Jaarverslag en onderzoeksrapportage 2008

Dit is het eerste volle jaar dat Ei/Ψ actief is. Voor een zo'n jonge nieuwe groep is er al een grote mate van saamhorigheid bereikt. Dit resulteert ook in gezamenlijke projectaanvragen.
De Grand Opening van Ei/Ψ op 21 en 22 april mag een groot succes genoemd worden. Het programma (als bijlage toegevoegd) bevatte klinkende namen en trok de eerste dag een volle Blauwe Zaal (305 deelnemers) en de tweede dag 160 deelnemers.

Wetenschappelijke activiteiten in 2008

EiPSI seminar

9 april Yvo Desmedt, *Applying Recreational Mathematics to Secure Multiparty Computation*
7 mei Fred Spiessens, *Patterns of Safe Collaboration*
21 mei Tomas Toft, *Improved Constant-Rounds Bit-Decomposition of Secret Shared Values*
4 juni Jerry den Hartog, *Consent policies: From Patient to XACML*
18 juni Peter van Liesdonk, *Searching in encrypted data*
2 juli Peter Birkner, *The group structure of elliptic curves*
3 sept. Jing Pan, *An Operation-based Metrics for Correlation Power Analysis*
1 okt. Christiane Peters, *Attacking and defending the McEliece cryptosystem*
15 okt. Sebastiaan de Hoogh, *MPC based on Threshold Homomorphic Cryptosystems: an overview*
29 okt. Bruno Pontes Soares Rocha, *Language-based information flows*
12 nov. Peter Schwabe, *Achieving software speed records with qhasm*
26 nov. Relinde Jurrius, *Generalized weight enumerators*
10 dec. Boris Skoric, *Privacy amplification*

Cryptography Working Group

15 jan. Karin Poels,*Cryptanalysis of SFLASH; from a standard for fast signatures to an attack that forges fast signatures for any message*
Peter Birkner, *Edwards Curves and the ECM Factorisation Method*
Bert den Boer, *A Simple Side-Channel Attack on RSA*
Tomas Toft, *Practical MPC for practical problems*

3 okt. Rob van Esch, *Provable security in Cryptography. Reductionist security arguments for EC-KCDSA*

Jurjen Bos, *Zero knowledge and Sudoku*

Eric Verheul, *An analysis of the vector decomposition problem in elliptic curve groups (joint work with Steven Galbraith)*

Cees Jansen, *The Linear Equivalence Bias in Jump Controlled Linear Finite State Machines*

12 dec. Sebastiaan de Hoogh, *On the speed of VSH*

Henk van Tilborg, *Authentication Codes, from Error-Correcting Codes*

Wil Michiels, *State-of-the-art in white-box cryptography*

Gerard Tel, *Function Graphs in the Classroom Elgamal Demo*

Summer school/minicourse

- DIAMANT-Summer School on Elliptic and Hyperelliptic Curve Cryptography, September 15-19, 2008.

EiPSI Grand Opening, Eindhoven, April 21-22

David Kahn

Whitfield Diffie (Sun Microsystems), *Directions in signal intelligence*

Andrew Odlyzko (Digital Technology Center), *How to live and prosper with insecure cyberinfrastructure*

Ian Brown (Oxford Internet Institute), *Policy and privacy engineering*

Bruce Schneier (BT Counterpane),

Bart Jacobs (RUN and TU/e), *OV Chip card developments*

Berry Schoenmakers, *Practical approaches to secure computations between multiple parties*

Tanja Lange *Faster arithmetic on elliptic curves -- blessing to ECC, harm to RSA*

Sandro Etalle (TU/e and UT), *You have something to hide!*

Public forum on "IT Security and Society", chaired by Bart Jacobs

Members: Ian Brown, Whit Diffie, David Kahn, Andrew Odlyzko, Bruce Schneier, and, as further guests, Dan Bernstein (UIC), Bart Preneel (KUL), and Corien Prins (UvT).

Workshops

- Hash Functions in Cryptology: Theory and Practice", Leiden, Juni 2-6, Lorentz Center.
- The 12th Workshop on Elliptic Curve Cryptography (ECC 2008), Sept. 22-24, Utrecht.
- WISSEC 2008: 3rd Benelux Workshop on Information and System Security November 13-14, 2008, Eindhoven.
- Second Dutch Workshop on Information Risk Management. Eindhoven, September 26, 2008.

Organisatorische activiteiten in 2008

- Werving UD Security, resulterend in aanstelling van Boris Škorić.
- Werving PostDoc Security, resulterend in aanstelling van Kostas Chatzikokolakis.
- Werving PostDoc Security, resulterend in aanstelling van Jiqiang Lu.
- Werving Postdoc/UD Security, resulterend in aanstelling van Nicola Zannone
- Werving secretaresse Security, resulterend in aanstelling van Jolande Matthijsse-van Geenen
- Werving PhD student SecureSCM resulterend in aanstelling Sebastiaan de Hoogh
- Werving PhD op project generalized weight enumerators resulterend in aanstelling van Relinde Jurrius
- Vergaderingen van Ei/Ψ-top (Etalle, Jacobs, Lange, Tilborg) op 23 jan., 26 maart en 28 okt. (naast frequent informeel contact en ruggespraak).
- Gesprekken met twee kandidaten over eventueel deeltijdhoogleraarschappen.
- Uitbouwen webpagina (door Klooster en Kortsmit)
- Uitbouwen Eipsi & Security nieuws schermen aan liften (Kortsmit, Spiessens, Weger)

Blijken van externe waardering

Peter Birkner

- *Edwards Curves,* ECRYPT Summer School, Crete, Greece, 12-17 May 2008 (invited speaker)

Tanja Lange

Lid van buitenlandse promotiecommissie:

