

Научная статья  
УДК 519.16  
DOI: 10.26583/bit.2025.3.08

## АНАЛИЗ И РЕАЛИЗАЦИЯ КРИПТОСИСТЕМЫ НА ОСНОВЕ НЕИНЪЕКТИВНЫХ РАНЦЕВ

**Мария Сабина А. Волков**

*Московский государственный технический университет им. Н.Э. Баумана,  
2-я Бауманская ул., 5, стр.1, Москва, 105005, Россия  
sabina-volkoff@yandex.ru, <https://orcid.org/0009-0000-3291-733X>*

**Аннотация.** В работе исследуются свойства неинъективных линейных форм и их применение в ранцевых криптосистемах. Основной целью исследования является анализ возможностей использования неинъективных ранцев в качестве закрытых ключей для повышения криптографической стойкости ранцевых криптосистем к известным видам атак, включая атаки методом перебора и атаки, основанные на редукции базиса решеток. Особое внимание уделено выбору параметров криптосистемы, обеспечивающих баланс между безопасностью и вычислительной эффективностью. Определено, что для защиты от атак на основе редукции решеток, таких как LLL-атака, необходимо поддерживать плотность ранца выше 1,033. В качестве значения длины ключа выбрано  $n = 200$ , при котором элементы открытого ключа имеют длину 170–200 бит. Это обеспечивает достаточный уровень криптостойкости при разумных вычислительных затратах. Для контроля сложности алгоритма расшифрования предложены методы ограничения среднего числа решений задачи о ранце. Установлено, что ограничение числа решений значением 2048 позволяет достичь приемлемой вычислительной сложности, сохраняя высокий уровень безопасности. Дополнительно разработан механизм исключения избыточных коэффициентов и введена 16-битная контрольная сумма, позволяющая избежать неоднозначности при расшифровании. Результаты исследования показывают, что предложенные методы позволяют существенно повысить стойкость ранцевой криптосистемы при умеренных вычислительных затратах, делая её перспективной для практического применения.

**Ключевые слова:** NP-трудные задачи, задача об укладке ранца, криптография, ранцевая криптосистема.

**Для цитирования:** Волков, Мария Сабина А. Анализ и реализация криптосистемы на основе неинъективных ранцев. *Безопасность информационных технологий, [S.l.]*, т 32, № 3, с. 100–111, 2025. ISSN 2074-7136. URL: <https://bit.spels.ru/index.php/bit/article/view/1815>. DOI: <http://dx.doi.org/10.26583/bit.2025.3.08>.

Scientific article

## ANALYSIS AND IMPLEMENTATION OF A CRYPTOSYSTEM BASED ON NON-INJECTIVE KNAPSACKS

**Maria Sabina A. Volkov**

*Bauman Moscow State Technical University,  
2nd Baumanskaya str., 5, bld. 1, Moscow, 105005, Russia  
sabina-volkoff@yandex.ru, <https://orcid.org/0009-0000-3291-733X>*

**Abstract.** The paper explores the properties of non-injective linear forms and their application in knapsack cryptosystems. The primary objective of the study is to analyze the potential of using non-injective knapsacks as private keys to enhance the cryptographic strength of knapsack-based systems against known types of attacks, including brute-force attacks and lattice basis reduction attacks. Special attention is given to the selection of cryptosystem parameters that provide a balance between security and

computational efficiency. It is determined that, in order to protect against lattice-based attacks such as the LLL attack, the knapsack density must be maintained above 1.033. A key length of  $n = 200$  is chosen, where the elements of the public key have a length of 170–200 bits. This provides a sufficient level of cryptographic strength at reasonable computational cost. To control the complexity of the decryption algorithm, methods are proposed to limit the average number of solutions to the knapsack problem. It is established that restricting the number of solutions to 2048 enables acceptable computational complexity while maintaining a high level of security. Additionally, a mechanism for eliminating redundant coefficients is developed, and a 16-bit checksum is introduced to avoid ambiguity during decryption. The results of the study demonstrate that the proposed methods can significantly improve the robustness of the knapsack cryptosystem at moderate computational cost, making it a promising candidate for practical implementation.

**Keywords:** *NP-completeness, knapsack problem, cryptography, knapsack cryptosystem.*

**For citation:** *Volkov, Maria Sabina A. Analysis and implementation of a cryptosystem based on non-injective knapsacks. IT Security (Russia), [S.l.], v. 32, no. 3, p. 100–111, 2025. ISSN 2074-7136. URL: <https://bit.spels.ru/index.php/bit/article/view/1815>. DOI: <http://dx.doi.org/10.26583/bit.2025.3.08>.*

## Введение

Современное развитие криптографии требует создания новых методов шифрования, обладающих высокой степенью стойкости к современным криптоаналитическим атакам. Традиционные асимметричные криптосистемы, такие как RSA и протокол Диффи-Хеллмана, опираются на сложность решений задач факторизации целых чисел и дискретного логарифмирования. Однако развитие квантовой информатики ставит под угрозу безопасность этих систем, поскольку квантовый алгоритм Шора способен эффективно решать данные задачи. Поэтому особое значение приобретает разработка криптографических методов, основанных на сложных математических задачах, которые трудно решить даже с помощью квантового оборудования. Одним из альтернативных методов является использование NP-трудных задач, которые предоставляют основу для создания криптосистем, стойких к современным атакам, включая атаки, использующие квантовые алгоритмы. В этом контексте ранцевые криптосистемы представляют собой перспективное направление [1], способное обеспечить высокую криптостойкость при сравнительно низких вычислительных затратах.

