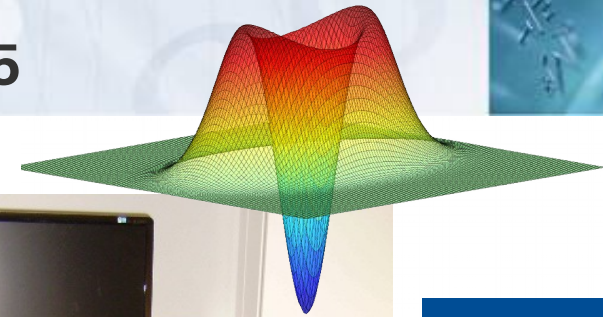


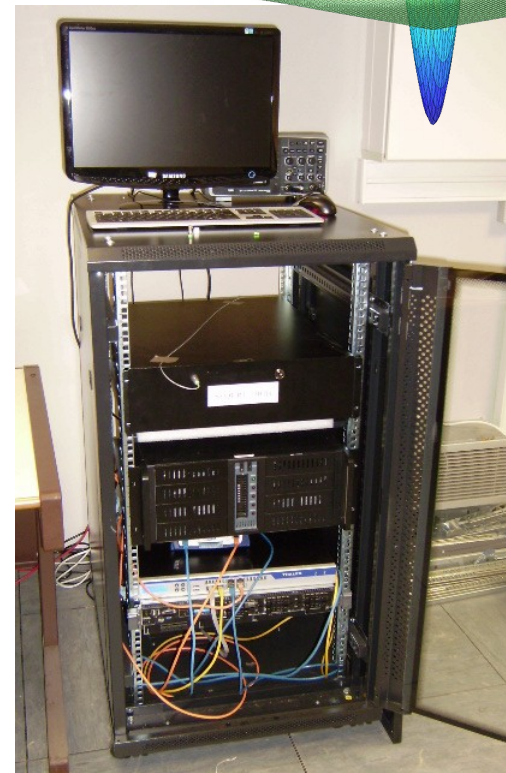


Project Seminar
Madrid
March 18, 2015



HIPERCOM

High-Performance Coherent
Quantum Communications

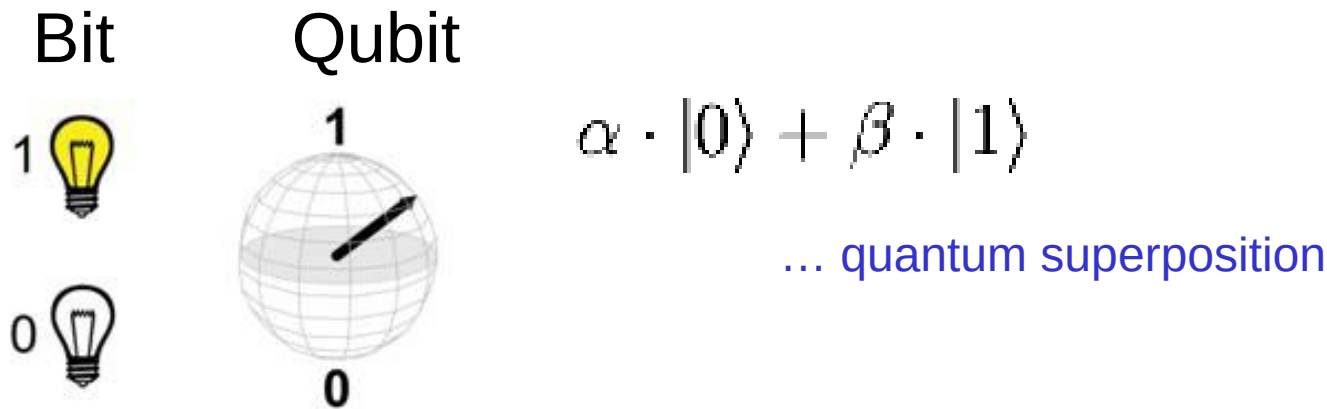


September 2011 – August 2014
Coordinated by Nicolas J. Cerf, ULB



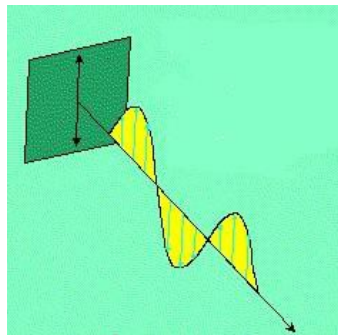
ESSENCE OF HIPERCOM

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



The qubit has become the « cornerstone » of quantum information sciences
(most QIPC processes have been originally developed with qubits)

► **but several advantages of CV information carriers !**



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

amplitude

... coherent communications

KEY CHALLENGES OF HIPERCOM

Develop coherent quantum communication in order to combine

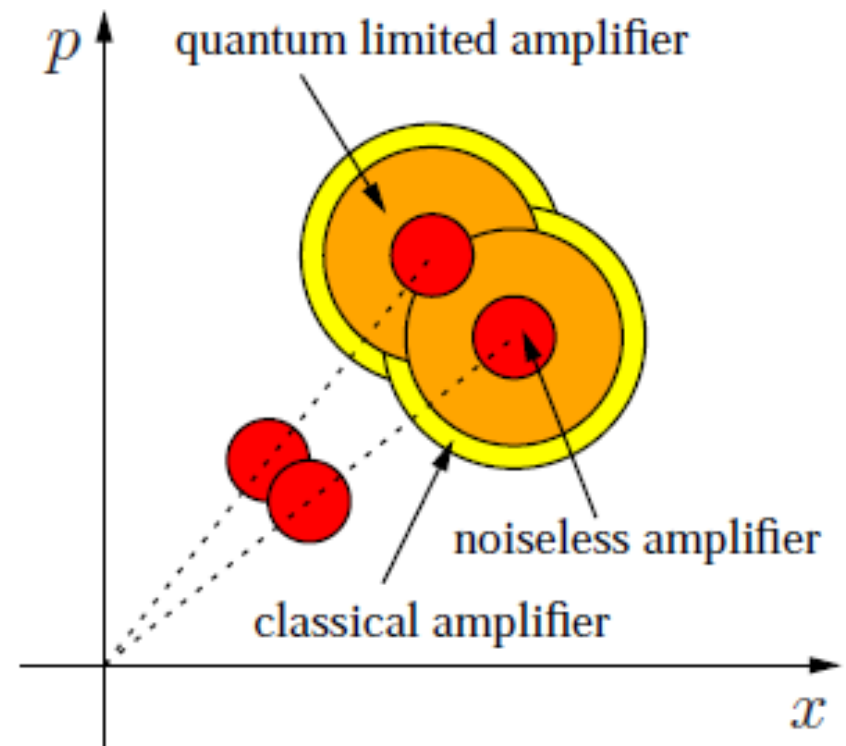
- ➡ the high bandwidth achievable by telecom components (e.g., homodyne detection)
- ➡ the fundamental benefits of quantum mechanics (e.g., information-theoretic security)

Fundamental problem : quantum optical amplifier cannot be used simply as a repeater because it is inherently limited by quantum noise.

The objective of HIPERCOM is to explore various techniques aiming at circumventing this problem and enhancing the range of coherent quantum communications

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

[see Eleni Diamanti's talk]



SPECIFICITIES OF HIPERCOM

Bottom-up approach :

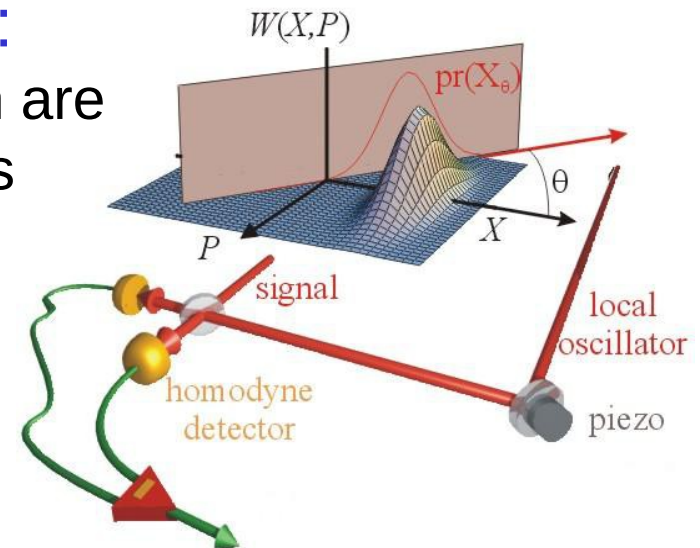
use techniques already proven successful in the lab and build CV information processes based on them (e.g., CV quantum key distribution)

Strong theory – experiments interplay :

devise theoretical concepts together with their experimental demonstration

Builds on coherent communication :

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



EXPECTED OUTCOMES OF HIPERCOM

Theoretical progresses on coherent quantum communications

quantum coding, Gaussian channel capacities, general security proofs of CV-QKD (incl. coherent attacks, side-channels, etc.)

Experimental demonstrations of heralded non-Gaussian quantum processes

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

Improved practical realizations of CV-QKD platform

working over longer distances and with stronger security assessment

➤ pave the way towards long-distance coherent CV quantum communications

➤ all scheduled tasks according to the Work Plan were completed

HIPERCOM CONSORTIUM

Th

Ex

Th-Ex

Th

Th-Ex

Ind

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

METHODOLOGY AND WORKPLAN

Different strategies were planned to 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 techniques relying on specific quantum optical schemes and ultimately on the use of quantum error-correcting codes.

In between these two extreme approaches, an investigation of the potential solution offered by the noiseless linear amplifier or similar heralded operations was planned.

WP1 : CV-QKD

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

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

WP3 : Full quantum solution to range enhancement
(e.g. **quantum coding**, non-Gaussian CV codes,
ultimate **capacity** of quantum optical channels)

applicable
with today's
techniques



longer-term
more theoretical
investigation

HIPERCOM WORKFORCE AND BUDGET

<i>N°</i>	<i>Partner</i>	<i>Person. months</i>	<i>Total costs</i>	<i>Percentage of requested budget</i>
1	Université Libre de Bruxelles, ULB	61 (12 PostD)	~ 158,000€	~ 100%
2	Institut d'Optique Graduate School, IO	15.5 (9 PostD)	170,013€	~100 %
3	Max Planck Inst. For the Science of Light, MPL	80 (21 PostD)	404,200€	~ 100%
4	University of York, UY	43.5 (Seniors)	£ 186,884 (Pounds)	~ 100%
5	Telecom Paris Tech, TPT	18 (16 PostD)	~ 150,000€	~ 100%
6	SeQureNet, SQN	18 (Engineer)	179,759€	~ 101%

MANAGEMENT AND KNOWLEDGE DISSEMINATION

WP0 : Management & organization of annual topical workshops

e.g. Continuous-variable Quantum Information Processing workshop series

HIPERCOM kick-off meeting, Telecom ParisTech, Paris, September 26-27, 2011,
organized by Eleni Diamanti, widened to non-HIPERCOM invited speakers,
was turned into 8th workshop CV-QIP '11

9th workshop CV-QIP '12, Copenhagen, April 27-30, 2012
organized by Ulrik Andersen with ~ 25% of the attendance from HIPERCOM

HIPERCOM mid-term meeting, Jussieu, Paris, January 30 - February 1st, 2013,
organized by Julien Laurat (coupled to project QSCALE), widened to other experts,
was turned into 10th workshop CV-QIP '13

21th Central-European Workhop on Quantum Optics, Brussels, June 23-27, 2014
organized by Evgueni Karpov & Nicolas Cerf (~ 200 participants)
including special sessions for HIPERCOM project & QSCALE project

CHIST-ERA project seminars 2012, 2013, 2014, 2015

RESEARCH RESULTS - DELIVERABLES

N°	Title	Nature	Delivery date		Partners in charge
			Plan	Fact	
1a.1	Improved fiber CV-QKD systems and side-channel analysis	Exper.	M36	M36	TPT (SQN, IO)
1a.2	Software development and protocol optimization for CV-QKD	Exper.	M24	M24	SQN (TPT, IO)
1a.3	Improved free-space CV-QKD systems	Exper.	M36	M36	MPL (TPT)
1b.1	Security of CV-QKD protocols in arbitrary Gaussian channels	Theor.	M36	M36	UY (ULB)
1b.2	Generalized security proofs of CV-QKD against coherent attacks	Theor.	M24	M24	ULB (TPT)
2a.1	Applications of noiseless amplification	Theor.	M24	M12	ULB (IO, MPL)
2a.2	Fundamental aspects of noiseless amplifiers	Theor.	M36	M36	ULB (IO, MPL)
2b.1	Experimental studies of heralded non-Gaussian protocols	Exper.	M36	M36	IO (ULB)
2b.2	Experiments on noiseless amplification and cloning	Exper.	M36	M12	MPL (ULB)
3.1	Continuous-variable quantum codes	Theor.	M36	M36	MPL (TPT, ULB)
3.2	Ultimate capacity of Gaussian quantum optical channels	Theor.	M36	M36	ULB (UY)

RESEARCH RESULTS

The research outcomes that would not have been possible without
the collaborative frame set by the HIPERCOM project

Security analysis of CV-QCD : ULB, TPT advanced towards

- the security proofs against most general coherent attack on CV-QKD protocols

Practical security of CV-QKD : TPT, SQN, MPL, IO performed

- a demonstration of the experimental implementation of a CV-QKD systems
[Nature Photonics 7, 350 (2013)]
- an experimental analysis of side channel and Trojan horse attacks on CV-QKD systems
[IEEE Journal of Selective Topics on Quantum Electronics 21, 3 (2014)]
- distrustful cryptography - practical coin-flipping protocol
[Nature Communications 5, 3717 (2014)]

RESEARCH RESULTS

The research outcomes that would not have been possible without
the collaborative frame set by the HIPERCOM project

Noiseless amplification of light and heralded protocols:

theory ULB, IO

- phase-insensitive squeezing of light
- noiseless amplifier & noiseless attenuator :
 - can be combined to turn a lossy channel into an ideal channel
 - ... noiseless loss suppression ...experiment is planned
 - can be exploited to improve the performances of CV QKD
 - ... Gaussian postselection

experimental demonstrations IO, MPL

- heralded generation of cat states and further of any quantum states of light
[Optics Express 20, 14030 (2012)]
- high-fidelity probabilistic CV quantum cloning

RESEARCH RESULTS

The research outcomes that would not have been possible without
the collaborative frame set by the HIPERCOM project

Quantum Information processing networks : MPL, TPT

- developed and experimentally implemented graph state schemes
for quantum error-correcting codes and secret sharing protocols in CV & DV
[Nature Communications 5, 3658 (2014)]
[Nature Communications 5, 5480 (2014)]
- demonstrated the feasibility of CV graph state quantum networks
and a usefulness of integration of different protocols in the same set-up

Quantum communication channels : ULB, UY

- found a way for determining optimal information transmission rates
by proving the longstanding Gaussian conjecture
[Nature Photonics 8, 796 (2014)]
and studying its relation to Gaussian discord thus achieving
a better understanding of the nature of quantum correlations

SCIENTIFIC PUBLICATIONS

60 journal publications + 9 preprints ; 101 conference contributions

INCLUDING:

- 2 Nature Photonics
- 3 Nature Communications,
- 2 Optics Express,
- 1 IEEE J. Selected Topics in quantum Electronics
- 10 Physical Review Letters
- 30 Physical Review A
- 4 New Journal of Physics

VALORIZATION and FOLLOW-UP

Industrial partner SQN is in charge of the research valorization

Improved the two products related to the research carried out within the project:

- Software stack for Quantum Key Distribution post-processing,
 - composed of high-performance error-correction and privacy amplification (designed for academic institutions)
- Cygnus, a CV - QKD system implementing the Gaussian protocol
 - able to share secret keys at distances of about 80 km
 - demonstrated a possibility of deployment alongside classical WDM channels

Patent application (Avril 2013)

- Family of countermeasures protecting a practical CV-QKD system against attacks on the QKD optical device
 - the local oscillator calibration attack
 - the wavelength attack

Research follow-up

Photonics integration

- Development of a CV-QKD system using silicon photonics (TPT, IO) within collaborative project QRYPTOS “Quantum cryptography on silicon”

SCIENTIFIC RESULTS

2 selected results in connection with the capacity of Gaussian quantum channels
& CV-QKD

- Fundamental limit to optical communication
Ultimate classical communication rates of
quantum optical channels

(ULB)

- CV-QKD experimental platform
Progress in optical implementation

(TNT & SQN)

FUNDAMENTAL LIMIT TO OPTICAL COMMUNICATION



Nicolas J. Cerf
ULB



Raúl García-Patrón Sánchez
ULB



Vittorio Giovannetti
Scuola Normale Superiore of Pisa



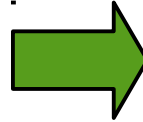
Alexander Holevo
Steklov Mathematical Institute of Moscow

CHANNEL CAPACITY

Alice



Channel noise of power N

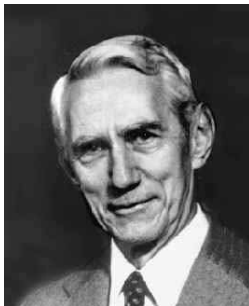


Bob



Capacity C – maximum rate of information transmission without errors

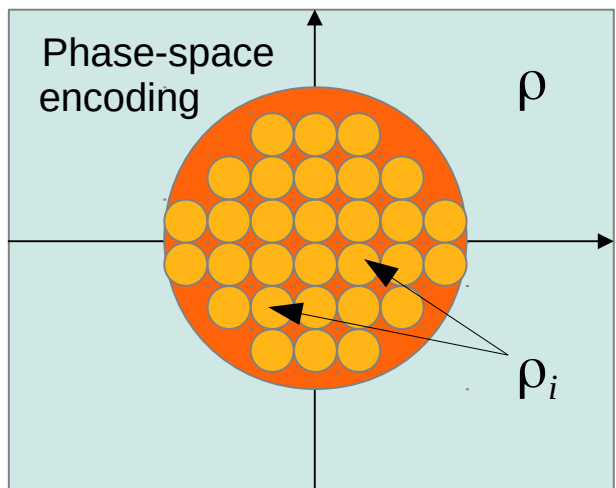
Shannon



$$C = \frac{1}{2} \log_2 \left[1 + \frac{P}{N} \right]$$

Infinite capacity with finite input power P (energy)!

