



Quantenkryptographie

Goluch Gernot
Riedl Bernhard

Agenda

- Die Theorie
- Die Verschlüsselung
- Die Entschlüsselung
- Die Schlüsselverteilung
- Angriffsmöglichkeiten
- Praxisbeispiel

Schrödinger's Katze



Abb.1: Schrödingers Katze
(Münchner Internetprojekt zur Lehrerfortbildung in Quantenmechanik)

Das Photon und die Polarisation

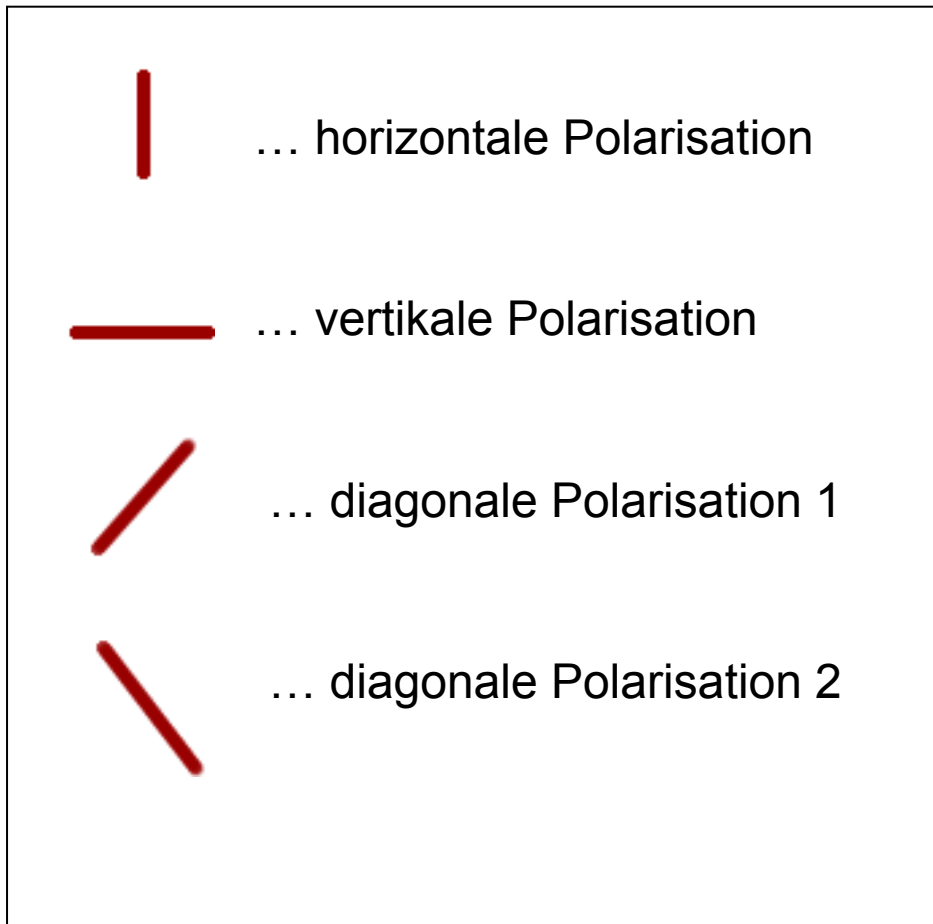


Abb.2: Die Polarisation
(eigene Darstellung)

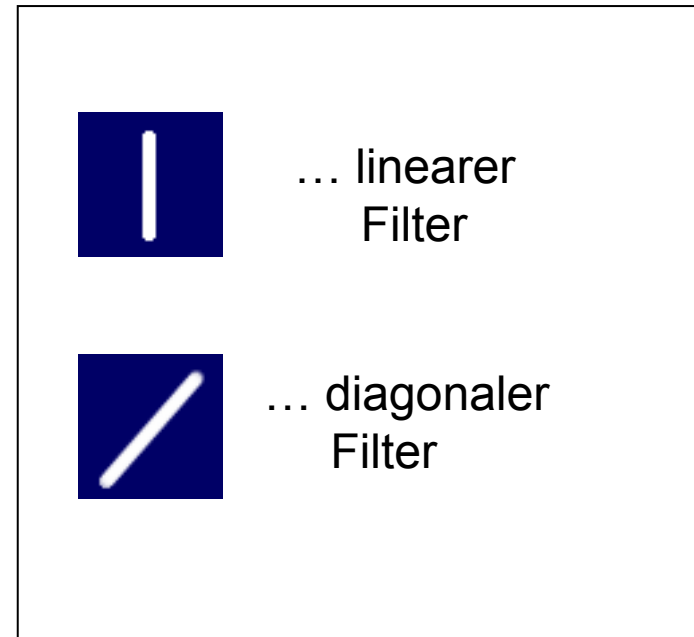


Abb.3: Der Filter
(eigene Darstellung)

Messung

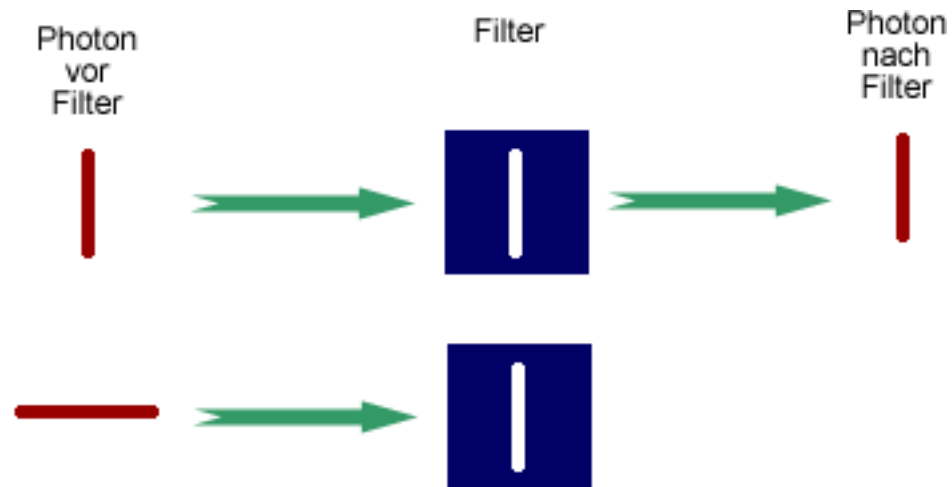


Abb.4: Die Messung
(eigene Darstellung)

Superposition

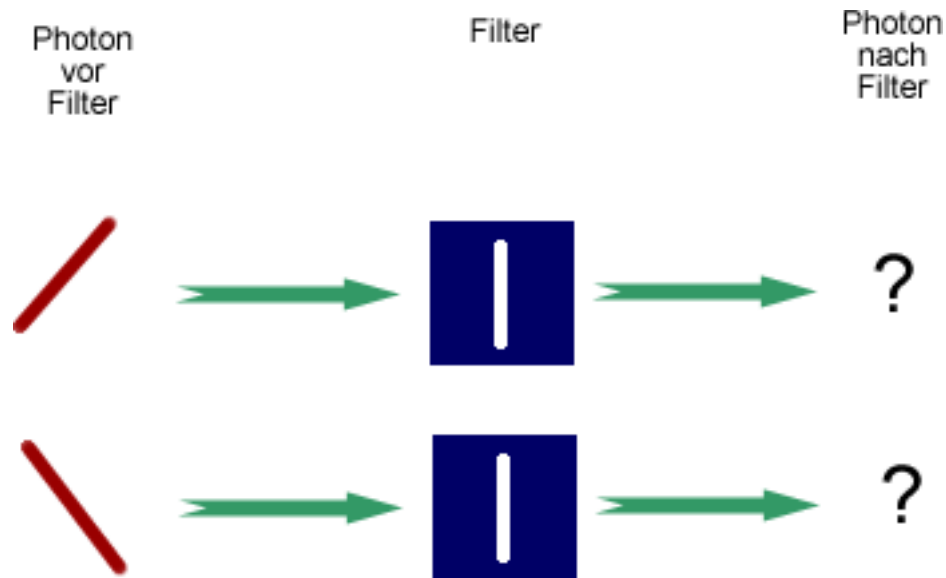


Abb.5: Die Superposition
(eigene Darstellung)

