УДК 003.26

ГОМОМОРФИЗМ В КРИПТОГРАФИИ

Д. О. Мартыщенко
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Работа посвящена поиску лучших методов шифрования и оптимальному применению гомоморфизма в криптографии. Рассмотрена гомоморфная система с учетом ее недостатков. Целью работы является определение недостатков гомоморфного шифрования и способов их устранения без потерь ресурсов, времени и конструктивной информации. Результаты исследования могут быть использованы для сохранения конфиденциальности пользователя в процессах поиска, хранения или передачи информации.
Ключевые слова: криптография, гомоморфное шифрование, шифр, зашифрованный запрос, ключ дешифрования.

HOMOMORPHISM IN CRYPTOGRAPHY

D. O. Martyshchencko
Don State Technical University (Rostov-on-Don, Russian Federation)

The article is devoted to the search for the best encryption methods and the optimal use of homomorphism in cryptography. A completely homomorphic system with its drawbacks is considered. The purpose of this work was to identify specific shortcomings of fully homomorphic encryption today and how to solve them without losing resources, time and valuable information. The results of the study can be used to preserve the absolute confidentiality of the user in the process of searching, storing or transmitting information.
Keywords: cryptography, homomorphic encryption, cipher, encrypted request, decryption key.

Введение. В работе рассмотрена полностью гомоморфная схема шифрования, решающая главную задачу криптографии, а также приведены альтернативные решения поставленной задачи. Полностью гомоморфная схема позволяет вычислять произвольные функции по зашифрованным данным без ключа дешифрования. Это данные шифрования $E(m_1), E(m_2), ..., E(m_t)$, где параметры $m_1, m_2, ..., m_t$ позволяют эффективно вычислить зашифрованный текст, который шифруется как $f(m_1, m_2, ..., m_t)$ для любой эффективно вычислимой функции f [1, 2]. Данная проблема рассматривалась еще в 1978 г. Ривестом (Ronald Linn Rivest).

Возможности гомоморфного шифрования. Полностью гомоморфное шифрование имеет множество применений. Например, оно позволяет реализовывать частные запросы к поисковой системе. Пользователь отправляет зашифрованный запрос и поисковая система вычисляет сжатый зашифрованный ответ, даже не воспринимая запрос в открытом виде. Такое шифрование также позволяет выполнять поиск по зашифрованным данным. В этом случае пользователь хранит зашифрованные файлы на удаленном сервере и позже может обязать сервер извлекать только те файлы, которые при расшифровке удовлетворяют некоторому логическому ограничению, даже если сервер не может расшифровать файлы самостоятельно. В более широком смысле, полностью гомоморфное шифрование повышает эффективность безопасных множественных вычислений.

Недавно появилась криптосистема, способная быть гомоморфной одновременно для математических операций сложения и умножения. Данная криптосистема получила название системы полностью гомоморфного шифрования. Проблематичность создания такой системы заключалась в том, что при каждой операции над текстом добавлялся «шум», мешающий

расшифровке, в какой-то момент накопления он полностью перекрывал текст и делал расшифровку невозможной.

Гомоморфное шифрование производит некоторые операции с зашифрованным текстом, что позволяет совершить математические действия с открытым текстом. Например, наиболее популярная криптосистема с открытым ключом RSA гомоморфна для операции умножения. Алгоритм RSA, первый из алгоритмов шифрования с открытым ключом, достойно выдержал испытание временем. Это алгоритм, основанный на задаче RSA [3], заключается в поиске простых делителей больших натуральных чисел. Можно утверждать, что криптостойкость алгоритма RSA базируется на сложности проблемы факторизации, но не в полной мере, поскольку задачу RSA можно решать, не прибегая к разложению модуля на множители.

Пусть некоторый пользователь А считает нужным разрешить всем желающим отправлять ему конфиденциальные сообщения, расшифровать которые способен только он. Тогда А подбирает два больших простых числа p и q. Держа эти числа в секрете, А публикует их произведение $N = p \times q$, которое называют модулем алгоритма [4, 5]. Кроме того, А выбирает число Е, удовлетворяющее соотношению:

$$\text{НОД}\big(E, (p-1)(q-1)\big) = 1.$$

Открытым ключом доступа является пара *(N, E),* секретным — *(N, D)*, где *D* удовлетворяет сравнению:

$$ED = 1\big(mod(p-1)(q-1)\big).$$

Число *D* можно найти, используя алгоритм Евклида.

Допустим, что некий пользователь Б намерен передать конфиденциальное сообщение пользователю А. Для этого он использует открытое сообщение в виде последовательности чисел или одного числа $m < N$. Зашифрованное сообщение C извлекается из открытого сообщения M следующим образом:

$$C = M^E (mod\ N).$$

Пользователь А расшифровывает послание следующим образом:

$$M = C^D (mod\ N).$$

Однако, как упоминалось выше, RSA имеет немаловажную проблему — каждая подобная операция добавляет «шум» в криптотекст, в следствие чего расшифровка либо сильно затруднена, либо невозможна. Крэйг Гэнтри один из первых опубликовал пример первой функции, которая решала подобную проблему. Он использовал двойное шифрование, согласно которому через определенное количество шифров необходимо «избавиться от верхнего слоя» и убрать накопившийся за это время «шум».

