Алгоритм экспоненциально гомоморфного шифрования без взаимодействия

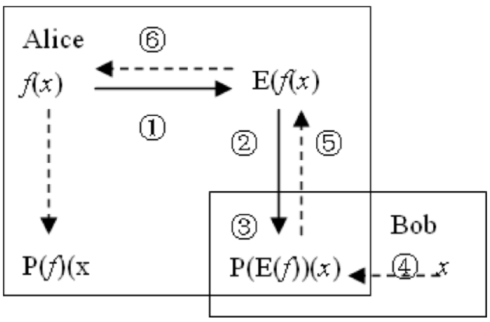
Вступление

Мобильный код – новая вычислительная парадигма, подходящая под распределенные приложения широкого масштаба. Но проблемы безопасности предотвращают широкое использование мобильного кода. Защитная техника, основанная на гомоморфном шифровании – важное направление исследований. Оно в предпосылке перевода мобильного кода в функции и поддерживается теорией сложности вычислений. Можно посчитать закодированную функцию от закодированного сообщения и потом раскодировать и получить тот же результат, что и после использования исходной функции на исходном сообщении. Поэтому этот способ сложнее обычного шифрования, которое шифрует только данные. В настоящее время исследования гомоморфного шифрования всё ещё на начальном этапе.

Базовые концепты

А. Вычисление закодированных функций без взаимодействия

У Алисы есть алгоритм f. У Боба есть вход x и он хочет посчитать $f(x)$ для неё, но Алиса не хочет, чтобы Боб знал что-то важное о f. Также Боб не должен взаимодействовать с Алисой во время вычисления.



Б. Принципы гомоморфного шифрования

Сандер с коллегами [2][3] определили принципы аддитивного, мультипликативного, смешанно мультипликативного и алгебраического гомоморфизма. Они развернули вычисление закодированных функций рациональных многочленов целочисленной области без взаимодействия.

Определение 1

R и S – кольца, функция E: R→S:

i. Аддитивно гомоморфна, если есть эффективный алгоритм PLUS расчета $E(x+y)$ по $E(x)$ и $E(y)$, который не раскрывает x и y.
ii. Мультипликативно гомоморфна, если есть эффективный алгоритм MULT расчета $E(xy)$ по $E(x)$ и $E(y)$, который не раскрывает x и y.
iii. Смешанно мультипликативно гомоморфна, если есть эффективный алгоритм MlXED-MULT расчета $E(xy)$ по $E(x)$ и y, который не раскрывает x.
iv. Алгебраически гомоморфна, если выполняется (i.) и (ii.) [2] [3]

Но схема Сандера может только кодировать константные коэффициенты рациональных полиномов, не может кодировать экспоненты и поэтому сливает часть данных. Поэтому нам нужно определить гомоморфное по экспоненте шифрование:

2) Определение 2

R и S – кольца, кодирующая функция E: R→S, декодирующая функция D;

Если $E(x^k) = x^{E1(k)}$ и выполняется
$D(E(x^k)) = D(x^{E1(k)})$ и нет утечки k, тогда E – экспоненциально гомоморфное шифрование.

Алгоритм экспоненциально гомоморфного шифрования

Для того, чтобы ввести алгоритм экспоненциально гомоморфного шифрования и доказать его корректность, напомним читателю про известный алгоритм RSA, основанный на сложности факторизации больших чисел [4].

A. Малая теорема Ферма

Если p – простое число и a – целое, не делящееся на p, то $a^{p-1} - 1$ делится на p.

Б. Расширение Эйлера для малой теоремы Ферма

Функция Эйлера $\phi(n)$ обозначает количество натуральный взаимно простых с n чисел.

Если n – простое, $\phi(n)=n-1$; если n= pq, и p, q простые, то $(\phi(n)=(p-1)(q-1)$.

Если наибольший общий делитель (a,n)=1, тогда $a^{\phi(n)} \bmod n = 1$.

