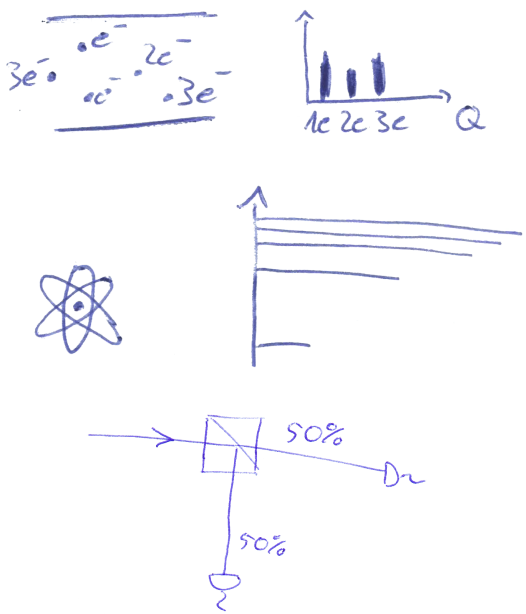
Zufall in der Quantenkryptographie

Nico Klein,
qutools GmbH, München

23. November 2017

Phänomene der Quantenwelt

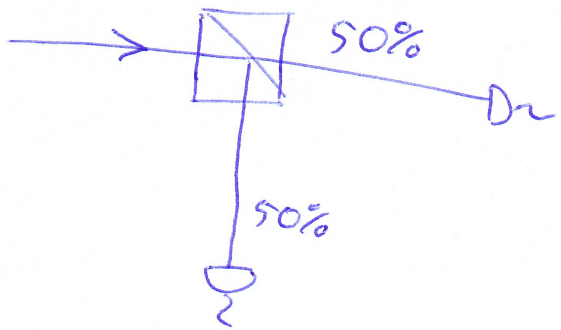
- Quantisierung
- Zufall



vgl. auch Küblbeck, J., Müller, R., *Die Wesenszüge der Quantenphysik*, 2002

Phänomene der Quantenwelt

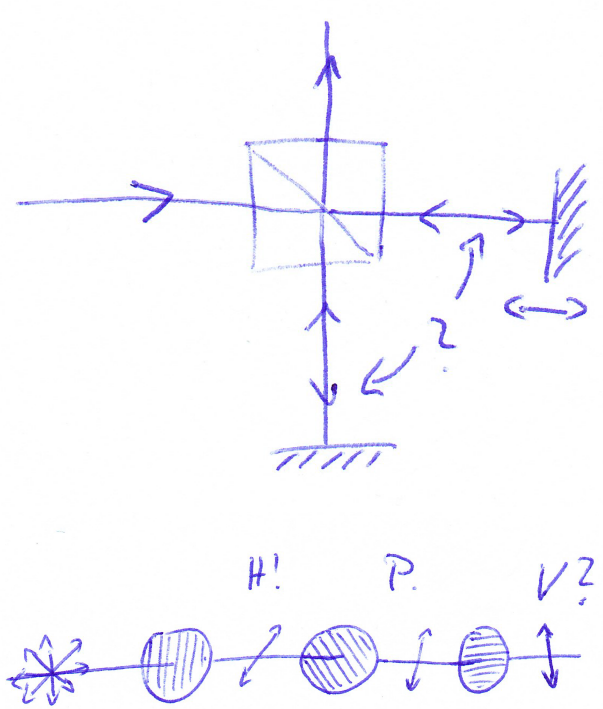
- Quantisierung
- Zufall
- Unbestimmtheit



