Quantum Cryptography

1. Introduction to Quantum Cryptography
2. Quantum Key Distribution: BB84 Protocol
3. Experimental Quantum Cryptography
4. QKD using Entanglement
5. Security of Quantum Cryptography
Introduction to Quantum Cryptography

• Traditional Cryptographic Communication
  – Private key cryptography is proven to be secure (Vernon cipher), but distributing key is a difficult problem
  – Public key cryptography is widely used today (RSA)
    • National security issues, Internet Commerce
    • Only computationally safe
  – Security of public key cryptography is threatened by quantum computers

• Quantum Cryptography
  – Early ideas by Wiesner in 1960s- Counterfeit-proof money
  – First proposed by Bennett in 1984
  – Quantum measurement guarantees security
  – Proven to be fundamentally secure
Quantum Cryptography

1. Introduction to Quantum Cryptography
2. Quantum Key Distribution: BB84 Protocol
3. Experimental Quantum Cryptography
4. QKD using Entanglement
5. Security of Quantum Cryptography
Quantum Key Distribution?

Goal: Share a string of Random Bits between Sender & Receiver
The bits are secure (no leakage to a third party)
This forms a key for a one-time pad cryptography
**Principles of BB84 Protocol**

**Bits are encoded in polarization of a single photon**

Two non-orthogonal bases: + (\[0:0 \leftrightarrow:1\]) and X (\[\leftarrow:0 \leftrightarrow:1\])

**Sender randomly selects between the two bases**

- Keeps the eavesdropper guessing which bases to use
- Induces higher error rate at the receiver
Brief History of QKD

3 most important people in Quantum Key Distribution

Alice (Sender), Bob (Receiver) and Eve (Eavesdropper)

1984 Bennett & Brassard First proposal for QKD (BB84)
1989 Bennett et al. First experiment for QKD (Free Space, 30 cm)
1993 Muller et al. First experiment on optical fiber (1 km)
1996 Muller et al. First experiment on commercial fiber (23 km)
1998 Buttler et al. Practical free-space at night (1 km)
2000 Buttler et al. Daylight free-space (1.6 km)
2002 id Quantique Commercially available QKD system (67 km)
2002 Beveratos et al. Single Photon Quantum Cryptography

1999 Lo & Chau Unconditional security (with Quantum Computers)
2000 Ralph et al. Continuous Variable Quantum Cryptography
2000 Lutkenhaus et al. Security Analysis of practical systems (individual attack)
2000 Shor & Preskill Unconditional security (w/o Quantum Computers)
**How it works (BB84 Protocol)**

**Bits are encoded in polarization of a single photon**

Two non-orthogonal bases: \(+ (\uparrow:0 \leftrightarrow:1)\) and \(X (\downarrow:0 \uparrow:1)\)

| Alice Bits  | 1 0 0 1 0 1 1 0 1 0 0 0 1 1 1 0 1 0 0 1 1 0 1 1 0 1 0 |
| Alice Basis | + X + + + X X + X + + X X + X + + X X + X + + + X X |
| Photon Pol.   | ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ |
| Eve Basis    | X + X + X X + + + X + X + + X + + X X + + + + X X |
| Eve Meas     | ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ |
| Eve Bits     | 1 1 0 0 0 0 |
| Bob Basis    | X + + + X X + X X X + X + + X + X X + X X + X + + + + |
| Bob Meas.    | ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ |
| Bob Meas (Eve) | ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ |
| Agreed Basis | ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ |
| Bob Bits (Secure) | 0 X 1 1 1 0 0 0 0 X 0 1 |
Security of Exchanged Key

- **Detection of Eavesdropper (Eve)**
  - Increased error rate in Bob’s receiver detects Eve’s presence
  - Intrinsic error rates has to be low
  - Multi-photon states are subject to beamsplitting attack
  
  Communication has to be done with SINGLE PHOTONS!!

