Kryptographie im Zeitalter des Quantencomputers

Fraunhofer Institut
Sichere Telekooperation

Kryptographie im Zeitalter des Quantencomputers

Dr. Andreas U. Schmidt

Fraunhofer SIT

AG Marktplatz Internet (MINT)

CAST Workshop

„Wie sicher ist Kryptographie?“

21. August 2003

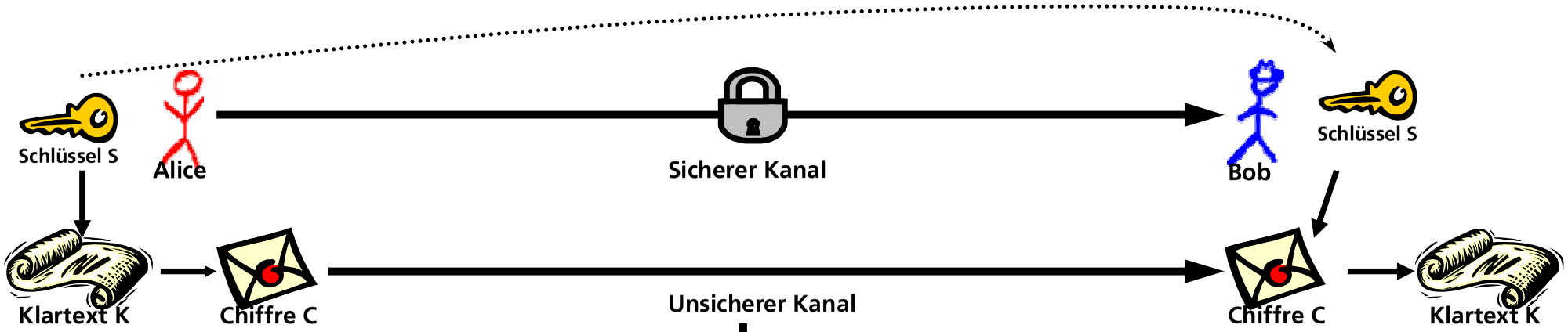
Von der klassischen zur Quantenkryptographie

- Fallstricke klassischer Kryptographie
- Asymmetrische Kryptographie
- Bedrohen Quantencomputer asymmetrische Kryptographie?
- Information in der Quantentheorie: Youngs Experiment
- Das Protokoll BB84
- Sicherheit in der Quantenkryptographie
- Grenzen der QK: Das Bit-commitment Problem
- Weitere Quantenkryptographische Verfahren
- Real existierende Implementierungen
- Forschungsaktivitäten: EU, USA, Welt

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Klassische (symmetrische) Kryptographie und ihr Grundproblem



Chiffre: Z.B. Vernam-C. oder one-time pad. (Vernam 1917 &Shannon 1948)

K	1000111011101
S	0100101100101
C=K XOR S	1100010111000
K=C XOR S	1000111011101

- **Informational perfekte Sicherheit H(K|C)=H(K)**
- **Schlüssel ist Zufallsstring, gleichlang wie K**

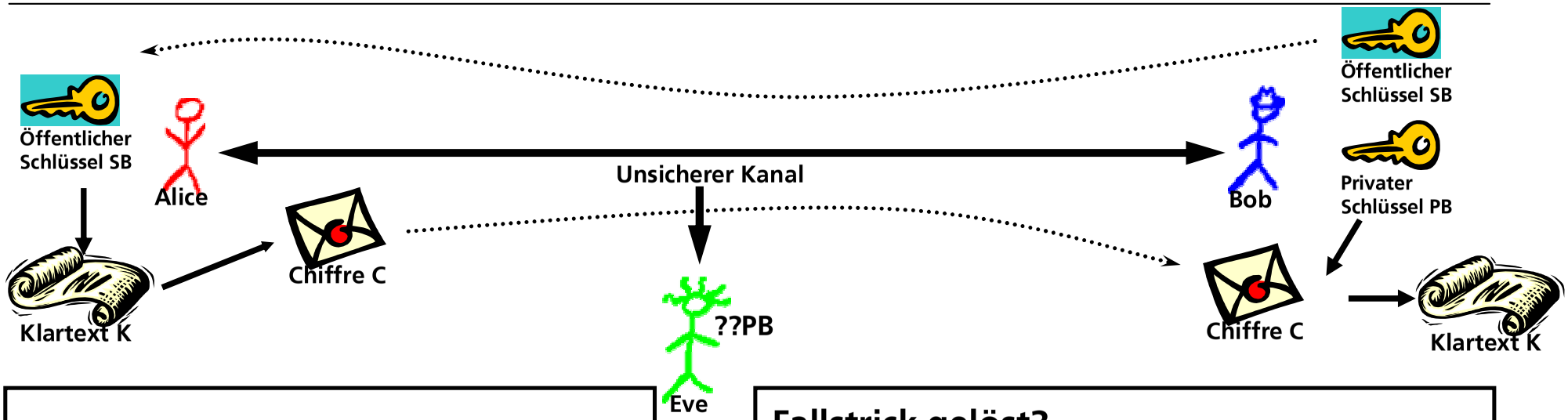
Fallstrick Key Distribution Problem:

- Sicherer Kanal wird vorausgesetzt
- Authentifizierung des Partners nicht gegeben – Man-in-the-middle Angriff auf sicheren Kanal stets möglich
- Intrusion detection nicht gegeben – Eavesdropping wird nicht bemerkt

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Asymmetrische Kryptographie



Chiffren benutzen trap-door functions, z.B. diskrete Logarithmen, Primfaktorzerlegung (RSA 1976):

C=SB(K); K=PB(C)

Selbst, wenn der Algorithmus bekannt ist, ist die Inversion PB=PB(SB) praktisch undurchführbar

Fallstrick gelöst?

- Sicherer Kanal nicht mehr nötig
- Authentifizierung möglich durch digitale Signaturen – aber: PKIs und CAs nötig
- Intrusion detection nicht gegeben – Eavesdropping wird nicht bemerkt
- Grundannahmen der Komplexität (P≠NP) unbewiesen

SIT
Fraunhofer Institut Sichere Telekooperation

Competence Center For Applied Security Technology
CAST

Bedrohung asymmetrischer Kryptographie:

Primfaktorisierung durch Quantencomputing

Die asymptotische Laufzeit des besten bekannten *klassischen* Algorithmus (Lenstra 1990/93) zur Faktorisierung einer Zahl n mit ca. $\log n$ Bits wächst exponentiell:

$$\exp\left(c(\log n)^{1/3}(\log\log n)^{2/3}\right)$$

Shors Quantenalgorithmus (1994) ist dagegen von polynomialer Laufzeit, asymptotisch:

$$(\log n)^2(\log\log n)(\log\log\log n)$$

Grund: Das Superpositionsprinzip ermöglicht es, einen QC mit allen möglichen Registerwerten gleichzeitig Ablaufen zu lassen, z.B.

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

Diese **massive Parallelität** befähigt QC insbesondere zu schneller **Fouriertransformation** die die Grundlage des Faktorisierungsalgorithmus ist.

SIT
Fraunhofer Institut
Sichere Telekooperation

Competence Center For
Applied Security Technology
CAST

Ist die Bedrohung durch Quantencomputer realistisch?

In der Theorie ja, denn entsprechende Quantenalgorithmen existieren:

- Shors Faktorisierungsalgorithmus (94) bedroht RSA, diskrete Logarithmen, elliptische Kurven, etc.; Grovers Suchalgorithmus (1996) bedroht DES

QC sind jedoch noch weit von der Praxis entfernt aufgrund fundamentaler Probleme:

- **Dekohärenz** begrenzt die Dauerhaftigkeit von Quantenspeichern und die Reichweite von Kommunikation
- **Separation von qubits** wird nötig, um unerqünschte Verschränkung zu vermeiden
- **Verarbeitung von qubits** führt zu Fehlern, die sich akkumulieren.

Für alle diese Probleme gibt es jedoch zumindest theoretische Lösungen:

- **Fehlerkorrektur (‚fault-tolerant QC') ist möglich (Shor 1995/96)**
- Dekohärenz scheint beherrschbar durch **adiabatisches Quantencomputing, dekohärenzfreie Unterräume, bang-bang Methoden,** etc.

! Mehrere, prinzipiell verschiedene Ansätze zur Realisierung koexistieren !

