Cryptanalysis of a Candidate Witness Encryption Scheme for Affine Determinant Programs

Sunghyeon Jo
Georgia Institute of Technology
August 19, 2026

Abstract. At ITCS 2020, Bartusek, Ishai, Jain, Ma, Sahai, and Zhandry proposed a framework for witness encryption based on affine determinant programs and gave a concrete witness encryption candidate. Yao, Chen, and Yu later broke the separate ADP-based indistinguishability-obfuscation candidate, while noting that their attack did not apply to the witness-encryption construction.

More recently, Soukhanov et al. proposed witness encryption from arithmetic affine determinant programs. Soukhanov subsequently described a commutator attack on that construction and noted that the original ADP construction is also subject to the attack for sparse circuits.

The recovery of hidden column spaces in our attack uses this commutator technique. We give a deterministic polynomial-time attack that recovers the encrypted bit from the public ciphertext matrices of this candidate. It covers every $q \geq 1$ in the theorem's recovery range, including $q(n) = \lceil n^{\varepsilon} \rceil$ for all sufficiently large n. Outside a fixed finite set of primes, it applies to every SUBSET-SUM instance whose coefficient vector is nonzero modulo p and that has no Boolean solution modulo p. On an explicit efficiently generated family of integer NO instances, the encrypted bit is recovered with probability $1 - \mathrm{negl}(n)$ under the field-size convention of the original paper.

1 Introduction

Witness encryption, introduced by Garg, Gentry, Sahai, and Waters [GGSW13], allows a message to be encrypted to an instance x of an NP language. Any witness for x decrypts, while a ciphertext associated with a false instance must hide the message. General constructions are known from powerful cryptographic assumptions, but obtaining a direct and concretely implementable candidate remains difficult.

Bartusek et al. proposed affine determinant programs (ADPs) as a framework for obfuscation and witness encryption [BIJ+20]. Their concrete witness encryption candidate combines three components: an instance-encoding ADP sampled by $\mathsf{VSS.Encode}$, a bit-encoding ADP $(bS, 0, \ldots, 0)$, and an intended All-Accept ADP sampled by $\mathsf{AllAcc.Gen}_{\mathrm{FORM}}$. The printed coefficient formula differs from that procedure in one term; Remark 8 records both readings. The All-Accept ADP is intended to provide "Rejection of Invalid Inputs," in the terminology

of Bartusek et al.: it is singular on Boolean inputs and, for each fixed non-binary field input, nonsingular with overwhelming probability over its sampling randomness.

The candidate first converts a SUBSET-SUM instance to a VECTOR-SUBSET-SUM instance with variables w_i and $\widehat{w}_i = 1 - w_i$. In the generalized version of $\mathsf{AllAcc.Gen}_{\mathrm{FORM}}$, the matrices U_i, V_i, S_i, T_i have q columns. We call q the *block width*; the width of the resulting ADP is $k = 2nq + 1$. Bartusek et al. analyze a correlated-span attack when sufficiently many unmasked coefficient matrices are available and a multivariate-quadratic linearization attack against a sparse, untransformed width-one instance [BIJ+20, Section 7]. Their candidate uses two safeguards against these attacks: the transformation to VECTOR-SUBSET-SUM, whose matrix has many linearly independent rows, and the superconstant choice $q(n) = n^{\varepsilon}$ for a fixed constant $\varepsilon > 0$.

The construction is a candidate and is not accompanied by a reduction to a standard assumption. Yao, Chen, and Yu broke the separate ADP-based indistinguishability-obfuscation (iO) candidate [YCY22], but explicitly state that their mod-4 attack does not apply to the witness encryption construction.

More recently, Soukhanov et al. introduced arithmetic affine determinant programs (AADPs), a variant of ADPs for arithmetic constraint systems, and used them to construct a witness encryption scheme for all NP languages [SRE+26]. Soukhanov subsequently described a commutator attack on this AADP construction [Sou26]. Given public matrices M^a, M^b, M^c, the attack forms $T_{ab} = (M^a)^{-1}M^b$ and uses low-rank commutators, in particular $[T_{ab}, T_{ac}]$, whose kernel spaces reveal the hidden basis. The post also notes that the original ADP construction is subject to this attack for sparse circuits.

The recovery of hidden column spaces in our attack uses this commutator technique. For this candidate, we show how public differences remove the $\mathsf{VSS.Encode}$ terms, how the recovered spaces yield a distinguisher using only the public ciphertext, and why recovery succeeds for every q in the stated range. The attack applies with both safeguards described above and uses neither the parity leakage of Yao et al. nor a satisfying Boolean witness.

1.1 Main Result

The result holds for every fixed public instance that has no Boolean solution modulo p and allows arbitrary zero coordinates in h, except for the all-zero vector. A simple efficiently generated family is

$$I_n = ((1, \ldots, 1), n + 1). \tag{1.1}$$

It is an integer SUBSET-SUM NO instance and remains a NO instance modulo p whenever $p > n + 1$. Nevertheless, the transformed VECTOR-SUBSET-SUM equations have a public non-binary solution over $\mathbb{F}_p$. The All-Accept ADP is intended to prevent precisely this invalid evaluation from revealing the message. We show that the required hidden column spaces can be recovered from the public coefficient matrices and then removed by vectors orthogonal to those spaces.

Theorem 1 (Informal main theorem)**.** *There is a fixed finite set of primes such that, for every $q \geq 1$ and n satisfying $2nq+1 \geq 30q-4$, every prime outside that set, and every SUBSET-SUM instance (h, ℓ) that has no Boolean solution modulo p and satisfies $h \neq 0$ in $\mathbb{F}_p^n$, a deterministic polynomial-time algorithm using only the public instance and ciphertext matrices distinguishes an encryption of 0 from an encryption of 1 with soundness advantage*

$$1 - O\left(\frac{n^2q^2}{p}\right).$$

For $q = \lceil n^{\varepsilon} \rceil$, the family I_n, and the source paper's superpolynomial field-size convention, this advantage is $1 - \mathrm{negl}(n)$.

Theorem 21 gives the exact failure probability and running time.

1.2 Attack Overview

The attack has three stages.

1. Remove the VSS.Encode terms. The matrices B_i and B_{n+i} correspond to w_i and $\widehat{w}_i = 1 - w_i$. The same random matrix R_i occurs in both, so their public difference is

$$D_i = B_i - B_{n+i} = h_i R_0 + G_i,$$

where G_i contains only terms from the All-Accept ADP. If $h_a \neq 0$, the weighted difference $F_{a,r} = h_a D_r - h_r D_a$ removes R_0. When at least four entries of h are zero, the corresponding D_i already contain no VSS.Encode term and give a second, lower-rank recovery method.

2. Recover the hidden column spaces. This stage uses the commutator technique described by Soukhanov [Sou26]. After changing the left and right bases, every off-diagonal term of G_i has a left or right factor in the two blocks indexed by i and $n+i$. For each i, the attack forms two triples (A, B, C) of public difference matrices and computes

$$K(A, B, C) = BA^{-1}C - CA^{-1}B.$$

Equivalently, $K = A[A^{-1}B, A^{-1}C]$, so it is a left multiple of the commutator of $A^{-1}B$ and $A^{-1}C$. The intersections of the two row spaces recover $\mathrm{col}[T_i \mid T_{n+i}]$, and the intersections of the two column spaces recover $\mathrm{col}[U_i \mid U_{n+i}]$. With at least four zero coefficients, it is enough to recover the spaces for those indices and use one additional public matrix to obtain the same final null vectors.

3. Evaluate outside the Boolean domain. The recovered spaces give a nonzero left null vector β for all U_i and a nonzero right null vector α for all T_i. At a non-binary solution of the transformed VECTOR-SUBSET-SUM equations, the VSS.Encode component is zero, while multiplication by $\beta^{\top}$ and α removes the All-Accept component. The remaining scalar is zero for an encryption of

0 and is a nonzero linear function of the random bit-encoding matrix for an encryption of 1.

The proof that the spaces are recovered has two separate parts. Partial Koszul flattenings give rank upper bounds. Explicit nonzero minors show that the bounds and the required intersection dimensions hold simultaneously, except with probability $O(n^2q^2/p)$. These minors are part of the success proof and are not computed by the attacker.

2 Preliminaries

For a positive integer m, write $[m] = \{1, \ldots, m\}$. All vector spaces and matrices are over the prime field $\mathbb{F}_p$ unless stated otherwise. Vectors are columns. For a matrix M, let $\operatorname{row} M$, $\operatorname{col} M$, and $\operatorname{rank} M$ denote its row space, column space, and rank. We write $[X, Y] = XY - YX$ for the matrix commutator. A probability bound is taken over all randomness of the encryption algorithm.

2.1 Affine Determinant Programs and Witness Encryption

Definition 2 (Affine determinant program)**.** An affine determinant program on m Boolean variables is a tuple $(A, B_1, \ldots, B_m)$ of $k \times k$ matrices and an evaluation map $\mathsf{Eval} : \mathbb{F}_p \to \{0, 1\}$. Write

$$M(x) = A + \sum_{i=1}^{m} x_i B_i.$$

On a Boolean input $x \in \{0,1\}^m$, the ADP outputs $\mathsf{Eval}(\det M(x))$. We also evaluate the same affine matrix expression on $x \in \mathbb{F}_p^m$; following Bartusek et al., a non-binary x is an *invalid evaluation*, not an input in the formal ADP domain.

We recall the standard definition of witness encryption for one-bit messages [GGSW13, BIJ+20].

Definition 3 (Witness encryption)**.** Let L be an NP language with witness relation R. A witness encryption scheme for L consists of two polynomial-time algorithms:

- $\mathsf{Encrypt}(1^\lambda, x, m)$ takes a security parameter, an instance x, and a message $m \in \{0, 1\}$, and outputs a ciphertext C;
- $\mathsf{Decrypt}(C, w)$ takes a ciphertext and a string w, and outputs a message or $\perp$.

