НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ВЫСШАЯ ШКОЛА ЭКОНОМИКИ

Факультет физики

Вопрос по выбору

Устойчивость различных протоколов квантового распределения ключей к PNS-атакам

Работу выполнил студент 3 курса
Захаров Сергей Дмитриевич

Москва
2021

Содержание

1. PNS-атака **2**

2. Атака на протокол BB84 **2**

3. Протокол B92 **2**

3.1. Атака на протокол B92 3

4. Протокол 4+2 **4**

4.1. Атака на протокол 4+2 4

5. Протокол SARG04 **5**

1. PNS-атака

Такая атака оказывается возможной в силу использования в реальных системах ослабленных лазерных импульсов, а не однофотонных источников. При этом вместо состояний $|0\rangle$ и $|1\rangle$ по каналу реально пересылаются состояния виде $|0\rangle^{\otimes n}$ и $|1\rangle^{\otimes n}$. В таком случае, если измерение Евы описывается т.н. разложением единицы, для которого:

$$M_1 = |0\rangle\langle 0| + |1\rangle\langle 1| \tag{1}$$
$$M_2 = |00\rangle\langle 00| + |11\rangle\langle 11| \tag{2}$$
$$M_3 = |000\rangle\langle 000| + |111\rangle\langle 111| \tag{3}$$
$$... \tag{4}$$
$$M_n = |0\rangle^{\otimes n}\langle 0|^{\otimes n} + |1\rangle^{\otimes n}\langle 1|^{\otimes n} \tag{5}$$

то Ева получает всю информацию о числе фотонов в этом импульсе, при этом не внеся в канал помех, т.е. знание о числе фотонов в импульсе не защищено фундаментальными законами квантовой механики. Имея эту информацию, Ева может, например заблокировать те импульсы, которые содержат только один фотон, а для тех импульсов, где несколько фотонов, пропустить Бобу только один из фотонов, производя над оставшимися некоторые действия. При этом понятно, что нужно как-то компенсировать блокировку одночастичных импульсов. Сделать это можно, например, за счет более совершенного канала для транспортировки оставшихся импульсов на сторону Боба. Это доступно с учетом предпосылки о том, что пользователи не имеют полного контроля над квантовым каналом связи, т.е. потенциально Ева может заменить его на свой канал (который, как было сказано, обеспечивает меньшее затухание), благодаря чему действия Евы не смогут быть детектированы.

2. Атака на протокол BB84

Поскольку протокол является самым известным среди всех, его описание не было приведено. Однако принцип атаки на этот протокол является основой для атаки на протокол B92, поэтому остановимся на нем. Приведем алгоритм атаки.

Если импульс содержит только один фотон, то Ева его блокирует. В противном случае она каким-то образом (например, с помощью линии задержки) сохраняет один из фотонов, а остальные пересылает Бобу по своему каналу (который более совершенный, чем канал Алисы и Боба, в идеале вообще не имеющий потерь). После того, как базисы были согласованы по открытому каналу, у Евы оказывается вся необходимая информация для различения оказавшихся у нее фотонов, благодаря чему она получает возможность узнать секретный ключ, т.е. протокол взломан. Таким образом, BB84 не защищен перед PNS-атакой.

3. Протокол B92

Приведем некоторую основную информацию о протоколе B92. Его отличие от BB84 заключается в использовании неортогональных состояний. Кодирование может выглядить, например, следующим образом:

1) Линейная поляризация

   - Горизонтальная

- Вертикальная

2) Круговая поляризация

   - Правая круговая
   - Левая круговая

Подобное позволяет исключить 25-ти процентную вероятность ошибки на приемной стороне до того, как базисы согласованы, даже при отсутствии действий перехватчика и помех в канале. Целью является возможность гибкого изменения параметров в зависимости от дополнительных условий, например, от качества канала, что, потенциально, может помочь добиться большей скорости передачи данных в некоторых ситуациях.

