On Opportunistic Selection of Common Randomness and LLR generation for Algebraic Group Secret-Key Generation

Rohit Joshi\* and J. Harshan\*,†

\*Bharti School of Telecom Technology and Management, Indian Institute of Technology Delhi, India.
†Department of Electrical Engineering, Indian Institute of Technology Delhi, India.

Abstract—It is well known that physical-layer key generation methods enable wireless devices to harvest symmetric keys by accessing the randomness offered by the wireless channels. Although two-user key generation is well understood, group secret-key (GSK) generation, wherein more than two nodes in a network generate secret-keys, still poses open problems. Recently, Manish Rao et al., have proposed the Algebraic Symmetrically Quantized GSK (A-SQGSK) protocol for a network of three nodes wherein the nodes share quantized versions of the channel realizations over algebraic rings, and then harvest a GSK. Although A-SQGSK protocol guarantees confidentiality of common randomness to an eavesdropper, we observe that the key-rate of the protocol is poor since only one channel in the network is used to harvest GSK. Identifying this limitation, in this paper, we propose an opportunistic selection method wherein more than one wireless channel is used to harvest GSKs without compromising the confidentiality feature, thereby resulting in remarkable improvements in the key-rate. Furthermore, we also propose a log-likelihood ratio (LLR) generation method for the common randomness observed at various nodes, so that the soft-values are applied to execute LDPC codes based reconciliation to reduce the bit mismatches among the nodes.

Index Terms—Wireless security, physical-layer key generation, group secret-key, common randomness, consensus algorithms

I. INTRODUCTION

It is well known that the randomness offered by wireless channels can be exploited to harvest symmetric keys among the nodes in a wireless network [1]. In two-user physical-layer key generation, the nodes observe the temporal variation in their wireless channel by sharing probing signals with each other, followed by a consensus algorithm to synthesize a secret-key. However, in a more generic model of group secret-key (GSK) generation, more than two nodes intend to harvest a secret-key for securing communication in broadcast and relaying applications, e.g., in vehicular networks. Broadly, physical-layer GSK generation can be classified into two types: (i) Pairwise GSK generation, wherein a central authority (which is one of the nodes in the network) generates a secret-key by applying two-user key generation algorithm with one of its neighbours, and then shares it with the other nodes in the network in a confidential manner [2], [3], and (ii) Group consensus based GSK generation, wherein the central authority assists multiple nodes in the network to witness a common source of randomness (CSR) so that all the nodes can synthesize a group secret-key using a group consensus algorithm [4], [5], [6], [7]. It is noted that the former scheme trusts the central authority in the process of key generation and key distribution whereas in the latter scheme all the nodes share the responsibility of synthesising the key through a group consensus algorithm on the observed CSR. One of the motivations for using the latter class of methods is that the group consensus algorithm, which is executed after sharing the CSR, allows the nodes to mitigate a number of insider attacks [8], which could be executed by the central authority. In this paper, we are interested in the latter class of GSK generation protocols for the above mentioned reasons.

Recently, [4], [5] have proposed a group secret-key (GSK) protocol, referred to as the Algebraic Symmetrically Quantized GSK (A-SQGSK) for a three-user network, wherein one of the channels in the network, which is chosen as the CSR, is appropriately quantized over an algebraic ring, and then shared among the nodes while ensuring zero leakage of the CSR to an external eavesdropper. It is observed that the A-SQGSK protocol is the only protocol that preserves confidentiality [4] in the class of group consensus based GSK generation, and this feature is attributed to the use of algebraic rings. Although A-SQGSK protocol provides zero leakage, we point out that its key-rate is low because the protocol uses only one of the channels in the network as the CSR. Furthermore, in the context of two-user key generation, it is well known that reconciliation algorithms, e.g., using low-density parity check (LDPC) codes, can be used to arrive at zero mismatch rate among the keys at the nodes. Towards employing such reconciliation methods in A-SQGSK, we observe that aspects of generating log-likelihood ratios (LLRs) of the secret bits using the CSR samples have not been addressed hitherto. Identifying the above mentioned limitations, we make the following contributions in this work:

1) For the framework of A-SQGSK protocol, we propose an opportunistic CSR selection strategy wherein the randomness offered by two channels are utilized to synthesize a GSK without compromising the confidentiality feature. We show that our approach provides higher key-
rate than the protocol proposed in [4, 5].

2) Furthermore, when both the channels are amenable to key generation, we emphasize that using both would lead to compromise in the confidentiality, and as a result, we present a likelihood based strategy to choose one of them so as to minimize the mismatch rate among the nodes.

