Lemma 3: Let a matrix $\mathbf{E}$ be of the form

$$\mathbf{E} = \mathbf{A}\mathbf{B},$$

where $\mathbf{A}$ is a $(t_1+n) \times \Delta$ matrix of full rank Δ and $\mathbf{B}$ is a $\Delta \times (t_1+n)$ of *column* rank Δ. There exist matrices $\mathbf{A}$ and $\mathbf{B}$ such that

$$\mathbf{B}\mathbf{A} = \gamma \mathbf{I}_\Delta,$$

where $\mathbf{I}_\Delta$ is the identity matrix of order Δ.

Proof: Choose a matrix $\mathbf{B}$ with column rank Δ as $\mathbf{B} = \begin{bmatrix}\mathbf{B}_1 & \mathbf{B}_2\end{bmatrix}$, where the square $\Delta \times \Delta$ submatrix $\mathbf{B}_1$ is nonsingular.

Choose a matrix $\mathbf{A}$ as $\mathbf{A} = \begin{bmatrix}\mathbf{A}_1 \\ \mathbf{A}_2\end{bmatrix}$, where the square $\Delta \times \Delta$ submatrix $\mathbf{A}_1$ will be chosen later. Let us require that

$$\mathbf{B}\mathbf{A} = \mathbf{B}_1\mathbf{A}_1 + \mathbf{B}_2\mathbf{A}_2 = \gamma \mathbf{I}_\Delta,$$

where $\gamma \in GF(q^N)$ and $\gamma \neq -1$. Take from this equation

$$\mathbf{A}_1 = \mathbf{B}_1^{-1}\left(\gamma \mathbf{I}_\Delta - \mathbf{B}_2\mathbf{A}_2\right).$$

■

Corollary 1: It follows that

$$\mathbf{E}^2 = \mathbf{A}\mathbf{B}\mathbf{A}\mathbf{B} = \mathbf{A}(\gamma\mathbf{I}_\Delta)\mathbf{B} = \gamma\mathbf{A}\mathbf{B} = \gamma\mathbf{E}.$$

Theorem 1: Let $(\mathbf{P}+\mathbf{Z})^{-1} = \mathbf{R}(\mathbf{I}+\mathbf{E})\mathbf{Q}$, where $\mathbf{R}$ and $\mathbf{Q}$ are nonsingular matrices over $GF(q)$. Then

$$\mathrm{Rk}_{\mathrm{col}}(\mathbf{e}(\mathbf{P}+\mathbf{Z})^{-1}) \leq \mathrm{Rk}_{\mathrm{col}}(\mathbf{e}) + \Delta.$$

The column scrambler $\mathbf{P}+\mathbf{Z}$ is represented as $\mathbf{P} = \mathbf{Q}^{-1}\mathbf{R}^{-1}$; $Z = -\frac{1}{1+\gamma}\mathbf{Q}^{-1}\mathbf{E}\mathbf{R}^{-1}$.

Proof: It follows from lemmata above. ■

5. Secure variants of the GPT cryptosystem

Consider a public key of the form

$$\mathbf{G}_{\mathrm{pub}} = \mathbf{S}\begin{bmatrix}\mathbf{Y} & \mathbf{G}_k\end{bmatrix}(\mathbf{P}+\mathbf{Z}),$$

where $\mathbf{Y}$ is a $k \times t_1$ distortion matrix with column rank t_1, $\mathbf{G}_k$ is a $k \times n$ generator matrix of a MRD code, $\mathbf{P}$ is a square $(t_1+n) \times (t_1+n)$ nonsingular matrix over the base field $GF(q)$, $\mathbf{Z}$ is a $(t_1+n) \times (t_1+n)$ matrix with column rank Δ. A ciphertext for a plaintext $\mathbf{m}$ has the form

$$\mathbf{c} = \mathbf{m}\mathbf{G}_{\mathrm{pub}} + \mathbf{e} = \mathbf{m}\mathbf{S}\begin{bmatrix}\mathbf{Y} & \mathbf{G}_k\end{bmatrix}(\mathbf{P}+\mathbf{Z}) + \mathbf{e}, \tag{27}$$

where an artificial error $\mathbf{e}$ has column rank t_3. An authorized party choose $t_3 + \Delta = \frac{n-k}{2}$. It allows to correct the emergent artificial error $\mathbf{e}(\mathbf{P}+\mathbf{Z})^{-1}$.

