УДК 003.26:621.39+530.145

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ КВАНТОВЫХ СИСТЕМ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДЛЯ ОГРАНИЧЕНИЯ ДОСТУПА К ТЕЛЕВИЗИОННЫМ КАНАЛАМ

Е.В. ВАСИЛИУ, С.В. НИКОЛАЕНКО, Р.С. МАМЕДОВ

Одесская национальная академия связи им. А.С. Попова

PROSPECTS OF QUANTUM KEYS' DISTRIBUTION SYSTEMS APPLICATION FOR ACCESS RESTRICTION TO TELEVISION CHANNELS

E.V. VASILIU, S.V. NIKOLAENKO, R.S. MAMEDOV

Odessa national academy of telecommunications n.a. O.S. Popov

Современное информационное общество постоянно испытывает необходимость в усовершенствовании методов защиты телекоммуникационных каналов от несанкционированного прослушивания. Предложенная в 80-х годах XX века идея применения принципов квантовой механики к криптографии привела к развитию целого мультидисциплинарного научного направления – квантовой криптографии [1]. Один из наиболее развитых к настоящему времени ее разделов – квантовые протоколы распределения ключей, позволяющие распределять секретные ключи с безусловной стойкостью [2].

Основным преимуществом квантового распределения ключей перед обычными классическими схемами является принципиальная возможность обнаружить прослушивание канала. Злоумышленник должен производить манипуляции с передаваемыми в квантовом канале фотонами, а также определенные квантовые измерения их состояний. Эти манипуляции и измерения неизбежно приводят к возмущению состояний, что и позволяет обнаружить любые попытки прослушивания квантового канала. Отметим, что законы квантовой механики позволяют не только обнаружить возмущение состояний, но и связать уровень ошибок при измерениях у легитимных пользователей с количеством информации, которую мог получить злоумышленник. Это позволяет провести так называемую процедуру усиления секретности, при которой длина переданного ключа уменьшается на некоторое число бит, которое зависит от уровня ошибок при передаче [1]. В результате количество информации о ключе, которую может получить злоумышленник после этой процедуры, ограничено сверху сколь угодно малой величиной, с вероятностью, сколь угодно близкой к единице [2]. Таким образом, протоколы квантового распределения ключей, в отличие от большинства классических схем, обладают безусловной стойкостью, не зависящей от вычислительных и других технических возможностей злоумышленника [1, 2].

Одна из возможных областей применения квантовых протоколов распределения ключей – системы ограничения доступа к телевизионным каналам. В любом современном декодере применяется сменный ключ, который хранит в себе учетный номер, коды шифрования канала, данные об оплате и т.д. Этим ключом является смарт-карта. Такая карта содержит в себе микрокомпьютер с энергонезависимой памятью и имеет специальную защиту. Декодер имеет возможность обмениваться информацией с картой – передавать ей специальные команды и получать из нее данные.

Для ограничения доступа к телевизионным каналам в большинстве схем используется либо определенная перестановка блоков кадра телесигнала, либо разрезка строк на две части и перестановка этих частей. Схема перестановки передается в составе служебной информации телесигнала в зашифрованном виде. Расшифровку этой схемы производит смарт-карта с помощью имеющегося в ней секретного ключа, называемого операционным. Оператор пе-

риодически проводит смену операционного ключа, передавая его, также в зашифрованном виде, через эфир в составе служебной информации. Такая схема автообновления ключей используется, например, в системе Eurocrypt. При этом операционный ключ шифруется с помощью управляющего ключа, который на стороне абонента также хранится в смарт-карте. Отметим, что получив каким-либо способом управляющий ключ, злоумышленник может впоследствии получать все новые операционные ключи. Однако для этого он должен либо взломать смарт-карту, что представляет собой очень трудную задачу, либо перехватить один или несколько зашифрованных операционных ключей и затем провести атаку на управляющий ключ. Эта задача также сложна, учитывая достаточно высокую стойкость современных алгоритмов шифрования, однако при использовании больших вычислительных мощностей (например, сети из нескольких тысяч современных персональных компьютеров) вполне разрешима.

Квантовая система распределения ключей между оператором и абонентами может закрыть эту уязвимость. При этом можно вообще отказаться от схемы шифрования операционных ключей управляющим, а непосредственно распределять операционные ключи с безусловной стойкостью. Однако технология квантового распределения ключей на сегодняшний день обладает и рядом существенных недостатков.

