Secret key generation over a lossy optical channel with a passive quantum eavesdropper: Capacity bounds and new explicit protocols

Saikat Guha*, Masahiro Takeoka*, Hari Krovi*, Mark M. Wilde‡, Cosmo Lupo§,

*Raytheon BBN Technologies, †NICT Japan, ‡LSU, §MIT

***Abstract*—The secret-key capacity of a quantum broadcast channel $\mathcal{N}^{A\to BE}$ is the information theoretic limit at which two parties A and B can generate shared keys per use of the channel that are kept secret from an eavesdropper E, while A and B may also have unlimited classical communication over an insecure, but authenticated, public channel. Since light is fundamentally quantum, ultimate limits on secret-key generation over an optical channel must be treated quantum-mechanically. The most powerful passive eavesdropper for a lossy bosonic channel is one who collects all the photons that do not reach the intended receiver, could store all such collected light over many channel uses (i.e., over the duration of the entire protocol) perfectly in a quantum memory, and make an arbitrary collective quantum measurement on her memory. For a key to be secure, E must have vanishingly small information about the key. In this paper, we propose three new protocols for the lossy bosonic channel, which are secure to the most general passive quantum eavesdropper. One of the explicit protocols we propose—inspired by a classical proposal by Maurer [1]—is readily implementable with standard optical technology, and can generate secret keys for any amount of channel loss. We also propose a well-informed conjecture on the ultimate secret-key capacity of the lossy bosonic channel, and compare the secret-key rates of one-way and two-way protocols.**

The *Private capacity* (C_p) of a discrete memoryless classical broadcast channel $P_{YZ|X}$ (X = Alice, Y = Bob and Z = Eve) is the maximum rate at which Alice can send data reliably to Bob while leaking asymptotically zero information to Eve in the limit of communicating over many channel uses. The private capacity of a classical broadcast channel $P_{YZ|X}$ can be expressed exactly in terms of entropic quantities involving the channel's inputs and outputs [2], [3], and there are explicit error-correcting strategies known that achieve the private capacity [4]. A similar statement could be made for the private capacity of a quantum broadcast channel $\mathcal{N}^{A\to BE}$, although the expression for private capacity for a general quantum channel requires a regularization over channel uses [5], [6]. Recently, explicit codes were found that in principle could achieve the private capacity of a quantum channel [7]. The *secret key capacity* (C_s) of a (classical or quantum) broadcast channel on the other hand is less well understood. We define the (one-way) secret-key capacity is defined as the maximum rate at which Alice and Bob can generate a shared secret key using the (classical or quantum) broadcast channel (one way) with unlimited classical communication over a two-way authenticated public channel. It is clear that $C_s \geq C_p$, since one way to generate a shared secret key is for Alice to generate a random bit string locally and send it privately to Bob. Lower and upper bounds on the secret-key capacity are known for classical and quantum channels. However, an exact information theoretic characterization of the secret-key capacity for a general channel still eludes us, even for classical channels. The secret-key capacity is however exactly known for a few classical channels.

In this paper, we explore the secret-key capacity, and explicit key-generation protocols, of the single-mode lossy bosonic channel $\mathcal{N}_\eta$ with transmissivity $\eta \in (0,1]$—such as an optical fiber or a finite-aperture-size diffraction-limited free-space optical channel—where the eavesdropper is assumed to be able to collect all the photons that do not reach Bob, and to have arbitrarily powerful quantum (memory and measurement) resources. This is a channel whose private capacity is exactly known, and is equal to zero when the channel loss is higher than 3 dB ($\eta < 1/2$) [8]. The secret-key capacity on the other hand is not known, but is positive for any amount of channel loss [9], [10]. Finally, one may also define a two-way secret-key capacity $C_s^{(2)}$ as the maximum secret-key generation rate permissible when a (classical or quantum) broadcast channel is used in both directions,

with the assistance of a two-way insecure authenticated public channel. For a classical broadcast channel, a lower bound for $C_s^{(2)}$ was recently proposed [11]. Not much is known about $C_s^{(2)}$ for quantum broadcast channels, even for simple quantum channel instantiations. However, key-generation protocols have recently been proposed for the two-way lossy bosonic channel [12], [13], which can achieve a non-zero secret-key rate for any channel loss.