Die Verschlüsselung

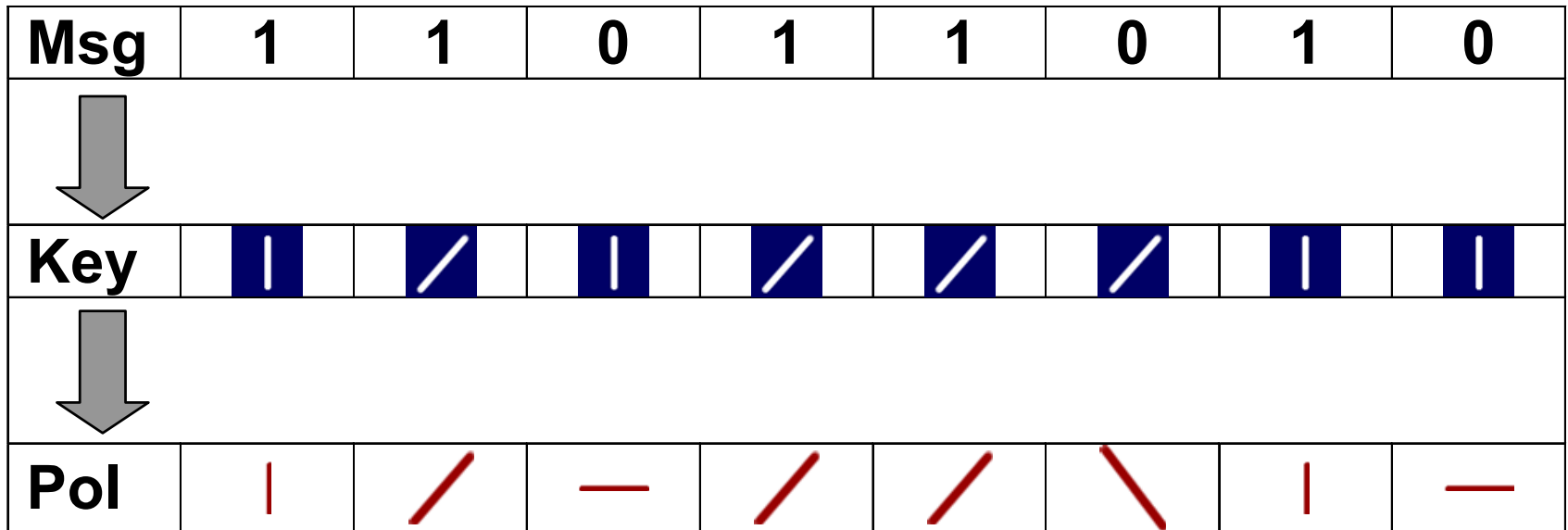


Abb.6: Die Verschlüsselung
(eigene Darstellung)