Физические аналоги шифрования, Необходимо отметить, что затруднительно создать идеальный физический аналог полностью гомоморфного шифрования, который являлся бы достаточно корректным. Рассмотрим гомоморфное шифрование с точки зрения физической аналогии темной комнаты разработчика фотографий для конкретного пользователя. Разработчик применяет определенную функцию *f*, то есть последовательность шагов для разработки готового продукта. Ему не нужно ничего видеть, чтобы применить эту процедуру. Эта аналогия неадекватна обычной практике тем, что разработчик не может выйти из темной комнаты и оценить готовый продукт. Такую оценку может провести только пользователь и никто более, потому что «Взгляд» — это его секретный ключ.

Рассмотрим другую физическую аналогию. Предположим, что владелец ювелирного магазина (пользователь) хочет, чтобы его работники монтировали исходные драгоценные материалы (алмазы, золото и т. д.) в готовые изделия. Пользователь беспокоится о краже и решает

проблему путем создания «перчаточных» боксов, от которых только у него есть ключ, и только он кладет исходные материалы внутрь. Используя перчатки, работник может манипулировать предметами внутри бокса. Более того, работник может положить инструмент в бокс — например, паяльник для обработки изделия, но он не может ничего оттуда извлечь. Кроме того, бокс прозрачен, так что работник может видеть, что он делает. В этой аналогии шифрование означает, что работник не может взять что-то из бокса, но может увидеть его содержимое. После того, как работник закончил техпроцесс, пользователь может извлечь готовый продукт, используя свой ключ. Эта аналогия неадекватна реальному процессу тем, что «перчаточный» бокс может стать загроможденным, в то время как в полностью гомоморфной схеме шифрования в боксе остается только конечный продукт. Однако у работника имеется способ заставить любой инструмент исчезнуть из перчаточного бокса.

Методика шифрования. Решение Крэйга Гэнтри заключается в криптографии на эрмитовых решетках. Нормальная форма идеальной решётки J имеет вид:

$$HNF(J) = \begin{bmatrix} d & \cdots & 0 \\ \vdots & \ddots & \vdots \\ -[r^{n-1}]_d & \cdots & 1 \end{bmatrix},$$

где $D = det(J)$; r — корень для $f_n(x)$ по модулю d.

Шифрование происходит следующим образом. Пусть требуется зашифровать бит $m \in (0,1)$, на входе имеется бит b и открытый ключ V. Выбирается шумовой вектор, компоненты которого принимают значения 0,1 и –1,0. Затем вычисляется вектор $a = 2u+be_1$, а шифротекст вычисляется по формуле:

$$C = a \bmod V = a - ([aV^{-1}]V).$$

Здесь для базиса V пространства L и данного вектора c выражение $c \bmod V$ используется для обозначения вектора $c' \in P(V)$ такого, что c — $c' \in L$. Для расшифровки имеется вектор C, а также матрицы V и W [6]. Исходный бит b получается в результате операции:

$$b = a \bmod 2 = (c \bmod V) = \left(c\left(\frac{W}{d}\right)\right) \bmod 2.$$

Шифрование гомоморфно относительно математических операций сложения и умножения, операции следует выполнять в базисе V.

Заключение (выводы). Реализация полностью гомоморфного шифрования возможна, но только при определенных условиях. Альтернативами такому шифрованию являются неполное гомоморфное шифрование и секретные распределенные вычисления. Все вычисления производятся не одним единственным блоком (узлом), шифрование происходит за счет вычислений сервера с помощью множества узлов. Чтобы сохранить конфиденциальность используется аддитивно гомоморфная схема, когда каждый отдельный узел и сервер выполняют вычисления функции по отдельно взятым частям секрета исходных данных, которые были предоставлены пользователем. Сегодня существует ряд платформ, позволяющих производить подобные вычисления, например, программы SEPIA, SecureSLM, FairPlayMP, TASTY, VMCrypt SHAREMIND, VIFF.

Библиографический список

1. Здор, С. Е. Кодированная информация. От первых природных кодов до искусственного интеллекта / С. Е. Здор. — Москва : Либроком, 2012. — 168 с.

2. Зубов, А. Н. Математика кодов аутентификации / А. Н. Зубов. — Москва : Гелиос АРВ, 2007. — 288 с.

3. Казарин, О. В. Методология защиты программного обеспечения. Научные проблемы безопасности и противодействия терроризму / О. В. Казарин. — Москва : Изд-во МЦНМО, 2009. — 464 с.

4. Криптография: скоростные шифры / А. А. Молдовян, Н. А. Молдовян, Н. Д. Гуц, Б. В. Изотов. — Санкт-Петербург : БХВ-Петербург, 2002. — 494 с.

5. Шнайер, Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. — Москва : Триумф, 2012. — 816 с.

6. Шумский, А. А. Системный анализ в защите информации / А. А. Шумский, А. А. Щелупанов. — Москва : Гелиос АРВ, 2005. — 224 с.

Об авторе:

Мартыщенко Дарья Олеговна, студент Донского государственного технического университета (344000, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), daria161sun@gmail.com

Author:

Martyschenko, Darya O., student, Don State Technical University (1, Gagarin square, Rostov-on-Don, 344000, RF), daria161sun@gmail.com