Cryptography in the Age of Quantum Computers

Fraunhofer Institut
Sichere Telekooperation

COMPETENCE CENTER FOR
APPLIED SECURITY TECHNOLOGY

CAST

Cryptography in the Age of Quantum Computers

Dr. Andreas U. Schmidt

Fraunhofer SIT

AG Marketplace Internet (MINT)

CAST Workshop

„Wie sicher ist Kryptographie?“

21. August 2003

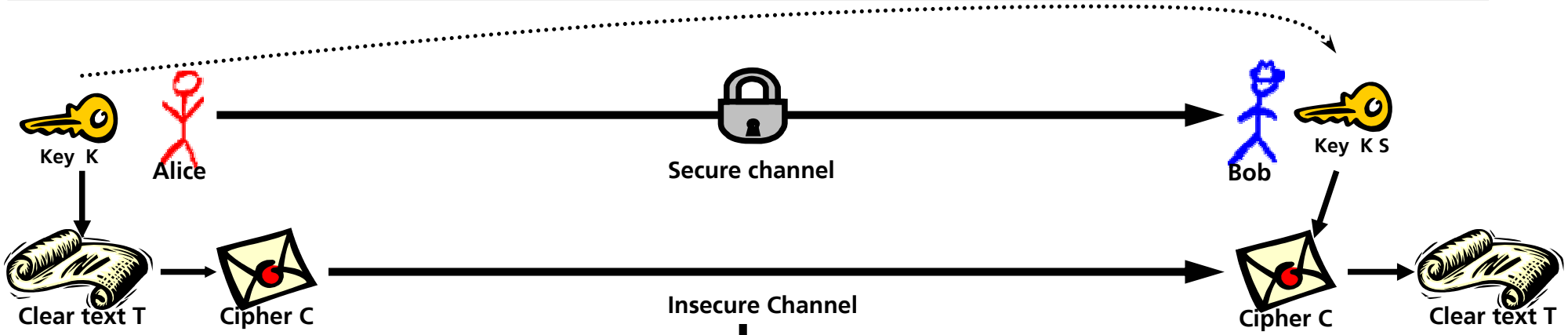
From Classical to Quantum Cryptography

- Pitfalls of classical to cryptography
- Asymmetric cryptography
- Pose quantum computers athreat to asymmetric cryptography?
- Information in quantum theory: Young‘s experiment
- The protocol BB84
- Security in quantum cryptography
- Limitations of QCr: The Bit-commitment problem
- Further quantum cryptographic methods
- Real existing implementations
- Research activities: EU, USA, World

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center for Applied Security Technology CAST

Classsical (symmetric) Cryptography and ist Basic Problems



Cipher: e.g. Vernam-C. or one-time pad. (Vernam 1917 & Shannon 1948)

T	1000111011101
K	0100101100101
C=T XOR K	1100010111000
T=C XOR K	1000111011101

- **Informational perfect security H(T\|C)=H(T)**
- **Key is a random string of the same length as T**

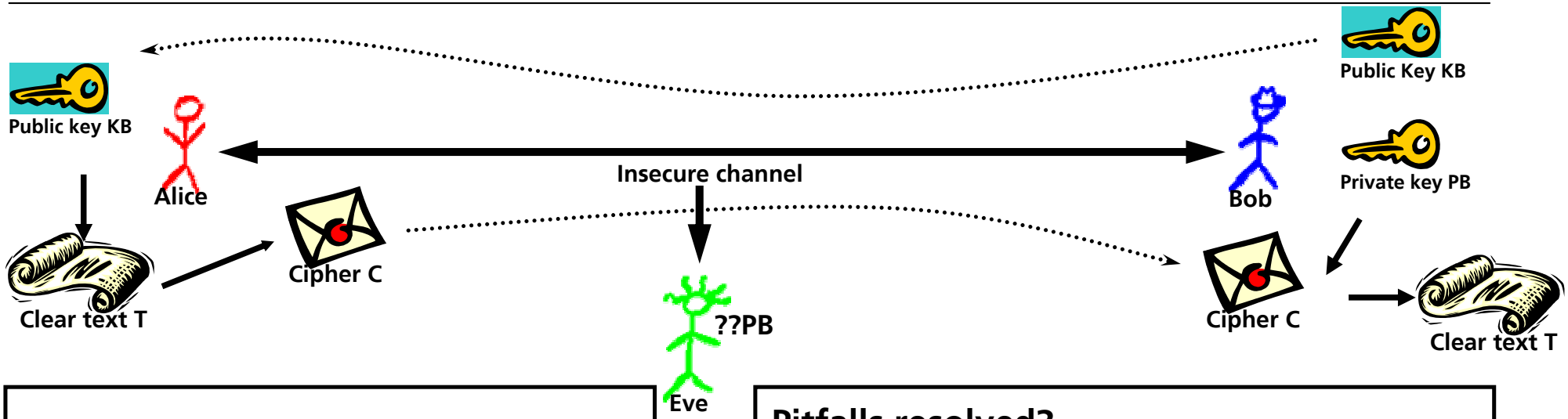
Pitfall Key Distribution Problem:

- Secure channel is assumed
- Authentication of partners not ensured – Man-in-the-middle attack on secure channel always possible
- Intrusion detection not possible – eavesdropping remains undiscovered

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Asymmetric Cryptography



Ciphers use trap-door functions, e.g. discrete logarithms, prime factor decomposition (RSA 1976):

C=KB(T); T=PB(C)

Even if the algorithm is publicly known, is the inversion PB=PB(KB) practically infeasible

Pitfalls resolved?

- Secure channel no longer necessary
- Authentication by digital signatures possible – but: PKIs and CAs needed
- Intrusion detection not given – eavesdropping remains undiscovered
- Principal assumtions of complexity theory (P≠NP) still not proven

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

A threat to Asymmetric Cryptography:

Prime Factoring by Quantum Computation

The asymptotic run-time of the best known c*lassical* algorithm (Lenstra 1990/93) for factoring a number n with approx. $\log n$ Bits grows exponentially:

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

Shor's quantum algorithm (1994), in contrast, is of polynomial run-time, asymptotically:

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

Reason: the superposition principle allows to let a QC run with all possible values of the input simultaneously, e.g.

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

This **massive parallelism** enables QC in particular to a fasr **Fourier transformation,** which is a tenet of the factoring algorithm.

Is the Threat by Quantum Computing Realisitc?

Theoretically yes, due to the existence of the necessary quantum algorithms:

- Shor's factoring algorithm (94) threatens RSA, discrete logarithms, elliptic curves, etc.; Grover's search algorithm (1996) threatens (to a lesser extent) DES

QCs are yet far from practical implementation and realisation faces fundamental problems:

- **Decoherence** limits the limits the persistence of Quibit storage range of Q-communication
- **Separation of Qubits** is necessary, to avoid unwanted entanglement
- **Processing of Quibits** leads to acccumulation of errors

However, there exist, at least theoretical, solutions for all these problems:

