УДК 519.1 **DOI: 10.14529/mmp230107**

МНОГОСТОРОННЕЕ ЗАЩИЩЕННОЕ ВЫЧИСЛЕНИЕ ПОЛИНОМОВ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

Ю.В. Косолапов, Южный федеральный университет, г. Ростов-на-Дону, Российская Федерация

Целью децентрализации вычислений, выполняемых участниками протоколов информационного взаимодействия, обычно является повышение надежности и защищенности информационных систем. Основу децентрализованных вычислений составляют протоколы многосторонних защищенных вычислений (ПМЗВ), которые обычно не являются универсальными, а строятся для конкретных вычисляемых функций. В настоящей работе строится ПМЗВ для вычисления значений полиномов от нескольких переменных над конечным полем. Построенные протоколы основаны на линейных схемах разделения секрета, а их характеристики, такие как мощность правомочных и неправомочных коалиций, могут быть описаны в терминах характеристик линейных кодов и их степеней Шура – Адамара. В работе приводятся некоторые коды и кодовые конструкции, для которых удается такие характеристики найти аналитически.

Ключевые слова: многосторонние защищенные вычисления; линейные коды.

Введение

Для функции $f : \mathcal{X} \times ... \times \mathcal{X} \to \mathcal{Y}$ рассмотрим задачу ее многостороннего защищенного вычисления группой из n участников, каждый из которых владеет секретом $x_i \in \mathcal{X}$, $i \in \{1, ..., n\}$. Под защищенным вычислением здесь и далее понимается такой протокол вычисления, в ходе которого участник с номером i не получает новой информации о секретных аргументах других участников, кроме той, которую он может извлечь только из пары $(f(x_1, ..., x_n), x_i)$. Классическим примером является задача определения, кто из двух миллионеров богаче [1]. В этом случае $n = 2$, $\mathcal{X} = \mathbb{R}_+$ – множество положительных действительных чисел, $\mathcal{Y} = \{0, 1\}$, где $y = 1$ означает, что у первого участника состояние не меньше, чем у второго, а $y = 0$ означает, что богаче второй участник. В качестве функции $f : \mathbb{R}_+ \times \mathbb{R}_+ \to \{0, 1\}$ можно рассмотреть $f(x_1, x_2) = \operatorname{sign}(x_1 - x_2)$. На практике протоколы многосторонних защищенных вычислений (ПМЗВ) находят применение при защите биометрических данных в системах аутентификации, при защите данных, обрабатываемых в облачных сервисах, в системах голосования [2]. Также такие протоколы находят применение и в машинном обучении [3].

ПМЗВ обычно строятся для заранее определенного класса функций и не являются универсальными. В настоящей работе множества $\mathcal{X}$ и $\mathcal{Y}$ являются полем Галуа $\mathbb{F}_q$ мощности q, а класс вычисляемых функций имеет вид

$$\mathcal{F}_{n,q,r} = \left\{ f(x_1, ..., x_n) = \sum_{\substack{\boldsymbol{\alpha}=(\alpha_1,...,\alpha_n)\in \\ \mathbb{N}_0\times...\times\mathbb{N}_0}} a_{\boldsymbol{\alpha}} \cdot x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n},\ a_{\boldsymbol{\alpha}} \in \mathbb{F}_q, \deg(f) \leqslant r \right\}, \qquad (1)$$

где $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ и $\deg(f) = \max\limits_{a_{\boldsymbol{\alpha}} \neq 0} \{\mathsf{sum}(\boldsymbol{\alpha}) = \sum_{i=1}^{n} \alpha_i\}$. Число $\deg(f)$ назовем степенью функции f, тогда $\mathcal{F}_{n,q,r}$ – это множество полиномов от n переменных степени не выше r с коэффициентами из $\mathbb{F}_q$. Отметим, что задача незащищенного вычисления функций из $\mathcal{F}_{n,q,r}$ возникает, например, в асимметричных криптографических системах, основанных на применении полиномов от многих переменных [4]. Ряд исследований

таких криптографических схем [5–7] показывают неустойчивость некоторых из них к атакам по побочным каналам [8]. Одним из способов защиты является способ на основе схем разделения секрета, когда секретные данные разделяются на доли: с ростом числа долей экспоненциально растет сложность атак на основе побочных каналов [9]. Так как ПМЗВ обычно строятся на основе схем разделения секрета, причем вычисления выполняются над долями, то ПМЗВ для $\mathcal{F}_{n,q,r}$ могут представлять интерес, например, для проектировщиков защищенных криптографических модулей, основанных на вычислении полиномов из $\mathcal{F}_{n,q,r}$.

В работе построены ПМЗВ для функций из $\mathcal{F}_{n,q,r}$ на основе линейных кодов. Найдена связь таких характеристик ПМЗВ, как мощности правомочных и неправомочных коалиций, с параметрами линейных кодов и параметрами n, q, r. Рассмотрены коды и кодовые конструкции, для которых удалось аналитически оценить такие характеристики.

1. Предварительные сведения

В этом разделе приведем необходимые сведения о линейных кодах, а также линейных схемах разделения секрета, которые являются основой для строящегося ПМЗВ.

Диапазон натуральных чисел от a до b включительно обозначим $[a, b]$. Носителем вектора $\mathbf{a} = (a_1, ..., a_n)$ назовем множество $\mathrm{supp}(\mathbf{a}) = \{i : a_i \neq 0\}$, а число $\mathrm{wt}(\mathbf{a}) = |\mathrm{supp}(\mathbf{a})|$ – весом вектора $\mathbf{a}$. Скалярное произведение векторов $\mathbf{a}$ и $\mathbf{b}$ обозначим $\langle \mathbf{a}, \mathbf{b} \rangle$. Линейное подпространство C пространства $\mathbb{F}_q^n$ размерности k, такое, что минимальный вес ненулевого вектора из C равен d, называется $[n, k, d]_q$-кодом или просто $[n, k]_q$-кодом, когда минимальный вес d не играет роль в описании свойств кода. Длину, размерность и минимальный ненулевой вес кода C иногда будем обозначать $n(C)$, $k(C)$ и $d(C)$, когда потребуется подчеркнуть, к какому коду относятся эти характеристики. Код $C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n : \langle \mathbf{x}, \mathbf{c} \rangle = 0 \, \forall \mathbf{c} \in C\}$ называется дуальный к коду C. Любая $k \times n$-матрица G ранга k над полем $\mathbb{F}_q$, такая, что линейная оболочка $\mathcal{L}(G)$, натянутая на строки матрицы G, совпадает с C, называется порождающей матрицей $[n, k]_q$-кода C, а $(n - k) \times n$-матрица H ранга $n - k$, такая, что $\mathcal{L}(H) = C^\perp$, называется проверочной матрицей этого кода. Множество всех порождающих матриц кода C обозначим $\mathcal{G}(C)$. Отметим, что $C = \mathcal{L}(G)$ для всех G из $\mathcal{G}(C)$. Иногда произвольную порождающую матрицу кода C будем обозначать G_C.

Пусть $[1, n]$ – множество участников. Схема разделения секрета (СРС) Σ для n участников состоит из двух протоколов: протокола разделения секрета Share и протокола восстановления секрета Recon. Секретом в СРС могут быть векторные величины, как, например, в [10], но обычно секретом являются скалярные величины, так как СРС часто являются базисом для построения ПМЗВ. В настоящей работе множество возможных значений секрета совпадает с $\mathbb{F}_q$. В этом случае линейная СРС (ЛСРС) может быть описана с помощью $e \times (n + 1)$-матрицы $H = (\mathbf{h}_0, \mathbf{h}_1 ..., \mathbf{h}_n)$, в которой столбец $\mathbf{h}_0$ имеет вид $(1, 0, ..., 0)^T$. Такую ЛСРС будем обозначать $\Sigma(H)$, а соответствующие протоколы разделения и восстановления секрета – $\Sigma(H).\mathsf{Share}$ и $\Sigma(H).\mathsf{Recon}$ соответственно. Протокол $\Sigma(H).\mathsf{Share}$ для секрета $s \in \mathbb{F}_q$ состоит в случайном выборе $e - 1$ значений $r_1, ..., r_{e-1}$ из $\mathbb{F}_q$ и передаче по защищенному каналу участнику i его доли $[s]_i = \langle (s, r_1, ..., r_{e-1}), \mathbf{h}_i^T \rangle$. Здесь и далее под защищенным каналом передачи понимается канал, защищенный от несанкционированного наблюдения и изменения/подмены содержимого.

Множество участников $\tau = \{t_1, ..., t_c\} \subseteq [1, n]$ может восстановить секрет s по набору долей $[s]_{t_1}, ..., [s]_{t_c}$, если для столбцов матрицы H с номерами из τ найдутся в $\mathbb{F}_q$ такие c элементов $w_1, ..., w_c$, что $\mathbf{h}_0 = \sum_{i=1}^{c} w_i \mathbf{h}_{t_i}$. Такая коалиция называется правомочной, а соответствующий ей вектор $\mathbf{w} = (w_1, ..., w_c)$ – ее вектором реконструкции.