Одним из главных недостатков систем квантового распределения ключей является ограниченность расстояний, на которые возможна передача с приемлемым уровнем ошибок, а также низкая скорость передачи. Это обусловлено целым рядом причин, среди которых деполяризация фотонов в оптоволоконных линиях, несовершенство излучателей и детекторов одиночных фотонов и др. В настоящее время возможна передача по оптоволоконной линии с приемлемым уровнем ошибок со скоростью порядка 1 Мбит/с на расстояние 10-20 км [3, 4] и со скоростью до 10 кбит/с на расстояние до 100 км [4]. Максимально достигнутое расстояние составляет порядка 150 км – при достаточно больших потерях и соответственно очень низкой скорости (порядка 0,5 бит/с) [5]. Что касается оптического беспроводного канала, т.е. передачи фотонов через атмосферу, то здесь помехой является солнечный свет, а также турбулентность атмосферы. Здесь пока достигнуты расстояния порядка 100 км при хорошей погоде.

Однако главным препятствием к применению систем квантового распределения ключей для ограничения доступа к телеканалам на сегодняшний день является дороговизна необходимого оборудования. Так, компания MagiQ с 2006 г. предлагает plug-n-play систему, позволяющую передавать по оптоволоконному каналу до ста 256-битных ключей в секунду на небольшие расстояния, а максимальная дальность передачи составляет 100 км [6]. Эти технические параметры вполне достаточны для обновления операционных ключей в системах ограничения доступа к телеканалам. Однако стоимость системы для пары абонентов составляет около $50000, что, конечно, не позволяет пока устанавливать такие системы у абонентов цифрового телевидения. Кроме того, для использования такой системы у абонента должен быть оптоволоконный канал, компьютер, к которому подключается оборудование для квантового распределения ключей, а также соответствующий интерфейс для переноса полученного ключа в смарт-карту.

Возможна передача ключа с помощью квантовой системы распределения ключей и через эфир, например, со спутника. Соответствующие эксперименты проводятся в настоящее время, однако подобных коммерческих систем пока не существует. Отметим, что необходимое для этого оборудование также достаточно дорого. Так, у абонента необходимо установить сложную оптическую систему приема сигналов, включающую небольшой телескоп и высокочувствительные детекторы одиночных фотонов.

Таким образом, квантовое распределение ключей представляет собой перспективную технологию, позволяющую распределять ключи с очень высокой степенью безопасности. Однако на данный момент технология является еще достаточно "сырой" и дорогостоящей, что ограничивает ее применение областями, где стоимость не является главным критерием,

но требуется высокий уровень безопасности, например, в системах правительственной и военной связи. В будущем, по мере развития этой технологии и снижения стоимости оборудования, системы квантового распределения ключей могут использоваться во многих системах конфиденциальной связи, и, в частности, для обновления ключей в системах ограничения доступа к телевизионным каналам.

В работе [7], выполненной в ОНАС им. А.С. Попова, проведено теоретическое исследование эффективности и стойкости к некогерентным атакам квантовых протоколов распределения ключей с многомерными квантовыми системами. Показано, что оптимальными одновременно по критериям стойкости и эффективности являются протоколы типа "приготовление – измерение" с использованием двух взаимно несмещенных базисов. Таким образом, эти протоколы, позволяющие повысить скорость передачи и обладающие большей стойкостью по сравнению с протоколами, используемыми в системе компании MagiQ, в будущем могут быть использованы в системах квантового распределения ключей, в том числе и для распределения операционных ключей операторами цифрового телевидения.

Литература

1. *Баумейстер Д., Экерт А., Цайлингер А*. Физика квантовой информации.- М.: Постмаркет, 2002.

2. SECOQC White Paper on Quantum Key Distribution and Cryptography.- Preprint: http://www.arxiv.org/abs/quant-ph/0701168v1. – 2007. – 28 p.

3. *Zhang Q., Takesue H., Honjo T. et al*. Megabits secure key rate quantum key distribution // New Journal of Physics. – 2009. V. 11. – 045010.

4. *Yuan Z.L., Dixon A.R., Dynes J.F. et al.* Practical gigahertz quantum key distribution based on avalanche photodiodes // New Journal of Physics. – 2009. V. 11. – 045019.

5. *Honjo T., Nam S.W., Takesue H. et al*. Long-distance entanglement-based quantum key distribution over optical fiber // Optics Express. – 2008. – V. 16, Is. 23. – P. 19118 – 19126.

6. http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf (16.06.2009).

7. *Василиу Е.В., Мамедов Р.С*. Сравнительный анализ эффективности и стойкости к некогерентным атакам квантовых протоколов распределения ключей с передачей многомерных квантовых систем // Наукові праці ОНАЗ ім. О.С. Попова. – 2008, № 2.