Weak Instances of the Two Matrix Code Equivalence Problem

Jesús-Javier Chi-Domínguez

Cryptography Research Center, Technology Innovation Institute, Abu Dhabi, UAE

Abstract. Nowadays, the Matrix Code Equivalence Problem shows potential applicability in constructing efficient and secure advanced digital signatures, focusing on linkable ring signatures, threshold signatures, and blind signatures. Current constructions of these advanced signatures rely on relaxed instantiations of the Matrix Code Equivalence Problem (namely, the 2-MCE problem): given two pairs of equivalent matrix codes, find (if it exists) the secret isometry connecting the pairs. For example, the linkable ring signature construction by Chou et al. (AFRICACRYPT, 2023) builds on top of the Inverse Matrix Code Equivalence Problem: given three equivalent matrix codes, where one pair of the codes is connected by the secret isometry and another by the inverse of that isometry, find the secret isometry.

This paper studies the 2-MCE problem, focusing on the family of instances where the secret isometry is (skew) symmetric. Our main contribution is a polynomial-time algorithm for these instances of the 2-MCE problem. We prove that the algorithm returns a valid solution whenever an explicit invertibility condition and two kernel-dimension conditions hold. Our results have a crucial security impact on the recent blind signature construction proposed by Kuchta, LeGrow, and Persichetti (Cryptography and Communications, 2026), whose security relies on the hardness of solving these kinds of instance of the Inverse Matrix Code Equivalence Problem: we show that this problem reduces to the instances we solve. More precisely, we show that we can recover the secret key of the blind signature construction by Kuchta, LeGrow, and Persichetti (Cryptography and Communications, 2026), with an estimated security of 128 bits, in less than a minute.

Keywords: Cryptanalysis · Kronecker Product · Matrix Code Equivalence · Tensor Product

1 Introduction

In the evolving landscape of post-quantum cryptography, designing efficient and secure cryptographic primitives that resist quantum adversaries remains a central challenge. The cryptographic community is currently increasing its interest in exploring the construction of post-quantum digital signatures that provide advanced functionalities, with a focus on

- Threshold signatures that allow a group of signers to generate a single digital signature collectively;
- Linkable ring signatures that allow a user to sign a message anonymously from within a group (called a "ring") while also providing a way to publicly identify if two signatures were created by the same individual, without revealing the signer's identity within the ring.

E-mail: jesus.dominguez@tii.ae (Jesús-Javier Chi-Domínguez)

This work is licensed under a "CC BY 4.0" license.
Date of this document: 2026-10-27.

- Blind signatures that allow a user to obtain a signature on a message without revealing its content to the signer.

In addition, there is an interesting trend in building these advanced signature schemes on top of equivalence problems (e.g., finding a linear transformation between linear codes, matrix codes, or lattices) — particularly, all relying on relaxed problems where the secret transformation is employed twice [BBN+22, CNP+23, BBMP24, KTS+23, KLP26]. Sadly, current constructions based on the relaxed instantiations of the linear code equivalence (LCE) problem and the lattice isomorphism problem (LIP) raise some security issues when employing the secret transformation twice [BCD+24, BCF25]. On the bright side, before this work, the matrix code equivalence looks like a notable candidate for building secure advanced signature schemes — it remains unaffected by the issues spotted in the LCE and LIP scenarios: as long as there is not enough structure on the secrets to be exploited.

The Relaxed Matrix Code Equivalence Problem. An isometry is a homomorphism of matrix codes (i.e., vector subspaces of matrices) that preserves the rank. The Matrix Code Equivalence (MCE) Problem considers finding an isometry between two equivalent matrix codes. Generic algorithms for the MCE problem essentially fall into two families. On the one hand, algebraic algorithms model the MCE problem as a system of polynomial equations and solve it with Gröbner basis techniques [RST24]. In particular, Ran and Samardjiska [RS24] combined the search for rare structures in the graphs associated with the underlying tensors with such algebraic modeling. Also, Narayanan, Qiao, and Tang [NQT24] proposed further algorithms based on new isomorphism invariants of matrix codes. On the other hand, the recent algorithm of Couvreur and Levrat [CL25] is, to the best of our knowledge, the fastest generic algorithm for a wide family of parameters: it solves the MCE problem with exponential time complexity of $\tilde{O}(q^{k/2})$ field operations in $\mathbb{F}_q$ for $(m \times n, k)$-matrix codes with $m \leq n$, and $k < m^2 - 1$ or $(mn - k) < m^2 - 1$. All these algorithms have exponential complexity for generic instances.

The Two Matrix Code Equivalence Problem (2-MCE) is a relaxed variant of the MCE problem and asks to determine the secret isometry connecting two given pairs of equivalent matrix codes. In the general case, we are not aware of an approach to the 2-MCE problem that improves over solving the original MCE problem, i.e., that takes advantage of knowing two applications of the same secret isometry. The only dedicated cryptanalysis of a relaxed 2-MCE-type assumption that we are aware of is the concurrent work of Gilchrist, Marco, Petit, and Tang [GMPT26], which analyses the blind signature schemes of [KLP26]. They exploit the additional structure of the secret by means of a polynomial modeling solved with Gröbner bases, which leads to exponential-time attacks, and they recommend scaling the matrix dimensions of the parameter sets by a factor of about $\sqrt{2}$; for the smallest of these scaled parameter sets they estimate a cost of 72 bits. In contrast, our algorithm relies on solving overdetermined *linear* systems, running in polynomial time: we solve all the parameter sets considered in [GMPT26, KLP26] in less than one minute on a laptop.

1.1 Motivation

Chou et al. describe in [CNP+23] a linkable ring signature scheme based on the hardness of the so-called Inverse Matrix Code Equivalence (IMCE) Problem, which asks to retrieve the secret isometry connecting three equivalent matrix codes (one pair of codes is connected by the secret isometry, while another by the inverse of that isometry).Subsequently, Battagliola et al. present in [BBMP24] a threshold signature based on the Two Matrix Code Equivalence Problem. Recently, Kuchta, LeGrow, and Persichetti introduce in [KLP26] a novel blind signature scheme based on a new relaxed computational assumption: the Modified Inverse Matrix Code Equivalence (MIMCE) Problem, where the secret isometry is (skew) symmetric, and the task corresponds to finding the square of such an isometry. The authors argue

that using the matrix code equivalent setting, where the attack from [BCD+24] does not apply, avoids the pitfalls associated with linear codes when using twice the secret. However, despite the recent cryptanalysis from [CL25, GMPT26], the authors of [KLP26] make a conservative choice and propose sets of parameters with an estimated complexity of 128-bit security.

As an interesting observation, depending on the required advanced functionality of the signature, the current state-of-the-art constructions impose some additional properties on the secret isometry. For example, the Relaxed Matrix Code Equivalence Problem from [KLP26] is a special instantiation of IMCE, and the IMCE problem determines a particular instantiation of the 2-MCE problem. However, restricting the secret isometry in this way may inadvertently reduce security. This motivates our central question:

> *Given an instance of 2-MCE where the secret isometry is constrained to a special family, does this restriction make the problem easier to solve?*

We answer this question in the affirmative for a large class of cases, with particular focus on the scenario where the isometries are (skew) symmetric as instantiated in [KLP26]. Specifically, we give a polynomial-time algorithm for these structured instances, we prove that it is correct whenever an explicit kernel-dimension condition holds, and we show, heuristically and experimentally, that this condition holds for random instances with probability $1 - O(1/q)$.

1.2 Technical Overview

Let k, m, and n be three positive integers, and q a power of a prime number. Informally, given four k-dimensional vector subspaces of $\mathbb{F}_q^{mn}$ generated by $\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2}, \mathbf{G_3} \in \mathbb{F}_q^{k \times mn}$, the Two Matrix Code Equivalence Problem asks to find (if they exist) three invertible matrices $\mathbf{S}$, $\mathbf{A}$, and $\mathbf{B}$ defined over the finite field $\mathbb{F}_q$ such that $\mathbf{G_1} = \mathbf{S}\mathbf{G_0}\mathbf{Q}$ and $\mathbf{G_3} = \mathbf{S}\mathbf{G_2}\mathbf{Q}$ where $\mathbf{Q} = \mathbf{A}^\top \otimes \mathbf{B}$. This work focuses on the scenario where the matrices $\mathbf{A}$ and $\mathbf{B}$ are (skew) symmetric, and presents a new approach to recovering such matrices $\mathbf{S}$, $\mathbf{A}$, and $\mathbf{B}$.

The algorithm. If $\mathbf{A}$ and $\mathbf{B}$ are (skew) symmetric, then $\mathbf{Q}^\top = \epsilon\mathbf{Q}$ for some sign $\epsilon \in \{1, -1\}$. Consequently, the $k \times k$ Gram matrices $\mathbf{G_0}\mathbf{Q}\mathbf{G_0}^\top$, $\mathbf{G_2}\mathbf{Q}\mathbf{G_2}^\top$ and $\mathbf{G_0}\mathbf{Q}\mathbf{G_2}^\top$ of the (skew) symmetric bilinear form defined by $\mathbf{Q}$ are related to the public products $\mathbf{G_i}\mathbf{G_j}^\top$ through the unknown changes of basis only: for instance, $\mathbf{S_1}^{-1}\mathbf{G_1}\mathbf{G_0}^\top = \mathbf{G_0}\mathbf{Q}\mathbf{G_0}^\top$ is ϵ-symmetric. The (skew) symmetry of these three matrices yields *linear* equations in the unknowns $\mathbf{S_1}^{-1}$ and $\mathbf{S_2}^{-1}$ (Step 1 of Figure 1), whose solution space contains the secret and has a small dimension d (Proposition 1). The remaining relation $\mathbf{S_1}^{-1}\mathbf{G_1} = \mathbf{G_0}(\mathbf{A}^\top \otimes \mathbf{B})$ is bilinear in the d unknown coefficients and in $\mathbf{A}^{-\top}$, and linear in $\mathbf{B}$; after multiplying it by a random vector $\mathbf{u}$, the coefficients only appear multiplied by the single unknown vector $\mathbf{A}^{-\top}\mathbf{u}$, so that it becomes a small linear system in d unknown vectors and in $\mathbf{B}$ (Step 2), whose unique solution gives back the coefficients and $\mathbf{B}$; a last linear system then gives $\mathbf{A}$ (Step 3), and the secret is recovered up to harmless scalar factors (Proposition 2). We describe the main steps of our algorithm in Figure 1.

