Continuous Variable Quantum Cryptography

Towards High Speed Quantum Cryptography

Frédéric Grosshans

LPQM
laboratoire de photonique quantique et moléculaire
CNRS / ENS Cachan

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Palacký University, Olomouc, 2011

Conditions for Perfect Secrecy

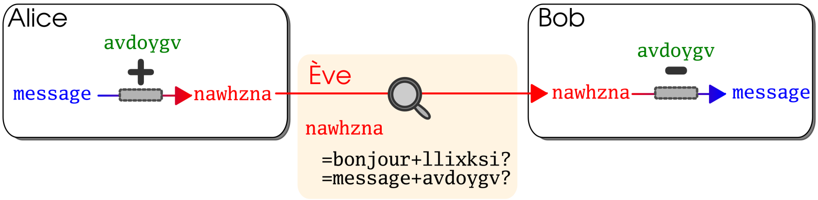
Alice sends a secret message to **Bob**

Conditions for Perfect Secrecy

Alice sends a secret message to **Bob** through a channel observed by **Eve**.

Conditions for Perfect Secrecy

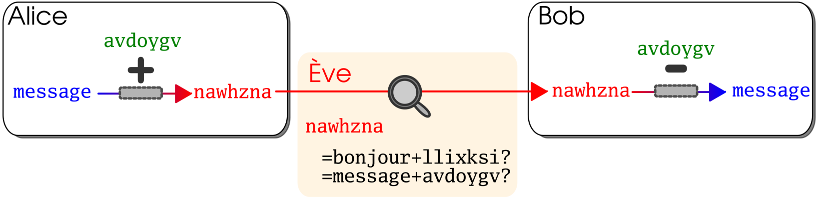
Alice sends a secret message to **Bob** through a channel observed by **Eve**.



She encrypts the message with a secret key

Conditions for Perfect Secrecy

Alice sends a secret message to **Bob** through a channel observed by **Eve**.



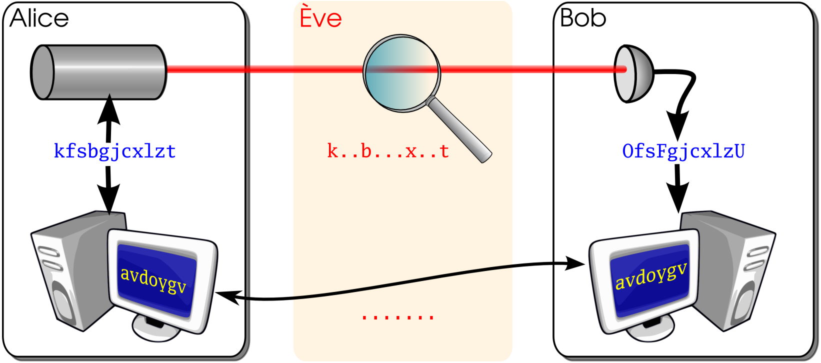
She encrypts the message with a secret key as long as the message.

Quantum Key Distribution

Alice sends quantum objects to Bob

Quantum Key Distribution

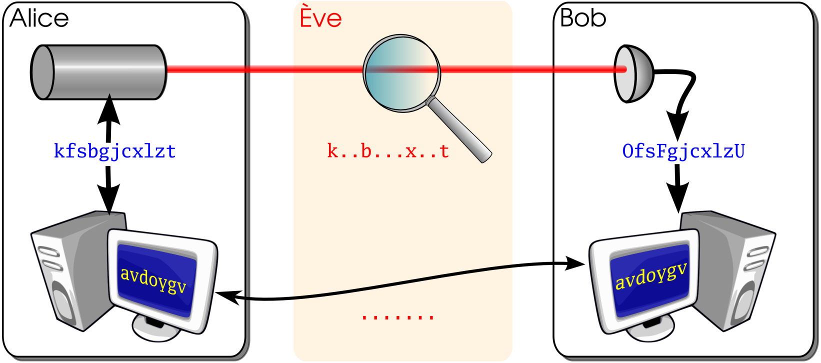
Alice sends quantum objects to Bob



Eve's Measurenents

Quantum Key Distribution

Alice sends quantum objects to Bob



Eve's Measurenents ⇒ measurable perturbations

⇒ secret key generation

Unconditionnally Secure Systems . . .

