КИБЕРНЕТИКА

В.Г. СКОБЕЛЕВ

УДК 518.6+681.3

О ВЫЧИСЛИТЕЛЬНОЙ СТОЙКОСТИ КВАНТОВЫХ АЛГОРИТМОВ ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ

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

ВВЕДЕНИЕ

В настоящее время во всем мире ведутся интенсивные исследования в области квантовых вычислений [1–3] — нового перспективного направления современных информационных технологий. В квантовой системе для экспоненциального уменьшения времени вычислений требуется только линейное увеличение объема необходимого физического пространства. Данные исследования проводят в двух направлениях: синтез квантового компьютера; разработка квантовой теории алгоритмов.

Применение квантовых вычислений к решению задач криптологии [3–5] обосновывает актуальность рассмотрения вычислительной стойкости квантовых алгоритмов, предназначенных для преобразования информации. Возникает вопрос: что и как подвергается атаке? Сложность ответа состоит в том, что пока 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 [6]. В связи с этим актуальным является исследование вычислительной стойкости квантовых алгоритмов, предназначенных для решения модельных задач криптологии.

В настоящей работе в качестве таких задач выбран анализ атак на классический квантовый протокол передачи ключа и анализ построенного в работе квантового шифра, основанного на алгоритме плотного кодирования. В разд. 1 рассмотрен квантовый протокол передачи ключа, даны постановки задач атаки на этот протокол. В разд. 2 рассматривается атака в предположении, что криптоаналитик управляет только вероятностями выбора базисных векторов для измерения кубита, а в разд. 3 — усиление этой атаки, состоящее в том, что криптоаналитик также может управлять одновременным изменением базисов отправителя и адресата. В разд. 4 изложен алгоритм плотного кодирования и предложен шифр, построенный на его основе. В разд. 5 исследуется вычислительная стойкость этого шифра. Заключение содержит ряд выводов.

1. КВАНТОВЫЙ ПРОТОКОЛ ПЕРЕДАЧИ КЛЮЧА

Предполагается, что отправитель и адресат располагают квантовым и классическим каналами: первый применяется для передачи ключа последовательностью кубитов, второй — для контроля вычислений (рис.1).

Обозначим $\mathsf{B}_j = \{\mathbf{e}_0^{(j)}, \mathbf{e}_1^{(j)}\}$ $(j = 0, 1)$ такие ортонормированные базисы пространства H_2, что $\mathbf{e}_i^{(1)} = 2^{-0,5}(\mathbf{e}_0^{(0)} + (-1)^{1+i}\mathbf{e}_1^{(0)})$ $(i = 0, 1)$. Для передачи значения

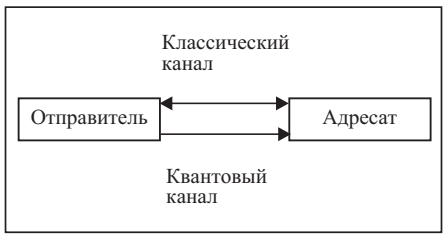

Рис. 1

очередного бита отправитель случайным образом выбирает базис B_j $(j = 0, 1)$, измеряет кубит (представляющий собой случайным образом поляризованный фотон) в этом базисе и передает измеренный кубит адресату по квантовому каналу. Для того чтобы принять значение очередного бита, адресат случайным образом выбирает базис B_j $(j = 0, 1)$, а затем измеряет принятый кубит в нем. По завершении процесса передачи последовательности битов отправитель и адресат по классическому каналу сообщают друг другу, какие базисы были выбраны для кодирования и измерения каждого бита. Биты, при обработке которых отправитель и адресат использовали один и тот же базис, принимаются в качестве ключа, а остальные отбрасываются. Доказано, что в среднем длина ключа составляет 50% длины переданной последовательности.

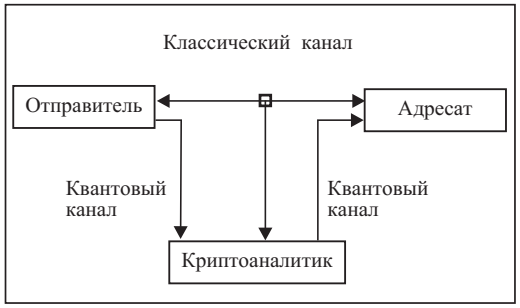

Рис. 2

Классическая атака на этот протокол состоит в следующем. Криптоаналитик перехватывает передаваемые кубиты, измеряет их, а затем пересылает адресату. Кроме того, криптоаналитик имеет возможность прослушивать классический канал (рис. 2). Доказано, что в этом случае адресат в среднем верно измерит только 50% от длины ключа. Поэтому, сравнив по открытому каналу некоторое число битов ключа, отправитель и адресат с соответствующей вероятностью обнаружат наличие атаки.

Хотя об этом нигде явно не сказано, рассмотренный анализ атаки на квантовый протокол передачи ключа основан на предположении о том, что криптоаналитик и адресат при измерении кубита в базисе B_j $(j = 0, 1)$ вычисляют его проекцию на один и тот же фиксированный базисный вектор. Ослабим это предположение, а именно: будем считать, что только отправитель в процессе передачи значения i $(i = 0, 1)$ бита, выбрав базис B_j $(j = 0, 1)$, всегда конструирует проекцию передаваемого кубита на базисный вектор $\mathbf{e}_i^{(j)}$.

Рассмотренная атака на квантовый протокол передачи ключа предполагает, что в распоряжении криптоаналитика имеется минимум средств. Усилим ее за счет следующих предположений:

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

Предположение 2. Криптоаналитик определяет вероятность $p_2^{(j)}(i)$ $(i, j \in \{0, 1\})$ выбора адресатом базисного вектора $\mathbf{e}_i^{(j)}$ 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.