Since each calculation in the algorithm presented in Figure 1 includes matrix multiplications and linear system resolutions, we find that our proposed algorithm runs in polynomial time on the variables k, m, and n (see Theorem 1 for a precise bound). We discuss in Section 3 the correctness of the algorithm, and for which parameter tuples (k, m, n) it recovers the secret matrices of random 2-sMCE instances, separating the proven statements from the main result for random instances, which relies on heuristics.

Algorithm: Solver for the 2-sMCE problem

Input: An instance $\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2}, \mathbf{G_3} \in \mathbb{F}_q^{k \times mn}$ of the 2-sMCE problem, and the symmetry types (ϵ_A, ϵ_B) of $(\mathbf{A}, \mathbf{B})$, with $\epsilon = \epsilon_A \epsilon_B$
Output: Invertible matrices $\mathbf{S_1}, \mathbf{S_2}, \mathbf{A}$ and $\mathbf{B}$ such that $\mathbf{G_1} = \mathbf{S_1 G_0 Q}$ and $\mathbf{G_3} = \mathbf{S_2 G_2 Q}$ where $\mathbf{Q} = \mathbf{A}^\top \otimes \mathbf{B}$, or $\perp$

1. Compute a basis $(\mathbf{U_{1,j}}, \mathbf{U_{2,j}})_{j=1,\dots,d}$ of the solution space of the linear system in $(\mathbf{U_1}, \mathbf{U_2}) \in (\mathbb{F}_q^{k \times k})^2$

$$\mathbf{U_1 G_1 G_0}^\top = \epsilon\, \mathbf{G_0 G_1}^\top \mathbf{U_1}^\top, \qquad \mathbf{U_2 G_3 G_2}^\top = \epsilon\, \mathbf{G_2 G_3}^\top \mathbf{U_2}^\top,$$
$$\mathbf{U_2 G_3 G_0}^\top = \epsilon\, \mathbf{G_2 G_1}^\top \mathbf{U_1}^\top.$$

2. Let $t = \max\{1, \lceil (d_{\epsilon_B}(n) - 1)/(2kn - dm) \rceil\}$ and pick uniformly random vectors $\mathbf{u}_1, \dots, \mathbf{u}_t \in \mathbb{F}_q^m$. Compute the solution space of the linear system in $(\mathbf{v}_{i,j})_{i \le t,\, j \le d} \in (\mathbb{F}_q^m)^{td}$ and $\mathbf{Y} \in \mathcal{S}_{\epsilon_B}(n)$

$$\sum_{j=1}^{d} \mathbf{v}_{i,j}^\top \mathbf{W}_{j,r} = \mathbf{u}_i^\top \mathbf{D}_r \mathbf{Y}, \qquad \sum_{j=1}^{d} \mathbf{v}_{i,j}^\top \mathbf{W}'_{j,r} = \mathbf{u}_i^\top \mathbf{D}'_r \mathbf{Y},$$
$$r = 1, \dots, k, \quad i = 1, \dots, t,$$

   where $\mathbf{W}_{j,r}, \mathbf{W}'_{j,r}, \mathbf{D}_r, \mathbf{D}'_r \in \mathbb{F}_q^{m \times n}$ are the r-th rows of $\mathbf{U_{1,j}} \mathbf{G_1}$, $\mathbf{U_{2,j}} \mathbf{G_3}$, $\mathbf{G_0}$, $\mathbf{G_2}$, reshaped as $m \times n$ matrices. If it is one-dimensional, spanned by $((\mathbf{v}_{i,j})_{i,j}, \mathbf{Y})$, pick (i_0, j_0) with $\mathbf{v}_{i_0,j_0} \neq \mathbf{0}$ and $\lambda_j \in \mathbb{F}_q$ with $\mathbf{v}_{i_0,j} = \lambda_j \mathbf{v}_{i_0,j_0}$. Otherwise, **return** $\perp$.

3. Let $(\mathbf{U_1}, \mathbf{U_2}) = \sum_j \lambda_j (\mathbf{U_{1,j}}, \mathbf{U_{2,j}})$ and $\mathbf{W}_r = \sum_j \lambda_j \mathbf{W}_{j,r}$. Solve the linear system $\mathbf{X}^\top \mathbf{W}_r = \mathbf{D}_r \mathbf{Y}$, $r = 1, \dots, k$, for $\mathbf{X} \in \mathcal{S}_{\epsilon_A}(m)$, and **return** $\left(\mathbf{U_1}^{-1}, \mathbf{U_2}^{-1}, \mathbf{X}^{-\top}, \mathbf{Y}\right)$.

Figure 1: We consider integers $nm > k$ and $n \ge m$ (otherwise, apply Corollary 2), and odd prime powers q. The number t of projections equals 1 for $k = m = n$. The symmetry types (ϵ_A, ϵ_B) are part of the problem specification in [KLP26]; otherwise, the algorithm is run for each of the at most four admissible pairs.

Outline. Section 2 introduces the required mathematical definitions and theory concerning matrices, tensors and matrix codes. In particular, Section 2.1 focuses on the properties of tensor products and Section 2.2 describes the Relaxed Matrix Code Equivalence Problems analyzed in this work. In addition, Section 2.3 presents new definitions and results that link Matrix Code Equivalence instances with the dual of the matrix codes, which could be of independent interest. Section 3 details the main results on the Two Matrix Code Equivalence Problem when the secret isometry is (skew) symmetric, Section 4 discusses the cryptographic implications on [KLP26], and Section 4.2 reports the experiments that support our heuristics.

2 Preliminaries

Let q be a small odd prime number and let $\mathbb{F}_q$ be a finite field that has q elements. We denote the group of invertible $n \times n$ matrices with entries in $\mathbb{F}_q$ by $\mathsf{GL}_n(\mathbb{F}_q)$, and the set of invertible symmetric and skew-symmetric matrices by $\mathbb{S}_k(\mathbb{F}_q)$. We define $\mathbb{M}_r^{m \times n}(\mathbb{F}_q)$ as the

set of m-by-n matrices of rank r, that is, $\mathbb{M}_r^{m\times n}(\mathbb{F}_q) = \{\mathbf{M} \in \mathbb{F}_q^{m\times n} : \text{rank}(\mathbf{M}) = r\}$. If $r = m$, we write $\mathbb{M}^{m\times n}(\mathbb{F}_q)$ to mean $\mathbb{M}_m^{m\times n}(\mathbb{F}_q)$. For any matrix $\mathbf{M} \in \mathsf{GL}_n(\mathbb{F}_q)$, we write $\mathbf{M}^{-\top}$ to mean the inverse of the matrix $\mathbf{M}^\top$. We denote the Kronecker product of two matrices $\mathbf{A} \in \mathbb{F}_q^{n\times m}$ and $\mathbf{B} \in \mathbb{F}_q^{r\times s}$ by $\mathbf{A} \otimes \mathbf{B} \in \mathbb{F}_q^{nr\times ms}$. We denote the n-by-n identity matrix by $\mathbf{I}_n$.

2.1 The Kronecker Product and Some Useful Properties

For any matrix $\mathbf{M} \in \mathbb{F}_q^{m\times n}$, $\mathsf{vec}(\mathbf{M})$ denotes the column vector of mn coefficients consisting of the concatenation of the rows of the matrix $\mathbf{M}$. We emphasize that the Kronecker product is a tensor product between matrices viewed as vector spaces. We highlight some useful properties below.

- For any two m-by-n matrices $\mathbf{M}$ and $\mathbf{N}$, and two n-by-r matrices $\mathbf{S}$ and $\mathbf{R}$, it holds that $(\mathbf{M} \otimes \mathbf{N})(\mathbf{R} \otimes \mathbf{S}) = (\mathbf{MR} \otimes \mathbf{NS})$.
- For any two matrices $\mathbf{M}$ and $\mathbf{N}$, it holds that $(\mathbf{M} \otimes \mathbf{N})^\top = \mathbf{M}^\top \otimes \mathbf{N}^\top$.
- For any two matrices $\mathbf{M}$ and $\mathbf{N}$ and constant a, $a(\mathbf{M} \otimes \mathbf{N}) = (a\mathbf{M}) \otimes \mathbf{N} = \mathbf{M} \otimes (a\mathbf{N})$ holds.
- For any two invertible matrices $\mathbf{M}$ and $\mathbf{N}$, $(\mathbf{M} \otimes \mathbf{N})^{-1} = \mathbf{M}^{-1} \otimes \mathbf{N}^{-1}$ holds.
- For any two matrices $\mathbf{M}$ and $\mathbf{N}$, we have $\text{rank}(\mathbf{M} \otimes \mathbf{N}) = \text{rank}(\mathbf{M})\text{rank}(\mathbf{N})$.
- For any three matrices $\mathbf{M} \in \mathbb{F}_q^{m\times n}$, $\mathbf{N} \in \mathbb{F}_q^{s\times t}$ and $\mathbf{X} \in \mathbb{F}_q^{n\times t}$, we have $\big[\mathbf{M} \otimes \mathbf{N}\big]\,\mathsf{vec}(\mathbf{X}) = \mathsf{vec}(\mathbf{MXN}^\top)$.

