2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)
August 28-29, 2018; Shahid Rajaee Teacher Training University - Tehran, Iran

A Practical and Secure Lattice-based Scheme for Full-Duplex Gaussian One-Way Relay Channels*

Hassan Khodaiemehr
Department of Mathematics,
K. N. Toosi University of Technology,
16315-1618, Tehran, Iran
Email: ha.khodaiemehr@kntu.ac.ir
School of Mathematics,
Institute for Research in Fundamental Sciences (IPM),
19395-5746, Tehran, Iran
Email: khodaiemehr@ipm.ir

Taraneh Eghlidos
Electronics Research Institute,
Sharif University of Technology,
11365-11155, Tehran, Iran
Email: teghlidos@sharif.edu

***Abstract*—Unidirectional or one-way relaying, where two wireless nodes, each of which would like to create an information flow from one node to the other one via a single decode-and-forward (DF) relay, has been an active area of recent research. We consider an additional secrecy constraint for protection against an *honest but curious* relay. Indeed, while the relay should decode the source message, it should be fully ignorant of the message content. We provide a secure lattice coding strategy based on quasi-cyclic low-density parity check (QC-LDPC) lattice codes for unidirectional Gaussian relay channels. QC-LDPC lattice codes are carved from infinite QC-LDPC lattices using a shaping algorithm. These lattice codes are practically implementable in high dimensions due to their low-complexity encoding and decoding algorithms. Our proposed scheme combines a Rao-Nam like encryption with a new DF relaying scheme for QC-LDPC lattice codes. Some chosen-plaintext attacks and recent attacks on the Rao-Nam like schemes are considered over the proposed scheme. The scheme is efficient due to its high information rate and low overhead of the encryption and decryption algorithms. According to our simulation results, the proposed relaying scheme outperforms its counterparts in terms of error performance, efficiency and security.**

***Index Terms*—One-way relaying, QC-LDPC lattice, Rao-Nam scheme.**

I. Introduction

In the Recent years, an explosive growth has been happened in the generation of mobile data by wireless devices. After emerging the Internet of Things (IoT), the amount of traffic from wireless and mobile devices is predicted to be more than 63 percent of total IP traffic by 2021 which is expected to be three times as high as the global population in 2021 [1]. To keep pace with such demands, the primary challenge is how to increase the data transmission rate over a bandwidth limited wireless radio channel with high reliability and security and, at the same time, as low power consumption as possible. One of the effective solutions to increase the range and reliability of wireless networks is cooperative relaying. Lattice codes are one of the effective coded modulation schemes for bandlimited AWGN channels. The use of lattice codes in relay networks has received significant attentions in recent years [2]–[9]. Among different relaying strategies, amplify-and-forward (AF) and decode-and-forward (DF) relaying are two of the most popular relaying protocols. In fact, these two relaying schemes have been widely adopted in practice [10], [11]. It was shown in [3], [5] and [6] that lattice codes can achieve the DF rates for the relay channel. All of these achievable schemes rely on asymptotic code lengths, which is a drawback in practical implementation.

Most of the previous AF and DF relaying strategies assume that the relay operates in half-duplex (HD) mode, i.e., the relay can either transmit or receive on a single channel, but not simultaneously. While the ideas of full-duplex (FD) radio have been around for a while, it is not until recently that a number of encouraging FD designs have been proposed to overcome the self-interference problem. It has been demonstrated in [12], [13] that the information rate achieved by FD relaying is better than that of HD relaying in different wireless environments. Recently, two practical schemes have been proposed based on low-density lattice codes (LDLCs), for the real-valued, full-duplex one-way and two-way relay channels [4], [6] which have been developed for quasi-cyclic low-density parity check (QC-LDPC) lattice codes afterwards [7], [8]. In this work, we propose another scheme, based on QC-LDPC lattice codes, which are Euclidean space analogous to binary QC-LDPC codes, for the real-valued, full-duplex one-way relay channels which outperforms the proposed schemes in [4], [8] and [7] in terms of error performance, efficiency and security. As an advantage, in QC-LDPC lattice codes both the encoder and the channel use the same real algebra which is natural for the continuous-valued AWGN channel.

Security of wireless networks has been considered a challenging task due to the broadcast nature of wireless environments. While traditional approaches are based on cryptographic methods [14], physical layer security methods are based on information theory [15]. In wireless physical layer security, the key idea is to exploit the characteristics of wireless channels to transmit a message from a source to a destination while keeping this message unrevealed from passive eavesdroppers. Here, the relay nodes can be considered as trusted nodes to provide a secured transmission in the presence of one or more eavesdroppers. There is another method, so-called *cooperative jamming* in which a weighted jamming signal will be generated from the relay to confound the adversary. Most the works on cooperating relaying under the context of physical layer security, only consider HD relaying. Given the recent developments, the

*This research was in part supported by a grant from IPM (1396-97).

capability of a FD relay to further enhance the secrecy is certainly appealing. However, to date, a little work has been done for FD relaying. In recent works, FD relaying has been used for sending jamming signals to the eavesdropper while forwarding information signals to the destination [16]. The main drawbacks of these studies is the assumption of significant suppression of self-interference in FD operation. The optimal power allocation scheme and the secrecy rate of a FD relay wire-tap channel under the assumption of residual self-interference are investigated in [17] and [18] for AF and DF relaying, respectively.

Security against an eavesdropping two-way relay using friendly jammers that create a wiretap channel, was considered in [19]. In this model, the relay node is treated as an eavesdropper from whom the information transmitted by the sources needs to be kept secret, despite the fact that its cooperation in relaying this information is essential. Here, a key assumption is that the sources have perfect knowledge of the jamming signals transmitted by the friendly jammers. Application of lattice codes for Gaussian wiretap channels has been considered in [20]. Security of a network with several two-way relays in companion with cooperative jamming was considered in [21], where a lattice-based scheme was proposed.

As mentioned above, the traditional security approaches in wireless networks are based on cryptography. Lattice-based cryptography and its counterpart code-based cryptography are two strong candidates of post-quantum cryptographic methods [22], [23]. The first public-key cryptosystem based on error-correcting codes was introduced by McEliece. Secret-key cryptosystems have smaller key sizes than public-key cryptosystems and also offer a higher level of security. Hence, several secret-key variants of McEliece system like Rao and Nam (RN) [24] cryptosystem have been proposed to reduce the key sizes. In [25], QC-LDPC lattices have been exploited to design a Rao-Nam like encryption scheme.

Our proposed scheme, in one hand can be seen a mechanism that provides security against an eavesdropping one-way relay using a friendly jammer. Thus, it can be considered as a physical layer security scheme. From another point of view, it provides security using a lattice-based secret-key encryption scheme. Consequently, it can be considered in the intersection of two different paradigms of providing security in the wireless networks. The main contributions of this paper can be highlighted as follows:

- We present a new full-duplex one-way relaying scheme based on QC-LDPC lattice codes that outperforms those proposed in [7] and [8],
- We combine a Rao-Nam like encryption with the proposed DF relaying scheme that can also be modeled using a friendly jammer in wireless physical layer security,
- The scheme is secure against chosen plaintext attacks and recent attacks on the Rao-Nam like schemes,
- The scheme is efficient due to its high information rate and low overhead of the encryption and decryption algorithms both of which are linear in terms of the lattice dimension.

The rest of this paper is organized as follows. In Section II, we provide the required background on lattices; the main concepts of QC-LDPC lattices. Section III introduces a secret key cryptosystem based on QC-LDPC lattices. Section IV is devoted to a new secure full-duplex one-way relaying scheme based on QC-LDPC lattice codes. Section V provides the simulation results. Section VI deals with security analysis of the proposed scheme. Finally, Section VII summarizes the paper and provides the concluding remarks.

II. Preliminaries on Lattices

A discrete, additive, subgroup Λ of the m-dimensional real space $\mathbb{R}^m$ is a lattice. Every lattice Λ has a basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{R}^m$ where every $\mathbf{x} \in \Lambda$ can be represented as an integer linear combination of vectors in $\mathcal{B}$ [26]. For a lattice point $\mathbf{x}$ in $\Lambda \subset \mathbb{R}^n$, a Voronoi cell $\mathcal{V}(\mathbf{x})$ is the set of those points of $\mathbb{R}^n$ that are at least as close to $\mathbf{x}$ as to any other point in Λ. We call the Voronoi region associated with the origin, the fundamental Voronoi region of Λ, denoted by $\mathcal{V}$ or $\mathcal{V}(\Lambda)$.

