Annual- and research report 2010

This is the third full year of activity of EIPSI. The cooperation between the Coding and Crypto group and the Security Group is now made even more concrete by the presence of three externally funded PhD students that are co-supervised by members of both groups. Members of EIPSI are regularly in the news, and the visibility of EIPSI at national level is still increasing.

The highlight of the year has been the SuperTU/esday that was organized at record speed, and which attracted more than 400 people to Eindhoven; our thanks for putting together a such a superbly organized event goes to Henk van Tilborg, and to the whole organizing committee.

Scientific activities 2010

EiPSI Seminar

February 3, 2010	Tanya Ignatenko, *Fuzzy Commitment for Biometrics: Information Leakage and Coding.*
March 3, 2010	Jufeng Fan, *Efficient and secure (H)ECC co-processor design: challenge and response.*
April 14, 2010	Bruno Pontes Soares Rocha, *Towards Static Flow-based Declassificaton for Legacy and Untrusted Programs.*
May 26, 2010	Elisa Costante, *Trust and Web Services: Reputation and Evidence for the Service Selection.*
September 9, 2010	Meilof Veeningen, *Modeling identity-related properties and their privacy strength.*
October 13, 2010	Berry Schoenmakers, *Anonymous Credential Schemes with Encrypted Attributes.*
November 3, 2010	Christian Schaffner, *Position-based Quantum Cryptography: Impossibility And Constructions.*
November 24, 2010	Mohammad Mousavi, *Reconciling Operational and Epistemic Approaches to the Analysis of Security Protocols.*

TU/e-Philips Colloquium

April 12, 2010	Mikkel Krøigard, *On the Overhead of Secure Multiparty Computation.*
June 23, 2010	Muhammad Asim, *Attribute based encryption: Updating privacy policy and sharing among multiple domains.*

Cryptography Working Group

April 23, 2010	Ronny Wichers Schreur, *Dismantling SecureMemory, CryptoMemory and CryptoRF*.
	Peter van Liesdonk, *Hidden vector encryption and its application to searchable Encryption.*
	Wouter Slegers, *Real world hacks of certified-secure cryptographic products.*
	Jan Peter van Zandwijk, *Cryptanalysis of the DECT standard Cipher (paper by Karsten Nohl et al from FSE 2010).*
October 1, 2010	Christiane Peters, *Wild McEliece.*
	Cees Jansen, *Times were when.*
	Svetla Nikova, *Side-channel attack resisting hardware implementations of the AES.*
	Jurjen Bos, *Decimal encryption.*
December 3, 2010	Peter Roelse, *A cryptographic mechanism for pay –TV receivers.*
	Jaap-Henk Hoepman, *Towards Revocable Privacy: The case of the Canvas Cutters.*
	Antonino Simone, *Accusation probabilities in Tardos codes.*
	Len Sassaman, *Minimizing Attack Surfaces with Language-Theoretic Security.*

SuperTU/esday

February 8-12, 2010	Exhibition from Scryption about cryptologie.
February 11, 2010	NBV exhibition
February 11, 2010	Cryptowerkplaats, Tanja Lange and Cristiane Peters.
February 11, 2010	Company exhibitions (Com-connect, Compumatica, LaQuSo / NIRICT, Madison Gurkha, Siemens Nederland N.V., Philips, Securitymatters, ORIBI Software, Irdeto, Fox-IT).
February 11, 2010	Andy Clark, *Forensics, Security and the Wisdom of Users.*
	Boris Škorić, *Masterclass Security.*
	Berry Schoenmakers, *Crypto 2.0. Achieving security and privacy at the same time.*
	Stan Hegt, *Phishing and the (in)security of Internet banking.*
	Jan de Boer, *Herstel van de zwaktste schakel; List en bedrog in de Informatiebeveiliging.*
	Wilfred van Roij, *Hebt u als ondernemer ook een digitaal slot met ketting op uw bedrijf?*
	Henk van Tilborg, *Het kraken van een oude code. Hoe kun je een geheim afspreken als je afgeluisterd wordt?*
	Sandro Etalle, *From Network Intrusion Detection to the protection of the Critical Infrastructure: semirandomthoughts on security.*

Marc Witteman, *Side channel attacks on a smart card*
Nicole van der Meulen / Arnold Roosendaal, *Identiteitsfraude en digitale Kwetsbaarheid.*
Paul Overbeek, *Hoe besteel je de MKB-er via het Internet?*
Charles den Tex,*Your Identity is on (the) line.*

Workshops

- FAST 2010, 7th International Workshop on Formal Aspects of Security and Trust. Pisa, Italy, September 16-17, 2010.
- Dagstuhl Seminar 10141 on Distributed Usage Control. Dagstuhl, Deutschland, April 6-9, 2010.
- PASC Seminar Practical Approaches to Secure Computation, April 29, TU Eindhoven.

Staff activities 2010

- Selection of PhD student Elisa Costante for project TAS3.
- Selection Postdoc, Mikkel Krøigard for project CASE.
- Selection of PhD student Ruben Niederhagen
- Departure of Jiqiang Lu, Xiaoping Liang, José Villegas Bautista and Anita Klooster.

Press 2010

See attachment 1

Involvement in the organization of symposium, conferences, and alike

Gaetan Bisson

PC Member of:

- Program Committee Member of MAJECSTIC 2010, Université de Bordeaux, France, October 13-15, 2010.

Kostas Chatzikokolakis

PC Member of:

- Program Committee Member of the 8th International Workshop on Security Issues in Concurrency, SecCo 2010, Paris France, August 30, 2010.
- Program Committee Member of FCS-PrivMod 2010, Edinburgh, UK, July 14-15, 2010.
- Program Committee Member of the 8th Workshop on Quantitative Aspects of Programming Languages (QAPL 2010), Paphos, Cyprus, March 27-28, 2010.

Sandro Etalle

Program Chair of:

- Program Chair together with Joshua Guttman and Pierpaolo Degano of the FAST 2010, 7th International Workshop on Formal Aspects of Security and Trust. Pisa, Italy, September 16-17, 2010.

PC Member of

- Program Committee Member of W3C Workshop on Privacy and data usage control, Cambridge (MA), October 4-5, 2010.
- Program Committee Member of the Fourth IFIP International Conference on Trust Management, Morioka, Iwate, Japan, June 16-18, 2010.
- Program Committee Member of the Workshop on Security and Privacy in Cloud Computing Brussels, Belgium, January 29, 2010.

Member of steering committees:

- Member of the steering committee of FOSAD International School on Foundations of Security Analysis and Design, September 6-11, 2010.

Co-organizer of:

- Co-organizer of Dagstuhl Seminar 10141 on Distributed Usage Control, Dagstuhl, Deutschland, April 6-9, 2010.

Invited Speaker

- Invited speaker at the SYMPOSIUM AUS ANLASS DER ERÖFFNUNG DES CENTER FOR SECURITY AND SOCIETY. Freiburg 8-9 July 2010.

External member of PhD committees:

- Srijith Nair,Remote Policy Enforcement Using Java Virtual Machine, January 9, 2010, Vrije Universiteit Amsterdam.
- Giorgios Portokalidis, Using Virtualisation to Protect Against Zero-Day Attacks, February 25, 2010, Vrije Universiteit Amsterdam.
- Anna Sperotto, Flow-based intrusion detection, October 14, 2010, Universiteit Twente.
- Haiyun xu, Spectral Minutiae Representations for Fingerprint Recognition, October 22, 2010, Universiteit Twente.

Jerry den Hartog

PC Member of:

- Program Committee Member of the 8th International Workshop on Security Issues in Concurrency SecCo2010, Paris, France, August 30, 2010.

Co-chair of:

- Co-chair of the International Workshop on Policies for the Future Internet (POFI 2010), Pisa, Italy, February 5, 2010.

Tanya Ignatenko

Organizer of:

- Organizer of the special session on "Privacy and Security in Biometrics" at the IEEE Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IHH-MSP), Darmstadt, Germany, October 15-17, 2010.
- Organizer and moderator of panel "Future Tends in Template Protection" at the IEEE Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IHH-MSP), Darmstadt, Germany, October 15-17, 2010.

Invited Lecture of:

- Invited talk at IS&T/SPIE Electronic Imaging: Media Forensics and Security XII, "On Information Leakage in Fuzzy Commitment", San Jose, CA, USA, January 17-21, 2010.

Colloquium/Seminar lecture of:

- Lecture on "Biometric Secrecy Systems: Authentication vs. Identificaction" at Information Theory Colloquium on Cognitieve Radio, Interference, and Biometric Systems, April 15, 2010.

Tanja Lange

Co-program chair of:

- Co-program chair (with D.J. Bernstein) of Africacrypt 2010, Stellenbosch, South Africa, May 3-6, 2010.

Co-organizer of:

- Co-organizer of the Computer Security and Cryptography, (as part of the special semester on Number Theory as Experimental and Applied Science) at CRM Montreal, Canada, April 12-16, 2010.
- Co-organizer of the Workshop on Elliptic Curves and Computation, Redmond, WA, USA, October 18-22, 2010.

PC member of:

- Program Committee Member of Indocrypt 2010, Hyderabad, India, December 12-15, 2010.
- Program Committee Member of CRYPTO 2010, Santa Barbara, California, USA, August 15-19, 2010.
- Program Committee Member of SAC 2010, Waterloo, Ontario, Canada, August 11-13, 2010.
- Program Committee Member of Latincrypt 2010, Puebla, Mexico, August 8-11, 2010.
- Program Committee Member of ECRYPT II, Egham, UK, June 22-23, 2010.
- Program Committee Member of WAIFI 2010, Istanbul, Turkey, June 27-30, 2010.
- Program Committee Member of PQCrypto 2010, Darmstadt. Germany, May 25-28, 2010.
- Program Committee Member of Africacrypt 2010, Stellenbosch, South Africa, May 3-6, 2010.

Member of steering committees:

- Member of Steering Committee Pairing conference, Yamanaka Hot Spring, Ishikawa, Japan, December 13-15, 2010.
- Member of Steering Committee (Chair) Workshop on Elliptic Curve Cryptography (ECC), Redmond, USA, October 18-22, 2010.
- Member of Steering Committee Post-Quantum Cryptography workshop, Darmstadt, Germany, May 25-28, 2010.

External member of PhD committees:

- Naomi Benger, *Cryptographic pairings: efficient algorithms and DLP security.* Dublin City University, Ireland, July 16, 2010.
- Sorina Ionica, *Pairing the volcano*, Universit\é de Versailles, France, January 18, 2010.
- Emanuele Cesena, *Trace Zero Varieties in Pairing-based Cryptography***,** Politecnico di Torino, Italy, 2010.

Invited Speaker:

- Invited speaker at the 5th Workshop on Embedded Systems Security (WESS'2010). Scottsdale, AZ, USA, October 24, 2010.
- Invited speaker at the Workshop on Elliptic Curves and Computation. Redmond, WA, USA, October 18-22, 2010.
- Invited speaker at The first Taiwanese Workshop on Security and System-on-Chip. Taipei, Taiwan, February 26, 2010.

