Code-Based Cryptography

1. Error-Correcting Codes and Cryptography
2. McEliece Cryptosystem
3. Message Attacks (ISD)
4. **Key Attacks**
5. Other Cryptographic Constructions Relying on Coding Theory

4. Key Attacks

1. Introduction
2. Support Splitting Algorithm
3. Distinguisher for GRS codes
4. Attack against subcodes of GRS codes
5. Error-Correcting Pairs
6. Attack against GRS codes
7. **Attack against Reed-Muller codes**
8. Attack against Algebraic Geometry codes
9. Goppa codes still resist

Reed-Muller codes

- Were introduced by **D. Muller** in 1954.
- **I. Reed** provided an efficient decoding algorithm.

D. E. Muller.
Application of boolean algeba to switching circuit desing and to error detection.
IEEE Trans. on Computers, 3:6—12, 1954.

I. S. Reed.
A class of multiple-error correcting codes and the decoding scheme.
IEEE Trans. on Information Theory, 4:38—49, 1954.

Reed-Muller codes

- Were introduced by **D. Muller** in 1954.
- **I. Reed** provided an efficient decoding algorithm.

D. E. Muller.
Application of boolean algeba to switching circuit desing and to error detection.
IEEE Trans. on Computers, 3:6—12, 1954.

I. S. Reed.
A class of multiple-error correcting codes and the decoding scheme.
IEEE Trans. on Information Theory, 4:38—49, 1954.

Reed-Solomon codes

Univariate polynomials

Reed-Muller codes

- Were introduced by **D. Muller** in 1954.
- **I. Reed** provided an efficient decoding algorithm.

D. E. Muller.
Application of boolean algeba to switching circuit desing and to error detection.
IEEE Trans. on Computers, 3:6—12, 1954.

I. S. Reed.
A class of multiple-error correcting codes and the decoding scheme.
IEEE Trans. on Information Theory, 4:38—49, 1954.

Reed-Solomon codes

Univariate polynomials

Reed-Muller codes

Multivariate polynomials

Binary Reed-Muller codes

Reed-Muller codes

$$\mathcal{R}(r, m) = \{f(\alpha)_{|\alpha \in \mathbb{F}_2^n} \mid f \in \mathbb{F}_2[X_1, \ldots, X_m] \text{ and } \deg(f) \leq r\}$$

Binary Reed-Muller codes

Reed-Muller codes

$$\mathcal{R}(r, m) = \{ f(\alpha)_{|\alpha \in \mathbb{F}_2^n} \mid f \in \mathbb{F}_2[X_1, \ldots, X_m] \text{ and } \deg(f) \leq r \}$$

Total degree bound

Binary Reed-Muller codes

Reed-Muller codes

$$\mathcal{R}(r, m) = \{f(\alpha)_{|\alpha \in \mathbb{F}_2^n} \mid f \in \mathbb{F}_2[X_1, \ldots, X_m] \text{ and } \deg(f) \leq r\}$$

Total degree bound

Number of Variables

Binary Reed-Muller codes

Reed-Muller codes

$$\mathcal{R}(r, m) = \{ f(\alpha)|_{\alpha \in \mathbb{F}_2^n} \mid f \in \mathbb{F}_2[X_1, \ldots, X_m] \text{ and } \deg(f) \leq r \}$$

Total degree bound

Number of Variables

Parameters of $\mathcal{R}(r, m)$

Block Length: $n = 2^m$

Binary Reed-Muller codes

Reed-Muller codes

$$\mathcal{R}(r, m) = \{f(\alpha)_{|\alpha \in \mathbb{F}_2^n} \mid f \in \mathbb{F}_2[X_1, \ldots, X_m] \text{ and } \deg(f) \leq r\}$$

Total degree bound (r)

Number of Variables (m)

Parameters of $\mathcal{R}(r, m)$

Block Length: $n = 2^m$

Dimension: "Number of polynomials in $\mathbb{F}_2[X_1, \ldots, X_n]$ of degree $\leq r$" : $k = \sum_{i=0}^{r} \binom{m}{i}$

