UCDAVIS

Aleksander Zujev

Quantum Cryptography talk 11-18-2009

Quantum Cryptography

Outline

- Classical Cryptography
- Quantum Cryptography
- Quantum Cryptography: Applications

Classical Cryptography: Caesar Protocol

Substitution:
A $\rightarrow$ B
B $\rightarrow$ C
...
Z $\rightarrow$ A

QUANTUM $\rightarrow$ RVBOUVN

- Easy to use
- Easy to break

Classical Cryptography: One-Time-Pad Protocol

- Step 0. Alice generates key K - sequence of random bits, and gives K to Bob.

Alice sends message T to Bob:

- Step 1. Alice calculates $E = T \oplus K$ ($\oplus \equiv$ bitwise XOR, or exclusive OR).
- Step 2. Alice sends E to Bob by insecure public channel.
- Step 3. Bob receives E and calculates $T = E \oplus K$.

- Difficult to use: Step 0 requires secure channel, eg: Physical contact
- "Impossible" to break: Message E is sequence of random bits

Quantum Cryptography

- Step 0. Alice generates key K and gives K to Bob by Secure Quantum Channel.

Alice sends message T to Bob:

- Step 1. Alice calculates $E = T \oplus K$ ($\oplus \equiv$ bitwise XOR, or exclusive OR).
- Step 2. Alice sends E to Bob by insecure public channel.
- Step 3. Bob receives E and calculates $T = E \oplus K$.

- Easy to use
- "Impossible" to break

Quantum Cryptography: BB84 Protocol - Bennett and Brassard, 1984

Information encoded by photon polarization in one of two conjugate bases:

Basis	0	1
+	↑	→
×	↗	↘

Quantum Cryptography: BB84 Protocol

Basis	0	1
+	↑	→
×	↗	↘

• Step 1. Alice generates random bit, selects random base ($\times$ or $+$), and sends polarized photon to Bob.

Quantum Cryptography: BB84 Protocol

Basis	0	1
+	↑	→
×	↗	↘

• Step 1. Alice generates random bit, selects random base ($\times$ or $+$), and sends polarized photon to Bob.

• Step 2. Bob selects random base ($\times$ or $+$), and measures polarization of photon in this base.

• Case 1: Bob's base the same as Alice: then bit read correctly. Eg:
Alice uses $+$ base and sends bit $0 = |\uparrow\rangle$ photon
Bob uses $+$ base and measures $|\uparrow\rangle$ photon

• Case 2: Bob's base different from Alice. Eg:
Alice uses $+$ base and sends bit $0 = |\uparrow\rangle$ photon
Bob uses $\times$ base. In this base $|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\searrow\rangle)$,
$\text{Prob}(|\nearrow\rangle) = \text{Prob}(|\searrow\rangle) = \frac{1}{2}$, or $\text{Prob}(0) = \text{Prob}(1) = \frac{1}{2}$.

Quantum Cryptography: BB84 Protocol

Basis	0	1
+	↑	→
×	↗	↘

• Step 1. Alice generates random bit, selects random base (× or +), and sends polarized photon to Bob.

• Step 2. Bob selects random base (× or +), and measures polarization of photon in this base.

• Step 3. Bob sends the base he used to Alice by public channel.

Quantum Cryptography: BB84 Protocol

Basis	0	1
+	↑	→
×	↗	↘

• Step 1. Alice generates random bit, selects random base (× or +), and sends polarized photon to Bob.

• Step 2. Bob selects random base (× or +), and measures polarization of photon in this base.

• Step 3. Bob sends the base he used to Alice by public channel.

• Step 4. If Bob used the correct base, Alice informs Bob that the bit he measured is part of the key, otherwise that it isn't.

Quantum Cryptography: BB84 Protocol

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

Quantum Cryptography: BB84 Protocol

Enter Eve the Eavesdropper

Eve wants to read Alice - Bob communication.

Quantum Cryptography: BB84 Protocol

Enter Eve the Eavesdropper

Eve wants to read Alice - Bob communication.

No-cloning theorem - Eve cannot copy photon.

Can: Measure and Resend.

Quantum Cryptography: BB84 Protocol

- Case 1. Eve: correct base, Bob: correct base. Eg:

Alice sends $0 = |\uparrow\rangle$

Eve reads $|\uparrow\rangle$, sends $|\uparrow\rangle$

Bob reads $|\uparrow\rangle = 0$

Result: Eve gained one bit of the key.

