# Polynomial-Time Cryptanalysis of the Subspace Flooding Assumption for Post-Quantum $i\mathcal{O}$

Aayush Jain * Huijia Lin † Paul Lou ‡ Amit Sahai §

**Abstract.** Indistinguishability Obfuscation ($i\mathcal{O}$) is a highly versatile primitive implying a myriad advanced cryptographic applications. Up until recently, the state of feasibility of $i\mathcal{O}$ was unclear, which changed with works (Jain-Lin-Sahai STOC 2021, Jain-Lin-Sahai Eurocrypt 2022) showing that $i\mathcal{O}$ can be finally based upon well-studied hardness assumptions. Unfortunately, one of these assumptions is broken in quantum polynomial time. Luckily, the line work of Brakerski et al. Eurocrypt 2020, Gay-Pass STOC 2021, Wichs-Wee Eurocrypt 2021, Brakerski et al. ePrint 2021, Devadas et al. TCC 2021 simultaneously created new pathways to construct $i\mathcal{O}$ with plausible post-quantum security from new assumptions, namely a new form of circular security of LWE in the presence of leakages. At the same time, effective cryptanalysis of this line of work has also begun to emerge (Hopkins et al. Crypto 2021).

It is important to identify the simplest possible conjectures that yield post-quantum $i\mathcal{O}$ and can be understood through known cryptanalytic tools. In that spirit, and in light of the cryptanalysis of Hopkins et al., recently Devadas et al. gave an elegant construction of $i\mathcal{O}$ from a fully-specified and simple-to-state assumption along with a thorough initial cryptanalysis.

Our work gives a polynomial-time distinguisher on their "final assumption" for their scheme. Our algorithm is extremely simple to describe: Solve a carefully designed linear system arising out of the assumption. The argument of correctness of our algorithm, however, is nontrivial.

We also analyze the "T-sum" version of the same assumption described by Devadas et. al. and under a reasonable conjecture rule out the assumption for any value of $T$ that implies $i\mathcal{O}$.

## 1 Introduction

Indistinguishability obfuscation ($i\mathcal{O}$) for programs computable in polynomial-time [11] makes a program as unintelligble as possible while preserving the functionality. Mathematically, $i\mathcal{O}(P)$ is indistinguishable to $i\mathcal{O}(P')$ for any functionally equivalent programs $P, P'$ of the same size. $i\mathcal{O}$'s importance is evident in its

*CMU. Email: aayushja@andrew.cmu.edu
†UW. Email: rachel@cs.washington.edu
‡UCLA. Email: pslou@cs.ucla.edu
§UCLA. Email: sahai@cs.ucla.edu

central position as a powerful and versatile primitive for building a wide variety of modern cryptographic tools (see e.g., [6,15,21,22,25,38,46,55]). Up until recently, the feasibility of $i\mathcal{O}$ from well-established assumptions was not known. In recent works, Jain, Lin, and Sahai [44,45] constructed $i\mathcal{O}$ from three well-studied assumption: Decisional Linear assumption (DLIN) over bilinear maps [8], Learning Parity with Noise over general fields [42], and Pseudorandom Generators in $\mathsf{NC}_0$ [37]. DLIN over bilinear maps, however, is an assumption broken in quantum polynomial time.

In an effort to construct $i\mathcal{O}$ from conjectured post-quantum secure assumptions, specifically lattice-based ones, an exciting line of works [18,33,56] construct $i\mathcal{O}$ based on new circular security type assumptions of LWE in the presence of structured leakages of their errors. Typically there is a lot of room in how you can instantiate leakages that imply $i\mathcal{O}$, and at the moment we do not have a stable understanding of what constitutes an acceptable leakage. In fact, very recently [40] showed that instantiations of several assumptions of Gay-Pass and Wee-Wichs can be broken in classical polynomial time.

Ideally we would like to construct post-quantum $i\mathcal{O}$ based solely on well-studied post-quantum assumptions such as LWE/LPN. Unfortunately, however, our understanding of conjectures implying post-quantum $i\mathcal{O}$ is severely limited, and our confidence in them is much lower than those in classical constructions (LPN, DLIN and PRGs). Therefore, it is important that we strive to identify assumptions that are:

- Simple-to-state, and yet imply $i\mathcal{O}$,
- Can be reasoned about with cryptanalytic study.