Binary Reed-Muller codes

Reed-Muller codes

$$\mathcal{R}(r, m) = \{f(\alpha)_{|\alpha \in \mathbb{F}_2^n} \mid f \in \mathbb{F}_2[X_1, \ldots, X_m] \text{ and } \deg(f) \leq r\}$$

Total degree bound (r)

Number of Variables (m)

Parameters of $\mathcal{R}(r, m)$

Block Length: $n = 2^m$

Minimum Distance: $d = 2^{m-r}$

Dimension: "Number of polynomials in $\mathbb{F}_2[X_1, \ldots, X_n]$ of degree $\leq r$" : $k = \sum_{i=0}^{r} \binom{m}{i}$

Binary Reed Muller codes - Example

Consider the code $\mathcal{R}(1,3)$

This code is an $[8,4,4]_2$ code .

The monomials in $\mathbb{F}_2[X_1, X_2, X_3]$ up to degree 1 are: $\{\mathbf{1}, X_1, X_2, X_3\}$

The vectors in $\mathbb{F}_2^8$ associated to these monomials are:

$$
\begin{array}{ccc}
\mathbf{1} & \longrightarrow & (11111111) \\
X_1 & \longrightarrow & (01010101) \\
X_2 & \longrightarrow & (00110011) \\
X_3 & \longrightarrow & (00001111)
\end{array}
$$

Binary Reed Muller codes - Example

Consider the code $\mathcal{R}(1,3)$

This code is an $[8,4,4]_2$ code.

The monomials in $\mathbb{F}_2[X_1, X_2, X_3]$ up to degree 1 are: $\{\mathbf{1}, X_1, X_2, X_3\}$

The vectors in $\mathbb{F}_2^8$ associated to these monomials are:

$$\begin{array}{lcl} \mathbf{1} & \longrightarrow & (11111111) \\ X_1 & \longrightarrow & (01010101) \\ X_2 & \longrightarrow & (00110011) \\ X_3 & \longrightarrow & (00001111) \end{array}$$

$\longrightarrow$ **Generator matrix for $\mathcal{R}(1,3)$**

Binary Reed Muller codes - Example

Consider the code $\mathcal{R}(1,3)$

This code is an $[8,4,4]_2$ code.

The monomials in $\mathbb{F}_2[X_1, X_2, X_3]$ up to degree 1 are: $\{\mathbf{1}, X_1, X_2, X_3\}$

The vectors in $\mathbb{F}_2^8$ associated to these monomials are:

$$\begin{array}{lcl} \mathbf{1} & \longrightarrow & (11111111) \\ X_1 & \longrightarrow & (01010101) \\ X_2 & \longrightarrow & (00110011) \\ X_3 & \longrightarrow & (00001111) \end{array}$$

Generator matrix for $\mathcal{R}(1,3)$

The code $\mathcal{R}(1,m)$ has a particular shape

(After removing the first row)

Binary Reed Muller codes - Example

Consider the code $\mathcal{R}(1, 3)$

This code is an $[8, 4, 4]_2$ code .

The monomials in $\mathbb{F}_2[X_1, X_2, X_3]$ up to degree 1 are: $\{\mathbf{1}, X_1, X_2, X_3\}$

The vectors in $\mathbb{F}_2^8$ associated to these monomials are:

$$
\begin{array}{lcl}
\mathbf{1} & \longrightarrow & (11111111) \\
X_1 & \longrightarrow & (01010101) \\
X_2 & \longrightarrow & (00110011) \\
X_3 & \longrightarrow & (00001111)
\end{array}
$$

Generator matrix for $\mathcal{R}(1, 3)$

The code $\mathcal{R}(1, m)$ has a particular shape

(After removing the first row)

The i-th column is the $(i-1)_2$ number

(read as a binary number)

Binary Reed Muller codes - Example

Consider the code $\mathcal{R}(2,4)$ This code is an $[16,11,4]_2$ code .

The monomials in $\mathbb{F}_2[X_1,X_2,X_3,X_4]$ up to degree 1 are:

$$\{\mathbf{1}, X_1, X_2, X_3, X_4, X_1X_2, X_1X_3, X_1X_4, X_2X_3, X_2X_4, X_3X_4\}$$

The vectors in $\mathbb{F}_2^{16}$ associated to these monomials are:

$$\begin{array}{lcl}
\mathbf{1} & \longrightarrow & (\ 11111111 \quad 11111111\ ) \\
X_1 & \longrightarrow & (\ 01010101 \quad 01010101\ ) \\
X_2 & \longrightarrow & (\ 00110011 \quad 00110011\ ) \\
X_3 & \longrightarrow & (\ 00001111 \quad 00001111\ ) \\
X_4 & \longrightarrow & (\ 00000000 \quad 11111111\ ) \\
X_1X_2 & \longrightarrow & (\ 00010001 \quad 00010001\ ) \\
X_1X_3 & \longrightarrow & (\ 00000101 \quad 00000101\ ) \\
X_1X_4 & \longrightarrow & (\ 00000000 \quad 01010101\ ) \\
X_2X_3 & \longrightarrow & (\ 00000011 \quad 00000011\ ) \\
X_2X_4 & \longrightarrow & (\ 00000000 \quad 00110011\ ) \\
X_3X_4 & \longrightarrow & (\ 00000000 \quad 00001111\ )
\end{array}$$

Binary Reed Muller codes - Example

Consider the code $\mathcal{R}(2,4)$ This code is an $[16, 11, 4]_2$ code.

The monomials in $\mathbb{F}_2[X_1, X_2, X_3, X_4]$ up to degree 1 are:

$$\{\mathbf{1}, X_1, X_2, X_3, X_4, X_1X_2, X_1X_3, X_1X_4, X_2X_3, X_2X_4, X_3X_4\}$$

The vectors in $\mathbb{F}_2^{16}$ associated to these monomials are:

$$
\begin{array}{lcl}
\mathbf{1} & \longrightarrow & (\ 11111111 \quad 11111111\ ) \\
X_1 & \longrightarrow & (\ 01010101 \quad 01010101\ ) \\
X_2 & \longrightarrow & (\ 00110011 \quad 00110011\ ) \\
X_3 & \longrightarrow & (\ 00001111 \quad 00001111\ ) \\
X_4 & \longrightarrow & (\ 00000000 \quad 11111111\ ) \\
X_1X_2 & \longrightarrow & (\ 00010001 \quad 00010001\ ) \\
X_1X_3 & \longrightarrow & (\ 00000101 \quad 00000101\ ) \\
X_1X_4 & \longrightarrow & (\ 00000000 \quad 01010101\ ) \\
X_2X_3 & \longrightarrow & (\ 00000011 \quad 00000011\ ) \\
X_2X_4 & \longrightarrow & (\ 00000000 \quad 00110011\ ) \\
X_3X_4 & \longrightarrow & (\ 00000000 \quad 00001111\ )
\end{array}
$$

Generator matrix for $\mathcal{R}(2,4)$

Properties of Reed Muller codes

Properties:

Properties of Reed Muller codes

Properties:

Property 1. $\mathcal{R}(0, m) \subseteq \mathcal{R}(1, m) \subseteq \ldots \subseteq \mathcal{R}(m, m)$

Properties of Reed Muller codes

Properties:

Property 1. $\mathcal{R}(0, m) \subseteq \mathcal{R}(1, m) \subseteq \ldots \subseteq \mathcal{R}(m, m)$

Property 2. $\mathcal{R}(m, m) = \mathbb{F}_2^n$

Properties of Reed Muller codes

Properties:

Property 1. $\mathcal{R}(0,m) \subseteq \mathcal{R}(1,m) \subseteq \ldots \subseteq \mathcal{R}(m,m)$

Property 2. $\mathcal{R}(m,m) = \mathbb{F}_2^n$

Property 3. $\mathcal{R}(r,m)^{\perp} = \mathcal{R}(m-r-1,m)$

Proof: Take notice that:

1. $\dim(\mathcal{R}(r,m)) + \dim(\mathcal{R}(m-r-1,m)) = 2^m$
2. $\mathcal{R}(r,m) * \mathcal{R}(m-r-1,m) = \mathcal{R}(m-1,m)$
3. The code $\mathcal{R}(m-1,m)$ is the code of all even weight vectors.

