A Look at a Three State Quantum Key Distribution Protocol

Jamie Batuwantudawe

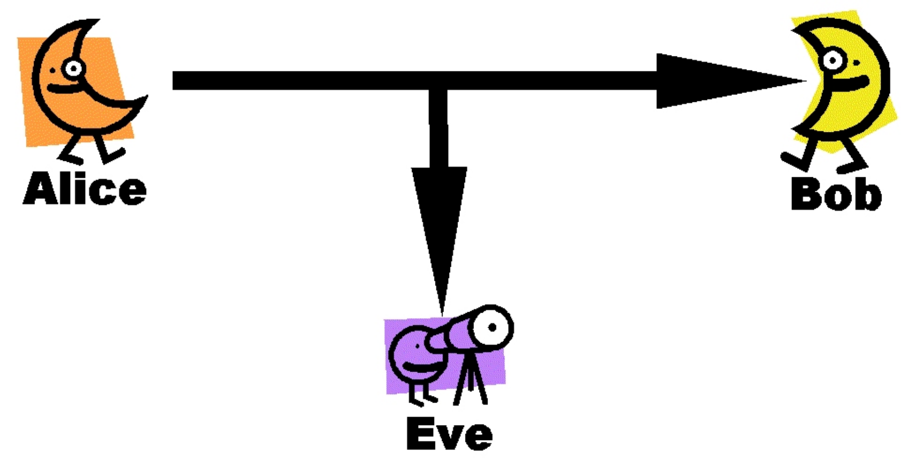
Institute for Quantum Computing
University of Waterloo

Canadian Students' Quantum Information Conference, 2005

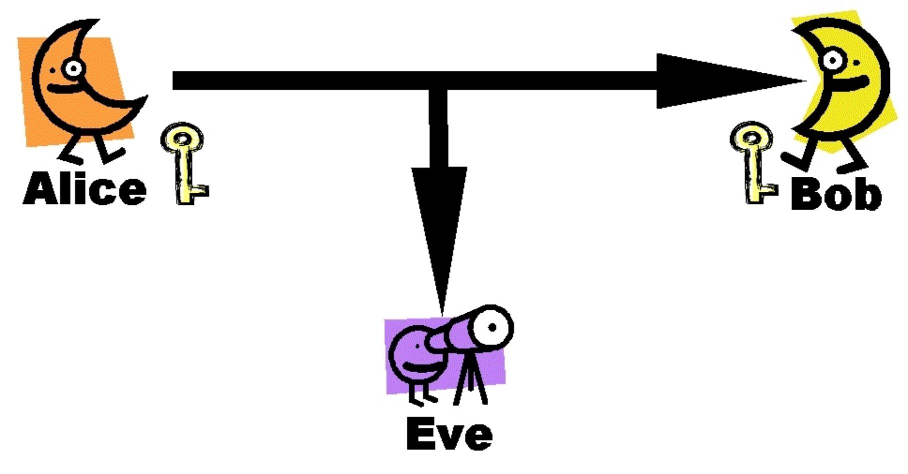
Outline

Outline

What is Cryptography?



What is Cryptography?



One-Time Pad

Encryption

$\texttt{PLAINTEXT} \oplus \texttt{KEY} \Longrightarrow \texttt{CIPHERTEXT}$

Decryption

$\texttt{CIPHERTEXT} \oplus \texttt{KEY} = \texttt{PLAINTEXT} \oplus \texttt{KEY} \oplus \texttt{KEY} \Longrightarrow \texttt{PLAINTEXT}$

Security of the One-Time Pad

```
PLAINTEXT:    JAMIE
KEY:        ⊕ AEALD
-------------------
CIPHERTEXT: KFMUI
```

Security of the One-Time Pad

```
PLAINTEXT:    HEATH
KEY:        ⊕ CALAA
─────────────────────
CIPHERTEXT:   KFMUI
```

The Key Problem

Classical Key Schemes

- Shamir's No Key Protocol
- Public Key Cryptography (ie. RSA)

