Шифр Вернама и протокол Диффи-Хеллмана-Меркла как квантово-устойчивая система шифрования.

Чайко Владимир Иванович, студент
Сибирский государственный индустриальный университет
(г. Новокузнецк).

В статье автор предлагает систему шифрования, основанную на шифре Вернама и протоколе Диффи-Хеллмана-Меркла, как квантово-устойчивою систему шифрования. Так же автор приводит реальный пример использования данной системы на практике и практическую попытку взлома данной системы.

Ключевые слова: *Шифр Вернама, протокол Диффи-Хеллмана-Меркла, шифрование, квантово-стойкий, RSA.*

23 декабря 2022 года была опубликована статья «Факторинг целых чисел с сублинейными ресурсами на сверхпроводящем квантовом процессоре». [1] Согласно данной статье взлом шифра RSA с длинной ключа 2048 бит возможен уже сегодня. Такое положение дел фактически подрывает информационную безопасность во всем мире. Однако стоит отметить, что взлом шифра RSA, с длинной ключа 2048 бит, на практике, они так и не осуществили, поэтому данная статья – только теоретическая. [2] [3]

Тем не менее, эра квантовых суперкомпьютеров все ближе, что делает проблему информационной безопасности актуальнее с каждым годом. Квантовые суперкомпьютеры работают на совершенно иных принципах, нежели наши привычные офисные и домашние ПК. Именно благодаря этому они способны взламывать современные шифры, в том числе AES, Twolfish и Serpent, что несет огромную угрозу информационной безопасности, в том числе в телекоммуникационном, банковском и военном секторах. [4]

Ученые со всего мира уже давно ведут исследования и разработки в области криптографии, пытаясь разработать такую систему шифрования,

которая могла быть использована простым компьютером и не поддавалась взлому при помощи квантового суперкомпьютера. Стоит отметить, что уже сегодня существует большое количество наработок в этой области, однако они, в большинстве своем, только теоретические. Эффективность этих шифров против взлома квантовым суперкомпьютером не была доказана на практике. [5] Именно поэтому сегодня существует потребность в создании квантово-устойчивого шифра на практике.

В качестве такого шифра я предлагаю систему шифрования, основанную на шифре Вернама [6] и протоколе Диффи-Хеллмана-Меркла [7].

Гилберт Вернам, в 1917 году, изобрел шифр, который стал называться его именем – «шифром Вернама». Позже, в 1930-х годах, невзламываемость данного шифра была доказана математиком Клодом Шенноном. Данный шифр реализуется при помощи побитного сложения по модулю 2 (побитного «XOR») текста сообщения и его ключа. Получающаяся в результате шифрования последовательность битов не поддается какому-либо анализу и взлому. [8] Такое положение дел сохраняется и сегодня – данный шифр невозможно взломать на компьютере любой мощности, в том числе и квантовом суперкомпьютере. [9]

Несмотря на надежность, от использования данного шифра отказались по целому ряду причин. Наиболее важные из них – это величина ключа, уровень его (ключа) случайности, и необходимость его передачи собеседнику по защищенному каналу («проблема распределения ключей»). Эти три требования сделали его, в начале, неудобным, а впоследствии, и непригодным к применению в современное время. Взамен этого шифра было решено использовать симметричные шифры и шифр RSA (в сетях передачи данных). [6]

Сегодня шифр Вернама – единственный тип шифра, который может противостоять квантовому суперкомпьютеру на практике, и возможен для

реализации на обычных компьютерах. Именно поэтому в основу предлагаемой мной системы лег именно этот шифр.

В 1976 году два математика Диффи и Хеллман опубликовали метод безопасного создания общего ключа шифрования при помощи обмена открытыми числами. [7] Этот метод стал называться протоколом Диффи-Хеллмана, но позже, в 2002 году, по просьбе Хеллмана, данный протокол стали называть Диффи-Хеллмана-Меркла. Используя данный протокол модифицированной версии, предлагаемая система шифрования лишена «проблемы распределения ключей».

Чтобы понять суть модификации, необходимо разобрать сам процесс взлома протокола Диффи-Хеллмана-Меркла:

Алиса и Боб договариваются о двух простых числах p=23, g=5. Алиса выбирает в качестве секретного числа a=6, а Боб b=15. Алиса вычисляет число A по формуле $A = g^a \ mod \ p = \ 5^6 \ mod \ 23 = 8$, и передает его Бобу. Боб вычисляет число B по формуле $B = g^b \ mod \ p = \ 5^{15} \ mod \ 23 = 19$ и передает Алисе. Алиса вычисляет ключ k по формуле $k = B^a \ mod \ p = \ 19^6 \ mod \ 23 = 2.$ Боб вычисляет ключ k по формуле $k = A^b \ mod \ p = \ 8^{15} \ mod \ 23 = 2.$ У Алисы и Боба есть общий ключ k=2, которым они могут шифровать свои сообщения. Ева, которая хочет узнать общий ключ k, знает только числа p=23, g=5, A=8, B=19. Чтобы найти ключ k она должна решить уравнение $A^x \ mod \ p = B^y \ mod \ p \ \rightarrow 8^x \ mod \ 23 = 19^y \ mod \ 23$, подбирая значения x и y методом перебора. После того, как такое совпадение будет найдено, Ева вычисляет значение любой из частей уравнения и получает ответ. Далее она пробует расшифровать передаваемое сообщение, используя ответ в качестве ключа, до тех пор, пока он не подойдет. Учитывая, что шифрование осуществляется современным блочным шифром, рано или поздно сообщение будет расшифровано единственно верным способом. Наглядно перебор Евы возможных значений, для данного примера, представлен в таблице 1.

Таблица 1. Перебор Евы

№ попытки	x	y	k	Результат
1	2	5	16	Не подходит
2	4	10	3	Не подходит
3	6	4	2	Подходит

Модификация протокола Диффи-Хеллмана-Меркла заключается в том, что в предлагаемой системе шифрования итоговый ключ создается из нескольких ключей шифрования («полуключей»), полученных при помощи данного протокола. «Полуключи» создаются и подставляются друг к другу до тех пор, пока получающейся итоговый ключ будет больше или равен длине передаваемого сообщения, поэтому количество таких ключей за ранее неизвестно, но обязательно должно быть больше 1.

Общий алгоритм предлагаемой системы шифрования таков:

1. Сгенерировать несколько ключей (>2) при помощи протокола Диффи-Хеллмана-Меркла. Количество ключей должно быть таким, чтобы количество их бит было больше или равно шифруемому сообщению.
2. Совместить все сгенерированные ключи в один путем подстановки.
3. Если ключ больше передаваемого сообщения, то убрать лишние биты.
4. Зашифровать передаваемое сообщение шифром Вернама, используя полученный ключ.
5. Передать зашифрованное сообщение собеседнику.

Для понимания данного механизма стоит привести пример:

Алиса хочет передать Бобу сообщение «856». В бинарном виде это «1101011000» (10 бит).

Алиса и Боб, при помощи протокола Диффи-Хеллмана-Меркла создают ключ «2». В бинарном виде это «10» (2 бита). Это меньше, чем длина сообщения (10 бит), поэтому они создают второй ключ «1». В бинарном виде это «1» (1 бит). Совмещаем ключи «10» и «1» и получаем «101» (3 бита). Это меньше

чем сообщение, поэтому Алиса и Боб генерируют третий ключ «9». В бинарном виде это «1001» (4 бита). Совмещаем ключи и получаем «1011001» (7 бит). Этого мало, поэтому Алиса и Боб генерируют четвертый «48». В бинарном виде это «110000» (6 бит). Совмещаем ключи и получаем «1011001110000». Это 13 бит, больше чем сообщение (10 бит) поэтому Алиса отбрасывает последние 3 бита и получает ключ «1011001110». Далее, она шифрует сообщение шифром Вернама, получая шифр «0110010110» и передает Бобу.

