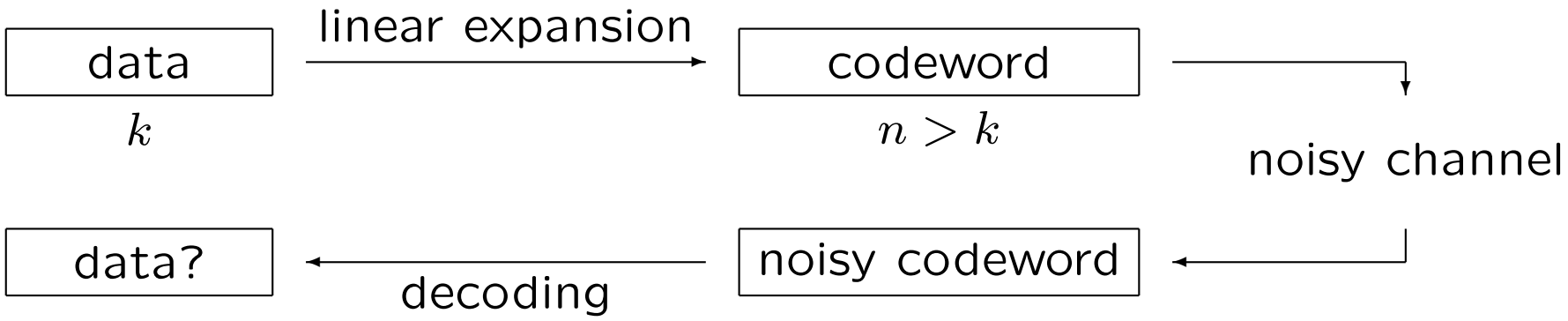
Quantum Safe Cryptography from Codes: Present and Future

16th IMA International Conference on Cryptography and Coding

Oxford, December 13, 2017

Nicolas Sendrier

Linear Codes for Telecommunication



[Shannon, 1948]

For any rate $R = k/n$, one can correct up to τn errors
($\tau = h^{-1}(1 - R)$, $\tau = 0.11$ if $R = 0.5$, binary case)

Non constructive $\longrightarrow$ no poly-time algorithm for decoding in general

Decoding – Easy or Hard?

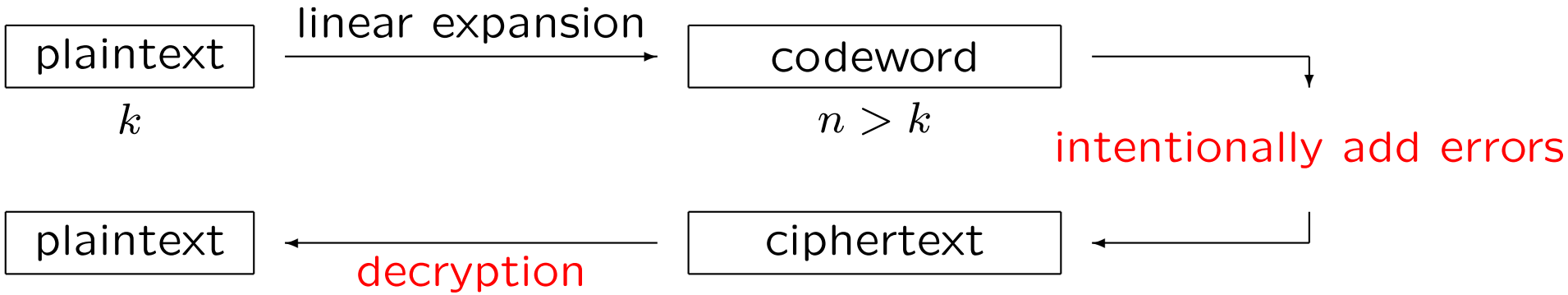
Some "good" codes exist:

- some classes of codes have a poly-time decoders for $\Theta(n)$ errors (algebraic geometry, expander graphs, concatenation, ...),
- alternant codes have a poly-time decoders for $\Theta\left(\frac{n}{\log n}\right)$ errors.

But, in general:

- decoding is NP-hard [Berlekamp, McEliece & van Tilborg, 78],
- believed to be hard on average [Alekhnovich, 2003].

Linear Codes for Cryptography



By choosing a "good" code:

- the legitimate user has access to a poly-time decoder,
- for anyone else the code should look random.

Outline

I. Code-based Cryptography

II. QC-MDPC McEliece

III. Digital Signature

I. Code-based Cryptography

Motivation – Quantum Safe Cryptography

- Quantum computing and Shor's algorithm will render obsolete many essential cryptographic primitives

- This will happen in a decade or more, but [Mosca, 13] adding the *migration time* and the *required lifetime of your secrets*, we should realize *it is time to worry*.

  $\rightarrow$ NIST call for standardization of quantum safe primitives (also ETSI, NSA, . . .)

- Attacks speedup against code-based schemes is "only" quadratic (Grover search)

  $\rightarrow$ increasing parameters should be enough

McEliece in a Nutshell

Let $\mathcal{F}$ be a family of t-error correcting q-ary linear $[n, k]$ codes

Key generation:	pick $\mathcal{C} \in \mathcal{F}$
	public: G a generator matrix
	private: Φ a (fast) t-bounded decoder
Encryption:	$x \mapsto xG + e$ with e random of weight t
Decryption:	$y \mapsto \Phi(y)$

[McEliece, 78]: $\mathcal{F}$ the family of binary irreducible Goppa codes

[Niederreiter, 86]: proposed a dual variant, with equivalent security

Security Reduction

For given code length n, code dimension k, and error weight t
Let $\mathcal{G} \subset \{0,1\}^{k \times n}$ denote the set of all public keys

If we assume that

1. decoding t errors in a random $[n,k]$ code is hard on average
2. elements of $\mathcal{G}$ cannot be efficiently distinguished from random $k \times n$ matrices

then McEliece's scheme (with public keys in $\mathcal{G}$) is secure "on average"

+ a semantically secure conversion $\rightarrow$ stronger security level
(note that those conversions allow systematic matrices)

Hardness of Decoding

[Berlekamp, McEliece & van Tilborg, 78]

Syndrome Decoding (SD) NP-complete

Instance: $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, t integer

Question: Is there $e \in \{0,1\}^n$ such that $|e| \leq t$ and $eH^T = s$?

Conjectured difficult on average for $t = n^\varepsilon$ errors and for any $\varepsilon > 0$ [Alekhnovich, 2003]. ($\varepsilon = 1/2$ will be of particular interest)

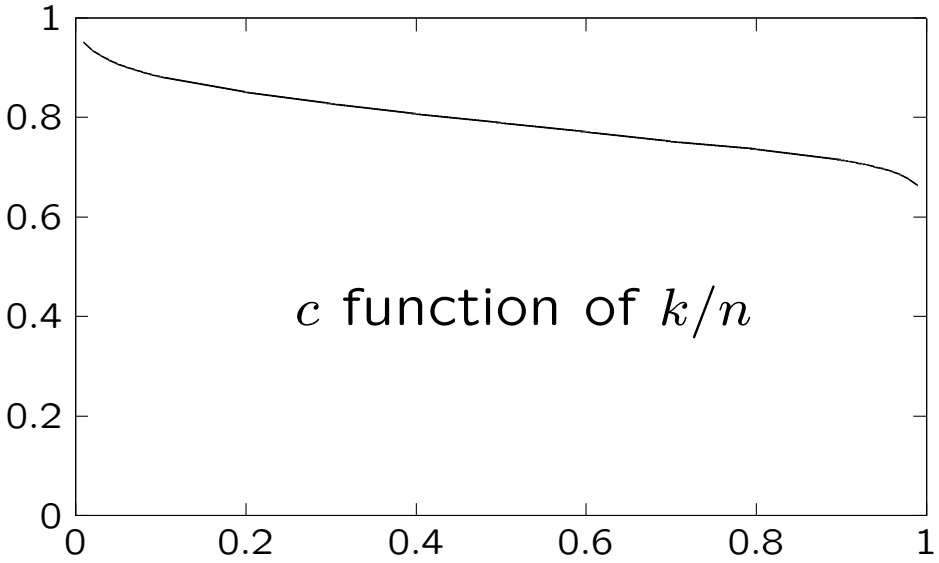
Best solvers run in time $2^{c\alpha t}$ with $\alpha \approx \log_2\left(\frac{n}{n-k}\right)$ and $c \leq 1$