Single Photon QKD

- Long Range ($\sim$ 100 km)
- Low rate (kbit/s)

Unconditionnally Secure Systems . . .

Single Photon QKD

- Long Range ($\sim$ 100 km)
- Low rate (kbit/s) maybe a few Mbit/s in the long run

Unconditionnally Secure Systems . . .

Single Photon QKD

- Long Range ($\sim$ 100 km)
- Low rate (kbit/s) maybe a few Mbit/s in the long run

Classical One-Time-Pad

- Very Long Range (Paris–Olomouc)
- Not so small rate :

Unconditionnally Secure Systems . . .

Single Photon QKD

- Long Range ($\sim$ 100 km)
- Low rate (kbit/s) maybe a few Mbit/s in the long run

Classical One-Time-Pad

- Very Long Range (Paris–Olomouc)
- Not so small rate :
  - 1 CD / year = 180 bits/s

Unconditionnally Secure Systems . . .

Single Photon QKD

- Long Range ($\sim$ 100 km)
- Low rate (kbit/s) maybe a few Mbit/s in the long run

Classical One-Time-Pad

- Very Long Range (Paris–Olomouc)
- Not so small rate :
    - 1 CD / year = 180 bits/s
    - 1 iPod (160 GB)/ year = 40 kbit/s

Unconditionnally Secure Systems . . .

Single Photon QKD

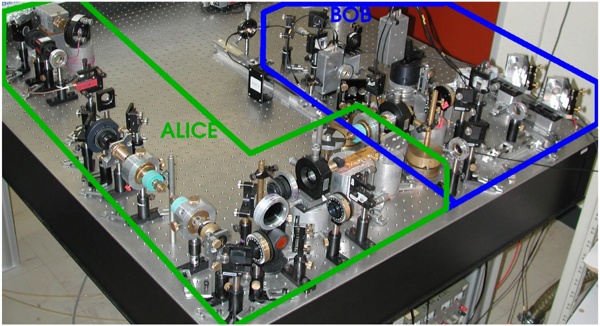
- Long Range ($\sim$ 100 km)
- Low rate (kbit/s) maybe a few Mbit/s in the long run

Classical One-Time-Pad

- Very Long Range (Paris–Olomouc)
- Not so small rate :
  - 1 CD / year = 180 bits/s
  - 1 iPod (160 GB)/ year = 40 kbit/s
- But the data has to stay here

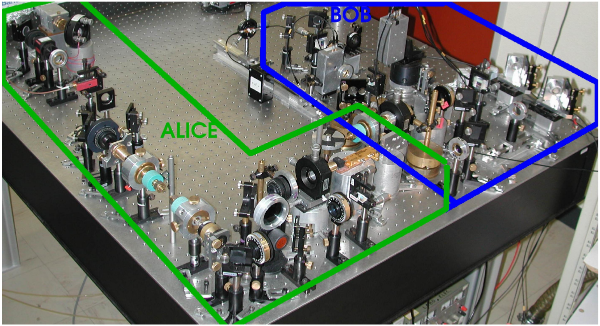
. . . and Continuous Variable

- Medium Range :∼ 25 km
- Medium Rate :∼ a few kbit/s



. . . and Continuous Variable

- Medium Range :∼ 25 km
- Medium Rate :∼ a few kbit/s
- Much less mature



. . . and Continuous Variable

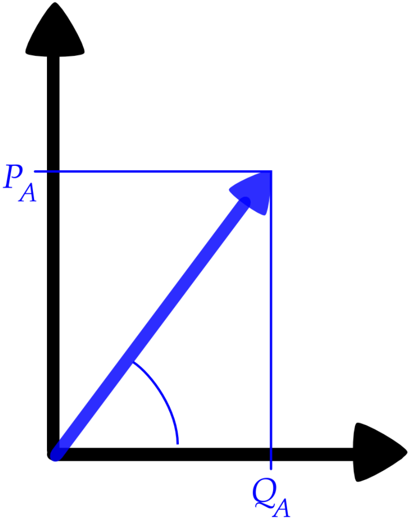
- Medium Range :∼ 25 km ; 80 km soon ?
- Medium Rate :∼ a few kbit/s ; Mbits/s soon ?
- Much less mature ⇒ Much room for improvements

