И. Д. Чхайло
Тюменский государственный университет, г. Тюмень
УДК 004.056.5

ВОПРОСЫ АУТЕНТИФИКАЦИИ В СЕТЯХ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Аннотация. В работе исследуется возможность применения предварительно распределенных ключей для аутентификации устройств в сети квантового распределения ключей магистральной топологии. Приводится описание проблем, связанных с использованием сетей КРК, а также предлагается протокол для аутентификации узлов в сети КРК.

Ключевые слова: квантовые вычисления, аутентификация, сети квантового распределения ключей.

Введение. Использование технологий и сетей квантового распределения ключей (КРК) в настоящий момент кажется очень перспективным. Исходя из существующих практик, описанных, например, в [1], следует, что по достижению определенного объема обработанных данных ключ блочного шифра должен быть заменен. При этом, новый ключ не должен быть чувствителен к компрометации старого ключа.

Существуют разные подходы к решению этой задачи, например, доставка нового ключа с доверенным курьером или безопасное получение нового ключа из старого (посредством других секретных ключей, хэш-функций и криптографических протоколов). Одним из вариантов решения этой задачи является использование сети КРК.

Посредством использования квантовых и классических каналов связи между двумя узлами сети, обычно называемыми Клиентом КРК и Сервером КРК, формируется новый секретный ключ (рис. 1).

Рис. 1. Взаимодействие двух узлов для формирования ключа

При этом квантовый канал можно предполагать открытым к прослушиванию. Из-за особенностей реализации протоколов КРК, основанных на использовании принципов квантовой физики, как, например, описанном в [2] протоколе BB84 или протоколе SARG04 [3], прослушивание канала не поможет нарушителю получить полный доступ к секретному ключу.

Это основано на невозможности реализовать протокол достоверного различения двух неортогональных квантовых состояний, а также на невозможности клонирования состояний (*no-cloning theorem*) [5].

Однако те же самые особенности, что не дают злоумышленнику незаметно перехватывать траффик в квантовом канале, не дают это делать и промежуточным узлам в сети КРК.

Так, при масштабировании сети, например, при добавлении дополнительных клиентов КРК или при увеличении расстояния между клиентами (на сегодняшний день возможная

длина квантового канала составляет приблизительно 100 км), возникает необходимость добавления промежуточных узлов, то есть специального сетевого оборудования (рис. 2) [7].

Рис. 2. Взаимодействие целевых узлов посредством промежуточных узлов

Для преодоления этих ограничений возможно использовать либо доверенные промежуточные узлы, либо недоверенные промежуточные узлы. В случае использования недоверенных промежуточных узлов требуется высокоточная реализация квантовых повторителей, что в настоящий момент признано затруднительным [8].

В случае использования доверенных промежуточных узлов, между каждой парой узлов в цепочке будет устанавливаться отдельное соединение, защищенное своим ключом. Тот ключ, который должен будет использоваться для защиты сообщений между клиентом и сервером в таком случае будет появляться на промежуточных узлах в открытом виде (но, тем не менее, остается защищенным в смысле теоретико-информационной стойкости, потому как для его передачи используются квантовые каналы).

Таким образом, промежуточные узлы становятся желаемой целью нарушителя — при компрометации любого из них, например, при его подмене, распределяемый ключ будет скомпрометирован. Стоит отметить, что, учитывая относительно большую физическую удаленность устройств и тенденцию минимизировать их количество, обеспечить контролируемую и соответствующую ожиданиям физическую безопасность промежуточных узлов было бы затруднительно, хоть и возможно.

Проблема исследования. Проблема безопасности узлов сети приводит к необходимости разработки для сетей КРК, соответствующих актуальным угрозам методам обеспечения ИБ, как, например, их аутентификация.

Вопрос аутентификации для устройств, сопряженных квантовым каналом, детально описывается, в частности, в [9]. При этом, под аутентификацией понимается проверка подлинности устройства или участника генерации общего ключа.

Существуют разные способы аутентификации и методы их классификации. Основным способом аутентификации является контроль сообщений, или MAC (*message authentication code*). При этом, у участников обмена предполагается наличие предварительно распределенного общего ключа, или *pre-shared key*, как, например, в работах [10] и [11].

Большинство представленных подходов имеют существенный недостаток, связанный с ресурсоемкостью протокола. Так, методы, предложенные авторами в [9], требуют удвоения количества передаваемых кубитов. При этом, предложенные подходы подразумевают использование топологии «точка-точка», что не отвечает современным тенденциям развития сетей, которые представлены в работе [12].

В частности, в работе [12] приводится следующая классификация топологий сетей КРК:

– Топология «точка-точка», представляющая собой два целевых узла.

– Магистральная топология, представляющая цепочку узлов, целевыми среди которых являются самый первый и самый последний узлы, а промежуточные узлы являются вспомогательными.

– Смешанная топология, представляющая все остальные случаи.

Главный интерес для исследования представляют собой сети магистральной топологии, потому как в смешанных топологиях протоколы основаны на выделении магистральных топологий.

Постановка задачи. Для того, чтобы предложить эффективный способ аутентификации, укажем на две особенности, которые позволят увеличить эффективность по сравнению с протоколами аутентификации для топологии «точка-точка».

– Исследуя магистральную топологию, состоящую из доверенных узлов, не обязательно проводить полную процедуру аутентификации в квантовом канале для каждой последовательной пары узлов.

– В работе [12] предложено разделять все узлы сети КРК на целевые и промежуточные. Поэтому можно допустить разный уровень «осведомленности» целевых и промежуточных узлов касаемо используемых ключей. В частности, знание полного набора всех ключей на промежуточных узлах со стороны целевых узлов мало влияет на уровень защищенности всей сети.

Для решения поставленной задачи предполагается, что исследуемая магистральная сеть состоит из 2 целевых узлов Z_1 и Z_n, а также из $n-2$ промежуточных узлов M_2, M_3, …, M_{n-1}. При этом, для каждой пары смежных узлов существует предварительно распределенный на этих узлах ключ из n бит. Таким образом, в сети используются ключи $k_{12}, k_{23}, \dots, k_{(n-1)n}$ (рис. 3).

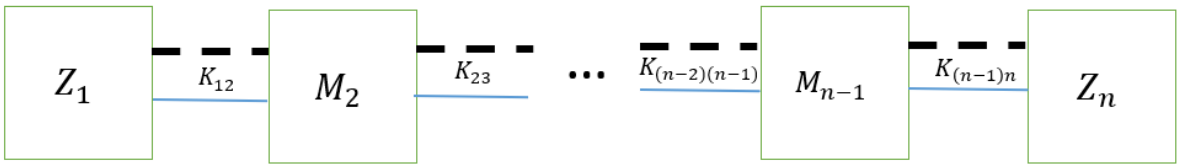

Рис. 3. Магистральная сеть с распределенными ключами

Как уже было отмечено выше, у целевых узлов предполагается знание всех ключей. У промежуточных узлов предполагается знание лишь только двух ключей, разделяемых с двумя соседними узлами.

Материалы и методы. Аутентификация заключается в составлении такой последовательности из битов или кубитов, каждый из которых будет сформирован одним из узлов, будет зависеть от предыдущих сформированных битов или кубитов, а также будет зависеть от номера формирующего его узла и ключей, которыми этот узел обладает. При проверке данной последовательности целевым узлом на корректность произойдет и косвенная аутентификация всех промежуточных узлов.

Рассмотрим матрицу, составленную из ключей $k_{l(l+1)}$, записанных по строкам. Для нумерации элементов матрицы воспользуемся верхними индексами так, что элемент $k_{l(l+1)}^{ij}$ — это *j*-й элемент *i*-й строки, который принадлежит ключу $k_{l(l+1)}$. Для удобства длину ключа полагаем равной количеству узлов в сети. Тем самым, получаем квадратную матрицу:

$$\begin{matrix} k_{12}^{11} & k_{12}^{12} & \dots & k_{12}^{1n} \\ k_{23}^{21} & k_{23}^{22} & \dots & k_{23}^{2n} \\ \dots & \dots & \dots & \dots \\ k_{(n-1)n}^{n1} & \dots & \dots & k_{(n-1)n}^{nn} \end{matrix}$$

Пара ключей $k_{(l-1)l}$ и $k_{l(l+1)}$ известны проходящему аутентификацию узлу с номером *l*. Первому и последнему узлу известны только ключи k_{12} *и* $k_{(n-1)n}$ соответственно.

Протокол аутентификации следующий:

1) Начиная со второго узла, узел с номером *l*, обладающий ключами $k_{(l-1)l}$ и $k_{l(l+1)}$, кодирует элемент $k_{(l-1)l}^{(l-1)(l-1)}$, выбирая базис в зависимости от значения $k_{l(l+1)}^{l(l-1)}$ из двух повернутых на $\frac{\pi}{8}$, как это делается в протоколе BB84 [2]. Обозначая базисы за $|+>, |->$, а также $|1>, |0>$, можно составить таблицу, какой формируется аутентификационный кубит в зависимости от двух рассматриваемых битов ключей:

Таблица 1

Кодирование битов

$k_{(l-1)l}^{(l-1)(l-1)}$ — кодируемый бит	$k_{l(l+1)}^{l(l-1)}$ — бит выбора базиса	Аутентификационный кубит
0	0	$\|0>$
0	1	$\|->$
1	0	$\|1>$
1	1	$\|+>$

2) Аутентификационный кубит передается узлу с номером *l+1*. Обладая ключом $k_{l(l+1)}$, этот узел знает, в каком базисе проводить измерение этого кубита. Результат измерения фиксируется. В зависимости от результата измерения, то есть получения бита «1» или бита «0» биты ключа $k_{l(l+1)}$ с номерами $k_{l(l+1)}^{ll}$ и $k_{l(l+1)}^{l(l+1)}$в дальнейшем меняются местами.