vgl. auch Küblbeck, J., Müller, R., *Die Wesenszüge der Quantenphysik*, 2002

Phänomene der Quantenwelt

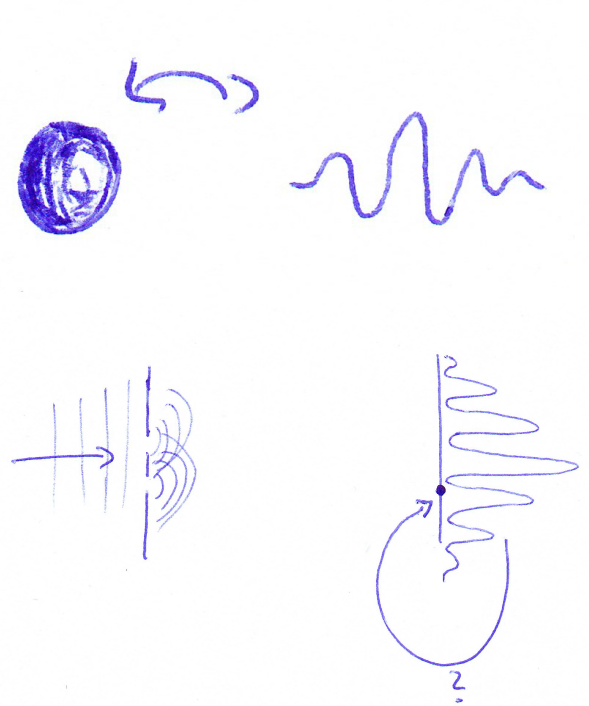
- Quantisierung
- Zufall
- Unbestimmtheit
- Welle-Teilchen Dualismus



vgl. auch Küblbeck, J., Müller, R., *Die Wesenszüge der Quantenphysik*, 2002

Phänomene der Quantenwelt

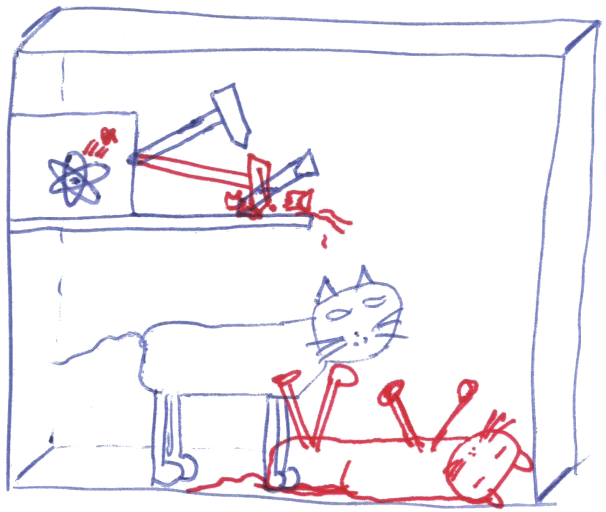
- Quantisierung
- Zufall
- Unbestimmtheit
- Welle-Teilchen Dualismus
- (De-)Kohärenz/Messproblem



vgl. auch Küblbeck, J., Müller, R., *Die Wesenszüge der Quantenphysik*, 2002

Phänomene der Quantenwelt

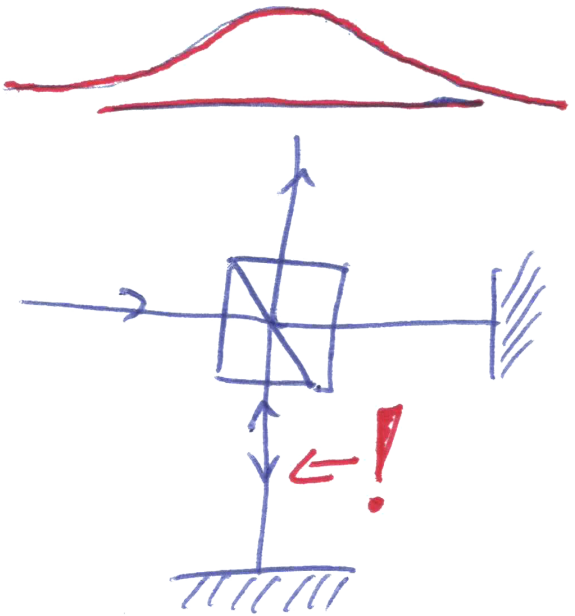
- Quantisierung
- Zufall
- Unbestimmtheit
- Welle-Teilchen Dualismus
- (De-)Kohärenz/Messproblem
- Welcher-Weg-Information