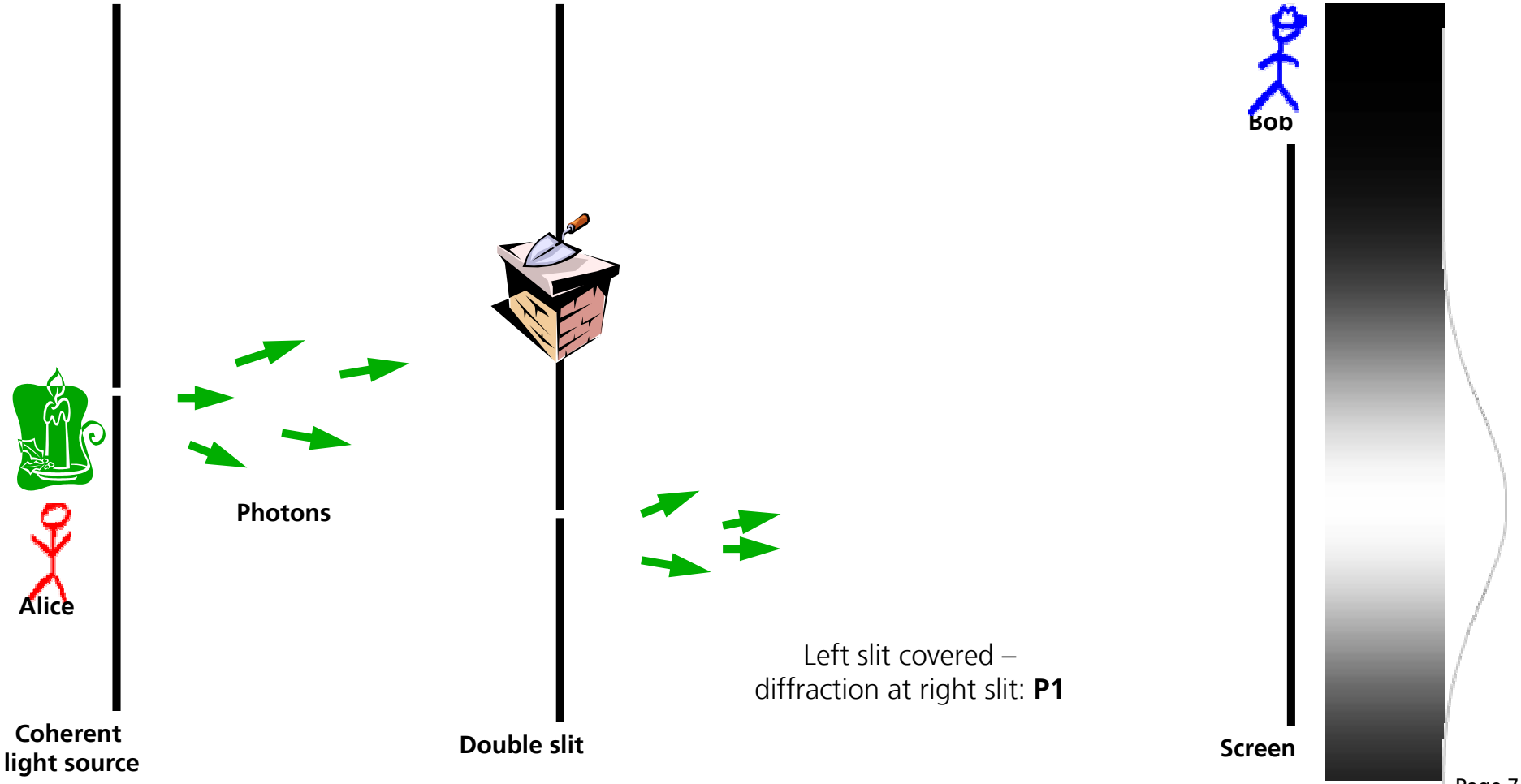
- **Error correction (‚fault-tolerant QC')** is possible (Shor 1995/96)
- Decoherence seems maangeable, e.g., by **adiabatic quantum computing, decoherence free subspaces, bang-bang method,** etc.

! Divers, in princple different approaches for the realisation of QC coexist !

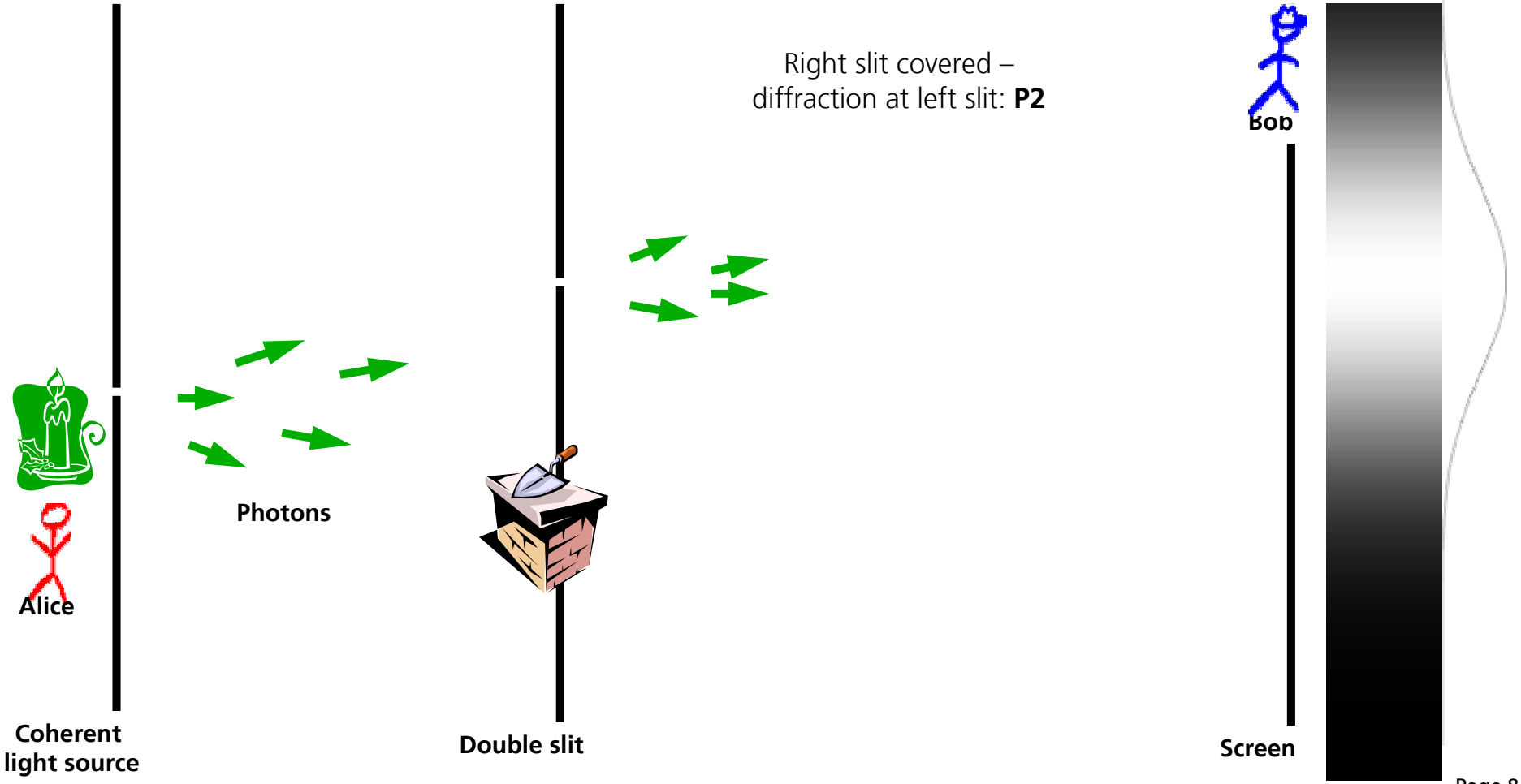
- **Single Atoms and cavity QED** first, and technically most advanced approach
- **Nuclear magnetic resonance**: nuclear excitations of molecules are manipulated with pulsed magnetic fields
- **Quantum dots** in superconductors are the first realisation of Quibits in solids
- **Non-abelian anyons** and **topological QC**

Conclusion: Assesments which consider QC as unfeasible in principle, or defer their realisation into an indefinitely distant future, seem dubious

Young's Experiment: The Role of Information in Quantum Theorie



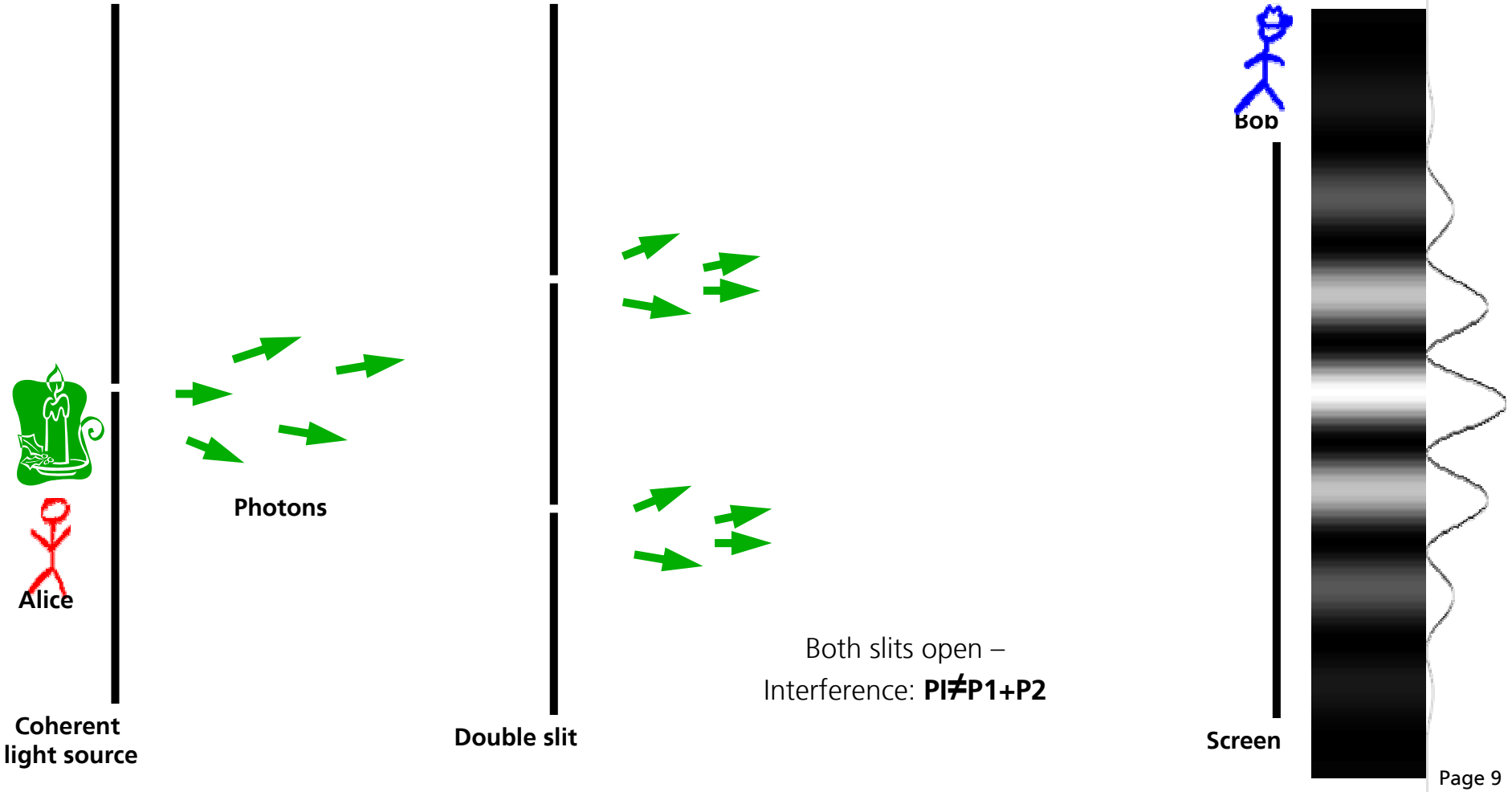
Young's Experiment: The Role of Information in Quantum Theorie



Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

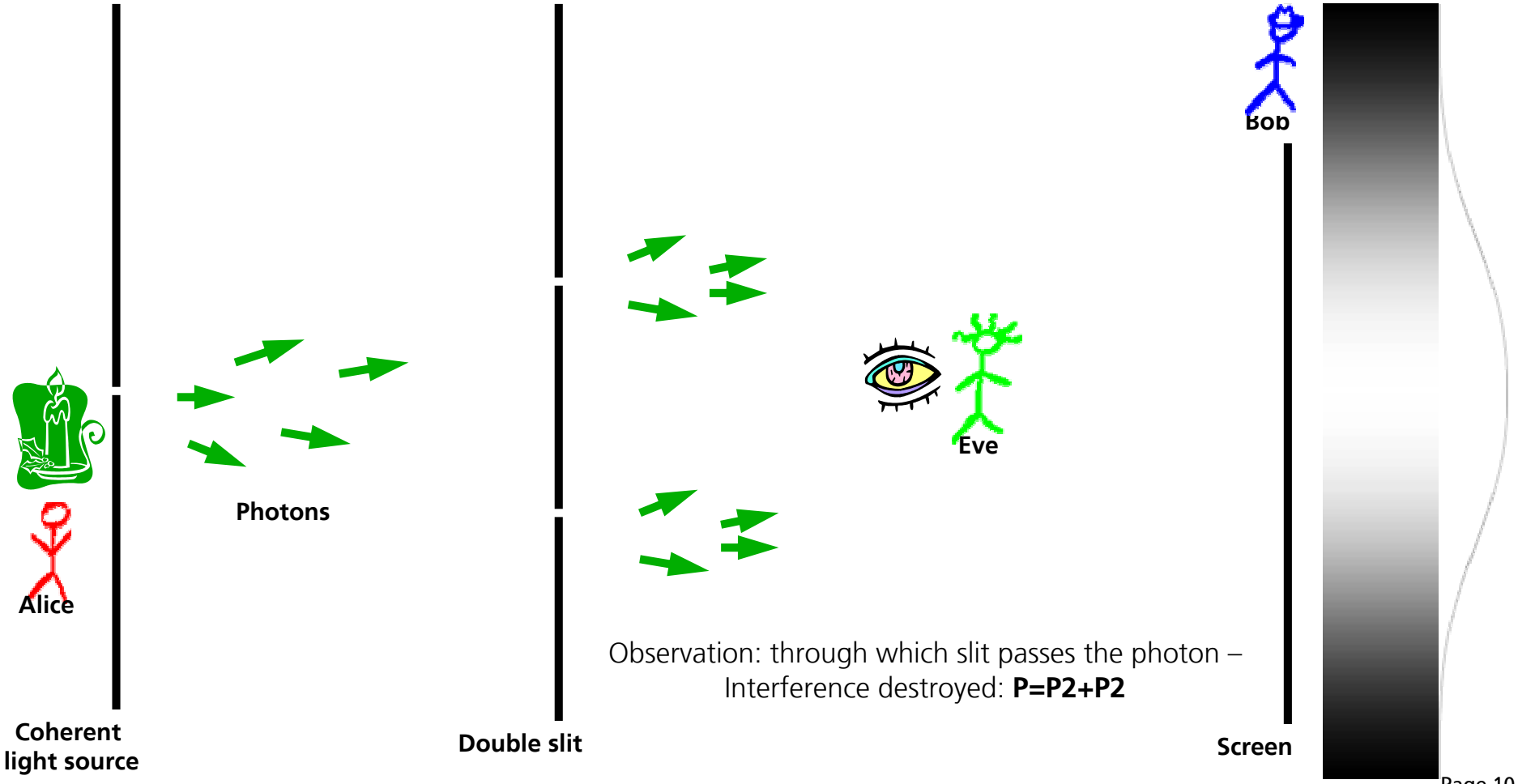
Young's Experiment: The Role of Information in Quantum Theorie



Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Young's Experiment: The Role of Information in Quantum Theorie



Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

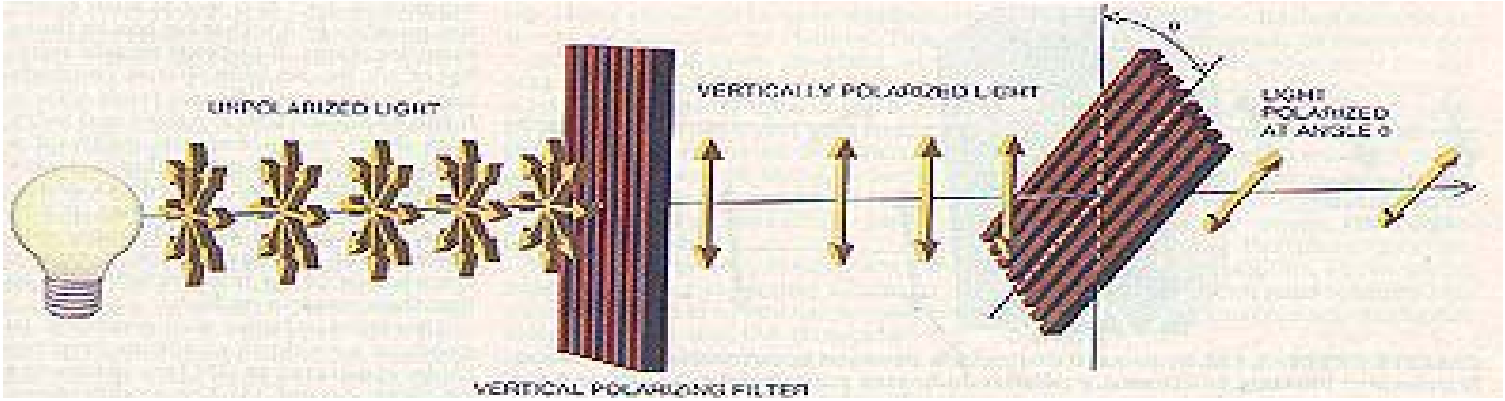
What is Quantum Cryptography?

If Alice uses **inkompatibla Observables** to convey Information to Bob
then every attempt of Eve to eavesdrop will disturb the transmission, that is

Quantum cryptography is
a method to
detect automatically,
and with physical certainty
any attempt to eavesdrop

The Protocol BB84 (Bennet, Brassard 1984)

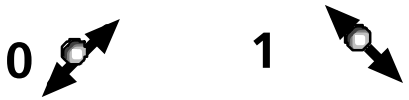
I. Polarised Light and Alice's Alphabets



Alice uses a Polaroid filter, to code binary information in **two different, incompatible** alphabets.

Alphabet **A** uses rectilinear polarisation:

Alphabet **B** uses diagonal polarisation:



Picture: 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

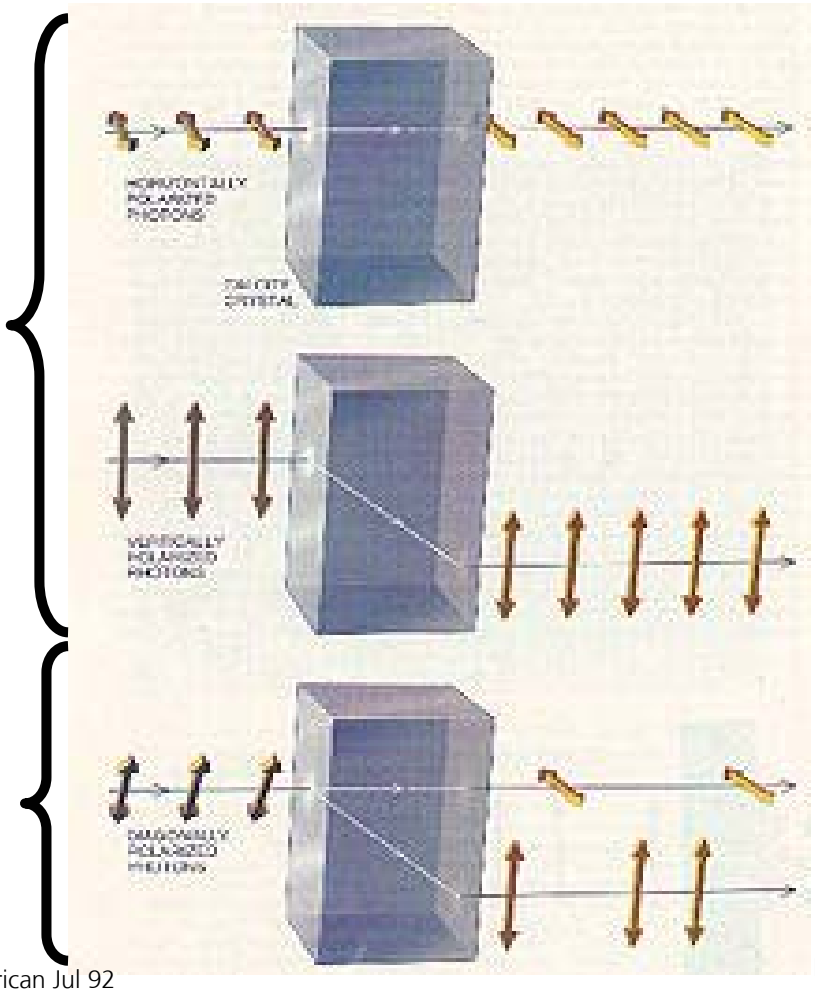
The Protocol BB84

II. Bob's Detector

Bob's Detector is vertically aligned for the detection of photons that code Bits in the alphabet A

The Calcite crystal relaibly discriminates between 0 and 1

In this alignment, it is impossible for Bob's detector to distinguish the Bits of alphabet B – he measures for **50%** of the sent B-Bits the wrong value. To measure B-Bits correctly, the detector has to be rotated by **45°.**



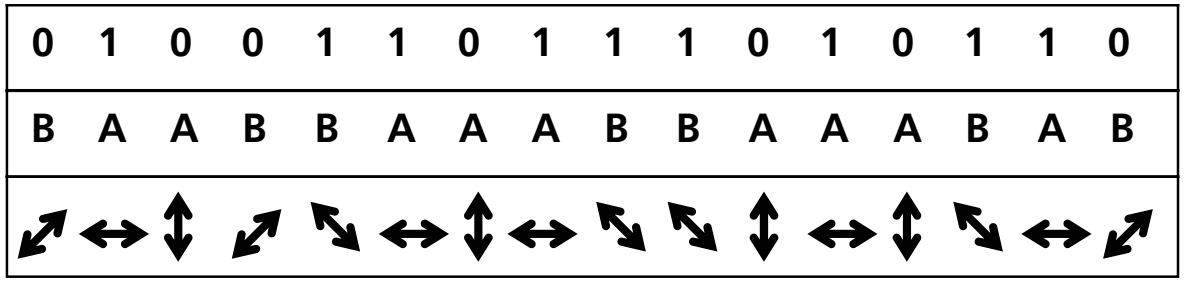
Picture: C. H. Bennett, G. Brassard and A. K. Ekert: *Quantum Cryptography,* Scientific American Jul 92

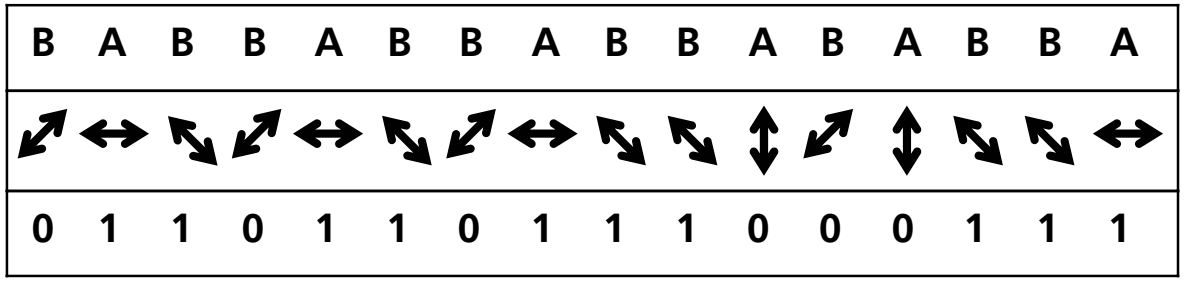
Fraunhofer SIT Institut Sichere Telekooperation

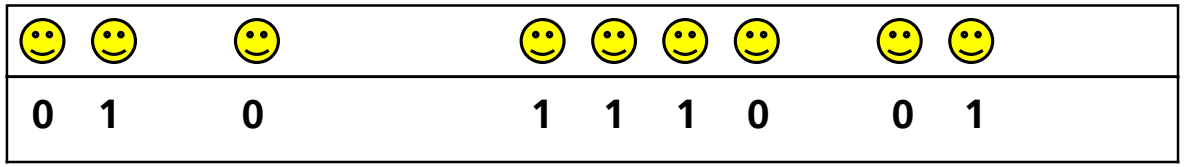
Competence Center For Applied Security Technology CAST

The Protocol BB84

III. Transmission of a Random Binary Key







Alice dices a Bit sequence **S(A)** (e.g. with a **quantum random number generato**r)

Alice

Equally randomly, she chooses the coding Alphabets **Alph(A)** to code each Bit

She codes **S(A)** according to the chosen Alphabets with her polariser

Alice sends this code through the **quantum channel** to Bob

Bob randomly chooses allphabets **Alph(B)** for decoding

Bob

And measures the polarisations accordingly

Bob decodes these measurements pursuant to **Alph(B)** and receives a Bit sequence **S(B)**

Alice and Bob compare the alphabets **Alph(A) a**nd **Alph(B)** publicly

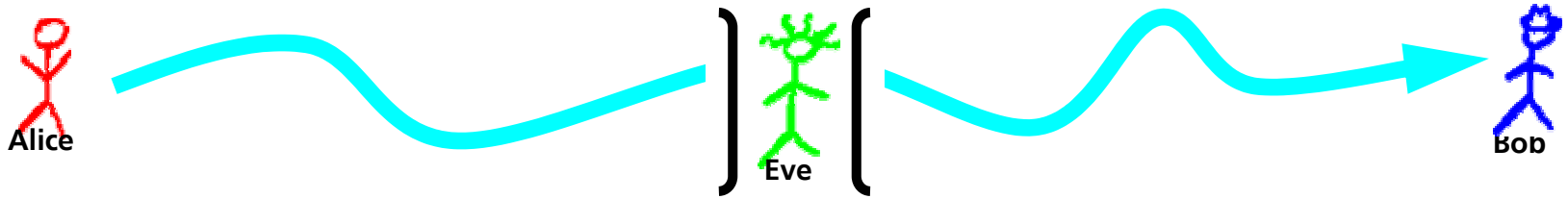
and retain only the coinciding places of the sequence as **raw key R(A,B)**

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

The Protocol BB84

IV. Eve's Impact on the Raw Key R(A,B)



Eve exerts an ***Intercept-Resend*** attack on the qunatum channel

This results in a Bit error of **25%** for **R(A,B)**!
Example**:** Alice sent **0** in alphabet **A**

Alice's coding (**0** in **A**)	↔	
Eve's alphabet	**A**	**B**
Eve's measurement & resend	↔	⤡ ⤢
Bob's measurement (in **A**)	↔	↕ ↔ ↕ ↔

Alice and Bob complete the protocol BB84 by comparing a part of length ***N*** of the raw key and discarding it. If the don't ascertain any deviation then the quantum channel is clean with probability $1 - (3/4)^N$.

The shared key can now be used for a classical cryptographic protocol.

The Notion of Security in Quantum Cryptography

Pitfall Key Distribution Problem resolved?

- **Channel security** is achieved, within certain realistic bounds
- **Authentication** is *not* possible, as in classical cryptography
- Physikally secure **Intrusion Detection** is the essential contribution of QCr

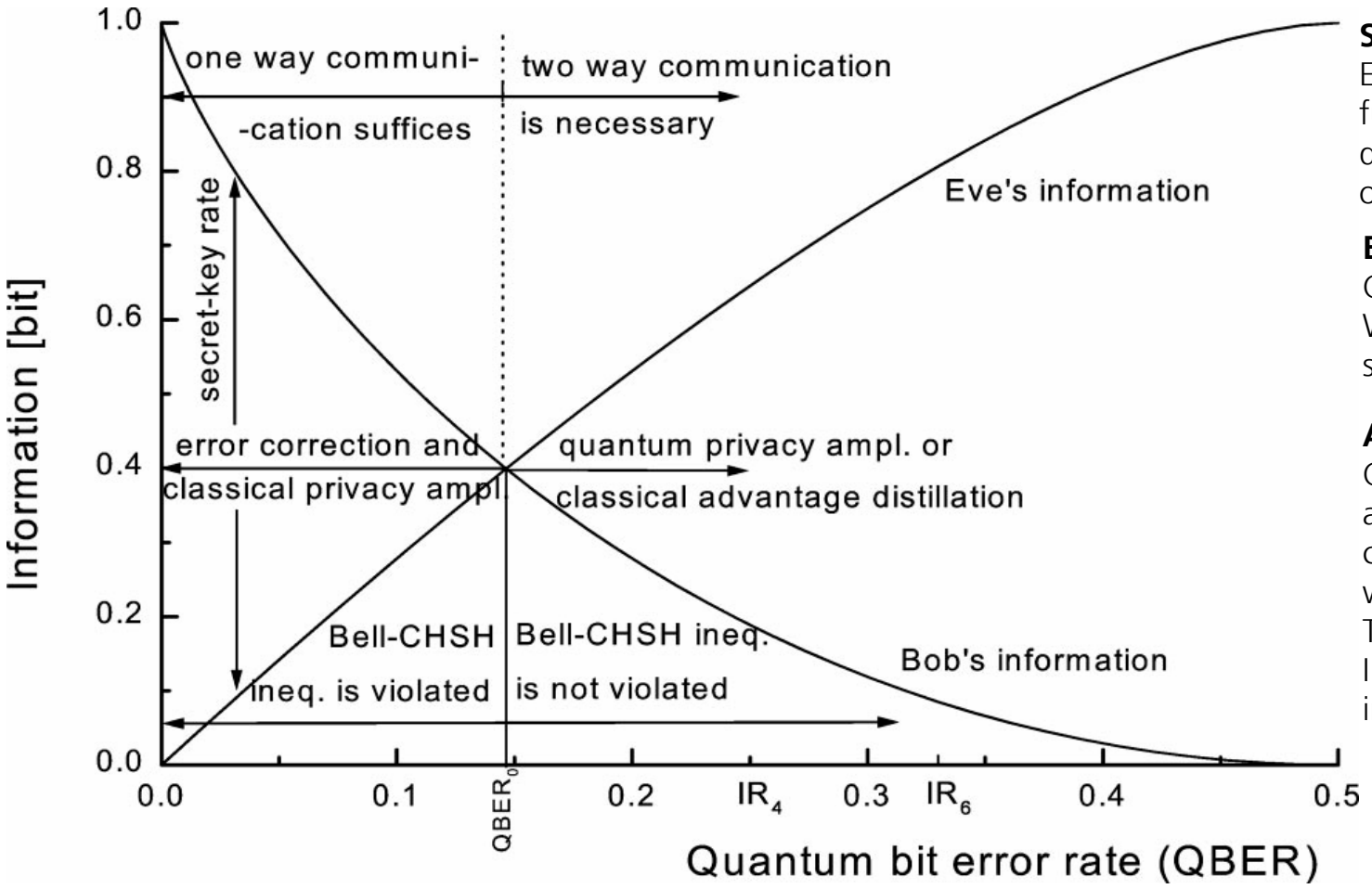
Fundamental Attacks on and Principal Limitation of QKD

