2008 Математические методы криптографии № 2(2)

DOI 10.17223/20710410/2/13

УДК 518.6+681.3

АНАЛИЗ АТАК НА КВАНТОВЫЙ ПРОТОКОЛ ПЕРЕДАЧИ КЛЮЧА

В.Г. Скобелев

Институт прикладной математики и механики НАН Украины, г. Донецк

E-mail: skbv@iamm.ac.donetsk.ua

Исследуется вычислительная стойкость квантового протокола передачи ключа в предположении, что криптоаналитик управляет вероятностями выбора базисных векторов для измерения кубита, а также одновременным изменением базисов отправителя и адресата.

***Ключевые слова*:** *квантовая криптография*, *криптоанализ*, *активная атака*, *квантовый протокол передачи ключа.*

Применение квантовых вычислений к решению задач криптологии [1, 2] обосновывает актуальность исследования вычислительной стойкости квантовых алгоритмов. Возникает вопрос: что и как подвергается атаке? Сложность состоит в том, что в настоящее время недостаточно проработана формальная модель квантового компьютера, а искажение передаваемой информации за счет ее измерения приводит к новым типам атак, представляющим собой симбиоз пассивных и активных атак [3]. Поэтому естественно исследовать вычислительную стойкость квантовых алгоритмов решения конкретных, модельных задач криптологии. В настоящей работе в качестве такой задачи выбран анализ атак на классический квантовый протокол передачи ключа [4, 5].

Структура работы следующая: в п. 1 введены основные понятия и дана постановка задачи; в п. 2 исследуется атака на квантовый протокол передачи ключа в предположении, что криптоаналитик управляет только вероятностями выбора базисных векторов для измерения кубита. В п. 3 исследуется усиление этой атаки при условии, что криптоаналитик также может управлять одновременным изменением базисов отправителя и адресата. Заключение содержит ряд выводов.

1. Основные понятия и постановка задачи

Пусть $B = \{\boldsymbol{e}_0, \boldsymbol{e}_1\}$ − ортонормированный базис в 2-мерном комплексном векторном пространстве H. Кубит − это физическая система, состояние которой представлено вектором $|\xi\rangle = \lambda_0\boldsymbol{e}_0 + \lambda_1\boldsymbol{e}_1$, где $\lambda_0, \lambda_1 \in \mathbf{C}$ ($|\lambda_0|^2 + |\lambda_1|^2 = 1$). При измерении в базисе B кубит переходит в базисное состояние $\boldsymbol{e}_i$ ($i = 0, 1$) с вероятностью $|\lambda_0|^2$. В [4, 5] предложен следующий квантовый протокол передачи ключа (рис. 1, *а*).

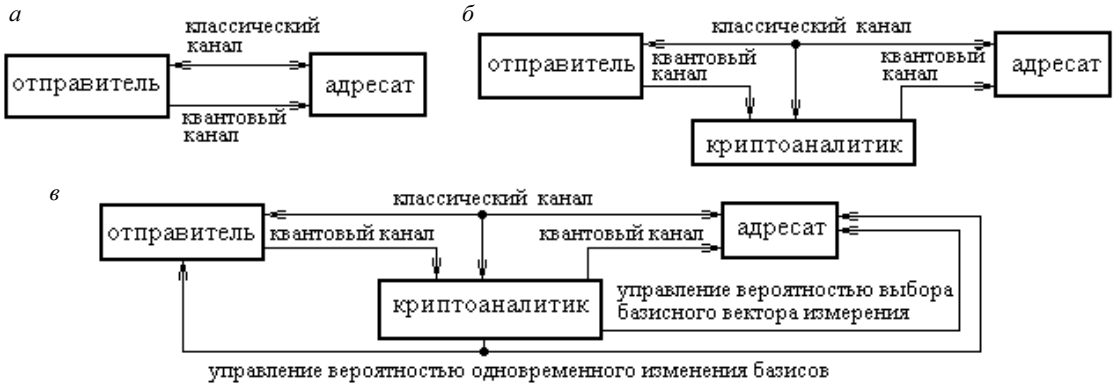

Рис. 1. Квантовый протокол передачи ключа: *а* – передача ключа при отсутствии атаки; *б* – передача ключа при классической атаке; *в* – передача ключа при исследуемых атаках

