УДК 003.26.09 **DOI** 10.15622/sp.18.1.230-262

Л. К. Бабенко, А. В. Трепачева

О НЕСТОЙКОСТИ ДВУХ СИММЕТРИЧНЫХ ГОМОМОРФНЫХ КРИПТОСИСТЕМ, ОСНОВАННЫХ НА СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Бабенко Л.К., Трепачева А.В. **О нестойкости двух симметричных гомоморфных криптосистем, основанных на системе остаточных классов.**

Аннотация. Одной из наиболее актуальных задач, связанных с защитой облачных вычислений, является анализ криптостойкости гомоморфных шифров. Данная статья посвящена изучению вопроса о защищенности двух недавно предложенных гомоморфных криптосистем, которые, в связи с их высокой вычислительной эффективностью, могут быть использованы для шифрования данных на облачных серверах. Обе криптосистемы основаны на системах остаточных классов, что позволяет рассмотреть их с единых позиций. Именно использование систем остаточных классов делает применение этих криптосистем в реальных приложениях заманчивым с точки зрения эффективности по сравнению с другими гомоморфными шифрами, так как появляется возможность легко распараллелить вычисления. Однако их криптостойкость не была в достаточной мере изучена в литературе и нуждается в анализе.

Отметим, что ранее предшественниками была рассмотрена криптосистема похожая на один из шифров, криптостойкость которого исследуется. Была предложена идея адаптивной атаки по выбранным открытым текстам на эту конструкцию и дана оценка необходимого для раскрытия ключа количества пар «открытый текст, шифртекст». Здесь проводится анализ этой атаки и показываем, что иногда она может работать некорректно. Также описывается более общий алгоритм атаки с известными открытыми текстами. Приводятся теоретические оценки вероятности успешного раскрытия секретного ключа с его помощью и практические оценки этой вероятности, полученные в ходе вычислительного эксперимента.

Защищенность второй криптосистемы не была исследована ранее в литературе. Изучена её стойкость к атаке с известными открытыми текстами. Проанализирована зависимость необходимого для взлома количества пар «открытый текст, шифртекст» от параметров криптосистемы и даны рекомендации, которые могут помочь улучшить криптостойкость.

Итог проведенного анализа заключается в том, что обе криптосистемы являются уязвимыми к атаке с известными открытыми текстами. Поэтому использовать их для шифрования конфиденциальных данных может быть небезопасно.

Основным алгоритмом, используемым в предложенных атаках на криптосистемы, является алгоритм поиска наибольшего общего делителя. Как следствие, время, необходимое для реализации атак, является полиномиальным от размера входных данных.

Ключевые слова: гомоморфное шифрование, облачные вычисления, криптоанализ, атака с известными открытыми текстами, система остаточных классов.

1. Введение. Гомоморфное шифрование (ГШ) позволяет вычислять функции над зашифрованными данными без знания ключа расшифрования. Владелец ключа может извлечь результат вычислений над исходными данными из результата вычислений над соответствующими зашифрованными данными. Это делает ГШ перспективным решением для защищенного делегирования облачному серверу вычислений над

конфиденциальными данными клиента. Перед загрузкой данных на сервер клиент должен зашифровать их с помощью ГШ. Затем сервер проведет вычисление над зашифрованными данными и вернет зашифрованный результат клиенту.

Понятие ГШ было введено в 1978 году [1]. После этого криптографы предложили и проанализировали множество различных гомоморфных криптосистем [2-5], позволяющих выполнять одну арифметическую операцию (сложение или умножение). Криптосистема RSA [5] — наиболее известный пример: она позволяет вычислять умножение гомоморфно.

В 2009 году исследователь из IBM Крейг Джентри разработал первую схему *полностью гомоморфного шифрования (ПГШ)* на основе идеальных решеток [6]. Криптосистема Джентри позволяет выполнять *произвольные* вычисления над зашифрованными данными. Отправной точкой при построении криптосистемы Джентри является ГШ, разрешающее лишь ограниченное число гомоморфных умножений и сложений. Ограничение вызвано «шумом» в шифртекстах — некоторой величиной, встраиваемой в шифртекст в процессе шифрования. «Шум» необходим для обеспечения криптостойкости. Но после каждой гомоморфной операции его значение возрастает. В какой-то момент это приводит к невозможности корректно расшифровать. Поэтому второй шаг в конструкции Джентри — обновить шифртексты так, чтобы уменьшить «шум». Процедура обновления шифртекстов основана на вычислении функции расшифрования, но не непосредственно над битами шифртекста и секретного ключа, а над шифртекстами этих битов гомоморфно. Это так называемый метод *«самокоррекции»* (англ. *«bootstrapping»*).

В последующих работах был представлен широкий спектр схем ПГШ. Все эти криптосистемы можно разделить на две категории.

Первая категория содержит схемы ПГШ с открытым ключом, основанные на внесении «шума» [7-13]. Эти криптосистемы базируются на методике Джентри. Авторы пытаются улучшить производительность оригинальной криптосистемы [6]. Исходная криптосистема Джентри доказуемо криптостойка к атаке по выбранным открытым текстам, но практически нереализуема. Однако, несмотря на все усилия, криптосистемы ПГШ, разработанные на основе идей Джентри, по-прежнему криптостойки, но непрактичны [14].

Ко *второй категории* можно отнести симметричные криптосистемы ПГШ, не использующие «шум» и метод «самокоррекции». Здесь можно найти ПГШ, основанное на разных математических объектах. Кипнис (Kipnis), Сяо (Xiao) и другие [15-17] предложили ПГШ на основе матриц. Работы Ягисавы (Yagisawa) [18, 19] представляют ПГШ, использующее

октонионную алгебру. Очень популярны гомоморфные криптосистемы на основе полиномов [20-25]. И, наконец, существуют криптосистемы на системах остаточных классов (СОК) [26-28].

Большинство криптосистем второй категории устроено более просто и имеет бОльшую вычислительную эффективность, чем криптосистемы, использующие метод Джентри. Для многих из них стойкость обосновывается с помощью того факта, что задача факторизации чисел сложна. Но эти обоснования не являются строгими доказательствами, и зачастую криптосистемы оказываются уязвимыми. В частности, работы [29-32] описывают эффективные атаки по известным открытым текстам (АИО) на матричные схемы ПГШ. В [33-38] можно найти АИО на ПГШ на основе полиномов. Криптосистемы, базирующиеся на октонионах, также уязвимы к АИО [39-41]. И, наконец, есть попытки провести атаки с использованием только шифртекстов (АТШ) [42-44]. Итак, вопрос о существовании *эффективного и криптостойкого* ПГШ на данный момент по-прежнему является открытым.

2. Постановка задачи и основные результаты. Основная цель настоящей работы – изучить криптостойкость против АИО двух недавно предложенных симметричных схем ПГШ на основе систем остаточных классов (СОК) — криптосистемы Вишневского и Князева [27] и криптосистемы Бабенко, Кучерова и Червякова [28]. Напомним, что АИО предполагает, что криптоаналитик перехватил s пар «открытый текст, шифртекст», созданных на одном ключе, и его задача — восстановить секретный ключ.

Криптосистема Вишневского и Князева была построена для решения систем линейных уравнений в недоверенной вычислительной среде. А криптосистема Бабенко, Кучерова и Червякова предназначена для защиты данных в облаках. Эти две криптосистемы очень похожи, поэтому схема атаки для них является общей. Отличие заключается в том, что в [27] базовый объект — целые числа, а в [28] — полиномы. Это влияет на метод оценки вероятности успеха атаки.

Обе криптосистемы не были проанализированы ранее в литературе на предмет стойкости к АИО, поэтому в данной работе мы восполняем этот пробел. Очень важно понять уровень стойкости криптосистемы перед тем, как начать использовать ее в реальных приложениях.

Описанная здесь атака на криптосистемы [27, 28] основана на том же подходе, что и АИО из работ [33-38]. Суть его заключается в том, что криптоаналитик проводит преобразования над перехваченными данными и получает некоторые величины (числа или полиномы), которые в качестве одного из сомножителей содержат секретный ключ или некоторую его

часть. Тогда основным инструментом поиска ключа становится алгоритм вычисления наибольшего общего делителя (НОД).

Отметим, что в работе [45] был рассмотрен вопрос о стойкости к адаптивной атаке по выбранным открытым текстам (ААВО) криптосистемы похожей на конструкцию [27]. Данная атака также подразумевает, что криптоаналитик имеет s пар «открытый текст, шифртекст». Эти пары он получает за счет того, что у него есть доступ к шифрующему устройству, как к черному ящику. Поэтому он может получить пары для открытых текстов, выбранных по своему усмотрению. Адаптивность атаки означает, что криптоаналитик имеет возможность получать новые пары непосредственно в ходе атаки.

В [45] была представлена идея того, как можно осуществить ААВО. Доказана теорема о том, что если $s = O(\tau)$, где τ — количество модулей в используемой для шифрования СОК, то секретный ключ может быть восстановлен однозначно. Однако представленный авторами результат не исключает того, что ключ можно раскрыть и при меньшем s.

В данной работе мы проанализировали ААВО, описанную в [45], и пришли к заключению, что в общем случае она не всегда будет гарантированно выдавать ключ при $s = O(\tau)$. Данное событие может произойти лишь с вероятностью < 1. Мы приведем пример, демонстрирующий это. Для криптосистемы Вишневского и Князева [27], которую мы изучаем здесь, данный подход к проведению ААВО будет работать полностью корректно и при $s = O(\tau)$ ключ действительно будет всегда раскрыт однозначно.

В рамках ААВО криптоаналитик находится в более сильной позиции, чем в случае АИО. Поэтому факт уязвимости к ААВО не умаляет важности исследования стойкости к АИО. Здесь наш основной результат состоит в том, что при $s \approx O(\log(\tau))$ криптоаналитик может раскрыть секретный ключ в рамках АИО на криптосистему [27], однако не гарантированно, а с вероятностью ≈ 1. Этот результат подтвержден большим количеством компьютерных экспериментов, хотя и нуждается в дополнительном более строгом теоретическом обосновании. Похожий результат получен и для криптосистемы [28].

3. Обозначения. Ниже мы используем следующие обозначения: $\mathbb{Z}_n$ — кольцо вычетов по модулю n, $n \in \mathbb{Z}, n > 1$; $\mathbb{Z}_n[x]$ — кольцо полиномов с коэффициентами из $\mathbb{Z}_n$; $\mathbb{Z}_{n,d}[x]$ — множество полиномов над $\mathbb{Z}_n$ степени меньше d; $\mathsf{M}_N(\mathbb{Z}_n)$ — кольцо квадратных $N \times N$-матриц над $\mathbb{Z}_n$. Для $a \in \mathbb{Z}$ его остаток от деления на n обозначается через $[a]_n \in \mathbb{Z}_n$, а остаток от деления полинома $f(x)$ на $g(x)$ соответственно — $[f(x)]_{g(x)}$. Строчными буквами полужирного шрифта (например, $\mathbf{v}$) будем обозначать

векторы $\mathbf{v} = (v_1, ..., v_N)$, а прописными буквами жирным шрифтом (например, $\mathbf{A}$) — матрицы $\mathbf{A} = \{a_{i,j}\}_{i=\overline{1,N}, j=\overline{1,N}}$. Для $f(x) \in \mathbb{Z}_n[x]$ обозначим через f_i его i-й коэффициент. Для $\mathbf{A} \in \mathsf{M}_N(\mathbb{Z})$ обозначим через $[\mathbf{A}]_n \in \mathsf{M}_N(\mathbb{Z}_n)$ матрицу, имеющую элементы $[a_{i,j}]_n$. Аналогичные обозначения используются для векторов и полиномов.

Через $Pr\{A\}$ обозначается вероятность события A; $x \xleftarrow{\$} R$ обозначает случайный элемент, полученный по равномерному распределению на множестве R; $x \xleftarrow{\mathcal{D}} R$ — элемент, сгенерированный по распределению вероятностей $\mathcal{D}$ на R; $f(x) \xleftarrow{\$} \mathbb{Z}_n[x]$ означает, что $f_i \xleftarrow{\$} \mathbb{Z}_n, i = \overline{0, \deg(f) - 1}$, $f_{\deg(f)} \xleftarrow{\$} \mathbb{Z}_n \setminus \{0\}$.

Для $a, b \in \mathbb{Z}$ запись $a|b$ означает, что a делит b, GCD — наибольший общий делитель (от англ. greatest common divisor).

4. Сведения из теории чисел. В этом разделе собраны все необходимые известные утверждения и теоремы для представления криптосистем в рамках исследования и криптоанализа. В первую очередь напомним китайскую теорему об остатках (КТО).

Теорема 1. ([46]) Пусть $n = \prod_{i=1}^{\tau} n_i$, где $GCD(n_i, n_j) = 1$ при $i \neq j$. Существует изоморфизм:

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_\tau}.$$

Для вычисления $a \in \mathbb{Z}_n$, соответствующего вектору $([a]_{n_1}, ..., [a]_{n_\tau}) \in \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_\tau}$, используется формула:

$$a = CRT_{n_1,...,n_\tau}([a]_{n_1}, ..., [a]_{n_\tau}) = \sum_{i=1}^{\tau} [a]_{n_i} \cdot S_i \cdot S_i^{-1}, \qquad (1)$$

где $S_i = \frac{n}{n_i}, S_i^{-1} \equiv \frac{1}{S_i} (\mathrm{mod} n_i)$.

Теорема 2. ([47]) Пусть $z_i \xleftarrow{\$} \{1, 2, ..., n\}, i = \overline{1, s}, n \in \mathbb{N}, s > 1$ — случайные числа, полученные независимо по равномерному распределению. Для $s \geqslant 3$ справедливо равенство:

$$Pr\{GCD(z_1, ..., z_s) = 1\} = \frac{1}{\zeta(s)} + O\left(\frac{1}{n}\right),$$

а для $s = 2$ справедливо:

$$Pr\{GCD(z_1, z_2) = 1\} = \frac{1}{\zeta(2)} + O\left(\frac{\log(n)}{n}\right),$$

где $\zeta(s)$ – дзета-функция Римана.

Значения функции $\frac{1}{\zeta(s)}$ проиллюстрированы в таблице 1 с точностью $\varepsilon = 10^{-4}$. Видно, что при $s \geqslant 5$ вероятность взаимной простоты s случайных чисел, выбранных из диапазона $\{1, 2, ..., n\}$, равна ≈ 1.

Таблица 1. Значения $\frac{1}{\zeta(s)}$

s	$1/\zeta(s)$
2	0.6079
3	0.8319
4	0.9259
5	0.9643
6	0.9829
7	0.9917
8	0.9959
9	0.9979

Теорема 3. [48] Пусть даны полиномы $f_i(x) \xleftarrow{\$} \mathbb{Z}_{q,d}[x], i = \overline{1, s}$, где q — простое число. Тогда справедливо:

$$Pr\{GCD(f_1(x), ..., f_s(x)) = 1\} = 1 - \frac{1}{q^{s-1}} + \frac{q-1}{q^{s \cdot d}}.$$

Ясно, что с ростом q, s и d вероятность, указанная в теореме 3, будет стремиться к 1.

5. Гомоморфное шифрование. Гомоморфное шифрование позволяет проводить вычисления над зашифрованными данными без знания секретного ключа. В ходе такого вычисления производится зашифрованный результат. Его расшифрование дает результат обработки соответствующих открытых текстов.

Часто симметричные полностью гомоморфные криптосистемы обладают следующим свойством: пространства открытых текстов и шифртекстов являются *кольцами*. Для произвольных открытых текстов m_1, m_2 выполняются равенства:

$$\begin{aligned} Dec_{sk}(Enc_{sk}(m_1) + Enc_{sk}(m_2)) &= m_1 \oplus m_2, \\ Dec_{sk}(Enc_{sk}(m_1) \cdot Enc_{sk}(m_2)) &= m_1 \odot m_2, \end{aligned} \tag{2}$$

где $\oplus, \odot$ — операции в кольце открытых текстов, $+, \cdot$ — операции в кольце шифртекстов, Enc, Dec — функции зашифрования и расшифрования, параметризованные ключом sk.

6. Описание анализируемых гомоморфных криптосистем. *ГШ Вишневского и Князева ([27]).* Криптосистема Вишневского и Князева построена с использованием числовой СОК. Она была предложена для решения специальной задачи. Авторы искали способ найти корни системы линейных уравнений $\mathbf{A} \cdot \vec{x} = \mathbf{b}$ в недоверенной вычислительной среде, где

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,N} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{N,2} & \cdots & a_{N,N} \end{pmatrix} \in \mathsf{M}_N(\mathbb{Z}), \mathbf{b} \in \mathbb{Z}^N = \begin{pmatrix} b_1 \\ \cdots \\ b_N \end{pmatrix}.$$

Входные данные $\mathbf{A}$, $\mathbf{b}$ и полученные корни не должны раскрываться недоверенному серверу, выполняющему вычисления.

Алгоритмы шифрования и расшифрования основаны на теореме 1. Секретный ключ sk — вектор случайных и независимо выбранных простых чисел $(k_1, ..., k_\tau) \in \mathbb{N}^\tau$, таких что $k_i > 1, i = \overline{1,\tau}$, $k_i \neq k_j$ при $i \neq j$. Пространство открытых текстов $\mathcal{M}$ — множество $\mathcal{R}_t = \{0, ..., t-1\} \subset \mathbb{Z}$, где $t = \prod_{i=1}^{\tau} k_i$, пространство шифртекстов $\mathcal{C}$ — это подмножество $\mathbb{Z}^\tau$.

Алгоритм зашифрования $Enc(m \in \mathcal{R}_t, sk)$:
– вычислить $\mathbf{c} = ([m]_{k_1}, ..., [m]_{k_\tau}) \in \mathbb{Z}^\tau$.

Алгоритм расшифрования $Dec(\mathbf{c} = (c_1, ..., c_\tau), sk)$:
– вычислить $m = CRT_{k_1,...,k_\tau}(c_1, ..., c_\tau)$.

Умножение и сложение шифртекстов выполняется покоэффициентно. По теореме 1 такое шифрование обладает мультипликативным и аддитивным гомоморфизмами.

Рассмотрим, как это шифрование применяется для безопасного решения уравнения $\mathbf{A} \cdot \vec{x} = \mathbf{b}$ на облачном сервере. Числа k_i выбираются так, что:

$$k_i < k_{i-1},$$

$$\prod_{i=1}^{\tau-2} k_i \leqslant \max_{i,j}\{a_{i,j}\} < \prod_{i=1}^{\tau-1} k_i < \prod_{i=1}^{\tau} k_i.$$

Чтобы зашифровать $\mathbf{A}$ и $\mathbf{b}$, клиент вычисляет набор матриц и векторов $\mathbf{A}_i = [\mathbf{A}]_{k_i}, \mathbf{b}_i = [\mathbf{b}]_{k_i}, i = \overline{1,\tau}$. Они отправляются на облачный сервер для вычисления зашифрованного решения. Из теоремы 1 следует,

что можно решать τ отдельных линейных систем:

$$\mathbf{A}_i \cdot x = \mathbf{b}_i, i = \overline{1,\tau}.$$

Пусть $\mathbf{x}_i = (x_{i,1}, ..., x_{i,N}) \in \mathbb{Q}^N$ является решением $\mathbf{A}_i \cdot x = \mathbf{b}_i$. Сервер вычисляет $\mathbf{x}_i, i = \overline{1,\tau}$ и отправляет клиенту. Клиент может получить решение $\mathbf{x}$ исходной системы $\mathbf{A} \cdot x = \mathbf{b}$ следующим образом:

$$\mathbf{x} = \begin{pmatrix} CRT_{k_1,...,k_\tau}(x_{1,1}, ..., x_{\tau,1}) \\ \cdots \\ CRT_{k_1,...,k_\tau}(x_{1,N}, ..., x_{\tau,N}) \end{pmatrix}.$$

ГШ Бабенко, Кучерова и Червякова ([28]). В криптосистеме [28] используется система полиномиальных остаточных классов и обобщенная версия КТО для полиномов. Пусть дано простое число q, $q \geqslant 2$ (это публичный параметр). Секретный ключ — это вектор полиномов $sk = (k_1(x), ..., k_\tau(x)) \in (\mathbb{Z}_q[x])^\tau$, где $k_i(x) = x^d - \alpha_i \in \mathbb{Z}_q[x]$, $GCD(k_i(x), k_j(x)) = 1$ при $i \neq j$. Пространство открытых текстов $\mathcal{M}$ — это $\mathbb{Z}_{q,t}[x]$, где $t < d \cdot \tau$, пространство шифртекстов $\mathcal{C}$ — подмножество $(\mathbb{Z}_q[x])^\tau$.

Алгоритм зашифрования $Enc(m(x) \in \mathbb{Z}_q[x], sk)$:
– вычислить $\mathbf{c} = (c_1(x), ..., c_\tau(x)) \in (\mathbb{Z}_q[x])^\tau$, $c_i(x) = [m(x)]_{k_i(x)}$.

Алгоритм расшифрования $Dec(\mathbf{c} = (c_1(x), ..., c_\tau(x)), sk)$:
– вычислить $m(x) = CRT_{k_1(x),...,k_\tau(x)}(c_1(x), ..., c_\tau(x))$.

В [28] описывается, как формула (1) может быть адаптирована для полиномов. Основная идея такова: по sk и $c_1(x), ..., c_\tau(x)$ можно вычислить $m(x) = \sum_{i=1}^{\tau} c_i(x) \cdot B_i(x)$, где $B_i(x) \in \mathbb{Z}_q[x], i = \overline{1,\tau}$ — полиномы, составленные с использованием $k_i(x), i = \overline{1,\tau}$. Гомоморфные свойства также обеспечивает теорема 1.

Авторы [28] не отметили такой важный момент, что предложенный метод построения секретного ключа приводит к тому, что $\tau \leqslant q$.

7. Общие замечания о стойкости анализируемых криптосистем. Описанные криптосистемы являются детерминированными при условии, что используется некоторая фиксированная система вычетов. Это значит, что их алгоритмы шифрования отображают данный открытый текст всегда в один и тот же шифртекст на заданном ключе. Для такого типа шифрования характерна следующая уязвимость: злоумышленник всегда может по паре шифртекстов понять, шифруют ли они одно и то же сообщение или разные; эта уязвимость достаточно существенна [49].

Рассмотрим криптосистему Вишневского и Князева. Пусть $m \in \mathcal{R}_t$ — открытый текст. И пусть $\mathbf{c} = (c_1, ..., c_\tau) \in \mathbb{Z}^\tau$ шифрует m на ключе $(k_1, ..., k_\tau)$. Предположим, что алгоритм шифрования использует стандартную полную систему вычетов $K_j = \{0, ..., k_j - 1\}$ для каждого k_j и тогда $c_j = [m]_{k_j} \in K_j$. Если для некоторого j выполняется $m < k_j$, то $c_j = m$. А если $m < \min_{j=\overline{1,\tau}}\{k_j\}$, то получим $\mathbf{c} = (m, ..., m) \in \mathbb{Z}^\tau$. Таким образом, открытый текст, по сути, остается *незашифрованным*.

Поэтому очевидной мерой безопасности здесь является требование $k_j \ll t, j = \overline{1,\tau}$. Это предотвратило бы высокую вероятность появления m в векторе $\mathbf{c}$ в случае равномерного распределения на $\mathcal{R}_t$. Вспоминая, что $t = \prod_{j=1}^{\tau} k_j$, получаем, что для улучшения безопасности предпочтительнее выбирать большее τ и меньшие числа k_j. Для других распределений вероятностей выбор $(k_1, ..., k_\tau)$ может быть более сложным.