Первой асимметричной ранцевой криптосистемой считается система Меркла-Хеллмана [2]. В её основе лежит использование сверхрастающего ранцевого вектора, который затем подвергается запутывающему преобразованию. Закрытый ключ системы включает сверхрастающий вектор  $A = (a_1, \dots, a_n)$ , два вспомогательных числа  $u$  и  $M$ , где  $u$  является элементом мультипликативной группы целых чисел по модулю  $M$  и  $M \geq \sum_{i=1}^n a_i$ . Также в закрытый ключ входит значение  $t = u^{-1} \bmod M$ . Открытым ключом является вектор  $B = (b_1, \dots, b_n)$ , элементы которого получаются путём преобразования  $b_i = (a_i * u) \bmod M$ . Процесс шифрования заключается в вычислении суммы  $C = \sum_{i=1}^n b_i x_i$ , где  $x = (x_1, x_2, \dots, x_n)$  представляет собой бинарное сообщение. Расшифрование осуществляется с использованием секретного ключа: вычисляется  $C' = (C * t) \bmod M$ , после чего решается задача о ранце  $\sum_{i=1}^n b_i x_i = C'$ , используя последовательное извлечение битов  $x_i$ .

Поскольку в криптографических системах требуется однозначное восстановление зашифрованного сообщения, для шифрования используются инъективные ранцевые векторы.

**Определение 1.** Вектор  $A$  называется инъективным или криптографическим, если  $\forall A', A'' \subset A, A' \neq A''$  выполняется  $\sum_{a' \in A'} a' \neq \sum_{a'' \in A''} a''$ .

Особый класс инъективных ранцевых векторов представляют сверхрастущие последовательности.

**Определение 2.** Вектор  $A = (a_1, \dots, a_n)$  называется сверхрастущим, если  $\forall k = 2, \dots, n$  выполняется условие  $a_k > \sum_{i=1}^{k-1} a_i$ .

Данное свойство позволяет решать задачу о ранце за линейное время путем последовательного извлечения битов  $x_i$ . Использование сверхрастущих последовательностей упрощает процесс расшифрования, но делает систему уязвимой к атакам, основанным на редукции решеток.

Позднее было установлено, что многие ранцевые криптосистемы, включая схему Меркла–Хеллмана, подвержены криптоанализу [3], в первую очередь из-за недостаточной плотности ранцевого вектора, определяемой как  $d(A) = \frac{n}{\log_2 \max A}$ , где  $n$  – длина вектора  $A$ , а  $\max A = \max \{a_1, \dots, a_n\}$  – наибольший элемент этого вектора. При  $d(A) \leq 0,9408$  задача о ранце эффективно решается методами редукции решеток, такими как алгоритм Ленстры–Ленстры–Ловаса (LLL) [4], а применение сверхрастущих последовательностей делает систему уязвимой к атаке Шамира [5].

Для обеспечения криптостойкости плотность ранца должна превышать 0,9408, однако значение  $d(A) > 1$  приводит к неоднозначности расшифрования. Это ограничение требует подбора ранцевых векторов, обеспечивающих баланс между криптостойкостью и корректностью расшифрования. Несмотря на данные сложности, существуют ранцевые криптосистемы, криптографическая уязвимость которых пока не доказана [6–8]. Одним из подходов является использование плотных ранцев с  $d(A) \approx 1$ , которые обладают сложной структурой множества решений, что затрудняет их анализ методами редукции решеток.

В данной работе предлагается модификация криптосистемы Меркла–Хеллмана, основанная на применении неинъективных ранцевых последовательностей и алгоритма поиска всех решений. В отличие от классической схемы, предложенная система использует контрольную сумму, позволяющую однозначно выбирать корректное разложение среди возможных решений задачи о ранце. Такая модификация направлена на повышение криптостойкости и устранение недостатков традиционной ранцевой криптосистемы.

## 1. Сюръективные линейные формы

Конструирование закрытых ключей ранцевой криптосистемы требует выбора специальных числовых последовательностей, обеспечивающих необходимые криптографические свойства. Приведенные в данном разделе определения, теоремы и следствия, формирующие основу разработанной криптосистемы, были ранее строго доказаны в [9]. В настоящей работе они используются для выбора параметров системы и обоснования ее криптографической стойкости.

Рассмотрим частный случай задачи  $\sum_{i=1}^n a_i x_i = b$ , при котором все целочисленные значения от 0 до  $\sum_{i=1}^n a_i$  могут быть представлены в виде частичных сумм элементов ранцевого вектора  $A$ .

Обозначим линейную форму, составленную из компонентов вектора весов задачи о ранце, как  $L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i$ . Множество возможных значений этой формы обозначим через  $L^*(x_1, \dots, x_n)$ . Уравнение  $L(x_1, \dots, x_n) = b$  имеет решение тогда и только тогда, когда  $b \in L^*(x_1, \dots, x_n)$ .

Понятие линейной формы с булевыми переменными  $f(x_1, \dots, x_n) = \sum_{j=1}^n c_j x_j$ , принимающей все значения из интервала  $[0, \sum_{j=1}^n c_j]$ , было ранее рассмотрено в [10, 11], а её комбинаторные свойства подробно исследованы в [12].

Далее будем считать, что выполняется условие  $a_1 \leq a_2 \leq \dots \leq a_n$  и  $x \in \{0,1\}$ .

**Определение 3.** Линейная форма  $L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i$  называется сюръективной, если она принимает все значения в диапазоне интервала  $[0, \sum_{i=1}^n a_i]$ , иными словами,  $\forall b \in \{0, 1, 2, \dots, \sum_{i=1}^n a_i\} \quad b \in L^*(x)$ . Далее будем обозначать  $L^*(x) = [0, \sum_{i=1}^n a_i]$ .

Важность сюръективных линейных форм объясняется тем, что проверка на разрешимость системы булевых уравнений, левые части которых образованы сюръективными линейными формами, является тривиальной. Для каждого уравнения достаточно убедиться, что  $b \leq \sum_{i=1}^n a_i$ .

Следующая теорема формулирует необходимые и достаточные условия сюръективности линейной формы.

**Теорема 1.** Линейная форма  $L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i$  является сюръективной тогда и только тогда, когда выполняется

$$a_1 = 1, \text{ и } a_k \leq \sum_{i=1}^{k-1} a_i + 1 \quad \forall k = 2, \dots, n. \quad (1)$$

Данная теорема показывает, что процесс создания сюръективной линейной формы настолько же прост, как и процесс формирования сверхрастущей последовательности. Это свойство особенно полезно при генерации закрытых ключей в ранцевых криптосистемах.

Условия (1) будем называть условиями сюръективности линейной формы. Они позволяют определить максимальные значения её компонентов, а также минимальную плотность сюръективного ранцевого вектора.

В следующей теореме выведены необходимые и достаточные условия сюръективности линейной формы.

**Следствие 2.** Плотность сюръективного ранцевого вектора удовлетворяет неравенству  $d(A) \geq \frac{n}{n-1} > 1$ .

Это означает, что криптосистемы, основанные на сюръективных ранцах, не подвержены уязвимостям, связанным с недостаточной плотностью. Однако при этом теряется свойство однозначности расшифрования, что необходимо учитывать при их практическом применении.

Для эффективного использования сюръективных форм в качестве закрытых ключей важно также удостовериться, что их общее количество достаточно велико, чтобы противостоять атаке полным перебором.

**Следствие 3.** Число сюръективных линейных форм ограничено следующими оценками:  $n! < L_c(n) < 2^{n \cdot \frac{n-1}{2}}$ .

Анализ нижней границы показывает, что количество таких форм растёт экспоненциально с увеличением числа переменных. Это означает, что при достаточно больших  $n$  общее число возможных закрытых ключей становится настолько велико, что атака методом полного перебора требует экспоненциальных затрат времени и становится вычислительно неэффективной.

Ключевым преимуществом сюръективных форм в криптографическом контексте является их вычислительная эффективность: каждое решение задачи, содержащей такую форму в качестве левой части, может быть найдено за время, пропорциональное числу переменных и количеству решений.

**Теорема 2.** Если форма  $L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i$  сюръективна и  $b \in L^*(x_1, \dots, x_n)$ , то все решения задачи  $\sum_{i=1}^n a_i x_i = b$  можно найти за время  $O(ns)$ , где  $s$  – число этих решений.

В [9] в рамках доказательства данной теоремы был представлен алгоритм поиска всех решений сюръективного ранца. Алгоритм основан на рекурсивной процедуре, которая, начиная с последней переменной, на каждом шаге либо однозначно определяет её значение, либо осуществляет ветвление по двум возможным значениям, в зависимости от

сравнения текущей суммы с коэффициентами. Такой подход позволяет эффективно перебрать все допустимые решения задачи и гарантирует корректность декодирования при работе с сюръективными формами.

Для обоснования применения сюръективных форм в криптографических системах также важно изучить их поведение при модульном умножении на число взаимно простое с модулем.

**Утверждение 5.** Пусть  $B(x_1, \dots, x_n)$  получается из  $A(x_1, \dots, x_n)$  путём умножения каждого коэффициента на число  $u$ , взаимно простое с  $M$ , с последующим приведением по модулю  $M$ :  $b_i = ua_i \pmod{M}$ . Обозначим упорядоченные компоненты формы  $B(x_1, \dots, x_n)$  через  $b^{(1)} < b^{(2)} < \dots < b^{(n)}$ . Тогда математическое ожидание компоненты  $b^{(k)}$  приблизительно равно:

$$E[b^{(k)}] \cong \frac{Mk}{n+1}, \quad k = 1, \dots, n.$$

Из данного утверждения следует, что операция модульного умножения значительно увеличивает минимальные компоненты линейной формы, что приводит к невозможности равномерного покрытия всего диапазона значений от 1 до  $\sum_{i=1}^n b_i$  без пропусков. В результате преобразованная линейная форма теряет свойство сюръективности, и нахождение её решений становится классической NP-трудной задачей. Согласно формуле, определяющей среднее количество решений линейных уравнений заданной размерности, представленной в [13], можно оценить среднее число решений уравнения  $\sum_{i=1}^n a_i x_i = b$  при различных значениях  $b$ . Для больших значений  $M$  эта величина оказывается значительно меньше 1, что дополнительно подтверждает сложность нахождения решений для таких форм.

Таким образом, сюръективные ранцевые векторы являются перспективным кандидатом для использования в модификации криптосистемы Меркла-Хеллмана, предлагая криптостойкость к известным видам атак при сохранении приемлемой вычислительной сложности. В следующем разделе будут рассмотрены конкретные параметры системы, необходимые для обеспечения криптографической стойкости, а также приведён их обоснованный выбор.

## 2. Подбор параметров криптосистемы

**Выбор длины ключа** в ранцевых криптосистемах определяется требованиями к криптостойкости, вычислительными ресурсами атакующих и сценариями применения атак. Основные критерии включают защиту от полного перебора, стойкость к современным методам криптоанализа и совместимость с аппаратными ограничениями.

В оригинальной схеме Меркла-Хеллмана [2] типичное значение  $n$  составляло 100. Дальнейшие исследования рекомендуют увеличивать  $n$  для повышения стойкости к современным атакам. В частности, в [14] предложено использовать  $n = 150$ , поскольку увеличение длины ключа снижает вероятность успешного криптоанализа при сохранении разумного уровня вычислительной сложности. В [15] также указывают, что  $n$  может быть увеличено до 150, чтобы повысить стойкость к атакам, включая методы, основанные на роевой оптимизации. В данной работе, исходя из анализа современных атак и оценки криптостойкости, выбрана длина  $n = 200$ , а элементы открытого ключа имеют размер от 170 до 200 бит. Это обеспечивает высокую безопасность при умеренных вычислительных затратах.

Выбор такой длины ключа обоснован необходимостью обеспечения стойкости к криптоаналитическим атакам, в частности к методам, использующим алгоритм редукции решёток LLL. Эффективность данного метода возрастает при низкой плотности ранцевого

вектора. При малых  $n$  атака остаётся успешной даже при  $d > 0,9408$ , поскольку ограниченное пространство значений упрощает редукцию решётки. Теоретическая сложность атаки LLL оценивается как  $O(n^6 * \log^3 a_n) \approx O(n^9)$ , что делает её нецелесообразной при  $n \geq 200$ . Увеличение длины ключа до 200 элементов существенно усложняет атаку и делает её практически неосуществимой для злоумышленников.

Как будет продемонстрировано далее, при фиксированном среднем числе решений задачи увеличение длины ключа снижает плотность ранца из-за более значительного разброса значений компонентов ранцевого вектора. Если не поддерживать плотность на оптимальном уровне, криптосистема может оказаться уязвимой для атак редукции решёток.

**Утверждение.** Сложность решения задачи с сюръективной формой в среднем случае при заданной плотности  $d$  ограничена снизу оценкой  $\Omega\left(n * 2^{\left(n\left(1-\frac{1}{d}\right)-1\right)}\right)$ .

**Доказательство:** Поскольку форма  $L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i$  сюръективна и принимает все значения в интервале  $[0, \sum_{i=1}^n a_i]$ , её среднее число решений по всем  $b$  в данном интервале выражается как  $N(L) = \frac{2^n}{\sum_{i=1}^n a_i + 1}$ . При заданной плотности  $d$  из формулы

$d(A) = \frac{n}{\log_2 \max A} = \frac{n}{\log_2 a_n}$  можно выразить  $a_n = 2^{\frac{n}{d}}$ . Подставляя это в выражение для среднего числа решений и учитывая условия сюръективности, получаем  $N(L) = \frac{2^n}{\sum_{i=1}^n a_i + 1} \geq \frac{2^n}{2a_n} = 2^{n\left(1-\frac{1}{d}\right)-1}$ .

Так как в предлагаемой криптосистеме среднее число решений выбирается минимально возможным при заданном  $d$ , можно считать, что асимптотическая сложность в среднем случае близка к этой нижней границе, то есть  $\Theta\left(n * 2^{\left(n\left(1-\frac{1}{d}\right)-1\right)}\right)$ .

Поэтому увеличение длины ключа выше  $n = 200$  приводит к значительному увеличению времени обработки данных, что может быть нежелательно для практического применения криптосистемы.

Таким образом, выбор длины ключа  $n = 200$  обоснован необходимостью защиты от атак на основе редукции решёток, включая атаку LLL, и желанием минимизировать вычислительные накладные расходы.

**Определение плотности ранца.** На основе эмпирического теста в [16], установлено, что задачи о ранце наибольшей сложности возникают при плотности ранцевого вектора около  $1 + \frac{\log_2 \frac{n}{2}}{n}$ , что часто приводит к наличию нескольких решений, особенно при правой части уравнения, близкой к  $\frac{1}{2} \sum_{i=1}^n a_i$ . В [17] отмечается отсутствие известных атак на задачи с  $n \approx 100$  и плотностью  $d \approx 1$ , при весе сообщения около  $\frac{n}{2}$ . Это указывает на возможность того, что ранцы с плотностью между 1 и плотностью, предложенной в [16], могут вызывать аналогичные сложности в криптоанализе. При выбранном значении  $n = 200$  плотность, определенная по формуле  $1 + (\log_2 n/2)/n$ , приблизительно равна  $d \approx 1,033$ , что обеспечивает высокую сложность решения задачи о ранце и повышенную криптостойкость за счёт уменьшения уязвимости к атакам методом редукции решёток.

Для усиления защищенности алгоритма было решено исключить из открытого ключа первые  $p$  младших коэффициентов линейной формы. Начальные элементы сюръективной последовательности формируются предсказуемо:  $a_1 = 1, a_2 = 2, a_k \in [a_{k-1} + 1; \sum_{i=1}^{k-1} a_i + 1]$ , – что позволяет злоумышленнику с высокой вероятностью

восстановить параметры  $t$  и  $M$  при малых  $k$ . Вместо этого в открытый ключ включаются только последние  $(n - p)$  старших коэффициентов, где  $p \geq 5$ , а при расшифровании допустимыми считаются лишь решения с первыми  $p$  нулевыми битами. Это повышает безопасность и снижает вероятность ошибок.

Однако такое сокращение длины открытого ключа приводит к уменьшению плотности открытого ключа, которая становится пропорциональной  $d(A) \approx \frac{n-p}{\log_2 \max B}$ . Поэтому параметры криптосистемы должны учитывать уменьшенную длину ключа  $n' = n - p$  для сохранения требуемой криптостойкости. В текущей реализации  $p$  выбрано равным 5, что позволяет максимизировать плотность при заданном числе решений.

**Выбор модуля  $M$  для модульного умножения** критически влияет на безопасность и производительность системы. Корректная настройка этого параметра позволяет сохранить требуемую плотность ранца и противостоять атакам на основе редукции решёток.

Как было показано в утверждении 5, при применении модульного умножения плотность открытого ключа можно оценить выражением:  $d(A) \approx \frac{n'}{\log_2 M}$ . Выбор слишком большого значения  $M$  приводит к снижению плотности ранца, что делает систему более уязвимой к атакам методом редукции решёток. Из этого следует, что для достижения желаемой плотности  $d^* \geq 1,033$  при длине ключа  $n = 200$  и  $p = 5$  модуль  $M$  должен удовлетворять условию:  $M \leq 2^{\frac{n'}{d}} = 2^{\frac{195}{1,033}} \approx 2^{189}$ . При этом для сохранения распределения решений требуется выбирать  $M \geq \sum_{i=1}^n a_i$ . В частности, в [14] предложено использовать  $M \approx \sum_{i=1}^n a_i$ . Однако выбор слишком малого  $M$  значительно упрощает задачу подбора модуля при криптоанализе. В текущей реализации было принято решение выбирать  $M \approx \sum_{i=1}^n a_i + k$ , где  $k \in [0; a_{n-1}]$ , поскольку для больших  $n$  такая надбавка  $k$  на порядок меньше значения  $\sum_{i=1}^n a_i$  и не оказывает существенного влияния на величину плотности. Такой подход снижает размер открытого ключа и повышает эффективность шифрования при сохранении необходимого уровня криптостойкости.

**Выбор среднего числа решений.** Основной недостаток алгоритма решения, приведенного в теореме 2, заключается в том, что число допустимых решений уравнения  $\sum_{i=1}^n a_i x_i = b$  с сюръективной формой может значительно превышать величину  $n$ . Например, для формы  $L(x_1, \dots, x_{100}) = \sum_{i=1}^{100} i x_i$  число решений задачи  $L(x_1, \dots, x_{100}) = 2525$  приблизительно равно  $1,73e+27$ , что во много раз превышает значение  $n$ .

Однако при построении сюръективной формы можно ограничить среднее число её решений. Поскольку среднее число решений сюръективной формы  $L(x_1, \dots, x_n)$  по всем  $b$  в интервале  $[0, \sum_{i=1}^n a_i]$  выражается как  $N(L) = \frac{2^n}{\sum_{i=1}^n a_i + 1}$ , чтобы среднее число решений не превышало некоторого  $\tilde{N}$  и распределение числа решений по интервалу  $[0; \sum_{i=1}^n a_i]$  было близко к равномерному, достаточно при ее построении выбирать каждый следующий  $a_k$  так, чтобы выполнялось  $a_k \geq \frac{2^{k-1}}{\tilde{N}}$ . Таким образом, можно выбирать коэффициенты линейной формы так, чтобы сложность алгоритма нахождения ее решений не превышала выбранного значения  $O(\tilde{N}n)$ . Плотность ранца, построенного по описанной процедуре, будет  $d(A) \leq \frac{n}{(n-1) - \log_2 \tilde{N}}$ . Таким образом можно подобрать требуемое соотношение между плотностью ранца и средним числом решений задачи. Это позволяет конструировать эффективные криптосистемы с управляемой вычислительной сложностью.

Для обеспечения желаемой плотности  $d^* \approx 1,033$  необходимо учитывать следующие соотношения:  $2^{189} \geq M \geq \sum_{i=1}^n a_i \geq 2a_n \geq \frac{2^n}{\tilde{N}}$ . Из этого выражения можно вывести, что  $\tilde{N} \geq \frac{2^{200}}{2^{189}} = 2048$ .

С учетом выполнения условий сюръективности, плотность ранца, построенного по такой процедуре, будет ограничена неравенствами  $\frac{n}{(n-1)} \leq d(A) \leq \frac{n}{(n-1) - \log_2 \tilde{N}}$ . Получившаяся плотность всегда будет больше 1, что превышает значение плотности, необходимой для проведения успешной атаки Костера-Лагариаса-Одлышко. Поскольку большинство предложенных в последние годы атак на ранцевые криптосистемы представляют собой модификации атаки Лагариаса-Одлышко [18, 19] и также основываются на предположении о низкой плотности ранцевого вектора, то применение сюръективных ранцев препятствует успешному применению подобных атак и значительно увеличивает стойкость к атакам, основанным на методах редукции базиса решеток.

**Выбор контрольной суммы.** При большом количестве допустимых решений задачи о ранце неизбежно возникает проблема неоднозначности при расшифровании сообщений. Для её устранения вводится избыточность в виде контрольной суммы. Учитывая, что старшим битам соответствуют большие коэффициенты формы, а различные решения для одного и того же  $b$  обычно совпадают по старшим коэффициентам, контрольную сумму целесообразно размещать в начале сообщения. Вероятность случайного совпадения контрольной суммы в разных решениях может быть оценена как  $2^{-l}$ , где  $l$  — длина контрольной суммы в битах.

С учетом ограничений на длину ключа и вычислительные ресурсы контрольная сумма должна быть компактной и легко вычисляемой. С этой целью предлагается использование криптографической хэш-функции, такой как усечённая версия SHA-1, из которой берутся только первые  $l$  бит результата. При  $l = 16$  вероятность случайного совпадения контрольных сумм с учетом отброшенных ранее  $p = 5$  элементов приблизительно составляет  $2^{-21} = \frac{1}{2097152}$ , что является приемлемым для большинства приложений. В системе с параметрами  $n = 200, l = 16, p = 5$  контрольная сумма и отброшенные элементы занимают лишь 10,5% от общего объема сообщения, обеспечивая баланс между корректностью восстановления данных и пропускной способностью.

### 3. Анализ результатов исследования

Для оценки практической применимости предложенной ранцевой криптосистемы была выполнена практическая реализация разработанных алгоритмов и проведена серия экспериментов, охватывающих основные аспекты функционирования и безопасности системы.

**Проверка корректности шифрования и расшифрования.** В ходе серии экспериментов с использованием фиксированных параметров системы:  $n = 200, l = 16, p = 5, \tilde{N} = 2000, d^* \approx 1,031$  было выполнено 10 000 запусков шифрования и расшифрования сгенерированных открытых сообщений длиной до 1 000 бит. Во всех случаях расшифрованный текст в точности совпадал с исходным, что свидетельствует о корректной работе алгоритма на данной выборке. Следует, однако, отметить, что при больших объёмах передаваемой информации теоретически возможны коллизии, приводящие к некорректному расшифрованию. Для таких ситуаций в практической реализации может быть предусмотрен механизм повторной отправки сообщения при множественности допустимых решений, либо других признаках искажения.

**Оценка производительности.** С целью оценки эффективности предложенного алгоритма была проведена серия измерений времени выполнения базовых криптографических операций: генерации ключей, шифрования и расшифрования. Эксперименты выполнялись на процессоре Intel Core i7-1165G7 с использованием стандартной реализации RSA, предоставляемой модулем `cryptography.hazmat.primitives.asymmetric.rsa` библиотеки `cryptography`, в которой криптографические операции реализованы на основе высокооптимизированной библиотеки `OpenSSL`. Среднее время выполнения операции шифрования и расшифрования с использованием RSA при размере ключа 2048 бит составило около 0,6 мс и 1,7 мс соответственно. Время генерации ключей RSA 2048 составило в среднем 340 мс. В разработанной ранцевой криптосистеме, при фиксированных параметрах, полное время выполнения процедуры шифрования составило в среднем 0,6 мс, а расшифрования – 26 мс. Время генерации ключей в разработанной криптосистеме в среднем составило 0,05 мс. Следует подчеркнуть, что текущая реализация ранцевой криптосистемы выполнена на языке Python и не оптимизирована с точки зрения вычислительной производительности. Отсутствие низкоуровневой реализации, а также использование интерпретируемого языка накладывают ограничения на скорость выполнения, особенно на этапе расшифрования. Таким образом, несмотря на несколько более длительное время расшифрования по сравнению с RSA, представленные значения свидетельствуют о потенциальной применимости предложенного подхода. Кроме того, существует значительный резерв для ускорения реализации за счёт ее оптимизации и использования компилируемых языков программирования.

**Стойкость к LLL-атакам.** Для оценки криптостойкости предложенной криптосистемы была проведена серия экспериментов, направленных на изучение устойчивости к атакам, основанным на методах редукции решёток, в частности — с применением алгоритма LLL. При фиксированной плотности ранца  $d \approx 1,031$  анализировалась зависимость вероятности успешной дешифровки от длины блока исходного сообщения. Полученные результаты показывают, что при длине блока 8 бит доля успешных атак составляет менее 0,5%. При увеличении длины блока вероятность успешного взлома заметно снижается. Совокупность экспериментальных данных представлена в табл. 1.

Таблица 1. Зависимость доли успешных атак от длины блока при выбранных параметрах

Длина блока (бит)	Доля успешных атак (%)
8	0,47
12	0,33
16	0,18
32	0,05
64	0,008
128	0,0003

Таким образом, полученные результаты демонстрируют корректную работу системы в условиях моделируемых экспериментов.

### Заключение

В работе рассмотрена реализация модифицированной ранцевой криптосистемы на основе сюръективных ранцев и проведен подбор параметров, обеспечивающих высокий уровень криптостойкости при допустимых вычислительных затратах.

Основное внимание уделено выбору длины ключа, плотности ранца, размера модуля и числа решений, поскольку эти параметры оказывают ключевое влияние на безопасность системы. В частности, длина ключа  $n = 200$  и плотность  $d \approx 1,033$  позволяют защитить систему от атак, основанных на редукции решеток, включая LLL-атаку. Для контроля числа решений предложен метод регулирования размера компонентов открытого ключа, что снижает сложность поиска решений. Кроме того, реализован механизм повышения однозначности расшифрования, основанный на использовании контрольных сумм, полученных усечением хэш-функции, что позволило уменьшить вероятность ошибок при расшифровании за счёт дополнительной проверки целостности сообщения. Также обоснован выбор модуля  $M$ , оптимального с точки зрения обеспечения требуемой плотности и предотвращения атак подбора.