Milan Petkovic

Organizer of:

- Organizer of the workshop "Consent Management and Privacy in Healthcare", with representatives of Royal Dutch Medical Association (KNMG), PrivaSense, Electronic Record Services, TU/e, Windsor University and Sheridan Institute of Technology, Eindhoven, Netherlands, November 15, 2010.

General chair of:

- General chair of Secure Data Management SDM 2010, Singapore, September 17, 2010.

PC member of:

- Program Committee Member of OTM Information Security 2010, Crete, Greece, October 26, 2010.
- Program Committee Member of SECRYPT'10, International Conference on Security and Cryptography, Athens, Greece, July 26-28, 2010.
- Program Committee Member of IFIP SEC'10, 25th International Information Security Conference, Brisbane, Australia, September 20-23, 2010.
- Program Committee Member of WASP'10, International Workshop on AAL Servoce Platform, Lyon, France, July 2, 2010.
- Program Committee Member of CCNC-DRM'10, 7th International CCNC Workshop on Digital Rights Management, Las Vegas, USA, January 9-12, 2010.

- Program Committee Member of 10th ACM Digital Rights Management Workshop, Chicago, USA, October 4, 2010.
- Program Committee Member of STC'10, EFMI Special Topic Conference, Reykjavik, Iceland, June 2-4, 2010

Invited Lectures of:
- Invited Lecture of Privacy and Security in the Internet of Things", IEEE Symposium on Connected World, May 17, 2010.
- Invited Lecture of Anticiper les risques émergents et futurs à partir du projet Being Diabetic in 2011, 2nd Risk Management in Healthcare Conference, Toulouse, June 2010.

External member of PhD committees:
- Zekerya Erkin, *Secure Signal Processing: Privacy Preserving Cryptographic Protocols for Multimedia*, Delft University of Technology, June 24, 2010.

Berry Schoenmakers

PC member of:
- Program Committee Member of IACR conferences: 29th Eurocrypt'10, French Riviera, May 30 until June 3, 2010.
- Program Committee Member of 10th CT-RSA 2010, San Francisco, CA, USA, March 1-5, 2010.
- Program Committee Member of 15th Australasian Conference on Information Security and Cryptology (ACISP 2010), Sydney, Australia, July 5-7, 2010.
- Program Committee Member of 12th Information Hiding Conference (IH 2010), Calgary, Alberta, Canada, June 28-30, 2010.
- Program Committee Member of 7th Conference on Security and Cryptographu for Networks (SCN 2010), Amalfi, Italy, September 13-15, 2010.
- Program Committee Member of 5th Benelux Workshoip on Information and System Security (WISSEC'10).
- Program Committee Member of 4th Provable Security Conference (ProvSec 2010), Malacca, Malaysia, October 13-15, 2010.
- Program Committee Member of 3rd Africacrypt 2010, Stellenbosch, South Africa, May 3-6, 2010.
- Program Committee Member of 4th International Information Security and Cryptology Conference (ISCTURKEY'10), Ankara, Turkey, May 6-8, 2010.
- Program Committee Member of IACR conference 30th Eurocrypt'11.
- Program Committee Member of 14th International Workshop on Practice and Theory in Public Key Cryptography (PCK'11).
- Program Committee Member of RSA Conference 2011, 11th Cryptographers'Treack (CT-RSA 2011).

Co-organizer of:
- Co-organizer of PASC Seminar Practical Approaches to Secure Computation, April 29, TU Eindhoven.

Invited lectures:

- Invited Lecture Series at TUBITAK, Electronic Voting and Secure Multiparty Computation, Istanbul, Turkey, May 18- 21, 2010.
- Invited Lecturer on Electronic Elections at Winter School in Information Security, Finse – April 25-30, 2010.
- Invited Talk Secure Multiparty Computation: A Showcase for Modern Cryptography at 4th International Information Security and Cryptology Conference (ISC'10), METU, Ankara, Turkey, May 6, 2010.
- Invited Speaker on "Protocols for Multi-Party Computation" at Summer School on Applied Cryptographic Protocols 2010, Mykonos, Greece, Sep. 26- Oct. 1, 2010.
- Invited Talk "Gates and Circuits for Secure Multiparty Computation" at ISP Lab Colloquium, TU Delft, November 5, 2010.

Member of steering committees:

- Member of steering committee Vote ID steering committee, bi-annual international conference on research in electronic voting.

External member of PhD committees:

- Referee on PhD committee of Roland Wen, Online Elections in Terra Australis, School of Computer Science and Engineering, The University of New South Wales, November 2010.

Boris Skoric

PC-member of:

- Program Committee Member of Workshop on Information Forensics and Security (WIFS) 2010, Seattle, USA, December 12-15, 2010.

Invited Lectures:

- Invited Keynote Speech at Information Hiding 2010, Security with Noisy Data, Calgary, Alberta, Canada, June 28-30, 2010.
- Seminar talk at the Complex Photonic Systems (COPS) group, Quantum Readout of Physical Unclonable Functions, February 19, 2010, TU Twente.
- Invited talk at Technical University Darmstadt, Security Engineering group, Accusation probabilities in Tardos codes, September 14, 2010

Member of the PhD committee:

- Member of the PhD committee of Bruno Kindarji, Protection de donn´ees biom´etriques, June 4, 2010, Telecom ParisTech.

Henk van Tilborg

Organizer of:

- Organizer of EIDMA Cryptography Working Group meetings.

PC member of:

- Program Committee Member of YACC 2010, Porquerolles Island, France, October 4-8, 2010.

Benne de Weger

Organizer of:

- Co-organizer of the 3TU AMI Opening Symposium, April 15, 2010
- Guest-organizer of the exhibition "Tijdrekken", Scryption, Tilburg October 2010 – January 2011.