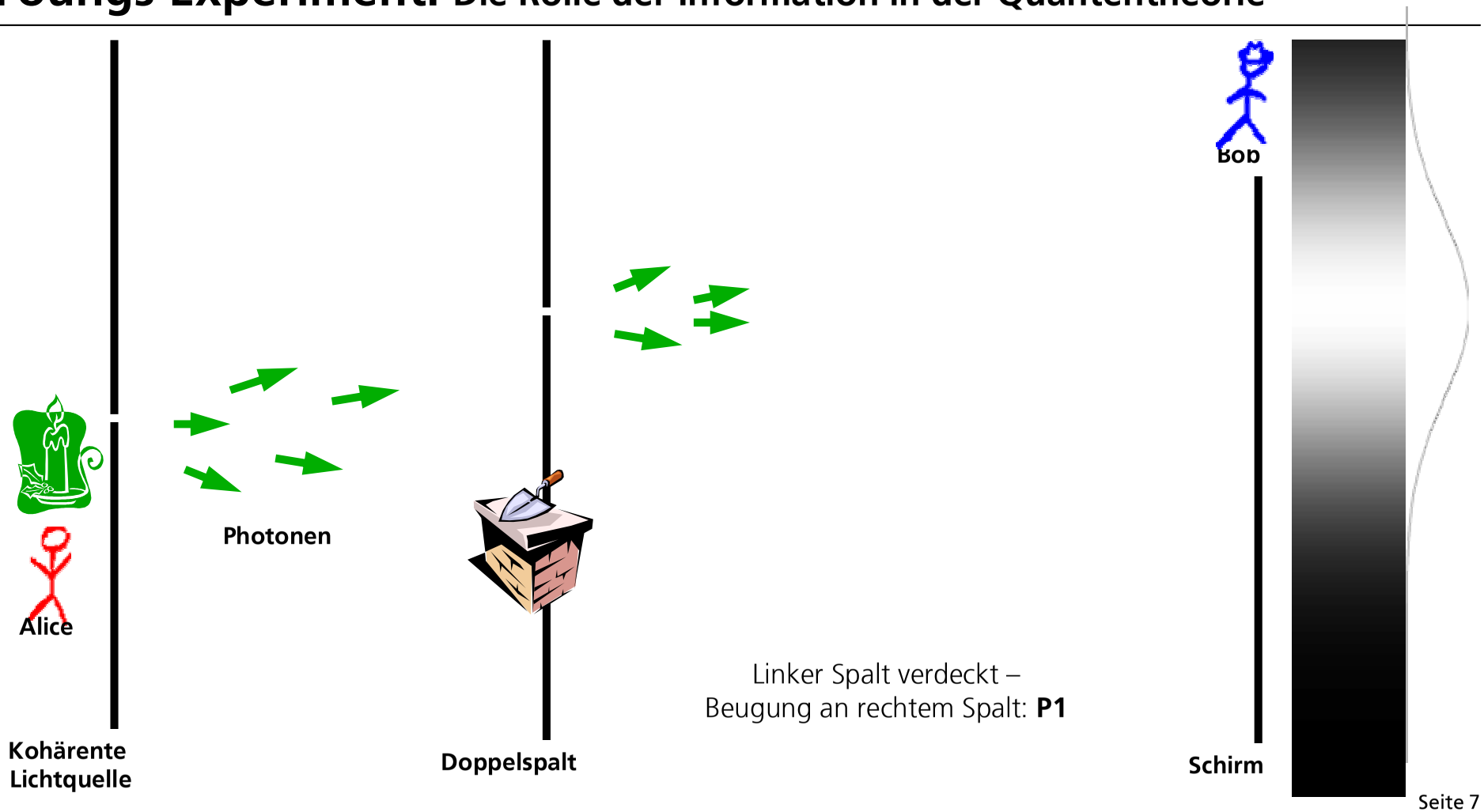
- **Einzelne Atome und QED in Kavitäten** als erster, am weitesten entwickelter Ansatz
- **Nuklearmagnetische Resonanz**: Molekülanregungen werden mit gepulsten Magnetfeldern manipuliert
- **Quantenpunkte** in Supraleitern sind die erste Realisierung von qubits in Festkörpern
- **Nichtabelsche Anyonen** und **topologisches QC**

Schluß: Bewertungen, die QC für grundsätzlich unrealisierbar halten, oder die Realisierung in beliebig ferne Zunkünfte verschieben, scheinen unseriös

