Threshold-Secure Coding With Shared Key

Nasser Aldaghri, and Hessam Mahdavifar
Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI, USA
Email: aldaghri@umich.edu, hessam@umich.edu

***Abstract*—Cryptographic protocols are often implemented at upper layers of communication networks, while error-correcting codes are employed at the physical layer. In this paper, we consider utilizing readily-available physical layer functions, such as encoders and decoders, together with shared keys to provide a *threshold-type* security scheme. To this end, the effect of physical layer communication is abstracted out and the channels between the legitimate parties, Alice and Bob, and the eavesdropper Eve are assumed to be noiseless. We introduce a model for threshold-secure coding, where Alice and Bob communicate using a shared key in such a way that Eve does not get any information, in an information-theoretic sense, about the key as well as about any subset of the input symbols of size up to a certain threshold. Then, a framework is provided for constructing threshold-secure codes form linear block codes while characterizing the requirements to satisfy the reliability and security conditions. Moreover, we propose a threshold-secure coding scheme, based on Reed-Muller (RM) codes, that meets security and reliability conditions. Furthermore, it is shown that the encoder and the decoder of the scheme can be implemented efficiently with quasi-linear time complexity. In particular, a low-complexity successive cancellation decoder is shown for the RM-based scheme. Also, the scheme is flexible and can be adapted given any key length.**

I. Introduction

Conventional cryptosystems are often designed to be computationally secure by relying on unproven assumptions of hardness of mathematical problems. Information-theoretic security methods provide an alternative approach by constructing codes for keyless secure communication, as in wiretap channels introduced in the seminal work of Wyner [1]. Since then, various types of wiretap channels have been considered in the literature [2], [3], and using different coding schemes as in [4], [5].

Several approaches to provide security in the physical layer assuming shared secret keys have been considered in the literature. For instance, a variation of the wiretap channel model, where a shared secret key is assumed to be constantly generated by Alice and Bob, is studied in [6]. Another approach is to design an encryption scheme that utilizes properties of certain modulation schemes such as orthogonal frequency-division multiplexing (OFDM) to ensure security, see, e.g., [7]–[9]. Other related works include using channel reciprocity properties [10], classical stream ciphers at the physical layer [11], introducing artificial noise [12], multiple-input and multiple-output (MIMO) systems [13], public-key based McEliece cryptosystem [14], and using error-correcting codes for encryption [15], [16]. These prior works either consider noisy channels as in the wiretap channel model, or utilize cryptographic primitives being evaluated using cryptographic measures rather than information theoretical measures to ensure security. Another related line of research is secure network coding, where a wiretapper has access to a certain number of edges in a network over which a source wishes to communicate messages securely. Several works have considered information-theoretic security measures while designing network codes, see e.g., [17], [18].

Utilizing error-correcting codes to provide security in the physical layer enables sharing hardware resources between reliability and security schemes in low-cost devices. Consequently, this leads to a promising approach for low-complexity applications, such as Internet-of-Things (IoT) networks. In this paper, we consider using block codes to provide a *threshold-type* security scheme. A fixed key is assumed to be securely shared between the legitimate parties Alice and Bob a priori. Alice communicates to Bob over a noiseless channel and her transmissions reach an eavesdropper Eve, also through a noiseless channel, as shown in Figure 1. The security condition in this model is described as follows. Alice encodes her message using the shared key while ensuring that Eve does not obtain any information about the key as well as about any subset of the input message symbols of size up to a certain threshold t. Such condition is referred to as t-threshold security condition. The considered threshold-type security becomes relevant in applications where the knowledge of most, if not all, of the individual data symbols is needed in order to deduce meaningful knowledge about the content of the message. Examples of this type of data includes measurement numbers, network commands, address of data in a dataset, as well as barcodes or data in any application where the data symbols are already scrambled, hashed, or masked prior to being encoded. Furthermore, ensuring the security of the key in the model guarantees that it can be, theoretically, used infinitely many times without leaking any information about it to Eve.

In the setup considered in this paper, we completely deviate from physical-layer security protocols by assuming noiseless channels. However, we still describe the schemes as a communication setup in physical layer with the aim of, eventually, integrating such schemes with physical layer encoding and decoding. To this end, a general scheme using lin-

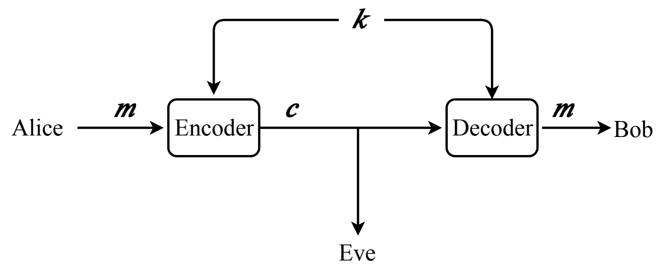

Figure 1. System setup for the proposed coding scheme.

ear block codes for the t-threshold-secure coding scheme is shown. Furthermore, we describe a specific construction based on RM codes [19] that meets the threshold security conditions, and show low-complexity quasi-linear encoder and decoder to reliably retrieve the message using the shared key.

The rest of the paper is organized as follows. In Section II we describe our setup and formulate the reliability and security conditions based on information theoretic measures. The proposed coding scheme based on linear codes is described in detail and its security and reliability are evaluated in Section III. Then we describe an explicit coding scheme based on RM codes together with an encoder and a successive-cancellation decoder in Section IV. Finally, we conclude our work in Section V, and discuss some directions for future work.

II. SYSTEM MODEL

A system model is considered in which Alice wishes to securely communicate with Bob, both are legitimate parties, through a noiseless channel. The eavesdropper, namely Eve, is tapping into that channel and observes all the bits that are transmitted over it as shown in Figure 1. Alice and Bob share a common key sequence $\boldsymbol{k}$ of length k, that can be used for encoding and decoding of message $\boldsymbol{m}$ of length m. Elements of both the key and the message symbols are from alphabet of size q, where q is a prime power. Some known permutation $\pi(.)$ of Alice's message $\boldsymbol{m}$ and key $\boldsymbol{k}$ is fed as the input to the encoder denoted as $\boldsymbol{u} = \pi(\boldsymbol{k}, \boldsymbol{m})$ of length $n = m + k$ to produce a codeword $\boldsymbol{c}$ of length m. The distributions of elements in $\boldsymbol{m}$, and $\boldsymbol{k}$ are assumed to be independent and uniform. Alice then transmits the codeword $\boldsymbol{c}$ to Bob over the noiseless channel. Bob receives the codeword and decodes it using the key $\boldsymbol{k}$ to retrieve $\boldsymbol{m}$. Eve observes $\boldsymbol{c}$ and tries to extract information about the message elements in $\boldsymbol{m}$ as well as the key sequence $\boldsymbol{k}$. In this setup, Alice and Bob agree on the encoder and the decoder a priori, which are also disclosed to Eve.

In this model, the security condition is that although parts of input $\boldsymbol{u}$ are disclosed to Eve, from information-theoretic point of view, no information about any subset of size up to a certain parameter t of the input symbols will be leaked to Eve. This is in contrast with the traditional measure of information-theoretic security where one wants the mutual information between the entire message block and Eve's observation to be almost zero. In a sense, we consider a *sub-block-wise* measure of information-theoretic security. We aim at designing encoder and a decoder for a noiseless channel that utilizes a shared key $\boldsymbol{k}$ to encode a message $\boldsymbol{m}$ such that the following conditions are met:

1) *Reliability*: Bob is able to decode the message using the key with probability one, i.e.,

$$H(\boldsymbol{m}|\boldsymbol{c}, \boldsymbol{k}) = 0. \quad (1)$$

2) *Key security*: the codeword $\boldsymbol{c}$ does not reveal any information about the key $\boldsymbol{k}$, i.e.,

$$I(\boldsymbol{k}; \boldsymbol{c}) = 0. \quad (2)$$

3) *t-threshold security*: for any $\boldsymbol{v} \subseteq \{u_1, u_2, ..., u_n\}$ with $|\boldsymbol{v}| = t$, we have

$$H(\boldsymbol{v}|\boldsymbol{c}) = H(\boldsymbol{v}), \quad (3)$$

where t is a design parameter specified later.

Remark 1. Note that the secrecy capacity of the model in Figure 1, even with a relaxed security condition of $I(\boldsymbol{m}, \boldsymbol{c}) \approx 0$, is zero [1]. In a related work [6], a source of common randomness is required to generate a key with some rate R_k to ensure non-zero secrecy capacity. However, here, a key of a fixed length is used repeatedly. In a sense, this implies that the key rate is zero as the message length grows large. In addition to that, this model aims to look at sub-blocks of the message rather than the entire message. It is worth noting that this model subsumes some well-known security schemes. For example, the perfectly secure one-time-pad (OTP) encryption is a code with threshold $t = m$, hence, we have $H(\boldsymbol{m}|\boldsymbol{c}) = H(\boldsymbol{m})$. Another *keyless* type of work is known as unconditionally-secure all-or-nothing transform (AONT) [20]. Some works study the case where the eavesdropper observes a vector $\boldsymbol{z}$ whose elements are a subset of size $m - t$ of the set of elements of $\boldsymbol{c}$, where $\boldsymbol{c}$ is of length m. The security condition translates to $H(\boldsymbol{v}|\boldsymbol{z}) = H(\boldsymbol{v})$ for all $\boldsymbol{v}$ of size t as in [21].

A formal definition of the threshold security parameter t follows

Definition 1: The threshold security parameter t for an encoder whose input is $\boldsymbol{u}$ and output is $\boldsymbol{c}$ is defined as

$$t = \max(\{|\boldsymbol{v}| \mid \forall \boldsymbol{v} \subseteq \{u_1, u_2, ..., u_n\} \text{ s.t. } H(\boldsymbol{v}|\boldsymbol{c}) = H(\boldsymbol{v})\}). \quad (4)$$

Now, we are ready to define a code that is t-threshold secure code.

Definition 2: We say a code is t-threshold secure if it meets the reliability and security conditions, where t is as defined in Definition 1.

III. Coding Schemes

With a slight abuse of terminology, we refer to a scheme meeting the reliability and security conditions, as described in Section II as a coding scheme. When constructing the coding scheme, we aim to design an encoder and a decoder as well as specifying the code. For an input $\boldsymbol{u} = \pi(\boldsymbol{k}, \boldsymbol{m})$ the encoder produces a codeword $\boldsymbol{c}$ as follows

$$\boldsymbol{c} = \boldsymbol{u}\mathbf{W} = \pi(\boldsymbol{k}, \boldsymbol{m})\mathbf{W} \tag{5}$$

where $\mathbf{W}$ is an $n \times m$ matrix with $n = m + k$. Such matrix is the transpose of a generator matrix $\mathbf{G}$ of a linear block code.

Consider a $[n, m, d_{\min}]_q$ linear code with generator matrix $\mathbf{G}$, i.e., a linear code whose elements are from alphabet of size q, of rate $R = m/n$, and minimum distance $d_{\min}$. In our coding scheme, we require that $n = m + k$ because the channel is noiseless, which implies that there is no need for redundancy symbols. We aim at using $\mathbf{G}$ to produce a matrix $\mathbf{W}$ such that the reliability and security conditions are met. One can assume that the length of the key is less than the length of the message; otherwise, if $k \geqslant m$, then the straightforward perfectly-secure one-time pad meets the conditions for $t = m$. Let us denote the indices of the rows $\mathbf{W}$ that are dedicated for the message as $\mathcal{A} \subseteq [m+k] \overset{\text{def}}{=} \{1, 2, ..., m+k\}$, and the rows dedicated for the the key $\boldsymbol{k}$ as $\mathcal{A}^c = [m+k] \setminus \mathcal{A}$. The codeword $\boldsymbol{c}$ is then expressed as follows:

$$\boldsymbol{c} = \boldsymbol{m}\mathbf{W}_{\mathcal{A}} + \boldsymbol{k}\mathbf{W}_{\mathcal{A}^c}. \tag{6}$$

The choice of $\pi(.)$ which corresponds to the choice of $\mathcal{A}$ and $\mathcal{A}^c$ is critical in ensuring security and reliability conditions. Hence, we have the following definition.

Definition 3: A code, as described above, is called *proper* if its matrix satisfies the following requirements:

1) The resulting submatrix $\mathbf{W}_{\mathcal{A}}$ is full row rank, i.e., $\text{rank}(\mathbf{W}_{\mathcal{A}}) = m$.
2) The resulting submatrix $\mathbf{W}_{\mathcal{A}^c}$ is also full row rank, i.e., $\text{rank}(\mathbf{W}_{\mathcal{A}^c}) = k$.

An example of codes that are not *proper* is the turbo code [22] whose generator matrix can be written in the form $\mathbf{G} = [\mathbf{I}_m \ \mathbf{A}_1 \ \mathbf{A}_2]$ where $\mathbf{I}_m$ is the identity matrix whose columns are dedicated to the message while the rest is dedicated for the key. It is known that $\mathbf{A}_2$ is some row-permuted version of $\mathbf{A}_1$, where such permutation may not necessarily result in $[\mathbf{A}_1 \ \mathbf{A}_2]^T$ being a full row-rank matrix, hence it shows that such code is not *proper*. A code that is not *proper* will result in a lower equivocation rate for Eve about the message as will be evident throughout this section.

Next, we show that if the code is *proper*, then it meets the reliability condition, as specified in (1), and the key security conditions, as specified in (2) and (3). The following lemma shows that the reliability condition is satisfied:

Lemma 1: Assuming the code is *proper*, as defined in Definition 3, Bob can recover the message with probability one under maximum a posteriori (MAP) decoding. In other words,

$$H(\boldsymbol{m}|\boldsymbol{c}, \boldsymbol{k}) = 0. \tag{7}$$

Proof: We use (6) to show that if Bob has $\boldsymbol{c}$ and $\boldsymbol{k}$, and since $\mathbf{W}_{\mathcal{A}}$ is full rank, then Bob can subtract $\boldsymbol{k}\mathbf{W}_{\mathcal{A}^c}$ from $\boldsymbol{c}$ then find $\boldsymbol{m}$ from $\mathbf{W}_{\mathcal{A}}$, which has a unique solution. ■

In the next theorem, we show that a *proper* code meets the key security condition, as specified in (2). Note that this condition is crucial as even a very small leakage of the key $\boldsymbol{k}$ can lead to the entire key being revealed to Eve, after using the scheme several times, thereby compromising the security of the message.

Theorem 2: Assuming the code is *proper*, as defined in Definition 3, the codeword $\boldsymbol{c}$, with elements from alphabet of size q, leaks no information about the key $\boldsymbol{k}$, i.e.,

$$I(\boldsymbol{k}; \boldsymbol{c}) = 0 \tag{8}$$

Proof: The proof is by observing the following set of equalities:

$$\begin{aligned} I(\boldsymbol{k}; \boldsymbol{c}) &= H(\boldsymbol{c}) - H(\boldsymbol{c}|\boldsymbol{k}) && (9)\\ &= m\log_2(q) - H(\boldsymbol{m}\mathbf{W}_{\mathcal{A}} + \boldsymbol{k}\mathbf{W}_{\mathcal{A}^c}|\boldsymbol{k}) && (10)\\ &= m\log_2(q) - H(\boldsymbol{m}\mathbf{W}_{\mathcal{A}}) && (11)\\ &= \log_2(q)(m - \text{rank}(\mathbf{W}_{\mathcal{A}})) && (12)\\ &= 0, && (13) \end{aligned}$$

where (10) holds by (6) and the uniformity of the key and message symbols, (11) holds because $\boldsymbol{m}$ and $\boldsymbol{k}$ are independent, (12) is by noting that elements of $\boldsymbol{m}$ are uniformly distributed and independent, and (13) holds because $\text{rank}(\mathbf{W}_{\mathcal{A}}) = m$ since the encoder is *proper*, as mentioned in Definition 3. ■

The following well-known lemma is instrumental in characterizing the threshold security of the linear-code-based scheme:

Lemma 3: [23] For a $[n, m, d_{\min}]_q$ linear code with generator matrix $\mathbf{G}$, any submatrix of $\mathbf{G}$ of size $m \times (n - s)$ obtained by deleting some columns indexed by $\mathcal{D} \subseteq [n]$ such that $|\mathcal{D}| = s$, where $s = d_{\min} - 1$, has full row rank, i.e.,

$$\text{rank}(\mathbf{G}_{\mathcal{D}^c}) = m. \tag{14}$$

Proof: This is a direct consequence of the fact that decoding is successful for any number of erasures up to $s = d_{\min} - 1$. ■

Theorem 4: A code generated by a matrix $\mathbf{W}$, which is the transpose of a generator matrix $\mathbf{G}$ of a $[n, m, d_{\min}]_q$ linear code, satisfies

$$H(\boldsymbol{v}|\boldsymbol{c}) = H(\boldsymbol{v}), \tag{15}$$

for any $\boldsymbol{v} \subseteq \{u_1, u_2, ..., u_n\}$ such that $|\boldsymbol{v}| = t = d_{\min} - 1$.

Proof: Let us denote $\boldsymbol{v}$ with elements of $\boldsymbol{u}$ indexed by $\mathcal{B} = \{i_1, i_2, ..., i_t\} \subseteq [n]$, and $\tilde{\boldsymbol{u}}$ with elements of $\boldsymbol{u}$ indexed by $\mathcal{B}^c = [n] \setminus \mathcal{B}$. Then we have the following:

$$
\begin{aligned}
I(\boldsymbol{v};\boldsymbol{c}) &= H(\boldsymbol{c}) - H(\boldsymbol{c}|\boldsymbol{v}) && (16)\\
&= m\log_2(q) - H(\tilde{\boldsymbol{u}}\mathbf{W}_{\mathcal{B}^c} + \boldsymbol{v}\mathbf{W}_{\mathcal{B}}|\boldsymbol{v}) && (17)\\
&= m\log_2(q) - H(\tilde{\boldsymbol{u}}\mathbf{W}_{\mathcal{B}^c}) && (18)\\
&= \log_2(q)(m - \mathrm{rank}(\mathbf{W}_{\mathcal{B}^c})) && (19)\\
&= 0, && (20)
\end{aligned}
$$

where (17) follows because of uniformity of codewords and expansion of random variables, (18) is due to the independence of $\boldsymbol{v}$ and $\tilde{\boldsymbol{u}}$, (19) holds due to the uniformity of $\tilde{\boldsymbol{u}}$, and (20) holds due to the property of the generator matrix of the linear code as mentioned in Lemma 3 if $t = d_{\min} - 1$. Since the mutual information is zero, then it implies that the t-threshold security criteria is met for parameter $t = d_{\min} - 1$, i.e.,

$$H(\boldsymbol{v}|\boldsymbol{c}) = H(\boldsymbol{v}), \quad (21)$$

for any $\boldsymbol{v}$ such that $|\boldsymbol{v}| = t = d_{\min} - 1$.

Next, we need to show that $t = d_{\min} - 1$ is the maximum for which the security condition holds. To prove this, we need to show this condition does not hold for some $\boldsymbol{v}$ if $t > d_{\min} - 1$. Consider a codeword generated by the linear code that has the minimum Hamming weight with non-zero elements at indices denoted by $\mathcal{F} = \{i_1, i_2, ..., i_{d_{\min}}\}$. Then we have the following:

$$
\begin{aligned}
H(u_{i_1}, ..., u_{i_{d_{\min}}}|\boldsymbol{c}) &= H(u_{i_1}, ..., u_{i_{d_{\min}-1}}|\boldsymbol{c})\\
&\quad + H(u_{i_{d_{\min}}}|\boldsymbol{c}, u_{i_1}, ..., u_{i_{d_{\min}-1}}) && (22)\\
&= H(u_{i_1}, ..., u_{i_{d_{\min}-1}}|\boldsymbol{c}) && (23)\\
&\neq H(u_{i_1}, ..., u_{i_{d_{\min}}}), && (24)
\end{aligned}
$$

where (22) follows from the chain rule of entropy, and (23) follows because there exists some linear combination of $\{c_1, c_2, ..., c_m\}$, which are elements of the vector $\boldsymbol{c}$, such that the eavesdropper can find $\sum_{i=1}^{m} \lambda_i c_i = \sum_{j\in\mathcal{F}} u_j$. Hence the second term becomes zero, since there is no uncertainty about $u_{i_{d_{\min}}}$ given $\boldsymbol{c}$ and $\{u_{i_1}, ..., u_{i_{d_{\min}-1}}\}$. Therefore, as in (24), the relationship does not hold for $d_{\min}$ and we conclude that $t = d_{\min} - 1$. ■

Corollary 5: For any t-threshold secure coding scheme, constructed from linear block codes, of message length m, key length k, and code length $n = m + k$, we have $t \leqslant k$.

Proof: The proof follows by Theorem 4 and Singleton bound. ■

Next, we characterize Eve's equivocation about the entire message $\boldsymbol{m}$ after observing the codeword as follows

Corollary 6: If the code is *proper*, then the passive eavesdropper Eve's equivocation about the entire encoded message $\boldsymbol{m}$ after observing the codeword is equal to the entropy of the key, i.e.,

$$H(\boldsymbol{m}|\boldsymbol{c}) = k\log_2(q). \quad (25)$$

Proof: We have the following

$$
\begin{aligned}
H(\boldsymbol{m}|\boldsymbol{c}) &= H(\boldsymbol{m}) - H(\boldsymbol{c}) + H(\boldsymbol{c}|\boldsymbol{m}) && (26)\\
&= H(\boldsymbol{k}\mathbf{W}_{\mathcal{A}^c} + \boldsymbol{m}\mathbf{W}_{\mathcal{A}}|\boldsymbol{m}) && (27)\\
&= H(\boldsymbol{k}\mathbf{W}_{\mathcal{A}^c}) && (28)\\
&= k\log_2(q) && (29)
\end{aligned}
$$

where (27) follows due to the uniformity of messages and codewords, and expansion of random vectors, (28) holds because of independence of $\boldsymbol{m}$ and $\boldsymbol{k}$, and (29) holds because the matrix $\mathbf{W}_{\mathcal{A}^c}$ is full row rank, since the code is *proper*. This results in probability of successfully retrieving the entire message block by Eve of q^{-k}. ■

Now that we have shown the properties that the proposed coding scheme satisfies, we need to show that such coding schemes exist, while maximizing the threshold t as stated in Corollary 5, provided that q is large enough. To prove the existence of such codes, we utilize maximum distance separable (MDS) codes to arrive at the following theorem.

Theorem 7: For any message length m and key length k, there exists a *proper* code with threshold $t = k$, provided that the alphabet size $q \geqslant m + k + 1$.

Proof: To prove the theorem, we give an example of a code that is shown to be *proper* with $t = k$. We utilize Reed-Solomon (RS) codes, which are a well-known family of codes that are maximum distance separable (MDS) codes, i.e., $d_{\min} = n - m + 1 = k + 1$ [23]. For any $[n, m, d_{\min}]_q$ RS code, all we need to show is that the matrix $\mathbf{W}$ which is the transpose of the generator matrix $\mathbf{G}$ of the RS code can be used to construct a *proper* code. One of the properties of MDS codes is that every set of m columns of the matrix $\mathbf{G}$ are linearly independent [23, Proposition 11.4]. Rows of $\mathbf{W}$ correspond to columns of $\mathbf{G}$, hence, any choice of m columns of $\mathbf{G}$ will have rank m, and the remaining $k < m$ columns of $\mathbf{G}$ will also have rank k. Therefore, The code generated by $\mathbf{W}$ is *proper*, with threshold $t = k$. ■

Remark 2. Randomization of the codeword corresponding to a specific message is possible by shortening the message $\boldsymbol{m}$ and adding some random symbols $\boldsymbol{s}$, and feeding the new vector $\bar{\boldsymbol{m}} = \pi_1(\boldsymbol{m}, \boldsymbol{s})$ as the message to the encoder.

IV. Low-Complexity Construction

In this section, we focus on designing codes to meet the reliability and security conditions while providing a linear/quasi-linear complexity for encoding and decoding. To this end, we consider Reed-Muller (RM) codes due to their recursive construction and low-complexity decoder. In addition, since they are designed with the objective of maximizing the minimum distance, given the particular recursive structure, we can achieve high threshold t for the t-threshold security.

A. Encoder

First, we briefly describe Reed-Muller codes. A RM(r,s) is a $[2^s, \sum_{i=0}^{r}\binom{s}{i}, 2^{s-r}]_2$ linear code whose generator matrix $\mathbf{G}$ can be generated by keeping the rows with the Hamming weight of at least 2^{s-r} from the matrix $\mathbf{F}^T = (\mathbf{F}_2^{\otimes s})^T$, where $\otimes$ denotes the Kronecker product, T is the transpose operator, and $\mathbf{F}_2$ is the following kernel matrix

$$\mathbf{F}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \tag{30}$$

It is well-known that Reed-Muller codes are built recursively using different constructions [23]. Though there are different ways of constructing such generator matrix, the above description helps us choose the message and bit indices, which is the next step towards designing a code that is *proper*. Due to the recursive structure of $\mathbf{F}$, it is straightforward to see that indices of rows with lowest weight from $\mathbf{F}$ correspond to indices with columns with highest column weight from $\mathbf{F}$ and vice versa. When building the matrix $\mathbf{G}$ from $\mathbf{F}^T$ we choose the set of indices of the rows deleted as $\mathcal{A}^c$ to denote the rows of $\mathbf{W}$ dedicated for the key, while the rest are used as the message indices $\mathcal{A}$. Hence, we have the following proposition

Proposition 8: The choice of the sets $\mathcal{A}$, and $\mathcal{A}^c$ as mentioned above results in a *proper* code.

Proof: To prove this proposition, it suffices to show that $\mathbf{W}_{\mathcal{A}}$ and $\mathbf{W}_{\mathcal{A}^c}$ are both full row rank.

First, we start by showing $\mathbf{W}_{\mathcal{A}}$ is full row rank. This can be easily seen as $\mathcal{A}^c$ denotes deleted columns and rows dedicated for the key from $\mathbf{F}$. For a triangular matrix, the submatrix generated by removing any columns and rows with the same indices results in a triangular matrix. Hence, $\mathbf{W}$ contains m columns indexed by $\mathcal{A}$, and after removing the rows with the indices $\mathcal{A}^c$, the resulting matrix is triangular and full row rank. Hence, the first condition is satisfied, i.e., the matrix $\mathbf{W}_{\mathcal{A}}$ is full row rank.

As for the matrix $\mathbf{W}_{\mathcal{A}^c}$ being full row rank, we will show it using induction. But first, we require $k \leqslant m$ as we mentioned before. We re-write the parameters $k = \sum_{i=0}^{r} \binom{s}{i}$, and $m = \sum_{i=r+1}^{s} \binom{s}{i}$. This also leads to having, at most, $r = \left\lfloor \frac{s-1}{2} \right\rfloor$. From the $2^s \times 2^s$ matrix $\mathbf{F}$, let us have a submatrix $\mathbf{W}_{\mathcal{A}^c} = \mathbf{F}(s,r)$ which contains the $\sum_{i=0}^{r} \binom{s}{i}$ rows dedicated for the key from $\mathbf{F}$ with same number of lowest-weight columns removed. Let us also have another matrix $\mathbf{F}'(s,r)$ which contains the $\sum_{i=0}^{r} \binom{s}{i}$ rows dedicated for the key from $\mathbf{F}$ with only $\sum_{i=0}^{r-1} \binom{s}{i}$ lowest weight columns removed. Due to the structured construction of the matrix $\mathbf{F}$, it can be easily seen that we can express $\mathbf{F}(s,r)$ as follows:

$$\mathbf{F}(s,r) = \begin{bmatrix} \mathbf{F}(s-1,r-1) & \mathbf{0} \\ \mathbf{F}'(s-1,r) & \mathbf{F}(s-1,r) \end{bmatrix} \tag{31}$$

where the row rank of this matrix is the sum of the row rank of $[\mathbf{F}(s-1,r-1) \;\; \mathbf{0}]$ and $[\mathbf{F}'(s-1,r) \;\; \mathbf{F}(s-1,r)]$ due to their intersection being the zero vector, which can be directly seen because of $\mathbf{F}(s-1,r)$. Next, we prove that the matrix $\mathbf{F}(s,r)$ is full row rank.

Now, we now state our claim: the matrix $\mathbf{F}(s,r)$ is full row rank for $s \geqslant 2$, i.e., $\text{rank}(\mathbf{F}(s,r)) = \sum_{i=0}^{r} \binom{s}{i}$.

Step 1: We show the base cases hold for $s = 2$ and $r = 0$, then for $s = 3$ and $r = 1$. For $s = 2$ and $r = 0$, the rank of the matrix $\mathbf{F}(2,0)$ is 1. As for $s = 3$ and $r = 1$ the rank of the matrix $\mathbf{F}(3,1)$ is 4. Hence the two base cases are validated.

Step 2: We state our induction hypothesis. Let us assume that matrix $\mathbf{F}(s,r)$ has full row rank for $s \geqslant 2$.

Step 3: First, for odd s with corresponding parameter r, we have the following matrix:

$$\mathbf{F}(s+1,r) = \begin{bmatrix} \mathbf{F}(s,r-1) & \mathbf{0} \\ \mathbf{F}'(s,r) & \mathbf{F}(s,r). \end{bmatrix} \tag{32}$$

We need to show that $\text{rank}(\mathbf{F}(s+1,r)) = \sum_{i=0}^{r} \binom{s+1}{i}$. First, let us start with $\mathbf{F}(s,r)$, which is full row rank based on our induction hypothesis, i.e., $\text{rank}(\mathbf{F}(s,r)) = \sum_{i=0}^{r} \binom{s}{i}$. As for $\mathbf{F}(s,r-1)$, which contains a subset of the rows in $\mathbf{F}(s,r)$ with additional columns, it is also full row rank because $\mathbf{F}(s,r)$ is full row rank according to our induction hypothesis. Hence, we have $\text{rank}(\mathbf{F}(s,r-1)) = \sum_{i=0}^{r-1} \binom{s}{i}$. Therefore,

$$\begin{aligned} \text{rank}(\mathbf{F}(s+1,r)) &= \text{rank}(\mathbf{F}(s,r-1)) \\ &\quad + \text{rank}(\mathbf{F}(s,r)) \quad (33) \\ &= \sum_{i=0}^{r-1} \binom{s}{i} + \sum_{i=0}^{r} \binom{s}{i} \quad (34) \\ &= \sum_{i=0}^{r} \binom{s+1}{i} \quad (35) \end{aligned}$$

which is equal to the number of rows in $\mathbf{F}(s+1,r)$. Hence it is full row rank.

As for even s with corresponding parameter r, we need to show the following matrix is full row rank

$$\mathbf{F}(s+1,r+1) = \begin{bmatrix} \mathbf{F}(s,r) & \mathbf{0} \\ \mathbf{F}'(s,r+1) & \mathbf{F}(s,r+1) \end{bmatrix} \tag{36}$$

First, we have $\text{rank}(\mathbf{F}(s,r)) = \sum_{i=0}^{r} \binom{s}{i}$ which holds based on our induction hypothesis. As for $\text{rank}(\mathbf{F}'(s,r+1))$, we can see that the matrix $\mathbf{F}'(s,r+1)$ has $\sum_{i=0}^{r} \binom{s}{i}$ rows that are in $\mathbf{F}(s,r)$, however, when considering such rows in the matrices $[\mathbf{F}(s,r) \;\; \mathbf{0}]$ and $[\mathbf{F}'(s,r+1) \;\; \mathbf{F}(s,r+1)]$ such rows are independent from all other rows in $[\mathbf{F}(s,r) \;\; \mathbf{0}]$ due to the intersection of the subspaces spanned by rows of the two matrices being the zero vector. In addition to that, there are $\binom{s}{r+1}$ additional rows in $\mathbf{F}'(s,r+1)$ that are linearly independent from the remaining rows due to the structure of the zero blocks in such matrix which is of similar fashion to (31). We can find the rank of $\mathbf{F}(s+1, r+1)$ as follows

$$\begin{aligned}\operatorname{rank}(\mathbf{F}(s+1, r+1)) &= \operatorname{rank}(\mathbf{F}(s, r)) \\ &\quad + \operatorname{rank}(\mathbf{F}'(s, r+1)) \qquad (37)\\ &= \sum_{i=0}^{r}\binom{s}{i} + \sum_{i=0}^{r}\binom{s}{i} \\ &\quad + \binom{s}{r+1} \qquad (38)\\ &= \sum_{i=0}^{r}\binom{s}{i} + \sum_{i=0}^{r+1}\binom{s}{i} \qquad (39)\\ &= \sum_{i=0}^{r+1}\binom{s+1}{i}. \qquad (40)\end{aligned}$$

Hence, $\mathbf{F}(s+1, r+1)$ is full row rank, and the statement is verified by induction for the maximum length key, i.e., $r = \left\lfloor \frac{s-1}{2} \right\rfloor$. For shorter keys, it is straightforward to see that for any $r' < r$, a matrix $\mathbf{F}(s, r')$ whose rows are a subset of the $\mathbf{F}(s, r)$ rows with additional columns appended at different locations, such matrix is still full row rank.

Therefore, such choice of rows dedicated for the key and the message bits results in a *proper* code. ■

It is worth noting that such construction of the matrix $\mathbf{W}$ is closely related to the construction of the generator matrix for polar codes [24]. For polar codes, choice of rows to be removed from the matrix $\mathbf{F}$ is done according to some parameter that is calculated recursively. As for Reed-Muller codes as described, the Hamming weight of rows can be calculated in a similar recursive manner as polar code parameters due to the structure of the matrix. This approach has been shown to be done in quasi-linear time complexity [24].

B. Decoder

The decoder used to decode the message utilizing the shared key is known as the successive-cancellation decoder. Again, as Reed-Muller codes are closely related to the polar codes, a decoder similar to the one described in [24] is used here. For the above coding scheme, we describe the decoder to retrieve $\boldsymbol{u} = \pi(\boldsymbol{k}, \boldsymbol{m})$, which can then be used to retrieve the message bits. The decoder described in Algorithm 1 takes the key bits $\boldsymbol{k}$ the codeword $\boldsymbol{z} = \boldsymbol{z}_1^n = \pi(\boldsymbol{e}_k, \boldsymbol{c})$, indices of the key bits $\mathcal{A}^c$ and a recursion index i as inputs, and outputs the vector $\boldsymbol{u} = [u_1, u_2, ..., u_n] = \pi(\boldsymbol{k}, \boldsymbol{m})$ from which the message can be retrieved $\boldsymbol{m} = \boldsymbol{u}_{\mathcal{A}}$, and $\boldsymbol{h}_1^n = \boldsymbol{u}\mathbf{F}^{\otimes \log_2(n)}$.

The following claim verifies that the decoder successfully outputs the message bits with probability 1 for any key length.

Claim 9: The coding construction described can be successfully decoded using the aforementioned successive-cancellation decoder for any key length k.

Proof: First, let us denote the input to the successive cancellation decoder as the codeword including the erasures $\boldsymbol{z}_1^n = \pi(\boldsymbol{e}_k, \boldsymbol{c}) = [\boldsymbol{z}_1^{n/2}, \boldsymbol{z}_{n/2+1}^n]$ where $\boldsymbol{c}$ is the codeword, $\boldsymbol{e}_k$ is an erasure vector of length k at locations denoted by $\mathcal{A}^c$, which as mentioned before corresponds to the location of the key bits at the encoder. The vector $\boldsymbol{z}$ is divided into two halves: $\boldsymbol{z}_1^{n/2} = [z_1, z_2, ..., z_{n/2}]$ and $\boldsymbol{z}_{n/2+1}^n = [z_{n/2+1}, z_{n/2+2}, ..., z_n]$ to be decoded recursively. We use induction hypothesis to show such claim as follows:

Algorithm 1 Successive-cancellation decoder

Initialization: $i = 1$.
Input: $\boldsymbol{k}$, $\boldsymbol{z}_1^n = \pi(\boldsymbol{e}_k, \boldsymbol{c})$, $\mathcal{A}^c$, i.
Output: $\boldsymbol{h}_1^n$, $\boldsymbol{u} = [u_1, u_2, ...u_n]$.
if $n = 2$ **then**
  if $z_2 = e$ **then**
    $u_i = k_i$
  else
    $u_i = z_2$
  end if
  if $z_1 = e$ **then**
    $u_{i-1} = k_{i-1}$
  else
    $u_{i-1} = u_i \oplus z_1$
  end if
  $\boldsymbol{h}_1^n = [u_{i-1} \oplus u_i, u_i]$
else
  $\boldsymbol{h}' \leftarrow$ Decoder($\boldsymbol{k}_2, \boldsymbol{z}_{n/2+1}^n, \mathcal{A}_2^c, 2i$)
  $\bar{\mathbf{z}}_1^{n/2} = \mathbf{z}_1^{n/2} \oplus \boldsymbol{h}'$
  $\boldsymbol{h}'' \leftarrow$ Decoder($\boldsymbol{k}_1, \bar{\mathbf{z}}_1^{n/2}, \mathcal{A}_1^c, 2i-1$)
  $\boldsymbol{h}_1^n = [\boldsymbol{h}'' \oplus \boldsymbol{h}', \boldsymbol{h}']$
end if
return $\boldsymbol{h}_1^n$

Step 1: For our base step, let us have $n = 2^1$. We need to show decoding is successful for any k. We start with $k = 0$, i.e., no erasures at the input of the decoder. We build a binary tree where the right leaf is $z_2 = c_2 = u_2$, then we find $u_1 = z_1 \oplus z_2$. Now, we show it succeeds for $k = 1$ for both possible cases for $\mathcal{A}^c$. First, let us consider that $z_1 = e$ and $z_2 = c_1$, which corresponds to $u_1 = k_1$, and $u_2 = m_1$. In this case, the decoder outputs $u_1 = k_1$ and $u_2 = z_2$. For the other case where $z_1 = c_1$ and $z_2 = e$, which corresponds to $u_1 = m_1$, and $u_2 = k_1$. The decoder first corrects the erasure, assigning $u_2 = k_1$, then computes $u_1 = m_1 = u_2 \oplus z_1 = k_1 \oplus z_1$. Finally, we show it succeeds for $k = 2$ where both z_1 and z_2 are erased, then $u_1 = k_1$ and $u_2 = k_2$ and the decoder is successful.

Step 2: Now, we state our induction hypothesis. Let us assume that our statement in the claim is correct for $n = 2^l$ and for any k erasures and k key bits at locations $\mathcal{A}^c$, i.e., the decoder is successful for any k erasures and k key bits.

Step 3: We now show that the claim is true for $n = 2^{l+1}$ and any $k = i + j$. Let us split the key indices $\mathcal{A}^c$ into two sets, $\mathcal{A}_1^c$ and $\mathcal{A}_2^c$, with sizes $|\mathcal{A}_1^c| = i$ and $|\mathcal{A}_2^c| = j$. The set

$\mathcal{A}_1^c$ contains the indices of the key bits $\boldsymbol{k}_1$ in $\boldsymbol{z}_1^{n/2}$, and $\mathcal{A}_2^c$ contains the indices of the key bits $\boldsymbol{k}_2$ in $\boldsymbol{z}_{n/2+1}^n$. First, we start with the right leaf of the binary tree, i.e., $\boldsymbol{z}_{n/2+1}^n$, which has j erasures and j known key bits located at $\mathcal{A}_2^c$. The decoder is then run on this leaf, which has an input of length $n' = 2^l$ and $k = j$ erasures and key bits $\boldsymbol{k}_2$ located at $\mathcal{A}_2^c$. The decoder succeeds according to our induction hypothesis. The right leaf then passes $\boldsymbol{u}_{n/2+1}^n \mathbf{G}^{\otimes l} \oplus \boldsymbol{z}_1^{n/2} = \boldsymbol{h}' \oplus \boldsymbol{z}_1^{n/2} = \bar{\boldsymbol{z}}_1^{n/2}$ to the left leaf. The decoder is then run on $\bar{\boldsymbol{z}}_1^{n/2}$, which is of length $n' = 2^l$ and has i erasures and i known key bits $\boldsymbol{k}_1$ both are located at $\mathcal{A}_1^c$. The decoder is successful on this leaf based on our induction hypothesis. Hence, the decoder is successful for $n = 2^{l+1}$. Therefore, by induction, the claim is proven. ■

V. Conclusion

In this work, we propose a model for threshold-secure coding with a shared key such that specific conditions for reliability and security based on information-theoretic measures are met. The specification of such model includes a threshold parameter which is to be designed based on the application for such coding scheme. In addition to that, a novel method utilizing error-correcting linear codes for constructing threshold-secure coding schemes is introduced, where the threshold parameter t is shown to be directly related to the minimum distance of the linear code. Furthermore, a low-complexity coding scheme based on Reed-Muller linear codes was described. Its encoder is generated recursively and has been shown to satisfy the conditions for a *proper* code. The successive-cancellation decoder was also described, and its success has also been shown.

A possible directions for future work is to design coding schemes based on punctured Reed-Muller codes to allow for more flexible rates. Moreover, studying t-threshold-secure coding schemes in combination with noisy physical layer channels in order to design protocols that can correct errors of physical layer while providing threshold security is another future direction.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," in *2007 IEEE International Symposium on Information Theory*. IEEE, 2007, pp. 1306–1310.

[3] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[4] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[5] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[6] W. Kang and N. Liu, "Wiretap channel with shared key," in *2010 IEEE Information Theory Workshop*. IEEE, 2010, pp. 1–5.

[7] W. Zhang, C. Zhang, W. Jin, C. Chen, N. Jiang, and K. Qiu, "Chaos coding-based QAM IQ-encryption for improved security in OFDMA-PON," *IEEE Photonics Technology Letters*, vol. 26, no. 19, pp. 1964–1967, 2014.

[8] F. Huo and G. Gong, "A new efficient physical layer OFDM encryption scheme," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*. IEEE, 2014, pp. 1024–1032.

[9] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an OFDM physical layer encryption scheme," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2114–2127, 2017.

[10] M. Tahir, S. P. Jarot, and M. Siddiqi, "Wireless physical layer security using encryption and channel pre-compensation," in *2010 International Conference on Computer Applications and Industrial Electronics*. IEEE, 2010, pp. 304–309.

[11] A. Zuquete and J. Barros, "Physical-layer encryption with stream ciphers," in *2008 IEEE International Symposium on Information Theory*. IEEE, 2008, pp. 106–110.

[12] X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *2009 3rd International Conference on Signal Processing and Communication Systems*. IEEE, 2009, pp. 1–5.

[13] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE transactions on wireless communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[14] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *Coding Thv*, vol. 4244, pp. 114–116, 1978.

[15] C. N. Mathur, K. Narayan, and K. Subbalakshmi, "High diffusion cipher: Encryption and error correction in a single cryptographic primitive," in *International Conference on Applied Cryptography and Network Security*. Springer, 2006, pp. 309–324.

[16] Y.-S. Kim, J.-H. Kim, and S.-H. Kim, "A secure information transmission scheme with a secret key based on polar coding," *IEEE communications letters*, vol. 18, no. 6, pp. 937–940, 2014.

[17] N. Cai and R. W. Yeung, "Secure network coding," in *Proceedings IEEE International Symposium on Information Theory,*. IEEE, 2002, p. 323.

[18] K. Bhattad, K. R. Narayanan *et al.*, "Weakly secure network coding," in *Proceedings First Workshop on Network Coding, Theory, and Applications (NetCod)*, 2005.

[19] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," MIT Lexington Lincoln Lab, Tech. Rep., 1953.

[20] D. R. Stinson, "Something about all or nothing (transforms)," *Designs, Codes and Cryptography*, vol. 22, no. 2, pp. 133–138, 2001.

[21] N. N. Esfahani, I. Goldberg, and D. R. Stinson, "Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 3136–3143, 2017.

[22] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," in *Proceedings of ICC'93-IEEE International Conference on Communications*, vol. 2. IEEE, 1993, pp. 1064–1070.

[23] R. Roth, *Introduction to coding theory*. Cambridge University Press, 2006.

[24] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.