О СТРАТЕГИЯХ ПРЕХВАТА В ДВУХКАНАЛЬНОЙ СИСТЕМЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА

С.Г.Скобля

Барановичский государственный университет,
кафедра информационных систем и технологий
ул. Королика 8, Барановичи, Республика Беларусь
телефон: + (37529) 790-17-23; e-mail: skoblia@tut.by

Рассмотрены некоторые стратегии перехвата формируемой ключевой последовательности в двухканальной системе квантового формирования ключа, при прослушивании не всей формируемой последовательности, определена наиболее выгодная для злоумышленника стратегия прослушивания, обоснована возможность обнаружения злоумышленника при неполном прослушивании только одного из каналов.

Ключевые слова – двухканальная система квантового распределения ключа, квантовое распределение ключа, перехват ключа, стратегия злоумышленника.

1 ВВЕДЕНИЕ

Одним из интенсивно развивающихся направлений в современной криптографии является квантовая криптография. Это относительно молодое направление зародилось в конце двадцатого века во многом благодаря публикации Ч. Беннета и Г. Брассара «Квантовая криптография: квантовое распределение ключа и подбрасывание монеты» [1]. В этой работе был описан первый протокол квантового распределения ключа, названный позднее протоколом BB84. Этот протокол стал классическим квантовокриптографическим протоколом и, несмотря на то, что позднее были предложены и другие протоколы, описанный в [1] способ формирования ключа широко используется как в лабораторных, так и в промышленных установках.

Одним из недостатков протокола BB84 является потеря в силу алгоритмических особенностей, в среднем, 50% переданных бит ещё до начала этапа коррекции ошибок.

В [2] предложена двухканальная система квантового формирования ключа (далее – двухканальная система) и особый протокол его формирования, имеющие некоторые преимущества перед BB84. Позднее была описана математическая модель двухканальной системы, однако случаи прослушивания злоумышленником только части формируемой ключевой последовательности достаточно подробно рассмотрены не были.

2 КРАТКОЕ ОПИСАНИЕ ДВУКАНАЛЬНОЙ СИСТЕМЫ

В двухканальной системе квантового формирования ключа передающая сторона (Алиса) каждый бит передаёт по двум квантовым каналом одновременно. Базис, в котором передается бит по первому каналу, выбирается случайным образом. Базис, в котором передается этот же бит по второму каналу, выбирается противоположным базису первого канала для данного бита.

Принимающая сторона (Боб) регистрирует фотоны, в которых закодированы биты ключа, выбирая базисы случайным образом, но одинаковыми для двух каналов. Таким образом, если базис Боба не совпадает с базисом, использованным Алисой, для первого канала, он будет совпадать с базисом, использованным Алисой для второго канала. Как следствие, после оглашения использованных сторонами базисов, Алиса и Боб могут сформировать ключ, в который войдут все переданные биты (в случае идеальных приемной и передающей установок), т.е. потери 50% передаваемых бит, как в протоколе BB84 не произойдет.

При перехвате ключа злоумышленником (Евой) в формируемый ключ вносится некоторое количество ошибок, которое в общем случае зависит от стратегии прослушивания. По наличию ошибок в ключе Алиса и Боб могут сделать вывод о наличии прослушивания.

3 ПАРАМЕТРЫ ДВУХКАНАЛЬНОЙ СИСТЕМЫ ПРИ НЕПОЛНОМ ПРОСЛУШИВАНИИ КЛЮЧА ЗЛОУМЫШЛЕННИКОМ

При рассмотрении случаев перехвата формируемой ключевой последовательности будем исходить из того, что злоумышленник обладает техническими ресурсами, не уступающими по возможностям ресурсам, используемым сторонами, формирующими ключ.

Основными частными случаями неполного прослушивания формируемого ключа в двухканальной системе являются следующие случаи:

1. Злоумышленник прослушивает часть формируемой последовательности, таким образом, что из n передаваемых бит, прослушиваются m бит одновременно в двух каналах. Прием осуществляется Евой с помощью установки аналогичной приемной установке Боба (базисы выбираются случайными, но одинаковыми для двух каналов), а пересылка фотонов Бобу осуществляется с помощью установки, аналогичной передающей установке Алисы (базисы в двух каналах противоположны).

2. Ева прослушивает m бит из n, но только в одном канале. Приемная и передающая установки Евы аналогичны приемным и передающим установкам для одноканальной системы, использующей тот же принцип кодирования бит.

В первом случае количество ошибок Боба, вносимых Евой в прослушиваемый фрагмент ключа, будет состав-

лять D_{Bm}=0,25m, а количество информации, которое получит в этом случае Ева после оглашения базисов, составит I_{Em}=4D_{Bm}=m. Соответственно, при длине ключа n, доля ошибок в сыром ключе составит

$$D_B = 0{,}25\frac{m}{n}, \quad (1)$$

а доля бит ключа, известных Еве

$$I_E = \frac{m}{n}. \quad (2)$$

Во втором случае количество ошибок, вносимых Евой в прослушиваемый фрагмент, будет равно D_{Bm}=0,25m, а количество бит прослушиваемого фрагмента, которые станут известны Еве после оглашения базисов I_{Em}=2D_B=0,5m. Однако ввиду того, что, в среднем, в 50% бит прослушиваемой Евой последовательности войдут в сырой ключ Боба после оглашения базисов, доля ошибок в сыром ключе составит

$$D_B = 0{,}125\frac{m}{n}, \quad (3)$$

а доля бит ключа, известных Еве

$$I_E = 0{,}25\frac{m}{n}. \quad (4)$$

Рассмотрим более общий случай, когда при длине прослушиваемой последовательности m (m<n), первым способом прослушивается k бит из m, а вторым – оставшиеся m-k. В этом случае доля ошибок в сыром ключе Боба с учетом (1) и (3) составит:

$$D_B = 0{,}25\frac{k}{n} + 0{,}125\frac{m-k}{n}. \quad (5)$$

Доля бит сырого ключа, которые станут достоверно известны Еве, после оглашения базисов, с учетом (2) и (3) будет равно:

$$I_E = \frac{k}{n} + 0{,}25\frac{m-k}{n} \quad (6)$$

Выразив из (5) m и подставив в (6) получим:

$$I_E = \frac{1}{2n}(k + 4nD_B) \quad (7)$$

Легко заметить, что использование такой стратегии с точки зрения максимизации информации, получаемой Евой, не даст Еве никаких преимуществ, т.к. I_E будет иметь максимально возможное значение при k=m, т.е. когда на всем подмножестве m прослушиваются оба канала.

4 ОСНОВНЫЕ ВЫВОДЫ

На основании изложенного выше можно заключить, что:

1. Зависимость количества информации Евы от количества ошибок Боба при обеих стратегиях перехвата линейна, что следует учитывать при принятии решения о возможности использования сформированного сырого ключа после процедуры коррекции ошибок, в процессе которой количество информации, известной Еве увеличится.

2. С точки зрения максимизации получаемой информации о ключе, Еве более выгодно прослушивать оба канала одновременно.

3. При фиксированном количестве ошибок в сыром ключе, обусловленных наличием прослушивания злоумышленником, более выгодной стратегией прослушивание для Евы также является прослушивание двух каналов одновременно, т.к. по сравнению с прослушиванием одного канала количество получаемой Евой информации будет в два раза большим.

4. Несмотря на то, что стратегия, при которой осуществляется прослушивание части формируемой ключевой последовательности только в одном из каналов двухканальной системы, является менее выгодным для Евы, с точки зрения количества получаемой информации о ключе, её использование может быть вполне оправданным, с учетом того, что для перехвата можно использовать более простую установку. При этом, если прослушивается вся формируемая ключевая последовательность, Еве после оглашения базисов будет известно, в среднем, 25% бит ключа, а количество ошибочных бит в ключе Боба, обусловленных наличием прослушивания составит 12,5%.

5. Двухканальная система позволяет обнаруживать злоумышленника при полном либо неполном прослушивании только одного канала двухканальной системы по ошибкам, которые возникают в формируемой ключевой последовательности, вследствие наличия злоумышленника.

6. При прослушивании двух каналов одновременно злоумышленнику нет необходимости использовать квантовую память. Стратегия прослушивания одного канала при наличии у злоумышленника квантовой памяти требует отдельного исследования.

ЛИТЕРАТУРА

[1] Bennet, C. H. Quantum cryptography: quantum key distribution and coin tossing / C.H. Bennet, G, Brassard // Int. conf. on computers systems ans signal processing. Bangalore. India. - 1984. P.175-179.

[2] Голиков, В.Ф. Способ кодирования и передачи квантового ключа // В.Ф. Голиков, С.Г. Скобля // Заявка на получение патента. Номер 20080283 от 12.03.2008.