Quantum Resistant Public Key Encryption Scheme HermitianRLCE ⋆ ⋆⋆

Gretchen L. Matthews[1] and Yongge Wang[2]

[1] Virginia Polytechnic Institute and State University, Blacksburg, VA 24061, USA
gmatthews@vt.edu
[2] UNC Charlotte, 9201 University City Blvd., NC 28223, USA yonwang@uncc.edu

Abstract. Recently, Wang (2017) introduced a random linear code based quantum resistant public key encryption scheme RLCE which is a variant of McEliece encryption scheme. Wang (2017) analyzed an instantiation of RLCE scheme using Generalized Reed-Solomon codes. In this paper, we introduce and analyze Hermitian code based RLCE schemes HermitianRLCE. Based on our security analysis, we provide HermitianRLCE parameters at the 128, 192, and 256 bits security level. These parameters show that HermitianRLCE has much smaller public keys than GRS-RLCE.

Key words: Random linear codes; McEliece encryption scheme; linear code based encryption scheme

1 Introduction

Since McEliece encryption scheme [8] was introduced more than thirty years ago, it has withstood many attacks and still remains unbroken for general cases. It has been considered as one of the candidates for post-quantum cryptography since it is immune to existing quantum computer algorithm attacks. The original McEliece cryptography system is based on binary Goppa codes. Several variants have been introduced to replace Goppa codes in the McEliece encryption scheme though most of them have been broken. Up to the writing of this paper, secure McEliece encryption schemes include MDPC/LDPC code based McEliece encryption schemes [1,9], Wang's RLCE [12,13], and the original binary Goppa code based McEliece encryption scheme. The advantage of the RLCE encryption scheme is that its security does not depend on any specific structure of underlying linear codes, instead its security is believed to depend on the NP-hardness of decoding random linear codes.

The RLCE scheme [12,13] could be used as a template to design encryption schemes based on any linear codes. Wang [12,13] analyzed Generalized Reed-Solomon code based RLCE security. This paper proposes a Hermitian code based RLCE scheme. It is shown that Hermitian code based RLCE scheme has smaller key sizes compared with Generalized Reed-Solomon code based RLCE schemes. For example, for the AES

⋆ The first author is supported by NSF-DMS 1855136.
⋆⋆ The second author is supported by Qatar Foundation Grant NPRP8-2158-1-423.

128, 192, and 256 security levels, the GRS-RLCE schemes have public keys of size 183KB, 440KB, and 1203KB respectively. For HermitianRLCE schemes, the corresponding public keys are of the size 103KB, 198KB, 313KB respectively. It should be noted that several authors have tried to design algebraic-geometric code based McEliece encryption scheme (see, e.g., [6]). However, most of these algebraic-geometric code based McEliece encryption schemes have been broken (see, e.g., [3]). Hermitian RLCE provides an alternative approach which combines the algebraic geometric construction based on Hermitian curves (and more generally, the extended norm-trace curves) with that of a random linear code.

Unless specified otherwise, bold face letters such as $\mathbf{a}, \mathbf{b}, \mathbf{e}, \mathbf{f}, \mathbf{g}$ are used to denote row or column vectors over $\mathbb{F}_q$. It should be clear from the context whether a specific bold face letter represents a row vector or a column vector.

2 McEliece and RLCE Encryption schemes

For given parameters n, k and t, the McEliece scheme [8] chooses an $[n, k, 2t+1]$ linear Goppa code $\mathcal{C}$. Let G_s be the $k \times n$ generator matrix for the code $\mathcal{C}$. Select a random dense $k \times k$ non-singular matrix S and a random $n \times n$ permutation matrix P. Then the public key is $G = SG_sP$ and the private key is G_s. The following is a description of encryption and decryption processes.

$\texttt{Mc.Enc}(G, \mathbf{m}, \mathbf{e})$. For a message $\mathbf{m} \in \{0,1\}^k$, choose a random vector $\mathbf{e} \in \{0,1\}^n$ of weight t and compute the cipher text $\mathbf{c} = \mathbf{m}G + \mathbf{e}$

$\texttt{Mc.Dec}(S, G_s, P, \mathbf{c})$. For a received ciphertext $\mathbf{c}$, first compute $\mathbf{c}' = \mathbf{c}P^{-1} = \mathbf{m}SG$. Next use an error-correction algorithm to recover $\mathbf{m}' = \mathbf{m}S$ and finally compute the message $\mathbf{m}$ as $\mathbf{m} = \mathbf{m}'S^{-1}$.

The protocol for the RLCE Encryption scheme by Wang [12] consists of the following three processes:
$\texttt{RLCE.KeySetup}$, $\texttt{RLCE.Enc}$, and $\texttt{RLCE.Dec}$. Specifically the revised RLCE scheme proceeds as follows.

$\texttt{RLCE.KeySetup}(n, k, d, t, w)$. Let $n, k, d, t > 0$, and $w \in \{1, \cdots, n\}$ be given parameters such that $n-k+1 \geq d \geq 2t+1$. Let G_s be a $k \times n$ generator matrix for an $[n, k, d]$ linear code $\mathcal{C}$ such that there is an efficient decoding algorithm to correct at least t errors for this linear code given by G_s. Let P_1 be a randomly chosen $n \times n$ permutation matrix and $G_sP_1 = [\mathbf{g}_0, \cdots, \mathbf{g}_{n-1}]$.

1. Let $\mathbf{r}_0, \mathbf{r}_1, \cdots, \mathbf{r}_{w-1} \in \mathbb{F}_q^k$ be column vectors drawn uniformly at random and let
$$G_1 = [\mathbf{g}_0, \cdots, \mathbf{g}_{n-w}, \mathbf{r}_0, \cdots, \mathbf{g}_{n-1}, \mathbf{r}_{w-1}] \tag{1}$$
be the $k \times (n+w)$ matrix obtained by inserting column vectors $\mathbf{r}_i$ into G_sP_1.
2. Let $A_0 = \begin{pmatrix} a_{0,00} & a_{0,01} \\ a_{0,10} & a_{0,11} \end{pmatrix}, \cdots, A_{w-1} = \begin{pmatrix} a_{w-1,00} & a_{w-1,01} \\ a_{w-1,10} & a_{w-1,11} \end{pmatrix} \in \mathbb{F}_q^{2\times 2}$ be non-singular 2×2 matrices chosen uniformly at random such that $a_{i,00}a_{i,01}a_{i,10}a_{i,11} \neq 0$ for all $i = 0, \cdots, w-1$. Let $A = \text{diag}[1, \cdots, 1, A_0, \cdots, A_{w-1}]$ be an $(n+w) \times (n+w)$ non-singular matrix.

3. Let S be a random dense $k \times k$ non-singular matrix and P_2 be an $(n+w) \times (n+w)$ permutation matrix.
4. The public key is the $k \times (n+w)$ matrix $G = SG_1AP_2$ and the private key is (S, G_s, P_1, P_2, A).

$\texttt{RLCE.Enc}(G, \mathbf{m}, \mathbf{e})$. For a row vector message $\mathbf{m} \in \mathbb{F}_q^k$, choose a random row vector $\mathbf{e} = [e_0, \ldots, e_{n+w-1}] \in \mathbb{F}_q^{n+w}$ such that the Hamming weight of $\mathbf{e}$ is at most t. The cipher text is $\mathbf{c} = \mathbf{m}G + \mathbf{e}$.

$\texttt{RLCE.Dec}(S, G_s, P_1, P_2, A, \mathbf{c})$. For a received cipher text $\mathbf{c} = [c_0, \ldots, c_{n+w-1}]$, compute

$$\mathbf{c}P_2^{-1}A^{-1} = \mathbf{m}SG_1 + \mathbf{e}P_2^{-1}A^{-1} = [c'_0, \ldots, c'_{n+w-1}].$$