Nicola Zannone

PC member of:

- Program Committee Member of 4th Workshop on Combining Context with Trust, Security, and Privacy (CAT 2010), August 23-24, 2010, Nice, France.
- Program Committee Member of 5th International Workshop on Data Privacy Management (DPM 2010), September 23, 2010, Athens, Greece.
- Program Committee Member of International Workshop on Security Measurements and Metrics (MetriSec 2010), September 15, 2010, Bolzano-Bozen, Italy.
- Program Committee Member of 3rd International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ 2010), June 13-19, 2010, Athens, Greece.
- Program Committee Member of 5th International Conference on Availability, Reliability and Security (ARES 2010), 15-18 February, 2010, Krakow, Poland.

Publication chair of:

- Publication chair of International Symposium on Engineering Secure Software and Systems (ESSoS 2010), 3-4 February, 2010, Pisa, Italy.

Editorial work

Sandro Etalle

- Guest editor of the Special Issue of the Journal of Automated Reasoning on Computer Security: Foundations and Automated Reasoning.

Jerry den Hartog

- Guest editor of the Special Issue of the Journal of Automated Reasoning on Computer Security: Foundations and Automated Reasoning.

Tanja Lange

- Member of the Editorial board of Applicable Algebra in Engineering, Communication and Computing (AAECC).
- Member of the Editorial board of Advances in Mathematics of Communications (AMC), since 2008.
- Associate editor of Encyclopedia of Cryptology and Security, since 2008.

Berry Schoenmakers

- Member of the Editorial board of International Journal of Applied Cryptography (IJACT).
- Co-editor of Encyclopedia of Cryptology and Security.

Henk van Tilborg

- Editor of *Advances in Mathematics of Communications (AMC).*
- Advisory Editor of *Advances in Mathematics of Communications (AMC).*
- Editor or the *Asian-European Journal of Mathematics (AEJM).*
- Associate Editor of *Designs, codes and Cryptography.*
- Associate Editor of the *Journal of Combinatorics, Information & System Sciences.*
- Editor of Encyclopedia of Cryptology and Security.

Current and accepted projects

(http://www.win.tue.nl/sec/research.html or 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); 2008 - 2010.
- SecureSCM –Secure Supply Chain Management (EU-project, FP7); 1-2-2008 until 31-1-2011.
- ECRYPT II - Network of Excellence in Cryptography (EU-project, FP7); June 2008 until June 2012.
- Pearl – Privacy Enhanced security Architecture for RFID labels (STW/Sentinels project), January 2007 until January 2011.
- S-Mobile - Security of Software and Services for Mobile Systems (STW/Sentinels project), January 2007 until January 2011.
- PINPASJC - Program Inferred Power Analysis in Software -- JavaCard (STW/Sentinels project), 2005 - 2008.
- SEDAN - Searchable Data Encryption (STW/Sentinels project), 2007 - 2011.
- Pace – Pairing Acceleration for Cryptography using Elliptic Curves; 1-7-2011 till 1-7-2013. Awarded in 2010.
- 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), June 2007 until June 2011.
- CREST – Collusion Resistant Tracing (STW/Sentinels project), 2009 – 2013.
- Identity Management for Mobile Devices, 2010 - 2014.
- "Toegepaste Cryptografie" – long-lasting WBSO subsidy.
- Philips NatLab adviser (Schoenmakers)
- DIAMANT (Cryptologie professor), 2006 - 2011.
- CEDICT (Embedded System Security professor) 2007 - 2012.
- ASCA – Advanced Side Channel Attacks (Subsidy arrangement knowledge worker) 2009 - 2010.

Teaching

De Group members took care of the following Security related lectures.
- 2IC95 Seminar security
- 2IC99 Capita selecta security
- 2IS35 Verification of security protocols
- 2IC95 Seminar Information Security Technology
- 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

Eduction available by the Kerckhoff Institute:
- 2IC35 Physical Aspects of Digital Security
- 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 (UT)
- 2IF12 Law in Cyberspace (RU)
- 2IF13 Privacy Seminar (RU)
- 2IF14 Hardware and operating system security (RU)
- 2IF15 Secure Data Management (UT)
- 2IF16 Security of Information Services (UT)

TU/e Mathematics for Industry (2-year program):
- Coding 1
- Coding 2
- Crypto 1
- Crypto 2

Master math:
- Cryptology course, with other lecturers from CWI.
- Coding theory
- Number Theory and Cryptology

Master class Security for high school students, January 15, 2010 and February 5, 2010.

Scientific output 2010

See attachment 2

EiPSI personnel

Coding & Crypto

Permanent staff

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

Guest

Bernstein, Daniel

Postdoc

Ignatenko, Tanya (shared with Electro)
Krøigard, Mikkel (from February 1, 2010)

Ph.D. students

Bisson, Gaetan
Hoogh, Sebastiaan
Juririus, Relinde
Liesdonk, Peter van
Niederhagen, Ruben (from April 1, 2010)
Oosterwijk, Jan-Jaap
Peters, Christiane
Schwabe, Peter
Villegas Bautista, José (till May 1, 2010)

Support staff

Klooster, Anita (secretary CC and Ei/Ψ, till October 15, 2010)
Rianne van Lieshout (secretary CC, from October 15, 2010)
Kortsmit, Wil (IT specialist)

Security

Permanent staff

Etalle, Sandro
Hartog, Jerry den
Škorić, Boris

Parttime staff

Petkovic, Milan

Postdoc

Chatzikokolakis, Kostas
Lu, Jiqiang (till June 14, 2010)
Zannone, Nicola

Ph.D. student

Boesten, Dion
Bruso, Mayla
Costante, Elisa (from May 1, 2010)
Liang, Xiaoping (till January 15, 2010)
Pontes Soares Rocha, Bruno
Simone, Antonino
Trivellato, Daniel
Veeningen, Meilof

