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

Aurélie Denys, Peter J Brown, Anthony Leverrier

# Explicit asymptotic secret key rate of continuous-variable QKD with an arbitrary modulation

*Quantum* 5, 540 (2021)

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

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

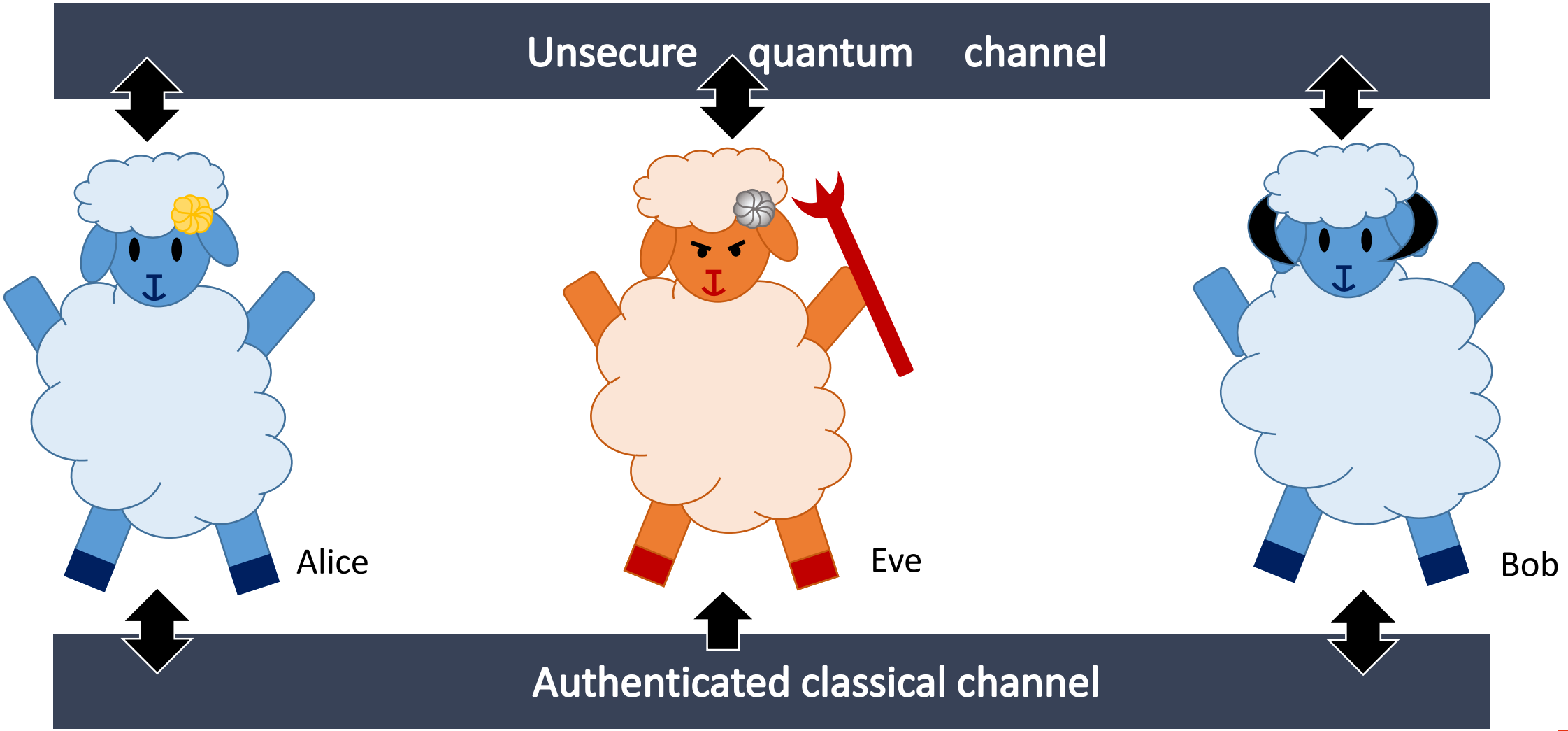
# Outline

1. Motivation, protocol and main result

2. Optimised constellations

# 1st part: Motivation, protocol and main result

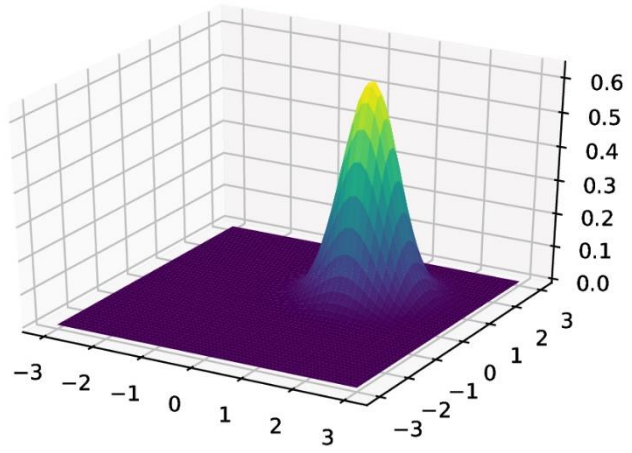
# Quantum key distribution (QKD)



# Discrete-variable (DV) QKD versus Continuous-variable (CV) QKD

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| | D | R | D | R | R | R | R | R | D |
| Bob | ↙ | ↕ | ↘ | ↔ | ↕ | ↕ | ↔ | ↔ | ↘ |
| | R | D | D | R | R | D | D | R | D |
| | 1 | | 1 | | 1 | 0 | 0 | 0 | |
| Public discussion | R | | D | | R | D | D | R | |
| | | | OK | | OK | | | OK | |
| | | | 1 | | 1 | | | 0 | |
| | | | | | 1 | | | | |
| | | | | | OK | | | | |
| | | | 1 | | | | | 0 | |

BB84




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

| DV | CV |
|---|---|
| Information encoded on discrete variables (e.g. polarisation of photons) | Information encoded on the quadratures of the quantified electromagnetic field |
| Problem : require the use of single photon detectors (expensive) | Easier to perform experimentally, cheaper |
| | But : harder proofs, less tolerant to loss |

# Continuous modulation versus discrete modulation

❖ Gaussian modulation : Alice sends $|\alpha\rangle$ with $\alpha \sim N(0, V_A)$ [1]
Well understood security [2-4]