The highlights of our main accomplishments in this paper are summarized below:

1. A key generation protocol with one-way laser-light optical and two-way public communication: We propose a new secret-key-generation protocol for the lossy bosonic channel $\mathcal{N}_\eta$, and show that it can generate shared secret keys at any amount of channel loss. When the channel loss is greater than 3 dB ($\eta < 1/2$), Eve has a better channel from Alice than what Bob has. The two-way public discussion helps give Alice and Bob an edge over Eve. Our protocol is inspired by a key-generation protocol proposed by Maurer for the binary-symmetric classical broadcast channel [1]. The protocol starts with Alice preparing a stream of binary-phase shift keyed (BPSK) coherent state pulses, chosen randomly from $\{|\alpha\rangle, |-\alpha\rangle\}$, and sending them to Bob over the lossy channel (see Fig. 1). Bob receives coherent states $\left\{|\sqrt{\eta}\,\alpha\rangle, |-\sqrt{\eta}\,\alpha\rangle\right\}$, where $\eta \in (0,1]$ is the channel's power transmissivity. Bob then makes a balanced homodyne detection measurement, followed by a binary hard decision. He then adds to it modulo 2 a locally generated binary-valued random variable V, and sends it over the public channel. Alice retrieves V (the shared secret key) by another modulo-2 addition and a classical decoder. We show that, even if Eve is allowed to collect all the photons that do not reach Bob, and receive Bob's transmission on the public channel, Alice and Bob can generate shared keys securely at a rate given by, $C_s^{(\mathrm{BPSK,hom})} = 1 - h(\epsilon) - h\left(\frac{1+\kappa}{2}\right) + h\left(\frac{1+\sqrt{1-4\epsilon(1-\epsilon)(1-\kappa^2)}}{2}\right)$, where $h(\cdot)$ is the binary entropy function, $\epsilon = \frac{1}{2}\mathrm{erfc}(\sqrt{2\eta\bar{n}})$ and $\kappa = e^{-2(1-\eta)\bar{n}}$. The key rates are plotted in Fig. 2. Our protocol can be readily extended to Alice using an M-ary PSK alphabet $\left\{|\alpha e^{j2\pi k/M}\rangle\right\}$, $0 \le k \le M-1$, Bob using heterodyne detection, and adding V—chosen uniformly at random in $\{0, 1, \ldots, M-1\}$—modulo M to the hard-decision heterodyne output, which he broadcasts over the public channel. The key rate of this M-ary PSK protocol will be higher than the BPSK protocol, and can be calculated following the same method illustrated in [18].

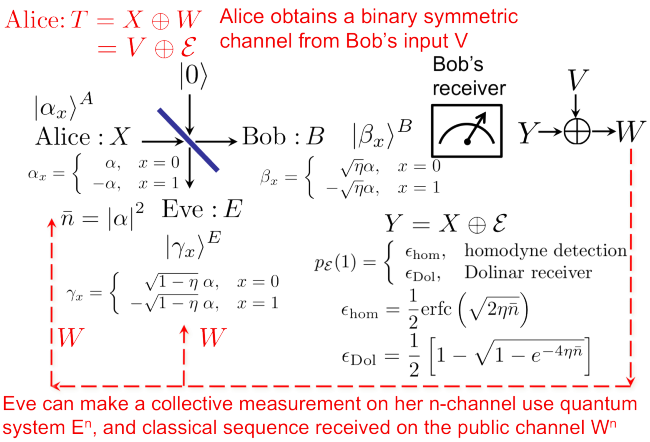

Fig. 1. A schematic diagram of our key generation protocol over the lossy optical channel, which uses one-way quantum communication and a two-way insecure, but authenticated, public classical channel.

A couple of things to note about the above result are as follows:

(a) First exact secret-key capacity evaluation of a quantum channel with a constrained transceiver: Under simple, and implementable, structural constraints on Alice's transmitter and Bob's receiver, we *exactly* computed the secret-key capacity of the lossy bosonic channel. We first characterized the achievable rate versus loss performance of our protocol using [5]. We then evaluated an upper bound to the achievable secret key rate under the structural assumptions that the transmitter uses binary-phase laser-light modulation and that Bob uses an ideal homodyne detection measurement, using the intrinsic information [16]. We showed that the achievable rate exactly matches the upper bound, thereby showing it cannot be exceeded by any other protocol operating with the same transceiver structural constraints.

(b) Ease of implementation of our protocol: Our protocol does not need non-classical or entangled optical states (unlike Shapiro's two-way quantum-illumination protocol [13] and Pirandola *et al.*'s two-way protocol [12]), but it can still beat the most general passive quantum eavesdropping. We need a BPSK laser transmitter, near-unity detection-efficiency homodyne detection (which is fairly standard), and a good binary code for a symmetric error channel (for the reverse classical communication). Assuming Alice uses an ideal laser transmitter with 100 ps (10 GHz) binary phase modulated pulses with roughly 0.08 photons per pulse, and while Bob uses a LO-shot-noise-limited homodyne detection measurement, our protocol can generate shared secret keys at a rate of roughly 1 Mbps at an end-

to-end channel loss of $\sim$ 27 dB ($\approx$ 135 km of 0.2 dB/km telecom fiber). Garcia-Patron and Cerf [9], and Pirandola *et al.* [10] proposed a less-explicitly defined strategy which uses an entangled two-mode squeezed vacuum transmitter and homodyne detection. However, that strategy can be implemented on the lossy bosonic channel using coherent states generated from a Gaussian distribution and public communication. The key rate of this *reverse-reconciliation* strategy is shown in Fig. 2.