Knowledge worker

Pan, Jing

On secondment

Erik Luit

Support staff

Matthijsse-van Geenen, Jolande (secretary SEC and Ei/Ψ)

Guests:

Daniel Bernstein	Almost continuous.
Jufeng Fan	March 3-5, 2010.
	Guest C&C + speaker at the EIPSI-seminar on Wednesday, March 3, 2010.
J.A. Garay	April 28 until May 1, 2010.
	Member PhD Committee José Villegas Bautista.
Bo-Yin Yang	June 4-7, 2010 and September 23-26, 2010.
Chen-Mou Cheng	June 4 until June 7, 2010.
Irene Marquez Corbella	September 15 until December 15, 2010.
André Apitzsch	October 1, 2010 until December 31, 2010.

Attachment 1 Press

General:

January 14, 2010	Article in Nederlands Dagblad, Henk van Tilborg.
January 28, 2010	Article in Cursor, Sandro Etalle.
February 19, 2010	Article in Automatiseringsgids, Sandro Etalle.
March 3, 2010	Article in NRCNext, Benne de Weger.
June 9, 2010	Article in NRC, Berry Schoenmakers.
September 23, 2010	Article in "Cursor", Benne de Weger.
October 9, 2010	TV-interview with Sandro Etalle by NOS Nieuwsuur. (http://nieuwsuur.nl/video/190342-het-gevaar-van-stuxnet.html).
October 15, 2010	Article in De Ingenieur, Sandro Etalle. (http://www.win.tue.nl/~setalle/presentations/2010_stuxnet_INGR.pdf).
November 2, 2010	Interview Natuurwetenschap & Techniek, article in NWT Online, Benne de Weger.
December16-17, 2010	Article in AD, Trouw, Telegraaf and 22 other papers. (http://www.win.tue.nl/~setalle/media/decrypt_media_2010.html).
December 18, 2010	Article in Elsevier, Tanja Lange.

SuperTU/esday:

January 28, 2010	Announcement Super TU/esday in Cursor 17. (http://web.tue.nl/cursor/internet/jaargang52/cursor17/onderzoek/onder-zoek.php)
February 5, 2010	Announcement Super TU/esday in De Ingenieur (nr. 2).
February 6, 2010	Articles about Scryption and SuperTU/esday in Eindhovens Dagblad.
February 8, 2010	About Scryptions exhibition during Goede morgen Nederland, 9.30 h. with Jolande Otten and Henk van Tilborg. Radio 1, KRO. (http://player.omroep.nl/?aflID=10631337).
February 8, 2010	Brabant 10 TV in Nieuws about Scryptions exhibition. (www.brabant10.nl and http://www.brabant10.nl/UitzendingGemist.asp?itemsID=1769).
February 8, 2010	Omroep Brabant radio about Scryptions exhibition.
Februari 8, 2010	Omroep Brabant TV, in the news broadcast as from 18.30 hour. (http://www.omroepbrabant.nl/mediaplayer.aspx?object=missed-&ssmp=true&id=3).
February 8, 2010	ED-TV on the website ED.nl as from 16.30 hour. (http://www.ed.nl/regio/eindhovenstad/6212397/geheimschrift-ontcijferen-op-TUe.ece).
February 8, 2010	E-TV (Lokale Omroep Eindhoven) in the news broadcast as from 18.00 hour. (www.omroepeindhoven.nl and http://www.dezendervooreindhoven.nl/uitz_gemist/viewer.php?vid=1287&q=0&q=1).

February 9, 2010	Teleac-radio interview with Bart Jacobs and Henk van Tilborg. (www.hoezoradio.nl and http://www.teleac.nl/radio/index.jsp?site+siteradio&nr+1683209-&item=2771790).
February 11, 2010	Vara Radio, Kassa op Radio 1 (Jan Peels). (http://kassa.vara.nl/radio/afspeelpagina/fragment/scholieren-leren-codes-kraken/speel/1/).
February 11, 2010	A report about Scryption (De geheimen van Geheimschrift) in Cursor 19. (http://web.tue.nl/cursor/internet/jaargang52/cursor19/nieuws/index.php)
February 15, 2010	Article in NRC, Bewijs maar eens je onschuld.
February 16, 2010	BNR Denktank, interview with Henk van Tilborg, Marcel Spruit en Jan de Boer, by Hamke Pijpers. (http://www.bnr.nl/radio/programmas/denktank/14163061?archief).
February 17, 2010	A report about Super TU/esdayD(igitale veiligheid blijft “hot item”) in De Trompetter.

Attachment 2 Scientific output

Journal article

Yudistira Asnar, Fabio Massacci, Ayda Saidane, Carlo Riccucci, Massimo Felici, Alessandra Tedeschi, Paul El Khoury, Keqin Li, Magali Segurun, and Nicola Zannone. *Organizational Patterns for Security and Dependability: from design to application*. International Journal of Secure Software Engineering, 2010. To appear.

Gaetan Bisson and Andrew V. Sutherland. *Computing the endomorphism ring of an ordinary elliptic curve over a finite field.* Journal of Number Theory, issue on Elliptic Curve Cryptography, to appear.

A. Blokhuis, A.E. Brouwer, E. Chowdhury, P. Frankl, T. Mussche, B. Patkós, and T. Szőnyi. *A Hilton-Milner theorem for vector spaces*, Electr. J. of Combinatorics **17** (2010) R71.

