Алина В. Трепачева
Южный федеральный университет,
ул. Большая Садовая, 105/42, г. Ростов-на-Дону, 344006, Россия,
e-mail: alina1989malina@ya.ru, ORCID iD 0000-0001-7625-569X

О СООТНОШЕНИЯХ МЕЖДУ АТАКАМИ НА СИММЕТРИЧНЫЕ ШИФРЫ, ГОМОМОРФНЫЕ НАД КОЛЬЦОМ ВЫЧЕТОВ[1]

DOI: http://dx.doi.org/10.26583/bit.2017.2.09

Аннотация. Работа посвящена изучению криптостойкости симметричных гомоморфных шифров над кольцами вычетов. Основной задачей является выяснить, возможно ли установить эквивалентность между атакой только по шифртекстам (АТШ) и атакой по известным открытым текстам (АИОТ) для таких шифров. Для этого вводится понятие сводимости между атаками и дается достаточное условие сводимости от АТШ к АИОТ. Основная идея заключается в том, что для доказательства сводимости от АТШ к АИОТ необходимо найти функцию над кольцом вычетов, которая является эффективно вычислимой и имеет небольшой размер образа по сравнению с размером всего кольца вычетов. Исследование наличия сводимости интересно тем, что оно может позволить лучше понять уровень криптостойкости существующих симметричных гомоморфных криптосистем (ГК). Поскольку для большинства из них в литературе уже установлена уязвимость к АИОТ, то доказательство существования сводимости может показать, что эти криптосистемы не стойки даже к АТШ, а, следовательно, совсем не стойки и непригодны для применения. Приводится пример сводимости АТШ к АИОТ для случая, когда кольцо вычетов является простым полем. На основе этого примера описывается эффективная АТШ на одну симметричную ГК в случае кольца вычетов небольшого размера. Также отдельно рассматривается случай, когда кольцо вычетов для ГК строится по труднофакторизуемому модулю n. Для таких n на данный момент не известен эффективный алгоритм построения эффективно вычислимых функций с «небольшим» образом. Ввиду этого дальнейшая работа по криптоанализу существующих симметричных ГК будет направлена на изучение свойств функций над кольцами вычетов по труднофакторизуемым модулям.

Ключевые слова: гомоморфное шифрование над кольцом вычетов, полностью гомоморфное шифрование, задача RSA, задача факторизации чисел, атака только по шифртекстам, атака по известным открытым текстам.

Для цитирования. ТРЕПАЧЕВА, Алина В. О соотношениях между атаками на симметричные шифры, гомоморфные над кольцом вычетов. Безопасность информационных технологий, [S.l.], v. 24, n. 2, p. 82-91, june 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/108>. Дата доступа: 23 june 2017. doi:http://dx.doi.org/10.26583/bit.2017.2.09.

[1] ***Благодарности:*** Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 15-07-00597 А

Alina V. Trepacheva
Southern Federal University,
Bolshaya Sadovaya St., 105/42 Rostov-on-Don, 344006, Russia
e-mail: alina1989malina@ya.ru, ORCID iD 0000-0001-7625-569X

On the relations between the attacks on symmetric homomorphic encryption over the residue ring[1]

DOI: http://dx.doi.org/10.26583/bit.2017.2.09

Abstract. The paper considers the security of symmetric homomorphic cryptosystems (HC) over the residue ring. The main task is to establish an equivalence between ciphertexts only attack (COA) and known plaintexts attack (KPA) for HC. The notion of reducibility between attacks

and sufficient condition of reducibility from COA to KPA are given for this purpose. The main idea is: to prove reducibility from COA to KPA we need to find a function over residue ring being efficiently computable and having a small image size comparing with the size of residue ring. The study of reducibility existence is important since it allows to understand better the security level of symmetric HC proposed in literature. A vulnerability against KPA has been already found for the majority of these HC. Thus the reducibility presence can demonstrate that cryptosystems under the study are not secure even against COA, and therefore they are totally insecure and shouldn't be used in practice. We give an example of reducibility from COA to KPA for residue ring being a simple field. Based on this example we show an efficient COA on one symmetric HC for small field. Also we separately consider the case of residue ring composed using number n being hard-to-factor. For such n an efficient algorithm to construct an efficiently computable function with small image is unknown so far. So further work related to cryptanalysis of existing symmetric HC will be directed into study of functions properties over residue rings modulo numbers hard for factorization.

Keywords: ring-homomorphic encryption, fully homomorphic encryption, RSA problem, number factorization problem, ciphertexts only attack, known plaintext attack.

For citation. TREPACHEVA, Alina V. On the Relations between the Attacks on Symmetric Homomorphic Encryption over the Residue Ring. IT Security (Russia), [S.l.], v. 24, n. 2, p. 82-91, june 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/108>. Date accessed: 23 june 2017. doi:http://dx.doi.org/10.26583/bit.2017.2.09.

