**УДК 519.1** **DOI: 10.14529/mmp210302**

# О КРИПТОАНАЛИЗЕ СИСТЕМЫ BBCRS НА ДВОИЧНЫХ КОДАХ РИДА – МАЛЛЕРА

***Ю.В. Косолапов*[1], *А.А. Лелюк*[1]**
[1]Южный федеральный университет, г. Ростов-на-Дону, Российская Федерация

В работе рассматривается система система BBCRS – модификация криптосистемы Мак-Элиса, предложенная М. Балди и др. В модификации матрица $G_{pub}$ публичного ключа представляет собой произведение трех матриц: невырожденной $(k\times k)$-матрицы $S$, порождающей матрицы $G$ секретного $[n,k]_q$-кода $C_{sec}$ и невырожденной $(n\times n)$-матрицы $Q$ специального вида. Отличие системы BBCRS от системы, предложенной Р. Мак-Элисом, состоит в том, что подстановочная матрица, используемая в системе Мак-Элиса, заменена матрицей $Q$, представляющей сумму подстановочной матрицы $P$ и матрицы $R$ малого ранга $r(R)$. Позже В. Готье и др. построили атаку, позволяющую дешифровать сообщения в случае, когда $C_{sec}$ – обобщенный код Рида – Соломона (ОРС-код) и $r(R)=1$. Ключевыми этапами построенной атаки являются, во-первых, нахождение пересечения линейных оболочек $\mathcal{L}(G_{pub})=C_{pub}$ и $\mathcal{L}(GP)=C$, натянутых соответственно на строки матриц $G_{pub}$ и $GP$, а во-вторых, нахождение кода по подкоду $C_{pub}\cap C$. В настоящей работе строится атака в случае, когда $C_{sec}=\mathrm{RM}(r,m)$ – двоичный код Рида – Маллера порядка $r$ и длины $2^m$ при $r(R)=1$. В построенной в настоящей работе атаке этапы нахождения кодов $C_{pub}\cap C$ и $C$ полностью отличаются от соответствующих этапов для ОРС-кодов, а остальные шаги атаки адаптируют известные результаты криптоанализа системы BBCRS на ОРС-кодах.

*Ключевые слова: криптосистема BBCRS; коды Рида – Маллера; криптоанализ.*

## Введение

Первой асимметричной кодовой криптосистемой считается система на кодах Гоппы, предложенная Робертом Мак-Элисом в 1978 г. [1]. В основе криптосистем типа Мак-Элиса лежит использование помехоустойчивого $[n,k]_q$-кода $C_{sec}$ размерности $k$ и длины $n$ над конечным полем $\mathbb{F}_q$. Матрица $\tilde{G}$ публичного ключа имеет вид

$$\tilde{G}=SGP, \tag{1}$$

где $S$ – невырожденная $(k\times k)$-матрица, $G$ – порождающая матрица кода $C_{sec}$, $P$ – подстановочная $(n\times n)$-матрица. Далее такую криптосистему будем обозначать $\mathrm{McE}(C_{sec})$. Исследования показывают, что стойкость асимметричных кодовых криптосистем зависит от используемых кодов и от конструкции ключа. В [2] построен алгоритм расщепления носителя, который может быть использован для нахождения подходящего секретного ключа в случае, когда $C_{sec}$ не является секретным. Сложность этого алгоритма экспоненциально зависит от размерности остова (hull) используемого в криптосистеме кода – пересечения $C_{sec}$ и дуального к нему $C_{sec}^{\perp}$. При случайном выборе кода эта размерность небольшая, поэтому в среднем алгоритм расщепления носителя считается эффективным. Для некоторых кодов размерность остова сопоставима с размерностью кода, и поэтому алгоритм расщепления носителя в этом случае не является эффективным. В частности, для двоичного кода Рида – Маллера $C_{sec}$ размерность остова равна минимуму между $\dim(C_{sec})$ и $\dim(C_{sec}^{\perp})$. Тем не менее в [3]

и [4] построены эффективные алгоритмы нахождения подходящих секретных ключей для криптосистемы типа Мак-Элиса на двоичных кодах Рида – Маллера. Когда используемый в криптосистеме $C_{sec}$ является секретным, задача нахождения подходящего секретного ключа считается сложнее. Однако в случае применения в системе типа Мак-Элиса обобщенных кодов Рида – Соломона в [5] найден полиномиальный алгоритм восстановления подходящего секретного ключа по публичному ключу. Модификация матрицы $SG$ в (1) или применение известных кодовых конструкций не всегда усиливает стойкость. В частности, в работах [6] и [7] для обобщенных кодов Рида – Соломона и бинарных кодов Рида – Маллера соответственно показано, что в некоторых случаях подходящий секретный ключ для системы из [8], в которой в отличие от систем типа Мак-Элиса ранг матрицы $S$ меньше $k$, может быть найден за полиномиальное время. В [9] Сидельниковым В.М. было предложено усилить стойкость кодовой криптосистемы за счет использования вместо $SG$ в (1) конкатенации случайно выбранных порождающих матриц кода $C_{sec}$. Эта конструкция обобщена в [10] за счет конкатенации порождающих матриц разных кодов $C_1$, ..., $C_u$. В ряде случаев криптоанализ таких систем может быть эффективным образом сведен к анализу систем типа Мак-Элиса $\mathrm{McE}(C_1)$, ..., $\mathrm{McE}(C_u)$ [11].

Заметим, что для оригинальной системы Мак-Элиса на кодах Гоппы до настоящего момента не найдено эффективного алгоритма нахождения подходящего секретного ключа по публичному ключу. Однако эта система характеризуется большим размером публичного ключа. В [12] с целью уменьшения размера ключа и повышения стойкости системы типа Мак-Элиса предложено вместо подстановочной матрицы $P$ в (1) для маскировки порождающей матрицы кода использовать невырожденную матрицу $Q = P + R$, где $R$ – матрица ранга 1. В случае применения обобщенных кодов Рида – Соломона это означает, что атака из [5] для такой криптосистемы неприменима. Однако в [14] был найден эффективный способ сведения криптоанализа системы из [12] на обобщенных кодах Рида – Соломона (ОРС-кодах) к применению криптоаналитического алгоритма из [5]. Одним из ключевых этапов атаки является нахождение пересечения линейных оболочек $\mathcal{L}(SGQ) = C_{pub}$ и $\mathcal{L}(GP) = C$, натянутых соответственно на строки матриц $SGQ$ и $GP$, и нахождение кода по подкоду $C_{pub} \cap C$. Настоящая работа посвящена адаптации алгоритма из [14] к системе из [12], построенной на бинарном коде Рида – Маллера $C_{sec} = \mathrm{RM}(r, m)$ порядка $r$ и длины $2^m$. В построенной в настоящей работе атаке этапы нахождения кодов $C_{pub} \cap C$ и $C$ полностью отличаются от соответствующих этапов для ОРС-кодов, а остальные шаги атаки адаптируют известные результаты криптоанализа, примененные в случае использования ОРС-кодов.

Кроме введения и заключения работа содержит три раздела. В первом разделе приводятся необходимые сведения о линейных кодах и двоичных кодах Рида – Маллера, свойствах произведения Шура – Адамара для кодов, а также доказывается теорема о некоторых свойствах степени подкода кода $\mathrm{RM}(1, m)$. Во втором разделе описывается криптосистема BBCRS из [12], и излагаются в удобном виде основные этапы атаки из [14]. Третий раздел посвящен реализации этапов атаки в случае, когда в основе системы BBCRS лежит код $\mathrm{RM}(r, m)$.

# 1. Предварительные сведения и результаты

## 1.1. Линейные коды

Пусть $\mathbb{F}_q$ – поле Галуа мощности $q$ и $[k] = \{1, ..., k\}$ для $k \in \mathbb{N}$. Носителем $\mathrm{supp}(\mathbf{x})$ вектора $\mathbf{x} = (x_1, ..., x_n)$ из пространства $\mathbb{F}_q^n$ называется множество номеров его ненулевых координат, а весом $\mathrm{wt}(\mathbf{x})$ этого вектора – количество ненулевых координат. В частности, для нулевого вектора $\mathbf{0} \in \mathbb{F}_q^n$ имеем: $\mathrm{supp}(\mathbf{0}) = \varnothing$, $\mathrm{wt}(\mathbf{0}) = 0$. Линейным $[n, k, d]_q$-кодом $C \subset \mathbb{F}_q^n$ называется подпространство $\mathbb{F}_q^n$ размерности $k$, для которого $d = \min_{\mathbf{c} \in C \setminus \{\mathbf{0}\}} \mathrm{wt}(\mathbf{c})$ – кодовое расстояние. Далее предполагается, что $\cup_{\mathbf{c} \in C} \mathrm{supp}(\mathbf{c}) = [n]$ для $[n, k, d]_q$-кода $C$, то есть $C$ не имеет фиктивных координат. Иногда $[n, k, d]_q$-код называют $[n, k]_q$-кодом и кодом коразмерности $n - k$. Дуальным или ортогональным кодом к $[n, k]_q$-коду $C$ называется $[n, n-k]_q$-код $C^\perp = \{\mathbf{y} \in \mathbb{F}_q^n : \forall \mathbf{c} \in C \ (\mathbf{c}, \mathbf{y}) = 0\}$, где $(\mathbf{c}, \mathbf{y}) = \sum_{i=1}^n c_i y_i$ – скалярное произведение векторов из $\mathbb{F}_q^n$. Пусть $\mathcal{S}_n$ – симметрическая группа подстановок элементов множества $[n]$, $\sigma (\in \mathcal{S}_n)$ – некоторая подстановка, подстановочную $(n \times n)$-матрицу, соответствующую $\sigma$, обозначим $P_\sigma$. Для $[n, k, d]_q$-кода $C$ код $D = \{(c_{\sigma(1)}, ..., c_{\sigma(n)}) : (c_1, ..., c_n) \in C\}$ называется перестановочно эквивалентным к $C$ (будем писать $C \sim D$). Множество $\mathrm{PAut}(C) = \{\sigma : \sigma(C) = C\}$ называется группой перестановочных автоморфизмов $C$.

Для векторов $\mathbf{a} = (a_1, ..., a_n)$ и $\mathbf{b} = (b_1, ..., b_n)$ из $\mathbb{F}_q^n$ рассмотрим покоординатное умножение $\mathbf{a} \star \mathbf{b} = (a_1 b_1, ..., a_n b_n)$, также называемое произведением Шура – Адамара [13]. Произведением Шура – Адамара матриц $A$ и $B$ называется матрица $A \star B$, строки которой имеют вид $\mathbf{a} \star \mathbf{b}$, где $\mathbf{a}$ пробегает все строки матрицы $A$, а $\mathbf{b}$ – все строки матрицы $B$. Для $[n, k_1]_q$-кода $C_1$ и $[n, k_2]_q$-кода $C_2$ их произведение Шура – Адамара определяется как линейная оболочка, натянутая на множество векторов $\{\mathbf{a} \star \mathbf{b} : \mathbf{a} \in C_1, \mathbf{b} \in C_2\}$: $C_1 \star C_2 = \mathcal{L}(\{\mathbf{a} \star \mathbf{b} : \mathbf{a} \in C_1, \mathbf{b} \in C_2\})$. Квадратом кода $C$ называется пространство (код) $C \star C = C^2$. Аналогично может быть определена любая степень $s$ кода $C$: $C^s = C^{s-1} \star C$. Некоторые свойства произведения Шура – Адамара для векторов и кодов можно найти в [13]. В частности, известно, что $C^s = \mathcal{L}(G^s)$ для любого $s \in \mathbb{N}$ и любой порождающей матрицы $G$ кода $C$.

Над полем $\mathbb{F}_2$ рассмотрим кольцо полиномов $\mathbb{F}_2[X_1, ..., X_m]$ от $m$ переменных. Для полинома $f = f(X_1, ..., X_m)$ рассмотрим вектор $\mathrm{eval}(f) := (f(0, ..., 0), f(0, ..., 1), ..., f(1, ..., 1))$, составленный из значений полинома $f$, вычисленных для всех возможных наборов значений переменных $X_1, ..., X_m$ (наборы значений переменных упорядочены в естественном порядке). Двоичный $[n, k, d]_2$-код Рида – Маллера $\mathrm{RM}(r, m)$ порядка $r$ для $n = 2^m$, $k = \dim(\mathrm{RM}(r, m)) = \sum_{i=0}^r C_m^i$, $d = 2^{m-r}$ определяется так: $\mathrm{RM}(r, m) = \{\mathrm{eval}(f) : f \in \mathbb{F}_2[X_1, ..., X_m], \deg(f) \leqslant r\}$. Получим, что для каждого $\mathbf{c} (\in \mathrm{RM}(r, m))$ найдется единственный полином из $\mathbb{F}_2[X_1, ..., X_m]$

$$f^{\mathbf{c}} = f^{\mathbf{c}}(X_1, ..., X_m) = \sum_{\substack{(\alpha_1, ..., \alpha_m) \in \{0,1\}^m \\ \mathrm{wt}((\alpha_1, ..., \alpha_m)) \leqslant r}} f_{(\alpha_1, ..., \alpha_m)} X_1^{\alpha_1} \cdot ... \cdot X_m^{\alpha_m}, \ f_{(\alpha_1, ..., \alpha_m)} \in \mathbb{F}_2, \quad (2)$$

что $\mathbf{c} = \mathrm{eval}(f^{\mathbf{c}})$. Полином (2) состоит из $\sum_{i=0}^r C_m^i$ слагаемых. Через $M(\mathrm{RM}(r, m))$ обозначим подмножество из $\mathbb{F}_2[X_1, ..., X_m]$, соответствующих кодовым словам из $\mathrm{RM}(r, m)$. Из теории двоичных кодов Рида – Маллера известно, что $\mathrm{RM}(r, m) \subseteq \mathrm{RM}(\min\{r+1; m\}, m)$ и $\mathrm{RM}(r, m)^\perp = \mathrm{RM}(m-r-1, m)$. Тогда остов (hull) кода Рида – Маллера, определяемый как пересечение кода с ортогональным к нему кодом, также

код Рида – Маллера:

$$\mathrm{RM}(r,m)\cap\mathrm{RM}^{\perp}(r,m)=\mathrm{RM}(\min\{r;m-r-1\},m). \tag{3}$$

### 1.2. Свойства произведения Шура – Адамара для подкодов коразмерности один кода $\mathrm{RM}(1,m)$

Из определения кодов Рида – Маллера вытекает, что если $\mathbf{c}_1,\mathbf{c}_2\in\mathrm{RM}(r,m)$, то $\mathbf{c}_1\star\mathbf{c}_2=\mathrm{eval}(f^{\mathbf{c}_1}\cdot f^{\mathbf{c}_2})$. Таким образом, вектору $\mathbf{c}_1\star\mathbf{c}_2$ соответствует полином $f^{\mathbf{c}_1}\cdot f^{\mathbf{c}_2}$ степени не выше $\min\{2r,m\}$. Так как $\mathbf{c}\star\mathbf{c}=\mathbf{c}$ для любого вектора над двоичным полем, то из равенства $\mathbf{c}\star\mathbf{c}=\mathrm{eval}(f^{\mathbf{c}}\cdot f^{\mathbf{c}})=\mathbf{c}=\mathrm{eval}(f^{\mathbf{c}})$ легко получить, что

$$f^{\mathbf{c}}\cdot f^{\mathbf{c}}=f^{\mathbf{c}},\ f^{\mathbf{c}}\cdot(1+f^{\mathbf{c}})=0. \tag{4}$$

В [4] доказано, что $\mathrm{RM}(r_1,m)\star\mathrm{RM}(r_2,m)=\mathrm{RM}(\min\{r_1+r_2;m\},m)$, в [7], что квадрат подкода размерности $k-1$ кода Рида – Маллера $\mathrm{RM}(r,m)$ для $r\leqslant\lfloor m/2\rfloor$ часто совпадает с $\mathrm{RM}(2r,m)$. Найдем условия, когда степень $s\in\mathbb{N}$ любого собственного подкода $C$ кода $\mathrm{RM}(1,m)$ не совпадает ни с одним кодом $\mathrm{RM}(r,m)$, $r\in[m]$. Так как $\dim(\mathrm{RM}(1,m))=m+1$, достаточно рассмотреть случай, когда $\dim(C)=m$. Обозначим $r(A)$ ранг матрицы $A$.

**Лемма 1.** *Пусть* $f_i=f_i(X_1,...,X_n)=a_0^i+a_1^iX_1+...+a_m^iX_m\in\mathbb{F}_2[X_1,...,X_m]$ – *ненулевой полином степени не выше* 1, $i=1,...,n$. *Равенство* $\deg(f_1\cdot...\cdot f_n)=n$ *выполняется, тогда и только тогда, когда* $r(M_n)=n$, *где*

$$M_n=(a_j^l),\ l=1,\dots,n,j=1,\dots,m. \tag{5}$$

*Доказательство.* Докажем по индукции, что из равенства $\deg(f_1\cdot...\cdot f_n)=n$ вытекает равенство $r(M_n)=n$. Пусть $n=2$ и $\deg(f_1\cdot f_2)=2$. Из (4) получаем, что $f_1\neq f_2+1$. Предположим, что строки $(a_1^1,...,a_m^1)$ и $(a_1^2,...,a_m^2)$ линейно зависимые. В поле $\mathbb{F}_2$ это означает, что эти строки совпадают. А из $f_1\neq f_2+1$ тогда получаем, что $f_1=f_2$. Но из (4) вытекает, что $f_1\cdot f_2=f_1=f_2$ и $\deg(f_1\cdot f_2)\leqslant 1$, что противоречит условию. Поэтому ранг матрицы $M_2$ равен двум. Пусть теперь утверждение верно для $n>2$. Докажем, что утверждение справедливо для случая $n+1$. Предположим, что матрица

$$M_{n+1}=\begin{pmatrix}M_n\\a_1^{n+1},...,a_m^{n+1}\end{pmatrix}$$

имеет ранг $n$, но при этом $\deg(f_1\cdot...\cdot f_{n+1})=n+1$. Без потери общности можно полагать, что матрица $M_n$ имеет ранг $n$. Тогда существуют такие $h_1,...,h_n\in\mathbb{F}_2$, что коэффициенты $a_1^{n+1},...,a_m^{n+1}$ полинома $f_{n+1}=f_{n+1}(X_1,...,X_m)=a_0^{n+1}+a_1^{n+1}X_1+...+a_m^{n+1}X_m$ представимы в виде: $a_i^{n+1}=\sum_{j=1}^n h_ja_i^j, i=1,...,m$. В этом случае, либо $f_{n+1}=h_1f_1+...+h_nf_n$, либо $f_{n+1}=h_1f_1+...+h_nf_n+1$. Из (4) для $b\in\mathbb{F}_2$ получаем

$$f_1\cdot...\cdot f_{n+1}=h_1(f_1\cdot...\cdot f_n)+...+h_n(f_1\cdot...\cdot f_n)+b(f_1\cdot...\cdot f_n).$$

Но тогда $\deg(f_1\cdot...\cdot f_{n+1})\leqslant n$, что противоречит условию.

Докажем, что $\deg(f_1\cdot...\cdot f_n)=n$, если ранг матрицы (5) равен $n$. Так как $r(M_n)=n$, то найдутся такие $n$ переменных $X_{i_1},...,X_{i_n}$, $\tau=\{i_1,...,i_n\}$, что $M_n^\tau=(a_{i_j}^l)$, где

$l = 1, \ldots, n, j = 1, \ldots, n$, полного ранга. Пусть $A$ – коэффициент при мономе $X_{i_1} \cdot \ldots \cdot X_{i_n}$ в произведении $n$ полиномов $f_1$,....,$f_n$. Несложно заметить, что $A = \sum_{\sigma \in \mathcal{S}_n} a_{1,i_{\sigma(1)}} \cdot \ldots \cdot a_{n,i_{\sigma(n)}}$. Так как $(-1)^s = 1$ для любого натурального $s$ в $\mathbb{F}_2$, то определитель $(n \times n)$-матрицы $M_n^\tau$ по определению равен

$$\mathtt{det}(M_n^\tau) = \sum_{\sigma \in \mathcal{S}_n} (-1)^{N(\sigma)} \cdot a_{1,i_{\sigma(1)}} \cdot \ldots \cdot a_{n,i_{\sigma(n)}} = \sum_{\sigma \in \mathcal{S}_n} a_{1,i_{\sigma(1)}} \cdot \ldots \cdot a_{n,i_{\sigma(n)}},$$

где $N(\sigma)$ – четность подстановки $\sigma$. Таким образом, $\mathtt{det}(M_n^\tau) = A$. Так как $r(M_n^\tau) = n$, то $A = 1$, откуда получаем, что $\deg(f_1 \cdot \ldots \cdot f_n) = n$. □

**Лемма 2.** *Пусть $C \subset \mathrm{RM}(1, m)$. Тогда $C^n \neq \mathrm{RM}(n, m)$ для любого $1 \leqslant n \leqslant m$.*

*Доказательство.* Без потери общности, рассмотрим случай $\dim(C) = m$. Пусть $G = (\mathbf{g}_i)_{i=1,\ldots,m}$ – порождающая матрица $C$. Оценим $\dim(C^n)$. Заметим, что $C^n = \mathcal{L}(G^n)$. Строки $G^n$ имеют вид $\mathbf{g}_{i_1} \star \cdots \star \mathbf{g}_{i_n}$, где $i_1, \ldots, i_n \in \{1, \ldots, n\}$. Так как разных (по набору множителей) произведений всего $\chi = \sum_{j=1}^{n} C_m^l$, то $\dim(C^n) \leqslant \chi$. С другой стороны, $\dim(\mathrm{RM}(n, m)) = 1 + \chi$, поэтому $C^n \neq \mathrm{RM}(n, m)$. □

**Теорема 1.** *Пусть $C \subset \mathrm{RM}(1, m)$, $\dim(C) = m$. Если в $M(C)$ найдутся такие полиномы $f_1, \ldots, f_m$, что ранг матрицы $M_n$ вида (5) при $n = m$ равен $m$, то $C^s \neq \mathrm{RM}(v, m)$ для любых $1 \leqslant v \leqslant s \leqslant m$.*

*Доказательство.* Пусть $G$ – произвольная порождающая матрица кода $C$. Так как каждому вектору из $C$ соответствует полином из $\mathbb{F}_2[X_1, \ldots, X_m]$ степени не выше одного, то из $C^n = \mathcal{L}(G^n)$ получаем, что для любого натурального $s$ код $C^s$ не содержит векторов, соответствующих полиному из $\mathbb{F}_2[X_1, \ldots, X_m]$ степени выше $s$. Отсюда $C^s \neq \mathrm{RM}(r, m)$ для $r > s$. Из условия теоремы и леммы 1 получаем, что в коде $C^s$ найдется вектор, соответствующий полиному степени $s$. Отсюда $C^s \neq \mathrm{RM}(r, m)$ для $r < s$. А из леммы 2 вытекает, что $C^s \neq \mathrm{RM}(s, m)$. □

## 2. Система BBCRS и известные результаты ее криптоанализа

### 2.1. Криптосистема BBCRS

В [12] с целью противодействия известным структурным атакам построена модификация системы Мак-Элиса, в которой в публичном ключе вместо подстановочной матрицы $P$ используется невырожденная матрица. Опишем эту криптосистему. Пусть $C_{sec}$ – $[n, k, d]_q$-код с полиномиальным алгоритмом декодирования $\mathrm{Dec}_{C_{sec}} : \mathbb{F}_q^n \to \mathbb{F}_q^k$. Секретным ключом системы является набор $(G_{sec}, S, Q)$, где $G_{sec}$ – порождающая $(k \times n)$-матрица $C_{sec}$, $S$ – невырожденная $(k \times k)$-матрица над полем $\mathbb{F}_q$, $Q = \Pi + R$ – невырожденная $(n \times n)$-матрица, где $\Pi$ – подстановочная $(n \times n)$-матрица, $R$ – случайная $(n \times n)$-матрица ранга 1 над полем $\mathbb{F}_q$. Публичный ключ — $(k \times n)$-матрица

$$G_{pub} = S^{-1} G_{sec} Q^{-1}. \tag{6}$$

Шифрование сообщения $\mathbf{m} (\in \mathbb{F}_q^k)$ выполняется по правилу

$$\mathbf{c} = \mathbf{m} G_{pub} + \mathbf{e}, \ \mathrm{wt}(e) \leqslant t := \lfloor (d-1)/2 \rfloor. \tag{7}$$

При расшифровании $\mathbf{c}$ сначала умножается на секретную матрицу $Q$: $\mathbf{c}Q = \mathbf{m}S^{-1}G_{sec} + \mathbf{e}\Pi + \mathbf{e}R$. Так как $r(R) = 1$, то $R$ можно представить в виде $R = \boldsymbol{\beta}^T \cdot \boldsymbol{\alpha}$, где $\boldsymbol{\beta}, \boldsymbol{\alpha} \in \mathbb{F}_q^n$. Поэтому вектор $\mathbf{e}R$ имеет $q$ возможных значений $a_i\boldsymbol{\alpha}$, которые можно перебрать за полиномиальное по $q$ число операций, $a_1$,...,$a_q$ – попарно различные элементы $\mathbb{F}_q$. Расшифрование $\mathbf{c}$ заключается в переборе возможных значений $a_i\boldsymbol{\alpha}$ неизвестного $\mathbf{e}R$ и проверке неравенства

$$\mathrm{wt}(\mathbf{c} - \mathbf{m}_i G_{pub}) \leqslant t, \ \mathbf{m}_i = \mathrm{Dec}_{C_{sec}}(\mathbf{c}Q - a_i\boldsymbol{\alpha})S. \tag{8}$$

Вектор $\mathbf{c}Q - a_i\boldsymbol{\alpha} = \mathbf{m}S^{-1}G_{sec} + \mathbf{e}\Pi$ является зашумленным кодовым слово кода $C_{sec}$ при $a_i\boldsymbol{\alpha} = \mathbf{e}R$, при этом вес ошибки $\mathbf{e}\Pi$ не больше $t$. Тогда $\mathbf{m}_i = \mathbf{m}$ и (8) будет выполнено. Однако возможно ошибочное расшифрование, когда (8) выполняется для разных $\mathbf{m}_i$ и $\mathbf{m}_j$. Описанную криптосистему обозначим $\mathrm{BBCRS}(C_{sec})$.

## 2.2. Известные результаты криптоанализа

### 2.2.1. Представление матрицы $G_{pub}$

Единичную матрицу порядка $k$ обозначим $I_k$.

**Лемма 3.** *Публичный ключ системы $BBCRS(C_{sec})$ представим в виде*

$$G_{pub} = G(I_n - A), \ \mathcal{L}(G) \sim C_{sec}, \ r(A) = 1. \tag{9}$$

*Доказательство.* Представим $Q^{-1}$ из (6) в виде $Q^{-1} = \Pi^{-1} + \tilde{R}$, где $\tilde{R}$ – неизвестная матрица. Тогда из равенства $Q^{-1}Q = I_n + \Pi^{-1}R + \tilde{R}\Pi + \tilde{R}R = I_n$ получаем $\tilde{R}(\Pi + R) = -\Pi^{-1}R$, откуда $\tilde{R} = -\Pi^{-1}R(\Pi + R)^{-1} = -\Pi^{-1}RQ^{-1}$. Из (6) вытекает $G_{pub} = S^{-1}G_{sec}\Pi^{-1}(I_n - RQ^{-1})$. Очевидно, что $\mathcal{L}(S^{-1}G_{sec}\Pi^{-1}) \sim C_{sec}$. Так как $r(R) = 1$ и $r(Q^{-1}) = n$, то $r(RQ^{-1}) = 1$. Полагая $G = S^{-1}G_{sec}\Pi^{-1}$ и $A = RQ^{-1}$, получим доказываемое утверждение. □

Из $Q^{-1} = \Pi^{-1}(I_n - RQ^{-1})$ и $r(Q^{-1}) = r(\Pi^{-1}) = n$ вытекает, что $r(I_n - RQ^{-1}) = n$. Пусть

$$C_{pub} = \mathcal{L}(G_{pub}), \ C = \mathcal{L}(S^{-1}G_{sec}\Pi^{-1}) = \mathcal{L}(G_{sec}\Pi^{-1}) = \pi^{-1}(C_{sec}), \tag{10}$$

где подстановка $\pi^{-1}$ соответствует $\Pi^{-1} = P_{\pi^{-1}}$. Представим $A$ из (9) в виде

$$A = \mathbf{b}^T \cdot \mathbf{a}, \ \mathbf{b}, \mathbf{a} \in \mathbb{F}_q^n. \tag{11}$$

Пара $(\mathbf{a}_0, \mathbf{b}_0)$ называется *подходящей*, если для $A_0 = \mathbf{b}_0^T \cdot \mathbf{a}_0$ найдется такая порождающая матрица $G'$ кода $C$, что

$$G_{pub} = G'(I_n - A_0). \tag{12}$$

### 2.2.2. Представление векторов кода $C_{pub}$

**Лемма 4.** *Для любого вектора $\mathbf{c}$ из $C_{pub}$ найдется единственный вектор $\mathbf{p}$ из $C$, такой, что $\mathbf{c} = \mathbf{p} - (\mathbf{p}, \mathbf{b})\mathbf{a}$, где $(\mathbf{p}, \mathbf{b})$ – скалярное произведение векторов $\mathbf{p}$ и $\mathbf{b}$.*

*Доказательство.* Для любого $\mathbf{c}$ из $C_{pub}$ найдется единственный $\mathbf{m}$ из $\mathbb{F}_q^k$, такой, что, учитывая (9) и (11), имеет место представление $\mathbf{c} = \mathbf{m}G_{pub} = \mathbf{p} - (\mathbf{p}, \mathbf{b})\mathbf{a}$. Единственность $\mathbf{p} = \mathbf{m}G$ вытекает из единственности $\mathbf{m}$ и того, что $r(G) = k$. □

Если $(\mathbf{a}_0, \mathbf{b}_0)$ – подходящая пара, то для каждого кодового вектора $\mathbf{c}(\in C_{pub})$ найдется такой уникальный вектор $\mathbf{p}$, что $\mathbf{c} = \mathbf{p} - (\mathbf{p}, \mathbf{b}_0)\mathbf{a}_0$.

### 2.2.3. Схема атаки из [14]

В [14] на $\mathrm{BBCRS}(C_{sec})$ построена атака в случае, когда $C_{sec}$ – обобщенный код Рида – Соломона и $r(R) = 1$. Атака состоит из трех этапов: на первом этапе находится код

$$C_{\mathbf{b}} = C_{pub} \cap C = \{\mathbf{p} - (\mathbf{p}, \mathbf{b})\mathbf{a} : (\mathbf{p}, \mathbf{b}) = 0, \mathbf{p} \in C\}; \tag{13}$$

на втором этапе к коду $C^2_{\mathbf{b}}$ применяется криптоаналитический алгоритм Сидельникова – Шестакова [5] и находится код $C$; на третьем этапе находится подходящая пара $(\mathbf{a}_0, \mathbf{b}_0)$. Успех нахождение кода (13) и кода $C$ во многом, как представляется, зависит от используемого кода $C_{sec}$. В частности, технику, примененную в [14], не удалось адаптировать авторами настоящей статьи для случая $C_{sec} = \mathrm{RM}(r, m)$. В то же время найдены другие способы нахождения $C_{\mathbf{b}}$ и $C$ в этом случае. Описанию этих способов посвящены подразделы 3.1и 3.2. Нахождение же подходящей пары $(\mathbf{a}_0, \mathbf{b}_0)$, во многом совпадает с алгоритмом из [14]. Этот алгоритм с некоторыми упрощениями и полным обоснованием приведен в разделе 3.3.

### 2.2.4. Некоторые соотношения кодов $C_{pub}$ и $C$

Далее приводятся соотношения для $C_{pub}$ и $C$, используемые при нахождении $C_{\mathbf{b}}$ и $(\mathbf{a}_0, \mathbf{b}_0)$. В [14] многие свойства не доказываются. Здесь приводятся их доказательства.

**Лемма 5.** *Пусть $C$, $C_{pub}$ и $C_{\mathbf{b}}$ – коды, определенные в соответствии с* (10) *и* (13), *$\mathbf{b} \notin C^\perp$, $\mathbf{a} \notin C$. Тогда*

*1)* $C_{\mathbf{b}} = \{\mathbf{p} \in C : (\mathbf{p}, \mathbf{b}) = 0\}$;
*2)* $\dim(C_{pub} \cap C) = k - 1$;
*3)* $C^\perp \cap C^\perp_{pub} = \{\mathbf{x} \in C^\perp : (\mathbf{x}, \mathbf{a}) = 0\}$;
*4)* $\dim(C^\perp \cap C^\perp_{pub}) = n - k - 1$;
*5)* $(C \cap C_{pub})^\perp = C^\perp + C^\perp_{pub}$;
*6)* $(C^\perp \cap C^\perp_{pub})^\perp = C + C_{pub}$.

*Доказательство.* Утверждение 1) вытекает непосредственно из определения (13). Докажем 2). Из равенства $(\mathbf{p}, \mathbf{b}) = 0$ в определении (13) вытекает, что

$$C_{pub} \cap C = C \cap \mathcal{L}(\mathbf{b})^\perp. \tag{14}$$

Учитывая условие $\mathbf{b} \notin C^\perp$, имеем: $C \cap \mathcal{L}(\mathbf{b})^\perp \neq C$. Так как $\dim(\mathcal{L}(\mathbf{b})^\perp) = n - 1$, то $\mathcal{L}(\mathbf{b})^\perp + C = \mathbb{F}_q^n$. Поэтому из (14) следует $\dim(C_{pub} \cap C) = \dim(C) + \dim(\mathcal{L}(\mathbf{b})^\perp) - \dim(C + \mathcal{L}(\mathbf{b})^\perp) = k - 1$. Докажем 3). В $C^\perp \cap C^\perp_{pub}$ лежат векторы из $C^\perp$, ортогональные векторам из $C_{pub}$:

$$\begin{aligned} C^\perp \cap C^\perp_{pub} &= \{\mathbf{x} \in C^\perp : (\mathbf{x}, \mathbf{p}) - (\mathbf{x}, (\mathbf{p}, \mathbf{b})\mathbf{a}) = 0, \forall \mathbf{p} \in C\} \\ &= \{\mathbf{x} \in C^\perp : (\mathbf{x}, (\mathbf{p}, \mathbf{b})\mathbf{a}) = 0, \forall \mathbf{p} \in C\} \\ &= \{\mathbf{x} \in C^\perp : (\mathbf{p}, \mathbf{b})(\mathbf{x}, \mathbf{a}) = 0, \forall \mathbf{p} \in C\}. \end{aligned}$$

Так как $\mathbf{a} \notin C$, то найдется $\mathbf{p}'(\in C)$, что $(\mathbf{p}', \mathbf{b}) \neq 0$. Тогда $C^\perp \cap C^\perp_{pub} = \{\mathbf{x} \in C^\perp : (\mathbf{x}, \mathbf{a}) = 0\}$. Свойства 4), 5) и 6) вытекают из свойств ортогонального дополнения. □

Если $\mathbf{b} \in C^{\perp}$ или $\mathbf{a} \in C$, то $C_{pub} = C$. В этом случае матрица публичного ключа BBCRS($C_{sec}$) представляет собой матрицу публичного ключа McE($C_{sec}$). Поэтому известные для McE($C_{sec}$) структурные атаки применимы к BBCRS($C_{sec}$). К таким атакам относятся алгоритмы, построенные, в [3–5]. Далее предполагается, что

$$\mathbf{b} \notin C^{\perp},\ \mathbf{a} \notin C. \tag{15}$$

## 3. Криптоанализ в случае $C_{sec} = \mathrm{RM}(r, m)$

### 3.1. Нахождение подкода $C_{\mathbf{b}}$

Пусть $C_{sec}$ – бинарный $[n, k, d]_2$-код Рида – Маллера $\mathrm{RM}(r, m)$, $n = 2^m$, $k = \sum_{i=0}^{r} \binom{m}{i}$, $d = 2^{m-r}$. Рассмотрим фактор-множество $C_{pub}/(C_{pub} \cap C) = C_{pub}/C_{\mathbf{b}}$. Так как $\dim(C_{pub}) = k$, $\dim(C_{pub} \cap C) = k - 1$, то

$$C_{pub}/C_{\mathbf{b}} = \{C_1 = C_{\mathbf{b}}, C_2\}, C_i = \mathbf{h} + C_{\mathbf{b}} = \{\mathbf{h} + \mathbf{c} : \mathbf{c} \in C_{\mathbf{b}}\}, i = 1, 2.$$

#### 3.1.1. Случай нечетного $\mathrm{wt}(\mathbf{a})$

**Лемма 6.** *Пусть $C_{sec} = \mathrm{RM}(r, m)$, для векторов $\mathbf{a}$ и $\mathbf{b}$ в (11) выполняется (15) и $\mathrm{wt}(\mathbf{a})$ – нечетное. Тогда все векторы из $C_2$ имеют нечетный вес.*

*Доказательство.* Из леммы 4 и (15) получаем, что в $C_{pub}$ найдется вектор вида $\mathbf{p}+\mathbf{a}$. Так как $\mathrm{wt}(\mathbf{p}+\mathbf{a}) = \mathrm{wt}(\mathbf{p}) + \mathrm{wt}(\mathbf{a}) - 2|\mathrm{supp}(\mathbf{p}) \cap \mathrm{supp}(\mathbf{a})|$ в $\mathbb{F}_2$, то $\mathrm{wt}(\mathbf{p}+\mathbf{a})$ – нечетное. Так как для $r = 0, ..., m-1$ ненулевые векторы из $\mathrm{RM}(r, m)$ имеют четный вес, то ненулевые векторы из $C_{\mathbf{b}}$ также имеют четный вес. Следовательно в $C_2$ найдется хотя бы один вектор $\mathbf{a}_0$ нечетного веса. Из представления $C_2 = \mathbf{a} + C_{\mathbf{b}}$ получаем, что векторы из $C_2$ имеют нечетный вес. □

**Замечание 1.** При выполнении условий леммы 6, для нахождения $C_{\mathbf{b}}$ достаточно в $C_{pub}$ найти $k-1$ линейно независимых векторов четного веса.

#### 3.1.2. Случай четного $\mathrm{wt}(\mathbf{a})$, $r \leqslant m - r - 1$

При четном $\mathrm{wt}(\mathbf{a})$ в ряде случаев можно найти подкод кода $C_{\mathbf{b}}$ размерности $k-2$, вычислив $C_{pub} \cap C_{pub}^{\perp}$. Чтобы показать это, рассмотрим следующую задачу.

**Задача 1.** *Пусть $\mathbf{y} \notin \mathrm{RM}(r, m)$, $\mathrm{wt}(\mathbf{y})$ – четное, $K \subset \mathcal{L}(\mathbf{y}+\mathrm{RM}(r, m))$ – подпространство размерности $\dim(\mathrm{RM}(r, m))$, $K \neq \mathrm{RM}(r, m)$. Найти размерность $K \cap K^{\perp}$.*

Из $r \leqslant m - r - 1$ и (3) вытекает, что $\mathrm{RM}(r, m) \subseteq \mathrm{RM}(r, m)^{\perp} = \mathrm{RM}(m - r - 1, m)$.

**Теорема 2.** *Пусть $\mathbf{y} \in \mathbb{F}_2^{2^m}$, $\mathbf{y} \notin \mathrm{RM}(r, m)$, $\mathrm{wt}(\mathbf{y})$ – четное, $r \leqslant m - r - 1$, $K \subset \mathcal{L}(\mathbf{y} + \mathrm{RM}(r, m))$, $\dim(K) = \dim(\mathrm{RM}(r, m))$, $K \neq \mathrm{RM}(r, m)$. Тогда*

$$K \cap K^{\perp} = \begin{cases} K, \mathbf{y} \in U^{\perp}, U = \mathrm{RM}(r, m) \cap K, \\ W \subset \mathrm{RM}(r, m) \cap K, \mathbf{y} \notin U^{\perp},\ \dim(W) = \dim(\mathrm{RM}(r, m)) - 2. \end{cases} \tag{16}$$

*Доказательство.* Найдем размерность $U = \mathrm{RM}(r,m) \cap K$:

$$\begin{aligned}\dim(U) = \dim(\mathrm{RM}(r,m) \cap K) &= \dim(\mathrm{RM}(r,m)) + \dim(K) - \dim(\mathrm{RM}(r,m) + K) \\ &= 2\dim(\mathrm{RM}(r,m)) - \dim(\mathcal{L}(\mathbf{y}) + \mathrm{RM}(r,m)) = \\ &= \dim(\mathrm{RM}(r,m)) - 1.\end{aligned}$$

Теперь представим $K$ в виде: $K = U \cup \{\mathbf{y} + U\}$. Тогда $K^\perp = U^\perp \cap \{\mathbf{y} + U\}^\perp$. Так как $\{\mathbf{y} + U\}^\perp = U^\perp \cap \mathcal{L}(\mathbf{y})^\perp$, то $K^\perp = U^\perp \cap \mathcal{L}(\mathbf{y})^\perp$. Поэтому

$$\begin{aligned}K \cap K^\perp &= (U \cup \{\mathbf{y} + U\}) \cap (U^\perp \cap \mathcal{L}(\mathbf{y})^\perp) \\ &= \left(U \cap (U^\perp \cap \mathcal{L}(\mathbf{y})^\perp)\right) \cup \left(\{\mathbf{y} + U\} \cap (U^\perp \cap \mathcal{L}(\mathbf{y})^\perp)\right).\end{aligned}$$

Так как $U \subset \mathrm{RM}(r,m)$ и $r \leqslant m - r - 1$, то $\mathrm{RM}(m - r - 1, m) \subset U^\perp$ и $U \subset U^\perp$. Рассмотрим два случая: $\mathbf{y} \in U^\perp$ и $\mathbf{y} \notin U^\perp$. Пусть $\mathbf{y} \in U^\perp$. Его вес четный, поэтому $(U \cup \{\mathbf{y} + U\}) \subset U^\perp$, $U \subset \mathcal{L}(\mathbf{y})^\perp$ и $\mathbf{y} \in \mathcal{L}(\mathbf{y})^\perp$. Следовательно $\{\mathbf{y} + U\} \subset \mathcal{L}(\mathbf{y})^\perp$ и $K \cap K^\perp = (U \cup \{\mathbf{y} + U\}) = K$.

Пусть теперь $\mathbf{y} \notin U^\perp$, откуда $U \not\subset \mathcal{L}(\mathbf{y})^\perp$ и $\dim(U + \mathcal{L}(\mathbf{y})^\perp) = 2^m$. Тогда

$$\begin{aligned}\dim\left(U \cap (U^\perp \cap \mathcal{L}(\mathbf{y})^\perp)\right) &= \dim\left(U \cap \mathcal{L}(\mathbf{y})^\perp\right) \\ &= \dim(U) + \dim(\mathcal{L}(\mathbf{y})^\perp) - \dim(U + \mathcal{L}(\mathbf{y})^\perp) = \dim(U) - 1.\end{aligned}$$

Покажем, что $\{\mathbf{y} + U\} \cap (U^\perp \cap \mathcal{L}(\mathbf{y})^\perp) = \varnothing$. Действительно, $\{\mathbf{y} + U\} \cap U^\perp = \{\mathbf{y} + \mathbf{c}, \mathbf{c} \in U \subseteq U^\perp : \mathbf{y} + \mathbf{c} \in U^\perp\}$. Отсюда $\mathbf{y} \in U^\perp$, что противоречит условию. Поэтому $K \cap K^\perp \subset U$ для $\mathbf{y} \notin U^\perp$, причем $\dim(K \cap K^\perp) = \dim(U) - 1$. □

Рассмотренная выше задача эквивалентна поиску условий на вектор $\mathbf{a}$, при которых $C_{pub} \cap C_{pub}^\perp \subset C_{\mathbf{b}}$, причем $U$ соответствует $C_{\mathbf{b}}$. Пусть $\mathbf{a}$ четного веса выбирается случайно и равновероятно из $\mathbb{F}_2^{2^m} \setminus C$ (где $C$ определен в (10)), при этом выполняется (15). Обозначим $p_{\mathbf{a} \in C_{\mathbf{b}}^\perp}$ вероятность того, что $\mathbf{a} \in C_{\mathbf{b}}^\perp$. Учитывая, что $C_{\mathbf{b}} \subset C \subseteq C^\perp \subset C_{\mathbf{b}}^\perp$, получим

$$p_{\mathbf{a} \in C_{\mathbf{b}}^\perp} = \frac{2^{\dim(C_{\mathbf{b}}^\perp)} - 2^{\dim(C)}}{2^{2^m} - 2^{\dim(C)}} = \frac{2^{2^m - \dim(C) + 1} - 2^{\dim(C)}}{2^{2^m} - 2^{\dim(C)}} \leqslant \frac{1}{2^{\dim(\mathrm{RM}(r,m)) - 1}}.$$

Таким образом, с вероятностью не менее $1 - p_{\mathbf{a} \in C_{\mathbf{b}}^\perp}$ код $C_{pub} \cap C_{pub}^\perp$ является подкодом кода $C_{\mathbf{b}}$ размерности $k - 2$. Чтобы найти $C_{\mathbf{b}}$ по $C_{pub} \cap C_{pub}^\perp$ следует, например, случайно выбирать векторы из $C_{pub}$. С одинаковой вероятностью $1/2$ выбираемый вектор принадлежит $C_{\mathbf{b}}$ или $C_{pub} \cap C_{pub}^\perp$. Тогда с вероятностью $1/4$ выбранный вектор принадлежит $C_{\mathbf{b}} \setminus (C_{pub} \cap C_{pub}^\perp)$. Таким образом, потребуется в среднем четыре попытки для нахождения базиса $C_{\mathbf{b}}$.

### 3.1.3. Случай четного $\mathrm{wt}(\mathbf{a})$, $r > m - r - 1$

В этом разделе рассматривается способ нахождения кода

$$\tilde{C}_{\mathbf{b}} = C^\perp \cap C_{pub}^\perp, \tag{17}$$

в общем случае, отличного от $C_{\mathbf{b}}$. Однако, как показано в далее в лемме 8, этот код также может использоваться для нахождения секретного кода $C$.

В рамках условий задачи 1 рассмотрим случай $r > m-r-1$. В частности, имеем: $\mathrm{RM}(r,m) \supset \mathrm{RM}(r,m)^{\perp} = \mathrm{RM}(m-r-1,m)$. Из $\mathbf{y} \notin \mathrm{RM}(r,m)$ получаем: $\mathcal{L}(\mathbf{y})^{\perp} \not\supset \mathrm{RM}(m-r-1,m)$. Обозначим $V = \mathcal{L}(\mathbf{y})^{\perp} \cap \mathrm{RM}(m-r-1,m)$, $\dim(V) = n-k-1$. Заметим, что $\mathrm{RM}(m-r-1,m) \subset U^{\perp}$ для $U$ из (16). Для $K^{\perp} = U^{\perp} \cap \mathcal{L}(\mathbf{y})^{\perp}$ получаем: $V \subset K^{\perp}$. Так как $\dim(K^{\perp}) = n-k$, то $K^{\perp}$ представим в виде объединения смежных классов: $V$ и $V+\mathbf{x}$, где $\mathbf{x} \in K^{\perp} \setminus \mathrm{RM}(m-r-1,m)$, $m-r-1 < r$, и $\mathrm{wt}(\mathbf{x})$ – четное число. Таким образом, используя теорему 2, можно описать пересечение $K^{\perp} \cap K$:

$$K^{\perp} \cap K = \begin{cases} K^{\perp}, \mathbf{x} \in V^{\perp} \\ \tilde{W} \subset \mathrm{RM}(m-r-1,m) \cap K^{\perp}, \mathbf{x} \notin V^{\perp}, \end{cases}$$

где $\dim(\tilde{W}) = \dim(\mathrm{RM}(m-r-1,m)) - 2$. Получим, что с вероятностью $1/4$ случайно выбранный вектор из $K^{\perp}$ принадлежит $V \setminus (K^{\perp} \cap K)$. Поэтому в среднем один из четырех случайно выбранных векторов позволяет построить $\tilde{C}_{\mathbf{b}}$.

### 3.2. Нахождение кода $C$

В [7] показано, что квадрат подкода коразмерности один кода $\mathrm{RM}(r,m)$ с большой вероятностью равен $\mathrm{RM}(2r,m)$. Леммы 7 и 8 позволяют перейти от $C_{\mathbf{b}}^2$ и $\tilde{C}_{\mathbf{b}}^2$ к $C$.

#### 3.2.1. Случай $r > 1$

**Лемма 7.** *Пусть $2 \leqslant 2r \leqslant m-2$, а $C_{pub}$, $C$ и $C_{\mathbf{b}}$ определенны в (10) и (13), причем*

$$\sigma(C_{\mathbf{b}}^2) = \mathrm{RM}(2r,m), \sigma \in \mathcal{S}_{2^m}. \tag{18}$$

*Тогда $\pi^{-1} \circ \sigma \in \mathrm{PAut}(\mathrm{RM}(r,m))$.*

*Доказательство.* Из определения (10) кода $C$ вытекает, что в $C_{sec} = \mathrm{RM}(r,m)$ найдется такой подкод $D_0$ размерности $\dim(\mathrm{RM}(r,m)) - 1$, что $C_{\mathbf{b}} = \pi^{-1}(D_0)$. Из (18) и $D_0^2 \subseteq \mathrm{RM}(2r,m)$ вытекает, что $D_0^2 = \mathrm{RM}(2r,m)$. Так как $\sigma(C_{\mathbf{b}}^2) = \mathrm{RM}(2r,m)$, то

$$\begin{aligned} \mathrm{RM}(2r,m) &= \sigma(C_{\mathbf{b}}^2) = \sigma((\pi^{-1}(D_0))^2) = \sigma(\pi^{-1}(D_0^2)) \\ &= \sigma(\pi^{-1}(\mathrm{RM}(r,m)^2)) = \sigma(\pi^{-1}(\mathrm{RM}(2r,m))). \end{aligned}$$

Отсюда $\pi^{-1} \circ \sigma \in \mathrm{PAut}(\mathrm{RM}(2r,m))$. Так как $\mathrm{PAut}(\mathrm{RM}(1,m)) = ... = \mathrm{PAut}(\mathrm{RM}(m-2,m))$, то $\pi^{-1} \circ \sigma \in \mathrm{PAut}(\mathrm{RM}(r,m))$. □

**Лемма 8.** *Пусть $2 \leqslant 2(m-r-1) \leqslant m-2$, а $C_{pub}$, $C$ и $\tilde{C}_{\mathbf{b}}$ из (10) и (17), причем*

$$\sigma(\tilde{C}_{\mathbf{b}}^2) = \mathrm{RM}(2(m-r-1),m), \sigma \in \mathcal{S}_{2^m}. \tag{19}$$

*Тогда $\pi^{-1} \circ \sigma \in \mathrm{PAut}(\mathrm{RM}(r,m))$.*

*Доказательство.* Из (10) вытекает, что $C^{\perp} = \pi^{-1}(\mathrm{RM}(m-r-1,m))$ и в $C_{sec}^{\perp} = \mathrm{RM}(m-r-1,m)$ найдется такой подкод $D_0$ размерности $\dim(\mathrm{RM}(m-r-1,m)) - 1$, что $\tilde{C}_{\mathbf{b}} = \pi^{-1}(D_0)$. Из (19) и $D_0^2 \subseteq \mathrm{RM}(2r,m)$ вытекает, что $D_0^2 = \mathrm{RM}(2r,m)$. Повторяя выкладки из леммы 7, получим $\pi^{-1} \circ \sigma \in \mathrm{PAut}(\mathrm{RM}(r,m))$. □

Из $\sigma(\pi^{-1}(\mathrm{RM}(r,m))) = \mathrm{RM}(r,m)$, для $\sigma$ из (18) или (19), и (10) получаем

$$C = \pi^{-1}(C_{sec}) = \pi^{-1}(\mathrm{RM}(r,m)) = \sigma^{-1}(\mathrm{RM}(r,m)). \tag{20}$$

Поэтому с помощью $\sigma$ по произвольной порождающей матрице кода $\mathrm{RM}(r,m)$ может быть найдена порождающая матрица кода $C$ (см. (10)). Заметим, что нахождение такой $\sigma$, что $\sigma(C^2_{\mathbf{b}}) = \mathrm{RM}(2r,m)$, может быть выполнено эффективно (см. [3,4]).

### 3.2.2. Случай $r = 1$

Из теоремы 1 вытекает, что $D^s \neq \mathrm{RM}(v,m)$ для любого $D \subseteq \mathrm{RM}(1,m)$ размерности $m$, такого, что в $M(D)$ найдутся $m$ линейно независимых полиномов $f_1$,...,$f_m$, коэффициенты которых при $X_1,...,X_m$ образуют невырожденную $(m \times m)$-матрицу. Заметим, что любые $m$ линейно независимых векторов из $D$ образуют его порождающую матрицу, причем $G_1 = TG_2$ для любых порождающих матриц $G_1$ и $G_2$ кода $D$, где $r(T) = m$. Поэтому, если для линейно независимых $f_1$,...,$f_m$ матрица (5) при $n = m$ имеет ранг $m-1$, то и для любых $m$ линейно независимых полиномов из $M(D)$ ранг такой матрицы равен $m-1$.

Заметим, что $C_{\mathbf{b}}$ – подкод кода $C$, перестановочно эквивалентного $\mathrm{RM}(1,m)$, причем перестановка, переводящая $\mathrm{RM}(1,m)$ в $C$, неизвестна. Поэтому невозможно найти $M(C_{\mathbf{b}})$ и по рангу матрицы (5) при $n = m$, составленной из полиномов множества $M(C_{\mathbf{b}})$, проверить выполнение условий теоремы 1. Рассмотрим случай, когда по коду $C_{\mathbf{b}}$ можно определить, выполняются ли условия теоремы 1. Напомним, что код $D \subseteq \mathbb{F}_2^n$ называется самодополнительным, если вектор из всех единиц $\mathbf{1}$ содержится в $D$ [15]. Например, двоичные коды Рида – Маллера и коды Хэмминга являются самодополнительными кодами.

**Лемма 9.** *В $M(C_{\mathbf{b}})$ найдутся такие $f_1,...,f_m$, что ранг $M_n$ вида (5) при $n = m$ равен $m$, тогда, и только тогда, когда $C_{\mathbf{b}}$ не является самодополнительным кодом.*

*Доказательство.* Вектору $\mathbf{1} \in \mathbb{F}_2^{2^m}$ соответствует полином $f(X_1,...,X_m) \equiv 1$. Если $C_{\mathbf{b}}$ – самодополнительный код, то для любого полинома $f \in M(C_{\mathbf{b}})$ имеем: $1+f \in M(C_{\mathbf{b}})$.

Сначала докажем, что при $r(M_m) = m$ код $C_{\mathbf{b}}$ не является самодополнительным. Предположим, что это не так. Тогда $M(C_{\mathbf{b}})$ можно представить в виде объединения непересекающихся равномощных классов: $M(C_{\mathbf{b}}) = M_0 \cup M_1$, где $M_0$ содержит все полиномы с нулевым свободным коэффициентом, а $M_1$ – с ненулевым. Заметим, что $M_0$ – группа по сложению, поэтому $M(C_{\mathbf{b}}) = M_0 \cup \{1 + M_0\}$. Так как $M(C_{\mathbf{b}})$ можно рассматривать, как векторное подпространство размерности $m$ в пространстве размерности $m+1$ над полем $\mathbb{F}_2$, то в $M_0$ можно выбрать $m-1$ линейно независимых полиномов $f_1,...,f_{m-1}$. Добавим к этому набору любой $f_m$ из $M_1$ и получим $m$ линейно независимых полиномов. Тогда в $m \times (m+1)$-матрице $M_0 = (a^l_j)$, $l = 1,\ldots,m$, $j = 0,\ldots,m$, составленной из коэффициентов этих полиномов, первый по счету столбец будет иметь везде нулевые значения, кроме нижнего элемента $a^m_0$, а последняя строка матрицы (5) при $n = m$ будет линейно выражаться через первые $m-1$ строк, что противоречит условию $r(M_m) = m$.

Докажем теперь, что если $C_{\mathbf{b}}$ – не самодополнительный код, то $r(M_m) = m$. Предположим, что матрица (5) при $n = m$ имеет ранг $m-1$. Отсюда следует, что первая строка матрицы $M_m$ линейно выражается через остальные $m-1$ строк при

использовании подходящих коэффициентов $h_1, ..., h_{m-1} \in \mathbb{F}_2$. Но так как $r(M_0) = m$, то $\sum_{i=1}^{m-1} h_i a_0^{i+1} \neq a_0^1$. Следовательно, в $M(C_{\mathbf{b}})$ существуют $f$ и $1+f$. Так как $M(C_{\mathbf{b}})$ – группа, то $1 \in M(C_{\mathbf{b}})$ и код $C_{\mathbf{b}}$ – самодополнительный, что противоречит предположению. Поэтому $r(M_m) = m$. □

Из леммы 9 получаем, что в случае, когда $C_{\mathbf{b}}$ не самодополнительный, исследуемый способ атаки неприменим. В силу теоремы 1, степени $C_{\mathbf{b}}$ не позволяют получить код Рида – Маллера и найти $\sigma$, используемую при нахождении $C$ (см. (20)). Выяснить, является ли $C_{\mathbf{b}}$ самодополнительным, можно путем проверки на принадлежность вектора $\mathbf{1}$ этому коду.

### 3.3. Нахождение подходящей пары $(\mathbf{a}_0, \mathbf{b}_0)$

Из (13) получаем, что $\mathbf{b} \in (C_{pub} \cap C)^{\perp}$, а из утверждения 3) леммы 5, что $\mathbf{a} \in (C_{pub}^{\perp} \cap C^{\perp})^{\perp}$. Тогда из (15) и утверждений 5) и 6) леммы 5 следует, что $\mathbf{b} \in (C \cap C_{pub})^{\perp} \setminus C^{\perp}$ и $\mathbf{a} \in (C^{\perp} \cap C_{pub}^{\perp})^{\perp} \setminus C$. Пусть $\mathbf{b}_0$ и $\mathbf{a}_0$ – произвольные векторы из $(C \cap C_{pub})^{\perp} \setminus C^{\perp}$ и $(C^{\perp} \cap C_{pub}^{\perp})^{\perp} \setminus C$ соответственно. Так как $\dim((C_{pub} \cap C)^{\perp}) = n-k+1$, $\dim(C^{\perp}) = n-k$, то $(C_{pub} \cap C)^{\perp}/C^{\perp} = \{\tilde{C}_1 = C^{\perp}, \tilde{C}_2\}$, причем неизвестные $\mathbf{b}$ и $\mathbf{b}_0$ лежат в классе

$$\tilde{C}_2 = \mathbf{b} + C^{\perp} = \mathbf{b}_0 + C^{\perp}. \tag{21}$$

Аналогично, неизвестные $\mathbf{a}$ и $\mathbf{a}_0$ лежат в одном смежном классе фактор-множества $(C^{\perp} \cap C_{pub}^{\perp})^{\perp}/C$. Поэтому существуют такие $\mathbf{p}_0 (\in C^{\perp})$ и $\mathbf{q}_0 (\in C)$, что

$$\mathbf{b}_0 = \mathbf{p}_0 + \mathbf{b}, \ \mathbf{a}_0 = \mathbf{q}_0 + \mathbf{a}. \tag{22}$$

Для всех $\mathbf{p} \in C \cap C_{pub}$ верно равенство $\mathbf{c} = \mathbf{p} - (\mathbf{p}, \mathbf{b}_0)\mathbf{a}_0$, так как $(\mathbf{p}, \mathbf{b}_0) = (\mathbf{p}, \mathbf{p}_0 + \mathbf{b}) = (\mathbf{p}, \mathbf{p}_0) + (\mathbf{p}, \mathbf{b}) = 0$ из (22) и (13). В этом случае $(\mathbf{p}, \mathbf{b}_0) = 0$ не зависит от $\mathbf{a}_0$. Пусть теперь $\mathbf{p} \in C \setminus C_{pub}$. Найдем условия на $\mathbf{a}_0$ и $\mathbf{b}_0$, при которых $\mathbf{p} - (\mathbf{p}, \mathbf{b}_0)\mathbf{a}_0$ ортогонален $C_{pub}^{\perp}$, то есть $(\mathbf{p} - (\mathbf{p}, \mathbf{b}_0)\mathbf{a}_0) \in C_{pub}$. Пусть $\mathbf{r} \in C_{pub}^{\perp}$, тогда $(\mathbf{p} - (\mathbf{p}, \mathbf{b}_0)\mathbf{a}_0, \mathbf{r}) = (\mathbf{p}, \mathbf{r}) - (\mathbf{p}, \mathbf{b}_0)(\mathbf{a}_0, \mathbf{r})$. Так как

$$\mathbf{p} \in C \setminus C_{pub} = C \setminus C_{\mathbf{b}}, \tag{23}$$

то из определения $C_{\mathbf{b}}$ получаем $(\mathbf{p}, \mathbf{b}) \neq 0$, и поэтому $(\mathbf{p}, \mathbf{b}_0) \neq 0$. Так как $(\mathbf{p} - (\mathbf{p}, \mathbf{b}_0)\mathbf{a}_0, \mathbf{r}) = (\mathbf{p}, \mathbf{r}) - (\mathbf{a}_0, \mathbf{r})$ в $\mathbb{F}_2$, то рассмотрим два случая: $\mathbf{r} \in C_{pub}^{\perp} \cap C^{\perp}$ и $\mathbf{r} \in C_{pub}^{\perp} \setminus C^{\perp}$. Пусть $\mathbf{r} \in C_{pub}^{\perp} \cap C^{\perp}$. Тогда, с одной стороны, $(\mathbf{p}, \mathbf{r}) = 0$, а с другой стороны, $(\mathbf{a}_0, \mathbf{r}) = (\mathbf{a}, \mathbf{r}) + (\mathbf{q}_0, \mathbf{r}) = 0$ (п. 3 леммы 5). В этом случае $(\mathbf{p} - (\mathbf{p}, \mathbf{b}_0)\mathbf{a}_0, \mathbf{r}) = 0$ для любых $\mathbf{a}_0$ и $\mathbf{b}_0$ из $(C^{\perp} \cap C_{pub}^{\perp})^{\perp} \setminus C$ и $(C \cap C_{pub})^{\perp} \setminus C^{\perp}$ соответственно. Пусть $\mathbf{r} \in C_{pub}^{\perp} \setminus C^{\perp}$. Из пункта 5) леммы 5 имеем: $C_{pub}^{\perp} \subseteq (C_{pub} \cap C)^{\perp}$, поэтому $\mathbf{r} \in \tilde{C}_2$ (см. (21)), и существует такой $\mathbf{y}_r \in C^{\perp}$, что $\mathbf{r} = \mathbf{y}_r + \mathbf{b} = \mathbf{y}_r + \mathbf{b}_0 - \mathbf{p}_0$. Тогда $(\mathbf{p}, \mathbf{r}) = (\mathbf{p}, \mathbf{y}_r) + (\mathbf{p}, \mathbf{b}) = 1$, так как $(\mathbf{p}, \mathbf{b}) = 1$ из (13) и (23). Таким образом, $(\mathbf{p}, \mathbf{r}) - (\mathbf{a}_0, \mathbf{r}) = 1 - (\mathbf{a}_0, \mathbf{r})$. Поэтому $\mathbf{a}_0$ следует выбрать так, чтобы $(\mathbf{a}_0, \mathbf{r}) = 1$ для всех $\mathbf{r} \in C_{pub}^{\perp} \setminus C^{\perp}$.

**Лемма 10.** *Пусть $C \not\subseteq C_{pub}$, тогда найдется $\mathbf{a}_0 \in (C^{\perp} \cap C_{pub}^{\perp})^{\perp} \setminus C$, что $(\mathbf{a}_0, \mathbf{r}) = 1$ для всех $\mathbf{r} \in C_{pub}^{\perp} \setminus C^{\perp}$.*

*Доказательство.* Заметим, что $\mathbf{r}$ принадлежит классу из $C_{pub}^{\perp}/(C_{pub}^{\perp} \cap C^{\perp})$, отличному от $C_{pub}^{\perp} \cap C^{\perp}$. Следовательно существует $\mathbf{r}_0 \in C_{pub}^{\perp} \setminus C^{\perp}$, что для каждого $\mathbf{r}$ найдется $\mathbf{z}_r \in C_{pub}^{\perp} \cap C^{\perp}$, для которого выполняется $\mathbf{r} = \mathbf{r}_0 + \mathbf{z}_r$. Поэтому $(\mathbf{a}_0, \mathbf{r}) = (\mathbf{a}_0, \mathbf{r}_0) +$

$(\mathbf{a}_0, \mathbf{z}_r) = (\mathbf{a}_0, \mathbf{r}_0)$ и $\mathbf{a}_0$ следует выбрать так, чтобы $(\mathbf{a}_0, \mathbf{r}_0) = 1$ хотя бы для одного $\mathbf{r}_0$ из $C_{pub}^{\perp} \setminus C^{\perp}$. Покажем, что такой $\mathbf{a}_0$ существует. Предположим, что $(\mathbf{a}_0, \mathbf{r}_0) = 0$ для каждого $\mathbf{a}_0 \in (C^{\perp} \cap C_{pub}^{\perp})^{\perp} \setminus C$. Тогда в фактор-множестве $(C^{\perp} \cap C_{pub}^{\perp})^{\perp}/C = \{\hat{C}_1 = C, \hat{C}_2\}$ класс $\hat{C}_2$ ортогонален $C_{pub}^{\perp}$ и все векторы из $C$ ортогональны $C_{pub}^{\perp}$. Откуда $C \subseteq C_{pub}$, что противоречит условию леммы. □

**Теорема 3.** *Пусть* $\mathbf{b}_0 \in (C_{pub} \cap C)^{\perp} \setminus C^{\perp}$, $\mathbf{a}_0 \in (C^{\perp} \cap C_{pub}^{\perp})^{\perp} \setminus C$ *такой, что* $(\mathbf{a}_0, \mathbf{r}) = 1$ *хотя бы для одного вектора* $\mathbf{r} \in C_{pub}^{\perp} \setminus C^{\perp}$. *Тогда* $(\mathbf{a}_0, \mathbf{b}_0)$ – *подходящая пара.*

### 3.4. Использование $(\mathbf{a}_0, \mathbf{b}_0)$ и $C$ при дешифровании

Пусть публичный ключ $G_{pub}$ представим в виде (12), где матрица $A_0 = \mathbf{b}_0^T \mathbf{a}_0$ известна, $(\mathbf{a}_0, \mathbf{b}_0)$ – подходящая пара. Если в (12) матрица $r(I_n - A_0) = n$, то $G' = G_{pub}(I_n - A_0)^{-1}$. Рассмотрим случай, когда не делается предположений о ранге матрицы $I_n - A_0$. Тогда $G'$ неизвестна, однако код $C = \mathcal{L}(G') \sim \mathrm{RM}(r, m)$ известен. Поэтому можно выбрать произвольную порождающую матрицу $\hat{G}$ кода $C$. Известно (см., например, [3], [4]), что по $\hat{G}$ для фиксированной порождающей матрицы $G_{\mathrm{RM}(r,m)}$ кода Рида – Маллера можно найти такую невырожденную $(k \times k)$-матрицу $\hat{S}$, подстановочную $(n \times n)$-матрицу $\hat{P}$, что $\hat{G} = \hat{S} G_{\mathrm{RM}(r,m)} \hat{P}$. Принятый шифртекст $\mathbf{c}$ вида (7) может быть представлен в виде

$$\begin{aligned}\mathbf{c} &= \mathbf{m}G_{pub} + \mathbf{e} = \mathbf{m}G'(I_n - A_0) + \mathbf{e} = \mathbf{m}G' - \mathbf{m}G'A_0 + \mathbf{e} \\ &= \mathbf{m}G' - a \cdot \mathbf{a}_0 + \mathbf{e}, a = (\mathbf{m}G', \mathbf{b}_0) \in \mathbb{F}_2.\end{aligned}$$

Так как матрицы $G'$ и $\hat{G}$ порождают один и тот же код, то существует такой $\hat{\mathbf{m}}$, что $\mathbf{m}G' = \hat{\mathbf{m}}\hat{G}$. Тогда $\mathbf{c} = \mathbf{m}'\hat{S}G_{\mathrm{RM}(r,m)}\hat{P} - a \cdot \mathbf{a}_0 + \mathbf{e}$. Так как $a \in \{0, 1\}$, то по $\mathbf{c}$ можно построить два вектора: $\mathbf{z}_0 = \mathbf{c} + 0 \cdot \mathbf{a}_0, \mathbf{z}_1 = \mathbf{c} + 1 \cdot \mathbf{a}_0$. Учитывая, что $\mathbf{b}_0 \notin C^{\perp}$, получаем $\dim(C \cap \mathcal{L}(\mathbf{b}_0)^{\perp}) = k - 1$. Другими словами, для одной половины векторов из $C$ имеем $a = 0$, а для другой половины – $a = 1$. Поэтому при равновероятности информационных сообщений значения $a = 0$ и $a = 1$ равновероятны. Используя подходящий ключ $(\hat{S}, \hat{P})$ и быстрый декодер для кода Рида – Маллера, по $\mathbf{z}_0$ и $\mathbf{z}_1$ соответственно могут быть найдены два возможных вектора ошибок $\mathbf{e}_1$ и $\mathbf{e}_2$, где

$$\mathbf{e}_i = \mathbf{z}_i - (\mathsf{Dec}(\mathbf{z}_i \hat{P}^{-1})\hat{S}^{-1})\hat{G}.$$

Тот $\mathbf{e}_i$, для которого $\mathrm{wt}(\mathbf{e}_i) \leqslant t$, выбирается в качестве вектора, который использовался как вектор ошибок $\mathbf{e}$ при шифровании по правилу (7). Используя найденный $\mathbf{e}_i$, по вектору $\mathbf{c} - \mathbf{e}_i$ и матрице $G_{pub}$, решая систему уравнений $\mathbf{m}G_{pub} = \mathbf{c} - \mathbf{e}_i$ может быть найден $\mathbf{m}$. Если вес $\mathbf{e}_1$ и $\mathbf{e}_2$ не превышает $t$, то в этом случае не представляется возможным определить, какой из них использовался при шифровании. При возникновении такой ситуации возможным решением является сохранение двух вариантов дешифрования. Стоит отметить, что вероятность такой ситуации равна вероятности того, что вектор $\mathbf{a}_0 + \mathbf{e}$ попадает в шар радиуса $t$ некоторого кодового слова кода $C$, при условии, что $\mathbf{e}$ выбирается случайно среди векторов веса не выше $t$, при этом на $\mathbf{a}_0$ накладываются условия из теоремы 3. В настоящей работе эта вероятность не оценивается, однако заметим, что при шифровании часто для большей маскировки используют векторы ошибок максимального веса $t$. В частности, если $\mathrm{wt}(\mathbf{e}) = t$ в правиле (7), то при криптоанализе эта информация о весе может использоваться для выбора из векторов $\mathbf{e}_0$ и $\mathbf{e}_1$ того, который использовался при шифровании.

## Заключение

В настоящей работе получены результаты, которые могут применяться для определения слабых ключей криптосистемы BBCRS($C_{sec}$) в случае $C_{sec} = \mathrm{RM}(r, m)$. В частности, представляется, что к слабым ключам следует относить те, для которых найдется такое $s \in \mathbb{N}$, что $C_{\mathfrak{b}}^s$ совпадет с каким-нибудь кодом Рида – Маллера $\mathrm{RM}(r, m)$ для $r < m$ (обобщенное условие (19)). Из теоремы 1 вытекает, что в качестве кандидатов на сильные ключи могли бы рассматриваться ключи, построенные на коде $\mathrm{RM}(1, m)$, так как среди подкодов коразмерности 1 этого кода найдутся те, для которых любая их степень не совпадает ни с каким двоичным кодом Рида – Маллера. Однако представляется, что криптосистема на кодах первого порядка является малоперспективной, так как имеет малую скорость передачи данных: длина кода экспоненциально зависит от размерности кода.

## Литература / References


1. McEliece R.J. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *DSN Progress Report*, 1978, pp. 42–44.
2. Sendrier N. Finding the Permutation Between Equivalent Linear Codes: the Support Splitting Algorithm. *IEEE Transactions on Information Theory*, 2000, vol. 46, no. 4, pp. 1193–1203.
3. Minder L., Shokrollahi A. Cryptanalysis of the Sidelnikov Cryptosystem. *Advances in Cryptology*, 2007, vol. 4515, pp. 347–360. DOI: 10.1007/978-3-540-72540-4_20
4. Borodin M.A., Chizhov I.V. Efficiency of Attack on the McEliece Cryptosystem Constructed on the Basis of Reed–Muller Codes. *Discrete Mathematics and Applications*, 2014, vol. 24, no. 5, pp. 273–280. DOI: 10.1515/dma-2014-0024
5. Sidel'nikov V.M., Shestakov S.O. On an Encoding System Constructed on the Basis of Generalized Reed–Solomon Codes. *Discrete Mathematics and Applications*, 1992, vol. 2, no. 4, pp. 439–444. DOI: 10.1515/dma.1994.4.3.191
6. Wieschebrink C. Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes. *Post-Quantum Cryptography*, Darmstadt, 2010, pp. 61–72. DOI: 10.1007/978-3-642-12929-2_5
7. Chizhov I.V., Borodin M.A. Hadamard Products Classification of Subcodes of Reed–Muller Codes Codimension 1. *Discrete Mathematics and Applications*, 2020, vol. 32, no. 1, pp. 115–134.
8. Berger T., Loidreau P. How to Mask the Structure of Codes for a Cryptographic Use. *Designs, Codes and Cryptography*, 2005, vol. 35, no. 1, pp. 63–79.
9. Sidelnikov V.M. Public-Key Cryptosystem Based on Binary Reed–Muller Codes. *Discrete Mathematics and Applications*, 1994, vol. 4, no. 3, pp. 191–208. DOI: 10.1515/dma.1994.4.3.191
10. Egorova E., Kabatiansky G., Krouk E., Tavernier C. A New Code-Based Public-Key Cryptosystem Resistant to Quantum Computer Attacks. *Journal of Physics*, 2019, no. 1163, pp. 1–5. DOI: 10.1088/1742-6596/1163/1/012061
11. Deundyak V.M., Kosolapov Yu.V. On the Strength of Asymmetric Code Cryptosystems Based on the Merging of Generating Matrices of Linear Codes. *Proceedings of the XVI International Symposium Problems of Redundancy in Information and Control Systems*, Moscow, 2019, pp. 143–148.

12. Baldi M., Bianchi M., Chiaraluce F., Rosenthal J., Schipani D. *Enhanced Public Key Security for the McEliece Cryptosystem*. Available at: https://arxiv.org/abs/1108.2462 (accessed 28 July 2021).
13. Randriambololona H. *On Products and Powers of Linear Codes Under Componentwise Multiplication*. Available at: http://arxiv.org/abs/1312.0022 (accessed 28 July 2021).
14. Gauthier V., Otmani A., Tillich J.-P. *A Distinguisher-Based Attack on a Variant of McEliece's Cryptosystem Based on Reed–Solomon Codes*. Available at: https://arxiv.org/abs/1204.6459 (accessed 28 July 2021).
15. Betten A., Braun M., Fripertinger H., Kerber A., Kohnert A., Wassermann A. *Error-Correcting Linear Codes: Classification by Isometry and Applications*, Heidelberg, Springer, 2006.

Юрий Владимирович Косолапов, кандидат технических наук, кафедра «Алгебра и дискретная математика», Южный федеральный университет (г. Ростов-на-Дону, Российская Федерация), itaim@mail.ru.

Анастасия Андреевна Лелюк, студент, кафедра «Алгебра и дискретная математика», Южный федеральный университет (г. Ростов-на-Дону, Российская Федерация), lelyukanastasiya@mail.ru.

*Поступила в редакцию 14 марта 2021 г.*

**MSC 94A60, 68P25** **DOI: 10.14529/mmp210302**

## CRYPTANALYSIS OF THE BBCRS SYSTEM ON REED–MULLER BINARY CODES

***Yu.V. Kosolapov*[1], *A.A. Lelyuk*[1]**
[1]Southern Federal University, Rostov-on-Don, Russian Federation
E-mail: itaim@mail.ru, lelyukanastasiya@mail.ru

The paper considers the BBCRS system which is a modification of the McEliece cryptosystem proposed by M. Baldi and some others. In this modification matrix $G_{pub}$ of the public key is the product of three matrices: a non-singular $(k \times k)$-matrix $S$, a generator matrix $G$ of a secret $[n, k]_q$-code $C_{sec}$, and a non-singular $(n \times n)$-matrix $Q$. The difference between the modified system and the original system is that the permutation matrix used in the McEliece system is replaced by a non-singular matrix $Q$. The matrix $Q$ is obtained as the sum of a permutation matrix $P$ and a matrix $R$ of small rank $r(R)$. Later, V. Gauthier and some others constructed an attack that allows decrypting messages in the case when $C_{sec}$ is a generalized Reed–Solomon code (GRS code) and $r(R) = 1$. The key stages of the constructed attack are, firstly, finding the intersection of the linear span $\mathcal{L}(G_{pub}) = C_{pub}$ and $\mathcal{L}(GP) = C$ that spanned on the rows of the matrices $G_{pub}$ and $GP$ respectively, and secondly, finding the code $C$ by the subcode $C_{pub} \cap C$. In this paper we present an attack in the case when $C_{sec}$ is the Reed–Muller binary code of order $r$, length $2^m$ and $r(R) = 1$. The stages of finding the codes $C_{pub} \cap C$ and $C$ in this paper are completely different from the corresponding steps in attack by V. Gauthier and some others and other steps are the adaptation of the known results of cryptanalysis that applied in the case of GRS codes.

*Keywords: BBCRS cryptosystem; Reed–Muller codes; cryptanalysis.*

*Received March 14, 2021*