Simple Security Proof for QKD

Michael Ben-Or
The Hebrew Univ.

Proof Outline

The quantum communication complexity of the function

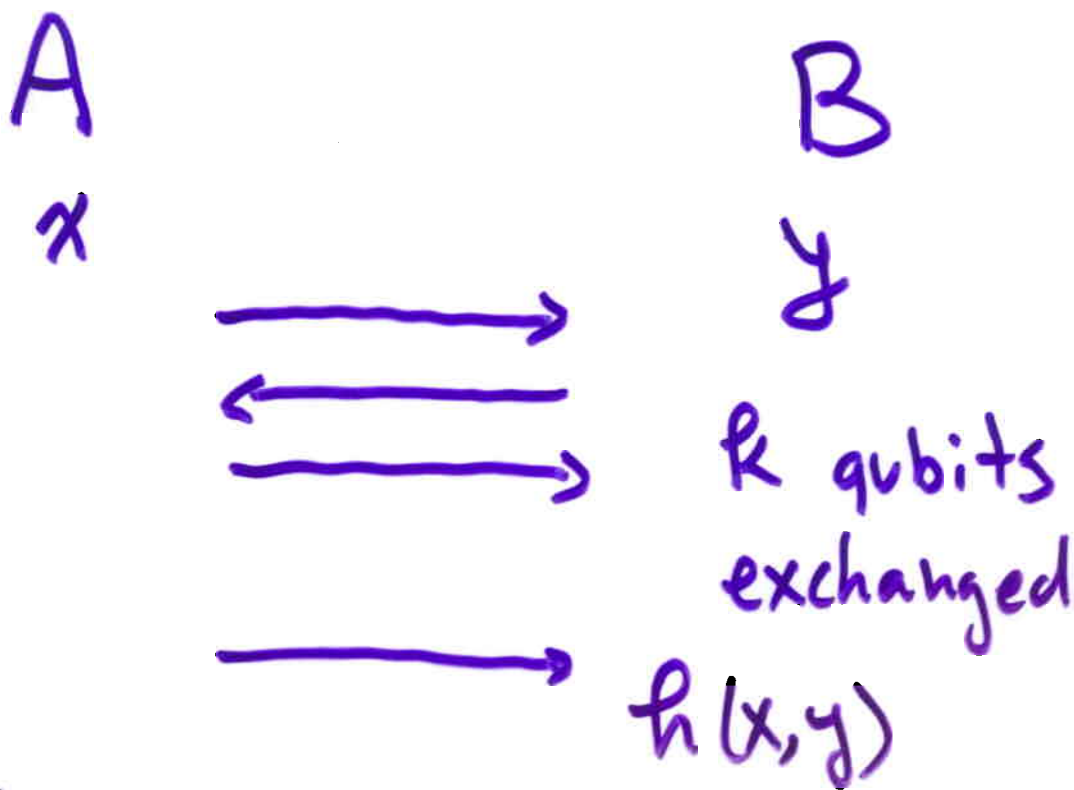
$$f(x,y) = \sum_{i=1}^{n} x_i y_i \pmod 2$$

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

is high $(\Omega(n))$

This is true for $f(x,h) = h(x)$

$x \in \{0,1\}^n$, $h \in \{\text{Universal hash function collection}\}$



Thm [ASTVW]

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

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

$\longleftarrow$
$\longrightarrow$

error
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!

$(\lambda \ll 1)$

Goal: 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 $\frac{1}{2} + \frac{1}{2^{(1-\lambda)n}}$

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

EPR pair via noisy channel

(I) Alice prepares n EPR pairs

$$\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes n}$$

and sends half of each pair to Bob.

(II) A & B agree on random selection of X, Z measurements (publicly) and measure.

(III) A & B run error correction:

If "fail" they abort

Else apply privacy amplification

Notation:

$$\Phi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Bell Basis: Apply to Φ

$I \otimes Z$ $\quad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

$I \otimes X$ $\quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

$I \otimes XZ$ $\quad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

Bell Basis for $\mathcal{H}_A \otimes \mathcal{H}_B$

$J \subset \{1, \dots, n\}$, $K \subseteq \{1, \dots, n\}$, $I \in \{0,1\}^n$

$$\Phi^{\otimes n} = \frac{1}{2^{n/2}} \sum_I |I, I\rangle$$

X_J = apply X to coordinates in J
Z_K = " Z " " in K

Bell Basis

$$\Phi_{J,K} = \frac{1}{2^{n/2}} \sum_I |I, X_J Z_K (I)\rangle$$

Purify Eve's attack the state of the system after phase (I)

$$\rho = \sum_{J,K} |\Phi_{J,K}, \Psi_{J,K}\rangle$$

where $\Psi_{J,K}$ some (un normalized) vectors in Eve's space

$$= \frac{1}{2^{n/2}} \sum_{J,K} \sum_{I} |I, X_J Z_K(I), \Psi_{JK}\rangle$$

Testing:

Alice and Bob measure $X \otimes X$ or $Z \otimes Z$ on each pair and these commute so probabilities behave as classical.

Error correction test check that if Alice & Bob would measure in the Bell Basis they will fall with probability $1 - 1/2^{\alpha n}$ to the space with not to many X, Z, XZ coordinates.

Define

$$\mathcal{H}_{good} = \{ \Phi_{J,K} \mid |J| < \varepsilon n, |K| < \varepsilon n \}$$

$$\mathcal{H}_{good} \otimes \mathcal{H}_E \subseteq \mathcal{H}_{ABE}$$

P projection on

$$\rho' = \frac{\langle P | \rho | P \rangle}{\mathrm{Tr}(P\rho)}$$

has fidelity $1 - 1/2^{\beta n}$ to ρ

if test succeeds.

$$\dim \mathcal{H}_{good} \le 2^{2nH(\varepsilon)}$$

if the error rate is $< \varepsilon$.

$\Rightarrow$ Eve's state is supported by a space of the same dimension $\sim 2nH(\varepsilon)$ qubits

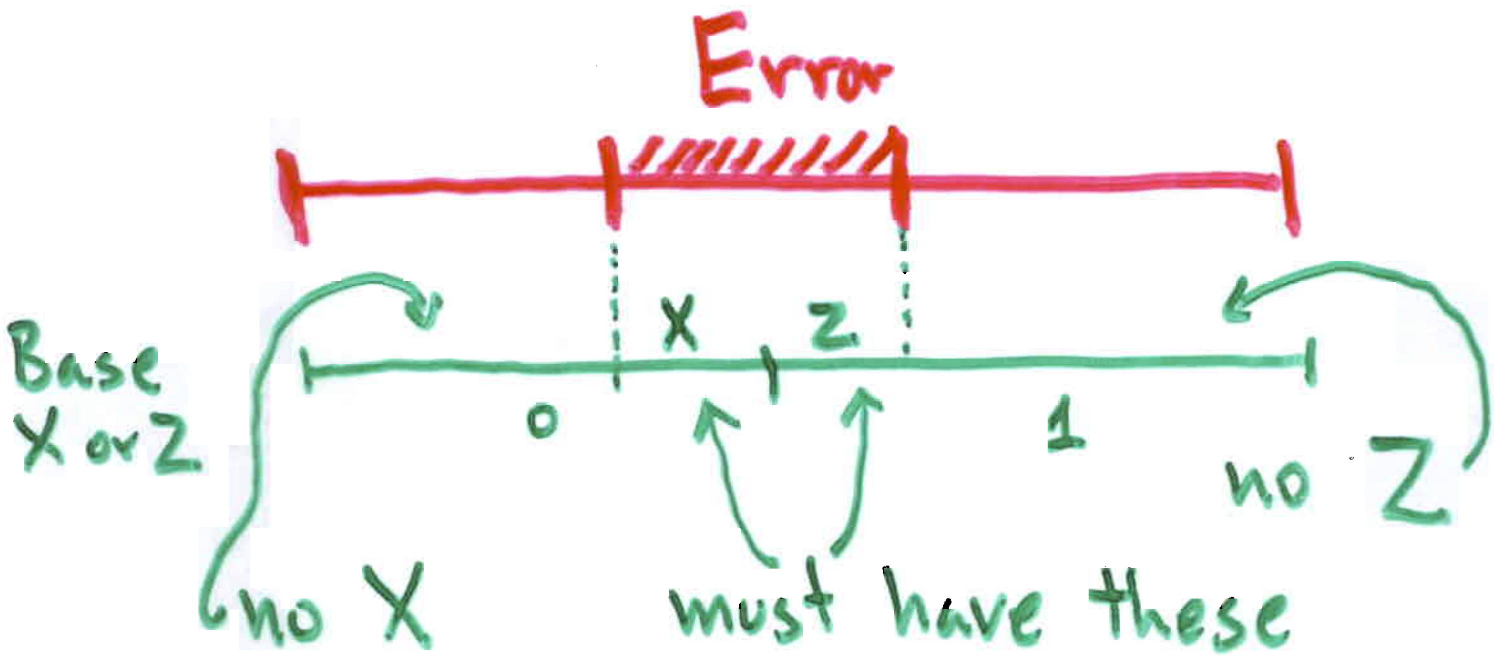
The error correcting phase reveals $nH(\varepsilon)$ bits giving a total of $3nH(\varepsilon)$ qubits for Eve's state.

$$3nH(\varepsilon) < n$$

$$3H(\varepsilon) < 1$$

$$\varepsilon \approx 6\%$$

Better bounds on ε:



known error reduces the dim of $\mathcal{H}_{good}$ to

$$2^{\frac{n}{2}H(\varepsilon)} \times 2^{\frac{n}{2}H(\varepsilon)} = 2^{nH(\varepsilon)}$$

so with error correction

$$2H(\varepsilon) < 1 \implies \epsilon \sim 11\%$$

Errors:

Koashi Preskill show that dim $\mathcal{H}_{good}$ does not change.

GLLP: Handle many cases but all are easier to analyze by bounding the support of Eve's state.

$$\begin{tikzcd} A \arrow[r] & \boxed{\text{Fred}} \arrow[r] \arrow[rr, bend right, leftrightarrow] & \text{Eve} \arrow[r] & \boxed{\text{Fred}} \arrow[r] & \text{Bob} \end{tikzcd}$$

prob δ for >1 photon

$nH(\delta)$ $\qquad$ $2H(\varepsilon) + H(\delta) < \underline{1}$