Принцип следующий: Алиса на каждом шаге посылает Бобу одно из двух неортогональных состояний $|\psi_0\rangle$ и $|\psi_1\rangle$, для которых основным параметром протокола является $\cos\eta = \langle\psi_0|\psi_1\rangle$. Боб производит т.н. измерение с тремя исходами:

$$M_0 = \frac{|\psi_1^\perp\rangle\langle\psi_1^\perp|}{1+\cos\eta} = \frac{I - |\psi_1\rangle\langle\psi_1|}{1+\cos\eta} \tag{6}$$

$$M_1 = \frac{|\psi_0^\perp\rangle\langle\psi_0^\perp|}{1+\cos\eta} = \frac{I - |\psi_0\rangle\langle\psi_0|}{1+\cos\eta} \tag{7}$$

$$M_? = I - M_0 - M_1 \tag{8}$$

Применение этого метода эффективно, поскольку первые два исхода при отсутствии ошибок будет отвечать точным результатам, а исход "?", который называется **несовместным**, не будет давать полезных сведений о передаваемом состоянии.

После передачи сообщений, как и в BB84, часть битовых последовательностей раскрываются Алисой и Бобом, после чего оценивается число ошибок, и, если их оказалось больше некоторого порога, то протокол останавливается, поскольку из оставшейся части строк можно полностью получить секретный ключ.

Как уже было сказано, отличие B92 от BB84 заключается в наличии параметра η. Очевидно, что чем ближе η к $\pi/2$, тем больше совпадают протоколы и тем выше скорость передачи данных (поскольку невилика вероятность получения несовместных исходов), однако и тем ниже стойкость против перехвата.

3.1. Атака на протокол B92

Из-за сильного сходства между BB84 и B92, атаки между ними похожи по своей сути, при том что атака на B92 оказывается даже более простой и возможно даже если источник будет строго однофотонным. Отметим, что приведенный алгоритм, строго говоря, не является PNS-атакой, поскольку не задействует как таковой операции разделения фотонов. Однако эта атака кажется даже более серьезной уязвимостью для B92, при которой даже не требуется использования PNS-атаки, поэтому все равно рассмотрим ее. Алгоритм следующий.

Ева проводим у себя то же самое измерение, что должен на своей стороне проводить Боб. Если измерение дало совместный исход, то Ева получает всю информацию о сигнале, а значит может передать его Бобу без ошибок. Если же измерение дало несовместный исход, то Ева блокирует импульс, а использование более качественного канала позволяет ей компенсировать потери.

4. Протокол 4+2

Как мы узнаем дальше, уязвимость к PNS-атаке у BB84 вызвана тем, что после того, как базисы оказались согласованы, Ева может получить точную информацию о передаваемом состоянии. Чтобы избавиться от этой уязвимости, можно состояния внутри каждого из базисов сделать неортоганальными. В таком случае Ева, даже зная базис, не сможет точно определить передаваемое состояние. Если же Ева решит провести то же измерение, что проводит у себя Боб, то она внесет в канал ошибку из-за измерения наугад в выбранном базисе, по которой ее можно будет обнаружить. Поскольку протокол выглядит как смесь BB84 и B92 (применение неортогональных состояний), протокол и называется 4+2. В качестве примера подобной конфигурации стандартным является пример со сферой Пуанкаре, где:

$$|0_x\rangle = \cos\frac{\eta}{2}|0\rangle + \sin\frac{\eta}{2}|1\rangle, \quad |1_x\rangle = \cos\frac{\eta}{2}|0\rangle - \sin\frac{\eta}{2}|1\rangle \tag{9}$$

$$|0_y\rangle = \cos\frac{\eta}{2}|0\rangle + i\sin\frac{\eta}{2}|1\rangle, \quad |1_y\rangle = \cos\frac{\eta}{2}|0\rangle - i\sin\frac{\eta}{2}|1\rangle \tag{10}$$

Наложение векторов можно посчитать как:

$$\langle 0_x|1_x\rangle = \langle 0_y|1_y\rangle = \cos^2\frac{\eta}{2} - \sin^2\frac{\eta}{2} = \cos\eta \tag{11}$$

4.1. Атака на протокол 4+2

Атака производится за счет проведения измерения, которое называется **фильтрацией**:

$$A = \frac{1}{\sqrt{1+\cos\eta}}(|+x\rangle\langle 1_x^\perp| + |-x\rangle\langle 0_x^\perp|), \quad A_? = \sqrt{I - AA^\dagger} \tag{12}$$

Такое измерение в случае успеха состояния из базиса X ортогональными, проецируя их при этом на $|\pm x\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, а в случае неудачи дает несовместный исход. Проблема уязвимости 4+2 заключается в том, что это же измерения ортогонализует состояния и в базисе Y. Докажем это.

