Experimental Demonstration of Long-distance Continuous-Variable Quantum Key Distribution

Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, Eleni Diamanti

SeQureNet, Télécom ParisTech

2012-11-28

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

QKD: four main limitations (1/2)

Speed

- Not enough for OTP: not a serious issue
- Physical parameters estimation over large blocks: hardware drifts, latency

Distance

- Asymmetric crypto is not limited
- Trusted nodes are not a good solution: quantum repeaters are required

QKD: four main limitations (2/2)

Security

- Incomplete security proofs
- Distance between proofs and practical implementations

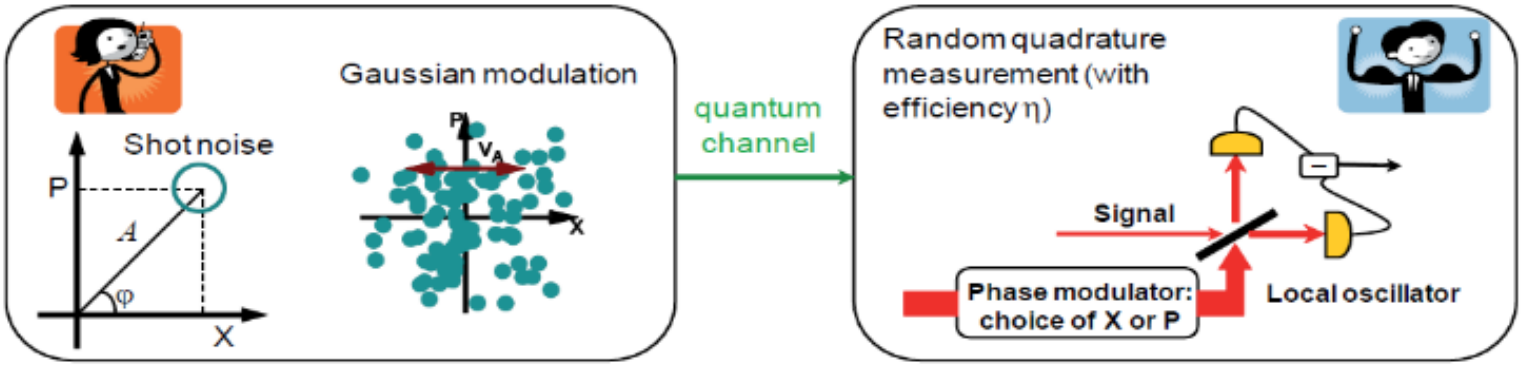
Deployment

- QKD requires a dark fiber: $$$
- WDM compatibility: lowers QKD extra premium

Two technologies

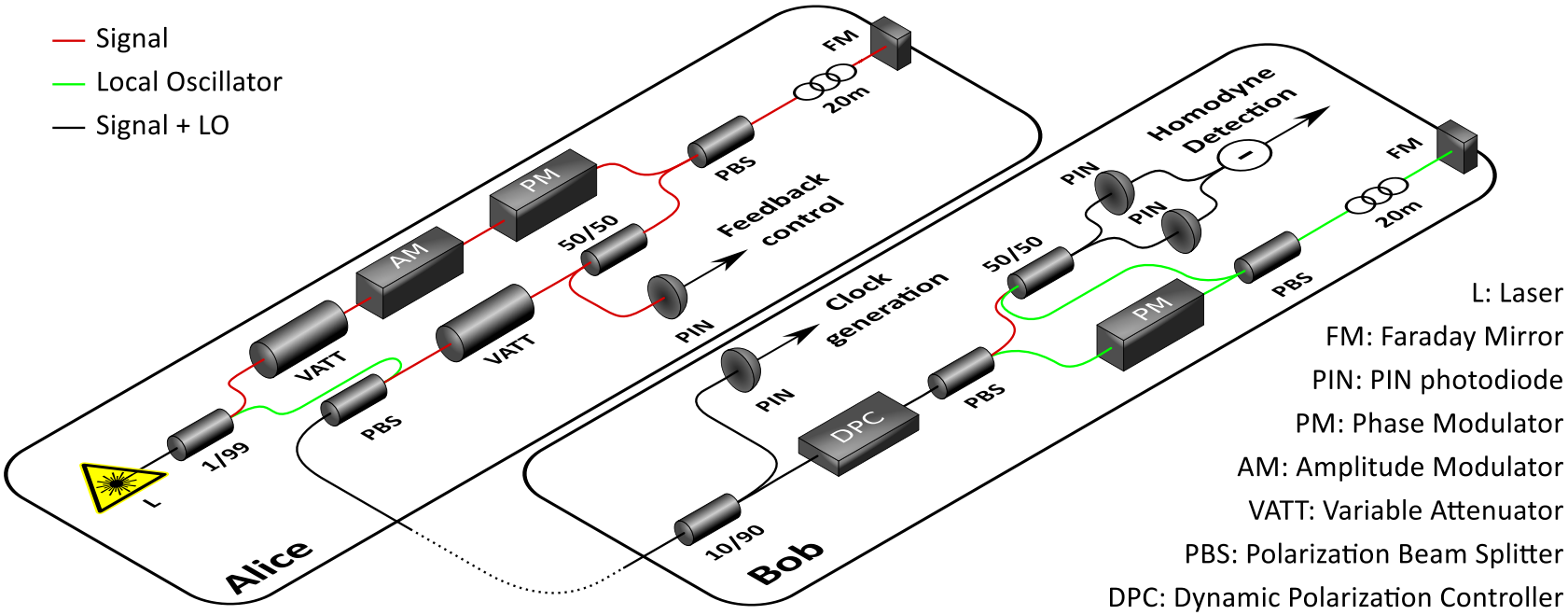
	Discrete variables	Continuous variables
medium	photon phase/polar.	field amplitude-phase
detection	photon counters	coherent detection
range	100 km	25km
rate	1Mb/s	10kb/s
components	active cooling	standard
integration	CWDM	DWDM
security	yes	yes

Gaussian protocol



Losses and excess noise lower the SNR.

Optical setup



- For a field demonstration, see T. Debuisschert's poster.

Speed limitations

