



Project Acronym

HIPERCOM

Project Full Title

High Performance Coherent Quantum Communications

September 2011 – August 2014

Coordinated by Nicolas J. Cerf

Kick-Off Seminar, Warsaw, March 7-8, 2012.

HIPERCOM CONSORTIUM

	<i>Partner Number</i>	<i>Country</i>	<i>Institution/ Department</i>	<i>Name of the group leader</i>	<i>Other personnel participating in the project</i>
Th	1 <i>Coord.</i>	Belgium	Université Libre de Bruxelles (ULB) / Centre for Quantum Information and Communication	Nicolas J. Cerf	Evgueni Karpov, Raul Garcia-Patron
Ex	2	France	Institut d'Optique Graduate School (IO) / Laboratoire Charles Fabry	Philippe Grangier	Rosa Tualle-Brouri, Rémi Blandino
Th/Ex	3	Germany	Max Planck Society / Max Planck Institute for the Science of Light (MPL)	Gerd Leuchs	Peter van Loock, Christoph Marquardt
Th	4	UK	University of York (UY) / Computer Science Department	Samuel L. Braunstein	Stefano Pirandola
Th/Ex	5	France	Telecom Paris Tech (TPT) / Laboratoire Traitement et Communication de l'Information	Eleni Diamanti	Damian Markham
Ind	6	France	SeQureNet (SQN)	Sebastien Kunz-Jacques	Paul Jouguet

THRUST OF HIPERCOM

using optical « **continuous variables** » instead of qubits

Bit



Qubit

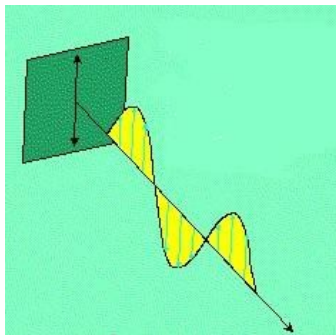


$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle$$

... quantum superposition and entanglement

- The qubit has become the « cornerstone » of quantum information sciences
- All quantum information processes have been developed originally with qubits (cryptography, coding, teleportation, algorithms, etc.)

► BUT several distinct advantages of CV information carriers !



amplitude

e.g., light field: $A \cos(\omega t + \varphi)$

... coherent communications

SPECIFICITIES OF HIPERCOM

Bottom-up approach :

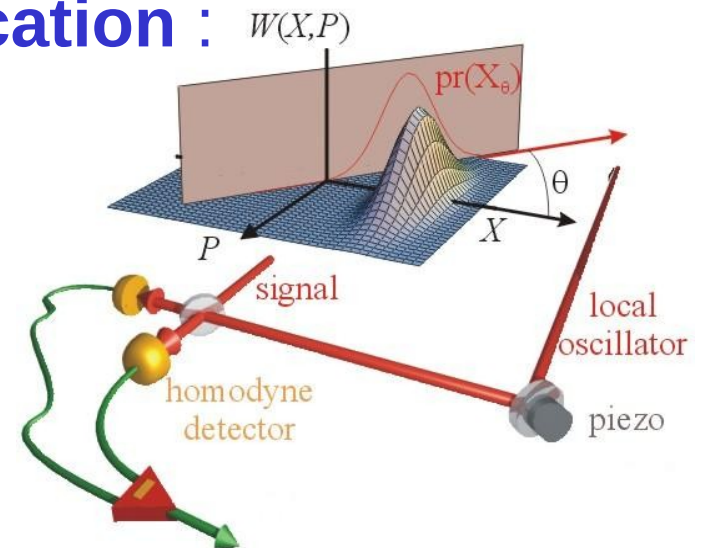
use techniques already proven successful in the lab and build CV information processes based on them (e.g., CV quantum key distribution)

Strong theory – experiments interplay :

devise theoretical concepts together with their experimental demonstration

Builds on classical coherent communication :

main ingredients of optical CV communication are standard high-bandwidth telecom components (e.g., coherent / homodyne detection)



PROMISES OF HIPERCOM

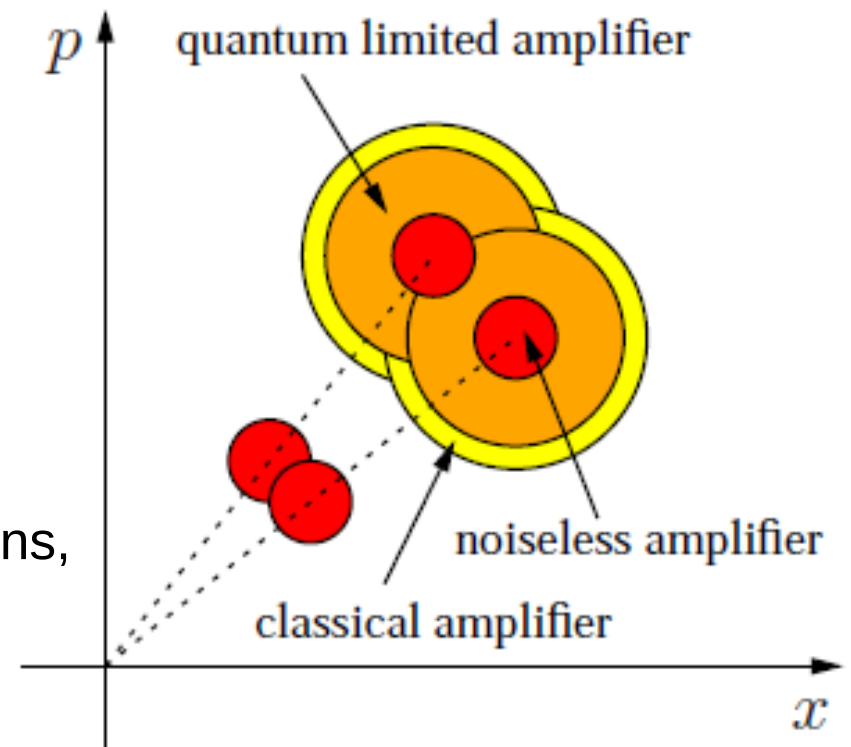
- Focused on coherent quantum communication as a way to combine
- ➡ the **very high rates** achievable by homodyne detection
 - ➡ the **fundamental benefits of quantum mechanics**, such as unconditional security.

The fundamental problem we face is that a **quantum optical amplifier** cannot be used simply as a repeater because it is inherently limited by quantum noise.

The **promise of HIPERCOM** is to explore several techniques aiming at circumventing this problem and enhancing the range of coherent CV quantum communications

with a special emphasis on today's most developed platform towards practical applications, namely CV Quantum Key Distribution

[see Eleni Diamanti's talk]



METHODOLOGY OF HIPERCOM

Different strategies will be followed in order to approach long-distance coherent CV quantum communications

ranging from the use of classical coding and other post-processing algorithms, which is the most directly applicable solution in the short term, to more elaborate longer-term techniques relying on specific quantum optical schemes and ultimately on the use of quantum coding.

In between these two extreme approaches, the potential solution offered by the noiseless linear amplifier or similar heralded operations will be investigated.

WP1 : Improve classical and optical post-processing
(e.g. classical coding, bidirectional protocols)

WP2 : Beyond classical coding but exper. accessible
(e.g. noiseless amplifier & other heralded proc.)

WP3 : Full quantum solution to range enhancement
(e.g. quantum coding, non-Gaussian CV codes)

applicable
with today's
techniques



longer-term
more theoretical
investigation

Workpackage 1 :

The first workpackage (divided in WP1a/b) is the most directly applicable one for realistic systems, so that the industrial partner plays a large role therein. It mainly focuses on quantum key distribution, viewed as the quantum communication platform that is the closest to applications today [20]. The objective is to enhance the range and the rate of continuous-variable quantum key distribution (CV-QKD) schemes, and to demonstrate the feasibility of these improved schemes. Both the optical and classical post-processing aspects will be covered, as well as new (fully general) approaches to the security analysis. The basic idea here is that classical coding, although it is not the ultimate solution, may already be quite an interesting tool for enhancing the distance. The advantage, of course, is that the quantum optical features remain simple and well mastered, while the range- and rate-enhancement effect essentially results from the improved classical coding. An alternative approach that will also be explored is to resort to optical schemes that involve a double (bidirectional) quantum communication.

Workpackage 2 :

In the second workpackage (divided in WP2a/b), we will go one step further and investigate techniques that go beyond classical coding, while they do not reach quantum coding. We will in particular spend a significant part of this workpackage to explore the promises of the concept of “heralded noiseless linear amplifier” [21], which was discovered only recently and may be a very elegant tool towards range enhancement. More generally, we will study the so-called heralded quantum operations, that is, operations that are obtained conditionally on detection events and may go beyond some limitation. This is, for example, the way the noiseless amplifier works, while a deterministic version of this process is forbidden by quantum mechanics. This is also a known method to generate non-Gaussian operations with linear optics components, which otherwise can only effect Gaussian operations. So, although this workpackage will be more theoretically oriented than the first one, it will also contain a significant experimental component based of the established expertise of the project partners. We will in particular focus on the realization of heralded non-Gaussian operations and gates.

Workpackage 3 :

In the third workpackage (WP3), we will address the full quantum solution to this range-enhancement problem, namely quantum coding [22]. Given its more prospective approach, this workpackage will be mostly theoretical. We will explore whether practical continuous-variable quantum codes could be devised to in different scenarios, including non-Gaussian codes, and whether the so-called concatenation of codes may provide an interesting solution here. This will finally lead us to investigate very fundamental questions such as the ultimate limit of coherent quantum communication in optical channels, the so-called channel capacity, which is asymptotically reached using an optimal quantum code.

EXPECTED OUTCOMES OF HIPERCOM

Theoretical progresses on coherent quantum communications

quantum coding, Gaussian channel capacities, general security proofs of CV-QKD (incl. side-channels and other security loopholes)

Experimental demonstrations of heralded non-Gaussian quantum processes

(noiseless linear amplifier & beyond ; its application to CV-QKD)

New practical realizations of CV-QKD platforms

working over longer distances and with stronger security assessment

 pave the way towards long-distance coherent CV quantum communications

KNOWLEDGE DISSEMINATION

WP0 : Management & organization of annual workshop in the series :

Continuous-variable Quantum Information Processing CV-QIP

HIPERCOM kick-off meeting, Telecom ParisTech, Paris, September 26-27, 2011, organized by Eleni Diamanti, was widened with non-HIPERCOM invited speakers so it was turned into

[8th CV-QIP workshop](#)

The next CV-QIP workshop will take place in Copenhagen, April 27-30, 2012 with approximately half of the attendance from the HIPERCOM consortium (+ non-HIPERCOM speakers & overseas experts).

Outline of the rest of this talk

(2 selected results so far)

- Other heralded process: phase-insensitive squeezing of light
Probabilistic scheme that always enhances squeezing,
regardless of the quadrature that is initially squeezed !

(ULB) [this talk]

- CV-QKD experimental platform
Progress on classical coding & optical implementation

(TNT & SQN) [Eleni Diamanti's talk]

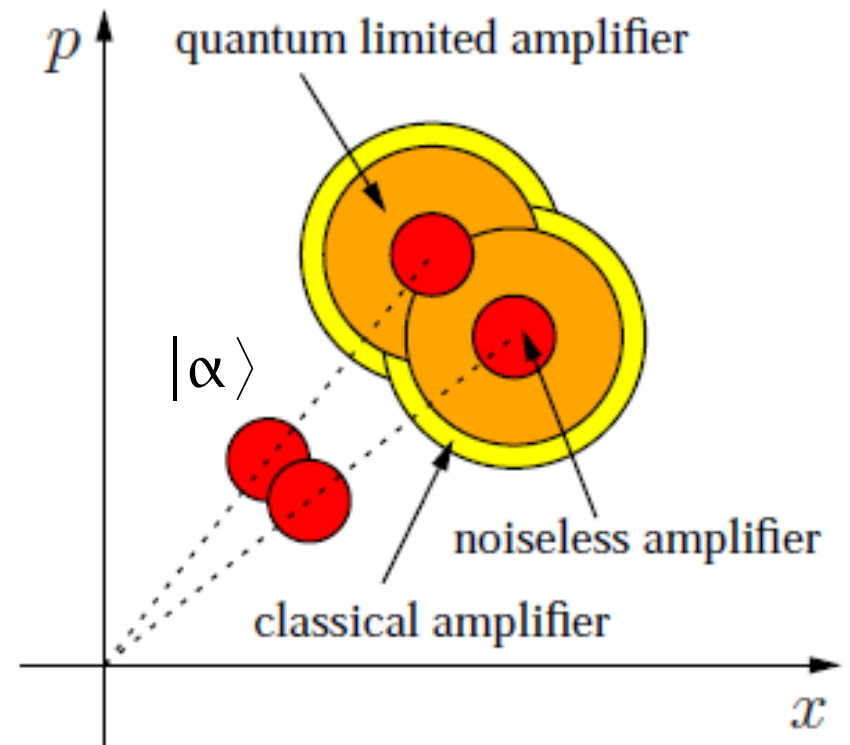
TOPIC 1. Amplification of light

1. Optimal classical amplifier

$$|\alpha\rangle \rightarrow \alpha + \text{noise} \rightarrow |g\alpha\rangle + \text{noise}$$

where $g > 1$ is amplitude gain

(heterodyne) measure and prepare



2. Optimal quantum-noise limited amplifier

$$\hat{a}_{out} = g \hat{a}_{in} + \sqrt{g^2 - 1} \hat{b}^+ \quad (\text{C. Caves, PRD, 1982})$$

added vacuum noise

3. Noiseless linear amplifier ???

$|\alpha\rangle \rightarrow |g\alpha\rangle$... **unphysical operation for $g > 1$**
... **cannot be implemented exactly and deterministically**

Probabilistic noiseless amplification of coherent states

T.C. Ralph and A.P. Lund, in: Quantum Communication Measurement and Computing, Proc. of 9th Int. Conf., ed. A. Lvovsky, 155-160 (AIP, New York, 2009).

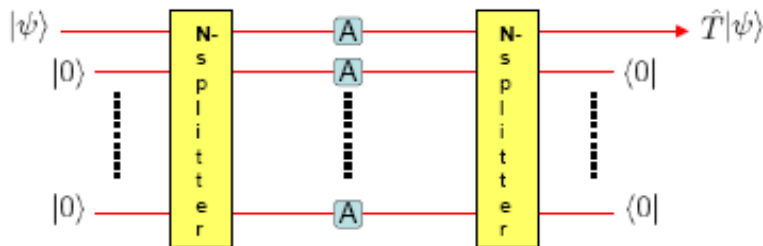
... a non-deterministic non-unitary transformation may work

$$|\alpha\rangle\langle\alpha| \rightarrow \rho_\alpha = P_{\text{success}} |g\alpha\rangle\langle g\alpha| + (1 - P_{\text{success}}) |0\rangle\langle 0|$$

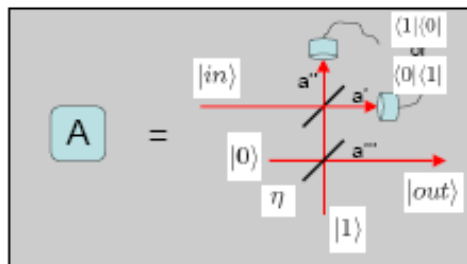
heralded
vacuum when failure

... overall, it cannot increase distinguishability between $|0\rangle$ and $|\alpha\rangle$

$$|\langle 0|\alpha\rangle|^2 \leq \langle 0|\rho_\alpha|0\rangle = P_{\text{success}} |\langle 0|g\alpha\rangle|^2 + (1 - P_{\text{success}})$$



$$P_{\text{success}} \leq \frac{1 - e^{-|\alpha|^2}}{1 - e^{-|g\alpha|^2}}$$



Heralded Noiseless Linear Amplifier (HNLA)

How does it work ?

Target non-unitary “*amplification*” operation

$$|n\rangle \rightarrow g^{\hat{n}} |n\rangle \quad \text{with } g > 1$$

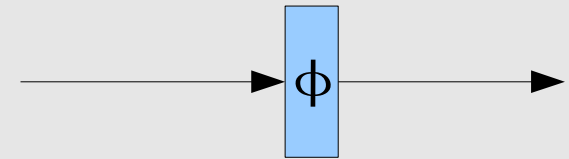
filtration in Fock basis

$$\{ |0\rangle, |1\rangle, |2\rangle, \dots \}$$

This operator is **unbounded**, so it cannot be implemented exactly,
albeit with a zero success probability !

However, an **approximate truncated version** in space $\{|0\rangle, |1\rangle, \dots, |N\rangle\}$
with non-zero success probability is physical !

“complex phase plate”



$$e^{i\phi\hat{n}}$$

$$\text{with } \phi = -i \ln(g)$$

truncation

Ideal (near-zero success probability) noiseless amplifier

$|n\rangle \rightarrow c g^{\hat{n}} |n\rangle$ in infinite-dimensional space $\{|0\rangle, |1\rangle, |2\rangle, \dots\}$

where $c \rightarrow 0$ is normalization constant

$$\begin{aligned} |\alpha\rangle &\rightarrow c g^{\hat{n}} e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \\ &= c e^{(g^2-1)|\alpha|^2/2} e^{-|g\alpha|^2/2} \sum_{n=0}^{\infty} \frac{(g\alpha)^n}{\sqrt{n!}} |n\rangle \end{aligned}$$

filtration

$|g\alpha\rangle$

$$\alpha \rightarrow \alpha' = g\alpha$$

$$P_{\text{success}} = |c|^2 e^{(g^2-1)|\alpha|^2}$$

(diverges as $\alpha \rightarrow \infty$,
so $c \rightarrow 0$ if no truncation)

Physical approximation to this ideal target operation

- Truncation based on “quantum scissors” $\{|0\rangle, |1\rangle, \dots, |N\rangle\}$

Xiang, Ralph, Lund, Walk, and Pryde, Nature Photonics **4**, 316 (2010).

Ferreyrol, Barbieri, Blandino, Fossier, Tualle-Brouri, and Grangier, PRL **104**, 123603 (2010).

