

Weight two Masking in the McEliece system

Violetta Weger

University of Zurich

**The 13th International Conference
on Finite Fields and their Applications
June 5, 2017**

- 1 Preliminaries
- 2 BBCRS Scheme
- 3 Distinguisher Attack
- 4 Weight two Masking

Preliminaries

Choose $n = 2^m$, $t < \frac{n}{m}$ and Γ a binary Goppa code of length n , dimension $k \geq n - mt$, which can correct upto t errors. Γ has a generator matrix G of size $k \times n$. Choose a $k \times k$ invertible matrix S and a $n \times n$ permutation matrix P and compute $G' = SGP$.

$$\text{Public Key} = (G', t)$$

$$\text{Private Key} = (S, G, P)$$

Encryption: Let $x \in \mathbb{F}_2^k$ be the message and $e \in \mathbb{F}_2^n$ the error vector, s.t. $\text{wt}(e) \leq t$, then the cipher is computed as

$$y = xG' + e.$$

Decryption: Compute

$$yP^{-1} = xSG + eP^{-1},$$

then xSG is a code word of Γ and since $\text{wt}(eP^{-1}) \leq t$, we can apply the decoding algorithm and get xS and by multiplication with the inverse of S we get the message x .

Let \mathbb{F}_q be a finite field. Let $1 \leq k < n \leq q$ be integers. Construct a $[n, k]$ -linear code C , that can correct upto t errors and has an efficient decoding algorithm. C has a parity check matrix H of size $r \times n$, where $r = n - k$. Choose a $r \times r$ invertible matrix S and a $n \times n$ permutation matrix P and compute $H' = SHP$.

$$\text{Public Key} = (H', t)$$

$$\text{Private Key} = (S, H, P)$$

Encryption: Let $x \in \mathbb{F}_q^n$ be the message, s.t. $\text{wt}(x) \leq t$, then the cipher is computed as

$$y^T = H'x^T.$$

Decryption: Compute

$$S^{-1}y^T = HPx^T = H(xP^T)^T.$$

Since $\text{wt}(xP^T) \leq t$, we can apply syndrome decoding to get xP^T and by multiplication with the inverse of P^T we get the message x .

Definition (Schur Product)

Let $x, y \in \mathbb{F}_q^n$. The Schur product of x and y is

$$x \star y = (x_1y_1, \dots, x_ny_n).$$

Definition (Schur Product)

Let $x, y \in \mathbb{F}_q^n$. The Schur product of x and y is

$$x \star y = (x_1y_1, \dots, x_ny_n).$$

Definition (Schur Product of Codes and Square Code)

Let A, B be two codes of length n . The Schur product of A and B is

$$\langle A \star B \rangle = \langle \{a \star b \mid a \in A, b \in B\} \rangle.$$

If $A = B$, then we call $\langle A \star A \rangle$ the square code of A and denote it by $\langle A^2 \rangle$.

Definition (Schur Matrix)

Let G be a $k \times n$ matrix, with rows g_i for $1 \leq i \leq k$. We denote by $S(G)$ the Schur matrix of G , which consists of the rows $g_i \star g_j$ for $1 \leq i \leq j \leq k$. Thus $S(G)$ is of the size $\frac{1}{2}(k^2 + k) \times n$.

Proposition

Let A be a code of length n and dimension k , then

$$\dim(\langle A^2 \rangle) \leq \min \left\{ n, \binom{k+1}{2} \right\} \quad (1)$$

Proposition (Márquez-Corbella, Pellikaan (2016))

Let A be an $[n, k]$ linear code chosen at random, then with high probability the square code of A has maximal dimension.

Proposition (Márquez-Corbella, Pellikaan (2016))

Let A be an $[n, k]$ linear code chosen at random, then with high probability the square code of A has maximal dimension.

Proposition

If $2k - 1 < n$

$$\langle GRS_{n,k}(\alpha, \beta)^2 \rangle = GRS_{n,2k-1}(\alpha, \beta \star \beta) \quad (2)$$

BBCRS Scheme

Baldi, Bianchi, Chiaraluce, Rosenthal and Schipani proposed a variant of the McEliece cryptosystem, in order to reconsider the use of GRS codes as secret code.

Instead of the permutation matrix they use as scrambling matrix the sum $T + R$, where T is a sparse matrix of row weight m and R is a matrix of rank z .

Let \mathbb{F}_q be a finite field. Let $1 \leq k < n \leq q$ be integers. Let

$G = k \times n$ generator matrix of GRS code,

$T = n \times n$ permutation matrix,

$R = n \times n$ rank 1 matrix, $R = \alpha^T \beta$,

$Q = n \times n$ invertible matrix, $Q = R + T$,

$S = k \times k$ invertible matrix.

Compute: $G' = S^{-1}GQ^{-1}$ and $t_{\text{pub}} = t = \lfloor \frac{n-k}{2} \rfloor$.

Public Key = (G', t)

Private Key = (G, T, R, Q, S)

Encryption: Let $x \in \mathbb{F}_q^k$ be the message and $e \in \mathbb{F}_q^n$, s.t. $\text{wt}(e) \leq t$ be the error vector. Compute the cipher as

$$y = xG' + e.$$

Decryption: Guess the value of eR . Then compute

$$y' = yQ - eR = xS^{-1}G + eT.$$

Since $\text{wt}(eT) \leq t$ by decoding algorithm we get xS^{-1} and by multiplication with S we get the message x .

Distinguisher Attack

Distinguisher Attack

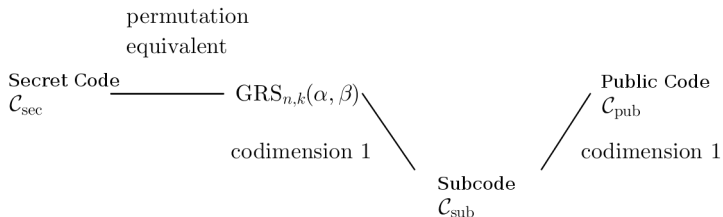
Couvreur, Gaborit, Gauthier-Umaña, Otmani and Tillich presented for some parameters a distinguisher attack on the BBCRS scheme.

Proposition (Couvreur, Gaborit, Gauthier-Umaña, Otmani, Tillich (2015))

Let \mathcal{C}_{pub} denote the public code of length n and dimension k of the BBCRS scheme. Then

$$\dim(\langle \mathcal{C}_{pub}^2 \rangle) \leq 3k - 1.$$

Overview Distinguisher Attack



Overview Distinguisher Attack

1. Find subcode \mathcal{C}_{sub}

Take a basis g_1, \dots, g_k of \mathcal{C}_{pub} and random other elements z_1, z_2, z_3 from \mathcal{C}_{pub} . Then define

$$\mathcal{B} = \langle \{z_i \star g_j \mid 1 \leq i \leq 3, 1 \leq j \leq k\} \rangle.$$

Proposition (Couvreur, Gaborit, Gauthier-Umaña, Otmani, Tillich (2015))

If $\dim(\mathcal{B}) \leq 2k + 2$, then z_i is in \mathcal{C}_{sub} for $i \in \{1, 2, 3\}$.

2. Find $\text{GRS}_{n,k}(x, y)$

Remark (Márquez-Corbella, Martínez-Moro, Pellikaan (2013))

Let \mathcal{A} be an ℓ dimensional subspace of $\text{GRS}_{n,k}(\alpha, \beta)$. If ℓ is large enough, then with high probability we have

$$\langle \mathcal{A}^2 \rangle = \langle \text{GRS}_{n,k}(\alpha, \beta)^2 \rangle.$$

Weight two Masking

Let \mathbb{F}_q be a finite field and $1 \leq k < n \leq q$ integers. Let G be a $k \times n$ generator matrix of $\text{GRS}_{n,k}(\alpha, \beta)$ code over \mathbb{F}_q^n , which is able to correct upto $t = \lfloor \frac{n-k}{2} \rfloor$ errors. We choose a $k \times k$ invertible matrix S , and a $n \times n$ invertible matrix Q , which is of row and column weight 2, both over \mathbb{F}_q . We define $t_{\text{pub}} = \lfloor \frac{t}{2} \rfloor$ and compute $G' = S^{-1}GQ^{-1}$.

$$\text{Public Key} = (G', t_{\text{pub}})$$

$$\text{Private Key} = (G, S, Q)$$

Encryption: Let $x \in \mathbb{F}_q^k$ be the message and $e \in \mathbb{F}_q^n$ be the error vector, s.t. $\text{wt}(e) \leq t_{\text{pub}}$ and compute the cipher

$$y = xG' + e.$$

Decryption: Compute

$$y' = yQ = xS^{-1}G + eQ.$$

Since $\text{wt}(eQ) \leq t$ we can decode and get xS^{-1} and by multiplication with S we get the message x .

In order for the ISD attack to reach a work factor greater than 2^{80} the following key sizes are needed with the different systems.

	n	k	Key Size
McEliece	1632	1269	460647
BBCRS scheme	346	252	199899
Weight two Masking	450	225	447326

Monte Carlo test with 1000 tries

q	n	r	Success rate
512	500	250	1
256	255	100	1
151	100	50	1
128	100	50	1

Let Q_n be a matrix of row and column weight two of the following form

$$Q_n = \begin{bmatrix} x_1 & & & & y_n \\ y_1 & x_2 & & & \\ & \ddots & \ddots & & \\ & & & y_{n-1} & x_n \end{bmatrix}. \quad (3)$$

Remark

For every $n \times n$ matrix R over \mathbb{F}_q of row and column weight two, there exist permutation matrices P, P' , s.t.

$$PRP' = \begin{bmatrix} Q_{n_1}^1 & & \\ & \ddots & \\ & & Q_{n_l}^l \end{bmatrix} \quad (4)$$

where $Q_{n_i}^i$ are $n_i \times n_i$ matrices of the form (3) for $1 \leq l < n$.

Let $H_{n,r}$ denote a generator matrix of GRS code of length n and dimension r . Let m denote the maximal square code dimension of an $[n, r]$ code, i.e.

$$m = \min \left\{ n, \frac{1}{2}(r^2 + r) \right\}.$$

Define

$$\begin{aligned} A_n &= \{R_n \in \text{GL}_n(\mathbb{F}_q) \mid R_n \text{ is of the form (4)}\}, \\ \mathcal{G}_{H_{n,r}} &= \{R_n^T \in A_n \mid S(H_{n,r}R_n^T) \text{ has rank } m\}. \end{aligned}$$

Lemma

Let \mathbb{F}_q be a finite field and $1 \leq n \leq q$ integers. Let p be a nontrivial homogeneous polynomial in $\mathbb{F}_q[x_1, \dots, x_n, y_1, \dots, y_n]$, of total degree $2n$, in each variable of degree at most 2, which has that each monomial is of the form

$$\prod_{i=1}^n x_i^{d_i} y_i^{2-d_i},$$

for $0 \leq d_i \leq 2$, $\forall 1 \leq i \leq n$. Then there exist at least

$$((q-1)^2 - 2(q-1))^n$$

choices for $x_1, \dots, x_n, y_1, \dots, y_n$ in \mathbb{F}_q^\times , s.t. p evaluated in these choices is nonzero.

Under the assumption that there exists a nontrivial principal minor of $S(H_{n,r}R_n^T)$ we get that the probability for R_n to avoid the distinguisher attack is greater than or equal to

1. case: $n \leq \frac{1}{2}(r^2 + r)$

$$\frac{((q-1)^2 - 2(q-1))^n}{(q-1)^{2n}} = \left(1 - \frac{2}{q-1}\right)^n.$$

2. case: $n \geq \frac{1}{2}(r^2 + r)$

$$\frac{((q-1)^2 - 2(q-1))^m (q-1)^{2(n-m)}}{(q-1)^{2n}} = \left(1 - \frac{2}{q-1}\right)^m.$$

1. Assume constant row weight two matrix is of the form Q_n

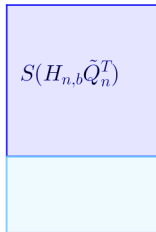
$$Q_n = \begin{bmatrix} x_1 & & & y_n \\ y_1 & x_2 & & \\ & \ddots & \ddots & \\ & & y_{n-1} & x_n \end{bmatrix}.$$

2. Reduce to quadratic case: $n = \frac{1}{2}(r^2 + r)$

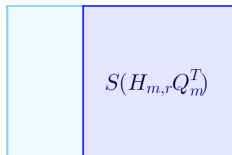
If $n \leq \frac{1}{2}(r^2 + r)$

If $n \geq \frac{1}{2}(r^2 + r)$

$$S(H_{n,r}Q_n^T) =$$



$$S(H_{n,r}Q_n^T) =$$



3. Transformations to get rid of β and y

Define

$$\begin{aligned}\tilde{x}_i &= x_i \beta_i \quad \forall 1 \leq i \leq n, \\ \tilde{y}_i &= y_i \beta_{i+1} \quad \forall 1 \leq i \leq n-1 \text{ and } \tilde{y}_n = y_n \beta_1.\end{aligned}$$

Then

$$S(H_{n,r}(\alpha, \beta)Q_n^T(x, y)) = S(H_{n,r}(\alpha, \mathbf{1})Q_n^T(\tilde{x}, \tilde{y})).$$

Now divide each column $j \in \{1, \dots, n\}$ by y_j^2 and define

$$\tilde{x}_i = \frac{x_i}{y_i} \quad \forall 1 \leq i \leq n.$$

Then

$$\det(S(H_{n,r}(\alpha, \beta)Q_n^T(x, y))) = \det(S(H_{n,r}(\alpha, \beta)Q_n^T(\tilde{x}, \mathbf{1}))).$$

Remaining to show:

For all $\alpha \in \mathbb{F}_q^n$ distinct n -tuple, there exists a $x \in (\mathbb{F}_q^\times)^n$, such that

$$\det (S(H_{n,r}(\alpha, \mathbf{1})Q_n^T(x, \mathbf{1}))) \neq 0.$$

Thank you!