Chapter 13: Photons for quantum information

Quantum only tasks

- Teleportation
- Superdense coding
- Quantum key distribution

Quantum teleportation

(Theory: Bennett et al. 1993; Experiments: many, by now)

Teleportation = some kind of disembodied transport. (S.L. Braunstein 1995)

Only information (not matter) is transferred to another location, such that the state of a quantum system can be reconstructed (not copied) perfectly.

If Alice and Bob own two identical quantum systems they can try to transfer the quantum state of Alice's system to Bob's system:

$$|\psi\rangle_A \otimes |\text{something}\rangle_B \longrightarrow |\text{something else}\rangle_A \otimes |\psi\rangle_B$$

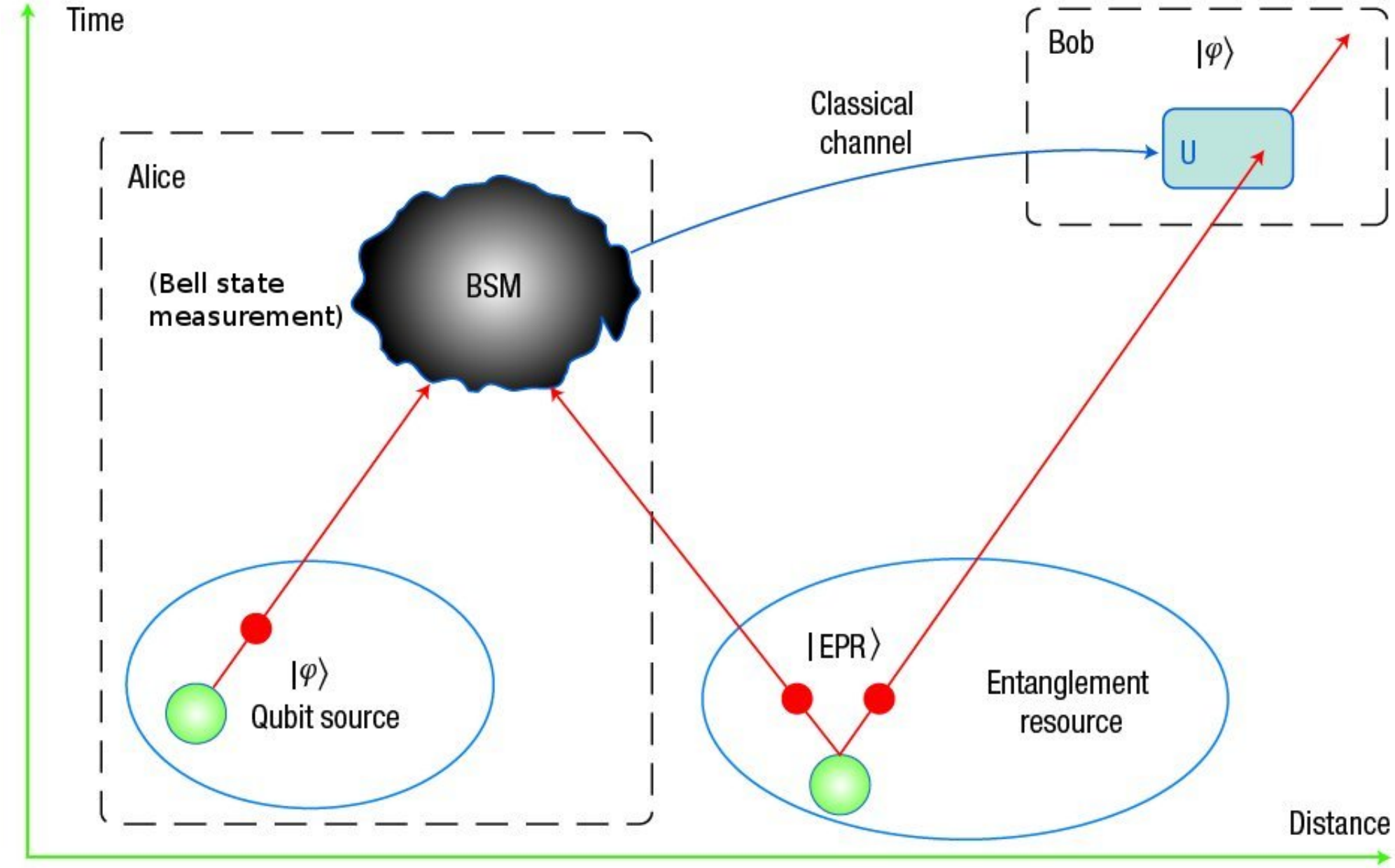


Figure 4 Quantum teleportation. Alice performs a BSM, a joint measurement, on the unknown qubit $|\varphi\rangle$ and one photon from the entangled state $|EPR\rangle$. The result does not reveal the state of the qubit, but is sent to Bob, who performs a result-dependent operation U to complete the teleportation.