Отправитель и адресат располагают квантовым и классическим каналами: 1-й применяется для передачи ключа последовательностью кубитов, а 2-й − для контроля вычислений. Пусть $B_j = \{\boldsymbol{e}_0^{(j)}, \boldsymbol{e}_1^{(j)}\}$ ($j = 0, 1$) − такие ортонормированные базисы, что $\boldsymbol{e}_i^{(1)} = 2^{-0,5}(\boldsymbol{e}_0^{(0)} + (-1)^{1+i}\boldsymbol{e}_1^{(0)})$ ($i = 0, 1$). Значение i ($i = 0, 1$) бита кодируется в базисе B_j ($j = 0, 1$) вектором $\boldsymbol{e}_i^{(j)}$. Для каждого бита и отправитель и адресат случайным образом выбирают базис B_0 или B_1. По завершении процесса передачи последовательности отправитель и адресат со-

общают друг другу по классическому каналу, какие базисы были выбраны для кодирования и измерения каждого бита. Те биты, для которых базисы согласованы − ключ. Остальные биты отбрасываются. Доказано, что в среднем длина ключа составляет 50 % длины переданной последовательности.

Классическая атака на этот протокол состоит в следующем. Криптоаналитик перехватывает, измеряет передаваемые кубиты и пересылает измеренные кубиты адресату. Кроме того, криптоаналитик прослушивает классический канал (рис. 1, *б*). Доказано, что адресат в среднем верно измерит только 50 % от длины ключа. Поэтому, сравнив по открытому каналу некоторое число бит ключа, отправитель и адресат с соответствующей вероятностью обнаружат атаку. Отметим, что, хотя об этом нигде явно не сказано, такая атака основана на предположении о том, что адресат и криптоаналитик используют для измерения каждого кубита в каждом базисе B_j ($j = 0, 1$) один и тот же фиксированный базисный вектор $\boldsymbol{e}_i^{(j)}$.

Рассмотренная выше атака предполагает, что в распоряжении криптоаналитика имеется минимум средств. Усилим эту атаку за счет следующих предположений (рис. 1, *в*):

Предположение 1. Для измерения перехваченного кубита в базисе B_j ($j = 0, 1$) криптоаналитик выбирает базисный вектор $\boldsymbol{e}_i^{(j)}$ ($i = 0, 1$) с вероятностью $p_1^{(j)}(i)$.

Предположение 2. Криптоаналитик определяет вероятность $p_2^{(j)}(i)$ ($i, j \in \{0, 1\}$) выбора адресатом базисного вектора $\boldsymbol{e}_i^{(j)}$ при измерении кубита в базисе B_j, причем адресат не располагает информацией о том, что у него произошло изменение базисного вектора.

Предположение 3. Криптоаналитик может одновременно изменять у отправителя и адресата базис B_j ($j = 0, 1$) на базис B_{1-j} с вероятностью $p_0(j)$, причем ни отправитель, ни адресат не располагают информацией о том, что у них произошло изменение базиса.

Из предположений 1 и 2 вытекает, что $p_k^{(j)}(1 - i) = 1 - p_k^{(j)}(i)$ для всех $i, j \in \{0, 1\}$ и $k \in \{1, 2\}$.

2. Атака при управлении вероятностями выбора базисных векторов для измерения кубита

Рассмотрим атаку на квантовый протокол передачи ключа, определяемую предположениями 1 и 2.

Пусть $P_{jhj}^{(i)}$ ($i, h, j \in \{0, 1\}$) − вероятность правильного считывания адресатом значения i-го бита при условии, что для данного кубита отправитель и адресат используют базис B_j, а криптоаналитик − базис B_h. Из анализа процесса передачи бита при согласованных базисах отправителя и адресата, представленного на рис. 2 и 3, вытекает

