Structural Cryptanalysis of McEliece-Like Schemes with Monoidic Keys

F. de Portzamparc
Joint work with J.-C. Faugère,
A. Otmani, L. Perret and J.-P. Tillich

Journées C2 2014

25 mars 2014

Code-based Cryptography : Syndrome decoding problem

- Solving a linear system over $\mathbb{F}_q$ with errors : given $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ and $\boldsymbol{c} \in \mathbb{F}_q^n$, find $\boldsymbol{m}$ and $\mathbf{e}$ with $w_H(\mathbf{e}) \leqslant w$ such that

$$\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G} + \mathbf{e}.$$


E. Berlekamp, R. McEliece, H. van Tilborg.
On the inherent intractability of certain coding problems.
IEEE Transactions on Information Theory, 1978


R.J. McEliece.
A public-key cryptosystem based-on algebraic coding theory.
DSN Progress Report 44, 1978


N. Courtois, M. Finiasz, N. Sendrier.
How to achieve a McEliece-based digital signature scheme.
ASIACRYPT 2001

Code-based Cryptosystem (1978)

- **Public key** : $\boldsymbol{G}_{pub}$ generating $\mathscr{C}_{pub}$ code with parameters $[n, k, t]_q$
- **Private key** : a fast decoder for $\mathscr{C}_{pub}$ ($\boldsymbol{x}, \boldsymbol{y}$ for an alternant code)
- Message $\boldsymbol{m} \in \mathbb{F}_q^k$, ciphertext $\boldsymbol{c} \in \mathbb{F}_q^n$, error $\mathbf{e} \in \mathbb{F}_q^n$ with $w_H(\mathbf{e}) \leqslant t$:

$$\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G}_{pub} + \mathbf{e}$$

- Huge public key

McEliece Schemes with Symmetric Keys

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{t-1} \\ a_{t-1} & a_0 & \cdots & a_{t-2} \\ \vdots & \ddots & \cdots & \vdots \\ a_1 & \cdots & a_{t-1} & a_0 \end{pmatrix}$$

Cyclic block

$$\left(\begin{array}{cc|cc} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ \hline a_2 & a_3 & a_0 & a_1 \\ a_3 & a_2 & a_1 & a_0 \end{array}\right)$$

Dyadic block with $t = 4$

T. Berger, P.-L. Cayrel, Ph. Gaborit, A. Otmani.

Reducing Key Length of the McEliece Cryptosystem.

AFRICACRYPT 2009

R. Misoczki, P. Barreto.

Compact McEliece Keys from Goppa Codes.

SAC 2009

$$\boldsymbol{G} = \left(\begin{array}{c|c|c} \cdots & M_i & \cdots \\ & & \end{array}\right)$$

- M_i matrices with symmetries of size $t \times t$.
- Compression factor t for $\boldsymbol{G}$.
- Find codes with known **permutation group.**

Algebraic Key-Recovery Cryptanalysis (EC'10)

J.-C. Faugère, A. Otmani, L. Perret, J.-P. Tillich.
Algebraic Cryptanalysis of McEliece Variants with Compact Keys.
EUROCRYPT 2010

- $\boldsymbol{x}, \boldsymbol{y}$ secret vectors are solutions of :

$$\left\{ \sum_{j=0}^{n-1} g_{i,j} Y_j X_j^{\ell} = 0 \mid 0 \leqslant i < k, 0 \leqslant \ell \leqslant t-1 \right\}.$$

- $g_{i,j}$ entries of $\boldsymbol{G}_{pub}$,

Algebraic Cryptanalysis & McEliece compact variants (EC'10)

	McEliece	QC McEliece	QD McEliece
X variables	n	n/t	$n/t+\lambda$
Y variables	$n-k$	$(n-k)/t$	$(n-k)/t$

t = compression factor, $\lambda = \log_p(t)$.

