A Code-Based Cryptosystem using GRS Codes

Violetta Weger

University of Zurich

Master Thesis Presentation
Seminar Coding Theory and Cryptography

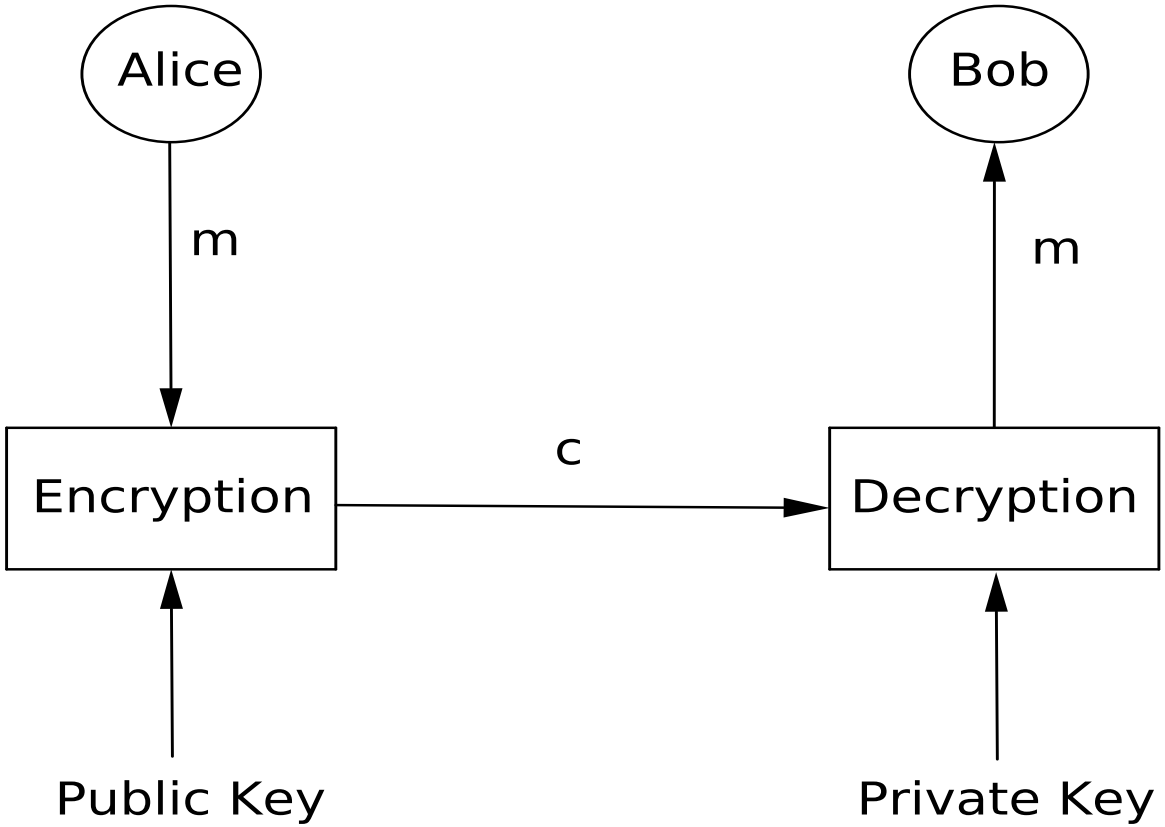
07 December 2016

Outline

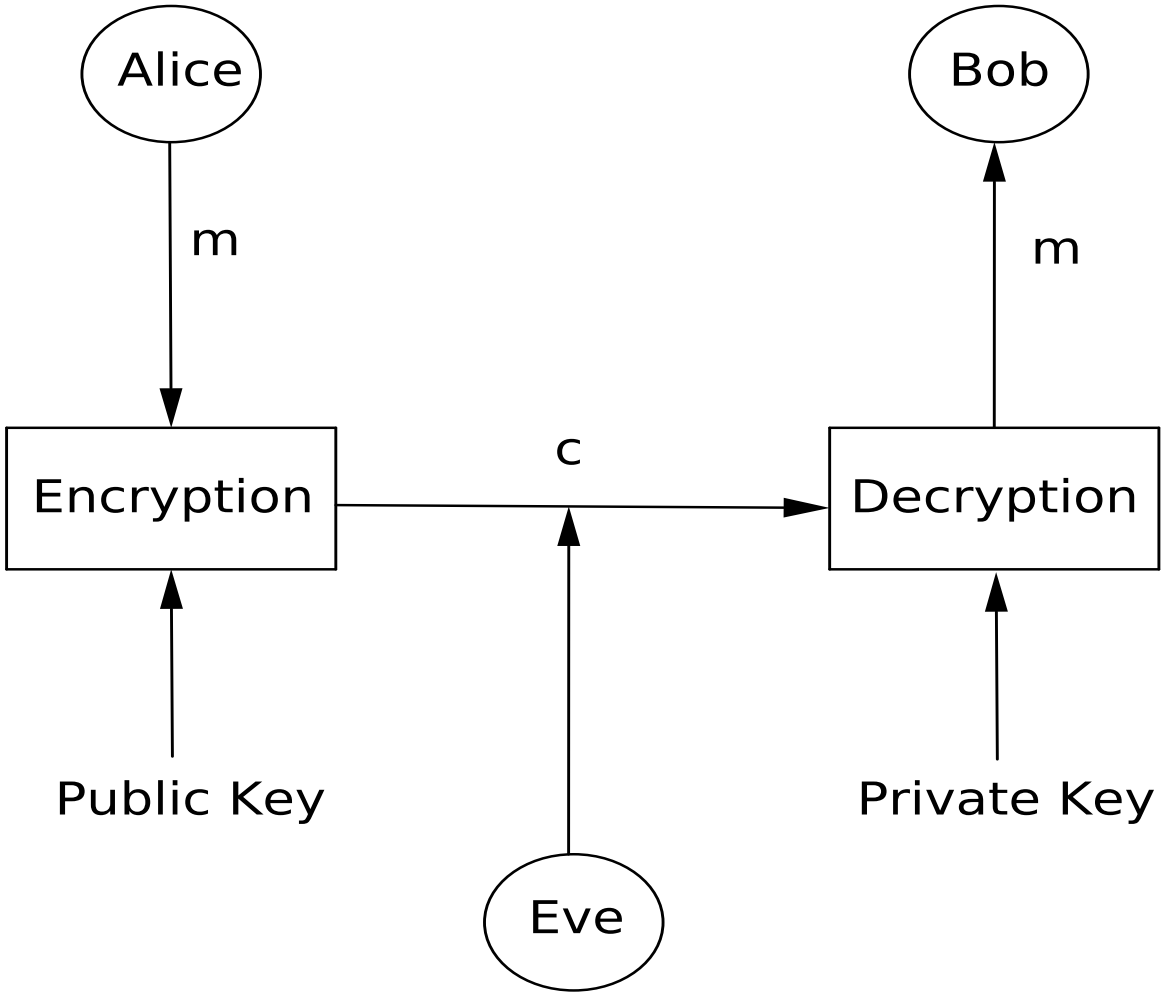
Motivation

Public-Key Cryptography

Public-Key Cryptography



Public-Key Cryptography



Example: RSA

Let p, q be primes. Compute $n = pq$ and the Euler-totient function $\phi(n) = (p-1)(q-1)$. Choose $e < \phi(n)$, s.t. $\gcd(e, n) = 1$.

$$\begin{aligned} \text{Public Key} &= (n, e) \\ \text{Private Key} &= (p, q) \end{aligned}$$

Encryption: Let m be the message. The cipher is computed as

$$c = m^e \bmod n.$$

Decryption: Compute d and b s.t.

$$de + b\phi(n) = 1.$$

Then by computing c^d we recover the message, since

$$c^d = (m^e)^d = m^{1-b\phi(n)} = m(m^{\phi(n)})^{-b} \equiv m1^{-b} = m.$$

Code-based Cryptography

- Code-based cryptography is a promising candidate for post-quantum cryptography.
- The McEliece cryptosystem in its original version using Goppa codes is still unbroken, but has the main drawback of having large key sizes.
- Using GRS codes directly in the McEliece system is broken by the attack of Sidelnikov and Shestakov.
- Rosenthal *et al.* proposed a variant of the McEliece cryptosystem, denoted by the BBCRS scheme, in order to reconsider the use of GRS codes, by changing the scrambling matrices.
- Couvreur *et al.* presented a distinguisher attack on this cryptosystem.

Basic Definitions

Let $\mathbb{F}_q$ be a finite field.

Definition

An $[n,k]$-linear block code over $\mathbb{F}_q$ is a k-dimensional linear subspace $C \subseteq \mathbb{F}_q^n$. There exists a $k \times n$ generator matrix G and a $(n-k) \times n$ parity check matrix H defined by the properties:

$$C = \left\{ uG \mid u \in \mathbb{F}_q^k \right\} = \left\{ x \in \mathbb{F}_q^n \mid Hx^T = \boldsymbol{0} \right\}.$$

Let $x, y \in \mathbb{F}_q^n$.

Definition

The Hamming distance of x, y is defined as

$$d_H(x,y) = \mid \{ i \in \{1, \ldots, n\} \mid x_i \neq y_i \} \mid .$$

Let C be an $[n, k]$-linear block code.

Definition

We define the minimum distance of C to be

$$d(C) = min\{d_H(x, y) \mid x, y \in C, x \neq y\}.$$

Definition

We denote by $C^{\perp}$ the dual code of C, defined as

$$C^{\perp} = \left\{x \in \mathbb{F}_q^n \mid x \cdot y = 0 \ \forall y \in C\right\}.$$

Theorem (Singleton Bound)

Let C be an $[n, k]$-linear block code. Then $d(C) \leq n - k + 1$.

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

Definition (Generalized Reed-Solomon Code)

Let $\alpha \in \mathbb{F}_q^n$ be an n-tuple of distinct elements and $\beta \in \mathbb{F}_q^n$, be an n-tuple of nonzero elements.

$$GRS_{n,k}(\alpha, \beta) = \{(\beta_1 p(\alpha_1), \ldots, \beta_n p(\alpha_n)) \mid p \in \mathbb{F}_q[x],\ deg(p) < k\}.$$

We can write the generator matrix of $GRS_{n,k}(\alpha, \beta)$ as

$$G = \begin{pmatrix} \beta_1 & \cdots & \beta_n \\ \beta_1\alpha_1 & \cdots & \beta_n\alpha_n \\ \vdots & & \vdots \\ \beta_1\alpha_1^{k-1} & \cdots & \beta_n\alpha_n^{k-1} \end{pmatrix}.$$

Proposition

$d(GRS_{n,k}(\alpha, \beta)) = n - k + 1.$

Proposition

$$GRS_{n,k}(\alpha, \beta)^{\perp} = GRS_{n,n-k}(\alpha, \gamma).$$

Where

$$\gamma_i = \beta_i^{-1} \prod_{\substack{j=1 \\ j \neq i}}^{n} (\alpha_i - \alpha_j)^{-1}.$$

Let $n = q^m$ and $\mathbb{F}_{q^m}$ be a finite field.

Definition (Goppa Code)

Let $G \in \mathbb{F}_{q^m}[x]$. Then define

$$S_m = \mathbb{F}_{q^m}[x] \Big/ \langle G \rangle .$$

Let $L = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^m}^n$, with $\alpha_i \neq \alpha_j \ \forall i \neq j \in \{1, \ldots, n\}$ and $G(\alpha_i) \neq 0 \ \forall i \in \{1, \ldots, n\}$. Then we can define the classical q-ary Goppa code as

$$\Gamma(L, G) = \left\{ a \in \mathbb{F}_q^n \;\middle|\; \sum_{i=1}^{n} \frac{a_i}{x - \alpha_i} = 0 \ \text{in } S_m \right\}.$$

McEliece System

McEliece System

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 $G' = SGP$.

$$\begin{aligned} \text{Public Key} &= (G', t) \\ \text{Private Key} &= (S, G, P) \end{aligned}$$

Encryption: Let $x \in \mathbb{F}_2^k$ be the message and $e \in \mathbb{F}_2^n$ the error vector, s.t. $\mathrm{wt}(e) \leq t$, 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 $\mathrm{wt}(eP^{-1}) \leq t$, we can apply the decoding algorithm and get xS and by multiplication with the inverse of S we get the message x.

Niederreiter system

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 $H' = SHP$.

$$\begin{aligned} \text{Public Key} &= (H', t) \\ \text{Private Key} &= (S, H, P) \end{aligned}$$

Niederreiter system

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

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

Decryption: Compute

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

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

BBCRS Scheme

BBCRS Scheme

Rosenthal, Schipani *et al.* 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. This thwarts the attack of Sidelnikov and Shestakov.

BBCRS Scheme for $m = 1, z = 1$

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

$$\begin{aligned} G &= k \times n \text{ generator matrix of GRS code,} \\ T &= n \times n \text{ permutation matrix,} \\ R &= n \times n \text{ rank 1 matrix, } R = \alpha^T \beta, \\ Q &= n \times n \text{ invertible matrix, } Q = R + T, \\ S &= k \times k \text{ invertible matrix.} \end{aligned}$$

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

$$\begin{aligned} \text{Public Key} &= (G', t) \\ \text{Private Key} &= (G, T, R, Q, S) \end{aligned}$$

BBCRS Scheme for $m = 1, z = 1$

Encryption: Let $x \in \mathbb{F}_q^k$ be the message and $e \in \mathbb{F}_q^n$, s.t. $\mathrm{wt}(e) \leq t$ 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 $\mathrm{wt}(eT) \leq t$ by decoding algorithm we get xS^{-1} and by multiplication with S we get the message x.

Distinguisher Attack

Definition (Schur Product)

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

$$x \star y = (x_1 y_1, \ldots, x_n y_n).$$

Definition (Schur Product)

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

$$x \star y = (x_1 y_1, \ldots, x_n y_n).$$

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

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

Properties of Square Codes

Proposition

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

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

Proposition

If $2k - 1 < n$

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

Idea of the proof.

Let c and c' be two codewords of the $\mathrm{GRS}_{n,k}(\alpha, \beta)$ code, i.e.

$$\begin{aligned} c &= (\beta_1 p(\alpha_1), \ldots, \beta_n p(\alpha_n)), \\ c' &= (\beta_1 q(\alpha_1), \ldots, \beta_n q(\alpha_n)). \end{aligned}$$

Then their Schur product has the following form.

$$\begin{aligned} c \star c' &= (\beta_1^2 p(\alpha_1) q(\alpha_1), \ldots, \beta_n^2 p(\alpha_n) q(\alpha_n)) \\ &= (\beta_1^2 r(\alpha_1), \ldots, \beta_n^2 r(\alpha_n)), \end{aligned}$$

where $\deg(r) \leq 2k - 2$.

Distinguisher Attack

Couvreur *et al.* presented for some parameters a distinguisher attack on the BBCRS scheme.

- Find a large subcode of the public code, by using the small square code dimension.
- The square code of this subcode is a square code of a GRS code.
- One can recover this GRS code, which is permutation equivalent to the secret code.
- With this GRS code one can recover the message.

The attack has a gap for $k \in \left\{\frac{n-2}{2}, \frac{n+2}{2}\right\}$. We will assume for the overview $2k + 2 < n$.

Overview Distinguisher Attack

Let $\mathcal{C}_{\text{pub}}$ be the public code of the BBCRS scheme and $\mathcal{C}_{\text{sec}}$ the secret code. Let Π be a $n \times n$ permutation matrix. Define

$$\mathcal{C} = \mathcal{C}_{\text{sec}}\Pi^{-1}.$$

Hence $\mathcal{C} = \text{GRS}_k(x, y)$. Take $a, b \in \mathbb{F}_q^n$, s.t. $R\Pi = b^T a$. Define

$$\lambda = -\frac{1}{1 + a \cdot b} b.$$

Lemma

For any c in $\mathcal{C}_{pub}$, there exists p in $\mathcal{C}$ such that:

$$c = p + (p \cdot \lambda)a. \tag{3}$$

Overview Distinguisher Attack

Define

$$\mathcal{C}_{\lambda^\perp} = \mathcal{C} \cap \langle \lambda \rangle^\perp.$$

This is a subcode of $\mathcal{C}_{\text{pub}}$ and of $\mathcal{C}$.

We can recover $\mathcal{C}_{\lambda^\perp}$, by taking a basis $g_1, \ldots, g_k$ of $\mathcal{C}_{\text{pub}}$ and random other elements z_1, z_2, z_3 from $\mathcal{C}_{\text{pub}}$. Then define

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

If $\dim(\mathcal{B}) \leq 2k + 2$, then z_i in $\mathcal{C}_{\lambda^\perp}$.

Pellikaan *et al.* showed that a large subcode of $\text{GRS}_{n,k}(x, y)$ has with high probability as square code $\text{GRS}_{n,2k-1}(x, y \star y)$.

With this we can find the code $\mathcal{C} = \text{GRS}_{n,k}(x, y)$.

Overview Distinguisher Attack

Now it is enough to find a pair (a, λ), which has the properties as in (3). With this pair one can recover the message.

Assume that we received $z = c + e$, where $c \in \mathcal{C}_{\text{pub}}$. We know that there exists a $p \in \mathcal{C}$, s.t. $c = p + (\lambda \cdot p)a$.
We compute for all $\alpha \in \mathbb{F}_q$ the value $z + \alpha a$. If we have chosen the correct $\alpha = -\lambda \cdot p$, then $z + \alpha a = p + e$ and by the decoding algorithm of $\mathcal{C}$ we get the message.

Proposal

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 $\mathrm{GRS}_{n,k}(\alpha, \beta)$ 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 $G' = S^{-1}GQ^{-1}$.

$$\begin{aligned} \text{Public Key} &= (G', t_{\text{pub}}) \\ \text{Private Key} &= (G, S, Q) \end{aligned}$$

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

$$y = xG' + e.$$

Decryption: Compute

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

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

Let $\mathbb{F}_q$ be a finite field and $1 \leq k < n \leq q$ integers. Let H be a $r \times n$ parity check matrix of $\mathrm{GRS}_{n,k}(\alpha, \beta)$ code over $\mathbb{F}_q$, with $r = n - k$. We choose a $r \times r$ 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 $H' = S^{-1} H Q^T$.

$$\begin{aligned} \text{Public Key} &= (H', t_{\text{pub}}) \\ \text{Private Key} &= (H, S, Q) \end{aligned}$$

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

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

Decryption: Compute

$$y' = Sy = HQ^T x^T.$$

Since $\mathrm{wt}(Q^T x^T) \leq t$ we can do syndrome decoding and get $Q^T x^T$ and by multiplication with the inverse of Q^T we get the message x.

Security

Example We refer to the Niederreiter version. Let $q = 5, n = 3, r = 2$. Let $\alpha = (1, 2, 4)$ and $\beta = (4, 3, 3)$, hence

$$H = \begin{bmatrix} 4 & 3 & 3 \\ 4 & 1 & 2 \end{bmatrix}.$$

Let

$$Q^T = \begin{bmatrix} 1 & 0 & 4 \\ 1 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix},$$

then the Schur matrix of HQ^T is the following matrix:

$$S(HQ^T) = \begin{bmatrix} 4 & 1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 4 \end{bmatrix}.$$

Security against the Distinguisher Attack

- For each generator matrix of a GRS code there exists an invertible matrix of row and column weight 2, s.t. the square code of the public matrix has maximal dimension.

Security against the Distinguisher Attack

- For each generator matrix of a GRS code there exists an invertible matrix of row and column weight 2, s.t. the square code of the public matrix has maximal dimension.

- For each generator matrix of a GRS code the probability of a random invertible matrix of row and column weight 2, to satisfy that the square code of the public matrix has maximal dimension tends to one for $q \to \infty$.

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

$$Q_n = \begin{bmatrix} x_1 & & & y_n \\ y_1 & x_2 & & \\ & \ddots & \ddots & \\ & & y_{n-1} & x_n \end{bmatrix} \tag{4}$$

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

$$Q_n = \begin{bmatrix} x_1 & & & y_n \\ y_1 & x_2 & & \\ & \ddots & \ddots & \\ & & y_{n-1} & x_n \end{bmatrix} \tag{4}$$

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.

$$PRP' = \begin{bmatrix} Q_{n_1}^1 & & \\ & \ddots & \\ & & Q_{n_l}^l \end{bmatrix} \tag{5}$$

where $Q_{n_i}^i$ are $n_i \times n_i$ matrices of the form (4) for $1 \leq l < n$.

Idea of Argument

Let $H_{n,r}$ be a generator matrix of a $\mathrm{GRS}_{n,r}(\alpha, \beta)$ code. Define

$$\begin{aligned} A_n &= \{R_n \in \mathrm{GL}_n(\mathbb{F}_q) \mid R_n \text{ is of the form (5)}\}, \\ \mathcal{G}_{H_{n,r}} &= \left\{R_n^T \in A_n \mid S(H_{n,r}R_n^T) \text{ has full rank } m\right\}. \end{aligned}$$

Where

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

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

Let $\mathbb{F}_q$ be a finite field and $1 \leq r < n \leq q$ be integers, s.t. $n \leq \frac{1}{2}(r^2 + r)$.

Under the assumption that there exists a nontrivial minor of $S(H_{n,r}R_n^T)$ we get the following lower bound on the size of $\mathcal{G}_{H_{n,r}}$

$$\mid \mathcal{G}_{H_{n,r}} \mid \geq ((q-1)^2 - 2(q-1))^n.$$

Lemma

Let $\mathbb{F}_q$ be a finite field and $1 < n \leq q$ integers. Let p be a nontrivial homogeneous polynomial in $\mathbb{F}_q[x_1, \ldots, x_n, y_1, \ldots, y_n]$, 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

$$((q-1)^2 - 2(q-1))^n \tag{6}$$

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

The proof of this lemma is by induction over n.

Idea of Argument

Corollary

We have the existence of R_n *in* $\mathcal{G}_{H_{n,r}}$. *Since* $\left| \mathcal{G}_{H_{n,r}} \right| \geq 1$ *for* $q > 3$.

Corollary

We have the existence of R_n in $\mathcal{G}_{H_{n,r}}$. Since $\left|\mathcal{G}_{H_{n,r}}\right| \geq 1$ for $q > 3$.

Corollary

The probability of $R_n \in A_n$ to be in $\mathcal{G}_{H_{n,r}}$ is greater than or equal to

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

And we can observe that for fixed n this quantity tends to one for $q \to \infty$.

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

Let $\mathbb{F}_q$ be a finite field and $1 \leq r < n \leq q$ be integers, s.t. $n \geq \frac{1}{2}(r^2 + r) = m$.

Under the assumption that there exists a nontrivial minor of $S(H_{n,r}R_n^T)$ we get the following lower bound on the size of $\mathcal{G}_{H_{n,r}}$

$$\mid \mathcal{G}_{H_{n,r}} \mid \geq ((q-1)^2 - 2(q-1))^m (q-1)^{2(n-m)}.$$

Idea of the Argument

Corollary

We have the existence of R_n in $\mathcal{G}_{H_{n,r}}$. Since $\left|\mathcal{G}_{H_{n,r}}\right| \geq 1$ for $q > 3$.

Corollary

The probability of $R_n \in A_n$ to be in $\mathcal{G}_{H_{n,r}}$ is greater than or equal to

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

And we can observe that for fixed n this quantity tends to one for $q \to \infty$.

Idea of Argument

The argument in the McEliece version is the similar to the Niederreiter version with the only change, that the polynomial is of total degree $2n(n-1)$ and in each variable of degree at most $2(n-1)$.

Hence for $q > 2n-2$, the probability for $R_n \in A_n$ to be in $\mathcal{G}_{G_{n,k}}$ is greater than or equal to

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

Experimental Results

q	n	r	Monte Carlo test with 1000 tries	probability bound
512	500	250	1	$\geq 1/8$
256	255	100	1	$\geq 1/8$
151	100	50	1	$\geq 1/4$
128	100	50	1	$\geq 1/5$

Complexity and Key Size

Key Size

The public key of the proposed system is a $r \times n$ matrix over $\mathbb{F}_q$, if we write the public matrix in systematic form, we have a $r \times (n-r)$ matrix. Thus we consider the key size to be q^{rk}.

We have smaller key sizes, than the original McEliece system.

In the Goppa-based system a received codeword is in $\mathbb{F}_2^n$. We need to go through all words which have at most distance t to the received word. Hence there are

$$\sum_{i=0}^{t} \binom{n}{i}$$

many words to check in a brute-force attack.

Key Size

Whereas in the proposal a received codeword is in $\mathbb{F}_q^n$. We need to go through all words which have at most distance t_{pub} to the received word. Hence there are

$$\sum_{i=0}^{t_{\text{pub}}} \binom{n}{i} (q-1)^i$$

many words to check in a brute-force attack.

Complexity

The cost $\mathcal{S}$ of one addition over a finite field $\mathbb{F}_q$ is considered equal to $l = \lceil \log_2(q) \rceil$ binary operations and the cost of one multiplication $\mathcal{M}$ equals to $2l$ additions, thus $\mathcal{M} = 2l^2$ binary operations. Hence we get in the proposed system the complexity of the Niederreiter version to be

$$\begin{aligned} \mathcal{M} \quad & \left\{ t_{\text{pub}} r + r^2 + 10t^2 + t(n+9) - n + tn \right\} + \\ \mathcal{S} \quad & \left\{ (t_{\text{pub}} - 1)r + r(r-1) + 6t^2 + t(n+1) + (t-1)n \right\}. \end{aligned}$$

Which is an improvement to the BBCRS scheme.

Conclusion

Conclusion

- There are also other code-based cryptosystems, which have been attacked by similar distinguisher attacks.
- Janwa and Moreno proposed the use of AG codes, or codes derived from them by subfield restriction or concatenation, for a code-based cryptosystem.
- Couvreur *et al.* came up with an attack on this cryptosystem, by deriving a t-error correcting pair with the aid of a filtration that is based on the Schur product.
- One could investigate if one can find a set of scrambling transformations where the best known distinguisher attacks based on the Schur product will fail. This then hopefully will provide post-quantum cryptosystems with reasonable key sizes.

Thank you!