- Amplification based on photon “addition” and “subtraction”

Zavatta, Fiurášek, Bellini, Nature Photonics **5**, 52 (2011).

$$g^{\hat{n}} = (1 + (g - 1))^{\hat{n}} \approx 1 + (g - 1)\hat{n} = (g - 2)\hat{a}^+ \hat{a} + \hat{a} \hat{a}^+$$

... keep only 1st order term

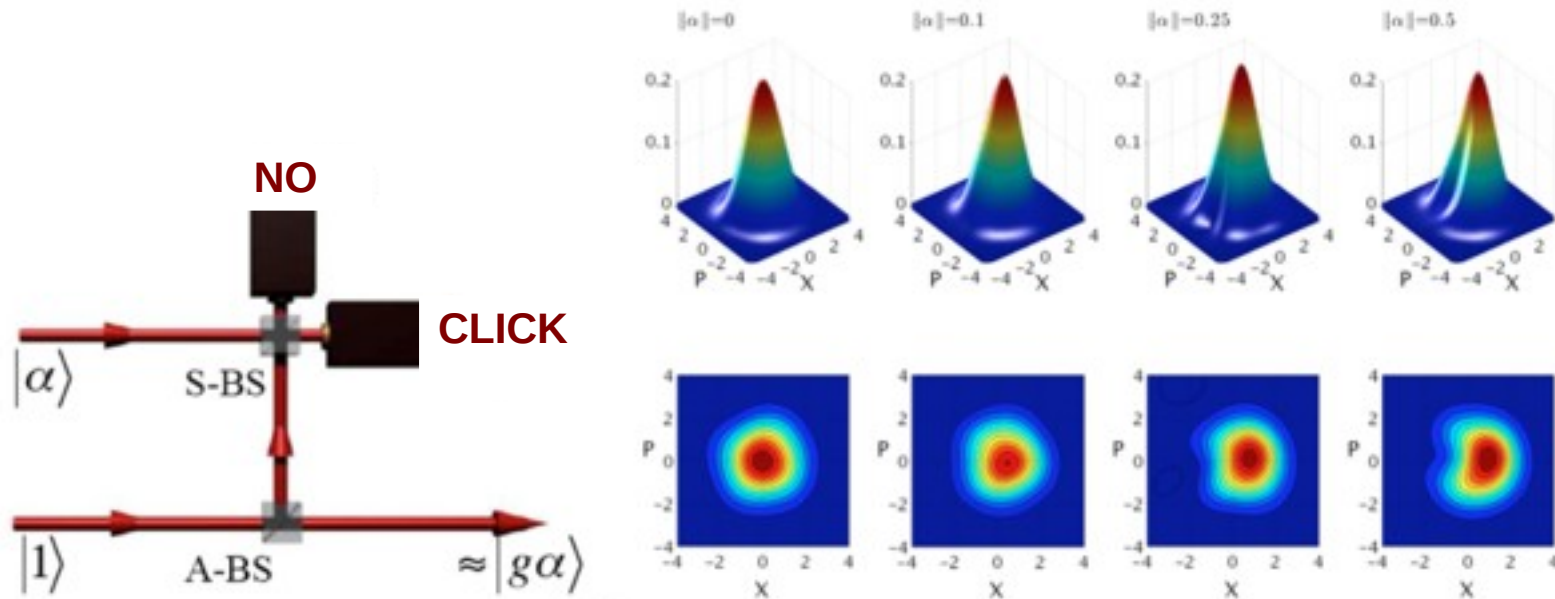
... very crude approximation, works well only for $|g| \ll 1$

for $g = 2$ one has simply $g^{\hat{n}} = \hat{a} \hat{a}^+$ (addition then subtraction)

Experimental demonstration (Palaiseau)

Truncation to space spanned by vacuum and single-photon state

$$|\alpha\rangle \simeq |0\rangle + \alpha|1\rangle \rightarrow |0\rangle + g\alpha|1\rangle$$

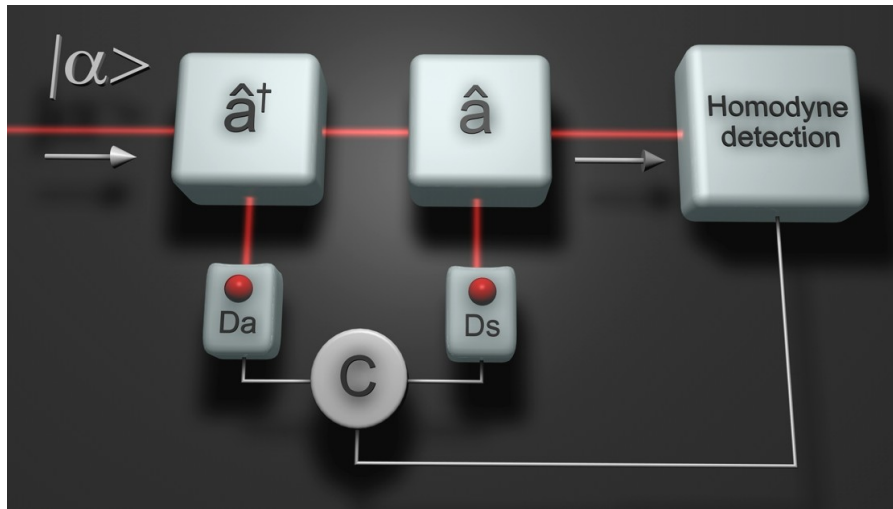


$$\left(t|1\rangle_T|0\rangle_R + r|0\rangle_T|1\rangle_R \right) \left(|0\rangle_{\text{in}} + \alpha|1\rangle_{\text{in}} \right) \rightarrow r|0\rangle_T + t\alpha|1\rangle_T \propto |0\rangle_T + g\alpha|1\rangle_T$$

... choose $t/r = g$

The performance may be improved by a complex interferometric scheme involving multiple quantum scissors – extremely difficult to implement.

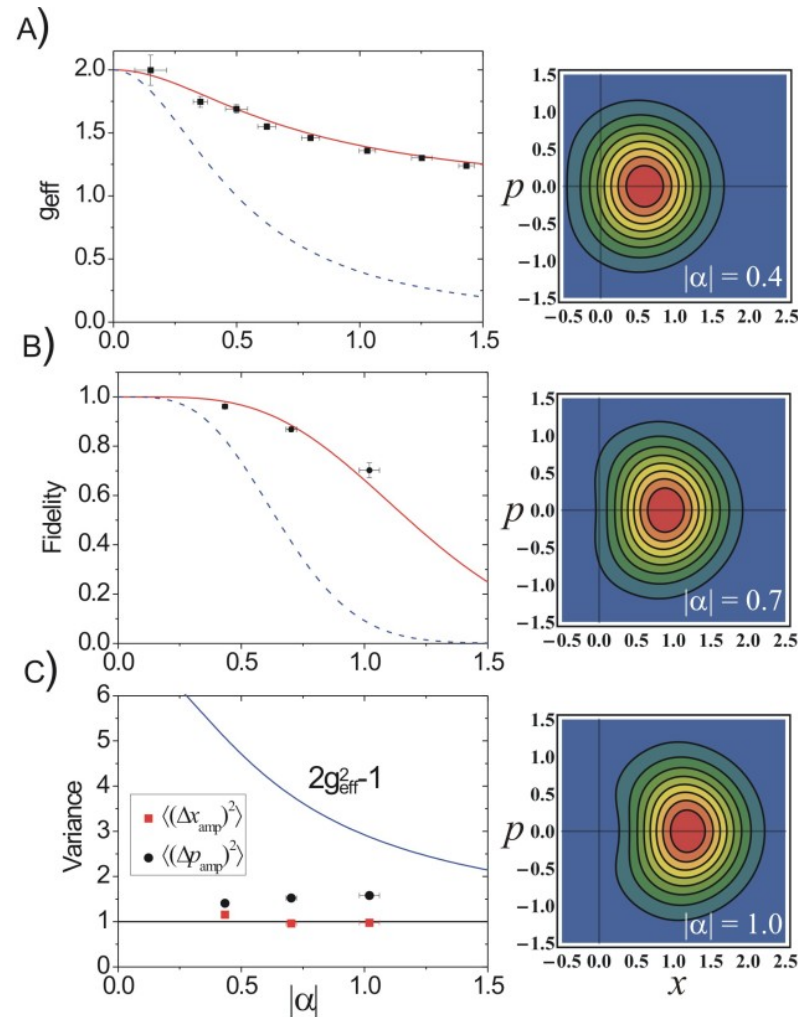
Experimental demonstration (Florence)



$$g^{\hat{n}} \approx (g-2)\hat{a}^+ \hat{a} + \hat{a} \hat{a}^+ = (g-1)\hat{n} + 1$$

↓

$$\hat{G}_{g=2} = \hat{a} \hat{a}^\dagger$$

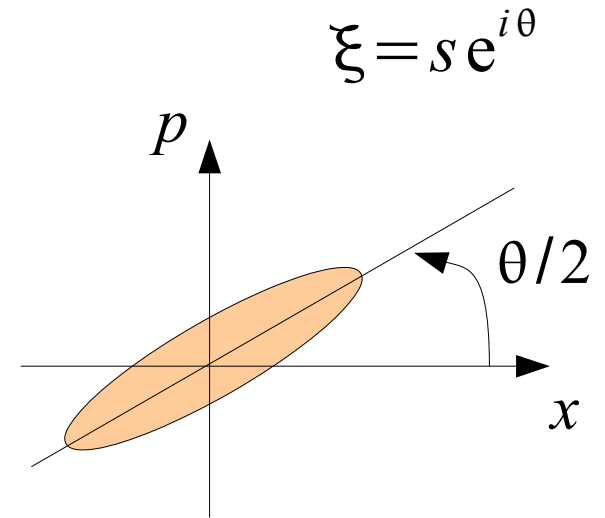


$$|\alpha\rangle = |0\rangle + \alpha|1\rangle \quad \hat{a}\hat{a}^\dagger(|0\rangle + \alpha|1\rangle) \rightarrow \hat{a}(|1\rangle + \sqrt{2}\alpha|2\rangle) \rightarrow |0\rangle + 2\alpha|1\rangle$$

