The Cryptology Group (PNA5)

Ronald Cramer

Thursday, May 12, 2011

Tenured Staff

Established: **June 1, 2004**

Tenured Staff (**3**):

- **Ronald Cramer**
  Founder & group-leader
  Also at *Math Inst, UL*
- **Serge Fehr**
  Tenured since Jan 1, 2009
- **Herman te Riele**
  Retires in December 2011

Other current senior staff (**3**):

- **Krzysztof Pietrzak**
- **Wieb Bosma**
  seconded from KUN
- **Arjen Lenstra**
  external advisor (EPFL)

Current Postdocs (**4**):

- **Nacho Cascudo**
- **Erwin Dassen**
  As of June 2011.
- **Robbert de Haan**
- **Alexander Kruppa**

Current PhD students (**3**):

- **Niek Bouman** (Fehr)
- **Joachim Schipper** (Pietrzak)
- **Marc Stevens** (Cramer)

NOTE:
3 more postdocs and **1** PhD student will be hired, starting in 2011–2012.

Collaboration

Some primary, longstanding research contacts abroad:
(*all are co-authors*)

- (DK) *Aarhus* : Ivan Damgaard, Jesper Nielsen
- (DE) *Bochum* : Eike Kiltz
- (CH) *EPFL* : Arjen Lenstra
- (CH) *ETH Zurich* : Ueli Maurer, Renato Renner
- (DE) *Karlsruhe* : Dennis Hofheinz
- (CA) *McGill* : Louis Salvail
- (US & IL) *MIT & Weizmann Institute*: Shafi Goldwasser
- (SIN) *NTU* : Chaoping Xing, Carles Padró, Alp Bassa
- (US) *NYU* : Victor Shoup
- (IL) *Technion* : Yuval Ishai
- (US) *UCLA*: Rafail Ostrovsky

Industry (*abroad*):
(*all are co-authors*)

- (US) *AT&T Labs*: Juan Garay
- (DK) *Cryptomathic*: Torben Pedersen
- (US) *Google*: Moti Yung
- (US) *IBM TJ Watson*: Tal Rabin
- (US) *NTT (Japan)*: Tatsuaki Okamoto, Masa Abe

Collaboration (national)

Academic:

- CWI*: Harry Buhrman, Christian Schaffner (PNA6, quantum computing)
- UL*: Bas Edixhoven, Hendrik Lenstra
- KUN: Jaap-Henk Hoepman, Erik Verheul
- TU/e: Berry Schoenmakers, Benne de Weger

Industry:

- TNO (NL): Jaap-Henk Hoepman
- Philips Research (NL): Pim Tuyls
- (FOX-IT (NL))

Fundamental and practice-oriented cryptology

Focal areas in the group:

- **Mathematical Cryptography**
  Cramer, Cascudo, Bosma, Dassen, Pietrzak
- **Computational Number Theory**
  te Riele, Kruppa, Bosma, (AK Lenstra)
- **Quantum Information Theory and -Cryptography**
  Fehr, Bouman
- **Complexity-Based Cryptography**
  Cramer, Fehr, Pietrzak, Schipper
- **Cryptanalysis**
  Stevens
- **Applications of Secure Multi-Party Computation**
  Cramer, de Haan

Long Term Goal

Cryptology studies the extent to which
problems pertaining to security in the presence of
malicious adversaries
can be solved by means of data processing,
and, where it applies,
how this can be done efficiently.

Cryptographic Functionalities: Examples

Encryption schemes and **digital signatures**:

- Building blocks for *private and authentic* communication channels (*unilateral security*).
- Instrumental to secure internet transactions and payments, mobile telephony, etc.

Secure computation:

- Enables secure cooperation between *mutually distrusting parties* or *parties with conflicting interests* (*multilateral security*).
- Uses in particular *dedicated cryptographic techniques*.
- Industrial applications on the rise.
  E.g., (micro-) auctions that hide bidding strategy.

Examples of Cryptographic Questions We Ask

- *Reliability* of cryptographic methods in use *today*?
  (E.g., how "computationally intractable" is factoring really?)
- *Strengthening of security possible*? *More efficiency*?
  (E.g., practical chosen ciphertext security)
- *Enhanced Functionality?*
  (E.g., security against side-channel attacks)

Cryptography in the presence of quantum computing:

- *Alternatives* to RSA, Elliptic Curve Crypto?
  (E.g., lattice-based cryptography?)
- Which cryptographic tasks can be performed *information-theoretically secure* and how?
  (E.g., secure multi-party computation)
- *Alternative models* for cryptography?
  (compared to comp. intractability; e.g., bounded storage)

Some Research Highlights 2005–2010

Selection: from each focal area, one main result

(2009) *RSA-768 factorized*.

