A.V. Trepacheva

About Cryptanalysis of One Fully Homomorphic Cryptosystem Based on Factorization Problem

Key words: fully homomorphic cryptosystem, known plaintext attack, big integer factorization problem.

We present a known plaintext attack (KPA) on a recently proposed fully homomorphic cryptosystem (FHC), based on the problem of big integers factoring. We show that the considered FHC is insecure against KPA even if only one pair (plaintext, ciphertext) was intercepted by an adversary. The complexity of the proposed KPA depends polynomially on the parameters of FHC and logarithmically on the size of plaintexts space. Also we discuss how ciphertexts only attack (COA) on this FHC may be reduced to KPA.

Трепачева А.В.

О КРИПТОАНАЛИЗЕ ОДНОЙ ПОЛНОСТЬЮ ГОМОМОРФНОЙ КРИПТОСИСТЕМЫ НА ОСНОВЕ ЗАДАЧИ ФАКТОРИЗАЦИИ[1]

Введение

ПГК – это криптосистема, разрешающая вычисление произвольной функции $f(x_1,...,x_t)$ над зашифрованными аргументами $\{c_1 = \mathrm{Enc}(m_1),...,c_t = \mathrm{Enc}(m_t)\}$ без знания ключа расшифрования sk. Владелец sk может извлечь результат вычислений $f(m_1,...,m_t)$, расшифровав $c = f(c_1,...,c_t)$. Это свойство делает ПГК важным средством для защиты данных в облачных серверах. Клиент, не имеющий больших вычислительных ресурсов, может зашифровать свои данные с помощью ПГК и делегировать вычисления над ними мощному серверу, не беспокоясь о нарушении конфиденциальности данных. Первая ПГК была предложена в 2009 году в [1]. Было доказано, что АИО на нее не легче, чем поиск короткого вектора решетки, что является NP-трудной задачей. Также было доказано, что издержки вычисления над зашифрованными данными полиномиальны от параметров ПГК. Однако несмотря на это, ее оказалось невозможно использовать на практике. В последующих работах эффективность ПГК [1] была улучшена. Однако на сегодняшний день она по-прежнему непрактична. Новейшие версии преобразуют 4 MB данных в 73 TB зашифрованных данных (при необходимом уровне криптостойкости) [2], что является неприемлемым на практике. В силу этого за последнее время было предложено много альтернативных ПГК, не использующих метод из [1]. В данной работе проводится анализ криптостойкости одной из таких ПГК – криптосистемы из работы [3]. Актуальность этого исследования объясняется тем, что авторы использовали ее для реализации защищенной БД [4].

В конструкции ПГК [3] использован экземпляр задачи факторизации трудно факторизуемого целого числа. На основании этого в [3] предположено, что ПГК будет защищена против АИО и АТШ. Однако строгого доказательства представлено не было. И на самом деле, как было выяснено, ПГК [3] не защищена против АИО. Также установлено, что она не является стойкой и к АТШ в случае неравномерно распределенных открытых данных. Поэтому использовать ее в реальных приложениях опасно. Представ-

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

ленная здесь АИО похожа на атаку на гомоморфную криптосистему Доминго-Феррера из [5], которая имеет некоторые общие свойства с ПГК [3]. Однако в отличие от [5] здесь приводится точная оценка вероятности взлома криптосистемы с помощью данной атаки.

