УДК 519.688

*З. Х. Нгуен*

Московский физико-технический институт (государственный университет)

# Криптосистема, основанная на новых ранговых кодах

Криптосистемы с открытым ключом или асимметричные криптосистемы, характеризуются тем, что ключ зашифрования является общедоступным, а ключ расшифрования является секретным и известен только получателю зашифрованного сообщения. В настоящее время основные варианты асимметричных криптосистем основаны на использовании трудных вычислительных задач, таких как разложение целого числа на множители или задачи дискретного логарифма. Менее популярными являются асимметричные криптосистемы, основанные на линейных кодах. Однако в перспективе они могут вытеснить криптосистемы на других принципах, так как с появлением квантовых компьютеров последние станут не стойкими. Ниже будет описана асимметричная криптосистема на линейных кодах в ранговой метрике.

**Ключевые слова:** ранговые коды, система ГПТ, порождающая матрица.

*D. H. Nguyen*

Moscow Institute of Physics and Technology (State University)

# Cryptosystem based on new rank metric codes

The characteristic feature of public key cryptosystems or asymmetric cryptosystems is that the encryption key is public and the decryption key is secret and known only to the recipient of the encrypted message. At present, the main versions of asymmetric cryptosystems are based on the use of difficult computational problems, such as the factorization of an integer or the problems of a discrete logarithm. Asymmetric cryptosystems based on linear codes are less popular. However, in the future they can displace cryptosystems on other principles, since with the advent of quantum computers the latter will not be stable. Below, an asymmetric cryptosystem on linear codes in a rank metric will be described.

**Key words:** rank codes, cryptosystem GPT, generator matrix.

## 1. Введение

Пусть $GF(q)$ – базовое конечное поле, а $GF(q^m)$ – его расширение степени $m$. Пространство векторов $GF(q^m)^m$ длины $m$ снабдим ранговой весовой функцией: ранговый вес вектора $\boldsymbol{g} = (g_1\ g_2\ \dots g_m) \in GF(q^m)^m$ равен максимальному числу координат, линейно независимых над базовым полем.

Линейное пространство векторов размерности $n$ над расширенным полем $GF(q^m)$ обозначается $GF(q^m)^n$. Оно состоит из векторов с координатами из расширенного поля:

$$\boldsymbol{v} = \begin{bmatrix} v_0 & v_1 & \cdots & v_v n-1 \end{bmatrix}, v_{i,j} \in GF(q^m). \tag{1}$$

Ранг вектора $\boldsymbol{v}$ определяется как максимальное число линейно независимых над основным полем $GF(q)$ координат вектора.

В этой статье мы рассмотриваем только случай когда $n = m$.

*Векторным ранговым кодом* $\mathcal{V}$ называется любой набор векторов из векторного пространства $GF(q^m)^m$.
*Ранговым расстоянием* $d$ векторного кода $\mathcal{V}$ называется наименьший ранг попарных разностей кодовых векторов:

$$d = \min_{v_1 \neq v_2} Rk(v_1 - v_2), v_1, v_2 \in \mathcal{V}.$$

Линейный векторный ранговый $[m, k, d]$-код над $GF(q^m)$ — это $k$-мерное подпространство пространства векторов $GF(q^m)^m$ с ранговым расстоянием $d$. Число векторов в $k$-мерном подпространстве равно $q^{mk}$.

Из границы Синглтона следует

$$k \leq m - d + 1.$$

Если достигается знак равенства, то код называется кодом с максимальным ранговым расстоянием (MPP-кодом).