- Record in integer factorization, using Number Field Sieve.
- Significance exlained later on.

(2008) Invention of *efficient chosen-prefix collision attacks, full cryptanalysis of the MD5 hash-function*.

- Significance explained later on.

(2008) Invention of a *practical crypto-system secure against chosen cipher-text attack under the factoring assumption*.

- Resolved an open question that stood for two decades.

Some Research Highlights 2005–2010

(2008) Invention of *leakage-resilient cryptography*.

- First promising theoretical framework security against side-channel attacks.
- Currently a hot topic.

(2006) *Asymptotic version of the Fundamental Theorem on Information-Theoretically Secure Multi-Party Computation*.

- Discovers a deep link with algebraic geometry.
- Several surprising applications in two-party cryptography.
- Motivates new work on algebraic geometry: *torsion-limits in towers of function fields* (2010).

(2005) Invention of *the "quantum-bounded storage" paradigm*.

- *First ever* application of quantum crypto *beyond key-exchange*: oblivious transfer.

Scientific Reputation (Selection)

EUROCRYPT/CRYPTO Publ. & Best Paper Awards (BPA)

Total: **44**. BPA: **1** CRYPTO ('10), **3** EUROCRYPT ('09, '10, '11)

Honors

1 EUROCRYPT 2011 Invited Speaker

1 Membership De Jonge Akademie (KNAW), 2005-2010

Editorial Boards, Program Committees

1 J. Cryptology, **1** J. Math. Crypt., **1** IEEE Trans. Inf. Theory,
1 EUROCRYPT 2005 PC Chair, **1** PKC 2008 PC Chair
1 FOCS PC, **4** CRYPTO PC, **4** EUROCRYPT PC
1 UCLA IPAM, **2** Dagstuhl, **2** CRM, **3** Lorentz Center

Career Development Awards

1 NWO Vici, **1** ERC Starting Grant,
1 Sofya Kovalevskaya (von Humboldt Foundation), **2** NWO Veni

Other Grants

2 STW Sentinels, **1** NSF (USA), **2** NWO Vrije Competitie,
2 NWO Diamant Math. Cluster

Relevance to Society (Non-Scientific)

- "Number Field Sieve Project" (1990s–):
  sets the world-wide industrial standards for key-length of the RSA-system on the Internet.
- Our MD5 cryptanalysis undermined Internet-security (spoofing of secure websites!!!).

  Result: *worldwide withdrawal of MD5 from the Internet*.
- The Cramer-Shoup encryption scheme is an *ISO-standard*.

Our work was featured in **popular media**, for example

- *NRC Handelsblad* (3 interviews; 2 recent, 1 past)
- *The New York Times* (1 recent, 1 past)
- *De Automatisering Gids* (2 recent)
- (other)

“Spin Outs”

Postdocs:

- 2 tenure-track full professorships.
  Bochum (Math.), Karlsruhe (CS)
- 2 tenure-track associate professorships.
  Barcelona (Math.), Istanbul (Math.)
- 1 NSF-position at *Stanford* (CS).
- 1 postdoc position at Aarhus (CS).
- 1 Israeli *high-tech industry*.

PhD Alumni:

- 1 professorship (Antwerp) & CWI-position.
- 2 CWI PNA5 postdocs.
- 1 Dutch defense industry
  Thales.

Strengths, Threats & Weaknesses

Strengths:

- International impact of our results.
- Visibility, very strong world-wide network.
- Attractive research environment.
- Hiring young talented international researchers.
- Successful with career development awards.
- Strong interplay with (pure) mathematics, (theoretical) computer science, and physics.

Threats and Weaknesses:

- So far, most (but certainly not all!) funding obtained from “one-time” career development awards.
- Political support for funding of foundational research in sharp decline.

Strategy

Strategy:

- *Focus on breaking new ground*, patiently but persistently.
- *Advance through deeper understanding of the links between crypto and mathematics, physics, and cs*.
- *Two-way* scientific interplay:

  great fun plus attracting top researchers from neighboring areas for collaboration on crypto problems, or problems inspired by crypto.

  (e.g., researchers from number theory, algebraic geometry, coding theory, (quantum) information theory)
- *Fish in the top-end of the international post-doc market*.

  Keep them long enough to develop their own program and prepare for professorship (or career development grant.)

Scientific Challenges

Focal areas for the coming period

- **Lattice-based cryptography**
  "post-quantum security"
- **Algebraic function fields and codes, and their applications to cryptography**
- **Leakage resilient cryptography**.
- **Public-key cryptography on low-resource devices**.
- **Practical secure computation**
  Collaboration with CFEM consortium, Denmark
- **Location-based quantum cryptography, applications of quantum bounded storage**
  Collaboration with PNA6, physicists

NOTE: In these emerging areas we are already in the lead, jointly with international collaborators.