Code-based cryptosystems evolution*

Marina Samokhina
Independent researcher
Sydney, Australia
marina@samokhins.com

Oksana Trushina
Department of Radio Engineering and Cybernetics
MIPT
Dolgoprudny, Russia
trushina@phystech.edu

***Abstract*—This paper describes the original linear code-based cryptosystem and shows how it evolves after successful structural-based attacks have been discovered. All existing modifications of the original Niederreiter public-key algorithm have been classified based on improvements and classified accordingly common characteristics and variety of parameters. Based on the analysis authors approximates further code-based systems movement towards the development of real-life implementations and possible standarts.**

Keywords—public key cryptosystem; linear code; code-based cryptography; postquantum encryption; cryptanalysis

I. Introduction

The public-key cryptosystems are used worldwide, they are part of our everyday life despite the fact we might don't suspect they exist. Each second thousands of connections are established and protected by public-key cryptosystems. All those systems are mainly based on the practical difficulty of large prime factorization and discrete logarithms calculations.

Today we are facing to the new Quantum computer era. The concept of Quantum computing is relatively new, Richard Feynman puts forward the idea of Quantum computing in the early 1980s [1]. Individual Quantum computer memory cells based on various physical principles are not limited by theoretical models only the practical implementations have been claimed by many leading research laboratories and commercial companies across the globe. The latest news inspire confidence that we are very close to the moment when the easy reproducible memory cell would be created. Despite the fact the the Quantum computer invention is a huge scientific breakthrough it produces few challenges. Peter Shor shows in 1994 [2] that the classic public-key cryptography used today is vulnerable by quantum computer attacks. Inventing of alternative algorithms is a key problem of postquantum cryptography nowadays.

Code-based cryptography relies on generic decoding problem. That's why code-based algorithms are one of the few classes of mathematical techniques that can be claimed as an competitive alternatives to the current standards that are resistant to the Quantum computer attacks.

II. Classic code-based cryptosystems

Robert J. McEliece was the first who proposed a public-key cryptosystem based on an elements of algebraic coding theory in 1978 [3]. Harald Niederreiter has published his "Knapsack-type cryptosystems and algebraic coding theory" 6 years later [4]. The design and general principles for both cryptosystems are quite similar. The equivalence of McEliece's and Niederreiter's public-key cryptosystems has been demonstrated by Y. Li, R. Deng and X. Wang in [5] in 1994.

A. McEliece cryptosystem

The main theoretical concept of the McEliece public-key cryptosystem [3] is to generate a code with particular set of parameters and to disguise it as a common linear code. Classic McElise cryptosystem based on binary *(n, k)* Goppa code.

The public-key is a matrix calculates as $G_{pub}=SGP$, where G is a generator matrix of Goppa code and permutation matrix P and nonsingular matrix S are chosen randomly to mask the structure of G. The private key is a set of $\{G,P,S\}$ to used separately.

Assuming the chosen code can correct up to t errors the message $\underline{m}$ could be masked by random generated vector $\underline{z}$ with Hamming weight do not exceed t. The cipher text would be calculated as $\underline{c}=\underline{m}G_{pub} + \underline{z}$.

The decryption process includes the calculation of $\underline{c}P^{-1}$ as a first stage and the usage of fast decoding algorithm to obtain $\underline{m}_1$ as a second stage. The final calculation results in obtaining the plain text by multiplying $\underline{m}_1$ to matrix S^{-1}.

The algorithm is relatively fast and operates tenfold times faster than a standard RSA system, but has a one disadvantage – the public key is quite large. Due to the large public key the cipher text is approximately twice as long as public key. This means that a larger message must be transmitted and the system application becomes more complicated.

B. The cryptosystem designed by H. Niederreiter

The Niederreiter system has no disadvantages of McEliece system as described above, it is also based on Reed-Solomon codes. The private key consists of:

- The check matrix $H=[z_j x_j^i]$, where $j=1,...,n$ and $i=0,...,r-1$, of Reed-Solomon code over a finite field $GF(q)$.
- S – a random non-singular scrambling matrix over the finite field $GF(q)$. This matrix is introduced in order to conceal visible patterns from a cryptanalyst by corrupting the structure of the check matrix.

Scrambled check matrix SH is a public key.

Messages are all vectors with coordinates from the field $GF(q)$ the weight of which is no greater than $r/2$. Messages are not codewords of the chosen Reed-Solomon code, but represent all kinds of errors which this code can correct.

The cipher text which corresponds to message $\underline{m}$ is a syndrome vector and is calculated as follows:

$$\underline{c}=\underline{m}H^T S^T \quad (1)$$

Upon receiving the cipher text $\underline{c}$, an authorised user multiplies it from the right side by matrix $(S^T)^{-1}$, then applies a fast decoding algorithm, known to this user only, this returns the transmitted message .

This algorithm is unique based on the fact it has been designed on two independent coding theories, it's joining error correction and cryptographic coding.

C. Cryptoanalisys

The Niederreiter cryptosystem proved vulnerable and was hacked by Sidelnikov and Shestakov [6]. Taking into account the equivalence of the systems [5] the attack can be modified for McElise cryptosystem so the attacker can get a plaintext without knowing a secret. The cryptanalysts managed to find such matrices S_1 and H_1, that $S_1H_1=SH$. The matrix H_1 has the same structure as H however the parameters might vary.

Sidelnikov and Shestakov used the concept of a "distinguisher" which aims at detecting a behaviour different from the one that one would expect from a random code. All the distinguishers are based on the notion of component-wise product of codes. It results in both McEliece and Niederreiter cryptosystems based on Reed-Solomon codes were recognised as cryptographicaly not strong. This successful attack and another structural cryptoanalytical approach we'll describe below provide more opportunities for researchers to improve the design of original systems and create new modifications that we believe would be strong enough to compete with such algorithms as elliptic curve based systems.

III. Modifications of code-based cryptosystems

In recent years, the main idea of modification was to conceal the structure of the syndrome in the best possible way. This is done in order to prevent structural attacks, similar to Sidelnikov-Shestakov attacks. The structure of the private key becomes so complex that the syndrome of the parent code acts as an artificially created error of the new code in the new metric.

A. Modifications of the Niederreiter system

Table 1 presents some of the possible modifications to the Niederreiter system.

TABLE I. Table Styles

Code	*Metric*	*Type of cipher text*	*Cryptosystem*
Codes with maximum rank distance	Rank metric	$\underline{m}H^T_{pub}=\underline{m}(SH)^T$	Described by T. Berger and P. Loidreau in 2004
Generalised Reed-Solomon codes	New metric based on Vandermonde matrix	$H_{pub}\underline{m}=S(F+G^TU)P\underline{m}$	Designed by E. Gabidullin and V. Obernikhin in 2002
Modified rank code	Based on Frobenius matrix	$H_{pub}\underline{m}=S(F+G^TU)P\underline{m}$	Designed by E. Gabidullin and M. Samokhina in 2005

The first row of Table 1 shows Berger-Loidreau [7] modification which uses codes with maximum rank distance. Apparently, a Sidelnikov-Shestakov attack can be possible for such a system, though no results of this sort have been reported.

Cryptosystems in the second and third rows of Table 1 use a new idea: cipher text can be presented as a sum of vectors , multiplied by a randomly selected matrix S.

In order to decrypt, a legitimate user must first calculate the error vector by applying the fast decoding algorithm to a new code, which in fact is a syndrome of the parent code. The second stage of decryption is to apply the fast decoding algorithm of the parent code. As a result a legitimate user obtains the public text.

The cryptosystem algorithm corresponding to the second row of Table 1, with a metric based on the Vandermonde matrix, begins with choosing matrix F with elements from an extended field. The algorithm has been proposed in 2002 [8] as one of possible applications of new codes constructed by authors. Matrix F is a check matrix for the parent code. This code must be designed in such a way that it has a fast decoding algorithm in the parent metric. Next step is to choose the generator matrix G of some linear code, which must have a fast decoding algorithm in the new metric.

A secret key would consist of set of matrices: $\{F, G^T, S, P\}$ and matrix U. Then the public key is calculated as follows :

$$H_{pub}=S(F+G^TU)P \quad (2)$$

During encryption stage, the public text $\underline{m}$ would be multiplied by public-key matrix: $\underline{c}=\underline{m}H_{pub}^T$. Upon receiving the cipher text $\underline{c}$, a legitimate user multiplies it by matrix $(S^T)^{-1}$. This results in a vector which can be represented as a sum: $(\underline{g}+\underline{e})$. Then a fast decoding algorithm should be applied in the Vadermonde metric. As a result, it straight away returns vector

$\underline{m}_1$. In order to obtain the public text $\underline{m}$, $\underline{m}_1(P^T)^{-1}$ must be calculated.

The modification given in the third row of Table 1 has been described in [9] in 2005 and is the main result of the Ph.D Thesis published in 2009. The main advantage of this system is based on the fact it is designed using the metric associated with certain way generated elements of Frobenius matrix [10] F. Each element of the matrix belongs to the extended field $GF(q^N)$ and the first column elements are chosen to be linear independent over the base field $GF(q)$. The similar structure matrix G should be generated for creating the code. Then, the concatenation of matrices F and G are used to identify whether all elements are collectively independent over the base field.

The public key has the same structure as (2): $H_{pub}=S(F+G^TU)P$. During encryption, the public text is multiplied by public-key matrix.

During decryption, a legitimate user multiplies the obtained cipher text $(\underline{g}+\underline{e})S^T$ by $(S^T)^{-1}$. Then the fast decoding algorithm is applied in the new metric. As a result, the user will obtain $\underline{g}$ and $\underline{e}$ as the separate vectors. After applying the fast decoding algorithm of the parent code, the user will obtain vector $\underline{m}_1$. Further multiplication of the vector $\underline{m}_1$ by matrix $(P^T)^{-1}$ will give the legitimate user the public text.

B. Other modifications

Some number of modifications are based on the popular idea to consider the codes in different metrics. Gabidulin code [11] was the single optimal rank metric code until 2016 year. The idea of the cryptosystem based on the Gabidulin code was proposed in 1991 [12] and called GPT cryptosystem.

The public key of GPT cryptosystem is the matrix: $G_{pub} = S(G + X)$, where G is generator matrix of (n,k) Gabidulin code, S is $k\times k$ scambler matrix over $\mathbb{F}_qN$ and $X - k\times n$ noise matrix of rank up to t over $\mathbb{F}_qN$. The private key is (G,S) and decoding algorithm. The ciphertext is calculated based on random generated error vector $\underline{e}$ as follows: $\underline{c} = \underline{m}G_{pub} + \underline{e} = \underline{m}SG + (\underline{m}SX + \underline{e})$.

A sum of ranks of vectors $\underline{m}SX$ and $\underline{e}$ must not exceed t which is the maximum rank distance. Decryption includes two steps. Firstly, after decoding $\underline{c}$ a legitimate user gets vector $\underline{m}S$. Secondly, the original message can be obtained by multiplying $\underline{m}S$ and S^{-1}. Although, matrix X is not used to calculate a plain text it is necessary to keep it as a secret.

Generator matrix of Gabidulin code has a featured structure. This results into successful structure recovering attack. As it has been shown in [13] this attack allows to find matrices S', G', X': $G_{pub} = S'(G' + X')$.

There were couple of attempts to improve GPT systems strength. Unfortunately they result in modifications of structural attack. One of the latest successful structural cryptoanalytical approach has been described in [14] and as a result the system can be cracked in polynomial time.

IV. Possible structural attacks on existing modifications of Niederreiter cryptosystem

There are two main types of attacks applicable to the described cryptosystems: direct attacks and structural attacks. Structural attacks are the most sufficient and most interesting class. Most of the structural attacks are various modifications of the Gibson attack [15], adapted to the particular modification of the cryptosystem. In fact it's based on the Sidelnikov-Shestakov attack. When assessing the complexity of each attack, it is important to consider the size of the public key and some of the parameters. For example, any cryptosystem with relatively small key size can be vulnerable for brute force attack

As per results of the cryptanalysis showed in [16] the computational complexity for the most successful structural attack for the latest modifications [9] are of the order for a public key of 1024 bytes. As of today, this computational complexity is more than sufficient to consider the cryptosystem to be secure. Although this can't be considered as an evidence that the successful attack doesn't exist. This field might be considered as a matter of further exploration.

Decades of research of code-based cryptography results in a certain level of maturity. As per today some of code-based crytosystems might be a strong candidates as one of the future Quantum-resistand standards. Despite the fact most of described systems complexity significantly increased since 1978 all of them rely on the original idea of usage error-correcting code. There are lots of different applications for the code-based systems which required further investigation including contracting code-based digital signature.

References

[1] R. P. Feynman, “Simulating Physics with Computers,” International Journal of Theoretical Physics, Vol. 21, No. 6-7, 1982, pp. 467-488

[2] P.Shor, “Polynomial-Time Algorithms for Prime factorization and Discrete Logarithms on a Quantum Computer,” SIAM J. Computing, vol. 26, no. 5, 1997, pp. 1484-1509.

[3] Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Jet Propulsion Laboratory DSN Progress Report 42–44, 114–116.

[4] Harald Niederreiter. "Knapsack-type cryptosystems and algebraic coding theory." Problems of Control and Information Theory 15, 19–34. Problemy Upravlenija i Teorii Informacii 15, 159–166.

[5] Y. Li, R. Deng and X. Wang, “The equivalence of McEliece’s and Niederreiter’s public-key cryptosystems,” IEEE Transactions on Information Theory, vol. 40, 1994, pp. 271–273.

[6] Sidelnikov, V., Shestakov, S.: On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Math. Appl. 2, 439–444 (1992).

[7] Berger, T.P., Loidreau, P.: Designing an efficient and secure public-key cryptosystem based on reducible rank codes. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 218–229. Springer, Heidelberg (2004)

[8] Gabidulin E.M., Obernikhin V.A., Codes in the Vandermonde F-metric and their applications. Proc. Eighth Int. Workshop on Algebraic and Combinatorial Coding Theory, Tsarskoe Selo – Moscow, Russia. 2002. - P. 124--127.

[9] M.A. Churusova, E.M.Gabidulin. The modified Niederreiter cryptosystem based on new metric. Proceedings of ISCTA2005, Ambleside, Lake District, UK, July, 2005.

[10] Gene H. Golub and Charles F. Van Loan (1996). Matrix Computations, third edition, Johns Hopkins University Press

[11] E. Gabidulin, "Theory of codes with maximum rank distance," *Problems Inform. Transmission*, vol. 21, 1985, pp. 1–12.

[12] E. M. Gabidulin, A.V. Paramonov, O.V. Tretjakov, "ideals over a noncommutative ring and their application in cryptology," Lecture Notes in Computer Science, vol. 547, 1991, pp. 482-489.

[13] K. Gibson, "The security of the Gabidulin public-key cryptosystem," Lecture Notes in Computer Science, vol. 1070, 1996, pp. 212-223.

[14] R. Overbeck, "Structural attacks for public key cryptosystem based on Gabidulin codes," Journal of Cryptology, vol. 21, 2008, pp. 280-301.

[15] Gibson, K.: The security of the Gabidulin public-key cryptosystem. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 212–223. Springer, Heidelberg (1996)

[16] M.A. Samokhina. The cryptanalysis of systems based on linear codes. Problems of information security. Computer system. Quarterly magazine of Saint-Petersburg State Polytechnical University publishers edited by professor P. Zegjda. St. Petersburg 2008. – P.94-103.