Can Two-Way Direct Communication Protocols Be Considered Secure?

Mladen Pavičić

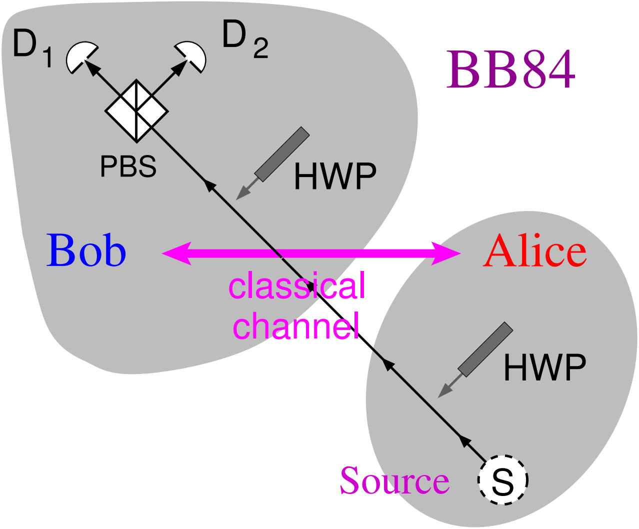
Center of Excellence for Advanced Materials and Sensors (CEMS), Research Unit *Photonics and Quantum Optics*, *Institute Ruđer Bošković (IRB)*, Zagreb, Croatia.

Nano Optics, Department of Physics, Humboldt University (HU), Berlin, Germany.

EMN Meeting on Quantum, June 18-22, 2017, Vienna, Austria.

EMN Quantum-2017

Quantum Cryptography, QKD, BB84 Protocol



Direct Two-Way Communication with Entangled Pairs of Photons in Bell States

Linear optics:

Two Bell States, $|\Psi^{\mp}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 \mp |V\rangle_1|H\rangle_2)$, *Ping-Pong* Protocol.

Kim Boström and Timo Felbinger, Deterministic Secure Direct Communication Using Entanglement, *Phys. Rev. Lett.*, **89**, 187902 (2002).

Direct Two-Way Communication with Entangled Pairs of Photons in Bell States

Linear optics:

Two Bell States, $|\Psi^{\mp}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 \mp |V\rangle_1|H\rangle_2)$, *Ping-Pong* Protocol.

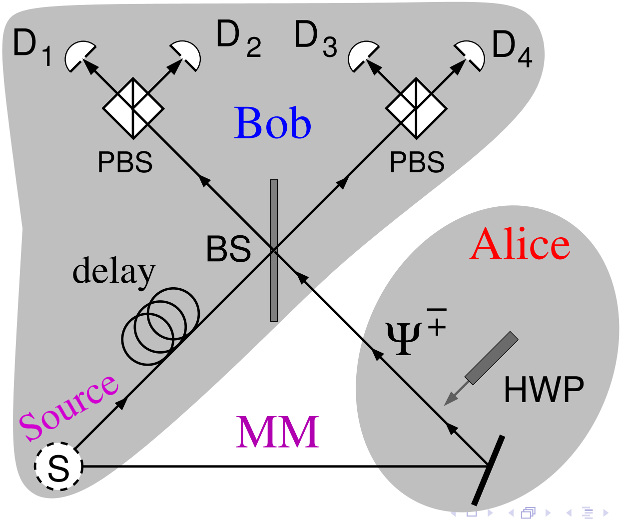
Kim Boström and Timo Felbinger, Deterministic Secure Direct Communication Using Entanglement, *Phys. Rev. Lett.*, **89**, 187902 (2002).