Боб, получив сообщение «0110010110» видит, что размер сообщения 10 бит, поэтому он понимает, что с конца ключа нужно отбросить 3 бита и тоже получает ключ «1011001110». Далее он расшифровывает сообщение шифром Вернама и получает первоначальное сообщение «1101011000», что в десятичной системе счисления значит «856».

Ева, перехватывающая все сообщения между Алисой и Бобом, для взлома шифра, должна решить следующую систему уравнений:

$$\begin{cases} k_1 = {A_1}^{x_1} \; mod \; p_1 = {B_1}^{y_1} \; mod \; p_1 \\ k_2 = {A_2}^{x_2} \; mod \; p_2 = {B_2}^{y_2} \; mod \; p_2 \\ k_3 = {A_3}^{x_3} \; mod \; p_3 = {B_3}^{y_3} \; mod \; p_3 \\ k_4 = {A_4}^{x_4} \; mod \; p_4 = {B_4}^{y_4} \; mod \; p_4 \end{cases}$$

Учитывая, что каждое k может принимать несколько разных значений, то итоговый ключ $k_1 \, k_2 \, k_3 \, k_4$ может быть большим количеством равновероятных значений, поэтому Ева не может точно определить, какой ключ используют Алиса и Боб. Это приводит к тому, что Еве придется взламывать зашифрованное сообщение путем перебора. Однако, учитывая, что сообщение зашифровано шифром Вернама, не поддающемуся взлому методом перебора, данная система, с точки зрения криптографии, не может быть взломана, в том числе и квантовым суперкомпьютером.

Литература:

1. Factoring integers with sublinear resources on a superconducting quantum processor. — Текст : электронный // Arxiv. Cornell University. : [сайт]. — URL: https://arxiv.org/abs/2212.12372 (дата обращения: 11.01.2023).
2. Schneier, B. Breaking RSA with a Quantum Computer. / B. Schneier. — Текст : электронный // Schneier on Security. : [сайт]. — URL: https://schneier.com/blog/archives/2023/01/breaking-rsa-with-a-quantum-computer.html (дата обращения: 11.01.2023).
3. Stan Kaminsky. Взломают ли шифрование RSA на квантовом компьютере в 2023 году? / Kaminsky Stan. — Текст : электронный // kaspersky daily : [сайт]. — URL: https://www.kaspersky.ru/blog/quantum-computers-and-rsa-2023/34503/ (дата обращения: 11.01.2023).
4. Serge, Malenkovich Квантовые компьютеры и конец безопасности. / Malenkovich Serge. — Текст : электронный // kaspersky daily : [сайт]. — URL: https://www.kaspersky.ru/blog/kvantovye-kompyutery-i-konec-bezopasnosti/1989/ (дата обращения: 11.01.2023).
5. Open Quantum Safe. Software for prototyping quantum-resistant cryptography. — Текст : электронный // Open Quantum Safe. : [сайт]. — URL: https://openquantumsafe.org/ (дата обращения: 11.01.2023).
6. Vernam, G. S. Sicret signaling system. / G. S. Vernam. — Текст : электронный // Google Patents. : [сайт]. — URL: https://patents.google.com/patent/US1310719 (дата обращения: 11.01.2023).
7. Diffie W., Hellman M. E. New Directions in Cryptography / W. Diffie, M. E. Hellman. — Текст : непосредственный // IEEE Transactions on Information Theory. — 1976. — № 6. — С. 644 - 654.
8. Shannon, C. E. Communication Theory of Secrecy Systems / C. E. Shannon. — Текст: непосредственный // Bell System Technical Journal. — 1949. — № 28. — С. 656–715.

9. Шнайер, Б. Прикладная криптография: протоколы, алгоритмы и исходный код на С. / Б. Шнайер. — 2. — М. : Вильямс, 2016. — 1040 с. — Текст : непосредственный.