- K.P. Vidya (Madras Christian College, India)
- Christian Robenhagen Ravnshoj (University of Aarhus, Denmark)

Invited speaker at:

- *Post-Quantum Cryptography*, at 9th International Conference on Cryptology in India (INDOCRYPT 2008), Kharagpur, Dec. 14-17 .
- *Binary Edwards Curves*, Seminario Matematico, Universidad Autonoma Madrid, Spain, 09 May 2008.
- *Scalar Multiplication and Weierstrass Curves*, 3rd ECRYPT Summer School, Crete, Greece, 12-17 May 2008.
- *Secure and Efficient Implementations*, ECRYPT: Challenges and Perspectives for Academia and Industry Antwerp, Belgium, 27 - 29 May 2008.
- *Binary Edwards Curves*, Séminaire de Cryptographie de Rennes, Universite de Renes, France, 20 June 2008.
- *Background (Alice, Bob, and finite fields),* Summer School on Elliptic and Hyperelliptic Curve Cryptography, Technische Universiteit Eindhoven, The Netherlands, 15-19 September 2008.
- *Different forms of elliptic curves*, Summer School on Elliptic and Hyperelliptic Curve Cryptography, Technische Universiteit Eindhoven, The Netherlands, 15-19 September 2008.

Christiane Peters

- Edwards Curves, Séminaire de Cryptographie de Rennes. Universite de Renes, France, 20 June 2008 (invited speaker)

Ruud Pellikaan

Lid van buitenlandse promotiecommissie

- M. Prem Laxman Das, Studies on construction and list decoding of codes on some towers of function fields", March 2008, Indian Statistical Institute, Kolkata. Promotoren: K. Sikdar en R. Barua.

Reza Rezaeian Farashahi

- Binary Edwards Curves, at the 12th Workshop on Elliptic Curve Cryptography (ECC 2008), Utrecht, Sept. 22-24 (invited speaker)

Berry Schoenmakers

- Workpackage leader ECRYPT PROVILAB WG2
- Symposium 'The categorical challenges of electronic voting', *The E-voting Crisis – and the Role of Cryptography*, Nijmegen (Jan. 21, 2008) (invited speaker)..
- ECRYPT: Achievements and Perspectives, *Secure Multiparty Computation Based on Threshold Homomorphic Cryptosystems*, Antwerp, May 27, 2008 (invited speaker)..

Henk van Tilborg

- "Key note speaker" op *de 9th International Pure Mathematics Conference 2008*, Islamabad, Aug. 22-24, as guest of the Pakistan Mathematical Society.
- "Key note speaker" op de NATO Advanced Research Workshop "Enhancing Crypto-Primitives with Techniques from Coding Theory", Veliko Turnovo, Oct. 6-9.
- Voorzitter van de onderzoeks evaluatiecommissie van DTU-Mathematics, Lyngby, Dec. 2-4.

<u>Betrokkenheid bij organisatie van symposia, conferenties, e.d.</u>

Sandro Etalle

Co-PC-Chair of

- FCS-ARSPA-WITS'08 Joint Workshop on Foundations of Computer Security, Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security Affiliated to LICS 2008 and CSF 21. Pittsburgh, PA, USA, June 21-22, 2008.
- APE First International Workshop on Advances in Policy Enforcement (APE'08). Collocated with ARES 2008 Barcelona, Catalonia, March 4th-7th 2008.

PC Member of

- EC2ND 2008, European Conference on Computer Network Defense. December 11th and 12th 2008 Dublin City University, Dublin, Ireland.
- BDIM 2008 Third IEEE/IFIP International Workshop on Business-driven IT Management (BDIM 2008) In conjunction with IEEE Network Operations and Management Symposium (NOMS 2008) Salvador, Bahia, Brazil, April 7th, 2008.

- IFIPTM'08 Joint iTrust and PST Conferences on Privacy, Trust Management and Security. PC Member.

Jerry den Hartog

Co-PC-Chair of

- FCS-ARSPA-WITS'08 Joint Workshop on Foundations of Computer Security, Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security Affiliated to LICS 2008 and CSF 21. Pittsburgh, PA, USA, June 21-22, 2008.

Tanja Lange

Leider van Ecrypt II Lab VAMPIRE "Virtual Applications and Implementations Research Lab"

Leider van CACE working group "Accelerating Secure Networking"

Main organizer and PC Chair of

- The 12th Workshop on Elliptic Curve Cryptography (ECC 2008), Sept. 22-24, 2008, Utrecht, The Netherlands.
- DIAMANT-Summer School on Elliptic and Hyperelliptic Curve Cryptography, Sept. 15-19, 2008, Eindhoven, The Netherlands.

PC member of:

- Indocrypt 2008,
- Asiacrypt 2008,
- PQCrypto 2008
- Pairings'08
- CECC 2008
- ACISP 2008
- Africacrypt,

Member of steering committees:

- International Conference on Pairings
- International Workshop on Post-Quantum Cryptography (PQCrypto)
- Workshop on Elliptic Curve Cryptography (ECC; chairman)

Ruud Pellikaan

Extern lid van het computer algebra project KryFoVe van Dependable Adaptive Systems and Mathematical Modeling.

Invited lectures

- *Decoding error-correcting codes with Groebner bases*, EMS Joint Math Weekend, University of Copenhagen, February 29-March, 2008.
- *Efficient construction of algebraic geometry codes; the q-th power algorithm*, RISC seminar at CWI, 21 Oct. 2008.
- Series of four lectures on ``Algebraic Geometry Codes", for Soria Summer School on Computational Mathematics, July 7-11, 2008.

Berry Schoenmakers

Visiting fellow, Macquarie University, Sydney, Australia with Crypto group of prof. Josef Pieprzyk (30 dec 2008 - 27 mar 2009).

