



CHORUS

This is the accepted manuscript made available via CHORUS. The article has been published as:

Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels

Panagiotis Papanastasiou, Cosmo Lupo, Christian Weedbrook, and Stefano Pirandola

Phys. Rev. A **98**, 012340 — Published 31 July 2018

DOI: [10.1103/PhysRevA.98.012340](https://doi.org/10.1103/PhysRevA.98.012340)

Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels

Panagiotis Papanastasiou,¹ Cosmo Lupo,¹ Christian Weedbrook,² and Stefano Pirandola¹

¹*Computer Science and York Centre for Quantum Technologies,
University of York, York YO10 5GH, United Kingdom*

²*Xanadu, 372 Richmond St W, Toronto, M5V 2L7, Canada*

We consider discrete-alphabet encoding schemes for coherent-state quantum key distribution. The sender encodes the letters of a finite-size alphabet into coherent states whose amplitudes are symmetrically distributed on a circle centered in the origin of the phase space. We study the asymptotic performance of this phase-encoded coherent-state protocol in direct and reverse reconciliation assuming both loss and thermal noise in the communication channel. In particular, we show that using just four phase-shifted coherent states is sufficient for generating secret key rates of the order of 4×10^{-3} bits per channel use at about 15 dB loss in the presence of realistic excess noise.

I. INTRODUCTION

Quantum cryptography, or more accurately known as quantum key distribution (QKD), is based on the laws of quantum information [1–3] to provide in principle secure communication between two authorized parties [4, 5], traditionally called Alice and Bob. In particular these two parties exchange many signals using a quantum channel which prohibits an exact duplication of them [6]. This fact allows the remote parties to quantify and bound the amount of information that a potential eavesdropper (Eve) may intercept, so that they can still extract and share a secret key. Such key may then be used for data encryption by means of the one-time pad [7].

Since the first QKD protocol [8], many advances have been made including theoretical proofs, proof-of-principle experiments and in-field tests. Despite these efforts, the performance of any point-to-point QKD protocol cannot surpass the fundamental repeater-less PLOB bound established in Ref. [9] based on the relative entropy of entanglement of the channel (see Ref. [10] for a review, and Ref. [11] for an extension to repeaters and arbitrary networks). However, it is also true that continuous-variable (CV) QKD [12] has a key rate performance which is not far from this ultimate bound when we assume ideal reconciliation and detectors with high efficiency. Furthermore, another advantage of CV systems [13] relies on the use of cheap room temperature equipment, easily integrable in the current telecommunication infrastructure.

In recent years, we have witnessed the introduction of many protocols based on a CV encoding, e.g., exploiting a Gaussian modulation of the amplitude of Gaussian states. These protocols were designed for squeezed states [14, 15], coherent states [16, 17], thermal states [18–21], and also extended from one-way to two-way quantum communication [22–26] or reduced to one-dimensional encoding [27]. In addition, protocols such as in Ref. [28–30], assuming measurement-device-independence (MDI) [31, 32] as a counter-measure against detectors’ side-channel attacks, have extended the concept of CV-QKD to end-to-end network implementations [33]. For most of these protocols, not only

experiments were shown [28, 34–41], but also their security analysis has been gradually refined to incorporate finite-size effects [42–44] and composable aspects [45–47].

We know that Gaussian encoding may be subject to a reduced performance due to the reconciliation codes. This issue can be easily fixed by resorting to a discrete-alphabet encoding, e.g., coherent states with fixed energy but discrete shifting of their phase as in Ref. [48]. Nevertheless, the study of these protocols has been mainly restricted to the case of a pure-loss channel. In Ref. [49–51] a bound for the secret key rate has been calculated for two or four coherent states in a thermal loss channel. However, this was based on a Gaussian approximation [52] of the alphabet, which rapidly becomes loose when the energy of the states increases. Also note that Refs. [53, 54] studied binary and ternary modulation protocols in the presence of collective attacks.

In this work, we consider a multi-letter protocol where the letters are encoded in different phases of a coherent state with fixed energy, so as to form a symmetric constellation of coherent states equidistant from the origin of the phase space. For this phase-encoded protocol, we compute the secret key rate in direct and reverse reconciliation assuming a thermal-loss channel, i.e., the presence of an entangling cloner collective attack [12, 55]. This is the most realistic collective Gaussian attack [56] since it encapsulates the most essential aspects of a typical communication line. Although the Gaussian attacks have been proven to be optimal only in the case of a protocol with Gaussian encoding, notice that in the regime where the multi-letter protocol approximates the Gaussian-encoding protocol we can certainly assume the same optimal attack. In the other regimes, where the approximation is not exact, we expect, because of continuity arguments, that the optimal attack will be a perturbation to the Gaussian counterpart.

We perform an asymptotic security analysis based on infinitely-many uses of the channel [57]. While our analysis is for arbitrary N number of phases, we specify the results for the case of $N = 4$ which well approximates the continuous limit $N \rightarrow \infty$ when the energy of the states is sufficiently low.

II. PROTOCOL

Consider a discrete alphabet with N letters, randomly drawn by Alice. Each letter k is encoded into a coherent state with amplitude $a_k = ze^{i\phi_k}$, where z is a fixed radius in phase space (it is just the square root of the mean number of photons) and the phase is given by $\phi_k = \frac{2\pi}{N}k$. We call each realization $C(z, N)$ of this encoding scheme a “constellation”. As an example, a four-state constellation is shown in Fig. 1. The coherent state is prepared on mode A which is sent through a thermal-loss channel, whose output B is detected by Bob. In a practical realization of the protocol, this measurement is an heterodyne detection [58].

As already mentioned, the thermal-loss channel describes the effect of an entangling cloner collective attack [55]. In each use of the channel, Eve’s modes e and E are prepared in a two-mode squeezed vacuum (TMSV) state with variance $\omega \geq 1$, so that $\bar{n} = \frac{\omega-1}{2}$ is the mean number of photons in each thermal mode [12]. Mode E interacts with Alice’s mode A via a beam splitter with transmissivity τ , which characterizes the channel losses. Eve’s output mode E' and kept mode e are then stored in a quantum memory which is measured at the end of the protocol. Note that for $\bar{n} = 0$ Eve is injecting a vacuum mode, so that the channel becomes a pure-loss channel [9, 12]. In this case, the output modes E' and B are described by coherent states with attenuated amplitudes.

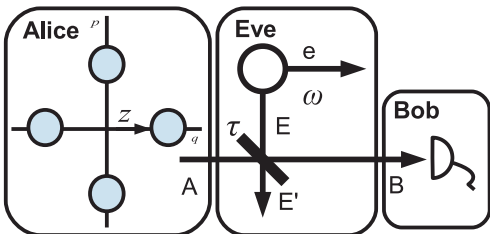


FIG. 1: Alice prepares mode A in one of the four coherent states of the constellation $C(z, 4)$ with radius z and sends it to Bob through a thermal-loss channel dilated into an entangling-cloner attack. In particular, the beam splitter has transmissivity τ , characterizing the channel loss, and the variance $\omega \geq 1$ of Eve’s TMSV state provides additional thermal noise to the channel. Eve’s output modes are stored in a quantum memory measured at the end of the protocol, i.e., after the entire quantum communication and Alice and Bob’s classical communication. At the output of the channel, Bob applies an heterodyne detection to mode B . An upper bound on the performance of the parties can be computed by assuming that also Bob has a quantum memory that he measures at the end of the entire communication process.

III. DIRECT RECONCILIATION

We start by presenting the analysis of the protocol in direct reconciliation [16], where Bob infers Alice’s input.

This analysis is first given for the pure-loss channel, considering an upper bound for the key rate (assuming a quantum memory for Bob) and then a realistic key rate (where Bob applies heterodyne detection). We then generalize the realistic key rate to a thermal-loss channel, presenting the specific results for $N = 4$ coherent states.

A. Pure loss channel

1. Upper bound for the secret key rate

In this section, we assume that Bob has a quantum memory so that he may apply an optimal joint detection. This gives an upper bound to the actual performance of the protocol. This analysis provides simple results that allow us to give an insight on the performance with respect to different constellation parameters z and N . In particular, we may show the conditions where $N = 4$ coherent states allow the parties to achieve essentially the same performance as $N \rightarrow \infty$ coherent states.

Because Alice is sending coherent states $|a_k\rangle$ with the same probability $p_k = 1/N$, the average state before the channel is given by

$$\rho_A = \frac{1}{N} \sum_{k=0}^{N-1} |a_k\rangle\langle a_k|. \quad (1)$$

It is clear that this state is parameterized by N and z . In Fig. 2, we have plotted the von Neumann entropy $S(\rho_A)$ of ρ_A for different N over the radius of the encoding scheme z . Recall that

$$S(\rho) := -\text{Tr}(\rho \log_2 \rho) = -\sum_j n_j \log_2 n_j, \quad (2)$$

where n_j are the eigenvalues of a generic state ρ (see Appendix A for more details on how to compute this entropy via a preliminary Gram-Schmidt procedure). The entropy $S(\rho_A)$ is larger as we increase the number of states in the circle. For any given N , the entropy saturates to a constant value after a certain value of the radius z . We also consider the limit of $N \rightarrow \infty$ (see Appendix B for the calculation of the corresponding average state).

After a pure-loss channel with transmissivity $\tau \in (0, 1)$, Bob’s average state will be

$$\rho_B = \frac{1}{N} \sum_{k=0}^{N-1} |\sqrt{\tau}a_k\rangle\langle\sqrt{\tau}a_k|. \quad (3)$$

Assuming that Bob accesses a quantum memory and may perform a collective optimal detection of all the output modes, his accessible information is bounded by the Holevo information [12]

$$\chi(B : \{a_k\}) = S(\rho_B) - \frac{1}{N} \sum_{k=0}^{N-1} S(|a_k\rangle\langle a_k|). \quad (4)$$

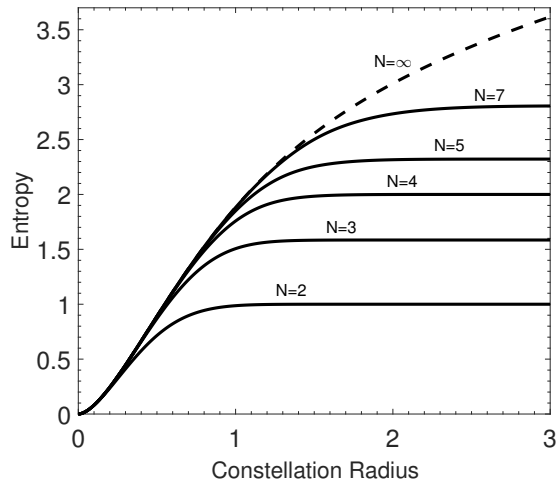


FIG. 2: The von Neumann entropy $S(\rho_A)$ of the Alice's average state ρ_A for different number N over the radius z of the constellation circle (solid lines). We plotted also the entropy of the continuous uniform distribution ($N \rightarrow \infty$) of the constellation states (dashed line).

In particular, since a coherent state is a pure state its von Neumann entropy is zero, which simplifies Eq. (4) into $\chi(B : \{a_k\}) = S(\rho_B)$. In order to calculate the von Neumann entropy of the mixture ρ_B , we express the N coherent states in terms of a Gram-Schmidt orthonormal basis (see details in Appendix A).

In the same fashion, we calculate the Holevo information of the eavesdropper, who can keep in a quantum memory the other output E' of the beam splitter. Then Eve's average state will be given by

$$\rho_{E'} = \frac{1}{N} \sum_{k=0}^{N-1} |\sqrt{1-\tau}a_k\rangle\langle\sqrt{1-\tau}a_k| \quad (5)$$

and her accessible information by

$$\chi(E' : \{a_k\}) = S(\rho_{E'}). \quad (6)$$

Therefore, we get the optimal secret key rate

$$R = \chi(B : \{a_k\}) - \chi(E' : \{a_k\}) = S(\rho_B) - S(\rho_{E'}). \quad (7)$$

In Fig. 3 we plotted this optimal rate for $N = 4$ as a function of the transmissivity τ and for different values of the radius z . We see that there is an optimal intermediate value for z , so that it cannot be too small (so that all the coherent states are too similar to the vacuum), neither too large (so that all the coherent states become almost-perfectly distinguishable). Then, we also show that the optimal performance for the $N = 4$ protocol is very close to that of the continuous-alphabet protocol $N = \infty$ for the relevant values of the radius z . In Fig. 4, we see that the rate is maximized by a specific value of z for any given value of the transmissivity.

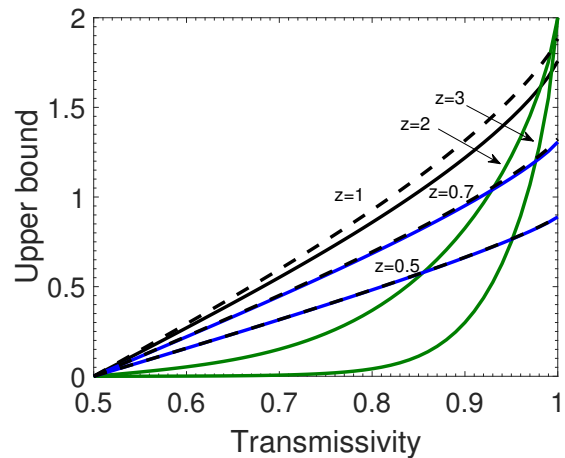


FIG. 3: The optimal secret key rate of Eq. (7) for $N=4$ is plotted over the transmissivity τ for different values of the radius z of the constellation. We can see that for values $z < 1$ the rate decreases as z is decreasing (blue lines) while for the $z > 1$ the rate decreases as z increases till it gets to zero for $z = 10^6$ (green lines). We also plotted the optimal secret key rate for the continuous uniform distribution of states (black dashed lines). We see that for $z < 0.6$ the two rates become almost identical. This corresponds to a saturation point for the 4-state protocol, so that it makes no difference to use four coherent states or an infinite number.

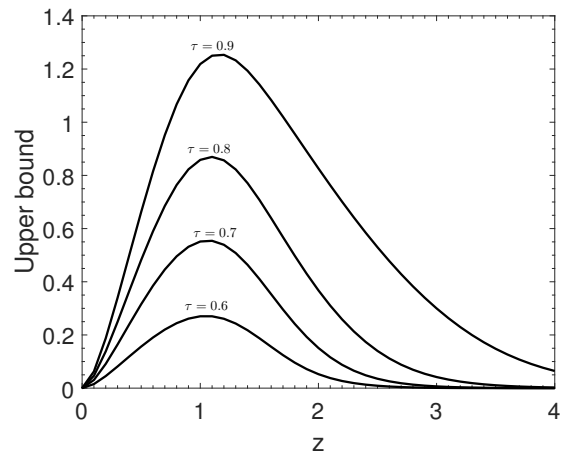


FIG. 4: We plotted the optimal rate (upper bound) as a function of the radius z with fixed transmissivities $\tau = 0.6, 0.7, 0.8, 0.9$. We can observe that there are certain values that maximize the rate for a given transmissivity.

2. Realistic secret key rate

Contrary to the previous discussion, the realistic situation is dictated by the limitations in the current technology. In this case, Bob does not use a quantum memory and an optimal collective measurement but individual heterodyne detections, with a continuous (complex) outcome b . Therefore, in order to calculate the secret key rate, we need to consider the corresponding mutual in-

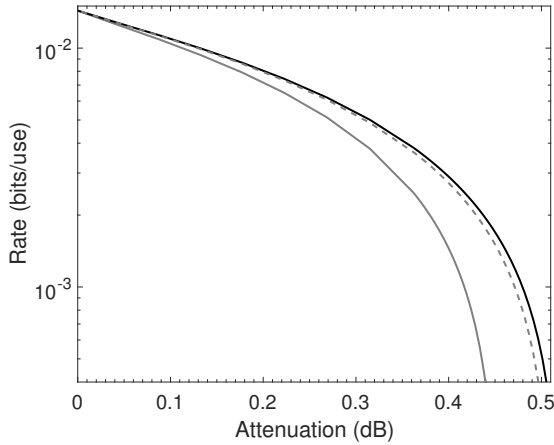


FIG. 5: Realistic secret-key rate (bits/use) over the attenuation (decibels) in direct reconciliation for $N = 4$ and $z = 0.1$. We plot the rate for a pure-loss channel (upper solid line) and a thermal-loss channel with mean photon number $\bar{n} = 0.01$ (middle dashed line) and $\bar{n} = 0.1$ (lower solid line).

formation between Alice and Bob. Let us define the variables $X_A = \{a_k, p_k\}$ with $p_k = 1/N$ and $X_B = \{b, p(b)\}$. Then, we consider

$$I(X_A : X_B) = H(X_A) - H(X_A|X_B), \quad (8)$$

where H is the Shannon entropy and $H(\dots|\dots)$ the conditional Shannon entropy. Recall that

$$H(X_A|X_B) = \int p(b)H(X_A|X_B = b)d^2b. \quad (9)$$

It is clear that $H(X_A) = \log_2 N$. In order to calculate the probability distribution $p(a_k|b)$, i.e., the probability that the state $|a_k\rangle$ was sent through the channel given that Bob measured the amplitude b . The probability that Bob measures b given that the coherent state $|\alpha_k\rangle$ was sent through the channel is given by $p(b|a_k) = \frac{1}{\pi}e^{-|b-\sqrt{\tau}a_k|^2}$. Therefore, we can apply Bayes' rule to obtain

$$p(a_k|b) = \frac{1}{N\pi p(b)}e^{-|b-\sqrt{\tau}a_k|^2}, \quad (10)$$

where $p(b) = \frac{1}{N} \sum_{k=0}^N p(b|a_k)$. With all these elements we can compute the asymptotic rate $R = I(X_A : X_B) - S(\rho_{E'})$ which is plotted in Fig. 5 for $N = 4$.