Non-linear optics:

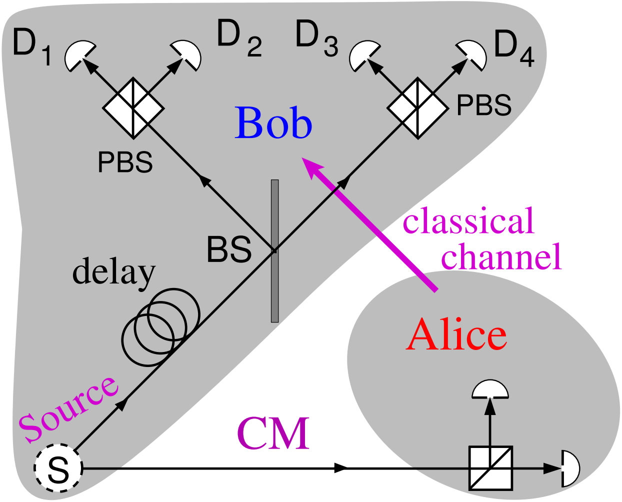
Four Bell States, $|\Psi^{\mp}\rangle$, $|\Phi^{\mp}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 \mp |V\rangle_1|V\rangle_2)$.

Quing-yu Cai and Ban-wen Li, Improving the Capacity of the Boström-Felbinger Protocol, *Phys. Rev. A*, **69**, 054301 (2004).

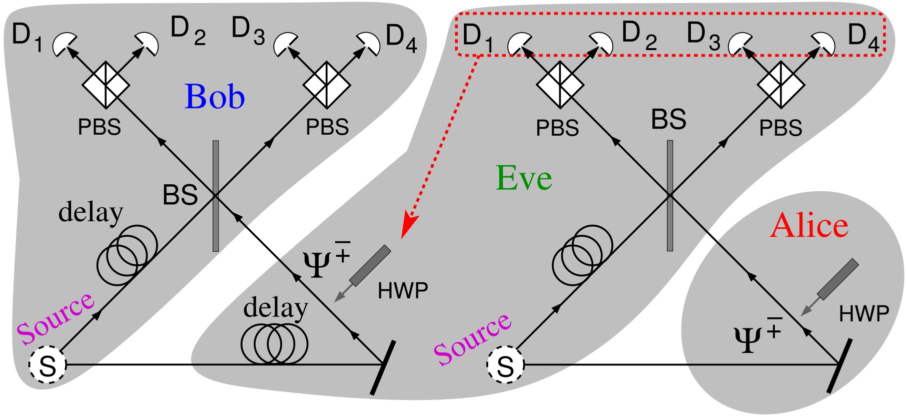
Direct Quantum Communication, QKD, Ping-Pong Protocol; Message Mode (MM)



Direct Quantum Communication, QKD, Ping-Pong Protocol; Control Mode (CM)



Nguyen's Attack on Ping-Pong Protocol, Nguyen, B.A., *Phys. Lett. A*, **328**, 6 (2004).



Undetectable Eve copies all messages in MM (msg. mode)

Direct Two-Photon Communication with Single Photons

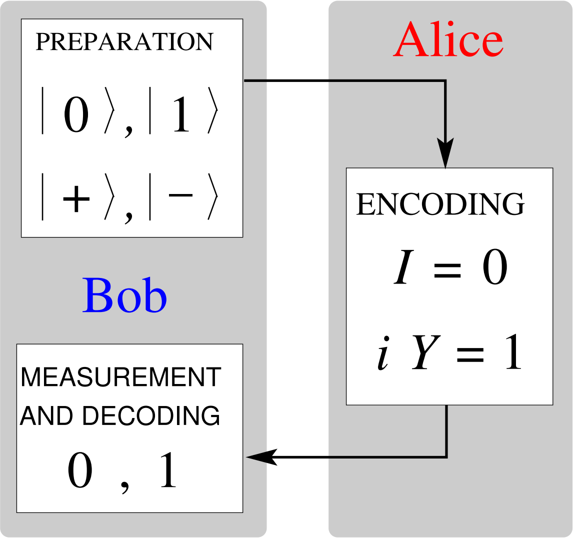
Linear optics:

Single photon states, in two bases ($\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$) as in the BB84 protocol

Marco Lucamarini,
Quantum Decoherence and Quantum Cryptography,
PhD Thesis, *University of Rome La Sapienza*, 2003,
http://sapienzadigitallibrary.uniroma1.it/identifier/RMSFI_00000130

Marco Lucamarini and Stefano Mancini,
Secure Deterministic Communication without Entanglement,
Phys. Rev. Lett., **94**, 140501 (2005)