A. Blokhuis, A.E. Brouwer, and T. Szőnyi. *Covering all points except one.* J. Algebr. Combin. **32** (2010) 59-66.

Klemens Bohm, Sandro Etalle, Jerry den Hartog, Christian Hutter, Slim Trabelsi, Daniel Trivellato, and Nicola Zannone. *A Flexible Architecture for Privacy-Aware Trust Management*. Journal of Theoretical and Applied Electronic Commerce Research, 5(2):77–96, 2010. ISSN 0718-1876.

A.E. Brouwer, and M. Popoviciu. *The invariants of the binary nonic.* J. Symb. Comput. **45** (2010) 709-720.

A.E. Brouwer, and M. Popoviciu. *The invariants of the binary decimic.* J. Symb. Comput. **45** (2010) 837-843.

M. Bruso, A. Cortesi (2010). *Non-repudiation analysis with LYSA with annotations*. Computer Languages, Systems and Structures, 36(4), 352-377.

K. Chatzikokolakis, C. Palamidessi. *Making Random Choices Invisible to the Scheduler*. Information and Computation, 2010, to appear. (http://www.lix.polytechnique.fr/~kostas/papers/scheduler_journal.pdf)

Golnaz Elahi, Eric Yu, and Nicola Zannone. *A Vulnerability-Centric Requirements Engineering Framework: Analyzing Security Attacks, Countermeasures, and Requirements Based on Vulnerabilities*. Requirements Engineering, 15(1):41–62, 2010. ISSN 1432-010X.

T. Ignatenko, F. Willems. *Fuzzy Commitment Scheme: Privacy and Security Analysis.* IEEE Transactions on Information Forensics and Security, vol.5, no.2, pp. 337-348, Jun. 2010.

Florian Luca and Benne de Weger. *"\sigma_k(F_m) = F_n"*. To appear in the New Zealand Journal of Mathematics.

Marco Montali, Paolo Torroni, Nicola Zannone, Paola Mello, and Volha Bryl. *Engineering and Verifying Agent-Oriented Requirements augmented by Business Constraints with B-Tropos*. Autonomous Agents and Multi-Agent Systems, 2010. To appear.

Bruno P.S. Rocha, Sruthi Bandhakavi, Jerry den Hartog, William H. Winsborough and Sandro Etalle. *Information flow and declassification analysis for legacy and untrusted programs*. ACM Transactions on Programming Languages and Systems (TOPLAS). Submitted, under review.

Bruno P.S. Rocha, Daniel N.O. Costa, Rande A. Moreira, Cristiano G. Rezende, Antonio A.F. Loureiro, Azzedine Boukerche. *Adaptive Security Protocol Selection for Mobile Computing*. In Journal of Network and Computer Applications, Special Issue on Middleware Trends for Network Applications. Elsevier, number 5, volume 33, pages 569-587, September 2010.

Cristiano Rezende, Azzedine Boukerche, Richard W. Pazzi, Bruno P.S. Rocha, Antonio A.F. Loureiro. *The Impact of Mobility on Mobile Ad Hoc Networks through the Perspective of Complex Networks.* To appear in Journal of Parallel and Distributed Computing. Elsevier, 2011.

Skoric, B., Makkes, M.X. (2010). *Flowchart description of security primitives for Controlled Physical Unclonable Functions*. International Journal of Information Security, *9*(5), 327-335.

Verbitskiy, E.A., Tuyls, P.T., Obi, C., Schoenmakers, B., Skoric, B. (2010). *Key extraction from general non-discrete signals*. IEEE Transactions on Information Forensics and Security, 5(2), 269-279.

Book chapter

Stanislav Bulygin and Ruud Pellikaan. *Decoding and finding the minimu distance with Gröbner bases: history and new insights.* In I. Woungang, S. Misra and S.C. Misra (Eds.), Selected Topics in Information and Coding Theory, pages 585-622, World Scientific, London, 2010. http://www.worldscibooks.com/compsci/7116.html

Fabio Massacci, John Mylopoulos, and Nicola Zannone. *Security Requirements Engineering: the SI* Modeling Language and the Secure Tropos Methodology.* In Zbigniew Ras and Li-Shiang Tsay, editors, Advances in Intelligent Information Systems, volume 265 of Studies in Computational Intelligence, pages 147–174. Springer-Verlag GmbH, 2010. ISBN 978-3-642-05182-1.

Benne de Weger, *Hoe je het cryptosysteem RSA soms kunt kraken.* In: "Wiskunde: de uitdaging - Vakantiecursus 2010", CWI Syllabus 60, Amsterdam, 2010.

Conference proceeding

Bernstein, D.J., Birkner, P., Lange, T. (2010). *Starfish on strike*. In M. Abdalla, P.S.L.M. Barretto (Eds.), Progress in Cryptology - LATINCRYPT 2010 (First International Conference on Cryptology and Information Security in Latin America, Puebla, Mexico, August 8-11, 2010. Proceedings). (Lecture Notes in Computer Science, Vol. 6212, pp. 61-80). Berlin: Springer.

Bernstein, D.J., Chen, H.C., Cheng, C.M., Lange, T., Niederhagen, R.F., Schwabe, P., Yang, B.Y. (2010). ECC2K-130 on NVIDIA GPUs. In G. Gong, K.C. Gupta (Eds.), *Progress in Cryptology - INDOCRYPT 2010* (11th International Conference on Cryptology in India (Hyderabad, India, December 12-15, 2010. Proceedings). (Vol. 6498, pp. 328-346). Berlin: Springer.