SIT
Fraunhofer Institut Sichere Telekooperation

Competence Center For Applied Security Technology
CAST

Youngs Experiment: Die Rolle der Information in der Quantentheorie

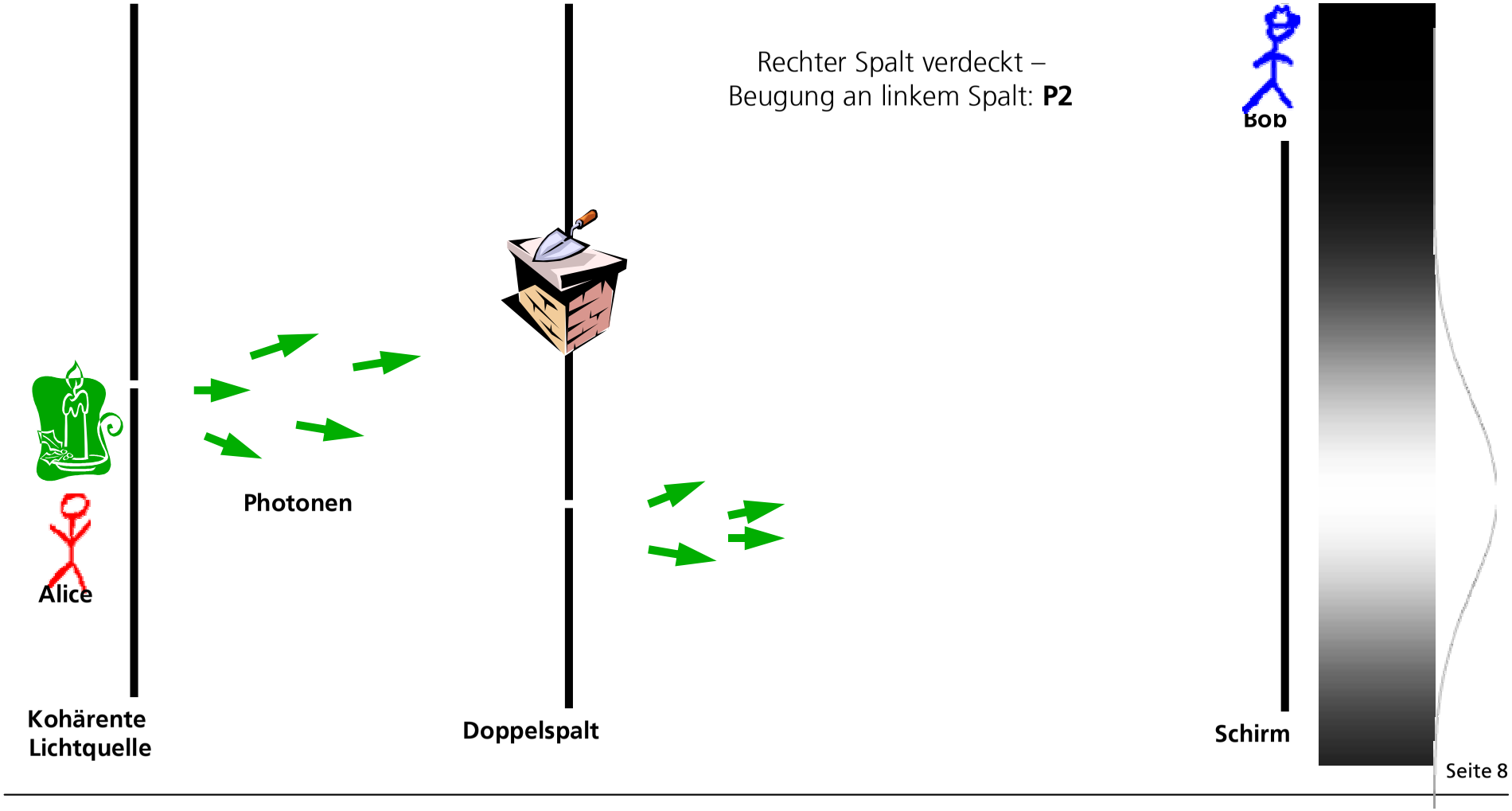


Linker Spalt verdeckt –
Beugung an rechtem Spalt: **P1**

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

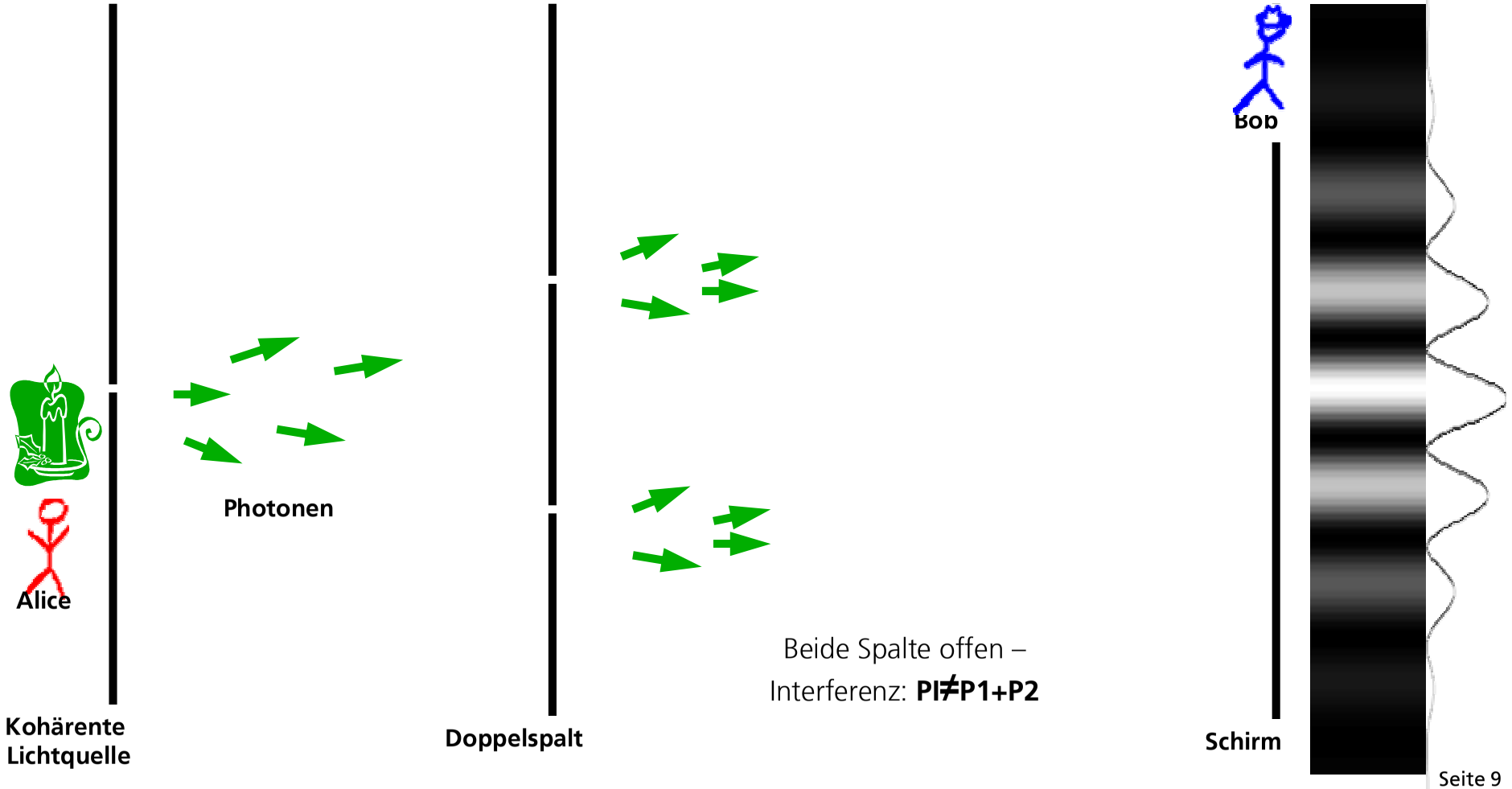
Youngs Experiment: Die Rolle der Information in der Quantentheorie



Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

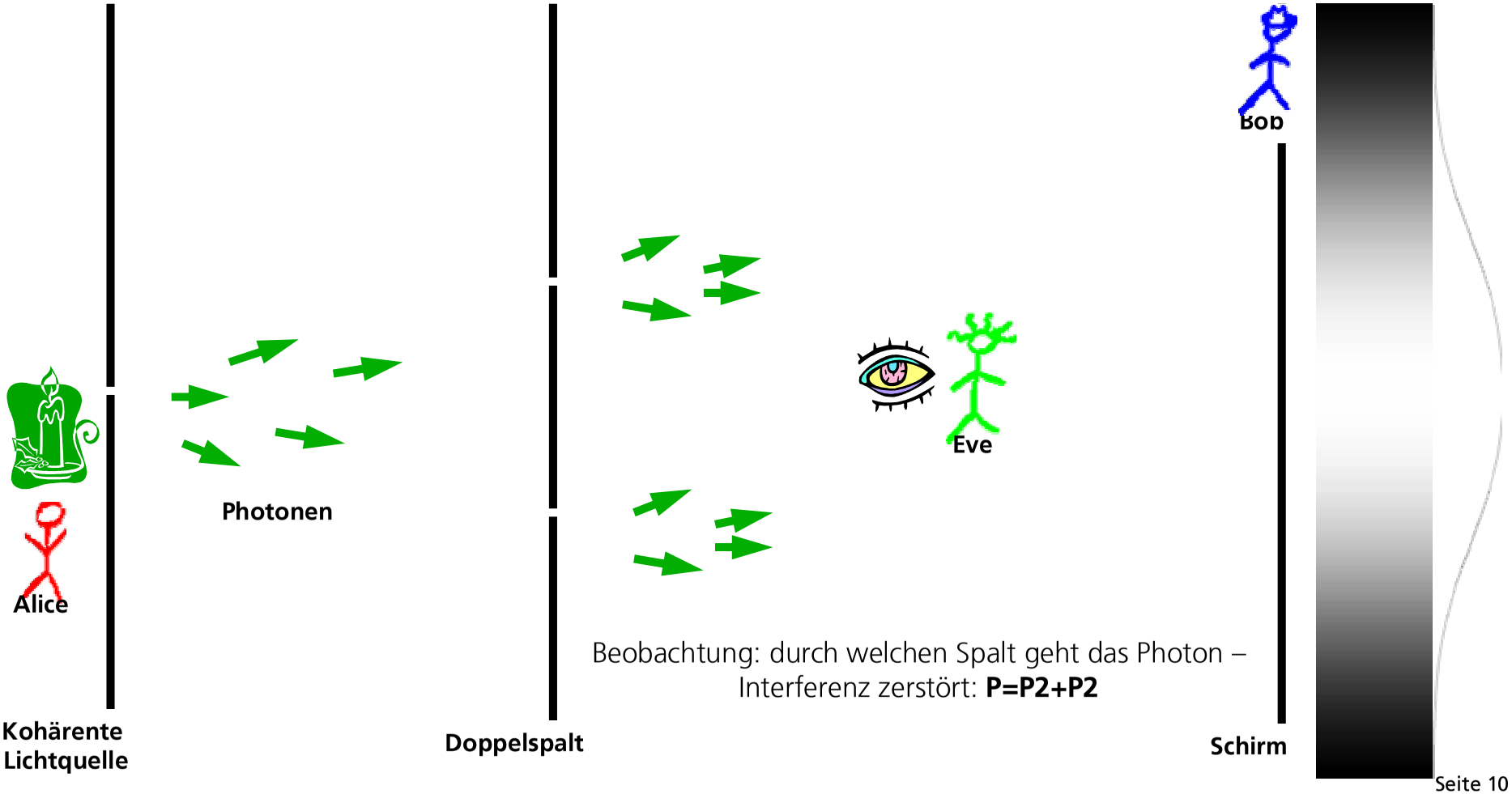
Youngs Experiment: Die Rolle der Information in der Quantentheorie



Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Youngs Experiment: Die Rolle der Information in der Quantentheorie



Beobachtung: durch welchen Spalt geht das Photon –
Interferenz zerstört: **P=P2+P2**

Fraunhofer SIT Institut Sichere Telekooperation
Competence Center For Applied Security Technology CAST

Was ist Quantentkryptographie?

Verwendet Alice **inkommensurable Observablen** zur Übertragung der Information an Bob, dann stört jeder Versuch des Abhörens durch Eve die Übertragung, das heißt

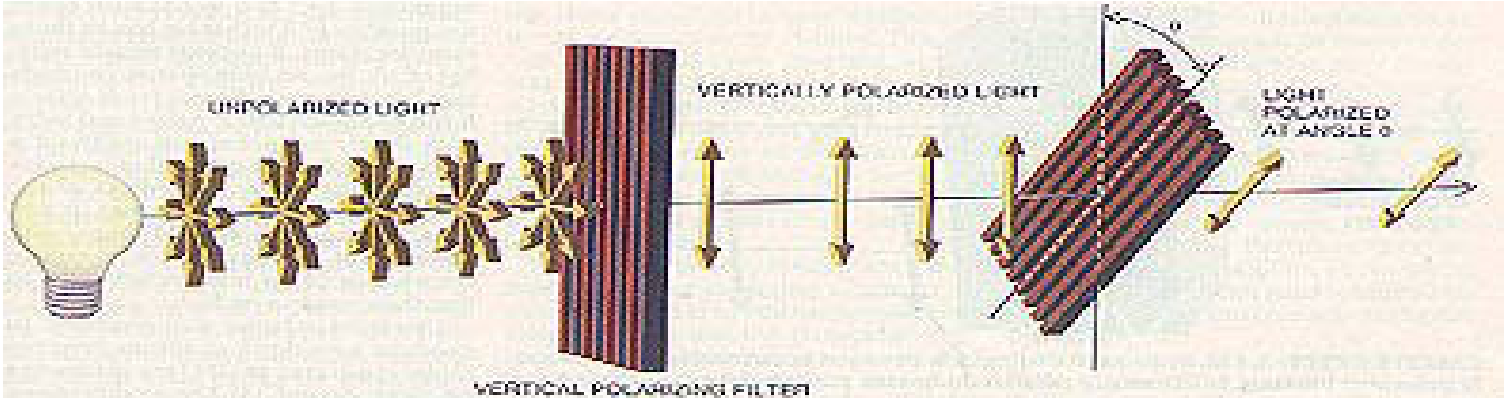
Quantenkryptographie ist eine Methode zur physikalisch sicheren, automatischen Feststellung von Abhörversuchen

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Das Protokoll BB84 (Bennet, Brassard 1984)

I. Polarisiertes Licht und Alices Alphabete



Alice benutzt einen Polaroidfilter, um binäre Information mit ***zwei verschiedenen, inkommensurablen*** Alphabeten zu kodieren.

