Secure Random Linear Code Based Public Key Encryption Scheme RLCE

Yongge Wang
KINDI Center for Computing Research
Qatar University, Qatar
and
Department of SIS, UNC Charlotte, USA
Email: yongge.wang@uncc.edu

Abstract

As potential post-quantum cryptographic schemes, lattice based encryption schemes and linear codes based encryption schemes have received extensive attention in recent years. Though LLL reduction algorithm has been one of the major cryptanalysis techniques for lattice based cryptographic systems, cryptanalysis techniques for linear codes based cryptographic systems are generally scheme specific. In recent years, several important techniques such as Sidelnikov-Shestakov attack and filtration attacks have been developed to crypt-analyze linear codes based encryption schemes. Though most of these cryptanalysis techniques are relatively new, they prove to be very powerful and many systems have been broken using these techniques. Thus it is important to systematically investigate and design linear code based cryptographic systems that are immune against these attacks. This paper proposes linear code based encryption schemes RLCE which share many characteristics with random linear codes. Our analysis shows that the scheme RLCE is secure against existing attacks and we expect that the security of the RLCE scheme is equivalent to the hardness of decoding random linear codes.

Index Terms

Random linear coding, McEliece Encryption scheme, secure public key encryption scheme.

I. Introduction

With rapid technology developments for quantum computing, our society is concerned with the security of current PKI infrastructures which are fundamentatal for Internet services. The core components for current PKI infrastructures are based on public cryptographic techniques such as RSA and DSA. However, it has been shown that these public key cryptographic techniques could be easily broken by quantum computers. Thus it is urgent to develop public key cryptographic systems that are secure against quantum computing.

Since the McEliece encryption scheme [14] 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 cryptographic system is based on Goppa codes. Several variants have been introduced to replace Goppa codes in the McEliece encryption scheme. For example, Niederreiter [17] introduced generalized Reed-Solomon codes' based scheme and Berger and Loidreau [2] recommended sub codes of Niederreiter's scheme. Sidelnikov [20] used Reed-Muller codes, Janwa and Moreno [8] used algebraic geometry codes, Baldi et al [1] used LDPC codes, Misoczki et al [15] used MDPC codes, and Löndahl and Johansson [11] used convolutional codes. Most of them have been broken though MDPC/LDPC codes based McEliece encryption schemes [1], [15] and the original Goppa codes based McEliece encryption scheme are still considered secure.

Goppa codes based McEliece encryption scheme is hard to attack since Goppa codes share many characteristics with random codes. Recently, Faugere et al [7] designed an algorithm to distinguish a random code from a high rate Goppa code. Márquez-Corbella and Pellikaan [13] simplified the distinguisher in [7] using component-wise product of codes. The product codes are used to define the square of a code which can be used to distinguish a high rate Goppa code from a random code.

Sidelnikov and Shestakov [21] show that for a given generalized Reed-Solomon code based McEliece encryption scheme, one can efficiently recover the parameters for the generalized Reed-Solomon code from the public key.

Using component-wise product of codes and techniques from [21], Wieschebrink [24] shows that Berger and Loidreau's sub codes [2] of Niederreiter's scheme could be broken efficiently also. A general filtration technique based on distinguisher (see, Couvreur et al [5]) have been proposed for algebraic structure and key recovery in generalized Reed-Solomon based McEliece scheme. The filtration attack was recently used by Couvreur et al [6] to attack Bernstein et al's wild Goppa codes based McEliece scheme [3].

General Goppa codes based McEliece schemes are still immune from these attacks. However, based on the new development of cryptanalysis techniques against linear code based cryptographic systems in recent years, it is important to systematically design general random linear code based cryptographic systems defeating these attacks. With this motivation, this paper presents a systematic approach of designing public key encryption schemes using any linear codes. For example, we can even use Reed-Solomon codes in our scheme which is impossible for McEliece's schemes. Since our design of linear codes based encryption schemes embeds randomness in each column of the generator matrix, it is expected that, without the corresponding private key, these codes are as hard as random linear codes for decoding. We run several experiments on our codes with different underlying linear codes such as Reed-Solomon codes, the experiments show that the product code of our codes have the square dimension of the underlying codes. This gives the further evidence that our codes behaves more like random codes.

It should be noted that the most powerful attacks on Goppa code based McEliece cryptosystem is the information-set decoding attack which was introduced by Prange [19]. In an information-set decoding approach, one finds a set of coordinates of a received ciphertext which are error-free and that the restriction of the code's generator matrix to these positions is invertible. The original message can then be computed by multiplying the ciphertext with the inverse of the submatrix. Improvements of the origianl information-set decoding attack have been designed by Lee and Brickell [9], Leon [10], and Stern [22]. Bernstein, Lange, and Peters [4] presented an exact complexity analysis on information-set decoding attack against McEliece cryptosystems. It should be noted all these attacks are against binary linear codes. Thus they are not applicable to when the underlying field is $GF(p^m)$ for a prime p. In our RLCE scheme, we recommend the use of either $GF(2^m)$ or $GF(p^m)$. Peters [18] presented an exact complexity analysis on information-set decoding attack against McEliece cryptosystems over $GF(p)$. These analysis could be used for the parameter selection for our RLCE scheme also. For example, it is showed in Peters [18] that $n = 961$, $k = 771$ and $w = 48$ is sufficient to achieve 128-bit security when the underlying field is $GF(31)$.

Unless specified otherwise, we will use $q = 2^m$ or $q = p^m$ for a prime p and our discussion are based on the field $GF(q)$ through out this paper. Bold face letters such as $\mathbf{a}, \mathbf{b}, \mathbf{e}, \mathbf{f}, \mathbf{g}$ are used to denote row or column vectors over $GF(q)$. It should be clear from the context whether a specific bold face letter represents a row vector or a column vector.

II. Goppa codes and McEliece Public Key Encryption scheme

In this section, we briefly review Goppa codes and McEliece's scheme. Let $n \leq q$. For a given polynomial $g(x)$ of degree t over $GF(q)$. Assume that $g(x)$ has no multiple zero roots and $\alpha_0, \cdots, \alpha_{n-1} \in GF(q)$ be different non root elements for $g(x)$. Then the following subspace $\mathcal{C}_{Goppa}(g)$ defines the code words of an $[n, d]$ binary Goppa code where $d \geq 2t + 1$. This binary Goppa code $\mathcal{C}_{Goppa}(g)$ can have dimension $k \geq n - tm$ and correct t errors.

$$\mathcal{C}_{Goppa}(g) = \left\{ c \in \{0,1\}^n : \sum_{i=0}^{n-1} \frac{c_i}{x - \alpha_i} \equiv 0 \bmod g(x) \right\}.$$

Furthermore, if $g(x)$ is irreducible, then $\mathcal{C}_{Goppa}(g)$ is called an irreducible Goppa code. The parity check matrix H for the Goppa codes looks as follows:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_0^1 & \alpha_1^1 & \cdots & \alpha_{n-1}^1 \\ \cdots & \cdots & \ddots & \cdots \\ \alpha_0^t & \alpha_t^1 & \cdots & \alpha_{n-1}^t \end{pmatrix} \begin{pmatrix} \frac{1}{g(\alpha_0)} & & \\ & \ddots & \\ & & \frac{1}{g(\alpha_{n-1})} \end{pmatrix} \tag{1}$$

The original McEliece scheme [14] is described as follows. For the parameter n, t, choose a Goppa code based on an irreducible polynomial $g(x)$ of degree t. Let G be the $k \times n$ generator matrix for a Goppa code. Choose a random dense $k \times k$ nonsingular matrix S, and a random $n \times n$ permutation matrix P. Then the public key is $G' = SGP$. G' will generate a linear code with the same rate and minimum distance as the code generated by G.

Encryption. For a k-bit message block $\mathbf{m}$, choose a random row vector $\mathbf{z}$ of length n and weight t. Compute the cipher text $\mathbf{x} = \mathbf{m}G' + \mathbf{z}$

Decryption. For a received ciphertext $\mathbf{x}$, compute $\mathbf{x}' = \mathbf{x}P^{-1}$. Using an error-correction algorithm, one can then compute $\mathbf{m}' = \mathbf{m}S$. Finally, $\mathbf{m}$ is computed by $\mathbf{m} = \mathbf{m}'S^{-1}$.

III. Random linear code based secure encryption schemes RLCE

In this section, we present our design of Random Linear Code based Encryption schemes RLCE. Let $n, k, d, t > 0$, and $r \geq 1$ be given parameters such that $n - k + 1 \geq d \geq 2t + 1$. Let $G = [\mathbf{g}_0, \cdots, \mathbf{g}_{n-1}]$ be a $k \times n$ generator matrix for an $[n, k, d]$ linear code. Assume that there is an efficient decoding algorithm to correct at least t errors for this linear code given by G. The private and public keys are generated using the following steps.

1) Let $C_0, C_1, \cdots, C_{n-1} \in GF(q)^{k\times r}$ be $k \times r$ matrices drawn uniformly at random and let
$$G_1 = [\mathbf{g}_0, C_0, \mathbf{g}_1, C_1 \cdots, \mathbf{g}_{n-1}, C_{n-1}] \tag{2}$$
be the $k \times n(r + 1)$ matrix obtained by inserting the random matrices C_i into G.
2) Let $A_0, \cdots, A_{n-1} \in GF(q)^{(r+1)\times(r+1)}$ be dense nonsingular $(r + 1) \times (r + 1)$ matrices chosen uniformly at random and let
$$A = \begin{pmatrix} A_0 & & & \\ & A_1 & & \\ & & \ddots & \\ & & & A_{n-1} \end{pmatrix} \tag{3}$$
be an $n(r + 1) \times n(r + 1)$ nonsingular matrix.
3) Let S be a random dense $k \times k$ nonsingular matrix and P be an $n(r + 1) \times n(r + 1)$ permutation matrix.
4) The public key is the $k \times n(r + 1)$ matrix $G' = SG_1AP$ and the private key is S, G_1, A, P.

Encryption. For a row vector message block $\mathbf{m} \in GF(q)^k$, choose a random row vector $\mathbf{e} \in GF(q)^{n(r+1)}$ such that the Hamming weight of $\mathbf{e}$ is at most t. The cipher text is $\mathbf{x} = \mathbf{m}G' + \mathbf{e}$.

Decryption. For a received cipher text $\mathbf{x}$, compute

$$\mathbf{x}P^{-1}A^{-1} = [y_0, \cdots, y_{n(r+1)-1}] = \mathbf{m}SG_1 + \mathbf{e}P^{-1}A^{-1}$$

where

$$A^{-1} = \begin{pmatrix} A_0^{-1} & & & \\ & A_1^{-1} & & \\ & & \ddots & \\ & & & A_{n-1}^{-1} \end{pmatrix} \tag{4}$$

Let $\mathbf{y} = [y_0, y_{r+1}, \cdots, y_{(n-1)(r+1)}]$ be the row vector of length n selected from the length $n(r + 1)$ row vector $\mathbf{x}P^{-1}A^{-1}$. Then it is straightforward to check that $\mathbf{y} = \mathbf{m}SG + \mathbf{e}'$ where the Hamming weight of $\mathbf{e}' \in GF(q)^n$ is at most t. Using the efficient decoding algorithm, one can compute $\mathbf{m}' = \mathbf{m}S$. Finally, $\mathbf{m}$ is computed by $\mathbf{m} = \mathbf{m}'S^{-1}$.

IV. Robustness of RLCE codes against existing attacks

A. Randomness of generator matrix columns

We first use the following theorem to show that each column of the underlying generator matrix could be completely randomized in a RLCE public key.

