An Introduction to Post-Quantum Cryptography

Christiane Peters

Technische Universiteit Eindhoven

CrossFyre
Darmstadt

April 14, 2011

Code-based Cryptography

Christiane Peters

Technische Universiteit Eindhoven

CrossFyre
Darmstadt

April 14, 2011

Bad news

Quantum computers will break the most popular public-key cryptosystems:

- RSA,
- DSA,
- ECDSA,
- ECC,
- HECC
- ...

can be attacked in polynomial time using Shor's algorithm.

Good news

Post-quantum cryptography deals with cryptosystems that

- run on conventional computers and
- are secure against attacks by quantum computers.

Examples:

- Hash-based cryptography.
- Code-based cryptography.
- Lattice-based cryptography.
- Multivariate-quadratic-equations cryptography.

Overview:
Bernstein, Buchmann, and Dahmen, eds., Post-Quantum Cryptography. Springer, 2009.

1. Code-based cryptography

2. Wild McEliece

Linear codes

- A linear code C of length n and dimension k is a k-dimensional subspace of $\mathbf{F}_q^n$.

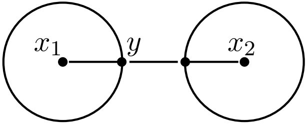
- A generator matrix for C is a $k \times n$ matrix G such that

$$C = \left\{ m\,G : m \in \mathbf{F}_q^k \right\}.$$

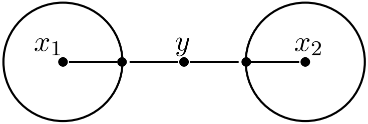
- The matrix G corresponds to a map $\mathbf{F}_q^k \to \mathbf{F}_q^n$ sending a message m of length k to an n-bit string.

Hamming distance

- The Hamming distance between two words in $\mathbf{F}_q^n$ is the number of coordinates where they differ.
- The Hamming weight of a word is the number of non-zero coordinates.
- The minimum distance of a linear code C is the smallest Hamming weight of a non-zero codeword in C.



code with minimum distance 3



code with minimum distance 4

Decoding problem

Classical decoding problem: find the closest codeword $c \in C$ to a given $y \in \mathbf{F}_q^n$, assuming that there is a unique closest codeword.

There are lots of code families with fast decoding algorithms

- E.g., Goppa codes/alternant codes, Reed-Solomon codes, Gabidulin codes, Reed-Muller codes, Algebraic-geometric codes, BCH codes etc.

However, given a linear code with no obvious structure.

Berlekamp, McEliece, van Tilborg (1978) showed that the general decoding problem for binary linear codes is NP-complete.

- About $2^{(0.5+o(1))n/\log_2(n)}$ binary operations required for a code of length n and dimension $\approx 0.5n$.

Goppa codes

- Fix a prime power q; a positive integer m, a positive integer $n \leq q^m$; an integer $t < \frac{n}{m}$; distinct $a_1, \ldots, a_n \in \mathbf{F}_{q^m}$;
- and a polynomial $g(x)$ in $\mathbf{F}_{q^m}[x]$ of degree t such that $g(a_i) \neq 0$ for all i.

The Goppa code $\Gamma_q(a_1, \ldots, a_n, g)$ consists of all words $c = (c_1, \ldots, c_n)$ in $\mathbf{F}_q^n$ with

$$\sum_{i=1}^{n} \frac{c_i}{x - a_i} \equiv 0 \pmod{g(x)}$$

- $\Gamma_q(a_1, \ldots, a_n, g)$ has length n and dimension $k \geq n - mt$.
- The minimum distance is at least $\deg g + 1 = t + 1$ (in the binary case $2t + 1$).
- Patterson decoding efficiently decodes t errors in the binary case; otherwise only $t/2$ errors can be corrected.

The McEliece cryptosystem

- Given public system parameters n, k, w.
- The public key is a random-looking $k \times n$ matrix $\hat{G}$ with entries in $\mathbf{F}_q$.
- Encrypt a message $m \in \mathbf{F}_q^k$ as

$$m\hat{G} + e$$

  where $e \in \mathbf{F}_q^n$ is a random error vector of weight w.
- Need to correct w errors to find m.
- Decoding is not easy without knowing the structure of the code generated by $\hat{G}$.