Probabilistic phase-insensitive squeezer

$||\xi, 0\rangle\rangle \equiv S(\xi) |0\rangle$ vacuum squeezed state

with $S(\xi) = \exp((\xi^* \hat{a}^2 - \xi \hat{a}^{+2})/2)$



$||\xi, 0\rangle\rangle$

$$\begin{aligned}
 ||\xi, 0\rangle\rangle &\rightarrow c g^{\hat{n}} \underbrace{\frac{1}{\sqrt{\cosh(s)}} \sum_{n=0}^{\infty} \sqrt{\binom{2n}{n}} \left(\frac{1}{2} e^{i\theta} \tanh(s) \right)^n |2n\rangle}_{\propto ||\xi', 0\rangle\rangle} \\
 &= c \frac{1}{\sqrt{\cosh(s)}} \sum_{n=0}^{\infty} \sqrt{\binom{2n}{n}} \underbrace{\left(\frac{1}{2} e^{i\theta} g^2 \tanh(s) \right)^n}_{\propto ||\xi', 0\rangle\rangle} |2n\rangle
 \end{aligned}$$

$$\xi \rightarrow \xi' = s' e^{i\theta'}$$

$$s \rightarrow s' > s \quad \text{s. t.} \quad \tanh(s') = g^2 \tanh(s)$$

$$\theta \rightarrow \theta' = \theta$$

**stronger squeezing
of the same quadrature,
regardless of θ**

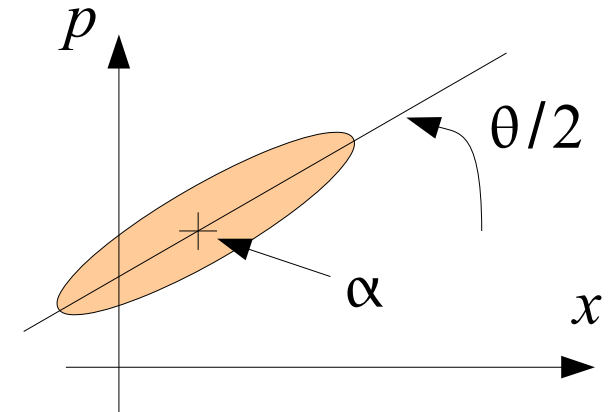
$||\xi, \alpha\rangle\rangle \equiv D(\alpha)S(\xi)|0\rangle$ squeezed coherent state

$$\xi = s e^{i\theta}$$

with $D(\alpha) = \exp(\alpha \hat{a}^+ - \alpha^* \hat{a})$

$$||\xi, \alpha\rangle\rangle = \frac{1}{\sqrt{\cosh(s)}} \sum_{n=0}^{\infty} \sqrt{\frac{1}{n!}} \left(\frac{1}{2} e^{i\theta} \tanh(s) \right)^{n/2}$$

$$\times e^{-\left(|\alpha|^2 - \alpha^{*2} e^{i\theta} \tanh(s)\right)/2} H_n \left(\frac{\alpha + \alpha^* e^{i\theta} \tanh(s)}{(2 e^{i\theta} \tanh(s))^{1/2}} \right) |n\rangle$$



$$||\xi, \alpha\rangle\rangle \rightarrow ||\xi', \alpha'\rangle\rangle$$

Hermite polynomial

same $\xi' = s' e^{i\theta'}$ as before

$$\alpha \rightarrow \alpha' \begin{cases} x_{\alpha} \rightarrow x_{\alpha}' = g x_{\alpha} \frac{1 + e^{i\theta} \tanh(s)}{1 + e^{i\theta} g^2 \tanh(s)} \\ p_{\alpha} \rightarrow p_{\alpha}' = g p_{\alpha} \frac{1 - e^{i\theta} \tanh(s)}{1 - e^{i\theta} g^2 \tanh(s)} \end{cases}$$

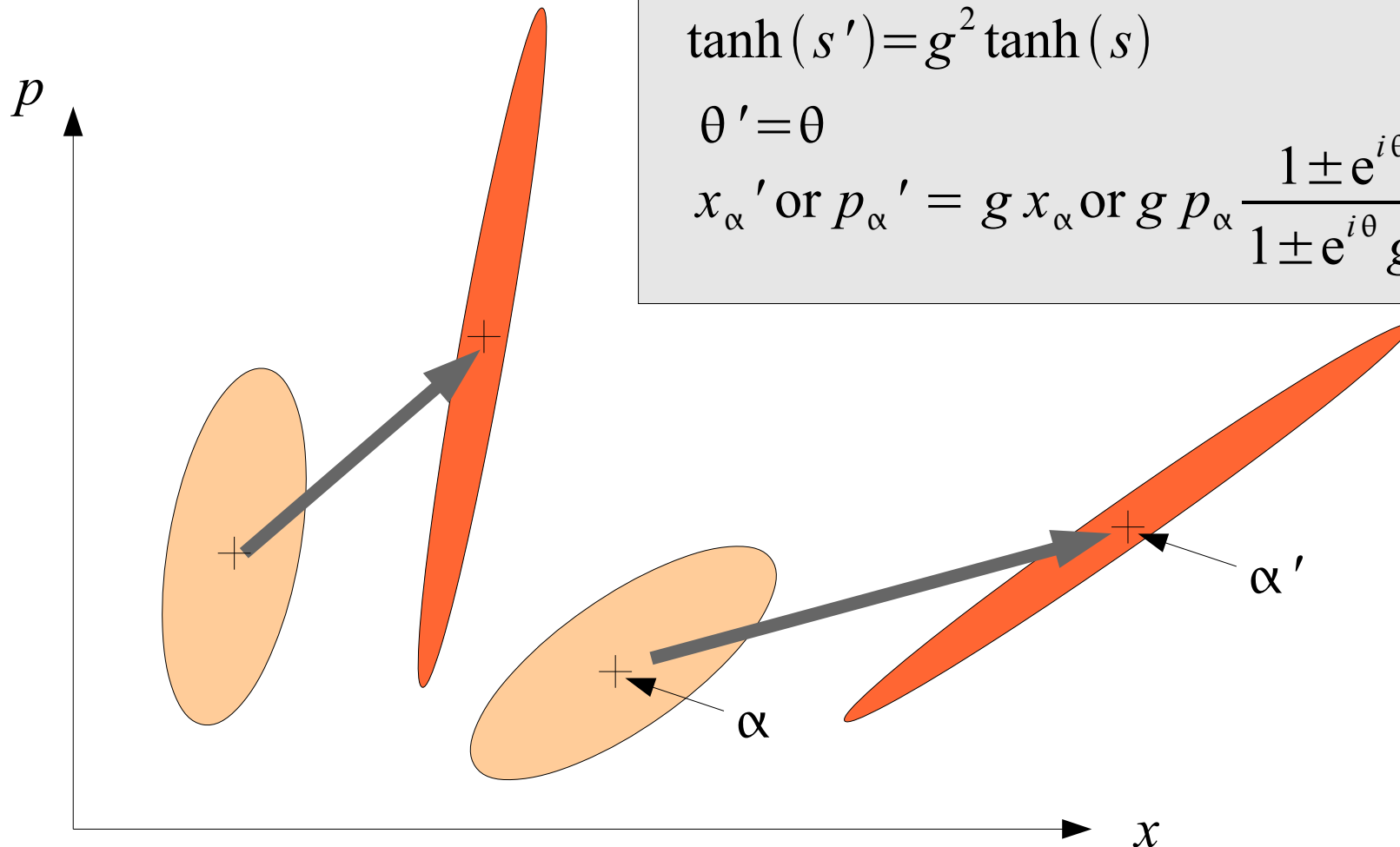
“Universal” (but heralded) single-mode squeezer

$$||\xi, \alpha\rangle\rangle \begin{cases} \xi = s e^{i\theta} \\ \alpha = (x_\alpha + i p_\alpha)/2 \end{cases} \longrightarrow ||\xi', \alpha'\rangle\rangle \begin{cases} \xi' = s' e^{i\theta'} \\ \alpha' = (x_{\alpha'} + i p_{\alpha'})/2 \end{cases}$$

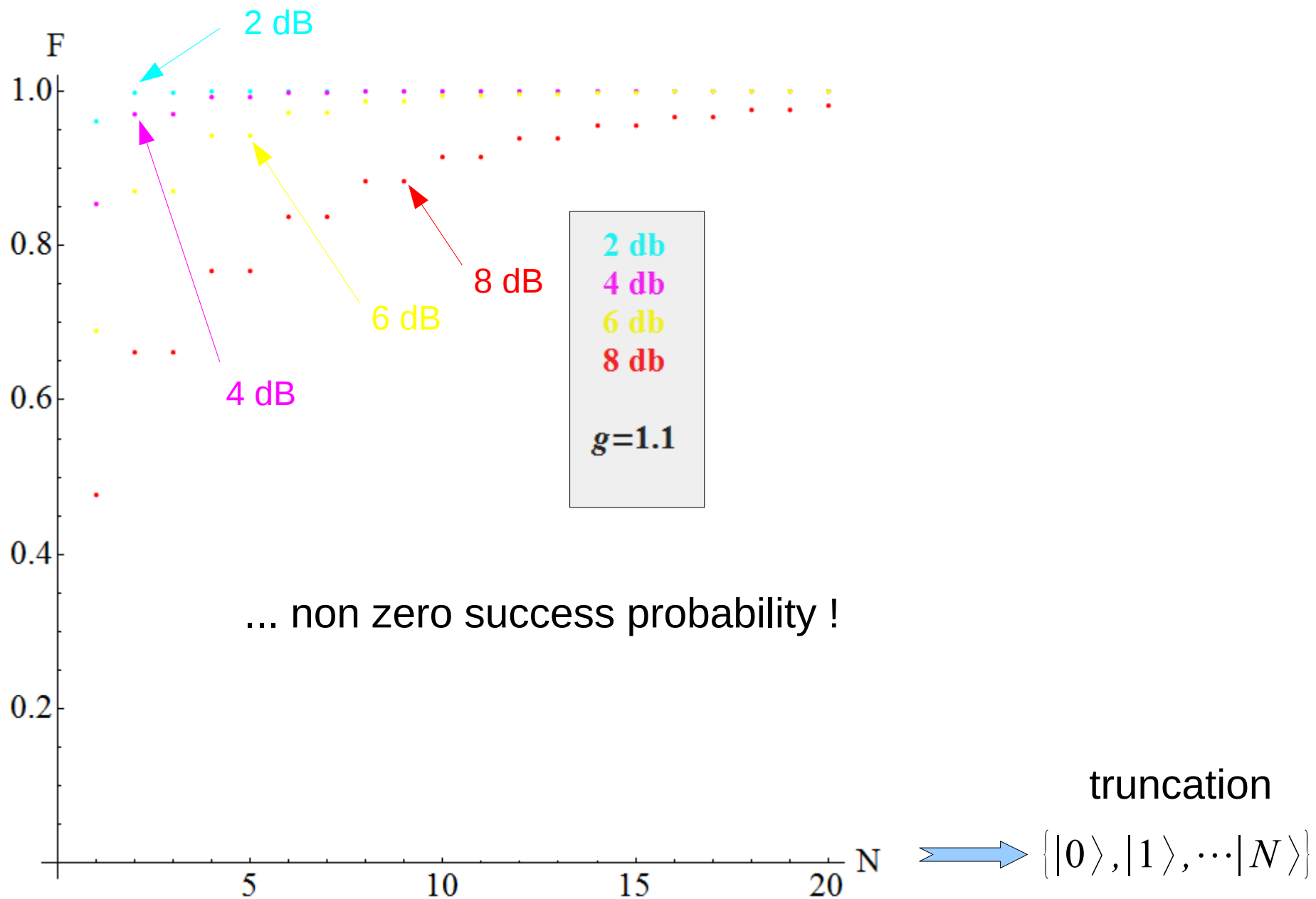
$$\tanh(s') = g^2 \tanh(s)$$

$$\theta' = \theta$$

$$x_{\alpha'} \text{ or } p_{\alpha'} = g x_\alpha \text{ or } g p_\alpha \frac{1 \pm e^{i\theta} \tanh(s)}{1 \pm e^{i\theta} g^2 \tanh(s)}$$



