A modification of the McEliece cryptosystem based on Generalized Reed-Solomon codes

Marco Baldi[1], Franco Chiaraluce[1], Joachim Rosenthal[2], Davide Schipani[2]

[1] Università Politecnica delle Marche, Ancona, Italy,
{m.baldi, f.chiaraluce}@univpm.it
[2] University of Zurich, Zurich, Switzerland,
{rosenthal, davide.schipani}@math.uzh.ch

Generalized Reed-Solomon codes in the McEliece cryptosystem

- Generalized Reed-Solomon (GRS) codes would allow reducing the public key size (since they are MDS codes)
- They are widespread and already widely implemented in software and hardware
- But they have more structure than Goppa codes, and this facilitates attacks

We have recently proposed a new GRS code-based variant of the McEliece cryptosystem which provides a higher protection to the structure of the secret GRS code [1]

An attack procedure already devised in [2] has been improved in [3], resulting in a polynomial-time attack against the system parameters proposed in [1]

- The attack can be avoided by changing some parameters, without modifying the system
- But this way the advantage of using GRS codes is lost

We propose a modification of the system which restores security with practical parameters at a small cost in terms of public key size

Original System

- Niederreiter version of the system
- Bob's secret key is a GRS code:
  - with length n and dimension k
  - defined over $\mathbb{F}_q$
  - able to correct t errors
  - described through its $r \times n$ parity-check matrix $\mathbf{H}$
- Bob's public key:

$$\mathbf{H}' = \mathbf{S}^{-1} \cdot \mathbf{H} \cdot \mathbf{Q}^T$$

where:

- $\mathbf{S}$ is a non-singular $r \times r$ scrambling matrix
- $\mathbf{Q}$ is a transformation matrix replacing the classical permutation matrix
- $\mathbf{Q} = \mathbf{R} + \mathbf{T}$
- $\mathbf{R}$ is a dense $n \times n$ matrix with rank $z \ll n$
- $\mathbf{T}$ is a sparse $n \times n$ matrix with average row and column weight $m \ll n$
- $\mathbf{R} = \mathbf{a}^T \cdot \mathbf{b}$
- $\mathbf{a}$ and $\mathbf{b}$ are two $z \times n$ matrices with rank z

Encryption:

$$\mathbf{x} = \mathbf{H}' \cdot \mathbf{e}^T$$

where:

- $\mathbf{e}$ is the error vector corresponding to the message
- $\mathbf{e}$ has weight $t_{pub} = \lfloor \frac{t}{m} \rfloor$

Decryption:

$$\mathbf{x}' = \mathbf{S} \cdot \mathbf{x} = \mathbf{H} \cdot \mathbf{Q}^T \cdot \mathbf{e}^T = \mathbf{H} \cdot (\mathbf{e} \cdot \mathbf{Q})^T$$
$$\mathbf{x}' = \mathbf{H} \cdot \mathbf{b}^T \cdot \gamma + \mathbf{H} \cdot \mathbf{T}^T \cdot \mathbf{e}^T$$
$$\text{with } \gamma = \mathbf{a} \cdot \mathbf{e}^T$$

then:

- Bob guesses the value of γ
- Bob computes $\mathbf{x}'' = \mathbf{x}' - \mathbf{H} \cdot \mathbf{b}^T \cdot \gamma = \mathbf{H} \cdot \mathbf{T}^T \cdot \mathbf{e}^T$
- $\mathbf{x}''$ is a correctable syndrome since $\mathbf{T}^T \cdot \mathbf{e}^T$ has weight $\leq m \cdot t_{pub} \leq t$
- Bob recovers $\mathbf{e}_T = \mathbf{T}^T \cdot \mathbf{e}^T$, with weight $\leq t$, through syndrome decoding
- Bob multiplies the result by $(\mathbf{T}^T)^{-1}$ to recover $\mathbf{e}$

Main issue

In the original system, both m and z must be small, since:

- for a given t_{pub}, increasing m requires to increase t and, hence, the code size and the public key size
- Bob needs $q^z/2$ attempts on average to guess the value of γ, hence increasing z increases the decryption complexity

Keeping both z and m small exposes the system to polynomial-time attacks [3]

New system

Modifications:

- Make $\mathbf{a}$ public
- Choose $\mathbf{b}$ such that it has rank $z' < z$
- Make a basis of the kernel of $\mathbf{b}^T$ public
- This basis is represented through a $z' \times z$ matrix $\mathbf{B}$, having rank z'
- Alice computes $\gamma' = \gamma + \mathbf{v}$, where $\mathbf{v}$ is a $z \times 1$ vector in the kernel of $\mathbf{b}^T$ (*i.e.*, $\mathbf{b}^T \cdot \mathbf{v} = \mathbf{0}$)
- Alice sends γ' along with the ciphertext
- Bob computes $\mathbf{b}^T \cdot \gamma' = \mathbf{b}^T \cdot \gamma$, thus he no longer needs to guess γ
- This allows to choose high values of z

Using high values of z prevents attacks exploiting the subcode defined by the parity-check matrix $\mathbf{H}_S = \begin{bmatrix} \mathbf{H}' \\ \mathbf{a} \end{bmatrix}$ [1]

$m = 1$ can be used, with code rate $> 2/3$ to avoid the attack in [4] against a shortened version of the public code

Assessment and comparisons

- Classical binary Goppa code-based Niederreiter cryptosystem
- New system with:
  - $m = 1$
  - $z = k$
  - $z' = \lfloor k/2 \rfloor$
  - codes with rate $> 2/3$

Work factor (WF) of the most dangerous attacks (Information Set Decoding) estimated according to [5] and public key size (KS) in KiB:

•	Binary Goppa code-based Niederreiter ($n = 4096$)									
k	3004	2884	2764	2644	2524	2404	2284	2164	2044	1924
t	91	101	111	121	131	141	151	161	171	181
WF	**180**	184	187	189	189	189	187	184	180	176
KS	**400.4**	426.7	449.4	468.6	484.3	496.5	505.2	510.4	512.0	510.1
•	New system with GRS codes over $\mathbb{F}_{521}$ ($n = 520$)									
k	348	340	332	324	316	308	300	292	284	276
t	86	90	94	98	102	106	110	114	118	122
WF	**180**	181	182	183	183	183	183	183	182	181
KS	**367.9**	361.1	354.2	347.3	340.2	333.1	325.9	318.7	311.3	303.9

References

[1] Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D. (2014): Enhanced Public Key Security for the McEliece Cryptosystem. Journal of Cryptology, in press.

[2] Couvreur, A., Gaborit, P., Gauthier-Umaña, V., Otmani, A., Tillich, J.-P. (2014): Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. Designs, Codes and Cryptography, Vol. 73, pp. 641–666.

[3] Couvreur, A., Otmani, A., Tillich, J.-P., Gauthier-Umaña, V. (2015): A Polynomial-Time Attack on the BBCRS Scheme. In: Katz, J. (ed.) Public-Key Cryptography – PKC 2015, Lecture Notes in Computer Science 9020, 175–193. Springer (2015).

[4] Wieschebrink, C.: Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. In: Sendrier, N. (ed.) Post-Quantum Cryptography (PQCrypto 2010), Lecture Notes in Computer Science 6061, 61–72. Springer (2010).

[5] Peters, C.: Information-set decoding for linear codes over $\mathbb{F}_q$. In: Sendrier, N. (ed.) Post-Quantum Cryptography, Lecture Notes in Computer Science 6061, 81–94. Springer (2010).