УДК 621.391:519.2

С.М. ИГНАТЕНКО

ОЦЕНКИ СТОЙКОСТИ СИММЕТРИЧНОЙ ШИФРСИСТЕМЫ RING-LWE ОТНОСИТЕЛЬНО АТАКИ С ВЫБРАННЫМ ОТКРЫТЫМ ТЕКСТОМ

Аннотация. Получены оценки стойкости симметричной шифрсистемы Ring-LWE относительно атаки с выбранным открытым текстом, основанные на применении обобщенного алгоритма BKW. Найденные оценки позволяют непосредственно выбирать значения параметров шифрсистемы, исходя из требований к ее стойкости относительно известных атак с выбранным открытым текстом. Возможность применения обобщенного алгоритма BKW является существенным фактором, влияющим на стойкость данной шифрсистемы относительно таких атак.

Ключевые слова: шифрсистема Ring-LWE, атака с выбранным открытым текстом, обобщенный алгоритм BKW, оценка стойкости.

Рассмотрим симметричную шифрсистему, которая является специальным случаем частично гомоморфной схемы шифрования Ring-LWE, предложенной в [1]. Эта шифрсистема определяется следующими параметрами: натуральное число $n>1$; нечетное число $q \geq 5$; унитарный многочлен $f(x)$, $\deg f(x) = n$, над кольцом $\mathbf{Z}_q$. Множество открытых текстов шифрсистемы $U = \{u_0 + u_1 x + \ldots + u_{n-1} x^{n-1} : u_i \in \{0,1\},\ i \in \overline{0, n-1}\}$, а множество ключей совпадает с кольцом $R_{n,q} = \mathbf{Z}_q[x]/(f(x))$. Шифртекст, получаемый в результате шифрования открытого текста $u \in U$ на ключе $s \in R_{n,q}$, определяется по формуле

$$E_s(u) = (c_1 = a,\ c_2 = as + 2e + u), \tag{1}$$

где a — случайный равновероятный элемент кольца $R_{n,q}$, e — полином степени не выше n, коэффициенты которого являются независимыми случайными величинами с равномерным распределением на множестве $\mathbf{Z}_{q'}$, $q' = 1/2 \cdot (q-1)$. Для нахождения открытого текста u по шифртексту (c_1, c_2) с помощью ключа s следует вычислить

$$D_s(c_1, c_2) = (c_2 - c_1 s) \bmod 2. \tag{2}$$

Отметим, что в формулах (1) и (2) полиномы c_2 и $c_2 - c_1 s$ вычисляются в кольце $R_{n,q}$. Корректность расшифрования следует из того, что при выполнении (1) полином $c_2 - c_1 s = u + 2e \in R_{n,q}$ равен сумме полиномов u и $2e$ в кольце $\mathbf{Z}[x]$, поскольку максимальный коэффициент этой суммы находится в интервале от 0 до $1 + 2(q'-1) \leq q-1$. Отсюда $D_s(c_1, c_2) = (u + 2e) \bmod 2 = u$.

В [1] проанализирована стойкость (security) шифрсистемы в предположении, что q является простым числом, $f(x) = x^n + 1$, где n — степень двойки такая, что $2n$ делит $q-1$, а случайный полином e в формуле (1) имеет дискретное гауссово распределение. Показано, что в этом случае любую атаку на шифрсистему с выбранным открытым текстом (chosen plaintext attack) можно эффективно преобразовать в алгоритм решения задачи Ring-LWE, которая является вычислительно трудной [2]. Вместе с тем в [1], а также в других известных публикациях не приводятся оценки стойкости шифрсистем этого вида относительно конкретных атак.

Цель настоящей статьи — получить оценки стойкости описанной шифрсистемы относительно атаки, при проведении которой противник m раз зашифровывает открытый текст $u = 0$ на одном и том же (неизвестном) ключе $s \in R_{n,q}$.

В результате шифрования противник получает систему уравнений (СУ) $a_i s+2e_i = c_{2,i}$, $i \in \overline{1, m}$, над кольцом $R_{n,q}$, которую с учетом нечетности числа q можно записать в виде

$$\widetilde{a}_i s+e_i = \widetilde{c}_{2,i},\ i \in \overline{1, m}, \tag{3}$$

где $\widetilde{a}_i = 2^{-1} a_i$, $\widetilde{c}_{2,i} = 2^{-1} c_{2,i}$, $a_1, \dots, a_m$ и $e_1, \dots, e_m$ — независимые случайные равновероятные величины со значениями в кольце $R_{n,q}$ и множестве $\mathbf{Z}_{q'}$ соответственно.