Alphabet **A** verwendet rektilineare Polarisation: **0** **1**

Alphabet **B** verwendet diagonale Polarisation: **0** **1**

Bildquelle: C. H. Bennett, G. Brassard and A. K. Ekert: *Quantum Cryptography,* Scientific American Jul 92

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

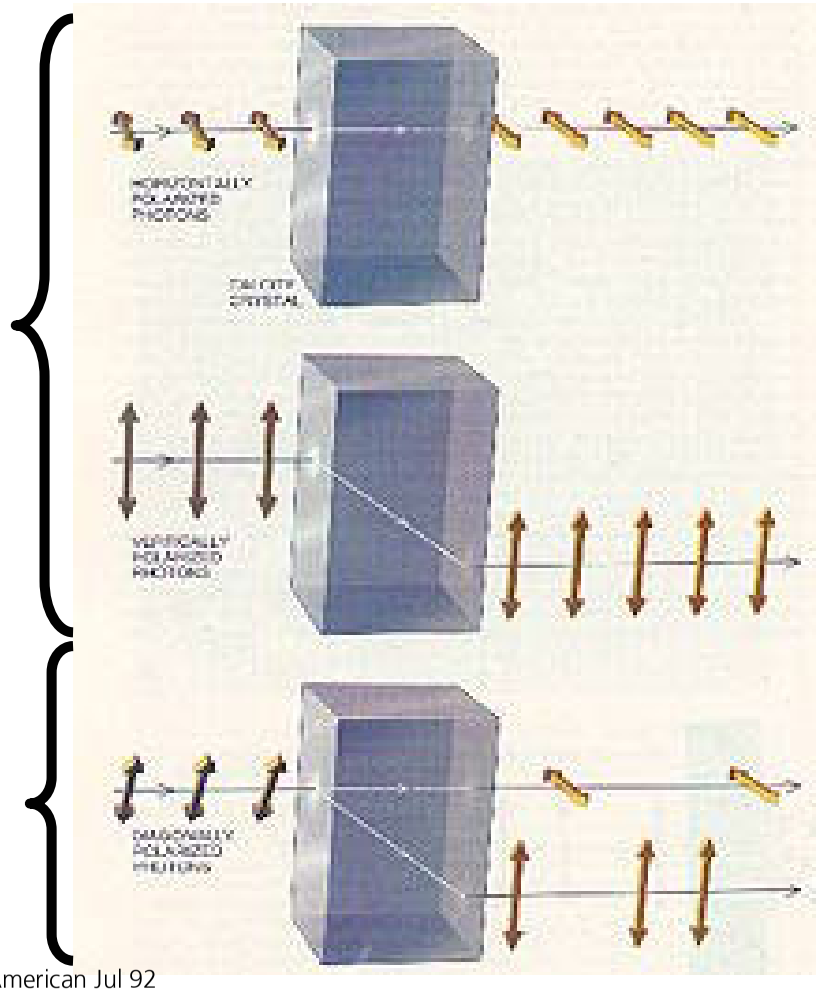
Das Protokoll BB84

II. Bobs Detektor

Bobs Detektor steht aufrecht zur Detektion von Photonen, die Bits im Alphabet A kodieren

Der Kalzitkristall unterscheidet zuverlässig zwischen 0 und 1

Bobs Detektor kann in dieser Stellung Bits des Alphabets B nicht unterscheiden – er mißt für **50%** der gesendeten Bits den falschen Wert. Um B-Bits richtig zu messen, muß der Detektor um 45° gedreht werden.



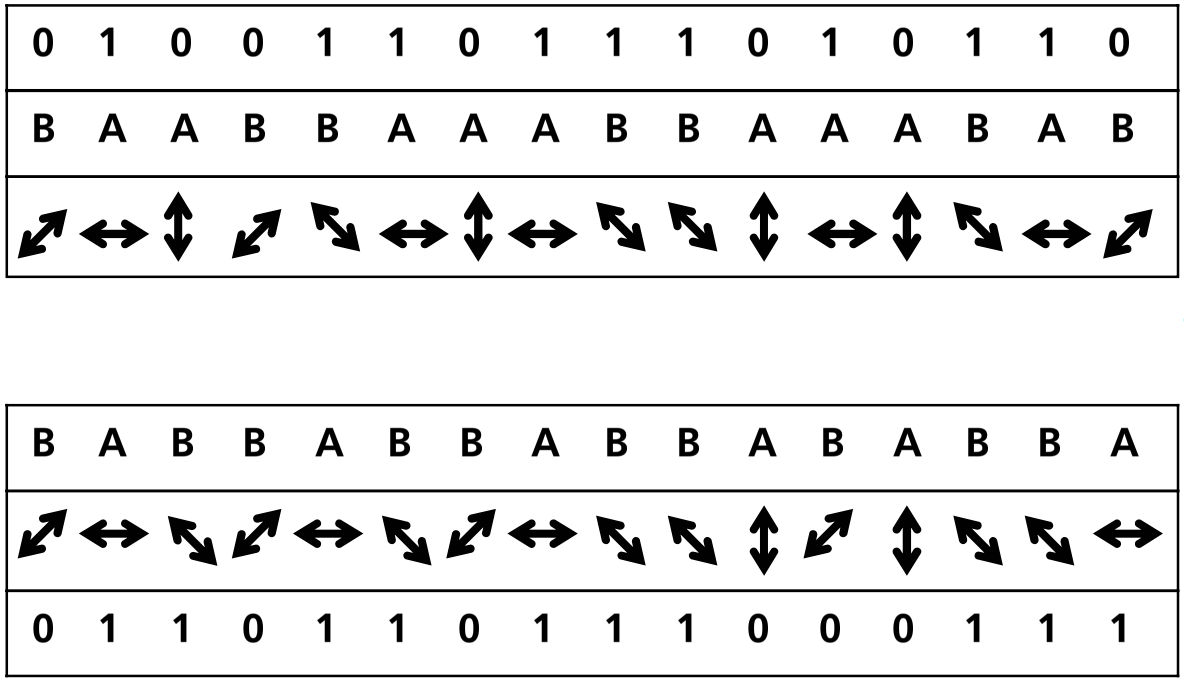
Bildquelle: C. H. Bennett, G. Brassard and A. K. Ekert: *Quantum Cryptography,* Scientific American Jul 92

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Das Protokoll BB84

III. Übetragung eines zufälligen Schlüssels



Alice würfelt eine zufällige Bitfolge **S(A)** (z.B. mit einem **Quantenzufallsgenerator**)

Sie wählt ebenso zufällig die Alphabete **Alph(A)** zur Kodierung der einzelnen Bits

Alice

Sie kodiert **S(A)** entsprechend den gewählten Alphabeten mit ihrem Polarisator

Alice sendet den Kode über den **Quantenkanal** an Bob

Bob wählt zufällig Alphabete **Alph(B)** zur Dekodierung

und mißt entsprechend die Polarisierung

Bob

Bob dekodiert die Messungen gemäß **Alph(B)** und erhält eine Bitfolge **S(B)**

Alice und Bob vergleichen ihre Alphabete **Alph(A)** und **Alph(B)** öffentlich

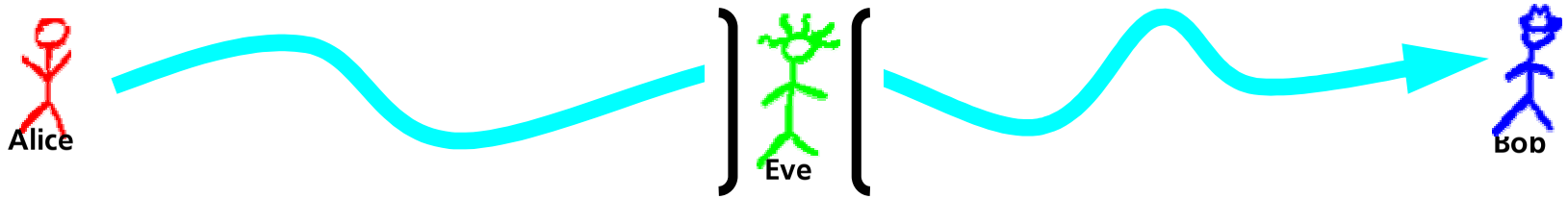
und behalten die übereinstimmenden Stellen als **Rohschlüssel R(A,B)** zurück

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Das Protokoll BB84

IV. Auswirkung von Eve auf den Rohschlüssel R(A,B)



Eve führt einen ***Intercept-Resend*** Angriff auf den Quantenkanal durch

Dies hat einen Bitfehler von **25%** für **R(A,B)** zur Folge !
Beispiel: Alice hat **0** in Alphabet **A** gesendet

Alices Kodierung (**0** in **A**)	↔	
Eves Alphabet	**A**	**B**
Eves Messung und Resend	↔	⤡ ⤢
Bobs Messung (in **A**)	↔	↕ ↔ ↕ ↔

Alice und Bob komplettieren das Protokoll BB84, indem sie einen Teil der Länge ***N*** des Rohschlüssels vergleichen und verwerfen. Stellen sie dabei keine Abweichung fest, ist der Quantenkanal mit der Wahrscheinlichkeit $1 - (3/4)^N$ sauber.
Der gemeinsame Schlüssel kann für ein klassisches Krypto-Protokoll verwendet werden.

Fraunhofer SIT Institut Sichere Telekooperation
Competence Center For Applied Security Technology CAST

Der Sicherheitsbegriff der Quantenkryptographie

Fallstrick Key Distribution Problem gelöst?

- **Kanalsicherheit** wird erreicht, innerhalb realistischer Grenzen
- **Authentisierung** ist *nicht* möglich, genauso wenig wie in klassischer Kryptographie
- Physikalisch sichere **Intrusion Detection** ist der wesentliche Beitrag der QK

Fundamentale Angriffe auf und prinzipielle Grenzen der QKD

- Angriffe auf Grund von **Implementierungsschwächen**, insbesondere ‚durchscheinendes Abhören' (**translucent eavesdropping**) z.B. durch Strahlteiler (**beam-splitting attack**)
- **Man-in-the-middle-attack** wegen fehlender Authentisierung
- Stets vorhandenes **Kanalrauschen** (**noise**) auf dem Quantenkanal ist ***prinzipiell ununterscheidbar*** von den durch Abhören verursachten Störungen – Grenzen der Intrusion detection

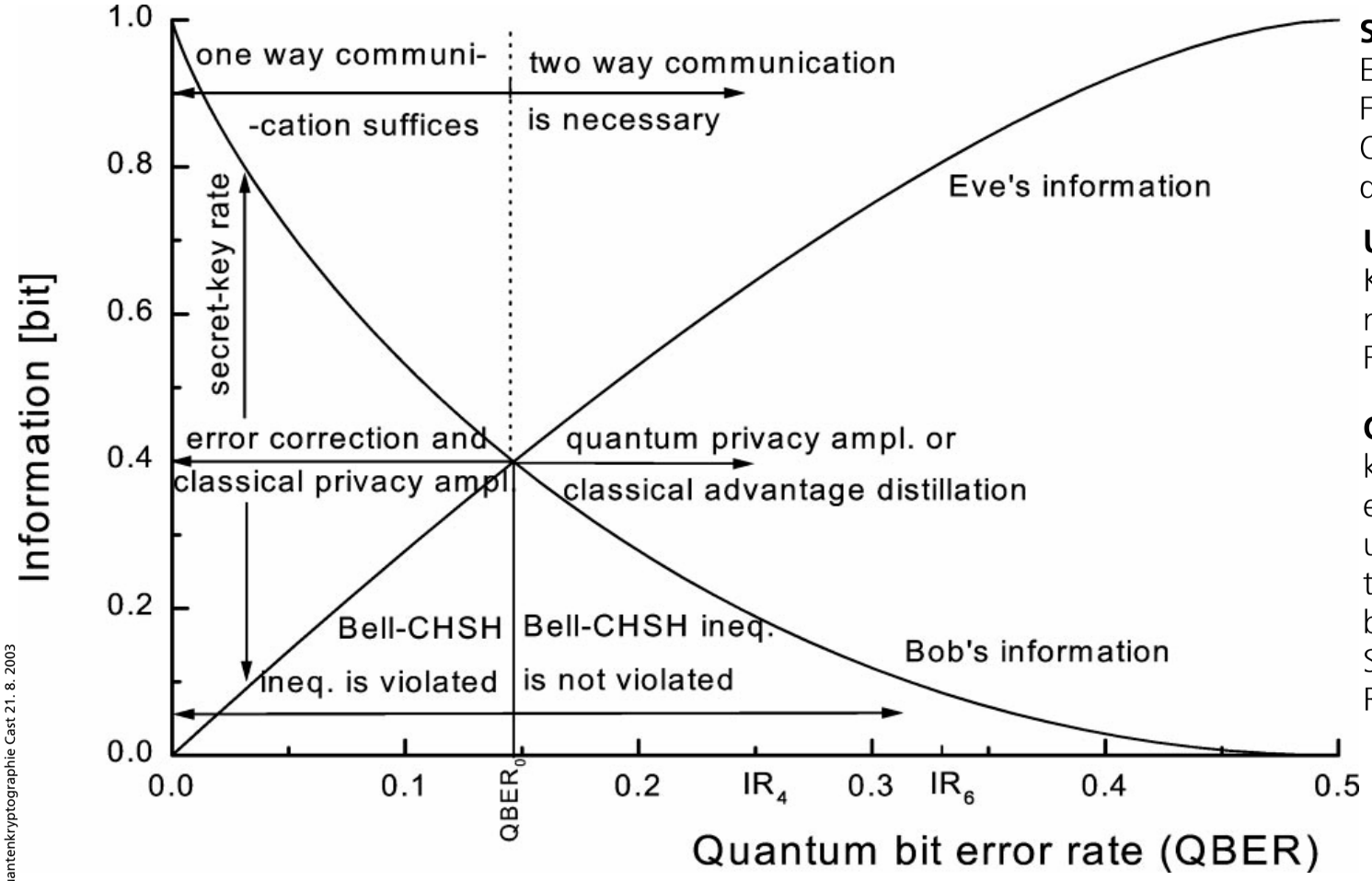
Zusätzliche Schritte in realistischen QKD Protokollen: Schlüssel-Distillation

- **Fehlerkorrektur:** klassische Protokolle zur Bitfehlerkorrektur (Checksummen, Binärsuche, ...)
- **Privacy Amplification:** klassische Protokolle zur Reduktion von Eves Information über den zunächst nur ***teilweise geheimen*** Rohschlüssel (Bildung von Blockparitäten, Bennett et al., 1988, 1995)
- **Advantage distillation:** Weniger effiziente Protokolle benutzen zwei-Wege Kommunikation über einen authentisierten Kanal. Sie werden evtl. nötig, wenn Eve zuviel Information besitzt
- **Quanten-privacy-amplification** verwendet ***verschränkte*** Quantenzustände

SIT
Fraunhofer Institut Sichere Telekooperation

Competence Center For Applied Security Technology
CAST

Sicherheitsanalyse am Beispiel BB84



Sicherheit von QKD-Protokollen:
Eves Information ist beschränkt als Funktion der resultierenden Quanten-Bitfehlerrate **QBER** des Rohschlüssels

Unterhalb der Schwelle $QBER_0$:
Klassische Fehlerkorrektur und PA mit ein-Wege Kommunikation reichen Für eine effektive QKD aus

Oberhalb der Schwelle $QBER_0$:
klassische Fehlerkorrektur kann ergänzt werden durch Quanten-PA und/oder klassische advantage distillation, die zwei-Wege Kommunikation benötigen. Dies geht bis zu gewissen Schwellen IR_4, IR_6 für die Intercept-Resend Strategie bei 4 (6) Zuständen

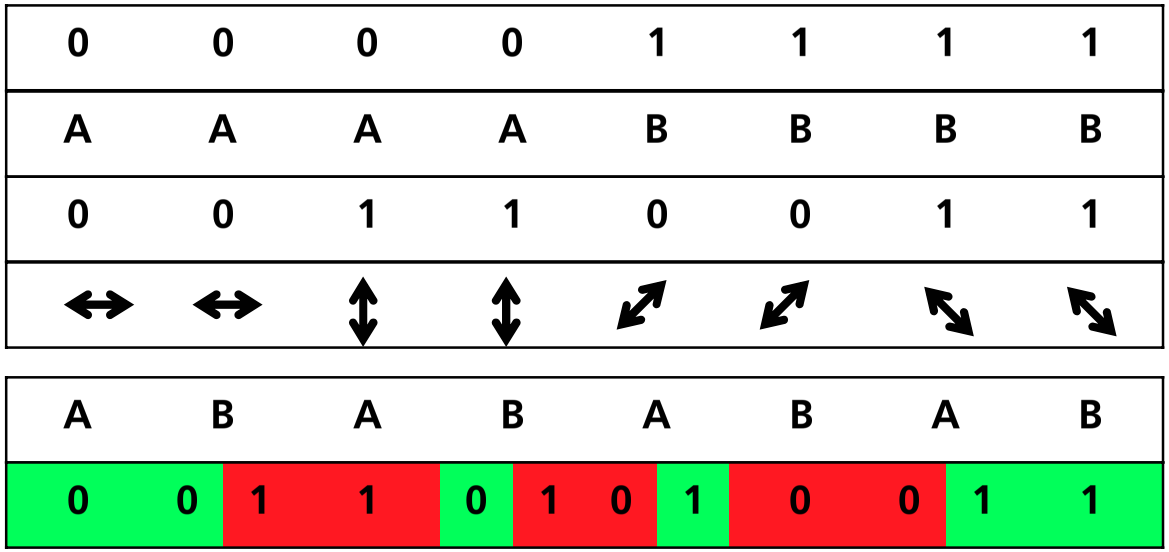
Quelle: Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden: *Quantum Cryptography*, Rev. Modern Phys. 74 (2002) 145

