A new code-based cryptosystem as an application of McNie with Gabidulin codes

Jon-Lark Kim
Department of Mathematics
Sogang University, Seoul, Korea

Joint work with Young Sik Kim, Lucky Galvez, and Myung Jae Kim

March 23, 2019
Special Session on Coding Theory and Information Theory
AMS sessional meeting, Honolulu, Hawaii
Introduction

- In 1994, Peter Shor developed a quantum algorithm that solves integer factorization problem in polynomial time.
- Advances in the development of quantum computers pose a threat to cryptosystems currently in use, such as RSA.
- Quantum-resistant cryptosystems: post-quantum cryptography.
- Cryptosystems based on error-correcting codes, lattices, and multivariate functions are among the promising candidates for post-quantum cryptography.
McEliece: the first code-based cryptography

**Key generation.** Generate the following:
- $G'$ a generator matrix for a code with an efficient decoding algorithm $\Phi$ correcting up to $t$ errors
- an invertible matrix $S$ and a permutation matrix $P$
- secret key: $(S, P, \Phi)$
- public key: $G = SG'P$

**Encryption.** To encrypt a message $m$, generate a vector $e$ of weight $t$ and obtain

$$c = mG + e$$

**Decryption.** Use $\Phi$ to decode $cP^{-1} = (mS)G'$ and then multiply by $S^{-1}$ to finally recover $m$
Niederreiter cryptosystem

Key generation. Generate the following:

- $H'$ a parity-check matrix for a code with an efficient decoding algorithm $\Phi$ that corrects up to $t$ errors
- An invertible matrix $S$ and a permutation matrix $P$

Secret key: $(S, P, \Phi)$
Public key: $H = SH'P$

Encryption. To encrypt a message $m$, use a one-to-one function that converts the $m$ into a vector $e(m)$ of weight $r$ and obtain

$$c = e(m)H$$

Decryption. Decode as in the McEliece cryptosystem and recover back $m$ using the inverse of $e$. 
McNie public key cryptosystem

- McNie = McEliece + Niederreiter
- McNie is a new code-based public key cryptosystem and is one of the 64 algorithms which passed the first round of the NIST Post-Quantum Cryptography standardization.
- Any code (in Hamming or rank weight) with an efficient decoding algorithm using the parity check matrix can be used.
- The original McNie proposal uses quasi-cyclic low rank parity check (QC-LRPC) codes.
- Many codes used in the McEliece cryptosystem (including Gabidulin codes) which were previously broken in the McEliece setting can still be considered safe in the McNie cryptosystem.
 McNie- Key generation

- Secret key: \((H, P, S, \Phi_H)\)
  - \(H\): a parity check matrix for an \([n, k]\) code \(C\) over \(\mathbb{F}_{q^m}\)
  - \(P\): an \(n \times n\) permutation matrix
  - \(S\): an \((n - k) \times (n - k)\) invertible matrix over \(\mathbb{F}_{q^m}\)
  - \(\Phi_H\): an efficient decoding algorithm for \(C\) which corrects errors of weight up to \(r\)

- Public key: \((G', F)\)
  - \(G'\): Generator matrix for a random \([n, l]\) code over \(\mathbb{F}_{q^m}\)
  - \(F = G'P^{-1}H^TS\)
McNie- Encryption

Message: \( m \in \mathbb{F}_{q^m}^l \)

- Randomly generate \( e \in \mathbb{F}_{q^m}^n \) of weight \( r \)
- \( Enc(m) = (c_1, c_2) \)
  \[ c_1 = mG' + e \]
  \[ c_2 = mF = mG'P^{-1}H^T S \]
McNie- Decryption

Received vector: $c = (c_1, c_2)$

- Compute

$$s' = c_1P^{-1}H^T - c_2S^{-1}$$
$$= (mG' + e)P^{-1}H^T - (mG'P^{-1}H^TS)S^{-1}$$
$$= eP^{-1}H^T$$
$$e' = \Phi_H(s') = eP^{-1}$$
$$e = e'P$$

- Solve the system

$$mG' = c_1 - e$$

to recover $m$. 

Jon-Lark Kim  Department of Mathematics  Sogang University, Seoul, Korea

A new code-based cryptosystem as an application of McNie with Gabidulin codes
Why modify McNie?

- Gaborit’s message recovery attack [3]
  - obtain a set of linear equations from $c_2$ which is then used to reduce $c_1$ into a system of equations with $l - (n - k)$ unknowns
  - does not completely break the system, but significantly lowered the security of the given parameters

- Decoding of QC-LRPC codes is probabilistic
  - there is a non-zero probability of decoding failure
  - parameters have to be adjusted to achieve negligible decoding failure probability, at the expense of the key size
Rank metric codes

Let \( \{\alpha_1, \alpha_2, \ldots, \alpha_m\} \) be a basis for \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \).

\[
c = (c_1, \ldots, c_n) \in \mathbb{F}_{q^m}^n \iff \bar{c} = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mn} \end{bmatrix}, \quad c_j = \sum_{i=1}^m c_{ij} \alpha_i
\]

- **rank weight**: \( w_R(c) = \text{Rank}(\bar{c}) \)
- **rank distance**: \( d_R(c, c') = \text{Rank}(\bar{c} - \bar{c}') \)

A **rank metric code** is an \([n, k]\) code over \( \mathbb{F}_{q^m} \) equipped with the rank metric.
Gabidulin codes

Definition

Let $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{F}_q^n$ such that $g_1, \ldots, g_n$ are linearly independent. The Gabidulin code of dimension $k$ generated by $\mathbf{g}$, denoted $\text{Gab}(\mathbf{g})$, is the code generated by the following matrix

$$G = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{bmatrix},$$

where $[i] = q^i$. 
McNie2-Gabidulin- Key Generation

- **Secret Key:** \((P, H, \Phi_H)\)
  
  \(H = \begin{bmatrix} H_1 & H_2 \end{bmatrix}\): parity check matrix for a \([2n - k, n]\) Gabidulin code \(C = Gab(g)\) over \(\mathbb{F}_{q^m}\), where \(H_2\) is an \((n - k) \times (n - k)\) invertible matrix.

  \(\Phi_H\): efficient decoding algorithm for \(C\) using \(H\), which can correct errors of weight up to \(r = \left\lfloor \frac{n-k}{2} \right\rfloor\).

- **Public Key:** \((G', F)\)

  \(G'\): a random \(l \times n\) partial circulant matrix

  \(F = G'P^{-1}H_1^T(H_2^T)^{-1}\)
McNie2-Gabidulin- Encryption

Generate random vectors $e_1 \in \mathbb{F}_q^n$ and $e_2 \in \mathbb{F}_q^{n-k}$ such that $e = (e_1, e_2)$ has weight $r$. Compute

$$c_1 = mG' + e_1$$
$$c_2 = mF + e_2.$$

The message $m \in \mathbb{F}_q^n$ is encrypted as $Enc(m) = (c_1, c_2)$. 

Jon-Lark Kim  Department of Mathematics  Sogang University, Seoul, Korea  Joint work with Young Sik Kim, Lucky Galvez, and Myung Jae Kim  March 23, 2019  Special Session on Coding Theory and Information Theory  AMS sessional meeting, Honolulu, Hawaii

A new code-based cryptosystem as an application of McNie with Gabidulin code
McNie2-Gabidulin- Decryption

When a ciphertext \( c = (c_1, c_2) \) is received, compute

\[
\begin{align*}
    c_1 P^{-1} H_1^T - c_2 H_2^T &= m_1 G' P^{-1} H_1^T + e_1 P^{-1} H_1^T - m G' P^{-1} H_1^T (H_2^T)^{-1} H_2^T \\
    &\quad - e_2 H_2^T \\
    &= e_1 P^{-1} H_1^T - e_2 H_2^T \\
    &= (e_1 P^{-1}, -e_2) \begin{bmatrix} H_1^T \\ H_2^T \end{bmatrix} \\
    &= e' H^T
\end{align*}
\]

Since \( wt(e') = wt(e_1 P^{-1}, -e_2) = r \), \( \Phi_H \) can be applied such that \( \Phi(e' H^T) = (e'_1, -e_2) \).

Apply the permutation \( P \) to \( e'_1 = e_1 P^{-1} \) to obtain \( e_1 \).

Finally, solve the system \( m G' = c_1 - e_1 \) to recover \( m \).
Why Gabidulin code?

- Gabidulin code is a well studied rank metric code
- They have high minimum distance (maximum distance separable)
- An efficient decoding algorithm
- No decoding failure
Problem 1.
Given an $l \times (n - k)$ matrix $F$ and a full rank $l \times n$ matrix $G'$, find a permutation matrix $P$ and a parity matrix $H = [H_1|H_2]$ for a Gabidulin code such that $F = G'P^{-1}H_1^T(H_2^T)^{-1}$.

Problem 2. Rank Syndrome Decoding (RSD)
Let $H$ be an $(n - k) \times n$ matrix over $\mathbb{F}_{q^m}$ with $k \leq n$, $s \in \mathbb{F}_{q^m}^{n-k}$ and $r$ an integer. Find $x \in \mathbb{F}_{q^m}^n$ such that the rank weight of $x = r$ and $Hx^T = s$.

The first problem is a form of a matrix factorization problem. Problem 2 on the other hand is the rank metric version of the syndrome decoding (SD) problem. The RSD problem is proven hard in by a probabilistic reduction to the SD problem, which is proven NP-complete.
The McNie2-Gabidulin PKE is IND-CPA secure under the assumption of Problems 1 and 2.
Gaborit’s attack is avoided because of the error $e_2$ in $c_2$. This way, it is not possible to rewrite $c_1$ in terms of $c_2$.

Lau and Tan [5] proposed a key recovery attack to the McNie cryptosystem which will not work in McNie2-Gabidulin since we are not using quasi-cyclic LRPC codes.

The presence of $G'$ gives an additional scrambling effect to the public matrix so that Overbeck’s attack fails.
Our Suggested parameters

**Table:** Parameter set values for the McNie2-Gabidulin PKE for each of the 128, 192 and 256-bit security levels. PK refers to the public key size, SK and CT refer to secret key and ciphertext sizes respectively.

<table>
<thead>
<tr>
<th>Sec</th>
<th>n</th>
<th>k</th>
<th>l</th>
<th>q</th>
<th>m</th>
<th>r</th>
<th>PK</th>
<th>SK</th>
<th>CT</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>24</td>
<td>12</td>
<td>22</td>
<td>2</td>
<td>41</td>
<td>6</td>
<td>1.476KB</td>
<td>0.308KB</td>
<td>0.185KB</td>
</tr>
<tr>
<td>192</td>
<td>32</td>
<td>16</td>
<td>24</td>
<td>2</td>
<td>53</td>
<td>8</td>
<td>2.756KB</td>
<td>0.530KB</td>
<td>0.318KB</td>
</tr>
<tr>
<td>256</td>
<td>36</td>
<td>18</td>
<td>29</td>
<td>2</td>
<td>59</td>
<td>9</td>
<td>4.116KB</td>
<td>0.664KB</td>
<td>0.399KB</td>
</tr>
</tbody>
</table>
McNie2-Gabidulin vs other PKEs

**Table:** Public key sizes (in kilobytes) of McNie2-Gabidulin and other public key cryptosystems with no decoding failure probability

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td><strong>1.476</strong></td>
<td>1.88</td>
<td>4.096</td>
<td>192.192</td>
</tr>
<tr>
<td>192</td>
<td><strong>2.756</strong></td>
<td>3.21</td>
<td>5.632</td>
<td>-</td>
</tr>
<tr>
<td>256</td>
<td><strong>4.116</strong></td>
<td>4.70</td>
<td>8.192</td>
<td>958.482</td>
</tr>
</tbody>
</table>

McNie2-Gabidulin has the smallest public key size among known code-based public key cryptosystems with no probability of decoding failure.
We modify the McNie public key cryptosystem and used Gabidulin codes in key generation. This new cryptosystem, called McNie2-Gabidulin, has the following features:

- safe against known attacks on McNie and other similar code-based cryptosystems
- Gabidulin code used in the McEliece is broken but safe to use in McNie2
- no decryption failure probability
- IND-CPA secure
- provides relatively low key size, the smallest among code based cryptosystems with zero decoding failure probability


THANK YOU!