Quantenkryptographie

Kryptographie

- **Ziele:**
  - **Vertraulichkeit**
  - **Integrität**
  - **Authenzität**
- **symmetrische und asymmetrische Verfahren**

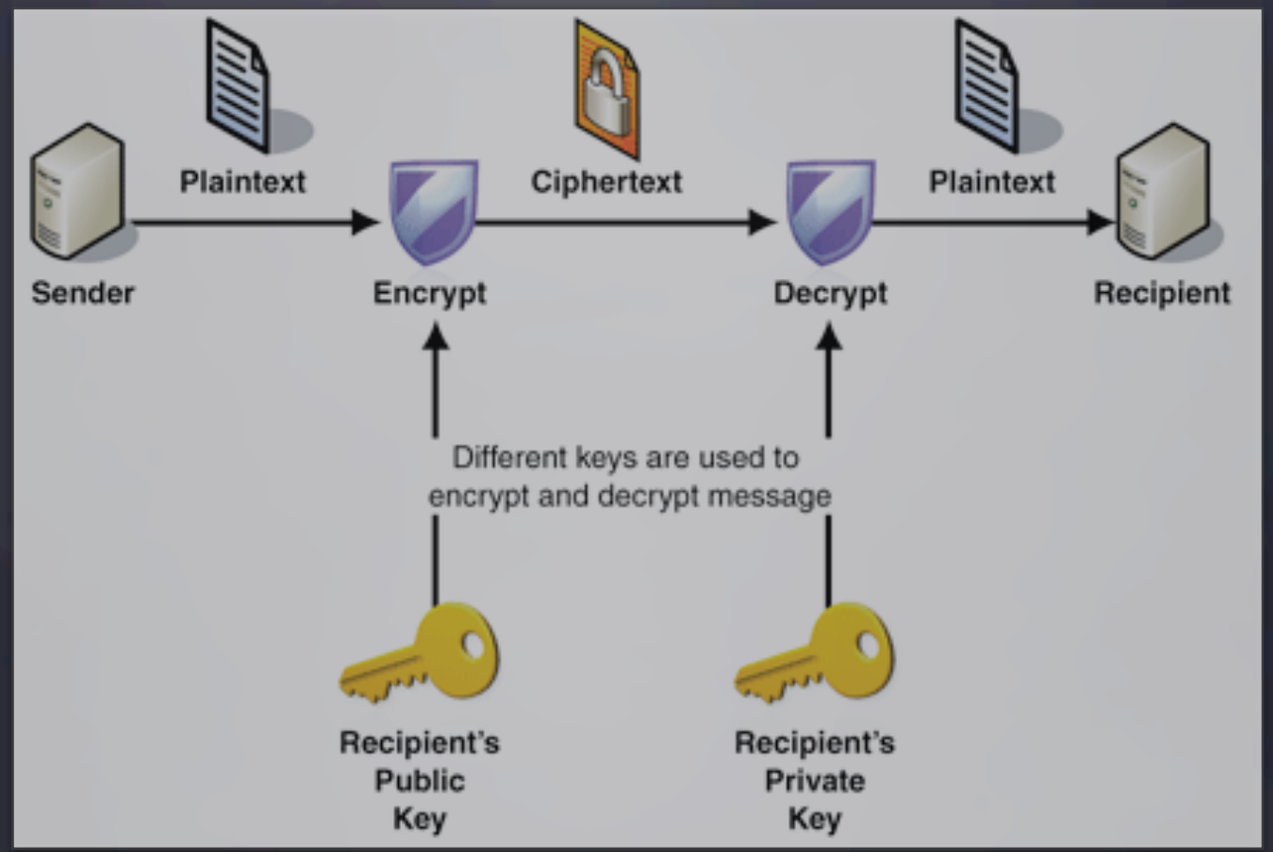
One-Time-Pad Verfahren

- **zufälliger Schlüssel**
- **Schüssellänge** entspricht Zeichenanzahl
- einmal verwendbar

	23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	Key
+	7 (H)	4 (E)	11 (L)	11 (L)	4 (O)	Message
=	30	16	13	21	15	Message + Key
=	4 (E)	16 (Q)	13 (N)	21 (V)	15 (Z)	Cypher (mod 26)
	4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	Cypher
−	23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	Key
=	-19	4	11	11	14	Cypher − Key
=	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	Message (mod 26)

Public Key Verfahren

- öffentlicher Schlüssel für Verschlüsselung
- privater Schlüssel für Entschlüsselung
- Öffentlicher wird aus Privatem generiert
  - “One-Way” Funktion



Quantenkryptographie

- **grundsätzliche Folgerungen der Quantentheorie:**

  1) Messungen beeinflussen das System.