Предварительные сведения

Обозначения

Кольцо целых положительных чисел обозначается как $\mathbf{Z}_+$; кольцо целых чисел по модулю $n \in \mathbf{Z}_+$, $n > 1$ – $\mathbf{Z}_n$; кольцо полиномов от одной переменной над $\mathbf{Z}_n$ – $\mathbf{Z}_n[x]$; подмножество $\mathbf{Z}_n[x]$, состоящее из полиномов степени d, – $\mathbf{P}_{n,d}$; подмножество $\mathbf{P}_{n,d}$, состоящее из полиномов со старшим коэффициентом равным единице, – $\mathbf{P}_{d,n,mon}$; подмножество $\mathbf{P}_{d,n,mon}$, состоящее из неприводимых полиномов, – $\mathbf{I}_{n,d}$; для $a \in \mathbf{Z}_+$ его остаток от деления на n – $[a]_n$. Для $f(x) = \sum_{i=0}^{d} f_i \cdot x^i \in \mathbf{Z}_n[x]$ и $t \in \mathbf{Z}_+, t > 1$ будем обозначать $[f(x)]_t = \sum_{i=0}^{d} [f_i]_t \cdot x^i \in \mathbf{Z}_t[x]$. Тогда $x \xleftarrow{\$} R$, $x \xleftarrow{D} R$ означает, что x генерируется по равномерному или вероятностному распределению D на множестве R (или что случайная величина x имеет равномерное или соответственное распределение D); $x_i \xleftarrow{\$} R, i = \overline{1,d}$ – x_i выбраны равномерно и независимо; $f(x) \xleftarrow{\$} \mathbf{P}_{n,d}$ означает, что $f_i \xleftarrow{\$} \mathbf{Z}_n$, $i = \overline{0, d-1}, f_d \xleftarrow{\$} \mathbf{Z}_n \setminus \{0\}$.

Китайская теорема об остатках и результант полиномов

Теорема 1 (Китайская теорема об остатках, КТО, [6]). Для $n = n_1 \cdot \ldots \cdot n_k$, НОД $(n_i, n_j)=1$, $i \neq j$, выполняется $\mathbf{Z}_n \cong \mathbf{Z}_{n_1} \times \ldots \times \mathbf{Z}_{n_k}$. При этом $([a]_{n_1}, \ldots, [a]_{n_k}) \in \mathbf{Z}_{n_1} \times \ldots \times \mathbf{Z}_{n_k}$ соответствует $a = \sum_{i=1}^{k} [a]_{n_i} \cdot S_i \cdot S_i^{-1} \in \mathbf{Z}_n$, где $S_i = n / n_i$, $S_i^{-1} := 1 / \mathrm{S}_i (\mathrm{mod}\, n_i)$.

Определение 1 ([6]). Результант полиномов $f_j(x) = \sum_{i=0}^{d_j} f_{i,j} \cdot x^j \in \mathbf{Z}_n[x], j = 1,2$ – это определитель $\Delta = \mathrm{Res}(f_1(x), f_2(x)) = [\det(\mathbf{S})]_n \in \mathbf{Z}_n$ матрицы Сильвестра $\mathbf{S} \in \mathbf{Z}_n^{(d_1+d_2)\times(d_1+d_2)}$, составленной из $f_{i,j}$.

Лемма 1. Пусть даны $f_1(x), f_2(x) \in \mathbf{Z}_n[x]$. Если n имеет делитель $p \in \mathbf{Z}_+$, $p > 1$, то $[f_1(x)]_p, [f_2(x)]_p \in \mathbf{Z}_p[x]$ не взаимно просты по модулю $p \Leftrightarrow [\Delta]_p = 0$.

Доказательство. Является следствием КТО, а также свойств сравнений по модулю и результанта полиномов над полем, которые можно найти в [6].

Симметричная ПГК из работы [3]

Выбирается $n \in \mathbf{Z}_+, n = p \cdot q$, $p \neq q$, $\log_2 p = \log_2 q$, $\log_2 p \geq 512$, p, q – простые числа. Открытый текст $m \in \mathbf{Z}_p$ отображается в $c(x) = [s(x) \cdot u(x) + p \cdot r(x) + m]_n \in \mathbf{P}_{2 \cdot d, n, mon}$ посредством алгоритма шифрования из [3], где $u(x) \xleftarrow{\$} \mathbf{I}_{p,d}$, $s(x) \xleftarrow{\$} \mathbf{I}_{p,d}$, $r(x) \xleftarrow{\$} \mathbf{P}_{n,2 \cdot d-1}$. Секретный ключ – $sk = \{p, u(x)\}$, а n – публичный параметр. Расшифрование вычисляется как $\left[\left[c(x) \right]_p \right]_{u(x)}$. Криптосистема [3] – ПГК, так как $+$ и $\cdot$ шифровок в $\mathbf{Z}_n[x]$ на одном *sk* соответствует $+$ и $\cdot$ открытых текстов. Для ограничения роста размеров шифртекстов при их умножении, публикуется ключ для проведения вычислений $EK = \{w(x) = [s_0(x) \cdot u(x) + p \cdot r_0(x)]_n \in \mathbf{P}_{2 \cdot d+1, n, mon}\}$, $s_0(x) \xleftarrow{\$} \mathbf{I}_{p,d+1}$, $r_0(x) \xleftarrow{\$} \mathbf{P}_{n,2 \cdot d}$. Вычислителю предлагается приводить произведение шифртекстов по модулю $w(x)$. Доказывается, что это не влияет на результат вычислений над открытыми текстами.

3. Атака по известным открытым текстам на ПГК [3]

Модуль n в [3] является трудным для факторизации, и на основе этого в [3] сделано предположение, что ПГК защищена против АИО. Однако из данного свойства следует, что при знании n нужно перехватить лишь две пары $(m_i, c_i(x)), i = 1,2$ для его факторизации.

Лемма 2. Пусть даны шифртексты $c_i(x) = [s_i(x) \cdot u(x) + p \cdot r_i(x) + m_i]_n \in \mathbf{P}_{2 \cdot d, n, mon}, i = 1,2.$ $g_i(x) = \left[c_i(x) - m_i \right]_n \in \mathbf{P}_{2 \cdot d, n, mon}, i = 1,2$ имеют общий множитель по модулю p.

Доказательство. Так как $\left[g_i(x) \right]_p = \left[s_i(x) \cdot u(x) \right]_p \in \mathbf{P}_{2d, p, mon}$, то $\text{НОД}(\left[g_1(x) \right]_p, \left[g_2(x) \right]_p) = u(x)$.

В соответствии с леммами 1, 2 для $\Delta = \text{Re}\, s(g_1(x), g_2(x)) \in \mathbf{Z}_n$ выполняется $\left[\Delta \right]_p = 0$ и $\Rightarrow \Delta = p \cdot k$, $k \in \{0,1,...,q-1\}$. И если $\Delta \neq 0$, то в силу простоты q выполняется $p = \text{НОД}(n, \Delta)$, что и дает способ раскрытия p.

По теореме 1 $\Delta \neq 0 \Leftrightarrow \left[\Delta \right]_q \neq 0$. А по лемме 1 $\left[\Delta \right]_q \neq 0 \Leftrightarrow \left[g_i(x) \right]_q \in \mathbf{P}_{2 \cdot d, q, mon}, i = 1,2$ взаимно простые. И тогда вероятность факторизовать n равна $\delta = \Pr[\text{НОД}(\left[g_1(x) \right]_q, \left[g_2(x) \right]_q) \in \mathbf{Z}_q]$.

Шифрование [3] вероятностное? и потому $\left[g_i(x) \right]_q, i = 1,2$ можно мыслить как независимые случайные величины над $\mathbf{P}_{2 \cdot d, q, mon}$. Для оценки δ нужно узнать их вероятностное распределение. Тут нам понадобятся несколько вспомогательных лемм, характеризующих изменения вероятностных распределений случайных величин из $\mathbf{Z}_q$ при проведении над ними различных алгебраических операций.

