Security of BB84 QKD Protocol

Michael Ben-Or

Prouf Outline

1. The qauntum communication complexity of the function

$$f(x,y) = \sum_{i=1}^{n} x_i y_i \pmod 2$$

$x, y \in \{0,1\}^n$

is high $(\Omega(n))$

A $\qquad\qquad\qquad$ B

x $\qquad\qquad\qquad$ y

$\longrightarrow$

$\longleftarrow$

$\longrightarrow$ $\quad$ k qubits exchanged

$\longrightarrow$ $\quad$ $h(x,y)$

<u>Thm [ASTVW]</u>

If $\Pr(h(x,y)=f(x,y)) \geq \frac{1}{2}+\frac{1}{2^{\ell}}$

then $k \geq \frac{1}{2}(n-\ell+1)$

For one-way communication

$$k \geq n-\ell+1$$

Proof Outline (Cont.)

A $\xrightarrow{\text{n-qubits}}$ B

random S
random basis
sequence b

$\longleftarrow$ error
$\longrightarrow$ corection
etc.

If Eve has a small amount of information about S, with high probability we can compress this information to few, $\lambda \cdot n$ qubits!
($\lambda \ll 1$)

<u>Goal:</u> Show that if the probability of not detecting Eve is $> 2^{-\delta n}$ then we can compress Eve's state to $\lambda \cdot n$ qubits for some $\lambda < 1$.

For random $y \in \{0,1\}^n$ given later Eve cannot predict $f(s,y) = s \cdot y \pmod 2$ better than $\frac{1}{2} + \frac{1}{2^{(1-\lambda)n}}$

$$\left[t \text{ Times} \qquad \frac{1}{2^{(1-\lambda)n - t/2}} \right]$$

$$|\varphi_E\rangle|I\rangle \xrightarrow{\mathcal{U}_E} \sum_J |\varphi_{IJ}\rangle|J\rangle$$

$$|I\rangle \rightarrow \sum_{J,K} |\psi_{JK}\rangle X_J Z_K (|I\rangle)$$

where

$$|\psi_{JK}\rangle = \frac{1}{2^n} \sum_S (-1)^{S\cdot K} |\varphi_{S, S\oplus J}\rangle$$

Note: $\sum_{J,K} \|\psi_{JK}\|^2 = 1$

$$\sum_{JK} \langle\psi_{JK}|\psi_{JK}\rangle = \frac{1}{2^{2n}} \sum_{S_1 S_2 JK} (-1)^{(S_1\oplus S_2)\cdot K} \langle\varphi_{S_1, S_1\oplus J}|\varphi_{S_2, S_2\oplus J}\rangle$$

$$= \frac{1}{2^n} \sum_{SJ} \langle\varphi_{S, S\oplus J}|\varphi_{S, S\oplus J}\rangle = \frac{1}{2^n} 2^n = 1$$

One Qubit

$$|s\rangle \longrightarrow \left[|\Psi_{00}\rangle I + |\Psi_{01}\rangle Z + |\Psi_{10}\rangle X + |\Psi_{11}\rangle XZ \right](|s\rangle)$$

$s \in \{0,1\}$

Let $b=0$ denote the base 

$b=1$ " " " 

Eve's state when Bob has no error

$b=0 \quad s\in\{0,1\} \quad |\Psi_{00}\rangle + (-1)^s |\Psi_{01}\rangle$

$b=1 \quad s\in\{0,1\} \quad |\Psi_{00}\rangle + (-1)^s |\Psi_{10}\rangle$

$$\Rightarrow \quad |\Psi_{00}\rangle\langle\Psi_{00}| + \tfrac{1}{2}|\Psi_{01}\rangle\langle\Psi_{01}| + \tfrac{1}{2}|\Psi_{10}\rangle\langle\Psi_{10}|$$

If Bob detects an error

$$\left.\begin{array}{ll} b=0 & |\Psi_{10}\rangle + (-1)^s |\Psi_{11}\rangle \\ b=1 & |\Psi_{01}\rangle + (-1)^s |\Psi_{11}\rangle \end{array}\right\} \Rightarrow$$

$$\tfrac{1}{2}|\Psi_{01}\rangle\langle\Psi_{01}| + \tfrac{1}{2}|\Psi_{10}\rangle\langle\Psi_{10}| + |\Psi_{11}\rangle\langle\Psi_{11}|$$

