S. M. Ratseev, Constructions of some secret sharing schemes based on linear codes, *Izv. Saratov Univ. Math. Mech. Inform.*, 2024, Volume 24, Issue 3, 330–341

DOI: 10.18500/1816-9791-2024-24-3-330-341

Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2024. Т. 24, вып. 3. С. 330–341
Izvestiya of Saratov University. Mathematics. Mechanics. Informatics, 2024, vol. 24, iss. 3, pp. 330–341
https://mmi.sgu.ru https://doi.org/10.18500/1816-9791-2024-24-3-330-341, EDN: FDXFXL

Научная статья
УДК 519.725

Конструкции некоторых схем разделения секрета на основе линейных кодов

С. М. Рацеев

Ульяновский государственный университет, Россия, 432017, г. Ульяновск, ул. Льва Толстого, д. 42

Рацеев Сергей Михайлович, доктор физико-математических наук, профессор кафедры информационной безопасности и теории управления, ratseevsm@mail.ru, https://orcid.org/0000-0003-4995-9418, AuthorID: 662208

Аннотация. Среди пороговых схем разделения секрета существуют совершенные схемы со свойством идеальности (например, схема Шамира). Для случая схем разделения секрета с произвольной структурой доступа можно построить совершенную схему для любой структуры доступа (например, схему Ито – Саито – Нишизеки, схему Бенало – Лейхтера), но в общем случае такая схема свойством идеальности обладать уже не будет. В работе для некоторых классов структур доступа приводится конструкция совершенных схем разделения секрета со свойством идеальности на основе линейных кодов. Также приводится конструкция совершенных проверяемых схем разделения секрета для любой структуры доступа, для которой существует линейных код, реализующий эту структуру.

Ключевые слова: криптография, линейный код, схема разделения секрета, структура доступа

Для цитирования: *Рацеев С. М.* Конструкции некоторых схем разделения секрета на основе линейных кодов // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2024. Т. 24, вып. 3. С. 330–341. https://doi.org/10.18500/1816-9791-2024-24-3-330-341, EDN: FDXFXL

Article

Constructions of some secret sharing schemes based on linear codes

S. M. Ratseev

Ulyanovsk State University, 42 Leo Tolstoy St., Ulyanovsk 432017, Russia

Sergey M. Ratseev, ratseevsm@mail.ru, https://orcid.org/0000-0003-4995-9418, AuthorID: 662208

Abstract. There are perfect and ideal threshold secret sharing schemes, for example, Shamir's secret sharing scheme. For the case of general secret sharing schemes with an arbitrary access structure, it is possible to construct a perfect scheme for any access structure (for example, the Ito – Saito – Nishizeki scheme, the Benaloh – Leichter scheme), but in general, such a scheme will not be an ideal secret sharing scheme. In the paper, for some classes of access structures, the construction of perfect and ideal secret sharing schemes based on linear codes is given. We also give a construction of perfect verifiable secret sharing schemes for any access structure for which there is a line code that implements this structure.

Keywords: cryptography, linear code, secret sharing scheme, access structure

For citation: Ratseev S. M. Constructions of some secret sharing schemes based on linear codes. *Izvestiya of Saratov University. Mathematics. Mechanics. Informatics*, 2024, vol. 24, iss. 3, pp. 330–341 (in Russian). https://doi.org/10.18500/1816-9791-2024-24-3-330-341, EDN: FDXFXL

Введение

Одним из направлений исследований схем разделения секрета являются схемы, построенные на основе линейных кодов. Это связано с тем, что схемы разделения секрета на основе линейных кодов очень часто помимо свойства совершенности обладают также свойством идеальности, что является важной характеристикой при практической реализации этих схем. Схему разделения секрета назовем совершенной, если любая правомочная коалиция может восстановить секрет, при этом доли секрета любой неправомочной коалиции не дают никакой информации о секрете (в теоретико-информационном смысле). Схема разделения секрета обладает свойством идеальности, если размер секрета и размеры долей секрета совпадают.

Взаимосвязь между схемами разделения секрета и корректирующими кодами первыми заметили Мак-Элис и Сарвате [1]. Они показали обобщение схемы разделения секрета Шамира с помощью кодов Рида – Соломона. Секретом является одна из компонент информационного вектора, а долями секрета — компоненты кодового вектора. В этом обобщении восстановление секрета можно интерпретировать как декодирование вектора, содержащего стирания (отсутствующие доли некоторых участников). Также в этом обобщении может быть рассмотрена ситуация, когда некоторые участники в процессе восстановления секрета предоставляют заведомо некорректные доли. В этом случае можно применить алгоритм декодирования для случая стираний и ошибок. Ренвалл и Динг обобщили эту конструкцию для любого линейного кода [2]. В этом случае кодирование информационного вектора, содержащего компоненту, равную значению секрета, происходит на основе порождающей матрицы кода, а компоненты кода являются долями секрета. Если линейный код является кодом МДР, то полученная конструкция является пороговой схемой разделения секрета со свойствами идеальности и совершенности. Похожая конструкция приводится в работе Динга с соавт. [3]. Здесь исследуются схемы разделения мультисекретов на основе линейных кодов. В этом случае весь информационный вектор (или его часть) является набором секретов, который при кодировании с помощью порождающей матрицы переходит в (кодовый) вектор, компоненты которого являются долями секрета.

Карнин с соавт. [4] привели конструкцию схем разделения секрета на основе линейных кодов, в которой секрет является частью не информационного вектора, а кодового. В этой конструкции компонента $u_0 = s$ кодового вектора u линейного $[n+1, k]$-кода является секретом, а все остальные компоненты $u_1, \ldots, u_n$ — долями секрета. Если линейный код является кодом МДР, то получается совершенная и идеальная пороговая схема разделения секрета. В работе [5] приводятся конструкции пороговых схем разделения секрета на основе кодов МДР, которые обобщают конструкцию Карнина и др. В этих конструкциях при восстановлении секрета возможно наличие участников с заведомо некорректными долями. В этом случае число собравшихся участников должно быть не менее $2t + k$, где k — порог, t — число участников с некорректными долями.

