Comment on TechRxiv preprint 1374260 (DOI: 10.36227/techrxiv.176765338.86836807/v1): "Dimension Padding as a Structural Countermeasure to Linear Inversion in Dual-Public-Key Code-Based Cryptosystems"

Mohammad Sadegh Ghoralivandzadeh

February 13, 2026

Abstract

A recent "dimension padding" note proposes a structural countermeasure to linear inversion in a dual-public-key code-based encryption construction. The note argues that padding makes the private parity structure non-identifiable from the public key and suggests phrasing security in terms of this non-identifiability. This comment points out that non-identifiability of a particular trapdoor representation does not prevent message recovery. In the padded construction, the public relations used for decryption remain linear constraints. Any solution to these public constraints suffices to recover the encryption randomness and then the plaintext by linear algebra. Consequently, public-key-only decryption remains polynomial-time.

1 What is claimed in the padding note

The padding note proposes increasing the ambient dimension so that the stacked public matrix becomes non-square, with the goal of destroying uniqueness of the private parity-side representation. The security discussion emphasizes that an adversary may construct some matrix consistent with the public relations, but cannot determine the "true" structured trapdoor matrix among many candidates. The note then frames security as non-identifiability of the private parity structure.

2 Model and notation (padded scheme)

Work over F_2. Let the public key be

$$\mathrm{pk} = (p_1, p_2), \tag{1}$$

where $p_1 \in \mathrm{F}_2^{k\times n}$ and $p_2 \in \mathrm{F}_2^{(n-k)\times n}$ are public matrices. Encryption outputs

$$c' = m\,p_1 + s\,p_2, \tag{2}$$

for a message $m \in \mathrm{F}_2^{1\times k}$ and a random vector $s \in \mathrm{F}_2^{1\times(n-k)}$. Correctness is described via a (secret) matrix $Q \in \mathrm{F}_2^{n\times(n-k)}$ satisfying the public relations

$$p_1 Q = 0, \quad p_2 Q = I_{n-k}. \tag{3}$$

Decryption first computes $s = c'Q$ and then removes the p_2-component to obtain mp_1.

3 Main observation: any public solution enables decryption

Theorem. Assume ciphertexts satisfy (2) and that the public linear system (3) is solvable (as required for stated correctness). Then there is a public-key-only, polynomial-time algorithm that recovers (s, m) from (pk, c').

Proof. Compute any solution $Q' \in \mathrm{F}_2^{n\times(n-k)}$ to the public constraints

$$p_1 Q' = 0, \quad p_2 Q' = I_{n-k}, \tag{4}$$

using Gaussian elimination over F_2. Then

$$\begin{aligned} s &= c'Q' \\ &= (mp_1 + sp_2)Q' \\ &= m(p_1Q') + s(p_2Q') \\ &= m \cdot 0 + s \cdot I_{n-k} \\ &= s. \end{aligned}$$

Next set $v = c' + sp_2$. Using (2),

$$v = (mp_1 + sp_2) + sp_2 = mp_1.$$

Finally, recover m from $v = mp_1$. For meaningful (unique) decryption, p_1 must have full row rank k; under this standard condition, there exists a right-inverse $R \in \mathrm{F}_2^{n\times k}$ such that

$$p_1 R = I_k. \tag{5}$$

Compute one such R by Gaussian elimination and output $m = vR$. All steps are linear algebra over F_2, hence polynomial time. □

4 Explicit attack algorithm

1. Input: public key (p_1, p_2) and ciphertext c'.
2. Solve the linear system (4) for any Q'.
3. Compute $s \leftarrow c'Q'$.
4. Compute $v \leftarrow c' + sp_2$ (then $v = mp_1$).
5. Compute any right-inverse R satisfying (5).
6. Output: $m \leftarrow vR$.

Complexity. The dominant cost is solving linear systems over F_2 (Gaussian elimination), i.e., polynomial time. No decoding hardness is invoked.

5 Why non-identifiability does not imply confidentiality

The padding note's security rationale concerns the inability to uniquely identify a particular structured trapdoor matrix Q among many candidates. However, for message recovery the adversary does not need the "true" trapdoor form. Any Q' satisfying the same public linear constraints already yields $s = c'Q'$ and reduces ciphertext processing to the public linear relation $v = mp_1$, from which m is recovered by a public right-inverse of p_1. Thus, an exponential-size equivalence class of solutions does not help: the existence of any efficiently findable solution is sufficient to decrypt.

References

1. F. H. Makoui, T. A. Gulliver, and M. Dakhilalian. A McEliece-type cryptosystem using a random inverse matrix and an error vector with large Hamming weight. Proc. ACIT 2024, pp. 490–495.

2. F. H. Makoui. Dimension Padding as a Structural Countermeasure to Linear Inversion in Dual-Public-Key Code-Based Cryptosystems. Technical note / preprint (9 pages).