01.01.09
УДК 004.9, 004.94, 004.56

ДИСКРЕТНАЯ МАТЕМАТИКА И МАТЕМАТИЧЕСКАЯ КИБЕРНЕТИКА

Коляда А.А., Институт прикладных физических проблем имени А.Н. Севченко, Белорусского государственного университета, Минск, Республика Беларусь
Бабенко М.Г., Северо-Кавказский федеральный университет,
Протасеня С.Ю. г. Ставрополь, Российская Федерация

МЕТОД ВЫПОЛНЕНИЯ ДЕКОДИРУЮЩЕЙ ОПЕРАЦИИ В ПОРОГОВОЙ МИМА-КРИПТОСИСТЕМЕ РАЗДЕЛЕНИЯ СЕКРЕТА С МАСКИРУЮЩИМ ПРЕОБРАЗОВАНИЕМ

Введение. В статье предложен новый метод восстановления пространственно разделяемого секрета в рамках порогового принципа по наборам частичных секретов, принадлежащих группам абонентов, число которых ограничено снизу установленным порогом.

Материалы и методы исследований. В целях сокращения временных затрат на выполнение данной операции в качестве компьютерно-арифметической базы применена минимально избыточная модулярная арифметика (МИМА). В отличие от неизбыточных аналогов МИМА обладает более эффективными немодульными процедурами, что позволяет оптимизировать декодирующую операцию в пороговой МИМА-криптосхеме разделения секрета.

Результаты исследований и их обсуждение. Отличительной особенностью развиваемого подхода является использование для секрета-оригинала областей изменения, представляющих собой кольца вычетов по модулям вида степеней числа 2. Это значительно упрощает декодирующую операцию, выполняемую по методу деления на двоичную экспоненту.

Выводы. Благодаря отмеченным особенностям, разработанный метод реконструкции исходного секрета по кодам секрета-маски превосходит неизбыточные аналоги как минимум в $\frac{l(19l-3)}{2(11l-3)}$ – раз (l – число абонентов, восстанавливающих секрет-оригинал). При l = 7÷ 40 достигается (6.15 ÷ 34,65) — кратное увеличение производительности.

Ключевые слова: пороговое разделение секрета, криптосхемы разделения секрета, маскирующее преобразование, декодирующая операция, модулярный код, модулярные системы счисления, минимально избыточная модулярная арифметика.

Kolyada A.A, A.N. Sevchenko Institute of Applied Physical Problems of Belarusian State University, Minsk, Belarus
Babenko M.G., North-Caucasus Federal University,
Protasenia S. Yu. Stavropol, Russia

Method for Performing a Decoding Operation in a Threshold Mrma Cryptosystem of Secret Separation with Masking Transformation

Introduction: the article proposes a new method for recovering a spatially shared secret within the threshold principle based on sets of partial secrets belonging to subscriber groups, the number of which is limited from below by a specified threshold.

Materials and methods of the research: to reduce the time spent on performing this operation, minimally redundant modular arithmetic (MRMA) is used as a computer arithmetic base. Unlike non-redundant analogs, MRMA possesses more efficient non-modular procedures, which makes it possible to optimize the decoding operation in the threshold MRMA-crypto-scheme of secret sharing.

The results of the research and their discussion: a distinctive feature of the developed approach is the use of change areas for the original secret, which are rings of residues in moduli of the form of powers of 2. This greatly simplifies the decoding operation performed by the binary exponential division method.

Conclusions: due to the noted features, the developed method for reconstructing the original secret using secret-mask codes surpasses the non-redundant counterparts by at least $\frac{l(19l-3)}{2(11l-3)}$ times (l is the number of subscribers restoring the original secret). At l = 7÷ 40, a (6.15 ÷ 34,65) – fold increase in productivity is achieved.

Keywords: threshold secret sharing, secret sharing cryptographic schemes, masking conversion, decoding operation, modular code, modular number systems, minimally redundant modular arithmetic

ВВЕДЕНИЕ

Важнейшей актуальной задачей современного процесса развития распределенных компьютерных и инфокоммуникационных систем является надежное обеспечение необходимого уровня безопасности при хранении, обработке и передаче данных [1, 2]. При решении обозначенной задачи особую роль выполняет применяемая технология управления криптографическими ключами. В настоящее время к наиболее перспективным технологиям такого рода относят технологию активной безопасности [1, 3], которая базируется на периодическом обновлении ключей, одноразовых паролях и пространственном разделении секрета. На практике разделение секретной информации обычно осуществляется в рамках пороговых схем [1–12].

Реализуемое (t, n)-пороговой системой решающее правило обеспечивает разделение секрета n абонентами с возможностью его восстановления по компонентам, принадлежащим любым l участникам сеан-

са связи ($2 \le t \le 1 \le n$); t – пороговое число абонентов). При этом группы абонентов числом $k < t$ реконструировать секрет-оригинал по соответствующим компонентам не могут. Исходный и долевые секреты представляют собой большие целые числа (ЦЧ), поэтому эффективность выполняемых в пороговых криптосистемах преобразований определяется реализационными свойствами используемой технологии перевода осуществляемых вычислений из диапазонов больших чисел в диапазоны ЦЧ стандартной разрядности. В свете сказанного в качестве компьютерно-арифметической основы для криптографических приложений рассматриваемого класса целесообразно принять модулярную арифметику – арифметику модулярных систем счисления (МСС). Фундаментальные преимущества МСС наиболее полно удается реализовать в рамках так называемого минимально избыточного кодирования [2, 12–14].

