Aalborg Universitet

AALBORG UNIVERSITY
DENMARK

Relative generalized matrix weights of matrix codes for universal security on wire-tap networks

Martinez Peñas, Umberto; Matsumoto, Rytaro Yamashita

Published in:
I E E E Transactions on Information Theory

DOI (link to publication from Publisher):
10.1109/TIT.2017.2766292

Creative Commons License
Unspecified

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

Link to publication from Aalborg University

Citation for published version (APA):
Martinez Peñas, U., & Matsumoto, R. Y. (2018). Relative generalized matrix weights of matrix codes for universal security on wire-tap networks. *I E E E Transactions on Information Theory*, *64*(4), 2529 - 2549. https://doi.org/10.1109/TIT.2017.2766292

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy
If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Relative Generalized Matrix Weights of Matrix Codes for Universal Security on Wire-Tap Networks

Umberto Martínez-Peñas, *Student Member, IEEE*, and Ryutaroh Matsumoto, *Member, IEEE*

***Abstract*— Universal security over a network with linear network coding has been intensively studied. However, previous linear codes and code pairs used for this purpose were linear over a larger field than that used on the network, which restricts the possible packet lengths of optimal universal secure codes, does not allow to apply known list-decodable rank-metric codes and requires performing operations over a large field. In this paper, we introduce new parameters (relative generalized matrix weights and relative dimension/rank support profile) for code pairs that are linear over the field used in the network, and show that they measure the universal security performance of these code pairs. For one code and non-square matrices, generalized matrix weights coincide with the existing Delsarte generalized weights, hence we prove the connection between these latter weights and secure network coding, which was left open. As main applications, the proposed new parameters enable us to: 1) obtain optimal universal secure linear codes on noiseless networks for all possible packet lengths, in particular for packet lengths not considered before, 2) obtain the first universal secure list-decodable rank-metric code pairs with polynomial-sized lists, based on a recent construction by Guruswami *et al*; and 3) obtain new characterizations of security equivalences of linear codes. Finally, we show that our parameters extend relative generalized Hamming weights and relative dimension/length profile, respectively, and relative generalized rank weights and relative dimension/intersection profile, respectively.**

***Index Terms*— Network coding, rank weight, relative dimension/rank support profile, relative generalized matrix weight, universal secure network coding.**

I. Introduction

LINEAR network coding was first studied in [1], [23] and [25], and enables us to realize higher throughput than the conventional storing and forwarding. Error correction in this context was first studied in [5], and security, meaning information leakage to an adversary wire-tapping links in the network, was first considered in [6]. In that work, the authors give outer codes with optimal information rate for the given security performance, although using large fields on the network. The field size was later reduced in [15] by reducing the information rate. In addition, the approach in [14] allows us to see secure network coding as a generalization of secret sharing [4], [37], which is a generalization of the wire-tap channel of type II [33].

However, these approaches [6], [14], [15] require knowing and/or modifying the underlying linear network code, which does not allow us to perform, for instance, random linear network coding [21], which achieves capacity in a decentralized manner and is robust to network changes. Later, the use of pairs of linear (block) codes as outer codes was proposed in [39] to protect messages from errors together with information leakage to a wire-tapping adversary (see Remark 4), depending only on the number of errors and wire-tapped links, respectively, and not depending on the underlying linear network code, which is referred to as *universal security* in [39].

In [39], the encoded message consists of n (number of outgoing links from the source) vectors in $\mathbb{F}_{q^m}$ or $\mathbb{F}_q^m$, called packets, where m is called the packet length and where $\mathbb{F}_q$ is the field used for the underlying linear network code, as opposed to previous works [6], [14], [15], where $m = 1$. The universal performance of the proposed linear codes in [39] is measured by the rank metric [9], and the authors in [39] prove that linear codes in $\mathbb{F}_{q^m}^n$ with optimal rank-metric parameters when $n \leq m$ [17], [36] are also optimal for universal security. This approach was already proposed in in [38] and [40] for error correction, again not depending on the underlying network code. Later the authors in [20] obtained the first list-decodable rank-metric codes whose list sizes are polynomial in the code length and which are able to list-decode universally on linearly coded networks roughly twice as many errors as optimal rank-metric codes [17], [36] can correct. The rank metric was then generalized in [24] to relative generalized rank weights (RGRWs) and relative dimension/intersection profiles (RDIPs), which were proven in [24] to measure exactly and simultaneously the universal security performance and error-correction capability of pairs of linear codes, in the same way as relative generalized Hamming weights (RGHWs) and relative dimension/length profiles (RDLPs) [26], [42] do on wire-tap channels of type II.

Manuscript received December 7, 2016; revised August 25, 2017; accepted October 15, 2017. Date of publication October 25, 2017; date of current version March 15, 2018. U. Martínez-Peñas was supported by The Danish Council for Independent Research under Grant DFF-4002-00367 and Grant DFF-5137-00076B (EliteForsk-Rejsestipendium). R. Matsumoto was supported by the Japan Society for the Promotion of Science under Grant 26289116. This paper was presented at the 2016 54th Annual Allerton Conference on Communication, Control, and Computing [29].

U. Martínez-Peñas is with the Department of Mathematical Sciences, Aalborg University, 9220 Aalborg, Denmark (e-mail: umberto@math.aau.dk).

R. Matsumoto is with the Department of Information and Communication Engineering, Nagoya University, Nagoya 464-8603, Japan.

Communicated by P. Sadeghi, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2017.2766292

0018-9448 © 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

TABLE I
NEW AND EXISTING NOTIONS OF GENERALIZED WEIGHTS

Work	Paremeters	Codes they are used on	Measured security
Definitions 10 & 11, & Theorem 1	RGMW & RDRP	$\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$, $\mathbb{F}_q$-linear	Universal security on networks
[24], [32]	RGRW & RDIP	$\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, $\mathbb{F}_{q^m}$-linear	Universal security on networks
[34]	DGW	$\mathcal{C}_2 = \{0\} \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$, $\mathbb{F}_q$-linear	Universal security on networks for $\mathbb{F}_{q^m}$-linear
[26], [42]	RGHW & RDLP	$\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^n$, $\mathbb{F}_q$-linear	Security on wire-tap channels II
[31], [45]	RNGHW	$\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^n$, $\mathbb{F}_q$-linear	Non-universal security on networks

Unfortunately, the codes studied and proposed in [24], and [38]–[40] are linear over the extension field $\mathbb{F}_{q^m}$. This restricts the possible packet lengths of optimal universal secure codes, requires performing computations over the larger field $\mathbb{F}_{q^m}$ and leaves out important codes, such as the list-decodable rank-metric codes in [20], which are only linear over $\mathbb{F}_q$.

In this work, we introduce new parameters, called relative generalized matrix weights (RGMWs) and relative dimension/rank support profiles (RDRPs), for codes and code pairs that are linear over the smaller field $\mathbb{F}_q$, and prove that they measure their universal security performance in terms of the worst-case information leakage. As main applications, we obtain the first optimal universal secure linear codes on noiseless networks for all possible packet lengths, we obtain the first universal secure list-decodable rank-metric code pairs with polynomial-sized lists, and obtain new characterizations of security equivalences of linear codes.

A. Notation

Let q be a prime power and m and n, two positive integers. We denote by $\mathbb{F}_q$ the finite field with q elements, which we will consider to be the field used for the underlying linear network code (see [23, Definition 1]).

Most of our technical results hold for an arbitrary field, which we denote by $\mathbb{F}$ and which mathematically plays the role of $\mathbb{F}_q$. $\mathbb{F}^n$ denotes the vector space of row vectors of length n with components in $\mathbb{F}$, and $\mathbb{F}^{m\times n}$ denotes the vector space of $m \times n$ matrices with components in $\mathbb{F}$. Throughout the paper, a (block) code in $\mathbb{F}^{m\times n}$ (respectively, in $\mathbb{F}^n$) is a subset of $\mathbb{F}^{m\times n}$ (respectively, of $\mathbb{F}^n$), and it is called linear if it is a vector space over $\mathbb{F}$. In all cases, dimensions of vector spaces over $\mathbb{F}$ will be denoted by dim.

Finally, we recall that we may identify $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_q^{m\times n}$ as vector spaces over $\mathbb{F}_q$. Fix a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$. We define the *matrix representation map* $M_{\boldsymbol{\alpha}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m\times n}$ associated to the previous basis by

$$M_{\boldsymbol{\alpha}}(\mathbf{c}) = (c_{i,j})_{1\le i\le m, 1\le j\le n}, \tag{1}$$

where $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,n}) \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$, are the unique vectors in $\mathbb{F}_q^n$ such that $\mathbf{c} = \sum_{i=1}^m \alpha_i \mathbf{c}_i$. The map $M_{\boldsymbol{\alpha}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m\times n}$ is an $\mathbb{F}_q$-linear vector space isomorphism.

The works [24], [38]–[40] consider $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$, which are a subfamily of $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m\times n}$ through the map given in (1). In this paper, we will consider arbitrary linear (meaning $\mathbb{F}$-linear) codes in $\mathbb{F}^{m\times n}$.

B. Our Motivations

Our main motivation to study universal secure network coding is to avoid knowing and/or modifying the underlying linear network code, and in particular be able to apply our theory on random linearly coded networks [21], which achieve capacity in a decentralized manner and are robust to network changes.

Our main motivation to study pairs of linear codes is to be able to protect messages simultaneously from errors, erasures and information leakage to a wire-tapper. See also Section II and more concretely, Remark 4.

Our main motivations to study codes which are linear over the base field $\mathbb{F}_q$ instead of the extension field $\mathbb{F}_{q^m}$ are the following:

1) $\mathbb{F}_q$-linear codes with optimal rank-metric parameters [9], and thus with optimal universal security and error-correction capability, cannot be $\mathbb{F}_{q^m}$-linear for most packet lengths m when $m < n$. In many applications, packet lengths satisfying $m < n$ are required (see the discussion in [24, Sec. I-A], for instance).

2) The only known list-decodable rank-metric codes [20] with polynomial-sized lists are linear over $\mathbb{F}_q$, but not over $\mathbb{F}_{q^m}$. Hence the previous studies on universal security cannot be applied on these codes. In particular, no construction of universal secure list-decodable rank-metric coding schemes with polynomial-sized lists are known.

3) In previous works [38]–[40], the proposed codes are $\mathbb{F}_{q^m}$-linear and $m \ge n$. In many cases, this requires performing operations over a very large field, instead of the much smaller field $\mathbb{F}_q$.

C. Related Works and Considered Open Problems

We consider the following four open problems in the literature, which correspond to the main four contributions listed in the following subsection:

1) Several parameters have been introduced to measure the security performance of linear codes and code pairs on different channels, in terms of the worst-case information leakage. The original RGHWs and RDLPs [26], [42] measure security performance over wire-tap channels of type II, and relative network generalized Hamming weigths (RNGHWs) [31], [45] measure security performance over networks depending on the underlying linear network code (non-universal security). Later, RGRWs and RDIPs were introduced [24] and [32] to measure universal security performance of $\mathbb{F}_{q^m}$-linear code pairs $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$. A notion of generalized weight for one $\mathbb{F}_q$-linear code (that is, for an arbitrary $\mathcal{C}_1$ and for $\mathcal{C}_2 = \{0\}$) in $\mathbb{F}_q^{m\times n}$, called Delsarte generalized weights (DGWs), was

TABLE II

NEW AND EXISTING OPTIMAL SECURE CODES FOR NOISELESS NETWORKS (N = # LINKS, μ = # OBSERVATIONS, t = # DESTINATIONS)

Work	Universality	Field size (q) used over the network	Packet length (m)
Theorem 2	Yes	Any	Any
[39]	Yes	Any	$m \geq n$ or $n = lm$
[6]	No	$q > \binom{N}{\mu}$	–
[15]	No	$q = \Theta(N^{\mu/2})$	–
[14]	No	$q > \binom{N-1}{\mu-1} + t$ or $q > \binom{2n^3t^2-1}{\mu-1} + t$	–

TABLE III

NEW AND EXISTING CHARACTERIZATIONS OF LINEAR ISOMORPHISMS BETWEEN VECTOR SPACES OF MATRICES PRESERVING CERTAIN PROPERTIES

Work	Domain & codomain	Linearity	Properties preserved
Theorem 4	$\phi : \mathcal{V} \longrightarrow \mathcal{W}$, $\mathcal{V} \in \mathrm{RS}(\mathbb{F}^{m\times n})$, $\mathcal{W} \in \mathrm{RS}(\mathbb{F}^{m\times n'})$	$\mathbb{F}$-linear	Universal security on networks
[28]	$\phi : \mathcal{V} \longrightarrow \mathcal{W}$, $\mathcal{V} \in \mathrm{RS}(\mathbb{F}_q^{m\times n})$, $\mathcal{W} \in \mathrm{RS}(\mathbb{F}_q^{m\times n'})$	$\mathbb{F}_{q^m}$-linear	Ranks & universal security on networks
[3]	$\phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$	$\mathbb{F}_{q^m}$-linear	Ranks
[27], [30]	$\phi : \mathbb{F}^{m\times n} \longrightarrow \mathbb{F}^{m\times n}$	$\mathbb{F}$-linear	Ranks, determinants & eigenvalues
[10]	$\phi : \mathbb{F}^{n\times n} \longrightarrow \mathbb{F}^{n\times n}$	$\mathbb{F}$-linear	Invertible matrices

introduced in [34], but its connection with universal security was only given for $\mathbb{F}_{q^m}$-linear codes. Thus, no measure of universal security performance for all $\mathbb{F}_q$-linear codes or code pairs is known. See also Table I.

2) The first optimal universal secure linear codes for noiseless networks were obtained in [39, Sec. V], whose information rate attain the information-theoretical limit given in [6]. However, these codes only exist when $m \geq n$. The cartesian products in [39, Sec. VII-C] are also optimal among $\mathbb{F}_q$-linear codes (see Remark 22), but only exist when m divides n. No optimal universal secure $\mathbb{F}_q$-linear codes for noiseless networks have been obtained for the rest of values of m. See also Table II for an overview of existing optimal constructions, including non-universal codes [6], [14], [15].

3) In [20], the authors introduce the first list-decodable rank-metric codes in $\mathbb{F}_{q^m}^n$ able to list-decode close to the information-theoretical limit and roughly twice as many errors as optimal rank-metric codes [17], [36] are able to correct, in polynomial time and with polynomial-sized lists (on the length n). However, no universal secure coding schemes with such list-decoding capabilities are known. Observe that list-decoding rank errors implies list-decoding errors in linear network coding in a universal manner [38].

4) Several characterizations of maps between vector spaces of matrices preserving certain properties have been given in the literature [3], [10], [27], [28], [30]. The maps considered in [3] are linear over the extension field $\mathbb{F}_{q^m}$ and preserve ranks, and the maps considered in [10], [27], [30] are linear over the base field ($\mathbb{F}_q$ or an arbitrary field) and preserve fundamental properties of matrices, such as ranks, determinants, eigenvalues or invertible matrices. Characterizations of maps preserving universal security performance were first given in [28], although the considered maps were only linear over $\mathbb{F}_{q^m}$. No characterizations of general $\mathbb{F}_q$-linear maps preserving universal security are known. See also Table III.

D. Our Contributions and Main Results

In the following, we list our four main contributions together with our main result summarizing each of them. Each contribution tackles each open problem listed in the previous subsection, respectively.

1) We introduce new parameters, RGMWs and RDRPs, in Definitions 10 and 11, respectively, which measure the universal security performance of $\mathbb{F}_q$-linear code pairs $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$, in terms of the worst-case information leakage. The main result is Theorem 1 and states the following: The r-th RGMW of the code pair is the minimum number of links that an adversary needs to wire-tap in order to obtain at least r bits of information (multiplied by $\log_2(q)$) about the sent message. The μ-th RDRP of the code pair is the maximum number of bits of information (multiplied by $\log_2(q)$) about the sent message that can be obtained by wire-tapping μ links of the network.

Since $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ are also $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m\times n}$, RGMWs and RDRPs must coincide with RGRWs and RDIPs [24], respectively, for $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$, which we prove in Theorem 7.

When $\mathcal{C}_2 = \{0\}$ and $m \neq n$, we will also show in Theorem 9 that the RGMWs of the pair coincide with their DGWs, given in [34], hence proving the connection between DGWs and universal security for general $\mathbb{F}_q$-linear codes, which was left open.

2) We obtain optimal universal secure $\mathbb{F}_q$-linear codes for noiseless networks for any value of m and n, not only when $m \geq n$ or m divides n, as in previous works [39]. The main result is Theorem 2, which states the following: Denote by ℓ the number of packets in $\mathbb{F}_q^m$ that the source can transmit and by t the number of links the adversary may wire-tap without obtaining any information about the sent packets. For any m and n, and a fixed value of ℓ (respectively t), we obtain a coding scheme with optimal value of t (respectively ℓ).

3) We obtain the first universal secure list-decodable rank-metric code pairs with polynomial-sized lists. The main result is Theorem 3, and states the following: Defining ℓ and t as in the previous item, assuming that n divides m, and fixing $1 \leq k_2 < k_2 \leq n$, $\varepsilon > 0$ and a positive integer s such that $4sn \leq \varepsilon m$ and $m/n = \mathcal{O}(s/\varepsilon)$, we obtain an $\mathbb{F}_q$-linear code pair such that $\ell \geq m(k_1 - k_2)(1 - 2\varepsilon)$, $t \geq k_2$ and which can

list-decode $\frac{s}{s+1}(n-k_1)$ rank errors in polynomial time, where the list size is $q^{\mathcal{O}(s^2/\varepsilon^2)}$.

4) We obtain characterizations of vector space isomorphisms between certain spaces of matrices over $\mathbb{F}_q$ that preserve universal security performance over networks. The main result is Theorem 4, which gives several characterizations of $\mathbb{F}_q$-linear vector space isomorphisms $\phi : \mathcal{V} \longrightarrow \mathcal{W}$, where $\mathcal{V}$ and $\mathcal{W}$ are rank support spaces in $\mathbb{F}_q^{m\times n}$ and $\mathbb{F}_q^{m\times n'}$ (see Definition 7), respectively.

As application, we obtain in Subsection VI-B ranges of possible parameters m and n that given linear codes and code pairs can be applied to without changing their universal security performance.

E. Organization of the Paper

First, all of our main results are stated as *Theorems*. After some preliminaries in Section II, we introduce in Section III the new parameters of linear code pairs (RGMWs and RDRPs), give their connection with the rank metric, and prove that they exactly measure the worst-case information leakage universally on networks (Theorem 1). In Section IV, we give optimal universal secure linear codes for noiseless networks for all possible parameters (Theorem 2). In Section V, we show how to add universal security to the list-decodable rank-metric codes in [20] (Theorem 3). In Section VI, we define and give characterizations of security equivalences of linear codes (Theorem 4), and then obtain ranges of possible parameters of linear codes up to these equivalences. In Section VII, we give upper and lower Singleton-type bounds (Theorems 5 and 6) and study when they can be attained, when the dimensions are divisible by m. Finally, in Section VIII, we prove that RGMWs extend RGRWs [24] and RGHWs [26], [42], and we prove that RDRPs extend RDIPs [24] and RDLPs [16], [26] (Theorems 7 and 8, respectively). We conclude the section by showing that GMWs coincide with DGWs [34] for non-square matrices, and are strictly larger otherwise (Theorem 9).

