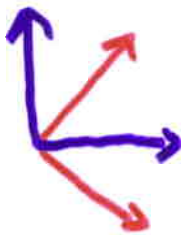
# Security of Quantum Key Distribution Protocols

Michael Ben-Or

(Following Lo & Chau)

# History

BB 84



Ekert 91

$|00\rangle + |11\rangle$

? B92


96 →

Lo-Chan '98

Mayers '98 , BBBMR '99

Shor-Preskill '00

Ben-Or '00

# Ekert 91 / Lo-Chau 98

(I) Alice (or Eve) prepares EPR pairs and send half of each pair to Bob

(II) Alice & Bob perform Entanglement Purification

(III) Measurement of almost clean EPR pairs.

# Bell Basis for 2-qubits

$$\phi^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

$$\psi^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

Testing a pair: $\psi^-$

measure with equal probability

X-axis, y-axis, z-axis

outcome should always be different

| | | | | |
|---|---|---|---|---|
| x-axis | OK for | $\psi^-$, $\phi^-$ | H |
| y-axis | OK for | $\psi^-$, $\phi^+$ | (!,!) |
| z-axis | OK for | $\psi^-$, $\psi^+$ | I |

# Classical Game

P sends N object of type

W, X, Y, Z

claiming all are of type W

We can distinguish $\{W,X\}$ from $\{Y,Z\}$

or $\{W,Y\}$ " $\{X,Z\}$

or $\{W,Z\}$ " $\{X,Y\}$

Prob. testing N-1 that the last one is not W

$$\leq \frac{e}{N}\left(\frac{1}{3}\right)^{e-1} \leq \frac{1}{N}$$

(if e are not W)

# Quantum Scheme

Eve prepares

$$|u\rangle = \sum_{0 \le i_1 \cdots i_N \le 3} \sum_{j} \alpha_{i_1 \cdots i_N j} |i_1 \cdots i_N\rangle \otimes |j\rangle$$

P-cheating =

$$= \frac{1}{N 3^{N-1}} \sum_{S_1} \sum_{S_2} \sum_{S_3} \sum_{i_1 \cdots i_N}{}' \sum_{j} |\alpha_{i_1 \cdots i_N j}|^2$$

$|S_1 \cup S_2 \cup S_3| = N-1$, $S_i$ disjoint

$\sum'$ = $l \in S_1$ $i_l = 2,3$

$l \in S_2$ $i_l = 0,3$

$l \in S_3$ $i_l = 1,3$

(index 3 - $\Psi^-$)

# Quatum to Classical

Eve prepares $|\psi\rangle = \cdots$

and measures $|\psi\rangle$ in the Bell basis

$$\rho = \sum_{i_1 \cdots i_n} |\alpha_{i_1 \cdots i_n, j}|^2 |i_1\rangle\langle i_1| \cdots |i_n\rangle\langle i_n| \, |j\rangle\langle j|$$

and sends this to Alice & Bob

Probability of cheating is exactly the same!

Better error bounds with hashing test P-error $< 2^{-m}$

same quantum to classical reduction

After testing

$$\langle \psi^{-\otimes N} | \rho_{AB} | \psi^{-\otimes N} \rangle \geq 1 - 2^{-m} = \delta$$

$\Rightarrow$ Eve's information

$$S(\rho_E) = S(\rho_{AB}) \leq H(\delta) + N \cdot \delta$$

Now Alice & Bob measure and obtain a random Key of which Eve has essentially no information

# Handling Errors

Use quantum computation codes working on "logical qubits" instead of unprotected qubits.