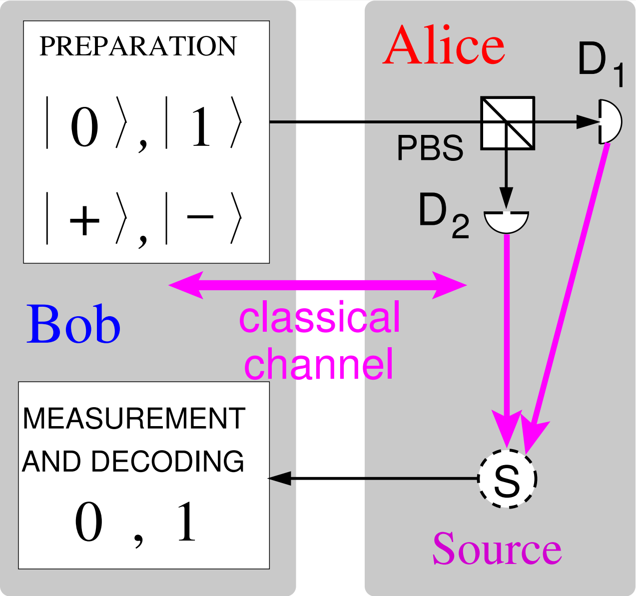
Lucamarini-Mancini Protocol—LM05—Message Mode



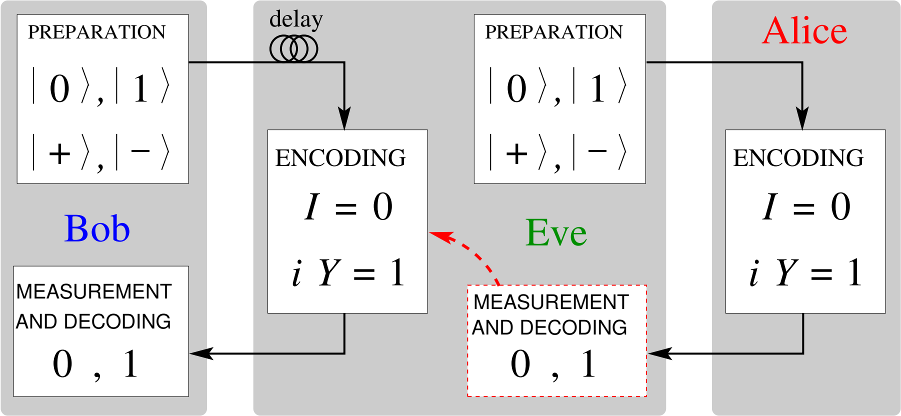
$$I|0\rangle = |0\rangle$$
$$I|1\rangle = |1\rangle$$
$$I|+\rangle = |+\rangle$$
$$I|-\rangle = |-\rangle$$

$$iY|0\rangle = -|1\rangle$$
$$iY|1\rangle = |0\rangle$$
$$iY|+\rangle = |-\rangle$$
$$iY|-\rangle = -|+\rangle$$

Lucamarini-Mancini Protocol—LM05—Control Mode



Lucamarini's Attack on LM05, Lucamarini,M., PhD Thesis, *University of Rome La Sapienza* (2003); p. 61, Fig. 5.5,



Undetectable Eve copies all messages in MM (msg. mode)

Alice-Bob and Alice-Eve Mutual Information

Security of a protocol, critical QBER via secret fraction

$r = \lim_{N\to\infty} \frac{l}{n} = I_{AB} - I_{AE}$

l = length of the final key, n = length of the raw key,
I_{AB}, I_{AE} = Alice-Bob, Alice-Eve mutual information

Alice-Bob and Alice-Eve Mutual Information

Security of a protocol, critical QBER via secret fraction

$r = \lim_{N\to\infty} \frac{l}{n} = I_{AB} - I_{AE}$

l = length of the final key, n = length of the raw key,
I_{AB}, I_{AE} = Alice-Bob, Alice-Eve mutual information

