ВОПРОСЫ ПРИМЕНЕНИЯ ПРИКЛАДНОЙ ГОМОМОРФНОЙ КРИПТОГРАФИИ

Аракелов Г.Г.[1]

Аннотация

Гоморфное шифрование современная и многогранная область криптографии, которая обладает весомой практической значимостью для современного мира технологий. В данной статье рассматриваются некоторые практические аспекты гомоморфного шифрования.

Цель статьи: *исследование методов для организации гомоморфных вычислений, на основе комбинации частично гомоморфных схем шифрования.*

Метод: *Использование для шифрование открытого текста двух частично-гомоморфных схем, одна из которых аддитивная – вторая другая мультипликативная.*

Полученный результат: *дается кратикий исторический очерк полностью гомоморфного шифрования. Рассматривается подход к построению гомоморфных вычислений на базе комбинации частично-гомоморфных схем шифрования. Приводится пример использования комбинации схем RSA и Пэйе. Описанный подход позволяет организовать гомоморфное вычисления с приемлимыми вычислительными затратами.*

Ключевые слова: *Полностью гомоморфное шифрование, частично-гомоморфное шифрование, комбинация схем шифрования, вычислимость функций, полином Жегалкина*.

DOI:10.21681/2311-3456-2019-5-70-74

Введение

Гомоморфное шифрование — форма шифрования, позволяющая производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполняемых с открытым текстом. Например, один человек мог бы сложить два зашифрованных числа, а затем другой человек мог бы расшифровать результат, не используя ни одно из них.

Особый же интерес представляла возможность построения **полностью гомоморфного шифрования**, т.е. шифрования, позволяющего проводить над шифртекстами любые необходимые вычисления. Впервые идея полностью гомоморфного шифрования была предложена в 1978 году изобретателями криптографического алгоритма с открытым ключом RSA Рональдом Ривестом и Ади Шамиром совместно с Майклом Дертузосом. Уже сама криптосистема RSA обеспечивала мультипликативный гомоморфизм, т.е. позволяла выполнять операцию умножения над шифртекстами, и после расшифрования извлекать из полученного шифротекста произведение исходных текстов, т.е. выполнялось следующее:

$$Dec(Enc(m_1)\otimes Enc(m_2))=m_1m_2$$

Однако на начальных этапах попытки создания полностью гомоморфных криптосистемы неудачны. Многие годы было непонятно, возможно ли вообще полностью гомоморфное шифрование, хотя попытки создания такой системы предпринимались неоднократно. Так, например, криптосистема, предложенная в 1982 году Шафи Гольдвассером и Сильвио Микали, имела достаточно высокий уровень криптостойкости, но была лишь частично гомоморфной (гомоморфной только по сложению), и могла зашифровать только один бит. Еще одна аддитивно гомоморфная система шифрования была предложена в 1999 году Паскалем Пэйе. Прорыв в развитии полностью гомоморфного шифрования приходится на 2009 год, когда Крейг Джантри в работе [13] впервые предложил вариант полностью гомоморфной криптосистемы, основанной на криптографии на решетках. С тех пор появилось большое количество работ, среди которых [10], [11], [13] в которых предлагается модификация криптосистемы Джантри с целью улучшения ее производительности. В работе [6] представлена полностью гомоморфная схема шифрования на основе матричных полиномов.

Для того, чтобы криптосхема была полностью гомоморфной достаточно ее гомоморфности одновременно и по операции сложения, и по операции умножения,

$$Dec(Enc(m_1)\otimes Enc(m_2))=m_1m_2$$
$$Dec(Enc(m1)\oplus Enc(m_2))=m_1+m_2$$

где$\otimes$ и $\oplus$ — операции над шифротекстами, соответствующие операциям $*$ и $+$ над открытыми текстами.

Достаточность гомоморфизма по сложению и умножению следует из того, что над битами операции сложения и умножения формируют полный по Тьюрингу базис. Следовательно, если такая криптосистема сможет надежно шифровать два бита, то станет возможным вычислить любую булеву, а следовательно, и любую вычислимую функцию.