Fidelity of physical (truncated) universal squeezer



Use of phase-insensitive squeezer

- Possible applications ???
 - improved phase estimation
 - probabilistic high-fidelity cloning
 - CV entanglement concentration or distillation
 - CV quantum error correction (compensation of losses)
 - breeding of Schrödinger cat states of light
 - etc...
- Fundamental questions ???
 - link with perfect cloning and causality
 - etc...

TOPIC 2: Continuous-variable distribution

- Existence of general security proofs
- Standard components compatible with telecom networks
- Competitive secret key rate performance
- WDM friendly

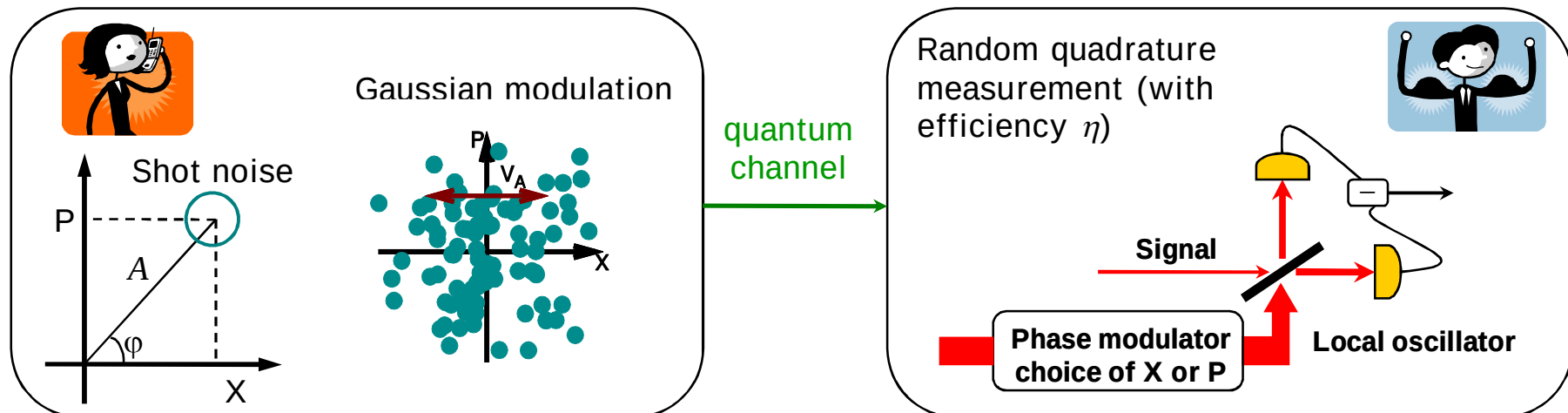
but...

- Relatively recent technology
- Complex post-processing
- Finite-size effects
- Short secure distance

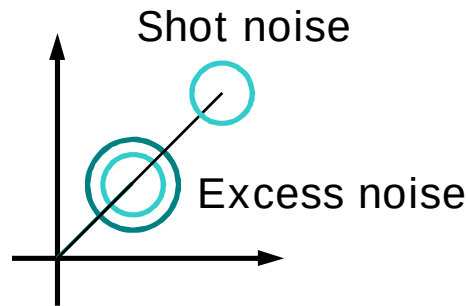
QKD with coherent states

- Quantum key distribution offers, in principle, **information-theoretic security**
- In CVQKD, Alice encodes key information in **quantum continuous variables** → **random modulation** of the **amplitude and phase** of coherent states
- Bob **measures randomly** the quadrature of each coherent state with a **homodyne detection system**

N. J. Cerf, M. Levy, G. Van Assche, Phys. Rev. A 2001
F. Grosshans and P. Grangier, Phys. Rev. Lett. 2002



Protocol security



- In the **Gaussian channel mode**, coherent states are modified by **losses and excess noise**
- These are introduced by Eve and degrade the signal-to-noise ratio (SNR) → her presence is revealed by **noise variance measurements**

- Shannon's theory links the information exchanged between Alice and Bob, and the SNR

$$I_{AB} = \frac{1}{2} \log_2 (1 + \text{SNR}) = \frac{1}{2} \log_2 \left(1 + \frac{\eta T V_A}{1 + \eta T \xi} \right)$$

- Eve's information on **Bob's key (reverse reconciliation)** is bounded using a **Heisenberg inequality**

$$I_{BE} \leq \frac{1}{2} \log_2 \frac{\eta T V_A + 1 + \eta T \xi}{\eta / \left(1 - T + T \xi + \frac{T}{V_A + 1} \right) + 1 - \eta}$$

- All parameters (V_A, η, T, ξ) are known to or measured by Alice and Bob

Secret key generation rate:

$$\Delta I = I_{AB} - I_{BE} > 0, \text{ for any transmission } T, \text{ if } \xi < \frac{V_A}{2(1 + V_A)}$$

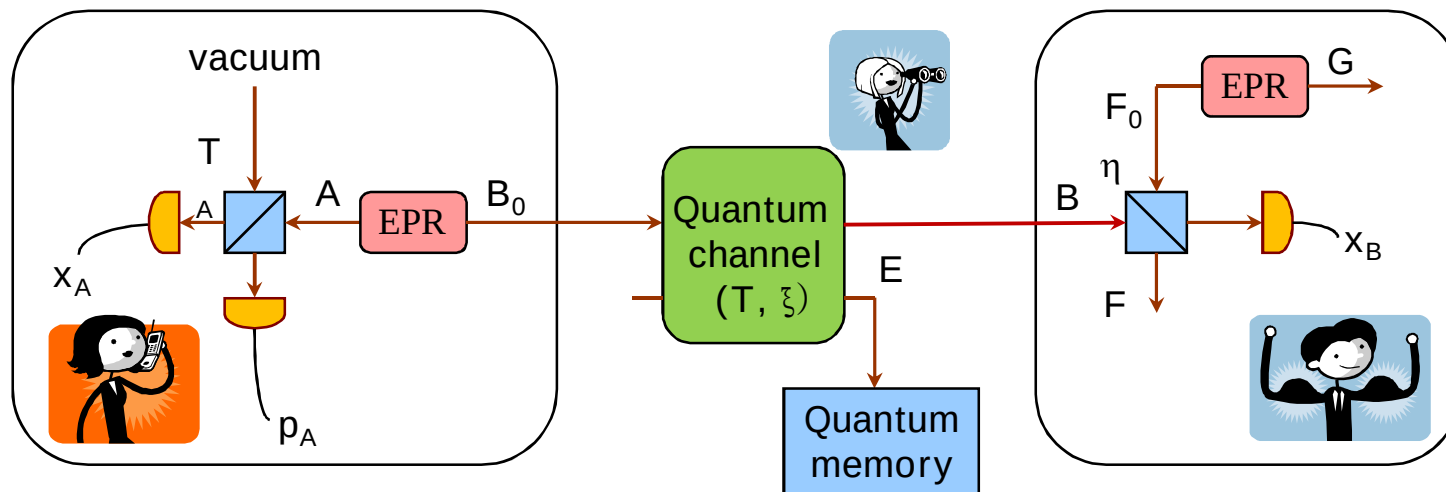
- Security proof applies to **individual, Gaussian attacks**

F. Grosshans et al, Nature 2003

- Security for **general collective attacks**

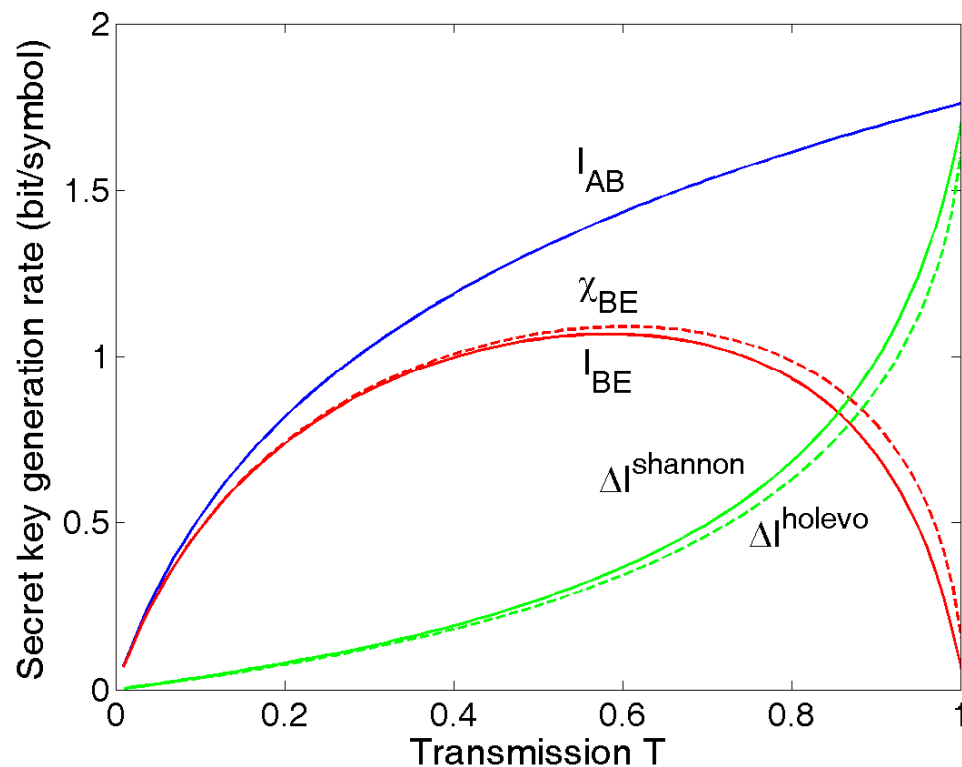
F. Grosshans, Phys. Rev. Lett. 2005

M. Navasques and A. Acin, Phys. Rev. Lett. 2005



Equivalent entanglement-based protocol + imperfect detector model

→ upper bound Eve's accessible information using appropriate **Holevo quantity** 4



$V_A = 21$ (shot noise units)
 $\xi = 0.005$ (shot noise units)
 $\eta = 0.5$

- For both individual and collective attacks, **Gaussian attacks are optimal**
 F. Grosshans and N. J. Cerf, Phys. Rev. Lett. 2004
 M. Navasques, F. Grosshans and A. Acin, Phys. Rev. Lett. 2006
 R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. 2006
 N. J. Cerf and P. Grangier, JOSA B 2007 (review)
- Alice and Bob assume that **Eve's attack is Gaussian** and estimate her information using the **Shannon** I_{BE} or the **Holevo quantity** χ_{BE}

Information-theoretic security

- Extension of **de Finetti theorem to infinite dimensional systems**, holds if certain experimentally verifiable conditions are satisfied

R. Renner and J. I. Cirac, Phys. Rev. Lett. 2009

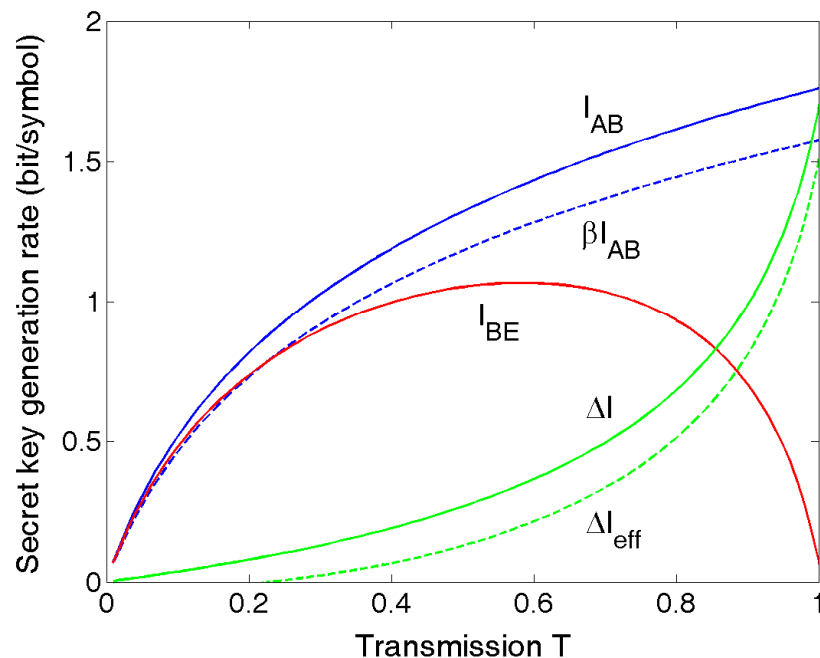
→ the derived bounds for the achievable secret key generation rate against collective attacks are **asymptotically valid for arbitrary coherent states**

V. Scarani et al, Rev. Mod. Phys. 2009

- There is a wealth of other coherent state QKD protocols, for example with **post-selection** or **discrete modulation**, with more or less advanced security proof status

Reconciliation of correlated Gaussian variables

- After the quantum transmission, Alice and Bob share a set of **correlated quadrature measurements**
- To **distill a secret string of bits**, they need to:
 - Discretize their data to obtain discrete symbols → **slice algorithm**
 - Correct the errors (reconciliation) → **multi-level iterative soft decoding using Low Density Parity Check (LDPC) codes**
 - Eliminate any remaining key information available to Eve (privacy amplification) → **universal hash functions**



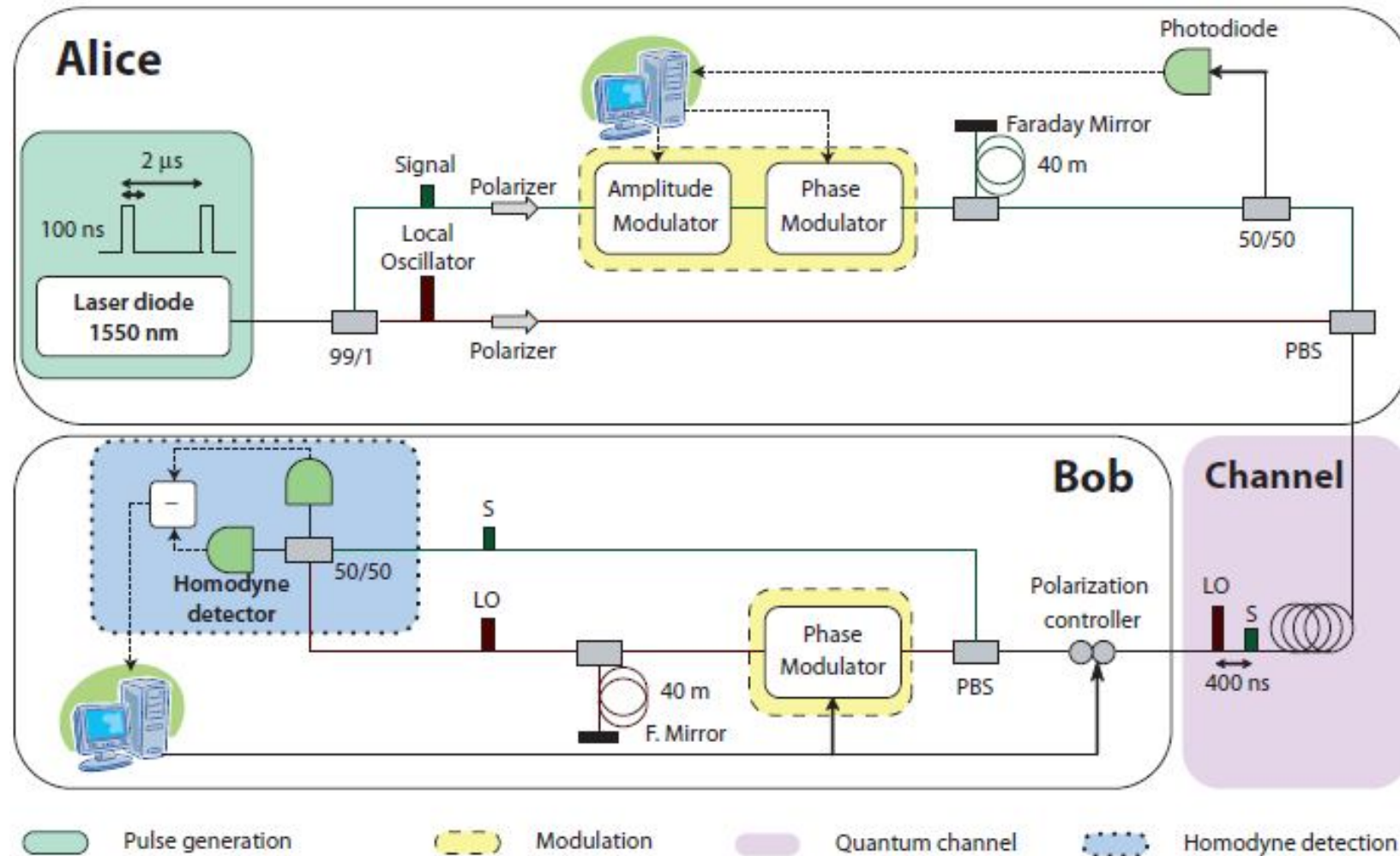
- Communication **distance limited by reconciliation efficiency:**

$$\Delta I_{\text{eff}} = \beta I_{AB} - I_{BE} < 0$$

for small transmission efficiency

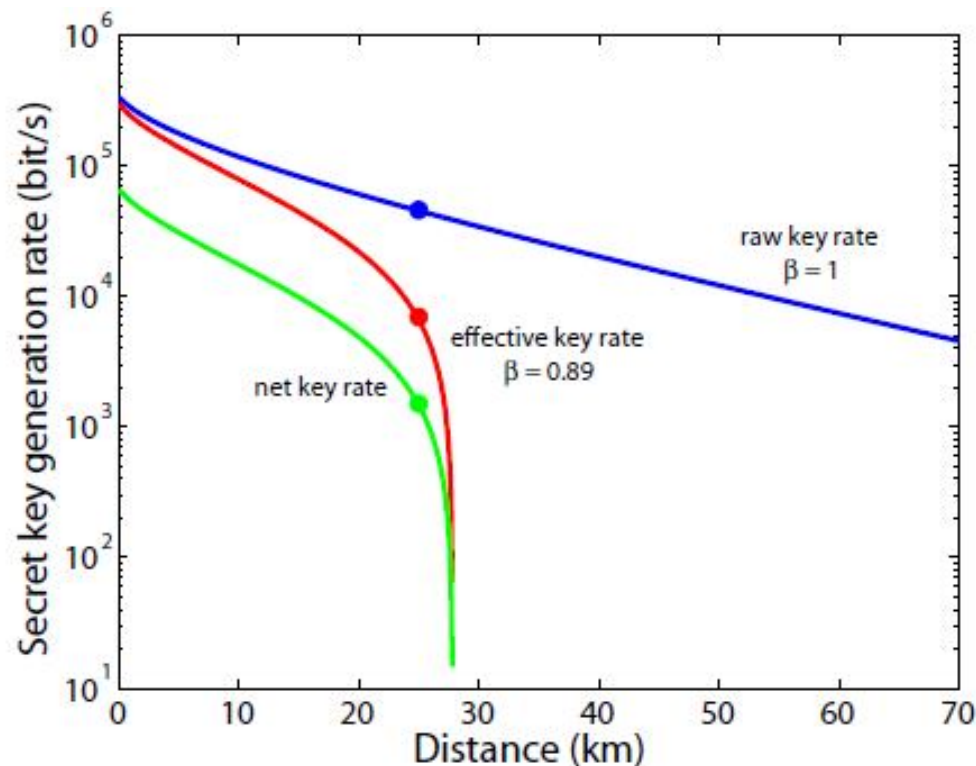
$$\begin{aligned} V_A &= 21 \\ \xi &= 0.005 \\ \eta &= 0.5 \\ \beta &= 0.89 \end{aligned}$$

The CVQKD prototype: optical setup



The CVQKD prototype: experimental setup

Stable and automatic operation
Robust and compact prototype
Standard telecom components
Real time secret key generation



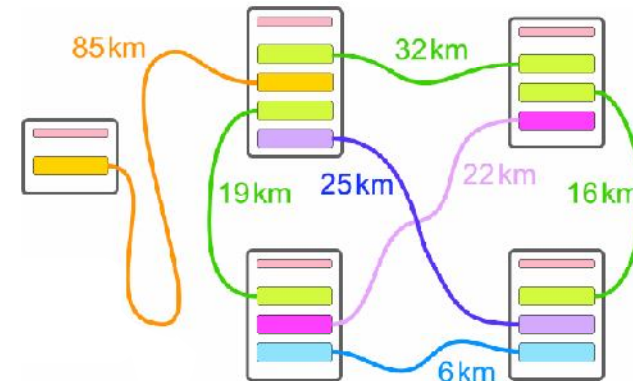
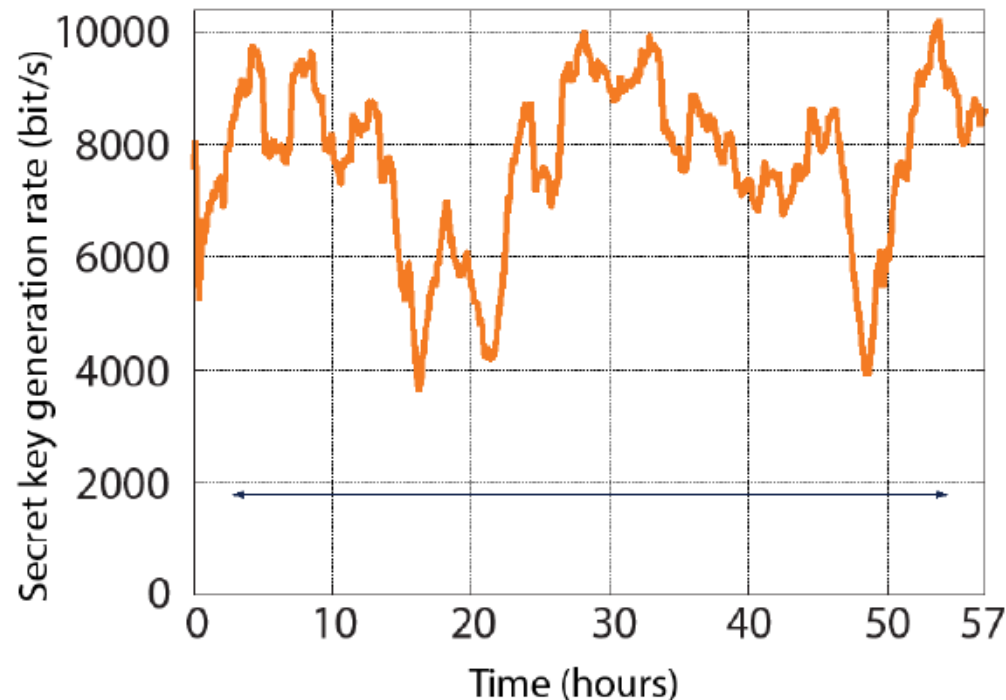
Performance (2 kbit/s @ 25km)
limited by reconciliation
efficiency and execution speed

J. Lodewyck et al, Phys. Rev. A 2007

S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Broui, P. Grangier, J. Phys. B 2009

Application to the SECOQC network

Integration of various QKD technologies into the first European quantum cryptography network, installed over the Siemens fiber infrastructure in Vienna, October 2008

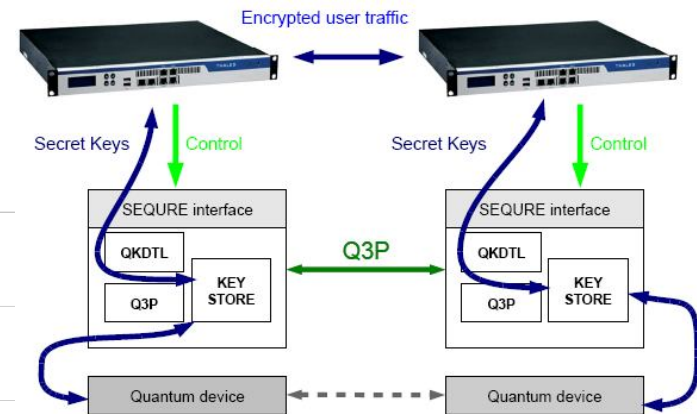
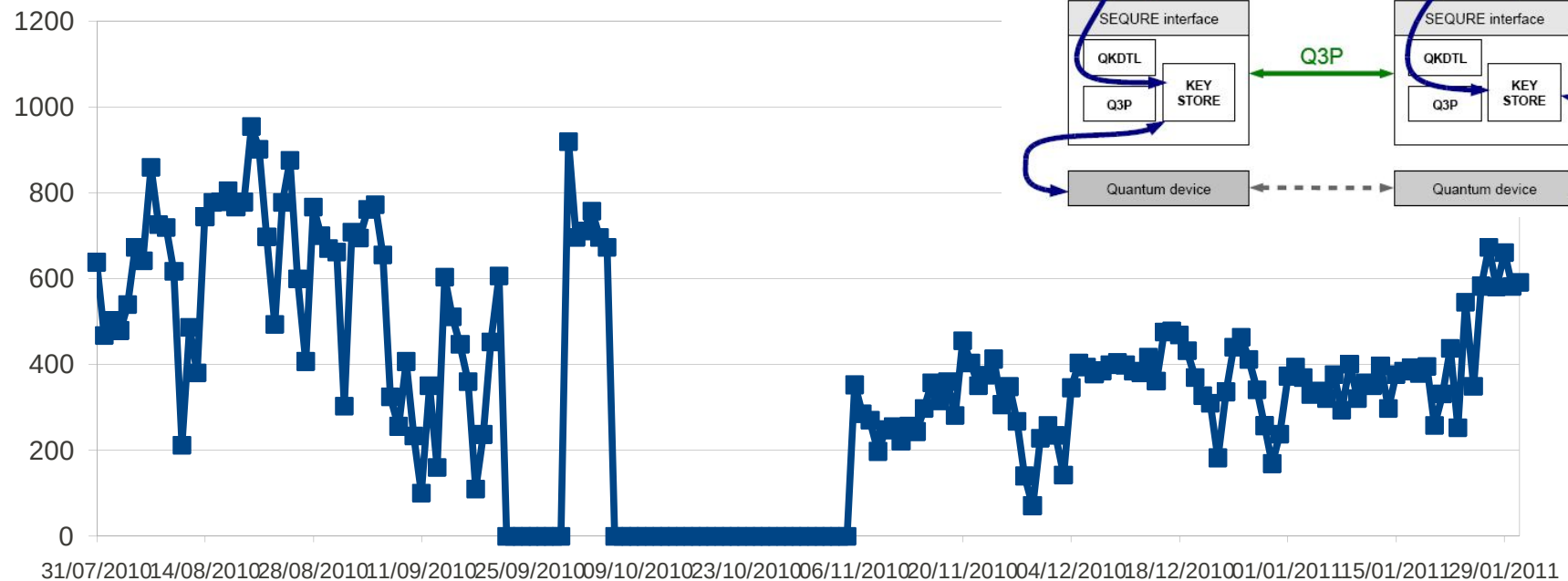


8 kbit/s @ 15 km
during 3 days

S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, A. Villing, P. Grangier
New J. Phys. 2009
M. Peev et al, New J. Phys. 2009

Application to the SEQURE network

Symmetric key Encryption with QUantum key REnewal



- Compatibility with commercial classical encoders (Thales) based on AES protocol, and dedicated software interface
- Metropolitan distance (20 km) over a an installed fiber network → long-term stability demonstration performed in extended Parisian area between July 2010 and February 2011

HIPERCOM objectives for CVQKD

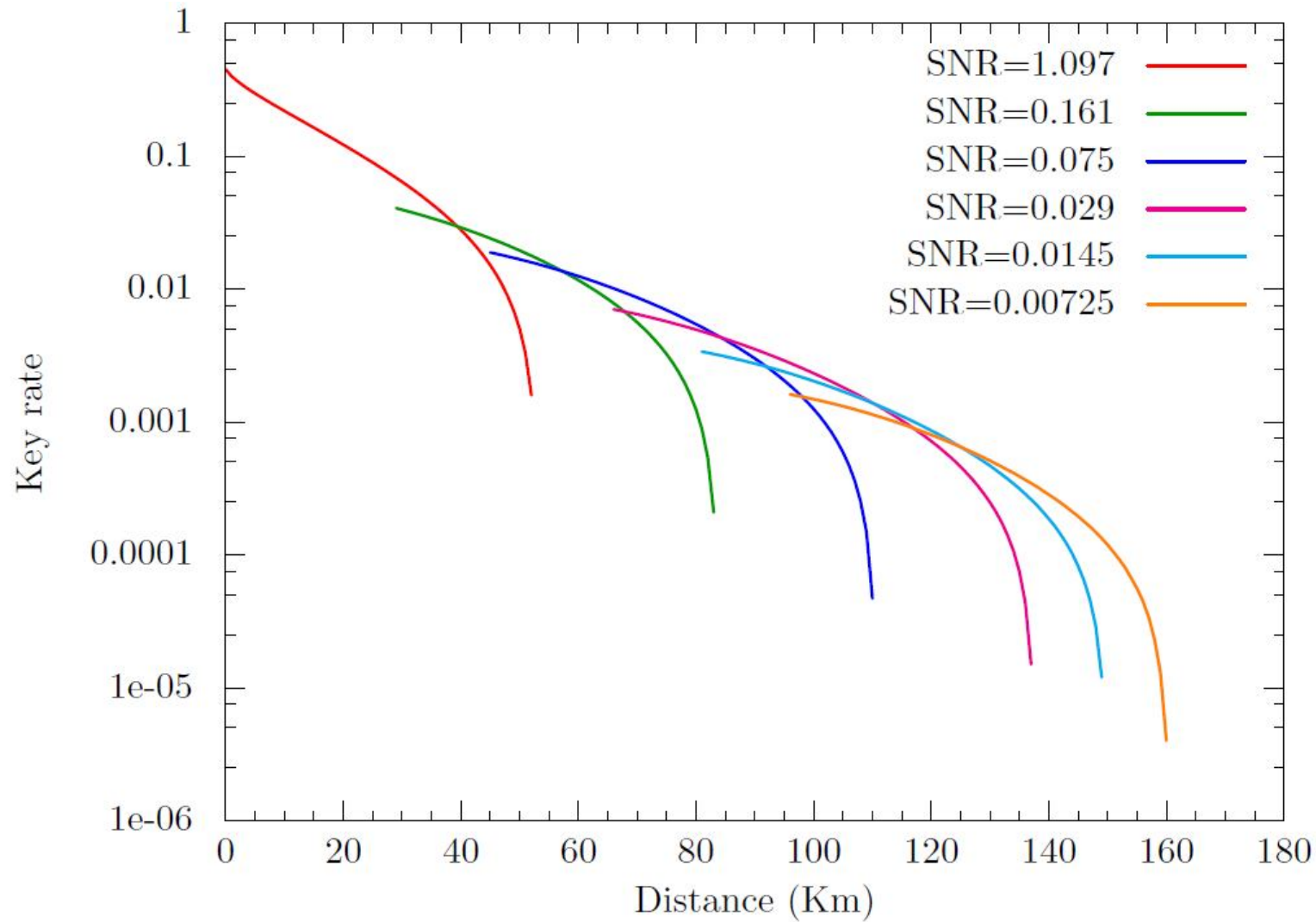
- Improve performance in terms of **rate, distance** and **classical network compatibility**
 - Develop **practical security assurance** of CVQKD systems
-
- What limits the secure distance?
 - Gaussian modulation is optimal
 - Error correction with Gaussian variables is hard
 - Long distance means **error correction at low SNR**
 - Replace slice algorithm (30 km) with **multidimensional reconciliation** (50 km)
→ translates initial problem into a channel coding problem on a '**good**' **channel** (binary input additive white Gaussian noise channel - BIAWGNC)

A. Leverrier et al, Phys. Rev. A 2008

- Recently, improved approximation between the channels and **designed high efficiency LDPC codes** for BIAWGNC

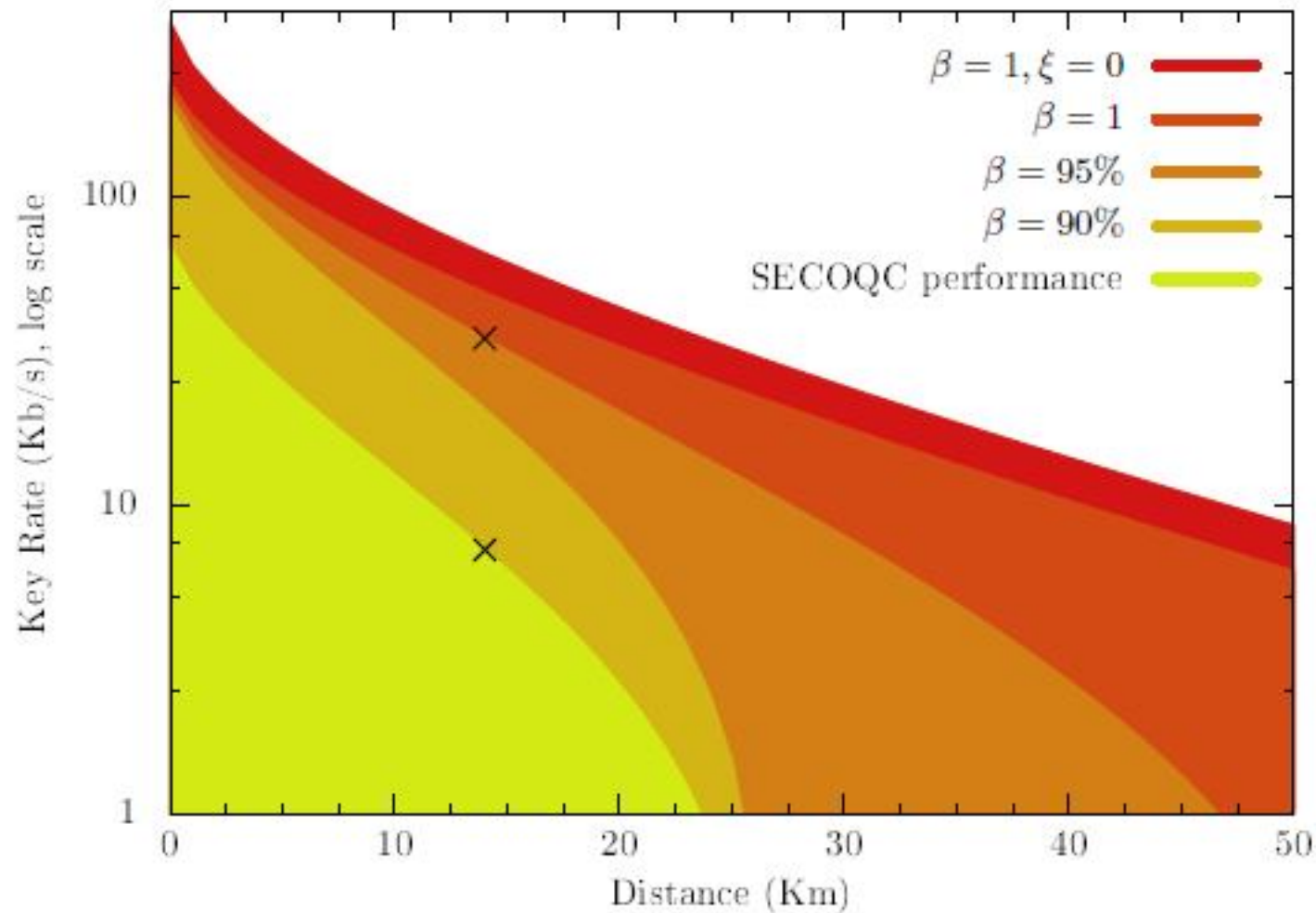
P. Jouguet et al, Phys. Rev. A 2011

Towards long-distance QKD with Gaussian modulation



V_A optimized, $\xi = 0.01$, $\eta = 0.6$, resulting β between 0.93 and 0.97

- With current SNR (about 3) and improved reconciliation efficiency (about 95%) we have **successfully tested a newly developed system at 50 km**
- Envisaged **short term goal: 75 km**



Further improvements

- Envisaged **longer term goal: 100 km and above**
- Modifications of the optical setup will be necessary: with operation at low SNR, the local oscillator power will be too low for proper homodyne detection operation → **amplification in Bob's setup**
- Optical setup modifications also necessary to further **increase secret key generation rate**
- Already increased by an order of magnitude with new error correction codes and use of GPUs instead of CPUs
- Envisaged **goal: adapt system to 5 MHz operation** (instead of 500 kHz)
- Laser source, data acquisition cards, random number generation, homodyne detector
- Implement **wavelength division multiplexing (WDM)** for CVQKD
- Potentially high advantage because of **high cost of fiber use**
- Homodyne detector acts as a **natural filter**

Practical security assurance

- Widely studied for discrete-variable protocols, almost not at all for CVQKD
- Identified natural **candidates**
 - Local oscillator reference signal → careful control and monitoring
 - Homodyne detectors → less vulnerable than single-photon detectors?
 - Noisy modulators, for example eavesdropping via emitted acoustic waves
 - Calibration procedure, crucial for protocol and system operation
 - needs thorough investigation, for example shot noise vs. local oscillator relationship needed for calibration depends on clock signal form, determined by local oscillator!
 - countermeasure: real-time shot noise evaluation
 - Finite-size effects, linked to statistical uncertainty over calculated parameters
 - studied for discrete-modulation protocols
 - A. Leverrier, F. Grosshans, P. Grangier, Phys. Rev. A 2010
 - extended analysis for Gaussian modulation: positive secret key until 70 km for blocks of size 10^8
 - include uncertainty in shot noise estimation