cryptography

MDPI

Article

A New Class of Q-Ary Codes for the McEliece Cryptosystem

Jürgen Freudenberger * and Johann-Philipp Thiers

Institute for System Dynamics (ISD), HTWG Konstanz, University of Applied Sciences, 78462 Konstanz, Germany; jthiers@htwg-konstanz.de

* Correspondence: jfreuden@htwg-konstanz.de; Tel.: +49-7531-206-647

Abstract: The McEliece cryptosystem is a promising candidate for post-quantum public-key encryption. In this work, we propose q-ary codes over Gaussian integers for the McEliece system and a new channel model. With this one Mannheim error channel, errors are limited to weight one. We investigate the channel capacity of this channel and discuss its relation to the McEliece system. The proposed codes are based on a simple product code construction and have a low complexity decoding algorithm. For the one Mannheim error channel, these codes achieve a higher error correction capability than maximum distance separable codes with bounded minimum distance decoding. This improves the work factor regarding decoding attacks based on information-set decoding.

Keywords: public-key cryptography; code-based cryptosystem; McEliece cryptosystem; Gaussian integers; decoding attack; information-set decoding

Citation: Freudenberger, J.; Thiers, J.-P. A New Class of Q-Ary Codes for the McEliece Cryptosystem. *Cryptography* **2021**, *5*, 11. https://doi.org/10.3390/cryptography5010011

Received: 8 February 2021
Accepted: 9 March 2021
Published: 15 March 2021

1. Introduction

Today, the most common-used public-key cryptosystem are the Rivest-Shamir-Adleman (RSA) system and elliptic curve cryptography (ECC). However, large-scale quantum computers threaten the security of such public-key cryptosystems. For instance, RSA is based on the intractability of integer factorization for which a polynomial-time quantum algorithm was proposed by Shor [1].

The McEliece cryptosystem was proposed in 1978 [2] but did not gain wide practical usage due to the large size of the public key. This code-based cryptosystem is among the best candidates for post-quantum cryptography standardization [3]. So far, no effective quantum algorithm is known to break the McEliece system. The security of this system is based on the problem of decoding an arbitrary linear code. This task is computationally demanding and known to be NP-complete [4]. Reed-Solomon (RS) codes [5,6], BCH codes [7], LDPC codes [8–11], and polar codes [12] have been proposed for the McEliece cryptosystem. These codes have polynomial-time decoding algorithms which is required for deciphering.

Today, the best known attacks against the McEliece cryptosystem are based on information-set decoding (ISD). For instance, such cryptanalytic attacks were developed in [13–16]. Typically, the ISD attack determines the work factor of the McEliece cryptosystem. The work factor is the expected number of computations potential attackers have to perform.

In this work, we consider a new class of q-ary codes for the McEliece cryptosystem. These codes are constructed over Gaussian integers which are complex numbers with integer real and imaginary parts. Linear codes over Gaussian integer fields were first studied by Huber in [17]. Huber also introduced the Mannheim distance as a performance measure for such codes. Later on, codes over groups and rings of Gaussian integers were considered in [18–20]. However, most of these code constructions can correct only a small number of errors. A code-based cryptosystem with codes over Gaussian integers was proposed in [21]. However, the limited error-correcting capability of the known code constructions is not sufficient for a secure McEliece cryptosystem.

In this work, we propose a code construction, which achieves a high error correction capability with a very simple decoding strategy. This construction is based on product codes. Product codes over Gaussian integers were investigated in [22,23], where all component codes are codes over Gaussian integers. In contrast, we consider a different construction where ordinary RS codes over prime fields are combined with simple one Mannheim error correcting (OMEC) codes. We compare the proposed codes with maximum distance separable (MDS) codes. MDS codes are optimal with respect to the minimum Hamming distance, that is, these codes achieve equality in the Singleton bound [24]. Nevertheless, we demonstrate that the error correction capability of the proposed q-ary codes with bounded minimum distance decoding can exceed that of MDS codes. This is possible because we restrict the elements of the error vector to Mannheim weight one. This restriction increases the correctable number of errors and improves the work factor compared with MDS codes with comparable parameters. Furthermore, we investigate the one Mannheim error channel, where errors are limited to Mannheim weight one. We derive the channel capacity of this channel and discuss its relation to the McEliece system.

This publication is organized as follows—in Section 2, we introduce the notation and review the basic concept of the McEliece cryptosystem, the information-set decoding attack and of codes over Gaussian integers. The new product code construction is presented in Section 3. We provide some code examples that achieve a higher error correction capability than maximum distance separable codes with bounded minimum distance decoding. The decoding procedure is discussed in more detail in Section 4. In Section 5, we consider the performance for decoding beyond the guaranteed error correction capability. In Section 6, we investigate the capacity of the one Mannheim error channel and its relation to the McEliece system. Conclusions are drawn in Section 7.

2. Preliminaries and Problem Statement

In this section, we discuss the McEliece cryptosystem and the attack by information-set decoding. Moreover, we review some basic properties of codes over Gaussian integers.

2.1. The McEliece Cryptosystem

We briefly review the McEliece public-key cryptosystem for q-ary codes [2]. We assume that the plaintext is represented as a q-ary vector $\mathbf{u}$ of length k. The original McEliece cryptosystem is based on t-error correcting linear code $\mathcal{C}$ of length n, dimension k, and minimum Hamming distance $d = 2t + 1$. We use the common notation $\mathcal{C}(n, k, d)$ to denote the code parameters. The code can be represented by its $k \times n$ generator matrix $\mathbf{G}$. Moreover, an efficient decoding algorithm $\phi(\cdot)$ is required that corrects up to t errors in polynomial time.

The public key is the pair $(\mathbf{G}', t)$, where $\mathbf{G}'$ is a matrix used for encoding and t is the error-correcting capability of the code. The matrix $\mathbf{G}' = \mathbf{SGP}$, where $\mathbf{S}$ is a random non-singular $k \times k$ matrix with elements from the Galois field $GF(q)$. The $n \times n$ matrix $\mathbf{P}$ is a random permutation matrix, that is, it has exactly one entry 1 in each row and each column and 0s elsewhere. The secret key consist of the matrices $(\mathbf{G}, \mathbf{S}, \mathbf{P})$.

Encryption: Using the public matrix $\mathbf{G}'$, the plaintext $\mathbf{u}$ can be encoded as $\mathbf{v} = \mathbf{u}\mathbf{G}' + \mathbf{e}$, where $\mathbf{e}$ is a random q-ary error vector with at most t non-zero elements.

Decryption: With the knowledge of $\mathbf{G}$, $\mathbf{S}$, and $\mathbf{P}$, the ciphertext $\mathbf{v}$ can be decrypted as follows: Calculate $\mathbf{r} = \mathbf{v}\mathbf{P}^{-1} = \mathbf{u}\mathbf{S}\mathbf{G} + \mathbf{e}\mathbf{P}^{-1}$. The matrix $\mathbf{P}^{-1}$ is the inverse permutation and $\mathbf{e}\mathbf{P}^{-1}$ is the permuted error vector which has at most t non-zero elements. Hence, we can apply the decoding algorithm $\phi(\cdot)$ which obtains $\phi(\mathbf{r}) = \phi(\mathbf{v}\mathbf{P}^{-1}) = \mathbf{u}\mathbf{S}$. Finally, the plaintext is calculated as $\mathbf{u} = \mathbf{u}\mathbf{S}\mathbf{S}^{-1}$.

Without knowledge of secret key, cryptanalysis has to solve the complex task of decoding an arbitrary code described by the generator matrix $\mathbf{G}'$. This task is known to be NP-complete [4].

2.2. Information-Set Decoding

One of the best known attacks against the McEliece cryptosystem is based on information-set decoding (ISD). This type of attack was already mentioned in the initial proposal of the cryptosystem. Such cryptanalytic attacks were developed by Lee and Brickell [13] or Stern [14]. More recent, different improvements to Stern's algorithm were proposed in [15,16]. We review the general concept of these attacks.

Information-set decoding is a probabilistic decoding strategy. The task of the decoder is to recover information vector $\mathbf{u}' = \mathbf{u}\mathbf{S}$ from $\mathbf{v} = \mathbf{u}'\mathbf{G}' + \mathbf{e}$. The attacker tries to guess k correct positions $\mathbf{u}''$ in the ciphertext $\mathbf{v}$ such that the corresponding columns of $\mathbf{G}'$ form an invertible matrix $\mathbf{G}''$. A codeword $\mathbf{v}''$ agreeing with the ciphertext $\mathbf{v}$ on the guessed positions $\mathbf{u}''$ can easily be computed using Gaussian elimination. If the codeword $\mathbf{v}''$ differs in at most t positions from $\mathbf{v}$ than there is no error in $\mathbf{u}''$. In this case, we obtain $\mathbf{u}' = \mathbf{u}''\mathbf{G}''^{-1}$.

The probability P_s of successful decoding is equal to the probability of having no errors in the guessed k positions [25]

$$P_s = \frac{\binom{n-t}{k}}{\binom{n}{t}} = \frac{\binom{n-k}{t}}{\binom{n}{t}}. \tag{1}$$

The complexity of Information-set decoding is the expected number of decoding attempts

$$N_{ISD} = \frac{1}{P_s} = \frac{\binom{n}{t}}{\binom{n-k}{t}}. \tag{2}$$

For the McEliece cryptosystem, a complexity of order 2^{80} is considered to be secure [9,10].

From (2), we observe that the code length n and the error correction capability t of the code should be large to achieve a high complexity for the attack. Code families with large minimum distances allow to use shorter codes. For instance, maximum distance separable (MDS) codes achieve equality in the Singleton bound $d \leq n - k + 1$ for the minimum Hamming distance d [24]. Thus, MDS codes can correct $t = (n-k)/2$ errors with bounded minimum distance decoding. Generalized Reed-Solomon (GRS) codes are MDS codes with an efficient decoding algorithm and were proposed for the McEliece cryptosystem in [5,6].

In this work, we demonstrate that the error correction capability of a q-ary code can exceed the value $t = (n-k)/2$. Due to the Singleton bound, this is not possible if the non-zero elements of error vector are arbitrary q-ary symbols. However, by restricting the values of the errors we can increase the number of errors. Note that the work factor in (2) does not depend on the number of error values. Restricting the number of possible error values can increase the work factor. We demonstrate this for codes over Gaussian integers.

2.3. Gaussian Integers

Most known code constructions for Gaussian integers are linear codes based on finite Gaussian integer fields $\mathcal{G}_p$. These finite fields are constructed from primes p of the form $p \equiv 1 \bmod 4$ [17]. Such a prime is the sum of two perfect squares, that is, $p = a^2 + b^2$ with the integers a and b. In this case, we have $p = \pi \cdot \pi^* = |a|^2 + |b|^2$, with the Gaussian integer $\pi = a + b\mathrm{i}$. The Gaussian integer π^* is the conjugate of the complex number π. We use the notation $[\cdot]$ to denote rounding, that is, we have $[z] = [a] + [b]\mathrm{i}$ for a complex number $z = a + b\mathrm{i}$. The modulo function of a Gaussian integer z is defined as [17]

$$z \bmod \pi = z - \left[\frac{z\pi^*}{\pi \cdot \pi^*}\right] \cdot \pi. \tag{3}$$

The finite Gaussian integer field is the set $\mathcal{G}_p = \{z \bmod \pi : z = 0, \ldots, p-1, z \in \mathbb{Z}\}$. This set is isomorphic to the finite field $GF(p)$ [17].

The Mannheim weight of a Gaussian integer z is defined as [26]

$$wt_{\mathrm{M}}(z) = \min_{a+b\mathrm{i}\in\mathcal{K}(z)} |a| + |b|, \tag{4}$$

where the class $\mathcal{K}(z)$ of a Gaussian integer z is the set of all numbers z' such that $z = z' \bmod \pi$. The Mannheim weight of a vector $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1})$ is

$$wt_{\mathrm{M}}(\mathbf{y}) = \sum_{i=0}^{n-1} wt_{\mathrm{M}}(y_i). \tag{5}$$

The Mannheim distance between two Gaussian integers y and z is

$$d_{\mathrm{M}}(y, z) = wt_{\mathrm{M}}(y - z). \tag{6}$$

Similarly, the Mannheim distance between the vectors $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1})$ and $\mathbf{z} = (z_0, z_1, \ldots, z_{n-1})$ is

$$d_{\mathrm{M}}(\mathbf{y}, \mathbf{z}) = \sum_{i=0}^{n-1} d_{\mathrm{M}}(y_i, z_i) = wt_{\mathrm{M}}(\mathbf{y} - \mathbf{z}). \tag{7}$$

2.4. One Mannheim Error Correcting (OMEC) Codes

OMEC codes were presented in [17] for Gaussian integer fields and in [20] for Gaussian integer rings. We consider only codes over the Gaussian integer field $\mathcal{G}_p$, where α is a primitive element of the field. An OMEC code of length $n \leq (p-1)/4$ over $\mathcal{G}_p$ is defined by its parity check matrix, where the elements are generated by powers of α, that is,

$$\mathbf{H} = (\alpha^0, \alpha^1, \ldots, \alpha^{n-1}). \tag{8}$$

Codewords are all vectors $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ with $v_i \in \mathcal{G}_p$ for which $\mathbf{H}\mathbf{v}^T = 0$. An OMEC code has minimum Hamming distance $d_H = 2$ and minimum Mannheim distance $d_M = 3$. It can correct a single error of Mannheim weight one with simple syndrome decoding [17].

In the following, we consider a slightly different OMEC construction for codes of length $n = 2$. For sufficiently large field sizes, we can obtain codes with minimum Mannheim distance $d_M = 4$ based on an element $a \in \mathcal{G}_p$ of Mannheim weight $wt_{\mathrm{M}}(a) = 3$. Such a code has parity check matrix $\mathbf{H} = (1, a)$ and the generator matrix $\mathbf{G} = c(-a, 1)$, where c is an arbitrary non-zero field element. Hence, we have $\mathbf{H}\mathbf{G}^T = 0$. This code can correct a single error of Mannheim weight one and detect any error of weight two with syndrome decoding.

Example 1. *We consider an OMEC code for the prime $p = 41$ with $\pi = 5 + 4\mathrm{i}$. With $a = 3 + \mathrm{i}$ we construct the parity check matrix $\mathbf{H} = (1, a) = (1, 3 + \mathrm{i})$ and the generator matrix $\mathbf{G} = (-a, 1) = (-3 - \mathrm{i}, 1)$. Assume the transmitted codeword $\mathbf{v} = (-3 - \mathrm{i}, 1)$ and the received vector $\mathbf{r} = (-3, 1)$ with an error in the first symbol. To decode this vector, we calculate the syndrome*

$$\sigma = \mathbf{H} \cdot \mathbf{r}^T = \mathrm{i}. \tag{9}$$

Based on the syndrome we can determine the error position and the error value using a table look-up procedure. An error of weight one in the first position corresponds to syndrome values $\sigma \in \{\pm 1, \pm \mathrm{i}\}$, whereas an error of weight one in the second position corresponds to syndrome values $\sigma \in \{\pm a, \pm \mathrm{i}a\}$. All other syndrome values indicate uncorrectable error patterns.

The syndrome decoding of OMEC codes can be implemented efficiently using the Montgomery arithmetic for Gaussian integers proposed in [27] for the syndrome calculation. The error correction can be implemented using two-dimensional look-up tables for the

error positions and error values, where the real and imaginary parts of the syndrome are the arrays' indices.

On the other hand, the Gaussian integer field $\mathcal{G}_p$ is isomorphic to the finite field $GF(p)$. Hence, we can use the set $\mathcal{G}_p$ only to determine the elements $\mathfrak{i} \in GF(p)$ and $\mathfrak{a} \in GF(p)$ corresponding to the complex numbers $\mathfrak{i} \in \mathcal{G}_p$ and $a \in \mathcal{G}_p$ such that $\mathfrak{i} = \mathfrak{i} \bmod \pi$ and $a = \mathfrak{a} \bmod \pi$. The other error and syndrome values can be calculated in the ordinary integer field, since $-1 = p - 1 \bmod \pi$ and $-\mathfrak{i} = p - \mathfrak{i} \bmod \pi$. Similarly, we have $-a = p - \mathfrak{a} \bmod \pi$, $\mathfrak{i}a = \mathfrak{i}\mathfrak{a} \bmod \pi$, and $-\mathfrak{i}a = p - \mathfrak{i}\mathfrak{a} \bmod \pi$. Consequently, the encoding and decoding can be implemented with ordinary prime field arithmetic.

A code-based cryptosystem with OMEC codes over Gaussian integers was proposed in [21]. The results in [21] demonstrate some advantages of codes over Gaussian integers compared with binary codes. However, OMEC codes are not sufficient to achieve a high work factor. In [21], the work factor for ISD was considered but not according to (2). Yet there exists an even simpler decoding attack which was not considered in [21]. When the weight of the errors is fixed to Mannheim weight one and the number of errors is fixed to t, then the number of correctable error patterns is

$$N_P = 4^t \binom{n}{t} \geq \left(4\frac{n}{t}\right)^t, \tag{10}$$

which follows from the lower bound on binomial coefficients

$$\left(\frac{n}{t}\right)^t \leq \binom{n}{t}.$$

Hence, a code with large error correction capability t is needed to prevent a decoding attack, where all possible error patterns are tested. An attacker can determine the parity check matrix $\mathbf{H}'$ for the public key $\mathbf{G}'$. An error pattern that satisfies $(\mathbf{r} - \mathbf{e})\mathbf{H}' = \mathbf{0}$ solves the decoding problem. OMEC codes with $t = 1$ result in $N_P = 4n$. Thus, the decoding attack on the cryptosystem from [21] can be performed in polynomial time.

Most known code constructions over Gaussian integers can correct only a small number of errors [17–20]. The error-correcting capability of these code constructions does not suffice for a secure McEliece cryptosystem. A suitable code family is proposed in the next section, where we demonstrate that the error correction capability of the proposed q-ary codes with bounded minimum distance decoding can exceed that of MDS codes. This is possible because we restrict the non-zero elements of the error vector to Mannheim weight one.

3. Product Codes Based on OMEC Codes

Product codes over Gaussian integers were investigated in [22,23], where all component codes are codes over Gaussian integers. In contrast, we consider a different construction where outer RS codes $\mathcal{C}_o(n_o, k_o, d_o)$ over the prime field $GF(p)$ are combined with inner codes $\mathcal{C}_i(n_i, k_i, d_i)$ over $\mathcal{G}_p$. The parameter $d_o = n_o - k_o + 1$ denotes the minimum Hamming distance of the RS code, whereas d_i is the minimum Mannheim distance of the inner code.

A codeword is represented by an $(n_o \times n_i)$-matrix. For encoding, we first encode k_i codewords of the RS code and store these codewords row-wise into the first k_i columns of the codeword matrix, where the code symbols are mapped to elements from $\mathcal{G}_p$. Then, we use the OMEC code n_o-times to encode each column of the matrix.

Proposition 1. *The product code with outer RS codes $\mathcal{C}_o(n_o, k_o, d_o)$ and inner codes $\mathcal{C}_i(n_i, k_i, d_i)$ over $\mathcal{G}_p$ has length $n = n_o n_i$, dimension $k = k_o k_i$, and minimum Mannheim distance $d = d_o d_i = d_i(n_o - k_o + 1)$.*

Proof. The length and dimension directly follow from the construction. The product code $\mathcal{C}$ is a linear code, that is, the sum of two codewords $\mathbf{v}', \mathbf{v}'' \in \mathcal{C}$ is also a codeword. Hence, we have

$$d = \min_{\mathbf{v}', \mathbf{v}'' \in \mathcal{C}, \mathbf{v}' \neq \mathbf{v}''} d_{\mathrm{M}}(\mathbf{v}', \mathbf{v}'') = \min_{\mathbf{v} \in \mathcal{C}, \mathbf{v} \neq \mathbf{0}} wt_{\mathrm{M}}(\mathbf{v}). \tag{11}$$

According to (11), the minimum Mannheim distance of the product code is equivalent to the minimum Mannheim weight of a non-zero codeword. A non-zero codeword has at least one non-zero row. This row is a codeword of the code $\mathcal{C}_o(n_o, k_o, d_o)$ and has at least Hamming weight d_o, that is, a non-zero row contains at least d_o non-zero elements. Each non-zero element of this row results in a non-zero column, where each non-zero column is a codeword of the code $\mathcal{C}_i(n_i, k_i, d_i)$ and has at least Mannheim weight d_i. Consequently, a non-zero codeword has at least d_o non-zero columns with minimum weight d_i. □

In order to demonstrate the error correction capability, we consider a special case of these product codes with $\mathcal{C}_i(2, 1, 4)$ inner codes as introduced in Section 2.4. To avoid systematic encoding for the inner codes, we use the generator matrices $\mathbf{G}_l = c_l(-a, 1)$, $l = 0, \ldots, n_o - 1$, where c_l are random non-zero field elements.

According to Proposition 1, the resulting code has length $n = 2n_o$, dimension $k = k_o$ and even minimum Mannheim distance $d = 4d_o = 4(n_o - k_o + 1)$. Thus, the code should correct $t = (d-2)/2 = 2(n_o - k_o) + 1 = n - 2k + 1$ errors. This can be achieved with a simple error and erasure decoding procedure. Note that the inner codes can correct any error of Mannheim weight one, whereas two errors of Mannheim weight one result in a decoding failure. If the errors are limited to Mannheim weight one then the inner decoding results in a correct decoding or a decoding failure. Erroneous decoding cannot occur. A decoding failure can be utilized for erasure decoding of the outer Reed-Solomon code. An RS code can correct $n_o - k_o$ erasures. Hence, we can decode all error patterns with up to $n_o - k_o$ erasures in the outer codeword, that is, $n_o - k_o$ codewords of the inner code with two errors. Additionally, the inner codes can correct all single errors in the remaining k_o columns of the codeword matrix. Consequently, at least $2(n_o - k_o) + 1$ channel errors and up to $2(n_o - k_o) + k_o = n - k$ of Mannheim weight one are correctable. This proves the following proposition.

Proposition 2. *The product code with outer RS codes $\mathcal{C}_o(n_o, k_o, d_o)$ and inner codes $\mathcal{C}_i(2, 1, 4)$ over $\mathcal{G}_p$ has length $n = 2n_o$, dimension $k = k_o$, and minimum Mannheim distance $d = 4(n_o - k_o + 1)$, where error and erasure decoding can correct any error pattern with $t = n - 2k + 1$ errors of Mannheim weight one.*

Due to the rate of the inner codes, this construction is limited to code rates $R = k/n \leq 1/2$. For $n - 3k \geq 2$, the proposed product codes can correct more errors than an MDS code, that is, $t \geq (n-k)/2$. Hence, the proposed construction is favorable for low code rates. We illustrate this in the following example.

Example 2. *We consider a product code $\mathcal{C}(272, 55, 328)$ for $p = 137$ with the outer RS code $\mathcal{C}_o(136, 55, 81)$. The product code has length $n = 2n_o = 272$ and dimension $k = k_o = 55$. The minimum Mannheim distance is $d = 4(n_o - k_o + 1) = 328$. The error and erasure decoding procedure can correct at least $t = 163$ errors of Mannheim weight one which exceeds the MDS bound $(n-k)/2 = 108$ by 55 errors. This code contains more than 2^{390} codewords and the number of error patterns exceeds 2^{587}. The work factor for information-set decoding is $N_{ISD} = 2^{88}$ according to (2). A comparable RS code can be constructed over the field $GF(277)$, for example, the RS code $\mathcal{C}_o(272, 55, 218)$. This MDS code can correct $t = 108$ errors of arbitrary weight which corresponds to a work factor $N_{ISD} = 2^{46}$ for information-set decoding. Note that we can achieve higher work factors by using RS codes with larger dimension but this results in a larger public key.*

The parameters of some codes with work factors between 2^{88} and 2^{124} are summarized in Table 1. For comparison this table provides work factors of MDS codes with comparable code parameters.

Table 1. Parameters of some codes with work factors between 2^{88} and 2^{124}.

Proposed Codes Over Gaussian Integers					**MDS Codes**				
p	n	k	t	N_{ISD}	p	n	k	t	N_{ISD}
137	272	55	163	2^{88}	277	272	55	109	2^{46}
157	312	63	187	2^{101}	313	312	63	124	2^{53}
173	344	69	207	2^{111}	347	344	69	137	2^{58}
193	384	77	231	2^{124}	389	384	77	153	2^{65}

4. Erasure Only Decoding of RS Codes

The decoding of the RS codes can be simplified due to the fact that we require only erasure decoding. In this section, we discuss this decoding procedure in more detail. The decoding of RS codes typically consists of four steps: syndrome calculation, solving the key-equation, Chien search, and the Forney algorithm [24,28,29]. For instance, the Berlekamp-Massey algorithm (BMA) can be used for solving the key-equation which results in the error-location polynomial. The Chien search determines the roots of the error-location polynomial which indicate the error positions. Finally, the Forney algorithm calculates the error values. With the proposed code construction, we can avoid the BMA and Chien search for the algebraic decoding.

For decoding the proposed product code we first decode the n_o inner OMEC codes. We calculate the n_o syndrome values. For the error correction, we use a look-up table for the non-zero syndrome values. The table stores the error position and error value for each syndrome resulting from a single error of Mannheim weight one. For these values the errors can be corrected by subtracting the stored error values from the received vector. Note, that the proposed OMEC code of length two is able to detect any error of weight two and therefore no decoding error can happen. Instead an erasure is declared and the erasure location is stored. This decoding of the OMEC codes can be performed in linear time since only two field multiplications and one field addition are required per syndrome value. Additionally, one table look-up and at most one field subtraction is required for each non-zero syndrome.

Afterward, the n_o symbols of the outer RS code are the information symbols of the OMEC codes and can be used to determine the received symbols $r_{\mathrm{RS}}(x) = r_0 + r_1 x + \ldots + r_{n_o-1} x^{n_o-1}$ of the RS code. These received symbols only have errors in the positions where the OMEC decoders declare erasures. Hence, the error-location polynomial can be calculated from the erasure positions as

$$\Lambda(x) = \prod_{i=1}^{\nu} (1 - x X_i), \tag{12}$$

where ν is the number of erasures and $\Lambda(x)$ has roots at $X_1^{-1}, \ldots, X_\nu^{-1}$ with $X_i = \alpha^{j_i}$. The values j_i for $i = 1, \ldots, \nu$ are the erasure positions. Hence, neither the BMA nor the Chien search are required to determine the error positions.

However, we need the Forney algorithm to determine the error values. For the Forney algorithm, we first calculate the syndrome polynomial $S(x) = s_0 + s_1 x + \ldots + s_{n_o-k-1} x^{n_o-k-1}$ with the syndrome values $s_i = r_{\mathrm{RS}}(\alpha^{i+1})$. Next, the error-evaluator polynomial $\Omega(x)$ can be computed using the key-equation

$$\Omega(x) = S(x)\Lambda(x) \bmod x^{n_o-k}. \tag{13}$$

Finally, the error values are calculated as

$$e_i = -\frac{\Omega\left(X_i^{-1}\right)}{\Lambda'\left(X_i^{-1}\right)}, \tag{14}$$

where $\Lambda'(x)$ is the derivative of $\Lambda(x)$.

Consequently, the erasure only decoding of the outer RS code requires the syndrome calculation and the Forney algorithm but omits the BMA and the Chien search. This reduces the overall decoding complexity significantly because the BMA typically dominates the computational complexity. Consider for instance the RS decoder architectures for error and erasure decoding reported in [30,31]. In [30], the BMA requires 84% of the total logic of the decoder for an RS code of length $n = 508$, whereas the syndrome calculation and the Forney algorithm need only 11%. Similarly, in [31] a decoder for RS codes of length $n = 334$ is considered. The BMA occupies 51%, the syndrome calculation 14%, and the Forney algorithm 14% of the area for logic, respectively.

The syndrome calculation and the Forney algorithm have a complexity of order $O(n^2)$. Hence, the complexity order of the decryption is not increased by the decoding of the proposed codes since the matrix operations required for the McEliece system have complexity of order $O(n^2)$.

5. Decoding beyond Half the Minimum Distance

In Section 3 we have shown that the proposed decoding algorithm is not limited to bounded minimum distance decoding. Hence, it is possible to increase the number of errors and the work factor by allowing a certain failure probability for the decryption. Such a failure probability is inherent in all McEliece systems that decode beyond the guaranteed error correction capability of the code, for example, systems based on LDPC codes [8–11]. However, there is an important difference with the proposed coding scheme. A decoding error with LDPC codes results typically in an erroneous message. The proposed decoding approach can fail, when the number of errors exceeds the error-correcting capability $t = n - 2k + 1$. Yet such a failure can always be detected since it implies that the number of erasures for the outer code exceeds $n_o - k_o$ and the number of erasures is known after the inner decoding stage.

In this section, we present results for the decoding beyond half the minimum distance. We present numerical results for the one Mannheim error channel. The one Mannheim error channel was introduced in [23] as an approximation to the additive white Gaussian noise channel. The numerical results demonstrate that the proposed decoding can correct many error patterns where the number of errors exceeds $t = n - 2k + 1$. We show that the work factor for information-set decoding can be increased by exploiting this decoding beyond half the minimum distance.

The one Mannheim error channel is a discrete, symmetric, and memory-less channel, which considers only errors of Mannheim weight one. This channel model is defined by

$$\mathbf{r} = \mathbf{v} + \mathbf{e} \bmod \pi, \tag{15}$$

where addition is performed element-wise and modulo π. The vector $\mathbf{v}$ denotes the transmitted codeword with $v_i \in \mathcal{G}_p$ and $\mathbf{r}$ is the received vector. The error vector $\mathbf{e}$ contains elements $e_i \in \{0, \pm 1, \pm \mathrm{i}\}$. Errors (non-zero values e_i) occur independently with probability ϵ, where all error symbols $\{\pm 1, \pm \mathrm{i}\}$ are equally likely.

We assume that bounded minimum distance (BMD) decoding fails when the actual number of error exceeds the error-correcting capability $t = n - 2k + 1$. This error probability is

$$P_{BMD} = \sum_{i=t+1}^{n} \epsilon^i (1-\epsilon)^{n-i} \binom{n}{i}. \tag{16}$$

Similarity, we can determine the error probability P_F of a decoding failure with the proposed decoding. An erasure in the decoding of an inner code occurs with probability ϵ^2, that is, when both received symbols are in error. The outer decoding fails when the number of erasures exceeds $n_o - k_o$ which happens with probability

$$P_F = \sum_{i=n_o-k_o+1}^{n_o} \epsilon^{2i}(1-\epsilon^2)^{n_o-i}\binom{n_o}{i}. \tag{17}$$

Figure 1 depicts the probability of a decoding failure with BMD decoding and the proposed decoding algorithm for the one Mannheim error channel with error probability ϵ, where we consider the code from Example 2. The solid and dashed lines are calculated according to (16) and (17), whereas the markers depict simulation results. These results demonstrate that the proposed decoding achieves a significant performance gain compared with BMD decoding.

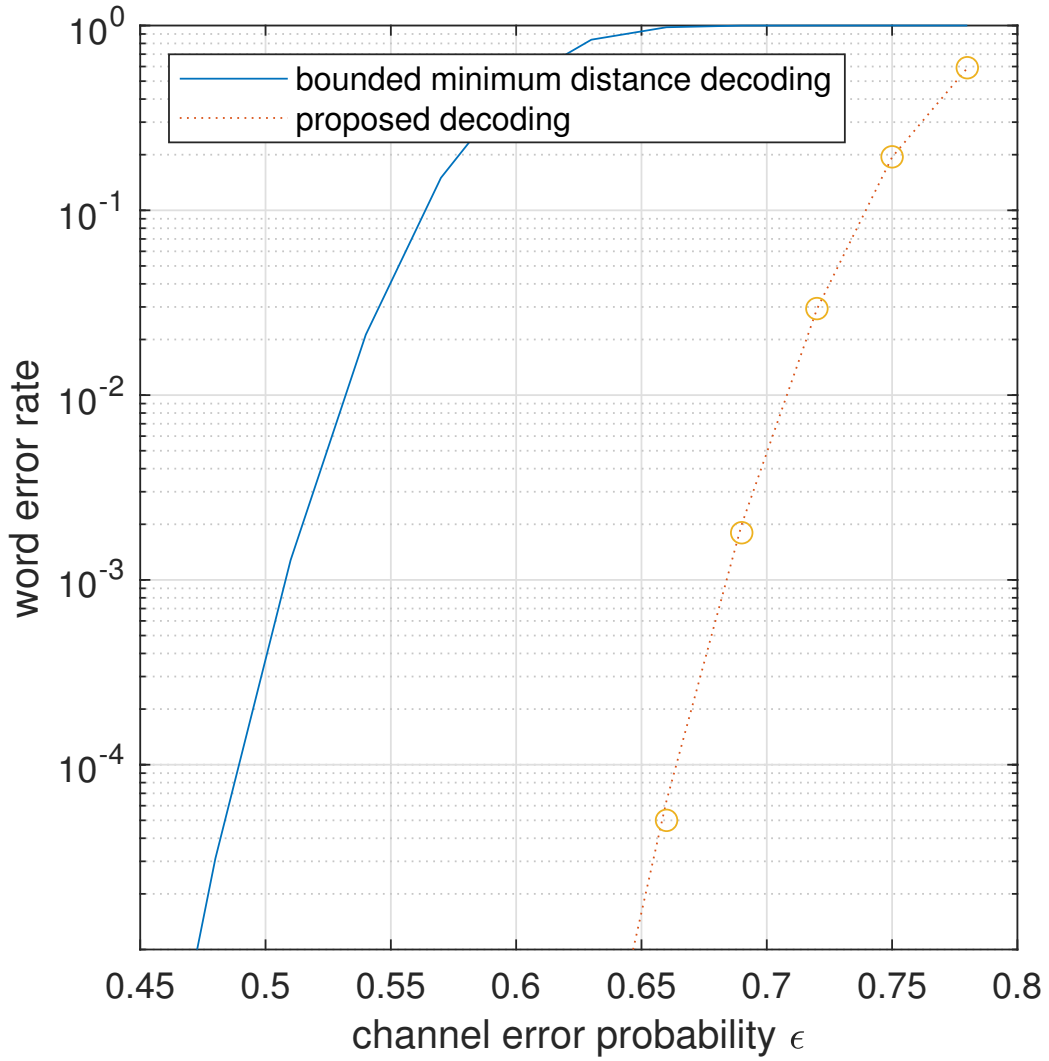

Figure 1. Probability of a decoding failure with bounded minimum distance (BMD) decoding and the proposed decoding algorithm for the one Mannheim error channel with error probability ϵ (code from Example 2).

Figure 2 also depicts results for the code from Example 2. Now, the number of errors is fixed and only the error positions and error values are chosen randomly. We observe that the number of errors can be much higher than the guaranteed error correction capability $t = 168$. For instance with $t = 199$ errors, we achieve a failure probability $P_F = 10^{-4}$ which

might be acceptable. The increased number of errors also increases the work factor for ISD from 2^{88} with BMD decoding to 2^{138} with $t = 199$ channel errors.

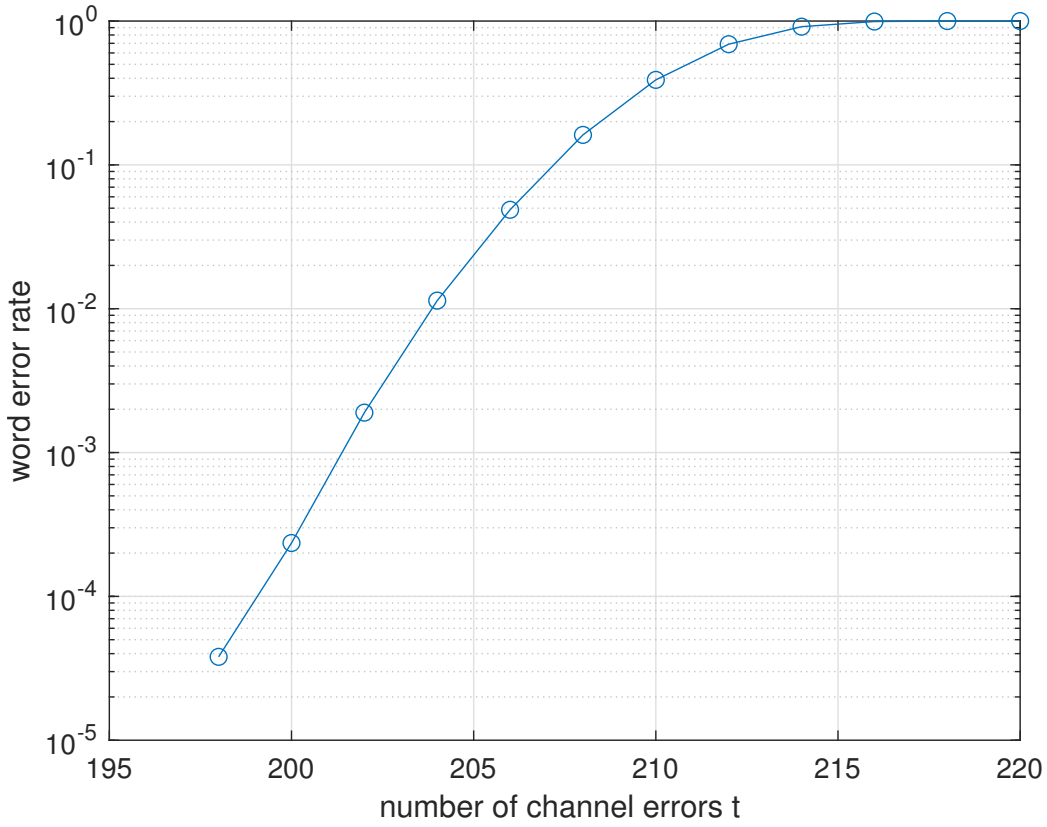

Figure 2. Probability of a decoding failure versus the number of errors with the proposed decoding algorithm (code from Example 2).

6. Capacity of the One Mannheim Error Channel

In the previous sections, we have shown that a code over Gaussian integers can correct up to $n - k$ errors of Mannheim weight one. Note that for $t > n - k$ there exist no error free information set. In this section, we show that $t > n - k$ is attainable with capacity achieving codes, that is, we consider the decoding problem from an information theoretic point of view. We investigate the one Mannheim error channel model and discuss its channel capacity.

The channel capacity C is the supremum of all achievable code rates. We calculate the channel capacity in bits per transmitted symbol.

Proposition 3. *The channel capacity C of the one Mannheim error channel with transmitted symbols $v_i \in \mathcal{G}_p$ is*

$$C = \log_2(p) + (1-\epsilon) \cdot \log_2(1-\epsilon) + \epsilon \cdot \log_2\left(\frac{\epsilon}{4}\right). \tag{18}$$

Proof. The one Mannheim error channel is a discrete memory-less channel which can be characterized by a transition matrix that contains all transmission probabilities from an input symbol $\mathcal{V}$ to the channel output $\mathcal{R}$ (see Figure 3). For the one Mannheim error

channel, we have $\mathcal{V} = \mathcal{R} = \mathcal{G}_p$. Errors (non-zero values e_i) occur independently with probability ϵ, where all error symbols $\{\pm 1, \pm \mathrm{i}\}$ are equally likely, that is,

$$P(e_i = 0) = 1 - \epsilon \tag{19}$$

$$P(e_i = 1) = P(e_i = -1) = P(e_i = \mathrm{i}) = P(e_i = -\mathrm{i}) = \frac{\epsilon}{4}. \tag{20}$$

Hence, each row of the transition matrix contains the non-zero elements $1 - \epsilon, \frac{\epsilon}{4}, \frac{\epsilon}{4}, \frac{\epsilon}{4}, \frac{\epsilon}{4}$ and all other elements are zero. All rows of the transition matrix are permutations of each other and all columns are permutations of each other. Hence, the channel is symmetric. The capacity of a symmetric discrete memory-less channel is [32]

$$C = \log_2(|\mathcal{R}|) - H(\mathbf{P}) \tag{21}$$

where $|\mathcal{R}| = p$ denotes the cardinality of the output alphabet and $H(\mathbf{P})$ is the entropy of a row $\mathbf{P}$ of the transition matrix. We have

$$H(\mathbf{P}) = -(1 - \epsilon)\log_2(1 - \epsilon) - \epsilon \cdot \log_2\left(\frac{\epsilon}{4}\right) \tag{22}$$

for the one Mannheim error channel. Hence, we obtain Equation (18). □

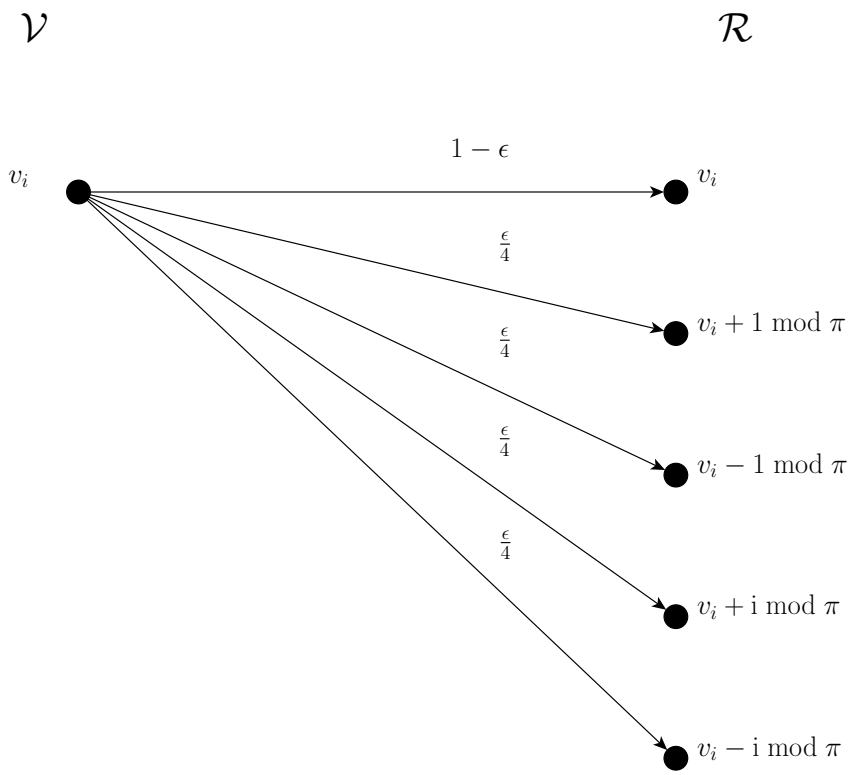

Figure 3. Channel model for the one Mannheim error channel.

Figure 4 shows two examples for the channel capacity as a function of the symbol error probability ϵ for the field sizes $p = 41$ and $p = 89$. In this figure, we have plotted the normalized capacity $C/\log_2(p)$. The normalized channel capacity satisfies the inequality $C \geq 1 - \log_p(5)$, where the minimum occurs for $\epsilon = 0.8$ when all values $e_i \in \{0, \pm 1, \pm \mathrm{i}\}$ are equally likely. The expected number of errors is $t = \epsilon n$. The expected number of errors t exceeds $n - k = n(1 - R)$ for $R > 1 - \epsilon$. Hence, we have plotted the line $1 - \epsilon$ in both figures. For $t > n - k$ there exist no error free information sets. Figure 4 shows that this condition is attainable with capacity achieving codes. We observe from Figure 4 that $t > n - k$ is attainable for $R < 0.76$ ($p = 41$) and $R < 0.88$ ($p = 89$), respectively.

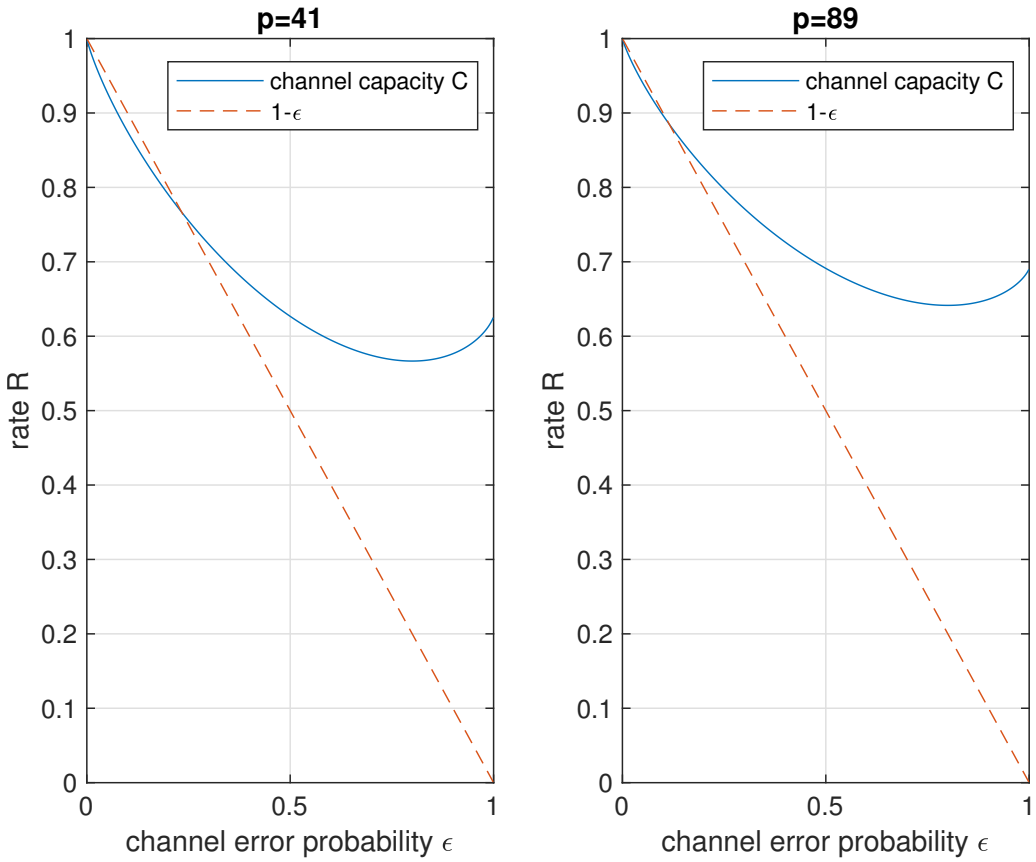

Figure 4. Channel capacity for the one Mannheim error channel for p = 41 and p = 89.

7. Conclusions

In this work, we have proposed q-ary codes over Gaussian integers for the McEliece system. In particular, we have proposed codes based on a product code construction with outer RS and inner OMEC codes. These codes can be decoded with a low complexity decoding algorithm based on erasure only decoding of RS codes. For the one Mannheim error channel, these codes achieve a higher error correction capability than maximum distance separable codes with bounded minimum distance decoding. This improves the work factor regarding decoding attacks based on information-set decoding. An analysis of the security against other attacks is subject to future work, such as the attacks proposed in [33,34].

The proposed decoding algorithm is not limited to bounded minimum distance decoding. We have shown that some error patterns with up to $n - k$ errors of Mannheim weight one can be corrected. Hence, it is possible to increase the number of errors and the work factor by allowing a certain failure probability for the decryption. Such a failure probability is inherent in all McEliece systems that decode beyond the guaranteed error correction capability of the code, for example, systems based on LDPC codes [8–11].

Furthermore, we have investigated the channel capacity of one Mannheim error channel and have discussed its relation to the McEliece system. These results demonstrate that codes are attainable where the expected number of errors t exceeds the number of redundancy symbols $n - k$ which prevents error free information sets.

On the other hand, the proposed codes have some limitations. Codes over Gaussian integers can only be constructed for primes of the form $p \equiv 1 \bmod 4$. A generalization of the construction to codes over Eisenstein integers should be possible [35]. This would enable similar codes for primes of the form $p \equiv 1 \bmod 6$. Moreover, the code design is limited to codes of rates $R = k/n < 1/2$. In comparison with MDS codes, these codes are favorable for rates $R < 1/3$ only. To construct good codes with higher rates, the short inner codes have to be replaced. Further improvements could be achieved by using generalized concatenated codes instead of the product code construction [20,28].

Author Contributions: The research for this article was exclusively undertaken by J.F. and J.-P.T. Conceptualization and investigation, J.F. and J.-P.T.; writing—review and editing, J.F. and J.-P.T.; writing—original draft preparation, J.F.; supervision, project administration, and funding acquisition J.F. All authors have read and agreed to the published version of the manuscript.

Funding: The German Federal Ministry of Research and Education (BMBF) supported the research for this article (16ES1045) as part of the PENTA project 17013 XSR-FMC.

Data Availability Statement: The study did not report any data.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134. [CrossRef]
2. McEliece, R. A public-key cryptosystem based on algebraic coding theory. *DSN Prog. Rep.* **1978**, *42–44*, 114–116.
3. Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Kelsey, J.; Liu, Y.K.; Miller, C.; Moody, D.; Peralta, R.; et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*; Nistir 8309; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
4. Berlekamp, E.; McEliece, R.; van Tilborg, H. On the inherent intractability of certain coding problems. *IEEE Trans. Inf. Theory* **1978**, *24*, 384–386. [CrossRef]
5. Wieschebrink, C. Two NP-complete problems in coding theory with an application in code based cryptography. In Proceedings of the 2006 IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006; pp. 1733–1737. [CrossRef]
6. Berger, T.P.; Cayrel, P.L.; Gaborit, P.; Otmani, A. Reducing key length of the McEliece cryptosystem. In *Progress in Cryptology—AFRICACRYPT*; Preneel, B., Ed.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 77–97.
7. Le Van, T.; Hoan, P.K. McEliece cryptosystem based identification and signature scheme using chained BCH codes. In Proceedings of the International Conference on Communications, Management and Telecommunications (ComManTel), DaNang, Vietnam, 28–30 December 2015; pp. 122–127. [CrossRef]
8. Monico, C.; Rosenthal, J.; Shokrollahi, A. Using low density parity check codes in the McEliece cryptosystem. In Proceedings of the 2000 IEEE International Symposium on Information Theory, Sorrento, Italy, 25–30 June 2000; p. 215. [CrossRef]
9. Shooshtari, M.K.; Ahmadian, M.; Payandeh, A. Improving the security of McEliece-like public key cryptosystem based on LDPC codes. In Proceedings of the 11th International Conference on Advanced Communication Technology, Gangwon-Do, Korea, 15–18 February 2009; Volume 2, pp. 1050–1053.
10. Baldi, M.; Bianchi, M.; Maturo, N.; Chiaraluce, F. Improving the efficiency of the LDPC code-based McEliece cryptosystem through irregular codes. In Proceedings of the IEEE Symposium on Computers and Communications (ISCC), Split, Croatia, 7–10 July 2013; pp. 000197–000202. [CrossRef]
11. Moufek, H.; Guenda, K.; Gulliver, T.A. A New Variant of the McEliece Cryptosystem Based on QC-LDPC and QC-MDPC Codes. *IEEE Commun. Lett.* **2017**, *21*, 714–717. [CrossRef]
12. Hooshmand, R.; Shooshtari, M.K.; Eghlidos, T.; Aref, M.R. Reducing the key length of McEliece cryptosystem using polar codes. In Proceedings of the 11th International ISC Conference on Information Security and Cryptology, Tehran, Iran, 3–4 September 2014; pp. 104–108. [CrossRef]
13. Lee, P.J.; Brickell, E.F. An observation on the security of McEliece's public-key cryptosystem. In *Advances in Cryptology—EUROCRYPT'88*; Barstow, D., Brauer, W., Brinch Hansen, P., Gries, D., Luckham, D., Moler, C., Pnueli, A., Seegmüller, G., Stoer, J., Wirth, N., et al., Eds.; Springer: Berlin/Heidelberg, Germany, 1988; pp. 275–280.

14. Stern, J. A method for finding codewords of small weight. In *Coding Theory and Applications*; Cohen, G., Wolfmann, J., Eds.; Springer: Berlin/Heidelberg, Germany, 1989; pp. 106–113.
15. May, A.; Meurer, A.; Thomae, E. Decoding random linear codes in $\mathcal{O}(2^{0.054n})$. In *Advances in Cryptology—ASIACRYPT 2011*; Lee, D.H., Wang, X., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 107–124.
16. Bernstein, D.J.; Lange, T.; Peters, C. Attacking and defending the McEliece cryptosystem. In *Post-Quantum Cryptography*; Buchmann, J., Ding, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 31–46.
17. Huber, K. Codes over Gaussian integers. *IEEE Trans. Inf. Theory* **1994**, *40*, 207–216. [CrossRef]
18. Rifa, J. Groups of complex integers used as QAM signals. *IEEE Trans. Inf. Theory* **1995**, *41*, 1512–1517. [CrossRef]
19. Dong, X.; Soh, C.B.; Gunawan, E.; Tang, L. Groups of algebraic integers used for coding QAM signals. *IEEE Trans. Inf. Theory* **1998**, *44*, 1848–1860. [CrossRef]
20. Freudenberger, J.; Ghaboussi, F.; Shavgulidze, S. New Coding Techniques for Codes over Gaussian Integers. *IEEE Trans. Commun.* **2013**, *61*, 3114–3124. [CrossRef]
21. Juraphanthong, W.; Jitprapaikulsarn, S. An asymmetric cryptography using Gaussian integers. *Eng. Appl. Sci. Res.* **2020**, *47*, 153–160.
22. Freudenberger, J.; Shavgulidze, S. New Four-Dimensional Signal Constellations From Lipschitz Integers for Transmission Over the Gaussian Channel. *IEEE Trans. Commun.* **2015**, *63*, 2420–2427. [CrossRef]
23. Rohweder, D.; Freudenberger, J.; Shavgulidze, S. Low-density parity-check codes over finite Gaussian integer fields. In Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT), Vail, CO, USA, 17–22 June 2018; pp. 481–485. [CrossRef]
24. Neubauer, A.; Freudenberger, J.; Kühn, V. *Coding Theory: Algorithms, Architectures and Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2007.
25. Ivanov, F.; Kabatiansky, G.; Krouk, E.; Rumenko, N. A new code-based cryptosystem. In Proceedings of the 8th International Workshop on Code-Based Cryptography, CBCrypto, Zagreb, Croatia, 9–10 May 2020; pp. 41–49.
26. Martinez, C.; Beivide, R.; Gabidulin, E. Perfect Codes for Metrics Induced by Circulant Graphs. *IEEE Trans. Inf. Theory* **2007**, *53*, 3042–3052. [CrossRef]
27. Safieh, M.; Freudenberger, J. Montgomery Reduction for Gaussian Integers. *Cryptography* **2021**, *5*, 6. [CrossRef]
28. Bossert, M. *Channel Coding for Telecommunications*; Wiley: Hoboken, NJ, USA, 1999.
29. Jiang, Y. *A Practical Guide to Error-Control Coding Using Matlab*; Artech House: Boston, MA, USA 2010.
30. Spinner, J.; Freudenberger, J. Decoder Architecture for Generalized Concatenated Codes. *IET Circuits Devices Syst.* **2015**, *9*, 328–335. [CrossRef]
31. Spinner, J.; Rohweder, D.; Freudenberger, J. Soft input decoder for high-rate generalised concatenated codes. *IET Circuits Devices Syst.* **2018**, *12*, 432–438. [CrossRef]
32. Gallager, R.G. *Information Theory and Reliable Communication*; John Wiley & Sons, Inc.: New York, NY, USA, 1968.
33. Sidelnikov, V.M.; Shestakov, S.O. On insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discret. Math. Appl.* **1992**, *2*, 439–444. [CrossRef]
34. Fabsic, T.; Hromada, V.; Stankovski, P.; Zajac, P.; Guo, Q.; Johansson, T. A reaction attack on the QC-LDPC McEliece cryptosystem. In Proceedings of the Post-Quantum Cryptography—8th International Workshop (PQCrypto), Utrecht, The Netherlands, 26–28 June 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 51–68. [CrossRef]
35. Huber, K. Codes over Eisenstein-Jacobi Integers. *Contemp. Math.* **1994**, 165–179.