2. A key generation protocol with two-way optical communication: We propose an explicit implementable protocol that uses the optical channel in both directions, but does not make use of the two-way public channel. This protocol uses laser-light BPSK modulation (Alice), homodyne detection (Bob), and phase-matched local-oscillator lasers at both Alice's and Bob's stations (for applying phase-space displacement operations, $\hat{D}(\alpha)$). It is similar in spirit to the one-way protocol in Fig. 1, except that Bob, instead of making a measurement, 'adds' V by a coherent amplitude translation and uses the optical channel for sending the quantum state back to Alice. We find that the achievable key rate—secure against the general passive quantum eavesdropper—is non zero for channel transmissivities $\eta > 1/3$. This is intriguing since key extraction purely by using the one-way wiretap-channel protocol (which also doesn't use public communication)—even when using the channel in both directions—cannot generate secret keys for $\eta < 1/2$ [8].

3. A key generation protocol with one-way entangled-light transmission and two-way public communication: We propose a (not-so-practical yet) protocol that uses a bipartite temporal-mode-entangled optical state in a hybrid single-photon-polarization coherent-state qubit state given by $C[|1\rangle^{\mathrm{H}}|\alpha\rangle^{A'} + |1\rangle^{\mathrm{V}}|-\alpha\rangle^{A'}]$ at Alice's end. Alice sends the optical modes (A') on the lossy channel to Bob, and Bob makes a collective measurement over many channel uses using a joint-detection receiver (JDR). The achievable key rate for this protocol exceeds that of the one-way protocol, and is given by: $C_s^{\mathrm{BPSK-entangled}} = h\left([1+e^{-2\bar{n}}]/2\right) - h\left([1+e^{-2(1-\eta)\bar{n}}]/2\right)$.

4. Conjecture on the secret-key capacity: Finally, we conjecture that the secret-key capacity of the lossy bosonic channel $\mathcal{N}_\eta$ is given by $C_s = \ln(1/(1-\eta))$. The *reverse coherent information* of a quantum channel is known to be an achievable secret key distillation rate [5]. The reverse coherent information for the lossy bosonic channel $\mathcal{N}^{A\to BE}$ was found by Pirandola *et al.*, and is given by $E_R(\mathcal{N}^{A\to BE}) = \ln(1/(1-\eta))$ [10]. An upper bound on the distillable secret key

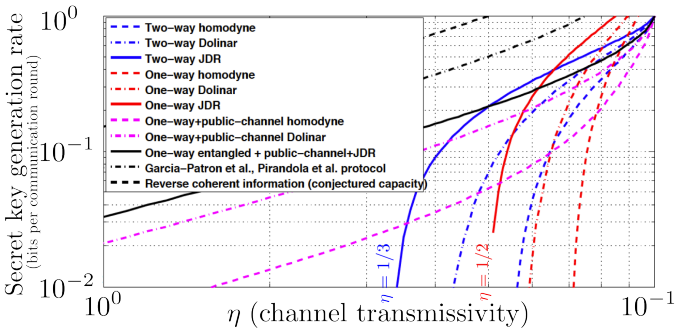

Fig. 2. Secret key generation rate as a function of channel's transmissivity η. One-way private capacities, used for key generation, multiplied by 2 for fair comparison with two-way protocols.

rate from $(\rho^{ABE})^{\otimes n}$ was found by Christandl *et al.* in terms of the *intrinsic information*, $I(A;B\downarrow E) \equiv \inf_{\Lambda^{E\to E'}} I(A;B|E')$ [16]. We evaluated a potentially loose upper bound $I(A;B|E)$ for $\mathcal{N}_\eta$ under i.i.d. coherent-state transmissions from a Gaussian ensemble, and found it to equal $\max_{\bar{n}}\left[g(\bar{n}) - g((1-\eta)\bar{n})\right] = \ln(1/(1-\eta))$, which matches the achievable rate. However, the analysis in Ref. [16] was done for finite dimensional channels, whereas the unconstrained optical channel (no structural assumptions on the transmitter, receiver and protocol) is infinite dimensional. Furthermore, it is not clear whether an alternative (non i.i.d., non-classical) transmission strategy might increase the intrinsic information upper bound.

The secret-key rates of all the above protocols and the conjectured secret-key capacity of the lossy bosonic channel are plotted in Fig. 2. As expected, the rates of all the BPSK protocols go to 1 bit (2 bit per round for one-way private protocols) at $\eta = 1$. For details, see [18].

Conclusions

The information-theoretic limits on the rate of secret-key generation over a noisy channel (either classical or quantum), with unlimited public discussion are not known for general channels. We proposed new key-generation protocols for the lossy bosonic channel (such as lossy fiber or a diffraction-limited free-space optical channel), two of which can be implemented easily. We also presented a conjecture, backed by strong evidence, on the ultimate secret key capacity of the lossy bosonic channel. In continuing work, we are investigating explicit protocols, codes, and structured realizations of optical receivers to achieve the ultimate secret-key capacity. We are also pursuing extensions of the security analysis of our one- and two-way protocols to prove security under general coherent-attacks by an active eavesdropper.

ACKNOWLEDGMENTS

This research was supported by the MIT-BBN-LSU DARPA Quiness QuSecComm program. SG thanks Ashish Khisti for introducing him to secret key capacity with public discussion, and Refs. [1] and [15]. The authors thank Profs. Jeffrey H. Shapiro and Seth Lloyd for several helpful discussions.

REFERENCES

[1] U. Maurer, "Secret Key Agreement by Public Discussion from Common Information", IEEE Transactions on Information Theory, Vol. 39, No. 3, May (1993).

[2] A. D. Wyner, "The wire-tap channel", Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, (1975).

[3] I. Csiszár and J. Korner, "Broadcast channels with confidential messages", IEEE Transactions on Information Theory, vol. IT-24, pp. 339-348, May (1978).

[4] Hessam Mahdavifar and Alexander Vardy, "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes", arXiv:1001.0210 [cs.IT], to appear in the IEEE Transactions on Information Theory (2011).

[5] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel", IEEE Transactions on Information Theory , vol. IT-51(1), pp. 44-55, January (2005).

[6] N. Cai, A. Winter, R. W. Yeung, "Quantum Privacy and Quantum Wiretap Channels", Probl. Peredachi Inf., 40:4, 26-47, (2004).

[7] Joseph M. Renes and Mark M. Wilde, "Polar codes for private and quantum communication over arbitrary channels", arXiv:1212.2537 [quant-ph], (2012).

[8] S. Guha, J. H. Shapiro, B. I. Erkmen, "Capacity of the Bosonic Wiretap Channel and the Entropy Photon-Number Inequality", Proceedings of the IEEE International Symposium on Information Theory, pp. 91-95, Toronto, ON (2008).

[9] Raul Garcia-Patron and Nicolas J. Cerf, "Continuous-variable quantum key distribution protocols over noisy channels", Phys. Rev. Lett. 102, 130501 (2009).

[10] Stefano Pirandola, Raul Garcia-Patron, Samuel L. Braunstein, Seth Lloyd, "Direct and Reverse Secret-Key Capacities of a Quantum Channel", Phys. Rev. Lett. 102, 050503 (2009).

[11] H. Ahmadi, R. S.-Naini, "Secret Key Agreement over Two-Way Broadcast Channels", *dspace.ucalgary.ca/bitstream/1880/47531/1/2009-948-27.pdf*, (2009).

[12] Stefano Pirandola, Stefano Mancini, Seth Lloyd, Samuel L. Braunstein, "Security of two-way quantum cryptography against asymmetric Gaussian attacks", Nature Physics 4, 726 (2008).

[13] J. H. Shapiro, "Defeating passive eavesdropping with quantum illumination", Phys. Rev. A **80**, 022320 (2009).

[14] M. van Dijk, On a special class of broadcast channels with confidential messages, IEEE Transactions on Information Theory , vol. IT-43(2), pp. 712-714, March (1997).

[15] R. Ahlswede and I. Csiszár, "Common Randomness in Information Theory and Cryptography-Part I: Secret Sharing", IEEE Transactions on Information Theory, Vol. 39, No. 4, May (1993).

[16] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, R. Renner, "Unifying classical and quantum key distillation", Proceedings of the 4th Theory of Cryptography Conference, Lecture Notes in Computer Science vol. 4392, pp. 456-478, (2007).

[17] M. M. Wilde, "From Classical to Quantum Shannon Theory", arXiv:1106.1445v5 [quant-ph], *to be published by Cambridge University Press*, (2013).

[18] S. Guha, M. Takeoka, H. Krovi, M. M. Wilde, C. Lupo, "Secret key generation over a lossy optical channel with a passive quantum eavesdropper: Capacity bounds and new explicit protocols: LONG PAPER", *submitted to AQIS 2013*, (2013)