  2) Die Polarisation eines Photons kann nicht in verschiedenen Basen gleichzeitig gemessen werden.

  3) Ein unbekannter Quantenzustand kann nicht kopiert werden. (No-Cloning Theorem)

$$U(|\psi\rangle|\varphi\rangle) = |\psi\rangle|\psi\rangle$$

$$U[(|\psi_1\rangle + |\psi_2\rangle)|\varphi\rangle] = U(|\psi_1\rangle|\varphi\rangle) + U(|\psi_2\rangle|\varphi\rangle) = (|\psi_1\rangle + |\psi_2\rangle)(|\psi_1\rangle + |\psi_2\rangle)$$

$$|\psi_1\rangle|\psi_1\rangle) + |\psi_2\rangle|\psi_2\rangle \neq |\psi_1\rangle|\psi_1\rangle + 2|\psi_1\rangle|\psi_2\rangle + |\psi_2\rangle|\psi_2\rangle$$

BB84-Protokoll

- benötigt mind. 2-Zustands Quantensystem, hier: Polarisation von Photonen
- 2 Basen mit jeweils 2 Zuständen:
  - horizontal und vertikal in einer Basis sowie
  - rechts und links in einer zur ersten verdrehten Basis
- vertikal und rechts ≙ Bitwert 1
- horizontal und links ≙ Bitwert 0
- Prinzip:
  - Alice präpariert zufällig einen Zustand
  - Bob misst in einer zufällig gewählten Basis
  - Vergleich der verwendeten Basen
    - aus Messungen in gleichen Basen wird Schlüssel erzeugt
    - andere Messungen werden verworfen

Alice										
Basis	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
Zustand	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|H\rangle$	$\|L\rangle$	$\|L\rangle$	$\|R\rangle$	$\|L\rangle$	$\|H\rangle$	$\|V\rangle$
Bitwert	0	1	1	0	0	0	1	0	0	1
Bob										
Basis	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$
Zustand	$\|R\rangle$	$\|R\rangle$	$\|L\rangle$	$\|R\rangle$	$\|H\rangle$	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|H\rangle$	$\|L\rangle$
Bitwert	1	1	0	1	0	0	1	0	0	1
Key										
Bitwert		1		0		0		0		1
Alice		1		**0**		0		**0**		1
Bob		1		**1**		0		**1**		1

Ekert-Protokoll

- basiert auf Verschränkung
  - die Quelle erzeugt ein Paar verschränkter Teilchen (zufällige Basis)
  - Alice und Bob erhalten je ein Teilchen und messen in zuffällig gewählten Basen
  - A und B verwenden nur Messungen in selber Basis für den Schlüssel

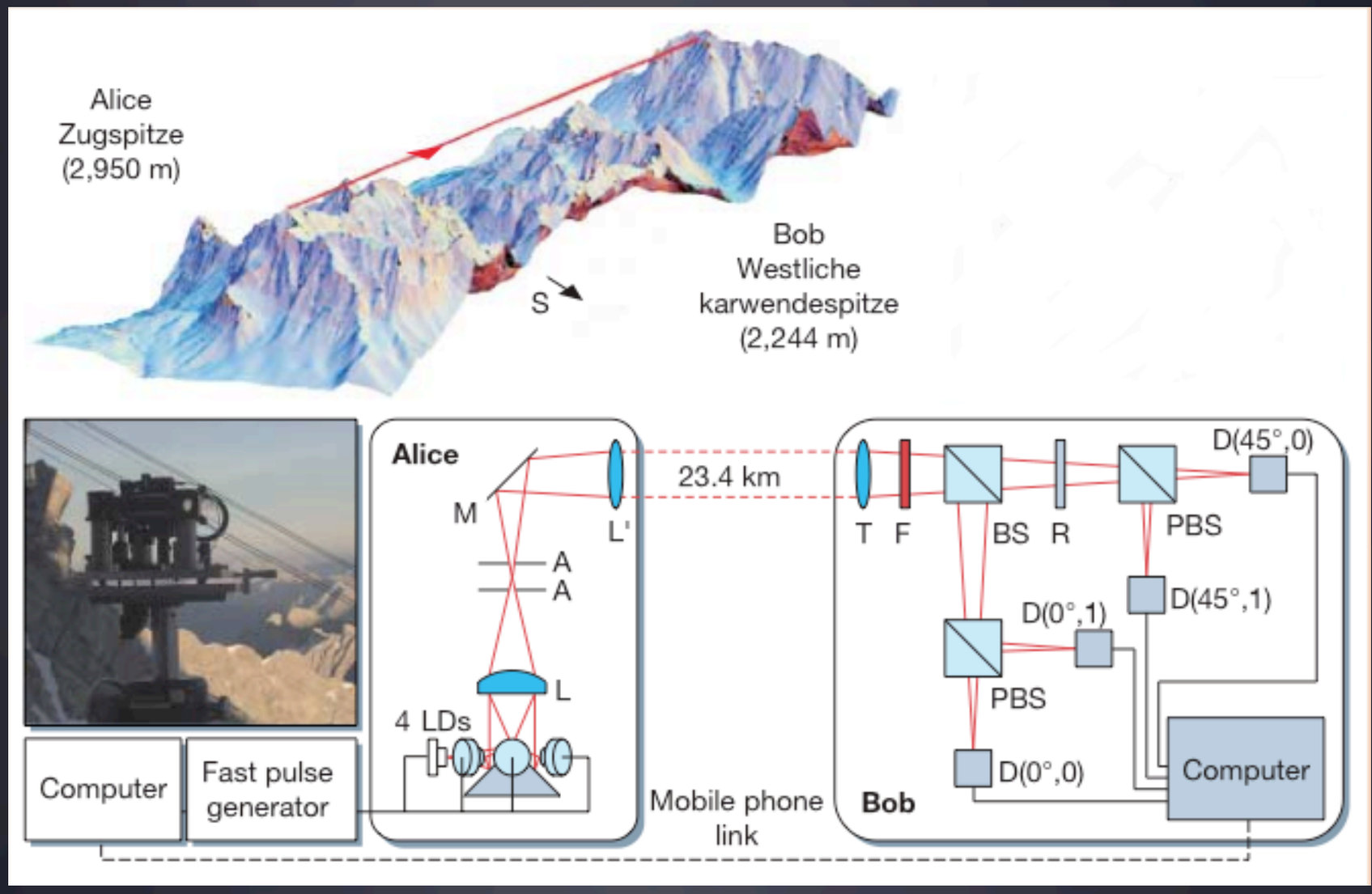
- das Prinzip anderer Protokolle ist gleich

Technische Umsetzung

- Erzeugung von Photonen
  - Photon-Guns
  - schwache Laserpulse
    - Problem: Wahrscheinlichkeit für Emission von Photonen unterliegt einer Poisson-Verteilung --> niedrige Bitrate
- Übermittelung
  - Kabel
    - exponentieller Verlust mit größerer Distanz
    - Wellenlänge ≈1300nm, Distanz ≈67km
  - free space
    - abhängig von äußeren Bedingungen
    - Wellenlänge ≈800nm, Distanz ≈23km
    - Satelliten-Kommunikation möglich

- Detektion
  - Ansprüche:
    - hohe Effizienz für ein breites Spektrum
    - Verzögerung zwischen eingehendem Photon und ausgehendem Signal möglichst kurz
    - schnelle Detektionsrate (“recovery time”)
  - verwendet werden Photodioden (APD)

Beispiel: free space



Phasenmodulation