vgl. auch Küblbeck, J., Müller, R., *Die Wesenszüge der Quantenphysik*, 2002

Phänomene der Quantenwelt

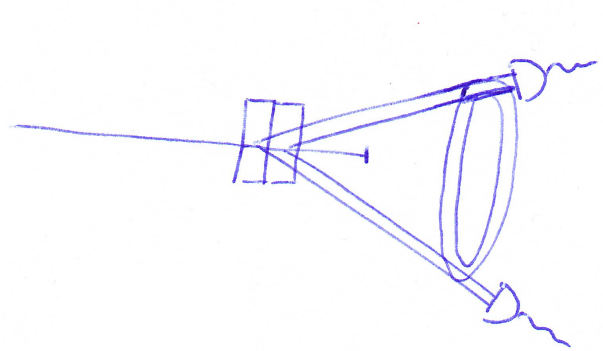
- Quantisierung
- Zufall
- Unbestimmtheit
- Welle-Teilchen Dualismus
- (De-)Kohärenz/Messproblem
- Welcher-Weg-Information
- Verschränkung



vgl. auch Küblbeck, J., Müller, R., *Die Wesenszüge der Quantenphysik*, 2002

Phänomene der Quantenwelt

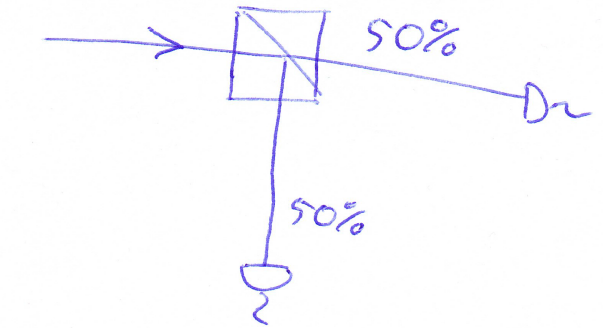
- Quantisierung
- Zufall
- Unbestimmtheit
- Welle-Teilchen Dualismus
- (De-)Kohärenz/Messproblem
- Welcher-Weg-Information
- Verschränkung



vgl. auch Küblbeck, J., Müller, R., *Die Wesenszüge der Quantenphysik*, 2002

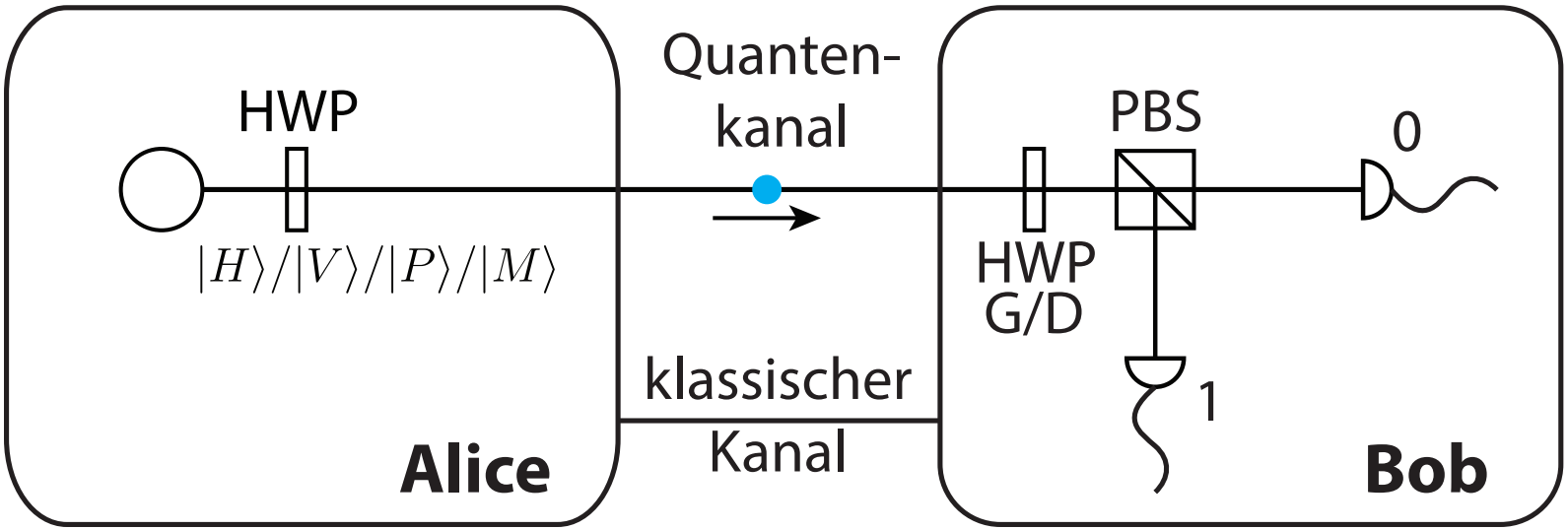
Phänomene der Quantenwelt

- Quantisierung
- **Zufall**
- **Unbestimmtheit**
- Welle-Teilchen Dualismus
- (De-)Kohärenz/Messproblem
- Welcher-Weg-Information
- Verschränkung



