Key Assistance, Key Agreement, and Layered Secrecy for Bosonic Broadcast Channels

Uzi Pereg
Technical University of Munich
uzi.pereg@tum.de

Roberto Ferrara
Technical University of Munich
roberto.ferrara@tum.de

Matthieu R. Bloch
Georgia Institute of Technology
matthieu.bloch@ece.gatech.edu

2021 IEEE Information Theory Workshop (ITW) | 978-1-6654-0312-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ITW48936.2021.9611359

***Abstract*—Secret-sharing building blocks based on quantum broadcast communication are studied. The confidential capacity region of the pure-loss bosonic broadcast channel is determined with key assistance, under the assumption of the long-standing minimum output-entropy conjecture. If the main receiver has a transmissivity of $\eta < \frac{1}{2}$, then confidentiality solely relies on the key-assisted encryption of the one-time pad. We also address conference key agreement for the distillation of two keys, a public key and a secret key. A regularized formula is derived for the key-agreement capacity region. In the pure-loss bosonic case, the key-agreement region is included within the capacity region of the corresponding broadcast channel with confidential messages. We then consider a network with layered secrecy, where three users with different security ranks communicate over the same broadcast network. We derive an achievable layered-secrecy region for a pure-loss bosonic channel that is formed by the concatenation of two beam splitters.**

I. Introduction

Physical-layer security requires the communication of private information to be secret regardless of the computational capabilities of a potential eavesdropper [1]. Secret-key agreement is a promising method to achieve this goal, whereby the sender and receiver generate a secret key before communication takes place. Maurer [2] and Ahlswede and Csiszár [3] independently developed the information-theoretic model for such a protocol, whereby Alice and Bob use pre-existing correlations, along with a public insecure channel, to generate a secret key. Devetak and Winter [4] considered the quantum counterpart and addressed key distillation from a shared quantum state. In practice, quantum key distribution (QKD) is the most mature application of quantum information theory [5, 6]. A QKD protocol aims to distribute a secret symmetric key between authorized partners, with no assumption regarding the channel but the laws of quantum mechanics. The key can later be used to communicate using classical encryption schemes, such as the one-time pad (OTP). Information-theoretic security is then guaranteed if and only if the entropy of the key string is at least as large as the message length [7]. Classical channel coding with key assistance, *i.e.*, given a pre-shared key, is studied, *e.g.*, in [8, 9].

In some noise models, communication can also be secured without key assistance. The broadcast channel with confidential messages is a network setting that involves transmission of information to two users, such that part of the information should be accessible for both users, while the other part is only intended for one of them. In the classical model, the sender transmits a sequence X^n over a memoryless broadcast channel, such that the output sequences Y^n and Z^n are decoded by two independent receivers. The transmission encodes two types of messages, a common message sent to both receivers and a private message sent to Receiver Y, while eavesdropped by Receiver Z. The broadcast channel with layered secrecy generalizes the model with confidential messages [10–12]. The model describes a network in which multiple users have different credentials to access confidential information. For example, consider a WiFi network of an agency, in which a user is allowed to receive files up to a certain security clearance, but should be kept ignorant of classified files that require a higher security level [12]. The agency can set the channel quality on a clearance basis by assigning more communication resources to users with a higher security rank. In some models, the layered-secrecy structure allows the provision of secrecy in hindsight, deferring the decisions as to which bits are secret to a later stage [13]. A recent overview of information security can be found in [14].

The broadcast channel with confidential messages can be viewed as a generalization of the wiretap channel. Devetak [15] and Cai *et al.* [16] addressed the quantum wiretap channel without key assistance and established a regularized characterization of the secrecy capacity. Connections to the coherent information were drawn in [4]. Hsieh *et al.* [17] and Wilde [18] presented a regularized formula for the secret-key-assisted quantum wiretap channel. Quantum state masking was recently considered in [19]. Key distillation is further considered in [20, 21]. Quantum broadcast channels were studied in various settings as well, *e.g.*, [22–24].

Optical communication forms the backbone of the Internet [25–27]. An optical communication system consists of a modulated source of photons, the optical channel, and an optical detector. For a single-mode bosonic broadcast channel, the channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the outputs are associated with operators $\hat{b}$ and $\hat{e}$. The annihilation operators correspond to the transmitter (Alice), the legitimate receiver of the common and confidential information (Bob), and the receiver that eavedrops on the confidential information (Eve), respectively. The input-output relation of the bosonic broadcast channel is given by

$$\hat{b} = \sqrt{\eta}\,\hat{a} + \sqrt{1-\eta}\,\hat{c} \tag{1}$$

$$\hat{e} = \sqrt{1-\eta}\,\hat{a} - \sqrt{\eta}\,\hat{c} \tag{2}$$

978-1-6654-0312-2/21/$31.00 ©2021 IEEE
Authorized licensed use limited to: Georgia Institute of Technology. Downloaded on January 02,2022 at 20:39:21 UTC from IEEE Xplore. Restrictions apply.

