

Experimental Quantum Cryptography (1991)

*Bennett, Bessette, Brassard, Salvail,
Smolin*

Overview

- History
- Purpose
- Key Distribution
- Quantum Key Distribution
- Physical Apparatus
- Possible Attacks
- How it is applied today

History

- Roots of Quantum Cryptography in a proposal by Stephen Wiesner called “Conjugate Coding”
 - Published in 1983
- First quantum cryptography protocol created in 1984, called BB84
 - Unpublished until 1991 (this paper)

Purpose

- Public Key cryptography based on:
 - Unproven mathematics
 - Current limits on computational power
- Security in this manner is not satisfactory
 - Developments in computational power could render all previously “secure” data insecure
- Quantum Cryptography based on the strength of the laws of physics
 - We will focus on its use for key exchange

Key Distribution

- **Key Distribution**
 - Purpose: Alice and Bob agree on random key
 - Share no information initially
 - Eavesdropper Eve cannot get key
- **In conventional cryptography, it is assumed that communications can be monitored**
 - Sender and receiver unaware

Quantum Key Distribution

- **Digital information encoded in elementary quantum systems cannot be eavesdropped upon**
 - Eavesdropper would disrupt transmission
 - Sender/Receiver would be aware
- **The amount of information that can be transmitted is not very large, but is provably very secure**

Quantum Key Distribution

- Why it works
 - photons are put into a particular state by one sender and observed by recipient
 - Because of Heisenberg's Uncertainty Principle, some quantum information occurs as *conjugates*
 - polarization in three bases: circular, diagonal and rectilinear
 - observing in one basis randomizes the conjugates
 - If you do not know what basis to test, you destroy the information

Quantum Key Distribution Protocol

1. Alice sends random sequence of the four kinds of polarized photons to Bob
2. Bob chooses randomly for each photon whether to measure rectilinear or circular polarization
3. Bob announces which kind of measurement he made
4. Alice tells him whether he made the correct measurement

Quantum Key Distribution Protocol

5. Alice and Bob agree publicly to discard all incorrect measurements
6. Alice and Bob agree publicly to discard all positions where photons were not detected
7. Polarizations of resulting photons are 0 for horizontal & left-circular
8. Polarizations of resulting photons are 1 for vertical & right-circular
9. Resulting binary string is secret key

1.	⊖	↑	⊖	↔	↓	↓	↔	↔	⊖	⊖	↑	⊖	⊖	↑
2.	+	○	○	+	+	○	○	+	○	+	○	○	○	+
3.	↓	⊖		↓	⊖	⊖	↔		↓	⊖	⊖		⊖	↓
4.	+	○		+	○	○	+		+	○	○		○	+
5.		✓		✓			✓			✓			✓	✓
6.		⊖		↑			↔			⊖			⊖	↑
7.				1			1						1	0

Figure 1: Basic quantum key distribution protocol.

1. Alice sends a random sequence of photons polarized horizontal (↔), vertical (↑), right-circular (⊖) and left-circular (⊖);
2. Bob measures the photons' polarization in a random sequence of bases, rectilinear (+) and circular (○).
3. Results of Bob's measurements (some photons may not be received at all).
4. Bob tells Alice which basis he used for each photon he received;
5. Alice tells him which bases were correct;
6. Alice and Bob keep only the data from these correctly-measured photons, discarding all the rest.
7. This data is interpreted as a binary sequence according to the coding scheme ↔ = ⊖ = 0 and ↑ = ⊖ = 1.

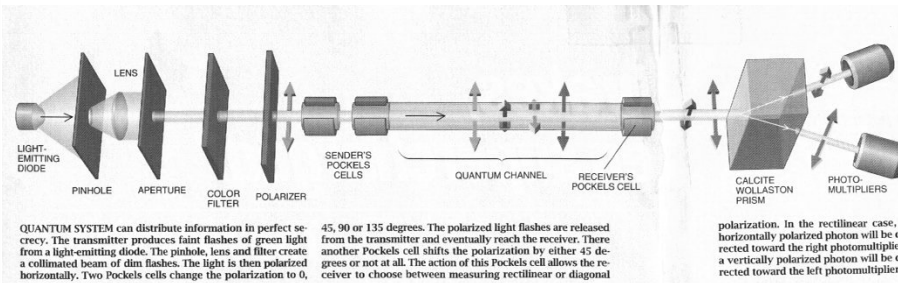
Quantum Key Distribution

- In the presence of noise, Alice and Bob must ensure they possess the same string of bits
 - Polarizations observed may not be the same as those transmitted
- This is completed using binary search with parity checks
- Done publicly, and last bit is discarded

Quantum Key Distribution

- *Privacy Amplification* can be used to reduce an outsider's knowledge of the bit string
- If attacker knows L bits of the length n string x , hash function may be used to map the string x to $h(x)$ of length $L-n-s$ for any s
- Attacker's expected knowledge of $h(x)$ is less than $2^{-s/\ln 2}$ bits

Physical Apparatus



Possible Attacks

- Intercept/Resend
- Beamsplitting
- Denial of Service

Intercept/Resend

- Quantum cryptography provides no protection against man-in-the-middle attacks
 - When Alice tries to establish a secret key, Eve intercepts and responds to messages in both directions
- Quantum Cryptography is based on the assumption that this is not possible

Beamsplitting

- It is difficult to send single photons, so small bursts of coherent light are used
- Eve may be able to split single photons out of the burst
 - She must have some way to hold the photons
 - By observing these photons she may gain information about the messages

DoS

- Eavesdropping and noise are indistinguishable to communicating parties
- Either one can cause quantum exchanges to fail
- Thus, eavesdropper can cause DoS by eavesdropping too much!

How it is applied today

- November 15, 2002 CNET news article
 - “Noisy light’ is new key to encryption”
- Benefits:
 - No eavesdropping
 - “If eavesdropper disturbs photons, then they are gone”
 - Fairly fast - 250mbps
- Drawbacks:
 - Only works on fiber-optic cable, not on internet

http://news.com.com/2100-1001-965957.html?tag=fd_top

Review

- History
- Purpose
- Key Distribution
- Quantum Key Distribution
- Physical Apparatus
- Possible Attacks
- How it is applied today

Questions?