3) Finally, for the A-SQGSK protocol, we also propose an LLR generation scheme, using which all the nodes employ a reconciliation algorithm. We also use LDPC based reconciliation to validate the effectiveness of our LLR generation scheme. Although LLR generation on CSR samples for two-user key generation is well known, we highlight that the statistics of the underlying noise is different at different set of nodes in the A-SQGSK protocol [5]. Therefore, the proposed LLR generation scheme is a non-trivial contribution in GSK generation.

II. SYSTEM MODEL AND BACKGROUND

A network comprising three nodes: node-1, node-2, and node-3 is considered, as shown in Fig. 1. The channel between node-j and node-k is denoted by $h_{jk}$, where $j \neq k$ and $h_{jk} \sim \mathcal{C} \mathcal{N}(0, 1)$. Channel $h_{jk}$ is assumed: (i) to be flat-fading and remains quasi-static for a block of at least 4 channel uses, (ii) it exhibits pairwise reciprocity within the coherence-block i.e., $h_{jk} = h_{kj}$ and (iii) the $\{h_{jk}\}$ are statistically independent and identically distributed. Another assumption made is that all the nodes witness Additive White Gaussian Noise (AWGN) distributed as $\mathcal{C} \mathcal{N}(0, \sigma^2)$, so that the average signal-to-noise ratio (SNR) is $\frac{\sigma}{\sigma^2}$. To synthesize a GSK, a subset of $\{h_{12}, h_{13}, h_{23}\}$, referred to as the CSR, must be learned by all the nodes. In [4], the authors proposed the A-SQGSK scheme, wherein the channel $h_{12}$ is the chosen CSR among the nodes. While a noisy version of $h_{12}$ can be estimated at node-2 and node-1 by probing pilot symbols within a coherence-block, it is clear that node-3 needs to learn $h_{12}$ explicitly. To help this cause, [4] proposed a protocol to share quantized version of $h_{12}$ over an algebraic ring. First, we recall the A-SQGSK protocol, and then point out its limitations.

A. A-SQGSK Protocol

To execute the A-SQGSK protocol, the three nodes must be equipped with two complex constellations $\mathcal{A}$ and $\mathcal{A}$, as exemplified in Fig. 2. To formally define, $\mathcal{A}$ is the algebraic ring $\mathbb{Z}_{2^m}[i]$ where the set $\mathbb{Z}_{2^m}$, for some integer $m > 1$, is given by $\{0, 1, \ldots, 2^m - 1\}$. $\mathcal{A}$ is a regular square quadrature amplitude modulation (QAM) constellation of size $2^m$, given by

- $\mathcal{A} = \mathbb{A}_t \bigoplus i\mathbb{A}_Q$, such that $\mathbb{A}_t = \mathbb{A}_Q = \{-2^{\frac{m}{2}} + 1, -2^{\frac{m}{2}} + 3, \ldots, 2^{\frac{m}{2}} - 3, 2^{\frac{m}{2}} - 1\}$, where $i = \sqrt{-1}$, and $m$ is even. The one-one transformation from $\mathcal{A}$ to $\mathcal{A}'$, represented by $\phi : \mathcal{A} \rightarrow \mathcal{A}'$, is $\phi(\alpha) = \frac{\alpha - 2^{\frac{m}{2}} + 1 + (2^{\frac{m}{2}} - 1)}{2}$. The A-SQGSK protocol consists of four phases:

Phase-1: node-1 broadcasts a pilot symbol $x = 1$ using which node-2 and node-3 receive $y_{12}^{(1)} = h_{12}x + n_{12}^{(1)}$ and $y_{3}^{(1)} = h_{13}x + n_{3}^{(1)}$, where the noise $n_{12}^{(1)}$ and $n_{3}^{(1)}$ are distributed as $\mathcal{C} \mathcal{N}(0, \sigma^2)$ respectively. In this notation, the superscript denotes the phase number in each coherence-block and the subscript denotes the node index. These two nodes then estimate the channel as $h_{12} + e_{12}^{(1)}$ and $h_{13} + e_{13}^{(1)}$, where the estimation errors are distributed as $e_{12}^{(1)}, e_{13}^{(1)} \sim \mathcal{C} \mathcal{N}(0, \gamma)$. Furthermore, these estimates are then quantized as

$C_{12}^{h_{12}} = \phi(h_{12} + e_{12}^{(1)}) \in \mathcal{A}$ and $C_{13}^{h_{13}} = \phi(h_{13} + e_{13}^{(1)}) \in \mathcal{A},$

wherein in the superscript denotes the inherently observed channel and the subscript denotes the node index. Also, the quantization operator $\phi(\beta)$ for $\beta \in \mathbb{C}$ is given as

$\phi(\beta) = \arg \min_{\alpha \in \mathcal{A}} |\beta - \alpha|^2 \in \mathcal{A},$

where $\phi(\cdot)$ works independently on-in-phase and the quadrature components.

