QCRYPT 2013

August 04,2013
IQC, University of Waterloo
Canada

Saturation Attack on Continuous-Variable Quantum Key Distribution System

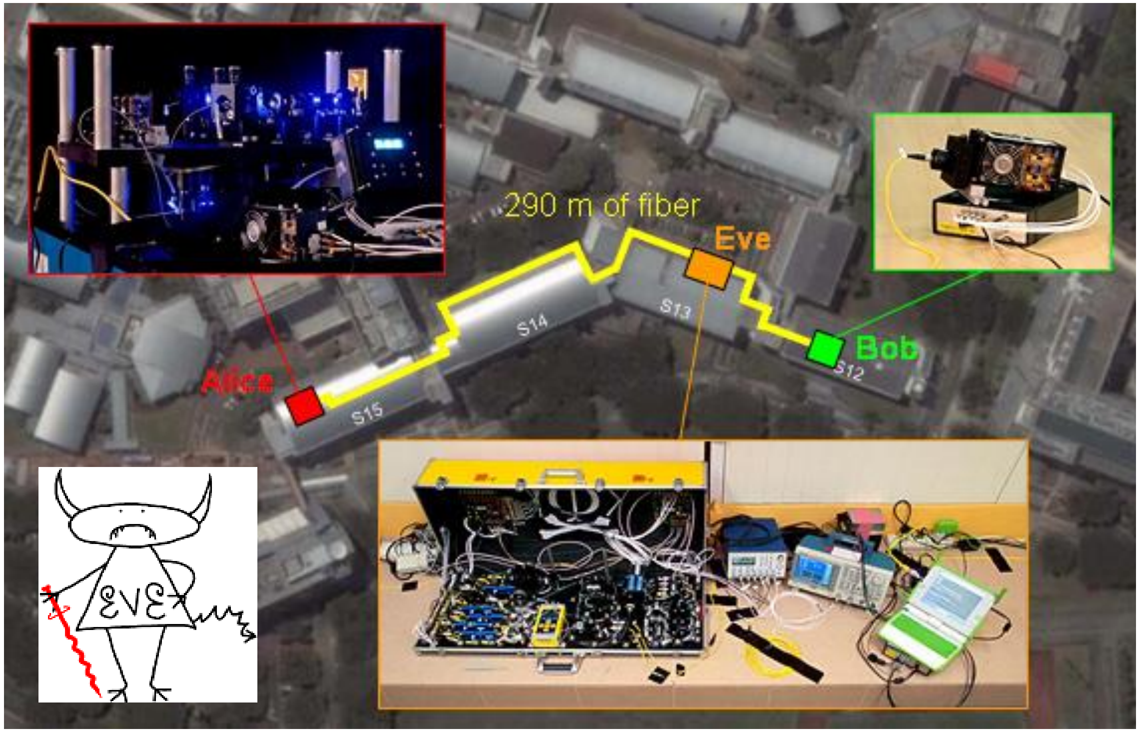
Hao Qin*, Rupesh Kumar, and Romain Alléaume

Quantum Information Team @ TELECOM ParisTech,
Institut MINES-TELECOM, LTCI UMR 5141,CNRS

*Contact:hao.qin@telecom-paristech.fr

Practical security of Quantum Key Distribution

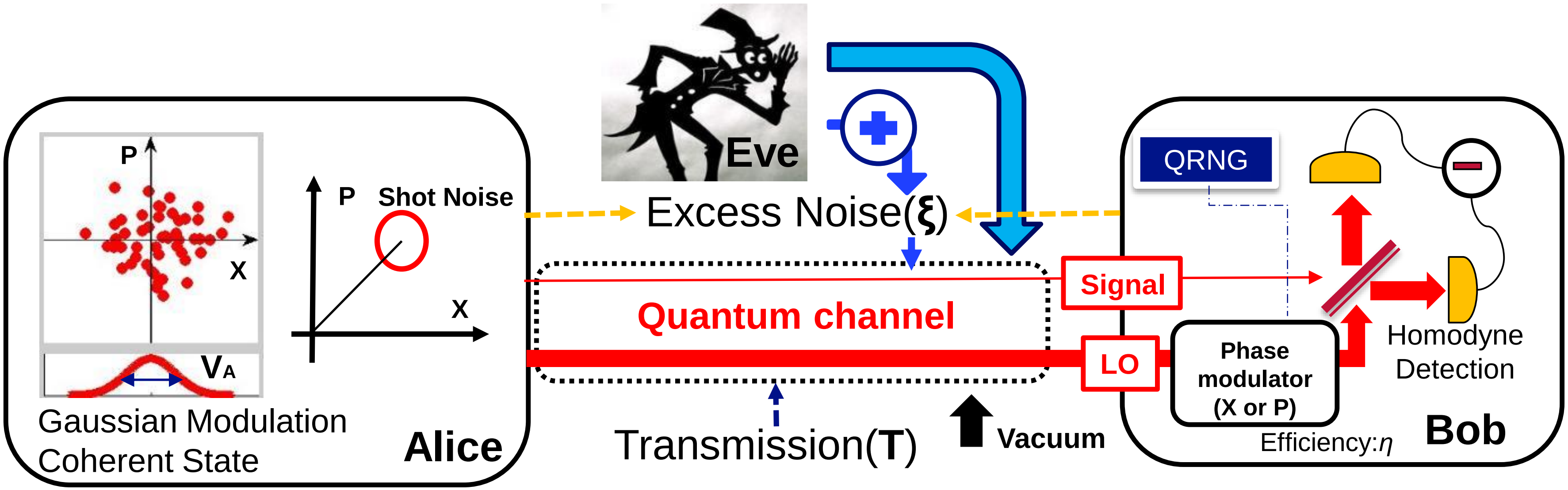
- Security of practical QKD depends on physical implementations
- Side channel attacks in DV QKD
- **Single photon detector is often a target**



Full-field implementation of a perfect eavesdropper on a quantum cryptography system

V. Makarov *et al.* **, Nature Comm.2, 349 (2011)**

Continuous-Variable Quantum Key Distribution



- Gaussian modulation coherent state (GMCS) protocol (F. Grosshans *et al.*, Nature, 421:238–241, 2003)
- Quantum channel is totally characterized by ***T*** and ***ξ***
- Side channel in CV QKD? Practical security?

