3. Положить x^* равным такому вектору над кольцом R, для которого выполняется равенство $\varphi(x^*) = \min_{x \in R^n} \varphi(x)$.

Указанный алгоритм предполагает вычисление преобразования Ферма N раз, однако число уравнений в СЛУ (1) при этом ограничивается приведенным выше условием 2.

В заключение отметим, что предложенная модификация метода максимума правдоподобия позволяет при больших значениях числа неизвестных решать СЛУ (1) с меньшей трудоемкостью по сравнению с самим ММП, при той же надежности. Так, например, при n = 10 система линейных уравнений над кольцом Z/16 может быть решена более чем в 10 раз быстрее предложенным алгоритмом, чем методом максимума правдоподобия (см. табл. 1). Аналогично, при n = 13 над кольцом Z/32 можно достичь выигрыша в трудоемкости более чем в 25 раз. Однако уменьшение времени решения системы линейных уравнений приводит к необходимости использования больших объемов памяти.

Список литературы

1.*Балакин Г.В.* Введение в теорию случайных систем уравнений // Труды по дискретной математике. – М.: ТВП. – 1997. – Т. 1. – С. 1 – 18.

2.*Смирнов В.Г.* Системы булевых уравнений рекуррентного типа // Обозрение прикл. промышл. матем. – 1995. – Т. 2. – Вып. 3. – С. 477 – 482.

3.*Алексейчук А.Н.* Системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N // Захист інформації. – 2001. – № 4. – С. 12 – 19.

4.*Golic J. Dj.*, *Morgari G.* Vectorial fast correlation attaks // http://eprint.iacr.org/ 2004/247.

5.*Балакин Г.В.* О вероятностном подходе к решению систем уравнений с целочисленными неизвестными // Дискретная математика. –1995. –Т. 7. –Вып. 1. –С. 88– 98.

6.*Леман Э.* Проверка статистических гипотез: Пер. с англ. – М.: Наука, 1964. – 498 с.

7.*Алексейчук А.Н.*, *Игнатенко С.М.* Оценки эффективности универсальных методов восстановления искаженных линейных рекуррент над кольцом вычетов по модулю 2^N // Збірник наукових праць ІПМЕ НАН України – Вып. 20. – Киев, 2003. – С. 40 – 48.

8.*Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов: Пер. с англ. – М.: Мир, 1989. – 448 с.

9.*Ноден П., Китте К.* Алгебраическая алгоритмика: Пер. с франц. – М.: Мир, 1999.

Поступила 24.11.2006 г.

УДК 621.391.15

Алексеев Д.А., Корнейко А.В.

ПРАКТИЧЕСКАЯ РЕАЛЬНОСТЬ КВАНТОВО-КРИПТОГРАФИЧЕСКИХ СИСТЕМ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Квантовая криптография (КК, Quantum Cryptography) – одно из наиболее активно развиваемых в настоящее время направлений квантовой информатики. Из отдельных занимательных экспериментов с поляризацией фотонов она превратилась в теоретически обоснованную область криптографической науки.

Технология КК опирается на принципиальную неопределенность поведения квантовой системы – невозможно одновременно получить координаты и импульс частицы, невозможно измерить один параметр фотона, не исказив другой. Это фундаментальное свойство природы в физике известно как принцип неопределенности Гейзенберга, сформулированный в 1927 г.

Процесс распределения ключей, основанный на принципах КК, получил название квантовое распределение ключей (КРК, Quantum Key Distribution), а системы распределения

ключей, основанные на технологии КК – квантово-криптографических систем распределения ключей (ККСРК). В некоторой литературе ККСРК называют также квантовыми криптографическими системами.

В ККСРК отправитель кодирует отправляемые фотоны, задавая определенные квантовые состояния, а получатель регистрирует эти состояния. Затем получатель и отправитель по заранее оговоренному правилу совместно обсуждают результаты наблюдений. В итоге можно быть уверенным, что переданная и принятая кодовые последовательности, которые характеризуют ключи, тождественны. Обсуждение результатов касается ошибок, внесенных шумами или злоумышленником, и ни в малейшей мере не раскрывает содержимого сообщения, т.е. ключа. В ККСРК сторонами может обсуждаться четность сообщения, но не отдельные биты ключа.

Следовательно, в основе безопасной передачи ключей шифрования методом КК лежат физические законы квантовой механики, а не математические расчеты теории сложности, как в традиционной криптографии с открытым ключом.

Интенсивное развитие средств волоконной оптики как типовой транспортной среды телекоммуникаций, переход в перспективе к технологиям полностью оптических сетей связи (All Optical Networks, AON), делает ККСРК, где информация обрабатывается полностью в оптическом базисе, одними из наиболее перспективных методов распределения ключей.

Поэтому в ряде ведущих стран мира, в первую очередь в США, Великобритании, Франции, Швейцарии и России, интенсивно ведутся как теоретические, так и практические работы по разработке ККСРК.

В настоящее время работы по созданию ККСРК наиболее активно в мире проводятся в исследовательских центрах США. Активные исследования в области КК ведут IBM, Национальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт, компания MagiQ и др.

Первое экспериментальное подтверждение технической возможности создания ККСРК удалось провести в 1989 году в Исследовательском центре фирмы IBM, впервые продемонстрировав работоспособность теоретической основы протокола BB84, разработанного группой Чарльза Беннетта (Charles Bennett) в 1984 году и впервые опубликованного в [1]. В настоящее время в IBM технологией КК продолжает заниматься принадлежащая корпорации лаборатория Almaden Research Center [2]. О практических достижениях IBM в квантовой криптографии известно немногое – эти работы ими выполняются по заказу АНБ и поэтому мало рекламируются.

В Лос-Аламосской национальной лаборатории завершена разработка и введена в опытную эксплуатацию ВОЛС общей длиной 48 км (4x12 км), в которой осуществляется КРК со скоростью несколько десятков кбит/с [3].

К исследованиям в области КК присоединилось и MagiQ Technologies Inc. из Нью-Йорка, которая была создана в 1999 г. для исследований в области квантовой электроники на средства крупных финансовых институтов [2]. Помимо собственных сотрудников с MagiQ взаимодействуют научные работники из целого ряда университетов США, Канады, Великобритании и Германии. В [4] сообщается, что в 2001 году MagiQ осуществила в штате Навахо связь с использованием квантово-оптических технологий (по известному протоколу BB84) на расстояние 30 км. В продукте MagiQ средство для КРК названо Navajo – по имени индейцев Навахо, уникальный язык которых во время Второй мировой войны американцы использовали для передачи секретных сообщений. В 2004 году на исследования в области КК MagiQ получила 7 млн. долл. от нескольких инвесторов [2].

В [5] сообщается, что Northwestern University и BBN Technologies of Cambridge создали ККСРК, получившую название AlphaEta, где по ВОЛС длиной 9 км каждые три секунды передается заново созданный квантовый ключ длиной 1 Кбит.

В 2002 году ученые из Северо-Западного университета Northwestern University, Эванстон, штат Иллинойс) усовершенствовали известный протокол BB84 и реально продемонстрировали прототип ККСРК, работающей на новом принципе КК [6]. Они предложили в ККСРК квантовое кодирование всех данных, а не только одного бита ключа. Разработанный ими прототип ККСРК позволяет передавать данные уже на скорости порядка 250 Мбит/с. Теперь ученые решают практическую задачу доказательства, что схема позволяет сигналам проходить сквозь оптические усилители. В этом случае метод можно будет использовать не только в ВОЛС между двумя точками, но и в сетях технологии AON. Еще эта команда работает над тем, чтобы достичь скоростей порядка 2,5 Гбит/с.

Ученые уже получили несколько патентов на свои разработки и сейчас работают вместе со своими промышленными партнерами Telcordia Technologies и BBN Technologies над дальнейшим усовершенствованием системы. Исследования Северо-Западного университета в области КК финансируются оборонным агентством по передовым исследовательским проектам DARPA (the Defense Advanced Research Projects Agency) в объеме 4,7 млн. долларов [6].

Работы по созданию реальных прототипов ККСРК проводятся также в исследовательском центре HP Labs в Бристоле американской компании Hewlett-Packard [7].

Работы по созданию ККСРК широко проводятся и в Европе. Так, в 1995 г. швейцарская группа квантовой оптики под руководством Никола Жизена (Nicolas Gisin) из университета Женевы, благодаря финансовой поддержке, оказанной компанией Swisscom, продемонстрировала работоспособность теории КК, с помощью протокола BB84 сгенерировав общий секретный ключ в двух пунктах (Женева и Нион), находящихся на разных берегах Женевского озера и соединенных подводным оптическим кабелем длиной около 23 километров [8]. В 1997 году группой был проведен первый эксперимент с протоколом E91, устроенный между двумя поселками под Женевой, находящимися в южном и северном пригородах на расстоянии свыше 10 километров друг от друга. В настоящее время группа принимает активное участие в общеевропейском проекте EQCSPOT.

Швейцарская компания id Quantique занимается разработкой коммерческих продуктов, в основе работы которых использована технология КК [9]. Система КРК, разработанная компанией, успешно тестировалась на 67-километровом оптоволоконном канале между Женевой и Лозанной, при этом скорость передачи ключа на этой дистанции составляла 60 бит/с [2]. На более коротких дистанциях при работе системы с существующими оптоволоконными кабелями скорость передачи возрастает до 1 Мбит/с. Коммуникационная система, задействованная в экспериментах id Quantique, может подключаться к ПК через USB-порт. В [9] также сообщается, что id Quantique специализируется также на разработке квантовых генераторов случайных чисел (RNG) для криптографических систем.

В Великобритании интересы к созданию ККСРК проявляют правительственное агентство по коммуникациям GCHQ (Government Communications Headquaters), который является британским аналогом американского АНБ и действует параллельно с известными службами MI5 и MI6, а также подразделения Минобороны DERA (Defence Evaluation and Research Agency), компания British Telecom и др.

Центр квантовых вычислений (Centre for Quantum Computation) Кларендонской лаборатории (Clarendon Lab.) Оксфордского университета ведет разработки в области создания ККСРК с 1992-1993 гг. [10]. Группой ученых под руководством Артура Экерта (Artur Ekert), автора протокола E91, в лабораториях агентства DERA в эти годы была построена первая британская экспериментальная установка ККСРК, основанная на этом протоколе КК. В настоящее время работы по совершенствованию ККСРК в этом центре ведутся благодаря финансированию GCHQ, фонда EPSRC (Engineering and Physical Sciences Research Council), проекта EQCSPOT.

Министерством обороны Великобритании поддерживается исследовательская корпорация QinetiQ, активно совершенствующая технологию КК [11]. Эта компания появилась на свет в результате деления британского агентства DERA в 2001 г., вобрав в себя все неядерные оборонные исследования. Однако о своих достижениях в области КК QinetiQ широкой публике пока не сообщает.

Исследования в области КК ведутся и в европейском исследовательском центре TREL (Toshiba Research Europe Limited), расположенном в Кембридже (Великобритания) [2, 11]. В них участвуют сотрудники Кембриджского университета и Империал-колледжа в Лондоне. Экспериментальная ККСРК, созданная TREL, передает ключи со скоростью до 2 кбит/с, однако, по оценкам разработчиков, она может работать и быстрее [12].

В связи с перспективностью СРК, основанных на технологии КК, Еврокомиссия решила поддержать два крупных международных проекта в Европе по созданию ККСРК, чтобы ускорить работы в этой области криптографии.

Так, с апреля 2004 года начат проект создания глобальной защищенной оптической системы связи SECOQC (Secure Communication based on Quantum Cryptography), включающий 43 научно-исследовательские и научно-производственные организации из 11 стран Европы [13]. Общий бюджет проекта SECOQC, рассчитанный на четыре года, составляет 11,4 млн. евро. Координатором проекта SECOQC является подразделение квантовых технологий компании ARS Seibersdorf Researsh. Цель SECOQC заключается в разработке принципов инфраструктуры для КРК, которая будет представлять собой развитую сеть безопасных коммуникаций. Проект разделен на восемь проектных областей, объединенные в два блока: это физические основы устройств, инфраструктура и протоколы. Первые фазы проекта нацелены на решение следующих задач: разработка устройств, обеспечивающих выполнение КРК; разработка безопасной архитектуры и протоколов КРК; разработка сетевой архитектуры КРК [13]. Первых результатов реализации SECOQC ожидают к середине 2008 года.

