1. Abhängig von b_0, b_1 berechnet Alice:
   Falls $b_0 = 1$: Flip auf 1. Qubit
   Falls $b_1 = 1$: NOT auf 1. Qubit

b_0	b_1	Zustand
0	0	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
0	1	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
1	0	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle$
1	1	$\frac{1}{\sqrt{2}}(\|10\rangle - \|01\rangle$

   Alice sendet $|z\rangle$ an Bob.
2. Bob wendet die folgende unitäre Matrix U auf $|z\rangle$ an.

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix}$$

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \overset{U}{\longmapsto} \frac{1}{2}(|00\rangle + |10\rangle + |00\rangle - |10\rangle) = |00\rangle$ Interpretation: $(b_0, b_1) = (0, 0)$
$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \overset{U}{\longmapsto} \frac{1}{2}(|00\rangle + |10\rangle - |00\rangle + |10\rangle) = |01\rangle$ Interpretation: $(b_0, b_1) = (0, 1)$
$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \overset{U}{\longmapsto} \frac{1}{2}(|00\rangle + |10\rangle - |00\rangle + |10\rangle) = |10\rangle$ Interpretation: $(b_0, b_1) = (1, 0)$
$\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \overset{U}{\longmapsto} \frac{1}{2}(-|01\rangle + |11\rangle + |01\rangle + |11\rangle) = |11\rangle$ Interpretation: $(b_0, b_1) = (1, 1)$

7.3 Quanten Schlüsselaustausch

One-Time Pad für n-Bit Nachricht $m = m_1 m_2 \dots m_n \in \{0,1\}^n$

Alice $(SK = k_1 \dots k_n \in \{0,1\}^n)$ $\xrightarrow{E_{SK}(m) = m \oplus SK}$ Bob $(SK = k_1 \dots k_n \in \{0,1\}^n)$

$D_{SK}(E_{SK}(m)) = E_{sk}(m) \oplus SK = m \oplus SK \oplus SK = m$

Szenario:
- Alice und Bob besitzen Quantenkanal
- Alice und Bob besitzen authentisierten klassischen Kanal
- Kanäle werden belauscht und manipuliert durch Eve.

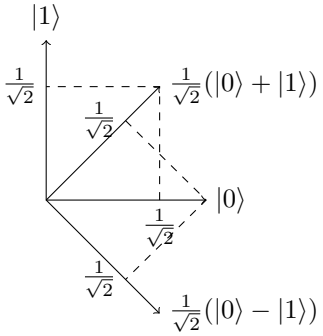
Ziel: Austausch von n klassischen Bits, so dass

- Eve durch Belauschen keine Information erhält
- Manipulation von Eve entdeckt wird

Einfache Lösung: falls Alice und Bob n EPR-Paare $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$teilen:
Messen in derselben Basis $|0\rangle$, $|1\rangle$ liefert n identische Zufallsbits.

Definition(Z und X-Basis): Wir nennen $|0\rangle$, $|1\rangle$ die Z-Basis des $\mathbb{C}^2$
Die Basis $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, die durch Anwendung von W_2 auf die Basisvektoren der Z-Basis entsteht, bezeichnen wir als X-Basis.

Beobachtung:
- Messung von $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ in Z-Basis liefert $|0\rangle$, $|1\rangle$ jeweils mit $Ws.\frac{1}{2}$.
- Messung von $|0\rangle$ oder $|1\rangle$ in X-Basis liefert $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ jeweils mit $Ws.\frac{1}{2}$.



Idee: Kodiere Bit $a \in \{0,1\}$ entweder in der X-Basis oder in der Z-Basis.

Kodierungstabelle:

Bit a	Basis b	Zustand $\|z_{ab}\rangle$
0	0	$\|z_{00}\rangle = \|0\rangle$
1	0	$\|z_{10}\rangle = \|1\rangle$
0	1	$\|z_{01}\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
1	1	$\|z_{11}\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$

, 0 = Z-Basis, 1 = X-Basis

7.3.1 BB84-Protokoll (Bennet-Brassard)

1. Alice wählt zufällige $4n$-Bit Strings $a = a_1 \dots a_{4n}, a = b_1 \dots b_{4n} \in \{0,1\}^{4n}$.
   Alice sendet 4n Qubits $|z_{a_i b_i}\rangle, i = 1 \dots 4n$ an Bob

2. Bob wählt einen zufälligen Bitstring $b' = b'_1 \dots b'_{4n} \in \{0,1\}$.
   Falls $b_i = 0$ Messe $|z_{a_i b_i}\rangle$ zur Z-Basis. Falls $|0\rangle$, setze $a'_i = 0$, sonst $a'_i = 1$
   Falls $b_i = 1$ Messe $|z_{a_i b_i}\rangle$ zur X-Basis. Falls $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, setze $a'_i = 0$, sonst $a'_i = 1$
   Bob erklärt, dass er gemessen hat.

3. Alice gibt die Basen $b_1, \dots, b_{4n}$ bekannt. Für $b_i \neq b'_i$ wird das i-te Bit a_i verworfen.
   Im Erwartungswert bleiben $2n$ Bits übrig.

4. Alice und Bob vergleichen von den $2n$ übrigen Bits n zufällig gewählte Testbits. Stimmen nicht alle Testbits überein, Abbruch (Manipulationsversuch von Eve). Sonst bilden die restlichen n Bits den geheimen Schlüssel SK.

Korrektheit: Falls keine Manipulation der Qubits vorliegt, gilt $Ws(a_i = a'_i | b_i = b'_i) = 1$, denn Bob misst Basiszustand in der korrekt gewählten Basis.

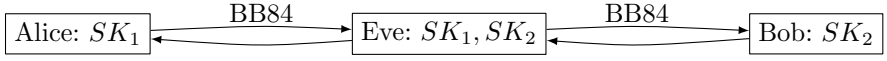
Sicherheit: Eve erhält nur dann das i-te Bit, falls sie $|z_{a_i b_i}\rangle$ misst.

1. Fall: Eve misst zur korrekten Basis mit Ws. $\frac{1}{2}$. In diesem Fall sendet sie $|z_{a_i b_i}\rangle$ an Bob und kennt a_i.

2. Fall: Eve misst zur inkorrekten Basis $\bar{b_i}$ mit Ws. $\frac{1}{2}$.
Sie sendet $|z_{\tilde{a_i}\hat{b_i}}\rangle$ an Bob, wobei $\tilde{a_i} \in_R \{0,1\}$. Misst Bob in Basis b_i, so erhält er a'_i mit $Ws(a'_i = a_i) = \frac{1}{2}$.
D.h. wird das i-te Bit für die Menge der Testbits ausgewählt, erfolgt Abbruch mit $Ws.\frac{1}{2}$.

Damit ist nicht schwer zu zeigen, das Eves Erfolgswahrscheinlichkeit, unbemerkt k bits zu ermitteln exponentiell klein in k ist.

Beobachtungen:
- Eve kann Denial-of-Service Angriff durchführen, d.h. Abbruch erzwingen.
- Bei nicht-authentisierten Kanal kann Eve Man-in-the-Middle Angriff durchführen.



7.3.2 BB92-Protokoll (Bennet)

Führe die folgenden Schritte durch, bis n Bits ausgetauscht wurden:

1. Alice wählt ein Zufallsbit $a \in_R \{0,1\}$ und sendet: $|z\rangle = \begin{cases} |0\rangle & \text{falls } a = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \text{falls } a = 1 \end{cases}$

2. Bob wählt $a' \in_R \{0,1\}$. Bob misst $|z\rangle$ in der

   - Z-Basis für $a' = 0$: Falls Ergebnis $|0\rangle$, setze $b = 0$, sonst setze $b = 1$.
   - X-Basis für $a' = 1$: Falls Ergebnis $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, setze $b = 0$, sonst setze $b = 1$.

   Bob sendet b an Alice

3. Falls $b = 0$: Zurück zu Schritt 1.
   Falls $b = 1$: Schlüsselbit ist a für Alice, $1 - a'$ für Bob

In jedem Durchlauf wird ein Schlüsselbit generiert gdw. $b = 1$ gilt.

Satz: Ws. $(b = 1) = \frac{1}{4}$

Beweis: Es gilt

$$\text{Ws.}\,(b=1) = \text{Ws.}\,(b=1|a=a')\cdot\text{Ws.}\,(a=a') + \text{Ws.}\,(b=1|a\neq a')\cdot\text{Ws.}\,(a\neq a') = 0\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}.$$

Denn im Fall $a = a'$ misst Bob stets den von Alice gesendeten Basiszustand ($b = 0$), im Fall $a \neq a'$ misst Bob einen anderen Zustand mit Ws. $\frac{1}{2}$

D.h also, dass wir im Erwartungswert $4n$ Protokolldurchläufe benötigen, bis n Schlüsselbits generiert sind. Es bleibt zu zeigen, dass die erzeugten Schlüsselbits korrekt sind, d.h $a = 1 - a'$.

