Some public-key cryptosystems over finite fields

SELDA CALKAVUR
Math Dept, Kocaeli University, Kocaeli, TURKEY

Abstract—In this paper, we present two public-key cryptosystems over finite fields. First of them is based on polynomials. The presented system also considers a digital signature algorithm. Its security is based on the difficulty of finding discrete logarithms over GF(q^{d+1}) with sufficiently large q and d. Is is also examined along with comparison with other polynomial based public-key systems. The other public-key cryptosystem is based on linear codes. McEliece studied the first code-based public-key cryptosystem. We are inspired by McEliece system in the construction of the new system. We examine its security using linear algebra and compare it with the other code-based cryptosystems. Our new cryptosystems are too reliable in terms of security.

Keywords: Polynomials over finite fields, public-key cryptography, digital signature, linear codes

Received: April 17, 2021. Revised: February 28, 2022. Accepted: March 30, 2022. Published: April 26, 2022.

1. Introduction

Public-key cryptography was introduced [10] in 1976 and then many public-key cryptosystems have been proposed. One of the most important is RSA cryptosystem [39] which was presented by Rivest, Shamir and Adleman. The other good studies are ElGamal cryptosystem [12] and DSS [35]. These systems [12], [35] are based on the difficulty of solving of discrete logarithm problem defined over the finite fields. It is used the linear feedback shift-register (LFSR) sequences in the RSA encryption [39] and the Diffie-Hellman public-key exchange scheme [10]. The first-order LFSR sequence over $GF(p)$ or $\mathbb{Z}_n$, where n is a product of two prime numbers, is the ElGamal digital signature scheme. Dickson polynomial scheme [28], [37] or LUC [46], [47] are similar to RSA, Diffie Hellman and ElGamal public-key cryptosystems, respectively. The second-order LFSR sequence over $GF(p)$ with a special initial state is the mathematical function used in this family of the public-key cryptosystems. This is coset constant [16].

Shor [42] wrote a quantum algorithm to solve the abelian hidden subgroup problem. Some quantum-safe public-key cryptosystems have been proposed recently [40], [19], [11].

The theory of polynomials over finite fields is important investigating the cryptography for many applications. Çalkavur et al. [5] presented a new secret sharing scheme based on polynomials over finite fields.

Code-based cryptography was first suggested by McEliece [30] using binary Goppa codes in 1978. This system has the efficient encryption and decryption algorithms. The security of the McEliece cryptosystem is related to decoding a random linear code in some metric. Many new cryptosystems have been presented using different codes replacing Goppa codes [3], [4], [7], [21], [29], [33], [34], [36], [43], but most of them are broken by using the algebraic structures of the codes [2], [6], [8], [13], [26], [32], [41], [44], [49].

Gabidulin et al. [14] proposed a kind of McEliece cryptosystem based on Gabidulin codes. They are a family of rank metric-codes. Overbeck [38] broke the Gabudulin's cryptosystem. Next, Gaborit et al. [15] developed a new family of rank-metric codes is called Low Rank Parity Check (LRPC) codes. LRPC code-based cryptosystem is a reliable system.

In this work, we first construct a new-public-key cryptosystem as well as digital signature generation and verification operations. Our cryptosystem, whose security is based on discrete logarithm problem, is based on polynomials over finite fields. Its security improves on that of public-key cryptosystems. Then we introduce another public-key cryptosystem based on linear codes by combining McEliece cryptosystem. We give the encryption and decryption algorithms by using coding theory and linear algebra. We analyse its effectiveness by means of security and result by the comparison between our cryptosystem and the three other code-based public-key cryptosystems in the literature: McEliece's system [30], Krouk et al. [25] and Kim et al. [23] system.

The material is organized as follows. Section II reminds the necessary background in cryptography, finite fields and coding theory. Section III describes the new cryptosystems and explains their security. Section IV considers the comparison with the other systems. Section V concludes the paper.

2. Preliminaries

We begin with the necessary informations to explain our systems.

2.1 Public-Key Cryptosystems

A public-key cryptosystem or asymmetric cryptosystem is one in which messages encrypted with one key only be decrypted with a second key, and vice versa. That is the system has two different keys, public-key and private key. The public-key can be known by everyone, since it cannot decryption, only can encryption, but the private key must be known only by user. These keys are not completely independent of each other. There must be a mathematical relationship between them. Thus the public-key cryptosystems are built on mathematical functions. A strong public-key cryptosystem which possession of both the algorithm and the one key gives no useful information about the other key. So no clues as to how to decrypt the message.

The public-key cryptosystems can also be used to achieve user authentication and non-repudiation aspects of information security. A message encrypted using a private key can be decrypted using the corresponding public-key. Since the public-key may be known by everyone, this would not provide confidentiality, but, as the private key is only known to the sender, it authenticates the sender, and the sender cannot deny that he or she send the message. This means the security of a public-key cryptosystem depends on the security of the private key.

Public-key algorithms are main security principles in modern cryptosystems. Asymmetric encryption is slower than good symmetric encryption. Both symmetric and asymmetric encryption systems are used today.

2.2 Digital Signature Algorithm

Digital signatures consist of a public/private key pairs. So they use a public-key cryptosystem. A message is signed by a private key and the signature is verified by the corresponding public-key. The digital signature provides message authentication (the receiver can verify that the message has not been modified since it was signed) and non-repudiation (the sender cannot falsely claim that they have not signed the message).

2.3 Polynomials over Finite Fields

The theory of polynomials over finite fields is important for investigating many applications. These polynomials are used in cryptographic protocols.

Definition 1. ([27]) Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a non-zero polynomial of degree n over an arbitrary field $GF(q)$, q being a prime. Then a_n is said to be the leading coefficient of $f(x)$ and a_0 is the constant term.

Definition 2. ([27]) A polynomial $f \in GF(q)[x]$ is said to be irreducible over $GF(q)$ if f has positive degree and $f = bc$ with $b, c \in GF(q)[x]$ implies that either b or c is a constant polynomial.

2.4 Linear Codes

Definition 1. ([18]) Let q be a prime power. $\mathbb{F}_q$ being denote the finite field of order q, an $[n, k]$- linear code C over $\mathbb{F}_q$ is a subspace of $(\mathbb{F}_q)^n$ where n is length of the code C and k is dimension of C.

Definition 2. ([18]) The dual code of C is the set of those vectors $(\mathbb{F}_q)^n$ which are orthogonal to every codeword of C. It is denoted by $C^{\perp}$. $C^{\perp}$ is an $[n, n-k]$- linear code.

Definition 3. ([18]) A $k \times n$ matrix G is the generator matrix for a linear code C. The rows of G consist of a basis of C. Note that an $[n, k]$- code C over $\mathbb{F}_q$ has q^k codewords.

3. The System

In this section, we present our new public-key cryptosystems over finite fields.

3.1 First System

We consider the polynomials belong to the field F of q^{d+1} elements, d being an arbitrary positive integer. We should define F. Consider an irreducible polynomial $Q(x) \in GF(q)[x]$ of degree $d+1$ and set $F = GF(q)[x]/(Q(x))$. The system will be based on $GF(q^{d+1})$, the non-zero polynomials of degree d over $GF(q)$.

3.2 Key-Generation Procedure

An user Alice follows the below steps to generate her public and private key.

1) Selects any random polynomial $p(x) \in GF(q)[x]$ of degree d.

2) Gets an irreducible polynomial $Q(x) \in GF(q)[x]$ of degree $d+1$.

3) By using Euclid algorithm, calculates the polynomials $f(x) \in GF(q)[x]$ satisfying $p(x)f(x) \equiv 1$ (mod $Q(x)$).

4) The public-key is $(p(x), Q(x))$ and private key is $f(x)$.

3.3 Encryption Algorithm

If Bob wants to send a message $m(x)$ to Alice, then he should do the following.

I-) Gets the Alice's public-key $(p(x), Q(x))$.

II-) Considers the message $m(x)$ such that $m(x) \in GF(q)[x]$ of degree d.

III-) Calculates the ciphertext as $c(x) \equiv m(x)p(x)$ (mod $Q(x)$).

IV-) Sends the ciphertext $c(x) \in GF(q)[x]$ to Alice.

3.4 Decryption Algorithm

Alice should do the following to find the plaintext $m(x)$ from the ciphertext $c(x)$.

i) Uses the private key $f(x) \in GF(q)[x]$.

ii) Calculates the plaintext $m(x) \equiv c(x)f(x)$ (mod $Q(x)$).

Proposition 1. *The size of the plaintext is* $log_q^{(q^{d+1}-1})$.

Proof. The plaintext is selected from the non-zero polynomials of degree d over $GF(q)$ and the number of these polynomials is $q^{d+1}-1$. So the plaintext can be written using $d+1$ elements of $\mathbb{F}_q$.

□

3.5 Examination of the Public-Key Encryption Algorithm

A public polynomial $p(x) \in GF(q)[x]$ of degree d is used encryption algorithm. The private polynomial $f(x) \in GF(q)[x]$ of degree $\leq d$ is satisfied the equation

$$p(x)f(x) \equiv 1(modQ(x)) \qquad (1)$$

Since the other public polynomial $Q(x) \in GF(q)[x]$ of degree $d+1$ is an irreducible polynomial, Equation (1) has always a solution over $GF(q^{d+1})$.

Now we examine this equaiton in detail.

$$p(x)f(x) \equiv 1(modQ(x)) \Rightarrow f(x) \equiv (p(x))^{-1}(modQ(x))$$

$$\Rightarrow (p(x))^{-1} \equiv f(x)(modQ(x))$$

$$\Rightarrow p(x) \equiv (f(x))^{-1}(modQ(x))$$

$$\Rightarrow (f(x))^{-1} \equiv p(x)(mod(Q(x))$$

The ciphertext $c(x)$ is calculated as follows.

$$c(x) \equiv m(x)p(x)(modQ(x))$$

$$m(x) \equiv c(x)f(x)(modQ(x)) \Rightarrow f^{-1}(x)m(x) \equiv c(x)(modQ(x))$$

$$\Rightarrow m(x) \equiv m(x)p(x)(p(x))^{-1}(modQ(x))$$

$$m(x) \equiv m(x)(modQ(x))$$

Example 1. Suppose that $q = 2, d = 2, Q(x) = x^3+x+1$ and $F = GF(2)[x]/(Q(x))$. Alice selects any random polynomial $p(x) = x^2+1 \in GF(2)[x]$. Then she calculates the polynomial $f(x) \in GF(2)[x]$ satisfying

$$p(x)f(x) \equiv 1(mod(Q(x)).$$

$$(x^2 + 1)f(x) \equiv 1(modx^3 + x + 1)$$

Since $x^3 + x + 1 = x(x^2 + 1) + 1 \Rightarrow x^3 + x + 1 - x(x^2 + 1) = 1$, $f(x)$ will be $x \in GF(2)[x]$. So her public-key is $(x^2 + 1, x^3 + x + 1)$ and private key is x.

Encryption. Bob gets Alice's public-key to encrypt the message $m(x) = x^2 + x + 1 \in GF(2)[x]$ and calculates the ciphertext $c(x) \in GF(2)[x]$ as $c(x) \equiv m(x)p(x)$ (mod $Q(x)$). That is $c(x) \equiv (x^2+x+1)(x^2+1)$ (mod x^3+x+1) $\equiv x^2+x$ (mod $x^3 + x + 1$). Then he sends the ciphertext $c(x)$ to Alice.

Decryption. Alice calculates the plaintext $m(x) \in GF(2)[x]$ by her own private key as follows.
$m(x) \equiv c(x)f(x)$ (mod $Q(x)$)
$m(x) \equiv (x^2 + x)x$ (mod $x^3 + x + 1$)
$m(x) \equiv x^2 + x + 1$ (mod $x^3 + x + 1$)

Example 2. Suppose that $q = 3, d = 3, Q(x) = x^4 + 2x^3 + 2$ and $F = GF(3)[x]/(Q(x))$. Alice selects any random polynomial $p(x) = x^3 + 2x^2 \in GF(3)[x]$ and calculates the polynomial $f(x) \in GF(2)[x]$ satisfying $p(x)f(x) \equiv 1$ (mod $Q(x)$).
$(x^3 + 2x^2)f(x) \equiv 1$ (mod $x^4 + 2x^3 + 2$)
Since $x^4 + 2x^3 + 2 = x(x^3 + 2x^2) + 2$
$1 \equiv x(x^3 + 2x^2)$ (mod $x^4 + 2x^3 + 2$),
the polynomial $f(x) = x \in GF(3)[x]$. So her public-key is $(x^3 + 2x^2, x^4 + 2x^3 + 2)$ and private key is x.

Encryption: Bob gets Alice's public-key to encrypt the plaintext $m(x) = x^3 + x^2 + 1 \in GF(3)[x]$ and calculates the ciphertext $c(c) \in GF(3)[x]$ as follows.
$c(x) \equiv (x^3 + x^2 + 1)(x^3 + x^2)$ (mod $x^4 + 2x^3 + 2$)
$c(x) \equiv x^3 + x$ (mod $x^4 + 2x^3 + 2$).
Then he sends the ciphertext $c(x)$ to Alice.

Decryption: Alice calculates the plaintext $m(x) \in GF(3)[x]$ by her own private key.
$m(x) \equiv c(x)f(x)$ (mod $Q(x)$)
$m(x) \equiv (x^3 + x)x$ (mod $x^4 + 2x^3 + 2$)
$m(x) = x^3 + x^2 + 1 \in GF(3)[x]$.

3.6 Security of the System

In this part, we analyze the security of the proposed system. It is very difficult to prove the security of a public-key cryptosystem in general [31], [48]. We will give some security arguments and evidence that our cryptosystem is secure.

The security of the new system is based on the difficulty of solving the discrete logarithm in $GF(q^{d+1})$. Since the publi-key $(p(x), Q(x))$ is known by everyone, an attacker also knows these values. If the attacker can solve the discrete logarithm problem $p(x)f(x) \equiv 1$ (mod $Q(x)$), then he/she can reach the private key $f(x)$. However, according to [1], [9], [20], [24], [45], solving the discrete logarithm in $GF(q^{d+1})$ is much harder than solving discrete logarithm in $GF(q)$ for the same q. Furthermore, it is benefical having the large q and d. In this case, the solution of the discrete logarithm will be much more difficult because of the number of plaintext will increase. So, if an enemy cryptanalyst cannot guess the plaintext. Also there is no mathematical relation between the plaintext and ciphertext. This means the system is too strong against attacks.

3.7 Digital Signatures

The polynomial based public-key cryptosystem can be used for the digital signatures.

1) Signature generation: If Alice wants to send the signed message $m(x)$ to Bob, then she applies to the message her own private key as follows.
$\sigma(x) = m(x)f(x)$ (mod $Q(x)$), it is clear that $\sigma(x) \in GF(q)[x]$. Then she sends the signed message $(m(x), \sigma(x))$ to Bob.

2) Signature verification: Bob calculates
$m(x) = \sigma(x)p(x)$ (mod $Q(x)$) to verify signature.

Example 3. (continued to Example 1)
Sign: Alice calculates $\sigma(x) \equiv m(x)f(x)$ (mod $Q(x)$) to sign the message $m(x) = (x^2 + x + 1) \in GF(2)[x]$.
$\sigma(x) = m(x)f(x)$ (mod $Q(x)$)
$\sigma(x) \equiv (x^2 + x + 1)x$ (mod $x^3 + x + 1$)
$\sigma(x) = x^2 + 1$
and she sends the signed message $(m, \sigma) = (x^2+x+1, x^2+1)$ to Bob.

Verify signature: Bob should do the following to verify signature.
$m(x) = \sigma(x)p(x)$ (mod $Q(x)$)
$m(x) = (x^2 + 1)(x^2 + 1)$ (mod $x^3 + x + 1$)
$m(x) = x^2 + x + 1$

Example 4. (continued to Example 2)
Sign: Alice calculates $\sigma(x) \equiv m(x)f(x)$ (mod $Q(x)$) to sign the message $m(x) = (x^3 + x^2 + 1) \in GF(3)[x]$.
$\sigma(x) = m(x)f(x)$ (mod $Q(x)$)
$\sigma(x) \equiv (x^3 + x^2 + 1)x$ (mod $x^4 + 2x^3 + 2$)
$\sigma(x) = 2x^3 + x + 1$
and she sends the signed message $(m, \sigma) = (x^3+x^2+1, 2x^3 + x + 1)$ to Bob.

Verify signature: Bob should do the following to verify the signature.
$m(x) = \sigma(x)p(x)$ (mod $Q(x)$)

$m(x) \equiv (2x^3 + x + 1)(x^3 + 2x^2) \pmod{x^4 + 2x^3 + 2}$
$m(x) = x^3 + x^2 + 1$

3.8 Second System

In this section, we present a new public-key cryptosystem based on linear codes by a different approach. Consider the following steps to construct the public and private key.

3.9 Key-Generation Procedure

The user named Alice does the following.
1) Selects an $[n, k]$- linear code C over $\mathbb{F}_q$ with $k \times n$ generator matrix G.
2) Selects random a non-singular $n \times n$ matrix M over $\mathbb{F}_q$.
3) Calculates the $k \times n$ matrix $G^{'} = GM$ and the invers matrix M^{-1}.
4) The public-key is $G^{'}$ and private key is (G, M, M^{-1}).

3.10 Encryption Algorithm

If the other user named Bob wants to send the message m of length k, then he should do the following, where m is non-zero element of $(\mathbb{F}_q)^k$.
I-) Gets the Alice's public-key $G^{'}$.
II-) Considers the message $m \in (\mathbb{F}_q)^k$.
III-) Calculates the ciphertext $c \in (\mathbb{F}_q)^n$ as $c = mG^{'}$.
IV-) Sends the ciphertext c to Alice.

3.11 Decryption Algorithm

Alice gets the ciphertext c and follows the below steps to decrypt the message.
i) Uses the private key (G, M, M^{-1}).
ii) Calculates $c^{'} = cM^{-1}$.
iii) Obtains m from $c^{'}$ by solving the linear system $c^{'} = cM^{-1}$ of rank k.

Decryption is correct since $c^{'} = cM^{-1} = mG^{'}M^{-1} = mGMM^{-1} = mG$.

Proposition 2. *Let C be an $[n, k]$- linear code over $\mathbb{F}_q$ with generator matrix G. The size of plaintext is $q^k - 1$ in the new system.*

Proof. The plaintext is any non-zero element of $(\mathbb{F}_q)^k$ and $(\mathbb{F}_q)^k$ has $q^k - 1$ non-zero elements. □

Proposition 3. *The number of ciphertext is q^n.*

Proof. The ciphertext is any element of $(\mathbb{F}_q)^n$. So the size of ciphertext is q^n. □

Example 5. Consider the $[4, 2]$- linear code over $\mathbb{F}_3$. The generator matrix G of C is

$$G = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

Select any random non-singular matrix is

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 2 & 2 & 0 & 1 \end{pmatrix}$$

over $\mathbb{F}_3$. The invers matrix is

$$M^{-1} = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix}.$$

In this case, the matrix $G^{'} = GM$ will be

$$G^{'} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix}$$

over $\mathbb{F}_3$. So Alice's public-key is

$$G^{'} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix}$$

and private key is $(G, M, M^{-1}) = \left(\begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 2 & 2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix}\right)$.

Encryption: Bob gets Alice's public-key to encrypt the plaintext $m = (12) \in (\mathbb{F}_3)^2$ and calculates the ciphertext $c \in (\mathbb{F}_3)^4$ as

$$c = mG^{'} = (12) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix} = (0202).$$

Then he sends the ciphertext $c = (0202)$ to Alice.
Decryption: Alice calculates the plaintext $m \in (\mathbb{F}_3)^2$ by her own private key as follows.

$$c^{'} = cM^{-1} = mG$$

$$(0202) \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix} = (m_1 m_2) \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

$$(1201) = (m_1, m_2, 2m_1 + 2m_2, 2m_1 + m_2).$$

It is obtained $m_1 = 1, m_2 = 2$ by solving the above linear system. So the plaintext will be $m = (m_1 m_2) = (12)$.

3.12 Security of the System

The security of the second system is based on the difficulty of solving the factorization problem of matrices in linear algebra. The mathematical relationship between the public-key and private key is very strong. This relationship is the factorization problem of matrices, the size of matrix being too big. That is the problem of finding matrices G and M. There is no easy way to solve this problem in mathematics. Thus it is benefical having the large q, n and k. More clearly, even if an attacker knows the public-key, it is not possible to find the private key, and knows the public-key and ciphertext, it is impossible practically. So our new code-based public-key cryptosystem is robust against attacks since the solution of the algebra problem on which it is based is unknown. The only way to crack the cipher is by trial and error, but is not possible practically.

Theorem 1. *Let C be an $[n, k]$- linear code over $\mathbb{F}_q$ with generator matrix G. If the code parameters are large enough, the system will be too reliable by means of security.*

Proof. If k and q are large enough, then the system can generate a large number of plaintext. In this case, it will be difficult to reach the plaintext for the attacker. Moreover, if k, q and n are large enough, it will be impossible to obtain the private key for the attacker. Because the solution of factorization problem of matrices is very hard. So the code parameters must be large enough to ensure the security of the system. □

4. Comparison with the Other Systems

Gong et al. [17] explored to construct the public-key cryptosystem by using third-order LFSR sequences over $GF(p)$. The security of their key distribution scheme is based on the dificulty of solving the discrete logartihm in $GF(p^3)$. The method presented there can lead to the construction of public-key cryptosystems by using nth- order characteristic sequences over $GF(p)$ of any degree $n > 3$.

Khachatrian and Kyureghyan [22] developed a new public-key encryption system based on permutation polynomials. Public-key encryption of the proposed system requires evaluation of the polynomial of weight t at any point of the field $GF(2^N)$ regarded as a polynomial of degree less than N with no modular reduction.

In our first framework, the polynomials over finite fields are considered to construct a public-key cryptosystem. The system is based on $GF(q^{d+1})$. So our cryptosystem is more comprehensive than the others based on finite fields. That is the working area is wider. This means the new system will be more preferred.

McEliece [30] introduced the public-key cryptosystem based on error-correcting codes. McEliece used binary Goppa codes, providing efficient encryption and decryption algorithms. The security of the McEliece cryptosystem depends on the difficulty of decoding a random linear code in some metric. Krouk and Ovchinnikov [25] developed the public-key cryptosystem based on bursts-correcting codes. They inspired by McEliece cryptosystem. The security of their system is also based on the hardness of decoding in the linear code. However, Krouk and Ovchinnikov's cryptosystem is safer than McEliece's. Kim et al. [23] suggested a new code-based public-key encryption scheme which is called McNie. They also inspired by McEliece and Niederreiter cryptosystems, but they showed that is not more difficult to crack McEliece than McNie. The security of McNie is based on the (Rank) Syndrome Decoding Problem.

In our second system, we propose another code-based public-key cryptosystem. This system is based on any linear code. Its security relies on the hardness of solving the factorization problem of matrices using the linear algebra. Our system is faster than the other code-based public-key cryptosystem by means of implementation. So it is safer than cryptosystems of this class.

5. Conclusion

In this work, we propose two new public-key cryptosystems over finite fields. We show how polynomials over finite field $GF(q^{d+1})$ can be used to construction efficient public-key cryptosystem and digital signature algorithm in the first part. The system is constructed by using polynomials over finite fields. Its security is ensured by difficulty solving the discrete logarithm problem. We compare our system with the other polynomial based public-key cryptosystems.

In the second part, we construct a new code-based public-key cryptosystem using linear codes. This system is inspired by McEliece cryptosystem. The security is based on linear algebra. More clearly, it depends on the difficulty of solving the factorization problem of matrices. The size of parameters of the linear code is considered in terms of security and efficiency. It is compared with the other code-based public-key cryptosystems. Our new cryptosystems stand well by means of security.

Acknowledgment. I would like to thank to Dr. Patrick Solé and Dr. Alexis Bonnecaze for their valuable comments which helped to improve their content of the paper.

Funding. This research received no external funding.

Conflicts of Interest. The author declares no conflict of interest.

References

[1] S. Al-Bassam, and B. Bose, On balanced codes, IEEE Trans. Inform. Theory, vol. 36, pp. 406-408, March 1990.

[2] M. Baldi and F. Chiaraluce, Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes, In Information Theory, 2007, ISIT 2007, IEEE International Symposium, pp. 2591-2595, 2007.

[3] M. Baldi, F. Chiaraluce, R. Garello, and F. Mininni, Quasi-cyclic low-density parity-check codes in the McEliece cryptosystem, In Communications, ICC'07, IEEE International Conference, pp. 951-956, June, 2007.

[4] T. Berger and P. Loidreau, How to mask the structure of codes for a cryptographic use, Designs, Codes and Cryptography, vol. 35, no. 1, pp. 63-79, 2005.

[5] S. Çalkavur, P. Solé A. Bonnecaze, A New Secret Sharing Scheme Based on Polynomials over Finite Fields, Mathematics. 8. 1200, doi:10.3390/math8081200, July 2020.

[6] I. V. Chizhov and M. A. Borodin, The failure of McEliece PKC based on Reed-Muller codes, IACR Cryptology ePrint Archive, p. 287, 2013.

[7] A. Conteaut and F. Chabaud, A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511, IEEE Transactions on Information Theory, vol. 44, no. 1, pp. 367-378, 1998.

[8] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan, A polynomial time attack against algebraic geometry code based public key cryptosystems, In Information Theory (ISIT), IEEE International Symposium, pp. 1446-1450, 2014.

[9] -, Design of efficient balanced codes, IEEE Trans. Comput., vol. 43, pp. 362-365, March 1994.

[10] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, vol. 22, pp. 644-654, 1976.

[11] L. Eldar and P. W. Shor, An efficientquantum algorithm for a variant of the closest lattice-vector problem, arXiv preprint, arXiv: 1611.06999, 2016.

[12] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory (31), pp.469-472, 1985.

[13] C. Faure and L. Minder, Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes, In Proceedings of the 11th international workshop on Algebraic and Combinatorial Coding Theory, ACCT, vol. 2008, pp. 99-107, June 2008.

[14] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, Ideals over a non-commutative ring and their application in cryptology, Workshop on the Theory and Application of Cryptographic Techniques, pp. 482-489, Springer, Berlin, Heidelberg, 1991.

[15] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor, Low rank parity check codes and their application to cryptography, The Proceedings of Workshop on Coding and Cryptography (WCC), pp. 168-180, Borgen, Norway, 2013.

[16] S. W. Golomb, Shift Register Sequences, Laguna Hills, CA: Aegean Park, 1982.

[17] G. Gong, L. Harn, Public-Key Cryptosystems Based on Cubic Finite Field Extensions, IEEE Transactions on Information Theory, vol. 45, no. 7, pp. 2601-2605, 1999.

[18] R. Hill, A First Course in Coding Theory, Oxford University, Oxford, 1986.

[19] J. Hoffstein, J. Pipher, and J. Silverman, NTRU: A ring-based public-key cryptosystem, Algorithmic number theory, pp. 267-288, 1998.

[20] K. A. S. Immink, Spectrum shaping with DC^2- constrained channel codes, Philips J. Res., vol. 40, pp. 40-53, 1985.

[21] H. Janwa and O. Moreno, McEliece public key cryptosystems using algebraic-geometric codes, Designs, Codes and Cryptography, 8(3), pp. 293-307, 1996.

[22] G. Khachatrian, M. Kyureghyan, Pemutation polynomials and a new public-key encryption, Discrete Applied Mathematics, vol. 216, pp. 622-626, 2017.

[23] J. L. Kim, Y. -S. Kim, L. Galvez, M. J. Kim, N.Lee, McNie: A new code-based public-key cryptosystem, arXiv: 1812.05008v2 [cs.CR], 27 Jan. 2019.

[24] D. E. Knuth, Efficient balanced codes, IEEE Trans. Inform. Theory, IT-32, pp. 51-53, January 1986.

[25] E. Krouk, A. Ovchinnikov, Code Based Public-Key Cryptosystem Based on Bursts-Correcting Codes, AICT 2017: The Thirteenth Advanced International Conference on Telecommunications, IARIA, 2017.

[26] G. Landais and J. P. Tillich, An efficient attack of a McEliece cryptosystem variant based on convolutional codes, In International Workshop on Post-Quantum Cryptography, pp. 102-117, Springer, Berlin, Heidelberg, 2013.

[27] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, University of London: London, UK, vol. 20, 1983.

[28] R. Lidl, G. L. Mullen, and G. Turnwald, Dickson Polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics 65, New York: Willey, 1993.

[29] C. Löndhal and T. Johansson, A New Version of McEliece Based on Convolutional Codes, In ICICS, vol. 7618, pp. 461-470, 2012.

[30] R. J. McEliece, A Public-Key Cryptosystem Based on Algebraic Coding Theory, DSN progress report 42(44), pp. 114-116, 1978.

[31] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, New York: CRC Press, 1997.

[32] L. Minder and A. Shokrollahi, Cryptanalysis of the Sidelnikov cryptosystem, Advances in Cryptology-EUROCRYPT 2007, pp. 347-360, 2007.

[33] R. Misoczki, J. P. Tillich, N. Sendrier, and P. Barreto, MDPC-McEliece: New McEliece variants from moderate density parity-check codes, IEEE International Symposium on Information Theory-ISIT 2013, pp. 2069-2073, 2013.

[34] C. Monico, J. Rosenthal, and A. Shokrollahi, Using low density parity check codes in the McEliece cryptosystem, In Information Theory, Proceedings, IEEE International Symposium, p. 215, 2000.

[35] NIST, A proposed federal information processing standard for digital signature standard (DSS), Federal Register, vol. 56, pp. 42980-42982, 1991.

[36] H. Niedderreiter, Knapsack-type cryptosystems and algebraic coding theory, Problems of Control and Information Theory, vol. 15, no. 1934, 1986.

[37] W. Nöbauer, Cryptanalysis of a public-key cryptosystem based on Dickson polynomials, Math. Slovaca, vol.38, pp. 309-323, 1989.

[38] R. Overbeck, A new structural attack for GPT and variants, Mycrypt 2005: Progress in Cryptology, LNCS, vol. 3715, pp. 50-63, 2005.

[39] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, https://doi.org/10.1145/359340-359342, February 1978.

[40] O. Regev, On lattices, learning with errors, random linear codes and cryptography, Journal of the ACM, vol. 56, no.6, Art. 34, 40, 2009.

[41] N. Sendrier, On the concatenated structure of a linear code, Applicable Algebra in Engineering, Communication and Computing, vol. 9, no. 3, pp. 221-242, 1998.

[42] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM journal on computing, vol. 26, no. 5, pp. 1484-1509, 1997.

[43] V. M. Sidelnikov, A public-key cryptosystem based on binary Reed-Muller codes, Discrete Mathematics and Applications, vol. 4, no. 3, pp. 191-208, 1994.

[44] V. M. Sidelnikov and S. O. Shestakov, On insecurity of cryptosystems based on generalized Reed-Solomon codes, Discrete Mathematics and Applications, vol. 2, no. 4, pp. 439-444, 1992.

[45] V. Skachek, T. Etzion, and R. M. Roth, Efficient encoding algorithm for third-order spectral-null codes, IEEE Trans. Inform. Theory, vol. 44, pp. 846-851, March 1998.

[46] P. Smith, LUC public-key encryption,Dr. Dobb's J., pp. 44-49, January 1993.

[47] P. Smith and C. Skinner, A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logartihms, in Proc. Asiacrypt'94, pp. 298-306, November 1994.

[48] D. R. Stinson, Cryptography: Theory and Practice, Boca Raton, FL: CRC Press, 1995, The CRC Series on Discrete Mathematics and Its Applications.

[49] C. Wieschebrink, Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes, In International Workshop on Post-Quantum Cryptography, pp. 61-72, Springer, Berlin, Heidelberg, May 2010.