Title: Distributed phase reference schemes for QKD: Explicit attacks and security considerations

Date: Jun 02, 2007 02:30 PM

URL: http://pirsa.org/07060011

Abstract: <div id="Cleaner">"Distributed phase reference schemes are a new class of protocols for Quantum Key Distribution, in which the quantum signals have overall phase-relationships to each other. This is expected to protect against some loss-related attacks. However, proving the full security of these schemes is a new challenge for theorists, as one can no longer identify individual signals (such as qubits in BB84, for instance), and so the security proof techniques do not apply directly.<div id="Cleaner"><div id="Cleaner">In this talk I will present two such protocols (the Differential Phase Shift and the Coherent One Way protocols). Their ""unconditionnal security"" has not been proven yet, but I will present some specific attacks on these schemes, which give us upper bounds for the security, as well as a ""feeling"" on how these schemes should perform."

Distributed Phase Reference schemes for QKD :

Explicit attacks and security considerations

Cyril Branciard

UNIVERSITÉ DE GENÈVE
FACULTÉ DES SCIENCES

Outline

- Distributed Phase Reference schemes
  2 examples : DPS & COW protocols

- Can we directly apply the standard methods to prove the security of these schemes ?

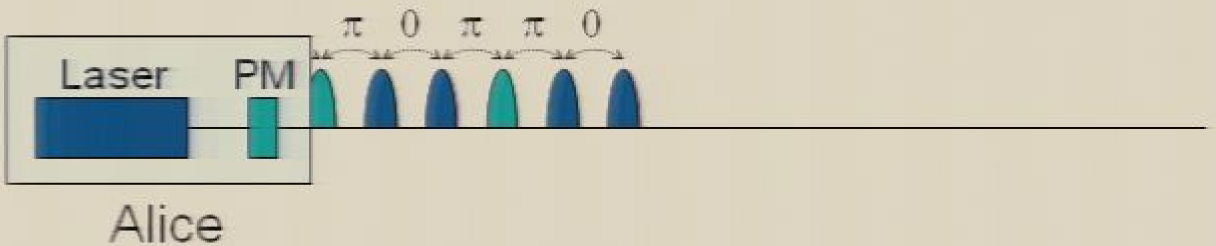
- Examples of explicit attacks :
  – Beam Splitting attack
  – New non-zero-error attacks

[Inoue, Waks, Yamamoto, PRA 68, 022317 (2003)]

Differential Phase Shift protocol

[Inoue, Waks, Yamamoto, PRA 68, 022317 (2003)]

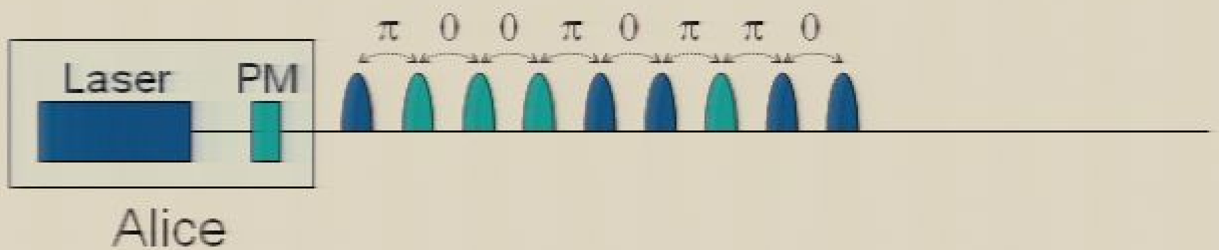
Differential Phase Shift protocol



- Alice sends a train of *wea*

[Inoue, Waks, Yamamoto, PRA 68, 022317 (2003)]

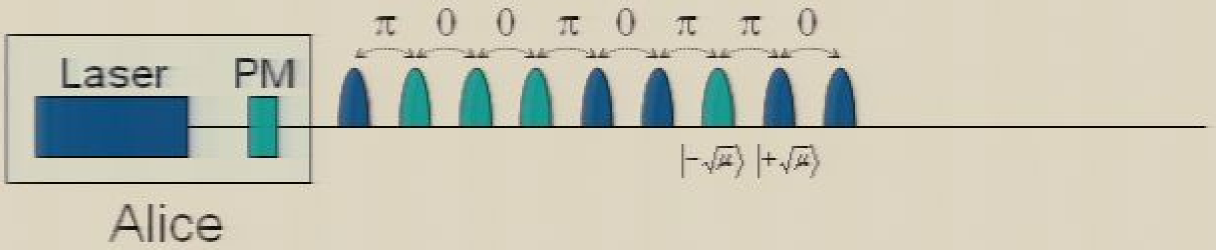
Differential Phase Shift protocol



- Alice sends a train of *weak coherent pulses*

[Inoue, Waks, Yamamoto, PRA 68, 022317 (2003)]

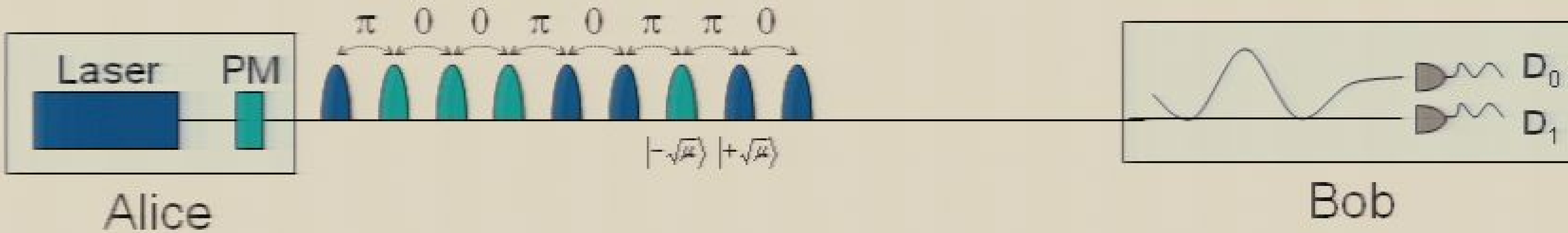
Differential Phase Shift protocol



- Alice sends a train of *weak coherent pulses* $\left|\pm\sqrt{\mu}\right\rangle$.
- The pulses have *overall phase relationships* (mode-locked laser); the *classical bits* are encoded in the *relative phase* between two successive coherent pulses.

[Inoue, Waks, Yamamoto, PRA 68, 022317 (2003)]

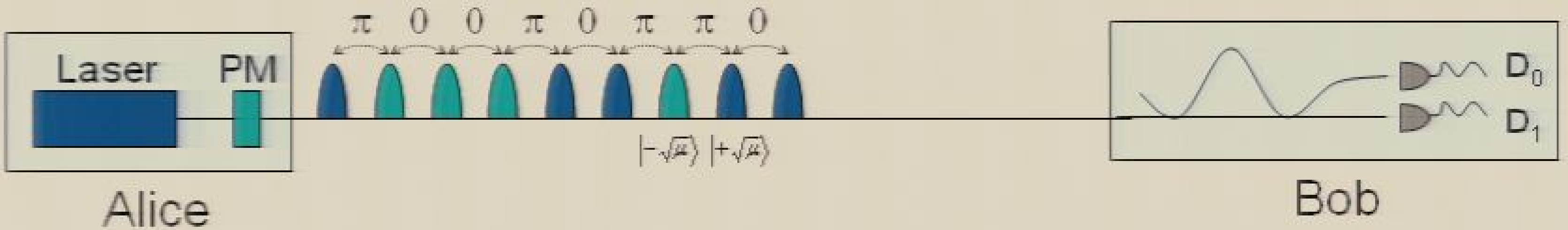
Differential Phase Shift protocol



- Alice sends a train of *weak coherent pulses* $\left|\pm\sqrt{\mu}\right\rangle$.
- The pulses have *overall phase relationships* (mode-locked laser);
  the *classical bits* are encoded in the *relative phase* between two successive coherent pulses.
- Bob inputs Alice's states into an unbalanced interferometer.
  Two successive pulses will interfere, so that Bob can determine the phase difference, and therefore the classical bit.