II. Coset Coding Schemes for Universal Security in Linear Network Coding

This section serves as a brief summary of the model of linear network coding that we consider (Subsection II-A), the concept of universal security under this model (Subsection II-B) and the main definitions concerning coset coding schemes used for this purpose (Subsection II-C). The section only contains definitions and facts known in the literature, which will be used throughout the paper.

A. Linear Network Coding Model

Consider a network with several sources and several sinks. A given source transmits a message $\mathbf{x} \in \mathbb{F}_q^\ell$ through the network to multiple sinks. To that end, that source encodes the message as a collection of n packets of length m, seen as a matrix $C \in \mathbb{F}_q^{m\times n}$, where n is the number of outgoing links from this source. We consider linear network coding on the network, first considered in [1] and [25] and formally defined in [23, Definition 1], which allows us to reach higher throughput than just storing and forwarding on the network. This means that a given sink receives a matrix of the form

$$Y = CA^T \in \mathbb{F}_q^{m\times N},$$

where $A \in \mathbb{F}_q^{N\times n}$ is called the transfer matrix corresponding to the considered source and sink, and A^T denotes its transpose. This matrix may be randomly chosen if random linear network coding is applied [21].

B. Universal Secure Communication Over Networks

In secure and reliable network coding, two of the main problems addressed in the literature are the following:

1) Error and erasure correction [5], [24], [38]–[40]: An adversary and/or a noisy channel may introduce errors on some links of the network and/or modify the transfer matrix. In this case, the sink receives the matrix

$$Y = CA'^T + E \in \mathbb{F}_q^{m\times N},$$

where $A' \in \mathbb{F}_q^{N\times n}$ is the modified transfer matrix, and $E \in \mathbb{F}_q^{m\times N}$ is the final error matrix. In this case, we say that $t = \mathrm{Rk}(E)$ errors and $\rho = n - \mathrm{Rk}(A')$ erasures occurred, where Rk denotes the rank of a matrix.

2) Information leakage [6], [14], [15], [24], [39]: A wire-tapping adversary listens to $\mu > 0$ links of the network, obtaining a matrix of the form $CB^T \in \mathbb{F}_q^{m\times\mu}$, for some matrix $B \in \mathbb{F}_q^{\mu\times n}$.

Outer coding in the source node is usually applied to tackle the previous problems, and it is called *universal secure* [39] if it provides reliability and security as in the previous items for fixed numbers of wire-tapped links μ, errors t and erasures ρ, independently of the transfer matrix A used. This implies that no previous knowledge or modification of the transfer matrix is required and random linear network coding [21] may be applied.

C. Coset Coding Schemes for Outer Codes

Coding techniques for protecting messages simultaneously from errors and information leakage to a wire-tapping adversary were first studied by Wyner in [43]. In [43, p. 1374], the general concept of coset coding scheme, as we will next define, was first introduced for this purpose. We use the formal definition in [24, Definition 7]:

Definition 1 (Coset Coding Schemes [24], [43]): A coset coding scheme over the field $\mathbb{F}$ with message set $\mathcal{S}$ is a family of disjoint nonempty subsets of $\mathbb{F}^{m\times n}$, $\mathcal{P}_\mathcal{S} = \{\mathcal{C}_\mathbf{x}\}_{\mathbf{x}\in\mathcal{S}}$.

If $\mathbb{F} = \mathbb{F}_q$, each $\mathbf{x} \in \mathcal{S}$ is encoded by the source by choosing uniformly at random an element $C \in \mathcal{C}_\mathbf{x}$.

Definition 2 (Linear Coset Coding Schemes [28, Definition 2]): A coset coding scheme as in the previous definition is said to be linear if $\mathcal{S} = \mathbb{F}^\ell$, for some $0 < \ell \leq mn$, and

$$a\mathcal{C}_\mathbf{x} + b\mathcal{C}_\mathbf{y} \subseteq \mathcal{C}_{a\mathbf{x}+b\mathbf{y}},$$

for all $a, b \in \mathbb{F}$ and all $\mathbf{x}, \mathbf{y} \in \mathbb{F}^\ell$.

With these definitions, the concept of coset coding scheme generalizes the concept of (block) code, since a code is a

coset coding scheme where $|\mathcal{C}_{\mathbf{x}}| = 1$, for each $\mathbf{x} \in \mathcal{S}$. In the same way, linear coset coding schemes generalize linear (block) codes.

An equivalent way to describe linear coset coding schemes is by nested linear code pairs, introduced in [44, Sec. III.A]. We use the description in [7, Sec. 4.2].

Definition 3 (Nested Linear Code Pairs [7], [44]): A nested linear code pair is a pair of linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m\times n}$. Choose a vector space $\mathcal{W}$ such that $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{W}$, where $\oplus$ denotes the direct sum of vector spaces, and a vector space isomorphism $\psi : \mathbb{F}^{\ell} \longrightarrow \mathcal{W}$, where $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$. Then we define $\mathcal{C}_{\mathbf{x}} = \psi(\mathbf{x}) + \mathcal{C}_2$, for $\mathbf{x} \in \mathbb{F}^{\ell}$. They form a linear coset coding scheme called nested coset coding scheme [24].

Remark 4: As observed in [33] for the wire-tap channel of type II, linear code pairs where $\mathcal{C}_1 = \mathbb{F}^{m\times n}$ are suitable for protecting information from leakage on noiseless channels. Analogously, linear code pairs where $\mathcal{C}_2 = \{0\}$ are suitable for error correction without the presence of eavesdroppers. Observe that these two types of linear code pairs are dual to each other (see Definition 15 and Appendix A): If $\mathcal{C}_1' = \mathcal{C}_2^{\perp}$ and $\mathcal{C}_2' = \mathcal{C}_1^{\perp}$, then $\mathcal{C}_1 = \mathbb{F}^{m\times n}$ if, and only if, $\mathcal{C}_2' = \{0\}$. To treat both error correction and information leakage, we need general linear coset coding schemes.

We recall here that the concept of linear coset coding schemes and nested coset coding schemes are exactly the same. An object in the first family uniquely defines an object in the second family and vice-versa. This is formally proven in [28, Proposition 1].

Finally, we recall that the exact universal error and erasure correction capability of a nested coset coding scheme was found, in terms of the rank metric, first in [38, Sec. IV.C] for the case of one code ($\mathcal{C}_2 = \{0\}$) that is maximum rank distance, then in [39, Th. 2] for the general case of one linear code (again $\mathcal{C}_2 = \{0\}$), then in [24, Th. 4] for the case where both codes are linear over an extension field $\mathbb{F}_{q^m}$, and finally in [28, Th. 9] for arbitrary coset coding schemes (linear over $\mathbb{F}_q$ and non-linear).

III. New Parameters of Linear Coset Coding Schemes for Universal Security on Networks

This is the main section of the paper, which serves as a basis for the rest of sections. The next sections can be read independently of each other, but all of them build on the results in this section. Here we introduce rank support spaces (Subsection III-A), which are the main technical building blocks of our theory, then we define of our main parameters and connect them with the rank metric (Subsection III-B), and we conclude by showing (Theorem 1) that these parameters measure the worst-case information leakage universally on linearly coded networks (Subsection III-C).

A. Rank Supports and Rank Support Spaces

In this subsection, we introduce rank support spaces, which are the mathematical building blocks of our theory. The idea is to attach to each linear code its rank support, given in [22, Definition 1], and based on this rank support, define a vector space of matrices containing the original code that can be seen as its ambient space with respect to the rank metric.

We remark here that the family of rank support spaces can be seen as the family of vector spaces in [35, Notation 25] after transposition of matrices, or the family of vector spaces in [22, Definition 6] taking $\mathcal{C} = \mathbb{F}_q^{m\times n}$. We start with the definitions:

Definition 5 (Row Space and Rank): For a matrix $C \in \mathbb{F}^{m\times n}$, we define its row space $\mathrm{Row}(C)$ as the vector space in $\mathbb{F}^n$ generated by its rows. As usual, we define its rank as $\mathrm{Rk}(C) = \dim(\mathrm{Row}(C))$.

Definition 6 (Rank Support and Rank Weight [22, Definition 1]): Given a vector space $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$, we define its rank support as

$$\mathrm{RSupp}(\mathcal{C}) = \sum_{C\in\mathcal{C}} \mathrm{Row}(C) \subseteq \mathbb{F}^n.$$

We also define the rank weight of the space $\mathcal{C}$ as

$$\mathrm{wt_R}(\mathcal{C}) = \dim(\mathrm{RSupp}(\mathcal{C})).$$

Observe that $\mathrm{RSupp}(\langle\{C\}\rangle) = \mathrm{Row}(C)$ and $\mathrm{wt_R}(\langle\{C\}\rangle) = \mathrm{Rk}(C)$, for every matrix $C \in \mathbb{F}^{m\times n}$, where $\langle\mathcal{A}\rangle$ denotes the vector space generated by a set $\mathcal{A}$ over $\mathbb{F}$.

Definition 7 (Rank Support Spaces): Given a vector space $\mathcal{L} \subseteq \mathbb{F}^n$, we define its rank support space $\mathcal{V}_{\mathcal{L}} \subseteq \mathbb{F}^{m\times n}$ as

$$\mathcal{V}_{\mathcal{L}} = \{V \in \mathbb{F}^{m\times n} \mid \mathrm{Row}(V) \subseteq \mathcal{L}\}.$$

We denote by $RS(\mathbb{F}^{m\times n})$ the family of rank support spaces in $\mathbb{F}^{m\times n}$.

The following lemma shows that rank support spaces behave as a sort of ambient spaces for linear codes and can be attached bijectively to vector spaces in $\mathbb{F}^n$, which correspond to the rank supports of the original linear codes.

Lemma 8: Let $\mathcal{L} \subseteq \mathbb{F}^n$ be a vector space. The following hold:

1) *$\mathcal{V}_{\mathcal{L}}$ is a vector space and the correspondence $\mathcal{L} \mapsto \mathcal{V}_{\mathcal{L}}$ between subspaces of $\mathbb{F}^n$ and rank support spaces is a bijection with inverse $\mathcal{V}_{\mathcal{L}} \mapsto \mathrm{RSupp}(\mathcal{V}_{\mathcal{L}}) = \mathcal{L}$.*
2) *If $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ is a vector space and $\mathcal{L} = \mathrm{RSupp}(\mathcal{C})$, then $\mathcal{V}_{\mathcal{L}}$ is the smallest rank support space containing $\mathcal{C}$.*

We conclude the subsection with the following characterizations of rank support spaces, which we will use throughout the paper. In particular, item 2 will be useful to prove Theorem 4, and item 3 will be useful to prove Theorem 1.

Proposition 9: Fix a set $\mathcal{V} \subseteq \mathbb{F}^{m\times n}$. The following are equivalent:

1) *$\mathcal{V}$ is a rank support space. That is, there exists a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\mathcal{V} = \mathcal{V}_{\mathcal{L}}$.*
2) *$\mathcal{V}$ is linear and has a basis of the form $B_{i,j}$, for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, k$, where there are vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{F}^n$ such that $B_{i,j}$ has the vector $\mathbf{b}_j$ in the i-th row and the rest of its rows are zero vectors.*
3) *There exists a matrix $B \in \mathbb{F}^{\mu\times n}$, for some positive integer μ, such that*

$$\mathcal{V} = \{V \in \mathbb{F}^{m\times n} \mid VB^T = 0\}.$$

In addition, the relation between items 1, 2 and 3 is that $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ *are a basis of* $\mathcal{L}$*,* B *is a (possibly not full-rank) parity check matrix of* $\mathcal{L}$ *and* $\dim(\mathcal{L}) = n - \mathrm{Rk}(B)$.

In particular, it holds that

$$\dim(\mathcal{V}_{\mathcal{L}}) = m \dim(\mathcal{L}). \tag{2}$$

Proof: We prove the following implications:

- $1 \iff 2$: Assume item 1, let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ be a basis of $\mathcal{L}$, and let $B_{i,j}$ be as in item 2. Then we see that $\mathcal{V} = \langle \{B_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq k\} \rangle$. The reversed implication follows in the same way by defining $\mathcal{L} = \langle \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \rangle \subseteq \mathbb{F}^n$.
- $1 \iff 3$: Assume item 1 and let $B \in \mathbb{F}^{\mu \times n}$ be a parity check matrix of $\mathcal{L}$. That is, a generator matrix of the dual $\mathcal{L}^{\perp} \subseteq \mathbb{F}^n$. Then it holds by definition that $V \in \mathbb{F}^{m \times n}$ has all its rows in $\mathcal{L}$ if, and only if, $VB^T = 0$. Conversely, assuming item 3 and defining $\mathcal{L}$ as the code with parity check matrix B, we see that $\mathcal{V} = \mathcal{V}_{\mathcal{L}}$ by the same argument. Hence the result follows. □

B. Definition and Basic Properties of the New Parameters

Definition 10 (Relative Generalized Matrix Weight): Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, we define their r-th relative generalized matrix weight (RGMW) as

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\dim(\mathcal{L}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}}) \geq r\}.$$

For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, and $1 \leq r \leq \dim(\mathcal{C})$, we define its r-th generalized matrix weight (GMW) as

$$d_{M,r}(\mathcal{C}) = d_{M,r}(\mathcal{C}, \{0\}). \tag{3}$$

Observe that it holds that

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \geq d_{M,r}(\mathcal{C}_1), \tag{4}$$

for all nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and all $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$.

Definition 11 (Relative Dimension/Rank Support Profile): Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and $0 \leq \mu \leq n$, we define their μ-th relative dimension/rank support profile (RDRP) as

$$K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{\dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) \leq \mu\}.$$

Now, if $\mathcal{U} \subseteq \mathcal{V} \subseteq \mathbb{F}^{m \times n}$ are vector spaces, the natural linear map $\mathcal{C}_1 \cap \mathcal{U}/\mathcal{C}_2 \cap \mathcal{U} \longrightarrow \mathcal{C}_1 \cap \mathcal{V}/\mathcal{C}_2 \cap \mathcal{V}$ is one to one. Therefore, since we are taking maximums, it holds that

$$K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{\dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) = \mu\}.$$

We remark here that some existing notions of relative generalized weights from the literature are particular cases of RGMWs. The corresponding connections are given in Section VIII. In particular, GMWs of one linear code coincide with DGWs (introduced in [34]) for non-square matrices.

We next obtain the following characterization of RGMWs that gives an analogous description to the original definition of GHWs by Wei [42]:

Proposition 12 Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$*, and an integer* $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$*, it holds that*

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\mathrm{wt_R}(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C}_1, \mathcal{D} \cap \mathcal{C}_2 = \{0\}, \dim(\mathcal{D}) = r\}.$$

Proof: Denote by d_r the number on the left-hand side and by d'_r the number on the right-hand side. We prove both inequalities:

$d_r \leq d'_r$: Take a vector space $\mathcal{D} \subseteq \mathcal{C}_1$ such that $\mathcal{D} \cap \mathcal{C}_2 = \{0\}$, $\dim(\mathcal{D}) = r$ and $\mathrm{wt_R}(\mathcal{D}) = d'_r$. Define $\mathcal{L} = \mathrm{RSupp}(\mathcal{D})$.

Since $\mathcal{D} \subseteq \mathcal{V}_{\mathcal{L}}$, we have that $\dim((\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}})/(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}})) \geq \dim((\mathcal{C}_1 \cap \mathcal{D})/(\mathcal{C}_2 \cap \mathcal{D})) = \dim(\mathcal{D}) = r$. Hence

$$d_r \leq \dim(\mathcal{L}) = \mathrm{wt_R}(\mathcal{D}) = d'_r.$$

$d_r \geq d'_r$: Take a vector space $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\dim((\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}})/(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}})) \geq r$ and $\dim(\mathcal{L}) = d_r$.

There exists a vector space $\mathcal{D} \subseteq \mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}$ with $\mathcal{D} \cap \mathcal{C}_2 = \{0\}$ and $\dim(\mathcal{D}) = r$. We have that $\mathrm{RSupp}(\mathcal{D}) \subseteq \mathcal{L}$, since $\mathcal{D} \subseteq \mathcal{V}_{\mathcal{L}}$, and hence

$$d_r = \dim(\mathcal{L}) \geq \mathrm{wt_R}(\mathcal{D}) \geq d'_r.$$

□

Thanks to this characterization, we may connect RGMWs with the rank distance [9]. This will be crucial in the next section, where we will use maximum rank distance codes from [9] to obtain optimal universal secure linear codes for noiseless networks. Recall the definition of minimum rank distance of a linear coset coding scheme, which is a particular case of [28, eq. (1)], and which is based on the analogous concept for the Hamming metric given in [13]:

$$d_R(\mathcal{C}_1, \mathcal{C}_2) = \min\{\mathrm{Rk}(C) \mid C \in \mathcal{C}_1, C \notin \mathcal{C}_2\}. \tag{5}$$

The following result follows from the previous theorem and the definitions:

Corollary 13 (Minimum Rank Distance of Linear Coset Coding Schemes): Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$*, it holds that*

$$d_R(\mathcal{C}_1, \mathcal{C}_2) = d_{M,1}(\mathcal{C}_1, \mathcal{C}_2).$$

By Theorem 9, the previous corollary coincides with item 1 in [34, Th. 30] when $\mathcal{C}_2 = \{0\}$ and $m \neq n$.

We conclude by showing the connection between RDRPs and RGMWs:

Proposition 14 (Connection Between RDRPs and RGMWs): Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$ *and* $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$*, it holds that*

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\mu \mid K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) \geq r\}.$$

Proof: It is proven as [24, Proof of Lemma 4]. □

C. Measuring Information Leakage on Networks

In this subsection, we show how the introduced parameters (RGMWs and RDRPs) measure the universal security performance of nested linear code pairs.

Assume that a given source wants to convey the message $\mathbf{x} \in \mathbb{F}_q^\ell$, which we assume is a random variable with uniform distribution over $\mathbb{F}_q^\ell$. Following Subsection II-C, the source encodes $\mathbf{x}$ into a matrix $C \in \mathbb{F}_q^{m\times n}$ using nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$. We also assume that the distributions used in the encoding are all uniform (see Subsection II-C).

According to the information leakage model in Subsection II-B, item 2, a wire-tapping adversary obtains $CB^T \in \mathbb{F}_q^{m\times \mu}$, for some matrix $B \in \mathbb{F}_q^{\mu\times n}$.

