Симметричное шифрование квантовыми ключами

А.П. Плёнкин

Южный федеральный университет, Таганрог

Аннотация: в статье рассматриваются проблема обеспечения секретности при распределении ключа шифрования. Приведена структура стенда квантово-криптографической сети на основе коммерческой автокомпенсационной системы квантового распределения ключа с фазовым кодированием состояний фотонов. Описан процесс интеграции квантовых ключей в протоколы шифрования данных телекоммуникационной сети. Приведены результаты экспериментальных исследований по использованию квантовых ключей в сети передачи данных.
Ключевые слова: квантовый ключ, криптография, протокол, телекоммуникационная сеть, шифрование.

Проблема обеспечения защищенности при передаче информации формулируется как проблема распределения секретного ключа между двумя удалёнными пользователями [1]. У пользователей формируется одинаковый набор бит, который используется в качестве криптографического ключа. Для реализации абсолютной секретности необходимо соблюдение известных условий: ключ может быть использован только один раз, ключ должен быть случайным, его длина должна быть больше или равна длине кодируемого сообщения [2].

Защищенность классических криптографических методов базируется на математических закономерностях и теоретически ограничивается вычислительными возможностями злоумышленника. Физическим решением проблемы обеспечения секретности при распределении ключа является использование принципов квантовой криптографии [3, 4]. При этом секретность базируется на законах квантовой физики и предполагает кодирование квантового состояния одиночной частицы (фотона). Квантовое распределение ключа (КРК) реализовано в программно-аппаратных комплексах, которые именуются системами квантового распределения ключа (СКРК). Среди реализованных СКРК выделяются коммерческие системы,

функционирующие по автокомпенсационной схеме [5, 6]. Конфигурация таких систем базируется на волоконно-оптических компонентах [7].

Формирование ключей в автокомпенсационных системах КРК обеспечивается работой протокола квантовой криптографии. В СКРК применяются симметричные схемы, при этом один ключ используется для шифрования и дешифрования информации [8].

С целью применения квантовых ключей в алгоритмах шифрования данных телекоммуникационной сети, создан экспериментальный стенд (рис.1) [9, 10]. Структура стенда включает в себя: систему КРК, состоящую из двух станций (СКРК В и СКРК А); два аппаратных модуля (IP B, IP A) с программным обеспечением для управления системами КРК и сетью передачи данных. Взаимодействие аппаратных модулей с системами КРК осуществляется по сервисному каналу связи (USB-интерфейс). Доверенный канал связи реализован на основе одноволоконного одномодового оптического волокна. В схеме сеть передачи данных сконфигурирована по топологии «точка-точка» и базируется на стандарте Ethernet.

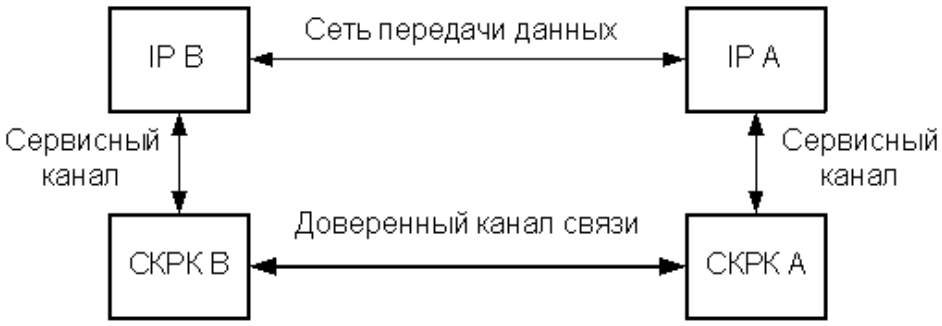

Рис. 1. – Структурная схема экспериментального стенда

Процесс формирования квантовых ключей системой КРК инициируется согласно алгоритму работы протокола квантовой криптографии. Ключи генерируются и накапливаются в буферной зоне программного обеспечения аппаратных модулей в циклическом режиме. На базе Ethernet конфигурируется виртуальный туннель vpn на основе ipsec, который представляет систему протоколов для защиты данных на сетевом

уровне телекоммуникационных сетей. Этапы создания защищенного туннеля включают в себя конфигурирование политик безопасности, задания правил маршрутизации, аутентификации и шифрования. Настройка аутентификации и шифрования производится для каждого создаваемого канала на каждое направление и для каждого из протоколов.