Satz: Ws. $(a = 1 - a'|b = 1) = 1$

Beweis: Es gilt Ws. $(a = 1 - a'|b = 1 \cdot$ Ws. $(b = 1) =$ Ws. $(b = 1|a = 1 - a') \cdot$ Ws. $(a = 1 - a')$
$\Rightarrow$ Ws. $(a = 1 - a'|b = 1) = \frac{\text{Ws.}\,(b=1|a=1-a')\cdot\text{Ws.}\,(a=1-a')}{\text{Ws.}\,(b=1)} = \frac{\frac{1}{2}\cdot\frac{1}{2}}{\frac{1}{4}} = 1$
D.h. falls $b = 1$, so müssen a und a' verschiedene Bits sein. Damit erhalten Alice und Bob dasselbe Bit $a = 1 - a'$

8 Boolesche Schaltkreise, Schaltkreiskomplexitäten

Ziel: Berechne Boolesche Funktion $f_n : \mathbb{F}_2^n \to \mathbb{F}_2^m, n \in \mathbb{N}$

Beispiel: Und $\wedge : \mathbb{F}_2^2 \to \mathbb{F}_2, (x_1, x_2) \overset{\wedge}{\longmapsto} x_1 \wedge x_2 = x_1x_2$ bzw. $\mathbb{F}_2^n \to \mathbb{F}_2$,
$(x_1, \ldots, x_n) \mapsto (((x_1 \wedge x_2) \wedge x_3) \ldots x_n)$

Oder $\vee : \mathbb{F}_2^2 \to \mathbb{F}_2, (x_1, x_2) \overset{\vee}{\longmapsto} x_1 \vee x_2 = x_1 + x_2 + x_1x_2$ bzw. $\mathbb{F}_2^n \to \mathbb{F}_2$,
$(x1, \ldots, x_n) \mapsto (((x_1 \vee x_2) \vee x_3) \ldots x_n)$

Nicht $\neg : \mathbb{F}_2 \to FZ, x \overset{\neg}{\longmapsto} 1 - x$ Schreibweise auch: $\overline{x}$

Kopierfunktion $\mathtt{c} : \mathbb{F}_2 \to \mathbb{F}_2^2, x \overset{\mathtt{c}}{\longmapsto} (x, x)$

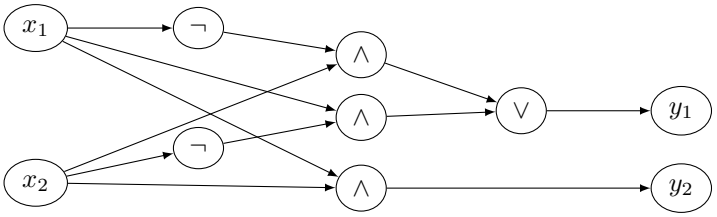
Entscheiden von Sprachen $\mathtt{L} : X_{\mathtt{L}} : \mathbb{F}_2^n \to \mathbb{F}_2, X_{\mathtt{L}}(\omega) = \begin{cases} 1 & \text{falls } \omega \in \mathtt{L} \\ 0 & \text{sonst} \end{cases}$

Definition (Boolescher Schaltkreis): Sei S eine Menge von Booleschen Funktionen, die eine konstante Anzahl von Eingabebits auf eine konstante Anzahl von Ausgabebits abbildet (z.b. $S = \{\wedge, \vee, \neg\}$)
Ein Boolescher Schaltkreis über S ist ein azyklischer, gerichteter Graph $G = (V, E)$ mit:

- Die Knoten V sind gelabelt mit Eingabe-/Ausgabevariablen oder Elementen aus S.
- Eingabeknoten haben Eingrad 0. Ausgabeknoten haben Eingrad 1, Ausgrad 0.
- Knoten mit Label $s \in S, s : \mathbb{F}_2^n \to \mathbb{F}_2^m$ haben Eingrad n und Ausgrad m.
- Die Komplexität des Booleschen Schaltkreises ist definiert als $|V| + |E|$ (Bezüglich S).

Beispiel: Addierer $f(x_1, x_2) = (y_1, y_2)$ mit $y_1 = x_1 \oplus x_2, y_2$ Übertrag

x_1	x_2	y_1	y_2
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1



Komplexität bezüglich $\{\wedge, \vee, \neg\} : |V| + |E| = 10 + 12 = 22$