Quantum Key Sharing

(1) Alice chooses a sequence of $(4+\delta)n$ uniformly random information bits $a = (a_i)$ and a sequence of $(4+\delta)n$ instruction bits $b = (b_i)$.
(2) Alice encodes a_i using states $|0\rangle$ and $|1\rangle$ if $b_i = 0$, and using states $|+\rangle$ and $|-\rangle$ if $b_i = 1$, and sends them to Bob.
(3) Bob chooses a sequence of $(4+\delta)n$ uniformly random decoding bits $c = (c_i)$ and measures the received qubits in the base $\{|0\rangle, |1\rangle\}$, if $c_i = 0$, and in the base $\{|+\rangle, |-\rangle\}$, if $c_i = 1$.
(4) Bob then publishes the sequence c and Alice publishes the sequence b.
(5) Alice and Bob choose $2n$ indexes for which $b_i = c_i$, and for which the value measured by Bob should be a_i. There are enough such indexes with a high probability controlled by the number δ.
(6) Uniformly randomly, Alice and Bob then choose half of these indexes to publicly verify that they are really equal. This gives them an idea of the degree of distortion that can be expected from the remaining bits.
(7) If the expected violation rate is acceptable, they use the remaining bits as a shared key (they can correct the corrupted bits using a self-correcting code mechanism).

Let's illustrate the principle of protocol security on the simplest attack, in which an attacker measures k individual qubits in one of the bases $|0\rangle, |1\rangle$ or $|+\rangle, |-\rangle$. Let's denote the choice of the attacker's base on a given qubit by e_i.

- If the i-th bit is attacked, the attacker knows the value of the a_i bit from the key if $b_i = c_i = e_i$ a i has not been selected for the public control. This happens on average in $k/8$ cases.
- On the other hand, the attack on the i-th bit is detected if $b_i = c_i \neq e_i$, i has been selected for the public control and the control reveals an inconsistency. Note that after the attacker measured the bit in the wrong base, it is in one of the base states of this wrong base, and the result of measuring in the correct base is therefore a uniformly random bit. Thus, the discrepancy is detected on average in $k/16$ cases.

Therefore, if the fault test detects t errors, the attacker can be expected to know about $2t$ bits. The meaning of the word „roughly“ corresponds to the central limit theorem, resp. Chernoff's bound.

The basic shortcoming of our analysis is the assumption of the form of the attack. It is the task of quantum information theory to obtain an upper bound on the amount of information obtainable by any attack, depending on the probability of detection.