Parameter Estimations in CV QKD

- **Gaussian linear model** $y = tx + z \ (\sigma_z^2 = N_0 + \eta T\xi + \nu_{ele})$
- Gaussian random variable: x: Alice, y: Bob, z: Noise, t: $\sqrt{\eta T}$
- $< x^2 > = V_A$
- $< xy > = \sqrt{\eta T} V_A$
- $< y^2 > = \eta T V_A + N_0 + \eta T\xi + \nu_{ele}$

Transmission

$$T = \frac{< xy >^2}{\eta < x^2 >^2}$$

Calibration of shot noise (N_0) on Bob side (Alice and Bob close the quantum channel)

- $< {y_0}^2 > = N_0 + \nu_{ele}$

Excess noise in shot noise unit (SNU)

$$\xi_{SNU} = \frac{\xi}{N_0} = \frac{< y^2 >}{\eta T} - \frac{V_A}{N_0} - \frac{1}{\eta T} - \frac{\nu_{ele}}{\eta T N_0}$$

- **Secret key rate based on collective attack**

$$\Delta I = \beta I_{AB} - \chi_{BE}$$

Side channel attack in practical CV QKD system

Manipulation of Local oscillator

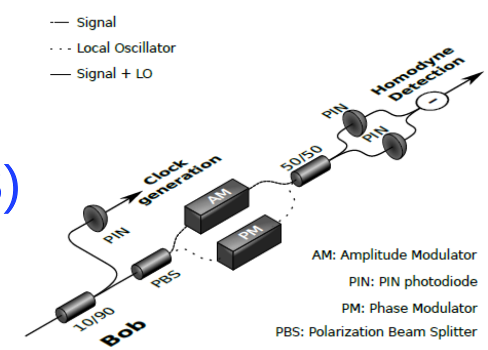
Equal-amplitude attack

- H.Häseler *et al.* Phys. Rev. A 77, 032303 (2008)

Calibration attack and preventing

- A. Ferenczi *et al.* CLEOE-IQEC, Vol. 13 (2007)
- P. Jouguet *et al.* Phys. Rev. A 87, 062313 (2013)

Influence on shot noise calibration.



LO fluctuation opens a loophole

- X-C. Ma *et al.* arXiv:1303.6043 (2013)

Inaccurate LO monitoring could lead to attack.

➢ **Counter measure : Monitor LO Intensity & Real time shot noise calibration**

Side channel attack in practical CV QKD system

Wavelength attack

- X-C. Ma *et al.* Phys. Rev. A 87, 052309 (2013)
- J-Z. Huang *et al.* Phys. Rev. A 87, 062329 (2013)
- Wavelength dependent beam splitter
- **Attack is possible even if LO is monitored.**

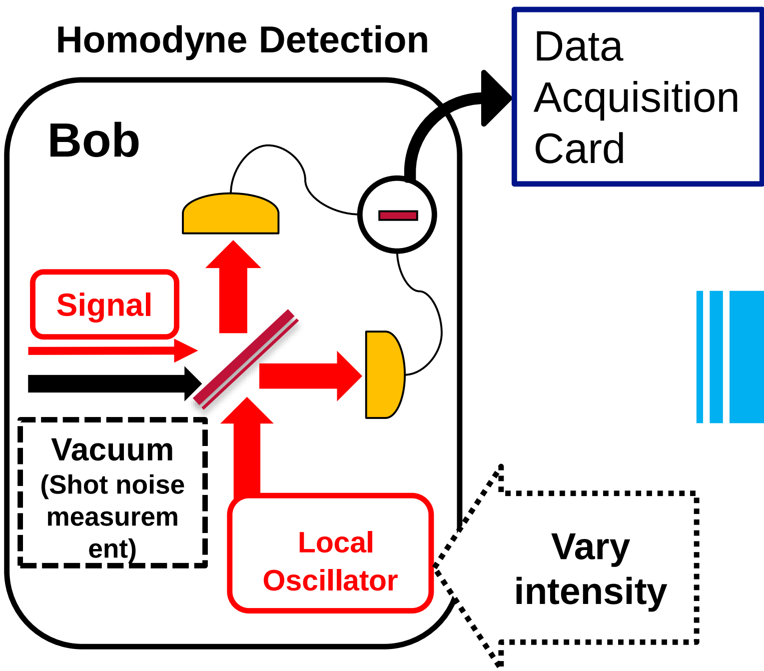
Counter measure :

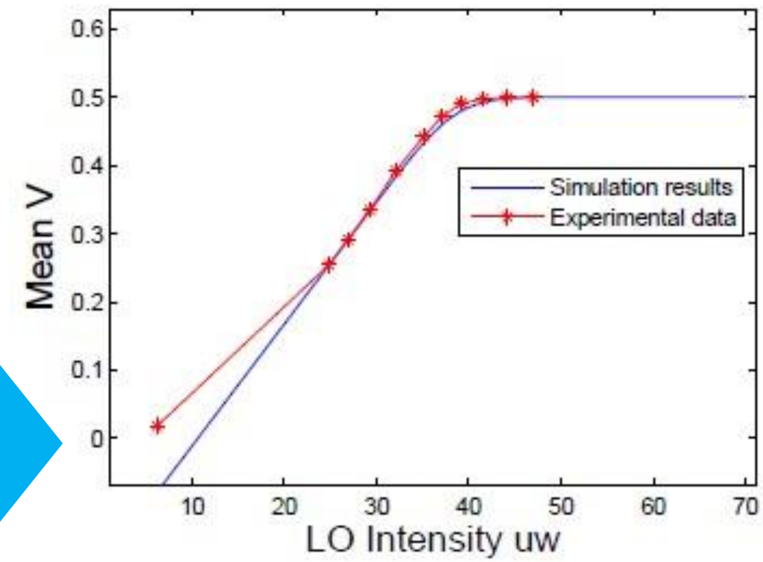
- Wavelength filter
- Wavelength independent beam splitter

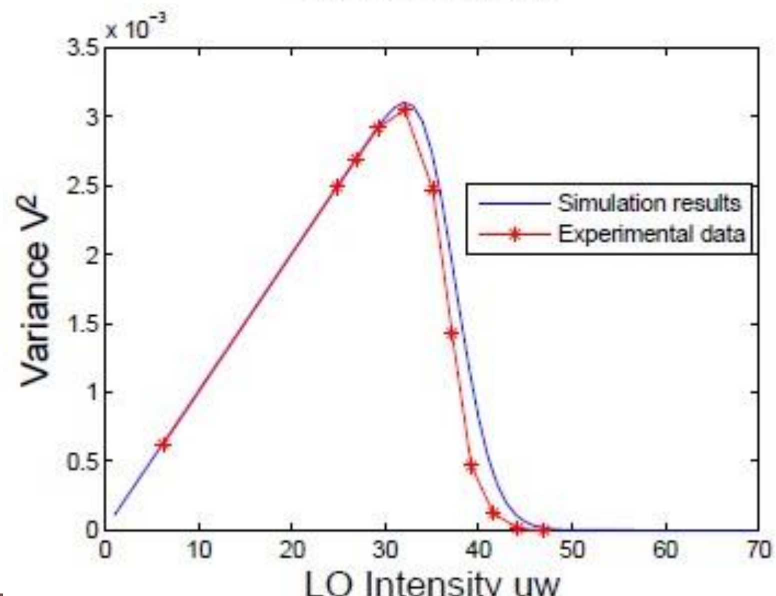
✓ Combined with intercept resend attack

✓ Entanglement breaking: R. Namiki *et al.* Phys. Rev. A 72, 024301 (2005)
✓ Experimental demonstration of intercept resend attack on CV QKD:
J. Lodewyck, *et al.* Phys. Rev. Lett, 98, 030503 (2007)

Experimental observation : Saturation of homodyne detection (Shot noise calibration)





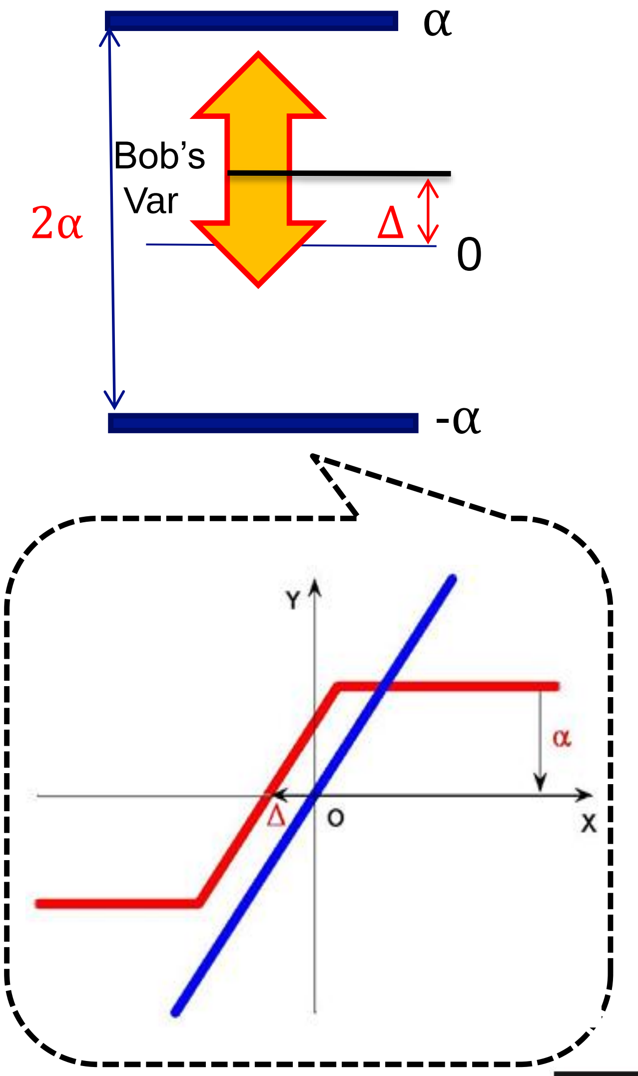


- HD response saturates: Violation of the assumption in security proof of CV QKD
- Impact on the security? **New threat?**

Saturation model

- $y_{sat} = \begin{cases} \alpha & y \geq \alpha \\ tx + z + \Delta & -\alpha < y < \alpha \\ -\alpha & y \leq -\alpha \end{cases}$
- Detection range can not be infinity
- α is a **characteristic** of the detector
- Δ can be **manipulated** by Eve
- When α is large and Δ is small, saturation model returns to Gaussian linear model
  $y = tx + z$

Homodyne detector's
Data acquisition card



What happens when there is saturation ?

- **Saturation case:** $y_{sat} = \begin{cases} \alpha & y \geq \alpha \\ tx + z + \Delta & -\alpha < y < \alpha \\ -\alpha & y \leq -\alpha \end{cases}$

Analysis in the low saturation region $(\alpha^2 \gg V_B, \alpha^2 \gg N_0)$:

- $< x^2 > = V_A$ unchanged
- $< xy_{sat} > = \sqrt{\eta T_{sat}} V_A$ T_{sat} $<T$
  - $< xy_{sat} > \approx \frac{1}{2}\left[1 + \mathrm{erf}\left(\frac{\alpha - \Delta}{\sqrt{2\sigma_Z^2 + 2t^2\sigma_X^2}}\right)\right] < xy >$
- $V_{B,sat} = \eta T' V_A + N_0 + \eta T' \xi' + v_{ele}$ $V_{B,sat} < V_B$