Secret key

The public key $\hat{G}$ has a hidden Goppa-code structure allowing fast decoding:

$$\hat{G} = SGP$$

where

- G is the generator matrix of a Goppa code Γ of length n and dimension k and error-correcting capability w; McEliece's proposal uses Goppa codes over $\mathbf{F}_2$;
- S is a random $k \times k$ invertible matrix; and
- P is a random $n \times n$ permutation matrix.

The triple (G, S, P) forms the secret key.

Note: Detecting this structure, i.e., finding G given $\hat{G}$, seems even more difficult than attacking a random $\hat{G}$.

Decryption

The legitimate receiver knows S, G and P with $\hat{G} = SGP$ and a decoding algorithm for Γ.

How to decrypt $y = m\hat{G} + e$.

1. Compute $yP^{-1} = mSG + eP^{-1}$.
2. Apply the decoding algorithm of Γ to find mSG which is a codeword in Γ from which one obtains m.

Attacks

Bernstein, Lange, P., PQCrypto 2008:

- Break of McEliece's original setup: a binary code of length 1024, dimension 524 and 50 added errors.

- Suggestion: for 128-bit security of the McEliece cryptosystem take a length-2960, dimension-2288 classical binary Goppa code ($t = 56$), with 57 errors added by the sender.

- The public-key size here is 1537536 bits.

Reduce key size

- Smaller-key variants use other codes such as Reed-Solomon codes, generalized Reed-Solomon codes, quasi-cyclic codes, quasi-dyadic codes or geometric Goppa codes.

- Beware: several variants allowed structural attacks.

Using larger fields

- Classical Goppa codes are the most confidence-inspiring choice.

- Using Goppa codes over larger fields decreases the key size at the same security level against information-set decoding (P., PQCrypto 2010).

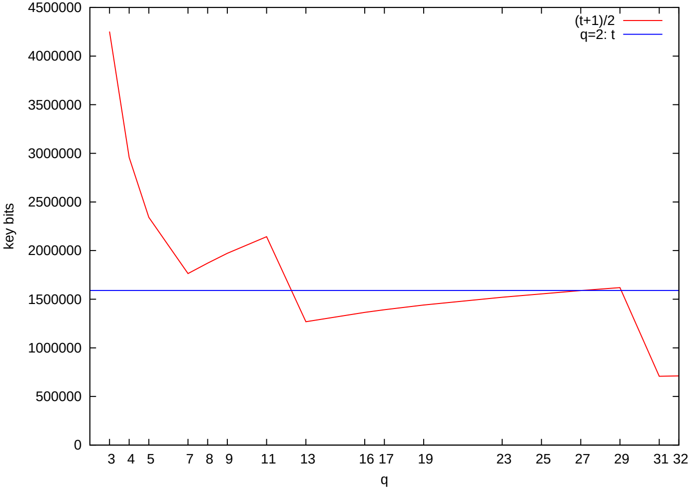
- A Goppa code over $\mathbf{F}_{31}$ leads to a 725741-bit key for 128-bit security.

- Drawback: can correct only $t/2$ errors if $q > 2$ (vs. t in the binary case).

- However, Goppa codes over smaller fields such as $\mathbf{F}_3$ are not competitive in key size with codes over $\mathbf{F}_2$.

Key sizes for various q at a 128-bit security level

McEliece with $\Gamma_q(a_1, \ldots, a_n, g)$ with an alternant decoder.



1. Code-based cryptography

2. Wild McEliece

Proposal

Bernstein, Lange, P. (SAC 2011) + tweak from 2011: Use the McEliece cryptosystem with Goppa codes of the form

$$\Gamma_q(a_1, \ldots, a_n, fg^{q-1})$$

where f and g are coprime squarefree monic polynomials in $\mathbf{F}_{q^m}[x]$.

- Note the exponent $q-1$ in g^{q-1}.
- We refer to these codes as wild Goppa codes.
- Polynomial f is a correction factor; choose f so that the number of polynomials fg^{q-1} becomes too large to search.

Minimum distance of wild Goppa codes

Theorem

$$\Gamma_q(a_1, \ldots, a_n, fg^{q-1}) = \Gamma_q(a_1, \ldots, a_n, fg^q)$$

where f is a squarefree monic polynomial in $\mathbf{F}_{q^m}[x]$ of degree s and g a squarefree monic polynomial in $\mathbf{F}_{q^m}[x]$ of degree t; f and g coprime.

- Generalized version of a proof of theorem by Sugiyama-Kasahara-Hirasawa-Namekawa, 1976.
- Our paper contains a streamlined proof.
- The case $q = 2$ and $f = 1$ of this theorem is due to Goppa, using a different proof that can be found in many textbooks.

Error-correcting capability

- Since $\Gamma_q(\dots, fg^{q-1}) = \Gamma_q(\dots, fg^q)$ the minimum distance of $\Gamma_q(\dots, fg^{q-1})$ equals the one of $\Gamma_q(\dots, fg^q)$ and is thus $\geq \deg fg^q + 1 = s + qt + 1$.

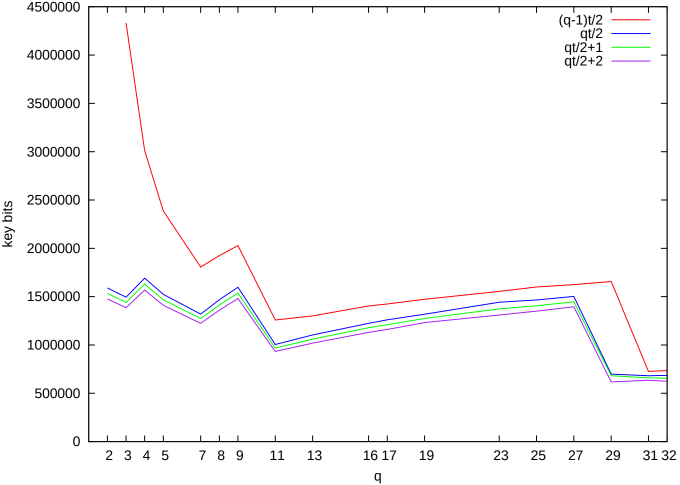
- Can use an alternant decoder that allows efficient correction of $\lfloor (s + qt)/2 \rfloor$ errors for $\Gamma_q(\dots, fg^{q-1})$.

- In fact, can use any Reed-Solomon decoder for Wild Goppa codes.

- In particular, can use list decoding methods such as the Guruswami-Sudan decoder to correct beyond half the minimum distance.

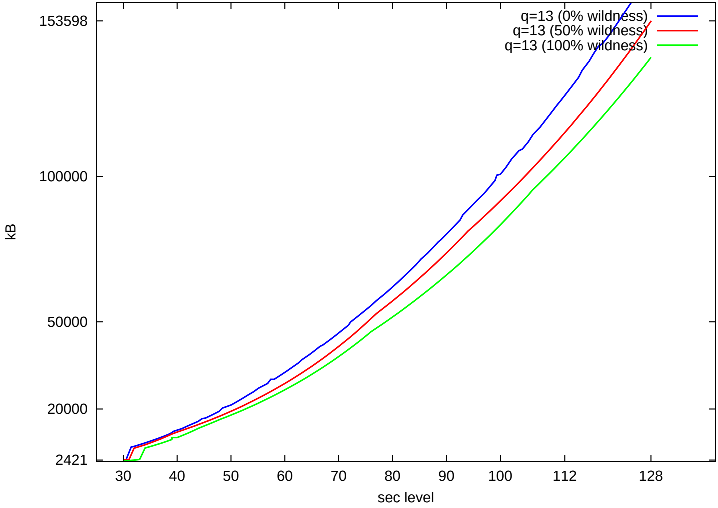
Key sizes for various q at a 128-bit security level

McEliece with $\Gamma_q(a_1, \ldots, a_n, g^{q-1})$ and $\lfloor (q-1)t/2 \rfloor$, $\lfloor qt/2 \rfloor$, $\lfloor qt/2 \rfloor + 1$, or $\lfloor qt/2 \rfloor + 2$ added errors (here $f = 1$).



Key sizes for $q = 13$ for various security levels

McEliece with $\Gamma_q(a_1, \ldots, a_n, fg^{q-1})$ and $\lfloor (s + qt)/2 \rfloor$ added errors.



Code-based Cryptography Workshop

May 11–12, Eindhoven, The Netherlands

`http://www.win.tue.nl/cccc/cbc`

PQCrypto 2011

Nov 29 – Dec 2, Taipei

`http://pq.crypto.tw/pqc11/`

Thank you for your attention!