Bernstein, D.J., Lange, T. (2010). Type-II optimal polynomial bases. In M.A. Hasan, T. Helleseth (Eds.), *Arithmetic of Finite Fields* (Third International Workshop, WAIFI 2010, Istanbul, Turkey, June 27-30, 2010. Proceedings). (Lecture Notes in Computer Science, Vol. 6087, pp. 41-61). Berlin: Springer.

Daniel J. Bernstein, Tanja Lange, Christiane Peters. *Wild McEliece*. To appear in proceedings of SAC 2010.

Joppe W. Bos, Thorsten Kleinjung, Ruben Niederhagen, Peter Schwabe (2010). *ECC2K-130 on Cell CPUs.* AFRICACRYPT 2010, Stellenbosch, South Africa, May 3-6, 2010 (Lecture Notes in Computer Science 6055 Springer 2010, ISBN 978-3-642-12677-2, pp. 225-242).

Charles Bouillaguet, Hsieh-Chung Chen, Chen-Mou Cheng, Tony Chou, Ruben Niederhagen, Adi Shamir, and Bo-Yin Yang. *Fast Exhaustive Search for Polynomial Systems in F_2*, Cryptographic Hardware and Embedded Systems — CHES 2010, Lecture Notes in Computer Science, Vol. 6225, pp. 203—218. Springer, 2010.
http://www.polycephaly.org/papers/fesearch.pdf

Bruso, M., Chatzikokolakis, K., Hartog, J.I. den (2010). *Formal verification of privacy for RFID systems*. Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10, Edinburgh, UK, July 17-19, 2010). (pp. 75-88). IEEE Computer Society.

K. Chatzikokolakis, T. Chothia and A. Guha. *Statistical Measurement of Information Leakage*. Proceedings of TACAS '10, to appear.

Costello, C., Lange, T., Naehrig, M. (2010). *Faster pairing computations on curves with high-degree twists*. In P.Q. Nguyen, D. Pointcheval (Eds.), Public Key Cryptography - PKC 2010 (13th International Conference on Practice and Theory in Public-Key Cryptography, Paris, France, May 26-28, 2010. Proceedings). (Lecture Notes in Computer Science, Vol. 6056, pp. 224-242). Berlin: Springer.

Ivan Damgård, Yuval Ishai and Mikkel Krøigaard. *Perfectly Secure Multiparty Computation and the Computational Overhead of Cryptography*. EUROCRYPT 2010, report 2010/106.

Guajardo, J., Mennink, B. & Schoenmakers, B. (2010). *Modulo reduction for Paillier encryptions and application to secure statistical analysis*. In R. Sion (Ed.), Financial Cryptography and Data Security (14th International Conference, FC 2010, Tenerife, Canary Islands, January 25-28, 2010. Revised Selected Papers). (Lecture Notes in Computer Science, Vol. 6052, pp. 375-382). Berlin: Springer.

Guajardo, J., Mennink, B. & Schoenmakers, B. (2010). *Anonymous credential schemes with encrypted attributes*. In S.-H. Heng, R.N. Wright & B.-M. Goi (Eds.), Cryptology and Network Security (9th International Conference, CANS 2010, Kuala Lumpur, Malaysia, December 12-14, 2010. Proceedings). (Lecture Notes in Computer Science, Vol. 6467, pp. 314-333). Berlin: Springer.

Ibraimi, L., Asim, M., Petkovic, M. (2010). *An encryption scheme for a secure policy updating*. *SECRYPT 2010 (*Proceedings of the 5th International Conference on Security and Cryptography, Athens, Greece, July 26-28, 2010). (pp. 399-408). INSTICC.

T. Ignatenko, F.M.J. Willems, *Fundamental Limits for Biometric Identification with a Database Containing Protected Templates.* in Proc. of the IEEE International Symposium on Information Theory and its Applications (ISITA), Oct. 17-20, 2010.

T. Ignatenko, F.M.J. Willems, *Secret-Key and Identification Rates for Biometric Identification Systems with Protected Templates*. in Proc. of the 31st Symposium on Information Theory in the Benelux, May 11-12, 2010, Rotterdam, The Netherlands, 2010, pp.121-128.

T. Ignatenko, F. Willems, *On Information Leakage in Fuzzy Commitment*. In Proc. of IS&T/SPIE Electronic Imaging: Media Forensics and Security XII, Vol. 7541, Jan. 17–21, 2010, San Jose, CA, USA, pp. 75410P-1-75410P-14.

Jiqiang Lu, *Differential Attack on Five Rounds of the SC2000 Block Cipher*. In Feng Bao, Moti Yung, Dongdai Lin, Jiwu Jing (eds.): Proceedings of INSCRYPT '09 --- The 5th China International Conference on Information Security and Cryptology, Lecture Notes in Computer Science, Vol. 6151, pp. 50--59, Springer-Verlag (2010). An enhanced version is available as Report 2010/593, Cryptology ePrint Archive.

J. Lu, J. Pan, and J. den Hartog. *Principles on the security of aes against first and second-order differential power analysis*. In Jianying Zhou and Moti Yung, editors, Proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS'10), volume 6123 of Lecture Notes in Computer Science, pages 168–185. Springer-Verlag, 2010.

Michael Naehrig, Ruben Niederhagen, Peter Schwabe (2010). *New Software Speed Records for Cryptographic Pairings.* LATINCRYPT 2010, Puebla,Mexiko, August 8-11, 2010 (Lecture Notes in Computer Science 6212, Springer 2010, ISBN 978-3-642-14711-1, pp. 109-123).

J. Pan, J.I. den Hartog, J.G.J. van Woudenberg, and M.F. Witteman. *Optimizing dpa by peak distribution analysis*. In Proceedings of Selected Areas in Cryptography, Waterloo, Ontario, Canada, 2010. Springer-Verlag. (To appear in LNCS).

