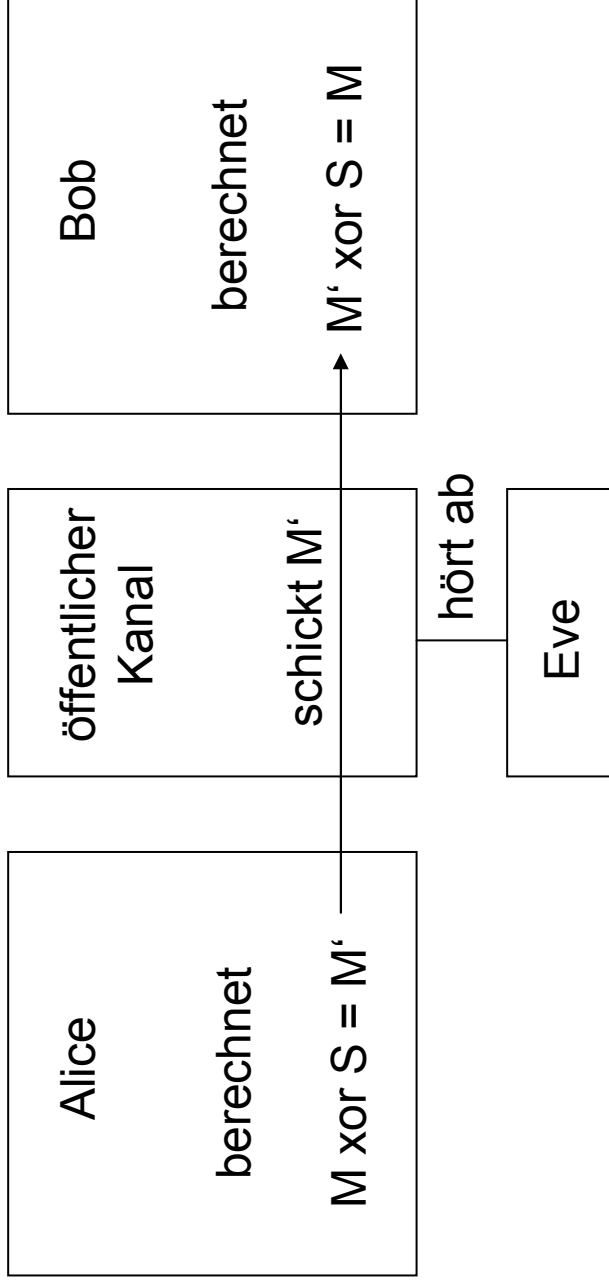


Quantenkryptographie

Marc Rochel

1 Sicheres klassisches Protokoll

- Alice und Bob besitzen einen Schlüssel S ,
- Alice möchte Nachricht M an Bob schicken
- $\text{Länge}(M) \leq \text{Länge}(S)$



2 Informationsgewinn impliziert Störungen

Seien $|\psi\rangle$ und $|\varphi\rangle$ verschiedene, nicht orthogonale Zustände, $|u\rangle$ Eves Qubits.

Eves Operation:

$$|\psi\rangle|u\rangle \rightarrow |\psi\rangle|v\rangle$$

$$|\varphi\rangle|u\rangle \rightarrow |\varphi\rangle|v'\rangle$$

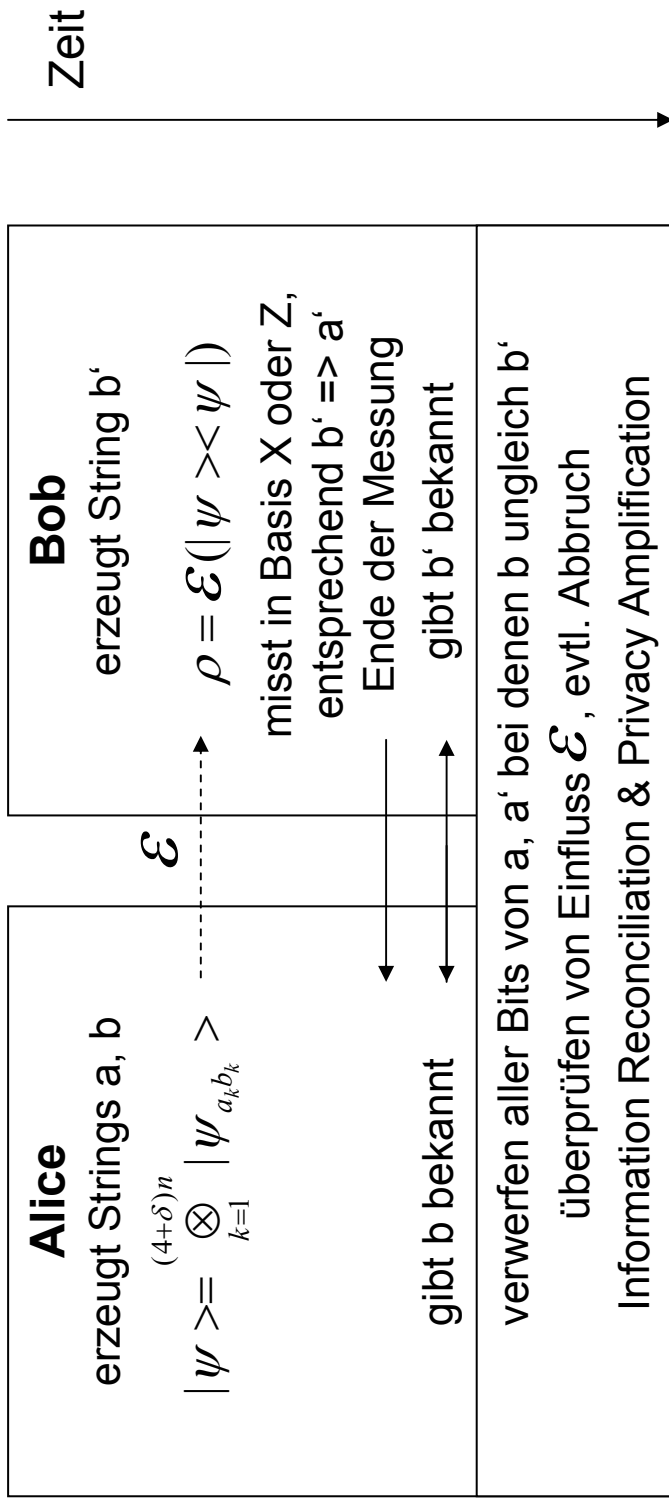
$$\Rightarrow (|\psi\rangle|u\rangle, |\varphi\rangle|u\rangle) = (|\psi\rangle|v\rangle, |\varphi\rangle|v'\rangle)$$

$$\Leftrightarrow \langle \psi | \varphi \rangle \langle u | u \rangle = \langle v | v' \rangle \langle \psi | \varphi \rangle$$

$$\Leftrightarrow |v\rangle = |v'\rangle$$

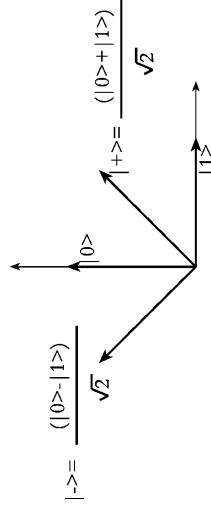
Eve kann so nicht zwischen den beiden Zuständen unterscheiden!
Also stört Eves Abhören die Übertragung.

2.1 Das BB84 Protokoll

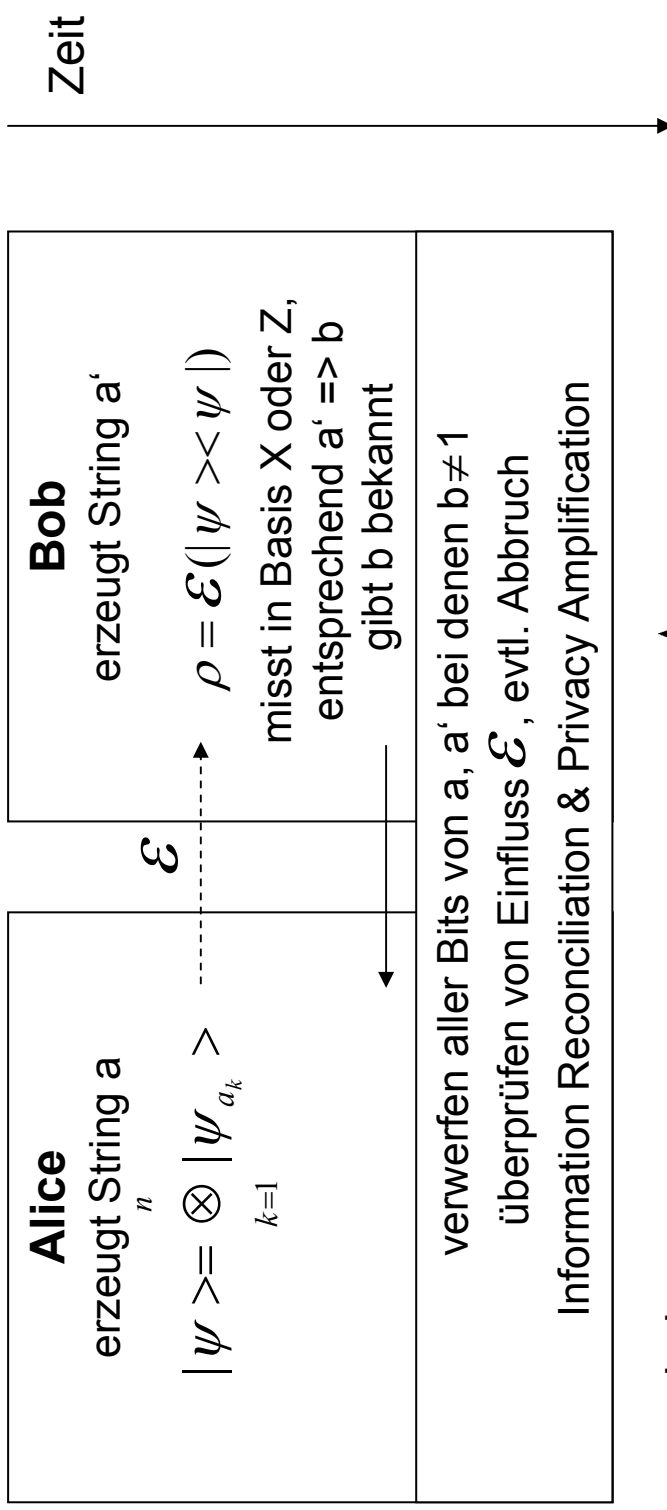


wobei

$$\begin{aligned}
 |\psi_{00}\rangle &= |0\rangle \\
 |\psi_{10}\rangle &= |1\rangle \\
 |\psi_{01}\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
 |\psi_{11}\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}}
 \end{aligned}$$



2.2 Das B92 Protokoll

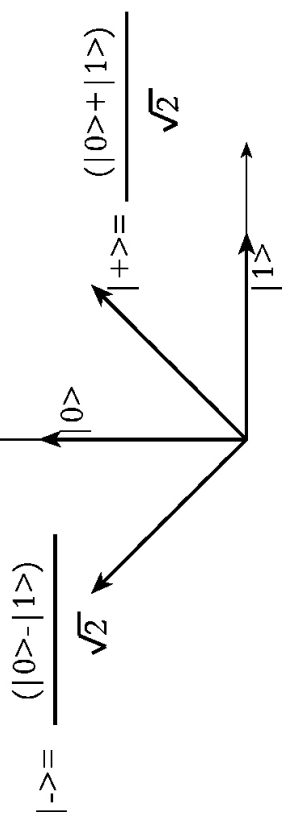


wobei $|\psi_0\rangle = |0\rangle$

$$|\psi_1\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$$

2.2 Das B92 Protokoll

$$|\psi_0\rangle = |0\rangle$$



$$|\psi_1\rangle = |+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$$

Alices Bit a_k	Bobs Bit a'_k	Bobs Messung b_k
0	0	0
0	1	0 mit Wk 0.5 1 mit Wk 0.5
1	0	0 mit Wk 0.5 1 mit Wk 0.5
1	1	0

2.3 Das EPR Protokoll

Alice und Bob teilen sich EPR Paare:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Zustand des EPR Paares vor der Messung	Alices Messung ihres Bits	Zustand des Qubit Paares nach Alices Messung
$\frac{ 00\rangle + 11\rangle}{\sqrt{2}}$	0	$ 00\rangle$
	1	$ 11\rangle$

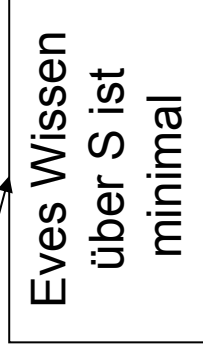
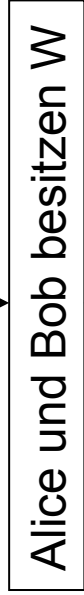
3 Information Reconciliation & Privacy Amplification

Strings X, Y, Z, W

X, Y, Z
korreliert



W, Z
korreliert



3 Information Reconciliation & Privacy Amplification

nötiges Vorwissen:

- Klasse der universalen Hashfunktionen G
 A, B Mengen von n -Bit, bzw. m -Bit Strings, Elemente von $G: A \rightarrow B$

$$\forall a_1, a_2 \in A \wedge a_1 \neq a_2. \mu\{G(a_1) = G(a_2)\} \leq \frac{1}{|B|}$$

- Collision Entropy: $H_c(X) = -\log\left(\sum_x p(x)^2\right)$ ($H(X) \geq H_c(X)$)

▪ Theorem 1: $H(G(X) | G) \geq H_c(G(X) | G) \geq m - 2^{m-H_c(X)}$

▪ Theorem 2: $H_c(X | U = u) \geq H_c(X) - 2\log_2 |U'| - 2s$

mit einer Wahrscheinlichkeit $\geq 1 - 2^{-s}$, $s > 0$

3 Information Reconciliation & Privacy Amplification

Betrachtung der Privacy Amplification:

Sei $H_c(W | Z = z) \geq d$

Dann gilt nach Theorem 1: $m \geq H_c(S | G, Z = z) \geq m - 2^{m-d}$

Berücksichtigung der Information Reconciliation:

Durch Übermittlung der Nachricht u erfährt Eve: $k > H(W | Y)$

Dann gilt nach Theorem 2:

$$H_c(W | Z = z, U = u) \geq H_c(W | Z = z) - 2 \log_2 |U'| - 2s \geq d - 2(k + s)$$

Zusammen mit Theorem 1:

$$m \geq H_c(S | G, Z = z, U = u) \geq m - 2^{m-d+2(k+s)}$$

4.1 Privacy und Kohärente Information

▪ Theorem 3, Holevo Bound: $H(X : Y) \leq S(\rho) - \sum_x p_x S(\rho_x)$

Also gilt: $H_{Bob:Alice} \leq \chi^B = S(\rho^B) - \sum_k p_k S(p_k^B)$

$H_{Eve:Alice} \leq \chi^E = S(\rho^E) - \sum_k p_k S(p_k^E)$

Definition Privacy: $P := \sup(H_{Bob:Alice} - H_{Eve:Alice})$

Es lässt sich zeigen: $P \geq I(\rho, \mathcal{E})$

4.2 Anforderungen an ein sicheres QKD Protokoll

Sicherheitskriterium:

Ein QKD Protokoll heißt sicher, wenn es für jeden Sicherheitsparameter $s > 0$ und $l > 0$ ausgewählt von Alice und Bob und für jede Strategie die Eve anwenden kann, entweder abbricht oder mit einer Wahrscheinlichkeit von mindestens $1 - O(2^{-s})$ zum Erfolg führt und es garantiert, dass Eves gemeinsame Information mit dem erzeugten Schlüssel kleiner als 2^{-l} ist. Außerdem muss der erzeugte Schlüssel zufällig sein.

- Einfluss von Eve messen
- Es soll kein Quantenspeicher und kein perfekter Quantencomputer nötig sein

4.2 Anforderungen an ein sicheres QKD Protokoll

- Lemma 1: Hohe Fidelity impliziert niedrige Entropie

Wenn $F(\rho, |\beta_{00}\rangle^{\otimes n})^2 > 1 - 2^{-s}$, dann gilt

$$S(\rho) < \left(2n + s + \frac{1}{\ln 2} \right) \cdot 2^{-s} + O(2^{-2s})$$

Nach dem Holevo Bound gilt dann:

$$H(XY : Z) \leq S(\rho) < \left(2n + s + \frac{1}{\ln 2} \right) \cdot 2^{-s} + O(2^{-2s})$$

Somit ist gezeigt:

Wenn es ein Verfahren gibt, das Alice und Bob mit hoher Wahrscheinlichkeit mit EPR Paaren mit Fidelity von mindestens $1 - 2^{-s}$ versorgt, so ist es sicher.

4.3 Untere Schranke für Fidelity

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Fidelity überprüfen durch messen von:

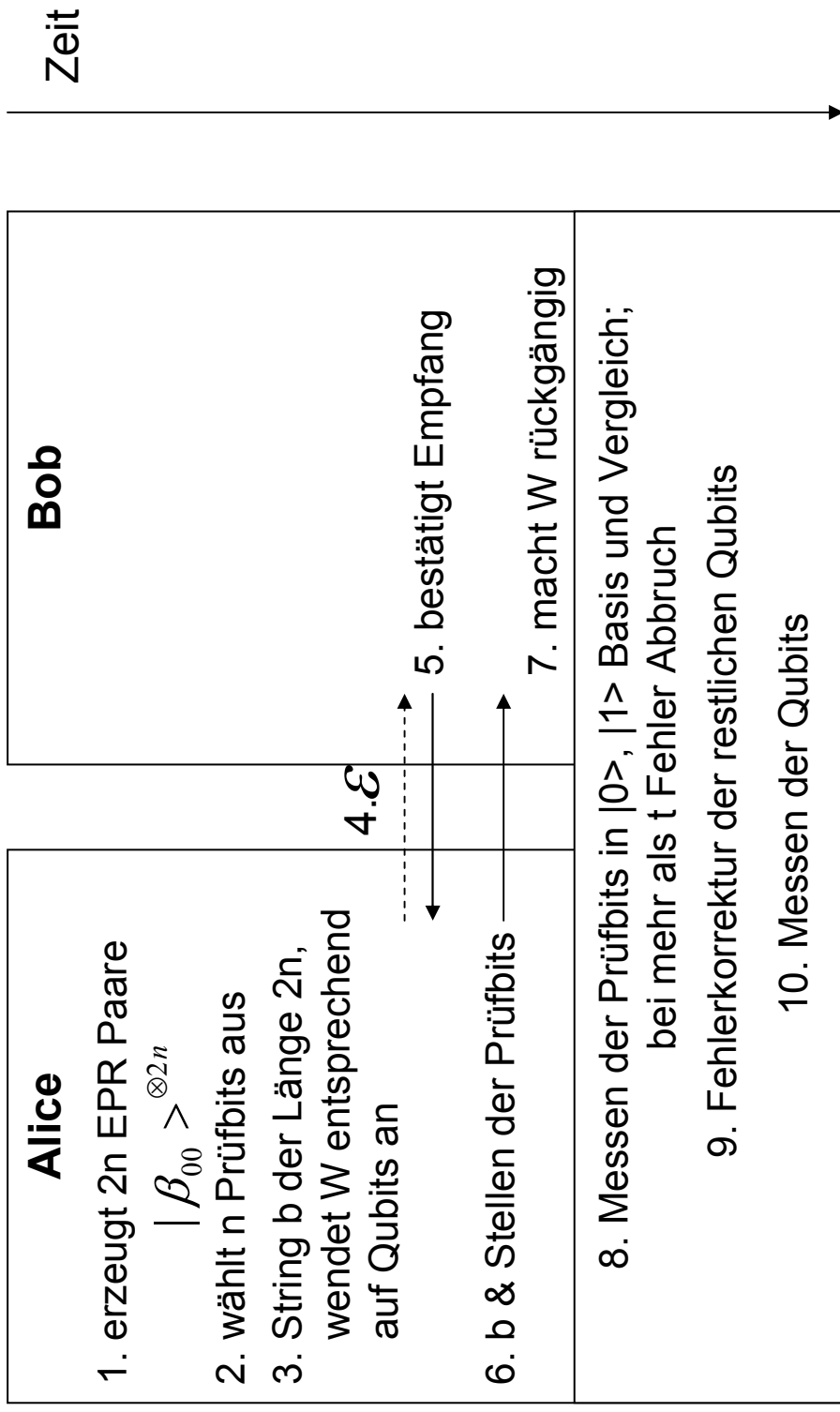
Bitflip: $\Pi_{bf} = |\beta_{01}\rangle\langle\beta_{01}| + |\beta_{11}\rangle\langle\beta_{11}| \quad I - \Pi_{bf}$

Phasenflip: $\Pi_{pf} = |\beta_{10}\rangle\langle\beta_{10}| + |\beta_{11}\rangle\langle\beta_{11}| \quad I - \Pi_{pf}$

Messungen lokal möglich:

$$\Pi_{bf} = (I \otimes I - Z \otimes Z) / 2 \quad \Pi_{pf} = (I \otimes I - X \otimes X) / 2$$

4.4 Das modifizierte Lo-Chau Protokoll



4.5 Das Quantenfehlerkorrektur Protokoll

1. Vereinfachung:

Alice kann direkt am Anfang messen, bzw. erst gar keine EPR Paare erstellen sondern direkt einzelne Qubits, denn

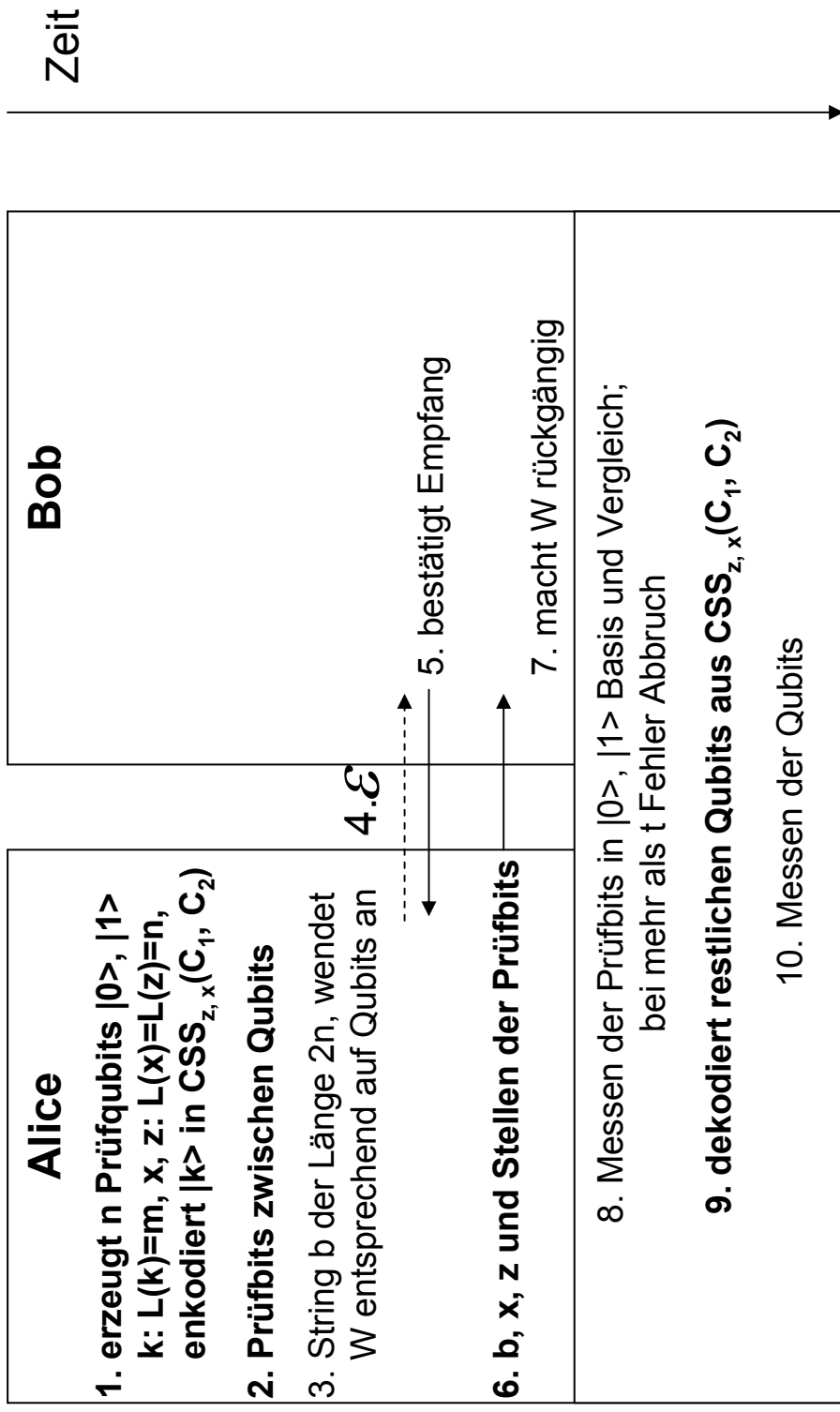
Alices Messungen erzeugen Qubits in einem zufälligen Quantenfehlerkorrekturcode:

$$|v_k + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |v_k + w\rangle$$

$$|\xi_{v_k, z, x}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{z \cdot w} |v_k + w + x\rangle$$

$$|\beta_{00}\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle |j\rangle = \frac{1}{\sqrt{2^n}} \sum_{v_k, z, x} |\xi_{v_k, z, x}\rangle > |\xi_{v_k, z, x}\rangle >$$

4.5 Das Quantenfehlerkorrektur Protokoll / CSS Code Protokoll



4.6 Vereinfachung zu BB84

2. Vereinfachung:

Fehlerkorrektur klassisch berechnen, dadurch fällt der Quantencomputer weg

$$\begin{aligned}
 \rho_{v_k, x} &= \frac{1}{2^n} \sum_z |\xi_{v_k, z, x}\rangle \langle \xi_{v_k, z, x}| \\
 &= \frac{1}{2^n |C_2|} \sum_z \sum_{w_1, w_2 \in C_2} (-1)^{z \cdot (w_1 + w_2)} |v_k + w_1 + x\rangle \langle v_k + w_2 + x| \\
 &= \frac{1}{|C_2|} \sum_{w \in C_2} |v_k + w + x\rangle \langle v_k + w + x|
 \end{aligned}$$

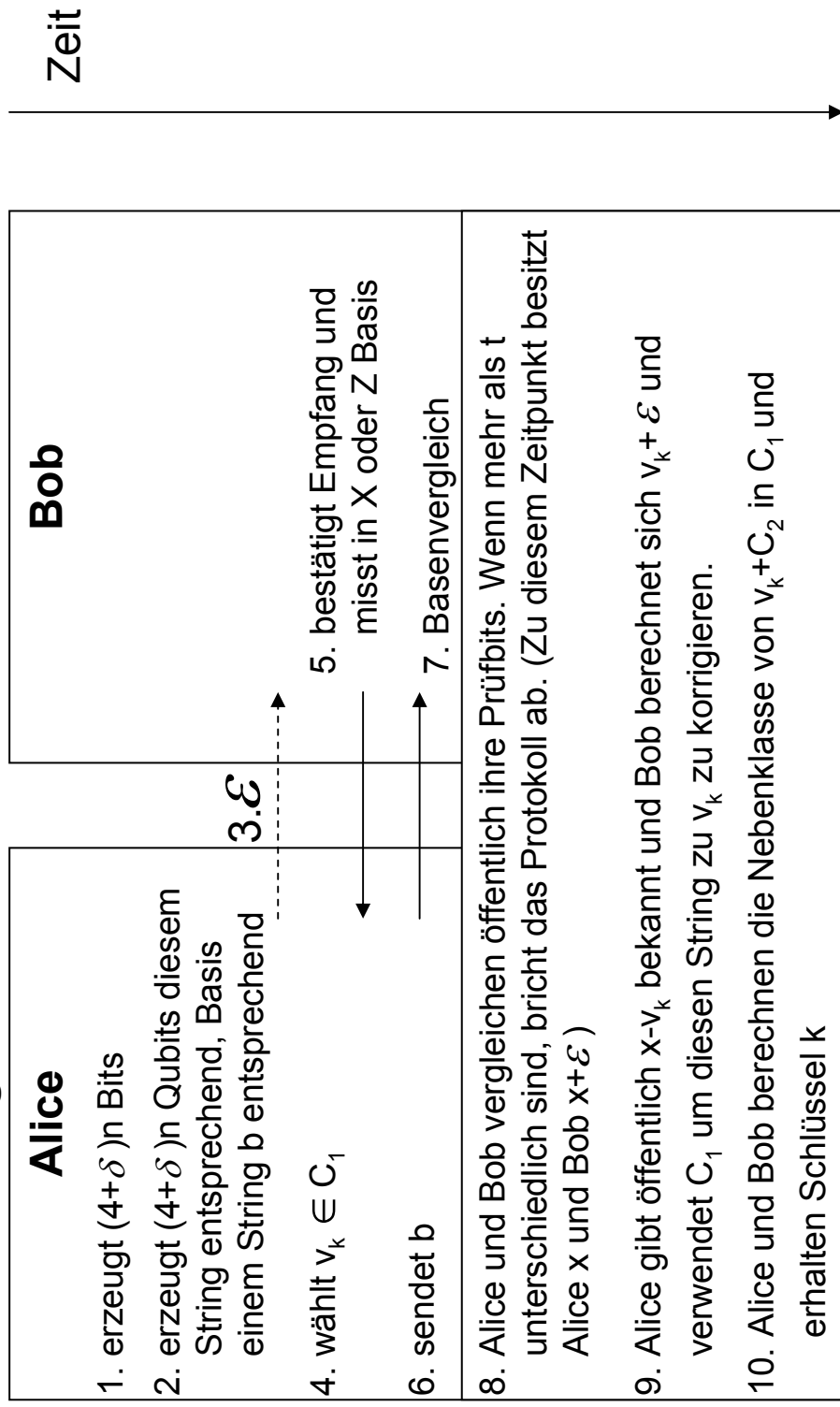
4.6 Vereinfachung zu BB84

3. Vereinfachung:

Messung der Qubits direkt nach der Messung läßt Bob auf den Quantenspeicher verzichten.

Allerdings doppelt so viele Qubits notwendig da Bob mit nur mit Wk 0.5 in der richtigen Basis misst.

4.6 Vereinfachung zu BB84 / Sicheres BB84



4.7 Qubits doch kopierbar?

23. Mai 2002: Antia Lamas-Linares,
Christoph Simon, John C. Howell
und Dik Bouwmeester:

Experimental Quantum Cloning of Single Photons

Kopieren von Qubits mit $Wk < 1/6$.

Jedoch unkritisch für Quantenkryptographie, solange $Wk < 1$,
denn dann gilt:

$$H(XY : Z) = H(XY) + H(Z) - H(XY, Z) \leq H(XY)$$

Privacy Amplification kann gemeinsame Information Eves
noch minimieren

5 Experimentelle Durchführung von Quantenkryptographie