Для решения СУ (3) можно применить следующий естественный метод. Зафиксируем число $i \in \overline{1, m}$, для которого элемент $\widetilde{a}_i$ обратим в кольце $R_{n,q}$. Далее, перебирая все $\left(\frac{q-1}{2}\right)^n$ значений полинома e_i, вычисляем полином $s = \widetilde{a}_i (\widetilde{c}_{2,i} - e_i)$ и проверяем для каждого $j \in \overline{1, m} \setminus \{i\}$, принадлежат ли коэффициенты полинома $e_j = \widetilde{c}_{2,i} - \widetilde{a}_j s$ множеству $\mathbf{Z}_{q'}$. Очевидно, что трудоемкость решения СУ (3) методом перебора составляет не менее чем

$$T(n, q) = \left(\frac{q-1}{2}\right)^n \tag{4}$$

операций в наихудшем случае.

Для решения СУ (3) можно применить также другой известный метод (см., например, [2]).

Для любого полинома $a = a(x) \in R_{n,q}$ обозначим $M(a)$ матрицу размера $n \times n$, j-й столбец которой равен вектору коэффициентов полинома $(x^j a(x)) \bmod f(x)$, $j \in \overline{0, n-1}$. Тогда вектор коэффициентов полинома $\widetilde{a}_i s$ равен произведению матрицы $M(\widetilde{a}_i)$ на вектор-столбец коэффициентов полинома s. В качестве следствия системы (3) получим СУ с искаженными правыми частями над кольцом $\mathbf{Z}_q$ относительно искомого вектора s:

$$A_i s+\xi_i = b_i,\ i \in \overline{1, m}, \tag{5}$$

где A_i — строка с номером 0 матрицы $M(\widetilde{a}_i)$, b_i — координата с тем же номером вектора $\widetilde{c}_{2,i}$, а ξ_i — случайная величина с равномерным распределением на множестве $\mathbf{Z}_{q'}$. Отметим, что $A_1, \dots, A_m$ являются независимыми случайными равновероятными векторами длины n над кольцом $\mathbf{Z}_q$, а случайные величины $\xi_1, \dots, \xi_m$ независимы в совокупности и не зависят от векторов $A_1, \dots, A_m$.

Для оценки сложности решения СУ (5) с помощью одного из наиболее эффективных алгоритмов (а именно обобщенного алгоритма BKW [3, 4]) можно воспользоваться следующим утверждением.

Утверждение 1 [4]. Пусть n_1, $1 \le n_1 \le n-3$, — натуральное число, $\delta \in (0, 1)$,

$$u = \left\lceil \frac{\log(n-n_1)}{2} \right\rceil,\ v = \left\lceil \frac{2(n-n_1)}{\log(n-n_1)} \right\rceil,\ k = 2^{u-1},\ l = (u + \left\lceil \ln (2t\delta^{-1}) \right\rceil - 1) q^v,$$

$$m = lt, \tag{6}$$

где

$$t = \left\lceil \frac{2n_1 \ln (2q\delta^{-1})(\log p_{\max} - \log p_{\min})^2}{(D(p_\xi || \omega) + D(\omega || p_\xi))^2} \right\rceil.$$

Здесь $p_\xi = (p(z): z \in \mathbf{Z}_q)$ — распределение вероятностей случайной величины $\eta_k = \xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$, $p_{\max} = \max\limits_{z \in R} p(z)$, $p_{\min} = \min\limits_{z \in N_\xi(R)} p(z)$ и $D(p_\xi || \omega) = \sum\limits_{z \in N_\xi} p(z) \log(qp(z))$, $D(\omega || p_\xi) = -q^{-1} \sum\limits_{z \in N_\xi} \log(qp(z))$, $N_\xi = \{z \in \mathbf{Z}_q: p(z) > 0\}$. Тогда, применив к системе (5) обобщенный алгоритм BKW, можно восстановить с вероятностью, не меньшей $1 - \delta$, первые n_1 координат искомого вектора s с использованием

$$T_{\mathrm{BKW}} = 2n_1 t q^{n_1} + O(ult) \tag{7}$$

операций над n-мерными векторами над кольцом $\mathbf{Z}_q$.

Для того чтобы воспользоваться утверждением 1, докажем следующее утверждение, устанавливающее аналитические выражения для вероятностей значений случайной величины $\eta_k = \xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$.