❖ Infinite continuous constellation ≠ modulators have a finite precision and range → unrealistic

⇒ Discretely modulated CVQKD protocols

[1] Grosshans, Grangier 2002
[2] Garcia Patron, Cerf 2006
[3] Navascues, Grosshans, Acín 2006
[4] Leverrier 2017

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

Classical post-processing

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

# Main result : Asymptotic secret key rate of CV QKD protocols

- Security proof in the asymptotic regime, under the restriction to collective attacks

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

**Mutual information** between Alice and Bob

Upper bound on the **Holevo information** given by the extremality of Gaussian states [García Patrón, Cerf 2006, Navascués, Grosshans, Acín 2006]

  - Function of a covariance matrix $\sup_{N:A'\to B} \chi(Y;E) \leq \mathrm{f}(\Gamma)$ where $\Gamma = \begin{bmatrix} V\, I_2 & Z\, \hat{\sigma}_z \\ Z\, \hat{\sigma}_z & W\, I_2 \end{bmatrix}$
  - Z cannot be measured directly in the prepare & measure protocol ⇒ we write it as a Semidefinite Program (SDP).
  - Bound its solution: $\mathrm{Z} \geq \mathrm{Z}^* := 2c_1 - 2\left(\left(n_B - \frac{c_2^2}{\langle n \rangle}\right) w\right)^{1/2}$

Depends on the modulation

Estimated experimentally

Average photon number in the modulation

# 2nd part: Optimised constellations

# Methods to get practical results

- Typical Gaussian channel with transmittance $T$ and excess noise $\xi$

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

$$Z^* = 2\sqrt{T}\, tr\left(\tau^{1/2}\, a\, \tau^{1/2}\, a^{\dagger}\right) - \sqrt{2\, T\, \xi w(\tau)} \text{ where } \tau = \sum_k p_k |\alpha_k\rangle\langle\alpha_k|$$