Given a matrix $\mathbf{M} \in \mathbb{F}_q^{m\times n}$, the commutation matrix $\mathbf{K}_{m,n}$ is the mn-by-mn permutation matrix that satisfies $\mathbf{K}_{m,n}\mathsf{vec}(\mathbf{M}) = \mathsf{vec}(\mathbf{M}^\top)$. In particular, for any pairs of matrices $\mathbf{A} \in \mathbb{F}_q^{m\times n}$ and $\mathbf{B} \in \mathbb{F}_q^{r\times s}$, the commutation matrix relates $\mathsf{vec}(\mathbf{A} \otimes \mathbf{B})$ with $\mathsf{vec}(\mathbf{A}) \otimes \mathsf{vec}(\mathbf{B})$ as follows:

$$\mathsf{vec}(\mathbf{A} \otimes \mathbf{B}) = (\mathbf{I}_n \otimes \mathbf{K}_{s,m} \otimes \mathbf{I}_r)(\mathsf{vec}(\mathbf{A}) \otimes \mathsf{vec}(\mathbf{B})).$$

Moreover, the commutation matrices $\mathbf{K}_{m,r}$ and $\mathbf{K}_{n,s}$ link the matrices $\mathbf{A} \otimes \mathbf{B}$ and $\mathbf{B} \otimes \mathbf{A}$ by equality $\mathbf{A} \otimes \mathbf{B} = \mathbf{K}_{m,r}\mathbf{B} \otimes \mathbf{A}(\mathbf{K}_{n,s})^\top$.

2.2 Matrix Code Equivalence Problems

A $(m \times n, k)$ *matrix code* is a subspace $\mathcal{D}$ of dimension k of the space of $m \times n$ matrices. We say that two matrix codes $\mathcal{D}, \mathcal{D}'$ are *equivalent* if there exist two matrices $\mathbf{A} \in \mathsf{GL}_m(\mathbb{F}_q)$ and $\mathbf{B} \in \mathsf{GL}_n(\mathbb{F}_q)$ such that $\mathcal{D}' = \mathbf{A}\mathcal{D}\mathbf{B}$. Each $(m \times n, k)$ *matrix code* $\mathcal{D}$ is isomorphic to the k dimensional $\mathbb{F}_q$ subspace $\mathsf{vec}(\mathcal{D}) = \{\mathsf{vec}(\mathbf{D}) \mid \mathbf{D} \in \mathcal{D}\}$ of $\mathbb{F}_q^{mn}$ [CNP+23]. We call $\mathbf{G} \in \mathbb{F}_q^{k\times mn}$ a generator matrix of $\mathcal{D}$ if its rows form a basis of $\mathsf{vec}(\mathcal{D})$. In particular, we focus on the definition of the MCE and IMCE problems from [CNP+23] given in terms of the Kronecker product.

Definition 1 (Matrix Code Equivalence (MCE) Problem)**.** Let $\mathbf{G_0}, \mathbf{G_1} \in \mathbb{F}_q^{k\times mn}$ be generator matrices of two equivalent $(m \times n, k)$-matrix codes $\mathcal{D}_0, \mathcal{D}_1$ respectively. The Matrix Code Equivalence problem asks to find $\mathbf{S} \in \mathsf{GL}_k(\mathbb{F}_q)$, $\mathbf{A} \in \mathsf{GL}_m(\mathbb{F}_q)$ and $\mathbf{B} \in \mathsf{GL}_n(\mathbb{F}_q)$ such that $\mathbf{G_1} = \mathbf{SG_0}(\mathbf{A}^\top \otimes \mathbf{B})$.

Definition 2 (Inverse Matrix Code Equivalence (IMCE) Problem)**.** Let $\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2} \in \mathbb{F}_q^{k\times mn}$ be generators of three $(m \times n, k)$-matrix codes $\mathcal{D}_0, \mathcal{D}_1$ and $\mathcal{D}_2$ respectively. The Inverse Matrix Code Equivalence problem is to find (if they exist) $\mathbf{S_1}, \mathbf{S_2} \in \mathsf{GL}_k(\mathbb{F}_q)$, $\mathbf{A} \in \mathsf{GL}_m(\mathbb{F}_q)$ and $\mathbf{B} \in \mathsf{GL}_n(\mathbb{F}_q)$ such that $\mathbf{G_1} = \mathbf{S_1G_0Q}$ and $\mathbf{G_2} = \mathbf{S_2G_0Q}^{-1}$ with $\mathbf{Q} = (\mathbf{A}^\top \otimes \mathbf{B}) \in \mathsf{GL}_{mn}(\mathbb{F}_q)$.

For completeness, we also formally introduce the Two Matrix Code Equivalence problem, of which the MCE problem is a special case.

Definition 3 (Two Matrix Code Equivalence (2-MCE) Problem)**.** Let $\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2}, \mathbf{G_3} \in \mathbb{F}_q^{k \times mn}$ be generator matrices of four $(m \times n, k)$-matrix codes $\mathcal{D}_0, \mathcal{D}_1, \mathcal{D}_2$ and $\mathcal{D}_3$, respectively. The Two Matrix Code Equivalence problem is to find (if they exist) $\mathbf{S_1}, \mathbf{S_2} \in \mathsf{GL}_k(\mathbb{F}_q)$, $\mathbf{A} \in \mathsf{GL}_m(\mathbb{F}_q)$ and $\mathbf{B} \in \mathsf{GL}_n(\mathbb{F}_q)$ such that $\mathbf{G_1} = \mathbf{S_1 G_0 Q}$ and $\mathbf{G_3} = \mathbf{S_2 G_2 Q}$ with $\mathbf{Q} = (\mathbf{A}^\top \otimes \mathbf{B}) \in \mathsf{GL}_{mn}(\mathbb{F}_q)$.

Notice that the relations $\mathbf{G_1} = \mathbf{S G_0 Q}$ and $\mathbf{G_2} = \mathbf{S}^{-1}\mathbf{G_0 Q}^{-1}$ of Definition 2 are equivalent to $\mathbf{G_1} = \mathbf{S G_0 Q}$ and $\mathbf{G_0} = \mathbf{S G_2 Q}$; that is, an MCE instance $(\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2})$ is the 2-MCE instance $(\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2}, \mathbf{G_0})$, with the same solutions. When the secret matrices are restricted to be (skew) symmetric, we obtain the following variant, which we use in Section 4.

Definition 4 (Symmetric Inverse Matrix Code Equivalence (sMCE) Problem)**.** The sMCE problem is the MCE problem of Definition 2 where the secret matrices are required to satisfy $\mathbf{A} \in \mathbb{S}_m(\mathbb{F}_q)$ and $\mathbf{B} \in \mathbb{S}_n(\mathbb{F}_q)$.

In the context of blind signatures, the recent construction from [KLP26] introduces the following variant of the sMCE problem, in which only the "square" of the secret isometry is asked for.

Definition 5 (Modified Inverse Matrix Code Equivalence (MIMCE) Problem [KLP26, Definition 2.20])**.** Let $(\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2})$ be an sMCE instance, i.e., $\mathbf{G_1} = \mathbf{S_1 G_0 Q}$ and $\mathbf{G_2} = \mathbf{S_2 G_0 Q}^{-1}$ with $\mathbf{Q} = (\mathbf{A}^\top \otimes \mathbf{B})$ for some $\mathbf{S_1}, \mathbf{S_2} \in \mathsf{GL}_k(\mathbb{F}_q)$, $\mathbf{A} \in \mathbb{S}_m(\mathbb{F}_q)$ and $\mathbf{B} \in \mathbb{S}_n(\mathbb{F}_q)$. The Modified Inverse Matrix Code Equivalence problem asks to find $\mathbf{S'} \in \mathsf{GL}_k(\mathbb{F}_q)$, $\mathbf{C} \in \mathbb{S}_m(\mathbb{F}_q)$ and $\mathbf{D} \in \mathbb{S}_n(\mathbb{F}_q)$ such that $\mathbf{G_1} = \mathbf{S'G_2}(\mathbf{C}^\top \otimes \mathbf{D})$.

Remark 1. In [KLP26], the problem is stated for codes: given $\mathcal{D}_1 = \mathbf{A}\mathcal{D}_0\mathbf{B}^\top$ and $\mathcal{D}_2 = \mathbf{A}^{-1}\mathcal{D}_0\mathbf{B}^{-\top}$, find $(\mathbf{C}, \mathbf{D})$ with $\mathcal{D}_1 = \mathbf{C}\mathcal{D}_2\mathbf{D}^\top$, and generator matrices are in systematic form. Definition 5 is its translation to generator matrices (with the isometry written as $\mathbf{A}^\top \otimes \mathbf{B}$), in which $\mathbf{S_1}$ and $\mathbf{S_2}$ are arbitrary and unrelated. The same holds for all the definitions above: the algorithm of Section 3 is invariant under changes of generator matrices (see Remark 3), so that it solves the problems about codes.

2.3 Duality for Equivalent Matrix Codes

This section collects new definitions and results relating equivalent matrix codes to their duals; unlike Section 2, its content is new.

Let $\mathcal{D}$ be a $(m \times n, k)$ matrix code and $\mathbf{G} \in \mathbb{F}_q^{k \times mn}$ be the generator matrix of $\mathcal{D}$. We define the *rate* of the code $\mathcal{D}$ as the quantity $\delta = \frac{k}{mn}$. Furthermore, we define the parity-check matrix of $\mathcal{D}$ as the matrix $\mathbf{H} \in \mathbb{F}_q^{(mn-k) \times mn}$ such that $\mathbf{Hd} = \mathbf{0}$ for each $\mathbf{d} \in \mathsf{vec}(\mathcal{D})$. The parity-check matrix generates the dual code of $\mathsf{vec}(\mathcal{D})$, and thus we define the dual code of $\mathcal{D}$ as the $(m \times n, mn - k)$ matrix code $\mathcal{D}^\perp$ isomorphic to the code generated by the parity check matrix $\mathbf{H}$. We present in Lemma 1 and Corollary 1 the relation between the parity-check matrices of two equivalent matrix codes.