An unauthorized party does not know the matrix $(\mathbf{P}+\mathbf{Z})^{-1}$. Also one can not apply the second Overbeck attack since a scramble matrix $(\mathbf{P}+\mathbf{Z})$ is chosen over the extension field. There is still a possibility to use the first Overbeck attack. An unauthorized party tries to represent the public key over the superextension field $GF(q^{aN})$, where $a = \left\lceil \frac{t_1+n}{N} \right\rceil$. It allows to introduce a virtual generator matrix of extended MRD code of the form

$$\widehat{\mathbf{G}}_k = \begin{bmatrix}\mathbf{G}_k(t_1) & \mathbf{G}_k\end{bmatrix},$$

where $\mathbf{G}_k(t_1)$ is a $k \times t_1$ matrix of Frobenius-type over the superextension field. A column $\mathbf{f}$ is called Frobenius-type if it has the form $\mathbf{f} = \begin{pmatrix} f & f^{[1]} & \ldots & f^{[k-1]}\end{pmatrix}^\top$. A matrix $\mathbf{F}$ is called Frobenius-type if it consists of Frobenius-type columns. By this assumption, the public key can be considered as follows:

$$\begin{aligned}\mathbf{G}_{\mathrm{pub}} &= \mathbf{S}\left[\widehat{\mathbf{G}}_k + \widehat{\mathbf{Y}}\right](\mathbf{P}+\mathbf{Z}) = \\ &= \mathbf{S}\left(\widehat{\mathbf{G}}_k\mathbf{P} + \widehat{\mathbf{Y}}\mathbf{P} + (\widehat{\mathbf{G}}_k + \widehat{\mathbf{Y}})\mathbf{Z}\right),\end{aligned} \tag{28}$$

where

$$\widehat{\mathbf{Y}} = \begin{bmatrix}\mathbf{Y} - \mathbf{G}_k(t_1) & \mathbf{0}\end{bmatrix}.$$

The term $\widehat{\mathbf{G}}_k\mathbf{P}$ is a virtual $k \times (t_1+n)$ generator matrix of an MRD code over the superextension field $\mathbb{F}_{q^{aN}}$. The term $\widehat{\mathbf{Y}}\mathbf{P}$ has column rank t_1. The term $(\widehat{\mathbf{G}}_k + \widehat{\mathbf{Y}})\mathbf{Z}$ has column rank Δ. The Overbeck–Gibson attack does not work if

$$t_1 + \Delta > \frac{t_1+n-k}{2}.$$

Recall that an authorized user has chosen $t_3 + \Delta = \frac{n-k}{2}$. Hence we should choose $t_1 > 2t_3$ to prevent the Overbeck–Gibson attack.

Nevertheless it is possible to rewrite the public key (28) as an instance of Overbeck's attack:

$$\mathbf{G}_{\mathrm{pub}} = \mathbf{S}\begin{bmatrix}\mathbf{Y_1} + \mathbf{F}_1 & \mathbf{F}_2\end{bmatrix}(\mathbf{Q}),$$

where $\mathbf{F}_1$ is a $r \times t_1 + \Delta$ matrix, $\mathbf{F}_2$ is $k \times n - \Delta$ matrix such that the matrix $\begin{bmatrix}\mathbf{F}_1 & \mathbf{F}_2\end{bmatrix}$ is a generator matrix of a MRD (t_1+n, k, d) code over the superextension field $GF(q^{aN})$. The matrix $\mathbf{Y}_1$ is a new $k \times (t_1 + \Delta)$ distortion matrix. This approach is under investigation now.