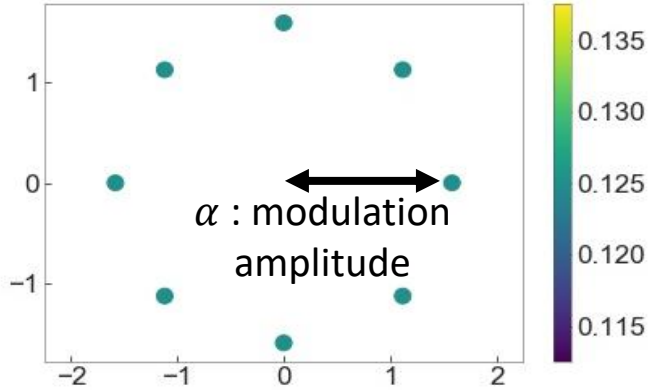
- Reconciliation efficiency $\boldsymbol{\beta}$

- Heterodyne detection

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

# Phase-shift keying (PSK) modulations

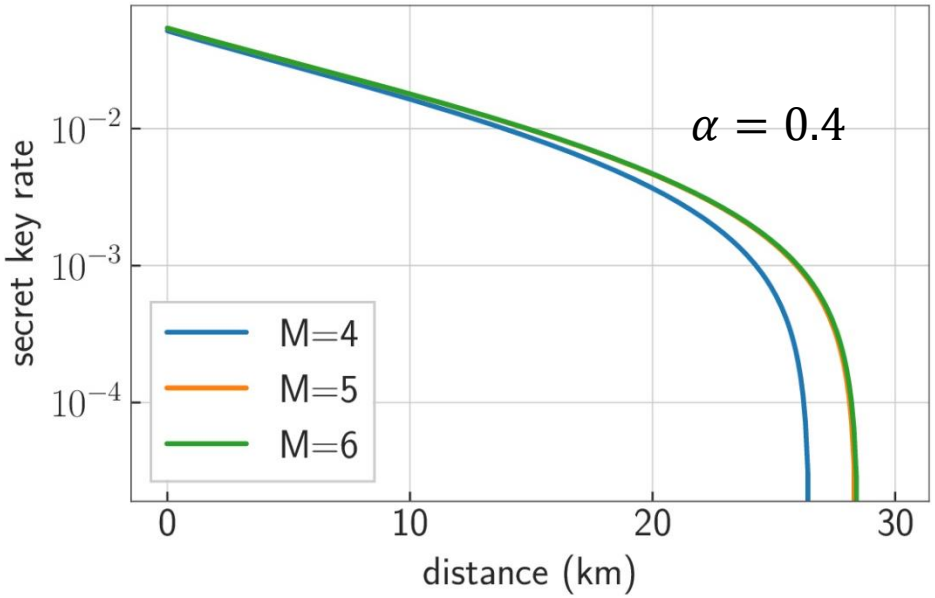
- Recover some numerical results for the quadrature PSK [Ghorai et al 2019]
- When the modulation amplitude is optimised, going beyond M=5 is essentially useless

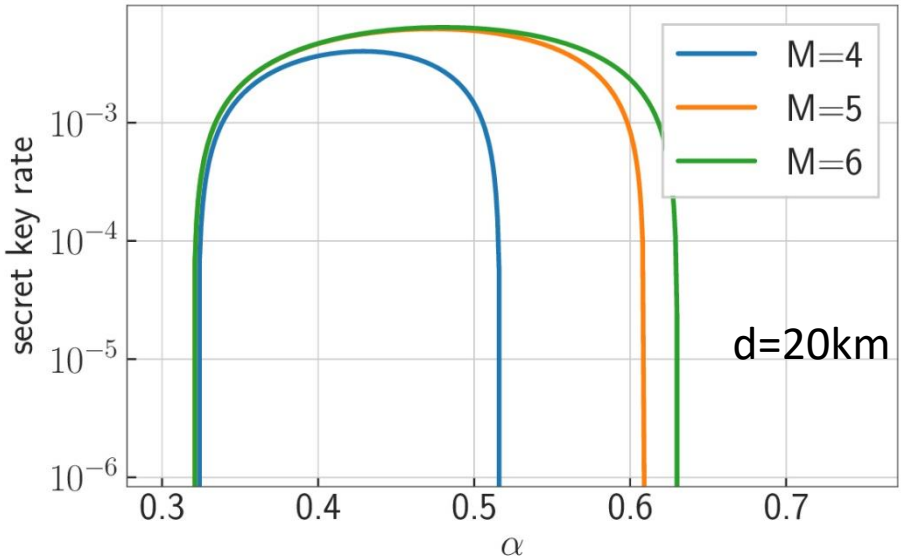


8-PSK constellation

- Increasing M allows for larger possible values of the modulation amplitude.

⇒ Approach of [Lin et al 2019; Upadhyaya et al 2021] gives better results for QPSK