Линейные ранговые коды определяются порождающейся матрицей [1]:

$$\boldsymbol{G}_k = \begin{pmatrix} g_1 & g_2 & \cdots & g_m \\ g_1^q & g_2^q & \cdots & g_m^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_m^{q^2} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_m^{q^{k-1}} \end{pmatrix} \in GF(q^m)^m. \tag{2}$$

## 2. Система ГПТ

Система ГПТ с открытым ключом предложена Габидулиным, Парамоновым, Третьяковым в 1991 году [2]. Открытый текст – это любой $k$-вектор $\boldsymbol{m} = (m_1, m_2, ..., m_k), m_i \in GF(q^m)$ Открытый ключ – это $k \times (m + t)$ матрица.

$$\boldsymbol{G_{pub}} = \boldsymbol{S}(\boldsymbol{Y} \quad \boldsymbol{G}_k)\boldsymbol{P}. \tag{3}$$

Здесь $\boldsymbol{G_{pub}} \in GF(q^m)^{k \times m}$ – это открытый ключ, известный всем пользователем.
Матрица $\boldsymbol{S} \in GF(q^m)^{k \times k}$ – это строчный скремблер, который перемешивает строки последующих матриц.
Матрица $\boldsymbol{Y} \in GF(q^m)^{k \times t}$ – это матрица искажения, имеющая ранг $t$.
Матрица $\boldsymbol{G_k}$ (2) – порождающая матрица рангового кода.
Матрица $\boldsymbol{P} \in GF(q)^{(t+m)\times(t+m)}$ – это столбцевой скремблер, который перемешивает столбцы матрицы $(\boldsymbol{Y} \quad \boldsymbol{G_k})$.
Секретные ключи – это матрицы $\boldsymbol{S, Y, G_k, P}$ и быстрый алгоритм декодирования MPP кода.
**Шифрование**: Пусть $\boldsymbol{m}$ – открытый текст. Тогда шифротекст задается соотношением

$$\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G}_{pub} + \boldsymbol{e}_{art}, \tag{4}$$

где $\boldsymbol{e}_{art}$ – вектор искусственной ошибки рангового веса $t_2 < t = (n - k + 1)/2$.
**Расшифрование**: После получения шифротекста $\boldsymbol{c}$ легальный пользователь вычисляет:

$$\boldsymbol{c}^{'} = (c_1, c_2, \cdots, c_{t_1+m}) = \boldsymbol{c}\boldsymbol{P}^{-1} = \boldsymbol{m}\boldsymbol{S}[\boldsymbol{Y} \ \boldsymbol{G_k} + \boldsymbol{X}] + \boldsymbol{e}\boldsymbol{P}^{-1}.$$

Из вектора $\boldsymbol{c}^{'}$ извлекает подвектор:

$$\boldsymbol{c}^{''} = (c_{t+1}^{'}, c_{t+2}^{'}, \cdots, c_{t_1+m}^{'}) = \boldsymbol{m}\boldsymbol{S}\boldsymbol{G_k} + \boldsymbol{m}\boldsymbol{S}\boldsymbol{X} + \boldsymbol{e}_{art}^{''}, \tag{5}$$

где $\boldsymbol{e}''_{art}$ – подвектор $\boldsymbol{e}\boldsymbol{P}^{-1}$. Применяя к вектору $\boldsymbol{c}''$ быстрый алгоритм декодирования, легальный пользователь находит вектор $\boldsymbol{m}\boldsymbol{S}$ и открытый текст как вектор $\boldsymbol{m}$.

**Атаки Овербека**: Овербек в работе [3] предложил следующую структурную атаку, цель которой восстановить закрытые ключи $\boldsymbol{G}_{pub}$.

Искусственная ошибка $\boldsymbol{e}_{art}$ является исправляемой ранговой ошибкой. Столбцевой скремблер $\boldsymbol{P}$ нужно выбрать так, чтобы вектор $\boldsymbol{e}_{art}\boldsymbol{P}^{-1}$ являлся исправляемой ранговой ошибкой. В этом случае:

$$Rk_{col}(\boldsymbol{e}_{art}) = Rk(\boldsymbol{e}_{art}\boldsymbol{P}^{-1}) \leq t = [\frac{d-1}{2}].$$

Овербек показал, что систему ГПТ можно взломать в полиномиальное время. Критический момент атаки обоснован при условии, что все элементы матрицы $\boldsymbol{P}$ находятся в базовом поле $GF_q$.

