Received 26 August 2022; accepted 10 September 2022. Date of publication 13 September 2022; date of current version 26 September 2022.

Digital Object Identifier 10.1109/OJCOMS.2022.3206395

Code-Based Cryptography With Generalized Concatenated Codes for Restricted Error Values

JOHANN-PHILIPP THIERS (Graduate Student Member, IEEE), AND JÜRGEN FREUDENBERGER (Member, IEEE)

Institute for System Dynamics, HTWG Konstanz, University of Applied Sciences, 78462 Konstanz, Germany

CORRESPONDING AUTHOR: J. FREUDENBERGER (e-mail: jfreuden@htwg-konstanz.de)

This work was supported by the German Federal Ministry of Research and Education (BMBF) as part of the PENTA Project 17013 XSR-FMC under Grant 16ES1045, and in part by the Hyperstone GmbH.

ABSTRACT Code-based cryptosystems are promising candidates for post-quantum cryptography. Recently, generalized concatenated codes over Gaussian and Eisenstein integers were proposed for those systems. For a channel model with errors of restricted weight, those q-ary codes lead to high error correction capabilities. Hence, these codes achieve high work factors for information set decoding attacks. In this work, we adapt this concept to codes for the weight-one error channel, i.e., a binary channel model where at most one bit-error occurs in each block of m bits. We also propose a low complexity decoding algorithm for the proposed codes. Compared to codes over Gaussian and Eisenstein integers, these codes achieve higher minimum Hamming distances for the dual codes of the inner component codes. This property increases the work factor for a structural attack on concatenated codes leading to higher overall security. For comparable security, the key size for the proposed code construction is significantly smaller than for the classic McEliece scheme based on Goppa codes.

INDEX TERMS Code-based cryptography, generalized concatenated codes, McEliece cryptosystem, public-key cryptography, restricted error values.

I. INTRODUCTION

PUBLIC-KEY cryptographic algorithms are vital for today's cyber security. They are required for key exchange protocols and digital signatures, as in communication standards like Transport Layer Security (TLS), S/MIME, and PGP. Public-key cryptographic algorithms are based on trapdoor functions which are easy to compute in one direction but are difficult to invert. The idea is that the legitimate receiver uses a private key to solve the relatively easy calculation, while an attacker has to solve a sufficiently hard problem.

The most-common public-key cryptosystems nowadays are the Rivest-Shamir-Adleman algorithm and the elliptic curve cryptography, which are based on the intractability of integer factorization and the elliptic curve discrete logarithm problem, respectively. Both problems can be solved in polynomial time using the quantum algorithms presented in [1], [2]. Hence, large-scale quantum computers threaten the security of today's public-key cryptosystems.

Many post-quantum secure public-key cryptographic algorithms were proposed to cope with this issue. One of them is code-based cryptography. Code-based cryptography is based on the problem of decoding random linear codes, which is known to be NP-hard [3]. The most common code-based cryptosystems are the McEliece system [4] and the Niederreiter system [5], which are equivalent regarding their security. For the McEliece system, the public key is a scrambled version of a generator matrix, while the original generator matrix is part of the private key. The sender encrypts a message by encoding it with the public generator matrix and adding a random but correctable error vector. The legitimate receiver knows the original code and therefore can decode this cryptogram efficiently, while an attacker has to decode the cryptogram in a seemingly random linear code.

The best-known attacks on the McEliece and Niederreiter system are based on information set decoding (ISD) [6]. Such attacks were proposed in [7], [8], [9], [10]. Those attacks

search for an error-free information set, which is then used for re-encoding.

The original proposal of the McEliece system was based on binary Goppa codes. But many other code classes were proposed since then, e.g., generalized Reed-Solomon (GRS) codes, Reed-Muller codes, or quasi-cyclic moderate density parity check (QC-MDPC) codes [5], [11], [12]. Structural attacks exists for many of those code classes. These attacks exploit the structure of the code to compute the private generator matrix from the public key [13], [14]. The original McEliece system with binary Goppa codes remains unbroken but requires very large public keys.

Lately, code-based cryptography with restricted error values was investigated [15], [16], [17], [18], [19], [20], [21], [22]. For example, in [17], [19] the hardness of ISD and computational syndrome decoding in the Lee metric were considered. In [15], [20] the applicability of LDPC codes in the Lee metric were analyzed. LDPC codes enable code-based cryptosystems with very short public keys. However, LDPC codes have a non-zero decoding failure rate (DFR) because they are decoded beyond the guaranteed error correction capability. Depending on the application, this may be undesirable. Furthermore, the complexity of LDPC decoders [23] is significantly higher than for comparable decoders for binary Goppa codes [24].

In [22], concatenated codes with inner codes over Gaussian integer fields and outer Reed-Solomon (RS) codes were proposed for the McEliece system. These codes have a high error correction capability if the error values are restricted to Mannheim weight one. For this one-Mannheim error channel, the error correction capability of the concatenated codes exceeds the capability of maximum distance separable (MDS) codes. The complexity for ISD attacks only depends on the number of errors but not on their weight. Hence, the proposed concatenated codes allowed for very high work factors for ISD-based attacks.

On the other hand, in [25] an attack on concatenated codes was proposed, which together with the attack on GRS codes [13] can retrieve the private parity check matrix. In [26], a generalized concatenated (GC) code construction with inner OMEC codes over Gaussian integers and outer RS codes was proposed for the one-Mannheim error channel. GC codes are more robust against the structural attack from [25] than ordinary concatenated codes [27].

In this work, we introduce a new channel model with restricted error values. This weight-one error channel is a binary channel model where at most one bit-error occurs in each block of m bits. Alternatively, this channel can be interpreted as a memoryless channel, where the input and the output symbols are from the binary extension field $\mathbb{F}_{2^m}$ and the additive error symbols are limited to the field elements of Hamming weight one. This channel model is similar to the channels for Gaussian and Eisenstein integers which use complex-valued isomorphic representations of prime fields $\mathbb{F}_p$ and the error symbols are the roots of unity [21], [26], [28]. Likewise, restrictions of the Lee weight of the error symbols are considered in [15], [16], [17], [18], [19], [29]. In this work, we propose a slightly different channel model, since we do not limit the value of the errors in the base field, but the number of errors in a vector of base field elements, i.e., the vector representation of an extension field element. We analyze the capacity of this weight-one error channel over $\mathbb{F}_{2^m}$ and discuss its application in code based cryptography.

Furthermore, we propose a GC code construction for this weight-one error channel. For the outer codes, we propose RS codes as in [26], which allows for a low complexity erasure decoding. The inner codes are binary Bose-Chaudhuri-Hocquenghem (BCH) codes. While the proposed code construction has a lower work factor against ISD attacks than codes over Gaussian integers, the work factor for the structural attack can be significantly increased leading to higher overall security. This results from the fact that the binary inner codes have dual codes with larger minimum Hamming distance which improves the robustness against structural attacks [27].

We compare the proposed coding scheme with other proposals for the McEliece system [30], [31], [32] in terms of their public key sizes for the same security category in the current NIST standardization process [33]. It is shown in [34] that the GC codes also have advantages concerning the size and speed of hardware implementations of the decoder.

This work is structured as follows. In Section II, we discuss the McEliece cryptosystem, ordinary concatenated codes, and the corresponding structural attack. In Section III, we propose the weight-one error channel and analyze its capacity. The proposed code construction and decoding algorithm are discussed in Section IV, where also some exemplary codes are given. In Section V, we consider the performance for decoding beyond guaranteed error correction capability. We compare our work with other code-based cryptosystems in Section VI and finally conclude this work in Section VII.

II. PRELIMINARIES

In this section, we briefly review the McEliece cryptosystem and the corresponding attacks.

A. THE MCELIECE CRYPTOSYSTEM

Consider a linear code $\mathcal{C}(q; n, k, d)$ of length n over the q-ary field $\mathbb{F}_q$. The code has dimension k, minimum distance d, and a $k \times n$ generator matrix $\mathbf{G}$. The code should also enable an efficient decoding algorithm $\phi(\cdot)$. The public key consists of the error correction capability t and a scrambled version of the generator matrix $\mathbf{G}' = \mathbf{SGP}$, where $\mathbf{S}$ is a random non-singular $k \times k$-matrix and $\mathbf{P}$ is a random $n \times n$ permutation matrix. The private key consists of the matrices $\mathbf{S}$, $\mathbf{G}$, and $\mathbf{P}$.

For encrypting a message $\boldsymbol{u} \in \mathbb{F}_q^k$, the sender computes

$$\boldsymbol{c} = \boldsymbol{u}\mathbf{G}' + \boldsymbol{e}, \tag{1}$$

where $\boldsymbol{e} \in \mathbb{F}_q^n$ is a random error vector of Hamming weight at most t. For decryption, the receiver first inverts the permutation

$$\boldsymbol{v} = \boldsymbol{c}\mathbf{P}^{-1} = \boldsymbol{u}\mathbf{S}\mathbf{G} + \boldsymbol{e}\mathbf{P}^{-1}, \tag{2}$$

and then decodes $\boldsymbol{v}$ as $\boldsymbol{u}\mathbf{S} = \phi(\boldsymbol{v})$. Note that the permutation of the error vector does not change its weight, hence the decoding algorithm is able to correct t errors. Finally, the receiver utilizes the inverse scrambling matrix $\mathbf{S}^{-1}$ to obtain the message $\boldsymbol{u}$. Without knowledge of the private key, an attacker needs to decode t errors in a seemingly random linear code which is NP-hard [3].

