УДК 003.26

И.С. Слонкина, А.И. Пестунов

Новосибирский государственный университет экономики и управления

ИНТЕРАКТИВНЫЙ ИНТЕРНЕТ-ТРЕНАЖЕР ПО КВАНТОВОЙ КРИПТОГРАФИИ

Представлен проект интерактивного Интернет-тренажера для изучения основных физических принципов квантовой криптографии и протоколов квантовой криптографии. Тренажер предлагает обучающемуся участнику несколько сценариев задач, в ходе которых он должен правильно смоделировать те или иные шаги протокола.

Ключевые слова: квантовая криптография, интерактивный тренажер, квантовый протокол.

Введение

В настоящее время многие организации занимаются исследованиями в области протоколов квантового распределения ключей. С 1984 г. (год создания Чарльзом Беннетом первого протокола квантовой криптографии – протокола BB84) создано более десятка QKD-протоколов, основанных на физических принципах [1]. На основе некоторых из них практически реализованы работающие квантовые каналы и сети связи исследовательского и коммерческого назначения. С развитием квантовых криптографических систем развиваются и атаки на них. Согласно [2,3], протоколы квантовой криптографии имеют доказанную стойкость, в отличие от классических протоколов, стойкость которых основана на вычислительной сложности. При этом особенности квантовых протоколов допускают целый ряд специфичных атак. Системы квантового распределение ключей постепенно становятся неотъемлемой частью информационной безопасности (примером можно считать запуск квантового канала связи Газпромбанком в 2016 году), поэтому обучение студентов принципом квантовой криптографии становится все более актуальным.

1. Структура приложения

Основными требованиями к проектируемому приложению является его интерактивность и наглядность представления функционирования квантовых

каналов связи. Для реализации используется библиотека three.js на языке JavaScript. Данные для заданий (например, используемые одним из участников базисы) должны генерироваться случайно для каждой попытки решения задания. Во избежание подмены результатов игры основная проверка решения проводится на серверной стороне.

В приложении представлен ряд заданий по протоколам квантового распределения ключей, объединенных в основные категории по физическим принципам, на которых основан представленный в них протокол, и, затем, в подкатегории в зависимости от протокола, к которому они относятся. Также существуют подкатегории, в которых представлены задания на понимание физических принципов квантовой криптографии. Подкатегории в рамках категории упорядочены в виде дерева. Подкатегории, включающие модификации протоколов связаны с подкатегориями, включающими исходные протоколы, которые, в свою очередь, связаны с подкатегориями, представляющие физические принципы.

Каждое задание в системе предваряется теоретической частью, включающей сведения, необходимые для выполнения задания. При решении задания участник выполняет действия либо одной из формирующих общий ключ сторон, либо злоумышленника. В частности, участник управляет моделями определенных устройств (источников фотонов, поляризационных фильтров, измерительных базисов), дает ответы на вопросы (например, о возможных результатах детектирования одного из пары запутанных фотонов на определенном измерительном базисе при известном значении детектирования другого), выполняет различные действия (перемешивание, сравнение контрольных сумм) и математические операции с промежуточными результатами (например, подсчет QBER). Планируется реализовать возможность полной симуляции канала связи, когда участник взаимодействует не с проверяющей системой, а с другим участником.

2. Представленные протоколы

Основу приложения составляют протоколы, основанные на кодировании квантового состояния одиночной частицы (принципа неопределенности Гейзенберга), эффекте квантового запутывания и когерентных состояниях. К первой категории относятся протоколы BB84, BB92 (модификация BB84), SSP, SARG04, KMB09, S13, ко второй – E91, DPS, к последней – COW.

В приложении смоделирован ряд атак на QKD-системы, например, атака «человек посередине» или перехват фотонов, расщепление луча (PNS) –

перехват «лишних» фотонов, излучаемых генераторами сторон обмена, «trojan-horse» - определение поляризации устройства, «Faked States» - атака, основанная на измерении времени смены измерительного базиса устройством, а также способы коррекции ошибок и обнаружения злоумышленника, например, подсчет QBER и противодействия атакам [4].

3. Примеры заданий

Задание 0. Понятие кет- и бра- векторов. Выполнение над векторами операции эрмитова сопряжения [5].

Задание 1. В теоретической части описываются основные используемые в протоколе понятия (например, базис, взаимнонесмещенность) и сам протокол до момента формирования сырого ключа; производится демонстрация его работы. В практической части участник должен самостоятельно выбрать подходящие базисы для Алисы и Боба, назначить 0 и 1 для базисов и наблюдать за поляризацией и измерением фотонов сторонами. Во время отправки фотонов он должен выбирать результат измерения (0, 1 или равновероятно). Из всех измерений участнику необходимо выбрать подходящие для формирования ключа (с одинаковыми базисами Алисы и Боба). Если ключ верен, задание считается решенным.

Задание 2. В теоретической части описывается сущность атаки «человек посередине». В практической части участник выполняет эту атаку: перехватывает и измеряет фотоны Алисы, отправляет Бобу собственные поляризованные фотоны, узнает базисы, использованные Алисой и Бобом, делает вывод о сформированных Алисой и Бобом ключах (различных), перехватывает, расшифровывает и зашифровывает сообщения.

Задание 3. В теоретической части описывается простейший способ обнаружения «человека посередине». В практической части участник «играет» за Боба: измеряет получаемые от Алисы фотоны выбранными базисами, обменивается с Алисой информацией о базисе и определяет наличие злоумышленника, сверяя значения выбранных измерений с Алисой

Задание 4. В теоретической части описывается способ коррекции ошибок путем многократного перемешивания последовательности, разбиения ее на блоки и подсчет контрольных сумм. Блоки с обнаруженной ошибкой разбиваются на еще меньшие блоки, пока ошибка не будет локализована в блоке минимальной длины и отброшена вместе с ним. В практической части участнику выдается «сырой ключ» и размер отбрасываемого блока. Сравнивая

собственные контрольные суммы с контрольными суммами, полученными от Алисы, он должен сформировать ключ, полностью идентичный ключу Алисы.

Задание 5. В теоретической части описывается атака путем перехвата сдвоенных фотонов и способы противостояния ей. В практической части участник реализует данную атаку: перехватывает и измеряет поляризацию «сдвоенных» фотонов (в данном задании около 70% от ключа), узнает сведения об использованных фильтрах, восстанавливает часть ключа и расшифровывает некоторое сообщение.

Задание 6. В теоретической части описывается атака Trojan horse. В практической части участник играет роль «злоумышленника»: узнает базисы, используемые Алисой, применяет аналогичные базисы, определяет поляризации фотонов Алисы, отправляет аналогично поляризованные фотон Бобу, вычисляет ключ, расшифровывает передаваемое сообщение.

Задание 6. В теоретической части описывается способ вывода из строя одного из детекторов. В практической части участник должен реализовать подобную атаку: взять под управление детектор Боба, измерять фотоны Алисы и выбирать результат измерений Боба в соответствии с ними.

Задание 7. Задание выполняют два (Алиса и Боб) или три (Алиса, Боб и Ева) участника. Задачей Алисы и Боба является формирование общего (одинакового) секретного ключа, неизвестного злоумышленнику, задача Евы состоит в перехвате ключа. Алиса и Боб могут выбирать необходимую комплектацию своих устройств, договариваться о параметрах системы, выполнять различные действия с сырым ключом. Ева знает комплектацию их устройств наряду с параметрами и может выбирать средства атаки.

Литература

1. Mosca M., Stebila D., Ustaoglu B. Quantum Key Distribution in the Classical Authenticated Key Exchange Framework // Cryptology ePrint Archive, 2012.

2. Singh H., Gupta D., Singh A. Quantum Key Distribution Protocols: A Review // IOSR J. Computer Engineering. Vol. 16, No. 2. Pp. 1-9.

3. Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. Квантовая криптография. Учебное пособие // МГУ им. М.В. Ломоносова.

4. Aggarwal R., Sharma H., Gupta D. Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol. International Journal of Computer Applications (0975-8887). 2011. Vol. 20, No. 8.

5. М. Л. Золотарев. Математический аппарат квантовой теории. Учебно-методическое пособие // Кемерово, 2006.