1 Построение полностью гомоморфной схемы шифрования на базе частично-гомоморфных

Для того, чтобы некоторая схема шифрования была полностью гомоморфной, необходимо и достаточно ее гомоморфности относительно операций сложения и умножения. В настоящее время разработано уже достаточное

1 Аракелов Гургенович, аспирант механико-математического факультета Московского государственного университета им М.В. Ломоносова, г. Москва, Россия. E-mail: g.g.arakelov@gmail.com

УДК 004.382.2 DOI: 10.21681/2311-3456-2019-5-70-74

количество полностью гомоморфных схем шифрования, однако до сих пор не существует схемы, которая была бы практически полезна. Все существующие полностью гомоморфные схемы шифрования в большей мере являются пока лишь теоретическими и их практическое применение пока невозможно. В тоже время, уже довольно давно, существуют эффективные схемы, обладающие свойствами частичного гомоморфизма. Основная идея данной работы — это построение полностью гомоморфной схемы шифрования на базе частично-гомоморфных схем.

Пусть Z_p – это пространство открытых шифротекстов. Пусть у нас имеется две схемы шифрования: A и M где A — аддитивная схема шифрования, а M — мультипликативная. Enc и Dec — это функции шифрования и расшифровки соответствующих схем. Будем обозначать CIPH(A) — пространство шифротекстов криптосхемы A. Без потери общности можно пренебречь типом схемы шифрования, а именно, не учитывать сейчас являются схемы симметричными или нет, а также какие ключи используются для шифрования и расшифровки. Предполагаем, что пространство открытых шифротекстов у данных схем совпадает.

Предположим, что существует функция$g_{M\to A(\cdot)}$, такая, что выполняется следующее условия:

$\forall m\in Z_p(m^*=Enc^*_M(m))\leftrightarrow g(m^*)=m^+$ и $Dec_A^*(m^+)=m$

То есть, функция g по некоторому заданному шифротексту в мультипликативной схеме шифрования строит шифротекст соответствующий тому же элементу в адитивной схеме.

Построим схему шифрования, состоящую из следующих компонентов{A+ M^* g_{MA}()Enc() Dec() }.

1.1 Шифрование

Шифротекстом для открытого текста m будет являться вектор состоящий из двух элементов:

$$Enc(m)= \bar{v} =\{Enc_A(m)\ Enc_M(m)\}$$

Мы для каждого открытого текста m храним по сути два шифротекста, один в аддитивной схеме, а второй в мультипликативной.

1.2. Расшифрование

Функция расшифровки выглядит следующим образом:

$Dec(\bar{v}) =Dec_A \bar{v}_1$

Здесь мы для расшифровки используем аддитивную схему шифрования, но мы также могли бы использовать и мультипликативную. В этом случае нам пришлось бы использовать второй элемент вектора.

1.3. Вычисления

Пусть мы хотим вычислить некоторую функцию, вычисление которой сводится к вычислению некоторого полинома. Без потери общности можно считать, что алгоритм вычисления данной функции состоит из последовательности сложений и умножений. Через *a* - будем обозначать шифротекст соответствующий элементу a. Напомним, что a является вектором, поэтому мы будем обозначать через a —аддитивную составляющую шифра, а через a — мультипликативную соответственно. Рассмотрим несколько случаев, к которым сводится вычисление любого полинома.

$(a+b)=Dec(a^{',1}+b^{',1})$

$a*b=Dec(a^{',2}+b^{',2})$

$a*b+c=Dec(g(a^{',1}\cdot b^{',2})_1+c^{',1})$

С помощью индукции легко доказать, что если мы умеем гомоморфно вычислять выражения, представленные выше, то мы также можем гомоморфно вычислить и произвольный полином.

2 Комбинация схем

2.1. RSA + Пэйе

Рассмотрим вопрос построения функции $g(\cdot)$ для криптосхемы RSA и криптосхемы Пэйе. Для полноты изложения приведем алгоритмы обеих схем.

RSA

Генерация ключей

1. Выбираются два больших простых числа p,q
2. Вычисляется $n=p\cdot q$ и значение функции Эйлера $\varphi(n)=(p-1)(q-1)$
3. Выбирается небольшое n, взаимно простое с $\varphi(n)$
4. Вычисляется d, обратное к e по модулю $\varphi(n)$, $ed\equiv 1\varphi(n)$
5. Пара P=(e,n) публикуется в качестве открытого ключа
6. Пара S=(d,n) публикуется в качестве закрытого ключа

Шифрование

Функция шифрования $E_P(m)$, где P – определенный выше открытый ключ, а m — открытый текст, строится следующим образом:

$$E_P(m)=m^e n$$

Дешифрование

Функция расшифровки $D_S(c)$, где c — шифротекст, а S секретный ключ, определяется следующим образом:

$D_S(c)=c^d n$

Криптосистема Пэйе

Генерация ключей

1. Выбираются два больших простых числа p и q такие, что $gcd(pq,(p-1)(q-1))=1$.
2. Вычисляется $n=pq$ и $\lambda=lcm(p-1,q-1)$
3. Выбирается случайное целое число g, такое что $g\in Z$
4. Вычисляется $\mu=(L(g^\lambda n^2))^{-1} mod n$
5. Открытым ключом является пара (n,g)
6. Закрытым ключом является пара (λ,μ).

Шифрование

1. Предположим, что необходимо зашифровать открытый текст m, $m\in Z_n$.
2. Выбираем случайное число r, $r\in Z^{*,n}$
3. Вычисляем шифротекст $c=g^m\cdot r^n mod n^2$

Расшифрование

1. Принимаем шифротекст $c\in Z^{*,n}$.
2. Вычисляем исходное сообщение $m=L(c^\lambda mod n^2)\cdot\mu mod n$

Задача построения функции g(·)

Мы можем добиться совпадения пространства открытых текстов в обеих схемах шифрования, если зафиксируем для обеих схем одно и то же значение параметра n. Это означает, что мы выбираем одни и те же значения p и q.

Будем считать, что мы зафиксировали все параметры двух криптосхем, выбрав для обеих схем одинаковые значения p и q, а также построили открытые и закрытые ключи. У нас имеется пара схем {A,M}, где A — это аддитивная схема Пэйе, а M — мультипликативная схема RSA.

Рассмотрим задачу о построении функции g(·), которая по заданному шифру в системе RSA строит соответствующий шифр в системе Пэйе.

Пусть дано некоторое зашифрованное схемой RSA сообщение m'. По определению:

$$m'=m^e n \qquad (1)$$

Ввыражении(?)известнымисчитаютсяе и *n*, а *m* - является зашифрованным сообщением, которое считается неизвестным. Функция *g*(·) должна по данному *m'* и известным e,g и n, построить c, $c \in Z^{2,n}$ и c представимо в виде (2), где r — произвольный элемент $Z^{2,n}$ такой, что:

$$c=g^m \cdot r^n n^2 \qquad (2)$$

Если удастся построить такую функцию g(·), то мы сможем построить полностью гомоморфную схему шифрования. Здесь необходимо учитывать, что функция должны быть построены таким образом, чтобы полученная система оставалась криптостойкой.

2.2 Криптостойкость при комбинации схем

Для построения комбинации мы можем использовать криптосхемы, стойкость которых уже доказана. Однако, это не означает, что построенная схема с помощью композиции также окажется криптостойкой. В предыдущем параграфе, например, мы выбрали в качестве криптосхем RSA и Пэйе. Если мы будем использовать схемы без дополнительных ограничений на выбор параметров, то в это случае, можно говорить о криптостойкости их совместного использования. Можно считать, что каждая из них в отдельности является криптостойкой, однако нельзя утверждать, что использование их комбинации приведет к такой же по надежности схеме.

3 Практическое гомоморфное шифрование

Как было сказано выше, все существующие схемы полностью гомоморфного шифрования в настоящий момент далеки от их внедренияв практическое использование. При этом существует достаточное количество практически интересных схем со свойствами частичного гомоморфизма. Примером может служить схема RSA, обладающая мультипликативным гомоморфизмом. Среди аддитивных схем шифрование, также существуют модели с практически интересными временными оценками. Если предположить, что существуют такие две схемы шифрования *A*,*M*, и функция $g_{M \to A}$, что каждая из схем обладает приемлемыми временными оценками, а также алгоритм, вычисляющий функцию *g*, то мы смогли бы получить полностью гомоморфную схему шифрования, которая оказалась бы практически полезна. Одним из подходов к построению полностью гомоморфных схем шифрования, может считаться подход описанный выше, который заключается в том, что мы пытаемся подобрать одну аддитивную схему шифрования, а вторую мультипликативную и построить отображение шифротекстов из мультипликативной в аддитивную.

Рассмотрим на примере клиент-серверной архитектуры, когда у клиента имеются конфиденциальные данные, которые нужно хранить и обрабатывать на стороне сервера. На практике добиться возможности производить вычисления над зашифрованными данными можно следующим образом.

