2. Bob wendet die folgende unitäre Matrix $\mathcal{U}$ auf $|z\rangle$ an.

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

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

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

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

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

Quanten Schlüsselaustausch

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

$$\boxed{\begin{array}{l}\text{Alice} \\ SK = k_1 \dots k_n \in \{0,1\}^n\end{array}} \xrightarrow[= m \oplus SK]{E_{SK}(m)} \boxed{\begin{array}{l}\text{Bob} \\ SK = k_1 \dots k_n \in \{0,1\}^n\end{array}}$$

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

Szenario:
- Alice und Bob besitzen Quantenkanal
- —— " —— 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

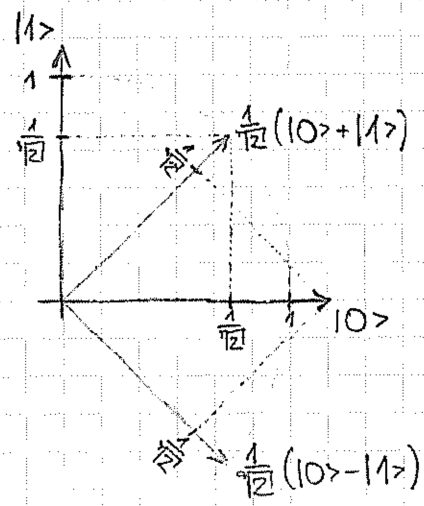
Einfache Lösung, falls Alice & Bob n EPR-Paare $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$ teilen:

Messen in derselben Basis $|0\rangle, |1\rangle$ liefert n identische Zufallsbits.

Def (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 " $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ —— " ——.



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

Kodierungstabelle:

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

BB84 - Protokoll (Bennett - Brassard)

1. Alice wählt zufällige 4n-Bit Strings $a = a_1 \dots a_{4n}, b = b_1 \dots b_{4n} \in \{0,1\}^{4n}$.
   Alice sendet 4n Qubits $|z_{a_i b_i}\rangle$, $i = 1 \dots 4n$, an Bob.
2. Bob wählt einen zufälligen Bitstring $b' = b'_1 \dots b'_{4n} \in \{0,1\}^{4n}$.
   Falls $b'_i = 0$: Messe $|z_{a_i b_i}\rangle$ zur Z-Basis. Falls $|0\rangle$, setze $a'_i = 0$. Sonst $a'_i = 1$.
   $b'_i = 1$: 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

$$Ws(a_i = a'_i \mid b_i = b'_i) = 1,$$ denn Bob misst Basiszustände in der korrekt gewählten Basis.

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

<u>1. Fall</u>: 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.

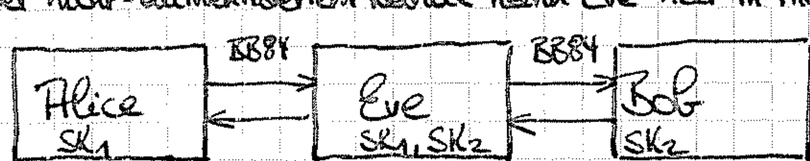
<u>2. Fall</u>: Eve misst zur inkorrekten Basis $\bar{b}_i$ mit Ws $\frac{1}{2}$.

Sie sendet $|z_{\tilde{a}_i \bar{b}_i}\rangle$ an Bob, wobei $\tilde{a}_i \in_R \{0,1\}$. Misst Bob in Basis b_i, so erhält er a_i' mit $Pr(a_i' = a_i) = \frac{1}{2}$.

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, dass Eves Erfolgsws., unbemerkt k Bits zu ermitteln, exponentiell klein in k ist.

<u>Beobachtungen</u>:
- Eve kann Denial-of-Service Angriff durchführen, d.h. Abbruch erzwingen.
- Bei nicht-authentisierten Kanal kann Eve Meet-in-the-Middle Angriff durchführe



<u>B92 Protokoll (Bennett)</u>

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 $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, ——— " ———.

   Sende 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.

<u>Satz</u>: $Ws(b=1) = \frac{1}{4}$