



HAL
open science

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

Aurélie Denys, Peter Brown, Anthony Leverrier

► **To cite this version:**

Aurélie Denys, Peter Brown, Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable QKD with an arbitrary modulation. IQFA - 12ème Colloque du DGR IQFA, Nov 2021, Lyon, France. hal-03537979

HAL Id: hal-03537979

<https://inria.hal.science/hal-03537979>

Submitted on 20 Jan 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

Quantum 5, 540 (2021)

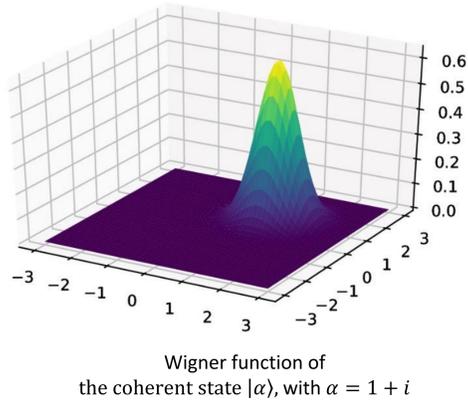
Aurélie Denys¹, Peter Brown², Anthony Leverrier¹

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

CONTINUOUS VARIABLE QKD PROTOCOL

Quantum part (repeated):

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 β_k .



+ Classical post-processing

SECURITY PROOF

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

❖ Main steps:

▪ Devetak-Winter bound : bound on the asymptotic secret key rate

$$k = I(X; Y) - \sup_{N: A' \rightarrow B} \chi(Y; E)$$

▪ Function of a covariance matrix :

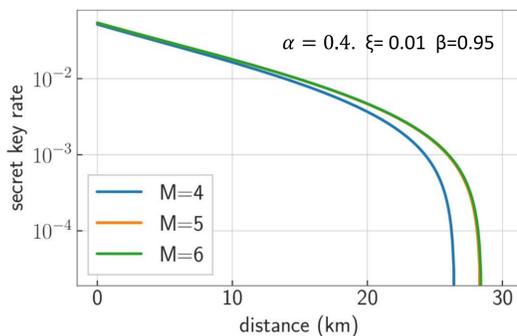
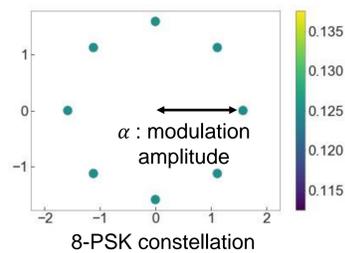
$$\sup_{N: A' \rightarrow B} \chi(Y; E) \leq f(\Gamma) \quad \text{where } \Gamma = \begin{bmatrix} V I_2 & Z \hat{\sigma}_z \\ Z \hat{\sigma}_z & W I_2 \end{bmatrix}$$

▪ Z cannot be measured directly in the prepare & measure protocol \Rightarrow we write it as a Semidefinite Program (SDP)

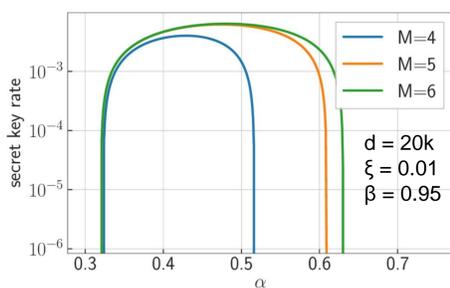
▪ Bound on its solution: $Z \geq Z^* := 2 c_1 - 2 \left(\left(n_B - \frac{c_2^2}{n} \right) w \right)^{1/2}$ (*)

OPTIMAL CONSTELLATIONS?

Phase-shift keying modulations

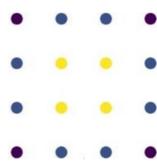


Asymptotic secret key rate as a function of the distance for the M-PSK modulation schemes.



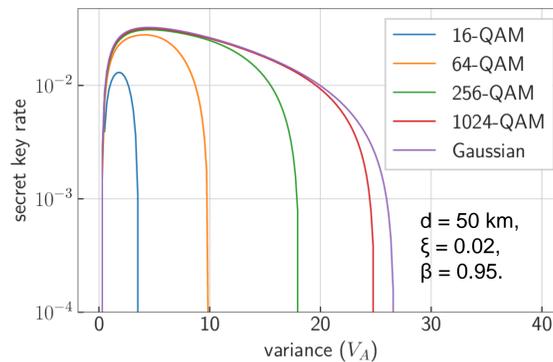
Asymptotic secret key rate as a function of the modulation amplitude for the M-PSK modulation schemes.

Quadrature amplitude modulations (QAM)

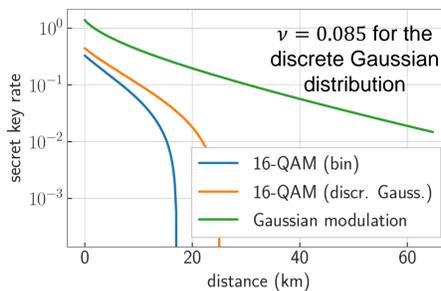


Before our work, only simple modulations (Gaussian modulation, quadrature phase-shift keying [1,2], etc.) could be analysed. The analytical formula (*) now makes possible the study of more relevant discrete modulations, such as the QAM.

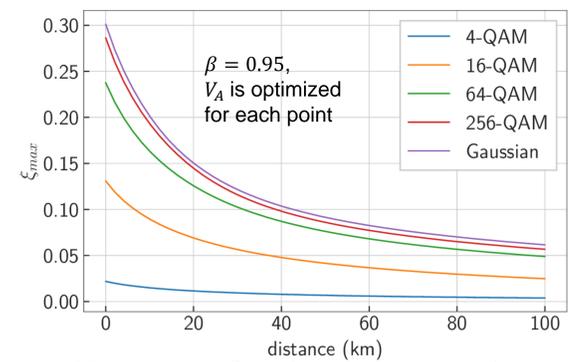
- [1] Ghorai et al., Phys. Rev. X, 9, 2, 021059, (2019)
[2] Lin et al., Phys. Rev. X, 9, 4, 041064, (2019)



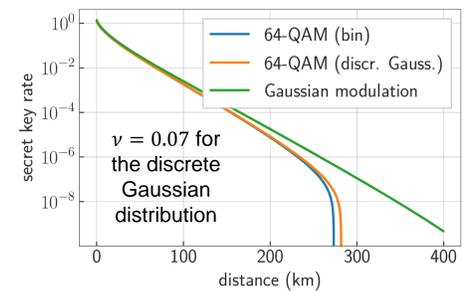
Secret key as a function of the modulation variance V_A , for various modulation schemes (with binomial distribution).



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



Maximum value ξ_{\max} of excess noise compatible with a positive key rate as a function of the distance, for various QAM sizes (with binomial distribution).



Parameters: d : distance between Alice and Bob, V_A : modulation variance, ξ : excess noise, β : reconciliation efficiency, ν : parameter for the discretised Gaussian distribution.

“ Relatively small constellation sizes, with say 64 states, are essentially sufficient to obtain a performance close to a true Gaussian modulation ”