Secret key distillation over a pure loss quantum wiretap channel under restricted eavesdropping

Ziwen Pan*, Kaushik P. Seshadreesan[†], William Clark[#], Mark R. Adcock[#],
Ivan B. Djordjevic*, Jeffrey H. Shapiro[‡], Saikat Guha[†]
*Department of Electrical & Computer Engineering, the University of Arizona, Tucson, AZ
[†]College of Optical Sciences, the University of Arizona, Tucson, AZ
[#]General Dynamics Mission Systems, Scottsdale, AZ
[‡]Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA

***Abstract*—Quantum cryptography provides absolute security against an all-powerful eavesdropper (Eve). However, in practice Eve's resources may be restricted to a limited aperture size so that she cannot collect all paraxial light without alerting the communicating parties (Alice and Bob). In this paper we study a quantum wiretap channel in which the connection from Alice to Eve is lossy, so that some of the transmitted quantum information is inaccessible to both Bob and Eve. For a pure-loss channel under such restricted eavesdropping, we show that the key rates achievable with a two-mode squeezed vacuum state, heterodyne detection, and public classical communication assistance—given by the Hashing inequality—can exceed the secret key distillation capacity of the channel against an omnipotent eavesdropper. We report upper bounds on the key rates under the restricted eavesdropping model based on the relative entropy of entanglement, which closely match the achievable rates. For the pure-loss channel under restricted eavesdropping, we compare the secret-key rates of continuous-variable (CV) quantum key distribution (QKD) based on Gaussian-modulated coherent states and heterodyne detection with the discrete variable (DV) decoy-state BB84 QKD protocol based on polarization qubits encoded in weak coherent laser pulses.**

For a full version see: https://arxiv.org/abs/1903.03136.

I. Introduction

In classical information theory, private communication over a wiretap channel $P_{Y,Z|X}$ between a sender X and a legitimate receiver Y in the presence of a wiretapper Z (Fig. 1 (a)), both without public discussion [1], and with public discussion [2], has been widely studied. The capacity of the channel for the latter task, often known as the secret key agreement capacity P_2, can exceed the capacity for the former (the private capacity P_1), and is upper bounded by the intrinsic information [3]

$$P_1 \le P_2 \le \min I(X;Y|Z') \qquad (1)$$

v

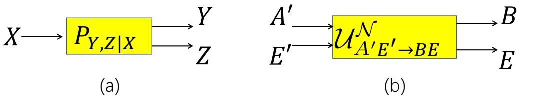

Fig. 1. (a) A Classical wiretap channel. (b) A quantum wiretap channel $\mathcal{N}_{A'E'\to BE}$ from sender A' to receiver B, isometrically extended to depict a wiretapper E, who has access to the full purification of the channel.

In the quantum case, Takeoka et al [4] gave an upper bound on the P_2 capacity of a quantum wiretap channel (Fig. 1 (b)) based on the squashed entanglement [5] of the channel, an entanglement measure inspired by the intrinsic information. More recently, Pirandola et al. [6] gave an upper bound to the P_2 capacity based on the relative entropy of entanglement of the channel. In the case of a pure-loss bosonic channel, this upper bound matches the best known lower bound [7], [8] on its P_2 capacity, and thus establishes its capacity [6].

Traditionally, in a quantum wiretap channel as shown in Fig. 1(b), the eavesdropper Eve is considered as all-powerful. Mathematically, this is referring to an isometric extension $\mathcal{U}^{\mathcal{N}}_{A'E'\to BE}$ (Note that $U_{A'E'\to BE}$ is a unitary, $\mathcal{N}_{A'\to B}$ is a channel (TPCP map), and $U_{A'\to BE}$ is an isometry. We don't need to define an isometry formally for the purposes of this paper.) of the quantum channel $\mathcal{N}_{A'\to B}$, a trace-preserving completely positive map from A to B. Eve has access to an input quantum system E', which is in a state statistically independent of Alice's system A', and jointly evolves with A' under a unitary transformation U leading to Bob's quantum system B and Eve's system E, where the BE joint system may be classical correlated or in general entangled. Physically, this implies that Eve has access to all the light Alice transmits that doesn't arrive at Bob, and all operations at the input and the output of the channel as allowed by the laws of quantum physics. However, in most realistic scenarios, Eve's capabilities are limited. Various forms of relaxations to this all powerful Eve have considered in the literature, such as lossy power collection [9], imperfect reverse classical communication [10] and finite memory lifetimes [11]. One such restriction on Eve is with regard to her flux-collection capability, e.g., in wireless communication she could be limited by the size of her receiver aperture, or more generally, she may be forbidden from collecting light from an exclusion zone around Bob's receiver without being detected. A similar model is the trusted noise QKD, see [12] for a related review.