QUANTUM CHANNEL CAPACITY



$$\rho = \sum_i p_i \rho_i \quad P = \sum_i p_i P(\rho_i)$$

$$\rho^{(n)} \left\{ \begin{array}{c} \xrightarrow{\quad} \mathcal{M} \xrightarrow{\quad} \\ \xrightarrow{\quad} \mathcal{M} \xrightarrow{\quad} \\ \xrightarrow{\quad} \mathcal{M} \xrightarrow{\quad} \end{array} \right\} M^n(\rho^{(n)})$$

$$C(M, P) = \lim_{n \rightarrow \infty} \left(\frac{1}{n} \right) \max_{[p_i, \rho_i]_{\rho, P}} \left[S(M^n[\rho]) - \sum p_i S(M^n[\rho_i]) \right]$$

Max. by average output thermal state

Minimum output entropy state

$$C(M, P) \leq S(M^n[\rho_{th}]) - S(M^n[\rho_{min}])$$

MINIMUM-OUTPUT ENTROPY CONJECTURE

$$\min_{\rho_i} S(M^n(\rho_i)) = n S(M(|0\rangle\langle 0|)) \quad \Rightarrow \quad \rho_{min} = |0\rangle\langle 0|$$

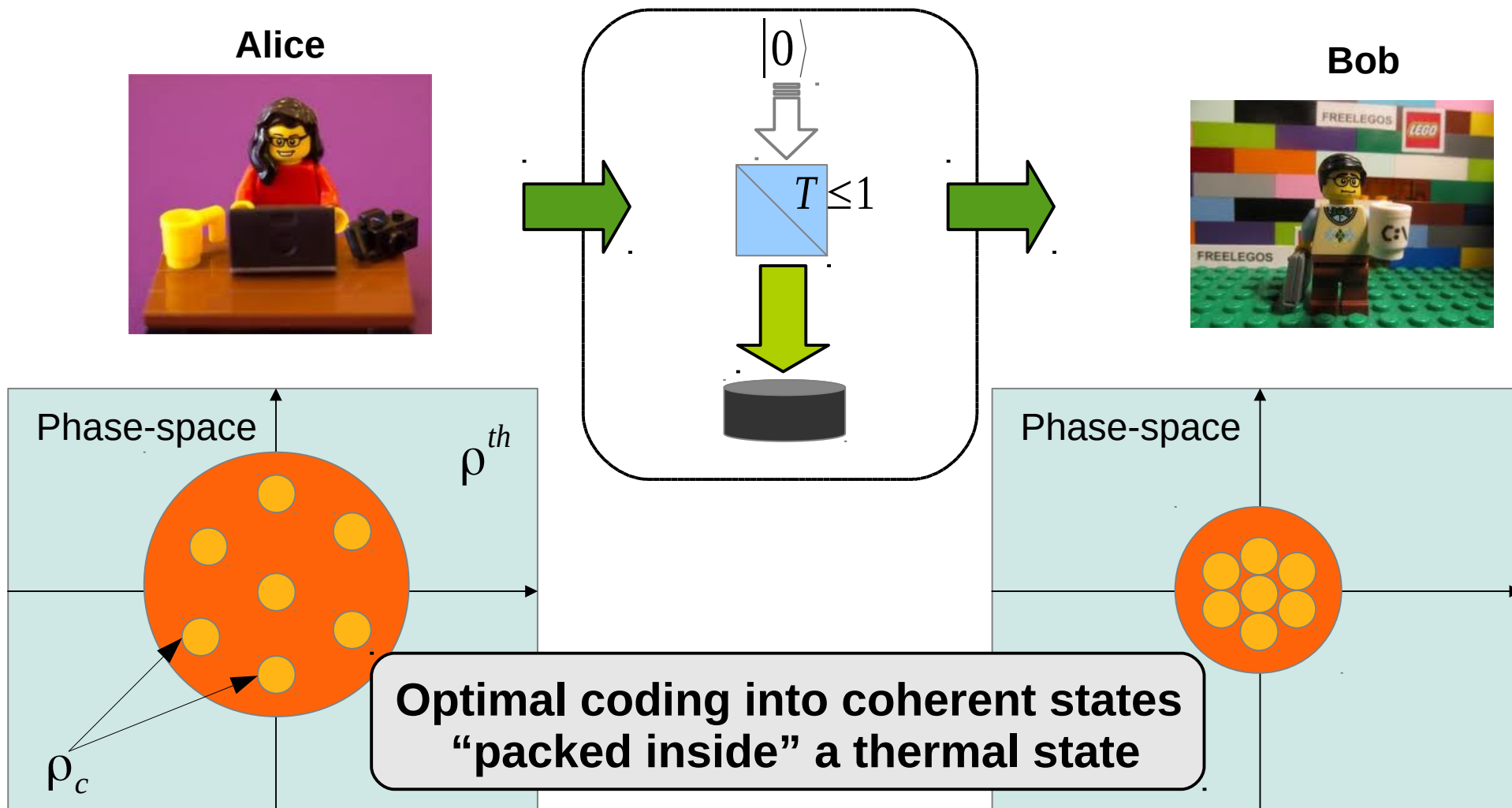
Proven for “lossy” (attenuation) channel