В памяти аппаратных модулей при помощи специализированной программной компоненты формируются файлы с ключевым материалом. Особенность схемы формирования состоит в том, что файлы и их содержимое не передаются по сети, а формируется непосредственно в аппаратных модулях. Файлы идентичны и их содержимое представляет собой массив из ключей и их идентификаторов. На рис.2 приведена выдержка из сформированного файла, содержащего 512-битные ключи и их 128-битные идентификаторы.

```
10:28:46 DEBUG - *** Ask New Key ***
10:28:46 DEBUG - Udp: Setting up UDP client to connect to 10.10.131.39:5323
10:28:46 DEBUG - Udp: UDP client successfully configured
10:28:46 DEBUG - The HEX key ID is : 0000000000009b72
10:28:46 DEBUG - The HEX key is : 6776379c3f817e57d0bb1cbfe87411eef4170032d4b86b9ecc2ccd255061a52c
10:28:47 DEBUG - *** Ask New Key ***
10:28:47 DEBUG - Udp: Setting up UDP client to connect to 10.10.131.39:5323
10:28:47 DEBUG - Udp: UDP client successfully configured
10:28:47 DEBUG - The HEX key ID is : 0000000000009b70
10:28:47 DEBUG - The HEX key is : 1ca68d77407db7bb6f77dc3a9f1039d5bb731c319b27aae331c8f7da4e065d86
10:28:47 DEBUG - *** Ask New Key ***
10:28:47 DEBUG - Udp: Setting up UDP client to connect to 10.10.131.39:5323
10:28:47 DEBUG - Udp: UDP client successfully configured
10:28:47 DEBUG - The HEX key ID is : 0000000000009b6e
10:28:47 DEBUG - The HEX key is : 50305046b2740f1dc8be34cae89c9ec2307a5dbc6f93dac45b67b2cc808f2a1c
```

Рис. 2. – Сформированный файл с ключами шифрования

Поиск необходимых ключей в файлах осуществляется по их идентификаторам. Длина ключа задается при формировании файлов в пределах от 32 до 512 бит. Ключи интегрируются в конфигурацию протокола ipsec одновременно на удаленных аппаратных модулях. Скорость формирования ключей системой КРК в эксперименте составляет порядка 500 бит/с. Для интеграции квантовых ключей в алгоритмы шифрования vpn туннеля, ключи необходимой длины копируются в соответствующие области конфигурации протокола ipsec. На рис.3 приведена работоспособная типовая конфигурация vpn туннеля с интегрированными 256-битными квантовыми

ключами для каждого из четырех направлений шифрования.

```
#!/sbin/setkey -f
flush;
spdflush;

# AH
add 10.10.131.39 10.10.131.32 ah 15700 -A hmac-sha256 "bfe3aa8b4b3737387257cf3b6aa14a6d";
add 10.10.131.32 10.10.131.39 ah 24500 -A hmac-sha256 "726f8275afeca27ef01241d8249d9a56";

# ESP
add 10.10.131.39 10.10.131.32 esp 15701 -E aes-cbc "462d48002ae306736ec30368af35e7f7";
add 10.10.131.32 10.10.131.39 esp 24501 -E aes-cbc "fc2380f7eac1b08251400ff40025cc39";

spdadd 10.10.131.32 10.10.131.39 any -P out ipsec
          esp/transport//require
          ah/transport//require;

spdadd 10.10.131.39 10.10.131.32 any -P in ipsec
          esp/transport//require
          ah/transport//require;
```

Рис. 3. – Листинг конфигурации туннеля

Для проверки работоспособности стенда, применяется метод анализа трафика телекоммуникационной сети. Рис.4 демонстрирует результат применения команды «tcpdumb», которая позволяет проводить анализ всех передаваемых пакетов данных по сети Ethernet между аппаратными модулями. Из рисунка видно, что все передаваемые по телекоммуникационной сети данные зашифрованы с применением квантовых ключей.

```
10:52:49.797461 IP 10.10.131.39 > 10.10.131.32: AH(spi=0x00003d54,seq=0x15): ESP(spi=0x00003d55,seq=0x15), length 104
10:52:49.797605 IP 10.10.131.32 > 10.10.131.39: AH(spi=0x00005fb4,seq=0x15): ESP(spi=0x00005fb5,seq=0x15), length 104
10:52:50.797684 IP 10.10.131.39 > 10.10.131.32: AH(spi=0x00003d54,seq=0x16): ESP(spi=0x00003d55,seq=0x16), length 104
10:52:50.797820 IP 10.10.131.32 > 10.10.131.39: AH(spi=0x00005fb4,seq=0x16): ESP(spi=0x00005fb5,seq=0x16), length 104
10:52:51.797864 IP 10.10.131.39 > 10.10.131.32: AH(spi=0x00003d54,seq=0x17): ESP(spi=0x00003d55,seq=0x17), length 104
10:52:51.798019 IP 10.10.131.32 > 10.10.131.39: AH(spi=0x00005fb4,seq=0x17): ESP(spi=0x00005fb5,seq=0x17), length 104
10:52:52.798065 IP 10.10.131.39 > 10.10.131.32: AH(spi=0x00003d54,seq=0x18): ESP(spi=0x00003d55,seq=0x18), length 104
10:52:52.798190 IP 10.10.131.32 > 10.10.131.39: AH(spi=0x00005fb4,seq=0x18): ESP(spi=0x00005fb5,seq=0x18), length 104
```

Рис. 4. – Анализ передаваемых данных

Таким образом, разработанный стенд обеспечивает применение квантовых ключей для шифрования данных в телекоммуникационной сети.

Возможности конфигурации протокола шифрования позволяют применять ключи длиной от 32 до 512 бит с управляемым параметром «время жизни ключа».

