

Article

Public-Key Cryptosystems and Bounded Distance Decoding of Linear Codes

Selda Çalkavur

Math Department, Faculty of Arts and Science, Kocaeli University, Kocaeli 41380, Turkey;
selda.calkavur@kocaeli.edu.tr

Abstract: Error-correcting codes form an important topic in information theory. They are used to correct errors that occur during transmission on a noisy channel. An important method for correcting errors is bounded distance decoding. The public-key cryptosystem is a cryptographic protocol that has two different keys. One of them is a public-key that can be known by everyone, and the other is the private-key only known to the user of the system. The data encrypted with the public-key of a given user can only be decrypted by this user with his or her private-key. In this paper, we propose a public-key cryptosystem based on the error-correcting codes. The decryption is performed by using the bounded distance decoding of the code. For a given code length, dimension, and error-correcting capacity, the new system allows dealing with larger plaintext than other code based public-key cryptosystems.

Keywords: public-key cryptosystem; error correcting code; bounded distance decoding



Citation: Çalkavur, S. Public-Key Cryptosystems and Bounded Distance Decoding of Linear Codes. *Entropy* **2022**, *24*, 498. <https://doi.org/10.3390/e24040498>

Academic Editors: Stanisław Drożdż, Jarosław Kwapien and Marcin Wątarek

Received: 9 March 2022

Accepted: 31 March 2022

Published: 1 April 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Public-key cryptosystems or asymmetric cryptosystems have been a subject of study since 1976. These systems consider two different keys, which are called public-key and private-key. These keys are not completely independent of each other. There must be a mathematical relationship as factoring, discrete logarithm, etc. [1,2]. The public-key cryptosystem was first introduced in 1976 by Diffie and Hellman [3]. Rivest, Shamir and Adleman's paper, known as the RSA cryptosystem [4], also present a public-key cryptosystem. The RSA cryptosystem was based on the factorization integers [5]. Merkle and Hellman [6] suggested a cryptosystem based on the difficulty of the integer packing "knapsack" problem.

The first public-key cryptosystem based on the error-correcting codes was presented by R. J. McEliece in 1978 [7]. He has employed error correcting codes, in particular binary Goppa codes, with a known decoding algorithm to construct the system. The generator matrix G plays an important role. The most important property of McEliece's cryptosystem is its large key size. Niederreiter suggested another code-based public-key cryptosystem that is based on the syndrome decoding of linear codes [8]. This system is used for the parity-check matrix H of a linear code. Thus, it is also the dual version of McEliece's cryptosystem. If it is used with exactly the same parameters [9], McEliece's cryptosystem and Niederreiter's cryptosystem offer an equivalent security. Li et al. [10] proposed new classes of trapdoor functions to solve the bounded distance decoding problem in lattices. Moreover, a lot of cryptosystems have been presented by using linear codes after McEliece's and Niederreiter's schemes. The use of subcodes of generalized Reed–Solomon codes was introduced by Berger and Loidreau [11]. Berlekamp et al. [12] studied the complexity of the decoding of arbitrary linear codes. Krouk [13] proposed a different class of public-key cryptosystems. Sidelnikov [14] introduced the use of Reed–Muller codes for cryptosystems. Berger et al. [15] and Misoczki-Barreto [16] proposed using quasi-cyclic and quasi-dyadic codes to shorten the McEliece key. The original parameters of the McEliece cryptosystem have been broken [17], but the general system is still considered safe.

In this study, we propose a public-key cryptosystem based on the error-correcting codes using a known bounded distance decoding method. We present the encryption and decryption algorithms by inspiring both McEliece's and Niederreiter's cryptosystems.

- McEliece's system has been constructed based on linear codes over \mathbb{F}_2 .
- Both Niederreiter's and our system have been constructed based on linear codes over \mathbb{F}_q .
- However, in our cryptosystem, since it is easier to generate the pieces of keys, the encryption, decryption, and key generation are more effective than Niederreiter's cryptosystem.
- Another difference of our system from Niederreiter's is the use of the bounded distance decoding method, which corrects errors and guarantees unique decoding.
- It is impossible to find the private-key with public-key by an attacker in our public-key cryptosystem.
- Similarly, even if an enemy knows the public-key and ciphertext, he/she cannot calculate the plaintext.

These conditions ensure the new system is safe. Moreover, we consider some possible attacks in this paper. So, we analyze its security and performance, and we calculate some important parameters for our cryptosystem. When we compared it with McEliece's and Niederreiter's cryptosystems, we can say that our system performs better as regards encryption speed.

The rest of the paper is organized as follows. The next section gives the necessary background on coding theory and cryptography. Section 3 introduces the new public-key cryptosystem. Section 4 analyzes its security and examines some possible attacks. Section 5 compares it to the other code-based public-key cryptosystems. Section 6 concludes the paper.

2. Preliminaries

In this section, we remind of some important topics [18,19] that are necessary for the paper.

2.1. Linear Codes

Definition 1 (Linear Code). A linear code C of length n and dimension k is a subspace of $(\mathbb{F}_q)^n$, where \mathbb{F}_q is the finite field with q elements, q is a prime power, and k and n are positive integers such that $k \leq n$. It is denoted by an $[n, k]$ -code. The error-correcting capacity of C is the maximum number t of errors that C can skillfully decode. All vectors of $(\mathbb{F}_q)^n$ that are orthogonal to every codeword of C consist of the dual code C^\perp which is an $[n, n - k]$ -code.

Definition 2 (Hamming Weight). The Hamming weight $w(x)$ of a vector x in $(\mathbb{F}_q)^n$ is the number of non-zero entries of x .

Definition 3 (Generator Matrix). A generator matrix G of C is the rows that are a basis of C . G is also a $k \times n$ matrix.

Definition 4 (Parity-Check Matrix). A parity-check matrix H for a linear code C is an $(n - k) \times n$ matrix which is a generator matrix for its dual code C^\perp .

2.2. Coset Decoding

Definition 5. Let C be an $[n, k]$ -code over \mathbb{F}_q and u be any vector in $(\mathbb{F}_q)^n$. The coset of C is defined as follows.

$$u + C = \{u + x \mid x \in C\}. \quad (1)$$

Theorem 1 (Lagrange). Suppose C is an $[n, k]$ -code over \mathbb{F}_q . Then,

- Every vector of $(\mathbb{F}_q)^n$ is in some coset of C ;
- Every coset contains exactly q^k vectors;

- (iii) Two cosets either are disjointed or coincided;
- (iv) C contains exactly q^{n-k} cosets.

Definition 6 (Coset Leader). The coset leader is the vector having a minimum weight in a coset. If a coset contains more than one vector which has the minimum weight, then it is chosen at random as the coset leader.

Definition 7 (Syndrome Decoding). Consider H is a parity-check matrix of an $[n, k]$ -code C . In this case,

$$S(y) = yH^T \quad (2)$$

is called the syndrome of y , where y is any vector of $(\mathbb{F}_q)^n$, the $1 \times (n - k)$ row vector. Moreover,

$$S(y) = 0 \implies y \in C. \quad (3)$$

Lemma 1. Two vectors u and v are in the same coset of C if and only if they have the same syndrome.

Corollary 1. There is a one-to-one correspondence between cosets and syndromes.

2.3. Public-Key Cryptosystems

A cryptosystem is an application of cryptographic methods and ensures the information security services. The cryptosystems can be examined under two titles as the public-key and private-key. Each person has a pair of keys; one is the public-key, and the other is the private-key. The public-key is accessible to the other users; however, the private-key should be stored so that only the owner can access it. Any person can send an encrypted message using the public-key, but only the private-key, which is a pair of public-keys, can decrypt the encrypted message. There is always the mathematical relationship between the public-key and private-key in the public-key cryptosystems. The hardness of two mathematical problems, as integer factoring and discrete logarithm, are used to generate these keys. So, it is impossible to obtain the private-key using the public-key.

The Diffie–Hellman cryptosystem [3] and RSA cryptosystem [4] are pioneers of public-key cryptosystems. However, McEliece [7] and Niederreiter [8] are the first founders of the code-based public-key cryptosystems.

2.4. McEliece's Public-Key Cryptosystem

McEliece's public-key cryptosystem is the first system based on the algebraic block codes; it was presented in 1978 [7]. In order to construct his cryptosystem, it used a binary $(n, k, 2t + 1)$ Goppa code C . It is clear that n is the code length, k is the code dimension, and t is the error-correcting capacity of C . The encryption and decryption algorithms are as follows.

Private-key: G, S, P ; where G is a $k \times n$ generator matrix, S is any $k \times k$ non-singular matrix, and P is any $n \times n$ permutation matrix.

Public-key: $G' = SG$ and t .

Plaintexts: k bit vectors m over \mathbb{F}_2 .

Encryption:

$$c = mG' + e, \quad (4)$$

where e is an n -bit error vector with Hamming weight t . So, c is the n -bit ciphertext.

Decryption:

$$cP^{-1} = (mS)G + eP^{-1} \quad (5)$$

since

$$c = mSGP. \quad (6)$$

It is used as the fast decoding algorithm for C to correct the error eP^{-1} ; then, it is found mS and therefore m .

2.5. Niederreiter's Public-Key Cryptosystem

Niederreiter [8] proposed a knapsack-type public-key cryptosystem which is based on $(n, k, 2t + 1)$ linear code C over \mathbb{F}_q .

Private-key: H, M , and P , where H is an $(n - k) \times n$ parity-check matrix of C , M is any $(n - k) \times (n - k)$ non-singular matrix, and P is any $n \times n$ permutation matrix, all over \mathbb{F}_q .

Public-key: $H' = MHP$ and t .

Plaintexts: n -dimensional vectors m over \mathbb{F}_q with weight t .

Encryption: $c = mH'^T$, c is the ciphertext of dimension $n - k$.

Decryption:

$$c(M^T)^{-1} = (mP^T)H^T \quad (7)$$

since

$$c = m(MHP)^T. \quad (8)$$

It is used as the fast decoding algorithm for C to obtain mP^T and m .

3. The System

The construction of our public-key cryptosystem is based on $[n, k, 2t + 1]$ -code over \mathbb{F}_q . The syndrome-decoding procedure is used for decryption. The public-key and private-key are constructed by each user as follows.

- (1) Select a generator $k \times n$ matrix G of a linear $[n, k, 2t + 1]$ -code C over \mathbb{F}_q , where t is the error-correcting capability.
- (2) Construct a parity-check $(n - k) \times n$ matrix H from G for the code C .
- (3) Select any non-zero syndrom vector h which has weight t and dimension $(n - k)$.
- (4) Select a random non-singular $(n - k) \times (n - k)$ matrix M over \mathbb{F}_q .
- (5) Calculate $n \times (n - k)$ matrix $H' = H^T \cdot M$, where H^T is denoted by the transpose of H .
- (6) The public-key is (H', h) .
- (7) The private-key is (G, H, M) .

Encryption:

Message: n dimension vector m over \mathbb{F}_q with weight t .

Cryptogram: $c = mH' + h$

Decryption:

- (1) Calculate $c' = cM^{-1}$;
- (2) Obtain m by syndrome decoding c' in the code C .

Decryption is correct, since

$$w(hM^{-1}) = w(h), \quad (9)$$

it can be computed

$$c' = cM^{-1} = (mH' + h)M^{-1} = mH'M^{-1} + hM^{-1} \quad (10)$$

$$cM^{-1} = mH^TMM^{-1} + hM^{-1} \quad (11)$$

$$cM^{-1} = mH^T + hM^{-1} \quad (12)$$

$$cM^{-1} - hM^{-1} = mH^T \quad (13)$$

and the procedure of syndrome decoding may be effectively used.

Example 1. Consider an $[4, 2, 3]$ -code C over \mathbb{F}_3 . The generator matrix G and parity-check matrix H are

$$G = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}, \quad (14)$$

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}. \quad (15)$$

$C = \{0000, 0121, 0212, 1022, 1110, 1201, 2011, 2102, 2220\}$. Select any non-singular matrix $M = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$. The syndromes and coset leaders of C are as follows.

Syndromes	Coset Leaders
(00)	(0000)
(11)	(1000)
(12)	(0100)
(10)	(0010)
(01)	(0001)
(22)	(2000)
(21)	(0200)
(20)	(0020)
(02)	(0002)

The size of different cosets of C is

$$3^{4-2} = 3^2 = 9.$$

So, there are also nine syndrome vectors, which are $\{00, 11, 12, 10, 01, 22, 21, 20, 02\}$. Calculate the matrix

$$H' = H^T \cdot M = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 2 & 2 \\ 1 & 2 \\ 2 & 0 \end{pmatrix} \quad (16)$$

and

$$M^{-1} = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}. \quad (17)$$

Let h be the syndrome vector (20). Since $d = 3$, C is the corrected $t = 1$ error. So, the public-key is

$$H' = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, h = (20) \quad (18)$$

and the private-key is

$$(G, H, M) = \left(\begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \right). \quad (19)$$

Encryption: Let the message vector be $m = (1000)$ and $h = (20)$. The cryptogram is

$$c = mH' + h = (1000) \cdot \begin{pmatrix} 0 & 2 \\ 2 & 2 \\ 1 & 2 \\ 2 & 0 \end{pmatrix} + (20) = (02) + (20) = (22). \quad (20)$$

Decryption: Calculate

$$c' = cM^{-1} = (22) \cdot \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} = (12). \quad (21)$$

Since

$$c = mH' + h \quad (22)$$

and

$$H' = H^T \cdot M, \quad (23)$$

c' is also equal to

$$c' = (mH' + h)M^{-1} = mH'M^{-1} + hM^{-1} = mH^TMM^{-1} + hM^{-1} \quad (24)$$

$$c' = mH^T + hM^{-1}. \quad (25)$$

So,

$$(12) = (m_1m_2m_3m_4) \cdot \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} + (20) \cdot \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}. \quad (26)$$

$$(12) = (m_1 + m_2 + m_3, m_1 + 2m_2 + m_4) + (01) \quad (27)$$

$$(12) - (01) = (m_1 + m_2 + m_3, m_1 + 2m_2 + m_4) \quad (28)$$

$$(11) = (m_1 + m_2 + m_3, m_1 + 2m_2 + m_4). \quad (29)$$

We get the message $m = (1000)$ by solving the linear system.

Proposition 1. The size of the plaintext is $\log_q \binom{n}{t}$.

Proof. The plaintext is an $n - q$ tuple word of weight t . These are the integers between 1 and $\binom{n}{t}$ to the set of words of weight t and length n . Therefore, the size of the plaintext is $\log_q \binom{n}{t}$. \square

Proposition 2. The size of the ciphertext is $(n - k)$.

Proof. Since the ciphertext is a $(n - k) - q$ tuple word, the proof is clear. \square

Corollary 2. The transmission rate of the new system is

$$\frac{\log_q \binom{n}{t}}{(n - k)}.$$

Proof. The proportion of the number of information symbols to the number of transmitted symbols gives the transmission rate. So, it is

$$\frac{\log_q \binom{n}{t}}{(n - k)}.$$

\square

Proposition 3. Given a syndrome vector y of weight w , the number of eligible h 's is $\binom{w}{t}(q - 1)^t$.

Proof. It is known that the weight of h is t , and h is non-zero. Thus, the number of non-zero vectors of weight t among the vectors of w is $\binom{w}{t}(q - 1)^t$. \square

Example 2. Let C be the extended binary Hamming code of parameters $[8, 4, 4]$. Its packing radius is 1. We examine some properties of the public-key cryptosystem based on C . The size of the plaintext is

$$\log_2 \binom{8}{1} = \log_2 8 = 3.$$

The size of the ciphertext is

$$8 - 4 = 4.$$

The transmission rate is

$$\frac{\log_2 \binom{8}{1}}{(8 - 4)} = 0,75.$$

4. Security Comments

In this section, we examine the security of the new system. We recommend using a linear $[n, k, 2t + 1]$ -code over \mathbb{F}_q . The decryption method is based on the bounded distance decoding task. In order to be a secure public-key cryptosystem, the following conditions should be implemented.

- The size of the public-key should be fairly small. In our cryptosystem, this size is $(n - k)$, which is reasonably small.
- The encryption, decryption, and key generation should be effective. It is computationally simple to create the public-key and private-key. Thus, the encryption and decryption algorithms are too efficient.
- It should be impossible to reach the plaintext by an attacker.
- The system should be resistant to all possible attacks. Now, we discuss these attacks for the new system.

4.1. Algebraic Attack

The security of a public-key cryptosystem depends on the security of the private-key. So, the first attack will be factorization H' to find the private-keys G, H , and M . If the code parameters n, k, d are large enough, this attack is impracticable, because it is difficult to recover the factors of H' . This means the security is ensured with the private-key. The security of the new system is also based on decoding in the code H' , while H' is not only non-equivalent to the code H in the cryptosystem, but after multiplying H^T by M from the right, the error-correction capability of public-key H' is unknown. Furthermore, the vector h is secret. Thus, the best attack may not carry out the complete decoding.

4.2. Generic Attack

The second attack is to reach m from c without using the private-key. The plaintext is an n -q tuple word of weight t . We require an useful algorithm that matches the integers between 1 and $\binom{n}{t}$ to the set of words of weight t and length n and vice versa, since the plaintext is a n -q tuple word of weight t . In this case, the attacker will try to repeatedly select n bits at random from an $(n - k)$ -bit ciphertext vector and guess m based on the n selected bits, which is impossible. So, our cryptosystem is strong to all possible attacks. At the same time, the described system presents a general access, which is not for the specific cryptosystem.

Moreover, the probability of no error in the constructing of this system is

$$\left(1 - \frac{t}{n - k}\right)^n.$$

Consider the Goppa code, which has the parameters

$$n = 1024, k = 524, t = 50.$$

In the public-key cryptosystem constructing based on this code, the probability of no error is

$$\left(1 - \frac{50}{500}\right)^{1024} = (0.9)^{1024}.$$

It is a very small number.

5. Comparison with the Other Public-Key Cryptosystems

In this section, we compare our system with the other code-based cryptosystem for an $[n, k, d]$ -code C over \mathbb{F}_q , where $d \geq 2t + 1$. We denote by S, R, T , and K , respectively, the size of plaintext, ciphertext, the transmission rate, and the dimension of the public-key.

The new system is a further development of the McEliece and Niederreiter cryptosystems. McEliece's system is constructed based on binary linear codes, but both Niederreiter's and our new system are constructed based on linear codes over \mathbb{F}_q . Especially, we use the bounded distance decoding to construct our system. In the new system, as the public-key is smaller than McEliece's cryptosystem, it is more useful in industry. Moreover, as it is seen in Table 1, the plaintext is a word of small weight, which is one of the coset leaders, and the number of operations involved during the encryption is less than McEliece's cryptosystem. Furthermore, it is seen that the public-keys in our system and Niederreiter's system are equivalent. However, our system is more effective than Niederreiter's cryptosystem, since it is easier to generate the pieces of keys. This condition increases the security. It is impossible to reach the private-key with public-key by an attacker in the new system. In addition, the plaintext cannot be calculated even if the public-key and ciphertext are known by an enemy cryptanalyst. When the transmission rates of systems are compared, it is noticed that the proposed system has the bigger magnitude. That is, the encryption is faster than the others. So, it is more reliable by means of security.

Table 1. Comparison with other schemes.

System	[7]	[8]	This Paper
S	k	n	n
R	k	$n - k$	$n - k$
T	$\frac{k}{n}$	$\frac{\log_2 \binom{n}{t}}{(n-k)}$	$\frac{\log_q \binom{n}{t}}{(n-k)}$
K	k	$n - k$	$n - k$

6. Conclusions

We presented a new public-key cryptosystem based on error-correcting codes in this study. This system refers to the class of cryptosystems based on the bounded distance decoding task. The sizes of the plaintext and ciphertext of the system are calculated. Therefore, the transmission rate is given. The possible attacks are considered. It is determined that the new system stands well when compared with known systems.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: I would like to thank to Patrick Solé for his valuable comments, which helped to improve the content of the paper.

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

References

1. Krasnobayev, V.A.; Yanko, A.S.; Koshman, S.A. A Method for arithmetic comparison of data represented in a residue number system. *Cybern. Syst. Anal.* **2016**, *52*, 145–150. [\[CrossRef\]](#)
2. Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1997.
3. Diffie, W.; Hellman, M.E. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *IT-22*, 644–654. [\[CrossRef\]](#)
4. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *26*, 96–99. [\[CrossRef\]](#)
5. Markku-Juhani, O. Saarinen, Linearization attacks against syndrome based hashes. In Proceedings of the 8th International Conference on Cryptology in India, Chennai, India, 9–13 December 2007.
6. Merkle, R.C.; Hellman, M.E. Hiding information and signatures in trapdoor knapsacks. *IEEE Trans. Inform. Theory* **1978**, *24*, 525–530. [\[CrossRef\]](#)
7. McEliece, R.J. *A Public-Key Cryptosystem Based on Algebraic Coding Theory*; DSN Progress Report; Jet Propulsion Laboratory: Pasadena, CA, USA, 1978; pp. 42–44.
8. Niederreiter, H. Knapsack-type cryptosystems and algebraic coding theory. *Probl. Control. Inf. Theory* **1986**, *15*, 19–34.
9. Li, Y.X.; Deng, R.H.; Wang, X.M. On the equivalence of mceliece's and niederreiter's public-key cryptosystems. *IEEE Trans. Inf. Theory* **1994**, *40*, 271.
10. Li, Z.; Ling, S.; Xing, C.; Yeo, S.L. On the Bounded Distance Decoding Problem for Lattices Constructed and Their Cryptographic Applications. *IEEE Trans. Inf. Theory* **2020**, *66*, 2588–2598. [\[CrossRef\]](#)
11. Berger, T.P.; Loidreau, P. How to mask the structure of codes for a cryptographic use. *Des. Codes Cryptogr.* **2005**, *35*, 63–79. [\[CrossRef\]](#)
12. Berlekamp, E.; McEliece, R.; van Tilborg, H. On the inherent intractability of certain coding problems (corresp.). *IEEE Trans. Inf. Theory* **1978**, *24*, 384–386. [\[CrossRef\]](#)
13. Krouk, E. A New Public-Key Cryptosystem. In Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, 11–15 May 1997; pp. 285–286.
14. Sidelnikov, V.M. A public-key cryptosystem based on binary reed-muller codes. *Discret. Math. Appl.* **1994**, *4*, 191–208. [\[CrossRef\]](#)
15. Berger, T.P.; Cayrel, P.-L.; Gaborit, P.; Otmani, A. Reducing key length of the mceliece cryptosystem. In Proceedings of the Second International Conference on Cryptology in Africa, Gammarth, Tunisia, 21–25 June 2009; pp. 77–97.
16. Misoczki, R.; Barreto, P. Compact mceliece keys from goppa codes. In *Selected Areas in Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 376–392.
17. Canteaut, A.; Chabaud, F. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Trans. Inf. Theory* **1998**, *44*, 367–378. [\[CrossRef\]](#)
18. Hill, R. *A First Course in Coding Theory*; Oxford University: Oxford, UK, 1986.
19. Véron, P. Code based cryptography and steganography. In Proceedings of the 5th International Conference, CAI 2013, Porquerolles, France, 3–6 September 2013.