BB84

BB84[1][2] is a quantum key distribution scheme developed by Charles Bennett and Gilles Brassard in 1984. It is the first quantum cryptography protocol.[3] The protocol is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states one is trying to distinguish are not orthogonal (see no-cloning theorem). It is usually explained as a method of securely communicating a private key from one party to another for use in one-time pad encryption.[4]

Description

In the BB84 scheme, Alice wishes to send a private key to Bob. She begins with two strings of bits, a and b, each n bits long. She then encodes these two strings as a string of n qubits:

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle,$$

where a_i and b_i are the i-th bits of a and b respectively. Together, $a_i b_i$ give us an index into the following four qubit states:

$$\begin{aligned}
|\psi_{00}\rangle &= |0\rangle, \\
|\psi_{10}\rangle &= |1\rangle, \\
|\psi_{01}\rangle &= |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \\
|\psi_{11}\rangle &= |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.
\end{aligned}$$

Note that the bit b_i is what decides which basis a_i is encoded in (either in the computational basis or the Hadamard basis). The qubits are now in states that are not mutually orthogonal, and thus it is impossible to distinguish all of them with certainty without knowing b.

Alice sends $|\psi\rangle$ over a public and authenticated quantum channel $\mathcal{E}$ to Bob. Bob receives a state $\mathcal{E}(\rho) = \mathcal{E}(|\psi\rangle\langle\psi|)$, where $\mathcal{E}$ represents both the effects of noise in the channel and eavesdropping by a third party we'll call Eve. After Bob receives the string of qubits, all three parties, namely Alice, Bob and Eve, have their own states. However, since only Alice knows b, it makes it virtually impossible for either Bob or Eve to distinguish the states of the qubits. Also, after Bob has received the qubits, we know that Eve cannot be in possession of a copy of the qubits sent to Bob, by the no-cloning theorem, unless she has made measurements. Her measurements, however, risk disturbing a particular qubit with probability ½ if she guesses the wrong basis.

Bob proceeds to generate a string of random bits b' of the same length as b and then measures the string he has received from Alice, a'. At this point, Bob announces publicly that he has received Alice's transmission. Alice then knows she can now safely announce b. Bob communicates over a public channel with Alice to determine which b_i and b'_i are not equal. Both Alice and Bob now discard the qubits in a and a' where b and b' do not match.

From the remaining k bits where both Alice and Bob measured in the same basis, Alice randomly chooses $k/2$ bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see whether more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques to create some number of shared secret keys. Otherwise, they cancel and start over.

See also

- SARG04
- E91 – quantum cryptographiccommunication protocol

References

1. C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*volume 175, page 8. New York, 1984. http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf
2. Bennett, Charles H.; Brassard, Gilles (2014-12-04)."Quantum cryptography: Public key distribution and coin tossing" (http://www.sciencedirect.com/science/article/pii/S0304397514004241) *Theoretical Computer Science* Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. 560, Part 1: 7–11. doi:10.1016/j.tcs.2014.05.025 (https://doi.org/10.1016%2Fj.tcs.2014.05.025)
3. Branciard, Cyril; Gisin, Nicolas; Kraus, Barbara; Scarani, Valerio (2005). "Security of two quantum cryptography protocols using the same four qubit states"*Physical Review A* **72** (3). arXiv:quant-ph/0505035 (https://arxiv.org/abs/quant-ph/0505035). doi:10.1103/PhysRevA.72.032301(https://doi.org/10.1103%2FPhysRevA.72.032301)
4. *Quantum Computing and Quantum Information*, Michael Nielsen and Isaac Chuang