Оператор плотности состояния ρ после фильтрации переходит в одно из состояний:

$$\rho_i = \frac{A_i\rho A_i^\dagger}{\mathrm{Tr}\ (A_i\rho A_i^\dagger)} \tag{13}$$

Для ситуации 4+2:

$$\begin{aligned} A|0_y\rangle\langle 0_y|A^\dagger &= \frac{1}{1+\cos\eta}(|+x\rangle\langle 1_x^\perp| + |-x\rangle\langle 0_x^\perp|)\ |0_y\rangle\langle 0_y|\ (|1_x^\perp\rangle\langle +x| + |0_x^\perp\rangle|-x\rangle) = \\ &= \frac{2\cos^2(\eta/2)\sin^2(\eta/2)}{1+\cos\eta}(|+x\rangle\langle +x| + |-x\rangle\langle -x| + i|+x\rangle\langle -x| - i|-x\rangle\langle +x|) = \\ &= (1-\cos\eta)|+y\rangle\langle +y| \end{aligned}$$

Аналогично:

$$A|1_y\rangle\langle 1_y|A^\dagger = (1-\cos\eta)|-y\rangle\langle -y| \tag{14}$$

То есть за счет фильтрации мы свели все снова к ортогональным состояниям, т.е. к атаке на BB84, которую мы уже описали. Получается, что 4+2 тоже незащищен перед PNS-атакой.

5. Протокол SARG04

Как будет показано ниже, уязвимость 4+2 заключается в возможности проведения измерения, которое с ненулевой вероятностью в каждой паре базисов делало состояния ортогональными. Утверждение в том, что общем случае требование для того, чтобы это было невозможно, заключается в том, чтобы вектора не были связаны унитарным преобразованием. Докажем это.

Пусть есть две пары базисов, a и b:

$$a : \{|0_a\rangle, |1_a\rangle\} \tag{15}$$
$$b : \{|0_b\rangle, |1_b\rangle\} \tag{16}$$

А вектора из разных базисов при этом связаны унитарным преобразованием U:

$$\begin{pmatrix}|0_b\rangle\\|1_b\rangle\end{pmatrix} = U\begin{pmatrix}|0_a\rangle\\|1_a\rangle\end{pmatrix} \quad \Leftrightarrow \quad \begin{cases}|0_b\rangle = u_{11}|0_a\rangle + u_{12}|1_a\rangle\\|1_b\rangle = u_{21}|0_a\rangle + u_{22}|1_a\rangle\end{cases} \tag{17}$$

Фильтрация Евы может формально быть записана следующим образом (при проецировании состояния из a на ортогональные состояния $\{|0'_a\rangle, |1'_a\rangle\}$):

$$M|i_a\rangle = \frac{1}{\sqrt{p_a}}|i'_a\rangle, \quad i = 0, 1 \tag{18}$$

Согласно 17, для векторов из b:

$$M|0_b\rangle = M(u_{11}|0_a\rangle + u_{12}|1_a\rangle) = \frac{1}{\sqrt{p_a}}(u_{11}|0'_a\rangle + u_{12}|1'_a\rangle) \tag{19}$$
$$M|1_b\rangle = M(u_{21}|0_a\rangle + u_{22}|1_a\rangle) = \frac{1}{\sqrt{p_a}}(u_{21}|0'_a\rangle + u_{22}|1'_a\rangle) \tag{20}$$

Наложение векторов в базис b после этого преобразования записывается как:

$$|\langle 0'_b|1'_b\rangle| = |u_{11}u_{21} + u_{12}u_{22}| \tag{21}$$

В силу того, что оператор U унитарный, $U = U^\dagger$, $|u_{11}u_{21} + u_{12}u_{22}| = 0$, а значит, всегда можно подобрать такое измерение, что наложения не будет, т.е. будут состояния будут ортогональными. Верно и обратное: если ортогональности не будет, то модуль будет давать что-то положительное, а значит при ортогонализации одной пары будет уменьшаться угол между состояниями другой пары, т.е. они будут становиться менее различимыми, а это значит, что PNS-атака будет неэффективна.

Для SARG04 предлагается следующая конфигурация векторов:

$$|0_a\rangle = \begin{pmatrix}\cos(\eta/2)\\\sin(\eta/2)\end{pmatrix}, \quad |1_a\rangle = \begin{pmatrix}\cos(\eta/2)\\-\sin(\eta/2)\end{pmatrix} \tag{22}$$
$$|0_b\rangle = \begin{pmatrix}\sin(\eta/2)\\-\cos(\eta/2)\end{pmatrix}, \quad |1_b\rangle = \begin{pmatrix}\sin(\eta/2)\\\cos(\eta/2)\end{pmatrix} \tag{23}$$

Это две пары базисов:

$$\{|0_a\rangle, |1_a\rangle\}, \quad \{|0_b\rangle, |1_b\rangle\} \tag{24}$$

Состояния связаны между собой следующими соотношениями:

$$\langle 0_a|1_a\rangle = \cos\eta, \quad \langle 0_b|1_b\rangle = -\cos\eta \tag{25}$$
$$\langle 0_a|0_b\rangle = \langle 1_a|1_b\rangle = 0 \tag{26}$$
$$\langle 0_a|1_b\rangle = \langle 1_a|0_b\rangle = \sin\eta \tag{27}$$

Вектора базисов между собой связаны следующим преобразованиями:

$$|0_b\rangle = c\,|0_a\rangle + c'\,|1_a\rangle \tag{28}$$
$$|1_b\rangle = c'\,|0_a\rangle + c\,|1_a\rangle \tag{29}$$

Здесь были введены соотношения:

$$c = -\frac{\cos\eta}{\sin\eta}, \quad c' = \frac{1}{\sin\eta} \tag{30}$$

Значение перекрытия тогда равно:

$$|cc' + c'c| = 2|cc'| = 2\left|\frac{\cos\eta}{\sin^2\eta}\right| \geq |\cos\eta| \tag{31}$$

Видно, что при $\eta \neq 0$ перекрытие ненулевое, а значит, данный алгоритм может противостоять PNS-атаке.

Конечно, стойкость может быть нарушена, если Ева в состоянии блокировать все одно- и двуфотонные импульсы, а в трехфотонных импульсах измерять два фотона в различных базисах, блокируя импульс, если получении хотя бы одного несовместного исхода. Если $\eta < \pi/4$, то вероятность несовместного исхода при хотя бы одном измерении оказывается большей $\cos^2(\pi/4) = 1/2$. Это означает, что для того, эффективного прослушивания нужно уметь блокировать и трехфотонные посылки (которых оказывается нужно блокировать не так мало). Итого мы имеем, что протокол оказывается уязвимым в случае, когда Ева в состоянии блокировать и одно-, и двух-, и трехфотонные посылки, а это уже существенно большая защищенность, чем, например, у BB84.

Существует также частный случай, при котором рассматривается угол $\eta = \pi/4$, тогда после поворота сигнальными состояниями можно считать (как в BB84) $|\pm z\rangle$ и $|\pm z\rangle$. Алиса в таком протоколе называет одну из четырех пар состояний $A_{m,n}; m, n \in \{\pm\}$, а Боб случайно измеряет компоненту σ_x или σ_z. Полагается, что "0" кодируется $|\pm x\rangle$, а "1" — $|\pm z\rangle$, т.е., например, если Алиса хочет послать "1", то она может, например, послать $|-z\rangle$ и объявить $A_{+,-}$. Тогда Боб достоверно распознает этот результат, только если мерил σ_x и получил -1. Все остальное не даст ему достоверности: при получении $+1$ он не сможет отличить Алисины "0" в базисе σ_x и что угодно в базисе σ_z; если же он измерит σ_z, то он получит -1, но не сможет узнать, из какого базиса состояние посылалась Алисой. Это означает, что после согласования базисов совпадет лишь четверть пересланных сигналов, а скорость становится в два раза меньше, чем, например, в BB84.