Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation

Aurélie Denys[1], Peter Brown[2], Anthony Leverrier[1]

1. Inria Paris, France 2. ENS de Lyon, France

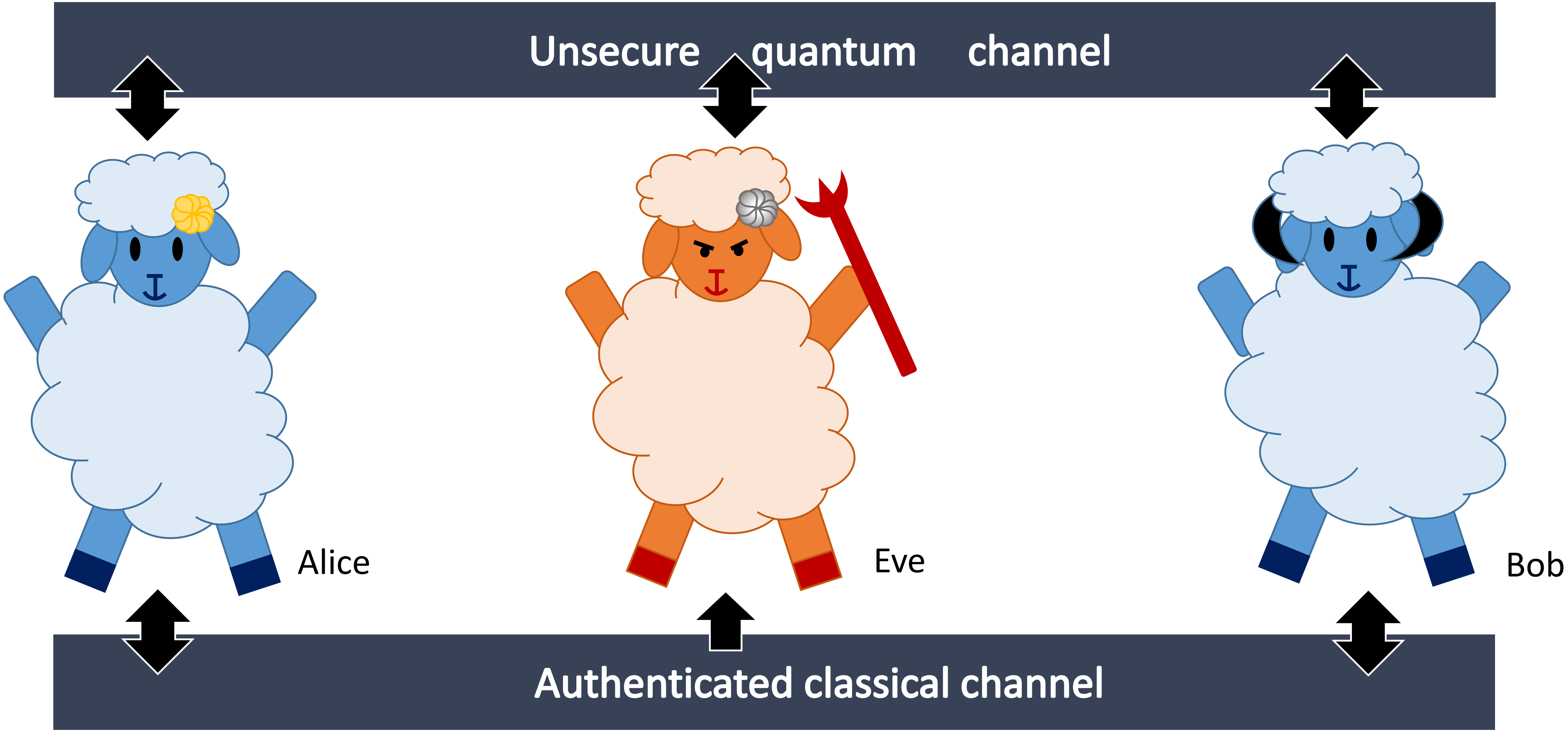
ENS DE LYON

Outline

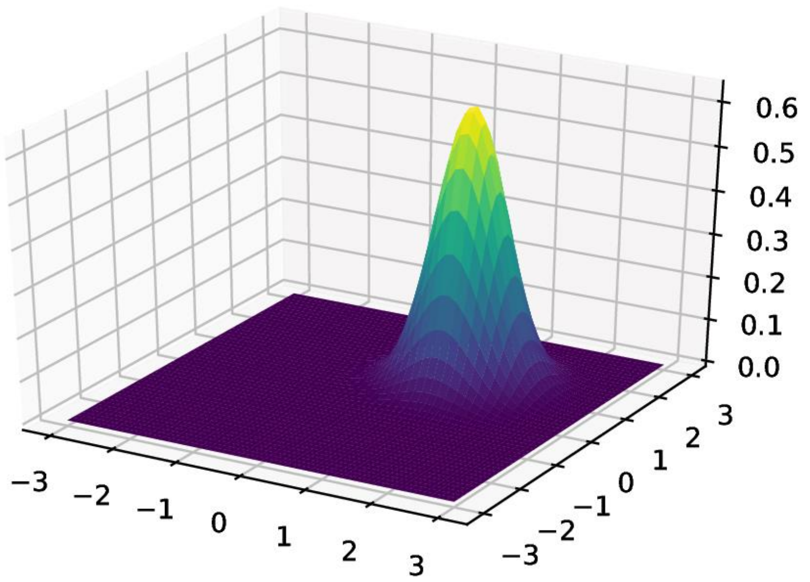
1. Motivation, main result and methods
2. Applications and extensions

1st part: Motivation, main result and methods

Quantum key distribution (QKD)



Continuous-variable (CV) QKD



Wigner function of the coherent state $|\alpha\rangle$ with $\alpha = 1 + i$

- Historically, discrete-variable (DV) protocols such as BB84
- DV QKD requires single-photon detectors → expensive
- Continuous variables [Ralph 1999] :
  - encoding on the quadratures of the quantified electromagnetic field + coherent detection

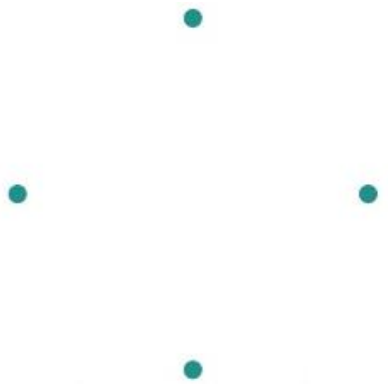
  → experimentally friendlier
  - But harder proofs (infinite-dimensional Fock space), and less tolerant to loss

Discretely modulated (DM) CVQKD

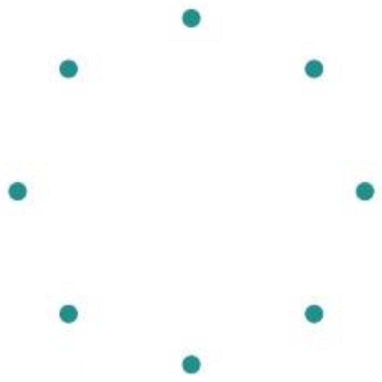
- Gaussian modulation : Alice sends $|\alpha\rangle$ with $\alpha \sim N(0, V_A)$ [Grosshans, Grangier 2002]
  (Almost complete) security proof [Garcia-Patron, Cerf 2006; Navascues, Grosshans, Acín 2006, Leverrier 2017]
- Infinite continuous constellation ≠ modulators have a finite precision and range → unrealistic

⟹ Discretely modulated CVQKD protocols

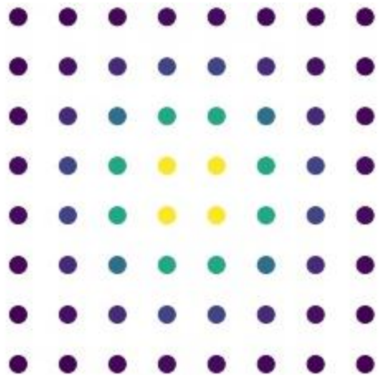
QPSK
(quadrature phase shift keying)



M-PSK
(M-phase shift keying)



QAM
(quadrature amplitude modulation)



→ Security proofs ?

(Prepare and measure) Protocol

Quantum part
(repeated many times)

1. Alice randomly chooses one coherent state $|\alpha_k\rangle$ with probability p_k from a set of coherent states $\{|\alpha_k\rangle\}_{k\in I}$ and sends it to Bob.

$$\tau = \sum_{k\in I} p_k \, |\alpha_k\rangle\langle\alpha_k|$$

2. Bob measures the quadratures of the states he receives, using coherent detection, and obtains β_k.

Classical post-processing

1. Discretisation of Bob's variables
2. Reconciliation step
3. Parameter estimation
4. Privacy amplification

Main result: analytical bound on the asymptotic secret key rate of DM CV QKD

- Security proof in the asymptotic regime, under the restriction to coherent attacks
- Asymptotic secret key rate = Important figure of merit to compare various protocols
- Numerical bounds [Ghorai et al PRX 2019; Lin et al PRX19], but : computationally-expensive, time-consuming, difficult to optimise over parameters, less reliable.
- Result : explicit analytical bound on the asymptotic secret key rate of any DM CV QKD protocol

Equivalent entanglement-based protocol and Devetak Winter bound

- Devetak-Winter bound :

Mutual information between Alice and Bob

Secret key rate $\mathrm{k} = I(X;Y) - \sup_{N:A' \to B} \chi(Y;E)$

- (Symmetrised) Covariance matrix :

Fixed by modulation V = $(V_A + 1)$

$$\Gamma = \begin{bmatrix} V\, I_2 & Z\, \hat{\sigma}_z \\ Z\, \hat{\sigma}_z & W\, I_2 \end{bmatrix}$$

Measured locally by Bob

Extremality of Gaussian states [García Patrón, Cerf 2006, Navascués, Grosshans, Acín2006]
→ upper bound on Holevo information depends on Γ and on the type of coherent detection used :

$$\sup_{N:A' \to B} \chi(Y;E) \leq \mathrm{f}(\Gamma)$$

⇒ Goal : Bound on $\mathrm{Z} = tr(\rho(\hat{a}\hat{b} + \hat{a}^{\dagger}\hat{b}^{\dagger}))$

Semidefinite Program

$$\min_{\rho} tr(\rho C)$$

$$\text{s.t.} \begin{cases} tr_B(\rho) = \bar{\tau} \\ tr(\rho C_1) = 2c_1 \\ tr(\rho C_2) = 2c_2 \\ tr\left(\rho(\mathrm{I} \otimes b^\dagger b)\right) = n_b \\ \rho \succcurlyeq 0 \end{cases}$$

ρ : state shared by Alice and Bob ; $C = \hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger$

ρ is obtained by applying a channel to the bipartite state prepared by Alice ; $\tau = \sum_k p_k |\alpha_k\rangle\langle\alpha_k|$.