from N. Gisin and R. Thew, Nature Photonics **1**, 165 (2007)

The simplest system is a qubit, in a state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

(with unkown α and β).
Alice and Bob also need a shared pair of qubits in a Bell state (an EPR pair)

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Initial state of the combined three-qubit system:

$$|\chi\rangle := |\psi\rangle|\phi\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right].$$

Alice applies CNOT(1,2) followed by a Hadamard gate $\mathbf{H}_1$ acting on the first qubit.
This entangles $|\psi\rangle$ with $|\phi\rangle$:

$$|\tilde{\chi}\rangle = \mathbf{H}_1 \text{ CNOT } (1,2)|\chi\rangle = \mathbf{H}_1\frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\right]$$

$$= \frac{1}{2}\left[\alpha(|0\rangle+|1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle-|1\rangle)(|10\rangle + |01\rangle)\right].$$

We rewrite this state in order to see clearly what has happened on Bob's end of the EPR pair

$$|\tilde{\chi}\rangle = \frac{1}{2}\left[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right]$$

$$= \frac{1}{2}\left[|00\rangle|\psi\rangle + |01\rangle\mathbf{X}_3|\psi\rangle + |10\rangle\mathbf{Z}_3|\psi\rangle + |11\rangle\underbrace{(-i\mathbf{Y}_3)}_{\mathbf{X}_3\mathbf{Z}_3}|\psi\rangle\right] = \frac{1}{2}\sum_{M_1=0}^{1}\sum_{M_2=0}^{1}|M_1M_2\rangle\mathbf{X}_3^{M_2}\mathbf{Z}_3^{M_1}|\psi\rangle$$

$\mathbf{X}_3$, $\mathbf{Y}_3$, and $\mathbf{Z}_3$ are the Pauli matrices applied to the qubit 3 (Bob's qubit).

Bob's state: a superposition of four distorted variants of Alice's original state.

Alice now measures the states of her two qubits. $\rightarrow$ one of the four combinations $|M_1 M_2\rangle$. The state of the complete system has collapsed to

$$|M_1 M_2\rangle \mathbf{X}_3^{M_2} \mathbf{Z}_3^{M_1} |\psi\rangle$$

Bob now possesses a definite modification of the desired state $|\psi\rangle$, but he does not yet know which one!

Alice tells Bob the two measured classical bits (M_1, M_2), Bob applies to his qubit the operator

$$\mathbf{Z}_3^{M_1} \mathbf{X}_3^{M_2} = (\mathbf{X}_3^{M_2} \mathbf{Z}_3^{M_1})^{-1}$$

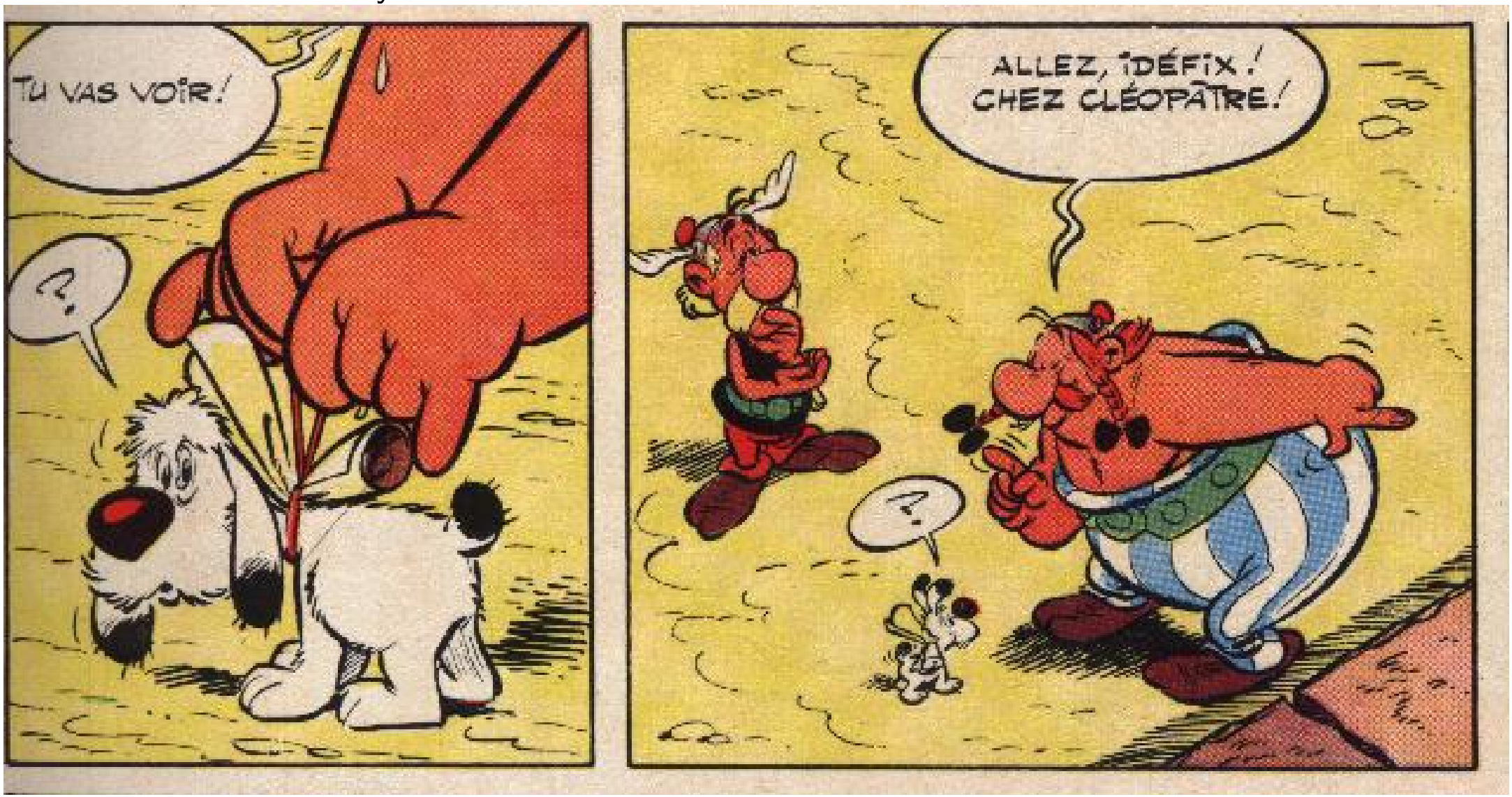
and can enjoy the state $|\psi\rangle$ which he now owns, while Alice's original qubit is in the state $|M_1\rangle$.

Note: No spooky action at a distance since the classical transmission of measurement results between Alice and Bob obeys the Einstein speed limit c.

Secure quantum communication

(Theory: Bennett and Brassard 1984; Experiments: many, by now)

Data transmission always was a matter of confidence:



Even in Cleopatra's times, however, people rather relied on cryptography.

Secure communication with a one-time pad

Symmetric key: all communication partners (and only they) have identical copies of the key.

Beispiel: Alice wants to tell Bob her date of birth:

Alice's message	2	1	1	2	8	2
...binary	0010	0001	0001	0010	1000	0010
Alice's key	0101	1101	1001	1110	0011	1011
encrypted text	0111	1100	1000	1100	1011	1001
Bob's key	0101	1101	1001	1110	0011	1011
decrypted text	0010	0001	0001	0010	1000	0010
decimal	2	1	1	2	8	2

Encryption *and* decryption by bitwise addition without carry ($\oplus$) according to the rules

$0 \oplus 0 = 0 \quad 0 \oplus 1 = 1$

$1 \oplus 1 = 0$

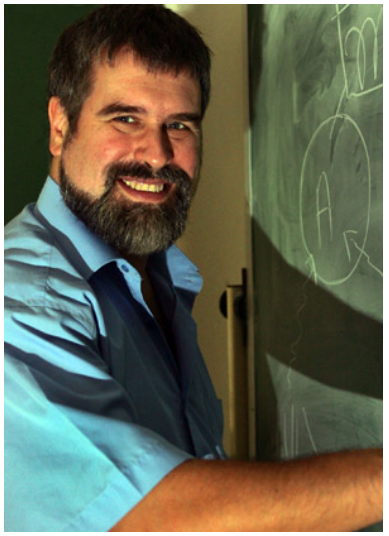
The key is a purely random bit string which masks all structure in the original message. It must be discarded after use, because otherwise evil Eve, the eavesdropper, can get a handle on the message.

