How to make network communications secure in post-quantum era

Elena Egorova
Skoltech and HSE
Moscow, Russia
egorovahelene@gmail.com

Grigory Kabatiansky
Skoltech
Moscow, Russia
g.kabatyansky@skoltech.ru

Evgenii Krouk
HSE
Moscow, Russia
ekrouk@hse.ru

Cedric Tavernier
ASSYSTEM
France
tavernier.cedric@gmail.com

***Abstract*—We propose a new type of post-quantum system based on repetition of different error-correcting codes. The scheme can work as a public-key cryptosystem (PKC) and as digital signature at the same time. All previously known code-based PKC can work only in one of these two modes. We also investigate how this new scheme can be used for so-called light-weight cryptography what is an inherent property of communication networks in post-quantum era.**

***Index Terms*—communication network, public-key cryptosystem, digital signature, repetition of codes**

INTRODUCTION

First public-key cryptosystem (PKC) based on error-correcting codes was proposed by McEliece in [1] forty years ago, and later a dual PKC (in some sense) was suggested in [2], which is based on syndrom decoding of linear codes. After that many different families of error-correcting codes were investigated as a candidate to replace Goppa codes used in [1]. In this paper we propose a new PKC based on repetition of different error-correcting codes what is a generalization of the construction of [3]. We analyze resistance of the new PKC to attacks of [4], [5] as well as to decoding attacks. We also show how the new PKC can be used for digital signature purpose. Importance of our scheme as well as other code-based schemes is that there are no known attacks on these scheme based on a quantum computer similar to the famous Shor attack on RSA scheme [6].

CONSTRUCTION

Let us recall some basic facts about code-based cryptography .

A user A chooses a generator $k \times n$ matrix G_A of some linear (n, k)-code C_A, which has decoding algorithm Φ correcting t errors with polynomial in n complexity. The user A takes randomly two matrices: $k \times k$ nonsingular matrix S_A and $n \times n$ permutation matrix P_A and then construct *public*,i.e., known to all other users, matrix $G_{pub} = S_A G_A P_A$. Any other user (say B) to deliver a message m of length k bits to the user A sends to A via a channel vector $y = mG_{pub} + e$ of length n, where e is a vector of weight t which is *randomly* generated by B. The user A after receiving vector y calculates

$$y' = yP_A^{-1} = mG_{pub}P_A^{-1} + eP_A^{-1} = (mS)G_A + e',$$

where $e' = eP_A^{-1}$ and $wt(e') = wt(e) \leq t$ since P is a permutation.Then A applies the decoding algorithm Ψ of the (n, k)-code C_A to vector $y' = m'G + e'$, obtains the vector $m' = mS$ and finally A receives $m := m'S^{-1}$. Any other user will deal either with the problem of correcting t errors by some linear code, which looks like a random code, or with the problem to recover the code structure from its public-key matrix.

Our construction works in the following way. Consider for simplicity two linear codes V_1 and V_2 of the same dimension k but different lengths n_1 and n_2. Let G_1 and G_2 be some generator matrices of these codes. Construct $k \times n$ generator matrix $G_{1,2}$ of a new code by concatenation of matrices G_1 and G_2 (hence, $n = n_1 + n_2$).We call this construction *pseudorepetition* and denote this code as $V_1 \bigsqcup V_2$. Surely this construction can be defined for any multiplicity u of pseudorepetition, and in particular, when $V_1 = V_2 = \ldots = V_u = RM(s, m)$, one has the Sidelnikov scheme [3]. Let us note that the main obstacle for previously known structural attacks is a difficulty to find splitting the set of all coordinates on two subsets corresponding to coordinates of codes V_1 and V_2. Another advantage of the new scheme is that one code can be used for correction of many errors (probably by list decoding or by probabilistic decoding) while second code used for detecting if the first code was decoded correctly. We show how it works for pseudorepetition of RM-codes and Goppa codes.

The research of first three authors was supported by RFBR grant 16-01-00716.

REFERENCES

[1] R.J. McEliece, " A public-key cryptosystem based on algebaric coding theory," In *Jet Propulsion Lab* pp.114–116, 1978.
[2] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory, v. 15, pp. 159-166, 1986.
[3] V.M. Sidelnikov, "Public-key cryptosystem based on binary Reed-Muller codes," Discrete Mathematics, vol. 6 (2), pp. 3–20,1994.
[4] Minder L. and Shokrollahi A. Cryptanalysis of the Sidelnikov cryptosystem. In *LNCS v. 4515*,pp. 347-360, 2007.
[5] M. A. Borodin, I. V. Chizhov, Effective attack on the McEliece cryptosystem based on ReedMuller codes, Discrete Math. Appl., vol. 4, no 3, pp. 191207, 2014.
[6] Peter W. Shor, "Polynominal time algorithms for discrete logarithms and factoring on a quantum computer," SIAM Journal on Computing, vol. 26, 5, pp. 1484–1509, Oct. 1997.