Co-chair of

- 3rd Benelux Workshop on Information and System Security (WISSec'08)
- VOTE-ID 2009 Second Conference on E-Voting and Identity in Luxembourg, September 7-8, 2009, LNCS proceedings.

PC member of

- IACR conferences: 27th Eurocrypt'08
- IACR workshops: 12th International Workshop on Practice and Theory in Public Key Cryptography (PKC'09)
- RSA Conference 2009 9th Cryptographers' Track (CT-RSA 2009)
- 7th International Conference on Cryptology and Network Security (CANS'08)
- 5th European PKI Workshop (EuroPKI'08)
- 3rd International Conference on Security and Cryptography (SECRYPT'08)
- 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'08)
- IAVoSS Workshop On Trustworthy Elections (WOTE'08)
- 3rd Benelux Workshop on Information and System Security (WISSec'08)
- 3rdInternational Conference on Electronic Voting 2008 (EVOTE08)
- International Workshop on Security and Privacy in Enterprise Computing (InSPEC 2008) in conjunction with 12th IEEE International EDOC Conference

Henk van Tilborg

Key note speaker at

- 9th International Pure Mathematics Conference 2008, *Communication graphs, key graphs, and Harary graphs*, Islamabad, 8-22-2008.
- NATO Advanced Research Workshop "Enhancing Crypto-Primitives with Techniques from Coding Theory", *Authentication codes by using coding theory*, Veliko Tarnovo, Bulgaria, 10- 6-2008.

Organizer of the

- Cryptography Working Group meetings
- Grand Opening of Ei/Ψ.

PC lid van

- WCC2009, Ullensvang, Norway, May 10-15, 2009

Benne de Weger

Leader of Ecrypt Aztec WG2

(Co-)Organizer of

- Ecrypt Aztec WG2 Research Retreat, May 9, Paris
- Hash Functions in Cryptology: Theory and Practice", Leiden, Juni 2-6, Lorentz Center.

<u>Editorial werk</u>

Andries Brouwer

- Journal of Algebraic Combinatorics
- European Journal of Combinatorics

Bart Jacobs

- Editor van het Journal Theoretical Computer Science

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

- Chairman of the *Evaluation Committee* of the Department of Mathematics of the Technical University of Denmark, Dec. 2-4, 2008.
- 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

Bart Jacobs

- Member Advisory Committee Computer Science of NWO
- Dagelijks bestuur SENTINELS
- Lid commissie herinrichting verkiezingsproces (commissie Korthals Altes).

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 - Network of Excellence in Cryptography (EU-project), afgesloten in zomer 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), 2007-2008.
- 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.
- "Toegepaste Cryptografie" - langdurig lopende WBSO subsidie.
- Philips NatLab adviseurschap (Schoenmakers)
- DIAMANT (Cryptologie hoogleraar), 2006-2011.
- CEDICT (Embedded System Security hoogleraar) 2007-2012.

Nieuwe projectaanvragen (zie voor samenvatting Bijlage 2)

- Identity Management for Mobile Devices (Etalle, Hoepman, Weger, Zannone)
- CREST (Collusion RESistant Tracing (Skoric, Etalle, Tilborg)
- Generalized weight enumerators (Pellikaan, Tilborg, Asch)
- FLIPPA - Factorization and primality proving (Lange)
- PQCrypto - FET-open; first round (Lange)
- STAMINA – Security, Trust, Availability for Medical Information (Hartog, Etalle, Hartel, Jonker)
- Post-Quantum Cryptography (PQCrypto) EU FP-7 application (Tanja Lange)
- Factorization and primality proving - FLIPPA (Tanja Lange)

Onderwijs

De groepsleden verzorgen het volgende security-gerelateerd onderwijs.
- 2IF03/2IC95 Seminar Information Security Technology
- 2IF11 Distributed trust management
- 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

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.

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

Toft, Tomas

Ph.D. students

Birkner, Peter
Bisson, Gaetan
Hoogh, Sebastiaan (vanaf 1 febr.2008)
Kiraz, Mehmet (t.e.m. febr. 2008)
Liesdonk, Peter van
Naehrig, Michael
Peters, Christiane
Rezaeian Farashahi, Reza (t.e.m. okt. 2008)
Relinde Jurrius (vanaf 1 oct. 2008)
Schwabe, Peter
Villegas Bautista, José

Security

Vaste staf

Etalle, Sandro

Hartog, Jerry den
Skoric, Boris (vanaf 1 aug. 2008)

Deeltijd

Jacobs, Bart

Postdoc

Chatzikokolakis, Kostas (vanaf 15 aug. 2008)
Lu, Jiqiang (vanaf 15 juni 2008)
Spiessens, Fred
Zannone, Nicola (vanaf 1 nov. 2008)

Ph.D. student

Pan, Jing
Pontes Soares Rocha, Bruno
Trivellato, Daniel

Ondersteunend

Klooster, Anita (secretaresse CC en Ei/Ψ)
Kortsmit, Wil (IT specialist)
Matthijsse-van Geenen, Jolande (secretaresse SEC, vanaf 9 juni 2009)

Huisvestiging

- Zaal 8.74 is geschikt gemaakt voor 9 PhD studenten. Hierdoor is er genoeg ruimte voor studenten.
- Op de 10de verdieping zijn drie kamers (72, 73, 75) toe gewezen aan Ei/Ψ. Hiermee is het kamerprobleem van Postdocs, UD's en gasten opgelost. De bilocatie van Ei/Ψ is nu wel een trilocatie geworden! Een ruil met drie kamers of de 8ste verdieping, tegenover de aio ruimtes, is erg gewenst voor de cohesie van de groep.
- Het computer lab van Ei/Ψ is gehuisvest in 9.78. Het continu draaiende computer cluster veroorzaakt een hoge temperatuur die niet afgevoerd kan worden.

Media

- De resultaten van Benne de Weger, zijn voormalige afstudeerder Marc Stevens, en Arjen Lenstra over hash clashes hebben aangetoond dat MD5 niet meer geschikt is voor gebruik van certificaten. Dit was aanleiding tot een radio interview van Benne de Weger en Marc Stevens door Herbert Blankesteijn (De Electronische Eeuw) op 10 januari 2008. Een presentatie op het Chaos Communication Congress in Berlijn op 30 december 2008 heeft wereldwijd veel aandacht getrokken op het internet en in de pers. De website van het project trok nog op 30 en 31 december 50,000 bezoekers. Zie Appendix 2 voor de Press Release en ook http://www.win.tue.nl/hashclash/rogue-ca/ .
- Tanja Lange, Christiane Peters en Dan Bernstein hebben het McEliece cryptosysteem met de indertijd voorgestelde parameters gebroken. Zie Appendix 2 voor de Press Release en http://www.hyperelliptic.org/tanja/press/mceliece.html voor een lijst van plaatsen waar hier over geschreven is.

- De Grand Opening van Ei/Ψ heeft veel aandacht gehad. Meest opvallend waren de radio interviews door Herbert Blankesteijn met Whit Diffie en Andrew Odlyzko, die samen de hele uitzending op 24 april van De Electronische Eeuw vulden. Verder waren er korte radio interviews en de volgende artikelen:
  - voorjaar 2008, artikel in "Vector", *Beveiligen van digitale informatie*
  - voorjaar 2008, artikel in "Matrix", *Beveiligen van digitale informatie*
  - 17 april 2008, artikel in "De Cursor", *EiPSI: Wedloop tussen geheimhouders en codebrekers*
  - 23 april 2008, artikel in "Eindhovens Dagblad", *NXP had chip in ban moeten doen*
  - 26 april 2008, artikel in "Volkskrant", *Laat ze maar lekker kraken*
  - 5 mei 2008, artikel in "De Ingenieur", *ICT is niet veilig te maken*
- De evaluatie van het RIES Internet Voting System voor de Waterschapverkiezingen, waar EIPSI leden een hoofdrol in vervulden, heeft geleid tot een gewijzigde politieke stelling name over deze manier van stemmen. Zie artikel in "NRC Handelsblad", *Internetstemmen van de baan door onveiligheid*.

Scientific output 2008
Zie Bijlage 3

Dissertation
- M.S. Kiraz, *Secure and fair two-party computation*, TUE, 8-27-2008.
- R. Rezaeian Farashahi, *Curves and Jacobians; number extractors and efficient arithmetic*, TUE, 10-27-2008.

Gasten

Daniel Bernstein	bijna continu
Gaetan Bisson	februari en maart
Laura Hitt	2 - 11 februari
Yvo Desmedt	31 maart – 11 april
Bruce Schneier	21 en 22 april
Andrew Odlyzko	21 en 22 april
Ian Brown	21 en 22 april
Whitfield Diffie	21 en 22 april
Nigel Smart	27 en 28 aug.
Benny Pinkas	27 en 28 aug.
Christophe Doche	14 - 24 sept.
David Lubicz	18 - 24 sept.
Benjamin Smith	15 - 24 sept.
Igor Shparlinsky	27 en 28 oct.

Bijlage 1 Projectaanvragen

Collusion RESistant Tracing (CREST)
Principal proposer: Boris Škorić

Forensic watermarking is a technique for tracing the source of unauthorized copies of content such as audio, video and software. A watermark is embedded in the content, carrying a unique identifier of the recipient. This method of protection is based on deterrence. It is more user-friendly than copy protection, and also more cost-effective, since it requires neither additional cryptography nor hardware compliance. Collusion attacks, in which multiple pirates cooperate, represent the main security challenge for forensic watermarking. The scope of this proposal is to perform fundamental research and to provide practical solutions with respect to the resistance of tracing methods against collusion attacks. The ambition is to develop practical tracing techniques that can be combined with current content protection methods and to improve the theoretical foundations of collusion-resistance.

Generalized weight enumerators
Principal proposer: Ruud Pellikaan

Codes are used to correct errors if a message is unreliable stored or send over a noisy channel. This is done by adding redundant information to a message in a clever way. So there is a restriction to code words in a code of all possible words. The weight enumerator of a code is a polynomial that encodes the number of code words of a given weight. The support weight of a subcode is a generalization of the Hamming weight of a word and has several applications in coding theory and cryptology.
The aim of this project is to study properties of the generalized and extended weight enumerator and the two variable zeta function of a code. We want to apply this to derive (non-)existence results of certain codes, to estimate the error-probability of decoding algorithms, and to cryptology. Furthermore the numerous interrelations with many branches of mathematics will be studied.

Identity management for mobile devices
Principal proposer: Sandro Etalle

We are witnessing a change in the use of services in which users increasingly need to be able to access services securely from different locations (home, work, internet cafe). Identity management is therefore becoming a crucial issue both for organizations and individuals. IBM's ""Next 5 in 5" predicts2 that we will have our own digital shopping assistants and that forgetting will become a distant memory "because such details of everyday life will be recorded, stored, analyzed, and provided at the appropriate time and place by both portable and stationary smart appliances".
Present identity management systems do not have the flexibility required for emerging mobile applications. Another problem is the changing balance between privacy,

accountability, and usability. Where present identity management systems often favour usability above security, future systems will have to be more secure while maintaining usability. For instance, in 2007 identity theft was the fastest-growing cybercrime. We – as citizens – are also making increasingly critical and multimodal use of our mobile devices (e.g. for access control, for internet banking, etc), and this makes the consequences of identity theft even more serious than they are now.