Constraints obtained from observed statistics in the prepare & measure protocol :

- First moment constraints
- Second moment constraint

ρ is a density matrix

Bound on a solution of the SDP

$$K = z\left(A - x\,P^\dagger\right) + \frac{1}{z}B^\dagger$$

where x, z et P are parameters that we later optimise

$$KK^\dagger = E - C$$

$$KK^\dagger \succcurlyeq 0 \Rightarrow tr(\rho C) \leq tr(\rho E)$$

Depends on the modulation

$$tr(\rho C) \geq 2c_1 - 2\left(\left(n_B - \frac{c_2^2}{\langle n\rangle}\right)w\right)^{\frac{1}{2}} := Z^*$$

Estimated experimentally

Average photon number in the modulation

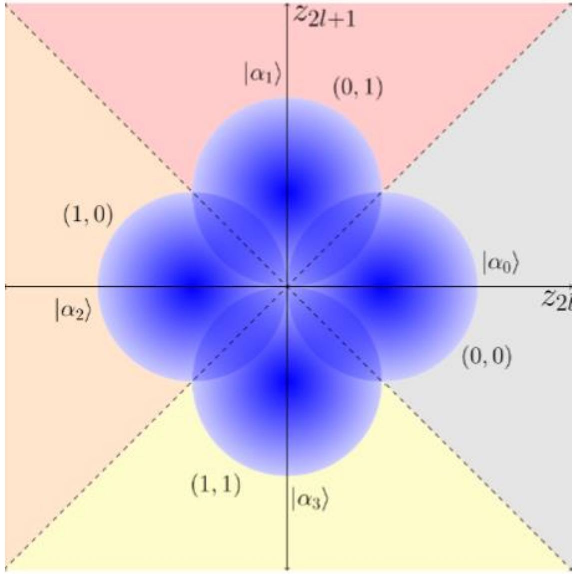
Continuity with known results: Gaussian modulation

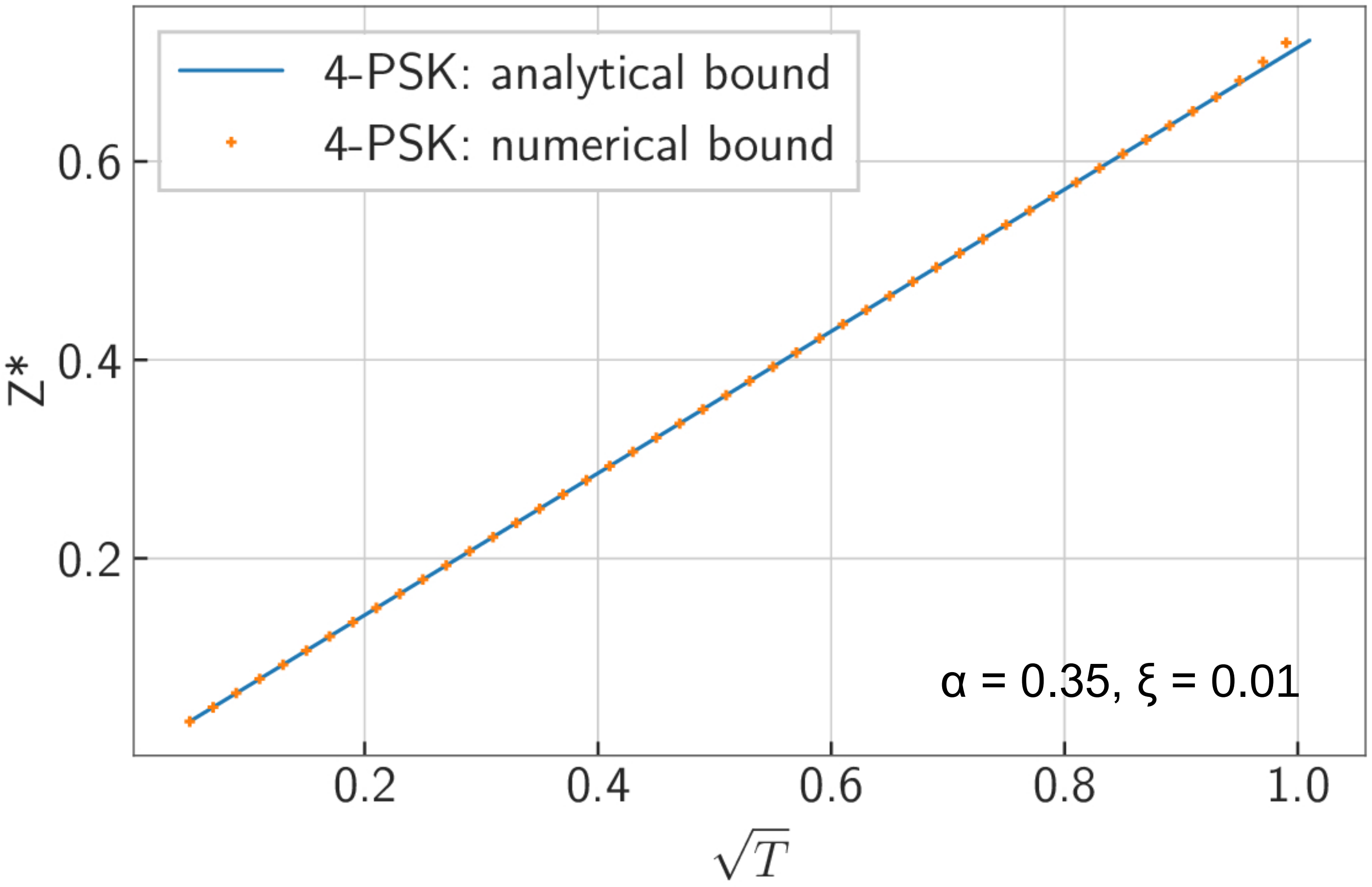
- Recall : $tr(\rho C) \leq 2\, c_1 - 2\left(\left(n_B - \frac{c_2^2}{\langle n\rangle}\right) w\right)^{\frac{1}{2}}$
- w vanishes for a Gaussian modulation
- If the transmittance channel is T, recover

