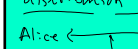
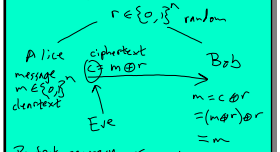
Quantum cryptographic key distribution



If Alice & Bob can share a string of length n of random bits, unknown to any one else, Alice can send a message to Bob of length $\leq n$ bits.

One-time pad



Perfect secrecy. Eve gets no info about m, given c (without r)

Can't use the same r twice:

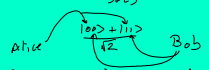
$c_1 = m_1 \oplus r$

$c_2 = m_2 \oplus r$

Eve: $c_1 \oplus c_2 = m_1 \oplus m_2$

In practice, Alice & Bob use r as a secret AES key

3DES



EPR pair must be securely distributed

BB84 (Bennett & Brassard) protocol

Alice & Bob share an (insecure) quantum channel and public classical channel but secure against active attack (tampering)

Fix n. Alice will send n qubits to Bob over the quantum channel

1. Alice: Prepares n qubits each one uniformly at random from the four possible states

$\{\underbrace{|0\rangle, |1\rangle}_{\text{computational basis}}, \underbrace{|+\rangle, |-\rangle}_{\text{Hadamard basis}}\}$

Alice sends each qubit to Bob

2. Bob: measures each of Alice's qubits as follows (indep for each qubit):
   a) chooses one of the two bases (comp. or Hadamard) uniformly at random (u.a.r.)
   b) measures the qubit in this basis.
   c) on the public channel, Bob tells Alice which basis he used.

[If Bob measures Alice's qubit in the same basis that Alice used to prepare it, then he knows Alice's bit with certainty.]

[Alice & Bob interpret $|0\rangle$ or $|+\rangle$ as a 0 & $|1\rangle$ or $|-\rangle$ as 1.]

3. Alice: Tells Bob (public channel) which qubits Bob measured in the same basis as Alice's prep. Alice & Bob discard the other bits, leaving about $\frac{n}{2}$ "quality bits" (meas. base = prep basis)

4. Security check:

a) Alice chooses each quality bit with prob $\frac{1}{2}$ indep at random, & if chosen, sends that bit to Bob (with info about its position) over the public channel. "check bits"

b) Bob compares the value of each check bit Alice sent. If Bob's measured value is the same for each check bit then he reports success: The unchecked quality bits serve as the shared random secret, of length $\frac{n}{4}$ on average. Otherwise, Bob reports evidence of eavesdropping & the protocol fails

Ex: If no tampering by Eve.

Alice: $n = 8$: 8 bits u.a.r.

bit: 1 1 0 1 0 0 1 0 u.a.r.

basis: c h c c h c h h (comp., h = Hadamard)

sent: $|1\rangle, |+\rangle, |0\rangle, |1\rangle, |0\rangle, |0\rangle, |+\rangle, |0\rangle$

Ex: If no tampering by Eve:

Alice: n=8; 8 bits u.a.r.

bit: 1 1 0 1 0 0 1 0 u.a.r.

basis: c h c c h c h h c=comp. h=Hadamard

qubit: |1>, |+>, |0>, |1>, |+>, |0>, |->, |+>

Alice to Bob

basis: h c c h h c h c Bob

? ? 0 ? 0 0 1 ?

After talking with Alice, they throw away the ? (bits 1,2,4,8)

leaving 0 0 0 1 (bits 3,5,6,7)

Security check: Alice chooses each bit with prob $\frac{1}{2}$ as a check bit:

5, 7, say: 0 1 — sent

Bob sees 0 1 — measured

Equal, so success.

If Eve eavesdrops on a qubit to get info, she measures. Assume Eve can measure in the c or the h basis.

1. prob $\frac{1}{2}$: Eve chooses Alice's basis, gets Alice's bit with certainty, sends it to Bob, Alice & Bob can't detect this — good for Eve

2. If Eve chooses the other basis, she gets uniformly random bit uncorrelated with Alice's:

$\frac{1}{2}$: $|\langle 0|+\rangle| = |\langle 1|+\rangle| = |\langle 0|-\rangle| = |\langle 1|-\rangle| = \frac{1}{\sqrt{2}}$

Best Eve can do is send a random qubit to Bob. If check bit Bob's bit is diff from Alice's with prob $\frac{1}{2}$,

$\frac{1}{2}$:

Each tampered check has a $\frac{1}{4}$ chance of flipping.

Eve tampers with k check bit then Eve escapes detection with

prob $\left(\frac{3}{4}\right)^k = \left(1-\frac{1}{4}\right)^k$

exponentially small in k.