Entanglement $\implies$ Secrecy

Suppose Alice and Bob share a Bell state

\[
\Phi^+ = \frac{1}{2}(|00\rangle + |11\rangle)
\]

Alice measures w/ \{|0\rangle , |1\rangle\} to obtain $k$. Bob measures similarly to obtain $k'$. Then $k = k'$, and no one can guess these bits.

Suppose Alice has a secret msg. $m_1, \ldots, m_n \in \{0, 1\}$.

<table>
<thead>
<tr>
<th>Protocol:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Alice and Bob share $n$ Bell states, and measure them to produce a shared key $k_1, \ldots, k_n \in {0, 1}$.</td>
</tr>
</tbody>
</table>
| \[
\begin{array}{c}
\text{Alice} \\
\text{public channel} \\
\text{Bob}
\end{array} \\
\text{O} \quad \text{O} \quad \text{O}
\]
| 2. Alice sends Bob $m_1 \oplus k_1, \ldots, m_n \oplus k_n$. |
| 3. Bob recovers $m$ (by XORing again with $k_1, \ldots, k_n$). |
Upside: Complete security.

Downsides: Requires trusting the state distribution & measurements.

Can we do better?

**Quantum Key Distribution**

Classical crypto is based on computational hardness assumptions. Quantum crypto is based on physical assumptions.


A simple eavesdropping scenario:

![Eavesdropping Scenario Diagram]

Can Alice and Bob share a key?

Let $\phi$ be a unit vector in $\mathbb{C}^2 \otimes \mathbb{C}^2$ such that (X and Z measurements tend to agree):

$$\langle \phi | X \otimes X | \phi \rangle \geq 1 - \epsilon, \quad (1)$$

$$\langle \phi | Z \otimes Z | \phi \rangle \geq 1 - \epsilon. \quad (2)$$

Then,

$$\left\langle \phi \left| \frac{X \otimes X + Z \otimes Z}{2} \right| \phi \right\rangle \geq 1 - \epsilon. \quad (3)$$

By calculation,

$$\frac{X \otimes X + Z \otimes Z}{2} = |\Phi^+\rangle \langle \Phi^+ | - |\Psi^-\rangle \langle \Psi^- | \leq |\Phi^+\rangle \langle \Phi^+ |,$$  

(4)

(where $\Psi^- = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$) so

$$\langle \phi | \Phi^+ \rangle^2 \geq 1 - \epsilon, \quad (5)$$
which implies $\langle \phi | \Phi^+ \rangle \geq 1 - \epsilon$.

A state for which $X$ and $Z$ measurements tend to agree must be close to $\Phi^+$.

**Protocol (similar to BB84):**

1. Alice prepares $\Phi^+$ and sends one qubit to Bob.
2. Alice and Bob each (independently) choose either basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ at random and measure. $k :=$ Alice’s output, $k' :=$ Bob’s output.
3. Repeat to obtain $k_1, \ldots, k_n$ and $k'_1, \ldots, k'_n$.
4. Alice and Bob share their basis choices and discard any rounds in which they disagreed.
5. Alice and Bob randomly compare an $n/4$-subset of their bits. If more than $\epsilon n$ of them disagree, abort.
6. Label remaining bits as $s_1, s_2, \ldots$ (for Alice) and $s'_1, s'_2, \ldots$ (for Bob). (Roughly $n/4$ bits for each.)

Classical sampling arguments imply (w/ probability $\to 1$):

- $s$ and $s'$ are close in Hamming distance.
- $s$ is highly unpredictable to Eve. (*s cannot be guessed except with exponentially small probability.*)

Perform information reconciliation:
Performs privacy amplification:

\[ z = F(s) \]

Then, \( z \) is uniform to Eve.

A different eavesdropping scenario:

\[ \text{classical channel} \]

Security proof can be extended to this case.

Yet another eavesdropping scenario:

"Device-independent" scenario. Harder.