$$tr(\rho C) = 2\sqrt{T\,(\langle n\rangle^2 + \langle n\rangle)}$$

⇒ tight bound in the case of a Gaussian modulation.

Continuity with known results: Quadrature Phase Shift Keying





Numerical bounds [from Ghorai et al PRX 2019] and our analytical bounds match except for transmittances very close to 1.

2nd part: Applications

Study of M-PSK &QAM, other applications, extensions

Methods to get practical results

- Typical Gaussian channel with transmittance T and excess noise ξ

$$\Gamma = \begin{bmatrix} (V_A + 1)\, I_2 & Z^*\, \hat{\sigma}_z \\ Z^*\, \hat{\sigma}_z & (1 + T\, V_A + T\, \xi) I_2 \end{bmatrix}$$

$$Z^* = 2\sqrt{T}\, tr\left(\tau^{1/2}\, a\, \tau^{1/2}\, a^\dagger\right) - \sqrt{2\, T\, \xi w}$$

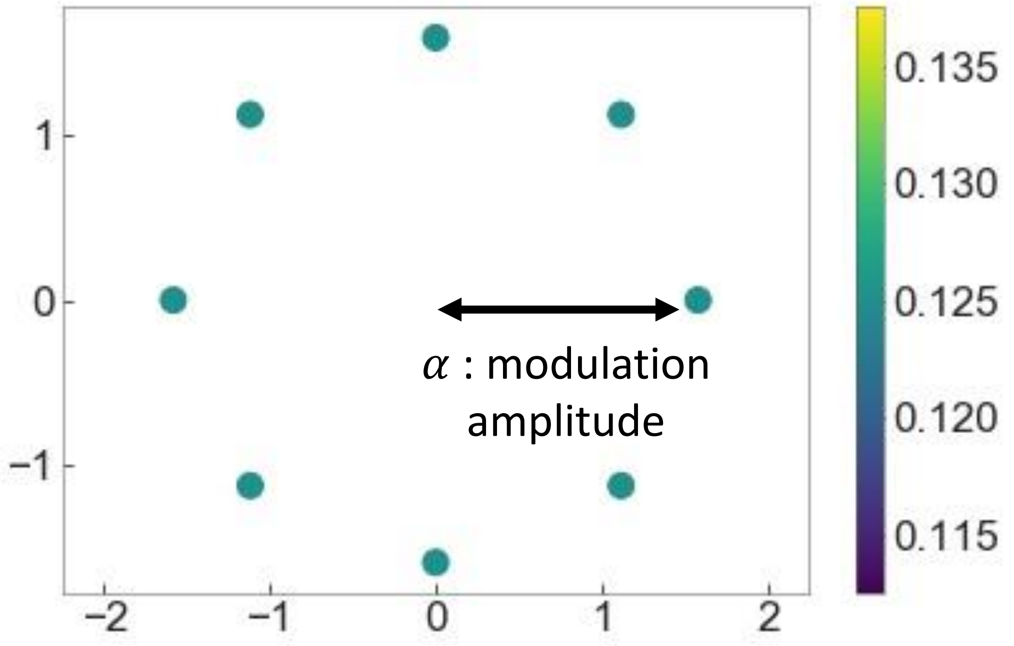
- Reconciliation efficiency

- Heterodyne detection

$$k = \beta I(X;Y) - \sup_{N:A' \to B} \chi(Y;E) \leq \beta I(X;Y) - f(\Gamma)$$

Phase-shift keying modulations (PSK)

Constellation made of coherent states regularly arranged on a circle in phase space, drawn with equal probability.

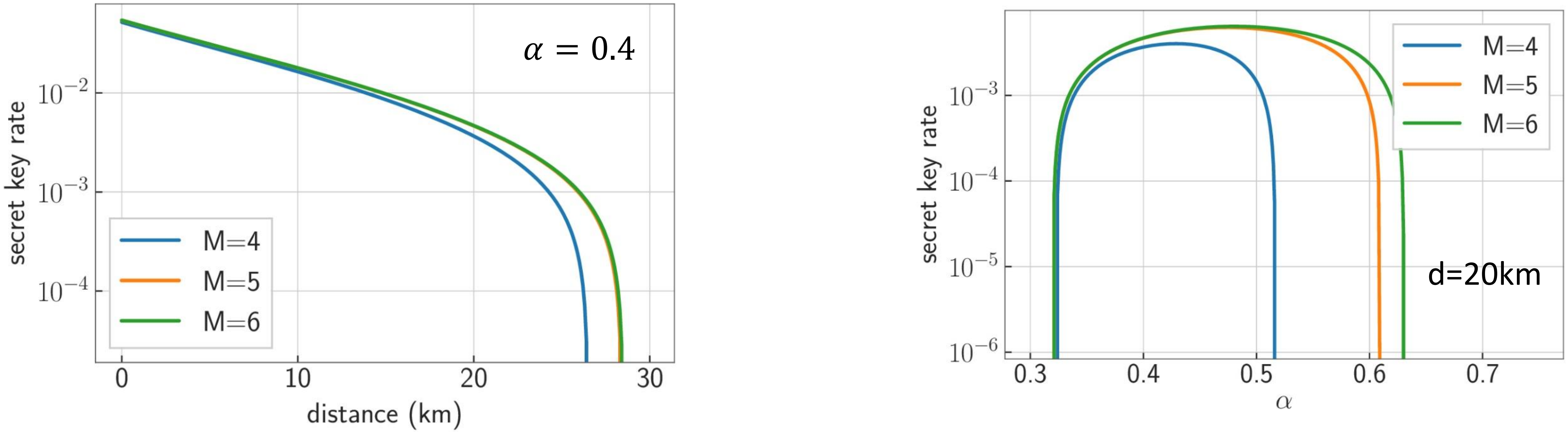


8-PSK constellation

Phase-shift keying modulations

- When the modulation amplitude is optimised, going beyond M=5 is essentially useless.
- But increasing M allows for larger possible values of the modulation amplitude.

⇒ The method of [Lin, Upadhyaya, Lütkenhaus 2019; Upadhyaya et al 2021] seems to give better bounds for M-PSK modulations.

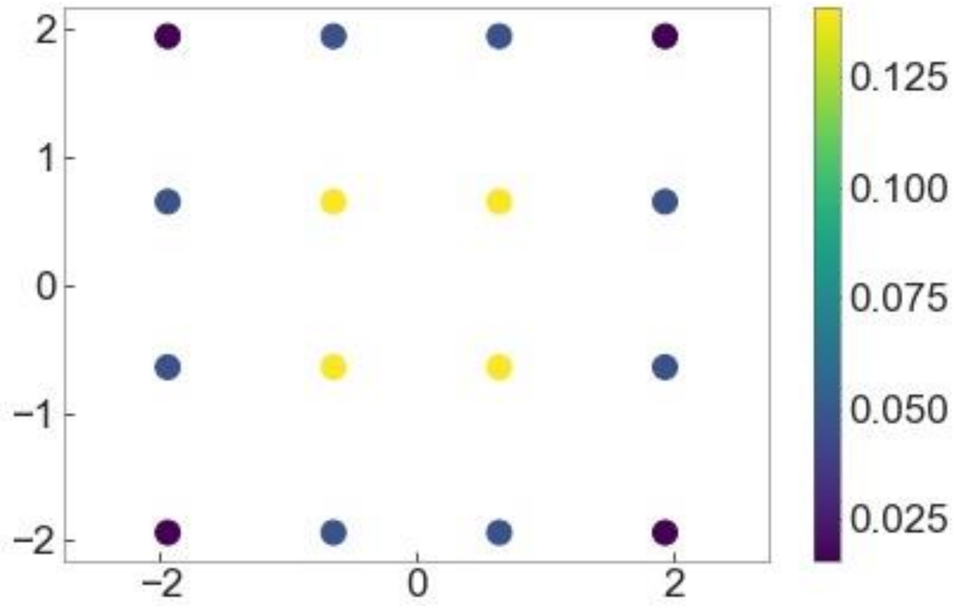


Asymptotic secret key rate for the M-PSK modulation schemes. ξ= 0.01 ; β=0.95.

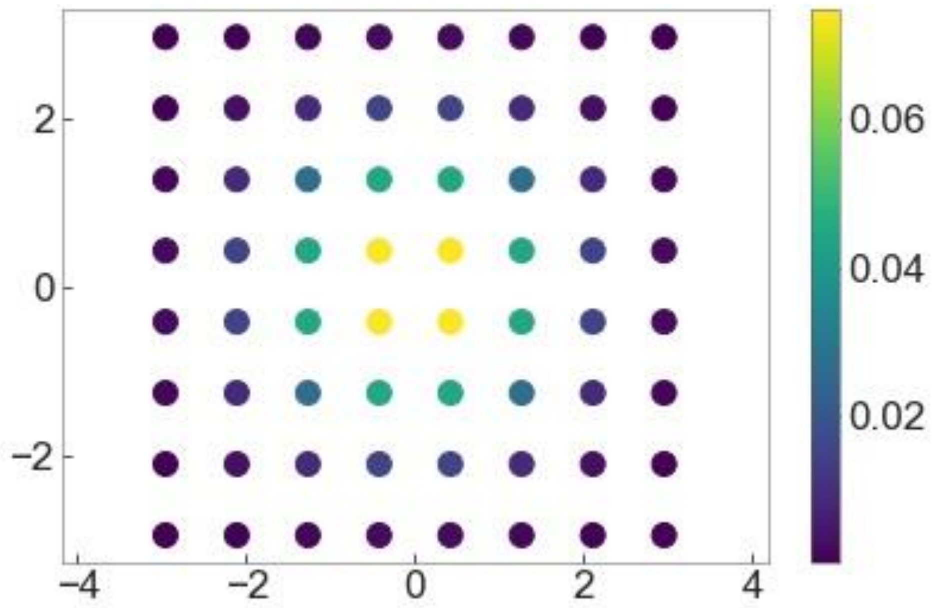
Quadrature-amplitude modulations (QAM)

Constellation : coherent states regularly arranged on a grid in phase space, drawn according to a certain distribution (e.g. binomial or discretised Gaussian distribution).

→ what people want to do in practise to use standard telecom equipment



16-QAM

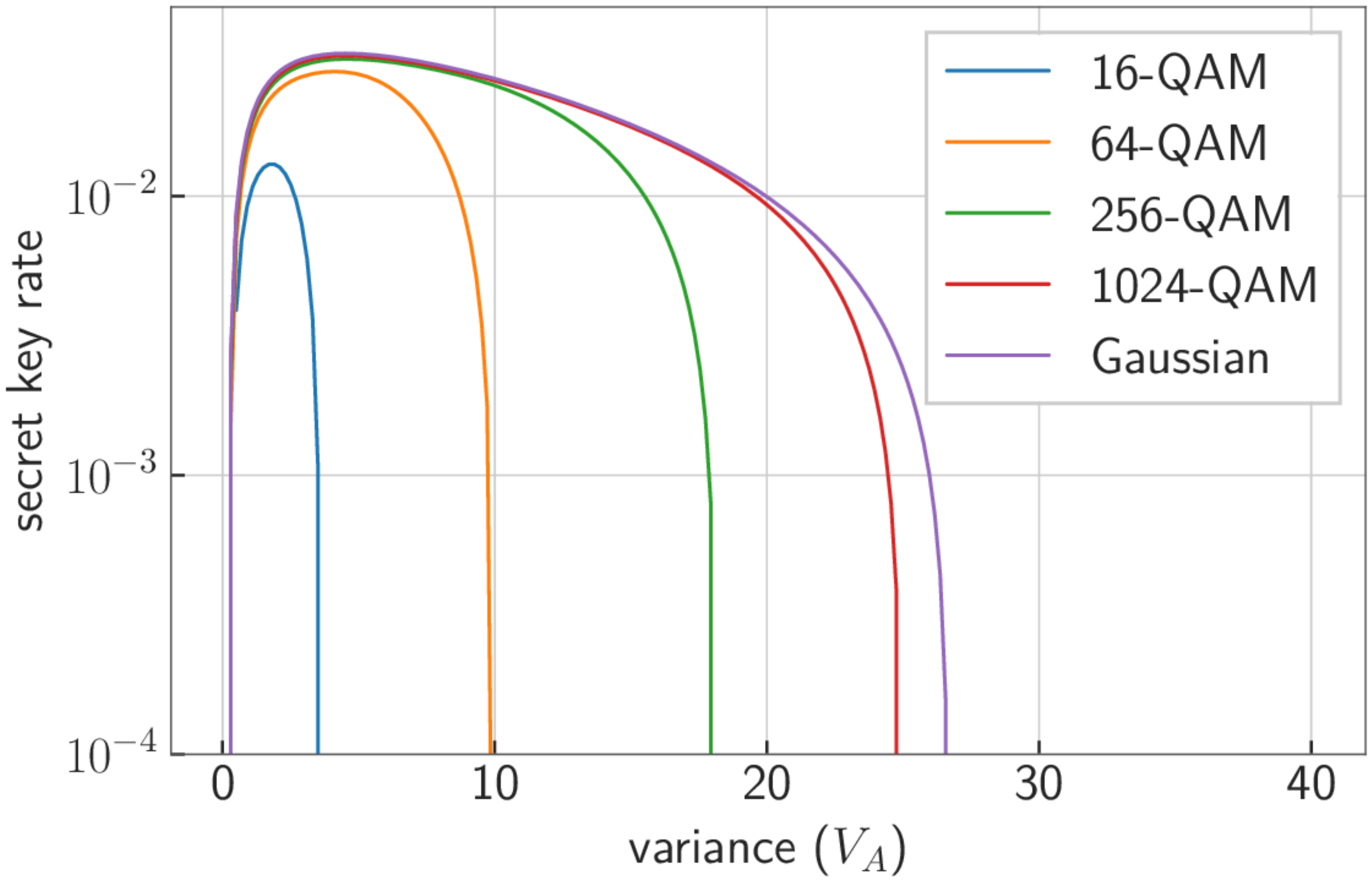


64-QAM

Colors indicate the probabilities corresponding to each state.

Quadrature amplitude modulations

- 64-QAM already gives performances close to that of the Gaussian.
- Increasing the constellation size enables to work at higher signal-to-noise ratio.

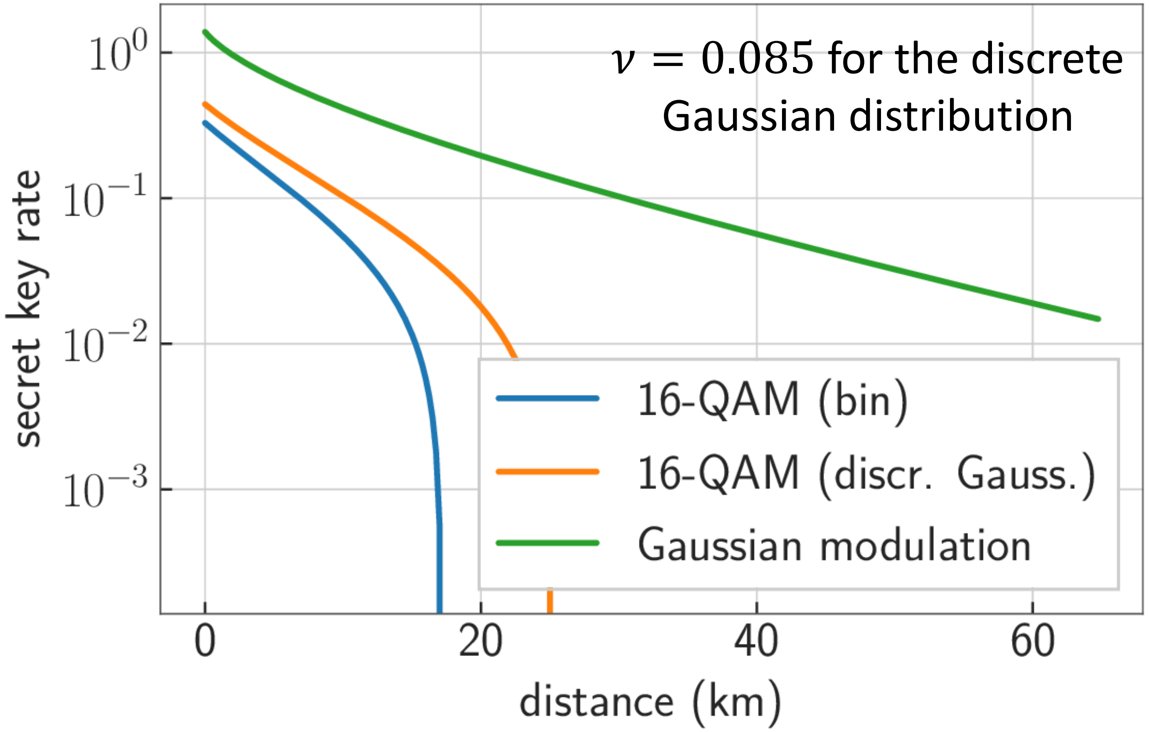


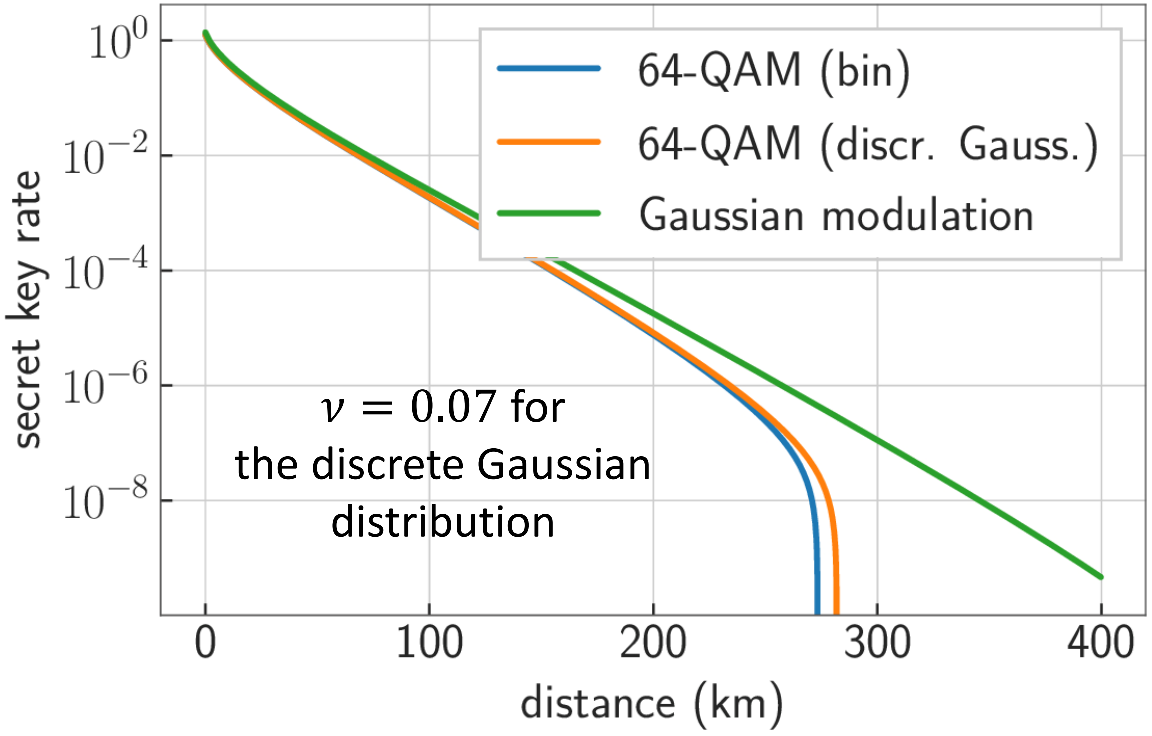
Secret key rate at 50 km as a function of the modulation variance VA, for various modulation schemes.
Parameters : ξ = 0.02 , β = 0.95.
For this choice of distance and excess noise, our bound gives a vanishing secret key rate for the QPSK scheme.

Comparison of QAM constellations

For the 16-QAM, the discrete Gaussian (with optimal parameter) outperforms the binomial distribution.

For a 64-QAM both distributions yield essentially the same performance.

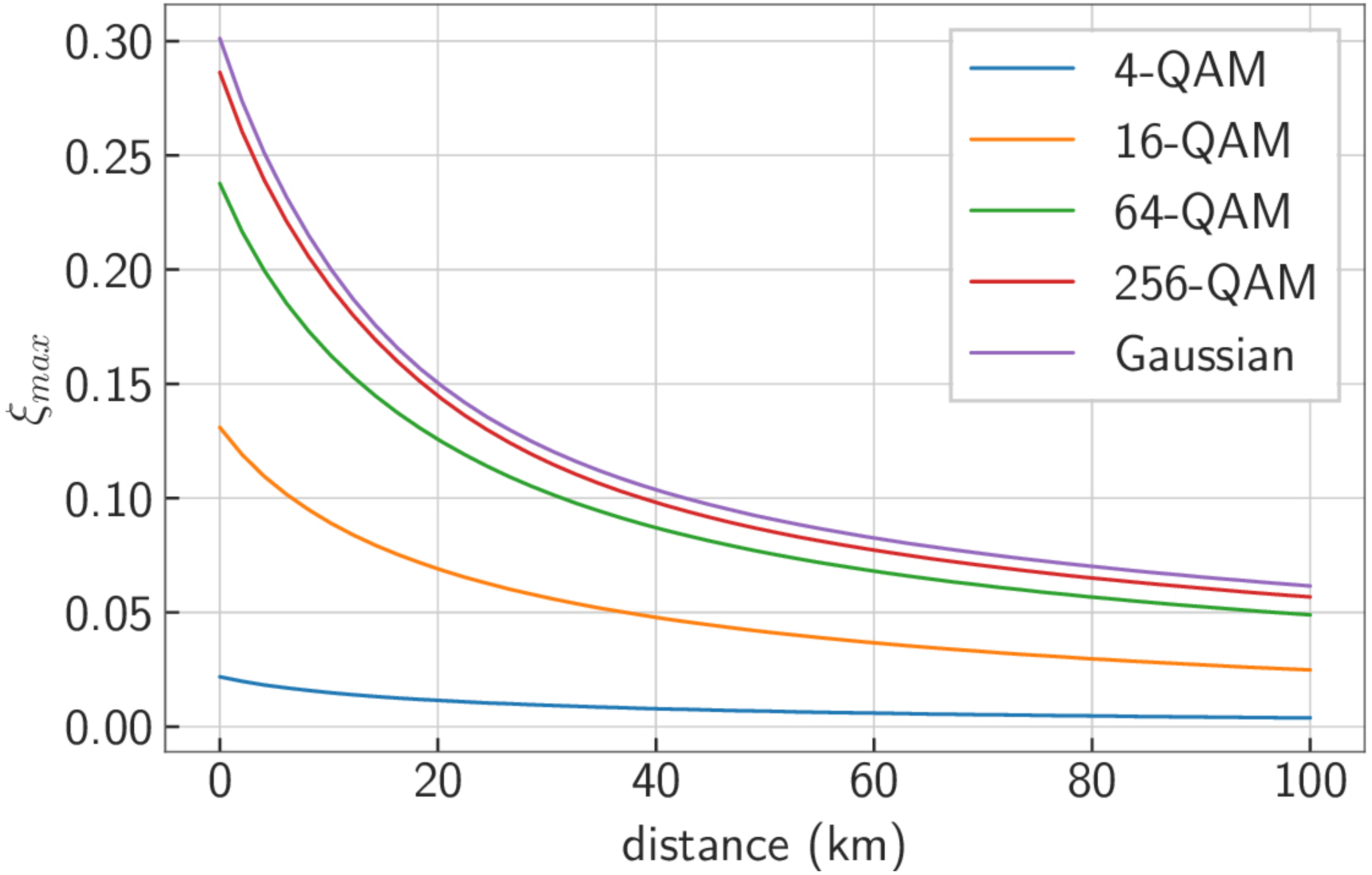




Bound on the asymptotic secret key rate as a function of the distance.
Fixed parameters parameters : $V_A = 5$, $\xi = 0.02$, $\beta = 0.95$

Maximum tolerable excess noise

- Maximum value of the excess noise ξ which gives a positive secret key rate?
  - 64-QAM : performance close to the Gaussian modulation
  - 256-QAM : almost indistinguishable from the Gaussian modulation.



Maximum value $\xi_{\max}$ of excess noise compatible with a positive key rate as a function of distance, for various QAM sizes (with binomial distribution). $\beta = 0.95$, V_A is optimized for each point.

Arbitrary modulations

- Similar method (with a different K operator)

- Applications :
  - protocols with e.g. thermal states
  - assess impact of imperfect state preparation on the security

- Bound has one more term → tightness : open question

Conclusion

Main result: Analytical bound on the asymptotic secret key rate of CV QKD protocols with an arbitrary modulation of coherent states (and more generally any arbitrary modulation)

Most impactful applications:

- Choice of modulation sizes (e.g. 64 states)
- Step towards full security proof

Other benefits:

Makes possible the

- Study of optimal constellations
- Study of the impact of imperfect state preparation on the security

Open questions:

- Tightness of bounds
- Extensions to other schemes
- Optimality of collective attacks among general attacks

Thank you !