ISSN 1561-8323 (Print)
ISSN 2524-2431 (Online)

ИНФОРМАТИКА

INFORMATICS

УДК 004.9, 004.94, 004.56
https://doi.org/10.29235/1561-8323-2019-63-6-662-671

Поступило в редакцию 17.04.2019
Received 17.04.2019

Академик А. Ф. Чернявский, А. А. Коляда, А. О. Мартинов, С. Ю. Протасеня

Институт прикладных физических проблем имени А. Н. Севченко Белорусского государственного университета, Минск, Республика Беларусь

ПРОБЛЕМА КОРРЕКТНОСТИ ПОРОГОВОГО МЕТОДА МОДУЛЯРНОГО РАЗДЕЛЕНИЯ СЕКРЕТА С МАСКИРУЮЩИМ ПРЕОБРАЗОВАНИЕМ

Аннотация. Сформулированы принципы построения пороговых криптосхем разделения секрета, базирующихся на модулярном кодировании и линейной маскирующей функции с аддитивной вариационной компонентой псевдослучайного типа. Главное внимание уделено проблеме корректности схем рассматриваемого класса в рамках принятой модели. Для пороговых криптосхем модулярного разделения секрета получено необходимое и достаточное условие равноостаточности по модулю кольца принадлежности секрета-оригинала значений функции маскирования и отвечающих им элементов диапазонов, определяемых наборами оснований числом, меньшим порогового значения. На базе установленного условия разработан метод корректной реализации порогового принципа разделения секретной информации. Предложенный подход к решению исследуемой проблемы демонстрируется на конкретных числовых примерах.

Ключевые слова: модулярное разделение секрета, пороговая схема разделения секрета, модулярная система счисления, маскирующая функция, проблема корректности порогового метода, критичные значения псевдослучайного параметра

Для цитирования: Проблема корректности порогового метода модулярного разделения секрета с маскирующим преобразованием / А. Ф. Чернявский [и др.] // Докл. Нац. акад. наук Беларуси. – 2019. – Т. 63, № 6. – С. 662–671. https://doi.org/10.29235/1561-8323-2019-63-6-662-671

Academician Alexander F. Chernyavsky, Andrey A. Kolyada, Anton O. Martinov, Stella Yu. Protasenia

Institute of Applied Physical Problems named after A. N. Sevchenko of the Belarusian State University, Minsk, Republic of Belarus

CORRECTNESS PROBLEM OF THE THRESHOLD METHOD OF MODULAR SHARING OF SECRETS WITH MASKING TRANSFORMATION

Abstract. The article formulates the principles of constructing threshold cryptographic schemes for secret sharing based on a modular coding and a linear masking function with an additive variational component of pseudo-random type. The main attention is paid to the correctness problem of schemes of the considered class within the limits of the accepted model. The congruent condition in the module of the secret-original ring of the masking function values in full and partial modular number systems is obtained. On the basis of the above-said, the method of correct implementation of the threshold principle of secret information sharing is developed. The proposed approach to solving the problem under study is demonstrated by specific numerical examples.

Keywords: modular secret sharing, threshold secret sharing scheme, modular number system, masking function, problem of the correctness of the threshold method, critical values of a pseudo-random parameter

For citation: Chernyavsky A. F., Kolyada A. A., Martinov A. O., Protasenia S. Yu. Correctness problem of the threshold method of modular sharing of secrets with masking transformation. *Doklady Natsional'noi akademii nauk Belarusi = Doklady of the National Academy of Sciences of Belarus*, 2019, vol. 63, no. 6, pp. 662–671 (in Russian). https://doi.org/10.29235/1561-8323-2019-63-6-662-671

Введение. Неотъемлемой составляющей современного процесса развития распределенных компьютерных и инфокоммуникационных систем является обеспечение информационной безопасности при хранении, обработке и передаче данных [1–3]. Эффективное решение обозначенной задачи дает так называемая технология активной безопасности, предусматривающая периодическое обновление криптографических ключей, а также их пространственное разделение. На практике разделение секретной информации обычно осуществляется в рамках пороговых схем [1–6]. Реализуемое пороговой (t, n)-системой решающее правило обеспечивает разделение секрета (криптографического ключа) n абонентами с возможностью восстановления его по компонентам, принадлежащим любым l участникам сеанса связи ($2 \le t \le l \le n$), причем группы абонентов числом k меньше порогового значения t реконструировать искомый секрет по соответствующим компонентам не могут.

Перспективный инструментарий для построения пороговых криптосхем разделения секрета представляет собой арифметика модулярных систем счисления (МСС) [1–3; 5; 6]. Модулярное кодирование служит простым средством декомпозиции (разделения) секрета на составные части и позволяет минимизировать временные и аппаратурные затраты при оперировании в диапазонах больших чисел. В криптографических приложениях фактор производительности занимает центральное место. В случае пороговых систем разделения секретной информации особенно жесткие требования к скоростным характеристикам предъявляют, в частности, схемы пролонгированной безопасности со сменой секрета по принципу «блуждающих ключей» [2] с использованием операций возведения в степень по большим модулям и дискретного логарифмирования. Трудоемкими являются также процедуры восстановления ключа-оригинала по частичным секретам, принадлежащим тем или иным группам абонентов. Таким образом, применение модулярной арифметики (МА) для решения проблем построения криптосистем рассматриваемого класса имеет особую важность.

Наряду с разработками, нацеленными на оптимизацию базового компьютерно-арифметического инструментария, актуальными представляются также исследования по обеспечению корректности порогового метода модулярного разделения секрета. Преимущественно именно этой проблеме посвящено настоящее сообщение.

Пороговый принцип модулярного разделения секрета.