Утверждение 2. Для любого $l \in \mathbf{Z}_q$ справедливо равенство

$$\mathbf{P}(\eta_k = l) = \frac{2^{k/2}}{(q-1)^k q} \sum_{j=0}^{q-1} \frac{\cos(2\pi q^{-1} jl)}{(1 + \cos(\pi q^{-1}(q-1)j))^{k/2}}. \tag{8}$$

Доказательство. Прежде всего найдем преобразование Фурье распределения вероятностей случайной величины $\xi = \xi_1$.

Обозначим $\omega = \exp\{2\pi i q^{-1}\}$, где $i^2 = -1$. Тогда

$$\hat{p}_\xi(\alpha) \stackrel{\mathrm{def}}{=} \sum_{j=0}^{q-1} \mathbf{P}(\xi = j)\omega^{-\alpha j} = \frac{2}{q-1} \sum_{j=0}^{q'} \omega^{-\alpha j}, \ \alpha \in \mathbf{Z}_q.$$

Поскольку для ненулевого числа α

$$0 = \sum_{j=0}^{q-1} \omega^{-\alpha j} = \sum_{j=0}^{q'} \omega^{-\alpha j} + \sum_{j=q'+1}^{q-1} \omega^{-\alpha j} = \frac{q-1}{2} \hat{p}_\xi(\alpha) + \sum_{j=1}^{q-q'-1} \omega^{-\alpha(j+q')} =$$

$$= \frac{q-1}{2} \hat{p}_\xi(\alpha) + \sum_{j=1}^{q'} \omega^{-\alpha(j+q')} = \frac{q-1}{2} \hat{p}_\xi(\alpha) + \omega^{-\alpha q'} \sum_{j=1}^{q'} \omega^{-\alpha j} =$$

$$= \frac{q-1}{2} \hat{p}_\xi(\alpha) + \omega^{-\alpha q'} \left(\frac{q-1}{2} \hat{p}_\xi(\alpha) - 1 \right),$$

имеем

$$\hat{p}_\xi(\alpha) = \frac{2}{q-1} \left(\frac{\omega^{-\alpha q'}}{1 + \omega^{-\alpha q'}} \right), \ \alpha \in \mathbf{Z}_q \setminus \{0\}. \tag{9}$$

Кроме того,

$$\hat{p}_{-\xi}(\alpha) \stackrel{\mathrm{def}}{=} \sum_{j=0}^{q-1} \mathbf{P}(-\xi = j)\omega^{-\alpha j} = \sum_{j=0}^{q-1} \mathbf{P}(\xi = j)\omega^{\alpha j} = \hat{p}_\xi(-\alpha), \ \alpha \in \mathbf{Z}_q. \tag{10}$$

Далее, поскольку $\eta_k = \xi_1 + \ldots + \xi_{k/2} - (\xi_{k/2+1} + \ldots + \xi_k)$, где $\xi_1, \ldots, \xi_k$ — независимые одинаково распределенные случайные величины, на основании теоремы о свертке (см., например [5]) и формул (9), (10) справедливы следующие равенства:

$$\hat{p}_{\eta_k}(\alpha) = (\hat{p}_\xi(\alpha))^{k/2}(\hat{p}_\xi(-\alpha))^{k/2} = \frac{2^k}{(q-1)^k}\left(\frac{\omega^{-\alpha q'}}{1+\omega^{-\alpha q'}} \cdot \frac{\omega^{\alpha q'}}{1+\omega^{\alpha q'}}\right)^{k/2} =$$

$$= \frac{2^{k/2}}{(q-1)^k}\left(\frac{1}{1+\cos(\pi q^{-1}(q-1)\alpha)}\right), \ \alpha \in \mathbf{Z}_q \setminus \{0\}.$$

Отсюда, используя формулу обращения для преобразования Фурье и тот факт, что вероятности являются действительными числами, получаем

$$\mathbf{P}(\eta_k = l) = q^{-1}\sum_{j=0}^{q-1}\hat{p}_{\eta_k}(j)\omega^{lj} = \frac{2^{k/2}}{(q-1)^k q}\sum_{j=0}^{q-1}\frac{\omega^{lj}}{(1+\cos(\pi q^{-1}(q-1)j))^{k/2}} =$$

$$= \frac{2^{k/2}}{(q-1)^k q}\sum_{j=0}^{q-1}\frac{\cos(2\pi q^{-1}jl)}{(1+\cos(\pi q^{-1}(q-1)j))^{k/2}}.$$

Таким образом, справедливо равенство (8), что и требовалось доказать.

С использованием утверждений 1 и 2 оценим временную сложность (7) и объем шифрматериала (6), необходимого для восстановления ключа симметричной шифрсистемы Ring-LWE с помощью обобщенного алгоритма BKW (табл. 1).

Как видно из таблицы, возможность применения обобщенного алгоритма BKW является существенным фактором, влияющим на стойкость шифрсистемы относительно атак с выбранным открытым текстом. В частности, при $n = 128$ и $q = 151$ сложность (4) восстановления ключа шифрсистемы с помощью естественного метода перебора составляет не менее $2^{797.29}$ операций, в то время как сложность решения этой задачи с помощью обобщенного алгоритма BKW равна $2^{251.75}$. С увеличением параметра n или параметра q выигрыш в трудоемкости атаки за счет применения обобщенного алгоритма BKW увеличивается от $2^{55.71}$ раз при $n = 32$ и $q = 37$ до $2^{1408.73}$ раз при $n = 256$ и $q = 327$.

Таблица 1. Характеристики эффективности атак с выбранным открытым текстом на шифрсистему Ring-LWE ($\delta = 0.01$)

n	q	$\log T(n,q)$	$\log T_{\mathrm{BKW}}$	$\log m$
32	37	133.44	75.53	71.94
32	57	153.84	82.66	79.08
32	107	183.29	93.05	89.47
64	71	328.27	130.41	126.82
64	91	351.48	136.97	133.38
64	141	392.27	148.52	144.93
80	121	472.55	165.98	162.07
80	141	490.34	170.67	166.76
80	191	525.59	179.97	176.07
128	131	770.86	245.34	241.01
128	151	797.29	251.75	247.43
128	201	850.41	264.67	260.34
256	257	1791.99	454.04	448.61
256	277	1819.78	459.80	454.37
256	327	1881.27	472.54	467.11

Таким образом, полученные результаты позволяют непосредственно выбирать значения параметров симметричной шифрсистемы Ring-LWE, исходя из требований к ее стойкости относительно известных атак с выбранным открытым текстом.

СПИСОК ЛИТЕРАТУРЫ:

1. Brakersky Z., Vaikuntanathan V. Fully homomorphic encryption from Ring-LWE and security for key dependent messages. In: Rogway P. (ed.). *Advances in Cryptology — CRYPTO 2011. LNCS*. 2011. Vol. 6841. P. 505–524.
2. Lyubashevsky V., Peikert C., Regev O. On ideal lattices and learning with errors over rings. In: Gillbert H. (ed.). *Advances in Cryptology — EUROCRYPT 2010. LNCS*. 2010. Vol. 6110. P. 1–23.
3. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*. 2003. Vol. 50, Issue 4. P. 506–519.
4. Олексійчук А.М., Ігнатенко С.М., Поремський М.В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Сер.: Технічні науки*. 2017. Вип. 15. С. 150–155.
5. Wood J.A. Duality for modules over finite rings and application to coding theory. *American Journal of Mathematics*. 1999. Vol. 121, N 3. P. 555–575.

Надійшла до редакції 27.11.2019

С.М. Ігнатенко

ОЦІНКИ СТІЙКОСТІ СИМЕТРИЧНОЇ ШИФРСИСТЕМИ RING-LWE ВІДНОСНО АТАКИ З ПІДІБРАНИМ ВІДКРИТИМ ТЕКСТОМ

Анотація. Отримано оцінки стійкості симетричної шифрсистеми Ring-LWE відносно атаки з підібраним відкритим текстом, які базуються на застосуванні узагальненого алгоритму BKW. Отримані оцінки дають змогу безпосередньо вибирати значення параметрів шифрсистеми, виходячи з вимог до її стійкості відносно відомих атак з підібраним відкритим текстом. Можливість застосування узагальненого алгоритму BKW є суттєвим фактором для визначення стійкості постквантових шифрсистем типу Ring-LWE відносно цих атак.

Ключові слова: шифрсистема Ring-LWE, атака з підібраним відкритим текстом, узагальнений алгоритм BKW, оцінка стійкості.

S.M. Ihnatenko

SECURITY ESTIMATES OF A RING-LWE SYMMETRIC CRYPTOSYSTEM AGAINST CHOSEN PLAINTEXT ATTACK

Abstract. In terms of application of the generalized BKW algorithm, the estimates of security of Ring-LWE symmetric cryptosystem against chosen plaintext attack have been obtained. These estimates allow us to choose the cryptosystem parameters directly proceeding from requirements of its security against chosen plaintext attacks. The ability to apply the generalized BKW algorithm is an important factor that affects the cryptosystem security against chosen plaintext attacks.

Keywords: Ring-LWE cryptosystem, chosen plaintext attack, generalized BKW algorithm, security estimate.

Игнатенко Сергей Михайлович,
сотрудник Службы безопасности Украины, Киев, e-mail: mongol_1979@ukr.net.