Таким образом, протокол $\Sigma(H).\mathsf{Recon}$ заключается в вычислении правомочной коалицией τ скалярного произведения векторов $(w_1, ..., w_c)$ и $([s]_{t_1}, ..., [s]_{t_c})$:

$$\langle (w_1, ..., w_c), ([s]_{t_1}, ..., [s]_{t_c}) \rangle = \sum_{i=1}^{c} w_i \langle (s, r_1, ..., r_{e-1}), \mathbf{h}_{t_i}^T \rangle = \langle (s, r_1, ..., r_{e-1}), \mathbf{h}_0^T \rangle = s.$$

Если набор столбцов матрицы H с номерами из множества τ не порождает столбец $\mathbf{h}_0$, то для коалиции τ их набор долей не несет новой информации о секрете. В этом случае коалиция называется неправомочной. Множество всех правомочных коалиций называется структурой доступа и обозначается $\Gamma(\Sigma(H))$, а множество всех неправомочных – структурой противника и обозначается $\mathcal{A}(\Sigma(H))$. Минимальной правомочной коалицией называется такая правомочная коалиция, ни одно собственное подмножество которой не является правомочной коалицией. Множество всех таких коалиций обозначим $\delta(\Gamma(H))$.

Для $[n, k]_q$-кода C известно, что в его проверочной матрице любые $d(C)-1$ столбцов линейно независимы, при этом подматрица проверочной матрицы, составленная из любых $n - d(C^\perp) + 1$ столбцов, имеет ранг $n - k$ [11]. Отсюда вытекает простое утверждение.

Утверждение 1. *Пусть H проверочная матрица $[n+1, n+1-e]_q$-кода C, $d(C) \geqslant 2$. Тогда для $\Sigma(H)$ любая коалиция мощности $d(C)-2$ и менее является неправомочной, а любая коалиция мощности $n - d(C^\perp) + 2$ и более является правомочной.*

Рассмотрим в качестве примера $\Sigma(\mathcal{H}_n)$, где $n \times (n+1)$-матрица $\mathcal{H}_n$ имеет вид

$$\mathcal{H}_n = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & -1 \\ \vdots & \vdots & \ddots & 0 & -1 \\ 0 & 0 & \cdots & 1 & -1 \end{pmatrix}.$$

Так как любые n столбцов этой матрицы линейно независимы, то $\mathcal{H}_n$ – проверочная матрица $[n+1, 1, n+1]_q$-кода. Следовательно, любая коалиция из $n-1$ участника является неправомочной, в то время как все участники образуют правомочную коалицию. Отметим, что протокол $\Sigma(\mathcal{H}_n).\mathsf{Recon}$ заключается в суммировании всех долей участников, так как первый по счету столбец матрицы $\mathcal{H}_n$ есть сумма последних n столбцов этой матрицы.

2. Защищенное вычисление функций из $\mathcal{F}_{n,q,r}$

Прежде чем построить ПМЗВ, напомним определение произведения Шура – Адамара и тензорного произведения. Для $\mathbf{a} = (a_1, ..., a_n)$ и $\mathbf{b} = (b_1, ..., b_n)$ из $\mathbb{F}_q^n$ вектор $\mathbf{a} \star \mathbf{b} = (a_1 b_1, ..., a_n b_n)$ называется произведением Шура – Адамара $\mathbf{a}$ и $\mathbf{b}$ [12]. Произведением Шура – Адамара $k_A \times n$-матрицы $A = (\mathbf{a}_i)_{i=1}^{k_A}$ и $k_B \times n$-матрицы $B = (\mathbf{b}_i)_{i=1}^{k_B}$ называется $k_A k_B \times n$-матрица, обозначаемая $A \star B$ и состоящая из строк вида $(\mathbf{a}_i \star \mathbf{b}_j)$, $i \in [1, k_A]$, $j \in [1, k_B]$. Произведение $A \star A$ будем обозначать A^2. Для $[n, k_A]_q$-кода C_A и $[n, k_B]_q$-кода C_B их произведение Шура – Адамара определяется так: $C_A \star C_B = \mathcal{L}(\{\mathbf{a} \star \mathbf{b} : \mathbf{a} \in C_A, \mathbf{b} \in C_B\})$. Известно также, что $C_A \star C_B = \mathcal{L}(G_A \star G_B)$, для $G_A \in \mathcal{G}(C_A)$, $G_B \in \mathcal{G}(C_B)$ [12, 13]. Квадратом кода C называется пространство (код) $C \star C$, которое далее обозначается C^2. Аналогично может быть определена любая степень s кода C: $C^s = C^{s-1} \star C$. Тензорным произведением двух векторов $\mathbf{a} = (a_1, ..., a_n)$ и $\mathbf{b}$ назовем вектор $\mathbf{a} \otimes \mathbf{b} := (a_1 \mathbf{b}, ..., a_n \mathbf{b})$, представляющий собой соединение n копий вектора $\mathbf{b}$, умноженных на соответствующие элементы вектора $\mathbf{a}$.

Рассмотрим линейную ЛСРС $\Sigma(H)$, где H – проверочная матрица кода C. Если u, v – секреты, $([u]_1, ..., [u]_n)$ и $([v]_1, ..., [v]_n)$ – наборы соответствующих долей, то i-й участник без обращения к другим участникам может вычислить свою долю, соответствующую секрету $u+v$: $[u+v]_i = [u]_i + [v]_i$. В этом случае говорят, что ЛСРС $\Sigma(H)$ обладает свойством аддитивности. Свойство аддитивности непосредственно вытекает из того, что векторы $[u] = (u, [u]_1, ..., [u]_n)$ и $[v] = (v, [v]_1, ..., [v]_n)$ являются кодовыми векторами кода $C^\perp$, поэтому и их сумма также принадлежит этому коду. Отсюда также вытекает, что каждый участник может вычислить долю секрета $\alpha \cdot u + \beta \cdot v$, где $\alpha, \beta \in \mathbb{F}_q$ – известные участникам скаляры. Однако для выполнения многосторонних защищенных вычислений часто необходимо также уметь «умножать» доли: получать такие доли, которые в протоколе восстановления секрета позволяют найти произведение секретов $u \cdot v$. Так как $[u]_i \cdot [v]_i = \langle (u, r_1, ..., r_{e-1}) \otimes (v, p_1, ..., p_{e-1}), (\mathbf{m}_i \otimes \mathbf{m}_i)^T \rangle$, то $(uv, [u]_1[v]_1, ..., [u]_n[v]_n) = (u, [u]_1, ..., [u]_n) \star (v, [v]_1, ..., [v]_n) \in C^\perp \star C^\perp$. Следовательно, секрет uv не может быть восстановлен в рамках $\Sigma(H)$. Однако он может быть восстановлен в рамках $\Sigma(H^2)$ на основе матрицы $H^2 = H \star H$, которая может быть вычислена каждым участником по несекретной матрице H. Таким образом, $\alpha[u] + \beta[v] = [\alpha u + \beta v] \in C^\perp$, $[u] \star [v] \in (C^\perp)^2$. Умножение двух секретов обобщается на умножение $l \in \mathbb{N}$ секретов.

Утверждение 2. *Пусть H – проверочная матрица $[n+1, n+1-e]_q$-кода C, $l \in \mathbb{N}$, $d(((C^\perp)^l)^\perp) \geqslant 2$. В рамках ЛСРС $\Sigma(H^l)$ любая коалиция мощности $d(((C^\perp)^l)^\perp) - 2$ и менее является неправомочной, а коалиция мощности $n - d((C^\perp)^l) + 2$ является правомочной.*