B. Thermal loss channel

We now consider the more general case of a thermal-loss channel, i.e., the presence of an entangling-cloner attack. Let us write Eve's TMSV state in the Fock basis [12]

$$\rho_{Ee}(\lambda) = (1 - \lambda^2) \sum_{n=0}^{\infty} (-\lambda)^{(k+l)} |k\rangle\langle l| \otimes |k\rangle\langle l|, \quad (11)$$

with $\lambda = \tanh\left[\frac{1}{2}\text{arcosh}(2\bar{n} + 1)\right]$, where \bar{n} is the mean number of thermal photons. Let us apply the beam splitter operation to Alice's mode A and Eve's mode E , with annihilation operators \hat{a}_A and \hat{a}_E , respectively. This is given by [12]

$$U(\theta) = \exp\left[\theta\left(\hat{a}_A^\dagger\hat{a}_E - \hat{a}_A\hat{a}_E^\dagger\right)\right], \quad (12)$$

where $\theta = \arcsin(\sqrt{\tau})$. Therefore, the global output state of Bob (mode B) and Eve (modes e and E'), is given by

$$\rho_{BE'e}(\theta, a_k, \lambda) = U(\theta)\Pi_A(a_k)\rho_{Ee}(\lambda)U^\dagger(\theta), \quad (13)$$

where $\Pi_A(a_k) := |a_k\rangle\langle a_k|$. By tracing out B , we obtain Eve's state

$$\rho_{Eve|k} := \rho_{E'e}(\theta, a_k, \lambda) = \text{Tr}_B[\rho_{BE'e}(\theta, a_k, \lambda)]. \quad (14)$$

The average state of Eve is given by the convex sum

$$\rho_{Eve}(\theta, z, \lambda) = \frac{1}{N} \sum_{k=0}^N \rho_{Eve|k}. \quad (15)$$

Therefore, the Holevo information is given by

$$\chi(\text{Eve} : X_A) = S(\rho_{Eve}) - \frac{1}{N} \sum_{k=0}^N S(\rho_{Eve|k}). \quad (16)$$

The entropy of the state $\rho_{Eve|k}$ does not depend on k , i.e., the phase of the amplitude of the coherent state that Alice has sent. Thus Eq. (16) can be simplified to

$$\chi(\text{Eve} : X_A) = S(\rho_{Eve}) - S(\rho_{Eve|k}), \quad (17)$$

for any k . In order to calculate the mutual information, we follow the reasoning of Section III A 2 with the difference that Bob's probability distribution is given by

$$p(b|a_k)(\bar{n}) = \text{Tr}[\Pi(b)\rho(\sqrt{\tau}a_k, (1-\tau)\bar{n})\Pi^\dagger(b)], \quad (18)$$

where $\Pi(b) := |b\rangle\langle b|$ and $\rho(\sqrt{\tau}a_k, (1-\tau)\bar{n})$ is a displaced thermal state with amplitude $\sqrt{\tau}a_k$ and mean photon number $(1-\tau)\bar{n}$. We find (see Appendix C)

$$p(b|a_k)(\bar{n}) = \frac{\exp\left[\frac{|b-\sqrt{\tau}a_k|^2}{1+(1-\tau)\bar{n}}\right]}{\pi(1+(1-\tau)\bar{n})}. \quad (19)$$

Using the Bayes' rule we can derive $p(a_k|b)(\bar{n})$ and compute Alice and Bob's mutual information via the formula in Eq. (8). Altogether, we then compute (numerically) the direct reconciliation secret-key rate

$$R(\bar{n}) = I(X_A : X_B)(\bar{n}) - \chi(\text{Eve} : X_A). \quad (20)$$

In Fig. 5, we plot this secret key rate over the attenuation for a protocol with $N = 4$ and $z = 0.1$. In particular, we see that the performance obtained in the presence of thermal noise $\bar{n} = 0.01$ is not so far from the performance

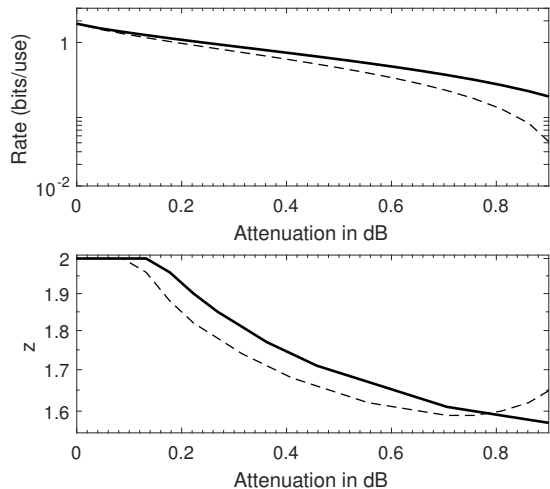


FIG. 6: Protocol for $N = 4$ in direct reconciliation. Upper panel: Key rate is optimized over $z \in (0, 2)$ and plotted versus attenuation. We assume a pure loss channel (solid line) and a thermal loss channel with $\bar{n} = 0.1$ (dashed line). Lower panel: We plot the optimal value of z versus attenuation, for the pure loss case (solid line) and the thermal loss case (dashed line).

achievable in the presence of a pure-loss channel. In other words, the four-state protocol is sufficiently robust to the presence of excess noise. In Fig. 6, we optimize the rate with respect to the radius z for both pure loss and thermal loss channels. In the lower panel, we can see the difference between the two optimal radii corresponding to the two cases. In Fig. 7, we also see incremental changes in the security threshold of the protocol by increasing the number of encoding states, e.g. from $N = 4$ to 10, assuming a thermal loss channel. In order to estimate the excess noise ϵ we assume a variation of the original protocol [59]. As expected, we also have that direct reconciliation restricts the use of the protocol to low loss. The case is different for reverse reconciliation that we study below.

IV. REVERSE RECONCILIATION

As before, for the sake of simplicity, we start by considering the case of a pure-loss channel in reverse reconciliation [34] and then we extend the results to the presence of thermal noise. We just need to re-compute Eve's Holevo bound (now with respect to Bob's outcomes). More specifically, we need to re-compute Eve's conditional entropy.

Eve's state conditioned to Bob's outcome b is

$$\rho_{E'|b} = \sum_{k=0}^{N-1} p(a_k|b) |\sqrt{1-\tau}a_k\rangle \langle \sqrt{1-\tau}a_k|, \quad (21)$$

where $p(a_k|b)$ is given in Eq. (10). We can then compute $S(\rho_{E'|b})$ which is now depending on b . Using this

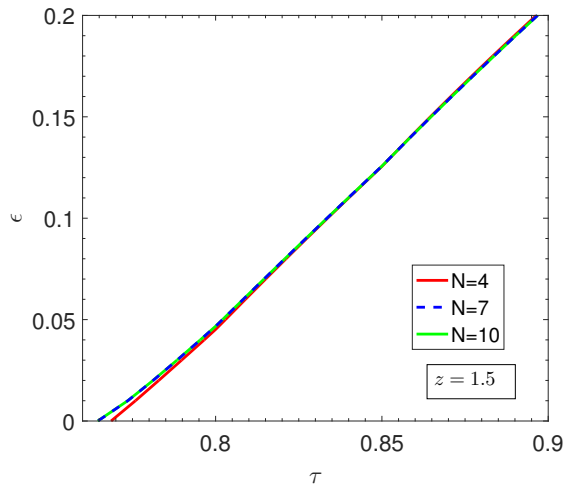


FIG. 7: We plot the security thresholds in direct reconciliation, i.e., maximum tolerable excess noise ϵ versus transmissivity τ for $N = 4$ (red line), $N = 7$ (blue dashed line) and $N = 10$ (green line).

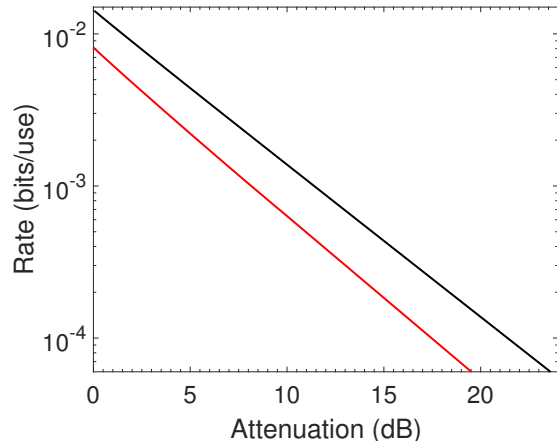


FIG. 8: Realistic secret key rate (bits/use) over the attenuation (decibels) in reverse reconciliation for $N = 4$ and $z = 0.1$. We have plotted the rate for a pure-loss channel (upper black line) and a thermal-loss channel with excess noise $\epsilon = 0.001$ (lower red line). Both these rates coincide with the corresponding rates achievable by a Gaussian protocol modulating coherent states with variance $V_M = 0.02$.

quantity, we may write the secret-key rate

$$R = I(X_A : X_B) - S(\rho_{E'}) + \int d^2b p(b) S(\rho_{E'|b}). \quad (22)$$

This rate is plotted in Fig. 8 for the four-state protocol $N = 4$ and radius $z = 0.1$.

Let us now consider the presence of thermal noise. In this case, Eve's conditional state is given by

$$\rho_{E'e|b} = \sum_{k=0}^{N-1} p(a_k|b) (\bar{n}) \rho_{Eve|k}, \quad (23)$$

where $\rho_{E'Ve|k}$ is given in Eq. (14) and $p(a_k|b)$ comes from Eq. (19). Therefore, we may derive $S(\rho_{E'Ve|b})$ and calculate the secret-key rate

$$R(\bar{n}) = I(X_A : X_B)(\bar{n}) - S(\rho_{E'Ve}) + \int d^2b p(b)(\bar{n})\rho_{E'Ve|b}, \quad (24)$$

where $p(b)(\bar{n}) := \frac{1}{N} \sum_{k=0}^{N-1} p(b|a_k)(\bar{n})$. Numerically, we compute this rate by truncating the Hilbert space to a suitable number of photons, which is of the order of $\simeq 10 - 15$ photons for the specific regime of parameters considered.

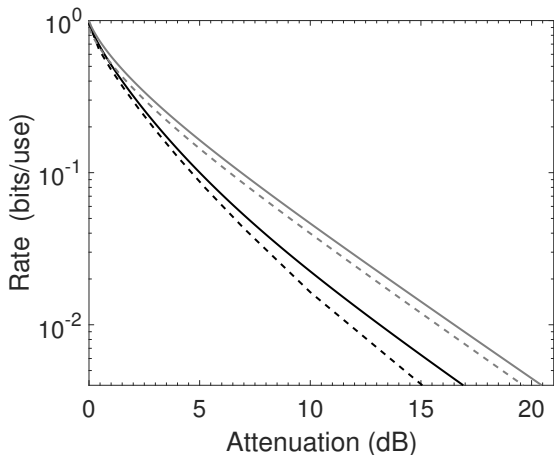


FIG. 9: Realistic secret key rate (bits/use) over the attenuation (decibels) in reverse reconciliation over the attenuation (decibels) for $N = 4$ and $z = 1$. We have plotted the rate for a pure-loss channel (lower solid line) and a thermal-loss channel with excess noise $\epsilon = 0.01$ (lower dashed line). The corresponding secret key rate for the protocol with Gaussian modulation ($V_M = 2$) has also been plotted for the case of pure-loss channel (upper solid line) and thermal-loss channel with excess noise $\epsilon = 0.01$ (upper dashed line). We see that, for this regime of energies, the rate of the four-state protocol does not coincide with the rate of the Gaussian protocol.

In Fig. 8, we plot the reverse reconciliation secret key rate over the attenuation for the four-state protocol $N = 4$ with radius $z = 0.1$ and excess noise $\epsilon = 0.001$ [59]. We can see that the protocol is sufficiently robust to excess noise, achieving a rate of 6×10^{-4} bits per channel use for attenuation values of about 20 dB. In this regime of energy, the performance of the protocol coincides with that of a Gaussian protocol modulating coherent state with modulation variance $V_M = 2z^2$ (and performing heterodyne detection on the channel output). On the contrary, for larger energies, e.g., for a constellation radius $z = 1$, the rate of the four-state protocol does not coincide with its Gaussian counterpart, as also illustrated in Fig. 9. Here the four-state protocol can achieve a rate of the order of 4×10^{-3} bits per channel use for attenuation values of about 15 dB and excess noise $\epsilon = 0.01$.

V. CONCLUSION

In this work, we have investigated finite-alphabet coherent-state QKD protocols, where the encoding is performed by randomly choosing the phase of the coherent states so that they are iso-energetic and symmetrically distributed around the origin of the phase space. Considering an optimal scenario where Bob may access a quantum memory and the channel is pure-loss, we have analyzed the conditions under which the use of four states can approximate a continuous alphabet. Our analysis is asymptotic, i.e., we assume the limit of infinite signal states exchanged by the remote parties, so that it does not account for finite-size effects and composable aspects. Nevertheless, this is the first study of these types of protocols in the presence of realistic thermal-loss conditions, without assuming Gaussian approximations. In particular, we assume an entangling cloner attack, which, as the dilation of the thermal loss channel, is describing a typical communication line. In reverse reconciliation, we find that the four-state phase-encoded protocol is sufficiently robust to loss and noise, so that it may be used to extract secret keys at metropolitan mid-range distances (e.g. around 75 km).

VI. ACKNOWLEDGEMENTS

C.W. would like to acknowledge the Office of Naval Research program Communications and Networking with Quantum Operationally-Secure Technology for Maritime Deployment (CONQUEST), awarded to Raytheon BBN Technologies under prime contract number N00014-16-C-2069. P. P. acknowledges support from the EP-SRC via the ‘UK Quantum Communications Hub’ (EP/M013472/1) and would like to thank Thomas Cope for advices on the use of the computer cluster of the University of York (YARCC). C. L. acknowledges support from Innovation Fund Denmark (Qubiz project).

Appendix A: Orthonormal basis for N coherent states

Suppose that we have N coherent states described by amplitudes a_k for $k = 0, 1 \dots N-1$. Since these states are non-orthogonal we can have a matrix \mathbf{V} that describes their overlaps, which are given by

$$V_{ij} = \langle a_i | a_j \rangle = \exp \left[-\frac{1}{2} (|a_i|^2 + |a_j|^2 - 2a_i^* a_j) \right]. \quad (A1)$$

For a constellation of states as described before and after the attenuation due to the propagation through a pure-loss channel, the overlaps for Bob are given by

$$V_{ij}^B = \langle \sqrt{\tau} a_i | \sqrt{\tau} a_j \rangle = \exp \left[\tau z^2 \left(e^{i \frac{2\pi}{N}(j-i)} - 1 \right) \right], \quad (A2)$$

while for Eve we may write

$$\begin{aligned} V_{ij}^E &= \langle \sqrt{1-\tau}a_i | \sqrt{1-\tau}a_j \rangle = \\ &= \exp \left[(1-\tau)z^2 \left(e^{i\frac{2\pi}{N}(j-i)} - 1 \right) \right]. \end{aligned} \quad (\text{A3})$$

Then, according to the Gram-Schmidt procedure, we can derive an orthonormal basis $\{|i\rangle\} = \{|0\rangle, |1\rangle, \dots, |N-1\rangle\}$ for the subspace spanned by these N coherent states. As a result, each state will be expressed as a superposition of this basis vectors as

$$|a_k\rangle = \sum_{i=0}^k M_{ki} |i\rangle \quad (\text{A4})$$

where the M_{ki} can be computed by the algorithm

$$\begin{aligned} M_{k0} &= V_{0k}, \\ M_{ki} &= \frac{1}{M_{ii}} \left(V_{ik} - \sum_{j=0}^{i-1} M_{ij}^* M_{kj} \right) \text{ if } 1 \leq i < k, \\ M_{ki} &= 0 \text{ otherwise,} \\ M_{kk} &= \sqrt{1 - \sum_{i=0}^{k-1} |M_{ki}|^2} \text{ for } k > 0. \end{aligned}$$

Then the density matrix $\rho(a_k) = |a_k\rangle\langle a_k|$ is given by

$$\rho(a_k) = \sum_{i,j=0}^k M_{k,i} M_{k,j}^* |i\rangle\langle j|, \quad (\text{A5})$$

and the average state takes the form

$$\rho = \frac{1}{N} \sum_{k=0}^{N-1} \rho(a_k) = \frac{1}{N} \sum_{k=0}^{N-1} \sum_{i,j=0}^k M_{k,i} M_{k,j}^* |i\rangle\langle j|. \quad (\text{A6})$$

Diagonalizing the previous state, we then compute its von Neumann entropy.

Appendix B: Asymptotic state for a continuous alphabet

Let us express a coherent state in the Fock basis, i.e.,

$$\Pi(a) := |a\rangle\langle a| = e^{-|a|^2} \sum_{n,m=0}^{\infty} \frac{a^n (a^\dagger)^m}{\sqrt{n!}\sqrt{m!}} |n\rangle\langle m| \quad (\text{B1})$$

In order to be able to do numerical calculations, we have to truncate the Fock space and a very good approximation is given by $n \sim 2|\alpha|^2$. As a result, in this truncated Fock basis, the state will be

$$\Pi^{\text{tranc}}(a) \simeq e^{-|a|^2} \sum_{n,m=0}^{2\lfloor |a|^2 \rfloor} \frac{a^n (a^\dagger)^m}{\sqrt{n!}\sqrt{m!}} |n\rangle\langle m|. \quad (\text{B2})$$

For N coherent states in a constellation with radius z , the average state can be written as

$$\rho = \frac{e^{-z^2}}{N} \sum_{n,m=0}^{2\lfloor z^2 \rfloor} \frac{z^{(n+m)} \sum_{j=0}^{N-1} e^{i\frac{2\pi}{N}(n-m)j}}{\sqrt{n!}\sqrt{m!}} |n\rangle\langle m|, \quad (\text{B3})$$

where the non zero terms are the terms with $m-n=0$ and $n=m$. For a continuous distribution $p(a_\phi) = \frac{1}{2\pi}$ of phase-encoded coherent states $|a_\phi\rangle$ with fixed radius $z = |a|$ and $\phi = \arg(a_\phi)$, Eq. (B3) becomes

$$\begin{aligned} \rho &= \frac{e^{-z^2}}{2\pi} \sum_{n,m=0}^{2\lfloor z^2 \rfloor} \frac{z^{(n+m)} \int_0^{2\pi} e^{i\phi(n-m)} d\phi}{\sqrt{n!}\sqrt{m!}} |n\rangle\langle m| = \\ &= e^{-z^2} \sum_{n=0}^{2\lfloor z^2 \rfloor} \frac{z^{2n}}{n!} |n\rangle\langle n|. \end{aligned} \quad (\text{B4})$$

Appendix C: Displaced thermal state

A thermal state with mean number of photons \bar{n} may be expressed as a convex sum of coherent states $|a\rangle$ according to the P-Glauber representation as

$$\rho(\bar{n}) = \int p(a, \bar{n}) |a\rangle\langle a| d^2 a, \quad p(a, \bar{n}) = \frac{1}{\bar{n}\pi} e^{-|a|^2/\bar{n}}. \quad (\text{C1})$$

Applying the displacement operator $D(d)$, which displaces a coherent state $|a\rangle$ with amplitude a into a coherent state $|a+d\rangle$ with amplitude $a+d$, we obtain a displaced thermal state

$$\begin{aligned} \rho(d, \bar{n}) &= D(d)\rho(\bar{n})D^\dagger(d) = \\ &= \int p(a, \bar{n}) D(d)|a\rangle\langle a| D^\dagger(d) d^2 a = \\ &= \int p(a, \bar{n}) |a+d\rangle\langle a+d| d^2 a = \\ &= \int p(c-d, \bar{n}) |c\rangle\langle c| d^2 c \end{aligned} \quad (\text{C2})$$

with $p(c-d, \bar{n}) = \frac{1}{\bar{n}\pi} e^{-|c-d|^2/\bar{n}}$. According to equation Eq. (B1), we can have a representation of this state in Fock basis, so that

$$\rho(d, \bar{n}) = \int \sum_{n,m=0}^{\infty} p(a-d, \bar{n}) e^{-|a|^2} \frac{a^n (a^*)^m}{\sqrt{n!}\sqrt{m!}} |n\rangle\langle m| d^2 a \quad (\text{C3})$$

The state after projecting to a coherent state $|b\rangle$ (heterodyne measurement), i.e., $\Pi(b)\rho(d, \bar{n})\Pi^\dagger(b)$, will be calculated as

$$\begin{aligned} &\int d^2 a \sum_{n,m,k,l,i,j=0}^{\infty} p(a-d, \bar{n}) e^{-|a|^2} \frac{\alpha^n (\alpha^*)^m}{\sqrt{n!}\sqrt{m!}} e^{-|b|^2} \frac{b^k (b^*)^l}{\sqrt{k!}\sqrt{l!}} \times \\ &\times e^{-|b|^2} \frac{b^i (b^*)^j}{\sqrt{i!}\sqrt{j!}} |k\rangle\langle l| |n\rangle\langle m| |i\rangle\langle j| = \end{aligned} \quad (\text{C4})$$

$$\begin{aligned} &\int d^2 a p(a-d, \bar{n}) e^{-|a|^2} e^{-2|b|^2} \sum_{n,m=0}^{\infty} \frac{(ab^*)^n (ba^*)^m}{\sqrt{n!}\sqrt{m!}} \times \\ &\times \sum_{k,j=0}^{\infty} \frac{b^k (b^*)^j}{\sqrt{k!}\sqrt{j!}} |k\rangle\langle j|, \end{aligned} \quad (\text{C5})$$

and, applying the trace operation, we obtain the probability distribution

$$\begin{aligned}
 p(b|d)(\bar{n}) &= \int d^2a \frac{1}{\bar{n}\pi} e^{-|a-d|^2/\bar{n}} e^{-(|a|^2+|b|^2-b^*a-ba^*)} = \\
 &= \frac{1}{\bar{n}\pi} \int e^{-|a-d|^2/\bar{n}} e^{-|a-b|^2} d^2a = \\
 &= \frac{1}{(\bar{n}+1)\pi} \exp(-|b-d|^2/(\bar{n}+1)). \quad (\text{C6})
 \end{aligned}$$

Let us write this probability distribution for the thermal output state of a thermal-loss channel with transmissivity τ and mean thermal photon number \bar{n} when applied to an input coherent state $|a_k\rangle$ ($d := \sqrt{\tau}a_k$). We find Eq. (19).

