УДК 519.7: 004: 681.5

**А.В. Трепачева**

# КРИПТОАНАЛИЗ СИММЕТРИЧНЫХ ПОЛНОСТЬЮ ГОМОМОРФНЫХ ЛИНЕЙНЫХ КРИПТОСИСТЕМ НА ОСНОВЕ ЗАДАЧИ ФАКТОРИЗАЦИИ ЧИСЕЛ*

*Рассматриваются полностью гомоморфные схемы шифрования, криптостойкость которых их авторы обосновывают с использованием сложности решения задачи факторизации больших чисел. В частности, проводится анализ стойкости криптосистем, в которых шифртексты представляют собой матрицы над кольцом вычетов по составному модулю, трудному для факторизации, а шифрование и расшифрование являются преобразованиями подобия. Проводится подробный анализ основных свойств шифртекстов, производимых алгоритмами шифрования этих криптосистем. На основе этого анализа выделяются основные уязвимости, которым они подвержены. Наиболее подробно анализируется криптостойкость двух недавно предложенных криптосистем указанного вида против атаки по известным открытым текстам. Рассматривается ранее описанная в литературе стратегия атаки на одну из этих криптосистем, основанная на решении системы линейных уравнений по составному модулю. Основным результатом настоящей работы является то, что по сравнению с предшественниками даются строгие теоретические оценки вероятности раскрытия секретного ключа при использовании этой стратегии. А также приводятся практические оценки вероятности раскрытия ключа, которые хорошо согласуются с теоретическими предсказаниями. Проведенный анализ показал, что первая из рассмотренных криптосистем является нестойкой к рассмотренной атаке по известным открытым текстам. Однако для раскрытия ключа с вероятностью ≈1 необходимо иметь количество пар (открытый текст, шифртекст), зависящее полилогарифмически от числа сомножителей, образующих составное число, по модулю которого ведутся вычисления. При числе пар меньшем данной величины криптосистема является защищенной, что частично соответствует оценкам защищенности, данным её авторами. Для взлома же второй криптосистемы нужно гораздо меньшее количество пар и уровень её криптостойкости совсем не соответствует заявленному.*

*Полностью гомоморфная криптосистема; атака по известным открытым текстам; защищённые облачные вычисления; задача факторизация чисел.*

**A.V. Trepacheva**

# CRYPTANALYSIS OF SYMMETRIC FULLY HOMOMORPHIC LINEAR CRYPTOSYSTEMS BASED ON NUMBERS FACTORIZATION PROBLEM

*This paper considers the fully homomorphic cryptosystems based by their authors on a factorization problem. In particular, the paper analyses the security of cryptosystems whose ciphertexts are matrices with elements modulo composite number that is hard to factorize, while encryption and decryption procedures are similarity transformations. We carefully analyze the properties of ciphertexts produced by their encryption algorithms. And on the base of this analysis main vulnerabilities of the cryptosystems are highlighted. The main focus of this paper is placed on analysis of resistance against known plaintext attack of two recently proposed cryptosystems belonging to this type. In particular, we discuss one strategy of known plaintext attack on them proposed in literature. It is based on solving of linear system modulo composite number. Our main result in comparison with predecessors is providing a strict theoretical estimation of probability to recover secret key for different number of intercepted pairs (plaintext, ciphertext) using this strategy. Also practical estimations of probability to find a key based on computer experiments are given. They correlate well with theoretical predictions. Our analysis shows that the first considered cryptosystem is vulnerable to known plaintext attack based on linear system solving. However to recover key with probability ≈1 one needs to have the number of pairs (plaintext, ciphertext) depending polylogarithmically on the*

* Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта №15-07-00597 а.

*number of factors in exploiting composite modulus. And for the less number of pairs the cryptosystem is secure. This to some extent corresponds to security estimations given by the authors of cryptosystem. As for the second cryptosystem, its breaking requires much less number of pairs and thus its security level doesn't match with level stated by the authors.*

*Fully homomorphic cryptosystem; known plaintext attack; secure cloud computing; factorization problem.*

**Введение.** Разработка *полностью гомоморфных криптосистем* (ПГК), позволяющих вычислять над зашифрованными данными любые функции, очень актуальна из-за необходимости защищать приватные данные, хранящиеся и обрабатываемые удаленными облачными серверами [1]. В связи с этим на данный момент предложено много разных ПГК [2]. Лидирующим направлением работы является построение ПГК, основанных на методе Джентри [3]. Основная особенность этих ПГК – наличие строго обоснованной семантической криптостойкости и при этом полная непригодность для практики в силу низкой эффективности. Например, согласно [2], наиболее эффективная на сегодня ПГК, базирующаяся на [3], преобразует 4 MB открытых текстов в 73 TB шифртекстов при значениях параметров ПГК, гарантирующих приемлемый уровень криптостойкости. Ясно, что такое расширение объема данных неприемлемо в приложениях. В силу этого не прекращаются попытки построить альтернативные ПГК [4–6], не использующие метод из [3] и являющиеся простыми, эффективными и гарантированно криптостойкими.

**Постановка задачи.** В литературе наиболее активно предлагаются различные ПГК, основанные на сложности задачи факторизации чисел [7–13], поскольку эта задача является общепринятым эталоном вычислительной сложности [14]. Эти ПГК – достаточно простые и эффективные для применения на практике, однако криптостойкость многих из них ([7–10]) оказалась недостаточной [15–18], а криптостойкость других [11–13] плохо исследована.

В данной работе подробно рассматриваются ПГК из [11–13], основанные на следующем подходе. Открытый текст $m \in \mathbb{Z}_n$ отображается в $\mathbf{D} \in \mathbb{Z}_n^{k\times k}$ так, что $m$ – собственное число $\mathbf{D}$, где $n \in \mathbb{N}$ – трудное для факторизации число, состоящее из $k$ взаимно простых сомножителей битовой длины $\lambda \geq 1024$. Ключ – обратимая матрица $\mathbf{K} \in \mathbb{Z}_n^{k\times k}$ и тогда шифртекст – $\mathbf{C} = \mathbf{K}^{-1} \cdot \mathbf{D} \cdot \mathbf{K} \in \mathbb{Z}_n^{k\times k}$.

*Основные результаты.* В работе анализируется стратегия *атаки по известным открытым текстам* (АИОТ) на ПГК [7], описанная в [17], и для неё приводится точная формула вероятности найти ключ по $t$ парам (открытый текст, шифртекст). Из этой формулы следует, что для раскрытия ключа с вероятностью $\approx 1$ должно выполняться $t > k$. Более точно, установлено, что при рекомендуемых в [11] значениях $2 \leq k \leq 1024$ взлом [11] успешен с вероятностью $\approx 1$ при $t = \alpha \cdot k$, где $\alpha = \alpha(k)$, $\alpha \in [5,10]$ – величина, не зависящая от $\lambda$. Также показано, что при $t \leq k$ вероятность успеха АИОТ [17] $\approx 0$ для $\forall k$. Эти данные подтверждаются вычислительными экспериментами. Все это в итоге показывает неточность оценок, указанных в [17]. А именно, в [17] утверждалось, что независимо от выбора $k$ достаточно $t = O(1)$ пар для взлома [11] с вероятностью $\approx 1$.

Заметим еще, что в [11] говорится, что ПГК стойка к АИОТ при $t < k \cdot \ln poly(\lambda)$, где $poly$ – $\forall$ полином, $\deg(poly) \geq 1$. Однако, исходя из указанных выше оценок, ясно, что в [11] степень стойкости ПГК против АИОТ была переоценена.

Также в данной работе рассмотрена применимость АИОТ [11] к ПГК из [8, 9], являющейся модификацией [11] и ранее не проанализированной в литературе. Было выявлено, что ПГК [8, 9] гораздо слабее исходной ПГК [11]. Хотя авторы [8, 9] утверждают, что ПГК защищена против АИОТ при $t \le k$, АИОТ [11] находит ключ [8,9] с вероятностью $\approx 1$ при $t \in [\nu, k]$, где $\nu \in (2, k)$.

**1. Необходимые сведения и обозначения.** Кольцо целых чисел по модулю числа $n \in \mathbb{N}$ обозначается как $\mathbb{Z}_n$; подгруппа обратимых по умножению элементов $\mathbb{Z}_n$ – $\mathbb{Z}_n^*$; функция Эйлера – $\varphi$ и выполняется $\left|\mathbb{Z}_n^*\right| = \varphi(n)$; для $a \in \mathbb{Z}$ остаток от деления $a$ на $n \in \mathbb{N}$ – $[a]_n$. Кольцо матриц $k \times k$ с элементами из $\mathbb{Z}_n$ будем обозначать $\mathbb{Z}_n^{k\times k}$, где $GL(\mathbb{Z}_n^{k\times k})$ – подгруппа обратимых матриц и матрицы обозначаются как $\mathbf{M} = \{m_{i,j}\}_{i=\overline{1,k}, j=\overline{1,k}}$. Диагональная матрица $\in \mathbb{Z}_n^{k\times k}$ с элементами $a_1, ..., a_k \in \mathbb{Z}_n$ на главной диагонали обозначается $diag(a_1, ..., a_k)$.

Модуль, состоящий из векторов длины $k$ с элементами $\in \mathbb{Z}_n$, обозначается как $\mathbb{Z}_n^k$, а сами векторы, например, так – $\mathbf{v} = (v_1, ..., v_k)$. Вектор $\mathbf{v}$ такой, что $\exists i \mid v_i = 1$ и $v_j = 0$ для $\forall j \mid j \ne i$, будем обозначать $\mathbf{e}_i$. Нулевой вектор обозначим как $\mathbf{0}$. Отметим, что, как и в векторных пространствах, любой базис в $\mathbb{Z}_n^k$ имеет фиксированный размер $k$ [19]. Это справедливо и для всех его подмодулей, где подмодуль $\mathrm{Lin}(\mathbf{v}_1, ..., \mathbf{v}_d)$ модуля $\mathbb{Z}_n^k$ размерности $d \le k$ состоит из всевозможных линейных комбинаций линейно независимых векторов $\{\mathbf{v}_1, ..., \mathbf{v}_d\}$.

Запись $[\mathbf{M}]_p$ (или $[\mathbf{v}]_p$) означает, что $\forall m_{i,j}$ (или $\forall v_i$) приводится по $\bmod p$. Вероятность события $M$ будем обозначать как $\Pr[M]$. Если задано кольцо $R$, то $s \xleftarrow{\$} R$ означает, что $s$ из $R$ выбирается по равномерному распределению.

**Теорема 1 (Китайская теорема об остатках, КТО, [20]).** Для $n = \prod_{i=1}^{k} f_i$, где НОД($f_i$, $f_j$)=1, $i \ne j$, выполняется $\mathbb{Z}_n \cong \mathbb{Z}_{f_1} \times ... \times \mathbb{Z}_{f_k}$ (в $\mathbb{Z}_{f_1} \times ... \times \mathbb{Z}_{f_k}$ операции $+, \cdot$ поточечные). Для вычисления по $([a]_{f_1}, ..., [a]_{f_k}) \in \mathbb{Z}_{f_1} \times ... \times \mathbb{Z}_{f_k}$ соответствующего ему числа $a \in \mathbb{Z}_n$ можно воспользоваться формулой:

$$a = \text{КТО}([a]_{f_1}, f_1 ..., [a]_{f_k}, f_k) = \sum_{i=1}^{k} [a]_{f_i} \cdot S_i \cdot S_i^{-1}, \quad S_i = \frac{n}{f_i}, S_i^{-1} := \frac{1}{S_i} \pmod{f_i} \cdot \square$$

Если есть векторы $\mathbf{v}_i = (v_{i,1}, ..., v_{i,t}) \in \mathbb{Z}_{f_i}^t, i = \overline{1,k}$, то $\mathbf{v} = (v_1, ..., v_t) =$ $=$КТО $(\mathbf{v}_1, f_1, ..., \mathbf{v}_k, f_k) \in \mathbb{Z}_n^t$ – вектор такой, что $v_j =$ КТО $(v_{1,j}, f_1, ..., v_{k,j}, f_k)$.

**2. Простейшая симметричная ПГК на основе факторизации и линейных преобразований и анализ её защищенности.** Конструкция этого типа впервые была предложена в [10]. Открытый текст $m \in \mathbb{Z}_n$, где $n = p \cdot q$, $p, q \in \mathbb{N}, p \neq q$ – простые числа, $\log n = \lambda \geq 1024$, $\log p = \log q$ (т.е. $n$ – трудный для факторизации RSA-модуль), шифруется в два этапа: 1) $\mathbf{D} := diag(m, r) \in \mathbb{Z}_n^{2\times 2}$, где $r \xleftarrow{\$} \mathbb{Z}_n$; 2) $\mathbf{C} := \mathbf{K}^{-1} \cdot \mathbf{D} \cdot \mathbf{K}$, где $\mathbf{K} \xleftarrow{\$} GL(\mathbb{Z}_n^{2\times 2})$ – секретный ключ. Так как осуществляется преобразование подобия, то $m$ – собственное число (с.ч.) $\mathbf{C}$, имеющее собственный вектор (с.в.) $\mathbf{v}_1 = \mathbf{K}^{-1} \cdot \mathbf{e}_1 = (v_{1,1}, v_{1,2})$. Для расшифрования $\mathbf{C}$ вычисляется $\mathbf{v} = \mathbf{C} \cdot \mathbf{v}_1$, а затем $m := v_1 / v_{1,1}$.

Криптосистема [10] – ПГК, так как для $\mathbf{C}_i = \mathbf{K}^{-1} \cdot \mathbf{D}_i \cdot \mathbf{K} \in \mathbb{Z}_n^{2\times 2}, i = 1, 2$, $\mathbf{D}_i = diag(m_i, r_i) \in \mathbb{Z}_n^{2\times 2}$ справедливо $\mathbf{C}_1 + \mathbf{C}_2 = \mathbf{K}^{-1} \cdot \mathbf{D}_+ \cdot \mathbf{K}$, $\mathbf{C}_1 \cdot \mathbf{C}_2 = \mathbf{K}^{-1} \cdot \mathbf{D}_* \cdot \mathbf{K}$, где $\mathbf{D}_+ = diag([m_1 + m_2]_n, [r_1 + r_2]_n)$, $\mathbf{D}_* = diag([m_1 \cdot m_2]_n, [r_1 \cdot r_2]_n)$. Поэтому можно гомоморфно вычислить $\forall$ полином, причем операции $+, \cdot$ над шифртекстами вычислительно «дешевые».

ПГК [10] стойка против атаки по шифртекстам, так как для нахождения $m$ по $\mathbf{C}$ нужно решить квадратное уравнение над $\mathbb{Z}_n$, что эквивалентно факторизации $n$ [21]. Однако против АИОТ ПГК нестойка. Если есть пара $(m, \mathbf{C})$, то можно составить СЛАУ $(\mathbf{C} - m \cdot \mathbf{I}) \cdot \mathbf{v} = \mathbf{0}$ по $\bmod n$, множество решений которой $= \mathrm{Lin}(\mathbf{v}_1)$ при $[r - m]_n \in \mathbb{Z}_n^*$. Так как $r \xleftarrow{\$} \mathbb{Z}_n$, то в силу выбора $n$ $\Pr\left[[r - m]_n \in \mathbb{Z}_n^*\right] = \dfrac{\varphi(n)}{n} \approx 1$, и поэтому даже наличие одной пары $(m, \mathbf{C})$ компрометирует [10]. Более подробную информацию по осуществлению АИОТ на ПГК [10] можно найти в [17].