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Das Bit-commitment Problem

I. Das BB84 Protokoll zum verdeckten Hinterlegen von Information



Alice wählt eine Folge von Bits, die sie bei Bob hinterlegen möchte

Entsprechend dieser Bits wählt sie die Kodierungsbasen

Sie wählt eine (anders als gezeigt) ***zufällige*** Folge von Prüfbits und kodiert sie in den gewählten Alphabeten

Egal, welche Meßbasis Bob (zufällig) wählt...
gemessener Bitwert und hinterlegter Bitwert stimmen nur in 50% aller Fälle überein, d.h. sie sind **unkorreliert** – Verdeckung ist erreicht

In der **Eröffnungsphase** sendet Alice die hinterlegten Bits und die Zufallsbits über einen klassischen Kanal an Bob.

Würde sie dabei über das hinterlegte Bit die Unwahrheit sagen, kann Bob dies in 50% aller Fälle feststellen, weil sein Meßresultat physikalisch nicht möglich ist – das Protokoll ist **Betrugssicher.**

Zumindest, wenn Alice nur ***klassische*** Strategien verwendet...

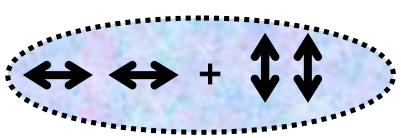
Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Das Bit-commitment Problem

II. Verschränkte Zustände ermöglichen Alice Betrug

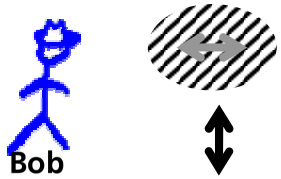
Alice verwendet ***zwei* verschränkte** Photonen und das **Überlagerungsprinzip** für ihren Betrug



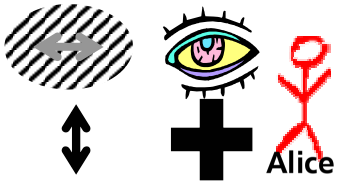
Alice präpariert eine symmetrische Überlagerung von zwei Photonen

Sie sendet ***eines*** davon an Bob und behält das andere zurück

Alice möchte eine **1** aufdecken, also glaubhaft machen, sie hätte das gesendete Photon in Basis **A** kodiert



Dadurch wird die Überlagerung auf ***beiden*** Seiten zerstört und die Photonen haben die gleiche Polarisierung – mit Wahrscheinlichkeit 50% **0**(**A**) oder **1**(**A**)

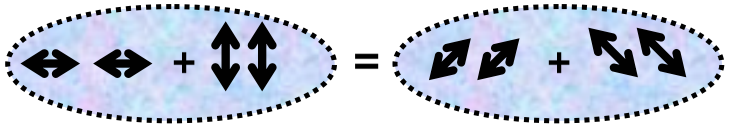


Dazu mißt sie ihr Photon in der Basis **A**

Ihr Meßergebnis sendet sie als angebliches Prüfbit

Mißt Bob in **A**, erhält er zu 100% **1**, mißt er in **B**, zu 50% **0** oder **1** – genauso, als hätte Alice **A** verwendet um **1** zu kodieren, wie behauptet

Will Alice **0** aufdecken, so verwendet sie Basis **B** und die Identität



Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Das Bit-commitment Problem

III. Quanten Bit-commitment ist unmöglich!

Verschiedene Autoren versuchten das Problem durch Verfeinerung des Protokolls zu lösen,
Zum Beispiel BC91 (Brassard, Crépeau), BCJL93 (Brassard, Crépeau, Jozsa, Langlois).

Aber 1996 bewiesen Lo und Chau, sowie unabhängig Mayers die Unmöglichkeit
Von Quanten Bit-commitment:

**Ist Alices Information bei Bob verdeckt hinterlegt,
das heißt Bob hat keine Möglichkeit,
sie vor der Eröffnungsphase in Erfahrung zu bringen,
so hat Alice immer eine Möglichkeit des Betrugs,
das heißt den aufzudeckenden Bitwert
vor der Eröffnung nach Belieben zu wählen**

SIT
Fraunhofer Institut
Sichere Telekooperation

Competence Center For
Applied Security Technology
CAST

Einige weitere Methoden der Quantenkryptographie

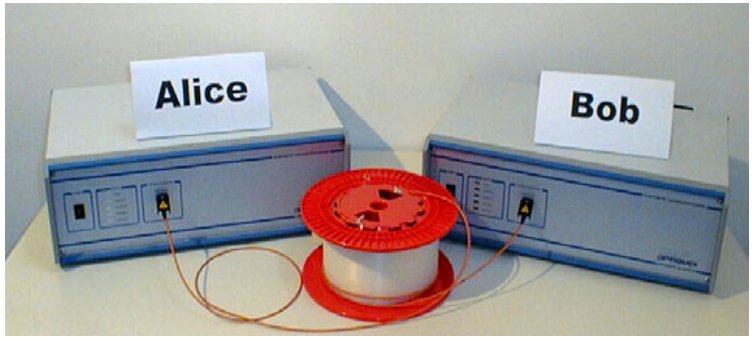
- **Verschränkte (EPR) Zustände:** Alternatives QKD Protokoll (Ekert 1991), bei dem eine Quelle maximal schränkte Paare von Qubits erzeugt und an Alice und Bob verteilt. Sicherheit basiert auf Bells Ungleichung
- **Quanten-Repeater**, basierend auf **entanglement purification**, ermöglichen QKD mit theoretisch unbegrenzter Reichweite (Dür, Briegel, Cirac, Zoller 1999)
- Das **Ping-Pong Protokoll** (Weinfurter et. al. 2002; Boström, Felbinger 2002) benutzt EPR-Paare zur ***direkten, sicheren Informationsübertragung***
- **Quanten-Verschlüsselung:** Die Verschlüsselung von ***Quanteninformation*** mit ***klassischen*** Schlüsseln erfordert optimal 2 Bits pro Qubit (Ambainis, Mosca, Tapp, de Wolf 2000) – **Quanten-one-time-pad**
- **Quanten-Authentisierung:** Authentisierung von Quanteninformation ***erfordert ihre Verschlüsselung*** (Barnum, Crépeau, Gottesman, Smith, Tapp 2002). Daraus folgt: ***Signieren von Quanteninformation ist unmöglich***, denn jedes Protokoll, das einem Empfänger das lesen einer Quantennachricht erlaubt, erlaubt ihm auch ihre unbemerkte Manipulation.
- **Quanten-Signaturen:** Das signieren ***klassischer*** Informationen mit quantenkryptographischen Methoden ist möglich unter Verwendung eines Quanten-Notars und leistet ***zweiseitige Nichtabstreitbarkeit*** – weder Alice noch Bob können die Nachricht verändern, noch ihre Übertragung abstreiten (Zeng, Keitel 2002)
- **Gegenmaßnahmen für Angriffsszenarien:** Z. B. senden von Ablenkungssignalen (**decoy-pulses**) konterkariert Photon-Number-Splitting Angriffe (Hwang 2003)
- **Kontinuierliche Variablen** ermöglichen höhere Übertragungsraten und niedrigere Fehlerraten in realistischen QKD Modellen (u.A.: Cerf 2000; Gottesman, Preskill 2001; Grosshans, Grangier 2002)

SIT
Fraunhofer Institut Sichere Telekooperation

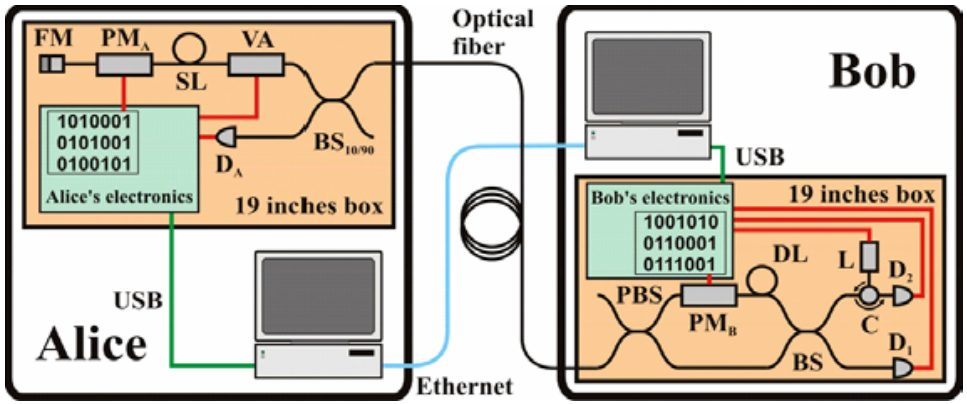
Competence Center For Applied Security Technology
CAST

