Quantum Cryptography and Quantum Key Distribution

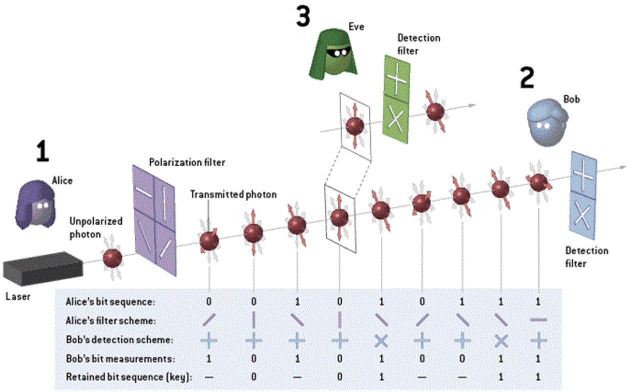
F. Vogiatzian

Why Quantum Cryptography? As we have seen during the course, modern cryptography relies on the computational inability of an adversary to break an encryption scheme in polynomial time. While this is in general a strong enough assumption, it is not enough to guarantee the long-term security of an encryption as the computational power that is available to an adversary increases rapidly. Also most schemes rely on the hardness for a classical computer to solve problems such as the factorisation of integers which is a problem that will be solvable in polynomial time for an adversary with access to a working quantum computer.

Quantum cryptography on the other hand relies only on the fact that the laws of quantum physics describe nature accurately enough. If this is the case there are protocols that are provably secure ([1],[3]).

Post-quantum cryptography is a new field of research that has developped during the last decade trying to find cryptographic primitives that cannot be broken efficiently by quantum or classical computers. For example, using lattice-based cryptographic schemes, etc. Also most current cryptographic schemes using hash functions could be made secure against quantum adversaries by increasing the key size [4].

Quantum Key Distribution One interesting possibility using quantum cryptography is quantum key distribution (QKD) which allows two parties (Alice and Bob) to exchange a key using a public quantum channel on which an eavesdropper (Eve) has complete control in a way that Eve has no information about the key Alice and Bob exchanged. This private key then allows Alice and Bob to communicate with perfect secrecy using an encryption scheme such as the One-Time Pad. Such a scheme is very powerful as it allows for perfect secret communication between two parties relying only on the assumption that quantum physics describes accurately enough the laws of nature.



Alice's bit sequence:	0	0	1	0	1	0	1	1	1
Alice's filter scheme:	/	|	\	|	\	/	\	\	—
Bob's detection scheme:	+	+	+	+	×	+	+	×	+
Bob's bit measurements:	1	0	1	0	1	0	0	1	1
Retained bit sequence (key):	–	0	–	0	1	–	–	1	1

Figure 1: Short example of Alice and Bob sharing a key using QKD, such as in BB84 QKD up to the error estimation step

BB84 QKD Introduced by Bennett and Brassard in 1984 [2], this is one of the first working schemes to achieve quantum key

BB84-QKD

Preparation: Alices chooses random strings $X, \Theta \in \{0,1\}^N$ and sends the qubits $H^{\Theta_1} |X_1\rangle \cdots H^{\Theta_N} |X_N\rangle$ to Bob, where H^b with $b = 0, 1$ denotes two different bases in which the qubit is transformed (for example the Hadamard basis or the different photon polarizations). At the same time Bob chooses a random $\Theta' \in \{0,1\}^N$ and for $j = 1, \ldots, n$ measures the $j-$th qubit upon arrival in basis $H^{\Theta'_j}\{|0\rangle, |1\rangle\}$ to obtain Y_j, and he confirms the receipt of the qubits. Alice and Bob exchange Θ and Θ', and they update X and Y, respectively, by restricting them to the coordinates in $J = \{j : \Theta_j = \Theta'_j\}$

Error estimation: Alice chooses a random subset $Test \subset \{1, \ldots, n\}$ of linear size and sends it to Bob. Then, Alice and Bob exchange and compare $X_{Test} = (X_i)_{i \in Test}$ and $Y_{Test} = (Y_i)_{i \in Test}$. If they differ at too many positions Bob and Alice abort.

Error correction: Alice sends suitable error correcting information U to Bob that allows him to correct the remaining errors in Y and thus recover X.

Key extraction/Privacy Amplification: Alice and Bob apply a suitable function to transform the weakly-secret key X, for which Eve has some limited information, to a fully secure key K, about which Eve has no information by applying a suitably chosen function. This is generally done by means of universal hashing functions.

distribution[1]. It is shortly described in the following table. More QKD protocols such as Ekert91, B92 as well as security proofs and more details are provided in the PhD thesis of N.J. Beaudry [3].

Applications Although we often consider quantum computers to belong in the future in the last decade there have been a few successful implementations of quantum key distribution and there are a few companies that provide commercial QKD. But it is still only available in limited range networks and it usually depends on expensive and sensitive equipment so although it seems that QKD might be the future it is still a few steps away.

References

[1] **Quantum Cryptography** S Fehr *Foundations of Physics, 2010*

[2] **Quantum Cryptography: Public Key Distribution and Coin Tossing** Bennett and Brassard *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Vol. 175. No. 0. 1984.*

[3] **Assumptions in Quantum Cryptography** NJ Beaudry *PhD Thesis ETHZ, 2014*

[4] **Post-Quantum Cryptography** Wikipedia Article