Exact Equivocation Expressions for Wiretap Coding over Erasure Channel Models

Willie K. Harrison, *Senior Member, IEEE*

***Abstract*—Traditional security analysis of wiretap codes requires evaluation of equivocation in the asymptote as the code blocklength tends to infinity. Finite blocklength codes, however, require exact expressions for equivocation so as to allow for comparison of parameterized codes across different code constructions or within the same construction. In this paper, we present two exact equivocation expressions for coset coding over the wiretap channel model with binary erasure channels (BECs) for both the main channel and the eavesdropper's channel. The expressions are functions of the algebraic structure of the binary wiretap codes, and they also hold for the special case when the main channel is noiseless.**

***Index Terms*—Information theoretic security, wiretap codes, finite blocklength analysis, binary erasure channels.**

I. Introduction

Security efforts at the physical-layer of a communication system are known to be capable of providing a standalone layer of protection against eavesdropping [1], [2] that can also enhance security at other layers in the protocol stack [3], [4]. Recent results have further shown the potential for physical-layer security techniques in real-world environments. Achieving secure communication over real wireless channels requires strategic antenna placement, precise control of the transmit power, and appropriate application of wiretap coding [5].

Analysis of the security gained through wiretap coding has traditionally been accomplished with either weak, strong, or semantic secrecy metrics (see [6], [7] and references). Each of these metrics is information theoretic in nature; however, each metric lends itself to security analysis only in the asymptotic blocklength regime. Real-world application of secrecy coding, especially when smaller blocklength codes are deployed, requires the security analysis to be applied over the finite blocklength regime. A few works have provided bounds for security measures at finite blocklength [8], [9], but these bounds are quite loose for small blocklength codes, and do not directly take into account the algebraic structure of the code. Exact expressions of security for specific wiretap codes can be used to identify *best* codes [10], [11], and thereby discover the ultimate achievable limits of wiretap coding in practice. If these expressions can be linked to the algebraic structure of the code, their value increases, as the results can guide overarching design principles for constructing better codes.

In this paper, we provide two expressions for measuring the exact amount of information theoretic security for binary coset codes designed to operate over networks with binary erasure channels (BECs) connecting the transmitter and legitimate receiver as well as the transmitter and an eavesdropper. These expressions are functions of the algebraic structure of the wiretap code constructions, and are generalized forms of the expressions that apply when the intended receiver has a noiseless channel. High-level design principles to find better/best codes are then inferred from the expressions.

II. Preliminaries

A. Channel Model

Let M be a secret message chosen uniformly at random over the alphabet $\mathcal{M} = \{1, 2, \ldots, 2^k\}$. Alice wishes to communicate M to Bob while leaking as little information as possible to an eavesdropper named Eve. Alice encodes M into a length-n codeword X^n, which is transmitted. Bob observes Y^n through the *main channel* of communication and decodes the message to form $\hat{M}$, while Eve observes Z^n through the *eavesdropper's channel* of communication. This channel model is known as the *wiretap channel model*, and the first version of this model was published in [1]. For this work, both the main channel and the eavesdropper's channel are BECs, where input bits are *erased* independently with probabilities ϵ_m and ϵ_e over the respective channels.

Communication over the wiretap channel model is done with two goals in mind:

1) reliability for Bob, i.e., $\Pr(\hat{M} \neq M) < \delta_m$, and
2) security against Eve, i.e., $\mathbb{H}(M) - \mathbb{H}(M|Z^n) < \delta_e$,

where δ_m and δ_e are small and chosen by the code designer, $\mathbb{H}(\cdot)$ is the usual average entropy function [12], and $\mathbb{H}(M) - \mathbb{H}(M|Z^n)$ is the *exact* average leakage to the eavesdropper rather than a weaker asymptotic metric. The security metric

$$\Delta = \mathbb{H}(M|Z^n) = \sum_{z^n \in \mathcal{Z}^n} p(z^n)\mathbb{H}(M|Z^n = z^n) \qquad (1)$$

is termed the *average equivocation*, where z^n is a realization of Z^n, $p(z^n)$ is the probability mass function of Z^n, and $\mathcal{Z}^n$ is the range of Z^n. Clearly, the security constraint is satisfied to a greater degree as Δ is made closer to $\mathbb{H}(M)$. This paper provides two expressions for calculating the exact equivocation $\mathbb{H}(M|Z^n = z^n)$ based only on algebraic properties of a coset-style wiretap code, which can be used to obtain Δ in (1). Such expressions are valuable, since they yield insights into good finite blocklength code design, and are easy to compute [2]. For small codes, our expressions can be used to calculate Δ exactly by summing over all possible $z^n \in \mathcal{Z}^n$. For larger codes the expressions can be used, along with Monte Carlo simulations, to estimate $\mathbb{H}(M|Z^n)$ as outlined in [13]. Further

W. K. Harrison is with the Department of Electrical and Computer Engineering, Brigham Young University, Provo, UT, 84602 USA e-mail: willie.harrison@byu.edu.

This work was funded by the US National Science Foundation: Grant Award Number #1910812.

Manuscript received May XX, 2020; revised XXX XX, XXXX.

note that our techniques may also be used to evaluate the worst case exact equivocation as is done for wiretap channels of type II (e.g., see [14], [15]).

B. Coding for Secrecy

In this paper, we consider a coset-coding structure that is capable of keeping secrets and correcting errors over BECs. The basic code structure was first presented in [16] and two-edge type low-density parity-check (LDPC) codes were applied to the structure later in [17] (see also [6], [18]). Let

$$H = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix} \tag{2}$$

be an $n(1-R) \times n$ parity check matrix, and H_1 be an $n(1-R_1) \times n$ parity check matrix, where $R_1 > R$. H defines the code $\mathcal{C}$ with generator matrix G, and H_1 defines the code $\mathcal{C}_1$ with generator matrix

$$G_1 = \begin{bmatrix} G' \\ G \end{bmatrix}. \tag{3}$$

Here G' is an $n(R_1 - R) \times n$ matrix, which must have linearly independent rows not in $\mathcal{C}$ so as to form a full-rank generator G_1. Of course $GH^T = 0$ and $G_1 H_1^T = 0$, as expected.

The encoding of an $n(R_1 - R) = k$ bit message is accomplished by

$$x^n = \begin{bmatrix} m & v \end{bmatrix} G_1 = \begin{bmatrix} m & v \end{bmatrix} \begin{bmatrix} G' \\ G \end{bmatrix} = mG' + vG, \tag{4}$$

where v is an auxiliary message comprised of nR bits chosen uniformly at random from $\mathbb{F}_2^{nR}$. Effectively, the rows of G form a basis of a linear block code $\mathcal{C}$, and G' allows one to map onto a subset of the cosets of $\mathcal{C}$ using (4). The portion of x^n that is mG' chooses the coset, while the portion vG randomizes the codeword within the prescribed coset.

If G_1 is $n \times n$, then the code allows no error correction since $R_1 = 1$, and every n-tuple in $\mathbb{F}_2^n$ is a valid codeword; thus, H_1 has zero rows. This forms a special case that is often used when the main channel is noiseless. Assuming $R_1 < 1$, the decoder first corrects errors using H_1 as the parity check matrix to form an estimate $\hat{x}^n$ of the transmitted codeword x^n. For a BEC, this can be accomplished efficiently using message passing over a Tanner graph corresponding to H_1 [4]. Let us assume for now that $\hat{x}^n = x^n$ (note that this is always true when the main channel is noiseless). The decoder next calculates the syndrome

$$s = xH_2^T = \begin{bmatrix} m & v \end{bmatrix} \begin{bmatrix} G' \\ G \end{bmatrix} H_2^T = mG'H_2^T + vGH_2^T. \tag{5}$$

Since the rows of H_2 are a subset of a basis for the dual space of G, the second term is zero, and

$$s = mG'H_2^T. \tag{6}$$

If G' and H_2 are chosen such that $G'H_2^T = I_k$ (the $k \times k$ identity), then $s = m$ [13]. Either way, the matrix $G'H_2^T$ forms a bijective mapping between s and m. If the set of erasures over the BEC cannot be corrected, then multiple messages may be consistent with the observation, although all consistent codewords may still map to the same message.

TABLE I
CODE TABLE FOR COSET CODE DEFINED BY (8).

	$v = 0$	$v = 1$
$m = [0\,0]$	$[0\,0\,0\,0]$	$[1\,1\,1\,1]$
$m = [0\,1]$	$[0\,1\,0\,1]$	$[1\,0\,1\,0]$
$m = [1\,0]$	$[0\,0\,1\,1]$	$[1\,1\,0\,0]$
$m = [1\,1]$	$[0\,1\,1\,0]$	$[1\,0\,0\,1]$

By way of example, consider a specific code with $n = 4$, $R = 0.25$, and $R_1 = 0.75$. Messages are of size $k = n(R_1 - R) = 2$ bits. This example code is fully defined by

$$H = \left[\begin{array}{c} H_1 \\ \hdashline H_2 \end{array}\right] = \left[\begin{array}{cccc} 1 & 1 & 1 & 1 \\ \hdashline 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right], \tag{7}$$

and

$$G_1 = \left[\begin{array}{c} G' \\ \hdashline G \end{array}\right] = \left[\begin{array}{cccc} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ \hdashline 1 & 1 & 1 & 1 \end{array}\right]. \tag{8}$$

The codewords associated with each (m, v) pair are specified in Table I. For this particular code, the message to syndrome mapping is $m = s$. Since G_1 is 3×4, the code design allocates $4 - 3 = 1$ coded bit for error correction. Furthermore, since G is comprised of only one row, then exactly one coded bit is allocated towards secrecy. The remaining two coded bits are information bits for the message.

III. EQUIVOCATION EXPRESSIONS

This section presents the main results of the paper: two exact expressions for $\mathbb{H}(M|Z^n = z^n)$ when the coding procedure in Section II-B is used over the channel model specified in Section II-A. Each expression is followed by a proof, and both expressions are shown to be generalizations that cover the noiseless main channel as a special case. Examples are provided, and a discussion of the implications of these expressions on coset-style wiretap code design is given.

A. Rank Method

Consider a matrix $B = [b_1\, b_2 \cdots b_n]$, where b_i is the ith column of B. For $S \subseteq \{1, 2, \ldots, n\}$, B_S is a submatrix of B formed by concatenating together only the columns of B specified in the index set S. Furthermore, let $r(z^n) = \{i : z_i \neq ?\}$, where z_i is the observation of x_i (the ith coded bit) through a BEC, and the symbol '?' indicates an erased bit.

Theorem 1. *The exact equivocation for the observation z^n over a BEC, given the coding scheme from Section II-B is*

$$\begin{aligned} \mathbb{H}(M|Z^n = z^n) &= \mathbb{H}(M) - \operatorname{rank}[(G_1)_{r(z^n)}] + \operatorname{rank}[G_{r(z^n)}] \\ &= k - \operatorname{rank}[(G_1)_{r(z^n)}] + \operatorname{rank}[G_{r(z^n)}]. \end{aligned} \tag{9}$$

Proof. First, note that there are $2^{\operatorname{rank}[(G_1)_{r(z^n)}]}$ unique tuples in the code table for the bit locations specified by the index set $r(z^n)$, and there are $2^{\operatorname{rank}[G_{r(z^n)}]}$ unique tuples in these bit locations for any specific row of the code table. These tuples may be repeated throughout the table, but these ranks still specify the unique entries as stated. Now, there are 2^k rows (cosets) in the code table, meaning there are $2^{k+\mathrm{rank}[G_{r(z^n)}]}$ total tuples if we don't count duplicates across rows.

Recognize that each unique tuple must be in the same number of cosets. To see this, consider the cosets that have a consistent entry with an arbitrarily chosen z^n. Since cosets are offsets from $\mathcal{C}$, all consistent cosets with z^n have the same list of unique tuples in the revealed bit locations. Since $\mathcal{C}$ and $\mathcal{C}_1$ are vector subspaces in $\mathbb{F}_2^n$, the number of consistent codewords to z^n is a power of two, which is the same power of two regardless of the specific bit values in the revealed bits of z^n. Thus, every unique tuple in the code table must be in the same number of cosets.

Now we calculate the number of consistent cosets with the observation z^n as the number of rows that contain the tuple consistent with z^n. This is the simple ratio of total tuples (discounting duplicates across rows, but allowing duplicates in separate rows) over the total number of unique tuples in the code table, which is calculated as

$$\frac{2^{k+\mathrm{rank}[G_{r(z^n)}]}}{2^{\mathrm{rank}[(G_1)_{r(z^n)}]}}. \tag{10}$$

Since all messages are assumed to be equally likely, then all cosets are *a priori* equally likely, and

$$\begin{aligned}\mathbb{H}(M|Z^n = z^n) &= \log_2\left(\frac{2^{k+\mathrm{rank}[G_{r(z^n)}]}}{2^{\mathrm{rank}[(G_1)_{r(z^n)}]}}\right) &(11)\\ &= k + \mathrm{rank}[G_{r(z^n)}] - \mathrm{rank}[(G_1)_{r(z^n)}]. &(12)\end{aligned}$$

An alternative proof of this theorem was given in [18]. □

Consider the example code given by (7) and (8), with code table as in Table I. Suppose $z^n = [0\,?\,?\,1]$; then $r(z^n) = \{1, 4\}$. Clearly $\mathrm{rank}[(G_1)_{r(z^n)}] = 2$, and $\mathrm{rank}[G_{r(z^n)}] = 1$. The difference in ranks is the reduction in equivocation from $k = 2$, resulting in $\mathbb{H}(M|Z^n = z^n) = 1$ bit. Further notice that the ratio (10) perfectly counts the number of consistent cosets to z^n as two cosets, and that Table I confirms this with consistent codewords in the second and third rows, verifying the result of one bit of equivocation.

B. Zero Patterns Method

Consider the code $\mathcal{C}$ with blocklength n. For $S \subseteq \{1, 2, \ldots, n\}$, let $N[S]$ be the number of codewords in $\mathcal{C}$ with zeros for all bit locations in the index set S. If $S = \emptyset$, then $N[S] = |\mathcal{C}|$, since all codewords satisfy the requirement to be counted. (Note that we will use this expression to count codewords that are consistent to a channel observation, and clearly this interpretation for the empty set is the proper interpretation for counting consistent codewords when no bits have been revealed.) Further let $N_1[S]$ be the number of codewords in $\mathcal{C}_1$ with zeros for all bit locations in the index set S. The expression $r(z^n) = \{i : z_i \neq ?\}$, as before.

Theorem 2. *The exact equivocation for the observation z^n over a BEC, given the coding scheme from Section II-B is*

$$\mathbb{H}(M|Z^n = z^n) = \log_2 N_1[r(z^n)] - \log_2 N[r(z^n)]. \tag{13}$$

Proof. Note from Theorem 1, that $\mathbb{H}(M|Z^n = z^n)$ is not a function of the specific message to be transmitted nor the specific codeword chosen by the encoder; thus, without loss of generality in the expression of the exact equivocation, we may assume that the encoder chooses the all-zero codeword (which always corresponds to the all-zero message). Since all cosets in the code table are simply offsets of $\mathcal{C}$, then all cosets consistent with the observation z^n over the erasure channel have the same number of consistent codewords. One of the consistent cosets is the code $\mathcal{C}$, which carries the all-zero codeword.

The number of consistent codewords to z^n in any consistent coset is $N[r(z^n)]$, and the total number of consistent codewords in $\mathcal{C}_1$ is $N_1[r(z^n)]$. Thus, the number of consistent cosets to z^n is simply the ratio

$$\frac{N_1[r(z^n)]}{N[r(z^n)]}. \tag{14}$$

Since all messages are assumed to be equally likely, then all cosets are *a priori* equally likely, and

$$\begin{aligned}\mathbb{H}(M|Z^n = z^n) &= \log_2\left(\frac{N_1[r(z^n)]}{N[r(z^n)]}\right) &(15)\\ &= \log_2 N_1[r(z^n)] - \log_2 N[r(z^n)]. &(16)\end{aligned}$$

□

Consider again the example code given by (7) and (8), with code table as in Table I. Suppose $z^n = [0\,?\,?\,1]$ and $r(z^n) = \{1, 4\}$, as before. Note from Table I that $N[r(z^n)] = 1$ because one codeword from $\mathcal{C}$ (the top row in the code table) has zeros in both the first and fourth bit locations. Also, $N_1[r(z^n)] = 2$ because two codewords from $\mathcal{C}_1$ (the entire collection of codewords in the code table) have zeros in the first and fourth bit locations. Thus, Theorems 1 and 2 consistently calculate the equivocation for this example to be one bit.