In BB84—D = disturbance in MM:
$I_{AB} = 1 + D\log_2 D + (1-D)\log_2(1-D)$,
$I_{AE} = -D\log_2 D - (1-D)\log_2(1-D)$

Alice-Bob and Alice-Eve Mutual Information

Security of a protocol, critical QBER via secret fraction

$r = \lim_{N\to\infty} \frac{l}{n} = I_{AB} - I_{AE}$

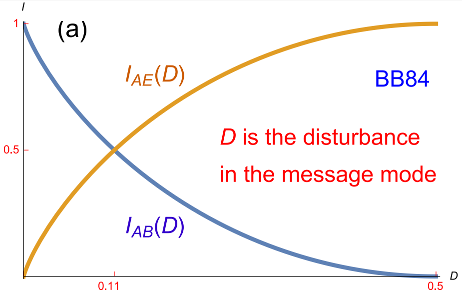
l = length of the final key, n = length of the raw key,
I_{AB}, I_{AE} = Alice-Bob, Alice-Eve mutual information

In BB84—D = disturbance in MM:
$I_{AB} = 1 + D\log_2 D + (1-D)\log_2(1-D)$,
$I_{AE} = -D\log_2 D - (1-D)\log_2(1-D)$

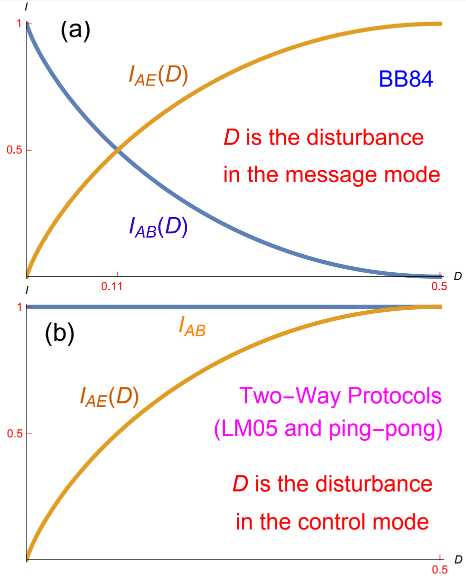
In two-way protocols—D = disturbance in CM:
$I_{AB} = 1$,
$I_{AE} = -D\log_2 D - (1-D)\log_2(1-D)$

In MM D = presence of Eve;
$D = 0$—Eve is absent; $D = 0.5$ (max disturbance)—Eve is always present.

BB84 has a critical *D*—2-way protocols do not



BB84 has a critical D—2-way protocols do not



Proofs of security of two-way protocols

Han, Y.-G. et al., Security of Modified Ping-Pong Protocol in Noisy and Lossy Channel, *Sci. Rep.*, **4**, 4936 (2007).

Proofs of security of two-way protocols

Han, Y.-G. et al., Security of Modified Ping-Pong Protocol in Noisy and Lossy Channel, *Sci. Rep.*, **4**, 4936 (2007).

Lu, H., et al., Unconditional Security Proof of a Deterministic Quantum Key Distribution with a Two-Way Quantum Channel, *Phys. Rev. A*, **84**, 042344 (2011).

Proofs of security of two-way protocols

Han, Y.-G. et al., Security of Modified Ping-Pong Protocol in Noisy and Lossy Channel, *Sci. Rep.*, **4**, 4936 (2007).

Lu, H., et al., Unconditional Security Proof of a Deterministic Quantum Key Distribution with a Two-Way Quantum Channel, *Phys. Rev. A*, **84**, 042344 (2011).

Both proofs are made for variable I_{AB} which depends on D and both proofs assume that Eve changes I_{AB}, while for the above attacks $I_{AB} = 1$.

Proofs of security of two-way protocols

Han, Y.-G. et al., Security of Modified Ping-Pong Protocol in Noisy and Lossy Channel, *Sci. Rep.*, **4**, 4936 (2007).

Lu, H., et al., Unconditional Security Proof of a Deterministic Quantum Key Distribution with a Two-Way Quantum Channel, *Phys. Rev. A*, **84**, 042344 (2011).

Both proofs are made for variable I_{AB} which depends on D and both proofs assume that Eve changes I_{AB}, while for the above attacks $I_{AB} = 1$.

Can privacy amplification work without a critical D in MM?

Proofs of security of two-way protocols

Han, Y.-G. et al., Security of Modified Ping-Pong Protocol in Noisy and Lossy Channel, *Sci. Rep.*, **4**, 4936 (2007).

Lu, H., et al., Unconditional Security Proof of a Deterministic Quantum Key Distribution with a Two-Way Quantum Channel, *Phys. Rev. A*, **84**, 042344 (2011).

Both proofs are made for variable I_{AB} which depends on D and both proofs assume that Eve changes I_{AB}, while for the above attacks $I_{AB} = 1$.

Can privacy amplification work without a critical D in MM?

With $I_{AB} = 1$ and max D, privacy amplification obviously cannot work.

Proofs of security of two-way protocols

Han, Y.-G. et al., Security of Modified Ping-Pong Protocol in Noisy and Lossy Channel, *Sci. Rep.*, **4**, 4936 (2007).

Lu, H., et al., Unconditional Security Proof of a Deterministic Quantum Key Distribution with a Two-Way Quantum Channel, *Phys. Rev. A*, **84**, 042344 (2011).

Both proofs are made for variable I_{AB} which depends on D and both proofs assume that Eve changes I_{AB}, while for the above attacks $I_{AB} = 1$.

Can privacy amplification work without a critical D in MM?

With $I_{AB} = 1$ and max D, privacy amplification obviously cannot work.

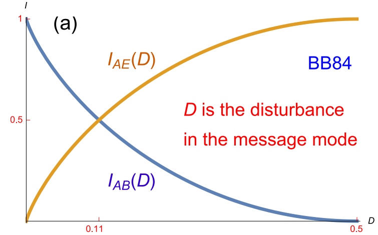
There is nothing in CM which can determine critical D for MM $\Longrightarrow$ the proof of unconditionally security of 2-way protocols cannot be valid.

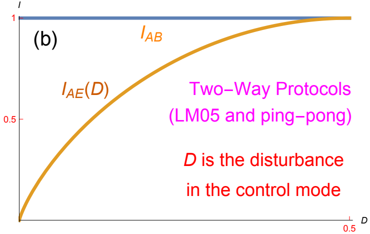
Can Two-Way Protocols Be Considered Secure?

There is no disturbance in the message mode (MM).

Disturbance D belongs to the control mode (CN)

MM and CM are completely disjoint and D from CM cannot have any influence on I_{AB} from MM—which is constant $I_{AB} = 1$.





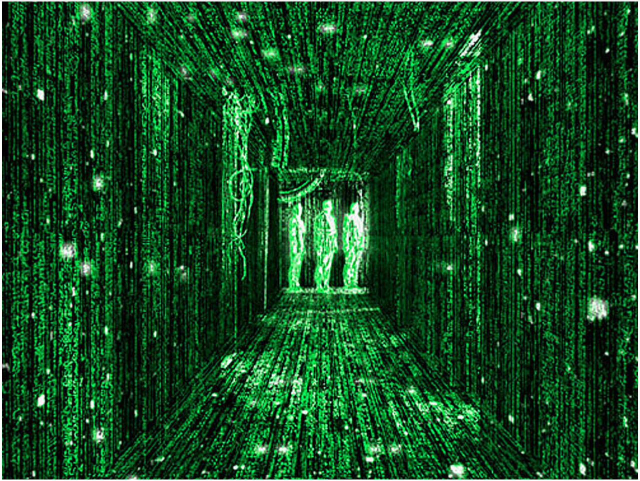
Privacy amplification cannot work when Eve is in the line all the time.

Can one find a level of Eve's presence—determined by D from CM—for which the privacy amplification would unconditionally work?

Acknowledgements 😎

The work is supported by the *Croatian Science Foundation* through project IP-2014-09-7515 and CEMS funding by the *Ministry of Science and Education of Croatia*.

Thanks for your attention 😎



http://cems.irb.hr/en/research-units/photonics-and-quantum-optics/
http://www.irb.hr/users/mpavicic/