Phase-2: Similarly, node-2 broadcasts a pilot symbol $x = 1$, which is used by node-1 and node-3 to estimate the channel as $h_{12} + e_{12}^{(2)}$ and $h_{23} + e_{23}^{(2)}$, respectively, with similar noise statistics as in Phase-1. Subsequently, the estimates are quantized as

$C_{12}^{h_{12}} = \phi(h_{12} + e_{12}^{(2)}) \in \mathcal{A}$ and $C_{23}^{h_{23}} = \phi(h_{23} + e_{23}^{(2)}) \in \mathcal{A}.$

Phase-3: Similarly, node-3 transmits a pilot symbol $x = 1$, whereby node-1 and node-2 estimate the channel as $h_{13} + e_{13}^{(3)}$ and $h_{23} + e_{23}^{(3)}$, respectively. Subsequently, both the nodes obtain the quantized version of estimates as

$C_{13}^{h_{13}} = \phi(h_{13} + e_{13}^{(3)}) \in \mathcal{A}$ and $C_{23}^{h_{23}} = \phi(h_{23} + e_{23}^{(3)}) \in \mathcal{A}.$

Phase-4: Assuming that the CSR is derived using $h_{12}$, node-3 does not have the access to it. To bridge the gap, node-1 computes the sum $c_{sum} = \phi(C_{12}^{h_{12}}) \oplus \phi(C_{13}^{h_{13}}) \in \mathcal{A'}$ over the ring $\mathbb{Z}_{2^m}[i]$ and then it broadcasts $\frac{1}{E_{avg}} \phi^{-1}(c_{sum})$ to node-2 and node-3, where $E_{avg}$ is the average energy of the QAM constellation.

With the knowledge of $h_{13} + e_{3}^{(1)}$, node-3 obtains the maximum a posteriori probability (MAP) estimate of $\phi^{-1}(c_{sum})$, denoted by $\hat{\theta}_3 \in \mathcal{A}$. Using the above estimate, node-3 obtains the CSR as

$C_{3}^{h_{13}} = \phi^{-1}\left(\phi(\hat{\theta}_3) \oplus \phi(\phi(h_{13} + e_{3}^{(1)}))\right) \in \mathcal{A},$

where $\oplus$ is the subtraction over the ring $\mathbb{Z}_{2^m}[i]$. Similarly, node-2 will recover $C_{2}^{h_{13}}$, which is the decoded version of the
bands. Subsequently, all the nodes mutually agree on common list of all the CSR samples that are lying outside the guard nodes, \[4\] proposed all the three nodes to parse through their between any two nodes. To achieve consensus among the three error rate), which is the fraction of bits that do not agree with the rule \(Q\), which is the fraction of bits that do not agree with the rule \(Q\), which is the fraction of bits that do not agree with

\[
I(C_1^{h_{12}}, C_1^{h_{13}}; \phi^{-1}(c_{\text{sum}})) = H(C_1^{h_{12}}, C_1^{h_{13}}) - H(C_1^{h_{12}}, C_1^{h_{13}} | \phi^{-1}(c_{\text{sum}}))
\]

(1)

\[
H(C_1^{h_{12}}, C_1^{h_{13}}) = H(C_1^{h_{12}}) + H(C_1^{h_{13}} | C_1^{h_{12}}) = H(C_1^{h_{12}}) + H(C_1^{h_{13}})
\]

(2)

\[
H(C_1^{h_{12}}, C_1^{h_{13}} | \phi^{-1}(c_{\text{sum}})) = \sum_{j=1}^{2m} H(C_1^{h_{12}} | C_1^{h_{13}} | \phi^{-1}(c_{\text{sum}}) = c_j) P(\phi^{-1}(c_{\text{sum}}) = c_j)
\]

(3)

\[
- \sum_{k=1}^{2m} \sum_{l=1}^{2m} P(C_1^{h_{12}} = b_k, C_1^{h_{13}} = a_l | \phi^{-1}(c_{\text{sum}}) = c_j) \log_2(P(C_1^{h_{12}} = b_k, C_1^{h_{13}} = a_l | \phi^{-1}(c_{\text{sum}}) = c_j))
\]

(4)

\[
P(C_1^{h_{12}} = b_k, C_1^{h_{13}} = \phi^{-1}(\phi(a_l) \oplus \phi(c_j))) = \begin{cases} P(C_1^{h_{12}} = b_k), & \text{if } b_k = \phi^{-1}(\phi(a_l) \oplus \phi(c_j)) \\ 0, & \text{otherwise} \end{cases}
\]

