Block-MDS QC-LDPC Codes with Application to High-Dimensional Quantum Key Distribution

Lev Tauz, Debarnab Mitra, Jayanth Shreekumar, Murat Can Sarihan, Chee Wei Wong, and Lara Dolecek
Department of Electrical and Computer Engineering, University of California, Los Angeles, USA
email: {levtauz, debarnabucla, jayshreekumar98, mcansarihan, cheewei.wong, and dolecek}@ucla.edu

***Abstract*—High-dimensional quantum key distribution (QKD) is a popular protocol that provides information theoretically secure keys to multiple parties. Two important steps of QKD are 1) the information reconciliation (IR) step, where parties reconcile mismatches in generated keys through classical communication, and 2) the privacy amplification (PA) step, where parties distill their common key into a new secure key that the adversary has little to no information about. In general, these two steps have been abstracted as two distinct problems. In this work, we design our IR protocol to be aware of the PA step and utilize sampling to relax the requirement on the IR step without sacrificing the final key length of the PA step, allowing for more bits generated in key creation utilizing practical decoders. We provide a novel PA-aware LDPC code construction known as Block-MDS QC-LDPC codes that can utilize the relaxed requirement. We demonstrate through simulations that our technique of sampling can provide notable gains in successfully creating secret keys.**

2024 IEEE Information Theory Workshop (ITW) | 979-8-3503-4893-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/ITW61385.2024.10806945

I. Introduction and Motivation

Quantum communication technologies have been identified as a valuable component of upcoming 6G systems for both communication and computation [1], [2]. One important method in quantum communications is Quantum Key Distribution (QKD) which allows for secret key agreement between two parties (Alice and Bob) using quantum mechanical principles to guarantee security against eavesdroppers (Eve) [3]. QKD is an important tool in a future where quantum computers can break many of the cryptographic protocols we rely on today and, thus, has received significant research attention [4]–[8].

QKD can be broken down into 3 major steps: 1) Raw Key Generation: Alice and Bob generate keys from some quantum mechanical source and they have some measure about how much information Eve has about the keys; 2) Information Reconciliation (IR): Due to imperfections in the channel, Alice and Bob must reconcile the errors in their keys by communicating through a classical channel where Eve can eavesdrop; 3) Privacy Amplification (PA): Assuming the IR step was successful, Alice and Bob now distill their common key into a smaller key in order to remove any leaked information that Eve may have. In this paper, we investigate how the IR step can be improved with knowledge about the subsequent PA step in order to improve the overall performance of the QKD system. The main goal is to have a high *secret key rate* which is the expected ratio of the final key length in bits over the number of photons used to generate the keys [9], [10]. The secret key rate depends on the success probability of the IR step and the overall information provided to Eve.

To the best of our knowledge, many previous works have considered each step of the QKD process individually and have abstracted the problem into three separate problems [11]–[13]. In this work, we seek to create a PA-aware IR protocol for high-dimensional QKD, by relaxing the requirements of the IR step, thereby allowing it to succeed more often and increase the secret key rate. The key idea of our work is that the PA step will be removing redundant information from the common key reconciled during the IR step. As such, it seems unnecessary for the IR step to reconcile all the mismatches if redundant data will be removed during the PA step anyway. By requiring the IR step to *reconcile only a subset* of the key instead of the full key (essentially sampling the common key), we increase the probability that the IR step will succeed. This idea is similar to only decoding the systematic bits in classical channel coding setting. Additionally, our scheme is agnostic of the key generation and works for any high-dimensional quantum key generation and, thus, we abstract the information loss during key generation as will be discussed.

Our contributions are as follows. First, we demonstrate an efficient sampling technique in the IR step that causes no information loss for the PA step, thus relaxing the requirements for the IR step without sacrificing the final key length. Second, we construct PA-aware codes with Quasi-Cyclic Low Density Parity Check (QC-LDPC) codes which we term as *Block-MDS* QC-LDPC codes that work jointly with our sampling technique. While designed with QKD in mind, we hypothesize that Block-MDS QC-LDPC codes can have further uses in other areas where LDPC codes are prominent. Finally, we provide simulation results to demonstrate the benefits of our novel decoding technique and code design.

The rest of this paper is organized as follows. In Section II, we provide the preliminaries and the system model. In Section III, we demonstrate our novel sampling technique for privacy amplification. In Section IV, we provide the design of our novel Block-MDS QC-LDPC codes. Finally, we provide simulation results and concluding remarks in Section V.

Notation: $\mathbb{F}_q$ denotes a finite field of order q. For positive integers n and m, $\mathbb{F}_q^n$ ($\mathbb{F}_q^{n,m}$) denotes all vectors (matrices) of length n (size $n \times m$) with elements from $\mathbb{F}_q$. For random variables X and Y, $\mathcal{I}(X;Y)$ denotes the mutual information and $H(X)$ denotes the Shannon entropy. All logarithms are in base 2. For positive integers a and b, let $[a] = \{1, 2, \dots, a\}$ and $(a)_b = a \mod b$. Given two integers n and k such that $k \leq n$, $\binom{[n]}{k}$ denotes all subsets of $[n]$ of size k. For a vector $\mathbf{x}$ (matrix $\mathbf{H}$) of size n ($m \times n$) and set $\mathcal{S} \subseteq [n]$, we denote $\mathbf{x}_\mathcal{S}$ ($\mathbf{H}_\mathcal{S}$) as the subset of the elements (columns) of $\mathbf{x}$ ($\mathbf{H}$) indexed by $\mathcal{S}$. Let S_n denote the set of all permutations of the set $[n]$. Given two polynomials $f(x)$ and $g(x)$, $\gcd(f(x), g(x))$ is a polynomial of the highest possible degree that is a factor of both $f(x)$ and $g(x)$.

II. Background and Model

A. System Model

For the purposes of this work, QKD systems can be broken down into three major components: Key Generation, Information Reconciliation, and Privacy Amplification [9], [10]. We shall describe each of these steps and focus on the relevant components of each step.

1) *Key Generation:* We assume Alice and Bob generate high-dimensional raw keys, i.e., symbols in some alphabet. For example, they could use energy-time entanglement protocols [14]–[18]. The general idea of high-dimensional schemes is that entangled photons pairs are generated at the source and one member of the pair is sent to each user, who measures their photon. In principle, the measurements should be the same, allowing for both parties to extract keys. Yet, errors can still occur due to detector imperfections or interference from Eve. We abstract the key generation as follows.

Let $\mathbf{x} = \{x_1, \dots, x_N\}$, $x_i \in \mathbb{F}_q$ and $\mathbf{y} = \{y_1, \dots, y_N\}$, $y_i \in \mathbb{F}_q$ be the raw keys of length N recorded by Alice and Bob, respectively. Each pair (x_i, y_i) is generated by a pair of entangled photons. Due to the protocol, we can assume that the random variables $x_i, i \in [N]$ are independent and uniform on $\mathbb{F}_q$. Due to imperfections in the detectors, the raw keys may differ in some positions. For simplicity, we assume that the symbol mismatch can be modeled by a q-ary symmetric channel where the errors are independent, see [13]. As such, the conditional probability for x_i given y_i for $i \in [N]$ is $Pr(x_i|y_i) = 1 - p$ if $y_i = x_i$ otherwise $Pr(x_i|y_i) = \frac{p}{1-q}$ where p denotes the channel transition probability. Additionally, the adversary Eve may contain some information, possibly from the quantum channel, about the raw keys which we denote as $\mathcal{E}$. Since the keys are in the classical space, the information that the adversary has is classical and, thus, we focus on Shannon entropy as a measure of information.

2) *Information Reconciliation:* In this step, Alice and Bob reconcile the raw keys by communicating through a public channel which Eve has access to. Let $\mathbf{z}$ represent the data communicated between Alice and Bob which Eve can access. In this work, we consider single-round communication schemes which are equivalent to asymmetric Slepian-Wolf coding with side information at the receiver [12]. We employ a linear coset scheme where Alice encodes the data $\mathbf{x}$ using a matrix $\mathbf{H} \in \mathbb{F}_q^{M,N}$ into syndrome $\mathbf{z} = \mathbf{H}\mathbf{x}$ and transmits $\mathbf{z}$ to Bob. Bob then uses the syndrome $\mathbf{z}$ and the side information $\mathbf{y}$ in order to decode $\mathbf{x}$. If Bob successfully decodes, i.e., $\mathbf{x}$ is known to Bob, then the protocol proceeds to the next step. If Bob fails, then the algorithm stops and no key is generated. We assume that $\mathbf{H}$ is public.

3) *Privacy Amplification:* In this step, Alice and Bob start with a common key $\mathbf{x}$ since the IR step succeeded. Eve has information about $\mathbf{x}$ through $(\mathcal{E}, \mathbf{z})$ and Alice and Bob wish to distill $\mathbf{x}$ into a smaller key which is independent of $(\mathcal{E}, \mathbf{z})$. PA can be accomplished through the use of *universal hash functions* [19]. The length of the final key depends on the amount of information leaked from $(\mathcal{E}, \mathbf{z})$ and has to be subtracted. Assuming that the PA step incurs no further information leakage, the final key length can be written as $H(\mathbf{x}) - \mathcal{I}(\mathbf{x}; \mathcal{E}, \mathbf{z}) = H(\mathbf{x}|\mathcal{E}, \mathbf{z})$ where $H(\mathbf{x})$ represents the amount of information in the raw keys and $\mathcal{I}(\mathbf{x}; \mathcal{E}, \mathbf{z})$ represents the amount of information Eve knows about $\mathbf{x}$.

For a key distribution system, we consider the main measure of interest as the average number of generated bits in the final key per photon pair detected which is named the *secret key rate*. Thus, the secret key rate [9], [10] can be defined as

$$SKR = Pr(A)\frac{H(\mathbf{x}) - \mathcal{I}(\mathbf{x}; \mathcal{E}, \mathbf{z})}{N} \tag{1}$$

where A is the event that the IR step is successful and is necessary in the equation to account for wasted photons when the IR step fails. We note that the success probability of the IR step is highly dependent on not only the channel but the type of decoder used for the linear coset scheme.

B. LDPC code preliminaries

An LDPC code over $\mathbb{F}_q$ is defined by a sparse parity check matrix $\mathbf{H} \in \mathbb{F}_q^{M,N}$. For the coset scheme, LDPC codes can be decoded using a variant of the sum-product decoding algorithm specialized for the Slepian-Wolf problem (see [20] for more details). All simulations in this work utilize this decoder.

One method to construct an LDPC code is known as the scaled protograph-based method [21], [22]. This method starts with a small bipartite graph represented by a $\gamma \times \kappa$ base matrix of non-negative integers and the parity check matrix of the LDPC code is created by replacing each entry a by a summation of a scaled permutation matrices of size $z \times z$. We denote γ as the column weight, κ as the row weight, and z as the lifting factor. When the base matrix is the all-ones matrix and the permutation matrices are all circulant shift matrices, then the resultant LDPC code is known as a Type-1 Quasi-Cycli LDPC (QC-LDPC) code [23], [24]. For the rest of this paper, we shall focus on these types of codes. Thus, the parity check matrix of QC-LDPC codes can be written as

$$\mathbf{H} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} & \cdots & s_{1,\kappa}\mathbf{C}^{p_{1,\kappa}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} & \cdots & s_{2,\kappa}\mathbf{C}^{p_{2,\kappa}} \\ \vdots & & \ddots & \vdots \\ s_{\gamma,1}\mathbf{C}^{p_{\gamma,1}} & s_{\gamma,2}\mathbf{C}^{p_{\gamma,2}} & \cdots & s_{\gamma,\kappa}\mathbf{C}^{p_{\gamma,\kappa}} \end{bmatrix} \tag{2}$$

where $\mathbf{C}^p$ is a circulant shift matrix (CSM) of size $z \times z$ with a one at column $((r-1)-p \mod z)+1$ for row $r, 1 \le r \le z$ and zero elsewhere. We note that $\mathbf{H}$ can be uniquely determined by the scaling matrix $\mathbf{S} = \{s_{i,j}\}_{i\in[\gamma],j\in[\kappa]}, s_{i,j} \in \mathbb{F}_q$ and power matrix $\mathbf{P} = \{p_{i,j}\}_{i\in[\gamma],j\in[\kappa]}, 0 \le p_{i,j} \le z-1$.

An important measure for LDPC codes is the girth, which is the length of the shortest cycle in the graph of the LDPC code. A necessary and sufficient condition for a QC-LDPC code to have a certain girth is given in the following lemma:

Lemma 1. *[23] A QC-LDPC code in the form of Eq.*(2) *has girth at least* $2(g+1)$ *if and only if*

$$\sum\nolimits_{k=1}^{m} p_{i_k,j_k} - p_{i_{k+1},j_k} \not\equiv 0 \mod z \tag{3}$$

for all m, $2 \leq m \leq g$, *all* i_k, $i \in [\gamma]$, *and all* j_k, $j \in [\kappa]$ *with* $i_1 = i_m$, $i_k \neq i_{k+1}$, *and* $j_k \neq j_{k+1}$.

Finally, we note that a matrix of size $m \times n$ with $m \leq n$ is considered Maximum-Distance Separable (MDS) if and only if every square submatrix of size $m \times m$ is full rank.

III. Privacy Amplification with Sampling

In this section, we demonstrate how we can achieve privacy amplification by properly sampling the decoded sequence $\mathbf{x}$. The benefit of this approach is that the IR decoder only needs to decode a subset of $\mathbf{x}$ which has a higher probability of success than fully decoding $\mathbf{x}$. We term the decoder that decodes the full $\mathbf{x}$ as the *full codeword* (FC) decoder and the decoder that decodes a subset of $\mathbf{x}$ as the *subset codeword* (SC) decoder. We formally define the SC decoder as follows:

Definition 1. *Given a set* $\mathcal{S} \subseteq [N]$*, the SC decoder takes* $\mathbf{x}_\mathcal{S}$ *from the output of the FC decoder and inputs it into the PA step. As such, the secret key rate can be written as*

$$SKR = Pr(\widetilde{A})\frac{H(\mathbf{x}_\mathcal{S}) - \mathcal{I}(\mathbf{x}_\mathcal{S};\mathcal{E},\mathbf{z})}{N} \tag{4}$$

where $\widetilde{A}$ *is the event that* $\mathbf{x}_\mathcal{S}$ *is decoded successfully.*

The following lemma provides sufficient conditions when the SC decoder cannot have a lower secret key rate than the FC decoder.

Lemma 2. *Assume that there exists a set* $\mathcal{S} \subset [N], |\mathcal{S}| = N - M$ *such that the submatrix* $\mathbf{H}_{\overline{\mathcal{S}}}$ *is full rank. Thus, we can write* $\mathbf{z} = \mathbf{H}\mathbf{x} = \mathbf{H}_\mathcal{S}\mathbf{x}_\mathcal{S} + \mathbf{H}_{\overline{\mathcal{S}}}\mathbf{x}_{\overline{\mathcal{S}}}$*. If* SKR_1 *and* SKR_2 *are the secret key rates of the FC decoder and SC decoder, respectively, then* $SKR_1 \leq SKR_2$*.*

Proof. First, we note that the probability of success for the FC decoder is clearly not higher than the probability of success for the SC decoder since the event that $\mathbf{x}$ is correctly decoded is encompassed in the event that $\mathbf{x}_\mathcal{S}$ is correctly decoded. Thus, $Pr(\widetilde{A}) \geq Pr(A)$.

Next, we note that by $\mathbf{H}_{\overline{\mathcal{S}}}$ being invertible we have

$$\mathbf{z} = \mathbf{H}_\mathcal{S}\mathbf{x}_\mathcal{S} + \mathbf{H}_{\overline{\mathcal{S}}}\mathbf{x}_{\overline{\mathcal{S}}} \implies \mathbf{x}_{\overline{\mathcal{S}}} = \mathbf{H}_{\overline{\mathcal{S}}}^{-1}(\mathbf{z} - \mathbf{H}_\mathcal{S}\mathbf{x}_\mathcal{S}).$$

Thus, $\mathbf{x}_{\overline{\mathcal{S}}}$ is a function of $\mathbf{z}$ and $\mathbf{x}_\mathcal{S}$. As such,

$$H(\mathbf{x}) - \mathcal{I}(\mathbf{x};\mathcal{E},\mathbf{z}) = H(\mathbf{x}|\mathcal{E},\mathbf{z}) = H(\mathbf{x}_\mathcal{S},\mathbf{x}_{\overline{\mathcal{S}}}|\mathcal{E},\mathbf{z})$$
$$= H(\mathbf{x}_\mathcal{S}|\mathcal{E},\mathbf{z}) + \overbrace{H(\mathbf{x}_{\overline{\mathcal{S}}}|\mathcal{E},\mathbf{x}_\mathcal{S},\mathbf{z})}^{0} = H(\mathbf{x}_\mathcal{S}) - \mathcal{I}(\mathbf{x}_\mathcal{S};\mathcal{E},\mathbf{z})$$

implying that the final key length is the same for both decoders.

Since the final key lengths are the same and the probability of success of the SC decoder is not lower than for the FC decoder, we guarantee that $SKR_1 \leq SKR_2$. ☐

The key idea of Lemma 2 is that carefully sampling $\mathbf{x}$ allows us to use the entropy of the non-sampled bits to increase privacy despite the reconciled vector $\mathbf{x}_\mathcal{S}$ being smaller than $\mathbf{x}$. In total, the final key length can be made the same with relaxed requirements. The proposed approach relaxes the success condition for the IR step. We note that this relaxation would not improve a maximum likelihood decoder since it is clear that $Pr(A) = Pr(\widetilde{A})$. Yet, it can increase the success probability of a sub-optimal but practical decoder such as the sum-product belief propagation decoder used for LDPC codes. Additionally, the proof of Lemma 2 did not rely on $\mathcal{S}$ being the only set with this property. We can thus generalize the SC decoder to decoding at least one of multiple subsets with the full rank property as shown in the following definition:

Definition 2. *Let* $\mathbb{S} = \{\mathcal{S}_i : i \in [k]\}$ *be a set of* k *subsets of* $[n]$ *that are possibly non-disjoint. The multiple subset codeword (MSC) decoder samples the subset* $\mathbf{x}_{\mathcal{S}_i}$ *with the highest secret key rate as defined by*

$$SKR_i = Pr(\widetilde{A}_i)\frac{H(\mathbf{x}_{\mathcal{S}_i}) - \mathcal{I}(\mathbf{x}_{\mathcal{S}_i};\mathcal{E},\mathbf{z})}{N}, i \in [k] \tag{5}$$

where $\widetilde{A}_i$ *is the event that* $\mathbf{x}_{\mathcal{S}_i}$ *is decoded successfully.*

Note that the MSC decoder chooses which $\mathcal{S}$ to sample at the time of decoding based on which subset is most likley to provide the highest secret key rate. Utilizing Lemma 2, we get the following lemma for the MSC decoder.

Lemma 3. *If* $|\mathcal{S}| = N - M$ *and* $\mathbf{H}_{\overline{\mathcal{S}}}$ *is full rank for every* $\mathcal{S} \in \mathbb{S}$*, then the MSC decoder achieves a secret key rate that is equal to or greater than the secret key rate of an SC decoder for any particular* $\mathcal{S} \in \mathbb{S}$*. Additionally, the secret key length is the same for all choices of* $\mathcal{S} \in \mathbb{S}$*.*

In the sequel, we assume that $\mathbb{S}$ satisfies Lemma 3 whenever we discuss the MSC decoder. To properly utilize Lemma 3, the FC decoder must be able to estimate $Pr(\widetilde{A}_i)$ in order to select which set to sample, a property that works naturally with the belief propagation decoder for LDPC codes.

IV. Block-MDS QC-LDPC Codes

In this section, we demonstrate how to construct QC-LDPC codes for the MSC decoder. In theory, we could randomly sample an LDPC code from a code ensemble and find all the square full rank submatrices of the parity check matrix to satisfy Lemma 3. Yet, this approach would be quite difficult to analyze since the number of full rank submatrices can differ between samples. As such, we turn towards structured codes such as QC-LDPC codes and devise construction methods that guarantee certain subsets have the full rank property. We formally define this notion as follows:

Definition 3. *A QC-LDPC code is* ***Block-MDS*** *if all the submatrices* $\mathbf{H}_{\mathcal{S}_\mathcal{B}}, \mathcal{B} \in \binom{[\kappa]}{\gamma}$ *are full rank, where* $\mathcal{S}_\mathcal{B} \triangleq \{(i-1) \times z + j : i \in \mathcal{B}, j \in [z]\}$*,* κ *is the row weight,* γ *is the column weight, and* z *is the lifting factor.*

At a high level, a Block-MDS QC-LDPC code guarantees that every square submatrix that corresponds to the lifting of a $\gamma \times \gamma$ submatrix in the parity check matrix of the protograph is full rank. This is conceptually similar to an MDS matrix where every square submatrix is full rank but instead we focus on the lifted block matrices being full rank. As such, the MSC decoder subsets for the Block-MDS code are $\mathbb{S} = \{\overline{\mathcal{S}_\mathcal{B}} : \mathcal{B} \in \binom{[\kappa]}{\gamma}\}$. Example 1 demonstrates Definition 3.

Example 1. Consider the following parity check matrix of a QC-LDPC code with $(\gamma, \kappa) = (2, 3)$ (see Section II-B):

$$\mathbf{H} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}.$$

$\mathbf{H}$ is Block-MDS if the following submatrices are full rank:

$$\mathbf{H}_{\mathcal{S}_{1,2}} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} \end{bmatrix},$$
$$\mathbf{H}_{\mathcal{S}_{1,3}} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix},$$
$$\mathbf{H}_{\mathcal{S}_{2,3}} = \begin{bmatrix} s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}.$$

By focusing on Block-MDS QC-LDPC codes, we can significantly simplify the design of LDPC codes that can utilize the MSC decoder. For the rest of this section, we shall investigate techniques to construct Block-MDS QC-LDPC codes. We first state an important result in linear algebra that we rely on extensively in this paper:

Lemma 4. *[25, Theorem 1] Let $\mathcal{R}$ be a commutative subring of $\mathbb{F}_q^{z,z}$, i.e., $\mathcal{R}$ is a set of matrices of size $z \times z$ that form a commutative ring with the standard operations of matrix addition and multiplication. Let $\mathbf{M} \in \mathcal{R}^{a\times b}$, i.e., $\mathbf{M}$ is a block matrix where each block is an element in $\mathcal{R}$. Then,*

$$\det_{\mathbb{F}_q}(\mathbf{M}) = \det_{\mathbb{F}_q}(\det_{\mathcal{R}}(\mathbf{M})), \tag{6}$$

where $\det_F$ is the determinant function over a ring F.

Consider the set $\mathcal{C} \subset \mathbb{F}_q^{z,z}$ as the set of all circulant matrices of size $z \times z$ with elements in the field $\mathbb{F}_q$. It is well known that $\mathcal{C}$ is a commutative ring in regards to operations of the standard matrix addition and multiplication [26, Theorem 7.3.2]. Since a QC-LDPC code is a block matrix consisting of CSMs, Lemma 4 states that a necessary and sufficient condition for the QC-LDPC code to be Block-MDS is that it satisfies

$$\det_{\mathbb{F}_q}\left(\sum_{\sigma\in S_\gamma} sign(\sigma)\prod_{i=1}^{\gamma} s_{\sigma(i),\tau(i)}\mathbf{C}^{p_{\sigma(i),\tau(i)}}\right) \neq 0,\ \forall\tau \in \binom{[\kappa]}{\gamma}, \tag{7}$$

where we have expressed the determinant function using the well-known Leibniz formula and $sign(\sigma)$ is the parity of the permutation σ. Note that the inner sum must be a circulant due to $\mathcal{C}$ being a commutative ring. Thus, the Block-MDS condition can be checked for a particular QC-LDPC code by whether $\binom{\kappa}{\gamma}$ circulant matrices of size $z \times z$ are singular. The direct way would be to take the determinant of each circulant matrix in the field $\mathbb{F}_q$. For circulant matrices, there is a much easier check for singularity. First, let us define the associated polynomial of a circulant matrix as $f(x) = \sum_{i=1}^{z} a_i x^{i-1} \in \mathbb{F}_q[x]$ where a_i is the i^{th} element in the first column of the circulant matrix. The following lemma provides a simple condition to check whether a circulant matrix is singular [27], [28]:

Lemma 5. *Let $f(x)$ be the associated polynomial of a circulant matrix $\mathbf{A} \in \mathbb{F}_q^{z,z}$. Then, $\mathbf{A}$ is non-singular if and only if* $\gcd(f(x), x^z - 1) = 1$.

Using Lemmas 4 and 5, we arrive at the following theorem:

Theorem 1. *A sufficient condition for a QC-LDPC code with parameters (γ, κ, z) to be Block-MDS is that for all $\tau \in \binom{[\kappa]}{\gamma}$ the scaling matrix $\mathbf{S}$ and power matrix $\mathbf{P}$ satisfy*

$$f_\tau(x) = \sum_{\sigma\in S_\gamma} sign(\sigma)\left(\prod_{i=1}^{\gamma} s_{\sigma(i),\tau(i)}\right) x^{\left(\sum_{i=1}^{\gamma} p_{\sigma(i),\tau(i)}\right)_z}, \tag{8}$$

$$\gcd(f_\tau(x), x^z - 1) = 1, \tag{9}$$

$$\sum_{i=1}^{\gamma} p_{\sigma(i),\tau(i)} - p_{\rho(i),\tau(i)} \not\equiv 0 \bmod z,\ \forall\rho,\sigma \in S_\gamma, \rho \neq \sigma. \tag{10}$$

Proof. To simplify Eq. (7), we can enforce that all circulant matrices in the inner sum (after performing the products) do not have any overlap in their non-zero positions. This ensures that each matrix contributes to only one coefficient in the associated polynomial of the summed up circulant matrix. Eq. (10) accomplishes this by requiring that for a given column subset τ all the matrix powers in that particular sum are distinct which ensures no overlap in the non-zero terms of the summed circulant matrix. As such, the associated polynomial $f_\tau(x)$ for a given τ can be written as Eq. (8). Applying Lemma 5 results in Eq. (9) which completes the proof. □

At first glance, Theorem 1 seems to provide a sufficient condition that is quite restrictive on the parameters due to Eq.(10). In fact, the following example demonstrates that Theorem 1 broadly applies to QC-LDPC codes of high girth which are attractive for their error correcting performance.

Example 2. Consider the QC-LDPC code in Example 1. According to Theorem 1, the following equations are sufficient for this QC-LDPC code to be Block-MDS:

$$\gcd(s_{1,1}s_{2,2}x^{(p_{1,1}+p_{2,2})_z} - s_{2,1}s_{1,2}x^{(p_{2,1}+p_{1,2})_z}, x^z - 1) = 1 \tag{11}$$

$$\gcd(s_{1,1}s_{2,3}x^{(p_{1,1}+p_{2,3})_z} - s_{2,1}s_{1,3}x^{(p_{2,1}+p_{1,3})_z}, x^z - 1) = 1 \tag{12}$$

$$\gcd(s_{1,2}s_{2,3}x^{(p_{1,2}+p_{2,3})_z} - s_{2,2}s_{1,3}x^{(p_{2,2}+p_{1,3})_z}, x^z - 1) = 1 \tag{13}$$

$$p_{1,2} + p_{2,3} \not\equiv p_{2,2} + p_{1,3} \mod z \tag{14}$$

$$p_{1,1} + p_{2,3} \not\equiv p_{2,1} + p_{1,3} \mod z \tag{15}$$

$$p_{1,2} + p_{2,3} \not\equiv p_{2,2} + p_{1,3} \mod z \tag{16}$$

Note that Eqs.(14),(15),(16) are a subset of the cycle conditions in Lemma 1 to ensure that the QC-LDPC code has no cycles of length 4. In fact, we can see that Eq. (10) in Theorem 1 is always a subset of the cycle conditions in Lemma 1 for containing no cycles of length γ. Thus, we get the following corollary:

Corollary 2. *A QC-LDPC code with column weight γ and girth $2\gamma+2$ is Block-MDS if and only if it satisfies the equations in Theorem 1.*

Theorem 1 is sufficient to guarantee Block-MDS among high girth QC-LDPC codes, which are the class of QC-LDPC

TABLE I: (Code Parameters) All lifting factors z were chosen to get code lengths close to 2000 for fair comparison while satisfying Theorem 3.

Code	(γ, κ)	Lifting Factor	Rate	Length
C_1	(4,5)	389	1/5	1945
C_2	(3,4)	491	1/4	1964
C_3	(3,5)	389	2/5	1945

codes of general interest due to their higher error-correcting performance. We note that Corollary 2 becomes less meaningful for $\gamma \geq 6$ as it is well known that type-I QC-LDPC codes have a minimum girth of 12 [23]. This is not a problematic constraint since many practical type-I QC-LDPC codes generally have γ be 3 or 4. A future research direction is generalizing our result to more complex constructions of QC-LDPC codes that permit a higher girth.

For special values of the lifting factor z, Theorem 1 can also be used to derive a simpler condition that allows for decoupling the search for matrices $\mathbf{S}$ and $\mathbf{P}$. The following theorem provides sufficient conditions where a high girth QC-LDPC code can be made into a Block-MDS code where the finite field size scales linearly with κ.

Theorem 3. *If the lifting factor z is an odd prime and the polynomial $\sum_{i=0}^{z-1} x^i$ is irreducible in $\mathbb{F}_q$, then a QC-LDPC code with girth $2\gamma+2$ can be made into a Block-MDS code with a careful choice of $\mathbf{S}$ for all $\kappa \leq |\mathbb{F}_q|$ and $\gamma! < z$.*

Proof. Let us consider Eq.(9). When z is a prime, then we can easily factor $x^z - 1$ into $(x-1)(\sum_{i=0}^{z-1} x^i)$. By the theorem statement, these are the irreducible factors of $x^z - 1$. The left factor indicates that for the gcd to be 1, then 1 cannot be a root of $f_\tau(x)$, i.e.,

$$f_\tau(1) = \sum_{\sigma \in S_\gamma} sign(\sigma) \left(\prod_{i=1}^{\gamma} s_{\sigma(i),\tau(i)} \right) \neq 0 \in \mathbb{F}_q. \quad (17)$$

Note that $f_\tau(1)$ is simply the determinant of the $\gamma \times \gamma$ submatrix of $\mathbf{S}$ where the columns are selected by τ. Since this condition needs to be true for every choice of τ, then $\mathbf{S}$ must be an MDS matrix. Now, we only need to prove that $f_\tau(x)$ is not a factor of $\sum_{i=0}^{z-1} x^i$ since the degree of $f_\tau(x)$ is less than or equal to $z-1$. Since $\sum_{i=0}^{z-1} x^i$ is irreducible, we only need to show that $\sum_{i=0}^{z-1} x^i \neq f_\tau(x)$. This is true by noting that the number of non-zero elements in the polynomial $f_\tau(x)$ is upper bounded by $\gamma!$ which is less than z by the theorem statement. Hence, Eq.(9) is equivalent to requiring that $\mathbf{S}$ is an MDS matrix.

We complete the proof by using the well-known Vandermonde matrix of size $\gamma \times \kappa$ for $\mathbf{S}$ since it is MDS and it only needs a field size of $\kappa \leq |\mathbb{F}_q|$ [29]. □

Theorem 3 allows us to decouple the constructions of matrices $\mathbf{P}$ and $\mathbf{S}$. Thus, we can first find a matrix $\mathbf{P}$ with sufficient girth properties and then transform it using an easily defined matrix $\mathbf{S}$ where the finite field size scales linearly with the row weight. This property is very useful in practice since large finite field sizes incur significant complexity in decoding which translates to higher latency or more complex circuitry. Our design allows for Block-MDS QC-LDPC codes that are almost independent of the block length since the field size depends on κ for lifting factors that satisfy Theorem 3.

TABLE II: Secret Key Rates at representative points for high noise regime.

Code	Transition Probability	FC SKR	MSC SKR
C_1	$p = 0.28$	0.4114	0.45
C_2	$p = 0.275$	0.3913	0.4832
C_3	$p = 0.2$	0.8883	0.9679

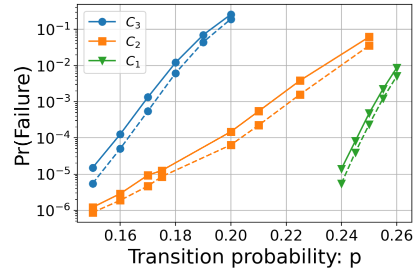

Fig. 1: Probability of IR failure for different transition probabilities for a 8-ary symmetric channel. Bold line indicates the FC decoder and dotted lines indicates the MSC decoder.

V. Simulations and Conclusion

In this section, we shall demonstrate the benefits of using our new decoding method to jointly perform information reconciliation and privacy amplification on our Block-MDS QC-LDPC codes. We shall be comparing the secret key rate using FC and MSC decoding on our Block-MDS QC-LDPC codes to demonstrate the gains offered by the relaxation of the IR step. Since the final key length for a code is the same regardless of the decoder chosen (FC or MSC), the major measure of interest is the IR failure probability for the secret key rate. As such, we shall demonstrate the improvements that the MSC decoder has over the FC decoder in terms of the IR failure probability for the low noise regime and the secret key rate at the high noise regime.

We perform simulations on three QC-LDPC codes with parameters described in Table I. All codes were constructed to have girth 10. The power matrix $\mathbf{P}$ and scaling matrix $\mathbf{S}$ for each code can be found in the Appendix of the full paper [30]. Fig. 1 plots the probability of IR failure for different values of the transition probability for an 8-ary symmetric channel. We see that the MSC decoder can improve the IR failure probability by about 0.25 orders of magnitude. Clearly, the gains differ for different code parameters which suggests further study into how code parameters affect the decoding probability of the MSC decoder. Yet, we see that the MSC decoder can provide significant gains. Additionally, Table II demonstrates the improvement in the SKR at the high noise regime which is commonly found in practice. In this regime, even a small improvement in the FER can have significant gains in the secret key rate as demonstrated by the MSC decoder.

In conclusion, we demonstrated a relaxation for the IR step in QKD utilizing sampling, thus allowing us to improve the success rate of the IR step. This allowed use to create PA-aware LDPC codes in the form of Block-MDS QC-LDPC codes that can capitalize on this relaxation. We empirically demonstrate the improvements of our new decoder on these LDPC codes through simulations. Future work is focused on generalizing our ideas to a broader set of graph codes and providing a full security analysis on the total QKD system.

References

[1] C. Wang and A. Rahman, "Quantum-enabled 6G wireless networks: Opportunities and challenges," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 58–69, 2022.

[2] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.

[3] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, *et al.*, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," *New Journal of Physics*, vol. 17, no. 2, p. 022002, 2015.

[4] L. Dolecek and E. Soljanin, "Qkd based on time-entangled photons and its key-rate promise," *IEEE BITS Information Theory Magazine*, vol. 2, no. 3, pp. 39–48, 2022.

[5] K. Brádler, M. Mirhosseini, R. Fickler, A. Broadbent, and R. Boyd, "Finite-key security analysis for multilevel quantum key distribution," *New Journal of Physics*, vol. 18, no. 7, p. 073030, 2016.

[6] Q. Zhuang, Z. Zhang, J. Dove, F. N. Wong, and J. H. Shapiro, "Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates," *Physical Review A*, vol. 94, no. 1, p. 012322, 2016.

[7] Z. Zhang, C. Chen, Q. Zhuang, F. N. Wong, and J. H. Shapiro, "Experimental quantum key distribution at 1.3 gigabit-per-second secret-key rate over a 10 db loss channel," *Quantum Science and Technology*, vol. 3, no. 2, p. 025007, 2018.

[8] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. B. Dixon, F. N. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, "Large-alphabet encoding for higher-rate quantum key distribution," *Optics express*, vol. 27, no. 13, pp. 17539–17549, 2019.

[9] H. Zhou, L. Wang, and G. Wornell, "Layered schemes for large-alphabet secret key distribution," in *2013 Information Theory and Applications Workshop (ITA)*, pp. 1–10, IEEE, 2013.

[10] D. Mitra, J. Shreekumar, L. Tauz, M. C. Sarihan, C. W. Wong, and L. Dolecek, "Efficient information reconciliation in quantum key distribution systems using informed design of non-binary ldpc codes," *Quantum Information Processing*, vol. 23, no. 4, pp. 1–30, 2024.

[11] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 210–229, 1988.

[12] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *IEEE International Symposium on Information Theory*, pp. 1879–1883, 2009.

[13] R. Müller, D. Bacco, L. K. Oxenløwe, and S. Forchhammer, "Information reconciliation for high-dimensional quantum key distribution using nonbinary ldpc codes," in *International Symposium on Topics in Coding (ISTC)*, pp. 1–5, 2023.

[14] K.-C. Chang, X. Cheng, M. C. Sarihan, A. K. Vinod, Y. S. Lee, T. Zhong, Y.-X. Gong, Z. Xie, J. H. Shapiro, F. N. Wong, *et al.*, "648 hilbert-space dimensionality in a biphoton frequency comb: entanglement of formation and schmidt mode decomposition," *npj Quantum Information*, vol. 7, no. 1, p. 48, 2021.

[15] C. Lee, Z. Zhang, J. Mower, G. Steinbrecher, H. Zhou, L. Wang, R. D. Horansky, V. B. Verma, M. S. Allman, A. E. Lita, R. P. Mirin, F. Marsili, A. D. Beyer, M. D. Shaw, S. W. Nam, G. Wornell, F. N. C. Wong, J. H. Shapiro, and D. Englund, "High-dimensional time-energy entanglement-based quantum key distribution using dispersive optics," (San Jose, CA, USA), pp. 1–2, IEEE, 2014.

[16] M. Y. Niu, F. Xu, J. H. Shapiro, and F. Furrer, "Finite-key analysis for time-energy high-dimensional quantum key distribution," *Physical Review A*, vol. 94, no. 5, p. 052323, 2016.

[17] C. Lee, J. Mower, Z. Zhang, J. H. Shapiro, and D. Englund, "Finite-key analysis of high-dimensional time–energy entanglement-based quantum key distribution," *Quantum Information Processing*, vol. 14, no. 3, pp. 1005–1015, 2015.

[18] K.-C. Chang, M. C. Sarihan, X. Cheng, Z. Zhang, and C. W. Wong, "Large-alphabet time-bin quantum key distribution and einstein–podolsky–rosen steering via dispersive optics," *Quantum Science and Technology*, vol. 9, p. 015018, dec 2023.

[19] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[20] E. Dupraz, V. Savin, and M. Kieffer, "Density evolution for the design of non-binary low density parity check codes for slepian-wolf coding," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 25–36, 2015.

[21] J. Thorpe, "Low-density parity-check (ldpc) codes constructed from protographs," *IPN progress report*, vol. 42, no. 154, pp. 42–154, 2003.

[22] L. Dolecek, D. Divsalar, Y. Sun, and B. Amiri, "Non-Binary Protograph-Based LDPC Codes: Enumerators, Analysis, and Designs," *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 3913–3941, 2014.

[23] M. Fossorier, "Quasicyclic low-density parity-check codes from circulant permutation matrices," *IEEE Transactions on Information Theory*, vol. 50, no. 8, pp. 1788–1793, 2004.

[24] R. Smarandache and P. O. Vontobel, "Quasi-Cyclic LDPC Codes: Influence of Proto- and Tanner-Graph structure on minimum hamming distance upper bounds," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 585–607, 2012.

[25] J. R. Silvester, "Determinants of Block Matrices," *Mathematical Gazette*, vol. 84, no. 501, pp. 460–467, 2000.

[26] D. Hachenberger and D. Jungnickel, *Topics in Galois fields*, vol. 4. Springer, 2020.

[27] A. W. Ingleton, "The rank of circulant matrices," *Journal of the London Mathematical Society*, vol. 1, no. 4, pp. 445–460, 1956.

[28] T. Fabšič, V. Hromada, P. Stankovski, P. Zajac, Q. Guo, and T. Johansson, "A reaction attack on the qc-ldpc mceliece cryptosystem," in *Post-Quantum Cryptography International Workshop*, pp. 51–68, Springer, 2017.

[29] A. Klinger, "The vandermonde matrix," *The American Mathematical Monthly*, vol. 74, no. 5, pp. 571–574, 1967.

[30] L. Tauz, D. Mitra, J. Shreekumar, M. C. Sarihan, C. W. Wong, and L. Dolecek, "Block-mds qc-ldpc codes for information reconciliation in key distribution," *arXiv preprint arXiv:2403.00192*, 2024.