1. Выбираем две частично-гомоморфные схемы шифрования (например RSA + Пэйе) {A,M}
2. В качестве функции g возьмем следующую: $g^{(m'M)}=Enc_A(Dec_M(m'^{,M}))$

   Здесь, m — открытый текст, $m'^{,B}=Enc_M(m)$

Такое определение функции *g* приводит, к тому, что данная схема перестает быть полностью гомоморфной, так, как в вычислениях требуется расшифровка и зашифровка промежуточных значений. С теоретической точки зрения, мы, конечно, таким образом не получим полностью гомоморфную схему шифрования, но с практической стороны, такое определение позволит нам производить вычисления над зашифрованными данными без их расшифровки на стороне вычислителя.

Идея данного подхода заключается в том, что мы строим криптосхему, как было описано в разделе 1. Предположим, что данные хранятся на удаленном сервере, на котором необходимо производить вычисления произвольных функций. В том момент, когда алгоритму, вычисляющему значение функции, необходимо произвести «перевод» промежуточного результата из одной схемы шифрования в другую, а точнее из мультипликативной в аддитивную, сервер отправляет клиенту запрос на проведение таких операций. Клиент, обладая ключами шифрования, расшифровывает полученное от сервера значение, шифрует его в аддитивной схеме шифрования и отправляет назад серверу. Сервер, получив значение от клиента, продолжает вычисления.

В итоге, заданная функция вычисляется на стороне сервера таким образом, что сервер не получает доступа к закрытой информации.

Литература

1. Arakelov G. G. Gribov A. V. Mikhalev A. V. Applied homomorphic cryptography: examples // Journal of Mathematical Sciences. — 2019. — Vol. 237, no. 3. — P. 353–361.
2. Аракелов Г. Г. Грибов А. В. Михалев А. В. Прикладная гомоморфная криптография: примеры // Фундаментальная и прикладная математика. — 2016. — Т. 21, № 3. — С. 27–38.
3. Грибов А. В. Золотых П. А. Михалёв А. В. Построение алгебраической криптосистемы над квазигрупповым кольцом // Математические вопросы криптографии. — 2010. — Т. 1, № 4. — С. 23–32.
4. Катышев С.Ю. Марков В.Т. Нечаев А.А. Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей // Дискретная математика — 2014. — Т. 26, № 3. — С. 45–64.
5. Кузьмин А. С. Марков В. Т. Михалев А. А. Михалев А.В Нечаев А.А. Криптографические алгоритмы на группах и алгебрах// Дискретная математика — 2014. — Т. 26, № 3. — С. 45–64.
6. Буртыка Ф.Б. Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов // Известия Южного федерального университета. Технические науки.. 2014 стр. 107-122
7. D.Song, D.Wagner, A.Perrig Practical Techniques for Searches on Encrypted Data // University of California, Merkeley Security and Privacy,2000
8. R. Curtmola, J. Garay, S.Kamara, and R. Ostrovsky Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions // Proceedings of the 13th ACM conference on Computer and communication security. 2006
9. D. Cash, J. Jaeger, St. Jarecki, Ch. Jutla, H. Krawczyk, M-Cat. Rosu, and M. Steiner Highly-Scalable Searchable Symmetric Encryption with Support for Moolean Queries // Advances in Cryptology - CRYPTO 2013.
10. D. Moneh, C. Gentry, S. Halevi,F. Wang, D. J wu. Private database queries using somewhat homomorphic encryption // Applied cryptography and network security Springer, 2013,p.102-118.
11. D. Cash, J. Jaeger, St. Jarecki, Ch.t Jutla, H. Krawczyk, M-Cat. Rosu, and M. Steiner Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation // IACR Cryptology Fuzzy identity-based encryption // Advances in Cryptology – EUROCRYPT 2005. ePrint 2014.
12. D. Moneh, A. Sahai, M. Waters Functional encryption: Definitions and challenges // Theory od Cryptography. 2011 pp. 253-273
13. Gentry C. A fully homomorphic encryption scheme: Ph.D. thesis. – Stanford University. –2009
14. Stehle D., Steinfeld R. Faster fully homomorphic encryption // Advances in Cryptology-ASIACRYPT 2010. Springer Merlin Heidelberg. 2010 pp. 377-394

QUESTIONS OF APPLICATION OF APPLIED HOMOMORPHIC CRYPTOGRAPHY

***Arakelov G.G.*[2]**

Annotation

Homorphic encryption is a modern and multifaceted field of cryptography, which has a significant practical significance for the modern world of technology.

This article discusses some practical aspects of homomorphic encryption.

A brief historical sketch of fully homomorphic encryption is given. An approach to the construction of homomorphic calculations based on a combination of partially homomorphic encryption schemes is considered. An example of using a combination of RSA and Peye schemes is given.

Purposes: *The purpose of the article is to study methods for the organization of homomorphic calculations based on a combination of partially homomorphic encryption schemes.*

Method: *Use two partially homomorphic schemes for plaintext encryption, one of which is additive and the other is multiplicative.*

Results: *The paper presents an approach for the organization of homomorphic calculations based on a combination of partially homomorphic encryption schemes. The described approach allows to organize homomorphic calculations with acceptable computational costs.*

Keywords

Fully homomorphic encryption, partially homomorphic encryption, combination of encryption schemes, computability of functions, Zhegalkin polynomial.

References:

1. Arakelov G. G. Gribov A. V. Mikhalev A. V. Applied homomorphic cryptography: examples // Journal of Mathematical Sciences. — 2019. — Vol. 237, no. 3. — P. 353–361.

2 Gurgen Arakelov, M.V. Lomonosov, PhD student at Ehaniko And Mathematics Facultyof MoscowState University, Moscow, Russia. E-mail: g.g.arakelov@gmail.com

2. Arakelov G. G. Gribov A. V. Mihalev A. V. Prikladnaja gomomorfnaja kriptografija: primery // Fundamental'naja i prikladnaja matematika. — 2016. — T. 21, № 3. — S. 27–38.
3. Gribov A. V. Zolotyh P. A. Mihaljov A. V. Postroenie algebraicheskoj kriptosistemy nad kvazigruppovym kol'com // Matematicheskie voprosy kriptografii. — 2010. — T. 1, № 4. — S. 23–32.
4. Katyshev S.Ju. Markov V.T. Nechaev A.A. Ispol'zovanie neassociativnyh gruppoidov dlja realizacii procedury otkrytogo raspredelenija kljuchej // Diskretnaja matematika — 2014. — T. 26, № 3. — S. 45–64.
5. Kuz'min A. S. Markov V. T. Mihalev A. A. Mihalev A.V Nechaev A.A. Kriptograficheskie algoritmy na gruppah i algebrah// Diskretnaja matematika — 2014. — T. 26, № 3. — S. 45–64.
6. Burtyka F.B. Simmetrichnoe polnost'ju gomomorfnoe shifrovanie s ispol'zovaniem neprivodimyh matrichnyh polinomov // Izvestija Juzhnogo federal'nogo universiteta. Tehnicheskie nauki.. 2014 str. 107-122
7. D.Song, D.Wagner, A.Perrig Practical Techniques for Searches on Encrypted Data // University of California, Merkeley Security and Privacy,2000
8. R. Curtmola, J. Garay, S.Kamara, and R. Ostrovsky Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions // Proceedings of the 13th ACM conference on Computer and communication security. 2006
9. D. Cash, J. Jaeger, St. Jarecki, Ch. Jutla, H. Krawczyk, M-Cat. Rosu, and M. Steiner Highly-Scalable Searchable Symmetric Encryption with Support for Moolean Queries // Advances in Cryptology - CRYPTO 2013.
10. D. Moneh, C. Gentry, S. Halevi,F. Wang, D. J wu. Private database queries using somewhat homomorphic encryption // Applied cryptography and network security Springer, 2013,p.102-118.
11. D. Cash, J. Jaeger, St. Jarecki, Ch.t Jutla, H. Krawczyk, M-Cat. Rosu, and M. Steiner Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation // IACR Cryptology Fuzzy identity-based encryption // Advances in Cryptology – EUROCRYPT 2005. ePrint 2014.
12. D. Moneh, A. Sahai, M. Waters Functional encryption: Definitions and challenges // Theory od Cryptography. 2011 pp. 253-273
13. Gentry C. A fully homomorphic encryption scheme: Ph.D. thesis. – Stanford University. –2009
14. Stehle D., Steinfeld R. Faster fully homomorphic encryption // Advances in Cryptology-ASIACRYPT 2010. Springer Merlin Heidelberg. 2010 pp. 377-394