- Attacks due to **implementation weaknesses**, in particular **translucent eavesdropping** e.g. the **beam-splitting** or **photon number splitting attack**
- **Man-in-the-middle attack** fue to lack of authentication
- The always present **noise** in realistic quantum channels is ***indistinguishable by principle*** from the errors caused by eavesdropping – this limits intrusion detection

Additional steps taken in realistic QKD Protocols: Key-Distillation

- **Error Correction:** classical protocols for bit-error correction (checksums, binary search, ...)
- **Privacy Amplification:** classical protocols for the reduction of Eve's information about the at first only ***partially secret*** raw key (block parities, Bennett et al., 1988, 1995)
- **Advantage distillation:** Less efficient protocols that use two-way communication over a classical, authenticated channel. The become necessary if Eve has too much information
- **Quantum privacy amplification** uses ***entangled*** quantum states

Security Analysis for BB84



Security of QKD protocols:
Eve'*s Information is limited as a function of the resulting quantum Bit error rate **QBER** of the raw key

Below the threshold $QBER_0$:
Classical error correction and PA With one-way communication suffice for effective QKD

Above $QBER_0$:
Classical error correction can be augmented by quantum PA and/or classical advantage distillation, which require two-way communication. This is possible up to certain thresholds IR_4, IR_6 for the intercept-resend strategy in BB84 with 4 (6) states.

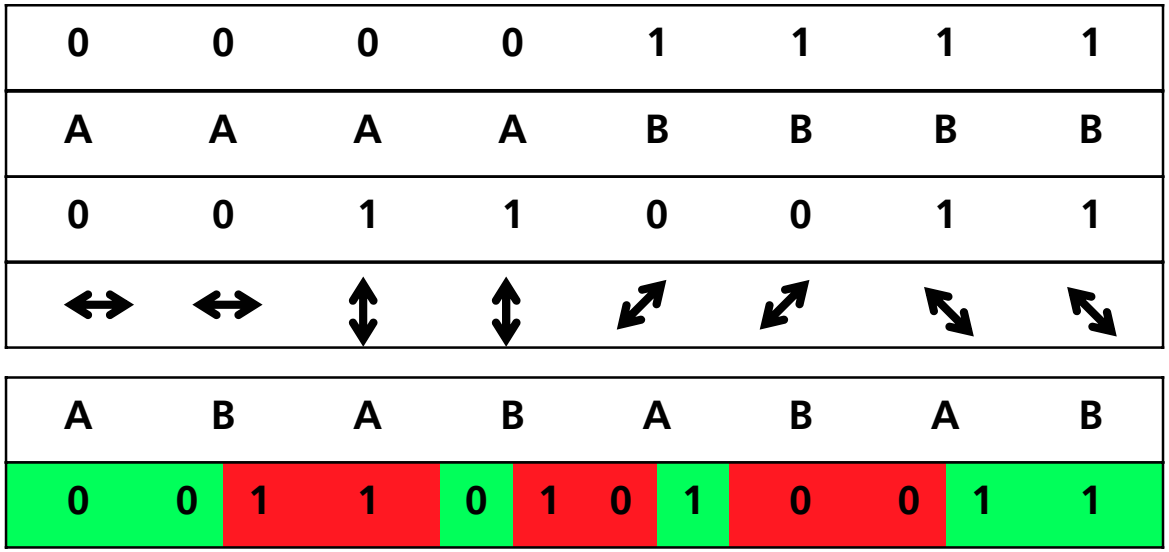
Source: Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden: *Quantum Cryptography*, Rev. Modern Phys. 74 (2002) 145

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

The Bit-Commitment Problem

I. The BB84 Protocol for the concealed escrow of Information



Alice chooses a sequence of Bits to be escrowed with Bob

And chooses the coding alphabets ***according to the Bit values***

She chooses a (different from what is shown) ***random*** sequence of con-Trol Bits and codes them in the cho-sen alphabets

Indifferent from which measurement Base Bob chooses (at random)... Measured Bit value and escrow co-Incide in 50% of all cases, that is They are completely **uncorrelated** – Concealment is achieved

In the **disclosure phase,** Alice sends the escrowed Bits
And the random control Bits over a classical channel to Bob.

Would she change her commitment, i.e. lie about an escrowed Bit, then Bob would detect this, since his meas-urement result would be physically impossible in 50% of all cases – the protocol is **secure against cheating**...

At least as long Alice uses only ***classical strategies***...

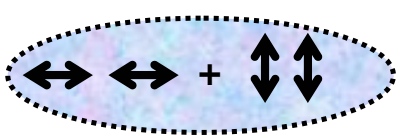
Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

The Bit-Commitment Problem

II. Entangled States Allow Alice to Cheat

Alice uses ***two entangled*** photons and the **superposition principle** for her fraud

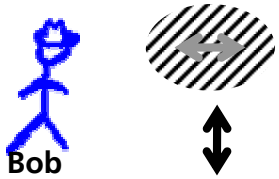


Alice

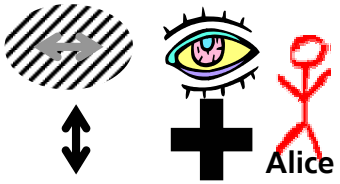
Alice prepares a symmetric Superposition of two photons

She sends ***one*** of them to Bob as her escrow and retains the other

Alice wants to disclose a **1**, that is, credibly assert that she used alphabet **A** to code the sent photon



Through Alice's measurement, the superposition is destroyed on ***both*** sides and the photons now have the same polarisation – with equal probability 50% **0**(**A**) or **1**(**A**)

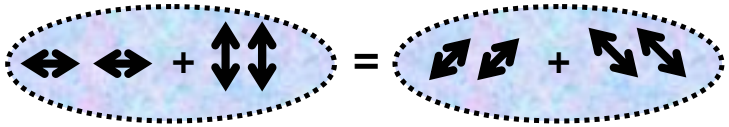


To that end, she measures her photon in basis **A**

She sends her result as **alleged control bit**

If Bob measures in **A**, he obtains **1** at 100%, if he measures in **B**, **0** or **1** at 50% – exactly as if Alice had used **A** to code **1**, as alleged

If Alice wants to disclose a **0** she uses basis **B** and the Identity



Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

The Bit-Commitment Problem

III. Quantum Bit-Commitment is impossible!

Several authors tried to fix the problem by reffining the protocol, for example BC91 (Brassard, Crépeau), BCJL93 (Brassard, Crépeau, Jozsa, Langlois).