Вычисление функции $f \in \mathcal{F}_{n,q,r}$ могло бы сводиться к выполнению трех шагов: 1) вычислению каждым участником значений $\tilde{A}_{i,\boldsymbol{\alpha}} = a_{\boldsymbol{\alpha}} \prod_{l \in [1,n]} [x_l]_i^{\alpha_l}$ для ненулевых слагаемых ($a_{\boldsymbol{\alpha}} \neq 0$), где $[x_l]_i^{\alpha_l} = [x_l]_i \cdot ... \cdot [x_l]_i \in \mathbb{F}_q$, 2) суммированию значений $\tilde{A}_i = \sum_{a_{\boldsymbol{\alpha}} \neq 0} \tilde{A}_{i,\boldsymbol{\alpha}}$, а затем 3) к применению протокола восстановления секрета по значениям $\tilde{A}_i$ в рамках ЛСРС с подходящей степенью матрицы H. Однако заметим, что в функции f слагаемые в общем случае имеют разную степень. Поэтому простое суммирование значений $\tilde{A}_{i,\boldsymbol{\alpha}}$ является некорректным: числа $\tilde{A}_{i,\boldsymbol{\alpha}_1}$ и $\tilde{A}_{i,\boldsymbol{\alpha}_2}$, где $\mathsf{sum}(\boldsymbol{\alpha}_1) \neq \mathsf{sum}(\boldsymbol{\alpha}_2)$, являются долями из векторов долей $[a_{\boldsymbol{\alpha}_1} \cdot x_1^{\alpha_{1,1}} \cdot ... \cdot x_n^{\alpha_{1,n}}]$ и $[a_{\boldsymbol{\alpha}_2} \cdot x_1^{\alpha_{2,1}} \cdot ... \cdot x_n^{\alpha_{2,n}}]$, полученных в рамках ЛСРС с разными матрицами $H^{\mathsf{sum}(\boldsymbol{\alpha}_1)}$ и $H^{\mathsf{sum}(\boldsymbol{\alpha}_2)}$. Поэтому в ПМЗВ $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$ перед суммированием выполняется приведение всех значений $\tilde{A}_{i,\boldsymbol{\alpha}}$ к значениям $A_{i,\boldsymbol{\alpha}}$, которые для всех $a_{\boldsymbol{\alpha}} \neq 0$ являются долями из векторов долей, полученных в рамках ЛСРС $\Sigma(H^{\deg(f)})$:

$$A_{i,\boldsymbol{\alpha}} = \tilde{A}_{i,\boldsymbol{\alpha}} \cdot [1]_i^{\deg(f) - \mathsf{sum}(\boldsymbol{\alpha})},\ [1] = (1, 0, .., 0) \cdot H.$$

Протокол 1. $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$

Входные данные. Каждый участник $i \in [1, n]$ имеет секретный аргумент x_i, ЛСРС $\Sigma(H)$ и вид вычисляемой функции $f \in \mathcal{F}_{n,q,r}$, $\mathbf{w} = (w_1, ..., w_n)$ – вектор реконструкции для коалиции из n участников в рамках ЛСРС $\Sigma(H^{\deg(f)})$.
Цель. Вычислить значение $f(x_1, ..., x_n)$ всеми участниками.
Протокол.

1. **Этап обмена.** Каждый участник $i \in [1, n]$
   (a) используя $\Sigma(H).\mathsf{Share}$ для x_i, строит $[x_i]$;
   (b) передает $[x_i]_j$ по защищенному каналу участнику $j \in \{1, ..., n\} \setminus \{i\}$.

2. **Этап вычислений.** Каждый участник $i \in [1,n]$ вычисляет
   (a) $A_i = \sum_{a_{\boldsymbol{\alpha}} \neq 0} \left(a_{\boldsymbol{\alpha}} \big(\prod_{l \in [1,n]} [x_l]_i^{\alpha_l} \big) [1]_i^{\deg(f) - \mathsf{sum}(\boldsymbol{\alpha})} \right)$;
3. **Этап реконструкции.** Каждый участник $i \in [1,n]$
   (a) используя $\Sigma(\mathcal{H}_n).\mathsf{Share}$ для секрета A_i строит $[A_i] = (A_i, a_{i,1}, ..., a_{i,n})$;
   (b) каждому $j \in [1,n] \setminus \{i\}$ по защищенному каналу передает $a_{i,l}$, $l \neq j$;
   (c) для $l = i (\bmod n) + 1$ вычисляет $B_l = \langle \mathbf{w}, (a_{1,l}, ..., a_{n,l}) \rangle$ и передает его остальным участникам по защищенным каналам;
   (d) используя $\Sigma(\mathcal{H}_n).\mathsf{Recon}$ находит $f(x_1, ..., x_n) = \sum_{i=1}^{n} B_i$.

Теорема 1. *Каждый участник* $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$ *находит значение функции* $f \in \mathcal{F}_{n,q,r}$.

Доказательство. На шаге (d) этапа реконструкции каждый участник имеет набор B_1, ..., B_n. При этом в протоколе $\Sigma(\mathcal{H}_n).\mathsf{Recon}$ восстановление секрета выполняется суммированием всех долей. Учитывая это, а также то, что $A_i = \sum_{l=1}^{n} a_{i,l}$ для $i \in [1,n]$, получаем

$$\sum_{i \in [1,n]} B_i = \sum_{i \in [1,n]} \langle \mathbf{w}, (a_{1,i}, ..., a_{n,i}) \rangle = \left\langle \mathbf{w}, \left(\sum_{i \in [1,n]} a_{1,i}, ..., \sum_{\in [1,n]} a_{n,i} \right) \right\rangle = \langle \mathbf{w}, (A_1, ..., A_n) \rangle.$$

Так как A_i можно рассматривать как долю i-ого участника в $\Sigma(H^r)$ для секрета $f(x_1, ..., x_n)$, и $\mathbf{w}$ – вектор реконструкции для этой ЛСРС, то $\langle \mathbf{w}, (A_1, ..., A_n) \rangle = f(x_1, ..., x_n)$. □

Теорема 2. *Участник* $i \in [1,n]$ *протокола* $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$ *для функции* $f \in \mathcal{F}_{n,q,r}$ *не получает новой информации о значениях секретов* x_j, $j \in [1,n] \setminus \{i\}$, *за исключением той, которую он может получить из пары* $(f(x_1, ..., x_n), x_i)$.

Доказательство. На этапе обмена каждый участник не узнает какой-либо информации о секретах других участников в силу того, что располагает только одной долей от каждого секрета. Этап вычислений каждый участник выполняет локально без обмена данными с другими участниками, поэтому на этом этапе информация о секретах не добавляется. На этапе реконструкции значения A_i разделяются на доли в соответствии с $\Sigma(\mathcal{H}_n)$, для которой правомочной коалицией является только коалиция из всех участников, поэтому полученные на шаге (b) этапа реконструкции $n-1$ долей не несут новой информации о значениях A_i и соответственно о секретных аргументах. Осталось показать, что наборы $(B_1, ..., B_n)$, полученные после выполнения шага (c) участником $i \in [1,n]$, не дают новой информации о секретах, за исключением той, которую он может получить из пары $(f(x_1, ..., x_n), x_i)$. Предположим, что перед выполнением шага (c) участник i получает от оракула значение $f(x_1, ..., x_n)$. Тогда участник i может найти набор $(B_1, ..., B_n)$. Действительно, значения B_l для $l \neq i$ участник i может вычислить после завершения шага (b) этапа реконструкции, а $B_i = f(x_1, ..., x_n) - \sum_{l \neq i} B_l$. Это и означает, что лишней информации о секретах в протоколе $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$ участники не получают.

□

В $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$ только при взаимодействии всех участников может быть вычислена функция $f \in \mathcal{F}_{n,q,r}$. Построим протокол $\mathrm{GSMPC}_{\mathcal{F}_{n,q,r}}$, когда на этапе реконструкции взаимодействует только некоторая коалиция $\mathcal{G} \subset [1,n]$, являющаяся правомочной для $\Sigma(H^{\deg(f)})$ и $\mathcal{G} \in \delta(\Gamma(H^{\deg(f)}))$. Пусть $\mathbf{w}$ – вектор реконструкции для $\mathcal{G}$, очевидно, что $\mathrm{wt}(\mathbf{w}) \leqslant |\mathcal{G}|$.

Протокол 2. $\mathrm{GSMPC}_{\mathcal{F}_{n,q,r}}$

Входные данные. Для всех $i \in [1,n]$, участник i имеет секретный аргумент x_i, $\Sigma(H)$ и вид вычисляемой функции $f \in \mathcal{F}_{n,q,r}$, $\mathbf{w} = (w_1, ..., w_g)$ – вектор реконструкции для $\mathcal{G} = \{j_1, ..., j_g\} \in \delta(\Gamma(H^{\deg(f)}))$ участников в рамках ЛСРС $\Sigma(H^{\deg(f)})$, $j_1 < ... < j_g$.
Цель. Вычислить $f(x_1, ..., x_n)$ участниками коалиции $\mathcal{G}$.
Протокол.

1. **Этап обмена.** Как в $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$.
2. **Этап вычислений.** Как в $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$.
3. **Этап реконструкции.** Каждый участник $j_i \in \mathcal{G}$
   (a) используя $\Sigma(H^{\deg(f)})$.Share для секрета A_{j_i} строит $[A_{j_i}] = (A_{j_i}, a_{j_i,1}, ..., a_{j_i,n})$;
   (b) каждому $j \in \mathcal{G} \setminus \{j_i\}$ по защищенному каналу передает $a_{j_i,l}$, $l \in \mathcal{G}, l \neq j$;
   (c) для $l = i(\bmod |\mathcal{G}|)+1$ вычисляет $B_{j_l} = \langle \mathbf{w}, (a_{j_1,j_l}, ..., a_{j_g,j_l})\rangle$ и передает его остальным участникам из $\mathcal{G}$ по защищенным каналам.
   (d) используя $\Sigma(H^{\deg(f)})$.Recon находит $f(x_1, ..., x_n) = \sum_{m\in[1,g]} w_m B_{j_m}$.

Теорема 3. *Каждый участник* $\mathrm{GSMPC}_{\mathcal{F}_{n,q,r}}$ *находит значение функции* $f \in \mathcal{F}_{n,q,r}$.

Доказательство. На шаге $3(d)$ протокола $\mathrm{GSMPC}_{\mathcal{F}_{n,q,r}}$ каждый участник $\mathcal{G}$ имеет набор $B_{j_1}, ..., B_{j_g}$. По правилу восстановления секрета коалицией $\mathcal{G}$ в $\Sigma(H^r)$.Recon, получаем

$$\begin{aligned}\sum_{m\in[1,g]} w_m B_{j_m} &= \sum_{m\in[1,g]} w_m \langle \mathbf{w}, (a_{j_1,j_m}, ..., a_{j_g,j_m})\rangle \\ &= w_1 w_1 a_{j_1,j_1} + w_1 w_2 a_{j_2,j_1} + ... + w_1 w_g a_{j_g,j_1} + \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &+ w_g w_1 a_{j_1,j_g} + w_g w_2 a_{j_2,j_g} + ... + w_g w_g a_{j_g,j_g} \\ &= \sum_{m\in[1,g]} w_m \langle \mathbf{w}, (a_{j_m,j_1}, ..., a_{j_m,j_g})\rangle = \sum_{m\in[1,g]} w_m A_{j_m} = f(x_1, ..., x_n).\end{aligned}$$

Предпоследнее равенство вытекает из того, что $[A_{j_m}] = (A_{j_m}, a_{j_m,1}, ..., a_{j_m,n})$ и $\mathbf{w}$ – вектор реконструкции для $\Sigma(H^{\deg(f)})$. Значение A_{j_m} можно рассматривать как долю участника j_m в рамках $\Sigma(H^{\deg(f)})$ для секрета $f(x_1, ..., x_n)$. Отсюда вытекает последнее равенство. □

Теорема 4. *Пусть* $\mathcal{G} \in \delta(\Gamma(H^{\deg(f)}))$. *Участник* $i \in \mathcal{G}$ *протокола* $\mathrm{GSMPC}_{\mathcal{F}_{n,q,r}}$ *для* $f \in \mathcal{F}_{n,q,r}$ *не получает новой информации о значениях секретов* x_j, $j \in [1,n] \setminus \{i\}$, *за исключением той, которую он может получить из пары* $(f(x_1, ..., x_n), x_i)$.

Доказательство. Так как $\mathrm{GSMPC}_{\mathcal{F}_{n,q,r}}$ отличается от $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$ только в этапе реконструкции, то покажем, что наборы $(B_{j_1}, ..., B_{j_g})$, полученные после выполнения шага (c) участником $j_i \in \mathcal{G}$, не дают новой информации о секретах, за исключением той, которую он может получить из пары $(f(x_1, ..., x_n), x_i)$. Предположим, что перед выполнением шага (c) участник j_i получает от оракула значение $f(x_1, ..., x_n)$. Тогда j_i может найти набор $(B_{j_1}, ..., B_{j_g})$: значения B_{j_l} для $l \neq i$ участник j_i может вычислить после шага (b) реконструкции, а $B_{j_i} = w_i^{-1}(f(x_1, ..., x_n) - \sum_{j_l\in\mathcal{G}, l\neq i} w_l B_{j_l})$, причем $w_i \neq 0$, так как $\mathcal{G} \in \delta(\Gamma(H^{\deg(f)}))$. □

Протокол $\mathrm{GSMPC2}_{\mathcal{F}_{n,q,r}}$ является обобщением $\mathrm{GSMPC}_{\mathcal{F}_{n,q,r}}$ на случай произвольной коалиции из $\Gamma(H^{\deg(f)})$, а теоремы 5 и 6 доказываются по аналогии с теоремами 1 и 2.

Протокол 3. $\mathrm{GSMPC2}_{\mathcal{F}_{n,q,r}}$

Входные данные. Для всех $i \in [1,n]$, участник i имеет секретный аргумент x_i, $\Sigma(H)$ и вид функции $f \in \mathcal{F}_{n,q,r}$, $\mathbf{w} = (w_1, ..., w_g)$ – вектор реконструкции для $\mathcal{G} = \{j_1, ..., j_g\} \in \Gamma(H^{\deg(f)})$ участников в рамках СРС $\Sigma(H^{\deg(f)})$, $j_1 < ... < j_g$.
Цель. Вычислить $f(x_1, ..., x_n)$ участниками коалиции $\mathcal{G}$.
Протокол.

1. **Этап обмена.** Как в $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$.
2. **Этап вычислений.** Как в $\mathrm{SMPC}_{\mathcal{F}_{n,q,r}}$.
3. **Этап реконструкции.** Каждый участник $j_i \in \mathcal{G}$
   (a) используя $\Sigma(\mathcal{H}_{|\mathcal{G}|})$.$\mathsf{Share}$ для A_{j_i} строит $[A_{j_i}] = (A_{j_i}, a_{j_i,1}, ..., a_{j_i,n})$;
   (b) как в $\mathrm{GSMPC}_{\mathcal{F}_{n,q,r}}$.
   (c) как в $\mathrm{GSMPC}_{\mathcal{F}_{n,q,r}}$.
   (d) используя $\Sigma(\mathcal{H}_{|\mathcal{G}|})$.$\mathsf{Recon}$ находит $f(x_1, ..., x_n) = \sum_{m \in [1,g]} B_{j_m}$.

Теорема 5. *Каждый участник* $\mathrm{GSMPC2}_{\mathcal{F}_{n,q,r}}$ *находит значение функции* $f \in \mathcal{F}_{n,q,r}$.

Теорема 6. *Пусть* $\mathcal{G} \in \delta(\Gamma(H^{\deg(f)}))$. *Участник* $i \in \mathcal{G}$ *протокола* $\mathrm{GSMPC2}_{\mathcal{F}_{n,q,r}}$ *для* $f \in \mathcal{F}_{n,q,r}$ *не получает новой информации о значениях секретов* x_j, $j \in [1,n] \setminus \{i\}$, *за исключением той, которую он может получить из пары* $(f(x_1, ..., x_n), x_i)$.

Теорема 7. *Пусть* $f \in \mathcal{F}_{n,q,r}$, H – *проверочная матрица кода* $C \subseteq \mathbb{F}_q^{n+1}$, $(C^\perp)^r \neq \mathbb{F}_q^{n+1}$, $T_r = \min\{d(C), d(((C^\perp)^r)^\perp)\} \geqslant 2$, $R_r = \min\{d(C^\perp), d((C^\perp)^r)\} \geqslant 2$. *Тогда существует ПМЗВ такой, что любые* $n - R_r + 2$ *могут вычислить значение функции* f, *а любая коалиция мощности не более* $T_r - 2$ *является неправомочной.*

Доказательство. Доказательство вытекает из утверждений 1 и 2 и того, что для любой правомочной коалиции может быть применен ПМЗВ $\mathrm{GSMPC2}_{\mathcal{F}_{n,q,r}}$. □

Оценим сложность построенных ПМЗВ. При этом сложность построения степеней матрицы H не будет учитываться, так как такие матрицы могут быть построены заранее. Пусть $f \in \mathcal{F}_{n,q,r}$. Через $n_+(f)$ обозначим количество операций алгебраического сложения, а через $n_\times(f)$ – количество операций умножения в представлении (1). При этом будем считать, что для $\alpha \in \mathbb{N}$ выражение x^α вычисляется за $\alpha - 1$ операцию умножения (варианты оптимизации вычисления степеней здесь не рассматриваются), а умножение на скаляр выполняется за одну операцию. Тогда

$$n_+(f) = \max\left\{\Big(\sum_{a_{\boldsymbol{\alpha}} \neq 0} 1\Big) - 1, 0\right\},\ n_\times(f) = \sum_{a_{\boldsymbol{\alpha}} \neq 0} \Big(1 + \sum_{l=1}^{n} \max\{\alpha_l - 1, 0\}\Big).$$

Для удобства обозначим через $N_+(f)$ и $N_\times(f)$ соответственно количество сложений и умножений, выполняемых каждым участником на этапе вычислений (в каждом из построенных протоколов этот этап одинаковый). Эти величины выражаются следующим образом:

$$N_+(f) = n_+(f),\ N_\times(f) = \sum_{a_{\boldsymbol{\alpha}} \neq 0} \big(\max\{\deg(f) - \mathsf{sum}(\boldsymbol{\alpha}) - 1, 0\}\big) + n_\times(f) = \psi_f + n_\times(f).$$

В табл. 1 N_+, $N_\times$ и N_t обозначают соответственно число операций сложения в поле $\mathbb{F}_q$, число операций умножения в этом поле, а также объем пересылаемых данных, где единицей объема является объем, необходимый для представления одного элемента поля $\mathbb{F}_q$. Таким образом, для вычисления функции $f \in \mathcal{F}_{n,q,r}$ каждому участнику требуется выполнить не более $e + 3n - 4 + N_+(f)$ операций сложения и не более $e + n + N_\times(f)$ операций умножения в поле $\mathbb{F}_q$, а также отправить по защищенным каналам данные в объеме, необходимом для раздельной передачи $(n-1)^2 + 2(n-1)$ элементов поля $\mathbb{F}_q$.