В работах [6, 7] Месси показал взаимосвязь между монотонной структурой доступа и минимальными векторами дуального кода, у которых первая компонента равна 1. В работе [8] Танг с соавт. привели критерий существования линейного кода, реализующего монотонную структуру доступа для идеальной схемы разделения секрета на основе минимальных векторов дуального кода. В работе [9] приводятся схемы на основе линейных кодов с использованием линейных хэш-функций. Тенту с соавт. в работе [10] построили совершенную и идеальную иерархическую схему разделения секрета на основе кодов МДР.

Более подробную информацию о корректирующих кодах можно найти, например, в [11].

О криптосистемах со свойством совершенности, в частности о схемах разделения секрета, можно найти информацию, например, в [12].

Пусть $P = \{1, 2, \ldots, n\}$ — конечное множество участников разделения секрета (для удобства изложения дальнейшего материала сопоставим участников с их номерами), $\widetilde{P}$ — множество, состоящее из всех возможных непустых подмножеств множества P, R — множество, состоящее из подмножеств участников, которым разрешено восстановление секрета (правомочные коалиции), Z — множество, состоящее из подмножеств участников, которые не могут восстановить секрет (неправомочные коалиции). *Структура доступа* — разбиение $\widetilde{P} = R \cup Z$. Структура доступа называется монотонной, если все надмножества правомочных коалиций также входят в R, т. е. если $X \in R$, $X \subseteq Y \in \widetilde{P}$, то $Y \in R$. Коалицию $X \in R$ называют минимальной правомочной коалицией, если $Y \notin R$ всегда, когда выполнено строгое включение $Y \subset X$. Множество минимальных правомочных коалиций из R обозначается как $R_{\min}$ и называется базисом R. $X \in Z$ называют максимальной неправомочной коалицией, если $Y \in R$ всегда, когда выполнено строгое включение $X \subset Y$. Множество максимальных неправомочных коалиций из Z обозначается как $Z_{\max}$. Заметим, что множество $R_{\min}$ однозначно задает структуру доступа. Аналогично множество $Z_{\max}$ однозначно задает структуру доступа. Если структура доступа задается на основе R или $R_{\min}$, то такую структуру доступа будем обозначать через Γ. Любая (n, t)-пороговая схема разделения секрета — схема разделения секрета с n участниками для структуры доступа, в которой правомочными являются все коалиции, содержащие не менее t участников, а все коалиции с меньшим числом участников — неправомочны.

1. Структуры доступа на основе линейных кодов

В [6, 7] предложен метод построения структур доступа на основе минимальных векторов дуального кода к коду A. Если на основе дуального кода к заданному линейному коду A строится структура доступа, то будем ее обозначать через $\Gamma(A)$. Пусть A — некоторый $[n+1, k, d]$-линейный код над конечным полем $F = GF(q)$ с порождающей матрицей G и проверочной матрицей H, $s \in F$ — секрет. Пусть номера $i_1 = 0, i_2, \ldots, i_k$, где $0 = i_1 < i_2 < \ldots < i_k \leqslant n$, образуют информационную совокупность. Это значит, что в матрице G столбцы с номерами $i_1, i_2, \ldots, i_k$ линейно независимы, поэтому компоненты $u_0, u_{i_2}, \ldots, u_{i_k}$ определяют все компоненты кодового вектора u. Определим $u_0 = s$, а компоненты $u_{i_2}, \ldots, u_{i_k} \in F$ сгенерируем случайным (равновероятным) образом. На основе компонент $u_0, u_{i_2}, \ldots, u_{i_k}$ вычислим кодовый вектор $u \in A$. Компоненты $u_1, u_2, \ldots, u_n$ вектора u будут являться долями секрета.

Пусть $A^{\perp}$ — дуальный $[n+1, n+1-k, d^{\perp}]$-код к коду A. Для кода $A^{\perp}$ матрица H является порождающей матрицей. Будем говорить, что вектор x покрывает вектор y, если для любого индекса $i = 0, 1, \ldots, n$ из $y_i \neq 0$ следует $x_i \neq 0$. Определим понятие минимального кодового вектора кода $A^{\perp}$. Ненулевой вектор $x = (x_0, x_1, \ldots, x_n) \in A^{\perp}$ называется *минимальным* кодовым вектором, если:

1) первая ненулевая компонента (считая слева направо) равна единице;

2) для любого ненулевого $y \in A^{\perp}$, $x \neq y$, у которого первая ненулевая компонента равна 1, вектор x не покрывает вектор y.

Замечание 1. Заметим, что не существует двух различных минимальных кодовых векторов, у которых ненулевые компоненты имеют те же самые индексы. Действительно, пусть x, y — два таких вектора. Тогда ненулевой кодовый вектор $x - y$ имеет меньший вес, нежели вес векторов x и y, причем векторы x и y покрывают вектор $x - y$. Пусть $c \in F$ — значение первой ненулевой компоненты вектора $x - y$. Тогда вектор $z = c^{-1}(x - y)$ является кодовым вектором, у которого первая ненулевая компонента равна 1. Причем $x \neq z$, $y \neq z$, x и y покрывают вектор z. Это противоречит минимальности векторов x и y.

Линейная оболочка, натянутая на множество всех минимальных кодовых векторов, совпадает с кодом $A^{\perp}$. На самом деле имеет место более сильное утверждение.

Предложение 1 ([6]). *Любой неминимальный кодовый вектор y является линейной комбинацией минимальных кодовых векторов, каждый из которых покрывается вектором y. При этом для любого ненулевого кодового вектора y найдется минимальный кодовый вектор x, у которого номер первой ненулевой компоненты (на которой стоит 1) совпадает с номером первой ненулевой компоненты вектора y, причем вектор y покрывает вектор x.*

Для вектора $x = (x_0, x_1, \ldots, x_n)$ обозначим

$$\operatorname{supp}(x) = \{i \mid 0 \leqslant i \leqslant n,\ x_i \neq 0\}.$$

Обозначим через V_0 множество всех минимальных кодовых векторов u кода $A^{\perp}$, у которых $u_0 = 1$:

$$V_0 = \{(1, a_{11}, \ldots, a_{1n}),\ (1, a_{21}, \ldots, a_{2n}), \ldots\}.$$

Множество V_0 не держится в секрете. Определим множество минимальных правомочных коалиций $R_{\min}$ следующим образом. $X \in R_{\min}$ тогда и только тогда, когда для некоторого $x \in V_0$ выполнено $X = \operatorname{supp}(x) \setminus \{0\}$.