Field quadratures

Classical field

Electromagnetic field described by Q_A and P_A

$E(t) = Q_A \cos \omega t + P_A \sin \omega t$



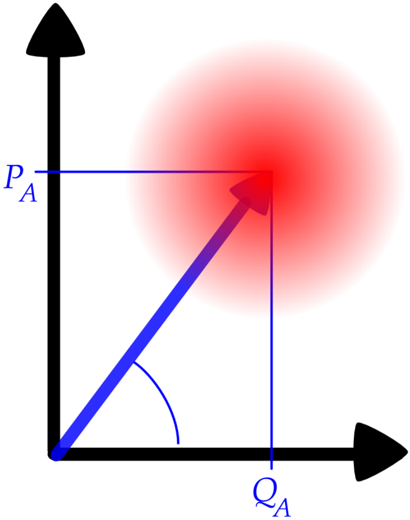
Field quadratures

Classical field

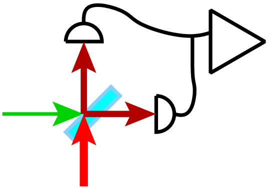
Electromagnetic field described by Q_A and P_A
$E(t) = Q_A \cos \omega t + P_A \sin \omega t$

Quantum description

Q and P do not commute:
$$[Q, P] \propto i\hbar.$$
Add a "quantum noise":
$$Q = Q_A + B_Q \text{ et } P = P_A + B_P$$
Heisenberg $\Longrightarrow \Delta B_Q \Delta B_P \geq 1$



Homodyne Detection : Theory



Photocurrents:

$$i_\pm \propto \overline{(E_{\text{osc.}}(t) \pm E_{\text{signal}}(t))^2}$$
$$\propto \overline{E_{\text{osc.}}(t)^2 \pm 2E_{\text{osc.}}(t)E_{\text{signal}}(t)}$$

after substraction:

$$\delta i \propto \overline{E_{\text{osc.}}(t)E_{\text{signal}}(t)}$$
$$\propto \boxed{E_{\text{osc.}}(Q_{\text{signal}} \cos\varphi + P_{\text{signal}} \sin\varphi)}$$

XXth century CVQKD

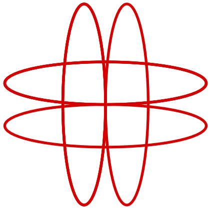
At the end of XXth century it was obvious that a generalization of QKD to continuous variables could be interesting.
Problem : discrete bits $\neq$ continuous variable

XX$^{\text{th}}$ century CVQKD

At the end of XXth century it was obvious that a generalization of QKD to continuous variables could be interesting.
Problem : discrete bits $\neq$ continuous variable

Adapting BB84?

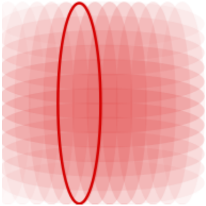
Mark Hillery, "Quantum Cryptography with Squeezed States",
`arXiv:quant-ph/9909006`/PRA **61** 022309



XXth century CVQKD

At the end of XXth century it was obvious that a generalization of QKD to continuous variables could be interesting.
Problem : discrete bits $\neq$ continuous variable

Natural modulation + information theory!
Nicolas J. Cerf, Marc Lévy, Gilles Van Assche : "Quantum distribution of Gaussian keys using squeezed states", `arXiv:quant-ph/0008058`/PRL **63** 052311



Where are the bits ?

Quite frequent discussion with discrete quantum cryptographers :

DQC : How do you encode a 0 or a 1 in CVQKD?

Me : I don't care, C. E. Shannon tells me "$\forall \varepsilon > 0, \exists$ code of rate $I - \varepsilon$."

Where are the bits ?

