УДК 004.9, 004.94, 004.56 DOI: 10.17587/it.27.77-88

А. А. Коляда, д-р физ.-мат. наук, доц., e-mail: razan@tut.by,
П. В. Кучинский, д-р физ.-мат. наук, доц., e-mail: niipfp@bsu.by,
С. Ю. Протасеня, мл. науч. сотр., estellita@mail.ru,
Научно-исследовательское учреждение "Институт прикладных физических проблем имени А. Н. Севченко" Белорусского государственного университета, Минск

Метод и алгоритм выполнения декодирующей операции в пороговом криптомодуле разделения секрета с использованием минимально избыточной модулярной системы счисления

Представлена новая разработка метода и алгоритма выполнения в пороговом криптомодуле разделения секрета с маскирующим преобразованием декодирующей операции. Для решения рассматриваемой задачи применены рекурсивная схема деления на двоичную экспоненту и вычислительная технология на диапазонах больших чисел таблично-сумматорного типа, основанная на минимально избыточной модулярной арифметике (МИМА). Отличительной особенностью развиваемого подхода является использование в качестве области принадлежности секрета-оригинала конечных колец вычетов по модулям, имеющим вид степеней числа 2. Это существенно уменьшает сложность результирующей декодирующей МИМА-процедуры. Осуществляемая в рамках базовой технологии декомпозиция масштабируемых вычетов по большим модулям позволяет эффективно отображать реализуемый вычислительный процесс на наборы легко реализуемых операций извлечения данных из табличной памяти и их суммирования, обеспечивая высокий уровень производительности, однородности и унификации базовых структур. По быстродействию синтезированный декодирующий МИМА-алгоритм превосходит неизбыточные аналоги как минимум в $\frac{l(19l-3)}{22l-6}$ *раз (l — число абонентов, восстанавливающий 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*

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 сеанса связи ($2 \leqslant t \leqslant l \leqslant n$; t — пороговое число абонентов). При этом группы абонентов числом $k < t$ реконструировать секрет-оригинал по соответствующим компонентам не могут. Криптографический ключ фактически представляет собой главный секрет во всем процессе шифрования. Механизм ключей предполагает использование специальной операционной базы, обеспечивающей генерирование и надежное хранение ключей, декомпозицию ключей на компоненты в целях распределения их между абонентами системы, а также восстановление ключей-оригиналов по их составным частям. 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). Модулярное кодирование служит простым средством декомпозиции (разделения) секрета на составные части и позволяет минимизировать затраты при оперировании в диапазонах больших чисел. 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 [1, 2, 12—15]. Настоящая статья посвящена разработке метода и алгоритма выполнения декодирующей операции в пороговом криптомодуле разделения секрета, базирующемся на минимально избыточной модулярной арифметике (МИМА) [2, 12—14]. Применение вычислительной МИМА-технологии на диапазонах больших чисел для решения рассматриваемой задачи позволяет в значительной мере минимизировать необходимые временные и аппаратурные затраты.

1. Постановка задачи и методы ее решения

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;

$\mathbf{Z}_m = \{0, 1, ..., m-1\}$ и $\mathbf{Z}_m^- = \left\{-\frac{m}{2}, -\frac{m}{2}+1, \ldots, \frac{m}{2}-1\right\}$ — множества наименьших неотрицательных и абсолютно наименьших вычетов (остатков) по натуральному модулю $m > 1$;

$A \equiv B \pmod{m}$ — условная запись равноостаточности по модулю m целых чисел A и B;

$\chi = |A/B|_m = (A/B) \pmod{m}$ и $\chi^- = |A/B|_m^-$ — элементы соответственно множеств $\mathbf{Z}_m$ и $\mathbf{Z}_m^-$, удовлетворяющие сравнениям $B\chi \equiv A \pmod{m}$ и $B\chi^- \equiv A \pmod{m}$ ($B \neq 0$, НОД (B, m) = 1);

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

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

Пусть $p_1, p_2, ..., p_n$ — упорядоченные по возрастанию попарно простые большие натуральные числа ($n > 1$); $P_i = \prod_{s=1}^{i} p_s$; $\_P_j = \prod_{s=1}^{j} p_{n-s+1} = /P_{n-j}$ ($i, j = \overline{1,n}$); $\mathbf{P} = \{p_1, ..., p_2, ..., p_n\}$; $\mathbf{I}\_l = \{\forall(i_1, i_2, ..., i_l) | 1 \leqslant i_1 < i_2 < ... < i_l \leqslant n;\ 2 \leqslant t \leqslant l \leqslant n\}$

(t — фиксированное натуральное число); $I\_l = (i_1, i_2, ..., i_l)$ — произвольный элемент множества $\mathbf{I}\_l$; $\mathbf{P}_{I\_l} = \{p_{i_1}, p_{i_2}, \ldots, p_{i_l}\}$; $P_{I\_l} = \prod_{j=1}^{l} p_{i_j}$.

Концептуальную основу (t, n)-пороговой схемы разделения секрета с модулярным базисом $\mathbf{P} = \mathbf{P}\_n = \{p_1, p_2, ..., p_n\}$, 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 $p_1, p_2, ..., p_n$).

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

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

где C — псевдослучайный целочисленный параметр.

Цифры $\tilde{\sigma}_i = |\tilde{S}|_{p_i} = |\sigma_i + |Cp|_{p_i}|_{p_i}$ ($\sigma_i = |S|_{p_i}$; $i = \overline{1, n}$) получаемого кода $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_n)$ рассматриваются как долевые (частичные) секреты, принадлежащие одноименным абонентам.

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

Построение теоретико-методологической, алгоритмической и инструментальной базы, обеспечивающей оптимальную реализацию перечисленных основополагающих принципов порогового разделения секретной информации в распределенных системах обработки данных является важнейшим направлением развития технологии активной безопасности [1—3].

Представляемые исследования нацелены на решение задачи восстановления секрета-оригинала S по кодам $(\tilde{\sigma}_{i_1}, \tilde{\sigma}_{i_2}, \ldots, \tilde{\sigma}_{i_l})$ 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 результирующей 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]. Применяемый методологический и реализационный инструментарий адаптирован к решаемой проблеме.