-
- [1] J. Watrous, *The theory of quantum information* (Cambridge University Press, Cambridge, 2018). Also available from <https://cs.uwaterloo.ca/~watrous/TQI/TQI.pdf>
- [2] M. Hayashi, *Quantum Information Theory: Mathematical Foundation* (Springer-Verlag Berlin Heidelberg, 2017)
- [3] M. A. Nielsen, and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000)..
- [4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2008)
- [6] W. K. Wootters and W. H. Zurek, *Nature* **299**, 802-803 (1982).
- [7] B. Schneier, *Applied Cryptography* (John Wiley & Sons, New York, 1996).
- [8] C. H. Bennett and G. Brassard, *Theoretical Computer Science* **560**, 7-11 (2014).
- [9] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Nat. Commun.* **8**, 15043(2017). See also arXiv:1510.08863 and arXiv:1512.04945 (2015).
- [10] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi, *Theory of channel simulation and bounds for private communication*, arXiv:1711.09909 (2017).
- [11] S. Pirandola, *Capacities of repeater-assisted quantum communications*, arXiv:1601.00966 (2016).
- [12] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621 (2012).
- [13] S. L. Braunstein and P. van Loock, *Rev. Mod. Phys.* **77**, 513 (2005).
- [14] M. Hillery, *Phys. Rev. A* **61**, 022309 (2000).
- [15] N. J. Cerf, M. Levy, and G. Van Assche, *Phys. Rev. A* **63**, 052311 (2001).
- [16] F. Grosshans and P. Grangier, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [17] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **93**, 170504 (2004).
- [18] R. Filip, *Phys. Rev. A* **77**, 022310 (2008).
- [19] C. Weedbrook, S. Pirandola, and T. C. Ralph, *Phys. Rev. Lett* **105**, 110501 (2010).
- [20] V. C. Usenko and R. Filip, *Phys. Rev. A* **81**, 022318 (2010).
- [21] C. Weedbrook, S. Pirandola, and T. C. Ralph, *Phys. Rev. A* **86**, 022318 (2012).
- [22] C. Weedbrook, C. Ottaviani, and S. Pirandola, *Phys. Rev. A* **86**, 012309 (2014).
- [23] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, *Nat. Phys.* **4**, 726 (2008).
- [24] C. Ottaviani and S. Pirandola, *Sci. Rep.* **6**, 22225 (2016).
- [25] J. H. Shapiro, *Phys. Rev. A* **80**, 022320 (2009).
- [26] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, *Phys. Rev. A* **94**, 012322 (2016).
- [27] V. C. Usenko, and F. Grosshans, *Phys. Rev. A* **92**, 062337 (2015).
- [28] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Ghering, C. S. Jacobsen, and U. L. Andersen, *Nat. Photon.* **9**, 397 (2015).
- [29] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Ghering, C.S. Jacobsen, and U. L. Andersen, *Nat. Photon.* **9**, 773 (2015).
- [30] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, *Phys. Rev. A* **91**, 022320 (2015).
- [31] S. L. Braunstein and S. Pirandola, *Phys. Rev. Lett.* **108**, 130502 (2012).
- [32] M. Curty, B. Qi, H.K. Lo, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [33] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, *High-rate secure quantum conferencing*, arXiv:1709.06988 (2017).
- [34] F. Grosshans, G. Van Ache, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, *Nature* **421**, 238 (2003).
- [35] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin *et al.*, *Phys. Rev. A* **76**, 042305 (2007).
- [36] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, *Nat. Commun.* **3**, 1083 (2012).
- [37] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, *Nat. Photon.* **7**, 378 (2013)
- [38] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, *Phys. Rev. Lett.* **111**, 010501 (2013).
- [39] J. H. Shapiro, Z. Zhang, and F. N. C. Wong, *Quantum Inf. Process.* **13**, 2171 (2014).
- [40] C. S. Jacobsen, T. Ghering, and U. L. Andersen, *Entropy* **17**, 4654 (2015).
- [41] Y.-C. Zhang *et al.*, *Continuous-variable QKD over 50km commercial fiber*, arXiv:1709.04618 (2017).
- [42] A. Leverrier, F. Grosshans, and P. Grangier, *Phys. Rev. A* **81**, 062343 (2010).
- [43] L. Ruppert, V. C. Usenko, and R. Filip, *Phys. Rev. A* **90**, 062310 (2014).
- [44] P. Papanastasiou, C. Ottaviani, and S. Pirandola, *Phys. Rev. A* **96**, 042332 (2017)
- [45] A. Leverrier, *Phys. Rev. Lett.* **114**, 070501 (2015).

- [46] A. Leverrier, *Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction*, arXiv:1701.03393 (2017).
- [47] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, *CV MDI QKD: Composable Security against Coherent Attacks*, arXiv:1704.07924 (2017).
- [48] D. Sych and G. Leuchs, *New J. Phys.* **12**, 053019 (2010).
- [49] A. Leverrier and P. Grangier, *Phys. Rev. Lett.* **102**, 180504 (2009).
- [50] A. Leverrier and P. Grangier, *Continuous-variable Quantum Key Distribution protocols with a discrete modulation*, arXiv:1002.4083 (2010).
- [51] A. Leverrier and P. Grangier, *Phys. Rev. A* **83**, 042312 (2011).
- [52] R. Garcia-Patron and N. J. Cerf, *Phys. Rev. Lett.* **97**, 190503 (2006).
- [53] Y. Bo, M. Heid, J. Rigas, and N. Lütkenhaus, *Phys. Rev. A* **79**, 012307 (2009).
- [54] K. Brádler and C. Weedbrook, *Phys. Rev. A* **97**, 022310 (2018).
- [55] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, *Quantum Inf Comput* **3**, 535-552 (2003).
- [56] S. Pirandola, S. L. Braunstein, and S. Lloyd, *Phys. Rev. Lett.* **101**, 200504 (2008).
- [57] F. Furrer, Ph.D., Leibniz Universität Hannover, 2012.
- [58] J. H. Shapiro, *IEEE Journal of Quantum Electronics* **21**, 237-250 (1985).
- [59] In order to evaluate the excess noise of the thermal-loss channel, Alice may send Gaussian-modulated decoy coherent states to Bob (interleaved with coherent states used for the key). At the end of all quantum communication, Alice informs Bob in which instances she was sending decoys so that they can use their data to compute ϵ . In the asymptotic regime, we may write $\epsilon = \frac{(1-\tau)(\omega-1)}{\tau}$.