[Inoue, Waks, Yamamoto, PRA 68, 022317 (2003)]

Differential Phase Shift protocol



- Alice sends a train of *weak coherent pulses* $\left|\pm\sqrt{\mu}\right\rangle$.
- The pulses have *overall phase relationships* (mode-locked laser);
  the *classical bits* are encoded in the *relative phase* between two successive coherent pulses.
- Bob inputs Alice's states into an unbalanced interferometer.
  Two successive pulses will interfere, so that Bob can determine the phase difference, and therefore the classical bit.
  - Security parameters : $Q,V \quad \left(Q=\frac{1-V}{2}\right)$

[Gisin *et al*, quant-ph/0411022 (2004);
Stucki *et al*, APL 87, 194108 (2005)]

Coherent One Way protocol

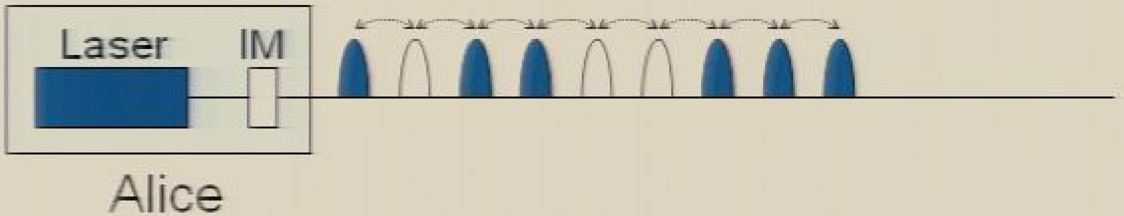
[Gisin *et al*, quant-ph/0411022 (2004);
Stucki *et al*, APL 87, 194108 (2005)]

Coherent One Way protocol

- Alice sends a train of *weak coherent pulses* or *empty*

[Gisin *et al*, quant-ph/0411022 (2004); Stucki *et al*, APL 87, 194108 (2005)]

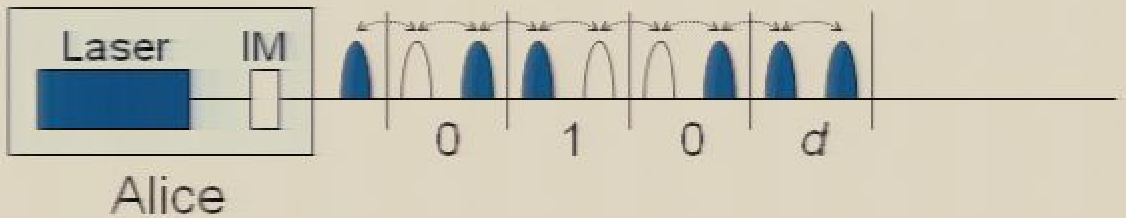
Coherent One Way protocol



- Alice sends a train of *weak coherent pulses* $|\sqrt{\mu}\rangle$ or *empty pulses* $|0\rangle$.
- Again, the pulses have *overall phase relations*.

[Gisin *et al*, quant-ph/0411022 (2004);
Stucki *et al*, APL 87, 194108 (2005)]

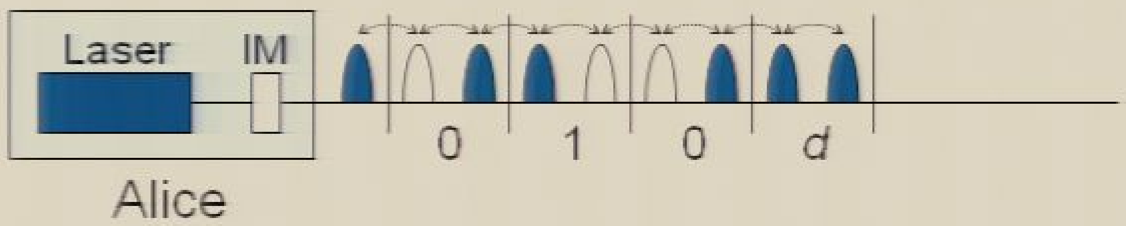
Coherent One Way protocol



- Alice sends a train of *weak coherent pulses* $|\sqrt{\mu}\rangle$ or *empty pulses* $|0\rangle$.
- Again, the pulses have *overall phase relationships*.
- The pulses are taken two by two to form *bit seque*

[Gisin *et al*, quant-ph/0411022 (2004); Stucki *et al*, APL 87, 194108 (2005)]

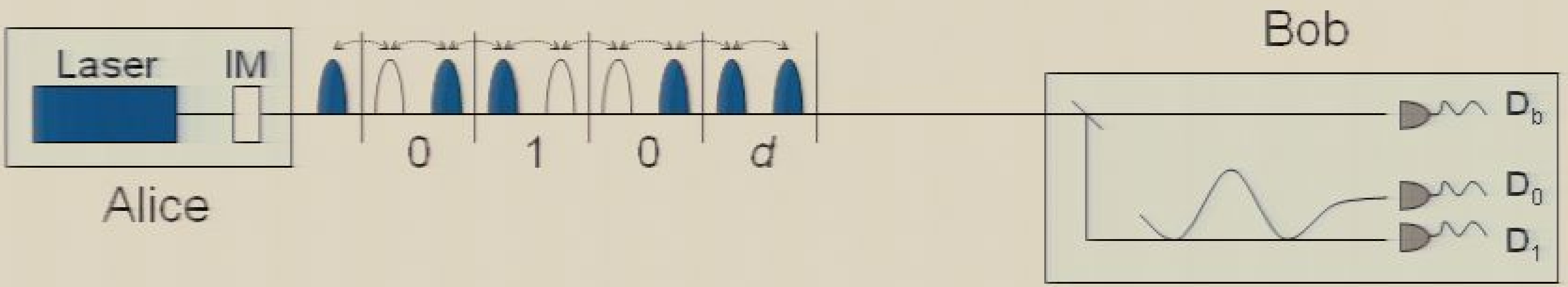
Coherent One Way protocol



- Alice sends a train of *weak coherent pulses* $|\sqrt{\mu}\rangle$ or *empty pulses* $|0\rangle$.
- Again, the pulses have *overall phase relationships*.
- The pulses are taken two by two to form *bit sequences* $|0\sqrt{\mu}\rangle$ or $|\sqrt{\mu}0\rangle$.

[Gisin *et al*, quant-ph/0411022 (2004);
Stucki *et al*, APL 87, 194108 (2005)]

Coherent One Way protocol

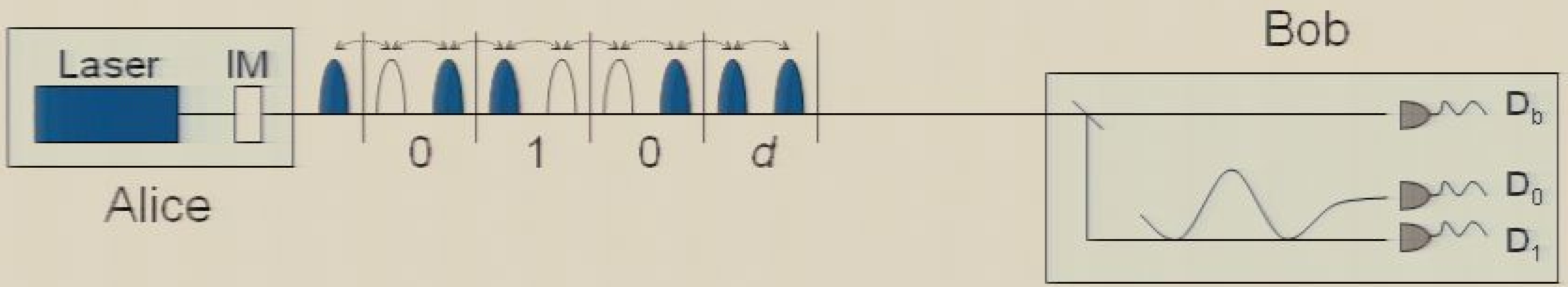


- Alice sends a train of *weak coherent pulses* $|\sqrt{\mu}\rangle$ or *empty pulses* $|0\rangle$.
- Again, the pulses have *overall phase relationships*.
- The pulses are taken two by two to form *bit sequences* $|0\sqrt{\mu}\rangle$ or $|\sqrt{\mu}0\rangle$.

- On a first line, Bob measures the time of arrival of the pulses to get the bits.
- Bob also takes a fraction of the incoming signal and inputs it into an unbalanced interferometer to check for the coherence between two successive non-empty pulses.

[Gisin *et al*, quant-ph/0411022 (2004);
Stucki *et al*, APL 87, 194108 (2005)]

Coherent One Way protocol



- Alice sends a train of *weak coherent pulses* $|\sqrt{\mu}\rangle$ or *empty pulses* $|0\rangle$.
- Again, the pulses have *overall phase relationships*.
- The pulses are taken two by two to form *bit sequences* $|0\sqrt{\mu}\rangle$ or $|\sqrt{\mu}0\rangle$.

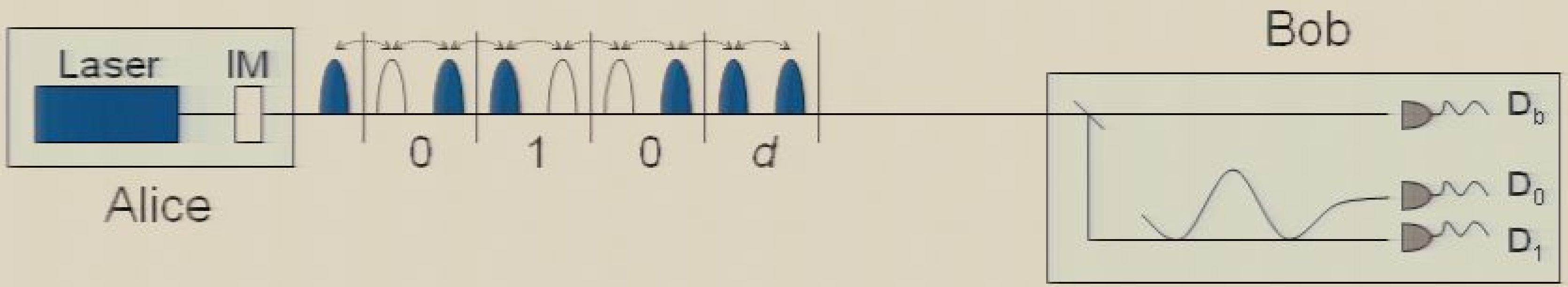
« Qubits » ?

- On a first line, Bob measures the time of arrival of the pulses to get the bits.
- Bob also takes a fraction of the incoming signal and inputs it into an unbalanced interferometer to check for the coherence between two successive non-empty pulses.

➢ Security parameters : Q, V

[Gisin *et al*, quant-ph/0411022 (2004);
Stucki *et al*, APL 87, 194108 (2005)]

Coherent One Way protocol



- Alice sends a train of *weak coherent pulses* $\left|\sqrt{\mu}\right\rangle$ or *empty pulses* $\left|0\right\rangle$.
- Again, the pulses have *overall phase relationships*.
- The pulses are taken two by two to form *bit sequences* $\left|0\sqrt{\mu}\right\rangle$ or $\left|\sqrt{\mu}0\right\rangle$.

« Qubits » ? No : additional phase relation…

- On a first line, Bob measures the time of arrival of the pulses to get the bits.
- Bob also takes a fraction of the incoming signal and inputs it into an unbalanced interferometer to check for the coherence between two successive non-empty pulses.

➢ Security parameters : Q, V

Security of these schemes ?

Security of these schemes ?

- Quite general methods have been developed to prove the security of a large class of « *standard* » QKD protocols, for which each classical bit is encoded into an independant quantum system (*qubit*).

Security of these schemes ?

- Quite general methods have been developed to prove the security of a large class of « *standard* » QKD protocols, for which each classical bit is encoded into an independant quantum system (*qubit*).
- Problem : for those distributed phase reference schemes, we cannot define such qubits…

  The standard proofs do not apply directly!

Security of these schemes ?

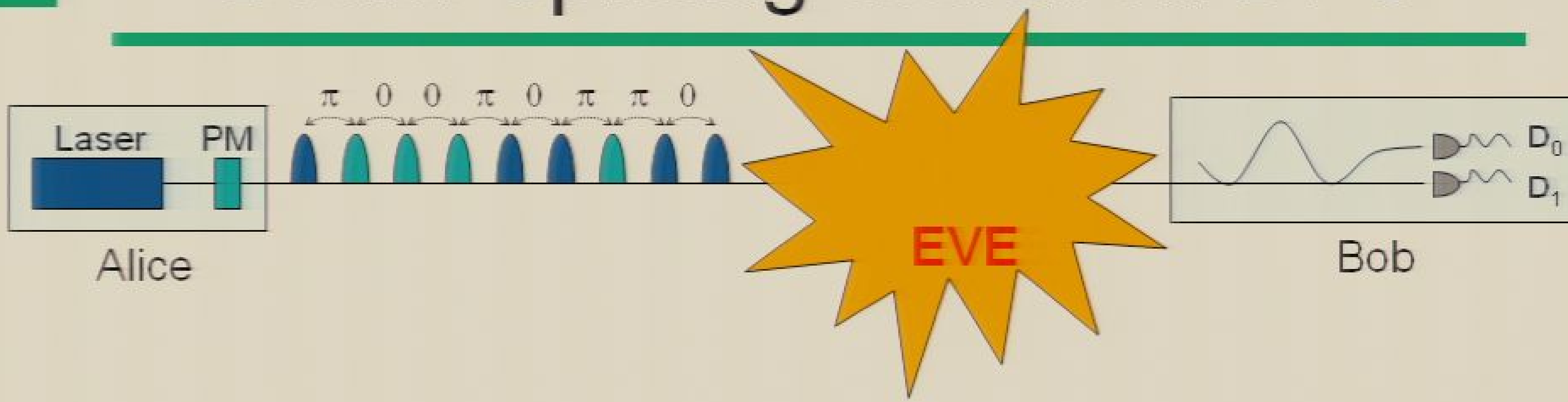
- Quite general methods have been developed to prove the security of a large class of « *standard* » QKD protocols, for which each classical bit is encoded into an independant quantum system (*qubit*).
- Problem : for those distributed phase reference schemes, we cannot define such qubits…

  The standard proofs do not apply directly!
- Before we try to develop new techniques, we want to get a feeling of how secure these schemes should be, of their limitations…

  In order to do so, we study specific attacks.

Beam-Splitting attack on DPS

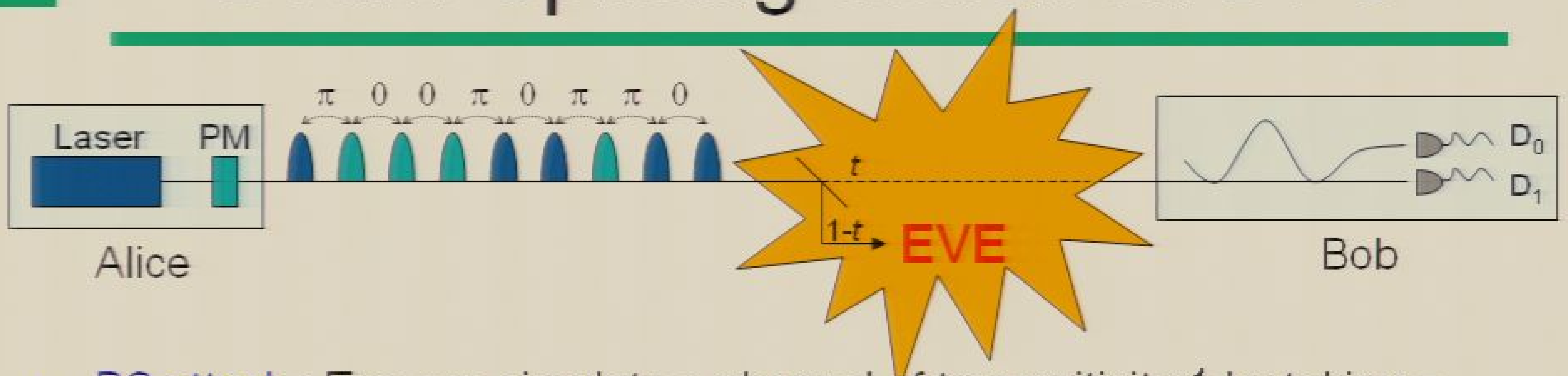
Beam-Splitting attack on DPS



Beam-Splitting attack on DPS

- BS attack : Eve can simulate a channel of transmitivity t by taking a fraction $(1-t)$ of the signal (states $|\pm\sqrt{\mu}\rangle$), and forwarding the other fraction t through a lossless channel to Bob.

Beam-Splitting attack on DPS

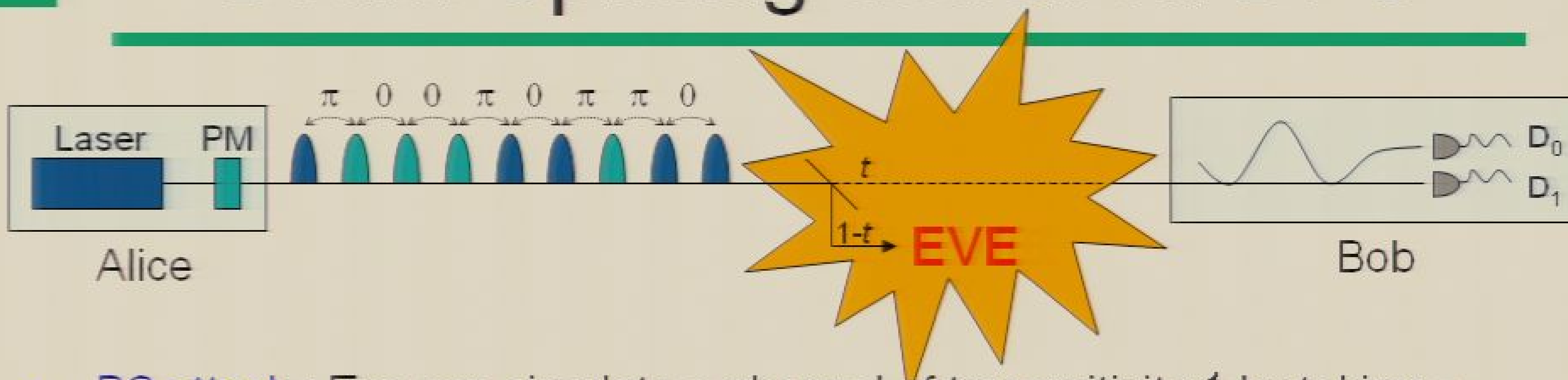


- BS attack : Eve can simulate a channel of transmitivity t by taking a fraction $(1-t)$ of the signal (states $\left|\pm\sqrt{\mu}\right\rangle$), and forwarding the other fraction t through a lossless channel to Bob.

- Eve's information ? She has states $\left|\pm\sqrt{\mu_E}\right\rangle$ where $\mu_E=(1-t)\mu$.
  For each bit detected by Bob, one can compute her states $\rho_E^{A=0/1}$ and ρ_E .
  Eve's information is upper-bounded by Holevo's quantity

$$\chi_{AE}=S(\rho_E)-\frac{1}{2}S(\rho_E^{A=0})-\frac{1}{2}S(\rho_E^{A=1})$$

Beam-Splitting attack on DPS

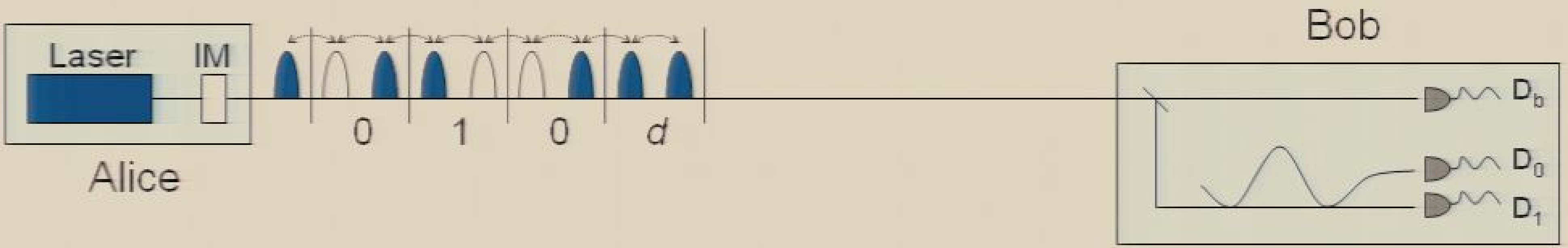


- BS attack : Eve can simulate a channel of transmitivity t by taking a fraction $(1-t)$ of the signal (states $|\pm\sqrt{\mu}\rangle$), and forwarding the other fraction t through a lossless channel to Bob.
- Eve's information ? She has states $|\pm\sqrt{\mu_E}\rangle$ where $\mu_E=(1-t)\mu$.
  For each bit detected by Bob, one can compute her states $\rho_E^{A=0/1}$ and ρ_E .
  Eve's information is upper-bounded by Holevo's quantity

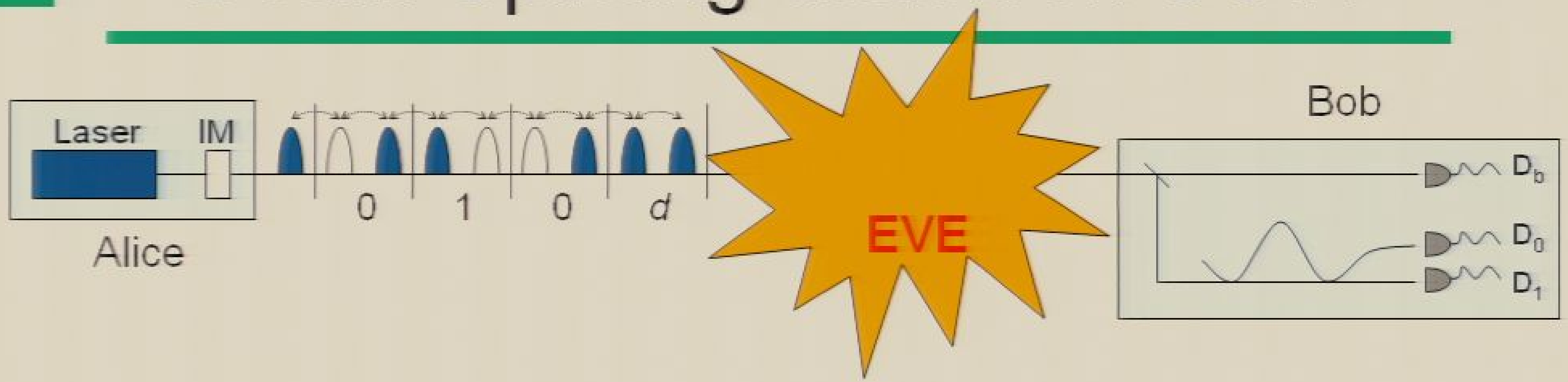
$$\chi_{AE}=S(\rho_E)-\frac{1}{2}S(\rho_E^{A=0})-\frac{1}{2}S(\rho_E^{A=1})$$

- Secret key rate ? $r=\mu t\eta\left(1-h(Q)-\chi_{AE}\right)$

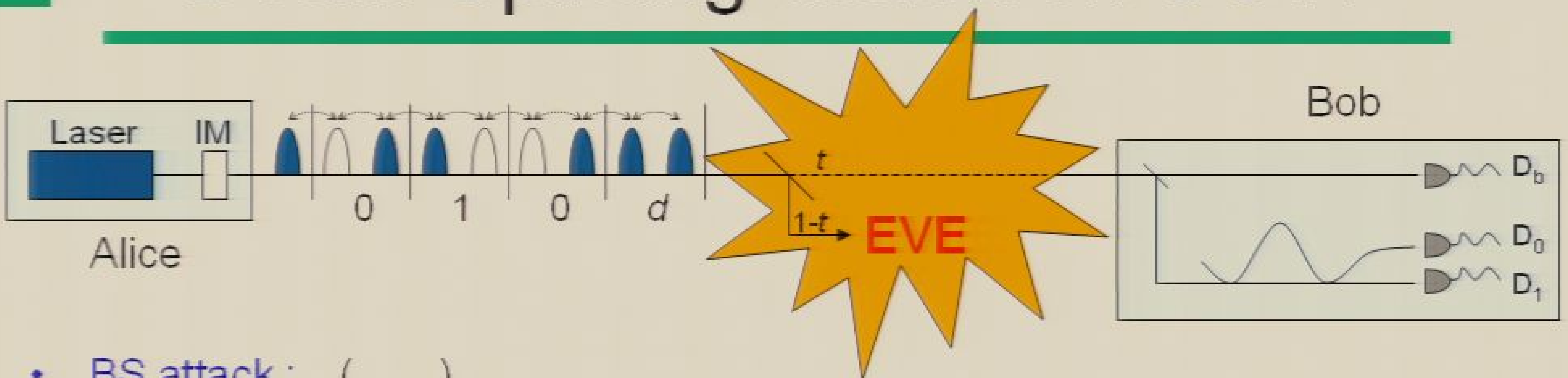
Beam-Splitting attack on COW



Beam-Splitting attack on COW



Beam-Splitting attack on COW



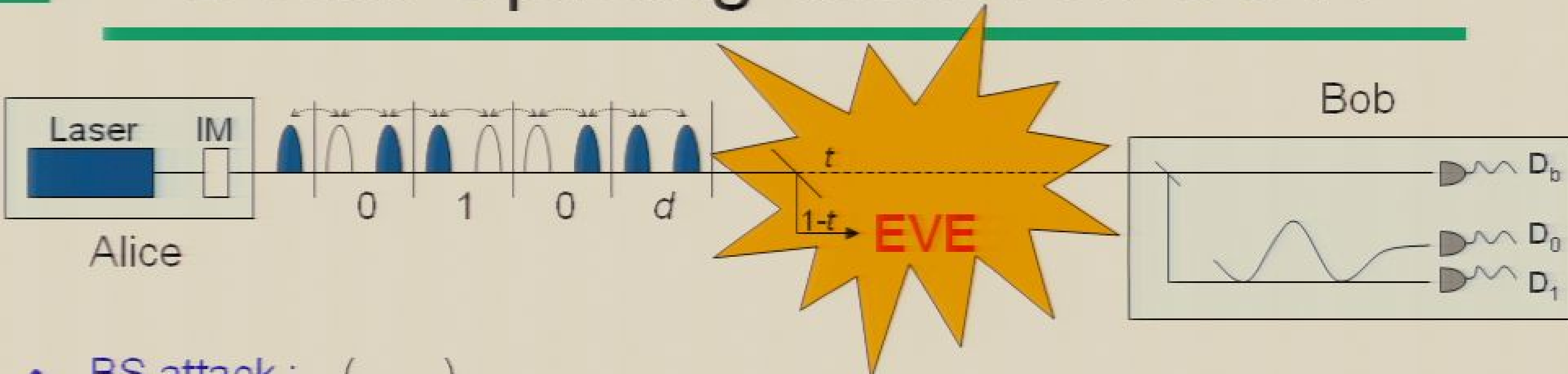
- BS attack : (……)
- Eve's information ?

  For each bit detected by Bob, Eve has one of the two states $\left|0,\sqrt{\mu_E}\right\rangle$ or $\left|\sqrt{\mu_E},0\right\rangle$.
  Again, Eve's information is upper-bounded by Holevo's quantity

$\mu_E = (1-t)\mu$

$$\chi_{AE} = S(\rho_E) - \frac{1}{2}S(\rho_E^{A=0}) - \frac{1}{2}S(\rho_E^{A=1})$$

Beam-Splitting attack on COW



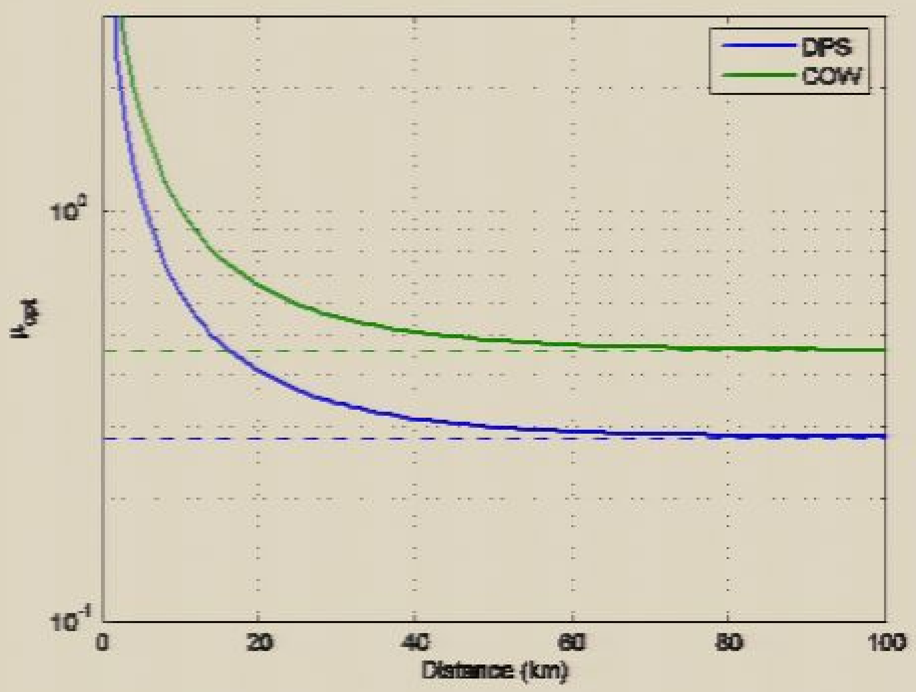
- BS attack : (… …)
- Eve's information ?

