Covert Communication by Exploiting Error-Correcting Codes

Alon Marzin*, Moshe Schwartz*†, and Michael Segal*
* School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer Sheva 8410501, Israel
† Department of Electrical and Computer Engineering, McMaster University, Hamilton, ON L8S 4K1, Canada

***Abstract*—Covert channels, enabling concealed communication within seemingly innocuous data streams, pose significant challenges to traditional information security measures. This paper presents a novel method for constructing covert channels by leveraging Error-Correcting Codes (ECCs) and minimal-weight codewords. Adversaries embed their covert messages within the benign traffic of unsuspecting victims, carefully controlling the introduced errors to avoid detection. The proposed approach not only ensures the security and reliability of covert communication but also provides protection against channel errors. By integrating ECCs and minimal-weight codewords, our method offers an advanced level of stealth, data integrity, and resilience. Extensive simulations validate the feasibility and performance of the approach, highlighting its potential for practical implementation in real-world scenarios. This research opens new avenues for the construction of covert channels, enhancing information hiding capabilities and reinforcing communication security in the face of ever-evolving threats.**

***Index Terms*—Covert channels, error-correcting codes, minimal-weight codewords.**

I. Introduction

Communication between various units is essential for coordinated operation in different environments. For security, the communicating nodes may use cryptography, i.e., authenticate and encrypt the communication between them. However, cryptography does not prevent detection of the presence of communication between units. Therefore, cryptographic protection alone is insufficient in case of a covert operation, where the operating units (for example, police) must remain undetected while performing their activities. The covert transmission of sensitive information through hidden communication channels presents an ongoing challenge to information security professionals. The design of a covert communication channel in network environment [2], [4], [24], [31], [34] poses interesting questions; in particular, how the attacker can hide covert communication in existing traffic and increase the channel capacity. From the other direction, the problem is how the defender can analyze the traffic in order to find any hidden enclosed message. Adversaries adeptly exploit vulnerabilities in conventional communication systems to clandestinely exchange covert messages, evading detection and compromising data integrity. Detecting and preventing these covert channels pose significant challenges due to their ability to exploit existing communication infrastructure.

This paper continues a line of work that was started in [33], which exploits Error-Correcting Codes (ECCs) to construct the covert channel. Since in many cases the ECC used by victims is stronger than what is actually required by the channel, errors may be introduced by the adversaries to convey information. However, [33] only considered a probabilistic channel, and did not provide any concrete method of realizing the covert channel. Follow-up works took this approach further: [6] analyzed WiMax, and manipulated some of the parity-bits of the Reed-Solomon (RS) code. [30] examined 802.11a/g, and introduced noise to convey information by overwriting a certain ratio of bits. Finally, [9] studied 802.11ad and replaced the parity bits of an LDPC code with the covert message. Except for [9], all the works do not offer error protection to the covert information. Additionally, all works study probabilistic channels, and do not optimize the amount of noise by the adversaries since not all overwritten symbols differ from the original ones.

The goal of this paper is to create a covert information channel in an adversarial (worst-case) channel analysis. Additionally, we optimize the noise introduced by the adversaries, and provide inherent error-correction capabilities to the covert information as well, all while providing concrete efficient algorithms. Our approach utilizes a specially designed encoding algorithm that encodes covert messages into minimal-weight codewords. These minimal-weight codewords make the scheme harder to detect by the victims, seamlessly blending into the victims' traffic, thereby evading suspicion. Additionally, adversaries employ a dedicated decoding algorithm that accurately retrieves the hidden information from minimal-weight codewords after correcting additional errors that might have been introduced by the communication channel, allowing for the successful extraction of the covert messages.

Crucially, our proposed method not only guarantees secure covert communication but also safeguards the adversaries' covert messages against channel errors. Prior to embedding, the adversaries encode their covert messages using their own error-correcting code, ensuring resilience against noise or interference in the communication channel. By integrating this additional layer of error correction, our approach provides enhanced reliability and robustness for covert data transmission.

The versatility of our method extends to the usage of two types of error-correcting codes for the construction of a covert channel: Generalized Reed-Solomon codes for non-binary communication channels and Reed-Muller codes for binary communication channels. This adaptability allows for the construction of covert channels in diverse communication environments, accommodating various applications and sce-

979-8-3503-4897-2/24/$31.00 ©2024 IEEE

narios. To our best knowledge, there were no previous attempts to design covert channels in this way.

To validate the effectiveness of our method, extensive simulations were conducted, demonstrating the feasibility and performance of our approach. The results showcase the potential of leveraging minimal-weight codewords, ECCs, and comprehensive error correction for covert communication, offering a secure and resilient covert channel.

The remainder of this paper is structured as follows: Section II provides an overview of related work in the fields of covert channels and error-correcting codes. Section III presents the threat model and the general framework for our proposed covert channel methods, furthermore this section gives an overview of the notations used throughout this paper. Section IV presents the proposed encoding and decoding algorithms for minimal-weight codewords. Section V describes the simulation setup and evaluates the performance of our approach for different code parameters of the adversaries error-correcting code, and finally, Section VI concludes the paper by summarizing the contributions.

II. Background and Related Work

A. Covert Channels

Covert channels are a type of communication that is designed to be hidden from detection or interception. These channels can be used for nefarious purposes, including data exfiltration, Command and Control (C&C), and evasion of security measures. They can be implemented using various methods and are designed to remain hidden or undetected by authorized system users and administrators. Covert-channels are considered a serious threat to the security of computer systems, as they can be used to bypass traditional security measures and gain unauthorized access to sensitive information. Various methods have been proposed for implementing covert-channels, including steganography, timing channels, and tunneling.

One example of implementing covert-channels using steganography to hide information within other types of data is given in a study by Mielikainen [19]. The proposed method embeds covert messages into grey-scale images to form stego images. The embedding process treats a pair of pixels as a unit. After the message embedding, the value of the ith message bit m_i is equal to the Least Significant Bit (LSB) of stego image's ith pixel y_i. The value of the $i+1$th message bit m_{i+1} is a function of y_i and y_{i+1}; this allows embedding the same amount of information as in [28], but with fewer changed pixel values. The proposed method does not exhibit imbalance in the embedding distortion an asymmetric property between even and odd valued pixel regions, making detection more difficult for methods like those proposed in [12]. Other examples of steganographic covert-channels can be found in [3], [15], [20], [32] with the recent one in [22] that proposes dynamic steganographic algorithm for the covert VoIP communications.