Acknowledgements: This ***w***ork is executed at financial support RFBR, research project No. 15-07-00597 A.

Введение

Эффективное и криптостойкое полностью гомоморфное шифрование (ПГШ) дает принципиально новые возможности по обеспечению информационной безопасности в таких областях как облачные вычисления, обработка медицинских и финансовых данных, поскольку позволяет проводить любые вычисления над данными в зашифрованном виде без знания ключа расшифрования в недоверенной среде [1]. Именно поэтому интерес к ПГШ в последние годы все больше возрастает. Предложено уже большое количество полностью гомоморфных криптосистем (ПГК). Одним из наиболее популярных направлений в этой области является построение ПГК с открытым ключом [2,3], основанных на теории решеток. Родоначальником этого направления была ПГК из работы [3], разработанная Джентри в 2009 году. Достоинством этих ПГК является строго доказуемая криптостойкость против атаки по выбранным открытым текстам (АВОТ). Однако на практике их применение на данный момент весьма ограничено из-за того, что вычисления над зашифрованными данными сильно усложняются по сравнению с вычислениями над исходными данными [1].

Вследствие этого было предложено большое количество альтернативных вариантов симметричных гомоморфных криптосистем (ГК) над кольцами вычетов [4-15]. Особенно активны попытки построить симметричные ПГК, криптостойкость которых основывалась бы некоторым образом на задаче факторизации больших чисел [5-14], являющейся эталоном сложной задачи в компьютерной безопасности [16]. Некоторые из ГК [4-15] даже были использованы в реальных приложениях. К примеру, авторы [5] использовали свою ПГК для защиты облачной БД [17], а ГК из работ [12,15] были использованы для защиты данных в беспроводных сенсорных сетях [18,19].

Однако строгое обоснование защищенности ни для одной ГК из работ [4-15] не было приведено. Проведенный в работах [20-29] криптоанализ показал нестойкость ГК [4-13,15] к атаке по известным открытым текстам (АИОТ). Как следствие, к примеру, в работе [30] было выявлено, что защищенная БД из [17] имеет уязвимость.

Но вопрос о криптостойкости относительно атаки только по шифртекстам (АТШ) не был изучен в полной мере. Целью данной работы является предложить метод анализа

криптостойкости к АТШ указанных симметричных криптосистем, гомоморфных над кольцами вычетов. Основная идея этого метода – попробовать свести АТШ к АИОТ.

Вводные замечания и обозначения

Определение 1. Гомоморфной над кольцом криптосистемой (ГКК, англ. ring-homomorphic encryption) называют криптосистему, у которой множество открытых текстов P имеет алгебраическую структуру кольца и обладающую свойствами:

$$D\big(E(m_1)\oplus E(m_2)\big) = m_1 + m_2, \quad (1)$$
$$D\big(E(m_1)\odot E(m_2)\big) = m_1 \cdot m_2, \quad (2)$$

где E – функция шифрования, D – функция расшифрования, $\oplus,\odot$ – операции над кольцом шифртекстов C, $+$, $\cdot$ – операции над кольцом открытых текстов P.

Гомоморфный шифр называется *компактным*, если размер шифртекста, получающегося в результате проведения вычислений, ограничен некоторым числом, полиномиальным от параметров шифра.

ПГК является компактной гомоморфной ГКК, а также должно выполняться, что $\oplus,\odot$ можно вычислить над шифртекстами любое число раз корректно и эффективно.

В данной работе будут рассматриваться ГКК, для которых $P = \mathbb{Z}_n, n \in \mathbb{N}, n > 1$.

Определение 2. Эффективно вычислимой над $\mathbb{Z}_n$ функцией будем называть функцию, которую можно вычислить за $O(\log n)$ операций $+$, $\cdot$ кольца $\mathbb{Z}_n$.

Простейшими примером эффективно вычислимой функций над $\mathbb{Z}_n$ является полином $(x + c)^n$, т.к. существуют алгоритмы, которые могут возвести в степень n за $\log_2 n$ шагов (например, т.н. алгоритмы двоичного возведения в степень [31]).

Будем обозначать образ функции $f(x)$ на множестве S как $\mathrm{Im}(f(S))$, а количество элементов в этом образе как $|\mathrm{Im}(f(S))|$.

Основные типы атак на криптосистемы и определение сводимости

Известно, что существуют три основных типа атак на криптосистемы [32]:

1) АТШ (ciphertexts-only attack), подразумевающая что криптоаналитику доступны только шифртексты, изготовленные на одном ключе;

2) АИОТ (known-plaintexts attack), в которой криптоаналитик перехватил пары $(m_1, E(m_1)), \dots, (m_s, E(m_s))$, изготовленные на одном ключе;

3) АВОТ (chosen-plaintexts attack), предполагающая что криптоаналитик имеет доступ к шифрующему устройству и может зашифровать выбранные по своему усмотрению открытые тексты, т.е. может получить пары $(m_1, E(m_1)), \dots, (m_s, E(m_s))$ для выбранных m_i.

Есть также и другие виды атак, но здесь мы опускаем их описание.

Для криптосистем с открытым ключом наиболее актуально обоснование криптостойкости относительно АВОТ, поскольку получение пар «открытый текст – шифртекст» общедоступно. Поэтому для ПГК с открытым ключом [2,3] обычно доказывают АВОТ-стойкость. Для симметричных же криптосистем имеет смысл рассматривать стойкость против АТШ и АИОТ отдельно. В частности, анализируемые в данной работе ГКК [4-15], как уже упоминалось, симметричны.

Атаку на криптосистему можно рассматривать как алгоритмическую задачу [33] и в этом случае можно рассмотреть вопрос о сводимости одной атаки к другой.

Определение 3. Сводимость атаки $\mathcal{A}$ к атаке $\mathcal{B}$ – это эффективно вычислимая функция, которая преобразует исходные данные для атаки $\mathcal{A}$ в исходные данные для атаки $\mathcal{B}$.

Для любой криптосистемы есть тривиальные сводимости: АИОТ → АТШ, АВОТ → АИОТ. Однако в случае гомоморфных шифров могут иметь место и обратные сводимости, которые сделают некоторые атаки эквивалентными для ГШ. В частности, исследование наличия сводимости АТШ → АИОТ для ранее упомянутых ГКК [4-15] может позволить ответить на вопрос об их защищенности относительно АТШ.

Пример сводимости АТШ к АИОТ для случая, когда пространство открытых текстов – кольцо вычетов по модулю простого числа

Проанализируем сводимость АТШ к АИОТ на ГКК для случая $P = \mathbb{Z}_p$, где p – простое число. Как известно, по теореме Эйлера выполняется $\forall m \in \mathbb{Z}_p: m^p - m = 0(mod\ p)$. Поэтому, пользуясь гомоморфными свойствами шифра, криптоаналитик может составить функцию $f(x) = x^p - x$, благодаря которой он может превратить АТШ в АИОТ. Для этого ему достаточно подставить любой шифртекст в f и он получит шифртекст нуля.

Рассмотрим этот процесс более подробно на примере ГКК [4], для которой $P = \mathbb{Z}_p$. Шифрование в [4] сводится к формуле $c(x) = m + k(x) \cdot r(x) \in \mathbb{Z}_p[x]$, где $m \in \mathbb{Z}_p$ – открытый текст, $k(x) \in \mathbb{Z}_p[x]$ – секретный ключ, $r(x) \in \mathbb{Z}_p[x]$ – случайный полином, полученный по равномерному распределению, $\deg(k), \deg(r) > 0$. Основная идея АИОТ на [4], описанной в [22,23], следующая: пусть криптоаналитик перехватил пары $(m_1, c_1(x)), \dots, (m_s, c_s(x))$, зашифрованные на $k(x)$; тогда для раскрытия $k(x)$ он может вычислить $g(x) = \text{НОД}(c_1(x) - m_1, \dots, c_s(x) - m_s)$. В силу случайности $r_i(x)$ полином $g(x)$ с вероятностью ≈ 1 равен $k(x)$ для небольших значений s. К примеру, для $\mathbb{Z}_2$ достаточно взять $s > 5$.

На число p в [4] не накладывается ограничений. Рассмотрим случай, когда p – простое. Предположим криптоаналитик имеет $c_1(x), \dots, c_s(x)$, изготовленные на $k(x)$, и знает p. Он может вычислить $c_i'(x) = (c_i(x))^p - c_i(x),\ i = 1, \dots, s$ и это даст ему пары для АИОТ $(0, c_1'(x)), \dots, (0, c_s'(x))$.

Однако необходимо отметить, что вероятностное распределение шифртекстов $c_i'(x)$ отлично от того, по которому получаются «свежие» шифртексты (произведенные непосредственно алгоритмом зашифрования). Имеем

$$c_i'(x) = (c_i(x))^p - c_i(x) = k(x) \cdot r_i(x) \cdot ((k(x) \cdot r_i(x))^{p-1} - 1).$$

Полином данного вида будет нацело делиться на $x^p - x$ для любых $k(x), r_i(x)$. Однако, для «свежих» шифртекстов такое свойство выполняться не будет.

АИОТ из [22,23], описанная ранее, была рассчитана именно на «свежие» шифртексты. В данном же случае в неё необходимо внести поправку. Полином $g(x)$ необходимо разделить на $x^p - x$, т.е. провести нормировку $g(x)$. В результате мы получим $k(x)$, если $k(x)$ не имеет линейных сомножителей. Если же имеет, то мы получим некоторый сомножитель $k(x)$, но, очевидно, и его достаточно для взлома ГКК [4]. Описанные выше действия формализованы в виде *Алгоритма 1*.

Алгоритм 1 CoaAdHoc($c_1, \dots, c_t$)

Вход: «свежие» шифртексты $c_1(x), \dots, c_s(x)$ ГКК [4], простое число p
Выход: $k(x)$ или его множитель
1: **for** *i=1* to *s* **do**
2: $c_i^*(x) := (c_i(x))^p - c_i(x)$
3: **end for**
4: **return** НОД$(c_1^*(x), \dots, c_s^*(x))/(x^p - x)$

Рассмотрим теперь вопрос об эффективности алгоритма 1. Функция $f(x) = x^p - x$ является эффективно вычислимой над $\mathbb{Z}_p$ для любого p. Однако описанная ГКК некомпактна, т.к. при умножении размеры шифртекстов растут с экспоненциальной скоростью. Поэтому для больших p эта атака не будет эффективна. Для того чтобы получить эффективную атаку для любого p необходима функция f, имеющая небольшую степень, к примеру $log_2 p$.

В случае, когда $P = \mathbb{Z}_n$ и n – составное число, можно использовать функцию $f(x) = x^{\varphi(n)} - x$, где $\varphi(n)$ – функция Эйлера. Если n – небольшое легко факторизуемое число, то мы снова получаем эффективную атаку на ГКК [4]. Если же n трудно факторизуемо, то так действовать не получится, поскольку вычисление $\varphi(n)$ будет трудной задачей.

Обобщение идеи о сводимости АТШ к АИОТ

Итак, как видно из примера в предыдущем разделе, для получения сводимости АТШ → АИОТ была использована функция $f: P \to P$, которая отображает любой открытый текст $m \in P$ в одно фиксированное значение, т.е. $|\mathrm{Im}(f(P))| = 1$. *Однако, в общем, для получения сводимости атаки может быть достаточно, чтобы выполнялось соотношение* $|Im(f(P))| \ll |P|$. *И тогда полный перебор элементов* $Im(f)$ *не затруднит атаку.*

Определение 4. Назовем функцию $f: P \to P$ σ - *логарифмически сжимающей*, если $|\mathrm{Im}(f(P))| < \sigma \cdot \log_2 |P|$, т.е. количество элементов в её образе не превышает двоичного логарифма от общего количества элементов в P, умноженного на константу $\sigma \in \mathbb{R}$, где $\sigma \ll |P|$

В качестве примера приведем σ - логарифмически сжимающую функцию над $\mathbb{Z}_6$ -- полином $f(x) = x^2 + x + 1$ переводит элементы $\mathbb{Z}_6$ в два элемента: 1 и 3.

Также для наших целей подойдет не только функция «гарантированно» отправляющая все элементы P в «небольшой» образ, но и функция, которая «с большой вероятностью» отправляет их туда.

Определение 5. Назовем функцию $f: P \to P$ Ω - *вероятностно* σ - *логарифмически сжимающей*, если существует такое подмножество элементов $S \subseteq P$, $|S| > \Omega \cdot |P|$ что $|\mathrm{Im}(f(S))| < \sigma \cdot \log_2 |P|$, $\sigma, \Omega \in \mathbb{R}$, $0 < \Omega \leq 1$.

Заметим, что σ – логарифмически сжимающая функция является частным случаем P Ω - вероятностно σ - логарифмически сжимающей для $\Omega = 1$.

Основные теоремы о достаточном условии эквивалентности АИОТ и АТШ для АГК сформулируем уже для $P = \mathbb{Z}_n$, $n \in \mathbb{N}, n > 1$.

Теорема 1. Если существует алгоритм, работающий на всех входах за не более чем $O(\log_2 n)$ шагов, который для заданного пространства открытых текстов $\mathbb{Z}_n$ некоторой ГКК, возможно не обладающей свойством компактности, и некоторого σ выдает Ω-

вероятностно σ - логарифмически сжимающую функцию $f: \mathbb{Z}_n \to \mathbb{Z}_n$ с $\Omega \approx 1$, выражаемую полиномом степени не более $O(\log_2 n)$, то АТШ и АИОТ на эту ГКК эквивалентны.

Теорема 2. Если существует алгоритм, работающий на всех входах за не более чем $O(\log n)$ шагов, который для заданного пространства открытых текстов $\mathbb{Z}_n$ некоторой ПГК, и некоторого σ выдает эффективно вычислимую Ω-вероятностно σ-логарифмически сжимающую функцию $f: \mathbb{Z}_n \to \mathbb{Z}_n$ с $\Omega \approx 1$, то АТШ и АИОТ на эту ГКК эквивалентны.

Для иллюстрации теорем приведен общий алгоритм CoaHom$(c_1, \dots, c_s)$ для осуществления АТШ на ГКК посредством сведения к АИОТ с применением σ - логарифмически сжимающей функции $f: \mathbb{Z}_n \to \mathbb{Z}_n$.

Алгоритм 2 CoaHom$(c_1, \dots, c_s)$

Вход: шифртексты $c_1, \dots, c_s$ криптосистемы, произведенные на одном ключе; s – число пар «открытый текст, шифртекст», необходимых для АИОТ; функция f
Выход: секретный ключ sk в случае успешной атаки
1: **for** *i=1* to *s* **do**
2: $c_i^* := f(c_i)$
3: **end for**
4: **for** $(p_1, \dots, p_s) \in Im(f) \times \dots \times Im(f)$ **do**
5: sk′ = АИОТ $((p_1, c_1^*), \dots, (p_s, c_s^*))$
5: **if** АИОТ $((p_1, c_1^*), \dots, (p_s, c_s^*))$ прошла успешно **then**
6: sk = Normalize(sk′)
7: **return** sk
8: **end if**
9: **end for**

Функция Normalize, упомянутая в алгоритме, необходима для нормализации результата АИОТ атаки. Она может быть нужна, если в результате применения функции f к шифртекстам поменяются их вероятностные распределения из-за чего у них появятся дополнительные свойства и закономерности. В общем случае функция Normalize будет существенно зависеть от вида функции f и самой ГКК. Для примера, рассмотренного в предыдущем разделе, Normalize реализовывалась делением результата АИОТ на полином $x^p - x$.

тметим также, что критерий того, что АИОТ прошла успешна в общем случае тоже сформулировать затруднительно, т.к. он зависит от ГКК и, возможно, самой АИОТ. В качестве примера рассмотрим случай, когда $P = \mathbb{Z}_n$, где n – труднофакторизуемый RSA-модуль. Опираясь на существующий опыт по проведению АИОТ на ГКК с таким P [20-25], можно сказать, что в этом случае критерием успеха атаки может, к примеру, служить раскрытие факторизации числа n.

Напоследок отметим, что общая асимптотическая сложность алгоритма $CoaHom(c_1, \dots, c_s)$ составляет $\approx O(\log_2^s n) \cdot Complexity_{\text{АИОТ}}$.

О сводимости АТШ к АИОТ для случая, когда пространство открытых текстов – кольцо вычетов по модулю труднофакторизуемого числа

Большая часть существующих симметричных ГКК [5-14], как уже отмечалось, построена таким образом, что их защищенность пытаются обосновать с привлечением классической и хорошо изученной трудной задачи факторизации больших чисел. Эти ГКК взламываются при факторизации некоторого числа n, входящего в их конструкцию. Хотя

строгая сводимость криптостойкости к этой задаче ни в одной из указанных работ не была установлена и факторизация n не является необходимым условием для их взлома (по крайней мере для АИОТ это уже известно точно согласно работам по их криптоанализу [20-27]).

Однако актуальность построения доказуемо стойкого и эффективного полностью гомоморфного шифра на основе задачи факторизации по-прежнему не теряет смысла и актуальности, поскольку в работе [34] было предъявлено доказательство того, что теоретически возможно построить АТШ-криптостойкую ГКК над $\mathbb{Z}_n$, основанную на задаче факторизации n.

Существующие ГКК, связанные с задачей факторизации чисел (ФГГК), можно условно классифицировать по структуре их пространств открытых текстов на 2 группы:

1) $P = \mathbb{Z}_n$, где $n = p \cdot q$ – труднофакторизуемое число, p, q – большие криптографически стойкие, простые числа [6-14];
2) $P = \mathbb{Z}_p$, однако $n = p \cdot q$ также используется в алгоритме шифрования [5].

Для ФГКК 2-го типа из работы [5] была показана её нестойкость к АИОТ в [20]. Однако, применение описанной выше концепции для анализа её стойкости к АТШ выглядит на данный момент затруднительно, поскольку фактически авторы [5] скрывают P, нарушая тем самым принцип Керхгоффса. И пока не вполне ясно, как можно было бы построить необходимую для сводимости сжимающую функцию $f: P \to P$ в предположении, что криптоаналитику не известно P.

Для ФГКК 1-го типа σ - логарифмически сжимающую функцию можно построить, например, с помощью интерполяции. Однако, возможно, что степень полинома, реализующего эту функцию, будет слишком большой и как следствие вычисление функции будет неэффективно. Можно также действовать и полным перебором, однако это неэффективно. Пытаться получить такую функцию, случайно выбрав некоторый полином, также представляется неэффективным подходом, хотя данный вопрос требует отдельного подробного изучения (в частности, проведение компьютерных экспериментов для небольших n с вычислением процента сжимающих функций над $\mathbb{Z}_n$ по сравнению с общим числом функций над $\mathbb{Z}_n$). Итого, вопрос об эффективном алгоритме построения эффективно вычислимых логарифмически сжимающих функций для произвольного труднофакторизуемого числа n на данный момент является открытым и требует дальнейшего изучения.

