CMSC 858K - Quantum Key Distribution

Carl Miller

December 8, 2016

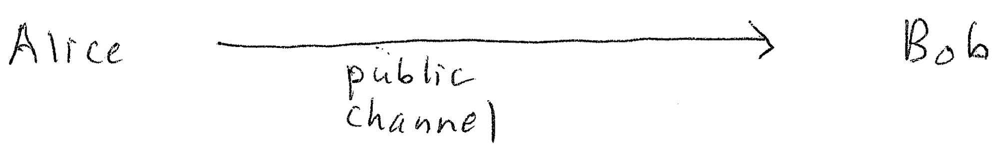
Entanglement $\Longrightarrow$ Secrecy

Suppose Alice and Bob share a Bell state

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

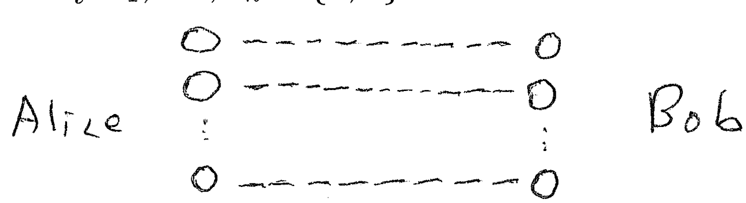
Alice measures w/ $\{|0\rangle, |1\rangle\}$ to obtain k. Bob measures similarly to obtain k'. Then $k = k'$, and no one can guess these bits.

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



Protocol:

1. Alice and Bob share n Bell states, and measure them to produce a shared key $k_1, \ldots, k_n \in \{0, 1\}$.



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.

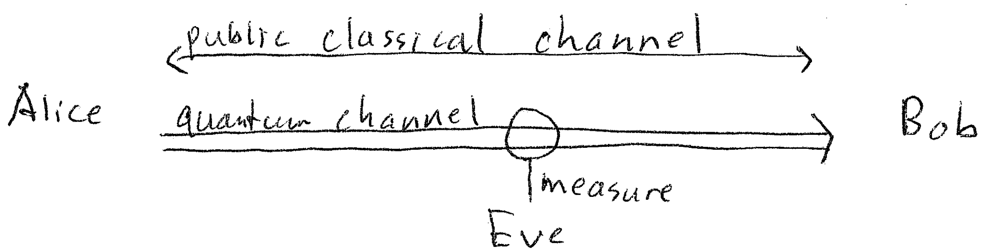
Can we do better?

Quantum Key Distribution

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

[Bennett-Brassard 1984] proposed QKD (based on [Wiesner 1983]). Security proofs followed and are still evolving today.

A simple eavesdropping scenario:



Can Alice and Bob share a key?

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

$$\langle\phi| X \otimes X |\phi\rangle \geq 1 - \epsilon, \tag{1}$$
$$\langle\phi| Z \otimes Z |\phi\rangle \geq 1 - \epsilon. \tag{2}$$

Then,

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

By calculation,

$$\frac{X \otimes X + Z \otimes Z}{2} = \left|\Phi^+\right\rangle \left\langle\Phi^+\right| - \left|\Psi^-\right\rangle \left\langle\Psi^-\right| \leq \left|\Phi^+\right\rangle \left\langle\Phi^+\right|, \tag{4}$$

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

$$\left\langle \phi \mid \Phi^+ \right\rangle^2 \geq 1 - \epsilon, \tag{5}$$

which implies $\langle \phi \mid \Phi^+ \rangle \geq 1 - \epsilon$.

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

Protocol (similar to BB84):

1. Alice prepares Φ^+ 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 ϵn 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:

Alice $\xrightarrow{\quad e \quad}$ Bob

s $\qquad$ $\cancel{s'}$ $\quad s^{\#}$

Perform privacy amplification:

Alice

$z := f(s)$

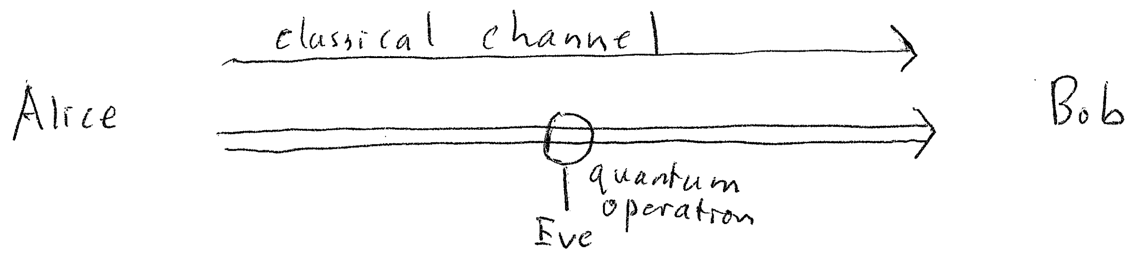
Bob

$z := f(s)$

(f = random function)
(z is shorter than s)

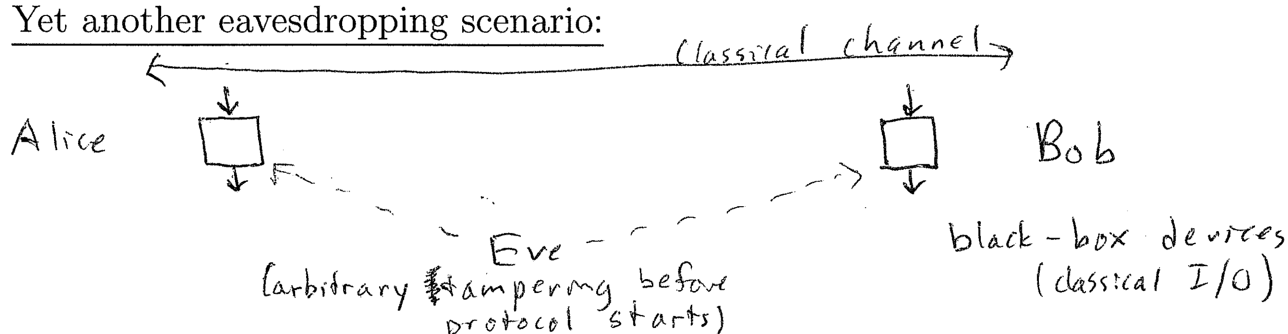
Then, z is $\approx$ uniform to Eve.

A different eavesdropping scenario:



Security proof can be extended to this case.

Yet another eavesdropping scenario:



"Device-independent" scenario. Harder.