PURE-LOSS (ATTENUATION) CHANNEL

Alice

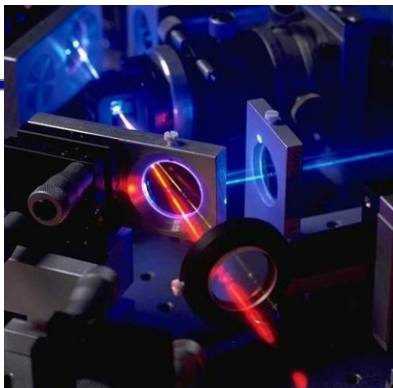


Bob

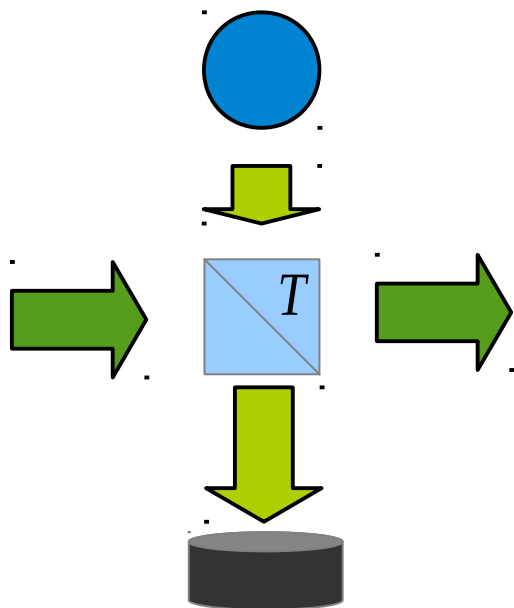


$$C(T, P) = S(\rho_{TP}^{th}) = S(T[\rho_P^{th}])$$

GAUSSIAN BOSONIC CHANNELS



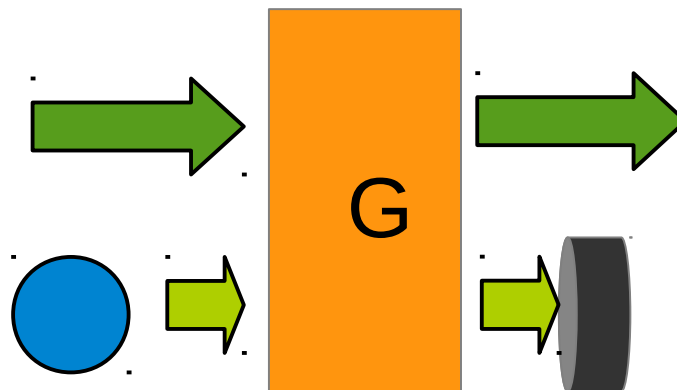
Lossy channel



$$0 \leq \tau = T \leq 1$$

$$y \geq 1 - \tau$$

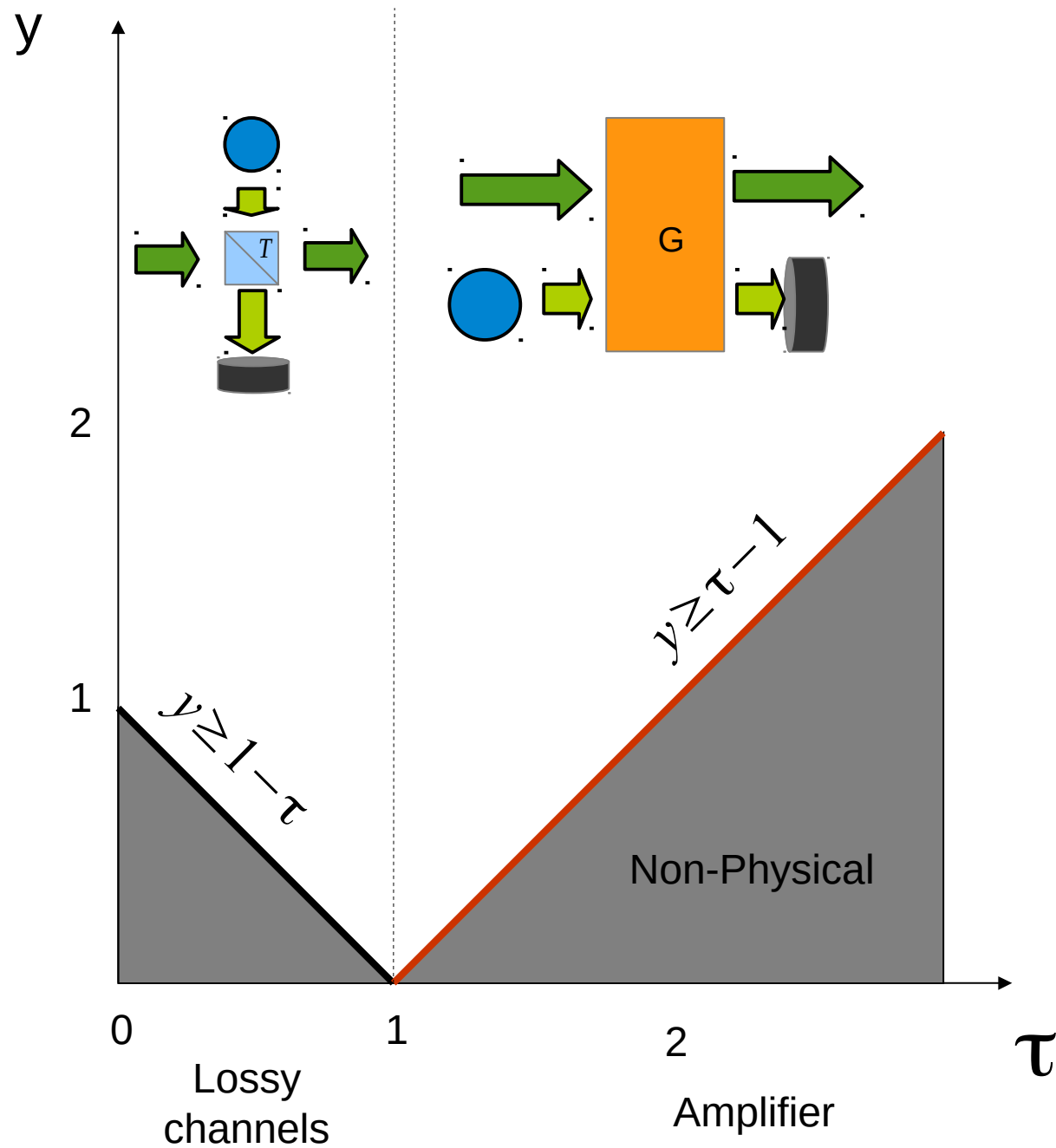
Amplifier



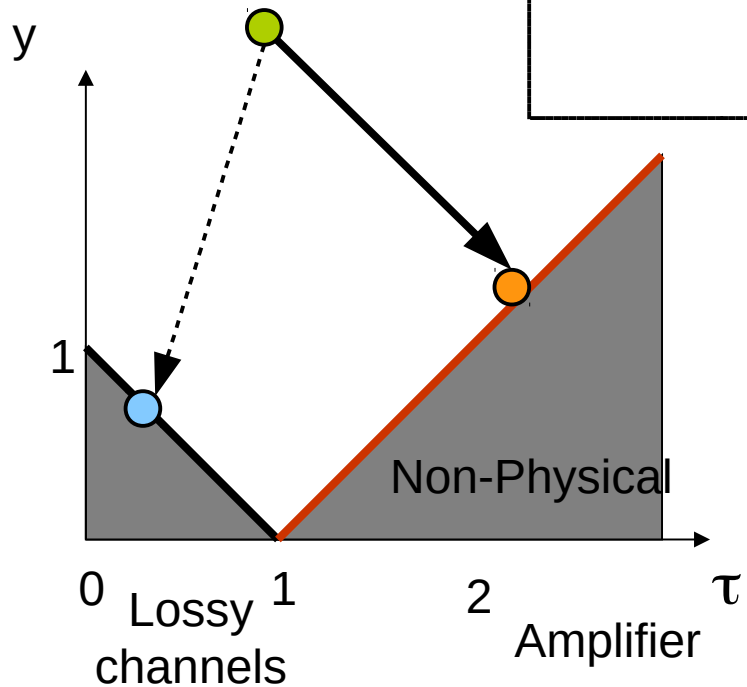
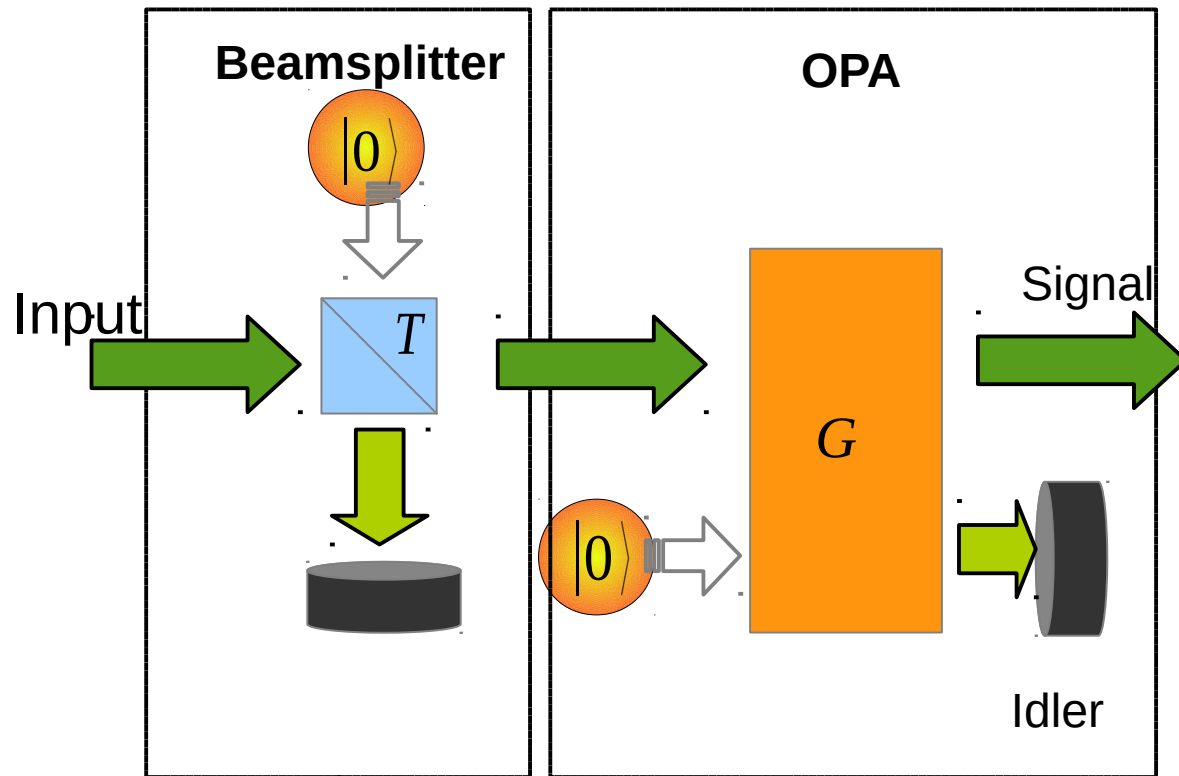
$$\tau = G \geq 1$$

$$y \geq \tau - 1$$

PHASE-INSENSITIVE CHANNELS



CHANNEL DECOMPOSITION



$$\tau = T G$$

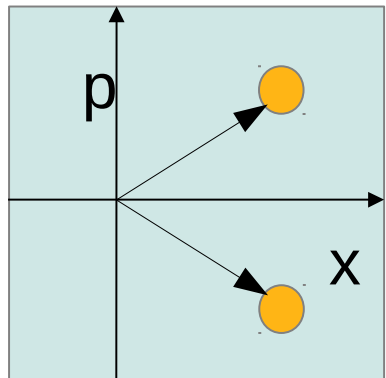
$$y = G(1 - T) + G - 1$$

PHASE-CONJUGATION CHANNELS

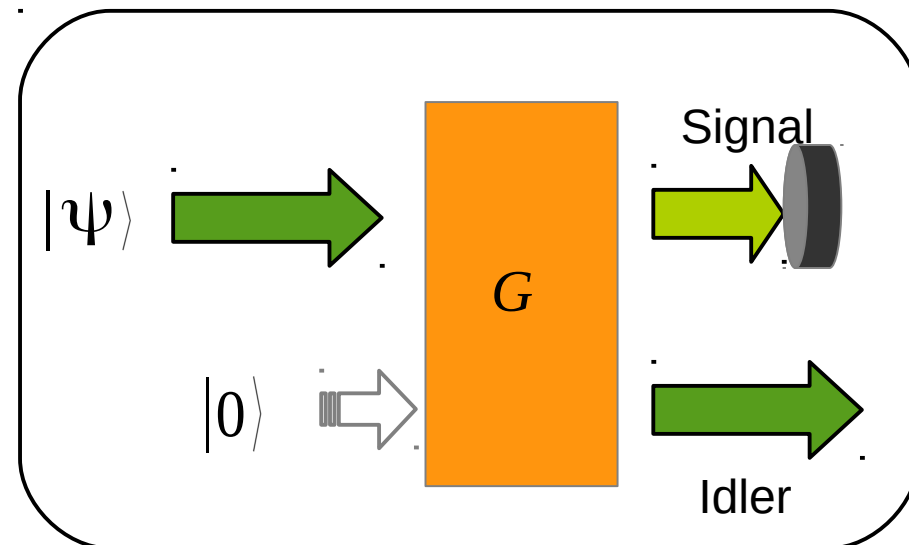
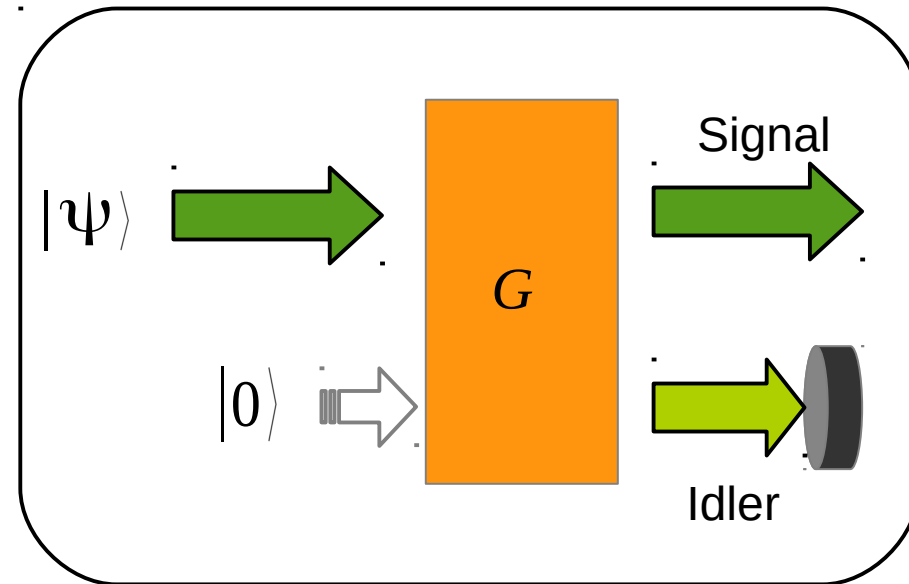
Phase-conjugation channel
is complementary to Amplifier



