матизация производственных процессов": материалы конференции, Минск, 28-29 октября 2009 г. – Минск, 2009. – С. 69-70.

8. Шутько, Н. П. Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов текста / Н. П. Шутько, П. П. Урбанович // Информационные технологии: материалы 83-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4-15 февраля 2019 г. / отв. за изд. И. В. Войтов; УО БГТУ. – Минск: БГТУ, 2019. – С. 41-43.

УДК 004.056+003.26

Студ. М. А. Тихонович
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий,БГТУ)

КРИПТОСТОЙКОСТЬ ГОМОМОРФНЫХ ШИФРОВ

Гомоморфное шифрование – форма шифрования, позволяющая производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполняемых с открытым текстом.

Задачи гомоморфной криптографии:

– необходимо производить вычисления над зашифрованными данными так, чтобы результат после расшифрования соответствовал результату тех же вычислений над открытыми данными (m_1 иm_1). Сформулирована в 1978 году Ривестом, Адлеманом и Дертузосом. Является основной для систем полностью гомоморфного шифрования (FHE);

– имеется 2 или более стороны. Необходимо вычислить произвольную функцию, аргументы которой являются секретными данными этих сторон, таким образом, чтобы ни одна из сторон не узнала вход другой стороны, а результат вычисления функции был корректен. Сформулирована Яо в 1982 году. Является основной задачей протоколов секретных распределенных вычислений (SMC).

Риверст и Адлеман впервые обосновали, что методом, позволяющим успешно проводить операции над зашифрованными данными, не искажая и не расшифровывая их, является так называемое гомоморфное шифрование [1].

Полностью гомоморфные схемы шифрования позволяют выполнять арифметические операции над зашифрованными данными без их предварительного расшифровывания. Частично гомоморфные

криптосистемы обладают свойством гомоморфности относительно только одной операции, например, сложения или умножения

Система шифрования является гомоморфной относительно операции умножения, если

$$D(E(m_1)\otimes E(m_2))=m_1*m_1.$$

Система шифрования является гомоморфной относительно операции сложения, если

$$D(E(m_1)\oplus E(m_2))=m_1+m_1.$$

Система шифрования является гомоморфной относительно операций умножения и сложения, т.е. полностью гомоморфной, если

$$D(E(m_1)\otimes E(m_2))=m_1*m_1 \text{ и } D(E(m_1)\oplus E(m_2))=m_1+m_1,$$

где $\otimes$, $\oplus$– операции умножения и сложения над шифрованными текстами, соответствующие операциям умножения и сложения над открытыми текстами; D – функция расшифрования; E – функция зашифрования.

Если криптосистема с такими свойствами сможет зашифровать два бита, то, поскольку операции сложения и умножения формируют над битами полный по Тьюрингу базис, становится возможным вычислить любую булеву функцию, а, следовательно, и любую другую вычислимую функцию.

Любую стандартную систему шифрования можно описать в виде трех операций: генерации ключей, зашифрования и расшифрования [2, 3]. Гомоморфная система шифрования, кроме трех перечисленных выше операций, включает в себя операцию вычислений. Таким образом, в каждой гомоморфной криптосистеме можно выделить некоторые общие алгоритмы:

– генерация секретного ключа *sk* и открытого ключа *pk*;
– функция зашифрования *Enc*;
– функция расшифрования *Decrypt*;
– гомоморфное вычисление *Eval*;

Функция зашифрования *Enc* представляется в следующем виде:

$$C = Enc\ (pk, O),$$

где O – принимаемый на вход алгоритма открытый текст; C – полученный шифротекст.

Функция расшифрования *Decrypt* в математическом виде представляется следующим образом:

$$O = Decrypt(sk, C).$$

Гомоморфное вычисление *Eval* оперирует некоторой математической функцией *f()* и парой шифротекстов C_1, C_2. Результатом вычисления будет некий шифротекст C, причем такой, что:

$$C = Eval(f(), C_1, C2), \qquad O = Decrypt(sk, C) = f(O_1, O_2) .$$

Схематично алгоритм *Eval* можно представить следующим образом [4].

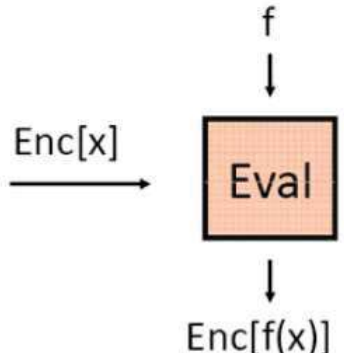

Рисунок 1 – Алгоритм Eval

На вход алгоритму подается зашифрованное сообщение *Enc(M)* и некая математическая функция *f()*. Результатом работы алгоритма является другое зашифрованное сообщение $Enc(M_2)$, причем $M_2=f(M)$.

Операции гомоморфного шифрования:

– генерация ключей: клиент генерирует открытый ключ *pk* и секретный ключ *sk* для шифрования открытого текста;

– зашифрование: используя секретный ключ *sk*, клиент шифрует открытый текст *O*, и вместе с открытым ключом *pk* отправляет шифрованный текст *C* на сервер;

– вычисление: сервер получает функцию *f()* для проведения вычислений над шифрованным текстом *C* и выполняет их в соответствии с требованиями данной функции, используя *pk*;

– расшифрование: для получения искомого результата значение *Eval(f(O))*, полученное в ходе вычислений, расшифровывается клиентом с использованием своего секретного ключа *sk*.

Рассмотрим частично гомоморфную схему, а именно схему гомоморфную относительно операции сложения [5]. Данная схема построена на группе вычетов целого числа *N*. Таким образом, закрытый ключ в данной схеме представляет собой целое число, на которое накладываются следующие условия:

– число должно быть много больше *N*;

– число должно быть взаимно простым с *N*;

Этапы шифрования и некоторые подробности реализации частично гомоморфной схемы относительно операции сложения:

1. ***Выбор числа N***. Группа целых чисел, с которыми способна работать криптосистема генерируется как, группа вычетов по модулю *N*. Таким образом, в качестве открытого текста могут выступать числа от 0 до *N*.

2. ***Генерация ключей***. Генерируется случайное число *sk*, такое что $sk >> N$ и НОД(*sk*, *N*) = 1. В данной реализации накладывается еще одно условие: $sk \leq 2^{31}$, т.к. при $sk > 2^{31}$ число выходит за границу диапазона структуры данных Int32.

Открытым ключом *pk* является набор больших чисел $\{a_1, a_2,..,a_n\}$ таких что $a_i \bmod N = 2e_i$, где $e_i << N$. В данной реализации *N* является константой.

3. ***Зашифрование***. Функция зашифрования принимает на вход открытый текст *O* и открытый ключ *pk*. Из набора *pk* случайным образом выбирается 50 элементов a_i и суммируются с *O*.

4. ***Дешифрование***. Алгоритм дешифрования принимает на вход шифротекст *C* и секретный ключ *sk*. Открытый текст $O = (C \bmod sk) \bmod N$.

5. ***Операции над шифротекстом***. Как было сказано ранее, описанная схема является гомоморфной только относительно операции сложения. Поэтому, для того чтобы произвести операцию над зашифрованными данными, достаточно просто сложить или вычесть два шифротекста.

Плюсом данной гомоморфной системы относительно других гомоморфных систем является малая потребность в вычислительных ресурсах.

Минусы данной гомоморфной системы относительно других гомоморфных систем.

1. Данная схема оперирует с числами из группы вычетов некоторого числа *N*, что означает, что множество открытых текстов – конечное.

2. Описанная схема – частично гомоморфная, поэтому в ней доступна лишь операция сложения.

Свыше 30 лет оставалась нерешенной задача полностью гомоморфного шифрования − создания системы, гомоморфной относительно операций сложения и умножения одновременно. Только в 2009 г. аспирант Стэндфордского университета и стажер IBM Крейг Джентри теоретически обосновал принципиальную возможность создания такой системы шифрования. В схеме Джентри [6] выполняются свойства гомоморфизма как относительно умножения, так и сложения, т. е. она является алгебраической гомоморфной системой.

Следует учитывать, что некоторые гомоморфные криптосистемы могут поддаваться преднамеренным внешним воздействиям (например, принципиально уязвимы к атаке с адаптивно подобранным шифрованным текстом) и поэтому не всегда подходят для безопасной передачи данных в компьютерных системах и сетях [7].

ЛИТЕРАТУРА

1. Rivest, R.L. On data banks and privacy homomorphisms / R.L. Rivest, L. Adleman, M.L. Dertouzos // Foundations of secure computation. – 1978. – Vol. 32, no. 4. – P. 169–178.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ./ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

3. Урбанович, П. П. Информационная безопасность и надежность систем: учебно-методическое пособие по одноименному курсу для студентов специальности 1-40 01 02-03 "Информационные системы и технологии" / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. – Минск : БГТУ, 2007. – 87 с.

4. Гомоморфное шифрование своими руками. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/150067/. – Дата доступа: 12.04.2019.

5. Gentry G.A Fully Homomorphic Encryption Scheme, 2009 – P. 71-80.

6. Gentry, C. A Fully homomorphic encryption using ideal lattices / C. Gentry // Symposium on the Theory of Computing (STOC). – Bethesda, USA, 2009. – P. 169–178.

7. Урбанович, П. П. Компьютерные сети: учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. – Минск: БГТУ, 2011. – 399 с.