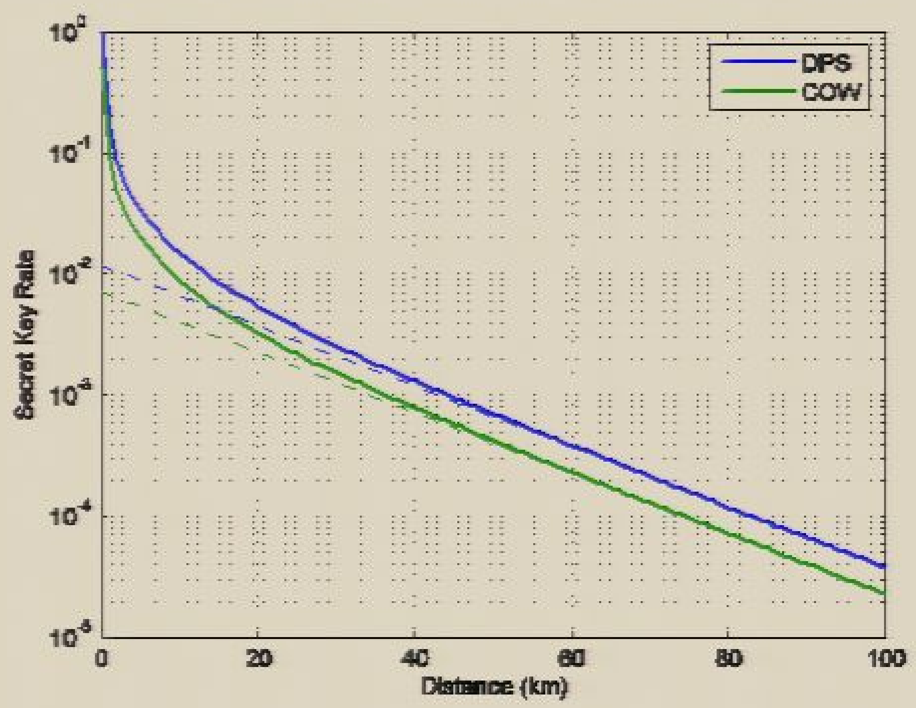
  For each bit detected by Bob, Eve has one of the two states $\left|0,\sqrt{\mu_E}\right\rangle$ or $\left|\sqrt{\mu_E},0\right\rangle$.
  Again, Eve's information is upper-bounded by Holevo's quantity $\mu_E = (1-t)\mu$

$$\chi_{AE} = S(\rho_E) - \frac{1}{2}S(\rho_E^{A=0}) - \frac{1}{2}S(\rho_E^{A=1})$$

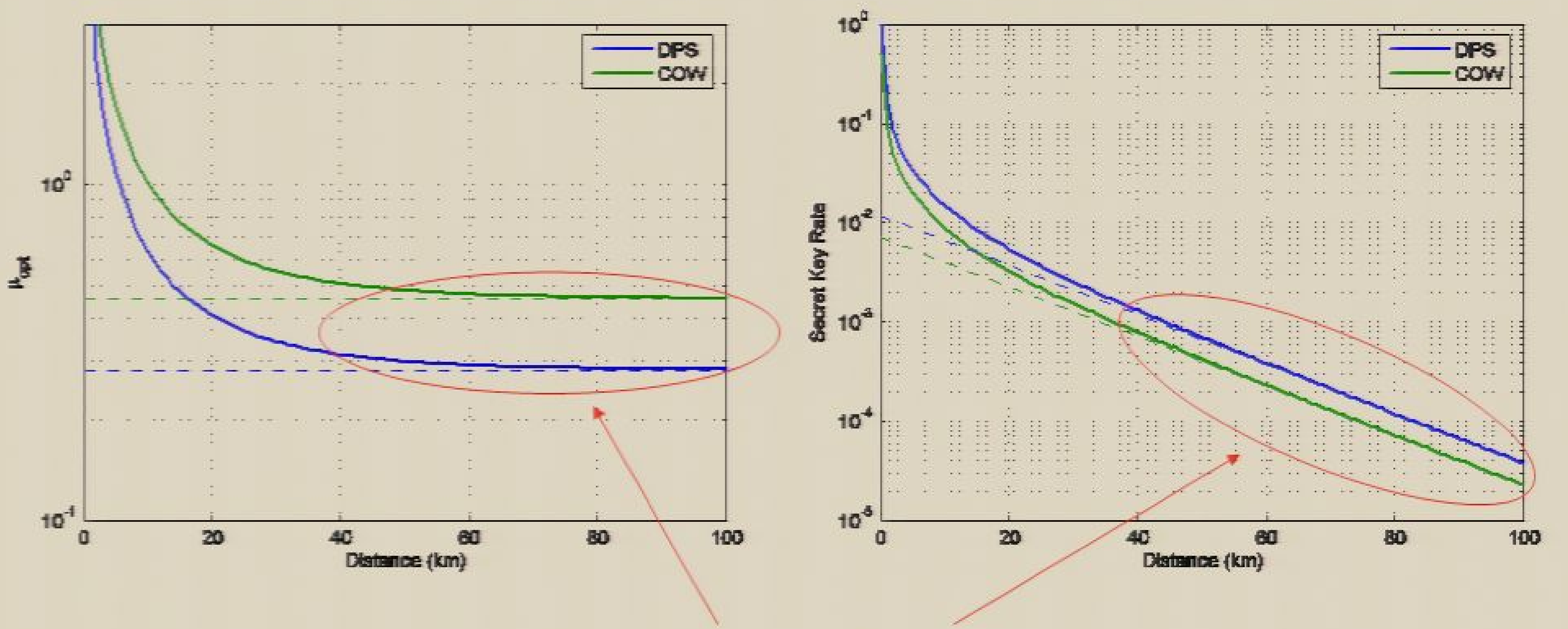
- Secret key rate ? $r = \frac{1}{2}\mu t\eta(1 - h(Q) - \chi_{AE})$

BS attack : DPS vs COW





BS attack : DPS vs COW



Linear regime :

for $\mu t << 1, \quad r = r_0 t \eta, \quad r_0 = r_0(\mu)$

Let's imagine other attacks…

Let’s imagine other attacks…

- BS attack is a zero-error attack

$$\left|\sqrt{\mu}\right\rangle_A \rightarrow \left|\sqrt{\mu t}\right\rangle_B \left|\sqrt{\mu_E}\right\rangle_E$$

Let's imagine other attacks…

- BS attack is a zero-error attack

$$\left|\sqrt{\mu}\right\rangle_A \rightarrow \left|\sqrt{\mu t}\right\rangle_B \left|\sqrt{\mu_E}\right\rangle_E$$

$$\text{For } \mu t << 1, \quad \left|\sqrt{\mu}\right\rangle_A \rightarrow \left(|0\rangle + \sqrt{\mu t}|1\rangle\right)_B \left|\sqrt{\mu_E}\right\rangle_E$$

Let's imagine other attacks…

- BS attack is a zero-error attack

$$\left|\sqrt{\mu}\right\rangle_A \rightarrow \left|\sqrt{\mu t}\right\rangle_B \left|\sqrt{\mu_E}\right\rangle_E$$

For $\mu t << 1,\quad \left|\sqrt{\mu}\right\rangle_A \rightarrow \left(|0\rangle + \sqrt{\mu t}|1\rangle\right)_B \left|\sqrt{\mu_E}\right\rangle_E$

- We are looking for more efficient attacks.

  Let's entangle Eve's system to Bob's !

Let's imagine other attacks…

- BS attack is a zero-error attack

$$\left|\sqrt{\mu}\right\rangle_A \rightarrow \left|\sqrt{\mu t}\right\rangle_B \left|\sqrt{\mu_E}\right\rangle_E$$

For $\mu t << 1$, $\left|\sqrt{\mu}\right\rangle_A \rightarrow \left(|0\rangle + \sqrt{\mu t}|1\rangle\right)_B \left|\sqrt{\mu_E}\right\rangle_E$

- We are looking for more efficient attacks.

  Let's entangle Eve's system to Bob's !

