

# Quantum key distribution (QKD)

February 21, 2002

All the messages are sent over a *public* (quantum or classical) line.

## 1 Bell-state-based, raw version

1. Alice prepares  $n$  states  $|\Phi^+\rangle$ , i.e.

$$|\Phi^+\rangle^{\otimes n} = \bigotimes_{j=1}^n |\Phi^+\rangle,$$

and sends the second qubit of each pair to Bob.

2. Bob announces to Alice that he received the  $n$  qubits.
3. Alice and Bob measure their qubits in the standard basis  $[|0\rangle\langle 0|, |1\rangle\langle 1|]$ , the outcome for both is  $\mathbf{k}[j] \in \{0, 1\}$ , for  $j \in \{1, \dots, n\}$ . If no noise or eavesdropping occurred, they now share  $\mathbf{k}$ , a  $n$ -bit long classical random key.

## 2 Bell-state-based, raw version with random sampling

1. Alice prepares  $2n$  states  $|\Phi^+\rangle$  and sends the second qubit of each pair to Bob.
2. Bob announces to Alice that he received the  $2n$  qubits.
  - S1. Alice chooses uniformly at random a set  $S$  of  $n$  positions among  $\{1, \dots, 2n\}$ , and sends  $S$  to Bob.
  - S2. Bob announces to Alice that he received  $S$ .
  - S3. Alice and Bob measure their qubits at the positions in  $S$  in the standard basis. They compare their classical outcomes. If the outcomes disagree at more than  $t$  positions then they decide to abort the protocol.
3. Alice and Bob measure their remaining  $n$  qubits in the standard basis. With probability exponentially close to 1 in  $n$ , i.e. greater than  $1 - e^{-\alpha n}$ , they now share a  $n$ -bit long classical random key with no more than  $\beta t$  errors.

### 3 Bell-state-based, with random sampling and error-correction

1. Alice prepares  $2n$  states  $|\Phi^+\rangle$  and sends the second qubit of each pair to Bob.
2. Bob announces to Alice that he received the  $2n$  qubits.
  - S1. Alice chooses uniformly at random a set  $S$  of  $n$  positions among  $\{1, \dots, 2n\}$ , and sends  $S$  to Bob.
  - S2. Bob announces to Alice that he received  $S$ .
  - S3. Alice and Bob measure their qubits at the positions in  $S$  in the standard basis. They compare their classical outcomes. If the outcomes disagree at more than  $t$  positions then they decide to abort the protocol.
- E1. Alice and Bob measure their remaining  $n$  qubits according to a  $[n, m]$  quantum error-correcting code that can correct errors occurring on up to  $\beta t$  qubits. They correct their states and obtain, with probability exponentially close to 1,  $m$  Bell pairs.
3. Alice and Bob measure their remaining  $m$  qubits in the standard basis. They now share a secure  $m$ -bit long classical random key.

## 4 Principles involved in the proof of security

- Random sampling sets an upper bound on the number of errors in the remaining positions.
- High fidelity implies low entropy, implies an upper bound on the mutual information between the eavesdropper and the messages.
- *Good* quantum error correcting codes exist and error-correction can be performed locally by Alice and Bob if they use a *stabilizer* code.
- The Bell-state-based protocol may be modified into an equally secure *BB84-state*-based protocol that does not require robust quantum computing and quantum information storage.