Theorem 4.1: Let $\mathbf{g} \in GF(q)^k$ be a given non-zero column vector. For any randomly chosen $k \times (r + 1)$ matrix $R \in GF(q)^{k\times(r+1)}$, there exist a $k \times k$ nonsingular matrix S, a $(r + 1) \times (r + 1)$ matrix A, and a $k \times r$ matrix $C \in GF(q)^{k\times r}$ such that

$$R = S[\mathbf{g}, C]A \tag{5}$$

Proof. The theorem could be proved using the fundamental properties of matrix equivalence and the details are omitted here. □

Though Theorem 4.1 shows that each column of the public key G' is completely randomized. It says nothing about the correlations among entire columns of G'. In the following, we show that G' shares the properties of common random linear codes. Thus the security of the RLCE scheme is believed to be equivalent to decoding a random linear code which is **NP**-hard.

B. Niederreiter's scheme and Sidelnikov and Shestakov's attack

Sidelnikov and Shestakov's cryptanalysis techniques [21] was originally used to analyze Niederreiter's scheme which is based on generalized Reed-Solomon codes. Let $\alpha = (\alpha_0, \cdots, \alpha_{n-1})$ be n distinct elements of $GF(q)$ and let $v = (v_0, \cdots, v_{n-1})$ be nonzero (not necessarily distinct) elements of of $GF(q)$. Then the generalized Reed-Solomon (GRS) code of dimension k, denoted by $GRS_k(\alpha, v)$, is defined by the following subspace.

$$\{(v_0 f(\alpha_0), \cdots, v_{n-1} f(\alpha_{n-1})) : f(x) \in GF(q)[x]_k)\}$$

where $GF(q)[x]_k$ is the set of polynomials in $GF(q)[x]$ of degree less than k. Alternatively, we can interpret $GF(q)[x]_k$ as a vector space of dimension k over $GF(q)$. For each code word $c = (v_0 f(\alpha_0), \cdots, v_{n-1} f(\alpha_{n-1}))$, $f(x) = f_0 + f_1 x + \cdots + f_{k-1} x^{k-1}$ is called the associate polynomial of the code word c that encodes the message $(f_0, \cdots, f_{k-1})$. $GRS_k(\alpha, v)$ is an $[n, k, d]$ MDS code where $d = n - k + 1$. Niederreiter's scheme [17] replaces the binary Goppa codes in McEliece scheme using GRS codes as follows. With security parameters n, k, one first chooses a GRS code parameters α and v. Let G be the $k \times n$ generator matrix for this GRS code. Choose a random $k \times k$ nonsingular matrix S over $GF(q)$. Then the public key is $G' = SG$ and $t = \lfloor \frac{n-k}{2} \rfloor$. G' generates a linear code with the same rate and minimum distance as the code generated by G. The encryption and decryption process are the same as in the original McEliece scheme.

The best attack on Niederreiter scheme is presented by Sidelnikov and Shestakov [21]. In Sidelnikov-Shestakov attack, one can recover a private key (α, v) from a public key G' for the code $GRS_k(\alpha, v)$. It should be noted that the recovered key may be different from the original private key, but they are equivalent. For the given public key G', one first computes the systematic form $E(G') = [I|G'']$ (also called echelon form) using Gaussian elimination.

$$E(G') = \begin{pmatrix} 1 & 0 & \cdots & 0 & b_{0,k} & \cdots & b_{0,n-1} \\ 0 & 1 & \cdots & 0 & b_{1,k} & \cdots & b_{1,n-1} \\ & & \ddots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & b_{k-1,k} & \cdots & b_{k-1,n-1} \end{pmatrix} \tag{6}$$

For the ith row $\mathbf{b}_i$ of $E(G')$, assume the associated polynomial is f_{b_i}. Since the only non-zero elements are $b_{i,i}, b_{i,k+1}, \cdots, b_{i,n-1}$, we have

$$\begin{aligned} & v_0 f_{b_i}(\alpha_0) = 0 \\ & \cdots \\ & v_i f_{b_i}(\alpha_i) = 1 \\ & \cdots \\ & v_{n-1} f_{b_i}(\alpha_{n-1}) = b_{i,n-1} \end{aligned} \tag{7}$$

Thus f_{b_i} can be written as

$$f_{b_i} = c_{b_i} \cdot \prod_{j=1, j \neq i}^{k} (y - \alpha_j) \tag{8}$$

for some $c_{b_i} \neq 0$. By the fact that

$$GRS_k(\alpha, v) = GRS_k(a\alpha + b, cv) \tag{9}$$

for all $a, b, c \in GF(q)$ with $ab \neq 0$ (see [12]), we may assume that $\alpha_0 = 0$ and $\alpha_1 = 1$. In the following, we try to recover $\alpha_2, \cdots, \alpha_{n-1}$. Using equation (8), one can divide the row entries in (6) by the corresponding nonzero entries in another row to get several equations. For example, if we divide entries in row i_0 by corresponding nonzero entries in row i_1, we get

$$\frac{b_{i_0,j}}{b_{i_1,j}} = \frac{v_j f_{b_{i_0}}(\alpha_j)}{v_j f_{b_{i_1}}(\alpha_j)} = \frac{c_{b_{i_0}}(\alpha_j - \alpha_{i_1})}{c_{b_{i_1}}(\alpha_j - \alpha_{i_0})} \tag{10}$$

for $j = k, \cdots, n-1$. First, by taking $i_0 = 0$ and $i_1 = 1$, equation (10) could be used to recover $\alpha_k, \cdots, \alpha_{n-1}$ by guessing the value of $\frac{c_{b_0}}{c_{b_1}}$ which is possible when q is small. By letting $i_0 = 0$ and $i_1 = 2, \cdots, k-1$ respectively, equation (10) could be used to recover α_{i_1}. Sidelnikov and Shestakov [21] also showed that the values of v can then be recovered by solving some linear equation systems based on $\alpha_0, \cdots, \alpha_{n-1}$.

Wieschebrink [23] revised Niederreiter's scheme by inserting some random column vectors into random positions of G before obtaining the public key G'. Couvreur et al [5] showed that Wieschebrink's revised scheme is not secure under the product code attacks.

Berger and Loidreau [2] recommend using sub codes of Niederreiter's scheme to avoid Sidelnikov and Shestakov's attack. Specifically, in Berger and Loidreau's scheme, one uses a random $(k-l) \times k$ matrix S' of rank $k-l$ instead of the $k \times k$ matrix S to compute the public key $G' = S'G$.

For smaller values of l, Wieschebrink [24] shows that a private key (α, v) for Berger and Loidreau scheme [2] could be recovered using Sidelnikov-Shestakov algorithm. For larger values of l, Wieschebrink used product code to recover the secret values for Berger-Loidreau scheme.

Let $G' = S \cdot G$ be the $(k-l) \times n$ public generator matrix for Berger-Loidreau scheme, $\mathbf{r}_0, \cdots, \mathbf{r}_{k-l-1}$ be the rows of G', and $f_0, \cdots, f_{k-l-1}$ be the associated polynomials to those rows. For two row vector $a, b \in GF(q)^n$, the component wise product $\mathbf{a} * \mathbf{b} \in GF(q)^n$ is defined as

$$\mathbf{a} * \mathbf{b} = (a_0 b_0, \cdots, a_{n-1} b_{n-1}) \tag{11}$$

By the definition in (11), it is straightforward to observe that

$$\mathbf{r}_i * \mathbf{r}_j = (v_0^2 f_i(\alpha_0) f_j(\alpha_0), \cdots, v_{n-1}^2 f_i(\alpha_{n-1}) f_j(\alpha_{n-1})) \tag{12}$$

For $2k - 1 \leq n - 2$, if the code generated by $\mathbf{r}_i * \mathbf{r}_j$ equals to $GRS_{2k-1}(\alpha, \mathbf{v}')$ for $\mathbf{v}' = (v_0^2, \cdots, v_{n-1}^2)$, then the Sidelnikov-Shestakov algorithm could be used to recover the values α and v. For $2k - 1 \leq n - 2$, if the code generated by $\mathbf{r}_i * \mathbf{r}_j$ does not equal to $GRS_{2k-1}(n, \mathbf{v}')$, then the attack fails. Wieschebrink shows that the probability that the attack fails is very small. For the case of $2k - 1 > n - 2$, Wieschebrink applied Sidelnikov-Shestakov algorithm on the component wise product code of a shortened code of the original $GRS_k(\alpha, \mathbf{v})$.

From the description of the above Sidelnikov and Shestakov attack, it is straightforward to observe that Sidelnikov and Shestakov attack does not apply to our RLCE schemes.

C. Filtration attacks

Using distinguisher techniques [7], Couvreur et al. [5] designed a filtration technique to attack McEliece scheme based on GRS codes. The filtration technique was further developed by Couvreur et al [6] to attack wild Goppa codes based McEliece scheme. In the following, we briefly review the filtration attack in [6]. 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 $a * b$ for all pairs $(a, b) \in \mathcal{C}_1 \times \mathcal{C}_2$ where $a * b$ is defined in (11). For $\mathcal{C}_1 = \mathcal{C}_2$, $\mathcal{C}_1 * \mathcal{C}_1$ is called the square code of $\mathcal{C}_1$.

Couvreur et al [6] showed that the square code of an alternant code of extension degree 2 may have an unusually low dimension when its dimension is larger than its designed rate. Specifically, this happens for wild Goppa codes. Using a shortening trick, Couvreur et al showed that the square of a shortened wild Goppa code of extension degree 2 is contained in an alternant code of non trivial dimension. Based on those observations, Couvreur et al designed the code filtration techniques. Specifically, create a family of nested codes defined for any $a \in \{0, \cdots, n-1\}$ as follows.

$$\mathcal{C}^a(0) \supseteq \mathcal{C}^a(1) \supseteq \cdots \supseteq \mathcal{C}^a(q+1) \tag{13}$$

This family of nested codes is called a filtration. Roughly speaking, $\mathcal{C}^a(j)$ consists in the codewords of $\mathcal{C}$ which correspond to polynomials which have a zero of order j at position a. It is shown that the first two elements of this filtration are just punctured and shortened versions of $\mathcal{C}$ and the rest of them can be computed from $\mathcal{C}$ by computing star products and solving linear systems. Furthermore, the support values $\alpha_0, \cdots, \alpha_{n-1}$ for the Goppa code could be recovered by this nested family of codes efficiently. Thus the private keys for wild Goppa codes based McEliece scheme could be recovered from the public keys.

The crucial part of the filtration techniques is the efficient algorithm to compute the nested family of codes in (13). For our RLCE scheme, the public generator matrix G' contains random columns. Thus linear equations constructed in Couvreur et al [6] could not be solved and the nested family (13) could not be computed correctly.

Furthermore, the important characteristics for a code $\mathcal{C}$ to be vulnerable is that one can find a related code $\mathcal{C}_1$ of dimension k such that the dimension of the square code of $\mathcal{C}_1$ has dimension less than k^2. We have implemented our RLCE scheme using common linear codes such as Reed-Solomon codes. We tried to construct related codes $\mathcal{C}_1$ using commonly used cryptanalysis techniques. Our experiments show that for all these codes $\mathcal{C}_1$ of dimension k, the square code of $\mathcal{C}_1$ has dimension k^2.

V. Practical considerations

Though we have introduced the RLCE scheme with the parameter r, it is sufficient to take $r = 1$ in practice. That is, for each column of the generator matrix, a random column is inserted after that column in the generator matrix. For commonly used McEliece-based crypto-systems parameters (see, e.g., Niebuhr et al [16]) with 128-bit security, we have $n \sim 2800$, $k \sim 2000$, and $t \sim 60$. These parameters are sufficient to guarantee 128-bit security for our RLCE encryption schemes with $r = 1$. In other words, For 128-bit security, we may choose $[n, k, t] = [2800, 2000, 60]$ to achieve 128 bit security. For this parameter, the approximate public key size is 360KB.

VI. Conclusions

In this paper, we presented techniques for designing general random linear code based public encryption schemes using any linear codes. We then showed that our schemes are secure against exisitng attacks on linear codes based encryption schemes. In addition to being a post-quantum cryptographic technique, our scheme RLCE has recently been used by Wang and Desmedt to design fully homomorphic encryption schemes.

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] T Berger and P Loidreau. How to mask the structure of codes for a cryptographic use. *Designs, Codes and Cryptography*, 35(1):63–79, 2005.

[3] D. Bernstein, T. Lange, and C. Peters. Wild mceliece. In *Selected Areas in Cryptography*, pages 143–158. Springer, 2011.

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

[5] A. Couvreur, P. Gaborit, V. Gauthier-Umaña, A. Otmani, and J. Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes. *Designs, Codes and Cryptography*, pages 1–26, 2013.

[6] A Couvreur, A Otmani, and J Tillich. Polynomial time attack on wild McEliece over quadratic extensions. In *EUROCRYPT 2014*, pages 17–39. Springer, 2014.

[7] J-C Faugere, V. Gauthier-Umana, A. Otmani, L. Perret, and J. Tillich. A distinguisher for high rate mceliece cryptosystems. In *Information Theory Workshop (ITW), 2011 IEEE*, pages 282–286. IEEE, 2011.

[8] H. Janwa and O. Moreno. Mceliece public key cryptosystems using algebraic-geometric codes. *Designs, Codes and Cryptography*, 8(3):293–307, 1996.

[9] Pil Joong Lee and Ernest F Brickell. An observation on the security of mcelieceâĂŹs public-key cryptosystem. In *Advances in CryptologyâĂŤEUROCRYPTâĂŹ88*, pages 275–280. Springer, 1988.

[10] Jeffrey Leon. A probabilistic algorithm for computing minimum weights of large error-correcting codes. *Information Theory, IEEE Transactions on*, 34(5):1354–1359, 1988.

[11] C. Löndahl and T. Johansson. A new version of mceliece pkc based on convolutional codes. In *Information and Communications Security*, pages 461–470. Springer, 2012.

[12] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. NH Pub. Company, 1978.

[13] I. Márquez-Corbella and R. Pellikaan. Error-correcting pairs for a public-key cryptosystem. *arXiv preprint arXiv:1205.3647*, 2012.

[14] R.J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN progress report*, 42(44):114–116, 1978.

[15] R. Misoczki, J. Tillich, N. Sendrier, and P. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In *Proc. ISIT*, pages 2069–2073. IEEE, 2013.

[16] R Niebuhr, M Meziani, S Bulygin, and J Buchmann. Selecting parameters for secure McEliece-based cryptosystems. *Int. J. Information Security*, 11(3):137–147, 2012.

[17] H Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Informaiton Theory*, 15(2):159–166, 1986.

[18] Christiane Peters. Information-set decoding for linear codes over f q. In *Post-Quantum Cryptography*, pages 81–94. Springer, 2010.

[19] Eugene Prange. The use of information sets in decoding cyclic codes. *Information Theory, IRE Transactions on*, 8(5):5–9, 1962.

[20] V Sidelnikov. A public-key cryptosystem based on binary Reed-Muller codes. *Discrete Mathematics and Applications*, 4(3):191–208, 1994.

[21] V. M Sidelnikov and S. Shestakov. On insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Mathematics and Applications*, 2(4):439–444, 1992.

[22] Jacques Stern. A method for finding codewords of small weight. In *Coding theory and applications*, pages 106–113. Springer, 1989.

[23] C. Wieschebrink. Two NP-complete problems in coding theory with an applica- tion in code based cryptography. In *Proc. IEEE ISIT*, pages 1733–1737. IEEE Press, 2006.
[24] C. Wieschebrink. Cryptanalysis of the niederreiter public key scheme based on GRS subcodes. In *Post-Quantum Cryptography*, pages 61–72. Springer, 2010.