But 1996 Lo und Chau, as well as Mayers independently showed the impossibility Of quantum Bit-commitment:

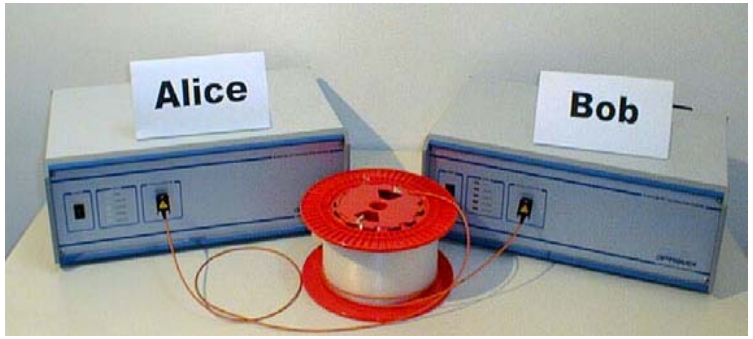
**If Alice's escrowed information is concealed from Bob,
that is, Bob has no possibility to uncover it
before the disclosure phase,
then Alice has always a possibility for cheating,
that is, to choose the committed bit value
at her discretion at disclosure time.**

Some Further Methods of Quantum Cryptography

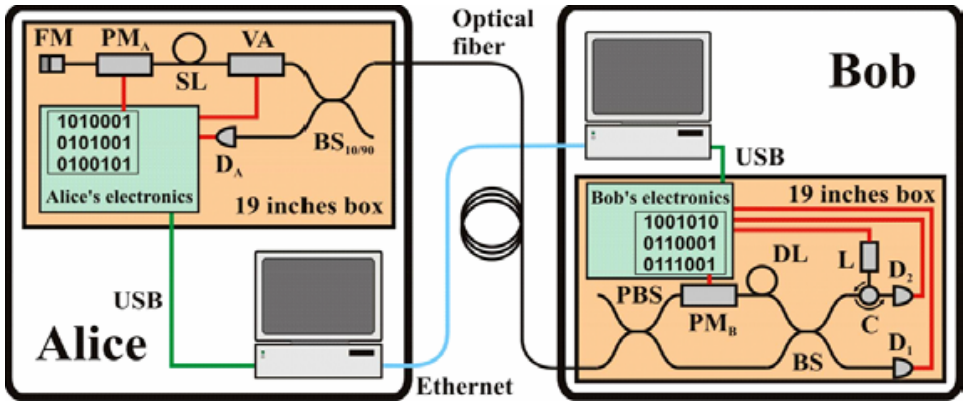
- **Entangled (EPR) states:** An alternative QKD Protocol (Ekert 1991), where a source generates maximally entangled pairs of states and distributes them to Alice und Bob. Security is based on Bell's inequality.
- **Quantum repeater**, based on **entanglement purification**, allow for QKD with theoretically unlimited range (Dür, Briegel, Cirac, Zoller 1999)
- The **Ping-Pong Protokoll** (Weinfurter et. al. 2002; Boström, Felbinger 2002) uses EPR-Pairs for ***direct, secure transmission of information***
- **Quantum encryption:** The encryption of q***uantum information*** with ***classiscal*** cryptography uses optimally 2 Bits per Qubit (Ambainis, Mosca, Tapp, de Wolf 2000) – **quantum one-time-pad**
- **Quantum authentication:** Authentication of quantum information ***requires ist encryption*** (Barnum, Crépeau, Gottesman, Smith, Tapp 2002). This entails: ***Signatures of quantum information are impossible***, since every protocol, that allows a receiver to read a quantum message, also allows him ist undetected manipulation
- **Quantum signatures:** The authentication of ***classcal*** Information methods of quantum cryptography is possible using a quantum-Notary, and accomplishes ***mutual non-repudiation*** – weder Alice nor Bob can alter the message, nor decline ist receipt (Zeng, Keitel 2002)
- **Countermeasures for attack scenarios:** E. g. sending of **decoy pulses** counteracts photon-number-splitting attacks (Hwang 2003)
- **Continuous variables** allow for higher transmission rates and lower error rates in realistic QKD models (u.A.: Cerf 2000; Gottesman, Preskill 2001; Grosshans, Grangier 2002)

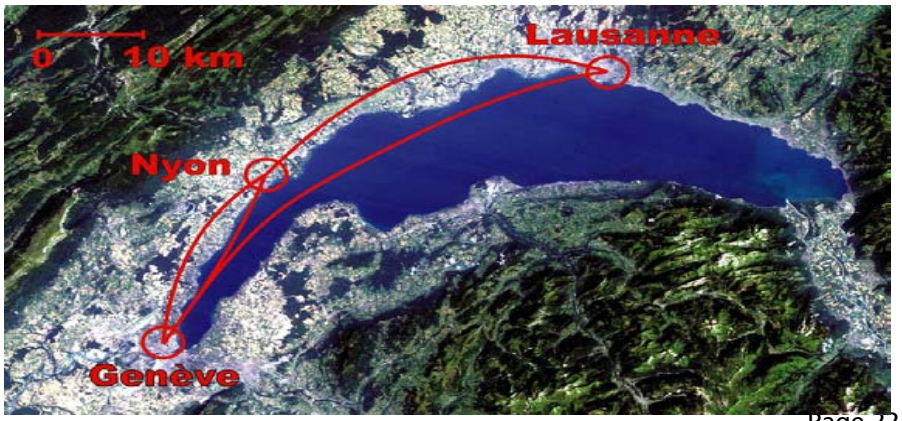
Two Real Existing Implementations 2002/3

N Gisin, G. Ribordy, H. Zbinden et. al. of the unviersity Geneva accomplished in summer 2002 with a self-correcting **plug&play s**ystem QKD (with **phase coding**) over distances of up to **67 km** on standard optical fibres. Their spin-off **id Quantique** markets this system commercially for approx. €80000 per piece. (current range record: **100 km**, Toshiba Research Europe, UK, May 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