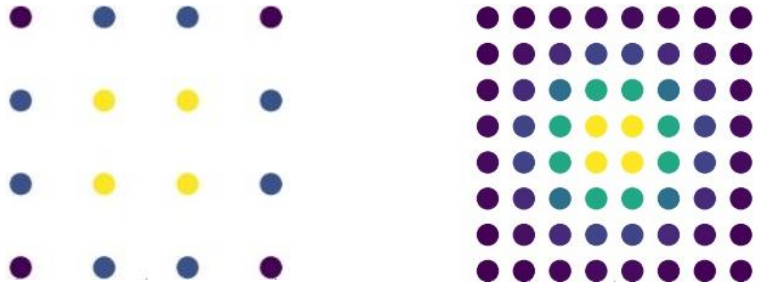


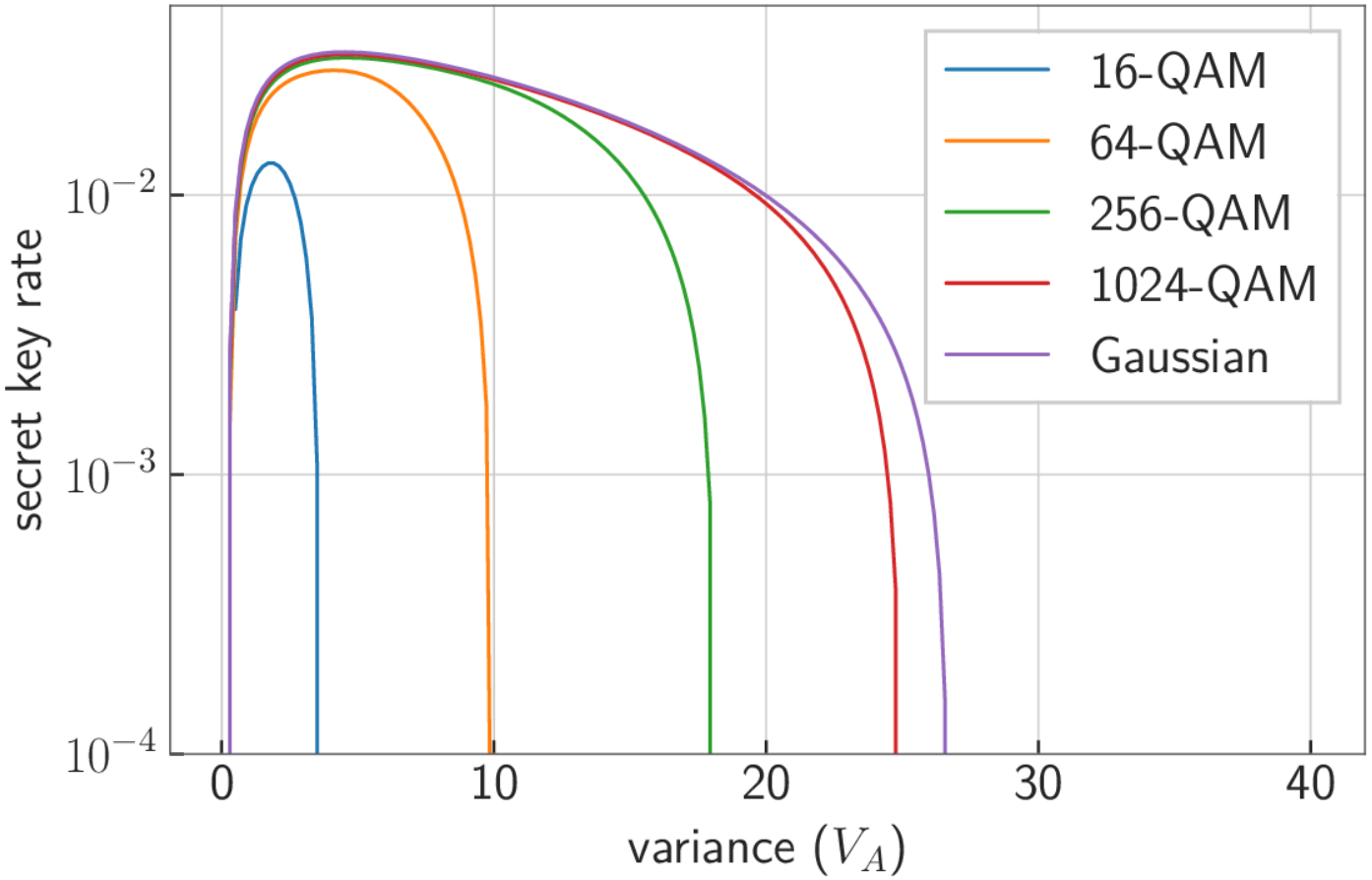

Asymptotic secret key rate for the M-PSK modulation schemes. ξ= 0.01 ; β=0.95.

# Quadrature amplitude modulations (QAM)

- Analytical bound ⇒ we can consider bigger constellations



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

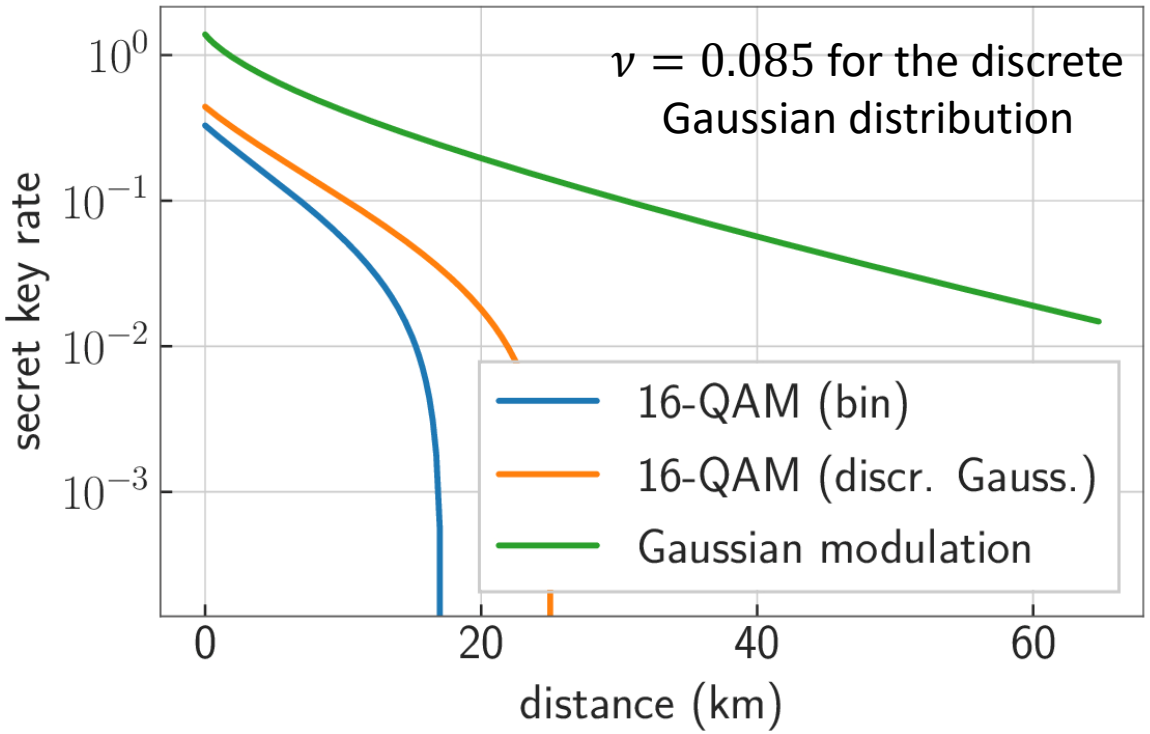


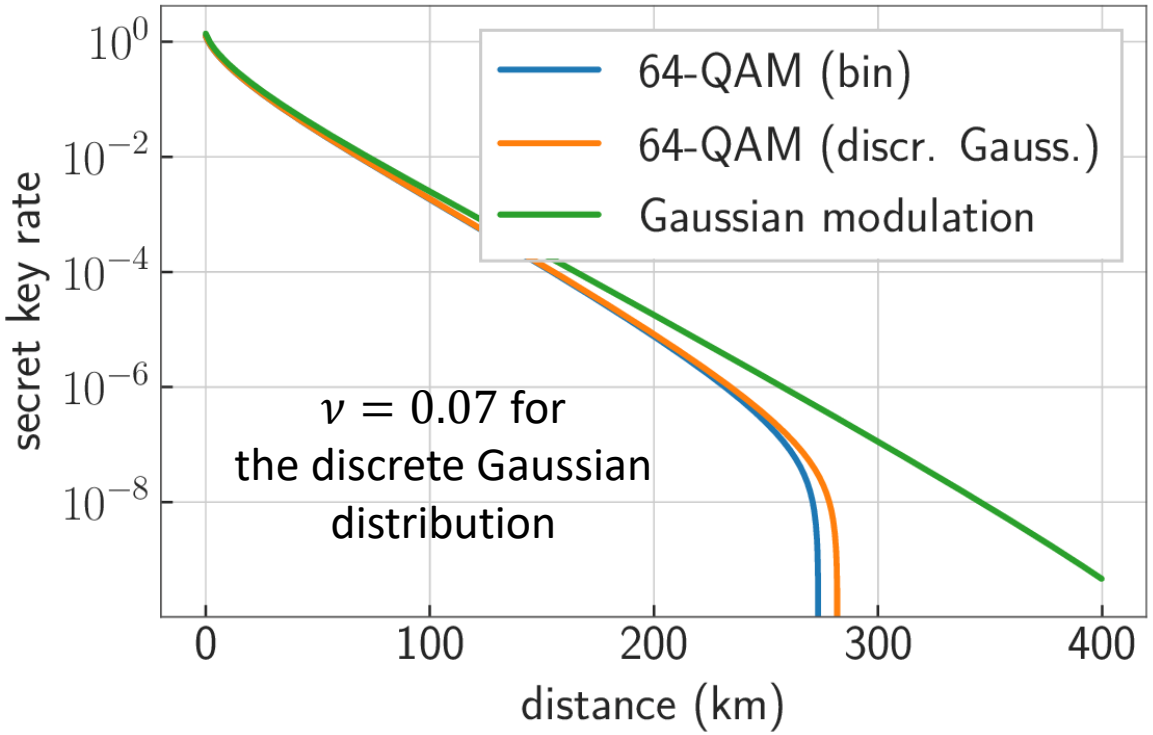

Secret key rate at 50 km as a function of the modulation variance $V_A$, for various modulation schemes.
Parameters : ξ = 0.02 , β = 0.95.

# 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.

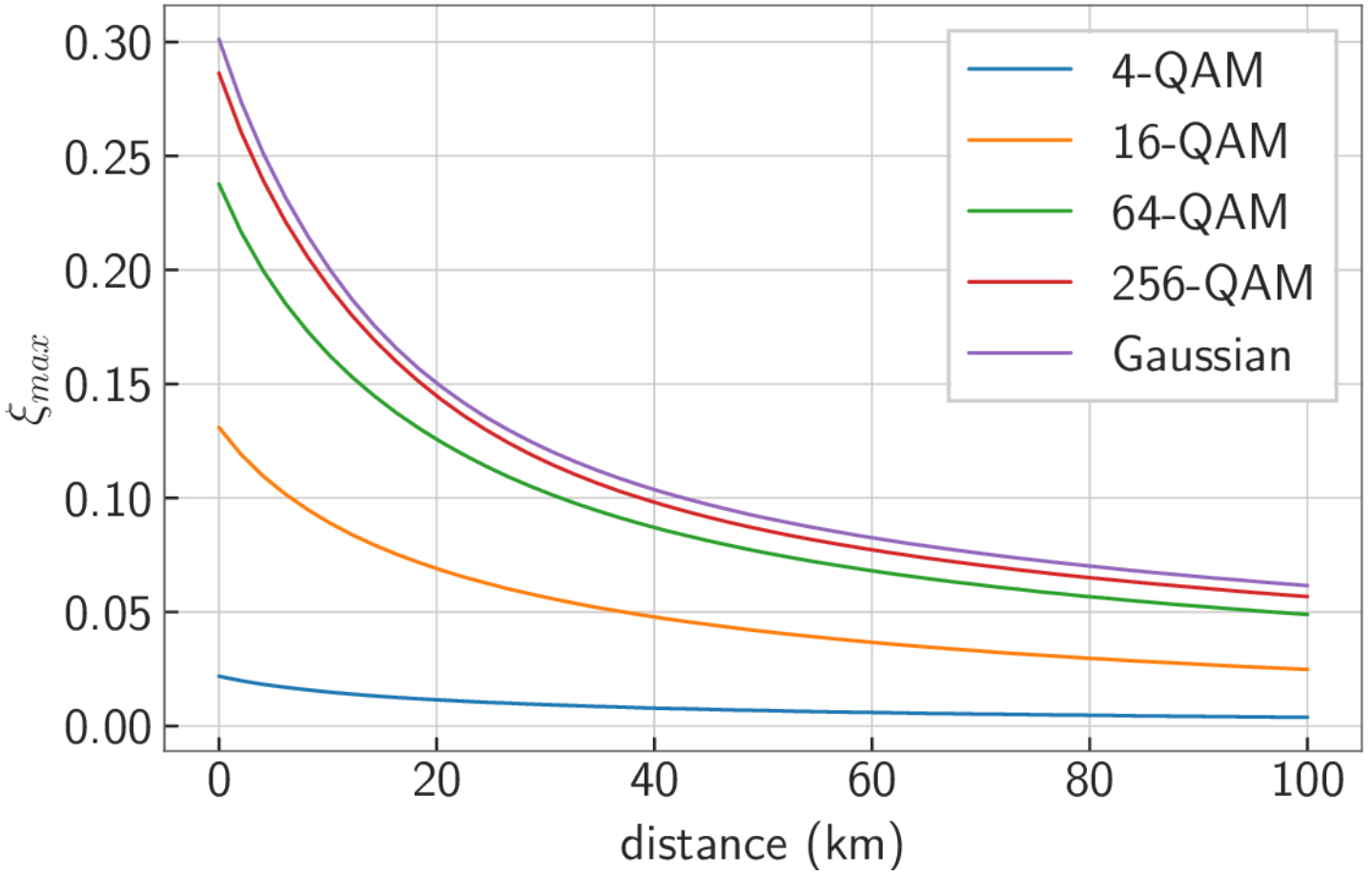



Bound on the asymptotic secret key rate as a function of the distance.
Fixed parameters parameters : $V_A$ = 5, ξ = 0.02, β = 0.95

# 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.

# 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)

Main applications:

- Comparison of modulations
- Choice of constellation sizes (e.g. 64 states)

Open questions:

- Tightness of bounds
- Extension of the result to get a full security proof

Thank you !