Check for updates

УДК 004.832, 519.6
DOI: 10.37661/1816-0301-2025-22-1-90-97

Оригинальная статья
Original Article

Адаптация модулярной системы счисления в пороговых схемах разделения секрета

А. Ф. Чернявский, Е. И. Козлова✉, В. С. Садов, А. А. Коляда

Белорусский государственный университет,
пр. Независимости, 4, Минск, 220030, Беларусь
✉E-mail: kozlova@bsu.by

Аннотация

Цели. Целью проведенных исследований является проверка применимости варианта адаптации модулярной системы счисления с использованием маскирующего преобразования с псевдослучайной целочисленной величиной к секрету-оригиналу S в модификации (k, n)-пороговой схемы Ади Шамира разделения секрета для сведения к теоретическому минимуму сложности расчета базовой интегральной характеристики.

Методы. Рассмотрена модификация схемы Ади Шамира разделения секрета в пороговой криптосистеме на основе модулярной арифметики (МА-криптосистеме) с генерацией долей участников разделения секрета в два этапа. Схема Шамира выбрана как оптимальная по параметрам сложности, ресурсоемкости, совершенности и идеальности. Кроме того, она масштабируема – количество участников можно увеличивать до порядка поля p, при этом не меняется способность восстанавливать секрет. Применено маскирующее преобразование с использованием слагаемого с псевдослучайной целочисленной величиной C для разделяемого секрета S и согласование диапазона изменения псевдослучайного параметра C и области изменения значений оригинала сигнала. Применена также интервально-модулярная форма числа значения секрета.

Результаты. Показано, что использование интервально-модулярной формы числа $\overline{S}$ – маскирующего преобразования с псевдослучайным параметром числа S секрета-оригинала – снижает сложность расчета базовых интервально-индексных характеристик при решении задач порогового кодирования практически до теоретического минимума. Адаптивное согласование диапазона изменений псевдослучайного параметра маскирующей функции с областью ее значений позволяет реализовать минимально избыточную модулярную декомпозицию функции маскирования при любом допустимом базисе оснований схемы.

Заключение. Результаты представленной работы позволяют для модулярных пороговых криптосистем разделения секрета в распределенных системах обработки данных сделать вывод о том, что применение линейной маскирующей функции и сужение области изменения маскирующего аналога $\tilde{S}$ секрета-оригинала S, допускающее при выбранных $p_1, p_2, \ldots, p_n$ минимально избыточное кодирование, обусловливают существенное снижение вычислительной сложности расчетных соотношений минимально-избыточной модулярной арифметики интегральных характеристик в рамках исследуемой модели. Благодаря этому достигается более высокий уровень производительности на стадии декодирования секрета-оригинала по сравнению с другими решениями.

Ключевые слова: минимальная избыточность, модулярное кодирование, маскирующее преобразование, пороговая криптосистема, секрет-оригинал, интервальные характеристики

Благодарности. Работа выполнена в рамках Государственной программы научных исследований «Цифровые и космические технологии, безопасность общества и государства» (подпрограмма «Цифровые технологии и космическая информатика», задание 5.1.6.3), 2021–2025 гг.

Для цитирования. Адаптация модулярной системы счисления в пороговых схемах разделения секрета / А. Ф. Чернявский, Е. И. Козлова, В. С. Садов, А. А. Коляда // Информатика. – 2025. − Т. 22, № 1. – С. 90–97. – DOI: 10.37661/1816-0301-2025-22-1-90-97.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию | Received 31.01.2025
Подписана в печать | Accepted 14.02.2025
Опубликована | Published 31.03.2025

Adaptation of the modular number system in threshold secret sharing schemes

Alexander F. Chernyavskiy, Alena I. Kazlova✉, Vasiliy S. Sadov, Andrei A. Kolyada

Belarusian State University,
av. Nezavisimosti, 4, Minsk, 220030, Belarus
✉*E-mail: kozlova@bsu.by*

Abstract

Objectives. The purpose of the research is to test the applicability of the adaptation of the modular number system using a masking transformation with a pseudo-random integer value to the original secret *S* in a modification of Adi Shamir's (*k*, *n*)-threshold secret sharing scheme to reduce the complexity of calculating the basic integral characteristic to a theoretical minimum.