C. Noiseless Main Channel Special Case

When coding for a noiseless main channel, no error correction for Bob is needed, and the entire coding overhead is allocated to keeping the message secure. As mentioned in Section II-B, this results in a square $n \times n$ matrix G_1. The matrix G is then $(n-k) \times n$, H_1 is an empty matrix, and v is $(n-k)$ bits long. Since G_1 is square, and full rank, then $\mathcal{C}_1 = \mathbb{F}_2^n$.

Corollary 1. When the coding scheme from Section II-B is such that G_1 is $n \times n$, then the exact equivocation is

$$\mathbb{H}(M|Z^n = z^n) = \mathbb{H}(M) - |r(z^n)| + \mathrm{rank}[G_{r(z^n)}]. \tag{17}$$

The proof only requires one to note that if G_1 is $n \times n$, then it must have full column rank as well as row rank, and $\mathrm{rank}[(G_1)_{r(z^n)}] = |r(z^n)|$ in (9). An alternative proof of this Corollary was given in [13].

Corollary 2. When the coding scheme from Section II-B is such that G_1 is $n \times n$, then the exact equivocation is

$$\mathbb{H}(M|Z^n = z^n) = n - |r(z^n)| - \log_2 N[r(z^n)]. \tag{18}$$

This corollary is proved by noting that a full-rank square matrix G_1 implies that $N_1[r(z^n)] = 2^{n-|r(z^n)|}$ because $\mathcal{C}_1 = \mathbb{F}_2^n$. This substitution into (13) gives the result.

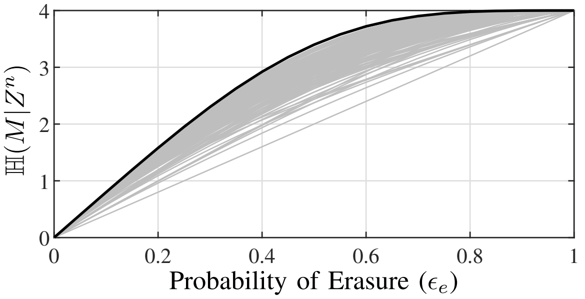

Fig. 1. All ($n=8$, $k=4$) binary coset codes for the noiseless main channel. The best code's equivocation curve is the dark line, and the generator for the code is defined by (19).

D. Examples

This section considers two codes, and highlights the application of the new expressions for $\mathbb{H}(M|Z^n=z^n)$ in calculating Δ. The expressions allow the codes to be compared side by side. Let $n=8$, $R_1=0.75$, and $R=0.5$. The number of information bits is then $k=n(R_1-R)=2$ bits. Let

$$G=\begin{bmatrix}1&0&0&0&0&1&1&1\\0&1&0&0&1&0&1&1\\0&0&1&0&1&1&0&1\\0&0&0&1&1&1&1&0\end{bmatrix} \tag{19}$$

for both codes. Coincidently, G is an equivalent generator to that of the Reed Muller code with order one and blocklength eight [19]. This generator also defines the best wiretap code for all possible erasure probabilities in the eavesdropper's channel ϵ_e when $n=8$, $R_1=1$, and $R=0.5$, which is suitable for the noiseless main channel case with $k=4$. Fig. 1 shows $\mathbb{H}(M|Z^n)$ for all such codes (enumerated ignoring isomorphic generators) when the main channel is error free, with the black line giving the equivocation curve for the code defined by (19).

Now, consider two different G' options that can be coupled with G in (19) as shown in Section II-B to form codes for the erasure main channel case, where Code A has

$$G'_A=\begin{bmatrix}0&0&1&1&0&1&1&1\\1&1&1&1&0&1&0&0\end{bmatrix}, \tag{20}$$

and Code B has

$$G'_B=\begin{bmatrix}0&0&1&1&0&1&1&0\\1&1&1&1&0&1&0&1\end{bmatrix}. \tag{21}$$

The algebraic properties for Codes A and B are detailed in Table II, and the average equivocation curves for both codes are plotted in two ways in Fig. 2. In the figure, the average equivocation is plotted versus the eavesdropper's erasure probability ϵ_e, and then also plotted versus the number of revealed bits $|r(z^n)|$. These curves are average functions of the exact equivocation expressions calculated over all possible revealed-bit patterns using the data tabulated in Table II. Notice that the differences between the codes occur when $|r(z^n)|$ is high (or equivalently when ϵ_e is low). Code A exhibits higher equivocation than Code B, but Code B also allows all erasure patterns of size one to be corrected, which may be useful for Bob. Finally, we see that the wiretap II case is easily solved for both codes given the data in Table II.