The algorithms satisfy the following conditions.

Correctness. For every λ, every $m \in \{0, 1\}$, and every (x, w) such that $R(x, w) = 1$,

$$\Pr[\mathsf{Decrypt}(\mathsf{Encrypt}(1^\lambda, x, m), w) = m] = 1.$$

Soundness security. For every probabilistic polynomial-time adversary $\mathcal{A}$, there is a negligible function μ such that, for every $x \notin L$,

$$\left|\Pr[\mathcal{A}(\mathsf{Encrypt}(1^\lambda, x, 0)) = 1] - \Pr[\mathcal{A}(\mathsf{Encrypt}(1^\lambda, x, 1)) = 1]\right| \le \mu(\lambda).$$

For the concrete one-bit candidate analyzed here, fix parameters (n, q, p) and a false instance $I \notin L$, and let $C_b \leftarrow \mathsf{Enc}_{n,q,p}(I, b)$ for $b \in \{0, 1\}$. We measure a deterministic distinguisher by its soundness advantage, matching the definition above:

$$\mathrm{Adv}^{\mathrm{snd}}_{\mathcal{A}}(I; n, q, p) = \left|\Pr[\mathcal{A}(C_1) = 1] - \Pr[\mathcal{A}(C_0) = 1]\right|. \tag{2.1}$$

If a standard challenge bit is uniform and the adversary uses $\mathcal{A}(C)$ as its guess, then

$$\Pr[\widehat{b} = b] = \frac{1}{2} + \frac{\Pr[\mathcal{A}(C_1) = 1] - \Pr[\mathcal{A}(C_0) = 1]}{2} \tag{2.2}$$

whenever the displayed difference is nonnegative. Thus soundness advantage and advantage over random guessing differ only by a factor of two. Soundness security requires this advantage to be negligible for every polynomial-time adversary. We use the standard convention that $\mu(n) = \mathrm{negl}(n)$ if, for every constant $c > 0$, one has $\mu(n) < n^{-c}$ for all sufficiently large n.

2.2 Algebraic Tools

For a square matrix A, let $\mathrm{adj}(A)$ denote its adjugate. We use the identity

$$A^{-1} = \frac{\mathrm{adj}(A)}{\det A} \tag{2.3}$$

whenever A is invertible. We also use the following standard form of the Schwartz–Zippel lemma [Sch80, Zip79].

Lemma 4 (Schwartz–Zippel)**.** *Let f be a nonzero polynomial of total degree at most D in independent uniform variables over $\mathbb{F}_p$. Then*

$$\Pr[f = 0] \le D/p.$$

For three $k \times k$ matrices (A, B, C) and a matrix $J \in \mathbb{F}_p^{k \times s}$ selecting an s-dimensional column subspace, define the following block matrix, called a partial Koszul flattening:

$$\Phi_J(A, B, C) = \begin{bmatrix} 0 & A & BJ \\ -A & 0 & CJ \\ -B & -C & 0 \end{bmatrix}. \tag{2.4}$$

Write $\Phi(A, B, C) = \Phi_{I_k}(A, B, C)$.

3 The [BIJ+20] Witness Encryption Scheme

A ciphertext in this construction is itself an ADP. The generic candidate samples an instance encoding $M_{H,\boldsymbol{\ell}}$ using $\mathsf{VSS.Encode}$, an All-Accept ADP M_{AA} of the same width, and a uniform matrix S^{msg}, and publishes

$$C_b = M_{\mathsf{AA}} + M_{H,\boldsymbol{\ell}} + (bS^{\mathsf{msg}}, 0, \ldots, 0). \tag{3.1}$$

Given a Boolean witness y, decryption evaluates the ADP at y and applies $\mathsf{Eval}_{\neq 0}$, which returns 1 exactly when the determinant is nonzero. The instance encoding vanishes at a witness, while the All-Accept generator is singular on every Boolean input. When the field size p is superpolynomial in the input length, it is intended to be nonsingular at each fixed nonbinary point, preventing invalid evaluations from revealing the bit.

3.1 VSS.Encode and the SUBSET-SUM Transformation

Let

$$(H, \boldsymbol{\ell}) \in \mathbb{Z}^{d \times N} \times \mathbb{Z}^d$$

be a VECTOR-SUBSET-SUM instance. It is a YES instance if some $y \in \{0,1\}^N$ satisfies $Hy = \boldsymbol{\ell}$ over the integers. The procedure $\mathsf{VSS.Encode}((H, \boldsymbol{\ell}), p, k)$ interprets the entries modulo p, samples one independent uniform matrix $\mathcal{R}_r \in \mathbb{F}_p^{k \times k}$ for each row $r \in \{0, \ldots, d-1\}$, and outputs the ADP with coefficients

$$A_{\mathsf{VSS}} = -\sum_{r=0}^{d-1} \boldsymbol{\ell}_r \mathcal{R}_r, \tag{3.2}$$

$$B_c^{\mathsf{VSS}} = \sum_{r=0}^{d-1} H_{r,c} \mathcal{R}_r, \qquad c \in [N]. \tag{3.3}$$

For every $y \in \mathbb{F}_p^N$, its evaluation is

$$M_{H,\boldsymbol{\ell}}(y) = \sum_{r=0}^{d-1} \big((Hy)_r - \boldsymbol{\ell}_r\big) \mathcal{R}_r. \tag{3.4}$$

Thus a VECTOR-SUBSET-SUM witness makes the instance encoding zero.

For a SUBSET-SUM instance $(h_1, \ldots, h_n; \ell)$, Bartusek et al. write $x = (w, \widehat{w}) \in \{0,1\}^{2n}$ and use the transformed instance

$$H = \begin{bmatrix} h_1 & \cdots & h_n & 0 & \cdots & 0 \\ & & I_n & & I_n & \end{bmatrix}, \qquad \boldsymbol{\ell} = (\ell, 1, \ldots, 1)^\top. \tag{3.5}$$

The last n equations enforce $\widehat{w}_i = 1 - w_i$. Consequently, $Hx = \boldsymbol{\ell}$ if and only if $h \cdot w = \ell$ and $\widehat{w}_i = 1 - w_i$ for every i. The transformation therefore preserves membership.

Index the rows by $0, 1, \ldots, n$ and rename their random matrices $R_0, R_1, \ldots, R_n$. Substitution into (3.2)–(3.3) gives

$$A_{\mathsf{VSS}} = -\ell R_0 - \sum_{i=1}^{n} R_i, \tag{3.6}$$

$$B_i^{\mathsf{VSS}} = h_i R_0 + R_i, \qquad i \in [n], \tag{3.7}$$

$$B_{n+i}^{\mathsf{VSS}} = R_i, \qquad i \in [n]. \tag{3.8}$$

The column for $\widehat{w}_i$ has a single 1 in row i, so it necessarily uses the same random matrix R_i as the column for w_i. For $w \in \{0,1\}^n$ and $\widehat{w}_i = 1 - w_i$,

$$\begin{aligned} A_{\mathsf{VSS}} + \sum_i w_i B_i^{\mathsf{VSS}} + \sum_i (1 - w_i) B_{n+i}^{\mathsf{VSS}} \\ = (h \cdot w - \ell) R_0 + \sum_i \big(w_i + (1 - w_i) - 1\big) R_i. \end{aligned} \tag{3.9}$$

When all Boolean subset sums $h \cdot w$ and the target ℓ lie in an integer interval of length less than p, equality modulo p is the same as integer equality. We call this the *no-wrap condition*.

Definition 5 (NO instance modulo p)**.** A SUBSET-SUM instance (h, ℓ) is a *NO instance modulo* p if $h \cdot w \neq \ell$ in $\mathbb{F}_p$ for every $w \in \{0,1\}^n$. Under the no-wrap condition, an integer SUBSET-SUM NO instance remains a NO instance modulo p.

Lemma 6 (Explicit family of NO instances)**.** *The family* (1.1) *is false in the integer SUBSET-SUM language and is a NO instance modulo* p *for every prime* $p > n + 1$.

Proof. For every $w \in \{0,1\}^n$, one has $h \cdot w = \sum_i w_i \leq n < n+1 = \ell$. If $p > n+1$, all these values and ℓ remain distinct modulo p whenever they are distinct as integers. □

Remark 7 (Coefficient determined by $\mathsf{VSS.Encode}$)**.** The coefficient formula printed in [BIJ+20, Section 5.2] contains an undefined mask index. Applying $\mathsf{VSS.Encode}$ to (3.5) determines the intended coefficient: the column $n+i$ is zero except for a 1 in row i, and hence $B^{\mathsf{VSS}}_{n+i} = R_i$. We use this coefficient throughout.

3.2 The Ciphertext Distribution

The procedure $\mathsf{AllAcc.Gen}_{\mathrm{FORM}}$ is based on the tautology $\bigwedge_{r=1}^{2n}(x_r \vee \neg x_r)$ and has block width q. At a Boolean evaluation its terms group into $2n$ matrices of rank at most q, so $k = 2nq + 1$ makes the component singular. We analyze the concrete coefficients printed in [BIJ+20, Section 5.2], which retain this rank bound, with the coefficient in Remark 7 determined by $\mathsf{VSS.Encode}$.

We state the distribution for every $q \geq 1$ and prime p. The candidate of Bartusek et al. sets $q(n) = n^{\varepsilon}$ and chooses a superpolynomial p larger than $|h \cdot w|$ for every Boolean w. Our soundness statement uses the condition in Definition 5.

Fix

$$q \geq 1, \qquad k = 2nq + 1. \tag{3.10}$$

For every $r \in [2n]$, sample independently and uniformly

$$U_r, V_r, S_r, T_r \in \mathbb{F}_p^{k \times q}, \tag{3.11}$$

and for every $r, s \in [2n]$ sample independent uniform scalars $c_r^{(s)} \in \mathbb{F}_p$. Sample independent uniform $k \times k$ matrices

$$R_0, R_1, \ldots, R_n, S^{\mathsf{msg}} \in \mathbb{F}_p^{k \times k}. \tag{3.12}$$

Bartusek et al. write the final $k \times k$ matrix as S. We write S^{msg} to distinguish it from the matrices S_r in $\mathsf{AllAcc.Gen}_{\mathrm{FORM}}$.

For encrypted bit b, the constant matrix is

$$A_b = \sum_{r=1}^{2n} U_r V_r^{\top} - \ell R_0 - \sum_{i=1}^{n} R_i + b S^{\mathsf{msg}}. \tag{3.13}$$

For $i \in [n]$, the coefficient for w_i is

$$B_i = -U_i V_i^\top + V_i T_i^\top + \sum_{s=1}^{2n} c_i^{(s)} U_s T_s^\top + h_i R_0 + R_i, \tag{3.14}$$

and the coefficient for $\widehat{w}_i$ is

$$B_{n+i} = -U_{n+i} V_{n+i}^\top + S_{n+i} T_{n+i}^\top + \sum_{s=1}^{2n} c_{n+i}^{(s)} U_s T_s^\top + R_i. \tag{3.15}$$

The ciphertext is $C_b = (A_b, B_1, \ldots, B_{2n})$. This is the distribution $C_b \leftarrow \mathsf{Enc}_{n,q,p}((h,\ell), b)$ used in (2.1).

Let $M_{\mathsf{AA}}(x)$ denote the affine evaluation of all terms in (3.13)–(3.15) that contain U_r, V_r, S_r, T_r, or $c_r^{(s)}$. Let $M_{H,\boldsymbol{\ell}}(x)$ denote the instance-encoding ADP sampled by $\mathsf{VSS.Encode}$. Then the evaluated ciphertext matrix has the decomposition

$$C_b(x) = M_{\mathsf{AA}}(x) + M_{H,\boldsymbol{\ell}}(x) + bS^{\mathsf{msg}}. \tag{3.16}$$

Only the sum C_b is public; the three terms in (3.16) are its conceptual components.

Given a SUBSET-SUM witness w, set $\widehat{w}_i = 1 - w_i$ and $x = (w, \widehat{w})$, and decrypt by

$$\mathsf{WE.Dec}(C_b, w) = \mathsf{Eval}_{\neq 0}(\det C_b(x)). \tag{3.17}$$

Equation (3.9) makes the instance component zero, and the Boolean rank bound makes $M_{\mathsf{AA}}(x)$ singular. Hence decryption returns 0 when $b = 0$. When $b = 1$, the evaluated matrix is a uniform $k \times k$ matrix, so it is nonsingular with probability

$$\Pr[\det C_1(x) \neq 0] = \prod_{j=1}^{k} (1 - p^{-j}) = 1 - O(1/p). \tag{3.18}$$

Thus the concrete distribution has correctness probability $1 - O(1/p)$. For superpolynomial p this is overwhelming, but it is not the perfect correctness required by Definition 3.

Remark 8 (Alternative formula term)**.** The matrices S_i for $i \in [n]$ are unused in the coefficients above. If B_i instead uses the independently sampled $S_i T_i^\top$ in place of $V_i T_i^\top$ in (3.14), that All-Accept part of B_i agrees with $\mathsf{AllAcc.Gen}_{\mathrm{FORM}}$. The attack then applies with the sharper failure bound of Lemma 18.

The attack below recovers enough hidden structure to remove the All-Accept component at a nonbinary solution of the field equations.

4 The Attack

The algebraic recovery works for every fixed public coefficient vector $h \neq 0$ in $\mathbb{F}_p^n$, while the witness encryption consequence requires a NO instance modulo p. From this point on, h_i and ℓ in field or matrix expressions denote their reductions modulo p.

4.1 Eliminating the Instance Encoding

For every $i \in [n]$, define the public difference

$$D_i = B_i - B_{n+i}. \tag{4.1}$$

Equations (3.14)–(3.15) and the shared random matrix R_i give

$$D_i = h_i R_0 + G_i, \tag{4.2}$$

where

$$\begin{aligned} G_i = & -U_i V_i^\top + V_i T_i^\top + U_{n+i} V_{n+i}^\top - S_{n+i} T_{n+i}^\top \\ & + \sum_{s=1}^{2n} \gamma_i^{(s)} U_s T_s^\top, \end{aligned} \tag{4.3}$$

where

$$\gamma_i^{(s)} = c_i^{(s)} - c_{n+i}^{(s)}. \tag{4.4}$$

Lemma 9 (Coefficient independence)**.** *For every fixed $h \in \mathbb{F}_p^n$, conditional on the shared $(U_r, T_r)_{r\in[2n]}$, the family $(G_1, \ldots, G_n)$ is independent of h and is generated by the mutually independent uniform families $(\gamma_i^{(s)})_{i,s}$, $(V_i)_i$, $(V_{n+i})_i$, and $(S_{n+i})_i$, subject to the displayed shared factors and to the fact that both terms for w_i use the same V_i.*

Proof. The coefficient vector occurs only in the term $h_i R_0$ of (4.2). For each (i, s), the map $(c_i^{(s)}, c_{n+i}^{(s)}) \mapsto (c_i^{(s)} - c_{n+i}^{(s)}, c_{n+i}^{(s)})$ is bijective. The claimed distribution follows from the sampling rule in (3.11)–(3.12). In particular, this claim retains the dependence between $-U_i V_i^\top$ and $V_i T_i^\top$. □

For distinct indices $a, r \in [n]$, define the weighted difference

$$F_{a,r} = h_a D_r - h_r D_a = h_a G_r - h_r G_a. \tag{4.5}$$

It contains neither an instance-encoding term nor the bit-encoding matrix. It is useful whenever $h_a \neq 0$, including when $h_r = 0$.

4.2 Hidden Block Structure

Concatenate the left and right factor matrices:

$$\mathbf{U} = [U_1 | \cdots | U_{2n}], \qquad \mathbf{T} = [T_1 | \cdots | T_{2n}]. \tag{4.6}$$

Define left and right basis matrices

$$P = [\mathbf{U} | e_k], \qquad Q = [\mathbf{T} | e_k]. \tag{4.7}$$

The polynomial in Subsection 5.3 that encodes all recovery conditions includes $\det P \det Q$. Hence P and Q are invertible whenever it is nonzero.

Let $E_r \in \mathbb{F}_p^{k\times q}$ select the q hidden coordinates of block r, so that

$$U_r = PE_r, \qquad T_r = QE_r. \tag{4.8}$$

Define the corresponding matrices in these bases

$$Z_i = Q^{-1}V_i, \qquad W_i = P^{-1}V_i, \tag{4.9}$$

$$\widehat{Z}_i = Q^{-1}V_{n+i}, \qquad \widehat{W}_i = P^{-1}S_{n+i}. \tag{4.10}$$

Then

$$G_i = P\widetilde{G}_i Q^\top, \tag{4.11}$$

where

$$\widetilde{G}_i = \Gamma_i - E_i Z_i^\top + W_i E_i^\top + E_{n+i}\widehat{Z}_i^\top - \widehat{W}_i E_{n+i}^\top, \tag{4.12}$$

$$\Gamma_i = \operatorname{diag}(\gamma_i^{(1)} I_q, \ldots, \gamma_i^{(2n)} I_q, 0). \tag{4.13}$$

Thus $\widetilde{G}_i$ is block diagonal plus terms whose rows or columns meet the two coordinate blocks

$$\mathcal{E}_i = \operatorname{col}[E_i | E_{n+i}], \qquad \dim \mathcal{E}_i = 2q. \tag{4.14}$$

For each original SUBSET-SUM index i, the two transformed-variable blocks are i and $n+i$. In public coordinates, define their right and left column spaces by

$$\mathcal{T}_i = Q\mathcal{E}_i = \operatorname{col}[T_i | T_{n+i}], \tag{4.15}$$

$$\mathcal{U}_i = P\mathcal{E}_i = \operatorname{col}[U_i | U_{n+i}]. \tag{4.16}$$

4.3 Recovering the Hidden Spaces

Assume

$$q \geq 1, \qquad 2nq + 1 \geq 30q - 4. \tag{4.17}$$

Equivalently, $n \geq 13$ for $q = 1$, $n \geq 14$ for $q = 2$, and $n \geq 15$ for $q \geq 3$. Put

$$\mathsf{S} = \{i : h_i \neq 0\}, \quad m = |\mathsf{S}|, \qquad \mathsf{Z} = \{i : h_i = 0\}, \quad z = |\mathsf{Z}|. \tag{4.18}$$

The algorithm has two public branches. Both use the commutator technique described by Soukhanov [Sou26]. Whenever A is invertible, define the matrix

$$K(A, B, C) = BA^{-1}C - CA^{-1}B. \tag{4.19}$$

Indeed,

$$[A^{-1}B, A^{-1}C] = A^{-1}K, \qquad [BA^{-1}, CA^{-1}] = KA^{-1}. \tag{4.20}$$

Thus K can be obtained from either of two ordinary matrix commutators, and its row and column spaces are public.

Weighted difference branch ($z \leq 3$). For each index i, choose distinct $x_i, y_i, w_i \in \mathsf{S} \setminus \{i\}$ and use the two ordered triples

$$(a_{i,1}, b_{i,1}, j_{i,1}) = (x_i, y_i, w_i), \qquad (a_{i,2}, b_{i,2}, j_{i,2}) = (y_i, w_i, x_i). \tag{4.21}$$

Such a choice always exists because (4.17) implies $n \geq 13$, hence $m \geq 10$. Form

$$A_{i,g} = F_{a_{i,g},b_{i,g}}, \qquad B_{i,g} = F_{a_{i,g},i}, \qquad C_{i,g} = F_{a_{i,g},j_{i,g}},$$
$$K_{i,g} = K(A_{i,g}, B_{i,g}, C_{i,g}). \tag{4.22}$$

The recovered spaces are

$$\widehat{\mathcal{T}}_i = \operatorname{row} K_{i,1} \cap \operatorname{row} K_{i,2}, \tag{4.23}$$
$$\widehat{\mathcal{U}}_i = \operatorname{col} K_{i,1} \cap \operatorname{col} K_{i,2}. \tag{4.24}$$

and are summed to obtain two column spaces of dimension $k-1$.

Zero coefficient branch ($z \geq 4$). For each $i \in \mathsf{Z}$, choose distinct $x_i, y_i, w_i \in \mathsf{Z} \setminus \{i\}$ and use the same two ordered triples (4.21). Since $D_t = G_t$ for $t \in \mathsf{Z}$, form instead

$$A^0_{i,g} = D_{b_{i,g}}, \quad B^0_{i,g} = D_i, \quad C^0_{i,g} = D_{j_{i,g}}, \qquad K^0_{i,g} = K(A^0_{i,g}, B^0_{i,g}, C^0_{i,g}). \tag{4.25}$$

Intersecting the two row spaces and the two column spaces recovers only the spaces for indices in Z. Sum them as

$$\mathcal{T}_{\mathsf{Z}} = \sum_{i \in \mathsf{Z}} \mathcal{T}_i, \qquad \mathcal{U}_{\mathsf{Z}} = \sum_{i \in \mathsf{Z}} \mathcal{U}_i. \tag{4.26}$$

Choose $k \times d$ public basis matrices

$$L_{\mathsf{U}} \text{ for } \ker \mathcal{U}_{\mathsf{Z}}^{\top}, \qquad L_{\mathsf{T}} \text{ for } \ker \mathcal{T}_{\mathsf{Z}}^{\top}, \qquad d = 2mq + 1. \tag{4.27}$$

For a fixed $j_0 \in \mathsf{Z}$, put

$$M_{\mathsf{Z}} = L_{\mathsf{U}}^{\top} D_{j_0} L_{\mathsf{T}}. \tag{4.28}$$

If M_{Z} has rank $d-1$, choose nonzero $u \in \ker M_{\mathsf{Z}}^{\top}$ and $v \in \ker M_{\mathsf{Z}}$, and output

$$\beta = L_{\mathsf{U}} u, \qquad \alpha = L_{\mathsf{T}} v. \tag{4.29}$$

If any inversion, prescribed dimension check, or nullspace check fails, the distinguisher outputs 0. Subsections 5.1–5.3 prove that, except with explicitly bounded probability, the weighted-difference branch satisfies

$$\widehat{\mathcal{T}}_i = \mathcal{T}_i, \qquad \widehat{\mathcal{U}}_i = \mathcal{U}_i \quad \text{for every } i \in [n]. \tag{4.30}$$

In the zero-coefficient branch, all spaces for indices in Z are exact and (4.29) gives the same two global null vectors without recovering the remaining pairs.

4.4 Recovering the Encrypted Bit

In the weighted-difference branch, form the public sums

$$\mathcal{U}_{\mathrm{rec}} = \sum_{i=1}^{n} \widehat{\mathcal{U}}_i, \qquad \mathcal{T}_{\mathrm{rec}} = \sum_{i=1}^{n} \widehat{\mathcal{T}}_i \tag{4.31}$$

and check that both have dimension $k-1$. Whenever the recovery conditions of Theorem 20 hold, these spaces equal $\operatorname{col}\mathbf{U}$ and $\operatorname{col}\mathbf{T}$, respectively. Compute nonzero vectors

$$\beta \in \ker \mathcal{U}_{\mathrm{rec}}^{\top}, \qquad \alpha \in \ker \mathcal{T}_{\mathrm{rec}}^{\top}. \tag{4.32}$$

The zero-coefficient branch computes vectors with the same orthogonality properties by (4.29). Every term of the All-Accept ADP has either a left factor among the columns of $\mathbf{U}$ or a right factor among the columns of $\mathbf{T}$. Hence, whenever recovery is correct,

$$\beta^{\top} M_{\mathsf{AA}}(x)\alpha = 0 \qquad \text{for every } x \in \mathbb{F}_p^{2n}. \tag{4.33}$$

Choose any $t \in \mathsf{S}$ and define

$$a_t = \ell h_t^{-1}, \qquad a_i = 0 \quad (i \neq t), \qquad \widehat{a}_i = 1 - a_i, \qquad x = (a, \widehat{a}) \in \mathbb{F}_p^{2n}. \tag{4.34}$$

Then $h \cdot a = \ell$ and $a_i + \widehat{a}_i = 1$, so $M_{H,\boldsymbol{\ell}}(x) = 0$ by (3.9). This is generally a non-binary field solution, or an invalid evaluation in the terminology of Bartusek et al. Using (3.16), the public evaluation is

$$Y_b = A_b + \sum_{r=1}^{2n} x_r B_r = M_{\mathsf{AA}}(x) + bS^{\mathsf{msg}}. \tag{4.35}$$

The distinguisher computes the scalar

$$\tau = \beta^{\top} Y_b \alpha \tag{4.36}$$

and outputs 1 exactly when $\tau \neq 0$. Denote this public algorithm by $\mathcal{A}$.

The distinguisher returns 0 if $h = 0$, an inverse does not exist, or any required rank, dimension, intersection, or nullspace check fails. It is therefore defined on every input ciphertext.

5 Proof of the Main Theorem

This section proves the attack stated informally in Theorem 1. We first establish deterministic rank bounds, then derive exact space recovery criteria, prove that those criteria hold generically, and finally translate recovery into distinguishing advantage.

5.1 Rank Bounds

We begin with the relation between Koszul flattenings and the commutators used by the attack. Fix $k \times k$ matrices A, B, C with A invertible and put

$$K = BA^{-1}C - CA^{-1}B. \tag{5.1}$$

Recall the partial flattening Φ_J from (2.4).

Lemma 10 (Partial flattening identity)**.** *For every column inclusion $J \in \mathbb{F}_p^{k \times s}$,*

$$\operatorname{rank} \Phi_J(A, B, C) = 2k + \operatorname{rank}(KJ). \tag{5.2}$$

For $J = I_k$,

$$\operatorname{rank} \Phi(A, B, C) = 2k + \operatorname{rank} K. \tag{5.3}$$

Moreover,

$$[A^{-1}B, A^{-1}C] = A^{-1}K, \qquad [BA^{-1}, CA^{-1}] = KA^{-1}. \tag{5.4}$$

Proof. The leading $2k \times 2k$ block of Φ_J is

$$K_0 = \begin{bmatrix} 0 & A \\ -A & 0 \end{bmatrix}, \qquad K_0^{-1} = \begin{bmatrix} 0 & -A^{-1} \\ A^{-1} & 0 \end{bmatrix}.$$

Its Schur complement is $-KJ$, proving (5.2). Equation (5.3) is the case $J = I_k$, and direct multiplication gives (5.4). □

We also need the following rank bound for triples whose matrices span a two-dimensional space.

Lemma 11 (Two-dimensional slice span)**.** *Suppose three matrices lie in the span of two matrices, and their joint row span and joint column span each have dimension at most m. Then their Koszul flattening has rank at most $2m$.*

Proof. After embedding the row and column spaces into m dimensions and extending the field algebraically, it suffices to consider two $m \times m$ matrices. Pairs for which the first matrix is invertible and its inverse times the second has distinct eigenvalues form a dense set. Such a pair decomposes as

$$M_0 = UV^\top, \qquad M_1 = U\Lambda V^\top$$

with Λ diagonal. It is therefore a sum of at most m triples whose matrix factor has rank one. Each such triple contributes rank at most two to the Koszul flattening. The condition that a matrix have rank at most $2m$ is preserved under limits, so the same bound holds for every pair. Extending the field does not change matrix rank. □

We now apply these facts block by block. Work in the hidden bases of Subsection 4.2. Fix four distinct indices $\{a, b, i, j\}$ and write $(\widetilde{A}, \widetilde{B}, \widetilde{C})$ for the three matrices after the basis change. Put $\widetilde{K} = K(\widetilde{A}, \widetilde{B}, \widetilde{C})$. For an index t, define its three coefficients by

$$\lambda_t = \begin{cases} (-h_b, -h_i, -h_j), & t = a, \\ (h_a, 0, 0), & t = b, \\ (0, h_a, 0), & t = i, \\ (0, 0, h_a), & t = j, \\ (0, 0, 0), & \text{otherwise.} \end{cases} \tag{5.5}$$

The diagonal coefficients on each block form an arbitrary vector in $\mathbb{F}_p^3$, while the off-diagonal terms at index t are multiplied by λ_t. Because $a, b, j \in \mathsf{S}$, exactly four indices are active even when $h_i = 0$.

Lemma 12 (Inactive and active contributions)**.** *An inactive index contributes at most* $4q$ *to the flattening rank. An active index contributes at most* $8q$*.*

Proof. For $d = (d_1, d_2, d_3) \in \mathbb{F}_p^3$, write $d \otimes M$ for the triple $(d_1 M, d_2 M, d_3 M)$. For an inactive index, the triple of block slices is

$$d \otimes (EE^\top)$$

for some $d \in \mathbb{F}_p^3$. Since $EE^\top$ has rank q, this is a sum of q triples whose matrix factor has rank one; each contributes at most two to the flattening. The two blocks for that index together contribute at most $4q$.