Depend on unproved math problems!
ie. Factoring, Discrete Log

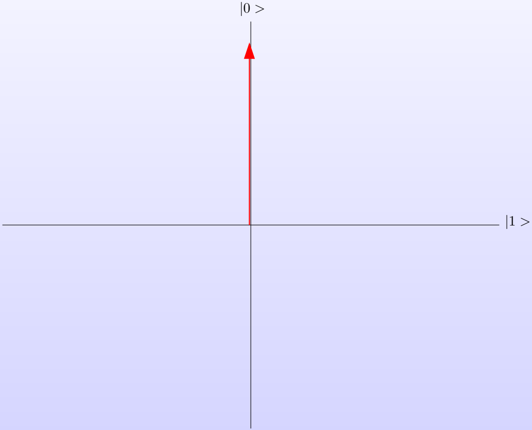
Outline

The No Cloning Theorem

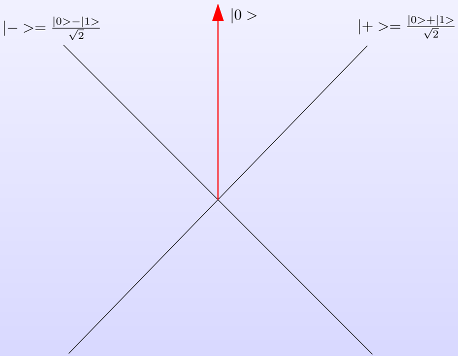
Theorem

Given an arbitrary, unknown quantum state, there exists no valid quantum operation that can produce a second, independently measurable copy of the state.

Non-orthogonal States



Non-orthogonal States



Outline

BB84 and Unbiased Bases

$$B_0 = \{ |b_{0,0}\rangle = |0\rangle, |b_{0,1}\rangle = |1\rangle \}$$
$$B_1 = \{ |b_{1,0}\rangle = |+\rangle, |b_{1,1}\rangle = |-\rangle \}$$

BB84

BB84 Protocol

1. Alice randomly chooses binary strings, $d^{(A)}$ and $t^{(A)}$, each of length $4n$. The former holds Alice's data bits and the latter determines Alice's choices of bases.
2. Let $d_i^{(A)}$ and $t_i^{(A)}$ denote the i^{th} bits of string $d^{(A)}$ and $t^{(A)}$ resepectively. For each i, Alice prepares the state $\left| b_{t_i^{(A)}, d_i^{(A)}} \right\rangle$. Alice sends all prepared states to Bob via the insecure quantum channel.
3. Bob publicly announces, using the authenticated classical channel, when he has received all $4n$ qubits.

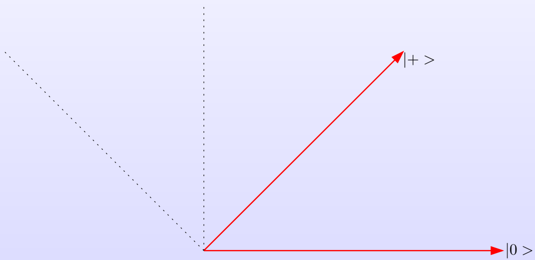
BB84 Protocol

4. Bob randomly chooses a binary string $t^{(B)}$ of length $4n$. Bob measures the i^{th} qubit in the $B_{t_i^{(B)}}$ basis. If the measurement yields $\left|b_{t_i^{(B)},0}\right\rangle$, Bob sets his corresponding data bit $d_i^{(B)} = 0$. Conversely, if the measurement yields $\left|b_{t_i^{(B)},1}\right\rangle$, Bob sets his corresponding data bit $d_i^{(B)} = 1$.
5. Alice publicly announces the string $t^{(A)}$, indicating the basis used for each qubit. Observe that it is too late for Eve to use this information to affect the state she sends to Bob.
6. Alice and Bob, via public discussion, agree to discard the i^{th} qubit if $t_i^{(A)} \neq t_i^{(B)}$. $2n$ bits are expected to remain.