Another way to prevent Overbeck's attack is given in Note 1. The cryptographer should choose a distortion $k \times t_1$ matrix $\mathbf{Y}$ such that the rank of the matrix $\mathbf{W}_{ext}$ satisfies the condition (22). Choose the matrix $\mathbf{Y}$ as follows:

$$\mathbf{Y} = \begin{bmatrix} \mathbf{m}_0 \\ \mathbf{m}_0^{[1]} + \mathbf{m}_1 \\ \mathbf{m}_0^{[2]} + \mathbf{m}_1^{[1]} + \mathbf{m}_2 \\ \mathbf{m}_0^{[3]} + \mathbf{m}_1^{[2]} + \mathbf{m}_2^{[1]} + \mathbf{m}_3 \\ \vdots \\ \mathbf{m}_0^{[k-1]} + \mathbf{m}_1^{[k-2]} + \cdots + \mathbf{m}_{k-1} \end{bmatrix}, \tag{29}$$

where $\mathbf{m}_0$ is a vector of column rank t_1. Calculating the matrix $\mathbf{W}$ gives

$$\mathbf{W} = \sigma(\mathbf{Y}_1) - \mathbf{Y}_2 = -\begin{bmatrix}\mathbf{m}_1 \\ \mathbf{m}_2 \\ \mathbf{m}_3 \\ \vdots \\ \mathbf{m}_{k-1}\end{bmatrix}. \tag{30}$$

Choose all vectors $\mathbf{m}_i$ over the *base field* $GF(q)$ in such a manner that the column rank of the matrix $\mathbf{W}$ is equal to

$t_1 - a$. Hence

$$\mathbf{W}_{\text{ext}} = \begin{bmatrix} \mathbf{W} \\ \sigma(\mathbf{W}) \\ \sigma^2(\mathbf{W}) \\ \dots \\ \sigma^{k-1}(\mathbf{W}) \end{bmatrix} = \begin{bmatrix} \mathbf{W} \\ \mathbf{W} \\ \mathbf{W} \\ \dots \\ \mathbf{W} \end{bmatrix}. \tag{31}$$

Therefore

$$\text{Rk}(\mathbf{W}_{\text{ext}} \mid GF(q^N)) = \text{Rk}(\mathbf{W} \mid GF(q^N) = t_1 - a,$$

and the condition (22) is satisfied.

In a similar manner we can show that even more secure variant of the GPT cryptosystem can be obtained if we use the general public key

$$\mathbf{G}_{\text{pub}} = \mathbf{S}\begin{bmatrix}\mathbf{Y} & \mathbf{G}_k + \mathbf{X}\end{bmatrix}(\mathbf{P} + \mathbf{Z}).$$

6. GPT-M in random network coding

We denote secure variants as GPT-M.

We consider the GPT cryptosystem which has been presented in [15].

We took the matrix $\mathbf{P} + \mathbf{Z}$ over the extension field $GF(q^N)$, or, the proper choice of the distortion matrix $\mathbf{Y}$. Then the Overbeck attack completely fails: all equations since (13) do not work.

Now, we consider a network with one source and one destination. The similar model was used in the work [18]. The difference is the following: we implement the GPT-M instead of the GPT.

The source transmits messages $\overline{\mathbf{u}} = (u_1 \dots u_k)$ which are enciphered by the cryptosystem GPT-M. As a result we have a ciphertext in vector representation $\mathbf{c} = (c_1 \dots c_n)$. The enciphered messages c_j are represented as n packets over the extension field. Each of them can be converted into vectors of length m over the base field. These packets are gathered in the matrix $\mathbf{M}$ with elements over the base field. A concatenation $\mathbf{V}$ of two matrices $\mathbf{M}$ and $\mathbf{I}_n$ is created.

$$\mathcal{V} = \left\{\mathbf{V} : \mathbf{V} = \begin{bmatrix}\mathbf{I}_n & \mathbf{M}\end{bmatrix}\right\}, \tag{32}$$

where $\mathbf{I}_n$ is the identity matrix of order n.

$V(1), \dots, V(n)$ are rows of the matrix $\mathbf{V}$. Then each row is a packet which has length $n+m$ and consists of elements over the base field $GF(q)$. The matrix $\mathbf{V}$ has size $n \times (n+m)$. Every packet is also an element of the finite field $GF(q^{n+m})$. In the Silva–Kötter–Kschischang network model [16] a message is a row spanned subspace of the matrix $\mathbf{V}$. Hence, the matrix $\mathbf{V}$ can be considered as a generator matrix of the subspace.

In this paper, to provide secure transmission in random network coding we focus on using the GPT public key cryptosystem to transmit encrypted messages and information on secret keys distribution. Both random network coding and the GPT cryptosystem are based on rank codes. It allows to combine in a most effective way the problems of deciphering and decoding. It is shown that our system provides secure communication in random network coding under definite conditions on the system parameters. In the GPT cryptosystem, a plaintext is an information vector $\mathbf{u}$ of dimension k over the extension field $GF(q^m)$. The corresponding ciphertext $\mathbf{c}$ is calculated as

$$\mathbf{c} = \mathbf{u}\mathbf{G}_{\text{pub}} + \mathbf{e}_{\text{art}}, \tag{33}$$

where the public key $\mathbf{G}_{\text{pub}}$ is a generator matrix of size $k \times n$ over the extension field $GF(q^m)$. It is a product of three matrices:

$$\mathbf{G}_{\text{pub}} = \mathbf{S}[\mathbf{Y}_k \;\; \mathbf{G}_k]\mathbf{P} + \mathbf{Z}.$$

In the network, every inner node calculates a random linear combination of the received packets which is express as operation:

$$\mathbf{Y} = \mathbf{A}\mathbf{V}, \tag{34}$$

where $\mathbf{A}$ is a matrix of the size $n_r \times n$ corresponding to all linear transformations at all inner nodes. If inside of the network there is an adversary, who insert his own packets in common flow, the network channel model is the following:

$$\mathbf{Y} = \mathbf{A}\mathbf{V} + \mathbf{E}_{\text{out}}, \tag{35}$$

where $\mathbf{A}$ is the same matrix as in (35), $\mathbf{E}_{\text{out}}$ is a matrix of size $n_r \times (n+m)$, which corresponds to the adversary messages. These messages are errors which a legal user has to correct.

At the receiver, packets $Y(1), \dots, Y(n_r)$ of length $n+m$ are gathered. The matrix $\mathbf{Y}$ of size $n_r \times (n+m)$ is constructed. For the random number n_r, we have three possibilities: be equal to n, or greater than, or less than n. The problem is to reconstruct $\mathbf{V}$ from $\mathbf{Y}$. To solve this problem it is necessary to do two rounds of linear transformations (see, [18] for details).

$\mathbf{A}$ is the matrix of size $n_r \times n$ corresponding to all the linear transformations at inner nodes. For the noncoherent network model, the matrix $\mathbf{A}$ is unknown but in our case we can find it. Represent the matrix $\mathbf{Y}$ as the concatenation of matrices $\mathbf{Y}_1$ and $\mathbf{Y}_2$, where the matrix $\mathbf{Y}_1$ has size $n_r \times n$.

We get at the receiver side the matrix $\mathbf{Y} = [\mathbf{A} \;\; \mathbf{A}\mathbf{M}]$, or, $\mathbf{Y}_1 = \mathbf{A}$. Therefore the matrix $\mathbf{A}$ is known in this case. Assume that the rank of $\mathbf{A}$ is equal to r, where $r \le n$.

Before decoding we fulfill the preliminary linear transformations over the matrix $\mathbf{Y}$ which correspond to the Gauss elimination procedure over $\mathbf{Y}_1 = \mathbf{A}$ and create the row reduced echelon form of the matrix $\mathbf{Y}_1$.

As a result of the first round we have (see, [17], for details)

$$\widehat{\mathbf{R}} = \mathbf{M} + \mathbf{L}\mathbf{M} + \mathbf{D}\mathbf{C} + \mathbf{E}_{\text{rest}}, \tag{36}$$

where the matrix $\mathbf{L}$ of rank $n - r$, and the matrix $\mathbf{C}$ of rank $n_r - r$ are known. Convert the matrix $\widehat{\mathbf{R}}$ over the base field into a vector $\widehat{\mathbf{r}}$ over the extended field:

$$\widehat{\mathbf{r}} = \mathbf{u}\mathbf{G}_{\text{pub}} + \mathbf{e}_{\text{art}} + \mathbf{a}(\mathbf{M}_1 + \mathbf{E}_{\text{art}}) + \mathbf{d}\mathbf{C} + \mathbf{e}_{\text{rest}}, \tag{37}$$

where the matrix $\mathbf{M}$ is converted into a vector $\mathbf{u}\mathbf{G}_{\text{pub}} + e_{\text{art}}$; the matrix $\mathbf{L}$ is converted into a vector $\mathbf{a}$ of rank $n - r$ with known coordinates; the matrix $\mathbf{D}$ is converted into a vector $\mathbf{d}$ of rank $n_r - r$ with unknown coordinates; the matrix $\mathbf{E}_{\text{rest}}$ is converted into an error vector $\mathbf{e}_{\text{rest}}$.

Then we have to do the second round of transformations. Choose a matrix $(\mathbf{P} + \mathbf{Z})^{-1}$ as in Eq. (**??**). Multiply on the right the both sides of the equation (37) by the matrix $(\mathbf{P}+\mathbf{Z})^{-1}$:

$$\widehat{\mathbf{v}} \overset{def}{=} \widehat{\mathbf{r}}(\mathbf{P}+\mathbf{Z})^{-1} = \mathbf{uSG} + \mathbf{e}_{\text{art}}(\mathbf{P}+\mathbf{Z})^{-1} + \mathbf{a}(\mathbf{M}_1+\mathbf{E}_{\text{art}})(\mathbf{P}+\mathbf{Z})^{-1} + \mathbf{dC}(\mathbf{P}+\mathbf{Z})^{-1} + \mathbf{e}_{\text{rest}}(\mathbf{P}+\mathbf{Z})^{-1}. \quad (38)$$

The first member $\mathbf{uSG}$ is a vector of the rank code. It corresponds to the information vector $\mathbf{u}$. The second member $\mathbf{e}_{\text{art}}\mathbf{P}+\mathbf{Z}^{-1}$ is a vector of rank $t_2+\Delta$. The last three members we can take as row erasures, column erasures and additional errors. The rank of row erasures is $n-r$. The rank of column erasures (the matrix $\mathbf{C}$) is n_r-r. Denote the rank of the additional error by p. The next operation is rank decoding. Decoding will be successful, if the following inequality satisfies:

$$2(t_2+\Delta+p)+(n-r)+(n_r-r) \leq d-1,$$

where $d=n-k+1$ is the rank distance of the code.

7. Conclusion

Secure capability of all versions GPT cryptosystems depends on values of its parameters.

The known decoding attacks can be prevent by a proper choice of parameters.

Overbeck's structural attack of 2008 year was successful, it had broken a version of GPT cryptosystem. To prevent new structural attacks of such type we have introduced structure and parameter changes. We propose a new family of column scramble matrices $\mathbf{P}+\mathbf{Z}$ to prevent structural attacks.

We use GPT-M cryptosystem in the network with random network coding. We show it provides secure communication in network under a definite condition on the system parameters.

8. Acknowledgment

This work was partially supported by Grant RFBR 12-07-00122-a.

9. References

[1] McEliece R.J. A Public Key Cryptosystem Based on Algebraic Coding Theory// JPL DSN Progress Report 42–44, Pasadena, CA. P. 114–116, 1978.

[2] Niederreiter H. Knapsack-Type Cryptosystem and Algebraic Coding Theory// Probl. Control and Inform. Theory. V. 15. P. 19-34, 1986.

[3] Sidelnikov V.M., Shestakov S.O. On insecurity of cryptosystems based on generalized Reed-Solomon codes// Discrete Mathematics and Applications 2.

[4] Gabidulin E.M., Paramonov A.V., Tretjakov O.V. Ideals over a Noncommutative Ring and Their Application in Cryptology// in: Advances in Cryptology — Eurocrypt '91, LNCS 547. P. 482–489.1991.

[5] Gibson J. K. Severely denting the Gabidulin version of the McEliece public key cryptosystem// J-DESIGNS-CODES-CRYPTOGR, 6(1):3745, July 1995.

[6] Gibson J. K. The security of the Gabidulin public-key cryptosystem", in: U. M. Maurer, ed. // Advances in Cryptology – EUROCRYPT'96, LNCS 1070. P. 212–223, 1996.

[7] R. Overbeck: "Extending Gibsons Attacks on the GPT Cryptosystem", Coding and Cryptography International Workshop, WCC 2005 Bergen, Norway, March 14-18, 2005. Lecture Notes in Computer Science 3969. P. 178-188.

[8] R.Overbeck Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes// Journal of Cryptology. V. 21, no 2, April 2008.

[9] Gabidulin E.M. Theory of Codes with Maximum Rank Distance// Probl. Inform. Transm. V. 21, No. 1. P. 1–12, July, 1985.

[10] Gabidulin E. M. A Fast Matrix Decoding Algorithm for Rank-Error-Correcting Codes// In G. Cohen, S. Litsyn, A. Lobstein, G. Zemor (Eds.) ALGEBRAIC CODING, pp. 126 - 133; Lecture Notes in Computer Science. V. 573, Springer-Verlag, 1991.

[11] Johansson T., Ourivski A.V. New technique for decoding codes in the rank metric and its cryptography applications//Problems Inform. Transm. 38(3). P. 237-246, 2002.

[12] Gaborit P., Ruatta O., Schrek J. On the complexity of the Rank Syndrome Decoding Problem//arXiv:1301.1026v1[cs.CR] 6 Jan 2013.

[13] Levy-dit-Vehel1 F., Jean-Charles Faug'ere J.-Ch., Perret L. Cryptanalysis of MinRank, in: Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008, Proceedings. Series: Lecture Notes in Computer Science. Subseries: Security and Cryptology , Vol. 5157. Wagner, David (Ed.). P. 280-296.2008.

[14] Gabidulin E.M, Pilipchuk N.I., Ourivski A.V. Security of the modified GPT cryptosystem// Proc. ITA, San Diego, February 2014.

[15] Gabidulin E.M., Pilipchuk N.I. GPT Cryptosystem for Information Network Security // International Conference on Information Society (i-Society 2013). i-Society 2013 Proceedings. June 24-26, 2013, Toronto, Canada. P. 21-25.

[16] Silva D., Kschischang F. R., Koetter R. A Rank-Metric Approach to Error Control in Random Network Coding // IEEE Trans. Inform. Theory. 2008. V. 54. 9. P. 3951-3967.

[17] Gabidulin E.M., Pilipchuk N.I., Bossert M. Decoding of the random network codes// Problems of Information Transmission. V.46, issue 4. P.300-320. 2010.

[18] Gabidulin E.M., Pilipchuk N.I., Honary B., Rashwan H. Information security in a random network coding network// Problems of Information Transmission. V.49, issue 2. P.179-191, 2013.