Множество всех правомочных коалиций R определяется как множество всех надмножеств коалиций из $R_{\min}$, причем эти правомочные коалиции являются подмножествами в $\{1, 2, \ldots, n\}$:

$$R = \{X \subseteq \{1, 2, \ldots, n\} \mid \exists \widetilde{X} \in R_{\min},\ \widetilde{X} \subseteq X\}.$$

Пусть X — некоторая правомочная коалиция. Для восстановления секрета сначала отыскивается минимальная правомочная коалиция, являющаяся подмножеством в X, а уже по долям секрета минимальной правомочной коалиции восстанавливается секрет s, используя множество V_0. Если минимальная правомочная коалиция соответствует i-му вектору множества V_0, то секрет определяется из равенства $s + a_{i1}u_{i1} + \ldots + a_{in}u_{in} = 0$, где u_{ij} — доли участников минимальной правомочной коалиции. Тем самым показано, что любая правомочная коалиция однозначно восстановит секрет.

Любая неправомочная коалиция восстановить секрет не сможет. Действительно, пусть $u_{i_1}, \ldots, u_{i_m}$ — доли некоторых участников, по которым секрет s можно восстановить. Тогда найдутся такие скаляры $a_{i_1}, \ldots, a_{i_m} \in F$, для которых $s = u_0 = a_{i_1}u_{i_1} + \ldots + a_{i_m}u_{i_m}$. Поэтому из равенства

$$1 \cdot u_0 - a_{i_1} \cdot u_{i_1} - \ldots - a_{i_m} \cdot u_{i_m} = 0$$

следует, что вектор $a = (1, \ldots, -a_{i_1}, \ldots, -a_{i_m}, \ldots)$ принадлежит пространству $A^{\perp}$, где скаляры $a_{i_1}, \ldots, a_{i_m}$ стоят на позициях соответственно $i_1, \ldots, i_m$. Из сказанного выше следует, что вектор a покрывает некоторый вектор из множества V_0. Это значит, что коалиция участников $\{i_1, \ldots, i_m\}$ является правомочной.

Заметим, что, помимо свойства совершенности, данная схема обладает свойством идеальности [6].

2. Структура доступа, связанная с разбиением множества участников

В данном разделе рассмотрим вопрос построения линейных кодов, которые определяют множества минимальных правомочных коалиций в виде декартова произведения подмножеств множества участников, т. е. простой случай, когда $R_{\min} = X_1 \times \ldots \times X_k$. Следующий критерий отражает взаимосвязь множества V_0 с проверочной матрицей G. Через $[G]_i$ будем обозначать i-й столбец матрицы G.

Предложение 2 ([8]). *Пусть $(u_0, u_1, \ldots, u_n) \in A$, где $u_0 = s$, G — порождающая матрица $[n+1, k]$-линейного кода A над полем F. Коалиция участников $X \subseteq \{1, \ldots, n\}$ может восстановить секрет тогда и только тогда, когда столбец $[G]_0$ является линейной комбинацией столбцов $[G]_i$, $i \in X$.*

Пусть $\{1,\dots,n\} = X_1 \cup \dots \cup X_k$ — некоторое разбиение множества $\{1,\dots,n\}$. Построим совершенную идеальную схему разделения секрета на основе кодов, для которой коалиция $X \subseteq \{1,\dots,n\}$ является правомочной тогда и только тогда, когда $X \cap X_i \neq \varnothing$ для любого $i = 1,\dots,k$, т. е. коалиция X содержит хотя бы по одному участнику из каждого множества X_i, $i = 1,\dots,k$. Для этого построим матрицу G размером $k \times (n+1)$ над множеством $\{0,1\}$ следующим образом. Столбец $[G]_0$ состоит из единиц. Элементы первой строки матрицы G с номерами i, $i \in X_1$, равны единице, а остальные элементы (кроме элемента столбца $[G]_0$) равны нулю. Аналогичным образом расставлены элементы в остальных строках. Например, если для любых $i < j$ любой элемент множества X_i строго меньше любого элемента множества X_j, то схематично матрица G примет такой вид:

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 & & & & \dots & & & \\ 1 & & & & 1 & \dots & 1 & \dots & & & \\ \vdots & & & & & & & \ddots & & & \\ 1 & & & & & & & \dots & 1 & \dots & 1 \end{pmatrix}. \tag{1}$$

Предложение 3. *Пусть G — порождающая матрица указанного выше вида для $[n+1,k]$-линейного кода A над полем F. Коалиция $X \subseteq \{1,\dots,n\}$ является правомочной (т. е. может восстановить секрет) тогда и только тогда, когда $X \cap X_i \neq \varnothing$ для любого $i = 1,\dots,n$. Более того, множество минимальных правомочных коалиций является декартовым произведением множеств $X_1,\dots,X_k$: $R_{\min} = X_1 \times \dots \times X_k$.*

Доказательство. Применим критерий из предложения 2. Из вида (1) матрицы G понятно, что если столбец $[G]_0$ является линейной комбинацией некоторых других столбцов матрицы G, то в этой линейной комбинации для любого $i = 1,\dots,k$ должен участвовать хотя бы один столбец $[G]_j$, $j \in X_i$.

Обратно, возьмем по одному элементу $j_i \in X_i$ из каждого множества X_i, $i = 1,\dots,k$. Тогда $[G]_0 = [G]_{j_1} + \dots + [G]_{j_k}$. □

Пусть матрица G имеет вид (1). Обозначим $n_i = |X_i|$, $i = 1,\dots,k$. В этом случае индексы $0, 1, n_1+1, n_2+1, \dots, n_{k-2}+1$ образуют информационную совокупность линейного кода, порожденного матрицей G, так как столбцы матрицы G с данными номерами линейно независимы. Это значит, что компоненты u_0, u_1, u_{n_1+1},..., $u_{n_{k-2}+1}$ однозначно определяют весь кодовый вектор u. Для этого сначала находится решение системы уравнений

$$(x_0, x_1, \dots, x_{k-1})([G]_0, [G]_1, [G]_{n_1+1}, \dots, [G]_{n_{k-2}+1}) = (u_0, u_1, u_{n_1+1}, \dots, u_{n_{k-2}+1})$$

относительно неизвестных x_i. Таким решением будет

$$x_0 = u_1, \quad x_1 = u_{n_1+1}, \dots, x_{k-2} = u_{n_{k-2}+1}, \quad x_{k-1} = u_0 - (u_1 + u_{n_1+1} + \dots + u_{n_{k-2}+1}).$$

Теперь весь кодовый вектор определяется следующим образом:

$$u = xG = (u_0, \underbrace{u_1, \dots, u_1}_{n_1}, \underbrace{u_{n_1+1}, \dots, u_{n_1+1}}_{n_2}, \dots, \underbrace{u_{n_{k-2}+1}, \dots, u_{n_{k-2}+1}}_{n_{k-1}},$$

$$\underbrace{u_0 - (u_1 + u_{n_1+1} + \dots + u_{n_{k-2}+1}), \dots, u_0 - (u_1 + u_{n_1+1} + \dots + u_{n_{k-2}+1})}_{n_k}).$$

Пусть некоторая правомочная коалиция X хочет восстановить секрет s. Пусть X_0 — некоторая минимальная правомочная коалиция, причем $X_0 \subseteq X$. Если $u_{i_1}, \dots, u_{i_k}$ — доли участников коалиции X_0, то $s = u_{i_1} + \dots + u_{i_k}$. При этом доли любой неправомочной коалиции не дадут никакой информации о секрете, так как если в коалиции нет ни одного представителя из некоторого множества X_i, то, варьируя неизвестную долю, можно получить любое значение секрета s из F. Поэтому схема является совершенной. Идеальность схемы очевидна.

3. Построение линейного кода, реализующего структуру доступа

Рассмотрим вопрос о возможности построения линейного кода по заданной структуре доступа. Для этого на основе работы [8] определим матрицы $\mathbb{G}$ и $\mathbb{H}$.

Пусть A — линейный $[n+1,k]$-код над полем F, $X \subseteq \{1,2,\ldots,n\}$. Напомним, что X является правомочной коалицией тогда и только тогда, когда найдется вектор $v \in A^{\perp}$, $v_0 = 1$, для которого $\mathrm{supp}(v) \subseteq X \cup \{0\}$. Это равносильно существованию такого минимального вектора $u \in V_0$, для которого $\mathrm{supp}(u) \subseteq X \cup \{0\}$. Обозначим через $\Gamma(A)$ множество всех минимальных правомочных коалиций, определяемых на основе кода A. Получаем, что X — правомочная коалиция тогда и только тогда, когда X является надмножеством некоторой коалиции из $\Gamma(A)$.

Пусть $\Gamma = \{X_1,\ldots,X_m\}$ — некоторая совокупность непустых подмножеств в $\{1,2,\ldots,n\}$. Будем считать, что ни одно множество из Γ не содержит другое множество из Γ, т. е. $\Gamma = R_{\min}$. Также будем считать, что каждый участник 1, 2,..., n входит хотя бы в одно множество (коалицию) X_j. В этом случае Γ определяет структуру доступа следующим образом: подмножество $X \subseteq \{1,\ldots,n\}$ является правомочной коалицией тогда и только тогда, когда X является надмножеством некоторого множества из Γ. При этом $Y \subseteq \{1,\ldots,n\}$ является неправомочной коалицией тогда и только тогда, когда Y не является надмножеством ни для одного множества из Γ.

Пусть $\Gamma = \{X_1,\ldots,X_m\}$ — некоторая структура доступа (более точно — Γ определяет структуру доступа, но иногда будем использовать такую терминологию), где $X_i \subset \{1,\ldots,n\}$, $i = 1,\ldots,m$. Γ можно представить в виде матрицы

$$\Gamma = \begin{pmatrix} h_{11} & h_{12} & \ldots & h_{1n} \\ h_{21} & h_{22} & \ldots & h_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ h_{m1} & h_{m2} & \ldots & h_{mn} \end{pmatrix},$$

где $h_{ij} \neq 0$ при $j \in X_i$, $h_{ij} = 0$ при $j \notin X_i$, $i = 1,\ldots,m$, $j = 1,\ldots,n$. В этом случае каждая строка матрицы Γ характеризует соответствующее множество X_i. На основе матрицы Γ построим матрицу $\mathbb{H}$:

$$\mathbb{H} = \begin{pmatrix} 1 & h_{11} & h_{12} & \ldots & h_{1n} \\ 1 & h_{21} & h_{22} & \ldots & h_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & h_{m1} & h_{m2} & \ldots & h_{mn} \end{pmatrix}, \qquad (2)$$

т. е. к матрице Γ добавили столбец из единиц, который будет являться столбцом с нулевым номером. У остальных столбцов будут номера $1,2,\ldots,n$, которые соответствуют участникам разделения секрета. Через $(\mathbb{H})_i$ и $[\mathbb{H}]_j$ будем обозначать соответственно i-ю строку и j-й столбец матрицы $\mathbb{H}$. Заметим, что в матрице $\mathbb{H}$ нет нулевых столбцов.

Теорема 1. *Пусть $\Gamma = \{X_1,\ldots,X_m\} = R_{\min}$ — некоторая структура доступа, F — некоторое конечное поле. Составим на основе Γ матрицу H вида (2), в которой всем ненулевым элементам h_{ij} придадим некоторые конкретные значения из F^*. Пусть $A^{\perp}$ — линейная оболочка над F, натянутая на векторы-строки матрицы H. Пусть V_0 — множество минимальных кодовых векторов и кода $A^{\perp}$, у которых $u_0 = 1$. Равенство $\Gamma = \Gamma(A)$ выполнено тогда и только тогда, когда множество V_0 и множество строк матрицы H равны.*

Доказательство. Пусть на основе $\Gamma = \{X_1,\ldots,X_m\} = R_{\min}$ получены матрица H, код $A^{\perp}$, множество V_0.

Если множество V_0 и множество строк матрицы H равны, то $R_{\min} = R_{\min}(A)$. Так как множество минимальных правомочных коалиций полностью определяет структуру доступа, то исходная структура доступа Γ и структура доступа, задаваемая кодом A, равны.

Обратно, пусть $\Gamma = \Gamma(A)$. Из построения кода $A^{\perp}$ понятно, что множество строк матрицы H является подмножеством в V_0. Если бы в V_0 был вектор, которого нет среди строк матрицы H, то, учитывая замечание 1, было бы выполнено строгое включение $\Gamma \subset \Gamma(A)$, что противоречит условию. □

В следующем утверждении приводится критерий неправомочной коалиции.

Предложение 4 ([8]). *Пусть A — линейный $[n+1, k]$-код над конечным полем F. Множество $T \subset \{1, \ldots, n\}$ является неправомочной коалицией тогда и только тогда, когда найдется кодовый вектор $u = (u_0, u_1, \ldots, u_n) \in A$, для которого $u_0 = 1$ и $u_i = 0$ для любого $i \in T$.*

Матрица (2) несет информацию о минимальных правомочных коалициях. На основе предложения 4 определим еще одну матрицу. Пусть $\Gamma = \{X_1, \ldots, X_m\}$. На основе Γ определим $Z_{\max} = \{Y_1, \ldots, Y_l\}$ — множество всех максимальных неправомочных коалиций. Учитывая критерий неправомочной коалиции из предложения 4, определим матрицу

$$\mathbb{G} = \begin{pmatrix} 1 & g_{11} & g_{12} & \ldots & g_{1n} \\ 1 & g_{21} & g_{22} & \ldots & g_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & g_{l1} & g_{l2} & \ldots & g_{ln} \end{pmatrix}, \tag{3}$$

где $g_{ij} = 0$ при $j \in Y_i$, $g_{ij} \neq 0$ при $j \notin Y_i$.

Теорема 2 ([8]). *Для заданной структуры доступа $\Gamma = \{X_1, \ldots, X_m\}$ существует линейный код A над конечным полем F, определяющий структуру доступа $\Gamma = \Gamma(A)$, тогда и только тогда, когда система квадратных уравнений*

$$\mathbb{G}\mathbb{H}^T = O \tag{4}$$

имеет решение над полем F для g_{ij}, $j \notin Y_i$, h_{ij}, $j \in X_i$.

Пример 1. Пусть $\Gamma = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}\} = R_{\min}$. В этом случае $Z_{\max} = \{\{1, 2\}, \{1, 3, 4, 5\}, \{2, 3, 4, 5\}\}$. Найдем линейный код (если он существует), реализующий Γ. Составим матрицы $\mathbb{G}$ и $\mathbb{H}$:

$$\mathbb{G} = \begin{pmatrix} 1 & 0 & 0 & g_{13} & g_{14} & g_{15} \\ 1 & 0 & g_{22} & 0 & 0 & 0 \\ 1 & g_{31} & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \mathbb{H} = \begin{pmatrix} 1 & h_{11} & h_{12} & h_{13} & 0 & 0 \\ 1 & h_{21} & h_{22} & 0 & h_{24} & 0 \\ 1 & h_{31} & h_{32} & 0 & 0 & h_{35} \end{pmatrix},$$

где все элементы g_{ij}, h_{st}, кроме явно выписанных нулей, не равны нулю. Учитывая теорему 2, получаем такую систему уравнений:

$$\begin{cases} 1 + g_{13}h_{13} = 0, \\ 1 + g_{14}h_{24} = 0, \\ 1 + g_{15}h_{35} = 0, \\ 1 + g_{22}h_{12} = 0, \\ 1 + g_{22}h_{22} = 0, \\ 1 + g_{22}h_{32} = 0, \\ 1 + g_{31}h_{11} = 0, \\ 1 + g_{31}h_{21} = 0, \\ 1 + g_{31}h_{31} = 0. \end{cases}$$

Вычитая из 4-го уравнения по очереди 5-е и 6-е уравнения, получаем, что $h_{12} = h_{22} = h_{32} = -g_{22}^{-1}$. Аналогичным образом из первых трех уравнений системы получаем $h_{13} = -g_{13}^{-1}$,

$h_{24} = -g_{14}^{-1}$, $h_{35} = -g_{15}^{-1}$, а из последних трех — $h_{11} = h_{21} = h_{31} = -g_{31}^{-1}$. Поэтому данная система имеет решение над любым полем F.

Возьмем, например, поле $F = GF(2^m)$ для некоторого фиксированного m. Тогда в качестве матриц G и H можно определить

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Пусть A — линейная оболочка над полем F, натянутая на векторы, являющиеся строками матрицы G. Получим $[6, 3]$-линейный код A, причем $\Gamma = \Gamma(A)$.

4. Построение линейных кодов на основе некоторых структур доступа

Пусть $X_0 \subset \{1, 2, \ldots, n\}$ — некоторое подмножество, причем X_0 может быть пустым. Определим на множестве $\{1, 2, \ldots, n\} \setminus X_0$ разбиение вида

$$\{1, 2, \ldots, n\} \setminus X_0 = X_1 \cup X_2 \cup \ldots \cup X_m.$$

Рассмотрим структуру доступа $\Gamma = \{X_0 \cup X_1,\ X_0 \cup X_2, \ldots,\ X_0 \cup X_m\}$. Пусть каждый элемент множества X_i строго меньше каждого элемента множества X_j при $i < j$. Пусть F — некоторое конечное поле. На основе Γ составим матрицу H вида (2), в которой ненулевым элементам придадим значение 1. Тогда схематично матрица H примет такой вид:

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 & \ldots & 1 & & & & \ldots & & & \\ 1 & 1 & \ldots & 1 & & & & 1 & \ldots & 1 & \ldots & & & \\ \vdots & \vdots & \ddots & \vdots & & & & & & & \ddots & & & \\ 1 & 1 & \ldots & 1 & & & & & & & \ldots & 1 & \ldots & 1 \end{pmatrix}. \tag{5}$$

Столбец с номером 0 матрицы H состоит из единиц. Далее следуют $|X_0|$ столбцов, тоже состоящих из единиц. Напомним, что множество X_0 может быть пустым (в отличие от множеств $X_1, \ldots, X_m$). Серия единиц в i-й строке (за исключением первых $|X_0| + 1$ столбцов из единиц) матрицы H соответствует множеству X_i, $i = 1, \ldots, m$. Например, матрица H из примера 1 соответствует случаю $X_0 = \{1, 2\}$, $X_1 = \{3\}$, $X_2 = \{4\}$, $X_3 = \{5\}$.