Наиболее трудоемкой операцией в пороговых криптосистемах модулярной арифметики разделения секретной информации является реконструкция секрета-оригинала по модулярным кодам маскирующего аналога. Это обусловлено главным образом использованием в операциях данного класса вычислительных технологий, ориентированных на диапазоны больших чисел, а также соответствующих конфигураций интегрально-характеристической базы системы счисления в остатках. Настоящее сообщение посвящено разработке метода выполнения декодирующей операции в пороговом криптомодуле разделения секрета, базирующемся на минимально избыточной модулярной арифметике (МИМА) [1]. Применение вычислительной МИМА-технологии на диапазонах больших чисел для решения рассматриваемой задачи позволяет в значительной мере минимизировать необходимые временные и аппаратурные затраты.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЙ

1 Принципиальные основы пороговых МИМА-криптосхем разделения секрета с маскирующим преобразованием

Введем обозначения:

— $\lfloor a \rfloor$ и $\lceil a \rceil$ – наибольшее и наименьшее ЦЧ соответственно не большее и не меньшее вещественной величины a;

— НОД (A, B) – наибольший общий делитель целых чисел A и B;

— $\boldsymbol{Z}_m = \{0, 1, \ldots, m-1\}$ – множество наименьших неотрицательных вычетов (остатков) по натуральному модулю $m > 1$;

— $\chi = |A/B|_m = (A/B) \pmod m$ – элемент множества $\mathbf{Z}_m$, удовлетворяющий сравнению $B\chi \equiv A(\mathrm{mod}\, m)$ (B $\neq$ 0, НОД $(B, m) = 1$);

— $\mathbf{M}\_l = \{m_1, m_2, \ldots, m_l\}$ – базис МСС, состоящий из $l > 1$ попарно простых модулей (оснований);

— $(|X|_{m_1}, |X|_{m_2}, |X|_{m_l})$ – представление ЦЧ X (модулярный код) в МСС с базисом $\mathbf{M}\_l$.

Пусть $p_1, p_2, \ldots, p_n$ – упорядоченные по возрастанию попарно простые большие натуральные числа ($n > 1$); $\mathrm{P}_i = \prod_{s=1}^{i} p_s$; $\_P_j = \prod_{s=1}^{j} p_{n-s+1} = / P_{n-j}$ $(i, j = 1, n)$; $\mathbf{P} = \{p_1, p_2, \ldots, p_n\}$; $\mathbf{I}\_l = \{\forall(i_1, i_2, \ldots, i_l)\} | 1 \le i_1 < i_2 < \ldots < i_l \le n$; ($t$ – фиксированное натуральное число); $I\_l = (i_1, i_2, \ldots, i_l)$ – произвольный элемент множества I_l $\mathbf{P}_{I\_l} = \{p_{i_1}, p_{i_2}, \ldots, p_{i_l}\}$; $\mathrm{P}_{I\_l} = \prod_{j=1}^{l} p_{i_j}$.

Концептуальную основу (t, n)-пороговой схемы разделения секрета с модулярным базисом $\mathbf{P} = \mathbf{P}\_n = \{p_1, p_2, \ldots, p_l\}$ которая рассчитана на полное число n и пороговое число t абонентов распределенной системы, составляют нижеследующие определяющие положения.

А. Исходный секрет (секрет-оригинал) представляет собой ЦЧ $S \in \mathbf{Z}_p$ (p – большой модуль, взаимно простой с $p_1, p_2, \ldots, p_n$).

Б. Над S в МСС с базисом $\mathbf{P}$ выполняется маскирующее преобразование вида

$$\tilde{\boldsymbol{S}} = S + C \cdot p, \qquad (1)$$

где C – псевдослучайный целочисленный параметр.

Цифры $\tilde{\boldsymbol{\sigma}}_{i_1} = |\tilde{\boldsymbol{S}}|_{p_i} = \left|\sigma_i + |\mathrm{C} \cdot p|_{p_i}\right|_{p_i}$ $(\sigma_i = |S|_{p_i};\ i = 1, n)$ получаемого кода $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ рассматриваются как долевые (частичные) секреты, принадлежащие одноименным абонентам.

В. Любые l абонентов $(t \le l \le n)$ могут восстановить секрет-оригинал S по принадлежащим им долевым (маскирующим) секретам. Но никакая группа абонентов количеством $k < t$ сделать этого не может.

Представляемые исследования нацелены на решение задачи восстановления секрета-оригинала S по кодам $(\tilde{\boldsymbol{\sigma}}_{i_1}, \tilde{\boldsymbol{\sigma}}_{i_2}, \tilde{\boldsymbol{\sigma}}_{i_l})$ МСС с базисами $\mathbf{P}_{I\_l}$ $(I\_l \in \mathbf{I}\_l)$ маскирующего аналога (1) (см. пункт А) с обеспечением минимизации временных затрат на выполнение резуль-

тирующей декодирующей процедуры при сохранении максимального уровня криптостойкости, присущего классическим пороговым схемам, таким, в частности, как схемы Шамира, Блэкли и другие [3–11]. При этом для синтеза искомого декодирующего алгоритма (алгоритма восстановления секрета-оригинала) используются метод деления на двоичную экспоненту, а также вычислительная МИМА-технология [2].

Основополагающая идея предлагаемой алгоритмизации преобразования $\tilde{S} \to S$ состоит в использовании для кодирования секрета-маски $\tilde{S}$ семейства минимально избыточных МСС (МИМСС), определяемых базисами $\mathbf{P}_{I\_l}$, которые отвечают группам абонентов числом l. Без нарушения общности изложение дальнейшего материала преимущественно проводится на примере группы абонентов, за которыми закрепляются основания $p_1, p_2, \ldots, p_l$ набора $\mathbf{P}\_l$ – представителя множества $\mathbf{P}_{\mathbf{I}\_l}$ с $I\_l = (1, 2, \ldots, l)$ $\mathbf{I}\_l$. Долевые секрета, принадлежащие абонентам указанной группы являются цифрами кода $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ МСС с модулями $p_1, p_2, \ldots, p_l$ секрета-маски $\tilde{S}$.