For $\mu t << 1$, $\left|\sqrt{\mu}\right\rangle_A \rightarrow |0\rangle_B |\varphi\rangle_E + \sqrt{\mu t}|1\rangle_B |\psi\rangle_E$

The price to pay will be the introduction of errors…

[Ex: For the above attack on a sequence $\left|\sqrt{\mu}\sqrt{\mu}\right\rangle$, the interference will show a visibility $V = \left|\langle\varphi|\psi\rangle\right|^2$]

New attacks on DPS and COW

In fact, it is more efficient for Eve to attack the pulses 2 by 2 :

New attacks on DPS and COW

In fact, it is more efficient for Eve to attack the pulses 2 by 2 :

- For DPS :

$$\left|\sigma\sqrt{\mu},\omega\sqrt{\mu}\right\rangle_A \rightarrow |00\rangle_B\left|\varphi_{\sigma\omega}\right\rangle_E + \sqrt{\mu t}\,|01\rangle_B\left|\psi^{01}_{\sigma\omega}\right\rangle_E + \sqrt{\mu t}\,|10\rangle_B\left|\psi^{10}_{\sigma\omega}\right\rangle_E \qquad (\sigma,\omega\in\{+,-\})$$

Loss of visibility, QBER :

$$V_{\sigma\omega} = \mathrm{Re}\left\langle\psi^{01}_{\sigma\omega}\middle|\psi^{10}_{\sigma\omega}\right\rangle, \quad V_{\sigma\omega,\sigma'\omega'} = \mathrm{Re}\left\langle\varphi_{\sigma\omega}\middle|\psi^{01}_{\sigma\omega}\right\rangle\left\langle\psi^{10}_{\sigma'\omega'}\middle|\varphi_{\sigma'\omega'}\right\rangle, \quad QBER = \frac{1-V}{2}$$

New attacks on DPS and COW

In fact, it is more efficient for Eve to attack the pulses 2 by 2 :

- For DPS :

$$\left|\sigma\sqrt{\mu},\omega\sqrt{\mu}\right\rangle_A \to |00\rangle_B|\varphi_{\sigma\omega}\rangle_E + \sqrt{\mu t}|01\rangle_B\left|\psi_{\sigma\omega}^{01}\right\rangle_E + \sqrt{\mu t}|10\rangle_B\left|\psi_{\sigma\omega}^{10}\right\rangle_E \qquad (\sigma,\omega\in\{+,-\})$$

Loss of visibility, QBER :

$$V_{\sigma\omega} = \mathrm{Re}\left\langle\psi_{\sigma\omega}^{01}\middle|\psi_{\sigma\omega}^{10}\right\rangle,\quad V_{\sigma\omega,\sigma'\omega'} = \mathrm{Re}\left\langle\varphi_{\sigma\omega}\middle|\psi_{\sigma\omega}^{01}\right\rangle\left\langle\psi_{\sigma'\omega'}^{10}\middle|\varphi_{\sigma'\omega'}\right\rangle,\quad QBER = \frac{1-V}{2}$$

- For COW :

$$\left|0,\sqrt{\mu}\right\rangle_A \to |00\rangle_B|\varphi_0\rangle_E + \sqrt{(1-Q)\mu t}|01\rangle_B\left|\psi_0^{01}\right\rangle_E + \sqrt{Q\mu t}|10\rangle_B\left|\psi_0^{10}\right\rangle_E$$

$$\left|\sqrt{\mu},0\right\rangle_A \to |00\rangle_B|\varphi_1\rangle_E + \sqrt{Q\mu t}|01\rangle_B\left|\psi_1^{01}\right\rangle_E + \sqrt{(1-Q)\mu t}|10\rangle_B\left|\psi_1^{10}\right\rangle_E$$

Study of the new attacks

Study of the new attacks

- So far we didn't say anything about Eve's states; she will of course chose them so as to maximize her information.

Study of the new attacks

- So far we didn't say anything about Eve's states; she will of course chose them so as to maximize her information.

[Eve's states should satisfy a few constraints : unitarity, visibilities.]

Study of the new attacks

- So far we didn't say anything about Eve's states; she will of course chose them so as to maximize her information.

  [Eve's states should satisfy a few constraints : unitarity, visibilities.]

  [Eve's information will be again measured by Holevo's quantity χ_{AE} or χ_{BE}]

Study of the new attacks

- So far we didn't say anything about Eve's states; she will of course chose them so as to maximize her information.

  [Eve's states should satisfy a few constraints : unitarity, visibilities.]

  [Eve's information will be again measured by Holevo's quantity χ_{AE} or χ_{BE}]

- As for Alice and Bob, they should optimize the value of μ so as to maximize the secret key rate r (or r_0).

Study of the new attacks

- So far we didn't say anything about Eve's states; she will of course chose them so as to maximize her information.

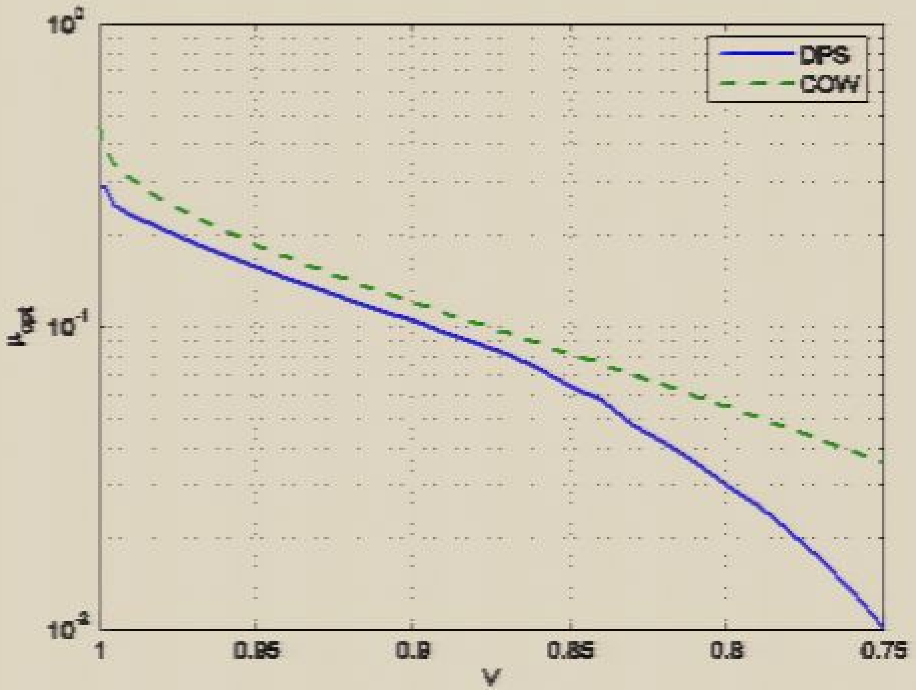
  [Eve's states should satisfy a few constraints : unitarity, visibilities.]

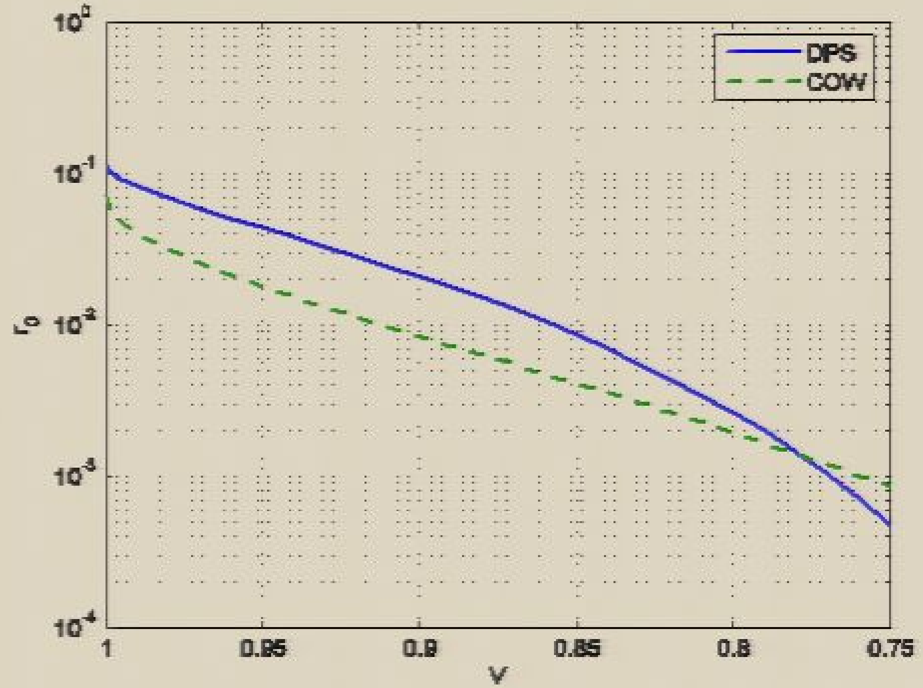
  [Eve's information will be again measured by Holevo's quantity χ_{AE} or χ_{BE}]

- As for Alice and Bob, they should optimize the value of μ so as to maximize the secret key rate r (or r_0).

- The two rounds of optimization were performed numerically.

