Algebraic Attack of McEliece with Goppa Polynomial of a Special Form

J.-C. Faugère, L. Perret, F. de Portzamparc
(Polsys (UPMC/Inria/CNRS)/Gemalto)

AsiaCrypt 2014

Challenges in Public-Key Cryptography

- Need for **alternatives** to RSA and elliptic curves
  - Hard problems no longer hard ... (Discrete log over $\mathbb{F}_{2^m}$)
  - Quantum Computer ?

2nd Quantum-Safe Crypto Workshop (Oct. 2014)

NIST Workshop on Cybersecurity in a Post-Quantum World (Apr. 2015)

Code-based Cryptography

- McEliece encryption : no attack since 1978 (parameters rescaled).
- Very fast encryption, fast decryption.
- **Post-Quantum security**
- Big public keys (1535 kB for sec level 2^{128}).
- Potential future standardization

Code-based Encryption

$$\underset{\text{plaintext } \boldsymbol{m}\in\mathbb{F}_q^k}{\left(\ 0,\ldots,1\ \right)} \overset{\text{public key } \boldsymbol{G}_{pub}\in\mathbb{F}_q^{k\times n}}{\begin{pmatrix} \\ \boldsymbol{G}_{pub} \\ \\ \end{pmatrix}} + \underset{\text{error } \boldsymbol{e}\in\mathbb{F}_q^n}{\left(\ 1,0,\ldots,0,1\ \right)} = \underset{\text{ciphertext } \boldsymbol{c}\in\mathbb{F}_q^n}{\left(\ 1,0,\ldots,1,1\ \right)}$$

- Syndrom Decoding Problem (NP-complete for $\boldsymbol{G}$ random).

  E. Berlekamp, R. McEliece, H. van Tilborg.
  On the Inherent Intractability of Certain Coding Problems, 1978.

- Best message-recovery algorithms : Information-Set Decoding (ISD).

- Requirement : a code **with a trapdoor**
  - **Examples :**Generalized Reed-Solomon , Goppa,Reed-Muller codes ...

Code-based Encryption

$$\underset{\text{plaintext } \boldsymbol{m}\in\mathbb{F}_q^k}{\left(\ 0,\ldots,1\ \right)} \overset{\text{public key } \boldsymbol{G}_{pub}\in\mathbb{F}_q^{k\times n}}{\begin{pmatrix} \\ \boldsymbol{G}_{pub} \\ \\ \end{pmatrix}} + \underset{\text{error } \boldsymbol{e}\in\mathbb{F}_q^n}{\left(\ 1,0,\ldots,0,1\ \right)} = \underset{\text{ciphertext } \boldsymbol{c}\in\mathbb{F}_q^n}{\left(\ 1,0,\ldots,1,1\ \right)}$$

- Syndrom Decoding Problem (NP-complete for $\boldsymbol{G}$ random).