Lemma 1. *Let $\mathbf{G_0}, \mathbf{G_1} \in \mathbb{F}_q^{k \times mn}$ be generator matrices of two equivalent $(m \times n, k)$-matrix codes $\mathcal{D}_0, \mathcal{D}_1$ respectively; that is, there exist matrices $\mathbf{S} \in \mathsf{GL}_k(\mathbb{F}_q)$, $\mathbf{A} \in \mathsf{GL}_m(\mathbb{F}_q)$ and $\mathbf{B} \in \mathsf{GL}_n(\mathbb{F}_q)$ such that $\mathbf{G_1} = \mathbf{S G_0}(\mathbf{A}^\top \otimes \mathbf{B})$. Let $\mathbf{H_0}, \mathbf{H_1}$ be the parity-check matrices of $\mathcal{D}_0, \mathcal{D}_1$ respectively. Then, $\mathbf{H_1} = \mathbf{R H_0}(\mathbf{A}^{-1} \otimes \mathbf{B}^{-\top})$ holds for some $\mathbf{R} \in \mathsf{GL}_{mn-k}(\mathbb{F}_q)$.*

Proof. By definition, the parity-check matrices $\mathbf{H_0}$ and $\mathbf{H_1}$ satisfy $\mathbf{H_0 G_0}^\top = \mathbf{0}$ and $\mathbf{H_1 G_1}^\top = \mathbf{0}$. Notice that the matrix $\mathbf{H} = \mathbf{H_0}(\mathbf{A}^{-1} \otimes \mathbf{B}^{-\top}) \in \mathbb{F}_q^{(mn-k) \times mn}$ has rank

$(mn-k)$, and

$$\begin{aligned}\mathbf{H}\mathbf{G_1}^\top &= \big(\mathbf{H_0}(\mathbf{A}^{-1}\otimes\mathbf{B}^{-\top})\big)\big(\mathbf{S}\mathbf{G_0}(\mathbf{A}^\top\otimes\mathbf{B})\big)^\top\\ &= \big(\mathbf{H_0}(\mathbf{A}^{-1}\otimes\mathbf{B}^{-\top})\big)\big((\mathbf{A}\otimes\mathbf{B}^\top)\mathbf{G_0}^\top\mathbf{S}^\top\big)\\ &= \mathbf{H_0}(\mathbf{I}_m\otimes\mathbf{I}_n)\mathbf{G_0}^\top\mathbf{S}^\top = \mathbf{H_0}\mathbf{I}_{mn}\mathbf{G_0}^\top\mathbf{S}^\top\\ &= \mathbf{H_0}\mathbf{G_0}^\top\mathbf{S}^\top = \mathbf{0}.\end{aligned}$$

In other words, $\mathbf{H}$ is a generator matrix of dual code $\mathcal{D}_1^\perp$. Hence, there exists $\mathbf{R}\in\mathsf{GL}_{mn-k}(\mathbb{F}_q)$ such that $\mathbf{H_1}=\mathbf{R}\mathbf{H_0}(\mathbf{A}^{-1}\otimes\mathbf{B}^{-\top})$.

□

Corollary 1. *Let $\mathcal{D}_0,\mathcal{D}_1$ be two equivalent $(m\times n,k)$-matrix codes; that is, there exist two matrices $\mathbf{A}\in\mathsf{GL}_m(\mathbb{F}_q)$ and $\mathbf{B}\in\mathsf{GL}_n(\mathbb{F}_q)$ such that $\mathcal{D}_1=\mathbf{A}\mathcal{D}_0\mathbf{B}$. Then, $\mathcal{D}_1^\perp=\mathbf{A}^{-\top}\mathcal{D}_0^\perp\mathbf{B}^{-\top}$, where $\mathcal{D}_0^\perp$ and $\mathcal{D}_1^\perp$ are $(m\times n,mn-k)$-matrix codes. Equivalently, in terms of the Kronecker product, if $\mathbf{H_0},\mathbf{H_1}\in\mathbb{F}_q^{(mn-k)\times mn}$ are parity-check matrices of $\mathcal{D}_0,\mathcal{D}_1$, then $\mathbf{H_1}=\mathbf{R}\mathbf{H_0}(\mathbf{A}^{-1}\otimes\mathbf{B}^{-\top})$ for some $\mathbf{R}\in\mathsf{GL}_{mn-k}(\mathbb{F}_q)$.*

Proof. The proof follows from the equivalence given by Lemma 1, which is shown in terms of Kronecker product: for any $\mathbf{M}\in\mathbb{F}_q^{m\times n}$, we have $\mathsf{vec}(\mathbf{M})^\top(\mathbf{A}^{-1}\otimes\mathbf{B}^{-\top})=\mathsf{vec}(\mathbf{A}^{-\top}\mathbf{M}\mathbf{B}^{-\top})^\top$, so the rows of $\mathbf{H_0}(\mathbf{A}^{-1}\otimes\mathbf{B}^{-\top})$ are the vectorizations of a basis of $\mathbf{A}^{-\top}\mathcal{D}_0^\perp\mathbf{B}^{-\top}$. □

Remark 2 (On the relation between $\mathbf{R}$ and $\mathbf{S}$). The matrix $\mathbf{R}$ of Lemma 1 does not depend on $\mathbf{S}$: replacing $\mathbf{G_1}$ by $\mathbf{T}\mathbf{G_1}$ for any $\mathbf{T}\in\mathsf{GL}_k(\mathbb{F}_q)$ changes neither $\mathcal{D}_1$ nor $\mathcal{D}_1^\perp$, hence it does not change the admissible parity-check matrices $\mathbf{H_1}$. Instead, $\mathbf{R}$ only reflects the choice of a basis of $\mathcal{D}_1^\perp$: replacing $\mathbf{H_1}$ by $\mathbf{T}\mathbf{H_1}$ with $\mathbf{T}\in\mathsf{GL}_{mn-k}(\mathbb{F}_q)$ replaces $\mathbf{R}$ by $\mathbf{T}\mathbf{R}$, and the choice $\mathbf{H_1}=\mathbf{H_0}(\mathbf{A}^{-1}\otimes\mathbf{B}^{-\top})$ gives $\mathbf{R}=\mathbf{I}_{mn-k}$. Hence, there is no intrinsic relation between $\mathbf{S}$ (a change of basis of $\mathcal{D}_1$) and $\mathbf{R}$ (a change of basis of $\mathcal{D}_1^\perp$). A consequence is that the dual of a 2-MCE instance is not, in general, a 2-MCE instance: applying Lemma 1 to the pairs $(\mathbf{G_0},\mathbf{G_1})$ and $(\mathbf{G_2},\mathbf{G_3})$ provides two matrices $\mathbf{R}$ and $\mathbf{R}'$ that need not coincide.

We highlight that Corollary 1 illustrates a different result from [CL25, Lemma 2] since our definition of the dual code focuses on the generator matrix, which differs from the definition in [CL25]. For example, [CL25, Lemma 2] allows us to swap the usage of the matrices $\mathbf{A}$ and $\mathbf{B}$ in the code equivalence relation between two $(n\times m,k)$-matrix codes $\tilde{\mathcal{D}}_0$ and $\tilde{\mathcal{D}}_1$, more precisely, $\tilde{\mathcal{D}}_1=\mathbf{B}^{-\top}\tilde{\mathcal{D}}_0\mathbf{A}^{-\top}$. In the tensor product notation, this means an equivalence determined by $\mathbf{B}^{-1}\otimes\mathbf{A}^{-\top}$ instead of $\mathbf{A}^\top\otimes\mathbf{B}$. We show in Corollary 2 which $(n\times m,k)$-matrix codes allow a result similar to [CL25, Lemma 2], that is, that swaps the usage of the matrices $\mathbf{A}$ and $\mathbf{B}$ in the code equivalence. Figure 2 summarizes the code equivalences that Corollaries 1 and 2 imply.

Corollary 2. *Let $\mathcal{D}_0,\mathcal{D}_1$ be two equivalent $(m\times n,k)$-matrix codes; that is, there exist two matrices $\mathbf{A}\in\mathsf{GL}_m(\mathbb{F}_q)$ and $\mathbf{B}\in\mathsf{GL}_n(\mathbb{F}_q)$ such that $\mathcal{D}_1=\mathbf{A}\mathcal{D}_0\mathbf{B}$. Let $\mathbf{G_0}$ and $\mathbf{G_1}\in\mathbb{F}_q^{k\times mn}$ be the generator matrices of $\mathcal{D}_0$ and $\mathcal{D}_1$, respectively. Let $\hat{\mathbf{G}}_\mathbf{i}=\mathbf{G_i}\mathbf{K}_{m,n}$ where $\mathbf{K}_{m,n}$ denotes the commutation matrix and $i\in\{0,1\}$. Let $\hat{\mathcal{D}}_0$ and $\hat{\mathcal{D}}_1$ be the $(n\times m,k)$-matrix codes with generator matrices $\hat{\mathbf{G}}_\mathbf{0}$ and $\hat{\mathbf{G}}_\mathbf{1}$, respectively. Then, $\hat{\mathcal{D}}_1=\mathbf{B}^\top\hat{\mathcal{D}}_0\mathbf{A}^\top$.*

Proof. Recall that $\mathbf{A}^\top\otimes\mathbf{B}=\mathbf{K}_{m,n}\mathbf{B}\otimes\mathbf{A}^\top(\mathbf{K}_{m,n})^\top$ holds, where $\mathbf{K}_{m,n}$ denotes the commutation matrix. Since $\mathbf{G_1}=\mathbf{S}\mathbf{G_0}(\mathbf{A}^\top\otimes\mathbf{B})$ for some matrix $\mathbf{S}\in\mathsf{GL}_k(\mathbb{F}_q)$, we find that $\mathbf{G_1}\mathbf{K}_{m,n}=\mathbf{S}(\mathbf{G_0}\mathbf{K}_{m,n})(\mathbf{B}\otimes\mathbf{A}^\top)$ holds. Hence, $\hat{\mathbf{G}}_\mathbf{1}=\mathbf{S}\hat{\mathbf{G}}_\mathbf{0}(\mathbf{B}\otimes\mathbf{A}^\top)$, which is equivalent to $\hat{\mathcal{D}}_1=\mathbf{B}^\top\hat{\mathcal{D}}_0\mathbf{A}^\top$.

□

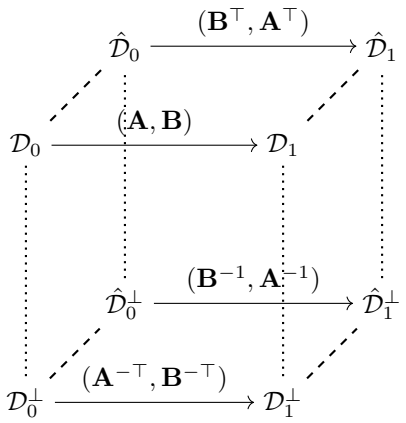

Figure 2: Code Equivalence Diagram determined by Corollaries 1 and 2: $\mathcal{D}_0, \mathcal{D}_1$ are two equivalent $(m \times n, k)$-matrix codes; that is, there exist two matrices $\mathbf{A} \in \mathsf{GL}_m(\mathbb{F}_q)$ and $\mathbf{B} \in \mathsf{GL}_n(\mathbb{F}_q)$ such that $\mathcal{D}_1 = \mathbf{A}\mathcal{D}_0\mathbf{B}$. Here, $\hat{\mathcal{D}}_0$ and $\hat{\mathcal{D}}_1$ denote the $(n \times m, k)$-matrix codes from Corollary 2. In addition, $\mathcal{D}_0^\perp$ and $\mathcal{D}_1^\perp$ determine the $(m \times n, mn - k)$-matrix dual codes of $\mathcal{D}_0$ and $\mathcal{D}_1$, while $\hat{\mathcal{D}}_0^\perp$ and $\hat{\mathcal{D}}_1^\perp$ the $(n \times m, mn - k)$-matrix dual codes of $\hat{\mathcal{D}}_0$ and $\hat{\mathcal{D}}_1$. The horizontal edges describe the code equivalence determined by specific pairs of matrices.

3 On Weak Instances of the 2-MCE problem

Throughout this section, $(\mathbf{S_1}, \mathbf{S_2}, \mathbf{A}, \mathbf{B})$ denotes a solution of a 2-sMCE instance

$$(\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2}, \mathbf{G_3}) \in (\mathbb{F}_q^{k \times mn})^4,$$

i.e., $\mathbf{G_1} = \mathbf{S_1}\mathbf{G_0}\mathbf{Q}$ and $\mathbf{G_3} = \mathbf{S_2}\mathbf{G_2}\mathbf{Q}$ with $\mathbf{Q} = \mathbf{A}^\top \otimes \mathbf{B}$, $\mathbf{A}^\top = \epsilon_A\mathbf{A}$, $\mathbf{B}^\top = \epsilon_B\mathbf{B}$, and $\mathbf{Q}^\top = \epsilon\mathbf{Q}$ with $\epsilon = \epsilon_A\epsilon_B$. We write $\mathbf{U_1} = \mathbf{S_1}^{-1}$ and $\mathbf{U_2} = \mathbf{S_2}^{-1}$, and $\mathbf{D}_r = \mathsf{vec}^{-1}(r\text{-th row of } \mathbf{G_0}) \in \mathbb{F}_q^{m \times n}$, $\mathbf{D}'_r = \mathsf{vec}^{-1}(r\text{-th row of } \mathbf{G_2}) \in \mathbb{F}_q^{m \times n}$, so that $\mathcal{D}_0 = \langle \mathbf{D}_1, \ldots, \mathbf{D}_k \rangle$ and $\mathcal{D}_2 = \langle \mathbf{D}'_1, \ldots, \mathbf{D}'_k \rangle$. Recall that $\mathsf{vec}(\mathbf{M})^\top\mathbf{Q} = \mathsf{vec}(\mathbf{AMB})^\top$ for every $\mathbf{M} \in \mathbb{F}_q^{m \times n}$, so that $\mathbf{G_1} = \mathbf{S_1}\mathbf{G_0}\mathbf{Q}$ is the matrix form of $\mathcal{D}_1 = \mathbf{A}\mathcal{D}_0\mathbf{B}$. We discuss the correctness of our algorithm in Figure 1 below.

3.1 On the Details of Step 1 in Figure 1

The key observation is that the three $k \times k$ matrices

$$\mathbf{P}_0 = \mathbf{G_0}\mathbf{Q}\mathbf{G_0}^\top, \qquad \mathbf{P}_2 = \mathbf{G_2}\mathbf{Q}\mathbf{G_2}^\top, \qquad \mathbf{N} = \mathbf{G_0}\mathbf{Q}\mathbf{G_2}^\top, \tag{1}$$

i.e., the Gram matrices of the ϵ-symmetric bilinear form $\mathbf{Q}$ on the rows of $\mathbf{G_0}$ and $\mathbf{G_2}$, can be expressed through the public products $\mathbf{G_i}\mathbf{G_j}^\top$ and the unknown changes of basis only, and that $\mathbf{P}_0, \mathbf{P}_2$ are ϵ-symmetric while $\mathbf{G_2}\mathbf{Q}\mathbf{G_0}^\top = \epsilon\mathbf{N}^\top$.

Lemma 2. *We have*

$$\mathbf{U_1}\mathbf{G_1}\mathbf{G_0}^\top = \mathbf{P}_0, \qquad \mathbf{U_2}\mathbf{G_3}\mathbf{G_2}^\top = \mathbf{P}_2, \qquad \mathbf{U_1}\mathbf{G_1}\mathbf{G_2}^\top = \mathbf{N}, \qquad \mathbf{U_2}\mathbf{G_3}\mathbf{G_0}^\top = \epsilon\mathbf{N}^\top.$$

Consequently, $(\mathbf{U_1}, \mathbf{U_2})$ *satisfies the linear equations*

$$\mathbf{U_1}\mathbf{G_1}\mathbf{G_0}^\top = \epsilon\,\mathbf{G_0}\mathbf{G_1}^\top\mathbf{U_1}^\top, \tag{2}$$

$$\mathbf{U_2}\mathbf{G_3}\mathbf{G_2}^\top = \epsilon\,\mathbf{G_2}\mathbf{G_3}^\top\mathbf{U_2}^\top, \tag{3}$$

$$\mathbf{U_2}\mathbf{G_3}\mathbf{G_0}^\top = \epsilon\,\mathbf{G_2}\mathbf{G_1}^\top\mathbf{U_1}^\top. \tag{4}$$

Proof. The four identities follow from $\mathbf{U_1G_1} = \mathbf{G_0Q}$ and $\mathbf{U_2G_3} = \mathbf{G_2Q}$, together with $(\mathbf{G_0QG_2}^\top)^\top = \mathbf{G_2Q}^\top\mathbf{G_0}^\top = \epsilon\,\mathbf{G_2QG_0}^\top$. Equations Equation (2) and Equation (3) state that $\mathbf{P}_0$ and $\mathbf{P}_2$ are ϵ-symmetric, i.e., $\mathbf{P}_0 = \epsilon\mathbf{P}_0^\top = \epsilon(\mathbf{U_1G_1G_0}^\top)^\top$; equation Equation (4) states that $\mathbf{U_2G_3G_0}^\top = \epsilon\mathbf{N}^\top = \epsilon(\mathbf{U_1G_1G_2}^\top)^\top$. □

The next proposition describes the solution space of the above linear system.

Proposition 1. *Let*

$$\mathcal{K} = \left\{(\mathbf{C_1}, \mathbf{C_2}) \in (\mathbb{F}_q^{k\times k})^2 \colon \mathbf{C_1P}_0 \in \mathcal{S}_\epsilon(k),\ \mathbf{C_2P}_2 \in \mathcal{S}_\epsilon(k),\ \mathbf{C_2N}^\top = \mathbf{N}^\top\mathbf{C_1}^\top\right\}.$$

The map $(\mathbf{C_1}, \mathbf{C_2}) \mapsto (\mathbf{C_1U_1}, \mathbf{C_2U_2})$ *is a linear bijection from* $\mathcal{K}$ *onto the solution space of Equation (2)–Equation (4). In particular, this solution space has dimension* $d = \dim\mathcal{K}$*, it contains* $(\mathbf{U_1}, \mathbf{U_2})$ *(the image of* $(\mathbf{I}_k, \mathbf{I}_k)$*), and*

$$d \geq \max\{1, \epsilon k\} = \begin{cases} k & \text{if } \epsilon = 1, \\ 1 & \text{if } \epsilon = -1. \end{cases}$$

Proof. Consider an arbitrary pair $(\mathbf{C_1U_1}, \mathbf{C_2U_2})$. By Lemma 2, $\mathbf{C_1U_1G_1G_0}^\top = \mathbf{C_1P}_0$ and $\mathbf{G_0G_1}^\top\mathbf{U_1}^\top\mathbf{C_1}^\top = (\mathbf{C_1P}_0)^\top$, so Equation (2) holds if and only if $\mathbf{C_1P}_0 = \epsilon(\mathbf{C_1P}_0)^\top$. Similarly, Equation (3) holds if and only if $\mathbf{C_2P}_2 \in \mathcal{S}_\epsilon(k)$. Finally, $\mathbf{C_2U_2G_3G_0}^\top = \epsilon\,\mathbf{C_2N}^\top$ and $\epsilon\,\mathbf{G_2G_1}^\top\mathbf{U_1}^\top\mathbf{C_1}^\top = \epsilon(\mathbf{C_1N})^\top = \epsilon\,\mathbf{N}^\top\mathbf{C_1}^\top$, so Equation (4) holds if and only if $\mathbf{C_2N}^\top = \mathbf{N}^\top\mathbf{C_1}^\top$. The map is linear and bijective. For the lower bound, $\mathcal{K}$ is the solution space of a homogeneous linear system in $2k^2$ unknowns: requiring a $k \times k$ matrix to be ϵ-symmetric imposes $k^2 - d_\epsilon(k) = \frac{1}{2}k(k-\epsilon)$ linear equations, and the last condition imposes k^2 equations; hence $\dim\mathcal{K} \geq 2k^2 - k(k-\epsilon) - k^2 = \epsilon k$, and $\dim\mathcal{K} \geq 1$ since $(\mathbf{I}_k, \mathbf{I}_k) \in \mathcal{K}$. □

Thus, Step 1 determines $(\mathbf{U_1}, \mathbf{U_2})$ up to d unknown coefficients:

$$(\mathbf{U_1}, \mathbf{U_2}) = \sum_{j=1}^{d} \lambda_j(\mathbf{U_{1,j}}, \mathbf{U_{2,j}}) \qquad \text{for some } \lambda_1, \ldots, \lambda_d \in \mathbb{F}_q.$$

In our experiments (Section 4.2), the lower bound of Proposition 1 is attained when $\epsilon = 1$, i.e., $d = k$, while $d = \lceil k/2 \rceil$ when $\epsilon = -1$; we state this as Heuristic 1 in Section 3.3. The crucial point is that d is small, of the order of k, whereas the unknowns of the problem are the $2k^2 + m^2 + n^2$ entries of $(\mathbf{S_1}, \mathbf{S_2}, \mathbf{A}, \mathbf{B})$.

Remark 3. If $\mathbf{G_1}$ is replaced by $\mathbf{TG_1}$ for some $\mathbf{T} \in \mathsf{GL}_k(\mathbb{F}_q)$ (another generator matrix of the same code), then $\mathbf{S_1}$ is replaced by $\mathbf{TS_1}$, and the solution space of Equation (2)–Equation (4) is replaced by its image under $(\mathbf{U_1}, \mathbf{U_2}) \mapsto (\mathbf{U_1T}^{-1}, \mathbf{U_2})$; the same holds for the other three generator matrices. Step 2 below transforms accordingly. Hence the algorithm depends only on the four codes, and the choice of generator matrices (e.g., systematic forms) is immaterial.

3.2 On the Details of Step 2 in Figure 1

Once a basis of the solution space of Step 1 is known, the relations $\mathbf{U_1G_1} = \mathbf{G_0Q}$ and $\mathbf{U_2G_3} = \mathbf{G_2Q}$ are the only ones left. Multiplying by $\mathbf{A}^{-\top} \otimes \mathbf{I}_n$ on the right,

$$\mathbf{U_1G_1}(\mathbf{A}^{-\top} \otimes \mathbf{I}_n) = \mathbf{G_0}(\mathbf{I}_m \otimes \mathbf{B}), \qquad \mathbf{U_2G_3}(\mathbf{A}^{-\top} \otimes \mathbf{I}_n) = \mathbf{G_2}(\mathbf{I}_m \otimes \mathbf{B}),$$

which, written row by row using $\mathsf{vec}(\mathbf{M})^\top(\mathbf{X} \otimes \mathbf{I}_n) = \mathsf{vec}(\mathbf{X}^\top\mathbf{M})^\top$ and $\mathsf{vec}(\mathbf{M})^\top(\mathbf{I}_m \otimes \mathbf{Y}) = \mathsf{vec}(\mathbf{MY})^\top$, gives

$$\mathbf{X}^\top\mathbf{W}_r = \mathbf{D}_r\mathbf{Y}, \qquad \mathbf{X}^\top\mathbf{W}'_r = \mathbf{D}'_r\mathbf{Y}, \qquad r = 1, \ldots, k, \tag{5}$$

with $\mathbf{X} = \mathbf{A}^{-\top}$, $\mathbf{Y} = \mathbf{B}$, and $\mathbf{W}_r, \mathbf{W}'_r$ the r-th rows of $\mathbf{U_1G_1}$ and $\mathbf{U_2G_3}$ reshaped as $m \times n$ matrices. Since $\mathbf{U_1G_1} = \sum_j \lambda_j \mathbf{U_{1,j}G_1}$, we have $\mathbf{W}_r = \sum_j \lambda_j \mathbf{W}_{j,r}$ and $\mathbf{W}'_r = \sum_j \lambda_j \mathbf{W}'_{j,r}$ with the notation of Figure 1, so that Equation (5) is bilinear in $(\lambda_1, \ldots, \lambda_d)$ and $\mathbf{X}$, and linear in $\mathbf{Y}$. The coefficients λ_j only occur in the products $\lambda_j \mathbf{X}$, so that Equation (5) could be linearised with the d matrices $\lambda_j \mathbf{X}$ as unknowns; this gives $d \cdot d_{\epsilon_A}(m) + d_{\epsilon_B}(n)$ unknowns, of the order of $n^4/2$ for $k = m = n$. We use a cheaper linearisation: multiplying Equation (5) on the left by a vector $\mathbf{u}_i^\top \in \mathbb{F}_q^{1\times m}$ gives

$$\sum_{j=1}^{d} \mathbf{v}_{i,j}^\top \mathbf{W}_{j,r} = \mathbf{u}_i^\top \mathbf{D}_r \mathbf{Y}, \qquad \sum_{j=1}^{d} \mathbf{v}_{i,j}^\top \mathbf{W}'_{j,r} = \mathbf{u}_i^\top \mathbf{D}'_r \mathbf{Y}, \qquad \mathbf{v}_{i,j} = \lambda_j \mathbf{X}\mathbf{u}_i, \tag{6}$$

which is linear in the d vectors $\mathbf{v}_{i,j} \in \mathbb{F}_q^m$ and in $\mathbf{Y} \in \mathcal{S}_{\epsilon_B}(n)$. With t vectors $\mathbf{u}_1, \ldots, \mathbf{u}_t$, this is the linear system of Step 2: it has $2knt$ equations and $tdm + d_{\epsilon_B}(n)$ unknowns. For each i, the vectors $\mathbf{v}_{i,1}, \ldots, \mathbf{v}_{i,d}$ are all multiples of $\mathbf{X}\mathbf{u}_i$, which is how the coefficients λ_j are read off; once λ and $\mathbf{Y}$ are known, Equation (5) is linear in $\mathbf{X}$, which is Step 3.

Proposition 2. *The tuple* $\big((\lambda_j \mathbf{A}^{-\top}\mathbf{u}_i)_{i\le t,\, j\le d}, \mathbf{B}\big)$ *is a nonzero solution of the linear system of Step 2. Assume that this solution space is one-dimensional and that the matrix* $[\mathbf{D}_1 \mid \cdots \mid \mathbf{D}_k] \in \mathbb{F}_q^{m\times kn}$ *has rank* m*. Then the algorithm in Figure 1 returns*

$$\big(\nu\mathbf{S_1},\ \nu\mathbf{S_2},\ (\mu\nu)^{-1}\mathbf{A},\ \mu\mathbf{B}\big) \qquad \text{for some } \mu, \nu \in \mathbb{F}_q^*,$$

which is a solution of the 2-sMCE instance whose last two matrices have the symmetry types of $\mathbf{A}$ *and* $\mathbf{B}$*.*

Proof. The first claim is the derivation above, read backwards: the r-th row of $\mathbf{U_1G_1} = \mathbf{G_0Q}$ is $\mathsf{vec}(\mathbf{AD_rB})^\top$, so $\mathbf{W}_r = \mathbf{AD}_r\mathbf{B}$ and $\sum_j (\lambda_j \mathbf{A}^{-\top}\mathbf{u}_i)^\top \mathbf{W}_{j,r} = \mathbf{u}_i^\top \mathbf{A}^{-1}\mathbf{W}_r = \mathbf{u}_i^\top \mathbf{D}_r\mathbf{B}$; similarly for $\mathbf{W}'_r$. If the solution space is one-dimensional, the computed tuple is $c\,\big((\lambda_j \mathbf{A}^{-\top}\mathbf{u}_i)_{i,j}, \mathbf{B}\big)$ for some $c \in \mathbb{F}_q^*$. Then $\mathbf{v}_{i_0,j} = \lambda_j\,(c\mathbf{A}^{-\top}\mathbf{u}_{i_0})$ for all j, with $\mathbf{v}_{i_0,j_0} \neq \mathbf{0}$, so the ratios λ_j/λ_{j_0} are recovered exactly, $(\mathbf{U_1}, \mathbf{U_2})$ computed in Step 3 equals $\lambda_{j_0}^{-1}(\mathbf{S_1}^{-1}, \mathbf{S_2}^{-1})$, and $\mathbf{Y} = c\mathbf{B}$. Hence $\mathbf{W}_r = \lambda_{j_0}^{-1}\mathbf{AD}_r\mathbf{B}$ in Step 3, and the system $\mathbf{X}^\top\mathbf{W}_r = \mathbf{D}_r\mathbf{Y}$ reads $(\mathbf{X}^\top\mathbf{A} - c\lambda_{j_0}\mathbf{I}_m)\mathbf{D}_r\mathbf{B} = \mathbf{0}$ for $r = 1, \ldots, k$; since $[\mathbf{D}_1 | \cdots | \mathbf{D}_k]$ has rank m, its unique solution is $\mathbf{X}^\top = c\lambda_{j_0}\mathbf{A}^{-1}$, which lies in $\mathcal{S}_{\epsilon_A}(m)$. With $\nu = \lambda_{j_0}$ and $\mu = c$, the returned matrices are $(\nu\mathbf{S_1}, \nu\mathbf{S_2}, (\mu\nu)^{-1}\mathbf{A}, \mu\mathbf{B})$; they satisfy $((\mu\nu)^{-1}\mathbf{A})^\top \otimes (\mu\mathbf{B}) = \nu^{-1}\mathbf{Q}$, hence $(\nu\mathbf{S_1})\mathbf{G_0}(\nu^{-1}\mathbf{Q}) = \mathbf{G_1}$ and $(\nu\mathbf{S_2})\mathbf{G_2}(\nu^{-1}\mathbf{Q}) = \mathbf{G_3}$, and the symmetry types are preserved by scalar multiplication. □

Remark 4. Both pairs are needed in Step 2: the first pair alone gives knt equations, which is less than the number $tdm + d_{\epsilon_B}(n)$ of unknowns when $d = k$ and $m = n$. When $m > n$, the roles of $\mathbf{A}$ and $\mathbf{B}$ (and hence of m and n in the size of the system) are exchanged by applying the algorithm to the transposed codes of Corollary 2; we assume $n \geq m$ from now on.

3.3 Complexity and Success Probability of the Algorithm

By Propositions 1 and 2, the algorithm in Figure 1 succeeds when the following conditions hold for the input instance and the chosen vectors $\mathbf{u}_i$:

(C1) the linear system of Step 2, built from a basis of the solution space of Step 1, has a one-dimensional solution space;

(C2) the matrix $[\mathbf{D}_1 | \cdots | \mathbf{D}_k]$ has rank m, i.e., no nonzero vector $\mathbf{x} \in \mathbb{F}_q^m$ satisfies $\mathbf{x}^\top\mathbf{D} = \mathbf{0}$ for all $\mathbf{D} \in \mathcal{D}_0$.

Condition (C1) does not depend on the chosen basis in Step 1 (a change of basis of the $(\mathbf{U_{1,j}}, \mathbf{U_{2,j}})$ induces an invertible linear change of the unknowns $\mathbf{v}_{i,j}$), and it requires $2knt \geq tdm + d_{\epsilon_B}(n) - 1$, which is possible if and only if $2kn > dm$; the value of t in Figure 1 is the smallest one satisfying this inequality. Condition (C2) is a property of the code $\mathcal{D}_0$ alone: for a uniformly random $\mathbf{G_0}$, a union bound over the nonzero $\mathbf{x}$ shows that it fails with probability at most $q^{m-kn} \leq q^{-1}$.

Theorem 1. *Let $(\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2}, \mathbf{G_3})$ be an instance of the 2-sMCE problem with a solution $(\mathbf{S_1}, \mathbf{S_2}, \mathbf{A}, \mathbf{B})$, and assume that (C1) and (C2) hold. Then the algorithm in Figure 1 returns a valid solution of the form $(\nu\mathbf{S_1}, \nu\mathbf{S_2}, (\mu\nu)^{-1}\mathbf{A}, \mu\mathbf{B})$ for some $\mu, \nu \in \mathbb{F}_q^*$, with a time complexity of*

$$\mathcal{O}\left(k^2mn + k^6 + dk^2mn + tkn\,(tdm + n^2)^2\right)$$

operations in $\mathbb{F}_q$, where $d \leq 2k^2$ is the dimension computed in Step 1 and t is the number of projections of Step 2; for $d = O(k)$ and $k = m = n$, where $t = 1$, this is $\mathcal{O}(n^6)$.

Proof. Correctness follows from Proposition 2, so we focus on determining the time complexity of the algorithm. Computing the products $\mathbf{G_i}\mathbf{G_j}^\top$ costs $\mathcal{O}(k^2mn)$ operations. The system of Step 1 has $3k^2$ rows and $2k^2$ columns, so Gaussian elimination costs $\mathcal{O}(k^6)$. Building the system of Step 2 requires the products $\mathbf{U_{1,j}}\mathbf{G_1}$ and $\mathbf{U_{2,j}}\mathbf{G_3}$, $\mathcal{O}(dk^2mn)$ operations, and solving it costs $\mathcal{O}(tkn(tdm + n^2)^2)$ since it has $2knt$ rows and at most $tdm + n^2$ columns. Step 3 amounts to solving $[\mathbf{W}_1|\cdots|\mathbf{W}_k]^\top\mathbf{X} = [\mathbf{D}_1\mathbf{Y}|\cdots|\mathbf{D}_k\mathbf{Y}]^\top$, a system with kn equations and m unknowns for each of the m columns of $\mathbf{X}$, in $\mathcal{O}(knm^2)$ operations; the remaining inversions cost $\mathcal{O}(k^3 + m^3 + n^3)$. □

Random instances. For given (k, m, n, q) and admissible signs (ϵ_A, ϵ_B), we consider the following two distributions of instances:

- $\mathcal{R}_{\text{2-sMCE}}$: $\mathbf{S_1}, \mathbf{S_2}$ are uniform and independent in $\mathsf{GL}_k(\mathbb{F}_q)$, $\mathbf{A}$ (resp. $\mathbf{B}$) is uniform among the invertible matrices of $\mathcal{S}_{\epsilon_A}(m)$ (resp. $\mathcal{S}_{\epsilon_B}(n)$), $\mathbf{G_0}$ and $\mathbf{G_2}$ are uniform and independent full-rank $k \times mn$ matrices, $\mathbf{G_1} = \mathbf{S_1}\mathbf{G_0}\mathbf{Q}$ and $\mathbf{G_3} = \mathbf{S_2}\mathbf{G_2}\mathbf{Q}$;
- $\mathcal{R}_{\mathsf{slMCE}}$: $\mathbf{S_1}, \mathbf{S_2}, \mathbf{A}, \mathbf{B}, \mathbf{G_0}$ as above, $\mathbf{G_1} = \mathbf{S_1}\mathbf{G_0}\mathbf{Q}$, $\mathbf{G_2} = \mathbf{S_2}\mathbf{G_0}\mathbf{Q}^{-1}$, and the instance is $(\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2}, \mathbf{G_0})$; by Remark 3, this is also the distribution of the public keys of [KLP26] (Section 4).

We state the expected behaviour of the two linear systems on random instances as heuristics, which we support experimentally in Section 4.2; the constants hidden in the $O(\cdot)$ notation depend only on (k, m, n).

Heuristic 1. *For instances sampled from $\mathcal{R}_{\text{2-sMCE}}$ or $\mathcal{R}_{\mathsf{slMCE}}$, with probability $1 - O(1/q)$, the dimension d computed in Step 1 equals k if $\epsilon = 1$ and $\lceil k/2 \rceil$ if $\epsilon = -1$.*

Heuristic 2. *Let $k \geq 2$, $n \geq m$, and d as in Heuristic 1, so that $2kn > dm$. For instances sampled from $\mathcal{R}_{\text{2-sMCE}}$ or $\mathcal{R}_{\mathsf{slMCE}}$ and uniformly random projection vectors $\mathbf{u}_1, \ldots, \mathbf{u}_t$, condition (C1) holds with probability $1 - O(1/q)$.*

Theorem 2. *Let $k \geq 2$, $n \geq m$, and $d = k$ if $\epsilon = 1$, $d = \lceil k/2 \rceil$ if $\epsilon = -1$. For instances sampled from $\mathcal{R}_{\text{2-sMCE}}$ or $\mathcal{R}_{\mathsf{slMCE}}$ and under Heuristics 1 and 2, the algorithm in Figure 1 returns a solution with probability $1 - O(1/q)$, using $\mathcal{O}\left(k^2mn + k^6 + dk^2mn + tkn(tdm + n^2)^2\right)$ operations in $\mathbb{F}_q$ with $t \leq \lceil (n+1)/(2k) \rceil$; for $k = m = n$, $t = 1$ and the cost is $\mathcal{O}(n^6)$.*

Proof. Since $d \leq k$ and $m \leq n$, we have $dm \leq kn < 2kn$, so t is well defined and $t \leq \lceil (d_{\epsilon_B}(n) - 1)/(kn) \rceil \leq \lceil (n+1)/(2k) \rceil$; for $k = m = n$, $2n^2 \geq n^2 + \frac{n(n+1)}{2} - 1$ gives $t = 1$. By Theorem 1, the algorithm fails only if (C1) or (C2) fails; the former happens with probability $O(1/q)$ by Heuristic 2 (whose hypothesis is satisfied since d has the value of Heuristic 1 with probability $1 - O(1/q)$), and the latter with probability at most $q^{m-kn} \leq 1/q$. □

Consequences for the design of schemes. Under these heuristics, the (skew) symmetric structure makes the 2-MCE problem easy for all parameters: every shape (k, m, n) with $k \geq 2$ is covered (up to exchanging m and n), including the square matrix codes of the MCE-based schemes [CNP+23, BBMP24, KLP26] and the codes in systematic form used in practice, at a cost of $\mathcal{O}(n^6)$ field operations for $k = m = n$. The field size only affects the failure probability, which is $O(1/q)$. We therefore recommend not to rely on 2-MCE-type assumptions with (skew) symmetric secret isometries.

4 Cryptographic Implications

In this section, we explain how the public key of the blind signature scheme of Kuchta, LeGrow, and Persichetti [KLP26] is recovered with the algorithm of Section 3, and we report experiments on the proposed parameter sets.

In the blind signature scheme of [KLP26, Sect. 4], a matrix code $X^{(0)}$ with generator matrix $\mathbf{G_0}$ is a public parameter, the signer's secret key consists of $(\mathbf{A}, \mathbf{B})$ with $\mathbf{A} \in \mathbb{S}_m(\mathbb{F}_q)$ and $\mathbf{B} \in \mathbb{S}_n(\mathbb{F}_q)$ sampled uniformly at random, and, in order to compensate for the lack of a quadratic twist in the MCE group action, the public key contains the two codes $X^{(1)} = (\mathbf{A}, \mathbf{B}) * X^{(0)}$ and $X^{(-1)} = (\mathbf{A}^{-1}, \mathbf{B}^{-1}) * X^{(0)}$, where $(\mathbf{A}, \mathbf{B}) * \mathcal{D} = \mathbf{A}\mathcal{D}\mathbf{B}^\top$. Codes are represented by their generator matrices in systematic form [KLP26, Sect. 2.4]. In our notation (where the isometry is written $\mathbf{Q} = \mathbf{A}^\top \otimes \mathbf{B}$), the public key is therefore

$$\mathbf{G_1} = \mathbf{S_1}\mathbf{G_0}\mathbf{Q}, \qquad \mathbf{G_2} = \mathbf{S_2}\mathbf{G_0}\mathbf{Q}^{-1}, \tag{7}$$

where $\mathbf{S_1}, \mathbf{S_2} \in \mathsf{GL}_k(\mathbb{F}_q)$ are the (unrelated) matrices bringing $\mathbf{G_0}\mathbf{Q}$ and $\mathbf{G_0}\mathbf{Q}^{-1}$ into systematic form. This is an sIMCE instance (Definition 4), which is in turn the 2-sMCE instance $(\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2}, \mathbf{G_0})$ with solution $(\mathbf{S_1}, \mathbf{S_2}^{-1}, \mathbf{A}, \mathbf{B})$. Hence, our algorithm in Figure 1 on input $(\mathbf{G_0}, \mathbf{G_1}, \mathbf{G_2}, \mathbf{G_0})$ returns a valid solution of this 2-sMCE instance with probability $O(1 - 1/q)$.

4.1 Experiments on the Proposed Parameter Sets

We focus our experiments on the standard setting $k = m = n$ as in [CNP+23, BBMP24], for an increased variant of the MEDS parameter sets as analyzed in [GMPT26] (the matrix dimensions are scaled by a factor of $\sqrt{2}$), and for the parameter set proposed in [KLP26], which was estimated to provide 128 bits of security. Table 1 reports the running time of our SageMath implementation [Com26] on sIMCE instances, i.e., public keys of the form Equation (7), and on 2-sMCE instances; in all cases, the solution space of Step 2 was one-dimensional and the output was verified. All the parameter sets, including the one of [KLP26] with $n = 46$, are solved in less than one minute.

Table 1: Experiments for solving the 2-sMCE for $k = m = n$ over $\mathbb{F}_q$. The column d is the dimension computed in Step 1; in all runs, the solution space of Step 2 was one-dimensional.

	Dimension (n)	**Field size** (q)	d	sIMCE	2-sMCE
[GMPT26]	20	4093	20	1.3 s	1.4 s
	31	4093	31	8.0 s	8.8 s
	42	2039	42	31.5 s	34.1 s
[KLP26]	46	4093	46	47.8 s	50.8 s

4.2 Experimental Validation

This section reports experiments that support Heuristics 1 and 2 (Section 3.3). All experiments use our SageMath implementation [Com26] of the algorithm in Figure 1 and instances sampled from $\mathcal{R}_{\text{2-sMCE}}$ and $\mathcal{R}_{\text{sIMCE}}$; the symmetry types (ϵ_A, ϵ_B) are drawn uniformly at random among the admissible ones for each instance (a skew-symmetric matrix of odd size is singular), except in Section 4.2, where they are fixed.

Kernel Dimensions and Success for Small Parameters Table 2 presents the parameters $k = m = n \in \{2, \ldots, 10, 12, 16, 20\}$ we test. We performed 25 random experiments for each distribution on 2-sMCE and sIMCE, and consider $q = 4093$ as this is usedin [CNP+23, KLP26]. In all experiments, the dimension d equaled k when $\epsilon = 1$ and $\lceil k/2 \rceil$ when $\epsilon = -1$, as stated in Heuristic 1; the solution space of Step 2 was one-dimensional and the secret was recovered. The number of projections was $t = 1$ in all runs, except for the shape $(2, 4, 4)$ with $\epsilon = 1$, where $t = 2$ as prescribed by Figure 1. We stress that this includes the parameters $k = 2$, for which no obstruction was observed.

Table 2: Tested values of k, m, and n, with fixed $q = 4093$.

k	2	3	4	5	6	7	8	9	10	12	16	20	2	2	4	3	4	5	7	5	6
m	2	3	4	5	6	7	8	9	10	12	16	20	3	4	3	4	4	4	4	6	4
n	2	3	4	5	6	7	8	9	10	12	16	20	4	4	5	6	6	6	6	6	8

Dependence on the Field Size Heuristics 1 and 2 predict failure probabilities of order $1/q$. To measure them, we ran the algorithm for each prime $q \in [3, 257]$, for $(\epsilon_A, \epsilon_B) \in \{(1, 1), (-1, 1)\}$ and both distributions on 2-sMCE and sIMCE. The numbers correspond to 25 experiments per q with fixed $k = m = n = 20$.We observed that the dimension d was never below the value of Heuristic 1, and exceeded it in all experiments. Skew-symmetric isometries ($\epsilon = -1$) fail much less often than symmetric ones.

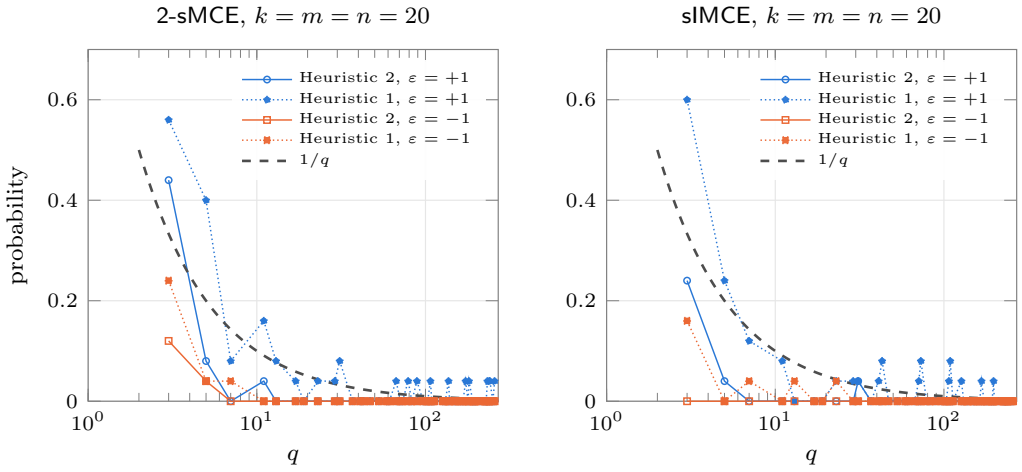

Figure 3: Empirical probability that Heuristic 2 fails (solid: (C1) does not hold, so that the algorithm fails) and that Heuristic 1 fails (dotted: d is above its predicted value) as a function of $3 \leq q \leq 257$, for $k = m = n = 20$, $(\epsilon_A, \epsilon_B) \in \{(1, 1), (-1, 1)\}$.

References

[BBMP24] Michele Battagliola, Giacomo Borin, Alessio Meneghetti, and Edoardo Persichetti. Cutting the GRASS: Threshold GRoup action signature schemes. In Elisabeth Oswald, editor, *CT-RSA 2024*, volume 14643 of *LNCS*, pages 460–489. Springer, Cham, May 2024. doi:10.1007/978-3-031-58868-6_18.

[BBN+22] Alessandro Barenghi, Jean-François Biasse, Tran Ngo, Edoardo Persichetti, and Paolo Santini. Advanced signature functionalities from the code equivalence problem. *International Journal of Computer Mathematics: Computer Systems Theory*, 7(2):112–128, 2022. URL: https://doi.org/10.1080/23799927.2022.2048206.

[BCD+24] Alessandro Budroni, Jesús-Javier Chi-Domínguez, Giuseppe D'Alconzo, Antonio J. Di Scala, and Mukul Kulkarni. Don't use it twice! Solving relaxed linear equivalence problems. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part VIII*, volume 15491 of *LNCS*, pages 35–65. Springer, Singapore, December 2024. doi:10.1007/978-981-96-0944-4_2.

[BCF25] Alessandro Budroni, Jesús-Javier Chi-Domínguez, and Ermes Franch. Don't use it twice: Reloaded! On the lattice isomorphism group action. *CiC*, 2(2):9, 2025. doi:10.62056/ay76chdj.

[CL25] Alain Couvreur and Christophe Levrat. Highway to hull: An algorithm for solving the general matrix code equivalence problem. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part I*, volume 16000 of *LNCS*, pages 253–283. Springer, Cham, August 2025. doi:10.1007/978-3-032-01855-7_9.

[CNP+23] Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Take your MEDS: Digital signatures from matrix code equivalence. In Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne, editors, *AFRICACRYPT 23*, volume 14064 of *LNCS*, pages 28–52. Springer, Cham, July 2023. doi:10.1007/978-3-031-37679-5_2.

[Com26] Companion Code Implementation. The code is provided at https://github.com/Crypto-TII/pqc-two-smce.git, 2026.

[GMPT26] Valerie Gilchrist, Laurane Marco, Christophe Petit, and Gang Tang. On the security of two blind signatures from code equivalence problems. *CiC*, 2(4), 2026. doi:10.62056/aesg893y6.

[KLP26] Veronika Kuchta, Jason T. LeGrow, and Edoardo Persichetti. Post-quantum (partially) blind signatures from matrix code equivalence. *Cryptography and Communications*, 2026. doi:10.1007/s12095-026-00879-x.

[KTS+23] Thanh Xuan Khuc, The Anh Ta, Willy Susilo, Dung Hoang Duong, Fuchun Guo, Kazuhide Fukushima, and Shinsaku Kiyomoto. Logarithmic-Size (Linkable) Ring Signatures from Lattice Isomorphism problems. In Francesco Regazzoni, Bodhisatwa Mazumdar, and Sri Parameswaran, editors, *Security, Privacy, and Applied Cryptography Engineering - 13th International Conference, SPACE 2023, Roorkee, India, December 14-17, 2023, Proceedings*, volume 14412 of *Lecture Notes in Computer Science*, pages 214–241. Springer, 2023. doi:10.1007/978-3-031-51583-5_13.

[NQT24] Anand Kumar Narayanan, Youming Qiao, and Gang Tang. Algorithms for matrix code and alternating trilinear form equivalences via new isomorphism invariants. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part III*, volume 14653 of *LNCS*, pages 160–187. Springer, Cham, May 2024. doi:10.1007/978-3-031-58734-4_6.

[RS24] Lars Ran and Simona Samardjiska. Rare structures in tensor graphs - bermuda triangles for cryptosystems based on the tensor isomorphism problem. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part VIII*, volume 15491 of *LNCS*, pages 66–96. Springer, Singapore, December 2024. doi:10.1007/978-981-96-0944-4_3.

[RST24] Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Hardness estimates of the code equivalence problem in the rank metric. *DCC*, 92(3):833–862, 2024. doi:10.1007/s10623-023-01338-x.