Die Entschlüsselung

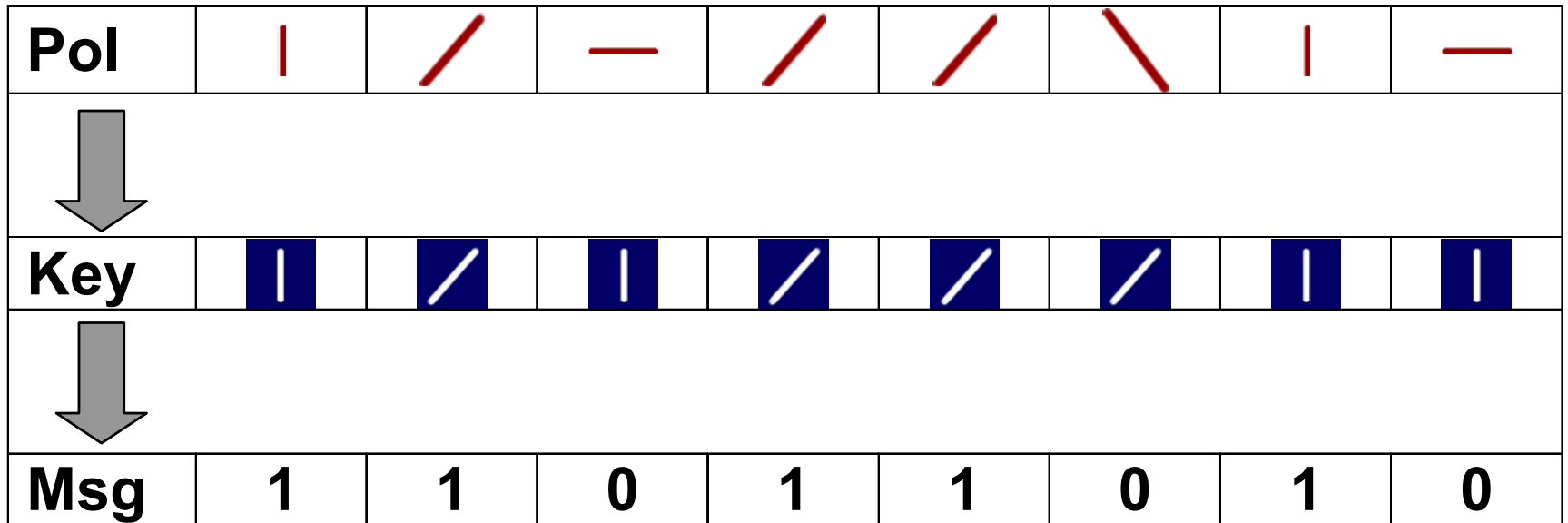


Abb.7: Die Entschlüsselung
(eigene Darstellung)

Kryptoanalyse

Pol		/	—	/	/	\		—
↓								
Key	/	/				/	/	/
↓								
Msg	?	1	0	?	?	0	?	?

Abb.8: Kryptoanalyse
(eigene Darstellung)

Die Schlüsselverteilung (1/3)

Msg	1	0	0	1	1	0	1	0
	↓							
Key			/	/	/		/	
	↓							
Pol		—	\	/	/	—	/	—

Abb.9: Die Schlüsselverteilung Alice
(eigene Darstellung)

Die Schlüsselverteilung (2/3)

Pol		—	↘	↗	↗	—	↗	—
	↓							
Key	↗	↗		↗	↗			
	↓							
Msg	?	?	?	1	1	0	?	0

Abb.10: Die Schlüsselverteilung Bob
(eigene Darstellung)

Die Schlüsselverteilung (3/3)