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 в соответствии с пунктом **В** отвечают группам абонентов числом l. Без нарушения общности изложение дальнейшего материала в целях упрощения употребляемых обозначений преимущественно проводится на примере группы абонентов, за которыми закрепляются основания $p_1, p_2, ..., p_l$ набора $\mathbf{P}\_l$ — представителя множества $\mathbf{P}_{\mathbf{I}\_l}$ с $I\_l = (1, 2, ..., l) \in \mathbf{I}\_l$. Долевые секреты, принадлежащие абонентам указанной группы, являются цифрами кода $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ МСС с модулями $p_1, p_2, ..., p_l$ 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 $P_{i,l-1} = \dfrac{P_{l-1}}{p_i}$, $P_{l-1} = \prod_{s=1}^{l-1} p_s$;

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

$I_l(\tilde{S})$ — 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 $\mathbf{Z}_P = \{0, 1, ..., P - 1\}$ ($P = p_0P_{l-1}$; p_0 — вспомогательный модуль) полностью определялся вычетом $\hat{I}_l(\tilde{S}) = \left|I_l(\tilde{S})\right|_{p_l}$, необходимо и достаточно выполнения условия

$$p_l \geqslant 2p_0 + l - 2 \ (p_0 \geqslant l - 2). \tag{4}$$

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

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

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

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

Главное преимущество МИМСС с базисами $\mathbf{P}_{\_l}$ ($I\_l \in \mathbf{I}\_l$) 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. Пусть $p_1, p_2, ..., p_n$ — упорядоченные по возрастанию попарно простые натуральные числа, составляющие базис $\mathbf{P} = \mathbf{P}\_n$ модулярной схемы разделения секрета, p — взаимно простой с $p_1, p_2, ..., p_n$ модуль кольца $\mathbf{Z}_p$ принадлежности секрета-оригинала S, который разделяется между n абонентами путем наделения их долевыми секретами $\tilde{\sigma}_i = |\tilde{S}|_{p_i}$ $(i = \overline{1,n})$, получаемыми в результате декомпозиции применяемой функции маскирования: $\tilde{S} = S + Cp$ (C — псевдослучайный целочисленный параметр). Для того чтобы любые l абонентов ($2 \leqslant t \leqslant l \leqslant n$; 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:

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

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 $p_0 \leqslant p_t - t + 2$;

$$\mathbf{C} = \{C_{\text{нп}}, C_{\text{нп}} + 1, \ldots, C_{\text{вп}}\}$$

$$(C_{\text{нп}} = \left\lfloor \tilde{S}_{\text{нп}}/p \right\rfloor; \quad C_{\text{вп}} = \left\lfloor \tilde{S}_{\text{вп}}/p \right\rfloor);$$

$$\mathbf{C}_p = \{\forall\, C \in \mathbf{C} \mid S + Cp \in (\tilde{S}_{\text{нп}}; \tilde{S}_{\text{вп}});$$

$$Q(\tilde{S}; j_1, j_2, \ldots, j_k) = \left\lfloor \frac{\tilde{s}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor$$

$(1 \leqslant j_1 < j_2 \ldots < j_k \leqslant n;\ 2 \leqslant k < t)\}$, p — делитель ЦЧ Q.

Использование в качестве допустимой области значений для псевдослучайного параметра C множества $\tilde{\mathbf{C}}$, как того требует условие $C \in \tilde{\mathbf{C}}$ теоремы 2, обеспечивает результирующей МИМА-криптосхеме максимальный уровень криптостойкости, свойственный схемам рассматриваемого класса.

Из соотношения (1) вытекает равенство $S = |\tilde{S}|_p$, указывающее на то, что для получения S по $\tilde{S}$ в принципе достаточно ЦЧ $\tilde{S}$ привести к остатку по модулю p. Но так как p — большое число, то в общем случае данная операция весьма трудоемка. Поэтому для ее выполнения целесообразно воспользоваться процедурами, в которых применяются модули p частного вида.

В статье рассматривается случай, когда p представляет собой двоичную экспоненту разрядностью b_p бит, т. е. имеет вид $p = 2^{b\_p}$, и пусть $r = 2^{b\_r}$, $b\_r \leqslant b\_p$, $\nu = \lceil b\_p/b\_r \rceil$, $(\tilde{s}_{\nu-1}\ \tilde{s}_{\nu-2} \ldots \tilde{s}_0)_r$ ($\tilde{s}_j \in \mathbf{Z}_r$; $j = \overline{0, \nu-1}$) — код числа $|\tilde{S}|_{r^\nu}$ в позиционной системе счисления (ПСС) с основанием r разрядностью ν цифр. Тогда основой для восстановления секрета-оригинала S по маскирующему секрету $\tilde{S}$ может служить формула

$$S = |\tilde{S}|_p = |\tilde{S}|_{2^{b\_p}} = (s_{\nu-1}\ s_{\nu-2} \ldots s_0)_r, \qquad (8)$$

где

$$s_j = \begin{cases} \tilde{s}_j \text{ при } j = \overline{0, \nu-2}, \\ \tilde{s}_{\nu-1}(\mathrm{mod}(\exp_2(b_p - (\nu-1)b\_r))) \\ \text{при } j = \nu - 1. \end{cases} \qquad (9)$$

Из соотношений (8), (9) следует, что в случае $p = 2^{b\_p}$ решение поставленной задачи для группы пользователей, отвечающей рассматриваемому набору оснований $\mathbf{P}\_l = \{p_1, p_2, ..., p_l\}$, сводится к преобразованию минимально избыточного модулярного кода (МИМК) $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ в позиционный r-ичный код $(\tilde{s}_{\nu-1}\ \tilde{s}_{\nu-2} \ldots \tilde{s}_0)_r$. 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.

2. Метод деления на двоичную экспоненту с применением МИМСС

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

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

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

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

где

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

интервально-индексная характеристика $I_l(\tilde{S}_j)$ 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

$$\tilde{\sigma}_i^{(j)} = \left\| \frac{\tilde{S}_{j-1}}{r} \right\|_{p_i} =$$
$$= \begin{cases} \tilde{\sigma}_i \text{ при } j = 0, \\ \left| \left| \tilde{\sigma}_i^{(j-1)} - \tilde{s}_{j-1} \right|_{p_i} |r^{-1}|_{p_i} \right|_{p_i} \text{ при } j = \overline{1, \nu-1} \end{cases} \qquad (13)$$
$$(i = \overline{1, l}).$$

Конкретный выбор способа компьютерной реализации базовых расчетных соотношений (10)—(13) рассматриваемого 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), т. е. в виде $X = \sum_{h=0}^{v-1} x_h u^h$ ($x_h \in \mathbf{Z}_u$; $v = \lceil b\_mod/b\_u \rceil$; $b\_mod = \lceil \log_2 m \rceil$ — разрядность модуля m), будем иметь:

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

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

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

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 выражению (14) является двухшаговым. На первом шаге с помощью таблиц (15) находится сумма

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

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

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

($b\_v = \lceil \log_2 v \rceil$ — 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 $(x_{b\_\Sigma-1}^{(\Sigma)} x_{b\_\Sigma-2}^{(\Sigma)} \ldots x_0^{(\Sigma)})_2$ дополнительный двоичный код суммы Σ разрядностью b_Σ бит, разобьем его на две части — младшую $(x_{b\_mod-2}^{(\Sigma)} x_{b\_mod-3}^{(\Sigma)} \ldots x_0^{(\Sigma)})_2$ и старшую $(x_{b\_\Sigma-1}^{(\Sigma)} x_{b\_\Sigma-2}^{(\Sigma)} \ldots x_{b\_mod-1}^{(\Sigma)})_2$, которые имеют соответственно разрядности $b\_mod - 1$ и $b\_v + 1$ бит, принимая во внимание равенство $\Sigma = \sum_{h=0}^{b\_\Sigma-2} x_h^{(\Sigma)} 2^h - x_{b\_\Sigma-1}^{(\Sigma)} 2^{b\_\Sigma-1}$.

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

$$\chi = |\Sigma|_m = |\Sigma_0 + \Sigma_1|_m, \qquad (18)$$

где

$$\Sigma_0 = \sum_{h=0}^{b\_mod-2} x_h^{(\Sigma)} 2^h; \qquad (19)$$

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

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

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

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

Описанный метод тривиальным образом распространяется и на случай принадлежности входного ЦЧ X и выходного вычета χ конечным кольцам по разным модулям. В частности, это относится к вычетам $R_{i,l}(\tilde{\sigma}_{i,l-1}^{(j)}) = \left| -p_i^{-1} \sigma_{i,\,l-1}^{(j)} \right|_{p_l}$ $(\sigma_{i,l-1}^{(j)} \in \mathbf{Z}_{p_i})$, т. е. к вычетам второго каскада операции формирования слагаемых $R_{i,l}(\tilde{\sigma}_i^{(j)})$ 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 $r = 2^{b\_r}$. Отметим, что исходными данными j-й итерации рекурсивного процесса (7) деления секрета-маски $\tilde{S}$ на r служат минимально избыточный модулярный код $(\tilde{\sigma}_1^{(j-1)}, \tilde{\sigma}_2^{(j-1)}, \dots, \tilde{\sigma}_l^{(j-1)})$ ЦЧ $\tilde{S}_{j-1}$ и цифра $\tilde{s}_{j-1}$ его r-ичного кода $(\tilde{s}_{v-1}\, \tilde{s}_{v-2} \dots \tilde{s}_0)_r$. 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

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

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

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

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 $f_i^{(j-1)} = \dfrac{d_i^{(j-1)}}{r}$ из (23) удовлетворяет неравенству $-(r-1) \leqslant d_i^{(j-1)} \leqslant r - 1$, 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 $\delta_i^{(j-1)}$, величина $\varphi_i^{(j-1)} = \left| \dfrac{\delta_i^{(j-1)}}{r} \right|_{p_i}$ может быть получена табличным способом. Необходимая таблица генерируется по правилу

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

Таким образом, вычисление i-й цифры МИМК числа $\tilde{S}_j$ по формуле (23) с использованием таблицы (24) сводится к выделению из двоичного кода цифры $\sigma_i^{(j-1)}$ ЦЧ $\tilde{S}_{j-1}$ старшей $((b\_mod\_i)\text{-}r)$-битовой части $\left\lfloor \tilde{\sigma}_i^{(j-1)} / r \right\rfloor$ 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 $\left\| \dfrac{\tilde{\sigma}_i^{(j-1)}}{r} \right\|_{p_i}$ и $\varphi_i^{(j-1)}$. Отметим, что емкость таблицы $TRes\_f\_i$ составляет $r + 1$ слов разрядностью $b\_mod\_i = \lceil \log_2 p_i \rceil$ бит.

Что касается базового расчетного соотношения (8) операций расширения МИМК $(\tilde{\sigma}_1^{(j)}, \tilde{\sigma}_2^{(j)}, \dots, \tilde{\sigma}_l^{(j)})$ 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 ЦЧ. Элементы этих таблиц определяются по формулам

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

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

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

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

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

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

sn — знаковая функция вида

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

Отметим, что вычеты $\tilde{\sigma}_{i,l-1}^{(j)}$ находятся в процессе вычисления интервально-индексной характеристики $\hat{I}_l(\tilde{S}_j)$. Так как *r* является двоичной экспонентой, то получение остатков $|\tilde{\sigma}_{i,l-1}^{(j)}|_r$ 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 формуле (28) для ее 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. Важным фактором, способствующим упрощению декодирующей процедуры на основе метода деления на двоичную экспоненту, является простота вычисления модульной суммы (27). Компьютерная реализация (27) осуществляется на *b_r*-битовых сумматорах, причем без контроля переполнений.

3. Алгоритм выполнения декодирующей операции

Изложенное позволяет сформулировать нижеследующий алгоритм восстановления секрета-оригинала с применением метода деления на двоичную экспоненту.

Параметрическая база алгоритма:

— $\mathbf{P} = \{p_1, p_2, ..., p_n\}$ — базис (*t*,*n*)-порогового МИМА-криптомодуля разделения секрета, состоящий из $n > t$ упорядоченных по возрастанию попарно простых оснований (*t* — пороговое число абонентов);

— p_0 — вспомогательный модуль, удовлетворяющий ограничению $\_qp_t \leqslant p_0 \leqslant p_t - t + 2$ $(0 \leqslant \_q \leqslant 1)$;

— *p* — модуль кольца $\mathbf{Z}_p = \{0, 1, ..., p - 1\}$ принадлежности секрета-оригинала *S*, взаимно простой с $p_1, p_2, ..., p_n$ и имеющий разрядность *b_p* битов;

— $\tilde{\mathbf{S}} = \{\lceil \_P_{t-1}pq \rceil, \lceil \_P_{t-1}pq \rceil + 1, ..., \lfloor \_qP_t \rfloor - 1\}$ — рабочий диапазон криптомодуля по маскирующему секрету $\tilde{S} = S + Cp$ ($\_P_{t-1} = \prod_{s=1}^{t-1} p_{n-s+1}$; $q \geqslant p^{-1}$; $P_t = \prod_{s=1}^{t} p_s$; $S \in \mathbf{Z}_p$; $C \in \tilde{\boldsymbol{C}}$; $\tilde{\boldsymbol{C}}$ — множество допустимых значений для псевдослучайного параметра *C* (см. теорему 2));

— $\mathbf{P}\_l = \{\forall\{p_{i_1}, p_{i_2}, ..., p_{i_l}\} \mid 1 \leqslant i_1 < i_2 < ... < i_l \leqslant n; t \leqslant l \leqslant n\}$ — множество *l*-компонентных наборов оснований из $\mathbf{P}$, распределяемых между группами абонентов, которые могут восстановить секрет-оригинал *S* по кодам секрета-маски $\tilde{S}$;

— $\{p_1, p_2, ..., p_l\}$ — фиксируемый представитель множества $\mathbf{P}\_l$;

— $r = 2^{b\_r}$ — модуль разрядностью *b_r* бит ($b\_r \leqslant b\_p$), используемый в базовом методе деления на двоичную экспоненту *r*;

— $u = 2^{b\_u}$ — основание позиционной системы счисления разрядностью *b_u* битов, применяемой для декомпозиции вычетов в процессе их преобразования с масштабированием в элементы колец по большим модулям в рамках таблично-сумматорной вычислительной технологии.

Входные данные алгоритма: подлежащий декодированию модулярный код $(\tilde{\sigma}_1, \tilde{\sigma}_2, ..., \tilde{\sigma}_l)$ секрета-маски $\tilde{S}$ по заданному набору $\mathbf{P}_{I\_l}$ оснований ($\mathbf{P}_{I\_l} = \{p_1, p_2, ..., p_l\}$).

Выходные данные: позиционный код $(s_{\nu-1}s_{\nu-2}...s_0)_r$ секрета-оригинала *S*, эквивалентный его двоичному коду разрядностью $b\_p = \lceil \log_2 p \rceil$ битов.

Предварительно получаемые данные:

- системные константы

$$C_i = |P_{i,l-1}|_r, \ \mu_{i,l-1} = |P_{i,l-1}^{-1}|_{p_i} \ (i = \overline{1, l-1});$$

$$C_l = |P_{l-1}|_r; |-P_l|_r; |r^{-1}|_{p_i} \ (i = \overline{1, l});$$

$$m_{i,l} = |-p_i^{-1}|_{p_l} \ (i = \overline{1, l-1}); \ \mu_{l,l} = |P_{l-1}^{-1}|_{p_l};$$

- таблицы остатков по модулю *r* слагаемых интервально-модулярной формы ЦЧ, генерируемые по расчетным соотношениям:

$$TRes\_AIMFi[\sigma] = \| |P_{i,l-1}|_r \sigma|_r,$$

$$TRes\_AIMFl[I] = \| |P_{l-1}|_r I|_r$$

$$(\sigma, I = \overline{0, r-1}; i = \overline{1, l-1});$$

- таблицы формальных частных для поитерационных операций деления на *r* расширенных минимально избыточных модулярных кодов, рассчитываемые по формуле

$$TRes\_f_{i[\delta]} = \left|\frac{\delta}{r}\right|_{p_i} \quad (\delta = \overline{-r, r-1}; i = \overline{1, l})$$

- таблицы аддитивных компонент масштабируемой позиционной формы ЦЧ по основанию $u = 2^{b\_u}$, формируемые согласно формулам

$$TACMPF\_i\_h[x] = \left\| P_{i,l-1}^{-1} \right|_{p_i} xu^h \Big|_{p_i}^{-}$$
$$(x = \overline{0, u-1};\ h = \overline{0, \lceil b\_mod\_i / b\_u \rceil - 1};\ i = \overline{1, l-1}), \quad (29)$$

$$\_TACMPF\_i\_h[x] =$$
$$= \begin{cases} \left\| -P_i^{-1} \right|_{p_l} xu^h \Big|_{p_l}^{-} \ (x = \overline{0, u-1}; \\ h = \overline{0, \lceil b\_mod\_i / b\_u \rceil - 1}) \text{ при } i = \overline{1, l-1}, \\ \left\| P_{l-1}^{-1} \right|_{p_l} xu^h \Big|_{p_l}^{-} \\ (x = \overline{0, u-1};\ h = \overline{0, \left\lceil \frac{b\_mod\_l}{b\_u} \right\rceil - 1}) \text{ при } i = l; \end{cases} \quad (30)$$

- таблицы старшей L-битовой части по основаниям p_i ЦЧ А с $b\_$-разрядным дополнительным двоичным кодом ($a_{b\_A-1}\ a_{b\_A-2}$ ... $a_{b\_A-L} \dots a_0)_2$ $(a_s \in \{0,1\}\ (s = \overline{0, b\_A-1}))$, генерируемые по правилу

$$TRes\_MP\_i[(a_{b\_A-1} a_{b\_A-2} \dots a_{b\_A-L})_2] =$$
$$= \left| \sum_{s=b\_A-L}^{b\_A-2} a_s 2^s - a_{b\_A-1} 2^{b\_A-1} \right|_{p_i} \ (i = \overline{1, l}). \quad (31)$$

Тело алгоритма восстановления секрета-оригинала (ВСО) по методу деления на двоичную экспоненту:

ВСО_Д.1. Активировать (l + 1)-элементный массив MC_Q для модулярных кодов неполных частных ЦЧ и поместить в него код $(\tilde{\sigma}_1^{(0)}, \tilde{\sigma}_2^{(0)}, \dots, \tilde{\sigma}_l^{(0)}) = (\tilde{\sigma}_1, \tilde{\sigma}_2, \dots, \tilde{\sigma}_l)$ числа $\tilde{S}_0 = \tilde{S}$ согласно правилу $MC\_Q[i] = \tilde{\sigma}_i^{(0)}$ $(i = \overline{1, l})$.

ВСО_Д.2. Определить число v итераций реализуемого рекурсивного процесса деления на экспоненту $r = 2^{b\_r}$ как $v = \lceil b\_p / b\_r \rceil$, активировать элементный массив PC_S для цифр r-ичного кода $(s_{\nu-1} s_{\nu-2} \dots s_0)_r$ секрета-оригинала S, записываемых в PC_S в порядке возрастания индексов (от 0 до $\nu - 1$), и порядковому номеру текущей итерации осуществляемого процесса (а значит и очередной цифры формируемого r-ичного кода) присвоить начальное значение $j = 0$.

ВСО_Д.3. Положить $s = 0$.

Вычисление компьютерного интервального индекса $\hat{I}_l(\tilde{S}_j)$ ЦЧ $\tilde{S}_j$.

ВСО_Д.4. Переменным I и i присвоить значения $I = 0$ и $i = 1$.

ВСО_Д.5. Выполнить операции: $X = 0$, $\sigma = MC\_Q[i] = \tilde{\sigma}_i^{(j)}$, $h = 0$, $v = \lceil b\_mod\_i / b\_u \rceil$.

Получение нормированного остатка $\tilde{\sigma}_{i,l-1}^{(j)}$ (см. (13)).

ВСО_Д.6. Следуя (14)—(16), выполнить операцию накопления, аккумулятивную операцию $X = X +$ TACMPF_i_h[$\sigma \wedge (u-1)$].

ВСО_Д.7. Инкрементировать переменную h ($h = h + 1$).

ВСО_Д.8. Если $h \neq v$, то значение переменной σ логически сдвинуть на b_u бит вправо ($\sigma = \sigma \gg= b\_u$) и перейти к ВСО_Д.6.

ВСО_Д.9. Текущее значение X привести к остатку по модулю p_i, реализуя операционную последовательность:

ВСО_Д.9А. Из двоичного кода ЦЧ X выделить младшую ((b_mod_i)-1)-битовую часть $X_0 = X \wedge (2^{(b\_mod\_i)-1} - 1)$.

ВСО_Д.9Б. Выделить старшую часть ЦЧ X разрядностью $L = (b\_v) + 1$ бит ($b\_v = \lceil \log_2 v \rceil$ и с помощью таблицы TRes_MP_i получить остаток $X_1 = TRes\_MP\_i\ [X \gg= ((b\_mod\_i) - 1)]$ (см. (18)—(21), (31)).

ВСО_Д.9В. Определить нормированный остаток $\tilde{\sigma}_{i,l-1}^{(j)} = \sigma = |X_0 + X_i|_{p_i}$ по модулю p_i.

ВСО_Д.10. Используя таблицу TRes_AIMFi, выполнить аккумулятивную операцию $s = s +$ $+ TRes\_AIMFi\ [\sigma \wedge (r-1)]$.

Вычисление вычета $R_{i,l}(\tilde{\sigma}_{i,l-1}^{(j)})$ по модулю p_l, определяемого согласно (11).

ВСО_Д.11. Положить $R = 0$, $h = 0$.

ВСО_Д.12. С помощью таблицы _TACMPF (см. (30)) выполнить операцию накопления $R = R +$ _TACMPF_i_h[$\sigma \wedge (u-1)$].

ВСО_Д.13. Инкрементировать переменную h ($h = h + 1$).

ВСО_Д.14. Если $h \neq v$, то значение переменной σ сдвинуть на b_u битов вправо ($\sigma = \sigma \gg= b\_u$) и перейти к ВСО_Д.12.

ВСО_Д.15. Текущее значение переменной R привести к остатку по модулю p_l, реализуя последовательность действий:

ВСО_Д.15А. Из двоичного кода ЦЧ R выделить младшую ((b_mod_l)-1)-битовую часть $R_0 = R \wedge (2^{(b\_mod\_l)-1} - 1)$.

ВСО_Д.15Б. Выделить старшую часть ЦЧ R разрядностью $L = (b\_v) + 1$ битов и с помощью таблицы TRes_MP_l получить остаток $R_1 = TRes\_MP\_l$ $[R \gg = ((b\_mod\_l) - 1)]$.

ВСО_Д.15В. Найти вычет $R_{i,l}(\tilde{\sigma}_{i,l-1}^{(j)}) =$ $= R = |R_0 + R_1|_{p_l}$.

ВСО_Д.16. Выполнить аккумулятивную операцию $I = I + R$.

ВСО_Д.17. Инкрементировать переменную i ($i = i + 1$).

ВСО_Д.18. При $i \neq l$ перейти к ВСО_Д.5.

Вычисление вычета $R_{l,l}(\tilde{\sigma}_l^{(j)})$ по модулю p_l, определяемого согласно (11).

ВСО_Д.19. Положить $R = 0$, $h = 0$, $v = \lceil b\_mod\_l / b\_u \rceil$, $\sigma = MC\_Q[l]$.

ВСО_Д.20. Выполнить аккумулятивную операцию $R = R +$ _TACMPF_$l_h[\sigma \wedge (u-1)]$ (см. (30).

ВСО_Д.21. Инкрементировать переменную h ($h = h + 1$).

ВСО_Д.22. При $h \neq v$ текущее значение переменной σ сдвинуть вправо на b_u битов ($\sigma = \sigma \gg = b\_u$) и перейти к ВСО_Д.20.

ВСО_Д.23. Текущее значение R привести к остатку по модулю p_l, реализуя последовательность:

ВСО_Д.23А. Выделить младшую ((b_mod_l)-1)-битовую часть $R_0 = R \wedge (2^{(b\_mod\_l)-1} - 1)$.

ВСО_Д.23Б. Выделить старшую часть ЦЧ R разрядностью $L = (b\_v) + 1$ бит и с помощью таблицы TRes_MP_l найти остаток $R_1 = TRes\_MP\_l$ $[R \gg = ((b\_mod\_l) - 1)]$.

ВСО_Д.23В. Получить вычет $R_{l,l}(\tilde{\sigma}_l^{(j)}) = R = \left|R_0 + R_1\right|_{p_l}$.

ВСО_Д.24. Выполнить операцию накопления $I = I + R$.

ВСО_Д.25. Полученное значение переменной I привести к остатку по модулю p_l, реализуя действия:

ВСО_Д.25А. Выделить младшую ((b_mod_l)-1)-битовую часть $I_0 = I \wedge (2^{(b\_mod\_l)-1} - 1)$ числа I.

ВСО_Д.25Б. Из двоичного кода ЦЧ I выделить старшую часть разрядностью $L = \lceil \log_2 l \rceil + 1$ бит и с помощью таблицы TRes_MP_l найти остаток $I_1 = TRes\_MP\_l$ $[I \gg = ((b\_mod\_l) - 1)]$.

ВСО_Д.25В. Вычислить компьютерный интервальный индекс ЦЧ $\tilde{S}_j$ по правилу $\hat{I}_l(\tilde{S}_j) = \left|I\right|_{p_l} = \left|I_0 + I_1\right|_{p_l}$.

ВСО_Д.26. Выполнить аккумулятивную операцию $s = s + TRes\_AIMFl$ $[I \wedge (r-1)]$ (см. (26)).

ВСО_Д.27. Если $I - p_0 \geqslant 0$, то в соответствии с (27) и (28) осуществить коррекцию переменной s по правилу $s = s + C\_II$ ($C\_II = |-P_l|_r$).

ВСО_Д.28. При $j \neq v - 1$ реализовать последовательность операций:

ВСО_Д.28А. В качестве j-й цифры позиционного r-ичного кода $(s_{v-1}\, s_{v-2} \ldots s_0)_r$ секрета-оригинала $S = \left|\tilde{S}\right|_p$ зафиксировать значение $s_j = |s|_r = s \wedge (r-1)$, поместив его в массив PC_S согласно правилу $PC\_S[j] = s_j$.

ВСО_Д.28Б. В соответствии с (23) сформировать минимально избыточный модулярный код $(\tilde{\sigma}_1^{(j+1)}, \tilde{\sigma}_2^{(j+1)}, \ldots, \tilde{\sigma}_l^{(j+1)})$ числа $\tilde{S}_{j+1}$ для следующей $(j+1)$-й итерации процесса деления на r, выполняя для всех $i = \overline{1,l}$ действия:

- получить симметрический остаток $\delta_i^{(j)} = \left|(r-1) \wedge MC\_Q[i] - s_j\right|_{2r}^{-}$ в дополнительном двоичном коде разрядностью $(b\_r) + 1$ битов;
- из таблицы $TRes\_f\_i$ извлечь вычет $\varphi_i^{(j)} = TRes\_f\_i\,[\delta] = \left|\delta_i^{(j)} / r\right|_{p_i}$;
- выделить из двоичного кода цифры $\tilde{\sigma}_i^{(j)} = MC\_Q[i]$ МИМК числа $\tilde{S}_j$ старшую $((b\_mod\_i) - b\_r)$-битовую часть $q_i^{(j)} = \left\lfloor \tilde{\sigma}_i^{(j)} / r \right\rfloor = \tilde{\sigma}_i^{(j)} \gg = b\_r$;
- завершить формирование i-й цифры минимально избыточного модулярного кода ЦЧ $\tilde{S}_{j+1}$, вычисляя модульную сумму $MC\_Q[i] = \tilde{\sigma}_i^{(j+1)} = \left|q_i^{(j)} + \varphi_i^{(j)}\right|_{p_i}$.

ВСО_Д.28В. Инкрементировать переменную j ($j = j + 1$) и перейти к ВСО_Д.4.

ВСО_Д.29. По достижении равенства $j = \nu - 1$ в качестве $(\nu - 1)$-й цифры позиционного r-ичного кода секрета-оригинала S зафиксировать значение $PC\_S[\nu - 1] = s_{\nu-1} = (s \wedge (r-1))$ $(\mathrm{mod}(\exp_2(b\_p - (\nu - 1)b\_r)))$ (см. (6)).

ВСО_Д.30. В качестве искомого r-ичного кода секрета-оригинала S зафиксировать $(s_{\nu-1}\, s_{\nu-2} \ldots s_0)_r = (PC\_S[\nu - 1]\ PC\_S[\nu - 2] \ldots PC\_S[0])_r$ и завершить работу алгоритма.