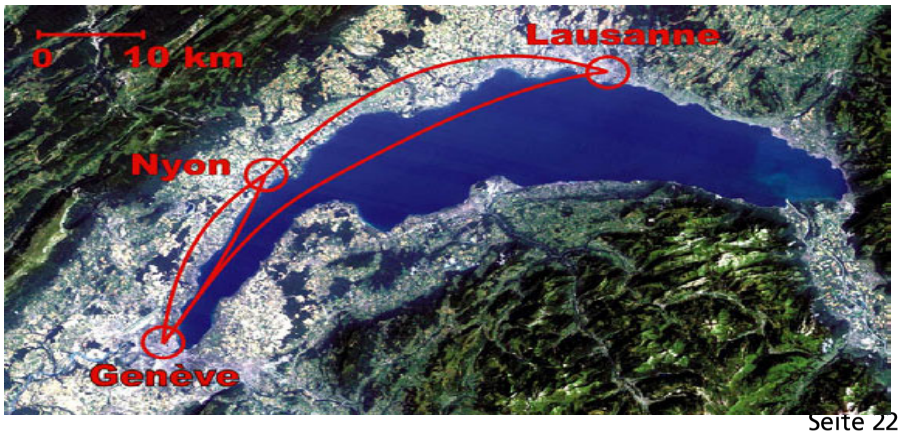
Zwei reale Implementierungen 2002/3

N Gisin, G. Ribordy, H. Zbinden et. al. Von der Unviersität Genf erreichten Mitte 2002 mit einem selbstkorrigierenden **plug&play** System QKD (mit **Phasenkodierung**) über Distanzen von bis zu **67 km** auf handelsüblichen Glasfasern. Ihre Ausgründung **id Quantique** vertreibt das System kommerziell für ca. €80000 pro Stück (derzeitiger Reichweitenrekord: **100 km**, Toshiba Research Europe, UK, Mai 2003)



Fibre	Length (km)	Key (kbit)	R_{raw}(kHz)	$QBER$ (%)	R_{net} (kHz)
Geneva–Nyon (under lake)	22.0	27.9	2.06	2.0 ± 0.1	1.51
Geneva–Nyon (terrestrial)	22.6	27.5	2.02	2.1 ± 0.1	1.39
Nyon–Lausanne (terrestrial)	37.8	25.1	0.50	3.9 ± 0.2	0.26
Geneva–Lausanne (under lake) A	67.1	12.9	0.15	6.1 ± 0.4	0.044
Geneva–Lausanne (under lake) B	67.1	12.9	0.16	5.6 ± 0.3	0.051
Ste Croix (aerial) A	8.7	63.8	6.29	3.0 ± 0.1	4.34
Ste Croix (aerial) B	23.7	117.6	2.32	3.0 ± 0.1	1.57





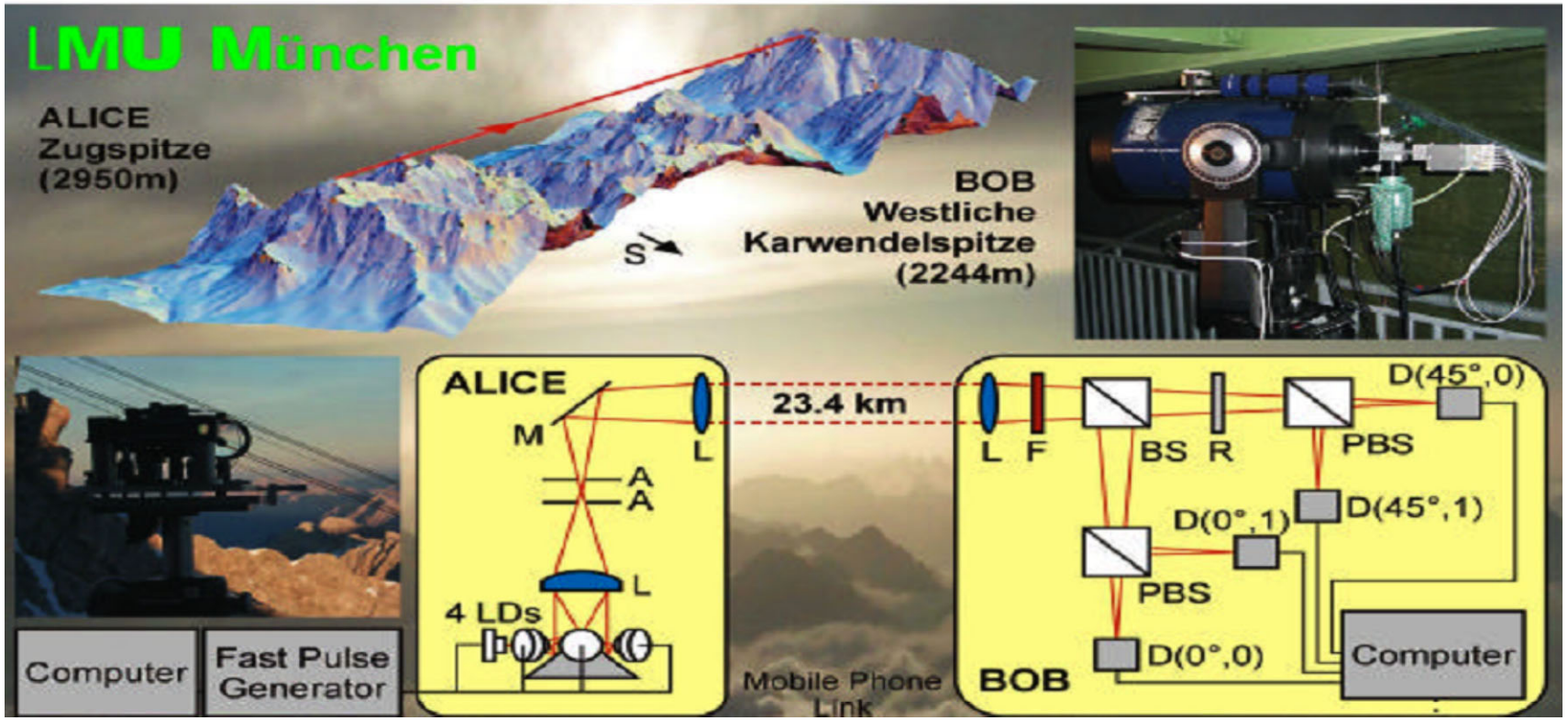
Quelle: New. J. Phys. **4** (2002) 41

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Zwei reale Implementierungen 2002/3

Ch. Kurtsiefer und H. Weinfurter (LMU München) realisierten im September 2002 QKD über 23,4 km **Freiluftstrecke**, mit polarisierten Photonen bei ca. 1kBit/s Rohschlüsselrate
(im EU-Projekt EQCSPOT, in Zusammenarbeit mit DERA/Qinetiq)



