

# Group Secret-Key Generation Using Algebraic Rings in Wireless Networks

Harshan Jagadeesh , Rohit Joshi , and Manish Rao

**Abstract**—It is well known that physical-layer Group Secret-Key (GSK) generation techniques allow multiple nodes of a wireless network to synthesize a common secret-key, which can be subsequently used to keep their group messages confidential. As one of its salient features, the wireless nodes involved in physical-layer GSK generation extract randomness from a subset of their wireless channels, referred as the common source of randomness (CSR). Unlike two-user key generation, in GSK generation, some nodes must act as *facilitators* by broadcasting quantized versions of the linear combinations of the channel realizations, so as to assist all the nodes to observe a CSR. However, we note that broadcasting linear combination of channel realizations incurs non-zero leakage of the CSR to an eavesdropper, and moreover, quantizing the linear combination also reduces the overall key-rate. Identifying these issues, we propose a practical GSK generation protocol, referred to as Algebraic Symmetrically Quantized GSK (A-SQGSK) protocol, in a network of three nodes, wherein due to quantization of symbols at the facilitator, the other two nodes also quantize their channel realizations, and use them appropriately over algebraic rings to generate the keys. First, we prove that the A-SQGSK protocol incurs zero leakage to an eavesdropper. Subsequently, on the CSR provided by the A-SQGSK protocol, we propose a consensus algorithm among the three nodes, called the Entropy-Maximization Error-Minimization (EM-EM) algorithm, which maximizes the entropy of the secret-key subject to an upper-bound on the mismatch-rate. We use extensive analysis and simulation results to lay out guidelines to jointly choose the parameters of the A-SQGSK protocol and the EM-EM algorithm.

**Index Terms**—Common source of randomness, group key generation, rings, security, wireless networks.

## I. INTRODUCTION

**G**IVEN the broadcast nature of wireless communication, it is well known that messages transmitted to an intended receiver can also be heard by eavesdroppers in the vicinity, thereby compromising the much needed *confidentiality* feature.

Manuscript received September 10, 2019; revised April 28, 2020 and August 31, 2020; accepted January 11, 2021. Date of publication January 25, 2021; date of current version March 10, 2021. This work was supported by the Indigenous 5G Test Bed project from the Department of Telecommunications, Ministry of Communications, New Delhi, India. This paper was presented in part at the IEEE International Symposium on Personal Indoor and Mobile Radio Communications 2019 Istanbul, Turkey, and in part at the IEEE International Conference on Signal Processing and Communications 2018, Bangalore, India. The review of this article was coordinated by Prof. H. Wang. (*Corresponding author: Harshan Jagadeesh.*)

Harshan Jagadeesh and Manish Rao are with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, Delhi 110016, India (e-mail: jharshan@gmail.com; manish.eee15@ee.iitd.ac.in).

Rohit Joshi is with the Bharti School of Telecommunication Technology, and Management, Indian Institute of Technology Delhi, New Delhi, Delhi 110016, India (e-mail: Rohit.Joshi@cse.iitd.ac.in).

Digital Object Identifier 10.1109/TVT.2021.3054031

A standard technique to circumvent this problem is to employ crypto-primitives at the higher-layer between the transmitter and the receiver, e.g., symmetric-key encryption or public-key encryption methods [1]. With symmetric-key techniques being favoured for application in low-cost wireless devices, the communicating parties need to possess a pre-shared secret-key to execute the crypto-primitives. While a plethora of crypto-techniques are well known for key-exchange mechanisms, the concept of physical-layer key generation techniques has also received traction in the wireless community as the communicating nodes can harvest shared-keys just by witnessing the randomness in their channel realizations [2]–[17]. Thus, this mode of key generation can provide additional layer of security other than the higher-layer crypto-primitives. In the context of physical-layer key generation, the wireless channel realizations are referred to as the Common Source of Randomness (CSR). While a number of contributions have been reported under physical-layer two-user key generation, its generalization to a network comprising more than two nodes have also been studied, under the framework of Group Secret-Key (GSK) generation techniques [18]–[27]. In such a framework, more than two nodes generate a common secret-key by observing the temporal variation of their wireless channels so that these secret-keys can be used to keep their group messages confidential when implementing broadcast and relaying strategies among the group members. Typical applications of GSK generation for broadcast, relaying and multi-cast communication include Device-to-Device communication in ad hoc networks, e.g., vehicular networks [17] and mobile networks.

Physical-layer GSK generation techniques can be broadly classified into two types: (i) pair-wise key based generation, wherein pairs of users in the network synthesize secret-keys using their wireless links, and subsequently distribute a GSK by using their pair-wise keys at the digital level [18], [19], [21], and (ii) GSK generation, wherein multiple nodes in the network first exchange a CSR, and then generate a GSK after executing a group consensus algorithm [20], [22]. While the former class of methods piggyback on the simplicity of two-user key generation protocols, such schemes expose the generated digital key to threats to a possible insider attack in the wireless network. In contrast, using the latter class of methods, it has been shown that manipulating the CSR by an insider is power-inefficient, and may also be detected by the neighboring nodes provided the detection algorithms are carefully designed [25]. Due to such advantages, we are interested in designing the latter class of GSK protocols.

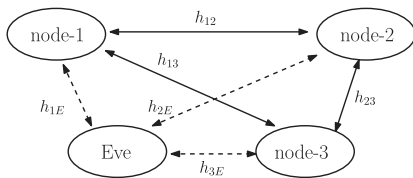


Fig. 1. Network model with three wireless nodes, which intend to generate a GSK in the presence of the passive eavesdropper, referred to as Eve. All the channels in the network are assumed to be statistically independent. First, the three nodes share a common source of randomness, and then synthesize a group secret-key using a group consensus algorithm.

### A. Motivation

In this section, we use the three-node network shown in Fig. 1 to illustrate the challenges involved in securely sharing a CSR among the nodes in the network. From Fig. 1, it is clear that the available channels in the network are  $h_{12}$ ,  $h_{13}$ , and  $h_{23}$ , where  $h_{jk}$  represents the complex baseband channel from node- $j$  to node- $k$ . Towards executing physical-layer GSK generation, the three nodes have to pick at least one of these channels as the CSR. Suppose that the channel  $h_{12}$  is the chosen CSR. With that choice, although node-1 and node-2 can witness this CSR by transmitting pilot symbol turn-by-turn within the coherence-time, node-3 cannot learn this channel during the pilot transmission phase, and therefore either node-1 or node-2 must act as *facilitator* to help node-3 in observing  $h_{12}$ . Assuming node-1 plays the role of facilitator, upon observing the channel realizations  $h_{12}$  and  $h_{13}$  in the pilot transmission phase, it must broadcast a function of  $h_{12}$  and  $h_{13}$ , denoted by  $g(h_{12}, h_{13}) \in \mathbb{C}$  such that  $h_{12}$  must be recovered by node-3, whereas an eavesdropper in the vicinity must not be able to recover  $h_{12}$  from the broadcast signal. However, from a practical viewpoint, since radio devices are designed to transmit baseband symbols from finite constellations, such as Quadrature-Amplitude-Modulation (QAM), Phase-Shift-Keying (PSK), etc, the broadcast signal  $g(h_{12}, h_{13})$  cannot be transmitted as an arbitrary complex number in an unquantized fashion. Although the facilitator can quantize  $g(h_{12}, h_{13})$  to binary sequences of large block-lengths and then map those bits to complex constellations to reduce the quantization error, such a strategy may not be applicable when the CSR has to be shared within a short coherence-block [27].

To address the above pointed issue in sharing the CSR, we consider a new framework of practical GSK generation, wherein the broadcast signal  $g(h_{12}, h_{13})$  is quantized directly to points in a complex constellation. As a result, the noise level of the CSR observed at node-3 will be different compared to that at node-1 and node-2. Identifying this disparity in the noise levels at the CSR observed at the three nodes, first, we propose a new method to share the CSR in the network model given in Fig. 1, and subsequently present consensus algorithms among the three nodes to synthesize a GSK when using the shared CSR.

### B. Contributions

We consider a three-user wireless network, as shown in Fig. 1, wherein the legitimate nodes, denoted by node-1, node-2 and node-3, are interested in witnessing a CSR so as to synthesize a

GSK in the presence of an eavesdropper, denoted by Eve. The CSR of interest in our model are the channel realizations of one of the links in the network. First, we identify that unlike the case of two-user key generation protocols, broadcasting pilot symbols one after the other within the coherence-time of the channels is not sufficient for the nodes to witness a CSR. As a result, one of the nodes, referred to as the facilitator, will have to transmit a function of the channel realizations observed by it in addition to broadcasting pilots. Assuming node-1 as the facilitator and  $h_{12}$  as the chosen CSR, we make the following two crucial observations with respect to Fig. 1: (i) although node-1 can broadcast the sum  $h_{12} + h_{13}$  to facilitate node-3 to witness  $h_{12}$ , this technique does not ensure zero leakage of the CSR to an external eavesdropper, and (ii) transmitting the complex number  $h_{12} + h_{13}$  (with infinite precision values) within a short coherence-block is challenging, and as a result, the facilitator is constrained to directly quantize  $h_{12} + h_{13}$  to points in a complex constellation before broadcasting them to the other nodes. Incorporating the above observations, in this paper, we make the following two-fold contributions:

*C1:* We propose a GSK protocol to exchange a CSR among the nodes in the network given in Fig. 1 such that (i) the channel realizations shared by the facilitator are quantized within the coherence-block thereby making the scheme amenable to implementation in practice, and importantly, (ii) the protocol incurs zero-leakage of the CSR to an external eavesdropper.

*C2:* On the CSR provided in *C1*, we propose a multi-level consensus algorithm, referred to as the EM-EM algorithm, among the three nodes to generate a GSK such that the entropy of the key is maximized subject to an upper bound on the mismatch rate. Given that the proposed multi-level consensus algorithm is closely coupled with the protocol used to exchange the CSR, we lay out design rules to jointly choose the parameters of the A-SQGSK protocol and the EM-EM algorithm as a function of underlying signal-to-noise-ratio and the required mismatch rate on the generated GSK.

Specific contributions of this work with respect to *C1* and *C2* are listed below:

Under *C1*, we propose a practical GSK protocol, referred to as Algebraic Symmetrically Quantized GSK (A-SQGSK), wherein due to the quantization of channel realizations at the facilitator, the other two nodes also quantize their channel realizations, and use them appropriately over algebraic rings to generate GSKs. Specifically, in this protocol, the facilitator, instead of quantizing the sum  $h_{12} + h_{13}$  directly, quantizes the channel realizations  $h_{12}$  and  $h_{13}$  individually and then adds them over an algebraic ring before transmitting the result to the other nodes. Meanwhile, the other nodes, also quantize their channel realizations and subsequently recover the CSR using the symbols transmitted by the facilitator through successive interference cancellation. We show that the proposed protocol incurs zero leakage to an external eavesdropper, and this important property is attributed to the algebraic nature of operations at the facilitator (See Section III-C).

Under *C2*, we highlight that the CSR observed using the A-SQGSK protocol takes values from a discrete constellation. We show that the underlying discrete constellation must be carefully

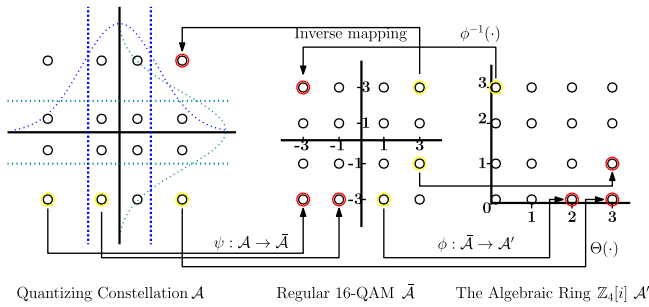


Fig. 2. Example for the three constellations used in the A-SQGSK protocol with  $m = 4$ : Constellation  $\mathcal{A}$  is used to quantize the channel realizations such that the quantized values are uniformly distributed. Constellation  $\mathcal{A}'$  is the ring  $\mathbb{Z}_2^{\frac{m}{2}}[i]$  used to compute linear combination of the quantized samples at the facilitator, whereas  $\tilde{\mathcal{A}}$  is used by the facilitator for broadcasting the linear combination of the CSR samples to node-2 and node-3.

chosen so that the three nodes must be able to derive a GSK such that (i) the key rate (the number of bits per sample) is maximized, (ii) the entropy of the generated key is maximized, and (iii) the mismatch rate between the keys at the three nodes must be bounded within a negligible number.

C2.1: In order to meet the above design criteria, it is straightforward to note that a consensus algorithm must be designed using the knowledge of the joint probability distribution function (PDF) on the CSR observed at the three nodes. However, given that the three-dimensional joint PDF is intractable, we propose relaxed criteria to design a consensus algorithm by making use of the two-dimensional joint PDF on the CSR at node-2 and node-3, which captures the worst-case link for group-key generation when node-1 is the facilitator and  $h_{12}$  is the channel realization for CSR (See Section IV).

C2.2: Given the number of levels for quantization and the knowledge of the two-dimensional distribution, we formulate a constrained optimization problem to maximize the key rate with strict constraints on the entropy and the mismatch rate of the generated keys. Towards solving the optimization problem, we propose an iterative algorithm, referred to as the Entropy-Maximization Error-Minimization (EM-EM) algorithm, which carefully introduces guard bands in  $\mathbb{R}^2$ , as shown in Fig. 4, to satisfy the underlying constraints. In the EM-EM algorithm, iterations mainly involve two blocks, namely: (i) the entropy block, which shifts the guard bands to achieve the constraint on entropy, and (ii) the error block, which prudently increases the width of each guard band to satisfy the constraint on mismatch rate. Unlike existing approaches on multi-level quantization, we show that the EM-EM algorithm guarantees secret-keys with entropy of  $b$ -bits per sample in consensus when using a  $2^b$ -level quantization. We show that the EM-EM algorithm outperforms multi-level quantization methods, which are optimized using the marginal distributions, and other traditional quantization methods, such as uniform quantization and Max-Lloyd quantization [28]. In summary, our algorithm can be applied on a wide range of joint distributions, and thus can serve as a software package to design multi-level quantizers for key generation (See Section V).

