УДК 004.056.55 + 003.26 Вестник УрФО № 4(34) / 2019, с. 30–34

Крохалева Я. Н., Кротова Е. Л.

DOI: 10.14529/secur190404

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУЩЕСТВУЮЩИХ ПРОТОКОЛОВ ОБМЕНА КЛЮЧАМИ ДЛЯ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ

Данная статья посвящена актуальной в настоящий момент проблеме – распределению ключей в криптографических системах. В работе подробно рассмотрено и проведено сравнение двух базовых методов распределения ключей, которые в настоящее время используются при проектировании криптографических систем. Алгоритм Диффи-Хеллмана является основным методом распределения ключей в существующих протоколах для автоматизированных распределенных систем. Технологии квантовой криптографии получают все большее развитие и требуют анализа и сравнения с другими методами классической криптографии на предмет конкурентоспособности.

Ключевые слова: *криптография, квантовая криптография, распределение ключей, протокол, Диффи-Хеллман, BB84.*

Krokhaleva Y. N., Krotova E. L.

COMPARATIVE ANALYSIS OF EXISTING KEY EXCHANGE PROTOCOLS FOR SYMMETRIC CRYPTOSYSTEMS

This article is devoted to the current problem - the distribution of keys in cryptographic systems. In the work, two basic methods of key distribution, which are currently used in the design of cryptographic systems, are examined and compared in detail. The Diffie-Hellman algorithm is the primary key distribution method in existing protocols for automated distributed systems. The technologies of quantum cryptography are getting more and more development and require analysis and comparison with other methods of classical cryptography regarding competitiveness.

Keywords: *cryptography, quantum cryptography, key distribution, protocol, Diffie-Hellman, BB84.*

Сложность и надежность любой криптосистемы основана, в том числе, на использовании криптографических ключей. Для обеспечения конфиденциальности при обмене информацией между двумя пользователями, обмен ключами относительно прост. Но в системах, где количество пользователей доходит до сотен и тысяч, процесс управления ключами становится серьезной проблемой.

Под ключевой информацией понимается комплекс всех ключей, которые есть в системе. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает полный доступ ко всей информации.

Управление ключами – информационный процесс, включающий в себя три этапа:

- генерацию ключей;
- накопление ключей;
- распределение ключей.

В данной статье был рассмотрен только последний самый важный и ответственный этап управления криптографическими ключами – распределение ключей. К этому этапу предъявляются два требования:

- оперативность и точность распределения;
- секретность распределяемых ключей.

Для многих протоколов возможно использовать алгоритмы ассиметричного шифрования, в которых система распределения ключей решена, но существует много протоколов и приложений, защищенных с помощью алгоритмов симметричного шифрования, в данном случае распределение ключевой информации требует новых эффективных решений.

Практически все протоколы распределения ключей построены на основе алгоритма Диффи-Хеллмана.

Протокол Диффи-Хеллмана. Формирование общего ключа

Пусть два пользователя, которых условно назовем пользователь 1 и пользователь 2, желают сформировать общий ключ для алгоритма симметричного шифрования.

1. Оба пользователя должны выбрать достаточно большое простое число P и некоторое специальное число A, называемое первообразным корнем P, $1<A<P$-1, такое, что все числа из интервала [1, 2, ..., P-1] могут быть представлены как различные степени A mod P. Эти числа должны быть известны всем абонентам системы и могут выбираться открыто. Это будут так называемые общие параметры.

2. Пользователь 1 выбирает число X_1 ($X_1<P$), которое желательно формировать с помощью датчика случайных чисел. Это будет закрытый ключ первого пользователя, и он должен держаться в секрете.

3. На основе своего закрытого ключа пользователь 1 вычисляет $Y_1 = A^{x1} \bmod P$.

4. Пользователь 1 отправляет полученное число Y_1 пользователю 2.

5. Аналогичным образом пользователь 2 выбирает число X_2 и вычисляет $Y_2 = A^{x2} \bmod P$.

6. Полученное значение Y_2 пользователь 2 отправляет пользователю 1.

7. Из полученного числа Y_2 пользователь 1 формирует секретный ключ $Z = (Y_2)^{x1} \bmod P$.

8. Аналогичным образом пользователь 2 формирует секретный ключ $Z = (Y_1)^{x2} \bmod P$.

Если весь протокол формирования общего секретного ключа выполнен верно, значения Z у обоих пользователей должны получиться одинаковыми, т.к. $(Y_2)^{x1} \bmod P = (A^{x2} \bmod P)^{x1} \bmod P = A^{x1x2} \bmod P = (A^{x1} \bmod P)^{x2} = A^{x2} \bmod P$.

Несмотря на легкость вычисления экспоненты по модулю простого числа, обратная задача вычисления дискретного логарифма является достаточно сложной в вычислительном отношении задачей.

