CSCE 785
11/14/2023

Quantum Cryptography

The BB84 key exchange protocol

Goal: Alice & Bob want to communicate secretly.

If they share some secret, uniformly random bits $r \in \{0,1\}^n$ then for any message m Alice wants to send to Bob, where $|m| = |r|$, she does as follows:

- computes $c := m \oplus r$
- sends $\boxed{c}$ to Bob over a public channel
- Bob computes $c \oplus r = m \oplus r \oplus r = m$

m = cleartext, or plaintext; c = ciphertext

Eavesdropper Eve only sees c, which is completely uncorrelated with m (Eve doesn't know r.)

One-time pad — A & B should not re-use r for another message. Otherwise,
Eve gets $m \oplus r$ and $m' \oplus r$
computes $m \oplus r \oplus m' \oplus r = m \oplus m'$

Upshot: to send a secret message, it is enough to share secret, uniformly random bits (the key)

BB84 provides a quantum protocol to share a secret random key.

<u>Def</u>: Let $\mathcal{H}$ be a d-dim $\mathbb{C}$-space & let $\mathcal{B} := \{b_1, \ldots, b_d\}$, $\mathcal{C} := \{c_1, \ldots, c_d\}$ be two orthonormal bases for $\mathcal{H}$. We say that $\mathcal{B}$ & $\mathcal{C}$ are <u>mutually unbiased</u> if $\forall i, j$

$$|\langle b_i, c_j \rangle|^2 \left(= 2^{-d/2}\right) \text{ independent of } i, j.$$

A collection of bases is mut. unbiased if any pair of them is mut. unbiased.

For $\mathbb{C}^2$: $\{\underset{|0\rangle}{|\uparrow\rangle}, \underset{|1\rangle}{|\downarrow\rangle}\}$, $\{\underset{|+\rangle}{|\rightarrow\rangle}, \underset{|-\rangle}{|\leftarrow\rangle}\}$, and $\{|\times\rangle, |\odot\rangle\}$ are mutually unbiased

BB84 uses two of these bases: $\updownarrow := \{|\uparrow\rangle, |\downarrow\rangle\}$ and $\leftrightarrow := \{|\rightarrow\rangle, |\leftarrow\rangle\}$

$$|\langle \uparrow | \rightarrow \rangle| = \frac{1}{\sqrt{2}}$$

<u>The protocol</u>: Assumptions:

A & B share an insecure q-channel
a classical public channel

(1) Done for $j := 1$ to n (for some large n):

Indep. for each j:
- Alice chooses a bit $b_j \in \{0, 1\}$ at random
- " chooses a basis $\mathcal{B}_j \in \{\updownarrow, \leftrightarrow\}$ at random

" prepares $|b_j\rangle_{\mathcal{B}_j}$ with respect to $\mathcal{B}_j$:

$b_j = 0$: $|\uparrow\rangle$ or $|\rightarrow\rangle$

$b_j = 1$: $|\downarrow\rangle$ or $|\leftarrow\rangle$

- Sends $|b_j\rangle_{\mathcal{B}_j}$ to Bob over the quantum channel
- Bob gets some state $|\psi\rangle \in \mathbb{C}^2$
- Bob chooses a basis $\mathcal{C}_j \in \{\updownarrow, \leftrightarrow\}$ unif. at random. (u.a.r.)
- Measures $|\psi\rangle$ with respect to this basis, $\mathcal{C}_j$, obtaining a bit $c_j \in \{0,1\}$

end of quantum portion of the protocol

(2) Bob has bits $c_1 \ldots c_n$ (A & B discard useless bits)

~~Bob chooses a random subset~~ $\cancel{C \subseteq \{1,\ldots,n\}}$

Bob t/ - ~~tells Alice what~~ $\cancel{C}$ ~~is and what~~ $\cancel{c_j}$ ~~is for every~~ $\cancel{j \in C}$. ~~and what~~ $\cancel{\mathcal{C}_j}$ ~~was for each~~ $j \in \{1,\ldots,n\}$

$\cancel{|C| \approx \frac{n}{2}}$.

- Bob tells Alice what $\mathcal{C}_j$ is for all $j \in \{1,\ldots,n\}$
- Alice ~~tess~~ tells Bob $R := \{j : \mathcal{B}_j = \mathcal{C}_j\}$
- Then discard the bits b_j, c_j for $j \notin R$. (about $\frac{n}{2}$ bits)

(3) Security Check: Bob chooses a random subset $S \subseteq R$, tells Alice S (S = security check)

$|S| \approx \frac{1}{2}|R| \approx \frac{n}{4}$

- ~~Bob tel~~ Alice tells Bob ~~what S is~~ what b_j is for every $j \in S$.
- Bob checks whether $b_j = c_j$ for all $j \in S$.
  If yes, then Bob tells Alice to accept the protocol, ~~and Alice & Bob share (secretly) the the bits $b_j \stackrel{?}{=} c_j$ for all $j \in R \setminus S$ (about $\frac{n}{4}$ bits)~~
  That is, they assume the bits in $R \setminus S$ are a shared random secret. (about $\frac{n}{4}$ bits).
- Otherwise, if Bob finds ~~somg~~ some $j \in S$ such that $b_j \neq c_j$, then Bob tells Alice to reject the protocol. They will start over from the beginning.

Assume: Eve gets info in two ways:
- measures state in either $\updownarrow$ or $\Leftrightarrow$ basis.
- prepares a state consistent with her measurement & sends this to Bob.

Case 1: Eve chooses, for j^{th} qubit, basis $\mathcal{B}_j$
($j \in R$) — Eve gets perfect info about b_j
and can send same state to Bob, undetected.

[prob $\frac{1}{2}$]

Case 2: Eve choose the other basis (not $\mathcal{B}_j$), gets no info about b_j & sends a qubit in the wrong basis to Bob.

- Bob gets the same bit Alice sent (prob $\frac{1}{4}$)
~~or~~ Eve goes undetected
- Bob gets the opposite bit (prob $\frac{1}{4}$)
(If $j \in S$, then Bob detects tampering & they reject the protocol.)

For every $j \in S$, Eve is detected with prob $\frac{1}{4}$.

If Eve does this for k bits in S, then she is undetected with prob $\left(\frac{3}{4}\right)^k$
~~Dete~~ $\therefore$ detected w prob $1 - \left(\frac{3}{4}\right)^k \approx 1$.