The Niederreiter cryptosystem and Quasi-Cyclic codes

Upendra Kapshikar Ayan Mahalanobis

Abstract

McEliece and Niederreiter cryptosystems are robust and versatile cryptosystems. These cryptosystems work with any linear error-correcting codes. They are popular these days because they can be quantum-secure. In this paper, we study the Niederreiter cryptosystem using quasi-cyclic codes. We prove, if these quasi-cyclic codes satisfy certain conditions, the corresponding Niederreiter cryptosystem is resistant to the hidden subgroup problem using quantum Fourier sampling. Our proof requires the classification of finite simple groups.

Keywords– Hidden subgroup problem, Niederreiter cryptosystem, Quasi-cyclic codes

1 Introduction

In last couple of decades, modern view of the theory of computer science has taken huge leap due to advances in quantum computing. First significant impact of quantum computing was in 1995 with Shor's factoring algorithm [27]. This quantum algorithm could factorize numbers in polynomial time. This breaks RSA. Soon this algorithm was extended for the discrete logarithm problem. This triggered *post-quantum cryptography.*

All the algorithms mentioned above, the factoring algorithm, solving the discrete algorithm problem are instances of the *hidden subgroup problem.* Roughly speaking, hidden subgroup problem is an instance where a function hides a subgroup and our task is to recover the subgroup. Quantum computing gives a solution to this problem via *quantum Fourier sampling* (QFS) when the parent group is commutative. So far, not much progress has been made in the hidden subgroup problem for non-commutative groups. In this paper, we look at one such cryptosystem, a code based Niederreiter cryptosystem using quasi-cyclic codes.

The idea of (in)effectiveness of QFS was introduced by Kempe and Shalev [18], where they characterized subgroups in permutation groups that can be distinguished from the identity subgroup via a quantum Fourier sampling. This idea gave way of showing that some subgroups can not be distinguished from the identity subgroup and hence a hidden subgroup problem can not be solved by QFS. Dinh et. al. [7], used this to show that McEliece and Niederreiter cryptosystems resist QFS for goppa codes followed by Kapshikar and Mahalanobis [16]. We prove similar result for a large class of quasi-cyclic codes (QCC). Our main theorem is the following:

Theorem A (Main Theorem)**.** *For quasi-cyclic codes, which satisfy conditions (i) - (v) in Section 4.1, the corresponding Niederreiter cryptosystems resists quantum Fourier sampling attack.*

Our proof can be divided up into 3 parts. Let $\mathcal{H}$ be the parity-check matrix of size $k \times n$ to be used in the Niederreiter cryptosystem. We write $\mathcal{H} = [\mathrm{I}|C]$, where C is a block matrix with each block a circulant matrix of size p over a proper extension of $\mathbb{F}_2$ for some prime p.

A) First we show that for any codes, the hidden subgroup problem over $(\mathrm{GL}_k(\mathbb{F}_2) \times \mathrm{S}_n)^2 \rtimes \mathbb{Z}_2$ can be broken down into $\mathrm{GL}_k(\mathbb{F}_2)$ and S_n with an additional overhead in terms of the size of the hidden subgroup. Note that this decomposition into individual

components is true for any error correcting code. It can be useful for other codes as well.

B) In the second part we use the structure of quasi-cyclic codes to find some important bounds. Here we also show, for our codes, the hidden subgroup is contained in $S_k \times S_n$.

C) We finish by combining the above arguments with some important results from the theory of permutation groups to show that the hidden subgroup can not be distinguished from the identity subgroup. Hence the Niederreiter cryptosystem thus constructed will be resistant to quantum Fourier sampling. This part uses the *classification of finite simple groups*.

1.1 A quick survey

Niederreiter or McEliece cryptosystems were not so popular. The main reason for this is large key sizes and in some cases low transmission rates. Various attempts were made to decrease key sizes. Many of them were later broken down with one or the other attack but the original McEliece and Niederreiter cryptosystem is still believed to be secure. Balsdi and Chairaluce [3] suggested implementation of QC-LDPC codes for McEliece cryptosystem. Later similar construction based on QC-MDPC [23] was also recommended. Guo et. al. [12] presented a reaction attack on QC-MDPC. Later similar attack was also presented on QC-LDPC [9]. Other than these, there are other notable attempts by Monico et. al. [2,24] including a recent work by Li et. al. [21]. For more information on the use of quasi-cyclic LDPC matrices in code based cryptosystem we refer to [1] and NIST round 1 proposals. Other than these, there are broadly two major general classical attacks on code based cryptography which fall under ISD (information set decoding). One of them is based on Stern's strategy [28] which was later improved by Bernstein et. al. [5] and other attack is due to Lee and Brickell [20]. For more on code based cryptography and attacks on it, we refer the reader to two NIST submissions for post-quantum cryptography [4,30].

1.2 Structure of the paper

In Section 2, we introduce briefly the *standard method* for quantum Fourier sampling and associated hidden subgroup problem along with a result by Kempe and Shalev [17, 18]. In the following section, we briefly talk about code based cryptosystems and in particular the Niederreiter cryptosystem. We also mention the main quantum attack *the scrambler-permutation attack* and its connection to the hidden subgroup problem which is a main objective of this paper. Then we move to the main contribution of this paper – proof of Theorem A. This paper is based on the work of Kempe and Shalev [17, 18]. Similar work was also done by Dinh et al. [7] and Kapshikar and Mahalanobis [16].

2 The hidden subgroup problem

One of the unifying theme in quantum computing is the *hidden subgroup problem*. Most of the practical algorithms that offer exponential speedup in quantum computer science can be modeled in this form. Popular examples are, factoring integers by Shor's algorithm, the discrete logarithm problem and others [13].

Definition 2.1 (Hidden Subgroup Problem)**.** *Let* G *be a group and* H *be a (unknown) subgroup of* G*. We are given a function f from* G *such that $f(g_1) = f(g_2)$ whenever $g_1\mathrm{H} = g_2\mathrm{H}$. The function in this case is said to be separating cosets of the subgroup* H*. The hidden subgroup problem is to find a set of generators of* H*.*

The hidden subgroup problem is easy to solve when the group G is abelian but for non-commutative groups it is far from realized. Efforts to solve the hidden subgroup

problem can be broadly characterized into two categories. One of which is based on a generalization of quantum Fourier sampling from abelian to non-abelian groups [14, 26]. The second direction is on some particular non-abelian black-box groups where instead of doing quantum Fourier transform over the group, it is done on the abelian group [15, 29]. Apart from this, some strong structural results are available in the non-commutative case, see Vazirani [10]. In this paper, we follow the first approach and our *indistinguishability depends on the quantum Fourier transforms on non-abelian groups.* The function for the Fourier transform is given by an irreducible representation over the field of complex numbers. Thus our Fourier transforms are matrix valued. In the case of abelian groups, the Fourier transforms were scalar valued.

