedings 4th Workshop on Special-purpose Hardware for Attacking Cryptograhic Systems, Lausanne, Switserland, September 9-10, 2009)* (pp. 51-82).

Bernstein, D.J., Chen, T.R., Cheng, C.M., Lange, T. & Yang, B.Y. (2009). ECM on graphics cards. In A. Joux (Ed.), *Advances in Cryptology - Eurocrypt 2009 (28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings) Vol. 5479. Lecture Notes in Computer Science* (pp. 483-501). Berlin: Springer.

Bernstein, D.J., Lange, T., Peters, C.P. & Tilborg, H.C.A. van (2009). Explicit bounds for generic decoding algorithms for code-based cryptography. In *International Workshop on Coding and Cryptography (WCC 2009, Ullensvang, Norway, May 10-15, 2009. Pre-proceedings)* (pp. 168-180). Bergen: Selmer Center, University of Bergen.

Bernstein, D.J., Lange, T., Niederhagen, R.F., Peters, C.P. & Schwabe, P. (2009). FSBday : Implementing Wagner's generalized birthday attack against the SHA-3 round-1

candidate FSB. In B. Roy & N. Sendrier (Eds.), *Progress in Cryptology - INDOCRYPT 2009 (Proceedings 10th International Conference on Cryptology in India, New Dehli, India, December 13-16, 2009) Vol. 5922. Lecture Notes in Computer Science* (pp. 18-38). Berlin: Springer.

Bernstein, D.J., Lange, T., Niederhagen, R.F., Peters, C.P. & Schwabe, P. (2009). FSBday : Implementing Wagner's generalized birthday attack against the SHA-3 round-1 candidate FSB. In *SHARCS'09 Workshop Record (Proceedings 4th Workshop on Special-purpose Hardware for Attacking Cryptograhic Systems, Lausanne, Switserland, September 9-10, 2009)* (pp. 85-104).

Bernstein, D.J., Chen, H.C., Chen, M.S., Cheng, C.M., Hsiao, C.H., Lange, T., Lin, Z.C. & Yang, B.Y. (2009). The billion-mulmod-per-second PC. In *SHARCS'09 Workshop Record (Proceedings 4th Workshop on Special-purpose Hardware for Attacking Cryptograhic Systems, Lausanne, Switserland, September 9-10, 2009)* (pp. 131-144).

Birkner, P. & Thériault, N. (2009). Faster halvings in genus 2. In R. Avanzi, L. Keliher & F. Sica (Eds.), *Selected Areas in Cryptography (15th Annual Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, 2008, Revised Selected Papers) Vol. 5381. Lecture Notes in Computer Science* (pp. 1-17). Berlin: Springer.

Bogetoft, P., Christensen, D.L., Damgard, Ivan, Geisler, M., Jakobsen, T., Kroigaard, M., Nielsen, J.D., Nielsen, J.B., Nielsen, K., Pagter, J., Schwartzbach, M. & Toft, T. (2009). Secure multiparty computation goes live. In R. Dingledine & Ph. Golle (Eds.), *Financial Cryptography and Data Security (13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers) Vol. 5628. Lecture Notes in Computer Science* (pp. 325-343). Berlin: Springer.

Bolzoni, D., Etalle, S. & Hartel, P.H. (2009). Panacea: Automating attack classification for anomaly-based network intrusion detection systems. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Recent Advances in Intrusion Detection (12th International Symposium, RAID 2009, Saint-Malo, France, September 23-25, 2009. Proceedings) Vol. 5758. Lecture Notes in Computer Science* (pp. 1-20). Berlin: Springer.

Braun, C., Chatzikokolakis, K. & Palamidessi, C. (2009). Quantitative notions of leakage for one-try attacks. In S. Abramsky, M. Mislove & C. Palamidessi (Eds.), *Proceedings of the 25th Conference on Mathematical Foundations of Programming Semantics (MFPS 2009, Oxford, UK, April 3-7, 2009) Vol. 249. Electronic Notes in Theoretical Computer Science* (pp. 75-91).

Busnel, P., El Khoury, P., Li, K., Saidane, A., Zannone, N. (2009). S&D pattern deployment at organizational level: A prototype for remote healthcare system. In T. Dimitrakos, F. Martinelli (Eds.), *Proceedings of the 4th International Workshop on Security and Trust Management (STM'08, Trondheim, Norway, June 16-17, 2008). (Electronic Notes in Theoretical Computer Science, Vol. 244, pp. 27-30).*

Chatzikokolakis, K., Norman, G. & Parker, D. (2009). Bisimulation for demonic schedulers. In L. de Alfaro (Ed.), *Foundations of Software Science and Computational Structures (12th International Conference, FoSSaCS 2009, York, UK, March 22-29, 2009, Proceedings) Vol. 5504. Lecture Notes in Computer Science* (pp. 318-332). Berlin: Springer.

Chatzikokolakis, K., Knight, S. & Panangaden, P. (2009). Epistemic strategies and games on concurrent processes. In M. Nielsen, A. Kucera, P.B. Miltersen, C. Palamidessi, P. Tuma & F. Valencia (Eds.), *SOFSEM 2009 : Theory and Practice of Computer Science (35th Conference, Spindleruv Mlyn, Czech Republic, January 24-30, 2009, Proceedings) Vol. 5404. Lecture Notes in Computer Science* (pp. 153-166). Berlin: Springer.

Cortesi, A. & Brusò, M. (2009). Non-repudiation analysis with LYSA. In D. Gritzalis & J. Lopez (Eds.), *Proceedings of the IFIP 24th International Information Security Conference (IFIP SEC'09, Pafos, Cyprus, Greece, May 18-20, 2009) Vol. 297. IFIP Conference Proceedings* (pp. 318-329). Boston: Springer.

Costigan, N. & Schwabe, P. (2009). Fast elliptic-curve cryptography on the Cell Broadband Engine. In B. Preneel (Ed.), *Progress in Cryptology - AfricaCrypt 2009 (Second International Conference on Cryptology in Africa, Gammarth, Tunisia, June 21-25, 2009, Proceedings) Vol. 5580. Lecture Notes in Computer Science* (pp. 368-385). Berlin: Springer.

Czenko, M.R. and Etalle, S. (2009) *LP with Flexible Grouping and Aggregates Using Modes.* In: Preliminary Proceedings of the 19th International Symposium on Logic-Based Program Synthesis and Transformation LOPSTR 2009., 9-11 Sep 2009, Coimbra, Portugal. pp. 59-73. LOPSTR (TR 2009/04). University of Coimbra. ISSN 0874-338X

Elahi, G., Yu, E. & Zannone, N. (2009). A modeling ontology for integrating vulnerabilities into security requirements conceptual foundations. In A.H.F. Laender, S. Castano, U. Dayal, F. Casati & J. Palazzo Moreira de Oliveira (Eds.), *Conceptual Modeling - ER 2009 (28th International Conference on Conceptual Modeling, Gramado, Brazil, November 9-12, 2009. Proceedings) Vol. 5829. Lecture Notes in Computer Science* (pp. 99-114). Berlin: Springer.

Hoogh, S.J.A. de, Schoenmakers, B., Skoric, B. & Villegas Bautista, J.A. (2009). Verifiable rotation of homomorphic encryptions. In S. Jarecki & G. Tsudik (Eds.), *Public Key Cryptography - PKC 2009 (12th International Conference on Practice and Theory in Public-Key Cryptography, Irvine CA, USA, March 18-20, 2009, Proceedings) Vol. 5443. Lecture Notes in Computer Science* (pp. 393-410). Berlin: Springer.

Ibraimi, L., Petkovic, M., Nikova, S.I., Hartel, P.H. & Jonker, W. (2009). Mediated ciphertext-policy attribute-based encryption and Its application. In H.Y. Youm & M. Yung (Eds.), *Information Security Applications (10th International Workshop, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers) Vol. 5932. Lecture*

Notes in Computer Science (pp. 309-323). Berlin: Springer.

Jonge, W. de & Jacobs, B.P.F. (2009). Privacy-friendly electronic traffic pricing via commits. In P. Degano, J. Guttman & F. Martinelli (Eds.), *Formal Aspects in Security and Trust (5th International Workshop, FAST 2008, Malaga, Spain, October 9-10, 2008. Revised Selected Papers) Vol. 5491. Lecture Notes in Computer Science* (pp. 143-161). Berlin: Springer.

Jurrius, R.P.M.J. & Pellikaan, G.R. (2009). Extended and generalized weight enumerators. In *International Workshop on Coding and Cryptography (WCC 2009, Ullensvang, Norway, May 10-15, 2009. Proceedings)* (pp. 76-91). Bergen: Selmer Center, University of Bergen.

Jurrius, R.P.M.J. & Pellikaan, G.R. (2009). The extended coset leader weight enumerator. In T.J. Tjalkens & F.M.J. Willems (Eds.), *Proceedings 30th Symposium on Information Theory on the Benelux (Eindhoven, The Netherlands, May 28-29, 2009)* (pp. 217-224). Eindhoven: Technische Universiteit Eindhoven.

Kammler, D., Zhang, D., Schwabe, P., Scharwaechter, H., Langenberg, M., Auras, D., Ascheid, G. & Mathar, R. (2009). Designing an ASIP for cryptographic pairings over Barreto-Naehrig curves. In C. Clavier & K. Gaj (Eds.), *Cryptographic Hardware and Embedded Systems - CHES 2009 (11th International Workshop Lausanne, Switzerland, September 6-9, 2009. Proceedings) Vol. 5747. Lecture Notes in Computer Science* (pp. 254-271). Berlin: Springer.

Käsper, E. & Schwabe, P. (2009). Faster and timing-attack resistant AES-GCM. In C. Clavier & K. Gaj (Eds.), *Cryptographic Hardware and Embedded Systems - CHES 2009 (11th International Workshop Lausanne, Switzerland, September 6-9, 2009. Proceedings) Vol. 5747. Lecture Notes in Computer Science* (pp. 1-17). Berlin: Springer.

Kerschbaum, F., Biswas, D. & Hoogh, S.J.A. de (2009). Performance comparison of secure comparison protocols. In *Database and Expert Systems Applications (Proceedings 20th International Workshop, DEXA'09, Linz, Austria, August 31-September 4, 2009)* (pp. 133-136). IEEE Computer Society.

Künzi, J., Petkovic, M. & Koster, P. (2009). Data-centric protection in DICOM. In K.M. Siddiqui & B.J. Liu (Eds.), *Medical Imaging 2009: Advanced PACS-based Imaging Informatics and Therapeutic Applications (Lake Buena Vista FL, USA, February 11-12, 2009) Vol. 7264. Proceedings of SPIE* (pp. 726419-1/11). SPIE.

Künzi, J., Koster, P. & Petkovic, M. (2009). Emergency access to protected health records. In K.P. Adlassnig, B. Blobel, J. Mantas & I. Masic (Eds.), *Medical Informatics in a United and Healthy Europe (Proceedings of MIE 2009, The XXIInd International Congress of the European Federation for Medical Informatics, Sarajevo, Bosnia and Herzegovina, August 30-September 2, 2009) Vol. 150. Studies in Health Technology and Informatics* (pp. 705-709). IOS Press.

Kursawe, K., Sadeghi, A.R., Schellekens, D., Skoric, B. & Tuyls, P.T. (2009). Reconfigurable Physical Unclonable Functions : enabling technology for tamper-resistant storage. In *Proceedings IEEE International Conference on Hardware-Oriented Security and Trust (HOST'09, San Francisco CA, USA, July 27, 2009)* (pp. 22-29). IEEE.

López, H.A., Massacci, F., Zannone, N. (2009). Goal-equivalent secure business process re-engineering. In E. Di Nitto, M. Ripeanu (Eds.), *Service-Oriented Computing - ICSOC 2007 Workshops (International Workshops, Vienna, Austria, September 17, 2007, Revised Selected Papers). (Lecture Notes in Computer Science, Vol. 4907, pp. 212-223).* Berlin: Springer.

Morali, A., Zambon, E., Houmb, S.H., Sallhammar, K. & Etalle, S. (2009). Extended eTVRA vs. security checklist: Experiences in a value-web. In *Proceedings 31st International Conference on Software Engineering (ICSE'09, Vancouver, Canada, May 16-24, 2009)* (pp. 130-140). IEEE Computer Society Press.

Pan, J., Hartog, J.I. den & Lu, J. (2009). You cannot hide behind the mask: Power analysis on a provably secure S-box implementation. In H.Y. Youm & M. Yung (Eds.), *Information Security Applications (10th International Workshop, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers) Vol. 5932. Lecture Notes in Computer Science* (pp. 178-192). Berlin: Springer.

Petkovic, M. (2009). Remote patient monitoring: Information reliability challenges. In *Telecommunication in Modern Satellite, Cable, and Broadcasting Services (Proceedings 9th International Conference, TELSIKS'09, Nis, Serbia, October 7-9, 2009)* (pp. 295-301). IEEE.

Skoric, B. & Tuyls, P.T. (2009). An efficient fuzzy extractor for limited noise. In T.J. Tjalkens & F.M.J. Willems (Eds.), *Proceedings 30th Symposium on Information Theory on the Benelux (Eindhoven, The Netherlands, May 28-29, 2009)* (pp. 193-200). Eindhoven: Technische Universiteit Eindhoven.

Skoric, B., Katzenbeisser, S., Schaathun, H.G. & Celik, M.U. (2009). Tardos fingerprinting codes in the combined digit model. In *Proceedinfs First IEEE Workshop on Information Forensics and Security (WIFS'09, London, UK, December 6-9, 2009)* (pp. 41-45). IEEE.

Spiessens,F.., Hartog, J.I. den & Etalle, S. (2009). Know what you trust: Analyzing and designing trust policies with Scoll. In P. Degano, J. Guttman & F. Martinelli (Eds.), *Formal Aspects in Security and Trust (5th International Workshop, FAST 2008, Malaga, Spain, October 9-10, 2008. Revised Selected Papers) Vol. 5491. Lecture Notes in Computer Science* (pp. 129-142). Berlin: Springer.

Stevens, M., Sotirov, A., Appelbaum, J., Lenstra, A.K., Molnar, D., Osvik, D.A. & Weger, B.M.M. de (2009). Short chosen-prefix collisions for MD5 and the creation of a

rogue CA certificate. In S. Halevi (Ed.), *Advances in Cryptology - CRYPTO 2009 (29th Annual International Cryptology Conference, Santa Barbara CA, USA, August 16-20, 2009. Proceedings) Vol. 5677. Lecture Notes in Computer Science* (pp. 55-69). Berlin: Springer.

Toft, T. (2009). Constant-rounds, almost-linear bit-decomposition of secret shared values. In *Topics in Cryptology – CT-RSA 2009 (The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings) Vol. 5473. Lecture Notes in Computer Science* (pp. 357-371). Berlin: Springer.

Toft, T. (2009). Solving linear programs using multiparty computation. In *Financial Cryptography and Data Security (FC'09) Vol. 5628. Lecture Notes in Computer Science* (pp. 90-107). Berlin: Springer.

Trivellato, D., Spiessens, A.O.D., Zannone, N. & Etalle, S. (2009). POLIPO : Policies & ontologies for interoperability, portability, and autonomy. In *Proceedings IEEE International Symposium on Policies for Distributed Systems and Networks (London, UK, July 20-22, 2009)* (pp. 110-113). IEEE.

Trivellato, D., Spiessens, A.O.D., Zannone, N. & Etalle, S. (2009). Reputation-based ontology alignment for autonomy and interoperability in distributed access control. In *Proceedings 12th IEEE International Conference on Computational Science and Engineering (CSE'09, Vancouver BC, Canada, August 29-31, 2009), Volume 3* (pp. 252-258). IEEE.

Edited book

Massacci, F., Redwine, S.T. & Zannone, N. (Eds.). (2009). *Engineering Secure Software Systems (First International Symposium, ESSoS 2009, Leuven, Belgium, February 4-6, 2009, Proceedings)* (Lecture Notes in Computer Science, 5429). Berlin: Springer.

Schoenmakers, B. & Ryan, P.Y.A. (Eds.). (2009). *E-voting and identity (Second International Conference, VOTE-ID 2009, Luxembourg, September 7-8, 2009. Proceedings)* (Lecture Notes in Computer Science, 5767). Berlin: Springer.

External report

Arène, C., Lange, T., Naehrig, M. & Ritzenthaler, C. (2009). *Faster computation of Tate pairings.* Cryptology ePrint Archive (Ext. rep. 2009/155). -: IACR.

Bailey, D.V., Batina, L., Bernstein, D.J., Birkner, P., Bos, J.W., Chen, H.C., Cheng, C.M., Damme, G. van, De Meulenaer, G., Dominguez Perez, L.J., Fan, J., Güneysu, T., Gurkaynak, F., Lange, T., Mentens, N., Niederhagen, R.F., Paar, C., Regazzoni, F., Schwabe, P., Uhsadel, L., Van Herrewege, A. & Yang, B.Y. (2009). *Breaking ECC2K-130.* Cryptology ePrint Archive (Ext. rep. 2009/541). -: -.

Bailey, D.V., Baldwin, B., Batina, L., Bernstein, D.J., Birkner, P., Bos, J.W., Damme, G. van, De Meulenaer, G., Fan, J., Güneysu, T., Gurkaynak, F., Kleinjung, T., Lange, T., Mentens, N., Paar, C., Regazzoni, F., Schwabe, P. & Uhsadel, L. (2009). *The Certicom Challenges ECC2-X.* Cryptology ePrint Archive (Ext. rep. 2009/466). -: -.

Bernstein, D.J. & Lange, T. (2009). *A complete set of addition laws for incomplete Edwards curves.* Cryptology ePrint Archive (Ext. rep. 2009/580). -: -.

Bernstein, D.J., Lange, T., Niederhagen, R.F., Peters, C.P. & Schwabe, P. (2009). *FSBday : Implementing Wagner's generalized birthday attack against the SHA-3 round-1 candidate FSB.* Cryptology ePrint Archive (Ext. rep. 2009/292). -: IACR.

Birkner, P. & Thériault, N. (2009). *Efficient halving for genus 3 curves over binary fields.* Cryptology ePrint Archive (Ext. rep. 2009/157). -: IACR.

Bisson, G. & Sutherland, A.V. (2009). *Computing the endomorphism ring of an ordinary elliptic curve over a finite field.* Cryptology ePrint Archive (Ext. rep. 2009/100).

Bolzoni, D., Etalle, S. & Hartel, P.H. (2009). *Panacea : Automating attack classification for anomaly-based network intrusion detection systems.* CTIT Technical Report (Ext. rep. TR-CTIT-09-10). Enschede: Universiteit Twente.

Costello, C., Lange, T. & Naehrig, M. (2009). *Faster pairing computations on curves with high-degree twists.* Cryptology ePrint Archive (Ext. rep. 2009/615). -: -.

Costigan, N. & Schwabe, P. (2009). *Fast elliptic-curve cryptography on the Cell Broadband Engine.* Cryptology ePrint Archive (Ext. rep. 2009/016). -: IACR.

Kammler, D., Zhang, D., Schwabe, P., Scharwaechter, H., Langenberg, M., Auras, D., Ascheid, G., Leupers, R., Mathar, R. & Meyr, H. (2009). *Designing an ASIP for cryptographic pairings over Barreto-Naehrig curves.* Cryptology ePrint Archive (Ext. rep. 2009/056). -: IACR.

Käsper, E. & Schwabe, P. (2009). *Faster and timing-attack resistant AES-GCM.* Cryptology ePrint Archive (Ext. rep. 2009/129). -: IACR.

Luca, F., Moree, P. & Weger, B.M.M. de (2009). *Some Diophantine equations from finite group theory: $\Phi_m (x) = 2p^n -1$.* arXiv.org (Ext. rep. 0907.5323). -: -.

Morali, A., Zambon, E., Etalle, S. & Wieringa, R.J. (2009). *CRAC : confidentiality risk analysis and IT-architecture comparison of business networks.* CTIT Technical Report (Ext. rep. TR-CTIT-09-30). Enschede: Universiteit Twente.

Peters, C.P. (2009). *Information-set decoding for linear codes over Fq.* Cryptology ePrint Archive (Ext. rep. 2009/589). -: IACR.

Skoric, B. & Tuyls, P.T. (2009). *An efficient fuzzy extractor for limited noise.* Cryptology ePrint Archive (Ext. rep. 2009/030). -: IACR.

Skoric, B. & Makkes, M.X. (2009). *Flowchart description of security primitives for Controlled Physical Unclonable Functions.* Cryptology ePrint Archive (Ext. rep. 2009/328). -: IACR.

Skoric, B. (2009). *Quantum readout of Physical Unclonable Functions: Remote authentication without trusted readers and authenticated Quantum Key Exchange without initial shared secrets.* Cryptology ePrint Archive (Ext. rep. 2009/369). -: IACR.

Skoric, B., Katzenbeisser, S., Schaathun, H.G. & Celik, M.U. (2009). *Tardos fingerprinting codes in the combined digit model.* Cryptology ePrint Archive (Ext. rep. 2009/244). -: IACR.

Stevens, M., Sotirov, A., Appelbaum, J., Lenstra, A.K., Molnar, D., Osvik, D.A. & Weger, B.M.M. de (2009). *Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate.* Cryptology ePrint Archive (Ext. rep. 2009/111). -: -.

Trivellato, D., Spiessens, A.O.D., Zannone, N. & Etalle, S. (2009). *POLIPO: Policies & ontologies for interoperability, portability, and autonomy.* Computer Science Report (Ext. rep. 09-06). Eindhoven: Technische Universiteit Eindhoven.

Verbitskiy, E.A., Tuyls, P.T., Obi, C., Schoenmakers, B. & Skoric, B. (2009). *Key extraction from general non-discrete signals.* Cryptology ePrint Archive (Ext. rep. 2009/303). -: IACR.

Zambon, E., Etalle, S., Wieringa, R.J. & Hartel, P.H. (2009). *Architecture-based qualitative risk analysis for availability of IT infrastructures.* CTIT Technical Report (Ext. rep. TR-CTIT-09-35). Enschede: Universiteit Twente.

Dissertation

Birkner, P. (2009, February 16). *Efficient arithmetic on low-genus curves.* Technische Universiteit Eindhoven (iv,140 pag.) (Eindhoven: Technische Universiteit Eindhoven). Prom./coprom.: prof.dr. T. Lange & prof. D.J. Bernstein.

Naehrig, M. (2009, May 7). *Constructive and computational aspects of cryptographic pairings.* Technische Universiteit Eindhoven (x,141 pag.) (Eindhoven: Technische Universiteit Eindhoven). Prom./coprom.: prof.dr. T. Lange.