10. *Plenkin A.P., Rumyantsev K.E.* Stend dlya nauchnykh issledovaniy kvantovo-kriptograficheskoy sistemy [Stand for scientific research of quantum-cryptographic systems], *Sovremennye tendentsii v obrazovanii i nauke: Sb. nauch. tr. po materialam Mezhdunarodnoy nauch.-prakt. konferentsii 31 oktyabrya 2013 g.: V 26 ch. Ch. 2* [Sat. scientific papers on materials of the International scientific-practical conference on October 31, 2013: In 26 parts. Part 2. Tambov: Izd-vo TROO «Biznes–Nauka–Obshchestvo», 2013, pp. 108-111.
11. *Gorbunov A.V., Mamaev A.V., Rumyantsev K.E., Panyushkin S.A.* Razrabotka kvantovo-kriptograficheskoy sistemy na baze apparatnoy platformy inostrannogo proizvodstva [The development of a quantum-cryptographic system based on the hardware platform of foreign production], Materialy chetvertoy Vserossiyskoy konferentsii po volokonnoy optike «VKVO–2013» (g. Perm', 16–19 oktyabrya 2013 goda) [The materials of the fourth all-Russian conference on fiber optics "wcwo-2013" (, Perm, 16-19 October 2013)]. Perm': Foton–ekspress, 2013, No. 6 (110), pp. 84-85.

Статью рекомендовал к опубликованию д.т.н., профессор Д.А. Безуглов.

Румянцев Константин Евгеньевич – Южный федеральный университет; e-mail: rke2004@mail.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 89281827209; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Плёнкин Антон Павлович – e-mail: pljonkin@mail.ru; тел.: 89054592158; кафедра информационной безопасности телекоммуникационных систем; аспирант.

Rumyatsev Konstantin Evgen'evich – Southern Federal University; e-mail: rke2004@mail.ru; 44, Nekrasovskiy, Taganrog, 347928, Russia; phone: +79281827209; the department of information security of telecommunication systems; head of department; dr. of eng. sc.; professor.

Pljonkin Anton Pavlovich – e-mail: pljonkin@mail.ru; phone: +79054592158; the department of information security of telecommunication systems; postgraduate student.

УДК 003.26.09

А.В. Трепачева

КРИПТОАНАЛИЗ ШИФРОВ, ОСНОВАННЫХ НА ГОМОМОРФИЗМАХ ПОЛИНОМИАЛЬНЫХ КОЛЕЦ

Проводится анализ защищенности симметричных гомоморфных криптосхем шифрования, построенных на гомоморфизмах полиномиальных колец. Предлагается простой метод вычисления секретного ключа при наличии у криптоаналитика нескольких пар (шифртекст, открытый текст) в случае, когда пространство открытых текстов – конечное поле $\mathbb{F}_q$. *Он позволяет определить правильный ключ с вероятностью, равной единице, при наличии хотя бы пяти пар в случае небольших* q. *Для больших же значений* q *достаточно уже двух пар. Обсуждается, каким образом можно адаптировать этот метод для случая, когда пространство открытых текстов – кольцо вычетов* $\mathbb{Z}_n$, *где* n *– составное число. Также обсуждается метод, позволяющий скорректировать вычисленное с использованием пар значение ключа в случае, когда количество пар (шифротекст, открытый текст) меньше пяти. Для его работы необходимо знание вероятностного распределения на множестве открытых текстов и наличие дополнительной последовательности шифртекстов, зашифрованных на том же ключе. Данный метод успешно раскрывает ключ практически в 100 % случаев, если на открытых текстах задано распределение, достаточно сильно отличающееся от равномерного (например, нормальное распределение с небольшой дисперсией).*

Атака по известным открытым текстам; гомоморфное шифрование; облачные вычисления; полиномы.

A.V. Trepacheva

CRYPYOANALYSIS OF CRYPTOSYTEMS BASED ON POLYNOMIAL RING HOMOMORHISMS

In this paper we analyze security issues of some symmetric homomorphic cryptosystems that are based on polynomial ring homomorphisms. We propose a method to recover a secret key of cryptosystem for plaintext space being a finite field $\mathbb{F}_q$ if several pairs (ciphertext, plaintext) were intercepted. For small values of q this method allows to find a correct key with probability ≈ 1, if the number of pairs is at least five. For large q two pairs are enough. We discuss how this method can be adapted for plaintext space being a set of integers modulo n, where n is a composite number. Also a method to correct the value of secret key computed using pairs (ciphertext, plaintexts) is discussed. It's important for the case when the number of pairs is less than five. This method requires knowledge of probabilistic distribution over plaintext space and the presence of additional ciphertexts sequence encrypted on the same key. The method is successful with probability close to 1, if the distribution over plaintext space is not too close to uniform (for example, normal distribution with moderate dispersion).

Known plaintext attack; homomorphic encryption; cloud computations; polynomials.

Введение. Гомоморфная схема шифрования (ГСШ) – это криптосхема, позволяющая проводить вычисления над данными в зашифрованном виде с последующей возможностью извлечения результата вычислений над соответствующими открытыми текстами с помощью секретного ключа. Разработка и криптоанализ существующих криптосхем ГСШ представляют значительный интерес на сегодняшний день в связи с большой популярностью облачных сервисов. Это обусловлено тем, что к данным, хранящимся на облачных серверах, могут получить доступ злоумышленники. Поэтому данные необходимо шифровать перед загрузкой на сервер. Ясно, что для того чтобы при этом было возможно проводить некоторую обработку зашифрованных данных, не давая серверу ключ расшифрования, необходимо использовать именно ГСШ.

Особенный интерес для практики представляют полностью гомоморфные схемы шифрования (ПГСШ), которые позволяют вычислять над шифртекстами любые функции. С 2009 г., было предложено большое количество ПГСШ [1–6]. Однако всем этим криптосхемам для их использования требуются значительные вычислительные ресурсы, а также они используют сложный математический аппарат.

В связи с этим в работах [7] и [8] были предложены симметричные ПГСШ, являющиеся концептуально простыми и более практичными. Криптосхемы из [7] и [8] объединяет то, что они используют гомоморфизм колец $R[x] \to R$, осуществляемый подстановкой некоторого секретного значения $t \in R$ в $f(x) \in R[x]$ (*гомоморфизм вычисления*). Здесь $R = \mathbb{Z}$ (кольцо целых чисел) или $R = \mathbb{Z}_m$ (кольцо целых чисел по модулю m), $R[x]$ – кольцо многочленов от переменной x с коэффициентами из R.

Стандартным требованием к защищенности гомоморфной криптосхемы является стойкость к атаке по выбранным открытым текстам. Криптостойкость криптосхем из [7], [8] относительно этой атаки не была оценена в полной мере. Поэтому целью данной работы является проанализировать вопрос о том, насколько в действительности они защищены против неё. Отметим, что здесь пока что будет рассмотрен только случай, когда $R = \mathbb{Z}_m$.

1. Описание криптосистем. Кратко напомним устройство криптосхемы из [7]. Пространство открытых текстов M – это кольцо R, пространство шифротекстов C и пространство ключей K вложены в $R[x]$. Для зашифрования $m \in M$

кодируется в случайный полином $\tilde{r}(x) = m + r_1 \cdot x + ... + r_n \cdot x^n$, где $r_i \xleftarrow{\$} R,\ i = 1,...,n$ (эта запись означает, что r_i сгенерированы по равномерному распределению над R). Шифртекст $c(x)$ вычисляется как композиция полиномов $c(x) = \tilde{r}(k(x))$, где $k(x)$ – секретный ключ. Поскольку справедливо $c(x) = m + r_1 \cdot k(x) + ... + r_n \cdot (k(x))^n$, то расшифрование может быть вычислено как $c(x_0)$, где x_0 – некоторый корень $k(x)$. Также расшифровать можно, вычислив $c(x) \bmod k(x)$, так как $c(x) = m + r(x) \cdot k(x),\ r(x) = r_1 + r_2 \cdot k(x) ... + r_n \cdot (k(x))^{n-1}$.

Ясно, что если есть шифротексты $c(x) = \tilde{r}_1(k(x))$ и $c(x) = \tilde{r}_2(k(x))$, шифрующие m_1 и m_2, то выполняется $c_+(x) = c_1(x) + c_2(x) = (\tilde{r}_1 + \tilde{r}_2)(k(x))$ и $c_*(x) = c_1(x) \cdot c_2(x) = (\tilde{r}_1 \cdot \tilde{r}_2)(k(x))$. Тогда расшифрование $c_+(x)$ даст $m_1 + m_2$, а расшифрование $c_*(x)$ – $m_1 \cdot m_2$.

Описанная криптосистема не является полностью гомоморфной в строгом смысле, поскольку при умножении шифртекстов степени многочленов разрастаются очень быстро. На практике это приводит к ограничению на количество умножений, которые можно вычислить над данными в зашифрованном виде.

Данное ограничение было устранено в [8] за счет того, что в качестве пространства шифртекстов C было выбрано факторкольцо $R[x]/(f(x))$, где $f(x)$ – многочлен, кратный $k(x)$. Шифрование в [8] вычисляется как $c(x) = m + r(x) \cdot k(x)$ (т.е. шифрование [7] является частным случаем шифрования [8]). После умножения шифртексты приводятся по модулю $f(x)$, что очевидно не нарушает корректность последующего расшифрования, поскольку $f(x) = k(x) \cdot r'(x)$. Для $R = \mathbb{Z}$ и $R = \mathbb{Z}_p$ (где p – простое число) опубликование $f(x)$ является недопустимым, поскольку $f(x)$ можно легко факторизовать на неприводимые сомножители [9] и, следовательно, найти ключ. Поэтому в [8] предлагается использовать $R = \mathbb{Z}_n$, где n – трудное для факторизации число (RSA модуль), поскольку факторизация многочленов в $\mathbb{Z}_n[x]$ требует знания разложения n [10].

2. Атаки по известным и выбранным открытым текстам на криптосистемы из [7] и [8]. Для криптосистем из [7, 8] справедлив следующий формальный результат.

Лемма 1. Атака по выбранным открытым текстам на криптосистемы из [7, 8] эквивалентна атаке по известным открытым текстам.

Доказательство. Очевидно, что атака по известным открытым текстам всегда формально может быть трансформирована в атаку по выбранным открытым текстам. Это справедливо для любой криптосистемы. Утверждение же в обратную сторону справедливо не всегда. Покажем, что для криптосистемы из [7] оно выполняется.

Предположим, есть атака $\mathbf{A}$ по выбранным открытым текстам на криптосистему из [7]. Покажем, что с её помощью можно построить атаку $\mathbf{A}'$ по известным открытым текстам. Предположим, криптоаналитик A перехватил пары

$(m_i \in M, c_i(x) \in C),\ i = \overline{1, n_1},\ n_1 > 1,$ где $c_i(x) = \tilde{r_i}(k(x)) = m_i + r_i(x) \cdot k(x)$, $M = \mathbb{Z}_m$. Если m – простое число, то $M = \mathbb{Z}_m$ – поле. В этом случае ясно, что поскольку криптосистема гомоморфна, то, складывая, умножая между собой и домножая $c_i(x)$ на некоторые множители из $\mathbb{Z}_m$ в разном порядке, криптоаналитик сможет получить шифртекст, шифрующий любой наперед заданный $m \in M$. Для $m = p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$ может случиться так, что арифметические операции над $c_i(x)$ в разных комбинациях не смогут дать в итоге шифртекста, шифрующего любой наперед заданный $m \in M$. Например, это случится, если в перехваченных парах все m_i кратны одному и тому же p_j.

Однако необходимо отметить, что шифровку для $\forall m \in M$ можно получить из $c_i(x)$, просто прибавив к $c_i(x)$ константу $m' \in M$, такую что $m' = m - m_i$. Здесь, по сути, используется то, что $\forall m' \in M$ в случае данной криптосистемы является тривиальной шифровкой самого себя, т.е. сгенерированной с $\tilde{r}(x) = m'$. Этот способ получения шифровок годится и для $M = \mathbb{Z}_n$, и для $M = \mathbb{Z}_p$.

Таким образом, гомоморфные свойства криптосистемы из [7] позволяют из перехваченных пар (открытый текст, шифртекст) сгенерировать пары для выбранных криптоаналитиком открытых текстов. Тогда для того, чтобы получить из атаки **A** по выбранным открытым текстам атаку **A′** по известным открытым текстам, криптоаналитик сначала трансформирует известные пары в выбранные, а затем запускает атаку **A**.

Рассуждения, приведенные выше, очевидно справедливы и для криптосистемы из [8].□

Теперь покажем, что криптосистема из [7] не защищена против атаки по известным открытым текстам. Рассмотрим сначала случай $M = \mathbb{Z}_p$, где p – простое число. Криптоаналитик A имеет пары $(m_i \in M, c_i^1(x) \in C),\ i = \overline{1, n_1},\ n_1 > 1$, где $c_i^1(x) = \tilde{r_i^1}(k(x)) = m_i + r_i^1(x) \cdot k(x)$. Тогда A можно вычислить с помощью алгоритма Евклида

$$g(x) = НОД(c_1^1(x) - m_1, \ldots, c_{n_1}^1(x) - m_{n_1}) = НОД(r_1^1(x) \cdot k(x), \ldots, r_{n_1}^1(x) \cdot k(x)),$$

где $НОД$ – это наибольший общий делитель полиномов. Очевидно, справедливо $g(x) = r(x) \cdot k(x)$, где $r(x) = НОД(r_1^1(x), \ldots, r_{n_1}^1(x)) \cdot$

Оценим вероятность Pr того, что $\deg(r(x)) = 0$ и тогда $g(x) = k(x)$ с точностью до константного множителя. Ясно, что Pr равна вероятности того, что $\deg(НОД(r_1^1(x), \ldots, r_{n_1}^1(x))) = 0$. Для оценки последней напомним теорему, доказанную в [11].

Теорема 1. Пусть есть полиномы $p_1(x), \ldots, p_m(x) \in \mathbb{Z}_p[x]$, $\forall i : \deg(p_i(x)) < n$, чьи коэффициенты сгенерированы по равномерному распределению над $\mathbb{Z}_p$, где p – простое число. Вероятность того, что $\deg(НОД(p_1(x), \ldots, p_m(x))) = 0$, равна $1 - 1/p^{m-1} + (p-1)/p^{m \cdot n}$.□

Если предположить, что полиномы $r_i^1(x)$ сгенерированы по равномерному распределению, то на основании данной теоремы имеем $\Pr = 1 - 1/\ p^{n_1 - 1} + (p-1)/\ p^{(\max\{\deg(r_i^1)\}+1)\cdot n_1}$. Однако поскольку в [7] для шифрования используется композиция полиномов, то коэффициенты $r_i^1(x)$ можно разбить на несколько групп, в пределах каждой из которых они коррелируют друг с другом. И таким образом $r_i^1(x)$ имеют не совсем равномерное распределение (хотя и достаточно близкое к нему). Однако, несмотря на это, компьютерные эксперименты показали, что вероятность, вычисленная согласно формуле $\Pr = 1 - 1/\ p^{n_1 - 1} + (p-1)/\ p^{(\max\{\deg(r_i^1)\}+1)\cdot n_1}$, достаточно хорошо аппроксимирует вероятность того, что $\deg(НОД(r_1^1(x),...,r_{n_1}^1(x))) = 0$. В табл. 1, приведены значения $\Pr$, подсчитанные по формуле, и значения $\Pr$, оцененные посредством компьютерного эксперимента. Здесь были выбраны $M = \mathbb{Z}_2$, $\deg(k(x)) = 4$ и $\max_i\{\deg(r_i(x))\} = 5$. Для реализации всех алгоритмов криптосистемы из [7] и предложенного метода раскрытия ключа использовалась библиотека NTL [12]. Чтобы практически оценить $\Pr$, проводились 1000 итераций, на каждой из которых генерировалась последовательность $(m_i, c_i^1(x)),\ i = \overline{1, n_1}$, а затем вычислялось $g(x)$.

