DOI 10.37882/2223-2966.2024.12-2.09

ИССЛЕДОВАНИЕ МЕТОДОВ ГОМОМОРФНОГО ШИФРОВАНИЯ ДЛЯ ЗАЩИТЫ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

STUDY OF HOMOMORPHIC ENCRYPTION METHODS FOR DATA PROTECTION IN CLOUD COMPUTING

R. Kamensky

Summary. The article deals with the issues related to the protection of information in cloud storage, which have found their widespread use in different industries and spheres of activity. The methods of homomorphic encryption are studied in detail in the process of research, the features and principles of its implementation are outlined. The distinctive features and specifics of application of partial, incomplete and full homomorphic encryption are described. Special emphasis is made on free-noise fully homomorphic encryption schemes, which are a new direction of development in data protection.

Keywords: encryption, cloud computing, data, defence, technology.

Каменский Руслан Сергеевич
БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова
zmo72106@voenmeh.ru

Аннотация. В статье рассматриваются вопросы, связанные с защитой информации в облачных хранилищах, которые нашли свое широкое распространение в разных отраслях и сферах деятельности. Детально в процессе исследования изучены методы гомоморфного шифрования, обозначены особенности и принципы его реализации. Описаны отличительные черты и специфика применения частичного, неполного и полного гомоморфного шифрования. Особый акцент сделан на свободно-шумных полностью гомоморфных схемах шифрования, которые являются новым направлением развития в защите данных.

Ключевые слова: шифрование, облачные вычисления, данные, защита, технология.

На фоне динамично расширяющихся требований к современным ИТ-инфраструктурам, в первую очередь с точки зрения вычислительной мощности и емкости хранения при обработке данных, использование облачных вычислений растет стремительными темпами. Концепция облачных вычислений предлагает масштабируемые ресурсы, которые предоставляются в виде услуги через Интернет. Ключевым драйвером развития данной технологии являются экономические выгоды, которые включают снижение эксплуатационных расходов и капитальных затрат [1]. Благодаря постоянной доступности данных, которая, не зависит от местоположения пользователя, время принятия решений уменьшается. Облачные вычисления предоставляют межсайтовый доступ к системам благодаря центральной синхронизации и анализу данных. Кроме того, резервное копирование данных в облаке позволяет защитить их в случае локальной аварийной ситуации. Эти преимущества приводят к прогнозируемому глобальному ежегодному росту облачных вычислений в производстве на 16,1 % с 2020 по 2030 год [2].

Очевидным является тот факт, что с широким распространением облачных вычислений все больше конфиденциальной информации и частных данных хранится пользователями в облаке. Обеспечение защиты облачных хранилищ — один из важных вопросов безопасности. Чтобы защитить конфиденциальность пользовательских данных в облаке они должны храниться в виде шифрованного текста.

В настоящее время на практике большинство конфиденциальных вычислений выполняется в доверенных средах исполнения (Trusted Execution Environments, TEE), в которых центральный процессор обеспечивает изоляцию области памяти для конфиденциальных вычислений. Только в этой области памяти данные расшифровываются для использования. В свою очередь гомоморфное шифрование (РН) представляет собой метод обеспечения конфиденциальных вычислений, выходящий за рамки TEE. Он дает возможность осуществлять вычисления над шифротекстом, при этом все данные остаются полностью зашифрованными. РН открывает ряд новых возможностей для конфиденциальных вычислений в облачных средах, поэтому его изучение представляет собой актуальную научно-практическую задачу, что и предопределило выбор темы данной статьи.

Оценка и анализ потенциала гомоморфного шифрования для его различных приложений в облачных вычислениях проводятся такими авторами как Частикова В.А., Жерлицын С.А., Пешков А.Н., Карапетян А.С., Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama.

Над вопросами устранения разрыва в производительности между работой с зашифрованными данными и работой с их открытой текстовой формой трудятся Быстревский С.А., Боршевников А.Е., Добржинский Ю.В., Юркевичюс С.П., Гриценко А.Е., Hong Zhong, Jie Cui, Runhua Shi.

Высоко оценивая накопленное научное наследие, следует отметить, что ряд вопросов в данной предметной плоскости требует уточнения и более детального анализа. Так, нерешенной остается проблема стандартизация гомоморфного шифрования. Кроме того, в дальнейшем развитии нуждаются алгоритмы гомоморфного шифрования с точки зрения их производительности.

Таким образом, цель статьи заключается в исследовании методов гомоморфного шифрования для защиты данных в облачных вычислениях.

РН — это достаточно широкий и объемный термин, который описывает различные криптографические достижения, позволяющие выполнять вычисления на зашифрованных данных. РН дает возможность проводить вычисления над зашифрованными данными при этом не расшифровывая их. Это достигается путем кодирования данных для выполнения вычислений на закодированных данных. Результаты анализа также кодируются, что позволяет данным оставаться зашифрованными на протяжении всего процесса. Затем закодированные данные можно расшифровать, чтобы узнать результаты вычислений [3].

Рисунок 1 описывает гомоморфизм шифрования в соответствии с квинтой криптосистем.

Аналогично математическому гомоморфизму, шифрование (уравнение (1)) и дешифрование (уравнение (2)) определяются следующим образом:

$$e_k(p \Diamond p') = e_k \circ e_k(p') = c \circ c' \quad (1)$$

$$d_k(c \Diamond c') = d_k(c) \Diamond d_k(c') = p \Diamond p' \quad (2)$$

где $\Diamond \in \{\oplus, \otimes\} \forall p, p' \in P, e_k$ — функция шифрования, d_k — функция дешифрования, p, p — открытый текст, c, c — зашифрованный текст, $\oplus$ обозначает сложение, а $\otimes$ — умножение.

Существует три основных метода РН:

1. Частично гомоморфное шифрование (PHE): позволяет выполнять отдельные математические функции над зашифрованными данными.
2. Неполное гомоморфное шифрование (SHE): дает возможность осуществлять ограниченное количество математических операций определенной сложности ограниченное количество раз.
3. Полностью гомоморфное шифрование (FHE): позволяет выполнять любые математические операции неограниченное число раз.

Рассмотрим более подробно эти методы.

Частично гомоморфное шифрование

Хотя схема PHE не поддерживает гомоморфизм над универсальным и логически полным набором операций, она по-прежнему очень полезна на практике. За последние три десятилетия было не только разработано множество зрелых схем PHE, но они также нашли свое применение в различных приложениях. Например, схема GM и схема Pai используются для агрегации зашифрованных данных, распределенного поиска данных с сохранением конфиденциальности и т.д. [4].

На протяжении нескольких последних лет криптографическое сообщество достигло заметных успехов в непрерывном совершенствовании вышеупомянутых схем PHE, особенно в плане компактности. Схема RSA представляет собой довольно простой дизайн в том смысле, что она 1-компактна. Однако компактность оригинальной GM-схемы столь же велика, как log*N*. На Eurocrypt T. Okamoto и S. Uchiyama, добились хорошего прогресса,

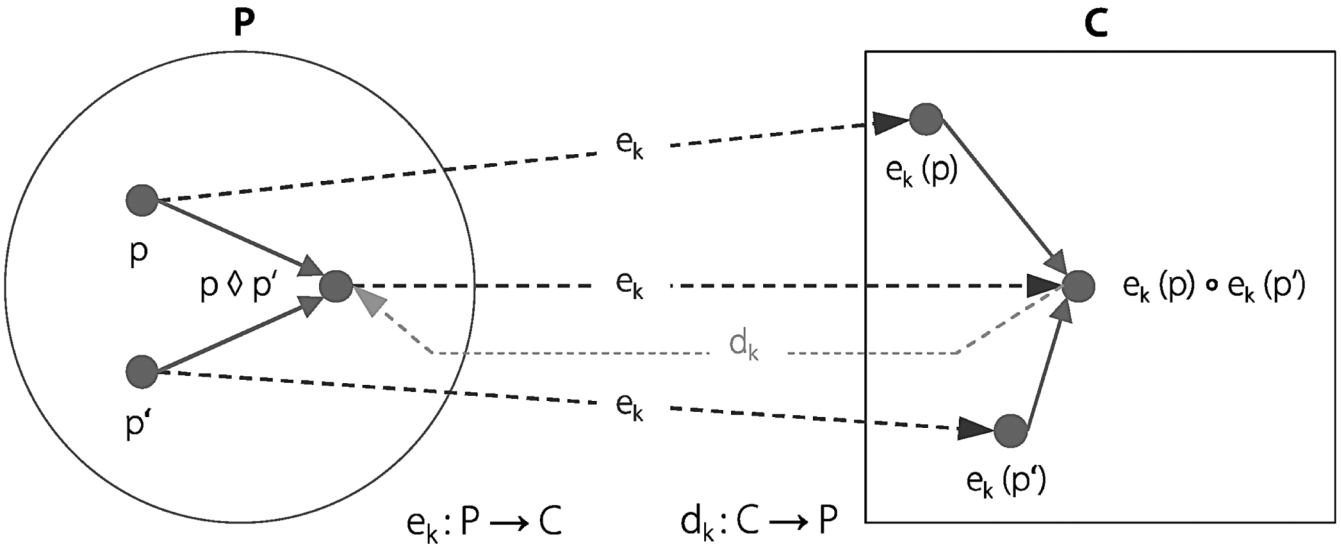

Рис. 1. Гомоморфизм функции шифрования

Таблица 1.

Частично гомоморфные схемы шифрования

Год	Авторы	Гомоморфные операции	ρ
1978	Rivest, Shamir and Adleman	$\langle\cdot\rangle_N$	1
1982	Goldwasser and Micali	$\langle+\rangle_2$	$O(\log N)$
1984	ElGamal	$\langle\cdot\rangle_p$	2
1985	Cohen and Fischer	$\langle+\rangle_p$ (для малых простых p)	$O\left(\frac{logN}{logp}\right)$
1994	Benaloh	$\langle+\rangle_p$ (для малых простых p)	$O\left(\frac{logN}{logp}\right)$
1998	Naccache and Stern	$\langle+\rangle_{\Pi pi}$ (для малых простых p_i)	$O\left(\frac{logN}{log\Pi pi}\right)$
1998	Okamoto and Uchiyama	$\langle+\rangle_p$	3
1999	Paillier	$\langle+\rangle_N$	2
2001	Damgård and Jurik	$\langle+\rangle_{N^{k-1}}$	$1+\frac{k-1}{k}$
2005	D. Boneh, E. Goh, and K. Nissim	$\langle+\rangle_p$	$O\left(\frac{logn}{logT}\right)$
		$\langle+\rangle_p$ (только один раз)	$(T<\sqrt{n})$
2013	Joye and Libert	$\langle+\rangle_{2^\alpha}$	≈ 4

получив 3-компактную аддитивную PHE-схему. На PKC I. Damgård и M. Jurik предложили аддитивную схему PHE, которая является почти 1-компактной за счет увеличения пространства шифротекстов с N до N^k для достаточно больших k. Совсем недавно M. Joye и B. Libert, улучшили криптосистему NaccacheStern, задав $k = 2^\alpha$, что привело к аддитивной схеме PHE с компактностью около 4.

В обобщенном виде основные схемы PHE, а также их особенности представлены в таблице 1.

Неполное гомоморфное шифрование

Первое формальное появление концепции SHE было фактически выдвинуто C. Джентри в 2009 году. Схема SHE C. Джентри способна гомоморфно оценивать полиномы «низких степеней». Точнее, она поддерживает сложение произвольных слоев по модулю 2 и умножение ограниченных слоев по модулю 2 над зашифрованными битами. Как и все известные криптосистемы на основе решеток, схема SHE C. Джентри, основанная на идеальной решетке, также вводит шум в качестве основы безопасности. Однако величина шума мгновенно возрастает по мере выполнения гомоморфных операций. Результирующий шум линейно увеличивается с числом слоев гомоморфных сложений, в то время как с числом слоев гомоморфных умножений он растет экспоненциально. Когда величина шума в шифротексте превышает определенный порог, шифротекст не может быть правильно расшифрован. Поэтому схема SHE C. Джентри может поддерживать только гомоморфные умножения логарифмической глубины. Чтобы преобразовать схему SHE в схему FHE, Джентри изобрел так называемую технику «бутстрэппинга», которая в настоящее время является основным образцом для проектирования FHE.

Полностью гомоморфное шифрование

Схемы FHE (рис. 2) рассматриваются учеными в качестве алгоритмов следующего поколения в криптографии. По сути, FHE представляет собой криптосистему интеллектуального шифрования, которая позволяет проводить произвольные вычисления над шифротекстами при этом, не расшифровывая и не раскрывая их [5]. Для облачных вычислений это очень ценная характеристика.

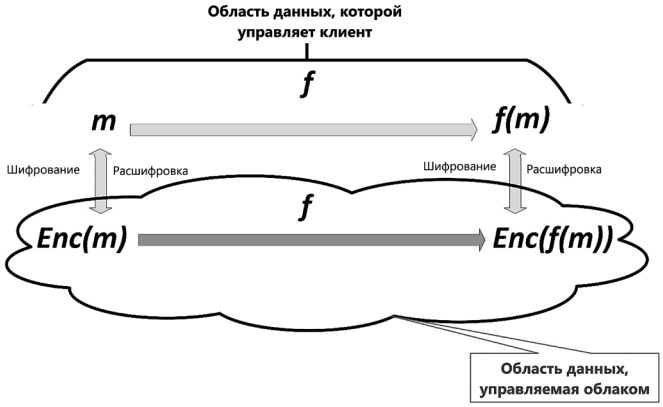

Рис. 2. Схема FHE в облачных вычислениях

Традиционно FHE применяется для аутсорсинга сложных вычислений, которые проводятся над конфиденциальными данными, хранящимися в облаке. Данный метод шифрования используется в таких приложениях для больших данных, как поиск частной информации, безопасный поиск в зашифрованных больших данных.

Также в литературе можно найти новую категорию РН, называемую свободно-шумными полностью гомоморфными схемами шифрования, которым не требуется техника управления шумом для обновления шифротекстов. Это перспективная технология, которая в настоящее время активно разрабатывается. В схеме свободно-шумного полностью гомоморфного шифрования можно выполнять бесконечное число операций над одним и тем же шифротекстом без роста шума. Этот класс схем шифрования известен тем, что он быстрее предыдущего, включает простые операции по оценке схем над шифротекстами и не требует техники управления шумом. Однако в этой схеме присутствуют проблемы с безопасностью, так как большинство разработанных схем сегодня криптоанализируются.

Таким образом, подводя итоги, отметим, что с развитием таких технологий, как облачные вычисления и машинное обучение, РН стало популярным методом зашиты данных. Преимуществом РН для облачных вычислений является то, что оно позволяет зашифровать каждый блок данных перед его загрузкой в облачное хранилище. Это дает возможность сохранить ключ шифрования и контролировать, какие стороны могут получить доступ к информации и расшифровать ее. В статье рассмотрены используемые на сегодняшний день методы РН.

ЛИТЕРАТУРА

1. Соболев С.Г. За пределами конфиденциальности: использование Zk-Snark и гомоморфного шифрования для разработки прозрачных и приватных проектов // Методы и технические средства обеспечения безопасности информации. 2024. № 33. С. 187–189.
2. Хаустова И.В. Использование полностью гомоморфного шифрования для защиты данных в машинном обучении в облаке // Вестник науки. 2024. Т. 3. № 4 (73). С. 482–491.
3. Boomija M.D. Threshold multiparty multi-randomness secure partially homomorphic encryption for data security in cloud // Expert Systems. 2022. Volume 40, Issue 6. P. 78–82.
4. Mohamed Sirajudeen Yoosuf FogDedupe: A Fog-Centric Deduplication Approach Using Multi-Key Homomorphic Encryption Technique // Journal of Sensors. 2022. Volume 20, Issue 1. P. 109–113.
5. Бабенко Л.К. Гибридное шифрование на основе использования симметричных и гомоморфных шифров // Известия ЮФУ. 2021. № 2. С. 6–18.

Журнал «Современная наука: актуальные проблемы теории и практики»