Quite frequent discussion with discrete quantum cryptographers :

DQC : How do you encode a 0 or a 1 in CVQKD?

Me : Gilles/Jérôme/Anthony/Sébastien developed a really efficient code, using sliced reconciliation/LDPC matrices/$\mathbb{R}^8$ rotations and octonions. Only he knows how it works.

Where are the bits ?

Quite frequent discussion with discrete quantum cryptographers :

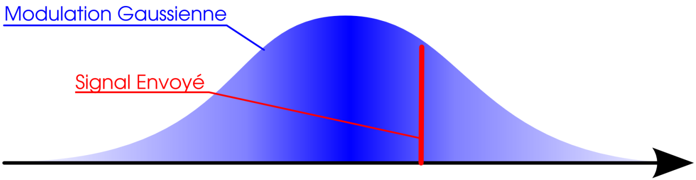
DQC : How do you encode a 0 or a 1 in CVQKD?

Me : Gilles/Jérôme/Anthony/Sébastien developed a really efficient code, using sliced reconciliation/LDPC matrices/$\mathbb{R}^8$ rotations and octonions. Only he knows how it works.

Computation of the ideal code performance is easy !

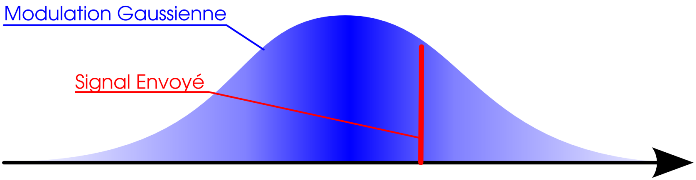
They're hidden

Availaible informationin a continuous signal



They're hidden

Availaible informationin a continuous signal



Differential entropy

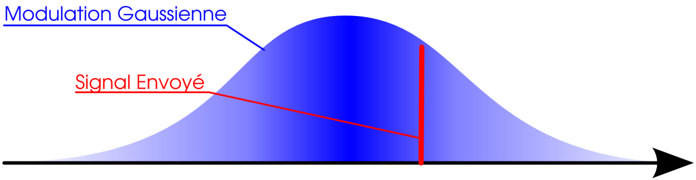
$$H(X) = -\sum \mathcal{P}(x)\,dx \log \mathcal{P}(x)\,dx$$

$$\simeq \underbrace{\int dx\, \mathcal{P}(x) \log \mathcal{P}(x)}_{\mathcal{H}(X)} - \underbrace{\log dx}_{\text{constante}}$$

They're hidden

Availible informationin a continuous signal

with noise ?



Differential entropy

$$H(X) = -\sum \mathcal{P}(x)\,dx \log \mathcal{P}(x)\,dx$$

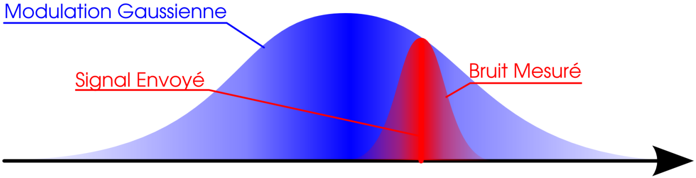
$$\simeq \underbrace{\int dx\,\mathcal{P}(x) \log \mathcal{P}(x)}_{\mathcal{H}(X)} - \underbrace{\log dx}_{\text{constante}}$$

$$\mathcal{H}(X) = \log \Delta X + \text{constante}$$

They're hidden

Availaible informationin a continuous signal

with noise ?