q	n/t	t	FGb(F5)
2^8	9	51	0.06 s
2^8	10	51	0.03 s
2^8	12	51	0.05 s
2^8	15	51	0.02 s
2^{10}	6	75	0.05s
2^{10}	6	93	0.05s
2^{10}	8	93	0.02s
2^8	15	255	0.08s

Table: Quasi-cyclic parameters $[n,k,t]_q$.

q	n/t	t	FGb(F5)
2^8	12	64	0.03 s
2^4	32	64	0.50 s
2^2	56	64	1776 s
2	158	128	NA
2	12	128	NA
2	511	16	NA
3	19682	9	NA
241	4	241	NA

Table: Quasi-dyadic/monoidic parameters $[n,k,t]_q$.

$\Rightarrow$ Very efficient for some instances ... not at all for binary dyadic codes !

Our Results

	McEliece	QD McEliece	Our work
X variables	n	$n/t + \lambda$	n/t
Y variables	$n-k$	$(n-k)/t$	$(n-k)/t$

t = compression factor, $\lambda = \log_p(t)$.

q	n/t	t	FGb(F5)/EC'10	Our work with Magma(F4)
2^8	12	64	0.03 s	0.010 s
2^4	32	64	0.50 s	0.010 s
2^2	56	64	1776 s	0.040 s
2	158	128	NA	18 s
2	12	128	NA	$2^{83.5}$ op
2	511	16	NA	1.9 s
3	19682	9	NA	3.4 s
241	4	241	NA	0.020 s

Table: Quasi-dyadic/monoidic parameters $[n, k, t]_q$.

the Folded Code

$$G = \left(\begin{array}{c|c|c} \cdots & M_i & \cdots \\ \hline & \vdots & \end{array}\right)$$