(5)

\[
H(C_1^{h_{12}} | C_1^{h_{13}} | \phi^{-1}(c_{\text{sum}}) = c_j) = \sum_{k=1}^{2m} P(C_1^{h_{12}} = b_k) \log_2(P(C_1^{h_{12}} = b_k)) = H(C_1^{h_{12}})
\]

(6)

III. OPPORTUNISTIC CSR SELECTION

One of the limitations of \[4\] is that only the CSR \(\{R_1^{h_{12}}, R_2^{h_{12}}, R_3^{h_{12}}\}\) was used to extract secret-keys. However, as depicted on the right-side of Fig. 5, it is clear that the three nodes can opportunistically make use of both \(\{R_1^{h_{12}}, R_2^{h_{12}}, R_3^{h_{12}}\}\) and \(\{R_1^{h_{13}}, R_2^{h_{13}}, R_3^{h_{13}}\}\) based on the coherence-block under consideration. In particular, the following possibilities arise on a given coherence-block: (i) Only one of the two sets of CSR samples is out of the guard band at all the three nodes, thereby contributing to the key. (ii) Both the CSR sets lie in the guard band of at least one of the nodes, thereby not contributing to the key for this coherence block. (iii) Both the CSR sets lie outside the guard band at all the nodes, and therefore, either of them is a good choice of CSR. In the first case, the nodes can use the CSR which is in consensus on a given coherence-block. As a result, there will be improvement in the key-rate in comparison with the A-SQGSK protocol \[4\]. We prove that using either of the subset as the CSR preserves confidentiality.

**Proposition 1:** For a \(2^n\)-QAM constellation, when the two CSR, \(C_1^{h_{12}}\) and \(C_1^{h_{13}}\), are identically distributed, we have \(I(C_1^{h_{12}}; \phi^{-1}(c_{\text{sum}})) = 0\) and \(I(C_1^{h_{13}}; \phi^{-1}(c_{\text{sum}})) = 0\), where \(\phi^{-1}(c_{\text{sum}})\) is the symbol transmitted by node-1.

**Proof:** Following the similar lines of the proof in \[5\] Theorem 1, it can be proved that \(I(C_1^{h_{12}}; \phi^{-1}(c_{\text{sum}})) = 0\) and likewise, \(I(C_1^{h_{13}}; \phi^{-1}(c_{\text{sum}})) = 0\).

Using Proposition 1 it follows that choosing either of the two CSR sets for a coherence block will not compromise the confidentiality feature of the CSR. As seen in the third case, on a given coherence-block, when both the CSR samples are in consensus, we cannot use both to extract the keys as it does not ensure confidentiality of the CSR samples as we prove next.

**Proposition 2:** For a \(2^n\)-QAM constellation, when the two complex CSR, \(C_1^{h_{12}}\) and \(C_1^{h_{13}}\), are identically distributed, we have non-zero value of \(I(C_1^{h_{12}}; C_1^{h_{13}}; \phi^{-1}(c_{\text{sum}}))\), where \(\phi^{-1}(c_{\text{sum}})\) is the symbol transmitted by node-1.

**Proof:** The expression for \(I(C_1^{h_{12}}; C_1^{h_{13}}; \phi^{-1}(c_{\text{sum}}))\) is expanded in \[1\], where \(H(C_1^{h_{12}}, C_1^{h_{13}})\) is given in \[2\] such that the second equality holds as \(C_1^{h_{12}}\) and \(C_1^{h_{13}}\) are statistically independent. Furthermore, \(H(C_1^{h_{12}}; C_1^{h_{13}}; \phi^{-1}(c_{\text{sum}}))\) is given in \[3\]. \[4\] to \[6\] show that the conditional

\[
inverse \quad \phi^{-1} : \Delta' \rightarrow \Delta
\]

Fig. 2. Example for the two constellations to facilitate one-to-one transformation in the A-SQGSK protocol with \(m = 4\).
entropy, \( H(C_{1|h_{12}}, C_{1|h_{13}}|\phi^{-1}(c_{sum})) \), is equal to \( H(C_{1|h_{12}}) \) as follows. The first terms after summation in (3), \( H(C_{1|h_{12}}, C_{1|h_{13}}|\phi^{-1}(c_{sum}) = c_j) \), is given in (4). The probability, \( P(C_{1|h_{12}} = b_k, C_{1|h_{13}} = a_l|\phi^{-1}(c_{sum}) = c_j) \) in (4) is given as \( P(C_{1|h_{12}} = b_k, C_{1|h_{13}} = \phi^{-1}(c_{sum}) = c_j) \) in (5). Substituting (4) in (3) gives \( H(C_{1|h_{12}}, C_{1|h_{13}}|\phi^{-1}(c_{sum}) = c_j) \) in (6), which is equal to \( H(C_{1|h_{12}}) \) and then substituting (5) in (4) and (3) in (1) gives \( I(C_{1|h_{12}}, C_{1|h_{13}};\phi^{-1}(c_{sum})) = H(C_{1|h_{12}}) \).

Assuming Eve can perfectly retrieve \( \phi^{-1}(c_{sum}) \), the leakage at Eve is non-zero using Proposition 2. Therefore, when \( \{ R_{1|h_{12}}, R_{2|h_{12}}, R_{3|h_{12}} \} \) and \( \{ R_{1|h_{13}}, R_{2|h_{13}}, R_{3|h_{13}} \} \) are in consensus on a given coherence-block, we present a method for selecting one of them such that the mismatch rate among the keys is minimized.

**Theorem 1:** On a coherence-block when both \( \{ R_{1|h_{12}}, R_{2|h_{12}}, R_{3|h_{12}} \} \) and \( \{ R_{1|h_{13}}, R_{2|h_{13}}, R_{3|h_{13}} \} \) are in consensus, the CSR of interest must be \( \{ R_{1|h_{12}}, R_{2|h_{12}}, R_{3|h_{12}} \} \) if

\[
\operatorname{Prob}(R_{3|h_{12}} \in S| R_{1|h_{12}} \in S) \geq \operatorname{Prob}(R_{3|h_{13}} \in S| R_{1|h_{13}} \in S)
\]

where \( \operatorname{Prob}(R_{2|h_{12}} \in S| R_{1|h_{12}} \in S) \) and \( \operatorname{Prob}(R_{2|h_{13}} \in S| R_{1|h_{13}} \in S) \) are given in (8) and (9), respectively. In this context, we have \( S = \hat{A}_f \), when \( S = \hat{A}_T \). Similarly, we have \( S = \hat{A}_T \), when \( S = \hat{A}_f \).

**Proof:** Let us consider a coherence-block for which both \( R_{j|h_{12}} \) and \( R_{j|h_{13}} \) are in consensus for each \( j \in \{1, 2, 3\} \). The corresponding quantized versions of the complex channels are \( C_{j|h_{12}} \) and \( C_{j|h_{13}} \). At sufficiently large SNR values, and an appropriate value of \( m \), we have \( C_{j|h_{12}} = C_{j|h_{12}} \) and \( C_{j|h_{13}} = C_{j|h_{13}} \) with high probability. Using \( R_{j|h_{12}} \) and \( R_{j|h_{13}} \), node-1 generates the point that was broadcast to node-2 and node-3 as \( \mu = \phi^{-1}(\phi(R_{j|h_{12}}) \oplus \phi(R_{j|h_{13}})) \). Using \( h_{12} + e_1(2) \) as an estimate of the channel seen between node-1 and node-2, node-1 builds an aposteriori PDF at node-2, and in this case it is Gaussian distributed given by \( N(\mu, E_{h_{12}} \sigma^2 / |h_{12} + e_1(2)|) \). Furthermore, since node-2 decodes on the CSR selection using MAP decoder, the corresponding aposteriori PMF on the PM

\[
\mathbb{U}(N(\mu, \gamma), \hat{A}_f) = \left\{ \int_{-\infty}^{\hat{A}_f(1)} P_{\theta}(\theta) d\theta, \int_{\hat{A}_f(2)}^{\infty} P_{\theta}(\theta) d\theta, \ldots, \int_{\hat{A}_f(2)}^{\infty} P_{\theta}(\theta) d\theta \right\}
\]

\[
\operatorname{Prob}(R_{3|h_{12}} \in S| R_{1|h_{12}} \in S) = \sum x \in S \theta^x_u \left( \phi(R_{1|h_{12}}) \left( \mathbb{U} \left( N \left( \phi^{-1} \left( \phi(R_{1|h_{12}}) \oplus \phi(R_{1|h_{13}}) \right) \right), E_{\theta_1(2)} \right) \right) \right)
\]

\[
\operatorname{Prob}(R_{3|h_{13}} \in S| R_{1|h_{13}} \in S) = \sum x \in S \theta^x_u \left( \phi(R_{1|h_{13}}) \left( \mathbb{U} \left( N \left( \phi^{-1} \left( \phi(R_{1|h_{12}}) \oplus \phi(R_{1|h_{13}}) \right) \right), E_{\theta_1(2)} \right) \right) \right)
\]
points is given by \( H_{R_{h13}^b} = \mathcal{U} \left( N \left( \mu, \frac{E_{aw} \sigma^2}{|h_{12} + e_{12}|^2} \right), \bar{A} \right) \),
wherein the PMF \( H_{R_{h13}^b} \) is listed on PM points when enumerated in the increasing order. Finally, since node-2 obtains the CSR \( R_{h13}^b \) by performing a modulo subtraction on the algebraic ring, node-1 incorporates the corresponding changes in the PMF as \( \tilde{H}_{R_{h13}^b} = \mathcal{G}(\mathcal{H}_{R_{h13}^b}) \). Therefore, node-1 generates an a posteriori PMF on the CSR \( R_{h13}^b \) at node-3. Finally, the CSR that provides lower probability of error is chosen for key generation.

Fig. 1 depicts an example for the likelihood selection strategy at node-1 when both the CSR are in consensus. We highlight that node-1 is able to generate the a posteriori PMFs at node-2 and node-3 by using the channel realizations available in the first four phases of the A-SQGSK protocol. As a result, no additional communication-overheads are involved. Furthermore, this method is optimal at moderate values of \( m \) and mid-to-high SNR values since the quantized values of the channels used at node-1 would be the same used at node-2 and node-3 with high probability.

### IV. LLR Based Reconciliation with LDPC Codes

We present an optimal LLR generation scheme for the CSR generated by the A-SQGSK protocol. Since node-1 observes the CSR samples from \( \phi(h_{12}) \) and \( \phi(h_{13}) \) through probing signals, we use the key generated at node-1 as the reference key, and then apply the LDPC reconciliation algorithm at node-2 and node-3. As the statistics of the underlying noise are different, the LLR generation scheme depends on whether the reconciliation is implemented at the (i) reciprocal node, which is the node that inherently observes the CSR through channel reciprocity, e.g., node-2 when the CSR is \( \{R_{h13}^{b1}, R_{h13}^{b2}, R_{h13}^{b3}\} \), or the (ii) decoding node, which is the node that learns the unseen CSR through the process of decoding and subtraction over the ring, e.g., node-2 when the CSR is \( \{R_{h13}^{b1}, R_{h13}^{b2}, R_{h13}^{b3}\} \). We discuss the LLR generation scheme at both these types of nodes.

#### A. LLR Generation at the Reciprocal Node

Let \( P(X, Y) \) denote the joint PMF between the CSR at node-1, denoted by \( X \), and the CSR at the reciprocal node, denoted by \( Y \). For all the 2\( m \) points in \( \tilde{A}_I \), the probability that the CSR sample at node-1 is quantized to bit 1 and bit 0 is given by \( \text{Prob}_1(p) = \sum_{X \in \tilde{A}_I^+} P(X, Y = p) \) and \( \text{Prob}_0(p) = \sum_{X \in \tilde{A}_I^-} P(X, Y = p) \), respectively, where \( \tilde{A}_I^+ \) and \( \tilde{A}_I^- \) are the positive and negative points of \( \tilde{A}_I \), respectively, and \( p \) is the CSR sample observed at the reciprocal node. Finally, the LLR is computed as \( \log \left( \frac{\text{Prob}_1(p)}{\text{Prob}_0(p)} \right) \).

#### B. LLR Generation at the Decoding Node

For exposition, we explain the LLR generation scheme at node-2 when the CSR is \( \{R_{h13}^{b1}, R_{h13}^{b2}, R_{h13}^{b3}\} \). As a result, using \( R_{h13}^{b2} \), node-2 generates the LLR on the bit generated at node-1 using \( R_{h13}^{b1} \). The corresponding quantized version of the channel with node-1, as seen by node-2, is \( C_{h12}^{b2} \). Henceforth, we use \( \tilde{A}_I^+ \) and \( \tilde{A}_I^- \) to represent the positive and negative points in \( \tilde{A}_I \), respectively, that are out of guard bands upon quantization using \( \Omega(\cdot) \).

**Theorem 2**: Using the CSR \( R_{h13}^{b1} \) at node-2, the probability that node-1 quantizes its CSR \( R_{h13}^{b1} \) to bit \( b \), for \( b \in \{0, 1\} \), is given in (10), where \( S = \tilde{A}_I^+ \) and \( S = \tilde{A}_I^- \) when \( b = 0 \) and \( b = 1 \), respectively.