Таблица 1

Вероятность того, что $g(x) = k(x)$ для $\mathbb{Z}_2$ при разных n_1

n_1	Точное значение $\Pr$	Практическое значение $\Pr$
2	0.5	0.489
3	0.75	0.76
4	0.875	0.86
5	0.9375	0.95
6	0.96875	0.967
7	0.984375	0.991
8	0.992188	0.99
9	0.996094	0.997
10	0.998047	0.999

Можно видеть, что при $n_1 \geq 5$ справедливо $\Pr \approx 1$, т.е. данный метод почти гарантированно раскрывает секретный ключ для $\mathbb{Z}_2$.

Таблица 2

Вероятность того, что $g(x) = k(x)$ для $\mathbb{Z}_{103}$ при разных n_1

n_1	Точное значение $\Pr$	Практическое значение $\Pr$
2	0.99	0.9902
3	1	0.999906
4	1	0.999999
≥5	1	1

Из табл. 2 видно, что при больших значениях p ($p > 100$) уже при $n_1 = 2$ будет выполняться $\Pr \approx 1$.

Перейдем теперь к случаю $M = \mathbb{Z}_n$, где $n = p \cdot q,\ p \neq q$, p, q – простые числа. Для кольца $\mathbb{Z}_n[x]$, в общем, корректно говорить о наибольшем общем множителе (НОМ) многочленов, а не о НОДе. Действительно, поскольку в $\mathbb{Z}_n[x]$ разложение на неприводимые однозначно [10], то для $\forall f, g\ \exists HOM(f,g)$, но $HOM(f,g)$ не обязательно делит f, g, так как в $\mathbb{Z}_n$ есть делители нуля. Если же $HOM(f,g)$ делит f, g, то это и есть $НОД(f,g)$. В итоге, A, получив $(m_i, c_i^1(x)), i = \overline{1, n_1}$, должен найти $g(x) = HOM(c_1^1(x) - m_1, ..., c_{n_1}^1(x) - m_{n_1})$, поскольку также очевидно будет выполняться $g(x) = r(x) \cdot k(x)$. Ниже приведены леммы, которые предлагают два разных способа вычисления $g(x)$.

Лемма 2. Для вычисления $g(x) = HOM(c_1^1(x) - m_1, ..., c_{n_1}^1(x) - m_{n_1})$ можно использовать алгоритм Евклида. Если он завершится успешно, то $g(x)$ будет найдено.

Доказательство. По сути, повторяет доказательство корректности алгоритма Евклида для полиномов с коэффициентами из поля.□

Лемма 3. Если известна факторизация $n = p \cdot q,\ p \neq q$, то $g(x) = HOM(c_1^1(x) - m_1, ..., c_{n_1}^1(x) - m_{n_1}) \in \mathbb{Z}_n[x]$ можно вычислить по коэффициентным применением Китайской теоремы об остатках (КТО) к многочленам $g_p(x) = НОД((c_1^1(x) - m_1) \bmod p, ..., (c_{n_1}^1(x) - m_{n_1}) \bmod p) \in \mathbb{Z}_p[x]$,
$g_q(x) = НОД((c_1^1(x) - m_1) \bmod q, ..., (c_{n_1}^1(x) - m_{n_1}) \bmod q) \in \mathbb{Z}_q[x]$.

Доказательство. Пусть есть полином $f(x) = f_0 + f_1 \cdot x + ... + f_t \cdot x^t \in \mathbb{Z}_n[x]$. Согласно КТО, ему однозначным образом соответствует пара $(f_p(x),\ f_q(x)) \in \mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$,
где

$$f_p(x) = (f_p)_0 + (f_p)_1 \cdot x + ... + (f_p)_t \cdot x^t,\ (f_p)_i = f_i \bmod p,$$

$$f_q(x) = (f_q)_0 + (f_q)_1 \cdot x + ... + (f_q)_t \cdot x^t,\ (f_q)_i = f_i \bmod q.$$

Справедливо равенство $f_i = KTO((f_p)_i, (f_q)_i)$. Введем обозначение $f(x) = KTO(f_p(x), f_q(x))$.

В кольце $\mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$ операции $+, *$ над парами определены поточечно (более подробно см. [10]).

Пусть теперь есть два полинома $f(x), g(x) \in \mathbb{Z}_n[x]$. По КТО для них определены пары $f' = (f_p(x),\ f_q(x)), g' = (g_p(x), g_q(x))$. Можно вычислить $d_p(x) = НОД(f_p(x), g_p(x)) \in \mathbb{Z}_p[x]$ и $d_q(x) = НОД(f_q(x), g_q(x)) \in \mathbb{Z}_q[x]$. Введём следующие обозначения: $a_p(x) = f_p(x) / d_p(x)$, $b_p(x) = g_p(x) / d_p(x)$, $a_q(x) = f_q(x) / d_q(x)$, $b_q(x) = g_q(x) / d_q(x)$. В силу того, что операции в $\mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$ поточечные, имеем $f' = (d_p(x), d_q(x)) \cdot (a_p(x), a_q(x))$ и $g' = (d_p(x), d_q(x)) \cdot (b_p(x), b_q(x))$. Поскольку $НОД(a_p(x), b_p(x))$ и $НОД(a_q(x), b_q(x))$ являются константами, то $d' = HOM(f', g') = (d_p(x), d_q(x))$. Вследствие однозначного соответствия между f' и f, g' и g по КТО получаем, что $HOM(f,g) = KTO(d_p(x), d_q(x))$.□

В случае, когда факторизация n может быть легко вычислена, алгоритм, содержащийся в Лемме 3, можно сразу применить для вычисления $g(x)$. Если же n трудно факторизовать, то для вычисления $g(x)$ можно сначала попытаться применить алгоритм Евклида. Однако на одной из его итераций могут появиться $f_1(x), f_2(x) \in \mathbb{Z}_n[x]$, такие, что $f_1(x)$ не делит $f_2(x)$. Тогда ясно, что $НОД(n, lc(f_1(x))) > 1$ или $НОД(n, lc(f_2(x))) > 1$, где $lc(f_1(x))$ и $lc(f_2(x))$ – коэффициенты при старшей степени полиномов $f_1(x)$ и $f_2(x)$ соответственно. Таким образом, факторизация n на данном этапе будет раскрыта. Далее для поиска $g(x)$ можно применить лемму 3.

Вероятность того, что $g(x) = r(x) \cdot k(x), \deg(r(x)) = 0$ в соответствии с КТО и правилом вычисления вероятности появления двух событий, может быть оценена по формуле

$$\Pr = (1 - \frac{1}{p^{n_1 - 1}} + \frac{p-1}{p^{(\max\{\deg(r_i^1 \bmod p)\}+1) \cdot n_1}})(1 - \frac{1}{q^{n_1-1}} 1/q^{n_1-1} + \frac{q-1}{q^{(\max\{\deg(r_i^1 \bmod q)\}+1) \cdot n_1}}).$$

В табл. 3 представлена практическая оценка Pr при $M = \mathbb{Z}_{9173503}, p = 3557, q = 2579$, $\max\limits_i \{\deg(c_i^1(x))\} = 20$, $\deg(k(x)) = 4$. Для того чтобы оценить Pr, также проводились 1000 итераций.

Таблица 3

Вероятность того, что $g(x) = k(x)$ для $\mathbb{Z}_{9173503}$

n_1	Практическое значение Pr
2	0.999
≥3	1

Замечание. Поскольку в криптосистеме из [8] всегда предполагается использовать большие модули n, то для неё достаточно двух пар (открытый текст, шифртекст) для того, чтобы с вероятностью ≈ 1 раскрыть секретный ключ. Более того, достаточно и одной пары $(m,\ c(x) = m + r(x) \cdot k(x))$, так как конструкция из [8] предполагает наличие у криптоаналитика полинома $f(x) = r_0(x) \cdot k(x)$. Тогда ясно, что $НОД(f(x),\ c(x) - m) = k(x)$ с вероятностью ≈ 1.

Рассуждения, приведенные выше, можно по аналогии корректно обобщить на случай $M = \mathbb{Z}_n$, где $n = p_1 \cdot \ldots \cdot p_t, p_i \neq p_j, p_i -$ простые числа. Случай же $n = p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}, p_i \neq p_j$, где $\exists k_i > 1$, требует отдельного рассмотрения. Известно, что для таких n факторизация многочленов в $\mathbb{Z}_n[x]$ на неприводимые сомножители является неоднозначной [10]. Поэтому вопрос о поиске $g(x)$ нуждается в дальнейшем изучении. Для $M = \mathbb{Z}$ можно действовать по аналогии с $M = \mathbb{Z}_p$.

3. Метод коррекции ключа с использованием дополнительной последовательности шифртекстов. Будем рассматривать $M = \mathbb{Z}_p$, где p – простое число, $n_1 < 5$. В этом случае при небольших p есть вероятность (небольшая, но ею нельзя пренебречь), что $g(x) = r(x) \cdot k(x), \deg(r(x)) > 0$. Поэтому $g(x)$ необходимо верифицировать и при необходимости скорректировать.

Предположим, что A имеет дополнительно последовательность шифртекстов $\{c_i^2(x)\}, c_i^2(x) = \tilde{r_i^2}(k(x)) = m_i^2 + r_i^2(x) \cdot k(x), i = \overline{1, n_2}$, а также ему известно вероятностное распределение $\mathbb{D}$ над $\mathbb{Z}_p$. Тогда для верификации $g(x)$ и его корректировки A может проделать следующую последовательность действий.

1) A должен вычислить $rem_i(x) = c_i^2(x) \bmod g(x)$. Если $\exists rem_i(x)$: $\deg(rem_i(x)) > 0$, то $g(x) \neq k(x)$, поскольку приведение шифровок по модулю $k(x)$ обязательно дает остаток нулевой степени. В этом случае необходимо продолжить работу с многочленом $g(x)$. Иначе A останавливается и полагает, что $g(x)$ – ключ.

Прежде чем перейти ко второму шагу, сделаем важное замечание. Для того чтобы A смог расшифровать любой шифртекст, зашифрованный на $k(x)$, ему не нужно раскрывать $k(x)$ целиком. Достаточно найти хотя бы один его сомножитель $k'(x)$, поскольку $c(x) = m + r^0(x) \cdot k(x) = m + r^0(x) \cdot k_1'(x) \cdot ... \cdot k_\alpha'(x)$, где $k_i'(x)$ – неприводимый сомножитель $k(x)$. Ясно, что так как $\deg(k_i'(x)) > \deg(m) = 0$, то $\forall i : c(x) \bmod k_i'(x) = m$.

2) Если приведение по модулю $g(x)$ дало хотя бы один остаток ненулевой степени, то для A надо найти все различные неприводимые сомножители $G = \{g_1(x), ..., g_\delta(x)\}$ полинома $g(x)$. Ясно, что все $k_i'(x)$ содержатся в G. A нужно найти хотя бы один из них.

3) A может попытаться сузить множество G, вычислив $\forall i \forall j : c_i^2(x) \bmod g_j(x)$. Сомножитель ключа не может дать остаток степени > 0, поэтому у A останется множество $G' = \{g_1'(x), ..., g_\beta'(x)\} \subseteq G$, такое что для $\forall g_j'(x) \exists mes_j = (m_1^j, ..., m_{n_2}^j) \in \mathbb{Z}_p^{n_2}, m_i^j = c_i^2(x) \bmod g_j'(x)$.

4) Для того чтобы выбрать $g_j'(x)$ из G', криптоаналитик может применить статистический критерий. А именно, выбирается тот $g_j'(x)$, для которого соответствующая последовательность mes_j имеет вероятностное распределение, наиболее близкое к $\mathbb{D}$ (близость меряется по статистическому расстоянию). Ясно, что успешность данного критерия зависит от $\mathbb{D}$. Если $\mathbb{D}$ близко к равномерному, то возрастает количество неверных результатов. Теоретически это можно объяснить тем, что для $g_j'(x)$, не связанные с ключом, по сути являются полиномами с коэффициентами, имеющими распределение, близкое к случайному. Тогда приведение $c_i^2(x)$ по модулю таких $g_j'(x)$ дает равномерно случайные остатки. И тогда в соответствующих последовательностях mes_j все m_i^j равновероятны. Также длина последовательности $\{c_i^2(x)\}, i = \overline{1, n_2}$ не должна быть слишком маленькой, поскольку при маленьких значениях n_2 частоты появления элементов $\mathbb{Z}_p$ могут достаточно сильно отклониться от вероятностей появления. Табл. 4–6 демонстрируют для $\deg(k(x)) = 4, \deg(r_i(x)) \leq 5$ практически оцененные вероятности Pr того, что при обращении к статистическому критерию он выбирает такое $g_j'(x)$, которое действительно является сомножителем ключа $k(x)$.

Таблица 4

Вероятность успеха Pr **статистического критерия для равномерного распределения** $\mathbb{D}$

$M = \mathbb{Z}_2$		$M = \mathbb{Z}_{103}$	
n_2	Pr	n_2	Pr
100	0,54	100	0,44
200	0,5	200	0,5
300	0,44	300	0,47
400	0,46	400	0,51

Таблица 5

Вероятность успеха Pr **статистического критерия для** $M = \mathbb{Z}_3$, $\mathbb{D}$ **– нормальное распределение с математическим ожиданием** $\mu = 0$ **и дисперсией** $\sigma = 2$

n_2	Pr
15	0.94
16	0.96
17	0.98
18	1

Таблица 6

$M = \mathbb{Z}_{9973}$, $\mathbb{D}$ **– нормальное распределение с** $\mu = 100$ **и** $\sigma = 500$

n_2	Pr
≥15	1

Представленные ниже табл. 7, 8 демонстрируют практически оцененную вероятность Pr успешного раскрытия ключа методом, описанным в данном и предыдущем разделах.

Таблица 7

$M = \mathbb{Z}_2$, $\mathbb{D}$ **– равномерное распределение,** $n_2 = 10$

n_1	Pr
1	0,76
2	0,83
3	0,95
4	1

Таблица 8

$M = \mathbb{Z}_3$, $\mathbb{D}$ **– нормальное распределение,** $\mu = 0$ **и** $\sigma = 2$, $n_2 = 10$

n_1	Pr
1	0,97
2	0,98
3	0,99
4	1

Замечание. В случае, когда A имеет только одну пару $(m, c(x))$, он сразу полагает $g(x) = c(x) - m$.

Для $\mathbb{Z}_n$, $n = p_1 \cdot \ldots \cdot p_t$, $p_i \neq p_j$ также можно применить описанный подход. Однако для того чтобы факторизовать полином $g(x)$, необходимо знать факторизацию n. В случае, если разложение n неизвестно и не было раскрыто в процессе вычисления $g(x)$, факторизовать $g(x)$ криптоаналитик не сможет. Поэтому после первого этапа (т.е. после вычисления $rem_i(x) = c_i^2(x) \bmod g(x), i = \overline{1, n_2}$) A в любом случае будет вынужден остановиться.

Рассмотрим вопрос о том, в каких случаях в процессе вычисления $g(x)$ обязательно будет раскрыта факторизация n (при условии, что n трудно факторизовать). Отметим, что если при шифровании выбираются полиномы $k(x)$ и $\tilde{r}(x)$ с необратимыми старшими коэффициентами, то $g(x)$ в итоге обязательно будет иметь необратимый старший коэффициент, что позволит факторизовать n. Теперь рассмотрим случай, когда шифртексты $c(x)$ имеют только обратимые старшие коэффициенты. В табл. 9 демонстрирует вероятность $\widehat{\Pr}$ того, что для $M = \mathbb{Z}_n$, $n = p \cdot q$ – 1042-битный RSA-модуль, алгоритм Евклида, применяемый последовательно для вычисления $g(x)$, раскроет p, q.

Таблица 9

Вероятность раскрытия p, q алгоритмом Евклида для $M = \mathbb{Z}_n$, где $n = p \cdot q$ – 1042-битный RSA-модуль

n_1	$\widehat{\Pr}$
2	0,006
5	0,005
10	0,008

Можно сделать вывод, что для улучшения защищенности при $M = \mathbb{Z}_n$, где n – составное и сложное для факторизации, необходимо составлять шифртексты так, чтоб их старшие коэффициенты были только обратимыми элементами.

Замечание. Все рассуждения для криптосистемы из [7] в случае составного n, очевидно, справедливы также и для криптосистемы из [8].

В свете вышесказанного может показаться, что в [7] с точки зрения защищенности предпочтительнее использовать в качестве n RSA-модуль. Однако на самом деле это справедливо, только если $n_1 = 1$. В случае $n_1 \geq 2$ при большом n вероятность того, что два случайных многочлена имеют нетривиальный НОД очень близка к нулю (см. табл. 2), т.е. с вероятностью ≈ 1 при $n_1 \geq 2$ будет выполняться $g(x) = k(x)$ с точностью до множителя. Тогда, по сути, необходимость вычисления факторизации $g(x)$ практически равна нулю.

Заключение. Проведенный анализ показал, что криптосистемы, предложенные в [7], [8] являются очень уязвимыми относительно атаки по известным открытым текстам, а как следствие и по выбранным. Для криптосистемы из [7] при $M = \mathbb{Z}_m$ (m – простое число или $p_1 \cdot \ldots \cdot p_t$, $p_i \neq p_j$), где m – небольшое

($m \geq 2$), достаточно пяти пар (открытый текст, шифртекст), чтобы раскрыть правильный секретный ключ с вероятностью ≈ 1. При условии, что пар меньше пяти, предложенный статистический подход позволяет также с вероятностью ≈ 1 раскрыть ключ, если вероятностное распределение на множестве открытых текстов достаточно отличается от равномерного (например, нормальное распределение с небольшой дисперсией).

При больших значениях m (больше 100) ключ раскрывается на первом этапе метода уже при $n_1 = 2$ с вероятностью ≈ 1 для [7]. Что касается криптосистемы из [8], то она защищена даже, если криптоаналитиком перехвачена только одна пара.

Все составные части предложенного метода криптоанализа представляют собой алгоритмы, время работы которых полиномиально от длины входа. Поэтому метод является достаточно эффективным.

Случай, когда $m = p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$, $p_i \neq p_j$, требует дальнейшего анализа в силу неоднозначности факторизации многочленов в кольце $\mathbb{Z}_m[x]$.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Gentry C.* A fully homomorphic encryption scheme: diss. – Stanford University, 2009.
2. *Van Dijk M. et al.* Fully homomorphic encryption over the integers // Advances in Cryptology–EUROCRYPT 2010. – Springer Berlin Heidelberg, 2010. – P. 24-43.
3. *Brakerski Z., Vaikuntanathan V.* Efficient fully homomorphic encryption from (standard) LWE // Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on. – IEEE, 2011. – P. 97-106.
4. *Gentry C., Sahai A., Waters B.* Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based // Advances in Cryptology–CRYPTO 2013. – Springer Berlin Heidelberg, 2013. – P. 75-92.
5. *Stehlé D., Steinfeld R.* Faster fully homomorphic encryption //Advances in Cryptology-ASIACRYPT 2010. – Springer Berlin Heidelberg, 2010. – P. 377-394.
6. *Gentry C., Halevi S.* Implementing gentry's fully-homomorphic encryption scheme // Advances in Cryptology–EUROCRYPT 2011. – Springer Berlin Heidelberg, 2011. – P. 129-148.
7. *Жиров А.О., Жирова О.В., Кренделев С.Ф.* Безопасные облачные вычисления с помощью гомоморфной криптографии // Безопасность информационных технологий. – 2013. – Т. 1. – С. 6-12.
8. *Rostovtsev A., Bogdanov A., Mikhaylov M.* Secure evaluation of polynomial using privacy ring homomorphisms // IACR Cryptology ePrint Archive. – 2011. – Vol. 2011. – P. 24.
9. *Lidl R., Niderreiter H.* Finite Fields (Vol. 20, Encyclopedia of Math. and its Appl.) // Englewood Cliffs, NJ: Addison~ lVesley. – 1983. – P. 74-85.
10. *Klivans A.* Factoring polynomials modulo composites. – CARNEGIE-MELLON UNIV PITTSBURGH PA DEPT OF COMPUTER SCIENCE, 1997. – №. CMU-CS-97-136.
11. *Benjamin A.T., Bennett C.D.* The probability of relatively prime polynomials // Mathematics Magazine. – 2007. – P. 196-202.
12. *Shoup V.* NTL: A library for doing number theory. – 2001.

REFERENCES

1. *Gentry C.* A fully homomorphic encryption scheme: diss, Stanford University, 2009.
2. *Van Dijk M. et al.* Fully homomorphic encryption over the integers, *Advances in Cryptology–EUROCRYPT 2010.* Springer Berlin Heidelberg, 2010, pp. 24-43.
3. *Brakerski Z., Vaikuntanathan V.* Efficient fully homomorphic encryption from (standard) LWE, *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on*, IEEE, 2011, pp. 97-106.
4. *Gentry C., Sahai A., Waters B.* Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based, *Advances in Cryptology–CRYPTO 2013*. Springer Berlin Heidelberg, 2013, pp. 75-92.

5. *Stehlé D., Steinfeld R.* Faster fully homomorphic encryption, *Advances in Cryptology-ASIACRYPT 2010.* Springer Berlin Heidelberg, 2010, pp. 377-394.
6. *Gentry C., Halevi S.* Implementing gentry's fully-homomorphic encryption scheme, *Advances in Cryptology–EUROCRYPT 2011.* Springer Berlin Heidelberg, 2011, pp. 129-148.
7. *Zhirov A.O., Zhirova O.V., Krendelev S.F.* Bezopasnye oblachnye vychisleniya s pomoshch'yu gomomorfnoy kriptografii, *Bezopasnost' informatsionnykh tekhnologiy*. 2013, Vol. 1, pp. 6-12.
8. *Rostovtsev A., Bogdanov A., Mikhaylov M.* Secure evaluation of polynomial using privacy ring homomorphisms, *IACR Cryptology ePrint Archive*, 2011, Vol. 2011, pp. 24.
9. *Lidl R., Niderreiter H.* Finite Fields (Vol. 20, Encyclopedia of Math. and its Appl.), *Englewood Cliffs, NJ: Addison~ lVesley*. 1983, pp. 74-85.
10. *Klivans A.* Factoring polynomials modulo composites. CARNEGIE-MELLON UNIV PITTSBURGH PA DEPT OF COMPUTER SCIENCE, 1997, No. CMU-CS-97-136.
11. *Benjamin A.T., Bennett C.D.* The probability of relatively prime polynomials, Mathematics *Magazine*, 2007, pp. 196-202.
12. *Shoup V.* NTL: A library for doing number theory, 2001.

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; тел.: 89085196604; кафедра БИТ; аспирантка.

Trepacheva Alina Viktorovna – South Federal University; e-mail: alina1989malina@ya.ru; 2, Chehova street, Taganrog, 347928, Russia; phone: +79085196604; postgraduate student.

УДК 004.056.55: 003.26

Ф.Б. Буртыка

СИММЕТРИЧНОЕ ПОЛНОСТЬЮ ГОМОМОРФНОЕ ШИФРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ НЕПРИВОДИМЫХ МАТРИЧНЫХ ПОЛИНОМОВ

Представлена новая симметричная компактная полностью гомоморфная криптосхема, основанная на использовании матричных полиномов и производящая шифрование в два раунда: сначала открытые тексты, являющиеся элементами кольца вычетов, кодируются в матрицы с помощью секретного вектора $\vec{k}$, *а затем эти матрицы отображаются в матричные полиномы с использованием секретного неприводимого матричного полинома* $\mathbf{K}(X)$. *Расшифрование также происходит в два раунда: сначала осуществляется приведение по модулю* $\mathbf{K}(X)$, *а затем умножение полученной в результате матрицы на* $\vec{k}$. *Отображение расшифрования является гомоморфизмом колец. Время работы всех алгоритмов криптосхемы зависит полиномиально от параметра защищенности* λ. *Временные издержки при её использовании для вычисления над зашифрованными данными также полиномиальны от* λ. *Введение специального ключа перешифрования, зависящего от секретного ключа, позволило добиться того, что при вычислениях над шифровками их размеры всегда остаются ограниченными фиксированным полиномом от* λ. *При практической реализации возможно эффективное распараллеливание. Проводится анализ криптостойкости предложенной криптосхемы относительно атак на основе только шифротекстов, по известным открытым текстам и на ключ перешифрования. Продемонстрировано то, что все эти атаки могут быть сведены к решению системы полиномиальных уравнений от многих переменных над кольцом вычетов. Рассматривается вопрос о сложности решения этих систем существующими методами.*

Полностью гомоморфная криптосхема; матричные полиномы; системы полиномиальных уравнений; атака по известным открытым текстам; защищённые облачные вычисления.