In general if the errors are at E we get for $b = 0 \cdots 0$ $\quad s \in \{0,1\}^n$

$$\sum_K |\psi_{E,K}\rangle (-1)^{K \cdot s}$$

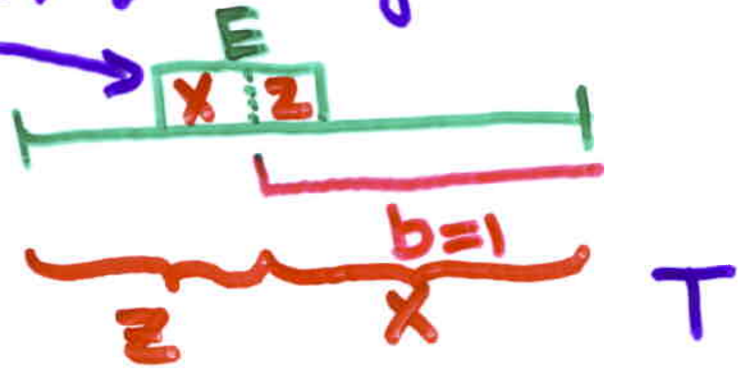
$$\sum_s \frac{1}{2^n} |-''-\rangle\langle -''-| =$$

$$= \sum_K |\psi_{E,K}\rangle\langle \psi_{E,K}|$$

For general $b \in \{0,1\}^n$ we get

must have

possible



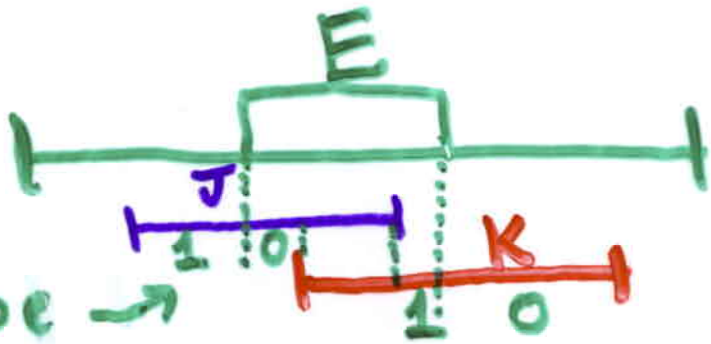
$$\sum_T |\psi_{(E \setminus b) \cup (T \cap b),\, (E \cap b) \cup (T \setminus b)}\rangle (-1)^{T \cdot s}$$

$\Rightarrow \sum_T |\cdots\rangle\langle\cdots|$ when summing over $s \in \{0,1\}^n$

Summing over $b \in \{0,1\}^n$ we get

$$\sum_{\substack{J,K \\ J\cap K \subseteq E \subseteq J\cup K}} |\psi_{J,K}\rangle\langle\psi_{J,K}| \cdot 2^{-|J\oplus K|}$$

b must be →



b must be

error for any b on $J\cap K$

# of fixed b's $= |J\oplus K|$

$$\rho_{\substack{\text{small}\\ \text{error}}} = c \cdot \sum_{|E| < \epsilon n} \sum_{\substack{J,K \\ J \cap K \subseteq E \subseteq J \cup K}} |\psi_{JK}\rangle\langle\psi_{JK}| \cdot 2^{-|J \oplus K|}$$

What is the coef. of $|\psi_{JK}\rangle\langle\psi_{JK}|$

$|J \cup K| = a$, $|J \cap K| = b$

$2^{-|J \oplus K|} = 2^{-(a-b)}$

We have to choose E of size $\leq \epsilon n - b$ out of $a-b$ elements

$$2^{-(a-b)} \cdot \sum_{l=0}^{\epsilon n - b} \binom{a-b}{l} \leq 2^{-(a-b)\left[1 - H\left(\frac{\epsilon n - b}{n(a-b)}\right)\right]}$$

$$< 2^{-\delta n}$$

for $a = |J \cup K| \geq (2\epsilon + \eta) n$

$$\rho_{\substack{\text{small}\\\text{error}}} = c \cdot \Bigg[\sum_{\substack{J,K \\ |J \cup K| < (2\epsilon+\eta)n}} c_{JK} |\psi_{JK}\rangle\langle\psi_{JK}| + \sum_{\substack{J,K \\ |J \cup K| \geq (2\epsilon+\eta)n}} c_{JK} |\psi_{JK}\rangle\langle\psi_{JK}| \Bigg]$$

$c = 1/\text{Probability of small error} < 2^{\delta n}$

$\Rightarrow$ Coef. of big $|J \cup K|$ is $< 2^{-(\delta_1 - \delta)n}$

$\Rightarrow$ $\boxed{\rho_{\substack{\text{small}\\\text{error}}} \text{ can be approximated very well by first sum}}$

$\tilde{\rho}$ is supported by the space spanned by all the small $|\psi_{JK}\rangle$ (J,K)

# of small $|J \cup K| \leq (2\epsilon+\eta)n$ can be bounded by

$$2^{n[H(2\epsilon+\eta)+2\epsilon+\eta]}$$

$\Rightarrow$ Eve's state can be approximated by $n \cdot [H(2\epsilon+\eta)+2\epsilon+\eta]$ qubits!

Error correction reveals another $n \cdot H(\epsilon)$ bits giving a total of

$$n\left[H(\epsilon)+H(2\epsilon+\eta)+2\epsilon+\eta\right]$$

qubits

Bound on ϵ

We need

$$H(\epsilon) + H(2\epsilon) + 2\epsilon < 1$$

$$\Rightarrow \quad \epsilon < 6.199\%$$

Imperfect A

Can handle any source that can be described by λn qubits together with a perfect source.