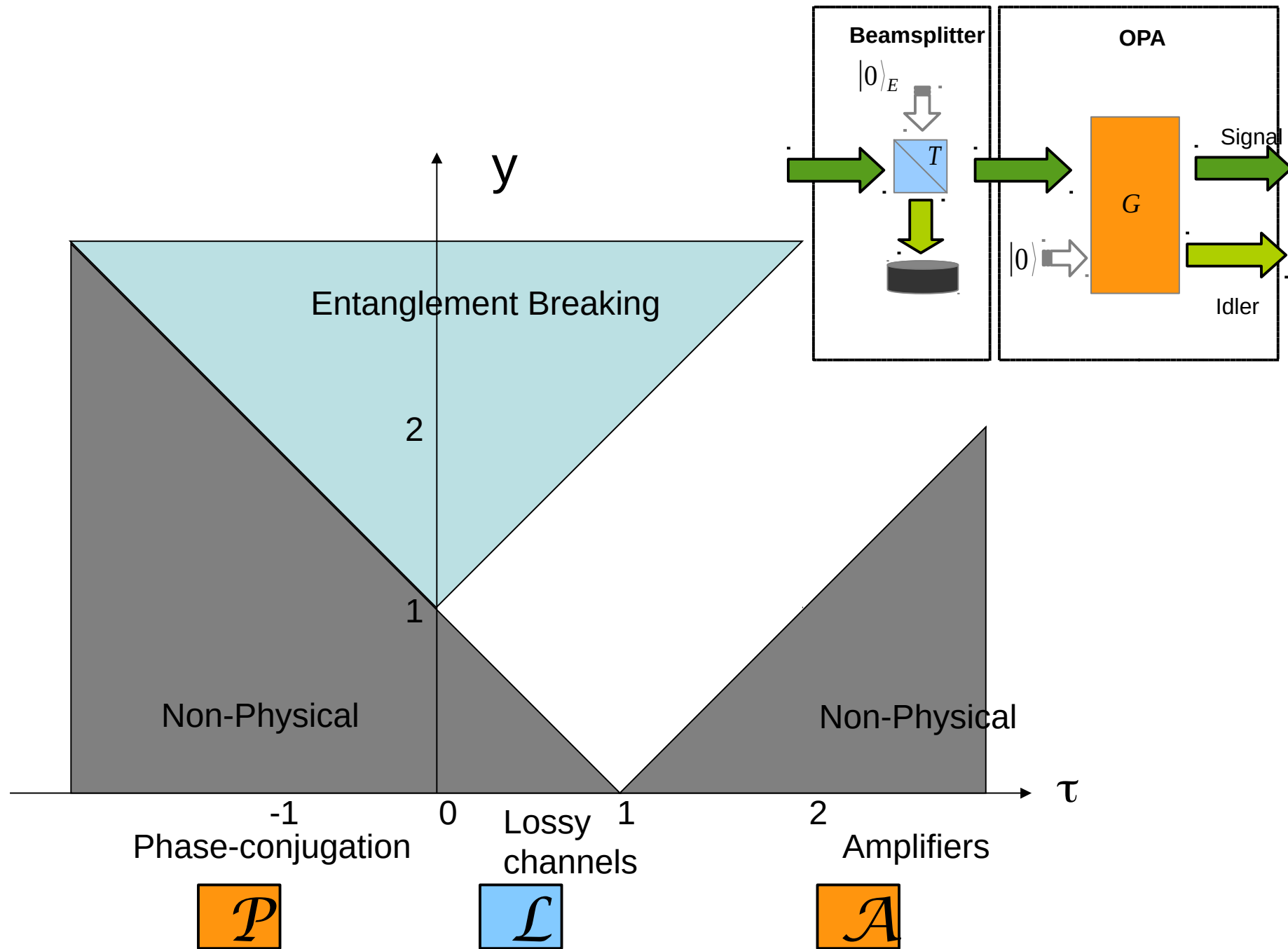
$$S(A(\rho)) = S(P(\rho))$$



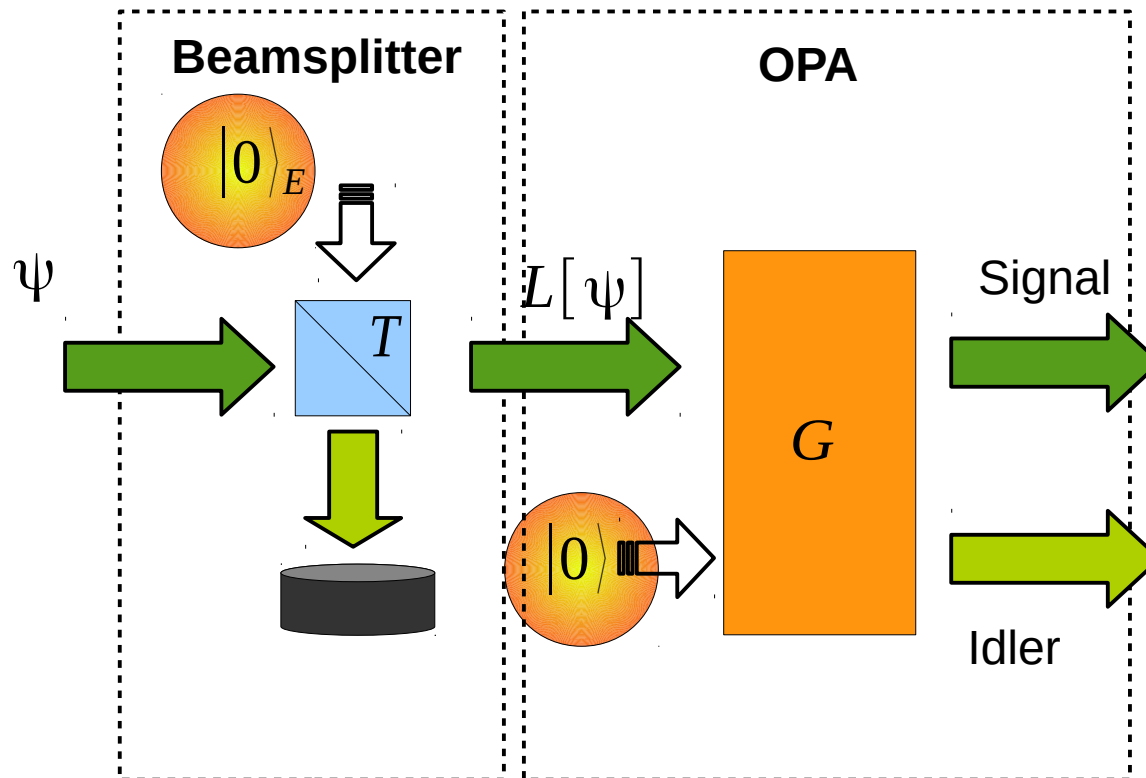
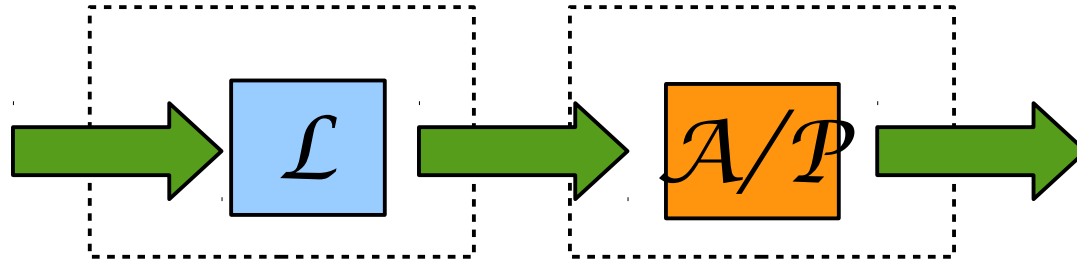
Phase-conjugation is entanglement-breaking



THE FULL FAMILY OF GAUSSIAN CHANNELS



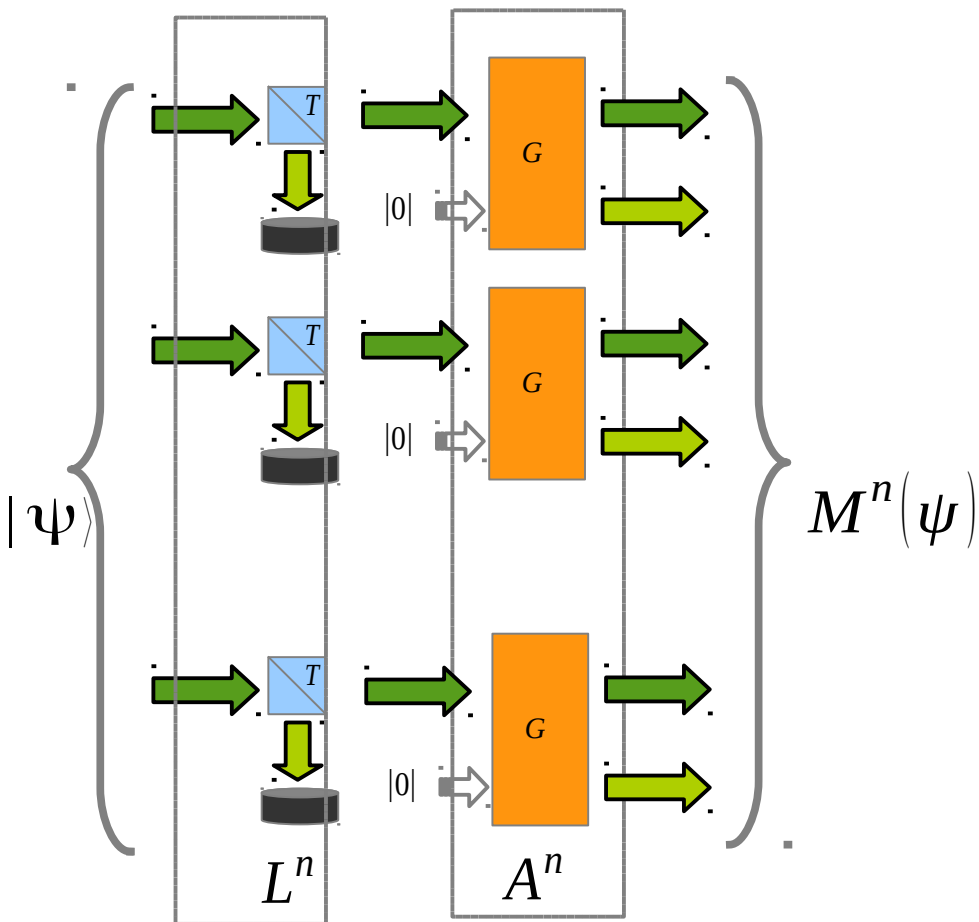
REDUCTION (1 use)



REDUCTION (N uses)

Phase-conjugation is entanglement-breaking

Holevo, Prob. Inf. Trans. **44**, 3 (2008)



$$\boxed{\mathcal{A} \leftrightarrow \mathcal{P}}$$

$$S(A_G(\psi)) = S(P_{G^{-1}}(\psi))$$

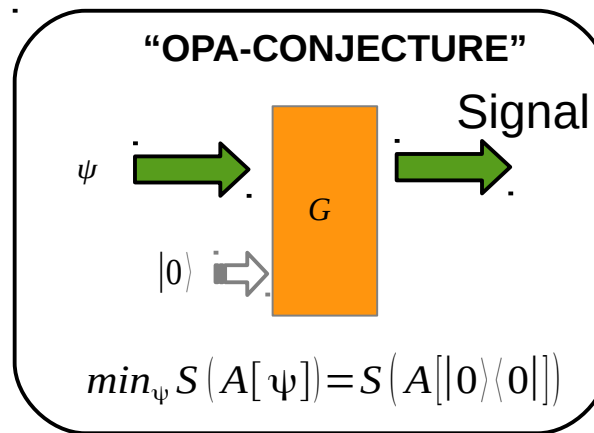
Additivity of the Classical Capacity of
Entanglement-Breaking Quantum Channels

Peter W. Shor

AT&T Labs, Florham Park, NJ 07922, USA

$$S(M^n[\psi]) \geq \min_{\varphi} S(A^n[\varphi]) \geq n \min_{\varphi} S(A[\varphi]) \stackrel{?}{\geq} n S(A[|0\rangle\langle 0|])$$

THE LAST MISSING PIECE OF THE PUZZLE

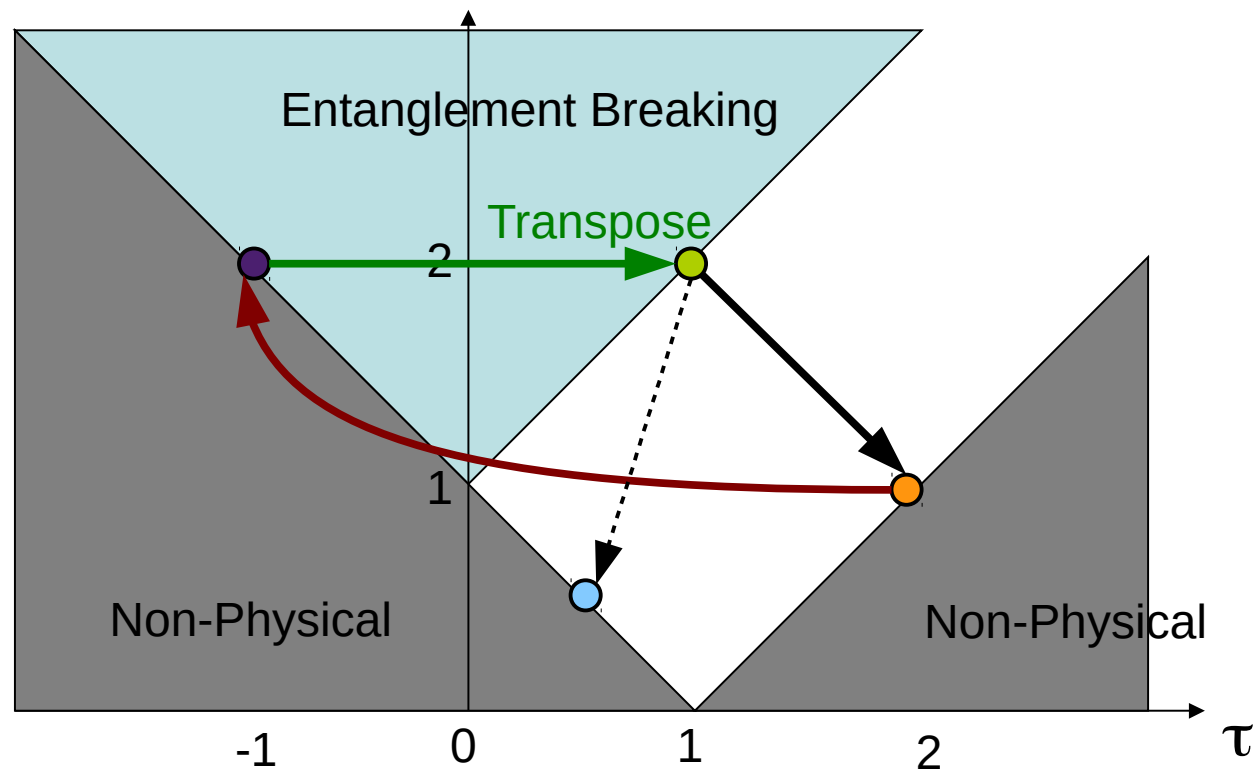


LAST STEPS



$$S(A_G(\psi)) = S(P_{G-1}(\psi)) = S(T \circ P_{G-1}(\psi)) = S(A_G \circ L_{(G-1)/G}(\psi))$$

$$\tilde{G} = G \quad T = \frac{G-1}{G}$$



LAST STEPS



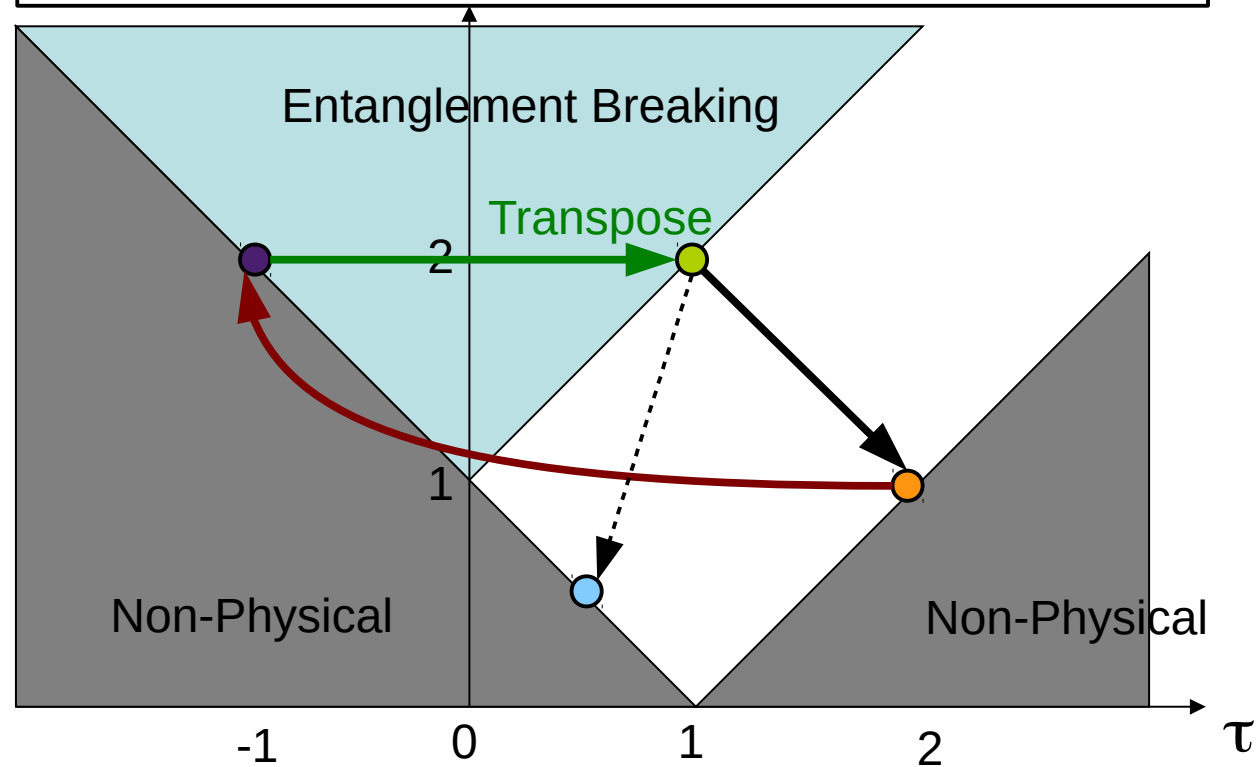
$$S(A_G(\psi)) = S(P_{G-1}(\psi)) = S(T \circ P_{G-1}(\psi)) = S(A_G \circ L_{(G-1)/G}^n(\psi))$$

$$\tilde{G} = G \quad T = \frac{G-1}{G}$$

Iterate...

$$S(A_G(\psi)) \geq \dots \geq \sum_i p_i S(A_G(\varphi_i))$$

$$\text{Where } \varphi_i \text{ s.t. } \sum_i p_i \varphi_i = L^n(\psi)$$



LAST STEP



$$S(A_G(\psi)) = S(P_{G-1}(\psi)) = S(T \circ P_{G-1}(\psi)) = S(A_G \circ L_{(G-1)/G}^n(\psi))$$

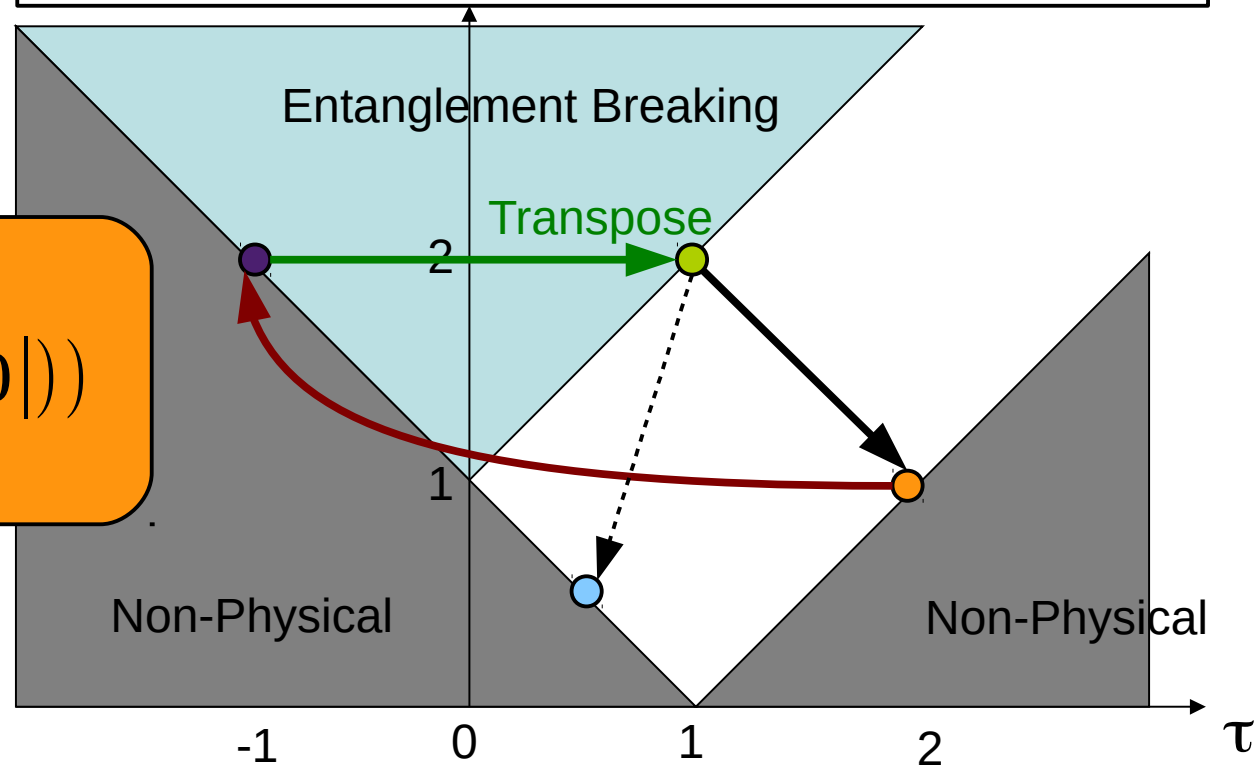
$$\tilde{G} = G \quad T = \frac{G-1}{G}$$

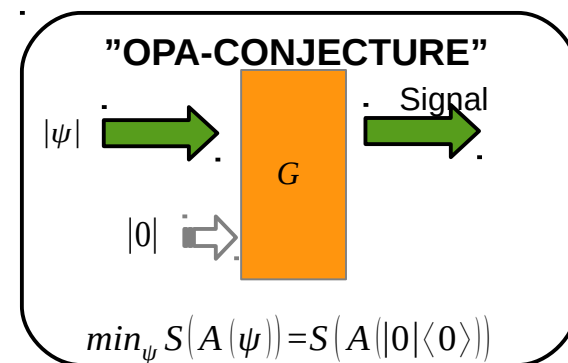
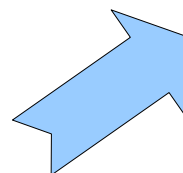
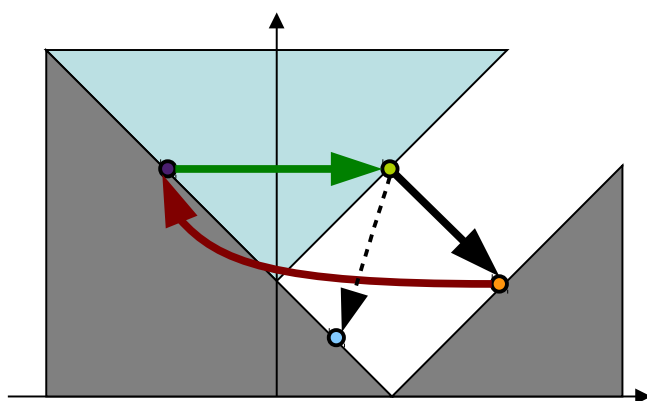
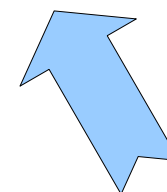
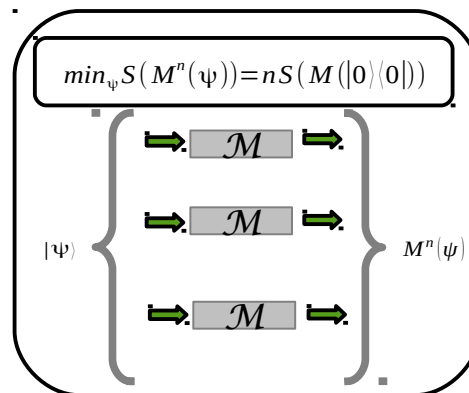
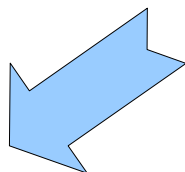
Iterate...

$$S(A_G(\psi)) \geq \dots \geq \sum_i p_i S(A_G(\varphi_i))$$

Where φ_i s.t. $\sum_i p_i \varphi_i = L^n(\psi)$

$$S(A_G(\psi)) \geq S(A_G(|0\rangle\langle 0|))$$





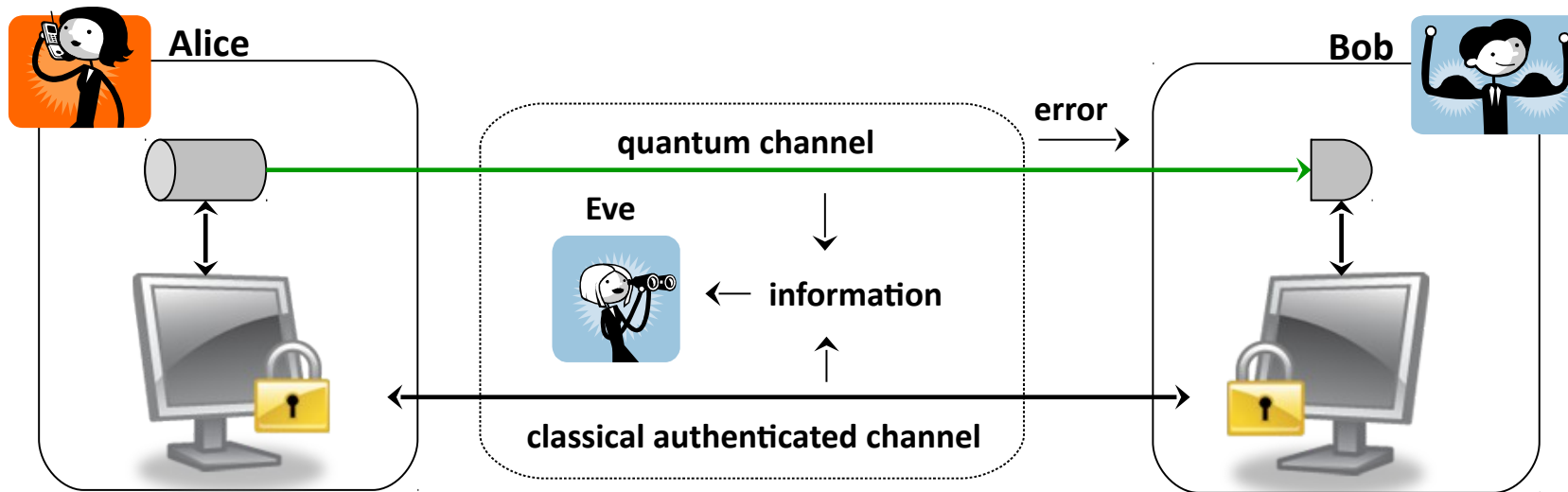
HIPERCOM experimental results on Continuous-Variable Quantum Key Distribution

HIPERCOM **objectives** for continuous-variable QKD

- Improve performance in terms of **rate and distance in experimental implementations**
- Improve **practical security** of CV-QKD systems

Quantum Key Distribution

Allows secret message exchange with information-theoretic security → guaranteed against an all-powerful eavesdropper



Key information is encoded in photonic carriers

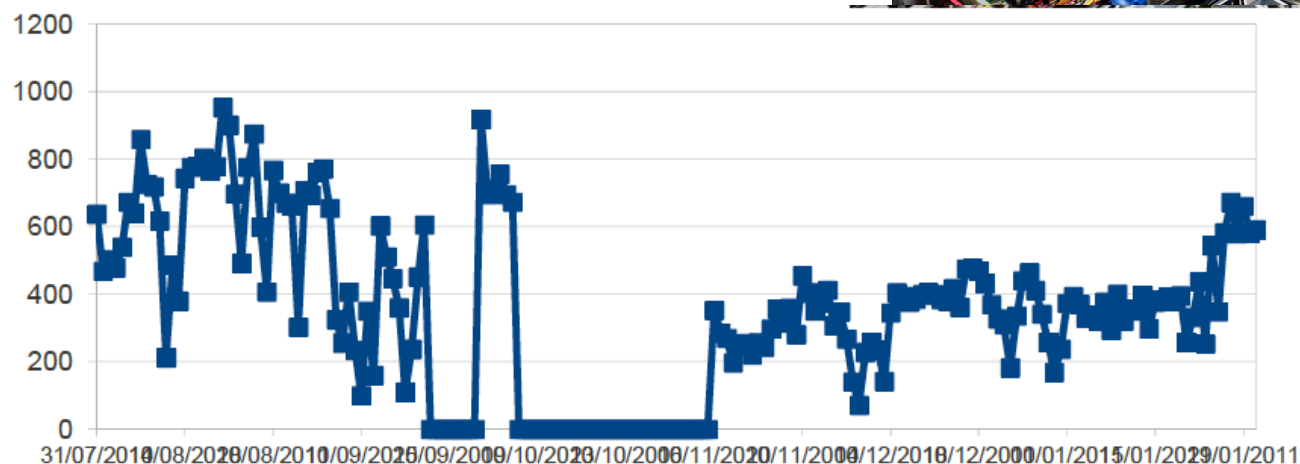
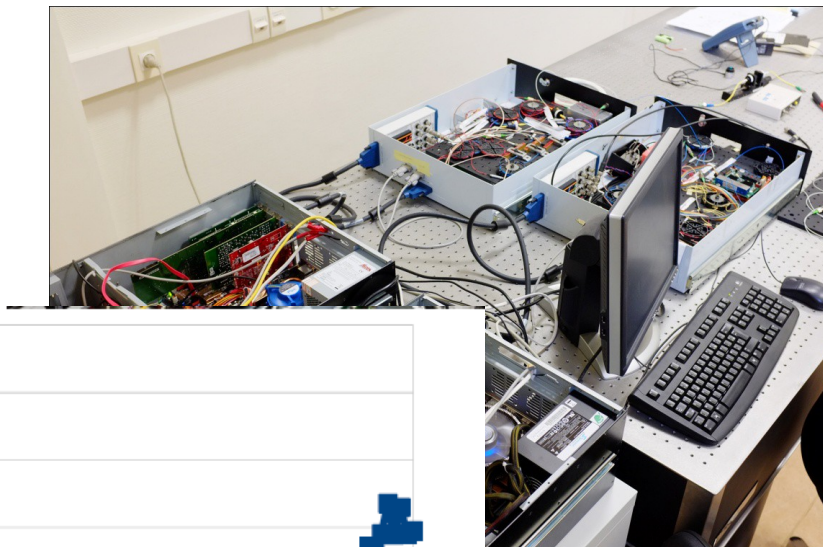
Analysis of errors due to Eve's measurements leads to secret key

Discrete and continuous-variable QKD

	Discrete variables	Continuous variables
Key encoding	Photon polarization/phase	EM field amplitude-phase
Detection	Single-photon	Coherent (homodyne/heterodyne)
Performance (range, rate)	200 km, 1 Mbit/s	100 km, 100 kbit/s
Post-processing	Key readily available	Complex error correction algorithms
Security	General attacks, finite-size , side channels	Collective attacks, finite-size, side channels
Network integration	WDM	WDM
Stability	Months	Months

CV-QKD implementations before HIPERCOM

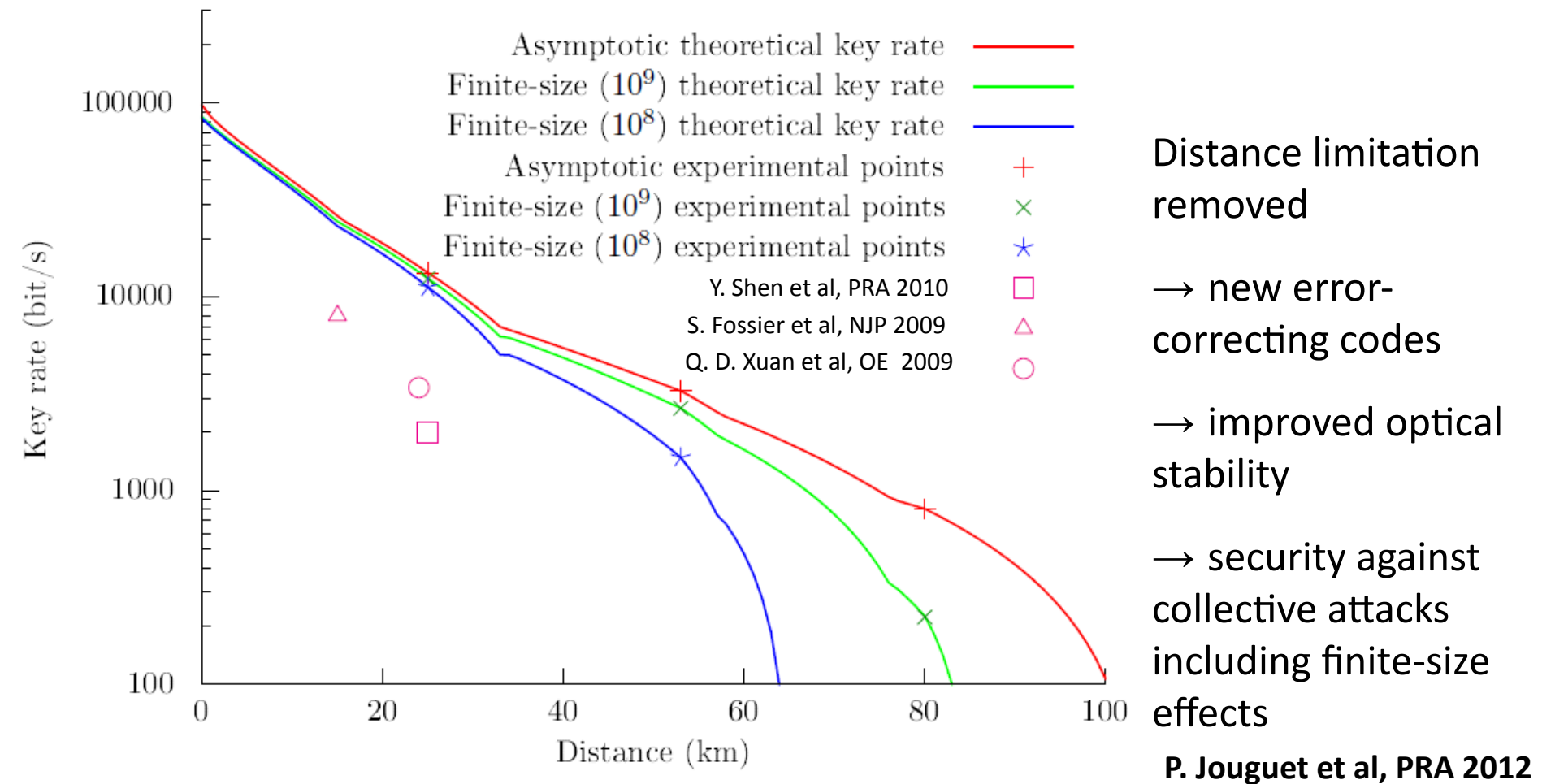
Integration into the  SECOQC
QKD network, Vienna 2008



Field test with classical encryption demonstrating long-term stability
over 20 km fibre link

S. Fossier et al, New J. Phys. 2009; **P. Jouguet et al, Opt. Express 2012**

Long-distance CV-QKD results @ TPT



P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Nature Photonics 2013

Dissemination at popular science magazines La Recherche and Science et Vie

CV-QKD commercial system : Cygnus



Courtesy: SeQureNet

Will be part of the next-generation Tokyo QKD network in 2015

Side channels and practical security

- Deviations of security proof assumptions from real implementations open the door to security loopholes → hacking
- Side channel attack based on ubiquitous calibration procedures
→ countermeasure: real-time shot noise evaluation

P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A 2013

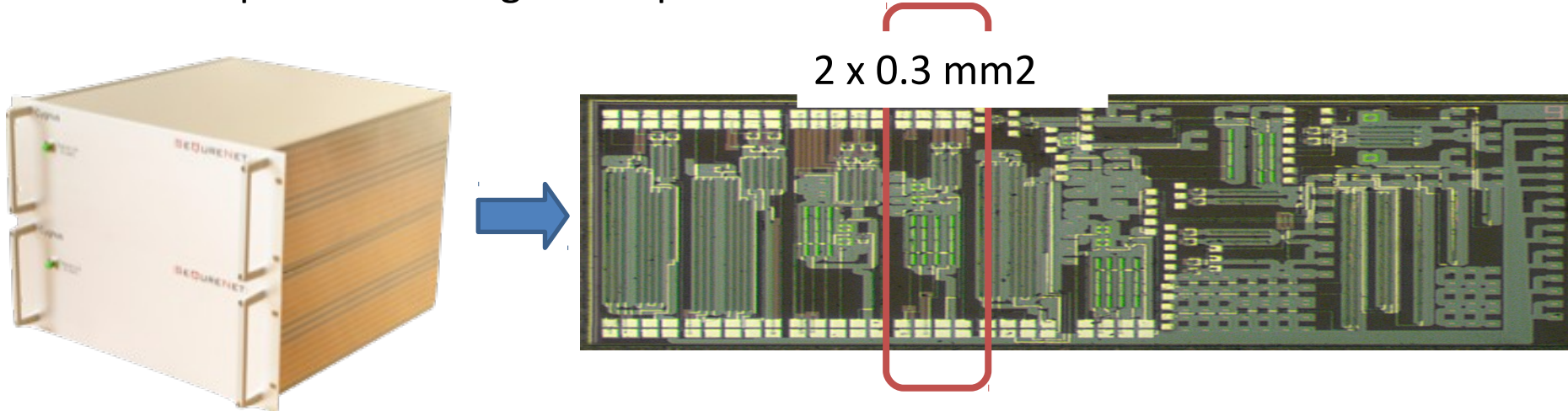
- Real-time Trojan horse-type of attack on commercial CV-QKD system
→ Eve probes Alice's modulators with a bright signal

HIPERCOM collaboration: TPT – MPL

**I.Khan, N. Jain, B. Stiller, P. Jouguet, S. Kunz-Jacques,
E. Diamanti, C. Marquardt, G. Leuchs, QCrypt 2014**

Current progress and perspectives

- On-chip CV-QKD using silicon photonics



ANR project QRYPTOS (TPT, IO), 2014 - 2017

- Towards satellite CV-QKD
- Network integration using wavelength division multiplexing techniques
R. Kumar et al, QCrypt 2013, New J. Phys. 2015
- Performance enhancement with locally generated phase reference
quant-ph arXiv: 1503.00662, 1503.04763
- Quantum cryptography beyond QKD