Об одном методе построения схемы полного гомоморфного шифрования

А.В. Шокуров (shok@ispras.ru), К.В. Сергеев (kosts88@mail.ru)

Аннотация. Предложен вариант метода Джентри для построения полного гомоморфного шифрования.

Ключевые слова: шифрование, гомоморфное шифрование, открытый ключ, секретный ключ.

1. Введение.

Гомоморфное шифрование позволяет производить вычисления над секретными данными, заменяя их вычислениями над соответствующими данными в зашифрованном виде. Гомоморфность шифрования относительно операции умножения целых чисел по некоторому модулю достигается, например, в криптосистемах RSA, Эль-Гамаля, Гольдвассер-Микали (см., например, [5]) .

Полностью гомоморфные схемы шифрования, обладающие свойством гомоморфности относительно операций сложения и умножения, были предложены недавно. Первая из них была представлена Крейгом Джентри в [1,2,3]. Эта криптосистема использует идеальные решетки. Позже Крейгом Джентри и другими в [4] была предложена еще одна полностью гомоморфная схема шифрования, обладающая схожими свойствами, но проводящая операции над целыми числами. В данной работе предложена новая система перешифрования внешне похожая на предложенную в [4] схему, однако не требующая введения дополнительной информации о секретном ключе.

2. Основные обозначения и определения.

Определение 1. Схемой шифрования с открытым ключом называется тройка алгоритмов *E=(Gen, Decr, Encr)* такая, что

- *Gen* - полиномиальный вероятностный алгоритм, *Encr* - полиномиальный алгоритм (и, возможно, вероятностный, тогда схема шифрования называется вероятностной), - *Decr* - полиномиальный алгоритм;

- алгоритм генерации ключа *Gen*, получая на вход некоторый параметр λ, называемый параметром безопасности , создает пару ключей: секретный ключ $k_s \in \Sigma^\lambda$ и открытый ключ $k_p \in \Sigma^\lambda$, $\Sigma = \{0,1\}$ где .

- алгоритм шифрования Encr, получая на вход открытый k_p ключ и открытый текст m, выдает на выходе щифротекст c.

- алгоритм дешифрования, получая на вход секретный k_s ключ и шифротекст c, выдает открытый текст.

- для любых открытых текстов $m \in \Sigma^{f(\lambda)}$, где f полиномиальная функция, и любой пары ключей , (k_s, k_p) полученной с помощью алгоритма Gen, выполняется соотношение

$$Decr\left(k_s, Encr\left(k_p, m\right)\right) = m$$

Введем следующие обозначения и определения.

Определение 2. Пусть дана схема шифрования с открытым ключом *(Gen, Decr, Encr)* и пусть даны алгоритм *Eval* и множество функций *F* такие, что для $f \in F$ любой функции от t переменных и для любых $c_1, \dots, c_t$ $c_i = Encr\left(k_p, m_i\right),\ i = 1, \dots, t$ шифротекстов алгоритм $Eval(k_p, f, c_1, \dots, c_t)$ вычисляет шифротекст *c* такой, что $Decr(k_s, c) = f(m_1, \dots, m_t)$. Тогда четверка алгоритмов *E=(Gen, Decr, Encr, Eval)* называется схемой шифрования, обладающей свойством гомоморфности на множестве фунций F.

Определение 3. Гомоморфной схемой шифрования на множестве функций F называется такая четверка алгоритмов *E=(Gen, Decr, Encr, Eval)*, для которой шифротексты обладают свойством компактности и алгоритм Eval является эффективным. Если множество F совпадает с множеством всех функций, то такая схема называется полностью гомоморфной схемой шифрования.

3. Частично гомоморфная схема шифрования.

Пусть заданы некоторые параметры λ, N, P, Q и τ , $N \ll P$ $Q = f(P, \log P)$ причем , а , где функция f полином. Для любых целых *x* и *y* $x \bmod y$ через будем понимать такое число *z*, что и *x* - *y* $-{}^{y}/_{2} < z \le {}^{y}/_{2}$ делится на *y*. Считаем, что битовая строка секретного ключа имеет старший k_s $2^P \le k_s < 2^{P+1}$ разряд 1, и .Рассмотрим следующую открытую схему шифрования *E**.

Алгоритм 1. $Gen_{E^*}(\lambda)$ выдает на выход случайную *P*-битовую нечетную строку k_s – секретный ключ и $Q \cdot \tau$ -битовую строку k_p - открытый ключ.

Алгоритм 2. $Encr_{E^*}(k_p, m)$ - выбирает для бита *m* случайную строку *c* вида

$$c = m' + k_s \cdot q,$$

где число m' имеет ту же четность, что и бит *m*, а число бит слова m' не превосходит *N*, а число битов слова *c* не превосходит *Q* .

Алгоритм 3. $Decr_{E^*}(k_s, c)$ выдает на выход $(c \bmod k_s) \bmod 2$.

Алгоритм 4. $Eval_{E^*}(f, c_1, \dots, c_t)$ переходит от представления функции $f(x_1, \dots, x_t)$ в виде схемы к представлению в виде полинома $F(m_1, \dots, m_t)$ в кольце многочленов над $\mathbb{Z}_2$. Заменим теперь все операции над битами в этом полиноме, соответствующими им целочисленного сложения и умножения над строками. Мы получим новый полином

$$F_Q(c_1, \dots, c_t)$$

от *t* переменных строк длины *Q*. На выход алгоритма выдается

$$c = F_Q(c_1, \dots, c_t).$$

Утверждение 1. (Корректность шифрования) Для любого шифротекста $c = Encr_{E^*}(k_p, m)$ выполнено $Decr_{E^*}(k_s, c) = m$.

Утверждение 2. (Свойство гомоморфности) Схема шифрования E^* обладает свойством гомоморфности на множестве фунций *F*, которые могут быть представлены многочленами степени не выше k и содержащими не более *l* слагаемых, для которых выполнено соотношение $Nk + \log l < P - 4$.

4. Алгоритм перешифрования.

Определение 4. Если схема шифрования *E* гомоморфна относительно собственной

функции расшифрования $Decr_E(k_s, c)$, а также функций

$$Decr_E(k_s, c_1) + Decr_E(k_s, c_2) \bmod 2 \text{ и}$$
$$Decr_E(k_s, c_1) \cdot Decr_E(k_s, c_2) \bmod 2,$$

то она называется расширяемой.

Утверждение 3. Для того, чтобы схема шифрования *E=(Gen, Decr,Encr,Eval)* являлась полностью гомоморфной схемой шифрования достаточно, чтобы она была гомоморфна относительно операций сложения и умножения по модулю 2 и расширяема.

5. Заключение. Построение полностью гомоморфной схемы шифрования.

Обозначим через *LSB(c)* функцию четности числа $c \in \mathbb{Z}$, т.е. такую, что *LSB(c)*=0, если *c* четно, и *LSB*(c)=1, если *c* нечетно. Обозначим через $[\![x]\!]$ ближайшее целое к числу $x \in \mathbb{R}$, если его дробная часть не равна $1/2$.

Утверждение 4. Функцию расшифрования в криптосистеме *E* можно представить в виде

$$Decr_E(k_s, c) = LSB(c)\ XOR\ LSB\left(\left[\!\left[c/k_s \right]\!\right]\right). \quad (1)$$

Утверждение 5. Пусть заданы $m_i \in \{0,1\}$, где $i = 1, \dots, n$ и $h: \mathbb{Z} \to \mathbb{Z}_2$ гомоморфизм колец, преобразующий 1 в 1. Положим $t_i = h(m_i)$ при $i = 1, \dots, n$. Тогда существуют симметрические функции $f_k(x_1, \dots, x_n) \in \mathbb{Z}_2[x_1, \dots, x_n]$ степени не выше 2^k *k*, для которых выполняется равенство

$$\sum_{i=1}^{n} m_i = \sum_{j=1}^{j<\log n} f_j(t_{1,\dots,} t_n) \cdot 2^{j-1} \quad (2)$$

Применим формулу (2) для суммирования *Q K*-разрядных чисел в двоичном представлении

$$\sum_{i=1}^{Q}\sum_{j=1}^{K} m_{i,j} \cdot 2^{j-1} = \sum_{j=1}^{K}\left(\sum_{i=1}^{Q} m_{i,j}\right) = \sum_{j=1}^{K}\left(\sum_{i=1}^{j<\log Q} f_i(t_{1,k}, \dots, t_{Q,k}) \cdot 2^{i-1}\right) \cdot 2^{j}. \quad (3)$$

Для вычислений с помощью формулы (1), достаточно использовать приближенное значение величины $r \approx 1/k_s$ с *2Q* двоичными битами. Для вычисления значения функции $[\![c/k_s]\!]$ требуется знание младшего целого разряда и первого двоичного дробного разряда произведения *rc*. В этом случае сумма по модулю 2 этих битов дает значение функции $[\![c/k_s]\!]$. Для вычисления этих двух битов достаточно использовать формулу (3) для значений $K = O(\log Q)$.

Следствие. Предложенная в разделе 3 частично гомоморфная схема расширяема при значениях

$$N = \omega(\log\lambda), P \geq N \cdot \Theta(\lambda\ log^2\ \lambda),\ Q = \omega(P^2 \log\lambda), \tau = Q + \omega(\log\lambda)$$

и поэтому является полностью гомоморфной.

Список литературы

[1] Craig Gentry, Computing arbitrary functions of encrypted data. ACM, 2010.
[2] Craig Gentry, Fully homomorphic encryption using ideal lattices. 41st ACM STOC, 2009.
[3] Craig Gentry, A fully homomorphic encryption scheme. Stanford University, Ph.D. thesis. 2009.
[4] M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, Fully homomorphic encryption over the integers. International Association for Cryptographic Research, 2010.
[5] Н. П. Варновский, А. В. Шокуров, Гомоморфное шифрование. Труды Института Системного Программирования. Том 12. М: ИСП РАН, 2007, с. 27-36.

On Constructing a Fully Homomorphic Encryption

Shokurov A.V., ISP RAS, Moscow, Russia
Sergeev K.V., MPTI, Dolgoprudni'j, Moscow Region, Russia

Abstract. Fully homomorphic encryption allows to perform calculations on private data, replacing them by computing the appropriate data in encrypted form. Gomomorphic encryption for one operation on integers is achieved, for example, by the RSA, El-Gamal, Goldwasser-Micali cryptosystems. Fully homomorphic encryption schemes that are gomomorphic over addition and multiplication were proposed recently. The first of them, using ideal lattices, was suggested by C. Gentry in 2009. Later C. Gentry and others offered another fully homomorphic encryption scheme with similar properties, but conducting operations on integers. The crucial part of these construction is the description of re-encryption procedure. In this paper we proposed a new system for the re-encryption that looks like suggested by C. Gentry's the scheme but, however, does not require the introduction of additional information about the secret key. In our scheme we use arbitrary representation inverse of private key that is represented using only logarithmic number on the length of input for possible distinct encryptions of bits. The proof uses the representation of the k-th bit of the integer sum of n bits as a symmetric polynomial on n variables of degree less then $2^k + 1$.

Keywords. Encryption scheme, homomorphic encryption scheme, public key, secret key.

References

[1] Craig Gentry, Computing arbitrary functions of encrypted data. ACM, 2010.
[2] Craig Gentry, Fully homomorphic encryption using ideal lattices. 41st ACM STOC,
[3] 2009.
[4] Craig Gentry, A fully homomorphic encryption scheme. Stanford University, Ph.D.
[5] thesis. 2009.
[6] M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, Fully homomorphic encryption over the integers. International Association for Cryptographic Research, 2010.
[7] Varnovskij N.P., Shokurov A.V., Gomomorfnoe shifrovanie [Homomorphic encryption], Trudy ISP RAN [The Proceedings of ISP RAS], 2007, vol. 12, pp. 27-36. (in Russian)