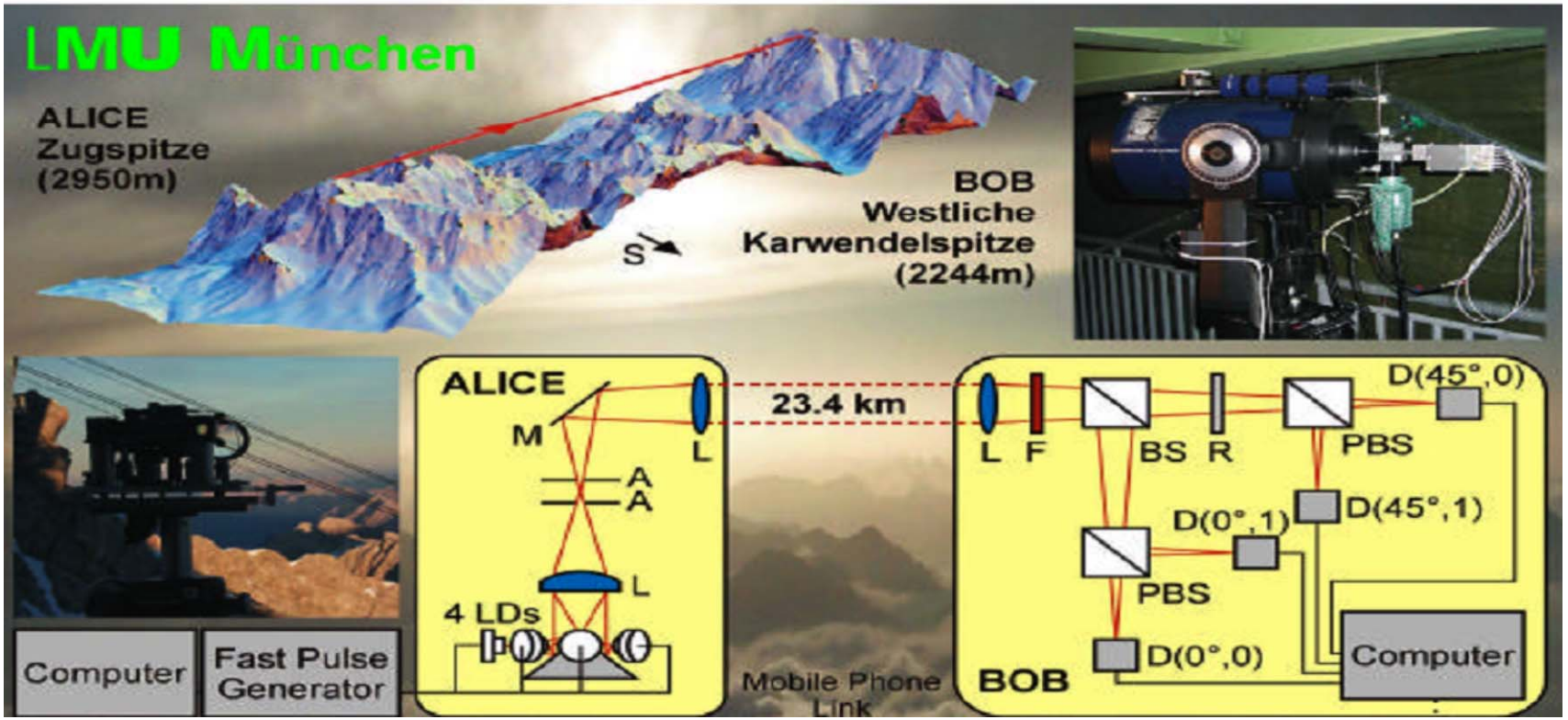
Source: New. J. Phys. **4** (2002) 41

Fraunhofer SIT Institut Sichere Telekooperation

Competence Center For Applied Security Technology CAST

Two Real Existing Implementations 2002/3

Ch. Kurtsiefer and H. Weinfurter (LMU Munich) realised in September 2002 QKD over 23,4 km **free air distance**, with polarised photons at approx. 1kBit/s raw key rate (within the EU-Project EQCSPOT, in collaboration with DERA/Qinetiq)



Source: Einsichten 1/2003. Magazin der Universität München

Fraunhofer SIT Institut Sichere Telekooperation

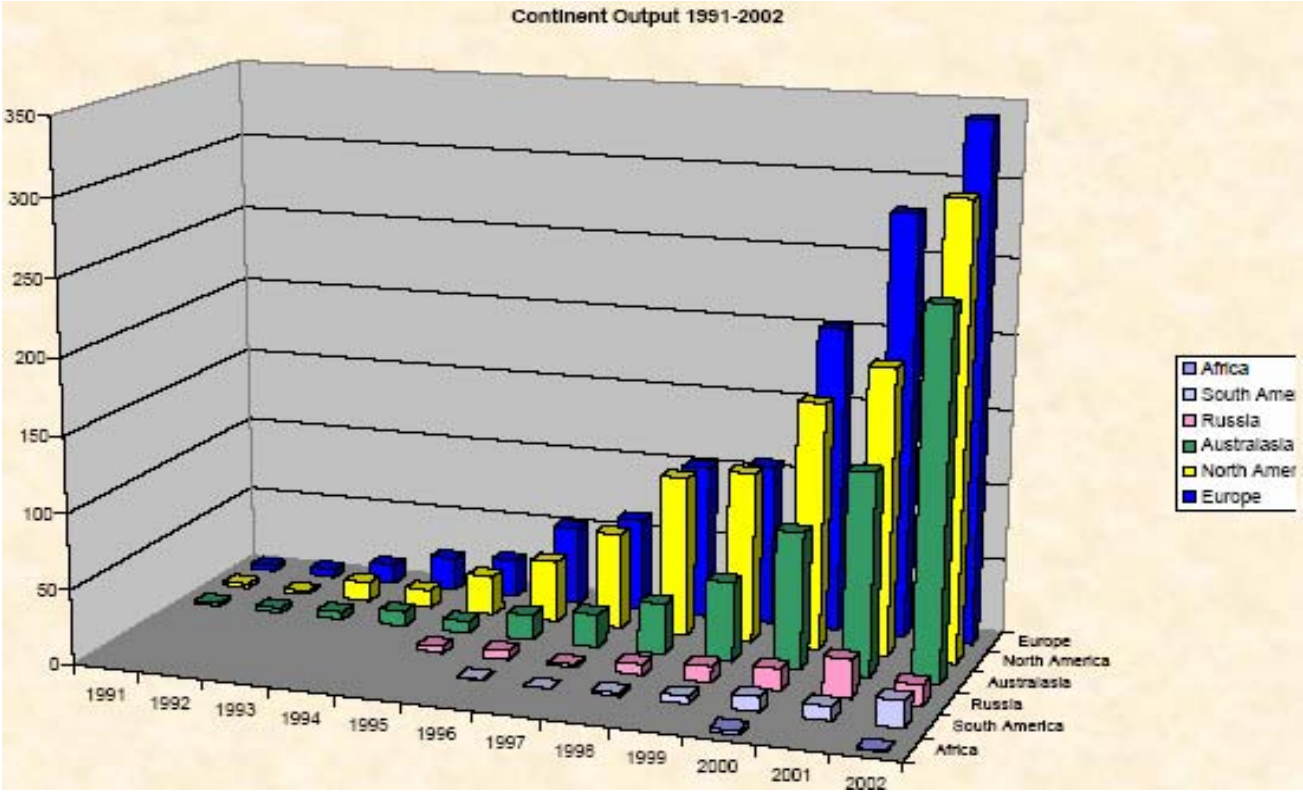
Competence Center For Applied Security Technology CAST

Reasearch in QI and QCr in EU, USA and Worldwide

- **DARPA** program on quantum informatics (QuIST) **100 M$** over 5 years from 2002 (Source: www.darpa.mil)
- **EU FP5**: approx. **30 M€** in the FET Proactive Initiave „Quantum Information Processing & Communication“ (QIPC) plus approx. **5 M€** in FET OPEN, in approx. 20 projects from 1998 to 2003 (Source: cordis.lu)
- **EU FP6:** Probably similar budget in up to now approx.12 projects

Publications in the compund area of quantum information by continent

(Source: QUIPROCONE)

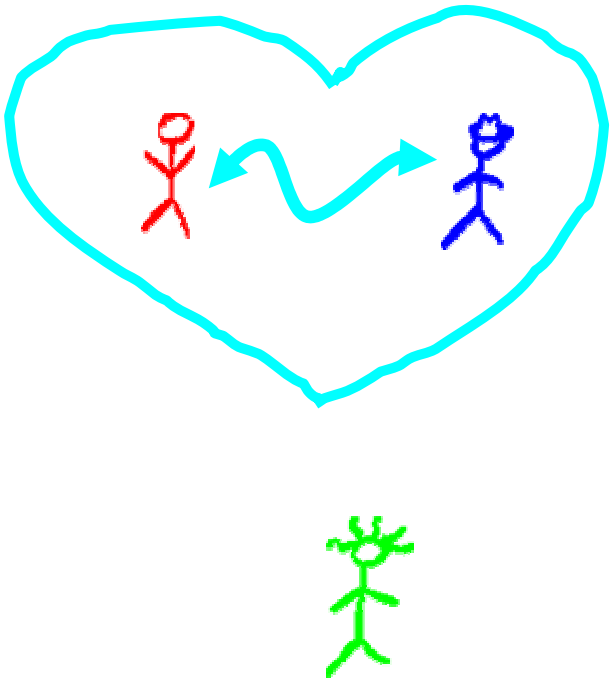


Fraunhofer SIT Institut Sichere Telekooperation

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-Resources

- Slides of this talk on the Homepage of the author: http://www.math.uni-frankfurt.de/~aschmidt/paper/cast_qcrypt_en.pdf
- id Quantique http://www.idquantique.com
- MagiQ Technologies http://www.magiqtech.com
- DARPA Programme 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 Project „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 Project „Entanglement in Quantum Information Processing and Communication“ (EQUIP) http://www.equip.qipc.org and its follow-up „Quantum Properties of Distributed Systems“ (QUPRODIS) http://www.quprodis.org
- EU Project „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
- Experimenal quantum physics at the LMU Munich http://xqp.physik.uni-muenchen.de/

Literature

- 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