Пусть в некоторой конечной мультипликативной абелевой группе G задано уравнение $g^x = a$. Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа x, удовлетворяющего уравнению $g^x = a$. Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы. Отсюда можно построить грубую оценку сложности алгоритма поиска решений сверху — алгоритм полного перебора нашел бы решение за число шагов не выше порядка данной группы. Часто рассматривается случай, когда $G = \langle g \rangle$ группа является циклической, порождённой элементом g. В этом случае уравнение всегда имеет решение. В случае же произвольной группы вопрос о разрешимости задачи дискретного логарифмирования требует отдельного рассмотрения.

Именно это свойство позволяет обеспечить безопасность формирования общего ключа. Наиболее быстрые алгоритмы решения этой задачи, основаны на методе решета числового поля и требуют выполнения $\exp(c(\ln P)^{\frac{1}{3}}(\ln \ln P)^{\frac{2}{3}})$ арифметических операций, где P – простое число, c – некоторая по-

ложительная постоянная. Это сравнимо со сложностью наиболее быстрых алгоритмов разложения на множители. [4]

Несмотря на то, что данный алгоритм достаточно быстро позволяет вычислить секретный ключ, главной его проблемой остается необходимость аутентификации пользователей. Без дополнительных алгоритмов пользователи не могут быть уверены, что обмениваются ключами друг с другом и между ними нет злоумышленника. Для защиты от атаки «человек посередине» протокол обрастает дополнительными транзакциями, делая процесс обмена ключами более сложным. Так же есть вероятность, что проблема вычисления дискретного логарифма все-таки будет решена и тогда весь алгоритм можно будет достаточно просто взломать.

В качестве альтернативного метода, решающего проблемы протокола Диффи-Хеллмана можно рассматривать квантовые протоколы распределения ключей.

Квантовое распределение ключей

В настоящее время квантовая криптография развивается достаточно активно и в системе распределения ключей выделились два основных направления.

Первое направление основано на кодировании квантового состояния одиночной частицы и базируется на принципе невозможности различить абсолютно надежно два неортогональных квантовых состояния.

Второе направление развития основано на эффекте квантового перепутывания (запутывания).

В рамках данной статьи будет рассматриваться основной протокол квантовой криптографии в одночастичных состояниях – протокол BB84.

Протокол BB84.

Данный протокол использует квантовый канал, по которому два пользователя обмениваются сообщениями, передавая их в виде поляризованных фотонов.

Схема BB84 работает следующим образом.

1. Пользователь 1 генерирует и посылает пользователю 2 последовательность фотонов, поляризация которых выбирается случайным образом (0º, 45º, 90º и 135º).

2. Пользователь 2 принимает эти фотоны и для каждого из них случайным образом решает, замерять его поляризацию как перпендикулярную или диагональную.

3. По открытому каналу пользователь 2 сообщает, какой тип измерений был сделан. Но при этом результаты полученных измерений не разглашаются.

4. По этому же открытому каналу пользователь 1 правильный ли выбор измерений был проведен для каждого фотона.

5. Затем оба пользователя отбрасывают все случаи, когда были сделаны неправильные измерения, а оставшиеся виды поляризации и будут секретной информацией или ключом.

Этот этап работы квантово-криптографической системы называется первичной квантовой передачей.

Следующим важным этапом является оценка попыток перехвата информации в квантово-криптографическом канале связи. Допускается проведение данного этапа по открытому каналу. Суть данного этапа заключается в сравнении некоторых случайных подмножеств полученных результатов. Если при таком сравнении обнаружится наличие перехвата, оба пользователя должны будут отбросить все свои данные и проводят повторное выполнение первичной квантовой передачи. В противном случае поляризация остается прежней. Согласно принципу квантовой неопределенности, злоумышленник не может замерить как прямоугольную, так и диагональную поляризацию одного и того же фотона. Даже если он для какого-либо фотона произведет измерение и перешлет полученный результат второму пользователю, то в итоге количество ошибок намного увеличится, и это станет заметно первому пользователю и приведет к стопроцентной уверенности в состоявшемся перехвате фотонов.

В данном случае более эффективной проверкой является проверка на четность. Достаточно проверить результат каждого четного фотона. Если данные пользователей отличаются, такая проверка поможет выявить количество ошибок при передаче. Достаточно повторить подобный тест несколько десятков раз с различными подмножествами, чтобы вычислить процент допущенных ошибок. Если процент ошибок довольно высок, считается, что был произведен перехват в квантово-криптографической системе. [2]

На первый взгляд может показаться, что квантовое распределение ключей решает большинство проблем традиционной криптографии, но данный метод имеет ряд своих существенных преимуществ и недостатков.

Несмотря на то, что идеальное квантовое

распределение ключей неуязвимо для хакеров, существующие реализации провести успешную атаку и похитить построенный ключ. Перечислим основные атаки на криптосистемы с протоколами квантового распределения ключа:

• Атака с помощью светоделителя — сканирование и расщеплении импульсов на две части и анализе каждой из частей в одном из двух базисов.

• Атака «Троянский конь» в данном случае реализуется как сканирование импульса через оптический мультиплексор по направлению к стороне-отправителю или стороне-получателю.

• Когерентные атаки, которые базируются на тактике ретрансляции. Атакующий перехватывает фотоны отправителя, измеряет их состояние, а затем отправляет получателю псевдофотоны в измеренных состояниях.

• Некогерентные атаки, при которых фотоны отправителя перехватываются и перепутываются с группой передаваемых одиночных фотонов. Затем состояние группы измеряется и изменённые данные отправляются получателю.

• Атака с ослеплением лавинных фотодетекторов, позволяющая злоумышленнику получить секретный ключ тал, что получатель не заметит факта перехвата.

• Атака с разделением фотонов. Заключается в обнаружении в импульсе более одного фотона, его отведении и перепутывании с пробой. Оставшаяся неизменная часть информации отправляется получателю, а перехватчик получает точное значение переданного бита без внесения ошибок в просеянный ключ.

• Спектральная атака. Когда фотоны сгенерированы четырьмя разными фотодиодами, они имеют разные спектральные характеристики. Злоумышленник будет измерять не поляризацию, а цвет фотона.

• Атака на ГПСП (генератор псевдослучайных последовательностей). В случае, когда отправитель использует ГПСП, злоумышленник может использовать этот же алгоритм с подобными начальными значениями и получить настоящую последовательность битов. [1]

К преимуществам можно отнести:

1. Квантовая криптография позволяет обнаружить злоумышленника – при перехвате фотонов появляется значительно больше ошибок, чем их возникает в квантовом канале в результате естественного шума. [3]

2. Принцип неопределенности Гейзенберга до сих пор не позволяет осуществить клонирование фотонов, что позволяет с большей вероятностью вычислить злоумышленника.

Недостатки:

1. Сложность реализации и высокая стоимость оборудования приводит к высокой конкуренции на рынке средств защиты информации, что в свою очередь приводит к банкротству небольших компаний. Стоимость такого оборудования, как правило, превышает сумму в несколько миллионов рублей.

2. Данный метод требует значительной и долгой коррекции результатов для избегания наличия злоумышленника в квантовом канале.

3. Для передачи квантовых сигналов необходимы открытие «чистые» расстояния, что ограничивает возможности использования данного протокола.

4. Очень низкая скорость протокола обмена ключами.

Заключение.

На данном этапе развития, квантовая криптография только приближается к практическому уровню использования. Подводя итог проделанной работы, хотелось бы сказать, что, несмотря на свое бурное развитие и практически 100% защищенность информации, квантовая криптография в настоящий момент имеет существенные недостатки, которые значительно усложняют внедрение данного метода во все сферы защиты информации.

Литература

1. Действительно ли надёжна квантовая криптография? // Блог компании Toshiba. URL: https://habr.com/ru/company/toshibarus/blog/444502/ (дата обращения: 17.12.2019)

2. Голубчиков Д. М., Румянцев К. Е. Квантовая криптография: принципы, протоколы, системы // Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению «Информационно-телекоммуникационные системы». 2008.

3. Филиппов М. А., Кротова Е. Л. Квантовая криптография. Преимущества и недостатки // Вестник УРФО. Информационная безопасность. 2017. № 4 (26). С. 25–27.

4. Ященко В. В. Введение в криптографию. / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012. — 348 с.

References

1. Deystvitel'no li nadezhna kvantovaya kriptografiya? // Blog kompanii Toshiba. URL: https://habr.com/ru/company/toshibarus/blog/444502/ (data obrashcheniya: 17.12.2019)

2. Golubchikov D. M., Rumyantsev K. E. Kvantovaya kriptografiya: printsipy, protokoly, sistemy // Vserossiyskiy konkursnyy otbor obzorno-analiticheskikh statey po prioritetnomu napravleniyu «Informatsionno-telekommunikatsionnye sistemy». 2008.

3. Filippov M. A., Krotova E. L. Kvantovaya kriptografiya. Preimushchestva i nedostatki // Vestnik URFO. Informatsionnaya bezopasnost'. 2017. № 4 (26). S. 25–27.

4. Yashchenko V. V. Vvedenie v kriptografiyu. / Pod obshch. red. V. V. Yashchenko. — 4-e izd., dop. M.: MTsNMO, 2012. — 348 s.

КРОХАЛЕВА Яна Николаевна, студентка кафедры Высшей математики Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. Email: zummer483_94@mail.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, кафедра Высшей математики Пермского национального исследовательского политехнического университета, доцент. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. Email: lenkakrotova@yandex.ru

KROKHALEVA Yana, student of the Department of Higher mathematics, Perm National Research Polytechnic University. 614990, Permsky Kray, Perm, Komsomolsky Prospect, 29. Email: zummer483_94@mail.ru

KROTOVA Elena, candidate of physico-mathematical sciences, Department of Higher mathematics, Perm National Research University, docent. 614990, Permsky Kray, Perm, Komsomolsky Prospect, 29. Email: lenkakrotova@yandex.ru