- **Requirement for Secure Communication**
  - Eve limited not by technology, but by laws of quantum physics
  - QKD system has to be built with existing technology
  - Assume all channel error is due to Eve’s activity

- **After Raw Quantum Transmission (RQT):**
  - Error correction has to be done on communicated bits
  - Privacy Amplification based on Eve’s estimated knowledge
  - These processes distill (shorter) secure key from RQT
Quantum Cryptography

1. Introduction to Quantum Cryptography
2. Quantum Key Distribution: BB84 Protocol
3. Experimental Quantum Cryptography
4. QKD using Entanglement
5. Security of Quantum Cryptography
## Commercial System Performance

“Plug & Play” Design – no optical alignment, only temporal training
Self-compensating polarization interferometer
1550 nm wavelength
Average Photon Number : 0.2 photons / pulse

<table>
<thead>
<tr>
<th>Fibre</th>
<th>Length (km)</th>
<th>Key (kbit)</th>
<th>$R_{\text{raw}}$ (kHz)</th>
<th>QBER (%)</th>
<th>$R_{\text{net}}$ (kHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geneva–Nyon (under lake)</td>
<td>22.0</td>
<td>27.9</td>
<td>2.06</td>
<td>2.0 ± 0.1</td>
<td>1.51</td>
</tr>
<tr>
<td>Geneva–Nyon (terrestrial)</td>
<td>22.6</td>
<td>27.5</td>
<td>2.02</td>
<td>2.1 ± 0.1</td>
<td>1.39</td>
</tr>
<tr>
<td>Nyon–Lausanne (terrestrial)</td>
<td>37.8</td>
<td>25.1</td>
<td>0.50</td>
<td>3.9 ± 0.2</td>
<td>0.26</td>
</tr>
<tr>
<td>Geneva–Lausanne (under lake) A</td>
<td>67.1</td>
<td>12.9</td>
<td>0.15</td>
<td>6.1 ± 0.4</td>
<td>0.044</td>
</tr>
<tr>
<td>Geneva–Lausanne (under lake) B</td>
<td>67.1</td>
<td>12.9</td>
<td>0.16</td>
<td>5.6 ± 0.3</td>
<td>0.051</td>
</tr>
<tr>
<td>Ste Croix (aerial) A</td>
<td>8.7</td>
<td>63.8</td>
<td>6.29</td>
<td>3.0 ± 0.1</td>
<td>4.34</td>
</tr>
<tr>
<td>Ste Croix (aerial) B</td>
<td>23.7</td>
<td>117.6</td>
<td>2.32</td>
<td>3.0 ± 0.1</td>
<td>1.57</td>
</tr>
</tbody>
</table>

http://www.idquantique.com/
Visible Photon (773nm)
1MHz rep rate
Broad daylight – Huge Background
Single photon isolated by
  - Time gating
  - Spectral Filtering
  - Spatial (Mode) Filtering
Average Photon Number :
  - 0.2-0.5 photons / pulse
Error Rate ~5%
Applicable to Earth-Satellite links

23.4 km Free-Space Experiment

Single Photon Sources

- Single Photon Source used in QKD (2002)

Quantum Dot in Microcavity
Yamamoto Group (Stanford)

Color Center in Diamond
Grangier Group (Paris)
# Quality of Single Photon Sources

<table>
<thead>
<tr>
<th></th>
<th>Stanford</th>
<th>Paris</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detector Dark Count</td>
<td>5-10K</td>
<td>Room T</td>
</tr>
<tr>
<td>$g^{(2)}(\tau=0)$</td>
<td>0.14</td>
<td>0.07</td>
</tr>
<tr>
<td>Repetition Rate</td>
<td>76 MHz</td>
<td>5.3 MHz</td>
</tr>
<tr>
<td>Avg. Photon No./Pulse</td>
<td>0.007</td>
<td>0.014</td>
</tr>
<tr>
<td>Multi-photon rate</td>
<td>$3.4 \times 10^{-6}$</td>
<td>$7 \times 10^{-6}$</td>
</tr>
<tr>
<td>Carrier Lifetime</td>
<td>4.4 ns</td>
<td>23 ns</td>
</tr>
</tbody>
</table>

![Counts](image1.png)

![Raw coincidences](image2.png)
## Other Experimental Parameters

<table>
<thead>
<tr>
<th></th>
<th>Stanford</th>
<th>Paris</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dark Count Prob.</td>
<td>&lt;1 x 10⁻⁶</td>
<td>7.5 - 19 x 10⁻⁶</td>
</tr>
<tr>
<td>Detector Quantum Eff.</td>
<td>30 %</td>
<td>60 %</td>
</tr>
<tr>
<td>Quantum BER</td>
<td>2.5 %</td>
<td>4.6 %</td>
</tr>
<tr>
<td>Key Exchange Rate</td>
<td>25 kbps</td>
<td>7.7 kbps</td>
</tr>
<tr>
<td>Max. Channel Loss</td>
<td>28 dB</td>
<td>20 dB</td>
</tr>
</tbody>
</table>

Both experiments are quantitatively better than what can be achieved using Weak Coherence Pulse (WCP)
Quantum Cryptography

1. Introduction to Quantum Cryptography
2. Quantum Key Distribution: BB84 Protocol
3. Experimental Quantum Cryptography
4. QKD using Entanglement
5. Security of Quantum Cryptography
EPR Protocol (Akert, 1991)

- Alice and Bob uses entangled states to "generate" the key
- **Start with EPR pairs (Bell states)**
  \[
  |\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{2}
  \]
  - Alice has one particle, and Bob has the other
  - They start with \(2n\) such pairs
  - They check the fidelity of the pairs by choosing a subset (say, \(n\) pairs) and performing Bell measurements: Detects Eve!!
  - With remaining \(n\) bits
    - Alice measures randomly in \(|0\rangle,|1\rangle\) or \(|+\rangle,|-\rangle\) bases
    - Bob does the same
    - They compare bases, and keep results from matching bases
- **Keys are generated during the procedure, not communicated!!**
Modified Lo-Chau Protocol

1. Alice creates $2n$ EPR pairs in the state $|\beta_{00}\rangle^\otimes 2^n$
2. Alice randomly selects $n$ of $2n$ pairs to serve as check bits
3. Alice chooses bits randomly and apply Hadamard transform on the second bit
4. Alice sends second bits of each pair to Bob
5. Bob received the bits and acknowledges the fact
6. Alice announces the bits to which Hadamard has been performed
7. Bob performs Hadamard on those bits
8. Alice and Bob each measure the check qubits in the $|0\rangle, |1\rangle$ basis, and publicly share the results. More than $t$ errors, abort protocol
9. Alice and Bob measure the remaining $n$ qubits according to the predetermined quantum code correcting up to $t$ errors. This leaves $m$ nearly-perfect EPR pairs
10. Use $m$ EPR pairs to obtain a secret key
Quantum Cryptography

1. Introduction to Quantum Cryptography
2. Quantum Key Distribution: BB84 Protocol
3. Experimental Quantum Cryptography
4. QKD using Entanglement
5. Security of Quantum Cryptography
Fundamental Security Proof

- BB84 protocol can be reduced to the modified Lo-Chau protocol using quantum error correction theory, to prove its security!!
  - Proof in Chapter 12.6.5 of Textbook
Practical Security Limitations

- Ideal (error free) channels proven to be unconditionally safe
- BB84 proven to be safe using proper error correction (Lo & Chau with quantum computers, Shore & Preskill w/o)
- Any experimental imperfection will open loophole in security
- Beamsplitting (Photon Number Splitting) attack

If Alice accidentally sends more than one photon, Eve can tap one photon and extract bit without being detected.

Photon number statistics for weak coherent light obeys Poisson Statistics

\[ P_\lambda(n) = e^{-\lambda} \frac{(\lambda)^n}{n!} \]

<table>
<thead>
<tr>
<th>(\lambda)</th>
<th>(P_\lambda(0))</th>
<th>(P_\lambda(1))</th>
<th>(P_\lambda(n&gt;1))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.37</td>
<td>0.37</td>
<td>0.26</td>
</tr>
<tr>
<td>0.5</td>
<td>0.61</td>
<td>0.30</td>
<td>0.09</td>
</tr>
<tr>
<td>0.1</td>
<td>0.9048</td>
<td>0.0905</td>
<td>0.0047</td>
</tr>
</tbody>
</table>
Critical Experimental Parameters

- **Goal:** Maximize loss budget while maintaining security
- **Photon Number Splitting Attack** puts security bound due to
  
  **Source Quality:** Low multi-photon emission probability
  
  \[ g^{(2)}(\tau=0) = \frac{\langle n(n-1) \rangle}{\langle n \rangle^2} \]
  
  \( g^{(2)} = 1 \) for coherent light, \( g^{(2)} > 1 \) for thermal light
  
  \( g^{(2)} < 1 \) means non-classical light

  **Detector Quality:** Low dark count, high quantum efficiency
  
  Low \( d_B/\eta_B \) where
  
  \( d_B \) Dark count at Bob’s Detector
  
  \( \eta_B \) Quantum efficiency of Bob’s Detector

- **Error Rate:** Quality of Bob’s measurement setup

- **Somewhat less important are**
  
  **Source Efficiency** to emit a photon
  
  **Overall Repetition Rate of the pulses**
Security Analysis (PNS Attack)

- Reasonable Loss budget
  - 30-50 dB
  - ~100 km in fibers
  - Earth-satellite possible
  - In free space

Notion of Quantum Repeaters

1. Requirements
Photons need to be added to compensate for the loss
Cannot involve direct measurement or amplification
Establish entanglement over a long distance
Success probability must not decay exponentially w.r.t. distance

2. Solution
Entanglement Swapping (Bennet et al., PRL 76, 722, 1996)
Quantum teleportation between two entangled pairs
Swapping process degrades fidelity of the pairs
Need to be “purified” using quantum computer at each node

First example (Briegel et al., PRL 81, 5932, 1998):
Purification with imperfect local operations to improve fidelity
Need for quantum memory and quantum computer

Second example (Duan, Lukin, Cirac and Zoller, Nature 414, 413, 2001)
Use of atomic ensembles and linear optics
Probabilistic success (no quantum computer needed)
**Scheme by Briegel et al (1998)**

**Entanglement Swapping**

\[
|\beta_{00}\rangle_{12} = \frac{1}{\sqrt{2}} (|00\rangle_{12} + |00\rangle_{12})
\]

\[
|\beta_{00}\rangle_{34} = \frac{1}{\sqrt{2}} (|00\rangle_{34} + |00\rangle_{34})
\]

\[
|\beta_{00}\rangle_{14} = \frac{1}{\sqrt{2}} (|00\rangle_{14} + |00\rangle_{14})
\]

(a) \(N = L^n\)

(b) \[\text{Diagram of entanglement swapping process.}\]

(c) \[\text{Graph showing the relationship between } F \text{ and } F'_L.\]

**Total # of Elementary pairs**

\[R = (LM)^n = N^{\log_L M + 1}\]

**Total Timestep**

\[T = M n = M \log_L N\]
Scheme by DLCZ (2001)

Entanglement Generation

\[ |g\rangle \rightarrow A \rightarrow |e\rangle \rightarrow |s\rangle \]

Entanglement Swapping

Noise and Purification

Main source of noise is photon loss, detector dark counts, and multiple excitation
Success is conditioned by detection events
When successful, the fidelity is high
Purification by post-selection

Experiments
Georgia Tech, Caltech, etc.