Таблица 1

Вычислительные и коммуникационные затраты одного участника ПМЗВ

Шаг	N_+	$N_\times$	N_t
1(a)	$\leqslant e-1$	$\leqslant e$	0
1(b)	0	0	$n-1$
2(a)	$N_+(f)$	$N_\times(f)$	0
3(a)	$\leqslant n-1$	0	0
3(b)	0	0	$\leqslant (n-1)^2$
3(c)	$\leqslant n-1$	$\leqslant n$	$\leqslant n-1$
3(d)	$\leqslant n-1$	0	0

Отметим, что при незащищенном вычислении функции, когда каждый участник располагает полным набором аргументов (например, после публикации аргументов от остальных участников), каждому участнику потребуется выполнить не более $n_+(f)$ операций сложения и не более $n_\times(f)$ операций умножения в поле $\mathbb{F}_q$. Поэтому $\Delta_+ = e + 3n - 4$, $\Delta_\times = e + n + \psi_f$ и $\Delta_t = (n-1)^2 + 2(n-1) - 1$ можно рассматриваться как накладные расходы, требуемые для обеспечения защищенности вычислений. Заметим, что количество дополнительных операций сложения и число пересылок не зависит от функции f, а число операций умножения зависит, так как выполняется процедура приведения долей к долям в рамках схемы СРС $H^{\deg(f)}$ (см. этап вычислений ПМЗВ).

3. Примеры кодов и кодовых конструкций для ПМЗВ

Как вытекает из теоремы 7, характеристики построенных ПМЗВ определяются с помощью минимальных кодовых расстояний кодов C и C^r, а также минимальных кодовых расстояний дуальных к ним кодов. Отметим, что для произвольного линейного кода C в общем случае неизвестно не только кодовое расстояние, но и размерность кода C^r. То же относится и к $(C^r)^\perp$. Поэтому для получения протокола с гарантированными свойствами требуются классы кодов, для которых отмеченные выше характеристики можно легко найти. Далее рассматриваются некоторые такие классы кодов и кодовых конструкций.

3.1. Обобщенные коды Рида – Соломона

Напомним, что обобщенным кодом Рида – Соломона (ОРС-кодом) размерности k и длины n называется подпространство $\mathbb{F}_q^n$ размерности k вида:

$$\mathrm{GRS}_{n,k}(\mathbf{x}, \mathbf{y}) = \{(f(x_1)y_1, ..., f(x_n)y_n) : f(x) \in \mathbb{F}_q[x], \deg(f(x)) < k\},$$

где $\mathbf{x} = (x_1, ..., x_n)$ – вектор с попарно различными элементами поля $\mathbb{F}_q$, а $\mathbf{y} = (y_1, ..., y_n) \in \mathbb{F}_q^n$ – вектор без нулевых координат. Из определения вытекает вложение

$$\mathrm{GRS}_{n,k_1}(\mathbf{x}, \mathbf{y}) \subseteq \mathrm{GRS}_{n,k_2}(\mathbf{x}, \mathbf{y}),\ k_2 \geqslant k_1. \tag{2}$$

Известно, что $\mathrm{GRS}_{n,k}(\mathbf{x}, \mathbf{y})^\perp = \mathrm{GRS}_{n,n-k}(\mathbf{x}, \tilde{\mathbf{y}})$ для некоторого $\tilde{\mathbf{y}}$, а также

$$\mathrm{GRS}_{n,k_1}(\mathbf{x}, \mathbf{y}) \star \mathrm{GRS}_{n,k_2}(\mathbf{x}, \mathbf{y}) = \mathrm{GRS}_{n,\min\{k_1+k_2-1,n\}}(\mathbf{x}, \mathbf{y} \star \mathbf{y}), \tag{3}$$

$$\mathrm{GRS}_{n,k}(\mathbf{x}, \mathbf{y})^r = \mathrm{GRS}_{n,\min\{r(k-1)+1,n\}}(\mathbf{x}, \mathbf{y}^r),\ \mathbf{y}^r = \underbrace{\mathbf{y} \star ... \star \mathbf{y}}_{r}. \tag{4}$$

Лемма 1. *Пусть H – проверочная матрица $[n+1, k]_q$-кода $\mathrm{GRS}_{n+1,k}(\mathbf{x}, \mathbf{y})$, $r \in \mathbb{N}$, $r < \lfloor n/(n-k) \rfloor$. Тогда $T_r = n-k+2$, $R_r = n-r(n-k)+1$.*

Доказательство. По свойствам ОРС-кодов и из условия леммы получаем

$$d((((\mathrm{GRS}_{n+1,k}(\mathbf{x}, \mathbf{y}))^\perp)^r)^\perp) = r(n-k)+2,\ d(((\mathrm{GRS}_{n+1,k}(\mathbf{x}, \mathbf{y}))^\perp)^r) = n - r(n-k) + 1.$$

Так как $d(\mathrm{GRS}_{n+1,k}(\mathbf{x}, \mathbf{y})) = n-k+2$, то из теоремы 7 получаем $T_r = n-k+2$. С другой стороны, $d(\mathrm{GRS}_{n+1,k}(\mathbf{x}, \mathbf{y})^\perp) = k+1$, поэтому из теоремы 7

$$R_r = \min\{k+1, n-r(n-k)+1\} = n - r(n-k) + 1 \geqslant 2,$$

где последнее неравенство вытекает из условия $r < \lfloor n/(n-k) \rfloor$. □

Теорема 8. *Пусть $f \in \mathcal{F}_{n,q,r}$, $n \leqslant q$, $r, t \in \mathbb{N}$, $rt < n$. Существует ПМЗВ для f, в котором любая коалиция мощности t является неправомочной, а любая коалиция мощности не менее $rt+1$ является правомочной.*

Доказательство. Для доказательства достаточно найти параметры обобщенного $[n+1, k]_q$-кода Рида – Соломона для $\mathrm{GSMPC2}_{\mathcal{F}_{n,q,r}}$. По теореме 7 с учетом леммы 1 получаем, что любая коалиция мощности $T_r - 2 = n-k$ не является правомочной. Отсюда $t = n-k$. Подставляя вместо R_r его выражение из леммы 1, из теоремы 7 получим, что любые $r(n-k)+1 = rt+1$ участников являются правомочной коалицией. □

3.2. Коды Рида – Маллера

Для определения бинарных кодов Рида – Маллера и исследования некоторых их свойств рассмотрим $\mathbb{F}_2[x_1, ..., x_m]$ – кольцо полиномов от m переменных над полем $\mathbb{F}_2$. Полиномы из $\mathbb{F}_2[x_1, ..., x_m]$ будем записывать в виде:

$$f(x_1, ..., x_m) = \sum_{\boldsymbol{\alpha}=(\alpha_1,...,\alpha_m) \in \mathbb{F}_2^m} f_{\boldsymbol{\alpha}} \bar{x}^{\boldsymbol{\alpha}},$$

где $\bar{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} ... x_m^{\alpha_m}$ – моном степени $\mathrm{wt}(\boldsymbol{\alpha})$. Для вектора $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_m) \in \mathbb{F}_2^m$ символом $f(\boldsymbol{\alpha})$ будем обозначать значение полинома $f(x_1, ..., x_m)$, вычисленное при $x_i = \alpha_i$, $i = 1, ..., m$. Степень $deg(f)$ полинома f определяется как максимальная степень его ненулевых мономов. Пусть $\mathbb{F}_2^{(r)}[x_1, ..., x_m]$ – линейное пространство полиномов из $\mathbb{F}_2[x_1, ..., x_m]$ степени не выше r. Определим оператор $C_{(m,r)} : \mathbb{F}_2^{(r)}[x_1, ..., x_m] \to \mathbb{F}_2^n$ следующим образом: $C_{(m,r)}(f) = (f(\boldsymbol{\alpha}_1), ..., f(\boldsymbol{\alpha}_{2^m}))$, где $\boldsymbol{\alpha}_i, \boldsymbol{\alpha}_j \in \mathbb{F}_2^m$, $\boldsymbol{\alpha}_i \neq \boldsymbol{\alpha}_j$ для $i \neq j$. Бинарный код Рида – Маллера $\mathrm{RM}(l, m)$ с параметрами m и l определяется

следующим образом: $\mathrm{RM}(m,l)=\{C_{(m,l)}(f)|f\in\mathbb{F}_2^{(l)}[x_1,...,x_m]\}$. Из определения и [14] вытекает, что

$$\mathrm{RM}(m,l_1)\subseteq\mathrm{RM}(m,l_2),\ l_1\leqslant l_2, \tag{5}$$

$$d(\mathrm{RM}(l,m))=2^{m-l},\ \mathrm{RM}(l,m)^{\perp}=\mathrm{RM}(m-l-1,m), \tag{6}$$

$$\mathrm{RM}(l_1,m)\star\mathrm{RM}(l_2,m)=\mathrm{RM}(\min\{m,l_1+l_2\},m). \tag{7}$$

Лемма 2. *Пусть H – проверочная матрица кода Рида – Маллера $\mathrm{RM}(l,m)$, $r\in\mathbb{N}$, $r<\lfloor m/(m-l-1)\rfloor$. Тогда $T_r=2^{m-l}, R_r=2^{m-r(m-l-1)}$.*

Доказательство. Из свойств кода Рида – Маллера получаем:

$$d(((\mathrm{RM}(l,m)^{\perp})^r)^{\perp})=2^{r(m-l-1)+1},\ d((\mathrm{RM}(l,m)^{\perp})^r)=2^{m-r(m-l-1)}.$$

Так как $d(\mathrm{RM}(l,m))=2^{m-l}$, $d(\mathrm{RM}(l,m)^{\perp})=2^{l+1}$, то $T_r=2^{\min\{m-l,r(m-l-1)+1\}}=2^{m-l}$ и, с учетом условия леммы, $R_r=\min\{2^{l+1},2^{m-r(m-l-1)}\}=2^{m-r(m-l-1)}\geqslant 2$. □

Теорема 9. *Пусть $f\in\mathcal{F}_{2^m-1,2,r}$, $t\in\mathbb{N}$, $rt<m$. Существует ПМЗВ для f, в котором любая коалиция мощности t является неправомочной, а любая коалиция мощности не менее $2^m-\lfloor 2^{m+r}/(t+2)^r\rfloor+1$ является правомочной.*

Доказательство. Найдем подходящие параметры кода $\mathrm{RM}(l,m)$. По теореме 7 и лемме 2 получаем, что любая коалиция мощности T_r-2 не является правомочной. Отсюда $t=2^{m-l}-2$ или $l=m-\lfloor\log_2(t+2)\rfloor$. Подставляя вместо R_r его выражение из леммы 2 и учитывая $2^m=n+1$, по теореме 7 получим $n-R_r+2\leqslant 2^m-\lfloor(2^{m+r})/((t+2)^r)\rfloor+1$. □

Характеристики степеней ОРС-кодов и кодов Рида – Маллера приведены в табл. 2 и могут быть использованы для оценки характеристик ПМЗВ в соответствии с теоремой 7.

Таблица 2

Характеристики степеней ОРС-кодов и двоичных кодов Рида – Маллера

	C	
	$\mathrm{GRS}_{n,k}(\mathbf{x},\mathbf{y})$	$\mathrm{RM}(l,m)$
$d(C)$	$n-k+2$	2^{m-l}
$d(C^{\perp})$	$k+1$	2^{l+1}
$d(((C^{\perp})^r)^{\perp})$	$r(n-k)+2$	$2^{r(m-l-1)+1}$
$d((C^{\perp})^r)$	$n-r(n-k)+1$	$2^{m-r(m-l-1)}$

3.3. Тензорное произведение кодов

Напомним, что тензорным произведением $k_A\times n_A$-матрицы A и $k_B\times n_B$-матрицы B называется $k_Ak_B\times n_An_B$-матрица, состоящая из строк вида $\mathbf{a}_i\otimes\mathbf{b}_j$, $i\in[1,k_A]$, $j\in[1,k_B]$. Тензорное произведение матриц обозначается $A\otimes B$. Внешнюю прямую сумму пространств V и W обозначим $V\oplus W$. Если $V,W\subseteq\mathbb{F}_q^n$, то внутренняя сумма подпространств V и W обозначается $W+V$. Тензорным произведением $[n_A,k_A,d_A]_q$-кода C_A и $[n_B,k_B,d_B]_q$-кода C_B называется код, обозначаемый $C_A\otimes C_B$ и порождаемый матрицей $G_A\otimes G_B$, где $G_A\in\mathcal{G}(C_A)$, $G_B\in\mathcal{G}(C_B)$. Известно, что код $C_A\otimes C_B$ является

$[n_An_B, k_Ak_B, d_Ad_B]_q$-кодом [11], а произведение Шура – Адамара для кодов $C_A \otimes C_B$ и $D_A \otimes D_B$, где $C_A, D_A \subseteq \mathbb{F}_q^{n_A}$, $C_B, D_B \subseteq \mathbb{F}_q^{n_B}$, обладает следующим свойством [13]:

$$(C_A \otimes C_B) \star (D_A \otimes D_B) = (C_A \star D_A) \otimes (C_B \star D_B). \tag{8}$$

Следующая теорема позволяет определить $d((C_A \otimes C_B)^\perp)$.

Теорема 10. *Пусть C_A – $[n_A, k_A, d_A]_q$-код, C_B – $[n_B, k_B, d_B]_q$-код, $d_A^\perp$ – минимальное кодовое расстояние кода $C_A^\perp$, $d_B^\perp$ – минимальное кодовое расстояние кода $C_B^\perp$, d – минимальное кодовое расстояние кода $(C_A \otimes C_B)^\perp$. Тогда $d = \min\{d_A^\perp, d_B^\perp\}$.*

Доказательство. Так как, $(C_A \otimes C_B)^\perp = \mathbb{F}_q^{n_A} \otimes C_B^\perp + C_A^\perp \otimes \mathbb{F}_q^{n_B}$, где $\mathbb{F}_q^{n_A} \otimes C_B^\perp = \oplus_{i=1}^{n_A} C_B^\perp$, а код $C_A^\perp \otimes \mathbb{F}_q^{n_B}$ перестановочно эквивалентен прямой сумме $\oplus_{i=1}^{n_B} C_A^\perp$, то $d \leqslant \min\{d_A^\perp, d_B^\perp\}$. Докажем равенство. Пусть $G_A = (g_1^A, \ldots, g_{n_A}^A)$ – порождающая матрица кода C_A, $G_B = (g_1^B, \ldots, g_{n_B}^B)$ – порождающая матрица кода C_B, где g_i^A – столбцы высоты k_A, g_j^B – столбцы высоты k_B. Тогда порождающая матрица $G_A \otimes G_B$ кода $C_A \otimes C_B$ является проверочной матрицей кода $(C_A \otimes C_B)^\perp$. Следовательно, любые $d-1$ столбцов матрицы $G_A \otimes G_B$ линейно независимы, при этом найдутся d линейно зависимых столбцов. Пусть такими столбцами являются

$$g_{i_1}^A \otimes g_{j_1}^B, \ldots, g_{i_d}^A \otimes g_{j_d}^B, \tag{9}$$

для некоторых $i_1, ..., i_d \in [1, n_A]$, $j_1, ..., j_d \in [1, n_2]$. Отметим, что в наборе $i_1, ..., i_d$ могут быть совпадающие элементы; аналогично и в наборе $j_1, ..., j_d$ также могут быть совпадающие элементы. Пусть $\tau_1 = \{a_1, \ldots, a_{t_1}\}$ – множество разных номеров из набора $i_1, \ldots, i_d$, а $\tau_2 = \{b_1, \ldots, b_{t_2}\}$ – множество разных номеров из набора $j_1, \ldots, j_d$. Пусть G_1 – матрица, состоящая из t_1 столбцов матрицы G_A, номера которых принадлежат τ_1, G_2 – матрица, аналогично строящаяся по матрице G_B и множеству τ_2. По определению тензорного произведения все столбцы из набора (9) содержатся в наборе столбцов матрицы $G_1 \otimes G_2$ (заметим, что в матрице $G_1 \otimes G_2$ могут быть и другие столбцы).

Предположим, что $d < \min\{d_A^\perp, d_B^\perp\}$. Так как любые $d_A^\perp - 1$ столбцов матрицы G_A и любые $d_B^\perp - 1$ столбцов матрицы G_B линейно независимы, то $\operatorname{rank}(G_1) = t_1 \leqslant d$, $\operatorname{rank}(G_2) = t_2 \leqslant d$. По свойству тензорного произведения в этом случае получаем $\operatorname{rank}(G_1 \otimes G_2) = \operatorname{rank}(G_1) \cdot \operatorname{rank}(G_2) = t_1 \cdot t_2$. Таким образом, в матрице $G_1 \otimes G_2$ все столбцы линейно независимы, и поэтому любое подмножество столбцов этой матрицы также линейно независимо. Отсюда получаем, что набор (9) должен быть линейно независимым, что противоречит предположению. Таким образом, d не может быть меньше $\min\{d_A^\perp, d_B^\perp\}$. □

Пусть C – $[n+1, k, d]_q$-код, причем $C = (V_1 \otimes V_2)^\perp$, где V_i – $[n_i, k_i, d_i]_q$-код, $i = 1, 2$. В этом случае $n = n_1n_2 - 1$, $k = n - k_1k_2$, $C^\perp = V_1 \otimes V_2$, $d(C^\perp) = d(V_1)d(V_2)$ и, как следует из теоремы 10, $d(C) = \min\{d(V_1^\perp), d(V_2^\perp)\}$. Из (8) вытекает равенство: $(C^\perp)^r = (V_1 \otimes V_2)^r = V_1^r \otimes V_2^r$. Поэтому $d((C^\perp)^r) = d(V_1^r)d(V_2^r)$, $d(((C^\perp)^r)^\perp) = \min\{d((V_1^r)^\perp), d((V_2^r)^\perp)\}$.

Теорема 11. *Пусть C – $[n+1, k]_q$-код, причем $C = (V_1 \otimes V_2)^\perp$, где V_i – $[n_i, k_i, d_i]_q$-код, $i = 1, 2$, $n = n_1n_2 - 1$. Тогда любые $\min\{d(V_1^\perp), d(V_2^\perp), d((V_1^r)^\perp), d((V_2^r)^\perp)\} - 2$ участников образуют неправомочную коалицию, а любые $n - \min\{d(V_1)d(V_2), d(V_1^r)d(V_2^r)\} + 2$ участников образуют правомочную коалицию.*

Характеристики тензорного произведения рассмотренных кодов, позволяющие по теореме 7 найти мощности неправомочных и правомочных коалиций, приведены в табл. 3.

Таблица 3

Характеристики степеней тензорного произведения

	$C=(V_1\otimes V_2)^\perp$	
	$V_i=\mathrm{GRS}_{n_i,k_i}(\mathbf{x}_i,\mathbf{y}_i)$, $i=1,2$	$V_i=\mathrm{RM}(l_i,m_i)$, $i=1,2$
$d(C)$	$\min\{k_1,k_2\}+1$	$2^{\min\{l_1,l_2\}+1}$
$d(C^\perp)$	$(n_1-k_1+1)\cdot(n_2-k_2+1)$	$2^{m_1-l_1+m_2-l_2}$
$d(((C^\perp)^r)^\perp)$	$\min\{rk_1-r+1,n_1,rk_2-r+1,n_2\}+1$	$2^{\min\{m_1,rl_1,m_2,rl_2\}+1}$
$d((C^\perp)^r)$	$\max\{n_1-(rk_1-r),1\}\max\{n_2-(rk_2-r),1\}$	$2^{m_1-\min\{m_1,rl_1\}+m_2-\min\{m_2,rl_2\}}$

3.4. Конструкция $(u|u+v)$

Еще одной кодовой конструкцией, для которой можно в ряде случаев найти характеристики степеней кода, является конструкция $(u|u+v)$. Для двух кодов C_1 и C_2 одинаковой длины с порождающими матрицами G_1 и G_2, код $C=UV(C_1,C_2)$, соответствующий $(u|u+v)$-конструкции, имеет следующие характеристики [11, 15]:

$$G_C=\begin{pmatrix}G_1 & G_1\\ O & G_2\end{pmatrix},\ H_C=\begin{pmatrix}H_1 & O\\ -H_2 & H_2\end{pmatrix} \tag{10}$$

$$k(C)=k(C_1)+k(C_2), n(C)=2n(C_1), d(C)=\min\{2d(C_1),d(C_2)\}. \tag{11}$$

Из вида (10) проверочной матрицы H вытекает, что $d(C^\perp)=d(UV(C_2^\perp,C_1^\perp))$:

$$d((UV(C_1,C_2))^\perp)=\min\{2d(C_2^\perp),d(C_1^\perp)\}. \tag{12}$$

Так как $C^2=\mathcal{L}(G^2)$, то из вида (10) вытекает, что $C^2=\mathcal{L}(G^2)$, где

$$G^2=\begin{pmatrix}G_1^2 & G_1^2\\ O & G_1\star G_2\\ O & G_2^2\end{pmatrix}.$$

Утверждение 3. *Пусть $r\in\mathbb{N}$, $C=UV(C_1,C_2)$. Тогда*

$$C^r=UV(\hat{C}_1,\hat{C}_2),\ \hat{C}_1=C_1^r,\hat{C}_2=C_2^r+\sum_{\substack{r_1,r_2\in\mathbb{N}:\\ r_1+r_2=r}}C_1^{r_1}\star C_2^{r_2}. \tag{13}$$

Доказательство. Доказывается построением r-й степени матрицы G вида (10). □

Теорема 12. *Пусть C – $[n+1,k]_q$-код, $C=(UV(V_1,V_2))^\perp$, где V_i – $[(n+1)/2,k_i,d_i]_q$-код, $i=1,2$. Тогда любые $\min\{2d(V_2^\perp),d(V_1^\perp),2d(\hat{V}_2^\perp),d(\hat{V}_1^\perp)\}-2$ участников образуют неправомочную коалицию, а любые $n-\min\{2d(V_1),d(V_2),2d(\hat{V}_1),d(\hat{V}_2)\}+2$ – правомочную коалицию.*

Доказательство. Так как $C=(UV(V_1,V_2))^\perp$, то из (11) и (12) следует: $d(C)=\min\{2d(V_2^\perp),d(V_1^\perp)\}$, $d(C^\perp)=\min\{2d(V_1),d(V_2)\}$. Из (12) и (13) получаем:

$$d((C^\perp)^r)=d(UV(\hat{V}_1,\hat{V}_2))=\min\{2d(\hat{V}_1),d(\hat{V}_2)\},\ d(((C^\perp)^r)^\perp)=\min\{2d(\hat{V}_2^\perp),d(\hat{V}_1^\perp)\},$$

где $\hat{V}_1$ и $\hat{V}_2$ имеют вид $\hat{C}_1$ и $\hat{C}_2$ из (13) при $C_1=V_1$, $C_2=V_2$. Следовательно, по теореме 7, любые $\min\{2d(V_2^\perp),d(V_1^\perp),2d(\hat{V}_2^\perp),d(\hat{V}_1^\perp)\}-2$ участников образуют неправомочную коалицию, а любые $n-\min\{2d(V_1),d(V_2),2d(\hat{V}_1),d(\hat{V}_2)\}+2$ – правомочную коалицию.

□

Для двоичных кодов Рида – Маллера и ОРС-кодов следующие утверждения позволяют найти характеристики степеней соответствующих $(u|u+v)$-конструкций.

Утверждение 4. *Пусть* $C_i = \mathrm{GRS}_{n,k_i}(\mathbf{x},\mathbf{y})$, $i=1,2$, $C = UV(C_1,C_2)$. *Тогда*

$$C^r = UV(\mathrm{GRS}_{n,K_1}(\mathbf{x},\mathbf{y}^r), \mathrm{GRS}_{n,K_2}(\mathbf{x},\mathbf{y}^r)), K_1 = \min\{rk_1 - r + 1, n\},$$
$$K_2 = \min\{n, \max\{rk_2 - r, r_1k_1 - r_1 + r_2k_2 - r_2 | r_1, r_2 \in \mathbb{N}, r_1 + r_2 = r\} + 1\}.$$

Доказательство. Рассмотрим представление (13). Из (4) получаем: $k(C_1^r) = k(\mathrm{GRS}_{n,\min\{rk_1-r+1,n\}}(\mathbf{x},\mathbf{y}^r)) = \min\{rk_1 - r + 1, n\}$. Слагаемые в представлении (13) для кода $\hat{C}_2$ имеют вид $\mathrm{GRS}_{n,K}(\mathbf{x},\mathbf{y}^r)$ для некоторого соответствующего этому слагаемому K, что следует из (3). Тогда из (2) получаем, что $\hat{C}_2$ совпадает с максимальным по мощности слагаемым. Откуда получаем выражение для K_2. □

Утверждение 5. *Пусть* $C_i = \mathrm{RM}(m,l_i)$, $i=1,2$, $C = UV(C_1,C_2)$. *Тогда*

$$C^r = UV(\mathrm{RM}(m,L_1), \mathrm{RM}(m,L_2)),\ L_1 = \min\{rl_1, m\},$$
$$L_2 = \min\{\max\{rl_2, r_1l_1 + r_2l_2 | r_1, r_2 \in \mathbb{N}, r_1 + r_2 = r\}, m\}.$$

Доказательство. Рассмотрим (13). Из (7) получаем: $C_1^r = \mathrm{RM}(m, \min\{rl_1, m\}$. Слагаемые в представлении (13) для $\hat{C}_2$ имеют вид $\mathrm{RM}(m,L)$ для соответствующего L, что следует из (7). Тогда $\hat{C}_2 = \mathrm{RM}(m, \min\{\max\{rl_2, r_1l_1 + r_2l_2 | r_1, r_2 \in \mathbb{N}, r_1 + r_2 = r\}, m\})$. □

Формулы, приведенные в табл. 4, позволяют с помощью теоремы 7 найти характеристики построенных ПМЗВ в случае применения конструкции $(u|u+v)$.

Таблица 4

Характеристики степеней $(u|u+v)$-конструкции

	$C = (UV(V_1,V_2))^\perp$	
	$V_i = \mathrm{GRS}_{n,k_i}(\mathbf{x},\mathbf{y})$, $i=1,2$	$V_i = \mathrm{RM}(l_i,m)$, $i=1,2$
$d(C)$	$\min\{2k_2, k_1\} + 1$	$2^{\min\{l_2+2, l_1+1\}}$
$d(C^\perp)$	$\min\{2(n-k_1), n-k_2\} + 1$	$2^{m-\max\{l_1-1, l_2\}}$
$d(((C^\perp)^r)^\perp)$	$\min\{2K_2, K_1\} + 1$	$2^{\min\{L_2+2, L_1+1\}}$
$d((C^\perp)^r)$	$\min\{2(n-K_1), n-K_2\} + 1$	$2^{m-\max\{L_1-1, L_2\}}$

Литература

1. Yao, A. Protocols for Secure Computations / A. Yao // IEEE Computer Society. – 1982. – P. 160–164.
2. Archer, D.W. From Keys to Databases-Real-World Applications of Secure Multi-Party Computation / D.W. Archer, D. Bogdanov, Y. Lindell et al // The Computer Journal. – 2018. – V. 61, № 12. – P. 1749–1771.
3. Garg, S. Outsourcing Private Machine Learning via Lightweight Secure Arithmetic Computation / S. Garg, Z. Ghodsi, C. Hazay et al – URL: https://arxiv.org/abs/1812.01372 (дата обращения 04.05.2022)
4. Jintai Ding. Multivariate Public Key Cryptography / Jintai Ding, Bo-Yin Yang // Post-Quantum Cryptography. – New York: Springer, 2009. – P. 193–241.

5. Bruneau, N. Optimal Side-Channel Attacks for Multivariate Leakages and Multiple Models / N. Bruneau, S. Guilley, A. Heuser // Journal of Cryptographic Engineering. – 2017. – № 7. – P. 331–341.
6. Aesun Park. Side-Channel Attacks on Post-Quantum Signature Schemes Based on Multivariate Quadratic Equations / Aesun Park, Kyung-Ah Shim, Namhun Koo et al // IACR Transactions on Cryptographic Hardware and Embedded Systems. – 2018. – № 3. – P. 500–523.
7. Weijian Li. Fuzzy Matching Template Attacks on Multivariate Cryptography: a Case Study / Weijian Li, Xian Huang, Huimin Zhao et al // Discrete Dynamics in Nature and Society. – 2020. – V. 2020. – P. 1–11.
8. Haibo Yi. On the Importance of Checking Multivariate Public Key Cryptography for Side-Channel Attacks: the Case of enTTS Scheme / Haibo Yi, Weijian Li // The Computer Journal. – 2017. – V. 60, № 8. – P. 1–13.
9. Carlet, C. Polynomial Evaluation and Side Channel Analysis / C. Carlet, E. Prouff // The New Codebreakers. – 2016. – V. 9100. – P. 315–341.
10. Косолапов, Ю.В. Схема разделения секрета типа схемы Блэкли, основанная на пересечении подпространств / Ю.В. Косолапов // Математические вопросы криптографии. – 2017. – Т. 8, № 1. – С. 13–30.
11. MacWilliams, F.J. The Theory of Error-Correcting Codes / F.J. MacWilliams, N.J.A. Sloane. – North Holland, North Holland Publishing, 1977.
12. Randriambololona, H. On Products and Powers of Linear Codes under Componentwise Multiplication / H. Randriambololona. – URL: http://arxiv.org/abs/1312.0022 (дата обращения 04.05.2022)
13. Деундяк, В.М. О некоторых свойствах произведения Шура – Адамара для линейных кодов и их приложениях / В.М. Деундяк, Ю.В. Косолапов // Прикладная дискретная математика. – 2020. – № 50. – С. 72–86.
14. Chizhov, I.V. Effective Attack on the McEliece Cryptosystem Based on Reed-Muller Codes / I.V. Chizhov, M.A. Borodin // Discrete Mathematics and Applications. – 2014. – V. 24, № 5. – P. 273–280.
15. Roumaissa, M. A Novel Niederreiter-Like Cryptosystem Based on the $(u|u+v)$-construction Codes / M. Roumaissa, L.C. Pierre, A. Sedat et al // RAIRO – Theoretical Informatics and Applications. – 2021. – № 55. – P. 1–16.

Юрий Владимирович Косолапов, кандидат технических наук, кафедра алгебры и дискретной математики, Южный федеральный университет (г. Ростов-на-Дону, Российская Федерация), itaim@mail.ru.

Поступила в редакцию 6 мая 2022 г.

MSC 94A60, 68P25 **DOI: 10.14529/mmp230107**

MULTI-PARTY SECURE COMPUTATION OF MULTI-VARIABLE POLYNOMIALS

Yu.V. Kosolapov, Southern Federal University, Rostov-on-Don, Russian Federation, itaim@mail.ru

The goal of decentralizing the calculations performed by participants in information interaction protocols is usually to improve the reliability and security of information

systems. Decentralized computing is based on multi-party secure computing protocols (MSCP), which are usually not universal, but are built for pre-specific functions calculated by participants. In this work, an MSCP is constructed to calculate polynomial values from several variables over a finite field. The constructed protocol is based on linear secret separation schemes, and its characteristics, such as the power of valid and unauthorized coalitions, can be described in terms of the characteristics of linear codes and their Schur-Hadamard degrees. Some codes and code constructs for which such characteristics can be determined analytically are described.

Keywords: secure computation; linear codes.

References

1. Yao A. Protocols for Secure Computations. *IEEE Computer Society*, 1982, pp. 160–164.
2. Archer D.W., Bogdanov D., Lindell Y. et al. From Keys to Databases-Real-World Applications of Secure Multi-Party Computation. *The Computer Journal*, 2018, vol. 61, no. 12, pp. 1749–1771.
3. Garg S., Ghodsi Z., Hazay C. et al. Outsourcing Private Machine Learning via Lightweight Secure Arithmetic Computation. Available at: https://arxiv.org/abs/1812.01372 (accessed 04.05.2022)
4. Jintai Ding, Bo-Yin Yang. Multivariate Public Key Cryptography. *Post-Quantum Cryptography*, New York, Springer, 2009, pp. 193–241.
5. Bruneau N., Guilley S., Heuser A. Optimal Side-Channel Attacks for Multivariate Leakages and Multiple Models. *Journal of Cryptographic Engineering*, 2017, no. 7, pp. 331–341.
6. Aesun Park, Kyung-Ah Shim, Namhun Koo et al. Side-Channel Attacks on Post-Quantum Signature Schemes Based on Multivariate Quadratic Equations. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018, no. 3, pp. 500–523.
7. Weijian Li, Xian Huang, Huimin Zhao et al. Fuzzy Matching Template Attacks on Multivariate Cryptography: A Case Study. *Discrete Dynamics in Nature and Society*, 2020, vol. 2020, pp. 1–11. DOI: 10.1155/2020/9475782
8. Haibo Yi, Weijian Li. On the Importance of Checking Multivariate Public Key Cryptography for Side-Channel Attacks: the Case of enTTS Scheme. *The Computer Journal*, 2017, vol. 60, no. 8, pp. 1–13. DOI: 10.1093/comjnl/bxx010
9. Carlet C., Prouff E. Polynomial Evaluation and Side Channel Analysis. *The New Codebreakers*, 2016, vol. 9100, pp. 315–341.
10. Kosolapov Yu.V. [Blakley Type Secret Sharing Scheme Based on the Intersection of Subspaces]. *Mathematical Aspects of Cryptography*, 2017, vol. 8, no. 1, pp. 13–30. (in Russian)
11. MacWilliams F.J., Sloane N.J.A. The Theory of Error-Correcting Codes. North Holland, North Holland Publishing, 1977.
12. Randriambololon H. *On Products and Powers of Linear Codes under Componentwise Multiplication*. Available at: http://arxiv.org/abs/1312.0022 (accessed 04.05.2022)
13. Deundayk V.M., Kosolapov Yu.V. [On Some Properties of the Schur–Hadamard Product for Linear Codes and their Applications]. *Applied Discrete Mathematics*, 2020, no. 50, pp. 72–86. (in Russian)
14. Chizhov I.V., Borodin M.A. Effective Attack on the McEliece Cryptosystem Based on Reed-Muller Codes. *Discrete Mathematics and Applications*, 2014, vol. 24, no. 5, pp. 273–280.
15. Roumaissa M., Pierre L.C., Sedat A. et al. A Novel Niederreiter-Like Cryptosystem Based on the $(u|u+v)$-construction Codes. *RAIRO – Theoretical Informatics and Applications*, 2021, no. 55, pp. 1–16.

Received May 6, 2022