Security, Trust, Availability for Medical Information (STAMINA)
Principal proposer: Jerry den Hartog

Healthcare information is sensitive data that needs to be shared amongst organizations with heterogeneous systems and different levels of trustworthiness. Main issues in secure data sharing are the lack of interoperable access control and lack of policy management mechanisms, and methods to determine the trustworthiness of organizations, systems and users. The STAMINA project will address these issues by building on the combination of digital rights management and attribute-based encryption, with decentralized trust management techniques to establish trusted attributes. Together, these techniques will enable the definition of trust levels and the use of protection mechanisms appropriate for the level of trust. By this approach, STAMINA will create a flexible framework for trustworthy, secure use of medical data which optimizes data availability, allows users to specify consent, and which can easily be integrated into existing healthcare systems and infrastructure.

Factorization and primality proving (FLIPPA)
Principal proposer: Tanja Lange

This proposal deals with problems in computational number theory with applications in cryptography.
Each positive integer has a unique factorization into prime powers but finding it can be difficult. Gauss wrote in his Disquisitiones ``The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. [...] Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated." Over the centuries many factorization algorithms have been developed; they range from simple trial division and the sieve of Eratosthenes to H. Lenstra's elliptic curve method (ECM) of factorization and the number-field sieve (NFS).
In this project we plan to investigate several improvements in state-of-the-art algorithms for integer factorization and primality proving. The better ECM speeds we obtained recently require adjustments and new optimizations of several steps of the NFS and we will study and quantify the effects. We also intend to study the use of highly parallel architectures for other parts of the NFS. On the theoretical side we will investigate the influence of larger rational torsion groups on the success probability of ECM.

Elliptic and hyperelliptic-curve primality proofs lead to fast-to-verify certificates. We will investigate usage of Edwards curves for elliptic-curve primality proving. We also plan to study the computational complexity of the hyperelliptic analogue and investigate its practical feasibility.

Post-Quantum Cryptography (PQCrypto) EU FP-7 application
Ccoordinator Tanja Lange

Quantum computers will break all factorization-based and discrete-log-based cryptography. The time frame for quantum computers to become technologically feasible is unclear but once they are available wealthy agencies, spies, and criminals will be able to mount attacks on RSA and ECC, the public-key cryptosystems used to protect the Internet today.
The defenders - smaller nations, companies, and normal households - need to be prepared to protect themselves against this emerging threat. In the foreseeable future they will be working with conventional computers and standard networks; they will need new cryptographic algorithms that are feasible to run on usual PCs but that resist attacks by quantum computers.
Such cryptographic algorithms are already needed now. Health data, police records and government communication often require long-term confidentiality beyond 30 years. An adversary who intercepts and stores an RSA-encrypted document today will be able to decipher it as soon as quantum computers are available.
Fortunately, there are some candidates for "post-quantum public-key cryptography": Hash-tree signatures and multivariate cryptography can be used for post-quantum signatures while lattice-based and coding-based systems can be used for post-quantum encryption.
Unfortunately, these systems are far less well studied and are less efficient in implementation speed, space, or both. Security concerns and efficiency concerns prevent widespread use today and need to be overcome. Users need post-quantum systems that are efficient (hopefully competitive in speed and key-size with RSA and ECC) and that have been thoroughly studied, producing confidence in their long-term security.
Furthermore, cryptographic applications do not use the naked crypto primitives but embed them into protocols. The systems mentioned above do not work as `plug-in' replacements for RSA or ECC; in particular new schemes for the ubiquitous authenticated key-exchange are needed.

Bijlage 2 Pers

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

A cryptosystem proposed in 1978, one of the leading candidates for "post-quantum cryptography", has been broken by researchers at TU/e. Physicists have been racing to build quantum computers that would break the public-key cryptosystems used to protect Internet commerce today, such as RSA and elliptic-curve cryptography. However, quantum computers are not believed to affect the "McEliece cryptosystem" published thirty years ago. Professor Tanja Lange (EiPSI), in a joint paper with her Ph.D. student Christiane Peters and with Professor Daniel J. Bernstein visiting from the University of Illinois at Chicago, described a way to speed up attacks against the McEliece cryptosystem. The researchers wrote software that would decrypt a McEliece ciphertext in just 14 days on a cluster of 100 computers.

The software was run on many computers in the Coding and Cryptography Computer Cluster (C4) and the SAN Distributed and Parallel Integrated Terminal (SANdpit) at TU/e, along with cooperating computers in Amsterdam (CWI), France, Ireland, Taiwan, and the United States. A lucky computer in Ireland found the ciphertext.
The successful attack was announced Saturday at a conference in Cincinnati on Post-Quantum Cryptography. The researchers said that the McEliece cryptosystem, when scaled to larger key sizes to avoid their attacks, remains a leading candidate for post-quantum cryptography.

Press coverage:
Eindhovens Dagblad, October 24, 2008.

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

Independent security researchers in California and researchers at the Centrum Wiskunde & Informatica (CWI) in the Netherlands, EPFL in Switzerland, and EiPSI (TU/e) in the Netherlands have found a weakness in the Internet digital certificate infrastructure that allows attackers to forge certificates that are fully trusted by all commonly used web browsers. As a result of this weakness it is possible to impersonate secure websites and email servers and to perform virtually undetectable phishing attacks, implying that visiting secure websites is not as safe as it should be and is believed to be. The results were presented at the 25C3 security congress in Berlin on the 30th of December 2008. It has already led to an increased adoption of more secure cryptographic standards on the Internet and therewith increased the safety of the Internet.

When you visit a website whose URL starts with "https", a small padlock symbol appears in the browser window. This indicates that the website is secured using a digital certificate issued by one of a few trusted Certification Authorities (CAs). To ensure that

the digital certificate is legitimate, the browser verifies its signature using standard cryptographic algorithms. The team of researchers has discovered that one of these algorithms, known as MD5, can be misused.

The first significant weakness in the MD5 algorithm was presented in 2004 at the annual cryptology conference "Crypto" by a team of Chinese researchers. They had managed to pull off a so-called "collision attack" and were able to create two different messages with the same digital signature. While this initial construction was severely limited, a much stronger collision construction was announced by the researchers from CWI, EPFL and TU/e in May 2007. Their method showed that it was possible to have almost complete freedom in the choice of both messages. The team of researchers has now discovered that it is possible to create a rogue certification authority (CA) that is trusted by all major web browsers by using an advanced implementation of the collision construction and a cluster of more than 200 commercially available game consoles.

The team of researchers has thus managed to demonstrate that a critical part of the Internet's infrastructure was not safe. A rogue CA, in combination with known weaknesses in the DNS (Domain Name System) protocol, can open the door for virtually undetectable phishing attacks. For example, without being aware of it, users could be redirected to malicious sites that appear exactly the same as the trusted banking or e-commerce websites they believe to be visiting. The web browser could then receive a forged certificate that will be erroneously trusted, and users' passwords and other private data can fall in the wrong hands. Besides secure websites and email servers, the weakness also affects other commonly used software.

"The major browsers and Internet players, such as Mozilla and Microsoft, have been contacted to inform them of our discovery and some have already taken action to better protect their users," reassures Arjen Lenstra, head of EPFL's Laboratory for Cryptologic Algorithms. "To prevent any damage from occurring, the certificate we created had a validity of only one month, August 2004, which expired more than four years ago. The only objective of our research was to stimulate better Internet security with adequate protocols that provide the necessary security." Verisign, a major Certificate Service Provider that was still using MD5, has announced that they have now stopped using MD5 for new certificates, and offer customers who recently purchased MD5-based certificates a free renewal. These immediate actions ensure that the risk for Internet users has been minimized.

According to the researchers, their discovery shows that MD5 can no longer be considered a secure cryptographic algorithm for use in digital signatures and certificates. Currently MD5 is still used by certain certificate authorities to issue digital certificates for a large number of secure websites. "Theoretically it has been possible to create a rogue CA since the publication of our stronger collision attack in 2007," says cryptanalyst Marc Stevens (CWI). "It's imperative that browsers and CAs stop using MD5, and migrate to more robust alternatives such as SHA-2 and the upcoming SHA-3 standard," insists Lenstra.

The expert team of researchers consists of: Alexander Sotirov (independent security researcher), Marc Stevens (Cryptology Group, CWI), Jacob Appelbaum (Noisebridge, The Tor Project), Arjen Lenstra (EPFL), David Molnar (UC Berkeley), Dag Arne Osvik (EPFL) and Benne de Weger (EiPSI, TU/e).

Bijlage 3 Wetenschappelijke output

Tijdschriftartikel

Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P. & Shi, H. (2008). Searchable encryption revisited : Consistency properties, relation to anonymous IBE, and extensions. *Journal of Cryptology, 21*(3), 350-391.

Asch, A.G. van & Martens, F.J.L. (2008). Lee weight enumerators of self-dual codes and theta functions. *Advances in Mathematics of Communications, 2*(4), 393-402.

Asch, A.G. van (2008). Matrix-product codes over finite chain rings. *Applicable Algebra in Engineering, Communication and Computing, 19*(1), 39-49.

Asnar, Y., Ciancarini, P., Giorgini, P., Moretti, R., Sebastianis, M., Zannone, N. (2008) Evaluation of Business Solutions in Manufacturing Enterprises. I*nternational Journal of Business Intelligence and Data Mining*, 3(3), 305–329.

Damgård, I. & Toft, T. (2008). Trading sugar beet quotas : secure multiparty computation in practice. *ERCIM News, 73*, 32-33.

Hartog, J.I. den (2008). Towards mechanized correctness proofs for cryptographic algorithms : Axiomatization of a probabilistic Hoare style logic. *Science of Computer Programming, 74*(1-2), 52-63.

Kiyavitskaya, N., Zannone, N. (2008) Requirements Model Generation to Support Requirements Elicitation: The Secure Tropos Experience. Automated Software Engineering, 15(2), 149–173.

Lu, J. & Kim, J. (2008). Attacking 44 rounds of the SHACAL-2 block cipher using related-key rectangle cryptanalysis. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E91-A*(9), 2588-2596.

Rezaeian Farashahi, R., Pellikaan, G.R. & Sidorenko, A. (2008). Extractors for binary elliptic curves. *Designs, Codes and Cryptography, 49* (1-3), 171-186.

Boek - Monografie

Etalle, S. (2008). *Nice to know (Intreerede TU/e 3 oktober 2008).* Eindhoven: Technische Universiteit Eindhoven.

Hoofdstuk in Boek

Bolzoni, D. & Etalle, S. (2008). Approaches in anomaly-based network intrusion detection systems. In R. Di Pietro & L.V. Mancini (Eds.), *Intrusion Detection Systems* (Advances in Information Security, 38) (pp. 1-15). London: Springer.

Congresbijdrage

Bernstein, D.J. & Lange, T. (2008). Analysis and optimization of elliptic-curve single-scalar multiplication. In G.L. Mullen, D. Panario & I.E. Shparlinski (Eds.), *Finite Fields and Applications (Proceedings 8th International Conference, Fq8, Melbourne, Australia, July 9-13, 2007) Vol. 461. Contemporary Mathematics Series* (pp. 1-20). Providence RI: AMS.

Bernstein, D.J., Lange, T. & Peters, C.P. (2008). Attacking and defending the McEliece cryptosystem. In J. Buchmann & J. Ding (Eds.), *Post-Quantum Cryptography (2nd International Workshop, PQCrypto 2008, Cincinnati OH, USA, October 17-19, 2008, Proceedings) Vol. 5299. Lecture Notes in Computer Science* (pp. 31-46). Berlin: Springer.

