Square Code Attack on a Modified Sidelnikov Cryptosystem

Ayoub Otmani[1] Hervé Talé Kalachi[1,2]

[1]LITIS University of Rouen (France)

[2]ERAL University of Yaounde I (Cameroon)

May 23, 2015

Introduction

Linear code

1. Linear code = vector space over a finite field

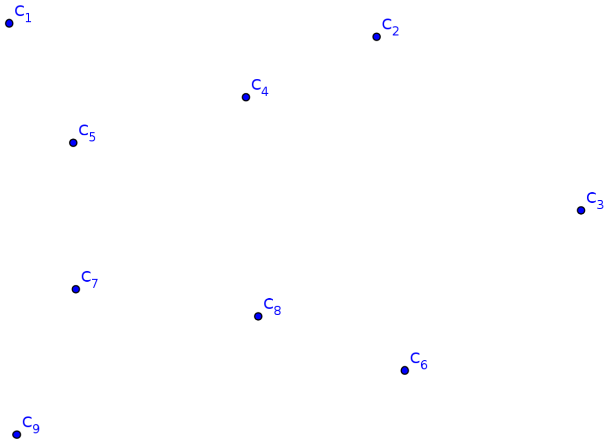
$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathbb{F}_q \, \vec{v}_i$$

   where $\vec{v}_i$ are linearly independent.

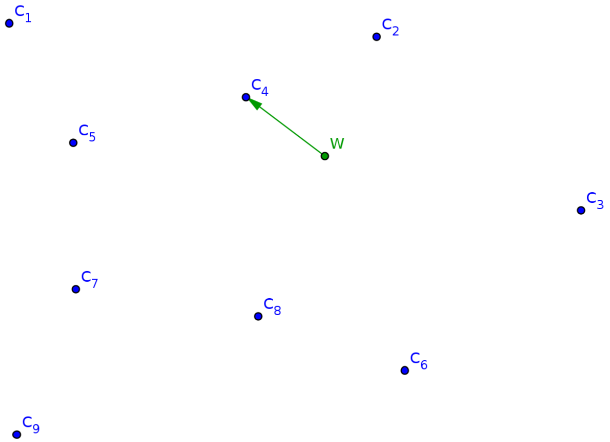
2. Any $k \times n$ matrix $\boldsymbol{G}$ whose rows form a basis of $\mathscr{C}$ is a generator matrix of $\mathscr{C}$.

3. Decoding a word $\vec{w} \in \mathbb{F}_q^n$ = Closest Vector Problem (CVP) for the Hamming metric

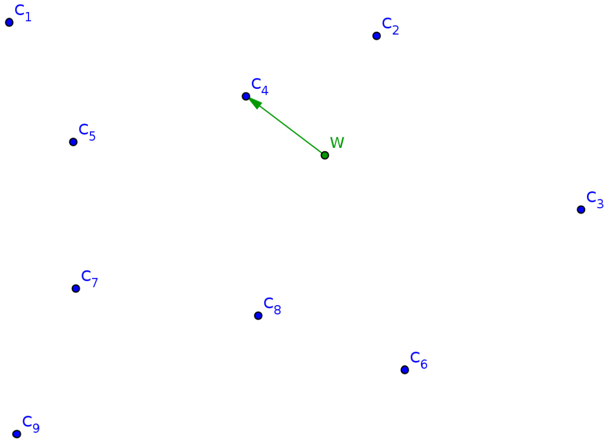
Introduction



Introduction



Introduction



- Decoding is NP-Hard for a random linear code (Berlekamp-McEliece-Van Tilborg '78)

Introduction

McEliece Public-Key Encryption Scheme ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm
2. McEliece proposed binary Goppa codes

McEliece Variants

1. GRS codes by Niederreiter '86
2. Binary Reed-Muller codes by Sidelnikov '94

Introduction

Designing hiding methods

1. Several families do not behave like random codes. eg.
   - GRS codes → Sidelnikov-Shestakov's attack '94
   - Reed-Muller code → Minder-Shokrollahi's attack '07
2. Adding some randomness
   - Berger-Loidreau '05 → Random subcode
   - Wieschebrink '06 → Random columns with GRS
   - Gueye-Mboup '13 → Random columns with Reed-Muller codes

Our contribution

Cryptanalysis of Gueye-Mboup's proposal

Outline

Plan

McEliece Encryption Scheme

Parameters setup

- Let $\mathscr{G}_{n,k,t}$ be a collection of codes of length n and dimension k that can decode t errors
- Choose n, k and t according to a security parameter

Key generation

- Randomly pick $\mathscr{C} \in \mathscr{G}_{n,k,t}$
- Choose a generator matrix $\boldsymbol{G}$ of $\mathscr{C}$ and let $f_{\boldsymbol{G}}$ be a decoding algorithm associated to $\boldsymbol{G}$
- Randomly pick $n \times n$ permutation matrix $\boldsymbol{P}$ and $k \times k$ invertible matrix $\boldsymbol{S}$
- Private key $= (\boldsymbol{S}, \boldsymbol{G}, \boldsymbol{P})$ and public key $= (\boldsymbol{G}_{pub}, t)$ with

$$\boldsymbol{G}_{pub} = \boldsymbol{SGP}$$

McEliece Encryption Scheme

Encryption

For $\vec{m} \in \mathbb{F}_q^k$,

1. Generate randomly $\vec{e} \in \mathbb{F}_q^n$ of Hamming weight t
2. Cipher text $\vec{c} = \vec{m}\boldsymbol{G}_{pub} + \vec{e}$

Decryption

1. Compute $\vec{z} = \vec{c}\boldsymbol{P}^{-1}$ $\qquad \vec{z} = \vec{m}\boldsymbol{S}\boldsymbol{G} + \vec{e}\boldsymbol{P}^{-1}$
2. Compute $\vec{y} = f_{\boldsymbol{G}}(\vec{z})$ $\qquad \vec{y} = \vec{m}\boldsymbol{S}$
3. Return $\vec{m}' = \vec{y}\boldsymbol{S}^{-1}$ $\qquad \vec{m}' = \vec{m}$

Wieschebrink's Variant

Key generation

1. Pick at random $k \times n$ generator matrix $\boldsymbol{G}$
2. Pick at random $k \times \ell$ matrix $\boldsymbol{R}$
3. Pick at random $k \times k$ invertible matrix $\boldsymbol{S}$ and a $(n+\ell) \times (n+\ell)$ permutation matrix $\boldsymbol{P}$
4. Public generator matrix is $\boldsymbol{G}_{pub} = \boldsymbol{S}(\boldsymbol{G} \mid \boldsymbol{R})\boldsymbol{P}$

Decryption

Eliminate the ℓ random components of the cipher text

Security

Number of errors t has to be increased $\rightsquigarrow$ decryption failure

Different Proposals

1. Wieschebrink ('06) based on GRS codes

   $\rightarrow$ cryptanalysed using component-wise product of codes by Couvreur-Gaborit-Gautier-Otmani-Tillich ('13)

2. Gueye and Mboup ('13) based on Reed-Muller codes

Different Proposals

1. Wieschebrink ('06) based on GRS codes

   $\rightarrow$ cryptanalysed using component-wise product of codes by Couvreur-Gaborit-Gautier-Otmani-Tillich ('13)

2. Gueye and Mboup ('13) based on Reed-Muller codes

Plan

Componentwise products based attacks

Definition 1 (Componentwise products)

Let $\vec{a} = (a_1, ..., a_n)$ and $\vec{b} = (b_1, ..., b_n)$ in $\mathbb{F}_q^n$

$$\vec{a} \star \vec{b} \overset{def}{=} (a_1 b_1, ..., a_n b_n)$$

Definition 2 (Star product code)

- $\mathscr{A}$ and $\mathscr{B}$ are two codes of length n.
- $\mathscr{A} \star \mathscr{B} \overset{\text{def}}{=} \left\{ \vec{a} \star \vec{b} : \vec{a} \in \mathscr{A}, \vec{b} \in \mathscr{B} \right\}$.
- $\mathscr{B} = \mathscr{A} \to \mathscr{A}^2$

Remark 1

The star product of codes was first used by Wieschebrink '11 to attack the Berger-Loidreau Scheme.

Recent attacks using the star product

Date	Scheme	Attack	Complexity
2013	Homomorphic RS	Couvreur-Gaborit-Gauthier-Otmani-Tillich	polynomial
2013	GRS	Couvreur-Gaborit-Gauthier-Otmani-Tillich	polynomial
2013	GRS with $\boldsymbol{P}+\boldsymbol{R}$	Couvreur-Gaborit-Gauthier-Otmani-Tillich	polynomial
2013	GRS + random col	Couvreur-Gaborit-Gauthier-Otmani-Tillich	polynomial
2013	$\mathcal{RM}(r,m)$	Chizhov-Borodin	polynomial
2014	wild McEliece $m=2$	Couvreur-Otmani-Tillich	polynomial
2014	AG	Couvreur-Màrquez Corbella-Pellikaan	polynomial

Behavior of the Star Product

Proposition 1

$\mathscr{A}$ and $\mathscr{B}$ are two linear codes of length n.