**3. ПГК из работы [11].** В [11] ПГК из [10] была модифицирована. Целью было перестроить [10] так, чтоб понизить вероятность успеха рассмотренной АИОТ. В [11] $n$ выбирается как $n = \prod_{i=1}^{k} f_i$, НОД($f_i, f_j$)=1 для $\forall i \neq j$, $f_i = p_i \cdot q_i$ – RSA модули, где $\lambda = \log f_i \geq 1024$ и $\log p_i = \log q_i$. Шифрование $m \in \mathbb{Z}_n$ осуществляется так:

1) $\mathbf{D} := diag(m, a, b, c) \in \mathbb{Z}_n^{4\times 4}$, где $a, b, c \in \mathbb{Z}_n$ – решения систем сравнений $a \equiv a_i (\bmod\ f_i), b \equiv b_i (\bmod\ f_i), c \equiv c_i (\bmod\ f_i), i = \overline{1,k}$. А для генерации $a_i, b_i, c_i$ поступают так. Генерируется $r \xleftarrow{\$} \mathbb{Z}_n$, а затем для $\forall i = \overline{1,k}$ $(a_i, b_i, c_i)$ выбирают по вероятностному распределению $\Upsilon$:

$$\Pr\left[(a_i, b_i, c_i) = (x, r, r)\right] = 1 - \frac{1}{k+1},$$

$$\Pr\left[(a_i, b_i, c_i) = (r, x, r)\right] = \Pr\left[(a_i, b_i, c_i) = (r, r, x)\right] = \frac{1}{2 \cdot (k+1)};$$

2) $\mathbf{C} := \mathbf{K}^{-1} \cdot \mathbf{D} \cdot \mathbf{K} \in \mathbb{Z}_n^{4\times 4}$, где $\mathbf{K} \in GL(\mathbb{Z}_n^{4\times 4})$ – секретный ключ.

Здесь, как и в [6] $m \in \mathbb{Z}_n$ – с.ч. $\mathbf{C} \in \mathbb{Z}_n^{4\times 4}$ и для расшифрования нужен $\mathbf{v}_1 = \mathbf{K}^{-1} \cdot \mathbf{e}_1 \in \mathbb{Z}_n^4$. Гомоморфные свойства [11] совершенно аналогичны гомоморфным свойствам [10]. Для достижения приемлемой скорости операций $+, \cdot$ над шифртекстами в [11] полагают $2 \le k \le 2^{10}$.

**4. Свойства шифртекстов ПГК [11].** Обсудим основные свойства шифртекстов ПГК [11], позволяющие повысить стойкость к АИОТ из [17] по сравнению с [10]. Отметим, что в [11,17] эти свойства имелись в виду, но подробно описаны не были.

Во-первых, в [11] для $\forall f_i, i = \overline{1,k}$ $[m]_{f_i}$ – с.ч. $[\mathbf{C}]_{f_i} \in \mathbb{Z}_{f_i}^{4\times 4}$ геометрической кратности $\ge 2$. Действительно, имеем $[\mathbf{C}]_{f_i} = \left[\mathbf{K}^{-1} \cdot [\mathbf{D}]_{f_i} \cdot \mathbf{K}\right]_{f_i}$, где $[\mathbf{D}]_{f_i} = diag([m]_{f_i}, [a]_{f_i}, [b]_{f_i}, [c]_{f_i})$ и только одно из $[a]_{f_i}, [b]_{f_i}, [c]_{f_i}$ равно $[m]_{f_i}$. Тогда для $\forall i = \overline{1,k}$ множество с.в. $[\mathbf{C}]_{f_i} \in \mathbb{Z}_{f_i}^{4\times 4}$, отвечающих с.ч. $[m]_{f_i}$, содержит $\Lambda_i = \mathrm{Lin}([\mathbf{v}_1]_{f_i}, [\mathbf{v}_*^i]_{f_i})$, где $\mathbf{v}_1 = \mathbf{K}^{-1} \cdot \mathbf{e}_1$, $\mathbf{v}_*^i = \mathbf{K}^{-1} \cdot \mathbf{e}_*^i$ – линейно независимы, так как по $\Upsilon$:

$$\Pr\left[\mathbf{e}_*^i = \mathbf{e}_2\right] = 1 - \frac{1}{k+1}, \ \Pr\left[\mathbf{e}_*^i = \mathbf{e}_3\right] = \Pr\left[\mathbf{e}_*^i = \mathbf{e}_4\right] = \frac{1}{2\cdot(k+1)}.$$

При этом к $\{[\mathbf{v}_1]_{f_i}, [\mathbf{v}_*^i]_{f_i}\}$ могут добавиться дополнительные линейно независимые с.в., соответствующие $[m]_{f_i}$. Пусть, к примеру, $[a]_{f_i} = [m]_{f_i}, [b]_{f_i} = [r]_{f_i}, [c]_{f_i} = [r]_{f_i}$ и тогда

$$[\mathbf{D}]_{f_i} - [m]_{f_i} \cdot \mathbf{I} \equiv diag(0, 0, [r-m]_{f_i}, [r-m]_{f_i}) (\mathrm{mod}\ f_i).$$

Исходя из последнего, при $[r-m]_{f_i} = 0$ множество с.в. $[\mathbf{C}]_{f_i}$ для с.ч. $[m]_{f_i}$ – $\mathrm{Lin}([\mathbf{v}_1]_{f_i}, [\mathbf{v}_2]_{f_i}, [\mathbf{v}_3]_{f_i}, [\mathbf{v}_4]_{f_i})$, где $\mathbf{v}_i = \mathbf{K}^{-1} \cdot \mathbf{e}_i, i = \overline{1,4}$. Если же $[r-m]_{f_i} = p_i \cdot \alpha, \alpha \in \mathbb{Z}_{q_i}^*$ (или $[r-m]_{f_i} = q_i \cdot \beta, \beta \in \mathbb{Z}_{p_i}^*$), то дополнительные с.в. имеют вид $\mathbf{v}_\mathbf{s} = [\mathbf{K}^{-1} \cdot \mathbf{s}]_{f_i}$, где $\mathbf{s} = (0, 0, q_i \cdot \gamma, q_i \cdot \tau) \in \mathbb{Z}_{f_i}^4$, $\gamma, \tau \in \mathbb{Z}_{p_i}^*$ (или $\mathbf{s} = (0, 0, p_i \cdot \omega, p_i \cdot \psi) \in \mathbb{Z}_{f_i}^4$, $\omega, \psi \in \mathbb{Z}_{q_i}^*$). Вектор $\mathbf{v}_\mathbf{s}$ не является линейно независимым от $\{[\mathbf{v}_1]_{f_i}, [\mathbf{v}_*^i]_{f_i}\}$, так как $\left[0 \cdot [\mathbf{v}_1]_{f_i} + 0 \cdot [\mathbf{v}_*^i]_{f_i} + [\beta \cdot \mathbf{v}_\mathbf{s}]_{f_i}\right]_{f_i} = \mathbf{0}$, где $\beta = p$ $(= q)$. Но тем не менее $\mathbf{v}_\mathbf{s} \notin \Lambda_i$, и это усложняет ситуацию.

Однако для $\forall i = \overline{1,k}$ можно полагать, что $[r-m]_{f_i} \xleftarrow{\$} \mathbb{Z}_{f_i}$, и тогда $\varepsilon = \Pr\left[[r-m]_{f_i} \notin \mathbb{Z}_{f_i}^*\right] = \frac{f_i - \varphi(f_i)}{f_i}$ и $\varepsilon << 1$, так как $f_i$ – RSA модуль. Поэтому с вероятностью $\approx 1$ $[m]_{f_i}$ – с.ч. $[\mathbf{C}]_{f_i} \in \mathbb{Z}_{f_i}^{4\times 4}$, имеющее множество с.в. строго $= \Lambda_i$.

Вероятность того, что множество с.в. для с.ч. $[m]_{f_i}$ совпадает с $\Lambda_i$ для $\forall i$, равна $\theta = \prod_{i=1}^{k} \frac{(p_i - 1)\cdot(q_i - 1)}{p_i \cdot q_i}$ (так как события «$[r-m]_{f_i} \in \mathbb{Z}_{f_i}^*$» не зависимы). С учетом выбора $k$ и $f_i, i = \overline{1,k}$ можно полагать $\theta = 1$. Поэтому всюду ниже будем для простоты работать со случаем, когда для $\forall i$ пространство с.в. $= \Lambda_i$.

Покажем, что с.ч. $m$ по модулю $n$ также имеет геометрическую кратность 2. Для этого понадобится следующая лемма.

**Лемма 1.** Пусть $n = \prod_{i=1}^{k} f_i$, НОД$(f_i, f_j) = 1$ при $i \neq j$, $\{\mathbf{v}_{i,j}\}_{j=1}^{l}, i = \overline{1,k}$ – наборы линейно независимых по $\mathrm{mod}\, f_i$ векторов, $\mathbf{v}_{i,j} \in \mathbb{Z}_{f_i}^d, l \le d$. Тогда $\Psi = \{\mathbf{v} \mid \mathbf{v} = \mathrm{КТО}(\sum_{j=1}^{l} \alpha_{1,j}\cdot \mathbf{v}_{1,j}, f_1, ..., \sum_{j=1}^{l} \alpha_{k,j}\cdot \mathbf{v}_{k,j}, f_k) \in \mathbb{Z}_n^d,\ \alpha_{i,j} \in \mathbb{Z}_{f_i}\}$ представляет собой подмодуль размерности $l$ с базисом $\{\mathbf{v}'_j\}_{j=1}^{l}$, $\mathbf{v}'_j = \mathrm{КТО}(\mathbf{v}_{1,j}, f_1, ..., \mathbf{v}_{k,j}, f_k) \in \mathbb{Z}_n^d$.

*Доказательство.* По КТО $\forall \mathbf{v} \in \Psi$ можно представить как $\mathbf{v} = \left[\sum_{j=1}^{l} \beta_j \cdot \mathbf{v}'_j\right]_n$, где $\beta_j \in \mathbb{Z}_n, j = \overline{1,l}$ однозначно определены из $\beta_j \equiv \alpha_{i,j} (\mathrm{mod}\, f_i), i = \overline{1,k}$. А также $\{\mathbf{v}'_i\}_{i=1}^{l}$ линейно независимы по $\mathrm{mod}\, n$, так как $\{\mathbf{v}_{i,j}\}_{j=1}^{l}$ линейно независимы для $\forall i$. Действительно, если предположить, что $\exists \delta_j \in \mathbb{Z}_n, j = \overline{1,l}$ не все равные нулю, такие, что $\left[\sum_{j=1}^{l} \delta_j \cdot \mathbf{v}'_j\right]_n = \mathbf{0}$, то по КТО $\exists i \in \overline{1,k}$ такое, что $\left[\sum_{j=1}^{l} [\delta_j]_{f_i} \cdot \mathbf{v}_{i,j}\right]_{f_i} = \mathbf{0}$, где $\exists j' \mid [\delta_{j'}]_{f_i} \neq 0$. Последнее противоречит тому, что $\{\mathbf{v}_{i,j}\}_{j=1}^{l}$ линейно независимы по $\mathrm{mod}\, f_i$. □

По лемме 1, КТО и свойствам сравнений СЛАУ $(\mathbf{C} - m\cdot\mathbf{I})\cdot\mathbf{v} = 0$ с вероятностью $\approx 1$ по $\mathrm{mod}\, n$ имеет множество решений $= \mathrm{Lin}(\mathbf{v}_1, \mathbf{v}_*)$, где $\mathbf{v}_* = \mathbf{K}^{-1}\cdot\mathbf{e}_*$, $\mathbf{e}_* = \mathrm{КТО}(\mathbf{e}_*^1, f_1, ..., \mathbf{e}_*^k, f_k) \in \mathbb{Z}_n^4$ и $\{\mathbf{v}_1, \mathbf{v}_*\}$ линейно независимы, так как $\{[\mathbf{v}_1]_{f_i}, [\mathbf{v}_*]_{f_i}\}$ линейно независимы для $\forall i$. Это означает, что геометрическая кратность с.ч. $m$ матрицы $\mathbf{C}$ по $\mathrm{mod}\, n$ будет = 2.

Теперь уже становится ясным замысел авторов [17]. Для $\forall \mathbf{C}$ вектор $\mathbf{v}_1 = \mathbf{K}^{-1}\cdot\mathbf{e}_1$ – с.в. для с.ч. $m \in \mathbb{Z}_n$ и следовательно его можно использовать для расшифрования. Однако шифрование случайным образом добавляет еще один линейно независимый с.в. $\mathbf{v}_*$ для с.ч $m \in \mathbb{Z}_n$. Поскольку $\mathbf{v}_*$ разный для разных $\mathbf{C}$, то им нельзя корректно расшифровать $\forall \mathbf{C}$. Это усложняет криптоанализ [11] по известным открытым текстам по сравнению с [10].

**6. Криптоанализ ПГК из [11].** Во-первых, отметим, что так как $n$ трудно факторизовать, то ПГК [11] защищена против атаки только по шифртекстам. Что же касается АИОТ, то теперь одной пары $(m,\mathbf{C})$ для раскрытия $\mathbf{v}_1=\mathbf{K}^{-1}\cdot\mathbf{e}_1$ недостаточно, так как $(\mathbf{C}-m\cdot\mathbf{I})\cdot\mathbf{v}=0$ по $\bmod n$ имеет множество решений $\mathrm{Lin}(\mathbf{v}_1,\mathbf{v}_*)$ с вероятностью $\approx 1$.

Рассмотрим случай, когда у противника есть $t\geq 2$ пар $(m_j,\mathbf{C}_j)$, $j=\overline{1,t}$, изготовленных на $\mathbf{K}$. Так как $\mathbf{v}_1$ – решение $(\mathbf{C}_j-m_j\cdot\mathbf{I})\cdot\mathbf{v}=0$ для $\forall j=\overline{1,t}$ по $\bmod n$, то для поиска $\mathbf{v}_1$ можно записать СЛАУ (1) с матрицей $\mathbf{A}\in\mathbb{Z}_n^{(4\cdot t)\times t}$ относительно неизвестного $\mathbf{v}$:

$$\begin{cases}(\mathbf{C}_1-m_1\cdot\mathbf{I})\cdot\mathbf{v}=0\\ \ldots\\ (\mathbf{C}_t-m_t\cdot\mathbf{I})\cdot\mathbf{v}=0.\end{cases} \tag{1}$$

Множество решений (1) имеет вид $V=V_1\cap\ldots\cap V_t$, где $V_j=\mathrm{Lin}(\mathbf{v}_1,\mathbf{v}_{*,j})$, $\mathbf{v}_{*,j}=\mathbf{K}^{-1}\cdot\mathbf{e}_{*,j}\in\mathbb{Z}_n^4$, $j=\overline{1,t}$ и в соответствии с $\Upsilon$ для $\forall i\in\overline{1,k}$:

$$\begin{gathered}\Pr\left[\mathbf{e}_{*,j}\equiv\mathbf{e}_2(\bmod f_i)\right]=1-\frac{1}{k+1},\\ \Pr\left[\mathbf{e}_{*,j}\equiv\mathbf{e}_3(\bmod f_i)\right]=\Pr\left[\mathbf{e}_{*,j}\equiv\mathbf{e}_4(\bmod f_i)\right]=\frac{1}{2\cdot(k+1)}.\end{gathered} \tag{2}$$

Ясно, что $\mathrm{Lin}(\mathbf{v}_1)\subseteq V$ и раскрыть ключ, решая (1), можно $\Leftrightarrow$ $\mathrm{Lin}(\mathbf{v}_1)=V$. Так что вопрос теперь лишь в величине $\eta=\Pr\left[\mathrm{Lin}(\mathbf{v}_1)=V\right]$.