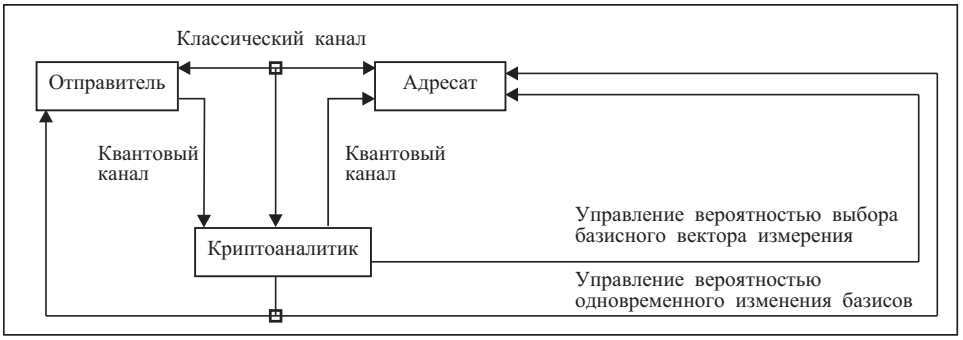

Рис. 3

Таким образом, получаем атаку на квантовый протокол передачи ключа, которая схематически представлена на рис. 3. Отметим, что из предположений 1 и 2 вытекает, что равенство

$$p_k^{(j)}(1-i) = 1 - p_k^{(j)}(i) \tag{1}$$

истинно для всех $i, j \in \{0, 1\}$ и $k \in \{1, 2\}$.

2. АТАКА ПРИ УПРАВЛЕНИИ ВЕРОЯТНОСТЯМИ ВЫБОРА БАЗИСНЫХ ВЕКТОРОВ ДЛЯ ИЗМЕРЕНИЯ КУБИТА

Исследуем атаку на квантовый протокол передачи ключа, определяемую предположениями 1 и 2. Обозначим $P_{jhj}^{(i)}$ $(i, h, j \in \{0, 1\})$ вероятность правильного считывания адресатом значения i бита при условии, что для данного кубита отправитель и адресат используют базис B_j, а криптоаналитик — базис B_h.

Лемма 1. Равенства

$$P_{jjj}^{(i)} = 1 - p_2^{(j)}(i) + p_1^{(j)}(i) p_2^{(j)}(i), \tag{2}$$

$$P_{j,1-j,j}^{(i)} = 0{,}75 - 0{,}5 p_2^{(j)}(i) \tag{3}$$

истинны для всех $i, j \in \{0, 1\}$.

Доказательство. Предположим, что при обработке очередного кубита отправитель, криптоаналитик и адресат используют один и тот же базис B_j $(j = 0, 1)$. С применением равенства (1) вычислим вероятности возможных элементарных событий, определяемых выбором криптоаналитиком и адресатом базисного вектора в базисе B_j $(j = 0, 1)$. Схема этих вычислений представлена на рис. 4 (знак «*» означает, что при измерении кубита криптоаналитиком фотон отражается). Следовательно, если $i, j \in \{0, 1\}$, то

$$P_{jjj}^{(i)} = p_1^{(j)}(i) p_2^{(j)}(i) + p_1^{(j)}(i) -$$

$$- p_1^{(j)}(i) p_2^{(j)}(i) + (1 - p_1^{(j)}(i))(1 - p_2^{(j)}(i)) = 1 - p_2^{(j)}(i) + p_1^{(j)}(i) p_2^{(j)}(i),$$

что и требовалось доказать.

Предположим, что при обработке очередного кубита отправитель и адресат используют базис B_j $(j = 0, 1)$, а криптоаналитик — базис B_{1-j}. С применением равенства (1) вычислим вероятности возможных элементарных событий, определяемых выбором адресатом базисного вектора в базисе B_j $(j = 0, 1)$, а криптоаналитиком — базисного вектора в базисе B_{1-j}. Схема этих вычислений представлена на рис. 5 (отметка «a» дуги означает фразу «фотон проходит с вероятностью 0,5», а отметка «b» — фразу «фотон отражается с вероятностью 0,5»). Следовательно, если $i, j \in \{0, 1\}$, то

$$P_{j,1-j,j}^{(i)} = 0{,}25 p_1^{(1-j)}(i) p_2^{(j)}(i) + 0{,}75 p_1^{(1-j)}(i)(1 - p_2^{(j)}(i)) +$$

$$+ 0{,}25(1 - p_1^{(1-j)}(i)) p_2^{(j)}(i) + 0{,}75(1 - p_1^{(1-j)}(i))(1 - p_2^{(j)}(i)) = 0{,}75 - 0{,}5 p_2^{(j)}(i).$$

Лемма доказана.

Передаваемый бит	Передаваемый кубит	Измерение кубита криптоаналитиком	Измерение кубита адресатом	Принятый адресатом бит	Вероятность элементарного события
$i \to$	$\mathbf{e}_i^{(j)} \to$	$p_1^{(j)}(i)$, $\mathbf{e}_i^{(j)} \to$	$p_2^{(j)}(i)$, $\mathbf{e}_i^{(j)} \to$	$i \Rightarrow$	$p_1^{(j)}(i)p_2^{(j)}(i)$
$i \to$	$\mathbf{e}_i^{(j)} \to$	$p_1^{(j)}(i)$, $\mathbf{e}_i^{(j)} \to$	$p_2^{(j)}(1-i)$, $\mathbf{e}_{1-i}^{(j)}$ * $\to$	$i \Rightarrow$	$p_1^{(j)}(i) - p_1^{(j)}(i)p_2^{(j)}(i)$
$i \to$	$\mathbf{e}_i^{(j)} \to$	$p_1^{(j)}(1-i)$, $\mathbf{e}_{1-i}^{(j)}$ * $\to$	$p_2^{(j)}(i)$, $\mathbf{e}_i^{(j)} \to$	$1-i$	
$i \to$	$\mathbf{e}_i^{(j)} \to$	$p_1^{(j)}(1-i)$, $\mathbf{e}_{1-i}^{(j)}$ * $\to$	$p_2^{(j)}(1-i)$, $\mathbf{e}_{1-i}^{(j)} \to$	$i \Rightarrow$	$(1-p_1^{(j)}(i))(1-p_2^{(j)}(i))$