M_i block $t \times t$

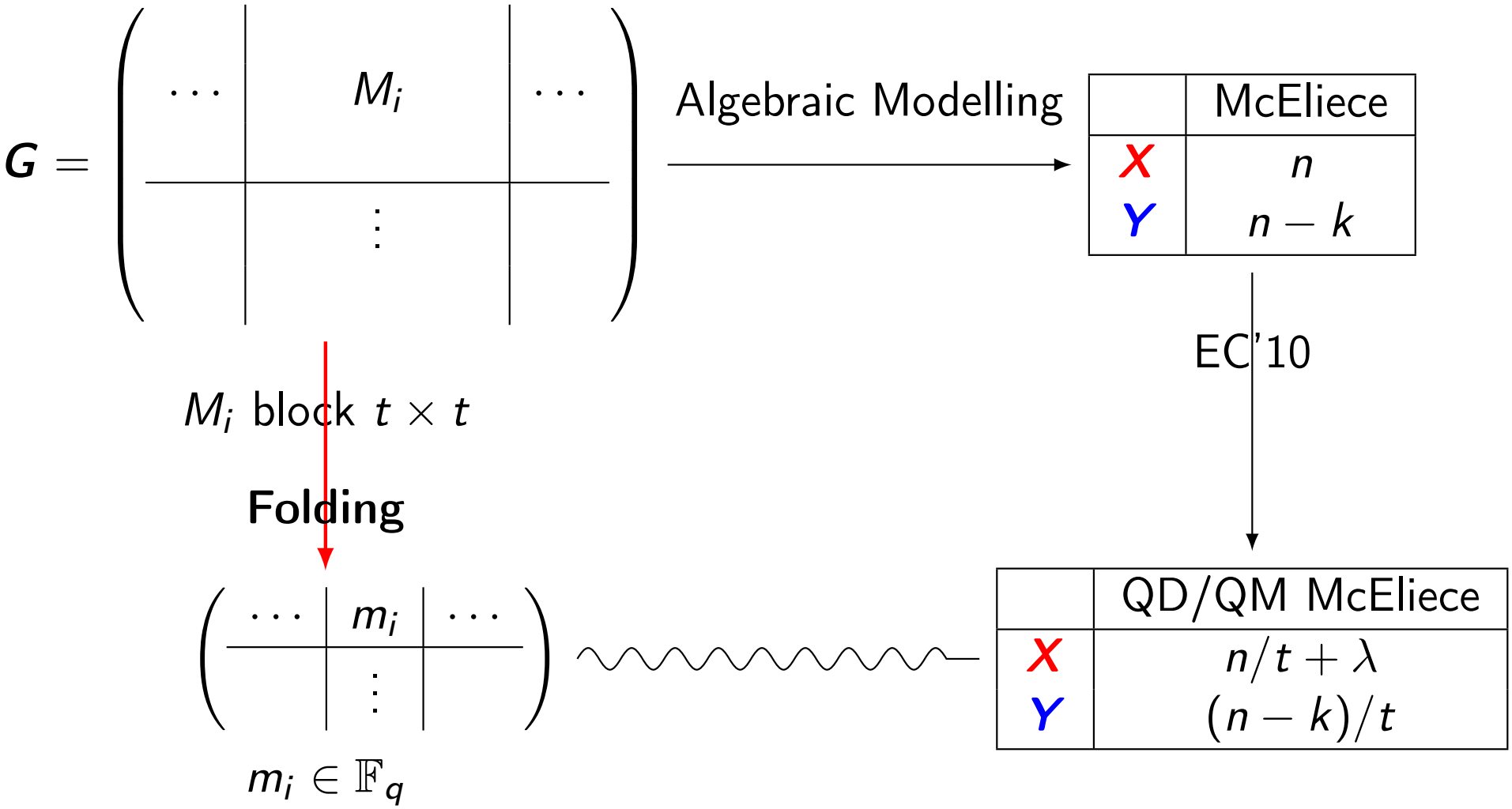
Algebraic Modelling

	McEliece
X	n
Y	$n-k$

EC'10

	QD/QM McEliece
X	$n/t + \lambda$
Y	$(n-k)/t$

the Folded Code



Alternant codes

Definition (Alternant code)

- A *support* : $\boldsymbol{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_{q^m}^n$, with $x_i \neq x_j$,
- A set of *multipliers* : $\boldsymbol{y} = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_{q^m}^n$, s.t. $y_i \neq 0$,

$$\boldsymbol{V}_t(\mathbf{x}, \mathbf{y}) = \begin{pmatrix} y_0 & y_1 & \cdots & y_{n-1} \\ y_0 x_0 & y_1 x_1 & \cdots & y_{n-1} x_{n-1} \\ \vdots & & \ddots & \vdots \\ y_0 x_0^{t-1} & & \cdots & y_{n-1} x_{n-1}^{t-1} \end{pmatrix}$$

$$\mathscr{A}_t(\boldsymbol{x}, \boldsymbol{y}) = \{\boldsymbol{m} \in {\mathbb{F}_q}^n | \boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y}) \boldsymbol{m}^T = \mathbf{0}\}$$

- Knowing $\boldsymbol{x}, \boldsymbol{y}$, we can decode $\frac{t}{2}$ errors in **polynomial time**

What's a code with symmetry ?

Definition (Permutation Group of a code)

Let $\mathscr{C} \subset \mathbb{F}_q^n$.

$$Perm(\mathscr{C}) = \left\{ \sigma \in \mathcal{S}_n \mid \forall \boldsymbol{m} \in \mathscr{C}, \boldsymbol{m}^\sigma \stackrel{\text{def}}{=} (m_{\sigma(0)}, \ldots, m_{\sigma(n-1)}) \in \mathscr{C} \right\}$$

- "with symmetries" = "with a non-trivial permutation group by construction"
- A code with symmetries admits **compact representations**

Example

$$\boldsymbol{G} = \left(\begin{array}{cc|cc|cc|cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{array} \right).$$

$\sigma \in \mathcal{S}_{14} : i \mapsto i \oplus 1$ is a permutation of the code spanned by $\boldsymbol{G}$.

Quasi-Monoidic Codes

Monoidic Codes ([T. Berger])

Let $p = \mathrm{char}(\mathbb{F}_q)$, $\mathscr{C} = \mathcal{A}_t(x, y)$ and

$$\sigma_p = \left(\begin{array}{c|ccc|c} \dots & ip & \dots & ip+p-1 & \dots \\ \dots & ip+1 & \dots & ip & \dots \end{array} \right) \in \mathcal{S}_n.$$

Suppose there exists $\alpha \in \mathbb{F}_{q^m}$ s.t.

$$\left\{ \begin{array}{rcl} x_{\sigma(i)} & = & x_i + \alpha \\ y_{\sigma(i)} & = & y_i \end{array} \right. \quad (\star)$$

Then, $\sigma_p \in \mathit{Perm}(\mathscr{C})$ and $\mathscr{C}$ is quasi-monoidic.

- P. Barreto, R. Misoczki :
  - Build x respecting $(\star)$ for several α_i's and σ's at the same time,
  - Alternant code with $\mathit{Perm}(\mathscr{C}) \simeq (\mathbb{Z}/p\mathbb{Z})^\lambda$.

Weakness of symmetric alternant codes

$$G = \left(\begin{array}{c|c|c} \cdots & M_i & \cdots \\ \hline & \vdots & \end{array}\right)$$

M_i block $t \times t$

Folding

$$\left(\begin{array}{c|c|c} \cdots & m_i & \cdots \\ \hline & \vdots & \end{array}\right)$$

$m_i \in \mathbb{F}_q$

Weakness of symmetric alternant codes

Definition (Folded code)

$\mathscr{C}$ a quasi-monoidic alternant code,

$\sigma_p = \left(\begin{array}{c|ccc|c} \dots & ip & \dots & ip+p-1 & \dots \\ \dots & ip+1 & \dots & ip & \dots \end{array} \right) \in Perm(\mathscr{C})$. Then,

$$\overline{\mathscr{C}^{\sigma_p}} = \left\{ (m_{ip} + \cdots + m_{ip+p-1})_{0 \leqslant i \leqslant n/p} \mid \boldsymbol{m} \in \mathscr{C} \right\}.$$

Example

$$\left(\begin{array}{cc|cc|cc|cc|cc|cc|cc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \right).$$

Fold with to $\sigma_2 \in \mathcal{S}_{14} : i \mapsto i \oplus 1$ <=> Replace (m_{2i}, m_{2i+1}) by $(m_{2i} + m_{2i+1})$

$$\left(\begin{array}{ccccccc} 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{array} \right).$$

Structure of the folded code

Theorem (Folded code of an alternant code, FOPPT)

$\mathscr{C} = \mathcal{A}_t(\boldsymbol{x}, \boldsymbol{y})$ a quasi-monoidic alternant code, $\sigma_p \in Perm(\mathscr{C})$.

1. $\overline{\mathscr{C}^{\sigma_p}} = \mathcal{A}_{t/p}(\boldsymbol{x}', \boldsymbol{y}')$, *with* $\boldsymbol{x}', \boldsymbol{y}' \in \mathbb{F}_{q^m}^{n/p}$ *defined by*

$$\begin{aligned} x'_i &= x_{ip}{}^p - \alpha^{p-1} x_{ip} \\ y'_i &= y_{ip} \end{aligned}$$

2. $\overline{\mathscr{C}^{\sigma_p}}$ *is quasi-monoidic and* $Perm(\overline{\mathscr{C}^{\sigma_p}}) \simeq (\mathbb{Z}/p\mathbb{Z})^{\lambda-1}$.

Consequence

Key security of a symmetric scheme equivalent to the security of a *non-symmetric scheme with same key size*!

- Key security of a $[4096, 2048, 128]_2$ code reduced that of a $[64, 32, 2]_2$ code

Sketch of the proof for monoidic alternant codes

Characterization of Alternant Codes

$$\mathscr{A}_t(\boldsymbol{x}, \boldsymbol{y}) = \{(\tilde{y}_i P(x_i))_{0 \leqslant i \leqslant n-1} \mid P \in \mathbb{F}_{q^m}[X], \deg(P) < n - t\} \bigcap \mathbb{F}_q^n$$

with $\tilde{y}_i = \frac{1}{y_i} \frac{1}{\prod_{j \neq i}(x_j - x_i)}$.

Quasi-monoidic alternant code's $\boldsymbol{x}$ and $\tilde{\mathbf{y}}$

$$\begin{array}{rcccccccc} \boldsymbol{x} & = & (\cdots \mid & x_{ip}, & x_{ip} + \alpha & , \ldots , & x_{ip} + (p-1)\alpha & \mid \ldots) \\ \tilde{\mathbf{y}} & = & (\cdots \mid & \tilde{y}_{ip}, & \tilde{y}_{ip} & , \ldots , & \tilde{y}_{ip} & \mid \ldots) \end{array}$$

Sketch of the proof for monoidic alternant codes

Characterization of Alternant Codes

$$\mathscr{A}_t(\boldsymbol{x}, \boldsymbol{y}) = \{(\tilde{y}_i P(x_i))_{0 \leqslant i \leqslant n-1} \mid P \in \mathbb{F}_{q^m}[X], \deg(P) < n - t\} \bigcap \mathbb{F}_q^n$$

with $\tilde{y}_i = \frac{1}{y_i} \frac{1}{\prod_{j \neq i}(x_j - x_i)}$.

Quasi-monoidic alternant code's $\boldsymbol{x}$ and $\tilde{\mathbf{y}}$

$$\begin{array}{rcl} \boldsymbol{x} & = & (\cdots \mid x_{ip}, \quad x_{ip} + \alpha \quad , \ldots , \quad x_{ip} + (p-1)\alpha \quad \mid \ldots) \\ \tilde{\mathbf{y}} & = & (\cdots \mid \tilde{y}_{ip}, \quad \tilde{y}_{ip} \quad , \ldots , \quad \tilde{y}_{ip} \quad \mid \ldots) \end{array}$$

- For a codeword $\boldsymbol{m} \in \mathscr{C}$, the folded codeword's coordinates are :

$$\begin{array}{rcl} m'_i & = & \tilde{y}_{ip} P(x_{ip}) + \tilde{y}_{ip+1} P(x_{ip+1}) + \cdots + \tilde{y}_{ip+p-1} P(x_{ip+p-1}) \\ & = & \tilde{y}_{ip} \left(P(x_{ip}) + P(x_{ip+1}) + \cdots + P(x_{ip+p-1}) \right) \\ & = & \tilde{y}_{ip} \underbrace{\left(P(x_{ip}) + P(x_{ip} + \alpha) + \cdots + P(x_{ip} + (p-1)\alpha) \right)}_{R(x_{ip})} \end{array}$$

Sketch of the proof for monoidic alternant codes

$$R(X) = P(X) + P(X + \alpha) + \cdots + P(X + (p-1)\alpha)$$

- Symmetry under $X \mapsto X + \alpha$:

$$R(X) = R(X + \alpha) = \cdots = R(X + (p-1)\alpha)$$

- For some $Q \in \mathbb{F}_{q^m}[X]$ in degree $\deg(R)/p$,

$$R(X) = Q(X^p - \alpha^{p-1}X).$$

Sketch of the proof for monoidic alternant codes

$$R(X) = P(X) + P(X+\alpha) + \cdots + P(X+(p-1)\alpha)$$

- Symmetry under $X \mapsto X + \alpha$:

$$R(X) = R(X+\alpha) = \cdots = R(X+(p-1)\alpha)$$

- For some $Q \in \mathbb{F}_{q^m}[X]$ in degree $\deg(R)/p$,

$$R(X) = Q(X^p - \alpha^{p-1}X).$$

- Back to $\boldsymbol{m}'$:

$$m'_i = \tilde{y}_{ip} Q({x_{ip}}^p - \alpha^{p-1} x_{ip}).$$

- Conclusion :

$$\boldsymbol{m}' \in \left\{ (\tilde{y}_{ip} Q(x'_i))_{0 \leqslant i \leqslant n/p-1} \mid Q \in \mathbb{F}_{q^m}[X]_{<(n-t)/p} \right\} \bigcap \mathbb{F}_q^{n/p}$$

and

$$\overline{\mathscr{C}^{\sigma_p}} \subseteq \mathscr{A}_{t/p}(\mathbf{x}', \mathbf{y}')$$

Algebraic Modellings

- EC'10 : for any alternant code of order t,

$$\boldsymbol{G}_{pub}\boldsymbol{V}_t(\mathbf{x},\mathbf{y})^T = (0)_{k\times t}.$$

- Our refined modelling :

Theorem (Extended code of a Goppa code)

Let $\mathscr{C}$ be a Goppa code with polynomial g of degree t,

$$\widetilde{\boldsymbol{G}}\boldsymbol{V}_{t+1}((\mathbf{x},\infty),(\mathbf{y},\mathbf{LC}(\mathbf{g})^{-1})^T = (0)_{k\times t+1},$$

where $\widetilde{\boldsymbol{G}}$ generates the extended code of $\mathscr{C}_{pub}$,

Theorem (Double error correcting capacity of binary Goppa codes)

Let $\mathscr{C}$ be Goppa code of degree t over $\mathbb{F}_2$,

$$\boldsymbol{G}_{pub}\boldsymbol{V}_{2t}(\mathbf{x},\mathbf{y}^2)^T = (0)_{k\times 2t}.$$

Algebraic Systems

- Systems to solve according to the structure of $\mathscr{C}_{pub}$

	$\#\boldsymbol{X}$	$\#\boldsymbol{Y}'$	Bi-degree
Alternant code	$n-2$	$n-k-1$	$(u,1)$, with $1 \leqslant u \leqslant t-1$
Goppa code	$n-2$	$n-k$	$(t,1)$
Binary Goppa code	$n-2$	$n-k$	$(u,2)$ with $1 \leqslant u \leqslant t-1$

- Systems with structural elimination tools (raises degrees)

	$\#\boldsymbol{X}'$	$\#\boldsymbol{Y}'$	Bi-degree
Alternant code	$n-k-2$	$n-k-1$	(p^u,p), with $1 \leqslant u \leqslant \lambda-1$
Goppa code	$n-k-2$	$n-k$	$(t,1)$
Binary Goppa code	$n-k-2$	$n-k$	$(2^u,2)$, with $0 \leqslant u \leqslant 2\lambda-1$

$t = p^\lambda$.

Cryptanalysis Strategy for monoidic codes with $t = p^\lambda$

$$\boldsymbol{G} = \left(\begin{array}{c|c|c} \cdots & M_i & \cdots \\ \hline & \vdots & \end{array}\right)$$

$k \times n$ matrix, $t = p^\lambda$

Cryptanalysis Strategy for monoidic codes with $t = p^\lambda$

$$\boldsymbol{G} = \left(\begin{array}{c|c|c} \cdots & M_i & \cdots \\ \hline & \vdots & \end{array}\right)$$

$k \times n$ matrix, $t = p^\lambda$

Folding

$$\overline{\boldsymbol{G}^\sigma} = \left(\begin{array}{c|c|c} \cdots & M'_i & \cdots \\ \hline & \vdots & \end{array}\right)$$

$k/p \times n/p$ matrix, $t = p^{\lambda-1}$

Cryptanalysis Strategy for monoidic codes with $t = p^\lambda$

$$\boldsymbol{G} = \left(\begin{array}{c|c|c} \cdots & M_i & \cdots \\ \hline & \vdots & \end{array}\right)$$

$k \times n$ matrix, $t = p^\lambda$

Successive Folding

$$\overline{\overline{\overline{\boldsymbol{G}^{\sigma}}^{\cdots}}^{\sigma}} = \begin{pmatrix} \cdots & m_i & \cdots \\ & \vdots & \end{pmatrix}$$

$k/\widetilde{t} \times n/\widetilde{t}$ matrix, $\widetilde{t} = p^s, s < \lambda$

Cryptanalysis Strategy for monoidic codes with $t = p^\lambda$

$$\boldsymbol{G} = \left(\begin{array}{c|c|c} \cdots & M_i & \cdots \\ \hline & \vdots & \end{array}\right)$$

$k \times n$ matrix, $t = p^\lambda$

Successive Folding

$$\overline{\overline{\boldsymbol{G}^{\sigma\cdots}}}^{\sigma} = \begin{pmatrix} \cdots & m_i & \cdots \\ & \vdots & \end{pmatrix}$$

$k/\widetilde{t} \times n/\widetilde{t}$ matrix, $\widetilde{t} = p^s, s < \lambda$

	McEliece	
$\boldsymbol{X}$	n	$n-k$
$\boldsymbol{Y}$	$n-k$	$n-k$

EC'10

	QD/QM McEliece	
$\boldsymbol{X}$	$n/t+\lambda$	$(n-k)/t+\lambda$
$\boldsymbol{Y}$	$(n-k)/t$	$(n-k)/t$

	Folded QM McE	
$\overline{\boldsymbol{X}^{\sigma}}$	$n/t+s$	$(n-k)/t+s$
$\boldsymbol{Y}$	$(n-k)/t$	$(n-k)/t$

Practical Cryptanalysis

- Implementation for Encryption and Signature parameters from :

R. Misoczki, P. Barreto.
Compact McEliece Keys from Goppa Codes.
SAC 2009

P. Barreto, P.-L. Cayrel, R. Misoczki, R. Niebuhr.
Quasi-Dyadic CFS Signatures.
Inscrypt 2010

P. Barreto, R. Lindner, R. Misoczki.
Monoidic Codes in Cryptography.
PQCrypto 2011

Practical Cryptanalysis : signature schemes

- Signature schemes : long codes, high dimension.
- Impossible to break with EC'10's attack.

q	m	t	n/t	unk.	equ.	Magma	ISD
2	13	16	511	26	996	1.9 s	2^{84}
2	14	13	1023	28	2018	3.0 s.	2^{81}
2	15	12	2047	30	4064	5.4 s.	2^{82}

$p > 2$	m	t	n/t	unk.	equ.	Magma	ISD
3	11	9	19682	22	19671	3.4 s	2^{80}
5	8	15	15624	16	15616	82 s.	2^{128}

Table: Practical attacks against signature schemes with parameters.

Practical Cryptanalysis : encryption schemes

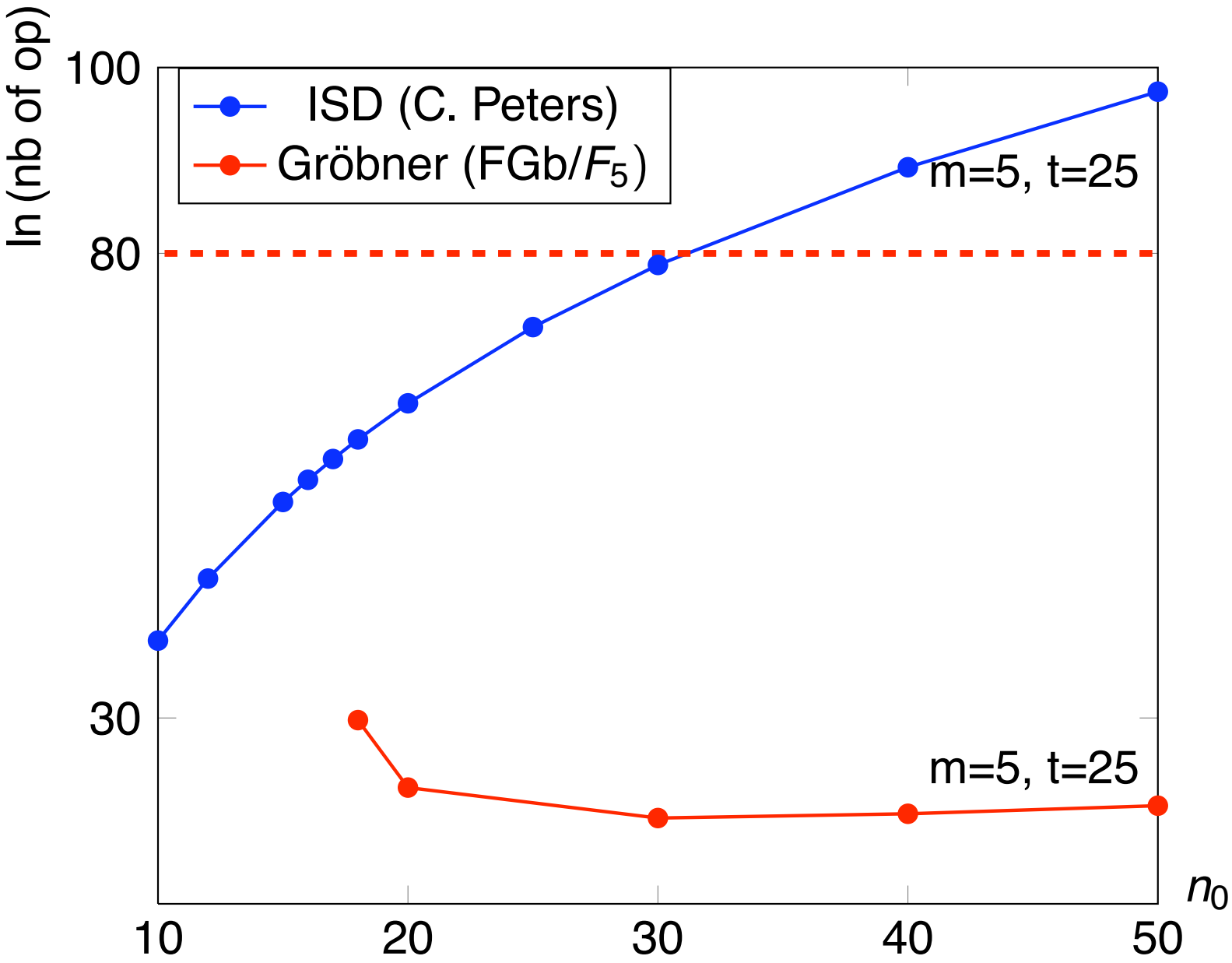
- Encryption schemes : smaller systems, smaller overdetermination ratio,

$q = 2^s$	m	t	n/t	unk.	equ.	Magma	EC'10	ISD
2^4	4	128	32	8	28	0.010 s	7.1 s	2^{128}
2^2	8	64	56	15	48	0.040 s	1,776 s	2^{128}

$q = 2$	m	t	n/t	unk.	equ.	Magma	EC'10	ISD
2	16	32	152	29	272	18 s	N.A.	2^{128}
2	12	128	25	23	22	$\leqslant 2^{83.5}$ op. (F5)	N.A.	2^{128}

q	m	t	n/t	unk.	equ.	Magma	EC'10	ISD
241	3	241	4	5	7	0.020 s	N.A.	2^{112}
7	5	49	15	18	60	900 s	N.A.	2^{80}

Complexity of ISD and Gröbner $q = 5$



Conclusion

Folding method

- Questions the idea of QD/QM codes with symmetries for crypto !
- More general framework for QC/QD/QM codes.
- Complexity bounds ?

Thank you for your attention, questions ?