Properties of Reed Muller codes

Properties:

Property 1. $\mathcal{R}(0, m) \subseteq \mathcal{R}(1, m) \subseteq \ldots \subseteq \mathcal{R}(m, m)$

Property 2. $\mathcal{R}(m, m) = \mathbb{F}_2^n$

Property 3. $\mathcal{R}(r, m)^{\perp} = \mathcal{R}(m - r - 1, m)$

We will use the following operations:

Properties of Reed Muller codes

Properties:

Property 1. $\mathcal{R}(0,m) \subseteq \mathcal{R}(1,m) \subseteq \ldots \subseteq \mathcal{R}(m,m)$

Property 2. $\mathcal{R}(m,m) = \mathbb{F}_2^n$

Property 3. $\mathcal{R}(r,m)^{\perp} = \mathcal{R}(m-r-1,m)$

We will use the following operations:

$\star$: $\mathcal{R}(r_1,m), \mathcal{R}(r_2,m) \xrightarrow{\mathcal{O}(n^4) \text{ bit operations}} \mathcal{R}(r_1+r_2,m)$ if $r_1 + r_2 \leq m-2$

Properties of Reed Muller codes

Properties:

Property 1. $\mathcal{R}(0, m) \subseteq \mathcal{R}(1, m) \subseteq \ldots \subseteq \mathcal{R}(m, m)$

Property 2. $\mathcal{R}(m, m) = \mathbb{F}_2^n$

Property 3. $\mathcal{R}(r, m)^{\perp} = \mathcal{R}(m - r - 1, m)$

We will use the following operations:

$\star$: $\mathcal{R}(r_1, m), \mathcal{R}(r_2, m) \xrightarrow{\mathcal{O}(n^4) \text{ bit operations}} \mathcal{R}(r_1 + r_2, m)$ if $r_1 + r_2 \leq m - 2$

$\perp$: $\mathcal{R}(r, m) \xrightarrow{\mathcal{O}(n^3) \text{ bit operations}} \mathcal{R}(m - r - 1, m)$

Properties of Reed Muller codes

Properties:

Property 1. $\mathcal{R}(0,m) \subseteq \mathcal{R}(1,m) \subseteq \ldots \subseteq \mathcal{R}(m,m)$

Property 2. $\mathcal{R}(m,m) = \mathbb{F}_2^n$

Property 3. $\mathcal{R}(r,m)^{\perp} = \mathcal{R}(m-r-1,m)$

We will use the following operations:

$\star$: $\mathcal{R}(r_1,m), \mathcal{R}(r_2,m) \xrightarrow{\mathcal{O}(n^4) \text{ bit operations}} \mathcal{R}(r_1+r_2,m)$ if $r_1+r_2 \leq m-2$

$\perp$: $\mathcal{R}(r,m) \xrightarrow{\mathcal{O}(n^3) \text{ bit operations}} \mathcal{R}(m-r-1,m)$

$\ominus$: $\mathcal{R}(r,m) \xrightarrow{\mathcal{O}(n^r) \text{ bit operations}} \mathcal{R}(r-1,m)$

We need to find minimum weight codewords.

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r, m) \xrightarrow{\mathcal{O}(n^4) \text{ bit operations}} \mathcal{R}(t, m)$

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r, m) \xrightarrow{\mathcal{O}(n^4) \text{ bit operations}} \mathcal{R}(t, m)$

Proof: We study 3 posible cases:

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r, m) \xrightarrow{\mathcal{O}(n^4) \text{ bit operations}} \mathcal{R}(t, m)$

Proof: We study 3 posible cases:

1. $a = 0, \quad b > 0$

$$\mathcal{R}(r, m) \xrightarrow{b \text{ times } \star} \mathcal{R}(br, m) = \mathcal{R}(t, m)$$

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r, m) \xrightarrow{\mathcal{O}(n^4)\ \text{bit operations}} \mathcal{R}(t, m)$

Proof: We study 3 posible cases:

1. $a = 0, \quad b > 0$

   $\mathcal{R}(r, m) \xrightarrow{b \ \text{times} \ \star} \mathcal{R}(br, m) = \mathcal{R}(t, m)$

2. $a \geq 0, \quad b < 0$,

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r,m) \xrightarrow{\mathcal{O}(n^4)\ \text{bit operations}} \mathcal{R}(t,m)$

Proof: We study 3 posible cases:

1. $a = 0,\ \ b > 0$

   $\mathcal{R}(r,m) \xrightarrow{b\ \ \text{times}\ \ \star} \mathcal{R}(br,m) = \mathcal{R}(t,m)$

2. $a \geq 0,\ \ b < 0,$ **i.e.** $b = -qa + s$ **with** $0 \leq s \leq a-1$

$\mathcal{R}(r,m)$

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r,m) \xrightarrow{\mathcal{O}(n^4)\text{ bit operations}} \mathcal{R}(t,m)$

Proof: We study 3 posible cases:

1. $a = 0,\ \ b > 0$

   $$\mathcal{R}(r,m) \xrightarrow{b\ \text{times}\ \star} \mathcal{R}(br,m) = \mathcal{R}(t,m)$$

2. $a \geq 0,\ \ b < 0$, **i.e.** $b = -qa + s$ **with** $0 \leq s \leq a-1$

$$\mathcal{R}(r,m) \xrightarrow{q\ \text{times}\ \star} \mathcal{R}(qr,m)$$

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r,m) \xrightarrow{\mathcal{O}(n^4)\ \text{bit operations}} \mathcal{R}(t,m)$

Proof: We study 3 posible cases:

1. $a = 0, \quad b > 0$

$$\mathcal{R}(r,m) \xrightarrow{b \ \text{times} \ \star} \mathcal{R}(br,m) = \mathcal{R}(t,m)$$

2. $a \geq 0, \quad b < 0,$ **i.e.** $b = -qa + s$ **with** $0 \leq s \leq a-1$

$$\mathcal{R}(r,m) \xrightarrow{q \ \text{times} \ \star} \mathcal{R}(qr,m) \xrightarrow{\perp} \mathcal{R}(m-1-qr,m)$$

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r,m) \xrightarrow{\mathcal{O}(n^4) \text{ bit operations}} \mathcal{R}(t,m)$

Proof: We study 3 posible cases:

1. $a = 0, \quad b > 0$

$$\mathcal{R}(r,m) \xrightarrow{b \text{ times } \star} \mathcal{R}(br,m) = \mathcal{R}(t,m)$$

2. $a \geq 0, \quad b < 0,$ **i.e.** $b = -qa + s$ **with** $0 \leq s \leq a-1$

$$\mathcal{R}(r,m) \xrightarrow{q \text{ times } \star} \mathcal{R}(qr,m) \xrightarrow{\perp} \mathcal{R}(m-1-qr,m) \xrightarrow{a \text{ times } \star} \mathcal{R}\left(a(m-1-qr),m\right)$$

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r,m) \xrightarrow{\mathcal{O}(n^4)\text{ bit operations}} \mathcal{R}(t,m)$

Proof: We study 3 posible cases:

1. $a = 0, \quad b > 0$

$$\mathcal{R}(r,m) \xrightarrow{b \text{ times } \star} \mathcal{R}(br,m) = \mathcal{R}(t,m)$$

2. $a \geq 0, \quad b < 0,$ **i.e.** $b = -qa + s$ **with** $0 \leq s \leq a-1$

$$\mathcal{R}(r,m) \xrightarrow{q \text{ times } \star} \mathcal{R}(qr,m) \xrightarrow{\perp} \mathcal{R}(m-1-qr,m) \xrightarrow{a \text{ times } \star} \mathcal{R}\left(a(m-1-qr),m\right)$$

$$\mathcal{R}(r,m)$$

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r,m) \xrightarrow{\mathcal{O}(n^4)\text{ bit operations}} \mathcal{R}(t,m)$

Proof: We study 3 posible cases:

1. $a = 0, \ \ b > 0$

$$\mathcal{R}(r,m) \xrightarrow{b \ \text{times} \ \star} \mathcal{R}(br,m) = \mathcal{R}(t,m)$$

2. $a \geq 0, \ \ b < 0,$ **i.e.** $b = -qa + s$ **with** $0 \leq s \leq a-1$

$$\mathcal{R}(r,m) \xrightarrow{q \ \text{times} \ \star} \mathcal{R}(qr,m) \xrightarrow{\perp} \mathcal{R}(m-1-qr,m) \xrightarrow{a \ \text{times} \ \star} \mathcal{R}\left(a(m-1-qr),m\right)$$

$$\mathcal{R}(r,m) \xrightarrow{s \ \text{times} \ \star} \mathcal{R}(sr,m)$$

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r,m) \xrightarrow{\mathcal{O}(n^4) \text{ bit operations}} \mathcal{R}(t,m)$

Proof: We study 3 posible cases:

1. $a = 0, \;\; b > 0$

   $$\mathcal{R}(r,m) \xrightarrow{b \;\; \text{times} \;\; \star} \mathcal{R}(br,m) = \mathcal{R}(t,m)$$

2. $a \geq 0, \;\; b < 0,$ **i.e.** $b = -qa + s$ **with** $0 \leq s \leq a-1$

$$\mathcal{R}(r,m) \xrightarrow{q \;\; \text{times} \;\; \star} \mathcal{R}(qr,m) \xrightarrow{\perp} \mathcal{R}(m-1-qr,m) \xrightarrow{a \;\; \text{times} \;\; \star} \mathcal{R}\left(a(m-1-qr),m\right)$$

$$\mathcal{R}(r,m) \xrightarrow{s \;\; \text{times} \;\; \star} \mathcal{R}(sr,m)$$

3. $a \leq 0, \;\; b > 0$

Properties of Reed Muller codes

Proposition [Chizhov - Borodin]

Let $t = a(m-1) + br$. Then, $\mathcal{R}(r,m) \xrightarrow{\mathcal{O}(n^4) \text{ bit operations}} \mathcal{R}(t,m)$

Proof: We study 3 posible cases:

1. $a = 0, \quad b > 0$

$$\mathcal{R}(r,m) \xrightarrow{b \text{ times } \star} \mathcal{R}(br,m) = \mathcal{R}(t,m)$$

2. $a \geq 0, \quad b < 0,$ **i.e.** $b = -qa + s$ **with** $0 \leq s \leq a-1$

$$\mathcal{R}(r,m) \xrightarrow{q \text{ times } \star} \mathcal{R}(qr,m) \xrightarrow{\perp} \mathcal{R}(m-1-qr,m) \xrightarrow{a \text{ times } \star} \mathcal{R}\left(a(m-1-qr),m\right)$$

$$\mathcal{R}(r,m) \xrightarrow{s \text{ times } \star} \mathcal{R}(sr,m)$$

3. $a \leq 0, \quad b > 0$

Take notice that $m-1-t = \underbrace{(1-a)}_{a' \geq 0}(m-1) - br$. Apply **case 2** to $\mathcal{R}(m-1-t,m)$

Reed-Muller codes for the McEliece scheme

Reed-Muller codes

V. Sidelnikov.
A public-key cryptosytem based on Reed-Muller codes.
Discrete Math. Appl., 4(3):191âĂŞ207, 1994.

Parameters	Key size	Security level
$[1024, 176, 128]_2$	22.5 ko	2^{72}
$[2048, 232, 256]_2$	59, 4 ko	2^{93}

Reed-Muller codes for the McEliece scheme

➢ Reed-Muller codes

V. Sidelnikov.
A public-key cryptosytem based on Reed-Muller codes.
Discrete Math. Appl., 4(3):191âĂŞ207, 1994.

Parameters	Key size	Security level
$[1024, 176, 128]_2$	22.5 ko	2^{72}
$[2048, 232, 256]_2$	59, 4 ko	2^{93}

✗ Attacks against this proposal:

L. Minder and A. Shokrollahi.
Cryptanalysis of the Sidelnikov cryptosystem.
In EUROCRYPT 2007, pages 347360, 2007.

I. V. Chizhov, and M. A. Borodin.
The failure of McEliece PKC based on Reed-Muller codes.
IACR Cryptology ePrint Archive, 287, 2013.

Attack

Public Key: $$\mathcal{K}_{\text{pub}} = \begin{cases} \text{a gen. matrix of } \mathcal{C} = \mathcal{R}^{\sigma}(r, m) \text{ for some permutation } \sigma \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$$

Attack

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a gen. matrix of } \mathcal{C} = \mathcal{R}^{\sigma}(r,m) \text{ for some permutation } \sigma \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm:

1. Compute the code $\mathcal{R}^{\sigma}(1,m)$ from $\mathcal{R}^{\sigma}(r,m)$

Proposition:

- If $\gcd(r, m-1) = 1$, i.e. $1 = a(m-1) + br$. Then,

$$\mathcal{R}(r,m) \xrightarrow{Prop.Chizhov-Borodin} \mathcal{R}(1,m)$$

Attack

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a gen. matrix of } \mathcal{C} = \mathcal{R}^\sigma(r, m) \text{ for some permutation } \sigma \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm:

1. Compute the code $\mathcal{R}^\sigma(1, m)$ from $\mathcal{R}^\sigma(r, m)$

Proposition:

- If $\gcd(r, m-1) = d$. Then,

$$\mathcal{R}(r, m) \xrightarrow{Prop.Chizhov-Borodin} \mathcal{R}(d, m) \xrightarrow{\perp} \mathcal{R}(m-d-1, m)$$

$$\mathcal{R}(d, m) \Big\downarrow \oplus \quad \mathcal{R}(d-1, m)$$

$$\mathcal{R}(d-1, m), \mathcal{R}(m-d-1, m) \xrightarrow{\star} \mathcal{R}(m-2, m) = \mathcal{R}(1, m)$$

Attack

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a gen. matrix of } \mathcal{C} = \mathcal{R}^{\sigma}(r,m) \text{ for some permutation } \sigma \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm:

1. Compute the code $\mathcal{R}^{\sigma}(1,m)$ from $\mathcal{R}^{\sigma}(r,m)$
2. Find τ such that $\mathcal{R}^{\sigma\circ\tau}(1,m) = \mathcal{R}(1,m)$

Attack

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a gen. matrix of } \mathcal{C} = \mathcal{R}^{\sigma}(r, m) \text{ for some permutation } \sigma \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm:

1. Compute the code $\mathcal{R}^{\sigma}(1, m)$ from $\mathcal{R}^{\sigma}(r, m)$
2. Find τ such that $\mathcal{R}^{\sigma \circ \tau}(1, m) = \mathcal{R}(1, m)$
3. Then $\mathcal{R}^{\sigma \circ \tau}(r, m) = \mathcal{R}(r, m)$

4. Key Attacks

1. Introduction
2. Support Splitting Algorithm
3. Distinguisher for GRS codes
4. Attack against subcodes of GRS codes
5. Error-Correcting Pairs
6. Attack against GRS codes
7. Attack against Reed-Muller codes
8. **Attack against Algebraic Geometry codes**
9. Goppa codes still resist