Ю. В. Косолапов

Криптографические протоколы на основе линейных кодов

учебное пособие

ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ЮФУ

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное автономное
образовательное учреждение высшего образования

«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Ю. В. Косолапов

Криптографические протоколы на основе линейных кодов

Учебное пособие

Ростов-на-Дону – Таганрог

Издательство Южного федерального университета

2020

УДК 003.26:512.64(075.8)
ББК 22.18я73
К71

Печатается по решению кафедры алгебры и дискретной математики Института математики, механики и компьютерных наук им. И. И. Воровича Южного федерального университета (протокол № 11 от 08 апреля 2019 г.)

Рецензенты:

доктор физико-математических наук, профессор кафедры алгебры и дискретной математики Института математики, механики и компьютерных наук им. И. И. Воровича Южного федерального университета *В. А. Скороходов*;

кандидат технических наук, доцент, главный инженер ООО «Стэл Юг» *А. В. Балакин*

Косолапов, Ю. В.

К71 Криптографические протоколы на основе линейных кодов : учебное пособие / Ю. В. Косолапов ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020. – 98 с.

ISBN 978-5-9275-3316-9

В учебном пособии рассматриваются вопросы построения примитивных и прикладных криптографических протоколов на основе линейных кодов. Такой подход к построению протоколов обусловлен необходимостью разработки криптографических примитивов, устойчивых в постквантовую эпоху.

Настоящее пособие содержит материал, входящий в учебную программу курса «Криптографические протоколы», изучаемого студентами по направлению подготовки «Прикладная математика и информатика», специализирующимися в области защиты информации.

УДК 003.26:512.64(075.8)
ББК 22.18я73

ISBN 978-5-9275-3316-9

Оглавление

Глава 1

Предварительные сведения

1.1. Введение

Для защиты информации в информационных и автоматизированных системах не всегда достаточно иметь набор средств защиты, таких как криптографические средства, средства разграничения и контроля, средства обнаружения вторжений и т. п. Необходимы четкие правила взаимодействия этих средств, правила их использования участниками взаимодействия (пользователями, процессами, вычислительными устройствами и т. п.). Регламентированная последовательность действий, выполняемых участниками взаимодействия для достижения заранее поставленной цели, обычно называется *протоколом*. Если в протоколе применяются криптографические средства, то такой протокол становится *криптографическим* протоколом. Современные криптографические протоколы строятся на криптографических методах, стойкость которых основана, как правило, на сложности факторизации целых чисел или сложности дискретного логарифмирования в конечной группе. Такие методы не являются стойкими в постквантовую эпоху. Альтернативой таким методам являются методы на основе линейных кодов.

В настоящем пособии рассматриваются примитивные и прикладные криптографические протоколы на основе линейных кодов. В первой главе приводятся необходимые сведения из линейной алгебры, теории информации, теории вероятности, криптографии. С использованием введенных в первой главе понятий во второй главе рассматриваются примитивные криптографические протоколы на линейных кодах. В пособии акцент в основном сделан на протоколах, которые могут применяться в многосторонних защищенных вычислениях. В частности, большая часть пособия посвящена протоколам разделения секрета (главы 3 и 4).

1.2. Матрицы и линейные операторы

Нам понадобятся понятия линейного оператора и его матрицы. Приведем соответствующие определения из [2].

Определение 1. *Оператор* $\mathcal{A}\colon V \to W$, *отображающий пространство* $\mathbb{K}^m$ *в пространство* $\mathbb{K}^n$, *называется линейным, если для любых* $\mathbf{x}, \mathbf{y} \in \mathbb{K}^m$ *и любого* $\alpha \in \mathbb{K}$

$$\mathcal{A}(\mathbf{x}+\mathbf{y}) = \mathcal{A}\mathbf{x} + \mathcal{A}\mathbf{y},\ \mathcal{A}(\alpha\mathbf{x}) = \alpha\mathcal{A}(\mathbf{x}).$$

Определение 2. *Пусть* $\mathcal{A}\colon V \to W$ *— линейный оператор,* $\mathbf{e}_1,\ldots,\mathbf{e}_n$ *и* $\mathbf{g}_1,\ldots,\mathbf{g}_m$ *— зафиксированные базисы в пространствах* V *и* W, *при этом*

$$\begin{aligned}\mathbf{g}_1 &= a_{1,1}\mathbf{e}_1 + \cdots + a_{1,n}\mathbf{e}_n\\ &\ldots\\ \mathbf{g}_m &= a_{m,1}\mathbf{e}_1 + \cdots + a_{m,n}\mathbf{e}_n.\end{aligned}$$

Матрица $A = (a_{i,j})_{i\in[m],\,j\in[n]}$ *называется матрицей оператора* $\mathcal{A}$.

Лемма 1. *Пусть* M *–* $(d\times e)$*-матрица линейного оператора, действующего из* $\mathbb{F}_q^e$ *в* $\mathbb{F}_q^d$. *Если* $(1,0,\ldots,0) \notin \operatorname{im}(M^T)$, *то в ядре* $\ker(M)$ *найдется такой вектор* $\mathbf{x} = (x_1,\ldots,x_e)$, *что* $x_1 \neq 0$.

Доказательство. Предположим, что в $\ker(M)$ все векторы такие, что их первая координата равна 0. Из определения ортогонального дополнения (см., например, [2, с. 233]) получаем

$$(\ker(M))^{\perp} = \{\mathbf{y} \in \mathbb{F}_q^e | \forall \mathbf{x} \in \ker(M)\colon (\mathbf{y},\mathbf{x}) = 0\}.$$

Из условия леммы вытекает, что $(1,0,\ldots,0) \in (\ker(M))^{\perp}$. Так как для любого линейного оператора выполняется равенство

$$\ker(M) = (\operatorname{im}(M^T))^{\perp},$$

то получаем

$$(1,0,\ldots,0) \in \operatorname{im}(M^T),$$

что приводит к противоречию. □

Лемма 2. *Пусть* $\mathbf{v}_1 = (v_{11},\ldots,v_{1n}), \mathbf{v}_2 = (v_{21},\ldots,v_{2n}) \in \mathbb{F}_q^n$. *Тогда*

$$\mathcal{L}(\mathbf{v}_1) \otimes \mathcal{L}(\mathbf{v}_2) = \mathcal{L}(\mathbf{v}_1 \otimes \mathbf{v}_2).$$

Доказательство. Очевидно, что

$$\mathcal{L}(\mathbf{v}_1 \otimes \mathbf{v}_2) \subseteq \mathcal{L}(\mathbf{v}_1) \otimes \mathcal{L}(\mathbf{v}_2).$$

Покажем, что каждый вектор из $\mathcal{L}(\mathbf{v}_1) \otimes \mathcal{L}(\mathbf{v}_2)$ содержится в $\mathcal{L}(\mathbf{v}_1 \otimes \mathbf{v}_2)$. Пусть $\mathbf{c} \in \mathcal{L}(\mathbf{v}_1) \otimes \mathcal{L}(\mathbf{v}_2)$. Тогда этот вектор имеет вид

$$\mathbf{c} = (a_1\mathbf{v}_1) \otimes (a_2\mathbf{v}_2)$$

для некоторых $a_1, a_2 \in \mathbb{F}_q$. Из определения тензорного произведения векторов получаем

$$\begin{aligned}(a_1\mathbf{v}_1) \otimes (a_2\mathbf{v}_2) = \\ &= (a_1v_{11}a_2v_{21}, \ldots, a_1v_{11}a_2v_{2n}, \ldots, a_1v_{1n}a_2v_{21}, \ldots, a_1v_{1n}a_2v_{2n}) = \\ &= a_1a_2(v_{11}v_{21}, \ldots, v_{11}v_{2n}, \ldots, v_{1n}v_{21}, \ldots, v_{1n}v_{2n}) = \\ &= a_1a_2(\mathbf{v}_1 \otimes \mathbf{v}_2) \in \mathcal{L}(\mathbf{v}_1 \otimes \mathbf{v}_2).\end{aligned}$$

Откуда получаем доказываемое утверждение. □

Определение 3. *Квадратная $(l \times l)$-матрица $A = (a_{i,j})$ называется симметричной, если $a_{i,j} = a_{j,i}$ для всех $i, j \in [n]$.*

Упражнение 1. *Покажите, что для симметричной матрицы A выполняется равенство $A = A^T$.*

Упражнение 2. *Пусть $\mathbf{a} = (a_1, \ldots, a_e)$. Покажите, что матрица*

$$A = \begin{pmatrix} a_1\mathbf{a} \\ a_2\mathbf{a} \\ \ldots \\ a_e\mathbf{a} \end{pmatrix}$$

является симметричной.

Очевидно, что если A и B — симметричные $(e \times e)$-матрицы, то матрица $\alpha A + \beta B$ является симметричной для любых элементов кольца, над которым определены эти матрицы.

1.3. Криптографические хеш-функции

Определение 4. *Функция h: $\{0,1\}^* \to \{0,1\}^k$, отображающая строку битов произвольной длины в строку битов фиксированной длины k, называется **хеш**-функцией. Функция h называется **криптографической**,*

если значение $h(\mathbf{x})$ *для любой строки* $\mathbf{x} \in \{0,1\}^*$ *может быть вычислено за полиномиальное число операций от длины строки* $\mathbf{x}$ *и при этом выполняются следующие свойства:*

- ***устойчивость к нахождению прообраза****: для заданной строки* $\mathbf{y} \in \{0,1\}^k$ *вычислительно сложно найти* $\mathbf{x} \in \{0,1\}^*$, *что* $h(\mathbf{x}) = \mathbf{y}$;
- ***устойчивость к нахождению второго прообраза*** *(слабая устойчивость к коллизиям): для заданной строки* $\mathbf{x} \in \{0,1\}^*$ *вычислительно сложно найти такую строку* $\mathbf{x}' \in \{0,1\}^*$, $\mathbf{x}' \neq \mathbf{x}$, *что* $h(\mathbf{x}) = h(\mathbf{x}')$;
- ***устойчивость к коллизиям*** *(сильная устойчивость к коллизиям): вычислительно сложно найти такие разные строки* $\mathbf{x}, \mathbf{x}' \in \{0,1\}^*$, *что* $h(\mathbf{x}) = h(\mathbf{x}')$.

Упражнение 3. *Покажите, что слабая устойчивость к коллизиям следует из сильной устойчивости к коллизиям.*

1.4. Элементы теории информации

Рассмотрим дискретную случайную величину X, принимающую значения из конечного множества $\mathcal{X}$, $p(x) = \mathtt{Pr}\{X = x\}$ – априорная вероятность появления значения x этой случайной величины. Набор

$$(p(x))_{x \in \mathcal{X}}$$

называется распределением вероятностей случайной величины X.

Определение 5. *Энтропией (по Шеннону) случайной величины* X *называется величина:*

$$\mathtt{H}(X) = -\sum_{x \in \mathcal{X}} p(x) \log_2 p(x).$$

Определение 6. *Пусть* X, Y *— дискретные случайные величины с множествами значений* $\mathcal{X}$, $\mathcal{Y}$ *и распределениями вероятностей* $(p(x))_{x \in \mathcal{X}}$, $(p(y))_{y \in \mathcal{Y}}$ *соответственно. Условной энтропией случайной величины* X *после* Y *называется величина:*

$$\mathtt{H}(X|Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x,y) \log_2 p(x|y),$$

а взаимной информацией называется величина:

$$\mathtt{I}(X;Y) = \mathtt{H}(X) - \mathtt{H}(X|Y) = \mathtt{H}(Y) - \mathtt{H}(Y|X) = \mathtt{I}(Y;X).$$

Для случайных величин X и Y справедливы следующие свойства:

- $0 \leqslant \mathtt{H}(X) \leqslant \log_2 |\mathcal{X}|$;
- $0 \leqslant \mathtt{I}(X;Y) \leqslant \min\{\log_2 |\mathcal{X}|, \log_2 |\mathcal{Y}|\}$;
- $\mathtt{H}(X) = \log_2 |\mathcal{X}|$, если X – равновероятная случайная величина;
- если X и Y – независимые, то $\mathtt{H}(X|Y) = \mathtt{H}(X)$ ($\mathtt{H}(Y|X) = \mathtt{H}(Y)$) и $\mathtt{I}(Y;X) = \mathtt{I}(X;Y) = 0$.

1.5. Линейные коды

Приведем необходимые сведения о линейных кодах.

Определение 7. *Линейным $[n,k,d]_q$-кодом C называется подпространство эффективной длины n и размерности k линейного пространства $\mathbb{F}_q^n$, такое, что*

$$\min_{\mathbf{c}\in C\setminus\{\mathbf{0}\}}\{\mathrm{wt}(\mathbf{c})\} = d, \quad |\cup_{\mathbf{c}\in C}\mathrm{supp}(\mathbf{c})| = n.$$

Напомним, что эффективной длиной кода C называется мощность множества $\{\cup_{\mathbf{c}\in C}\mathrm{supp}(\mathbf{c})\}$. В случае, когда кодовое расстояние d неизвестно или не используется в контексте, то код C называется $[n,k]_q$-кодом. Элементы кода будем называть кодовыми векторами или кодовыми словами. Матрица, строками которой являются все кодовые слова кода C, называется кодовой матрицей.

Упражнение 4. *Сколько строк и столбцов в кодовой матрице линейного $[n,k]_q$-кода?*

Определение 8. *Порождающей матрицей $[n,k]_q$-кода C называется $(k\times n)$-матрица G_C такая, что*

$$C = \{\mathbf{m}G_C\colon \mathbf{m}\in\mathbb{F}_q^k\} = \mathcal{L}(G_C). \tag{1.1}$$

Из (1.1) следует, что если G_C — порождающая матрица, то для любой невырожденной $(k\times k)$-матрицы S матрица SG_C также является порождающей.

Так как для $[n,k]_q$-кода C порождающая матрица G_C имеет ранг k, то среди столбцов этой матрицы найдутся k линейно независимых столбцов.

Определение 9. *Пусть C – линейный $[n,k]_q$-код. Множество номеров координат τ, $|\tau| = k$, такое, что $\mathrm{rank}(G_C|_\tau) = k$, называется информационной совокупностью.*

Число всех информационных совокупностей для $[n,k]_q$-кода C не превышает $\binom{n}{k}$.

Упражнение 5. *Покажите, что если τ — информационная совокупность кода $[n,k]_q$-кода, то для всех порождающих матриц этого кода выполняется равенство* $\operatorname{rank}(G_C|\tau) = k$.

Определение 10. *Если τ — информационная совокупность, то порождающая матрица вида*

$$(G_C|_\tau)^{-1} G_C$$

называется порождающей матрицей в систематическом виде.

Определение 11. *Проверочной матрицей $[n,k]_q$-кода C называется такая $(n-k \times n)$-матрица H_C полного ранга, что*

$$H_C G_C^T = O. \tag{1.2}$$

Из равенства (1.2) вытекает, что линейный $[n,k]_q$-код C может быть определен с помощью проверочной матрицы:

$$C = \{\mathbf{c} \in \mathbb{F}_q^n \colon H_C \mathbf{c}^T = \mathbf{0}^T (\in \mathbb{F}_q^{n-k})\}. \tag{1.3}$$

Определение 12. *Пусть C – линейный $[n,k]_q$-код. Подпространство пространства $\mathbb{F}_q^n$, порожденное строками матрицы H_C, называется кодом, дуальным к коду C:*

$$C^\perp = \mathcal{L}(H_C) = \{\mathbf{c}' \in \mathbb{F}_q^n \colon \forall \mathbf{c} \in C \ \ (\mathbf{c}, \mathbf{c}') = 0\}.$$

Для этого кода используется обозначение $C^\perp$.

Теорема 1. *В проверочной матрице H_C линейного $[n,k,d]_q$-кода C набор из любых $d-1$ столбцов является линейно независимым.*

Доказательство. Предположим, что существует линейно зависимый набор столбцов

$$H_C|_{i_1}, \ldots, H_C|_{i_{d-1}}.$$

Следовательно, существует такой ненулевой вектор $\mathbf{z} (\in \mathbb{F}_q^n)$ веса не более $d-1$, что

$$z_{i_1} H_C|_{i_1} + \cdots + H_C|_{i_{d-1}} z_{i_{d-1}} = \mathbf{0}^T (\in \mathbb{F}_q^{n-k}).$$

Иначе это равенство можно переписать в следующем виде:

$$H_C \mathbf{z}^T = \mathbf{0}^T (\in \mathbb{F}_q^{n-k}).$$

Учитывая (1.3), получаем, что $\mathbf{z} \in C$. Однако это противоречит тому, что код C имеет минимальное расстояние d, в то время как $\operatorname{wt}(\mathbf{z}) \leqslant d-1$. $\square$

Учебное издание

КОСОЛАПОВ Юрий Владимирович

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ НА ОСНОВЕ ЛИНЕЙНЫХ КОДОВ

Редактор *Н. Д. Никанорова*
Корректор *Н. Д. Никанорова*
Компьютерная верстка *Ю. В. Косолапов*