2.1 Quantum Fourier Sampling

The algorithms based on QFS were developed based on the *standard method* by Simons and Shor [27]. We roughly sketch the process. The quantum Fourier sampling is based on a unitary transformation defined as follows:

Definition 2.2 (QFT)**.** *A quantum Fourier transform takes an element of the group algebra* $\mathbb{C}[\mathrm{G}]$ *to the representation basis or the Fourier basis for group* G*.*

$$QFT(g) = \frac{1}{\sqrt{|\mathrm{G}|}} \sum_{\rho,i,j} \sqrt{d_\rho}\rho(g)_{i,j}(\rho, i, j)$$

where ρ *is an irreducible representation of* G *and* d_ρ *is its dimension.*

The standard method for QFS is the following: initialise the state in superposition of all states in the first register and $|0\rangle$ in the second register. Apply f (where $f(x, 0) = (x, f(x))$). This is followed by measurement on the second register which puts the state of the first register in a random left coset of a subgroup H i.e., $|g\mathrm{H}\rangle = \sum_{h\in\mathrm{H}} |gh\rangle$ for a random g. Finally QFT along with the measurement in the Fourier basis, gives the probability distribution as

$$\mathrm{P}_{g\mathrm{H}}(\rho, i, j) = \frac{|d_\rho|}{|\mathrm{G}|\ |\mathrm{H}|} \left| \sum_{h\in\mathrm{H}} \rho(gh)_{i,j} \right|^2. \tag{1}$$

As we have chosen g randomly and uniformly, $\mathrm{P}_{\mathrm{H}} = \frac{1}{|\mathrm{G}|} \sum_g \mathrm{P}_{g\mathrm{H}}$. To solve the hidden subgroup problem, one finds H in poly(log(|G|)) time. To distinguish H from the identity subgroup $\langle e\rangle$, it is necessary that L_1-distance between $\mathrm{P}_{\mathrm{H}}, \mathrm{P}_{\langle e\rangle}$ is greater than some inverse polynomial in log(|G|). Thus one says that H is distinguishable from $\langle e\rangle$ if there exists a constant c such that $\mathcal{D}_{\mathrm{H}} := \|\mathrm{P}_{\mathrm{H}} - \mathrm{P}_{\langle e\rangle}\|_1 \geq (\log|\mathrm{G}|)^{-c}$. Otherwise, we say that H is not distinguishable from $\langle e\rangle$. So, if for all constants c, H and $\langle e\rangle$ have L_1-distance smaller then $(\log(|\mathrm{G}|))^{-c}$, we say that H is not distinguishable from the identity subgroup. For more on this we refer to Kempe and Shalev [18]. It is well known that

$$\mathcal{D}_{\mathrm{H}} \leq \sum_i |C_i \cap \mathrm{H}||C_i|^{-\frac{1}{2}} = \sum_{h\in\mathrm{H}, h\neq e} |h^{\mathrm{G}}|^{-\frac{1}{2}} \tag{2}$$

where C_i is a non-identity conjugacy class of G and h^{G} denotes conjugacy class of h in G.

So, by showing $\mathcal{D}_{\mathrm{H}}$ is less than every inverse polynomial in log(|G|) one can show that, QFS can not successfully reveal the hidden subgroup H. This is how we proceed in this paper, building on the work on Kempe and Shalev [18].

3 Code based cryptosystems

There is a natural association between coding theory and cryptography because coding theory is a source of many computationally hard problems. More importantly, it is one

of the promising areas in post-quantum cryptography as the underlying structures is non-commutative. As mentioned earlier, Shor-like algorithms, that are based on QFS are very effective over abelian groups. So, cryptosystems based on non-commutative groups are thought to be potential candidates for post-quantum cryptography.

One of the earliest cryptosystems based on error correcting codes was by McEliece [22]. A similar cryptosystem was proposed by Niederreiter [25]. Later, a signature scheme based upon Niederreiter systems was also presented. Our cryptosystem is a Niederreiter cryptosystem, based on quasi-cyclic codes.

3.1 Niederreiter cryptosystems

Let $\mathcal{H}$ be a $k \times n$ parity-check matrix for a $[n, n-k]$ linear code $\mathcal{C}$ with a fast decoding algorithm. Let e be the number of errors that $\mathcal{C}$ can correct.
Private Key: $(A_0, \mathcal{H}, B_0)$ where $A_0 \in \mathrm{GL_k}(\mathbb{F}_2)$ and B_0 is a permutation matrix of size n.
Public Key: $\mathcal{H}' = A_0 \mathcal{H} B_0$.
Encryption:

Let $\mathcal{X}$ be a n-bit plaintext with weight at most e. The corresponding ciphertext $\mathcal{Y}$ of k-bits is obtained by calculating $\mathcal{Y} = \mathcal{H}' \mathcal{X}^{\mathrm{T}}$.

Decryption:

Compute $y = A_0^{-1}\mathcal{Y}$. Thus $y = \mathcal{H} B_0 \mathcal{X}^{\mathrm{T}}$.

Using Gaussian elimination find a z with weight at most e and $\mathcal{H} z^{\mathrm{T}} = y$. Since $y = \mathcal{H} B_0 \mathcal{X}^{\mathrm{T}}$, $\mathcal{H}\left(z^{\mathrm{T}} - B_0 \mathcal{X}^{\mathrm{T}}\right) = 0$. Hence we have $z - \mathcal{X} B_0^{\mathrm{T}} \in \mathcal{C}$.

Now use fast decoding on z with $\mathcal{H}$ to get $\mathcal{X} B_0^{\mathrm{T}}$ and recover $\mathcal{X}$.

3.1.1 Scrambler-Permutation Attack

Scrambler-permutation attacks are defined as, given $\mathcal{H}$ and $\mathcal{H}'$, find A and B. Note that any A, B that satisfying $\mathcal{H}' = A\mathcal{H}B$ breaks the system. Quantum computers, in principle, can exploit this attack. This follows from the fact that scrambler-permutation attacks can be reduced to a hidden subgroup problem. As we saw in previous sections, hidden subgroup problem is important because quantum computers have an advantage over classical computers for this class of problems over abelian groups.

To illustrate the reduction to hidden subgroup problem, we first define a problem that is very close to the hidden subgroup problem.

Definition 3.1 (Hidden shift problem)**.** *Let f_0, f_1 be two functions from group* G *to some set* X *such that: there is a g_0 such that for all g, $f_0(g) = f_1(g_0 g)$. The hidden shift problem is to find one such g_0.*

One can frame the scrambler-permutation attack as a hidden shift problem over $\mathrm{G} = GL_k(\mathbb{F}_2) \times \mathrm{S}_n$ where $f_0(A, B) = A^{-1}\mathcal{H}B$ and $f_1(A, B) = A^{-1}\mathcal{H}'B$. Moreover, it is known that for any non-commutative group G, a hidden shift problem can be reduced to a hidden subgroup problem on $\mathrm{G}^2 \rtimes \mathbb{Z}_2$ where the action of 1 on (x, y) is (y, x). In this paper we are interested in the particular case of $\mathrm{G} = \mathrm{GL}_k(\mathbb{F}_2) \times \mathrm{S}_n$. For that we refer to Dinh et. al. [7, Proposition 3], we use their notations for important subgroups for easy reference. The hidden subgroup is

$$K = \big((H_0, s^{-1}H_0 s), 0\big) \cup \big((H_0 s, s^{-1}H_0), 1\big) \tag{3}$$

where $H_0 = \{(A, P) \in \mathrm{GL}_k(\mathbb{F}_2) \times \mathrm{S}_n \ : \ A^{-1}\mathcal{H}P = \mathcal{H}\}$. Note that from now on wards we will use H for H_0.

Thus to break a Niederreiter cryptosystem using QFS, one needs to solve a hidden subgroup problem over $\mathrm{G}^2 \rtimes \mathbb{Z}_2$ for the hidden subgroup K. From our previous discussion

it follows, if one shows that K is indistinguishable from the identity subgroup, then QFS can not solve the required hidden subgroup problem. For an understanding of indistinguishability we refer to Kempe and Shalev [18].

4 Niederreiter cryptosystems and Quasi-Cyclic Codes

In this section we describe our Niederreiter cryptosystem which uses quasi-cyclic error correcting codes (QCC). Quasi-cyclic codes are a generalization of cyclic codes, codes where code-words are closed under right shifts. Since quasi-cyclic codes are a generalization of cyclic codes they can be expressed as nice algebraic objects. For more on QCC we refer Gulliver [11] and for algebraic structures of these codes to the work of Lally and Fitzpatrick [19].

An important underlying structure of a QCC is circulant matrices. Circulant matrices are a building block of quasi-cyclic codes.

Definition 4.1. *Circulant matrix: An $n \times n$ matrix C' over a field F is called circulant if every row, except for the first row, is a circular right shift of the row above that.*

A typical example of a circulant matrix is

$$\begin{bmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{bmatrix}.$$

It is known that a circulant matrix can be represented by its first row, as a polynomial of degree $n-1$ over the ring $F[x]/(x^n-1)$. In this paper, we define the *multiplicity* of a field element a in C' as the number of times it appear in the first row of C'. Multiplicity can be zero. For more on circulant matrices we refer to Davis [6].

4.1 Conditions on the parity-check matrix

We need some terminology before we can describe our requirements on parity-check matrices of a quasi-cyclic codes. These condition are easy to generate and a large class of block circulant matrices satisfy these conditions.

Definition 4.2 (Permutation equivalent rows and columns)**.** *Let c_i, c_j be two column matrices, we say columns c_i and c_j are permutation equivalent if there is a permutation $\sigma \in S_k$ such that $\sigma(c_i) = c_j$. The permutation group acts on the indices of the columns. Similarly, if there is a permutation $\tau \in S_n$ such that $\tau(r_i) = r_j$, we say that rows r_i and r_j are permutation equivalent.*

In short, two columns are permutation equivalent if one of them can can be reordered to get the other column. We now describe the quasi-cyclic code for our cryptosystem. We do this by stating conditions on the systematic parity-check matrix $\mathcal{H}$ for a error-correcting code over $\mathbb{F}_{2^n}$. The dimension of $\mathcal{H}$ is $m_1 p \times m_2 p$, where $m_1 < m_2$ are positive integers and p a prime. Furthermore, $\mathcal{H}$ is of the form $[\mathrm{I}|C]$ where I is an identity matrix of size $m_1 p \times (m_2 - m_1)p$ and C is a block-circulant matrix. Each block in C, is a circulant matrix C_{ij} where $i = 1, 2, \ldots, m_1$ and $j = 1, 2, \ldots, (m_2 - m_1)$ and is of size the prime p. It is well known that $C = \sum_i E_{i,j} \otimes C_{i,j}$ where E_{ij} is the matrix of same size as C with 1 in the $(i\,j)$ position and zero everywhere else.

i) Circulant matrices C_{ij} with all entries the same is forbidden. That means, $C_{i,j}$ is such that the polynomial corresponding to the circulant matrix $C_{i,j}$ is not $a \sum_k \mu^k$ for any a in the field.

ii) For each j there is at least one i where $C_{i,j}$ contain an element from an proper extension of $\mathbb{F}_2$. This condition is equivalent to saying that each column of C contains at least one element from some non-trivial extension of $\mathbb{F}_2$.

iii) Any two rows r_i, r_j in C are permutation equivalent only when $\left\lfloor \frac{i}{p} \right\rfloor = \left\lfloor \frac{j}{p} \right\rfloor$ where $0 \leq i, j \leq m_1 p$. Similarly, two columns c_i, c_j are permutation equivalent only when $\left\lfloor \frac{i}{p} \right\rfloor = \left\lfloor \frac{j}{p} \right\rfloor$ where $0 \leq i, j \leq m_2 p$.

Note that if $\left\lfloor \frac{i}{p} \right\rfloor = \left\lfloor \frac{j}{p} \right\rfloor$ then rows r_i, r_j and columns c_i, c_j are permutation equivalent because $C_{i,j}$ is a circulant matrix. So this condition simply says that apart from these permutation equivalences, there are no other permutation equivalence between columns or rows.

iv) There exists at least one $C_{i,j}$ for which corresponding polynomial is not $a \sum_{k \neq k_0} \mu^k + b\mu^{k_0}$, which is a matrix with two distinct entries a, b where a has multiplicity $p-1$ and b has multiplicity one.

v) The prime $p > 30$.

Remark: Condition (iii) can be alternatively stated as there exists $a \in \mathbb{F}_{2^n}$, such that, the multiplicity of a in r_i is not the same as in r_j where $\left\lfloor \frac{i}{p} \right\rfloor \neq \left\lfloor \frac{j}{p} \right\rfloor$. Equivalence of these two conditions follows directly as two rows are permutation equivalent if and only if one of them can be reordered to the other. Note that this equivalent condition of permutation equivalence is helpful in finding suitable C. This is because, if two rows are permutation equivalent, one can just count multiplicities rather that going through all possible permutations or, in other words, suitably create the rows so that the multiplicities are different. This says that there are a lot of such block-circulant matrices C.

4.2 From K to H

Recall from Equation (3), $\mathrm{G} = \mathrm{GL}_k(\mathbb{F}_2) \times \mathrm{S}_n$ and we are trying to solve the hidden subgroup problem in the group $\mathrm{G}^2 \rtimes \mathbb{Z}_2$. The subgroup in this case is $\mathrm{K} = K_0 \bigcup K_1$ where $\mathrm{K}_0 = \left(\left(\mathrm{H}, s^{-1}\mathrm{H}s\right), 0\right)$ and $\mathrm{K}_1 = \left(\left(\mathrm{H}s, s^{-1}\mathrm{H}\right), 1\right)$. Note that H replaces H_0 in Equation (3), K_1 is not a subgroup and the union is disjoint.

In this section, we reduce distinguishability of K, $\mathcal{D}_{\mathrm{K}}$ to the subgroup H. If we directly apply Equation (2), our optimization should be over $\left(\mathrm{GL}_k(\mathbb{F}_2) \times \mathrm{S}_n\right)^2 \rtimes \mathbb{Z}_2$. We reduce it to H, a subgroup of $\mathrm{GL}_k(\mathbb{F}_2) \times \mathrm{S}_n$. Then the later bound can be trivially decomposed into individual components $\mathrm{GL}_k(\mathbb{F}_2)$ and S_n. Apart from getting rid of the $\mathbb{Z}_2$ component it also serves one more, the most important purpose for further optimization. The bound that we develop are in terms of H. It has no shift term s. It is part of a subgroup H and has connections and structural properties that we exploit for our optimization.

Back to some more notations. Let x^{G} denote the conjugacy class of x in G and $C_{\mathrm{G}}(x)$ denotes the centralizer of x in G. Here the group acts on itself by conjugation. We abuse the notation slightly and use e for the identity element in a group. It should be clear from the context which group we are referring to.

From [17, Proposition 1 (2)] we know that

$$\mathcal{D}_K \leq \sum_{k \in \mathrm{K}, k \neq e} |k^{\mathrm{G}^2 \rtimes \mathbb{Z}_2}|^{-\frac{1}{2}} \leq \sum_{k_0 \in \mathrm{K}_0, k_0 \neq e} |k_0^{\mathrm{G}^2 \rtimes \mathbb{Z}_2}|^{-\frac{1}{2}} + \sum_{k_1 \in \mathrm{K}_1} |k_1^{\mathrm{G}^2 \rtimes \mathbb{Z}_2}|^{-\frac{1}{2}}.$$

Let S_0 be the sum over K_0 and S_1 be the sum over K_1 in the above expression.

We present an upper bound for $\mathcal{D}_K$ by restricting our action on S_0 and S_1. First we start with S_1. By the orbit-stabilizer property S_1 can be rewritten as

$$S_1 = \sum_{k_1 \in \mathrm{K}_1} \frac{|C_{\mathrm{G}^2 \rtimes \mathbb{Z}_2}(k_1)|^{\frac{1}{2}}}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|^{\frac{1}{2}}} \leq |\mathrm{K}_1| \, \frac{\max\limits_{k_1 \in \mathrm{K}_1} |C_{\mathrm{G}^2 \rtimes \mathbb{Z}_2}(k_1)|^{\frac{1}{2}}}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|^{\frac{1}{2}}}. \tag{4}$$

Now we compute an upper bound of $C_{\mathrm{G}^2 \rtimes \mathbb{Z}_2}(k_1)$. Let us define sets G_0, G_1, two disjoint subsets of the group G.

$$\mathrm{G}_0 = \{((A_0, P_0)\,(A_1, P_1)\,, 0) \ : \ A_0, A_1 \in \mathrm{GL}_k(\mathbb{F}_2), P_0, P_1 \in \mathrm{S}_n\}$$

and

$$\mathrm{G}_1 = \{((A_0, P_0)\,(A_1, P_1)\,, 1) \ : \ A_0, A_1 \in \mathrm{GL}_k(\mathbb{F}_2), P_0, P_1 \in \mathrm{S}_n\}.$$

Clearly $G^2 \rtimes \mathbb{Z}_2$ is a disjoint union of G_0 and G_1. Then $|C_{\mathrm{G}^2 \rtimes \mathbb{Z}_2}(k_1)| = |C_{\mathrm{G}_0}(k_1)| + |C_{\mathrm{G}_1}(k_1)|$. For $g_0 \in G_0$ one can show the following: if $g_0 = ((A_0, P_0)\,, (A_1, P_1)\,, 0)$ is an element of $C_{\mathrm{G}_0}(k_1)$ with $k_1 = \left((h_1 s, s^{-1} h_2)\,, 1\right)$, $h_1 s\,(A_1, P_1) = (A_0, P_0)\,h_1 s$. This result is a simple calculation using the fact that k_1 commutes with g_0.

After fixing (A_0, P_0) and h_1, there is at most one choice available for (A_1, P_1). Thus

$$|C_{\mathrm{G}_0}(k_1)| \leq |\mathrm{H}||\mathrm{GL}_k\,(\mathbb{F}_2) \times \mathrm{S}_n|. \tag{5}$$

Similarly, writing a particular commuting equation for k_1 to g_1 we get, $h_1 s\,(A_1, P_1) = (A_0, P_0)\,s^{-1} h_2$. In this case,

$$|C_{\mathrm{G}_1}(k_1)| \leq |\mathrm{H}|^2 |\mathrm{GL}_k\,(\mathbb{F}_2) \times \mathrm{S}_n|. \tag{6}$$

Combining Equations (5) and (6), we get $|C_{\mathrm{G}^2 \rtimes \mathbb{Z}_2}(k_1)| = \left(|H|^2 + |\mathrm{H}|\right) |\mathrm{GL}_k\,(\mathbb{F}_2) \times \mathrm{S}_n|$. Putting together above calculations along with $|\mathrm{K}_1| = |\mathrm{H}|^2$, we get

$$S_1 = |\mathrm{H}|^2 \left(\frac{\left(|\mathrm{H}|^2 + |\mathrm{H}|\right)^{\frac{1}{2}}}{|\mathrm{GL}_k\,(\mathbb{F}_2) \times \mathrm{S}_n|^{\frac{1}{2}}} \right). \tag{7}$$

Similar computation for $g_0 \in C_{\mathrm{G}_0}(k_0)$ leads us to two conditions:

i) $h_1(A_0, P_0) = (A_0, P_0)h_1$ i.e., $(A_0, P_0) \in C_{\mathrm{G}}(h_1)$

ii) $s^{-1} h_2 s(A_1, P_1) = (A_1, P_1)\,s^{-1} h_2 s$ i.e., $s\,(A_1, P_1)\,s^{-1} \in C_{\mathrm{G}}(h_2)$.

Thus, there is an upper bound of $C_{\mathrm{G}_0}(k_0)$ by $|C_{\mathrm{G}}(h_1) \cdot C_{\mathrm{G}}(h_2)|$. Hence,

$$\frac{|C_{\mathrm{G}_0}(k_0)|}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|} \leq \frac{|C_{\mathrm{G}}(h_1) \cdot C_{\mathrm{G}}(h_2)|}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|} \leq \frac{|\mathrm{G}| \min(|C_{\mathrm{G}}(h_1)|, |C_{\mathrm{G}}(h_2)|)}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|}. \tag{8}$$

Similar calculation for $C_{\mathrm{G}_1}(k_0)$ gives us the following two conditions:

i) $s\,(A_1, P_1)\,(A_0, P_0)s^{-1} \in C_{\mathrm{G}}(h_2)$.

ii) $(A_1, P_1)(A_0, P_0) \in C_{\mathrm{G}}(h_1)$.

Thus, there is an upper bound of $|C_{\mathrm{G}_1}(k_0)|$ by $|\mathrm{G}| \min(C_{\mathrm{G}}(h_1), C_{\mathrm{G}}(h_2))$. Hence,

$$\frac{|C_{\mathrm{G}_1}(k_0)|}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|} \leq \frac{|\mathrm{G}| \min(|C_{\mathrm{G}}(h_1)|, |C_{\mathrm{G}}(h_2)|)}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|}. \tag{9}$$

Combining Equations (8) and (9), we get

$$\frac{|C_{\mathrm{G}^2 \rtimes \mathbb{Z}_2}(k_0)|}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|} = \frac{|C_{G_0}(k_0)|}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|} + \frac{|C_{G_1}(k_0)|}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|} \leq \frac{\min(|C_{\mathrm{G}}(h_1)|, |C_{\mathrm{G}}(h_2)|)}{|\mathrm{G}|}.$$

Thus,

$$S_0 = \sum_{k_0 \neq e} \left(\frac{|C_{\mathrm{G}^2 \rtimes \mathbb{Z}_2}(k_0)|}{|\mathrm{G}^2 \rtimes \mathbb{Z}_2|} \right)^{\frac{1}{2}} \leq \sum_{(h_1,h_2) \neq (e,e)} \left(\frac{\min(|C_{\mathrm{G}}(h_1)|, |C_{\mathrm{G}}(h_2)|)}{|\mathrm{G}|} \right)^{\frac{1}{2}} \leq \sum_{h \neq e} |\mathrm{H}| \left(\frac{|C_G(h)|}{|\mathrm{G}|} \right)^{\frac{1}{2}}. \tag{10}$$

Again, from orbit-stabilizer theorem,

$$S_0 \leq |\mathrm{H}| \sum_{h \neq e} |h^{\mathrm{G}}|^{-\frac{1}{2}} \tag{11}$$

and thus we have achieved our goal for this section of writing $\mathcal{D}_{\mathrm{K}}$ in terms H. In particular, this can be done by putting multiplicative overhead for $|\mathrm{H}|$ and an additive term given by Equation (7).

$$\mathcal{D}_{\mathrm{K}} \leq |\mathrm{H}| \sum_{h \neq e} |h^{\mathrm{G}}|^{-\frac{1}{2}} + |\mathrm{H}|^2 \left(\frac{\left(|\mathrm{H}|^2 + |\mathrm{H}|\right)^{\frac{1}{2}}}{|\mathrm{GL}_k(\mathbb{F}_2) \times \mathrm{S}_n|^{\frac{1}{2}}} \right). \tag{12}$$

5 Size and minimal degree of H

Note that in the previous section, we have boiled down the indistinguishability of K to conjugacy classes of H. Similar to the work of Kempe and Shalev [18], minimal degree and size of the subgroup play an important role in showing indistinguishability of K. In this section, we give an upper bound on the size of H and the lower bound on minimal degrees.

Before that, we recall some well known definitions.

Definition 5.1. *For any group* $\mathrm{G} \leq \mathrm{G}_1 \times \mathrm{G}_2$ *we define* $\Pi^i(\mathrm{G})$ *as projection of the group* G *on* G_i *for* $i = 1, 2$.

Definition 5.2. *Let* $M_{k,n}$ *be the ring of* $k \times n$ *matrix. Then there is a natural group action of* $S_k \times S_n$ *on* $M_{k,n}$ *given by* $(P_1, P_2)M = P_1^{-1} M P_2$. *Let* $Stab(C)$ *be the stabilizer of* C. *Furthermore,* $T_C := \Pi^1(Stab(C))$.

The main theorem for this section is the following:

Theorem 5.1. *Let* H *be defined by Equation* (3) *for codes following conditions from Section 4.1 then*

(i) $|\mathrm{H}| \leq p^2$

(ii) The minimal degree of $\Pi^1(\mathrm{H}) \geq p - 1$ *and the minimal degree of* $\Pi^2(\mathrm{H}) \geq p - 1$.

To prove the above theorem, the key lemma needed is following:

(weak) Subgroup Decomposition Lemma. *Let* $\mathcal{H}$ *be a parity-check matrix such that it satisfies conditions from Section 4.1 then* $T_C \hookrightarrow S_p \times S_p \times \cdots \times S_p \times AGL(\mathbb{F}_p) \times S_p \times \cdots S_p$. *The direct product is taken* $m_1 - 1$ *terms of* S_p *and one term of affine general linear group.*

This establishes upper and lower bounds on the size and the minimal degree of T_C respectively. Later, we will translate this to that of H. We prove the above theorem by a series of lemmas.

Lemma 5.2. *Let* $(A, P) \in \mathrm{H}$ *then*

$$A = P_1$$

$$P = A^{-1} \oplus P_2 = P_1^{-1} \oplus P_2.$$

where $P_1 \in S_k$ and $P_2 \in S_{n-k}$. Moreover, $P_1 C P_2 = C$ and for each P_1 there is an unique P_2. It then follows, $T_C = \Pi^1(\mathrm{H})$ and $|T_C| = |\mathrm{H}|$.

Proof. Let $(A, P) \in \mathrm{H}$ then by definition we have

$$[\mathrm{I}|C] = A[\mathrm{I}|C]P = [A|AC]P.$$

Since action of right multiplication by P is equivalent to reordering of columns we infer that $[A|AC]$ and $[\mathrm{I}|C]$ have same columns possibly reordered. By construction (in particular condition (ii) in Section 4.1), C and the identity matrix I have no common columns as every column of C contains an element from proper extension. As C and I have distinct columns; A should have same columns as the identity matrix I. So by the action of multiplication by P first k columns must go to themselves, in other words, first k columns make up a permutation matrix of size k. Hence P is block diagonal matrix, having a block of size k and $n-k$ where each of the blocks is a permutation matrix of size k and $n-k$ respectively, we get $P = \sigma_k \oplus \sigma_{n-k}$. Now $A\sigma_k = \mathrm{I}$ gives $A = P_1$ and $P = A^{-1} \oplus P_2$ where $P_1 = {\sigma_k}^{-1}$ and $P_2 = \sigma_{n-k}$. It is easy to see from the fact $\mathcal{H} = [I|C]$ that $P_1 C P_2 = C$.

Clearly, $T_C = \Pi^1(\mathrm{H})$ as T_C being a subgroup, it is closed under inverse. Now, to show uniqueness of P_2 for every P_1, it suffices to prove for every P_1 there is at most one P_2. This follows from $P_1 C P_2 = C$ because no two columns of C are identical and so no two columns of $P_1 C$ are identical. Now P_2 should reorder the columns to give back C which can be done at most in one way. Hence, for every P_1 there is at most one corresponding P_2. □

Now we move to find an upper bound for the size of H by embedding it into direct product of m_1 affine general linear group over $\mathbb{F}_p$.

Lemma 5.3. *If $(P, Q) \in Stab(C)$ then $P = \sum_i E_{i,i} \otimes P_i$ and $Q = \sum_j E_{j,j} \otimes Q_j$ where P_i and Q_j are permutation matrices of size p.*

Proof. Note that the lemma simply says that all $P \in \Pi^1(\mathrm{Stab}(C))$ and all $Q \in \Pi^2(\mathrm{Stab}(C))$ are block diagonal matrices with blocks of size p. We prove the decomposition of Q, similar result for P can be achieved by similar arguments.

Suppose there exists a $Q \in \Pi^2(\mathrm{Stab}(C))$ that can not be decomposed into the block diagonal form. Then there is some i,j such that $Q(i) = j$ and $\left\lfloor \frac{j}{p} \right\rfloor \neq \left\lfloor \frac{i}{p} \right\rfloor$ (corresponding to off block diagonal entry at $P_2(i, j)$). Now by condition (iii) on C, c_i and c_j are not permutation equivalent. And thus i^{th} column of CQ and i^{th} column of C are not permutation equivalent. Thus for any P, the i^{th} column of PCQ can not be equal to i^{th} column of C. Thus for any permutation P, $PCQ \neq C$. Which leads to a contradiction. □

Lemma 5.4. *The group $T_C \hookrightarrow T_{C_{1r_1}} \times T_{C_{2r_2}} \times T_{C_{3r_3}} \times \cdots \times T_{C_{m_1 r_{m_1}}}$ for all $r_i \in \{1, 2, \cdots, m_2 - m_1\}$.*

Proof. By the decomposition above, it follows that for every i, j, we have $PC_{i,j}Q = C_{i,j}$.

$$\begin{aligned} PCQ &= (\Sigma_k E_{kk} \otimes P_k)(\Sigma_{i,j} E_{i,j} \otimes C_{i,j})(\Sigma_l E_{l,l} \otimes Q_l) \\ &= \Sigma_{i,j,k,l}(E_{kk} E_{i,j} E_{ll} \otimes P_k C_{i,j} Q_l) \\ &= \Sigma_{i,j}(E_{i,j} \otimes P_i C_{i,j} Q_j). \end{aligned}$$

The canonical map sending $P \to (P_1, P_2, P_3, \ldots, P_{m_1})$ gives the required inclusion. □

Remark 5.1. *Note that until now, we have used conditions ii) and iii). So, for any C satisfying those conditions, Lemma 5.4 is valid.*

To move further we need a theorem from the theory of permutation groups [8, Section 3.5]. The proof of this theorem requires the classification of finite simple groups.

Theorem 5.5. *Any transitive subgroup of degree prime p must be one of the following:*

(a) The symmetric group S_p or the alternating group A_p.

(b) A subgroup of the affine group on p letters $AGL(\mathbb{F}_p)$.

(c) One of the Mathieu groups M_{11} or M_{23} of degree 11 or 23, respectively.

(d) A projective group G *with $PSL_d(q) \leq G \leq P\Gamma L_d(q)$ of degree $p = \frac{q^{d-1}}{q-1}$.*

Now we apply this theorem on a particular choice of $T_{C_{ir_i}}$. The idea here is to choose a r_i for each i, such that, $T_{C_{ir_i}}$ as described in the Lemma 5.4 can not be (a), (c) or (d). Note that $T_{C_{ir_i}}$ are transitive because they contain the cycle $(1\,2\,3\ \ldots\ p)$, only choice left is a subgroup of the affine group.

Lemma 5.6. *Let C' be a circulant matrix of size p over a field F described by condition* iv) *of Section 4.1 (that is C' is neither a $\sum_k x^k$ nor $bx^{k_0} + \sum_{i \neq k_0} ax^i$) then $T_{C'}$ is neither S_p nor A_p.*

Proof. Consider group $\mathbb{Z}_p \times \mathrm{S}_p$ acting on the set of polynomials from the ring $F[x]/(x^p - 1)$. We want to compute a lower bound for the orbit of this action for a polynomial from the circulant matrix. The action is as follows:

$$(u, P)\left(\sum_{i=0}^{p-1} a_i x^i\right) \mapsto \sum_i a_{(P^{-1}(i))} x^i x^u$$

Notice that if $P \in T_{C'}$ then P should take the first column of C', denoted by c' to some column of C', say column c''. Since C' is a circulant matrix, $c' = \sum_j c'_j x^j$ for $c'_j \in F$. Now the polynomial for the column c'' is $c'x^k \mod (x^p - 1)$ for some k in $\mathbb{Z}_p$. Thus $(-k, P)$ is in the stabilizer of c' in the above action.

Now for C' satisfying condition (iv), the orbit of c', the first column of C' is at least $3p$. This can be seen in the following way:

First notice that if c is any column matrix of size p that is permutation equivalent to c' then c is in the orbit of c'. Thus every possible reordering of c' is also in the orbit. Let m_f denote the number of times of occurrence of f in c'. Then the number of such possible re-orderings is given by $\frac{p!}{\prod_{f \in c'} m_f!}$. This is less than $3p$ only in cases where the number of occurrences are of the form $m_a = p, m_b = 0$ for all $b \neq a$ or $m_b = 1, m_a = p - 1, m_c = 0$ for all $c \neq a, b$ which are precisely the cases forbidden by condition (iv).

Thus

$$|T_{C'}| \leq \left|\mathrm{Stab}(c')\right| = \frac{p!p}{|\mathrm{orbit}(c')|} \leq \frac{p!p}{3p} = \frac{p!}{3}.$$

Thus, $T_{C'}$ is neither S_p nor A_p. □

Lemma 5.7. *The group $T_{C'}$ for a circulant matrix C' of size a prime $p \geq 30$ is a subgroup of the affine group.*

Proof. Since $T_{C'}$ can not be S_p or A_p, the other possible groups are either Matheiu groups M_{11}, M_{23} or a subgroups of $P\Gamma L_d(q)$. These groups can not have an element of order p for $p \geq 30$. But the map $x \mapsto x + 1$ is the cycle $(1\,2\,3\ \ldots\ p)$ and is an element of order p in $T_{C'}$. Thus $T_{C'}$ must be a subgroup of the affine group. □

So, the required decomposition $T_C \hookrightarrow \mathrm{S}_p \times \mathrm{S}_p \times \ldots \times \mathrm{S}_p \times \mathrm{AGL}(\mathbb{F}_p) \times \mathrm{S}_p \times \ldots \times \mathrm{S}_p$ follows. Now we are in a position to reach the main theorem using condition (i).

Lemma 5.8. *If a circulant matrix C' of size a prime p over a field F that follows condition (i), that is its polynomial representation is other than a $\sum_i x^i$ then no two columns of C' are identical.*

Proof. Let $g(x)$ denote the polynomial for circulant C' such that two columns that are identical. Then for some $k_1 \neq k_2$, $x^{k_1}g(x) = x^{k_2}g(x)$. Consider group action of $\mathbb{Z}_p$ on ring $\frac{F[x]}{x^p-1}$. Now $(k_2 - k_1) \in \text{Stab}(g(x))$. As only non-identity of subgroup of $\mathbb{Z}_p$ is itself we get that $\text{Stab}(g(x))$ is whole of $\mathbb{Z}_p$ which is possible only for circulant matrices of polynomials $a\sum_k x^k$. □

One can similarly prove that for such C' no two rows are identical.

Lemma 5.9. *Let C_{ij} be matrices as in condition (i). For all i, j we have, for every P there is at most one solution Q such that $PC_{i,j}Q = C_{i,j}$. Similarly, for each Q there is at most one P such that $PC_{i,j}Q = C_{i,j}$.*

Proof. Since no two columns of $C_{i,j}$ are identical after action of P, no two columns of $PC_{i,j}$ are identical and then there is unique Q that can reorder columns to get back $C_{i,j}$. Similar row argument proves the unique P. □

Lemma 5.10. *Let $P_1, P_2 \in T_c$ under decomposition $P_1 = (P_{11}, P_{12}, \dots P_{1m_1})$ and $P_2 = (P_{21}, P_{22}, \dots, P_{2m_2})$. Then for any i, $P_{1i} \neq P_{2i}$.*

Proof. Suppose there exists i_0 such that $P_{1i_0} = P_{2i_0}$. Now for any j, $P_{1i_0}C_{i_0j}Q_{1j} = P_{2i_0}C_{i_0j}Q_{2j} = C_{i_0j}$ for some permutation matrices Q_{1j}, Q_{2j}. By Lemma 5.9 on $C' = C_{i_0j}$ there is an unique solution Q, we get $Q_{1j} = Q_{2j}$. Again applying Lemma 5.9 on C_{ij} there is an unique solution P and we get $P_{1i} = P_{2i}$ for any i. Thus we have proved that if for some i_0, $P_{1i_0} = P_{2_{i_0}}$ then for all i, $P_{1i} = P_{2i}$ making $P_1 = P_2$. □

Note, this means that there is an injective mapping from the group T_C to the group $T_{C_{ir_i}}$ for any component in the above decomposition. In particular, if we choose C_{ir_i} as a matrix satisfying condition (iv) then that corresponding component is the affine general linear group. Thus we get that $|T_C| \leq |T_{C'}| \leq p^2$.

Corollary 5.11. *The minimal degree of $\Pi^1(\mathrm{H})$ and $\Pi^2(\mathrm{H})$ is at least $p-1$.*

Proof. Clearly, from $T_C = \Pi^1(\mathrm{H})$ in lemma 5.2, we get the minimal degree of $\Pi^1(\mathrm{H})$ to be at least $p-1$. Because, non-identity elements of T_C must be non-identity in affine component of the direct product decomposition (by Lemma 5.10). Moreover, non-identity elements of an affine group can not fix more than one element. So, the minimal degree of $T_C = \Pi^1(\mathrm{H})$ is at least $p-1$. For minimal degree of $\Pi^2(\mathrm{H})$ we show that the minimal degree of $\Pi^2(\mathrm{H})$ is at least as large as that of $\Pi^1(\mathrm{H})$. Note that, if $P_1 \oplus P_2 \in \Pi^2(\mathrm{H})$ is a non-identity element then $P_1 \neq \mathrm{I}$. This follows from the uniqueness of P_2 in Lemma 5.2. Now, the non-identity element P_1 has support of at least the size of the minimal degree of $\Pi^1(\mathrm{H})$ as it is also an element of $\Pi^1(\mathrm{H})$.

Thus minimal degree of $\Pi^2(\mathrm{H})$ is greater than or equal the minimal degree of $\Pi^1(\mathrm{H}) \geq p-1$. □

6 Subgroup K is indistinguishable

In this section, we club the results from last section on bounds on projectors of H into Equation (3) to show that K is indistinguishable. Recall that $\mathrm{G} = \mathrm{GL}_k(\mathbb{F}_2) \times \mathrm{S}_n$ and $\mathrm{H} = \{(A, P) : A\mathcal{H}P = \mathcal{H}\}$. Now from the discussion in previous section, we know that A is a permutation matrix.

Let $h = (\sigma_1, \sigma_2) \in \mathrm{H}$. Then

$$|h^{\mathrm{G}}|^{-\frac{1}{2}} = \frac{|C_{\mathrm{G}}(h)|^{\frac{1}{2}}}{|\mathrm{G}|^{\frac{1}{2}}} = \left(\frac{C_{\mathrm{GL}_k(\mathbb{F}_2)}(\sigma_1)}{|\mathrm{GL}_k(\mathbb{F}_2)|}\right)^{\frac{1}{2}} \left(\frac{C_{\mathrm{S}_n}(\sigma_2)}{|\mathrm{S}_n|}\right)^{\frac{1}{2}}$$

$$= |\sigma_1^{\mathrm{GL}_k(\mathbb{F}_2)}|^{-\frac{1}{2}} |\sigma_2^{\mathrm{S}_n}|^{-\frac{1}{2}} \leq |\sigma_1^{\mathrm{S}_k}|^{-\frac{1}{2}} |\sigma_2^{\mathrm{S}_n}|^{-\frac{1}{2}}.$$

The last inequality follows because the conjugacy class of h in a permutation group is a subset of a conjugacy class in the general linear group. Also note, if h is not the identity in H then $\sigma_1 \neq \mathrm{I}$ and $\sigma_2 \neq \mathrm{I}$ by the uniqueness property in Lemma 5.2.

From Equation (12) we have,

$$\sum_{h\neq e} |h^{\mathrm{G}}|^{-\frac{1}{2}} \leq \sum_{\sigma_1,\sigma_2\neq e} |\sigma_1^{\mathrm{S}_k}|^{-\frac{1}{2}} |\sigma_2^{\mathrm{S}_n}|^{-\frac{1}{2}} = \sum_{\sigma_1\in\Pi^1(\mathrm{H})\setminus e} |\sigma_1^{\mathrm{S}_k}|^{-\frac{1}{2}} \sum_{\sigma_2\in\Pi^2(\mathrm{H})\setminus e} |\sigma_2^{\mathrm{S}_n}|^{-\frac{1}{2}} \tag{13}$$

We present this for sum over σ_1. Similar result can be obtained for σ_2.

Let Γ_t denote the set of elements of S_k of support t. Then from a well-known theorem [17, Theorem B] it follows that there exists an absolute constants b, ε such that if $\Pi^1(\mathrm{H})$ has minimal degree greater than $\delta \geq b$ then $|\Gamma_t| \leq k^{\frac{-\varepsilon\delta}{2}} \binom{k}{t}^{\frac{1}{2}} (t!)^{\frac{1}{4}}$.

From another well known theorem [17, Lemma 8], we know that if $\mathcal{C}$ is a conjugacy class of elements of support t inside S_k. Then $|\mathcal{C}| \geq c\binom{k}{t}\sqrt{t!}t^{-\frac{1}{2}}$ where c is some positive absolute constant.

Therefore,

$$\sum_{\sigma_1\in\Gamma_t} |\sigma_1^{\mathrm{S}_k}|^{-\frac{1}{2}} \leq c^{-\frac{1}{2}} |\Gamma_t| \binom{k}{t} (k!)^{-\frac{1}{4}} k^{\frac{1}{4}}.$$

This gives,

$$\sum_{\sigma_1\in\Pi^1(\mathrm{H})\setminus e} |\sigma_1^{\mathrm{S}_k}|^{-\frac{1}{2}} = \sum_{t=\delta}^{k} \sum_{\sigma_1\in\Gamma_t} |\sigma_1^{\mathrm{S}_k}|^{-\frac{1}{2}}$$

$$\leq \sum_{t=\delta}^{k} c^{-\frac{1}{2}} |\Gamma_t| \binom{k}{t} (k!)^{-\frac{1}{4}} k^{\frac{1}{4}}$$

Substituting,

$$\sum_{\sigma_1\in\Pi^1(\mathrm{H})\setminus e} |\sigma_1^{\mathrm{S}_k}|^{-\frac{1}{2}} \leq \sum_{t=\delta}^{k} c^{-\frac{1}{2}} k^{-\varepsilon\delta} k^{\frac{1}{4}} \leq a_k k^{-\varepsilon\delta} k^{\frac{5}{4}}$$

for some constant $a_k \geq 0$. Similarly we can get an upper bound for the other sum. Thus, we have

$\sum_{\sigma_1\in\Pi^1(\mathrm{H})\setminus e} |\sigma_1^{\mathrm{S}_k}|^{-\frac{1}{2}} \leq a_k k^{-\varepsilon\delta_1} k^{\frac{5}{4}}$

$\sum_{\sigma_1\in\Pi^1(\mathrm{H})\setminus e} |\sigma_1^{\mathrm{S}_n}|^{-\frac{1}{2}} \leq a_n n^{-\varepsilon\delta_2} n^{\frac{5}{4}}$

where δ_1, δ_2 are minimal degrees of $\Pi^1(\mathrm{H})$ and $\Pi^2(\mathrm{H})$. Putting this in Equation (13), we get

$$\sum_{h\neq e} |h^{\mathrm{G}}|^{-\frac{1}{2}} \leq a_k a_n k^{-\varepsilon\delta_1} k^{\frac{5}{4}} n^{-\varepsilon\delta_2} n^{\frac{5}{4}}. \tag{14}$$

Proof of Theorem A. To prove K is indistinguishable, we need to show that $\mathcal{D}_K \leq \big(\log(|\mathrm{G}^2 \rtimes \mathbb{Z}_2|)\big)^{-c}$ for every positive constant c.

From Equation (12), it suffices to prove that,

$$\log\left(|\mathrm{H}| \sum_{h\neq e} |h^{\mathrm{G}}|^{-\frac{1}{2}} + \frac{|\mathrm{H}|\left(|\mathrm{H}| + |\mathrm{H}|^2\right)^{\frac{1}{2}}}{|\mathrm{G}|^{\frac{1}{2}}}\right) \leq \log(\Delta_c)$$

$$\log\left(|\mathrm{H}| \sum_{h\neq e} |h^{\mathrm{G}}|^{-\frac{1}{2}} + \frac{|\mathrm{H}|\left(|\mathrm{H}| + |\mathrm{H}|^2\right)^{\frac{1}{2}}}{|\mathrm{G}|^{\frac{1}{2}}}\right) \leq \log\left(2\max\left\{|\mathrm{H}| \sum_{h\neq e} |h^{\mathrm{G}}|^{-\frac{1}{2}}, \frac{|\mathrm{H}|\left(|\mathrm{H}| + |\mathrm{H}|^2\right)^{\frac{1}{2}}}{|\mathrm{G}|^{\frac{1}{2}}}\right\}\right)$$

$$= \log(2) + \log\left(\max\left\{|\mathrm{H}|\sum_{h\neq e}|h^{\mathrm{G}}|^{-\frac{1}{2}}, \frac{|\mathrm{H}|\left(|\mathrm{H}|+|\mathrm{H}|^2\right)^{\frac{1}{2}}}{|\mathrm{G}|^{\frac{1}{2}}}\right\}\right)$$

Putting $|\mathrm{H}| \leq p^2$, $\delta_1, \delta_2 \geq p-1$ and Equation (14) one can verify that above term is less than $\log(\Delta_c)$ for large enough p.

This completes our proof of indistinguishability of the subgroup K, making the cryptosystem resistant to hidden subgroup attacks. □

7 A variation

In this section we show indistinguishability of the hidden subgroup for a class of quasi-cyclic codes that is slightly different from the one defined by conditions in Section 4.1. This serves two purposes. One, it shows that the class of quasi-cyclic codes can be further extended and two, it shows robustness and adaptability of our proof.

In particular, we show a way to relax condition i) from Section 4.1. We replace two conditions, which are the following:

i′) The integer $m_1 = o(p)$, where p is a prime.

iv′) For every i there exists a j such that the polynomial for $C_{i,j}$ is neither $a\sum_i x^i$ nor $bx^{k_0} + a\sum_{i\neq k_0} x^i$.

Note the trade-off between conditions i) and iv) from our previous set. Condition i) is relaxed from for all i, j to at least one j for every i; whereas condition iv) was needed for at least one i, j and now it is tightened to at least one j for every i. Conditions ii) and iii) carry forward as they were while condition i′) is required to ensure that the size of $|\mathrm{H}|$ does not blow-up. As before, we need a key lemma.

(strong) Subgroup Decomposition Lemma. *Let $\mathcal{H} = [I|C]$ be a parity-check matrix, such that, it satisfies conditions i′), ii), iii),* iv′) *and v) then $T_C \hookrightarrow AGL(\mathbb{F}_p) \times AGL(\mathbb{F}_p) \times \ldots \times AGL(\mathbb{F}_p)$. Direct product is taken m_1 times.*

Proof. First note that since conditions ii) and iii) are still satisfied, (ref. Remark 5.1) Lemma 5.4 holds. Moreover for each i, we can choose $C_{ir_i} = C_{ij}$ that satisfies condition (iv′), in particular, matrices other than given by $a\sum_k x^k$ or $bx^{k_0} + \sum_{i\neq k_0} ax^i$. Now for these matrices $T_{C_{ir_i}}$ is neither S_p or A_p. Now by similar argument to Lemma 5.7 we get that every $T_{C_{ir_i}}$ must be a subgroup of the affine group and we get the required subgroup decomposition. □

This gives an upper bound on the size of H, as $|\mathrm{H}| = |T_C| \leq p^{2m_1}$, and the minimal degree of $\Pi^1(\mathrm{H})$ is bounded by $p-1$ since at least one of the components must be a non-identity for a non-identity element of T_C. This makes minimal degree at least $p-1$. Now the minimal degree of $\Pi^2(\mathrm{H})$ is greater than or equal to $\Pi^1(\mathrm{H})$ by reasoning similar to Corollary 5.11.

Now putting these bounds of $|\mathrm{H}| \leq p^{2m_1}$ and minimal degree of $\Pi^2(\mathrm{H})$ greater than minimal degree of $\Pi^1(\mathrm{H}) \geq p-1$, one can see that with an additional condition (i′) $m_1 = o(p)$, the subgroup K is indistinguishable from the identity subgroup.

8 Conclusion

Niederreiter cryptosystems using quasi-cyclic codes are popular these days. The main reason behind this interest is quantum-security. This makes it a good candidate for post-quantum cryptography. This is evident from the NIST submissions [4, 30].

Historically speaking, post-quantum cryptography grew out of Shor's algorithm to factor integers which was later generalized to the discrete logarithm problem. These algorithms use the hidden subgroup problem in finite abelian groups. This hidden subgroup problem has a natural analog, the scrambler-permutation problem, in the non-commutative situation using characters of irreducible representations of the group. If this hidden subgroup is indistinguishable by the quantum Fourier sampling then we can not solve the corresponding scrambler-permutation problem. This makes Niederreiter cryptosystem quantum secure. The idea behind the hidden subgroup problem for Niederreiter cryptosystem was put forward by Dinh et. al. [7] and the idea of distinguishability of subgroups was put forward by Kempe and Shalev [18].

We prove that for a Niederreiter cryptosystem using quasi-cyclic codes, satisfying certain conditions, the corresponding hidden subgroup is indistinguishable from the identity subgroup by quantum Fourier sampling. This analysis is particularly relevant for the recent NIST submissions in post-quantum cryptography [4, 30].

Acknowledgements

The first author was supported by the Singapore Ministry of Education and the National Research Foundation through the core grants of the Centre for Quantum Technologies and the second author was supported by a MATRICS research grant of SERB, govt. of India. Authors thank Subhamoy Maitra and Joachim Rosenthal for insightful comments.

References

[1] Marco Baldi. *QC-LDPC Code-Based cryptography.* Springer, 2014.

[2] Marco Baldi, Marco Bianchi, Franco Chiaralunce, Joachim Rosenthal, and Davide Schipani. Enhanced public key security for the McEliece cryptosystem. *Journal of Cryptology*, 29(1):1–27, 2016.

[3] Marco Baldi, Marco Bodrato, and Franco Chiaraluce. A new analysis of the McEliece cryptosystem based on QC-LDPC codes. *Security and Cryptography for Networks*, pages 246–262, 2008.

[4] Marco Baldi et al. LEDAcrypt: Low-density parity-check code-based cryptographic systems. NIST round 2 submission for post-quantum cryptography, 2019.

[5] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Attacking and defending the McEliece cryptosystem. In *Post-Quantum Cryptography. PQCrypto 2008*, pages 31–46, 2008.

[6] Philip J. Davis. *Circulant Matrices.* Chelsa Publishing, 1994.

[7] Hang Dinh, Cristopher Moore, and Alexander Russell. McEliece and Niederreiter cryptosystems that resist quantum fourier sampling attacks. In *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *LNCS*, pages 761–779, 2011.

[8] J. D. Dixon and B. Mortimer. *Permutation Groups.* Graduate Texts in Mathematics. Springer, New York, 1996.

[9] Tomáš Fabšič, Viliam Hromada, Paul Stankovski, Pavol Zajac, Qian Guo, and Thomas Johansson. A reaction attack on the QC-LDPC McEliece cryptosystem. In *International Workshop on Post-Quantum Cryptography*, pages 51–68. Springer, 2017.

[10] Michelangelo Grigni, Leonard Schulman, Monica Vazirani, and Umesh Vazirani. Quantum mechanical algorithms for the nonabelian hidden subgroup problem. In *Proceedings of the thirty-third annual ACM symposium on theory of computing*, pages 68–74. ACM, 2001.

[11] Thomas A. Gulliver. *Construction of quasi-cyclic codes*. PhD thesis, University of Victoria, 1989.

[12] Qian Guo, Thomas Johansson, and Paul Stankovski. A key recovery attack on MDPC with CCA security using decoding errors. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 789–815. Springer, 2016.

[13] Sean Hallgrean, Alexander Russell, and Amnon Ta-Shma. The hidden subgroup problem and quantum computation using group representation. *SIAM Journal of Computation*, 32(4):916–934, 2003.

[14] Sean Hallgren, Alexander Russell, and Amnon Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. In *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, STOC '00, pages 627–635, New York, NY, USA, 2000. ACM.

[15] Gábor Ivanyos, Frédéric Magniez, and Miklos Santha. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. *International Journal of Foundations of Computer Science*, 14(05):723–739, 2003.

[16] Upendra Kapshikar and Ayan Mahalanobis. A quantum-secure Niederreiter Cryptosystem using quasi-cyclic codes. In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, ICETE 2018 - Volume 2: SECRYPT, Porto, Portugal, July 26-28, 2018.*, pages 506–513, 2018.

[17] Julia Kempe, Laszlo Pyber, and Aner Shalev. Permutation groups, minimal degrees and quantum computing. *Groups, Geometry, and Dynamics*, 1:553–584, 2007.

[18] Julia Kempe and Aner Shalev. The hidden subgroup problem and permutation group theory. In *Proceedings of the sixteenth annual ACM-SIAM symposium on discrete algorithms*, pages 1118–1125. SIAM, 2005.

[19] Kristine Lally and Patrick Fitzpatrick. Algebraic structure of quasicyclic codes. *Discrete applied Mathematics*, 111:157–175, 2001.

[20] Pil Joong Lee and Ernest F Brickell. An observation on the security of McEliece's public-key cryptosystem. In *Eurocrypt 1988*, volume 330 of *LNCS*, pages 275–280. Springer, 1988.

[21] Zhe Li, Chaoping Xing, and Sze Ling Yeo. Reducing the key size of McEliece cryptosystem from automorphism-induced goppa codes via permutations. In *IACR International Workshop on Public Key Cryptography*, pages 599–617. Springer, 2019.

[22] R. J. McElice. A public key cryptosystem based on algebraic coding theory. Technical report, Communications system research centre, NASA, Jan-Feb 1978.

[23] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo SLM Barreto. MDPC-McEliece: New mceliece variants from moderate density parity-check codes. In *2013 IEEE international symposium on information theory*, pages 2069–2073. IEEE, 2013.

[24] Chris Monico, Joachim Rosenthal, and Amin Shokrollahi. Using low density parity check codes in the McEliece cryptosystem. In *2000 IEEE International Symposium on Information Theory*, page 215. IEEE, 2000.

[25] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Prob. Control and Inf. Theory*, 15(2):159–166, 1986.

[26] Martin Roetteler and Thomas Beth. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. *arXiv preprint quant-ph/9812070*, 1998.

[27] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[28] Jacques Stern. A method for finding codewords of small weight. In *International Colloquium on Coding Theory and Applications*, pages 106–113. Springer, 1988.

[29] John Watrous. Succinct quantum proofs for properties of finite groups. *CoRR*, cs.CC/0009002, 2000.

[30] Atsushi Yamada et al. QC-MDPC KEM: A key encapsulation mechanishm based on the QC-MDPC McEliece encryption scheme. NIST round 1 submission for post-quantum cryptography, 2017.

U. Kapshikar, Center for Quantum Technologies and National Univeristy of Singapore
E-mail address, U. Kapshikar: uskapshikar@gmail.com

A. Mahalanobis (Corresponding author), IISER Pune, Pune, INDIA
E-mail address, A. Mahalanobis: ayan.mahalanobis@gmail.com