Quelle: Einsichten 1/2003. Magazin der Universität München

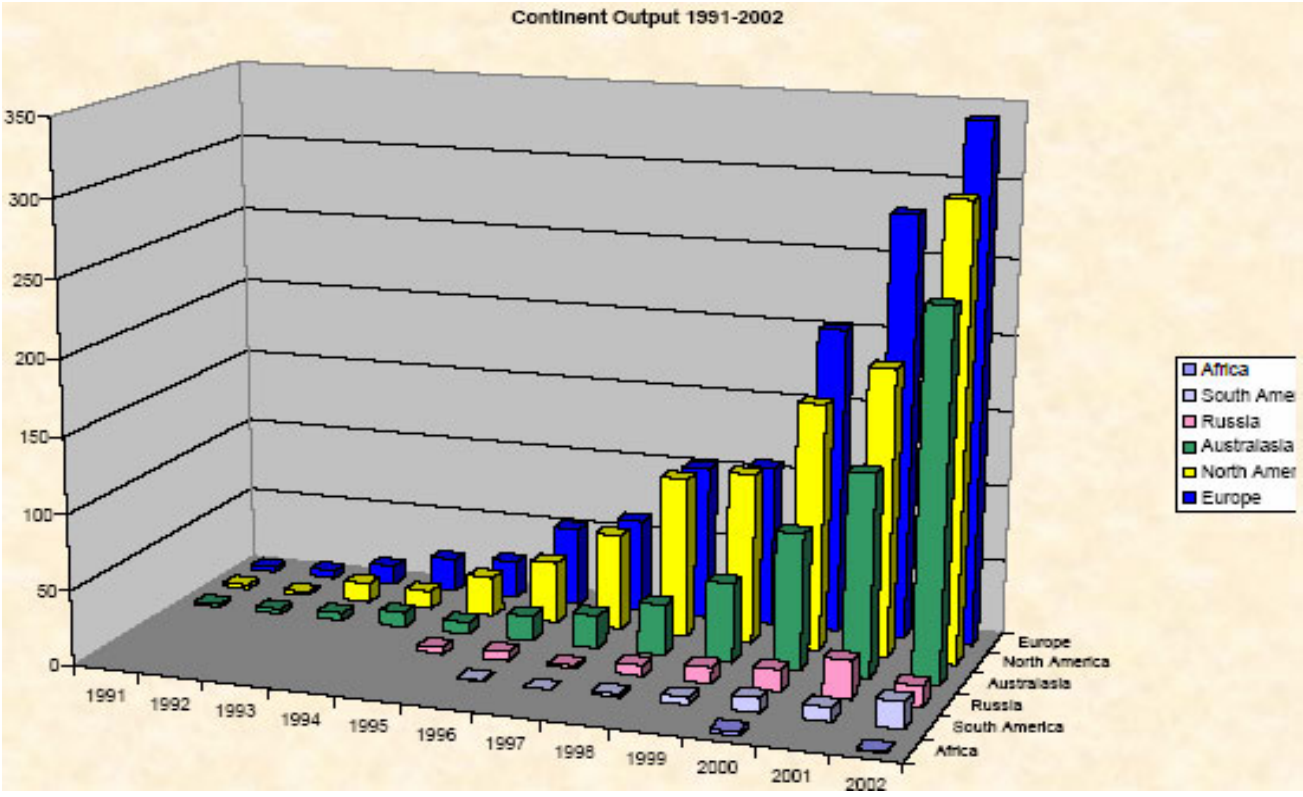
Fraunhofer Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Forschung in QI und QK in EU, USA und weltweit

- **DARPA** Programm zur Quanteninformatik (QuIST) **100 M$** über 5 Jahre ab 2002 (Quelle: www.darpa.mil)
- **EU FP5**: ca. **30 M€** in FET Proactive Initiave „Quantum Information Processing & Communication" (QIPC) plus ca. **5** M€ in FET OPEN in ca. 20 Projekten von 1998 bis 2003 (Quelle: cordis.lu)
- **EU FP6:** Wahrscheinlich ähnliches Budget in bisher ca. 12 Projekten

Veröffentlichungen im Bereich Quanten-information nach Kontinenten
(Quelle: QUIPROCONE)

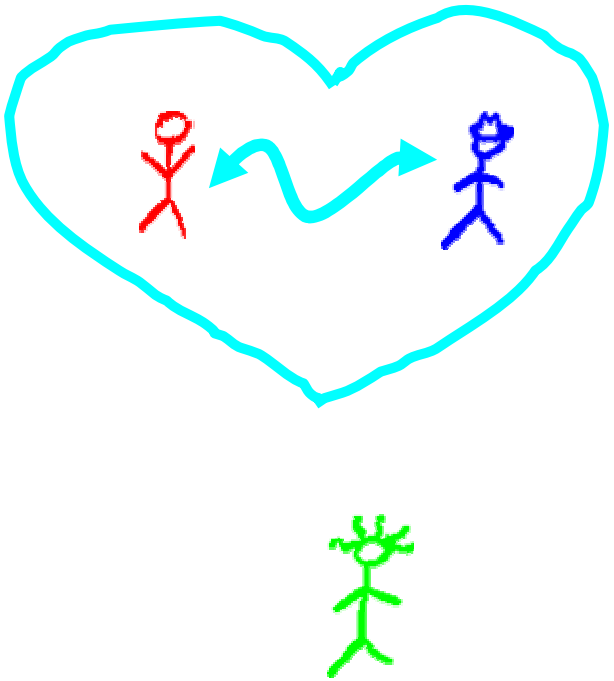


Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Quantum Cryptography:

http://www.theory.caltech.edu/people/preskill/colloquium/Quantum_Cryptography.html



Alice said to her friend Eve,
"Why do you practice to deceive?
You know I need to talk to Bob.
Without that I won't have a job.

"Bob can't know where my note has been.
He thinks that you are listening in.
He wonders if it's safe enough
For me to send him secret stuff.

"And Bob's right not to trust you, Eve,
With quantum tricks stuffed up your sleeve.
But he thinks we can freeze you out,
With quantum tricks we've learned about.

"With quantum states, what we achieve
Defeats whatever you conceive.
So even Bob has to believe
That you can't hear us, can you Eve?"

John Preskill
November 1, 2001

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Web-Ressourcen

- Folien dieses Vortrags auf der Homepage des Autors: http://www.math.uni-frankfurt.de/~aschmidt/paper/cast_qcrypt_de.pdf
- id Quantique http://www.idquantique.com
- MagiQ Technologies http://www.magiqtech.com
- DARPA Programm QuIST http://www.darpa.mil/ipto/programs/quist/index.htm
- Institute for Quantum Information http://www.iqi.caltech.edu
- Centre for Quantum Computation http://www.qubit.org
- EU-IST FET - Proactive Initiative „Quantum Information Processing & Communication“ (QIPC) http://www.cordis.lu/ist/fetqipc.htm
- EU Projekt „European Quantum Cryptography and Single Photon Optical Technology“ (EQCSPOT) http://www.eqcspot.org
- EU Network of Excellence „Quantum Information Processing and Communication“ (QUIPROCONE) http://www.quiprocone.org
- EU Projekt „Entanglement in Quantum Information Processing and Communication“ (EQUIP) http://www.equip.qipc.org und sein Nachfolger „Quantum Properties of Distributed Systems“ (QUPRODIS) http://www.quprodis.org
- EU Projekt „Long Distance Photonic Quantum Communication“ (QuComm) http://www.ele.kth.se/QEO/qucomm
- ARDA Quantum Information Science and Technology Roadmapping Project http://qist.lanl.gov
- Experimentelle Quantenphysik an der LMU München http://xqp.physik.uni-muenchen.de/

SIT
Fraunhofer Institut Sichere Telekooperation

Competence Center For Applied Security Technology
CAST

Literatur

- A. K. Ekert: *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67** (1991) 661–663.
- H. K. Lo, H. F. Chau: *Is Quantum Bit Commitment Really Possible?*, Phys. Rev. Lett. **78** (1997) 3410–3413, arXiv: quant-ph/9603004. D. Mayers: *Unconditionally Seccure Quantum Bit Commitment is Impossible,* Phys. Rev. Lett. **78** (1997) 3414–3417, arXiv: quant-ph/9603015.
- W. Dür, H.-J. Briegel, J. I. Cirac, P. Zoller: *Quantum repeaters based on entanglement purification,* Phys. Rev. A **59** (1999) 169-181
- P. W. Shor, J. Preskill: *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett. **85** (2000) 441–444, arXiv: quant-ph/0003004.
- H. Barnum, C. Crépeau, D. Gottesman, A. Smith, A. Tapp: *Authentication of Quantum Messages,* Proc. 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02), pp. 449-458. IEEE Press, 2002, arXiv: quant-ph/0205128.
- K. Boström, T. Felbinger: *Deterministic Secure Direct Communication Using Entanglement*, Phys. Rev. Lett. **89** (2002) 187902, arXiv: quant-ph/0209040. A. Beige, B.-G. Englert, C. Kurtsiefer, H.Weinfurter, Acta Phys. Pol. A **101**, (2002) 357.
- W. Geiselmann, J. Müller-Quade, R. Steinwandt, Th. Beth: *Über Quantencomputer und Quantenkryptographie,* Datenschutz und Datensicherheit **26** (2002) 8, 453–457.
- N. Gisin, G. Ribordy, W. Tittel, H. Zbinden: *Quantum Cryptography*, Rev. Mod. Phys. **74** (2002) 145, arXiv: quant-ph/0101098.
- F. Grosshans, P. Grangier: *Continuous Variable Quantum Cryptography Using Coherent States*, Phys. Rev. Lett. **88** (2002) 057902, arXiv: quant-ph/0109084. *Reverse reconciliation protocols for quantum cryptography with continuous variables*, arXiv: quant-ph/0204127
- G. Zeng, Ch. H. Keitel : *Arbitrated quantum-signature scheme,* Phys. Rev. A **65** (2002) 042312, arXiv: quant-ph/0109007.
- D. Stucki, N. Gisin, G. Guinnard, G. Ribordy, H. Zbinden: *Quantum key distribution over 67 km with a plug&play system,* New J. Phys. **4** (2002) 41.
- Ch. Kurtsiefer, H. Weinfurter: *Mit Photonen zum Schlüssel - Quantenphysik garantiert erstmals abhörsichere Kommunikation,* Einsichten 1/2003. Magazin der Universität München, http://scotty.quantum.physik.uni-muenchen.de/publ/ef.pdf

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST