SIMULATION EINER SCHLÜSSEL-GENERIERUNG NACH DEM BB84-PROTOKOLL

AUSTAUSCH VON DATEN

Die eigentlichen Informationen werden beim BB84-Protokoll in Form von Bit-Werten in der Polarisation verschlüsselt. Dafür ordnet man jeweils einem der beiden Polarisationszustände einer Basis den Bitwert 1 und dem anderen Zustand den Bitwert 0 zu. Die Zuordnung kann Beispielsweise wie rechts dargestellt aussehen.
Es gibt jetzt für jeden Bitwert zwei mögliche Kodierungen. Das ist genau so gewollt, um einen sicheren Schlüssel zu generieren.

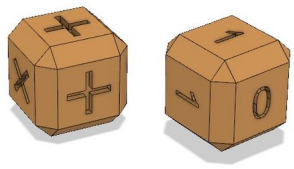
Basis	Pol.	Bit
×	$\|\nearrow\rangle$	1
×	$\|\nwarrow\rangle$	0
+	$\|\uparrow\rangle$	1
+	$\|\rightarrow\rangle$	0

EIN SICHERER SCHLÜSSEL

Damit ein Schlüssel sicher ist, dürfen nur Alice und Bob darauf Zugriff haben. Dazu muss im Wesentlichen dafür gesorgt werden, dass von der Kommunikation zwischen Alice und Bob nicht ausreichend Daten abgehört werden können, um den vollständigen Schlüssel daraus zu generieren. Außerdem sollte im Idealfall auffallen, wenn der Austausch des Schlüssels abgehört wird.
Mit dem BB84-Protokoll wird beides erreicht. Dazu nutzt man aus, dass Bob bei gleichen Basen ein verlässliches Messergebnis erhält und bei ungleichen Basen ein zufälliges Ergebnis misst. Durch die doppelte Belegung der Bitwerte können gerade beide Situationen auftreten. Durch eine zufällige Kombination beider Fälle kann dann ein sicherer Schlüsselaustausch erfolgen.

SIMULATION DES ZUFALLS

Weil bei dem vorhanden Experimentiermaterial keine Einzelphotonen genutzt werden, muss nachgeholfen werden, um den „Quantenzufall“ zu simulieren. Dazu werden Würfel (Siehe Abb. Rechts) verwendet. Es gibt einen Würfel, mit dem eine zufällig Basis gewählt werden kann und einen Würfel mit dem zufällig



Würfel zur Simulation des Zufalls

DURCHFÜHRUNG DES PROTOKOLLS

Auf den nächsten Seiten wird das BB84-Protokoll beispielhaft durchgespielt. Dazu wird in zwei Gruppen gearbeitet. Eine Gruppe bedient den Aufbau von Alice, eine den Aufbau von Bob.
Für die Durchführung des Protokolls wird neben dem vorhandenen Kommunikationskanal mit Einzelphotonen als Informationsträger noch ein zweiter Kanal benötigt. Dieser Kanal ist öffentlich und hat keine besonderen technischen Anforderungen. In der Realität könnte das beispielsweise eine Kommunikation durch das Internet sein. Im Modell können die entsprechenden Informationen einfach mündlich ausgetauscht werden.

1 Führt+ jetzt den Schlüsselaustausch durch.

- Teilt euch dazu in zwei Gruppen auf.
- Die erste Gruppe spielt die Rolle von Alice und orientiert sich an der entsprechenden Anleitung.
- Die zweite Gruppe spielt die Rolle von Bob. Auch dafür gibt es eine entsprechende Anleitung.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

ALICE' AUFGABE

ERZEUGUNG DES SCHLÜSSELS

Alice entscheidet sich für jedes übertragene Bit zufällig für einen Zustand. Dazu wählt sie jeweils eine Basis und einen Bitwert. Anschließend wird der entsprechende Polfilter in der korrekten Ausrichtung auf das Gitter gesetzt.

Basis	Pol.	Bit
×	$\|\nearrow\rangle$	1
×	$\|\nwarrow\rangle$	0
+	$\|\uparrow\rangle$	1
+	$\|\rightarrow\rangle$	0

① Versende zunächst 14 Bits in unterschiedlichen Basen an Bob. Gehe für jedes Bit wie folgt vor:

a) Wähle zufällig eine Basis und einen Bitwert (z.B. durch Würfeln).
b) Setze den entsprechenden Polfilter in der richtigen Ausrichtung auf das Gitter.
c) Sende den Bitwert, indem Du die LED aktivieren.
d) Notiere die Basis und den Bitwert in der Tabelle.

Messung	1	2	3	4	5	6	7
Basis							
Bitwert							

Messung	8	9	10	11	12	13	14
Basis							
Bitwert							

② Vergleiche für alle Bits die verwendete **Basis** mit der von Bob und streiche alle Spalten, in denen sich die Basis von Bobs Basis unterscheidet. Notiere die übrigen Bitwerte als *One-Time-Pad*.

One-Time-Pad
(Streng Geheim) _____

Schlüssellänge
Damit ein einzelner Buchstabe verschlüsselt werden kann, sind fünf Bits nötig. Bei 14 übertragenen Bits und einer Wahrscheinlichkeit für die gleiche Basis von 50%, liegt der Erwartungswert bei sieben Bits. Normalerweise sind also ausreichend viele Bits vorhanden. Sollte das One-Time-Pad zu kurz sein müssen weitere Bits ausgetauscht werden. Besonders bei sehr großen Mengen lässt sich über den Erwartungswert sehr gut abschätzen, wie viele Bits notwendig sind um einen ausreichend langen Schlüssel zu erzeugen, so dass die Zufallskomponente nicht zu Problemen in der Durchführung führt.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

VERWENDUNG DES SCHLÜSSELS

③ Verschlüssle einen beliebigen Buchstaben im (vereinfachten) ASCII-Format. Gehe dazu wie folgt vor:

a) Suche dir einen beliebigen Buchstaben aus und notiere die vereinfachte ASCII-Codierung (Tab. 1):

b) Addiere den Schlüssel zum gewählten Buchstaben (es gilt 1+0=1 und 1+1=0). So ergibt sich die verschlüsselte „Nachricht“.

Ausgewählter Buchstabe: ☐

Buchstabe in ASCII-Format: ☐☐☐☐☐

One-Time-Pad (Erste 5 Stellen) ☐☐☐☐☐

Verschlüsselter Buchstabe: ☐☐☐☐☐

c) Gib den verschlüsselten Buchstaben **öffentlich** an Bob weiter. Gleiche Deinen unverschlüsselten Buchstaben mit Bob ab, sobald er deine Nachricht entschlüsselt hat.

Schlüssel zu kurz?
Falls der Schlüssel weniger als 5 Stellen lang ist, werden die ersten Stellen des Schlüssels noch einmal verwendet.

Vereinfachte ASCII-Tabelle

A	00001	J	01010	S	10011
B	00010	K	01011	T	10100
C	00011	L	01100	U	10101
D	00100	M	01101	V	10110
E	00101	N	01110	W	10111
F	00110	O	01111	X	11000
G	00111	P	10000	Y	11001
H	01000	Q	10001	Z	11010
I	01001	R	10010	Φ	11011

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

BOBS AUFGABE

ERZEUGUNG DES SCHLÜSSELS

Bob entscheidet sich für jedes übertragene Bit zufällig für eine Basis, in der er Messen möchte. Falls das Ergebnis im Modellexperiment uneindeutig ist, muss er dann außerdem noch zufällig einen der beiden Bitwerte auswählen.

① Empfange 14 Bits von Alice. Gehe wie folgt vor.

a) Wähle zufällig eine Basis und stelle den Doppelpolfilter entsprechend ein. Notiere die Basis in der untenstehenden Tabelle
b) Gib Alice ein Zeichen, dass Du bereit für eine Übertragung bist.
c) Falls du ein eindeutiges Ergebnis misst, notieren den zugehörigen Bitwert in der untenstehenden Tabelle.
d) Falls du kein eindeutiges Ergebnis misst, entscheide dich zufällig für einen Bitwert und notieren diesen.

Basis	Pol.	Bit
×	$\|\nearrow\rangle$	1
×	$\|\nwarrow\rangle$	0
+	$\|\uparrow\rangle$	1
+	$\|\rightarrow\rangle$	0

Messung	1	2	3	4	5	6	7
Basis							
Bitwert							

Messung	8	9	10	11	12	13	14
Basis							
Bitwert							

② Vergleiche für alle Bits die verwendete **Basis** mit der von Alice und streiche alle Spalten, in denen sich die Basis von Alice' Basis unterscheidet. Notiere die übrigen Bitwerte als One-Time-Pad.

One-Time-Pad
(Streng Geheim) _____

Schlüssellänge
Damit ein einzelner Buchstabe verschlüsselt werden kann, sind fünf Bits nötig. Bei 14 übertragenen Bits und einer Wahrscheinlichkeit für die gleiche Basis von 50%, liegt der Erwartungswert bei sieben Bits. Normalerweise sind also ausreichend viele Bits vorhanden. Sollte das One-Time-Pad zu kurz sein müssen weitere Bits ausgetauscht werden. Besonders bei sehr großen Mengen lässt sich über den Erwartungswert sehr gut abschätzen, wie viele Bits notwendig sind um einen ausreichend langen Schlüssel zu erzeugen, so dass die Zufallskomponente nicht zu Problemen in der Durchführung führt.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

VERWENDUNG DES SCHLÜSSELS

③ Alice verwendet jetzt den Schlüssel um einen Buchstaben zu verschlüsseln. An dieser Stelle musst du dich einen Moment gedulden. Entschlüssle dann den verschlüsselten Buchstaben, den Alice dir mitteilt, wie folgt:

a) Notiere den verschlüsselten Buchstaben, den Alice dir übermittelt.
b) Addiere den Schlüssel zum verschlüsselten Buchstaben (es gilt 1+1=0). So ergibt sich der unverschlüsselte Buchstabe im Ascii-Format. Falls der Schlüssel weniger als 7 Stellen lang ist, werden die ersten Stellen des Schlüssels noch einmal verwendet.
c) Nutze die ASCII-Tabelle (Tabelle 3), um den Buchstaben zu bestimmen, und gleiche diesen mit Alice ab.

Verschlüsselter Buchstabe: ☐

Verschlüsselter Buchstabe (ASCII): ☐☐☐☐☐☐☐

One-Time-Pad (Erste 7 Stellen) ☐☐☐☐☐☐☐

Entschlüsselter Buchstabe (ASCII): ☐☐☐☐☐☐☐

Entschlüsselter Buchstabe: ☐

Vereinfachte ASCII-Tabelle

A	00001	J	01010	S	10011
B	00010	K	01011	T	10100
C	00011	L	01100	U	10101
D	00100	M	01101	V	10110
E	00101	N	01110	W	10111
F	00110	O	01111	X	11000
G	00111	P	10000	Y	11001
H	01000	Q	10001	Z	11010
I	01001	R	10010	Φ	11011

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG