BB84

Luc Spachmann

3. Februar 2022

Allgemeines

- Quantenprotokoll zum Schlüsseltausch
- Kann als Schlüssel für Onetime Pad verwendet werden
- Fast alle asymmetrischen Verfahren unsicher gegen Quantencomputer

Qubit

- Beschreibt einen Quantenzustand
- Kann mit einer beliebigen Basis $|0\rangle, |1\rangle$ und $a, b \in \mathbb{C}$ beschrieben werden

$$q = a|0\rangle + b|1\rangle$$

  mit $|a|^2 + |b|^2 = 1$
- 'No-Cloning-Theorem': Qubits können nicht kopiert werden
- Qubits können nur in Basis ausgewertet werden
- Ergebnis ist $|0\rangle$ mit W'keit $|a|^2$, und $|1\rangle$ mit W'keit $|b|^2$
- Alternative Basis: Hadamar-Basis:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

- Angepasste Parameter können genau so berechnet werden

BB84 Protokoll

- Alice erzeugt Zufallsbits $a_1, ..., a_n$ und $a'_1, ..., a'_n$.
- Alice kodiert das Bit a_i als $\begin{cases} |0\rangle \text{ bzw. } |1\rangle, \text{ falls } a'_i = 0 \\ |+\rangle \text{ bzw. } |-\rangle, \text{ falls } a'_i = 1 \end{cases}$
- Alice sendet kodierte Bits $a_1, ..., a_n$ über Quantenkanal an Bob
- Bob erzeugt Zufallsbits $b'_1, ..., b'_n$
- Bob misst a_i in der Basis $\begin{cases} |0\rangle \text{ bzw. } |1\rangle, \text{ falls } b'_i = 0 \\ |+\rangle \text{ bzw. } |-\rangle, \text{ falls } b'_i = 1 \end{cases}$
- Alice und Bob vergleichen $a'_1, ...$ und $b'_1, ...$ über klassischen ungesicherten Kanal
- Ist $a'_i \neq b'_i$ werden a_i, b_i gelöscht
- Alice und Bob tauschen k zufällige Bits a_i, b_i aus und vergleichen.
- Bei Fehler: Abbruch

Aufgaben

- Implementiert das BB84 Protokoll