Пусть $\sigma(x) = x^q$ для $x \in GF_{q^N}$ будет автоморфизмом Фробениуса. Для матрицы $\boldsymbol{T} = (t_{ij})$ над полем $GF_{q^N}$ пусть $\sigma(\boldsymbol{T} = (\sigma(t_{ij})) = (t^q_{ij})$. Для любого целого числа $s$ пусть $\sigma^s(\boldsymbol{T}) = \sigma(\sigma^{-1}(\boldsymbol{T}))$. Очевидно что $\sigma^N = \sigma$, а $\sigma$ имеет следующие простые свойства:

- $\sigma(a+b) = \sigma(a) + \sigma(b)$.
- $\sigma(ab) = \sigma(a)\sigma(b)$.
- Если матрица $\boldsymbol{P}$ над полем $F_q$ то $\sigma(\boldsymbol{P}) = \boldsymbol{P}$.

Для возлома системы ГПТ криптоаналитик для некоторого целого числа $u$ из открытого ключа $\boldsymbol{G}_{pub} = \boldsymbol{S}[\boldsymbol{Y}\ \boldsymbol{G}_k]\boldsymbol{P}$ сформировал расширенный ключ $\boldsymbol{G}_{ext,\,key}$ следующим образом:

$$\boldsymbol{G}_{ext,\,pub} = \begin{Vmatrix} \boldsymbol{G}_{pub} \\ \sigma(\boldsymbol{G}_{pub}) \\ \sigma^2(\boldsymbol{G}_{pub}) \\ \cdots \\ \sigma^u(\boldsymbol{G}_{pub}) \end{Vmatrix} = \begin{Vmatrix} \boldsymbol{S} & [\boldsymbol{Y} & \boldsymbol{G}_k] & \boldsymbol{P} \\ \sigma(\boldsymbol{S}) & [\sigma(\boldsymbol{Y}) & \sigma(\boldsymbol{G}_k)] & \boldsymbol{P} \\ \sigma^2(\boldsymbol{S}) & [\sigma^2(\boldsymbol{Y}) & \sigma^2(\boldsymbol{G}_k)] & \boldsymbol{P} \\ \cdots & \cdots & \cdots & \cdots \\ \sigma^u(\boldsymbol{S}) & [\sigma^u(\boldsymbol{Y}) & \sigma^u(\boldsymbol{G}_k)] & \boldsymbol{P} \end{Vmatrix}. \tag{6}$$

Здесь использовано свойство, что $\sigma(\boldsymbol{P}) = \boldsymbol{P}$, если матрица $\boldsymbol{P}$ над полем $F_q$. Перепишите эту матрицу так:

$$\boldsymbol{G}_{ext,pub} = \boldsymbol{S}_{ext}[\boldsymbol{Y}_{ext} \quad \boldsymbol{G}_{ext}]\boldsymbol{P}, \tag{7}$$

где

$$\boldsymbol{S}_{ext} = Diag[\boldsymbol{S}\ \sigma(\boldsymbol{S}) \cdots \sigma^u(\boldsymbol{S})],$$

$$\boldsymbol{W}_{ext} = \begin{bmatrix} \boldsymbol{Y} \\ \sigma(\boldsymbol{Y}) \\ \vdots \\ \sigma^u(\boldsymbol{Y}) \end{bmatrix}, \boldsymbol{G}_{ext} = \begin{bmatrix} \boldsymbol{G}_k \\ \sigma(\boldsymbol{G}_k) \\ \vdots \\ \sigma^u(\boldsymbol{G}_k) \end{bmatrix}.$$