Лемма 3. Пусть даны $n \in \mathbf{Z}_+, n > 2$, $q \in \mathbf{Z}_+, q > 2$ – делитель n, а также случайные величины $\xi \xleftarrow{\$} \mathbf{Z}_n$ и $\left[\xi \right]_q$, полученная приведением значений ξ по $\bmod q$. Выполняется $\left[\xi \right]_q \xleftarrow{\$} \mathbf{Z}_q$.

Доказательство. Для $\forall j \in \mathbf{Z}_q$ существует p элементов $\alpha_{i,j} = j + q \cdot i \in \mathbf{Z}_n$, $i \in \overline{0, p-1}$, для которых $\left[\alpha_{i,j} \right]_q = j$, где $p = n / q$. Все $\alpha_{i,j}$ разные и побегают все $\mathbf{Z}_n$. Следовательно, имеем $\Pr\left[\left[\xi \right]_q = j \right] = p / n = 1 / q$ и тогда $\left[\xi \right]_q \xleftarrow{\$} \mathbf{Z}_q$.

Лемма 4. Если $\xi \xleftarrow{\$} \mathbf{Z}_n \setminus \{0\}$, то вероятностное распределение $[\xi]_q$ следующее: $\Pr\left[[\xi]_q = 0\right] = \frac{p-1}{n-1} = \frac{1}{q} - \frac{q-1}{q\cdot(n-1)}$, а для $\forall j \in \mathbf{Z}_q \setminus \{0\}$ – $\Pr\left[[\xi]_q = j\right] = \frac{p}{n-1} = \frac{1}{q} + \frac{1}{q\cdot(n-1)}$.

Доказательство. По аналогии с леммой 3.

Определение 2. Вероятностное распределение над $\mathbf{Z}_q$, определенное в лемме 4, будем обозначать как Υ.

Лемма 5. Пусть даны $q \in \mathbf{Z}_+, q > 2$, произвольное распределение D над $\mathbf{Z}_q$ и независимые случайные величины $\xi_1 \xleftarrow{\$} \mathbf{Z}_q$, $\xi_2 \xleftarrow{D} \mathbf{Z}_q$. Тогда $\xi_+ = \xi_1 + \xi_2$ имеет распределение $\xi_+ \xleftarrow{\$} \mathbf{Z}_q$.

Доказательство. Для $\forall a \in \mathbf{Z}_q$ – $a = [j + j_a]_q$, где $j \in \mathbf{Z}_q$ произволен, $j_a = [q - j + a]_q \in \mathbf{Z}_q$. Для $j_1 \neq j_2$ выполняется $j_{a,1} \neq j_{a,2}$. Тогда $\Pr[\xi_+ = a] = \sum_{j=0}^{q-1} \Pr[\xi_1 = j]\cdot\Pr[\xi_2 = j_a] =$

$= \sum_{j=0}^{q-1} \left(\frac{1}{q}\cdot \Pr_D[j_a]\right) = \frac{1}{q}$, где $\Pr_D[j_a]$ – вероятность появления j_a по D.

Лемма 6. Пусть даны $q \in \mathbf{Z}_+, q > 2$ произвольное распределение D над $\mathbf{Z}_q$ и независимые случайные величины $\xi_1 \xleftarrow{\Upsilon} \mathbf{Z}_q$, $\xi_2 \xleftarrow{D} \mathbf{Z}_q$. Тогда $\xi_+ = \xi_1 + \xi_2$ имеет такое вероятностное распределение, что для $\forall a \in \mathbf{Z}_q$ выполняется $\frac{1}{q} - \frac{q-1}{q\cdot(n-1)} \le \Pr[\xi_+ = a] \le \frac{1}{q} + \frac{1}{q\cdot(n-1)}$.

Доказательство. $\Pr[\xi_+ = a] = \sum_{j=0}^{q-1} \Pr[\xi_1 = j]\cdot\Pr[\xi_2 = j_a] = \Pr_\Upsilon[0]\cdot\Pr_D[a] +$

$+ \sum_{j=0, j_a \neq a}^{q-1} \Pr_\Upsilon[j]\cdot\Pr_D[j_a] = \left(\frac{1}{q} - \frac{q-1}{q\cdot(n-1)}\right)\cdot\Pr_D[a] + \left(\frac{1}{q} + \frac{1}{q\cdot(n-1)}\right)\cdot(1 - \Pr_D[a]) =$

$= \frac{1}{q} + \frac{1}{n-1}\cdot\left(\frac{1}{q} - \Pr_D[a]\right)$. Поскольку $0 \le \Pr_D[a] \le 1$, то из последнего равенства следует утверждение леммы.

Лемма 7. Пусть даны $q \in \mathbf{Z}_+, q > 2$ – простое, $p \in \mathbf{Z}_+$ и случайная величина $\xi \xleftarrow{\$} \mathbf{Z}_q$. Тогда для $\xi_p = [p\cdot\xi]_q$ выполняется $\xi_p \xleftarrow{\$} \mathbf{Z}_q$.

Доказательство. Так как q простое, то $\forall a \in \mathbf{Z}_q$ можно представить в виде $a = \left[[p]_q \cdot \left[([p]_q^{-1}\cdot a)\right]_q\right]_q$, где $\left[[p]_q \cdot [p]_q^{-1}\right]_q = 1$. По свойствам $\mathbf{Z}_q$ для $a_1 \neq a_2$ справедливо $\left[([p]_q^{-1}\cdot a_1)\right]_q \neq \left[([p]_q^{-1}\cdot a_2)\right]_q$ и тогда $\Pr[\xi_p = a] = \Pr\left[\xi = \left[([p]_q^{-1}\cdot a)\right]_q\right] = 1/q$. □

Лемма 8. Пусть даны $q \in \mathbf{Z}_+, q > 2$ – простое, $p \in \mathbf{Z}_+, p > 2, \xi \xleftarrow{\Upsilon} \mathbf{Z}_q$. Тогда $\xi_p = [p\cdot\xi]_q$ имеет распределение $\xi_p \xleftarrow{\Upsilon} \mathbf{Z}_q$.

Доказательство. По аналогии с леммой 7.

Теперь мы готовы доказать теорему о распределении полиномов $[g_i(x)]_q, i = 1, 2$.

Теорема 2. Алгоритм шифрования [3] индуцирует на полиномах $g_q(x)=\left[g(x)\right]_q \in \mathbf{P}_{2\cdot d,q,mon}$, где $g(x)=\left[c(x)-m\right]_n$, распределение Ω такое, что для $\forall g_q(x)$ – $\left|\Pr_\Omega[g_q(x)]-\frac{1}{q^{2\cdot d}}\right|<\frac{1}{q^{2\cdot d-1}\cdot(n-1)}$.

Доказательство. Имеем некоторое произвольное $g_q(x)=x^{2d}+g_{q,2d-1}\cdot x^{2d-1}+...+g_{q,0}=$ $=\left[\left[s(x)\cdot u(x)\right]_q+\left[p\cdot r(x)\right]_q\right]_q \in \mathbf{P}_{2d,q,mon}$, $s(x)\xleftarrow{\$}\mathbf{I}_{p,d}$, $r(x)\xleftarrow{\$}\mathbf{P}_{n,2\cdot d-1}$, $\deg(u(x))=d$. Коэффициенты $r(x)$ можно мыслить как независимые случайные величины $r_i, i=\overline{0,2\cdot d-1}$, имеющие следующие распределения: $r_i\xleftarrow{\$}\mathbf{Z}_n, i=\overline{0,2\cdot d-2}$ и $r_{2\cdot d-1}\xleftarrow{\$}\mathbf{Z}_n\setminus\{0\}$. Тогда по леммам 3,4,7,8 коэффициенты $r_{p,q}(x)=\left[p\cdot r(x)\right]_q\in\mathbf{P}_{q,2\cdot d-1}$ будут распределены так: $r_{p,q,i}\xleftarrow{\$}\mathbf{Z}_q, i=\overline{0,2\cdot d-2}$, $r_{p,q,2\cdot d-1}\xleftarrow{\Upsilon}\mathbf{Z}_q$.

Для $g_q(x)$ имеем $\Pr_\Omega[g_q(x)]=\Pr\left[g_{q,2\cdot d-1}\right]\cdot\Pr\left[g_{q,2\cdot d-2}\mid g_{q,2\cdot d-1}\right]\cdot...\cdot\Pr\left[g_{q,0}\mid g_{q,2\cdot d-1},...,g_{q,1}\right]$. В силу независимости всех $r_{p,q,i}$ и леммы 5 получаем, что $\Pr_\Omega[g_q(x)]=\Pr\left[g_{q,2\cdot d-1}\right]\cdot\frac{1}{q^{2\cdot d-1}}$, где по лемме 6 $\frac{1}{q}-\frac{q-1}{q\cdot(n-1)}\le\Pr\left[g_{q,2\cdot d-1}\right]\le\frac{1}{q}+\frac{1}{q\cdot(n-1)}$. Исходя из этого, легко получить, что $\left|\Pr_\Omega[g_q(x)]-\frac{1}{q^{2\cdot d}}\right|<\frac{1}{q^{2\cdot d-1}\cdot(n-1)}$. □

Поскольку $\log q\ge 512$, то $\frac{1}{q^{2\cdot d-1}\cdot(n-1)}\approx 0$. И тогда из теоремы 2 следует, что $\left[g_i(x)\right]_q\in\mathbf{P}_{2\cdot d,q,mon}$, $i=1,2$ распределены практически равномерно. Следовательно для оценки $\delta=\Pr[\text{НОД}(\left[g_1(x)\right]_q,\left[g_2(x)\right]_q)\in\mathbf{Z}_q]$ можно привлечь следующий известный результат.

Теорема 3 ([7]). Пусть даны $q\in\mathbf{Z}_+, q>2$ – простое, $d\in\mathbf{Z}_+$ и $f_i(x)\xleftarrow{\$}\mathbf{P}_{q,d}, i=1,2$ Выполняется $\Pr[\text{НОД}(f_1(x),f_2(x))\in\mathbf{Z}_q]=1-1/q$.

Легко показать, что теорема 3 выполняется и для $f_i(x)\xleftarrow{\$}\mathbf{P}_{q,d,mon}, i=1,2$. Для этого достаточно воспользоваться тем, что если $\text{НОД}(f_1(x),f_2(x))\in\mathbf{Z}_q$, то и $\text{НОД}(a\cdot f_1(x),b\cdot f_2(x))\in\mathbf{Z}_q$ для $\forall a,b\in\mathbf{Z}_q\setminus\{0\}$. И тогда мы получаем, что $\delta=1-1/q$ и соответственно $\delta\approx 1$, т.к. $\log q\ge 512$. *Таким образом, мы получили, что вероятность раскрыть факторизацию n с помощью вычисления результанта* ≈ 1 *при наличии двух пар* $(m_i,c_i(x)), i=1,2.$

После получения p атакующий может вычислить $\left[g_i(x)\right]_p=\left[c_i(x)-m_i\right]_p=$ $=\left[s_i(x)\cdot u(x)\right]_p, i=1,2$. Тогда если $s_1(x)\ne s_2(x)$, то $\text{НОД}(\left[g_1(x)\right]_p,\left[g_2(x)\right]_p)=u(x)$. Ясно, что $\Pr\left[s_1(x)\ne s_2(x)\right]=1-1/\left|\mathbf{I}_{p,d}\right|\approx 1$, так как $\left|\mathbf{I}_{p,d}\right|$ – очень большое число. Тогда в силу того, что $s_1(x)\ne s_2(x)$ и $\text{НОД}(\left[g_1(x)\right]_q,\left[g_2(x)\right]_q)\in\mathbf{Z}_q$ в соответствии с алгоритмом шифрования [3] можно мыслить как независимые события, мы получаем финальную теорему 4.