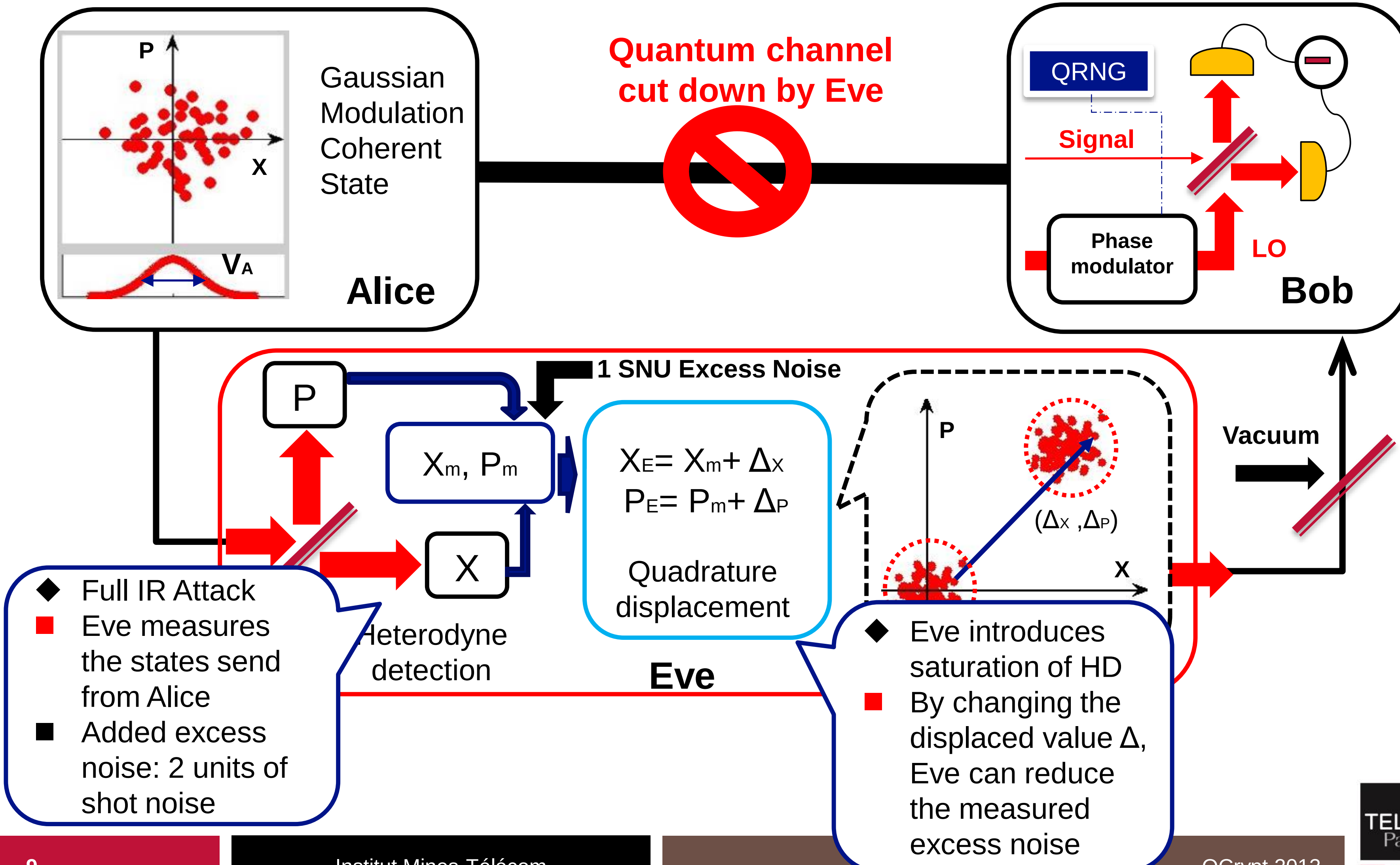
- ***Shot noise calibration***: $< {y_0}^2 > = < z^2 > \approx N_0 + v_{ele}$ unchanged

Excess noise in SNU will be changed and could be smaller

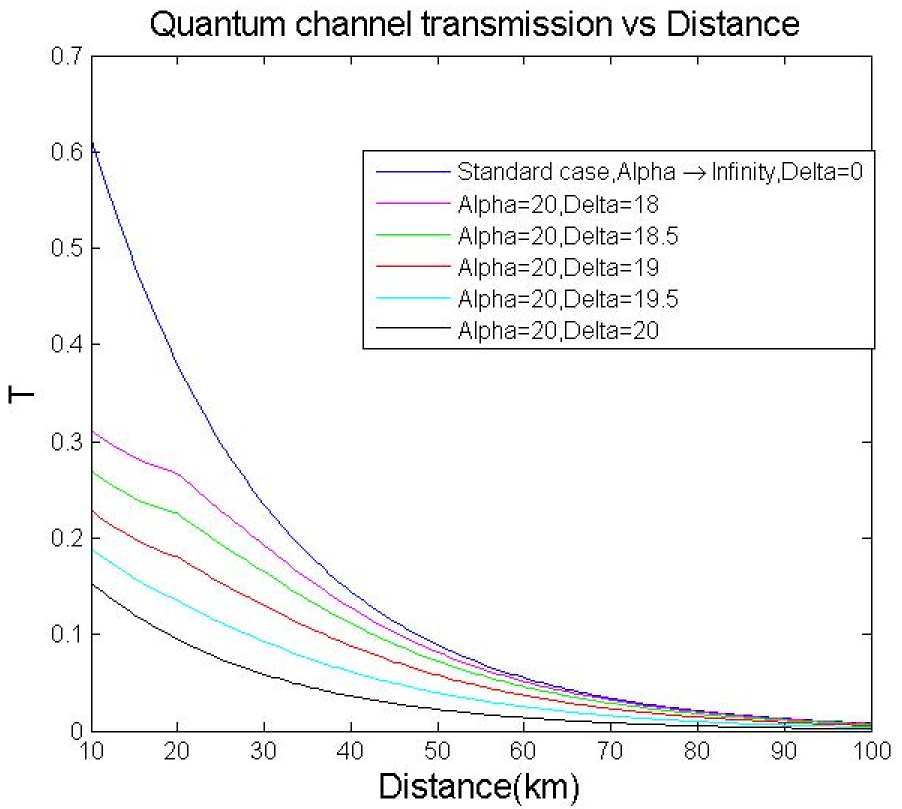
$$\xi'_{SNU} = \frac{\xi'}{N_0} = \frac{V_{B,sat}}{\eta T_{sat}} - \frac{V_A}{N_0} - \frac{1}{\eta T_{sat}} - \frac{v_{ele}}{\eta T_{sat} N_0}$$

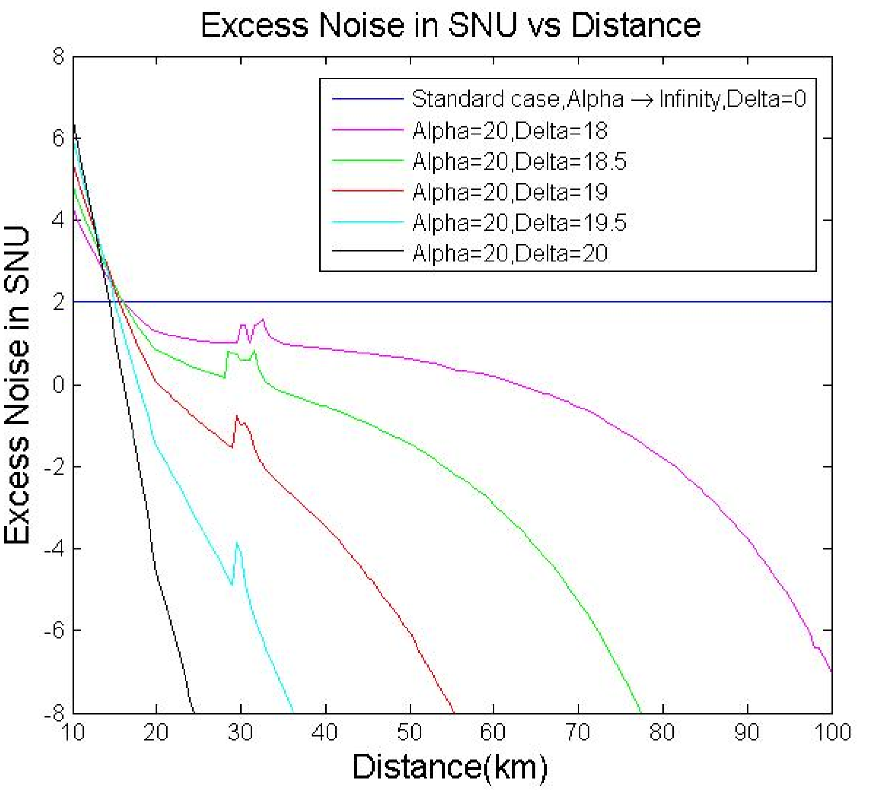
Saturation attack strategy

Full Intercept-resend attack+ Saturation of homodyne detection



T & Excess noise estimations based on a Full IR Attack+ Saturation of homodyne detection (Δ)



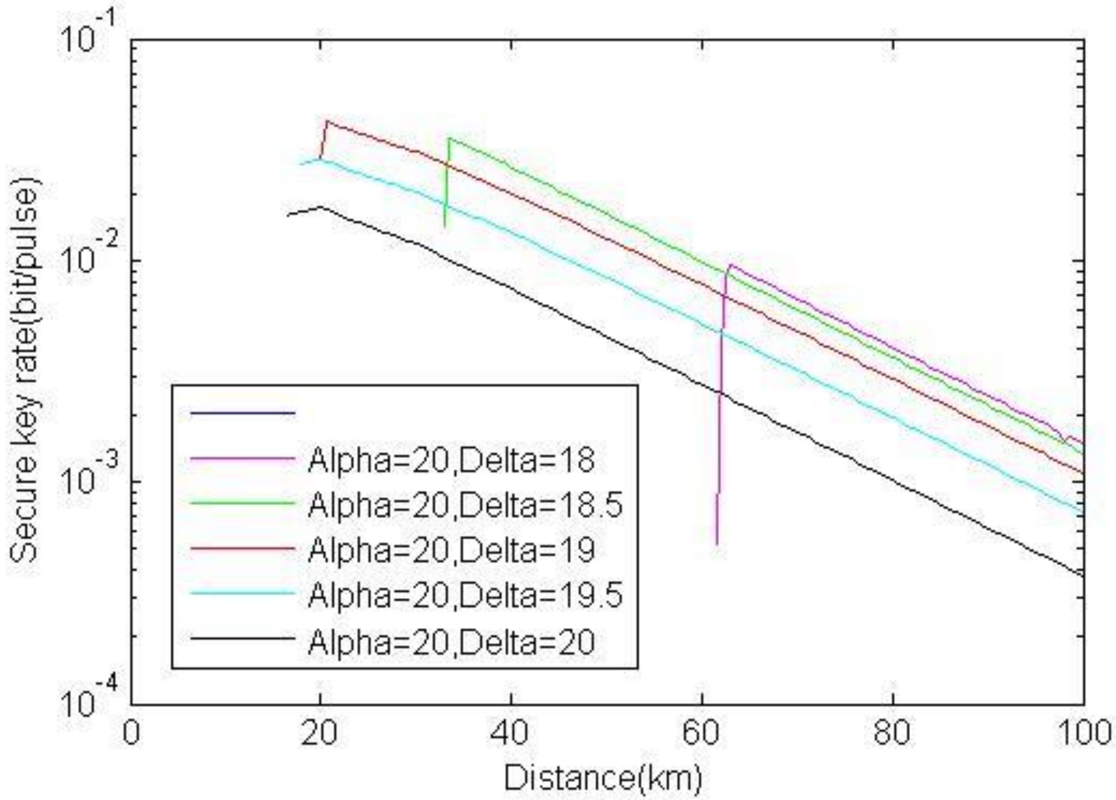


$V_A \in \{1,100\}$, η=60%, v_{ele}=0.01, ξ_{sys} =0.01, ξ_{Eve} =2, β=95%, a=0.21dB/km

- Excess noise can be reduced to an arbitrarily small value by changing Δ

Add noise if excess noise<0

Secret key rate estimated by Alice and Bob based on a Saturation model+ Full IR Attack



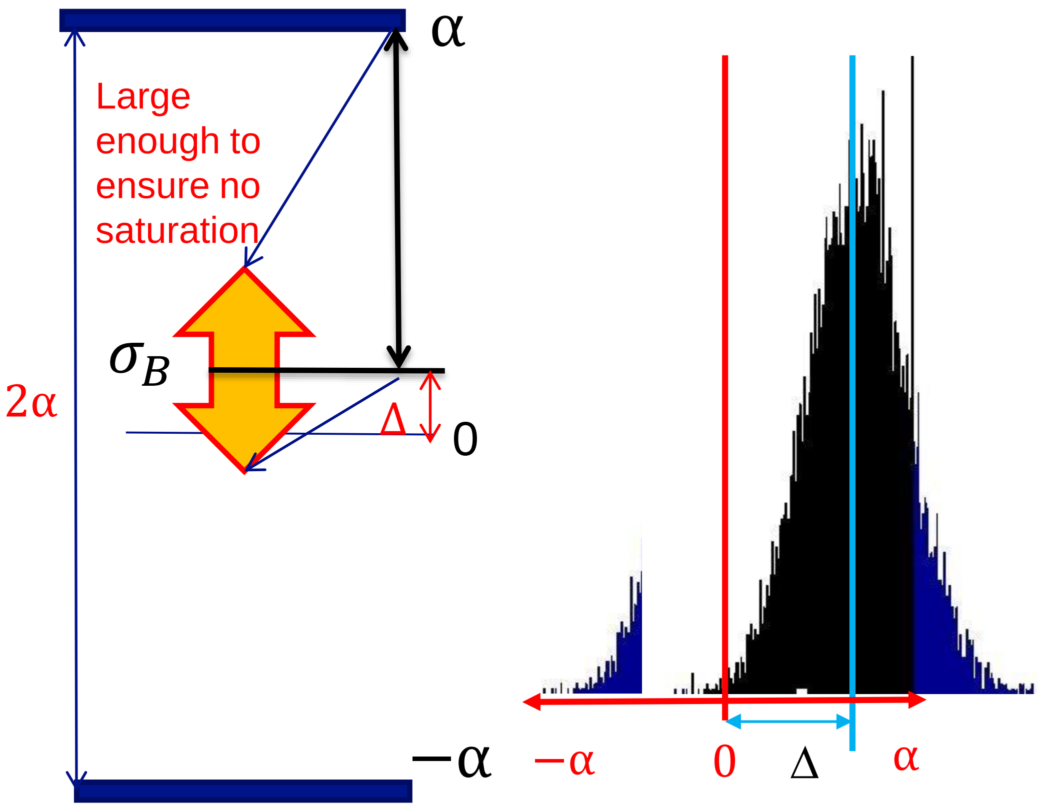
Parameter setup
$V_A \in \{1,100\}$
$\eta=60\%$
$v_{ele}=0.01$
$\xi_{sys}=0.01$
$\xi_{Eve}=2$
$\beta=95\%$
a=0.21dB/km

Collective attack
$\Delta I = \beta I_{AB} - \chi_{BE}$

- ✓ Alice and Bob believe they still have some positive "secret key rate". → **Effective attack, however T is reduced**
- ☐ Attack only possible above a distance which depends on Δ

TELECOM ParisTech

Counter measure



- No Saturation **if** $(\alpha-\Delta)^2 >> \sigma_B{}^2$

- Quantitatively, **if** [TEST(k)]
  - ✓ X_B passes χ_2 test with high confidence
  - ✓ $< y > +k\sigma_B < \alpha$ for large enough k

  Then

  - ❑ Pr(detector saturated) < ε(k)

- ➢ Proposed Counter-Measure Post-process on [TEST(k)]

➢ Alice and Bob should add a test on the first moment (mean value) of X_B

Conclusions

- We have experimentally observed the saturation of homodyne detection
- Propose saturation attack which fully compromises the practical security of CV QKD system implemented GMCS protocol
- Saturation attack is achievable with current technology
- Assumptions in security proofs ⟺ Agree?! ⟺ Practical setup
- Propose suitable counter measures against saturation based attack

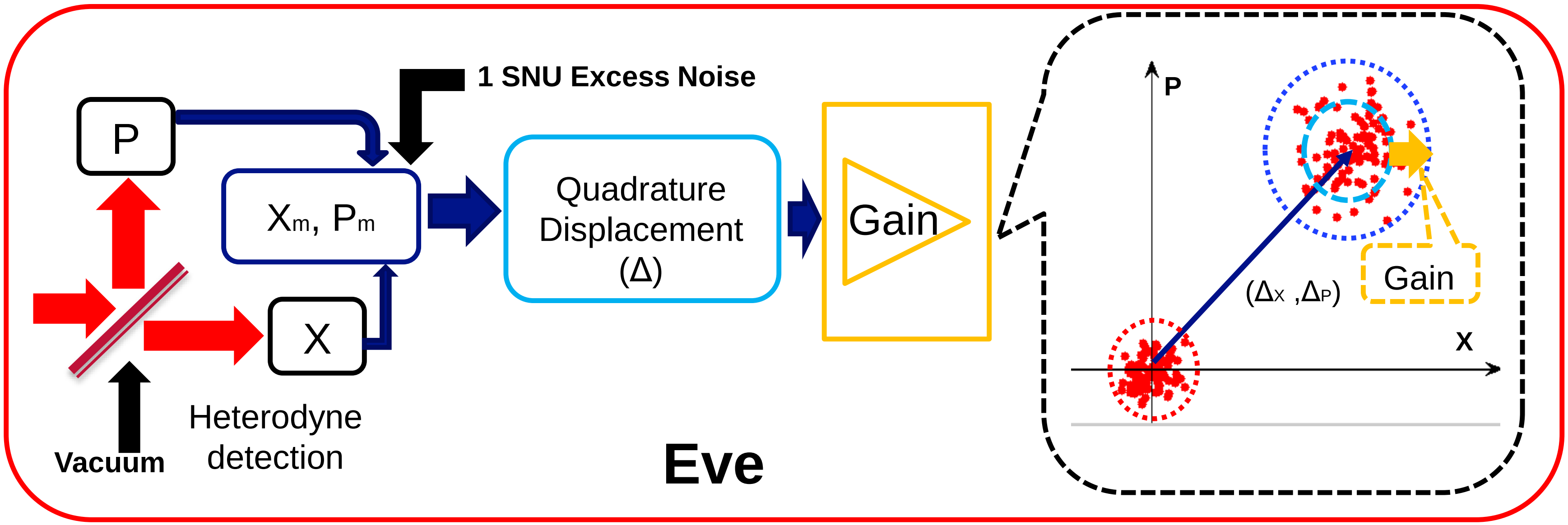
TELECOM ParisTech

THANK YOU!

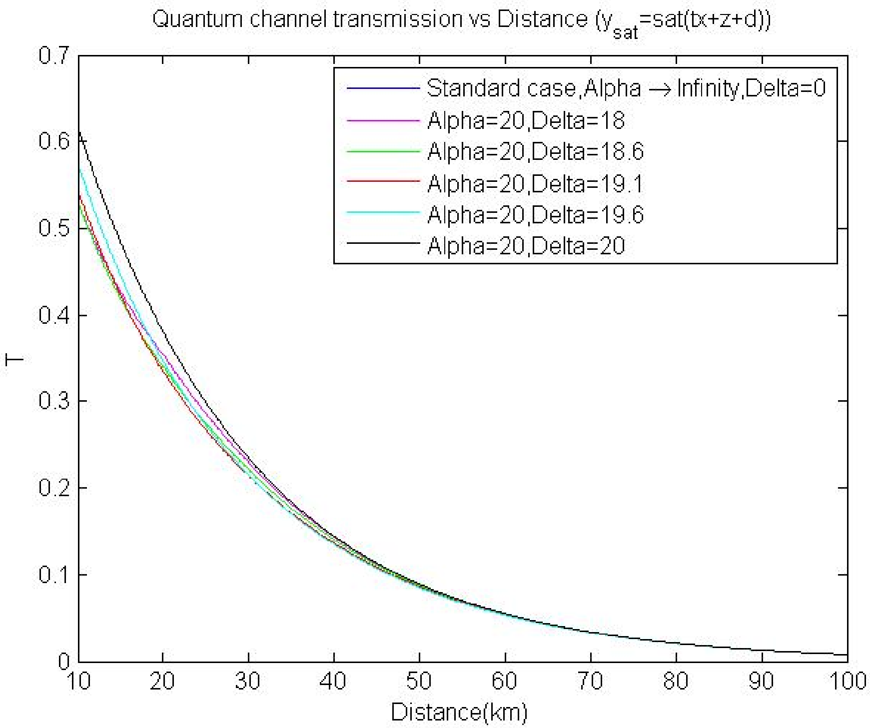
QUESTIONS?

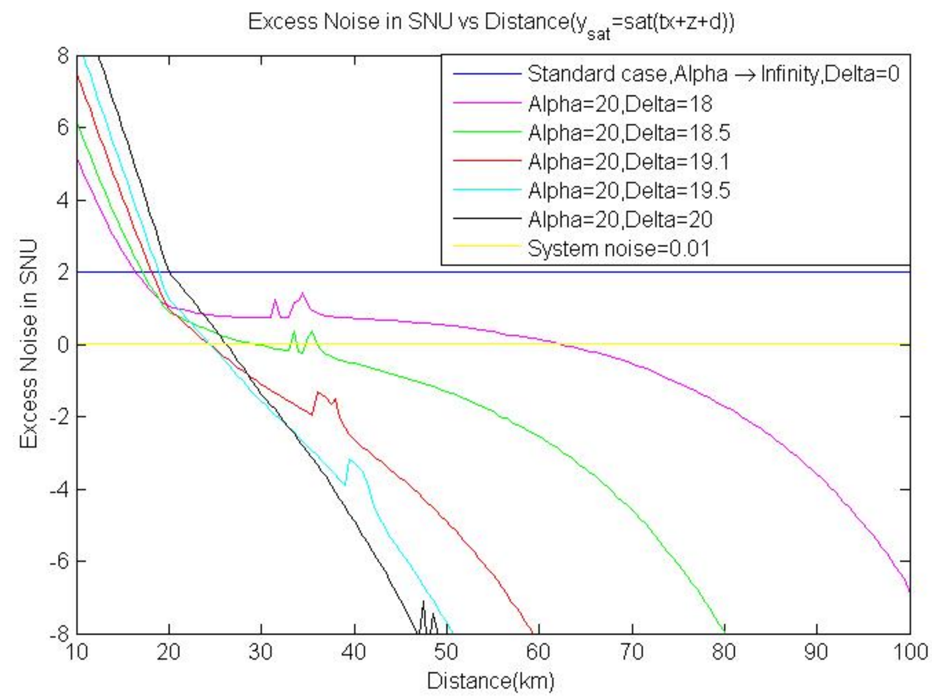
Looking for zero-error attack: Improved strategy

- Eve amplifies the states that she sends to Bob
- Eve has chance to control both T and ξ



T & Excess noise estimations under improved strategy



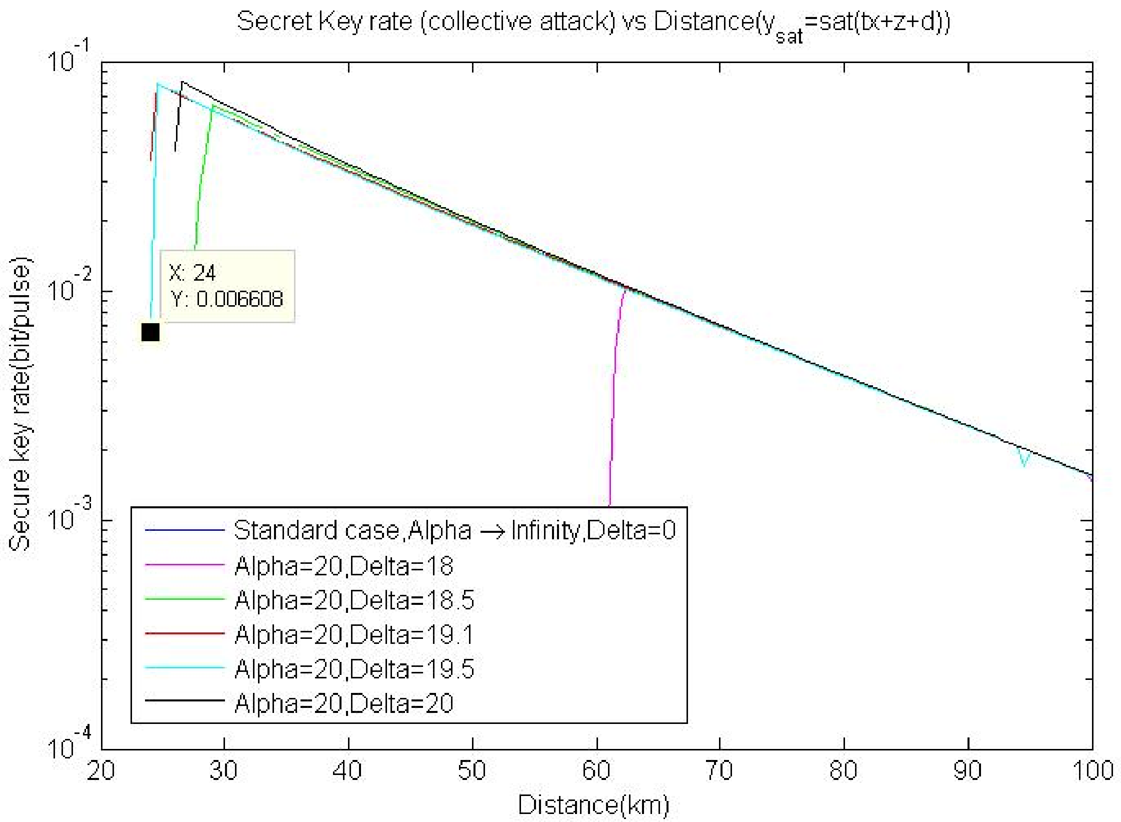


$V_A \in \{1,100\}$, η_{Bob}=60%, v_{ele}=0.01, ξ_{sys} =0.01, ξ_{Eve} =2, β=95%, a=0.21dB/km

✓ Quantum channel transmission is improved!

TELECOM ParisTech

Secret key rate estimated by Alice and Bob under improved strategy



Parameter setup

$V_A \in \{1,100\}$

$\eta=60\%$

$v_{ele}=0.01$

$\xi_{sys}=0.01$

$\xi_{Eve}=2$

$\beta=95\%$

a=0.21dB/km

Collective attack

$$\Delta I = \beta I_{AB} - \chi_{BE}$$

- Eve has achieved a “zero error” attack: T and ξ unchanged; Eve knows everything which Alice sends to Bob
- ✓ Key rate increases
- Attack distance from 24 km

Parameters taken for the simulations

- V_A, chosen according to Figure on the right (optimal choice of ECC, imposing a fixed SNR => V_A (vs Distance)).
- Efficiency of Bob : η=60%,
- Excess noise of electronics: v_{ele}=0.01
- Excess noise of system: ξ_{sys} =0.01
- Reconciliation efficiency: β=95%
- Attenuation coefficient: a=0.21dB/km

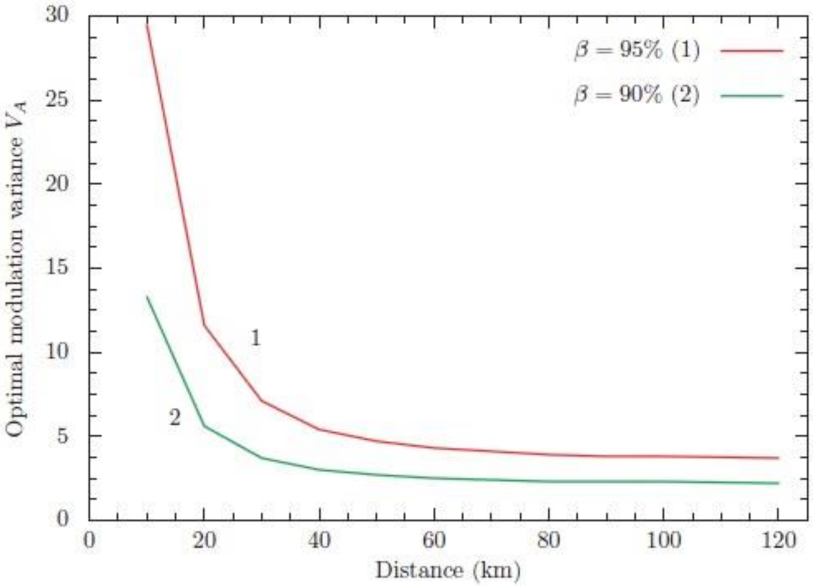


FIG. 2. (Color online) Optimal modulation variance with respect to the distance: $\eta = 0.6$, $V_{elec} = 0.01$, $\xi = 0.01$, $\alpha = 0.2$dB/km, and $\beta = 95\%$,90% from top to bottom.

Long-distance continuous-variable quantum key distribution with a Gaussian modulation
PRA 84, 062317, 2011

Experimental demonstration of long-distance continuous-variable quantum key distribution
Nature Photonics, 10, 1038, 2013