УДК 004.9, 004.94, 004.56 DOI: 10.17587/it.25.553-561

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,
Научно-исследовательское учреждение "Институт прикладных физических проблем имени А. Н. Севченко" Белорусского государственного университета,
Н. И. Червяков, д-р техн. наук, проф., e-mail: Chervyakov@yandex.ru,
Федеральное государственное автономное образовательное учреждение высшего профессионального образования "Северо-Кавказский федеральный университет"

Пороговый метод разделения секрета на базе избыточных модулярных вычислительных структур[1]

Дана формализация порогового метода модулярного разделения секрета с использованием минимально избыточного кодирования. В частности, определены условия, обеспечивающие возможность применения в пороговых криптосхемах разделения секрета в качестве компьютерно-арифметической базы минимально избыточной модулярной арифметики (МИМА). В сравнении с неизбыточными аналогами МИМА позволяет уменьшить трудоемкость операции восстановления секрета-оригинала по долевым секретам, принадлежащим группам абонентов. Получены также условия корректности порогового принципа в рамках модулярного кодирования, и на этой основе разработан метод нейтрализации критичных ситуаций с обеспечением должного уровня криптостойкости.

Ключевые слова: *разделение секрета, минимально избыточная модулярная арифметика, пороговая схема модулярного разделения секрета, псевдослучайная маскирующая функция, распределенные вычисления*

Введение

Неотъемлемой составляющей современного процесса развития распределенных систем обработки данных различного назначения является обеспечение безопасности при хранении, обработке и передаче информации. Для решения обозначенной задачи криптография предоставляет весьма обширный функциональный инструментарий, охватывающий многообразные локальные и распределенные средства [1—12], такие, например, как электронная цифровая подпись, идентификация и аутентификация абонентов, безопасное хранение ключей и т.п. Криптографический ключ фактически представляет собой главный секрет во всем процессе шифрования [3]. Механизм ключей предполагает использование специальной операционной базы, которая обеспечивает генерирование, надежное хранение, маскирующее преобразование ключей в векторные представления и распределение их компонентов как долевых (частичных) секретов между абонентами системы, а также восстановление ключей-оригиналов по наборам долевых секретов. Перспективные технологии защиты данных в распределенных системах, такие как технология активной безопасности, предусматривающая периодическое обновление и разделение ключей участниками сеансов связи, предъявляют к реализационным характеристикам алгоритмов перечисленных операций высокие требования. Поэтому исследования по созданию новых высокопроизводительных технологий выполнения операций над ключами в рамках пороговых схем разделения секретной информации представляют актуальное, активно развиваемое в последние годы направление в криптографии [1, 3, 4, 10—12].

Как известно, компьютерно-арифметической базой средств защиты информации служит арифметика больших целых чисел (ЦЧ)

[1]Исследования выполнены при финансовой поддержке БРФФИ (Договор № Ф18-005 от 30 мая 2018 г.) и ГПНИ "Информатика, космос и безопасность" (2016—2020 гг.).

[1—3, 13—17], вследствие чего эффективность криптопреобразований на практике в решающей мере определяется реализационными свойствами применяемой технологии перевода осуществляемых вычислений из диапазона больших чисел (ДБЧ) в диапазоны ЦЧ стандартной разрядности. Ввиду кодового параллелизма кольцевых операций в модулярной системе счислений (МСС) и благодаря высокому уровню модульности криптографических процедур в свете сказанного в качестве компьютерно-арифметической основы для приложений рассматриваемого класса целесообразно принять модулярную арифметику (МА). Важным дополнительным фактором, указывающим на целесообразность применения МСС для построения пороговых криптосхем разделения секретной информации, является обеспечение возможности использования модулярной системы доступа, которая обладает естественным кодовым параллелизмом.

Обращаясь к существующим методам построения пороговых схем разделения секрета, прежде всего следует отметить предложенный А. Шамиром [18,19] метод, базирующийся на интерполяционных полиномах Лагранжа. Схема Шамира отличается высоким уровнем криптостойкости. Однако ее реализация требует довольно большого числа трудоемких мультипликативых операций и операций инвертирования ЦЧ по большому модулю. Кроме того, схемы данного класса используют сравнительно большой набор псевдослучайных параметров. Еще в большей мере указанные недостатки присущи предложенной в 1979 году векторной схеме Блэкли [20], которая основана на маскирующем преобразовании секрета-оригинала с помощью гиперплоскостей в l-мерном пространстве (l — число сторон, разделяющих секрет). Несмотря на то что схемы Шамира и Блэкли используют только один большой модуль p — модуль рабочего поля GF(p), они допускают применение высокопараллельных вычислительных структур, например, структур, состоящих из l однотипных независимых друг от друга компонентов. Однако в этом отношении более продуктивным представляется подход, предусматривающий использование l различных модулей, что означает переход к МСС. Применение МСС для построения пороговых схем разделения секрета [1, 3, 4, 21, 22] открывает принципиально новые возможности в части существенного уменьшения вычислительной сложности этапов выработки долевых секретов и восстановления по ним секрета-оригинала. Модулярное кодирование дает простой способ формирования частичных секретов как цифр кода МСС, получаемого в результате маскирующего преобразования, причем само это преобразование может иметь минимальную вычислительную сложность. Его роль может, например, выполнять линейное преобразование лишь с одним псевдослучайным коэффициентом.

Наиболее трудоемкой операцией в пороговой МА-криптосистеме разделения секрета является операция восстановления секрета-оригинала по модулярным кодам маскирующего аналога, т.е. по l-компонентным наборам долевых секретов. Ее сложность определяется используемой позиционной формой модулярных чисел и связанными с ней интегральными характеристиками кода МСС [1, 3, 4, 21—23]. Декодирующие процедуры (процедуры восстановления), осуществляющие прямую реализацию китайской теоремы об остатках [3, 4, 22], малоэффективны, так как они требуют вычислений по большому модулю, представляющему собой произведение оснований соответствующей l-модульной МСС. Фундаментальные преимущества МА наиболее полно удается реализовать в рамках так называемого минимально избыточного модулярного кодирования [1, 9, 23] и ассоциированной с ним интервально-модулярной формы чисел. Интегрально характеристическая база минимально избыточной МА (МИМА) позволяет минимизировать временные и аппаратурные затраты на выполнение немодульных операций, в том числе и операций восстановления секрета-оригинала.

Цель представляемого исследования — разработка принципиальных основ пороговых криптосхем разделения секрета с использованием минимально избыточного модулярного кодирования.

Решаемая в статье задача включает определение ограничений на диапазон изменения маскирующего аналога секрета-оригинала, обеспечивающих возможность применения МИМА в пороговой схеме рассматриваемого класса без снижения ее криптостойкости, и получение условий корректности развиваемого метода разделения секретной информации.

1. Постановка задачи и методы ее решения

Введем следующие обозначения:

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

$\mathbf{Z}_m = \{0, 1, ..., m-1\}$ — 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, $|B|_m \neq 0$);

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

Пусть p_1, p_2, ..., p_n — упорядоченные по возрастанию попарно простые большие натуральные числа ($n > 1$);

$$P_i = \prod_{l=1}^{i} p_l \, (i = \overline{1,n});$$

$$\_P_j = \prod_{k=1}^{j} p_{n-k+1} = P_n / P_{n-j} \, (j = \overline{1,n});$$

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

$$\mathbf{I}\_l = \{\forall (i_1, i_2, \ldots, i_l) \mid 1 \leqslant i_1 < i_2 < \ldots$$
$$\ldots < i_l \leqslant n; 2 \leqslant t \leqslant l \leqslant n\}$$

(t — фиксированное натуральное число);

$$\mathbf{J}\_k = \{\forall (j_1, j_2, \ldots, j_k) \mid 1 \leqslant j_1 < j_2 < \ldots$$
$$\ldots < j_k \leqslant n; 2 \leqslant k < t\};$$

$I\_l = (i_1, i_2, \ldots, i_l)$ и $J\_k = (j_1, j_2, \ldots, j_k)$ — произвольные элементы соответственно множеств $\mathbf{I}\_l$ и $\mathbf{J}\_k$;

$$\mathbf{P}_{I\_l} = \{p_{i_1}, p_{i_2}, \ldots, p_{i_l}\};$$

$$\mathbf{P}_{J\_k} = \{p_{j_1}, p_{j_2}, \ldots, p_{j_k}\};$$

$$\mathbf{P}_{I\_l} = \prod_{j=1}^{l} p_{i_j}; \quad \mathbf{P}_{J\_k} = \prod_{i=1}^{k} p_{j_i}.$$

Концептуальную базу (t, n)-пороговой МИМА-схемы разделения секрета, которая рассчитана на полное число n и пороговое число t абонентов распределенной системы, составляют следующие определяющие ***положения***:

А. Исходный секрет, разделяемый n сторонами, представляет собой целое число $S \in \mathbf{Z}_p$, где p — большой модуль, взаимно простой с p_1, p_2, ..., p_n.

Б. Над S в МСС с базисом **P** выполняется маскирующее преобразование вида

$$\tilde{S} = S + Cp \qquad (1)$$

(C — псевдослучайная целочисленная величина).

Цифры $\tilde{\sigma}_i = \left|\tilde{S}\right|_{p_i} = \left|\sigma_i + |Cp|_{p_i}\right|_{p_i}$ ($\sigma_i = |S|_{p_i}$; $i = \overline{1,n}$) получаемого кода (σ_1, σ_2, ..., σ_n) рассматриваются как долевые (частичные) секреты, принадлежащие одноименным абонентам.

В. Любые t или более абонентов могут восстановить секрет-оригинал S по принадлежащим им маскирующим частичным секретам. Но никакая группа абонентов числом меньше t сделать этого не может.

Г. Область (диапазон) изменения маскирующего секрета $\tilde{S}$ согласуется с принципом минимально избыточного модулярного кодирования, что обеспечивает возможность выполнения декодирующей операции (операции восстановления секрета-оригинала) по упрощенным МИМА-процедурам.

Создание теоретической базы технологии реализации сформулированных основополагающих принципов построения пороговых МИМА-криптосхем разделения секрета является главной задачей представляемых исследований.

Применяемые методологические средства для решения поставленной задачи основаны на идее, которая предусматривает сужение области изменения маскирующего аналога $\tilde{S} = S + Cp$ секрета-оригинала S при выбранных p_1, p_2, ..., p_n до множества $\tilde{\mathbf{S}}$, допускающего определение на нем минимально избыточного модулярного кодирования. Несмотря на появляющуюся при этом незначительную (минимальную) дополнительную избыточность результирующего кода МСС она позволяет свести к теоретическому минимуму сложность операции расчета базовой интегральной характеристики кода (интервального индекса) [1, 23] и, как следствие, существенно упростить процедуру восстановления секрета-оригинала S. Для обеспечения корректности порогового принципа модулярного разделения секрета, т.е. для выполнения условия **В** (с необходимым уровнем криптостойкости), применяется метод нейтрализации порождаемых диапазоном $\tilde{\mathbf{S}}$ значений псевдослучайного параметра C, которые нарушают требование **В**.

2. Согласование диапазона изменения маскирующего секрета с принципом минимально избыточного модулярного кодирования

Рассмотрим два класса МСС, определяемых базисами

$$\mathbf{P}_{I\_l} = \{p_{i_1}, p_{i_2}, \ldots, p_{i_l}\}$$
$$(1 \leqslant i_1 < i_2 < \ldots < i_l \leqslant n; t \leqslant l \leqslant n)$$
и $$\mathbf{P}_{J\_k} = \{p_{j_1}, p_{j_2}, \ldots, p_{j_k}\}$$
$$(1 \leqslant j_1 < j_2 < \ldots < j_k \leqslant n; 2 \leqslant k < t).$$

К первому классу относятся МСС, отвечающие группам абонентов, число l которых не меньше порогового значения t, а ко второму — МСС, используемые группами из $k < t$ абонентов (см. условие **B**).

Ключевым аспектом проблемы выбора рабочего диапазона изменения секрета-маски (1) является поиск условий, обеспечивающих непересекаемость множеств (диапазонов) изменения целых чисел $\tilde{S}_{I\_l} = \tilde{S}(\mathrm{mod}\, P_{I\_l})$ и $\tilde{S}_{J\_k} = \tilde{S}(\mathrm{mod}\, P_{J\_k})$, имеющих в МСС с базисами $\mathbf{P}_{I\_l}$ и $\mathbf{P}_{J\_k}$ соответственно коды $(\tilde{\sigma}_{i_1}, \tilde{\sigma}_{i_2}, \ldots, \tilde{\sigma}_{i_l})$ и $(\tilde{\sigma}_{j_1}, \tilde{\sigma}_{j_2}, \ldots, \tilde{\sigma}_{j_k})$.

Справедливо следующее утверждение.

Теорема 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 (p — большой модуль). Для того чтобы диапазоны $\mathbf{Z}_{P_{J\_k}} = \{0, 1, \ldots, P_{J\_k} - 1\}$ изменения вычетов $\tilde{S}_{J\_k} = (\tilde{\sigma}_{j_1}, \tilde{\sigma}_{j_2}, \ldots, \tilde{\sigma}_{j_k})$ в МСС с базисами $\mathbf{P}_{J\_k} (2 \leqslant k < t)$ не пересекались с множеством значений секрета-маски $\tilde{S}$, имеющего в МСС с базисами $\mathbf{P}_{I\_l} (t \leqslant l \leqslant n)$ коды $(\tilde{\sigma}_{i_1}, \tilde{\sigma}_{i_2}, \ldots, \tilde{\sigma}_{i_l})$, достаточно выполнения условия

$$\tilde{S} \in \{\_P_{t-1}, \_P_{t-1} + 1, \ldots, P_t - 1\}. \qquad (2)$$

Доказательство. Предположим, что секрет S намерены разделить между собой любые l участников сеанса связи, за которыми закреплены основания базиса $\mathbf{P}_{I\_l}$. Поскольку модули базиса $\mathbf{P}$ криптосхемы упорядочены по возрастанию, то при всех рассматриваемых l выполняется неравенство

$$P_t \leqslant P_{I\_l} \left(l = \overline{t, n}\right). \qquad (3)$$

Маскирующий секрет (1) должен принадлежать диапазонам МСС с базисами $\mathbf{P}_{I\_l}$ — множествам $\mathbf{Z}_{P_{I\_l}}$ при всех $l = \overline{t, n}$. С учетом (3) для этого достаточно потребовать выполнения условия

$$\tilde{S} = S + Cp < P_t. \qquad (4)$$

Что касается модулей $p_{j_1}, p_{j_2}, \ldots, p_{j_k}$ класса $\mathbf{P}_{J\_k}$, отвечающих группам участников сеанса связи, число k которых меньше порогового значения t, то они удовлетворяют неравенству

$$P_{J\_k} \leqslant \_P_{t-1}. \qquad (5)$$

Как следует из соотношений (1)—(5), рабочий диапазон конструируемой пороговой схемы (по переменной $\tilde{S}$) легко может быть ориентирован исключительно только на значения $\tilde{S}$, отвечающие кодам $(\tilde{\sigma}_{i_1}, \tilde{\sigma}_{i_2}, \ldots, \tilde{\sigma}_{i_l})$ МСС с базисами $\mathbf{P}_{I\_l}$ $(t \leqslant l \leqslant n)$. Соответствующее множество значений секрета-маски $\tilde{S}$ описывается неравенством

$$\_P_{t-1} < S + Cp < P_t. \qquad (6)$$

Ввиду (5) диапазоны МСС с базисами $\mathbf{P}_{J\_k}$ находятся вне промежутка $(\_P_{t-1}; P_t)$. Кодам $(\tilde{\sigma}_{j_1}, \tilde{\sigma}_{j_2}, \ldots, \tilde{\sigma}_{j_k})$ указанных МСС отвечают вычеты $\tilde{S}_{J\_k}$ по модулям $P_{J\_k} \leqslant \_P_{t-1}$, т.е. ЦЧ, не принадлежащие диапазону изменения $\tilde{S}$ (см. условие (6)). Таким образом, ограничение (6) для $\tilde{S}$ обеспечивает непересекаемость множества результатов $\tilde{S}$ маскирования секрета S по правилу (1) с диапазонами $\mathbf{Z}_{P_{J\_k}}$ всех МСС, определяемых базисами $\mathbf{P}_{J\_k}$. *Теорема доказана.*

В случае применения маскирующего преобразования (1) областью изменения псевдослучайного параметра C, которая отвечает условию (6), служит множество

$$\mathbf{C} = \left\{\left\lfloor \frac{\_P_{t-1}}{p} \right\rfloor, \left\lfloor \frac{\_P_{t-1}}{p} \right\rfloor + 1, \ldots, \left\lfloor \frac{P_t - 1}{p} \right\rfloor\right\}. \qquad (7)$$

Замечание. Из вышеизложенного следует, что диапазоны $\mathbf{Z}_{P_{I\_l}}$ всех МСС, определяемых базисами $\mathbf{P}_{I\_l}$, включают диапазон $\mathbf{Z}_{P_t} = \{0, 1, \ldots, \_P_{t-1}, \_P_{t-1} + 1, \ldots, P_t - 1\}$ МСС с базисом $\{p_1, p_2, \ldots, p_t\}$. Это позволяет рассматривать множество $\tilde{\mathbf{S}} = \{\_P_{t-1}, \_P_{t-1} + 1, \ldots, P_t - 1\}$ как рабочий диапазон модулярной (t, n)-криптосхемы разделения секрета с основаниями $p_1, p_2, \ldots, p_n$ по переменной $\tilde{S} = S + Cp$. Поскольку восстановление секрета-оригинала S по кодам $(\tilde{\sigma}_{i_1}, \tilde{\sigma}_{i_2}, \ldots, \tilde{\sigma}_{i_l})$ маскирующего секрета $\tilde{S}$ в МСС с базисами $\mathbf{P}_{I\_l}$ является немодульной операцией, которая весьма сложна, особенно на диапазонах больших чисел, то ее целесообразно выполнять в рамках минимально избыточного кодирования [1, 9, 23], обеспечивающего минимизацию реализационных затрат. Предлагаемый подход предусматривает использование для выполнения необходимых немодульных операций МСС с базисами $\mathbf{P}_{I\_l}$ и диапазонами $\{0, 1, \ldots, p_0 P_{I\_(l-1)} - 1\} \subset$

$\subset \{0, 1, ..., P_{I\_l} - 1\}$, где p_0 — вспомогательный модуль, удовлетворяющий условию:

$$p_{i_l} \geqslant p_0 + l - 2 \quad (p_0 \geqslant t - 2) \tag{8}$$

при всех $l = \overline{t,n}$. Такие МСС называются *минимально избыточными* [23].

Переход от неизбыточных к соответствующим минимально избыточным МСС (МИМСС) влечет за собой замену рабочего диапазона $\tilde{\mathbf{S}}$ по переменной $\tilde{S}$ (см. замечание) на множество

$$\tilde{\mathbf{S}} = \{\_P_{t-1}, \_P_{t-1} + 1, \ldots, p_0 P_{t-1} - 1\}, \tag{9}$$

которое является составной частью диапазонов всех введенных МИМСС.

Сущность принципа минимально избыточного модулярного кодирования для пороговой (t, n)-криптосхемы разделения секрета раскрывает следующая теорема.

Теорема 2. Пусть $m_1 = p_{i_1}, m_2 = p_{i_2}, \ldots, m_l = p_{i_l}$; $M_{l-1} = \prod_{j=1}^{l-1} m_j$; $M_{j,l-1} = \dfrac{M_{l-1}}{m_j}$, $\tilde{\sigma}_j = \left|\tilde{S}\right|_{m_j} \left(j = \overline{1,l}\right)$; $I_l\left(\tilde{S}\right)$ — интервальный индекс (ИИ) числа $\tilde{S} = (\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ в МСС с базисом $\{m_1, m_2, m_l\}$ [23], определяемый равенством

$$\tilde{S} = \sum_{j=1}^{l-1} M_{j,l-1} \left|M_{i,l-1}^{-1} \tilde{\sigma}_j\right|_{m_j} + M_{l-1} I_l\left(\tilde{S}\right). \tag{10}$$

Для того чтобы в МСС с основаниями m_1, m_2, ..., m_l ИИ $I_l(\tilde{S})$ каждого элемента $\tilde{S}$ диапазона $\{\_P_{t-1}, \_P_{t-1} + 1, \ldots, p_0 P_{t-1} - 1\}$ (p_0 — вспомогательный модуль) полностью определялся компьютерным ИИ-вычетом $I_l(\tilde{S}) = \left|I_l(\tilde{S})\right|_{m_l}$, необходимо и достаточно, чтобы l-е основание удовлетворяло условию $m_l \geqslant p_0 + l - 2 \quad (p_0 \geqslant l - 2)$.

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

$$I_l(\tilde{S}) = \begin{cases} \hat{I}_l(\tilde{S}), & \text{если} \quad \hat{I}_l(\tilde{S}) < p_0; \\ \hat{I}_l(\tilde{S}) - m_l, & \text{если} \quad \hat{I}_l(\tilde{S}) \geqslant p_0; \end{cases} \tag{11}$$

$$\hat{I}_l(\tilde{S}) = \left| \sum_{j=1}^{l} R_{j,l}(\tilde{\sigma}_j) \right|_{m_l}; \tag{12}$$

$$R_{j,l}(\tilde{\sigma}_j) = \left| -m_j^{-1} \left|M_{j,l-1}^{-1} \tilde{\sigma}_j\right|_{m_j} \right|_{m_l} \quad (j \neq l), \qquad R_{l,l}(\tilde{\sigma}_l) = \left|M_{l-1}^{-1} \tilde{\sigma}_l\right|_{m_l}. \tag{13}$$

Позиционная форма (10) числа $\tilde{S}$ называется его интервально-модулярной формой по базису **M**. Применение минимально избыточного модулярного кодирования, сущность которого раскрывает ***теорема 2,*** снижает сложность расчета базовых интервально-индексных характеристик (см. (11)—(13)) практически до теоретического минимума. Это открывает принципиально новые возможности для повышения производительности пороговых МА-криптосхем разделения секрета.

3. Проблема корректности порогового принципа модулярного разделения секрета

Общая формула для восстановления секрета S по $\tilde{S}$ вытекает непосредственно из (1) и имеет вид

$$S = \left|\tilde{S}\right|_p. \tag{14}$$

В МИМСС с базисами $\mathbf{P}_{I\_l}$ $(t \leqslant l \leqslant n)$ и диапазонами $\left\{0, 1, \ldots, p_0 P_{I\_(l-1)} - 1\right\}$, содержащими множество (9) всех маскирующих секретов $\tilde{S}$ (см. теорему 1), преобразование $\tilde{S} \to S$ осуществляется корректно. Найдем ограничение на область изменения $\tilde{S}$, исключающее возможность восстановления S по $\tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right) = \left(\tilde{\sigma}_{j_1}, \tilde{\sigma}_{j_2}, \ldots, \tilde{\sigma}_{j_k}\right)$ любыми k абонентами ($2 \leqslant k < t$), за которыми закреплены модули $p_{j_1}, p_{j_2}, \ldots, p_{j_k}$. Справедлива следующая теорема.

Теорема 3. Маскирующий (модифицированный) секрет $\tilde{S}$ и вычет $\tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right)$ 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

$$Q = Q\left(\tilde{S}; J\_k\right) = \frac{\tilde{S}}{P_{J\_k}} \tag{15}$$

кратно модулю p.

Доказательство. Предположим, что число $\tilde{S}$ и вычет $\tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right)$ по модулю P_{J_k} при делении на p дают один и тот же остаток. Ввиду (14) в этом случае

$$\left|\tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right)\right|_p = \left|\tilde{S}\right|_p = S.$$

При этом

$$\tilde{S} \equiv \tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right)(\mathrm{mod}\, p).$$

Отсюда следует, что разность $\tilde{S} - \tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right)$ нацело делится на p. Согласно лемме Эвклида из теории делимости [1] ЦЧ $\tilde{S}$ с учетом обозначения (15) представимо в виде

$$\tilde{S} = \tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right) + \frac{\tilde{S}}{P_{J\_k}} P_{J\_k} =$$
$$= \tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right) + Q\left(\tilde{S}; J\_k\right) P_{J\_k}.$$

Следовательно

$$\tilde{S} - \tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right) = Q\left(\tilde{S}; J\_k\right) P_{J\_k}. \qquad (16)$$

Так как левая часть равенства (16) при принятом предположении нацело делится на p, а модуль p взаимно прост со всеми основаниями базиса **P** криптосхемы (см. пункт **А**), то ЦЧ $Q\left(\tilde{S}; J\_k\right)$ кратно p.

Пусть теперь ЦЧ $Q\left(\tilde{S}; J\_k\right)$ нацело делится на p, тогда из (16) вытекает делимость разности $\tilde{S} - \tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right)$ на модуль p. Это означает, что $\tilde{S} \equiv \tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right)(\mathrm{mod}\, p)$. Таким образом, из кратности числа $Q\left(\tilde{S}; J\_k\right)$ модулю p следует равноостаточность по данному модулю $\tilde{S}$ и $\tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right)$.

Теорема доказана.

Как показывает теорема 3, непересекаемость диапазона (9) принадлежности результатов $\tilde{S}$ маскирования секрета S с диапазонами $\mathbf{Z}_{P_{J\_k}}$ МСС, определяемых базисами $\mathbf{P}_{J\_k}$, полностью не исключает возможность восстановления k абонентами ($2 \leqslant k < t$) секрета S по соответствующим маскирующим аналогам — по модулярным кодам $(\tilde{\sigma}_{j_1}, \tilde{\sigma}_{j_2}, \ldots, \tilde{\sigma}_{j_k})$ вычетов $\tilde{S}\left(\mathrm{mod}\, P_{J\_k}\right)$. Это обеспечивает нейтрализация элементов диапазона $\mathbf{C} = \{C_{\text{НП}}, C_{\text{НП}} + 1, \ldots, C_{\text{ВП}}\}$ изменения псевдослучайного параметра C ($C_{\text{НП}}$ и $C_{\text{ВП}}$ — нижний и верхний пороги для C), которые порождают ЦЧ $Q\left(\tilde{S}; J\_k\right)$ вида (15), кратные модулю p. Искомые достаточные условия того, чтобы рассматриваемая (t, n)-криптосхема разделения секрета была пороговой, дает следующая теорема.

Теорема 4. Пусть $p_1, p_2, \ldots, p_n$ — упорядоченные по возрастанию попарно простые большие натуральные числа, используемые в качестве оснований модулярной криптосхемы разделения секрета $S \in \mathbf{Z}_p = \{0, 1, \ldots, p-1\}$ (p — большое число, взаимно простое со всеми $p_1, p_2, \ldots, p_n$) между n абонентами путем наделения их маскирующими частичными секретами $\tilde{\sigma}_i = \left|\tilde{S}\right|_{p_i}$ $\left(i = \overline{1, n}\right)$, где $\tilde{S} = S + Cp$; C — псевдослучайный целочисленный параметр. Для того чтобы любые l абонентов ($2 \leqslant t \leqslant l \leqslant n$; t — фиксированное ЦЧ), за которыми закреплены основания $p_{i_1}, p_{i_2}, \ldots, p_{i_l}$ $(1 \leqslant i_1 < i_2 < \ldots < i_l \leqslant n)$, могли восстановить секрет S по набору принадлежащих им частичных секретов — модулярному коду $\left(\tilde{\sigma}_{i_1}, \tilde{\sigma}_{i_2}, \ldots, \tilde{\sigma}_{i_l}\right)$ маскирующего секрета $\tilde{S}$, но никакая группа, включающая $k<t$ абонентов, которым отвечают основания $p_{j_1}, p_{j_2}, \ldots, p_{j_k}$ $(1 \leqslant j_1 < j_2 < \ldots < j_k \leqslant n)$, не имела возможности восстановления S по коду $(\tilde{\sigma}_{j_1}, \tilde{\sigma}_{j_2}, \ldots, \tilde{\sigma}_{j_k})$, достаточно выполнения следующей системы условий:

$$\begin{cases} \tilde{S} \in \left\{\tilde{S}_{\text{НП}}, \tilde{S}_{\text{НП}} + 1, \ldots, \tilde{S}_{\text{ВП}}\right\} \subseteq \\ \subseteq \{\_P_{t-1}, \_P_{t-1} + 1, .., p_0 P_{t-1} - 1\}, \\ C \in \left(\mathbf{C} \backslash \mathbf{C}_p\right), \end{cases} \qquad (17)$$

где $\tilde{S}_{\text{НП}}$ и $\tilde{S}_{\text{ВП}}$ — используемые нижнее и верхнее значения секрета-маски $\tilde{S}$;

$$\_P_{t-1} = \prod_{s=0}^{t-2} p_{n-s};\ P_{t-1} = \prod_{s=1}^{t-1} p_s;$$
$$\mathbf{C} = \{C_{\text{НП}}, C_{\text{НП}} + 1, \ldots, C_{\text{ВП}}\}$$
$$(C_{\text{НП}} = \lfloor \tilde{S}_{\text{НП}} / p \rfloor;\ C_{\text{ВП}} = \lfloor \tilde{S}_{\text{ВП}} / p \rfloor);$$
$$\mathbf{C}_p = \{C \in \mathbf{C} | S + Cp \in (\tilde{S}_{\text{НП}}; \tilde{S}_{\text{ВП}});$$

p — делитель ЦЧ $Q\left(\tilde{S}; J_k\right) = \dfrac{\tilde{S}}{P_{J_k}}$
$(1 \leqslant j_1 < j_2 < \ldots < j_k \leqslant n;\ 2 \leqslant k < t)\}$.

Сформулированная теорема практически является следствием теорем 1—3.

Элементы множества $\mathbf{C}_p$ из (17) могут быть рассчитаны предварительно и записаны в память. Сложность операции проверки принадлежности к $\mathbf{C}_p$ значений псевдослучайного параметра C при их генерировании в процессе маскирования секрета S по правилу (1), как того требует теорема 4, в решающей мере определяется мощностью $|\mathbf{C}_p|$ множества $\mathbf{C}_p$. В свете сказанного важнейшим оптимизационным аспектом проблемы синтеза модулярной пороговой (t, n)-криптосхемы разделения секрета, базирующейся на теореме 4, является минимизация характеристики $|\mathbf{C}_p|$.

4. Обсуждение результатов исследования

Конечной целью представляемого направления исследований является повышение эффективности модулярных пороговых схем разделения секрета за счет использования минимально избыточного кодирования. Разработанная теоретическая база МА-схем рассматриваемого класса позволяет уменьшить (в сравнении с аналогами) реализационные затраты (временные и аппаратурные) на выполнение этапа восстановления секрета-оригинала по наборам долевых секретов, принадлежащих группам абонентов числом не меньше порогового значения t, причем с обеспечением необходимого уровня криптостойкости.

Декодирующие процедуры (процедуры восстановления секрета-оригинала) как в неизбыточных, так и в минимально избыточных МСС базируются на операциях расширения кода. Выполнение этих операций с применением прямых реализаций китайской теоремы об остатках, т.е. выражений типа

$$\left|\tilde{S}\right|_{M_l} = \left|\sum_{j=1}^{l} M_{j,l} \left|M_{j,l}^{-1}\tilde{\sigma}_j\right|_{m_j}\right|_{M_l},$$

где $M_l = \prod_{s=1}^{l} m_s$; $M_{j,l} = \dfrac{M_l}{m_j}$; $m_1, m_2, \ldots, m_l$ — основания МСС (см. теорему 2), неэффективны, так как требуют вычислений по очень большим модулям M_l. Гораздо меньшей сложностью обладают процедуры, которые синтезируются на основе позиционных форм модулярных чисел, использующих интегральные характеристики кода, такие как ранг $\rho_l(\tilde{S})$ или коэффициенты полиадического представления ЦЧ $\tilde{S}$ [1, 3]. В частности, расчетное соотношение операции расширения кода на некоторый модуль m с помощью ранговой формы модулярных чисел имеет вид

$$\left|\tilde{S}\right|_m = \left|\sum_{j=1}^{l} M_{j,l} \left|M_{j,l}^{-1}\tilde{\sigma}_j\right|_{m_j} - M_l \rho_l(\tilde{S})\right|_m. \qquad (18)$$

В неизбыточной МСС вычисление характеристики $\rho_l(\tilde{S})$ занимает время порядка $O(l^2)t_{\text{сл}}$, где $t_{\text{сл}}$ — длительность операции сложения двух ЦЧ. Что касается минимально избыточной МСС, то формирование в ней базовой интегральной характеристики — интервального индекса по расчетным соотношениям (11)—(13) — осуществляется за l сложений. В сравнении с рангом это обеспечивает как минимум l-кратное сокращение временных затрат. Адекватное увеличение быстродействия достигается и для операции расширения кода (см. (10)—(13), (18)), а в конечном счете и для всего процесса восстановления секрета-оригинала S по коду $\left(\tilde{\sigma}_{i_1}, \tilde{\sigma}_{i_2}, \ldots, \tilde{\sigma}_{i_l}\right)$ [1, 9].

Отмеченное повышение производительности пороговой МИМА-схемы разделения секрета в сравнении с неизбыточными МА-аналогами достигается с сохранением предусматриваемого пороговым принципом уровня криптостойкости. Возникающие в рамках применяемого подхода для модулярного разделения секрета критические ситуации, описываемые ***теоремами 3*** и ***4***, устраняются путем нейтрализации соответствующих значений псевдослучайного параметра C в процессе генерирования маскирующего секрета $\tilde{S} = S + Cp$ (см. теорему 4).

Заключение

Основные результаты представленных в статье исследований по модулярным пороговым схемам состоят в нижеследующем.

1. Проведена формализация модели пороговой криптосхемы разделения секрета, компьютерно-арифметической базой которой служит МИМА. Благодаря снижению до теоретического минимума вычислительной сложности расчетных соотношений используемой в МИМА интегральной характеристики кода (интервального индекса) в рамках исследуемой модели достигается более высокий (в сравнении с традиционными решениями) уровень производительности на стадии декодирования секрета-оригинала.

2. Исходя из критерия простоты реализации для маскирования секрета-оригинала выбрана линейная функция с аддитивной вариационной компонентой псевдослучайного типа, которая кратна модулю p кольца принадлежности секрета. Это дает возможность выполнения декодирующей операции с помощью быстродействующих МИМА-процедур Монтгомери [9]. Показано, что адаптивное согласование диапазона изменения псевдослучайного параметра маскирующей функции с областью ее значений позволяет осуществлять минимально избыточную модулярную декомпозицию функции маскирования при любом допустимом базисе оснований схемы. Таким образом, минимально избыточные модулярные вычислительные структуры представляют

собой качественно новый инструментарий для реализации в пороговых схемах разделения секрета всех необходимых операций как при маскировании исходного секрета, так и в процессе его восстановления по кодам маскирующего аналога.

3. Для (t,n)-пороговой МИМА-схемы разделения секрета получены достаточные условия непересекаемости диапазона изменения секрета-маски с диапазонами МСС, определяемых k-компонентными базисами ($2 \leqslant k < t$), а также необходимое и достаточное условия равноостаточности по модулю p маскирующего секрета и отвечающего ему вычета в некоторой k-модульной МСС. Доказанные теоретические положения составляют основу корректной минимально избыточной реализации порогового принципа разделения секретной информации с обеспечением свойственного для схем исследуемого класса уровня криптостойкости.

Список литературы

1. **Червяков Н. И., Коляда А. А., Ляхов П. А.** и др. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. М.: ФИЗМАТЛИТ, 2017. 400 с.

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

3. **Червяков Н. И.** и др. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: Физматлит, 2012. 280 с.

4. **Galibus T. V., Matveev G. V.** Finite fields Grobner bases and modular secret sharing // J. of discrete mathematical sciences. 2012. Vol. 15, N. 6. P. 339—348.

5. **Schinianakis D., Stouraitis T.** Multifunction recidue architectures for cryptography // IEEE Trans. Circuits and Syst. I. 2014. Vol. 61, N. 4. P. 1156—1169.

6. **Alhasan A., Saeed I. Agbelnab.** The Hoffman's Method of Secured Data Encoding and Error Correction Using Residue Number System (RNS) // Communications and applied electronics (CAE). 2015. Vol. 2, N. 9. P. 14—18.

7. **Zalekian Azin, Mohammad Esmaeildoust, Amer Kaabi.** Efficient implementation of NTRU cryptography using residue number system // Int. Journal of Computer Applications. 2015. Vol. 124, N. 7. P. 33—37.

8. **Чен Ц., Яцкив В., Саченко А., Су Ц.** Беспроводные сенсорные сети на основе модулярной арифметики // Известия высших учебных заведений. Радиоэлектроника. 2017. Т. 60, N. 5. С. 274—285.

9. **Патент** на изобретение № 2652450 РФ.МПК:J06F7/57, H03K19/00. Устройство вычисления модулярного произведения Монтгомери / Н. И. Червяков (RU), А. А. Коляда (BY), В. А. Кучуков (RU), М. Г. Бабенко (RU). Заявка № 2017129526. Приоритеты: дата подачи заявки — 18.08.2017. Опубл. 26.04.2018, бюл. № 12.

10. **Gayathri B. NVSK, Rajendra G.** Efficient access control for security of cloud storage systems using RNS cryptography // Int. J. of Scientific research in computer science, engineering and information technology. 2018. Vol. 3, Iss. 4. P. 403—407.

11. **Bahramian Mojtaba, Khadijeh Eslami.** An efficient threshold verifiable multisecret sharing scheme using generalized jacobian of elliptic curves // Journal of algebraic structures and their applications. 2017. Vol. 4, Iss. 2. P. 45—55.

12. **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.

13. **Харин Ю. С., Берник В. И., Матвеев Г. В.** и др. Математические и компьютерные основы криптологии. Мн.: Новое знание, 2003. 382 с.

14. **Инютин С. А.** Основы модулярной алгоритмики. Ханты-Мансийск: Полиграфист, 2009. 347 с.

15. **Оцоков Ш. А.** Способ организации высокоточных вычислений в модулярной арифметике // Первая Международная конференция "Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах". Ставрополь, РФ, 20—24 окт., 2014. Сб. науч. тр. Ставрополь: ИИЦ "Фабула", 2014. С. 270—277.

16. **Комарова Ю. А., Талалаев И. А.** Аналитический обзор методов и структур для работы с большими данными // Первая Международная конференция "Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах". Ставрополь, РФ, 20—24 окт., 2014. Сб. науч. тр. Ставрополь: ИИЦ "Фабула", 2014. С. 477—485.

17. **Афонин М. С.** Способ обработки больших чисел на ПЛИС с малой ресурсной мощностью // Первая Международная конференция "Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах". Ставрополь, РФ, 20—24 окт., 2014. Ставрополь: ИИЦ "Фабула", 2014. С. 511—520.

18. **Shamir A.** How to share a secret // Communications of the ACM. 1979. Vol. 22, N. 11. P. 612—613.

19. **Шнайер Б.** Алгоритмы разделения секрета. Схема интерполяционных полиномов Лагранжа // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Н.: Триумф, 2002. С. 588—589.

20. **Blakley G. R.** Safe guarding cryptographic keys // Proc. Of the 1979 AFIPS national computer conference. Montvale: AFIPS press, 1979. P. 313—317.

21. **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.

22. **Shiong, Jian Shyu, Ying- Ru Chen.** Treshold secret image sharing by Chinese remainder theorem // IEEE Asia — Pacific Services Computing conference. 2008. Vol. 1. P. 1332—1337.

23. **Коляда А. А., Пак И. Т.** Модулярные структуры конвейерной обработки цифровой информации. Минск: Университетское, 1992. 256 с.

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,
Research establishment "Institute of Applied Physics Problems of A. N. Sevchenko" Belarusian State University,
N. I. Chervyakov, Doctor of Technical Sciences, Professor, e-mail: Chervyakov@yandex.ru, whbear@yandex.ru,
Federal State Autonomous Educational Institution of Higher Professional Education
"North-Caucasus Federal University"

The Threshold Method of Secret's Division Based on Redundant Modular Computing Structures

The article describes the formalization of the threshold method of modular separation of secret using minimally redundant coding. In particular, the conditions were determined to ensure the possibility of using minimum redundant modular arithmetic (MRMA) as the computer-arithmetic basis for the use in threshold cryptographic schemes of secret separation. In comparison with no redundant analogues, the MRMA allows to minimize the complexity of the operation of restoration of the secret-original on the basis of the share secrets belonging to groups of subscribers.

The conditions for the correctness of the threshold principle in the framework of modular coding are also obtained, and on this basis a method has been developed for neutralizing critical situations with ensuring an adequate level of cryptographic resistance.

Keywords: *separation of the secret, minimally redundant modular arithmetic, horny scheme of modular separation of the secret, pseudo-random masking function, distributed computing*

DOI: 10.17587/it.25.553-561

References

1. **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).

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

3. **Chervjakov N. I.** The use of artificial neural networks and the residual class system in cryptography, Moscow, FIZMATLIT Publ., 2012, 280 p. (in Russian).

4. **Galibus T. V., Matveev G. V.** Finite fields Grobner bases and modular secret sharing, *J. of discrete mathematical sciences*, 2012, vol. 15, no. 6, pp. 339—348.

5. **Schinianakis D., Stouraitis T.** Multifunction recidue architectures for cryptography, *IEEE Trans. Circuits and Syst. I,* 2014, vol. 61, no. 4, pp. 1156—1169.

6. **Alhasan A., Saeed I. Agbelnab.** The Hoffman's Method of Secured Data Encoding and Error Correction Using Residue Number System (RNS), *Communications and applied electronics (CAE),* 2015, vol. 2, no. 9, pp. 14—18.

7. **Zalekian Azin, Mohammad Esmaeildoust, Amer Kaabi**. Efficient implementation of NTRU cryptography using residue number system*, Int. Journal of Computer Applications*, 2015, vol. 124, no. 7, pp. 33—37.

8. **Chen Ts., Yatskiv V., Sachenko A., Su Ts.** Wireless sensor networks based on modular arithmetic, *Izvestiya vysshikh uchebnykh zavedeniy. Radioelektronika (Proceedings of higher educational institutions. Radio electronics*), 2017, vol. 60, no. 5, pp. 274—285 (in Russian).

9. **Chervyakov N. I.** (RU), **Kolyada A. A.** (BY), **Kuchukov V. A.** (RU), **Babenko M. G.** (RU). The patent for the invention no. 2652450 РФ.МПК:J06F7/57,H03K19/00. Ustroystvo vychisleniya modulyarnogo proizvedeniya Montgomeri (Montgomery Modular Product Computing Device) Application no. 2017129526. Priorities: filing date — 18.08.2017. Posted by 26.04.2018, bulletin no. 12 (in Russian).

10. **Gayathri B. NVSK, Rajendra G.** Efficient access control for security of cloud storage systems using RNS cryptography*, Int. J. of Scientific research in computer science, engineering and information technology*, 2018, vol. 3, iss. 4, pp. 403—407.

11. **Bahramian Mojtaba, Khadijeh Eslami.** An efficient threshold verifiable multisecret sharing scheme using generalized jacobian of elliptic curves, *Journal of algebraic structures and their applications*, 2017, vol. 4, iss. 2, pp. 45—55.

12. **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.

13. **Kharin Yu. S., Bernik V. I., Matveyev G. V.** Mathematical and computer fundamentals of cryptology, Minsk, Novoye znaniye, 2003, 382 p. (in Russian).

14. **Inyutin S. A.** Basics of modular algorithms, Khanty-Mansiysk, Poligrafist, 2009, 347 p. (in Russian).

15. **Ocokov Sh. A.** The way to organize high-precision calculations in modular arithmetic, *Pervaja mezhdunarodnaja konferencija "Parallel'naja komp'juternaja algebra i ee prilozhenija v novyh infokommunikacionnyh sistemah",* Stavropol, Russian Federation, 20—24 okt., 2014, Fabula Publ., 2014, pp. 270—277 (in Russian).

16. **Komarova Ju. A., Talalaev I. A.** Analytical review of methods and structures for working with large data, *Pervaja mezhdunarodnaja konferencija "Parallel'naja komp'juternaja algebra i ee prilozhenija v novyh infokommunikacionnyh sistemah",* Stavropol, Russian Federation, 20—24 okt., 2014, Fabula Publ., 2014, pp. 477—485 (in Russian).

17. **Afonin M. S.** The way of processing large numbers on a FPGA with a small resource capacity, *Pervaja mezhdunarodnaja konferencija "Parallel'naja komp'juternaja algebra i ee prilozhenija v novyh infokommunikacionnyh sistemah",* Stavropol, Russian Federation, 20—24 okt., 2014, Fabula Publ., 2014, pp. 511—520 (in Russian).

18. **Shamir A.** How to share a secret, *Communications of the ACM*, 1979, vol. 22, no. 11, pp. 612—613.

19. **Shnajer B.** Secret sharing algorithms. Lagrange interpolation polynomial scheme, *Applied cryptography. Protocols, algorithms and source code in C*, N., Triumf, 2002, pp. 588—589 (in Russian).

20. **Blakley G. R.** Safe guarding cryptographic keys. Of the 1979 AFIPS national computer conference, Montvale, AFIPS press, 1979, pp. 313—317.

21. **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.

22. **Shiong Jian Shyu, Ying- Ru Chen**. Treshold secret image sharing by Chinese remainder theorem, *IEEE Asia — Pacific Services Computing conference*, 2008, vol. 1, pp. 1332—1337.

23. **Koljada A. A., Pak I. T.** Modular structures of conveyor processing of digital information, Minsk, Universitetskoe, 1992, 256 p. (in Russian).