В компьютерных алгоритмах МИМА фундаментальную роль выполняет интервально-модулярная форма чисел. В случае ЦЧ $\tilde{S} = (\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ она имеет вид

$$\tilde{S} = \sum_{i=1}^{l-1} P_{i,l-1}\tilde{\sigma}_{i,l-1} + P_{l-1}I_l(\tilde{S}), \tag{2}$$

где
$$P_{i,l-1} = \frac{P_{l-1}}{p_i}, P_{l-1} = \prod_{s=1}^{l-1} p_s;$$

$$\tilde{\sigma}_{i,l-1} = \left|P_{i,l-1}^{-1}\tilde{\sigma}_l\right|_{p_i}; \tag{3}$$

интервальный индекс числа $\tilde{S}$ по базису $\mathbf{P}\_l$. Принцип минимально избыточного модулярного кодирования раскрывает нижеследующая теорема [2, 13, 14].

Теорема 1. Для того, чтобы в МСС с базисом $\mathbf{P}\_l$ интервальный индекс $I_l(\tilde{S})$ каждого элемента $\tilde{S}$ диапазона $\mathbf{Z}p = \{0, 1, \ldots, P-1\}$ ($\mathrm{P} = p_0\mathrm{P}_{l-1}$; p_0 – вспомогательный модуль) полностью определялся вычетом $\hat{I}_l(\tilde{S}) = |I_l(\tilde{S})|_{pl}$, необходимо и достаточно выполнения условия

$$p_l \geq 2\,p_0 + l\ (p_0 \geq l - 2) \tag{4}$$

При этом для $I_l(\tilde{S})$ верны расчетные соотношения:

$$I_l(\tilde{S}) = \begin{cases} \hat{I}_l(\tilde{S}), & \text{если } \hat{I}_l(\tilde{S}) < p_0, \\ \hat{I}_l(\tilde{S}) - p_l, & \text{если } \hat{I}_l(\tilde{S}) \geq p_0; \end{cases} \tag{5}$$

$$\hat{I}_l(\tilde{S}) = \left| \sum_{i=1}^{l} R_{i,l}(\tilde{\sigma}_i) \right|_{p_l} \tag{6}$$

$$R_{i,l}(\tilde{\sigma}_i) = \left| -p_i^{-1} \left| P_{i,l-1}^{-1} \tilde{\sigma}_i \right|_{p_i} \right|_{p_l} (i \neq l),\ R_{l,l}(\tilde{\sigma}_l) = \left| \frac{\tilde{\sigma}_l}{P_{l-1}} \right|_{p_l}. \tag{7}$$

Главное преимущество МИМСС с базисами $\mathbf{P}_{I\_l}$ ($I\_l \in \mathbf{I}\_l$) над неизбыточными аналогами обусловлено l-кратным сокращением реализационных затрат на вычисление интервального индекса, осуществляемое по формулам вида (5) – (7) [2, 13, 14].

Корректное согласование порогового принципа разделения секрета и минимально избыточного модулярного кодирования с обеспечением необходимого уровня криптостойкости результирующей МИМА-схемы дает нижеследующая теорема [12].

Теорема 2. Для того, чтобы любые l абонентов ($2 \le t \le l \le n$; t – фиксированное ЦЧ) могли восстановить S по соответствующему коду МСС маскирующего секрета $\tilde{S}$, удовлетворяющей условию вида (4) минимальной избыточности (см. теорему 1), но никакая группа абонентов числом $k < t$ не имела такой возможности, достаточно выполнения системы условий:

$$\begin{cases} \tilde{S} \in \tilde{\mathbf{S}} = \{\tilde{S}_{\text{нп}}, \tilde{S}_{\text{нп}} + 1, \ldots, \tilde{S}_{\text{вп}}\} \subseteq \{\_P_{t-1}, \_P_{t-1} + 1, \ldots, p_0 P_{t-1} - 1\}, \\ C \in \tilde{\mathbf{C}} = (\mathbf{C} \backslash \mathbf{C}_p), \end{cases}$$

где $\tilde{S}_{\text{нп}}$ и $\tilde{S}_{\text{вп}}$ – используемые нижнее и верхнее пороговые значения секрета-маски $\tilde{S}$;

p_0 – вспомогательный модуль, удовлетворяющий ограничению $p_0 \le p_0 - t + 2$;

$$\mathbf{C} = \{C_{\text{НП}}, C_{\text{НП}} + 1, \ldots, C_{\text{ВП}}\}\ (C_{\text{НП}} = \lfloor \tilde{S}_{\text{НП}}/p \rfloor;$$
$$C_{\text{ВП}} = \lfloor \tilde{S}_{\text{ВП}}/p \rfloor);$$
$$\mathbf{C}_p = \{\forall C \in \mathbf{C} | S + C \cdot p \in (\tilde{S}_{\text{НП}}; \tilde{S}_{\text{ВП}});$$
$$Q(\tilde{S}; j_1, j_2, \ldots, j_k) =$$
$$= \left\lfloor \frac{\tilde{S}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor (1 \le j_1 < j_2 < \cdots < j_k \le n; 2 \le k < t)\},$$

p – целитель ЦЧ Q.