Bernstein, D.J., Lange, T. & Rezaeian Farashahi, R. (2008). Binary Edwards curves. In E. Oswald & P. Rohatgi (Eds.), *Cryptographic Hardware and Embedded Systems - CHES 2008 (10th International Workshop, Washington DC, USA, August 10-13, 2008, Proceedings) Vol. 5154. Lecture Notes in Computer Science* (pp. 244-265). Berlin: Springer.

Bernstein, D.J. & Schwabe, P. (2008). New AES software speed records. In D.R. Chowdhury, V. Rijmen & A. Das (Eds.), *Progress in Cryptology - INDOCRYPT 2008 (Proceedings 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008) Vol. 5365. Lecture Notes in Computer Science* (pp. 322-336). Berlin: Springer.

Bernstein, D.J., Birkner, P., Joye, M., Lange, T. & Peters, C.P. (2008). Twisted Edwards curves. In S. Vaudenay (Ed.), *Progress in Cryptology - Africacrypt 2008 (First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008, Proceedings) Vol. 5023. Lecture Notes in Computer Science* (pp. 389-405). Berlin: Springer.

Bisson, G. & Satoh, T. (2008). More discriminants with the Brezing-Weng method. In D.R. Chowdury, V. Rijmen & A. Das (Eds.), *Progress in Cryptology - INDOCRYPT 2008 (Proceedings 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008) Vol. 5365. Lecture Notes in Computer Science* (pp. 389-399). Berlin: Springer.

Bolzoni, D. & Etalle, S. (2008). Boosting web intrusion detection systems by inferring positive signatures. In R. Meersman & Z. Tari (Eds.), *On the Move to Meaningful Internet Systems 2008: OTM 2008 Confederated International Conferences (Monterrey, Mexico, November 9-14, 2008), Part II Vol. 5332. Lecture Notes in Computer Science* (pp. 938-955). Berlin: Springer.

Czenko, M., Doumen, J.M. & Etalle, S. (2008). Trust management in P2P systems using standard TuLiP. In Y. Karabulut, J.C. Mitchell, P. Herrmann & C.D. Jensen (Eds.), *Trust Management II (Proceedings of IFIPTM2008: Joint iTrust and PST Conferences on Privacy, Trust Management and Security, Trondheim, Norway, June 18-20, 2008) Vol. 263. IFIP Conference Proceedings* (pp. 1-16). Berlin: Springer.

Dekker, M.A.C., Crampton, J. & Etalle, S. (2008). RBAC administration in distributed systems. In I. Ray & N. Li (Eds.), *SACMAT 2008 (13th ACM Symposium on Access Control Models and Technologies, Estes Park, CO, USA, June 11-13, 2008, Proceedings)* (pp. 93-102). New York: ACM Press.

Desmedt, Y. & Lange, T. (2008). Revisiting pairing based group key exchange. In G. Tsudik (Ed.), *Financial Cryptography and Data Security (12th International Conference, FC 2008, Cozumel, Mexico, January 28-31, 2008, Revised Selected Papers) Vol. 5143. Lecture Notes in Computer Science* (pp. 53-68). Berlin: Springer.

Desmedt, Y., King, B. & Schoenmakers, B. (2008). Revisiting the Karnin, Greene and Hellman bounds. In R. Safavi-Naini (Ed.), *Information Theoretic Security (Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings) Vol. 5155. Lecture Notes in Computer Science* (pp. 183-198). Berlin: Springer.

Garcia, F.D., Koning Gans, G. de, Muijrers, R., Rossum, P. van, Verdult, R., Wichers Schreur, R. & Jacobs, B.P.F. (2008). Dismantling MIFARE Classic. In S. Jajodia & J. Lopez (Eds.), *Computer Security - ESORICS 2008 (13th European Symposium on Research in Computer Security, Malaga, Spain, October 6-8, 2008, Proceedings) Vol. 5283. Lecture Notes in Computer Science* (pp. 97-114). Berlin: Springer.

Jacobs, B.P.F. (2008). Coalgebraic trace semantics for combined possibilitistic and probabilistic systems. In J. Adámek & C. Kupke (Eds.), *Proceedings of the Ninth Workshop on Coalgebraic Methods in Computer Science (CMCS 2008, Budapest, Hungary, April 4-6, 2008) Vol. 203(5). Electronic Notes in Theoretical Computer Science* (pp. 131-152).

Kiraz, M.S. & Schoenmakers, B. (2008). An efficient protocol for fair secure two-party computation. In T.G. Malkin (Ed.), *Topics in Cryptology - CT-RSA 2008 (Proceedings of The Cryptographers' Track at the RSA Conference 2008, San Francisco CA, USA, April 8-11, 2008) Vol. 4964. Lecture Notes in Computer Science* (pp. 88-105). Berlin: Springer.

Lu, J., Dunkelman, O., Keller, N. & Kim, J. (2008). New impossible differential attacks on AES. In D.R. Chowdhury, V. Rijmen & A. Das (Eds.), *Progress in Cryptology - INDOCRYPT 2008 (Proceedings 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008) Vol. 5365. Lecture Notes in Computer Science* (pp. 279-293). Berlin: Springer.

Massacci, F., Zannone, N. (2008) A Model-Driven Approach for the Specification and Analysis of Access Control Policies. In R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems (Proceedings of OTM 2008, OTM 2008 Confederated International Conferences, CoopIS, DOA, GADA, IS, and ODBASE 2008, Monterrey, Mexico, November 9-14, 2008, Part II). Vol. 5332. Lecture Notes in Computer Science (pp 1087–1103). Berlin: Springer.