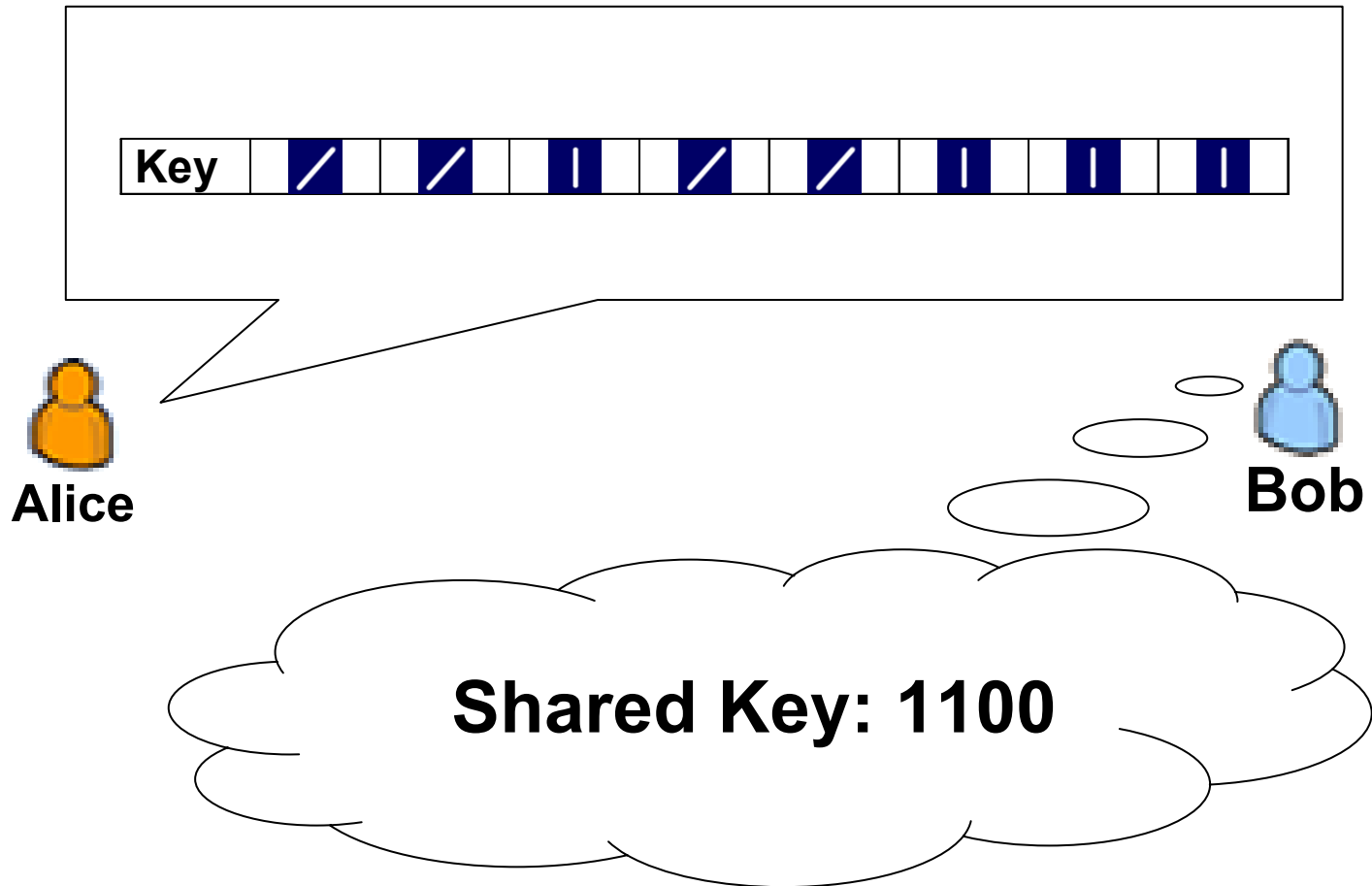


Abb.11: Die Schlüsselverteilung Alice - Bob (eigene Darstellung)

Eve und die Schlüsselverteilung

- Eve kann die Rolle von Bob annehmen
- Eve kann den Schlüssel von Alice mithören
- Eve fängt mit dieser Information nichts an

! Problem: Denial of Service Attacken !

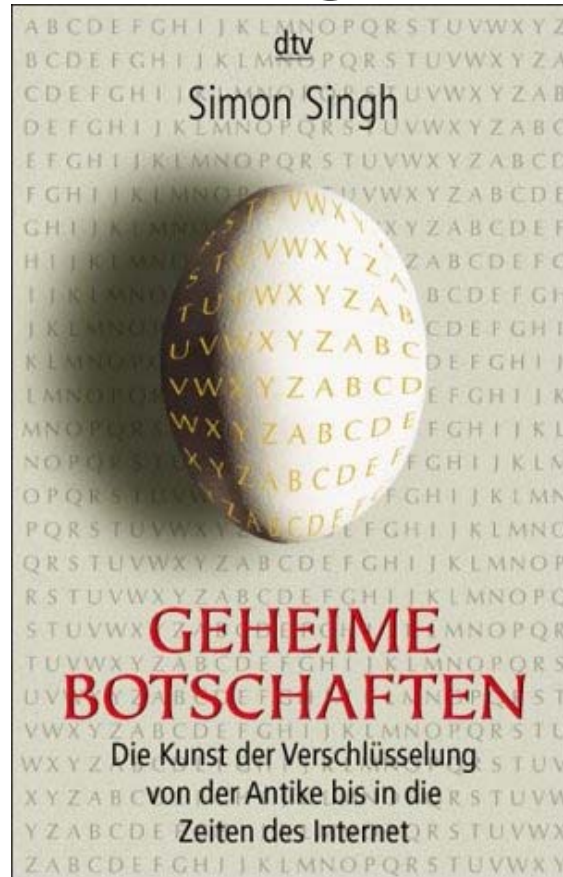
Von der Theorie zur Praxis



Abb.12: Praxisbeispiel

(Wolfgang Tittel, Jürgen Brendel, Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden)

Buchempfehlung



Erscheinungsdatum: Dezember 2001
ISBN: 3423330716