Li et al. [13], [14] designed robust packet-dropout covert timing channel through parity casecade coding. In their scheme, the covert message is modulated into the sequence numbers of the actively dropped packets, which can be retrieved by the receiver. With the help of the verification section, the actual codewords combination can be identified to retrieve the embedded covert message.

Hou and Zheng [11] introduced CloakLoRa, a covert channel over physical layer with Chirp Spread Spectrum modulation technique that is designed to enable low-power IoT devices to communicate with each other at long ranges. CloakLoRa embeds secret messages information into a regular LoRa packet by modulating the amplitudes of LoRa chirps while keeping the frequency intact.

Tunneling is another method for implementing covert channels, which involves encapsulating information within other types of network traffic. In a study by Oakley et al. [21] a covert channel for tunneling TCP traffic through protected static protocols was developed. Protected static protocols are UDP-based protocols with variable fields that cannot be blocked without collateral damage, such as power grid failures.

To prevent data loss in traditional covert communication techniques, researchers in Luo [17] proposed a Bitcoin transaction based covert approach. The scheme achieves covert communication by using address interactions and transaction amounts of Bitcoin.

The detection of covert channels is a critical task in computer security, as their presence can indicate the presence of malicious activity on a system. There have been several studies as well on detecting covert channels in various contexts, including network traffic analysis and file analysis. For example, Zuppelli et al. [36] allows to run a rich set of Berkeley Packet Filter (eBPF) programs for gathering condensed statistics on header fields and timings that can be further processed and combined with additional data to spot the presence of covert channels. Han et al. [8] proposed a covert timing channel detection method based on the k-Nearest Neighbor (k-NN) algorithm. This method uses a series of statistics related to the time interval and payload length as features to train a machine learning model. Shvartzman et al. [29] presented two network timing covert channel attacks, and a defense mechanism against them. The defense mechanism is based on semi-supervised machine learning and deep learning algorithms, which are both used for novelty detection in network traffic. By detecting unusual traffic, they can identify the disturbances needed to leak the information. The study [5] enumerates several machine learning approaches for covert channel detection. It should be noted that there is no best covert channel under all circumstances, and practically, those who operate well in certain scenarios will not work well in others. Thus, the selection of the best covert channel depends on its capacity, detectability and reliability.

B. Error-Correcting Codes

Error-Correcting Codes (ECCs) are an essential component of modern digital communication systems. These codes are designed to detect and correct errors that may occur during data transmission or storage, thereby improving the reliability and integrity of the information being transmitted. ECCs are

widely used in a variety of applications, including telecommunications, computer networks, and storage systems.

Starting with the seminal works of Shannon [26], [27] and Hamming [7], error-correcting codes work by mapping user messages into a set of vectors, called codewords, that are significantly dissimilar from one another. Thus, even if the vectors are corrupted during the transmission, upon reception they cannot be confused for corrupted versions of other codewords. The dissimilarity is usually measured using the Hamming metric, corresponding the channels that corrupt vectors by changing their entries to other symbols.

Significant effort has been made to design codes that allow for easy encoding, and decoding (i.e., recovering from errors). Two prime examples, which we shall use in this paper, are Generalized Reed Solomon codes, and Reed-Muller codes. The former operate by over-sampling a univariate polynomial over a sufficiently large field, whereas the latter work over a small field, but over-sample a multivariate polynomial. Many other codes are known, and for a recent overview on coding theory the reader is referred to [23].

III. Threat Model and Notations

First, we fix some notations. For an integer $n \in \mathbb{N}$ we define $[n] \triangleq \{0, 1, \ldots, n-1\}$. Scalars will be denoted by lowercase letters or Greek letters, vectors by overlined lowercase letters, and matrices and sets by uppercase letters. The finite field of size q is denoted by $\mathbb{F}_q$. If $\overline{v} \in \mathbb{F}_q^n$ we shall denote its components with appropriate subscripts, namely, $\overline{v} = (v_0, v_1, \ldots, v_{n-1})$.

If $\overline{v} \in \mathbb{F}_q^n$, then its support is the set of indices containing non-zero entries, i.e., $\mathrm{supp}(\overline{v}) \triangleq \{i \in [n] \,|\, v_i \neq 0\}$. The Hamming weight of $\overline{v}$ is the size of its support, i.e., $\mathrm{wt}(\overline{v}) \triangleq |\mathrm{supp}(\overline{v})|$. Given another vector $\overline{v}' \in \mathbb{F}_q^n$, the Hamming distance between $\overline{v}$ and $\overline{v}'$ is the weight of their difference, $\mathrm{d}(\overline{v}, \overline{v}') \triangleq \mathrm{wt}(\overline{v} - \overline{v}')$.

A linear Error-Correcting Code (ECC) of block length n, dimension (message length) k and minimal distance d over $\mathbb{F}_q$, is a k-dimensional subspace of $\mathbb{F}_q^n$ with the distance between any two distinct vectors in it lower bounded by d. Such a code is said to be an $[n, k, d]_q$ code, and it is known that it can correct any combination of up to $t \triangleq \lfloor \frac{d-1}{2} \rfloor$ errors without making a mistake (i.e., without misdecoding). A linear code may be specified as the row space of a generator matrix $G \in \mathbb{F}_q^{k \times n}$, or as the null space of a parity-check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$.

When referring to the adversaries and to the victims we add a subscript of A and V respectively. For example, the ECC of the adversaries is denoted by C_A and d_A is its minimal distance.

The threat model is given in Figure 1. It assumes the following:

- The adversaries are active eavesdroppers capable of altering the symbols being transmitted over the communication channel by the victims.
- The adversaries have full knowledge of the ECC used by the victims, C_V, and its parameters.

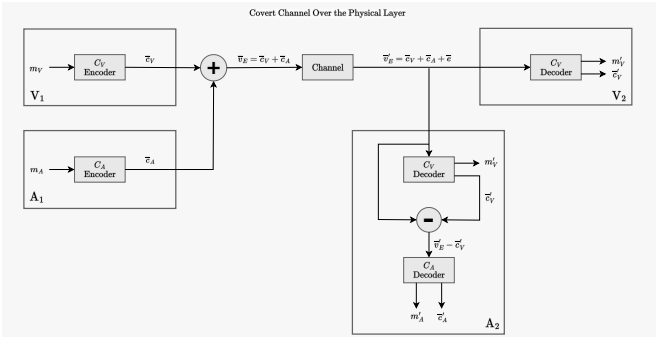

Fig. 1. The Threat Model

We briefly describe the process depicted in Figure 1: Let $\overline{m}_A \in \mathbb{F}_q^{k_A}$ be the covert message to be sent from A_1 to A_2, and let $\overline{m}_V \in \mathbb{F}_q^{k_V}$ be the message to be sent from V_1 to V_2. The adversaries A_1 and A_2 agree on C_A, over the same field $\mathbb{F}_q$ as C_V, such that $n_A \leqslant n_V$. If $n_A < n_V$ then the codewords of C_A may be padded with zeros to length n_V. Both A_1 and V_1 encode their messages using their respective ECC encoders to obtain $\overline{c}_A$ and $\overline{c}_V$. The embedding of $\overline{c}_A$ into $\overline{c}_V$ is a simple addition operation that results in $\overline{v}_E = \overline{c}_V + \overline{c}_A$, which is then transmitted over the communication channel. The channel may further corrupt the transmission, resulting in $\overline{v}'_E = \overline{c}_V + \overline{c}_A + \overline{e}$ being received, where $\overline{e}$ is the error vector introduced by the channel. V_2 uses the decoder for C_V to guess the transmitted codeword from V_1 and the message, namely, $\overline{c}'_V$ and $\overline{m}'_V$. Then, A_2 applies the decoder of C_A to $\overline{v}'_E - \overline{c}'_V$ to obtain $\overline{c}'_A$ and $\overline{m}'_A$.

First, we comment that it is sometimes convenient to think of the message to be encoded not as a vector $\overline{m} \in \mathbb{F}_q^k$, but rather as an integer, which we shall denote as m. Using any arbitrary ordering of the vectors $\mathbb{F}_q^k$ (e.g., lexicographic ordering), we can associate each integer in $m \in [q^k]$ with a unique vector from $\mathbb{F}_q^k$. We shall do so throughout the paper, which will allow for a simpler description of our scheme.

We also comment that the threat model considers a single hop case, where an adversary A_1 is located at victim node V_1 and on the other side of the communication channel adversary A_2 is located at victim node V_2. The model can be extended to a multi-hop case by applying the above assumptions to each hop on the route between A_1 to A_2.

A. MDS Codes

One covert channel we construct uses MDS codes. An $[n, k, d]_q$ is said to be MDS if it attains the Singleton bound with equality, namely, $d = n - k + 1$. The following property of MDS codes is well known.

Lemma 1 ([18, p. 319, Corollary 3]). *Let C be an $[n, k, d]_q$ code that is MDS, and assume $G \in \mathbb{F}_q^{k \times n}$ is a generator matrix for it. Then any k columns of G are linearly independent.*

Lemma 1 immediately implies the following result concerning the number and the structure of codewords of minimal weight.

Corollary 2. *Let C be a $[n,k,d]_q$ code that is MDS. Let $J \subseteq [n]$, $|J| = d = n-k+1$, be a set of coordinates. Then there exist exactly $q-1$ codewords $\overline{c} \in C$ with $\mathrm{supp}(\overline{c}) = J$, and they are all of the form $\beta \cdot \overline{c}'$ for some fixed $\overline{c}' \in C$ and $\beta \in \mathbb{F}_q \setminus \{0\}$.*

While any MDS code will do, a good choice is to use a Generalized Reed-Solomon (GRS) code, since it possesses an efficient decoding algorithm.

Definition 3 (Generalized Reed-Solomon codes)**.** *Let $n \geqslant k \geqslant 1$ be integers, and $q \geqslant n$ a prime power. Assume $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_q$ are distinct, and $v_0, v_1, ..., v_{n-1} \in \mathbb{F}_q \setminus \{0\}$. The Generalized Reed-Solomon code with these parameters is the set*

$$C = \{(v_0 u(\alpha_0), v_1 u(\alpha_1), \ldots, v_{n-1} u(\alpha_{n-1})) \mid u(x) \in \mathbb{F}_q[x], \deg(u(x)) \leqslant k-1\},$$

where $\mathbb{F}_q[x]$ denotes the set of all polynomials in the unknown x with coefficients from $\mathbb{F}_q$.

We comment that a simple generator matrix for the code is as follows:

$$G = \begin{pmatrix} v_0 \cdot \alpha_0^0 & v_1 \cdot \alpha_1^0 & \ldots & v_{n-1} \cdot \alpha_{n-1}^0 \\ v_0 \cdot \alpha_0^1 & v_1 \cdot \alpha_1^1 & \ldots & v_{n-1} \cdot \alpha_{n-1}^1 \\ v_0 \cdot \alpha_0^2 & v_1 \cdot \alpha_1^2 & \ldots & v_{n-1} \cdot \alpha_{n-1}^2 \\ \vdots & \vdots & & \vdots \\ v_0 \cdot \alpha_0^{k-1} & v_1 \cdot \alpha_1^{k-1} & \ldots & v_{n-1} \cdot \alpha_{n-1}^{k-1} \end{pmatrix} \quad (1)$$

B. Reed-Muller Codes

The second covert channel we construct uses binary Reed-Muller (RM) codes. These codes are useful in planning 5G wireless communication, see [35]. Codewords of RM consist of evaluation vectors of multivariate polynomials over the binary field $\mathbb{F}_2$.

Definition 4 (Reed-Muller codes)**.** *Let $s \geqslant r \geqslant 0$ be integers. Denote $n \triangleq 2^s$, and assume $\overline{v}_0, \ldots, \overline{v}_{n-1} \in \mathbb{F}_2^s$ are the 2^s binary vectors of length s in lexicographic order. The binary Reed-Muller code, $\mathrm{RM}(r,s)$, is the set*

$$C = \{(u(\overline{v}_0), u(\overline{v}_1), \ldots, u(\overline{v}_{n-1})) \mid u(\overline{x}) \in \mathbb{F}_2[x_0, \ldots, x_{s-1}], \deg(u(\overline{x})) \leqslant r\},$$

where $\mathbb{F}_2[x_0, \ldots, x_{s-1}]$ denotes the set of all polynomials in the s unknowns $x_0, \ldots, x_{s-1}$ with coefficients from $\mathbb{F}_2$.

The code $\mathrm{RM}(r,s)$ is a $[2^s, \sum_{i=0}^{r} \binom{s}{i}, 2^{s-r}]_2$ code. Other properties of it are best described in terms of finite geometries. One such property gives a characterization of the minimal-weight codewords. To that end we recall the definition of $(s-r)$-dimensional flats of the Eucledian geometry $EG(s,2)$. These are simply sets of vectors of the form $\{\overline{u} + \overline{v} \mid \overline{v} \in V\}$, where V is an $(s-r)$-dimensional linear subspace of $\mathbb{F}_2^s$, and $\overline{u} \in \mathbb{F}_2^s$ is an arbitrary vector.

Theorem 5 ([18, p. 380, Theorem 8])**.** *The codewords of minimal weight in $\mathrm{RM}(r,s)$ are exactly the incidence vectors of the $(s-r)$-dimensional flats in $EG(s,2)$. In the notation of Definition 4, the set minimal-weight codewords of $\mathrm{RM}(r,s)$ is the set of all binary vectors $(c_0, \ldots, c_{n-1})$, where $\{\overline{v}_i \mid c_i = 1\}$ is an $(s-r)$-dimensional flat of $EG(s,2)$.*

IV. Covert Channels via Error-Correcting Codes

The fundamental objective of a covert channel is to allow communication that is hidden from unsuspecting parties. The embedding of the covert messages into the victims' benign traffic inserts errors into their codewords. This reduces the amount of channel errors that can be corrected by the victims' code. If the adversaries inflict too many errors, the victims may notice a significant degradation of throughput leading to the exposure of the covert channel. The following theorem connects the code parameters $[n_A, k_A, d_A]_q$ of the adversaries' code C_A, the parameters $[n_V, k_V, d_V]_q$ of the victims' code C_V, and the channel errors in order to guarantee decodability of all the transmitted information. Recall that $t_V \triangleq \lfloor (d_V - 1)/2 \rfloor$ is the number of errors the victims' code can correct, and similarly t_A for the adversaries' code.

Theorem 6. *Consider the threat model as depicted in Figure 1, and assume the channel can introduce at most e errors. If $\mathrm{wt}(\overline{c}_A) + e \leqslant t_V$ holds, then the victims can correctly decode $\overline{c}_V$ and m_V. If additionally $e \leqslant t_A$ holds, then the adversaries can correctly decode $\overline{c}_A$ and m_A.*

Proof: For the first claim,

$$\mathrm{wt}(\overline{c}_A + \overline{e}) \leqslant \mathrm{wt}(\overline{c}_A) + \mathrm{wt}(\overline{e}) \leqslant \mathrm{wt}(\overline{c}_A) + e \leqslant t_V.$$

The victims' code, C_V, can correctly decode $\overline{v}'_E$ to find $\overline{c}_V$ and m_V. With this knowledge, the adversaries can compute $\overline{v}'_E - \overline{c}_V = \overline{c}_A + \overline{e}$, and since $\mathrm{wt}(\overline{e}) \leqslant e \leqslant t_A$, the adversaries' code, C_A can correctly decode $\overline{c}_A + \overline{e}$ to find $\overline{c}_A$ and m_A. ■

Remark 7. *If $d_A > t_V$, then, by the previous theorem, the only codeword the adversaries can send that guarantees not to cause a mis-decoding at the victims, is the all-zero codeword. This does not allow the adversaries any information transfer.*

In light of Theorem 6, an obvious strategy for our covert-channel algorithms is to restrict the encoding of the adversaries' messages into codewords of minimal weight in C_A. Since the previous theorem provides the guarantee for correct decoding, in the remainder of this section we focus on the important aspect of efficiently encoding information only into the minimal-weight codewords of an error-correcting code. This involves only the adversaries' code, so for ease of notation we omit the subscript A from code parameters. We present efficient covert channel algorithms for different use cases: non-binary and binary communication channels.

A. GRS-Based Covert Channel

We now present the encoding and decoding algorithms for a non-binary communication channel that is based on GRS codes. These codes are useful for satellite communications, see [16]. The algorithms use the constructive proof of Corollary 2 and a Combinatorial Number System (CNS) [1] for the

Notation	Description
G	A $k \times n$ generator matrix for C over $\mathbb{F}_q$
α	A primitive element of $\mathbb{F}_q$
m	The covert message as an integer
$\overline{c}$	A minimal-weight codeword encoding m
a	The part of m that is mapped to $\mathrm{supp}(\overline{c})$
b	The part of m that is mapped to β as in Corollary 2
$[n]$	The set $\{0, 1, \ldots, n-1\}$
L	The set from Corollary 2
$\overline{0}_k$	A vector of zeros of length k in $\mathbb{F}_q$
G_L	The restriction of G to the coordinates in L

TABLE I
NOTATIONS FOR GRS-BASED ENCODING AND DECODING ALGORITHMS

mapping of a covert message into a minimal-weight codeword and vice versa. We assume that the adversaries agree on an $[n, k, d]_q$ GRS code C, a generator matrix $G \in \mathbb{F}_q^{k \times n}$ for C (e.g., see (1)), and a primitive element $\alpha \in \mathbb{F}_q$.

Algorithm 1 Encoding for a GRS-Based Covert Channel

1: **procedure** ENCODECOVERTMESSAGE(m)
// Assumptions:
// The adversaries' code C has parameters $[n, k, d]_q$.
// $G \in \mathbb{F}_q^{k \times n}$ is a generator matrix for the code C.
// $\alpha \in \mathbb{F}_q$ is a primitive element.
// Input: $m \in [(q-1)\binom{n}{d}]$
// Output: A minimum-weight codeword $\overline{c} \in C \setminus \{\overline{0}\}$
2: $a \leftarrow \lfloor m/(q-1) \rfloor$
3: $b \leftarrow m \bmod (q-1)$
4: $L \leftarrow [n]$
5: **for** $i \leftarrow d$ to 2 **do**
6: $j \leftarrow \mathrm{argmax}_{r \geqslant i-1}\left\{a - \binom{r}{i} \geqslant 0\right\}$
7: $a \leftarrow a - \binom{j}{i}$
8: $L \leftarrow L \setminus \{j\}$
9: $j \leftarrow \mathrm{argmax}_{r \geqslant 0}\left\{a - \binom{r}{1} \geqslant 0\right\}$
10: $\overline{v} \leftarrow \overline{0}_k$
11: $v_j \leftarrow 1$
12: $\overline{c} \leftarrow \alpha^b \cdot \overline{v} G_L^{-1} G$
13: **return** $\overline{c}$

The size of the covert-messages dictionary is simply the number of minimum-weight codewords in the GRS code, which by Corollary 2 is $(q-1) \cdot \binom{n}{d}$. For convenience, we assume that covert message is an integer $m \in [(q-1) \cdot \binom{n}{d}]$. The encoding procedure in Algorithm 1 receives this integer as input, and outputs $\overline{c} \in C$ where $\mathrm{wt}(\overline{c}) = d$. In lines 2-3 the covert message m is decomposed into two integers a and b. The first integer $a \in [\binom{n}{d}]$ is used to map (via the CNS) into a support of a minimal-weight codeword. Here, the set L used in the algorithm is the same as L in the proof of Corollary 2. The second integer $b \in [q-1]$ is used in line 12 to determine $\beta = \alpha^b$ from Corollary 2. It can be seen that the encoding algorithm runtime complexity is $\mathcal{O}(\max(nk^2, nd^2 \log k))$.

The decoding procedure in Algorithm 2 receives a minimal-weight codeword $\overline{c} \in C$ after decoding $\overline{c}'$ using a conventional decoding algorithm of a GRS code and outputs the covert message $m \in [(q-1) \cdot \binom{n}{d}]$. Line 2 gives the support of $\overline{c}$ in ascending order. Line 3 is the reverse mapping of $\mathrm{supp}(\overline{c})$ into an integer $a \in [\binom{n}{d}]$ using the CNS. In line 4, the discrete logarithm gives the value of $b \in [q-1]$ that was used in the encoding procedure. The decoding algorithm runtime is $\mathcal{O}(nd^2)$ in the worst case since calculation of the sum of binomial coefficients requires this amount of time.

Algorithm 2 Decoding for a GRS-Based Covert Channel

1: **procedure** DECODECOVERTMESSAGE($\overline{c}$)
// Assumptions:
// The adversaries' code C has parameters $[n, k, d]_q$.
// $\alpha \in \mathbb{F}_q$ is a primitive element.
// Input: A minimum-weight codeword $\overline{c} \in C \setminus \{\overline{0}\}$
// Output: $m \in [(q-1)\binom{n}{d}]$
2: Let $\mathrm{supp}(\overline{c}) = \{j_1, j_2, \ldots, j_d\}$ where $\forall i : j_i < j_{i+1}$
3: $a \leftarrow \sum_{i=1}^{d} \binom{j_i}{i}$
4: $b \leftarrow \log_\alpha(c_{j_1})$
5: $m \leftarrow (q-1) \cdot a + b$
6: **return** m

B. Reed-Muller-Based Covert Channel

Notation	Description
m	The covert message as an integer
$\overline{c}$	A minimal-weight codeword encoding m
$\overline{c}'$	A possibly corrupted version of $\overline{c}$
a	The part of m that is mapped to an $(s-r)$-linear subspace
b	The part of m that is mapped to a shift of the $(s-r)$-linear subspace
$\mathcal{E}_{s,s-r;2}(\cdot)$	A function mapping an integer into a canonical generator matrix for an $(s-r)$-linear subspace
W	A canonical generator matrix for an $(s-r)$-linear subspace
$\Lambda(\cdot)$	The set of columns with leading 1's in a Reduced Row Echelon Form
$[s]$	The set $\{0, 1, \ldots, s-1\}$
$\overline{0}_s$	A vector of zeros of length s in $\mathbb{F}_2$
$V_s(\cdot)$	A function mapping an integer to its binary representation vector of length s in $\mathbb{F}_2$
$\mathcal{R}(\cdot)$	A function that returns the Reduced Row Echelon Form of a matrix
$\tau(\cdot)$	A function that Convert a matrix in Reduced Row Echelon Form into a canonical matrix
$\mathcal{D}_{s,s-r;2}(\cdot)$	A function that maps a canonical generator matrix of an $(s-r)$-linear subspace to an integer

TABLE II
NOTATIONS FOR RM-BASED ENCODING AND DECODING ALGORITHMS

We now switch our attention to a binary communication channel that is based on RM codes. While in the GRS based covert channel the adversaries are able to select the minimal distance of their GRS ECC in granularity of 2, for a RM based covert channel the adversaries have a limitation for selecting the minimal distance of their RM ECC in granularity of powers of 2.

First we define additional operators used by the algorithms. The function $V_s : [2^s] \to \mathbb{F}_2^s$ maps integers to their binary representation, where the first entry of the output vector corresponds to the Least-Significant Bit (LSB) of the integer.

Accordingly, V_s^{-1} is the inverse mapping. Given a matrix M, we use $\mathcal{R}(M)$ to denote its reduced row echelon form. Since in the following we shall require efficient procedures for mapping integers to subspaces and back, we will employ the procedures suggested in [25]. To that end, we recall a few notations and relevant facts from [25]. For integers $n \geqslant k \geqslant 0$ and a prime power q, the q-ary Gaussian coefficient is defined as

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \triangleq \frac{\prod_{i=1}^{n}(q^i-1)}{\prod_{i=1}^{k}(q^i-1)\cdot\prod_{i=1}^{n-k}(q^i-1)}.$$

It is well known that $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the number of k-dimensional subspaces of $\mathbb{F}_q^n$. Each such subspace may be represented by a $k \times n$ matrix M over $\mathbb{F}_q$ whose rows form a basis. To make this representation unique, one may use the reduced row echelon form, $\mathcal{R}(M)$, however, [25] uses a slightly different type of matrix denoted $\tau(\mathcal{R}(M))$ (see [25, p. 275]), and called a canonical matrix. The set of columns with leading 1's in $\mathcal{R}(M)$ is denoted by $\Lambda(M)$. To map from integers to canonical matrices, [25] introduced the function $\mathcal{E}_{n,k;q}(\cdot)$, and the inverse mapping, $\mathcal{D}_{n,k;q}(\cdot)$. For the mapping of a covert message into a minimal-weight codeword and the other way around, we use the characterization of the minimal-weight codewords for RM codes given in Theorem 5. We assume that the adversaries agree on $[n,k,d]_2$ $\mathrm{RM}(r,s)$ code.

Algorithm 3 Encoding for a RM-Based Covert Channel

1: **procedure** ENCODECOVERTMESSAGE(m)
// Assumptions:
// The adversaries' code C is $\mathrm{RM}(r,s)$.
// Input: $m \in [2^r \cdot \begin{bmatrix} s \\ s-r \end{bmatrix}_2]$
// Output: A minimum-weight codeword $\overline{c} \in C \setminus \{\overline{0}\}$
2: $a \leftarrow \lfloor m/2^r \rfloor$
3: $b \leftarrow m \bmod 2^r$
4: $W \leftarrow \mathcal{E}_{s,s-r;2}(a)$
5: $J \leftarrow [s] \setminus \Lambda(W) = \{j_0,\ldots,j_{r-1}\}$ s.t. $\forall i : j_i < j_{i+1}$
6: $\overline{u} \leftarrow \overline{0}_s$
7: $\overline{b} \leftarrow V_r(b)$
8: **for** $i \leftarrow 0$ to $r-1$ **do**
9: $u_{j_i} \leftarrow b_i$
10: $\overline{c} \leftarrow \overline{0}_{2^s}$
11: **for** $\overline{v}$ in $\mathbb{F}_2^{s-r}$ **do**
12: $\overline{p} \leftarrow \overline{v}W + \overline{u}$
13: $j \leftarrow V_s^{-1}(\overline{p})$
14: $c_j \leftarrow 1$
15: **return** $\overline{c}$

Given a covert message, and according to Theorem 5, we need to map it into the indices vector of a shifted $(s-r)$-dimensional linear subspace of $\mathbb{F}_2^s$. There are $\begin{bmatrix} s \\ s-r \end{bmatrix}_2$ subspaces of dimension $s-r$, and 2^r cosets for each such subspace (representing the shift), therefore the size of the covert-messages dictionary is $2^r \cdot \begin{bmatrix} s \\ s-r \end{bmatrix}_2$. For convenience, we assume that the covert message is an integer $m \in [2^r \cdot \begin{bmatrix} s \\ s-r \end{bmatrix}_2]$. The encoding procedure in Algorithm 3 receives this integer as an input, and outputs $\overline{c} \in C$ s.t. $\mathrm{wt}(\overline{c}) = d$. In lines 2-3 the covert message m is decomposed into two integers a and b. The first integer $a \in [\begin{bmatrix} s \\ s-r \end{bmatrix}_2]$ is mapped in line 4 into a canonical matrix W that is a basis for a $(s-r)$-dimensional linear subspace. The second integer $b \in [2^r]$ is mapped into a shift for the subspace. The set J in line 5 holds the indices of the columns of W that do not have a leading 1, in ascending order. Therefore, after lines 6-9 the vector $\overline{u}$ is the shift for the subspace. In lines 10-14 we compose the indices vector for the shifted subspace, i.e., the minimal-weight codeword of the RM code. Overall we have $\mathcal{O}(\max(d(s-r)s),(s-r)s^2)$ runtime complexity.

Algorithm 4 Decoding for a RM-Based Covert Channel

1: **procedure** DECODECOVERTMESSAGE($\overline{c}$)
// Assumptions:
// The adversaries' code C is $\mathrm{RM}(r,s)$.
// Input: A minimum-weight codeword $\overline{c} \in C \setminus \{\overline{0}\}$
// Output: $m \in [2^r \cdot \begin{bmatrix} s \\ s-r \end{bmatrix}_2]$
2: Let $\mathrm{supp}(\overline{c}) = \{j_0,\ldots,j_{d-1}\}$
3: $\overline{u} \leftarrow V_s(j_0)$
4: $W \leftarrow V_s(j_1) - \overline{u}$
5: $i \leftarrow 2$
6: **while** $\mathrm{rank}(W) < s-r$ **do**
7: $\overline{v} \leftarrow V_s(j_i) - \overline{u}$
8: $W' \leftarrow \begin{pmatrix} W \\ \overline{v} \end{pmatrix}$
9: $i \leftarrow i+1$
10: **if** $\mathrm{rank}(W') > \mathrm{rank}(W)$ **then**
11: $W \leftarrow W'$
12: $W \leftarrow \tau(\mathcal{R}(W))$
13: $a \leftarrow \mathcal{D}_{s,s-r;2}(W)$
14: Let $\Lambda(W) = \{j'_0,\ldots,j'_{s-r-1}\}$ s.t. $\forall i : j'_i < j'_{i+1}$
15: **for** $i = 0$ to $s-r-1$ **do**
16: **if** $u_{j'_i} = 1$ **then**
17: $\overline{v} \leftarrow i$th row of W
18: $\overline{u} \leftarrow \overline{u} - \overline{v}$
19: $\overline{b} \leftarrow \overline{0}_r$
20: $J \leftarrow [s] \setminus \Lambda(W) = \{j_0,\ldots,j_{r-1}\}$ s.t. $\forall i : j_i < j_{i+1}$
21: **for** $i \leftarrow 0$ to $r-1$ **do**
22: $b_i \leftarrow u_{j_i}$
23: $b \leftarrow V_r^{-1}(\overline{b})$
24: $m \leftarrow 2^r \cdot a + b$
25: **return** m

The decoding procedure in Algorithm 4 receives a minimal-weight codeword $\overline{c} \in C$, after applying a conventional decoding algorithm for RM code on $\overline{c}'$, and outputs the covert message $m \in [2^r \cdot \begin{bmatrix} s \\ s-r \end{bmatrix}_2]$. Line 2 gives the support of $\overline{c}$. In lines 3-12 we recover the basis for the $(s-r)$-linear subspace, i.e., the canonical matrix W. We use the vector $\overline{u}$ given in line 3 to cancel the shift of the subspace, this occurs in lines 4 and 7. In each iteration of the while loop in line 6, we append a vector $\overline{v}$ of the subspace to the current basis W in line 8, and check in line 10 if the dimension of the subspace has increased. If so, W is replaced with W'. This procedure carries on until we have $(s-r)$ spanning set for the subspace that we convert

into the canonical matrix in line 12. Line 13 is the reverse mapping of W into an integer $a \in [\begin{bmatrix} s \\ s-r \end{bmatrix}_2]$. In lines 14-18 we cancel any component of the subspace that might be in $\overline{u}$ in order to recover the shift vector for the subspace. Lines 19-23 gives the reverse mapping of the subspace shift $\overline{u}$ into an integer $b \in [2^r]$. Lastly, in line 24 we use the integers a and b to compose the covert message m. The runtime of Algorithm 4 is $\mathcal{O}(\max((s-r)s^2, d(s-r)s, kn))$.

V. Simulation Results

The simulation results presented in this section show how the behavior of the Word Error Rate (WER) of the adversaries' and victims' ECCs for different symbol error probability (channel errors) is affected by different code parameters for the adversaries' ECC. We have implemented a general framework for conducting simulations, i.e., the threat model as depicted in Section III, incorporating the proposed algorithms in Section IV using Python programming language. For the implementation of the encoding and decoding algorithms we used Numpy library which has a C based backend that improves the performance of calculations involving vectors and matrices. We used Galois library [10] which provides an implementation for finite fields and GRS. For RM we added an implementation of our own. Our simulation setup was a LENOVO YOGA 520 laptop with Intel's core i7 8th gen processor.

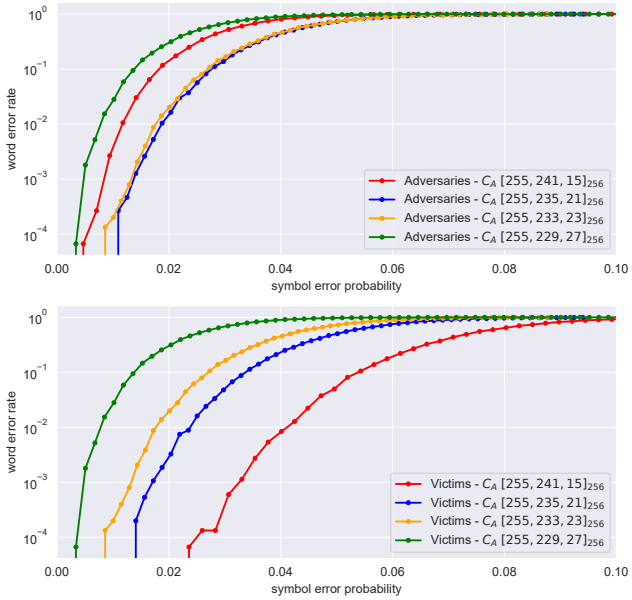

Fig. 2. WER in a GRS based covert channel incorporating Algorithm 1 and Algorithm 2 for the encoding and decoding, respectively. The victims' ECC WER is shown in the bottom graph for an $[255, 191, 65]_{256}$ GRS code with $t_V = 32$. The adversaries' ECCs WER is shown in the top graph for an $[255, 241, 15]_{256}$, $[255, 235, 21]_{256}$, $[255, 233, 23]_{256}$ and $[255, 229, 27]_{256}$ GRS codes with $t_A = 7, 10, 11, 13$, respectively.

For the non-binary communication channel with a GRS based covert channel the simulation results in Figure 2 bottom graph show the WER of the victims' ECC. As we expected, the WER curves are shifted to the right as the minimal distance of the adversaries' ECCs decrease. The reason for this shift is that the effective error-correction capability of the victims' ECC after the embedding of the covert message is $t'_V = t_V - d_A$. For the adversaries WER in the top graph of Figure 2, it can be seen that for the $[255, 229, 27]_{256}$ (the green curve) with greatest error-correction capability $t_A = 13$ has the worst WER, i.e. it is the leftmost curve on the graph. This is because the victims are left with $t'_V = 5$ errors that can still be corrected. When $t'_V < t_A$ and the channel inflicts more than t'_V additional errors into $\overline{v}_E$ the adversaries cannot successfully decode $\overline{v}'_E$ into $\overline{c}_V$ and use it for a successful decoding of $\overline{c}'_A$ into $\overline{c}_A$ and m_A. In this case t'_V becomes the effective error-correction capability for both the adversaries and the victims. Next is the red curve that fits the $[255, 241, 15]_{256}$ adversaries' ECC in this case $t_A = 7$ and $t'_V = 17$. Lastly, the yellow curve followed by the blue curve, the yellow curve fits the $[255, 233, 23]_{256}$ ECC that can correct $t_A = 11$ but actually has an effective error-correcting capability of $t'_V = 9$ and thus is slightly to the left of the blue curve that fits an $[255, 235, 21]_{256}$ ECC with $t_A = 10$ and $t'_V = 11$.

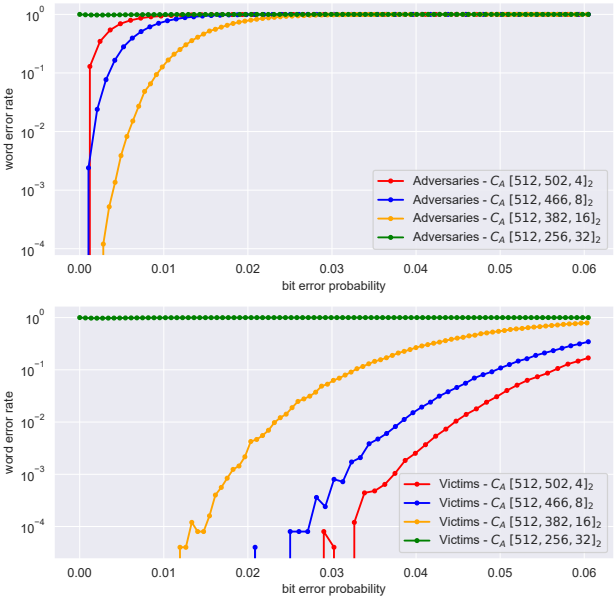

Fig. 3. WER in a RM based covert channel incorporating Algorithm 3 and Algorithm 4 for the encoding and decoding, respectively. The victims' ECC WER is shown in the bottom graph for an $[512, 130, 64]_2$ RM code with $t_V = 31$. The adversaries' ECCs WER is shown in the top graph for an $[512, 502, 4]_2$, $[512, 466, 8]_2$, $[512, 382, 16]_2$ and $[512, 256, 32]_2$ RM codes with $t_A = 1, 3, 7, 15$, respectively.

For the binary communication channel with a RM based covert channel where the decoding procedure in Algorithm 4 was used the simulation results in Figure 3 exhibit the same trend as for the non-binary communication channel with a GRS based covert channel with one exception, for the $[512, 256, 32]_2$ adversaries' ECC (green curves) where $d_A > t_V$ both the adversaries and the victims cannot successfully decode their codewords. This result fits Remark 7.

VI. Conclusions

We have presented a novel approach for the construction of a covert channel by exploiting error correcting codes and leveraging minimal weight codewords. The usage of minimal weight codewords for embedding covert messages into benign traffic that is protected by an ECC allows control over the trade-of between data integrity and stealth of communication.

Acknowledgments

This research was (partially) funded by the Israeli Science Foundation (Grant No. 465/22) and by the Army Research Office under Grant Number W911NF-22-1-0225. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

References

[1] E. F. Beckenbach and G. Polya, *Applied Combinatorial Mathematics*. John Wiley & Sons, 1964.

[2] K. Cabaj, L. Caviglione, W. Mazurczyk, S. Wendzel, A. Woodward, and S. Zander, "The new threats of information hiding: The road ahead," *IT Prof.*, vol. 20, no. 3, pp. 31–39, 2018. [Online]. Available: https://doi.org/10.1109/MITP.2018.032501746

[3] Y.-M. Cheng, C.-M. Wang, Y.-Y. Tsai, C.-H. Chang, and P.-C. Wang, "Steganography for three-dimensional models," in *Advances in Computer Graphics*, T. Nishita, Q. Peng, and H.-P. Seidel, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 510–517.

[4] A. El-Atawy and E. Al-Shaer, "Building covert channels over the packet reordering phenomenon," in *IEEE INFOCOM 2009*, 2009, pp. 2186–2194.

[5] M. A. Elsadig and A. Gafar, "Covert channel detection: Machine learning approaches," *IEEE Access*, vol. 10, pp. 38 391–38 405, 2022.

[6] I. Grabska and K. Szczypiorski, "Steganography in wimax networks," in *2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2013, pp. 20–27.

[7] R. W. Hamming, "Error detecting and error correcting codes," *Bell System Technical Journal*, vol. 29, no. 2, pp. 147–160, 1950.

[8] J. Han, C. Huang, F. Shi, and J. Liu, "Covert timing channel detection method based on time interval and payload length analysis," *Comput. Secur.*, vol. 97, p. 101952, 2020. [Online]. Available: https://doi.org/10.1016/j.cose.2020.101952

[9] P. M. B. Harley, M. Tummala, and J. C. McEachen, "High-throughput covert channels in adaptive rate wireless communication systems," in *2019 International Conference on Electronics, Information, and Communication (ICEIC)*, 2019, pp. 1–7.

[10] M. Hostetter, "Galois: A performant NumPy extension for Galois fields," 11 2020. [Online]. Available: https://github.com/mhostetter/galois

[11] N. Hou and Y. Zheng, "Cloaklora: A covert channel over lora phy," in *2020 IEEE 28th International Conference on Network Protocols (ICNP)*, 2020, pp. 1–11.

[12] A. Ker, "Improved detection of lsb steganography in grayscale images," in *Proc. Information Hiding Workshop*, ser. Springer LNCS, vol. 3200. Springer, 2004, pp. 97–115.

[13] Y. Li, J. Liu, X. Xu, X. Zhang, Z. Li, and Q. Zhang, "A robust packet-dropping covert channel for mobile intelligent terminals," *Int. J. Intell. Syst.*, vol. 37, no. 10, pp. 6928–6950, 2022. [Online]. Available: https://doi.org/10.1002/int.22868

[14] Y. Li, X. Zhang, X. Xu, and Y. Tan, "A robust packet-dropout covert channel over wireless networks," *IEEE Wirel. Commun.*, vol. 27, no. 3, pp. 60–65, 2020. [Online]. Available: https://doi.org/10.1109/MWC.001.1900431

[15] C.-C. Lin and P.-F. Shiu, "High capacity data hiding scheme for dct-based images," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, 07 2010.

[16] Y. Liu, Y. Guan, J. Zhang, G. Wang, and Y. Zhang, "Reed-solomon codes for satellite communications," in *International Conference on Control, Automation and Systems Engineering*, 2009, pp. 246–249.

[17] X. Luo, P. Zhang, M. Zhang, H. Li, and Q. Cheng, "A novel covert communication method based on bitcoin transaction," *IEEE Trans. Ind. Informatics*, vol. 18, no. 4, pp. 2830–2839, 2022. [Online]. Available: https://doi.org/10.1109/TII.2021.3100480

[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1978.

[19] J. Mielikainen, "Lsb matching revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285–287, 2006.

[20] S. J. Murdoch and S. Lewis, "Embedding covert channels into TCP/IP," in *Information Hiding*, ser. Lecture Notes in Computer Science, M. Barni, J. Herrera-Joancomartí, S. Katzenbeisser, and F. Pérez-González, Eds., vol. 3727. Berlin, Heidelberg: Springer, 2005.

[21] J. Oakley, L. Yu, X. Zhong, G. K. Venayagamoorthy, and R. R. Brooks, "Protocol proxy: An fte-based covert channel," *Comput. Secur.*, vol. 92, p. 101777, 2020. [Online]. Available: https://doi.org/10.1016/j.cose.2020.101777

[22] J. Peng and S. Tang, "Covert communication over voip streaming media with dynamic key distribution and authentication," *IEEE Trans. Ind. Electron.*, vol. 68, no. 4, pp. 3619–3628, 2021. [Online]. Available: https://doi.org/10.1109/TIE.2020.2979567

[23] R. Roth, *Introduction to Coding Theory*. USA: Cambridge University Press, 2006.

[24] T. Schmidbauer, J. Keller, and S. Wendzel, "Challenging channels: Encrypted covert channels within challenge-response authentication," in *ARES 2022: The 17th International Conference on Availability, Reliability and Security, Vienna,Austria, August 23 - 26, 2022*. ACM, 2022, pp. 50:1–50:10. [Online]. Available: https://doi.org/10.1145/3538969.3544455

[25] M. Schwartz, "Gray codes and enumerative coding for vector spaces," *IEEE Transactions on Information Theory*, vol. 60, no. 1, pp. 271–281, 2014.

[26] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, Jul. 1948.

[27] ——, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 623–656, Oct. 1948.

[28] T. Sharp, "An implementation of key-based digital signal steganography," in *Proc. Information Hiding Workshop*, ser. Springer LNCS, vol. 2137. Springer, 2001, pp. 13–26.

[29] O. Shvartzman, A. Ovadya, K. Zvi, O. Shwartz, R. Ogen, Y. Mallah, N. Gilboa, and Y. Oren, "Characterization and detection of cross-router covert channels," *Comput. Secur.*, vol. 127, p. 103125, 2023. [Online]. Available: https://doi.org/10.1016/j.cose.2023.103125

[30] K. S. Subramani, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "Infect: Inconspicuous fec-based trojan: A hardware attack on an 802.11a/g wireless network," in *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2017, pp. 90–94.

[31] R. Tahir, M. T. Khan, X. Gong, A. Ahmed, A. Ghassami, H. Kazmi, M. Caesar, F. Zaffar, and N. Kiyavash, "Sneak-peek: High speed covert channels in data center networks," in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, 2016, pp. 1–9.

[32] K.-C. Wu and C.-M. Wang, "Steganography using reversible texture synthesis," *IEEE Transactions on Image Processing*, vol. 24, no. 1, pp. 130–139, 2015.

[33] X. Yan, S. Guan, and X. Niu, "Research on the capacity of error-correcting codes-based information hiding," in *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2008, pp. 1158–1161.

[34] S. Zander, G. J. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Commun. Surv. Tutorials*, vol. 9, no. 1-4, pp. 44–57, 2007. [Online]. Available: https://doi.org/10.1109/COMST.2007.4317620

[35] H. Zhang, R. Li, J. Wang, Y. Chen, and Z. Zhang, "Reed-muller sequences for 5g grant-free massive access," in *2017 IEEE Global Communications Conference, GLOBECOM 2017, Singapore, December 4-8, 2017*. IEEE, 2017, pp. 1–7. [Online]. Available: https://doi.org/10.1109/GLOCOM.2017.8254233

[36] M. Zuppelli, M. Repetto, A. Schaffhauser, W. Mazurczyk, and L. Caviglione, "Code layering for the detection of network covert channels in agentless systems," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2282–2294, 2022.