Methods. A modification of Adi Shamir's secret sharing scheme in a threshold cryptosystem based on modular arithmetic (MA cryptosystem) with the generation of shares of secret sharing participants in two stages is considered. Shamir's scheme was chosen as optimal in terms of complexity, resource intensity, perfection and ideality; in addition, it is scalable – the number of participants can be increased to the order of the field *p*, without changing the ability to recover the secret. A masking transformation using a term with a pseudo-random integer value *C* for the shared secret *S*, the range of change of the pseudo-random parameter *C* agreed upon the range of changes in the values of the original signal is applied. The interval-modular form of the number of the secret value is applied too.

Results. It is shown that the use of the interval-modular form of the number $\bar{S}$ – a masking transformation with a pseudo-random parameter of the number *S* of the original secret – reduces the complexity of calculating basic interval-index characteristics when solving threshold coding problems almost to a theoretical minimum. Adaptive coordination of changes in the pseudo-random parameter of the masking function with the domain of its results makes it possible to implement a minimally redundant modular decomposition of the masking function for any admissible basis of the based scheme.

Conclusion. The results of the presented work allow to conclude for modular threshold cryptosystems of secret sharing in distributed data processing systems that the use of a linear masking function and narrowing the range of changes in the masking analogue $\tilde{S}$ of the original secret *S*, allowing for minimally redundant coding for the selected $p_1, p_2, \ldots, p_n$, causes a significant reduction in the computational complexity of the calculated minimal-redundant modular arithmetic relations of integral characteristics within the framework of the model under study. Due to which a higher level of performance is achieved at the stage of decoding the original secret compared to other solutions.

Keywords: minimal redundancy, modular coding, masking transformation, threshold cryptosystem, secret-original, interval characteristics

Acknowledgments. The work was carried out within the framework of the state scientific research program "Digital and space technologies, security of society and the state" (subprogram "Digital technologies and space informatics", task 5.1.6.3), 2021–2025.

For citation. Chernyavskiy A. F., Kazlova A. I., Sadov V. S., Kolyada A. A. *Adaptation of the modular number system in threshold secret sharing schemes*. Informatika [*Informatics*], 2025, vol. 22, no. 1, pp. 90–97 (In Russ.). DOI: 10.37661/1816-0301-2025-22-1-90-97.

Conflict of interest. The authors declare of no conflict of interest.

Введение. Обеспечение информационной безопасности информационных и инфокоммуникационных систем является сегодня одной из приоритетных задач как при разработке и реализации таких систем, так и при их эксплуатации. В процессе функционирования информационных систем применяются технологии активной безопасности, включающие такие методы защиты от прямых угроз, как периодическое обновление секретной информации и ее пространственное разделение. Одновременное использование этих методов позволяет повысить уровень безопасности систем криптографической защиты информации. Методы пространственного разделения информации основаны на возможности ее разделения между несколькими пользователями системы так, что применить ключ можно только с помощью части информации определенного числа участников разделения ключа из всего числа «хранителей» этих частей. Периодичность смены ключевой информации (в частности, криптографических ключей) в сочетании со случайным характером изменений и времени их проведения характерна для всех систем активной безопасности. Для того чтобы обеспечить доступность, конфиденциальность и целостность данных, в частности надежное хранение, применяются системы криптографического разделения секрета, отвечающие в том числе и требованиям периодичности, случайности и внезапности изменения ключей. К наиболее часто используемым системам такого типа относятся, например, пороговые схемы Шамира, Блэкли, Карнина – Грина – Хеллмана, Асмута – Блума и схема разделения секрета, основанная на эллиптической кривой [1–4]. Эти схемы решают задачу генерации ключей, применяя криптографически стойкие алгоритмы с использованием генератора псевдослучайной последовательности для получения таких последовательностей, которые статистически неотличимы от абсолютно случайных последовательностей, т. е. значения сгенерированной последовательности оказываются непредсказуемыми. Пороговая схема Шамира разделения секрета многими авторами указывается как наиболее эффективная среди известных. Хотя она не является наиболее быстрой, но оказывается оптимальной по ресурсоемкости, совершенности и идеальности и имеет простой способ разделения секрета [1–4].