Введем обозначения:

$\lfloor a \rfloor$ и $\lceil a \rceil$ – наибольшее и наименьшее целые числа (ЦЧ) соответственно не большее и не меньшее вещественной величины a;

$\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$ – множество наименьших неотрицательных вычетов по натуральному модулю m;

$|a|_m = A(\mathrm{mod}\ m)$ – элемент множества $\mathbf{Z}_m$, сравнимый с ЦЧ A по модулю m;

$|A / B|_m$ – элемент χ множества $\mathbf{Z}_m$, удовлетворяющий сравнению $B\chi \equiv A(\mathrm{mod}\ m)$ (A и B – ЦЧ, $|B|_m \ne 0$);

$(\chi_1, \chi_2, \ldots, \chi_s) = (|X|_{m_1}, |X|_{m_2}, ..., |X|_{m_s})$ – представление ЦЧ X (модулярный код) в МСС с основаниями $m_1, m_2, \ldots, m_s$, составляющими ее базис $\{m_1, m_2, \ldots, m_s\}$ ($s > 1$).

Пусть $p_1, p_2, \ldots, p_n$ – упорядоченные по возрастанию попарно простые большие натуральные числа ($n > 1$); $P_i = \prod_{s=1}^{i} p_s \ \ (i = \overline{1, n})$; $\_P_j = \prod_{s=0}^{i-j} p_{n-s} = P_n / P_{n-j}$ $(j = \overline{1, n})$;

$\mathbf{P} = \{p_1, p_2, \ldots, p_n\}$;

$\mathbf{P}(i_1, i_2, \ldots, i_l) = \{p_{i_1}, p_{i_2}, \ldots, p_{i_l}\}$ $(1 \le i_1 < i_2 < ... < i_l \le n;\ t \le l \le n)$;

$\mathbf{P}(j_1, j_2, \ldots, j_k) = \{p_{j_1}, p_{j_2}, \ldots, p_{j_k}\}$ $(1 \le j_1 < j_2 < ... < j_k \le n;\ 2 \le k < t)$;

p – большое натуральное число, взаимно простое с $p_1, p_2, \ldots, p_n$. Построение модулярной пороговой (t, n)-схемы разделения секрета с базисом $\mathbf{P}$, которая рассчитана на полное число n и пороговое число t разделяющих секрет сторон (абонентов), осуществляется в рамках следующих определяющих условий.

А. Исходный секрет, разделяемый n сторонами, представляет собой целое число $S \in \mathbf{Z}_p$.

Б. Секрет S разделяется путем его модулярной декомпозиции, т. е. по правилу $\sigma_i = |S|_{p_i} \quad (i = \overline{1, n})$. При этом i-я сторона имеет часть σ_i секрета S.

В. Над S выполняется маскирующее преобразование

$$\widetilde{S} = S + Cp, \tag{1}$$

где C – псевдослучайная целочисленная величина и результат маскирования подвергается модулярной декомпозиции: $\widetilde{\sigma}_i = \left|\widetilde{S}\right|_{p_i} = \left|\sigma_i + \left|Cp\right|_{p_i}\right|_{p_i}$ $(i = \overline{1, n})$.

Цифры модулярного кода $(\widetilde{\sigma}_1, \widetilde{\sigma}_2, \ldots \widetilde{\sigma}_n)$ рассматриваются как частичные маскирующие секреты, принадлежащие соответствующим абонентам.

Г. Любые t абонентов могут восстановить секрет S по принадлежащим им маскирующим частичным секретам. Но никакая группа абонентов числом меньше t сделать этого не может.

Ключевым аспектом применяемого подхода к реализации перечисленных основополагающих принципов порогового разделения секретной информации является обеспечение непересекаемости множеств (диапазонов) изменения ЦЧ $\widetilde{S}(\mathrm{mod}\prod_{j=1}^{l} p_{ij})$ и $\widetilde{S}(\mathrm{mod}\prod_{i=1}^{k} p_{ji})$, имеющих в МСС с базисами $\mathbf{P}(i_1, i_2, \ldots, i_l)$ $(t \le l \le n)$ и $\mathbf{P}(j_1, j_2, \ldots, j_k)$ $(2 \le k < t)$ соответственно коды $(\widetilde{\sigma}_{i1}, \widetilde{\sigma}_{i2}, \ldots \widetilde{\sigma}_{il}$ и $\widetilde{\sigma}_{j1}, \widetilde{\sigma}_{j2}, \ldots \widetilde{\sigma}_{jk})$.

Справедлива следующая теорема.

Т е о р е м а 1. *Пусть основания базиса* $\mathbf{P} = \{p_1, p_2, \ldots, p_n\}$ *модулярной* (t, n)*-схемы разделения секрета* $S \in \mathbf{Z}_p$ *упорядочены по возрастанию и взаимно просты с* p. *Для того чтобы диапазоны* $\{0, 1, \ldots, \prod_{i=1}^{k} p_{ji} - 1\}$ *изменения вычетов* $\widetilde{S}(\mathrm{mod}\prod_{i=1}^{k} p_{ji}) = (\widetilde{\sigma}_{j1}, \widetilde{\sigma}_{j2}, \ldots \widetilde{\sigma}_{jk})$ *в МСС с базисами* $\mathbf{P}(j_1, j_2, \ldots, j_k)$ $(2 \le k < t)$ *не пересекались с множеством* $\widetilde{S} = \{\widetilde{S}_{\text{нп}}, \widetilde{S}_{\text{нп}} + 1, \ldots, \widetilde{S}_{\text{вп}}\}$ *значений маскирующего секрета* $\widetilde{S}$ (*результата маскирования* S), *имеющего в МСС с базисами* $\mathbf{P}(i_1, i_2, \ldots, i_l)$ $(t \le l \le n)$ *коды*, *достаточно выполнения условия* $\widetilde{S}_{\text{нп}} = \_P_{t-1}, \widetilde{S}_{\text{вп}} = P_t - 1$, т. е.

$$\widetilde{S} \in \widetilde{\mathbf{S}} = \{\_P_{t-1}, \_P_{t-1} + 1, \ldots, P_t - 1\}.$$

Диапазоны $\{0, 1, \ldots, \prod_{j=1}^{l} p_{ij} - 1\}$ всех МСС с базисом $\mathbf{P}(i_1, i_2, \ldots, i_l)$ включают фигурирующее в теореме 1 множество $\widetilde{\mathbf{S}}$, вследствие чего его правомерно квалифицировать как диапазон модулярной пороговой (t, n)-криптосхемы разделения секрета.