1. $$dim(\mathscr{A} \star \mathscr{B}) \leqslant dim(\mathscr{A})dim(\mathscr{B})$$
2. $$dim(\mathscr{A}^2) \leqslant \binom{dim(\mathscr{A})+1}{2}$$

- Random code $\mathscr{A}$

$$dim(\mathscr{A}^2) = \binom{dim(\mathscr{A})+1}{2} \quad \text{with high probability}$$

- GRS code $\mathscr{A}$

$$dim(\mathscr{A}^2) = 2dim(\mathscr{A}) - 1$$

Reed-Muller Code

Definition 3

- Let r, m and n such that $0 \leqslant r \leqslant m$ and $n = 2^m$
- $\mathcal{BP}(r, m)$ the set of boolean polynomials of m variables with degree $\leqslant r$
- $\mathbb{F}_2^m = \{a_1, \ldots, a_n\}$

$$\mathcal{RM}(r, m) \stackrel{\text{def}}{=} \Big\{(f(a_1), \ldots, f(a_n)) \;/\; f \in \mathcal{BP}(r, m) \Big\}$$

Proposition 2

$$\mathcal{RM}(r, m)^2 = \mathcal{RM}(2r, m)$$

Description of our Attack – Preliminaries

Assumptions

- Let $\mathcal{RM}(r, m)$ be a Reed-Muller code such that

$$\dim(\mathcal{RM}(2r, m)) + \ell \leqslant n$$

- $\boldsymbol{G}_{pub}$ = public generator matrix of the Gueye-Mboup scheme
- $\mathscr{C}_{pub}$ the code generated by $\boldsymbol{G}_{pub}$

Proposition 3

$$\dim(\mathscr{C}^2_{pub}) = \dim(\mathcal{RM}(2r, m)) + \ell \quad \textit{with a high probability}$$

Description of our Attack

Definition 4 (Punctured code)

The punctured code of $\mathscr{C}$ at position i consists in removing the i^{th} coordinate of each element of $\mathscr{C}$

First step – Detection of random part

Let $\mathscr{D}_i$ be the punctured code of $\mathscr{C}_{pub}$ at i:

- i is a random position

$$dim(\mathscr{D}_i^2) = \ell - 1 + \dim(\mathcal{RM}(2r, m))$$

- i is not a random position

$$dim(\mathscr{D}_i^2) = \ell + \dim(\mathcal{RM}(2r, m))$$

Last step

Use the attack of [Minder, L. and Shokrollahi, M.A.] or the attack of [Chizhov, I.V., Borodin, M.A]

Our Attack

Complexity

- We use at most $O(k^2n^2)$ operations for each computation of $dim(\mathscr{D}_i^2)$ and this at most n times
- So the overall complexity for guessing the random columns is $O(n^5)$

Intel® Xeon Quad core @ 2.60GHz

(m, r, ℓ)	Time
$(9, 3, 10)$	32 minutes
$(10, 3, 10)$	3 Hours 13 minutes
$(11, 3, 10)$	23 Hours 36 minutes

Our Attack

Complexity

- We use at most $O(k^2n^2)$ operations for each computation of $dim(\mathscr{D}_i^2)$ and this at most n times
- So the overall complexity for guessing the random columns is $O(n^5)$

Intel® Xeon Quad core @ 2.60GHz

(m, r, ℓ)	Time
$(9, 3, 10)$	32 minutes
$(10, 3, 10)$	3 Hours 13 minutes
$(11, 3, 10)$	23 Hours 36 minutes

Plan

Conclusion

- Sidelnikov '94, Modified McEliece Cryptosystem based on Reed-Muller codes
- Minder-Shokrollahi '07, sub-exponential attack on the Sidelnikov cryptosystem
- Gueye-Mboup '13, Modified Sidelnikov cryptosystem with Random columns for more security

Our attack

This work shows that the random columns in the Sidelnikov scheme does not bring any security improvement

Conclusion

Chizhov-Borodin '13

- Attack on Sidelnikov cryptosystem,
- The attack is based on star product
- Polynomial, but only for some kind of parameters

$$\mathcal{RM}(r,m) : \gcd(r,m) = 1$$

A new challenge

Propose a polynomial time attack (using star product) on the Sidelnikov cryptosystem, without restriction on r and m