- when $t = o(n)$, we have $c = 1$ for all known variants of ISD, [Canto-Torres & Sendrier, 16]
- when $t = \Theta(n)$, best c is between 0.7 and 0.9 (varies with R), [many works over several decades . . .]
- against a quantum adversary, exponent divided by 2 at most [Bernstein, 09], [Kachigar & Tillich, 17]

Information Set Decoding Asymptotics

Let $\tau = \frac{t}{n}$, $\tau' = \frac{t}{n-k}$, and $\alpha = \frac{h(\tau)}{\tau} - \frac{h(\tau')}{\tau'} \approx \log_2 \frac{n}{n-k}$

($h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ the binary entropy function)



workfactor $= 2^{c\alpha t}$

($c = 1$ [Prange, 62])

($c = 1$ when $t = o(n)$)

Here, exponent for ISD variant by [May & Ozerov, 15] for $\tau = h^{-1}(1 - k/n)$ (GV bound)

Against a quantum adversary $c \leq 0.5$ [Bernstein, 09]

Difficult to always divide c by 2 [Kachigar & Tillich, 17]

Produced with CaWoF [Canto-Torres, 16] `https://gforge.inria.fr/projects/cawof/`

ISD – Credits

- Information Set Decoding: [Prange, 62]
- Relax the weight profile: [Lee & Brickell, 88]
- Compute sums on partial columns first: [Leon, 88]
- Use the birthday paradox: [Stern, 89], [Dumer, 91]
- First "real" implementation: [Canteaut & Chabaud, 98]
- Initial McEliece parameters broken: [Bernstein, Lange, & Peters, 08]
- Lower bounds: [Finiasz & Sendrier, 09]
- Ball-collision decoding [Bernstein, Lange, & Peters, 11]
- Asymptotic exponent improved [May, Meurer, & Thomae, 11]
- Decoding one out of many [Sendrier, 11]
- Even better asymptotic exponent [Becker, Joux, May, & Meurer, 12]
- "Nearest Neighbor" variant [May & Ozerov, 15]
- Sublinear error weight [Canto Torres & Sendrier, 16]
- Improved "Nearest Neighbor" [Both & May, 17]

Key Security

There are some bad choices for McEliece's code family

- Generalized Reed-Solomon codes [Sidelnikov & Shestakov 1992]
- Concatenated codes, Turbo-codes, LDPC codes, Polar codes

Often, the structure that allows decoding can be used to attack.

Fortunately, there are also some good choices

- binary Goppa codes are believed to be pseudorandom
- alternant codes (strict subfield subcodes)
- ...

$\rightarrow$ not as much confidence as for hardness of decoding

McEliece in Practice

[McEliece, 1978]
"A public-key cryptosystem based on algebraic coding theory"

The private code family consisted of irreducible binary Goppa codes of length 1024, dimension 524, and correcting up to 50 errors

- public key size: 262 kilobits (in systematic form)
- cleartext size: 524 bits
- ciphertext size: 1024 bits

A bit undersized today (attacked in [Bernstein, Lange, & Peters, 08] with $\approx 2^{60}$ CPU cycles – Security estimate 2^{52})

For secure parameters, key size is of order

- 2 megabits for a security equivalent to AES 128
- 10 megabits for a security equivalent to AES 256

Code-Based Cryptography – Issues

(i) Key size

Use cyclicity or dyadicity to (safely) reduce the key size

(ii) Proofs

Better indistinguishability assumptions

(iii) Digital signature

Design digital signatures, preferably of *hash-and-sign* type

Advertisement:
BIKE (a KEM proposed to NIST) addresses the first two issues

Compact Keys

The public key is formed of $p \times p$ circulant blocks, for instance:

$$G = \left(\begin{array}{c|c} \begin{array}{cc} 1 & \\ & \ddots \\ & 1 \end{array} & \boxed{g} \circlearrowright \end{array}\right)$$

$$G = \left(\begin{array}{ccc|c} \begin{array}{cc} 1 & \\ & \ddots \\ & 1 \end{array} & & & \boxed{g_{0,0}} \circlearrowright \\ \hline & \begin{array}{cc} 1 & \\ & \ddots \\ & 1 \end{array} & & \boxed{g_{1,0}} \circlearrowright \end{array} \begin{array}{c} \boxed{g_{0,1}} \circlearrowright \\ \hline \boxed{g_{1,1}} \circlearrowright \end{array} \begin{array}{c} \boxed{g_{0,2}} \circlearrowright \\ \hline \boxed{g_{1,2}} \circlearrowright \end{array}\right)$$