Теорема 1 остается в силе на любых диапазонах $\widetilde{\mathbf{S}} \subseteq \{\_P_{t-1}, \_P_{t-1} + 1, \ldots, P_t - 1\}$. Семейство таких диапазонов можно описать в виде

$$\widetilde{\mathbf{S}} = \{\widetilde{S}_{\text{нп}}, \widetilde{S}_{\text{нп}} + 1, \ldots, \widetilde{S}_{\text{вп}}\} = \{\lceil \_P_{t-1} pq \rceil, \lceil \_P_{t-1} pq \rceil + 1, \ldots, \lfloor \_qP_t \rfloor - 1\} \quad (q \ge p_{-1};\ 0 < q \le 1). \tag{2}$$

Как следует из (1), рабочий диапазон $\widetilde{\mathbf{S}}$ пороговой криптосхемы, принадлежащий семейству (2), порождается значениями псевдослучайного параметра C из множества

$$\mathbf{C} = \{C_{\text{нп}}, C_{\text{нп}} + 1, \ldots, C_{\text{вп}}\} = \left\{\left\lfloor \frac{\widetilde{S}_{\text{нп}}}{p} \right\rfloor, \left\lfloor \frac{\widetilde{S}_{\text{нп}}}{p} \right\rfloor + 1, \ldots, \left\lfloor \frac{\widetilde{S}_{\text{вп}}}{p} \right\rfloor\right\}. \tag{3}$$

Проблема корректности порогового метода модулярного разделения секрета. Общая формула для восстановления секрета S по $\widetilde{S}$ вытекает непосредственно из (1) и имеет вид

$$S = \left|\widetilde{S}\right|_p. \tag{4}$$

В МСС с базисами $\mathbf{P}(i_1, i_2, \ldots, i_l)$ $(t \le l \le n)$ и диапазонами $\{0, 1, \ldots, \prod_{j=1}^{l} p_{ij} - 1\}$, содержащими множество всех маскирующих секретов $\widetilde{S}$ (см. теорему 1), преобразование $\widetilde{S} \to S$ осуществляется корректно. Найдем ограничение на область изменения $\widetilde{S}$, исключающее возможность восстановления S по $\widetilde{S}(\mathrm{mod}\prod_{i=1}^{k} p_{ji}) = (\widetilde{\sigma}_{j1}, \widetilde{\sigma}_{j2}, \ldots \widetilde{\sigma}_{jk})$ любыми k абонентами $(2 \le k < t)$, за которыми закреплены модули $p_{j1}, p_{j2}, \ldots, p_{jk}$. Справедлива следующая теорема.

Т е о р е м а 2. *Маскирующий (модифицированный) секрет* $\widetilde{S}$ *и вычет* $\widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i})$ *являются равноостаточными по модулю p, т. е. дающими при делении на p один и тот же остаток S, тогда и только тогда, когда целое число*

$$Q = Q(\widetilde{S};\, j_1,\, j_2, ...,\, j_k) = \left\lfloor \frac{\widetilde{S}}{\prod_{i=1}^{k}p_{j_i}} \right\rfloor \tag{5}$$

кратно модулю p.

Д о к а з а т е л ь с т в о. Предположим, что число $\widetilde{S}$ и вычет $\widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i})$ по модулю $\prod_{i=1}^{k}p_{j_i}$ при делении на p дают один и тот же остаток. Ввиду (4) в этом случае

$$\left|\widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i})\right|_p = \left|\widetilde{S}\right|_p = S.$$

При этом

$$\widetilde{S} \equiv \widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i})(\mathrm{mod}\ p).$$

Отсюда следует, что разность $\widetilde{S} - \widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i})$ нацело делится на p. Согласно лемме Эвклида из теории делимости [7] ЦЧ $\widetilde{S}$ с учетом обозначения (5) представимо в виде

$$\widetilde{S} = \widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i}) + \left\lfloor \widetilde{S} / \prod_{i=1}^{k}p_{j_i} \right\rfloor \prod_{i=1}^{k}p_{j_i} = \widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i}) + Q(\widetilde{S};\, j_1,\, j_2, ...,\, j_k)\prod_{i=1}^{k}p_{j_i}.$$

Следовательно

$$\widetilde{S} = \widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i}) = Q(\widetilde{S};\, j_1,\, j_2, ...,\, j_k)\prod_{i=1}^{k}p_{j_i}. \tag{6}$$

Так как левая часть равенства (6) при принятом предположении нацело делится на p, а модуль p взаимно прост со всеми основаниями базиса **P** криптосхемы ЦЧ $Q(\widetilde{S};\, j_1,\, j_2, ...,\, j_k)$ кратно p.

Пусть теперь ЦЧ $Q(\widetilde{S};\, j_1,\, j_2, ...,\, j_k)$ нацело делится на p, тогда из (6) вытекает делимость разности $\widetilde{S} - \widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i})$ на модуль p. Это означает, что $\widetilde{S} \equiv \widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i})(\mathrm{mod}\ p)$. Таким образом, из кратности числа $Q(\widetilde{S};\, j_1,\, j_2, ...,\, j_k)$ модулю p следует равноостаточность по данному модулю $\widetilde{S}$ и $\widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i})$.