Differential entropy

$$H(X) = -\sum \mathcal{P}(x)\,dx \log \mathcal{P}(x)\,dx$$
$$\simeq \underbrace{\int dx\, \mathcal{P}(x) \log \mathcal{P}(x)}_{\mathcal{H}(X)} - \underbrace{\log dx}_{\text{constante}}$$

Mutual information

$$\begin{aligned} I(X:Y) &= H(Y) - H(Y|X) \\ &= \mathcal{H}(Y) - \mathcal{H}(Y|X) \\ &= \frac{1}{2} \log \frac{\Delta Y^2}{\Delta Y^2|X} \end{aligned}$$

The spy's power

Heisenberg :

$$\Delta B_{\text{Eve}} \Delta B_{\text{Bob}} \geq 1$$

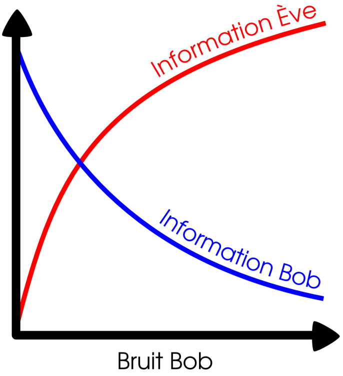
The spy's power

Heisenberg :

$$\Delta B_{\text{Eve}} \Delta B_{\text{Bob}} \geq 1$$

$\Rightarrow \Delta B_{\text{Bob}}$ gives

- I_{Eve}
- I_{Bob}



Quantum Key Distribution Protocols

Channel Evauation (noise measure)

Alice&Bob evaluate I_{Eve}

Quantum Key Distribution Protocols

Channel Evauation (noise measure)

Alice&Bob evaluate I_{Eve}

Reconciliation (error correction)

Alice&Bob share I_{Bob} identical bits.

Ève knows I_{Eve}.

Quantum Key Distribution Protocols

Channel Evauation (noise measure)

Alice&Bob evaluate I_{Eve}

Reconciliation (error correction)

Alice&Bob share I_{Bob} identical bits.

Ève knows I_{Eve}.

Privacy Amplification

Alice&Bob share $I_{\text{Bob}} - I_{\text{Eve}}$ identical bits.

Ève knows ~ 0.

Theoretical Progresses in the last 10 years

We went from a protocol

- using squeezed states,
- insecure beyond 50% losses (15 km),
- proved secure against Gaussian individual attack

Theoretical Progresses in the last 10 years

We went from a protocol

- using squeezed states,
- insecure beyond 50% losses (15 km),
- proved secure against Gaussian individual attack

to a protocol

- using coherent states

Theoretical Progresses in the last 10 years

We went from a protocol

- using squeezed states,
- insecure beyond 50% losses (15 km),
- proved secure against Gaussian individual attack

to a protocol

- using coherent states
- with no fundamental range limit
- proved secure against collective attacks

Theoretical Progresses in the last 10 years

We went from a protocol

- using squeezed states,
- insecure beyond 50% losses (15 km),
- proved secure against Gaussian individual attack

to a protocol

- using coherent states
- with no fundamental range limit
- proved secure against collective attacks
- likely secure against coherent attacks

Theoretical Progresses in the last 10 years

We went from a protocol

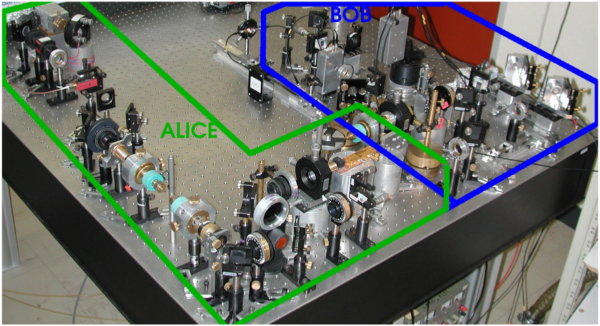
- using squeezed states,
- insecure beyond 50% losses (15 km),
- proved secure against Gaussian individual attack

to a protocol

- using coherent states
- with no fundamental range limit
- proved secure against collective attacks
- likely secure against coherent attacks
- and experimentally working

1st generation demonstrator

F. Grosshans *et. al.*, *Nature* (2003) & Brevet US

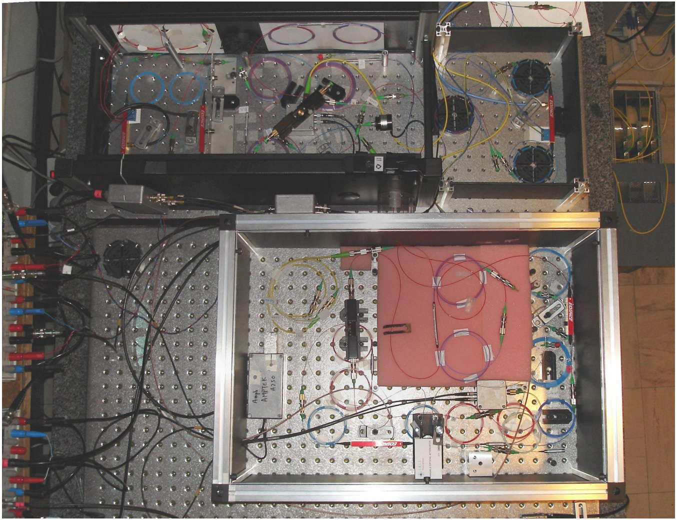


m

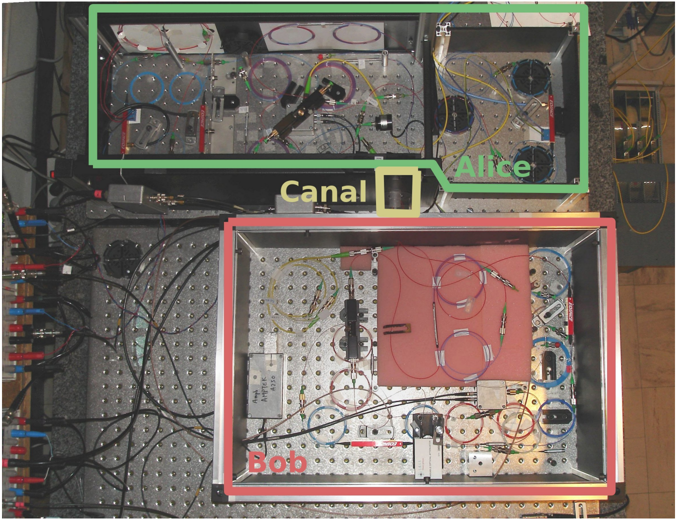
Key rate

- 75 kbit/s 3.1 dB (51%) losses
- 1.7 Mbit/s without losses

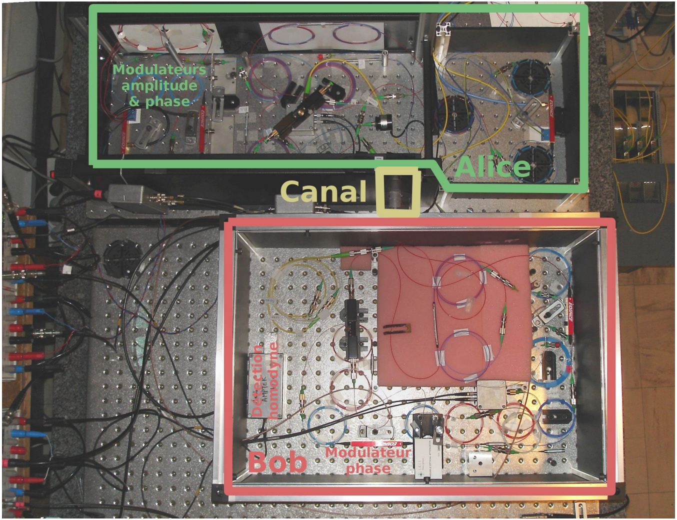
Integrated system



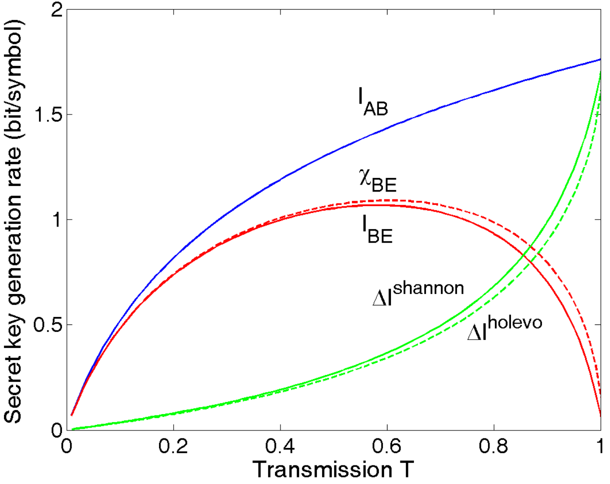
Integrated system



Integrated system

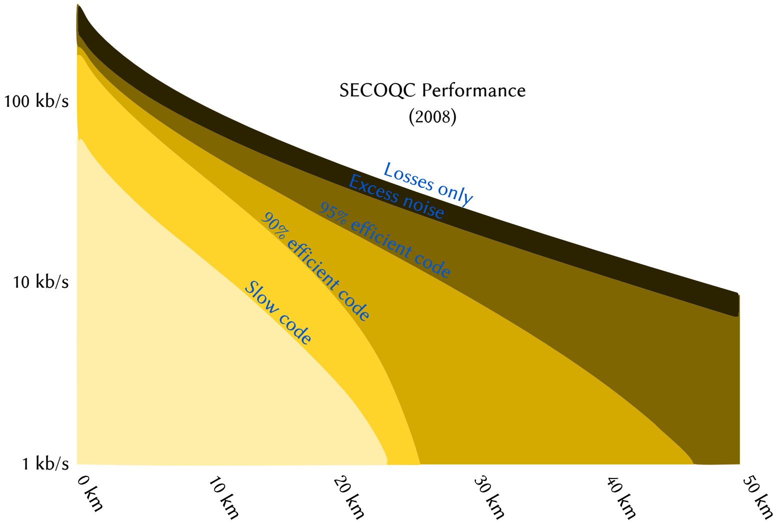


Key-Rates

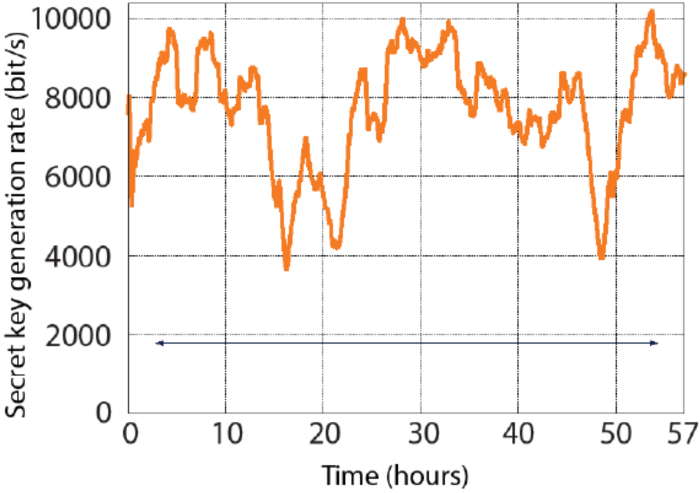


Secret key generation rate (bit/symbol)
Transmission T
I_{AB}
χ_{BE}
I_{BE}
$\Delta I^{shannon}$
ΔI^{holevo}
0
0.5
1
1.5
2
0
0.2
0.4
0.6
0.8
1

Key-Rates

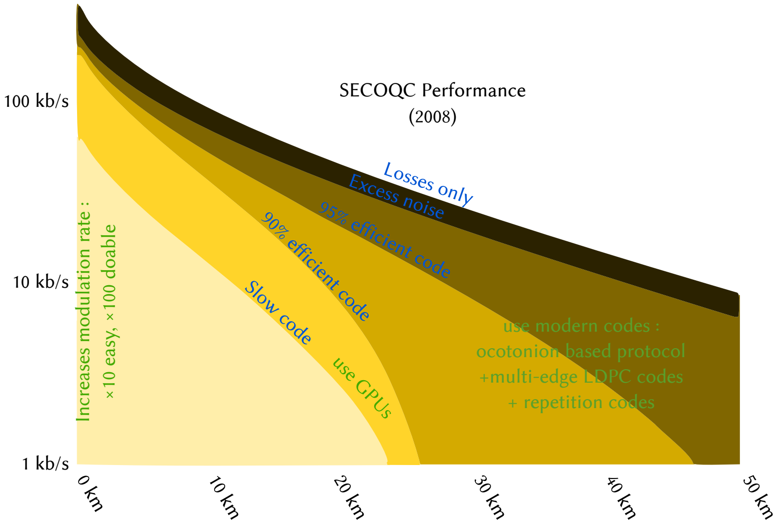

SECOQC Performance
(2008)
100 kb/s
10 kb/s
1 kb/s
0 km
10 km
20 km
30 km
40 km
50 km
Losses only
Excess noise
95% efficient code
90% efficient code
Slow code

Key-Rates

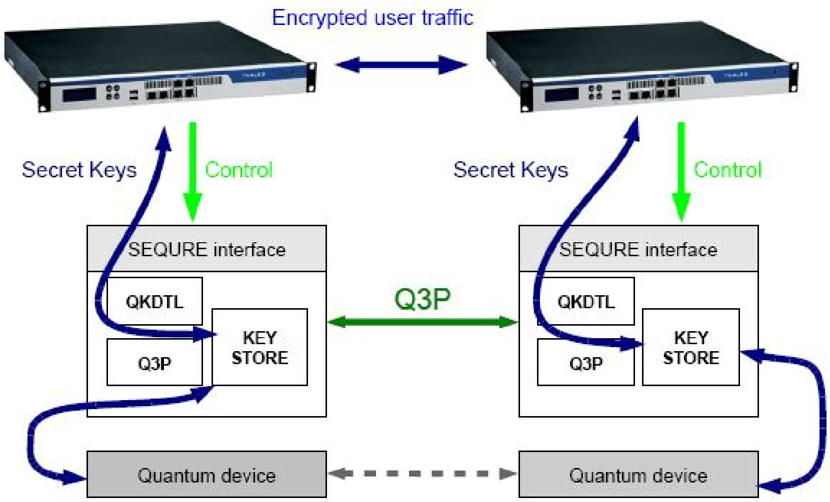


10000
8000
6000
4000
2000
0
Secret key generation rate (bit/s)
0
10
20
30
40
50
57
Time (hours)

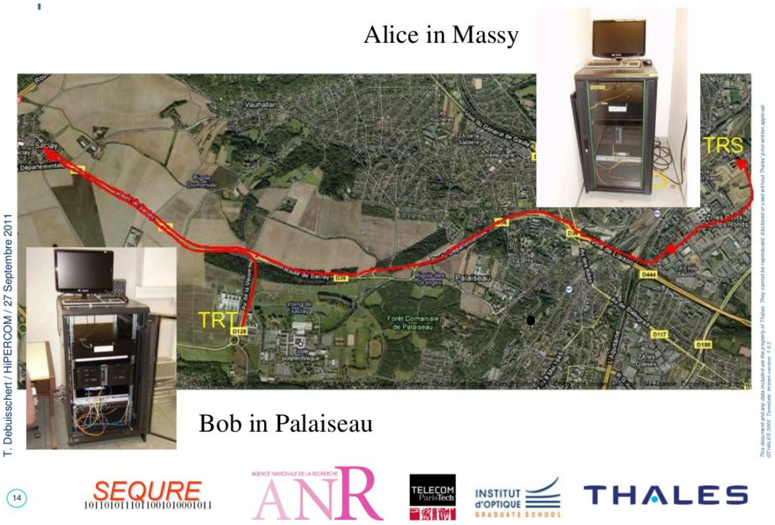
Key-Rates


SECOQC Performance
(2008)
100 kb/s
10 kb/s
1 kb/s
0 km
10 km
20 km
30 km
40 km
50 km
Losses only
Excess noise
95% efficient code
90% efficient code
Slow code
use GPUs
Increases modulation rate :
×10 easy, ×100 doable
use modern codes :
ocotonion based protocol
+multi-edge LDPC codes
+ repetition codes

Integration with classical cryptography



Integration with classical cryptography



Open Problems

- Finite size effects
- Link with post-selection based protocols (`.de`, `.au`)
- Side-channels and quantum hacking
- Other cryptographic applications