**Proof**: node-2 intends to build an a posteriori PMF on its samples conditioned on the hypothesis that the CSR \( h_{13} \in \tilde{A}_I^+ \). This way, node-2 generates the likelihood of CSR \( R_{h13}^{b1} \) being bit 1 conditioned on its CSR \( R_{h13}^{b1} \). Similarly, using all possible cases of \( h_{13} \in \tilde{A}_I^- \), it generates the likelihood of CSR \( R_{h13}^{b1} \) being bit 0 conditioned on its CSR \( R_{h13}^{b1} \). Henceforth, throughout this proof, we explain the steps for generating the likelihood of CSR \( R_{h13}^{b1} \) being bit 1. Similar steps can be followed to obtain the likelihood of CSR \( R_{h13}^{b1} \) being bit 0. Assuming CSR \( R_{h13}^{b1} = x_u \in \tilde{A}_I^+ \), wherein \( R_{h13}^{b1} \) takes the \( u \)-th element of \( \tilde{A}_I^+ \), for \( 1 \leq u \leq |\tilde{A}_I^+| \), node-2 hypothesizes the point broadcast by node-1 as \( \mu_{x_u} = \phi^{-1} \left( \phi(x_u) \right) \). Note that it is possible to assume
LLR of the bit at node-1 is given by $\log \hat{x}$ using the aposteriori PMF as $\mathcal{H}_{R_{2}^{13}}$. Furthermore, since node-2 decodes on the PAM constellation using MAP decoder, the recovered CSR point is given by $\hat{x}_{u}$, where $x_{u}$ was the CSR at node-1. Using the estimate of the channel between node-1 and node-2, the instantaneous SNR at node-2 is $\frac{\|h_{12}\|^2}{\sigma_{x}^{2}}$. Therefore, the PDF of the effective noise as seen by node-2 is Gaussian distributed given by $N\left(\mu_{x_{u}}, \frac{\sigma_{x}^{2}}{\|h_{12}\|^2}\right)$. Furthermore, since node-2 generates an aposteriori PMF on the CSR $\mathcal{H}_{R_{2}^{13}}$ and this is listed on PAM points when enumerated in the increasing order. Finally, since node-2 obtains the CSR $R_{2}^{13}$ by performing a modulo subtraction on the algebraic ring using $R_{2}^{13}$, node-1 incorporates the corresponding changes in the PMF as $\mathcal{H}_{R_{2}^{13}} = \mathcal{H}_{R_{2}^{13}} + \phi(R_{2}^{13})$. Thus, node-2 generates an aposteriori PMF on the CSR $R_{2}^{13}$ under the hypothesis that $x_{u}$ was the CSR at node-1. Using the recovered CSR point $R_{2}^{13}$, node-2 evaluates the probability using the aposteriori PMF as $\hat{x}_{u} = \mathcal{H}_{R_{2}^{13}}(\hat{R}_{2}^{13})$. Overall, by considering all possible CSR points of $\hat{R}_{2}^{13}$, the probability that the CSR point at node-1 is quantized to bit 1 is given by $\frac{\|h_{12}\|^2}{\sigma_{x}^{2}} \mathcal{H}_{R_{2}^{13}}(\hat{R}_{2}^{13})$. Similarly, the probability that the CSR $\mathcal{H}_{R_{2}^{13}}$ takes the value $x_{u}$. Along the similar lines, the probability that the CSR point at node-1 is quantized to bit 0 is given by $\frac{\|h_{12}\|^2}{\sigma_{x}^{2}} \mathcal{H}_{R_{2}^{13}}(\hat{R}_{2}^{13})$. Finally, the LLR of the bit at node-1 is given by $\log \left(\frac{\mathcal{H}_{R_{2}^{13}}(\hat{R}_{2}^{13})}{\mathcal{H}_{R_{2}^{13}}(\hat{R}_{2}^{13})}\right)$. Fig. 5 depicts an example for LLR generation at node-2 when it observes $\hat{R}_{2}^{13}$ as the decoded CSR.

$R_{2}^{13} = -3$

CSR: $R_{2}^{13} = +7$ (out of guard bands)

V. SIMULATION RESULTS

In this section, we present simulation results on the proposed CSR selection as well as the LLR generation strategy.

A. Opportunistic Selection of CSR

To showcase the advantages of the opportunistic CSR selection, we present its key-rate along with that of the A-SQGSK protocol, wherein the CSR is fixed to $\varphi(h_{12})$. In this context, key-rate is defined as the average number of secret bits generated among the three nodes per CSR sample. The plots are presented in Fig. 6 for the cases when the two-level consensus algorithm delivers secret-keys with an initial error rate of $10^{-3}$ and $10^{-2}$. In this context, initial error rate is defined as the upper bound on the desired mismatch rate among the nodes when choosing the guard bands for the quantizer $Q(\cdot)$. With an initial error rate of $10^{-1}$, the plots show that the benefits of the opportunistic method is marginal, and this observation is attributed to the fact that the number of samples from $\varphi(h_{12})$ and $\varphi(h_{13})$ that are jointly in consensus is large. However, when the initial error rate is $10^{-2}$, the benefits are significant since the number of additional CSR samples coming out of $\varphi(h_{13})$ is large. We note that the above observations continue to hold good for different values of $m$, which captures the size of the constellation. In this work, we have also proposed a method to choose the CSR sample on those coherence-blocks whenever both $\varphi(h_{12})$ and $\varphi(h_{13})$ are in consensus. To showcase the efficacy of the CSR selection method, in Fig. 7 we plot the error rate offered by our scheme on the CSR samples when both $\varphi(h_{12})$ and $\varphi(h_{13})$ are in consensus. The plots show that the likelihood based CSR selection outperforms the channel-strength based CSR selection, wherein node-1 chooses the CSR that offers weaker channel-strength since the weaker channel degrades the SNR when recovering the other CSR.

B. LDPC Based Reconciliation for Algebraic-SQGSK

In the context of opportunistic A-SQGSK protocol, the CSR samples in consensus come from either $\varphi(h_{12})$ or $\varphi(h_{13})$. With respect to the CSR samples from $\varphi(h_{12})$, node-2 and node-3 generate the LLR values on the bits generated at node-1 by following the algorithm at the reciprocal node and the decoding node, respectively. Similarly, for the CSR samples from $\varphi(h_{13})$, node-3 and node-2 generate the LLR values on the bits generated at node-1 by following the algorithm at the reciprocal node and the decoding node, respectively. To execute LDPC based reconciliation, an $(N, K)$ binary LDPC code characterized by the parity check matrix $H$ of dimension $(N - K) \times N$ is used. With $x \in \mathbb{F}_{2}^{N}$ denoting an $N$-length binary key generated at node-1, let $s$ denote its syndrome.

We highlight that no additional communication-overheads are involved in LLR generation. Furthermore, this method is also optimal at mid-to-high SNR and moderate values of $m$. 

Fig. 5. Figure depicts an example for LLR generation for $\hat{R}_{2}^{13}$ at node-2. The top figure illustrates the process of generating aposteriori PMFs on the QAM symbols, whereas the bottom figure illustrates the circular shift operation incorporating subtraction over algebraic ring, and also the computation of LLR.
reconciliation when an LDPC code is employed at node-2 and node-3.

VI. CONCLUSION

In this work, we have presented an opportunistic CSR selection scheme to achieve a higher key-rate than the state-of-the-art A-SQGSK scheme when synthesizing a GSK in a three-node network. Towards guaranteeing non-zero leakage of the CSR to an eavesdropper, we have shown that the proposed CSR selection strategy picks the CSR that minimizes the mismatch rate between the nodes. Finally, to facilitate information reconciliation on the proposed opportunistic CSR selection scheme, we have proposed a novel LLR generation scheme that exploits the underlying noise statistics at the nodes as well as the algebraic ring structure.

REFERENCES

[1] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, “Information-theoretically secret key generation for fading wireless channels,” IEEE Transactions on Information Forensics and Security, vol. 5, pp. 240–254, June 2010.
[2] C. Ye and A. Reznik, “Group secret key generation algorithms,” in 2007 IEEE ISIT, pp. 2596–2600, June 2007.
[3] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, “Group secret key generation in wireless networks: Algorithms and rate optimization,” IEEE Transactions on Information Forensics and Security, vol. 11, pp. 1831–1846, Aug 2016.
[4] M. Rao and J. Harshan, “Low-latency exchange of common randomness for group-key generation,” in IEEE PIMRC, pp. 1–6, 2019.
[5] H. Jagadeesh, R. Joshi, and M. Rao, “Group secret-key generation using algebraic rings in wireless networks,” IEEE Transactions on Vehicular Technology, pp. 1–1, 2021.
[6] Y. Wei, C. Zhu, and J. Ni, “Group secret key generation algorithm from wireless signal strength,” pp. 239–245, April 2012.
[7] 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 Transactions on Mobile Computing, vol. 13, pp. 2820–2835, Dec 2014.
[8] J. Harshan, S. Chang, and Y. Hu, “Insider-attacks on physical-layer group secret-key generation in wireless networks,” pp. 1–6, March 2017.
[9] G. Limei, R. Qi, J. Di, and H. Duan, “Qkd iterative information reconciliation based on ldpc codes,” Int. Journal of Theoretical Physics, pp. 1717–1729, March 2020.
[10] J. K. Wolf, “An Introduction to Error Correcting Codes,” available online at: acsweb.ucsd.edu/~afazelic/ee154c/ErrorCorrection-JackWolff.pdf.