- Delay between classical and quantum signals (200ns)
- Laser pulsed with a tunable frequency (1MHz)
- Data acquisition speed (up to 5MHz)
- Filtering: tradeoff between speed and electronic noise (current cutoff at 10MHz, 100MHz feasible arxiv:1006.1257 Yue-Meng Chi et al.)
- High-speed error correction: LDPC codes (GPU) or polar codes (CPU) (up to 10Mbit/s) (arxiv:1204.5882, P. Jouguet and S. Kunz-Jacques)

Range limitations

- High error-correction efficiency, even at low SNRs
- Finite-size effects
- Low SNR Alice/Bob synchronization mechanism
- Low-loss LO path
- Excess noise (imperfect relative phase estimation)

New SNR regions allowed by error-correction techniques.

Channel virtualization

- Idea introduced by Leverrier (Phys. Rev. A 77, 042325 (2008))
- Translates the initial problem into a channel coding problem on a *good* channel
- *Good* means very efficient error-correcting codes available
- Usual suspect: BIAWGNC

How to improve the efficiency of the multidimensional scheme?

- Improve the approximation between the virtual channel and the target channel
- Improve the efficiency of the codes on the target channel (Phys. Rev. A 84, 062317 (2011), P. Jouguet, S. Kunz-Jacques and A. Leverrier)

What is a good code for the BIAWGNC?