Заключение

Проведено исследование, устанавливающее взаимосвязь между атаками только по шифртекстам и по известным открытым текстам на шифры, гомоморфные над кольцом вычетов $\mathbb{Z}_n$. Установлено, что вопрос об эквивалентности этих атак можно свести к поиску семейства сжимающих функций над $\mathbb{Z}_n$, а также эффективного алгоритма, который для каждого $\mathbb{Z}_n$ предъявляет такую функцию.

В случае построения эффективного алгоритма нахождения сжимающих функций над $\mathbb{Z}_n$, где $n = p \cdot q$ – труднофакторизуемое число, можно будет сделать окончательные выводы о криптостойкости гомоморфных шифров из работ [6-13] к атаке только по шифртекстам. Поэтому дальнейшая работа по криптоанализу этих ГКК будет направлена на изучение свойств функций над $\mathbb{Z}_n$.

СПИСОК ЛИТЕРАТУРЫ:

1. Бабенко Л. К., Буртыка Ф. Б., Макаревич О. Б., Трепачева А. В. Полностью гомоморфное шифрование (обзор). Вопросы защиты информации. 2016, № 3, С. 3–25.
2. Gentry, Craig. "Fully homomorphic encryption using ideal lattices." STOC. Vol. 9. No. 2009. 2009.

3. Vaikuntanathan, V. Computing blindfolded: New developments in fully homomorphic encryption. Proceedings of IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS), 2011.
4. Жиров А. О., Жирова О. В., Кренделев С. Ф. Безопасные облачные вычисления с помощью гомоморфной криптографии. Безопасность информационных технологий, № 1, 2013. С. 6-12.
5. Zhirov A., Zhirova O, Krendelev S. Practical fully homomorphic encryption over polynomial quotient ring. Proceedings of World congress on internet security (WorldCIS), IEEE. 2013, С. 70-75. DOI: 10.1109/WorldCIS.2013.6751020
6. Ростовцев А., Богданов А., Михайлов М. Метод безопасного вычисления полинома в недоверенной среде с помощью гомоморфизмов колец. Проблемы информационной безопасности. Компьютерные системы. 2011. № 2. С. 76-85.
7. Yagisawa M. Fully Homomorphic Encryption with Composite Number Modulus. IACR Cryptology ePrint Archive. 2015. № 1040. URL: https://eprint.iacr.org/2015/1040.pdf (дата обращения: 25.01.2017).
8. Kipnis A., Hibshoosh E. Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification. IACR Cryptology ePrint Archive. 2012. № 637. URL: https://eprint.iacr.org/2012/637.pdf (дата обращения: 25.01.2017).
9. Xiao L., Bastani O., Yen I. L. An Efficient Homomorphic Encryption Protocol for Multi-User Systems. IACR Cryptology ePrint Archive. 2012. №. 193 URL: https://eprint.iacr.org/2012/193.pdf (дата обращения: 22.01.2017).
10. Gupta C. P., Sharma I. Department of Computer Sciences and Engineering Rajasthan Technical University, Kota, India. Network of the Future (NOF), 2013 Fourth International Conference on the. – IEEE, 2013. С. 1-4.
11. Gupta C. P. Fully Homomorphic Encryption Scheme with Symmetric Keys : дис. – Department of Computer Science & Engineering University College of Engineering, Rajasthan Technical University, Kota, 2013
12. J. Domingo-Ferrer, A new privacy homomorphism and applications, Information Processing Letters, vol. 60, no. 5, С. 277–282, 1996.
13. Chan A. C. F. Symmetric-key homomorphic encryption for encrypted data processing. Communications, 2009. ICC'09. IEEE International Conference on. – IEEE, 2009. – С. 1-5.
14. Gavin G. A general framework for building noise-free homomorphic cryptosystems. IACR Cryptology ePrint Archive. 2015. № 821. URL: https://eprint.iacr.org/2015/821.pdf (дата обращения: 25.01.2017).
15. J. Domingo-Ferrer, A provably secure additive and multiplicative privacy homomorphism. Information Security. 2002, С.471–483.
16. Rivest R. L., Kaliski Jr B. RSA problem. Encyclopedia of cryptography and security. – Springer US, 2011. – С. 1065-1069.
17. Shatilov K., Boiko V., Krendelev S., Anisutina D., Sumaneev A. Solution for secure private data storage in a cloud. Proceedings of Federated Conference on Computer Science and Information Systems (FedCSIS), IEEE, 2014, С. 885-889. DOI: 10.15439/2014F43
18. Ertaul L., Yang J. H. Implementation of Domingo-Ferrer's a new privacy homomorphism (df a new ph) in securing wireless sensor networks (wsn). Security and Management. Citeseer, 2008, С. 498–504.
19. Jariwala V., Jinwala D. Evaluating homomorphic encryption algorithms for privacy in wireless sensor networks. International Journal of Advancements in Computing Technology, vol. 3, no. 6, 2011.
20. Трепачева А.В. О криптоанализе одной полностью гомоморфной криптосистемы на основе задачи факторизации. Безопасность информационных технологий. 2015, № 4, С. 19-25
21. Трепачева А.В. Улучшенная атака по известным открытым текстам на гомоморфную криптосистему Доминго-Феррера. Труды Института системного программирования Российской академии наук. 2014. Том 25, Вып. 5. С. 83-98. DOI: 10.15514/ISPRAS-2014-26(5)-4
22. Трепачева А. В. Криптоанализ шифров, основанных на гомоморфизмах полиномиальных колец. Известия Южного федерального университета. Технические науки, том 157, №. 8, С. 96-107, 2014.
23. Trepacheva A., Babenko L. Known plaintexts attack on polynomial based homomorphic encryption. Proceedings of the 7th International Conference on Security of Information and Networks. – ACM, 2014. – С. 157.
24. Трепачева А.В. Криптоанализ симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел. Известия Южного федерального университета. Технические науки № 5 (том 166) (2015).

25. Трепачева А.В. Криптоанализ полностью гомоморфных криптосистем, основанных на алгебре октонионов. Обозрение прикладной и промышленной математики 23(4) 2016
26. Vizár D., Vaudenay S. Analysis of Chosen Symmetric Homomorphic Schemes. Central European Crypto Conference. – 2014. – №. EPFL-CONF-198992.
27. Tsaban B., Lifshitz N. Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme. Journal of Mathematical Cryptology. – 2014.
28. Cheon J. H., Kim W.-H., Nam H. S. Known-plaintext cryptanalysis of the Domingo-Ferrer algebraic privacy homomorphism scheme. Information Processing Letters, vol. 97, no. 3, C. 118–123, 2006.
29. Wagner, Cryptanalysis of an algebraic privacy homomorphism. Information Security. Springer, 2003, C. 234–239.
30. Бабенко Л.К., Трепачева А.В. Анализ защищенности одной криптографической системы для защиты конфиденциальности данных в облачных вычислениях. Безопасность информационных технологий. 2016, № 1, С. 11-15
31. Gordon D. M. A survey of fast exponentiation methods. Journal of algorithms. – 1998. – Т. 27. – №. 1. – С. 129-146.
32. Goldreich, O. Foundations of Cryptography–A Primer. Foundations and Trends® in Theoretical Computer Science 1.1 (2005): 1-116.
33. Гэри, М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. Москва: Мир, 1982. С. 416.
34. Altmann K., Jager T., Rupp A. On black-box ring extraction and integer factorization. International Colloquium on Automata, Languages, and Programming. 2008. C. 437-448. DOI : 10.1007/978-3-540-70583-3_36.

REFERENCES:

[1] Babenko L. K., Burtica F. B., Makarevich O. B., Trubacheva A. V. Fully homomorphic encryption (review). Problems of information security. 2016, no. 3, Pp. 3-25. (in Russian).
[2] Gentry, Craig. "Fully homomorphic encryption using ideal lattices." STOC. Vol. 9. No. 2009. 2009.
[3] Vaikuntanathan, Vinod. "Computing blindfolded: New developments in fully homomorphic encryption." Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on. IEEE, 2011.
[4] A. O. Zhirov, O. V. Zhirova, and S. F. Krendelev. Secure cloud computing using homomorphic cryptography. Security of information technologies, № 1, 2013. C. 6-12. (in Russian)
[5] Zhirov A., Zhirova O, Krendelev S. Practical fully homomorphic encryption over polynomial quotient ring. World congress on internet security (WorldCIS), IEEE. 2013, C. 70-75. DOI: 10.1109/WorldCIS.2013.6751020
[6] A. B. Alexander Rostovtsev and M. Mikhaylov. Secure evaluation of polynomial using privacy ring homomorphisms. Cryptology ePrint Archive, Report 2011/024, 2011. http://eprint.iacr.org/
[7] Yagisawa M. Fully Homomorphic Encryption with Composite Number Modulus. IACR Cryptology ePrint Archive. 2015. № 1040. URL: https://eprint.iacr.org/2015/1040.pdf (дата обращения: 25.01.2017).
[8] Kipnis A., Hibshoosh E. Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification. IACR Cryptology ePrint Archive. 2012. № 637. URL: https://eprint.iacr.org/2012/637.pdf (дата обращения: 25.01.2017).
[9] Xiao L., Bastani O., Yen I. L. An Efficient Homomorphic Encryption Protocol for Multi-User Systems. IACR Cryptology ePrint Archive. – 2012. – №. 193
[10] Gupta C. P., Sharma I. Department of Computer Sciences and Engineering Rajasthan Technical University, Kota, India. Network of the Future (NOF), 2013 Fourth International Conference on the. – IEEE, 2013. – C. 1-4.
[11] Gupta C. P. Fully Homomorphic Encryption Scheme with Symmetric Keys : дис. – Department of Computer Science & Engineering University College of Engineering, Rajasthan Technical University, Kota, 2013
[12] J. D. i. Ferrer, “A new privacy homomorphism and applications,”Information Processing Letters, vol. 60, no. 5, pp. 277–282, 1996.
[13] Chan A. C. F. Symmetric-key homomorphic encryption for encrypted data processing. Communications, 2009. ICC'09. IEEE International Conference on. – IEEE, 2009. – P. 1-5.

[14] Gavin G. A general framework for building noise-free homomorphic cryptosystems. IACR Cryptology ePrint Archive. 2015. № 821. URL: https://eprint.iacr.org/2015/821.pdf (дата обращения: 25.01.2017).
[15] J. Domingo-Ferrer, “A provably secure additive and multiplicative privacy homomorphism*,” in Information Security. Springer, 2002, pp.471–483.
[16] Rivest R. L., Kaliski Jr B. RSA problem. Encyclopedia of cryptography and security. – Springer US, 2011. – С. 1065-1069.
[17] Shatilov K., Boiko V., Krendelev S., Anisutina D., Sumaneev A. Solution for secure private data storage in a cloud. Federated Conference on Computer Science and Information Systems (FedCSIS), IEEE, 2014, С. 885-889. DOI: 10.15439/2014F43.
[18] L. Ertaul and J. H. Yang, “Implementation of domingo ferrer’s a new privacy homomorphism (df a new ph) in securing wireless sensor networks (wsn).” in Security and Management. Citeseer, 2008, pp. 498–504.
[19] V. Jariwala and D. Jinwala, “Evaluating homomorphic encryption algorithms for privacy in wireless sensor networks,” International Journal of Advancements in Computing Technology, vol. 3, no. 6, 2011.
[20] Trepacheva A.V. On the cryptanalysis of a fully homomorphic cryptosystem based on the problem of factorization. Security of information technologies. 2015, № 4, p. 19-25 (in Russian).
[21] Trepacheva A.V. Improved attack known open texts on the homomorphic cryptosystem, Domingo-Ferrer.Proceedings of Institute for system programming of the Russian Academy of Sciences. 2014. Volume 25, Issue. 5. S. 83-98. DOI: 10.15514/ISPRAS-2014-26(5)-4 (in Russian).
[22] Trepacheva A. V. Cryptanalysis of ciphers based on the homomorphisms of polynomial rings. News of southern Federal University. Engineering science, volume 157, No.. 8, pp. 96-107, 2014. (in Russian).
[23] Trepacheva A., Babenko L. Known plaintexts attack on polynomial based homomorphic encryption. Proceedings of the 7th International Conference on Security of Information and Networks. – ACM, 2014. – С. 157.
[24] Trepacheva A.V. Cryptanalysis of symmetric linear fully homomorphic public key cryptosystems based on the problem of factorization of numbers. News of southern Federal University. Technical Sciences, No. 5 (volume 166) (2015). (in Russian).
[25] Trepacheva A.V. Cryptanalysis of a fully homomorphic public key cryptosystems based on algebra of octonions. Review of applied and industrial mathematics 23(4) 2016 (in Russian).
[26] Vizár D., Vaudenay S. Analysis of Chosen Symmetric Homomorphic Schemes. Central European Crypto Conference. – 2014. – №. EPFL-CONF-198992.
[27] Tsaban B., Lifshitz N. Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme. Journal of Mathematical Cryptology. – 2014.
[28] J. H. Cheon, W.-H. Kim, and H. S. Nam, “Known-plaintext cryptanalysis of the domingo-ferrer algebraic privacy homomorphism scheme,” Information Processing Letters, vol. 97, no. 3, pp. 118–123, 2006.
[29] Wagner, “Cryptanalysis of an algebraic privacy homomorphism,” inInformation Security. Springer, 2003, pp. 234–239.
[30] Babenko L.K., Trepacheva A.V. Security analysis of a single cryptographic system to protect data privacy in cloud computing. Security of information technologies. 2016, no. 1, Pp. 11-15 (in Russian).
[31] Gordon D. M. A survey of fast exponentiation methods. Journal of algorithms. – 1998. – Т. 27. – №. 1. – С. 129-146.
[32] Goldreich, Oded. "Foundations of Cryptography–A Primer." Foundations and Trends® in Theoretical Computer Science 1.1 (2005): 1-116.
[33] Gari, M., and D. Dzhonson. Computers and trudnoreshaemyh tasks. Moscow: Mir, 1982. S. 416. (in Russian).
[34] Altmann K., Jager T., Rupp A. On black-box ring extraction and integer factorization. International Colloquium on Automata, Languages, and Programming. 2008. С. 437-448. DOI : 10.1007/978-3-540-70583-3_36

Поступила в редакцию – 22 февраля июля 2017 г. Окончательный вариант – 23 мая 2017 г.
Received – February 22, 2017. The final version – May 23, 2017.