Mazeika, A., Böhlen, M.H. & Trivellato, D. (2008). Analysis and interpretation of visual hierarchical heavy hitters of binary relations. In P. Atzeni, A. Caplinskas & H. Jaakkola (Eds.), *Advances in Databases and Information Systems (12th East European Conference, ADBIS 2008, Pori, Finland, September 5-9, 2008, Proceedings) Vol. 5207. Lecture Notes in Computer Science* (pp. 168-183). Berlin: Springer.

Morali, A., Zambon, E., Etalle, S. & Overbeek, P.L. (2008). IT confidentiality risk assessment for an architecture-based approach. In C. Bartolini, A. Sahai & J.P. Sauvé (Eds.), *Proceedings 3rd IEEE/IFIP International Workshop on Business-driven IT Management (BDIM 2008, Salvador, Brazil, April 7, 2008)* (pp. 31-40). IEEE.

Naehrig, M., Barreto, P.S.L.M. & Schwabe, P. (2008). On compressible pairings and their computation. In S. Vaudenay (Ed.), *Progress in Cryptology - Africacrypt 2008 (First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008, Proceedings) Vol. 5023. Lecture Notes in Computer Science* (pp. 371-388). Berlin: Springer.

Pan, J., Hartog, J.I. den & Vink, E.P. de (2008). An operation-based metric for CPA resistance. In S. Jajodia, P. Samarati & S. Cimato (Eds.), *Proceedings of the IFIP TC-11 23rd International Information Security Conference (IFIP 20th World Computer Congress, IFIP SEC'08, Milano, Italy, September 7-10, 2008) Vol. 278. IFIP Conference Proceedings* (pp. 429-443). Boston: Springer.

Rezaeian Farashahi, R. (2008). Extractors for Jacobians of binary genus-2 hyperelliptic curves. In Y. Mu, W. Susilo & J. Seberry (Eds.), *Information Security and Privacy (13th Australasian Conference, ACISP 2008, Wollongong, Australia, July 7-9, 2008, Proceedings) Vol. 5107. Lecture Notes in Computer Science* (pp. 447-462). Berlin: Springer.

Smans, J., Jacobs, B.P.F., Piessens, F. & Schulte, W. (2008). An automatic verifier for Java-like programs based on dynamic frames. In J. Fiadeiro & P. Inverardi (Eds.), *Fundamental Approaches to Software Engineering (Proceedings 11th International Conference, FASE 2008, Held as Part of the Joint European Conferences*

on Theory and Practice of Software, ETAPS 2008, Budapest, Hungary, March 29-April 6, 2008) Vol. 4961. Lecture Notes in Computer Science (pp. 261-275). Berlin: Springer.

Boekbespreking

Weger, B.M.M. de (2008). [Bespreking van het boek *Unsolved problems in number theory*]. *Nieuw Archief voor Wiskunde, 5/9*(4), 299-300.

Extern rapport

Bernstein, D.J., Lange, T. & Peters, C.P. (2008). *Attacking and defending the McEliece cryptosystem.* Cryptology ePrint Archive (Ext. rep. 2008/318). -: IACR.

Bernstein, D.J., Chen, T.R., Cheng, C.M., Lange, T. & Yang, B.Y. (2008). *ECM on graphics cards.* Cryptology ePrint Archive (Ext. rep. 2008/480). -: IACR.

Bernstein, D.J., Birkner, P., Lange, T. & Peters, C.P. (2008). *ECM using Edwards curves.* Cryptology ePrint Archive (Ext. rep. 2008/016). -: IACR.

Bernstein, D.J. & Schwabe, P. (2008). *New AES software speed records.* Cryptology ePrint Archive (Ext. rep. 2008/381). -: IACR.

Bernstein, D.J., Birkner, P., Joye, M., Lange, T. & Peters, C.P. (2008). *Twisted Edwards curves.* Cryptology ePrint Archive (Ext. rep. 2008/013). -: IACR.

Bisson, G. & Satoh, T. (2008). *More discriminants with the Brezing-Weng method.* Cryptology ePrint Archive (Ext. rep. 2008/137). -: -.

Bogetoft, P., Christensen, D.L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J.D., Nielsen, J.B., Nielsen, K., Pagter, J., Schwartzbach, M. & Toft, T. (2008). *Multiparty computation goes live.* Cryptology ePrint Archive (Ext. rep. 2008/068). -: IACR.

Castryck, W., Galbraith, S. & Rezaeian Farashahi, R. (2008). *Efficient arithmetic on elliptic curves using a mixed Edwards-Montgomery representation.* Cryptology ePrint Archive (Ext. rep. 2008/218). -: -.

Hitt O'Connor, L., McGuire, G., Naehrig, M. & Streng, M. (2008). *CM construction of genus 2 curves with p-rank 1.* Cryptology ePrint Archive (Ext. rep. 2008/491). -: IACR.

Hoepman, J.H., Hubbers, E., Jacobs, B.P.F., Oostdijk, M.D. & Wichers Schreur, R. (2008). *Crossing borders: Security and privacy issues of the European e-passport.* CoRR (Ext. rep. abs/0801.3930). -: -.

Hoepman, J.H. & Jacobs, B.P.F. (2008). *Increased security through open source.* CoRR (Ext. rep. abs/0801.3924). -: -.

Hubbers, E., Jacobs, B.P.F., Schoenmakers, B., Tilborg, H.C.A. van & Weger, B.M.M. de (2008). *Description and analysis of the RIES internet voting system.* Eindhoven: EIPSI Eindhoven Institute for the Protection of Systems and Information.

Skoric, B., Obi, C., Verbitskiy, E.A. & Schoenmakers, B. (2008). *Sharp lower bounds on the extractable randomness from non-uniform sources.* Cryptology ePrint Archive (Ext. rep. 2008/484). -: IACR.

Website

Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger , *MD5 considered harmful today, Creating a rogue CA certificate*, Dec. 30, 2008, http://www.win.tue.nl/hashclash/rogue-ca/