- A code is designed for a channel **and a SNR**
- Free parameter: the code rate $R = \frac{n-m}{n}$, m the number of parity-check equations, n the length
- Low SNR / Lot of redundancy / Low rate
- Efficiency $\beta(SNR) = \frac{R}{C(SNR)}$
- Typical values:
  - Slice reconciliation: $\beta = 90\%$, SNR$= 3$, @30km
  - Multidimensional reconciliation: $\beta = 89\%$, SNR$= 0.5$, @50km

Set of available codes

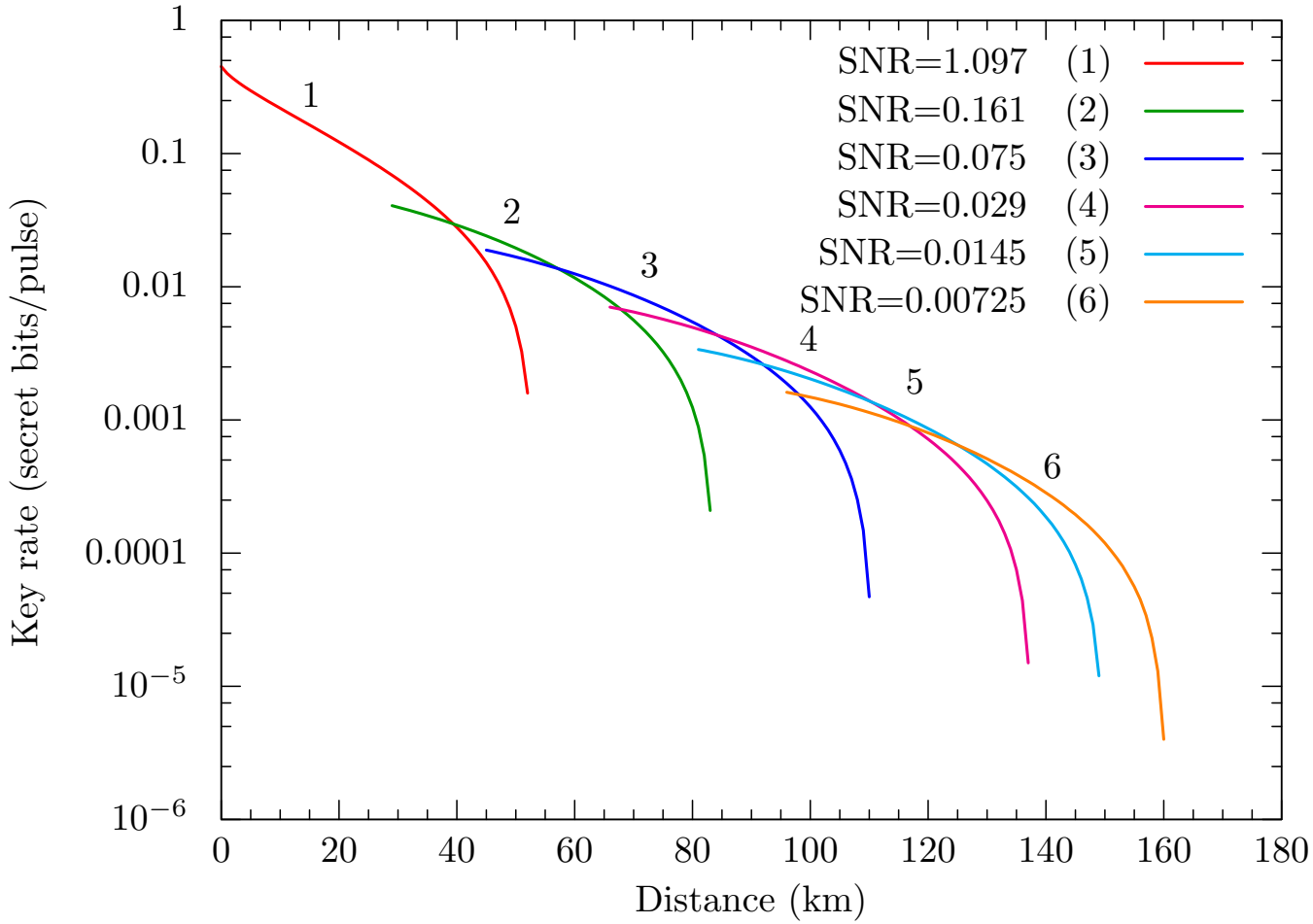
β	SNR
93.6%	1.097
93.1%	0.161
95.8%	0.075
96.9%	0.029
96.6%	0.0145
95.9%	0.00725

How to get more flexibility on the SNR?

- Possible to design codes with lower rates
- Not necessary: repetition codes
- Shortening, puncturing
- Optimization on the modulation variance

Theoretical secret key rate

$V_A \in \{1, 100\},\ T = 10^{-0.2d/10},\ \xi = 0.01,\ \eta = 0.6,\ V_{el} = 0.01$



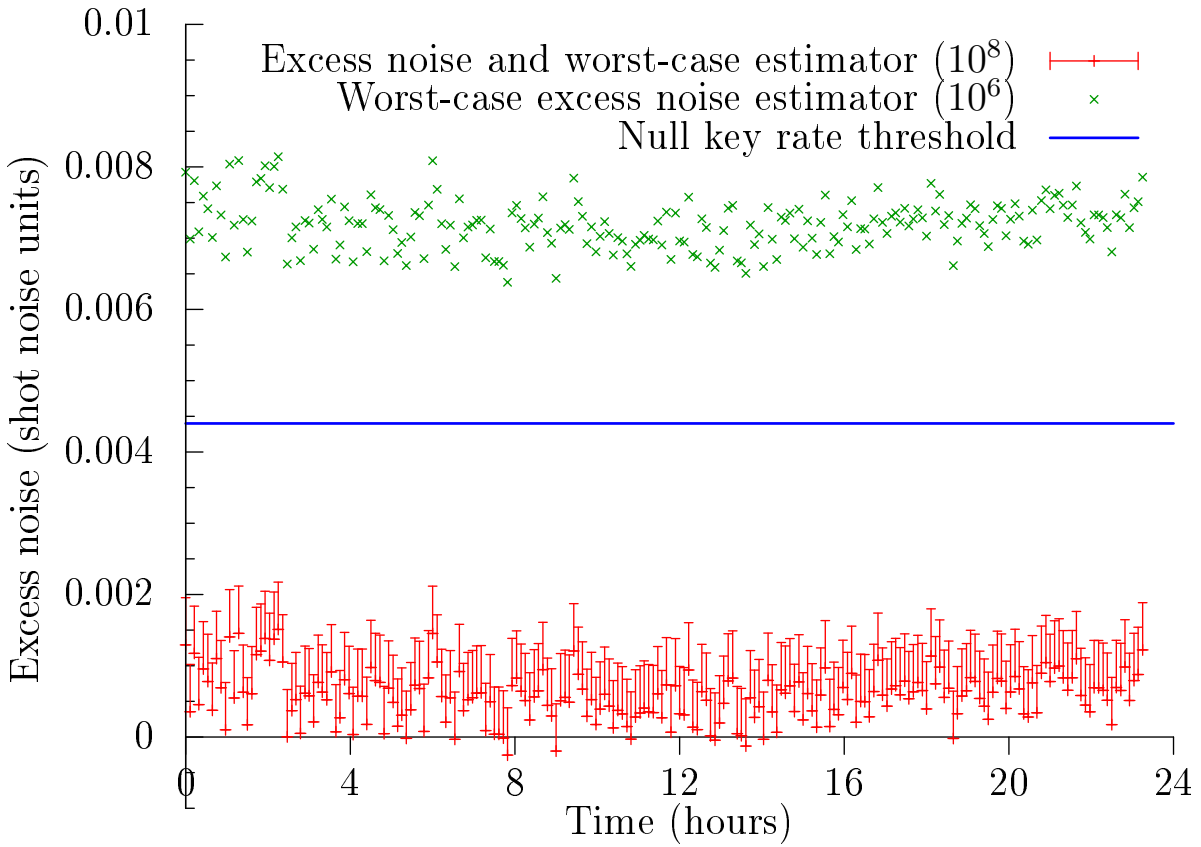
SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

Finite size effects

- First analysis for discrete modulation protocols in Phys. Rev. A 81, 062343 (2010), Leverrier et al.
- Statistical uncertainty over estimated parameters (T, ξ)
- $K = \frac{n}{N}(\beta I(x;y) - S^{\epsilon PE}(y;E) - \Delta(n))$
- Extended analysis for Gaussian modulation, including imperfect homodyne detection (efficiency, electronic noise) and shot noise estimation (Phys. Rev. A 86, 032309 (2012))
- Main effect: uncertainty on the excess noise ξ

Experimental results (arXiv:1210.6216)

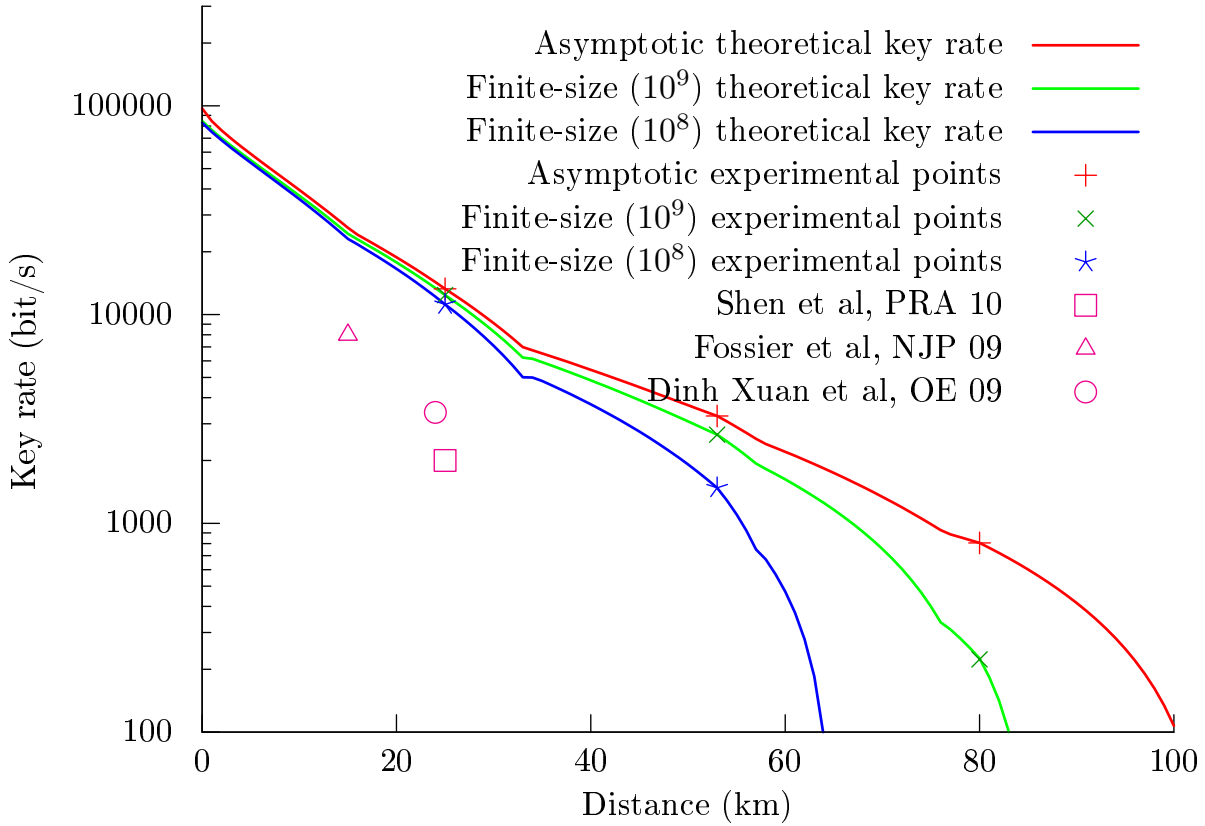
$d = 53$km, $\eta = 0.552$, $V_{el} = 0.015$, SNR$= 0.17$, $\beta = 94\%$, $\epsilon = 10^{-10}$



SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

Experimental results (arXiv:1210.6216)

Parameters: $d = 25$km,53km,80km, $\eta = 0.552$, $V_{elec} = 0.015$, SNR=1.1,0.17,0.08, $\beta = 94\%$, $\epsilon = 10^{-10}$



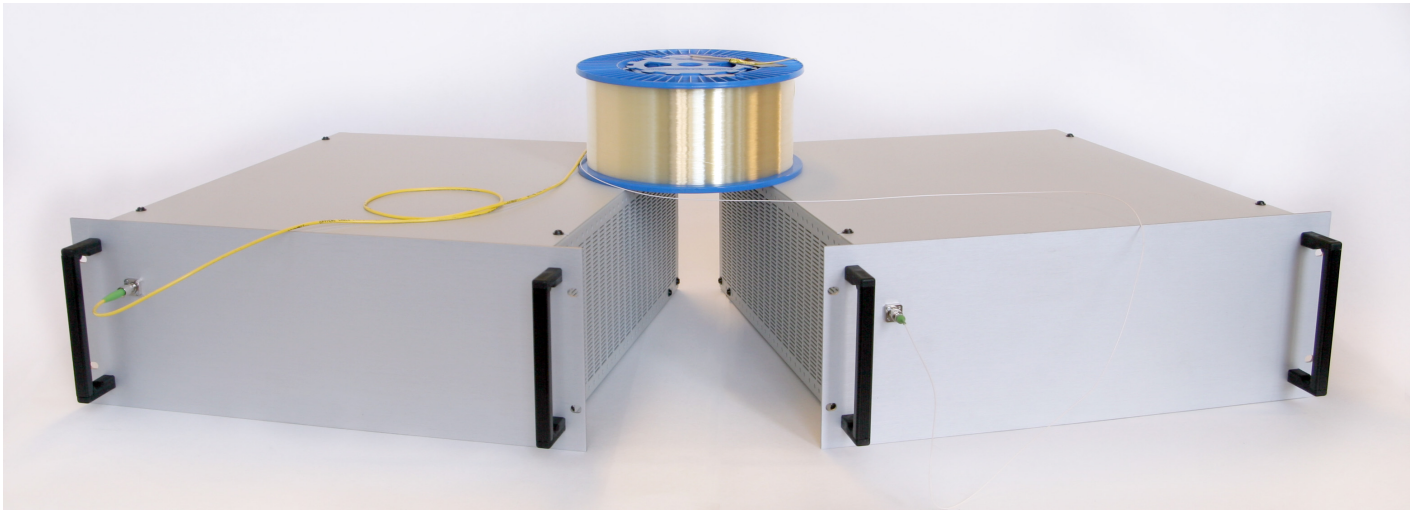
Imperfect preparation

- Thermal noise (Phys. Rev. A 81, 022318 (2010), Usenko and Filip)
- Gaussian modulation: truncated and discretized (finite amount of randomness)
  - Can be taken into account into the security proof (Phys. Rev. A 86, 032309 (2012))
  - But a lot of random numbers are required (+ sifting and multidimensional protocol)
- Calibration procedures
  - Calibration of the homodyne detection
  - Calibration of the phase noise

Summary

- Long distance CVQKD with Gaussian modulation is possible thanks to low SNR error-correction capability
- Computing-power consuming because of decoding close to the threshold
- We use GPU (30× faster than CPU plus friendly Moore's law)
- Higher secure distance with virtual Gaussian post-selection? (arxiv:1205.6933, J. Fiurasek, N. J. Cerf, arxiv:1206.0936, N. Walk et al.)
- Work on DWDM in the pipeline
- Side-channel attack based on the local oscillator calibration procedure (in preparation)

Enquire about Cygnus



- An **open and customizable** CVQKD research platform
- Tests/demonstrations of integration in optical networks

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY