А. С. Герасимов

СОВРЕМЕННЫЕ СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ С ПОМОЩЬЮ КВАНТОВО-МЕХАНИЧЕСКИХ МЕТОДОВ

Квантовая криптография открывает возможность гарантированно безопасной передачи данных, а также позволяет реализовать протоколы распространения ключа и поточного шифрования между пространственно удаленными пользователями. Фундаментальные законы квантовой механики, которые использует квантовая криптография, базируются на принципе неопределенности Гейзенберга — запрете на клонирование заранее неизвестного квантового состояния и невозможности получения какой-либо информации о передаваемых квантовых состояниях без их возмущения, а также на невозможности корректно получить квантовое состояние без знания базиса, в котором оно было подготовлено.

Основная исследовательская деятельность в области квантовой криптографии ведется по нескольким направлениям:

- разработка и усовершенствование технических характеристик приборов, участвующих в реализации квантовых протоколов;
- разработка квантовых протоколов на основе соответствующих квантово-механических принципов.

Исходя из этого, по нашему мнению, квантовая криптография представляет собой прикладную область квантовой механики. Однако использование квантовой криптографии как современного средства защиты информации требует решений, которые будут обеспечивать функциональность не хуже, чем у существующих классических методов. Но возможность замены методов распределения ключа и шифрования с безопасностью, основанной на сложностно-теоретических подходах, приборами с поддержкой квантово-криптографических функций вызывает справедливые вопросы об экономичности и удобстве замены.

Квантовые протоколы распределения ключа

Исторически сложилось, что работа протоколов описывается при помощи следующих участников: Алиса, Боб, Ева. Алиса и Боб представляются как легитимные участники протокола, а Ева как подслушивающий. Квантовое распределение ключей основано на том, что Ева не может извлечь никакой информации из квантовых состояний, передаваемых от Алисы к Бобу, не нарушив их состояние. Во-первых, согласно теореме о невозможности копирования, Ева не может копировать квантовое состояние, подготовленное Алисой. Во-вторых, невозможно различить два неортогональных квантовых состояния, так как извлечение информации сопровождается возмущением сигнала или шумом. Проверяя переданные состояния на предмет нарушения, Алиса и Боб получают верхнюю оценку любого шума и подслушивания. Квантовые протоколы распределения ключа можно разделять:

- по методу кодирования;
- по квантово-механическим принципам, лежащим в основе безопасности данного протокола.

Классические квантовые протоколы распределения ключей включают 3 этапа выполнения [1]:

- генерация первичных ключей через передачу квантовых состояний по квантовому каналу и дальнейших измерений на приемной стороне. Результатом измерений является строка битов, которая отличается от изначальной переданной последовательности Алисы. После получения результатов измерений производится обмен информацией через открытый классический канал связи. По окончании первой стадии у легитимных пользователей (Алиса и Боб) возникает первичный ключ;

- согласование информации (коррекция ошибок) посредством обмена классической информацией через открытый классический канал связи (например, Интернет). Принципиальное отличие этой процедуры от обычных методов коррекции ошибок в классической теории информации состоит в том, что вся информация, передаваемая по открытому каналу связи, считается известной подслушивателю, коррекция проводится между пространственно удаленными пользователями;
- усиление секретности очищенного ключа. После коррекции ошибок и отбрасывания части битов у легитимных пользователей остается битовая строка меньшей длины. Информация подслушивающего может быть уменьшена до экспоненциально малой величины по выбранному параметру секретности путем сжатия (хеширования универсальными хеш-функциями).

Метод квантового шифрования QSC (Quantum Stream Cipher)

Квантовое шифрование — новое направление в квантовой криптографии, которое основывается на квантовом детектировании и теории передачи квантовой информации. Метод был предложен учеными из Северо-Западного университета США в 2000-х годах и известен как шифрсистема AlphaEta [2—3]. С использованием секретного ключа, который определяет квантовые состояния, соответствующие разным битовым последовательностям, пользователи могут применять соответствующие оптимальные квантовые измерения для расшифрования данных. Основная идея квантового шифрования — использование общего ключа для определения набора квантовых сигналов. Общий секретный ключ является неотъемлемой частью протоколов на основе квантового шифрования, результатом работы протоколов могут быть безопасно переданные данные. Таким образом, современные методы квантовой криптографии могут обеспечивать как процедуры распределения ключа, так и процедуру шифрования, тем самым возможно обеспечивать полный цикл защищенного информационного обмена, используя только квантово-механические преобразования.

СПИСОК ЛИТЕРАТУРЫ:

1. *Hirota O., Kato K., Sohma M., Usuda T. S., Harasawa K.* Quantum Stream Cipher Based on Optical Communications. Tokyo: Research Center for Quantum Information Science, Tamagawa University.
2. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. М.: МИР, 2006.
3. *Yuen H. P., Corndorf E., Eguchi T., Kumar P.* Quantum Noise Randomized Ciphers. Evanston: Center for Photonic Communication and Computing Department of Electrical Engineering and Computer Science Northwestern University, 2006.

Е. И. Гончаров

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ШЛЮЗОВ ДЛЯ ВЗАИМОДЕЙСТВИЯ МЕЖДУ СИСТЕМАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАЗНОГО КЛАССА

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказом ФСТЭК России ФСБ России Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» [1] установлены правила в отношении порядка обработки и обеспечения конфиденциальности персональных