

A Cryptographer's Laundry List

Kristin Lauter
Microsoft Research

SAGE conference
February 4, 2006

Motivations:

- Crypto implementations
- Crypto research
- New algorithms
- Related math research

Cryptographic functionality to enable

- Stream and block ciphers
- Hash functions
- Random number generators
- Public key:
 - Encryption
 - Key exchange/AKE
 - Digital signatures/authentication
 - certificates
 - Identity-based encryption

Cryptographic Standards

- IEEE P1363 (Elliptic curve crypto)
- IETF groups for TLS, IPSec, SMIME
- ANSI X9.82 (RNG), X9.62 ECDH, X9.63 ECDSA, X509 (certificates)
- NIST SP 800-56 (AKE), SP 800-90 (RNG), FIPS
- European, Japanese, Wireless consortiums ...

Mathematical functionality

- Modular arithmetic modulo p ,
 $160 < \log(p) < 16,000$
- Finite field extensions
 - Small ($k=6, 10, \dots$ pairing-based)
 - Medium ($k=163, 1024 \dots$ binary fields)
 - Large (torsion points)
- Linear Algebra
- Matrix groups ($\text{PSL}(2, F_p)$)

Mathematical functionality (cont.)

- Elliptic curves
 - Arithmetic, “exponentiation”
 - Division polynomials
 - Point-counting
 - Complex multiplication techniques
- Pairings (Weil, Tate)
- Lattices, class groups, ...

Known protocols

- Hash functions: SHA family, block, stream ciphers, MD5, RC4, VSH
- RNG: RSA, ...
- ElGamal, RSA, Diffie-Hellman, DSA
- ECDH, ECDSA, MQV, NAXOS
- IBE, pairing-based signatures, ...

New protocols/directions

- Hash functions and RNGs from expander graphs
- Elliptic curves
 - Isogenies, maximal orders in quaternion algebras, CRT, p-adics
- Jacobians of genus 2 curves
 - Arithmetic, CM method, point counting, CRT method, p-adic methods, pairing

Jacobians of genus 2 curves

- Arithmetic (Cantor)
- Pairings (Tate)
- CM algorithm (Spallek, Weng, L-Cohn)
- Generating torsion (Cantor, vW, Groebner bases, resultants)
- Point counting (Gaudry, Kedlaya, Lauder,...)
- Computing endomorphism rings (joint with Eisentraeger)

New applications of Ramanujan graphs (joint work with Charles-Goren)

- Cryptographic hash functions from Pizer or LPS graphs
 - Output is the endpoint of a walk determined by the input
 - Proposed at NIST Halloween Hash Bash
- PseudoRandomBitGenerator
 - Output is bits from a walk determined by an input seed
 - Proposed to NIST SP 800-90 PRBGs

Pizer Ramanujan Graph of supersingular elliptic curves “mod p ”

- Roughly $p/12$ vertices
- Edges are isogenies of degree l , l a small prime different from p
- Vertices are labeled by j -invariants
- Collision resistance and bit unpredictability follows from hardness of finding isogenies between 2 given elliptic curves

Computation of Isogenies

- Velu's formulae (in Magma)
- Can compute modular polynomials (joint work with Charles)
- Need to compute extension fields where torsion is defined
- Can label vertices with bases for maximal orders in quaternion algebras

Related mathematics

- Computation of modular forms
(Brandt matrices, Kohel, MAGMA)
- Dimension 2 generalizations: (CGL) superspecial abelian varieties
- Computing Hilbert modular forms
(Nicole, Dembele, ...)
- Generating S -units (DeShalit-Goren, Goren-L)
- Shafarevich-Tate group, pairing
(Eisentraeger-Jetchev-L)

Pairing-based signatures

- Network coding applications (joint with Charles, Jain)
- Detect pollution attacks on P2P content distribution
- Linear combinations of packets are signed and distributed, recombined at each node, homomorphic signature needed to resign outgoing

Crypto research

- Factoring
- Discrete logarithm problem
- Index calculus methods
- Number field sieve methods
- Primality proving
- Point-counting