The one-time pad is the only mathematically provably secure encryption method.

Drawbacks: persistent need for fresh key; key distribution is risky $\rightarrow$ quantum key distribution (QKD).

The BB84 protocol

Alice and Bob protect their privacy by the protocol introduced by Charles H. Bennett (r.) and Gilles Brassard(l.) at a conference in Bangalore in 1984 (!). With that "BB84" protocol they can securely share a one-time key .



Alice's shopping list

- 1 photon source, with
- 4 polarization filters: $\uparrow, \rightarrow, \nearrow, \nwarrow$ and
- 1 random number generator

Bob's shopping list

- 1 photon detector, containing
- 2 polarization filters: $\uparrow, \nearrow$
- 1 random number generator

Starting at a previously fixed time, Alice transmits, say, 2000 photons. Bob knows exactly when to expect each photon.

Alice chooses the polarization ($\uparrow, \rightarrow, \nearrow, \nwarrow$) of the transmitted photons completely randomly. Bob also switches completely randomly between the two polarization filters in his detector. Both of them keep records of their random sequences.

Depending on the polarization of the photon and the orientation of Bob's filter the reaction of Bob's detector is either predictable or random:

photon (A)	filter (B)	detector
↑	↑	1
→	↑	0
↗	↑	50/50
↖	↑	50/50
↑	↗	50/50
→	↗	50/50
↗	↗	1
↖	↗	0

Bob does not know which of Alice's 2000 photons he has identified correctly until Alice tells him which photon pair ("basis") she has used for each of the 2000 photons transmitted: „+"=(↑, →) or „x"=(↗, ↖). Bob tells her the orientation of his polarization filter in each case.

After that, both of them (plus all eavesdroppers) know which of Alice's photons have been identified correctly by Bob. The results of that identification are known only to Alice and Bob and constitute roughly 1000 bits of key:

photon (A)	↑	↗	↖	↑	↑	→	↖	→	↑	→
filter (B)	↑	↗	↗	↗	↑	↗	↑	↑	↗	↑
detector (B)	1	1	0	0	1	1	0	0	0	0
basis (A)	+	x	x	+	+	+	x	+	+	+
key (A,B)	1	1	0		1			0		0

What about Eve?

Eve could
- buy the same equipment as Alice and Bob,
- intercept Alice's photons and measure them in the way Bob does,
- transmit "forged" photons to Bob.

Eve's problem:
She does not know which polarization filter ($\uparrow$ oder $\nearrow$) Bob uses until it is too late.
$\Rightarrow$ In 50% of all cases she uses a filter different from Bob's and thus sends him a photon with a polarization mismatch (of 45°) to Bob's filter. Due to the 45° angle half of these "wrong" photons are nevertheless registered "correctly".
$\Rightarrow$ Error rate of 25% in the key.

Alice's and Bob's espionage protection:
Draw 100 bits from the key randomly and compare them publicly. Probability that all 100 bits are equal although Eve generates 25% errors:

$$\left(\frac{3}{4}\right)^{100} = 3 \cdot 10^{-13}$$

Eve does not go unnoticed.

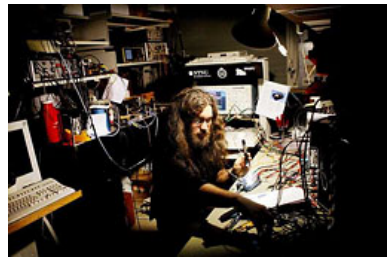
...or does she?

1 January 2010, 10:05 « previous | r

26C3: Researchers demonstrate brilliant quantum hack

31.12.2009 15:58 heise Security « Vorig

26C3: Forscher demonstrieren genialen Quanten-Hack



DON'T PANIC Quantum Mechanics is still valid.

Imperfections of existing hardware are used to perform an intercept and resend attack, as in some previous studies intended to make quantum key distribution safer.

The quantum hacking group at NTNU Trondheim: http://www.iet.ntnu.no/groups/optics/qcr/

Index to focus issue on quantum cryptography: New Journal of Physics **11**, 045005 (2009)

Details underlying this particular hack: V. Makarov, *Controlling passively quenched single photon detectors by bright light*, New Journal of Physics **11**, 065003 (2009).

Eve's scheme

Eve could
- buy the same equipment as Alice and Bob,
- intercept Alice's photons and measure them in the way Bob does,
- transmit "forged" photons to Bob.

Eve's problem:
She does not know which polarization filter ($\uparrow$ oder $\nearrow$) Bob uses until it is too late.

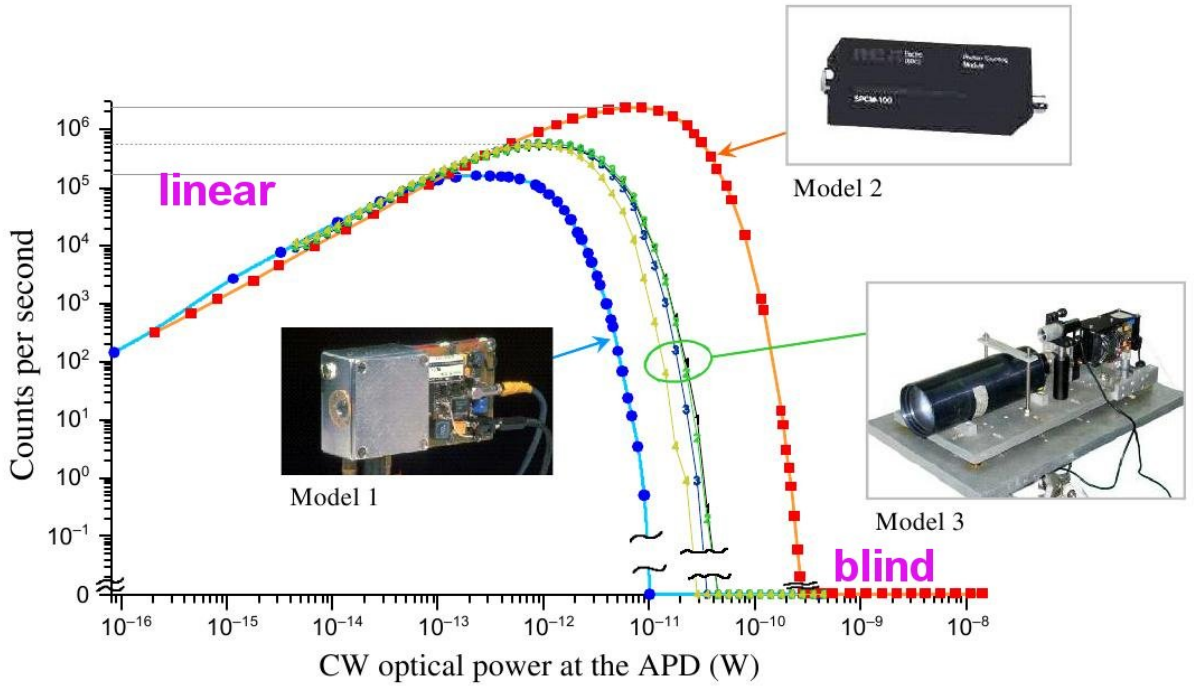
Eve's solution:
She manipulates Bob's detectors so that Bob's measurement is exactly equal to her own measurement, including his polarization filter setting.

From the abstract of Makarov's paper:

Single photon detectors (SPDs) based on passively quenched avalanche photodiodes can be temporarily blinded by relatively bright light...
....all SPDs in the receiver Bob are uniformly blinded by continuous illumination coming from the eavesdropper Eve. When Eve needs a certain detector in Bob to produce a click, she modifies the polarization (or other parameters used to encode quantum states) of the light she sends to Bob such that the target detector stops receiving light, while the other detector(s) continue to be illuminated. The target detector regains single photon sensitivity and, when Eve modifies the polarization again, produces a single click. Thus, Eve has full control of Bob...

More on Eve's scheme

The basis:
detector characteristics
(adapted from Makarov, op. cit.)



How does Eve know which polarization basis Bob is about to use for measurement?

She does not know, and does not have to know!

The trick: Eve does not send a single photon, but a carefully manipulated light pulse, based on her own choice of basis and result of measurement:

- Bob's basis = Eve's basis $\Longrightarrow$ One of Bob's detectors clicks, if Eve's corresponding detector has clicked.

- Bob's basis $\neq$ Eve's basis $\Longrightarrow$ All of Bob's detectors remain blinded and do not click.