In [35], a conversion algorithm was proposed which allows omitting the scrambling and instead performs Gaussian elimination to have the public key generator matrix in systematic form. If applicable, this conversion reduces the key size, since only the last $n-k$ columns of the generator matrix need to be part of the public key.

B. INFORMATION SET DECODING ATTACKS

An equivalent problem to decoding t errors in a random linear code is the computational syndrome decoding (CSD) problem. Consider an $(n-k) \times n$ parity check matrix $\mathbf{H}$, a length $n-k$ syndrome vector $\boldsymbol{s}$, and the error weight t. The CSD problem is the problem of finding a length n error vector $\boldsymbol{e}$ such that $\boldsymbol{e}\mathbf{H}^T = \boldsymbol{s}$. With the knowledge of the public generator matrix $\mathbf{G}'$ and the ciphertext $\boldsymbol{c} = \boldsymbol{m}\mathbf{G}' + \boldsymbol{e}$ an attacker can calculate a parity check matrix $\mathbf{H}$ for $\mathbf{G}'$ and the syndrome $\boldsymbol{s} = \boldsymbol{c}\mathbf{H}^T = \boldsymbol{e}\mathbf{H}^T$. A solution $\boldsymbol{e}$ to the CSD problem results in the codeword $\boldsymbol{m}\mathbf{G}'$, which allows to calculate the message $\boldsymbol{m}$.

One of the best approaches to the CSD problem is based on information set decoding (ISD). Such attacks were proposed in [6], [7], [8], [9], [10] and were already considered in the original proposal of the McEliece system. In the following, we review the ISD algorithm according to Prange [6].

The basic idea is to test random permutations until a permutation is found that solves the CSD problem. For this search, an attacker picks a random $n \times n$ permutation matrix $\mathbf{P}$ and computes an $n-k \times n-k$ matrix $\mathbf{U}$ such that $\mathbf{H}' = \mathbf{U}\mathbf{H}\mathbf{P} = (\mathbf{I}_{n-k}, \widetilde{\mathbf{H}})$ is in systematic form. With the permuted error vector $\boldsymbol{e}' = \boldsymbol{e}\mathbf{P}$ and the scrambled syndrome $\boldsymbol{s}' = \boldsymbol{s}\mathbf{U}^T$, we have the correspondence

$$\boldsymbol{e}\mathbf{H}^T = \boldsymbol{s} \iff \boldsymbol{e}'\mathbf{H}'^T = \boldsymbol{s}', \tag{3}$$

leading to the equivalent CSD problem on $\mathbf{H}' = \mathbf{U}\mathbf{H}\mathbf{P}$, $\boldsymbol{s}' = \boldsymbol{s}\mathbf{U}^T$, and error weight t.

The desired permutation leads to a permuted error vector having all non-zeros symbols in the first $n-k$ positions. In this case, we have $\boldsymbol{e}' = \boldsymbol{e}\mathbf{P} = (\boldsymbol{s}', \mathbf{0}_k)$ due to the structure of $\mathbf{H}'$ with the identity matrix in the leftmost $n-k$ columns. Such a case can be detected using the weight of the scrambled syndrome $\boldsymbol{s}' = \boldsymbol{s}\mathbf{U}^T$. If all non-zero entries in the permuted error vector are in the first $n-k$ positions, the scrambled syndrome $\boldsymbol{s}'$ has Hamming weight t.

The probability of occurrence P_{ISD} of a successful permutation can be determined as [7]

$$P_{ISD} = \frac{\binom{n-k}{t}}{\binom{n}{t}}. \tag{4}$$

We measure the work factor of ISD in terms of the expected number of iterations until a successful permutation is found, i.e.,

$$N_{ISD} = \frac{1}{P_{ISD}} = \frac{\binom{n}{t}}{\binom{n-k}{t}}. \tag{5}$$

Note that this is only the expected number of iterations and neglects the complexity of each iteration. Hence, the actual complexity of Pranges algorithm is significantly higher.

Many optimizations to this basic approach were proposed [7], [8], [10], [36], [37] which lead to lower overall asymptotic complexity than the algorithm according to Prange [6]. In [38, Table 4] the complexity of such optimized attacks on the Classic McEliece system with the parameters proposed in [30] was investigated. All but one of the attacks show a higher complexity as computed by (5), since we only consider the only the number of iterations and ignore the costs per iteration. The only attack that shows a lower work factor is the method according to [10], denoted as MMT after the authors May, Meurer, and Thomae. On the other hand, this attack requires a memory of about 2^{78} bits for the category 1 Classic McEliece parameters.

Similarly, in [39], an optimized ISD attack on the Goppa-based McEliece with reduced parameters was implemented. The complexity exponent for this attack is slightly higher than the estimate using (5). For sake of simplicity, we only consider the estimate according to (5) for the security analysis of ISD based attacks.

C. STRUCTURAL ATTACK ON CONCATENATED CODES

Sendrier presented an attack on concatenated codes in [25]. This attack uses the code structure to reconstruct the private key. In the following, we will shortly review Sendrier's attack. Later on, we discuss its applicability for generalized concatenated (GC) codes [27].

Let us first introduce some definitions and notation according to [25]. An ordinary concatenated (OC) code is constructed of an outer code $\mathcal{A}(q^{k_B}; n_A, k_A, d_A)$ and an inner code $\mathcal{B}(q; n_B, k_B, d_B)$ [40]. The OC code is uniquely defined by the two codes and a mapping θ from $\mathbb{F}_{q^{k_B}}$ to $\mathcal{B}$ [25], i.e., the mapping

$$\Theta : \mathbb{F}_{q^{k_B}}^{n_A} \to \mathcal{B}^{n_A} \tag{6}$$

$$(a_1, \ldots, a_{n_A}) \to (\theta(a_1), \ldots, \theta(a_{n_A})). \tag{7}$$

The resulting OC code has $q^{k_B^{k_A}}$ codewords. Each codeword of the OC code consists of n_A codewords of the code $\mathcal{B}$, i.e., a codeword has $n_{OC} = n_A \cdot n_B$ q-ary symbols.

The support of a vector $\boldsymbol{v}$ is the set of indices of all non-zero elements and is denoted as $\mathrm{supp}(\boldsymbol{v})$. The support of a

set of vectors is the union of supports of all its elements. We denote by $\mathscr{P}(\mathcal{C})$ the set of all minimal support codewords, i.e., the set of all codewords $\boldsymbol{c} \in \mathcal{C}$ fulfilling

$$\nexists\, \boldsymbol{c}' \in \mathcal{C}\backslash\{\mathbf{0}, \boldsymbol{c}\} : \operatorname{supp}(\boldsymbol{c}') \subseteq \operatorname{supp}(\boldsymbol{c}). \tag{8}$$

The generator matrix of an OC code has the form

$$\mathbf{G}_{OC} = \begin{pmatrix} a_{1,1}\mathbf{G}_B & a_{1,2}\mathbf{G}_B & \cdots & a_{1,n_A}\mathbf{G}_B \\ a_{2,1}\mathbf{G}_B & a_{2,2}\mathbf{G}_B & \cdots & a_{2,n_A}\mathbf{G}_B \\ \vdots & \vdots & \ddots & \vdots \\ a_{k_A,1}\mathbf{G}_B & a_{k_A,2}\mathbf{G}_B & \cdots & a_{k_A,n_A}\mathbf{G}_B \end{pmatrix}, \tag{9}$$

where each $a_{i,j}$ is an element of $\mathbb{F}_q$ and $\mathbf{G}_B$ is the generator matrix of the inner code.

We consider only the first step of Sendrier's attack. In this step, an attacker tries to find the support of each inner block $a_{i,j}\mathbf{G}_B$. For this, we search for minimal support codewords of the dual code $\mathcal{C}_{OC}^{\perp}$ with minimum Hamming distance $d_B^{\perp}$, where $d_B^{\perp}$ and $d_A^{\perp}$ are the minimum Hamming distances of the dual codes of the inner and outer code, respectively. As shown in [41], each codeword $\boldsymbol{c} \in \mathscr{P}(\mathcal{C}_{OC}^{\perp})$ of Hamming weight less than $d_A^{\perp}$ has its support included in a single inner block. Hence, by finding such codewords the support of each inner block can be found. The public generator matrix $\mathbf{G}'$ can be reordered such that each inner block has its support in adjacent columns.

The problem of finding dual codewords with given weight is equivalent to the CSD problem [8] and is NP-complete [3]. One approach to find such codewords is to randomly generate test patterns of length n_{OC} and weight $d_B^{\perp}$. To check if such a test pattern is a codeword of the dual code, we can use the public generator matrix $\mathbf{G}'$ as parity check matrix of the dual code. We estimate the success probability P_{SA} of this method in the following proposition.

Proposition 1: Let $d_B^{\perp}$ be the minimum Hamming distance of the dual of the inner code and $W_{\mathcal{C}^{\perp}}(\cdot)$ its weight distribution. The probability P_{SA} that a randomly generated pattern of Hamming weight $d_B^{\perp}$ is a codeword, is

$$P_{SA} = \frac{n_A \cdot W_{C^{\perp}}\left(d_B^{\perp}\right)}{\binom{n_{OC}}{d_B^{\perp}} \cdot (q-1)^{d_B^{\perp}}}, \tag{10}$$

Proof: The number of codewords of Hamming weight $d_B^{\perp}$ is $n_A \cdot W_{C^{\perp}}(d_B^{\perp})$. The total number of $d_B^{\perp}$ non-zero positions out of n_{OC} is $\binom{n_{OC}}{d_B^{\perp}}$. Each non-zero position can take $q-1$ values, hence the number of such patterns is $\binom{n_{OC}}{d_B^{\perp}}(q-1)^{d_B^{\perp}}$. ∎

We use the average number of attempts until a successful pattern is found as the work factor N_{SA} for Sendrier's attack, i.e., $N_{SA} = P_{SA}^{-1}$. Note that the actual complexity of this attack is higher, since multiple such codewords are required, and even finding enough codewords only solves the first step. On the other hand, there are alternatives to the other steps [27], but not for the first one. Hence, we use this N_{SA} as an estimate for the complexity of this attack scenario.

III. THE WEIGHT-ONE ERROR CHANNEL

In [21], [22], [26], [42], channel models with restricted error weights were proposed for Gaussian and Eisenstein integers to increase the error correction capability and therefore the security against ISD attacks. In this work, we consider a similar approach by restricting the Hamming weight of m adjacent bits to weight one.

We investigate the weight-one error (WOE) channel over $\mathbb{F}_{2^m}$, which takes blocks of m bits as input and for each block introduces at most one bit error. This channel can be interpreted as a memoryless channel, where the input as well as the output symbols are from the binary extension field $\mathbb{F}_{2^m}$ and the additive error symbols are limited to the field elements of Hamming weight one. Given a symbol error probability ϵ, each error symbol is all-zero with probability $1-\epsilon$ and with probability ϵ one of the m possible error symbols of Hamming weight one occurs. All non-zero error symbols have the have the same probability ϵ/m of occurring. Next, we analyze the capacity of the WOE channel and discuss its application in code based cryptography.

Proposition 2: The capacity C of the weight-one error channel over $\mathbb{F}_{2^m}$ and error probability ϵ is

$$C = m + (1-\epsilon)\log_2(1-\epsilon) + \epsilon \cdot \log_2\left(\frac{\epsilon}{m}\right). \tag{11}$$

Proof: The capacity of a discrete symmetric memory-less channel is

$$C = \log_2(|\mathcal{R}|) - \mathrm{H}(\mathbf{P}), \tag{12}$$

where $|\mathcal{R}|$ is the cardinality of the output alphabet and $\mathrm{H}(\mathbf{P})$ is the entropy of a row of the transition matrix [43]. We interpret the channel with the output alphabet $\mathbb{F}_{2^m}$ of cardinality 2^m. Note, that in this case the channel is memory-less. Each row of the transition matrix has $m+1$ non-zero entries. One entry with value $1-\epsilon$ for the case of error-free transition and m entries with value $\frac{\epsilon}{m}$ corresponding to all possible m-bit vectors of Hamming weight one. Hence, the entropy is

$$\begin{aligned} \mathrm{H}(\mathbf{P}) &= -(1-\epsilon)\log_2(1-\epsilon) - m\left(\frac{\epsilon}{m} \cdot \log_2\left(\frac{\epsilon}{m}\right)\right) \\ &= -(1-\epsilon)\log_2(1-\epsilon) - \epsilon \cdot \log_2\left(\frac{\epsilon}{m}\right). \end{aligned} \tag{13}$$

From $|\mathcal{R}| = 2^m$, (12), and (13) follows (11). ∎

Figure 1 shows the maximum achievable code rate of the proposed channel model versus the channel error probability ϵ for two different binary extension fields. Note that code rates $R = k/n > 1-\epsilon$ are achievable, as shown by the dashed line in Figure 1. This corresponds to $t > n-k$ errors in a received vector of length n.

For the application in code-based cryptography, we use relatively short codes to achieve short public keys. With such short codes it is typically not possible to operate close to the channel capacity. However, as shown later on, the codes proposed in this work have a guaranteed error correction capability of $t = n-k$ and therefore are on the dashed line in Figure 1.

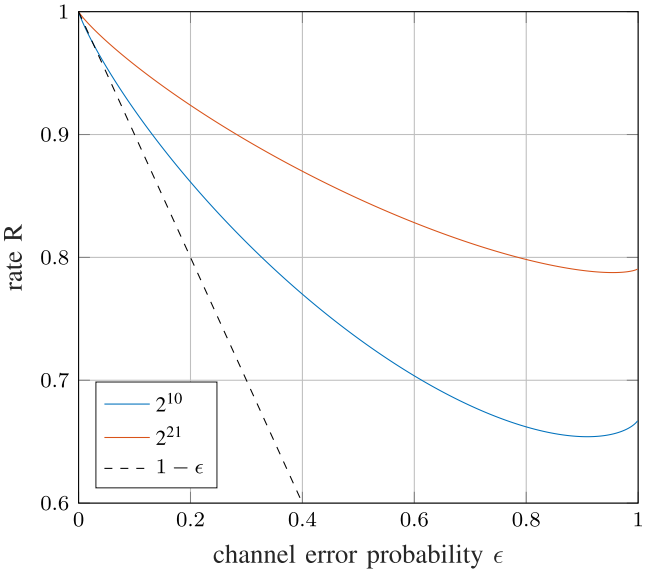

FIGURE 1. Capacity of the proposed channel model.

IV. GENERALIZED CONCATENATED CODE CONSTRUCTION

In this section, we introduce the proposed code construction as well as the decoding of those concatenated codes.

A. GENERALIZED CONCATENATED CODES

Generalized concatenated (GC) codes are a generalization of OC codes with different outer codes [44], [45]. A GC code is built from L inner codes $\mathcal{B}^{(i)}(q; n_B, k_B^{(i)}, d_B^{(i)})$, $i = 0, \ldots, L-1$ and L outer codes $\mathcal{A}^{(i)}(q; n_A, k_A^{(i)}, d_A^{(i)})$. Hence, the ordinary concatenated code is a special case of a GC code with $L = 1$. All outer codes have the same length but different dimensions and minimum distances. The inner codes $\mathcal{B}^{(i)}$ are nested, where nested means that a higher level code is a sub-code of its predecessor

$$\mathcal{B}^{(L-1)} \subset \mathcal{B}^{(L-2)} \subset \ldots \subset \mathcal{B}^{(0)} \tag{14}$$

The higher levels have inner codes with higher error correcting capabilities. The codeword is an $n_A \times n_B$-matrix over $\mathbb{F}_q$. Each column of the codeword matrix is the sum of the L codewords of the nested inner codes.

Figure 2 shows the encoding process of a GC code, where we consider only two outer codes $\mathcal{A}^{(0)}$ and $\mathcal{A}^{(1)}$. The information symbols are split into two vectors $\boldsymbol{u}_0 \in \mathbb{F}_q^{k_0}$ and $\boldsymbol{u}_1 \in \mathbb{F}_q^{k_1}$. These vectors are encoded to codewords of the two outer codes $\mathcal{A}^{(0)}$ and $\mathcal{A}^{(1)}$ which are then written to the first two rows of the codeword matrix. Afterward, each column of the codeword matrix is processed with the inner codes $\mathcal{B}^{(0)}$ and $\mathcal{B}^{(1)}$.

B. PROPOSED GC CODE CONSTRUCTION

In the following, we consider a GC code construction, which is optimized for the restriction of the WOE channel. We use outer codes over the extension field $\mathbb{F}_{2^m}$, corresponding to

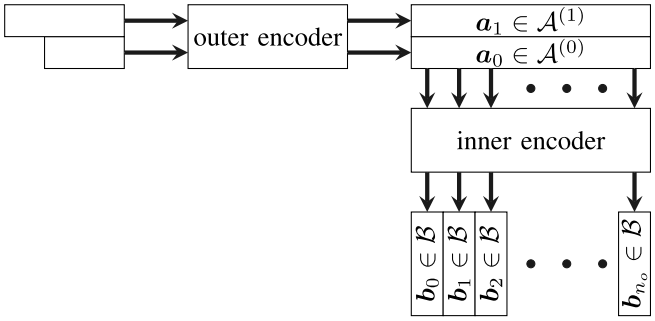

FIGURE 2. Schematic of the GCC encoding process.

the 2^m-ary channel. As inner codes, we consider L nested binary BCH codes. These codes have length $\mathfrak{n}_B = m \cdot (L+1)$ and dimensions $\mathfrak{k}_B^{(i)} = m \cdot (L-i)$. These codes can also be interpreted as codes over $\mathbb{F}_{2^m}$, where the codes have length $n_B = L+1$ and dimensions $k_B^{(i)} = L-i$. We use the fraktur font to indicate parameters over the base field $\mathbb{F}_2$.

With the WOE channel, we have at most $n_B = L+1$ bit errors in any inner codeword. We exploit this condition for the code design. This design requires only a single outer code for the protection of the first level. We use inner codes $\mathcal{B}^{(0)}$ with minimum Hamming distance $d_B^{(0)} \geq L+3$. This allows to correct one bit error, while any possible error pattern with $2, \ldots, L+1$ errors can be detected by the inner decoder of the first level. The error detection will be used for erasure decoding of the outer code $\mathcal{A}^{(0)}$. For the second level code $\mathcal{B}^{(1)}$, the minimum Hamming distance should be $d_B^{(1)} \geq 2L+3$. This condition guarantees that the decoder for $\mathcal{B}^{(1)}$ can correct any possible error pattern with at most $n_B = L+1$ bit errors.

Example 1: Consider $L = 2$ and $m = 10$. As inner code, we use the shortened binary BCH code $\mathcal{B}^{(0)}(2; 30, 20, 5)$. This code has the subcode $\mathcal{B}^{(1)}(2; 30, 10, 11)$ which is used in the second level. Note that we can consider both codes as codes of length $n_B = 3$ for transmission of the WOE with $\mathbb{F}_{2^{10}}$. The minimum Hamming distance $d_B^{(0)} = L+3 = 5$ allows correcting two bit errors introduced by the WOE channel. The code $\mathcal{B}^{(1)}(2; 30, 10, 11)$ has minimum distance $d_B^{(1)} = 11 > 2L+3 = 7$. Hence, this code can correct the maximum number $n_B = L+1 = 3$ of bit errors that can occur with the WOE channel.

For the inner BCH codes, we consider a generator matrix of a special form. For instance, for $L = 3$ this form is

$$\mathbf{G}_B = \begin{pmatrix} \mathbf{I}_m & \mathbf{G}_{0,1} & \mathbf{G}_{0,2} & \mathbf{G}_{0,3} \\ \mathbf{0}_m & \mathbf{I}_m & \mathbf{G}_{1,2} & \mathbf{G}_{1,3} \\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{I}_m & \mathbf{G}_{2,3} \end{pmatrix}, \tag{15}$$

where $\mathbf{I}_m$ is an $m \times m$-identity matrix, $\mathbf{0}_m$ is an $m \times m$-matrix of zeros, and $\mathbf{G}_{i,j}$ are $m \times m$-matrices over $\mathbb{F}_2$. $\mathbf{G}_B$ is the generator matrix of $\mathcal{B}^{(0)}$. The generator matrix for $\mathcal{B}^{(1)}$ consists of the first $2m$ rows of $\mathbf{G}_B$, whereas the fist m rows form the generator matrix for $\mathcal{B}^{(2)}$.

The m bits information of an inner code are additionally protected by an outer code over $\mathbb{F}_{2^m}$. In this work, we encode

only the first level with an outer code since the second level inner code corrects any possible error patterns introduced by the WOE channel. The outer RS code $\mathcal{A}^{(0)}$ has minimum distance $d_A^{(0)} = n_A - k_A^{(0)} - 1$. Choosing a low dimension for the outer RS code leads to high error correction performance. Later on, we discuss the parameter choices in more detail. In the following example, we consider the extreme case of dimension one, i.e., a repetition code as first level outer code.

Example 2: Consider the inner codes from Example 1. As outer code for the first level we consider a repetition code $\mathcal{A}^{(0)}(2^{10}; 80, 1, 80)$, whereas the second level remains uncoded. For encoding, we consider 800 information bits as 80 symbols of $\mathbb{F}_{2^{10}}$, which are written to the first row of the codeword matrix. Another 10 bits (one symbol in $\mathbb{F}_{2^{10}}$) are encoded using the outer code $\mathcal{A}^{(0)}(2^{10}; 80, 1, 80)$. This codeword has length 80 over $\mathbb{F}_{2^{10}}$ and is then stored in the second row of the codeword matrix. Afterward, we interpret each column of two symbols in $\mathbb{F}_{2^{10}}$ as 20 bits, which are encoded using the inner codes $\mathcal{B}^{(0)}(30, 20, 5)$ and $\mathcal{B}^{(1)}(2; 30, 10, 11)$.

The generator matrix for the inner code for $L = 2$ has the form

$$\mathbf{G}_B = \begin{pmatrix} \mathbf{I}_m & \mathbf{G}_{0,1} & \mathbf{G}_{0,2} \\ \mathbf{0}_m & \mathbf{I}_m & \mathbf{G}_{1,2} \end{pmatrix} \in \mathbb{F}_2^{(20\times 30)}, \tag{16}$$

where the first 10 rows correspond to a generator matrix of the code $\mathcal{B}^{(1)}(2; 30, 10, 11)$. Hence, the first 10 information bits are encoded using the subcode. The remaining bits are encoded with $\mathcal{B}^{(0)}(30, 20, 5)$.

The overall code has length $n = (L + 1) \cdot n_A = 240$ symbols in $\mathbb{F}_{2^{10}}$. The dimension is $k = k_A^{(0)} + n_A = 81$ symbols and therefore the rate is $R = 0.3375$. We can also interpret the length and dimension in bits instead of symbols, which we denote by $\mathfrak{n} = \mathfrak{n}_B \cdot n_A = 2400$ *bits* and $\mathfrak{k} = (k_A^{(0)} + n_A) \cdot m = 810$ *bits*.

C. DECODING

In the following, we present a low complexity decoding algorithm, where the outer decoder only corrects erasures. We assume transmission over the WOE channel, i.e., for each m-bit block at most one bit-error can occur.

An inner codeword of length $\mathfrak{n}_B = (L+1) \cdot m$ contains at most $n_B = (L+1)$ errors. The receiver first decodes the inner BCH codes with minimum Hamming distance at least $L+3$. With this minimum Hamming distance, we could correct $\lfloor \frac{L+2}{2} \rfloor$ errors. However, to prevent erroneous decoding, we correct only single errors for the inner code $\mathcal{B}^{(0)}$. Hence, the inner decoder is able to detect any error pattern with up to $L + 1$ errors, i.e., every possible error pattern introduced by the WOE channel. For two or more error, an erasure is declared by the inner decoder.

For each inner codeword with successful decoding, the first $m(L - 1)$ bits are used to re-encode the codeword of inner code $\mathcal{B}^{(1)}$ and subtract it from the received vector. The residual inner codeword has zeros in the first $m(L - 1)$ positions, while the next m bits are one code symbol in $\mathbb{F}_{2^m}$ from the outer code $\mathcal{A}^{(0)}$.

After decoding all inner codes, the outer RS code $\mathcal{A}^{(0)}$ can be decoded using erasure only decoding, e.g., with the Forney algorithm. This allows to correct $n_A - k_A^{(0)}$ erasures. If the outer decoding is successful it provides the last m information bits for each inner BCH code. Using those information bits, we can re-encode the codeword for $\mathcal{B}^{(0)}$ using the last m rows of the generator matrix. This codeword is then subtracted from the received vector. The resulting vector is a possibly erroneous codeword of the inner subcode $\mathcal{B}^{(1)}$. The condition $d_B^{(1)} \geq 2L+3$ guarantees that the decoder for $\mathcal{B}^{(1)}$ can correct any possible error pattern with at most $n_B = L + 1$ bit errors. Hence, the decoding procedure only fails when the number of erasures for the outer RS code exceeds $n_A - k_A^{(0)}$. This leads to the following proposition.

Proposition 3: Consider a GC code with outer RS code $\mathcal{A}^{(0)}(2^m; n_A, k_A, n_A - k_A^{(0)} + 1)$, inner code $\mathcal{B}^{(0)}(m(L + 1), mL, d_B^{(0)} \geq L + 3)$, and $\mathcal{B}^{(1)}(m(L + 1), m(L - 1), d_B^{(1)} \geq 2L + 3)$. For the WEO channel over $\mathbb{F}_{2^m}$, the proposed decoding algorithm corrects any possible error pattern with up to

$$t = 2\left(n_A - k_A^{(0)}\right) + 1 \tag{17}$$

errors.

Proof: The inner codes $\mathcal{B}^{(0)}$ can correct one error and declare an erasure if more than one error occurs. Similarly, the inner codes $\mathcal{B}^{(1)}$ can correct up to $L + 1$ errors.

Since the inner subcodes can detect or correct any possible error pattern with up to $L+1$ errors, the decoding only fails if the outer RS decoding fails. The RS decoding fails if the number of erasures exceeds $n_A - k_A^{(0)}$, because any $k_A^{(0)}$ error free positions are sufficient for erasure decoding of RS codes. Each erasure requires at least two errors in an inner codeword. Additionally, all inner codewords with a single error can be corrected. Therefore the guaranteed error correction capability is $t = 2(n_A - k_A^{(0)}) + 1$. ■

Example 3: Consider the GC code from Example 2. We interpret the codeword as a 30×80 binary matrix and decode each column in the inner binary BCH code $\mathcal{B}^{(0)}$. Note that each column has only three symbols in $\mathbb{F}_{2^{10}}$ and therefore the proposed channel can add at most three errors. Each column with at most one error is decoded correctly, while an erasure is declared for all other columns.

The first 10 bits of each inner codeword without erasure are the first 10 information bits. We use those bits to re-encode the codeword of the subcode $\mathcal{B}^{(1)}$ using the first 10 rows of the generator matrix $\mathbf{G}_B$. We subtract the codeword of the subcode from the codeword obtained by decoding $\mathcal{B}^{(0)}$. This results again in a codeword of $\mathcal{B}^{(0)}$. Due to the structure of the generator matrix (16), this codeword has only zeros in the first 10 bit positions, the next 10 bits are the code bits of the outer code and are passed to the outer decoder as one symbol of $\mathbb{F}_2^{10}$.

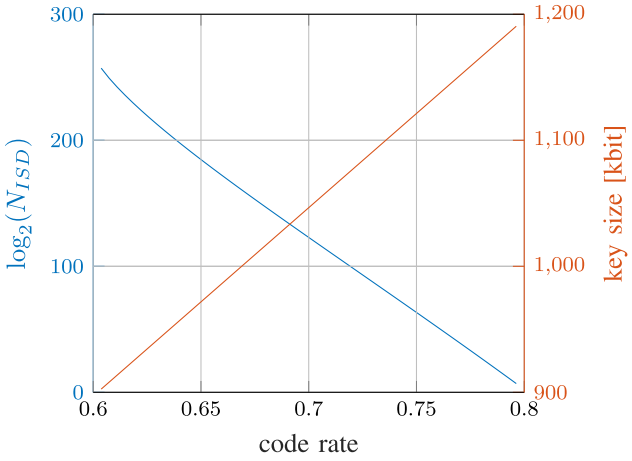

FIGURE 3. N_{ISD} over code rate for $\mathbb{F}_{221}$ code with $L = 4$ and $n = 270$.

The outer RS decoder is able to correct up to $n_A - k_A^{(0)}$ erasures. In this example, we used an outer repetition code. Hence, the outer codeword can be determined by any code symbol. Note that no decoding error is possible in the inner decoder, hence this produces the correct outer codeword as long as the number of erasures is at most $n_A - 1$.

To determine the inner codewords for the erasure positions, use the outer code symbols and re-encode them to an inner codeword from $\mathcal{B}^{(0)}$ using the last 10 rows of the generator matrix $\mathbf{G}_B$. Subtracting this codeword from the inner received vector results in a codeword in the subcode $\mathcal{B}^{(1)}$ with up to three errors. Since the subcode has minimum distance 11, we are able to correct all possible error patterns.

D. CODE EXAMPLES

Table 1 shows some examples for GC codes for the WOE channel. Given are the parameters L and m, the parameters of the inner code and its subcode, and the parameters of the GC code. We present the work factor N_{ISD} for information set decoding attacks as well as the key size and the work factor N_{SA} for the structural attack on concatenated codes as discussed in Section II-C.

Given the parameters L and m of the GC code, we found the inner BCH codes by testing combinations of cyclotomic cosets to find a primitive BCH code of length $(L+1)\cdot m+\delta$ and dimension $L\cdot m+\delta$ with a subcode of dimension $(L-1)\cdot m+\delta$. If the minimum distances of these codes are sufficient, we shorten them by δ to get the inner codes for the proposed scheme.

The code rate for these codes is always slightly above $\frac{L-1}{L+1}$ because the outer code $\mathcal{A}^{(0)}$ has dimension 1 and the other outer levels are uncoded. All codes in Table 1 have a guaranteed error correction capability of $t = n-k$. A higher dimension for $\mathcal{A}^{(0)}$ leads to a lower error correction capability and a higher key size as shown in Figure 3. Lowering the code rate of the other outer codes leads to a lower overall code rate without increasing the error correction capability.

The work factor for finding a minimum-weight codeword in the dual code mainly depends on the minimum distance of the dual of the inner code $\mathcal{B}^{(0)}$. This minimum distance increases with the inner code length and inner code rate. L is the parameter that has the highest impact on N_{SA} because the length of the inner code is $(L+1)m$ and its rate is $\frac{L}{L+1}$. The minimum distances and weight distributions, required for the work factors of the structural attack, were found by computing all codewords of the dual code.

The overall security is bounded by the lowest work factor for the known attacks. Hence, a higher work factor for ISD attacks than for the structural attack has no advantage. Figure 4 shows the work factors N_{ISD} and N_{SA} over the outer code length n_A. The key size is given over the outer code length on the right y-axis. Those plots show that increasing the outer code length over the intersection of the two work factors has only a minor effect on the overall security. On the other hand, the key size grows quadratically with the code length. Hence, we choose the code length such that the two work factors are balanced. An example for this choice is code 4 in Table 1, which is nearly balanced. Codes 1 to 3 have higher outer code lengths which require key sizes up to 320 kbit. These codes have much higher work factors against ISD attacks. However, the overall security is at most 2^{89}. For code 4 on the other hand, the work factors are nearly balanced at 2^{95} and the key size is only about 131 kbit.

Considering the proposed channel model, one may expect that ISD based attacks can exploit the structure of the channel error values, i.e., the knowledge that each m-bit block contains at most one error. In [46], such an attack was analyzed, which assumes that the exact Hamming weight for each error block is known due to side-channel information. Since each block has at most one error there are t erroneous blocks and $n-t$ error free blocks. For $k_A^{(0)} = 1$, we have $t = n-k$ and there are $n-t = k$ error free blocks, which form an information set. Hence, given the exact Hamming weight of each error block an attacker can easily retrieve the message.

On the other hand, without side-channel information, one would need to guess the weight of each block. Each block contains at most one error and therefore the vector of the weights is a length n binary vector of Hamming weight t. Guessing such a vector at random has a success probability of $\binom{n}{t}^{-1}$. For $t = n-k$, the probability of guessing the correct error weights is equal to the probability of success for the ISD algorithm according to (5).

E. DECODING COMPLEXITY

To analyze the complexity of the decoding, we only consider the special case $k_A^{(0)} = 1$. We approximate the complexity with respect to the number of finite field multiplications (FFMs), since addition in binary extension fields requires only bit-wise exclusive or gates and no field inverse is required for decoding.

Note, that the outer decoding is an erasure decoding of a code of dimension one and requires at most n_A field multiplications for re-encoding. Hence, the complexity is dominated by the inner BCH decoding. Decoding of the

TABLE 1. Examples for GC codes for the WOE channel.

	parameters			$\mathcal{B}$			$\mathcal{A}$	exemplary GC code								
	field	L	m	$\mathfrak{n}_B$	$d_{\mathcal{B}}$	$d_{\mathcal{B}^{(1)}}$	n_A	n	$\mathfrak{n}$	R	t	N_{ISD}	key size	$d_{\mathcal{B}^\perp}$	$W_{C^\perp}(d_B^\perp)$	N_{SA}
1	$\mathbb{F}_{2^{10}}$	2	10	30	≥ 5	≥ 11	80	240	2400	0.34	159	2^{217}	190 kbit	11	120	2^{85}
2	$\mathbb{F}_{2^{10}}$	2	10	30	≥ 5	≥ 11	94	282	2820	0.34	187	2^{255}	262 kbit	11	120	2^{87}
3	$\mathbb{F}_{2^{10}}$	2	10	30	≥ 5	≥ 11	104	312	3120	0.34	207	2^{283}	320 kbit	11	120	2^{89}
4	$\mathbb{F}_{2^{15}}$	3	15	60	≥ 6	≥ 12	40	160	2400	0.51	79	2^{156}	190 kbit	16	3	2^{128}
5	$\mathbb{F}_{2^{21}}$	3	21	84	≥ 7	≥ 13	48	192	4032	0.51	95	2^{188}	382 kbit	22	3	2^{186}
6	$\mathbb{F}_{2^{21}}$	4	21	105	≥ 7	≥ 13	55	275	5775	0.6	109	2^{262}	936 kbit	31	8	2^{266}
7	$\mathbb{F}_{2^{21}}$	4	21	105	≥ 7	≥ 13	54	270	5670	0.6	107	2^{257}	903 kbit	31	8	2^{265}
8	$\mathbb{F}_{2^{30}}$	4	30	150	≥ 7	≥ 13	81	405	12150	0.6	161	2^{388}	2895 kbit	41	1	2^{385}

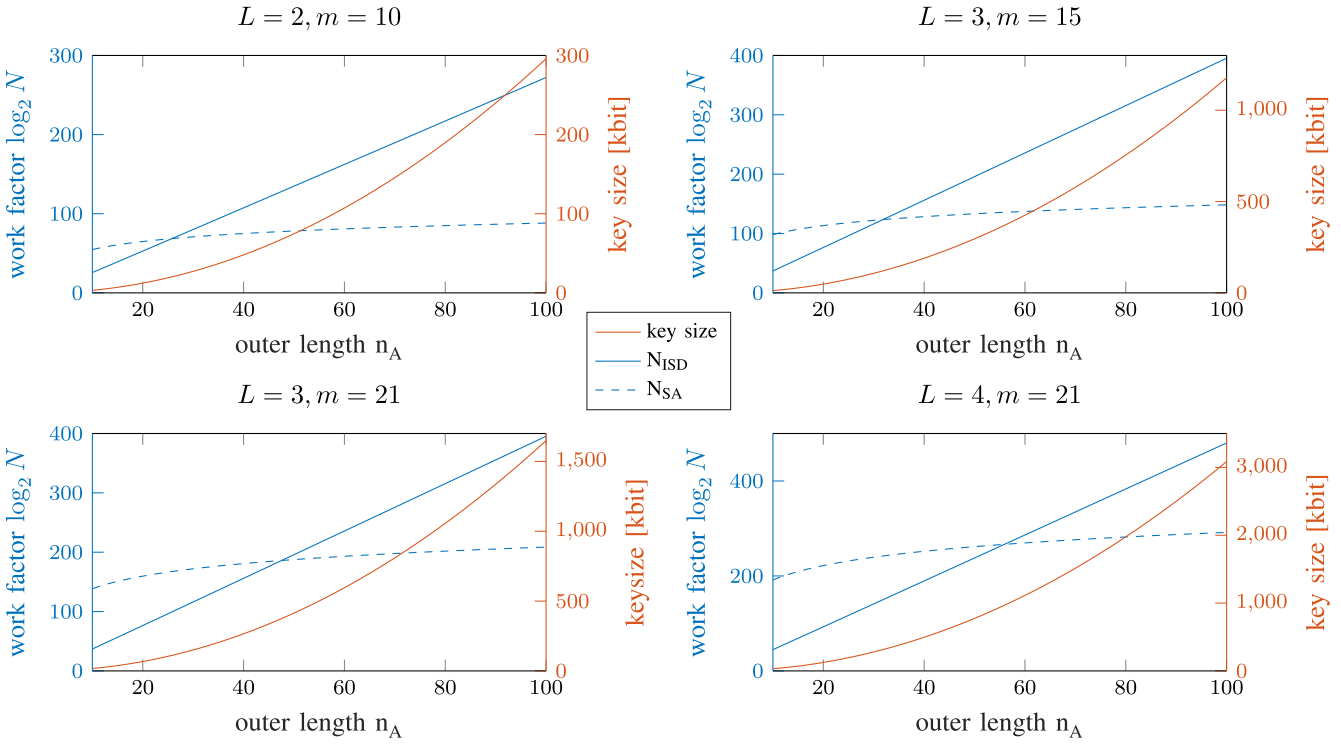

FIGURE 4. Work factor over outer length for different codes.

inner BCH codes is done in three steps: syndrome calculation, Berlekamp-Massey algorithm (BMA), and Chien search. The field multiplications for the syndrome calculation can be neglected because the received vector is binary. The BMA according to [47] requires $2t_B^2 + 2t_B$ FFMs and the Chien search requires $\mathfrak{n}_B t_B$ FFMs [48].

We have n_A inner BCH codes, where each code is decoded at most twice. The first round of inner decoding can stop as soon as one inner code is decoded without an erasure. In the second round, we have to decode all inner codes with erasures in the first round. But we consider the worst case, where all inner codes are decoded twice. Similarly, the complexity of the inner decoding operations vary from level to level. The decoding in the first level corrects one error and needs to detect up to $L+1$ errors, whereas the decoding in the second level has to correct up to $t_B = L+1$ errors. For simplicity, we consider the complexity of the more complex second level. This leads us to an upper bound for the overall number of FFMs N_{FFM} required for the BMA and the Chien search

$$\begin{aligned} N_{FFM} &\leq 2n_A\left(2t_B^2 + 2t_B + \mathfrak{n}_B t_B\right) \\ &= 4\mathfrak{n}\frac{\left(t_B^2 + t_B\right)}{\mathfrak{n}_B} + 2\mathfrak{n}t_B. \end{aligned}$$

Substituting $t_B = (L+1)$ and $\mathfrak{n}_B = m(L+1)$ according to the proposed code construction, we get

$$\begin{aligned} N_{FFM} &\leq 4\mathfrak{n}\frac{\left((L+1)^2 + (L+1)\right)}{m(L+1)} + 2\mathfrak{n}(L+1) \\ &= 4\mathfrak{n}\frac{(L+2)}{m} + 2\mathfrak{n}(L+1) \\ &= \mathfrak{n}\left(\frac{4}{m}(L+2) + 2(L+1)\right). \end{aligned}$$

Hence, for a constant number of levels L the complexity of the decoding grows only linearly with the binary length $\mathfrak{n}$, i.e., the complexity is of order $\mathcal{O}(\mathfrak{n})$.

Furthermore, the FFMs are in the field $\mathbb{F}_{2^{\widetilde{m}}}$ of the inner BCH codes. The value $\widetilde{m}$ is in the order of $\log_2(\mathfrak{n}_B + 1)$ and we have $\widetilde{m} = 9$ for the largest code in Table 1. Hence, these fields are significantly smaller than the fields over which the outer codes are defined ($m = 30$ for the largest code). In case of higher dimensions $k_A^{(0)}$ of the outer code $\mathcal{A}^{(0)}$, one would require additional arithmetic in this larger field, which could lead to a significantly higher decoding complexity.

V. DECODING BEYOND GUARANTEED ERROR CORRECTION CAPABILITY

Proposition 3 shows that the proposed decoding method guarantees an error correction capability of $t = 2(n_A - k_A^{(0)}) + 1$. On the other hand, many error patterns with more than t errors are correctable. Consider the case for t errors where $n_A - k_A^{(0)}$ inner codewords have 2 errors leading to an erasure and one other inner codeword has a single error which can be corrected. Now, an additional error only leads to a decoding failure if this error is introduced in the codeword with a single error. In all other cases, the proposed decoding method still produces the correct codeword.

Let us consider the maximum number of errors that may be corrected depending on the error positions. The outer decoder corrects up to $n_A - k_A^{(0)}$ erasures, where each inner codeword producing an erasure may have up to $L+1$ errors. Furthermore, each other inner codeword may have one error without producing an erasure. Hence, the maximum possible number of decodable errors is

$$t_{max} = (L+1)\left(n_A - k_A^{(0)}\right) + k_A^{(0)}. \tag{18}$$

Introducing more than t errors of course leads to a non-zero decoding failure rate (DFR), as is inherent for some code based cryptosystems [12], [31], [49]. This non-zero DFR may lead to security problems, depending on the application, but increases the work factor for ISD based attacks.

A decoding failure occurs when the number of erasures exceeds $n_A - k_A^{(0)}$. Given the code parameters L, n_A, $k_A^{(0)}$, and the channel error probability ϵ, the probability P_{DF} of a decoding failure can be calculated for the WOE channel as

$$P_{DF} = \sum_{j=n_A-k_A^{(0)}+1}^{n_A} \binom{n_A}{j} P_E^j (1-P_E)^{n_A-j}, \tag{19}$$

where P_E is the erasure probability in the inner decoder. For two or more symbol errors in an inner codeword, an erasure occurs. For the WOE channel, we have

$$P_E = \sum_{j=2}^{L+1} \binom{L+1}{j} \epsilon^j (1-\epsilon)^{L+1-j}. \tag{20}$$

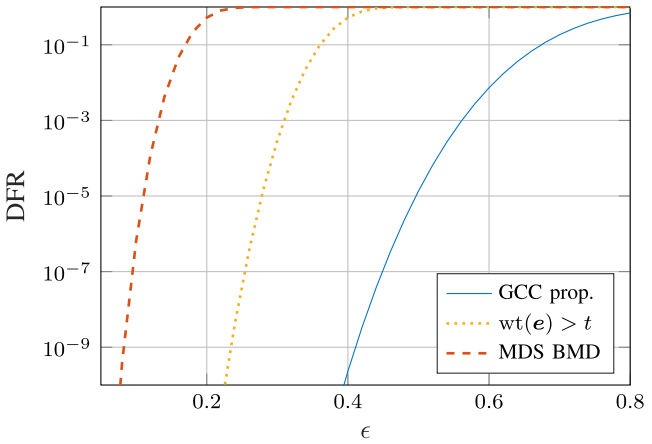

FIGURE 5. Comparison of MDS code with BMD decoding with proposed GC code and decoding for $L = 4$, $m = 21$, and $n_A = 54$.

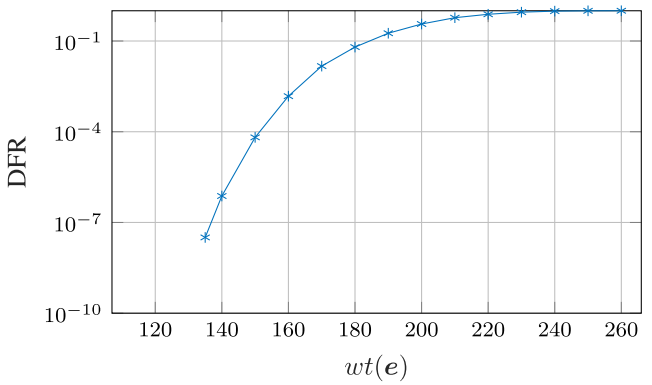

FIGURE 6. Simulated DFR over a fixed number of errors for $L = 4$, $m = 21$, and $n_A = 54$.

Figure 5 shows the DFR over the channel error probability ϵ of the WOE channel in comparison to the DFR of a maximum distance separable (MDS) code with bounded minimum distance (BMD) decoding. Also shown is the probability that more than t errors occur. As can be seen the proposed codes have a significant gain over MDS codes and the proposed decoding method can typically correct much more than t errors.

Figure 6 shows the simulated DFR over a fixed number of errors. For this simulation, we draw binary error patterns of size $\mathfrak{n}_B \times n_A$ and weight $wt(\boldsymbol{e})$ uniformly at random. We evaluated up to 10^9 such error patterns for each error weight and counted the number of uncorrectable error patterns. Any column with at least 2 errors leads to an erasure in the BCH decoding. If the number of erasures exceeds $n_A - k_A^{(0)}$ a decoding failure occurs in the outer decoding. The x-axis in Figure 6 starts at t errors. It can be seen that for a DFR up to 10^{-7} at least 28 additional errors can occur compared to the guaranteed error correction capability.

Note that the proposed codes all have $t = n - k$, hence, increasing the number of errors leads to more than $n - k$ errors. In this case, the ISD algorithm proposed by Prange [6] is not applicable, since this method searches for k error free

TABLE 2. Comparison with other code-based cryptosystems.

ref	failures	code family	parameters	category	N_{ISD}	N_{SA}	key size [kByte]
[26]	no	GCC	$\mathcal{G}_{157},\ n = 312$		2^{283}	2^{30}	33
[30]	no	Goppa	348864	I (AES128)	2^{143}		255
[31]	yes	QC-MDPC	12323, 142, 134	I (AES128)	2^{135}		1.5
prop.	no	GCC	$\mathbb{F}_{2^{15}},\ L = 3,\ n_A = 40$	I (AES128)	2^{156}	2^{128}	24
[30]	no	Goppa	460896	III (AES192)	2^{185}		512
[31]	yes	QC-MDPC	24659, 206, 199	III (AES192)	2^{200}		3
[32]	no	GRS	1282, 1146, 68	III (AES192)	2^{180}		393
prop.	no	GCC	$\mathbb{F}_{2^{21}},\ L = 3,\ n_A = 59$	III (AES192)	2^{232}	2^{193}	72
[30]	no	Goppa	6688128	V (AES256)	2^{262}		1021
[31]	yes	QC-MDPC	40973, 274, 264	V (AES256)	2^{265}		5
[32]	no	GRS	1950, 1754, 98	V (AES256)	2^{260}		917
prop.	no	GCC	$\mathbb{F}_{2^{21}},\ L = 4,\ n_A = 54$	V (AES256)	2^{257}	2^{265}	113

positions. Hence, also our approximation for the complexity of ISD attacks (5) cannot directly be applied.

VI. COMPARISON WITH OTHER CODE-BASED CRYPTOSYSTEMS

Table 2 presents some codes for comparison with other code-based cryptosystems. The table shows the work factor N_{ISD} for ISD attacks calculated according to (5). Additionally, the work factor N_{SA} for finding minimum-weight dual codewords for GC codes as well as the key size are presented. The security level is determined according to the categories in the NIST standardization process [33]. The proposed codes are compared to GC codes over Gaussian integers [21]. We also consider the cryptosystems in [30], [32], and [31]. These systems are compared with respect to the public key size for the same security category. Furthermore, we discuss the decoding complexity for these coding schemes.

For the key sizes of the proposed McEliece scheme, the complete generator matrix is taken into account, i.e., $n \cdot k \cdot m$ bits. The key sizes could be reduced to $(n-k) \cdot k \cdot m$ bits using the conversion algorithm in [35]. On the other hand, the Classic McEliece system from [30] is a Niederreiter scheme, where the public key is $(n-k) \cdot k$ bits. For the QC-MDPC based BIKE scheme [31], the key size is even further reduced due to the quasi cyclic code structure. For the scheme proposed in [32] the public key requires an additional matrix, leading to a larger key size.

We first compare the proposed GC codes to the GC codes over Gaussian integers. The inner codes over Gaussian or Einstein integers allow for a very high error correction capability. This leads to a high work factor for information set decoding at a relatively short public key size. On the other hand, the dual of the short inner code has a low minimum Hamming distance. Hence, the work factor for finding minimum-weight dual codewords is quite low. For instance, consider the codes over $\mathcal{G}_{157}$ and $\mathbb{F}_{2^{15}}$ with comparable key sizes. The GC code over Gaussian integers achieves a much higher work factor N_{ISD}. However, this code is less robust against structural attacks.

Next, we compare the proposed GC codes to the classic McEliece key encapsulation mechanism (KEM) [30], which is among the finalists for NIST standardization. The proposed GC code construction has a significant advantage over Goppa codes reducing the key size by a factor of 7 to 10, respectively.

The scheme proposed in [32] is based on generalized Reed-Solomon (GRS) codes. It differs slightly from the usual McEliece scheme to cope with structural attacks on these codes. In comparison to this scheme the proposed GC codes reduce the key size by a factor of 5 and 9, respectively.

We also compare the proposed design to another NIST candidate, the BIKE KEM. This scheme is based on quasi-cyclic moderate density parity check (QC-MDPC) codes. This allows for extremely small public keys. However, depending on the application the non-zero DFR of this scheme may be problematic. On the other hand, we consider only the security for the guaranteed error correction capability of the GC codes, where no decoding failures occur.

As shown in Section IV-E, the complexity of the proposed decoding grows linearly with the code length. For cyclic codes, such as the Goppa codes from [30] or the GRS codes from [32] the decoding complexity is at least $\mathcal{O}(n \log(n))$ [50]. Note that the code length of the proposed GC codes is significantly shorter than for the QC-MDPC-based system from [31] with the same security category. The QC-MDPC-based systems have significantly higher decoding complexity. This was shown in [34], where an FPGA implementation of the proposed decoding method was presented. A comparison to the QC-MDPC decoder from [23] showed that the proposed GC decoder is three times faster and requires less than 1% of the logic of the QC-MDPC decoder for the same security category. Similarly, the GC decoder outperforms the decoder for binary Goppa codes from [24] for the same security level. In [24], several implementations were proposed, where the one with the lowest area requirements needs about 2.5 times more logic and the number of clock cycles is about 8 times higher compared to the GC decoder.

As shown in Section V, the proposed decoding can correct more than t errors. This allows to reduce the public key

size for the same security level. However, this scheme is not able to compete with the QC-MDPC based BIKE KEM with respect to key size.

VII. CONCLUSION

In this work, we have introduced the weight-one error channel for code-based cryptosystems. Moreover, we have proposed a code construction for this channel based on generalized concatenated codes. These codes enable a low complexity decoding algorithm which is based on the decoding of BCH codes with low error-correcting capabilities [51]. Using the proposed channel model, all proposed GC codes have an error correction capability of $t = n - k$ which leads to a high security against ISD attacks. We showed that the proposed decoding scheme can typically correct significantly more errors than the guaranteed error correction capability. Hence, we may increase the number of errors without changing the decoder at the price of a non-zero DFR.

Additionally, we have investigated the work factor for the structural attack on concatenated codes proposed by Sendrier [25]. The complexity of the search for minimum-weight codewords of the dual code depends mainly on the minimum Hamming distances for the dual code of the first level inner component code. Compared to codes over Gaussian and Eisenstein integers [21], the binary inner codes achieve higher minimum Hamming distances for the dual codes. This increases the work factor for Sendrier's attack leading to higher overall security.

Finally, we have compared the proposed code construction with the classic McEliece KEM system from [30] and the BIKE scheme [31], which are candidates in the NIST standardization. The proposed codes reduce the public key size by a factor 5.5 to 10.6 in comparison to the schemes in [30], [32] which do not introduce decoding failures. In comparison to the BIKE scheme, the key size of the proposed codes is still relatively high. On the other hand, the BIKE scheme introduces decoding failures, which allow only for ephemeral keys. Furthermore, the QC-MDPC decoding is complex.

In [34], an FPGA implementation of a GC decoder is presented and compared to hardware decoders for binary Goppa codes as well as QC-MDPC codes. This implementation shows, that the proposed GC codes allow for a very efficient decoding, which significantly reduces the area and time requirements in comparison to the decoder for Goppa codes. Compared to the bit-flipping decoder for the QC-MDPC codes proposed in [31], the gain is even more pronounced, due to the complex iterative decoding of long QC-MDPC codes.

For comparable security, the key size for the proposed code construction is significantly smaller than for the classic McEliece scheme. On the other hand, the Goppa codes proposed for classic McEliece were already proposed by McEliece in 1978 and are believed to be secure because no structural attack on them is known.

A Niederreiter system or the use of the conversion proposed in [35] may reduce the public key size by a factor equal to the code rate, i.e., 0.34 to 0.6. An investigation of the applicability of the proposed decoding scheme for a Niederreiter system is subject to future work. Moreover, an analysis of the security when increasing the number of errors beyond the guaranteed error correction capability would be an interesting topic for further research.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.

[2] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *Quantum Inf. Comput.*, vol. 3, pp. 317–344, Jul. 2003.

[3] E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 384–386, May 1978.

[4] R. McEliece, "A public-key cryptosystem based on algebraic coding theory," Jet Propulsion Lab., Pasadena, CA, USA, DSN Progress Rep. 42–44, pp. 114–116, 1978.

[5] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," *Probl. Control Inf. Theory*, vol. 15, no. 2, pp. 159–166, 1986.

[6] E. Prange, "The use of information sets in decoding cyclic codes," *IRE Trans. Inf. Theory*, vol. 8, pp. 5–9, Sep. 1962.

[7] P. J. Lee and E. F. Brickell, "An observation on the security of McEliece's public-key cryptosystem," in *Advances in Cryptology (EUROCRYPT)*, D. Barstow *et al.*, Eds. Berlin, Germany: Springer, 1988, pp. 275–280.

[8] J. Stern, "A method for finding codewords of small weight," in *Coding Theory and Applications*, G. Cohen and J. Wolfmann, Eds. Berlin, Germany: Springer, 1989, pp. 106–113.

[9] D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *Post-Quantum Cryptography*, J. Buchmann and J. Ding, Eds. Berlin, Germany: Springer, 2008, pp. 31–46.

[10] A. May, A. Meurer, and E. Thomae, "Decoding random linear codes in $\mathcal{O}(2^{0.054n})$," in *Advances in Cryptology (ASIACRYPT)*, D. H. Lee and X. Wang, Eds. Berlin, Germany: Springer, 2011, pp. 107–124.

[11] V. M. Sidelnikov, "A public-key cryptosystem based on binary Reed-Muller codes," *Discrete Math. Appl.*, vol. 4, no. 3, pp. 191–207, 1994.

[12] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. S. L. M. Barreto, "MDPC-McEliece: New McEliece variants from moderate density parity-check codes," in *Proc. IEEE Int. Symp. Inf. Theory*, 2013, pp. 2069–2073.

[13] V. M. Sidelnikov and S. O. Shestakov, "On insecurity of cryptosystems based on generalized Reed-Solomon codes," *Discrete Math. Appl.*, vol. 2, no. 4, pp. 439–444, 1992.

[14] L. Minder and A. Shokrollahi, "Cryptanalysis of the Sidelnikov cryptosystem," in *Advances in Cryptology (EUROCRYPT)*, M. Naor, Ed. Berlin, Germany: Springer, 2007, pp. 347–360.

[15] P. Santini, M. Battaglioni, F. Chiaraluce, M. Baldi, and E. Persichetti, "Low-Lee-density parity-check codes," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1–6.

[16] T. S. C. Lau and C. H. Tan, "On the design and security of Lee metric McEliece cryptosystems," *Des. Codes Cryptogr.*, vol. 90, pp. 695–717, Jan. 2022.

[17] A.-L. Horlemann-Trautmann and V. Weger, "Information set decoding in the Lee metric with applications to cryptography," *Adv. Math. Commun.*, vol. 15, no. 4, pp. 677–699, 2021.

[18] M. Baldi *et al.*, "A new path to code-based signatures via identification schemes with restricted errors," 2020, *arXiv:2008.06403*.

[19] V. Weger, K. Khathuria, A.-L. Horlemann, M. Battaglioni, P. Santini, and E. Persichetti, "On the hardness of the Lee syndrome decoding problem," 2020, *arXiv:2002.12785*.

[20] J. Bariffi, H. Bartz, G. Liva, and J. Rosenthal, "Analysis of low-density parity-check codes over finite integer rings for the Lee channel," 2021, *arXiv:2105.08372*.

[21] J.-P. Thiers and J. Freudenberger, "Generalized concatenated codes over Gaussian and Eisenstein integers for code-based cryptography," *Cryptography*, vol. 5, no. 4, p. 33, 2021.
[22] J. Freudenberger and J.-P. Thiers, "A new class of Q-ary codes for the McEliece cryptosystem," *Cryptography*, vol. 11, no. 5, p. 11, 2021.
[23] S. Heyse, I. von Maurich, and T. Güneysu, "Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices," in *Cryptographic Hardware and Embedded Systems (CHES)*, G. Bertoni and J.-S. Coron, Eds. Berlin, Germany: Springer, 2013, pp. 273–292.
[24] P. M. C. Massolino, P. S. L. M. Barreto, and W. V. Ruggiero, "Optimized and scalable co-processor for McEliece with binary Goppa codes," *ACM Trans. Embedded Comput. Syst.*, vol. 14, no. 3, pp. 1–32, May 2015.
[25] N. Sendrier, "On the structure of randomly permuted concatenated code," Ph.D. dissertation, Dept. Comput. Sci., INRIA, Le Chesnay Cedex, France, 1995.
[26] J.-P. Thiers and J. Freudenberger, "Generalized concatenated codes over Gaussian integers for the McEliece cryptosystem," in *Proc. IEEE 11th Int. Conf. Consum. Electron. (ICCE-Berlin)*, Nov. 2021, pp. 1–6.
[27] S. Puchinger, S. Müelich, K. Ishak, and M. Bossert, "Code-based cryptosystems using generalized concatenated codes," in *Applications of Computer Algebra*, I. S. Kotsireas and E. Martínez-Moro, Eds. Cham, Switzerland: Springer Int., 2017, pp. 397–423.
[28] D. Rohweder, J. Freudenberger, and S. Shavgulidze, "Low-density parity-check codes over finite Gaussian integer fields," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 481–485.
[29] J.-P. Thiers and J. Freudenberger, "Decoding of generalized concatenated codes over the one-lee error channel for the McEliece cryptosystem," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2022, pp. 2785–2790.
[30] D. J. Bernstein *et al.*, *Classic McEliece: Conservative Code-Based Cryptography*, NIST PQC Competition, Gaithersburg, MD, USA, 2020.
[31] N. Aragon *et al.*, *BIKE: Bit Flipping Key Encapsulation*, BIKE Team, Sunnyvale, CA, USA, 2021.
[32] M. Baldi, F. Chiaraluce, J. Rosenthal, P. Santini, and D. Schipani, "Security of generalised Reed-Solomon code-based cryptosystems," *IET Inf. Security*, vol. 13, no. 4, pp. 404–410, 2019.
[33] G. Alagic *et al.*, "Status report on the second round of the NIST post-quantum cryptography standardization process," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, NISTIR 8309, 2020.
[34] J.-P. Thiers and J. Freudenberger, "A decoder for a lightweight McEliece cryptosystem based on concatenated codes," *IEEE Consum. Electron. Mag.*, early access, Jul. 19, 2022, doi: 10.1109/MCE.2022.3192126.
[35] K. Kobara and H. Imai, "Semantically secure McEliece public-key cryptosystems-conversions for McEliece PKC," in *Proc. Int. Workshop Public Key Cryptogr.*, 2001, pp. 19–35.
[36] M. Finiasz and N. Sendrier, "Security bounds for the design of code-based cryptosystems," in *Advances in Cryptology (ASIACRYPT)*, M. Matsui, Ed. Berlin, Germany: Springer, 2009, pp. 88–105.
[37] A. Becker, A. Joux, A. May, and A. Meurer, "Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2012, pp. 520–536.
[38] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, "A finite regime analysis of information set decoding algorithms," *Algorithms*, vol. 12, no. 10, p. 209, 2019.
[39] A. Esser, A. May, and F. Zweydinger, "McEliece needs a break—Solving McEliece-1284 and quasi-cyclic-2918 with modern ISD," IACR Cryptol. ePrint Arch., Lyon, France, Rep. 2021/1634, 2021. [Online]. Available: https://ia.cr/2021/1634
[40] G. Forney, *Concatenated Codes*. Cambridge, MA, USA: MIT Press, 1965.
[41] N. Sendrier, "On the concatenated structure of a linear code," *Appl. Algebra Eng. Commun. Comput.*, vol. 9, pp. 221–242, Nov. 1998.
[42] J.-P. Thiers and J. Freudenberger, "Codes over Eisenstein integers for the niederreiter cryptosystem," in *Proc. IEEE 11th Int. Conf. Consum. Electron. (ICCE-Berlin)*, Nov. 2021, pp. 1–6.
[43] R. G. Gallager, *Information Theory And Reliable Communication*. New York, NY, USA: Wiley, 1968.
[44] V. Zyablov, S. Shavgulidze, and M. Bossert, "An introduction to generalized concatenated codes," *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 609–622, 1999.
[45] J. Spinner and J. Freudenberger, "Decoder architecture for generalized concatenated codes," *IET Circuits Devices Syst.*, vol. 9, no. 5, pp. 328–335, 2015.
[46] A.-L. Horlemann, S. Puchinger, J. Renner, T. Schamberger, and A. Wachter-Zeh, "Information-set decoding with hints," in *Code-Based Cryptography*, A. Wachter-Zeh, H. Bartz, and G. Liva, Eds. Cham, Switzerland: Springer Int., 2022, pp. 60–83.
[47] H. Tsai, C. Yang, and H. Chang, "An efficient BCH decoder with 124-bit correctability for multi-channel SSD applications," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, 2012, pp. 61–64.
[48] D. N. Bailon, M. Bossert, J.-P. Thiers, and J. Freudenberger, "Concatenated codes based on the plotkin construction and their soft-input decoding," *IEEE Trans. Commun.*, vol. 70, no. 5, pp. 2939–2950, May 2022.
[49] C. A. Melchor *et al.*, "Hamming quasi-cyclic (HQC)," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep., 2020.
[50] F. MacWilliams and N. Sloane, *The Theory of Error Correcting Codes*, 12th ed. Amsterdam, The Netherlands: North-Holland, 2006.
[51] J. Freudenberger, D. N. Bailon, and M. Safieh, "Reduced complexity hard- and soft-input BCH decoding with applications in concatenated codes," *IET Circuits Devices Syst.*, vol. 15, no. 3, pp. 284–296, 2021.