Теорема доказана.

Как следует из теоремы 2 в случае возможной равноостаточности по модулю p некоторого элемента $\widetilde{S} \in \widetilde{\mathbf{S}}$ и отвечающего ему вычета $\widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i}) \in \{0, 1, ..., \prod_{i=1}^{k}p_{j_i} - 1\}$ группа абонентов числом $k < t$, за которыми закреплены основания $p_{j_1}, p_{j_2}, \ldots, p_{j_k}$, могут восстановить секрет-оригинал $\widetilde{S}$ по модулярному коду $\widetilde{\sigma}_{j_1}, \widetilde{\sigma}_{j_2}, \ldots \widetilde{\sigma}_{j_k}$, благодаря выполнению равенства $\left|\widetilde{S}(\mathrm{mod}\prod_{i=1}^{k}p_{j_i})\right|_p = S$. Несмотря на непересекаемость диапазонов $\widetilde{\mathbf{S}}$ и $\{0, 1, ..., \prod_{i=1}^{k}p_{j_i} - 1\}$, обеспечиваемую теоремой 1, в указанном случае имеет место нарушение порогового принципа разделения секрета. Приемлемый выход из описанной ситуации дает исключение из диапазона $\widetilde{\mathbf{S}}$ критичных элементов $\widetilde{S}$. Это достигается за счет нейтрализации элементов диапазона **C** (см. (3)), изменения псевдослучайного параметра C, которые порождают ЦЧ $Q = Q(\widetilde{S};\, j_1,\, j_2, ...,\, j_k)$ вида (5), кратные модулю p. Искомые достаточные условия того, чтобы рассматриваемая (t, n)-криптосхема разделения секрета была пороговой, дает нижеследующая теорема.

Т е о р е м а 3. *Пусть* $p_1, p_2, \ldots, p_n$ *– упорядоченные по возрастанию попарно простые натуральные числа, составляющие базис* **P** *модулярной схемы разделения секрета S, p – взаимно простой с* $p_1, p_2, \ldots, p_n$ *модуль кольца* $\mathbf{Z}_p$ *принадлежности секрета S, который разделяется между n абонентами путем наделения их частичными маскирующими секретами* $\widetilde{\sigma}_i = \left|\widetilde{S}\right|_{p_i}$ $(i = \overline{1, n})$, *получаемыми в результате модулярной декомпозиции применяемой функции маскирования:* $\widetilde{S} = \widetilde{S} + Cp$ *(C – псевдослучайный целочисленный параметр). Для того чтобы любых l абонентов* $(2 \le t \le l \le n)$, *за которыми закреплены основания* $p_{i_1}, p_{i_2}, \ldots, p_{i_l}$ $(1 \le i_1 < i_2 < \ldots < i_l \le n)$ *могли восстановить секрет S по набору принадлежащих им частичных секретов – модулярному коду* $(\widetilde{\sigma}_{i_1}, \widetilde{\sigma}_{i_2}, \ldots \widetilde{\sigma}_{i_l})$ *маскирующего секрета* $\widetilde{S}$, *но никакая группа, включающая* $k < t$ *абонентов,*

которым отвечают основания $p_{j1}, p_{j2}, \ldots, p_{jk}$ $(1 \le j_1 < j_2 < \ldots < j_k \le n)$ *не имели возможности восстановления S по коду* $\tilde{\sigma}_{j1}, \tilde{\sigma}_{j2}, \ldots \tilde{\sigma}_{jk}$ *достаточно выполнения системы условий:*

$$\begin{cases} \tilde{S} \in \tilde{\mathbf{S}} = \{\tilde{S}_{\text{нп}}, \tilde{S}_{\text{нп}} + 1, \ldots, \tilde{S}_{\text{вп}}\} = \{\lceil \_P_{t-1} pq \rceil, \lceil \_P_{t-1} pq \rceil + 1, \ldots, \lfloor \_qP_t \rfloor - 1\} \\ C \in (\mathbf{C} \setminus \mathbf{C}_p), \end{cases}$$

где $q \ge p^{-1}$; $0 < \_q \le p_0 / p_t$; $\_qp_t \le p_0 \le p_t - t + 2$; $\_P_{t-1} = \prod_{s=0}^{t-2} p_{n-s}$; $P_t = \prod_{s=1}^{t} p_s$);

$$\mathbf{C} = \{C_{\text{нп}}, C_{\text{нп}} + 1, \ldots, C_{\text{вп}}\} \left(C_{\text{нп}} = \left\lfloor \frac{\tilde{S}_{\text{нп}}}{p} \right\rfloor;\ C_{\text{вп}} \left\lfloor \frac{\tilde{S}_{\text{вп}}}{p} \right\rfloor \right);$$

$$\mathbf{C}_p = \{C \in \mathbf{C} \,|\, \tilde{S} = S + Cp \in \tilde{\mathbf{S}};\ p - \text{делитель ЧЧ } Q = Q(\tilde{S}; j_1, j_2, \ldots, j_k) = \left\lfloor \frac{\tilde{S}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor$$
$$(1 \le j_1 < j_2 < \ldots < j_k \le n;\ 2 \le k < t)\};$$

$$Q(\tilde{S}; j_1, j_2, \ldots, j_k) \in \{Q_{\text{нп}}, Q_{\text{нп}} + 1, \ldots, Q_{\text{вп}}\} = \left\{ \left\lfloor \frac{\tilde{S}_{\text{нп}}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor, \left\lfloor \frac{\tilde{S}_{\text{нп}}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor + 1, \ldots, \left\lfloor \frac{\tilde{S}_{\text{вп}}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor \right\}. \quad (7)$$

Сформулированная теорема практически является следствием теорем 1 и 2.

Оптимизация (по мощности, структуре, другим характеристикам) множества $\tilde{\mathbf{C}} \in (\mathbf{C} \setminus \mathbf{C}_p)$, элементы которого используются при маскировании S по правилу (1), является важнейшей задачей в общем процессе синтеза пороговых МА-криптосхем разделения секрета, базирующихся на теореме 3.

Оптимизация диапазона псевдослучайного параметра методом сужения рабочего диапазона криптосхемы

Из теорем 2 и 3 следует, что количество значений $C \in \mathbf{C}$, которые порождают ЧЧ $Q = Q(\tilde{S}; j_1, j_2, \ldots, j_k)$, кратные модулю p, и по этой причине подлежат нейтрализации при маскировании секрета-оригинала S, в значительной мере зависит от протяженности $L_{\tilde{S}} = \tilde{S}_{\text{вп}} - \tilde{S}_{\text{нп}}$ рабочего диапазона $\tilde{\mathbf{S}}$ криптосхемы (см. (2)). Исходя из сказанного, примем для $L_{\tilde{S}}$ ограничительные условия:

$$L_{\tilde{S}} < pp_1p_2. \quad (8)$$

Из (2) и (8) для p вытекает оценка

$$\frac{\_qP_t}{\_P_{t-1}}(q + p_1p_2 / \_P_{t-1})^{-1} < p < \frac{\_qP_t}{\_P_{t-1}} q^{-1}. \quad (9)$$

Еще одно ограничение на выбор модуля p и параметров $\_q$ и q дает условие $0 < L_{\tilde{S}} < pp_1p_2$ (см. (2), (8)). Оно имеет вид

$$\frac{\_qP_t}{\_P_{t-1}p} - \frac{p_1p_2}{\_P_{t-1}} < q < \frac{\_qP_t}{\_P_{t-1}p}. \quad (10)$$

Приведем также вытекающую из (2), (9), (10) верхнюю оценку для pq:

$$pq < \_q \frac{P_t}{P_{t-1}} = \_qp_1 \frac{p_2}{p_{n-t+2}} \frac{p_3}{p_{n-t+3}} \cdot \ldots \cdot \frac{p_t}{p_n} < \_qp_1. \quad (11)$$

В (11) учитывается возрастание оснований $p_1, p_2, \ldots, p_n$ криптосхемы.

Отметим, что благодаря (8) длина L_Q промежутка залегания значений ЧЧ $Q = Q(\tilde{S}; j_1, j_2, \ldots, j_k)$ (см. (7)) удовлетворяет ограничительному условию

$$L_Q = Q_{\text{вп}} - Q_{\text{нп}} \le \frac{L_{\tilde{S}}}{\prod_{i=1}^{k} p_{j_i}} + 1 < pp_1p_2 / \prod_{i=1}^{k} p_{j_i} + 1. \tag{12}$$

Верхний порог (12) для L_Q принимает максимальное значение $p + 1$ при $\prod_{i=1}^{k} p_{j_i} = p_1p_2$ $(k = 2;\ j_1 = 1,\ j_2 = 2)$. С возрастанием $\prod_{i=1}^{k} p_{j_i}$ порог (12) убывает. Таким образом, в рамках принятого ограничения для $L_{\tilde{S}}$, а следовательно, и для L_Q интервал изменения ЦЧ $Q(\tilde{S};\ j_1,\ j_2, ...,\ j_k)$ может содержать не более одного значения, кратного модулю p.

Остановимся кратко на вопросе обнаружения в диапазоне **C** (см. (3)) значений псевдослучайного параметра C, порождающих ЦЧ $Q = Q(\tilde{S};\ j_1,\ j_2, ...,\ j_k)$, кратные модулю p. С учетом (5) с помощью леммы Эвклида, примененной к маскирующему секрету $\tilde{S} = \tilde{S} + Cp$ и модулю произведений $\prod_{i=1}^{k} p_{j_i}$, которые отвечают требуемым C и Q вида

$$Q = Q(\tilde{S};\ j_1,\ j_2, ...,\ j_k) = \left| \tilde{S} / \prod_{i=1}^{k} p_{j_i} \right| = Dp \quad (D - \text{делитель ЦЧ } Q),$$

можно записать как

$$\tilde{S} = S + Cp = \left\lfloor \tilde{S} / \prod_{i=1}^{k} p_{j_i} \right\rfloor \prod_{i=1}^{k} p_{j_i} + R = Dp \prod_{i=1}^{k} p_{j_i} + R, \tag{13}$$

где $R = \tilde{S} (\text{mod} \prod_{i=1}^{k} p_{j_i})$ – остаток от деления $\tilde{S}$ на $\prod_{i=1}^{k} p_{j_i}$ $(R \in \{0, 1, ..., \prod_{i=1}^{k} p_{j_i} - 1\})$.

В свою очередь применение к вычету R и модулю p леммы Эвклида дает

$$\begin{gathered} R = \left\lfloor \frac{R}{p} \right\rfloor p + r = dp + r \\ d = \left(\left\lfloor \frac{R}{p} \right\rfloor \in \left\{ 0, 1, ..., \left\lfloor \frac{\prod_{i=1}^{k} p_{j_i}}{p} \right\rfloor \right\},\ r = |R|_p \in \mathbf{Z}_p \right). \end{gathered} \tag{14}$$

После подстановки (14) в (13) получим

$$\tilde{S} = S + Cp = Dp \prod_{i=1}^{k} p_{j_i} + dp + r. \tag{15}$$

Заметим, что в случае выполнения соотношения (15) остаток $r = |\tilde{S}|_p = |R|_p$ совпадает с исходным секретом S, что согласуется с теоремой 2.

Деление частей равенства (15) на p с последующей заменой результатов деления на их целые части приводит к необходимому выражению для искомых C, порождающих $Q = Q(S + Cp;\ j_1,\ j_2, ...,\ j_k)$, вида (15)

$$C = \left\lfloor \frac{\tilde{S}}{p} \right\rfloor = D \prod_{i=1}^{k} p_{j_i} + d \quad \left(d = 0, 1, ..., \left(\left\lfloor \prod_{i=1}^{k} p_{j_i} \right) / p \right\rfloor \right). \tag{16}$$

В представленном способе минимизации характеристики $|\mathbf{C}_p|$, естественно, могут применяться и менее жесткие, чем используемые в (8) ограничения на $L_{\tilde{S}}$. Например, порог pp_1p_2 можно заменить на $pp_1p_2p_3$. Это дает большую свободу для выбора оснований $p_1, p_2, \ldots, p_n$ криптосхемы, модуля p, а также параметров q и $\_q$. Вместе с тем, увеличение порога в (8) сопряжено с возрастанием мощности множества $\mathbf{C}_p$, что усложняет проверку условия теоремы 3.

Демонстрационный пример. Пусть в классе модулярных пороговых (4, 6)-схем разделения секрета, определяемом базисом **P** = {7, 11, 13, 17, 19, 23}, а также характеристиками pq = 2,09 и $\_q$ = 0,94, требуется выделить представителей, которые отличаются минимальным количеством значений псевдослучайного параметра C, подлежащих нейтрализации.

Прежде всего найдем:

$$P_t = P_4 = p_1p_2p_3p_4 = 7 \cdot 11 \cdot 13 \cdot 17 = 1001 \cdot 17;$$

$$\_P_{t-1} = \_P_3 = p_4 p_5 p_6 = 17 \cdot 19 \cdot 23 = 17 \cdot 437.$$

Решение поставленной задачи базируется на использовании множеств ЦЧ Q вида (5), рассчитанных для реперных наборов оснований из $\mathbf{P}$ согласно (7). Прежде всего найдем границы изменения $\widetilde{S} = S + Cp$, определяющие рабочий диапазон криптосхемы. В соответствии с (2) имеем

$$\widetilde{S}_{\text{нп}} = \_Ppq = 17 \cdot 19 \cdot 23 \cdot 2{,}09 = 15526{,}61;$$

$$\widetilde{S}_{\text{вп}} = \_qP_4 = 0{,}94 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = 15995{,}98.$$

Следовательно, значения переменной $\widetilde{S}$ являются элементами множества

$$\widetilde{\mathbf{S}} = \left\{ \left\lceil \widetilde{S}_{\text{нп}} \right\rceil, \left\lceil \widetilde{S}_{\text{нп}} \right\rceil + 1, ..., \left\lfloor \widetilde{S}_{\text{вп}} \right\rfloor \right\} = \{15527, 15528, ..., 15995\}. \tag{17}$$

Что касается ЦЧ $Q = Q(\widetilde{S}; j_1, j_2, ..., j_k)$, то согласно (7), они принадлежат диапазонам

$$Q(j_1, j_2, ..., j_k) = \left\{ \left\lfloor \frac{\widetilde{S}_{\text{нп}}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor, \left\lfloor \frac{\widetilde{S}_{\text{нп}}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor + 1, ..., \left\lfloor \frac{\widetilde{S}_{\text{вп}}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor \right\} =$$

$$= \left\{ \left\lfloor \frac{15526{,}61}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor, \left\lfloor \frac{15526{,}61}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor + 1, ..., \left\lfloor \frac{15995{,}98}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor \right\} \tag{18}$$

$$(1 \le j_1 < j_2 < ... < j_k \le 6;\ 2 \le k < t = 4).$$

Множества (18), сформированные для реперных наборов оснований $\mathbf{P}(j_1, j_2) = \{p_{j_1}, p_{j_2}\}$ и $\mathbf{P}(j_1, j_2, j_3) = \{p_{j_1}, p_{j_2}, p_{j_3}\}$, приведены в табл. 1. Результаты анализа множеств $\mathbf{Q}(j_1, j_2)$ и $\mathbf{Q}(j_1, j_2, j_3)$ в целях детектирования в них ЦЧ Q, кратных модулям p исследуемого набора и вычисления по (16), подлежащих нейтрализации соответствующих значений псевдослучайного параметра C, представлены в табл. 2. Данные табл. 2 позволяют выделить из рассмотренного класса модулярных пороговых (4, 6)-схем разделения секрета два представителя с минимальной мощностью множества $\mathbf{C}_p$ (см. теорему 3). В искомых криптосхемах применяются модули $p = 27$ и $p = 30$. При указанных p псевдослучайный параметр C принимает значения соответственно из диапазонов

$$\widetilde{\mathbf{C}} = \mathbf{C} / \mathbf{C}_{27} = \{575, 576, ..., 592\} \setminus \{575, 576, 577\} = \{578, 579, ..., 592\}$$

и

$$\widetilde{\mathbf{C}} = \mathbf{C} / \mathbf{C}_{30} = \{517, 518, ..., 533\} \setminus \{532, 533\} = \{517, 518, ..., 531\}.$$

Поскольку протяженность рабочего диапазона (17) выделенных криптосхем составляет 15995 – 15527 = 468, то как при $p = 27$, так и в случае $p = 30$ ограничительное условие (8) ввиду $27p_1p_2 = 27 \cdot 7 \cdot 11 = 2079$ и $30p_1p_2 = 30 \cdot 7 \cdot 11 = 2310$ выполняется. Полученные оптимальные значения модуля p ($p = 27$; 30) произведение $pq = 2{,}09$ и параметры $q = 2{,}09 / p$, $\_q = 0{,}94$ удовлетворяют также оценкам (9)–(11), так как

$$q = \frac{2{,}09}{27} = 0{,}0773 \in \left(\frac{0{,}94 \cdot 1001}{437 \cdot 27} - \frac{7 \cdot 11}{17 \cdot 437}; \frac{0{,}94 \cdot 1001}{437 \cdot 27} \right) = (0{,}069; 0{,}079);$$

$$q = \frac{2{,}09}{30} = 0{,}0697 \in \left(\frac{0{,}94 \cdot 1001}{437 \cdot 30} - \frac{7 \cdot 11}{17 \cdot 437}; \frac{0{,}94 \cdot 1001}{437 \cdot 30} \right) = (0{,}0615; 0{,}0718);$$

Т а б л и ц а 1. **Множества чисел Q, отвечающих k-компонентным наборам ($2 \le k < t = 4$) оснований из базиса P = {7, 11, 13, 17, 19, 23} модулярной пороговой (4, 6)-криптосхемы разделения секрета с рабочим диапазоном $\tilde{S}$ = {15527, 15528, …, 15995}**

T a b l e 1. **Set of the numbers Q obeying the k-component sets ($2 \le k < t = 4$) of the bases of the basis P = {7, 11, 13, 17, 19, 23} of the modular threshold (4, 6)-cryptographic scheme of secret sharing within the working range $\tilde{S}$ = {15527, 15528, …, 15995}**

Набор оснований Set of bases	Множество ЦЧ Q Set of integers Q
⟨7, 11⟩	201–207
⟨7, 13⟩	170–175
⟨7, 17⟩	130–134
⟨7, 19⟩	116–120
⟨7, 23⟩	96–99
⟨11, 13⟩	108–111
⟨11, 17⟩	83–85
⟨11, 19⟩	74–76
⟨11, 23⟩	61–63
⟨13, 17⟩	70–72
⟨13, 19⟩	62–64
⟨13, 23⟩	51–53
⟨17, 19⟩	48–49
⟨17, 23⟩	39–40
⟨19, 23⟩	35–36
⟨7, 11, 13⟩	15
⟨7, 11, 17⟩	11–12

Т а б л и ц а 2. **Модули p для пороговой (4, 6)-схемы разделения секрета с модулярным базисом P = {7, 11, 13, 17, 19, 23} и рабочим диапазоном $\tilde{S}$ = {15527, 15528, …, 15995}, обеспечивающие минимизацию мощности множества C_p**

T a b l e 2. **Modules p for the threshold (4, 6)-scheme of secret sharing with the modular basis P = {7, 11, 13, 17, 19, 23} and the working range $\tilde{S}$ = {15527, 15528, …, 15995} providing the minimization of the power of the set C_p**

Модуль p Module p	Диапазон изменения параметра C Range of the parameter C	Критичный набор оснований Critical set of bases	Число Q, кратное модулю p Number Q multiple of the module p	Нейтрализуемые значения C Neutralizable values of C
16	970–999	⟨7, 23⟩	96	970–976
		⟨13, 19⟩	64	988–999
		⟨17, 19⟩	48	970–989
18	862–888	⟨11, 13⟩	108	862–865
		⟨13, 17⟩	72	884–888
		⟨19, 23⟩	36	874–888
20	776–799	⟨7, 19⟩	120	798–799
		⟨17, 23⟩	40	782–799
24	646–666	⟨7, 19⟩	120	665–666
		⟨7, 23⟩	96	646–649
		⟨13, 17⟩	72	663–666
		⟨17, 19⟩	48	646–659
27	575–592	⟨11, 13⟩	108	575–577
29	535–551	⟨7, 11⟩	203	539–541
		⟨7, 19⟩	116	535–536
30	517–533	⟨7, 19⟩	120	532–533
31	500–515	⟨11, 23⟩	62	506–514
		⟨13, 19⟩	62	500–501
32	485–499	⟨7, 23⟩	96	485–488
		⟨13, 19⟩	64	494–499

$$p = 27 \in \left(\frac{0{,}94 \cdot 1001}{437\left(\left(\frac{2{,}09}{27}\right)+\left(7\frac{11}{17 \cdot 437}\right)\right)}; \frac{0{,}94 \cdot 1001}{437\frac{2{,}09}{27}} \right) = (24{,}53; 27{,}82);$$

$$p = 30 \in \left(\frac{0{,}94 \cdot 1001}{437\left(\left(\frac{2{,}09}{30}\right)+\left(7\frac{11}{17 \cdot 437}\right)\right)}; \frac{0{,}94 \cdot 1001}{437\frac{2{,}09}{30}} \right) = (26{,}9; 30{,}9);$$

$$pq = 2{,}09 < \frac{0{,}94 \cdot 1001}{437} = 2{,}153 < p_1 = 7.$$

Таким образом, построенная в рамках принятых исходных данных и ограничительных условий параметрическая база модулярных пороговых (4, 6)-криптосхем разделения секрета с базисом $\mathbf{P}$ = {7, 11, 13, 17, 19, 23}, рабочим диапазоном $\tilde{\mathbf{S}}$ = {15527, 15528, …, 15995} и модулями $p \in \{27, 30\}$ является корректной.

Заключение. Результаты представленных исследований по модулярным пороговым криптосистемам разделения секрета в распределенных средствах обработки данных состоят в нижеследующем.

1. Сформулированы базовые принципы порогового метода модулярного разделения секрета. Для принятой модели МА-криптосхем исследуемого класса определено семейство допустимых рабочих диапазонов (диапазонов секрета-маски), протяженность и местоположение которых на числовой оси могут гибко изменяться. Это открывает широкие возможности для адаптивного согласования рабочего диапазона криптосхемы с ее основаниями и множеством изменения псевдослучайного параметра маскирующей функции.

2. Для модулярной пороговой (t, n)-схемы разделения секрета получено необходимое и достаточное условие равноостаточности по модулю кольца принадлежности секрета-оригинала значений маскирующей функции и отвечающих им вычетов в некоторой усеченной k-модульной МСС ($k < t$). Доказанное теоретическое положение составляет основу корректной модулярной реализации порогового принципа разделения секретной информации.

3. Предложен новый подход к обеспечению корректности пороговых МА-криптосхем разделения секрета, реализующий механизм нейтрализации критичных значений псевдослучайного параметра применяемой маскирующей функции. Разработанный подход демонстрируется на конкретных числовых примерах.

Благодарности. Проведенные исследования выполнены при финансовой поддержке БРФФИ (договор № Ф18-005) и ГПНИ «Информатика, космос и безопасность» (задание № 1.2.09).

Acknowledgments. The present study is financially supported by the Belarusian Republican Foundation for Fundamental Research (agreement no. Ф18-005) and by the State Research Program “Informatics, Space and Security” (task no. 1.2.09).

Список использованных источников

1. Криптология / Ю. С. Харин [и др.]. – Минск, 2013. – 512 с.

2. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. – М., 2012. – 280 с.

3. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Н. И. Червяков [и др.]. – М., 2017. – 400 с.

4. Bahramian, Mojtaba. An efficient threshold verifiable multisecret sharing scheme using generalized jacobian of elliptic curves / Mojotaba Bahramian, Khadijeh Eslami // Algebraic Structures and their Applications. – 2017. – Vol. 4, N 2. – P. 45–55. https://doi.org/10.29252/asta.4.2.45

5. A new threshold changeable secret sharing scheme based on the Chinese remainder theorem / Xingxing Jia [et al.] // Information Sciences. – 2019. – Vol. 473. – P. 13–30. https://doi.org/10.1016/j.ins.2018.09.024

6. Ananda Mohan, P. V. Residue number systems: Theory and applications / P. V. Ananda Mohan. – Basel, 2016. – 351 p. https://doi.org/10.1007/978-1-4615-0997-4

7. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – СПб., 2009. – 176 с.

References

1. Kharin Yu. S., Agievich S. V., Vasiliev D. V., Matveev G. V. *Cryptology*. Minsk, 2013. 512 p. (in Russian).
2. Chervyakov N. I., Evdokimov A. A., Galushkin A. I., Lavrinenko I. N., Lavrinenko A. V. *The Use of Artificial Neural Networks and the Residual Class System in Cryptography*. Moscow, 2012. 280 p. (in Russian).
3. Chervyakov N. I., Kolyada A. A., Lyahov P. A., Babenko M. G., Lavrinenko I. N., Lavrinenko A. V. *Modular Arithmetic and its Applications in Infocommunication Technologies*. Moscow, 2017. 400 p. (in Russian).
4. Bahramian Mojtaba, Eslami Khadijeh. An efficient threshold verifiable multisecret sharing scheme using generalized jacobian of elliptic curves. *Algebraic Structures and their Applications*, 2017, vol. 4, no. 2, pp. 45–55. https://doi.org/10.29252/asta.4.2.45
5. Xingxing Jia, Daoshun Wang, Daxin Nie, Xiangyang Luo, Jonathan Zheng Sun. A new threshold changeable secret sharing scheme based on the Chinese remainder theorem. *Information Sciences*, 2019, vol. 473, pp. 13–30. https://doi.org/10.1016/j.ins.2018.09.024
6. Ananda Mohan P. V. *Residue number systems: Theory and applications*. Basel, 2016. 351 p. https://doi.org/10.1007/978-1-4615-0997-4
7. Vinogradov I. M. *Fundamentals of number theory*. Saint Petersburg, 2009. 176 p. (in Russian).

Информация об авторах

Чернявский Александр Федорович – академик, д-р техн. наук, профессор, заведующий лабораторией. Институт прикладных физических проблем им. А. Н. Севченко БГУ (ул. Курчатова, 7, 220045, Минск, Республика Беларусь). E-mail: niipfp@bsu.by.

Коляда Андрей Алексеевич – д-р физ.-мат. наук, доцент, гл. науч. сотрудник. Институт прикладных физических проблем им. А. Н. Севченко БГУ (ул. Курчатова, 7, 220045, Минск, Республика Беларусь). E-mail: razan@tut.by.

Мартинов Антон Олегович – науч. сотрудник. Институт прикладных физических проблем им. А. Н. Севченко БГУ (ул. Курчатова, 7, 220045, Минск, Республика Беларусь). E-mail: antonmartenov@gmail.com.

Протасеня Стелла Юрьевна – мл. науч. сотрудник. Институт прикладных физических проблем им. А. Н. Севченко БГУ (ул. Курчатова, 7, 220045, Минск, Республика Беларусь). E-mail: Estellita@mail.ru.

Information about the authors

Chernyavsky Alexander Fedorovich – Academician, D. Sc. (Engineering), Professor, Head of the Laboratory. Institute of Applied Physical Problems named after A. N. Sevchenko of the Belarusian State University (7, Kurchatov Str., 220045, Minsk, Republic of Belarus). E-mail: niipfp@bsu.by.

Kolyada Andrey Alexeyevich – D. Sc. (Physics and Mathematics), Associate professor, Chief researcher. Institute of Applied Physical Problems named after A. N. Sevchenko of the Belarusian State University (7, Kurchatov Str., 220045, Minsk, Republic of Belarus). E-mail: razan@tut.by.

Martinov Anton Olegovich – Researcher. Institute of Applied Physical Problems named after A. N. Sevchenko of the Belarusian State University (7, Kurchatov Str., 220045, Minsk, Republic of Belarus). E-mail: antonmartenov@gmail.com.

Protasenya Stella Yuryevna – Junior researcher. Institute of Applied Physical Problems named after A. N. Sevchenko of the Belarusian State University (7, Kurchatov Str., 220045, Minsk, Republic of Belarus). E-mail: Estellita@mail.ru.