Secure Quantum Cryptosystems

Hanhan Li
Outline

• Protocols in quantum cryptography
• Error correction and privacy amplification
• Security proofs
Protocols

• Prepare-and-measure protocols:
  1. BB84
  2. six-state
  3. two-state

• EPR protocols
Error correction and privacy amplification
Quantum Bit Error Rate (QBER)

\[
QBER = \frac{\text{Number of (sifted) incorrect counts}}{\text{Number of overall (sifted) counts}}
\]
Ideas from Class cryptography

The outcome of their measurements provide Alice, Bob, and Eve random variables a, b, and e, respectively, with a joint probability distribution $P(a, b, e)$.

**Theorem:**

For a given $P(a, b, e)$, Alice and Bob can establish a secret key (using only error correction and classical privacy amplification) if and only if $I(a, b) \geq I(a, e)$ or $I(a, b) \geq I(b, e)$, where $I(a, b)$ is the mutual information between a and b.
Error correction and privacy amplification

a) sifted key

b) error correction

c) privacy amplification

d) secret key
Advantage Distillation

In fact, Alice and Bob can still establish a secret key by using advantage distillation even if the conditions in the theorem are not satisfied.

Alice's bits: \textcolor{red}{0}0001010001010001101101100000

Bob's bits: \textcolor{red}{0}1100000111001001000000

Eve's bits: \textcolor{red}{0}110110010100101100100010
Quantum Privacy Amplification: Entanglement Purification Protocols (EPP)

One-way EPP

\( \varepsilon_a \)

EPR pair

\( \varepsilon_b \)

Two-way EPP

\( \varepsilon_{a1} \)

EPR pair

\( \varepsilon_{b1} \)

\( \varepsilon_{a2} \)

\( \varepsilon_{b2} \)
Security Proofs
Types of Attacks

- Individual attacks
- Joint attacks

Practical proofs vs. ultimate proofs
A conditional proof of the BB84
-Assuming individual attacks

\[ I(a, b) = 1 + D \log_2 D + (1 - D) \log_2 (1 - D) \]

\[ I(a, e) + I(a, b) \leq 1. \]

\[ I(a, b) \geq I(a, e) \quad \Rightarrow \quad \text{QBER: } D \leq 11\% \]
Unconditional proofs

Assumptions:

• Alice and Bob have perfect photon generators and detectors

• Eve cannot access Alice and Bob's encoding and decoding devices.

• The random number generators used by Alice and Bob must be trusted and truly random

• The classical communication channel must be authenticated using an unconditionally secure authentication scheme.
A one-way EPP: the Modified Lo-Chau

1: Alice creates 2n EPR pairs in the state $(|00> + |11>)/\sqrt{2}$.
2: Alice selects a random 2n bit string $b$, and performs a Hadamard transformation on the second half of each EPR pair for which $b$ is 1.
3: Alice sends the second half of each EPR pair to Bob.
4: Bob receives the qubits and publicly announces this fact.
5: Alice randomly selects n of the 2n encoded EPR pairs to serve as check bits to test for Eve’s interference.
6: Alice announces the bit string $b$, and which n EPR pairs are to be check bits.
7: Bob performs Hadamards on the qubits where $b$ is 1.
8: Alice and Bob each measure their halves of the n check EPR pairs in the Z basis and share the results. If more than $t$ of these measurements disagree, they abort the protocol.
9: Alice and Bob measure their remaining n qubits according to the same check matrix for a pre-determined [n,m] CSS quantum code correcting up to $t$ errors. Alice sends the error syndromes to Bob, and they transform their states so as to obtain m nearly perfect EPR pairs.
10: Alice and Bob measure the EPR pairs in the Z basis to obtain a shared secret key.
Shannon’s Bound:

- CSS codes exist with asymptotic rate:
  \[ \frac{k}{n} = 1 - 2H\left(\frac{t}{n}\right) \]
  where \( H(p) = -p \log p - (1-p) \log (1-p). \)

\[ 1 - 2H\left(\frac{t}{n}\right) > 0 \quad \text{if} \quad \frac{t}{n} \leq 11\% \]
The BB84 Protocol Reduced from the Modified Lo-Chau

1: Alice creates \((4 + \delta)n\) random bits.
2: Alice chooses a random \((4 + \delta)n\)-bit string \(b\). For each bit, she creates a state in the Z basis (if the corresponding bit of \(b\) is 0) or the X basis (if the bit of \(b\) is 1).
3: Alice sends the resulting qubits to Bob.
4: Bob receives the \((4+\delta)n\) qubits, measuring each in Z or X basis at random.
5: Alice announces \(b\).
6: Bob discards any results where he measured a different basis than Alice prepared. With high probability, there are at least \(2n\) bits left (if not, abort the protocol). Alice decides randomly on a set of \(2n\) bits to use for the protocol, and chooses at random \(n\) of these to be check bits.
7: Alice and Bob announce the values of their check bits. If more than \(t\) of these values disagree, they abort the protocol.
8: Alice announces \(u + v\), where \(v\) is the string consisting of the remaining non-check bits, and \(u\) is a random codeword in \(C_1\).
9: Bob subtracts \(u + v\) from his code qubits, \((v + \text{error})\), and corrects the result, \((u + \text{error})\), to a codeword in \(C_1\).
10: Alice and Bob use the coset of \(u + C_2\) as the key.
EPP to prepare-and-measure reductions

One-way EPPs → One-way BB84
One-way EPPs → One-way Six-state

Two-way EPPs → Two-way BB84
Two-way EPPs → Two-way Six-state
## Bounds on QBER

<table>
<thead>
<tr>
<th></th>
<th>The BB84 Protocol</th>
<th>The six-state Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>one-way</td>
<td>two-way</td>
</tr>
<tr>
<td>Upper bound</td>
<td>14.6%</td>
<td>1/4</td>
</tr>
<tr>
<td>Lower bound</td>
<td>11.0%</td>
<td>18.9%</td>
</tr>
<tr>
<td></td>
<td>1/6</td>
<td>1/3</td>
</tr>
<tr>
<td></td>
<td>12.7%</td>
<td>27.6%</td>
</tr>
</tbody>
</table>
The End