Теорема 1. Истинны равенства

$$P_{jjj}^{(i)} = 1 - p_2^{(j)}(i) + p_1^{(j)}(i) \cdot p_2^{(j)}(i) \quad (j = 0, 1),$$

$$P_{j,1-j,j}^{(i)} = 0{,}75 - 0{,}5\, p_2^{(j)}(i) \quad (j = 0, 1).$$

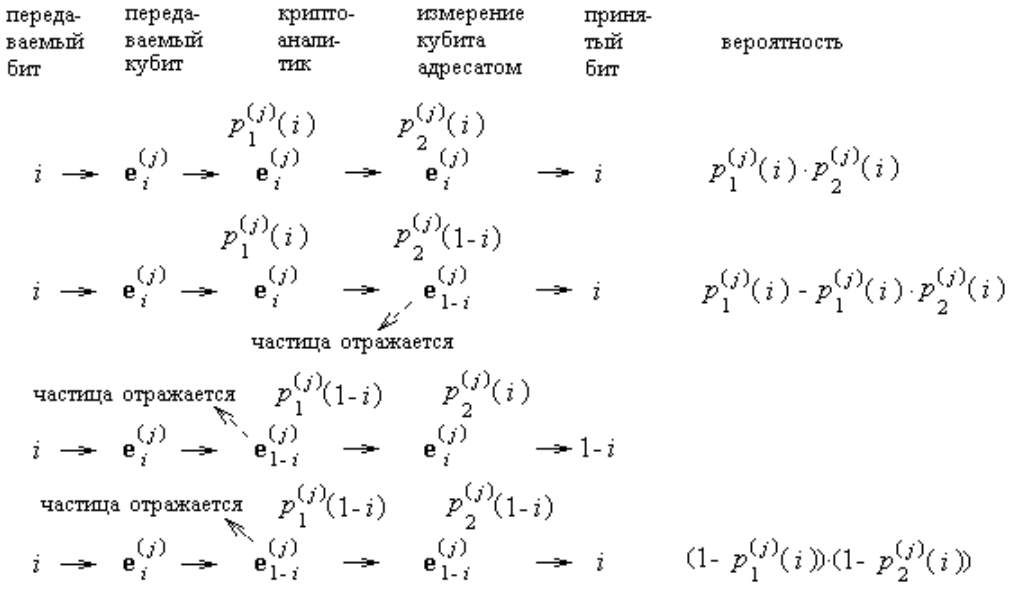

Рис. 2. Процесс передачи значения i ($i = 0, 1$) бита при условии, что для данного кубита отправитель, криптоаналитик и адресат используют базис B_j ($j = 0, 1$)