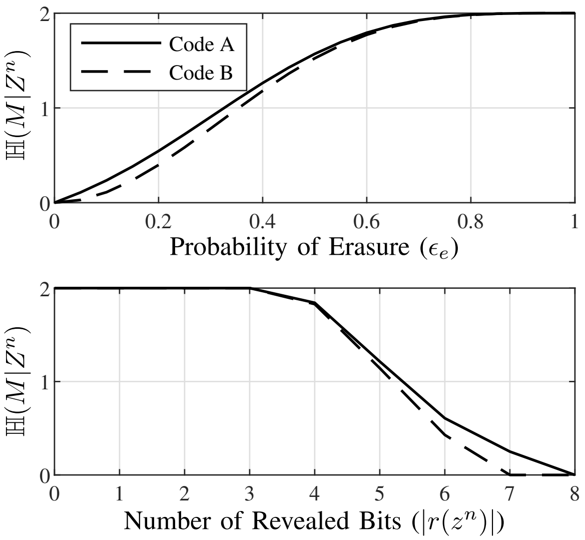

Fig. 2. Average equivocation $\Delta=\mathbb{H}(M|Z^n)$ for Codes A and B.

E. Implications on Wiretap Code Design

The elegance and simplicity of the theorems in this paper make them particularly useful. The *explicit* linking of equivocation to structural code parameters for erasure channel variants of the wiretap channel model has only been accomplished to date for the rank method, where these results are restated as Theorem 1 and Corollary 1 with simplified proofs from those given in [18], [13].

In this paper, we make a nice extension for the noiseless main channel case to zero patterns in codewords using Corollary 2. This new insight shows that codeword coverage is important in ensuring that revealed-bit patterns do not leak information. Consider the structure of Corollary 2, where we see that a revealed-bit pattern $r(z^n)$ is secure if and only if $n-|r(z^n)|-\log_2 N[r(z^n)]=k$, which implies that for $|r(z^n)|=(n-k)$, the bits of $r(z^n)$ can be all-zero only once in the codewords of $\mathcal{C}$. Since the all-zero codeword is in $\mathcal{C}$, this implies that all non-zero codewords must have at least a single one in the revealed-bit pattern to make it secure. This insight allows code designers to link secure code design to a covering problem of ones in codewords. Although some notion of the need to "spread the ones around in the codewords," has been suspected for good code design [10], [11], now the idea has a specific mathematical meaning. Notice also that every revealed-bit pattern where $|r(z^n)|>(n-k)$ must leak at least $|r(z^n)|-(n-k)$ bits due to the presence of the all-zero codeword in $\mathcal{C}$. This notion has already been shown in [11] using a different approach, but here we see that additional appearances of these larger zero patterns likewise ensures the additional appearances of smaller zero patterns that are subsets of the larger one. This implies the optimality of codes wherein all codewords have identical weight, such as the simplex code, which has been conjectured to be optimal but not yet proven [10].

Regarding code design for the noisy main channel, Theorem 1 implies that a revealed-bit pattern $r(z^n)$ is secure if

TABLE II
ALGEBRAIC PROPERTIES FOR CODES A AND B.

						Code A	Code B
$\lvert r(z^n)\rvert$	$\mathrm{rank}[G_{r(z^n)}]$	$\mathrm{rank}[(G_1)_{r(z^n)}]$	$N[r(z^n)]$	$N_1[r(z^n)]$	$\mathbb{H}(M\lvert Z^n = z^n)$	Occurrences	Occurrences
0	0	0	16	64	2	1	1
1	1	1	8	32	2	8	8
2	2	2	4	16	2	28	28
3	3	3	2	8	2	56	56
4	3	3	2	8	2	3	2
	3	4	2	4	1	11	12
	4	4	1	4	2	56	56
5	4	4	1	4	2	12	8
	4	5	1	2	1	44	48
6	4	4	1	4	2	1	0
	4	5	1	2	1	15	12
	4	6	1	1	0	12	16
7	4	5	1	2	1	2	0
	4	6	1	1	0	6	8
8	4	6	1	1	0	1	1

and only if $\mathrm{rank}[G_{r(z^n)}] = \mathrm{rank}[(G_1)_{r(z^n)}]$ (see also [18]). Theorem 2 implies that $r(z^n)$ is secure if and only if $N_1[r(z^n)]/N[r(z^n)] = 2^k$, which implies that the zero patterns consistent with z^n are evenly spread throughout the cosets (as required in the noiseless main channel case). For reliability, note that the theorems imply that the information about the message is revealed if and only if $\mathrm{rank}[(G_1)_{r(z^n)}] - \mathrm{rank}[G_{r(z^n)}] = k$, or equivalently $N_1[r(z^n)] = N[r(z^n)]$. Consider again the example code given by (7) and (8), with code table as in Table I. This code is designed so that *all* revealed-bit patterns of size one leak no information, while *all* revealed-bit patterns of size three reveal the message exactly. Coincidently, every revealed-bit pattern of size two must leak exactly one bit to make this possible [11]. Code B in Table II can also correct all singly-occurring erasures, and can provide perfect secrecy if no more than three coded bits are observed by an eavesdropper. Design principles from the theorems of this paper can be used to search for yet larger codes offering similar properties.

IV. CONCLUSION

This paper presents two expressions for quantifying the exact equivocation when coset coding is used over the erasure wiretap channel model with a noisy main channel. The expressions were shown to be generalizations that cover the noiseless main channel as a special case. These expressions are the first of their kind for noisy main channels, and they explicitly link structural parameters in the code design to security and reliability for finite blocklength codes. Insights gained from these expressions may soon lead to breakthroughs in finite blocklength code design over noisy erasure main channels. In particular, the true limits of the coset coding approach may be identified (in terms of security and reliability) for finite blocklength codes, with specific code constructions that achieve those limits.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] M. Bloch and J. Barros, *Physical Layer Security : From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[3] W. K. Harrison and S. W. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *Proc. IEEE Int. Conf. Communications (ICC)*, Dresden, DE, June 2009, pp. 1–5.

[4] W. K. Harrison, J. Almeida, S. W. McLaughlin, and J. Barros, "Coding for cryptographic security enhancement using stopping sets," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 575–584, 2011.

[5] B. Jensen, B. Clark, D. Flanary, K. Norman, M. Rice, and W. K. Harrison, "Physical-layer security: Does it work in a real environment?" in *Proc. IEEE Int. Conf. Communications (ICC)*, Shanghai, CN, 2019, pp. 1–7.

[6] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[7] M. R. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proceedings of IEEE*, vol. 103, no. 10, pp. 1725–1746, October 2015.

[8] C. W. Wong, T. Wong, and J. Shea, "Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 551 –564, sept. 2011.

[9] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel," in *Proc. IEEE Int. Conf. Communication Workshop (ICCW)*, June 2015, pp. 435–440.

[10] W. K. Harrison and M. R. Bloch, "On dual relationships of secrecy codes," in *Proc. IEEE Allerton Conference*, Oct. 2018, pp. 1–7.

[11] W. K. Harrison and M. R. Bloch, "Attributes of generators for best finite blocklength coset wiretap codes over erasure channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Paris, FR, 2019, pp. 827–831.

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ: John Wiley & Sons, Inc., 2006.

[13] J. Pfister, M. Gomes, J. P. Vilela, and W. K. Harrison, "Quantifying equivocation for finite blocklength wiretap codes," in *Proc. IEEE Int. Conf. Communications (ICC)*, Paris, FR, June 2017, pp. 1–6.

[14] L. H. Ozarow and A. D. Wyner, "Wiretap channel II," *AT&T Bell Labs. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, December 1984.

[15] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, 1991.

[16] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, August 2007.

[17] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge-type LDPC codes for the BEC wiretap channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1048–1064, 2013.

[18] N. Cai and T. Chan, "Theory of secure network coding," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 421–437, 2011.

[19] T. K. Moon, *Error Correction Coding : Mathematical Methods And Algorithms*. John Wiley & Sons, 2005.