A Quantum-Secure Niederreiter Cryptosystem using Quasi-Cyclic Codes

Upendra Kapshikar and Ayan Mahalanobis
IISER Pune, Pune, India

Keywords: Niederreiter Cryptosystem, Post-quantum Cryptography, Quantum Fourier Sampling.

Abstract: In this paper, we describe a new variant of Niederreiter cryptosystem over quasi-cyclic codes of rate $\frac{m-1}{m}$. We show that the proposed cryptosystem is quantum secure, in particular, it resists quantum Fourier sampling and has better transmission rate with smaller keys compared to the one using binary Goppa codes.

1 INTRODUCTION

In this paper, we develop a new Niederreiter cryptosystem using $\frac{m-1}{m}$ quasi-cyclic codes. These are well known *linear block codes*. The main result in this paper is, the Niederreiter cryptosystem built with these codes is *quantum-secure*. Many attempts were made by many distinguished authors to built new McEliece or Niederreiter cryptosystems using different codes. However, none of these authors demonstrated that their cryptosystem is quantum-secure. One of the main reason to study the Niederreiter cryptosystem is that it can be quantum-secure. In today's world designing cryptosystem just got twice as hard. One needs to ensure that it is secure from known classical attacks *as well as* secure from the known quantum attacks, *i.e.*, from the hidden subgroup problem arising out of quantum Fourier sampling.

The concept of security which is tied to quantum Fourier sampling for non-abelian groups has a rich tradition in the work of Hallgreen *et al.* (Hallgrean et al., 2003) and Kempe and Salev (Kempe and Shalev, 2005). Dinh *et al.* (Dinh et al., 2011) using earlier work showed that the McEliece cryptosystem built on binary Goppa codes is quantum-secure. We use their theorem (Dinh et al., 2011, Theorem 4) to show that our proposed cryptosystem is quantum-secure. This work is part of first author's master's thesis (Kapshikar, 2018).

Description of the Parity Check Matrix Used for the Proposed Niederreiter Cryptosystem. Recall that we are talking about $\frac{m-1}{m}$ quasi-cyclic codes over $\mathbb{F}_{2^l}$. For the cryptosystem to be quantum-secure the parity check matrix $\mathcal{H}$ for the $[n=mp, k=(m-1)p]$, $\frac{m-1}{m}$ quasi-cyclic code should satisfy the following conditions:

I. Integers m, p, such that p is a prime and m is bounded above by a polynomial in p.

II. The matrix $\mathcal{H}$ is of size $p \times mp$ over $\mathbb{F}_{2^l}$.

III. The matrix $\mathcal{H}$ is of the form $\mathcal{H} = [C_0 = I \,|\, C_1 \,|\, C_2 \,|\, \ldots \,|\, C_{m-1}]$, where each C_i is a circulant matrix of size p. Each C_i for $i > 0$ should contain an element from a proper extension of $\mathbb{F}_2$. Furthermore, we denote the matrix $\mathcal{H}$ as $[I \,|\, C]$ where C is the concatenation of the circulant matrices C_i, $i > 0$.

IV. We define $T_{\mathcal{H}}$ corresponding to a matrix $\mathcal{H}$ as $T_{\mathcal{H}} = \left\{P_1 \in \mathrm{S}_p \mid \exists P_2 \in \mathrm{S}_{p(m-1)} \text{ s. t. } P_1 C P_2 = C\right\}$, where S_n is the symmetric group acting on n letters. It is easy to see that $T_{\mathcal{H}}$ is a permutation group action on p letters. The condition we impose on $\mathcal{H}$ is that $T_{\mathcal{H}}$ is not 2-transitive.

V. No two columns of C are identical.

For more on quantum security of the proposed cryptosystem a reader can skip to Section 5.

2 REVIEW OF NIEDERREITER CRYPTOSYSTEM

In 1978, Robert McEliece (McElice, 1978) suggested a cryptosystem based on algebraic codes. The system did not gain much popularity then because of its large key sizes. However, with quantum computing becoming a reality, McEliece cryptosystems have become the center of attention for cryptographers. Unlike RSA or ElGamal cryptosystem, McEliece cryptosystem is based on a non-commutative structure

Kapshikar, U. and Mahalanobis, A.
A Quantum-Secure Niederreiter Cryptosystem using Quasi-Cyclic Codes.
DOI: 10.5220/0006843005060513
In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018) - Volume 2: SECRYPT*, pages 340-347
ISBN: 978-989-758-319-3

which allegedly makes it a strong candidate for *post-quantum cryptography*. Compared to traditional cryptosystems, a McEliece cryptosystem has following advantages:

a) It is fast. Faster than RSA or ElGamal.

b) It is believed to be quantum secure.

The disadvantages are the following:

a) The key sizes are huge.

b) The ciphertext becomes much larger than the plaintext because of the redundancy added by the encoding process.

In this paper we focus on building a Niederreiter cryptosystem. Apart from fulfilling the obvious requirement of a signature scheme, Niederreiter cryptosystem is faster compared to a McEliece cryptosystem. Li *et al*. (Li et al., 1994) proved that the security of a McEliece cryptosystem and its Niederreiter counterpart are equivalent under the Lee-Brickell attack (Lee and Brickell, 1988). For these reasons, in this paper our main focus is on **building a Niederreiter cryptosystem**.

All codes in this paper are *linear block codes* and our standard reference for coding theory is Blahut (Blahut, 2003, Chapter 3). A binary linear code $\mathcal{C}$ of length n and rank k is a k dimensional linear subspace of $\mathbb{F}_2^n$. Hamming weight or simply weight t of a codeword means that the codeword has t non-zero entries. Standard distance on $\mathcal{C}$ is the hamming distance. Distance of a linear code $\mathcal{C}$ is defined as minimum distance between two non-zero codewords. Traditionally, such a code is denoted as $[n,k]$ code. The ratio $\frac{k}{n}$ is the transmission rate of the code.

A generator matrix M of an $[n,k]$ linear code $\mathcal{C}$ is a $k \times n$ matrix such that $\mathcal{C} = \{xG : x \in F_q^k\}$. A generator matrix M of the form $[I_k \,|\, G']$ is said to be in the systematic form. A parity check matrix $\mathcal{H}$ of an $[n,k]$ linear code $\mathcal{C}$ is an $(n-k) \times n$ such that $\mathcal{H}x = 0$ if and only if $x \in \mathcal{C}$. A code generated by $\mathcal{H}$ is known as the dual code and denoted by $\mathcal{C}^{\perp}$.

A decoding problem is given $x \in \mathbb{F}_2^n$ find a codeword $c \in \mathcal{C}$ that is closest to x. This problem for a random linear code is called the *general decoding problem* and is known to be NP-hard (Berlekamp et al., 1978). But for some codes this decoding problem can be solved efficiently. If such an algorithm is available for a code $\mathcal{C}$, we say that $\mathcal{C}$ has a decoder.

2.1 Quasi-Cyclic Codes

A quasi-cyclic code (QCC) is a block linear code which is a simple generalisation of the cyclic code. It is such that any cyclic shift of any codeword by m symbols gives another codeword. We are particularly interested in $\frac{m-1}{m}$ rate codes. In particular our system is based on $\frac{m-1}{m}$ rate codes over $\mathbb{F}_{2^l}$. Such codes along with quasi-cyclic codes of rate $\frac{1}{m}$ were studied in great detail by Gulliver (Gulliver, 1989).

Definition 2.1 (Circulant matrix)**.** *A square matrix is called circulant if every row, except for the first row, is a circular right shift of the row above that.*

A rate $\frac{m-1}{m}$ systematic QCC has an $p \times mp$ parity check matrix of the form $\mathcal{H} = [I_p \,|\, C_1 \,|\, C_2 \,|\, \ldots \,|\, C_{m-1}]$ where each C_i is a circulant matrix of size p and I_p is the identity matrix of size p.

For compactness we denote $\mathcal{H} = [I \,|\, C]$. In a recent work Aylaj *et al.* (Aylaj et al., 2016) found a way to construct generator matrices for such codes over $\mathbb{F}_2$. Since these generator matrices are in systematic form one can easily construct parity check matrix from these generator matrices. As said previously, our main interest lies in codes over extension fields. Gulliver (Gulliver, 1989, Chapter 6) shows that quasi-cyclic codes over extension fields can be MDS (maximum distance separable) codes. As the name suggests, MDS codes can achieve large minimum distance and so there would be no low weight codewords. This plays an imporatnt role in the classical security of McEliece and Niederreiter cryptosystems, such as the Stern's attack and the Lee-Brickell attack. Though Gulliver (Gulliver, 1989) only presents examples of MDS codes with rate $\frac{1}{m}$, he does present a case to study quasi-cyclic codes of rate $\frac{m-1}{m}$ with large minimum distances.

2.2 Decoding

Quasi-cyclic codes are well studied and well established codes and depending on how one constructs them there are various decoders available. We briefly mention some of them here. Gulliver (Gulliver, 1989, Appendix B) presents a ML (majority logic) decodable QCCs. Another new and intersting way of decoding quasi-cyclic codes using Gröbner basis can be found in the work of Zeh and Ling (Zeh and Ling,).

2.3 Niederreiter Cryptosystem

Let $\mathcal{H}$ be a $k \times n$ parity check matrix for a $[n, n-k]$ linear code $\mathcal{C}$ for which a fast decoding algorithm exists. Let t 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 t. 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 such that weight of z is at most t 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 thus recover $\mathcal{X}$.

For further details on Niederreiter cryptosystem the reader is referred to (Niederreiter and Xing, 2009, Chapter 6).

3 CLASSICAL ATTACKS

In this seciton we briefly go over the generic classical attacks against McEliece and Niederreiter cryptosystems. We also mention some attacks exploiting the circulant structures in the keys. Interestingly, Li *et al.* (Li et al., 1994, Section III) proved (see also (Niederreiter and Xing, 2009, Theorem 6.4.1)) that both McElice and Niederreiter cryptosystems are equivalent in terms of classical security. The proof follows from the fact that the encryption equation for one can be reduced to the other. This implies the equivalence of security of both the cryptosystems for attacks that try to extract the plaintext from a ciphertext.

Most generic attacks over algebraic code based cryptosystems are *information set decoding attacks*(ISD). Two most popular ways of implementing ISD attacks are by Lee and Brickell (Lee and Brickell, 1988) and Stern (Stern, 1988). As mentioned by Baldi *et al*. (Baldi et al., 2008) ISD attacks are the best known attacks with the least work factor as far as classical cryptanalysis is considered. Hence these work factors are considered as security levels for a McEliece and Niederreiter cryptosystems.

The basic idea behind one of the attacks was suggested by McEliece himself. Lee and Brickell (Lee and Brickell, 1988) improved the attack and added an important verification step where attacker confirms that recovered message is the correct one. In this case, we are dealing with a McEliece cryptosystem over a $[n,k]$ linear code. The strategy is based on repeatedly selecting k bits at random from a n-bit ciphertext in hope that none of the selected bits are part of the error. Similar attacks can also be implemented over Niederreiter cryptosystems. Lee and Brickwell also provided a closed-form equation for complexity of the attack. As our system is based on $(n = mp, k = (m-1)p, d_{min} = 2\mathcal{E}+1)$ code the expression for minimal work factor (with $\alpha = \beta = 1$ as taken by Lee and Brickell) takes the following form

$$W_{min} = W_2 = T_2\left((m-1)^3 p^3 + (m-1)pN_2\right)$$

where $T_2 = \dfrac{1}{Q_0 + Q_1 + Q_2}$ and $Q_i = \binom{\mathcal{E}}{i}\binom{n-\mathcal{E}}{k-i} / \binom{n}{k}$ with $N_2 = 1 + k + \binom{k}{2}$.

In Table 1 we present numerical data for work factor for diferent values of parameters. Recently, Aylaj *et al.* (Aylaj et al., 2016) developed an algorithm to construct stack-circulant codes with high error correcting capacity which makes the proposed Niederreiter cryptosystem much more promising.

Other ISD attacks are based on a strategy given by Stern. To recover the intentional error vector e in a McEliece cryptosystem such strategies use an extension code C'' generated by generator matrix $M'' = \begin{bmatrix} M' \\ x \end{bmatrix}$. Bernstein *et al*. (Bernstein et al.,) later improved this attack. Probability of success and work factor for Stern's attack is described in (Hirotomo et al., 2005). In Table 1 we also provide probability of success for parameters $l = 16$ and $A_w \approx n - k$. Both the parameters can be optimized further to obtain the least work factor but not much variation is seen as we change any of these parameters. With such low probabilities, it is clear that the work factor for Stern's attack is worse than the Lee-Brickell attack. Even when one considers improvements suggested by Bernstein *et al.* (Bernstein et al.,), Lee-Brickell's (Lee and Brickell, 1988) attack seems to outperform the attack by Bernstein *et al.* as it produces speedup upto 12 times and hence the security of the system against the Lee-Brickell attack should be considered the security of the system. Key sizes should be devised according to that.

Another attack worth mentioning for quasi-cyclic codes is the attack on the dual code. This attack works only if the dual code has really low weight codewords and is often encountered only when sparse parity check matrices are involved. For example, McEliece with QC-LDPC (Baldi et al., 2008). Such attacks can easily be stopped by choosing codes that do not have low weight codewords. From the work of Aylaj *et al*. (Aylaj et al., 2016) this can be achieved.

After this discussion on classical security we now move towards quantum-security of the proposed McEliece and Niederreiter cryptosystems which is one of the major goal of this paper.

4 QUANTUM ATTACKS

4.1 Hidden Subgroup Problem

Quantum Fourier sampling works behind the scene for almost all known quantum algorithms. It is the reason Shor's algorithm for factoring and solving the discrete logarithm problem works. The main idea in this paper is to show that quantum Fourier sampling will not work in some situations, in particular, a Niederreiter cryptosystem using quasi-linear $\frac{m-1}{m}$ codes.

However, before we go there let us briefly sketch how quantum Fourier sampling is used to break a McEliece or Niederreiter cryptosystems. We recall, the scrambler-permutation attack (Dinh et al., 2011, Section 2). This structural attack is exactly same for a McEliece or a Niederreiter cryptosystem except that instead of finding a scrambler-permutation pair from generator matrix M to M' one has to find scrambler-permutation pair from parity check matrix $\mathcal{H}$ to $\mathcal{H}'$. The problem essentially remains the same. In this attack, we assume $\mathcal{H}$ and $\mathcal{H}'$ are known, the attack is to find A and B. Notice that finding any A' and B' such that $A'\mathcal{H}B' = \mathcal{H}'$ will also make the attack successful.

Definition 4.1 (Hidden Shift Problem)**.** *Let* G *be a group. Let f_0 and f_1 be two functions from group* G *to a set* X*. Given $f_0(g) = f_1(g_0 g)$ the task is to find a constant $g_0 \in$ G. Note that there can be many g_0 that satisfy the above condition. Hidden shift problem asks us to find any one of those constants.*

Let $M' = AMB$. A Niederreiter cryptosystem will be broken if we find one possible pair (A,B) from M and M'. Consider two functions from group $\mathrm{G} = \mathrm{GL_k}(\mathbb{F}_2) \times \mathrm{S_n}$ given by

$$f_0(A,B) = A^{-1}MB \tag{1}$$

$$f_1(A,B) = A^{-1}M'B. \tag{2}$$

Then one can check that $f_1(A,B) = f_0((A_0^{-1},B_0).(A,B))$, that is A_0^{-1},B_0 is the shift between f_0 and f_1. Hence, if one can solve the hidden shift problem over $\mathrm{G} = \mathrm{GL_k}(\mathbb{F}_2) \times \mathrm{S_n}$ he can break the Niederreiter cryptosystem. The general procedure to solve this hidden shift problem is to reduce it to a hidden subgroup problem.

Definition 4.2 (Hidden Subgroup Problem)**.** *Let* G *be a group and f a function*[1] *from* G *to a set* X*. We know that $f(g_0) = f(g_1)$ if and only if $g_0\mathrm{H} = g_1\mathrm{H}$ for some subgroup* H*. The problem is, given f find a generating set for the unknown subgroup* H*.*

[1]The function f in the hidden subgroup problem is said to be separating cosets of H as f is constant on a each coset and different on different cosets.

We can now reduce the hidden shift problem with functions f_0 and f_1 defined above on the group $\mathrm{G} = \mathrm{GL_k}(\mathbb{F}_2) \times \mathrm{S_n}$ to the hidden subgroup problem over $(\mathrm{G} \times \mathrm{G}) \rtimes \mathbb{Z}_2$ (Dinh et al., 2011, Section 2.2). The hidden subgroup in this case is

$$\mathrm{K} = (((\mathrm{H}_0, s^{-1}\mathrm{H}_0 s), 0) \cup ((\mathrm{H}_0 s, s^{-1}\mathrm{H}_0), 1)), \tag{3}$$

where $\mathrm{H}_0 = \{(A,P) \in \mathrm{GL_k}(\mathbb{F}_2) \times \mathrm{S_n} : \mathrm{A}^{-1}\mathrm{MP} = \mathrm{M}\}$ and s is a shift from f_0 to f_1.

In short, the scrambler-permutation problem is one of the key ways to attack a Niederreiter cryptosystem. This problem can be formulated as a hidden shift problem which further can be reduced to a hidden subgroup problem. So we can attack Niederreiter cryptosystems by trying to solve a hidden subgroup problem over $(\mathrm{G} \times \mathrm{G}) \rtimes \mathbb{Z}_2$ where $\mathrm{G} = \mathrm{GL_k}(\mathbb{F}_2) \times \mathrm{S_n}$.

4.2 Successful Quantum Attacks

In the previous section we saw that solving the hidden subgroup problem as a standard way to attack a Niederreiter cryptosystem. An interesting question is, when is the hidden subgroup problem hard to solve? This way we can ensure the security of a Niederreiter cryptosystem against known quantum attacks.

We briefly sketch some thoughts behind effectiveness of QFS. The algorithm of QFS in a general scenario and its use for solving the hidden subgroup problem is very well explained by Grigni *et al.* (Grigni et al., 2001). Arguments particular to Niederreiter cryptosystems and corresponding hidden subgroup problem are described in details by Dinh *et al.* (Dinh et al., 2011, Section 3). The standard model of QFS yields a probability distribution as a function of the hidden subgroup. The basic idea behind *indistinguisability* of two subgroups H_1 and H_2 with probability distributions $\mathsf{P}_{\mathrm{H}_1}$ and $\mathsf{P}_{\mathrm{H}_2}$ is that $\mathsf{P}_{\mathrm{H}_1}$ and $\mathsf{P}_{\mathrm{H}_2}$ are *very close*. For the purpose of defining closeness we need to define a metric on the space of probability distributions. In this case, the metric chosen is the total variation distance between two distributions. This follows from the work of Kempe and Shalev (Kempe and Shalev, 2005). Later Dinh *et al.* (Dinh et al., 2011) used the $\mathcal{L}_1$ distance to define distinguishability. Furthermore, the probability distribution for the hidden subgroup problem with the identity subgroup gives us the uniform distribution (Dinh et al., 2011, Section 3.2). When that is the case, QFS will not give us much information to solve the hidden subgroup problem. Kempe and Shalev (Kempe and Shalev, 2005) provided a necessary condition to distinguish a subgroup of S_n from the trivial subgroup $\langle e \rangle$. Later Dinh *et al.* (Dinh et al., 2011) extended this result while keeping the group relevant to

a Niederreiter cryptosystem in mind. Their result can be viewed as a study of the hidden subgroup problem for the group $G = (GL_k(\mathbb{F}_2) \times S_n)^2 \rtimes \mathbb{Z}_2$ which is the group for Niederreiter cryptosystems. They demonstrated a case when the hidden subgroup H can not be distinguished from either its conjugate subgroups gHg^{-1} or the trivial subgroup $\langle e \rangle$ and proved a general result on a sufficient condition for indistinguishibility (Dinh et al., 2011, Theorem 4). We use their result to prove that the proposed Niederreiter cryptosystem is quantum-secure.

First note that weak Fourier sampling gives the same distributions for all the conjugate subgroups, *i.e.*, P_H is the same as $P_{gHg^{-1}}$. Hence weak Fourier sampling can not differentiate a subgroup from its conjugate subgroup. Thus it suffices to look at strong Fourier sampling. Dinh *et al.* (Dinh et al., 2011), inspired by the work of Kempe and Shalev (Kempe and Shalev, 2005) defines distinguishability of a subgroup H by strong Fourier sampling.

Definition 4.3 (Distinguishability of a subgroup by strong QFS)**.** *We define distinguishability of a subgroup* H *of a group* G*, denote it by* D_H*, to be the expectation of the squared* $\mathcal{L}_1$ *distance between* $P_{gHg^{-1}}$ *and the uniform distribution, where* $g \in G$*. In other words,*

$$D_H := \mathbf{E}_{\rho,g}\left[\|P_{gHg^{-1}}(\cdot|\rho) - P_{\langle e\rangle}(\cdot|\rho)\|_1^2\right].$$

A subgroup H *is called* indistinguishable *by strong Fourier sampling if* $D_H \leq log^{-\omega(1)}|G|$*. The* ρ *above belongs to the set of irreducible complex representations of the group* G*.*

Note that if a subgroup H is indistinguishable according to this definition then by Markov's inequality, for all $c > 0$, $\|P_{gHg^{-1}}(\cdot|\rho) - P_{\{e\}}(\cdot|\rho)\|_{t.v.} \leq log^{-c}|G|$ which is analogous to the definition provided by Kempe and Shalev (Kempe and Shalev, 2005) for indistinguishability of a subgroup by weak Fourier sampling.

We now define the minimal degree of a permutation group, the automorphism group of a matrix (as defined by Dinh (Dinh et al., 2011, Section 4.2)) and recall the definition of T_M for a $k \times n$ matrix M.

Definition 4.4 (Automorphism Group)**.** *The automorphism group of M is defined as* $\mathrm{Aut}(M) = \{P \in S_n$ *such that there exists* $A \in GL_k(\mathbb{F}_q),\ AMP = M\}$.

Definition 4.5 (Minimal Degree)**.** *The minimal degree of a permutation group* $G \leqslant S_n$ *acting on set of n symbols is defined to be minimum number of elements moved by a non-identity element of the group* G*.*

Definition 4.6. *Consider a* $k \times n$ *matrix M, we define* T_M *for the matrix* $M = [I_k|M^*]$ *as* $T_M = \{\mathcal{P}_1 \in S_k$ *such that there exists* $\mathcal{P}_2 \in S_{n-k}$ *with* $\mathcal{P}_1 M^* \mathcal{P}_2 = M^*\}$.

We will use the following theorem which we state for the convinience of the reader.

Theorem 4.1 (Dinh *et al.* (Dinh et al., 2011, Theorem 4))**.** *Assume* $q^{k^2} \leqslant n^{an}$ *for some constant* $0 < a < 1/4$*. Let m be the minimal degree of the automorphism group Aut(M). Then for sufficiently large n, the subgroup K,* $D_K \leqslant O(|K|^2 e^{-\delta m})$*, where* $\delta > 0$ *is a constant.*

5 PROPOSED CRYPTOSYSTEM

In this section we explain the proposed Niederreiter cryptosystem and establish its quantum security against the hidden subgroup attack.

Recall that our variant of the Niederreiter cryptosystem consists of a parity check matrix $\mathcal{H}$ defined as follows: The matrix $\mathcal{H}$ is an array of circulants in the systematic form[2], that is, $\mathcal{H} = [C_0 = I\,|\,C_1\,|\,C_2\,|\,\ldots\,|\,C_{m-1}]$ where each C_i is a circulant matrix of size p (a prime) over $\mathbb{F}_{2^l}$. For simplicity let us denote $[C_1\,|\,C_2\,|\,\ldots\,|\,C_{m-1}]$ as C so that $\mathcal{H} = [I\,|\,C]$. Recall the conditions of the parity check matrix $\mathcal{H}$ from Section 1. A parity check matrix $\mathcal{H}$ satisfying these conditions is easy to construct. We present a way to do so in the next section. Before that, we prove security of the proposed Niederreiter cryptosystem against quantum attacks.

5.1 Proof of Indistinguishability

We prove indistinguishibility in a sequence of lemmas.

Lemma 5.1. *Let* $P \in \mathrm{Aut}(\mathcal{H})$ *then* $P = P_1 \oplus P_2$ *where* P_1 *is a block of size p and* P_2 *is a block of size* $(m-1)p$ *and* $P_1 \oplus P_2$ *is a block diagonal matrix of size* $mp \times mp$ *with the top block* P_1 *and the bottom block* P_2*.*

Proof. Let $P \in \mathrm{Aut}(\mathcal{H})$, from the definition of automorphism there is an A such that $A\mathcal{H}P = \mathcal{H}$. This implies that

$$A\,[I\,|\,C]\,P = [A\,|\,AC]\,P = [I\,|\,C].$$

As action of right multiplication by a permutation matrix permute columns, the above equality shows that $[A\,|\,AC]$ has same columns as $[I\,|\,C]$ possibly in different order. Now since every column of C contains an entry from a proper extension of $\mathbb{F}_q$, no column of A can be column of C. This forces A to have same columns as I and AC to have same columns as that of C. Hence P permutes first p columns within

[2]A systematic matrix is a matrix whose first block is the identity.

themselves and last $(m-1)p$ columns in themselves. Hence every $P \in \mathrm{Aut}(\mathcal{H})$ can be broken into $P_1 \oplus P_2$ so that P_1 acts on I and P_2 acts on C. •

The next lemma is central to quantum-security. It gives us a way to move from $\mathcal{H}$ to C by noting, the P_1 from the $P \in \mathrm{Aut}(\mathcal{H})$ is actually a member of $T_{\mathcal{H}}$.

Lemma 5.2. *The cardinality of* $\mathrm{Aut}(\mathcal{H})$ *is the cardinality of the set* $\{(P_1,P_2)\}$ *that satisfy* $P_1CP_2 = C$ *where* $\mathcal{H} = [I\,|\,C]$ *as defined earlier.*

Proof. The proof follows from the fact, if P belongs to $\mathrm{Aut}(\mathcal{H})$, then $P = P_1 \oplus P_2$. Then $A\,[I\,|\,C]\,P = [I\,|\,C]$ translates into $A\,[I\,|\,C]\,(P_1 \oplus P_2) = [I\,|\,C]$. Keeping in mind the block diagonal nature of P, it follows that $[AIP_1\,|\,ACP_2] = [I\,|\,C]$. Then $A = P_1^{-1}$ and $P_1^{-1}CP_2 = C$. This proves the lemma. •

The next lemma proves that for each P_1 there is atmost one P_2.

Lemma 5.3. *Cardinality of the set* $\{(P_1,P_2)$ *that satisfy* $P_1CP_2 = C\}$ *equals* $|T_{\mathcal{H}}|$.

Proof. Recall that $T_{\mathcal{H}} = \{P_1$ that satisfy $P_1CP_2 = C\}$. So it suffices to show that for every P_1 there is at most one P_2. Since no two columns of C are identical, no two columns of P_1C are identical. Hence, there is at most one way to re-order them to get back C. Thus for every P_1 there is at most one P_2. •

Theorem 5.4 (Burnside (Dixon and Mortimer, 1996, Theorem 3.5B))**.** *Let* G *be a subgroup of* $Sym(\mathbb{F}_p)$ *containing a* p*-cycle* $\mu : \xi \mapsto \xi + 1$. *Then* G *is either 2-transitive or* $G \leq A\mathrm{GL}_1(\mathbb{F}_\mathrm{p})$ *where* $A\mathrm{GL}_1(\mathbb{F}_\mathrm{p})$ *is the affine group over* p.

We prove a theorem on the size of the automorphism group of $\mathcal{H}$.

Theorem 5.5. *If* $\mathcal{H}$ *satisfies conditions I,II and III then* $|\mathrm{Aut}(\mathcal{H})| \leqslant \mathrm{p}(\mathrm{p}-1)$.

Proof. From Lemma 5.2 and Lemma 5.3, the group $\mathrm{Aut}(\mathcal{H})$ has same size as $T_{\mathcal{H}}$. It is now easy to check that the circulant matrix μ with first row $[0,1,0,\ldots,0]$ of size p belongs to $T_{\mathcal{H}}$. The corresponding P_2 will be a block diagonal $(m-1)p$ matrix with blocks of size p and each consisting of μ^{-1}. Now notice that the circulant matrix μ corresponds to the p-cycle $\xi \mapsto \xi + 1$. By our condition III, $T_{\mathcal{H}}$ is not 2-transitive. Now by Burnside's theorem $T_{\mathcal{H}} \leq A\mathrm{GL}_1(\mathbb{F}_\mathrm{p})$. Thus $|\mathrm{Aut}(\mathcal{H})| \leqslant \mathrm{p}(\mathrm{p}-1)$. •

After this bound on the size of the automorphism group we move towards the minimal degree of the Automorphism group.

Lemma 5.6. *The minimal degree of* $\mathrm{Aut}(\mathcal{H})$ *is bounded below by* $p-1$.

Proof. Notice that any $P \in \mathrm{Aut}(\mathcal{H}) = \mathrm{P}_1 \oplus \mathrm{P}_2$. By the twist, from $P \in \mathrm{Aut}(\mathcal{H})$ to $P_1^{-1} \in T_{\mathcal{H}}$, it is easy to see that $P_1 \in A\mathrm{GL}_\mathrm{k}(\mathbb{F}_\mathrm{q})$. Then $P_1(x) = ax + b \pmod q$ for some $a,b \in \mathbb{F}_q$. If P fixes two distinct points, then $a = 1$ and $b = 0$ is the only possible solution. This corresponds to the identity element and thus a non-identity element can not fix more that one point. So minimal degree of $\mathrm{Aut}(\mathcal{H})$ is bounded below by $p-1$. •

We now prove the main theorem of this paper.

Theorem 5.7. *Let* p *be a prime and* m *a positive integer bounded above by a polynomial in* p*, such that,* $p \leq \frac{1}{4}m(\log m + \log p)$. *Then the subgroup* K *(Equation 3) defined above is indistinguishable.*

Proof. We will use Theorem 4.1 in this proof. First note, the minimal degree is bounded below by $p-1$. Now it is well known that $|K| = 2|H_0|^2$ and $|H_0| = |\mathrm{Aut}(\mathcal{H})| \times |\mathrm{Fix}(\mathcal{H})|$. We have shown that $|\mathrm{Aut}(\mathcal{H})| \leq \mathrm{p}(\mathrm{p}-1)$ and it is easy to see that $|\mathrm{Fix}(\mathcal{H})| = 1$. Putting all these together, we see that $|K|^2 e^{-\delta p} \leq 4p^8 e^{-\delta p}$ for some positive constant δ. However, from the bound on the size of m, it is obviously true that $4p^8 e^{-\delta p} \leq (mp\log(mp))^{-\omega(1)}$ for large enough p.

Now, if $p \leq am(\log m + \log p)$, then $p^2 \leq amp(\log m + \log p)$ which gives $2^{p^2} \leq (mp)^{amp}$ for $0 < a < \frac{1}{4}$. This satisfies the premise of Theorem 4.1 and hence K is indistinguishable. •

5.2 Constructing the Parity Check Matrix

Now we address the last question about the proposed Niederreiter cryptosystem, how to construct a matrix $\mathcal{H}$ satisfying conditions I - V? Clearly, conditions I, II and III are trivial to set up and deserve no special attention. We suggest a particular way for construction of parity check matrix $\mathcal{H}$ so that condition IV is satisfied. It should be noted that there may be other ways to satisfy condition IV as well.

Choose a pair of distinct elements $a,b \in F_{q^l}$. Now construct $\mathcal{H}$ such that C_1 contains both a and b exactly once in each column and no other C_i contains both a and b. We restate this condition as our condition IV′. We could have replaced C_1 by any other C_i for $i > 1$ and the proof remains the same. For sake of simplicity we stick with C_1.

IV′ Two distinct elements $a,b \in F_{q^l}$ occurs as entries of C_1 exactly once in each column and no other C_i contain both a and b.

Table 1: Parameters for the proposed Niederreiter cryptosystem.

Security in bits	p	t	m_C	m_Q	m	Probability of success	Public Key Size		Rate
							No. rows	No. cols	
80-bits	101	15	17	35	35	2^{-132}	101	3535	0.60
		20	9	35	35	2^{-190}	101	3535	0.77
	211	35	4	62	62	2^{-398}	211	13082	0.71
		40	3	62	62	2^{-465}	211	13082	0.80
100-bits	101	15	40	35	40	2^{-136}	101	4040	0.61
		20	17	35	35	2^{-190}	101	3535	0.77
	211	35	5	62	62	2^{-398}	211	13082	0.71
		40	5	62	62	2^{-465}	211	13082	0.80
120-bits	101	15	95	35	95	2^{-171}	101	9595	0.67
		20	32	35	35	2^{-190}	101	3535	0.77
	211	35	8	62	62	2^{-398}	211	13082	0.71
		40	6	62	62	2^{-465}	211	13082	0.80
256-bits	211	35	98	62	98	2^{-443}	211	20678	0.75
		20	55	62	62	2^{-465}	211	13082	0.80

Lemma 5.8. *If the matrix $\mathcal{H}$ satisfies* IV$'$*, it also satisfies* IV.

Proof. Let $\mathcal{P}_1 \in T_{\mathcal{H}}$. From $\mathcal{P}_1 C \mathcal{P}_2 = C$ it follows that $\mathcal{P}_1 C$ should have the same set of columns as C but possibly in a different order. Let α denote the row of a in the first column of C_1 and β denote the row of b in the same column. Now notice that every column in C that contains both a and b contains them such that difference between rows of a and b is $\alpha - \beta \bmod p$ where p is the size of each circulant matrix. Now let $\sigma \in T_{\mathcal{H}}$ such that it sends β to α and α to β. It then follows from the fact that p is a odd prime, $\alpha = \beta$ which contadicts our assumption. Hence, $T_{\mathcal{H}}$ is not 2 transitive. •

Condition V can be easily satisfied using brute force and other means and this completes the construction of a parity check matrix $\mathcal{H}$ satisfying I - V and hence, a **Niederreiter cryptosystem that resists quantum Fourier sampling** is found.

6 ADVANTAGES OF THE PROPOSED CRYPTOSYSTEM

One of the prime advantages of our proposed cryptosystem is quantum-security. Apart from that it also has high transmission rate which translated into high encryption rate. It is known that the current McEliece cryptosystem built on Goppa codes has transmission rate of about 0.52. For a McEliece cryptosystem its rate is same as that of the transmission rate of the underlying code and is $\frac{k}{n}$. Niederreiter cryptosystems have a slightly different rates due to difference in their encryption algorithm. For a general cryptosystem its encryption rate or information rate can be defined as follows (Niederreiter and Xing, 2009, Chapter 6):

Let $\mathcal{S}(C)$ denote possible number of palintexts and $\mathcal{T}(C)$ denote possible number of ciphertexts then information rate of the system is defined by

$$\mathcal{R}(C) = \frac{\log \mathcal{S}(C)}{\log \mathcal{T}(C)}.$$

This information rate can be viewed as amount of information contained in one bit of ciphertext.

Our proposed Niederreiter cryptosystem have good encryption rate (see Table 1). This gives the proposed cryptosystem an edge over those constructed on classical Goppa codes or with GRS codes (generalized Reed-Solomon codes).

As discussed before another problem with McEliece and Niederreiter cryptosystems is large key size. Circulant matrices is a good choice when it comes to key-sizes. Matrices are 2-dimensional objects but circulant matrices behave like a 1-dimensional object as they can be described by their first row. Though this circulant structure is lost in public key due to the scrambler-permutation pair, the size of the key still remains smaller than the conventional Niederreiter cryptosystem. Our system is slightly better than original Niederreiter cryptosystem because of the less number of rows in the public key matrices. With $p = 101$, this number is less than one-tenth of the original Niederreiter cryptosystem. Though there are two factors that increases the size of the matrix in our variant compared to original McEliece: one, our matrices have large number

of columns and two, our system is based on extension field $\mathbb{F}_{2^l}$ which makes the effective size of the matrix l times compared to McEliece which is based on $\mathbb{F}_2$. However, in most cases due to less number of rows the net result indicates that our system requires shorter keys than original McEliece. For instance, at 80-bit security with $p = 101$ and $l = 3$ our keys are almost half of the keys corresponding to original McEliece at same security level. At 256-bit security level with $p = 211, t = 40$ and $l = 3$ the proposed cryptosystem has key size of about one-forth of the original McEliece.

In Table 1, we provide some parameters for the proposed Niederreiter cryptosystem and show in details the benefits of the proposed cryptosystem. There are two kind of attacks – classical and quantum. For the classical we come out with a value of m and call it m_C and for quantum we call it m_Q. The maximim of these two is the m that one should use for that said parameter. As explained earlier we use p for the size of the matrix and t as the error correcting capacity. We also provide success probability from classical attack, key size and the rate of the cryptosystem.

7 CONCLUSION

In this paper, we develop a Niederreiter cryptosystem using quasi-cyclic codes that is both classically and quantum secure against the current known attacks. In particular, we show that for the proposed cryptosystem the hidden subgroup problem from the natural reduction of the corresponding scrambler-permutation problem is indistinguishable by quantum Fourier sampling. We also show that the proposed cryptosystem has high encryption rate and shorter keys compared to classical McEliece cryptosystems. One of the important problem that needs to be addressed is finding quasi-cyclic codes that satisfy the suggested parameter sizes. It would be interesting to see if the cryptosystem remains classically secure if we use other sparse keys. It is very clear that the system remains secure against quantum computers as the group structure for the system remains the same. This is important because it could reduce key sizes substantially.

REFERENCES

Aylaj, B., Belkasmi, M., Nouh, S., and Zouaki, H. (2016). Good quasi-cyclic codes from circulant matrices concatenation using a heuristic model. *International journal of advanced computer science and applications*, 7(9):63–68.

Baldi, M., Bodrato, M., and Chiaraluce, F. (2008). A new analysis of the McEliece cryptosystem based on QC-LDPC codes. *Security and Cryptography for Networks*, pages 246–262.

Berlekamp, E., McEliece, R., and Van Tilborg, H. (1978). On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386.

Bernstein, D. J., Lange, T., and Peters, C. Attacking and defending the McEliece cryptosystem. In *Post-Quantum Cryptography. PQCrypto 2008*, pages 31–46.

Blahut, R. E. (2003). *Algebraic codes for data transmission*. Cambridge University Press.

Dinh, H., Moore, C., and Russell, A. (2011). McEliece and Niederreiter cryptosystems that resist quantum fourier sampling attacks. volume 6841 of *LNCS*. Crypto2011.

Dixon, J. D. and Mortimer, B. (1996). *Permutation Groups*. Graduate Texts in Mathematics. Springer, New York.

Grigni, M., Schulman, L., Vazirani, M., and Vazirani, U. (2001). 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.

Gulliver, T. A. (1989). *Construction of quasi-cyclic codes*. PhD thesis, University of Victoria.

Hallgrean, S., Russell, A., and Ta-Shma, A. (2003). The hidden subgroup problem and quantum computation using group representation. *SIAM Journal of Computation*, 32(4):916–934.

Hirotomo, M., Mohri, M., and Morii, M. (2005). A probabilistic computation method for the weight distribution of low-density parity-check codes. In *International Symposium on Information Theory*.

Kapshikar, U. (2018). McEliece-type cryptosystems over quasi-cyclic codes. Master's thesis, IISER Pune. https://arxiv.org/abs/1805.09972.

Kempe, J. and Shalev, A. (2005). The hidden subgroup problem and permutation group theory. In *Proceedings of the sixteenth annual ACM-SIAM symposium on discrete algorithms*, pages 1118–1125. Society for Industrial and Applied Mathematics.

Lee, P. J. and Brickell, E. F. (1988). An observation on the security of McEliece's public-key cryptosystem. In *Eurocrypt 1988*, volume 330 of *LNCS*, pages 275–280. Springer.

Li, Y. X., Deng, R. H., and Wang, X. M. (1994). On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273.

McElice, R. J. (1978). A public key cryptosystem based on algebraic coding theory. Technical report, Communications system research centre, NASA.

Niederreiter, H. and Xing, C. (2009). *Algebraic Geometry in Coding Theory and Cryptography*. Princeton University Press.

Stern, J. (1988). A method for finding codewords of small weight. In *International Colloquium on Coding Theory and Applications*, pages 106–113. Springer.

Zeh, A. and Ling, S. Decoding of quasi-cyclic codes up to a new lower bound on the minimum distance. In *2014 IEEE International Symposium on Information Theory, Honolulu, HI, 2014*.