BB84 Protocol

7. Alice randomly chooses half of the remaining data bits to be test bits. Alice notifies Bob of the position of the test bits.
8. Alice and Bob, via public discussion, compare the values of their corresponding test bits. If the number of disagreements is too high, they abort the protocol.
9. If they continue the protocol, Alice and Bob perform error correction and privacy amplification on the remaining n data bits to create a secure key.

B92



Outline

Using Entanglement

Entanglement Distillation Protocol

- Distant parties share n “imperfect” EPR pairs
- Use local operations and classical communication
- Finally share $m < n$ “perfect” EPR pairs

EPR pairs have perfect correlations
Third parties have no information about EPR pairs

EDP QKD

EDP-based BB84

1. Alice prepares $2n$ Bell states, $\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes 2n}$
2. Alice randomly chooses a binary string b of length $2n$. For the i^{th} Bell state, Alice performs a Hadamard operation on the second qubit if b_i, the i^{th} bit of b, is 1. The random Hadamard transformation hides information from Eve.
3. Alice sends the second half of each Bell state to Bob via the insecure quantum channel.

EDP QKD

EDP Protocol

4. Bob publicly announces, via the authenticated classical channel, the reception of $2n$ qubits.
5. Alice publicly announces the string b. Bob performs a Hadamard transformation on his i^{th} qubit if $b_i = 1$. Observe that Eve cannot use b to affect the qubit she passes along to Bob.
6. Alice randomly chooses half of the remaining data bits to be test bits. Alice notifies Bob of the position of the test bits.

EDP QKD

EDP Protocol

7. Alice and Bob each measure their test bits in the computational basis. Via public discussion, they compare the values of their corresponding test bits. If the number of disagreements is too high, they abort the protocol.
8. If they continue the protocol, Alice and Bob agree on a quantum error correcting code capable of correcting the number of errors in their qubits.
9. Alice and Bob decode their states to perfect copies of $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$. They each measure their halves in the computational basis to create a shared secret key.

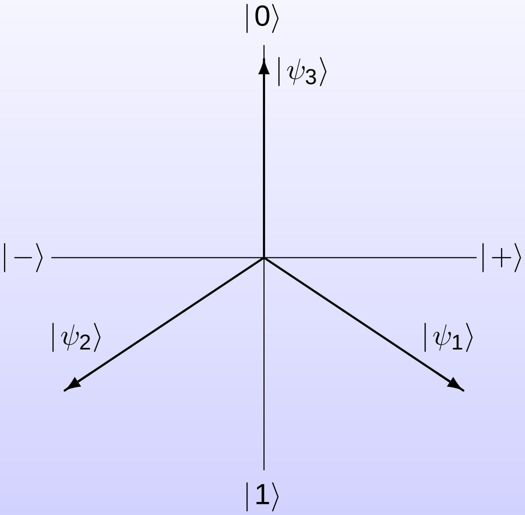
Security Proof of BB84

The Shor-Preskill Proof

- Can use CSS codes to seperate bit and phase error correction
- Can use classical error correcting code for bit error correction
- Can use classical hash functions for privacy amplification (corresponds to phase error correction)
- Simply need to find upper bounds on number of bit and phase errors

Outline

The Three States



The Protocol

PBC00

1. Alice creates a large trit string r and a large bit string b, both of length $3n$. Each r_i, the i^{th} trit value of r, determines the alphabet to be used for the i^{th} qubit. Each b_i, the i^{th} bit value of b, is the i^{th} classical bit that Alice tries to transmit to Bob.

Classical Bit	Quantum State		
	Alphabet 0	Alphabet 1	Alphabet 2
0	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_3\rangle$
1	$\|\psi_2\rangle$	$\|\psi_3\rangle$	$\|\psi_1\rangle$

Alice sends all prepared qubits to Bob through the quantum channel.

University of Waterloo IQC Institute for Quantum Computing

The Protocol

PBC00

2. On each received qubit, Bob performs a measurement described by the POVM

$$\left\{ \frac{2}{3} \left| \bar{\psi}_1 \right\rangle \left\langle \bar{\psi}_1 \right| , \frac{2}{3} \left| \bar{\psi}_2 \right\rangle \left\langle \bar{\psi}_2 \right| , \frac{2}{3} \left| \bar{\psi}_3 \right\rangle \left\langle \bar{\psi}_3 \right| \right\} \tag{1}$$

   Bob announces, using the public classical channel, when all of his measurements are done.
3. Alice announces the trit string r.
4. Bob uses his measurement outcome and r to determine the raw key.

The Protocol

PBC00

5. The expected number of bits remaining is $2n$. Alice randomly chooses half of these to be test bits. She publicly announces the positions of her test bits. Alice and Bob publicly compare the values of their test bits. If the number of errors is greater than the protocol's threshold, they abort.
6. If they do not abort, they run classical error correction and privacy amplification protocols to generate share a secure secret key from the remaining bits.

Phase Error Estimation

- For BB84, $e_{\text{bit}} = e_{\text{phase}}$ asymptotically since $HXH = Z$ and $HZH = X$.
- Not true for PBC00
- Difficult to analyze because general attacks can add dependence to errors.
- For any individual qubit, the probability of a phase error is $\frac{5}{4}$ the probability of a bit error

Azuma's Inequality

Theorem

Let $X_0, X_1, ..., X_N$ be a martingale sequence (ie. $E[X_i|X_{i-1}, X_{i-2}, ..., X_0] = X_{i-1}$) where $|X_i - X_{i-1}| \leq 1$. Then, for all $N \geq 0$ and any $\lambda \geq 0$,

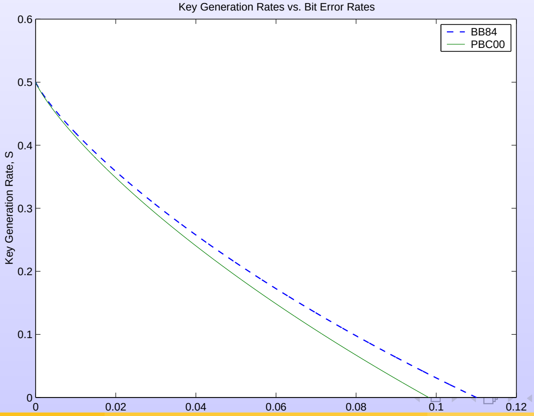
$$Pr[|X_N - X_0| \geq \lambda] \leq 2e^{-\frac{\lambda^2}{2N}}.$$

Can now show that $e_{\text{phase}} = \frac{5}{4} e_{\text{bit}}$

Key Generation Rates

$$\text{BB84}: \frac{1}{2}\left(1 - 2h(e_{\text{bit}})\right)$$

$$\text{PBC00}: \frac{1}{2 - e_{\text{bit}}}\left(1 - h(e_{\text{bit}}) - h\left(\frac{5}{4}e_{\text{bit}}\right)\right)$$



Error Estimation from Inconclusive Results

- Alice does not have to initially choose an alphabet. She could randomly send one of the three states and choose the alphabet later - after Bob's measurement.
- One choice by Alice will lead to a *good conclusive* result.
- The other choice will lead to an inconclusive result.
- Since only Alice's random choice of basis decides between good conclusive and inconclusive, asymptotically they will appear in equal numbers, by the central limit theorem.

Result is that $e_{\mathrm{bit}} = 2 - \frac{1}{p_{conclusive}}$

No Sampling

- PBC00's error estimation eliminates need for sampling
- This is good, right?
- What about sampling in BB84, B92?

Summary

- PBC00 is an unconditionally secure three state protocol
- Fewer states than BB84 might be good for implementations
- Higher threshold than B92 is beneficial
- Azuma's inequality allows generalization of Shor-Preskill proof to many QKD protocols
- Possibly useful no-sampling feature