Уникальный стенд квантово-криптографической сети с интегрированной системой квантового распределения ключа позволяет проводить всесторонние экспериментальные исследования алгоритмов

работы [11, 12] СКРК и анализ функциональных возможностей программного обеспечения оборудования квантовой криптографии [13].

Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-37-00003 мол_а.

Литература

1. Румянцев К.Е. Системы квантового распределения ключа: Монография. − Таганрог: Издательство ТТИ ЮФУ, 2011. − 264 с.

2. Бабаш А.В., Шанкин Г.П. Криптография. – М.: СОЛОН-Р, 2002. – 512 с.

3. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. «Hacking commercial quantum cryptography systems by tailored bright illumination», Nat. Phot., vol. 4, no. 686, p. 5, 2010.

4. Makarov V. Quantum cryptography and quantum cryptanalysis, doktor ingenior thesis, Norwegian University of Science and Technology. – 2007. – 158 p.

5. Gisin N., Ribordy G., Tittel W., Zbinden H., «Quantum cryptography», Rev. Mod. Phys., vol. 74, no. 1, pp. 145-195, 2002.

6. Stucki D., Gisin N., Guinnard O., Ribordy G., Zbinden H., «Quantum Key Distribution over 67 km with a plug & play system», Quantum Phys., p. 8, 2002.

7. Clavis. Plug & play quantum cryptography // id3000. Specifications. id Quantique SA. – Ver. 2.1. – January 2005. – 2 p.

8. Румянцев К.Е., Плёнкин А.П., Синхронизация системы квантового распределения ключа в режиме однофотонной регистрации импульсов для повышения защищенности // Радиотехника. – 2015. – № 2. – С. 125-134.

9. Румянцев К.Е., Плёнкин А.П. Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей // Телекоммуникации. – 2014. – № 10. – С. 11–16.

10. Румянцев К.Е., Плёнкин А.П. Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости // Известия ЮФУ. Технические науки. – 2014. – № 8. – С. 81-96.

11. Pljonkin A.P., Rumyantsev K.Y. Single-photon Synchronization Mode of Quantum Key Distribution System. India, New Delhi, 2016, pp.531-534. DOI: 10.1109/ICCTICT.2016.7514637.

12. Мациборко В.В., Будко А.Ю., Береснев А.Л., Мациборко М.А. Исследование устройств регистрации ионного тока в камере сгорания // Инженерный вестник Дона, 2014, №4 URL: ivdon.ru/ru/magazine/archive/n4y2014/2611/.

13. Шурховецкий А.Н. Многоканальная частотно-избирательная система СВЧ диапазона основе направленных фильтров бегущей волны// Инженерный вестник Дона, 2010, №4 URL: ivdon.ru/ru/magazine/archive/n4y2010/292.

Gratitude

The reported study was funded by RFBR according to the research project No.16-37-00003 mol_a.

References

1. Rumyantsev K.E. Sistemy kvantovogo raspredeleniya klyucha: Monografiya [Quantum key distribution systems: Monograph]. Taganrog: Izdatelstvo TTI YuFU, 2011. 264 p.

2. Babash A.V., Shankin G.P. Kriptografiya [Cryptography]. M.: SOLON-R, 2002. 512 p.

3. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. «Hacking commercial quantum cryptography systems by tailored bright illumination», Nat. Phot., vol. 4, no. 686, p. 5, 2010.

4. Makarov V. Quantum cryptography and quantum cryptanalysis, doktor ingenior thesis, Norwegian University of Science and Technology. 2007. 158 p.

5. Gisin N., Ribordy G., Tittel W., Zbinden H., «Quantum cryptography», Rev. Mod. Phys., vol. 74, no. 1, pp. 145-195, 2002.

6. Stucki D., Gisin N., Guinnard O., Ribordy G., Zbinden H., «Quantum Key Distribution over 67 km with a plug & play system», Quantum Phys., p. 8, 2002.

7. Clavis. Plug & play quantum cryptography. id3000. Specifications. idQuantique SA. Ver. 2.1. January 2005. 2 p.

8. Rumyantsev K.E., Pljonkin A.P., Radiotekhnika. 2015. № 2. pp. 125-134.

9. Rumyantsev K.E., Pljonkin A.P. Telekommunikatsii. 2014. № 10. pp. 11-16.

10. Rumyantsev K.E., Pljonkin A.P. Izvestiya YuFU. Tekhnicheskie nauki. 2014. № 8. pp. 81-96.

11. Pljonkin A.P., Rumyantsev K.Y. Single-photon Synchronization Mode of Quantum Key Distribution System. India, New Delhi, 2016, pp. 531-534. DOI: 10.1109/ICCTICT.2016.7514637.

12. Matsiborko V.V., Budko A.Yu., Beresnev A.L., Matsiborko M.A. Inženernyj vestnik Dona (Rus), 2014, №4, URL: ivdon.ru/ru/magazine/archive/n4y2014/2611/.

13. Shurkhovetskiy A.N. Inženernyj vestnik Dona (Rus), 2010, №4, URL: ivdon.ru/ru/magazine/archive/n4y2010/292.