Чтобы дать на него ответ, отметим, что по КТО $\forall\mathbf{v}'\in\mathbb{Z}_n^4$ такой, что $[\mathbf{A}\cdot\mathbf{v}']_n=\mathbf{0}$, имеет вид $\mathbf{v}'=\mathrm{КТО}([\mathbf{v}']_{f_1},f_1,\ldots,[\mathbf{v}']_{f_k},f_k)$, где $\left[\mathbf{A}\cdot[\mathbf{v}']_{f_i}\right]_{f_i}=\mathbf{0}$, $[\mathbf{v}']_{f_i}\in\mathbb{Z}_{f_i}^4$ и соответствие между $\mathbf{v}'$ и $([\mathbf{v}']_{f_1},\ldots,[\mathbf{v}']_{f_k})$ однозначное. Поэтому, если для $\forall i$ (1) имеет множество решений $V^i=\mathrm{Lin}([\mathbf{v}_1]_{f_i})$ по $\bmod f_i$, то и $\mathrm{Lin}(\mathbf{v}_1)=V$. Оценим вероятность последнего.

Рассмотрим СЛАУ (1) по $\bmod f_i$ для фиксированного $i$. Её множество решений имеет вид $V^i=V_1^i\cap\ldots\cap V_t^i$, где $V_j^i=\mathrm{Lin}([\mathbf{v}_1]_{f_i},[\mathbf{v}_{*,j}]_{f_i})$ и $[\mathbf{v}_{*,j}]_{f_i}=[\mathbf{K}^{-1}\cdot[\mathbf{e}_{*,j}]_{f_i}]_{f_i}$, $[\mathbf{e}_{*,j}]_{f_i}\in\{\mathbf{e}_2,\mathbf{e}_3,\mathbf{e}_4\}$. Если $\exists j_1,j_2\mid j_1\neq j_2$ такие, что $[\mathbf{e}_{*,j_1}]_{f_i}\neq[\mathbf{e}_{*,j_2}]_{f_i}$, то $V^i=\mathrm{Lin}([\mathbf{v}_1]_{f_i})$. Вероятность последнего в силу (2) и независимости $\mathbf{C}_j$, $j=\overline{1,t}$ равна:

$$\begin{gathered}\vartheta(k,t)=1-\left(1-\frac{1}{k+1}\right)^t-2\cdot\left(\frac{1}{2\cdot(k+1)}\right)^t=\\ =1-\left(\frac{k}{k+1}\right)^t-2\cdot\left(\frac{1}{2\cdot(k+1)}\right)^t.\end{gathered} \tag{3}$$

Так как для $\forall i \in \overline{1,k}$ векторы $[\mathbf{e}_{*,j}]_{f_i}$ выбираются независимо, то в соответствии со сказанным выше получаем:

$$\Omega(t,k) = \Pr\left[\forall i = \overline{1,k}: \mathrm{Lin}([\mathbf{v}_1]_{f_i}) = V^i\right] = \vartheta^k. \quad (4)$$

Осталось показать, что если $\exists i_*$ такое, что множество решений (1) по $\bmod f_{i_*}$ имеет вид $V^{i_*} = \mathrm{Lin}([\mathbf{v}_1]_{f_{i_*}}, \mathbf{s}_{i_*})$, $\mathbf{s}_{i_*} = \left[\mathbf{K}^{-1} \cdot \mathbf{e}_{s_{i_*}}\right]_{f_{i_*}}$, $\mathbf{e}_{s_{i_*}} \in \{\mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$, то $\mathrm{Lin}(\mathbf{v}_1) \subset V$. Пусть для некоторого $i_*$ – $V^{i_*} = \mathrm{Lin}([\mathbf{v}_1]_{f_{i_*}}, \mathbf{s}_{i_*})$, а для $\forall i \mid i \neq i_*$ – $V^i = \mathrm{Lin}([\mathbf{v}_1]_{f_i})$. По КТО $\forall \mathbf{v} \in V$ можно представить в виде $\mathbf{v} =$ КТО$(\alpha \cdot [\mathbf{v}_1]_{f_{i_*}} + \beta \cdot \mathbf{s}_{i_*}, f_{i_*}, [\mathbf{v}_1]_{n/f_{i_*}}, n/f_{i_*})$, где $\alpha, \beta \in \mathbb{Z}_{f_{i_*}}$. Исследуем взаимоотношения $\mathbf{v}_1, \mathbf{v}_{2,\mathbf{s}_{i_*}} \in V$, претендующих на роль базиса $V$, где $\mathbf{v}_{2,\mathbf{s}_{i_*}}$ = КТО $(\mathbf{s}_{i_*}, f_{i_*}, [\mathbf{v}_1]_{n/f_{i_*}}, n/f_{i_*})$. Ясно, что они линейно зависимы, так как существует их линейная комбинация $\gamma \cdot \mathbf{v}_1 + \delta \cdot \mathbf{v}_{2,\mathbf{s}_{i_*}} = \mathbf{0}$, где $\gamma, \delta \in \mathbb{Z}_n, \gamma, \delta \neq 0$ и выполняется $\gamma, \delta \equiv 0 (\bmod f_{i_*})$, $\gamma, \delta \equiv \pm 1 (\bmod (n/f_{i_*}))$. И так как $\{[\mathbf{v}_1]_{f_{i_*}}, \mathbf{s}_{i_*}\}$ линейно независимы по $\bmod f_{i_*}$, то нетривиальные линейные комбинации $\mathbf{v}_1, \mathbf{v}_{2,\mathbf{s}_{i_*}}$, равные $\mathbf{0}$, всегда таковы, что $\gamma, \delta \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$. Из этого следует, что $\mathrm{Lin}(\delta \cdot \mathbf{v}_{2,\mathbf{s}_{i_*}}) \subset \mathrm{Lin}(\mathbf{v}_1)$. Однако в силу необратимости $\gamma, \delta \in \mathbb{Z}_n$ $\mathbf{v}_{2,\mathbf{s}_{i_*}} \notin \mathrm{Lin}(\mathbf{v}_1)$ и $\Rightarrow \mathrm{Lin}(\mathbf{v}_1) \subset V$. Отметим, что если $V^{i_*} = \mathrm{Lin}([\mathbf{v}_1]_{f_{i_*}}, \mathbf{s}_{i_*})$ для нескольких $i_*$, то для доказательства $\mathrm{Lin}(\mathbf{v}_1) \subset V$, нужно учесть лемму 1.

Итак, мы получили, что $\mathrm{Lin}(\mathbf{v}_1) = V \Leftrightarrow \forall i = \overline{1,k}: \mathrm{Lin}([\mathbf{v}_1]_{f_i}) = V^i$. И, исходя из этого, имеем

$$\Pr\left[\mathrm{Lin}(\mathbf{v}_1) = V\right] = \Omega(t,k). \quad (5)$$

Итого, вероятность $\eta$ гарантированно отыскать по парам $(m_i, \mathbf{C}_i), i = \overline{1,t}$ вектор $\mathbf{v}_1 = \mathbf{K}^{-1} \cdot \mathbf{e}_1 \in \mathbb{Z}_n^4$ равна $\Omega(t,k)$. Рассмотрим некоторые свойства $\Omega(t,k)$.

1. Зафиксируем $\forall k \geq 0$, тогда $\Omega(t,k)$ – монотонно возрастающая функция и $\lim\limits_{t \to \infty} \Omega(t,k) = 1$. Однако т.к. $\dfrac{k}{k+1} \approx 1$, то $\Omega(t,k)$ медленно $\to 1$ для больших $k$.

2. Если в (5) положить $t = k$, то получим $\Omega(t,k) \approx \left(1 - \dfrac{1}{e}\right)^k \xrightarrow{k \to \infty} 0$.

В табл. 1 представлены значения $\Omega(t,k)$ для разных $k, t$, а также практические оценки $\eta$ – $\tilde{\Omega}(t,k)$, полученные при тестировании атаки на [11], реализованной с помощью Qt и библиотеки NTL. Для получения каждого $\tilde{\Omega}(t,k)$ проводилось $10^4$ независимых испытаний.

Таблица 1

**Значения $\Omega(t,k)$ и $\tilde{\Omega}(t,k)$ при $k=4$ и $k=32$**

| $k=4$ | | | $k=32$ | | |
|---|---|---|---|---|---|
| $t$ | $\Omega(t,k)$ | $\tilde{\Omega}(t,k)$ | $t$ | $\Omega(t,k)$ | $\tilde{\Omega}(t,k)$ |
| 2 | 0.01 | 0.005 | 32 | $0.3 \cdot 10^{-6}$ | $0.6 \cdot 10^{-6}$ |
| 4 | 0.1 | 0.14 | 64 | 0.01 | 0.02 |
| 8 | 0.5 | 0.53 | 128 | 0.6 | 0.67 |
| 16 | 0.9 | 0.92 | 256 | 1 | 0.99 |

Из табл. 1 и свойств 1 и 2 понятно, что при $t \le k$ вероятность успешной атаки $\approx 0$ для $\forall k$. Это согласуется с теоремой из [11], гласящей, что данная ПГК защищена против АИОТ при $t \le k$. А также это показывает, что утверждение из [11] о том, что для раскрытия ключа с вероятностью $\approx 1$ нужно $t = O(1)$ пар, не вполне корректно отражает степень защищенности [11].

Теперь более подробно исследуем, при каких $t$ мы имеем $\eta = \Omega(t,k) \approx 1$. Ясно, что из (5) можно точно определить такое $t$, чтоб при заданном $k$ выполнялось $\eta = \beta$ для $\forall \beta \in [0,1]$. Однако зависимость (5) достаточно сложна и в силу недостатка места точную аналитическую формулу для $t$ здесь выводить не будем. Приведем лишь численные данные, которые покажут характер зависимости $t$ от $k$ и $\beta$ для диапазона $2 \le k \le 1024$, представляющего интерес для практики.

Таблица 2

**Значения $t$ и $\tilde{t}$ для [11] при $\eta \approx 0{,}95$**

| $k$ | $t$ | $\tilde{t}$ |
|---|---|---|
| 16 | 95 | 93 |
| 32 | 210 | 207 |
| 64 | 460 | 455 |
| 128 | 1006 | 1004 |
| 256 | 2185 | 2186 |
| 512 | 4720 | 4715 |
| 1024 | 10145 | 10147 |

В табл. 2 $\tilde{t}$ – экспериментальная оценка необходимого количества пар для того, чтобы выполнялось $\eta \approx 0.95$. Из табл. 2 видно, что $\eta > 0{,}95$ (т.е. $\approx 1$) для $2 \le k \le 1024$ при условии, что $t > \alpha(k) \cdot k$, где $\alpha(k)$ – монотонно возрастающая функция, такая что $\alpha \in [5,10]$. Из анализа численных данных становится ясно, что $\alpha(k) \approx O(\log k)$.

*Замечание.* Строгое обоснование того, что $\alpha(k) = O(\log k)$ будет приведено в расширенной версии данной статьи.

Напомним, что в [11] утверждалось, что рассмотренная ПГК защищена против АИОТ при $t \le k \cdot \ln poly(\lambda)$, где $\lambda$ – битовая длина $f_i$ и $poly(\lambda)$ – $\forall$ полином. Однако как мы увидели, успех АИОТ [17] не зависит от $\lambda$ хоть сколько-нибудь существенным образом. Вследствие этого получается, что в [11] происходит переоценка криптостойкости криптосистемы против АИОТ. Например, в

[11] было указано, что если выбрать $poly(\lambda)$ полиномом 10-й степени, то при $\lambda = 1024$ и $k = 16$ ПГК защищена, если $t \le 1109$. Однако мы увидели, что $\eta > 0{,}95$ при $t > 95$, и ПГК [11] нестойка уже при $t > 95$.

*Замечание.* Если говорить совсем строго, то успех АИОТ [17] зависит от $\lambda$, но эта зависимость носит не такой характер, как указано в [11]. Принимая во внимание рассуждения из раздела 5, можно получить, что вероятность успеха АИОТ [17] $\eta = \theta \cdot \Omega(k,t)$, где $\theta = \prod_{i=1}^{k} \frac{(p_i - 1)\cdot(q_i - 1)}{p_i \cdot q_i} > \left(1 - \frac{1}{2^{\lambda/2-1}}\right)^{2\cdot k}$. Однако при $\lambda \ge 1024$ и $2 \le k \le 1024$ последнее число настолько близко к 1, что можно полагать $\theta = 1$ и не принимать во внимание зависимость $\eta$ от $\lambda$.

АИОТ из [11] состоит в решении СЛАУ размера $(4 \cdot t) \times t$ над кольцом $\mathbb{Z}_n$, где $n$ – произведение $2 \cdot k$ простых сомножителей. Общая вычислительная сложность атаки не превышает $O(t^2 \cdot k)$ элементарных операций в $\mathbb{Z}_n$.

Напоследок заметим, что в данном случае работа идет с ПГК и даже если $t$ меньше необходимого для успеха количества, можно попробовать произвести из пар $(m_j, \mathbf{C}_j),\ j = \overline{1,t}$ дополнительные пары за счет гомоморфных свойств. А именно, используя мультипликативный гомоморфизм можно добавить к СЛАУ (1) новые линейные уравнения, составленные по $([m_{j_1} \cdot \ldots \cdot m_{j_\beta}]_n, \left[\mathbf{C}_{j_1} \cdot \ldots \cdot \mathbf{C}_{j_\beta}\right]_n) \cdot$ Однако нетрудно видеть, что в соответствии со структурой $\mathbf{C}_j$ величины $\vartheta(k,t)$ и $\Omega(k,t)$ не изменятся от добавления этих уравнений. Поэтому гомоморфные свойства не делают криптосистему более уязвимой к АОИТ [17].

**7. Соотношение криптостойкости и эффективности [11].** Эффективность ПГК обычно в большой степени оценивается по времени, необходимому на умножение двух шифртекстов.

Значение $T_{mult} = 30$ с, получаемое при $k = 1024$, хоть и не является чересчур обременительным в сравнении с некоторыми вариантами ПГК в стиле Джентри [2], все же может значительно замедлить гомоморфное вычисление полинома большой степени.

Таблица 3

**Время $T_{mult}$ умножения двух шифртекстов [11] при $\lambda = 1024$**

| $k$ | $T_{mult}$ |
|---|---|
| 16 | 108 мс |
| 64 | 500 мс |
| 512 | 8 с |
| 1024 | 30 с |

Для получения скорости, пригодной для практики, исходя из табл. 3, желательно выбирать $k \le 64$. При $k = 64$ в соответствии с табл. 2 $\eta \approx 1$ выполняется для $t$ >460. И тогда ПГК [11] можно задействовать достаточно успешно для защищенных вычислений, если приложение таково, что есть гарантия, что у противника точно не окажется в руках более 400 пар.

**8. Модификация ПГК на основе факторизации из [12, 13] и её анализ.** В работах [12, 13] была представлена модификация ПГК [11]. Её основные отличия от [11] состоят в следующем: 1) $n=\prod_{i=1}^{k} f_i$ , $f_i = p_i \cdot q_i$, $p_i, q_i$ – нечетные числа такие, что НОД( $f_i$, $f_j$ ) = 1 для $\forall i \neq j$ ; 2) при составлении $\mathbf{D} \in \mathbb{Z}_n^{4\times 4}$ в процедуре шифрования из [11] $(a_i, b_i, c_i), i=\overline{1,k}$ генерируются так: $r \xleftarrow{\$} \mathbb{Z}_n$ , а затем для $\forall i=\overline{1,k}$ $(a_i, b_i, c_i)$ выбирают по распределению:

$$\Pr\left[(a_i, b_i, c_i)=(x,r,r)\right]=$$

$$\Pr\left[(a_i, b_i, c_i)=(r,x,r)\right]=\Pr\left[(a_i, b_i, c_i)=(r,r,x)\right]=1/3.$$

Первая модификация на первый взгляд кажется нецелесообразной, так как в [12, 13] утверждается, что сложность взлома основана на трудности факторизации больших чисел. Однако на самом деле $f_i$ и $n$ теперь не обязательно трудно факторизовать и решить характеристическое уравнение $char(x)$ для $\mathbf{C} \in \mathbb{Z}_n^{4\times 4}$, одним из корней которого является $m \in \mathbb{Z}_n$, также нетрудно. Поэтому единственная возможность обеспечения защиты от взлома только по шифртекстам состоит в том, что $n$ должно иметь большое число $\beta$ взаимно простых сомножителей. Тогда $char(x)$ несмотря на то, что оно лишь 4-й степени, имеет по КТО $2^{\beta}$ решений, среди которых противнику придется выбирать наиболее вероятного кандидата на роль открытого текста. Ясно, что если хотя бы $\beta > 100$, то перебор становится значительным. Однако описанный сценарий в [12, 13] не упоминался, и он требует проведения дополнительного анализа.

Вторая модификация затрагивает формулы (3-5). Заменяя в рассуждениях выше значения вероятностей $1-\frac{1}{k+1}, \frac{1}{2\cdot(k+1)}, \frac{1}{2\cdot(k+1)}$ на $\frac{1}{3}, \frac{1}{3}, \frac{1}{3}$, мы получим выражение $\vartheta = 1-\frac{1}{3^{t-1}}$ и соответственно:

$$\Omega(t,k)=\Pr\left[\mathrm{Lin}(\mathbf{v}_1)=V\right]=\vartheta^k=\left[1-\frac{1}{3^{t-1}}\right]^k. \qquad (6)$$

Таблица 4

**Значения $\Omega(t,k)$ для [12, 13] и [11] при $k=32$**

| $t$ | $\Omega(t,k)$ для [8,9] | $\Omega(t,k)$ для [7] |
|---|---|---|
| 2 | $0{,}2 \cdot 10^{-5}$ | $0{,}5 \cdot 10^{-39}$ |
| 4 | 0,3 | $0{,}11 \cdot 10^{-29}$ |
| 8 | 0,98 | $0{,}7 \cdot 10^{-21}$ |
| 16 | 1 | $0{,}74 \cdot 10^{-13}$ |

Отметим, что здесь $\Omega(t,k)$ так же как и для [11] обладает свойством 1). Хотя ясно, что $\Omega(t,k)$ для [12, 13] быстрее $\to 1$ при $t \to \infty$ для $\forall k \geq 0$ (фиксированного), так как $\frac{1}{3^{t-1}} \to 0$ гораздо быстрее, чем $\left(\frac{k}{k+1}\right)^t + 2\cdot\left(\frac{1}{2\cdot(k+1)}\right)^t$ в фор-

муле (5). А свойство 2) для [12, 13] заменяется на следующее: если в (6) положить $t = k$, то получим $\Omega(t,k) \approx \left(1 - \frac{1}{3^{k-1}}\right)^k \xrightarrow{k\to\infty} 1$.

Из свойств $\Omega(t,k)$ для [12, 13] и табл. 4 хорошо видно, что ПГК [12, 13] гораздо менее защищенная, чем [11], т.к. количество пар, необходимых для взлома [12, 13], с вероятностью $\approx 1$ $\leq k$. И таким образом вторая модификация в [12, 13] смысла не имеет.

Вычислительная сложность атаки здесь также составляет $O(t^2 \cdot \log n)$. Для решения СЛАУ необходимо привлекать методы, основанные на лемме Гензеля [22].

**Заключение.** В работе подробно проанализирована атака по известным открытым текстам из [17], применительно к ПГК [11] и [12, 13]. Основные выводы, полученные в ходе анализа, следующие:

- АИОТ из [17] находит ключ для ПГК [11] по $t$ парам (открытый текст, шифртекст) с вероятностью $\approx 1$ при $t > \alpha(k) \cdot k$ и $2 \leq k \leq 1024$, где $\alpha(k)$ – монотонно возрастает и $\alpha(k) \in [5,10]$, $k$ – параметр ПГК, равный числу RSA-модулей, входящих в состав модуля $n$, по которому в [11] предполагается производить все вычисления.
- Учитывая данные о производительности ПГК [11], для получения практичной криптосхемы нужно полагать $k \leq 64$, где $k = 64$ является наилучшим вариантом с точки зрения криптостойкости. При $k = 64$ ПГК для успешного взлома нужно $t > 400$ пар.
- Криптосистема [12, 13] не защищена против АИОТ [17] при количестве пар $t$ таком, что $t \in [\nu, k]$, где $\nu \in (2, k)$.

Оценивая ПГК [11] в общем, можно сказать, что на данный момент она является одной из наиболее защищенных ПГК на основе факторизации против АИОТ, так как другие ПГК на задаче факторизации [7–10] гораздо менее защищены. В частности, ПГК из [7–9] не стойки к АИОТ даже при наличии одной пары [15, 16].

Также ПГК [11] обладает неплохой производительностью. Поэтому её можно использовать в приложениях, в которых есть гарантия, что противник не может перехватить более нескольких сотен пар (открытый текст, шифртекст).

Однако вопрос о построении ПГК на задаче факторизации чисел, которая являлась бы эффективной и вместе с тем строго криптостойкой против АИОТ, попрежнему остается открытым.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Armbrust M. et al.* A view of cloud computing // Communications of the ACM. – 2010. – Vol. 53, №. 4. – P. 50-58.
2. *Guellier A.* Can Homomorphic Cryptography ensure Privacy?: diss. – Inria; IRISA; Supélec Rennes, équipe Cidre; Université de Rennes 1, 2014.
3. *Gentry C.* A fully homomorphic encryption scheme: diss. – Stanford University, 2009.
4. *Burtyka P., Makarevich O.* Symmetric Fully Homomorphic Encryption Using Decidable Matrix Equations // Proceedings of the 7th International Conference on Security of Information and Networks. – ACM, 2014. – P. 186.
5. *Nuida K.* A Simple Framework for Noise-Free Construction of Fully Homomorphic Encryption from a Special Class of Non-Commutative Groups // IACR Cryptology ePrint Archive. – 2014. – Vol. 2014. – P. 97.
6. Tamayo-Rios M. Method for fully homomorphic encryption using multivariate cryptography: заяв. пат. 13/915,500 США. – 2013.

7. *Rostovtsev A., Bogdanov A., Mikhaylov M.* Secure evaluation of polynomial using privacy ring homomorphisms // IACR Cryptology ePrint Archive. – 2011. – Vol. 2011. – P. 24.
8. *Zhirov A., Zhirova O., Krendelev S. F.* Practical fully homomorphic encryption over polynomial quotient rings // Internet Security (WorldCIS), 2013 World Congress on. – IEEE, 2013. – P. 70-75.
9. *Kipnis A., Hibshoosh E.* Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification // IACR Cryptology ePrint Archive. – 2012. – №. 637.
10. *Chan A.C.F.* Symmetric-key homomorphic encryption for encrypted data processing // Communications, 2009. ICC'09. IEEE International Conference on. – IEEE, 2009. – P. 1-5.
11. *Xiao L., Bastani O., Yen I. L.* An Efficient Homomorphic Encryption Protocol for Multi-User Systems // IACR Cryptology ePrint Archive. – 2012. – № 193.
12. *Gupta C. P., Sharma I.* Department of Computer Sciences and Engineering Rajasthan Technical University, Kota, India // Network of the Future (NOF), 2013 Fourth International Conference on the. – IEEE, 2013. – P. 1-4.
13. *Gupta C.P.* Fully Homomorphic Encryption Scheme with Symmetric Keys: diss. – Department of Computer Science & Engineering University College of Engineering, Rajasthan Technical University, Kota, 2013.
14. *Rivest R. L., Kaliski Jr B.* RSA problem // Encyclopedia of cryptography and security. – Springer US, 2011. – P. 1065-1069.
15. *Трепачева А.В.* Криптоанализ шифров, основанных на гомоморфизмах полиномиальных колец // Известия ЮФУ. Технические науки. – 2014. – № 8 (157). – С. 96-107.
16. *Trepacheva A., Babenko L.* Known plaintexts attack on polynomial based homomorphic encryption // Proceedings of the 7th International Conference on Security of Information and Networks. – ACM, 2014. – P. 157.
17. *Vizár D., Vaudenay S.* Analysis of Chosen Symmetric Homomorphic Schemes // Central European Crypto Conference. – 2014. – №. EPFL-CONF-198992.
18. *Tsaban B., Lifshitz N.* Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme // Journal of Mathematical Cryptology. – 2014.
19. *Ленг С.* Алгебра: Пер. с англ. / Под ред. А.И. Кострикина. – М.: Мир, 1968. – 564 с.
20. *Виноградов И.М.* Основы теории чисел. – М.: Наука, 1972. – 510 с.
21. *Klivans A.* Factoring polynomials modulo composites. – CARNEGIE-MELLON UNIV PITTSBURGH PA DEPT OF COMPUTER SCIENCE, 1997. – №. CMU-CS-97-136.
22. *Arvind V., Vijayaraghavan T. C.* The complexity of solving linear equations over a finite ring // STACS 2005. – Springer Berlin Heidelberg, 2005. – P. 472-484.

REFERENCES

1. *Armbrust M. et al.* A view of cloud computing, *Communications of the ACM*, 2010, Vol. 53, No. 4, pp. 50-58.
2. *Guellier A.* Can Homomorphic Cryptography ensure Privacy?: diss. Inria; IRISA; Supélec Rennes, équipe Cidre; Université de Rennes 1, 2014.
3. *Gentry C.* A fully homomorphic encryption scheme: diss. Stanford University, 2009.
4. *Burtyka P., Makarevich O.* Symmetric Fully Homomorphic Encryption Using Decidable Matrix Equations, *Proceedings of the 7th International Conference on Security of Information and Networks*. ACM, 2014, pp. 186.
5. *Nuida K.* A Simple Framework for Noise-Free Construction of Fully Homomorphic Encryption from a Special Class of Non-Commutative Group, *IACR Cryptology ePrint Archive*, 2014, Vol. 2014, pp. 97.
6. *Tamayo-Rios M.* Method for fully homomorphic encryption using multivariate cryptography: application Pat. 13/915,500 USA, 2013.
7. *Rostovtsev A., Bogdanov A., Mikhaylov M.* Secure evaluation of polynomial using privacy ring homomorphisms, *IACR Cryptology ePrint Archive*, 2011, Vol. 2011, pp. 24.
8. *Zhirov A., Zhirova O., Krendelev S. F.* Practical fully homomorphic encryption over polynomial quotient rings, *Internet Security (WorldCIS), 2013 World Congress on*. IEEE, 2013, pp. 70-75.

9. *Kipnis A., Hibshoosh E*. Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification, *IACR Cryptology ePrint Archive*, 2012, No. 637.
10. *Chan A.C.F*. Symmetric-key homomorphic encryption for encrypted data processing, *Communications, 2009. ICC'09. IEEE International Conference on*. IEEE, 2009, pp. 1-5.
11. *Xiao L., Bastani O., Yen I. L*. An Efficient Homomorphic Encryption Protocol for Multi-User Systems, *IACR Cryptology ePrint Archive*, 2012, No. 193.
12. *Gupta C.P., Sharma I.* Department of Computer Sciences and Engineering Rajasthan Technical University, Kota, India, *Network of the Future (NOF), 2013 Fourth International Conference on the*. IEEE, 2013, pp. 1-4.
13. *Gupta C.P*. Fully Homomorphic Encryption Scheme with Symmetric Keys: diss. – Department of Computer Science & Engineering University College of Engineering, Rajasthan Technical University, Kota, 2013.
14. *Rivest R. L., Kaliski Jr B*. RSA problem, *Encyclopedia of cryptography and security*. Springer US, 2011, pp. 1065-1069.
15. *Trepacheva A.V.* Kriptoanaliz shifrov, osnovannykh na gomomorfizmakh polinomial'nykh kolets [Crypyoanalysis of cryptosytems based on polynomial ring homomorhisms], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8 (157), pp. 96-107.
16. *Trepacheva A., Babenko L.* Known plaintexts attack on polynomial based homomorphic encryption, *Proceedings of the 7th International Conference on Security of Information and Networks*. ACM, 2014, pp. 157.
17. *Vizár D., Vaudenay S.* Analysis of Chosen Symmetric Homomorphic Schemes, *Central European Crypto Conference*, 2014, No. EPFL-CONF-198992.
18. *Tsaban B., Lifshitz N*. Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme, *Journal of Mathematical Cryptology*, 2014.
19. *Leng S.* Algebra: Translation from English, Under ed. A.I. Kostrikina. Moscow: Mir, 1968, 564 p.
20. *Vinogradov I.M.* Osnovy teorii chisel [Fundamentals of the theory of numbers]. Moscow: Nauka, 1972, 510 p.
21. *Klivans A*. Factoring polynomials modulo composites. CARNEGIE-MELLON UNIV PITTSBURGH PA DEPT OF COMPUTER SCIENCE, 1997. No. CMU-CS-97-136.
22. *Arvind V., Vijayaraghavan T. C.* The complexity of solving linear equations over a finite ring, *STACS 2005*. Springer Berlin Heidelberg, 2005, pp. 472-484.

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

**Трепачева Алина Викторовна** – Южный федеральный университет; e-mail: alina1989malina@ya.ru; 347928, г. Таганрог, ул. Чехова, 2, корпус "И"; тел.: +79085196604; кафедра безопасности информационных технологий; аспирантка.

**Trepacheva Alina Viktorovna** – Southern Federal University; e-mail: alina1989malina@ya.ru; Block “I”, 2 Chekhov street, Taganrog, 347928, Russia; phone: +79085196604; the department of information technologies security; postgraduate student.