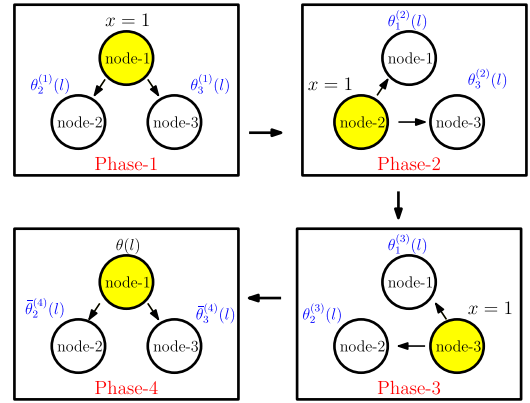


Fig. 3. Depiction of the four phases of the A-SQGSK protocol. In the first three phases, each node transmits a pilot symbol, whereas in the last phase, node-1, which acts as the facilitator, broadcasts a linear combination of its channels suitably quantized over the algebraic ring  $\mathbb{Z}_2^{\frac{m}{2}}[i]$ .

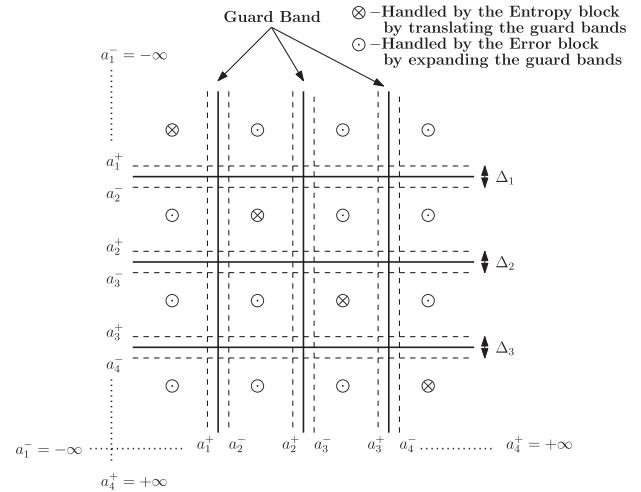


Fig. 4. Depiction of the proposed two-dimensional approach to solve multi-level quantization for key-generation. Unlike existing approaches, joint PDF is exploited to identify the placements and the widths of the guard bands.

C2.3: Using the proposed EM-EM algorithm on the CSR observed at node-2 and node-3, we show that the synthesized GSK exhibits maximum entropy of  $b$  bits per sample, for  $b \geq 1$ , provided the size of the discrete constellation is sufficiently large. We show that this behaviour with respect to the size of the discrete constellation is attributed to limited degrees of freedom in enlarging the guard bands when the constellation size is small. Through extensive simulation results, we recommend the following guidelines when using the proposed GSK generation method: (i) The discrete constellation  $\mathcal{A}$  chosen for quantization of the channel realizations in the A-SQGSK protocol must induce uniform distribution on the CSR at the individual nodes, (ii) After the algebraic operations during Phase 4, the facilitator must map the resultant symbols onto a regular QAM constellation before transmitting them to the other nodes, and (iii) the inputs to EM-EM algorithm must be the joint distribution of the CSR at node-2 and node-3, which constitute the worst-pair with reference to the CSR obtained from the channel realizations  $h_{12}$  (See Section VI).

TABLE I  
NOVELTY OF THE PROPOSED A-SQGSK PROTOCOL AND THE EM-EM ALGORITHM WITH RESPECT TO EXISTING CONTRIBUTIONS

Reference	Contributions on sharing the CSR	Limitation with respect to our work
[20], [22], [23]	Address algorithms to share the CSR among the nodes for GSK	Do not guarantee zero leakage to an eavesdropper as linear combination is computed over $\mathbb{C}$
[26]	A practical scheme to share the CSR is presented by us.	Unlike this work, the protocol in [26] leaks the CSR to an eavesdropper.
[27]	First version of A-SQGSK protocol is presented by us.	However, QAM constellations are used to quantize the channels thereby resulting in low entropy. Consensus algorithm in [27] is heuristic.
Reference	Contributions on consensus algorithms	Limitation with respect to our work
[28]	Max-Lloyd quantizer	Minimizes the distortion between input and quantized version. Not relevant to key generation.
[7]	Marginal distribution based equiprobable quantizer	Does not guarantee maximum entropy since the distribution of samples in consensus is different from marginal distribution
[2]	Two-level quantizer and consensus algorithm	Two-level quantizer using the mean of data set and consecutive excursion length. Multiple levels of quantization not explored.
[9]	Optimal guard band quantizer	Placement of guard bands to bound symbol-error-rate. Maximum entropy not guaranteed.
[10]	Vector quantization based multi-level quantizer	Handles temporally-correlated channel realizations. Specific to Gaussian distributions. In contrast, EM-EM algorithm is applicable on any joint distribution.

### C. Related Work

Physical-layer key generation between two radio devices is well studied starting from theory that focuses on fundamental limits [3], to testbed developments that showcase proof-of-concepts [5]. A wide range of contributions exist in this topic, wherein the specific choice of CSR [6], [8], [11], [12], [13], used to generate the keys depend on wireless platforms such as OFDM [14], multiple-input multiple-output (MIMO) systems [15], and fibre optical networks [16], to name a few.

In the rest of this section, we review the literature on GSK generation to highlight that none of the existing GSK generation protocols [18]–[24] together with the existing consensus algorithms [2]–[4], [7], [8], [10] have addressed the objectives of jointly achieving practicality, confidentiality, and maximum entropy in the GSK generation. As discussed in Section I, we are interested in the class of GSK generation protocols [20], [22], [23], wherein multiple nodes in the network first exchange a CSR, and then generate a GSK after executing a group consensus algorithm. These methods involve two phases: In the first phase (referred to as the protocol phase), nodes in the network need to securely exchange pilot symbols and their channel realizations such that all of them witness a CSR. In the second phase (referred to the consensus phase), all the nodes need to apply a consensus algorithm to synthesize a group-secret key on the CSR. With respect to the protocol phase, we note that [20], [22], [23] do not guarantee zero-leakage to an external eavesdropper, thereby compromising the confidentiality feature. Furthermore, with respect to the consensus phase, systematic algorithms that are customized to the distribution of the CSR have not been presented hitherto.

Under the class of consensus algorithms, [2] has proposed a two-level quantizer to derive secret bits in an unauthenticated channel. Subsequently, [3], [4] have proposed enhancements over the idea in [2] to maximize the entropy of the generated key with two-level quantizer. Further, [7], [8] have addressed scalar multi-level quantization schemes to generate more than

one bit per sample, whereas [9] has proposed methods to reduce the mismatch rate between the generated keys. Recently, [10] has also explored vector quantization methods to achieve consensus on channels with correlated variations over time. Although the above consensus algorithms are for two-user key generation, none of them maximize the entropy of the synthesized key, and are also not designed for the GSK setting.

In a nutshell, to fill the above mentioned gaps in the existing GSK protocols, we have proposed the A-SQGSK protocol and the EM-EM algorithm as listed in C1 and C2 of Section I-B. We highlight that this work is an extension of our earlier contributions in [26] and [27]. To emphasize the novelty, in Table I, we point out the differences between our work over existing contributions including that of [26] and [27].

### D. Notations

We use  $\mathbb{Z}$ ,  $\mathbb{Z}[i]$ ,  $\mathbb{N}$  and  $\mathbb{C}$  to denote the set of all integers, Gaussian integers, natural numbers and complex numbers, respectively, where  $i = \sqrt{-1}$ . A circularly symmetric complex Gaussian random variable with mean 0 and variance  $\sigma^2$  is represented as  $x \sim \mathcal{CN}(0, \sigma^2)$ . The set  $\{0, 1, 2, \dots, p-1\}$ , for some integer  $p > 1$ , is denoted by  $\mathbb{Z}_p$ . The term  $I(x; y)$  denotes the mutual information between two random variables  $x$  and  $y$ , and the term  $H(x)$  denotes the entropy of a discrete random variable  $x$ . Given two sets  $\mathcal{S}_1 \subset \mathbb{C}$  and  $\mathcal{S}_2 \subset \mathbb{C}$ , the term  $\mathcal{S}_1 \oplus \mathcal{S}_2 = \{s_1 + s_2 \mid s_1 \in \mathcal{S}_1, s_2 \in \mathcal{S}_2\}$  denotes their direct sum. We refer to the additive white Gaussian noise using its acronym AWGN. The notation  $|\mathcal{S}|$  represents the number of elements in the set  $\mathcal{S}$ . We use  $\text{Prob}(\cdot)$  to represent the regular probability operator. We use the notation  $[n]$  to represent the set of integers  $\{1, 2, \dots, n\}$ . Given a two-dimensional probability density function  $P(x, y)$  of continuous random variables  $X$  and  $Y$ , the probability that the pair lie in a given range is denoted by  $\int_{a_j^-}^{a_j^+} \int_{a_k^-}^{a_k^+} P(x, y) dx dy$ . In the special case of discrete random variables  $X$  and  $Y$ , the integral will collapse to summation of mass points in the given

interval as  $\sum_{a_j^-}^{a_j^+} \sum_{a_k^-}^{a_k^+} P(x, y)$ , where  $P(x, y)$  denotes the joint probability mass function  $P(X = x, Y = y)$ .

## II. SYSTEM MODEL FOR GSK GENERATION

As shown in Fig. 1, we consider a three-user wireless network comprising node-1, node-2 and node-3 along with an eavesdropper, denoted by Eve. The wireless channel between any two nodes in this network model is assumed to be frequency-flat and remain quasi-static for a block of four channel-uses. Specifically, we use a complex Gaussian random variable, denoted by  $h_{jk} \sim \mathcal{CN}(0, 1)$ , to represent the channel between node- $j$  and node- $k$ , for  $j \neq k$ . We assume that all the channels  $\{h_{jk} | j \neq k\}$  exhibit pair-wise reciprocity within the coherence-block, i.e.,  $h_{jk} = h_{kj}$ , and moreover, every pair of channels in  $\{h_{jk}\}$  are statistically independent. We also assume that the AWGN witnessed at all the nodes are distributed as  $\mathcal{CN}(0, \sigma^2)$ .

In this network model, the three nodes are interested in observing a subset of the channels  $\{h_{12}, h_{13}, h_{23}\}$  so as to synthesize a GSK. Henceforth, throughout the paper, we refer to this subset of channels as the CSR. Towards witnessing the chosen CSR, the three nodes follow the conventional approach of broadcasting pilot symbols turn-by-turn within each coherence-block. As a result, every node can learn the corresponding channels upon receiving the pilot symbols. Since pilot transmission does not help the three nodes to witness the CSR, one of the nodes, referred to as the facilitator, broadcasts a linear combination of its observed channels in order to assist all the nodes to acquire the CSR within the coherence-block. Gathering the CSR observed over several coherence-blocks, the three nodes subsequently apply an appropriate key generation algorithm to generate a GSK. To highlight the role of each coherence-block, we denote the channels using the coherence-block index  $l$  as  $\{h_{12}(l), h_{13}(l), h_{23}(l)\}$  for  $l = 1, 2, \dots, L$ , where  $L$  is the total number of coherence-blocks used to witness the CSR. In the following section, we present a GSK protocol wherein the three nodes choose  $\{h_{12}(l)\}$  for  $1 \leq l \leq L$  as the CSR. Since the objective of this work is to study the effects of quantization when generating a GSK, we choose  $\{h_{12}(l) | 1 \leq l \leq L\}$  to be CSR of interest throughout the paper.

### A. GSK Generation With no Quantization at the Facilitator

We present a detailed description of a GSK protocol [25] to exchange a CSR among the three nodes in the network shown in Fig. 1. We describe the four phases of the protocol for a given coherence-block  $l \in \{1, 2, \dots, L\}$ :

*Phase 1:* node-1 transmits a pilot symbol  $x = 1$ , which is used by node-2 and node-3 to estimate the channels  $h_{12}(l)$  and  $h_{13}(l)$ , respectively, as

$$\theta_2^{(1)}(l) = h_{12}(l) + e_2^{(1)}(l) \text{ and } \theta_3^{(1)}(l) = h_{13}(l) + e_3^{(1)}(l), \quad (1)$$

where  $e_2^{(1)}(l) \sim \mathcal{CN}(0, \gamma)$  and  $e_3^{(1)}(l) \sim \mathcal{CN}(0, \gamma)$  denote the channel estimation errors at node-2 and node-3, respectively. The superscripts denote the phase number in each coherence-block.

*Phase 2:* node-2 transmits a pilot symbol  $x = 1$ , which is used by node-1 and node-3 to estimate the channels  $h_{12}(l)$  and  $h_{23}(l)$ , respectively, as

$$\theta_1^{(2)}(l) = h_{12}(l) + e_1^{(2)}(l) \text{ and } \theta_3^{(2)}(l) = h_{23}(l) + e_3^{(2)}(l), \quad (2)$$

where  $e_1^{(2)}(l) \sim \mathcal{CN}(0, \gamma)$  and  $e_3^{(2)}(l) \sim \mathcal{CN}(0, \gamma)$  are the corresponding estimation errors.

*Phase 3:* node-3 transmits a pilot symbol  $x = 1$ , which is used by node-2 and node-1 to estimate the channels  $h_{23}(l)$  and  $h_{13}(l)$ , respectively, as

$$\theta_2^{(3)}(l) = h_{23}(l) + e_2^{(3)}(l) \text{ and } \theta_1^{(3)}(l) = h_{13}(l) + e_1^{(3)}(l), \quad (3)$$

where  $e_2^{(3)}(l) \sim \mathcal{CN}(0, \gamma)$  and  $e_1^{(3)}(l) \sim \mathcal{CN}(0, \gamma)$  are the corresponding estimation errors. We assume that all the nodes employ the same channel estimation algorithm, and as a result, we use  $\gamma$  as the variance of the estimation error at all the nodes.

*Phase 4:* By the end of Phase 3, node-1 and node-2 have noisy versions of the CSR  $\{h_{12}(l)\}$ , but not node-3. Therefore, to fill the gap, in the last phase, node-1 (which acts as the facilitator) transmits the sum  $\theta_1^{(2)}(l) + \theta_1^{(3)}(l)$ , using which node-3 receives  $\theta_3^{(4)}(l) = h_{13}(l)(\theta_1^{(2)}(l) + \theta_1^{(3)}(l)) + n_3^{(4)}(l)$ , where  $n_3^{(4)}(l)$  denotes the additive noise at node-3 distributed as  $\mathcal{CN}(0, \sigma^2)$ . Using  $\theta_3^{(1)}(l)$  and  $\theta_3^{(4)}(l)$ , node-3 learns a noisy version of  $h_{12}(l)$  as

$$\bar{\theta}_3^{(4)}(l) = \left( \left( \theta_3^{(1)}(l) \right)^{-1} \theta_3^{(4)}(l) \right) - \theta_3^{(1)}(l).$$

Thus, by the end of Phase 4, the three nodes witness noisy versions of the CSR  $\{h_{12}(l)\}$ .

Observe that all the nodes witness noisy version of the CSR, wherein the noise levels depend on the node. Specifically, node-1 and node-2 observe  $\{h_{12}(l)\}$ , which are perturbed by estimation errors. However, node-3 observes a noisy version of  $h_{12}(l)$ , which is perturbed by both estimation error and the recovery noise during Phase 4.

In terms of leakage, an external eavesdropper receives the following symbols in the four phases:  $y_E^{(1)}(l) = h_{1E}(l) + n_E^{(1)}(l)$ ,  $y_E^{(2)}(l) = h_{2E}(l) + n_E^{(2)}(l)$ ,  $y_E^{(3)}(l) = h_{3E}(l) + n_E^{(3)}(l)$ ,  $y_E^{(4)}(l) = h_{1E}(l)(\theta_1^{(2)}(l) + \theta_1^{(3)}(l)) + n_E^{(4)}(l)$ , where  $h_{jE}(l)$  is the complex channel between node- $j$  for  $1 \leq j \leq 3$  and the eavesdropper, and  $n_E^{(k)}(l)$  is the AWGN at the eavesdropper in Phase  $k$  for  $k = 1, 2, 3, 4$ . Note that the eavesdropper cannot learn the channel realizations  $\{h_{12}(l)\}$  during the first three phases by the virtue of its physical location (with the assumption that  $h_{1E}(l), h_{2E}(l), h_{3E}(l)$  are statistically independent of  $h_{12}(l)$ ). However, in Phase 4, it is straightforward to verify that the CSR is not confidential since the mutual information between the sum  $\theta_1^{(2)}(l) + \theta_1^{(3)}(l)$  and  $\theta_1^{(1)}(l)$  is not zero. Overall, in addition to the asymmetry in the noise levels of the CSR at different nodes, this protocol also leaks the CSR to an eavesdropper.

### B. GSK Generation With Quantization At the Facilitator

In this section, we discuss some practical aspects of GSK generation protocols. In Section II-A, the first three phases involve broadcast of pilot symbols, wherein the receiver nodes

estimate the corresponding channels using an appropriate channel estimation algorithm. However, in Phase 4, the sum of the two channel realizations, i.e.,  $\theta_1^{(2)}(l) + \theta_1^{(3)}(l)$ , is transmitted by node-1. Observe that the in-phase and the quadrature components of  $\theta_1^{(2)}(l) + \theta_1^{(3)}(l)$  can be irrational, and as a result, there will be loss of precision when the radio devices are implemented with limited hardware. Furthermore, most practical radios are designed to transmit baseband signals from finite constellations such as PSK, QAM etc. Due to constraints of short coherence-blocks, node-1 would need to transmit a quantized version of the sum  $\theta_1^{(2)}(l) + \theta_1^{(3)}(l)$ , given by  $\varphi(\theta_1^{(2)}(l) + \theta_1^{(3)}(l)) = \theta_1^{(2)}(l) + \theta_1^{(3)}(l) + z_{sum}(l)$ , where  $\varphi(\cdot)$  is an appropriate quantization algorithm that directly quantizes the channel estimates to points in a complex constellation, denoted by  $\mathcal{A}$ , and  $z_{sum}(l)$  is the corresponding quantization noise. We refer to this form of the GSK protocol as Asymmetrically Quantized GSK (AQGSK) [26], [27]. After transmitting the quantized version, the received symbols at node-3 is given by  $\theta_3^4(l) = h_{13}(l)(\theta_1^{(2)}(l) + \theta_1^{(3)}(l) + z_{sum}(l)) + n_3^{(4)}(l)$ .

Using the above received symbols, the channel estimates recovered at node-3 are corrupted by the quantization noise in addition to the recovery noise in Phase 4. Thus, with quantization at node-1, the common randomness across the three nodes are affected by different levels of noise. Although more practical than the GSK protocol in Section II-A, this method suffers from disparity in the effective noise levels at the three nodes, and importantly, the transmitted symbol from the facilitator  $\theta_1^{(2)}(l) + \theta_1^{(3)}(l) + z_{sum}(l)$  continues to leak the CSR  $\theta_1^{(2)}(l)$  at an external eavesdropper. Identifying these disadvantages of the AQGSK protocol, we propose a new GSK protocol that enables the facilitator (node-1) to transmit symbols from a finite constellation, and yet provide zero-leakage to an external eavesdropper.

### III. ALGEBRAIC SQGSK (A-SQGSK) PROTOCOL

Unlike the ideas discussed in Section II-B, the main idea to ensure zero-leakage to an external eavesdropper is to avoid quantizing  $\theta_1^{(2)}(l) + \theta_1^{(3)}(l)$ , which is the sum of the noisy channel realizations observed by node-1. In contrast, we propose to quantize the noisy channel realizations  $\theta_1^{(2)}(l)$  and  $\theta_1^{(3)}(l)$  separately at node-1, then appropriately transform them to points in an algebraic ring, and then compute their linear combination over the algebraic ring. Henceforth, throughout the paper, we refer to this scheme as the A-SQGSK protocol. In the following section, we first present the ingredients required to describe the A-SQGSK protocol.

#### A. Ingredients

The A-SQGSK protocol requires three complex constellations for the following purposes: (i) to quantize the channel realizations at all the three nodes, (ii) to execute the algebraic operations at node-1, and (iii) to broadcast a function of the channel realizations at node-1 (the facilitator). An example for the three constellations is provided in Fig. 2, along with the description of their functionality in Table II. In the proposed

TABLE II  
FUNCTIONALITY OF  $\mathcal{A}$ ,  $\bar{\mathcal{A}}$ , AND  $\mathcal{A}'$

Functionality	Constellation
Quantization at all the nodes	$\mathcal{A}$ is used. Both $\bar{\mathcal{A}}$ , and $\mathcal{A}'$ do not provide uniform distribution.
Algebraic operations at the facilitator	$\mathcal{A}'$ is used. Both $\bar{\mathcal{A}}$ and $\mathcal{A}$ have no algebraic structure.
Broadcasting at the facilitator	$\mathcal{A}'$ would be energy inefficient, $\mathcal{A}$ would lead to more errors due to smaller minimum distance. Therefore, $\bar{\mathcal{A}}$ is used.

A-SQGSK protocol, the facilitator quantizes the complex channel realizations to points in a complex constellation  $\mathcal{A} \subset \mathbb{C}$ , of size  $2^m$ , given by  $\mathcal{A} = \mathcal{A}_I \oplus i\mathcal{A}_Q$ , where  $i = \sqrt{-1}$ , such that  $\mathcal{A}_I = \mathcal{A}_Q$  and  $|\mathcal{A}_I| = 2^{\frac{m}{2}}$ . Using  $\varphi: \mathbb{C} \rightarrow \mathcal{A}$  to denote the quantization operator, we assume that  $\varphi(\cdot)$  works independently on the in-phase and the quadrature components of the input. For instance, with  $\beta \sim \mathcal{CN}(0, \Sigma)$ , we have

$$\varphi(\beta) = \arg \min_{a \in \mathcal{A}} |\beta - a|^2 \in \mathcal{A}. \quad (4)$$

We choose the constellation  $\mathcal{A}$  such that  $\varphi(\beta)$  is uniformly distributed over the support  $\mathcal{A}$  when  $\beta \sim \mathcal{CN}(0, \Sigma)$ . Given that  $\mathcal{A}_I = \mathcal{A}_Q$ , and the in-phase and the quadrature components of  $\beta$  are independent and identically distributed, it suffices to choose  $\mathcal{A}_I \subset \mathbb{R}$  such that  $\text{real}(\varphi(\beta))$  and  $\text{imag}(\varphi(\beta))$  are uniformly distributed over the support  $\mathcal{A}_I$  and  $\mathcal{A}_Q$ , respectively. We also require a regular square quadrature amplitude modulation (QAM) constellation  $\bar{\mathcal{A}} \subset \mathbb{C}$ , of size  $2^m$ , given by  $\bar{\mathcal{A}} = \bar{\mathcal{A}}_I \oplus i\bar{\mathcal{A}}_Q$ , such that  $\bar{\mathcal{A}}_I = \bar{\mathcal{A}}_Q = \{-2^{\frac{m}{2}} + 1, -2^{\frac{m}{2}} + 3, \dots, 2^{\frac{m}{2}} - 3, 2^{\frac{m}{2}} - 1\}$ , where  $i = \sqrt{-1}$ , and  $m$  is even. Assuming that the numbers of  $\mathcal{A}_I$  are arranged in the ascending order, for  $\nu \in \mathcal{A}$ , we define a one-to-one mapping, denoted by  $\psi: \mathcal{A} \rightarrow \bar{\mathcal{A}}$  as

$$\psi(\nu) = \bar{\mathcal{A}}_I(\mathcal{J}(\text{real}(\nu))) + i\bar{\mathcal{A}}_Q(\mathcal{J}(\text{imag}(\nu))), \quad (5)$$

where  $\mathcal{J}(\cdot) \in [2^{\frac{m}{2}}]$  provides the position of the argument in the ordered set  $\mathcal{A}_I$ , and  $\bar{\mathcal{A}}_I(t)$ , for  $t \in [2^{\frac{m}{2}}]$ , provides the  $t$ -th element in the ordered set  $\bar{\mathcal{A}}_I$ . We require a complex constellation  $\mathcal{A}' = \{0, 1, \dots, 2^{\frac{m}{2}} - 1\} \oplus \{0, i, \dots, i(2^{\frac{m}{2}} - 1)\}$ , which forms an algebraic ring  $\mathbb{Z}_{2^{\frac{m}{2}}}[i]$ , defined over regular addition and multiplication, however, with modulo  $2^{\frac{m}{2}}$  operation on both the in-phase and the quadrature components. A regular  $2^m$ -QAM constellation  $\bar{\mathcal{A}}$  can be written as a scaled and shifted version of  $\mathcal{A}'$ . In particular, for  $\alpha \in \bar{\mathcal{A}}$ , the one-one transformation from  $\bar{\mathcal{A}}$  to  $\mathcal{A}'$ , represented by  $\phi: \bar{\mathcal{A}} \rightarrow \mathcal{A}'$ , is

$$\phi(\alpha) = \frac{\alpha + 2^{\frac{m}{2}} - 1 + i(2^{\frac{m}{2}} - 1)}{2}. \quad (6)$$

Using the mappings  $\phi(\cdot)$  and  $\psi(\cdot)$ , it is straightforward to note that there is a one-to-one correspondence between the constellations  $\mathcal{A}$ ,  $\bar{\mathcal{A}}$ , and  $\mathcal{A}'$ . Henceforth, throughout the paper, the composite mapping  $\phi(\psi(\cdot))$  from  $\mathcal{A}$  to  $\mathcal{A}'$  is denoted by  $\Theta(\cdot)$ , and its inverse from  $\mathcal{A}'$  to  $\mathcal{A}$  is denoted by  $\Theta^{-1}(\cdot)$ .

### B. A-SQGSK Protocol

The three nodes agree upon the discrete constellations  $\mathcal{A}, \bar{\mathcal{A}}, \mathcal{A}' \subset \mathbb{C}$  of size  $2^m$ , for some integer  $m$ , where  $m$  is even. Similar to the GSK protocol in Section II-A, the A-SQGSK protocol also comprises four phases (as shown in Fig. 3), which are described below:

*Phase 1:* node-1 broadcasts a pilot symbol  $x = 1$  using which node-2 and node-3 receive  $y_2^{(1)}(l) = h_{12}(l)x + n_2^{(1)}(l)$ , and  $y_3^{(1)}(l) = h_{13}(l)x + n_3^{(1)}(l)$ , respectively, where  $n_2^{(1)}(l)$  and  $n_3^{(1)}(l)$  are the AWGN distributed as  $\mathcal{CN}(0, \sigma^2)$ . Using the received symbols, node-2 and node-3 estimate the channels  $h_{12}(l)$  and  $h_{13}(l)$ , respectively, as  $h_{12}(l) + e_2^{(1)}(l)$  and  $h_{13}(l) + e_3^{(1)}(l)$ , where  $e_2^{(1)}(l) \sim \mathcal{CN}(0, \gamma)$  and  $e_3^{(1)}(l) \sim \mathcal{CN}(0, \gamma)$  denote the channel estimation errors at node-2 and node-3, respectively. Further, these estimates are quantized to points in  $\mathcal{A}$  as

$$\begin{aligned}\theta_2^{(1)}(l) &= \varphi(h_{12}(l) + e_2^{(1)}(l)) \in \mathcal{A}, \\ \theta_3^{(1)}(l) &= \varphi(h_{13}(l) + e_3^{(1)}(l)) \in \mathcal{A},\end{aligned}$$

where  $\varphi(\cdot)$  is as given in (4).

*Phase 2:* Similar to Phase 1, node-2 transmits a pilot symbol  $x = 1$ , which is used by node-1 and node-3 to estimate the channels  $h_{12}(l)$  and  $h_{23}(l)$ , respectively, as  $h_{12}(l) + e_1^{(2)}(l)$  and  $h_{23}(l) + e_3^{(2)}(l)$ . Subsequently, the estimates are quantized as

$$\begin{aligned}\theta_1^{(2)}(l) &= \varphi(h_{12}(l) + e_1^{(2)}(l)) \in \mathcal{A}, \\ \theta_3^{(2)}(l) &= \varphi(h_{23}(l) + e_3^{(2)}(l)) \in \mathcal{A},\end{aligned}$$

where  $e_1^{(2)}(l) \sim \mathcal{CN}(0, \gamma)$  and  $e_3^{(2)}(l) \sim \mathcal{CN}(0, \gamma)$  are the corresponding estimation errors.

*Phase 3:* Similar to Phase 1 and Phase 2, node-3 transmits a pilot symbol  $x = 1$ , which is used by node-1 and node-2 to obtain quantized version of estimates in  $\mathcal{A}$  as

$$\begin{aligned}\theta_1^{(3)}(l) &= \varphi(h_{13}(l) + e_1^{(3)}(l)) \in \mathcal{A}, \\ \theta_2^{(3)}(l) &= \varphi(h_{23}(l) + e_2^{(3)}(l)) \in \mathcal{A},\end{aligned}$$

where  $e_2^{(3)}(l) \sim \mathcal{CN}(0, \gamma)$  and  $e_1^{(3)}(l) \sim \mathcal{CN}(0, \gamma)$  are the corresponding estimation errors. All the three nodes employ the same channel estimation algorithm, and as a result,  $\gamma$  is identical at the three nodes.

*Phase 4:* By the end of Phase 3, node-1 and node-2 have quantized versions of the estimates of the channel  $h_{12}(l)$ , whereas node-3 does not have access to  $h_{12}(l)$ . Therefore, to fill the gap, in the last phase, node-1 applies the composite transformation  $\Theta(\cdot)$  on  $\theta_1^{(2)}(l)$  and  $\theta_1^{(3)}(l)$  to obtain  $\Theta(\theta_1^{(2)}(l)) \in \mathcal{A}'$  and  $\Theta(\theta_1^{(3)}(l)) \in \mathcal{A}'$ , respectively. Subsequently, node-1 computes  $\theta_{sum}(l) = \Theta(\theta_1^{(2)}(l)) \oplus \Theta(\theta_1^{(3)}(l)) \in \mathcal{A}'$  where  $\oplus$  denotes addition over the ring  $\mathbb{Z}_{2^{\frac{m}{2}}}[i]$ , and then it broadcasts  $\theta(l) \triangleq \phi^{-1}(\theta_{sum}(l)) \in \bar{\mathcal{A}}$  to node-2 and node-3. Here  $\phi^{-1}(\cdot)$  denotes the inverse of  $\phi$ , defined in (6). With this, the received symbol at node-3 is given by  $\theta_3^{(4)}(l) = \sqrt{E_{avg}}h_{13}(l)\theta(l) + n_3^{(4)}(l)$ , where  $\sqrt{E_{avg}}$  is the scalar used to normalize the transmit power in

Phase 4 such that  $\mathbb{E}[|\theta(l)|^2] = 1$ . Since node-3 has the knowledge of both  $h_{13}(l) + e_3^{(1)}(l)$  and its quantized version, it obtains a *maximum a posteriori probability* (MAP) estimate  $\hat{\theta}_3(l) \in \bar{\mathcal{A}}$  of  $\theta(l)$ . Using the above estimate, node-3 obtains an estimate of the quantized version of  $h_{12}(l)$  as

$$\bar{\theta}_3^{(4)}(l) = \Theta^{-1}\left(\phi(\hat{\theta}_3(l)) \ominus \Theta(h_{13}(l) + e_3^{(1)}(l))\right) \in \mathcal{A}, \quad (7)$$

where the subtraction operator  $\ominus$  is over the ring  $\mathbb{Z}_{2^{\frac{m}{2}}}[i]$ . Thus, the CSR seen by node-1, node-2, node-3 are respectively given in (8). Unlike the protocol in Section II-A, the CSR witnessed at the three nodes belong to  $\mathcal{A}$ .

$$\left\{\varphi\left(h_{12}(l) + e_1^{(2)}(l)\right)\right\}, \left\{\varphi\left(h_{12}(l) + e_2^{(1)}(l)\right)\right\}, \text{ and } \left\{\bar{\theta}_3^{(4)}(l)\right\} \quad (8)$$

$$\begin{aligned}H\left(\theta_1^{(2)}(l) \mid \theta(l) = c_j\right) &= -\sum_{k=1}^{2^m} \text{Prob}\left(\theta_1^{(2)}(l) = b_k \mid \theta(l) = c_j\right) \\ \log_2\left(\text{Prob}\left(\theta_1^{(2)}(l) = b_k \mid \theta(l) = c_j\right)\right) &\end{aligned} \quad (9)$$

### C. Confidentiality of the CSR in Algebraic SQGSK

In this section, we prove that Eve will not be able to reconstruct the CSR chosen by the three nodes despite listening to all the four phases of the A-SQGSK protocol. Since the channel realization  $h_{12}(l)$  is chosen as the CSR of interest,  $\theta_1^{(2)}(l)$ , which is the quantized version of the CSR at node-1 qualifies as the quantity of interest to the external eavesdropper.

*Theorem 1:* With the use of constellation  $\mathcal{A} \subset \mathbb{C}$  for quantization, when  $\theta_1^{(2)}(l)$  and  $\theta_1^{(3)}(l)$  are identically distributed, we have  $I(\theta_1^{(2)}(l); \theta(l)) = 0$ , where  $\theta(l)$  is the symbol transmitted by node-1 in Phase 4 of the A-SQGSK protocol.

*Proof:* We highlight that this proof is similar to the proof of [27, Theorem 1] with the exception that the quantized random variables are uniformly distributed owing to the choice of  $\mathcal{A}$ . In contrast, the quantized random variables in [27, Theorem 1] were not uniformly distributed since regular-QAM constellations were used for quantization. In Phase 4 of the coherence-block  $l$ , the received symbol at the eavesdropper is given by  $y_E^{(4)}(l) = \sqrt{E_{avg}}h_{1E}(l)\theta(l) + n_E^{(4)}(l)$ , where  $h_{1E}(l)$  is the complex channel between node-1 and the eavesdropper, and  $n_E^{(4)}(l) \sim \mathcal{CN}(0, \Omega)$  is the AWGN noise at the eavesdropper. In this leakage analysis, we assume the worst-case scenario for the legitimate nodes that  $\Omega = 0$ , and also assume that the eavesdropper perfectly knows the channel  $h_{1E}(l)$  (using Phase 1 of the protocol). As a result, the eavesdropper can perfectly recover the transmitted point  $\theta(l) \in \bar{\mathcal{A}}$  by node-1. We now analyze the conditional entropy  $H(\theta_1^{(2)}(l) \mid \theta(l))$ , which quantifies the residual entropy at the eavesdropper. The residual entropy  $H(\theta_1^{(2)}(l) \mid \theta(l))$  at Eve is

$$-\sum_{j=1}^{2^m} H(\theta_1^{(2)}(l) \mid \theta(l) = c_j) \text{Prob}(\theta(l) = c_j),$$

where  $H(\theta_1^{(2)}(l) | \theta(l) = c_j)$  is given in (9), such that  $\text{Prob}(\theta_1^{(2)}(l) = b_k | \theta(l) = c_j)$  is the conditional probability on  $\theta_1^{(2)}(l)$ . Furthermore, we have the relation in (10)

$$\begin{aligned} & \text{Prob}\left(\theta_1^{(2)}(l) = b_k | \theta(l) = c_j\right) \\ &= \text{Prob}\left(\theta_1^{(3)}(l) = \Theta^{-1}(\phi(c_j) \ominus \Theta(b_k))\right), \end{aligned} \quad (10)$$

where  $\ominus$  denotes subtraction over the ring  $\mathbb{Z}_2 \frac{m}{2} [i]$ . Since  $c_j$  is fixed, the symbol  $\Theta^{-1}(\phi(c_j) \ominus \Theta(b_k))$  results in a distinct value of  $\mathcal{A}$  for each  $b_k$ . Therefore, we have  $H(\theta_1^{(2)}(l) | \theta(l) = c_j) = H(\theta_1^{(3)}(l))$ , and thus  $H(\theta_1^{(2)}(l) | \theta(l)) = H(\theta_1^{(3)}(l))$ . Since  $h_{12}(l) + e_1^{(2)}(l)$  and  $h_{13}(l) + e_1^{(3)}(l)$  are identically distributed, we have  $H(\theta_1^{(3)}(l)) = H(\theta_1^{(2)}(l))$ , and therefore, we have  $H(\theta_1^{(2)}(l) | \theta(l)) = H(\theta_1^{(2)}(l))$ . ■

#### IV. GROUP CONSENSUS ALGORITHM FOR A-SQGSK PROTOCOL

By the end of the A-SQGSK protocol, the CSR at the three nodes, as given in (8), belong to the complex constellation  $\mathcal{A}$ , for some  $m > 1$ . Out of the three observations in (8), the first two are a result of direct quantization of channel realizations during the first three phases, whereas as the third one is a consequence of MAP decoding and successive cancellation at node-3 during Phase 4. We note that the in-phase and the quadrature components of a complex CSR sample in (8) are statistically independent at each node owing to circularly symmetric complex channel and also perfect knowledge of the channel during the phase of MAP decoding and successive interference cancellation at node-3. Since the in-phase and the quadrature components of the CSR belong to  $\mathcal{A}_I$ , the three nodes can agree upon a consensus algorithm to identify the location of the real samples that lie at the same level. A straightforward technique to harvest shared secret-keys is to apply two-level quantization on the in-phase and the quadrature components of the samples given in (8), as proposed in [3], [4]. Although this idea is effective, its limitation is its inability to generate more than one bit per sample when the CSR offers significant randomness. A natural way to increase the number of bits per sample is to apply multi-level quantization on each sample, where the number of levels must be chosen depending on the CSR at the end of the A-SQGSK protocol. In order to generate  $b$  bits per real sample, for  $b \in \mathbb{N}$ , we formally define a  $2^b$ -level quantizer as follows.

*Definition 1:* A  $2^b$ -level quantizer, denoted by  $\mathcal{Q}_b \subset \mathbb{R}^2$ , is defined by a set of  $2^b$  pairs of real numbers, given by  $\mathcal{Q}_b = \{(a_j^-, a_j^+) | j = 1, 2, \dots, 2^b\}$ , satisfying the following constraints:

- $a_j^- < a_j^+$  for each  $1 \leq j \leq 2^b$ ,
- $a_j^+ \leq a_{j+1}^-$  for  $1 \leq j \leq 2^b - 1$ , and
- $a_1^- = -\infty$  and  $a_{2^b}^+ = \infty$ .

Henceforth, we refer to the interval  $(a_j^-, a_j^+]$  by a fixed representative in that region, denoted by  $a_j \in (a_j^-, a_j^+]$ . We call this set of representatives  $\{a_j | 1 \leq j \leq 2^b\}$  as the finite constellation  $\mathcal{C} \subset \mathbb{R}$  of size  $2^b$ . We use  $\mathcal{G}_{j,j+1} \triangleq (a_j^+, a_{j+1}^-]$  as the guard band separating the  $j$ -th and the  $(j+1)$ -th region, for

$1 \leq j \leq 2^b - 1$ . We also use  $\Delta_j \triangleq a_{j+1}^- - a_j^+$  to represent the width of  $\mathcal{G}_{j,j+1}$ .

*Definition 2:* A real number  $y \in \mathbb{R}$  is quantized to  $2^b + 1$  discrete values, denoted by  $\bar{\mathcal{C}} \triangleq \mathcal{C} \cup \{X\}$ , based on the following rule

$$\mathcal{Q}_b(y) = \begin{cases} a_j, & \text{if } y \in (a_j^-, a_j^+] \\ X, & \text{if } y \in (a_j^+, a_{j+1}^-] \text{ for } 1 \leq j \leq 2^b - 1, \end{cases} \quad (11)$$

where  $a_j$  is the chosen representative of the region  $(a_j^-, a_j^+]$ , and the symbol  $X$  is used to represent the samples lying in any of the guard bands.

Based on Definition 1 and Definition 2, the notation  $\mathcal{Q}_b$  is used to represent a quantizer, whereas the notation  $\mathcal{Q}_b(\cdot)$  is used to represent evaluation of the quantizer on a given real number. Although the quantizer is applicable on any real number, in this paper, we use this quantizer to apply on real samples in  $\mathcal{A}_I$ . In the next section, we discuss a group consensus algorithm among the three nodes using an appropriately designed quantizer  $\mathcal{Q}_b$ .

##### A. Consensus Phase for Group-Key Generation

To generate a GSK, node-1, node-2 and node-3 agree upon a quantizer  $\mathcal{Q}_b$ , as presented in Definition 1. Furthermore, they collect a sufficiently large number of CSR observations, denoted by

$$\mathcal{Y}_A^c = \left\{ \varphi \left( h_{12}(l) + e_1^{(2)}(l) \right) \mid l = 1, 2, \dots, L \right\},$$

$$\mathcal{Y}_B^c = \left\{ \varphi \left( h_{12}(l) + e_2^{(1)}(l) \right) \mid l = 1, 2, \dots, L \right\},$$

and

$$\mathcal{Y}_C^c = \left\{ \bar{\theta}_3^{(4)}(l) \mid l = 1, 2, \dots, L \right\},$$

over  $L$  coherence-blocks. After unfolding the in-phase and the quadrature components of the CSR, node-1, node-2 and node-3, respectively gather the sets of real samples  $\mathcal{Y}_A$ ,  $\mathcal{Y}_B$  and  $\mathcal{Y}_C$ , each of size  $2L$ . To achieve consensus, the three nodes execute the following protocol using the excursion length  $e \geq 1$ <sup>1</sup>

- node-2 obtains the set  $\bar{Y}_B = \{\mathcal{Q}_b(y_B(r)) | y_B(r) \in \mathcal{Y}_B\}$ , and then shares the index values  $\mathcal{J}_B = \{r \in [2L] | \mathcal{Q}_b(y_B(r)) = \mathcal{Q}_b(y_B(r+1)) = \dots = \mathcal{Q}_b(y_B(r+e-1)) = a_j, \text{ for some } a_j \in \mathcal{C}\}$  to node-1.
- node-1 obtains the set  $\bar{Y}_A = \{\mathcal{Q}_b(y_A(r)) | y_A(r) \in \mathcal{Y}_A\}$ , and then computes the corresponding set of index values  $\mathcal{J}_A = \{r \in [2L] | \mathcal{Q}_b(y_A(r)) = \mathcal{Q}_b(y_A(r+1)) = \dots = \mathcal{Q}_b(y_A(r+e-1)) = a_j, \text{ for } a_j \in \mathcal{C}\}$ . Subsequently, node-1 shares  $\mathcal{J}_{BA} \triangleq \mathcal{J}_B \cap \mathcal{J}_A$  with node-3, where  $\mathcal{J}_{BA}$  denotes the set of index values in consensus between node-2 and node-1.
- node-3 obtains the set  $\bar{Y}_C = \{\mathcal{Q}_b(y_C(r)) | y_C(r) \in \mathcal{Y}_C\}$ , and then computes the corresponding set of index values  $\mathcal{J}_C = \{r \in [2L] | \mathcal{Q}_b(y_C(r)) = \mathcal{Q}_b(y_C(r+1)) = \dots = \mathcal{Q}_b(y_C(r+e-1)) = a_j, \text{ for } a_j \in \mathcal{C}\}$ . Subsequently, node-3 shares  $\mathcal{J}_{CBA} \triangleq \mathcal{J}_C \cap \mathcal{J}_{BA}$  with node-1 and node-2, where  $\mathcal{J}_{CBA}$  denotes the set of index values

<sup>1</sup>This protocol for group consensus is a generalization of the protocol proposed for pair-wise key generation in [3].

in consensus between node-1, node-2 and node-3. We use  $N_{group}$  to denote the length of  $\mathcal{J}_{CBA}$ , i.e.,  $N_{group} = |\mathcal{J}_{CBA}|$ .

Using  $\mathcal{J}_{CBA}$ , node-1, node-2 and node-3 generate the following sequences  $\mathcal{K}_A = \{\mathcal{Q}_b(y_A(r)) | r \in \mathcal{J}_{CBA}\}$ ,  $\mathcal{K}_B = \{\mathcal{Q}_b(y_B(r)) | r \in \mathcal{J}_{CBA}\}$ , and  $\mathcal{K}_C = \{\mathcal{Q}_b(y_C(r)) | r \in \mathcal{J}_{CBA}\}$ . Note that  $\mathcal{K}_A$ ,  $\mathcal{K}_B$ , and  $\mathcal{K}_C$  are  $N_{group}$ -length sequences over the alphabet  $\mathcal{C}$ .

### B. Design Criteria on $\mathcal{Q}_b$

Based on the above consensus algorithm, the following properties are desired on  $\mathcal{K}_A$ ,  $\mathcal{K}_B$ , and  $\mathcal{K}_C$ :

- 1) The symbol-rate, given by  $\frac{N_{group}}{2L}$ , which captures the fraction of samples in consensus among the three nodes, is maximum.
- 2) The entropy of the three sequences must be maximum, i.e.,  $H(\mathcal{K}_A) = N_{group}b$ ,  $H(\mathcal{K}_B) = N_{group}b$ , and  $H(\mathcal{K}_C) = N_{group}b$  where  $H(\mathcal{K}_A)$ ,  $H(\mathcal{K}_B)$  and  $H(\mathcal{K}_C)$ , respectively denote the joint entropy of  $N_{group}$  random variables over  $\mathcal{C}$ .
- 3) The fraction of pair-wise disagreements between any two sequences must be negligible, i.e.,

$$\frac{1}{N_{group}}d_H(\mathcal{K}_E, \mathcal{K}_F) \leq \beta,$$

for  $E, F \in \{A, B, C\}$ , where  $d_H(\cdot, \cdot)$  denotes the Hamming distance operator, and  $\beta$  is a negligible number of our choice.

In the rest of this paper, we drop the reference to the sample index  $r$ , and refer to the real numbers at node-1, node-2 and node-3 as three correlated random variables  $y_A$ ,  $y_B$  and  $y_C$  with an underlying joint probability distribution function  $P(y_A, y_B, y_C)$ . The above listed criteria can be met provided we design a quantizer  $\mathcal{Q}_b$  based on  $P(y_A, y_B, y_C)$ . However, given that this three-dimensional distribution is intractable to handle, we propose relaxed design criteria on  $\mathcal{Q}_b$  which takes into account the two-dimensional joint distribution  $P(y_B, y_C)$  instead of  $P(y_A, y_B, y_C)$ . We choose the pair-wise distribution  $P(y_B, y_C)$  over  $P(y_A, y_B)$  and  $P(y_A, y_C)$  since  $y_C$  is more distorted with respect to  $y_B$  than  $y_A$  because of the combination of quantization noise as well as the recovery noise. Note that while the quantizer design is based on the CSR between the worst-pair of nodes in the network, the same quantizer will be used by all the three nodes during the group consensus phase of Section IV-A.

### C. Relaxed Design Criteria on $\mathcal{Q}_b$ Based on Pair-Wise Consensus

By focusing on the CSR available at node-2 and node-3, we design a quantizer  $\mathcal{Q}_b$  assuming that only node-2 and node-3 are participating in the key-generation process using their CSR  $\mathcal{Y}_B$  and  $\mathcal{Y}_C$ . The following protocol is assumed to take place between node-2 and node-3 with excursion length  $e \geq 1$ :

- node-2 obtains the set  $\bar{\mathcal{Y}}_B = \{\mathcal{Q}_b(y_B(r)) | y_B(r) \in \mathcal{Y}_B\}$ , and then shares the index values  $\mathcal{J}_B = \{r \in$

$[2L] | \mathcal{Q}_b(y_B(r)) = \mathcal{Q}_b(y_B(r+1)) = \dots = \mathcal{Q}_b(y_B(r+e-1)) = a_j, \text{ for } a_j \in \mathcal{C}\}$  to node-3.

- node-3 obtains the set  $\bar{\mathcal{Y}}_C = \{\mathcal{Q}_b(y_C(r)) | y_C(r) \in \mathcal{Y}_C\}$ , and then computes the corresponding set of index values  $\mathcal{J}_C = \{r \in [2L] | \mathcal{Q}_b(y_C(r)) = \mathcal{Q}_b(y_C(r+1)) = \dots = \mathcal{Q}_b(y_C(r+e-1)) = a_j, \text{ for } a_j \in \mathcal{C}\}$ . Subsequently, node-3 shares  $\mathcal{J}_{CB} \triangleq \mathcal{J}_C \cap \mathcal{J}_B$  with node-2, where  $\mathcal{J}_{CB}$  denotes the set of index values in consensus between node-2 and node-3. We use  $N$  to denote the length of  $\mathcal{J}_{CB}$ , i.e.,  $N = |\mathcal{J}_{CB}|$ .

Using  $\mathcal{J}_{CB}$ , node-2 and node-3 generate the following sequences  $\mathcal{K}_B = \{\mathcal{Q}_b(y_B(r)) | r \in \mathcal{J}_{CB}\}$ , and  $\mathcal{K}_C = \{\mathcal{Q}_b(y_C(r)) | r \in \mathcal{J}_{CB}\}$ .

Similar to the design criteria in Section IV-B, the following properties are desired on  $\mathcal{K}_B$  and  $\mathcal{K}_C$ :

- 1) The symbol-rate, given by  $\frac{N}{2L}$ , which captures the fraction of samples in consensus between node-2 and node-3, is maximum.
- 2) The entropy of the two sequences must be maximum, i.e.,  $H(\mathcal{K}_B) = Nb$  and  $H(\mathcal{K}_C) = Nb$ .
- 3) The fraction of pair-wise disagreements must be negligible, i.e.,  $\frac{1}{N}d_H(\mathcal{K}_B, \mathcal{K}_C) \leq \beta$ , where  $\beta$  is a small number of our choice.

We formally express the above criteria in terms of  $P(y_B, y_C)$ , and subsequently formulate an optimization problem to design the quantizer  $\mathcal{Q}_b$  when the consensus algorithm uses excursion length  $e = 1$ . Henceforth, throughout the paper, we formulate the problem statement with respect to a probability density function  $P(y_B, y_C)$ . However, when the CSR samples are discrete, the same formulation continues to hold after replacing the integrals by summation operations. To capture the criterion of symbol-rate, the consensus probability, denoted by  $p_c(\mathcal{Q}_b)$ , is given by,

$$p_c(\mathcal{Q}_b) = \text{Prob}(\mathcal{Q}_b(y_B) \in \mathcal{C}, \mathcal{Q}_b(y_C) \in \mathcal{C}) \\ = \sum_{j=1}^{2^b} \sum_{k=1}^{2^b} \int_{a_j^-}^{a_j^+} \int_{a_k^-}^{a_k^+} P(y_B, y_C) dy_B dy_C. \quad (12)$$

Out of the  $2L$  real samples that undergo consensus, the average number of samples in agreement after the consensus phase is  $2p_cL$ . Therefore, the symbol-rate of the quantizer  $\mathcal{Q}_b$  is

$$\frac{N}{2L} = p_c(\mathcal{Q}_b). \quad (13)$$

It is clear that  $\mathcal{Q}_b(y_B) \in \mathcal{K}_B$  if and only if  $\mathcal{Q}_b(y_B) \in \mathcal{C}$  and  $\mathcal{Q}_b(y_C) \in \mathcal{C}$ . As a result, the entropy of  $\mathcal{Q}_b(y_B) \in \mathcal{K}_B$  is

$$H(\mathcal{Q}_b(y_B) | \mathcal{Q}_b(y_C), \mathcal{Q}_b(y_B) \in \mathcal{C}) = - \sum_{j=1}^{2^b} g_j \log_2 g_j, \quad (14)$$

where

$$g_j = \text{Prob}(\mathcal{Q}_b(y_B) = a_j | \mathcal{Q}_b(y_B), \mathcal{Q}_b(y_C) \in \mathcal{C}) \\ = \frac{\sum_{k=1}^{2^b} \int_{a_j^-}^{a_j^+} \int_{a_k^-}^{a_k^+} P(y_B, y_C) dy_B dy_C}{\sum_{j=1}^{2^b} \sum_{k=1}^{2^b} \int_{a_j^-}^{a_j^+} \int_{a_k^-}^{a_k^+} P(y_B, y_C) dy_B dy_C}. \quad (15)$$

Since the samples after consensus are expected to be random, it is desired to achieve  $b$  bits on (14) when  $\mathcal{C}$  comprises  $2^b$  levels.

Two samples,  $\mathcal{Q}_b(y_B)$  and  $\mathcal{Q}_b(y_C)$  that are already in consensus, i.e.,  $\mathcal{Q}_b(y_B), \mathcal{Q}_b(y_C) \in \mathcal{C}$ , are said to be in error if  $\mathcal{Q}_b(y_B) \neq \mathcal{Q}_b(y_C)$ . Formally, using the joint PDF, the symbol error rate (SER) among the samples in consensus is given by

$$\begin{aligned} SER(\mathcal{Q}_b) &= \text{Prob}(\mathcal{Q}_b(y_B) \neq \mathcal{Q}_b(y_C) \mid \mathcal{Q}_b(y_B), \mathcal{Q}_b(y_C) \in \mathcal{C}) \\ &= \frac{p_{c,m}(\mathcal{Q}_b)}{p_c(\mathcal{Q}_b)}, \end{aligned} \quad (16)$$

where

$$p_{c,m}(\mathcal{Q}_b) = \sum_{j=1}^{2^b} \sum_{k \neq j}^{2^b} \int_{a_j^-}^{a_j^+} \int_{a_k^-}^{a_k^+} P(y_B, y_C) dy_B dy_C, \quad (17)$$

and  $p_c(\mathcal{Q}_b)$  is given in (12). The quantizer  $\mathcal{Q}_b$  must be designed such that  $SER(\mathcal{Q}_b)$  is upper bounded by a negligible number, say  $\beta > 0$ . In practice, the choice of  $\beta$  depends on the error-correction capability of the channel codes which are subsequently used to correct the residual errors in the secret-keys. Since  $SER(\mathcal{Q}_b)$  is inversely proportional to  $p_c(\mathcal{Q}_b)$ , we take the approach of maximizing  $p_c(\mathcal{Q}_b)$  for a given upper bound on  $p_{c,m}(\mathcal{Q}_b)$ .

Keeping in view of the expressions in (13), (14) and (16), the proposed objective function on the design of quantizer is formally given in Problem 1. The constrained optimization in Problem 1 must be solved for a given set of inputs  $\{P(y_B, y_C), \eta, b\}$ . With  $p_c(\mathcal{Q}_b)$  denoting the symbol-rate offered by the quantizer, the SER offered by it is upper bounded by  $\frac{\eta}{p_c(\mathcal{Q}_b)}$ . Therefore, one way to obtain a quantizer satisfying the upper bound  $SER(\mathcal{Q}_b) \leq \beta$ , for some  $\beta > 0$ , is to solve Problem 1 for various values of  $\eta > 0$ , and then choose the one which satisfies  $\frac{\eta}{p_c(\mathcal{Q}_b)} \leq \beta$ .

In the next section, we provide an iterative algorithm to design a quantizer that satisfies the constraints in (18)-(19) for a given  $\eta > 0$ .

*Problem 1:* Solve

$$\arg \max_{\mathcal{Q}_b} p_c(\mathcal{Q}_b)$$

such that

$$H(\mathcal{Q}_b(y_B) \mid \mathcal{Q}_b(y_C), \mathcal{Q}_b(y_B) \in \mathcal{C}) = b, \quad (18)$$

$$p_{c,m}(\mathcal{Q}_b) \leq \eta, \quad (19)$$

where  $\eta > 0$  is a given negligible number.

## V. EM-EM ALGORITHM

Towards solving Problem 1, we present an iterative algorithm, referred to as the Entropy-Maximization Error-Minimization (EM-EM) algorithm. As shown in Fig. 5, our algorithm comprises four blocks, namely: (i) the initialization block, which feeds an initial set of boundaries  $\{(a_j^-, a_j^+) \mid \forall j\}$  for a given  $b \in \mathbb{N}$ , (ii) the entropy block, which handles the constraint in (18), (iii) the error block, which addresses the constraint in (19),

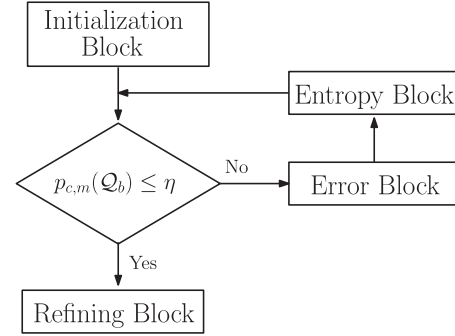


Fig. 5. Depiction of the proposed EM-EM algorithm to generate a multi-level quantizer  $\mathcal{Q}_b$ , which is matched to the joint PDF  $P(y_B, y_C)$ . The inputs to the algorithm are  $\{P(y_B, y_C), \eta, b\}$ , where  $2^b$  is the number of levels, and  $\eta$  is the upper bound on  $p_{c,m}(\mathcal{Q}_b)$ .

and finally (iv) the refining block, which corrects the suboptimality of the entropy block in achieving equality constraint on conditional entropy.

Given the inputs  $\{P(y_B, y_C), \eta, b\}$ , our approach is to solve Problem 1 by assuming that  $y_B$  and  $y_C$  are identical, and then use the corresponding quantizer as the initial set of boundaries. With identical  $y_B$  and  $y_C$ , the initial boundaries  $\{(a_j^-, a_j^+) \mid \forall j\}$  will be such that  $\Delta_j = 0$  for each  $j$ . As a result, the constraint on  $p_{c,m}(\mathcal{Q}_b)$  will not be satisfied when the SNR  $= \frac{1}{\sigma^2}$  is finite. To circumvent this problem, we feed these boundaries to the error block, which increases the width of the  $j$ -th guard band, for  $1 \leq j \leq 2^b - 1$ , as  $(a_j^+, a_{j+1}^-) \leftarrow (a_j^+ - \theta_j, a_{j+1}^- + \theta_j)$ , for some  $\theta_j \geq 0$ , in order to satisfy the constraint  $p_{c,m}(\mathcal{Q}_b) \leq \eta$ . Here, the notation  $\leftarrow$  is used to represent the update operator on the guard bands. Subsequently, since the conditional entropy might have been disturbed, the updated boundaries from the error block are fed to the entropy block, which translates the  $j$ -th guard band, for  $1 \leq j \leq 2^b - 1$ , as  $(a_j^+, a_{j+1}^-) \leftarrow (a_j^+ + \phi_j, a_{j+1}^- + \phi_j)$ , for some  $\phi_j \in \mathbb{R}$ , to satisfy the constraint on conditional entropy. This way, iterations between the error block and the entropy block continue until the constraints on the conditional entropy and  $p_{c,m}(\mathcal{Q}_b)$  are met. At the end of the algorithm, using the final set of boundaries  $\{(a_j^-, a_j^+) \mid \forall j\}$ , we compute  $p_c(\mathcal{Q}_b)$  and  $SER(\mathcal{Q}_b)$  using  $P(y_B, y_C)$ .

In the rest of this section, we explain the functionality of each block by providing the rationale behind its design.

### A. Initialization Block

For a given  $b \in \mathbb{N}$ , we obtain a quantizer  $\{(a_j^-, a_j^+) \mid \forall j\}$ , which is optimized to  $\sigma^2 = 0$ , i.e., when  $y_B$  and  $y_C$  are identical. For this extreme case, the boundaries are obtained by equating

$$P_j = \int_{a_j^-}^{a_j^+} P(y_B) dy_B \quad (20)$$

to  $\frac{1}{2^b}$ , for  $1 \leq j \leq 2^b$ , where  $a_1^- = -\infty$ ,  $a_{2^b}^+ = +\infty$  and  $P(y_B)$  is the PDF of  $y_B$ . A pseudocode description to solve (20) is given in Algorithm 1. It is straightforward to observe that  $\Delta_j = 0$ , for each  $j$ , since  $\sigma^2 = 0$ .

**Algorithm 1:** Initialization Block: The Case When  $\sigma^2 = 0$ .

---

**Input:**  $P(y_B)$ ,  $b$ , and step-size  $\theta > 0$   
**Output:**  $\{(a_j^-, a_j^+) | \forall j\}$

- 1: Initialize  $a_1^- = -\infty$  and  $a_1^+ = -\infty$
- 2: **for**  $j = 1 \rightarrow 2^b - 1$  **do**
- 3:     Compute  $P_j$  using (20)
- 4:     **while**  $P_j < \frac{1}{2^b}$  **do**
- 5:          $a_j^+ \leftarrow a_j^+ + \theta$
- 6:         update  $P_j$  using (20)
- 7:     **end while**
- 8:      $a_{j+1}^- = a_j^+$ ;  $a_{j+1}^+ = a_j^+$
- 9: **end for**
- 10:  $a_{2^b}^+ = +\infty$

---

**B. Error Block**

The objective of this block is to increase the widths of guard bands to satisfy the constraint

$$\sum_{j=1}^{2^b} \sum_{k \neq j}^{2^b} \int_{a_j^-}^{a_j^+} \int_{a_k^-}^{a_k^+} P(y_B, y_C) dy_B dy_C \leq \eta. \quad (21)$$

Out of the  $2^{2b} - 2^b$  terms in (21), the dominant terms are  $\int_{a_j^-}^{a_j^+} \int_{a_k^-}^{a_k^+} P(y_B, y_C) dy_B dy_C$  such that  $|k - j| = 1$ . Therefore, instead of addressing the constraint in (21), the error block satisfies the constraint on  $\delta_i$  given in (22), for each  $1 \leq i \leq 2^b - 1$ . Using  $P(y_B, y_C)$ , we compute the set  $\{\delta_i | i = 1, 2, \dots, 2^b - 1\}$ . Starting from  $i = 1$  to  $2^b - 1$ , the error block increases the width of  $\mathcal{G}_{i,i+1}$  until the constraint in (22) is satisfied, as shown in Algorithm 2. Proposition 1 provides guarantee that increasing the width of  $\mathcal{G}_{i,i+1}$  reduces  $\delta_i$ . If  $\delta_i$ , for some  $i$ , already satisfies the constraint, then  $\mathcal{G}_{i,i+1}$  remains unchanged. This way, the error block increases the width of each guard band prudently based on  $P(y_B, y_C)$ .

$$\begin{aligned} \delta_i = & \int_{a_i^-}^{a_i^+} \int_{a_{i+1}^-}^{a_{i+1}^+} P(y_B, y_C) dy_B dy_C \\ & + \int_{a_{i+1}^-}^{a_{i+1}^+} \int_{a_i^-}^{a_i^+} P(y_B, y_C) dy_B dy_C \leq \frac{\eta}{2^b - 1} \end{aligned} \quad (22)$$

*Proposition 1:* Increasing the width of  $\mathcal{G}_{i,i+1}$  reduces  $\delta_i$ .

*Proof:* This result follows from the definition of probability distribution function. ■

**C. Entropy Block**

The role of the entropy block is to maximize the conditional entropy in (14). Based on the expressions of  $\{g_j | 1 \leq j \leq 2^b\}$  given in (15), the entropy block translates the guard bands locally such that  $g_j = \frac{1}{2^b}$ , for each  $j$ . Unlike the error block, this block does not increase the widths of the guard bands; instead it translates them either to left or right to maximize the conditional entropy. Among the  $2^b$  terms in the numerator of each  $g_j$ , terms of the form  $\int_{a_j^-}^{a_j^+} \int_{a_k^-}^{a_k^+} P(y_B, y_C) dy_B dy_C$ , for  $j \neq k$ , are

**Algorithm 2:** Error Block.

---

**Input:**  $\{(a_j^-, a_j^+) | \forall j\}$ ,  $P(y_B, y_C)$ ,  $b$ ,  $\eta$ , and step-size  $\theta > 0$   
**Output:**  $\{(a_j^-, a_j^+) | \forall j\}$

- 1: **for**  $i = 1 \rightarrow 2^b - 1$  **do**
- 2:     Compute  $\delta_i$  using (22)
- 3:     **while**  $\delta_i > \frac{\eta}{(2^b - 1)}$  **do**
- 4:          $a_i^+ \leftarrow a_i^+ - \theta$ ;  $a_{i+1}^- \leftarrow a_{i+1}^- + \theta$
- 5:         update  $\delta_i$  using (22)
- 6:     **end while**
- 7: **end for**

---

already driven to negligible values by the error block. As a result, the entropy block neglects such terms, and considers an approximation on  $g_j$ , denoted by  $\tilde{g}_j$ , as

$$\tilde{g}_j = \frac{\alpha_j}{\alpha_1 + \alpha_2 + \dots + \alpha_{2^b}}, \quad (23)$$

where

$$\alpha_j = \int_{a_j^-}^{a_j^+} \int_{a_j^-}^{a_j^+} P(y_B, y_C) dy_B dy_C. \quad (24)$$

Using the boundaries received from the error block,  $\tilde{g}_j$  is computed as in (23) sequentially from  $j = 1$  to  $2^b$ . For a given  $j$ , if  $\tilde{g}_j$  is less than  $\frac{1}{2^b}$ , then the corresponding guard band is translated to right until  $\tilde{g}_j = \frac{1}{2^b}$ , as shown in Algorithm 3. On the other hand, if  $\tilde{g}_j$  is more than  $\frac{1}{2^b}$ , then the corresponding guard band is translated to left by an appropriate amount until the equality  $\tilde{g}_j = \frac{1}{2^b}$  is met. The following proposition shows that the direction of translation depends on whether  $\tilde{g}_j$  is more or less than  $\frac{1}{2^b}$ .

*Proposition 2:* If  $\tilde{g}_j$  is less than  $\frac{1}{2^b}$ , then shifting the guard band to right increases  $\tilde{g}_j$ . Similarly, if  $\tilde{g}_j$  is more than  $\frac{1}{2^b}$ , then shifting the guard band to left decreases  $\tilde{g}_j$ .

*Proof:* We provide a proof to show that translating the guard band to right increases the corresponding value of  $\tilde{g}_j$ . The result for the other direction can be proved in a similar manner. Before translating the guard band  $\mathcal{G}_{j,j+1} = (a_j^+, a_{j+1}^-)$ , let  $\tilde{g}_j$  be computed as in (23) using the initial set of values given by  $\{\alpha_j | \forall j\}$ . If this guard band is translated as  $(a_j^+ + \gamma, a_{j+1}^- + \gamma)$ , for some  $\gamma > 0$ , then based on the joint PDF, it is straightforward to observe that  $\alpha_j$  increases to  $\alpha_j + \gamma_{\alpha_j}$ , for some  $\gamma_{\alpha_j} > 0$ , and  $\alpha_{j+1}$  decreases to  $\alpha_{j+1} - \gamma_{\alpha_{j+1}}$ , for some  $\gamma_{\alpha_{j+1}} > 0$ , and the rest of the terms  $\{\alpha_k, |k \neq j, k \neq j + 1\}$  remain unchanged. As a result, the updated version of  $\tilde{g}_j$  is of the form

$$\tilde{g}_j = \frac{\alpha_j + \gamma_{\alpha_j}}{(\sum_{k=1}^{2^b} \alpha_k) + \gamma_{\alpha_j} - \gamma_{\alpha_{j+1}}}. \quad (25)$$

Since  $\tilde{g}_j$  is always less than one, it is straightforward to prove that the updated value in (25) will be more than  $\tilde{g}_j$  for any  $\gamma_{\alpha_j} \geq 0$ ,  $\gamma_{\alpha_{j+1}} \geq 0$ . ■

**D. Refining Block**

Notice that the entropy block forces each  $\tilde{g}_j$  to take  $\frac{1}{2^b}$  from  $j = 1$  to  $2^b$  in a sequential manner, and as a result, the overall

---

**Algorithm 3:** Entropy Block: Maximizing Conditional Entropy.

---

**Input:**  $\{(a_j^-, a_j^+) | \forall j\}$ ,  $P(y_B, y_C)$ ,  $b$ , and step-size  $\theta > 0$

**Output:**  $\{(a_j^-, a_j^+) | \forall j\}$

```

1: for  $j = 1 \rightarrow (2^b - 1)$  do
2:   Compute  $\tilde{g}_j$  using (23)
3:   if  $\tilde{g}_j < \frac{1}{2^b}$  then
4:     while  $\tilde{g}_j < \frac{1}{2^b}$  do
5:        $a_j^+ \leftarrow a_j^+ + \theta$ ;  $a_{j+1}^- \leftarrow a_{j+1}^- + \theta$ 
6:       update  $\tilde{g}_j$  using (23)
7:     end while
8:   else  $\tilde{g}_j > \frac{1}{2^b}$ 
9:     while  $\tilde{g}_j > \frac{1}{2^b}$  do
10:       $a_j^+ \leftarrow a_j^+ - \theta$ ;  $a_{j+1}^- \leftarrow a_{j+1}^- - \theta$ 
11:      update  $\tilde{g}_j$  using (23)
12:    end while
13:   end if
14: end for

```

---



---

**Algorithm 4:** Refining Block: Refining  $\tilde{g}_j = \frac{1}{2^b}$ .

---

**Input:**  $\{(a_j^-, a_j^+) | \forall j\}$ ,  $P(y_B, y_C)$ , and step-size  $\theta > 0$

**Output:**  $\{(a_j^-, a_j^+) | \forall j\}$

```

1: Compute  $\{\alpha_1, \alpha_2, \dots, \alpha_{2^b}\}$  using (24)
2:  $\alpha_{min} = \min_{1 \leq j \leq 2^b} \alpha_j$ 
3: for  $j = 1 \rightarrow 2^b$  do
4:   while  $\alpha_j > \alpha_{min}$  do
5:      $a_j^- \leftarrow a_j^- + \theta$ ;  $a_j^+ \leftarrow a_j^+ - \theta$ 
6:     update  $\alpha_j$  using (24)
7:   end while
8: end for

```

---

entropy  $-\sum_j \tilde{g}_j \log_2(\tilde{g}_j)$  may not be  $b$  after  $\tilde{g}_{2^b}$  is updated. This is because the process of forcing  $\tilde{g}_{j+1}$  to  $\frac{1}{2^b}$  disturbs  $\sum_j \alpha_j$ , which in turn changes  $\tilde{g}_j$ , which was optimized in the preceding step. To correct this suboptimal behaviour of the entropy block, the refining block expands the guard bands to ensure  $\tilde{g}_j = \alpha_{min}$ , where  $\alpha_{min} = \min\{\alpha_j | j = 1, 2, \dots, 2^b\}$ . This way, the equality constraint on entropy is met, and moreover the constraint on  $p_{c,m}(\mathcal{Q}_b)$  is not violated. A pseudocode description of the refining block is given in Algorithm 4.

### E. On Achieving the Desired SER Using the EM-EM Algorithm

After the refining block, the EM-EM algorithm guarantees that the entropy of the key is maximized for a given  $\eta > 0$ . However, at this point, the desired SER may not be achieved, i.e.,  $SER(\mathcal{Q}_b) > \beta$ . Further decreasing  $\eta$  decreases both the numerator and the denominator of (16), and as a result, lower values of  $SER(\mathcal{Q}_b)$  may not be guaranteed by decreasing  $\eta$ . In such cases, the pair  $(b, \beta)$  is not feasible as defined below:

*Definition 3:* When using a quantizer  $\mathcal{Q}_b$  with excursion length  $e = 1$ , the pair  $(b, \beta)$ , for a given  $b \in \mathbb{N}$  and  $\beta > 0$ , is said to be feasible if there exists an  $\eta \leq \beta$  such that  $SER(\mathcal{Q}_b) \leq \beta$ .

Based on Definition 3, when  $(b, \beta)$  is not feasible, we propose to design  $\mathcal{Q}_b$  using the EM-EM algorithm by feeding an  $\eta > 0$  such that  $SER(\mathcal{Q}_b)$  is minimized, i.e.,

$$\eta^* = \arg \min_{\eta} SER(\mathcal{Q}_b). \quad (26)$$

Subsequently, we use the corresponding quantizer  $\mathcal{Q}_b$  (which is designed with  $\eta^*$ ) in the consensus algorithm with excursion length  $e > 1$ . The minimum value of  $e$  for which the mismatch rate of  $\beta$  is achieved will be used in the consensus phase. The following result proves that if the consensus algorithm is employed with  $\mathcal{Q}_b$  (which is designed using the EM-EM algorithm) and excursion length  $e > 1$ , then the entropy of the synthesized key continues to be maximum.

*Proposition 3:* When using the quantizer  $\mathcal{Q}_b$  from the EM-EM algorithm along with excursion length  $e > 1$  in the consensus algorithm, the entropy of the synthesized key continues to be  $b$  bits per sample.

*Proof:* The EM-EM algorithm generates a quantizer  $\mathcal{Q}_b$  that guarantees maximum entropy on the generated key when  $e = 1$ , and this feature is contributed by the refining block of the algorithm. When using the consensus algorithm with  $\mathcal{Q}_b$  and  $e > 1$ , let  $\bar{Y}_B^e$  and  $\bar{Y}_C^e$  denote  $e$ -successive samples of  $\bar{Y}_B$  and  $\bar{Y}_C$ , respectively, and let  $P(\bar{Y}_B^e, \bar{Y}_C^e)$  denote the corresponding joint probability mass function of  $\bar{Y}_B^e$  and  $\bar{Y}_C^e$ . Note that the support of  $\bar{Y}_B^e$  and  $\bar{Y}_C^e$  are  $e$ -fold cross products of the set  $\bar{\mathcal{C}}$  given by  $\bar{\mathcal{C}}^e = \underbrace{\bar{\mathcal{C}} \times \bar{\mathcal{C}} \times \dots \times \bar{\mathcal{C}}}_{e \text{ times}}$  with size  $(2^b + 1)^e$ , where

$\bar{\mathcal{C}} = \mathcal{C} \cup X$ . As per the consensus algorithm in Section IV-C, the consensus probability is given by  $\sum_j \sum_k \text{Prob}(\bar{Y}_B^e = \bar{a}_j, \bar{Y}_C^e = \bar{a}_k)$ , where  $\bar{a}_j = [a_j a_j \dots a_j]$  and  $\bar{a}_k = [a_k a_k \dots a_k]$  such that  $a_j, a_k \in \mathcal{C}$ . Let us define the set  $\bar{\mathcal{C}}_X^e = \{v \in \bar{\mathcal{C}}^e | v(t) = X \text{ for some } 1 \leq t \leq e\}$ . With that, the conditional entropy with excursion length  $e > 1$  is given by  $H(\bar{Y}_B^e | \bar{Y}_B^e \notin \bar{\mathcal{C}}_X^e, \bar{Y}_C^e \notin \bar{\mathcal{C}}_X^e) = -\sum_{j=1}^{2^b} t_j \log_2(t_j)$ , where

$$\begin{aligned} t_j &= \frac{\sum_k \text{Prob}(\bar{Y}_B^e = \bar{a}_j, \bar{Y}_C^e = \bar{a}_k)}{\sum_j \sum_k \text{Prob}(\bar{Y}_B^e = \bar{a}_j, \bar{Y}_C^e = \bar{a}_k)} \\ &= \frac{\sum_k (\text{Prob}(\bar{Y}_B = a_j, \bar{Y}_C = a_k))^e}{\sum_j \sum_k (\text{Prob}(\bar{Y}_B = a_j, \bar{Y}_C = a_k))^e}, \end{aligned}$$

where the second equality is applicable because of statistical independence across the  $e$  samples. If the parameter  $\gamma$  of the EM-EM algorithm is appropriately chosen, then the cross-terms  $\text{Prob}(\bar{Y}_B = a_j, \bar{Y}_C = a_k)$ , for  $j \neq k$ , are negligible. As a result, we can approximate  $t_j$  as

$$t_j \approx \frac{(\text{Prob}(\bar{Y}_B = a_j, \bar{Y}_C = a_j))^e}{\sum_{k=1}^{2^b} (\text{Prob}(\bar{Y}_B = a_k, \bar{Y}_C = a_k))^e}.$$

Since the refining block of the EM-EM algorithm ensures identical values of  $\text{Prob}(\bar{Y}_B = a_j, \bar{Y}_C = a_j)$  for each  $1 \leq j \leq 2^b$ , we note that  $t_j \approx \frac{1}{2^b}$ , and therefore the conditional entropy of the symbols in consensus is maximum. ■

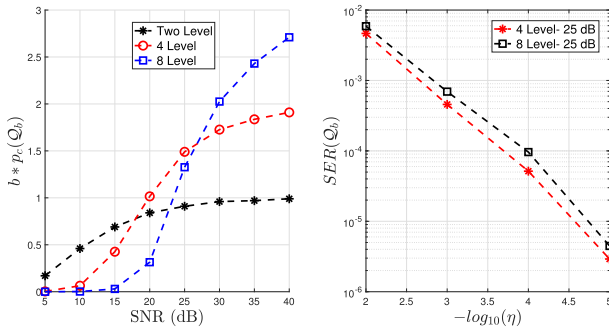


Fig. 6. Left-side: Average bits per sample offered by the EM-EM algorithm with the constraint  $SER(Q_b) \leq 10^{-3}$ . Right-side:  $SER(Q_b)$  values achieved by the EM-EM algorithm based on  $\eta$ .

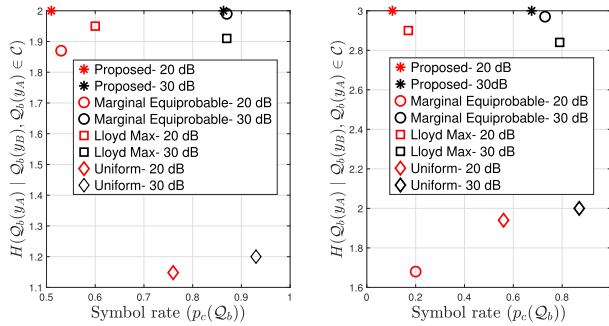


Fig. 7. Scatter plots of pairs  $(H(Q_b(y_A) | Q_b(y_A) \in \mathcal{C}), p_c(Q_b))$  and  $(H(Q_b(y_B) | Q_b(y_A) \in \mathcal{C}), p_c(Q_b))$  for various multi-level quantizers with  $b = 2$  and  $3$ , and  $SNR = 20$  and  $30$  dB, to achieve  $SER(Q_b) \leq 10^{-3}$ . The plots confirm that the EM-EM algorithm guarantees maximum entropy.

### F. Performance of the EM-EM Algorithm

Before applying the EM-EM algorithm with A-SQGSK protocol, we showcase the performance of the EM-EM algorithm on the CSR  $\{\theta_2^{(1)}(l)\}$  and  $\{\theta_1^{(2)}(l)\}$  in (1) and (2), respectively. On the left-side of Fig. 6, we present the key rate of the EM-EM algorithm, defined as  $b * p_c(Q_b)$ , when  $b = 1, 2,$  and  $3$ , against various values of  $SNR = \frac{1}{\sigma^2}$ . To generate the results, the constraint  $SER(Q_b) \leq 10^{-3}$  is satisfied at each SNR by feeding an appropriate value of  $\eta$  to the EM-EM algorithm. The left-side plots in Fig. 6 show that  $b$  must be chosen based on SNR in order to fully exploit the shared randomness. We highlight that the secret-keys generated for the above values of  $b$  exhibit maximum entropy at each SNR. The right-side plots of Fig. 6 show that lower values of  $SER(Q_b)$  can also be achieved by the EM-EM algorithm by choosing appropriate values of  $\eta$ .<sup>2</sup> In Fig. 7, we compare the proposed EM-EM algorithm with the following baselines: (i) Multi-level quantizers which are optimized to maximize the entropy using the marginal distribution, (ii) Max-Lloyd algorithm, which provides  $2^b$  points in  $\mathbb{R}$  by optimizing the average quantization error using the marginal distribution, and (iii) Uniform quantizer, wherein the  $2^b$  quantization levels are uniformly spread in  $\mathbb{R}$ ,

<sup>2</sup>Since the CSR of interest in this simulations are continuous random variables, the EM-EM algorithm is able to achieve the required SER with excursion length  $e = 1$ . However, when applying the EM-EM algorithm to A-SQGSK protocol, we will show that  $e = 1$  does not suffice due to discrete constellations.

independent of the marginal distribution. With each baseline, the widths of the guards bands are increased until the constraint  $SER(Q_b) \leq 10^{-3}$  is satisfied. The plots confirm that none of the baselines achieves entropy of  $b$  bits. However, at high SNR, the entropy achieved by optimizing marginal distributions is close to that of EM-EM algorithm owing to high probability of consensus. Interestingly, the uniform quantizer achieves higher symbol-rate than the EM-EM algorithm because of significant mass points near the origin. However, the corresponding entropy is low, thereby resulting in lower key-rate.

### G. Complexity of the EM-EM Algorithm

Given a joint probability distribution function on two correlated random variables, the EM-EM algorithm generates a two-dimensional discrete probability mass function (PMF) on an alphabet of size  $2^b$  so as to satisfy the conditions in Problem 1. Towards quantifying its complexity, the complexity of the error block, the entropy block, and the refining block, must be quantified. With respect to the error and the entropy blocks, we can quantify their complexity by counting the number of times the two-dimensional PMF is updated through the iterative process. Note that each time a guard band is expanded or shifted, the PMF has to be updated to check the condition given in line 3 of Algorithm 2 and Algorithm 3. If the two correlated random variables are continuous, then the number of PMF updates depends on the choice of the step-size  $\theta$  within each block. In particular, with smaller step-size, the EM-EM algorithm provides higher precision in achieving the entropy of  $b$  bits per symbol, however, at the cost of a large number of PMF updates. On the other hand, with large step-size, while the number of PMF updates decreases, the EM-EM algorithm may generate secret-keys with lower key-rate as guard bands may not be prudently expanded in the error block.

When applied to the A-SQGSK protocol, the input to the EM-EM algorithm is the joint PMF on the CSR between node-2 and node-3. Note that the CSR is discrete, wherein the size of the support set is given by  $2^{\frac{m}{2}}$ . Furthermore, upon mapping the CSR samples in (8) to the ring  $\mathbb{Z}_{2^{\frac{m}{2}}}[i]$  using  $\Theta(\cdot)$ , the minimum step-size that can be used in the EM-EM algorithm is  $\theta = 1$ . This implies that once the algorithm enters the error block, the maximum number of PMF updates is  $\lceil \frac{2^{\frac{m}{2}} - 2^b}{2} \rceil$ . However, when the algorithm is inside the entropy block the maximum number of PMF updates is  $2^{\frac{m}{2}} - 2^b$ . This difference in the PMF updates between the error block and the entropy block is attributed to the fact that the error block increments the width of a guard band on both sides, whereas the entropy block only shifts a guard band without increasing its width. Finally, after a number of iterations between these two blocks, the refining block also updates the PMF one more time so as to achieve the conditional entropy of  $b$  bits per sample (see line 4 of Algorithm 4). In order to present the total number of PMF updates through the iterative process, we count them when the CSR samples of the A-SQGSK protocol are fed to the EM-EM algorithm at various values of SNR and  $m$ . These plots are presented in Fig. 8 for both  $b = 1$  and  $b = 2$  in order to achieve the bound  $p_{c,m}(Q_b) \leq \eta$ , for  $\eta = 0.1$ . As shown in each of the two cases, it is clear that with

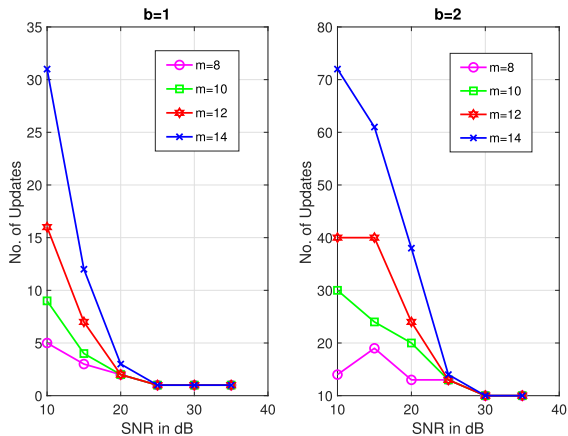


Fig. 8. Complexity of the EM-EM algorithm as a function of SNR, and the size of the constellation used to generate the CSR samples. We use the number of PMF updates during the iterations within the EM-EM block as a measure of complexity.

larger values of  $m$ , the number of updates is high since there is more room for the guard bands to shift and expand. Furthermore, as SNR increases, the number of updates decreases since the error block only needs to expand a guard band few times since the underlying noise is negligible to help achieve the bound  $p_{c,m}(\mathcal{Q}_b) \leq \eta$ . Overall, the plots in Fig. 8 show that the EM-EM algorithm can be deployed in practice owing to few PMF updates at moderate- and high-SNR values.

## VI. SIMULATION RESULTS USING EM-EM ALGORITHM ON THE A-SQGSK PROTOCOL

In this section, we present simulation results on the performance of the A-SQGSK protocol in conjunction with the proposed EM-EM algorithm. In the first three phases of the A-SQGSK protocol, all the nodes use the received symbols as the noisy estimates of the channels, i.e.,  $\gamma = \sigma^2$ . For a given value of  $m \in \{2, 4, 6, 8, 10, 12, 14\}$ , and the underlying signal-to-noise-ratio, defined by  $\text{SNR} = \frac{1}{\sigma^2}$ , we choose the complex constellation  $\mathcal{A}$  to ensure that the outputs of  $\varphi(\cdot)$  are uniformly distributed. Accordingly, we use 4-, 16-, 64-, 256-, 1024-, 4096- and 16384- QAM constellations as  $\mathcal{A}$ . We use  $L = 10\,000$  coherence-blocks to generate the CSR samples, after which each node generates 20 000 real samples, which correspond to the in-phase and the quadrature components of their CSR samples. Subsequently, we feed the joint probability distribution of the real samples at node-2 and node-3 as the input to the EM-EM algorithm by specifying the value of  $b \geq 1$  (which is the number of bits generated per real sample) and the mismatch rate. As discussed in Section V-E, if the bound on mismatch rate is not achieved with excursion length  $e = 1$ , then we design the quantizer  $\mathcal{Q}_b$  with  $\eta^*$  (as given in (26)) and then use it in the consensus algorithm with  $e > 1$ . Finally, we employ the designed quantizer  $\mathcal{Q}_b$  to achieve consensus on a GSK as per the protocol in Section IV-A. Throughout this section, mismatch rate is referred to as bit-error-rate (BER) and symbol-error-rate (SER) when  $b = 1$  and  $b > 1$ , respectively. Out of the  $2L$  real

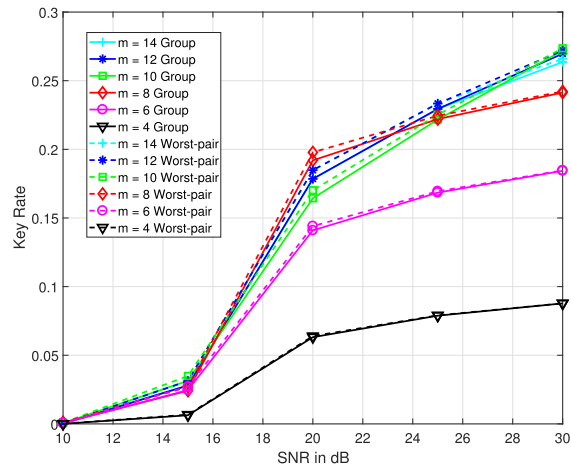


Fig. 9. Key rate against various SNR values and various sizes of the constellation  $\mathcal{A}$  to achieve entropy of  $b = 1$  bit per sample and a mismatch rate (BER) of at most  $10^{-2}$ .

samples available for consensus, we define the key rate as the average number of secret bits generated per real sample.

Using the EM-EM algorithm with  $b = 1$ , i.e., two-level quantization, the key rates of the A-SQGSK protocol are presented in Fig. 9 against  $\text{SNR} \in \{10, 15, 20, 25, 30\}$  dB so as to achieve an upper bound on the mismatch rate of  $10^{-2}$ . In this context, a bit is said to be in error if any two nodes disagree with the value at that location after executing the protocol in Section IV-A. At each SNR value, we capture the impact of the A-SQGSK protocol by employing different sizes of the discrete constellation  $\mathcal{A}$ . The plots in Fig. 9 show that the key rate increases with SNR, and this behaviour is attributed to more samples in consensus among the three nodes since the BER is upper bounded by  $10^{-2}$ . In addition to the key rate of the GSK, we also plot the key rate obtained by executing the pair-wise consensus algorithm (given in Section IV-C) which uses the EM-EM algorithm using the CSR samples at node-2 and node-3. Since the CSR samples between node-2 and node-3 capture the worst-case scenario (due to the combined effect of quantization noise as well as the recovery noise in Phase 4 of the A-SQGSK protocol), the plots show that the key rate of the GSK is marginally lower than that of the pair-wise key. The plots also show that while the key rate increases with  $m$ , it saturates after a certain value of  $m$ , which is dependent on the underlying SNR. The intuition for this behaviour is that as the size of  $\mathcal{A}$  increases, the recovery noise in phase 4 increases, and a result, the CSR witnessed between node-2 and node-3 are further degraded when compared to those at lower values of  $m$ . While this is the case with respect to recovery noise, larger value of  $m$  also provides finer granularity to expand and shift the guard bands in the EM-EM algorithm, thus providing more degrees of freedom to upper bound the BER within  $10^{-2}$ . Overall, due to the conflicting behaviour between the fraction of decoding errors and the smoothness offered to the EM-EM algorithm, the benefits in terms of key rate are marginal after a certain value of  $m$ .

In Fig. 10, we capture the performance of group key generation when different pair-wise samples are considered to design

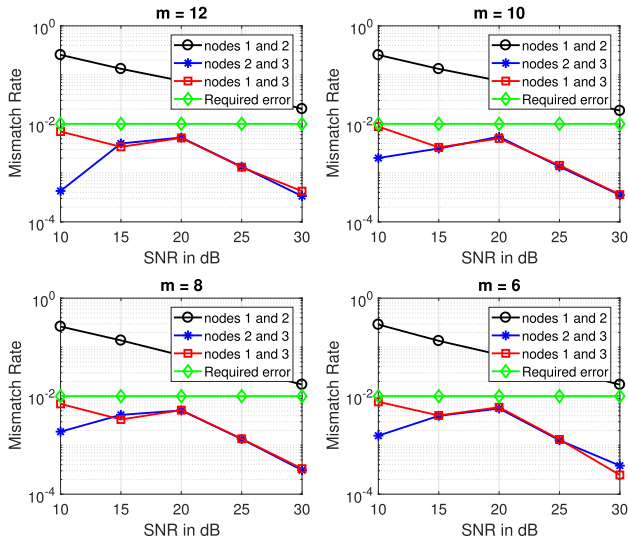


Fig. 10. Comparing the mismatch rate offered by the group consensus algorithm when  $\mathcal{Q}_b$  is designed based on the pair-wise CSR samples at (i) node-1 and node-2, (ii) node-1 and node-3, and (iii) node-2 and node-3.

$\mathcal{Q}_b$ . We plot the mismatch rate of the group key offered by feeding the joint distribution of several pairs, along with the threshold of  $10^{-2}$ , which is the intended mismatch rate fed to the EM-EM algorithm. The plots show that for all values of  $m$ , the joint distribution of CSR at node-1 and node-2 must not be used to design the quantizer; this is because those CSR samples are only perturbed by the effect of additive noise in the quantization process. As a result, at high SNR values, the impact of recovery noise in Phase 4 of the A-SQGSK protocol is neglected. Thus, while the quantizer design is made on good pair of CSR samples, the subsequently designed quantizer is used to achieve consensus on CSR samples that are poorer compared to that of node-1 and node-2. As a result, the overall mismatch rate achieved at the GSK level is more than the desired reliability level. The plots also show that instead of CSR samples at node-2 and node-3, we could also make use of the CSR samples at node-1 and node-3. This is because between the two sources of noise, the recovery noise in Phase 4 is more dominant, and therefore the resultant mismatch rate continues to lie below the desired reliability number. At lower SNR values, the quantization noise between node-1 and node-2 are also considered, and therefore the CSR samples at node-2 and node-3 offer better mismatch rate.

As a generalization of results presented in Fig. 9, in Fig. 11, we also present the key rate to synthesize a GSK with entropy of  $b = 2$  bits per real sample. In this context,  $b = 2$  implies that the quantizer  $\mathcal{Q}_b$  divides the CSR samples (which take  $2^{\frac{m}{2}}$  levels) at each user into  $2^b$  zones in order to arrive at consensus. Similar to the case of  $b = 1$ , the quantizer design continues to maintain an upper bound on the mismatch rate of  $10^{-2}$ . However, the mismatch rate corresponds to SER since the synthesized key is over the alphabet  $\mathcal{C}$  containing 4 values. The plots show that inferences drawn by observing Fig. 9 continue to hold when  $b = 2$ . We have also verified that the entropy of the generated keys is 2 bits per real sample. At lower SNR values, the proposed

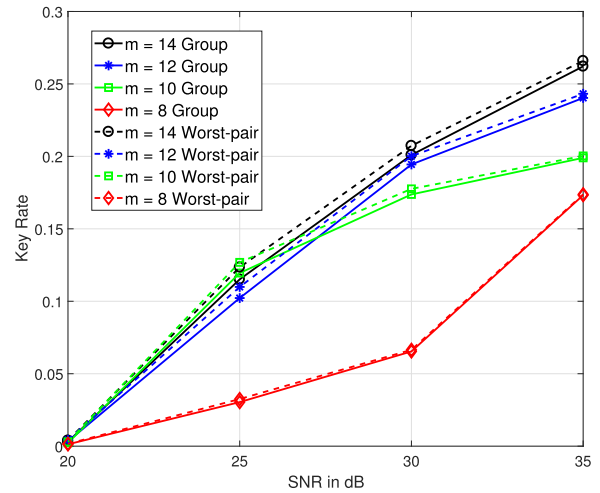


Fig. 11. Similar to Fig. 9, key rate against various SNR values and various sizes of the constellation  $\mathcal{A}$  to achieve entropy of  $b = 2$  bits per sample and a mismatch rate (SER) of at most  $10^{-2}$ .

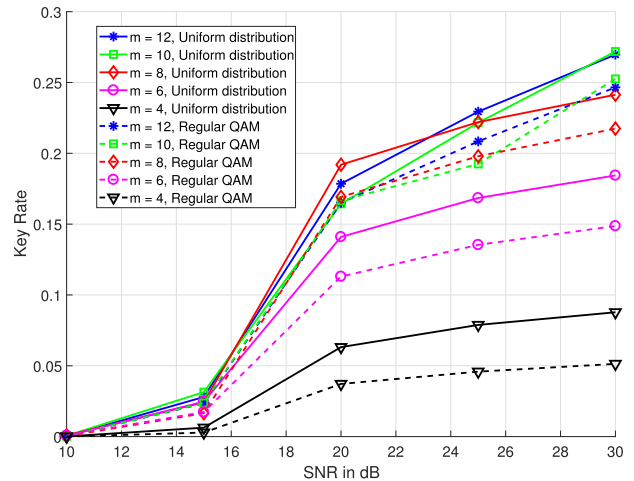


Fig. 12. Comparison of key rates to achieve entropy of  $b = 1$  bit per sample and a mismatch rate (BER) of at most  $10^{-2}$  using the EM-EM algorithm in conjunction with the A-SQGSK protocol: (i)  $\mathcal{A}$  is chosen to induce uniform distribution on the quantized values during the A-SQGSK protocol, and (ii)  $\mathcal{A}$  is uniformly spaced regular QAM constellation with unit average energy.

EM-EM algorithm was unable to generate non-zero key rate satisfying entropy of 2 bits per sample and a mismatch rate of  $10^{-2}$ .

Finally, we present a comparison between the key rate offered by the proposed combination of the A-SQGSK protocol and the EM-EM algorithm when the following two types of discrete constellations are considered for  $\mathcal{A}$ : (i)  $\mathcal{A}$  is chosen such that the resulting CSR samples after the A-SQGSK protocol exhibit uniform distribution, and (ii)  $\mathcal{A}$  is a regular square QAM constellation. To generate the simulation results under (ii), we use a regular square QAM normalized to unit average energy. The corresponding plots on key rate are presented in Fig. 12 for  $b = 1$ . The plots show that forcing uniform distribution on the CSR samples after A-SQGSK protocol outperforms regular-QAM since the latter method accumulates large number of samples around the mean value, and as a result, increasing the guard

band drops significant number of samples when compared to the former case.

In summary, stitching together the advantages of the A-SQGSK protocol and the EM-EM algorithm, we recommend to choose  $m$  and  $b$  based on the underlying SNR values. From the viewpoint of designing  $\mathcal{Q}_b$ , we recommend the use of joint distribution of CSR samples at node-2 and node-3, which constitute the worst-pair of common randomness when using  $h_{12}$  to harvest GSKs.

## VII. CONCLUSION

We have proposed a practical GSK generation protocol for exchanging a common source of randomness among the nodes in a three-user wireless network, followed by a consensus algorithm that guarantees maximum entropy of the generated secret-keys subject to upper bounds on the mismatch rate. With respect to the protocol for exchanging CSR, we have shown that the quantization operation at the facilitator ensures practicality, whereas the algebraic operation ensures confidentiality of the CSR to an external eavesdropper. With respect to the consensus algorithm, we have shown that the EM-EM algorithm provides maximum entropy to the generated keys by considering the discrete nature of the CSR samples provided by the protocol phase. For future work, we are interested in generalizing the proposed protocols to wireless networks with more than three nodes.

## REFERENCES

- [1] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
- [2] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, 2008, pp. 128–139.
- [3] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 2, pp. 240–254, Jun. 2010.
- [4] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th ACM MobiCom '09*, pp. 321–332, 2009.
- [5] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "The effect of eavesdropper's statistics in experimental wireless secret-key generation," 2013, *arXiv:1312.3304*.
- [6] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. IEEE INFOCOM*, pp. 1125–1133, 2011.
- [7] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2593–2597, 2006.
- [8] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.
- [9] Y. E. H. Shehadeh and D. Hogrefe, "An optimal guard-intervals based mechanism for key generation from multipath wireless channels," in *Proc. 4th IFIP Int. Conf. New Techno., Mobility Secur.*, 2011, pp. 1–5.
- [10] Y. W. P. Hong, L. Huang, and H. Li, "Vector quantization and clustered key mapping for channel-based secret key generation," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 5, pp. 1170–1181, May 2017.
- [11] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.
- [12] T. Chou, A. M. Sayeed, and S. C. Draper, "Minimum energy per bit for secret key acquisition over multipath wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, 2009, pp. 2296–2300.
- [13] C. Ling, L. Luzzi, and M. R. Bloch, "Secret key generation from gaussian sources using lattice hashing," in *Proc. IEEE Int. Symp. Infor. Theory*, 2013, pp. 2621–2625.
- [14] Y. Liu, S. C. Draper, and A. M. Sayeed, "Secret key generation through ofdm multipath channel," in *Proc. 45th Annu. Conf. Inf. Sci. Sys.*, 2011, pp. 1–6.
- [15] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.
- [16] K. Kravtsov, Z. Wang, W. Trappe, and P. R. Prucnal, "Physical layer secret key generation for fiber-optical networks," *Opt. Exp.*, vol. 21, pp. 23756–23771, Oct. 2013.
- [17] K. Li, L. Lu, W. Ni, E. Tovar, and M. Guizani, "Cooperative secret key generation for platoon-based vehicular communications," in *Proc. IEEE Int. Conf. Commun.*, 2019, pp. 1–6.
- [18] C. Ye and A. Reznik, "Group secret key generation algorithms," in *Proc. IEEE Int. Symp. Inf. Theory*, 2007, pp. 2596–2600.
- [19] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, "Group secret key generation in wireless networks: Algorithms and rate optimization," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 8, pp. 1831–1846, Aug. 2016.
- [20] Y. Wei, C. Zhu, and J. Ni, "Group secret key generation algorithm from wireless signal strength," in *Proc. 6th Int. Conf. Int. Comput. Sci. Eng.*, 2012, pp. 239–245.
- [21] G. Li, L. Hu, and A. Hu, "Lightweight group secret key generation leveraging non-reconciled received signal strength in mobile wireless networks," in *Proc. IEEE Int. Conf. Commun. Workshops*, 2019, pp. 1–6.
- [22] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, Dec. 2014.
- [23] C. D. Truyen Thai, J. Lee, and T. Q. S. Quek, "Secret group key generation in physical layer for mesh topology," in *Proc. IEEE Glob. Commun. Conf.*, 2015, pp. 1–6.
- [24] M. J. Siavoshani, S. Mishra, S. N. Diggavi, and C. Fragouli, "Group secret key agreement over state-dependent wireless broadcast channels," in *Proc. IEEE Int. Symp. Inf. Theory*, 2011, pp. 1960–1964.
- [25] J. Harshan, S. Chang, and Y. Hu, "Insider-attacks on physical-layer group secret-key generation in wireless networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2017, pp. 1–6.
- [26] M. Rao and J. Harshan, "Practical physical-layer group secret-key generation in three-user wireless networks," in *Proc. Int. Conf. Signal Process. Commun.*, 2018, pp. 342–346.
- [27] M. Rao and J. Harshan, "Low-latency exchange of common randomness for group-key generation," in *Proc. Int. Symp. Personal, Indoor Mobile Radio Commun.*, 2019, pp. 1–6.
- [28] J. Max, "Quantizing for minimum distortion," *IRE Trans. Inf. Theory*, vol. 6, no. 1, pp. 7–12, 1960.