2. Метод выполнения декодирующей операции в пороговом МИМА-криптомодуле разделения секрета с маскирующим преобразованием

Реконструкция секрета-оригинала по модулярным кодам маскирующего аналога является наиболее трудоемкой операцией в пороговых МА-криптосистемах разделения секрета. Из (1) вытекает равенство $S - |\tilde{S}|_p$, указывающее на то, что для получения S по $\tilde{S}$ достаточно ЦЧ $\tilde{S}$ привести к остатку по модулю p.

Рассмотрим случай, когда p представляет собой двоичную экспоненту: $p = 2^{b\_p}$ и пусть $r = 2^{b\_r}$, $b\_r \le b\_p$, $v = \lceil b\_r \le b\_p \rceil$, $(\tilde{S}_{v-1}, \tilde{S}_{v-2}, \ldots, \tilde{S}_0)_r$ $(\tilde{S}_j \in \mathbf{Z}_r;\ j = \overline{0, v-1})$ – код числа $|\tilde{S}|_{p^r}$ в позиционной системе счисления (ПСС) с основанием r разрядностью v цифр. Тогда основой для восстановления секрета-оригинала S по маскирующему секрету $\tilde{S}$ может служить формула

$$S = \left|\tilde{S}\right|_p = \left|\tilde{S}\right|_{2^{b\_p}} = (s_{v-1}\, s_{v-2}\, \ldots\, s_0)_r \tag{8}$$

$$s_j = \begin{cases} \tilde{s}_j \ \text{при}\ j = \overline{0, v-2}, \\ \tilde{s}_{v-1}\left(\operatorname{mod}\left(\exp_2(b\_p - (v-1)b\_r)\right)\right) \ \text{при}\ j = v-1. \end{cases} \tag{9}$$

Из (8), (9) следует, что в случае $p = 2^{b\_p}$ решение поставленной задачи: $\mathbf{P}\_l = \{p_1, p_2, \ldots, p_l\}$, сводится к преобразованию минимально избыточного модулярного кода (МИМК) $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ в позиционный r-ичный код $(\tilde{s}_{v-1}, \tilde{s}_{v-2}, \ldots, \tilde{s}_0)_r$. Это преобразование может быть осуществлено по методу деления на двоичную экспоненту [2]: маскирующего секрета $\tilde{S} = (\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ на $r = 2^{b\_r}$ причем по упрощенному МИМА-алгоритму.

Преобразование минимально избыточного модулярного кода $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ в позиционный r-ичный код $(\tilde{s}_{v-1}, \tilde{s}_{v-2}, \ldots, \tilde{s}_0)_r$ числа $\tilde{S}$ методом деления на двоичную экспоненту $r = 2^{b\_r}$ базируется на операционном кортеже рекурсивного типа:

$$\langle \tilde{S}_0 = \tilde{S}, \tilde{s}_0 = \left|\tilde{S}_0\right|_r; \tilde{S}_1 = \left\lfloor \tilde{S}_0 / r \right\rfloor, \tilde{s}_1 = \left|\tilde{S}_1\right|_r; \tag{10}$$
$$\tilde{S}_2 = \left\lfloor \tilde{S}_1 / r \right\rfloor, \tilde{s}_2 = \left|\tilde{S}_2\right|_r; \ldots; \tilde{S}_{v-1} = \left\lfloor \tilde{S}_{v-2} / r \right\rfloor, \tilde{s}_{v-1} = \left|\tilde{S}_{v-1}\right|_r \rangle.$$

На j-й итерации процесса реализации (10) сначала формируется минимально избыточный модулярной код $(\tilde{\sigma}_1^{(j)}, \tilde{\sigma}_2^{(j)}, \ldots, \tilde{\sigma}_l^{(j)})$ ЦЧ $\tilde{S}_j$, а затем находится цифра $\tilde{s}_j$ его r-ичного позиционного кода путем расширения полученного минимально избыточного модулярного кода на модуль $r = 2^{b\_r}$ согласно правилу:

$$\tilde{S}_j=\left|\tilde{S}_j\right|_r=\left|\sum_{i=1}^{l-1}\left|P_{i,l-1}\tilde{\sigma}_{i,l-1}^{(j)}\right|_r+\left|P_{l-1}I_l(\tilde{S}_j)\right|_r\right|_r (j=\overline{0,\eta-1}), \quad (11)$$

где

$$\tilde{\sigma}_{i,l-1}^{(j)}=\left|P_{i,l-1}^{-1}\tilde{\sigma}_i^{(j)}\right|_{p_i}; \quad (12)$$

интервально-индексная характеристика $I_j(\tilde{S}_j)$ числа $\tilde{S}$ j определяется по расчетным соотношениям (5)–(7) при $\tilde{S}=\tilde{S}_j$ и $\tilde{\sigma}_i=\tilde{\sigma}_i^{(j)}$ $(i=\overline{1,l})$.

Что касается числа $\tilde{S}_j$, то в соответствии с (10) для цифр его минимально избыточного модулярного кода верна формула

$$\tilde{\sigma}_i^{(j)}=\left|\left[\frac{\tilde{S}_{j-1}}{r}\right]\right|_{p_i}=\begin{cases}\tilde{\sigma}_i \text{ при } j=0,\\ \left|\left|\tilde{\sigma}_i^{(j-1)}-\tilde{S}_{j-1}\right|_{p_i}\cdot|r^{-1}|_{p_i}\right|_{p_i} \text{ при } j=\overline{1,\nu-1}\end{cases} \quad (13)$$

$$(i=\overline{1,l}).$$

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ И ИХ ОБСУЖДЕНИЕ

3. Реализационный инструментарий метода деления на двоичную экспоненту для восстановления секрета-оригинала

Конкретный выбор способа компьютерной реализации базовых расчетных соотношений (10) – (13) предлагаемого метода модулярно-позиционного кодового преобразования в первую очередь определяется необходимостью оперирования в диапазонах больших чисел – в конечных кольцах по большим модулям $p_1, p_2, \ldots, p_n$. В частности, это относится к нормированным остаткам (12), вычетам (7) и (13).

Наряду с отмеченным фактором важной особенностью предлагаемой конфигурации метода деления на двоичную экспоненту $r=2^{b\_r}$ является использование значений параметра b_r, допускающих применение так называемой таблично-сумматорной вычислительной технологии [2]. В процедурах расширения минимально избыточного модулярного кода и получения неполных частных на итерациях рекурсивного процесса (10) (см. (11), (13)).

Пусть $m \in \mathbf{P}$, X – элемент множества $\mathbf{Z}_m$, C – произвольный целочисленный масштаб. Тогда представляя X в позиционной системе счисления с основанием $u=2^{b\_u}$ (b_u – натуральное число), то есть в виде

$$X=\sum_{h=0}^{\nu-1}x_h u^h (x_h \in \mathbf{Z}_u;\ \nu=\lceil b\_\mathrm{mod}/b\_u\rceil;\ b\_\mathrm{mod}=\lceil\log_2 m\rceil$$

– разрядность модуля m), будем иметь:

$$\chi = |CX|_m = \left|\sum_{h=0}^{v-1}\left|Cx_h u^h\right|_m^-\right|_m. \quad (14)$$

Для компьютерной реализации выражений типа (14) воспользуемся таблицами аддитивных компонент масштабируемой позиционной формы ЦЧ CX, представляемых симметрическими остатками по модулю m. В соответствии с (14) необходимые таблицы формируются по правилу

$$TACMPF\_h[x] = \left|Cxu^h\right|_m^-(x = \overline{0,u-1};\ h = \overline{0,v-1}). \quad (15)$$

Слагаемые модульные суммы (14) могут быть как положительными, так и отрицательными, поэтому в таблицах (15) их следует хранить в двоичном дополнительном коде.

Применяемый способ вычисления вычетов χ по (14) является двух шаговым. На первом шаге с помощью таблиц (15) находится сумма

$$\Sigma = \sum_{h=0}^{v-1} TACMPF\_h[x_h], \quad (16)$$

а на втором – Σ приводится к остатку по модулю m. Определим максимальную разрядность b_Σ (в битах) суммы Σ. Из (15), (16) следует, что для нижнего и верхнего пороговых значений Σ верны оценки: $\Sigma_{НП} = -v(m/2)$ и $\Sigma_{ВП} = v(m/2) - 1)$. Таким образом,

$$b\_\Sigma = \lceil \log_2(\Sigma_{ВП} - \Sigma_{НП}) \rceil \le b\_mod + b\_v \quad (17)$$

($b\_v = \log_2 v\rceil$ – разрядность величины v).

Как показывает (17), суммирование вычетов (15) согласно (16) должно проводиться на двоичном сумматоре, разрядность b_Σ которого превышает разрядность b_mod сумматора по модулю m на b_v бит.

Обозначая через $(x^{(\Sigma)}_{b\_\Sigma-1}\ x^{(\Sigma)}_{b\_\Sigma-2}\ \dots x^{(\Sigma)}_0)$ дополнительный двоичный код суммы Σ разрядностью b_Σ бит, разобьем его на две части – младшую

$$(x^{(\Sigma)}_{b\_mod-2}\ x^{(\Sigma)}_{b\_mod-3}\ \dots\ x^{(\Sigma)}_0)_2$$

и старшую – $(x^{(\Sigma)}_{b\_\Sigma-1}\ x^{(\Sigma)}_{b\_\Sigma-2}\ \dots x^{(\Sigma)}_{b\_mod-1})_2$,

которые имеют соответственно разрядности $b\,mod - 1$ и $b\_v + 1$ бит, и принимая во внимание равенство $\Sigma = \sum_{h=0}^{b\_\Sigma-2} x_h^{(\Sigma)} 2^h - x^{(\Sigma)}_{b\_\Sigma-1} 2^{b\_\Sigma-1}$,

Заключаем, что для выполнения преобразования $\Sigma \to |\Sigma|_m$ может быть применена формула

$$\chi = |\Sigma|_m = |\Sigma_0 + \Sigma_1|_m, \tag{18}$$

где

$$\Sigma_0 = \sum_{h=0}^{b\_\mathrm{mod}-2} x_h^{(\Sigma)} 2^h; \tag{19}$$

$$\Sigma_1 = \left|\sum_{h=b\_\mathrm{mod}-1}^{b\_\Sigma-2} x_h^{(\Sigma)} 2^h - x_{b\_\Sigma-1}^{(\Sigma)} 2^{b\_\Sigma-1}\right|_m \tag{20}$$

Значения b-битового вычета Σ_1 по модулю m рассчитываются согласно (20) предварительно и записываются в табличную память – в таблицу TRes_MP по правилу

$$TRes\_MP[(x_{b\_\Sigma-1}^{(\Sigma)}\ x_{b\_\Sigma-2}^{(\Sigma)}\ \dots x_{b\_\mathrm{mod}-1}^{(\Sigma)})_2] = \Sigma_1. \tag{21}$$

Емкость таблицы (21) составляет 2^{b_ν} слов разрядностью b_mod бит.

Описанный метод тривиальным образом распространяется и на случай принадлежности входного ЦЧ X и выходного вычета Σ конечным кольцам по разным модулям. В частности, это относится к вычетам

$$R_{i,l}\left(\tilde{\sigma}_{i,l-1}^{(j)}\right) = \left|-p_i^{-1}\tilde{\sigma}_{i,l-1}^{(j)}\right|_{p_l} (\tilde{\sigma}_{i,l-1}^{(j)} \in \mathbf{Z}_{p_i}),$$

то есть к вычетам второго каскада операции формирования слагаемых

$R_{i,l}\left(\tilde{\sigma}_i^{(j)}\right)$ модульной суммы вида (6) (см. (7), (12)).

Остановимся теперь на особенностях предлагаемой компьютерной реализации расчетных соотношений (8) и (12) операции расширения минимально избыточного модулярного кода $(\tilde{\sigma}_1^{(j)}, \tilde{\sigma}_2^{(j)}, \dots, \tilde{\sigma}_l^{(j)})$ числа $\tilde{S}_j$ на модуль $r - 2^{b\_\nu}$. Отметим, что исходными данными j-й итерации рекурсивного процесса (7) деления секрета-маски $\tilde{S}$ на r служат минимально избыточный модулярный код $(\tilde{\sigma}_1^{(j-1)}, \tilde{\sigma}_2^{(j-1)}, \dots, \tilde{\sigma}_i^{(j-1)})$ ЦЧ $\tilde{S}_{j-1}$ и цифра $\tilde{s}_{j-1}$ его r-ичного кода $(\tilde{s}_{\eta-1}, \tilde{s}_{\eta-2}, \dots \tilde{s}_0)$. Следуя лемме Эвклида из теории делимости, представим i-ю цифру $\tilde{\sigma}_i^{(j-1)}$ минимально избыточного модулярного кода числа $\tilde{S}_{j-1}$ в виде

$$\tilde{\sigma}_i^{(j-1)} = \left|\tilde{\sigma}_i^{(j-1)}\right|_r + \left\lfloor\frac{\tilde{\sigma}_i^{(j-1)}}{r}\right\rfloor r. \tag{22}$$

С учетом (22) для всех $j = \overline{1, \eta - 1}$ из (12) получаем:

$$\tilde{\sigma}_i^{(j)} = \left| \left| \frac{\tilde{\sigma}_i^{(j-1)}}{r} \right| + \frac{\left| \tilde{\sigma}_i^{(j-1)} \right|_r - \tilde{s}_{j-1}}{r} \right|_{p_i} \Bigg|_{p_i} \quad (23)$$

Для компьютерной реализации выражение (23) более удобно, чем (12). Числитель $d_i^{(j-1)} = |\tilde{\sigma}_i^{(j-1)}| r - \tilde{s}_{j-1}$ дроби $f_i^{(j-1)} = d_i^{(j-1)}/r$ из (23) удовлетворяет неравенству $-(r-1) \le d_i^{(j-1)} \le r-1$, поэтому разность $d_i^{(j-1)}$ полностью определяется своим дополнительным $(b\_r + 1)$-битовым кодом или симметрическим остатком $\delta_i^{(j-1)} = |d_i^{(j-1)}|_{2^{b\_r+1}} = |d_i^{(j-1)}|_{2r}$ по модулю $2r$. Благодаря небольшой разрядности r, а значит и $\sigma_i^{(j-1)}$, величина $\varphi_i^{(j-1)} = |\delta_i^{(j-1)}/r|_{p_i}$ может быть получена табличным способом. Необходимая таблица генерируется по правилу

$$TRes\_f\_i[\delta\ ] = \left| \frac{\delta}{r} \right|_{p_i} (\delta = \overline{-r, r-1}). \quad (24)$$

Таким образом, вычисление i-й цифры МИМК числа $\tilde{S}_j$ по (23) с использованием таблицы (24) сводится к выделению из двоичного кода цифры $\sigma_i^{(j-1)}$ ЧЧ $\tilde{S}_{j-1}$ старшей $((b\_mod\_i)\text{-}r)$-битовой части $\tilde{\sigma}_i^{(j-1)}/r$ числа $\tilde{S}_{j-1}$, извлечению из таблицы $TRes\_f\_i$ по получаемому симметрическому остатку $\delta_i^{(j-1)} = |d_i^{(j-1)}|_{2r}$ величины $\varphi_i^{(j-1)} = TRes\_f\_i[\delta_i^{(j-1)}]$ и выполнению операции сложения по модулю p_i над вычетами $\|\tilde{\sigma}_i^{(j-1)}/r\|_{p_i}$ и $\varphi_i^{(j-1)}$. Отметим, что емкость таблицы $TRes\_f\_i$ составляет $r+1$ слов разрядностью $b\_mod\_i = \lceil log\, 2p_i \rceil$ бит.

Что касается базового расчетного соотношения (8) операций расширения МИМК $(\tilde{\sigma}_i^{(j)}, \tilde{\sigma}_i^{(j)}, \ldots, \tilde{\sigma}_l^{(j)})$ чисел $\tilde{S}_j$, то для его реализации также применима таблично-сумматорная вычислительная технология. Это обеспечивается выбором приемлемого по величине модуля r. Основой представляемого подхода к выполнению операций расширения минимально избыточного модулярного кода служат таблицы остатков по модулю r слагаемых интервально-модулярной формы ЧЧ. Элементы этих таблиц определяются по формулам:

$$TRes\_AIMFi[\sigma] = \left| |P_{i,l-1}|_r \sigma \right|_r (\sigma = \overline{0, r-1};\ i = \overline{1, l}), \quad (25)$$

$$TRes_{AIMFl[I]} = \left| |P_{l-1}|_r I \right|_r (I = \overline{0, r-1}). \quad (26)$$

Используя (13), (9), а также (25), (26) запишем соотношение (8) в виде:

$$\tilde{s}_j = \left| \sum_{i=1}^{l-1} TRes\_AIMFi[\left| \tilde{\sigma}_{i,l-1}^{(j)} \right|_r] + TRes\_AIMFl[\left| \hat{I}_l(\tilde{S}_j) \right|_r] + C\_II \right|_r, \quad (27)$$

где C_II – поправка для интервального индекса числа $\tilde{S}_j$, которое в соответствии с (9) вычисляется по формуле

$$C\_II=(1-sn(\hat{I}_l(\tilde{S}_j)-p_0)\cdot|-P_l|_r(P_l=P_{l-1}p_l); \quad (28)$$

sn – знаковая функция вида

$$sn(a)=\begin{cases}0, \text{если} a\geq 0,\\ 1, \text{если } a<0.\end{cases}$$

Отметим, что вычеты $\tilde{\sigma}^{(j)}_{i,l-1}$ находятся в процессе вычисления интервально-индексной характеристики $\hat{I}_l(\tilde{S}_j)$. Так как *r* является двоичной экспонентой, то получение остатков $|\tilde{\sigma}^{(j)}_{i,l-1}|_r$ и $|\hat{I}_l(\tilde{S}_j)|_r$, как аргументов для таблиц *TRes_AIMFi* и *TRes_AIMFl* в (27), а также остатка $|-P_l|_r$ сводится к выделению из двоичных кодов соответствующих ЦЧ *b_r*-битовых младших частей. Что касается интервально-индексной поправки *C_II*, то согласно (28) для её формирования требуется определить знак разности $\hat{I}_l(\tilde{S}_j) - p_0$. Это может быть осуществлено с помощью (1+*b*_mod_*l*)-битового сумматора. К важным факторам, способствующим упрощению декодирующей процедуры на основе метода деления на двоичную экспоненту, является простота вычисления модульной суммы (27). Компьютерная реализация (27) производится на *b_r*-битовых сумматорах причем без контроля переполнений.

Сравнительный анализ эффективности разработанного метода с неизбыточными версиями показывает, что по производительности он превосходит аналоги как минимум в l(19l-3)/(22l-6) раз. В частности, при l = 7 ÷ 40 достигается (6 ÷ 35)-кратное повышение производительности.

ВЫВОДЫ

Основные результаты представленных в статье исследований состоят в нижеследующем.

Изложены базовые концептуальные положения нового подхода к построению модулярных пороговых криптосхем разделения секрета с маскирующим преобразованием. Главными отличительными особенностями данного подхода являются применение согласованного с пороговым принципом минимально избыточного модулярного кодирования и использование для разработки метода выполнения декодирующей операции рекурсивной схемы деления на двоичную экспоненту, кратную модулю р кольца вычетов, содержащего секрет-оригинал. Это позволяет минимизировать необходимые временные и аппаратурные затраты с сохранением максимального уровня криптостойкости, свойственного схемам исследуемого класса.

Основной фактор, определяющий эффективность созданного метода восстановления секрета-оригинала по минимально избыточным

модулярным кодам секрета-маски, заключается в существенном упрощении поитерационных операций расширения кода на выбранную двоичную экспоненту. Главным образом это обусловлено l-кратным уменьшением сложности вычисления базовой интегральной характеристики кода (интервального индекса) по сравнению с традиционно применяемыми характеристиками. Отмеченное обстоятельство позволяет достичь повышения производительности предлагаемого метода в сравнении с аналогами не менее, чем в $\frac{l(19l-3)}{2(11l-3)}$ раз (l – число абонентов, реконструирующих секрет-оригинал).

Показано, что для компьютерной реализации разработанного метода успешно может быть применена таблично-сумматорная вычислительная технология. Для преобразований с ее помощью масштабируемых вычетов по большим модулям осуществляется приемлемая модулярная декомпозиция взвешенных позиционных форм вычетов с последующим табулированием результирующих аддитивных компонент. При этом получение искомого вычета сводится к извлечению из таблиц необходимых элементов и их суммированию по соответствующим модулям. Используемая таблично-сумматорная технология отличается высокой гибкостью.

Благодарность. Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-70023.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Червяков Н.И. и др. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: Физматлит, 2012. 280 с.
2. Червяков Н.И., Коляда А.А., Ляхов П.А. и др. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. М.: ФИЗМАТЛИТ, 2017. 400 с.
3. Харин Ю.С. и др. Криптология: учебник // Мн.: БГУ, 2013. 511 с.
4. Shamir Adi. How to share a secret // Communications of the ACM. 1979. Vol. 22, №11. P. 612-613.
5. Blakley G.R. Safe guarding cryptographic keys // Proc. Of the 1979 AFIPS national computer conference. Montvale: AFIPS press, 1979. P. 313-317.
6. Mignotte M. How to share a secret // Lecture notes in computer science. 1983. Vol. 149. P. 371–375.
7. Asmuth C.A., Bloom J. A modular appoach to key safe guarding // IEEE Tras. On information theory. 1983. Vol. 29, N. 2. P. 208–210.

8. Шнайер Б. Алгоритмы разделения секрета. Схема интерполяционных полиномов Лагранжа // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Н.: Триумф, 2002. С. 588-589.
9. Shiong Jian Shyu, Ying-Ru Chen. Treshold secret image sharing by Chinese remainder theorem // IEEE Asia – Pacific Services Computing conference. Yilan, Taiwan, 9–12 dec., 2008. Vol. 1. P. 1332–1337.
10. Bahramian Mojtaba, Khadijeh Eslami. An efficient threshold verifiable multisecret sharing scheme using generalized Jacobean of elliptic curves // Journal of algebraic structures and their applications. 2017. Vol. 4, Iss. 2. P. 45–55.
11. Jia Xingxing, 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. P. 13–30.
12. Коляда А.А., Кучинский П.В., Червяков Н.И. Пороговый метод разделения секрета на базе избыточных модулярных вычислительных структур // Информационные технологии. Т. 25, № 9. М.: Новые технологии, 2019. С. 553–561.
13. Коляда А.А., Пак И.Т. Модулярные структуры конвейерной обработки цифровой информации // Мн.: Университетское, 1992. 256 с.
14. Коляда А.А. Обобщенная интегрально-характеристическая база модулярных систем счисления // Информационные технологии. 2017. Т. 23, №9. М.: Новые технологии, 2017. С. 641–649.
15. Ananda Mohan P.V. Residue number systems: Theory and applications. Basel: Birghauser, Mathematics, 2016. 351 p.

References

1. Chervjakov N.I. The use of artificial neural networks and the residual class system in cryptography. Moscow: FIZMATLIT Publ., 2012, 280 p. (in Russian)
2. Chervjakov N.I., Koljada A.A., Ljahov P.A. ets. Modular arithmetic and its applications in infocommunication technologies. Moscow: FIZMATLIT Publ., 2017, 400 p. (in Russian)
3. Kharin Yu.S. and other. Cryptology: a textbook // Minsk: BSU, 2013. 511 p. (in Russian)
4. Shamir Adi. How to share a secret // Communications of the ACM. 1979. Vol. 22, N. 11. P. 612–613.
5. Blakley G.R. Safe guarding cryptographic keys // Proc. Of the 1979 AFIPS national computer conference. Montvale: AFIPS press, 1979. P. 313-317.
6. Mignotte M. How to share a secret // Lecture notes in computer science. 1983. Vol. 149. P. 371–375.
7. Asmuth C.A., Bloom J. A modular appoach to key safe guarding // IEEE Tras. On information theory. 1983. Vol. 29, N. 2. P. 208-210.
8. Schneier B. Secret Secretion Algorithms. Scheme of Lagrange interpolation polynomials, Prikladnaya kriptografiya. Protokoly, al-

goritmy, iskhodnyye teksty па yazyke Si. N.: Triumf, 2002. Pp. 588-589.
9. Shiong Jian Shyu, Ying-Ru Chen. Treshold secret image sharing by Chinese remainder theorem // IEEE Asia – Pacific Services Computing conference. Yilan, Taiwan, 9–12 dec., 2008. Vol. 1. P. 1332–1337.
10. Bahramian Mojtaba, Khadijeh Eslami. An efficient threshold verifiable multisecret sharing scheme using generalized Jacobean of elliptic curves // Journal of algebraic structures and their applications. 2017. Vol. 4, Iss. 2. P. 45–55.
11. Jia Xingxing, 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. P. 13–30.
12. Kolyada A.A., Kuchinsky P.V., Chervyakov N.I. The threshold secret sharing method based on redundant modular computing structures, Informatsionnyye tekhnologii. Vol. 25, no 9. M.: Novyye tekhnologii, 2019. Pp. 553–561. (in Russian)
13. Koljada A. A., Pak I. T. Modular structures of conveyor processing of digital information, Minsk, Universitetskoe, 1992, 256 p. (in Russian)
14. Kolyada A.A. Generalized integral-characteristic base of modular number systems, Informatsionnyye tekhnologii. 2017, Vol.23, no. 9, M.: Novyye tekhnologii, 2017, pp. 641–649. (in Russian)
15. Ananda Mohan P.V. Residue number systems: Theory and applications. Basel: Birghauser, Mathematics, 2016.351 p.

Поступило в редакцию 28.08.2020,
принята к публикации 01.09.2020

СВЕДЕНИЯ ОБ АВТОРАХ

Коляда Андрей Алексеевич, д.ф.-м.н., доц., главный научный сотрудник лаборатории специализированных вычислительных систем, Научно-исследовательское учреждение “Институт прикладных физических проблем имени А.Н. Севченко” Белорусского государственного университета (НИИПФП им. А.Н. Севченко БГУ)
Тел.: 8-10-375-17-212-47-45
E-mail: razan@tut.by

Бабенко Михаил Григорьевич кандидат физико-математических наук, доцент, **Северо-Кавказский федеральный университет**
Тел.: (8652) 95-68-00
E-mail: whbear@yandex.ru

Протасеня Стелла Юрьевна, научный сотрудник лаборатории специализи-

рованных вычислительных систем, Научно-исследовательское учреждение “Институт прикладных физических проблем имени А.Н. Севченко” Белорусского государственного университета (НИИПФП им. А.Н. Севченко БГУ).
Тел.: 8-10-375-17-212-47-45
E-mail: estellita@mail.ru

ABOUT THE AUTHORS

A.A. Kolyada, Doctor of Physical and Mathematical Sciences, associate professor of Scientific Research Institution“Institute of Applied Physical Problems named after A.N. Sevchenko” of the Belarusian State University
tel.: 8-10-375-17-212-47-45
E-mail: razan@tut.by

M.G. Babenko Candidate of Physical and Mathematical Sciences, Associate Professor, North-Caucasus federal university
tel.: (8652) 95-68-00
E-mail: mgbabenko@ncfu.ru

S.Yu. Protasenia, scientist, Laboratory of Specialized Computational Systems, Research Institution“Institute of Applied Physical Problems named after A.N. Sevchenko” of the Belarusian State University
tel.: 8-10-375-17-212-47-45
E-mail: estellita@mail.ru