entropy

MDPI

Article

On Best Erasure Wiretap Codes: Equivocation Matrices and Design Principles

Willie K. Harrison *, Truman Welling, Andrew Swain and Morteza Shoushtari

Department of Electrical and Computer Engineering, Brigham Young University, Provo, UT 84602, USA; truman.welling@gmail.com (T.W.); swain.andrew.g@gmail.com (A.S.); morteza.shoushtari@byu.edu (M.S.)
* Correspondence: willie.harrison@byu.edu

Abstract

Physical-layer security can aid in establishing secure telecommunication networks including cellular, Internet of Things, and telemetry networks, among others. Channel sounding techniques and/or telemetry systems for reporting channel conditions, coupled with superior wiretap code design are necessary to implement such secure systems. In this paper, we present recent results in best wiretap coset code design for the binary erasure wiretap channel. We define equivocation matrices, and showcase their properties and utility in constructing good, and even the best, wiretap codes. We outline the notion of equivalence for wiretap coset codes, and use it to reduce the search space in exhaustive searches for best small codes. Through example, we show that the best codes do not exist for some code sizes. We also prove that simplex codes are better than codes repeating one column multiple times in their generator matrix.

Keywords: information theoretic security; equivocation matrices; wiretap coset codes; finite blocklength analysis

check for updates

Academic Editor: Chi Wan Sung

Received: 22 October 2025
Revised: 21 November 2025
Accepted: 26 November 2025
Published: 9 December 2025

Citation: Harrison, W.K.; Welling, T.; Swain, A.; Shoushtari, M. On Best Erasure Wiretap Codes: Equivocation Matrices and Design Principles. *Entropy* **2025**, *27*, 1245. https://doi.org/10.3390/e27121245

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Wireless telecommunications are susceptible to eavesdropping due to their broadcast nature [1,2]. For cellular communications, it is expected that 6G networks will mitigate some of the threat of eavesdropping using beamforming/directional communications [3], but this will not solve the problem entirely. Additionally, networks of all kinds, not just cellular, exhibit this vulnerability. The IoT in general promises to place a heavy emphasis on small packet communications with low latency, low power, and high reliability requirements [4]. Unfortunately, the well-tested public-key/private-key cryptographic approaches [5] do not scale well to networks with these characteristics [6,7]. There is an urgent need for robust and adaptable security solutions for these new networks if they are to be trusted with future sensitive communications [6–9].

One option for addressing these security needs is physical-layer security [10], wherein the characteristics of the wireless channel are exploited for security gains. A host of recent papers [11–15] outline the multi-pronged approach needed to achieve physical-layer security. On one hand, system designers must test the environment using channel sounding techniques, which could include real-time telemetry systems that communicate channel conditions from various nodes in the network. On the other hand, good wiretap codes are needed to exploit favorable channel conditions for physical-layer security. This paper addresses the second aspect of implementing systems capable of achieving physical-layer security by addressing wiretap code design at finite blocklength.

Achieving information theoretic security over wiretap channels has been a topic of interest for several decades now [16,17]. Many works have focused on the fundamental limits of physical-layer security over various channels [10,18], but several others have tried to find explicit coding constructions for achieving those limits (see [19,20] and references). To date, the majority of coding results require codes to be analyzed in the asymptotic blocklength regime, mainly since the common information theoretic security metrics are analyzed in the limit as blocklength tends to infinity. Consider the wiretap channel model in Figure 1, where a user named Alice attempts to communicate a message M reliably over a *main channel* of communications to a user named Bob without leaking information to an eavesdropper named Eve over the *eavesdropper's channel*. Alice encodes M using code $\mathcal{C}$ to produce a length-n codeword X^n, which is broadcast over both the main and the eavesdropper's channels. Bob and Eve observe Y^n and Z^n through their respective channels, and Bob's estimate of the message is denoted $\hat{M}$ (note that we will use capital letters to denote random variables/vectors, with matching lowercase letters signifying realizations of those variables and matching calligraphic letters signifying the alphabets over which those variables are defined). Coding over the wiretap channel is typically carried out with two goals in mind. A reliability constraint on the problem requires $\lim_{n\to\infty} \Pr(\hat{M} \neq M) = 0$, and a security constraint based on information theory is imposed on the problem as well. The following security constraints are perhaps the most popular [10,21]:

- $\lim_{n\to\infty} \frac{1}{n}\mathbb{I}(M; Z^n) = 0$, where $M \sim U[0, 2^k - 1]$, (weak secrecy);
- $\lim_{n\to\infty} \mathbb{I}(M; Z^n) = 0$, where $M \sim U[0, 2^k - 1]$, (strong secrecy);
- $\lim_{n\to\infty} \max_{p_M(m)} \mathbb{I}(M; Z^n) = 0$, (semantic secrecy).

In these definitions, $\mathbb{I}(\cdot;\cdot)$ is the usual mutual information function [22], $M \sim U[0, 2^k - 1]$ signifies that the message is distributed as discrete uniform over the integers $[\![0, 2^k - 1]\!] = \{0, 1, \ldots, 2^k - 1\}$, and $p_M(m)$ is the probability mass function of M. In all three constraints, the range of M is taken to be $\mathcal{M} = [\![0, 2^k - 1]\!]$.

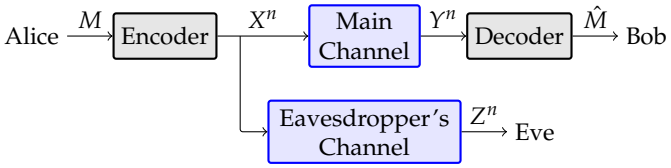


Figure 1. Wiretap channel model.

If finite blocklength wiretap codes are to be optimized, or even compared with each other, these asymptotic metrics are often insufficient. In this paper we consider only finite blocklength wiretap codes based on the cosets of a linear block code [17,23,24], and fix n to be relatively small as compared to blocklengths commonly encountered in error-control coding [25–27]. The design constraints for our fixed blocklength analysis are:

1. $\Pr(\hat{M} \neq M) < \delta_m$, (reliability constraint);
2. $\mathbb{I}(M; Z^n) < \delta_e$, where $M \sim U[0, 2^k - 1]$, (security constraint),

and δ_m and δ_e are assumed to be small positive real numbers. Note that

$$\mathbb{I}(M; Z^n) = \mathbb{H}(M) - \mathbb{H}(M|Z^n), \tag{1}$$

where $\mathbb{H}(\cdot)$ is the average entropy function [22], and

$$E = \mathbb{H}(M|Z^n) = \sum_{z^n \in \mathcal{Z}^n} p(z^n)\mathbb{H}(M|Z^n = z^n) \tag{2}$$

is called the *equivocation*. The goal of this current line of inquiry is to discover the best binary codes of a particular size, wherein we define a *best code* as follows.

Definition 1. *For fixed parameters n and k, a code that minimizes* $\mathbb{I}(M; Z^n)$ *(or, equivalently, maximizes* $\mathbb{H}(M|Z^n)$*)* for all possible eavesdropper's channel states *over the choice of binary wiretap codes with parameters n and k is termed* best *or* best for its size. *If no code with parameters n and k maximizes the equivocation for all possible eavesdropper's channel states, then we say that a best code* does not exist *for code parameters n and k. We restrict our analysis to wiretap codes that are built using the well-known coset coding structure.*

Knowledge of the best codes, where they exist, will allow engineers to maximize the secrecy in a communications network without worrying about achieving asymptotic security constraints. Furthermore, asymptotic security guarantees can only be made with knowledge of the eavesdropper's channel state information (CSI) [10,19,20], which is often not readily available during code design anyway. Perhaps a better approach is to simply set the code parameters, and then maximize the achievable secrecy with the choice of a best code [12] (note here that our techniques will also easily allow a worst-case leakage analysis to be completed, thereby also covering the wiretap-II case [23]).

A few works [28–31] have attempted to discover the best wiretap codes, but the results are somewhat inconclusive as the authors assume that large best codes can be grown from small best codes, which is an unproven assumption. A local search algorithm using a smaller code as a seed then provides the results for the larger code parameters. Our approach to best coset coding, however, is to provably identify codes with best performance and their properties [32–36]. Such research requires the analysis of algebraic properties of encoders along the lines of the work in [24,37,38]. Some other works have also sought to quantify the information theoretic security as a function of blocklength [39,40], but the results are only bounds that are quite pessimistic for small to medium blocklength codes. Our approach differs from these works in that we seek to quantify the equivocation exactly as we identify the best codes.