4. Оценка эффективности декодирующего МИМА-алгоритма

В (t, n)-пороговом МИМА-криптомодуле восстановление секрета-оригинала S по секрету-маске $\tilde{S}$ с помощью синтезированного алгоритма ВСО_Д.1 — ВСО_Д.30 деление на двоичную экспоненту осуществляется за время

$$t_{\text{ВСО}} = v(t_{\text{ИИ}} + t_{\text{р}} + t_{\text{МК}}), \tag{32}$$

где $v = \lceil b\_p / b\_r \rceil$ — число итераций процесса деления на r; $t_{\text{ИИ}}$ — время вычисления интервального индекса ЦЧ в l-модульной минимально избыточной МСС; t_p — время расширения кода на экспоненту $r = 2^{b\_r}$ (без учета затрат на получение интервального индекса); $t_{\text{МК}}$ — временные затраты на формирование модулярного кода неполного частного (для следующей итерации). Операционный анализ алгоритма ВСО_Д.1 — ВСО_Д.30 дает для $t_{\text{ИИ}}$, $t_{\text{р}}$, $t_{\text{МК}}$ оценочные выражения:

$$t_{\text{ИИ}} = ((2l-1)(\lceil b\_mod / b\_u \rceil + 1) + l + 3)t_{\text{сл},\,b\_mod}; \tag{33}$$

$$t_{\text{р}} = l t_{\text{сл}}; \tag{34}$$

$$t_{\text{МК}} = l(t_{\text{сл}} + 1 + t_{\text{сл},\,b\_mod}), \tag{35}$$

в которых $t_{\text{сл, }b\_\text{mod}}$ и $t_{\text{сл}}$ — длительности двух местных операций сложения в процессах суммирования *b_mod*-битовых вычетов и вычетов стандартной разрядности соответственно. С учетом (34), (35) оценку (32) можно записать в следующем развернутом виде:

$$t_{\text{ВСО}} = \left\lceil \frac{b\_p}{b\_r} \right\rceil \left(\left((2l-1)\left(\left\lceil \frac{b\_\text{mod}}{b\_u} \right\rceil + 1 \right) + \right. \right. \\ \left. \left. + 2l + 3 \right) t_{\text{сл},b\_mod} + 2lt_{\text{сл}} \right). \quad (36)$$

В случае применения в пороговом криптомодуле разделения секрета рассматриваемого класса вместо минимально избыточной МСС неизбыточного аналога оценка (32) суммарных временных затрат на выполнение декодирующей операции по алгоритму типа ВСО_Д.1 — ВСО_Д.30 принимает вид

$$t'_{\text{ВСО}} = \nu(t'_{\text{ИИ}} + t_{\text{р}} + t_{\text{МК}}), \quad (37)$$

где $t'_{\text{ИИ}}$ — время вычисления в неизбыточной l-модульной МСС интервально-индексной характеристики. Согласно представленному в работах [2, 14] алгоритму РИХ_ОА.1 — РИХ_ОА.8 расчет интервального индекса ЦЧ в l-модульной неизбыточной МСС требует примерно в l раз больше временных затрат, чем в минимально избыточных МСС с такими же основаниями, т. е. $t'_{\text{ИИ}} = lt_{\text{ИИ}}$. Таким образом, в виду (32)—(37) получаемый выигрыш по рассматриваемому показателю при использовании минимально избыточных МСС вместо неизбыточной МСС для построения порогового криптомодуля разделения секрета оценивается коэффициентом

$$V = \frac{lt_{\text{ИИ}} + t_{\text{р}} + t_{\text{МК}}}{t_{\text{ИИ}} + t_{\text{р}} + t_{\text{МК}}}. \quad (38)$$

Пусть

$$U = \frac{t_{\text{р}} + t_{\text{МК}}}{t_{\text{ИИ}}}, \quad (39)$$

тогда (38) можно записать в следующей эквивалентной форме:

$$V = \frac{l-1}{U+1} + 1. \quad (40)$$

Функциональная зависимость $V = V(U)$, описываемая соотношением (40), представляет собой участок гиперболы с асимптотами $U = -1$ и $V = 1$ (см. рисунок). Согласно (33)—(36) аргумент (39) функции (40) представим в виде

$$U = \frac{l(t_{\text{сл},b\_mod} + t_{\text{сл}})}{\left((2l-1)\left(\left\lceil \frac{b\_\text{mod}}{b\_u} \right\rceil + 1 \right) + l + 3 \right) t_{\text{сл},b\_mod}} = \\ = \frac{1 + \frac{t_{\text{сл}}}{t_{\text{сл},b\_mod}}}{\left(2 - \frac{1}{l} \right)\left(\left\lceil \frac{b\_mod}{b\_u} \right\rceil + 1 \right) + 1 + \frac{3}{l}}. \quad (41)$$

Так как $t_{\text{сл}} < t_{\text{сл},b\_mod}$, $l \geqslant 2$, а параметры *b_mod* и *b_u* на практике удовлетворяют ограничениям $b\_mod \geqslant 128$, $b\_u \leqslant 16$, то значения переменной U удовлетворяют неравенству $0 < U < 0 < U < \frac{3l}{19l-6}$ и, как нетрудно проверить, пороговый МИМА-криптомодуль разделения секрета по производительности превосходит аналог на основе традиционно используемых версий МА не менее чем в $\frac{l(19l-3)}{2(11l-3)}$ раз. При этом, однако, коэффициент (40) достигаемого

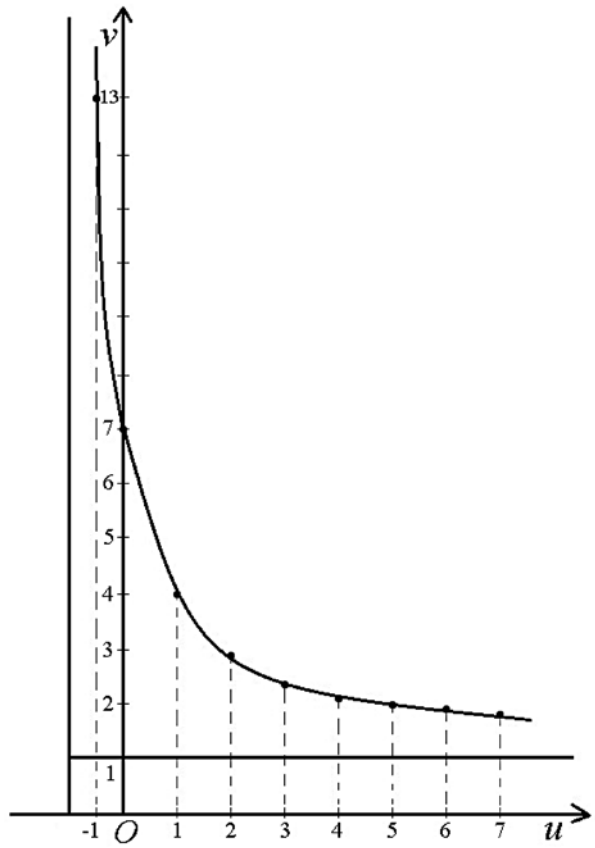

График коэффициента уменьшения времени выполнения декодирующей процедуры в пороговом МИМА-криптомодуле разделения секрета в сравнении с неизбыточным аналогом (для $l = 7$ абонентов)

