Направления развития гомоморфного шифрования

Дупленко Александр Геннадьевич
студент
Балтийский федеральный университет имени И. Канта (г. Калининград)

***Аннотация**: В статье представлены результаты исследования направлений развития гомоморфного шифрования. Выявлены четыре актуальных направления: разработка симметричного полностью гомоморфного шифрования, где за основу взяты неприводимые матричные полиномы; разработка симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел; разработка пороговых систем гомоморфного шифрования и защита информации в облачных вычислениях, а также исследование методов обеспечения конфиденциальности вычислений в облачной среде на основе китайской теоремы об остатках.*

***Ключевые слова**: гомоморфное шифрование, полностью гомоморфная криптосистема; пороговая система гомоморфного шифрования.*

Цель проведенного исследования состояла в выявлении актуальных направлений развития гомоморфного шифрования российскими учеными.

Под гомоморфным шифрованием понимается криптографический примитив, который представляет собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо алгебраических операций над открытыми текстами [1, с. 27].

В основе понятия «гомоморфное шифрование» находится понятие «privacy homomorphism», введенное Ривестом (Rivest) в статье «On data banks and privacy homomorphism» [2].

Математически «privacy homomorphism» можно описать следующим образом:

Пусть даны две алгебраические системы:

$$U = \langle S; f_1, \dots, f_k; p_1, \dots, p_l; s_1, \dots, s_m \rangle$$

$$C = \langle S; f'_1, \dots, f'_k; p'_1, \dots, p'_l; s'_1, \dots, s'_m \rangle$$

где S и S' – множества; $f_1, \dots, f_k$, $f'_1, \dots, f'_k$ - функции; $p_1, \dots, p_l$, $p'_1, \dots, p'_l$ - предикаты, определённые на множествах S и S' соответственно, а $\{s_1, \dots, s_m\} \subset S$, $\{s'_1, \dots, s'_m\}$ - известные константы.

Пусть существует обратимая функция φ: $S \rightarrow S'$. Тогда φ называется privacy homomorphism, если выполняются следующие условия:

$$\forall i \in \{1, \dots, k\} : f_i(a_1, \dots, a_n) = \varphi^{-1}\left(f'_i(\varphi(a_1), \dots, \varphi(a_n))\right)$$

$$\forall i \in \{1, \dots, l\} : p_i(a_1, \dots, a_n) = p'_i(\varphi(a_1), \dots, \varphi(a_n))$$

$$\forall i \in \{1, \dots, m\} : \varphi(s_i) = s'_i$$

а также:

a) функции φ и φ' легко вычислимы;

b) операции f'_i и предикаты p'_i так же эффективно вычислимы;

c) представление «зашифрованного» значения $\varphi(d_i)$, где $d_i \in S$, занимает не слишком много места по сравнению с d_i ;

d) знания $\varphi(d_i)$ для большого количества d_i недостаточно для восстановления φ (атака с известным шифротекстом)

e) знание некоторых пар $(d_i, \varphi(d_i))$ недостаточно для восстановления φ (атака с подобранным открытым текстом)

f) знания алгоритмов вычисления операций f'_i и предикатов p'_i недостаточно для построения алгоритма вычисления φ.

Создание наиболее эффективной и полностью гомоморфной криптографической системы смогло бы обеспечить практическую реализацию в аутсорсинге закрытых вычислений, примером могут быть облачные вычисления. Использование гомоморфного шифрования смогло бы объединить вместе различные услуги, при этом не предоставляя данные для каждой конкретной услуге. Например, объединение услуг каких-либо различных компаний позволило бы последовательно рассчитать налог,

учитывая последние изменения, применить к нему обменный курс и отправить необходимые документы для совершения сделки, при этом имея возможность не предоставлять фактические данные для каждой из задействованных услуг.

Гомоморфное свойство, используемое в различных криптографических системах, может быть применимо для создания наиболее безопасных систем голосования, всевозможных хеш-функций, которые будут стойки к коллизиям, закрытой информации поисковых систем, и сможет обеспечить гарантированную конфиденциальность обработанных данных в широком использовании публичных облачных вычислений.

В то же время гомоморфное шифрование обладает и рядом недостатков.

Во-первых, для модификации утерянных или удаленных данных необходимо будет передать секретный ключ по сети, иначе говоря, потребуется его раскрытие, что, конечно же, подставит под угрозу безопасность. Во-вторых, коренной недостаток, присущий гомоморфным криптосистемам, состоит в том, что в атаках на них может использоваться их дополнительная структура. К примеру, при использовании исходного варианта RSA для цифровой подписи произведение двух подписей будет давать корректную подпись для произведения двух соответствующих сообщений. Хотя есть много способов избежать такой атаки, к примеру, применяя хэш-функции, или используя избыточность вероятностных криптосистем, есть также более сложные атаки, где показывается нестойкость криптосхем. Для криптосхем с открытым ключом желание повысить криптостойкость приводит к снижению эффективности. Данный недостаток можно преодолеть снижением требований к криптосхеме, а именно позволив ей быть симметричной, но компактной и криптостойкой к атаке на основе известных открытых текстов.

В-третьих, одной из существенных проблем известных полностью гомоморфных криптосистем является их крайне низкая производительность. В настоящее время существует два основных пути её повышения: использование «ограниченного гомоморфизма» (и так называемый «метод

упаковки шифротекстов». Первый подразумевает криптосистему, которая может выполнять операции двух видов (сложения и умножение), но в ограниченном количестве. Суть второго в том, что в один шифротекст записывается сразу несколько открытых текстов, и при этом в процессе одиночной операции такого пакетного шифротекста происходит одновременная обработка всех входящих в него шифротекстов.

В-четвертых, если рассматривать свойство гомоморфности функции шифрования с точки зрения криптографических приложений, то оно уже не всегда может расцениваться как достоинство криптосистемы. Существуют примеры, когда данное свойство уже относится к слабостям. Например, преобразование, обратное функции шифрования криптосистемы RSA, задействовано в схеме электронной подписи RSA для генерации подписей. Пусть дано сообщение m, тогда подпись будет вычисляться по формуле s=m*d mod N, где d - секретная экспонента. Легко понять, что и это обратное преобразование будет гомоморфно относительно операции произведения сообщений. В конечном итоге, будет иметься следующий способ фальсификации подписей [1. С. 30].

В настоящее время ведутся активные исследования в области гомоморфного шифрования. В качестве основных направлений его развития можно назвать следующие.

Во-первых, разработка симметричного полностью гомоморфного шифрования с использованием неприводимых матричных полиномов. В Российской Федерации в данной области работает Ф.Б. Буртыка, который предложил проводить шифрование в два раунда: в начале берутся открытые тексты, которые являются элементами кольца вычетов, после чего кодируются в матрицы с использованием секретного вектора, а затем эти матрицы отображаются в матричные полиномы с использованием секретного неприводимого матричного полинома. Дешифрование также происходит в два раунда [3; 4].

Во-вторых, разработка симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел. В числе российских ученых, работающих в данном направлении, можно назвать А.В. Трепачеву [5], П.К. Бабенко [6]. Криптостойкость данных систем обосновывается использованием сложности решения задачи факторизации больших чисел.

В-третьих, разработка пороговых систем гомоморфного шифрования и защита информации в облачных вычислениях. Исследования в данном направлении ведут Варновский Н.П., Мартишин С.А., Храпченко М.В., Шокуров А.В. Ими предложен протокол облачных вычислений над конфиденциальными данными в модели с вспомогательными криптосерверами. В результате получена система, не требующая дополнительного открытого ключа и заменяющая наиболее неэффективную и проблемную процедуру перешифрования (bootstrapping) более эффективным протоколом перешифрования, выполняемым криптосерверами [7].

Четвертое направление развития гомоморфного шифрования в Российской Федерации – исследование методов обеспечения конфиденциальности вычислений в облачной среде на основе китайской теоремы об остатках. В данном направлении работают Червяков Н.И., Кучеров Н.Н., которые исследуют применимость пороговых схем разделения секрета для обеспечения безопасности облачных вычислений, а также неприменимость схемы разделения секрета Шамира. В сфере их научных интересов находятся также пороговые схемы разделения секрета Миньотта, Асмута-Блума и схемы HORNS и их модификаций, которые базируются на китайской теореме об остатках.

Таким образом, можно выделить следующие четыре направления развития гомоморфного шифрования в настоящее время в России: разработка симметричного полностью гомоморфного шифрования с использованием неприводимых матричных полиномов; разработка симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел;

разработка пороговых систем гомоморфного шифрования и защита информации в облачных вычислениях, а также исследование методов обеспечения конфиденциальности вычислений в облачной среде на основе китайской теоремы об остатках.

Список литературы

1. Варновский Н.П., Шокуров А.В. Гомоморфное шифрование // Труды Института системного программирования РАН. 2007. № 12. С. 27-36.
2. Rivest, R.L. On data banks and privacy homomorphism / R.L. Rivest, L. Adleman, M.L. Dertouzos // Foundations of secure computation. -1978. –Vol. 32, no. 4. –Pp. 169-178.
3. Буртыка Ф.Б. Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов // Известия ЮФУ. Технические науки. 2014. № 8. С. 107-122.
4. Буртыка Ф.Б. Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов // Труды Института системного программирования РАН. 2014. Т. 26. № -5. С. 99-116.
5. Трепачева А.В. Криптоанализ симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел // Известия ЮФУ. Технические науки. 2015. № 5 (166). С. 89-102.
6. Трепачева А.В., Бабенко Л.К. Формальный криптоанализ полностью гомоморфных систем, использующих задачу факторизации чисел // Информационное противодействие угрозам терроризма. 2015. № 24. С. 283-286.
7. Варновский Н.П., Мартишин С.А., Храпченко М.В., Шокуров А.В. Пороговые системы гомоморфного шифрования и защита информации в облачных вычислениях // Программирование. 2015. № 4. С. 47-51.
8. Червяков Н.И., Кучеров Н.Н. Исследование методов обеспечения конфиденциальности вычислений в облачной среде на основе китайской

теоремы об остатках // Сборник научных трудов ВНИИ ОиК. 2015. Т. 1. № 8. С. 633-635.