Advantage: much smaller key size

Difficulty: hide the code structure (*i.e.* the private decoder)

$\rightarrow$ Quasi-Cyclic (QC) codes of order p and index n/p

QC Security Reduction

For given code length n, code dimension k, and error weight t
Let $\mathcal{G} \subset \{0,1\}^{k \times n}$ denote the set of all public keys
($\mathcal{G}$ is a set of block-circulant matrices)

If we assume that

1. decoding t errors in a random $[n,k]$ *QC* code is hard on average
2. elements of $\mathcal{G}$ cannot be efficiently distinguished from random $k \times n$ *block-circulant* matrices

then McEliece's scheme (with public keys in $\mathcal{G}$) is secure "on average"

Quasi-Cyclic Instances of McEliece's Scheme

- Goppa (or alternant) codes, initiated by [Gaborit, 05]

  Too much algebraic structure, some attempts have failed, to be used with care [Faugère, Otmani, Perret, & Tillich, 10]

- "Disguised" LDPC (Low Density Parity Check) codes [Baldi & Chiaraluce, 07]

  Less structure but still no convincing security reduction

- MDPC (Moderate Density Parity Check) codes [Misoczki, Tillich, Sendrier, & Barreto, 13]

  Even less structure, a security reduction

[Misoczki & Barreto, 09]
Also possible with dyadic blocks instead of circulant blocks

II. QC-MDPC McEliece

MDPC codes

Binary linear codes which admit a sparse parity check matrices can be efficiently decoded [Gallager, 1963] (iterative decoder)

Low Density Parity Check (LDPC) codes of length n:

- constant row weight w (typically 6 to 10)
- correct errors of weight $t = \Theta(n)$

[Misoczki, Tillich, Sendrier, & Barreto, 13]
Moderate Density Parity Check (MDPC) codes of length n:

- row weight $w = \Theta(\sqrt{n})$
- correct errors of weight $t = \Theta(\sqrt{n})$

QC-MDPC-McEliece Key Generation

Parameters (for index 2): p, w, t
p prime, w even, $w/2$ odd, $w = \Theta\left(\sqrt{p}\right)$, $t = \Theta\left(\sqrt{p}\right)$
(*e.g.* $p = 10163$, $w = 142$, $t = 134$ for 128 bits of security)

Pick a two sparse vectors h_0, h_1 in $\{0,1\}^p$ both of weight $w/2$

$$H_{\text{private}} = \quad \boxed{h_0 \quad h_1}$$

Publish a systematic generator matrix of $\mathcal{C} = \langle H_{\text{private}} \rangle^{\perp}$

$$G_{\text{public}} = \quad \boxed{\begin{array}{|c|c|} \hline g & 1 \\ \hline & \searrow \\ & 1 \\ \hline \end{array}}$$

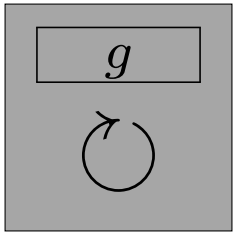
The vector g easily derives from h_0 and h_1.

Circulant Matrices as Polynomial Ring

Let $\mathcal{R} = \mathbf{F}_2[x]/(x^p - 1)$ denote the ring of polynomials modulo $x^p - 1$

$\mathcal{R}$ is isomorphic as a ring to the set of $p \times p$ circulant matrices

For any $g = (g_0, g_1, \ldots, g_{p-1}) \in \{0,1\}^p$



$$\longleftrightarrow \quad g(x) = g_0 + g_1 x + \cdots + g_{p-1} x^{p-1}$$

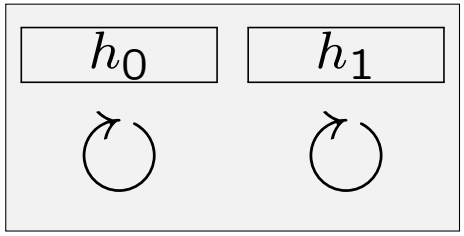
addition, multiplication, inversion are the same in both rings

matrix transposition corresponds to $g(x) \mapsto g^\top(x) = x^p g(x^{-1})$

QC-MDPC (private) Decoding

Index 2 QC-codes, $n = 2p$, $k = p$, row weight w, error weight t

Let $\mathcal{R} = \mathbf{F}_2[x]/(x^p - 1)$

Decode in the code of parity check matrix $H =$ 

$$\begin{cases} \text{Given } s, h_0, h_1 \in \mathcal{R} \text{ with } |h_0| = |h_1| = w/2 \\ \text{Find } e_0, e_1 \in \mathcal{R} \text{ such that } e_0 h_0 + e_1 h_1 = s \text{ and } |e_0| + |e_1| \leq t \end{cases}$$

Gallager's iterative decoders solve this problem efficiently with high probability when $w = \Theta\left(\sqrt{p}\right)$ and $t = \Theta\left(\sqrt{p}\right)$

QC-MDPC-McEliece Scheme

Parameters (index 2): $n = 2p$, $k = p$, w, t, $\mathcal{R} = \mathbf{F}_2[x]/(x^p - 1)$
p prime, w even, $w/2$ odd, $w = \Theta(\sqrt{n})$, $t = \Theta(\sqrt{n})$

Key generation: pick $h_0, h_1 \in \mathcal{R}$ both of weight $w/2$

public: $h = h_1 h_0^{-1}$

private: h_0, h_1

Encryption: given $m \in \mathcal{R}$,

$$m \mapsto (mh + e_0, m + e_1) \text{ with } |e_0| + |e_1| = t$$

Decryption: given $(c_0, c_1) \in \mathcal{R}^2$,

solve $c_0 h_0 + c_1 h_1 = e_0 h_0 + e_1 h_1$ with $|e_0| + |e_1| \leq t$

QC-MDPC-Niederreiter Scheme

Parameters (index 2): $n = 2p$, $k = p$, w, t, $\mathcal{R} = \mathbf{F}_2[x]/(x^p - 1)$
p prime, w even, $w/2$ odd, $w = \Theta(\sqrt{n})$, $t = \Theta(\sqrt{n})$

Key generation: pick $h_0, h_1 \in \mathcal{R}$ both of weight $w/2$

public: $h = h_1 h_0^{-1}$

private: h_0, h_1

Encryption: given $(e_0, e_1) \in \mathcal{R}^2$ with $|e_0| + |e_1| = t$,

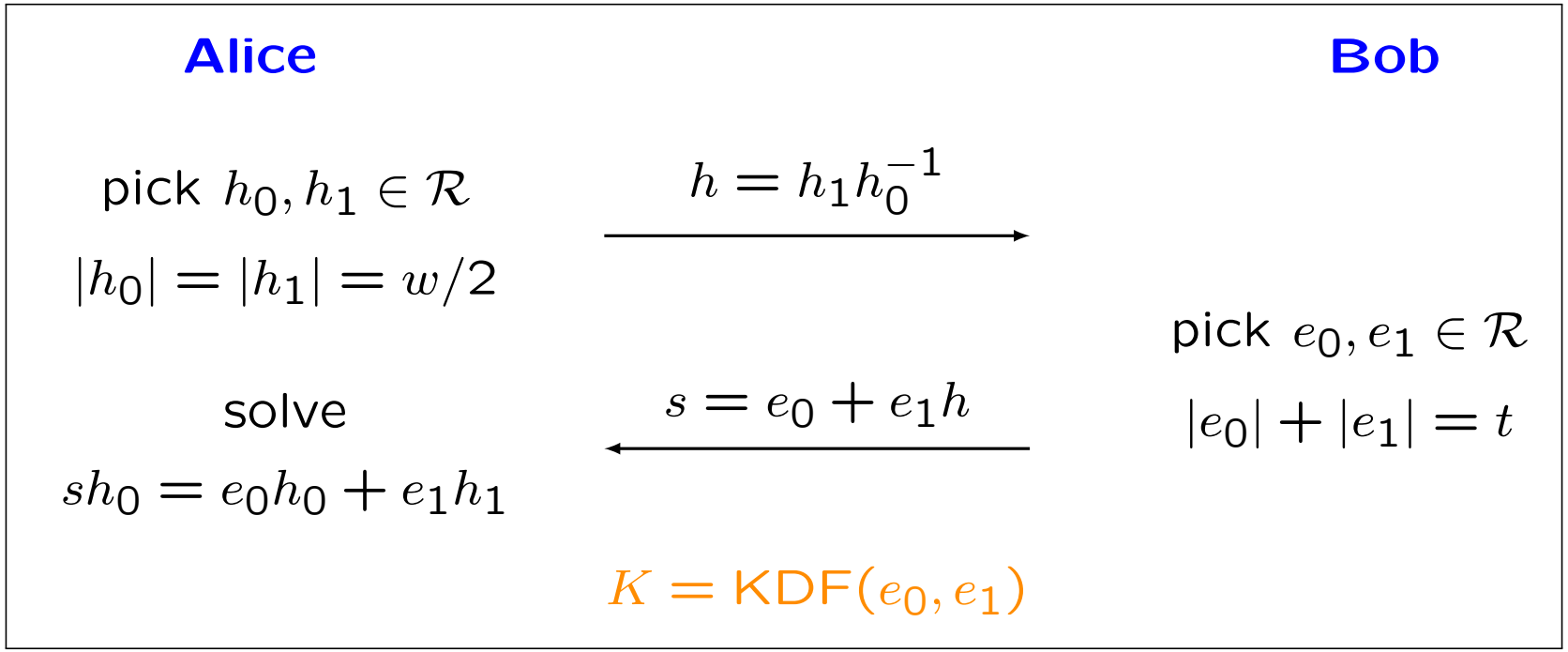
$$(e_0, e_1) \mapsto e_0 + e_1 h$$

Decryption: given $c \in \mathcal{R}$,

solve $ch_0 = e_0 h_0 + e_1 h_1$ with $|e_0| + |e_1| \leq t$

Key Encapsulation Mechanism

Block size p, row weight w, error weight t, $\mathcal{R} = \mathbf{F}_2[x]/(x^p - 1)$
(p a prime, w even, $w/2$ odd, w and t are close to $\sqrt{2p}$)

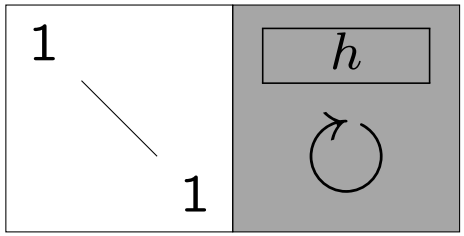


Ephemeral key pairs $\Rightarrow$ forward secrecy

The above is also known as BIKE-2 (second of three BIKE models)

Security Reduction

Let $\mathcal{R} = \mathbf{F}_2[x]/(x^p - 1)$

$H =$ 

Problem 1. **(2,1)-QC Syndrome Decoding**

Instance: $h \in \mathcal{R}$, $s \in \mathcal{R}$, t integer

Question: Is there $(e_0, e_1) \in \mathcal{R}$ such that $|e_0| + |e_1| \leq t$ and $e_0 + e_1 h = s$?

Problem 2. **(2,1)-QC Codeword Finding**

Instance: $h \in \mathcal{R}$, w integer

Question: Is there $(h_0, h_1) \in \mathcal{R}$ such that $|h_0| + |h_1| \leq w$ and $h_1 + h_0 h = 0$?

QC-MDPC secure if Problems 1 (search) and 2 (decision) are hard.

Reduction is tight except for search/decision in Problem 2.

Parameters Selection for QC-MDPC-based schemes

The final constraint is that the (private) decoder must run with a negligible DFR (Decoding Failure Rate). Happens when $tw \leq \Theta(p)$. Exact values need to be confirmed by simulation (so far).

Binary QC-MDPC $[2p, p]$ code with parity check equations of weight w correcting t errors

(p, w, t)	key size	security*
$(10\,163, 142, 134)$	$10\,163$	128
$(19\,853, 206, 199)$	$19\,853$	192
$(32\,749, 274, 264)$	$32\,749$	256

* logarithm in base 2 of the cost of the best known (classical) attack lower bound derived from ISD, BJMM variant

About Key Recovery Attacks

[Guo, Johansson, & Stankovski, 16] exhibit and use a correlation between the private key and faulty error patterns to mount a key recovery attack.

$\rightarrow$ need for a failure-free decoder

Failure-free decoder can be achieved by improving the decoder and/or increasing the block size. Not sufficient because the GJS attack can be extended into a timing attack

$\rightarrow$ need for a constant-time decoder (as in QcBits [Chou, 16])

Fixing this would allow static keys and CCA conversions (required for asynchronous key establishment – *e.g.* email)

QC-MDPC – Conclusions

- Key size is much smaller than Goppa-McEliece (factor 300).

  Still key size scales as the square of the security.
  Can we do better?

- Indistinguishability reduces to a generic problem (existence of a low weight word in a QC code).

  Even better with the Ouroboros variant (*a.k.a.* BIKE-3)

- Open problem: constant-time failure-free decoder to thwart GJS key recovery attack $\rightarrow$ improve applicability

III. Digital Signature

Code-Based Digital Signature

FDH (Full Domain Hash) Digital Signature (*a.k.a* hash-and-sign) is a key cryptographic primitive.

In addition to data integrity, it can be used as a building block in numerous schemes and protocols (blind signatures, ring signatures, IBE, . . .).

Today the only such code-based signature is CFS [Courtois, Finiasz, & Sendrier, 01] which suffers from several flaws:

- a very bad scaling, making it impractical for post-quantum security levels
- a flaw in the security reduction: Goppa codes of rate $\to 1$ are distinguishable.

Code-Based Digital Signature

Given a parity check matrix $H \in \mathbf{F}_q^{k \times n}$

To sign a message M

- Hash the text M into a syndrome $\text{Hash}(M) = s \in \mathbf{F}_q^r$
- Find e of minimal weight such that $eH^T = s$
- Use e as a signature

To verify (M, e)

- Hash the text M into a syndrome $\text{Hash}(M) = s \in \mathbf{F}_q^r$
- Check $eH^T = s$

Problem: hard to achieve poly-time maximum likelihood decoding

CFS: the legitimate user only has a computational advantage

Code-Based Digital Signature

Given a parity check matrix $H \in \mathbf{F}_q^{k \times n}$

To sign a message M

- Hash the text M into a syndrome $\text{Hash}(M) = s \in \mathbf{F}_q^r$
- Find e of small weight such that $eH^T = s$
- Use e as a signature

To verify (M, e)

- Hash the text M into a syndrome $\text{Hash}(M) = s \in \mathbf{F}_q^r$
- Check $eH^T = s$

Problem: this is not decoding any more

But: known as source distortion in information theory

Source Distortion

- For an $[n, k]$ code, achieving distortion better than $t = (n-k)/2$ is intractable (Syndrome Decoding Problem).

  Hardness already studied for code-based hash function FSB
  [Augot, Finiasz, & Sendrier, 05]

- Optimal distortion: Gilbert-Varshamov bound $d_{\mathsf{GV}} = nh^{-1}(1 - \frac{k}{n})$

- Polar codes achieve (almost) optimal distortion with a poly-time algorithm . . . but are too structured
  [Bardet, Chaulet, Dragoi, Otmani, & Tillich, 16]

The $(U, U+V)$ Construction

- Given two codes U and V of same length, define

$$(U, U+V) = \{(u, u+v) \mid u \in U, v \in V\}$$

(polar codes result of a "fractal" $(U, U+V)$ construction)

- $(U, U+V)$ codes with random U and V achieve in poly-time a distortion strictly smaller than $(n-k)/2$.
Opens the way to existential unforgeability (EUF-CMA).
[Debris-Alazard, Sendrier, & Tillich, 17]

- Unfortunately, randomly permuted $(U, U+V)$ codes can be distinguished from random $\rightarrow$ security reduction is useless.

- Other similar constructions, hopefully one of them will allow the design of a secure signature scheme.

Conclusions

A lot of changes in code-based cryptography in the last few years.

- Shorter key sizes and better security arguments: QC-MDPC

  Timely, considering the NIST initiative for quantum safe primitives

- Still no FDH signature scheme, but a new promising approach

- An interesting shift of paradigm:

  The codes that seem the most promising for cryptography are bad in term of information theoretic efficiency

  $\rightarrow$ cryptographers may have to design their own codes

Thank you for your attention