Теорема 4. При наличии двух пар $(m_i \in \mathbf{Z}_p, c_i(x) \in \mathbf{P}_{2\cdot d,n,mon}), i = 1,2$, произведенных на одном ключе sk ПГК [3], описанная атака позволяет раскрыть sk с вероятностью $\left(1-1/\left|\mathbf{I}_{p,d}\right|\right)\cdot(1-1/q)$. Сложность атаки составляет $O(d^3 \cdot \log_2^2(n))$.

В табл. 1, 2 представлены временные замеры и доля успешных атак для разных d, n, полученные при тестировании реализации на ПК со следующими характеристиками: AMD Phenom(tm) II P960 Quad-Core Processor 1.80 GHz, 4 GB RAM.

Таблица 1

d	Время для $\log n = 1024$	Время для $\log n = 2048$
64	10,7 с	29 с
128	55 с	2,2 мин
256	5,2 мин	12,3 мин
512	23 мин	52 мин

Таблица 2

$\log_2 n$	Общее количество проведенных атак	Количество успешных атак	Практическая оценка Pr вероятности успеха
512	10^5	99984	0,99984
1024	10^5	99996	0,99996

Полученные экспериментальные данные подтверждают теоретическое обоснование эффективности атаки и высокой вероятности найти ключ с ее помощью. Напоследок заметим, что ключ для проведения вычислений $EK = \{w(x) \in \mathbf{Z}_n[x]\}$ в ПГК [3], по сути, представляет собой шифровку нулевого открытого текста. То есть если он известен злоумышленнику, то необходимо перехватить лишь одну пару $(m \in \mathbf{Z}_p, c(x) \in \mathbf{P}_{2\cdot d,n,mon})$.

Атака только по шифртекстам на ПГК [3]

Предположим, что атакующий, пытающийся взломать ПГК [3], перехватил последовательность шифртекстов $\{c_i(x) = [s_i(x)\cdot u(x) + p\cdot r_i(x) + m_i]_n \in \mathbf{P}_{2\cdot d,n,mon}\}_{i=1}^t$. Тогда он может вычислить $c_{i,j}(x) = \left[c_i(x) - c_j(x)\right]_n$ для $\forall i, j, i \neq j$. В силу наличия аддитивного гомоморфизма $c_{i,j}(x)$ шифрует $\left[m_i - m_j\right]_p$. Тогда если в последовательности $\{m_i \in \mathbf{Z}_p\}_{i=1}^t$ $\exists m_i, m_j \mid m_i = m_j, i \neq j$, то при наличии EK можно атаковать ПГК описанным ранее способом, поскольку в этом случае у атакующего, по сути, имеются две пары (открытый текст, шифртекст). То есть алгоритм атаки следующий. Атакующий вычисляет $\Delta_{i,j} = \mathrm{Re}\, s(c_i - c_j, EK)$ и НОД$(\Delta_{i,j}, n)$ до тех пор, пока не получит НОД$\neq 1$. Если получен НОД$\neq 1$, то p найден и можно определить $u(x)$. Вероятность успеха данной стратегии можно оценить по следующей формуле: $\eta_t = \Pr\left[\exists m_i, m_j \mid m_i = m_j, i \neq j\right] = 1 - \prod_{m=0}^{p-1}\left(\left(1-\Pr_\Psi[m]\right)^t + t\cdot\left(1-\Pr_\Psi[m]\right)^{t-1}\cdot\Pr_\Psi[m]\right)$, где Ψ – распределение на множестве открытых текстов. η_t может быть ≈ 1 при небольших t

(около 100) и Ψ , являющимся, к примеру, дискретным нормальным распределением с небольшой дисперсией (например, $\Psi = N(0,800)$ для $\mathbf{Z}_p$ с $\log p \geq 512$)

Заключение

Представлена вычислительно эффективная атака по известным открытым текстам (АИО) на ПГК из работы [3]. Вероятность раскрытия ключа расшифрования с её помощью ≈ 1. Для проведения атаки необходимо перехватить лишь две пары (открытый текст, шифртекст). А при наличии ключа для проведения гомоморфных вычислений достаточно перехватить только одну пару. Таким образом, ПГК из [3] *крайне нестойка к АИО*. Также выяснено, что гомоморфные свойства и незащищенность против АИО немедленно влекут за собой незащищенность против атаки только по шифртекстам (АТШ) в случае неравномерного распределения на открытых текстах, например, нормального распределения с небольшой дисперсией. Отметим, что наличие такого распределения на данных на практике является весьма вероятным. Выходом, конечно, может являться дополнительное кодирование данных с целью их рандомизации. Однако, так как кодирование должно сохранить гомоморфные свойства, для его осуществления нужно решить ряд фундаментальных проблем. Поэтому можно сделать вывод, что использование ПГК [13] в приложениях на данном этапе является опасным даже, если у противника нет возможности перехватить пары (открытый текст, шифртекст). В дальнейшем будет изучено, позволяют ли гомоморфные свойства ПГК свести АТШ к АИО для равномерного распределения на открытых данных. Наконец, отметим, что, сегодня, существование доказуемо криптостойкой ПГК, основанной на задаче факторизации – важная открытая проблема. В будущем планируется провести исследование на тему того, возможно ли в принципе построение такой ПГК.

СПИСОК ЛИТЕРАТУРЫ:

1. Gentry C. A fully homomorphic encryption scheme // PhD thesis, Stanford University, 2009.
2. Guellier. Can Homomorphic Cryptography ensure Privacy? // PhD thesis, Inria; IRISA; Supelec Rennes, equipe Cidre; Universite deRennes 1, 2014.
3. Zhirov A., Zhirova O. and Krendelev S.F. Practical fully homomorphic encryption over polynomial quotient rings // Internet Security (WorldCIS), 2013 World Congress on. P. 70-75. IEEE, 2013.
4. Shatilov K., Boiko V., Krendelev S., Anisutina D. and Sumaneev A. Solution for secure private data storage in a cloud // In Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. P. 885-889. IEEE, 2014.
5. Wagner D. Cryptanalysis of an algebraic privacy homomorphism // Information Security. P. 234-239. Springer, 2003.
6. Куликов Л.Я. Алгебра и теория чисел. Рипол Классик, 1979.
7. Benjamin A.T. and Bennett C.D. The probability of relatively prime polynomials // Mathematics Magazine. P. 196-202, 2007.

REFERENCES:

1. Gentry C. A fully homomorphic encryption scheme // PhD thesis, Stanford University, 2009.
2. Guellier. Can Homomorphic Cryptography ensure Privacy? // PhD thesis, Inria; IRISA; Supelec Rennes, equipe Cidre; Universite deRennes 1, 2014.
3. Zhirov A., Zhirova O. and Krendelev S.F. Practical fully homomorphic encryption over polynomial quotient rings // Internet Security (WorldCIS), 2013 World Congress on. P. 70-75. IEEE, 2013.
4. Shatilov K., Boiko V., Krendelev S., Anisutina D. and Sumaneev A. Solution for secure private data storage in a cloud // Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. P. 885-889. IEEE, 2014.
5. Wagner D. Cryptanalysis of an algebraic privacy homomorphism // Information Security. P. 234-239. Springer, 2003.
6. Kulikov L. Ja. Algebra i teorija chisel. Ripol Klassik, 1979.
7. Benjamin A.T. and C. D. Bennett. The probability of relatively prime polynomials // Mathematics Magazine. P. 196-202, 2007.