This paper analyzes coset codes over the simplest wiretap channel model, where the main channel is noiseless and the eavesdropper's channel is a binary erasure channel (BEC); this model is called the binary erasure wiretap channel (BEWC). However, just as error-control coding results for the BEC have led to more powerful results over real-world channels (e.g., Gaussian channels) [27], it is expected that good (and even best) codes found while studying the BEWC will lead to optimal code structures for more interesting channels [35,41]. Note that focusing on this model allows us to effectively ignore the reliability constraint since $\Pr(\hat{M} \neq M) = 0$ for all valid codes; thus, it becomes possible to rank codes only according to how well they keep information secret from Eve.

The main contributions of this paper build on those previously presented in [32–36], and are as follows:

- A complete presentation of the equivocation matrix and its properties as a tool for finite blocklength analysis and code design over the BEWC (the tool has been used in [33,34] but will benefit from this more complete discussion);
- An explanation of search space reduction techniques that allow for the discovery of best small blocklength codes (the results from these techniques were shown in [32,33,35], but the techniques have not yet been explained in the literature);
- A discussion of the results regarding the existence of best coset codes for information theoretic security (it has been hypothesized that a best code exists for all valid (n, k) pairs in [33], but this is proved otherwise herein by way of counterexample);

- A high-level algorithm for the design of good wiretap coset codes for the BEWC of any size that follows an *outside-in* approach to code design that is backed by equivocation matrix properties for best codes;
- Results related to simplex and Hamming codes: notably that the simplex code is better for *all* eavesdropper channel states than any code of its size with exactly one column of the generator matrix repeated any number of times.

The rest of this paper is organized as follows. Section 2 presents the necessary background information required for the remainder of this paper, including an explanation of encoding and decoding using wiretap codes for the BEWC based on the cosets of a linear block code, and a sufficient condition for classifying a binary coset code as *best* that is easier to work with than Definition 1. Then, Sections 3–7 give the main results of this paper. Equivocation matrices and their properties are defined and discussed in Section 3. Search space reduction techniques for finding small best codes are presented in Section 4. Section 5 highlights our current knowledge regarding the existence of best codes. Section 6 shows how to build good codes of any size and links the method to properties of best codes' equivocation matrices. Finally, the new result regarding the optimality of simplex and Hamming codes is presented in Section 7. This paper is concluded in Section 8.

2. Background

2.1. Coset Coding for the Wiretap Channel

The binning technique known as coset coding used in many prior works [17,23,42] is the coding mechanism analyzed in this paper. Let $\mathcal{C}$ denote an $(n, n-k)$ linear block code, and $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{2^k-1}$ signify the cosets of $\mathcal{C}$, where $\mathcal{C}_0 = \mathcal{C}$. The generator and parity-check matrices for $\mathcal{C}$ are denoted G and H, respectively. The encoder function encodes the message m by choosing a codeword from $\mathcal{C}_m$ uniformly at random. This operation can be conducted using an auxiliary message M'.

The auxiliary message is an $(n-k)$-bit row vector that carries no real information, and is chosen uniformly at random from the elements in the field of length-$(n-k)$ binary vectors $\mathbb{F}_2^{(n-k)}$. Let m be written in the form of a k-bit binary row vector. Also let

$$G^* = \begin{bmatrix} G \\ G' \end{bmatrix}, \tag{3}$$

where the rows of G' are chosen to give G^* full rank, and must therefore be linearly independent and chosen from outside $\mathcal{C}$. The codeword is calculated as

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

and the mathematical encoding operation is carried out in $\mathbb{F}_2$. Clearly, $m'G$ chooses a codeword from $\mathcal{C}$, and mG' chooses an offset that maps the codeword into a specific coset of $\mathcal{C}$. Thus, m chooses the coset, and m' chooses the codeword from the coset uniformly at random.

For example, let

$$G^* = \left[\begin{array}{c} G \\ \hdashline G' \end{array}\right] = \left[\begin{array}{cccc} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ \hdashline 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right]. \tag{5}$$

This encoder defines the code in Table 1.

Table 1. Code table for coset code defined by (5).

Coset		$m' = [0\,0]$	$m' = [0\,1]$	$m' = [1\,0]$	$m' = [1\,1]$
$\mathcal{C}_0$	$m = [0\,0]$	[0 0 0 0]	[0 0 1 1]	[1 1 0 1]	[1 1 1 0]
$\mathcal{C}_1$	$m = [0\,1]$	[1 0 1 0]	[1 0 0 1]	[0 1 1 1]	[0 1 0 0]
$\mathcal{C}_2$	$m = [1\,0]$	[1 1 0 0]	[1 1 1 1]	[0 0 0 1]	[0 0 1 0]
$\mathcal{C}_3$	$m = [1\,1]$	[0 1 1 0]	[0 1 0 1]	[1 0 1 1]	[1 0 0 0]

Since we are operating over the BEWC, the main channel is noiseless and Bob needs only to map the codeword back to the proper message to do the decoding. The decoder function first calculates a syndrome

$$s = y^n H^T = x^n H^T = m'GH^T + mG'H^T = mG'H^T. \tag{6}$$

Notice that $G'H^T$ forms a bijective mapping between s and m. If G' and H are chosen so that $G'H^T = I_k$, the $(k \times k)$ identity, then $s = m$. Otherwise, the mapping will need to be inverted to complete the decoder [32]. For our example code, let

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}. \tag{7}$$

It can be verified that $G'H^T = I_2$; so, $s = m$ in this case.

2.2. Equivocation for Coset Codes

Let us write the generator matrix for $\mathcal{C}$ in terms of its columns as

$$G = \begin{bmatrix} \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_n \end{bmatrix}. \tag{8}$$

Also, for a set of integers $J = \{j_1, j_2, \ldots, j_{|J|}\}$ such that $1 \leq j_i \leq n$ for $i \in [\![1, |J|]\!]$, let

$$G_J = \begin{bmatrix} \mathbf{g}_{j_1} & \mathbf{g}_{j_2} & \cdots & \mathbf{g}_{j_{|J|}} \end{bmatrix}; \tag{9}$$

i.e., G_J is the submatrix of G comprising only the columns with indices in J. Note that the notation $|J|$ indicates the cardinality of the set J. Since Z^n is Eve's observation of the transmitted codeword through a BEC, then $\mathcal{Z}^n = \{0, 1, ?\}^n$, where '?' indicates an erased bit. Let

$$r(z^n) = \{i | z_i \neq ?\}; \tag{10}$$

thus, $r(z^n)$ is the set of indices for all revealed bits to Eve in z^n. It was shown in [32,35] that

$$\begin{aligned} \mathbb{H}(M|Z^n = z^n) &= \mathbb{H}(M) - |r(z^n)| + \text{rank}(G_{r(z^n)}) \\ &= k - |r(z^n)| + \text{rank}(G_{r(z^n)}). \end{aligned} \tag{11}$$

This quantity is the *exact equivocation* given a particular observation z^n, and it can be used to calculate the average equivocation $\mathbb{H}(M|Z^n)$ in (2) by summing over all possible $z^n \in \mathcal{Z}^n$.

By way of example, let us consider $z^n = [?\,1\,1\,?]$ with the code defined by (5). Then, $r(z^n) = \{2, 3\}$, and $\text{rank}(G_{r(z^n)}) = 2$ giving $\mathbb{H}(M|Z^n = z^n) = 2$ bits from (11). Notice that Table 1 verifies the equivocation at 2 bits since all four cosets have an entry consistent with z^n, and all four messages are a priori equally likely. However, it is also straightforward to see that if z^n were such that $r(z^n) = \{1, 2\}$, then $\text{rank}(G_{r(z^n)}) = 1$ and we would expect to leak one bit of information in this case. Again, the code in Table 1 verifies this claim, as any observation that reveals the first two bits will only have two consistent

cosets, and thereby one bit of equivocation. It is of note that the particular values of the revealed bits make no difference in the exact equivocation calculation, but rather only the revealed-bit pattern $r(z^n)$.