Отметим, что авторы криптосистемы не указали четких требований к тому, как будут соотноситься между собой битовые длины чисел t и $k_j, j = \overline{1,\tau}$. Исходя из численных примеров, можно предположить, что отдается предпочтение такой конфигурации: большое число t ($\log_2(t) \geqslant 32$) и $k_j \ll t, j = \overline{1,\tau}$.

Также эту проблему можно решить с помощью небольшой модификации алгоритма шифрования. Если $m < k_j$, то необходимо сгенерировать $r_j \xleftarrow{\$} \mathcal{R}_t \setminus \{0\}$, и j-ю координату шифртекста положить равной $c_j = [m]_{k_j} + r_j \cdot k_j$. Более того, можно поступать так для всех координат шифртекста. И тогда шифрование станет вероятностным.

Для криптосистемы Бабенко, Кучерова и Червякова ситуация аналогична, если используется стандартная система полиномиальных остатков. Если $\deg(m(x)) < d$, то $\mathbf{c} = (m(x), ..., m(x))$. Поэтому лучше выбирать $d \ll t$, где t — верхняя граница для степеней открытого текста, а d — степень полиномов в секретном ключе. Также можно рандомизировать координаты шифртекста посредством прибавления к ним полиномов вида $k_j(x) \cdot r_j(x)$, где $r_j(x)$ – случайный полином.

8. Общая схема атаки по известным открытым текстам. Криптосистемы [27, 28] очень похожи по своему устройству. Для них можно составить следующее общее описание. Пространство открытых текстов $\mathcal{M}$ — это подмножество некоторого Евклидова кольца $\mathcal{E}$, sk — случайный вектор $(k_1, ..., k_\tau) \in \mathcal{E}^\tau$, такой что $GCD(k_i, k_j) = 1$ при $i \neq j$, пространство шифртекстов $\mathcal{C}$ — подмножество $\mathcal{E}^\tau$. Открытый текст $m \in \mathcal{M}$ шифруется по формуле $\mathbf{c} = ([m]_{k_1}, \cdots, [m]_{k_\tau})$, где $[m]_{k_j}$ – остаток от деления m на k_j в $\mathcal{E}$. Для расшифрования применяется КТО, адаптированная для $\mathcal{E}$.

Входные данные: пары $(m_1, \mathbf{c_1}), ..., (m_s, \mathbf{c_s})$
Выходные данные: либо секретный ключ sk, либо сообщение «Атака не успешна»

for *i = 1 to* τ **do**
  $d_j := GCD(m_1 - c_{1,j}, ..., m_s - c_{s,j})$;
end
if $GCD(d_1, ..., d_\tau) = 1$ **then**
  Выдать $\mathbf{d}$ в качестве результата;
end
else
  Выдать сообщение «Атака не успешна»;
end

Алгоритм 1: АИО$((m_1, \mathbf{c_1}), ..., (m_s, \mathbf{c_s}))$

Исходя из этого описания, можно составить следующую схему атаки с известными открытыми текстами на самом общем уровне. Предположим, у криптоаналитика есть пары $(m_i, \mathbf{c_i}), i = \overline{1, s}$, где $m_i \in \mathcal{E}$, $\mathbf{c_i} = (c_{i,1}, ..., c_{i,\tau})$, $c_{i,j} = [m_i]_{k_j} \in \mathcal{E}$. Цель криптоаналитика — определить $sk = (k_1, ..., k_\tau)$. Чтобы найти k_j, криптоаналитик может вычислить:

$$d_j = GCD(m_1 - c_{1,j}, ..., m_s - c_{s,j}).$$

Действительно, существует следующее представление:

$$m_i = r_{i,j} \cdot k_j + c_{i,j}, \tag{3}$$

где $r_{i,j} \in \mathcal{E}$ — некоторый случайный элемент. Следовательно, мы имеем:

$$d_j = k_j \cdot GCD(r_{1,j}, ..., r_{s,j}). \tag{4}$$

Вероятность найти k_j указанным способом равна $\mathfrak{p}_{j,s} = Pr\{k_j = d_j\}$. И, очевидно, выполняется

$$\mathfrak{p}_{j,s} = Pr\{GCD(r_{1,j}, ..., r_{s,j}) = 1\}. \tag{5}$$

Величина $\mathfrak{p}_{j,s}$ зависит от закона, по которому распределены случайные элементы $r_{i,j}$ кольца $\mathcal{E}$. Вероятностное распределение чисел $r_{i,j}$, в свою очередь, зависит от распределения вероятностей $\mathcal{D}$ на пространстве открытых текстов $\mathcal{M}$. Вышеизложенное может быть формализовано в виде алгоритма 1, являющегося общей схемой АИО на [27, 28].

В следующих разделах мы проанализируем величину $\mathfrak{p}_{j,s}$ и общую вероятность раскрыть sk для [27] и [28].

9. АИО на криптосистему Вишневского и Князева. Во-первых, отметим, что алгоритм 1 для криптосистемы Вишневского и Князева можно дополнить еще одним шагом, если проверка на шаге 2 успешно пройдена: провести тест на простоту для каждого d_j [50].

Оценка вероятности раскрыть один элемент ключа k_j. Теперь перейдем к оценке вероятности $\mathfrak{p}_{j,s}$. Предположим, что все $r_{i,j}$ из формулы (3) являются независимыми и равномерно случайными положительными целыми числами. Тогда по теореме 2 выполняется $\mathfrak{p}_{j,s} \approx \frac{1}{\zeta(s)}$. Учитывая данные таблицы 1, получаем, что при $s \geqslant 5$ противник получит k_j с вероятностью ≈ 1.

Проанализируем, какое распределение имеют числа $r_{i,j}$ для криптосистемы Вишневского т Князева в случае равномерного распределения вероятностей на пространстве открытых текстов $\mathcal{M}$. Пусть есть случайная величина $m \xleftarrow{\$} \mathcal{R}_t$, где $t = \prod_{i=1}^{\tau} k_i$. Выполняется $m = r \cdot k_j + c$, где k_j — фиксированное число, частное $r = \lfloor \frac{m}{k_j} \rfloor$ — случайная величина, имеющая диапазон значений $\mathcal{R}_q = \{0, 1, ..., q-1\}$, где $q = \frac{t}{k_j}$.

Лемма 1. Случайная величина r имеет равномерное распределение над $\mathcal{R}_q$, где $q = \frac{t}{k_j}$.

Доказательство. Множество $\mathcal{R}_t$ можно представить как объединение $\mathcal{R}_t = \cup_{i=0}^{q} \overline{\mathcal{R}}_i$, где $\overline{\mathcal{R}}_i = \{i \cdot k_j, i \cdot k_j + 1, ..., i \cdot k_j + k_j - 1\}$. Тогда $|\overline{\mathcal{R}}_i| = k_j$ и для $m \in \overline{\mathcal{R}}_i$ имеем $r = i$. Поэтому получаем $Pr\{r = i\} = \frac{k_j}{t} = \frac{1}{q}$.□

Теорема 4. Для криптосистемы Вишневского и Князева выполняется $\mathfrak{p}_{j,s} = \sum_{l=0}^{s-2} C_s^l \cdot \left(\frac{q-1}{q}\right)^{s-l} \cdot \left(\frac{1}{q}\right)^{l} \cdot \left(\frac{1}{\zeta(s-l)} + O(\frac{1}{q-1})\right) + s \cdot \left(\frac{1}{q}\right)^{s}$, $q = \frac{t}{k_j}$.

Доказательство. Вероятность $\mathfrak{p}_{j,s}$ можно представить в виде следующей суммы: $Pr\{r_{i,j} \neq 0, i = \overline{1,s}\ \&\ GCD(r_{1,j}, \cdots, r_{s,j}) = 1\} + \sum_{z=2}^{s-1} Pr\{\exists r_{k_1,j}, \cdots, r_{k_z,j} | r_{k_l,j} \neq 0\ \&\ GCD(r_{k_1,j}, \cdots, r_{k_z,j}) = 1\} + Pr\{\exists r_{i,j} = 1\ \&\ r_{l,j} = 0, l \neq i\}$. Поясним, что событие, вероятность которого указана под знаком суммы, состоит в том, что z чисел из $r_{i,j}$ оказались не равными нулю и взаимно простыми, где $2 \leqslant z < s$, а остальные $r_{i,j}$ равны нулю.

Вероятность того, что l чисел из $r_{i,j}, i = \overline{1,s}$ равны нулю, а остальные нет, составляет $C_s^l \cdot \left(\frac{q-1}{q}\right)^{s-l} \cdot \left(\frac{1}{q}\right)^{l}$. А вероятность того, что ненулевые $s-l$ чисел взаимно просты, равна $\frac{1}{\zeta(s-l)} + O(\frac{1}{q-1})$ по теореме 2. Эти два

события можно считать независимыми. Все вместе это дает формулу для $\mathfrak{p}_{j,s}$.□

Следствием данной теоремы является следующая лемма.

Лемма 2. Для криптосистемы Вишневского и Князева выполняется $\mathfrak{p}_{j,s} > \eta_{j,s}$, *где* $\eta_{j,s} = \left(\frac{q-1}{q}\right)^s \cdot \left(\frac{1}{\zeta(s)} + O(\frac{1}{q-1})\right)$, $q = \frac{t}{k_j}$.

Предположим, что $\log_2(t) \geqslant 32$ и $k_j \ll t, j = \overline{1,\tau}$ (см. раздел 7). Тогда $(\frac{q-1}{q})^s \approx 1$ и можно положить $\eta_{j,s} \approx \frac{1}{\zeta(s)}$.

Таблица 2. Оценки вероятности $\mathfrak{p}_{j,s}$

s	$\widetilde{\mathfrak{p}_{j,s}}$	$1/\zeta(s)$
3	0.8323	0.8319
4	0.9269	0.9259
5	0.9664	0.9643
6	0.9812	0.9829
7	0.992	0.9917
8	0.9964	0.9959
9	0.9985	0.9979
10	0.999	0.999

Были проведены эксперименты для получения практической оценки $\widetilde{\mathfrak{p}_{j,s}}$ вероятности раскрыть один элемент ключа, который выбирался случайно по равномерному распределению из первой тысячи простых чисел. Здесь и далее для получения каждой оценки проводилось десять тысяч компьютерных экспериментов.

В таблице 2 представлены практические оценки $\widetilde{\mathfrak{p}_{j,s}}$ для $\mathfrak{p}_{j,s}$ и соответствующие значения $\frac{1}{\zeta(s)}$ для сравнения. Можно видеть, что выполняется $\widetilde{\mathfrak{p}_{j,s}} \approx \frac{1}{\zeta(s)}$ с вычислительной точностью $\varepsilon = 10^{-2}$.

Оценка вероятности раскрыть ключ sk полностью. Для вероятности $\overline{\mathfrak{p}_{s,\tau}}$ раскрыть ключ целиком справедлива следующая формула

$$\overline{\mathfrak{p}_{s,\tau}} = Pr\{GCD(r_{1,1}, ..., r_{s,1}) = 1, \ \cdots, \ GCD(r_{1,\tau}, ..., r_{s,\tau}) = 1\}. \quad (6)$$

Если используется детерминированный алгоритм шифрования, описанный в разделе 6, то события $GCD(r_{1,j}, ..., r_{s,j}) = 1, j = \overline{1,\tau}$ нельзя считать независимыми друг от друга, поскольку для каждого $i \in \overline{1,s}$ случайные величины $r_{i,1}, ..., r_{i,\tau}$ зависимы между собой. Поэтому

формула

$$\overline{\mathfrak{p}_{s,\tau}} = \prod_{j=1}^{\tau} \mathfrak{p}_{j,s} \tag{7}$$

не справедлива в этом случае.

Однако, если для шифрования использовать вероятностный алгоритм, упомянутый в разделе 7, то зависимости будут устранены прибавкой ко всем $r_{i,j}$ случайных равномерно распределенных независимых величин. Тогда (7) окажется справедливой и выполнится:

$$\overline{\mathfrak{p}_{s,\tau}} > \prod_{j=1}^{\tau} \left(\frac{q_j - 1}{q_j}\right)^s \cdot \left(\frac{1}{\zeta(s)} + O\left(\frac{1}{q_j - 1}\right)\right), \tag{8}$$

где $q_j = t/k_j$.

Если снова предположить, что $\log_2(t) \geqslant 32$ и $k_j \ll t, j = \overline{1,\tau}$, то правая часть (8) будет равна $\approx \frac{1}{\zeta(s)^\tau}$.

Таблица 3. Практические оценки вероятности $\overline{\mathfrak{p}_{s,\tau}}$

s	$\widetilde{\mathfrak{p}_{s,10}}$	$\frac{1}{\zeta(s)^{10}}$	$\widetilde{\mathfrak{p}_{s,50}}$	$\frac{1}{\zeta(s)^{50}}$	$\widetilde{\mathfrak{p}_{s,100}}$	$\frac{1}{\zeta(s)^{100}}$
3	0.1546	0.1587	0.0001	0.0001	0	10^{-17}
4	0.4629	0.4533	0.018	0.0191	0.0003	0.0003
5	0.697	0.6952	0.1561	0.1631	0.0298	0.0266
6	0.8406	0.8415	0.4244	0.4232	0.1748	0.1791
7	0.921	0.9200	0.6631	0.6598	0.4342	0.4354
8	0.9609	0.9679	0.8164	0.8159	0.663	0.6657
9	0.9809	0.9801	0.901	0.9045	0.818	0.8182
10	0.9907	0.9901	0.9523	0.9515	0.9059	0.9053
11	0.9962	0.9945	0.9761	0.9755	0.9574	0.9517
12	0.9974	0.9975	0.9883	0.9877	0.9739	0.9756
13	0.9986	0.9987	0.9941	0.9938	0.9878	0.9878
14	0.9994	0.9993	0.9962	0.9969	0.993	0.9938
15	0.9999	0.9996	0.9983	0.9984	0.9961	0.9969

В таблице 3 показаны практические оценки $\widetilde{\mathfrak{p}_{s,\tau}}$ вероятности $\overline{\mathfrak{p}_{s,\tau}}$ полного раскрытия sk для $\tau = 10, 50$ и 100, полученные в ходе вычислительного эксперимента для детерминированного варианта алгоритма шифрования. То есть формулы (7),(8) не выполняются в данном случае. Также приведены соответствующие значения функции $\frac{1}{\zeta(s)^\tau}$ для сравнения. Можно видеть, что её значения совпадают с $\widetilde{\mathfrak{p}_{s,\tau}}$ с точностью не

менее $\varepsilon = 10^{-2}$ в большинстве случаев. Поэтому, несмотря на отсутствие строгого теоретического обоснования, можно сделать вывод, что $\frac{1}{\zeta(s)^\tau}$ является хорошим приближением для $\overline{\mathfrak{p}_{s,\tau}}$.

Итак, мы получили следующую эмпирическую оценку:

$$\overline{\mathfrak{p}_{s,\tau}} \approx \frac{1}{\zeta(s)^\tau}. \tag{9}$$

Отметим, что при проведении эксперимента числа k_j выбирались случайно по равномерному распределению из первой тысячи простых чисел.

Из таблицы 3 видно, что с ростом τ криптоаналитику нужно все большее количество пар «открытый текст, шифртекст» для того, чтобы найти sk с вероятностью ≈ 1. К примеру, для длины ключа $\tau = 100$ необходимо не менее 11 пар.

Интересно выяснить общее соотношение между τ и числом пар s, которого будет достаточно для восстановления sk с вероятностью θ. Согласно (9) для получения $\overline{\mathfrak{p}_{s,\tau}} \approx \theta$ при данном τ нужно, чтобы s удовлетворяло равенству:

$$\frac{1}{\zeta(s)} = \sqrt[\tau]{\theta}. \tag{10}$$

Дзета-функция Римана при $s > 1$ представима в виде ряда Дирихле $\zeta(s) = 1 + \sum_{i=n}^{\infty} \frac{1}{n^s}$. Из этого легко видеть, что $\psi(s) = \frac{1}{1+\frac{1}{2^s}}$ можно использовать как значение, приближенное к $\frac{1}{\zeta(s)}$. Действительно, уже при $s \geqslant 5$ выполняется $|\frac{1}{\zeta(s)} - \psi(s)| < 10^{-2}$.

Чтобы получить некоторое представление о характере зависимости s от τ, заменим в (10) $\frac{1}{\zeta(s)}$ на $\psi(s)$. Тогда мы получим следующую формулу:

$$s \approx \log_2 \left(\frac{\sqrt[\tau]{\theta}}{1 - \sqrt[\tau]{\theta}} \right), \tag{11}$$

где $0 < \theta < 1$. Последовательность, указанная в правой части равенства (11), является бесконечно большой при $\tau \to \infty$. По мере того как θ становится все ближе к 1, порядок ее роста увеличивается.

Зафиксируем, к примеру, значение $\theta = 0.999$. Тогда будет выполняться $\frac{\sqrt[\tau]{\theta}}{1-\sqrt[\tau]{\theta}} < \tau^2$ и соответственно $s < 2 \cdot \log_2(\tau)$. Общий же характер

зависимости s от τ имеет вид:

$$s = O(\log(\tau)). \tag{12}$$

Эксперименты подтвердили, что (12) отражает реальную зависимость s от τ. На рисунке 1 представлены значения s для $\tau \in \overline{2, 10000}$, для которых согласно данным экспериментов выполняется $\theta = 0.999$. Из графика видно, что с ростом τ количество пар s, необходимых для раскрытия ключа, возрастает, но не очень быстро. Видно, что достаточно иметь $s \approx O(\log(\tau))$ пар, чтобы раскрыть секретный ключ.

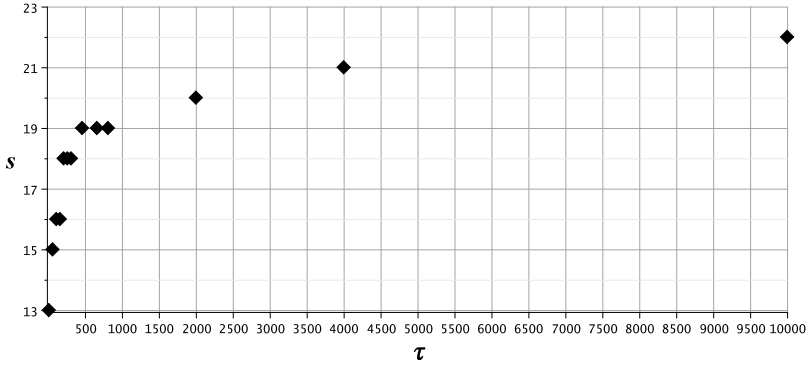

Рис. 1. Экспериментальные данные о числе пар «открытый текст, шифртекст» s, необходимом для раскрытия ключа размерности τ с вероятностью $\theta \geqslant 0.999$.

При построении данного графика для каждого τ элементы ключа k_j выбирались равномерно случайно из первых $5 \cdot \tau$ простых чисел.

Наконец, необходимо отметить, что алгоритм 1 применительно к криптосистеме Вишневского и Князева имеет полиномиальную временную сложность от параметров s, τ и $\log_2(t)$. В частности, временную сложность вычисления всех наибольших общих делителей можно оценить с помощью $s \cdot \tau \cdot O((\log(t))^2)$ [51]. А сложность тестов на простоту составляет $\tau \cdot O((\log_2(t))^3)$ [50].

Криптосистема Вишневского и Князева и АИО на нее были реализованы на языке C++ с использованием среды разработки Qt 1.3.1 и библиотеки NTL [53]. Для тестирования программы использовалась рабочая станция среднего класса: четырехъядерный процессор AMD Phenom (tm) II P960 1,80 ГГц, оперативная память 4 ГБ. Таблица 4 демонстрирует время работы описанной АИО для $\tau = 100$ и разных s. Числа k_j

были выбраны случайным образом из первой тысячи простых чисел. Из таблицы 4 видно, что атака достаточно эффективна.

Таблица 4. Время работы АИО на криптосистему Вишневского и Князева при $\tau = 100$

s	Время(мсек)
5	751.21
6	2147.27
7	2573.16
8	2718.41
9	3020.51
10	3235.11
11	3521.14
12	4011.36
13	4918.38
14	5100.41

10. АИО на криптосистему Бабенко, Кучерова и Червякова [28]. Алгоритм 1 для криптосистемы Бабенко, Кучерова и Червякова можно также дополнить еще одним шагом, если шаг 2 успешно пройден: провести проверку, что все найденные полиномы $d_j(x)$ имеют одну и ту же степень и вид $x^d - \alpha_j$.

Оценка вероятности раскрыть один элемент ключа $k_j(x)$. Проанализируем значения вероятности $\mathfrak{p}_{j,s}$ для криптосистемы Бабенко, Кучерова и Червякова. Предположим, что все $r_{i,j}(x)$ являются независимыми и равномерно случайными полиномами. Тогда по теореме 3 справедливо:

$$\mathfrak{p}_{j,s} > 1 - \frac{1}{q^{s-1}}. \tag{13}$$

Ясно, что с ростом s величина, указанная в (13), будет стремиться к 1. К примеру, при уже $q = 2$ и $s = 5$ выполнится $\mathfrak{p}_{j,s} \approx 1$.

Докажем, что $r_{i,j}(x), i = \overline{1,s}$ действительно являются случайными величинами с равномерным распределением, если распределение вероятностей на $\mathcal{M}$ равномерно.

Теорема 5. Для случайной величины $m(x) \xleftarrow{\$} \mathbb{Z}_{q,t}[x]$ и фиксированного полинома $k(x) \in \mathbb{Z}_q[x]$, где $d = \deg(k(x)) \leqslant t$, существует представление $m(x) = r(x) \cdot k(x) + c(x)$, где $r(x)$ — частное и $c(x)$ — остаток. При этом $r(x)$ — случайная величина, имеющая распределение $r(x) \xleftarrow{\$} \mathbb{Z}_{q,t-d}[x]$.

Таблица 5. $\widetilde{\mathfrak{p}_{j,s}}$ и $\mathfrak{p}_{j,s}$ для $q = 2$, $d = 3$

s	$\widetilde{\mathfrak{p}_{j,s}}$	$\mathfrak{p}_{j,s}$
4	0.86	0.875
5	0.957	0.9525
6	0.967	0.96875
7	0.991	0.984375
8	0.99	0.992188
9	0.997	0.996094
10	0.999	0.998047

Доказательство. Для фиксированного $k(x)$ существует взаимно-однозначное соответствие между полиномами $m(x) \in \mathbb{Z}_{q,t}[x]$ и парами $\{r(x) \in \mathbb{Z}_{q,t-d}[x], c(x) \in \mathbb{Z}_{q,d}[x]\}$. При этом каждому $r(x) \in \mathbb{Z}_{q,t-d}[x] \setminus \{0\}$ соответствует множество, состоящее из q^d различных полиномов $m(x) \in \mathbb{Z}_{q,t}[x]$ степени $d + \deg(r(x))$, имеющих частное $r(x)$ при делении на $k(x)$. А частному $r(x) = 0$ соответствуют все $m(x)$ такие, что $\deg(m(x)) < d$, и таких полиномов тоже будет q^d штук. Из этого следует, что $r(x)$ имеет равномерное распределение вероятностей.□

Тогда по теореме 3 мы получаем следующее утверждение

Теорема 6. Для криптосистемы Бабенко, Кучерова и Червякова выполняется $\mathfrak{p}_{j,s} = 1 - \frac{1}{q^{s-1}} + \frac{q-1}{q^{(t-d)\cdot s}}$.

Были проведены компьютерные эксперименты для того, чтобы определить практическую оценку $\widetilde{\mathfrak{p}_{j,s}}$ вероятности раскрыть один элемент ключа для различных значений параметров q, d, t. К примеру, таблица 5 иллюстрирует значения $\mathfrak{p}_{j,s}$ в соответствии с теоремой 6 и $\widetilde{\mathfrak{p}_{j,s}}$ для $q = 2$, $d = 3, t = 51$. Для указанных значений параметров для раскрытия одного элемента ключа $k_j(x)$ с вероятностью ≈ 1 нужно, чтобы выполнялось $s \geqslant 5$. Для больших q нужно еще меньшее количество пар.

Оценка вероятности раскрыть ключ sk полностью. Проанализируем вероятность $\overline{\mathfrak{p}_{s,\tau}}$ определить $sk = (k_1(x), ..., k_\tau(x)) \in (\mathbb{Z}_q[x])^\tau$. Для неё справедлива формула (6), адаптированная для случая полиномов. Так же, как и для криптосистемы Вишневского и Князева, равенство $\overline{\mathfrak{p}_{s,\tau}} = \prod_{j=1}^{\tau} \mathfrak{p}_{j,s}$ не выполняется, если используется детерминированный алгоритм шифрования, описанный в разделе 6. Однако, если использовать вероятностный алгоритм (см. раздел 7), то равенство будет справедливо и для криптосистемы Бабенко, Кучерова и Червякова получим следующее:

$$\overline{\mathfrak{p}_{s,\tau}} = \left(1 - \frac{1}{q^{s-1}} + \frac{q-1}{q^{(t-d)\cdot s}}\right)^{\tau}. \tag{14}$$

Таблица 6. Количество пар s, необходимых для взлома криптосистемы Бабенко Кучерова и Червякова при $2 \leqslant d \leqslant 60$, $2 \leqslant \tau \leqslant q$, $\theta = 0.95$

q	s
2	5..7
3	4..6
5	3..5
7	3..4
11	3..4
13	2..4

Эксперименты показали, что формула (14), несмотря на отсутствие строгого обоснования, хорошо работает и для случая детерминированного шифрования. Значения вероятностей, полученные по ней, хорошо коррелируют с практическими оценками $\widetilde{\mathfrak{p}_{s,\tau}}$.

На основании (14) можно получить представление о характере зависимости числа пар s, необходимого для раскрытия ключа с вероятностью θ, от τ и q. Для упрощения выкладок положим $\overline{\mathfrak{p}_{s,\tau}} \approx \left(1 - \frac{1}{q^{s-1}}\right)^{\tau}$. Тогда получим:

$$s \approx 1 + \log_q \left(\frac{1}{1 - \sqrt[\tau]{\theta}} \right). \tag{15}$$

При заданных q, θ зависимость s от τ имеет вид $\approx O(\log(\tau))$.

В таблице 6 приведены данные, полученные на основе экспериментов, о минимальном числе пар «открытый текст, шифртекст», необходимом для раскрытия секретного ключа с вероятностью $\theta = 0.95$, для различных значений q. Для каждого q степень полиномов ключа d перебиралась в диапазоне $2 \leqslant d \leqslant 60$, а для τ был сделан исчерпывающий перебор в диапазоне $2 \leqslant \tau \leqslant q$ (напоминаем, что τ не может превышать q). В правой колонке таблицы 6 указан диапазон для количества пар s, который был получен при указанном переборе для d и τ. Можно видеть, что с ростом q уменьшается количество пар s «открытый текст, шифртекст», необходимых для гарантированного взлома криптосистемы.

В ходе построения таблицы 6 было выявлено, что для фиксированного q с ростом τ увеличивается s. При $\tau = q$ достигается максимум. Но влияние τ на s не столь значительно, как влияние q.

Отметим, что значения s, которые можно получить по формуле (15), имеют хорошую корреляцию с данными таблицы 6.

В таблице 7 собрана подробная статистика о минимальном числе s пар, необходимом для раскрытия секретного ключа, для различных

Таблица 7. Зависимость количества пар s, необходимых для взлома криптосистемы Бабенко Кучерова и Червякова с вероятностью более 0.95 при $\tau = q$, от d

	q									
d	2	3	5	7	11	13	17	19	23	29
2	6	5	4	4	4	4	3	3	3	3
5	6	5	5	4	4	4	3	4	3	3
10	6	5	4	4	4	4	4	4	3	3
15	5	5	4	4	4	4	3	3	3	3
20	7	5	5	4	4	4	4	4	3	3
25	6	5	4	4	4	4	4	4	3	3
29	6	5	4	4	4	4	4	3	3	3

Таблица 8. Среднее время, необходимое для осуществления атаки на криптосистему Бабенко, Кучерова и Червякова с использованием **трех** пар (мсек)

	q					
d	5	7	11	13	17	19
2	1.5	2.156	3.48	4.26	6.84	9.08
5	2.132	3.688	8.52	12.81	27.19	32.78
10	4.062	7.9	24.51	38.95	79.44	132.81
15	6.428	14.86	51.14	96.208	171.19	246.54
20	9.908	23.728	104.30	151.41	275.36	407.02
25	14.124	34.914	138.47	195.50	422.23	533.58
29	18.094	54.684	167.59	299.92	560.84	704.88

значений q, d и максимального значения $\tau = q$. Таблица демонстрирует, что степень d довольно слабо влияет на s. Этот факт объясняется видом формулы для $\mathfrak{p}_{j,s}$ из теоремы 6.

В заключение этого раздела отметим, что алгоритм 1 применительно к криптосистеме Бабенко, Кучерова и Червякова имеет полиномиальную временную сложность от параметров s, τ и t. В частности, сложность вычисления всех наибольших общих делителей равна $s \cdot \tau \cdot O(t \cdot (\log(t))^2)$ элементарных операций в $\mathbb{Z}_q$ [52].

Криптосистема Бабенко, Кучерова и Червякова и атака на нее также были реализованы на языке программирования C++ с помощью среды разработки Qt 1.3.1 и библиотеки NTL [54]. Таблица 8 демонстрирует время работы описанной АИО для разных q, d и $\tau = q$, $s = 3$.

11. Адаптивная атака по выбранным открытым текстам. В работе [45] была описана идея адаптивной атаки по выбранным открытым

текстам для криптосистемы, похожей на криптосистему Вишневского и Князева. Основное отличие состоит в том, что в [45] ключ $sk = (k_1, ..., k_\tau) \in \mathbb{N}^\tau$ не обязательно состоит лишь из простых чисел, но $GCD(k_i, k_j) = 1$ при $i \neq j$.

Ниже представлен алгоритм 2 поиска одного модуля k_j ключа, идея которого предложена в [45]. Он принимает на вход пару «открытый текст, шифртекст» и имеет доступ к оракулу $\mathcal{O}_{Enc_{sk}}$, умеющему шифровать любые открытые тексты на ключе sk. С точки зрения криптоаналитика, $\mathcal{O}_{Enc_{sk}}$ представляет собой черный ящик. Изучая выходы, которые $\mathcal{O}_{Enc_{sk}}$ производит на различных входах, он пытается определить sk.

Далее будем использовать обозначение $(m, \mathbf{c}) \leftarrow \mathcal{O}_{Enc_{sk}}(m)$, смысл которого в том, что $\mathcal{O}_{Enc_{sk}}$, получив на вход открытый текст m, на выходе выдает пару $(m, \mathbf{c} = (c_1, ..., c_\tau))$, где $\mathbf{c} = Enc_{sk}(m)$.

Входные данные: $(m_1, \mathbf{c_1}),\ j$
Выходные данные: Модуль k_j

1 Вычислить факторизацию (если она не известна) на простые множители $m_1 - c_{1,j} = \prod_{i=1}^{L_j} p_{j,i}$;
2 $m_2 := \prod_{i=1}^{\lfloor \frac{L_j}{2} \rfloor} p_{j,i}$, $m_3 := \prod_{i=\lfloor \frac{L_j}{2} \rfloor + 1}^{L_j} p_{j,i}$;
3 $(m_2, \mathbf{c_2}) \leftarrow \mathcal{O}_{Enc_{sk}}(m_2)$, $(m_3, \mathbf{c_3}) \leftarrow \mathcal{O}_{Enc_{sk}}(m_3)$;
4 **if** $(c_{2,j} \neq 0)$ & $(m_2 \neq c_{2,j})$ & $(c_{3,j} \neq 0)$ & $(m_3 \neq c_{3,j})$ **then**
5 | **Выдать** $GCD(m_2, c_{2,j}) \cdot GCD(m_3, c_{3,j})$;
6 **end**
7 **else if** $(c_{2,j} = 0)$ & $(c_{3,j} \neq 0)$ **then**
8 | **Выдать** $\mathbf{CalcOneModulus}((m_2, \mathbf{c_2}), j)$;
9 **end**
10 **else if** $(c_{2,j} \neq 0)$ & $(c_{3,j} = 0)$ **then**
11 | **Выдать** $\mathbf{CalcOneModulus}((m_3, \mathbf{c_3}), j)$;
12 **end**
13 **else**
14 | **Выдать** сообщение «Атака не успешна»;
15 **end**

Алгоритм 2: $\mathbf{CalcOneModulus}\ ((m_1, \mathbf{c_1}), j)$

Пара $(m_1, \mathbf{c_1})$, которая изначально подается на вход $\mathbf{CalcOneModulus}$, вычисляется оракулом $\mathcal{O}_{Enc_{sk}}$ для некоторого случайно выбранного открытого текста m_1.

Авторы [45] утверждают, что если выполняется условие, указанное в строке 4 алгоритма 2, то справедливо $k_j = \alpha_j$, где $\alpha_j = GCD(m_2, c_{2,j}) \cdot$

$GCD(m_3, c_{3,j})$. Однако это не так: может оказаться, что $\alpha_j = v_j \cdot k_j$, где v_j — некоторый случайный множитель.

Действительно, имеем $m_2 = k_j \cdot r_{2,j} + c_{2,j}, m_3 = k_j \cdot r_{3,j} + c_{3,j}$ и разложение на простые множители $k_j = \prod_{t=1}^{l_j} p_{j,k_{z_t}}$. Числа m_2, m_3 построены таким образом, что одна часть сомножителей $p_{j,k_{z_t}}$ числа k_j делит m_2 и $c_{2,j}$, а другая часть делит m_3 и $c_{3,j}$. Исходя из этого, имеем $k_j | \alpha_j$. Однако не обязательно выполняется $k_j = \alpha_j$, так как, к примеру, в $GCD(m_2, c_{2,j})$ (или $GCD(m_3, c_{3,j})$) могут попасть простые сомножители числа $r_{2,j}$ (или $r_{3,j}$ соответственно).

Входные данные: $(m_1, \mathbf{c_1}),\ j$
Выходные данные: Модуль k_j

1 Вычислить факторизацию (если она не известна) на простые множители $m_1 - c_{1,j} = \prod_{i=1}^{L_j} p_{j,i}$;
2 $m_2 := \prod_{i=1}^{\lfloor \frac{L_j}{2} \rfloor} p_{j,i}$, $m_3 := \prod_{i=\lfloor \frac{L_j}{2} \rfloor + 1}^{L_j} p_{j,i}$;
3 $(m_2, \mathbf{c_2}) \leftarrow \mathcal{O}_{Enc_{sk}}(m_2)$, $(m_3, \mathbf{c_3}) \leftarrow \mathcal{O}_{Enc_{sk}}(m_3)$;
4 **if** $(c_{2,j} = 0)$ & $(c_{3,j} \neq 0)$ & (m_2 – *простое число)* **then**
5 | **Выдать** m_2;
6 **end**
7 **else if** $(c_{2,j} \neq 0)$ & $(c_{3,j} = 0)$ & (m_3 – *простое число)* **then**
8 | **Выдать** m_3;
9 **end**
10 **else if** $(c_{2,j} = 0)$ & $(c_{3,j} \neq 0)$ **then**
11 | **Выдать** $\mathbf{CalcOnePrimeModulus}((m_2, \mathbf{c_2}), j)$;
12 **end**
13 **else if** $(c_{2,j} \neq 0)$ & $(c_{3,j} = 0)$ **then**
14 | **Выдать** $\mathbf{CalcOnePrimeModulus}((m_3, \mathbf{c_3}), j)$;
15 **end**
16 **else**
17 | **Выдать** сообщение «Атака не успешна»;
18 **end**

Алгоритм 3: $\mathbf{CalcOnePrimeModulus}\ ((m_1, \mathbf{c_1}), j)$

Нетрудно привести соответствующий численный пример. Пусть $k_j = 15, m_1 - c_{1,j} = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2, m_2 = 2^2 \cdot 3^2, m_3 = 5^2 \cdot 7^2$. Выполняется $c_{2,j} = [m_2]_{k_j} = 6$, $c_{3,j} = [m_3]_{k_j} = 10$ и тогда $GCD(m_2, c_{2,j}) = 6$, $GCD(m_3, c_{3,j}) = 5$, $GCD(m_2, c_{2,j}) \cdot GCD(m_3, c_{3,j}) = 30 \neq k_j$.

Итого, событие $k_j = \alpha_j$ на шаге 5 алгоритма 2 происходит не гарантированно, как утверждается в [45], а лишь с некоторой вероят-

ностью. Поэтому в общем случае данный алгоритм, возможно, требует существенной доработки. Мы оставим этот вопрос для дальнейшего исследования.

Однако для случая, когда все k_j простые (как в схеме ПГШ [27]), алгоритм 2 с небольшим изменением будет работать и гарантированно выдавать k_j не более, чем за $\lceil \log_2(L_j) \rceil$ рекурсивных вызовов. При этом максимальное количество пар, которое придется запросить у оракула, составляет $2 \cdot \lceil \log_2(L_j) \rceil + 1$.

Здесь представлен алгоритм 3, позволяющий раскрыть один элемент ключа k_j, для криптосистемы Вишневского и Князева в рамках адаптивной атаки по выбранным открытым текстам. Полный алгоритм атаки будет состоять в том, что **CalcOnePrimeModulus** нужно вызвать τ раз для каждого k_j. Количество пар «открытый текст, шифртекст», которое необходимо запросить у оракула для того, чтобы гарантированно определить sk, составляет $O(\tau)$.

Похожий алгоритм можно предложить и для криптосистемы [28]. Однако, так же как и в случае конструкции, которая изначально анализировалась в [45], он не будет гарантированно выдавать k_j. В [28] элемент ключа $k_j(x) = x^d - \alpha_j$ не является неприводимым полиномом. Поэтому алгоритм раскрытия $k_j(x)$ — это, по сути, алгоритм 2, адаптированный для полиномов. На шаге 5 он будет вычислять корректный $k_j(x)$ лишь с некоторой вероятностью.

12. Заключение. Были изучены две симметричные полностью гомоморфные криптосистемы, основанные на применении систем остаточных классов и китайской теоремы об остатках — криптосистема Вишневского и Князева и криптосистема Бабенко, Кучерова и Червякова. Эти криптосистемы являются детерминированными, а потому для них априори характерна следующая уязвимость: злоумышленник всегда способен отличить пару шифртекстов, шифрующих одно и то же сообщение, от пары шифртекстов, шифрующих разные сообщения. Использование вероятностного шифрования всегда является более предпочтительным с точки зрения защищенности. Уже, исходя из этого, анализируемые криптосистемы не желательно применять в реальных приложениях. Здесь мы описали один из вариантов, как можно сделать их вероятностными. Примером может послужить еще одна схема ПГШ «HORNS» [26], основанная на системах остаточных классов, однако являющаяся вероятностной.

Проведенный в данной работе анализ показал, что анализируемые криптосистемы уязвимы к атаке по известным открытым текстам. Их секретный ключ представляет собой вектор $sk = (k_1, ..., k_\tau)$. Были получены точные формулы вероятности раскрытия одного элемента k_j

этого вектора. Согласно этим формулам необходимо перехватить хотя бы 5 пар «открытый текст, шифртекст» для обеих криптосистем в случае равномерного распределения на пространстве открытых текстов, чтобы найти k_j с вероятностью ≈ 1. Для криптосистемы Бабенко, Кучерова и Червякова с ростом размера используемого базового конечного поля q может хватить и двух пар. Эта информация подтверждена вычислительным экспериментом.

Также была проанализирована вероятность $\overline{\mathfrak{p}_{s,\tau}}$ полностью раскрыть ключ в зависимости от количества перехваченных пар s. Для криптосистемы Вишневского и Князева было установлено, что имеет место формула $\overline{\mathfrak{p}_{s,\tau}} \approx \frac{1}{\zeta(s)^\tau}$, где ζ — дзета-функция Римана. Она нуждается в дополнительном теоретическом обосновании, но при этом хорошо коррелирует с экспериментальными оценками вероятностей. Исходя из данной формулы и результатов экспериментов, было установлено, что для того, чтобы определить sk с вероятностью ≈ 1 при заданном τ, нужно перехватить $s = O(\log(\tau))$ пар. К примеру, при размерности секретного ключа $\tau = 10$ криптоаналитику необходимо иметь ≈ 13 пар, а при $\tau = 10000$ — соответственно 22 пары.

Для криптосистемы Бабенко, Кучерова и Червякова была получена формула $\overline{\mathfrak{p}_{s,\tau}} = \left(1 - \frac{1}{q^{s-1}} + \frac{q-1}{q^{(t-d)\cdot s}}\right)^\tau$. Она также нуждается в дополнительном более строгом обосновании. Однако значения вероятностей, посчитанные по ней, близки к оценкам вероятностей, полученным в ходе экспериментов. При фиксированном параметре q здесь также нужно иметь $\approx O(\log(\tau))$ пар, чтобы определить ключ с вероятностью ≈ 1.

Было выявлено, что для криптосистемы Бабенко, Кучерова и Червякова максимальным образом на рост числа пар s, необходимого для взлома, влияет параметр q. От степени полиномов секретного ключа d величина s зависит очень слабо. И, наконец, увеличение τ влечет за собой увеличение s. Однако способ генерации секретного ключа, выбранный авторами криптосистемы, приводит к естественному ограничению $\tau \leqslant q$. Поэтому при оценке вероятности раскрыть ключ можно сразу зафиксировать максимальную его размерность $\tau = q$. Исходя из полученных результатов экспериментов, было выявлено, что уже при $q = 29$ и $\tau = q$ количество пар s, необходимых для взлома с вероятностью ≈ 1, равно трем. С ростом q число s может только убывать.

В целом, можно отметить, что криптосистема Бабенко, Кучерова и Червякова находится в «тисках» жестких ограничений:

– нельзя существенно увеличивать q, так как тогда упадет сложность взлома;

– нельзя сделать размерность ключа τ больше, чем q;

– нельзя увеличить степень полиномов секретного ключа d, т.к. тогда открытые тексты небольшой степени фактически останутся незашифрованными.

В качестве рекомендации по увеличению сложности взлома криптосистемы Бабенко, Кучерова и Червякова можно предложить генерировать полиномы секретного ключа более произвольным образом. Это, по крайней мере, отменит ограничение $\tau \leqslant q$.

Отметим также, что в ходе анализа вероятности раскрытия ключа для анализируемых криптосистем использовалось предположение, что пространство открытых текстов имеет равномерное распределение вероятностей. Ситуация может отличаться, если пространство открытых текстов имеет другое распределение вероятностей, что может быть предметом отдельных исследований. Но необходимо напомнить, что наиболее трудный для криптоаналитика случай — это когда распределение на множестве открытых текстов равномерно.

Основным инструментом проведения атаки с известными открытыми текстами на анализируемые криптосистемы является алгоритм поиска наибольшего общего делителя. Поэтому, время, необходимое для реализации атак, является полиномиальным от размера входных данных.

Также в данной работе была проанализирована адаптивная атака по выбранным открытым текстам из работы [45] на шифр, похожий на криптосистему Вишневского и Князева. Было установлено, что алгоритм определения элемента ключа k_j, представленный в [45], не будет всегда гарантированно выдавать k_j. Это событие происходит с некоторой вероятностью < 1. Поэтому алгоритм нуждается в дополнительном исследовании и доработке. Но мы установили, что небольшая модификация делает его пригодным для криптоанализа криптосистемы Вишневского и Князева. Он будет гарантированно раскрывать ключ sk. Для работы ему нужно $O(\tau)$ пар «открытый текст, шифртекст». Аналогичный алгоритм можно предложить и для ПГШ [28]. Однако он, как и исходный алгоритм из [45], требует доработки.

Итог проведенного анализа заключается в том, что криптосистема Вишневского и Князева и криптосистема Бабенко, Кучерова и Червякова являются уязвимыми к атаке по выбранным открытым текстам и атаке с известными открытыми текстами. Поэтому использовать их для шифрования конфиденциальных данных может быть небезопасно.

В дальнейшем планируется провести анализ стойкости данных криптосистем к атаке только по шифртекстам.

Литература

1. *Rivest R. L., Adleman L., Dertouzos M. L.* On data banks and privacy homomorphisms // Foundations of secure computation. 1978. vol. 32. no. 4. pp. 169-178.
2. *Brickell E. F., Yacobi Y.* On privacy homomorphisms // Proceedings of Advances in Cryptology—EUROCRYPT'87. 1988. pp. 117-125.
3. *Goldwasser G., Micali S.* Probabilistic encryption & how to play mental poker keeping secret all partial information // Proceedings of the fourteenth annual ACM symposium on Theory of computing. 1982. pp. 365-377.
4. *Paillier P.* Public-key cryptosystems based on composite degree residuosity classes // Proceedings of Advances in cryptology—EUROCRYPT'99. 1999. pp. 223-238.
5. *Rivest R. L., Shamir A., Adleman L.* A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. 1978. vol. 21. no. 2. pp. 120-126.
6. *Gentry C.* A fully homomorphic encryption scheme // PhD thesis. Stanford University, 2009. 209 p.
7. *Cheon J. H., Coron J. S., Kim J., Lee M. S., Lepoint T., Tibouchi M., Yun A.* Batch fully homomorphic encryption over the integers // Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2013. pp. 315-335.
8. *Brakerski Z., Gentry C., Vaikuntanathan V.* (Leveled) fully homomorphic encryption without bootstrapping // Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ACM). 2012. pp. 309-325.
9. *Brakerski Z.* Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP // Proceedings of Advances in cryptology—CRYPTO 2012. 2012. pp. 868-886.
10. *Chillotti I., Gama N., Georgieva M., Izabachene M.* Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds // Proceedings of Advances in Cryptology—ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security. 2016. pp. 3-33.
11. *Cheon J. H., Han K., Kim D.* Faster Bootstrapping of FHE over the Integers // IACR Cryptology ePrint Archive. 2017. no. 79.
12. *Micciancio D., Sorrell J.* Ring packing and amortized FHEW bootstrapping // IACR Cryptology ePrint Archive. 2018. no. 532.
13. *Brakerski Z.* Quantum FHE (Almost) As Secure As Classical // Proceedings of Annual International Cryptology Conference. 2018. pp. 67-95.
14. *Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В.* Полностью гомоморфное шифрование (Обзор) // Вопросы защиты информации. 2015, № 3. С. 3–25.
15. *Kipnis A., Hibshoosh E.* Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification // IACR Cryptology ePrint Archive. 2012. no. 637.
16. *Xiao L., Bastani O, Yen I.-L.* An efficient homomorphic encryption protocol for multi-user systems // IACR Cryptology ePrint Archive. 2012. no. 193.
17. *Sharma I.* Fully homomorphic encryption scheme with symmetric keys // Master's of technology diss. in Department of Computer Science & Engineering (with specialization in Computer Engineering). 2013. 64 p.
18. *Yagisawa M.* Fully Homomorphic Encryption without bootstrapping // IACR Cryptology ePrint Archive. 2015. no. 474.
19. *Yagisawa M.* Improved Fully Homomorphic Encryption with Composite Number Modulus // IACR Cryptology ePrint Archive. 2016. no. 50.

20. *Ростовцев А.Г., Богданов А.Г., Михайлов М.Ю.* Метод безопасного вычисления полинома в недоверенной среде с помощью гомоморфизмов колец // Проблемы информационной безопасности. Компьютерные системы. 2011. № 2. С. 76-85.
21. *Zhirov A. O., Zhirova O. V., Krendelev S. F.* Practical fully homomorphic encryption over polynomial quotient rings // Proceedings of 2013 World Congress on Internet Security (WorldCIS). 2013. pp. 70-75.
22. *Жиров А. О., Жирова О. В., Кренделев С. Ф.* Безопасные облачные вычисления с помощью гомоморфной криптографии // Безопасность информационных технологий. 2013. Т. 20. № 1. С. 6-12.
23. *Dasgupta S., Pal S. K.* Design of a polynomial ring based symmetric homomorphic encryption scheme // Perspectives in Science. 2016. vol. 8. pp. 692-695.
24. *Domingo-Ferrer J.* A provably secure additive and multiplicative privacy homomorphism // Information Security. 2002. pp. 471-483.
25. *Domingo-Ferrer J.* A new privacy homomorphism and applications // Information Processing Letters. 1996. vol. 60. no 5. pp. 277-282.
26. *Gomathisankaran M., Tyagi A., Namuduri K.* HORNS: A homomorphic encryption scheme for Cloud Computing using Residue Number System // Proceedings of 2011 45th Annual Conference Information Sciences and Systems (CISS). 2011. pp. 1-5.
27. *Вишневский А. К., Князев В. В.* Комплексное применение гомоморфных криптографических преобразований для решения систем линейных алгебраических уравнений // Наукоемкие технологии. 2015. Т. 16. № 11. С. 28-35.
28. *Бабенко М. Г., Кучеров Н. Н., Червяков Н. И.* Разработка системы гомоморфного шифрования информации на основе полиномиальной системы остаточных классов // Сибирские электронные математические известия. Труды VI международной молодежной школы-конференции «Теория и численные методы решения обратных и некорректных задач». 2015. Т. 12. С. 33-41. URL: http://semr.math.nsc.ru/v12/c1-283.pdf (дата обращения: 02.12.2018).
29. *Vizár D., Vaudenay S.* Cryptanalysis of chosen symmetric homomorphic schemes // Studia Scientiarum Mathematicarum Hungarica. 2015. vol. 52. no. 2. pp. 288–306.
30. *Tsaban B., Lifshitz N.* Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme // Journal of Mathematical Cryptology. 2015. vol. 9. no. 2. pp. 75-78,
31. *Трепачева А. В.* Криптоанализ симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел // Известия Южного федерального университета. Технические науки. 2015. Т. 166, № 5. С. 89-100.
32. *El-Yahyaoui, A., Elkettani, M. D.* Cryptanalysis of fully homomorphic encryption schemes // International Journal of Computer Science and Information Security, LJS Publishing, 2016. vol. 14. no. 5. pp. 677-685.
33. *Cheon J. H., Kim W. H., Nam H. S.* Known-plaintext cryptanalysis of the Domingo-Ferrer algebraic privacy homomorphism scheme // Information Processing Letters. 2006. vol. 97 no. 3. pp. 118-123.
34. *Wagner D.* Cryptanalysis of an algebraic privacy homomorphism // Proceedings of International Conference on Information Security. 2003. pp. 234-239.
35. *Trepacheva A.V.* Improved known plaintexts attack on Domingo-Ferrer homomorphic cryptosystem // Труды Института системного программирования РАН. 2014. Т. 26. № 5. С. 83-98.
36. *Трепачева А.В.* О криптоанализе одной полностью гомоморфной криптосистемы на основе задачи факторизации // Безопасность информационных технологий. 2015. Т. 22, № 2. С. 19-25.

37. *Trepacheva A.V.* Known plaintext attack on a fully homomorphic cryptosystem based on factorization // Proceedings of 4th Workshop on Current Trends in Cryptology (CTCrypt'2015). 2015. pp. 205-215.
38. *Babenko L., Trepacheva A.* Known plaintexts attack on polynomial based homomorphic encryption // Proceedings of the 7th International Conference on Security of Information and Networks (ACM). 2014. pp.157-165.
39. *Трепачева А.В.* Криптоанализ полностью гомоморфных криптосистем, основанных на алгебре октонионов // Обозрение прикладной и промышленной математики. 2016. Т. 23. вып. 4. 2 с.
40. *Wang Y.* Notes on Two Fully Homomorphic Encryption Schemes Without Bootstrapping // IACR Cryptology ePrint Archive. 2015. no. 519.
41. *Wang Y.* Octonion Algebra and Noise-Free Fully Homomorphic Encryption (FHE) Schemes // IACR Cryptology ePrint Archive. 2016. no. 68.
42. *Babenko L.K.,Trepacheva A.V.* Cryptanalysis of factoring-based fully homomorphic encryption // Proceedings of the 8th International Conference on Security of Information and Networks. 2015. pp. 80-83.
43. *Трепачева А.В.* Атака по шифртекстам на одну линейную полностью гомоморфную криптосистему // Прикладная дискретная математика. Приложение. 2015. № 8. С. 75-78.
44. *Трепачева А.В.* О соотношениях между атаками на симметричные шифры, гомоморфные над кольцом вычетов // Безопасность информационных технологий. 2017. Т. 24. № 2. С. 82–91.
45. *Babenko, M., Chervyakov, N., Tchernykh, A., Kucherov, N., Deryabin, M., Radchenko, G., Navaux Ph., Svyatkin, V.* Security analysis of homomorphic encryption scheme for cloud computing: Known-plaintext attack // Proceedings of 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2018. pp. 270-274.
46. *Бухштаб А. А.* Теория чисел // М.: Просвещение. 1966. 384 С.
47. *Nymann J. E.* On the probability that k positive integers are relatively prime // Journal of Number Theory. 1972. vol. 4. no. 5. pp. 469-473.
48. *Benjamin A. T., Bennett C. D.* The probability of relatively prime polynomials // Mathematics Magazine. 2007. vol. 80. no. 3. pp. 196-202.
49. *Goldreich O.* Foundations of cryptography. // Cambridge university press. 2009. 800 p.
50. *Weenink T.* Deterministic primality testing // Bachelor's thesis. Technische Universiteit Eindhoven. 2015. 24 p.
51. *Knuth D. E.* The Art of Computer Programming – Volume 3 (Sorting and Searching) // Addison-Wesley professional. 1997. 800 p.
52. *Ахо А., Ульман Дж., Хопкрофт Дж.* Построение и анализ вычислительных алгоритмов // М.: Мир. 1979. 536 с.
53. Реализация криптосистемы Вишневского и Князева и атаки на нее. URL: https://github.com/alina1989malina/CryptanalysisVishnevskyKnyazev (дата обращения: 02.12.2018).
54. Реализация криптосистемы Бабенко, Кучерова и Червякова и атаки на нее. URL: https://github.com/alina1989malina/CryptanalysisBabenkoKucherovChervjakov (дата обращения: 02.12.2018).

Бабенко Людмила Климентьевна — д-р техн. наук, профессор, главный научный сотрудник, Южно-Российского регионального учебно-научного центра по проблемам информационной безопасности в системе высшей школы, профессор кафедры безопасности информационных технологий, Инженерно-технологическая академия Южного федерального университета

(ИТА ЮФУ). Область научных интересов: криптография, анализ стойкости криптографических алгоритмов, программно-аппаратная защита информации, анализ безопасности криптографических протоколов, вредоносное программное обеспечение, поведенческий анализ, параллельный алгоритм, распределенные многопроцессорные вычисления, нейропроцессорные вычисления. Число научных публикаций — более 200. lkbabenko@sfedu.ru, https://sfedu.ru/person/lkbabenko; ул. Чехова, 2, Таганрог, 347922; р.т.: +7(8634)312-018, факс: +7(8634)312-018.

Трепачева Алина Викторовна — младший научный сотрудник кафедры безопасности информационных технологий, Инженерно-технологическая академия Южного федерального университета (ИТА ЮФУ). Область научных интересов: криптоанализ гомоморфных шифров, анализ защищенности облачных систем, вычисления в недоверенной среде, математическая статистика, теория вероятности, дискретные функции, алгебраическая геометрия. Число научных публикаций — 22. alina1989malina@yandex.ru; ул. Чехова, 2, Таганрог, 347922; р.т.: +7(850)865-5415.

Поддержка исследований. Работа выполнена при финансовой поддержке Минобрнауки РФ (проект № 2.6264.2017/8.9).

DOI 10.15622/sp.18.1.230-262

L. K. Babenko, A. V. Trepacheva

TOWARDS UNSECURITY OF TWO HOMOMORPHIC ENCRYPTIONS BASED ON RESIDUE SYSTEM

Babenko L.K., Trepacheva A.V. **Towards Unsecurity of Two Homomorphic Encryptions Based on Residue System.**

Abstract. The security of two recently proposed symmetric homomorphic encryption schemes based on residue system is analyzed. Both schemes have a high computational efficiency since using residue system naturally allows parallelizing computations. So they could be good candidates to protect the data in clouds. But to the best of our knowledge there is a lack of security analysis for these encryption schemes.

It should be noted that the first cryptosystem under our consideration was already considered in literature. The sketch of adaptive chosen-plaintext attack was proposed and estimation of its success was given. In this paper the attack is analyzed and it is shown that in some cases it may work incorrectly. Also more general algorithm of known-plaintext attack is presented. Theoretical estimations of probability to recover the key using it and practical estimations of this probability obtained during the experiments are provided.

The security of the second cryptosystem has not been analyzed yet and we fill this gap for known-plaintext attack. The dependency between the number of «plaintext, ciphertext» pairs required to recover the key and parameters of the cryptosystem is analyzed. Also some recommendations for increasing the security level are provided.

The final conclusion of our analysis is that both cryptosystems are vulnerable to known-plaintext attack. And it may be dangerous to encrypt private data using them.

Finally it should be noted that the key element of the proposed attacks is the algorithm of computing the greatest common divisor. So their computational complexity depends polynomially on the size of input data.

Keywords: Homomorphic Encryption, Cloud Computing, Cryptanalyzis, Known-Plaintext Attack, Residue Number System.

Babenko Ludmila Kliment'evna — Ph.D., Dr. Sci., Professor, leading researcher of South-Russian regional scientific-educational centre, Professor of Information Technologies Security Department, Academy for Engineering and Technologies of Southern Federal University. Research interests: Cryptography, Security Analysis of Cryptographic Algorithms, Software and Hardware Information Protection, Security Analysis of Cryptographic Protocols, Malicious Software, Behavioral Analysis, Parallel Algorithm, Distributed Multiprocessor Computing, Neuroprocessor Computing. The number of publications — >200. lkbabenko@sfedu.ru, https://sfedu.ru/person/lkbabenko; 2, Chekhova str., Taganrog, 347922, Russia; office phone: +7(8634)312-018, fax: +7(8634)312-018.

Trepacheva Alina Viktorovna — Junior Researcher of Information Technologies Security Department, Academy for Engineering and Technologies of Southern Federal University. Research interests: Cryptanalysis of Homomorphic Encryption, Mathematical Statistics, Probability Theory, Algebraic Geometry. The number of publications — 18. alina1989malina@yandex.ru; 2, Chekhova str., Taganrog, 347922, Russia; office phone: +7(812)328-3337.

Acknowledgements. This research is supported by Russian Ministry of Education and Science (grant no. 2.6264.2017/8.9).

References

1. *Rivest R. L., Adleman L., Dertouzos M. L.* On data banks and privacy homomorphisms. Foundations of secure computation. 1978. vol. 32. no. 4. pp. 169-178.
2. *Brickell E. F., Yacobi Y.* On privacy homomorphisms. Proceedings of Advances in Cryptology—EUROCRYPT'87. 1988. pp. 117–125.
3. *Goldwasser G., Micali S.* Probabilistic encryption & how to play mental poker keeping secret all partial information. Proceedings of the fourteenth annual ACM symposium on Theory of computing. 1982. pp. 365-377.
4. *Paillier P.* Public-key cryptosystems based on composite degree residuosity classes. Proceedings of Advances in cryptology—EUROCRYPT'99. 1999. pp. 223-238.
5. *Rivest R. L., Shamir A., Adleman L.* A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978. vol. 21. no. 2. pp. 120-126.
6. *Gentry C.* A fully homomorphic encryption scheme. PhD thesis. Stanford University. 2009. 209 p.
7. *Cheon J. H., Coron J. S., Kim J., Lee M. S., Lepoint T., Tibouchi M., Yun A.* Batch fully homomorphic encryption over the integers. Proceedings of In Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2013. pp. 315-335.
8. *Brakerski Z., Gentry C., Vaikuntanathan V.* (Leveled) fully homomorphic encryption without bootstrapping. Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ACM). 2012. pp. 309-325.
9. *Brakerski Z.* Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. Proceedings of Advances in cryptology–CRYPTO'2012. 2012. pp. 868-886.
10. *Chillotti I., Gama N., Georgieva M., Izabachene M.* Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. Proceedings of 22nd International Conference on the Theory and Application of Cryptology and Information Security. 2016. pp. 3-33.
11. *Cheon J. H., Han K., Kim D.* Faster Bootstrapping of FHE over the Integers. IACR Cryptology ePrint Archive. 2017. no. 79.
12. *Micciancio D., Sorrell J.* Ring packing and amortized FHEW bootstrapping. IACR Cryptology ePrint Archive, 2018. no. 532.
13. *Brakerski Z.* Quantum FHE (Almost) As Secure As Classical. Proceedings of Annual International Cryptology Conference. 2018. pp. 67-95.
14. *Babenko L. K., Burtyka F. B., Makarevich O. B. Trepacheva A.V.* Polnost'ju gomomorfnoe shifrovanie (obzor) [Fully Homomorphic Encryption (A Survey)]. Voprosy zashhity informacii [The information security issues]. 2015. no. 3. pp. 3–25. (in Russ.).
15. *Kipnis A., Hibshoosh E.* Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification. IACR Cryptology ePrint Archive. 2012. no. 637.
16. *Xiao L., Bastani O, Yen I.-L.* An efficient homomorphic encryption protocol for multi-user systems. IACR Cryptology ePrint Archive. 2012. no. 193.
17. *Sharma I.* Fully homomorphic encryption scheme with symmetric keys. Master of Technology thesis in Department of Computer Science & Engineering (with specialization in Computer Engineering). 2013. 64 p.
18. *Yagisawa M.* Fully Homomorphic Encryption without bootstrapping. IACR Cryptology ePrint Archive. 2015. no. 474.
19. *Yagisawa M.* Improved Fully Homomorphic Encryption with Composite Number Modulus. IACR Cryptology ePrint Archive. 2016. no. 50.
20. *Rostovtsev A. G., Bogdanov A. G., Mikhaylov M. Yu.* Secure evaluation of polynomial using privacy ring homomorphisms. IACR Cryptology ePrint Archive. 2011. no. 24.

21. *Zhirov A. O., Zhirova O. V., Krendelev S. F.* Practical fully homomorphic encryption over polynomial quotient rings. Proceedings of 2013 World Congress on Internet Security (WorldCIS). 2013. pp. 70-75.
22. *Zhirov A. O., Zhirova O. V., Krendelev S. F.* Bezopasnye oblachnye vychisleniya s pomoshhyu homomorfnoj cryptographii [Secure Computing in the Cloud Storage Using Homomorphic Encryption]. Bezopasnost' informacionnyh tehnologij [Information Technologies Security]. 2013. no. 1. pp. 6-12. (In Russian)
23. *Dasgupta S., Pal S. K.* Design of a polynomial ring based symmetric homomorphic encryption scheme. Perspectives in Science. 2016. vol. 8. pp. 692-695.
24. *Domingo-Ferrer J.* A provably secure additive and multiplicative privacy homomorphism. Proceedings of International Conference on Information Security. 2002. pp. 471-483.
25. *Domingo-Ferrer J.* A new privacy homomorphism and applications. Information Processing Letters. 1996. vol. 60. no. 5. pp. 277–282.
26. *Gomathisankaran M., Tyagi A., Namuduri K.* HORNS: A homomorphic encryption scheme for Cloud Computing using Residue Number System. Proceedings of 2011 45th Annual Conference Information Sciences and Systems (CISS). 2011. pp. 1-5.
27. *Vishnevskij A. K., Knjazev V. V.* Kompleksnoe primenenie gomomorfnyh kriptograficheskih preobrazovanij dlja reshenija sistem linejnyh algebraicheskih uravnenij [Complex application of homomorphic cryptographic transformations for solving systems of linear algebraic equations]. Naukoemkie tehnologii [High technology]. 2015. vol. 16, no. 11, pp. 28-35. (In Russ.).
28. *Chervjakov N. I., Babenko M. G., Kucherov N. N.* Razrabotka sistemy gomomorfnogo shifrovanija informacii na osnove polinomial'noj sistemy ostatochnyh klassov [Development of a homomorphic information encryption system based on a polynomial residual classes system]. Sibirskie Elektronnye Matematicheskie Izvestiya. Trudy VI mezhdunarodnoj molodezhnoj shkoly-konferencii «Teorija i chislennye metody reshenija obratnyh i nekorrektnyh zadach» [Siberian Electronic Mathematical Reports. Proceedings of the VI International Youth School-Conference «Theory and numerical methods for solving inverse and ill-posed problems»]. 2015. vol. 12. pp. 33-41. Available at http://semr.math.nsc.ru/v12/c1-283.pdf (accessed: 02.12.2018). (In Russ.).
29. *Vizár D., Vaudenay S.* Cryptanalysis of chosen symmetric homomorphic schemes. Studia Scientiarum Mathematicarum Hungarica. 2015. vol. 52. no. 2. pp. 288–306.
30. *Tsaban B., Lifshitz N.* Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme. Journal of Mathematical Cryptology. 2015. vol. 9, no. 2. pp. 75-78,
31. *Trepacheva A.V.* Cryptanalysis of symmetric fully homomorphic linear cryptosystems based on numbers factorization problem. Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki [The SFEDU proceedings. Engineering Science]. 2015. vol. 166. no. 5. pp. 89-100. (In Russ.).
32. *El-Yahyaoui A., Elkettani M. D.* Cryptanalysis of fully homomorphic encryption schemes. International Journal of Computer Science and Information Security. 2016. vol. 14. no. 5. pp. 677-685.
33. *Cheon J. H., Kim W. H., Nam H. S.* Known-plaintext cryptanalysis of the Domingo-Ferrer algebraic privacy homomorphism scheme. Information Processing Letters. 2006. vol. 97 no. 3. pp. 118-123.
34. *Wagner D.* Cryptanalysis of an algebraic privacy homomorphism. Proceedings of International Conference on Information Security. 2003. pp. 234-239.
35. *Trepacheva A.V.* Improved known plaintexts attack on Domingo-Ferrer homomorphic cryptosystem. Trudy Instituta sistemnogo programmirovaniya RAN [Proceedings of the Institute for System Programming]. 2014. vol. 26. Issue 5. pp. 83-98.

36. *Trepacheva A.V.* O kriptoanalize odnoj polnost"ju gomomorfnoj kriptosistemy na osnove zadachi faktorizacii [About Cryptanalysis of One Fully Homomorphic Cryptosystem Based on Factorization Problem]. Bezopasnost' informacionnyh tehnologij [Information Technologies Security]. 2015. vol. 22. no. 2. pp. 19-25. (In Russ.).
37. *Trepacheva A.V.* Known plaintext attack on a fully homomorphic cryptosystem based on factorization. Proceedings of 4th Workshop on Current Trends in Cryptology CTCrypt'2015. 2015. pp. 205-215.
38. *Babenko L., Trepacheva A.* Known plaintexts attack on polynomial based homomorphic encryption. Proceedings of the 7th International Conference on Security of Information and Networks (ACM). 2014. pp.157-166.
39. *Trepacheva A.V.* Kriptoanaliz polnost'ju gomomorfnyh kriptosistem, osnovannyh na algebre oktonionov [Cryptanalyzis of fully homomorphic cryptosystem, based on octonion algebra]. Obozrenie prikladnoj i promyshlennoj matematiki [A survey of applied and industrial mathematics]. 2016. 2 p. (In Russ.).
40. *Wang Y.* Notes on Two Fully Homomorphic Encryption Schemes Without Bootstrapping. IACR Cryptology ePrint Archive. 2015. no. 519.
41. *Wang Y.* Octonion Algebra and Noise-Free Fully Homomorphic Encryption (FHE) Schemes. IACR Cryptology ePrint Archive. 2016. no. 68.
42. *Babenko L.K.,Trepacheva A.V.* Cryptanalysis of factoring-based fully homomorphic encryption. Proceedings of the 8th International Conference on Security of Information and Networks (ACM). 2015. pp. 80-83.
43. *Trepacheva A.V.* Ataka po shifrtekstam na odnu linejnuju polnost'ju gomomorfnuju kriptosistemu [Ciphertexts-only attack on one linear fully homomorphic cryptosystem]. Prikladnaja diskretnaja matematika. Prilozhenie [Applied discrete mathematics. Annex.]. 2015. no. 8. pp. 75-78. (In Russ.).
44. *Trepacheva A.V.* On the relations between the attacks on symmetric homomorphic encryption over the residue ring. Bezopasnost' informacionnyh tehnologij [Information Technologies Security]. 2017. no. 2. pp. 82-91. (In Russ.).
45. *Babenko M., Chervyakov N., Tchernykh A., Kucherov N., Deryabin M., Radchenko G., Navaux Ph., Svyatkin V.* Security analysis of homomorphic encryption scheme for cloud computing: Known-plaintext attack. Proceedings of 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2018. pp. 270-274.
46. *Buhshtab A. A.* Teoriya chisel [The Number Theory]. M.: Prosveshcheniye. 1966. 384 p. (In Russ.).
47. *Nymann J. E.* On the probability that k positive integers are relatively prime. Journal of Number Theory. 1972. vol. 4, no. 5, pp. 469-473.
48. *Benjamin A. T., Bennett C. D.* The probability of relatively prime polynomials. Mathematics Magazine. 2007. vol. 80. no. 3. pp. 196–202.
49. *Goldreich O.* Foundations of Cryptography. Cambridge University press. 2009. 800 p.
50. *Weenink T.* Deterministic primality testing. Bachelor thesis. Technische Universiteit Eindhoven. 2015. 24 p.
51. *Knuth D. E.* The Art of Computer Programming – Volume 3 (Sorting and Searching). Addison-Wesley. 1998. 800 p.
52. *Aho A., Ulman J., Hopcroft J.* The Design and Analysis of Computer Algorithms. Addison-Wesley Publishing Company. 1974. 536 p.
53. Implementation of Vishnevsky-Knyazev's cryptosystem and attack on it. Available at: https://github.com/alina1989malina/CryptanalysisVishnevskyKnyazev (accessed: 02.12.2018).

54. Implementation of Babenko-Kucherov-Chervjakov's cryptosystem and attack on it. Available at: https://github.com/alina1989malina/CryptanalysisBabenkoKucherovChervjakov (accessed: 02.12.2018).