Из (5) видно, что если для некоторого вектора u, являющегося линейной комбинацией строк матрицы H, выполнено $u_0 = 1$, то вектор u покрывает некоторую строку матрицы H. Поэтому по теореме 1 выполнено $\Gamma = \Gamma(A)$, где $A^{\perp}$ — линейная оболочка над F, натянутая на векторы-строки матрицы H.

Пусть $f(X_i)$ — значение максимального элемента множества X_i, $i = 1, \ldots, m$. Индексы $I = \{0, 1, \ldots, n\} \setminus \{f(X_1), f(X_2), \ldots, f(X_m)\}$ образуют информационную совокупность кода A. Поэтому компонентам u_i, $i \in I$, можно придавать произвольные значения поля F, где $u_0 = s$ — значение секрета. А все остальные компоненты кодового вектора u вычисляются на основе компонент u_i, $i \in I$, по следующим формулам:

$$u_{f(X_i)} = -(S_0 + S_i), \quad i = 1, \ldots, m,$$

где

$$S_0 = u_0 + \sum_{j \in X_0} u_j, \quad S_i = \sum_{j \in X_i \setminus \{f(X_i)\}} u_j, \quad i = 1, \ldots, m.$$

Пусть $u_{i_1}, \ldots, u_{i_r}$ — доли собравшихся участников некоторой минимальной правомочной коалиции. Тогда секрет $s = u_0$ восстанавливается исходя из равенства $u_0 + u_{i_1} + \ldots + u_{i_r} = 0$.

Замечание 2. Если структура доступа задается с помощью множества минимальных правомочных коалиций, состоящих из двух коалиций, то этот случай подпадает под рассматриваемый в этом разделе случай, поскольку

$$\{X_1,\ X_2\} = \{(X_1 \cap X_2) \cup (X_1 \setminus X_2),\quad (X_1 \cap X_2) \cup (X_2 \setminus X_1)\}.$$

Это значит, что для любой структуры доступа, которая задается на основе двух минимальных правомочных коалиций, существует совершенная схема разделения секрета со свойством идеальности.

Пример 2. Пусть $X_0 = \{1, 2, 3\}$, $X_1 = \{4, 5\}$, $X_2 = \{6, 7, 8\}$, $X_3 = \{9, 10\}$,

$$\Gamma = \{X_0 \cup X_1,\ X_0 \cup X_2,\ X_0 \cup X_3\}.$$

В данном случае матрицы H и G примут вид

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & & & & & & \\ 1 & 1 & 1 & 1 & & & 1 & 1 & 1 & & & \\ 1 & 1 & 1 & 1 & & & & & & 1 & 1 & \end{pmatrix},$$

$$G = \begin{pmatrix} -1 & 1 & & & & & & & & & & \\ -1 & & 1 & & & & & & & & & \\ -1 & & & 1 & & & & & & & & \\ 0 & & & & -1 & 1 & & & & & & \\ 0 & & & & 0 & & -1 & 1 & & & & \\ 0 & & & & 0 & & -1 & & 1 & & & \\ -1 & & & & 1 & & 1 & & & 1 & & \\ -1 & & & & 1 & & 1 & & & & 1 & \end{pmatrix},$$

где вне выписанных чисел стоят нули. Пусть A — линейный $[11, 8]$-код над некоторым полем F, порожденный матрицей G. В коде A выберем индексы 0, 1, 2, 3, 4, 6, 7, 9 в качестве информационной совокупности. Тогда кодовый вектор u на основе компонент u_0, u_1, u_2, u_3, u_4, u_6, u_7, u_9 вычисляется следующим образом:

$$u = \Big(u_0 = s,\ u_1,\ u_2,\ u_3,\ u_4,\ u_5 = -(u_0 + u_1 + u_2 + u_3 + u_4),\ u_6,\ u_7,$$
$$u_8 = -(u_0 + u_1 + u_2 + u_3 + u_6 + u_7),\ u_9,\ u_{10} = -(u_0 + u_1 + u_2 + u_3 + u_9)\Big).$$

Компонента u_i передается участнику с номером i, $i = 1, \ldots, 10$.

Предположим, что собрались вместе участники коалиции $X_0 \cup X_3 = \{1, 2, 3, 9, 10\}$. В этом случае секрет $s = u_0$ восстанавливается исходя из равенства $u_0 + u_1 + u_2 + u_3 + u_9 + u_{10} = 0$.

Заметим, что приведенную выше структуру доступа можно обобщить. Пусть Z_0, Y_1,..., Y_p — некоторые попарно пересекающиеся по пустому множеству подмножества в $\{1, \ldots, n\}$. Некоторые из данных множеств могут быть пустыми. Будем считать, что Z_0 является корнем дерева, $Y_1, \ldots, Y_p$ — его непосредственные потомки. Пусть $X_{11}, \ldots, X_{1n_1}$ — непосредственные потомки вершины Y_1. И так далее, $X_{p1}, \ldots, X_{pn_p}$ — непосредственные потомки вершины Y_p. При этом

$$\{1, \ldots, n\} \setminus (Z_0 \cup Y_1 \cup \ldots \cup Y_p) = X_{11} \cup \ldots \cup X_{1n_1} \cup \ldots \cup X_{p1} \cup \ldots \cup X_{pn_p}$$

— разбиение множества (которое стоит в левой части равенства). Рассмотрим структуру доступа

$$\Gamma = \{Z_0 \cup Y_1 \cup X_{11}, \ldots, Z_0 \cup Y_1 \cup X_{1n_1}, \ldots, Z_0 \cup Y_p \cup X_{p1}, \ldots, Z_0 \cup Y_p \cup X_{pn_p}\}.$$

В данном случае секрет $s \in F$ можно разделить следующим образом. Случайно равновероятно генерируются элементы u_i, $i \in I$, кроме $u_0 = s$, где $I = \{0, 1, \ldots, n\} \setminus \{f(X_{11}), \ldots, f(X_{1n_1}), \ldots, f(X_{p1}), \ldots, f(X_{pn_p})\}$. Пусть

$$S_0 = u_0 + \sum_{j \in Z_0} u_j, \quad S_i = \sum_{j \in Y_i} u_j, \ i = 1, \ldots, p,$$

$$S_{ij} = \sum_{k \in X_{ij} \setminus \{f(X_{ij})\}} u_k, \ i = 1, \ldots, p, \ j = 1, \ldots, n_i.$$

Тогда

$$u_{f(X_{ij})} = -(S_0 + S_i + S_{ij}), \ i = 1, \ldots, p, \ j = 1, \ldots, n_i.$$

Пусть собрались вместе участники правомочной коалиции $Z_0 \cup Y_i \cup X_{ij}$. Тогда значение секрета $u_0 = s$ восстанавливается исходя из равенства

$$u_0 + \sum_{j \in Z_0} u_j + \sum_{j \in Y_i} u_j + \sum_{k \in X_{ij} \setminus \{f(X_{ij})\}} u_k + u_{f(X_{ij})} = 0. \tag{6}$$

Пусть T — некоторая неправомочная коалиция. Тогда $(Z_0 \cup Y_i \cup X_{ij}) \not\subseteq T$ для любых $i = 1, \ldots, p, \ j = 1, \ldots, n_i$. Зафиксируем i и j. Тогда либо $Z_0 \not\subseteq T$ при $Z_0 \neq \varnothing$, либо $Y_i \not\subseteq T$ при $Y_i \neq \varnothing$, либо $X_{ij} \not\subseteq T$. Это значит, что в сумме (6) для нахождения u_0 не хватает некоторой компоненты u_s. Если в качестве значения u_s подставлять все значения поля F, то u_0 будет принимать все значения поля F. В силу произвольности индексов i и j получаем, что доли секрета любой неправомочной коалиции не дают никакой информации о секрете. Поэтому полученная схема является совершенной. Свойство идеальности схемы очевидно.

Приведенная структура доступа также легко может быть еще более обобщена.

5. Совершенные проверяемые схемы разделения секрета на основе линейных кодов

Рассмотрим ситуацию, когда участники разделения секрета, включая дилера D, не доверяют друг другу. Пусть p, q — большие простые числа, причем q — делитель числа $p - 1$, g — некоторый элемент мультипликативной группы поля $GF(p)^*$, имеющий порядок q. Теперь линейные коды будут рассматриваться над полем $GF(q)$. Пусть $d \in GF(q)$ — некоторый секретный случайный параметр, $h = g^d \pmod p$. Значения p, q, g, h являются открытыми параметрами.

Пусть Γ — некоторая структура доступа, причем для некоторого линейного $[n+1, k]$-кода над полем $GF(q)$ выполнено $\Gamma = \Gamma(A)$. Для разделения секрета $s \in GF(q)$ дилер находит вектор $x = (x_0, x_1, \ldots, x_{k-1})$, для которого $u = xG = (u_0, u_1, \ldots, u_n)$ (например, на основе компонент $u_{i_1}, u_{i_2}, \ldots, u_{i_k}$, где $i_1 = 0, i_2, \ldots, i_k$ — некоторая информационная совокупность кода A), где $s = u_0$, G — порождающая матрица кода A, генерирует случайным равновероятным образом вектор $y = (y_0, y_1, \ldots, y_{k-1})$ и вычисляет вектор $v = yG = (v_0, v_1, \ldots, v_n)$. В данной схеме i-й участник разделения секрета получит пару значений u_i, v_i, $i = 1, \ldots, n$. Для проверки корректности долей секрета дилер D вычисляет значения

$$r_i = g^{x_i} h^{y_i} \pmod p, \quad i = 0, 1, \ldots, k-1.$$

Эти значения являются открытыми и не хранятся в секрете.

Заметим, что $r_i = g^{x_i + dy_i} \pmod p$. Предположим, что злоумышленник умеет вычислять дискретные логарифмы. Тогда ему известны значения d, $x_i + dy_i$, $i = 0, 1, \ldots, k-1$. Так как все y_i вычислялись случайным равновероятным образом, то известные значения не дадут никакой информации о x_i (в теоретико-информационном смысле), $i = 0, 1, \ldots, k-1$.

Каждый участник может произвести проверку корректности своей доли секрета. Если i-я доля корректна, $i = 1, \ldots, n$, то должно выполняться следующее сравнение:

$$r_0^{g_{1i}} \cdot r_1^{g_{2i}} \cdot \ldots \cdot r_{k-1}^{g_{ki}} \equiv g^{u_i} h^{v_i} \pmod{p},$$

где $g_{1i}, \ldots, g_{ki}$ — элементы i-го столбца матрицы G, которая не держится в секрете.

Модификация проверяемой СРС на эллиптических кривых. Пусть, как и ранее, q — некоторый достаточно большой простой делитель числа $|E_p(a,b)|$, где $E_p(a,b)$ — эллиптическая кривая над полем $GF(p)$ вида $y^2 = x^3 + ax + b \pmod{p}$. Пусть некоторая точка $P \in E_p(a,b)$ имеет порядок q, $d \in GF(q)$ — некоторый секретный параметр, $Q = [d]P$ — открытый параметр (точка эллиптической кривой).

Пусть $u = xG$, $v = yG$, где $s = u_0$ — секрет. В данном случае дилер D вычисляет значения $R_i = [x_i]P + [y_i]Q \in E_p(a,b)$, $i = 0, 1, \ldots, k-1$. Эти значения являются открытыми и не хранятся в секрете. Теперь i-й участник разделения секрета может сделать проверку корректности доли. В этом случае должно выполняться равенство

$$[g_{1i}]R_0 + [g_{2i}]R_1 + \ldots + [g_{ki}]R_{k-1} = [u_i]P + [v_i]Q.$$

Список литературы

1. *McEliece R. J., Sarwate D. V.* On sharing secrets and Reed – Solomon codes // Communications of the ACM. 1981. Vol. 24, iss. 9. P. 583–584. https://doi.org/10.1145/358746.358762
2. *Renvall A., Ding C.* The access structure of some secret-sharing schemes // Information Security and Privacy. ACISP 1996 / ed. by J. Pieprzyk, J. Seberry. Berlin, Heidelberg : Springer, 1996. P. 67–78. (Lecture Notes in Computer Science, vol. 1172). https://doi.org/10.1007/BFb0023288
3. *Ding C., Laihonen T., Renvall A.* Linear multisecret-sharing schemes and error-correcting codes // Journal of Universal Computer Science. 1997. Vol. 3, iss. 9. P. 1023–1036.
4. *Karnin E. D., Greene J. W., Hellman M. E.* On secret sharing systems // IEEE Transactions on Information Theory. 1983. Vol. 29, iss. 1. P. 35–41. https://doi.org/10.1109/TIT.1983.1056621
5. *Pieprzyk J., Zhang X. M.* Ideal threshold schemes from MDS codes // Information Security and Cryptology — ICISC 2002 / ed. by P. J. Lee, C. H. Lim. Berlin, Heidelberg : Springer, 2003. P. 253–263. (Lecture Notes in Computer Science, vol. 2587). https://doi.org/10.1007/3-540-36552-4_18
6. *Massey J. L.* Minimal codewords and secret sharing // Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory. Molle, Sweden, 1993. P. 276–279.
7. *Massey J. L.* Some applications of coding theory in cryptography // Codes and Ciphers: Cryptography and Coding IV / ed. by P. G. Farrell. Essex, England : Formara Ltd., 1995. P. 33–47.
8. *Tang C., Gao S., Zhang C.* The optimal linear secret sharing scheme for any given access structure // Journal of Systems Science and Complexity. 2013. Vol. 26, № 4. P. 634–649. https://doi.org/10.1007/s11424-013-2131-4
9. *Cramer R., Damgård I. B., Döttling N., Fehr S., Spini G.* Linear secret sharing schemes from error correcting codes and universal hash functions // Advances in Cryptology — EUROCRYPT 2015 / ed. by E. Oswald, M. Fischlin. Berlin, Heidelberg : Springer, 2015. P. 313–336. (Lecture Notes in Computer Science, vol. 9057). https://doi.org/10.1007/978-3-662-46803-6_11
10. *Tentu A. N., Paul P., Venkaiah V. Ch.* Ideal and perfect hierarchical secret sharing schemes based on MDS codes // Proceeding of International Conference on Applied and Computational Mathematics. Ankara, Turkey, 2012. P. 256–272.
11. *Рацеев С. М.* Элементы высшей алгебры и теории кодирования : учеб. пособие для вузов. Санкт-Петербург : Лань, 2022. 656 с. EDN: EPVGNW
12. *Рацеев С. М.* Математические методы защиты информации : учеб. пособие для вузов. Санкт-Петербург : Лань, 2022. 544 с. EDN: QZANSJ

References

1. McEliece R. J., Sarwate D. V. On sharing secrets and Reed – Solomon codes. *Communications of the ACM*, 1981, vol. 24, iss. 9, pp. 583–584. https://doi.org/10.1145/358746.358762
2. Renvall A., Ding C. The access structure of some secret-sharing schemes. In: Pieprzyk J., Seberry J. (eds.) *Information Security and Privacy. ACISP 1996*. Lecture Notes in Computer Science, vol. 1172. Berlin, Heidelberg, Springer, 1996, pp. 67–78. https://doi.org/10.1007/BFb0023288

3. Ding C., Laihonen T., Renvall A. Linear multisecret-sharing schemes and error-correcting codes. *Journal of Universal Computer Science*, 1997, vol. 3, iss. 9, pp. 1023–1036.
4. Karnin E. D., Greene J. W., Hellman M. E. On secret sharing systems. *IEEE Transactions on Information Theory*, 1983, vol. 29, iss. 1, pp. 35–41. https://doi.org/10.1109/TIT.1983.1056621
5. Pieprzyk J., Zhang X. M. Ideal threshold schemes from MDS codes. In: Lee P. J., Lim C. H. (eds.) *Information Security and Cryptology — ICISC 2002*. ICISC 2002. Lecture Notes in Computer Science, vol. 2587. Berlin, Heidelberg, Springer, 2003, pp. 253–263. https://doi.org/10.1007/3-540-36552-4_18
6. Massey J. L. Minimal codewords and secret sharing. *Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory*. Molle, Sweden, 1993, pp. 276–279.
7. Massey J. L. Some applications of coding theory in cryptography. In: Farrell P. G. (ed.) *Codes and Ciphers: Cryptography and Coding IV*. Essex, England, Formara Ltd., 1995, pp. 33–47.
8. Tang C., Gao S., Zhang C. The optimal linear secret sharing scheme for any given access structure. *Journal of Systems Science and Complexity*, 2013, vol. 26, iss. 4, pp. 634–649. https://doi.org/10.1007/s11424-013-2131-4
9. Cramer R., Damgård I. B., Döttling N., Fehr S., Spini G. Linear secret sharing schemes from error correcting codes and universal hash functions. In: Oswald E., Fischlin M. (eds.) *Advances in Cryptology — EUROCRYPT 2015*. Lecture Notes in Computer Science, vol. 9057. Berlin, Heidelberg, Springer, 2015, pp. 313–336. https://doi.org/10.1007/978-3-662-46803-6_11
10. Tentu A. N., Paul P., Venkaiah V. Ch. Ideal and perfect hierarchical secret sharing schemes based on MDS codes. *Proceeding of International Conference on Applied and Computational Mathematics*. Ankara, Turkey, 2012, pp. 256–272.
11. Ratseev S. M. *Elementy vysshey algebry i teorii kodirovaniya* [Elements of Higher Algebra and Coding Theory]. St. Petersburg, Lan', 2022. 656 p. (in Russian). EDN: EPVGNW
12. Ratseev S. M. *Matematicheskie metody zashchity informatsii* [Mathematical Methods of Information Security]. St. Petersburg, Lan', 2022. 544 p. (in Russian). EDN: QZANSJ

Поступила в редакцию / Received 24.02.2023
Принята к публикации / Accepted 25.04.2023
Опубликована / Published 30.08.2024