Рис. 4

Передаваемый бит	Передаваемый кубит	Измерение кубита криптоаналитиком	Измерение кубита адресатом	Принятый адресатом бит	Вероятность элементарного события
$i \to$	$\mathbf{e}_i^{(j)} \to$	$p_1^{(1-j)}(i)$, $\mathbf{e}_i^{(1-j)}$	$p_2^{(j)}(i)$, $\mathbf{e}_i^{(j)}$	$1-i$	
			$p_2^{(j)}(i)$, $\mathbf{e}_i^{(j)}$	$1-i$	$0{,}25\,p_1^{(1-j)}(i)p_2^{(j)}(i)$
				i	
$i \to$	$\mathbf{e}_i^{(j)} \to$	$p_1^{(1-j)}(i)$, $\mathbf{e}_i^{(1-j)}$	$p_2^{(j)}(1-i)$, $\mathbf{e}_{1-i}^{(j)}$	i	$0{,}75\,p_1^{(1-j)}(i)(1-p_2^{(j)}(i))$
			$p_2^{(j)}(1-i)$, $\mathbf{e}_{1-i}^{(j)}$	i	
				$1-i$	
$i \to$	$\mathbf{e}_i^{(j)} \to$	$p_1^{(1-j)}(i)$, $\mathbf{e}_i^{(1-j)}$	$p_2^{(j)}(i)$, $\mathbf{e}_i^{(j)}$	$1-i$	
			$p_2^{(j)}(i)$, $\mathbf{e}_i^{(j)}$	$1-i$	$0{,}25\,(1-p_1^{(1-j)}(i))p_2^{(j)}(i)$
				i	
$i \to$	$\mathbf{e}_i^{(j)} \to$	$p_1^{(1-j)}(i)$, $\mathbf{e}_i^{(1-j)}$	$p_2^{(j)}(1-i)$, $\mathbf{e}_{1-i}^{(j)}$	i	$0{,}75\,(1-p_1^{(1-j)}(i))(1-p_2^{(j)}(i))$
			$p_2^{(j)}(1-i)$, $\mathbf{e}_{1-i}^{(j)}$	i	
				$1-i$	

Рис. 5

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

Теорема 1. При любом значении вероятности $\alpha \in [0;1]$ равенства

$$P_{jjj}(\alpha) = 1 - p_1^{(j)}(0) + p_1^{(j)}(0)p_2^{(j)}(0) + \alpha(p_1^{(j)}(0) - p_2^{(j)}(0)), \tag{4}$$

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

истинны для всех $j \in \{0,1\}$.

Доказательство. Так как $P_{jjj}(\alpha) = \alpha P_{jjj}^{(0)} + (1-\alpha)P_{jjj}^{(1)}$ $(j \in \{0,1\}, \alpha \in [0;1])$, воспользовавшись равенствами (1) и (2), получим

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

$$+(1-\alpha)(p_2^{(j)}(0) + (1-p_1^{(j)}(0))(1-p_2^{(j)}(0))) =$$

$$= 1 - p_1^{(j)}(0) + p_1^{(j)}(0)p_2^{(j)}(0) + \alpha(p_1^{(j)}(0) - p_2^{(j)}(0)) \ (j = 0,1),$$

что и требовалось доказать.

Поскольку $P_{j,1-j,j}(\alpha) = \alpha P_{j,1-j,j}^{(0)} + (1-\alpha)P_{j,1-j,j}^{(1)}$ $(j \in \{0,1\}, \alpha \in [0;1])$, воспользовавшись равенствами (1) и (3), получим

$$P_{j,1-j,j}(\alpha) = \alpha(0{,}75 - 0{,}5p_2^{(j)}(0)) +$$

$$+(1-\alpha)(0{,}75 - 0{,}5(1-p_2^{(j)}(0))) = \alpha(0{,}75 - 0{,}5p_2^{(j)}(0)) + (1-\alpha)(0{,}25 + 0{,}5p_2^{(j)}(0)) =$$

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

Теорема доказана.

Отметим ряд следствий из равенства (4).

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

$$P_{jjj}(\alpha) = 1 - (0{,}5-\alpha)p_1^{(j)}(0) - 0{,}5\alpha \quad (j \in \{0,1\}, \alpha \in [0;1]). \tag{6}$$

Из (6) вытекает, что

$$P_{jjj}(\alpha) = \begin{cases} 1 - 0{,}5\alpha, & \text{если } p_1^{(j)}(0) = 0, \\ 0{,}5(1+\alpha), & \text{если } p_1^{(j)}(0) = 1 \end{cases} \qquad (j \in \{0,1\}, \alpha \in [0;1]).$$

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

$$P_{jjj}(\alpha) = 1 - p^{(j)}(0) + (p^{(j)}(0))^2 \ \ (j \in \{0,1\}, \alpha \in [0;1]), \tag{7}$$

т.е. вероятность $P_{jjj}(\alpha)$ не зависит от вероятности α. Из (7) вытекает, что $P_{jjj}(\alpha) \in [0{,}75;1]$ $(j \in \{0,1\}, \alpha \in [0;1])$ для всех $p^{(j)}(0) \in [0;1]$, причем

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

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

1) для области значений вероятности $P_{jjj}(\alpha)$ $(\alpha \in [0;1])$, как функции от вероятности α, истинно равенство $\mathrm{Val}\, P_{jjj}(\alpha) = [l_1; L_1]$, где

$$l_1 = \min\{1 - p_1^{(j)}(0) + p_1^{(j)}(0)p_2^{(j)}(0);\ 1 - p_2^{(j)}(0) + p_1^{(j)}(0)p_2^{(j)}(0)\}, \qquad (8)$$

$$L_1 = \max\{1 - p_1^{(j)}(0) + p_1^{(j)}(0)p_2^{(j)}(0);\ 1 - p_2^{(j)}(0) + p_1^{(j)}(0)p_2^{(j)}(0)\}; \qquad (9)$$

2) из (8) и (9) вытекает, что для всех значений $\alpha \in [0; 1]$, если либо $p_k^{(j)}(0) \to 0$ $(k = 1, 2)$, либо $p_k^{(j)}(0) \to 1$ $(k = 1, 2)$, то $l_1 \to 1$ и $L_1 \to 1$, т.е. $P_{jjj}(\alpha) \to 1 (\alpha \in [0; 1])$;

3) вероятность $P_{jjj}(\alpha)$ — 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) если $p_1^{(j)}(0) \to 1$ и $p_2^{(j)}(0) \to 0$, то $P_{jjj}(\alpha) \to \alpha$ $(\alpha \in [0; 1])$;

5) если $p_1^{(j)}(0) \to 0$ и $p_2^{(j)}(0) \to 1$, то $P_{jjj}(\alpha) \to 1 - \alpha$ $(\alpha \in [0; 1])$.

Отметим ряд следствий из равенства (5).

1. Вероятность $P_{j,1-j,j}(\alpha)$ $(j \in \{0, 1\}, \alpha \in [0; 1])$ не зависит от вероятности выбора криптоаналитиком базисного вектора в базисе B_{1-j} для измерения перехваченного кубита.

2. Для всех $\alpha \in [0; 1]$

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

3. Пусть $p_2^{(j)}(0) = 0{,}5$ $(j = 0, 1)$. Тогда $P_{j,1-j,j}(\alpha) = 0{,}5$ $(\alpha \in [0; 1])$, т.е. вероятность $P_{j,1-j,j}(\alpha)$ не зависит от вероятности α.

4. Пусть $p_2^{(j)}(0) \neq 0{,}5$ $(j = 0, 1)$. Тогда:

1) для области значений вероятности $P_{j,1-j,j}(\alpha)$, как функции от вероятности α, истинно равенство $\mathrm{Val}\, P_{j,1-j,j}(\alpha) = [l_2; L_2]$, где

$$l_2 = \min\{0{,}25 + 0{,}5p_2^{(j)}(0);\ 0{,}75 - 0{,}5p_2^{(j)}(0)\}, \qquad (10)$$

$$L_2 = \max\{0{,}25 + 0{,}5p_2^{(j)}(0);\ 0{,}75 - 0{,}5p_2^{(j)}(0)\}; \qquad (11)$$

2) вероятность $P_{j,1-j,j}(\alpha)$ — 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 (10) и (11) вытекает, что если $p_2^{(j)}(0) \to 0{,}5$, то $l_2 \to 0{,}5$ и $L_2 \to 0{,}5$, т.е. $P_{j,1-j,j}(\alpha) \to 0{,}5$ $(\alpha \in [0; 1])$.

Обозначим $P_1(\alpha)$ $(\alpha \in [0; 1])$ вероятность правильного считывания адресатом значения бита при условии, что для обработки данного кубита отправитель и адресат используют один и тот же базис, а вероятность пересылки отправителем символа 0 равна α.

Теорема 2. Для всех $\alpha \in [0; 1]$ истинно равенство

$$P_1(\alpha) = 0{,}25\,(2{,}5 + \alpha - (1-\alpha)(p_1^{(0)}(0) + p_1^{(1)}(0)) +$$
$$+ (0{,}5 - 2\alpha)\,(p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0)p_2^{(0)}(0) + p_1^{(1)}(0)p_2^{(1)}(0)). \qquad (12)$$

Доказательство. Поскольку

$$P_1(\alpha) = 0{,}25(P_{000}(\alpha) + P_{111}(\alpha) + P_{010}(\alpha) + P_{101}(\alpha)) \ (\alpha \in [0; 1]),$$

воспользовавшись равенствами (4) и (5), получим

$$P_1(\alpha) = 0{,}25(1 - p_1^{(0)}(0) + p_1^{(0)}(0)p_2^{(0)}(0) + \alpha(p_1^{(0)}(0) - p_2^{(0)}(0)) +$$

$$+ 1 - p_1^{(1)}(0) + p_1^{(1)}(0)p_2^{(1)}(0) + \alpha(p_1^{(1)}(0) - p_2^{(1)}(0)) +$$

$$+ 0{,}25 + 0{,}5\alpha + (0{,}5 - \alpha)p_2^{(0)}(0) + 0{,}25 + 0{,}5\alpha + (0{,}5 - \alpha)p_2^{(1)}(0) =$$

$$= 0{,}25(2{,}5 + \alpha - (1 - \alpha)(p_1^{(0)}(0) + p_1^{(1)}(0)) +$$

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

Теорема доказана.

Отметим ряд следствий из равенства (12).

1. Вероятность $P_1(\alpha)$, как функция от вероятности α:

1) является монотонно возрастающей функцией, если

$$p_2^{(0)}(0) + p_2^{(1)}(0) < 0{,}5(1 + p_1^{(0)}(0) + p_1^{(1)}(0)),$$

причем $\operatorname{Val} P_1(\alpha) = [l_3; L_3]$, где

$$l_3 = 0{,}25(2{,}5 - (p_1^{(0)}(0) + p_1^{(1)}(0)) +$$

$$+ 0{,}5(p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0)p_2^{(0)}(0) + p_1^{(1)}(0)p_2^{(1)}(0)),$$

$$L_3 = 0{,}25(3{,}5 - 1{,}5(p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0)p_2^{(0)}(0) + p_1^{(1)}(0)p_2^{(1)}(0));$$

2) является монотонно убывающей функцией, если

$$p_2^{(0)}(0) + p_2^{(1)}(0) > 0{,}5(1 + p_1^{(0)}(0) + p_1^{(1)}(0)),$$

причем $\operatorname{Val} P_1(\alpha) = [l_4; L_4]$, где

$$l_4 = 0{,}25\,(3{,}5 - 1{,}5(p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0)p_2^{(0)}(0) + p_1^{(1)}(0)p_2^{(1)}(0)),$$

$$L_4 = 0{,}25(2{,}5 - (p_1^{(0)}(0) + p_1^{(1)}(0)) +$$

$$+ 0{,}5(p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0)p_2^{(0)}(0) + p_1^{(1)}(0)p_2^{(1)}(0));$$

3) не зависит от значения α, если

$$p_2^{(0)}(0) + p_2^{(1)}(0) = 0{,}5(1 + p_1^{(0)}(0) + p_1^{(1)}(0)), \tag{13}$$

причем

$$P_1(\alpha) = 0{,}25(2{,}75 - 0{,}75(p_1^{(0)}(0) + p_1^{(1)}(0)) + p_1^{(0)}(0)p_2^{(0)}(0) + p_1^{(1)}(0)p_2^{(1)}(0))$$

$$(\alpha \in [0; 1]). \tag{14}$$

2. Если $p_k^{(j)}(0) \to 0$ ($j = 0, 1$; $k = 1, 2$), то $P_1(\alpha) \to 0{,}625 + 0{,}250\alpha$ ($\alpha \in [0; 1]$), причем:

1) если $\alpha \to 0$, то $P_1(\alpha) \to 0{,}625$;

2) если $\alpha \to 0{,}5$, то $P_1(\alpha) \to 0{,}750$;

3) если $\alpha \to 1$, то $P_1(\alpha) \to 0{,}875$.

3. Если $p_1^{(j)}(0) \to 1$, $p_2^{(j)}(0) \to 0$ ($j = 0, 1$), то $P_1(\alpha) \to 0{,}125 + 0{,}750\alpha$ ($\alpha \in [0; 1]$), причем:

1) если $\alpha \to 0$, то $P_1(\alpha) \to 0{,}125$;

2) если $\alpha \to 0{,}5$, то $P_1(\alpha) \to 0{,}500$;

3) если $\alpha \to 1$, то $P_1(\alpha) \to 0{,}875$.

4. Если $p_1^{(j)}(0) \to 0$, $p_2^{(j)}(1) \to 1$ ($j = 0, 1$), то $P_1(\alpha) \to 0{,}875 - 0{,}750\alpha$ ($\alpha \in [0; 1]$), причем:

1) если $\alpha \to 0$, то $P_1(\alpha) \to 0{,}875$;

2) если $\alpha \to 0{,}5$, то $P_1(\alpha) \to 0{,}500$;

3) если $\alpha \to 1$, то $P_1(\alpha) \to 0{,}125$.

5. Если $p_k^{(j)}(0) \to 1$ ($j = 0, 1$; $k = 1, 2$), то $P_1(\alpha) \to 0{,}875 - 0{,}250\alpha$ ($\alpha \in [0; 1]$), причем:

1) если $\alpha \to 0$, то $P_1(\alpha) \to 0{,}875$;

2) если $\alpha \to 0{,}5$, то $P_1(\alpha) \to 0{,}750$;

3) если $\alpha \to 1$, то $P_1(\alpha) \to 0{,}625$.

6. Если $p_k^{(j)}(0) \to 0{,}5$ ($j = 0, 1$; $k = 1, 2$), то $P_1(\alpha) = 0{,}625$ ($\alpha \in [0; 1]$).

Проведенный анализ показывает, что из теоремы 2 вытекает следствие.

Следствие 1. При атаке, определяемой предположениями 1 и 2, если криптоаналитик располагает информацией о том, какое из утверждений, «$\alpha \in (0; 0{,}5)$» или «$\alpha \in (0{,}5; 1)$», истинно, то он всегда может выбрать свою стратегию так, что:

— в среднем приблизительно 75% ключа будет передано адресату верно, если генератор последовательностей, используемый отправителем, близок к псевдослучайному генератору;

— в среднем приблизительно 87,5% ключа может быть передано адресату верно, если генератор последовательностей, используемый отправителем, далек от псевдослучайного генератора.

Теорема 3. При атаке, определяемой предположениями 1 и 2, существует по крайней мере два связных континуальных множества таких стратегий криптоаналитика, что при любом значении $\alpha \in [0; 1]$ в среднем 68,75% ключа будет передано адресату верно.

Доказательство. Положив $p_1^{(0)}(0) = p_1^{(1)}(0) = 1$ в (13), получим $p_2^{(0)}(0) + p_2^{(1)}(0) = 1{,}5$. Следовательно, любая такая стратегия криптоаналитика, что

$$\begin{cases} p_1^{(0)}(0) = p_1^{(1)}(0) = 1, \\ p_2^{(0)}(0) + p_2^{(1)}(0) = 1{,}5, \end{cases} \tag{15}$$

удовлетворяет равенству (13). Подставив (15) в (14), получим

$$P_1(\alpha) = 0{,}25(2{,}75 - 0{,}75 \cdot 2 + 1{,}5) = 0{,}6875 \quad (\alpha \in [0, 1]).$$

Аналогичным образом, подставив $p_1^{(0)}(0) = p_1^{(1)}(0) = 0$ в (13), получим $p_2^{(0)}(0) + p_2^{(1)}(0) = 0{,}5$. Поэтому любая такая стратегия криптоаналитика, что

$$\begin{cases} p_1^{(0)}(0) = p_1^{(1)}(0) = 0, \\ p_2^{(0)}(0) + p_2^{(1)}(0) = 0{,}5, \end{cases} \tag{16}$$

также удовлетворяет равенству (13), причем из (16) и (14) вытекает

$$P_1(\alpha) = 0{,}25 \cdot 2{,}75 = 0{,}6875 \ (\alpha \in [0; 1]).$$

Множества (15) и (16) представляют собой два таких связных континуальных множества стратегий криптоаналитика, что при любом значении $\alpha \in [0; 1]$ в среднем 68,75% ключа будет передано адресату верно.

Теорема доказана.

3. АТАКА ПРИ УПРАВЛЕНИИ ИЗМЕНЕНИЕМ БАЗИСОВ ОТПРАВИТЕЛЯ И АДРЕСАТА

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

Обозначим $P_2(\alpha)$ ($\alpha \in [0; 1]$) вероятность правильного считывания адресатом значения бита при условии, что при обработке данного кубита отправитель и адресат ис-

пользуют один и тот же базис B_j $(j=0,1)$, вероятность пересылки символа 0 отправителем равна α, а вероятность одновременного изменения криптоаналитиком как у отправителя, так и у адресата базиса B_j $(j=0,1)$ на базис B_{1-j} равна $p_0(j)$.

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

$$P_2(\alpha) = 0,25(P_{000}(\alpha)+P_{111}(\alpha)+P_{010}(\alpha)+P_{101}(\alpha)+$$
$$+(p_0(1)-p_0(0))(P_{000}(\alpha)+P_{010}(\alpha)-P_{101}(\alpha)-P_{111}(\alpha))). \qquad (17)$$

Доказательство. Пусть при обработке очередного кубита отправитель и адресат считают, что они используют один и тот же базис B_j $(j=0,1)$, а криптоаналитик использует базис B_h $(h=0,1)$. Тогда при атаке, определяемой предположениями 1–3, для всех $\alpha \in [0;1]$ вероятность правильного считывания адресатом значения бита равна $(1-p_0(j))P_{jhj}(\alpha)+p_0(j)P_{1-j,h,1-j}(\alpha)$. Следовательно, для всех $\alpha \in [0;1]$ имеем

$$P_2(\alpha) = 0,25\left(\sum_{j=0}^{1}\sum_{h=0}^{1}(1-p_0(j))P_{jhj}(\alpha)+p_0(j)P_{1-j,h,1-j}(\alpha)\right) =$$

$$= 0,25((1-p_0(0))P_{000}(\alpha)+p_0(0)P_{101}(\alpha)+$$
$$+(1-p_0(0))P_{010}(\alpha)+p_0(0)P_{111}(\alpha)+(1-p_0(1))P_{101}(\alpha)+p_0(1)P_{000}(\alpha)+$$
$$+(1-p_0(1))P_{111}(\alpha)+p_0(1)P_{010}(\alpha)) =$$
$$= 0,25(P_{000}(\alpha)+P_{111}(\alpha)+P_{010}(\alpha)+P_{101}(\alpha)+$$
$$+(p_0(1)-p_0(0))(P_{000}(\alpha)+P_{010}(\alpha)-P_{101}(\alpha)-P_{111}(\alpha))).$$

Теорема доказана.

Из (17) вытекают два следствия.

Следствие 2. Неравенство $P_2(\alpha) > P_1(\alpha)$ $(\alpha \in [0;1])$ истинно тогда и только тогда, когда либо

$$\begin{cases} P_{000}(\alpha)+P_{010}(\alpha)-P_{101}(\alpha)-P_{111}(\alpha)<0, \\ p_0(1)-p_0(0)<0, \end{cases}$$

либо

$$\begin{cases} P_{000}(\alpha)+P_{010}(\alpha)-P_{101}(\alpha)-P_{111}(\alpha)>0, \\ p_0(1)-p_0(0)>0. \end{cases}$$

Следствие 3. Равенство $P_2(\alpha) = P_1(\alpha)$ $(\alpha \in [0;1])$ истинно тогда и только тогда, когда $p_0(1) = p_0(0)$ или когда $P_{000}(\alpha)+P_{010}(\alpha)-P_{111}(\alpha)-P_{101}(\alpha) = 0$.

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

Подставив (4) и (5) в (17), получим, что для всех $\alpha \in [0;1]$

$$P_2(\alpha) = 0,25(2,5+\alpha-(1-\alpha)(p_1^{(0)}(0)+p_1^{(1)}(0))+$$
$$+(0,5-2\alpha)(p_2^{(0)}(0)+p_2^{(1)}(0))+p_1^{(0)}(0)p_2^{(0)}(0)+p_1^{(1)}(0)p_2^{(1)}(0)+$$
$$+(p_0(1)-p_0(0))(p_1^{(0)}(0)p_2^{(0)}(0)-p_1^{(1)}(0)p_2^{(1)}(0)+$$
$$+(\alpha-1)(p_1^{(0)}(0)-p_1^{(1)}(0))+(0,5-2\alpha)(p_2^{(0)}(0)-p_2^{(1)}(0)))). \qquad (18)$$

Из (18) вытекает, что вероятность $P_2(\alpha)$ $(\alpha \in [0;1])$, как функция от вероятности α:

1) монотонно возрастает, если

$$1+(1+p_0(1)-p_0(0))(p_1^{(0)}(0)-2p_2^{(0)}(0))+$$
$$+(1-p_0(1)+p_0(0))(p_1^{(1)}(0)-2p_2^{(1)}(0))>0;$$

2) монотонно убывает, если

$$1+(1+p_0(1)-p_0(0))(p_1^{(0)}(0)-2p_2^{(0)}(0))+$$

$$+(1-p_0(1)+p_0(0))(p_1^{(1)}(0)-2p_2^{(1)}(0))<0.$$

Таким образом, если в процессе передачи ключа отправитель управляет вероятностью α пересылки символа 0, а криптоаналитику известен этот закон управления, то криптоаналитик располагает возможностью подобрать адаптивную стратегию атаки на квантовый протокол передачи ключа, определяемой предположениями 1–3, направленную либо на максимизацию, либо на минимизацию количества правильно прочитанных адресатом символов.

Подводя итог, заключаем, что атака на квантовый протокол передачи ключа, определяемая предположениями 1–3, может существенно усложнить работу легальных пользователей.

4. ШИФР НА ОСНОВЕ АЛГОРИТМА ПЛОТНОГО КОДИРОВАНИЯ

Задача плотного кодирования состоит в том, что отправитель должен переслать адресату 2-битовую последовательность $\alpha_1\alpha_2$, используя систему из двух кубитов $|\psi\rangle = 2^{-0,5}(|00\rangle + |11\rangle)$. При этом первый кубит находится у отправителя, а второй — у адресата.

Алгоритм плотного кодирования состоит в следующем. В зависимости от значения передаваемой последовательности $\alpha_1\alpha_2$ $(\alpha_1,\alpha_2 \in \{0,1\})$ отправитель выполняет над своим кубитом такое унитарное преобразование $U_{\alpha_1\alpha_2}$ $(\alpha_1,\alpha_2 \in \{0,1\})$ (а следовательно, над системой $|\psi\rangle$ выполняется унитарное преобразование $U_{\alpha_1\alpha_2} \otimes I$ $(\alpha_1,\alpha_2 \in \{0,1\})$, где $\otimes$ — тензорное произведение, I — тождественное преобразование), что

$$U_{00} = I,\ U_{01} = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\quad U_{10} = Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ U_{11} = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

После этого отправитель пересылает по квантовому каналу свой кубит адресату.

Адресат применяет к системе кубитов унитарное преобразование

$$C_{\text{not}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

измеряет второй кубит, применяет к первому кубиту преобразование Адамара

$$H = \begin{pmatrix} 2^{-0,5} & 2^{-0,5} \\ 2^{-0,5} & -2^{-0,5} \end{pmatrix},$$

а затем измеряет первый кубит. Декодирование адресатом переданной 2-битовой последовательности осуществляется в соответствии со следующей схемой:

$$\begin{cases} |00\rangle \to 00 \\ |01\rangle \to 01 \\ |10\rangle \to 11 \\ |11\rangle \to 10 \end{cases}. \tag{19}$$

Теорема 5. Алгоритм плотного кодирования остается корректным, если исходная система из двух кубитов имеет вид $|\xi\rangle = 2^{-0,5}(|01\rangle + |10\rangle)$. При этом схема декодирования адресатом переданной 2-битовой последовательности имеет вид

$$\begin{cases} |00\rangle \to 01 \\ |01\rangle \to 00 \\ |10\rangle \to 10 \\ |11\rangle \to 11 \end{cases}. \tag{20}$$

Доказательство. В соответствии с алгоритмом плотного кодирования после применения отправителем унитарного преобразования к первому кубиту получим

$$(U_{00} \otimes I)(|\xi\rangle) = (I \otimes I)(|\xi\rangle) = 2^{-0,5}(|01\rangle + |10\rangle),$$

$$(U_{01} \otimes I)(|\xi\rangle) = (X \otimes I)(|\xi\rangle) =$$

$$= 2^{-0,5}\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 2^{-0,5}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 2^{-0,5}(|00\rangle + |11\rangle),$$

$$(U_{10} \otimes I)(|\xi\rangle) = (Y \otimes I)(|\xi\rangle) =$$

$$= 2^{-0,5}\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 2^{-0,5}\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} = 2^{-0,5}(|00\rangle - |11\rangle),$$

$$(U_{11} \otimes I)(|\xi\rangle) = (Z \otimes I)(|\xi\rangle) =$$

$$= 2^{-0,5}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 2^{-0,5}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} = 2^{-0,5}(|01\rangle - |10\rangle).$$

После того как отправитель перешлет по квантовому каналу свой кубит адресату, а адресат применит к системе кубитов унитарное преобразование C_{not}, получим

$$C_{\text{not}}(2^{-0,5}(|01\rangle + |10\rangle)) =$$

$$= 2^{-0,5}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 2^{-0,5}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 2^{-0,5}(|01\rangle + |11\rangle),$$

$$C_{\text{not}}(2^{-0,5}(|00\rangle + |11\rangle)) =$$

$$= 2^{-0,5}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 2^{-0,5}\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 2^{-0,5}(|00\rangle + |10\rangle),$$

$$C_{\text{not}}(2^{-0,5}(|00\rangle + |11\rangle)) =$$

$$= 2^{-0,5}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix} = 2^{-0,5}\begin{pmatrix}1\\0\\-1\\0\end{pmatrix} = 2^{-0,5}(|00\rangle - |10\rangle),$$

$$C_{\text{not}}(2^{-0,5}(|00\rangle + |11\rangle)) =$$

$$= 2^{-0,5}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix} = 2^{-0,5}\begin{pmatrix}0\\1\\0\\-1\end{pmatrix} = 2^{-0,5}(|01\rangle - |11\rangle).$$

После измерения второго кубита адресат приходит к выводу:

1) если результат измерения равен $|1\rangle$, то передана последовательность 00 или 11;

2) если результат измерения равен $|0\rangle$, то передана последовательность 01 или 10.

Этот вывод может быть представлен разбиением $\pi_1 = \{\overline{00, 11}; \overline{01, 10}\}$.

После применения к первому кубиту преобразования Адамара имеем

$$H(2^{-0,5}(|0\rangle + |1\rangle)) = 2^{-1}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} = 2^{-1}\begin{pmatrix}2\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle,$$

$$H(2^{-0,5}(|0\rangle - |1\rangle)) = 2^{-1}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1\\-1\end{pmatrix} = 2^{-1}\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle.$$

Измерив первый кубит, адресат приходит к выводу:

1) если результат измерения равен $|0\rangle$, то передана последовательность 00 или 01;

2) если результат измерения равен $|1\rangle$, то передана последовательность 10 или 11.

Этот вывод можно представить разбиением $\pi_2 = \{\overline{00, 01}; \overline{10, 11}\}$.

Таким образом, исходная двоичная последовательность идентифицируется единственным образом (так как $\pi_1 \cdot \pi_2 = \{\overline{00}; \overline{01}; \overline{10}; \overline{11}\}$). При этом (20) представляет схему декодирования результатов измерения кубитов адресатом.

Теорема доказана.

Из теоремы 5 вытекает корректность квантового алгоритма $\mathsf{C}_{\text{кв}}$ шифрования $2n$-битовой последовательности $\alpha_1\alpha_2\alpha_3\alpha_4 \ldots \alpha_{2n-1}\alpha_{2n}$ посредством системы из $2n$ кубитов.

Пусть n-битовая последовательность $\beta_1 \ldots \beta_n$ — секретный сеансовый ключ, имеющийся и у отправителя, и у адресата. Отправитель подготавливает исходную систему из $2n$ кубитов, имеющую вид $\chi_{2n} = \zeta_1 \otimes \ldots \otimes \zeta_n$, где

$$\zeta_i = \begin{cases}\psi, \text{ если } \beta_i = 0,\\ \xi, \text{ если } \beta_i = 1\end{cases} \quad (i = 1, \ldots, n).$$

По квантовому каналу отправитель пересылает адресату кубиты с четными номерами. После этого отправитель преобразует каждый кубит с нечетным номером в соответствии с алгоритмом плотного кодирования, затем пересылает преобразованные кубиты адресату. Адресат, получив их, компонует пары соответствующих кубитов, а затем обрабатывает каждую пару в соответствии с алгоритмом плотного кодирования.

5. АНАЛИЗ ШИФРА $\mathsf{C}_{\text{кв}}$

Исследуем вычислительную стойкость шифра $\mathsf{C}_{\text{кв}}$ при атаке на квантовый канал, состоящей в том, что криптоаналитик, представившись адресатом, перехватывает кубиты, пересылаемые отправителем.

Из (19) и (20) вытекает, что если криптоаналитик выбрал не ту схему декодирования, то он правильно расшифровывает бит с нечетным номером и неправильно — бит с четным номером.

Пусть $p_i \in [0,1]$ $(i = 1, \ldots, n)$ — вероятность того, что в процессе передачи $2n$-битовой последовательности $\alpha_1\alpha_2\alpha_3\alpha_4 \ldots \alpha_{2n-1}\alpha_{2n}$, зашифрованной с помощью шифра $\mathsf{C}_{\text{кв}}$, криптоаналитик правильно определяет i-й бит секретного сеансового ключа $\beta_1 \ldots \beta_n$.

Теорема 6. Вероятность $P_{2n,k}(p_1, \ldots, p_n)$ $(k = 0, 1, \ldots, n)$ того, что в процессе расшифровки $2n$-битовой последовательности, зашифрованной посредством шифра $\mathsf{C}_{\text{кв}}$, криптоаналитик получит последовательность, отстоящую от исходной последовательности на расстоянии k $(0 \le k \le n)$ по Хеммингу, равна

$$P_{2n,k}(p_1, \ldots, p_n) = \sum_{1 \le i_1 < \ldots < i_k \le n} r_1 \ldots r_n \quad (k = 0, 1, \ldots, n), \tag{21}$$

где

$$r_i = \begin{cases} 1 - p_i, & \text{если } i \in \{i_1, \ldots, i_k\}, \\ p_i, & \text{если } i \notin \{i_1, \ldots, i_k\}. \end{cases} \tag{22}$$

Доказательство. Результат расшифровки криптоаналитиком $2n$-битовой последовательности, зашифрованной посредством шифра $\mathsf{C}_{\text{кв}}$, отстоит от исходной последовательности на расстоянии k $(0 \le k \le n)$ по Хеммингу тогда и только тогда, когда криптоаналитик неправильно определяет в точности k бит секретного сеансового ключа $\beta_1 \ldots \beta_n$.

Вероятность того, что криптоаналитик неправильно определяет биты секретного ключа, имеющие номера $i_1, \ldots, i_k$ $(1 \le i_1 < \ldots < i_k \le n)$, и правильно определяет биты секретного ключа, имеющие номера, принадлежащие множеству $\mathbf{N}_n \setminus \{i_1, \ldots, i_k\}$, равна $r_1 \ldots r_n$, где r_i $(i = 1, \ldots, n)$ определяется в соответствии с (22). Следовательно,

$$P_{2n,k}(p_1, \ldots, p_n) = \sum_{1 \le i_1 < \ldots < i_k \le n} r_1 \ldots r_n \quad (k = 0, 1, \ldots, n).$$

Теорема доказана.

Для всех $p \in [0,1]$ положим

$$P_{2n,k}(p) = P_{2n,k}(\underbrace{p, \ldots, p}_{n \text{ раз}}) \quad (0 \le k \le n). \tag{23}$$

Следствие 4. Для всех $p \in [0,1]$, $n \in \mathbf{N}$ и $k \in \mathbf{Z}_+$ $(0 \le k \le n)$ истинны равенства

$$P_{2n,k}(p) = \binom{n}{k} (1-p)^k \, p^{n-k} \quad (0 \le k \le n). \tag{24}$$

Доказательство. Подставив $p_1 = \ldots = p_n = p$ в (22), получим

$$r_i = \begin{cases} 1 - p, & \text{если } i \in \{i_1, \ldots, i_k\}, \\ p, & \text{если } i \notin \{i_1, \ldots, i_k\}. \end{cases} \tag{25}$$

Подставив (25) в (21), имеем

$$P_{2n,k}(p_1, \ldots, p_n) = \sum_{1 \le i_1 < \ldots < i_k \le n} (1-p)^k \, p^{n-k} =$$

$$= (1-p)^k \, p^{n-k} \sum_{1 \le i_1 < \ldots < i_k \le n} 1 = \binom{n}{k} (1-p)^k \, p^{n-k}. \tag{26}$$

Из (23) и (26) вытекает (24).

Следствие доказано.

Пусть $k^{\text{ср}}_{2n,k}(p)$ — среднее число ошибок, допускаемых криптоаналитиком в процессе расшифровки $2n$-битовой последовательности, зашифрованной посредством шифра $\mathsf{C}_{\text{кв}}$, при условии, что $p_1 = \ldots = p_n = p$.

Следствие 5. Для всех $p \in [0,1]$, $n \in \mathbf{N}$ и $k \in \mathbf{Z}_+$ $(0 \le k \le n)$ истинно равенство

$$k^{\text{ср}}_{2n,k}(p) = n(1-p). \tag{27}$$

Доказательство. При фиксированных значениях чисел $p \in [0,1]$, $n \in \mathbf{N}$ и $k \in \mathbf{Z}_+$ $(0 \le k \le n)$ правая часть формулы (24) представляет собой схему Бернулли с вероятностью события в каждом испытании, равной $1-p$. Подставив в формулу для математического ожидания биномиального распределения вместо вероятности значение $1-p$, получим (27).

Следствие доказано.

Случай $p = 0{,}5$ соответствует ситуации, когда секретный сеансовый ключ $\beta_1 \dots \beta_n$ — случайная последовательность, а криптоаналитик определяет значение каждого бита ключа случайным образом. Из (24) и (27) следует

$$P_{2n,k}(0{,}5) = \binom{n}{k}(0{,}5)^n \qquad (0 \le k \le n),$$

$$k^{\text{ср}}_{2n,k}(0{,}5) = 0{,}5n. \tag{28}$$

Из (28) вытекают два следствия.

Следствие 6. Если секретный сеансовый ключ $\beta_1 \dots \beta_n$ — случайная последовательность, а криптоаналитик определяет значение каждого бита ключа случайным образом, то в процессе расшифровки $2n$-битовой последовательности, зашифрованной посредством шифра $\mathsf{C}_{\text{кв}}$, в среднем 25% переданной последовательности расшифровывается криптоаналитиком неправильно.

Следствие 7. Если секретный сеансовый ключ $\beta_1 \dots \beta_n$ — случайная последовательность, а криптоаналитик определяет значение каждого бита ключа случайным образом, то в процессе расшифровки $2n$-битовой последовательности, зашифрованной посредством шифра $\mathsf{C}_{\text{кв}}$, для коррекции расшифрованного шифртекста криптоаналитик вынужден, в среднем, осуществлять полный перебор вариантов по четверти длины шифртекста.

Полученные результаты показывают, что построенный квантовый шифр $\mathsf{C}_{\text{кв}}$ обладает достаточно высокой вычислительной стойкостью, если секретный сеансовый ключ $\beta_1 \dots \beta_n$ — последовательность, близкая к случайной последовательности.

ЗАКЛЮЧЕНИЕ

В работе исследована вычислительная стойкость двух модельных задач квантовых вычислений, имеющих непосредственное отношение к разработке моделей и методов квантовой криптографии, а именно: классического квантового протокола передачи ключа и шифра, построенного на основе классического алгоритма плотного кодирования. Показано, что для квантового протокола передачи ключа расширение возможностей криптоаналитика за счет управления вероятностями выбора базисных векторов для измерения кубита, а также одновременного изменения базисов отправителя и адресата может значительно усилить его атаку на этот протокол. Эффективность такой атаки существенно зависит от генератора последовательностей, имеющегося у отправителя. Более тонкий анализ этой зависимости — одно из возможных направлений дальнейших исследований. Второе направление 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.

Предложенный шифр, построенный на алгоритме плотного кодирования, имеет достаточно высокую вычислительную стойкость. Для этого шифра естественно обобщение полученных результатов на случай, когда состояние каждой квантовой частицы представлено вектором h-мерного комплексного пространства, что может быть третьим направлением исследований. Четвертое направление связано с разработкой квантовых протоколов, предназначенных для эффективного обнаружения атаки на как можно более раннем этапе процесса передачи информации.

СПИСОК ЛИТЕРАТУРЫ

1. Ожигов Ю.И. Квантовые вычисления. — М.: МГУ, 2003. — 104 с.
2. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. — М.: Мир, 2006. — 824 с.
3. Rieffel E., Pollak W. An introduction to quantum computing for non-physicists // ACM Computing Surveys. — 2000. — **32**, N 3. — P. 300–335.
4. Bennett C.H., Brassard G. Quantum public key distribution system // IBM Techn. Disclosure Bull. — 1985. — **28**. — P. 3153–3164.
5. Bennett C.H., Brassard G. Quantum public key distribution reinvented // SIGACT News. — 1987. — **18**, N 4. — P. 51–53.
6. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин и др. — М.: Гелиос АРВ, 2002. — 480 с.

Поступила 21.01.2009