For an active index, the triple of block slices is

$$d \otimes (EE^\top) + \lambda_t \otimes X, \qquad X = -EZ^\top + WE^\top. \tag{5.6}$$

All columns lie in $\mathrm{span}(E, W)$ and all rows in $\mathrm{span}(E, Z)$, each of dimension at most $2q$; the three matrices span a space of dimension at most two. Lemma 11 therefore bounds their flattening rank by $4q$. The two blocks together contribute at most $8q$. □

Summing Lemma 12 over $n - 4$ inactive and four active indices gives

$$\begin{aligned} \operatorname{rank} \Phi(\widetilde{A}, \widetilde{B}, \widetilde{C}) &\le (n-4)4q + 4 \cdot 8q \\ &= 4nq + 16q = 2k + 16q - 2. \end{aligned} \tag{5.7}$$

By Lemma 10, the hidden-coordinate matrix $\widetilde{K}$ satisfies

$$\operatorname{rank} \widetilde{K} \le r := 16q - 2. \tag{5.8}$$

We next bound the part of $\widetilde{K}$ outside the target blocks. Let J_i include every hidden coordinate except the two target blocks E_i, E_{n+i}. Thus $E^\top J_i = 0$ for either target selector E.

Lemma 13 (Rank bound outside the target blocks)**.** *For the target* i*,*

$$\operatorname{rank}(\widetilde{K} J_i) \le 14q - 2, \tag{5.9}$$

and

$$\operatorname{rank}(J_i^\top \widetilde{K}) \le 14q - 2. \tag{5.10}$$

Proof. The off-diagonal target terms appear only in the middle matrix. One target block therefore has slices

$$A_E = aEE^\top, \qquad B_E = bEE^\top + X, \qquad C_E = cEE^\top,$$
$$X = -EZ^\top + WE^\top.$$

Define the $3k \times q$ column blocks

$$L_1 = \begin{bmatrix} E \\ 0 \\ 0 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 \\ aE \\ bE + W \end{bmatrix}, \quad L_3 = \begin{bmatrix} 0 \\ 0 \\ E \end{bmatrix}.$$

The three domain blocks of the partial flattening satisfy

$$\begin{bmatrix} 0 \\ -A_E \\ -B_E \end{bmatrix} = L_2(-E^\top) + L_3 Z^\top,$$
$$\begin{bmatrix} A_E \\ 0 \\ -C_E \end{bmatrix} = L_1(aE^\top) + L_3(-cE^\top),$$
$$\begin{bmatrix} B_E J_i \\ C_E J_i \\ 0 \end{bmatrix} = L_1(-Z^\top J_i).$$

Hence one target block contributes at most $3q$ to Φ_{J_i}, and both target blocks contribute at most $6q$. The other three active indices contribute at most $8q$ each and the inactive indices at most $4q$, so

$$\begin{aligned} \operatorname{rank} \Phi_{J_i}(\widetilde{A}, \widetilde{B}, \widetilde{C}) &\le (n-4)4q + 3 \cdot 8q + 6q \\ &= 2k + 14q - 2. \end{aligned} \tag{5.11}$$

Lemma 10 gives (5.9). Apply the same argument to $(\widetilde{A}^\top, \widetilde{B}^\top, \widetilde{C}^\top)$ to obtain (5.10). □

The zero coefficient branch gives smaller bounds because its triples have only the three active indices b, i, j. Write $(\widetilde{A}^0, \widetilde{B}^0, \widetilde{C}^0)$ for such a triple in the hidden bases and $\widetilde{K}^0 = K(\widetilde{A}^0, \widetilde{B}^0, \widetilde{C}^0)$. Lemma 12 therefore gives

$$\operatorname{rank} \Phi(\widetilde{A}^0, \widetilde{B}^0, \widetilde{C}^0) \le (n-3)4q + 3 \cdot 8q = 2k + 12q - 2, \tag{5.12}$$
$$\operatorname{rank} \widetilde{K}^0 \le r_0 := 12q - 2. \tag{5.13}$$

After removing the target blocks, those two blocks contribute at most $6q$, the other two active indices contribute at most $8q$ each, and every inactive index contributes at most $4q$. Hence

$$\operatorname{rank}(\widetilde{K}^0 J_i),\ \operatorname{rank}(J_i^\top \widetilde{K}^0) \le 10q - 2. \tag{5.14}$$

5.2 Space Recovery

The preceding rank bounds first imply containment of the target space.

Proposition 14 (Target space containment)**.** *In the hidden bases of Subsection 4.2, if $\widetilde{K}$ attains rank $16q-2$, then both its row space and its column space contain $\mathcal{E}_i$.*

Proof. Let $\mathcal{R} = \operatorname{row} \widetilde{K}$. Projection to the non-target coordinates has dimension at most $14q - 2$ by Lemma 13. If $\dim \mathcal{R} = 16q - 2$, the kernel of this projection inside $\mathcal{R}$ has dimension at least

$$(16q - 2) - (14q - 2) = 2q.$$

It is contained in the $2q$-dimensional target coordinate space $\mathcal{E}_i$, so it equals $\mathcal{E}_i$. The column statement follows identically from (5.10). □

We next show that intersecting two public spaces reduces this containment to equality. For each public matrix $K_{i,g}$ in (4.22), define its hidden-coordinate form $\widetilde{K}_{i,g}$ by

$$K_{i,g} = P\widetilde{K}_{i,g}Q^{\top}. \tag{5.15}$$

Proposition 15 (Recovery from two matrices)**.** *Suppose for a fixed index i that both hidden-coordinate matrices $\widetilde{K}_{i,1}, \widetilde{K}_{i,2}$ have rank $r = 16q - 2$ and their row-space sum has dimension*

$$\sigma = 30q - 4 = 2r - 2q. \tag{5.16}$$

Then

$$\operatorname{row} \widetilde{K}_{i,1} \cap \operatorname{row} \widetilde{K}_{i,2} = \mathcal{E}_i.$$

If their column-space sum has the same dimension, then

$$\operatorname{col} \widetilde{K}_{i,1} \cap \operatorname{col} \widetilde{K}_{i,2} = \mathcal{E}_i.$$

After undoing the hidden bases, the public intersections are respectively $\mathcal{T}_i$ and $\mathcal{U}_i$.

Proof. By Proposition 14, both spaces contain $\mathcal{E}_i$. The dimension formula gives

$$\dim(\operatorname{row} \widetilde{K}_{i,1} \cap \operatorname{row} \widetilde{K}_{i,2}) = 2r - \sigma = 2q.$$

Thus the intersection is exactly $\mathcal{E}_i$. The column argument is identical. Under (5.15), the hidden row-space intersection $\mathcal{E}_i$ maps to $Q\mathcal{E}_i = \mathcal{T}_i$, while the hidden column-space intersection maps to $P\mathcal{E}_i = \mathcal{U}_i$. □

The same argument yields exact recovery in the zero coefficient branch. As in Proposition 14, rank r_0 forces both the row and column spaces to contain $\mathcal{E}_i$. Two such spaces whose sum has dimension

$$\sigma_0 = 22q - 4 = 2r_0 - 2q \tag{5.17}$$

therefore intersect exactly in $\mathcal{E}_i$. Thus the zero-coefficient branch recovers $\mathcal{T}_i$,$\mathcal{U}_i$ for every $i \in \mathsf{Z}$ under these rank equalities, using the same public-to-hidden change of bases as in (5.15).

5.3 Generic Success

The rank bounds of Subsection 5.1 and the recovery criteria of Subsection 5.2 reduce exact recovery to specific rank equalities. We now prove that all of them hold simultaneously except when one explicit polynomial vanishes. The matrices for different indices are dependent, so separate heuristic "random matrix" claims would not suffice.

To encode these rank conditions polynomially, for a triple (A, B, C) define

$$\mathcal{N} = B \operatorname{adj}(A) C - C \operatorname{adj}(A) B. \tag{5.18}$$

When $\det A \neq 0$, the adjugate identity gives

$$\mathcal{N} = \det(A)K. \tag{5.19}$$

Thus one polynomial matrix certifies both the row and column spaces needed by the attack without introducing rational functions into the success polynomial.

For target i and group g, let

$$\delta_{i,g} = \det A_{i,g}. \tag{5.20}$$

Let $\rho_{i,g}$ be a selected $(16q-2)$-minor of $\mathcal{N}_{i,g}$. Let η_i^R be a selected $(30q-4)$-minor of

$$[\mathcal{N}_{i,1}^\top | \mathcal{N}_{i,2}^\top] \tag{5.21}$$

and η_i^L the corresponding minor of

$$[\mathcal{N}_{i,1} | \mathcal{N}_{i,2}]. \tag{5.22}$$

The ρ factors certify individual rank $16q-2$; the η factors certify sum dimension $30q-4$. For the zero-coefficient branch, the definitions are identical with minor sizes $r_0 = 12q-2$ and $\sigma_0 = 22q-4$.

It remains to show that the selected minors are not identically zero for all admissible parameters. We use three fixed integral assignments in the hidden bases, with $P = Q = I$, at $(n,q) = (13,1), (14,2), (15,1)$. At $(15,1)$ we use both the full assignment and the restriction obtained by removing the final e_k coordinate; we call these the *full* and *truncated* assignments. Appendix A specifies the assignments and the selected row and column indices.

For four matrices (G_a, G_b, G_i, G_j), the three cases use

$$\begin{aligned}
\text{weighted, } h_i \neq 0: &\quad (A,B,C) = (G_b - G_a, G_i - G_a, G_j - G_a),\\
\text{weighted, } h_i = 0: &\quad (A,B,C) = (G_b - G_a, G_i, G_j - G_a),\\
\text{zero coefficients}: &\quad (A,B,C) = (G_b, G_i, G_j).
\end{aligned}$$

The corresponding minor evaluations are listed in Table 1 of Appendix A; every listed value is nonzero over $\mathbb{F}_{1009}$.

Let $\mathcal{F}_{\text{base}}$ contain the integer evaluation of every δ, ρ, and η factor in the twelve rows of Table 1. Every value has nonzero reduction modulo 1009, so every underlying integer is nonzero. Let $\mathcal{P}_{\text{exc}}$ be the set of prime divisors of their product. This is a fixed finite set, independent of n, q, the public instance, and the index being recovered. The explicit description in Appendix A makes each of these finite calculations independently checkable.

Lemma 16 (Nonzero minors for all parameters)**.** *For every (n,q) satisfying (4.17), every index $i \in [n]$, and every prime $p \notin \mathcal{P}_{\text{exc}}$, there is an assignment to the hidden-basis variables for each of the weighted-nonzero, weighted-zero, and zero-coefficient cases, for which*

1. *both invertibility determinants $\delta_{i,g}$ are nonzero;*

2. *both individual minors $\rho_{i,g}$ of the case's prescribed size are nonzero; and*

3. *both sum minors $\eta_i^{R/L}$ are nonzero.*

Proof. Map base indices $1, 2, 3, 4$ to i and its three chosen auxiliary indices, then extend this injection arbitrarily to the remaining indices. For $q = 1$, the $(13, 1)$ assignments extend to every $n \geq 13$; for $q = 2$, the $(14, 2)$ assignments extend to every $n \geq 14$. On each added block set all off-diagonal variables to zero. For the weighted-nonzero and weighted-zero cases set

$$(G_i, G_{x_i}, G_{y_i}, G_{w_i}) = (3I, 0, I, 2I). \tag{5.23}$$

For the weighted-nonzero case the two restrictions are $(A, B, C) = (I, 3I, 2I)$ and $(I, 2I, -I)$; for the weighted-zero case they are $(I, 3I, 2I)$ and $(I, 3I, -I)$. Thus every matrix $K(A, B, C)$ vanishes while both matrices A remain invertible. For the zero-coefficient case use $(3I, 0, I, I)$; its restrictions are $(I, 3I, I)$ and $(I, 3I, 0)$. Again the matrices K vanish and the matrices A are invertible. The selected minors on the original blocks are unchanged.

For every q at $n = 15$, take one copy of the full $(15, 1)$ assignment and $q - 1$ copies of its truncated assignment. Form their direct sum, initially ordering coordinates by direct-sum copy, and then permute them so that the q coordinates belonging to each scheme block are consecutive, according to

$$(r, \text{copy}) \longmapsto rq + \text{copy},$$

followed by the final e_k coordinate. This assignment has $P = Q = I_k$; each U_r, T_r selects the q coordinates of block r; the off-diagonal matrices are direct sums of the base matrices; and each $\gamma_i^{(r)}$ is shared across copies, giving precisely $\gamma_i^{(r)} I_q$. Choosing $c_i^{(r)} = \gamma_i^{(r)}$ and $c_{n+i}^{(r)} = 0$ realizes every difference.

Individual ranks and two-space sum dimensions add across copies:

$$14 + 16(q - 1) = 16q - 2, \tag{5.24}$$

$$26 + 30(q - 1) = 30q - 4. \tag{5.25}$$

For the zero-coefficient case the corresponding equalities are

$$10 + 12(q - 1) = 12q - 2, \qquad 18 + 22(q - 1) = 22q - 4. \tag{5.26}$$

Under the direct-sum lift, each selected submatrix is block diagonal up to row and column permutations. Its determinant is therefore, up to sign, a product of the full and truncated values in Table 1 and powers of nonzero determinant values. It remains nonzero for every $p \notin \mathcal{P}_{\text{exc}}$. Additional diagonal identity blocks cover every $n > 15$. □

The condition (4.17) is necessary for this two-matrix intersection proof. Indeed, two rank-$(16q - 2)$ spaces that both contain the required $2q$-space and intersect exactly there have sum dimension $30q - 4$, which must fit in the ambient dimension $k = 2nq + 1$.

Although the witnessing assignment may depend on i, Lemma 16 shows that every selected determinant is a nonzero polynomial in the common setup variables. Their product is therefore nonzero.

We now combine the selected determinants into a single success polynomial. Fix $h \neq 0$. The deterministic auxiliary choices in Subsection 4.3 fix one list of selected minors. In the weighted-difference branch define

$$\Pi_h^{\mathrm{weighted}} = \det P \det Q \prod_{i=1}^{n} \left(\eta_i^R \eta_i^L \prod_{g=1}^{2} \delta_{i,g} \rho_{i,g} \right), \tag{5.27}$$

using the weighted-nonzero case when $h_i \neq 0$ and the weighted-zero case when $h_i = 0$. In the zero-coefficient branch fix $j_0 \in \mathsf{Z}$ and define

$$\Pi_h^{\mathrm{zero}} = \det P \det Q \prod_{i \in \mathsf{Z}} \left(\eta_i^R \eta_i^L \prod_{g=1}^{2} \delta_{i,g} \rho_{i,g} \right) \prod_{s \in \mathsf{S} \cup (n+\mathsf{S})} \gamma_{j_0}^{(s)}, \tag{5.28}$$

where $n + \mathsf{S} = \{n + s : s \in \mathsf{S}\}$. Write Π_h for the polynomial selected by the branch. Lemma 16 proves that, for every $p \notin \mathcal{P}_{\mathrm{exc}}$,

$$\Pi_h \not\equiv 0 \quad \text{over } \mathbb{F}_p. \tag{5.29}$$

Indeed, suppose first that $h_i \neq 0$, and let $G_t^\star$ denote the matrices in a witnessing assignment for the weighted-nonzero case. Set $G_t = h_t G_t^\star$ for each $t \in \{a, b, i, j\}$. Then the three weighted matrices are

$$A = h_a h_b A^\star, \qquad B = h_a h_i B^\star, \qquad C = h_a h_j C^\star.$$

If $h_i = 0$, scale the three auxiliary matrices in the same way and leave $G_i = G_i^\star$; then $B = h_a G_i^\star$, which is the weighted-zero case up to nonzero matrix scalars. Scaling A, B, C independently by nonzero scalars multiplies each δ factor and individual numerator minor by a nonzero scalar. In a sum minor, the selected columns from each numerator block likewise acquire only a nonzero block scalar. Hence every η factor also remains nonzero, even though different indices may use different witnessing assignments. The zero-coefficient branch uses its witnessing assignment directly. Finally, every γ factor in (5.28) is a nonzero linear polynomial. The integral-domain argument above therefore applies to the complete product.

The following lemma bounds the degree of this polynomial.

Lemma 17 (Degree bound)**.** *Assume (4.17), let $h \in \mathbb{F}_p^n \setminus \{0\}$, and let $k = 2nq+1$. Write "wt" for the weighted-difference branch. The degree of $\Pi_h^{\mathrm{weighted}}$ is at most*

$$\begin{aligned} \Delta_{\mathrm{wt}} &= 2(k-1) + n\big(6k + 6(k+1)(46q-6)\big) \\ &= 2(k-1) + n\big((276q-30)k + 276q - 36\big) < 552n^2q^2. \end{aligned} \tag{5.30}$$

The degree of Π_h^{zero} is at most

$$\begin{aligned} \Delta_{\mathrm{zero}} &= 2(k-1) + z\big(6k + 6(k+1)(34q-6)\big) + 2m \\ &= 2(k-1) + z\big((204q-30)k + 204q - 36\big) + 2m < 408n^2q^2. \end{aligned} \tag{5.31}$$

Proof. Each public F-matrix entry has degree at most three in the independent setup entries: bilinear terms have degree two and $cUT^\top$ has degree three. The public h_i have degree zero. Therefore

$$\deg \delta_{i,g} \le 3k. \tag{5.32}$$

Each adjugate entry is a $(k-1)$-minor and has degree at most $3(k-1)$. Every entry of $\mathcal{N}$ consequently has degree at most

$$3 + 3(k-1) + 3 = 3(k+1). \tag{5.33}$$

Put $r = 16q - 2$ and $\sigma = 30q - 4$. Then

$$\deg \rho_{i,g} \le 3(k+1)r, \qquad \deg \eta_i^{R/L} \le 3(k+1)\sigma. \tag{5.34}$$

The determinants $\det P$ and $\det Q$ each have degree $k-1$. There are two δ factors, two ρ factors, and two η factors per recovered index. This gives Δ_{wt}. For the zero-coefficient branch, substitute $r_0 = 12q - 2$, $\sigma_0 = 22q - 4$, use only the z zero indices, and add the $2m$ linear γ factors, giving Δ_{zero}. Since (4.17) implies $n \ge 13$, direct substitution yields

$$\begin{aligned} \Delta_{\mathrm{wt}} &= 552n^2q^2 - 60n^2q + 556nq - 66n < 552n^2q^2, \\ \Delta_{\mathrm{zero}} &\le 408n^2q^2 - 60n^2q + 412nq - 64n < 408n^2q^2. \end{aligned}$$

□

The independently sampled formula term admits a sharper bound.

Lemma 18 (Failure bound for the independent formula term)**.** *Assume* (4.17)*, $h \in \mathbb{F}_p^n \setminus \{0\}$, and $p \notin \mathcal{P}_{\mathrm{exc}}$. For the variant with the independent term $S_i T_i^\top$ in the coefficient for w_i, the recovery failure probability is at most $\Delta_{\mathrm{wt}}^{\mathrm{ind}}/p$ when $z \le 3$ and at most $\Delta_{\mathrm{zero}}^{\mathrm{ind}}/p$ when $z \ge 4$, where "ind" denotes this independent variant and*

$$\Delta_{\mathrm{wt}}^{\mathrm{ind}} = 2(k-1) + n\big(2k + 2(k+1)(46q-6)\big) < 184n^2q^2, \tag{5.35}$$

$$\Delta_{\mathrm{zero}}^{\mathrm{ind}} = 2(k-1) + z\big(2k + 2(k+1)(34q-6)\big) + 2m < 136n^2q^2. \tag{5.36}$$

Proof. First expose all U_r, T_r. The probability that P or Q is singular is at most $2(k-1)/p$. Conditional on fixed invertible P, Q, transform the independent matrices to $P^{-1}S_i$ and $Q^{-1}V_i$, and transform the matrices for $\widehat{w}_i$ similarly. These hidden matrices and the γ variables remain jointly independent and uniform. Every entry in the hidden bases now has degree at most one. The public and hidden matrices satisfy $K_{\mathrm{pub}} = PK_{\mathrm{hid}}Q^\top$, so all rank and intersection events are identical.

Let $\widetilde{\Pi}_h$ be the product of the same fixed selected hidden-coordinate invertibility determinants, rank minors, and sum minors (and, in the zero-coefficient branch, the same γ factors), omitting $\det P \det Q$. The explicit minor evaluations make this conditional polynomial nonzero. A determinant $\det A$ has degree k, an entry of $\mathcal{N}$ has degree $k+1$, and one recovered index contributes

$2k+2(k+1)(r+\sigma)$. Add the basis-failure term and substitute $r+\sigma = 46q-6$ to obtain (5.35). The zero-coefficient formula uses $r_0+\sigma_0 = 34q-6$ and the same $2m$ scalar factors. Substituting $k = 2nq+1$ and $n \geq 13$ gives the displayed strict inequalities. This conditioning argument gives the stated unconditional failure bounds. It uses the independence of the two formula terms and therefore does not improve the bound for the $V_i T_i^\top$ term, where those terms are dependent. □

For the zero coefficient branch, the same success event also provides the required global null vectors.

Lemma 19 (Null vectors in the zero coefficient branch)**.** *Assume* (4.17)*, $h \in \mathbb{F}_p^n \setminus \{0\}$, $z \geq 4$, and $p \notin \mathcal{P}_{\mathrm{exc}}$. On $\Pi_h^{\mathrm{zero}} \neq 0$, the vectors in* (4.29) *are orthogonal to all columns of $\mathbf{U}$ and $\mathbf{T}$, respectively.*

Proof. The rank conditions recover every space indexed by Z. Let $\mathbf{U}_\mathsf{Z}$ and $\mathbf{T}_\mathsf{Z}$ concatenate both blocks $i, n+i$ for $i \in \mathsf{Z}$, and define $\mathbf{U}_\mathsf{S}$ and $\mathbf{T}_\mathsf{S}$ analogously for $i \in \mathsf{S}$. The basis matrices $L_\mathsf{U}, L_\mathsf{T}$ in (4.27) have $d = 2mq+1$ columns. In $L_\mathsf{U}^\top D_{j_0} L_\mathsf{T}$, each off-diagonal term at j_0 vanishes: its left factor lies in $\mathcal{U}_{j_0} \subseteq \mathcal{U}_\mathsf{Z}$ or its right factor lies in $\mathcal{T}_{j_0} \subseteq \mathcal{T}_\mathsf{Z}$. Every diagonal term indexed by Z also vanishes. Therefore

$$M_\mathsf{Z} = X \Lambda Y^\top, \qquad X = L_\mathsf{U}^\top \mathbf{U}_\mathsf{S}, \quad Y = L_\mathsf{T}^\top \mathbf{T}_\mathsf{S}, \tag{5.37}$$
$$\Lambda = \mathrm{diag}(\gamma_{j_0}^{(s)} I_q : s \in \mathsf{S} \cup (n+\mathsf{S})).$$

On $\det P \neq 0$, the columns of $[\mathbf{U}_\mathsf{Z} | \mathbf{U}_\mathsf{S}]$ are independent. Moreover, $\ker L_\mathsf{U}^\top = \mathcal{U}_\mathsf{Z}$. If $Xc = 0$, then $\mathbf{U}_\mathsf{S} c \in \mathcal{U}_\mathsf{Z}$, and independence forces $c = 0$. Thus X has full column rank $2mq$. The identical argument with Q, L_T, T shows that Y has full column rank. The γ factors make Λ invertible. Thus $\mathrm{rank}\, M_\mathsf{Z} = 2mq = d-1$.

If $u^\top M_\mathsf{Z} = 0$, the full row rank of $Y^\top$ and invertibility of Λ imply $u^\top X = 0$. Hence $(L_\mathsf{U} u)^\top$ is orthogonal to both the recovered $\mathbf{U}_\mathsf{Z}$ columns and the remaining $\mathbf{U}_\mathsf{S}$ columns. The argument for $M_\mathsf{Z} v = 0$ and $L_\mathsf{T} v$ is symmetric. □

Combining these results gives simultaneous recovery.

Theorem 20 (Simultaneous space recovery)**.** *Assume $q \geq 1$ and $2nq+1 \geq 30q-4$. For every $p \notin \mathcal{P}_{\mathrm{exc}}$ and every public coefficient vector $h \in \mathbb{F}_p^n \setminus \{0\}$, define $\Delta(h) = \Delta_{\mathrm{wt}}$ when $z \leq 3$ and $\Delta(h) = \Delta_{\mathrm{zero}}$ when $z \geq 4$. Then*

$$\Pr[\textit{the algorithm fails to obtain the two global null vectors}] \leq \frac{\Delta(h)}{p}. \tag{5.38}$$

On the complementary event, the weighted-difference branch recovers every space $\mathcal{T}_i, \mathcal{U}_i$; the zero-coefficient branch recovers the spaces for $i \in \mathsf{Z}$ and obtains the same global null vectors through Lemma 19.

Proof. Apply Lemma 4 once to the single nonzero branch polynomial Π_h, using Lemma 17. In the weighted-difference branch, its nonvanishing gives the rank and sum conditions of Proposition 15 for every index. In the zero-coefficient

branch it gives the zero coefficient rank and intersection conditions of Subsections 5.1 and 5.2 for every zero coefficient, together with the scalar conditions of Lemma 19. Thus one Schwartz–Zippel application controls all indices and selected minors simultaneously. □

5.4 Distinguishing Advantage

We now translate recovery into output probabilities. If $b = 0$, Equation (4.33) gives $\tau = 0$ on the good event, so

$$\Pr[\mathcal{A}(C_0) = 1] \le \frac{\Delta(h)}{p}. \tag{5.39}$$

For $b = 1$, the conditioning must be handled explicitly. The bit-encoding matrix S^{msg} appears only in the constant ciphertext matrix A_b. Every recovery computation and the event $\Pi_h \neq 0$ depend only on the public coefficient matrices B_r. Thus S^{msg} remains independent and uniform after conditioning on the recovered nonzero α, β.

For fixed nonzero α, β, the map

$$S \longmapsto \beta^\top S \alpha \tag{5.40}$$

is a nonzero linear functional on $\mathbb{F}_p^{k\times k}$. Therefore

$$\Pr[\beta^\top S^{\mathsf{msg}} \alpha = 0 \mid \Pi_h \neq 0] = \frac{1}{p}, \tag{5.41}$$

and

$$\Pr[\mathcal{A}(C_1) = 1] \ge \left(1 - \frac{\Delta(h)}{p}\right)\left(1 - \frac{1}{p}\right) \ge 1 - \frac{\Delta(h)+1}{p}. \tag{5.42}$$

Combining (5.39) and (5.42) gives soundness advantage at least

$$1 - \frac{2\Delta(h)+1}{p}. \tag{5.43}$$

Theorem 21 (Attack on the Witness Encryption Candidate)**.** *There is a fixed finite set of primes $\mathcal{P}_{\mathrm{exc}}$ such that, for every $q \ge 1$ and n satisfying $2nq + 1 \ge 30q - 4$, every prime $p \notin \mathcal{P}_{\mathrm{exc}}$, and every SUBSET-SUM instance $I = (h, \ell)$ that is a NO instance modulo p and satisfies $h \not\equiv 0 \pmod p$, a deterministic algorithm using only the public instance and ciphertext matrices distinguishes encryptions of 0 and 1 in the distribution defined in Section 3 with soundness advantage at least*

$$\max\left\{0,\, 1 - \frac{2\Delta(h)+1}{p}\right\},$$

where

$$\Delta(h) = \begin{cases} \Delta_{\mathrm{wt}} < 552n^2q^2, & z \le 3, \\ \Delta_{\mathrm{zero}} < 408n^2q^2, & z \ge 4, \end{cases}.$$

More precisely, when its output is interpreted as the encrypted bit,

$$\Pr[\widehat{b} = 1 \mid b = 0] \le \frac{\Delta(h)}{p}, \qquad \Pr[\widehat{b} = 0 \mid b = 1] \le \frac{\Delta(h)+1}{p}.$$

Consequently, for a uniform challenge bit its message-recovery probability is at least $1 - (2\Delta(h)+1)/(2p)$ *whenever this bound is nonvacuous. With ordinary matrix elimination, the algorithm uses* $O(nk^3)$ *field operations and is polynomial in the ciphertext length and* $\log p$*. If the printed term* $V_i T_i^\top$ *is replaced by the independently sampled* $S_i T_i^\top$ *term, the same attack has the sharper bounds* $\Delta^{\mathrm{ind}}_{\mathrm{wt}} < 184n^2q^2$ *for* $z \le 3$ *and* $\Delta^{\mathrm{ind}}_{\mathrm{zero}} < 136n^2q^2$ *for* $z \ge 4$*.*

Proof. The raw differences and both branches are public. Theorem 20 and Equations (5.39)–(5.43) therefore prove the distinguishing bound for every stated I. For every index, the algorithm performs a constant number of $k \times k$ inversions, products, rank computations, and subspace intersections. Summing over n indices gives $O(nk^3)$ field operations with classical matrix arithmetic.

For the $S_i T_i^\top$ variant, the two matrices in the terms for w_i are independent. The rank bounds already permit this, and every witnessing assignment remains valid in the larger parameter space after setting $S_i = V_i$. Thus the attack applies, and Lemma 18 gives the sharper conditioning-based failure bounds. □

Remark 22 (The case $h = 0$)**.** If $\ell \neq 0$ in $\mathbb{F}_p$, then R_0 occurs only as the independent uniform term $-\ell R_0$ in the constant ciphertext matrix. Conditional on all coefficient matrices, the constant matrix is uniform for either message bit, so the two ciphertext distributions are identical. Under the no-wrap encoding, the remaining case $h = 0, \ell = 0$ has the empty Boolean witness and is not a NO instance. If an integer input reduces to this case modulo p, the modular instance is true and lies outside Theorem 21.

Corollary 23 (Asymptotic witness encryption security failure)**.** *Fix* $\varepsilon > 0$*, let* $q(n) = \lceil n^\varepsilon \rceil$*, and let* $p(n)$ *be any prime sequence satisfying*

$$\frac{p(n)}{n^c} \longrightarrow \infty \qquad \text{for every constant } c > 0.$$

For the efficiently generated integer NO instances I_n *from* (1.1)*, the distinguisher of Theorem 21 has soundness advantage* $1 - \mathrm{negl}(n)$ *for all sufficiently large* n*. Equivalently, in the uniform-challenge-bit game its guessing probability is* $1 - \mathrm{negl}(n)$*.*

Proof. Lemma 6 proves that I_n is a NO instance modulo $p(n)$ for all sufficiently large n because then $p(n) > n + 1$, and every coefficient equals one in $\mathbb{F}_{p(n)}$. Moreover, $\Delta_{\mathrm{wt}} = O(n^{2+2\varepsilon})$, while a fixed finite set $\mathcal{P}_{\mathrm{exc}}$ contains no unbounded prime sequence eventually. Hence $\Delta_{\mathrm{wt}}/p(n) = \mathrm{negl}(n)$, and the claim follows from (5.43) and (2.2). □

The convention for the field size deserves one clarification. Bartusek et al. write the field condition as $p = \omega(\mathrm{poly}(n))$. Corollary 23 uses their accompanying

prose interpretation as superpolynomial growth. If the notation is instead read as only $p = \omega(n^C)$ for one unspecified exponent C, the bound in Theorem 21 remains unconditional, while negligibility requires the additional quantitative condition $\Delta(h)/p = \mathrm{negl}(n)$.

Acknoledgement

AI usage disclosure

GPT-5.6 Sol was used in the discovery and development of the attack presented in this paper. OpenAI Codex was used to assist with manuscript preparation and with implementation experiments used to check the attack. The author reviewed the AI-assisted work, independently checked the stated mathematical claims and computational results, and takes full responsibility for the paper's contents and correctness.

References

[BIJ+20] James Bartusek, Yuval Ishai, Aayush Jain, Fermi Ma, Amit Sahai, and Mark Zhandry. Affine determinant programs: A framework for obfuscation and witness encryption. In *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*, LIPIcs 151, Article 82, 2020. https://doi.org/10.4230/LIPIcs.ITCS.2020.82.

[GGSW13] Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications. In *45th Annual ACM Symposium on Theory of Computing (STOC)*, pages 467–476, 2013.

[Sch80] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[SRE+26] Lev Soukhanov, Yaroslav Rebenko, Muhammad El Gebali, Mikhail Komarov, Handan Kilinc-Alper, Michel Abdalla, and Patrick Towa. Implementable witness encryption from arithmetic affine determinant programs. Cryptology ePrint Archive, Paper 2026/175, 2026. https://eprint.iacr.org/2026/175.

[Sou26] Lev Soukhanov. *AADP WE commutator attack & patch.* Research post, alloc[init], June 9, 2026. https://www.allocinit.xyz/posts/commutator-attack.

[YCY22] Li Yao, Yilei Chen, and Yu Yu. Cryptanalysis of candidate obfuscators for affine determinant programs. In *Advances in Cryptology—EUROCRYPT 2022*, LNCS 13276, Springer, 2022. Full version: https://eprint.iacr.org/2021/1684.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *EUROSAM 1979*, LNCS 72, pages 216–226, 1979.

A Explicit Minor Evaluations

For each $(n, q) \in \{(13, 1), (14, 2), (15, 1)\}$, set $k = 2nq + 1$, reset $s_0 = 1$, and generate

$$s_{t+1} = 1103515245 s_t + 12345 \pmod{2^{31}}, \qquad u_t = s_{t+1} \bmod 1009.$$

Without resetting again for that base point, consume the u_t first to fill $(\gamma_i^{(s)}) \in \mathbb{F}_{1009}^{n \times 2n}$ in lexicographic order (i, s), and then to fill, in this order, $(Z_i)_{i \in [n]}$, $(\widehat{Z}_i)_{i \in [n]}$, and $(\widehat{W}_i)_{i \in [n]}$, each of shape $n \times k \times q$, in lexicographic order $(i, \text{row}, \text{column})$; set $W_i = Z_i$ and use the $P = Q = I_k$ hidden form of Subsection 4.2. Using one-based scheme indices, take target $i = 1$, auxiliaries $(x_i, y_i, w_i) = (2, 3, 4)$, and groups $(a_{i,1}, b_{i,1}, j_{i,1}) = (2, 3, 4)$ and $(a_{i,2}, b_{i,2}, j_{i,2}) = (3, 4, 2)$. The truncated $(15, 1)$ assignment is obtained from the same full assignment by deleting the final e_k coordinate, equivalently the last row and column of every G_i, without generating a new stream. For the integer evaluations defining $\mathcal{P}_{\text{exc}}$, regard each u_t as its displayed representative in $\{0, \ldots, 1008\}$ and evaluate the same determinant polynomials over $\mathbb{Z}$.

We index rows and columns from zero and next list the indices that define the fixed minors. Write $[a{:}b] = \{a, a + 1, \ldots, b\}$ and concatenate disjoint lists in the order shown. Every ρ minor below is principal. The η row and column lists apply, respectively, to both $[\mathcal{N}_1^\top | \mathcal{N}_2^\top]$ and $[\mathcal{N}_1 | \mathcal{N}_2]$; only their determinant values differ.

The weighted-nonzero and weighted-zero cases use the same index lists:

$$\begin{aligned}
(13,1):\quad & I_1 = [0{:}11], 13, 16, & I_2 &= [0{:}11], 13, 14,\\
& R_\eta = [0{:}25], & C_\eta &= [0{:}11], 13, 16, [27{:}36], 40, 41;\\
(14,2):\quad & I_1 = [0{:}25], 28, 29, 34, 35, & I_2 &= [0{:}25], 28, 29, 30, 31,\\
& R_\eta = [0{:}55], & C_\eta &= [0{:}25], 28, 29, 34, 35, [57{:}78], [85{:}88];\\
(15,1)\text{ full}:\quad & I_1 = [0{:}11], 15, 18, & I_2 &= [0{:}11], 15, 16,\\
& R_\eta = [0{:}25], & C_\eta &= [0{:}11], 15, 18, [31{:}40], 46, 47;\\
(15,1)\text{ truncated}:\quad & I_1 = [0{:}13], 15, 18, & I_2 &= [0{:}13], 15, 16,\\
& R_\eta = [0{:}29], & C_\eta &= [0{:}13], 15, 18, [30{:}41], 45, 46.
\end{aligned}$$

The zero-coefficient case uses the following index lists:

$$\begin{aligned}
(13,1):\quad & I_1 = [0{:}7], 13, 16, & I_2 &= [0{:}7], 13, 14,\\
& R_\eta = [0{:}17], & C_\eta &= [0{:}7], 13, 16, [27{:}32], 40, 41;\\
(14,2):\quad & I_1 = [0{:}17], 28, 29, 34, 35, & I_2 &= [0{:}17], 28, 29, 30, 31,\\
& R_\eta = [0{:}39], & C_\eta &= [0{:}17], 28, 29, 34, 35, [57{:}70], [85{:}88];\\
(15,1)\text{ full}:\quad & I_1 = [0{:}7], 15, 18, & I_2 &= [0{:}7], 15, 16,\\
& R_\eta = [0{:}16], 18, & C_\eta &= [0{:}7], 15, 18, [31{:}36], 46, 47;\\
(15,1)\text{ truncated}:\quad & I_1 = [0{:}9], 15, 18, & I_2 &= [0{:}9], 15, 16,\\
& R_\eta = [0{:}21], & C_\eta &= [0{:}9], 15, 18, [30{:}37], 45, 46.
\end{aligned}$$

Evaluating the selected minors gives the following values.

Table 1: Explicit minor evaluations over $\mathbb{F}_{1009}$. Each entry is nonzero.

base point	case	(δ_1, δ_2)	(ρ_1, ρ_2)	η^R	η^L
$(13, 1)$	weighted, nonzero	$(709, 395)$	$(992, 513)$	768	477
$(13, 1)$	weighted, zero	$(709, 395)$	$(679, 388)$	296	141
$(13, 1)$	zero coefficients	$(621, 279)$	$(726, 188)$	256	396
$(14, 2)$	weighted, nonzero	$(279, 946)$	$(109, 848)$	53	716
$(14, 2)$	weighted, zero	$(279, 946)$	$(131, 721)$	623	418
$(14, 2)$	zero coefficients	$(187, 831)$	$(602, 975)$	373	296
$(15, 1)$ full	weighted, nonzero	$(991, 811)$	$(647, 232)$	833	520
$(15, 1)$ full	weighted, zero	$(991, 811)$	$(537, 429)$	236	182
$(15, 1)$ full	zero coefficients	$(541, 41)$	$(605, 663)$	834	494
$(15, 1)$ truncated	weighted, nonzero	$(159, 780)$	$(19, 231)$	860	458
$(15, 1)$ truncated	weighted, zero	$(159, 780)$	$(261, 6)$	158	717
$(15, 1)$ truncated	zero coefficients	$(999, 475)$	$(936, 775)$	749	607

For a general block width, use the full assignment in the first direct-sum copy and the truncated assignment in each remaining copy. The selected submatrices then factor as in the proof of Lemma 16.