Recall from [8] the definition of mutual information of two random variables X and Y:

$$I(X;Y) = H(Y) - H(Y \mid X), \tag{6}$$

where $H(Y)$ denotes the entropy of Y and $H(Y \mid X)$ denotes the conditional entropy of Y given X, and where we take logarithms with base q (see [8] for more details).

We will need to use the concept of duality with respect to the Hilbert-Schmidt or trace product. In Appendix A, we collect some basic properties of duality of linear codes. We now give the main definitions:

Definition 15 (Hilbert-Schmidt or Trace Product): Given matrices $C, D \in \mathbb{F}^{m\times n}$, we define its Hilbert-Schmidt product, or trace product, as

$$\langle C, D\rangle = \mathrm{Trace}(CD^T) = \sum_{i=1}^{m} \mathbf{c}_i \cdot \mathbf{d}_i = \sum_{i=1}^{m}\sum_{j=1}^{n} c_{i,j} d_{i,j} \in \mathbb{F},$$

where $\mathbf{c}_i$ and $\mathbf{d}_i$ are the rows of C and D, respectively, and where $c_{i,j}$ and $d_{i,j}$ are their components, respectively.

Given a vector space $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$, we denote by $\mathcal{C}^\perp$ its dual:

$$\mathcal{C}^\perp = \{D \in \mathbb{F}^{m\times n} \mid \langle C, D\rangle = 0, \forall C \in \mathcal{C}\}.$$

We first compute the mutual information of the message and the wire-tapper's observation via rank support spaces:

Proposition 16: Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$, a matrix $B \in \mathbb{F}_q^{\mu\times n}$, and the uniform random variables $\mathbf{x}$ and CB^T, as in the beginning of this subsection, it holds that

$$I(\mathbf{x}; CB^T) = \dim(\mathcal{C}_2^\perp \cap \mathcal{V}_\mathcal{L}) - \dim(\mathcal{C}_1^\perp \cap \mathcal{V}_\mathcal{L}), \tag{7}$$

where $I(\mathbf{x}; CB^T)$ is as in (6), and where $\mathcal{L} = \mathrm{Row}(B)$.

Proof: Define the map $f : \mathbb{F}_q^{m\times n} \longrightarrow \mathbb{F}_q^{m\times\mu}$ given by

$$f(D) = DB^T,$$

for the matrix $B \in \mathbb{F}_q^{\mu\times n}$. Observe that f is a linear map. It follows that

$$\begin{aligned} H(CB^T) &= H(f(C)) = \log_q(|f(\mathcal{C}_1)|) = \dim(f(\mathcal{C}_1)) \\ &= \dim(\mathcal{C}_1) - \dim(\ker(f) \cap \mathcal{C}_1), \end{aligned}$$

where the last equality is the well-known first isomorphism theorem. On the other hand, we may similarly compute the conditional entropy:

$$\begin{aligned} H(CB^T \mid \mathbf{x}) &= H(f(C) \mid \mathbf{x}) = \log_q(|f(\mathcal{C}_2)|) = \dim(f(\mathcal{C}_2)) \\ &= \dim(\mathcal{C}_2) - \dim(\ker(f) \cap \mathcal{C}_2). \end{aligned}$$

However, it holds that $\ker(f) = \mathcal{V}_{\mathcal{L}^\perp} \subseteq \mathbb{F}_q^{m\times n}$ by Proposition 9, since B is a parity check matrix of $\mathcal{L}^\perp$. Therefore

$$\begin{aligned} &I(\mathbf{x}; CB^T) \\ &\quad = H(CB^T) - H(CB^T \mid \mathbf{x}) = (\dim(\mathcal{C}_1) \\ &\qquad - \dim(\mathcal{V}_{\mathcal{L}^\perp} \cap \mathcal{C}_1)) - (\dim(\mathcal{C}_2) - \dim(\mathcal{V}_{\mathcal{L}^\perp} \cap \mathcal{C}_2)). \end{aligned}$$

Finally, the result follows by Lemmas 63 and 64 in Appendix A. □

The following theorem follows from the previous proposition, Corollary 13 and the definitions:

Theorem 1 (Worst-Case Information Leakage): Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$, and integers $0 \le \mu \le n$ and $1 \le r \le \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that

1) *$\mu = d_{M,r}(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$ is the minimum number of links that an adversary needs to wire-tap in order to obtain at least r units of information (number of bits multiplied by $\log_2(q)$) of the sent message.*
2) *$r = K_{M,\mu}(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$ is the maximum information (number of bits multiplied by $\log_2(q)$) about the sent message that can be obtained by wire-tapping at most μ links of the network.*

In particular, $t = d_R(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp) - 1$ is the maximum number of links that an adversary may listen to without obtaining any information about the sent message.

Remark 17: Proposition 16 extends [24, Lemma 7, item 2] from $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ to $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m\times n}$ due to Lemma 52 in Subsection VIII-A. Furthermore, as we will explain in Theorem 7, our Theorem 1 extends in the same sense [24, Th. 2] and [24, Corollary 5].

Remark 18: In Section VIII, we will prove that GMWs coincide with DGWs [34] when using one code ($\mathcal{C}_1^\perp = \{0\}$ in Theorem 1) and non-square matrices. Hence the results in this subsection prove that DGWs measure the worst-case information leakage in these cases, which has not been proven in the literature yet.

IV. Optimal Universal Secure Linear Codes for Noiseless Networks and Any Packet Length

In this section, we obtain linear coset coding schemes built from nested linear code pairs $\mathcal{C} \subsetneqq \mathbb{F}^{m\times n}$, which in this section will refer to those with $\mathcal{C}_2 = \mathcal{C}$ and $\mathcal{C}_1 = \mathbb{F}^{m\times n}$, with optimal universal security performance in the case of finite fields $\mathbb{F} = \mathbb{F}_q$ (Theorem 2). Recall from Subsection II-C that these linear coset coding schemes are suitable for noiseless networks, as noticed in [33] (see also Remark 4).

In this section, we consider perfect universal secrecy (the adversary obtains no information after wire-tapping a given number of links), thus we make use of the theory in last section concerning the first RGMW. In Section VII, we will consider bounds on the rest of RGMWs, for general code pairs (suitable for noisy networks), and their achievability.

Definition 19: For a nested linear code pair of the form $\mathcal{C} \subsetneqq \mathbb{F}_q^{m\times n}$, we define its information parameter as $\ell = \dim(\mathbb{F}_q^{m\times n}/\mathcal{C}) = \dim(\mathcal{C}^\perp)$, that is the maximum number of $\log_2(q)$ bits of information that the source can convey, and its security parameter t as the maximum number of links that an adversary may listen to without obtaining any information about the sent message.

Due to Theorem 1, it holds that $t = d_R(\mathcal{C}^\perp) - 1$. We study two problems:

1) Find a nested linear code pair $\mathcal{C} \subsetneqq \mathbb{F}_q^{m\times n}$ with maximum possible security parameter t when m, n, q and the information parameter ℓ are fixed and given.
2) Find a nested linear code pair $\mathcal{C} \subsetneqq \mathbb{F}_q^{m\times n}$ with maximum possible information parameter ℓ when m, n, q and the security parameter t are fixed and given.

We will deduce bounds on these parameters from the Singleton bound on the dimension of rank-metric codes [9, Th. 5.4]:

Lemma 20 [9, Th. 5.4]: For a linear code $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$, it holds that

$$\dim(\mathcal{C}) \leq \max\{m,n\}(\min\{m,n\} - d_R(\mathcal{C}) + 1). \tag{8}$$

As usual in the literature, we say that $\mathcal{C}$ is maximum rank distance (MRD) if equality holds in (8).

Thanks to Theorem 1 and the previous lemma, we may give upper bounds on the attainable parameters in the previous two problems:

Proposition 21: Given a nested linear code pair $\mathcal{C} \subsetneqq \mathbb{F}_q^{m\times n}$ with information parameter ℓ and security parameter t, it holds that:

$$\ell \leq \max\{m,n\}(\min\{m,n\} - t), \tag{9}$$

$$t \leq \min\{m,n\} - \left\lceil \frac{\ell}{\max\{m,n\}} \right\rceil. \tag{10}$$

In particular, $\ell \leq mn$ and $t \leq \min\{m,n\}$.

Proof: Recall that $\ell = \dim(\mathbb{F}_q^{m\times n}/\mathcal{C}) = \dim(\mathcal{C}^\perp)$ and, due to Theorem 1, $t = d_R(\mathcal{C}^\perp) - 1$. Hence the result follows from the bound (8) for $\mathcal{C}^\perp$. □

On the other hand, the existence of linear codes in $\mathbb{F}_q^{m\times n}$ attaining the Singleton bound on their dimensions, for all possible choices of m, n and minimum rank distance d_R [9, Th. 6.3], leads to the following existence result on optimal linear coset coding schemes for noiseless networks.

Theorem 2: For all choices of positive integers m and n, and all finite fields $\mathbb{F}_q$, the following hold:

1) *For every positive integer $\ell \leq mn$, there exists a nested linear code pair $\mathcal{C} \subsetneqq \mathbb{F}_q^{m\times n}$ with information parameter ℓ and security parameter $t = \min\{m,n\} - \lceil(\ell/\max\{m,n\})\rceil$.*
2) *For every positive integer $t \leq \min\{m,n\}$, there exists a nested linear code pair $\mathcal{C} \subsetneqq \mathbb{F}_q^{m\times n}$ with security parameter t and information parameter $\ell = \max\{m,n\}(\min\{m,n\} - t)$.*

Remark 22: We remark here that, to the best of our knowledge, only the linear coset coding schemes in item 2 in the previous theorem, for the special case $n \leq m$, have been obtained in the literature. It corresponds to [39, Th. 7]. Using cartesian products of MRD codes as in [39, Sec. VII-C], linear coset coding schemes as in item 2 in the previous theorem can be obtained when $n > m$, for the restricted parameters $n = lm$ and $\ell = mlk'$, where l and $k' < m$ are positive integers.

V. Universal Secure List-Decodable Rank-Metric Linear Coset Coding Schemes

In this section, we will obtain nested linear code pairs $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$ when n divides m that can list-decode rank errors on noisy networks (as opposed to the scenario in last section), whose list sizes are polynomial on the code length n, while being univeral secure under a given number of wire-tapped links. As in last section, we consider perfect universal secrecy, and thus make use of the results in Section III concerning the first RGMW of the dual code pair.

We give the construction in Subsection V-A, together with its parameters (Theorem 3): information parameter ℓ, security parameter t and number of list-decodable rank errors e. To measure the quality of the proposed code pair, we will compare in Subsection V-B their parameters with those obtained when choosing $\mathcal{C}_1$ and $\mathcal{C}_2$ as MRD codes [17], [36], which provide coset coding schemes with both optimal universal security and optimal error-correction capability [39]. We will also show (Subsection V-C) the near optimality of the obtained construction in terms of the introduced uncertainty on the secret message and the number of list-decodable rank errors.

A. The Construction and Its Main Properties

We start by extending the definition of rank list-decodable codes from [11, Definition 2] to coset coding schemes:

Definition 23: For positive integers e and L, we say that a coset coding scheme $\mathcal{P}_\mathcal{S} = \{\mathcal{C}_\mathbf{x}\}_{\mathbf{x}\in\mathcal{S}}$ over $\mathbb{F}_q$ is rank (e, L)-list-decodable if, for every $Y \in \mathbb{F}_q^{m\times n}$, we have that

$$|\{\mathbf{x} \in \mathcal{S} \mid \mathcal{P}_\mathbf{x} \cap \mathcal{B}(Y, e) \neq \emptyset\}| \leq L,$$

where $\mathcal{B}(Y, e)$ denotes the ball in $\mathbb{F}_q^{m\times n}$ with center Y and rank radius e. The number of list-decodable rank errors is e and the list sizes are said to be polynomial in n if $L = \mathcal{O}(F(n))$, for some polynomial $F(x)$.

Remark 24: Observe however that, if a coset coding scheme can list-decode e rank errors with polynomial-sized lists of cosets, we still need to decode these cosets to obtain the uncoded secret messages. In general, it is possible that the union of such cosets has exponential size while the scheme can still obtain all the corresponding uncoded messages via an algorithm with polynomial complexity. This is the case in the construction below.

We now give the above mentioned construction, which exists whenever n divides m. The main objective is to obtain simultaneously large information parameter ℓ, security parameter t and number of list-decodable rank errors e.

Construction 1: Assume that n divides m and fix $\varepsilon > 0$ and positive integers s and $1 \leq k_2 < k_1 \leq n$ such that $4sn \leq \varepsilon m$ and $m/n = \mathcal{O}(s/\varepsilon)$. In the next subsection, mk_1 and mk_2 will be the dimensions of the MRD linear codes constituting an

optimal universal secure nested coset coding scheme, but here they are just fixed parameters.

Fix a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$, such that $\alpha_1, \alpha_2, \ldots, \alpha_n$ generate $\mathbb{F}_{q^n}$ (recall that $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ since n divides m).

Recall that a q-linearized polynomial over $\mathbb{F}_{q^m}$ is a polynomial of the form $F(x) = \sum_{i=0}^{d} F_i x^{q^i}$, where $F_i \in \mathbb{F}_{q^m}$, for some positive integer d. Denote also $\mathrm{ev}_{\boldsymbol{\alpha}}(F(x)) = (F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_n)) \in \mathbb{F}_{q^m}^n$, and finally define the linear codes

$$\mathcal{C}_2 = \{M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))) \mid F_i = 0 \text{ for } i < k_1 - k_2 \text{ and } i \geq k_1\},$$
$$\mathcal{C}_1 = \{M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))) \mid F_i \in \mathcal{H}_i \text{ for } 0 \leq i < k_1 - k_2, \quad F_i \in \mathbb{F}_{q^m} \text{ for } k_1 - k_2 \leq i < k_1,\ F_i = 0 \text{ for } i \geq k_1\},$$

where $M_{\boldsymbol{\alpha}}$ is the map given in (1) and $\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{k_1-k_2-1} \subseteq \mathbb{F}_{q^m}$ are the $\mathbb{F}_q$-linear vector spaces described in [20, Th. 8]. We recall this description in Appendix B. Observe that these vector spaces depend on ε and s.

Let $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2) = \dim(\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1})$. We now show how $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$ form a coset coding scheme as in Definition 3. Define the vector space

$$\mathcal{W} = \{M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))) \mid F_i \in \mathcal{H}_i \text{ for } i < k_1 - k_2 \text{ and } F_i = 0 \text{ for } i \geq k_1 - k_2\},$$

which satisfies that $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{W}$. Now consider the secret space as $\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1} \cong \mathbb{F}_q^{\ell}$, and define the vector space isomorphism $\psi : \mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1} \longrightarrow \mathcal{W}$ as follows: For $\mathbf{x} \in \mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1}$, take $F(x) = \sum_{i=0}^{k_1-k_2-1} F_i x^{q^i}$ such that $\mathbf{x} = (F_0, F_1, \ldots, F_{k_1-k_2-1})$, and define

$$C = \psi(\mathbf{x}) = M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))).$$

We may now state the main result of this section:

Theorem 3: With the same assumptions and notation, the nested coset coding scheme in Construction 1 satisfies that:

1) $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2) \geq m(k_1 - k_2)(1 - 2\varepsilon)$.
2) *Its security parameter (Definition 19) satisfies* $t \geq k_2$.
3) *It is rank* (e, L)*-list-decodable for all* $e \leq \frac{s}{s+1}(n - k_1)$, *with* $L \leq q^{\mathcal{O}(s^2/\varepsilon^2)}$, *and it admits a list-decoding algorithm that obtains all corresponding uncoded messages with polynomial complexity in* n.

We devote the rest of the subsection to prove this theorem. We need to recall some definitions and results from [20]:

Definition 25 (Subspace Designs [20, Definition 3]): Assuming that n divides m and given positive integers r and N, a collection of $\mathbb{F}_q$-linear subspaces $\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_M \subseteq \mathbb{F}_{q^m}$ is called an (r, N, n) $\mathbb{F}_q$-linear subspace design if

$$\sum_{i=1}^{M} \dim(\mathcal{U}_i \cap \mathcal{V}) \leq N,$$

with dimensions taken over $\mathbb{F}_q$, for every $\mathbb{F}_{q^n}$-linear subspace $\mathcal{V} \subseteq \mathbb{F}_{q^m}$ of dimension at most r over $\mathbb{F}_{q^n}$.

The following lemma is part of [20, Th. 8]:

Lemma 26 [20]: With assumptions and notation as in Construction 1, the spaces $\mathcal{H}_0, \mathcal{H}_1, \ldots \mathcal{H}_{k_1-k_2-1}$ *defined in Appendix B form an* $(s, 2(m/n-1)s/\varepsilon, n)$ $\mathbb{F}_q$*-linear subspace design.*

Definition 27 (Periodic Subspaces [20, Definition 9]): Given positive integers r, l, k, we say that an affine subspace $\mathcal{H} \subseteq \mathbb{F}_{q^n}^{lk}$ is (r, l, k)-periodic if there exists an $\mathbb{F}_{q^n}$-linear subspace $\mathcal{V} \subseteq \mathbb{F}_{q^n}^{l}$ of dimension at most r over $\mathbb{F}_{q^n}$ such that, for every $j = 2, 3, \ldots, k$ and $\mathbf{a} \in \mathbb{F}_{q^n}^{(j-1)l}$, the affine space

$$\{\pi_{[(j-1)l+1, jl]}(\mathbf{x}) \mid \mathbf{x} \in \mathcal{H}, \pi_{[1,(j-1)l]}(\mathbf{x}) = \mathbf{a}\} \subseteq \mathbb{F}_{q^n}^{l}$$

is contained in $\mathbf{v_a} + \mathcal{V}$, for a vector $\mathbf{v_a} \in \mathbb{F}_{q^n}^{l}$ that depends on $\mathbf{a}$. Here, π_J denotes the projection over the coordinates in J, and $[a, b]$ denotes the set of integers i such that $a \leq i \leq b$.

We may now prove our main result:

Proof of Theorem 3: We prove each item separately:

1) By Lemma 69 in Appendix B, it holds that $\dim(\mathcal{H}_i) \geq m(1 - 2\varepsilon)$, for $i = 0, 1, 2, \ldots, k_1 - k_2 - 1$. Therefore

$$\ell = \dim(\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1}) \geq m(k_1 - k_2)(1 - 2\varepsilon).$$

2) By Theorem 1, the security parameter is $t = d_R(\mathcal{C}_2^{\perp}, \mathcal{C}_1^{\perp}) - 1 \geq d_R(\mathcal{C}_2^{\perp}) - 1$. Since $\mathcal{C}_2$ is MRD, then so is its trace dual [9], which means that $d_R(\mathcal{C}_2^{\perp}) = k_2 + 1$, and the result follows.