Quantum Cryptography: BB84 Protocol

- Case 2. Eve: wrong base, Bob: correct base. Eg:

Alice sends $0 = |\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\searrow\rangle)$

Eve reads $|\nearrow\rangle$ or $|\searrow\rangle$ with $Prob = \frac{1}{2}$, eg $|\nearrow\rangle$

Eve sends $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)$

Bob reads $|\uparrow\rangle$ or $|\rightarrow\rangle$ with $Prob = \frac{1}{2}$

Result: Bob reads on average $\frac{1}{2}$ bit of the key wrong.

Quantum Cryptography: BB84 Protocol

- Case 3. Eve: correct base, Bob: wrong base.

- Case 4. Eve: wrong base, Bob: wrong base.

Result: Since Bob uses wrong base, this bit is dismissed.

Quantum Cryptography: BB84 Protocol

Net Result: Eve gained $\frac{1}{2}$ bits of the key.

Bob got corrupted $\frac{1}{4}$ bits of the key.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	√		x			√		√

Quantum Cryptography: BB84 Protocol

$\Rightarrow$ Evident possible solution:

Use part of bits of the key to compare them through public channel (removing them from the key).

If Bob got key partially wrong, then there is eavesdropping, and communication will be aborted.

Quantum Cryptography: B92 Protocol - Bennett, 1992

- Similar to BB84.
- Instead of 2 bases $+$, $\times$, uses 1 base $\angle$, nonorthogonal.

Quantum Cryptography: E91 Protocol - Ekert, 1991

- Uses Quantum Entanglement

Quantum Cryptography: Applications

The highest bit rate system currently demonstrated exchanges secure keys at 1 Mbit/s (over 20 km of optical fibre) and 10 kbit/s (over 100 km of fibre), achieved by a collaboration between the University of Cambridge and Toshiba using the BB84 protocol with decoy pulses.

Quantum Cryptography: Applications

As of March 2007 the longest distance over which quantum key distribution has been demonstrated using optic fibre is 148.7 km, achieved by Los Alamos/NIST using the BB84 protocol. Significantly, this distance is long enough for almost all the spans found in today's fibre networks. The distance record for free space QKD is 144 km between two of the Canary Islands, achieved by a European collaboration using entangled photons (the Ekert scheme) in 2006, and using BB84 enhanced with decoy states in 2007. The experiments suggest transmission to satellites is possible, due to the lower atmospheric density at higher altitudes. For example although the minimum distance from the International Space Station to the ESA Space Debris Telescope is about 400 km, the atmospheric thickness is about an order of magnitude less than in the European experiment, thus yielding less attenuation compared to this experiment.

Quantum Cryptography: Applications

The DARPA Quantum Network, a 10-node quantum cryptography network, has been running since 2004 in Massachusetts, USA. It is being developed by BBN Technologies, Harvard University, Boston University and QinetiQ.

Quantum Cryptography: Applications

There are currently four companies offering commercial quantum cryptography systems; id Quantique (Geneva), MagiQ Technologies (New York), SmartQuantum (France) and Quintessence Labs (Australia). Several other companies also have active research programmes, including Toshiba, HP, IBM, Mitsubishi, NEC and NTT (See External links for direct research links).

Quantum Cryptography: Applications

Quantum encryption technology provided by the Swiss company Id Quantique was used in the Swiss canton (state) of Geneva to transmit ballot results to the capitol in the national election occurring on Oct. 21, 2007.

Quantum Cryptography: Applications

In 2004, the world's first bank transfer using quantum cryptography was carried in Vienna, Austria. An important cheque, which needed absolute security, was transmitted from the Mayor of the city to an Austrian bank.

Quantum Cryptography: Applications

The world's first computer network protected by quantum cryptography was implemented in October 2008, at a scientific conference in Vienna. The network used 200 km of standard fibre optic cable to interconnect six locations across Vienna and the town of St Poelten located 69 km to the west. The event was witnessed by Gilles Brassard and Anton Zeilinger.

References

[1] Stephen Wiesner, "Conjugate Coding", SIGACT News (15:1 pp. 78-88, 1983).

[2] Bennett, Brassard, "Quantum cryptography: Public key distribution and coin tossing", In Proceedings of IEEE International Conference on Computers Systems and Signal Processing, pp 175-179, 1984.

[3] Artur K. Ekert, "Quantum cryptography based on Bells theorem", Phys. Rev. Lett. 67, 661 - 663 (1991)