We say that a lattice Λ_s is nested in Λ_c if $\Lambda_s \subset \Lambda_c$. Using nested lattices in $\mathbb{R}^n$, define the codebook $\mathcal{C} = \mathcal{V}_s \cap \Lambda_c$ which has the rate

$$R = \frac{1}{n}\log_2(|\mathcal{C}|) = \frac{1}{n}\log_2\left(\frac{\mathrm{vol}(\mathcal{V}_s)}{\mathrm{vol}(\mathcal{V}_c)}\right). \quad (1)$$

A. QC-LDPC Lattices

The encoding and decoding operations of a general random lattice are challenging problems. Researchers have studied practical implementable lattices and lattice codes. Quasi-cyclic low-density parity check (QC-LDPC) lattices are an instance of such studies [27]. These lattices exploit Construction A lattices [28] together with a QC-LDPC code [29] as their underlying code.

Assume that $\mathcal{C}$ is a linear code over $\mathbb{F}_p$ where p is a prime number, i.e. $\mathcal{C} \subseteq \mathbb{F}_p^n$. A lattice Λ based on Construction A [28] can be derived from $\mathcal{C}$ as follows

$$\Lambda = p\mathbb{Z}^n + \epsilon(\mathcal{C}), \quad (2)$$

where $\epsilon\colon \mathbb{F}_p^n \rightarrow \mathbb{R}^n$ is the embedding function. In this paper, we are particularly interested in lattices with p=2 and consider a subclass of Construction A lattices that has efficient encoder and decoder [27].

Definition 1: A QC-LDPC lattice Λ is a Construction A lattice such that its underlying code $\mathcal{C}$ is a QC-LDPC code with quasi cyclic parity check matrix $\mathbf{H}_{qc}$. Equivalently, $\mathbf{x} \in \mathbb{Z}^n$ belongs to Λ if and only if $\mathbf{H}_{qc}\mathbf{x}^t = 0 \pmod 2$.
The generator matrix of Construction A lattice Λ using the underlying code $\mathcal{C} \subset \mathbb{F}_2^n$ is of the form

$$\mathbf{G}_\Lambda = \begin{bmatrix} \mathbf{I}_k & \mathbf{A}_{k\times(n-k)} \\ \mathbf{0}_{(n-k)\times k} & 2\mathbf{I}_{n-k} \end{bmatrix}, \quad (3)$$

where $\mathbf{G}_\mathcal{C} = \begin{bmatrix} \mathbf{I}_k & \mathbf{A}_{k\times(n-k)} \end{bmatrix}$ is the generator matrix of $\mathcal{C}$ in systematic form, k is the rank of $\mathcal{C}$, $\mathbf{I}_k$ and $\mathbf{0}_{(n-k)\times k}$ are the identity matrix of size k and the all zero matrix of size $(n-k)\times k$, respectively.

B. Shaping Methods for QC-LDPC Lattices

In [7] and [27], several efficient and practical shaping algorithms were proposed for QC-LDPC lattices. In order to perform shaping, the integer vector $\mathbf{b}$ is restricted to the following finite constellation

$$b_i \in \mathcal{L}_i = \left\{ x \in \mathbb{Z} \;\middle|\; \frac{-L_i}{2} \le x \le \frac{L_i}{2} - 1 \right\},\ i = 1, \ldots, n, \quad (4)$$

in which all the L_i's are even integers. The lattice codeword $\mathbf{x} = \mathbf{b}\mathbf{G}_\Lambda$ is shaped by translating each b_i by an integer multiple of L_i, $i = 1, \ldots, n$. Thus, the transmitted lattice point $\mathbf{x}'$ is

$$\mathbf{x}' = (\mathbf{b} - \mathbf{s}\mathbf{L})\mathbf{G}_\Lambda = \mathbf{x} - \mathbf{s}\mathbf{L}\mathbf{G}_\Lambda, \tag{5}$$

where $\mathbf{L} = \text{diag}(L_1, \ldots, L_n)$ is a diagonal matrix and the new integer vector is $\mathbf{b}' = \mathbf{b} - \mathbf{s}\mathbf{L}$. The choice of integer vector $\mathbf{s}$, depends on the employed shaping method. In hypercube shaping we choose $s_1 = s_2 = \cdots = s_k = 0$. Thus, we have $b'_i = b_i$ and $|x'_i| = |b_i| \leq L_i$, for $i = 1, \ldots, k$. For $i = k+1, \ldots, n$, we choose s_i as follows

$$s_i = \left\lfloor \frac{1}{L_i} \left(b_i + \frac{1}{2} \sum_{j=1}^{k} A_{j,i} b_j \right) \right\rfloor, \tag{6}$$

where $A_{i,j}$ is the (i,j)th entry of $\mathbf{A}$ in (3). Note that, after finding the shaped lattice codeword as discussed above, we must scale it by factor 2 and then translate it by $(-1, \ldots, -1)$. The proposed algorithm in [27] explains the method of obtaining original information $\mathbf{b}$ from the shaped lattice codeword $\mathbf{x}'$. The complexity of this algorithm is $O(nd)$, where d is the average number of nonzero elements in a row of $\mathbf{G}_\Lambda$. We use the notation MOD( ) in the case of using the reverse of shaping algorithm.

In order to improve the shaping performance, we consider nested lattice shaping, which is suboptimal but it offers more shaping gains comparing to hypercube shaping [7]. First, limit the rate of the code by restricting the integer row vector $\mathbf{b}$ to take values from a finite constellation in which $b_i \in \mathcal{L}_i = \{0, \ldots, L_i - 1\}$ for each $i = 1, \ldots, n$. Similar to the hypercube shaping, let $\mathbf{x}' = (\mathbf{b} - \mathbf{s}\mathbf{L})\mathbf{G}_\Lambda$. In this case, we choose the vector $\mathbf{s}$ as follows

$$\mathbf{s} = \underset{\mathbf{s}_0 \in \mathbb{Z}^n}{\text{argmin}} \, \|(\mathbf{b} - \mathbf{s}_0\mathbf{L})\mathbf{G}_\Lambda\|^2. \tag{7}$$

The complexity of solving (7) is exponential in the dimension of lattice, even when restricting the components of $\mathbf{b}$. Using the triangular structure of the generator matrix $\mathbf{G}_\Lambda$, the authors of [27] suggested a tree search with affordable complexity for shaping their lattices.

C. Encoding and Decoding of QC-LDPC Lattices

In the sequel, we present the decoding of QC-LDPC lattices, which is proposed in [27]. Construction and decoding of these new lattices can be done using the following steps. First, convert the codewords of $[n, k]$ binary code $\mathcal{C}$ into ± 1 notation (convert 0 to -1 and 1 to 1) which produces a set $\Lambda(\mathcal{C})$ consisting of the vectors of the form

$$\mathbf{c} + 4\mathbf{z}, \quad \mathbf{c} \in \mathcal{C}, \ \mathbf{z} \in \mathbb{Z}^n. \tag{8}$$

The set of points in (8), strictly speaking, is not a lattice, but a lattice translation by vector $(-1, -1, \ldots, -1)$. However, $\Lambda(\mathcal{C})$ is closed under the following addition. For any $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \Lambda(\mathcal{C})$, we have [7], [8]

$$\boldsymbol{\lambda}_1 \oplus \boldsymbol{\lambda}_2 \triangleq \boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2 + (1, \ldots, 1) \in \Lambda(\mathcal{C}). \tag{9}$$

The encoding of an integer row vector $\mathbf{b} \in \mathbb{Z}^n$ can be done as follows

$$\mathcal{E}(\mathbf{b}) = 2\mathbf{b}\mathbf{G}_\Lambda - (1, \ldots, 1), \tag{10}$$

where $\mathcal{E}$ is encoding function and $\mathbf{G}_\Lambda$ is defined as (3). Let $\mathbf{x} = \mathbf{c} + 4\mathbf{z}$ be the transmitted lattice vector and $\mathbf{y}$ be the received vector from AWGN channel

$$\mathbf{y} = \mathbf{c} + 4\mathbf{z} + \mathbf{n}, \tag{11}$$

where $\mathbf{c} \in \mathcal{C}$ and $\mathcal{C}$ is a binary LDPC code in ± 1 notation, $\mathbf{z} \in \mathbb{Z}^n$ and $\mathbf{n} \sim \mathcal{N}(0, \sigma^2)$. First, we decode $\mathbf{c}$ and next we find $\mathbf{z}$. The proposed algorithm in [27] is similar to the sum-product algorithm (SPA) for LDPC codes in message passing structure [30]. The inputs are the log likelihood ratios (LLR) for the a priori message probabilities from each channel. The estimation of the LLR vector $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_n)$ for LDPC lattices is proposed in [27] as follows

$$\begin{aligned} \gamma_i &= \log\left(\frac{\Pr\{c_i = -1 | y_i\}}{\Pr\{c_i = +1 | y_i\}}\right) \\ &\triangleq 2\left(\frac{(\frac{y_i - 1}{4} - \lfloor(\frac{y_i - 1}{4})\rceil)^2 - (\frac{y_i + 1}{4} - \lfloor(\frac{y_i + 1}{4})\rceil)^2}{\sigma^2}\right), \end{aligned} \tag{12}$$

where $\lfloor x \rceil$ is the nearest integer to x. Input the LLR vector $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_n)$ to SPA decoder of LDPC codes and consider $\hat{\mathbf{c}}$ as the output of this decoder. Convert $\hat{\mathbf{c}}$ to ± 1 notation and call the obtained vector $\hat{\mathbf{c}}'$. Estimate $\hat{\mathbf{z}}$ as follows

$$\hat{\mathbf{z}} = \left\lfloor \frac{\mathbf{y}}{4} - \frac{\hat{\mathbf{c}}'}{4} \right\rfloor. \tag{13}$$

Then, $\hat{\mathbf{x}} = \hat{\mathbf{c}}' + 4\hat{\mathbf{z}}$ is the final decoded lattice vector. The complexity of this decoding algorithm is significantly lower than other lattices with practical decoding algorithm like LDLCs [31].

III. Secret Key Cryptosystem Based on QC-LDPC Lattices

In this work, we use a Rao-Nam like secret key encryption scheme that uses QC-LDPC lattices in its design [25]. Encryption is done using the following two secret keys [25].

1) A secret $(n-k)$-bit initial value of a Linear Feedback Shift Register (LFSR).
2) An $n \times n$ block diagonal permutation matrix $\mathbf{P}$ as follows

$$\mathbf{P} = \begin{bmatrix} \pi_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \pi_2 & \cdots & \mathbf{0} \\ \vdots & & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \pi_{n_0} \end{bmatrix}, \tag{14}$$

where the diagonal elements π_i, for $i = 1, \ldots, n_0$, are $b \times b$ permutation submatrices.

Another secret parameter is the parity check matrix $\mathbf{H}_{qc}$ of a random regular $(n = n_0 b, r = b, w)$-QC-LDPC code of size $r \times n$ and constant row weight w, where n_0 is a non-negative integer and b is the size of circulant matrices. We use this parity check matrix in the decryption process. These keys are shared by the authorized sender and receiver. The secret $(n-k)$-bit initial value of the LFSR are used to generate a sequence of 2^{n-k} pseudorandom syndromes synchronously.

To encrypt a message $\mathbf{m} \in \mathbb{Z}^n$, a pseudorandom syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$ is generated using the LFSR. An error vector $\mathbf{e}(\mathbf{s})$ is considered as

$$\mathbf{e}(\mathbf{s}) = \mathbf{s}(\mathbf{H}_{qc}^{-1})^t \pmod 2, \tag{15}$$

where $\mathbf{H}_{qc}^{-1}$ is the right inverse of the parity check matrix of the QC-LDPC lattice $\mathbf{H}_{qc}$ in $\mathbb{F}_2$. The error vector $\mathbf{e(s)}$ has fixed zero coordinates which leads to information leakage. Therefore, the perturbation vector $\mathbf{e}_p$ is defined

$$\mathbf{e}_p = \mathbf{e(s)} + \mathbf{b(s)} \pmod 2. \tag{16}$$

The non-zero coordinates in $\mathbf{b(s)}$ can be filled with $\bar{\mathbf{s}}$ bits (the complement of the syndrome vector $\mathbf{s}$ in $\mathbb{F}_2$) or a succession of these bits in the case $n-k<k$.

The ciphertext is computed as follows

$$\mathbf{y} = (2\mathbf{m}\mathbf{G}_{\mathbf{\Lambda}} - \mathbf{1} + 2\mathbf{e}_p)\mathbf{P}, \tag{17}$$

in which $\mathbf{1}$ indicates the all-ones vector.

The authorized receiver attempts to decrypt the received encrypted signal $\mathbf{y}$ as follows:

1) Multiply $\mathbf{y}$ by $\mathbf{P}^{-1} = \mathbf{P}^t$

$$\mathbf{y}' = \mathbf{y}\mathbf{P}^t = 2\mathbf{m}'\mathbf{G}_{\mathbf{\Lambda}} - \mathbf{1} + 2\mathbf{e}_p.$$

2) For the corresponding syndrome $\mathbf{s}$, calculate the perturbation vector $\mathbf{e}_p$ and obtain $\mathbf{y}'' = \mathbf{y}' - 2\mathbf{e}_p$.
3) Recover the vector $\mathbf{m}$ as $(\mathbf{y}''+\mathbf{1})\frac{1}{2}\mathbf{G}_{\mathbf{\Lambda}}^{-\mathbf{1}}$, where

$$\mathbf{G}_{\mathbf{\Lambda}}^{-\mathbf{1}} = \begin{bmatrix} \mathbf{I_k} & -\frac{1}{2}\mathbf{A_{k\times(n-k)}} \\ \mathbf{0}_{(n-k)\times k} & \frac{1}{2}\mathbf{I_{n-k}} \end{bmatrix}. \tag{18}$$

IV. Secure One-Way Relaying Scheme Based on QC-LDPC Lattice Codes

A. One-Way Relay Channel

Let $\mathbf{x}_S$ and $\mathbf{x}_R$ denote the signals transmitted by the source and the relay, respectively. Denote the received signals at the relay and the destination by $\mathbf{y}_R$ and $\mathbf{y}_D$, respectively, which have the following forms

$$\mathbf{y}_R = h_{SR}\mathbf{x}_S + \mathbf{z}_R \tag{19}$$

$$\mathbf{y}_D = h_{SD}\mathbf{x}_S + h_{RD}\mathbf{x}_R + \mathbf{z}_D, \tag{20}$$

where $\mathbf{z}_R \sim \mathcal{N}(0, N_R)$, $\mathbf{z}_D \sim \mathcal{N}(0, N_D)$. Moreover, $h_{SR} = d_{SR}^{-\alpha_1}$, $h_{SD} = 1$, and $h_{RD} = d_{RD}^{-\alpha_2}$ are the path loss channel gains between source, relay, and destination. We assume the distance between the source and the destination to be 1 (other distances are normalized). We define d_{SR} and d_{RD} as the distance from source to relay and relay to destination, and α_1 and α_2 as their corresponding path-loss exponents. We also consider P_S and P_R as the constraints for the average powers of the source and the relay transmissions, respectively. To the best of our knowledge, the capacity of this channel, in its general form, is unknown. However, some DF schemes are available, like the one which is proposed in [32], that achieve the following inner bound:

$$R \leq \frac{1}{2}\min\left\{\log_2\left(1+\frac{h_{SR}^2 P_S E\left\{\mathbf{x}_S^2\right\}}{N_R}\right), \log_2\left(1+\frac{h_{SD}^2 P_S E\left\{\mathbf{x}_S^2\right\} + h_{RD}^2 P_R E\left\{\mathbf{x}_R^2\right\}}{N_D}\right)\right\}. \tag{21}$$

In the rest of this section, we present a secure practical block Markov encoding scheme for the one-way relay channel based on QC-LDPC lattice codes. The employed lattice decomposition method in this paper is proposed in [6] for LDLCs that achieves the decode-and-forward bound theoretically. Due to the structural differences between QC-LDPC lattices and LDLCs, as well as, differences between our shaping methods and theirs, and moreover due to the added security feature in this paper, all steps of this scheme are rephrased for QC-LDPC lattice codes. To the best of our knowledge, there is no secure lattice based relaying scheme in the litrature similar to the one proposed in this paper. Indeed, the security feature is lacked in all perevious similar schemes [4]–[8].