Минимальные значения коэффициента V увеличения быстродействия декодирующей МИМА-процедуры на основе метода деления на двоичную экспоненту в сравнении с неизбыточными МА-аналогами

№ п/п	Число абонентов, восстанавливающих секрет l	Минимальное увеличение быстродействия декодирующей процедуры $V_{\text{мин}}(l)$
1	5	4,423
2	7	6,149
3	12	10,465
4	16	13,919
5	20	17,373
6	25	21,691
7	30	26,009
8	35	30,327
9	40	34,645

повышения быстродействия сверху ограничен порогом l. В таблице приведены значения указанного нижнего порога $\frac{l(19l-3)}{2(11l-3)} = V_{\text{мин}}(l)$ показателя V для некоторых l.

Заключение

Основные результаты представленной разработки по проблематике создания математического обеспечения модулярных пороговых криптосистем разделения секрета кратко можно охарактеризовать следующим образом.

1. Предложена МИМА-конфигурация метода деления на двоичную экспоненту для выполнения декодирующей операции в пороговом криптомодуле разделения секрета с маскирующим преобразованием. Главные отличительные особенности разработанного подхода к решению рассматриваемой задачи обусловлены использованием колец принадлежности секрета-оригинала по модулям, имеющим вид степеней числа 2, а также вычислительной МИМА-технологии, согласованной с пороговым принципом. Это приводит к существенному сокращению реализационных затрат на этапе реконструкции исходного секрета по кодам маскирующего аналога.

2. Для перевода трудоемких вычислений, приходящихся на декодирующее преобразование, из диапазонов больших чисел в диапазоны ЦЧ стандартной разрядности наряду с модулярной арифметикой применена таблично-сумматорная технология. Осуществляемая в рамках этой технологии поразрядная декомпозиция двоичных кодов масштабируемых вычетов по большим модулям служит эффективным инструментарием отображения выполняемых вычислительных процедур на наборы легкореализуемых операций извлечения данных из табличной памяти и их суммирования, обеспечивая при этом высокий уровень производительности, однородности и унификации базовых структур.

3. На основе метода деления на двоичную экспоненту и вычислительной МИМА-технологии таблично-сумматорного типа синтезирован эффективный алгоритм восстановления секрета-оригинала по кодам секрета-маски. Проведен сравнительный анализ эффективности предложенного алгоритма с неизбыточными аналогами. Показано, что по производительности декодирующий МИМА-алгоритм превосходит аналоги как минимум в $\frac{l(19l-3)}{2(11l-3)}$ раз (l — число абонентов, реконструирующих секрет-оригинал). В частности, при $l = 7...40$ достигается (6,15...34,65)-кратное повышение производительности.

Список литературы

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, 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. **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.

A. A. Kolyada, Doctor of Physical and Mathematical Sciences, Associate Professor, e-mail: razan@tut.by,
P. V. Kuchynski, Doctor of Physical and Mathematical Sciences, Associate Professor, e-mail: niipfp@bsu.by,
S. Yu. Protasenia, Junior Scientist, Laboratory of Specialized Computational Systems, e-mail: estellita@mail.ru,
Research establishment "Institute of Applied Physics Problems of A. N. Sevchenko"
Belarusian State University, Minsk

Method and Algorithm for Implementation of Decoding Operation in the Threshold Cryptomodule of Secret Separation Using a Minimally Redundant Modular Number System

The article presents a new development of method and algorithm for performing secret separation in a threshold cryptomodule with masking transformation of the decoding operation. To solve this problem a recursive binary exponent division scheme and computational technology on the ranges of large numbers of the table-adder type, based on minimally redundant modular arithmetic (MRMA) are applied. A distinctive feature of the developed approach is usage the secret-original domain of finite residue rings for modules that have the form of powers of the number 2. This significantly reduces the complexity of the resulting decoding MRMA-procedure. Decomposition of scalable residues into large modules allows you to efficiently map the computational process being implemented to sets of easily implemented data extraction operations from table memory and their summation, providing a high level of performance, uniformity, and unification of basic structures. In terms of speed, the created MIMA decoding algorithm surpasses non-redundant analogues by at least $\frac{l(19l-3)}{2(11l-3)}$ *times (l is the number of subscribers restoring the secret original). When 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*

DOI: 10.17587/it.27.77-88

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.** et al. 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, no. 11, pp. 612—613.

5. **Blakley G. R.** Safe guarding cryptographic keys, *Proc. of the 1979 AFIPS National Computer Conference,* Montvale, AFIPS press, 1979, pp. 313—317.

6. **Mignotte M.** How to share a secret, *Lecture notes in computer science*, 1983, vol. 149, pp. 371—375.

7. **Asmuth C. A.**, **Bloom J.** A modular appoach to key safe guarding, *IEEE Tras. On Information Theory*, 1983, vol. 29, no. 2, pp. 208—210.

8. **Schneier B.** Secret Secretion Algorithms. Scheme of Lagrange interpolation polynomials, Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnyye teksty na 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, pp. 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, pp. 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, pp. 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*., 2019, vol. 25, no. 9, 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, pp. 641—649 (in Russian).

15. **Ananda Mohan P. V.** Residue number systems: Theory and applications. Basel, Birghauser, Mathematics, 2016, 351 p.