Let $\mathbf{c}' = [c'_0, c'_1, \cdots, c'_{n-w}, c'_{n-w+2}, \cdots, c'_{n+w-2}]$ be the row vector of length n selected from the length $n+w$ row vector $\mathbf{c}P_2^{-1}A^{-1}$. Then $\mathbf{c}'P_1^{-1} = \mathbf{m}SG_s + \mathbf{e}'$ for some error vector $\mathbf{e}' \in \mathbb{F}_q^n$ where the Hamming weight of $\mathbf{e}' \in \mathbb{F}_q^n$ is at most t. Using an efficient decoding algorithm, one can recover $\mathbf{m}SG_s$ from $\mathbf{c}'P_1^{-1}$. Let D be a $k \times k$ inverse matrix of SG'_s where G'_s is the first k columns of G_s. Then $\mathbf{m} = \mathbf{c}_1 D$ where $\mathbf{c}_1$ is the first k elements of $\mathbf{m}SG_s$. Finally, calculate the Hamming weight $wt = \texttt{wt}(\mathbf{c} - \mathbf{m}G)$. If $wt \leq t$ then output $\mathbf{m}$ as the decrypted plaintext. Otherwise, output error.

3 Hermitian codes

Consider the curve X given by

$$y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y = x^u \tag{2}$$

over the field $\mathbb{F}_{q^r}$ where $u | \frac{q^r-1}{q-1}$. Notice that when $u = \frac{q^r-1}{q-1}$, the equation (2) gives

$$Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q} = N_{\mathbb{F}_{q^r}/\mathbb{F}_q}.$$

When $r = 2$ and $u = \frac{q^r-1}{q-1}$, the equation (2) gives

$$y^q + y = x^{q+1}$$

over $\mathbb{F}_{q^2}$ which is the defining equation of the Hermitian curve. In general, the genus of X is

$$g = \frac{(u-1)(q^{r-1}-1)}{2}$$

and X has at least

$$\bar{n} = q^{r-1} + u(q^r - q^{r-1})$$

affine $\mathbb{F}_{q^r}$-rational points. We are interested in taking $q^r = 2^8$ which gives several options for r and q as shown in Table 1.

The Hermitian code over $\mathbb{F}_{q^2}$ is defined using the Hermitian curve $y^q + y = x^{q+1}$. To begin, fix $n \leq q^3$ and $2g + 1 < \alpha < n$. Select n distinct $\mathbb{F}_{q^2}$-rational affine points

$P_1, \ldots, P_n$ on X. Thus, each P_i is of the form P_{ab} where $a, b \in \mathbb{F}_{q^2}$ and $b^q + b = a^{q+1}$. Let $D = P_1 + \cdots + P_n$, and set

$$\mathcal{B} := \{x^i y^j : i \geq 0, 0 \leq j \leq q-1, iq + j(q-1) \leq \alpha\};$$

one may note that $\mathcal{B}$ is a basis for the vector space $\mathcal{L}(\alpha P)$, where P denotes the point at infinity on X. In the Hermitian code $C(D, \alpha P)$, the message is a polynomial $f \in \mathrm{Span}(\mathcal{B})$, and the codeword of the message polynomial f is the evaluations of f over the Hermitian curve. More precisely, $C = C(D, \alpha P)$ is the image of the evaluation map

$$\begin{aligned} ev : \mathcal{L}(\alpha P) &\to \mathbb{F}_{q^2}^n \\ f &\mapsto (f(P_1), \cdots, f(P_n)). \end{aligned}$$

It is noted that for the Hermitian code $C(D, \alpha P)$ with $\alpha \geq 2g - 1$, the length is n, the dimension is $\alpha + 1 - g$, and the minimum distance satisfies $d \geq n - \alpha$. The exact minimum distances are known [14].

4 HermitianRLCE

HermitianRLCE is an RLCE encryption scheme with Hermitian code as the underlying code. Specifically, HermitianRLCE replaces the the generator matrix G_s utilized in `RLCE.KeySetup`(n, k, d, t, w) in Section 2 with a Hermitian code $k \times n$ generator matrix.

5 Security analysis

In the following sections, we carry out heuristic security analyses on the revised RLCE scheme.

5.1 Classical and quantum Information-Set Decoding

Information-set decoding (ISD) is one of the most important message recovery attacks on McEliece encryption schemes. The state-of-the-art ISD attack for non-binary McEliece scheme is the one presented in Peters [10], which is an improved version of Stern's algorithm [11]. For the RLCE encryption scheme, the ISD attack is based on the number of columns in the public key G instead of the number of columns in the private key G_s. The cost of ISD attack on an $[n, k, t; w]$-RLCE scheme is equivalent to the cost of ISD attack on an $[n + w, k; t]$-McEliece scheme.

For the naive ISD, one first uniformly selects k columns from the public key and checks whether it is invertible. If it is invertible, one multiplies the inverse with the corresponding ciphertext values in these coordinates that correspond to the k columns of the public key. If these coordinates contain no errors in the ciphertext, one recovers the plain text. To be conservative, we may assume that randomly selected k columns from the public key is invertible. For each $k \times k$ matrix inversion, Strassen algorithm takes $O(k^{2.807})$ field operations (though Coppersmith-Winograd algorithm takes $O(k^{2.376})$

field operations in theory, it may not be practical for the matrices involved in RLCE encryption schemes). In a summary, the naive information-set decoding algorithm takes approximately $2^{\kappa_c'}$ steps to find k-error free coordinates where, by Sterling's approximation,

$$\begin{aligned}\kappa_c' &= \log_2\left(\frac{\binom{n+w}{k}\left(k^{2.807}+k^2\right)}{\binom{n+w-t}{k}}\right) \\ &\simeq (n+w)I\left(\frac{k}{n+w}\right) - (n+w-t)I\left(\frac{k}{n+w-t}\right) + \log_2\left(k^{2.807}+k^2\right)\end{aligned} \tag{3}$$

and $I(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy of x. There are several improved ISD algorithms in the literature. These improved ISD algorithms allow a small number of error positions within the selected k ciphertext values or select $k+\delta$ columns of the public key matrix for a small number $\delta > 0$ or both.

An HermitianRLCE scheme is said to have quantum security level κ_q if the expected running time (or circuit depth) to decrypt a HermitianRLCE ciphertext using Grover's algorithm based ISD is 2^{κ_q}. For a function $f : \{0,1\}^l \to \{0,1\}$ with the property that there is an $x_0 \in \{0,1\}^l$ such that $f(x_0) = 1$ and $f(x) = 0$ for all $x \neq x_0$, Grover's algorithm finds the value x_0 using $\frac{\pi}{4}\sqrt{2^l}$ Grover iterations and $O(l)$ qubits. Specifically, Grover's algorithm converts the function f to a reversible circuit C_f and calculates

$$|x\rangle \xrightarrow{C_f} (-1)^{f(x)}|x\rangle$$

in each of the Grover iterations, where $|x\rangle$ is an l-qubit register. Thus the total steps for Grover's algorithm is bounded by $\frac{\pi|C_f|}{4}\sqrt{2^l}$.

For the HermitianRLCE scheme, the quantum ISD attack first uniformly selects k columns from the public key and checks whether it is invertible. If it is invertible, one multiplies the inverse with the ciphertext. If these coordinates contain no errors in the ciphertext, one recovers the plain text. Though Grover's algorithm requires that the function f evaluate to 1 on only one of the inputs, there are several approaches (see, e.g., Grassl et al [5]) to cope with cases that f evaluates to 1 on multiple inputs.

For randomly selected k columns from a RLCE encryption scheme public key, the probability that the ciphertext contains no errors in these positions is $\frac{\binom{n+w-t}{k}}{\binom{n+w}{k}}$. Thus the quantum ISD algorithm requires $\sqrt{\binom{n+w}{k}/\binom{n+w-t}{k}}$ Grover iterations. For each Grover iteration, the function f needs to carry out the following computations:

1. Compute the inverse of a $k \times k$ sub-matrix G_{sub} of the public key and multiply it with the corresponding entries within the ciphertext. This takes $O\left(k^{2.807}+k^2\right)$ field operations if Strassen algorithm is used.
2. Check that the selected k positions contain no errors in the ciphertext. This can be done with one of the following methods:
   (a) Multiply the recovered message with the public key and compare the differences from the ciphertext. This takes $O((n+w)k)$ field operations.
   (b) Use the redundancy within message padding scheme to determine whether the recovered message has the correct padding information. The cost for this operation depends on the padding scheme.

It is expensive for circuits to use look-up tables for field multiplications. Using Karatsuba algorithm, Kepley and Steinwandt [7] constructed a field element multiplication circuit with gate counts of $7 \cdot (\log_2 q^2)^{1.585}$. In a summary, the above function f for the HermitianRLCE quantum ISD algorithm could be evaluated using a reversible circuit C_f with $O\left(7\left((n+w)k + k^{2.807} + k^2\right)(\log_2 q^2)^{1.585}\right)$ gates. To be conservative, we may assume that a randomly selected k-columns sub-matrix from the public key is invertible. Thus Grover's quantum algorithm requires approximately

$$7\left((n+w)k + k^{2.807} + k^2\right)(\log_2 q^2)^{1.585}\sqrt{\frac{\binom{n+w}{k}}{\binom{n+w-t}{k}}} \tag{4}$$

steps for the simple ISD algorithm against HermitianRLCE encryption scheme.

5.2 Schur product attacks on algebraic geometric codes

Couvreur, Marquez-Corbella, and Pellikaan [4] introdcued a Schur product based attack on algebraic geometry codes based McEliece encryption schemes. Their attack can decrypt any encrypted message in $O(n^3)$ operations after computing an Error Correcting Pair in $O(n^4)$ operations. Specifically, their attack works for high genus algebraic geometry codes. In this section, we show how to choose parameters for HermitianRLCE scheme to avoid the attacks in [4].

For two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length n, the star product code $\mathcal{C}_1 * \mathcal{C}_2$ is the vector space spanned by $\mathbf{a} * \mathbf{b}$ for all pairs $(\mathbf{a}, \mathbf{b}) \in \mathcal{C}_1 \times \mathcal{C}_2$ where $\mathbf{a} * \mathbf{b} = [a_0 b_0, a_1 b_1, \cdots, a_{n-1} b_{n-1}]$. For the square code $\mathcal{C}^2 = \mathcal{C} * \mathcal{C}$, we have $\dim \mathcal{C}^2 \leq \min\left\{n, \binom{\dim \mathcal{C}+1}{2}\right\}$. For an $[n, k]$ Hermitian code $\mathcal{C}$ with $2g < \alpha < \frac{n+1}{2}$, it follows from [4, Corollary 6] that $\dim \mathcal{C}^2 = 2k + g - 1$. The following is a brief proof on this fact. Note that $g = \frac{q(q-1)}{2}$. Fix $\mathcal{C} = \mathcal{C}(\alpha P)$. We claim $\mathcal{C}^2 = \mathcal{C}(2\alpha P)$. Suppose $W \in \mathcal{C}^2$. Then $W = (f(P_1)h(P_1), \cdots, f(P_n)h(P_n)) = (fh(P_1), \cdots, fh(P_n))$ for some $f, h \in \mathcal{L}(\alpha P)$. But $fh \in \mathcal{L}(2\alpha P)$ since $(fh) = (f) + (h) \geq -\alpha P - \alpha P = -2\alpha P$. Thus we have $W \in \mathcal{C}(2\alpha P)$. An argument in [4] could be used to show that $\mathcal{C}(2\alpha P)$.

Let G be the public key for an (n, k, d, t, w) HermitianRLCE encryption scheme based on a Hermitian code. Let $\mathcal{C}$ be the code generated by the rows of G. Let $\mathcal{D}_1$ be the code with a generator matrix D_1 obtained from G by replacing the randomized $2w$ columns with all-zero columns and let $\mathcal{D}_2$ be the code with a generator matrix D_2 obtained from G by replacing the $n - w$ non-randomized columns with zero columns. Since $\mathcal{C} \subset \mathcal{D}_1 + \mathcal{D}_2$ and the pair $(\mathcal{D}_1, \mathcal{D}_2)$ is an orthogonal pair, we have $\mathcal{C}^2 \subset \mathcal{D}_1^2 + \mathcal{D}_2^2$. It follows that

$$2k + g - 1 \leq \dim \mathcal{C}^2 \leq \min\{2k + g - 1, n - w\} + 2w \tag{5}$$

where we assume that $2w \leq k^2$. In the following discussion, we assume that *the* $2w$ *randomized columns in* $\mathcal{D}_2$ *behave like random columns in the attacks of [4]* . In all of our selected HermitianRLCE parameters, we have $2k + g - 1 > n - w$. Thus $\dim \mathcal{C}^2 = \mathcal{D}_1^2 + \mathcal{D}_2^2 = n - w + \mathcal{D}_2^2 = n + w$. Furthermore, for any code $\mathcal{C}'$ of length n' that is obtained from $\mathcal{C}$ using code puncturing and code shortening, we have $\dim \mathcal{C}'^2 = n'$.

Thus the techniques in [4] could not be used to recover any non-randomized columns in D_1.

As we have mentioned in the preceding paragraph, our selected parameters satisfies the condition $2k + g - 1 > n - w$. Thus plain filtration attacks will not identify the randomized columns. However, one may select $w' < w$ columns from the public key and shorten these w' columns. A similar analysis as in Couvreur, Lequesne, and Tillich [2] shows that if these w' columns are the added random columns, then the resulting code is a $(k-w') \times (n-w')$ HermitianRLCE code with $w-w'$ added random columns. In order for one to verify that w' columns are added random columns, one needs to observe that

$$2(k - w') + g - 1 + {w'}^2 < \min\{(k - w')^2, n - w'\} \tag{6}$$

In our parameter selection, we make sure that for all $w' < w$, the inequality (6) does not hold.

6 Recommended parameters

In this section, we propose parameters for HermitianRLCE schemes with equivalent security levels of AES-128, AES-192, and AES-256. If we take the code $C(D, \alpha P)$ where $D = P_1 + \cdots + P_n$ and $q(q-1) < \alpha < n$, then we have $k = \alpha + 1 - g$ and $d \geq n - \alpha$. That is, the Hermitian code will correct at least $t = \frac{n-\alpha-1}{2}$ errors. In this section, we will use the Hermitian curve with the parameter $q = 16$, $r = 2$, and $u = 17$ in Table 1. That is, we will work on the finite field $\mathbb{F}_{2^8}$ and the Hermitian curve contains $2^{12} = 4096$ elements with $g = 120$. Table 2 lists the parameters for HermitianRLCE encryption scheme at the security levels 128, 192, and 256 bits where κ_c is the classical security level and κ_q is the quantum security level. As a comparison, we also include the corresponding public key size for Generalized Reed-Solomon code based RLCE schemes. It is noted that for security level 128 and 192, HermitianRLCE's public key size is approximiately 80% of the GRS-RLCE public key size. For the security level 256, HermitianRLCE's public key size is approximiately 72% of the GRS-RLCE public key size.

7 HermitianRLCE with other extended norm-trace curves

In Section 6, we proposed HermitianRLCE parameters for Hermitian curves with $q = 16$, $r = 2$, and $u = 17$. It would be interesting to know whether other curves have advantages in reducing the public key sizes and improve the encryption/decryption performance. A product Hermitian code has dimension $2k + g - 1$ which is "closer" to the product code dimension of a random code (compared with the dimension $2k - 1$ for the product code of a GRS code). Thus smaller values w in HermitianRLCE schemes are sufficient to defeat filtration attacks. The smaller choice of w has significantly reduced the public key size of HermitianRLCE schemes (compared with GRS-RLCE schemes). However, the value of w should be sufficiently larger so that $\binom{n+w}{w} \geq 2^{128}$ (respectively 2^{192} and 2^{256}) for the security level of AES-128. For the parameter $q = 4$, $r = 4$,

and $u = 5$, Table 3 lists the parameters for HermitianRLCE encryption scheme at the security levels 128 and 192. For this parameter set, it is not possible to choose a parameter sets for the 256-bit security level since the Hermitian curve contains 1024 points. The public key size is relatively larger for the parameters $q = 4$, $r = 4$, and $u = 5$.

As another example, we analyze security levels for HermitianRLCE schemes based on extended norm-trace curves with parameter $q = 4$, $r = 4$, and $u = 17$. Table 4 lists the parameters for HermitianRLCE encryption schemes at the security levels 128, 192, and 256. The public key size is significantly larger for the parameters $q = 4$, $r = 4$, and $u = 17$.

Our analysis in Tables 2, 3, 4 shows that other extended norm-trace curves with smaller genus can be used to build HermitianRLCE schemes with smaller public key sizes. Thus the preferred extended norm-trace for HermitianRLCE encryption schemes are based on Hermitian curves with $q = 16$, $r = 2$, and $u = 17$

References

1. M. Baldi, M. Bodrato, and F. Chiaraluce. A new analysis of the mceliece cryptosystem based on QC-LDPC codes. In *Security and Cryptography for Networks*, pages 246–262. Springer, 2008.
2. A. Couvreur, M. Lequesne, and J.-P. Tillich. Recovering short secret keys of RLCE in polynomial time. *arXiv preprint arXiv:1805.11489*, 2018.
3. A. Couvreur, A. Otmañi, and J.-P. Tillich. Polynomial time attack on wild McEliece over quadratic extensions. In *Advances in Cryptology–EUROCRYPT 2014*, pages 17–39. Springer, 2014.
4. Alain Couvreur, Irene Márquez-Corbella, and Ruud Pellikaan. A polynomial time attack against algebraic geometry code based public key cryptosystems. In *Information Theory (ISIT), 2014 IEEE International Symposium on*, pages 1446–1450. IEEE, 2014.
5. M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt. Applying Grover's algorithm to AES: quantum resource estimates. In *Proc. Int. Workshop PQC*, pages 29–43. Springer, 2016.
6. H. Janwa and O. Moreno. Mceliece public key cryptosystems using algebraic-geometric codes. *Designs, Codes and Cryptography*, 8(3):293–307, 1996.
7. S. Kepley and R. Steinwandt. Quantum circuits for F_{2^m}-multiplication with subquadratic gate count. *Quantum Information Processing*, 14(7):2373–2386, 2015.
8. R.J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN progress report*, 42(44):114–116, 1978.
9. R. Misoczki, J.-P. Tillich, N. Sendrier, and P. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In *Proc. IEEE ISIT 2013*, pages 2069–2073, 2013.
10. C. Peters. Information-set decoding for linear codes over F_q. In *Proc. Int. Workshop PQC*, pages 81–94. Springer, 2010.
11. J. Stern. A method for finding codewords of small weight. In *Coding theory and applications*, pages 106–113. Springer, 1989.
12. Y. Wang. Quantum resistant random linear code based public key encryption scheme RLCE. In *Proc. IEEE ISIT*, pages 2519–2523, July 2016.
13. Y. Wang. Revised quantum resistant public key encryption scheme RLCE and IND-CCA2 security for McEliece schemes. In *IACR ePrint https://eprint.iacr.org/2017/206.pdf*, July 2017.

14. Kyeongcheol Yang and P. Vijay Kumar. On the true minimum distance of hermitian codes. In Henning Stichtenoth and Michael A. Tsfasman, editors, *Coding Theory and Algebraic Geometry*, pages 99–107, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg.

Table 1. Parameters for Hermitian Curves

q	r	u	$\bar{n}$	g
16	2	17	4096	120
4	4	5	1024	126
		17	3328	504
		85	16384	2646
2	8	3	512	127
		5	768	254
		15	2048	889
		17	2304	1016
		51	6656	3175
		85	11008	5334
		255	32768	16129

Table 2. Parameters for HermitianRLCE scheme with $q = 16$, $r = 2$, and $u = 17$

ID	κ_c	κ_q	n	k	t	w	cipher bytes	sk	pk bytes	GRS-RLCE pk bytes
0	128	84	635	280	118	22	635		105560	188001
1	192	118	870	421	165	33	870		202922	450761
2	256	148	1090	531	220	45	1090		320724	1232001

Table 3. Parameters for HermitianRLCE scheme with $q = 4$, $r = 4$, and $u = 5$

ID	κ_c	κ_q	n	k	t	w	cipher bytes	sk	pk bytes	GRS-RLCE pk bytes
0	128	84	640	295	110	22	640		108265	188001
1	192	118	870	435	155	33	870		203580	450761

Table 4. Parameters for HermitianRLCE scheme with $q = 4$, $r = 4$, and $u = 17$

ID	κ_c	κ_q	n	k	t	w	cipher bytes	sk	pk bytes	GRS-RLCE pk bytes
0	128	84	1270	357	205	22	1270		333795	188001
1	192	118	1540	537	250	33	1540		556332	450761
2	256	148	1810	687	310	45	1810		802416	1232001