АНАЛИЗ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Кузнецова А.В.
Научный руководитель: д-р техн. наук, проф. Василиу Е.В.
Одесская национальная академия связи им. А.С. Попова, Украина
E-mail: kuznetsova__anna@hotmail.com

Аннотация — Выполнен сравнительный анализ стойкость и эффективности двух протоколов квантового распределения ключей: протокола BB84 и протокола с шестью состояниями. Выяснено, что протокол с шестью состояниями является более стойким к атакам, однако имеет существенно меньшую эффективность.

1. Введение

Квантовая криптография является достаточно новым направлением защиты информации, которое, основываясь на законах квантовой физики, исключает попытки злоумышленника завладеть информацией [1]. Направлением квантовой криптографии, которое уже имеет практическую реализацию, является квантовые протоколы распределения ключей (КПРК).

В докладе на примере двух КПРК: *BB*84 и протокола с шестью состояниями рассматривается возможность повышения криптографической стойкости протокола за счет увеличения количества квантовых состояний фотонов.

2. Основная часть

Как известно, в протоколе *BB*84 используются 4 квантовых состояния фотонов. Это может быть направление поляризации, которое выбирается в зависимости от значения передаваемого бита (90° или 135° для бита «1», 0° или 45° для бита «0») [1]. Соответственно, число случаев, в которых выбранные базисы будут совпадать у участников протокола, будет составлять, в среднем, половину длины исходной последовательности. В результате после передачи ключа, в случае отсутствия помех и искажений, будут правильно зарегистрированы состояния примерно 50 % фотонов.

В случае же протокола с шестью состояниями добавляется еще один базис, а именно состояния:

$$|0_c\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right);$$
$$|1_c\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right).$$

Это еще два направления поляризации для переданного фотона: левая круговая и правая круговая. Таким образом, понижается и вероятность угадывания базисов злоумышленником.

Но стоит отметить, что после передачи ключа, будут правильно зарегистрированы состояния только 33 % фотонов.

На рис. 1 показаны кривые зависимости взаимной информации от уровня ошибок *D*, вносимых атакой злоумышленника, для когерентной и некогерентной атак на протоколы *BB*84 и с шестью состояниями [2]. Из графика видно, что кривые для протокола с шестью состояниями лежат ниже соответствующих кривых для протокола *BB*84, что говорит о большей стойкости протокола с шестью состояниями к различного рода атакам.

Однако скорость передачи ключа в протоколе с шестью состояниями является значительно меньшей, поскольку его средняя эффективность равна 1/3, в то время как для *BB*84 она равна 1/2.

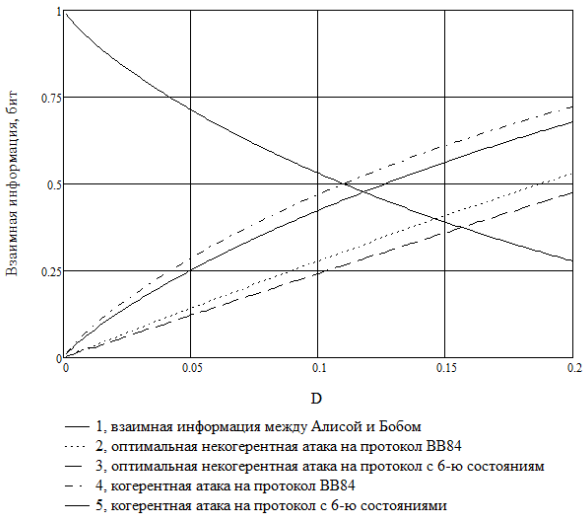

Рис. 1

3. Заключение

Таким образом, повышение стойкости КПРК путем увеличения числа поляризационных базисов и соответственно используемых состояний, приводит в то же время и к нежелательному последствию: уменьшению количества правильно принятых фотонов и соответственно уменьшению скорости передачи ключа.

При высокой степени секретности передаваемой информации потерями в скорости передачи можно пренебречь. Соответственно протокол с шестью состояниями, обеспечивающий несколько более высокую стойкость к атакам, в данном случае предпочтительнее протокола *BB*84.

4. Список литературы

[1] Кузнецова А.В. Квантовые технологии защиты информации // Сборник тезисов «Інфокомунікації – сучасність та майбутнє». — 2012. — Ч. 1. — С. 16 — 18.

[2] Василиу Е.В. Стойкость квантовых протоколов распределения ключей типа «распределение-измерение»/ Е.В. Василиу // Georgian Electronic Scientific Journal: Computer science and telecommunications. — 2007. — № .2(13). — С. 50 — 62.

EFFECTIVENESS ANALYSIS OF THE QUANTUM KEY DISTRIBUTION PROTOCOLS USING

Kuznetsova A.V.
Scientific adviser: Vasiliu E.V.
Odessa National Academy of Telecommunications named after O.S. Popov, Ukraine

Abstract — A comparative analysis of the stability and effectiveness of two quantum key distribution protocols: BB84 protocol and the six-states protocol, is executed. The results show that the six-state protocol is more resistant to attacks, but has a much lower efficiency.