Известно, что компьютерно-арифметической базой средств защиты информации является арифметика больших целых чисел [4]. При этом на практике эффективность вычислительного аппарата криптопреобразований определяется возможностями перевода вычислений из категории больших целых чисел в категорию целых чисел стандартной разрядности. Это обусловливает актуальность применения арифметики модулярных систем счисления (МСС) [4] для построения пороговых криптосхем разделения секрета. МСС обладает естественным кодовым параллелизмом. Вопрос производительности, в частности скорости проведения вычислений, является очень чувствительным в криптографических приложениях, что также обусловливает целесообразность применения в них модулярной арифметики. Модулярное кодирование позволяет достаточно просто произвести разделение секрета на части для участников с минимальными временными и аппаратными затратами в диапазонах больших чисел. Кроме задачи повышения производительности, применение МСС позволяет решить также задачу снижения трудоемкости процедуры восстановления ключа-оригинала по частичным секретам, выданным некоторой группе участников при его разделении.

В процессе анализа функциональных возможностей различных технологий вычисления установлено, что при использовании МСС введение в модулярный код минимальной избыточности существенно упрощает оценку интегральных характеристик и связанных с ними форм представления целых чисел [5, 6]. Это позволяет в том числе сократить до минимума временные и аппаратные затраты на выполнение операции восстановления ключа-оригинала. Интегральные характеристики модулярного кода (ИХМК) включают: ранговое число, интервальный индекс и его евклидовы компоненты.

Решающее правило, реализуемое (t, n)-пороговой системой разделения секрета, рассчитано на полное число $<n>$ и пороговое число $<t>$ абонентов. Ряд участников t разделения секрета из полного их числа n, которые могут получать секретные данные, считаются разрешенным множеством, или разрешенной коалицией участников. При этом в распределенных системах наиболее перспективной технологией защиты данных считается технология активной безопасности,

т. е. число абонентов такого множества должно быть больше одного. Множества участников, которые не могут получать секретные данные, относятся к запрещенной коалиции (множеству).

Интегральные характеристики модулярного кода и декодирующие процедуры восстановления секрета-оригинала в пороговых криптосхемах. На основе положений минимально избыточной модулярной арифметики (МИМА) разработан метод [7] выполнения декодирующей процедуры в пороговом устройстве разделения секрета и связанных с ней немодульных операций: расширения кода, масштабирования, деления целых чисел, преобразования модулярного кода, контроля ошибок и др., включая вычисление и использование множеств ИХМК, знаков или цифр полиадического кода. Многообразие применяемых формирователей ИХМК свидетельствует о их ключевой роли в модулярных арифметических устройствах автоматического управления. Благодаря оригинальности своей структуры они могут быть сформированы в рамках единого алгоритма [6]. Что касается машинной арифметики, то для построения любых ее вариантов как с фиксированной, так и с плавающей запятой достаточно сформировать следующий базовый набор ИХМК:

$$<x_1^-, x_2^-, \ldots, x_k^-; \hat{I}_k(X); \theta(X), \theta^-(X)>, \quad (1)$$

где x_i^- – i-я цифра симметрического полиадического кода ($i = 1, 2, \ldots, k$); $\hat{I}_k(X)$ – машинный интервальный индекс числа x; $\theta(X)$ и $\theta^-(X)$ – поправки Амербаева, соответствующие числу X во вспомогательной МСС с основаниями $m_1, m_2, \ldots, m_{k-1}, m_0$; X – произвольный элемент рабочего диапазона с попарно простыми основаниями $m_1, m_2, \ldots, m_k$ ($m_k > 2m_0 + \rho$, $m_0 \geq \rho$).

Базовый набор ИХМК (1) может либо расширяться за счет включения в него характеристик, являющихся производными базовых, либо применяться в сокращенном по сравнению с базовым виде, оставляя в нем, например, только одну интегральную характеристику $\hat{I}_k(X)$ – интервальный индекс.

Пороговая схема разделения секрета. В работе [8] разработана реализация (k, n)-пороговой схемы Ади Шамира [9]. Ее функциональной особенностью является интерполяция многочлена с коэффициентами из заданного поля Галуа с p элементами, которые становятся долевыми секретами участников эксперимента. В предложенной в [8] реализации работа схемы осуществляется в два этапа. На первом этапе дилер генерирует $(k-1)$ элементов из заданного поля, которые становятся коэффициентами многочлена $F(i)$, где $i \in (1, \ldots, k = l)$. На втором этапе каждому из n участников назначается не равный нулю номер и дилер формирует его долю секрета – пару $(i, F(i))$, где i – порядковый номер участника, а $F(i)$ – значение многочлена в соответствующей точке.

Достоинством схемы Шамира считается масштабируемость, так как количество участников можно увеличивать до порядка поля p. При этом не меняется способность восстанавливать секрет. С учетом специфики задач восстановления секрета важна временна́я составляющая этой способности.

Рассмотрим множество $Z_m \equiv (0, 1, \ldots, m-1)$, каждый элемент $\chi = \left|\frac{A}{B}\right|_m$ которого удовлетворяет сравнению $B_\chi \equiv A \pmod{m}$ (A и B – целые числа, $B_m \neq 0$). Система сравнения, формирующая множество всех целых чисел X и соответствующих кодов, определяется следующим образом:

$$\begin{cases} X \equiv \chi_1 \bmod m_1, \\ X \equiv \chi_2 \bmod m_2, \\ \ldots\ldots\ldots\ldots \\ X \equiv \chi_k \bmod m_k. \end{cases} \quad (2)$$

В МСС с основаниями ($m_1, m_2, \ldots, m_s$) ($s > 1$) модулярный код целых чисел X представляется в виде

$$(\chi_1, \chi_2, \ldots, \chi_s) = (|X|_{m_1}, |X|_{m_2}, \ldots, |X|_{m_S}). \quad (3)$$

В пороговой МА-криптосистеме разделения секрета наиболее трудоемкой является операция восстановления секрета-оригинала. Фундаментальные особенности МИМА, включая ее интегрально-аппаратную составляющую, позволяют минимизировать временны́е затраты на выполнение трудоемких немодульных операций и относительно сложную операцию восстановления секрета-оригинала по модулярным кодам маскирующих аналогов групп абонентов.

Результаты и обсуждение. Пороговые МИМА-схемы разделения секрета существуют в двух вариантах. К первому относятся системы, работающие с абонентами, число l которых не меньше порогового значения t, а ко второму – системы, в которых группа абонентов имеет численность $k < t$. Приведенные далее рассуждения применимы для обоих вариантов.

Особенность использования минимально избыточного кодирования для пороговой (t, n)-криптосхемы разделения секрета состоит в следующем [6, 10].

Основания МСС характеризуются перечнем значений m_i (4), определяемых выбранным базисом, а цифры $\tilde{\sigma}_j$, определяемые уравнением (5), рассматриваются как долевые секреты:

$$m_i = P_{I_1} = \prod_{i=1}^{i} p_i \ (i = \overline{1, n}); \qquad \tilde{\sigma}_j = |\tilde{s}|_{mj} \ (j = \overline{1,l}). \tag{4}$$

Над секрет-оригиналом S в МСС с базисом P выполняется маскирующее преобразование с помощью простой в реализации линейной функции следующего вида:

$$\tilde{S} = S + C \cdot p, \tag{5}$$

где C – псевдослучайная целочисленная величина из множества, порождающего кратные модулю P целые числа. Имеет место сужение области изменения маскирующего аналога $\tilde{S}$. При этом, естественно, сокращаются объем и требуемое время декодирования секрета. Реализация при выбранном базисе $p_{\_1}$, $p_{\_2}$, …, $p_{\_n}$ минимально избыточного кодирования сводит к теоретическому минимуму сложность расчета базовой интегральной характеристики.

Применение величины C в маскирующей функции вносит вариационную аддитивную компоненту псевдослучайного типа так, что она кратна модулю P выбранного базиса оснований МСС.

Интервальный индекс $I_l(\tilde{s})$ числа $\tilde{s} = (\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ в МСС с базисом $\{m_1, m_2, \ldots, m_l\}$ определяется позиционной формой числа $\tilde{s}$ по базису M, вычисляемому согласно принципу минимального избыточного модулярного кодирования (теорема 2 [10]):

$$\tilde{s} = \sum_{j=1}^{l-1} M_{j,l-1} \left| M^{-1}_{i,l-1} \tilde{\sigma}_J \right|_{m_j} + M_{l-1} I_l(\tilde{s}). \tag{6}$$

Разделяемый <n> сторонами исходный секрет представляет собой целое число $S \in Z_P$, где P – большой модуль, взаимно простой с $p_1, p_2 \ldots, p_n$:

$$\begin{gathered} P_{i\_l} = \prod_{i=1}^{l} P_{il}; \\ P_{i\_k} = \prod_{i=1}^{k} P_{ik}; \\ P_{I\_l} = \{p_{i_1}, p_{i_2}, \ldots, p_{i_l}\}; \\ P_{I\_k} = \{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}. \end{gathered} \tag{7}$$

Долевыми частичными секретами одноименных абонентов считаются следующие величины:

$$\tilde{\Sigma}_i = |\tilde{s}|_{p_i} = \left| \sigma_i + |C_p|_{p_i} \right|_{p_i} \ (\sigma_i = S_{p_i}, \ i = \overline{1, n}). \tag{8}$$

Восстанавливать секрет-оригинал S можно только по маскирующим частичным секретам абонентов (t, n)-пороговой системы разделения секрета маскирующей функции $\tilde{s}$. Предусматривается согласование диапазона изменения псевдослучайного параметра $<C>$ и области изменения оригинала сигнала. Это позволяет применять минимально избыточную модулярную декомпозицию функции маскирования при любом допустимом базисе оснований схемы.

Интервальный индекс $I_l(\tilde{s})$ числа $\tilde{s} = (\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ диапазона $\{\_P_{t-1}, \_P_{t-1} + 1, \ldots, p_0 P_{t-1} - 1\}$, где p_0 – вспомогательный модуль в МСС с базисом $\{m_1, m_2, \ldots, m_l\}$, полностью определяется компьютерным вычетом интервального индекса $\hat{I}_l(\tilde{s}) = | I_l(\tilde{s}) |_{m_l}$ только в случаях безусловного выполнения следующего требования [7]:

$$m_l \geq p_0 + l - 2 \ (p_0 \geq 2);$$

$$I_l(\tilde{s}) = \begin{cases} \hat{I}_l(\tilde{s}), \text{ если } \hat{I}_l(\tilde{s}) < p_0; \\ \hat{I}_l(\tilde{s}) - m_l, \text{ если } \hat{I}_l(\tilde{s}) \geq p_0; \end{cases}$$

$$\hat{I}_l(\tilde{s}) = \left| \sum_{j=1}^{l} R_{j,l}(\tilde{\sigma}_J) \right|_{m_l}; \ R_{j,l}(\tilde{\sigma}_j) = \left| M_{l-1}^{-1} \tilde{\sigma}_j \right|_{m_l}; \tag{9}$$

$$R_{j,l}(\tilde{\sigma}_J) = \left| -m_j^{-1} \left| M_{J,l-1}^{-1} \tilde{\sigma}_j \right|_{m_j} \right|_{m_l} \ (j \neq l).$$

Использование интервально-модулярной формы числа $\overline{S}$ снижает сложность расчета базовых интервально-индексных характеристик при решении задач порогового кодирования практически до теоретического минимума.

Процедуру выбора рабочего диапазона изменения секрета-маски необходимо совмещать с поиском условий, обеспечивающих непересекаемость диапазонов (множеств) целых чисел $\tilde{S}_{I\_i} \pmod{P_{I\_i}}$ [10].

Корректность пороговых МА-криптосистем разделения секрета во многом зависит от оптимальности множества псевдослучайных целочисленных величин, используемых при проведении маскирующего преобразования (5). Оптимизация может выполняться по мощности этого множества, его структуре или другим характеристикам. Важнейшим оптимизационным аспектом рассмотренной проблемы синтеза модулярной пороговой (t, n)-криптосхемы разделения секрета является минимизация мощности $|C_p|$ множества $C_p \in (\tilde{S}_{\text{НП}}, \tilde{S}_{\text{ВП}})$, где $\tilde{S}_{\text{НП}}$ и $\tilde{S}_{\text{ВП}}$ – нижнее и верхнее значения секрета. Параметры множества C_p рассчитываются предварительно и записываются в память.

Заключение. Результаты представленной работы позволяют сделать следующие выводы для модулярных пороговых криптосистем разделения секрета в распределенных системах обработки данных:

1. Применение линейной маскирующей функции и сужение области изменения маскирующего аналога $\tilde{S}$ секрета-оригинала S, допускающее при выбранных $p\_1, p\_2, \ldots, p\_n$ минимально избыточное кодирование, обусловливает существенное снижение вычислительной сложности расчетных соотношений МИМА интегральных характеристик в рамках исследуемой модели, благодаря чему достигается более высокий уровень производительности на стадии декодирования секрета-оригинала по сравнению с другими решениями.

2. Адаптивное согласование диапазона изменений псевдослучайного параметра маскирующей функции с областью ее значений позволяет реализовать минимально избыточную модулярную декомпозицию функции маскирования при любом допустимом базисе оснований схемы.

3. Для оптимального решения проблемы синтеза модулярной пороговой (t, n)-криптосхемы разделения секрета необходимо минимизировать мощность множества $C_p \in (\tilde{S}_{\text{НП}}, \tilde{S}_{\text{ВП}})$, где $\tilde{S}_{\text{НП}}$ и $\tilde{S}_{\text{ВП}}$ – нижнее и верхнее значения секрета.

Вклад авторов. *А. Ф. Чернявский* и *А. А. Коляда* разработали концепцию и основные положения работы, *А. Ф. Чернявский, Е. И. Козлова* и *В. С. Садов* провели критический анализ содержания статьи и подготовили окончательный вариант работы для публикации.

Список использованных источников

1. Артюхов, Ю. В. Анализ схем разделения секрета, использующих вероятностный и комбинаторный подход в реализации пороговых криптосистем, функционирующих в распределенных компьютерных системах / Ю. В. Артюхов // Актуальные вопросы технических наук : материалы Междунар. заоч. науч. конф., Пермь, июль 2011 г. / под общ. ред. Г. Д. Ахметовой. – Пермь : Меркурий, 2011. – 80 с.

2. Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц ; пер. с англ. М. А. Михайловой, В. Е. Тараканова. – М. : Научное издательство ТВП, 2001. – 254 с.

3. Носиров, З. А. Анализ криптографических схем разделения секрета для резервного хранения ключевой информации / З. А. Носиров, О. В. Щербинина // Прикаспийский журнал: управление и высокие технологии. – 2019. – № 2(46). – URL: https://cyberleninka.ru/article/n/analiz-kriptograficheskih-shem-razdeleniya-sekreta-dlya-rezervnogo-hraneniya-klyuchevoy-informatsii (дата обращения: 06.01.2025).

4. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Н. И. Червяков, А. А. Коляда, П. А. Ляхов [и др.]. – М. : Физматлит, 2017. – 400 с.

5. Харин, Ю. С. Математические и компьютерные основы криптологии : учеб. пособие / Ю. С. Харин. – Минск : Новое знание, 2003. – 382 с.

6. Коляда, А. А. Модулярные структуры конвейерной обработки цифровой информации / А. А. Коляда, И. Т. Пак. – Минск : Университетское, 1992. – 256 с.

7. Чернявский, А. Ф. Особенности машинной арифметики высокопроизводительных модулярных вычислительных структур / А. Ф. Чернявский, Е. И. Козлова, А. А. Коляда // Журнал Белорусского государственного университета. Математика. Информатика. – 2023. – № 2. – С. 94–101.

8. Виноградова, А. А. Системы разделения секрета / А. А. Виноградова. – 2017. – 19 с. – URL: http://hdl.handle.net/11701/11134 (дата обращения: 27.01.2025).

9. Shamir, A. How to share a secret / A. Shamir // Communications of the ACM. – Nov. 1979. – Vol. 22, iss. 11. – P. 612–613. – DOI: 10.1145/359168.359176.

10. Коляда, А. А. Пороговый метод разделения секрета на базе избыточных модулярных вычислительных структур / А. А. Коляда, П. В. Кучинский, Н. И. Червяков // Информационные технологии. – 2019. – Т. 25, № 9. – С. 553–560.

References

1. Artjukhov Yu. V. *Analysis of secret sharing schemes using probabilistic and combinatorial approaches in the implementation of threshold cryptosystems operating in distributed computer systems*. Aktual'nye voprosy tehnicheskih nauk : materialy Mezhdunarodnoj zaochnoj nauchnoj konferencii, Perm', ijul' 2011 g. [*Current Issues in Technical Sciences : Materials of the International Correspondence Scientific Conference, Perm, July 2011*]. In G. D. Akhmetova (ed.). Perm’, Mercurii, 2011, 80 p. (In Russ.).

2. Koblitz N. *A Course in Number Theory and Cryptography*, second edition. Springer, 1994, 245 p.

3. Nosirov Z. A., Shcherbina O. V. *Analysis of cryptographic secret sharing schemes for backup storage of key information*. Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii [*Caspian Journal: Management and High Technologies*], 2019, no. 2(46) (In Russ.). Available at: https://cyberleninka.ru/article/n/analiz-kriptograficheskih-shem-razdeleniya-sekreta-dlya-rezervnogo-hraneniya-klyuchevoy-informatsii (accessed 06.01.2025).

4. Chervyakov N. I., Kolyada A. A., Lyahov P. A., Babenko M. G., Lavrinenko I. N., Lavrinenko A. V. Moduljarnaja arifmetika i ee prilozhenija v infokommunikacionnyh tehnologijah. *Modular Arithmetic and its Applications in Infocommunication Technologies*. Moscow, Fizmatlit, 2017, 400 p. (In Russ.).

5. Kharin Yu. S. Matematicheskie i komp'juternye osnovy kriptologii. *Mathematical and Computer Foundations of Cryptology*. Minsk, Novoe znanie, 2003, 382 p. (In Russ.).

6. Kolyada A. A., Pak I. T. Modulyarnye struktury konveyernoy obrabotki tsifrovoy informatsii. *Modular Structures of Pipeline Processing of Digital Information*. Minsk, Universitetskoe, 1992, 256 p. (In Russ.).

7. Chernyavskiy A. F., Kozlova E. I., Kolyada A. A. *Features of machine arithmetic of high-performance modular computing structures.* Zhurnal Belorusskogo gosudarstvennogo universiteta. Matematika. Informatika [*Journal of the Belarusian State University. Mathematics and Informatics*], 2023, no. 2, pp. 94–101 (In Russ.).

8. Vinogradova A. A. Sistemy razdeleniya sekreta. *Secretion Separation Systems*, 2017, 19 p. (In Russ.). Available at: http://hdl.handle.net/11701/11134 (accessed 27.01.2025).

9. Shamir A. How to share a secret. *Communications of the ACM*, November 1979, vol. 22, iss. 11, pp. 612–613. DOI: 10.1145/359168.359176.

10. Kolyada A. A., Kuchinskiu P. V., Chervyakov N. I. *Threshold secret sharing method based on redundant modular computing structures*. Informatsionnye tekhnologii [*Information Technology*], 2019, vol. 25, no. 9, pp. 553–560 (In Russ.).

Информация об авторах

Чернявский Александр Федорович, доктор технических наук, академик НАН Беларуси, профессор, Белорусский государственный университет.
E-mail: ChernAA@bsu.by

Козлова Елена Ивановна, кандидат физико-математических наук, доцент, Белорусский государственный университет.
E-mail: kozlova@bsu.by

Садов Василий Сергеевич, кандидат технических наук, доцент, Белорусский государственный университет.
E-mail: sadov@bsu.by

Коляда Андрей Алексеевич, доктор физико-математических наук, Белорусский государственный университет.

Information about the authors

Alexander F. Chernyavskiy, D. Sc. (Eng.), Acad. of the National Academy of Sciences of Belarus, Prof., Belarusian State University.
E-mail: ChernAA@bsu.by

Alena I. Kazlova, Ph. D. (Phys.-Math.), Assoc. Prof., Belarusian State University.
E-mail: kozlova@bsu.by

Vasiliy S. Sadov, Ph. D. (Eng.), Assoc. Prof., Belarusian State University.
E-mail: sadov@bsu.by

Andrei A. Kolyada, D. Sc. (Phys.-Math.), Belarusian State University.