Security bounds for our attacks





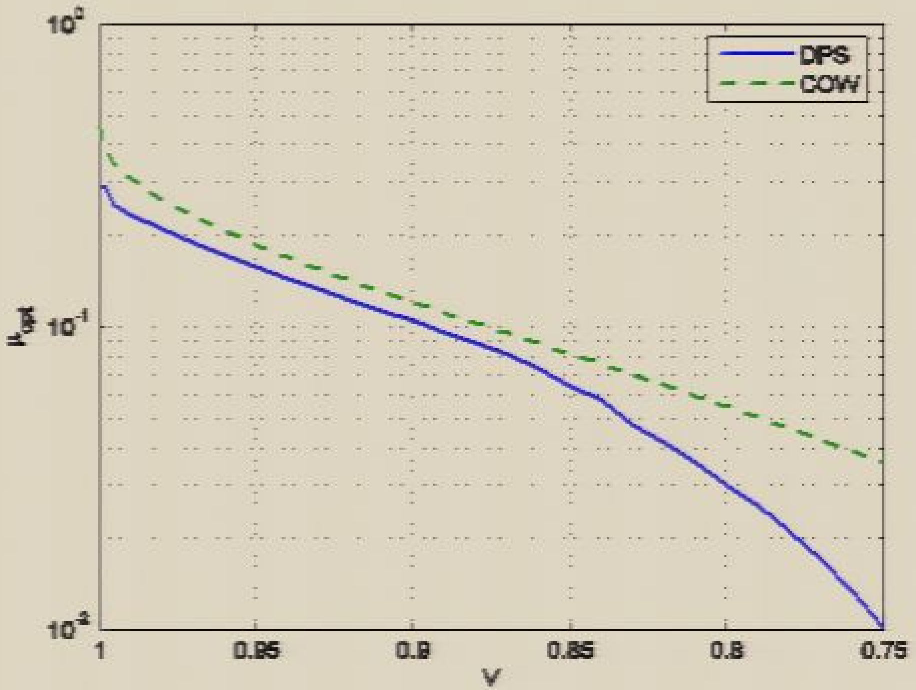
Secret key rates : $r = r_0 t \eta$

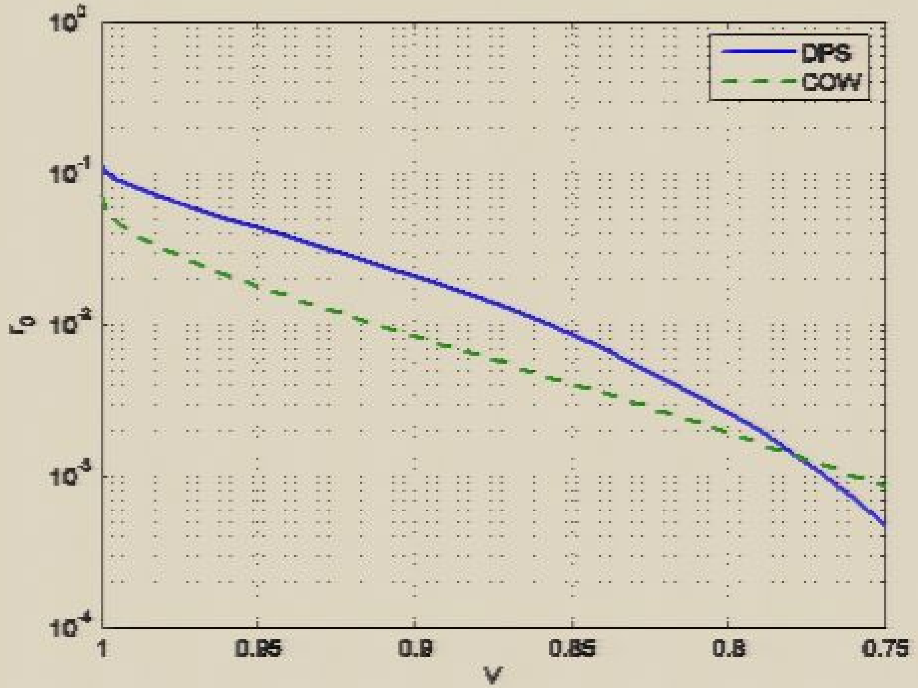
Note that…

Note that…

- Our attacks give us upper bounds on the secret key rates that one can achieve with the DPS or COW protocols.

Security bounds for our attacks





Secret key rates : $r = r_0 t \eta$

Note that…

- Our attacks give us upper bounds on the secret key rates that one can achieve with the DPS or COW protocols.
- Other types of attacks have also been studied:
  - On DPS: [Curty *et al*, quant-ph/0609094, to be published in QIC; T. Tsurumaru, quant-ph/0612204]
  - On COW: [Branciard *et al*, quant-ph/0609090, to be published in QIC]

Note that…

- Our attacks give us upper bounds on the secret key rates that one can achieve with the DPS or COW protocols.
- Other types of attacks have also been studied:
  - On DPS: [Curty *et al*, quant-ph/0609094, to be published in QIC;
    T. Tsurumaru, quant-ph/0612204]
  - On COW: [Branciard *et al*, quant-ph/0609090, to be published in QIC]
- These are specific attacks, they do not allow us to conclude that the protocols are secure !

Note that…

- Our attacks give us upper bounds on the secret key rates that one can achieve with the DPS or COW protocols.

- Other types of attacks have also been studied:
  - On DPS: [Curty *et al*, quant-ph/0609094, to be published in QIC;
    T. Tsurumaru, quant-ph/0612204]
  - On COW: [Branciard *et al*, quant-ph/0609090, to be published in QIC]

- These are specific attacks, they do not allow us to conclude that the protocols are secure !

  However, we hope our attacks are not that far from the optimal ones, and that our upper bounds are not that bad !

Conclusion

Conclusion

- Two « Distributed Phase Reference » protocols:
  the DPS and COW protocols.

Conclusion

- Two « Distributed Phase Reference » protocols:
  the DPS and COW protocols.
- Quite simple in principle, but the standard security proofs do not apply. ☹
- Study of some specific attacks,
  Upper bounds on the achievable secret key rates.
- Intuition on the performances of these schemes.
  That's a good start ! ☺

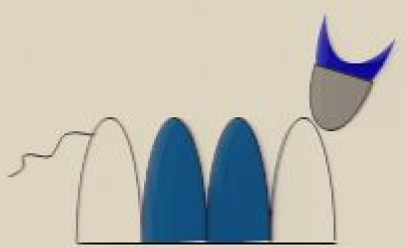
Conclusion

- Two « Distributed Phase Reference » protocols:
  the DPS and COW protocols.
- Quite simple in principle, but the standard security proofs do not apply. ☹
- Study of some specific attacks,
  Upper bounds on the achievable secret key rates.
- Intuition on the performances of these schemes.
  That's a good start ! ☺

THANKS

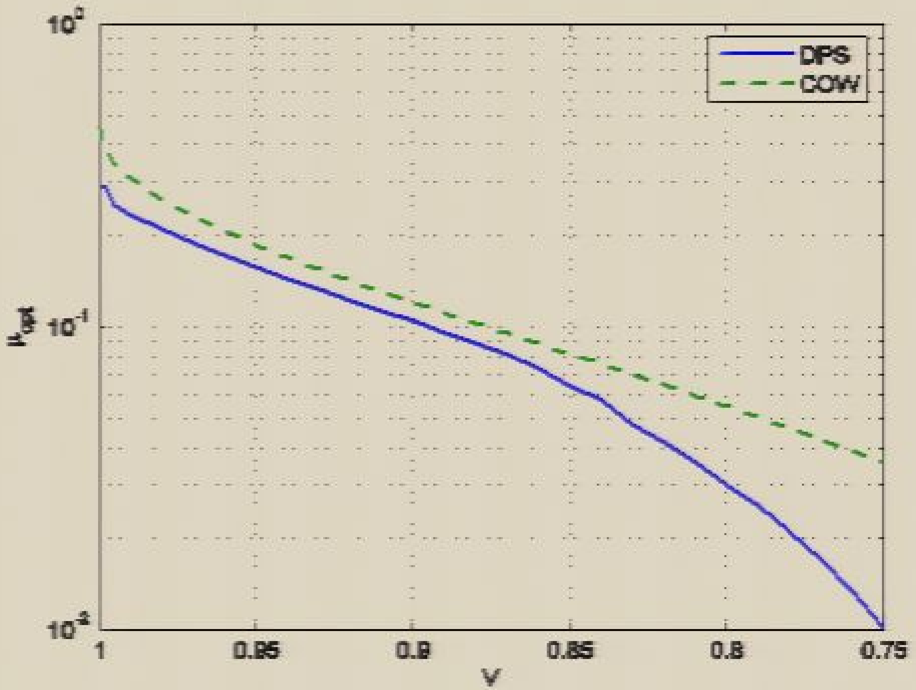
for your attention !

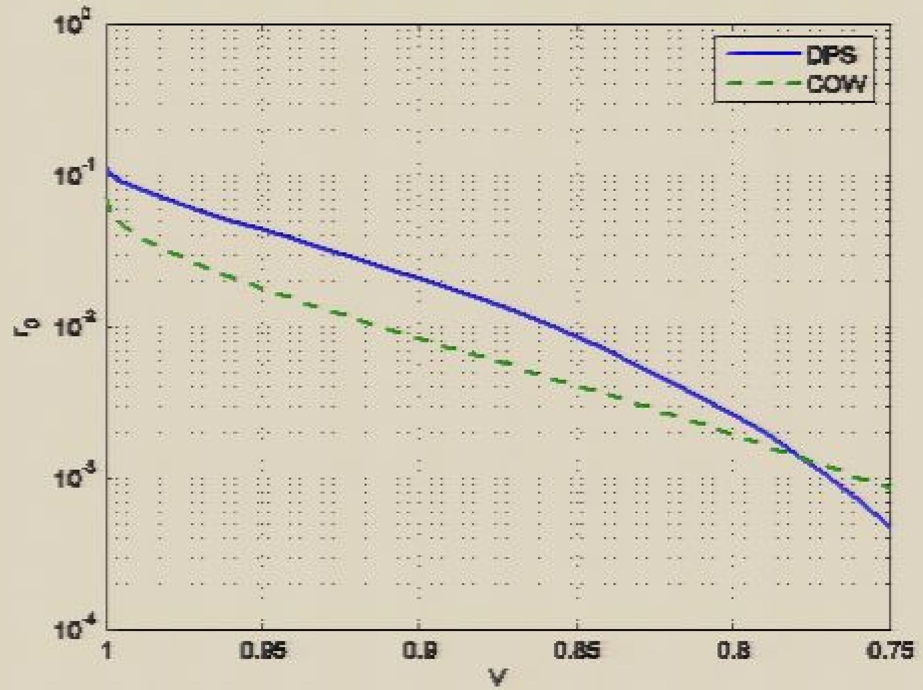
(and by the way, I also love you all very much ;-) !)



UNIVERSITÉ
DE GENÈVE
FACULTÉ DES SCIENCES

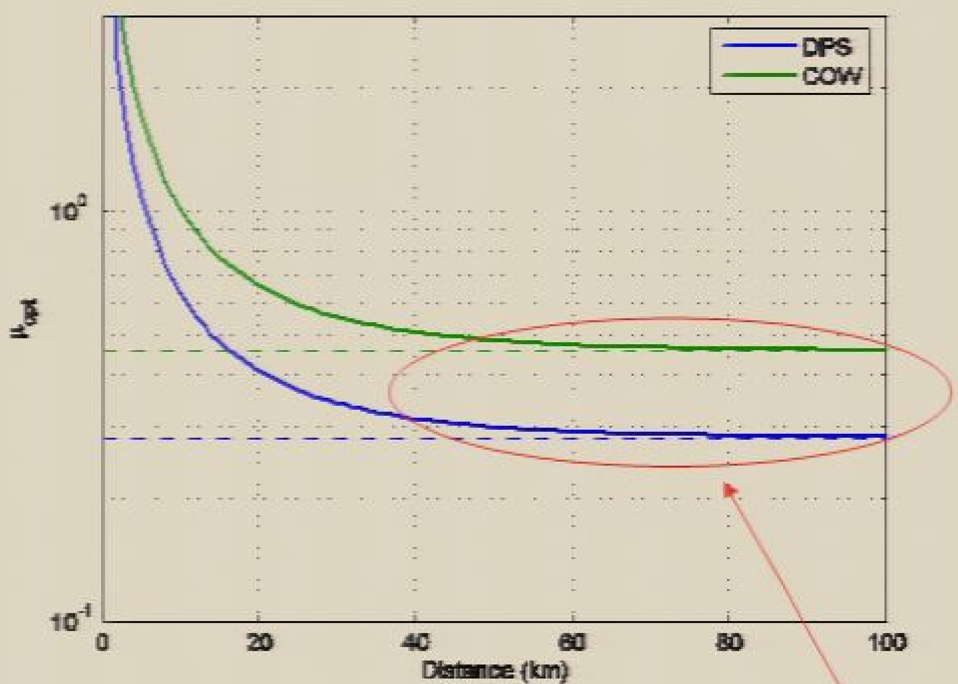
Security bounds for our attacks

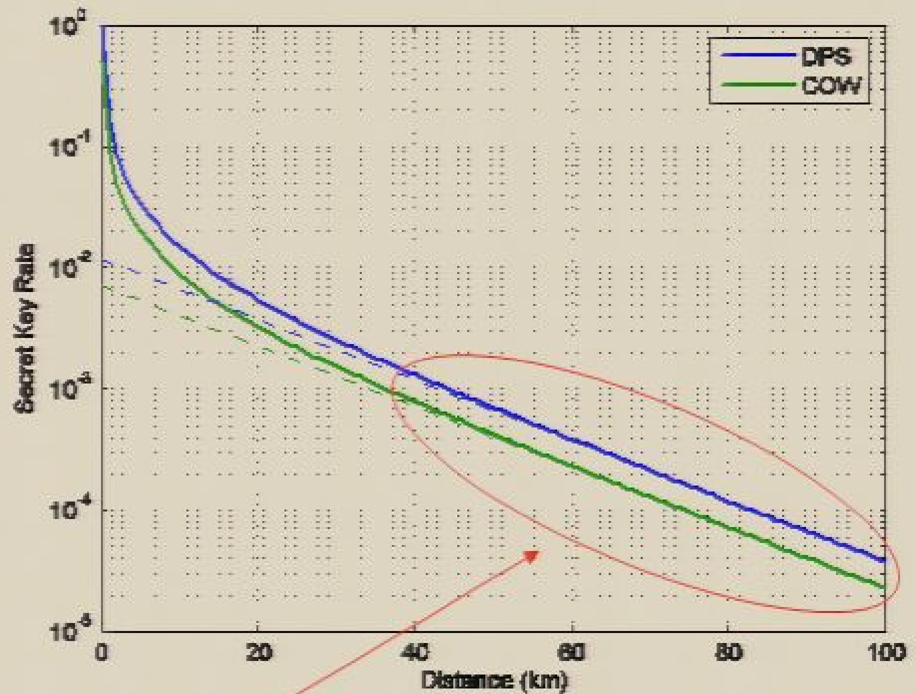




Secret key rates : $r = r_0 t \eta$

BS attack : DPS vs COW

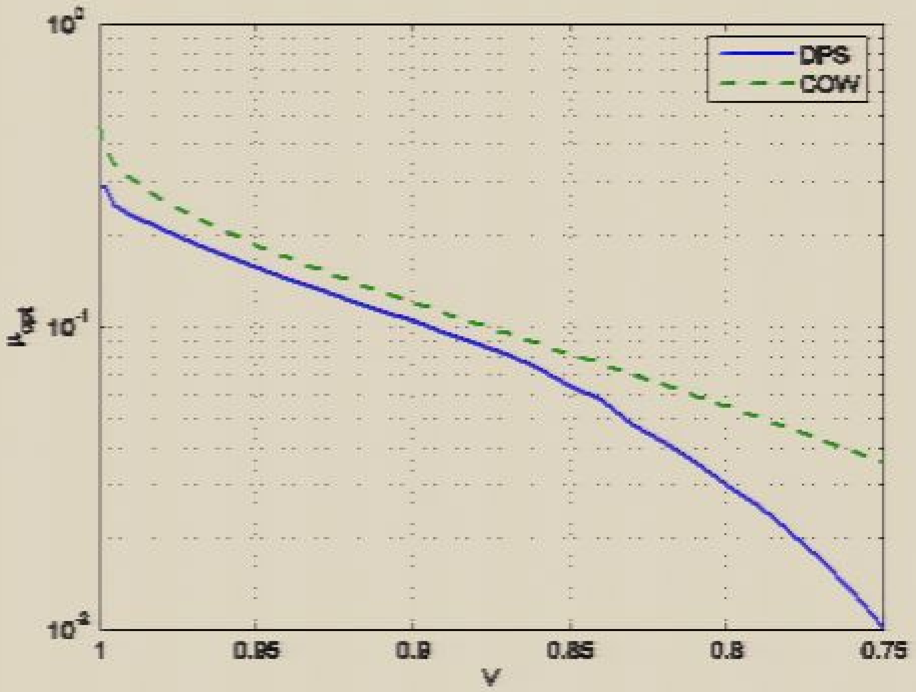


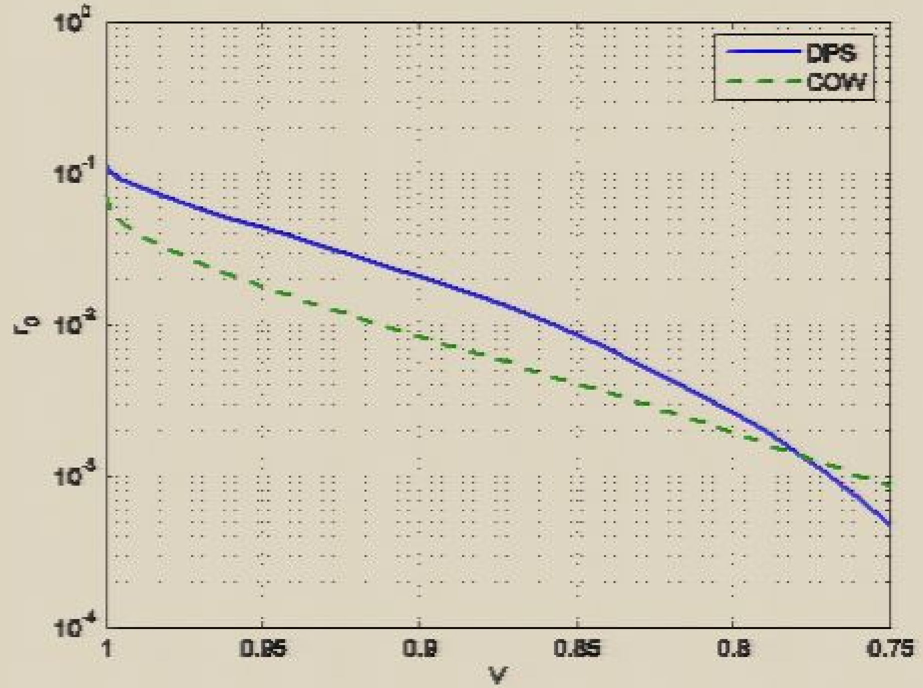


Linear regime :

for $\mu t << 1, \quad r = r_0 t \eta, \quad r_0 = r_0(\mu)$

Security bounds for our attacks





Secret key rates : $r = r_0 t \eta$