Einführung in die Quantenkryptographie

Irene Diener, Toni Roob, Jarod A. M. Békési

30. September 2025

Inhaltsverzeichnis I

BB84

Entwickelt durch Charles Bennett und Gilles Brassard im Jahr 1984

Übung[1]

Frage

Weshalb sollte Bob die Orientierungen bei seinen Messungen zufällig wählen?
Welche Gefahr besteht, wenn er für die Orientierungen beispielsweise abwechselnd h/v und $+/-$ wählt?

---

[1] Quelle [Fil23]

Übung[1]

Antwort

Die Gefahr besteht darin, dass Eve diese Vorliebe von Bob kennt.
In diesem Fall wählt sie dieselben Orientierungen bei den Messungen wie Bob. Wenn Alice und Bob später ihre gewählten Basissysteme vergleichen, erhalten sie dieselben Übereinstimmungen wie Alice und Eve. Bei den Photonen, bei denen die Orientierungen von Eve und Bob sich von denen von Alice unterscheiden, können die Messwerte verschieden sein, doch diese Bits werden verworfen. Bei den Bits, die behalten werden, stimmen Eve, Bob und Alice überein. Alice und Bob werden also nicht bemerken, dass sie belauscht wurden.

---

[1] Quelle [Fil23]

Inhaltsverzeichnis I

Inhaltsverzeichnis I

Inhaltsverzeichnis I

Quellenverzeichnis I

Filk, Thomas:
BB48 – Quantenkryptographie.
https://physikdidaktik.uni-freiburg.de/wp-content/uploads/2023/06/BB84-Quantenkryptographie.pdf.
Version: Juni 2023, Abruf: 17.09.2025