2.3. A Sufficient Condition for the Existence of Best Wiretap Coset Codes for All ϵ

Figure 2 gives equivocation curves for all possible coset codes with $n = 4$ and $k = 2$ as a function of the eavesdropper's erasure probability ϵ. Note there are only six codes analyzed, but G is $(n-k) \times n$ (2×4 in this case), and therefore comprises eight symbols. Certainly, we can produce more than six valid generators with eight binary symbols, but there are in fact exactly six codes up to isomorphisms in the code structure. This will be explained further in Section 4. It can be observed in Figure 2 that the equivocation curves of Codes 3 and 4 cross at $\epsilon = 0.5$, indicating that codes cannot simply be ordered from best to worst without an operating point for the eavesdropper's channel, say ϵ_0. However, Code 6 gives maximum equivocation over all codes for all ϵ, and hence can be labeled as *best*. These interesting features indicate that if we wish to find best codes, then we must first guarantee the existence of a code that is *best* for all possible eavesdropper's CSI. As will be shown in Section 5, the existence of a best code for any specific choices of n and k is not easily deducible. As a note, the equivocation curve for Code 6 is that of the example code given in (5) and Table 1.

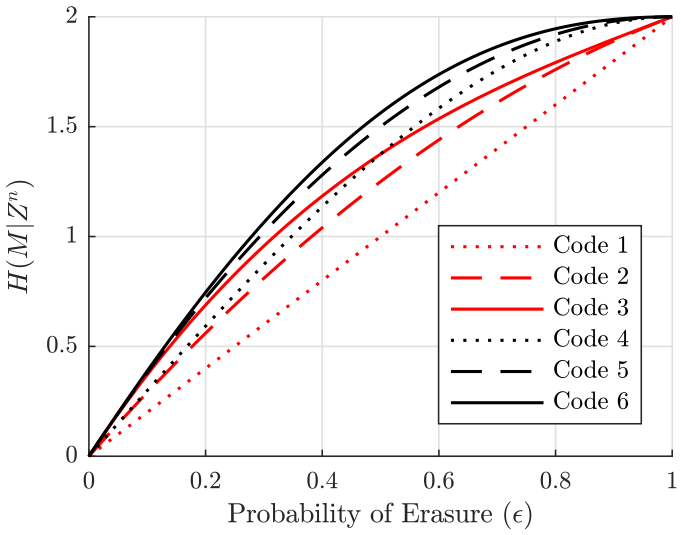


Figure 2. Equivocation of all $n = 4$, $k = 2$ secrecy codes as a function of Eve's channel's erasure probability ϵ.

Suppose that an $(n, n-k)$ linear block code $\mathcal{C}$ with generator G is used for coset coding as described in Section 2.1. Let $\mathcal{R}_\mu$ be the set of all possible revealed-bit patterns r, each of which is a subset of $[\![1, n]\!]$, such that $|r| = \mu$. Then, using (2) and (11),

$$\mathbb{H}(M|Z^n) = \sum_{z^n \in \mathcal{Z}^n} p(z^n) \mathbb{H}(M|Z^n = z^n) \tag{12}$$

$$= \sum_{z^n \in \mathcal{Z}^n} p(z^n) \Big[\mathbb{H}(M) - |r(z^n)| + \text{rank}(G_{r(z^n)}) \Big] \tag{13}$$

$$= \sum_{\mu=0}^{n} \sum_{r \in \mathcal{R}_\mu} (1-\epsilon)^\mu \epsilon^{n-\mu} [k - \mu + \text{rank}(G_r)]. \tag{14}$$

Note that a sufficient condition for a code to maximize (14) for all ϵ, and for fixed n and k, is for the code to maximize

$$\sum_{r \in \mathcal{R}_\mu} \text{rank}(G_r) \tag{15}$$

for all $\mu \in [\![0, \mu]\!]$ [33]. If such a code exists for specific n and k, then each iteration of the outer sum of (14) will be as large as possible, thus maximizing the entire equivocation. Such a code is clearly *best* for all possible ϵ.

3. Equivocation Matrices and Their Properties

It is now necessary to define the equivocation matrix to continue our study of best codes. Equivocation matrices were first presented in [33] and the basic presentation of the definitions is similar here. In comparing codes of a particular size, it is useful to know the number of revealed-bit patterns with μ revealed bits that maintain e bits of equivocation. There are $\binom{n}{\mu}$ ways to reveal μ of n bits through an erasure channel, and all of these patterns must be accounted for when calculating the equivocation $\mathbb{H}(M|Z^n)$.

3.1. Basic Definitions

Let us consider the expression for the exact equivocation in (11). Note that all the elements of the expression (k, $|r(z^n)|$, and $\text{rank}(G_{r(z^n)})$) are each confined to the set of non-negative integers. Since basic information theory [22] tells us that $\mathbb{H}(M|Z^n = z^n)$ must be between zero bits and $\mathbb{H}(M) = k$ bits, then the integer elements of (11) further tell us that $\mathbb{H}(M|Z^n = z^n) \in [\![0, k]\!]$. Therefore, since there are no revealed-bit patterns that can leak partial bits, we can count the number of revealed-bit patterns of size μ that maintain equivocation equal to e bits and collect this information in a matrix.

Definition 2. *Let the* $(k+1) \times (n+1)$ equivocation matrix A *for the* (n, k) *coset code defined by the* $(n, n-k)$ *linear block code* $\mathcal{C}$ *denote the number of revealed-bit patterns of size* μ *that maintain* e *bits of equivocation in the matrix element* $a_{e,\mu}$ *for* $\mu \in [\![0, n]\!]$ *and* $e \in [\![0, k]\!]$. *Let* $a_{0,0}$ *be the bottom left entry of the matrix, and indexing proceed from that point.*

Perhaps somewhat unconventionally, we start indexing the rows of the equivocation matrix from the bottom of the matrix. This is carried out to match plots of e vs μ in structure. By way of example, the equivocation matrix for the code defined by (5) and given in Table 1 is

$$A = \begin{bmatrix} 1 & 4 & 5 & 0 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \tag{16}$$

and the equivocation curves plotting $\mathbb{H}(M|Z^n)$ as a function of the number of revealed bits μ for all coset codes with $n = 4$ and $k = 2$ are given in Figure 3, with our example code being Code 6 as before.

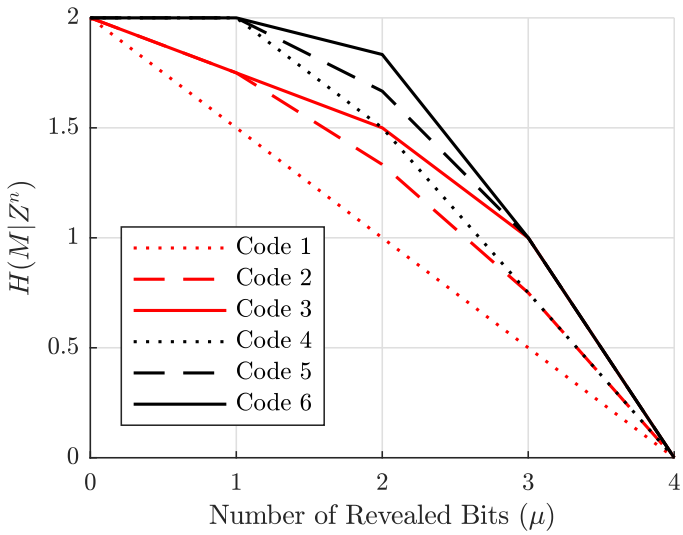


Figure 3. Equivocation of all $n = 4$, $k = 2$ coset codes as a function of the number of revealed bits to Eve μ.

Consider the third column (corresponding to $\mu = 2$) of the equivocation matrix. There are $\binom{4}{2} = 6$ ways to reveal two of four bits over a BEC; hence, the column sum is six. We see here that five of the six patterns leak no information about the message (equivocation is two bits), but the last pattern leaks one bit about M. This pattern was already mentioned in Section 2.2 as $r(z^n) = \{1, 2\}$. The average equivocation for Code 6 plotted in Figure 3 shows that $\mathbb{H}(M|Z^n) = 11/6 \approx 1.8333$ bits at $\mu = 2$. For all other μ values, $\mathbb{H}(M|Z^n)$ is an integer since all revealed-bit patterns of those sizes leak the same number of full bits.

3.2. Properties of the Equivocation Matrix

In our discussion of the properties of equivocation matrices, we first mention a finding from [33]. Let us define $A^\perp$ as the $(n-k+1) \times (n+1)$ equivocation matrix for the $(n, n-k)$ coset code built from the (n, k) dual code $\mathcal{C}^\perp$, and let the elements of $A^\perp$ be $a^\perp_{e,\mu}$, just as for A, but now letting $e \in [\![0, n-k]\!]$, and $\mu \in [\![0, n]\!]$ as before.

Lemma 1 (Lemma 1 from [33]). *Consider an $(n, n-k)$ linear block code $\mathcal{C}$ and its dual code $\mathcal{C}^\perp$. The equivocation matrices of the coset codes over the BEWC formed by the two linear block codes are related by $a_{e,\mu} = a^\perp_{e+\mu-k,n-\mu}$.*

The proof is given in [33], where it is shown that every pattern with μ revealing bits leading to equivocation e for coset coding with $\mathcal{C}$, maps precisely to one unique pattern with $n - \mu$ revealed bits leading to equivocation $e + \mu - k$ for coset coding with $\mathcal{C}^\perp$. In [43], we extended the result to show that the second pattern is the set complement of the first pattern, and we demonstrated that

$$\mathbb{H}(M|Z^n = z^n) = \operatorname{rank} H_{[\![1,n]\!]\setminus r(z^n)}. \tag{17}$$

Figure 4 illustrates the meaning of the lemma when $\mathcal{C}$ is the $(5, 2)$ code with the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{18}$$

When used for coset coding, this generator matrix produces a coset code with $n = 5$ and $k = 3$. When the dual code is used for coset coding, however, $n = 5$ and $k = 2$. Note that

the entries in A dictate precisely the entries in $A^{\perp}$, and the placement of the entries in $A^{\perp}$ is as prescribed by Lemma 1.

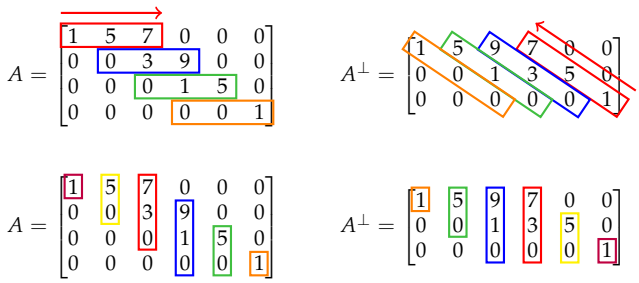


Figure 4. Pictorial representation of the dual relationship between equivocation matrices A and $A^{\perp}$. The colored boxes and ordering arrows highlight the locations of identical entries in the matrices for dual codes, which is consistent with Lemma 1.

In [33], it was further noted that all zeros in A can either be attributed to the generalized Hamming weights of $\mathcal{C}^{\perp}$ (see [24]) or the upper right triangle of zeros, which must be present in every equivocation matrix. Using further arguments from [24], it was shown that all binary maximum distance separable (MDS) codes are *best* codes. In fact, MDS codes are the only binary codes that can guarantee exactly one nonzero entry in A per column, and these entries always achieve maximum secrecy for each $\mu \in [\![0, n]\!]$. Thus, they are proved to be best codes because they satisfy the sufficient condition for best by maximizing (15) for all $\mu \in [\![0, \mu]\!]$. Due to the structural similarities of A and $A^{\perp}$, it was further shown that if $\mathcal{C}$ is a best code, then so is $\mathcal{C}^{\perp}$. Finally, it was shown in [34] that the equivocation matrix can be completely filled using only knowledge of the full-rank square submatrices in G; in other words, knowledge of the revealed-bit patterns counted in $a_{k,n-k}$ is sufficient to completely characterize a code's equivocation.

There are additional properties of these matrices that make them useful for coset code analysis. For example, it is shown in Figure 5 that revealed-bit patterns r counted along the same diagonal of A must have the same value for $\text{rank}(G_r)$. In fact, one can start from the bottom $\times$ in Figure 5 and fill out the entire equivocation matrix by looking for sets of columns in G with rank zero, then rank one, and so on. Consider, e.g., the largest collection of columns in G with rank zero. Each column in this set must be an all-zero column. Thus, all subsets of the set also have rank zero, and can be counted along the rank-zero diagonal for the appropriate size of the pattern. When repeating the exercise for the rank-one diagonal, one can consider large sets of columns in G with rank one. These must consist either of identical columns, or zero columns mixed with identical columns. Since the subsets of these sets with only zero columns were already counted in the previous diagonal, they should not be counted again, but all other subsets of these larger sets will have rank one. This procedure can be repeated until the remaining revealed-bit patterns are simply accounted for in the rank-$(n-k)$ diagonal of A.

$$A = \begin{bmatrix} \times & + & \circ & \cdots & * & 0 & 0 & \cdots & 0 \\ 0 & \times & + & \circ & \cdots & * & \ddots & \ddots & \vdots \\ 0 & 0 & \times & + & \circ & \cdots & * & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & \times & + & \circ & \cdots & * \end{bmatrix}$$

Figure 5. Diagonal properties of the equivocation matrix A. All revealed-bit patterns r counted in the same diagonal of A have the same value for $\text{rank}(G_r)$; patterns counted in $\times$ slots have rank 0, patterns counted in $+$ slots have rank 1, patterns counted in $\circ$ slots have rank 2, ..., patterns counted in $*$ slots have rank $(n-k)$.

Notice that the properties of the equivocation matrix allow for the discovery of relationships between codes that hold for small codes and large codes as well. Studying patterns in small codes often yields great insight that can then be extended to codes of all sizes through analytical proofs. Additional insights into the existence of best codes that arise from the properties of equivocation matrices are given below in Section 5.

4. Searching for Best Codes

4.1. Notions of Equivalence in Wiretap Codes

In general coding theory, there is a notion of *code equivalence*. Consider the following definition.

Definition 3. *Let $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$ be two $(n, n-k)$ linear codes with generator matrices G_α and G_β, respectively. Then $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$ are equivalent if there exists an $(n-k \times n-k)$ invertible scrambling matrix F and $(n \times n)$ permutation matrix Π such that*

$$G_\beta = FG_\alpha\Pi. \tag{19}$$

The codes $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$ have the same code parameters, e.g., code rate and minimum Hamming distance d. The effect of F is to perform elementary row operations on G_α, which does not alter the set of codewords, but rather changes the mapping of messages to codewords when the codes are used for error correction [25,26]. When the codes are used for secrecy with the coset coding approach, the mapping of auxiliary messages to codewords is altered, but the sets of codewords in the cosets remain unchanged by F. The codewords of the two equivalent codes are identical up to a consistent reordering of the symbols in the codewords according to Π. This reordering holds for error correction and secrecy applications.

4.2. Search Space Reduction Techniques

In this section, we outline techniques for searching through all possible codes of small size. This requires a reduction in the search space of all codes so that (11) can be used to efficiently evaluate the average equivocation (2).

Let us consider the example code defined by the generator matrix in (5) with codewords arranged as in Table 1. Although this code is of a very small size, we can learn much from observing its structure and comparing it to other codes of the same size (i.e., $n = 4$, and $k = 2$). Suppose we take a naive approach to counting all linear $(4, 2)$ block codes and their accompanying coset structures. Using simple counting techniques we find that there are 105 different ways to choose 2 of 15 potential nonzero codewords. These choices form the bases of a code space, and hence define different generator matrices G. However, most of them are, in fact, isomorphisms of each other. Either they give the same code exactly, or some equivalent code.

Lemma 2. *If generator matrices G_α and G_β correspond to respective equivalent codes $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$, then the respective equivocation matrices formed by coset coding with these codes A_α and A_β are identical.*

Proof. The proof of this lemma is straightforward. From Definition 3, we see that $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$ are equivalent codes if $G_\alpha = FG_\beta\Pi$ for some invertible scrambling matrix F and a permutation matrix Π. As F does not change the cosets of the wiretap code, it can have no effect on the equivocation. For any revealed bit pattern $r = \{r_1, r_2, \ldots, r_\mu\}$ with elements from $[\![1, n]\!]$, let $\pi(r)$ be the set of indices resulting from the reordering of Π; that is, $\pi(r_i)$ is

the new index of the column $(G_\alpha)_{r_i}$ in G_β for $i \in [\![1, \mu]\!]$. Thus, for any revealed bit pattern r, we have that

$$\text{rank}[(G_\beta)_{\pi(r)}] = \text{rank}[(G_\alpha)_r] \tag{20}$$

since $(G_\beta)_{\pi(r)}$ and $(FG_\alpha)_r$ are equivalent up to a reordering of the columns. By noting that the equivocation matrix must consider (11) for all patterns r, the equivalence of A_α and A_β is proved. □

Although the relationship in Lemma 2 is all that is needed to remove most (if not all) isomorphic generators from consideration when trying to analyze all codes of a specific size, we still benefit from known algorithms and/or shortcuts that can help us to remove a significant portion of isomorphic generators without having to test for equivalence. One way to remove a number of isomorphic codes from the list is to consider only systematic generators G. We recall that any generator matrix of a linear code can be put into systematic form through row operations and column pivots [25,26], and the resultant code is, therefore, equivalent to the original code. For the $n = 4$ and $k = 2$ case, this results in only 16 possible codes, and yet many of these are still isomorphic to each other leaving a list of codes with lingering redundancies.

Consider the graph-theoretic approach to algorithmically removing isomorphic codes by simply forming Tanner graphs, but based on generator matrices. For example, let us consider graphs corresponding to the following two systematic generators

$$G_A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \qquad G_B = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}. \tag{21}$$

Let v_0, v_1, v_2, v_3 be column nodes and u_0, u_1 be row nodes. Then connect node u_i to node v_j iff $G_{i,j} = 1$. The generators then produce the graphs in Figure 6. The two graphs can be made equal by swapping labels in one of the graphs between v_0 & v_1, v_2 & v_3, and u_0 & u_1; therefore, they are isomorphic graphs, and the codes that represent them are likewise isomorphic codes. Removing all such graph isomorphisms results in a list of seven unique systematic generators of size 2×4. The respective systematic generator matrices for Codes 1 through 6 represent Codes 1 through 6 in Figures 2 and 3. Codes 6 and 7 are given by the respective generator matrices

$$G_6 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \qquad G_7 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}. \tag{22}$$

Although these codes do not create isomorphic graphs, they are clearly equivalent codes since G_6 can be created from G_7 with a single row operation followed by a column swap [25,26]. Furthermore, the code defined in (5) is also isomorphic to the codes produced by G_6 and G_7. The final redundant code can therefore be removed by inspection, leaving only the six unique codes. Examination of the equivocation matrices for all codes of this size shows that Code 6 is indeed best, in that it maximizes (15) for all $\mu \in [\![0, n]\!]$.

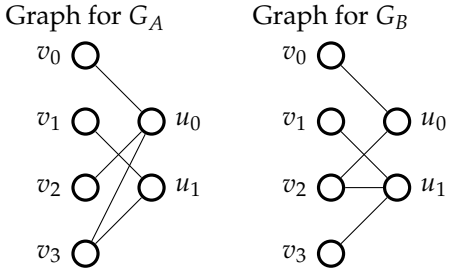


Figure 6. Two isomorphic bipartite graphs that represent equivalent generators.

Any set of algorithms that follow these guidelines for reducing the search space of all possible codes can be applied to any (n,k) design choices. Provided that both size parameters are small, numerical techniques can then create and compare all codes of the same size to identify the best ones. Although this approach will certainly not work for finding large best codes, it has been used effectively to identify several small best codes and various properties of best codes, which have then been proved analytically [32,33]. All (8,4) coset codes are given in the top plot of Figure 7, and all (9,6) coset codes are given in the bottom plot of Figure 7 by way of examples. Each of these cases has a best code that is provably-best through the sufficient condition of maximizing (15) for all $\mu \in [\![0, \mu]\!]$. The best code for the (8,4) case has generator and equivocation matrices

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}, \tag{23}$$

$$A = \begin{bmatrix} 1 & 8 & 28 & 56 & 56 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 14 & 56 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 28 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \tag{24}$$

while the best code for the (9,6) case has generator and equivocation matrices

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}, \tag{25}$$

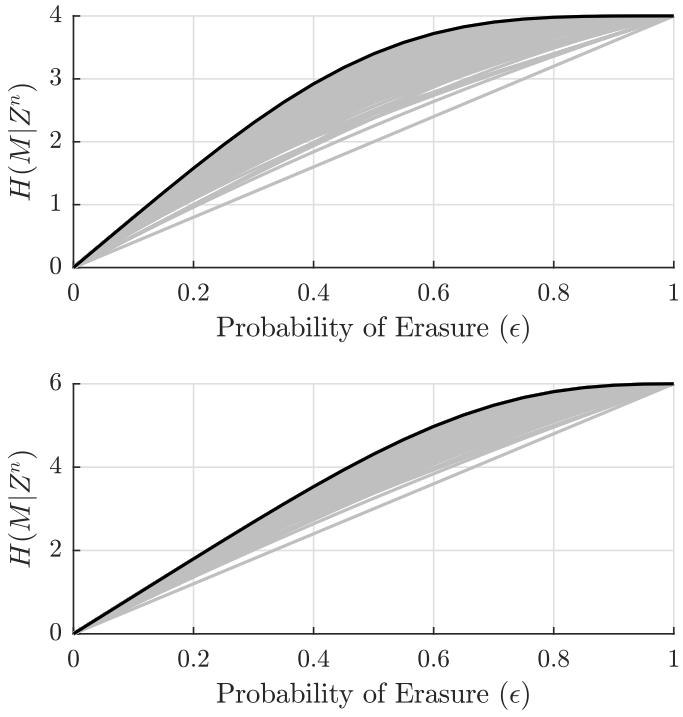


Figure 7. Equivocation of all $n = 8$, $k = 4$ secrecy codes (**top**) and all $n = 9$, $k = 6$ secrecy codes (**bottom**) as a function of Eve's channel erasure probability ϵ. The best code exists and is given by the black line in each case.

$$A = \begin{bmatrix} 1 & 9 & 34 & 56 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 28 & 117 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 & 125 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 84 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{26}$$

5. Search Results: Best Codes Do Not Always Exist

It is natural to hypothesize that for every (n, k) pair for which a coset code exists, there should be a best code. The simulation results, however, have shown this idea to be false. In this section, we prove that not all (n, k) parameters for coset codes have a best code. We also present and prove a theorem based on the existence of best codes and equivocation matrices.

Consider coset codes for $n = 11$ and $k = 6$. The search through all codes of these size parameters is time consuming. G is 5×11, and the left-most 5×5 block in G can be fixed to I_5, the 5×5 identity, using the systematic technique from Section 4. However, there remain 30 bits in G to set, and we have no efficient technique to move quickly from unique code to unique code. With the search-space-reduction techniques from Section 4, we find only 20,755 codes that do not form graph isomorphisms, which can actually be evaluated relatively quickly once they are identified. When we evaluate all possible codes, we find two candidate codes to be best. Each maximizes (15) for a range of μ values, but no code maximizes (15) for all $\mu \in [\![0, n]\!]$. We call the two competing codes Code L and Code R. These codes are defined by their respective generator matrices

$$G_L = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \tag{27}$$

and

$$G_R = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}. \tag{28}$$

The equivocation matrices are

$$A_L = \begin{bmatrix} 1 & 11 & 55 & 165 & 305 & 287 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 25 & 175 & 417 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 45 & 325 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 165 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 55 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 11 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

and

$$A_R = \begin{bmatrix} 1 & 11 & 55 & 163 & 300 & 288 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 30 & 173 & 420 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 42 & 326 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 165 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 55 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 11 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Code L optimizes the *left* side of the equivocation matrix, while Code R optimizes the *right* side. Both manage to maximize (15) for $\mu = (n-k)$, but in different ways. Note that the number of full-rank patterns of size $(n-k) = 6$ is 288 for Code R and only 287 for Code L. However, all remaining length-6 patterns have rank five for Code L, while exactly one pattern has rank four for Code R; thus, both codes have the same sum of ranks at $\mu = (n-k)$. Finally, we note that the actual equivocation curves for these codes cross. The curves are plotted in the top part of Figure 8, but the crossing point in ϵ can only be seen when the difference between the equivocation for Code L (given as $\mathbb{H}_L(M|Z^n)$) and the equivocation for Code R (given as $\mathbb{H}_R(M|Z^n)$) is plotted. This difference is given in the bottom plot of Figure 8, where we see Code L as superior (having higher equivocation) for higher ϵ. This high-ϵ region corresponds to the left side of the equivocation matrix, where a larger number of erasures are occurring. The crossing point occurs at roughly $\epsilon = 0.444$.

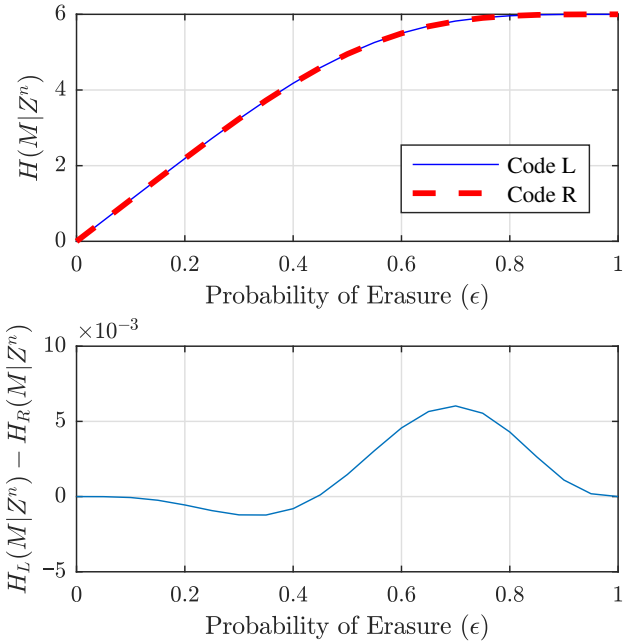


Figure 8. Equivocation curves for the two competing codes for the $n = 11$, $k = 6$ best code (**top**), and the difference between the two equivocation curves (**bottom**). Code L is best for the left-hand side of the equivocation matrix (right-hand side of the equivocation curve), and Code R is best for the right-hand side of the equivocation matrix (left-hand side of the equivocation curve).

Now that we understand that there exist (n,k) size parameters that do not have a best code, we can state the following new theorem.

Theorem 1. *Consider all possible coset codes for the size parameters (n,k). There exists a best coset code with these size parameters that satisfies the sufficient condition for best by maximizing (15) for all $\mu \in [\![0,n]\!]$ for use over the BEWC if and only if there exists a best code that satisfies the same sufficient condition for being classified as best for the size parameters $(n,n-k)$.*

Proof. The proof is straightforward using the dual relationship of the equivocation matrices given in Lemma 1. Recall that the lemma gives $A^{\perp}$ as being equal to A with the column order reversed while preserving the bottom left and upper right triangles of zeros. Since every code has a dual, the range of possible equivocation matrices for $A^{\perp}$ is the same as for A with this reordering. Optimality in one case implies optimality in the other case, and sub-optimality in one case implies sub-optimality in the other case. □

6. Principles of Code Design for Good Coset Codes of Any Size

In [33], we showed that Hamming codes and their duals (simplex codes) are almost surely best codes for their size parameters, and yet a complete proof of this almost sure fact is still missing, although we improve the result from [33] in Section 7. It would be good if a set of specific code families could be proved best, or even better if a generic algorithm for building best codes of any size parameters could be found. In this section, we present code design guidelines towards this goal. The end result is a set of design choices that can lead to very good codes of any size. We also present and prove a theorem that defines the relationship between maximum values of (15) and best codes in the reverse direction.

6.1. High-Level Design of Good/Best Codes

Let us consider again the implications of Lemma 1, and note that if an (n, k) coset code (built from an $(n, n-k)$ linear block code $\mathcal{C}$) has an associating equivocation matrix A that maximizes the sum in (15) for all $\mu \in [\![0, n]\!]$, then that code is provably-best for its size. Also, Theorem 1 states that the existence of the provably-best code $\mathcal{C}$ ensures the existence of a provably-best $(n, n-k)$ coset code (built from an (n, k) linear block code $\mathcal{C}^{\perp}$) such that the associating equivocation matrix $A^{\perp}$ likewise maximizes the sum in (15) for all $\mu \in [\![0, n]\!]$. Let G be a systematic generator matrix for $\mathcal{C}$ of the form

$$G = \begin{bmatrix} I_{n-k} & P \end{bmatrix}, \tag{29}$$

where P is an $(n-k) \times k$ submatrix of G. Then, it is well known [26] that an equivalent systematic generator for $\mathcal{C}^{\perp}$ can be formed by

$$G^{\perp} = \begin{bmatrix} I_k & -P^T \end{bmatrix}. \tag{30}$$

A code design algorithm for $\mathcal{C}$ chooses columns of P or equivalently $-P^T$. Since we are only considering binary codes in this paper, we will drop the negative sign and consider only P^T.

Consider Figure 9 as we discuss design principles for good codes. Suppose columns of P are chosen to ensure no rank-zero patterns exist in the revealed-bit patterns for the coset code defined by $\mathcal{C}$. This only amounts to not allowing any column of P to be all-zero, which sets an optimal structure for the elements in A along the diagonal dictated by the symbol $\times$, including the $\otimes$ entry. Since we know that optimal structures in $A^{\perp}$ also imply optimal structures in A, we can now shift our attention to P^T. Suppose we also ensure that no all-zero columns exist in P^T. This would fix the same optimal structure in $A^{\perp}$, which maps exactly to the entries of A marked by the $\circ$ symbol, including the $\otimes$ entry. Note that the $\otimes$ symbol is meant to be a merging of the $\times$ and $\circ$ symbols, since it is guaranteed optimal by both design steps. Thus, the first nonzero diagonal and the bottom row of A are optimized by ensuring no all-zero columns or rows are in P.

$$A = \begin{bmatrix} \times & \triangleright & + & \cdots & * & 0 & 0 & \cdots & 0 \\ 0 & \times & \triangleright & \ddots & \cdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & \uplus & \cdots & \cup & 0 & 0 \\ \vdots & \ddots & \ddots & \times & \bowtie & \triangleleft & \cdots & \triangleleft & 0 \\ 0 & \cdots & 0 & 0 & \otimes & \circ & \circ & \cdots & \circ \end{bmatrix}$$

Figure 9. Pictorial representation of code design inspired by Lemma 1. Each diagonal can be designed by considering G, while each row can be designed by considering $G^{\perp}$. The designs meet in the middle at the $\mu = (n-k)$th column. Symbols are merged in this column to indicate the meeting of designs.

We can continue this design process to the next nonzero diagonal and row in A by ensuring no weight-one columns or rows are in P and that all rows and columns of P are unique. The problem is not necessarily the weight of the columns or rows, but rather that all weight-one columns already exist in G due to the systematic structure of the matrix. Thus, allowing any column of P to have weight one ensures a duplicate column in G, and the pattern associated with those two columns would have rank one in the submatrix of G, rather than rank two. If the size of P is such that it can be formed with all unique columns in G and $G^{\perp}$, we guarantee optimality in the entries of the equivocation matrix marked, respectively, by the symbols $\triangleright$ and $\triangleleft$ along with the doubly designed entry marked by $\bowtie$.

This process can continue, albeit at greater and greater complexity, by ensuring that the columns and rows of P do not introduce certain linear dependencies in the columns of G and $G^{\perp}$, respectively. At some point it will not be possible to ensure no dependencies of a particular size unless a maximum distance seperable (MDS) code exists for the size parameters in question [33], but effort towards removing many small linear dependencies in the columns of G and $G^{\perp}$ still results in better codes, and may lead to a best code in some cases.

Note also that this approach is similar to designing codes with good generalized Hamming weights outlined in [24]. The minimum distance of the dual code is the first generalized Hamming weight of the code itself, and the worst case equivocation (see works on the wiretap channel of type II [23]) is perfectly characterized by the generalized Hamming weights. When we couple these facts from [24] with Lemma 1, we find that codes which exhibit (along with their dual codes) large minimum distance and/or good distance properties will also provide good wiretap codes. We can use the same technique outlined above, wherein optimizing the distance properties of the dual code builds an optimum equivocation matrix from the left, and optimizing distance properties of the code itself builds an optimum equivocation matrix from the right.

6.2. Best Codes from the Outside in

In the previous subsection, we saw that an overall design idea for building good, and perhaps best, codes can operate from the outside entries of the equivocation matrix and work towards the inside entries. Here, we present a property of best codes that makes this idea rigorous using two theorems from [36]. First, let us rewrite the sum from (15) as

$$s_{\mu} = \sum_{r \in \mathcal{R}_{\mu}} \operatorname{rank}(G_r). \tag{31}$$

Then let $s = (s_0, s_1, \ldots, s_n)$ be the collection of these values for a code $\mathcal{C}$ with $(n-k) \times n$ generator matrix G. Let $s' = (s'_0, s'_1, \ldots, s'_n)$ be the values from (31) calculated with the generator matrix for $\mathcal{C}'$ and let $s'' = (s''_0, s''_1, \ldots, s''_n)$ be the values from (31) calculated with the generator matrix for $\mathcal{C}''$. Also, let γ be the smallest value of μ such

that $s'_\mu \neq s''_\mu$, and let δ be the largest value of μ such that $s'_\mu \neq s''_\mu$. This implies that $s'_i = s''_i$ for $i \in \{[\![0, \gamma-1]\!], [\![\delta+1, n]\!]\}$. Note that $s'_0 = s''_0 = 0$ and $s'_n = s''_n = n-k$.

Lemma 3 (Corollary 1 from [36]). *If $s'_\gamma > s''_\gamma$, then $\mathcal{C}''$ cannot be the best code for its size. Similarly if $s'_\gamma < s''_\gamma$, then $\mathcal{C}'$ cannot be the best code for its size.*

Lemma 4 (Corollary 2 from [36]). *If $s'_\delta > s''_\gamma$, then $\mathcal{C}''$ cannot be the best code for its size. Similarly if $s'_\delta < s''_\delta$, then $\mathcal{C}'$ cannot be the best code for its size.*

From these two lemmas, our new theorem follows.

Theorem 2. *If $\mathcal{C}$ is best for its size, then compared to any other code of the same size, say $\mathcal{C}'''$ with $s''' = (s'''_0, s'''_1, \ldots, s'''_n)$ being the values from (31) calculated with the generator matrix for $\mathcal{C}'''$, it must be true that $s_\gamma > s'''_\gamma$ and that $s_\delta > s'''_\delta$.*

The proof is immediate from application of Lemmas 3 and 4. The theorem also completes our understanding, given the theoretical results to date, of the relationship between (15) and a best code. That is, any code that maximizes (15) for all $\mu \in [\![0, n]\!]$ is best; and any best code must at least maximize (15) for all $\mu \in \{[\![0, \gamma^*-1]\!], [\![\delta^*+1, n]\!]\}$. For this statement, γ^* is the maximum γ value obtained by letting $\mathcal{C}'$ be the best code and letting $\mathcal{C}''$ range over all other codes of its size. Similarly, δ^* is the minimum δ value obtained by letting $\mathcal{C}'$ be the best code and letting $\mathcal{C}''$ range over all other codes of its size.

7. On the Optimality of Simplex and Hamming Codes: Simplex Codes Are Better than Repeating Column Codes

In this section we prove that the simplex code maximizes (15) for all μ when compared to all codes of the same size with one column in G repeated any number of times.

Theorem 3. *For any integer $m \geq 2$, $n = 2^m - 1$, and $(n-k) = m$, the $(2^m-1, m)$ simplex code is better for secrecy over the BEWC(ϵ) for all $\epsilon \in (0,1)$ than any code with exactly one column appearing more than once in the generator matrix.*

Proof. The generator matrix G for the simplex code comprises all non-zero binary m tuples. Thus,

$$G = \begin{bmatrix} \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_n \end{bmatrix}, \tag{32}$$

where $\mathrm{g}_i \neq \mathrm{g}_j$ for $i \neq j$, and all columns have weight of at least 1. Suppose we also have a matrix G' such that

$$G' = \begin{bmatrix} \mathbf{g}'_1 & \mathbf{g}'_2 & \cdots & \mathbf{g}'_n \end{bmatrix}, \tag{33}$$

where

$$\mathbf{g}'_i = \begin{cases} \mathbf{g}_i \text{ for } 3 \leq i \leq n, \\ \mathbf{g}_2 \text{ for } i = 1, 2. \end{cases} \tag{34}$$

It was shown in [33] that the choice of index for the repeated column can be made without loss of generality. Similarly we have a matrix G'' defined as

$$G'' = \begin{bmatrix} \mathbf{g}''_1 & \mathbf{g}''_2 & \cdots & \mathbf{g}''_n \end{bmatrix}, \tag{35}$$

where

$$\mathbf{g}''_i = \begin{cases} \mathbf{g}_i \text{ for } 4 \leq i \leq n, \\ \mathbf{g}_2 \text{ for } i = 1, 2, 3. \end{cases} \tag{36}$$

For $j \in [\![1, n]\!]$ and $\mu \in [\![1, n]\!]$, we define a function ϕ as

$$\phi(j, \mu) = \sum_{r \in [\![1,n]\!] \setminus \{j\} : |r| = \mu - 1} \operatorname{rank} \begin{bmatrix} \mathbf{g}_j & G_r \end{bmatrix}, \tag{37}$$

where $\mathbf{g}_j$ is the jth column in G. As was shown in [33], all differences in rank between submatrices of G and G' are contained within the equations $\phi(1, \mu)$ and $\phi'(1, \mu)$ because all columns other than the first are identical. It was also shown in [33] that $\phi'(1, \mu) < \phi(1, \mu)$.

If we consider G'', we see that similar to the previous case, there is only one difference in a column between G' and G''. As with the prior case, this implies that all differences between G' and G'' must be contained within a single phi function. In this case, all differences are contained within $\phi''(3, \mu)$. Due to the fact that within G'' columns 1, 2, and 3 are identical, it is clear that $\phi''(1, \mu) = \phi''(2, \mu) = \phi''(3, \mu)$.

Next, consider $\phi'(1, \mu)$ and $\phi''(1, \mu)$. Notice that the only index that differs between G' and G'' is index 3 and, therefore,

$$\phi_{G' \setminus \mathbf{g}'_3}(1, \mu) = \phi_{G'' \setminus \mathbf{g}''_3}(1, \mu). \tag{38}$$

Because $\mathbf{g}''_3 = \mathbf{g}''_2 = \mathbf{g}''_1$, adding $\mathbf{g}''_3$ to $\phi_{G'' \setminus \mathbf{g}''_3}(1, \mu)$ cannot increase the rank of the subsets used to calculate $\phi''(1, \mu)$ and, therefore,

$$\phi''(1, \mu) \leq \phi'(1, \mu) < \phi(1, \mu). \tag{39}$$

This shows that G'' cannot have equivocation greater than G' and as such must be worse than G.

The inductive extension to any number of repeats of a single column is now straightforward. □

This result improves upon the best result to date in [33], which showed that simplex codes are better than codes with a single repeated column in G. Note that other codes with multiple unique columns appearing as repeats in G are unlikely to improve upon the equivocation over the simplex code. Additional repeats weaken the equivocation matrix in the $\mu = 2$ column, and these repeats are likely to harm other columns in A as well. Thus, we remain convinced that simplex codes are best for their size. We likewise continue to conjecture the optimality of Hamming codes due to their dual relation to simplex codes in Lemma 1.

8. Conclusions

This paper presents several results regarding the design of best coset codes for physical-layer security over the binary erasure wiretap channel. Equivocation matrices are defined and shown to be a useful tool in obtaining both practical and theoretical results regarding best codes. The search space reduction techniques showcased in this paper reduce the computation time required to find best codes of a given size. It was further shown that best codes do not exist for all size parameters of codes. The properties of best codes have also been extended to an *outside-in* property that shows that equivocation matrices of best codes must be optimal working from the outside columns of the matrix. Finally, we have shown that simplex codes are better than a family of codes with a single column repeated a number of times in the generator matrix.

This paper provides a framework on which future discoveries can be made. In particular, proving that simplex and Hamming codes are best for their size compared to all other codes may build on the results of this paper. Efficient algorithms for designing best codes may also be found by following the guidelines outlined in this work.

Author Contributions: Conceptualization, W.K.H.; methodology, W.K.H., T.W., A.S. and M.S.; formal analysis, W.K.H., T.W., A.S. and M.S.; writing—original draft preparation, W.K.H., T.W., A.S. and M.S.; writing—review and editing, W.K.H.; project administration, W.K.H. All authors have read and agreed to the published version of the manuscript.

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

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
2. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
3. Luzzi, L. Coding Theory Advances in Physical-Layer Secrecy. In *Physical-Layer Security for 6G*; Wiley: Hoboken, NJ, USA, 2024; pp. 19–42.
4. Durisi, G.; Koch, T.; Popovski, P. Toward Massive, Ultrareliable, and Low-Latency Wireless Communication with Short Packets. *Proc. IEEE* **2016**, *104*, 1711–1726. [CrossRef]
5. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
6. Burange, A.; Misalkar, H. Review of Internet of Things in development of smart cities with data management amp; privacy. In Proceedings of the Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances, Ghaziabad, India, 19–20 March 2015; pp. 189–195. [CrossRef]
7. McKay, K.A.; Bassham, L.E.; Turan, M.S.; Mouha, N.W. *Report on Lightweight Cryptography*; NIST Publications: Gaithersburg, MD, USA, 2017; pp. 1–21.
8. Xiong, L. Harnessing personal data from Internet of Things: Privacy enhancing dynamic information monitoring. In Proceedings of the Collaboration Technologies and Systems (CTS), 2015 International Conference, Atlanta, GA, USA, 1–5 June 2015; p. 37. [CrossRef]
9. Liang, W.; Peiji, S. Research on the protection algorithm and model of personal privacy information in internet of thing. In Proceedings of the E-Business and E-Government (ICEE), 2011 International Conference, Shanghai, China, 6–8 May 2011; pp. 1–4. [CrossRef]
10. Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: Cambridge, UK, 2011.
11. Johnson, M.H.; Harrison, W.K. A rateless approach to physical-layer security. In Proceedings of the IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; IEEE: New York, NY, USA, 2018; pp. 1–6.
12. Jensen, B.; Clark, B.; Flanary, D.; Norman, K.; Rice, M.; Harrison, W.K. Physical-Layer Security: Does it Work in a Real Environment? In Proceedings of the IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–7.
13. Flanary, D.; Jensen, B.; Clark, B.; Norman, K.; Nelson, N.; Rice, M.; Harrison, W.K. Manufacturing an Erasure Wiretap Channel from Channel Sounding Measurements. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019; IEEE: New York, NY, USA, 2019; pp. 320–324.
14. Rice, M.; Clark, B.; Flanary, D.; Jensen, B.; Nelson, N.; Norman, K.; Perrins, E.; Harrison, W.K. Physical-layer security for vehicle-to-everything networks: Increasing security while maintaining reliable communications. *IEEE Veh. Technol. Mag.* **2020**, *15*, 68–76. [CrossRef]
15. Harman, D.; Knapp, K.; Sweat, T.; Lundrigan, P.; Rice, M.; Harrison, W. Physical Layer Security: Channel Sounding Results for the Multi-Antenna Wiretap Channel. *Entropy* **2023**, *25*, 1397. [CrossRef]
16. Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* **1948**, *28*, 656–715. [CrossRef]
17. Wyner, A.D. The Wire-Tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
18. Csiszár, I.; Körner, J. Broadcast Channels with Confidential Messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348. [CrossRef]
19. Harrison, W.K.; Almeida, J.; Bloch, M.R.; McLaughlin, S.W.; Barros, J. Coding for Secrecy: An Overview of Error-Control Coding Techniques for Physical-Layer Security. *IEEE Signal Process. Mag.* **2013**, *30*, 41–50. [CrossRef]
20. Bloch, M.R.; Hayashi, M.; Thangaraj, A. Error-Control Coding for Physical-Layer Secrecy. *Proc. IEEE* **2015**, *103*, 1725–1746. [CrossRef]

21. Bloch, M.R.; Laneman, J.N. Strong Secrecy From Channel Resolvability. *IEEE Trans. Inf. Theory* **2013**, *59*, 8077–8098. [CrossRef]
22. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2006.
23. Ozarow, L.H.; Wyner, A.D. Wiretap Channel II. *AT&T Bell Lab. Tech. J.* **1984**, *63*, 2135–2157. [CrossRef]
24. Wei, V. Generalized Hamming weights for linear codes. *IEEE Trans. Inf. Theory* **1991**, *37*, 1412–1418. [CrossRef]
25. Lin, S.; Costello, D.J., Jr. *Error Control Coding*, 2nd ed.; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2004.
26. Moon, T.K. *Error Correction Coding: Mathematical Methods and Algorithms*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2005.
27. Richardson, T.; Urbanke, R. *Modern Coding Theory*; Cambridge University Press: New York, NY, USA, 2008.
28. Al-Hassan, S.; Ahmed, M.Z.; Tomlinson, M. Secrecy coding for the wiretap channel using best known linear codes. In Proceedings of the Global Information Infrastructure Symposium, Trento, Italy, 28–31 October 2013; pp. 1–6. [CrossRef]
29. Al-Hassan, S.; Ahmed, M.; Tomlinson, M. Extension of the parity check matrix to construct the best equivocation codes for syndrome coding. In Proceedings of the Global Information Infrastructure and Networking Symposium (GIIS), Montreal, QC, Canada, 15–19 September 2014; pp. 1–3. [CrossRef]
30. Zhang, K. Secure Coding Schemes and Code Design for the Wiretap Channel. Ph.D Thesis, University of Porto, Porto, Portugal, 2014.
31. Zhang, K.; Tomlinson, M.; Ahmed, M.; Ambroze, M.; Rodrigues, M. Best binary equivocation code construction for syndrome coding. *IET Commun.* **2014**, *8*, 1696–1704. [CrossRef]
32. Pfister, J.; Gomes, M.; Vilela, J.P.; Harrison, W.K. Quantifying Equivocation for Finite Blocklength Wiretap Codes. In Proceedings of the IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
33. Harrison, W.K.; Bloch, M.R. On Dual Relationships of Secrecy Codes. In Proceedings of the IEEE Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 2–5 October 2018; pp. 366–372.
34. Harrison, W.K.; Bloch, M.R. Attributes of Generators for Best Finite Blocklength Coset Wiretap Codes over Erasure Channels. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019; pp. 827–831.
35. Harrison, W.K. Exact Equivocation Expressions for Wiretap Coding Over Erasure Channel Models. *IEEE Commun. Lett.* **2020**, *24*, 2687–2691. [CrossRef]
36. Swain, A.; Harrison, W.K. Best Linear Wiretap Coset Codes Must Maximize Minimum Distance. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Ann Arbor, MI, USA, 22–27 June 2025; pp. 1–6. [CrossRef]
37. Forney, G. Dimension/length profiles and trellis complexity of linear block codes. *IEEE Trans. Inf. Theory* **1994**, *40*, 1741–1752. [CrossRef]
38. Cai, N.; Chan, T. Theory of Secure Network Coding. *Proc. IEEE* **2011**, *99*, 421–437. [CrossRef]
39. Wong, C.W.; Wong, T.; Shea, J. Secret-Sharing LDPC Codes for the BPSK-Constrained Gaussian Wiretap Channel. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 551–564. [CrossRef]
40. Baldi, M.; Ricciutelli, G.; Maturo, N.; Chiaraluce, F. Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel. In Proceedings of the IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 435–440.
41. Harrison, W.K.; Beard, E.; Dye, S.; Holmes, E.; Nelson, K.; Gomes, M.A.C.; Vilela, J.P. Implications of coding layers on physical-layer security: A secrecy benefit approach. *Entropy* **2019**, *21*, 755. [CrossRef] [PubMed]
42. Thangaraj, A.; Dihidar, S.; Calderbank, A.R.; McLaughlin, S.W.; Merolla, J.M. Applications of LDPC Codes to the Wiretap Channels. *IEEE Trans. Inf. Theory* **2007**, *53*, 2933–2945. [CrossRef]
43. Shoushtari, M.; Harrison, W.K. New Dual Relationships for Error-Correcting Wiretap Codes. In Proceedings of the 2021 IEEE Information Theory Workshop (ITW), Kanazawa, Japan, 17–21 October 2021; pp. 1–6. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.