3) As shown in [20, Sec IV-B], we may perform list-decoding for the Gabidulin code $\mathcal{G}_1 \supseteq \mathcal{C}_1$,

$$\mathcal{G}_1 = \{M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))) \mid F_i = 0 \text{ for } i \geq k_1\},$$

and obtain in polynomial time a list containing all possible sent messages that is an $(s-1, m/n, k_1)$-periodic subspace of $\mathbb{F}_{q^n}^{k_1 m/n} \cong \mathbb{F}_{q^m}^{k_1}$ (isomorphic as $\mathbb{F}_{q^n}$-linear vector spaces).

Project this periodic subspace onto the first $k_1 - k_2$ coordinates, which gives a $(s-1, m/n, k_1 - k_2)$-periodic subspace of $\mathbb{F}_{q^m}^{k_1-k_2}$, and intersect it with $\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1}$. Since $\mathcal{H}_0, \mathcal{H}_1, \ldots \mathcal{H}_{k_1-k_2-1}$ form an $(s, 2(m/n-1)s/\varepsilon, n)$ $\mathbb{F}_q$-linear subspace design by Lemma 26, such intersection is an $\mathbb{F}_q$-linear affine space of dimension at most $\mathcal{O}(s^2/\varepsilon^2)$ (recall that $m/n = \mathcal{O}(s/\varepsilon)$) by the definition of subspace designs and periodic subspaces.

B. Comparison With Optimal Unique-Decodable Linear Coset Coding Schemes Based on MRD Codes

In this subsection, we compare the schemes in Construction 1 with those obtained when using MRD codes [17], [36], whose information parameter ℓ is optimal for given security parameter t and number of unique-decodable rank errors e, due to [39, Ths. 11 and 12].

Proposition 28 [39]: Assume that $n \leq m$ *and* $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$ *are MRD linear codes of dimensions* $\dim(\mathcal{C}_1) = mk_1$ *and* $\dim(\mathcal{C}_2) = mk_2$ *(recall that, by the Singleton bound (8), dimensions of MRD codes are multiple of* m *when* $n \leq m$*).*

The linear coset coding scheme (Definition 3) constructed from this nested linear code pair satisfies that:

1) *Its information parameter is* $\ell = m(k_1 - k_2)$.
2) *Its security parameter is* $t = k_2$.
3) *If the number of rank errors is* $e \leq \lfloor \frac{n-k_1}{2} \rfloor$, *then rank error-correction can be performed, giving a unique solution.*

Therefore, assuming that n divides m and given MRD linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$ of dimensions $\dim(\mathcal{C}_1) = mk_1$ and $\dim(\mathcal{C}_2) = mk_2$, the linear coset coding scheme in Construction 1 has at least the same security parameter t as that obtained using $\mathcal{C}_1$ and $\mathcal{C}_2$, an information parameter ℓ that is at least $1-2\varepsilon$ times the one obtained using $\mathcal{C}_1$ and $\mathcal{C}_2$, and can list-decode in polynomial time (with list of polynomial size) roughly $n-k_1$ errors, which is twice as many as the rank errors that $\mathcal{C}_1$ and $\mathcal{C}_2$ can correct, due to the previous proposition and Theorem 3.

C. Near Optimality of the Obtained Construction

In this subsection, we will show the near optimality of Construction 1 in terms of its *introduced uncertainty* $H(C|\mathbf{x})$ compared to the maximum *observed information* $H(CB^T)$ by the wire-tapper, and the number of rank errors e that the scheme can list-decode.

Let $\mathbf{x} \in \mathbb{F}_q^\ell$ and $C \in \mathbb{F}_q^{m\times n}$ denote the random variables representing the secret message and the transmitted codeword, respectively, as in Subsection III-C.

The quantity $H(C|\mathbf{x})$ measures the amount of randomness of C given $\mathbf{x}$ introduced by the corresponding coset coding scheme, and we would like it to be as small as possible since generating randomness is difficult in practice. Observe that $H(C|\mathbf{x}) = \dim(\mathcal{C}_2)$ for nested coset coding schemes. On the other hand, the quantity $H(CB^T)$ measures the amount of observed information by wire-tapping μ links if $B \in \mathbb{F}_q^{\mu\times n}$, which satisfies $H(CB^T) \le m\mu$, being the inequality usually tight when $I(\mathbf{x}; CB^T) = 0$ or even an equality, as is the case for Gabidulin codes. Thus the following bound is a weaker version of a bound of the form $mt \le \dim(\mathcal{C}_2)$, which we leave as open problem.

Proposition 29: Fix an arbitrary coset coding scheme in $\mathbb{F}_q^{m\times n}$ with message set $\mathcal{S} = \mathbb{F}_q^\ell$, let $\mathbf{x} \in \mathbb{F}_q^\ell$, and let $C \in \mathbb{F}_q^{m\times n}$ be its encoding. It holds that

$$\max\{H(CB^T) \mid B \in \mathbb{F}_q^{\mu\times n}, I(\mathbf{x}; CB^T) = 0\} \le H(C|\mathbf{x}).$$

Proof: Fix $B \in \mathbb{F}_q^{\mu\times n}$. The result follows from the following chain of inequalities:

$$\begin{aligned} I(\mathbf{x}; CB^T) &= H(CB^T) - H(CB^T|\mathbf{x}) \\ &= H(CB^T) - H(CB^T|C,\mathbf{x}) \\ &\quad + H(CB^T|C,\mathbf{x}) - H(CB^T|\mathbf{x}) \\ &= H(CB^T) - H(CB^T|C) \\ &\quad + H(CB^T|C,\mathbf{x}) - H(CB^T|\mathbf{x}) \\ &\quad \text{(since } \mathbf{x} \to C \to CB^T \text{ is a Markov chain [8])} \\ &= I(C; CB^T) - I(C; CB^T|\mathbf{x}) \\ &\ge H(CB^T) - H(C|\mathbf{x}). \end{aligned}$$

□

Now consider the coset coding scheme in Construction 1, and fix $\mu \le k_1$. Define the Gabidulin code

$$\mathcal{G}_1 = \{M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))) \mid F_i = 0, i \ge k_1\} \subseteq \mathbb{F}_q^{m\times n},$$

and let G be the uniform random variable on $\mathcal{G}_1$. It holds that

$$\max_{B\in\mathbb{F}_q^{\mu\times n}} H(GB^T) = m\mu, \tag{11}$$

since $\mu \le k_1$. Equation (11) together with $\dim(\mathcal{G}_1/\mathcal{C}_1) \le 2m\varepsilon(k_1-k_2)$ implies that

$$\max_{B\in\mathbb{F}_q^{\mu\times n}} H(CB^T) \ge m(\mu - 2\varepsilon(k_1-k_2)).$$

Using that $H(C|\mathbf{x}) = \dim(\mathcal{C}_2) = mk_2$, we see that the bound in the previous proposition is tight for Construction 1:

$$\begin{aligned} 0 &\le H(C|\mathbf{x}) - \max\{H(CB^T) \mid B \in \mathbb{F}_q^{\mu\times n}, I(\mathbf{x}; CB^T) = 0\} \\ &\le m(k_2 - t + 2\varepsilon(k_1-k_2)) \le 2\varepsilon m(k_1-k_2). \end{aligned}$$

Next we show that the rank list-decoding capability cannot be improved for large s and small ε, compared to general nested coset coding schemes. Since rank list-decodable nested coset coding schemes still require decoding each coset, we will consider those such that a complementary space $\mathcal{W}$ as in Definition 3 is rank list-decodable with polynomial-sized lists after adding an error matrix from the smaller code $\mathcal{C}_2$:

Proposition 30: Fix a nested linear code pair $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$ and a subspace $\mathcal{W} \subseteq \mathcal{C}_1$ such that $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{W}$, and denote by M the maximum rank of a matrix in $\mathcal{C}_2$. If $\mathcal{W}$ is rank $(e+M, L)$-list-decodable with polynomial list sizes L, then

$$e \le n - \frac{\dim(\mathcal{C}_1)}{m}.$$

Proof: By [11, Proposition 1], if the linear code $\mathcal{W}$ is rank $(e+M, L)$-list-decodable with polynomial-sized lists L, then

$$e + M \le n - \dim(\mathcal{W})/m.$$

On the other hand, the maximum rank of codewords in $\mathcal{C}_2$ is at least $\dim(\mathcal{C}_2)/m$ by [35, Proposition 47]. Hence

$$e \le n - \frac{\dim(\mathcal{W})}{m} - \frac{\dim(\mathcal{C}_2)}{m} = n - \frac{\dim(\mathcal{C}_1)}{m},$$

and we are done. □

For the nested coset coding scheme in Construction 1, it holds that

$$e = \frac{s}{s+1}(n-k_1),$$

and

$$n - \frac{\dim(\mathcal{C}_1)}{m} = n - k_1(1-2\varepsilon) - 2\varepsilon k_2,$$

which are closer as s becomes larger and ε becomes smaller.

VI. Security Equivalences of Linear Coset Coding Schemes and Minimum Parameters

In this section, we study when two nested linear code pairs $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m\times n}$ and $\mathcal{C}_2' \subsetneq \mathcal{C}_1' \subseteq \mathbb{F}^{m'\times n'}$ have the same universal security and/or reliability performance.

First, we define security equivalences and give several characterizations of these in Theorem 4 (Subsection VI-A), which show that they also preserve error and erasure correction capabilities. As applications, we study ranges and minimum possible parameters m and n for linear codes (Subsection VI-B), and we study when they are degenerate (Subsection VI-C), meaning when they can be applied to networks with strictly smaller length n.

A. Security Equivalences and Rank Isometries

In this subsection, we first give in Theorem 4 the above mentioned characterizations, and we define afterwards security equivalences as maps satisfying one of such characterizations. We continue with Proposition 36, which shows that security equivalences actually preserve universal security performance as in Subsection II-B, thus motivating our definition. We conclude by comparing Theorem 4 with related results from the literature (see also Table III).

Due to the importance of the rank metric for error and erasure correction in linear network coding (see Subsection II-B), and for universal security (by Theorem 1 and Corollary 13), we start by considering rank isometries:

Definition 31 (Rank Isometries): We say that a map $\phi : \mathcal{V} \longrightarrow \mathcal{W}$ between vector spaces $\mathcal{V} \subseteq \mathbb{F}^{m\times n}$ and $\mathcal{W} \subseteq \mathbb{F}^{m'\times n'}$ is a rank isometry if it is a vector space isomorphism and $\mathrm{Rk}(\phi(V)) = \mathrm{Rk}(V)$, for all $V \in \mathcal{V}$. In that case, we say that $\mathcal{V}$ and $\mathcal{W}$ are rank isometric.

We have the following result, which was first proven in [27, Theorem 1] for square matrices and the complex field $\mathbb{F} = \mathbb{C}$. In [30, Proposition 3] it is observed that the square condition is not necessary and it may be proven for arbitrary fields:

Proposition 32 [27], [30]: If $\phi : \mathbb{F}^{m\times n} \longrightarrow \mathbb{F}^{m\times n}$ is a rank isometry, then there exist invertible matrices $A \in \mathbb{F}^{m\times m}$ and $B \in \mathbb{F}^{n\times n}$ such that

1) *$\phi(C) = ACB$, for all $C \in \mathbb{F}^{m\times n}$, or*
2) *$\phi(C) = AC^TB$, for all $C \in \mathbb{F}^{m\times n}$,*

where the latter case can only happen if $m = n$.

We will define security equivalences as certain vector space isomorphisms satisfying one of several equivalent conditions. We first show their equivalence in the following theorem, which is the main result of this section:

Theorem 4: Let $\phi : \mathcal{V} \longrightarrow \mathcal{W}$ be a vector space isomorphism between rank support spaces $\mathcal{V} \in RS(\mathbb{F}^{m\times n})$ and $\mathcal{W} \in RS(\mathbb{F}^{m\times n'})$, and consider the following properties:

(P 1) *There exist full-rank matrices $A \in \mathbb{F}^{m\times m}$ and $B \in \mathbb{F}^{n\times n'}$ such that $\phi(C) = ACB$, for all $C \in \mathcal{V}$.*
(P 2) *A subspace $\mathcal{U} \subseteq \mathcal{V}$ is a rank support space if, and only if, $\phi(\mathcal{U})$ is a rank support space.*
(P 3) *For all subspaces $\mathcal{D} \subseteq \mathcal{V}$, it holds that $\mathrm{wt_R}(\phi(\mathcal{D})) = \mathrm{wt_R}(\mathcal{D})$.*
(P 4) *ϕ is a rank isometry.*

Then the following implications hold:

$$(P\ 1) \Longleftrightarrow (P\ 2) \Longleftrightarrow (P\ 3) \Longrightarrow (P\ 4).$$

In particular, a security equivalence is a rank isometry and, in the case $\mathcal{V} = \mathcal{W} = \mathbb{F}^{m\times n}$ and $m \neq n$, the reversed implication holds by Proposition 32.

Proof: See Appendix C. □

Remark 33: Unfortunately, the implication $(P\ 3) \Longleftarrow (P\ 4)$ does not always hold. Take for instance $m = n$ and the map $\phi : \mathbb{F}^{m\times m} \longrightarrow \mathbb{F}^{m\times m}$ given by $\phi(C) = C^T$, for all $C \in \mathbb{F}^{m\times m}$.

Remark 34: Observe that, in particular, security equivalences also preserve (relative) generalized matrix weights, (relative) dimension/rank support profiles and distributions of rank weights of vector subspaces, and they are the only rank isometries with these properties.

Property (P 1) will be useful for technical computations and, in particular, for Proposition 36 below. As explained in Appendix C, (P 2) allows us to connect (P 1) with (P 3), and (P 3) allows us to connect the first two with the rank metric (P 4), crucial for error and erasure correction as in Subsection II-B. Finally, Property (P 2) also explains why we will consider security equivalences defined between rank support spaces, and intuitively explains that such spaces behave as ambient spaces in our theory, as mentioned in Subsection III-A.

Definition 35 (Security Equivalences): We say that a map $\phi : \mathcal{V} \longrightarrow \mathcal{W}$ between rank support spaces $\mathcal{V} \in RS(\mathbb{F}^{m\times n})$ and $\mathcal{W} \in RS(\mathbb{F}^{m\times n'})$ is a security equivalence if it is a vector space isomorphism and satisfies condition (P 1), (P 2) or (P 3) in Theorem 4.

Two nested linear code pairs $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m\times n}$ and $\mathcal{C}'_2 \subsetneqq \mathcal{C}'_1 \subseteq \mathbb{F}^{m\times n'}$ are said to be security equivalent if there exist rank support spaces $\mathcal{V} \in RS(\mathbb{F}^{m\times n})$ and $\mathcal{W} \in RS(\mathbb{F}^{m\times n'})$, containing $\mathcal{C}_1$ and $\mathcal{C}'_1$, respectively, and a security equivalence $\phi : \mathcal{V} \longrightarrow \mathcal{W}$ with $\phi(\mathcal{C}_1) = \mathcal{C}'_1$ and $\phi(\mathcal{C}_2) = \mathcal{C}'_2$.

We now motivate the previous definition with the next proposition, which makes use of Theorem 4. Observe that Remark 34 above already shows that security equivalences preserve the worst-case information leakage as described in Theorem 1. Now, given nested linear code pairs $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$ and $\mathcal{C}'_2 \subsetneqq \mathcal{C}'_1 \subseteq \mathbb{F}_q^{m\times n'}$, Proposition 36 below shows that if the dual pairs are security equivalent, then there exists a bijective correspondence between wire-tappers' transfer matrices (matrix B in Subsection II-B, item 2) that preserves the mutual information with the original sent message. If the original pairs are also security equivalent, we conclude that encoding with $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$ or $\mathcal{C}'_2 \subsetneqq \mathcal{C}'_1 \subseteq \mathbb{F}_q^{m\times n'}$ yields exactly the same universal error and erasure correction performance, and exactly the same universal security performance over linearly coded networks, as in Subsection II-B.

Proposition 36: Assume that $\mathbb{F} = \mathbb{F}_q$ and the dual pairs of $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$ and $\mathcal{C}'_2 \subsetneqq \mathcal{C}'_1 \subseteq \mathbb{F}_q^{m\times n'}$ are security equivalent by a security equivalence given by matrices $A \in \mathbb{F}_q^{m\times m}$ and $B \in \mathbb{F}_q^{n\times n'}$ as in item 1 in Theorem 4. For any matrix $M \in \mathbb{F}_q^{\mu\times n}$, it holds that

$$I\left(\mathbf{x}; CM^T\right) = I\left(\mathbf{x}; C'(MB)^T\right), \tag{12}$$

with notation as in Proposition 16, where $C \in \mathbb{F}_q^{m\times n}$ and $C' \in \mathbb{F}_q^{m\times n'}$ are the encodings of $\mathbf{x}$ using $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$ and $\mathcal{C}'_2 \subsetneqq \mathcal{C}'_1 \subseteq \mathbb{F}^{m\times n'}$, respectively.

Furthermore, assuming $n \leq n'$, the correspondence $M \mapsto MB$ is one to one and, for any matrix $N \in \mathbb{F}_q^{\mu\times n'}$, there exists $M \in \mathbb{F}_q^{\mu\times n}$ such that $I\left(\mathbf{x}; C'N^T\right) = I\left(\mathbf{x}; C'(MB)^T\right)$.

Proof: Denote by ϕ the security equivalence. Take a matrix $M \in \mathbb{F}_q^{\mu\times n}$, define $\mathcal{L} = \mathrm{Row}(M) \subseteq \mathbb{F}_q^n$ and $\mathcal{L}' = \mathrm{Row}(MB) \subseteq \mathbb{F}_q^{n'}$. Then $\phi(\mathcal{V}_{\mathcal{L}}) = \mathcal{V}_{\mathcal{L}'}$ and

$$\dim(\phi(\mathcal{C}_1^\perp) \cap \mathcal{V}_{\mathcal{L}'}) = \dim(\phi(\mathcal{C}_1^\perp \cap \mathcal{V}_{\mathcal{L}})) = \dim(\mathcal{C}_1^\perp \cap \mathcal{V}_{\mathcal{L}}),$$

and similarly for $\mathcal{C}_2$. Thus Equation (12) follows from Proposition 16.

Observe that we may assume $n \leq n'$ without loss of generality, since the inverse of a security equivalence is a security equivalence. Thus the injectivity of $M \mapsto MB$ follows from the fact that B has full rank.

Finally, if $N \in \mathbb{F}_q^{\mu \times n'}$, $\mathcal{L} = \mathrm{Row}(N)$ and $\mathcal{K} = \mathrm{Row}(B)$, then $\mathcal{C}_1^\perp \subseteq \mathcal{V}_\mathcal{K}$ and

$$\mathcal{C}_1^\perp \cap \mathcal{V}_\mathcal{L} = \mathcal{C}_1^\perp \cap (\mathcal{V}_\mathcal{L} \cap \mathcal{V}_\mathcal{K}),$$

and similarly for $\mathcal{C}_2^\perp$. Since $\mathcal{V}_\mathcal{L} \cap \mathcal{V}_\mathcal{K} = \mathcal{V}_{\mathcal{L}\cap\mathcal{K}}$ and $\mathcal{L} \cap \mathcal{K} = \mathrm{Row}(MB)$ for a matrix $M \in \mathbb{F}_q^{\mu \times n}$, the last statement follows again from Proposition 16. □

The topic of vector space isomorphisms $\phi : \mathbb{F}^{m\times n} \longrightarrow \mathbb{F}^{m\times n}$ preserving some specified property has been intensively studied in the literature (see also Table III), where the term *Frobenius map* is generally used for maps of the form of those in Proposition 32.

When $m = n$, it is proven in [10, Th. 3] that Frobenius maps are characterized by being those preserving invertible matrices and in [27] they are characterized by being those preserving ranks (this is extended to $m \neq n$ in [30, Proposition 3]), those preserving determinants and those preserving eigenvalues.

On the other hand, [3, Th. 1] shows that $\mathbb{F}_{q^m}$-linear vector space isomorphisms $\phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ preserving ranks are given by $\phi(\mathbf{c}) = \beta \mathbf{c} A$, for $\beta \in \mathbb{F}_{q^m} \setminus \{0\}$ and an invertible $A \in \mathbb{F}_q^{n\times n}$. This is extended in [28, Th. 5] to $\mathbb{F}_{q^m}$-linear vector space isomorphisms whose domain and codomain are $\mathbb{F}_{q^m}$-linear Galois closed spaces in $\mathbb{F}_{q^m}^n$, which correspond to rank support spaces in $\mathbb{F}_q^{m\times n}$ (see Lemma 52 below).

Therefore, we extend these works in three directions simultaneously: First, we consider the stronger properties (P 1), (P 2) and (P 3) than those considered in [3], [10], [27], and [30], which are essentially (P 4). Second, we extend the domains and codomains from $\mathbb{F}^{m\times n}$ to general rank support spaces whose matrices do not necessarily have the same sizes. Finally, in the case $\mathbb{F} = \mathbb{F}_q$, we consider general $\mathbb{F}_q$-linear maps, instead of the particular case of $\mathbb{F}_{q^m}$-linear maps as in [3] and [28].

B. Minimum Parameters of Linear Codes

As main application of the previous subsection, we study in this subsection the minimum parameters m and n for which there exists a linear code that is security equivalent to a given one. Recall from Subsection II-A that m corresponds to the packet length used in the network, and n corresponds to the number of outgoing links from the source.

Both cases of one linear code, that is $\mathcal{C}_2 = \{0\}$ and $\mathcal{C}_1 = \mathbb{F}^{m\times n}$, are covered since they are dual of each other (see also Remark 4 and Appendix A). Since security equivalences are rank isometries by Theorem 4, in the first case we find minimum parameters for error and erasure correction, and in the second case we find minimum parameters for universal security on noiseless linearly coded networks.

Proposition 37: Fix a linear code $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ of dimension k. There exists a linear code $\mathcal{C}' \subseteq \mathbb{F}^{m\times n'}$ that is security equivalent to $\mathcal{C}$ if, and only if, $n' \geq d_{M,k}(\mathcal{C})$.

Proof: First, if $\mathcal{C}' \subseteq \mathbb{F}^{m\times n'}$ is security equivalent to $\mathcal{C}$, then $\dim(\mathcal{C}') = k$ and $d_{M,k}(\mathcal{C}) = d_{M,k}(\mathcal{C}') \leq n'$.

On the other hand, assume that $n' \geq d_{M,k}(\mathcal{C})$. Take a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ with $d = \dim(\mathcal{L}) = d_{M,k}(\mathcal{C})$ and $\dim(\mathcal{C} \cap \mathcal{V}_\mathcal{L}) \geq k$, which implies that $\mathcal{C} \subseteq \mathcal{V}_\mathcal{L}$. Take a generator matrix $A \in \mathbb{F}^{d\times n}$ of $\mathcal{L}$. There exists a full-rank matrix $A' \in \mathbb{F}^{n\times d}$ such that $AA' = I \in \mathbb{F}^{d\times d}$.

The linear map $\phi : \mathcal{V}_\mathcal{L} \longrightarrow \mathbb{F}^{m\times d}$, given by $\phi(V) = VA'$, for $V \in \mathcal{V}_\mathcal{L}$, is a vector space isomorphism. By dimensions, we just need to see that it is onto. Take $W \in \mathbb{F}^{m\times d}$. It holds that $W = WI = WAA' = \phi(WA)$, and $WA \in \mathcal{V}_\mathcal{L}$ by definition.

On the other hand, ϕ is a security equivalence by Theorem 4. Therefore $\phi(\mathcal{C}) \subseteq \mathbb{F}^{m\times d}$ is security equivalent to $\mathcal{C}$. Finally, we see that appending $n' - d$ zero columns to the matrices in $\phi(\mathcal{C})$ gives a security equivalent code to $\mathcal{C}$ in $\mathbb{F}^{m\times n'}$. □

By transposing matrices, we obtain the following consequence, where we consider linear codes that are rank isometric to a given one. By [28, Th. 9], such equivalent codes perform equally when used for error and erasure correction, and by Theorem 1 and Corollary 13, they perform equally regarding the maximum number of links that an adversary may wire-tap without obtaining any information on noiseless networks.

Corollary 38: For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$, define the transposed linear code

$$\mathcal{C}^T = \{C^T \mid C \in \mathcal{C}\} \subseteq \mathbb{F}^{n\times m}.$$

If $m' \geq d_{M,k}(\mathcal{C}^T)$, where $k = \dim(\mathcal{C})$, then there exists a linear code $\mathcal{C}' \subseteq \mathbb{F}^{m'\times n}$ that is rank isometric to $\mathcal{C}$.

Proof: It follows from Theorem 4 and Proposition 37. □

As a related result, [28, Proposition 3] computes the minimum parameter n for which there exists an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ that is rank isometric to a given one. In contrast, we consider both parameters m and n, we consider security equivalences for the parameter n, and not only rank isometries, and as the biggest difference with [28], we consider general linear codes, and not only $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$.

C. Degenerate Codes

In this subsection, we study degenerate codes, which by the study in the previous subsection, can be applied to networks with less outgoing links or, by transposing matrices, with smaller packet length. Degenerateness of codes in the rank metric has been studied in [22, Sec. 6] and [28, Sec. IV-B], but only for $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$. We extend those studies to general linear codes in $\mathbb{F}^{m\times n}$.

Definition 39 (Degenerate Codes): We say that a linear code $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ is degenerate if it is security equivalent to a linear code $\mathcal{C}' \subseteq \mathbb{F}^{m\times n'}$ with $n' < n$.

The following lemma follows from Proposition 37:

Lemma 40: A linear code $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ is degenerate if, and only if, $d_{M,k}(\mathcal{C}) < n$, where $k = \dim(\mathcal{C})$.

Now we may give characterizations in terms of the minimum rank distance of the dual code thanks to Proposition 65 in Appendix A.

Proposition 41: Given a linear code $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$, the following hold:

1) *Assuming $\dim(\mathcal{C}^\perp) \geq m$, $\mathcal{C}$ is degenerate if, and only if, $d_{M,m}(\mathcal{C}^\perp) = 1$.*
2) *If $d_R(\mathcal{C}^\perp) > 1$, then $\mathcal{C}$ is not degenerate.*

Proof: From Proposition 65 (see Appendix A), we know that

$$\overline{W}_k(\mathcal{C}) \cup W_0(\mathcal{C}^\perp) = \{1, 2, \ldots, n\},$$

where the sets on the left-hand side are disjoint, and where $k = \dim(\mathcal{C})$. Now, the smallest number in $\overline{W}_k(\mathcal{C})$ is $n+1-d_{M,k}(\mathcal{C})$, and the smallest number in $W_0(\mathcal{C}^\perp)$ is $d_{M,m}(\mathcal{C}^\perp)$. Item 1 follows from this and the previous lemma. Item 2 follows from item 1 and Proposition 43 in Subsection VII-A. □

VII. Monotonicity and Singleton-Type Bounds

In this section, we give upper and lower Singleton-type bounds on RGMWs. We start with the monotonicity of RDRPs and RGMWs (Subsection VII-A), which have their own interest, but which are a crucial tool to prove the main bounds (Theorems 5 and 6 in Subsection VII-B). Finally we study linear codes $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$, meaning $\mathcal{C}_1 = \mathcal{C}$ and $\mathcal{C}_2 = \{0\}$, that attain these bounds and whose dimensions are divisible by m (Subsection VII-C).

A. Monotonicity of RGMWs and RDRPs

The monotonicity bounds presented in this subsection are crucial tools for Theorems 5 and 6, but they also have an interpretation in terms of the worst-case information leakage, due to Theorem 1: An adversary wire-tapping more links in the network will obtain more information in the worst case, and to obtain more information than the worst case for a given number of links, the adversary needs to wire-tap more links. We also bound the corresponding differences.

Proposition 42 (Monotonicity of RDRPs): Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m\times n}$, and $0 \le \mu \le n-1$, it holds that $K_{M,0}(\mathcal{C}_1, \mathcal{C}_2) = 0$, $K_{M,n}(\mathcal{C}_1, \mathcal{C}_2) = \dim(\mathcal{C}_1/\mathcal{C}_2)$ and

$$0 \le K_{M,\mu+1}(\mathcal{C}_1, \mathcal{C}_2) - K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) \le m.$$

Proof: The only property that is not trivial from the definitions is $K_{M,\mu+1}(\mathcal{C}_1, \mathcal{C}_2) - K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) \le m$. Consider $\mathcal{L} \subseteq \mathbb{F}^n$ with $\dim(\mathcal{L}) \le \mu + 1$ and $\dim(\mathcal{C}_1 \cap \mathcal{V}_\mathcal{L}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_\mathcal{L}) = K_{M,\mu+1}(\mathcal{C}_1, \mathcal{C}_2)$.

Take $\mathcal{L}' \subsetneqq \mathcal{L}$ with $\dim(\mathcal{L}') = \dim(\mathcal{L}) - 1$. Using (2), a simple computation shows that

$$\dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}'}) + m \ge \dim(\mathcal{C}_1 \cap \mathcal{V}_\mathcal{L}).$$

Since $\dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}'}) \le \dim(\mathcal{C}_2 \cap \mathcal{V}_\mathcal{L})$, it holds that

$$\dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}'}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}'}) + m \ge \dim(\mathcal{C}_1 \cap \mathcal{V}_\mathcal{L}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_\mathcal{L}),$$

and the result follows. □

Proposition 43 (Monotonicity of RGMWs): Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m\times n}$ with $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that

$$0 \le d_{M,r+1}(\mathcal{C}_1, \mathcal{C}_2) - d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \le \min\{m, n\},$$

for $1 \le r \le \ell - 1$, and

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) + 1 \le d_{M,r+m}(\mathcal{C}_1, \mathcal{C}_2),$$

for $1 \le r \le \ell - m$.

Proof: The first inequality in the first equation is obvious. We now prove the second inequality. By Proposition 12, there exists a subspace $\mathcal{D} \subseteq \mathcal{C}_1$ with $\mathcal{D} \cap \mathcal{C}_2 = \{0\}$, $\dim(\mathcal{D}) = r$ and $\mathrm{wt_R}(\mathcal{D}) = d_{M,r}(\mathcal{C}_1, \mathcal{C}_2)$. Now take $D \in \mathcal{C}_1$ not contained in $\mathcal{D} \oplus \mathcal{C}_2$, and consider $\mathcal{D}' = \mathcal{D} \oplus \langle\{D\}\rangle$. We see from the definitions that $\mathrm{RSupp}(\mathcal{D}') \subseteq \mathrm{RSupp}(\mathcal{D}) + \mathrm{Row}(D)$, and hence

$$\mathrm{wt_R}(\mathcal{D}') \le \mathrm{wt_R}(\mathcal{D}) + \mathrm{Rk}(D) \le d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) + \min\{m, n\}.$$

Therefore it follows that $d_{M,r+1}(\mathcal{C}_1, \mathcal{C}_2) \le d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) + \min\{m, n\}$.

The last inequality follows from Proposition 14 and Proposition 42. □

Due to Theorem 9, the first and third inequalities in the previous proposition coincide with items 3 and 4 in [34, Th. 30] when $\mathcal{C}_2 = \{0\}$ and $m \ne n$.

B. Upper and Lower Singleton-Type Bounds

Due to Theorem 1, it is desirable to obtain nested linear code pairs with large RGMWs. The following result gives a fundamental upper bound on them, whose achievability for one linear code ($\mathcal{C}_2 = \{0\}$) is studied in the next subsection.

Theorem 5 (Upper Singleton-Type Bound): Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m\times n}$ and $1 \le r \le \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \le n - \left\lceil \frac{\ell - r + 1}{m} \right\rceil + 1. \tag{13}$$

In particular, it follows that

$$\dim(\mathcal{C}_1/\mathcal{C}_2) \le \max\{m, n\}(\min\{m, n\} - d_R(\mathcal{C}_1, \mathcal{C}_2) + 1),$$

which extends (8) to nested linear code pairs.

Proof: First of all, we have that $d_{M,\ell}(\mathcal{C}_1, \mathcal{C}_2) \le n$ by definition. Therefore the case $r = \ell$ follows.

For the general case, we will prove that $md_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \le mn - \ell + r + m - 1$. Assume that $1 \le r \le \ell - hm$, where the integer $h \ge 0$ is the maximum possible. That is, $r + (h+1)m > \ell$. Using Proposition 43, we obtain

$$\begin{aligned} md_{M,r}(\mathcal{C}_1, \mathcal{C}_2) &\le md_{M,r+hm}(\mathcal{C}_1, \mathcal{C}_2) - hm \le md_{M,\ell}(\mathcal{C}_1, \mathcal{C}_2) - hm \\ &\le mn - \ell + r + m - 1, \end{aligned}$$

where the last inequality follows from $md_{M,\ell}(\mathcal{C}_1, \mathcal{C}_2) \le mn$ and $r + (h+1)m - 1 \ge \ell$.

Finally, the last bound is obtained by setting $r = 1$ and using Corollary 13 for the given nested linear code pair and the pair obtained by transposing matrices. □

Due to Theorem 9, the previous theorem coincides with item 5 in [34, Th. 30] when $\mathcal{C}_2 = \{0\}$ and $m \ne n$.

Remark 44: In view of [24, Proposition 1] or [26, eq. (24)], it is natural to wonder whether a sharper bound of the form

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \le n - \left\lceil \frac{\dim(\mathcal{C}_1) - r + 1}{m} \right\rceil + 1$$

holds. However, this is not the case in general, as the following example shows.

Example 45: Consider $m = 2$, the canonical basis $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ of $\mathbb{F}^n$, and the linear codes $\mathcal{C}_1 = \mathbb{F}^{2\times n}$ and

$$\mathcal{C}_2 = \left\langle \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{0} \end{pmatrix}, \begin{pmatrix} \mathbf{e}_2 \\ \mathbf{0} \end{pmatrix}, \ldots, \begin{pmatrix} \mathbf{e}_n \\ \mathbf{0} \end{pmatrix} \right\rangle.$$

Observe that $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2) = n$. A bound as in the previous remark would imply that $d_{M,n}(\mathcal{C}_1, \mathcal{C}_2) \leq \lceil n/2 \rceil$. However, a direct inspection shows that $d_{M,n}(\mathcal{C}_1, \mathcal{C}_2) = n$, since all vectors $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ must lie in the row space of any $\mathcal{D}$ with $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{D}$.

On the other hand, we have the following lower bound:

Theorem 6 (Lower Singleton-Type Bound): Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m\times n}$ and $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that $md_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \geq r$, which implies that

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \geq \left\lceil \frac{r}{m} \right\rceil. \tag{14}$$

Proof: Take a subspace $\mathcal{D} \subseteq \mathbb{F}^{m\times n}$ and define $\mathcal{L} = \mathrm{RSupp}(\mathcal{D})$. We have that $\mathcal{D} \subseteq \mathcal{V}_{\mathcal{L}}$. Using (2), we see that

$$m\mathrm{wt_R}(\mathcal{D}) = m\dim(\mathcal{L}) = \dim(\mathcal{V}_{\mathcal{L}}) \geq \dim(\mathcal{D}).$$

The result follows from this and Proposition 12. □

Due to Theorem 9, the previous theorem coincides with item 6 in [34, Th. 30] when $\mathcal{C}_2 = \{0\}$ and $m \neq n$.

C. Linear Codes Attaining the Bounds and Whose Dimensions Are Divisible by the Packet Length

In this subsection, we study the achievability of the bounds (13) and (14) for one linear code whose dimension is divisible by the packet length m. As we will show in Subsection VIII-C, DGWs [34] of one linear code coincide with its GMWs when $m \neq n$. Thus the two propositions below coincide with Corollaries 31 and 32 in [34] when $m \neq n$.

Recall from (8) that, if a linear code is MRD and $n \leq m$, then its dimension is divisible by m. In the next proposition, we show that GMWs of MRD linear codes for $n \leq m$ are all given by m, n and $\dim(\mathcal{C})$, and all attain the upper Singleton-type bound (13):

Proposition 46: Let $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ be a linear code with $\dim(\mathcal{C}) = mk$. The following are equivalent if $n \leq m$:

1) *$\mathcal{C}$ is maximum rank distance (MRD).*
2) *$d_R(\mathcal{C}) = n - k + 1$.*
3) *$d_{M,r}(\mathcal{C}) = n - k + \left\lfloor \frac{r-1}{m} \right\rfloor + 1$, for all $1 \leq r \leq mk$.*

Proof: Item 1 and item 2 are equivalent by definition, and item 3 implies item 2 by choosing $r = 1$.

Now assume item 2 and let $1 \leq r \leq mk$. Let $r = hm + s$, with $h \geq 0$ and $0 \leq s < m$. We need to distinguish the cases $s > 0$ and $s = 0$. We prove only the first case, being the second analogous. By Proposition 43, we have that

$$d_{M,r}(\mathcal{C}) \geq h + d_{M,s}(\mathcal{C}) \geq h + d_R(\mathcal{C}) = n - k + h + 1.$$

On the other hand, $\lceil (mk - r + 1)/m \rceil = k - h$, and therefore the bound (13) implies that

$$d_{M,r}(\mathcal{C}) \leq n - k + h + 1,$$

and hence $d_{M,r}(\mathcal{C}) = n - k + \lfloor (r-1)/m \rfloor + 1$ since $\lfloor (r-1)/m \rfloor = h$, and item 3 follows. □

Regarding the lower Singleton-type bound, we show in the next proposition that rank support spaces are also characterized by having the minimum possible GMWs in view of (14):

Proposition 47: Let $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ be a linear code with $\dim(\mathcal{C}) = mk$. The following are equivalent:

1) *$\mathcal{C}$ is a rank support space. That is, there exists a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\mathcal{C} = \mathcal{V}_{\mathcal{L}}$.*
2) *$d_{M,km}(\mathcal{C}) = k$.*
3) *$d_{M,r}(\mathcal{C}) = \lceil r/m \rceil$, for all $1 \leq r \leq mk$.*

Proof: Assume that $\mathcal{C} = \mathcal{V}_{\mathcal{L}}$, as in item 1. By taking a sequence of subspaces

$$\{\mathbf{0}\} \subsetneqq \mathcal{L}_1 \subsetneqq \mathcal{L}_2 \subsetneqq \ldots \subsetneqq \mathcal{L}_k = \mathcal{L},$$

we see that $d_{M,rm-p}(\mathcal{C}) \leq \dim(\mathcal{L}_r) = r$, for $1 \leq r \leq k$ and $0 \leq p \leq m-1$, since $\dim(\mathcal{C} \cap \mathcal{V}_{\mathcal{L}_r}) = \dim(\mathcal{V}_{\mathcal{L}_r}) = mr \geq mr - p$. Hence item 3 follows.

Item 3 implies item 2 by taking $r = km$.

Finally, assume item 2. Take a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\dim(\mathcal{L}) = d_{M,km}(\mathcal{C}) = k$ and $\dim(\mathcal{C} \cap \mathcal{V}_{\mathcal{L}}) \geq mk$. By definition and by (2), it holds that $\dim(\mathcal{C} \cap \mathcal{V}_{\mathcal{L}}) \geq mk = \dim(\mathcal{V}_{\mathcal{L}})$, which implies that $\mathcal{C} \cap \mathcal{V}_{\mathcal{L}} = \mathcal{V}_{\mathcal{L}}$, or in other words, $\mathcal{V}_{\mathcal{L}} \subseteq \mathcal{C}$. Since $\dim(\mathcal{C}) = mk = \dim(\mathcal{V}_{\mathcal{L}})$, we see that $\mathcal{V}_{\mathcal{L}} = \mathcal{C}$ and item 1 follows. □

VIII. Relation With Other Existing Notions of Generalized Weights

In this section, we study the relation between RGMWs and RDRPs and other notions of generalized weights (see Table I). We first show that RGMWs and RDRPs extend RGRWs and RDIPs [24], [32] (Theorem 7 in Subsection VIII-A), respectively, then we show that they extend RGHWs and RDLPs [16], [26], [42] (Theorem 8 in Subsection VIII-B), respectively, and we conclude by showing that GMWs coincide with DGWs [34] for one linear code, meaning $\mathcal{C}_1 = \mathcal{C}$ arbitrary and $\mathcal{C}_2 = \{0\}$, when $m \neq n$, and are strictly larger when $m = n$ (Theorem 9 in Subsection VIII-C).

A. RGMWs Extend Relative Generalized Rank Weights

In this subsection, we prove that RGMWs and RDRPs extend RGRWs and RDIPs [24], [32], respectively.

Definition 48 (Galois Closed Spaces [41]): We say that an $\mathbb{F}_{q^m}$-linear vector space $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is Galois closed if

$$\mathcal{V}^q = \{(v_1^q, v_2^q, \ldots, v_n^q) \mid (v_1, v_2, \ldots, v_n) \in \mathcal{V}\} \subseteq \mathcal{V}.$$

We denote by $\Upsilon(\mathbb{F}_{q^m}^n)$ the family of $\mathbb{F}_{q^m}$-linear Galois closed vector spaces in $\mathbb{F}_{q^m}^n$.

RGRWs and RDIPs are then defined in [24] as follows:

Definition 49 (Relative Generalized Rank Weigths [24, Definition 2]): Given nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$ (over $\mathbb{F}_{q^m}$), we define their r-th relative generalized rank weight (RGRW) as

$$d_{R,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\dim(\mathcal{V}) \mid \mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n), \\ \dim(\mathcal{C}_1 \cap \mathcal{V}) - \dim(\mathcal{C}_2 \cap \mathcal{V}) \geq r\},$$

where dimensions are taken over $\mathbb{F}_{q^m}$.

Definition 50 (Relative Dimension/Intersection Profile [24, Definition 1]): Given nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, and $0 \leq \mu \leq n$, we define their μ-th relative dimension/intersection profile (RDIP) as

$$K_{R,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{\dim(\mathcal{C}_1 \cap \mathcal{V}) - \dim(\mathcal{C}_2 \cap \mathcal{V}) \mid \mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n), \quad \dim(\mathcal{V}) \leq \mu\},$$

where dimensions are taken over $\mathbb{F}_{q^m}$.

The following is the main result of the subsection, which shows that Theorem 1 extends the study on worst-case information leakage on $\mathbb{F}_q$-linearly coded networks in [24] (see its Theorem 2 and Corollary 5) from $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ to general $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m\times n}$, when considering uniform probability distributions.

Theorem 7: Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be a basis of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$. Given nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, and integers $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$ (over $\mathbb{F}_{q^m}$), $0 \leq p \leq m-1$ and $0 \leq \mu \leq n$, we have that

$$d_{R,r}(\mathcal{C}_1, \mathcal{C}_2) = d_{M,rm-p}(M_{\boldsymbol{\alpha}}(\mathcal{C}_1), M_{\boldsymbol{\alpha}}(\mathcal{C}_2)),$$
$$mK_{R,\mu}(\mathcal{C}_1, \mathcal{C}_2) = K_{M,\mu}(M_{\boldsymbol{\alpha}}(\mathcal{C}_1), M_{\boldsymbol{\alpha}}(\mathcal{C}_2)),$$

where $M_{\boldsymbol{\alpha}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m\times n}$ is as in (1).

The theorem follows from the next two lemmas, where we take the first one from [41]:

Lemma 51 [41, Lemma 1]: An $\mathbb{F}_{q^m}$-linear vector space $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is Galois closed if, and only if, it has a basis of vectors in $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_{q^m}$.

Lemma 52: Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be a basis of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$, and let $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ be an arbitrary set. The following are equivalent:

1) *$\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is an $\mathbb{F}_{q^m}$-linear Galois closed vector space. That is, $\mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n)$.*
2) *$M_{\boldsymbol{\alpha}}(\mathcal{V}) \subseteq \mathbb{F}_q^{m\times n}$ is a rank support space. That is, $M_{\boldsymbol{\alpha}}(\mathcal{V}) \in RS(\mathbb{F}_q^{m\times n})$.*

Moreover, if $M_{\boldsymbol{\alpha}}(\mathcal{V}) = \mathcal{V}_{\mathcal{L}}$ for a subspace $\mathcal{L} \subseteq \mathbb{F}_q^n$, then

$$\dim(\mathcal{V}) = \dim(\mathcal{L}),$$

where $\dim(\mathcal{V})$ is taken over $\mathbb{F}_{q^m}$ and $\dim(\mathcal{L})$ over $\mathbb{F}_q$.

Proof: We first observe the following. For an arbitrary set $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$, the previous lemma states that $\mathcal{V}$ is an $\mathbb{F}_{q^m}$-linear Galois closed vector space if, and only if, $\mathcal{V}$ is $\mathbb{F}_q$-linear and it has a basis over $\mathbb{F}_q$ of the form $\mathbf{v}_{i,j} = \alpha_i \mathbf{b}_j$, for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, k$, where $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{F}_q^n$. By considering $B_{i,j} = M_{\boldsymbol{\alpha}}(\mathbf{v}_{i,j}) \in \mathbb{F}_q^{m\times n}$, we see that this condition is equivalent to item 2 in Proposition 9, and we are done. □

Remark 53: The results in this subsection can be extended to Galois extensions of fields $\mathbb{F} \subseteq \widetilde{\mathbb{F}}$ of finite degree m. For that purpose, we only need to define Galois closed spaces as those $\widetilde{\mathbb{F}}$-linear subspaces $\mathcal{V} \subseteq \widetilde{\mathbb{F}}^n$ that are closed under the action of every field morphism in the Galois group of the extension $\mathbb{F} \subseteq \widetilde{\mathbb{F}}$. The rest of definitions and results in this subsection can be directly translated word by word to this case, except for Lemma 51, which would be replaced by [18, Th. 1].

Thus the results in this subsection can be applied to generalizations of rank-metric codes such as those in [2].

B. RGMWs Extend Relative Generalized Hamming Weights

In this subsection, we show that RGMWs and RDRPs also extend RGHWs and RDLPs [16], [26], [42], respectively. We start with the definitions of Hamming supports and Hamming support spaces:

Definition 54 (Hamming Supports): Given a vector space $\mathcal{C} \subseteq \mathbb{F}^n$, we define its Hamming support as

$$\mathrm{HSupp}(\mathcal{C}) = \{i \in \{1, 2, \ldots, n\} \mid \exists (c_1, c_2, \ldots, c_n) \in \mathcal{C}, c_i \neq 0\}.$$

We also define the Hamming weight of the space $\mathcal{C}$ as

$$\mathrm{wt_H}(\mathcal{C}) = |\mathrm{HSupp}(\mathcal{C})|.$$

Finally, for a vector $\mathbf{c} \in \mathbb{F}^n$, we define its Hamming support as $\mathrm{HSupp}(\mathbf{c}) = \mathrm{HSupp}(\langle\{\mathbf{c}\}\rangle)$, and its Hamming weight as $\mathrm{wt_H}(\mathbf{c}) = \mathrm{wt_H}(\langle\{\mathbf{c}\}\rangle)$.

Definition 55 (Hamming Support Spaces): Given a subset $I \subseteq \{1, 2, \ldots, n\}$, we define its Hamming support space as the vector space in $\mathbb{F}^n$ given by

$$\mathcal{L}_I = \{(c_1, c_2, \ldots, c_n) \in \mathbb{F}^n \mid c_i = 0, \forall i \notin I\}.$$

We may now define RGHWs and RDLPs:

Definition 56 (Relative Generalized Hamming Weigths [26, Section III]): Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^n$, and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, we define their r-th relative generalized Hamming weight (RGHW) as

$$d_{H,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{|I| \mid I \subseteq \{1, 2, \ldots, n\}, \dim(\mathcal{C}_1 \cap \mathcal{L}_I) - \dim(\mathcal{C}_2 \cap \mathcal{L}_I) \geq r\}.$$

As in Proposition 12, it holds that

$$d_{H,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\mathrm{wt_H}(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C}_1, \mathcal{D} \cap \mathcal{C}_2 = \{0\}, \dim(\mathcal{D}) = r\}.$$

Given a linear code $\mathcal{C} \subseteq \mathbb{F}^n$, we see that its r-th GHW [42, Sec. II] is $d_{H,r}(\mathcal{C}) = d_{H,r}(\mathcal{C}, \{\mathbf{0}\})$, for $1 \leq r \leq \dim(\mathcal{C})$.

Definition 57 (Relative Dimension/Length Profile [16], [26]): Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^n$, and $0 \leq \mu \leq n$, we define their μ-th relative dimension/length profile (RDLP) as

$$K_{H,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{\dim(\mathcal{C}_1 \cap \mathcal{L}_I) - \dim(\mathcal{C}_2 \cap \mathcal{L}_I) \mid I \subseteq \{1, 2, \ldots, n\}, |I| \leq \mu\}.$$

To prove our results, we need to see vectors in $\mathbb{F}^n$ as matrices in $\mathbb{F}^{n\times n}$. To that end, we introduce the diagonal matrix representation map $\Delta : \mathbb{F}^n \longrightarrow \mathbb{F}^{n\times n}$ given by

$$\Delta(\mathbf{c}) = \mathrm{diag}(\mathbf{c}) = (c_i \delta_{i,j})_{1\leq i\leq n, 1\leq j\leq n}, \tag{15}$$

where $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}^n$ and $\delta_{i,j}$ represents the Kronecker delta. In other words, $\Delta(\mathbf{c})$ is the diagonal matrix whose diagonal vector is $\mathbf{c}$.

The map $\Delta : \mathbb{F}^n \longrightarrow \mathbb{F}^{n\times n}$ is linear, one to one and, for any vector space $\mathcal{D} \subseteq \mathbb{F}^n$, it holds that

$$\mathrm{wt_R}(\Delta(\mathcal{D})) = \mathrm{wt_H}(\mathcal{D}).$$

We may now give the main result of this subsection:

Theorem 8: Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^n$, and integers $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, and $0 \leq \mu \leq n$, we have that

$$d_{H,r}(\mathcal{C}_1, \mathcal{C}_2) = d_{M,r}(\Delta(\mathcal{C}_1), \Delta(\mathcal{C}_2)),$$
$$K_{H,\mu}(\mathcal{C}_1, \mathcal{C}_2) = K_{M,\mu}(\Delta(\mathcal{C}_1), \Delta(\mathcal{C}_2)).$$

Proof: We prove the first equality, being the second analogous. Denote by d_r the number on the left-hand side and by d'_r the number on the right-hand side, and prove both inequalities:

$d_r \leq d'_r$: Take a vector space $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\dim(\mathcal{L}) = d'_r$ and $\dim((\Delta(\mathcal{C}_1) \cap \mathcal{V}_\mathcal{L})/(\Delta(\mathcal{C}_2) \cap \mathcal{V}_\mathcal{L})) \geq r$. It holds that $\mathcal{V}_\mathcal{L} \cap \Delta(\mathbb{F}^n) = \Delta(\mathcal{L}_I)$, for some subset $I \subseteq \{1, 2, \ldots, n\}$. We have that $\dim((\mathcal{C}_1 \cap \mathcal{L}_I)/(\mathcal{C}_2 \cap \mathcal{L}_I)) \geq r$ and

$$d_r \leq |I| = \mathrm{wt_R}(\Delta(\mathcal{L}_I)) \leq \mathrm{wt_R}(\mathcal{V}_\mathcal{L}) = \dim(\mathcal{L}) = d'_r.$$

$d_r \geq d'_r$: Take a subset $I \subseteq \{1, 2, \ldots, n\}$ such that $|I| = d_r$ and $\dim((\mathcal{C}_1 \cap \mathcal{L}_I)/(\mathcal{C}_2 \cap \mathcal{L}_I)) \geq r$. Now it holds that $\Delta(\mathcal{L}_I) = \mathcal{V}_{\mathcal{L}_I} \cap \Delta(\mathbb{F}^n)$. Therefore $\dim((\Delta(\mathcal{C}_1) \cap \mathcal{V}_{\mathcal{L}_I})/(\Delta(\mathcal{C}_2) \cap \mathcal{V}_{\mathcal{L}_I})) \geq r$ and

$$d'_r \leq \dim(\mathcal{L}_I) = |I| = d_r.$$

□

C. Relation With Delsarte Generalized Weights

A notion of generalized weights, called Delsarte generalized weights (DGWs), for a linear code, which in this section means $\mathcal{C}_1 = \mathcal{C}$ arbitrary and $\mathcal{C}_2 = \{0\}$ has already been proposed in [34] as an algebraic invariant of the code. We will prove that GMWs are strictly larger than DGWs when $m = n$, and we will prove that both coincide in the other cases.

These weights are defined in terms of optimal anticodes for the rank metric:

Definition 58 (Maximum Rank Distance): For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$, we define its maximum rank distance as

$$\mathrm{MaxRk}(\mathcal{C}) = \max\{\mathrm{Rk(C)} \mid C \in \mathcal{C}, C \neq 0\}.$$

The following bound is given in [35, Proposition 47]:

$$\dim(\mathcal{C}) \leq m\mathrm{MaxRk}(\mathcal{C}). \tag{16}$$

This leads to the definition of rank-metric optimal anticodes:

Definition 59 (Optimal Anticodes [34, Definition 22]): We say that a linear code $\mathcal{V} \subseteq \mathbb{F}^{m\times n}$ is a (rank-metric) optimal anticode if equality in (16) holds.

We will denote by $A(\mathbb{F}^{m\times n})$ the family of linear optimal anticodes in $\mathbb{F}^{m\times n}$.

In view of this, DGWs are defined in [34] as follows:

Definition 60 (Delsarte Generalized Weights [34, Definition 23]): For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ and an integer $1 \leq r \leq \dim(\mathcal{C})$, we define its r-th Delsarte generalized weight (DGW) as

$$d_{D,r}(\mathcal{C}) = m^{-1}\min\{\dim(\mathcal{V}) \mid \mathcal{V} \in A(\mathbb{F}^{m\times n}), \dim(\mathcal{C} \cap \mathcal{V}) \geq r\}.$$

Observe that $d_{D,r}(\mathcal{C})$ is an integer since the dimension of optimal anticodes is a multiple of m by definition.

Before giving the main result, we need the following proposition:

Proposition 61: If a set $\mathcal{V} \subseteq \mathbb{F}^{m\times n}$ is a rank support space, then it is a (rank-metric) optimal anticode. In other words, $RS(\mathbb{F}^{m\times n}) \subseteq A(\mathbb{F}^{m\times n})$. The reversed inclusion also holds if $m \neq n$.

Proof: We first prove that $RS(\mathbb{F}^{m\times n}) \subseteq A(\mathbb{F}^{m\times n})$. Let $\mathcal{V} \in RS(\mathbb{F}^{m\times n})$ and let $B_{i,j}$, $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, k$, be a basis of $\mathcal{V}$ as in Proposition 9, item 2. For any $V = \sum_{i=1}^m \sum_{j=1}^k \lambda_{i,j} B_{i,j} \in \mathcal{V}$, with $\lambda_{i,j} \in \mathbb{F}$, it holds that

$$\mathrm{Rk}(V) \leq \dim(\langle \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\rangle) = k,$$

where $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ are as in Proposition 9, item 2. Therefore $\dim(\mathcal{V}) = mk \geq m\mathrm{MaxRk}(\mathcal{V})$ and $\mathcal{V}$ is an optimal anticode.

We now prove that $A(\mathbb{F}^{m\times n}) \subseteq RS(\mathbb{F}^{m\times n})$ when $m \neq n$. Let $\mathcal{V} \in A(\mathbb{F}^{m\times n})$. By [34, Th. 26], there exist full-rank matrices $A \in \mathbb{F}_q^{m\times m}$ and $B \in \mathbb{F}_q^{n\times n}$ such that $\mathcal{V} = \{ACB \in \mathbb{F}_q^{m\times n} \mid C \in \mathcal{V}_\mathcal{L}\}$, where $\mathcal{L} = \mathbb{F}_q^k \times \{0\}^{n-k}$ for some positive integer k. By Proposition 9, $\mathcal{V}$ is a rank support space and we are done. □

In [34, Th. 18] it is proven that $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is an $\mathbb{F}_{q^m}$-linear Galois closed vector space if, and only if, it is an $\mathbb{F}_{q^m}$-linear vector space satisfying equality in (16). Hence due to Lemma 52, the previous proposition strengthens [34, Th. 18] when $m \neq n$ by showing that the $\mathbb{F}_{q^m}$-linearity of $\mathcal{V}$ may be weakened to $\mathbb{F}_q$-linearity. Moreover, our result holds for any field $\mathbb{F} \neq \mathbb{F}_q$.

The main result of this subsection is the next theorem, which follows from the previous proposition and the corresponding definitions:

Theorem 9: For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ and an integer $1 \leq r \leq \dim(\mathcal{C})$, we have that

$$d_{D,r}(\mathcal{C}) \leq d_{M,r}(\mathcal{C}) \quad \text{if } m = n,$$

and

$$d_{D,r}(\mathcal{C}) = d_{M,r}(\mathcal{C}) \quad \text{if } m \neq n.$$

Due to Theorem 1, when considering universal security on linearly coded networks it is desirable to obtain linear codes $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ with large GMWs. Therefore, linear codes with large DGWs serve this purpose, but linear codes with low DGWs may still have large GMWs when $m = n$.

The next example shows that not all linear optimal anticodes are rank support spaces when $m = n$, that is, $RS(\mathbb{F}^{n\times n}) \subsetneq A(\mathbb{F}^{n\times n})$, for any n and any field $\mathbb{F}$. As a consequence, in some cases GMWs are strictly larger than DGWs. To that end, we will use the characterization of rank support spaces as matrix modules from Appendix D.

Example 62: Consider $m = n = 2$ and the linear code

$$\mathcal{C} = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\rangle \subseteq \mathbb{F}^{2\times 2}.$$

It holds that $\dim(\mathcal{C}) = 2$, $m = 2$ and $\mathrm{MaxRk}(\mathcal{C}) = 1$. Therefore $\mathcal{C}$ is an optimal anticode. However, it is not a matrix module, and therefore it is not a rank support space

(see Appendix D), since

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \notin \mathcal{C}.$$

In other words, $RS(\mathbb{F}^{2\times 2}) \subsetneq A(\mathbb{F}^{2\times 2})$.

On the one hand, we have that $d_{D,1}(\mathcal{C}) = d_{D,2}(\mathcal{C}) = 1$, by [34, Corollary 32], or just by inspection.

On the other hand, it is easy to check that $d_{M,1}(\mathcal{C}) = 1$, and since $\mathrm{RSupp}(\mathcal{C}) = \mathbb{F}^2$, it holds that $d_{M,2}(\mathcal{C}) = 2$. Therefore $d_{M,2}(\mathcal{C}) > d_{D,2}(\mathcal{C})$.

Observe that we may trivially extend this example to any value of $m = n$, and it holds for an arbitrary field $\mathbb{F}$.

IX. Conclusion and Open Problems

In this work, we have extended the study of universal security provided by $\mathbb{F}_{q^m}$-linear nested coset coding schemes from [24], [39] to that provided by $\mathbb{F}_q$-linear schemes, where $\mathbb{F}_q$ is the field used on the network and m is the packet length.

Thanks to this study, we have completed the list of parameters ℓ, t, m and n for which we can obtain optimal universal secure $\mathbb{F}_q$-linear codes for noiseless networks from [39], and we have added *near optimal* universal security to the rank list-decodable codes from [20], providing the first universal secure linear coset coding schemes able to list-decode in polynomial time roughly twice the rank errors that optimal universal secure schemes can unique-decode, with almost the same secret message size ℓ and security parameter t.

Motivated by our study, we defined a family of security equivalences between linear coset coding schemes and gave mathematical characterizations of such equivalences, which allowed us to obtain, in terms of the last generalized matrix weight, ranges of parameters m and n of networks on which a linear code can be applied with the same security performance.

Finally, we give the following list of open problems:

1) Obtain optimal universal secure and error-correcting linear coset coding schemes for noisy networks for all possible parameters ℓ, t, m, n, and number of rank errors.

2) Extend the concept of universal *strong security* from [24, Definition 6] to general $\mathbb{F}_q$-linear coset coding schemes, and provide optimal universal strong secure schemes as those in [24, Sec. V] for all possible parameters ℓ, t, m and n, for either noiseless or noisy networks.

3) Subsection V-C implies that ℓ is close to but smaller than $n-t-e$, where e is the number of list-decodable rank errors with polynomial list sizes L. We conjecture, but leave as open problem, that a bound similar to $\ell \leq n-t-e$ holds in general.

4) Study the sharpness of the bounds given in Theorem 6.

Appendix A
Duality Theory

In this appendix, we collect technical results concerning trace duality of linear codes in $\mathbb{F}^{m\times n}$ used throughout the paper. Some of the results are taken or expanded from the literature, and some are new. Recall first the definition of trace product and dual of a linear code in $\mathbb{F}^{m\times n}$ (Definition 15).

First, since the trace product in $\mathbb{F}^{m\times n}$ coincides with the usual inner product in $\mathbb{F}^{mn}$, it holds that

$$\begin{aligned} \dim(\mathcal{C}^\perp) &= mn - \dim(\mathcal{C}), \quad \mathcal{C} \subseteq \mathcal{D} \Longleftrightarrow \mathcal{D}^\perp \subseteq \mathcal{C}^\perp, \\ \mathcal{C}^{\perp\perp} &= \mathcal{C}, \quad (\mathcal{C}+\mathcal{D})^\perp = \mathcal{C}^\perp \cap \mathcal{D}^\perp, \\ (\mathcal{C}\cap\mathcal{D})^\perp &= \mathcal{C}^\perp + \mathcal{D}^\perp, \end{aligned}$$

for linear codes $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}^{m\times n}$. We have the following:

Lemma 63 [35, Lemma 27]: If $\mathcal{V} \in RS(\mathbb{F}^{m\times n})$, then $\mathcal{V}^\perp \in RS(\mathbb{F}^{m\times n})$. More concretely, for any subspace $\mathcal{L} \subseteq \mathbb{F}^n$, it holds that

$$(\mathcal{V}_\mathcal{L})^\perp = \mathcal{V}_{(\mathcal{L}^\perp)}.$$

Lemma 64 (Forney's Duality [16]): Given vector spaces $\mathcal{C}, \mathcal{V} \subseteq \mathbb{F}^{m\times n}$, it holds that

$$\dim(\mathcal{V}) - \dim((\mathcal{C}^\perp)\cap\mathcal{V}) = \dim(\mathcal{C}) - \dim(\mathcal{C}\cap(\mathcal{V}^\perp)).$$

We now show that all GMWs of a linear code determine uniquely those of the corresponding dual code. Since GMWs and DGWs [34] coincide when $\mathbb{F} = \mathbb{F}_q$ and $m \neq n$ by Theorem 9, the next result coincides with [34, Corollary 38] in such cases:

Proposition 65: Given a linear code $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ with $k = \dim(\mathcal{C})$, and given an integer $p \in \mathbb{Z}$, define

$$\begin{aligned} W_p(\mathcal{C}) &= \{d_{M,p+rm}(\mathcal{C}) \mid r \in \mathbb{Z}, 1 \leq p+rm \leq k\}, \\ \overline{W}_p(\mathcal{C}) &= \{n+1-d_{M,p+rm}(\mathcal{C}) \mid r \in \mathbb{Z}, 1 \leq p+rm \leq k\}. \end{aligned}$$

Then it holds that

$$\{1, 2, \ldots, n\} = W_p(\mathcal{C}^\perp) \cup \overline{W}_{p+k}(\mathcal{C}),$$

where the union is disjoint.

The proof of this proposition can be translated word by word from the proof of [34, Corollary 38] using the monotonicity properties from Proposition 43. However, [34, Corollary 38] relies on [34, Th. 37], and therefore we need to extend such result to the cases $\mathbb{F} \neq \mathbb{F}_q$ or $m = n$. The following lemma constitutes such extension:

Lemma 66: Given a linear code $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ with $k = \dim(\mathcal{C})$, and given $1 \leq r \leq k$ and $1 \leq s \leq mn-k$, it holds that

$$d_{M,s}(\mathcal{C}^\perp) \neq n+1-d_{M,r}(\mathcal{C})$$

if $r = p+k+r'm$ and $s = p+s'm$, for some integers $p, r', s' \in \mathbb{Z}$.

Proof: Assume that equality holds for a pair of such r and s. Denote $\mathcal{C}_\mathcal{L} = \mathcal{C}\cap\mathcal{V}_\mathcal{L}$, for a linear subspace $\mathcal{L} \subseteq \mathbb{F}^n$, and rewrite Proposition 14 as follows:

$$d_{M,r}(\mathcal{C}) = \min\{\mu \mid \max\{\dim(\mathcal{C}_\mathcal{L}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) = \mu\} \geq r\}. \quad (17)$$

Write $d_{M,r}(\mathcal{C}) = \mu$. Then Equation (17) implies that

$$\max\{\dim(\mathcal{C}_\mathcal{L}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) = \mu\} \geq r, \quad (18)$$

and μ is the minimum integer with such property. Now write $d_{M,s}(\mathcal{C}^\perp) = \nu = n+1-\mu$. In the same way, Equation (17) implies that

$$\max\{\dim((\mathcal{C}^\perp)_\mathcal{L}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) = \nu\} \geq s.$$

On the other hand, given a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ with $\dim(\mathcal{L}) = \nu$, we have that

$$\dim(\mathcal{C}_{\mathcal{L}^\perp}) = \dim(\mathcal{C} \cap (\mathcal{V}_{\mathcal{L}})^\perp) = k - m\nu + \dim((\mathcal{C}^\perp)_{\mathcal{L}}),$$

where the first equality follows from Lemma 63, and the second equality follows from Lemma 64 and Equation (2). Therefore, it holds that

$$\max\{\dim(\mathcal{C}_{\mathcal{L}}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \quad \dim(\mathcal{L}) = \mu - 1\} \geq k - m\nu + s = k - mn - m + m\mu + s. \quad (19)$$

From the fact that μ is the minimum integer satisfying Equation (18), and from Equation (19), we conclude that

$$k - mn - m + m\mu + s < r.$$

Now if we interchange the roles of $\mathcal{C}$ and $\mathcal{C}^\perp$, and the roles of r and s, then we automatically interchange the roles of μ and $n + 1 - \mu$, and the roles of k and $mn - k$. Therefore, we may also conclude that

$$k - mn + m\mu + s > r.$$

Using the expressions $r = p + k + r'm$ and $s = p + s'm$, and dividing everything by m, the previous two inequalities are, respectively

$$s' - n - 1 + \mu < r', \quad \text{and } s' - n + \mu > r',$$

which contradict each other. Hence the lemma follows. □

Observe that the duality theorem for GRWs [12] is a direct consequence of Theorem 7 and Proposition 65:

Corollary 67 [12]: Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k over $\mathbb{F}_{q^m}$, denote $d_r = d_{R,r}(\mathcal{C})$ and $d_s^\perp = d_{R,s}(\mathcal{C}^\perp)$, for $1 \leq r \leq k$ and $1 \leq s \leq n - k$. Then

$$\{1, 2, \ldots, n\} = \{d_1, d_2, \ldots, d_k\} \cup \{n + 1 - d_1^\perp, n+1-d_2^\perp, \ldots, n + 1 - d_{n-k}^\perp\},$$

where the union is disjoint.

Finally, we show that the duality theorem for GHWs [42] is a consequence of Theorem 8 and Proposition 65:

Corollary 68 [42]: Given a linear code $\mathcal{C} \subseteq \mathbb{F}^n$ of dimension k, denote $d_r = d_{H,r}(\mathcal{C})$ and $d_s^\perp = d_{H,s}(\mathcal{C}^\perp)$, for $1 \leq r \leq k$ and $1 \leq s \leq n - k$. Then

$$\{1, 2, \ldots, n\} = \{d_1, d_2, \ldots, d_k\} \cup \{n + 1 - d_1^\perp, n + 1 - d_2^\perp, \ldots, n + 1 - d_{n-k}^\perp\},$$

where the union is disjoint.

Proof: We will use the notation in Proposition 65 during the whole proof. First of all, by Theorem 8 it holds that $W_p(\Delta(\mathcal{C})) = \{d_{H,p}(\mathcal{C})\}$ if $1 \leq p \bmod n \leq k$ and $W_p(\Delta(\mathcal{C})) = \emptyset$ if $k + 1 \leq p \bmod n \leq n - 1$ or $p \bmod n = 0$. Therefore

$$\bigcup_{p=1}^{n} W_{p-k}(\Delta(\mathcal{C})) = \{d_1, d_2, \ldots, d_k\}.$$

On the other hand, from Proposition 65 it follows that

$$\left(\bigcup_{p=1}^{n} W_{p-k}(\Delta(\mathcal{C}))\right) \cup \left(\bigcap_{p=1}^{n} \overline{W}_p(\Delta(\mathcal{C})^\perp)\right) = \{1, 2, \ldots, n\},$$

where the union is disjoint. Hence we only need to show that $n + 1 - d_s^\perp \in \overline{W}_p(\Delta(\mathcal{C})^\perp)$, for $p = 1, 2, \ldots, n$ and $s = 1, 2, \ldots, n - k$.

Denote by $\mathcal{D}_n \subseteq \mathbb{F}^{n\times n}$ the vector space of matrices with zero components in their diagonals. It holds that $\Delta(\mathcal{C})^\perp = \Delta(\mathcal{C}^\perp) \oplus \mathcal{D}_n$.

Fix $1 \leq s \leq n-k$ and denote $d = d_{H,s}(\mathcal{C}^\perp)$. First, consider a subspace $\mathcal{D} \subseteq \mathcal{C}^\perp$ with $\mathrm{wt_H}(\mathcal{D}) = d$ and $\dim(\mathcal{D}) = s$, and define $\mathcal{D}' \subseteq \Delta(\mathcal{C})^\perp$ as the direct sum of $\Delta(\mathcal{D})$ and all matrices in $\mathcal{D}_n$ with columns in the Hamming support of $\mathcal{D}$. Since $\dim(\mathcal{D}') = d(n-1)+s$ and $\mathrm{wt_R}(\mathcal{D}') = d$, by Proposition 12 it follows that

$$d_{M,d(n-1)+s}(\Delta(\mathcal{C})^\perp) \leq d. \quad (20)$$

On the other hand, assume that $d_{M,(d-1)(n-1)+s}(\Delta(\mathcal{C})^\perp) = d' < d$. Let $\mathcal{E} \subseteq \Delta(\mathcal{C})^\perp$ be such that $\mathrm{wt_R}(\mathcal{E}) = d'$ and $\dim(\mathcal{E}) = (d-1)(n-1) + s$. Denote by $\mathcal{E}_D$ the vector space of matrices obtained by replacing the elements outside the diagonal of those matrices in $\mathcal{E}$ by zero. If $\mathcal{L} = \mathrm{RSupp}(\mathcal{E}) \subseteq \mathbb{F}^n$, we claim that

$$\dim(\mathcal{E} \cap \mathcal{D}_n) \leq n\mathrm{wt_R}(\mathcal{E}) - \mathrm{wt_H}(\mathcal{L}). \quad (21)$$

It is sufficient to show that $\dim(\mathcal{V}_{\mathcal{L}} \cap \mathcal{D}_n) = n\dim(\mathcal{L}) - \mathrm{wt_H}(\mathcal{L})$. Denote by $\mathcal{V}_{\mathcal{L}D}$ the vector space of matrices obtained by replacing the elements outside the diagonal of those matrices in $\mathcal{V}_{\mathcal{L}}$ by zero. Then, by Proposition 9, $\dim(\mathcal{V}_{\mathcal{L}D}) = \mathrm{wt_H}(\mathcal{L})$, and $\dim(\mathcal{V}_{\mathcal{L}} \cap \mathcal{D}_n) = \dim(\mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{V}_{\mathcal{L}D}) = n\dim(\mathcal{L}) - \mathrm{wt_H}(\mathcal{L})$.

By monotonicity (Proposition 43), we have that $d' = d - 1$, and thus $\dim(\mathcal{E}) = d'(n-1) + s$. Therefore, by (21), $\dim(\Delta^{-1}(\mathcal{E}_D)) = \dim(\mathcal{E}_D) = \dim(\mathcal{E}) - \dim(\mathcal{E} \cap \mathcal{D}_n) \geq s + \mathrm{wt_H}(\mathcal{L}) - d'$. Choose indices $i_1, i_2, \ldots, i_{\mathrm{wt_H}(\mathcal{L})-d'}$ from $\mathrm{HSupp}(\Delta^{-1}(\mathcal{E}_D))$, and define

$$\mathcal{W} = \{\mathbf{c} \in \Delta^{-1}(\mathcal{E}_D) \mid c_{i_j} = 0, 1 \leq j \leq \mathrm{wt_H}(\mathcal{L}) - d'\}.$$

Then $\mathcal{W} \subseteq \mathcal{C}^\perp$, $\dim(\mathcal{W}) \geq s$, and $\mathrm{wt_H}(\mathcal{W}) \leq \mathrm{wt_H}(\Delta^{-1}(\mathcal{E}_D)) - \mathrm{wt_H}(\mathcal{L}) + d' \leq d'$, which implies $d_{H,s}(\mathcal{C}^\perp) = d' < d$, which is a contradiction. Hence

$$d_{M,(d-1)(n-1)+s}(\Delta(\mathcal{C})^\perp) \geq d. \quad (22)$$

Combining Equation (20) and Equation (22), we conclude that

$$d_{M,(d-1)(n-1)+s+j}(\Delta(\mathcal{C})^\perp) = d,$$

for $j = 0, 1, 2, \ldots, n-1$, which implies that $n + 1 - d_s^\perp \in \overline{W}_p(\Delta(\mathcal{C})^\perp)$, for $p = 1, 2, \ldots, n$, and we are done. □

Appendix B
Construction of Explicit Subspace Designs

In this appendix, we recall how to construct the subspace design formed by $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2, \ldots \subseteq \mathbb{F}_{q^m}$ in Section V. This construction is given in [20], based on a construction in [19], and is explicit in the sense that it can be constructed using an algorithm of polynomial complexity on q.

Fix $\varepsilon > 0$ and a positive integer s such that $4sn \leq \varepsilon m$, and assume that n divides m. Let $d_1 = q^{m/n-1}$,

$d_2 = q^{m/n-2}, \ldots, d_{m/n} = 1$ and let $\gamma_1, \gamma_2, \ldots, \gamma_{m/n}$ be distinct non-zero elements of $\mathbb{F}_{q^n}$. Define

$$f_i(x_1, x_2 \ldots, x_{m/n}) = \sum_{j=1}^{m/n} \gamma_j^i x_j^{d_j},$$

for $i = 1, 2, \ldots, s$, and let $\mathcal{S} \subseteq \mathbb{F}_{q^n}^{m/n}$ be the set of common zeros of $f_1, f_2, \ldots, f_s$, which is an $\mathbb{F}_q$-linear vector space. We may assume that $\mathcal{S} \subseteq \mathbb{F}_{q^m}$ by an $\mathbb{F}_{q^n}$-linear vector space isomorphism $\mathbb{F}_{q^n}^{m/n} \cong \mathbb{F}_{q^m}$ (any isomorphism works).

Let β be a primitive element of $\mathbb{F}_{q^n}$. For $\alpha \in \mathbb{F}_{q^{n\lfloor \frac{\varepsilon m}{2ns} \rfloor}}$, let

$$\mathcal{S}_\alpha = \left\{ \alpha^{q^j} \beta^i \mid 0 \le j < \left\lfloor \frac{\varepsilon m}{2ns} \right\rfloor, 0 \le i < 2s \right\}.$$

The algorithm in [19, Sec. 4.3] gives in polynomial time over q a set $\mathcal{F} \subseteq \mathbb{F}_{q^{n\lfloor \frac{\varepsilon m}{2ns} \rfloor}}$ of size $q^{\Omega(\frac{\varepsilon m}{ns})}$ such that:

1) $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^{n\lfloor \frac{\varepsilon m}{2ns} \rfloor}}$, for all $\alpha \in \mathcal{F}$,
2) $\mathcal{S}_\alpha \cap \mathcal{S}_\beta = \emptyset$, for all distinct $\alpha, \beta \in \mathcal{F}$, and
3) $|\mathcal{S}_\alpha| = 2s\lfloor \frac{\varepsilon m}{2ns} \rfloor$, for all $\alpha \in \mathcal{F}$.

Define the $\mathbb{F}_{q^n}$-linear vector space $\mathcal{V}_\alpha \subseteq \mathbb{F}_{q^n}^{m/n}$ as

$$\mathcal{V}_\alpha = \{(a_0, a_1, \ldots, a_{m/n-1}) \in \mathbb{F}_{q^n}^{m/n} \mid \sum_{i=0}^{m/n-1} a_i (\alpha\beta^j)^i = 0 \mid 0 \le j < 2s\},$$

for every $\alpha \in \mathcal{F}$, where we may consider $\mathcal{V}_\alpha \subseteq \mathbb{F}_{q^m}$ as before.

Finally, the $\mathbb{F}_q$-linear vector spaces $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2, \ldots \subseteq \mathbb{F}_{q^m}$ in Section V are defined as $\mathcal{H}_i = \mathcal{S} \cap \mathcal{V}_{\alpha_i}$, for distinct $\alpha_i \in \mathcal{F}$.

The constructions of $\mathcal{F}$ and $\mathcal{V}_\alpha$ appeared first in [19, Sec. 4.2] and $\mathcal{S}$ appeared first in [20, Corollary 6].

We conclude the appendix by computing the dimensions of the vector spaces $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2, \ldots \subseteq \mathbb{F}_{q^m}$, which is done in the proof of [20, Th. 8]:

Lemma 69 [20]: The vector spaces $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2, \ldots \subseteq \mathbb{F}_{q^m}$ have dimension at least $m(1 - 2\varepsilon)$ over $\mathbb{F}_q$.

Appendix C
Proof of Theorem 4

In this appendix, we give the proof of Theorem 4, which we now recall:

Theorem 4: Let $\phi : \mathcal{V} \longrightarrow \mathcal{W}$ be a vector space isomorphism between rank support spaces $\mathcal{V} \in RS(\mathbb{F}^{m\times n})$ and $\mathcal{W} \in RS(\mathbb{F}^{m\times n'})$, and consider the following properties:

- (P 1) *There exist full-rank matrices $A \in \mathbb{F}^{m\times m}$ and $B \in \mathbb{F}^{n\times n'}$ such that $\phi(C) = ACB$, for all $C \in \mathcal{V}$.*
- (P 2) *A subspace $\mathcal{U} \subseteq \mathcal{V}$ is a rank support space if, and only if, $\phi(\mathcal{U})$ is a rank support space.*
- (P 3) *For all subspaces $\mathcal{D} \subseteq \mathcal{V}$, it holds that $\mathrm{wt_R}(\phi(\mathcal{D})) = \mathrm{wt_R}(\mathcal{D})$.*
- (P 4) *ϕ is a rank isometry.*

Then the following implications hold:

$$(P\ 1) \Longleftrightarrow (P\ 2) \Longleftrightarrow (P\ 3) \Longrightarrow (P\ 4).$$

In particular, a security equivalence is a rank isometry and, in the case $\mathcal{V} = \mathcal{W} = \mathbb{F}^{m\times n}$ and $m \neq n$, the reversed implication holds by Proposition 32.

Proof: First we prove (P 1) $\Longrightarrow$ (P 2): It follows immediately from the characterization of rank support spaces in Proposition 9, item 3.

Now we prove (P 2) $\Longrightarrow$ (P 3): Let $\mathcal{L} = \mathrm{RSupp}(\mathcal{D}) \subseteq \mathbb{F}^n$ and $\mathcal{L}' = \mathrm{RSupp}(\phi(\mathcal{D})) \subseteq \mathbb{F}^{n'}$. It holds that $\mathcal{V}_\mathcal{L} \subseteq \mathcal{V}$ and $\mathcal{V}_{\mathcal{L}'} \subseteq \mathcal{W}$, and they are the smallest rank support spaces in $\mathcal{V}$ and $\mathcal{W}$ containing $\mathcal{D}$ and $\phi(\mathcal{D})$, respectively, by Lemma 8. Since ϕ preserves rank support spaces and their inclusions, we conclude that $\phi(\mathcal{V}_\mathcal{L}) = \mathcal{V}_{\mathcal{L}'}$, which implies that $\dim(\mathcal{L}) = \dim(\mathcal{L}')$ by (2), and (P 3) follows.

Next we prove (P 2) $\Longleftarrow$ (P 3): Assume that $\mathcal{U} \subseteq \mathcal{V}$ is a rank support space. This means that $m\mathrm{wt_R}(\mathcal{U}) = \dim(\mathcal{U})$ by (2). Since ϕ satisfies (P 3) and is a vector space isomorphism, we conclude that $m\mathrm{wt_R}(\phi(\mathcal{U})) = \dim(\phi(\mathcal{U}))$, and thus $\phi(\mathcal{U})$ is a rank support space also by (2). Similarly we may prove that, if $\phi(\mathcal{U})$ is a rank support space, then $\mathcal{U}$ is a rank support space.

Now we prove (P 3) $\Longrightarrow$ (P 4): Trivial from the fact that $\mathrm{wt_R}(\langle\{C\}\rangle) = \mathrm{Rk}(C)$, for all $C \in \mathcal{V}$.

Finally we prove (P 1) $\Longleftarrow$ (P 2): Denote $\dim(\mathcal{V}) = \dim(\mathcal{W}) = mk$ and consider bases of $\mathcal{V}$ and $\mathcal{W}$ as in Proposition 9, item 2. By defining vector space isomorphisms $\mathbb{F}^{m\times k} \longrightarrow \mathcal{V}$ and $\mathcal{W} \longrightarrow \mathbb{F}^{m\times k}$, sending such bases to the canonical basis of $\mathbb{F}^{m\times k}$, we see that we only need to prove the result for the particular case $\mathcal{V} = \mathcal{W} = \mathbb{F}^{m\times n}$.

Denote by $E_{i,j} \in \mathbb{F}^{m\times n}$ the matrices in the canonical basis, for $1 \le i \le m$, $1 \le j \le n$, that is, $E_{i,j}$ has 1 in its (i, j)-th component, and zeroes in its other components.

Consider the rank support space $\mathcal{U}_j = \langle E_{1,j}, E_{2,j}, \ldots, E_{m,j}\rangle \subseteq \mathbb{F}^{m\times n}$, for $1 \le j \le n$. Since $\phi(\mathcal{U}_j)$ is a rank support space, it has a basis $B_{i,j}$, $i = 1, 2, \ldots, m$, as in Proposition 9, item 2, for a vector $\mathbf{b}_j \in \mathbb{F}^n$. This means that

$$\phi(E_{i,j}) = \sum_{s=1}^{m} a_{s,i}^{(j)} B_{s,j},$$

for some $a_{s,i}^{(j)} \in \mathbb{F}$, for all $s, i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. If we define the matrix $A^{(j)} \in \mathbb{F}^{m\times m}$ whose (s, i)-th component is $a_{s,i}^{(j)}$, and $B \in \mathbb{F}^{n\times n}$ whose j-th row is $\mathbf{b}_j$, then a simple calculation shows that

$$\phi(E_{i,j}) = A^{(j)} E_{i,j} B,$$

and the matrices $A^{(j)}$ and B are invertible. If we prove that there exist non-zero $\lambda_j \in \mathbb{F}$ with $A^{(j)} = \lambda_j A^{(1)}$, for $j = 2, 3, \ldots, n$, then we are done, since we can take the vectors $\lambda_j \mathbf{b}_j$ instead of $\mathbf{b}_j$, define $A = A^{(1)}$, and then it holds that

$$\phi(E_{i,j}) = A E_{i,j} B,$$

for all $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$, implying (P 1).

To this end, we first denote by $\mathbf{a}_i^{(j)} \in \mathbb{F}^m$ the i-th column in $A^{(j)}$ (written as a row vector). Observe that we have already proven that ϕ preserves ranks. Hence $\mathrm{Rk}(\phi(E_{i,j} + E_{i,1})) = 1$, which means that $\mathrm{Rk}(A^{(j)} E_{i,j} + A^{(1)} E_{i,1}) = 1$, which implies that there exist $\lambda_{i,j} \in \mathbb{F}$ with

$$\mathbf{a}_i^{(j)} = \lambda_{i,j} \mathbf{a}_i^{(1)}.$$

On the other hand, a matrix calculation shows that

$$\phi\left(\sum_{i=1}^{m}\sum_{j=1}^{n}E_{i,j}\right) = \left(\sum_{i=1}^{m}\mathbf{a}_i^{(1)}, \sum_{i=1}^{m}\mathbf{a}_i^{(2)}, \ldots, \sum_{i=1}^{m}\mathbf{a}_i^{(n)}\right)B = \left(\sum_{i=1}^{m}\mathbf{a}_i^{(1)}, \sum_{i=1}^{m}\lambda_{i,2}\mathbf{a}_i^{(1)}, \ldots, \sum_{i=1}^{m}\lambda_{i,n}\mathbf{a}_i^{(1)}\right)B.$$

Since $\mathrm{Rk}(\sum_{i=1}^{m}\sum_{j=1}^{n}E_{i,j}) = 1$ and the vectors $\mathbf{a}_i^{(1)}$, $1 \leq i \leq m$, are linearly independent, we conclude that $\lambda_{i,j}$ depends only on j and not on i, and we are done. □

Appendix D
Matrix Modules

Rank support spaces can also be seen as left submodules of the left module $\mathbb{F}^{m\times n}$ over the (non-commutative) ring $\mathbb{F}^{m\times m}$. This has been used in Example 62. Since we think this result is of interest by itself, we include the characterization in this appendix.

Definition 70 (Matrix Modules): We say that a set $\mathcal{V} \subseteq \mathbb{F}^{m\times n}$ is a matrix module if

1) $V + W \in \mathcal{V}$, for every $V, W \in \mathcal{V}$, and
2) $MV \in \mathcal{V}$, for every $M \in \mathbb{F}^{m\times m}$ and every $V \in \mathcal{V}$.

Proposition 71: A set $\mathcal{V} \subseteq \mathbb{F}^{m\times n}$ is a rank support space if, and only if, it is a matrix module.

Proof: Assume that $\mathcal{V}$ is a rank support space. Using the characterization in Proposition 9, item 3, it is trivial to see that $\mathcal{V}$ is a matrix module.

Assume now that $\mathcal{V}$ is a matrix module. It holds that $\mathcal{V}$ is a vector space. Let $\mathcal{L} = \mathrm{RSupp}(\mathcal{V})$, and take $\mathbf{v} \in \mathcal{L}$. There exist $V_1, V_2, \ldots, V_s \in \mathcal{V}$ and $\mathbf{v}_j \in \mathrm{Row}(V_j)$, for $j = 1, 2, \ldots, s$, such that $\mathbf{v} = \sum_{j=1}^{s}\mathbf{v}_j$.

For fixed $1 \leq i \leq m$ and $1 \leq j \leq s$, it is well-known that there exists $M_{i,j} \in \mathbb{F}^{m\times m}$ such that $M_{i,j}V_j$ has $\mathbf{v}_j$ as its i-th row and the rest of its rows are zero vectors. Since $\mathcal{V}$ is closed under sums of matrices, we conclude that $\mathcal{V}_{\mathcal{L}} \subseteq \mathcal{V}$ and therefore both are equal. □

Acknowledgment

The authors wish to thank Alberto Ravagnani for clarifying the relation between GMWs and DGWs. The first author is also thankful for the support and guidance of his advisors Olav Geil and Diego Ruano. At the time of submission, the first author was visiting the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto. He greatly appreciates the support and hospitality of Frank R. Kschischang. Finally, the authors also wish to thank the editor and anonymous reviewers for their very helpful comments.

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] D. Augot, P. Loidreau, and G. Robert, "Rank metric and Gabidulin codes in characteristic zero," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 509–513.

[3] T. P. Berger, "Isometries for rank distance and permutation group of Gabidulin codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3016–3019, Nov. 2003.

[4] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manag. Requirements Knowl.*, 1979, pp. 313–316.

[5] N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc. IEEE Inform. Theory Workshop*, Oct. 2002, pp. 119–122.

[6] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2002, p. 323.

[7] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 4515. Berlin, Germany: Springer, 2007, pp. 291–310.

[8] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY, USA: Wiley, 2006.

[9] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *J. Combinat. Theory A*, vol. 25, no. 3, pp. 226–241, 1978.

[10] J. Dieudonné, "Sur une généralisation du groupe orthogonal á quatre variables," *Archiv Math.*, vol. 1, no. 4, pp. 282–287, 1948.

[11] Y. Ding, "On list-decodability of random rank metric codes and subspace codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 51–59, Jan. 2015.

[12] J. Ducoat, "Generalized rank weights: A duality statement," in *Topics in Finite Fields* (Contemporary Mathematics), vol. 632, G. M. Kyureghyan and A. Pott, Eds. Providence, RI, USA: AMS, 2015, pp. 114–123.

[13] I. M. Duursma and S. Park, "Coset bounds for algebraic geometric codes," *Finite Fields Appl.*, vol. 16, no. 1, pp. 36–55, 2010.

[14] S. El Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type II," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1361–1371, Mar. 2012.

[15] J. Feldman, T. Malkin, R. A. Servedio, and C. Stein, "On the capacity of secure network coding," in *Proc. 42nd Annu. Allerton Conf. Commun., Control, Comput.*, 2004, pp. 63–68.

[16] G. D. Forney, Jr., "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 1741–1752, Nov. 1994.

[17] È. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems Inf. Transmiss.*, vol. 21, no. 1, pp. 1–12, 1985.

[18] M. Giorgetti and A. Previtali, "Galois invariance, trace codes and subfield subcodes," *Finite Fields Appl.*, vol. 16, no. 2, pp. 96–99, 2010.

[19] V. Guruswami and S. Kopparty, "Explicit subspace designs," *Combinatorica*, vol. 36, no. 2, pp. 161–185, Apr. 2016.

[20] V. Guruswami, C. Wang, and C. Xing, "Explicit list-decodable rank-metric and subspace codes via subspace designs," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2707–2718, May 2016.

[21] T. Ho *et al.*, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[22] R. Jurrius and R. Pellikaan, "On defining generalized rank weights," *Adv. Math. Commun.*, vol. 11, no. 1, pp. 225–235, 2017.

[23] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[24] J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3912–3936, Jul. 2015.

[25] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[26] Y. Luo, C. Mitrpant, A. J. H. Vinck, and K. Chen, "Some new characters on the wire-tap channel of type II," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1222–1229, Mar. 2005.

[27] M. Marcus and B. N. Moyls, "Linear transformations on algebras of matrices," *Can. J. Math.*, vol. 11, pp. 61–66, Jan. 1959.

[28] U. Martínez-Peñas, "On the similarities between generalized rank and Hamming weights and their applications to network coding," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 4081–4095, Jul. 2016.

[29] U. Martínez-Peñas and R. Matsumoto, "Unifying notions of generalized weights for universal security on wire-tap networks," in *Proc. 54th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2016, pp. 800–807.

[30] K. Morrison, "Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7035–7046, Nov. 2014.

[31] C. K. Ngai, R. W. Yeung, and Z. Zhang, "Network generalized Hamming weight," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1136–1143, Feb. 2011.

[32] F. Oggier and A. Sboui, "On the existence of generalized rank weights," in *Proc. Int. Symp. Inf. Theory Appl.*, Oct. 2012, pp. 406–410.
[33] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 209. Berlin, Germany: Springer, 1985, pp. 33–50.
[34] A. Ravagnani, "Generalized weights: An anticode approach," *J. Pure Appl. Algebra*, vol. 220, no. 5, pp. 1946–1962, 2016.
[35] A. Ravagnani, "Rank-metric codes and their duality theory," *Des., Codes Cryptogr.*, vol. 80, no. 1, pp. 197–216, 2016.
[36] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 328–336, Mar. 1991.
[37] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[38] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5479–5490, Dec. 2009.
[39] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.
[40] D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.
[41] H. Stichtenoth, "On the dimension of subfield subcodes," *IEEE Trans. Inf. Theory*, vol. 36, no. 1, pp. 90–93, Jan. 1990.
[42] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, Sep. 1991.
[43] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[44] R. Zamir, S. Shamai (Shitz), and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun. 2002.
[45] Z. Zhang and B. Zhuang, "An application of the relative network Generalized Hamming weight to erroneous wiretap networks," in *Proc. IEEE Inf. Theory Workshop*, Oct. 2009, pp. 70–74.

Umberto Martínez-Peñas (S'15) was born in Valladolid, Spain, on January 2, 1991. He received the B.E. and M.E. in mathematics from the University of Valladolid, Spain, in 2013 and 2014, respectively. He is currently a Ph.D. student at the Department of Mathematical Sciences, Aalborg University, Denmark. He has been awarded an EliteForsk Rejsestipendium (Elite Research Travel Grant) from the Danish Ministery of Education and Science. His research interests include algebraic coding, network coding and secret sharing.

Ryutaroh Matsumoto (M'00) was born in Nagoya, Japan, on November 29, 1973. He received the B.E. degree in computer science, the M.E. degree in information processing, and the Ph.D. degree in electrical and electronic engineering, all from Tokyo Institute of Technology, Japan, in 1996, 1998 and 2001, respectively. He was an Assistant Professor from 2001 to 2004, and has been an Associate Professor from 2004 to 2017 in the Department of Information and Communications Engineering, Tokyo Institute of Technology. He is now an Associate Professor in the Department of Information and Communication Engineering, Nagoya University, Japan. He also served as a Velux Visiting Professor at the Department of Mathematical Sciences, Aalborg University, Denmark, in 2011 and 2014. His research interests include error-correcting codes, quantum information theory, information theoretic security, and communication theory. Dr. Matsumoto received the Young Engineer Award from IEICE and the Ericsson Young Scientist Award from Ericsson Japan in 2001. He received the Best Paper Awards from IEICE in 2001, 2008, 2011 and 2014.