Christiane Peters. *Information-set decoding for linear codes over Fq*. In Post-Quantum Cryptography, Lecture Notes in Computer Science, Vol. 6061, pp. 81--94. Springer, 2010.

Pontes,Soares Rocha, B., Bandhakavi, S., Hartog, J.I. den, Winsborough, W.H., Etalle, S. (2010). *Towards static flow-based declassification for legacy and untrusted programs*. Proceedings IEEE Symposium on Security and Privacy (SP, Oakland CA, USA, May 16-19, 2010). (pp. 93-108). IEEE.

Skoric, B. (2010). *Quantum readout of Physical Unclonable Functions*. In D.J. Bernstein, T. Lange (Eds.), Progress in Cryptology - AfricaCrypt 2010 (Third International Conference on Cryptology in Africa, Steellenbosch, South Africa, May 3-6, 2010. Proceedings). (Lecture Notes in Computer Science, Vol. 6055, pp. 369-386). Berlin: Springer.

Skoric, B. (2010). *Security with noisy data* (Extended abstract of invited talk). In R. Böhme, P.W.L. Fong, R. Safavi-Naini (Eds.), Information Hiding (12th International Conference, IH 2010, Calgary, AB, Canada, June 28-30, 2010. Revised Selected Papers). (**Lecture Notes in Computer Science**, Vol. 6387, pp. 48-50). Berlin: Springer.

Meilof Veeningen, Benne de Weger, and Nicola Zannone. *Modeling identity-related properties and their privacy strength*. In Proceedings of the 7th International Workshop on Formal Aspects of Security & Trust (FAST'10), Lecture Notes in Computer Science, Pisa, Italy, 13-18 September 2010. Springer-Verlag GmbH. (Acceptance rate: 15/42 = 36%).

Wartena, F., Muskens, L., Schmitt, L., Petkovic, M. (2010). *Continua: The reference architecture of a personal telehealth ecosystem*. *Proceedings of the 12th IEEE International Conference on e-Health Networking, Application and Services (Healthcom 2010, Lyon, France, July 1-3, 2010).* IEEE

F.M.J. Willems, T. Ignatenko, Identification and Secret-Key Binding in Binary-Symmetric Template-Protected Biometric Systems, in Proc. of IEEE Workshop on Information Forensics and Security, Seattle, the USA.

F.M.J. Willems, T. Ignatenko, Identification and Secret-Key Generation in Biometric Systems with Protected Templates, in Proc. of The 12th ACM Workshop on Multimedia and Security, 2010, Rome, Italy, pp.63-66.

Nicola Zannone, Milan Petkovic, and Sandro Etalle. Towards Data Protection Compliance. In Proceedings of the International Conference on Security and Cryptography (SECRYPT'10), Athens, Greece, 26-28 July 2010.

Edited book

Bernstein, D.J., Lange, T. (Eds.).(2010). *Progress in Cryptology - AFRICACRYPT 2010 : third international conference on cryptology in Africa, Stellenbosch, South Africa, May 3-6, 2010, proceedings*. Berlin: Springer.

Jonker, W., Petkovic, M. (Eds.).(2010). *Secure data management (7th VLDB workshop, SDM 2010, Singapore, September 17, 2010. Proceedings)*. Berlin: Springer.

Fabio Massacci, Dan Wallach, and Nicola Zannone, editors. Engineering Secure Software and Systems. Second International Symposium, ESSoS 2010, Pisa, Italy, February 2010, Proceedings, volume 5965 of Lecture Notes in Computer Science. Springer-Verlag GmbH, 2010. ISBN 978-3-642-11746-6.

External report

Simone, A., Skoric, B. (2010). *Accusation probabilities in Tardos codes : the Gaussian approximation is better than we thought*. Cryptology ePrint Archive No. 2010/472, IACR.

Daniel J. Bernstein, Tanja Lange, Christiane Peters. Ball-collision decoding. Cryptology ePrint Archive 2010/585, IACR.

Gaetan Bisson. *Computing endomorphism rings of elliptic curves under the GRH.* Preprint posted on arXiv and IACR ePrint.

Gaetan Bisson and Andrew V. Sutherland. *A low-memory algorithm for finding short product representations in finite groups.* Preprint posted on arXiv and IACR ePrint.

Relinde Jurrius and Ruud Pellikaan, "Codes, arrangements and matroids", to appear in E. Martinez-Moro (Ed.), Selected topics on coding theory and cryptology. Algebraic geometry modeling in information theory, World Scientific, London 2011. ISBN: 978-981-4335-75-1.

Jiqiang Lu. New Methodologies for Differential-Linear Cryptanalysis and Its Extensions. In Cryptology ePrint Archive, Report 2010/025 (2010).

Irene Márquez-Corbella, Edgar Martínez-Moro and Ruud Pellikaan, "The non-gap sequence of a subcode of a GRS code", submitted to WCC-2011.

Ruud Pellikaan, X.-W. Wu and Stanislav Bulygin, "Error-correcting codes and cryptology". Werktitel van een boek te verschijnen bij Cambridge University Press.

Internal report

Daniel Trivellato, Nicola Zannone, Sandro Etalle, 2010. GEM: a Distributed Goal Evaluation Algorithm for Trust Management. Tech. Rep. CS 10-15, Eindhoven University of Technology

Dissertation

Mikkel Krøigaard, *On the Computational Overhead of Secure Multiparty Computation*, Aarhus, August 25, 2010.

J. Villegas Bautista, Design of Advanced Primitives for Secure Multiparty Computation. Special Shuffles and Integer Comparison, TU/e, April 29, 2010.