Стратегии Евы в BB84

Обозначения:
+ – прямой базис
X – диагональный базис

Речь идёт только о просеянных ключах, поэтому случаи, когда базисы Алисы и Боба не совпадают, не рассматриваются как не дающие вклада.

1 Ева не крутит базисы при чтении

1.1 Ева не крутит базисы ни при чтении, ни при отправке

Наиболее простая ситуация: в половине случаев Ева угадывает с базисом, Боб получает неискаженную информацию, а сама Ева знает, какое значение было отправлено Алисой и получено Бобом. Во второй половине случаев Ева ошибается с выбором базиса. Тогда информацию она не получает, но с вероятностью 50% Боб измеряет то значение, которое отправила Алиса (так как ему приходит случайное значение).

Базис Алисы и Боба	Базис Евы для чтения и отправки	Вероятность Бобу получить неискаженную информацию	Результат для Евы
+	+	100%	Знает этот бит
+	X	50%	Не знает этот бит
X	+	50%	Не знает этот бит
X	X	100%	Знает этот бит

Процент несовпадений в ключе: $1 - (\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2}) = 25\%$
Процент бит ключа, известных Еве: 50%

1.2 Ева не крутит базисы при чтении, но крутит при отправке

Пусть теперь при отправке Ева будет выбирать базис случайным образом. Различных равновероятных вариантов теперь восемь. Первые четыре совпадают с ситуацией, где Ева базис не крутит при отправке. В оставшихся четырёх вариантах Ева меняет базис на противоположный. В результате этого в 50% угадывает с базисом при чтении и получает информацию о значении, отправленном Алисой. Но что получил Боб, она знать не может. В 50% случаев она ошибается с базисом при чтении, то есть получает случайное значение, но отправляет в том базисе, в котором измерит его Боб. Таким образом, она не знает значение этого бита у Алисы, но знает у Боба.

Базис Алисы и Боба	Базис Евы для чтения	Базис Евы для отправки	Вероятность Бобу получить неискаженную информацию	Результат для Евы
+	+	+	100%	Знает этот бит
+	X	X	50%	Не знает этот бит
X	+	+	50%	Не знает этот бит
X	X	X	100%	Знает этот бит
+	+	X	50%	Знает этот бит только у Алисы
+	X	+	50%	Знает этот бит только у Боба
X	+	X	50%	Знает этот бит только у Боба
X	X	+	50%	Знает этот бит только у Алисы

Процент несовпадений в ключе: $1 - (\frac{2}{8} + \frac{6}{8} \cdot \frac{1}{2}) = 37.5\%$
Процент бит ключа, известных Еве: 25%, + в ещё 25% случаев знает значение в ключе Алисы, но не может знать, совпадает ли с ним значение в ключе Боба, а в других 25% знает значение в ключе Боба, но не знает значение в ключе

Алисы.

То есть Ева знает 50% ключа Алисы и 50% ключа Боба, только теперь между ключами Алисы и Бобы несовпадений больше.

2 Ева крутит базисы при чтении

На самом деле эта ситуация ничем не будет отличаться от той, где Ева выбирает какой-либо один базис и измеряет в нём все посылки Алисы. Если рассматривать ключ длиной $n = 1$ (то есть одну отдельную посылку), то вообще нельзя сказать, "крутит"ли Ева базис, или же выбрала один – эти ситуации тождественны, а значит и для $n > 1$ они будут тождественны.

Значение имеет только то, отправит ли Ева посылку Бобу в том же базисе или же выберет базис для отправки случайным образом. Выбранный же для чтения базис в 50% случаев совпадёт с базисом Алисы и в 50% не совпадёт вне зависимости от того, одининаковый он для всех посылок или выбирается случайным образом.

3 Выводы

- Нет никакой разницы между ситуациями, где Ева крутит базис при чтении и где она выбирает какой-либо один и все посылки измеряет в нём.
- Крутить базисы при отправке не выгодно для Евы: это увеличивает количество несовпадений в ключах Алисы и Боба.
- Наилучшая для Евы стратегия даёт 25% несовпадений в ключах Алисы и Боба. Таким образом, 25% и более несовпадений сигнализирует Алисе и Бобу о присутствии злоумышленника в системе.