We employ doubly-nested lattice codes in which $\Lambda_S^s \subset \Lambda_S^c$ are the shaping and coding lattices, respectively. Thus, the considered codebooks are $\mathcal{C}_S = \Lambda_S^c \cap \mathcal{V}(\Lambda_S^s)$. We also assume that $\sigma^2(\Lambda_S^s) = h_{SR}P_S$. There is another lattice, which is referred to as *meso-lattice*, that partitions the lattice codebook into lower-rate constituent codebooks [6]. All above lattices are nested as $\Lambda_S^s \subset \Lambda_m \subset \Lambda_S^c$. The resolution codebook is $\mathcal{C}_S^{(r)} = \Lambda_S^c \cap \mathcal{V}(\Lambda_m)$ and the vestigial codebook is $\mathcal{C}_S^{(v)} = \Lambda_m \cap \mathcal{V}(\Lambda_S^s)$. Let $R_S, R_S^{(r)}, R_S^{(v)}$ be the rates of $\mathcal{C}_S, \mathcal{C}_S^{(r)}, \mathcal{C}_S^{(v)}$, respectively. Then, we have $R_S = R_S^{(r)} + R_S^{(v)}$. In the preceding code construction, every full-rate codeword has a unique decomposition as a modulo sum of resolution and vestigial codewords.

B. Decomposition of QC-LDPC Lattice Codebooks

Let $\mathbf{b} \in \mathbb{Z}^n$ be the information vector, where each element b_i of $\mathbf{b}$ is drawn from finite constellations $\{-L_i/2, \ldots, (L_i/2)-1\}$ and $\{0, \ldots, L_i - 1\}$ for hypercube shaping and nested lattice shaping, respectively. The i^{th} element of the resolution component $\mathbf{b}_r$ is

$$b_i^{(r)} = b_i \pmod{L_i^{(r)}}, \tag{22}$$

where $L_i = \beta L_i^{(r)}$, for some $\beta \in \mathbb{Z}$. Thus, the i^{th} element of $\mathbf{b}^{(r)}$ lies in the finite constellation $\mathcal{L}_i^{(r)} = \left\{0, \ldots, L_i^{(r)} - 1\right\}$ and the rate of the obtained codebook $R^{(r)}$ can be acquired via Equation (1) and the amount of $L_i^{(r)}$'s.

The vestigial component is defined as follows

$$\mathbf{b}^{(v)} = \mathbf{b} - \mathbf{b}^{(r)}. \tag{23}$$

If the employed shaping method is hypercube shaping, it can be shown that the i^{th} element of $\mathbf{b}^{(v)}$ lies in the following finite constellation

$$\mathcal{L}_i^{(v)} = \left\{\frac{-\beta}{2}L_i^{(r)}, \frac{(-\beta+2)}{2}L_i^{(r)}, \ldots, \frac{(\beta-2)}{2}L_i^{(r)}\right\}. \tag{24}$$

If the employed shaping method is nested lattice shaping, the i^{th} element of $\mathbf{b}^{(v)}$ lies in the finite constellation $\left\{0, L_i^{(r)}, 2L_i^{(r)}, \ldots, (\beta-1)L_i^{(r)}\right\}$. The rate of the vestigial codebook is approximately $R^{(v)} = \log_2(\beta)$. Due to the aforementioned assumptions, each codeword $\mathbf{x} = \mathcal{E}(\mathbf{b})$ decomposes into its resolution component $\mathbf{x}^{(r)} = \mathcal{E}(\mathbf{b}^{(r)})$ and its vestigial component $\mathbf{x}^{(v)} = \mathcal{E}(\mathbf{b}^{(v)})$ as $\mathbf{x} = \mathbf{x}^{(r)} \oplus \mathbf{x}^{(v)} = \mathbf{x}^{(r)} + \mathbf{x}^{(v)} + (1, \ldots, 1)$.

C. Power-Constrained Decomposition of QC-LDPC Lattice Codebooks

Given the information vector b, the shaped lattice codeword is $\mathbf{x}' = \mathcal{E}(\mathbf{b} - \mathbf{sL})$, where $\mathbf{s}$ is given in (6) and (7), for hypercube shaping and nested lattice shaping, respectively. We shape the resolution component $\mathbf{b}^{(r)}$ to $\mathbf{b}'^{(r)}$ in such a way that the decomposition of the lattice codebook remains linear

$$b_i'^{(r)} = \mathrm{smod}(b_i, L_i^{(r)}) - s_i^{(r)}L_i^{(r)}, \tag{25}$$

where b_i and $b_i^{\prime(r)}$ are the i^{th} elements of $\mathbf{b}$ and $\mathbf{b}^{\prime(r)}$, respectively, and

$$\operatorname{smod}(x, L) = \begin{cases} \bar{x} = x \pmod{L}, & \text{if } \bar{x} < \frac{L}{2}, \\ x \pmod{L} - L, & \text{otherwise.} \end{cases} \tag{26}$$

We choose the elements of $\mathbf{s}^{(r)}$ according to

$$s_i^{(r)} = \left\lfloor \frac{1}{L_i^{(r)}} \left(b_i^{(r)} + \frac{1}{2} \sum_{j=1}^{k} P_{j,i} b_j^{(r)} \right) \right\rfloor, \quad i = 1, \ldots, n, \tag{27}$$

for hypercube shaping. For nested lattice shaping, we consider $b_i^{\prime(r)} = b_i \pmod{L_i^{(r)}} - s_i^{(r)} L_i^{(r)}$, where $\mathbf{s}^{(r)}$ is given by (7). Indeed, the smod function is regular modulo operation, when the employed shaping method is nested lattice shaping. Then, the shaped resolution component is given by $\mathbf{x}^{\prime(r)} = \mathcal{E}(\mathbf{b}^{\prime(r)})$. We map the vestigial integer vector $\mathbf{b}^{(v)}$ to $\mathbf{b}^{\prime(v)}$ as follows

$$\mathbf{b}^{\prime(v)} = \mathbf{b}^{\prime} - \mathbf{b}^{(r)} = \mathbf{b}^{(v)} - \mathbf{s}\mathbf{L}, \tag{28}$$

where $\mathbf{s}$ is given in (6) and (7), for hypercube shaping and nested lattice shaping, respectively. Using this decomposition gives us $\mathbf{b}^{\prime} \neq \mathbf{b}^{\prime(r)} + \mathbf{b}^{\prime(v)}$ in general. However, the decomposition preserves componentwise modulo linearity, that is, $\mathbf{b}_i^{\prime} \pmod{L_i} = \mathbf{b}_i^{\prime(r)} \pmod{L_i^{(r)}} + \mathbf{b}_i^{\prime(v)} \pmod{L_i}$. Then, the vestigial codeword is $\mathbf{x}^{\prime(v)} = \mathcal{E}(\mathbf{b}^{\prime(v)})$ and we have $\mathbf{x}^{\prime} = \mathbf{x}^{(r)} \oplus \mathbf{x}^{\prime(v)}$. As before, the vestigial lattice codeword $\mathbf{x}_v^{\prime}$ does not need to fulfil any power constraint. The original information vectors $\mathbf{b}, \mathbf{b}^{(v)}$ can be recovered from $\mathbf{b}^{\prime}, \mathbf{b}^{\prime(v)}$ by using the proposed MOD algorithm in [7] with $\mathbf{L} = (L_1, \ldots, L_n)$. Similarly, the resolution information vector $\mathbf{b}^{(r)}$ can be recovered from $\mathbf{b}^{\prime(r)}$ by using MOD algorithm with $\mathbf{L}^{(r)} = (L_1^{(r)}, \ldots, L_n^{(r)})$.

D. Encoding and Decoding in Secure One-Way Relay Networks

In the rest of this section, we present the implementation of a secure encoding-decoding scheme over one-way relay networks using QC-LDPC lattice codes which is based on the proposed framework in [6, Section IV-E] for LDLCs and the proposed secret key scheme in [25]. Next, we discuss our decoding scheme at the destination. We assume that the source S is using QC-LDPC lattice codes in its transmissions. We assume that the i^{th} element of $\mathbf{b}_S$ is chosen from a constellation of size L_S. The i^{th} element of the resolution codewords are selected from a constellation of size $L_i^{(r)}$, where $L_i^{(r)}$ divides $L_{S,i}$ [6].

First, we describe the encoding steps. For $t = 1, \ldots, T$, let $\mathbf{m}[t]$ denote the plaintext of source S at block t which is intended to be sent to destination D and it should be unrevealed for the relay R. Meanwhile, the relay should facilitate the communication between S and D. It should be able to decode the received information from the source and forward its resolution component without knowing the content of the message. We assume that the matrix $\mathbf{H}_{qc}\mathbf{P}$ is given to the relay, but the value of perturbation vector $\mathbf{e}_p[t]$, for $t = 1, \ldots, T$, is only known by S and D.

Let $\mathbf{m} = \mathbf{m}[t] \in \mathbb{Z}^n$ be the plaintext, where each element m_i of $\mathbf{m}$ is drawn from finite constellations $\{-(L_i - 2)/2, \ldots, (L_i/2) - 2\}$ and $\{1, \ldots, L_i - 2\}$ for hypercube shaping and nested lattice shaping, respectively. For a given secret value $\mathbf{e}_p$, consider $\mathbf{e}_p^{\prime} = \mathbf{e}_p - 4\boldsymbol{\alpha}\mathbf{I}_n$, in which the vector $\boldsymbol{\alpha}$ will be obtained as follows.

We choose $\boldsymbol{\alpha}$ such that the components of the vector $\mathbf{w}_p = \mathbf{e}_p^{\prime}\mathbf{G}_{\Lambda}^{-1}$ lie in the interval $[-1, 1]$, i.e. $|w_{p,i}^{\prime}| \leq 1$, for $i = 1, \ldots, n$. To this end, we need to solve the following system of linear equations

$$(w_{p,1}^{\prime}, \ldots, w_{p,n}^{\prime}) = (e_{p,1}^{\prime}, \ldots, e_{p,n}^{\prime}) \begin{bmatrix} \mathbf{I}_k & -\frac{1}{2}\mathbf{A}_{k\times(n-k)} \\ \mathbf{0}_{(n-k)\times k} & \frac{1}{2}\mathbf{I}_{n-k} \end{bmatrix}, \tag{29}$$

by choosing an integer vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ such that $|w_{p,i}^{\prime}| \leq 1$ for $i = 1, \ldots, n$. From (29), we have the following equations

$$w_{p,i}^{\prime} = \begin{cases} e_{p,i} - 4\alpha_i, & i = 1, \ldots, k \\ \frac{1}{2}(e_{p,i} - 4\alpha_i) + \sum_{j=1}^{k} A_{j,i} e_{p,j}^{\prime}, & i = k+1, \ldots, n. \end{cases} \tag{30}$$

By choosing $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$, we have $e_{p,i}^{\prime} = e_{p,i}$ and $|w_{p,i}^{\prime}| = |e_{p,i}| \leq 1$, for $i = 1, \ldots, k$. For $i = k+1, \ldots, n$, we have the following inequality

$$\frac{e_{p,i}}{4} - \frac{1}{2} - \frac{1}{4}\sum_{j=1}^{k} A_{j,i} e_{p,j} \leq \alpha_i \leq \frac{e_{p,i}}{4} + \frac{1}{2} - \frac{1}{4}\sum_{j=1}^{k} A_{j,i} e_{p,j}.$$

This interval contains only one integer number which is the unique solution

$$\alpha_i = \left\lfloor \frac{1}{4} \left(e_{p,i} - \sum_{j=1}^{k} A_{j,i} e_{p,j} \right) \right\rfloor. \tag{31}$$

Given $\mathbf{e}_p^{\prime}$, then $\mathbf{e}_p$ can be obtained by computing the components of $\mathbf{e}_p^{\prime}$ modulo 4. Now, we consider $\mathbf{b}_S[t]$ as $\mathbf{b}_S[t] = \mathbf{m}[t] + \mathbf{e}_p^{\prime}\mathbf{G}_{\Lambda}^{-1}$ and its corresponding lattice vector as $\mathbf{x}_S[t] = \mathcal{E}\left(\mathbf{b}_S[t]\right)\mathbf{P}$.

For $t = 2, \ldots, T$, the transmitted signals by the source S is $\sqrt{P_S}\mathbf{x}_S^{\prime}[t]$. The matrix $\mathbf{H}_{qc}\mathbf{P}$ is given to the relay from which it obtains an equivalent generator matrix $\mathbf{G}_{\Lambda}^{\prime} = \mathbf{T}\mathbf{G}_{\Lambda}\mathbf{P}$ for the lattice, where $\mathbf{T}$ is a unimodular matrix (an integer matrix with determinant ± 1). After decoding, the relay uses the generator matrix $\mathbf{G}_{\Lambda}^{\prime}$ for re-encoding the resolution component of the received lattice vector. During the time interval t, where $2 \leq t \leq T$, the relay receives the signal from S at t^{th} block while it is transmitting the resolution component of the decoded codeword $\sqrt{P_R}\mathbf{x}_R^{\prime(r)}[t-1]$. During the block $t = 1$, the relay transmits nothing and at block $t = T+1$, the source receive the resolution information $\sqrt{P_R}\mathbf{x}_R^{\prime(r)}[T]$ from the relay.

Next, we describe the decoding steps. The decoding occurs in three phases.

Phase 1: Using the parity check matrix $\mathbf{H}_{qc}\mathbf{P}$, the relay decodes the codeword $\mathbf{x}_S^{\prime}[t]$ by using its received signal at the t^{th} block

$$\mathbf{y}_R[t] = \sqrt{P_S} h_{SR} \mathbf{x}_S^{\prime}[t] + \mathbf{z}_R[t]. \tag{32}$$

For a given source vector $\mathbf{x}_S^{\prime}[t] = 2\mathbf{b}_S^{\prime}[t]\mathbf{G}_{\Lambda}\mathbf{P} - (1, \ldots, 1)$, there exists a vector $\mathbf{b}_{S,1}^{\prime}[t]$ such that $2\mathbf{b}_S^{\prime}[t]\mathbf{G}_{\Lambda}\mathbf{P} - (1, \ldots, 1) = 2\mathbf{b}_{S,1}^{\prime}[t]\mathbf{G}_{\Lambda}^{\prime} - (1, \ldots, 1)$ which implies $\mathbf{b}_S^{\prime}[t]\mathbf{G}_{\Lambda}\mathbf{P} = \mathbf{b}_{S,1}^{\prime}[t]\mathbf{T}\mathbf{G}_{\Lambda}\mathbf{P}$. Thus, we have $\mathbf{b}_S^{\prime}[t] = \mathbf{b}_{S,1}^{\prime}[t]\mathbf{T}$ and consequently

$$\begin{aligned} \mathbf{b}_S^{(r)}[t] &= \operatorname{smod}(\mathbf{b}_S^{\prime}, \mathbf{L}^{(r)}) = \operatorname{smod}(\mathbf{b}_{S,1}^{\prime}[t]\mathbf{T}, \mathbf{L}^{(r)}) \\ &= \operatorname{smod}(\mathbf{b}_{S,1}^{(r)}[t]\mathbf{T}, \mathbf{L}^{(r)}). \end{aligned} \tag{33}$$

Using the QC-LDPC lattice decoding which is denoted by $\text{DEC}_{\text{LDPCL}}(\mathbf{y}, \sigma^2)$ (we use $\mathbf{y}$ and σ^2 to estimate LLR vector in (12), the relay estimates $\mathbf{b}'_{S,1}[t]$ as follows

$$\hat{\mathbf{x}}'_R[t] = \hat{\mathbf{x}}'_S[t] = \text{DEC}_{\text{LDPCL}}\left(\frac{\mathbf{y}_R[t]}{\sqrt{P_S}h_{SR}}, \frac{N_R}{\sqrt{P_S}h_{SR}}\right),$$
$$\hat{\mathbf{b}}'_R[t] = \hat{\mathbf{b}}'_{S,1}[t] = \left\lfloor \mathcal{D}\left(\hat{\mathbf{x}}'_R[t]\right)\mathbf{G}'^{-1}_{\Lambda}\right\rceil, \quad (34)$$

where $\mathcal{D}(x_1, \ldots, x_n) = 0.5 \times (x_1 + 1, \ldots, x_n + 1)$. Then, the resolution information vector of $\hat{\mathbf{b}}'_R[t]$ can be obtained by applying smod function in (26) as follows

$$\hat{b}^{(r)}_{R,i} = \text{smod}\left(\hat{b}'_{R,i}, L^{(r)}_i\right). \quad (35)$$

Using the shaping methods, the relay maps $\hat{\mathbf{b}}^{(r)}_R[t]$ to $\hat{\mathbf{b}}'^{(r)}_R[t]$

$$\hat{\mathbf{b}}'^{(r)}_R[t] \;=\; \hat{\mathbf{b}}^{(r)}_R[t] - \mathbf{s}_R\mathbf{L}^{(r)}, \quad (36)$$

where $\mathbf{s}_R$ is given in (27) and (7) for hypercube shaping and nested lattice shaping, respectively. Then, the shaped lattice codeword is $\hat{\mathbf{x}}'^{(r)}_R[t] = \mathcal{E}\left(\hat{\mathbf{b}}'^{(r)}_R[t]\right)$. During block $t+1$, the relay transmits $\sqrt{P_R}\hat{\mathbf{x}}'^{(r)}_R[t]$.

Phase 2: In this phase, destination node decodes the resolution codeword $\mathbf{x}^{(r)}_S$ by using its received signal in block $t+1$

$$\mathbf{y}'_D[t+1] = h_{RD}\sqrt{P_R}\hat{\mathbf{x}}'^{(r)}_R[t] + h_{SD}\sqrt{P_S}\mathbf{x}'_S[t+1] + \mathbf{z}_D[t+1].$$

Giving the scaled version of $\mathbf{y}'_D[t+1]$ to LDPC lattice decoder yields

$$\tilde{\mathbf{b}}'^{(r)}_{S,1}[t] = \left\lfloor \mathcal{D}\left(\text{DEC}_{\text{LDPCL}}\left(\frac{\mathbf{y}'_D[t+1]}{\gamma}, \frac{N_D}{\gamma}\right)\right)\mathbf{G}'^{-1}_{\Lambda}\right\rceil,$$

where $\gamma = h_{RD}\sqrt{P_R}$. Let

$$\mathbf{b}_1[t] = \text{smod}\left(\tilde{\mathbf{b}}'^{(r)}_{S,1}[t], \mathbf{L}^{(r)}\right), \quad (37)$$

$$\mathbf{b}_2[t] = \text{smod2mod}\left(\mathbf{b}_1[t], \mathbf{L}^{(r)}\right), \quad (38)$$

in which the function $\text{smod2mod}(x, L)$, that is defined next, is applied componentwise

$$\text{smod2mod}(x, L) = \begin{cases} x, & \text{if } 0 \le x \le \frac{L}{2} - 1, \\ x + L, & \text{if } \frac{-L}{2} \le x < 0. \end{cases} \quad (39)$$

Now, since the legitimate destination knows the the value of matrix $\mathbf{T}$, using Equation (33), the resolution information of source S will be obtained as follows

$$\tilde{\mathbf{b}}^{(r)}_S[t] = \mathbf{b}_2[t]\mathbf{T} \pmod{\mathbf{L}^{(r)}}. \quad (40)$$

Phase 3: In this phase, S decodes the vestigial codeword $\mathbf{x}^{(v)}_S$. First, it computes $\tilde{\mathbf{x}}^{(r)}_S[t] = \mathcal{E}(\tilde{\mathbf{b}}^{(r)}_S[t])\mathbf{P}$. Thus, $\tilde{\mathbf{x}}'^{(r)}_R[t-1]$ and $\tilde{\mathbf{x}}^{(r)}_S[t]$ are obtained from $\mathbf{y}'_D[t]$ and $\mathbf{y}'_D[t+1]$, respectively. Then, S subtracts $h_{SD}\sqrt{P_S}\left(\tilde{\mathbf{x}}^{(r)}_S[t] + (1, \ldots, 1) + h_{RD}\sqrt{P_R}\tilde{\mathbf{x}}'^{(r)}_R[t-1]\right)$ from $\mathbf{y}'_D[t]$ that yields

$$\mathbf{y}''_D[t] = h_{SD}\sqrt{P_S}\mathbf{x}'^{(v)}_S[t] + \mathbf{e}_D + \mathbf{z}_D[t], \quad (41)$$

where $\mathbf{e}_D$ is

$$\mathbf{e}_D = h_{SD}\sqrt{P_S}\left[\mathbf{x}^{(r)}_S[t] - \tilde{\mathbf{x}}^{(r)}_S[t]\right] + h_{RD}\sqrt{P_R}\left[\hat{\mathbf{x}}'^{(r)}_R[t-1] - \tilde{\mathbf{x}}'^{(r)}_R[t-1]\right]. \quad (42)$$

Then, S uses QC-LDPC lattice decoding to find

$$\tilde{\mathbf{b}}'^{(v)}_S[t] = \mathbf{L}^{(r)} \circ \left\lfloor \mathcal{D}\left(\text{DEC}_{\text{LDPCL}}\left(\mathbf{y}_D\mathbf{P}^t, \boldsymbol{\sigma}_D\right)\right)\mathbf{G}^{-1}_{\Lambda}\right\rceil, \quad (43)$$

where $\circ$ denotes the Hadamard product or entrywise product of vectors, $y_{D,i} = \frac{y''_{D,i}}{L^{(r)}_i h_{SD}\sqrt{P_S}}$ and $\sigma_{D,i} = \frac{N_D}{L^{(r)}_i h_{SD}\sqrt{P_S}}$. The vestigial information is $\tilde{\mathbf{b}}^{(v)}_S[t] = \text{smod}(\tilde{\mathbf{b}}'^{(v)}_S[t], \mathbf{L}_S)$.

Hence, the shaped and unshaped full-rate information vectors of S are $\tilde{\mathbf{b}}'_S[t] = \tilde{\mathbf{b}}^{(r)}_S[t] + \tilde{\mathbf{b}}'^{(v)}_S[t]$ and $\tilde{\mathbf{b}}_S[t] = \tilde{\mathbf{b}}^{(r)}_S[t] + \tilde{\mathbf{b}}^{(v)}_S[t]$, respectively. Using the secret parameter $\mathbf{e}'_p$, the destination obtains $\tilde{\mathbf{m}}[t]$ as $\tilde{\mathbf{m}}[t] = \tilde{\mathbf{b}}_S[t] - \mathbf{e}'_p\mathbf{G}^{-1}_{\Lambda}$

Note that the above decoding process is presented for the case that the employed shaping method is hypercube shaping. When the employed shaping is nested lattice shaping, this decoding steps are still valid by changing smod function into regular modulo operation. This is due to the fact that, the components of lattice vectors, given as the inputs for hypercube shaping and nested lattice shaping, are drawn from different sets. For hypercube and nested lattice shading methods we use the sets $\{-L/2, \ldots, L/2-1\}$ and $\{0, \ldots, L-1\}$, respectively.

V. Numerical Results

In the simulations, we have used binary QC-LDPC codes with $(n, k) = (1000, 850), (5000, 4250)$ as underlying codes, where n and k are the codeword length and the dimension of the code, respectively. Symbol error rate (SER) performance of QC-LDPC lattice codes are plotted against the sum power at source and the relay, i.e., $P_S E\left\{x^2_S\right\} + P_R E\left\{x^2_R\right\}$. We have considered $d_1 = d_{SR} = 0.9$, $d_2 = d_{RD} = 0.1$ and $d_{SD} = 1$. The path loss exponents are $\alpha_1 = 1$, $\alpha_2 = 2$. The variances of the noise at the relay and destination are $N_r = N_d = 0\text{dB}$. The maximum number of iterations in each step of the decoding is assumed to be 50. We have considered $L_i = 8$, for $i = 1, \ldots, n$. Thus, for the cases in which we have employed hypercube shaping, based on (1), the corresponding rate is 3 bits/integer. For employing nested lattice shaping, we consider $L_1 = \cdots = L_k = 8$ and $L_{k+1} = \cdots = L_n = 4$. Then, based on (1), the corresponding rate is 2.85 bits/integer. In order to achieve these rates, according to (21), the total required powers are $P_1 = P_S E\left\{\mathbf{x}^2_S\right\} + P_R E\left\{\mathbf{x}^2_R\right\} \ge 51.88 = 17.15\text{dB}$, and $P_2 \ge 41.2 = 16.15\text{dB}$, respectively.

In Fig. 1, we have presented SER variation versus sum of transmission powers for both nested-lattice shaping and hypercube shaping. In [4], the implementation of block Markov encoding was proposed for LDLCs. We have considered h_{SD}, h_{SR}, h_{RD} and other parameters similar to their corresponding values in [4]. The SER performance of an LDLC lattice code with dimension 1000 and rate 2.78, which is obtained by employing nested lattice shaping, at 10^{-4} is 3.77dB away from its corresponding DF inner bound, which is 15.77dB. We observe that using the proposed scheme in this paper, the SER performance of a QC-LDPC lattice code of length 1000 at 10^{-4} is 4dB away from its corresponding DF inner bound. Using the proposed scheme in [7] and [8], the SER performance of a QC-LDPC lattice code of length 1000 at 10^{-4} is 4.5dB away from its corresponding DF inner bound. Thus, in addition to the fact that the new scheme has the same complexity as those proposed in [7], [8], it outperforms both of them in terms

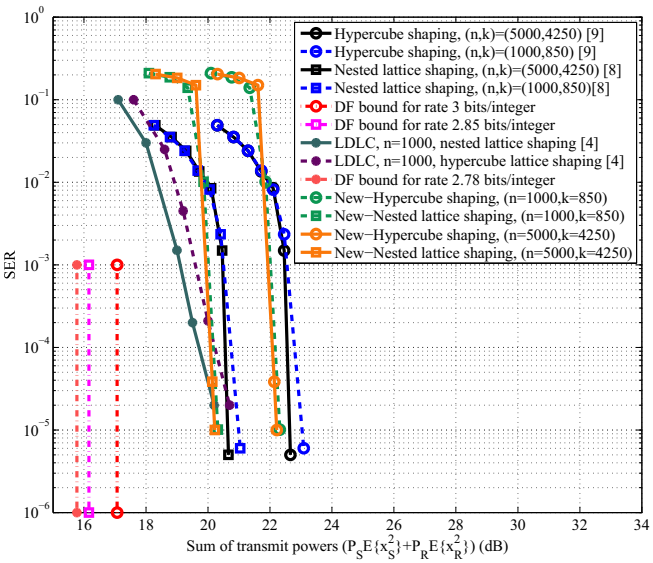

Fig. 1: SER of QC-LDPC lattice codes and LDLCs over the one-way relay channel.

of error performance. However, the proposed scheme for LDLCs have about 0.23dB better performance compared to our scheme. This is a natural result, due to the better SER performance of LDLCs compared to QC-LDPC lattice codes, over AWGN channels and also a bit difference in the considered parameters. The decoding complexity of LDLCs, by using proposed decoder in [33], is at least 24 times more than the decoding complexity of QC-LDPC lattices. Indeed, the decoding complexity of a QC-LDPC lattice of dimension 1000 is equivalent to the decoding complexity of an LDLC with dimension 24000. Results of Fig. 1 show that the increase in the dimension of the lattice can decrease the gap between DF bound and the performance curve. Using a QC-LDPC lattice code of dimension 5000 instead of dimension 1000 makes about 0.1dB improvement in the performance. This analysis also indicates the efficiency of our proposed scheme compared to its counterparts [4].

VI. Cryptanalysis

The main advantage of the proposed scheme is providing security against an honest but curious relay and at the same time employing its potential to improve the communication quality between a source and a destination. For the brute force attack on the relay that searches all possible secret keys, the number of block diagonal permutation matrices (14) is $(b!)^x$, where $x = n/b$. Considering $b = 100$ and $x = 10$, the lattice dimension n is high enough to avoid this attack. Moreover, the number of different error patterns $\mathbf{e}_p$ is given by 2^{n-k}, which is equal to 2^{150} for the lattice of dimension 1000 considered in the simulations. Therefore, the proposed scheme is resistant against the brute force attack. Furthermore, the resistance of the schemes proposed in [24] and [25] have already been shown against chosen plaintext attacks, e.g. Rao-Nam and Struik-Tilburg attacks. In the sequel, we analyze the security of our proposed scheme against Rao-Nam attack.

The received vector at the relay is given in (32) from which the vector $\mathbf{x}'_S[t] = 2\mathbf{b}'_S[t]\mathbf{G}_\Lambda\mathbf{P} - (1,\dots,1)$ is obtained. It is noteworthy that the probability of decoding failure in the relay is negligible, because the quality of the channel in which the relay is working is desirable. Indeed, the position of the relay is optimized to guarantee the quality of the channel. Otherwise, the failure in the first phase of decoding process results in the connection outage between the source and the destination nodes. Thus, we have

$$\begin{aligned}\mathbf{x}'_S[t] &= 2\mathbf{b}'_S[t]\mathbf{G}_\Lambda\mathbf{P} - (1,\dots,1)\\ &= 2(\mathbf{b}_S[t] - \mathbf{sL})\mathbf{G}_\Lambda\mathbf{P} - (1,\dots,1)\\ &= 2(\mathbf{m}[t] - \mathbf{sL} + \mathbf{e}'_p\mathbf{G}_\Lambda^{-1})\mathbf{G}_\Lambda\mathbf{P} - (1,\dots,1)\\ &= 2\mathbf{m}'\mathbf{G}'_\Lambda - (1,\dots,1) + 2\mathbf{e}'_p\mathbf{P},\end{aligned}$$

where $\mathbf{G}'_\Lambda = \mathbf{G}_\Lambda\mathbf{P}$ and $\mathbf{m}' = \mathbf{m}[t] - \mathbf{sL}$. Let $\mathbf{m}'_1$ and $\mathbf{m}'_2$ be two plaintexts differing in only one position, that is, $\mathbf{m}'_1 - \mathbf{m}'_2 = \mathbf{u}^i = (0,\dots,0,m_{1i} - m_{2i},0,\dots,0)$ with a single nonzero component $m'_{1i} - m'_{2i}$ in the i-th position. We have

$$\begin{aligned}\mathbf{x}'_1 &= 2\mathbf{m}'_1\mathbf{G}'_\Lambda - (1,\dots,1) + 2\mathbf{e}'_{1,p}\mathbf{P},\\ \mathbf{x}'_2 &= 2\mathbf{m}'_2\mathbf{G}'_\Lambda - (1,\dots,1) + 2\mathbf{e}'_{2,p}\mathbf{P}.\end{aligned}$$

It follows that

$$\begin{aligned}\mathbf{x}'_1 - \mathbf{x}'_2 &= 2\mathbf{u}^i\mathbf{G}'_\Lambda + 2(\mathbf{e}'_{1,p} - \mathbf{e}'_{2,p})\mathbf{P}\\ &= 2(m'_{1i} - m'_{2i})\mathbf{g}'_i + 2(\mathbf{e}'_{1,p} - \mathbf{e}'_{2,p})\mathbf{P},\end{aligned}$$

where $\mathbf{g}'_\mathbf{i}$ is the i-th row of the $\mathbf{G}'_\Lambda$. Thus, if the majority of the bits of the vector $\mathbf{x}'_1 - \mathbf{x}'_2$ are those of $\mathbf{g}'_i$, then $\mathbf{x}'_1 - \mathbf{x}'_2$ may be considered as an estimate of $\mathbf{g}'_i$. This could happen if the Hamming weight of $2(\mathbf{e}'_{1,p} - \mathbf{e}'_{2,p})$ is small. However, a chosen-plaintext attack can succeed only when the ratio of the Hamming weight of $\mathbf{e}'_p$ over n is small and it will not if the average weight of the vector is approximately $n/2$ [24]. Based on the computation of the perturbation vectors, the Hamming weight of the generated perturbation vector $\mathbf{e}_p$ is at most n and is approximately $n/2$ on average [25]. It remains to prove that the Hamming weight of $\mathbf{e}'_p$ is approximately $n/2$ on average, too. Using the assumptions, $\mathbf{e}'_p = \mathbf{e}_p - 4\boldsymbol{\alpha}\mathbf{I}_n$, where α is given in (31). Since $\mathbf{e}'_p$ and $\mathbf{e}_p$ are equal in the first k positions, the average weight in the first k positions is $k/2$ due to the uniform distribution of non-zero components of $\mathbf{e}_p$. Here, the constraint on the design of QC-LDPC lattices is helpful implying that $k \geq 0.85n$ [29]. This gives a lower bound on the average Hamming weight of $\mathbf{e}'_p$ as $k/2 = 0.42n$ which is close to $n/2$. Next we give a more precise analysis of the Hamming weight of $\mathbf{e}'_p$. Define the random variable $W = \sum_{i=k+1}^{n} \mathbf{1}_{e'_{p,i}}$, in which $\mathbf{1}_{e'_{p,i}} = 1$ if $e'_{p,i} \neq 0$ and $\mathbf{1}_{e'_{p,i}} = 0$ otherwise. Then the average Hamming weight of $\mathbf{e}'_p$ is $k/2 + \mathbb{E}(W)$ and $\mathbb{E}(W) = \sum_{i=k+1}^{n} \Pr\{e'_{p,i} \neq 0\} = \sum_{i=k+1}^{n} [1 - \Pr\{e'_{p,i} = 0\}]$. For $i = k+1,\dots,n$, we have $e'_{p,i} = 0$ if and only if $e_{p,i} = 4\alpha_i$ which is possible if and only if $\alpha_i = 0$. Hence, it is enough to compute $\Pr\{\alpha_i = 0\}$, for $i = k+1,\dots,n$. From $\alpha_i = 0$ we obtain the following inequalities

$$-\frac{1}{2} < \frac{1}{4}e_{p,i} - \frac{1}{4}\sum_{j=1}^{k} A_{j,i}e_{p,j} < \frac{1}{2}, \qquad (44)$$

which is equivalent to to the inequality $e_{p,i} - 2 < \sum_{j=1}^{k} A_{j,i}e_{p,j} < e_{p,i} + 2$. The left side of this inequality is always true, because $e_{p,i} - 2$ is a negative number and

$\sum_{j=1}^{k} A_{j,i} e_{p,j}$ is always a non-negative number. In order to make the right side of this inequality invalid, it suffices to choose the underlying QC-LDPC code $\mathcal{C}$ such that the non-identity part of its systematic generator matrix, i.e., the matrix $\mathbf{A}$ in (3), has minimum column weight more than 3. This happens naturally, since the parity check matrix is sparse and its systematic generator matrix is definitely a dense matrix. Consequently, $\Pr\left\{e'_{p,i} \neq 0\right\} = 1$ for $i = k+1, \ldots, n$ and we have $\mathbb{E}(W) = n - k$. We conclude that almost all $e'_{p,i}$s, for $i = k+1, \ldots, n$, are non-zero and the average Hamming weight of $\mathbf{e}'_p$ is $(n-k) + k/2$. Hence, a lower bound on the complexity of this attack is $\binom{n}{n-\frac{k}{2}} \geq \binom{n}{0.58n}$ which is of order $O(2^{n/2})$ and makes the attack infeasible, as n grows. More attacks can be considered like the ones in [25], but we cannot provide them here due to the lack of space. The proposed scheme is vulnerable to active attacks like denial-of-service (DoS) attack, because any intervention of an attacker that causes the decoding failure at the relay results in the connection outage between source and destination.

VII. Conclusions

In this paper, we have designed a new full-duplex one-way relaying scheme based on QC-LDPC lattice codes. The proposed scheme outperforms the available preceding scheme based on QC-LDPC lattice codes in terms of symbol error performance. Next, we have combined a Rao-Nam like encryption with the proposed DF relaying scheme. The main reason for considering an additional secrecy constraint is to provide protection against an honest but curious relay. Indeed, while the relay should decode the source message and improve the communication quality between the source and the destination, it should be fully ignorant about the message content. Some chosen plaintext attack scenarios and recent attacks on the Rao-Nam like schemes have been considered over the proposed scheme and it has been shown that our proposed scheme withstand all known types of cryptanalytic attacks. Furthermore, the scheme is efficient due to its high information rate and low encryption and decryption overheads.

References

[1] "Cisco visual networking index: Forecast and methodology, 2016-2021," https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html, note =, Sept. 2017.

[2] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. on Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.

[3] N. Yiwei and N. Devroye, "Lattice codes for the gaussian relay channel: Decode-and-forward and compress-and-forward," *IEEE Trans. on Inform. Theory*, vol. 59, no. 8, pp. 4927–4948, Aug. 2013.

[4] N. S. Ferdinand, M. Nokleby, and B. Aazhang, "Low density lattice codes for the relay channel," in *IEEE International Conference on Commun. (ICC), 2013*, Jun. 2013, pp. 3035–3040.

[5] M. Nokleby and B. Aazhang, "Lattice coding over the relay channel," in *IEEE International Conference on Commun. (ICC), 2011*, Jun. 2011, pp. 1–5.

[6] N. S. Ferdinand, M. Nokleby, and B. Aazhang, "Low-density lattice codes for full-duplex relay channels," *IEEE Trans. on Wireless Commun.*, vol. 14, no. 4, pp. 2309–2321, Apr. 2015.

[7] H. Khodaiemehr, D. Kiani, and M.-R. Sadeghi, "LDPC lattice codes for full-duplex relay channels," *IEEE Trans. on Commun.*, vol. 65, no. 2, pp. 536–548, Feb. 2017.

[8] ——, "One-level LDPC lattice codes for the relay channels," in *2015 Iran Workshop on Commun. and Inf. Theory (IWCIT)*, May 2015, pp. 1–6.

[9] H. Khodaiemehr, M.-R. Sadeghi, and D. Panario, "Construction of full-diversity 1-level LDPC lattices for block-fading channels," in *2016 IEEE International Symposium on Inf. Theory (ISIT)*, Jul. 2016, pp. 2714–2718.

[10] M. O. Hasna and M.-S. Alouini, "End-to-end performance of transmission systems with relays over Rayleigh-fading channels," *IEEE Trans. Wireless Commun.*, vol. 2, no. 6, pp. 1126–1131, Nov. 2003.

[11] L. J. Rodrguez, N. H. Tran, and T. Le-Ngoc, "Performance of full-duplex AF relaying in the presence of residual self-interference," *IEEE J. on Selected Areas in Commun.*, vol. 32, no. 9, pp. 1752–1764, Sept. 2014.

[12] T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE Trans. on Wireless Commun.*, vol. 10, no. 9, pp. 3074–3085, Sept. 2011.

[13] D. W. K. Ng, E. S. Lo, and R. Schober, "Dynamic resource allocation in MIMO-OFDMA systems with full-duplex and hybrid relaying," *IEEE Trans. on Commun.*, vol. 60, no. 5, pp. 1291–1304, May 2012.

[14] E. da Silva, A. L. dos Santos, L. C. P. Albini, and M. N. Lima, "Identity-based key management in mobile ad hoc networks: techniques and applications," *IEEE Wireless Commun.*, vol. 15, no. 5, pp. 46–52, Oct. 2008.

[15] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[16] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. on Inf. Forensics and Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[17] C. Dang, L. J. Rodrguez, N. H. Tran, S. Shelly, and S. Sastry, "Secrecy capacity of the full-duplex AF relay wire-tap channel under residual self-interference," in *2015 IEEE Wireless Commun. and Networking Conference (WCNC)*, Mar. 2015, pp. 99–104.

[18] L. Elsaid, M. Ranjbar, N. Raymondi, D. H. N. Nguyen, N. H. Tran, and A. Mahamadi, "Full-duplex decode-and-forward relaying: Secrecy rates and optimal power allocation," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Jun. 2017, pp. 1–6.

[19] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, Dec. 2010, pp. 1–6.

[20] F. Oggier, P. Solé, and J. C. Belfiore, "Lattice codes for the wiretap gaussian channel: Construction and analysis," *IEEE Trans. on Inf. Theory*, vol. 62, no. 10, pp. 5690–5708, Oct. 2016.

[21] X. He and A. Yener, "Providing secrecy with lattice codes," in *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, Sept. 2008, pp. 1199–1206.

[22] K. Bagheri, M.-R. Sadeghi, and T. Eghlidos, "An efficient public key encryption scheme based on qc-mdpc lattices," *IEEE Access*, vol. 5, pp. 25 527–25 541, 2017.

[23] K. Bagheri, M.-R. Sadeghi, and D. Panario, "A non-commutative cryptosystem based on quaternion algebras," *Designs, Codes and Cryptography*, Dec. 2017. [Online]. Available: https://doi.org/10.1007/s10623-017-0451-4

[24] T. N. R. Rao and K. H. Nam, "A private-key algebraic-coded cryptosystem," *Advances in Cryptology, Crypto'86*, p. 3548, 1986.

[25] K. Bagheri, M.-R. Sadeghi, T. Eghlidos, and D. Panario, "A secret key encryption scheme based on 1-level QC-LDPC lattices," in *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, Sept. 2016, pp. 20–25.

[26] M. Aliasgari, M.-R. Sadeghi, and D. Panario, "Grobner bases for lattices and an algebraic decoding algorithm," *IEEE Trans. on Commun.*, vol. 61, no. 4, pp. 1222–1230, Apr. 2013.

[27] H. Khodaiemehr, M.-R. Sadeghi, and A. Sakzad, "Practical encoder and decoder for power constrained QC LDPC-lattice codes," *IEEE Trans. on Commun.*, vol. 65, no. 2, pp. 486–500, Feb. 2017.

[28] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*. New York: Springer, 1998.

[29] H. Khodaiemehr and D. Kiani, "Construction and encoding of QC-LDPC codes using group rings," *IEEE Trans. on Inf. Theory*, vol. 63, no. 4, pp. 2039–2060, Apr. 2017.

[30] S. J. Johnson, *Iterative Error Correction: Turbo, Low-Density Parity-Check and Repeat-Accumulate Codes*. Cambridge University Press, 2009.

[31] N. Sommer, M. Feder, and O. Shalvi, "Low-density lattice codes," *IEEE Trans. on Inf. Theory*, vol. 54, no. 4, pp. 1561–1585, Apr. 2008.

[32] T. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. on Inf. Theory*, vol. 25, no. 5, pp. 572–584, Sep. 1979.

[33] Y. Yona and M. Feder, "Efficient parametric decoder of low density lattice codes," in *IEEE International Symposium on Inf. Theory (ISIT), 2009*, Jun. 2009, pp. 744–748.