Выбрать

$$u = m - k - 1. \tag{8}$$

Для матрицы $k \times t_1$

$$\boldsymbol{Y} = \begin{bmatrix} Y_{11} & Y_{12} & \cdots & Y_{1,t_1} \\ Y_{21} & Y_{22} & \cdots & Y_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ Y_{k,1} & Y_{k,2} & \cdots & Y_{k,t_1} \end{bmatrix}. \tag{9}$$

удалить последнюю строку, получается матрица $(k-1)\times t_1$:

$$\boldsymbol{Y}_1 = \begin{bmatrix} Y_{11} & Y_{12} & \cdots & Y_{1,t_1} \\ Y_{21} & Y_{22} & \cdots & Y_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ Y_{k-1,1} & Y_{k-1,2} & \cdots & Y_{k-1,t_1} \end{bmatrix}. \tag{10}$$

Из матрицы $\boldsymbol{Y}$ удалить первую строку, получается матрица:

$$\boldsymbol{Y}_2 = \begin{bmatrix} Y_{21} & Y_{22} & \cdots & Y_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ Y_{k-1,1} & Y_{k-1,2} & \cdots & Y_{k-1,t_1} \\ Y_{k,1} & Y_{k,2} & \cdots & Y_{k,t_1} \end{bmatrix}. \tag{11}$$

Функция $T$: $\mathbb{F}_{q^N}^{k\times t_1} \to \mathbb{F}_{q^N}^{(k-1)\times t_1}$, если $\boldsymbol{Y} \in \mathbb{F}_{q^N}^{k\times t_1}$ то

$$T(\boldsymbol{Y}) = \boldsymbol{W} = \sigma(\boldsymbol{Y}_1) - \boldsymbol{Y}_2.$$

Пусть

$$\boldsymbol{W}_{ext} = \begin{bmatrix} \boldsymbol{Y} \\ \sigma(\boldsymbol{Y}) \\ \vdots \\ \sigma^{u-1}(\boldsymbol{Y}) \end{bmatrix}. \tag{12}$$

Используя подходящие преобразования строк, можно переписать расширенный ключ в виде

$$\widetilde{\boldsymbol{G}}_{pub,ext} = \widetilde{\boldsymbol{S}}_{ext} \left[\begin{array}{cc|c} & & \\ \boldsymbol{Z} & & \boldsymbol{G}_{n-1} \\ & & \\ \hline \boldsymbol{W}_{ext} & & 0 \end{array}\right] \boldsymbol{P}, \tag{13}$$

где $\boldsymbol{G}_{n-1}$ – порождающая матрица $(m, m-1, 2)$ МРР кода.
Найти решение систем уравнений:

$$\widetilde{\boldsymbol{S}}_{ext} \left[\begin{array}{cc|c} & & \\ \boldsymbol{Z} & & \boldsymbol{G}_{n-1} \\ & & \\ \hline \boldsymbol{W}_{ext} & & 0 \end{array}\right] \boldsymbol{P}\boldsymbol{u}^T = 0, \tag{14}$$

где вектор-столбец $\boldsymbol{u}$ над полем $F_{q^N}$ длины $t_1 + m$.
Представлять вектор $\boldsymbol{P}\boldsymbol{u}^{\boldsymbol{T}}$ как:

$$\boldsymbol{P}\boldsymbol{u}^T = [\boldsymbol{y} \;\; \boldsymbol{h}]^T.$$

Здесь вектор $\boldsymbol{y}$ имеет длину $t_1$ и вектор $\boldsymbol{h}$ имеет длину $m$. Тогда система (11) эквивалентна следующей системе:

$$\boldsymbol{Z}\boldsymbol{y}^T + \boldsymbol{G}_{n-1}\boldsymbol{h}^T = 0, \tag{15}$$

$$\boldsymbol{W}_{ext}\boldsymbol{y}^T = 0. \tag{16}$$

Предположим, что выполнено следующее условие:

$$Rk(\boldsymbol{W}_{ext} \mid F_{q^N}) = t_1,$$

тогда уравнение (16) имеет только тривиальное решение $\boldsymbol{y}^T = \boldsymbol{0}$. Следовательно, уравнение (15) примет вид

$$\boldsymbol{G}_{n-1}\boldsymbol{h}^T = 0.$$

Из этого можно найти первую строку проверочной матрицы для кода с порождающей матрицей (2). Затем вычислить всю матрицу.

## 3. Новая система Шики

В настоящее время найдены новые МРР-коды с частично разрушенной структурой. Порождающая матрица новых кодов может быть представлена в следующем виде:

$$\widetilde{\boldsymbol{G}}_k = \begin{pmatrix} g_1 + \eta g_1^{q^k} & g_2 + \eta g_2^{q^k} & \cdots & g_m + \eta g_m^{q^k} \\ g_1^q & g_2^q & \cdots & g_m^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_m^{q^2} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{k-1}} & g_2 q^{k-1} & \cdots & g_m^{q^{k-1}} \end{pmatrix} \in \tag{17}$$

$$\in GF(q^m), \eta \in GF(q^m), N(\eta) = \eta^{\frac{q^m-1}{q-1}} \neq (-1)^{mk}.$$

Проверочная матрица имеет такой вид:

$$\widetilde{\boldsymbol{H}}_{m-k} = \begin{pmatrix} \boldsymbol{h}^{q^k} - \eta \boldsymbol{h} \\ \boldsymbol{h}^{q^{k+1}} \\ \boldsymbol{h}^{q^{k+2}} \\ \vdots \\ \boldsymbol{h}^{q^{m-1}} \end{pmatrix} \in GF(q^m). \tag{18}$$

**Атака Овербека на новую систему Шики**: Аналогично для системы ГПТ используется такой же подход к взлому кода Шики.
Из открытого ключа $\boldsymbol{G}_{pub} = \boldsymbol{S}[\boldsymbol{Y}\ \widetilde{\boldsymbol{G}}_k]\boldsymbol{P}$ сформирован расширенный ключ $\boldsymbol{G}_{ext,\,key}$ следующим образом:

$$\boldsymbol{G}_{ext,\,pub} = \begin{Vmatrix} \boldsymbol{G}_{pub} \\ \sigma(\boldsymbol{G}_{pub}) \\ \sigma^2(\boldsymbol{G}_{pub}) \\ \cdots \\ \sigma^u(\boldsymbol{G}_{pub}) \end{Vmatrix} = \begin{Vmatrix} \boldsymbol{S} & [\boldsymbol{Y} & \widetilde{\boldsymbol{G}}_k] & \boldsymbol{P} \\ \sigma(\boldsymbol{S}) & [\sigma(\boldsymbol{Y}) & \sigma(\widetilde{\boldsymbol{G}}_k)] & \boldsymbol{P} \\ \sigma^2(\boldsymbol{S}) & [\sigma^2(\boldsymbol{Y}) & \sigma^2(\widetilde{\boldsymbol{G}}_k)] & \boldsymbol{P} \\ \cdots & \cdots & \cdots & \cdots \\ \sigma^u(\boldsymbol{S}) & [\sigma^u(\boldsymbol{Y}) & \sigma^u(\widetilde{\boldsymbol{G}}_k)] & \boldsymbol{P} \end{Vmatrix}. \tag{19}$$

Здесь использовано свойство, что $\sigma(\boldsymbol{P}) = \boldsymbol{P}$, если матрица $\boldsymbol{P}$ над полем $F_q$. Перепишем эту матрицу так:

$$\boldsymbol{G}_{ext,\,pub} = \boldsymbol{S}_{ext}[\boldsymbol{Y}_{ext} \quad \boldsymbol{G}_{ext}]\boldsymbol{P},$$

где

$$\boldsymbol{S}_{ext} = Diag[\boldsymbol{S}\ \sigma(\boldsymbol{S}) \cdots \sigma^u(\boldsymbol{S})],$$

$$\boldsymbol{W}_{ext} = \begin{bmatrix} \boldsymbol{Y} \\ \sigma(\boldsymbol{Y}) \\ \vdots \\ \sigma^u(\boldsymbol{Y}) \end{bmatrix}, \boldsymbol{G}_{ext} = \begin{bmatrix} \widetilde{\boldsymbol{G}}_k \\ \sigma(\widetilde{\boldsymbol{G}}_k) \\ \vdots \\ \sigma^u(\widetilde{\boldsymbol{G}}_k) \end{bmatrix}.$$

Выберем $u = m - k - 1$. Для матрицы $k \times t_1$

$$\boldsymbol{Y} = \begin{bmatrix} Y_{11} & Y_{12} & \cdots & Y_{1,t_1} \\ Y_{21} & Y_{22} & \cdots & Y_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ Y_{k,1} & Y_{k,2} & \cdots & Y_{k,t_1} \end{bmatrix},$$

удалив последнюю строку, получаем матрицу $(k-1) \times t_1$:

$$\boldsymbol{Y}_1 = \begin{bmatrix} Y_{11} & Y_{12} & \cdots & Y_{1,t_1} \\ Y_{21} & Y_{22} & \cdots & Y_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ Y_{k-1,1} & Y_{k-1,2} & \cdots & Y_{k-1,t_1} \end{bmatrix}.$$

После удаления из матрицы $\boldsymbol{Y}$ первой строки, получается матрица

$$\boldsymbol{Y}_2 = \begin{bmatrix} Y_{21} & Y_{22} & \cdots & Y_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ Y_{k-1,1} & Y_{k-1,2} & \cdots & Y_{k-1,t_1} \\ Y_{k,1} & Y_{k,2} & \cdots & Y_{k,t_1} \end{bmatrix}.$$

Функция $T$: $\mathbb{F}_{q^N}^{k\times t_1} \to \mathbb{F}_{q^N}^{(k-1)\times t_1}$, если $\boldsymbol{Y} \in \mathbb{F}_{q^N}^{k\times t_1}$, то

$$T(\boldsymbol{Y}) = \boldsymbol{W} = \sigma(\boldsymbol{Y}_1) - \boldsymbol{Y}_2.$$

Пусть

$$\boldsymbol{W}_{ext} = \begin{bmatrix} \boldsymbol{Y} \\ \sigma(\boldsymbol{Y}) \\ \vdots \\ \sigma^{u-1}(\boldsymbol{Y}) \end{bmatrix}.$$

**Теорема 1.** *Для любых элементов $a$ и $b$ из $GF(p^m)$*

$$(a+b)^p = a^p + b^p.$$

Используя подходящие преобразования строк, можно переписать расширенный ключ в виде

$$\widetilde{\boldsymbol{G}}_{pub,ext} = \widetilde{\boldsymbol{S}}_{ext} \left[\begin{array}{c|c} \boldsymbol{Z} & \widetilde{\boldsymbol{G}}_m \\ \boldsymbol{W}_{ext} & 0 \end{array}\right] \boldsymbol{P}.$$

где $\widetilde{\boldsymbol{G}}_m$ имеет следующий вид:

$$\widetilde{\boldsymbol{G}}_m = \begin{pmatrix} g_1 + \eta g_1^{q^k} & g_2 + \eta g_2^{q^k} & \cdots & g_m + \eta g_m^{q^k} \\ g_1^q & g_2^q & \cdots & g_m^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_m^{q^2} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{k-1}} & g_2 q^{k-1} & \cdots & g_m^{q^{k-1}} \\ g_1^q + \eta^q g_1^{q^{k+1}} & g_2^q + \eta^q g_2^{q^{k+1}} & \cdots & g_m^q + \eta^q g_m^{q^{k+1}} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{m-k}} + \eta^{q^{m-k}} g_1^{q^m} & g_2^{q^{m-k}} + \eta^{q^{m-k}} g_2^{q^m} & \cdots & g_m^{q^{m-k}} + \eta^{q^{m-k}} g_m^{q^m} \end{pmatrix}. \tag{20}$$

Требуется найти решение системы уравнений:

$$\widetilde{\boldsymbol{S}}_{ext} \left[\begin{array}{c|c} \boldsymbol{Z} & \widetilde{\boldsymbol{G}}_m \\ \boldsymbol{W}_{ext} & 0 \end{array}\right] \boldsymbol{P}\boldsymbol{u}^T = 0, \tag{21}$$

где вектор-столбец $\boldsymbol{u}$ над полем $F_{q^N}$ длины $t_1 + m$. Представим вектор $\boldsymbol{P}\boldsymbol{u}^{\boldsymbol{T}}$ как

$$\boldsymbol{P}\boldsymbol{u}^T = [\boldsymbol{y} \;\; \boldsymbol{h}]^T.$$

Здесь векторы $\boldsymbol{y}$ и $\boldsymbol{h}$ имеют длину $t_1$ и $m$ соответственно. Тогда система (21) эквивалента следующей системе:

$$\boldsymbol{Z}\boldsymbol{y}^T + \widetilde{\boldsymbol{G}}_m \boldsymbol{h}^T = 0, \tag{22}$$

$$\boldsymbol{W}_{ext}\boldsymbol{y}^T = 0. \tag{23}$$

Предположим, что выполнено следующее условие:

$$Rk(\boldsymbol{W}_{ext} \mid F_{q^N}) = t_1,$$

тогда уравнение (23) имеет только тривиальное решение $\boldsymbol{y}^T = \mathbf{0}$. Следовательно, уравнение (22) примет вид

$$\widetilde{\boldsymbol{G}}_m \boldsymbol{h}^T = 0.$$

**Например**: Рассмотрим случай $m = 7, t_2 = 1, t = 2, k = 3, d = 5$. При декодировании не используется матрица $\boldsymbol{S}$, функция сигма от $\boldsymbol{P}$ не меняет вид матрицы, поэтому здесь рассмотрим только часть расширенного ключа $[\boldsymbol{Y} \quad \widetilde{\boldsymbol{G}}_k]$.
В случае стандартной системы ГПТ они имеют следующий вид:

$$\boldsymbol{Y} = \begin{bmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \\ Y_{31} & Y_{32} \end{bmatrix}, \boldsymbol{G}_k = \begin{pmatrix} g_1 & g_2 & \cdots & g_7 \\ g_1^q & g_2^q & \cdots & g_7^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_7^{q^2} \end{pmatrix}.$$

Для кода Шики:

$$\boldsymbol{Y} = \begin{bmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \\ Y_{31} & Y_{32} \end{bmatrix}, \boldsymbol{G}_{ext,pub} = \begin{pmatrix} g_1 + \eta g_1^{q^3} & g_2 + \eta g_2^{q^3} & \cdots & g_7 + \eta g_7^{q^3} \\ g_1^q & g_2^q & \cdots & g_7^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_7^{q^2} \end{pmatrix}.$$

При попытке взломать систему с помощью расширенного ключа для системы ГПТ:

$$[\boldsymbol{Y}_{ext} \quad \boldsymbol{G}_{ext}] = \begin{pmatrix} Y_{11} & Y_{12} & g_1 & g_2 & \cdots & g_7 \\ Y_{21} & Y_{22} & g_1^q & g_2^q & \cdots & g_7^q \\ Y_{31} & Y_{32} & g_1^{q^2} & g_2^{q^2} & \cdots & g_7^{q^2} \\ Y_{31}^q & Y_{32}^q & g_1^{q^3} & g_2^{q^3} & \cdots & g_7^{q^3} \\ Y_{31}^{q^2} & Y_{32}^{q^2} & g_1^{q^4} & g_2^{q^4} & \cdots & g_7^{q^4} \\ Y_{31}^{q^3} & Y_{32}^{q^3} & g_1^{q^5} & g_2^{q^5} & \cdots & g_7^{q^5} \\ Y_{11}^q - Y_{21} & Y_{12}^q - Y_{22} & 0 & 0 & \cdots & 0 \\ Y_{21}^q - Y_{31} & Y_{22}^q - Y_{32} & 0 & 0 & \cdots & 0 \\ Y_{11}^{q^2} - Y_{21}^q & Y_{12}^{q^2} - Y_{22}^q & 0 & 0 & \cdots & 0 \\ Y_{21}^{q^2} - Y_{31}^q & Y_{22}^{q^2} - Y_{32}^q & 0 & 0 & \cdots & 0 \\ Y_{11}^{q^3} - Y_{21}^{q^2} & Y_{12}^{q^3} - Y_{22}^{q^2} & 0 & 0 & \cdots & 0 \\ Y_{21}^{q^3} - Y_{31}^{q^2} & Y_{22}^{q^3} - Y_{32}^{q^2} & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Для кода Шики:

$$[\boldsymbol{Y}_{ext} \quad \boldsymbol{G}_{ext}] = \begin{pmatrix} Y_{11} & Y_{12} & g_1 + \eta g_1^{q^3} & g_2 + \eta g_2^{q^3} & \cdots & g_7 + \eta g_7^{q^3} \\ Y_{21} & Y_{22} & g_1^q & g_2^q & \cdots & g_7^q \\ Y_{31} & Y_{32} & g_1^{q^2} & g_2^{q^2} & \cdots & g_7^{q^2} \\ Y_{11}^q & Y_{12}^q & g_1^q + \eta^q g_1^{q^4} & g_2^q + \eta^q g_2^{q^4} & \cdots & g_7^q + \eta^q g_7^{q^4} \\ Y_{31}^q & Y_{32}^q & g_1^{q^3} & g_2^{q^3} & \cdots & g_7^{q^3} \\ Y_{11}^{q^2} & Y_{12}^{q^2} & g_1^{q^2} + \eta^{q^2} g_1^{q^5} & g_2^q + \eta^{q^2} g_2^{q^5} & \cdots & g_7^{q^2} + \eta^{q^2} g_7^{q^5} \\ Y_{31}^{q^2} & Y_{32}^{q^2} & g_1^{q^4} & g_2^{q^4} & \cdots & g_7^{q^4} \\ Y_{21}^q - Y_{31} & Y_{22}^q - Y_{32} & 0 & 0 & \cdots & 0 \\ Y_{21}^{q^2} - Y_{31}^q & Y_{22}^{q^2} - Y_{32}^q & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

## 4. Заключение

В работе проведен анализ криптостойкости системы ГПТ и нового кода Шики перед атакой Овербека. Новый код Шики является более стойким к атаке Овербека, чем система ГПТ. Таким образом, его можно использовать для противодействия атакам Овербека и обеспечить высокий уровень безопасности.

## Литература


1. *Габидулин Э.М.* Лекции по алгебраическому кодированию. М.: МФТИ, 2015.
2. *Gabidulin E.M., Paramonov A.V., Tretjakov O.V.* Ideals over a Non-commutative Ring and Their Application in Cryptology // Advances in Cryptology Eurocrypt' 91. LNCS 547. 1991. P. 482–489.
3. *Overbeck R.* Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes // Journal of Cryptology. 2008. V. 21, N 2.


## References


1. *Gabidulin E.M.* Lectures on algebraic coding. M.: MIPT, 2015.
2. *Gabidulin E.M., Paramonov A.V., Tretjakov O.V.* Ideals over a Non-commutative Ring and Their Application in Cryptology, in: Advances in Cryptology Eurocrypt' 91. LNCS 547. 1991. P. 482–489.
3. *Overbeck R.* Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes. Journal of Cryptology. 2008. V. 21, N 2.


*Поступила в редакцию 18.09.2018*