Евросоюзом финансируется также проект EQCSPOT или «Европейская квантовая криптография и однофотонные технологии» (European Quantum Cryptography and Single Photon Technologies), в реализации которого активное участие принимают ученые Швейцарии, Великобритании, Франции и других стран Европы [7, 10].

Ученые России уже перешли от чисто теоретических исследований к практической реализации идей КК в виде различных экспериментальных макетов ККСРК. Ряд исследований российских ученых финансируются по грантам SECOQC.

Работы по КК ведутся и в Азии [2, 12]. Японской корпорацией Mitsubishi Electric удалось передать квантовый ключ на расстояние 87 км, правда, на скорости в 1 байт/с. В 2004 году компанией NEC была построена ККСРК, работающая на дальность до 150 км по ВОЛС.

В настоящее время оборудование для создания ККСРК серийно не выпускается, однако в [14, 15] сообщается, что консорциумом, состоящим из швейцарской фирмы ID Quantique и американской компании Magiq Technologies Inc., предлагается для продажи комплект QPN Security Gateway (коммерческий аналог экспериментальной установки Navajo), обеспечивающий безусловно стойкое распределение квантовых ключей на расстояние до 120 км. Пока правительство США разрешили MagiQ продавать ККСРК только американским компаниям и ведомствам. Однако фирма добивается получения лицензии на продажу этой ККСРК и в других странах «большой восьмерки», то есть в Великобритании, Германии, Италии, Канаде, России, Франции и Японии. Цена одного комплекта устройства впечатляет – от 50 до 100 тыс. долларов, в зависимости от комплектации. Кроме того, выпускается «облегченная» версия QPN Security Gateway под названием Qbox ценой от 40 до 50 тыс. долларов. Это, по сути дела, открытая конфигурируемая система для лабораторных исследований в области КРК.

Таким образом, проведенный обзор позволяет сделать вывод, что работы в области создания ККСРК в настоящее время в ведущих странах мира «переросли» этап первоначальных теоретических исследований и привели к созданию реальных образцов систем КРК.

В тоже время нельзя говорить о законченности исследований в области создания ККСРК. Ведь эффективность разработанных и экспериментально опробованных ККСРК по ряду параметров (криптографические свойства вырабатываемых ключей, объем используемого первичного ключевого материала, количество раундов обмена информацией между пользователями, скорость передачи ключей и т.д.) не в полной мере удовлетворяет современным требованиям к системам распределения ключей для криптографических систем.

Список литературы

1. Bennett C., Brassard G. Quantum cryptography: Public-key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, Dec 1984, pp. 175-179.
2. http://www.pcweek.ru/Year2003/N43/CP1251/TematicReviews/chapt3.htm.
3. http://www.ict.nsc.ru/ws/show_abstract.dhtml?ru+111+8604.
4. http://kv.by/index2002474603.htm.
5. http://www.hardwareportal.ru/Newsarchive/2006_08_1.html.
6. http://kv.by/index2002474603.htm.
7. Волков Д. Лидер команды прагматиков//Открытые системы. – 2006. – №5.
8. http://old.computerra.ru/online/firstpage/hisi/6432.
9. http://www.setevoi.ru/cgi-bin/srch.pl?id=1739.
10. http://www.computerra.ru/2000/373/6060.
11. http://www.securitylab.ru/news/214732.php.
12. http://www2.computerra.ru/xterra/homo/27954.
13. http://www.secoqc.net.
14. http://www.inrecolan.com/rus/news.php?cp=1179&num=3.
15. http://pda.computerra.ru/index.php?action=article&section_id

Поступила 24.11.2006 г.