3) Узел с номером *l+1* каким-либо способом передает полученное значение целевому узлу.

4) Узел с номером *l+1* полностью повторяет процедуру. В дальнейшем, ее повторят и другие узлы.

5) Целевой узел, получив набор бит, полученный на разных узлах при выполнении указанного алгоритма, проводит проверку их корректности, самостоятельно реализуя алгоритм. При этом пользоваться кубитами с средствами квантовых вычислений не требуется. В случае совпадения присланного и полученного набора аутентификация признается успешной.

Результаты. Проведем оценку вероятности успешной подмены одного узла. При получении аутентификационного кубита и выбирая базис случайно, злоумышленник получит верный результат при измерении с вероятностью $\frac{3}{4}$. Далее, не обладая ключом $k_{(l-1)l}$, ему придется выбрать случайный бит, который он будет кодировать, а не обладая ключом $k_{l(l+1)}$, он будет вынужден также выбрать случайный базис. Вероятность корректной расшифровки следующим узлом в таком случае равна $\frac{1}{2}$, что равно случайному угадыванию бита. При этом, по ККС между каждой парой узлов передается ровно 1 кубит.

Таким образом, нарушитель, выполнивший подмену одного узла, остается необнаруженным с вероятностью $\frac{1}{2}$. При этом аутентификация происходит внутри квантового канала. Для того чтобы уменьшить эту вероятность, возможно провести процедуру аутентификации еще раз, при этом условившись перед началом протокола выполнить какую-либо перестановку на ключах, например, циклический сдвиг влево на 1 (иначе злоумышленник продолжит формировать те же самые сообщения). Такая процедура может быть выполнена до n раз, где n — длина каждого ключа, тем самым уменьшив вероятность остаться незамеченным до $(\frac{1}{2})^n$.

Заключение. Главное достоинство предложенного подхода является низкая ресурсоемкость с точки зрения передачи кубитов по ККС. Он позволяет проводить аутентификацию узлов внутри квантового канала связи, при этом регулировать точность работы в зависимости от предоставленных ресурсов.

Другой особенностью такого подхода является его независимость от передаваемых сообщений. В случае необходимости аутентифицировать сами сообщения, рекомендуется рассмотреть вариант применения «взаимоисключающего "или"» битов сообщения с битами, использующимися для аутентификации и замены на них битов аутентификации или битов сообщения.

СПИСОК ЛИТЕРАТУРЫ

1. Р 1323565.1.012-2017. Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. — М.: Стандартинформ. — 2018.
2. Bennet C.H. Quantum Cryptography: Public Key Distribution and Coin Tossing / C.H. Bennet, G. Brassard // Theoretical Computer Science — 2014. — Vol. 560, № 1 — P. 175-179.
3. Scarani V., Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations / V. Scarani, A. Acin, G. Ribordy, N. Gisin // Physical Review Letters, 92 — 2004. — Article ID: 057901.
4. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг; пер. с англ. — М.: Мир, 2006. — 824 с. — ISBN 5-03-003524-9.
5. Холево А.С. Квантовые системы, каналы, информация / А.С. Холево. — М.: МЦНМО, 2014. — 327 с. — ISBN 978-5-4439-2092-4. — Текст: электронный.
6. Жиляев А.Е. Методика построения сетей квантового распределения ключей смешанной топологии: дис. … канд. тех. наук / А.Е. Жиляев. — Томск: ТУСУР, 2022. — 240 с.
7. Lucamarini M., Yuan Z.L., Dynes J.F., Shields A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature. 2018; 557(7705): 400-3.

8. Перечень докладов конференции РусКрипто-2023. — URL: https://www.ruscrypto.ru/resource/archive/rc2023/files/12_gontcharov.pdf, свободный (дата обращения: 10.04.2024). — Текст: электронный.
9. Arindam Dutta, Anirban Pathak, A short review on quantum identity authentication protocols: How would Bob know that he is talking with Alice? Quantum information processing. Vol. 21, 2022.
10. Nayana Das, Goutam Paul, and Ritajit Majumdar. Quantum secure direct communication with mutual authentication using a single basis. arXiv preprint arXiv:2101.03577, 2021.
11. Piotr Zawadzki. Quantum identity authentication without entanglement. Quantum Information Processing, 18 (1):7, 2019.
12. Сети квантового распределения ключей в кибербезопасности / А.Е. Жиляев, А.Г. Сабанов, А.А. Шелупанов, А.А. Конев, Д.С. Брагин. — М.: Горячая линия — Телеком, 2023. — 152 с. — ISBN 978-5-9912-1028-7.