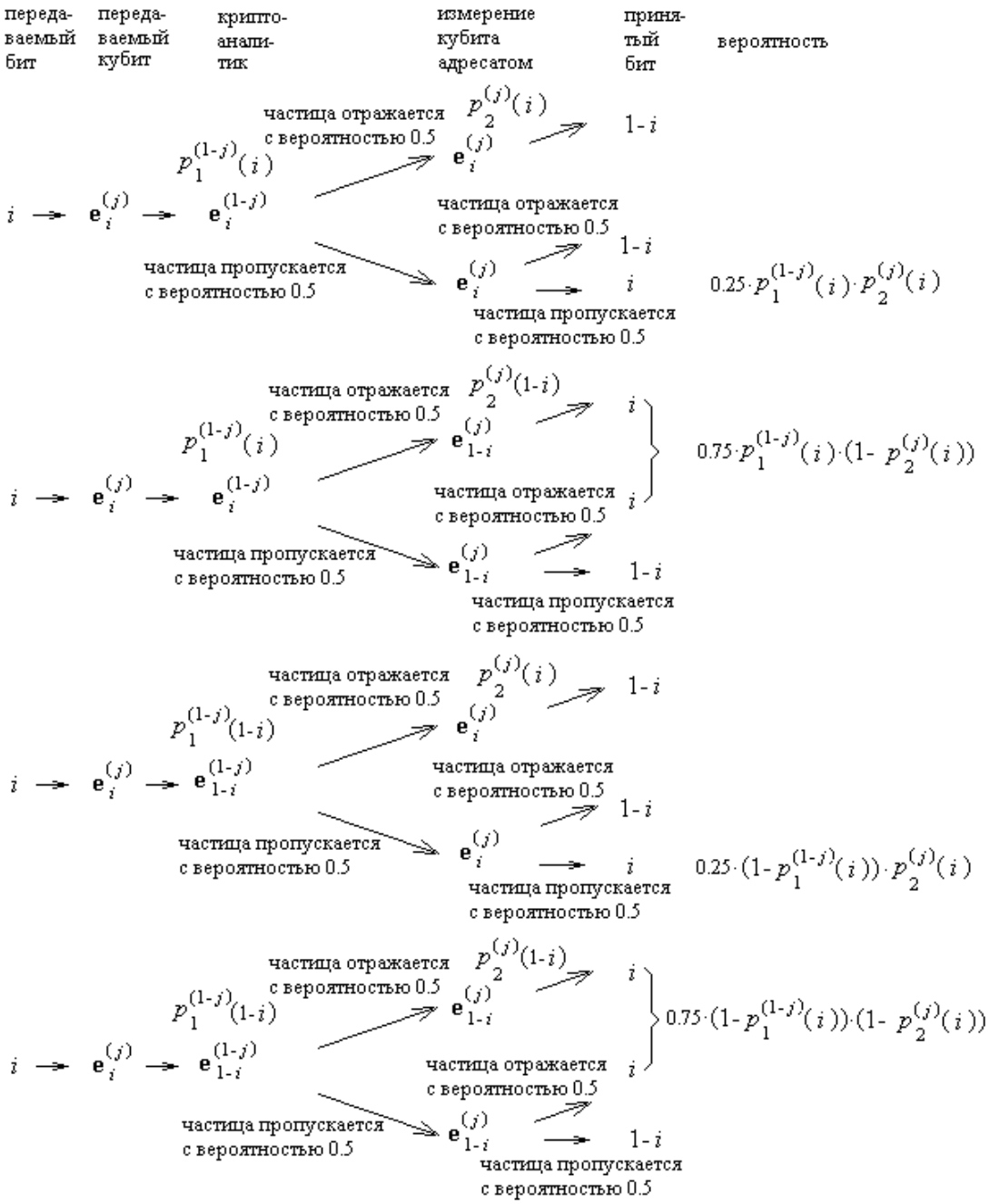

Рис. 3. Процесс передачи значения i (i = 0, 1) бита при условии, что для данного кубита отправитель и адресат используют базис B_j (j = 0, 1), а криптоаналитик − базис B_{1-j}

Обозначим через $P_{jhj}(\alpha)$ ($j, h \in \{0, 1\}$, $\alpha \in [0, 1]$) вероятность правильного считывания адресатом значения бита при условии, что для данного кубита отправитель и адресат используют базис B_j , криптоаналитик − базис B_h, а вероятность пересылки символа 0 отправителем равна α. Из теоремы 1 вытекает

Теорема 2. Для всех $\alpha \in [0 , 1]$ истинны равенства

$$P_{jjj}(\alpha) = 1 - p_1^{(j)}(0) + p_1^{(j)}(0) \cdot p_2^{(j)}(0) + \alpha\,(p_1^{(j)}(0) - p_2^{(j)}(0))\ \ (j = 0, 1); \tag{1}$$

$$P_{j,1-j,j}(\alpha) = 0{,}25 + 0{,}5\alpha + (0{,}5 - \alpha) \cdot p_2^{(j)}(0)\ \ (j = 0, 1). \tag{2}$$

Отметим ряд следствий из равенства (1).

I. Пусть $p_2^{(j)}(0) = 0{,}5$ (j = 0, 1). Тогда

$$P_{jjj}(\alpha) = 1 - (0{,}5 - \alpha) \cdot p_1^{(j)}(0) - 0{,}5\alpha\ \ (j = 0, 1). \tag{3}$$

При этом из (3) вытекает, что для всех $\alpha \in [0, 1]$

$$P_{jjj}(\alpha) = \begin{cases} 1-0,5\cdot\alpha, & \text{если } p_1^{(j)}(0)=0 \\ 0,5\cdot(1+\alpha), & \text{если } p_1^{(j)}(0)=1 \end{cases} \quad (j=0,\,1).$$

II. Пусть $p_1^{(j)}(0) = p_2^{(j)}(0) = p^{(j)}(0)$ $(j = 0, 1)$. Тогда

$$P_{jjj}(\alpha) = 1 - p^{(j)}(0) + (p^{(j)}(0))^2 \quad (j=0,\,1), \tag{4}$$

т. е. вероятность $P_{jjj}(\alpha)$ не зависит от вероятности α. Из (4) вытекает, что $P_{jjj}(\alpha) \in [0{,}75,\,1]$ $(j = 0, 1)$ для всех $p^{(j)}(0) \in [0;1]$, причем

$$P_{jjj}(\alpha) = \begin{cases} 0,75, & \text{если } p^{(j)}(0)=0,5 \\ 1, & \text{если } p^{(j)}(0)\in\{0;1\} \end{cases} \quad (j=0\,,\,1)\,.$$

III. Пусть $p_1^{(j)}(0) \neq p_2^{(j)}(0)$ $(j = 0, 1)$. Тогда

1. Для области значений вероятности $P_{jjj}(\alpha)$ $(j = 0, 1)$, как функции от вероятности α, истинно равенство

$$\mathrm{Val}\, P_{jjj}(\alpha) = [l_1, L_1] \quad (j=0,\,1),$$

где

$$l_1 = \min\{1 - p_1^{(j)}(0) + p_1^{(j)}(0)\cdot p_2^{(j)}(0),\, 1 - p_2^{(j)}(0) + p_1^{(j)}(0)\cdot p_2^{(j)}(0)\} \quad (j=0,\,1); \tag{5}$$

$$L_1 = \max\{1 - p_1^{(j)}(0) + p_1^{(j)}(0)\cdot p_2^{(j)}(0),\, 1 - p_2^{(j)}(0) + p_1^{(j)}(0)\cdot p_2^{(j)}(0)\} \quad (j=0,\,1). \tag{6}$$

2. Из (5) и (6) вытекает, что для всех значений $\alpha \in [0, 1]$, если либо $p_1^{(j)}(0) \to 0$, $p_2^{(j)}(0) \to 0$ $(j = 0, 1)$, либо $p_1^{(j)}(0) \to 1$, $p_2^{(j)}(0) \to 1$ $(j = 0, 1)$, то $l_1 \to 1$ и $L_1 \to 1$, т. е. $P_{jjj}(\alpha) \to 1$ $(j = 0, 1)$ для всех $\alpha \in [0, 1]$.

3. Вероятность $P_{jjj}(\alpha) \to 1$ $(j = 0, 1)$ − монотонная функция от вероятности α, причем $P_{jjj}(\alpha)$ монотонно возрастает, если $p_1^{(j)}(0) > p_2^{(j)}(0)$, и монотонно убывает, если $p_1^{(j)}(0) < p_2^{(j)}(0)$.

4. Пусть $p_1^{(j)}(0) \to 1$, $p_2^{(j)}(0) \to 0$ $(j = 0, 1)$. Тогда $P_{jjj}(\alpha) \to \alpha$ $(j = 0, 1)$ для всех $\alpha \in [0, 1]$.

5. Пусть $p_1^{(j)}(0) \to 0$, $p_2^{(j)}(0) \to 1$ $(j = 0, 1)$. Тогда $P_{jjj}(\alpha) \to 1 - \alpha$ $(j = 0, 1)$ для всех $\alpha \in [0, 1]$.

Отметим ряд следствий из равенства (2).

I. Вероятность $P_{j,1-j,j}(\alpha)$ $(j = 0, 1)$ вообще не зависит от вероятности выбора криптоаналитиком базисного вектора для измерения перехваченного кубита.

II. Для всех $\alpha \in [0, 1]$

$$P_{j,1-j,j}(\alpha) = \begin{cases} 0,25+0,5\cdot\alpha, & \text{если } p_2^{(j)}(0)=0 \\ 0,75-0,5\cdot\alpha, & \text{если } p_2^{(j)}(0)=1 \end{cases} \quad (j=0\,,\,1)\,.$$

III. Пусть $p_2^{(j)}(0) = 0{,}5$. Тогда $P_{j,1-j,j}(\alpha) = 0{,}5$ $(j = 0, 1)$, т. е. вероятность $P_{j,1-j,j}(\alpha)$ не зависит от α.

IV. Пусть $p_2^{(j)}(0) \neq 0{,}5$. Тогда

1. Для области значений вероятности $P_{j,1-j,j}(\alpha)$ $(j = 0, 1)$, как функции от α, истинно равенство

$$\mathrm{Val}\, P_{jjj}(\alpha) = [l_2\,,\, L_2] \quad (j=0,\,1),$$

где

$$l_2 = \min\{0{,}25 + 0{,}5\cdot p_2^{(j)}(0),\, 0{,}75 - 0{,}5\, p_2^{(j)}(0)\} \quad (j=0,\,1); \tag{7}$$

$$L_2 = \max\{0{,}25 + 0{,}5\cdot p_2^{(j)}(0),\, 0{,}75 - 0{,}5\, p_2^{(j)}(0)\} \quad (j=0,\,1). \tag{8}$$

2. Вероятность $P_{j,1-j,j}(\alpha)$ $(j = 0, 1)$ − монотонная функция от вероятности α, причем $P_{j,1-j,j}(\alpha)$ монотонно возрастает, если $p_2^{(j)}(0) < 0{,}5$, и монотонно убывает, если $p_2^{(j)}(0) > 0{,}5$.

3. Из (7) и (8) вытекает, что для всех значений $\alpha \in [0, 1]$, если $p_2^{(j)}(0) \to 0{,}5$, то $l_2 \to 0{,}5$ и $L_2 \to 0{,}5$, т. е.

$$P_{j,1-j,j}(\alpha) \to 0{,}5 \quad (j=0,\,1).$$

Пусть $P_1(\alpha)$ $(\alpha \in [0, 1])$ − вероятность правильного считывания адресатом значения бита при условии, что для данного кубита базисы отправителя и адресата согласованы, а вероятность пересылки символа 0 отправителем равна α. Тогда

$$P_1(\alpha) = 0{,}125(P_{000}(\alpha) + P_{111}(\alpha) + P_{010}(\alpha) + P_{101}(\alpha)). \tag{9}$$

Из теоремы 2 и равенства (9) вытекает

Теорема 3. Для всех $\alpha \in [0, 1]$ истинно равенство

$$P_1(\alpha) = 0{,}125(\,2{,}5 + \alpha - (1-\alpha)\cdot(p_1^{(0)}(0) + p_1^{(1)}(0)) +$$

$$+ (0{,}5 - 2\alpha)\cdot(p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0)\cdot p_2^{(0)}(0) + p_1^{(0)}(0)\cdot p_2^{(0)}(0))\,.$$

Отметим ряд следствий из равенства (9).

I. Если $p_1^{(j)}(0) \to 0$, $p_2^{(j)}(0) \to 0$ ($j = 0, 1$), то $P_1(\alpha) \to 0{,}3125 + 0{,}125\alpha$. При этом:

1) если $\alpha \to 0$, то $P_1(\alpha) \to 0{,}3125$;
2) если $\alpha \to 0{,}5$, то $P_1(\alpha) \to 0{,}3750$;
3) если $\alpha \to 1$, то $P_1(\alpha) \to 0{,}4375$.

II. Если $p_1^{(j)}(0) \to 1$, $p_2^{(j)}(0) \to 0$ ($j = 0, 1$), то $P_1(\alpha) \to 0{,}0625 + 0{,}3750\alpha$. При этом:

1) если $\alpha \to 0$, то $P_1(\alpha) \to 0{,}0625$;
2) если $\alpha \to 0{,}5$, то $P_1(\alpha) \to 0{,}2500$;
3) если $\alpha \to 1$, то $P_1(\alpha) \to 0{,}4375$.

Если $p_1^{(j)}(0) \to 1$, $p_2^{(j)}(0) \to 1$ ($j = 0, 1$), то $P_1(\alpha) \to 0{,}4375 - 0{,}125\alpha$. При этом:

1) если $\alpha \to 0$, то $P_1(\alpha) \to 0{,}4375$;
2) если $\alpha \to 0{,}5$, то $P_1(\alpha) \to 0{,}3750$;
3) если $\alpha \to 1$, то $P_1(\alpha) \to 0{,}3125$.

IV. Если $p_1^{(j)}(0) \to 0{,}5$, $p_2^{(j)}(0) \to 0{,}5$ ($j = 0, 1$), то $P_1(\alpha) = 0{,}3125$.

Проведенный анализ показывает, что значение вероятности $P_1(\alpha)$ ($\alpha \in [0, 1]$) колеблется в достаточно широких пределах, по крайней мере, в промежутке [0,2500, 0,4375], в зависимости от значений вероятностей $p_1^{(j)}(0)$, $p_2^{(j)}(0)$ ($j = 0, 1$) и α. Это означает, что криптоаналитик располагает достаточно широкими возможностями для того, чтобы существенно затруднить процесс обнаружения его действий. Действительно, если генератор последовательностей отправителя далек от псевдослучайного, то в среднем до 87,5% ключа может быть передано верно. Даже при наличии случайного генератора последовательностей у отправителя в среднем до 75% ключа может быть передано верно.

3. Атака при управлении изменением базисов отправителя и адресата

Рассмотрим теперь атаку на квантовый протокол передачи ключа, определяемую предположениями 1 – 3.

Пусть $P_2(\alpha)$ ($\alpha \in [0, 1]$) − вероятность правильного считывания адресатом значения бита при условии, что для данного кубита базисы отправителя и адресата согласованы, вероятность пересылки символа 0 отправителем равна α, а вероятность одновременного изменения криптоаналитиком у отправителя и адресата базиса B_j ($j = 0,1$) на базис B_{1-j} равна $p_0(j)$. Тогда имеет место

Теорема 4. Для всех $\alpha \in [0, 1]$ истинно равенство

$$P_2(\alpha) = 0{,}125(P_{000}(\alpha) + P_{111}(\alpha) + P_{010}(\alpha) + P_{101}(\alpha)) + \\ + (p_0(1) - p_0(0))(P_{000}(\alpha) + P_{010}(\alpha) - P_{111}(\alpha) - P_{101}(\alpha))). \qquad (10)$$

Из равенства (10) вытекает, что:

1) неравенство $P_2(\alpha) > P_1(\alpha)$ истинно тогда и только тогда, когда либо $P_{000}(\alpha) + P_{010}(\alpha) - P_{111}(\alpha) - P_{101}(\alpha) < 0$ и $p_0(1) - p_0(0) < 0$, либо $P_{000}(\alpha) + P_{010}(\alpha) - P_{111}(\alpha) - P_{101}(\alpha) < 0$ и $p_0(1) - p_0(0) > 0$;

2) равенство $P_2(\alpha) > P_1(\alpha)$ истинно тогда и только тогда, когда $P_{000}(\alpha) + P_{010}(\alpha) - P_{111}(\alpha) - P_{101}(\alpha) = 0$ или $p_0(1) = p_0(0)$.

Таким образом, показано, что дополнительная возможность криптоаналитика управлять одновременным изменением базисов отправителя и адресата может усилить его атаку на квантовый протокол передачи ключа.

Заключение

Показано, что расширение возможностей криптоаналитика за счет управления вероятностями выбора базисных векторов для измерения кубита, а также одновременным изменением базисов отправителя и адресата может значительно усилить его атаку на квантовый протокол передачи ключа. Показано, что эффективность атаки существенно зависит от генератора последовательностей, имеющегося у отправителя. Более тонкий анализ этой зависимости − одно из возможных направлений дальнейших исследований. Второе направление исследований связано с анализом зависимости вероятности $P_2(\alpha)$ от значений вероятностей $p_1^{(j)}(i)$, $p_2^{(j)}(i)$, $p_0(j)$ ($i, j \in \{0, 1\}$) и α.

ЛИТЕРАТУРА

1. *Ожигов Ю.И.* Квантовые вычисления. М.: МГУ, 2003.
2. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. М.: Мир, 2006.
3. *Алферов А.П. и др.* Основы криптографии. М.: Гелиос АРВ, 2002.
4. *Bennett C.H., Brassard G.* Quantum public key distribution system // IBM Techn. Disclosure Bulletin. 1985. V. 28. P. 3153 – 3164.
5. *Bennett C.H., Brassard G.* Quantum public key distribution reinvented. 1987. SIGACTN: SIGACT News. 18.