vgl. auch Küblbeck, J., Müller, R., *Die Wesenszüge der Quantenphysik*, 2002

Das BB84-Protokoll



Das BB84-Protokoll

Quantenkanal:													
Alices zufällige Bitfolge	0	1	1	0	1	0	0	0	1	0	1	0	1
Alices zufällige Basiswahl	⊗	⊗	⊕	⊕	⊕	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊕

Das BB84-Protokoll

Quantenkanal:													
Alices zufällige Bitfolge	0	1	1	0	1	0	0	0	1	0	1	0	1
Alices zufällige Basiswahl	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
gesendete Photonen $\|\cdot\rangle$	P	M	V	H	V	H	H	P	V	P	M	H	V

Das BB84-Protokoll

Quantenkanal:													
Alices zufällige Bitfolge	0	1	1	0	1	0	0	0	1	0	1	0	1
Alices zufällige Basiswahl	⊗	⊗	⊕	⊕	⊕	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊕
gesendete Photonen $\|\cdot\rangle$	P	M	V	H	V	H	H	P	V	P	M	H	V
Bobs zufällige Basiswahl	⊕	⊗	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊕	⊕

Das BB84-Protokoll

Quantenkanal:													
Alices zufällige Bitfolge	0	1	1	0	1	0	0	0	1	0	1	0	1
Alices zufällige Basiswahl	⊗	⊗	⊕	⊕	⊕	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊕
gesendete Photonen $\|\cdot\rangle$	P	M	V	H	V	H	H	P	V	P	M	H	V
Bobs zufällige Basiswahl	⊕	⊗	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊕	⊕
empfangene Bits	1	1	1		1	0	1	0	0	0		0	1

Das BB84-Protokoll

Quantenkanal:													
Alices zufällige Bitfolge	0	1	1	0	1	0	0	0	1	0	1	0	1
Alices zufällige Basiswahl	⊗	⊗	⊕	⊕	⊕	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊕
gesendete Photonen $\|\cdot\rangle$	P	M	V	H	V	H	H	P	V	P	M	H	V
Bobs zufällige Basiswahl	⊕	⊗	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊕	⊕
empfangene Bits	1	1	1		1	0	1	0	0	0		0	1
klassischer Kanal:													
Bob sendet Basen	⊕	⊗	⊗		⊗	⊕	⊗	⊕	⊗	⊗		⊕	⊕

Das BB84-Protokoll

Quantenkanal:													
Alices zufällige Bitfolge	0	1	1	0	1	0	0	0	1	0	1	0	1
Alices zufällige Basiswahl	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
gesendete Photonen $\lvert\cdot\rangle$	P	M	V	H	V	H	H	P	V	P	M	H	V
Bobs zufällige Basiswahl	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
empfangene Bits	1	1	1		1	0	1	0	0	0		0	1
klassischer Kanal:													
Bob sendet Basen	$\oplus$	$\otimes$	$\otimes$		$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$		$\oplus$	$\oplus$
Alice bestätigt		✓				✓				✓		✓	✓

Das BB84-Protokoll

Quantenkanal:													
Alices zufällige Bitfolge	0	1	1	0	1	0	0	0	1	0	1	0	1
Alices zufällige Basiswahl	⊗	⊗	⊕	⊕	⊕	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊕
gesendete Photonen $\|\cdot\rangle$	P	M	V	H	V	H	H	P	V	P	M	H	V
Bobs zufällige Basiswahl	⊕	⊗	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊕	⊕
empfangene Bits	1	1	1		1	0	1	0	0	0		0	1
klassischer Kanal:													
Bob sendet Basen	⊕	⊗	⊗		⊗	⊕	⊗	⊕	⊗	⊗		⊕	⊕
Alice bestätigt		✓				✓				✓		✓	✓
vermutlich geteilte Bits		1				0				0		0	1

