КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ.

Курушин А.А.
Оренбургский государственный университет, г. Оренбург

В работе показана роль, которую занимает гомоморфное шифрование в облачных вычислениях, а также плюсы и минусы применения данного способа шифрования. В рамках практической части была реализована криптосистема Пэйе и RSA и сравнены скорости шифрования данных и скорости операций гомоморфных свойств.

Использование облачных вычислений дает много преимуществ, но для обработки данных в публичных «облаках» в общем случае необходимо работать с открытыми данными. Но для работы с конфиденциальными данными необходима аппаратура или хотя бы организационные меры по хранению ключей. К провайдерам облачных вычислений такие требования представить не представляется возможным. Это по определению несет в себе риски, так как мы не можем повлиять никоим образом на то, как это происходит на третьей стороне. Было бы гораздо безопаснее передавать данные в зашифрованном виде с тем, чтобы операции, которые производятся над этими данными, никоим образом не распространяло информацию об этих данных.

В 1978 году авторами известного алгоритма с открытым ключем RSA Майклом Дертузосом, Рональдом Риверстом и Леонардом Адлеманом было сформировано понятие гомоморфного шифрования. В их работе они описали концепцию гомоморфного шифрования, а также задались вопросами возможно ли такое шифрование в принципе и для каких алгебраических систем такой гомоморфизм существует. Их попытки потерпели неудачу, и было решено, что эта идея не является реализуемой. Под формальным определением гомоморфного шифрования понимается криптографический примитив, представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо алгебраических операций над открытым текстом.

Гомоморфное шифрование как криптографический примитив представляет интерес как с прикладной, так и с чисто математической точек зрения. Несмотря на многолетние исследования в этой области, основные проблемы остаются нерешенными.

В литературе по теоретической криптографии под гомоморфным шифрованием понимается криптографический примитив, представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо алгебраических операций над открытыми текстами.

Пусть E(k,m) — функция шифрования, где m — открытый текст, k — ключ шифрования. Заметим, что для данных фиксированных k и m криптограмма E(k,m) может быть, вообще говоря, случайной величиной. В

таких случаях говорят о вероятностном шифровании. Функция E гомоморфна относительно операции op над открытыми текстами, если существует эффективный алгоритм M, который получив на вход любую пару криптограмм вида E(k,m1), E(k,m2), выдает криптограмму с такую, что при дешифровании с будет получен открытый текст m1opm2.

Гомоморфное шифрование как криптографический примитив может найти широкое применение в криптографии и, в более широком смысле, в разработке математических методов защиты информации. Здесь прежде всего следует выделить такую, интересную с прикладной точки зрения, задачу как вычисления над зашифрованными данными. Конфиденциальные данные хранятся в за- шифрованном виде. Для выполнения вычислений над ними данные можно рас- шифровать, произвести необходимые операции, и затем результаты вновь за- шифровать. Но для этого требуются защищенная аппаратура и, уж по крайней мере, организационные меры по хранению секретных ключей. Вычисления над зашифрованными данными, если они возможны, помогают избежать всех этих проблем.

Гомоморфные системы шифрования.

1. **Система** RSA.

Криптосистема RSA является одной из самых известных и популярных криптосистем. Она является гомоморфной относительно операции умножения открытых текстов.

Пусть

N – составной модуль,

e – открытая экспонента

$E\big((N,e),m\big) = m^e mod\ N$ – функция шифрования

Для любых двух m_1 и m_2

$$E(k,m_1) \times E(k,m_2 = m_1^e m_2^e mod\ N = E(k,m_1 \times m_2)$$

2. Криптосистема Эль Гамаля.

В криптосистеме Эль Гамаля в циклической группе G, если открытый ключ является (G,q,g,h), где $h = g^x$ и x закрытый ключ функция шифрования выглядит следующим образом для сообщения m

$$E(m) = (g^r, m \times h^r)$$

Где $r\epsilon\{0,\dots,q-1\}$

Свойство гомоморфности выглядит следующим образом:

$$E(m_1) \cdot E(m_2) = (g^{r_1}, m_1 \cdot h^{r_2})(g^{r_2}, m_2 \cdot h^{r_1}) = (g^{r_1+r_2}, (m_1 \cdot m_2)h^{r_1+r_2}) = E(m_1, m_2)$$

Таким образом, криптосистема Эль Гамаля является гомоморфной относительно операции умножения.

3. Криптосистема Пэйе.

Пусть p и q – два простых числа

$$n = pq$$

$\lambda = \text{НОК}(p-1, q-1)$. Выберем случайное число g из $Z_{n^2}^*$ и вычислим

$$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n, \text{где } L(u) = (u-1)/u$$

Открытым ключем служит пара $k = (n, g)$, а закрытым ключем – пара (λ, μ)

4. Модель Бракерски-Гентри-Вайкунтанатан.

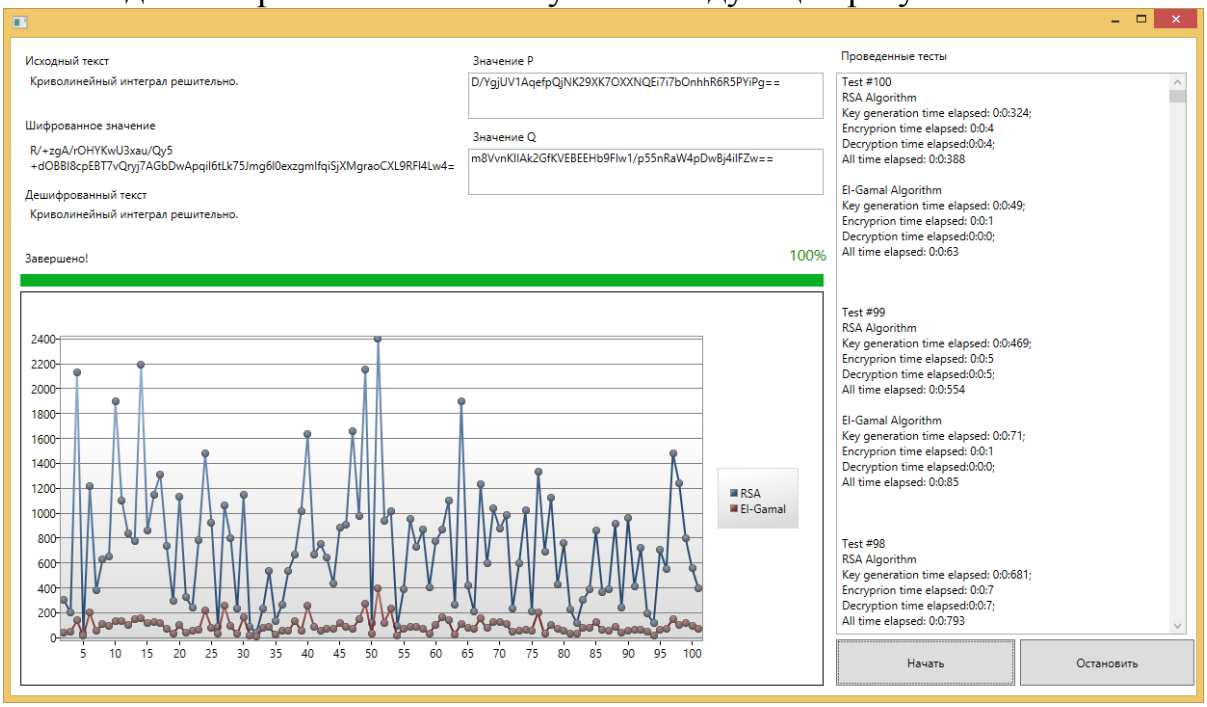
25 июня 2009 года аспирант Стэндфордского университета и стажер IBM Крейг Гентри предложил модель полностью гомоморфного шифрования, которая позволяла проводить глубокую обработку данных без их расшифровки. В алгоритме Гентри выполняются свойства гомоморфности относительно как умножения, так и сложения. Тем самым данную модель можно использовать в облачных вычислениях без ограничений. Передавая данные в облака, то есть в недоверенную зону, можно не задумываться об их конфиденциальности. Однако модель Гентри оказалась слишком непрактичной. С увеличением количества операций производимых над зашифрованным текстом сложность и размер шифр текста увеличивается с невероятной скоростью. И не смотря на то, что за последние несколько лет были произведены множество улучшений данной модели, она все еще остается скорее теоретической моделью, которая не применима на практике.

Описание практической части.

В рамках данной работы были протестированы криптосистема Пэйе и RSA и сравнены скорости шифрования данных и скорости операций гомоморфных свойств. Реализации были написаны на языке C#. Для каждой криптосистемы были реализованы выделены отдельные классы, которые содержали следующие функции:

1. Генерация ключей (KeyGeneration)
2. Шифрование (Encrypt)
3. Дешифрование (Decrypt)

В ходе эксперимента были получены следующие результаты:



Криптосистема	Генерация ключа	Шифрование	Расшифрование
RSA	0:0:212 мс	0:0:5 мс	0:0:4 мс
Эль Гамаля	0:0:143 мс	0:0:2 мс	0:0:1 мс

Характеристики компьютера, на котором проводились замеры:

- Процессор: Intel Core i5 2.6Ghz
- ОЗУ: 4Гб
- Жесткий диск: WDC - WD3200LPVT
- ОС: Windows 8.1 x64

Заключение.

В ходе работы рассмотрено гомоморфное шифрование, как наиболее перспективное направление в области защиты информации при использовании облачных вычислений. Проведены эксперименты производительности криптосистем RSA и Пэйе обладающих одним гомоморфным свойством. В ходе экспериментов выяснилось, что на данный момент криптосистема Гентри на практике не применима. В то же время, криптосистемы RSA и Пэйе могут использоваться в очень узконаправленных приложениях.

Список литературы

1. NIST Определение облачных вычислений

2. Ronald L. Rivest, Len Adleman, Michael L. Dertouzos On data banks and privacy homomorphisms (1978)

3. Ronald L. Rivest Voting, Homomorphic Encryption

4. Craig Gentry; Shai Halevi. "A Working Implementation of Fully Homomorphic Encryption" pdf

5. SattvaQ Homomorphic encryption

6. B. Barak Fully Homomorphic Encryption

7. Вик Уинклер Облачные вычисления: Вопросы безопасности в виртуальных облаках.

8. Cisco Безопасная сегментация в унифицированной архитектуре центров обработки данных Cisco 9. Ronald L. Krutz, Russel Dean Vines, Cloud Security: Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, 2011 27

10. Н.П. Варновский, А.В. Шокуров Гомоморфное шифрование

11.K. Lauter, M.Naehrig, V.Vaikuntanathan