where $\hat{c}$ is associated with the environment noise and the parameter η is the transmissivity, $0 \leq \eta \leq 1$, which captures, for instance, the absorption length of the optical fiber [28]. The relation above corresponds to a beam splitter, as illustrated in Figure 1. The bosonic channel can be viewed as the quantum counterpart of the classical channel with additive white Gaussian noise (AWGN), which is a well-known model in classical communications. As the bosonic broadcast channel, from A to BE (jointly), is isometric, it does not model the distortion introduced by the communication medium [29]. Instead, the bosonic broadcast channel models the de-modulation process at the destination location, where the optical signal is converted into two signals for two independent users by a beam splitter. In a pure-loss bosonic channel, the noise mode $\hat{c}$ is in the vacuum state. The channel is called 'pure-loss' since the marginal channels, from A to B, and from A to E, are non-reversible and involve loss of photons in favor of the other receiver.

In this paper, we study secret-sharing building blocks that are based on quantum broadcast communication. In particular, we determine the confidential capacity region of the pure-loss bosonic broadcast channel with shared key assistance, under the assumption of the long-standing minimum output-entropy conjecture. The achievability proof is based on rate-splitting, combining the "superposition coding" strategy with the OTP cypher using the shared key. The converse proof relies on the long-standing minimum output entropy conjecture, which is known to hold in special cases [30]. Without key assistance, confidential transmission is only possible if Bob's channel has a higher transmissivity than Eve's channel, *i.e.*, $\eta > \frac{1}{2}$. Otherwise, if Bob's channel is noisier than Eve's, *i.e.*, $\eta < \frac{1}{2}$, then confidentiality solely relies on the key-assisted encryption of the OTP. Next, we address key agreement for the distillation and distribution of two keys. The public key is distributed between Alice, Bob, and Eve, while the confidential key is only meant for Alice and Bob, and must be hidden from Eve. We obtain a regularized formula for the key-agreement capacity region for the distillation of public and secret keys. We then consider quantum layered secrecy, whereby Alice communicates with three receivers, Bob, Eve 1, and Eve 2. The information consists of different security layers. We derive a regularized formula for the layered-secrecy capacity region of the degraded quantum broadcast channel and an achievable region for the pure-loss bosonic broadcast channel. The full version of this paper with detailed proofs can be found in [31].

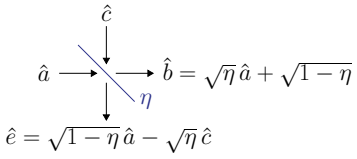

Fig. 1. The beam splitter relation of the single-mode bosonic broadcast channel.

II. Definitions

A. Notation and Channel Model

We use the following notation conventions. Script letters $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ are used for finite sets, X, Y, Z for classical random variables. The distribution of X is specified by a probability mass function (pmf) $p_X(x)$ over $\mathcal{X}$. In the continuous case, we use the the probability density function (pdf) $f_X(x)$. We write $X \sim \mathcal{N}_{\mathbb{R}}(\mu, \sigma^2)$ to indicate that X is a real-valued Gaussian variable, with $f_X(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/2\sigma^2}$, and $Z \sim \mathcal{N}_{\mathbb{C}}(\mu, \sigma^2)$ for a complex-valued Gaussian variable with $f_Z(z) = \frac{1}{2\pi\sigma^2} e^{-|z-\mu|^2/2\sigma^2}$. The state of a quantum system A is a density operator ρ on the Hilbert space $\mathcal{H}_A$. Define the quantum entropy, conditional entropy, and mutual information as $H(A)_\rho \triangleq -\mathrm{Tr}[\rho_A \log(\rho_A)]$, $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$, and $I(A;B)_\rho = H(A)_\rho + H(B)_\rho - H(AB)_\rho$, respectively. For a continuous-variable bosonic system, corresponding to an electromagnetic field, the Fock basis, vacuum state $|0\rangle$, annihilation operator $\hat{a}$, coherent state $|\alpha\rangle$, and thermal state, are defined as in [32].

A quantum broadcast channel is a linear, completely positive, trace-preserving map $\mathcal{L}_{A\to BE}$, mapping a quantum state at the sender to a quantum state at two receivers. Assume the channel is memoryless, *i.e.*, $\mathcal{L}_{A^n\to B^nE^n} \equiv \mathcal{L}^{\otimes n}_{A\to BE}$. The marginal channels are denoted by $\mathcal{L}^{(1)}_{A\to B}$ and $\mathcal{L}^{(2)}_{A\to E}$. The transmitter, Receiver 1, and Receiver 2 are often referred to as Alice, Bob, and Eve, respectively. A quantum broadcast channel $\mathcal{L}_{A\to BE}$ is called *degraded* if there exists a degrading channel $\mathcal{D}_{B\to E}$ such that $\mathcal{L}^{(2)}_{A\to E} \equiv \mathcal{D}_{B\to E} \circ \mathcal{L}^{(1)}_{A\to B}$. Intuitively, this means that Eve receives a noisier signal than Bob. A broadcast channel is called *reversely degraded* if $\mathcal{L}^{(1)}_{A\to B}$ is degraded with respect to $\mathcal{L}^{(2)}_{A\to E}$. The bosonic broadcast channel is degraded if $\eta > \frac{1}{2}$, and reversely degraded if $\eta \leq \frac{1}{2}$. In the former case, the degrading channel is a beam splitter with transmissivity $\eta' = \frac{1-\eta}{\eta}$.

B. Confidential Coding with and without Key Assistance

We define a confidential code with and without shared key assistance to transmit classical information over the broadcast channel. A common message is sent to both receivers, Bob and Eve, at a rate R_0, and a confidential message is sent to Bob at a rate R_1, while eavesdropped by Eve. The secret key consists of nR_K random bits, where R_K is a fixed key rate.

Definition 1. A $(2^{nR_0}, 2^{nR_1}, n)$ classical code for the quantum broadcast channel $\mathcal{L}_{A\to BE}$ with confidential messages and key assistance consists of the following: two message index sets $[1 : 2^{nR_0}]$ and $[1 : 2^{nR_1}]$, and a key index set $[1 : 2^{nR_K}]$; a collection of encoding maps $\mathcal{F}_{A^n|k}$ from the product set $[1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$ to the input Hilbert space $\mathcal{H}_{A^n}$, for $k \in [1 : 2^{nR_K}]$; and decoding POVMs, $\{\Gamma^{m_0,m_1}_{B^n|k}\}$, $k \in [1 : 2^{nR_K}]$, for Bob, and $\{\Xi^{m_0}_{E^n}\}$ for Eve.

The communication scheme is depicted in Figure 2. The sender Alice has the system A^n, and the receivers Bob and Eve have B^n and E^n, respectively. A key k is drawn from $[1 : 2^{nR_K}]$ uniformly at random, and shared between Alice and Bob. Alice chooses a common message $m_0 \in [1 : 2^{nR_0}]$

Authorized licensed use limited to: Georgia Institute of Technology. Downloaded on January 02,2022 at 20:39:21 UTC from IEEE Xplore. Restrictions apply.

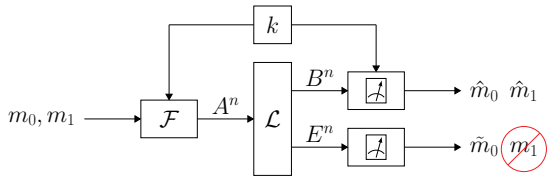

Fig. 2. The quantum broadcast channel with confidential messages and key assistance.

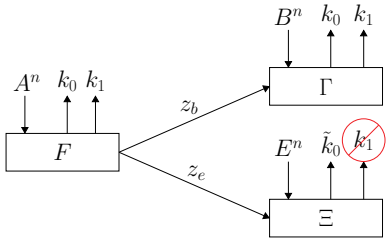

Fig. 3. Public and secret key agreement between three terminals.

which is intended for both users and a confidential message $m_1 \in [1 : 2^{nR_1}]$ for Bob, both uniformly at random. She encodes the messages by applying the encoding map $\mathcal{F}_{A^n|k}$, resulting in an input state $\rho_{A^n}^{m_0,m_1,k} = \mathcal{F}_{A^n|k}(m_0, m_1)$, and transmits the system A^n over n channel uses of $\mathcal{L}_{A\to BE}$. Hence, the output state is $\rho_{B^nE^n}^{m_0,m_1,k} = \mathcal{L}^{\otimes n}(\rho_{A^n}^{m_0,m_1,k})$. Eve receives the channel output system E^n, and performs the measurement $\{\Xi_{E^n}^{m_0}\}$, from which she obtains an estimate of the common message $\widetilde{m}_0$. Bob uses the key and performs $\{\Gamma_{B^n|k}^{m_0,m_1}\}$ on the output system B^n in order to find an estimate $(\hat{m}_0, \hat{m}_1)$.

The code performance is measured in terms of the probability of decoding error and the amount of confidential information that is leaked to Eve. The conditional probability of error of the code, given that the message pair (m_0, m_1) was sent, is given by

$$P_{e|m_0,m_1}^{(n)}(\mathcal{F}, \Gamma, \Xi) = 1 - \frac{1}{2^{nR_K}} \sum_{k=1}^{2^{nR_K}} \mathrm{Tr}[(\Gamma_{B^n|k}^{m_0,m_1} \otimes \Xi_{E^n}^{m_0}) \rho_{B^nE^n}^{m_0,m_1,k}]. \quad (3)$$

The confidential message m_1 needs to remain secret from Eve. Thereby, the leakage rate of the code $(\mathcal{F}, \Gamma, \Xi)$ is defined as

$$s^{(n)}(\mathcal{F}) \triangleq I(M_1; E^n|M_0)_\rho, \quad (4)$$

where M_1 is uniformly distributed over $[1 : 2^{nR_1}]$.

A $(2^{nR_0}, 2^{nR_1}, n, \varepsilon, \delta)$ confidential code satisfies $\frac{1}{2^{n(R_0+R_1)}} \sum_{m_0,m_1} P_{e|m_0,m_1}^{(n)}(\mathcal{F}, \Gamma, \Xi) \le \varepsilon$ and $s^{(n)}(\mathcal{F}) \le \delta$. A rate pair (R_0, R_1) is achievable if for every $\varepsilon, \delta > 0$ and sufficiently large n, there exists a $(2^{nR_0}, 2^{nR_1}, n, \varepsilon, \delta)$ code with key assistance. The capacity region $\mathcal{C}_{\text{k-a}}(\mathcal{L})$ of the quantum broadcast channel with confidential messages and key assistance is defined as the set of achievable rate pairs.

Remark 1. Taking $R_0 = 0$, the model reduces to the quantum wiretap channel, where Eve is is viewed as a malicious party who is not part of the network. If $\mathcal{L}_{A\to BE}$ is isometric, then the secrecy capacity of the wiretap channel is also referred to as the *private capacity* of the main channel $\mathcal{L}_{A\to B}^{(1)}$ [15].

Remark 2. The condition in (4) is referred to as strong secrecy. The results can be extended to stronger security criteria using the methods in [33].

C. Conference Key Agreement

Consider the following source model. Suppose that Alice, Bob, and Eve share a product state $\omega_{ABE}^{\otimes n}$. We define a code for the distillation of two keys using their access to this state, by local operations and one-way classical communication. A public key is to be shared with both receivers, Bob and Eve, at a rate R_0, and a secret key is sent to Bob at a rate R_1.

Definition 2. A key-agreement code for the distillation of public and secret keys consists of the following: two index sets $[1 : 2^{nR_0}]$ and $[1 : 2^{nR_1}]$, corresponding to the public key for both users and the secret key of Bob, respectively; and three POVMs, $\{F_{A^n}^{k_0,k_1,z_b,z_e}\}$, $\{\Gamma_{B^n|z_b}^{k_0,k_1}\}$, and $\{\Xi_{E^n|z_e}^{k_0}\}$.

The key-agreement protocol is depicted in Figure 3. Alice, Bob, and Eve share $\omega_{ABE}^{\otimes n}$. Alice performs the measurement $\{F_{A^n}^{k_0,k_1,z_b,z_e}\}$, and sends the measurement outcomes z_b and z_e to Bob and Eve, respectively, through a public channel. Upon receiving z_b and z_e, Bob and Eve perform their respective measurements. From the measurement outcomes, Alice obtains (K_0, K_1), Bob $(\hat{K}_0, \hat{K}_1)$, and Eve $\widetilde{K}_0$.

The performance of the code is based on the probability of distillation error, $P_e^{(n)}(F, \Gamma, \Xi) = \Pr\big(\widetilde{K}_0 \neq K_0 \text{ or } (\hat{K}_0, \hat{K}_1) \neq (K_0, K_1)\big)$, and the secrecy leakage. The keys should not be retrieved from the public channel communication, and K_1 needs to remain secret from Eve as well. Thereby, we define the leakage rates, $s_0^{(n)}(F) \triangleq I(Z_b, Z_e; K_0)$ and $s_1^{(n)}(F) \triangleq I(Z_b, Z_e, E^n; K_1)_\rho$. A key-rate pair (R_0, R_1) is achievable if for every $\alpha, \varepsilon, \delta > 0$ and large n, there exists a key-agreement code such that $\frac{1}{n} H(K_j) \ge R_j - \alpha$, $P_e^{(n)}(F, \Gamma, \Xi) \le \varepsilon$, and $s_j^{(n)}(F) \le \delta$, for $j = 0, 1$. The key-agreement capacity region $\mathcal{K}(\omega_{ABC})$ is defined as the set of achievable key-rate pairs (R_0, R_1).

Remark 3. If one removes the public key, the model reduces to the single-user key-agreement setting in [4].

III. Main Results — Confidential Communication with a Secret Key

Consider communication of a common message m_0 and a confidential message m_1 over a broadcast channel $\mathcal{L}_{A\to BE}$ with key assistance, as described in Subsection II-B and illustrated in Figure 2. If the broadcast channel $\mathcal{L}_{A\to BE}$ is reversely degraded, *i.e.*, Bob has a noisier channel than Eve, then secure communication requires that the private rate is zero. However, if Alice and Bob are provided with a secret key, then a positive private rate can be achieved.

We begin with the finite-dimensional case. We give a regularized capacity formula for the quantum broadcast channel

Authorized licensed use limited to: Georgia Institute of Technology. Downloaded on January 02,2022 at 20:39:21 UTC from IEEE Xplore. Restrictions apply.

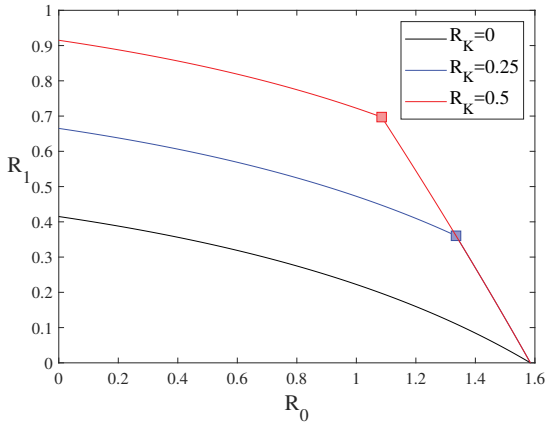

Fig. 4. The capacity region of the pure-loss bosonic broadcast channel with confidential messages and key assistance, given the transmissivity $\eta = 0.6$, and input constraint $N_A = 5$. The black, blue, and red lines correspond to the key rates $R_K = 0$, $R_K = 0.25$, and $R_K = 0.5$, respectively. The squares mark the phase transition ("breaking point") in each region.

with confidential messages and key assistance. Consider the broadcast channel $\mathcal{L}_{A\to BE}$ and define the rate region

$$\mathcal{R}_{\text{k-a}}(\mathcal{L}, R_K) = \bigcup_{p_{T,X},\, \varphi_A^{t,x}} \left\{ \begin{array}{l} (R_0, R_1) \,:\, R_0 \leq \min\left(I(T;B)_\rho,\, I(T;E)_\rho\right) \\ R_1 \leq [I(X;B|T)_\rho - I(X;E|T)_\rho]_+ + R_K \\ R_1 \leq I(X;B|T)_\rho \end{array} \right\} \tag{5}$$

where $[x]_+ = \max(x, 0)$, and the union is over the distribution $p_{T,X}$ of two classical auxiliary random variables and collections of quantum states $\{\varphi_A^{t,x}\}$, with $\rho_{BE}^{t,x} \equiv \mathcal{L}(\varphi_A^{t,x})$, $|\mathcal{T}| \leq |\mathcal{H}_A|^4 + 3$ and $|\mathcal{X}| \leq (|\mathcal{H}_A|^4 + 3)(|\mathcal{H}_A|^4 + 2)$. The characterization of the key-assisted capacity region is given in the theorem below.

Theorem 1. The capacity region of a quantum broadcast channel $\mathcal{L}_{A\to BE}$ with confidential messages and key assistance in finite dimensions is given by

$$\mathcal{C}_{\text{k-a}}(\mathcal{L}, R_K) = \bigcup_{n=1}^{\infty} \frac{1}{n} \mathcal{R}_{\text{k-a}}(\mathcal{L}^{\otimes n}, nR_K).$$

By taking a zero key rate, *i.e.*, $R_K = 0$, we recover the unassisted capacity region due to Salek *et al.* [23]. The proof of Theorem 1 is given in [31] (see Appendices A-B). To show the direct part, we use rate-splitting between one-time pad coding and the unassisted confidential code, similar to [8]. That is, the private rate is decomposed as $R_1 = R_{1\text{k}} + R_{1\text{c}}$, where the rates $R_{1\text{k}}$ and $R_{1\text{c}}$ correspond to the key-assisted encryption and the unassisted confidential code, respectively. This requires $R_{1\text{c}} \leq [I(X;B|T)_\rho - I(X;E|T)_\rho]_+$. Thus, if the quantum broadcast channel is reversely degraded, then $R_{1\text{c}} = 0$ and the confidentiality relies solely on the one-time pad cypher.

Next, we give our main result for the pure-loss bosonic broadcast channel. We determine the capacity region exactly, assuming that the minimum output-entropy conjecture holds. This long-standing conjecure is known to hold in special cases [30]. Let $g(N)$ denote the thermal state entropy, *i.e.*, $g(N) = (N+1)\log(N+1) - N\log(N)$ if $N > 0$, and $g(0) = 0$, where N is the mean photon number.

Conjecture 1. Given a pure-loss bosonic channel, if $H(A^n)_\rho = ng(N_A)$, then $H(B^n)_\rho \geq ng(\eta N_A)$.

Theorem 2. Assume that Conjecture 1 holds. Then, the capacity region of the pure-loss bosonic broadcast channel with confidential messages is as follows. If $\eta \geq \frac{1}{2}$, then

$$\mathcal{C}(\mathcal{L}_{\text{pure-loss}}) = \bigcup_{0\leq\beta\leq 1} \left\{ \begin{array}{l} (R_0, R_1) \,:\, R_0 \leq g((1-\eta)N_A) - g((1-\eta)\beta N_A) \\ R_1 \leq g(\eta\beta N_A) - g((1-\eta)\beta N_A) + R_K \\ R_1 \leq g(\eta\beta N_A) \end{array} \right\}.$$

Otherwise, if $\eta < \frac{1}{2}$,

$$\mathcal{C}(\mathcal{L}_{\text{pure-loss}}) = \bigcup_{0\leq\beta\leq 1} \left\{ \begin{array}{l} (R_0, R_1) \,:\, R_0 \leq g((1-\eta)N_A) - g((1-\eta)\beta N_A) \\ R_1 \leq \min\left(g(\eta\beta N_A),\, R_K\right) \end{array} \right\}.$$

The capacity region of the pure-loss bosonic broadcast channel is depicted in Figure 4 for different key rates. The squares mark a transition ("breaking point") in each region. For low common rates, the shared key is fully used to enhance the communication rates, whereas for higher rates, the key is only partially used. The breaking point corresponds to β_0 such that $g((1-\eta)\beta_0 N_A) = R_K$. The technical challenge is in the converse proof, which requires the conjecture. Achievability is interpreted as a "superposition coding scheme", which consists of cloud centers $t^n(m_0)$ and satellites $x^n(m_0, m_1) = t^n(m_0) + q^n(m_0, m_1)$. In order to ensure that Eve can recover the cloud center, but not the satellite, the cloud vector $q^n(m_0, m_{1,c})$ is chosen at random from a bin that consists of $2^{n[g((1-\eta)\beta N_A)+\delta]}$ sequences.

Authorized licensed use limited to: Georgia Institute of Technology. Downloaded on January 02,2022 at 20:39:21 UTC from IEEE Xplore. Restrictions apply.

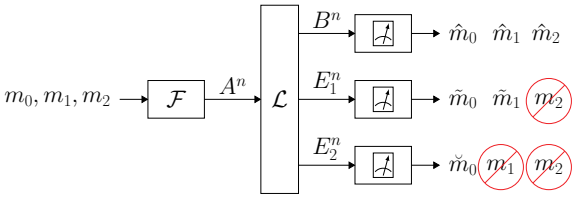

Fig. 5. The quantum broadcast channel with layered secrecy.

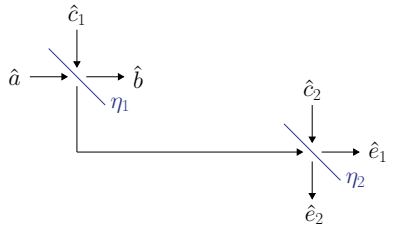

Fig. 6. The bosonic broadcast channel with layered secrecy.

IV. Main Results – Key Agreement

Consider the distillation of a public key and a secret key between Alice, Bob, and Eve, using a correlated state $\omega_{ABE}^{\otimes n}$, as described in Subsection II-C. We characterize the key-agreement capacity region for the case where A, B, and E have finite dimensions. Define a key-rate region,

$$\mathsf{K}(\omega_{ABE}) = \bigcup_{\Lambda_A,\, p_{T_0,T_1|X}} \left\{ \begin{array}{l} (R_0, R_1) \,:\, R_0 \leq \min\left(I(T_0;B)_\omega,\, I(T_0;E)_\omega\right) \\ R_1 \leq [I(X;B|T_0,T_1)_\omega - I(X;E|T_0,T_1)_\omega]_+ \end{array} \right\} \quad (6)$$

where the union is over the POVM $\Lambda_A = \{\Lambda_A^x\}_{x\in\mathcal{X}}$ and distributions $p_{T_0,T_1|X}$, with $\omega_{BE}^{t_0,t_1,x} \equiv \mathrm{Tr}_A\left((\Lambda_A^x \otimes \mathbb{1} \otimes \mathbb{1})\omega_{ABE}\right)$. The key-agreement theorem is given below.

Theorem 3. The key-agreement capacity region for the distillation of a public key and a secret key from ω_{ABE} in finite dimensions is given by

$$\mathcal{K}(\omega_{ABC}) = \lim_{n\to\infty} \frac{1}{n} \mathsf{K}(\omega_{ABC}^{\otimes n}).$$

The proof of Theorem 3 is given in [31]. The auxiliary variable T_1 only emerges in single-letter special cases, such as a classical channel. Next, we observe the following relation with the broadcast channel with confidential messages.

Corollary 4. For a degraded broadcast channel,

$$\mathcal{C}(\mathcal{L}) = \bigcup_{\omega_{ABE}\,:\,\omega_{BE}=\mathcal{L}_{A\to BE}(\omega_A)} \mathcal{K}(\omega_{ABC}).$$

In particular, the key-agreement capacity region for thermal states that are associated with a pure-loss bosonic channel is a subset of the confidential capacity region in Theorem 2.

V. Layered Secrecy

The quantum broadcast channel with layered generalizes the model with confidential messages. Consider a channel $\mathcal{L}_{A\to BE_1E_2}$ with three receivers, Bob, Eve 1, and Eve 2. As illustrated in Figure 5, Alice sends three messages. The common message m_0 is intended for all three receivers. In the next layer, the confidential message m_1 is decoded by Bob and Eve 1 but hidden from Eve 2. The confidential message m_2 is decoded by Bob, while remaining secret from Eve 1 and Eve 2. It is assumed that the broadcast channel is degraded, *i.e.*, there exist degrading channels $\mathcal{D}_{B\to E_1}^{(1)}$ and $\mathcal{D}_{E_1\to E_2}^{(2)}$.

A layered-secrecy code is defined such that a common message is sent at a rate R_0, and two confidential messages at rates R_1, R_2. Alice chooses a common message M_0 for all users, a layer-1 confidential message M_1 for Bob and Eve 1, and a layer-2 message M_2 for Bob. She encodes the messages and transmits A^n over the channel. Bob, Eve 1, and Eve 2 receive B^n, E_1^n, and E_2^n, and measure their estimates, $(\hat{M}_0, \hat{M}_1, \hat{M}_2)$, $(\tilde{M}_0, \tilde{M}_1)$, and $\check{M}_0$, respectively. The probability of error is defined accordingly, and the secrecy rates are $s_1^{(n)}(\mathcal{F}) \triangleq I(M_1; E_2^n|M_0)_\rho$ and $s_2^{(n)}(\mathcal{F}) \triangleq I(M_2; E_1^n, E_2^n|M_0)_\rho$. The layered-secrecy capacity region $\mathcal{C}_{\mathrm{LS}}(\mathcal{L})$ is defined in a similar manner as in Subsection II-B. Our main results on layered secrecy are given below. Define

$$\mathcal{R}_{\mathrm{LS}}(\mathcal{L}) = \bigcup_{p_{X_0,X_1,X_2},\,\varphi_A^{x_0,x_1,x_2}} \left\{ \begin{array}{l} (R_0, R_1, R_2) \,:\, R_0 \leq I(X_0;E_2)_\rho \\ R_1 \leq [I(X_1;E_1|X_0)_\rho - I(X_1;E_2|X_0)_\rho]_+ \\ R_2 \leq [I(X_2;B|X_0,X_1)_\rho - I(X_2;E_1E_2|X_0,X_1)_\rho]_+ \end{array} \right\}. \quad (7)$$

Theorem 5. The layered-secrecy capacity region of the quantum degraded broadcast channel $\mathcal{L}_{A\to BE_1E_2}$ in finite dimensions is given by

$$\mathcal{C}_{\mathrm{LS}}(\mathcal{L}) = \bigcup_{n=1}^{\infty} \frac{1}{n} \mathcal{R}_{\mathrm{LS}}(\mathcal{L}^{\otimes n}).$$

Theorem 6. A layered-secrecy rate tuple (R_0, R_1, R_2) is achievable over the pure-loss bosonic broadcast channel if

$$\begin{aligned} R_0 &\leq g\big((1-\eta_1)(1-\eta_2)N_A\big) \\ &\quad - g\big((\beta_1+\beta_2)(1-\eta_1)(1-\eta_2)N_A\big), \\ R_1 &\leq g\big((\beta_1+\beta_2)\eta_2(1-\eta_1)N_A\big) - g\big(\beta_2\eta_2(1-\eta_1)N_A\big) \\ &\quad - \big[g\big((\beta_1+\beta_2)(1-\eta_2)(1-\eta_1)N_A\big) \\ &\quad - g\big(\beta_2(1-\eta_2)(1-\eta_1)N_A\big)\big], \\ R_2 &\leq g\big(\eta_1\beta_2 N_A\big) - g\big((1-\eta_1)\beta_2 N_A\big), \end{aligned} \quad (8)$$

for some β_1, $\beta_2 \geq 0$, such that $\beta_1 + \beta_2 \leq 1$.

The proofs of Theorem 5 and Theorem 6 are given in [31].

VI. Acknowledgments

Pereg and Ferrara were supported by the German BMBF, Grant n. 16KIS0856; Bloch by the American NSF, Grant n. 1955401. Pereg was also supported by the Israel CHE Fellowship for Quantum Science and Technology.

Authorized licensed use limited to: Georgia Institute of Technology. Downloaded on January 02,2022 at 20:39:21 UTC from IEEE Xplore. Restrictions apply.

REFERENCES

[1] M. R. Bloch and J. Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[2] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory*, 39 (3):733–742, 1993.

[3] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography. i. secret sharing. *IEEE Trans. Inf. Theory*, 39(4):1121–1132, 1993.

[4] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proc. Royal Society A: Math., Phys. and Engin. Sciences*, 461(2053):207–235, 2005.

[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, and C. Ottaviani. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4): 1012–1236, 2020.

[6] M. Christandl, R. Ferrara, and K. Horodecki. Upper bounds on device-independent quantum key distribution. *Phys. Rev. Lett.*, 126(16):160501, 2021.

[7] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28(4):656–715, 1949.

[8] W. Kang and N. Liu. Wiretap channel with shared key. In *Proc. IEEE Inf. Theory Workshop(ITW'2010)*, pages 1–5, Dublin, Ireland, 2010.

[9] R. F. Schaefer, A. Khisti, and H. V. Poor. Secure broadcasting using independent secret keys. *IEEE Trans. Commmun.*, 66(2):644–661, 2018.

[10] H. D. Ly, T. Liu, and Y. Blankenship. Security embedding codes. *IEEE Trans. Inf. Foren. Secur.*, 7(1):148–159, 2012.

[11] S. Zou, Y. Liang, L. Lai, and S. Shamai. An information theoretic approach to secret sharing. *IEEE Trans. Inf. Theory*, 61(6):3121–3136, 2015.

[12] S. Zou, Y. Liang, L. Lai, H. V. Poor, and S. Shamai. Broadcast networks with layered decoding and layered secrecy: Theory and applications. *Proceedings of the IEEE*, 103(10):1841–1856, 2015.

[13] M. Tahmasbi, M. R. Bloch, and A. Yener. Learning an adversarys actions for secret communication. *IEEE Trans. Inf. Theory*, 66(3):1607–1624, 2020.

[14] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer. An overview of information-theoretic security and privacy: Metrics, limits and applications. *IEEE J. Selected Areas Info. Th.*, 2(1):5–22, 2021.

[15] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inf. Theory*, 51(1):44–55, 2005.

[16] N. Cai, A. Winter, and R. W. Yeung. Quantum privacy and quantum wiretap channels. *Probl. Info. Transm.*, 40 (4):318–336, 2004.

[17] M. H. Hsieh, Z. Luo, and T. Brun. Secret-key-assisted private classical communication capacity over quantum channels. *Physical Review A*, 78(4):042306, 2008.

[18] M. M. Wilde. Comment on secret-key-assisted private classical communication capacity over quantum channels. *Phys. Rev. A*, 83(4):046303, 2011.

[19] U. Pereg, C. Deppe, and H. Boche. Quantum channel state masking. *IEEE Trans. Inf. Theory*, 67(4):2245–2268, 2021.

[20] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.*, 102(5):050503, 2009.

[21] M. Takeoka, K. P. Seshadreesan, and M. M. Wilde. Unconstrained capacities of quantum key distribution and entanglement distillation for pure-loss bosonic broadcast channels. *Phys. Rev. Lett.*, 119(15):150501, 2017.

[22] J. Yard, P. Hayden, and I. Devetak. Quantum broadcast channels. *IEEE Trans. Inf. Theory*, 57(10):7147–7162, Oct 2011.

[23] F. Salek, M. Hsieh, and J. R. Fonollosa. Publicness, privacy and confidentiality in the single-serving quantum broadcast channel. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2019)*, pages 1712–1716, 2019.

[24] E. Anderson, S. Guha, and B. Bash. Fundamental limits of bosonic broadcast channels. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2021)*, 2021.

[25] B. R. Bardhan and J. H. Shapiro. Ultimate capacity of a linear time-invariant bosonic channel. *Phys. Rev. A*, 93 (3):032342, 2016.

[26] U. Pereg. Bosonic dirty paper coding. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2021)*, July 2021.

[27] S. Kumar and M. J. Deen. *Fiber optic communications: fundamentals and applications*. John Wiley & Sons, 2014.

[28] J. Eisert and M. M. Wolf. Gaussian quantum channels. In *Quantum Inf. Cont. Variab. Atoms and Light. Preprint is available in* `arXiv:quant-ph/0505151`, pages 23–42. World Scientific, 2007.

[29] J. H. Shapiro. The quantum theory of optical communications. *IEEE J. Selected Topics Quantum Electr.*, 15(6): 1547–1569, 2009.

[30] G. De Palma. New lower bounds to the output entropy of multi-mode quantum gaussian channels. *IEEE Trans. Inf. Theory*, 65(9):5959–5968, Sep. 2019.

[31] U. Pereg, R. Ferrara, and M. R. Bloch. Key assistance, key agreement, and layered secrecy for bosonic broadcast channels. `arXiv:2105.04033`, May 2021. URL `https://arxiv.org/pdf/2105.04033.pdf`.

[32] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012.

[33] J. M. Renes and R. Renner. Noisy channel coding via privacy amplification and information reconciliation. *IEEE Trans. Inf. Theory*, 57(11):7377–7385, 2011.

Authorized licensed use limited to: Georgia Institute of Technology. Downloaded on January 02,2022 at 20:39:21 UTC from IEEE Xplore. Restrictions apply.