B. Алгоритм RSA

a) Создадим публичный и приватный ключ

Выберем 2 больших простых числа p и q. Случайно выберем e, взаимно простое с $(p-1)(q-1)$. Посчитаем d, используя алгоритм Евклида - $ed \equiv 1 \bmod (p-l)(q-l)$.

Тогда $d \equiv e^{-1} \bmod (p-l)(q-l)$. e, n – публичные ключи, d – приватный. Числа p и q больше не нужны, но нельзя позволить их утечку.

b) Зашифруем сообщение

Разделим m данных по пакетам m_i, меньших n, закодируем их, $c_i = m_i^e \pmod n$

c) Расшифруем

$m_i = c_i^d \pmod n$

Г. Алгоритм гомоморфного шифрования

Алгоритм гомоморфного шифрования основан на RSA, как и было показано в алгоритме 1.

1) Экспоненциально гомоморфный алгоритм (EHA)

a) Получим публичный и закрытый ключи

Выберем 3 больших простых числа p, q, r. Пусть n = pq, N = pqr. Случайно выберем ключ e, взаимно простой с (p-l) (q-l). Посчитаем d: $ed \equiv l \bmod (p-1)(q-1)$.

N – публичный, e, d, n – приватные ключи. $k \in z+$, $\omega^k < n$ и ω взаимно простое с n.

b) Шифрование

$$\theta = E(\omega^k) = (\omega^k \omega^{ed-1}) \bmod N$$

c) Расшифровка D

$D(\theta) = \theta \bmod n$

d) Доказательство корректности EHA

$$D(E(\omega)^k)) = ((\omega^k \omega^{ed-1}) \bmod N) \bmod n \qquad (7)$$

Раз $N=nr$ тогда

$$D(E(\omega^k))=((\omega^k\omega^{ed-1}) \bmod N) \bmod n = bf(\omega^k\omega^{ed-l}) \bmod n = \omega^k\omega^{k(p-l)(q-l)} \bmod n = \omega^k \times 1 = \omega^k \quad (8)$$

e) Анализ безопасности

Алгоритм основан на сложности факторизации. e не публично, а факторизация $N=pqr$ сложна, противник не может разложить N, поэтому ed не могут быть вычислены, k тоже.

2) Предложение 1

Если $x,k \in z+, k < \min(p,q,r)$, $x_k < n$ взаимно простое с n и N, алгоритм $E \in$ ЕНА – алгоритм гомоморфного шифрования.

а) Доказательство

Из ЕНА получим следующее уравнение:

$$E(x_k)=x^k x^{ed-1} \bmod N = x^{k+ed-1} \bmod N = x^{E1(k)} \bmod N \quad (9)$$

Где $E_1(k)=k+ed-l$. Тогда

$$bf\, D(x^{E1(k)} \bmod N) = (x^{E1(k)} \bmod N) \bmod n = (^{xk+ed-l} \bmod N) \bmod n \quad (10)$$

Раз $N=nr$, (10) перепишем как:

$$D(x^{E1(k)}) = x^{k+ed-1} \bmod n = x^k x^{k(p-1)(q-1)} \bmod n = x^k \times 1 = x^k \quad (11)$$

Из корректности ЕНА, получим $D(E(x^k))=x^k$. Следовательно

$$D(E(x^k))=D(x^{E1(k)})=x^k \quad (12)$$

По определению 2 получим искомое. Чтобы зашифровать полином и организовать вычисление без взаимодействия, установим следующее предложение.

3) Предложение 2

Если полином $f(x)=\sum a_i x^i < n$, можно воспользоваться ЕНА, чтобы зашифровать f(x). Также можно использовать вычисление без взаимодействие, как было описано выше.

а) Доказательство

Согласно ЕНА, зашифрованный вид f(x) выглядит так:

$$E(f(x)) = \sum a_i^{eidi} x^{eidi-1+i} \bmod N.$$

Расшифруем: $D(E(f(x))) = \sum a_i^{eidi} x^{eidi-1+i} \bmod N \bmod n$

Раз N=nr, то получим

$$\left(\sum_{i=0}^{m} a_i^{e_i d\, t} x^{e_i d_i - 1 + i} \mathrm{mod N}\right)\mathrm{mod n}$$

$$= \left(\sum_{i=0}^{m} a_i^{e_i d_i - 1 + 1} x^{e_i d_i - 1 + i}\right)\mathrm{mod n}$$

$$= \sum_{i=0}^{m} [(a_i^{e_i d_i - 1} a_i) \bmod n (x^{e_i d_i - 1} x^i) \bmod n] \mathrm{mod n}$$

$$= \sum_{i=0}^{m} (1 \times a_i)(1 \times x^i) \bmod n] = \sum_{i=0}^{m} a_i x^i = f(x)$$

Пример

A. Функция

Возьмём функцию $f(x)=4x^2+5x^3$, $x \in z+$. У Боба есть x = 3 и закодированная функция, Алиса хочет, чтобы Боб посчитал f(x), но не узнал что-то существенное о f.

B. Решение

Воспользуемся полученными выше результатами, чтобы достичь нашей цели.

C. Алиса кодирует сообщение

Выбирает p=1049, q= 1097, r= $1$019. and then n=pq = 1150753, N = nr= 1172617307, (p-l)(q-l) = 1148608. $e_1=3$, $d_1= 765739$; $e_2= 5$, $d_2= 689165$. Публичное только N. Степени $k_1= 2$ и $k_2= 3$, коэффициенты $C_l = 4$: $k_1= 1$ и $c_2= 5$: $k_4=1$. Кодируем степени:

$k_3=1$, $E_1 (k_3)=k_3+e_1d_1-1=2297217$, $k_4=1$,$E_2(k_4)=k_4+e_2d_2-1=3445825$

И коэффициенты:

$c_1=4$, $E(c_1)=c_1E_1(K_3) \bmod N = 538552408$, $c_2 = 5$, $E(c_2)=c_2E_2(k_4) \bmod N = 939014453$

Функция:

$$E(\mathbf{f(x)}) = E(c_1)x^{E1(k2)} + E(c_2)x^{E2(k3)}=E(c_1)x^{E1(2)}+E(c_2)x^{E2(3)} = 538552408x^{2297218}+939014453x^{3445827}$$

И отправляет его Бобу.

D. Боб занимается вычислениями, ничего не зная о сути функции f

$$E(f(5))=(538552408\times5^{2297218}+ 939014453\times5^{3445837}) \bmod N =$$
$$(538552408\times1148451519+93901+1453\times23015185) \bmod N = (803225694 + 1100120493)$$
$$\bmod N = 730728880$$

И отправляет Алисе.

E. Алиса декодирует ответ

$f(5)=D(E(f(5))) = E(f(5)) \bmod n=730728880 \bmod 1\ 150753=725$,

$f(5)=4\times5^2+5\times5^3=4\times25+5\times125=100+625=725$

Два результата совпали, свою цель наше корректное шифрование выполнило.

Выводы

Гомоморфное шифрование – довольно важный раздел криптографии, который становится всё более популярным объектом для исследований. Но текущие методы гомоморфного шифрования (в частности, RSA), оставляют утечку скелета полинома (например, ax^3+bx^4), что не может быть положительно воспринято.

В данной статье был рассмотрен способ, основанный на RSA, и доказана его корректность, а также приведён пример шифрования, обеспечивающего возможность вычисления без взаимодействия. Закодированная функция не раскрывает скелет полинома.

Источники

[1] R.Rivest, L.Adleman, M. Dertouzos. On data banks and privacy homomorphisms [журнал], опубликован: Foundations of Secure Computation, 1978, стр.169-179
[2] T.Sander, C Tschudin. Towards mobile cryptography[конференция], опубликовано: Proc of the 1998 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 1998
[3] T.Sander, C.Tschudin. Protecting Mobile Agents Against Malicious Hosts[журнал], опубликован: Mobile Agent Security, 1998, стр.44-60
[4] Liang Chen, Chengmin Gao. Public Key Homomorphism Based on Modified ElGamal in Real Domain[конференция]. Опубликован: 2008 International Conference on Computer Science and Software Engineering.Vol3, стр.802-805.2008.