Das BB84-Protokoll

Quantenkanal:													
Alices zufällige Bitfolge	0	1	1	0	1	0	0	0	1	0	1	0	1
Alices zufällige Basiswahl	⊗	⊗	⊕	⊕	⊕	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊕
gesendete Photonen $\|\cdot\rangle$	P	M	V	H	V	H	H	P	V	P	M	H	V
Bobs zufällige Basiswahl	⊕	⊗	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊕	⊕
empfangene Bits	1	1	1		1	0	1	0	0	0		0	1
klassischer Kanal:													
Bob sendet Basen	⊕	⊗	⊗		⊗	⊕	⊗	⊕	⊗	⊗		⊕	⊕
Alice bestätigt		✓				✓				✓		✓	✓
vermutlich geteilte Bits		1				0				0		0	1
Lauscherentdeckung:													
Bob teilt zufällig		1								0			
Alice bestätigt		✓								✓			

Das BB84-Protokoll

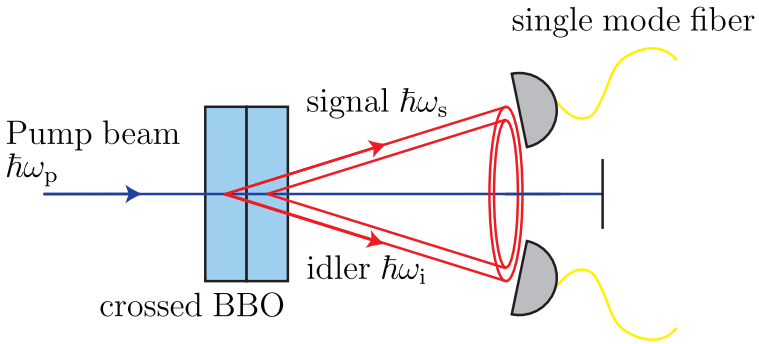
Quantenkanal:													
Alices zufällige Bitfolge	0	1	1	0	1	0	0	0	1	0	1	0	1
Alices zufällige Basiswahl	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
gesendete Photonen $\lvert\cdot\rangle$	P	M	V	H	V	H	H	P	V	P	M	H	V
Bobs zufällige Basiswahl	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
empfangene Bits	1	1	1		1	0	1	0	0	0		0	1
klassischer Kanal:													
Bob sendet Basen	$\oplus$	$\otimes$	$\otimes$		$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$		$\oplus$	$\oplus$
Alice bestätigt		✓				✓				✓		✓	✓
vermutlich geteilte Bits		1				0				0		0	1
Lauscherentdeckung:													
Bob teilt zufällig		1								0			
Alice bestätigt		✓								✓			
Restschlüssel						0						0	1

Das BB84-Protokoll

Quantenkanal:													
Alices zufällige Bitfolge	0	1	1	0	1	0	0	0	1	0	1	0	1
Alices zufällige Basiswahl	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
gesendete Photonen $\lvert\cdot\rangle$	P	M	V	H	V	H	H	P	V	P	M	H	V
Bobs zufällige Basiswahl	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
empfangene Bits	1	1	1		1	0	1	0	0	0		0	1
klassischer Kanal:													
Bob sendet Basen	$\oplus$	$\otimes$	$\otimes$		$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$		$\oplus$	$\oplus$
Alice bestätigt		✓				✓				✓		✓	✓
vermutlich geteilte Bits		1				0				0		0	1
Lauscherentdeckung:													
Bob teilt zufällig		1								0			
Alice bestätigt		✓								✓			
Restschlüssel						0						0	1

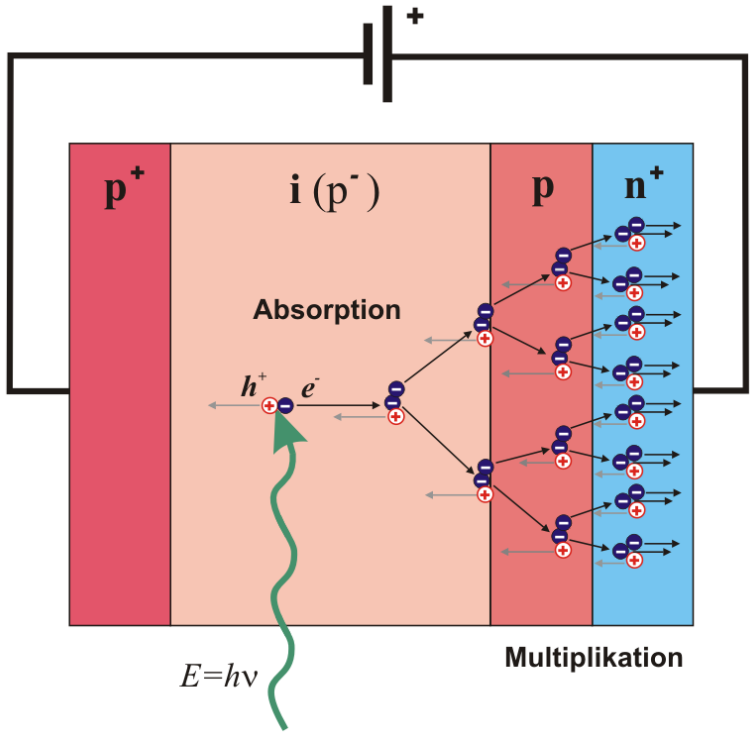
Hardware: Experimentierkits

- Erzeugung einzelner Photonenpaare über SPDC
- Detektion einzelner Photonen in APDs



Hardware: Experimentierkits

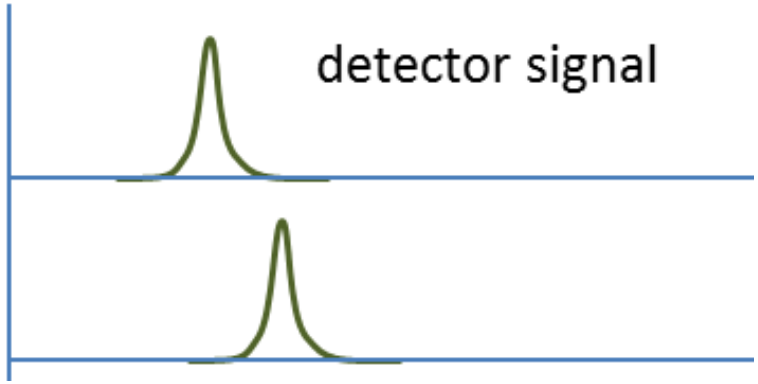
- Erzeugung einzelner Photonenpaare über SPDC
- Detektion einzelner Photonen in APDs
- Zeitauflösung bis zu ~20 ps per FPGA



Aus https://de.wikipedia.org/wiki/Avalanche-Photodiode, November 2017, Kirnehkrib

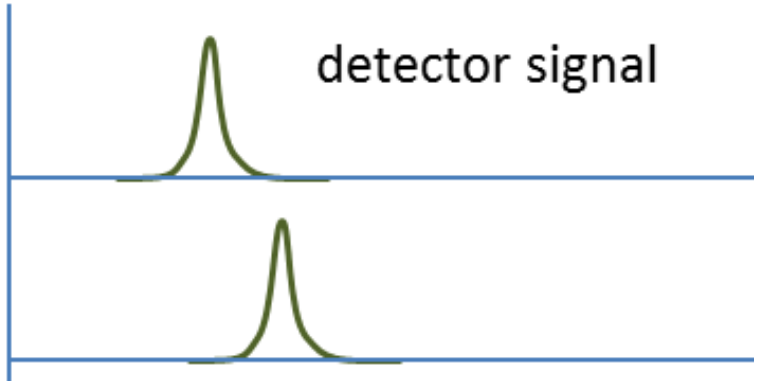
Hardware: Experimentierkits

- Erzeugung einzelner Photonenpaare über SPDC
- Detektion einzelner Photonen in APDs
- Zeitauflösung bis zu ~20 ps per FPGA
- Intuitive Software und umfangreiches Manual



Hardware: Experimentierkits

- Erzeugung einzelner Photonenpaare über SPDC
- Detektion einzelner Photonen in APDs
- Zeitauflösung bis zu ~20 ps per FPGA
- Intuitive Software und umfangreiches Manual



Der quED – quantum Entanglement Demonstrator

"Transparenz."

Der Quantenkoffer

"Usability."