Generic Error SDP and Generic Error CVE*

Felice Manganiello and Freeman Slaughter

Clemson University, Clemson SC, USA
{manganm,fslaugh}@clemson.edu

Abstract. This paper introduces a new family of CVE schemes built from generic errors (GE-CVE) and identifies a vulnerability therein. To introduce the problem, we generalize the concept of error sets beyond those defined by a metric, and use the set-theoretic difference operator to characterize when these error sets are detectable or correctable by codes. We prove the existence of a general, metric-less form of the Gilbert-Varshamov bound, and show that - like in the Hamming setting - a random code corrects a generic error set with overwhelming probability. We define the generic error SDP (GE-SDP), which is contained in the complexity class of NP-hard problems, and use its hardness to demonstrate the security of GE-CVE. We prove that these schemes are complete, sound, and zero-knowledge. Finally, we identify a vulnerability of the GE-SDP for codes defined over large extension fields and without a very high rate. We show that certain GE-CVE parameters suffer from this vulnerability, notably the restricted CVE scheme.

Keywords: Code-based cryptography · Syndrome Decoding Problem · generic error set · zero-knowledge scheme · CVE.

1 Introduction

Recently, the lack of acceptably secure post-quantum cryptography led to NIST creating a competition of sorts, comparing the pros and cons of proposed algorithms. Code-based cryptography has become an attractive post-quantum candidate over the years, as it is believed to present a computationally difficult problem even against quantum computers [14]. Classic McEliece [3], a code-based KEM has recently passed into Round 4 of the NIST Post-Quantum Standardization Competition and remains the candidate based on the oldest problem in the competition [1].

The CVE protocol is a zero-knowledge identification scheme based on the Syndrome Decoding Problem (SDP) for linear codes, with competitive computation speed and key sizes in practical instances. We focus on two variations: the restricted form of CVE, which takes a different error set than the standard protocol, and rank-CVE, which takes a different metric. This paper focuses on generic error sets and the theory of error correctability and detectability based on the set difference operator contained in [26, 27]. Using this framework, we

* Partially supported by the National Science Foundation under grant DMS-1547399.

generalize the SDP and CVE to general error sets independent of metric, introducing a new, NP-complete SDP based on these arbitrary errors. From this, we can construct a generic error CVE. We characterize the parameters of error sets for which this generic SDP has a polynomial-time decoding algorithm, leading to a vulnerability of generic error CVE for certain error sets. To be clear, we show that CVE based on the restricted SDP is vulnerable when it is defined for certain parameters of codes without a high rate.

The paper is organized as follows. In Section 2, we recall standard coding theory results and present the notation we will use throughout this paper. Section 3 introduces the set difference, an operator from set theory. When this operator repeatedly acts on a set of generic errors, we show that it will stabilize at a subspace. We introduce the notion of detectability and correctability using the set difference, resulting in a more general concept than the standard definition based on balls. These concepts also result in a generalization of the Gilbert-Varshamov Bound that guarantees the existence of a code correcting an arbitrary error set. Finally, we use the results of this section to prove that a random code will correct a general error set with a probability that tends towards one as the code length increases. Section 4 is devoted to complexity. From the Syndrome Decoding Problem (SDP), we define the Generic Error SDP (GE-SDP) and its decisional variant and provide evidence that they are NP-complete problems. For Section 5, we generalize the zero-knowledge Cayrel-Véron-El Yousfi Alaoui (CVE) scheme from [15] to generic errors and prove that it is complete, sound, and zero-knowledge. Paired with the complexity arguments of the previous section, we obtain strict bounds about the probability that an adversary can forge their veracity to a verifier in this generic error setting. Finally, we devote Section 6 to highlighting a vulnerability that results from this generic definition of detectability and correctability. We show that the GE-SDP can be solved in polynomial times under certain conditions. We apply this result to the Restricted Syndrome Decoding Problem (R-SDP) defined in [7] and show that for certain parameter choices, an adversary can correct the errors introduced to obfuscate the plaintext in a polynomial-time decoding algorithm.

2 Preliminaries

We introduce the notation used throughout this paper and recall some standard linear algebra and coding theory results.

Let $\mathbb{F}_q$ denote the finite field with q elements, with $q = p^N$ a prime power and $\mathbb{F}_q^n$ be the set of n-length vectors over $\mathbb{F}_q$. For $E \subseteq \mathbb{F}_q^n$, let E^* be $E \setminus \{0\}$. For a set $E \subseteq \mathbb{F}_q^n$ with k elements, let $\langle E \rangle_{\mathbb{F}_p}$ be the span of E over $\mathbb{F}_p$:

$$\langle E \rangle_{\mathbb{F}_p} = \lambda_1 e_1 + \lambda_2 e_2 + ... + \lambda_k e_k \text{ for } \lambda_i \in \mathbb{F}_p, e_i \in E.$$

Let $\mathfrak{M}_n$ be the set of monomial transformations. A monomial transformation $\tau : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a map that acts on vectors by permuting their entries and scaling them by non-zero multiples. That is, there exists $v \in \mathbb{F}_q^n \setminus \{0\}$ and $\sigma \in S_n$, the

symmetric group, such that

$$\tau(x) = (v_{\sigma(1)}x_{\sigma(1)}, v_{\sigma(2)}x_{\sigma(2)}, ..., v_{\sigma(n)}x_{\sigma(n)}) \text{ for all } x \in \mathbb{F}_q^n.$$

Recall that $GL_n(\mathbb{F}_q)$ is the set of $n \times n$ invertible matrices over the field $\mathbb{F}_q$, which forms a group under standard matrix multiplication. We define the stabilizer of a set $E \subseteq \mathbb{F}_q^n$, denoted $\mathfrak{S}_E$, as the set of invertible matrices that map E into E, meaning $\mathfrak{S}_E = \{M \in GL_n(\mathbb{F}_q) \mid eM \in E \text{ for all } e \in E\}$.

We continue with some basic definitions and results from coding theory, which may be found in [30].

Definition 1. *We say $\mathcal{C}$ is an $[n,k]$-linear code when $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_q$ of dimension k.*

We focus this work on linear codes, and we refer to them simply as codes. We also assume that $\mathcal{C}$ is a code over $\mathbb{F}_q$.

Definition 2. *For an $[n,k]$ code $\mathcal{C}$, a generator matrix $G \in \mathbb{F}_q^{k\times n}$ is a full-rank matrix where the rows are comprised of a basis of $\mathcal{C}$ over $\mathbb{F}_q$. The parity-check matrix of a code $\mathcal{C}$ is a (full-rank) matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ such that $\mathcal{C} = \{x \in \mathbb{F}_q^n \mid xH^t = 0\}$.*

For $x \in \mathbb{F}_q^n$, we define the Hamming weight $\omega(x)$ to be the number of non-zero entries in the vector x. This gives rise to the Hamming distance between two vectors, $d(x,y)$, defined as the weight of their difference $\omega(x-y)$. The Hamming ball with radius r and center x is denoted $B_r(x)$, and is defined as the set of vectors that are distance less than or equal to r from x. While we will not focus on the Hamming metric in this paper, it is used by tradition in certain definitions that we will generalize in future sections.

3 Generic Error Sets

In this section, we generalize the concepts of decodability and correctability with generic error sets beyond any metric. To do that, we need to introduce the concept of set difference.

Definition 3. *For some $E \subseteq \mathbb{F}_q^n$, the set difference of E is $\Delta E = \{e_1 - e_2 \mid e_1, e_2 \in E\}$.*

Since the set E will represent an error set for the purposes of our work, we assume that $0 \in E \subseteq \mathbb{F}_q^n$.

The following examples demonstrate that the cardinality of the set difference depends on if the elements themselves are in an arithmetic progression. This is a result of the Cauchy-Davenport Theorem for restricted sumsets; see [24, Theorem 25] and [25, Theorem 3]. We only use this example to show that the set difference is not immediate from the set itself and that one must inspect every element in the worst case to check for arithmetic progression.

Example 1. Consider $A = \{1, 2, 3\} \subseteq \mathbb{F}_7$, where the elements of A are in an arithmetic progression modulo 7. We can calculate $\Delta A = \{0, 1, 2, 5, 6\}$, thus $|\Delta A| = 2|A| - 1$.

Example 2. On the other hand, the elements of $B = \{1, 2, 4\}$ are not in an arithmetic progression. This time, despite having the same cardinality as A in Example 1, we see that $\Delta B = \{0, 1, 2, 3, 4, 5, 6\}$, with $|\Delta B| > 2|B| - 1$.

We introduce the concept of Δ-closure of a set $E \subseteq \mathbb{F}_q^n$, meaning the smallest set that contains E and all the difference sets originating by it.

Theorem 1. *For a set $E \subseteq \mathbb{F}_q^n$, the chain $E \subseteq \Delta E \subseteq \Delta^2 E \subseteq ...$ stabilizes, meaning that there exists some $k \in \mathbb{N}$ such that $\Delta^k E = \Delta^{k+1} E$. In this case, $\Delta^k E = \langle E \rangle_{\mathbb{F}_p}$.*

Proof. The chain stabilizes because we work with a finite sets.

Let $x \in \Delta^r E$ and $y \in \Delta^s E$ for $r, s \in \mathbb{N}$ with $r \geq s$. Then $-y \in \Delta^{r+1} E$, so $x + y = x - (-y) \in \Delta^{r+2} E$. Now for $x \in \Delta^r E$ and $\alpha \in \mathbb{F}_p$, then $\alpha x \in \Delta^{r+\alpha} E$. From this, we can see that for $x, y \in \Delta^k E = \Delta^{k+1} E$, we have that $x + y \in \Delta^k E$ and $\alpha x \in \Delta^k E$. Thus $\Delta^k E$ is an $\mathbb{F}_p$-subspace, so $\Delta^k E \subseteq \langle E \rangle_{\mathbb{F}_p}$.

On the other hand, for all $x \in \Delta^r E$, we can write $x = x_{r-1} - y_{r-1}$ for $x_{r-1}, y_{r-1} \in \Delta^{r-1} E$, so each element is the difference of two elements one step down on the difference chain. Continuing this, $x = \sum_{n=1}^{|E|} \alpha_n x_n$ for $x_i \in E$ and $\alpha_i \in \mathbb{F}_p$. Thus $\langle E \rangle_{\mathbb{F}_p} \subseteq \Delta^k E$, as every element in $\Delta^k E$ can be decomposed into a linear combination of elements from E.

Definition 4. *For a set $E \subseteq \mathbb{F}_q^n$, the Δ-closure of E is $\overline{E}^{\Delta} = \lim_{k \to \infty} \Delta^k E$. We say that a set $E \subseteq \mathbb{F}_q^n$ is Δ-closed if $E = \overline{E}^{\Delta}$.*

The cardinality of a Δ-closed set is as follows.

Corollary 1. *For a set $E \subseteq \mathbb{F}_q^n$, the $|\overline{E}^{\Delta}| = p^m$ for some $m \in \mathbb{N}$.*

This is a corollary of Theorem 1 where we show that the stabilizing set $\overline{E}^{\Delta}$ is a subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_p$.

Example 3. Since we will work on Δ-closed sets throughout this manuscript, we provide two examples that are going to be used.

- $\overline{B_r(0)}^{\Delta} = \mathbb{F}_q^n$ for any $r > 0$.
- If $E = \{0, 1\}^n \subseteq \mathbb{F}_q^n$, then $\overline{E}^{\Delta} = \mathbb{F}_p^n$.

3.1 Error Detectability and Correctability

When considering communication over a q-ary symmetric channel, errors are additive. More precisely, if $\mathcal{C} \subseteq \mathbb{F}_q^n$ is an $[n, k]$ code of minimum distance d and $c \in \mathcal{C}$ is sent through the channel $c + e$ with $e \in \mathbb{F}_q^n$ is received. Considering a minimum distance decoder, meaning a map that returns the unique closest

codeword to a received vector if it exists, then we can say that an error is detectable if $e \in B_{d-1}(0)$, and (uniquely) correctable if $e \in B_t(0)$ with $t = \lfloor \frac{d-1}{2} \rfloor$. These are well-known results from classical coding theory that can be reviewed in any coding theory textbook such as [30].

With another application in mind, similar definitions have been developed based on the rank distance, meaning the rank over $\mathbb{F}_p$ between two elements of $\mathbb{F}_q^n$. This metric is useful when communicating over a multicast network; for more information, see [29] and [31].

In [26] and [27], the author generalizes the concepts of error detectability and correctability to generic error sets. We recall some of the results in this section for matters of completeness.

Definition 5. *An error set $E \subseteq \mathbb{F}_q^n$ is detectable by some code $\mathcal{C} \subseteq \mathbb{F}_q^n$ if $E \cap \mathcal{C} = \{0\}$, or equivalently if $E^* \cap \mathcal{C} = \emptyset$. Similarly, this set of errors E is correctable by $\mathcal{C}$ if $\Delta E \cap \mathcal{C} = \{0\}$.*

This definition generalizes the classical concept of detectability and correctability based on Hamming balls and balls based on rank metric. In the case of Hamming balls,

$$\Delta B_t(0) \subseteq B_{d-1}(0), \tag{1}$$

meaning that any error that is detectable under the difference set definition is also detectable under the minimum distance of a code. Note that the difference set of a ball is a ball itself: if d is odd, then $\Delta B_t(0) = B_{d-1}(0)$, whereas if d is even, then $\Delta B_t(0) = B_{d-2}(0)$.

The following proposition can be viewed as a motivation for the language used in Definition 5.

Proposition 1. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a code with parity-check matrix $H \in \mathbb{F}_q^{n-k \times n}$. The set $E \subseteq \mathbb{F}_q^n$ is correctable by $\mathcal{C}$ if and only if its syndromes are unique, meaning that for $e, e' \in E$, $eH^t = e'H^t$ if and only if $e = e'$.*

Proof. Let $e, e' \in E$ be errors with the same syndrome, meaning that $eH^t = e'H^t$. This is equivalent to saying that $(e - e')H^t = 0$, meaning that $e - e' \in \mathcal{C}$. Since by hypothesis $\Delta E \cap \mathcal{C} = \{0\}$, then $e = e'$.

The following proposition is a direct consequence of Definition 5.

Proposition 2. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a code. $E \subseteq \mathbb{F}_q^n$ is decodable by $\mathcal{C}$ if and only if ΔE is detectable by $\mathcal{C}$.*

It follows the next corollary showing that Δ-closed sets are maximal sets for which detectability corresponds to correctability.

Corollary 2. *Given a code $\mathcal{C} \subseteq \mathbb{F}_q^n$, a set $E \subseteq \mathbb{F}_q^n$ is detectable and correctable if and only if E is Δ-closed, meaning that $\overline{E}^{\Delta} = E$.*

We focus now on results regarding the existence of codes correcting a generic error set $E \subseteq \mathbb{F}_q^n$.

3.2 Generic Gilbert-Varshamov Bound

The proof of the following results may be found in [26] or [27], and are based on the concept of a balanced family of codes.

Definition 6. *Let $\mathcal{B}$ be a collection of $[n,k]$-linear codes. We call $\mathcal{B}$ a balanced family of codes if each vector in $(\mathbb{F}_q^n)^*$ belongs to the same number of codes of $\mathcal{B}$.*

Theorem 2 ([26]). *Let $\mathcal{B}$ be a balanced family of codes and $f : \mathbb{F}_q^n \to \mathbb{C}$ be a complex-valued function. Then*

$$\frac{1}{|\mathcal{B}|}\sum_{\mathcal{C}\in\mathcal{B}}\sum_{c\in\mathcal{C}^*} f(c) = \frac{q^k-1}{q^n-1}\sum_{v\in(\mathbb{F}_q^n)^*} f(v).$$

Proof. Construct a bipartite graph where the upper nodes are linear codes in $\mathcal{B}$, the lower nodes are the non-zero elements of $\mathbb{F}_q^n$, and there is an edge if the code above contains the element below. Figure 1 depicts such a bipartite graph.

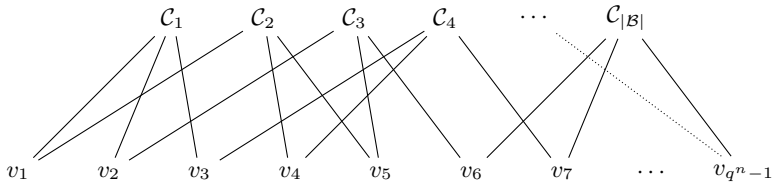

Fig. 1. Bipartite graph of a balanced family.

There are $|\mathcal{B}|$ nodes above and q^n-1 nodes below. This graph is regular, meaning each top node has the same degree of q^k-1, and each bottom node has the same degree $N_{\mathcal{B}}$. Counting the edges from both levels, we find

$$(q^n-1)N_{\mathcal{B}} = (q^k-1)|\mathcal{B}|. \tag{2}$$

Label each edge with the value $f(v)$, where $v \in (\mathbb{F}_q^n)^*$ is the lower node. Summing over all the edges of the graph, we obtain

$$\sum_{\mathcal{C}\in\mathcal{B}}\sum_{c\in\mathcal{C}^*} f(c) = N_{\mathcal{B}}\sum_{v\in(\mathbb{F}_q^n)^*} f(v) = |\mathcal{B}|\frac{q^k-1}{q^n-1}\sum_{v\in(\mathbb{F}_q^n)^*} f(v),$$

where the last equality follows from Equation (2).

Theorem 3. *Let $\mathcal{B}$ be a balanced family of codes, and $E \subseteq \mathbb{F}_q^n$ an error set such that*

$$(q^k-1)|E^*| < q^n-1.$$

Then there exists a code $\mathcal{C} \in \mathcal{B}$ such that $E \cap \mathcal{C} = \{0\}$. That is, E is detectable by $\mathcal{C}$.

Proof. Let $f : \mathbb{F}_q^n \to \mathbb{C}$ be such that $f(v) = \chi_{\{v \in E^*\}}$, the indicator function for the set E^*. Applying Theorem 2, we can see that

$$\frac{q^k - 1}{q^n - 1}|E^*| = \frac{1}{q^n - 1} \sum_{v \in (\mathbb{F}_q^n)^*} f(v) = \frac{1}{|\mathcal{B}|} \sum_{\mathcal{C} \in \mathcal{B}} \sum_{c \in \mathcal{C}^*} f(c) = \frac{1}{|\mathcal{B}|} \sum_{\mathcal{C} \in \mathcal{B}} |\mathcal{C} \cap E^*|.$$

Note that for every $\mathcal{C} \in \mathcal{B}$, it's true that $|\mathcal{C} \cap E^*| \in \mathbb{N} \cup \{0\}$. By the hypothesis of our statement, we have $\frac{q^k-1}{q^n-1}|E^*| < 1$, thus

$$\frac{1}{|\mathcal{B}|} \sum_{\mathcal{C} \in \mathcal{B}} |\mathcal{C} \cap E^*| < 1.$$

Hence, by an averaging argument, it must hold that there exists some $\mathcal{C} \in \mathcal{B}$ such that $\mathcal{C} \cap E^* = \emptyset$.

Theorem 3 tells us that any error set $E \subseteq \mathbb{F}_q^n$ can be detected via an $[n, k]$ code, so long as $|E^*| < \frac{q^n-1}{q^k-1}$. If we wish to correct this error set, it suffices to consider $|\Delta E^*| < \frac{q^n-1}{q^k-1}$. Note that if $|\Delta E| < q^{n-k}$, then it can be shown that

$$|\Delta E^*| < \frac{q^n - 1}{q^k - 1}. \tag{3}$$

Theorem 3 is a generalization of the Gilbert-Varshamov bound. Indeed, if one applies Equations (1) and (3) to the set $E \subseteq B_t(0)$, we obtain the following Theorem.

Theorem 4 (Gilbert-Varshamov Bound, [27]). *Let n, k, and d be such that*

$$\sum_{i=1}^{d-1} \binom{n}{i} (q-1)^i < q^{n-k}.$$

Then there exists $\mathcal{C}$ an $[n, k]$ code $\mathcal{C}$ of minimum distance d.

It is outside the purpose of this paper to prove results on balanced families of codes, nevertheless, it is easy to show that these families exist. (Desarguesian) spreads are an example.

Definition 7. *A (Desarguesian) spread $\mathcal{S}$ is a partition of $\mathbb{F}_q^n$ into k-dimensional subspaces. That is, a spread $\mathcal{S}$ is a collection of k-dimensional subspaces such that $\bigcup_{\mathcal{C} \in \mathcal{S}} \mathcal{C} = \mathbb{F}_q^n$, and for any $\mathcal{C}_1, \mathcal{C}_2 \in \mathcal{S}$, we have $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0\}$.*

It is well-known that Desarguesian spreads exist if and only if $k \mid n$. We refer the reader interested in the construction of spreads to see [22] and [23].

3.3 Density of Codes Correcting a Generic Error Set

The following theorem shows that, with high probability, a randomly chosen code corrects a fixed error set.

Theorem 5. *Let* $E \subseteq \mathbb{F}_q^n$*, and* $k \leq n\left(1 - \frac{\log_p(|E|)}{N} - \varepsilon\right)$ *for some* $0 < \varepsilon < 1 - \frac{\log_p(|E|)}{N}$*. Then for any* $G \in \mathbb{F}_q^{k\times n}$ *of rank* k *sampled uniformly at random, the code* $\mathcal{C}$ *generated from* G *corrects* E *with probability no less than* $1 - q^{-n\varepsilon}$*.*

Proof. Since G is sampled uniformly at random from $\mathbb{F}_q^{k\times n}$, each entry of G can be viewed as taken uniformly at random from $\mathbb{F}_q$. Then we can consider the codewords in $\mathcal{C}$ - which are linear combinations of the rows of G - as vectors with entries sampled uniformly from $\mathbb{F}_q$.

From this, the probability that an arbitrary codeword is in $E \cap \mathcal{C}$ is

$$\frac{|E^*|}{|\left(\mathbb{F}_q^n\right)^*|} = \frac{|E| - 1}{q^n - 1} < \frac{|E|}{q^n} = q^{-n(1-\log_q(|E|))}.$$

Applying logarithm rules, we calculate

$$\log_q(|E|) = \log_q(|E|) = \frac{\log_p(|E|)}{\log_p(p^N)} = \frac{\log_p(|E|)}{N}.$$

Because G has rank k, there will be a total of q^k codewords in $\mathcal{C}$. Since

$$q^k q^{-n(1-\frac{\log_p(|E|)}{N})} \leq q^{n(1-\frac{\log_p(|E|)}{N}-\varepsilon)} q^{-n(1-\frac{\log_p(|E|)}{N})} = q^{-n\varepsilon},$$

we obtain that the probability a non-zero codeword from $\mathcal{C}$ will also be in $E \cap \mathcal{C}$ is at most $q^{-n\varepsilon}$.

Thus, the probability that $E \cap \mathcal{C} = \{0\}$ is bounded from below by $1 - q^{-n\varepsilon}$.

4 Generic Error SDP

With the terminology introduced at the end of Section 2 in mind, we can introduce the standard formulation of the Syndrome Decoding Problem.

Problem 1 (The Syndrome Decoding Problem). For an $[n, k]$ code $\mathcal{C}$ with parity-check matrix H, a syndrome vector $s \in \mathbb{F}_q^{n-k}$, and some $t \in \mathbb{N} \cup \{0\}$, find a vector $e \in \mathbb{F}_q^n$ with Hamming weight $w(e) \leq t$ such that $eH^t = s$, if such e exists.

This Hamming weight case was shown to be NP-hard for binary codes in 1978 by Berlekamp, McEliece, and Tilborg [10], then over any finite field in 1997 by Barg [8]. We are now ready to move away from the Hamming weight and define the syndrome decoding problem based on generic errors, with no specific metric.

Problem 2 (The Generic Error Syndrome Decoding Problem (GE-SDP)). For an $[n, k]$ code $\mathcal{C}$ with parity-check matrix H, a syndrome vector $s \in \mathbb{F}_q^{n-k}$, and $E \subseteq \mathbb{F}_q^n$, find an $e \in E$ such that $eH^t = s$, if such an e exists.

Problem 3 (Decisional GE-SDP). For an $[n, k]$ code $\mathcal{C}$ with parity-check matrix H, a syndrome vector $s \in \mathbb{F}_q^{n-k}$, and $E \subseteq \mathbb{F}_q^n$, decide whether there exists an $e \in E$ such that $eH^t = s$.

This decisional GE-SDP is sometimes called the Coset Weights Problem [6]. Due to complexity theory, we know there exists a search-to-decision reduction that carries across the difficulty of the problem. Thus, the complexity of the Decisional GE-SDP will be the same as GE-SDP. We will abuse terminology and state that, for example, GE-SDP is NP-complete, despite the fact that this term applies only to the Decisional GE-SDP.

In [8], the q-ary SDP is shown to be NP-complete. More generally, over any finite ring with identity and any additive weight (ie: Hamming, Lee), the SDP will still be NP-complete [33]. Moreover, it is widely believed that the q-ary SDP is difficult on average, resulting in the difficulty of random instances [5].

Via a reduction argument, the authors of [7] demonstrate that the R-SDP problem is NP-complete based on the difficulty of the q-ary SDP problem. The GE-SDP presented here evidently contains all instances of SDP, as the metric is not specified. Since R-SDP is NP-complete, it represents a difficult type of problem in NP. As R-SDP is contained in our general form of SDP, we have that the hardest instances of our presentation of SDP are NP-complete, hence the GE-SDP is contained in the NP-complete complexity hierarchy. This sentiment is contained in the following theorem:

Theorem 6. *The Decisional GE-SDP is NP-complete.*

Note that this does not imply that all other instances of the GE-SDP are NP-complete. For example, the exact computational complexity of rank-SDP, the rank metric form of the SDP, is not known [34] - but it is widely believed to be a difficult problem [19]. In practice, this rank form seems to be more difficult to solve than the Hamming weight SDP [11], and cryptographic schemes built from the rank metric appear to be more secure against decoding attacks [32]. We note that [20] demonstrates there exists a randomized polynomial time algorithm that can reduce the rank-SDP to an NP-hard problem. This is a wonderful result but not a deterministic reduction - thus, the exact complexity of the rank-SDP remains open.

5 Generic Error CVE

We now generalize the format of the CVE scheme to accept generic errors that do not depend on a specific metric. Traditionally, CVE takes an error set being the sphere of some specific Hamming weight, and samples uniformly at random a monomial transformation from $\mathfrak{M}_n$ to permute and obfuscate an error from that

set [15]. In the R-SDP case from [7], this error set is taken to be $\{0, \pm 1\}^n$, with the set of monomial transformations $\widetilde{\mathfrak{M}}_n$ restricted to permit scaling factors of ± 1 only. Another variant of CVE is the one developed in [9] where the metric considered is the rank metric. Here, the error set is the set of vectors of a certain rank weight and the transformations are the natural analogue of monomial transformations in the rank-metric setting.

We note that for generic errors with no structure to speak of applying monomial transforms with no restrictions may be inappropriate. Indeed, for the set $E = \{(0, 2), (1, 0)\}$ over $\mathbb{F}_3$, the monomial transformation

$$M = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}.$$

would not be allowed in the generic error setting. To address this issue, we instead use the language of the stabilizer $\mathfrak{S}_E$, which may or not may not include $\mathfrak{M}_n$.

The CVE scheme based on a generic error set (GE-CVE) is shown in Figure 2.

Remark 1. The protocol described in Figure 2 is only one pass; in practice, many passes will be required to push the probability of error below some acceptable threshold.

We prove this system is a zero-knowledge identification scheme by showing that the following conditions hold.

- Completeness: an honest prover can convince an honest verifier.
- Soundness: a cheating prover can convince an honest verifier with only a small probability.
- Zero-Knowledge: the verifier learns nothing other than the statement's veracity.

The proofs mimic those in [7], [15], and [34].

Completeness:

The hash values should match the appropriate commitment if the prover is honest.

If $b = 0$, then

$$(yf^{-1})H^t - zs = ((u + ze)MM^{-1})H^t - zs = uH^t + zeH^t - zs = uH^t,$$

hence $\text{Hash}(f, (yf^{-1})H^t - zs)$ is the same as c_0, the original commitment.

On the other hand, if $b = 1$, then

$$y - zf = (u + ze)M - zeM = uM,$$

which matches commitment c_1.

GE-CVE

Public data: $q, n, k \in \mathbb{N}, E \subset \mathbb{F}_q^n, H \in \mathbb{F}_q^{(n-k)\times n}$

Private Key: $e \in E$

Public Key: $s = eH^t \in \mathbb{F}_q^{n-k}$

PROVER		**VERIFIER**
$u \leftarrow\$ \mathbb{F}_q^n,\ M \leftarrow\$ \mathfrak{S}_E$		
Set $c_0 = \text{Hash}(M, uH^t)$		
Set $c_1 = \text{Hash}(uM, eM)$		
	$\xrightarrow{(c_0, c_1)}$	
		$z \leftarrow\$ \mathbb{F}_q^*$
	$\xleftarrow{z}$	
Set $y = (u + ze)M$		
	$\xrightarrow{y}$	
		Choose $b \in \{0, 1\}$
	$\xleftarrow{b}$	
If $b = 0,$ set $f := M$		
If $b = 1,$ set $f := eM$		
	$\xrightarrow{f}$	
		If $b = 0,$ accept if
		$c_0 = \text{Hash}(f, (yf^{-1})H^t - zs)$.
		If $b = 1,$ accept if
		$f \in E$ and $c_1 = \text{Hash}(y - zf, f)$.

Fig. 2. One pass of the generic error CVE algorithm.

Soundness:

In the case of a dishonest prover, we show this adversary can convince the verifier that they are truthful with a probability that is limited by $\frac{q}{2(q-1)}$. There are two avenues to consider: the first in which the dishonest prover is expecting to receive challenge $b = 0$, and the second where they expect $b = 1$.

Call the first strategy st_0. Here, the adversary picks u and M uniformly at random, and will attempt to find e' such that $e'H^t = s$. The commitments are then

$$c_0 = \text{Hash}(M, uH^t) \text{ and } c_1 \text{ is a random string.}$$

Hence, independent of the verifier's sent value of z, the dishonest prover can respond to the challenge $b = 0$ and pass the verification test.

The second strategy st_1 is where the adversary anticipates the challenge $b = 1$. Again, u and M are chosen uniformly at random, but now they must pick $e' \in E \subseteq \mathbb{F}_q^n$. The commitments are then

$$c_0 \text{ is a random string and } c_1 = \text{Hash}(uM, e'M).$$

Since $M \in \mathfrak{S}_E$ has the property that $e'M \in E$ by definition, this is sufficient for the dishonest prover to pass the challenge for $b = 1$.

These strategies can both be improved somewhat from probability $\frac{1}{2}$ to $\frac{q}{2(q-1)}$. The dishonest prover attempts to guess the verifier's choice of z; call this guess z'. In st_0, we saw above that the adversary can correctly answer the challenge $b = 0$ independent of z, but if the guess of z' is correct they can answer the challenge $b = 1$ as well. Likewise, in st_1, they can respond to $b = 0$ if z' has been guessed correctly, and to $b = 1$ regardless of the value of z.

For one round of CVE, an adversary following strategy st_k can pick z' and thus respond correctly to the challenge b with probability

$$\mathbb{P}[b = k] + \mathbb{P}[b = 1 - k] \cdot \mathbb{P}(z' = z) = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{q-1}.$$

That is,

$$\mathbb{P}[\text{dishonest prover passes challenge } b] = \frac{q}{2(q-1)}.$$

Zero-Knowledge:

In the same vein as [21], we consider a resetable, probabilistic, polynomial-time simulator. The aim of this simulation is to perform as naturally as possible, so that a third party inspecting the simulator's communication history would view it as indistinguishable from a genuine interaction.

Given that in this 5-pass scheme the verifier only ever sends information to the prover twice, they will have exactly two strategies. Indeed, let st_0 be the strategy involving taking into consideration (c_0, c_1), then producing z. Let st_1 be the other strategy of accepting (c_0, c_1) and y, then generating b as the challenge.

The simulation is executed in the following fashion:

– If $b = 0$, uniformly at random select u and M, then solve $s = e'H^t$ for e', ignoring the condition that $e' \in E$. The commitments will then be $c_0 = \text{Hash}(M, uH^t)$ with c_1 generated randomly. By simulating the verifier, the simulator will apply st_0 and return z. Computing $y = (u+ze')M$ and sending it to the simulator, it will apply st_1 and return b'.
– If $b = 1$, the simulator still chooses u and M uniformly, but now selects a random vector e', this time with $e' \in E$. The commitments will then be c_0 generated randomly and $c_1 = \text{Hash}(uM, e'M)$. Upon calling the simulator and inputting (c_0, c_1), it will apply st_0 and return z. Again, computing and sending $y = (u + ze')M$, the simulator returns b'.

The simulator then goes through the following loop: if $b' = b$, halt the simulation and output the string of communication $[(c_0, c_1), z, y, b, \text{ and } f]$; else, restart the protocol from the top.

After an average of $2r$ rounds, because these values are distributed uniformly, the simulator's string of communication will be indistinguishable from one that was produced from an honest execution of the protocol after r rounds - thus satisfying ZK.

We now demonstrate the $(2, 2)$-special soundness of the protocol, which tightly implies knowledge soundness.

Proposition 3. *The protocol in Figure 2 is* $(2, 2)$*-special sound and has soundness error*

$$\frac{q}{2(q-1)}.$$

Proof. Consider the situation of an honest verifier and a cheating prover. Suppose there exist four transcripts T_1, T_2, T_3, T_4, all of which are valid and which correspond to the same commitment pair (c_0, c_1). That is, there exist $z \neq z'$ such that the prover was able to reply convincingly to queries $(z, 0)$, $(z, 1)$, $(z', 0)$ and $(z', 1)$. The commitments are then the following:

T_1: $\big(c_0, c_1, y, M\big)$;
T_2: $\big(c_0, c_1, y, eM\big)$;
T_3: $\big(c_0, c_1, y', M'\big)$;
T_4: $\big(c_0, c_1, y', eM'\big)$.

For the commitment c_0 to be valid for both transcripts T_1 and T_3, it must be that

$$\text{Hash}(M, (yM^{-1})H^t - zs) = c_0 = \text{Hash}(M', (y'M'^{-1})H^t - z's).$$

Therefore either there exists an extractor algorithm that can efficiently compute hash collisions, or M is indeed equal to M' and $((y - y')M^{-1})H^t = (z - z')s$.

Likewise, from the validity of transcripts T_2 and T_4, we see that

$$\text{Hash}(y - z(eM), eM) = c_1 = \text{Hash}(y' - z'(eM'), eM').$$

Recall however that $M = M'$, so either a cheating prover can find hash collisions or it holds that $y - y' = (z - z')(eM)$.

Combining these results, we find that $(e'M^{-1})H^t = s$ with $e'M^{-1} \in E$, where $e' = eM$. Thus either hash collisions have been found or this e' forms a valid key that can be used to impersonate an honest prover.

Finally, we calculate the soundness probability of Figure 2 from [4] as

$$1 - \left(1 - \frac{1}{q-1}\right)\left(1 - \frac{1}{2}\right) = \frac{q}{2(q-1)}.$$

We end with a theorem that shows if an adversary is, in the long run, able to guess correctly more often than expected, then one of our security assumptions must have been violated.

Theorem 7. *After r rounds of the protocol in Figure 2, if*

$$\mathbb{P}[\textit{honest verifier accepts dishonest prover}] \geq \left(\frac{q}{2(q-1)}\right)^r + \varepsilon$$

for $\varepsilon > 0$, then it is possible to either find a collision for Hash$(\cdot)$ or recover the private key e.

This is a direct result of Proposition 3. The consequence of this theorem is that either it is feasible to find collisions in the hash function, or that the GE-SDP is not an NP-complete problem - both of these violate standard cryptographic results.

6 On Polynomial Instances of GE-SDP

This section shows that if the generic error set $E \subseteq \mathbb{F}_q^n$ is included in a small Δ-closed set intersecting the code trivially, then Problem 2 can be solved by means of Gaussian elimination, leading to an attack of GE-CVE on that error set.

The attack here is a projection argument. Because the SDP was shown to be NP-complete for binary codes in [10], then over any finite field in [8], we cannot efficiently solve for an arbitrary syndrome in general.

However, solving this smaller instance over $\mathbb{F}_p$ is computationally feasible. This would not normally be of use - the errors $E \subseteq \mathbb{F}_q^n$ will generally not have any basis to speak of - but using the framework that $\overline{E}^{\Delta}$ forms a subspace allows us to find a basis. Once we recognize that we can solve this for vectors over $\mathbb{F}_p$, we can solve it for vectors over $\{0, \pm 1\}$, solving the R-SDP problem.

Recall the field $\mathbb{F}_q$, where $q = p^N$ is a prime power and that $\mathbb{F}_q$ is an N-dimensional vector space over $\mathbb{F}_p$. Thus we know that there exists an isomorphism

φ mapping $\mathbb{F}_q$ into $\mathbb{F}_p^N$. If we consider the action of this isomorphism on the entries of the parity-check matrix H, we obtain a new, reduced instance - call it $H' = \varphi(H) \in \mathbb{F}_p^{N(n-k)\times n}$. The same action on the entries of s will give $s' = \varphi(s) \in \mathbb{F}_p^{N(n-k)}$. With this in mind, we need only consider the projection of the code from $\mathbb{F}_q$ down to $\mathbb{F}_p$.

Let $E \subseteq \mathbb{F}_q^n$, and consider $\overline{E}^{\Delta}$ as defined in Section 3. By Theorem 1, we know that $\overline{E}^{\Delta}$ is an $\mathbb{F}_p$-subspace; let

$$\overline{E}^{\Delta} = \langle E \rangle_{\mathbb{F}_p} = \langle e_1, e_2, ..., e_m \rangle_{\mathbb{F}_p}$$

where $e_1, \ldots, e_m \in E$ form a $\mathbb{F}_p$-basis.

Concerning the GE-SDP, given syndrome $s \in \mathbb{F}_q^{n-k}$ and parity check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, we can then apply Gaussian Elimination and efficiently solve the system for $\overline{E}^{\Delta}$ over $\mathbb{F}_q$:

$$s = eH^t = \lambda_1 e_1 H^t + \lambda_2 e_2 H^t + ... + \lambda_m e_m H^t. \tag{4}$$

If $\overline{E}^{\Delta} \cap \mathcal{C} = \{0\}$, since $E \subseteq \overline{E}^{\Delta}$, then E is correctable and the error $e \in E$ such that $s = eH^t$ is unique and can be found solving Equation (4). We resume this argument in the following theorem.

Theorem 8. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a code and $E \subseteq \mathbb{F}_q^n$ an error set such that $\overline{E}^{\Delta} \cap \mathcal{C} = \{0\}$. Then Problem 2 can be solved in $\mathcal{O}(n^3)$.*

For a code $\mathcal{C} \subseteq \mathbb{F}_{p^N}^n$ and an error set $E \subseteq \mathbb{F}_{p^N}^n$, for $\overline{E}^{\Delta} \cap \mathcal{C} = \{0\}$ is it necessary that

$$\dim_{\mathbb{F}_p} \overline{E}^{\Delta} + \dim_{\mathbb{F}_p} C = kN + \dim_{\mathbb{F}_p} \overline{E}^{\Delta} \leq nN = \dim_{\mathbb{F}_p} \mathbb{F}_q^n.$$

This is equivalent to the condition that

$$R \leq 1 - \frac{\dim_{\mathbb{F}_p} \overline{E}^{\Delta}}{nN}. \tag{5}$$

Remark 2. Theorem 8 does not apply when $\overline{E}^{\Delta} \cap \mathcal{C} \neq \{0\}$. Indeed, in this case, the system from Equation 4 does not have a unique solution, rather as many as $|\overline{E}^{\Delta} \cap \mathcal{C}|$. This is the case for the SDP based on the Hamming metric or on the rank metric. Indeed given a ball $E = B_r(0)$, $\overline{E}^{\Delta} = \mathbb{F}_q^n$ for either metrics.

6.1 Vulnerability of R-SDP and R-CVE

The presented attack applies to R-CVE. As already mentioned, [7] shows that the R-SDP problem is an NP-complete problem.

The attack presented in the previous section applies to all R-CVE schemes defined over a code $\mathcal{C}$ with $C \cap \mathbb{F}_q^n = \{0\}$. Indeed, the error set considered for R-CVE is $E = \{0, \pm 1\}^n$ and $\overline{E}^{\Delta} = \mathbb{F}_p^n$. Equation 5, in this case, reduces to

$$R \leq \frac{N-1}{N},$$

meaning that it is sufficient to use codes with very high rates to nullify our attack.

The cardinality of the set of codes that intersect trivially with a given error set may be calculated as a function of the q-binomial coefficient. The exact formula is outside the purpose of this paper, but it may be found as [28, Corollary 3.3].

Note that if the R-CVE is defined over a prime field, then the attack cannot be performed since $\mathcal{C} \cap \mathbb{F}_p^n = \mathcal{C}$.

Example 4. Let $p^N = 5^5$, with $n = 10$ and $k = 9$. For this example, we take $\overline{E}^{\Delta}$ to be of dimension 5 over $\mathbb{F}_5$.

From the viewpoint of rate, the inequality looks like

$$R = 0.9 \leq 1 - \frac{5}{10 \cdot 5}.$$

Hence, this code is vulnerable to being solved via basis in $\overline{E}^{\Delta}$. This example highlights that the weakness only cares about the exponent in the prime power of the code rather than the specific prime used. One can readily see that p does not appear in the inequality. Taking $p = 5$ results in the same inequality as $p = 7$, or indeed any prime.

Example 5. Consider the exact same parameters as before, except now let $\overline{E}^{\Delta}$ be slightly larger, of dimension 6 over $\mathbb{F}_5$.

Now the inequality - which does not hold - looks like

$$R = 0.9 \not\leq 0.88 = 1 - \frac{6}{10 \cdot 5}.$$

For these values, the initial conditions are not met, so the vulnerability described above does not apply here. This highlights a more general fact: when $\dim_{\mathbb{F}_p} \overline{E}^{\Delta}$ is small, the rate R will have more flexibility in the values it can take.

7 Conclusions

We have generalized the SDP and CVE to accept an error set without structure and argued the complexity of these problems. Using the set difference operation, we have constructed a particularly generic notion of detectability and correctability and applied them to this GE-SDP and GE-CVE. This also results in a generalization of the Gilbert-Varshamov Bound. It was used to give conditions that determine when there exists a code that can correct a given error set and bounds on the probability that a random code will correct an arbitrary error set. This framework demonstrates that certain GE-SDP parameters have vulnerabilities, permitting an adversary to correct the errors that are crucial to the security of the problem. We have shown that this vulnerability is only applicable when the parameters satisfy a certain bound. To conclude, we have demonstrated a vulnerability in the GE-SDP, and thus R-SDP, and presented a method of working around this susceptibility.

In regard to future work, we would welcome concrete results about the average-case complexity of GE-SDP. Seeing as R-SDP is a special case of GE-SDP with error set $\{0, \pm 1\}^n$, it is possible that other choices of small error sets may result in a practical cryptosystem. These would in turn, result in special cases of GE-CVE, which may improve the scheme.

Additionally, many of these results may be improved with the use of a trusted helper or vector (see [16], [12], [13]) or by leveraging the "in the head" paradigm (see [17], [2], [18]). We relegate this to future work.

Acknowledgements

We would like to thank Violetta Weger and Paolo Santini for their helpful discussions, and Frank Kschischang for sharing some fundamental resources.

References

1. Nist's post-quantum cryptography standardization project, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization
2. Aguilar-Melchor, C., Gama, N., Howe, J., Hülsing, A., Joseph, D., Yue, D.: The return of the sdith. Cryptology ePrint Archive, Paper 2022/1645 (2022), https://eprint.iacr.org/2022/1645
3. Albrecht, M., Bernstein, D., Chou, T., Cid, C., Gilcher, J., Lange, T., Maram, V., von Maurich, I., Misoczki, R., Niederhagen, R., Paterson, K., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Tjhai, C.J., Tomlinson, M., Wang, W.: Classic mceliece: conservative code-based cryptography: cryptosystem specification (2022), https://classic.mceliece.org/nist.html
4. Attema, T., Fehr, S., Klooß, M.: Fiat-shamir transformation of multi-round interactive proofs. Cryptology ePrint Archive, Paper 2021/1377 (2021), https://eprint.iacr.org/2021/1377
5. Augot, D., Finiasz, M., Sendrier, N.: A fast provably secure cryptographic hash function. IACR Cryptology ePrint Archive **2003**, 230 (01 2003)
6. Baldi, M., Barenghi, A., Chiaraluce, F., Pelosi, G., Santini, P.: A finite regime analysis of information set decoding algorithms. Algorithms **12**(10) (2019). https://doi.org/10.3390/a12100209, https://www.mdpi.com/1999-4893/12/10/209
7. Baldi, M., Battaglioni, M., Chiaraluce, F., Horlemann-Trautmann, A.L., Persichetti, E., Santini, P., Weger, V.: A new path to code-based signatures via identification schemes with restricted errors. ArXiv **abs/2008.06403** (2020)
8. Barg, A.: Some new np-complete coding problems. Problemy Peredachi Informatsii **30**(3) (199)
9. Bellini, E., Caullery, F., Hasikos, A., Manzano, M., Mateu, V.: Code-based signature schemes from identification protocols in the rank metric. In: Cryptology and Network Security. Springer International Publishing (2018)
10. Berlekamp, E., McEliece, R., van Tilborg, H.: On the inherent intractability of certain coding problems (corresp.). IEEE Trans. Inf. Theory **24**, 384–386 (1978)

11. Bernstein, D.: Introduction to post-quantum cryptography. Springer Berlin Heidelberg (2009). https://doi.org/10.1007/978-3-540-88702-7_1
12. Beullens, W.: Sigma protocols for mq, pkp and sis, and fishy signature schemes. Cryptology ePrint Archive, Paper 2019/490 (2019), https://eprint.iacr.org/2019/490
13. Bidoux, L., Gaborit, P.: Compact post-quantum signatures from proofs of knowledge leveraging structure for the pkp, sd and rsd problems (2022), https://arxiv.org/abs/2204.02915
14. Bricout, R., Chailloux, A., Debris-Alazard, T., Lequesne, M.: Ternary syndrome decoding with large weight. Cryptology ePrint Archive, Paper 2019/304 (2019), https://eprint.iacr.org/2019/304
15. Cayrel, P.L., Véron, P., El Yousfi Alaoui, S.M.: A zero knowledge identification scheme based on the q-ary SD problem. In: Selected Areas in Cryptography. LNCS, vol. 6544, pp. 171–186. Springer, Waterloo, Canada (Aug 2010). https://doi.org/10.1007/978-3-642-19574-7_12, https://hal.inria.fr/hal-00674249
16. Feneuil, T., Joux, A., Rivain, M.: Shared permutation for syndrome decoding: New zero-knowledge protocol and code-based signature. Cryptology ePrint Archive, Paper 2021/1576 (2021). https://doi.org/10.1007/s10623-022-01116-1, https://eprint.iacr.org/2021/1576
17. Feneuil, T., Joux, A., Rivain, M.: Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs. Cryptology ePrint Archive, Paper 2022/188 (2022). https://doi.org/10.1007/978-3-031-15979-4_19, https://eprint.iacr.org/2022/188
18. Feneuil, T., Rivain, M.: Threshold linear secret sharing to the rescue of mpc-in-the-head. Cryptology ePrint Archive, Paper 2022/1407 (2022), https://eprint.iacr.org/2022/1407
19. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. CoRR **abs/1301.1026** (2013)
20. Gaborit, P., Zémor, G.: On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Transactions on Information Theory **62**(12), 7245–7252 (2016). https://doi.org/10.1109/TIT.2016.2616127
21. Goldreich, O.: Zero-knowledge twenty years after its invention. Cryptology ePrint Archive, Paper 2002/186 (2002), https://eprint.iacr.org/2002/186
22. Gorla, E., Manganiello, F., Rosenthal, J.: Spread codes and spread decoding in network coding. In: 2008 IEEE International Symposium on Information Theory. IEEE (jul 2008). https://doi.org/10.1109/isit.2008.4595113
23. Gorla, E., Manganiello, F., Rosenthal, J.: An algebraic approach for decoding spread codes (2012). https://doi.org/10.3934/amc.2012.6.443, ""
24. Károlyi, G.: A compactness argument in the additive theory and the polynomial method. Discrete Mathematics **302**, 124–144 (2005)
25. Károlyi, G.: An inverse theorem for the restricted set addition in abelian groups. Journal of Algebra **290**(2), 557–593 (2005), https://www.sciencedirect.com/science/article/pii/S0021869305002656
26. Loeliger, H.A.: Averaging bounds for lattices and linear codes. IEEE Transactions on Information Theory **43**(6), 1767–1773 (1997). https://doi.org/10.1109/18.641543
27. Loeliger, H.A.: On the Basic Averaging Arguments for Linear Codes, pp. 251–261. Springer US (1994). https://doi.org/10.1007/978-1-4615-2694-0_25
28. Ravagnani, A.: Whitney numbers of combinatorial geometries and higher-weight dowling lattices (2019). https://doi.org/10.48550/ARXIV.1909.10249

29. Ravagnani, A., Kschischang, F.: Adversarial network coding (2017). https://doi.org/10.48550/ARXIV.1706.05468
30. Roth, R.: Introduction to Coding Theory. Cambridge University Press (2006). https://doi.org/10.1017/CBO9780511808968
31. Silva, D., Kschischang, F.: Security for wiretap networks via rank-metric codes. In: 2008 IEEE International Symposium on Information Theory. pp. 176–180 (2008). https://doi.org/10.1109/ISIT.2008.4594971
32. Urivskiy, A., Johansson, T.: New technique for decoding codes in the rank metric and its cryptography applications. Problems of Information Transmission - PROBL INF TRANSM **38**, 237–246 (07 2002). https://doi.org/10.1023/A:1020369320078
33. Weger, V., Battaglioni, M., Santini, P., Horlemann-Trautmann, A.L., Persichetti, E.: On the hardness of the lee syndrome decoding problem. CoRR **abs/2002.12785** (2020)
34. Weger, V., Gassner, N., Rosenthal, J.: A survey on code-based cryptography (2022). https://doi.org/10.48550/ARXIV.2201.07119