Экспериментальные результаты продемонстрировали корректность функционирования реализованного алгоритма, а также его устойчивость к атакам на основе редукции решёток при выбранных параметрах. При плотности ранца около 1,031 доля успешных атак методом LLL для коротких блоков закрытого текста не превышала 0,5%. Кроме того, измерения времени выполнения операций указывают на удовлетворительную производительность, особенно с учётом возможности дальнейшей оптимизации реализации. Таким образом, предложенный подход может рассматриваться в качестве потенциально применимого решения в ряде практических сценариев.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Wang, J., Liu, L., Lyu, S., et al. Quantum-safe cryptography: crossroads of coding theory and cryptography. *Science China Information Sciences*. 2022, v. 65, no. 1, p. 111301. DOI: <https://doi.org/10.1007/s11432-021-3354-7>.
2. Merkle R., Hellman M. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*. September. 1978, v. 24, no. 5, p. 525–530. DOI: <https://doi.org/10.1109/TIT.1978.1055927>.
3. Odlyzko A. M. The rise and fall of knapsack cryptosystems. *Cryptology and computational number theory*, 1990, v. 42, no. 2. DOI: <https://doi.org/10.1090/psapm/042/1095552>.
4. Coster M., Joux A., Lamacchia B., Odlyzko A., Schnorr C., Stern J. Improved Low-Density Subset Sum Algorithms. *Computational Complexity*. 1992, v. 2, p. 111–128. DOI: <https://doi.org/10.1007/BF01201999>.
5. Lu B. A Review of Modern Cryptography: From the World War II Era to the Big-Data Era. *Optimization and Control for Systems in the Big-Data Era: Theory and Applications*. 2017, v. 252, p. 101–120. DOI: [https://doi.org/10.1007/978-3-319-53518-0\\_7](https://doi.org/10.1007/978-3-319-53518-0_7).
6. Okamoto T., Tanaka K., Uchiyama S. Quantum Public-Key Cryptosystems. In: Bellare, M. (eds) *Advances in Cryptology – CRYPTO 2000*. CRYPTO 2000. *Lecture Notes in Computer Science*, v. 1880. Springer, Berlin, Heidelberg. DOI: <https://doi.org/10.1007/3-540-44598-6>.
7. Murakami Y., Nasako T. Knapsack Public-Key Cryptosystem Using Chinese Remainder Theorem. *IACR Cryptology ePrint Archive*. 2007. – 12 p. URL: <https://www.semanticscholar.org/paper/Knapsack-Public-Key-Cryptosystem-Using-Chinese-Murakami-Nasako/2ae27b1b4fa41a7eccde83e329dd6378b545b04> (дата обращения: 05.10.2024).
8. Naccache D., Stern J. A new public key cryptosystem based on higher residues. In *Proceedings of the 5th ACM conference on Computer and communications security (CCS '98)*. Association for Computing Machinery, New York, NY, USA. 1998, p. 59–66. DOI: <https://doi.org/10.1145/288090.288106>.
9. Волков, Мария Сабина А.; Гордеев, Эдуард Н. Применение неинъективных векторов в ранцевых криптосистемах. *Безопасность информационных технологий*, [S.l.], 2025, т. 32, № 1, с. 122–131. DOI: <http://dx.doi.org/10.26583/bit.2025.1.08>.
10. Гордеев Э.Н., Леонтьев В.К. О некоторых комбинаторных свойствах задачи о ранце. *Журнал вычислительной математики и математической физики*. 2019, т. 59, № 8, с. 1439–1447. DOI: <https://doi.org/10.1134/S0044466919080076>. – EDN: NHFSAT.
11. Леонтьев В.К., Гордеев Э.Н. О числе решений системы булевых уравнений. *Автоматика и телемеханика*. 2021, № 9, с. 150–168. – EDN: UQANSY.

12. Леонтьев В.К., Гордеев Э.Н., Волков М.С.А. Классическая непрерывность и ее дискретный вариант. Прикладная физика и математика. 2022, № 1, с. 31–37. DOI: <https://doi.org/10.25791/pfim.01.2022.1221>. – EDN: ZITVKA.
13. Волков М.С.А. Комбинаторные свойства задачи об ограниченном ранце. Прикладная дискретная математика. 2024, № 63, с. 117–130. DOI: <https://doi.org/10.25791/10.17223/20710410/63/8>. – EDN: PKMABD.
14. Zhang W., Wang B., Hu Y. A New Knapsack Public-Key Cryptosystem, 2009 Fifth International Conference on Information Assurance and Security, Xi'an, China. 2009, p. 53–56. DOI: <https://doi.org/10.1109/IAS.2009.300>.
15. Jain, A., Chaudhari, N.S. Cryptanalytic Results on Knapsack Cryptosystem Using Binary Particle Swarm Optimization. In: de la Puerta, J., et al. International Joint Conference SOCO'14-CISIS'14-ICEUTE'14. Advances in Intelligent Systems and Computing. 2014, v. 299, p. 375–384. DOI: [https://doi.org/10.1007/978-3-319-07995-0\\_37](https://doi.org/10.1007/978-3-319-07995-0_37).
16. Schnorr, C.P., Euchner, M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Mathematical Programming 66, p. 181–199 (1994). DOI: <https://doi.org/10.1007/BF01581144>.
17. Koskinen A., Non-Injective Knapsack Public-Key Cryptosystems. Theoretical Computer Science, March 2001, v. 255, no. 1–2, p. 401–422. DOI: [https://doi.org/10.1016/S0304-3975\(99\)00297-2](https://doi.org/10.1016/S0304-3975(99)00297-2).
18. Liu J., Bi J. Xu S. An Improved Attack on the Basic Merkle–Hellman Knapsack Cryptosystem. IEEE Access, 2019, v. 7, p. 59388–59393. DOI: <https://doi.org/10.1109/ACCESS.2019.2913678>.
19. Khalaf R.Z., Hamza B.H., Thakwan A.J. Attacking the Knapsack Public-key Cryptosystem. Webology. 2022, v. 19, no. 1, p. 5302–5309. DOI: <https://doi.org/10.14704/web/v19i1/web19356>.

#### REFERENCES:

- [1] Wang, J., Liu, L., Lyu, S., et al. Quantum-safe cryptography: crossroads of coding theory and cryptography. Science China Information Sciences. 2022, v. 65, no. 1, p. 111301. DOI: <https://doi.org/10.1007/s11432-021-3354-7>.
- [2] Merkle R., Hellman M. Hiding information and signatures in trapdoor knapsacks. IEEE Transactions on Information Theory. September. 1978, v. 24, no. 5, p. 525–530. DOI: <https://doi.org/10.1109/TIT.1978.1055927>.
- [3] Odlyzko A. M. The rise and fall of knapsack cryptosystems. Cryptology and computational number theory, 1990, v. 42, no. 2. DOI: <https://doi.org/10.1090/psapm/042/1095552>.
- [4] Coster M., Joux A., Lamacchia B., Odlyzko A., Schnorr C., Stern J. Improved Low-Density Subset Sum Algorithms. Computational Complexity. 1992, v. 2, p. 111–128. DOI: <https://doi.org/10.1007/BF01201999>.
- [5] Lu B. A Review of Modern Cryptography: From the World War II Era to the Big-Data Era. Optimization and Control for Systems in the Big-Data Era: Theory and Applications. 2017, v. 252, p. 101–120. DOI: [https://doi.org/10.1007/978-3-319-53518-0\\_7](https://doi.org/10.1007/978-3-319-53518-0_7).
- [6] Okamoto T., Tanaka K., Uchiyama S. Quantum Public-Key Cryptosystems. In: Bellare, M. (eds) Advances in Cryptology – CRYPTO 2000. CRYPTO 2000. Lecture Notes in Computer Science, v. 1880. Springer, Berlin, Heidelberg. DOI: <https://doi.org/10.1007/3-540-44598-6>.
- [7] Murakami Y., Nasako T. Knapsack Public-Key Cryptosystem Using Chinese Remainder Theorem. IACR Cryptology ePrint Archive. 2007. – 12 p. URL: <https://www.semanticscholar.org/paper/Knapsack-Public-Key-Cryptosystem-Using-Chinese-Murakami-Nasako/2ae27b1b4fa41a7eccde83e329dd6378b545b04> (accessed: 05.10.2024).
- [8] Naccache D., Stern J. A new public key cryptosystem based on higher residues. In Proceedings of the 5th ACM conference on Computer and communications security (CCS '98). Association for Computing Machinery, New York, NY, USA. 1998, p. 59–66. DOI: <https://doi.org/10.1145/288090.288106>.
- [9] Volkov, Maria Sabina A.; Gordeev, Eduard N. The application of non-injective vectors in knapsack cryptosystems. IT Security (Russia), [S.l.], 2025, v. 32, no. 1, p. 122–131. DOI: <http://dx.doi.org/10.26583/bit.2025.1.08> (in Russian).
- [10] Gordeev E.N., Leontiev V.K. On combinatorial properties of the knapsack problem. Computational Mathematics and Mathematical Physics. 2019, v. 59, no. 8, p. 1380–1388. DOI: <https://doi.org/10.1134/S0965542519080074>. – EDN: QZNJJG.
- [11] Leontiev V. K., Gordeev E.N. On the Number of Solutions to a System of Boolean Equations. Automation and Remote Control. 2021, v. 82, no. 9, p. 1581–596. DOI: <https://doi.org/10.1134/S000511792109006X>. – EDN: TFPXWF.

- [12] Leontiev V.K. Gordeev E.N., Volkov M.S.A. Classical continuity and its discrete variant. Applied physics and mathematics. 2022, no. 1, p. 31–37. DOI: <https://doi.org/10.25791/pfim.01.2022.1221>. – EDN: ZITVKA (in Russian).
- [13] Volkov M.S.A. Combinatorial properties of the bounded knapsack problem. Applied discrete mathematics. 2024, no. 63, p. 117–130. DOI: <https://doi.org/10.25791/10.17223/20710410/63/8>. – EDN: PKMABD (in Russian).
- [14] Zhang W., Wang B., Hu Y. A New Knapsack Public-Key Cryptosystem, 2009 Fifth International Conference on Information Assurance and Security, Xi'an, China. 2009, p. 53–56. DOI: <https://doi.org/10.1109/IAS.2009.300>.
- [15] Jain, A., Chaudhari, N.S. Cryptanalytic Results on Knapsack Cryptosystem Using Binary Particle Swarm Optimization. In: de la Puerta, J., et al. International Joint Conference SOCO'14-CISIS'14-ICEUTE'14. Advances in Intelligent Systems and Computing. 2014, v. 299, p. 375–384. DOI: [https://doi.org/10.1007/978-3-319-07995-0\\_37](https://doi.org/10.1007/978-3-319-07995-0_37).
- [16] Schnorr, C.P., Euchner, M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Mathematical Programming 66, p. 181–199 (1994). DOI: <https://doi.org/10.1007/BF01581144>.
- [17] Koskinen A., Non-Injective Knapsack Public-Key Cryptosystems. Theoretical Computer Science, March 2001, v. 255, no. 1–2, p. 401–422. DOI: [https://doi.org/10.1016/S0304-3975\(99\)00297-2](https://doi.org/10.1016/S0304-3975(99)00297-2).
- [18] Liu J., Bi J. Xu S. An Improved Attack on the Basic Merkle–Hellman Knapsack Cryptosystem. IEEE Access, 2019, v. 7, p. 59388–59393. DOI: <https://doi.org/10.1109/ACCESS.2019.2913678>.
- [19] Khalaf R.Z., Hamza B.H., Thakwan A.J. Attacking the Knapsack Public-key Cryptosystem. Webology. 2022, v. 19, no. 1, p. 5302–5309. DOI: <https://doi.org/10.14704/web/v19i1/web19356>.

*Статья поступила в редакцию 11.04.2025; одобрена после рецензирования 23.05.2025;  
принята к публикации 07.07.2025*

*The article was submitted 11.04.2025; approved after reviewing 23.05.2025;  
accepted for publication 07.07.2025*