Number Theory and Cryptography

Alfred Menezes

University of Waterloo

Outline

- Univ Waterloo research areas:
  - Cryptography, Security and Privacy (CrySP)
  - Symmetric-key cryptography
  - Quantum cryptography
- Univ Calgary & Waterloo research areas:
  - Number-theoretic cryptography
  - Implementation

CrySP

- Cryptography, Security, and Privacy Research Group David R. Cheriton School of Computer Science, University of Waterloo
- Faculty: Ian Goldberg, Urs Hengartner, Doug Stinson
- Research topics include:
  - Distributed cryptographic protocols (key distribution, broadcast encryption, secret sharing,...)
  - Useful security and privacy technologies (Off-The-Record messaging, Tor, private information retrieval,...)
  - Security and privacy in emerging computing environments (pervasive computing, location-based services, vehicular networks, RFIDs, ...)

Symmetric-key cryptography

- Faculty: Guang Gong
- Research topics include:
  - Constructions of Boolean function (high nonlinearity, algebraic immunity, bent functions,...)
  - Design and analysis of stream ciphers
  - Sequence design for wireless CDMA communications
- Research ties with Nicolas Sendrier, Claude Carlet, Pascale Charpin, Anne Canteaut

Quantum cryptography

- Institute for Quantum Computing (IQC), U Waterloo
- Faculty: Daniel Gottesman, Debbie Leung, Norbert Lütkenhaus, Michele Mosca, John Watrous, Richard Cleve
- Research topics include:
  - Quantum cryptographic protocols (key distribution, interactive proof systems and zero-knowledge, multi-party computation,...)
  - Experimenting with quantum key distribution (free-space optical link)

Number-theoretic cryptography

- Calgary faculty: Mark Bauer, Michael Jacobson, Renate Scheidler, Hugh Williams
- Waterloo faculty: David Jao, Alfred Menezes, Edlyn Teske, Scott Vanstone
- Ottawa faculty: Isabelle Déchène
- Toronto faculty: Kumar Murty

Elliptic curve cryptography

- Discrete-log cryptography using the group of points on an elliptic curve $E : Y^2 = X^3 + aX + b$ defined over a finite field $\mathbb{F}_q$.
- The order of the group is $\approx q$.
- First proposed by Koblitz and Miller in 1985.
- For a well-chosen elliptic curve, the best attack on the discrete logarithm problem is Pollard's rho method, which takes $\approx q^{1/2}$ steps.
- Security for ECC scales nicely:
  - 160-bit ECC versus 1024-bit RSA
  - 256-bit ECC versus 3072-bit RSA
  - 384-bit ECC versus 7680-bit RSA
  - 512-bit ECC versus 15360-bit RSA
- ECC has been widely standardized and deployed

Hyperelliptic curve cryptography

- Discrete-log cryptography using the divisor class group of a genus-g hyperelliptic curve $C : Y^2 = X^{2g+1} + \cdots$ defined over a finite field $\mathbb{F}_q$.
- The order of the group is $\approx q^g$.
- First proposed by Koblitz in 1989.
- Pollard's rho method for computing discrete logs has running time $\approx q^{g/2}$.
- Potential advantage over elliptic curve systems:
  - Use a smaller field $\mathbb{F}_q$ for the same level of security.

Hyperelliptic curve discrete logs

- (1994; Adleman, DeMarrais and Huang): Subexponential-time algorithm for large genus.
- (2000; Gaudry): $O(q^2)$ for small $g \geq 5$.
- (2000; Harley): $O(q^{2-2/(g+1)})$ for small $g \geq 4$.
- (2003; Thériault): $O(q^{2-2/(g+0.5)})$ for small $g \geq 3$.
- (2005; Diem, Gaudry, Thomé, Thériault): $O(q^{2-2/g})$ for small $g \geq 3$.
- (2005; Diem) $O(q)$ for genus-3 non-hyperelliptic curves.
- (2007; Smith) $O(q)$ for 18.75% of genus-3 hyperelliptic curves.
- Still untouched: $g = 1$ and $g = 2$.

Pairing-based cryptography

- Use bilinear pairings from low-embedding degree elliptic and hyperelliptic curves to design cryptographic protocols
- Joux (2000) and Boneh-Franklin (2001)
- Lots of practical questions remain:
  - Real benefits of identity-based encryption?
  - Other applications (identity-based signatures, aggregate signatures, group signatures,...)
  - Optimal parameters and implementation?
  - Security?

Some ongoing projects

- Implementation of Weil descent attacks for the DLP in elliptic curves over $\mathbb{F}_{2^m}$ (m composite)
- Analysis of the effectiveness of Weil descent attack for the DLP in elliptic curves over optimal extension fields (OEFs) $\mathbb{F}_{p^m}$
- Rigorous and tighter bounds for computing isogenies between families of random elliptic curves (and designing signature schemes)
- Security of individual Diffie-Hellman bits over families of isogenous elliptic curves
- Analysis of methods for generating pairing-friendly elliptic curves

Algebraic number fields

- Development and implementation of algorithms for computing invariants of number fields and function fields
  - Fast arithmetic in the class group, regulator computation, discrete log computation, ...
- Cryptographic protocols using real and imaginary quadratic fields
- Cubic function fields
- Experiments on a cluster of 152 Dual Intel P4 2.4/2.8 GHz processors

Efficient implementation

- Faculty: Vassil Dimitrov (Calgary), Anwar Hasan (Waterloo), Alfred Menezes (Waterloo) Ali Miri (Ottawa)
- Research topics include:
  - Finite field arithmetic
  - Scalar multiplication
  - Edwards coordinates (Bernstein/Lange) and Theta functions (Gaudry)
  - Pairings
  - Protocol arithmetic
  - Fault-tolerant hardware design
- Existing research ties with Jean-Claude Bajard, Arnauld Tisserand, Laurent Imbert, Christopher Negre

Side-channel attacks

- Faculty: Catherine Gebotys
- Experimental testbed for electromagnetic (EM) and power-analysis attacks on embedded systems