In this work, we present a secure-key rate (SKR) analysis (lower and upper bounds) of secret key agreement over a pure-loss channel from a sender Alice to receiver Bob (Eve injects vacuum state) under such a restricted wiretap channel model, in which the eavesdropper Eve receives only a fraction of the

978-1-5386-9291-2/19/$31.00 ©2019 IEEE

photons that are lost in transmission as shown in Fig. 2. Note that this scenario is exclusive to the quantum case, i.e., it does not arise in the classical case, because the presence of any other correlated output to the channel, which neither Bob nor Eve h

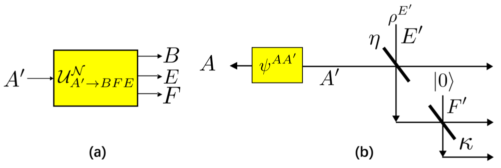

Fig. 2. (a) A restricted Eve quantum wiretap channel, modeled as a broadcast channel from sender Alice to receiver Bob, Eavesdropper Eve and a system F that neither Bob nor Eve can access. (b) Entanglement-based model for quantum communication over a lossy bosonic wiretap channel of transmissivity η from Alice to Bob under restricted eavesdropping. Alice prepares an entangled pure state $|\psi\rangle^{AA'}$ and sends A' through the channel to Bob. The restriction on the eavesdropper Eve is modeled by a pure-loss beam splitter of transmissivity κ. Eve is shown to inject a state $\rho^{E'}$ into the channel to Bob, which is a vacuum state (passive attack) in this paper.

II. Achievable Secure Key Rates over Pure-Loss Channel under Restricted Eavesdropping

Consider an asymptotically large number of independent and identically distributed (i.i.d.) copies of an entangled pure state $\psi^{AA'}$ at Alice's side, and A' being sent to Bob through the wiretap channel as illustrated in Fig. 2. Traditionally in security analysis, Eve is assumed to have access to all the light that doesn't arrive at Bob, i.e. access to the full purification of the state across the channel ρ^{AB}. In other words, Eve holds a quantum system E such that the systems A, B and E are in a pure state $|\psi\rangle^{ABE}$ satisfying $\rho^{AB} = \mathrm{Tr}_E(\psi^{ABE})$.

In this model, with collective attack as the optimal attack for an eavesdropper Eve [13], the Hashing lower bound on the key rate for direct reconciliation, namely when Alice measures system A to give rise to a classical outcome X that is publically communicated to Bob, is given by

$$K_{\rightarrow}(\rho) \geq I(X;B)_{\omega} - I(X;E)_{\omega}. \tag{2}$$

Here state $\omega^{XBE} = \sum_x P(x)|x\rangle\langle x|^X \otimes \rho_x^{BE}$, the quantum mutual information quantities $I(X;B)$ and $I(X;E)$ are the Holevo information quantities

$$I\left(P(x);B\right) = H(B) - \sum_x P(x)H\left(\rho_x^B\right) \tag{3}$$

$$I\left(P(x);E\right) = H(E) - \sum_x P(x)H\left(\rho_x^E\right). \tag{4}$$

Conditional quantum states ρ_x^B and ρ_x^E are defined as:

$$\rho_x^B = \sum_{|e\rangle}\langle e|\rho_x^{BE}|e\rangle,\ \ \rho_x^E = \sum_{|b\rangle}\langle b|\rho_x^{BE}|b\rangle, \tag{5}$$

where ρ_x^{BE} is the density matrix of system BE conditioned on the measurement result $X = x$.

$$\begin{aligned} K_{\rightarrow} &\geq I(X;B) - I(X;E) & (6)\\ &= H(B) - H(E) - \sum_x P(x)\left(H\left(\rho_x^B\right) - H\left(\rho_x^E\right)\right). & (7)\end{aligned}$$

For reverse reconciliation, similarly, by changing the roles of Alice and Bob, we arrive at an expression for a Hashing lower bound on the secret key distillation rate $K_{\leftarrow}$ given by

$$\begin{aligned} K_{\leftarrow} &\geq I(A;Y) - I(Y;E) & (8)\\ &= H(A) - H(E) - \sum_y P(y)\left(H\left(\rho_y^A\right) - H\left(\rho_y^E\right)\right) & (9)\end{aligned}$$

Y being the classical outcome of measuring Bob's quantum system B. Notice that because $\kappa \neq 1$ in Fig. 2, ρ^{ABE} is not a pure state . (Here the pure state would be $|\psi\rangle^{ABEF}$ for pure-loss channel.) That's why Eqs. (7) and (9) can't be further simplified. In unrestricted case ($\kappa = 1$), Eqs. (7) and (9) can give us coherent and reverse coherent information [14], [15].

III. Upper Bounds for Secret Key Distillation under Restricted Eavesdropping

In this section, we recall the relative entropy of entanglement [16] of a channel, which serves as an upper bound on the entanglement and secret key distillation capacities of the channel under unlimited two-way classical assistance. We extend these measures to the restricted eavesdropping model.

Definition 1: The relative entropy of entanglement of a state ρ_{AB} is defined as its relative entropy with the closest separable state in Hilbert space:

$$E_{\mathrm{R}}(\rho) := \inf_{\sigma\in\mathrm{SEP}} D(\rho||\sigma), \tag{10}$$

where $D(\rho||\sigma)$ is the relative entropy between states ρ and σ, defined as $D(\rho||\sigma) := \mathrm{Tr}\left(\rho\left(\log\rho - \log\sigma\right)\right)$.

Definition 2: The relative entropy of entanglement of a channel $\mathcal{N}_{A'\to B}$ is defined as [6]

$$E_{\mathrm{R}}(\mathcal{N}) := \sup_{\phi^{AA'}} E_{\mathrm{R}}\left(A;B\right)_{\rho}, \tag{11}$$

where $\rho^{AB} = \mathcal{N}_{A'\to B}(\phi^{AA'})$. In other words, it is the relative entropy of the state distributed across the channel optimized over all possible inputs to the channel.

Using the relative entropy of entanglement of a channel, Pirandola et al. (PLOB) [6] gave an upper bound to the energy-unconstrained, two-way unlimited LOCC-assisted secret key distillation capacity of a pure-loss channel of transmissivity η as $P_2 \leq -\log_2(1-\eta)$. Using the same method, Takeoka et al. [17], then derived the capacity region of a pure-loss broadcast channel.

An upper bound on the secret key distillation capacity under the restricted eavesdropping model considered here follows from the broadcast channel result [17][Eq. (26)] as:

$$E_{\mathrm{R}}(B;AF)_{\phi} = \log_2\left(\frac{1-\eta_F}{1-\eta_B-\eta_F}\right). \tag{12}$$

Here the notation $B;AF$ means that the closest separable state for the relative entropy entanglement calculation is a state separating system B from systems AF. In Ref. [17], key to obtaining the above bound was the different physical realizations of the same broadcast channel, one of them being as shown in Fig. 3. Since only vacuum states are injected from

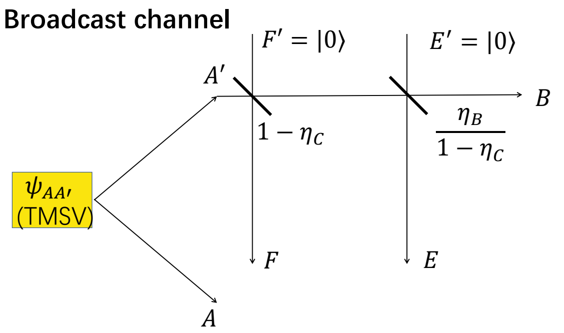

Fig. 3. Broadcast channel shown in [17], where a single sender sends information to receivers F, E and B through different lossy channels. Here the signal state is sent out from A' while only vacuum states are injected from F' and E'. This can be viewed as equivalent to our model if we consider mode F as an inaccessible system, and E as the eavesdropper Eve.

F' and E' in Fig. 3, it is equivalent to our model in Fig. 2 with $\eta_B = \eta$ and $\eta_C = (1-\kappa)(1-\eta)$. Thus, the upper bound expression for our restricted eavesdropping case is obtained as

$$E_{\mathrm{R}}(B;AF) = \log_2\left(\frac{\eta+\kappa(1-\eta)}{\kappa(1-\eta)}\right). \tag{13}$$

IV. Results

In this section, we apply the methods of secure key rate (SKR) analysis and upper bounds presented in Secs. II and III to pure-loss channels fed with an input two-mode squeezed vacuum (TMSV) state $|\Psi\rangle^{AA'} = (\cosh r)^{-1}\sum_{n=0}^{\infty}(\tanh r)^n|n\rangle|n\rangle$. The achievable rates are given for heterodyne detection either at Alice or Bob, which correspond to direct and reverse information reconciliation scenarios, respectively.

A. Achievable Secure Key Rates

First we will show the achievable rate with direct reconciliation, namely when Alice performs heterodyne detection on her system, as depicted in Fig. 4. Assuming TMSV state input, we calculate the achievable rate for this setup.

Since the heterodyne measurement on A projects the other part A' of the TMSV onto a coherent state $\rho_x^{A'} = |\alpha\rangle$, we know that the state at the outputs of the beam splitters conditioned on measurement result x, namely ρ_x^B, ρ_x^E, ρ_x^F, are also coherent states with attenuated amplitudes. Because they are pure states we have

$$H\left(\rho_x^B\right) = H\left(\rho_x^E\right) = 0 \tag{14}$$

So, using Eq. (7), we have

$$\begin{aligned} K_{\rightarrow} &\geq H(B) - H(E) & (15)\\ &= h\left(\eta\mu\right) - h\left(\kappa\mu\left(1-\eta\right)\right), & (16)\\ \lim_{\mu\to\infty} K_{\rightarrow} &= \log_2\frac{\eta}{\kappa(1-\eta)}, & (17)\end{aligned}$$

where $h(x) = (x+1)\log_2(x+1) - x\log_2(x)$ is the von Neumann entropy of a thermal Gaussian state of mean photon number x [18]. Eq. (17) gives the limiting value of the key rate when the input mean photon number μ is taken to infinity, which can be shown to be the optimal input power. Notice that in Eq. (17) κ is in the denominator inside the log function, thus restricting Eve's received power can help increase the achievable rate beyond the rate achievable against unrestricted Eve, viz., $\log_2\left(\frac{\eta}{1-\eta}\right)$ ($\kappa = 1$ in Eq. (17)).

In the case of an unrestricted Eve and direct reconciliation, we need to have $\eta > (1-\eta)$ to attain a positive key rate in Eq. (17). Similarly, for the key rate to be greater than zero in the restricted Eve case, we need to have $\eta > \kappa(1-\eta)$. This condition captures the limitation of direct reconciliation with regard to the transmission distance, namely that the key rate turns vanishes beyond a threshold distance because transmissivity η decreases with increasing transmission distance.

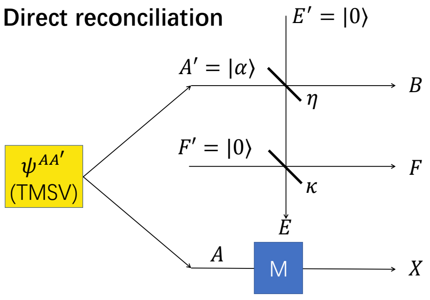

Fig. 4. Entanglement-based model for secret key distillation over a pure loss bosonic channel based on heterodyne detection and direct reconciliation. Here Alice performs heterodyne measurement of system A and this projects the system A' of the TMSV state onto a coherent state $|\alpha\rangle^{A'}$. She then sends side information in the classical channel to Bob to help him distill keys from his system. Here vacuum states are injected from E' and F' denoting a pure-loss channel. The restriction on Eve is imposed by letting only a fraction κ of the wiretapped light to arrive at Eve's receiver.

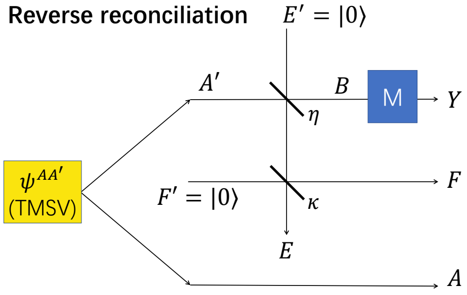

Fig. 5. Entanglement-based model for secret key distillation over a pure-loss bosonic channel based on heterodyne detection and reverse reconciliation. Here Bob performs heterodyne measurement on his system B; the states injected from E' and F' are vacuum states.

Now, consider the case of reverse reconciliation, as depicted in Fig. 5. Here, Bob performs heterodyne measurement on his system B and sends side information through a classical communication channel to Alice to help her distill secret key. Using Eq. (9), we get

$$\begin{aligned} K_{\leftarrow} \geq\ & h(\mu) - h(\kappa\mu(1-\eta)) \\ & - \sum_y P(y)\left(h\left(\frac{\mu(1-\eta)}{1+\eta\mu}\right) - h\left(\frac{(1-\eta)\kappa\mu}{1+\eta\mu}\right)\right) \end{aligned} \tag{18}$$

$$
\begin{aligned}
&= h(\mu) - h(\kappa\mu(1-\eta)) \\
&- \left(h\left(\frac{\mu(1-\eta)}{1+\eta\mu}\right) - h\left(\frac{(1-\eta)\kappa\mu}{1+\eta\mu}\right) \right),
\end{aligned} \tag{19}
$$

$$
\lim_{\mu\to\infty} K_{\leftarrow} = \log_2 \frac{1}{\kappa(1-\eta)} - h\left(\frac{1-\eta}{\eta}\right) + h\left(\frac{(1-\eta)\kappa}{\eta}\right). \tag{20}
$$

Since in this case the post-measurement conditional states are mixed states, we will have to derive the covariance matrix and calculate the von Neumann entropies shown in Eq. (18). Since the argument of the h functions in Eq. (18) is independent of $P(y)$, we get Eq. (19) by summing over $P(y)$ to equal one. Taking the limit of input photon number $\mu \to \infty$, we obtain the optimal achievable rate given in Eq. (20).

Eq. (20), when $\kappa = 1$, reduces to $-\log_2(1-\eta)$, which is the capacity for the pure-loss channel under unrestricted eavesdropping. If we compare Eq. (20) for $\kappa \neq 0$ with $-\log_2(1-\eta)$, not only do we have κ showing up in the denominator inside the log function, but we also have the correction term: $-(h(\frac{\mu(1-\eta)}{1+\eta\mu}) - h(\frac{(1-\eta)\kappa\mu}{1+\eta\mu}))$. This correction term changes differently with κ compared to the first term $\log_2(\frac{1}{\kappa(1-\eta)})$. Unlike the case with omnipotent Eve, we find that the achievable rate with reverse reconciliation is not always better than the rate with direct reconciliation.

Here in Fig. 6, we plot the SKR as a function of κ for channel transmissivity $\eta = 0.6$. When $1 - \kappa \ll 1$, which includes the unrestricted Eve's case ($\kappa = 1$), we find that reverse reconciliation gives a higher achievable rate than direct reconciliation. However this is not always the case, since for $\kappa \ll 1$ the rate with direct reconciliation is shown to exceed the rate with reverse reconciliation.

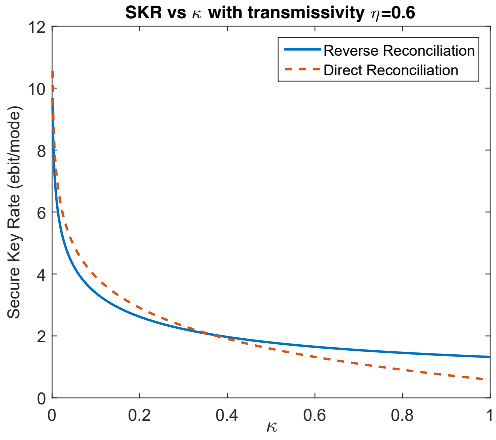

Fig. 6. Secure key rate against restricted eavesdropping over a pure-loss channel with TMSV state and heterodyne detection. Direct reconciliation vs. reverse reconciliation rates as a function of κ. Here the channel transmissivity is set to $\eta = 0.6$.

In Fig. 7, we plot the direct and reverse reconciliation achievable rates as a function of the channel loss in dB for $\kappa = 0.1$. We see that the reverse reconciliation scheme has a better transmission distance than the direct reconciliation scheme, which is similar to the case when Eve is unrestricted as was shown in [7]. However, here both direct reconciliation and reverse reconciliation can achieve higher rates than is the case when Eve is unrestricted.

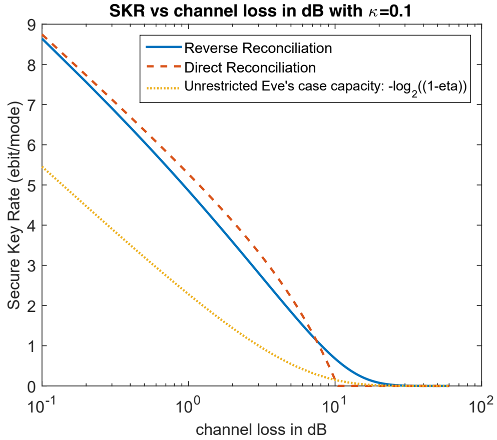

Fig. 7. Direct reconciliation vs. reverse reconciliation achievable rate as a function of channel loss in dB with $\kappa = 0.1$. Here the channel capacity against unrestricted Eve [6] is also shown for comparison.

B. Upper Bounds

In this section we apply Eq. (13) to plot the upper bound against lower bounds for different values of κ in Fig. 8. The plot shows how our upper bound works against lower bound in pure loss channel. We plot the relative entropy entanglement upper bound and lower bound for three sets of different values of κ, denoted by different colors.

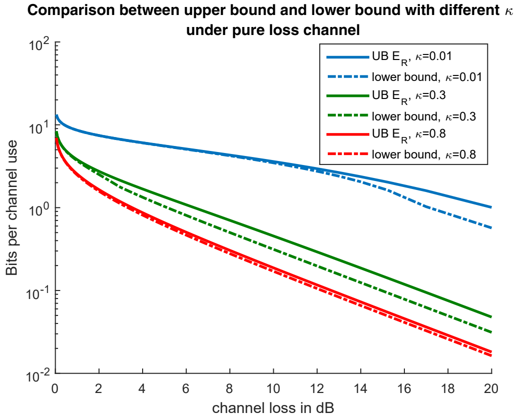

Fig. 8. Relative entropy of entanglement upper bounds (UB E_R) and lower bounds with different values of thermal noise. The input photon number for the upper bounds is 10^3.

Here we can see that when κ is close to 1, the upper bound almost matches the lower bound. And they match each other when $\kappa = 1$ which corresponds to the unrestricted case [6]. However when κ decreases the upper bound becomes looser, but still can give us a very narrow space for possible capacity of the channel for the task of secret key distillation. The small gaps between our upper bounds and lower bounds have narrow the region to search for this problem's capacity.

One interesting thing to see from Fig. 8 is that the region where direct reconciliation gives higher rate than reverse reconciliation has a large overlap with the region where the upper bound and lower bound are closest to each other. For example, when $\kappa = 0.01$ in Fig. (8) the upper bound and lower bound diverge from each other close to the point where direct reconciliation starts to give a lower rate than reverse reconciliation. Another observation from the plot is that when κ decreases the lower bound tends to decrease slower with increasing channel loss at least when channel loss is low.

V. Comparison between CV and DV QKD under Restricted Eavesdropping

In this section, we compare achievable rates against restricted Eve for the Gaussian-modulated CV QKD protocol (with coherent states and heterodyne detection) and the DV decoy-state BB84 protocol. A similar restricted eavesdropping model analysis on DS-BB84 is done in *"Exclusion-Zone Analysis for Decoy-State BB84 Quantum Key Distribution"* by Jeffrey H. Shapiro, to be published.

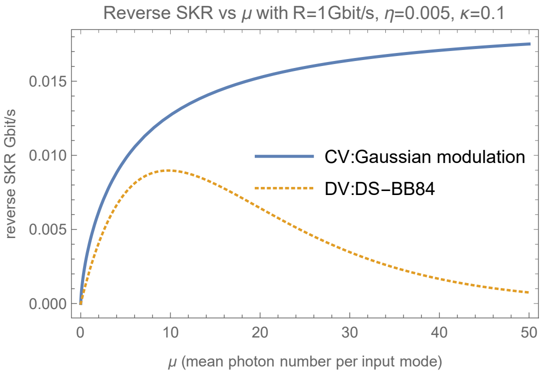

Fig. 9. Comparison of achievable rates for secret key distillation from TMSV state with heterodyne detection and reverse reconciliation vs. DS-BB84 protocol over a pure-loss channel. Here we assume the same Alice's signal-state transmission rate for both protocols: $R = 1$ Gbit/s. Plots with Bob and Alice both making heterodyne detection and imperfect reconciliation efficiency are included in [19].

In Fig. 9, we can see that for any value of input power, the CV scheme has a higher rate than DS-BB84. Also in the analysis of DS-BB84 there is an optimal input photon number, which is why we see the peak in the green curve whereas the optimal input photon number in the CV scheme is infinity, and hence the rate keeps increasing with increasing input photon number. This shows the potential of Gaussian-modulated CVQKD to outperform DS-BB84 in this restricted-eavesdropping scenario, opening competitive alternative options for realistic applications.

VI. Concluding Remarks

In summary, we showed lower bounds (achievable rates) for secret key distillation under restricted eavesdropping over pure-loss channels based on heterodyne detection. We showed that putting a reasonable restriction on Eve can increase the key rate and extend the transmission range under the same channel conditions. Furthermore, we calculated upper bounds under the same conditions using the relative entropy of entanglement and showed that they are very close to the achievable rates with heterodyne detection, thus establishing a narrow gap in which capacity must be. All our results capture how the key rates and the transmission distances can increase with the assumption of restricted eavesdropping, which could help with realistic applications in which Eve's light capture is apt to be restricted in the manner assumed in this paper.

References

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 499–514, March 1999.

[4] M. Takeoka, S. Guha, and M. M. Wilde, "The squashed entanglement of a quantum channel," *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4987–4998, Aug 2014.

[5] M. Christandl and A. Winter, ""squashed entanglement": An additive entanglement measure," *Journal of Mathematical Physics*, vol. 45, no. 3, pp. 829–840, 2004.

[6] S. Pirandola et al., "Fundamental limits of repeaterless quantum communications," *Nature communications*, vol. 8, p. 15043, 2017.

[7] R. García-Patrón et al., "Reverse coherent information," *Physical review letters*, vol. 102, no. 21, p. 210501, 2009.

[8] S. Pirandola et al., "Direct and reverse secret-key capacities of a quantum channel," *Physical review letters*, vol. 102, no. 5, p. 050503, 2009.

[9] J. Gariano et al., "Engineering trade studies for a quantum key distribution system over a 30 km free-space maritime channel," *Applied optics*, vol. 56, no. 3, pp. 543–557, 2017.

[10] D. Ding and S. Guha, "Noisy feedback and loss unlimited private communication," *arXiv preprint arXiv:1801.03996*, 2018.

[11] C. Lupo and S. Lloyd, "Quantum-locked key distribution at nearly the classical capacity rate," *Physical review letters*, vol. 113, no. 16, p. 160502, 2014.

[12] V. Usenko and R. Filip, "Trusted noise in continuous-variable quantum key distribution: a threat and a defense," *Entropy*, vol. 18, no. 1, p. 20, 2016.

[13] R. Renner and J. I. Cirac, "de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, p. 110504, Mar 2009.

[14] S. Pirandola, "Quantum discord as a resource for quantum cryptography," *Scientific reports*, vol. 4, p. 6956, 2014.

[15] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 461, no. 2053. The Royal Society, 2005, pp. 207–235.

[16] V. Vedral et al., "Quantifying entanglement," *Phys. Rev. Lett.*, vol. 78, pp. 2275–2279, Mar 1997.

[17] T. Masahiro et al., "Unconstrained distillation capacities of a pure-loss bosonic broadcast channel," in *Information Theory (ISIT), 2016 IEEE International Symposium on*. IEEE, 2016, pp. 2484–2488.

[18] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods*, 1st Edition 1st Edition, Ed. CRC Press, 2017.

[19] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, "Secret key distillation across a quantum wiretap channel under restricted eavesdropping," *arXiv preprint arXiv:1903.03136*, 2019.