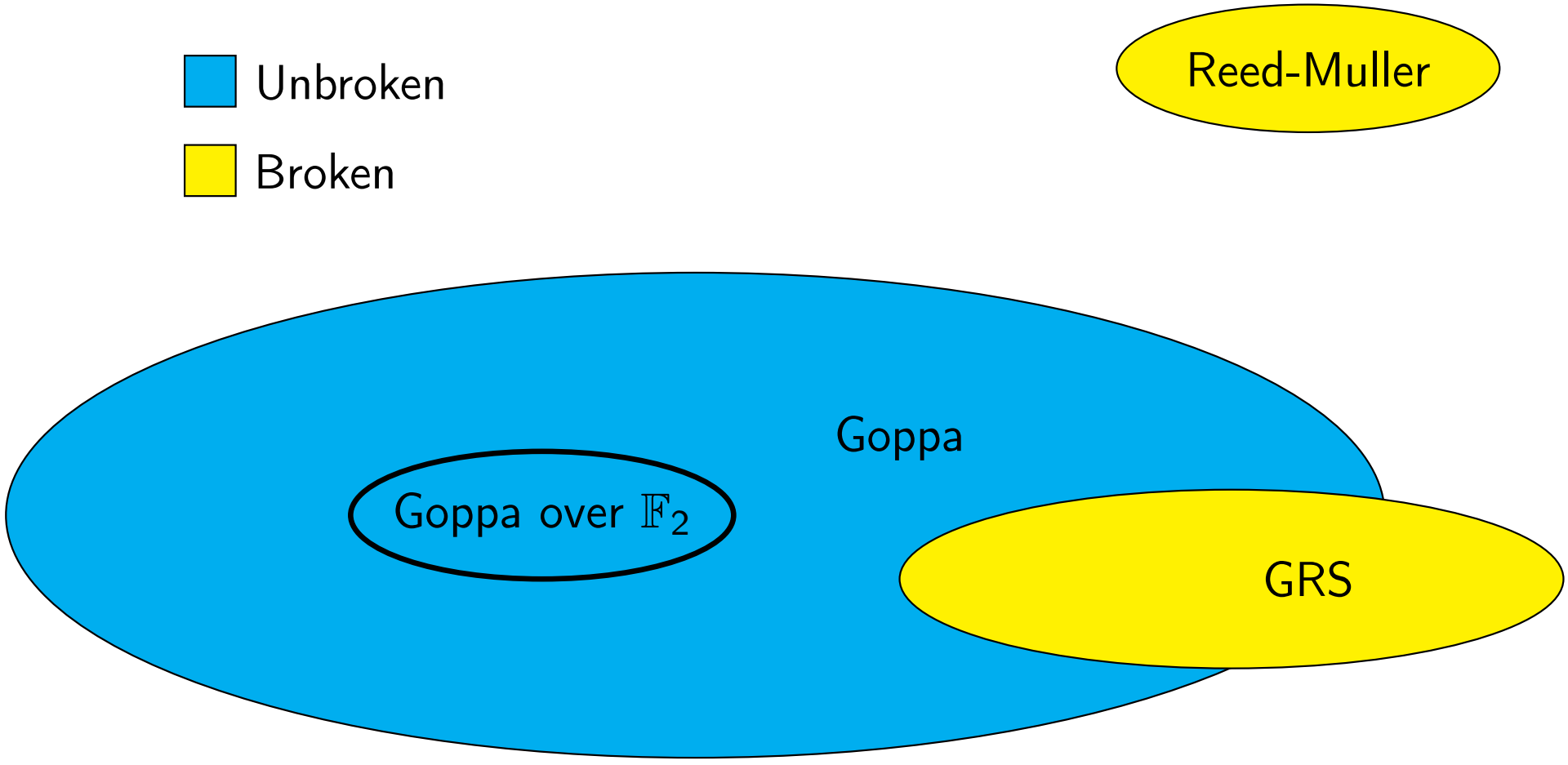
  

  E. Berlekamp, R. McEliece, H. van Tilborg.
  On the Inherent Intractability of Certain Coding Problems, 1978.

- Best message-recovery algorithms : Information-Set Decoding (ISD).

- Requirement : a code **with a secret trapdoor** ($\boldsymbol{G}_{pub}$ **looks** random)
  - **Examples :** ~~Generalized Reed-Solomon~~, Goppa, ~~Reed-Muller~~ codes ...

(Some) Codes with trapdoor proposed



A recent generalization of McEliece

	$\boldsymbol{G}_{pub}$ entries	Secret	Key size (2^{128} security)
Binary Goppa	$\in \mathbb{F}_2$	any $\Gamma \in \mathbb{F}_{2^m}[z]$	1535 kB
Wild Goppa & Incognito	$\in \mathbb{F}_q$ $(q \geqslant 2)$	$\Gamma = fg^{q-1} \in \mathbb{F}_{q^m}[z]$	down to 90 kB

D. Bernstein, T. Lange, C. Peters.
Wild McEliece (2010), Wild McEliece Incognito (2011).

A recent generalization of McEliece

	$\boldsymbol{G}_{pub}$ entries	Secret	Key size (2^{128} security)
Binary Goppa	$\in \mathbb{F}_2$	any $\Gamma \in \mathbb{F}_{2^m}[z]$	1535 kB
Wild Goppa & Incognito	$\in \mathbb{F}_q$ $(q \geqslant 2)$	$\Gamma = fg^{q-1} \in \mathbb{F}_{q^2}[z]$	down to 90 kB

D. Bernstein, T. Lange, C. Peters.

Wild McEliece (2010), Wild McEliece Incognito (2011).

A. Couvreur, A. Otmani and J.-P. Tillich

Polynomial Time Attack on Wild McEliece over Quadratic Extensions $m = 2$

EUROCRYPT 2014

Impact on key-security : use $m > 2$.

A recent generalization of McEliece

	$\boldsymbol{G}_{pub}$ entries	Secret	Key size (2^{128} security)
Binary Goppa	$\in \mathbb{F}_2$	any $\Gamma \in \mathbb{F}_{2^m}[z]$	1535 kB
Wild Goppa & Incognito	$\in \mathbb{F}_q$ $(q \geqslant 2)$	$\Gamma = fg^{q-1} \in \mathbb{F}_{q^m}[z]$	down to 90 kB

D. Bernstein, T. Lange, C. Peters.

Wild McEliece (2010), Wild McEliece Incognito (2011).

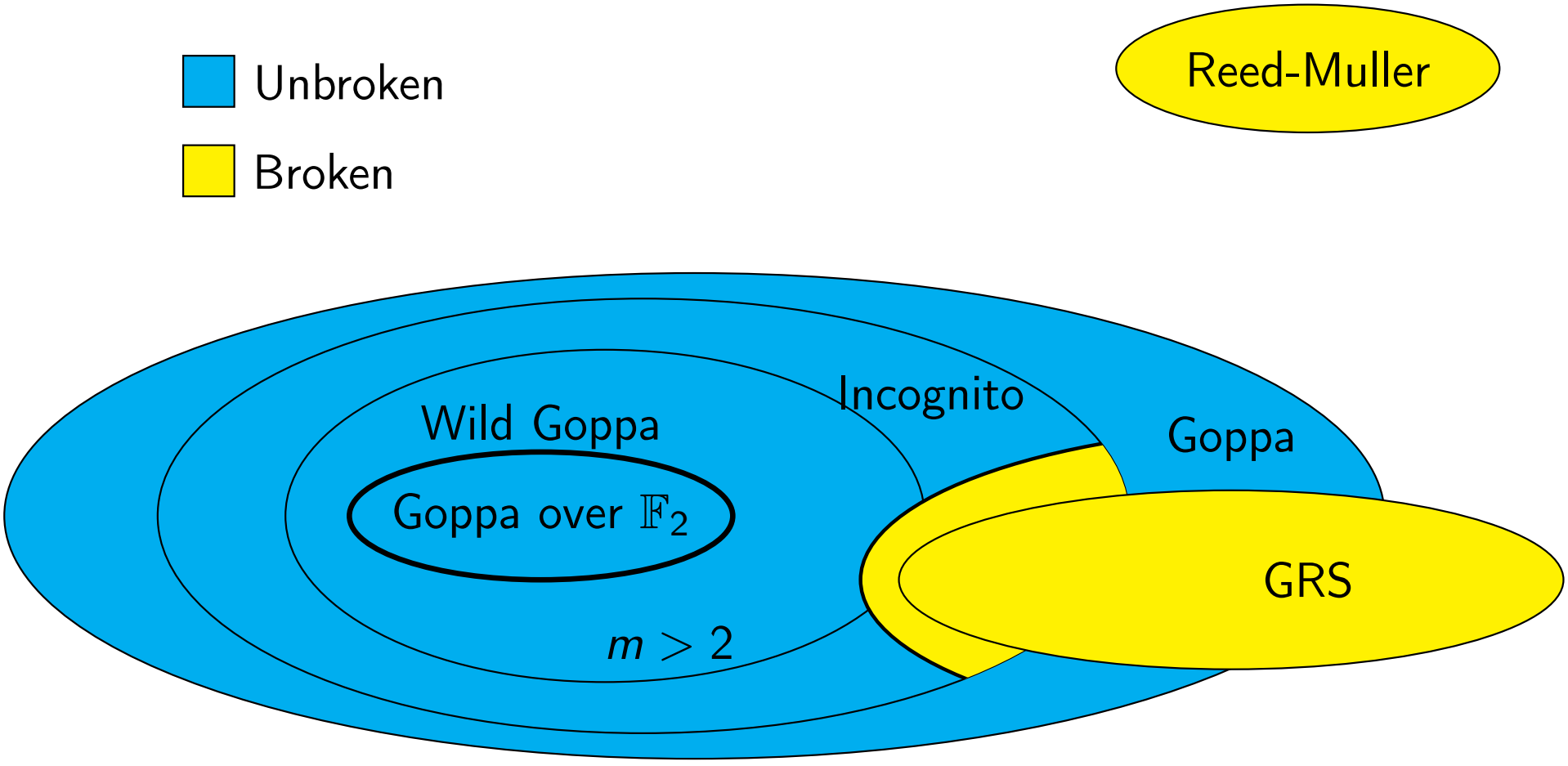
A. Couvreur, A. Otmani and J.-P. Tillich

Polynomial Time Attack on Wild McEliece over Quadratic Extensions $m = 2$

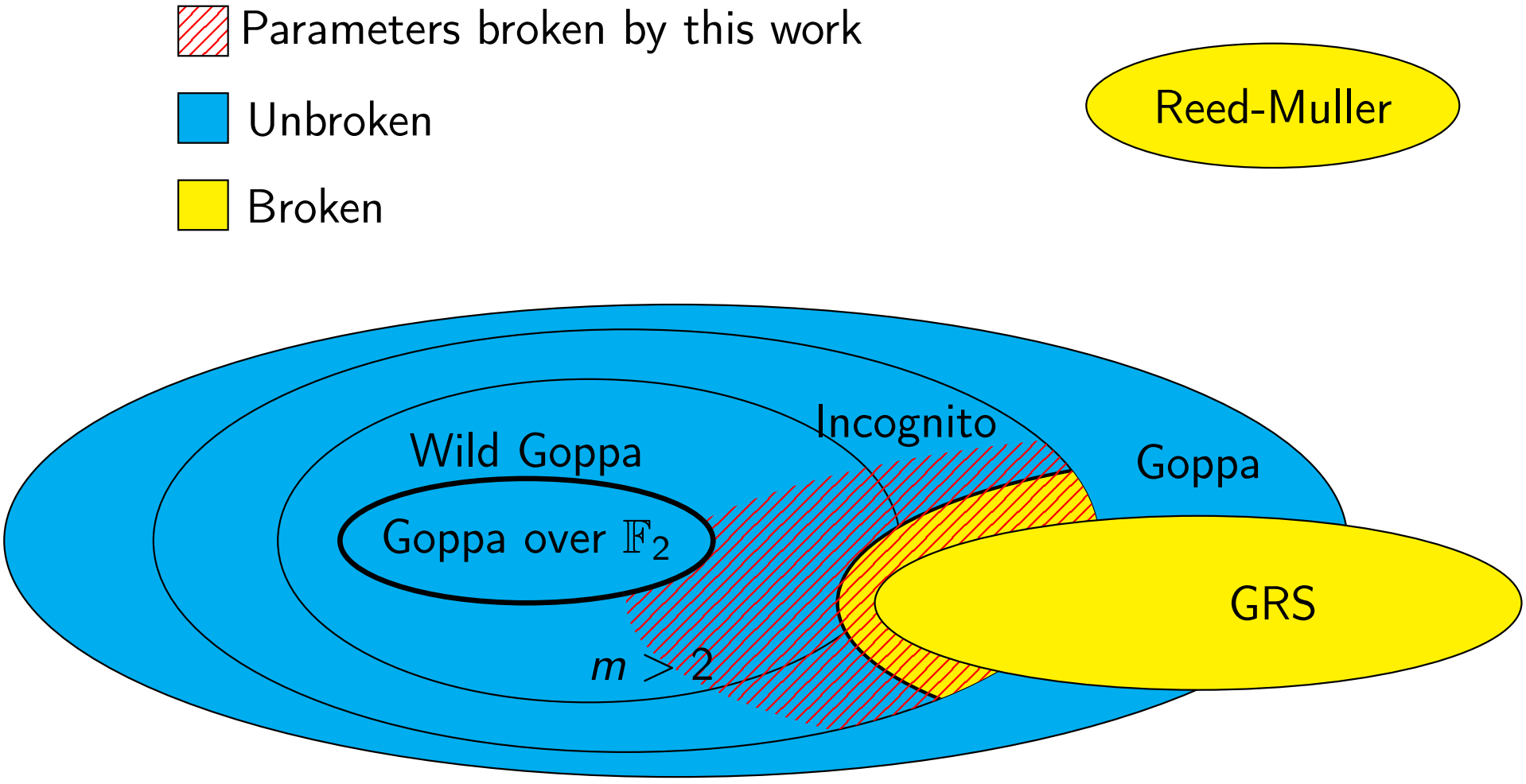
EUROCRYPT 2014

Impact on key-security : use $m > 2$.

(Some) Codes with trapdoor proposed



(Some) Codes with trapdoor proposed



Here : **Algebraic Cryptanalysis for Wild McEliece with** $q > 2, m \geqslant 2$

Algebraic Cryptanalysis

Here : Algebraic Cryptanalysis for Wild McEliece with $q > 2, m \geqslant 2$

Solving non-linear algebraic system $\mathcal{W}(\boldsymbol{Z}) \implies$ key-recovery.

Algebraic Cryptanalysis

Here : Algebraic Cryptanalysis for Wild McEliece with $q > 2, m \geqslant 2$

Solving non-linear algebraic system $\mathcal{W}(\boldsymbol{Z}) \implies$ key-recovery.

- A tool for resolution : **Gröbner bases** (F4 algorithm).
- Complexity relies on the amount of :
  - **variables** : the fewer, the better.
  - **equations** : the more, the better.

Algebraic Cryptanalysis

Here : Algebraic Cryptanalysis for Wild McEliece with $q > 2, m \geqslant 2$

Solving non-linear algebraic system $\mathcal{W}(\boldsymbol{Z}) \implies$ key-recovery.

- A tool for resolution : **Gröbner bases** (F4 algorithm).
- Complexity relies on the amount of :
  - **variables** : the fewer, the better.
  - **equations** : the more, the better.
- Algebraic modelling for Goppa codes :

J.-C. Faugère, A. Otmani, L. Perret, J.-P. Tillich (FOPT'10).
Algebraic Cryptanalysis of McEliece Variants with Compact Keys.

$\sum_j g_j Y_j X_j^{\ell} = 0$ (X_j, Y_j : unkowns)
No Wild structure exploited. - - -► **Bottleneck** Secret $\Gamma(z)$

Challenge : find a more compact modelling thanks to Wild structure

Our work vs existing algebraic modelling

	This work	[FOPT'10]
$\mathcal{W}(\boldsymbol{Z})$:	$\sum_j g_j Z_j{}^u$	$\sum_j g_j Y_j X_j{}^\ell$

g_j : public key entries,

X_j, Y_j, Z_j : unkowns

1. Compact : **fewer variables**.
2. Simpler equations to solve.
3. Non-prime q : exploits a weakness to reduce number of Z_j **for free**.

Code parameters $(q, m, \deg(g), \deg(f), n, k)$	Number of unkowns	
	[FOPT'10]	This work
$(32, 2, 3, 24, 852, 621)$	462	**18**
$(27, 3, 2, 42, 1500, 1218)$	564	**26**
$(25, 3, 3, 25, 1206, 915)$	582	**57**
$(9, 3, 6, 14, 728, 542)$	372	**54**
$(31, 2, 3, 25, 856, 626)$	460	**228**

Our work vs existing algebraic modelling

	This work	[FOPT'10]
$\mathcal{W}(\boldsymbol{Z})$:	$\sum_j g_j Z_j{}^u$	$\sum_j g_j Y_j X_j{}^\ell$

g_j : public key entries,

X_j, Y_j, Z_j : unkowns

1. Compact : **fewer variables**.
2. Simpler equations to solve.
3. Non-prime q : exploits a weakness to reduce number of Z_j **for free**.

Code parameters $(q, m, \deg(g), \deg(f), n, k)$	Number of unkowns	
	[FOPT'10]	This work
$(32, 2, 3, 24, 852, 621)$	462	**18**
$(27, 3, 2, 42, 1500, 1218)$	564	**26**
$(25, 3, 3, 25, 1206, 915)$	582	**57**
$(9, 3, 6, 14, 728, 542)$	372	**54**
$(31, 2, 3, 25, 856, 626)$	460	**228**

Our work vs existing algebraic modelling

$$\mathcal{W}(\boldsymbol{Z}): \quad \underbrace{\sum_j g_j Z_j{}^u}_{\text{This work}} \qquad \underbrace{\sum_j g_j Y_j X_j{}^\ell}_{\text{[FOPT'10]}}$$

g_j : public key entries,

X_j, Y_j, Z_j : unkowns

1. Compact : **fewer variables**.
2. Simpler equations to solve.
3. Non-prime q : exploits a weakness to reduce number of Z_j **for free**.

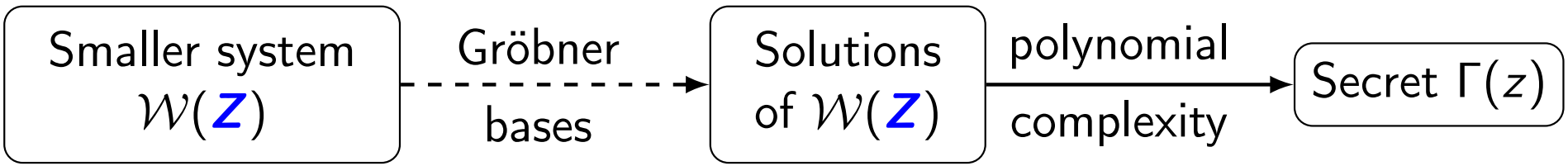
Code parameters $(q, m, \deg(g), \deg(f), n, k)$	Number of unkowns	
	[FOPT'10]	This work
$(32, 2, 3, 24, 852, 621)$	462	**18**
$(27, 3, 2, 42, 1500, 1218)$	564	**26**
$(25, 3, 3, 25, 1206, 915)$	582	**57**
$(9, 3, 6, 14, 728, 542)$	372	**54**
$(31, 2, 3, 25, 856, 626)$	460	**228**

Practical key recoveries

- Practical resolutions of $\mathcal{W}(\boldsymbol{Z})$ with Magma's F4.

Code parameters $(q, m, \deg(g), \deg(f), n, k)$	Unknowns	$\mathrm{F}_4(\mathcal{W}(\boldsymbol{Z}))$	ISD
$(32, 2, 3, 24, 852, 621)$	**18**	0.6 s	$\mathbf{2^{130}}$
$(27, 3, 2, 42, 1500, 1218)$	**26**	0.9 s	$\mathbf{2^{128}}$
$(25, 3, 3, 25, 1206, 915)$	**57**	1h 2 min	$\mathbf{2^{117}}$
$(9, 3, 6, 14, 728, 542)$	**54**	25h 13 min	$\mathbf{2^{81}}$
$(31, 2, 3, 25, 856, 626)$	**230**	∞	$\mathbf{2^{128}}$

- Complete key-recovery alorithm.



Construction of $\mathcal{W}(\boldsymbol{Z})$

Construction of $\mathcal{W}(\boldsymbol{Z})$

Goppa code

Secret $\boldsymbol{x} = (x_0, \ldots, x_{n-1}), \boldsymbol{y} = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_{q^m}^n (\iff \Gamma)$
Public $k \times n$ matrix $\boldsymbol{G}_{pub}$, $t = \deg(\Gamma)$.

Link between $\boldsymbol{G}_{pub}$ and secret :

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

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

Construction of $\mathcal{W}(\boldsymbol{Z})$

Goppa code

Secret $\boldsymbol{x} = (x_0, \ldots, x_{n-1}), \boldsymbol{y} = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_{q^m}^n (\iff \Gamma)$
Public $k \times n$ matrix $\boldsymbol{G}_{pub}$, $t = \deg(\Gamma)$.

$$
\begin{array}{lllll}
g_0 & y_0 & + \cdots + & g_{n-1} & y_{n-1} & = 0 \\
g_0 & y_0 x_0 & + \cdots + & g_{n-1} & y_{n-1} x_{n-1} & = 0 \\
 & & \vdots & & & \\
g_0 & y_0 x_0^{t-1} & + \cdots + & g_{n-1} & y_{n-1} x_{n-1}^{t-1} & = 0
\end{array}
$$

Construction of $\mathcal{W}(\boldsymbol{Z})$

Goppa code

Secret $\boldsymbol{x} = (x_0, \ldots, x_{n-1}), \boldsymbol{y} = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_{q^m}^n (\iff \Gamma)$
Public $k \times n$ matrix $\boldsymbol{G}_{pub}$, $t = \deg(\Gamma)$.

$$
\begin{array}{ccccccc}
g_0 & y_0 & + \cdots + & g_{n-1} & y_{n-1} & = 0 \\
g_0 & y_0 x_0 & + \cdots + & g_{n-1} & y_{n-1} x_{n-1} & = 0 \\
 & \vdots & & & & \\
g_0 & y_0 x_0^{t-1} & + \cdots + & g_{n-1} & y_{n-1} x_{n-1}^{t-1} & = 0 \\
 & \downarrow & & & \downarrow & \\
g_0 & Z_0 & + \cdots + & g_{n-1} & Z_{n-1} & = 0 \quad (\mathcal{E})
\end{array}
$$

Construction of $\mathcal{W}(\boldsymbol{Z})$

Goppa code

Secret $\boldsymbol{x} = (x_0, \ldots, x_{n-1}), \boldsymbol{y} = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_{q^m}^n (\iff \Gamma)$
Public $k \times n$ matrix $\boldsymbol{G}_{pub}$, $t = \deg(\Gamma)$.

$$
\begin{array}{ccccccc}
g_0 & y_0 & + \cdots + & g_{n-1} & y_{n-1} & = 0 \\
g_0 & y_0 x_0 & + \cdots + & g_{n-1} & y_{n-1} x_{n-1} & = 0 \\
 & \vdots & & & & \\
g_0 & y_0 x_0^{t-1} & + \cdots + & g_{n-1} & y_{n-1} x_{n-1}^{t-1} & = 0 \\
 & \downarrow & & & \downarrow & \\
g_0 & Z_0 & + \cdots + & g_{n-1} & Z_{n-1} & = 0 \quad (\mathcal{E})
\end{array}
$$

$$
\text{Row space of } \boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y}) = \begin{pmatrix} y_0 & \cdots & y_{n-1} \\ & \vdots & \\ y_0 x_0^{t-1} & \cdots & y_{n-1} x_{n-1}^{t-1} \end{pmatrix} \subset \text{Solutions of } (\mathcal{E})
$$

Construction of $\mathcal{W}(\boldsymbol{Z})$

$$\mathcal{E} : g_0 Z_0 + \cdots + g_{n-1} Z_{n-1} = 0 \quad (\mathbf{g} \text{ row of } \boldsymbol{G}_{pub})$$

$$\text{Row space of } \boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y}) \subset \text{Solutions of } (\mathcal{E})$$

Sidelnikov-Shestakov attack (1992)

Any basis of $\boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y})$'s row space

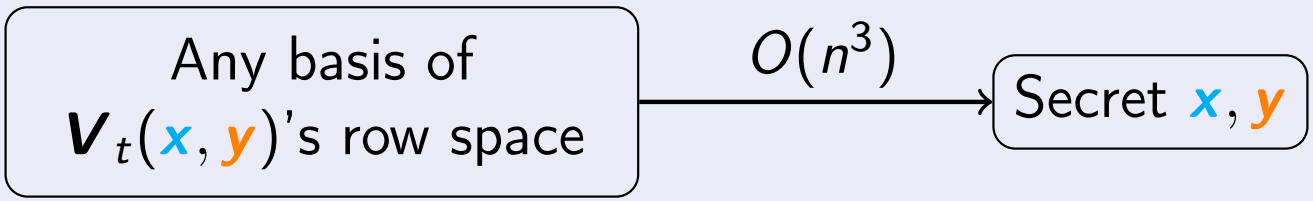
Secret $\boldsymbol{x}, \boldsymbol{y}$

Construction of $\mathcal{W}(\boldsymbol{Z})$

$$\mathcal{E} : g_0 Z_0 + \cdots + g_{n-1} Z_{n-1} = 0 \quad (\mathbf{g} \text{ row of } \boldsymbol{G}_{pub})$$

$$\text{Row space of } \boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y}) \subset \text{Solutions of } (\mathcal{E})$$

Sidelnikov-Shestakov attack (1992)

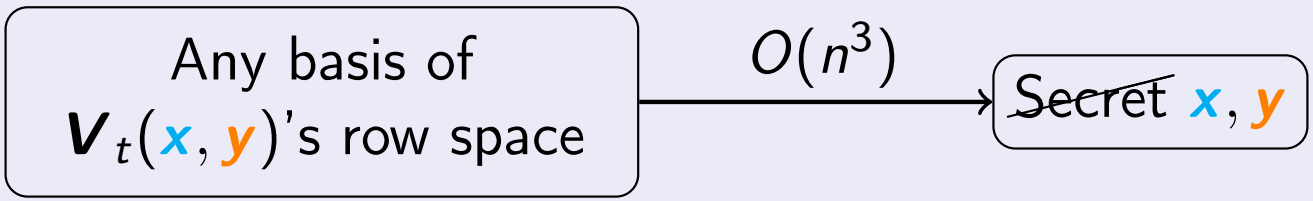


Construction of $\mathcal{W}(\boldsymbol{Z})$

$$\mathcal{E} : g_0 Z_0 + \cdots + g_{n-1} Z_{n-1} = 0 \quad (\mathbf{g} \text{ row of } \boldsymbol{G}_{pub})$$

$$\text{Row space of } \boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y}) \subset \text{Solutions of } (\mathcal{E})$$

Sidelnikov-Shestakov attack (1992)

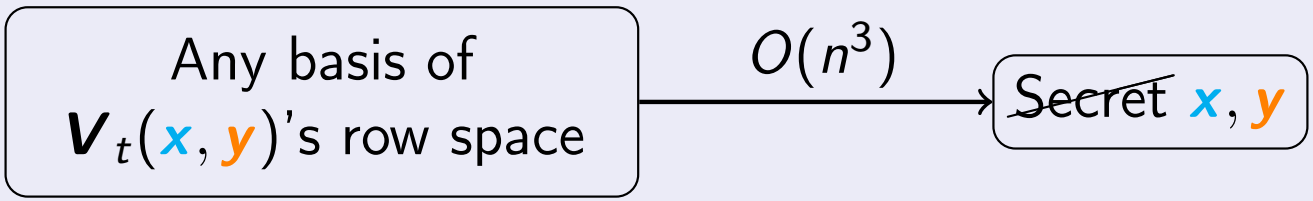


Construction of $\mathcal{W}(\boldsymbol{Z})$

$$\mathcal{E} : g_0 Z_0 + \cdots + g_{n-1} Z_{n-1} = 0 \quad (\mathbf{g} \text{ row of } \boldsymbol{G}_{pub})$$

$$\text{Row space of } \boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y}) \subsetneq \text{Solutions of } (\mathcal{E})$$

Sidelnikov-Shestakov attack (1992)



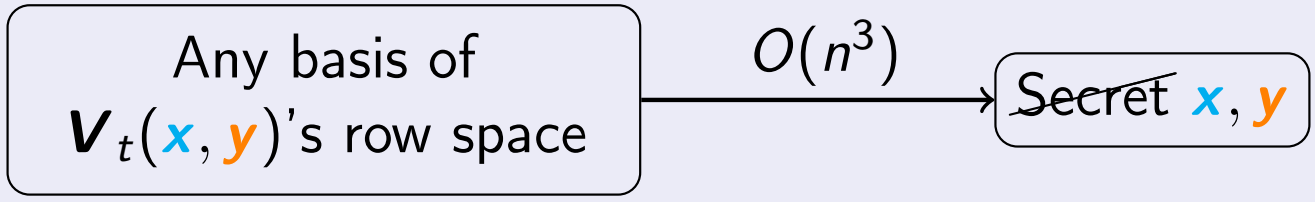
- Goppa : $(\mathcal{E})$ is **very underdefined** $\Longrightarrow$ no key-recovery.

Construction of $\mathcal{W}(\boldsymbol{Z})$

$$\mathcal{E} : g_0 Z_0 + \cdots + g_{n-1} Z_{n-1} = 0 \quad (\mathbf{g} \text{ row of } \boldsymbol{G}_{pub})$$

$$\text{Row space of } \boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y}) \subsetneq \text{Solutions of } (\mathcal{E})$$

Sidelnikov-Shestakov attack (1992)



- Goppa : $(\mathcal{E})$ is **very underdefined** $\implies$ no key-recovery.
- **This work.** Wild Goppa with $q>2$, we can write **more equations** !

Theorem (Algebraic System for Wild McEliece $\Gamma = fg^{q-1}$)

$$\mathcal{W}(\boldsymbol{Z}) = \{g_0 {Z_0}^u + \cdots + g_{n-1} {Z_{n-1}}^u = 0, 1 \leqslant u \leqslant q-1\}$$

has solutions exactly the row space of $\boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y})$.

Cryptanalysis strategy

Thm : $\mathcal{W}(\boldsymbol{Z}) = \{g_0 {Z_0}^u + \cdots + g_{n-1} {Z_{n-1}}^u = 0, 1 \leqslant u \leqslant q-1\}$ has solutions the row space of $\boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y})$ of rank $t = \deg(\Gamma)$.

1. Solve t times $\mathcal{W}(\boldsymbol{Z})$ with t variables fixed

$$\mathcal{W}(\boldsymbol{Z}) \bigcup \{\boldsymbol{Z} = (\underbrace{0, \ldots, 1, \ldots, 0,}_{\text{free variable elimination}} Z_t, \ldots, Z_{n-1})\}.$$

   $\rightarrow$ 1 basis element per resolution.

2. Deduce a basis of row space of $\boldsymbol{V}_t(\boldsymbol{x}, \boldsymbol{y})$:

$$\begin{pmatrix} 1 & \ldots & 0 & y_t Q_0(x_t) & \ldots & y_{n-1} Q_0(x_{n-1}) \\ 0 & \ddots & 0 & & \vdots & \\ 0 & & 1 & y_t Q_{t-1}(x_t) & \ldots & y_{n-1} Q_{t-1}(x_{n-1}) \end{pmatrix}$$

   Q_i polynomials of degree $\leqslant t-1$.

3. Recover secret $\boldsymbol{x}, \boldsymbol{y}, \Gamma = fg^{q-1}$ in $O(n^3)$ (adapted Sidel.-Shesta.)

More practical key-recoveries

Resolution of $\mathcal{W}(\boldsymbol{Z})$ with Magma's F_4 (Gröbner basis computation).

q	m	$\deg(g)$	$\deg(f)$	n	k	Unk.	$\mathrm{F}_4\,(\mathcal{W}(\boldsymbol{Z}))$	**ISD**	Key
☣32	2	4	0	841	593	24	16×10 s	$\mathbf{2^{128}}$	92 kB
☣27	3	4	0	1407	1095	52	20×(6 min 34 s)	$\mathbf{2^{128}}$	203 kB
☣16	3	6	0	1316	1046	54	18×(36h 26 min)	$\mathbf{2^{129}}$	141 kB
32*	2	3	24	852	621	18	12×0.6 s	$\mathbf{2^{130}}$	90 kB
27*	3	2	42	1500	1218	26	10×0.9 s	$\mathbf{2^{128}}$	204 kB
25	3	3	25	1206	915	57	15×(1h 2 min)	$\mathbf{2^{117}}$	155 kB
16*	3	6	16	1328	1010	54	18×(36h 35 min)	$\mathbf{2^{125}}$	160 kB
9	3	6	14	728	542	54	18×(25h 13 min)	$\mathbf{2^{81}}$	40 kB

☣ : Other potential weakness identified in

D. Bernstein, T. Lange, C. Peters.
Wild McEliece.
and patched in Incognito.

* : extracted from

D. Bernstein, T. Lange, C. Peters.
Wild McEliece Incognito.

This is the last slide

- In the article : more on the number of variables in $\mathcal{W}(\boldsymbol{Z})$
  - Extra-reduction when q non-prime.
  - Exact formula $\Longrightarrow$ criterion for design ?
- Overview
  - New algebraic modelling $\mathcal{W}(\boldsymbol{Z})$ dedicated to Wild Goppa codes.
  - Key-recoveries for parameters modelled by few variables (non-prime q's)
  - **Protection :** use large m,t, prime q.
  - Not relevant for binary Goppa codes (McEliece)
- Future work
  - **Complexity bounds** for solving $\mathcal{W}(\boldsymbol{Z})$ $\Longrightarrow$ criterion for design !

Thanks to the chairs for waiving my fees !