We believe that this symbiotic relationship between constructions and constructive cryptanalysis could further understanding of how to securely instantiate assumptions. To be clear, we do not endorse an unchecked break and repair cycle, but a cycle that identifies new conceptual pathways. In this spirit, following the cryptanalysis of [40], the work of Devadas et al. [29] recently gave an elegant construction from a *fully-specified* and simple-to-state assumption implying $i\mathcal{O}$. We emphasize that their construction has all parameters *fully-specified*. This is unlike the previous assumption of [56] which was very general, and required that for some implementation choices such as PRF scheme involved, the resulting assumption is secure. The same is true with the assumption of [33], where the circuit implementations of functions involved were not fully specified.

Moreover, Devadas et al. back their instantiation with a thorough (initial) cryptanalysis.

*Lessons from our work.* A major open area is constructing post-quantum $i\mathcal{O}$. The most promising approach currently being explored is formulating simple variations of LWE with certain leakage that are sufficient. The recent work of [40] shows the importance of fully specifying the assumption and cryptanalysis (indeed, the attack of [40] exploits freedom in specification). Incorporating these insights, the [29] assumption is fully specified, relatively simple, avoids [40] attacks, Furthermore, the authors of [29] performed cryptanalysis using existing

techniques. The purpose of our work is to identify and understand weaknesses in the approach of [29] so that these may be overcome in future work.

On a very high level, the intuition of [29] was that tensored polynomial systems derived from LWE not only bypasses the previous two attacks (as far as we know, the parameters are set so that sum-of-squares attacks of [12] do not apply, and at the same time, the specifications are set so that the attacks of [40] do not apply). Our main result shows a new way to get around the apparent difficulties introduced by tensoring. Therefore, we view our result contributing a new insight that will be useful in designing better assumptions.

A key aspect in which our attacks differs from previous attacks [12,40] on the new "LWE+Leakage" assumptions [3,43,18,33,56] is that all previous attacks apply to part of the leakage that is obtained over integer/small-valued domains such as the error or the polynomial evaluations. On the other hand, our attack applies to the leakage that is given out over the prime fields (the leakage on the secret in the LWE sample). This points to a new vulnerability in designing such assumptions towards the grand goal of achieving $i\mathcal{O}$.

*Our Technical Contribution.* In this work, we give a polynomial-time distinguisher and recovery algorithm on the "final assumption" of [29] (stated on page 7; also formulated as Conjecture 2 on page 25) with parameters as suggested (page 23, Section 4.3). Our attack is algorithmically simple to describe: solve a carefully designed linear system of equations. Our analysis, on the other hand, requires a significant amount of care. In particular, the techniques we present and introduce in our analysis are of general interest to the studying the usage of tensor products in cryptographic constructions. We contribute the following general ideas.

1. We first show that Kilian randomization on highly tensored matrices does not kill the tensor structure. Consider positive integers $m \gg w$ and consider the equation
$$\left[\mathbf{U}_1 \otimes \mathbf{I} \| \mathbf{I} \otimes \mathbf{U}_2\right] = \mathbf{Y}$$
where $\mathbf{I}$ denotes a $m \times m$ square identity matrix, the matrices $\mathbf{U}_1, \mathbf{U}_2$ are unknown and of shape $m \times w$, and $\mathbf{Y}$, of shape $m^2 \times 2mw$, is given as input to the algorithm. Suppose $\mathbf{Y} \leftarrow \left[\mathbf{A}_1 \otimes \mathbf{I} \| \mathbf{I} \otimes \mathbf{A}_2\right] \cdot \mathbf{R}$ for some tall random matrices $\mathbf{A}_1, \mathbf{A}_2 \in \mathbb{Z}_q^{m \times w}$ and some Kilian matrix $\mathbf{R} \in \mathbb{Z}_q^{2mw \times 2mw}$, all of which are unknown to the algorithm. Right-multiplication by the matrix $\mathbf{R}$ seemingly mixes up the columns of matrices $\mathbf{A}_1 \otimes \mathbf{I}$ and $\mathbf{I} \otimes \mathbf{A}_2$, preventing the recovery of $\mathbf{A}_1$ and $\mathbf{A}_2$. By considering column spans, however, we observe that Colspan($\mathbf{A}_1 \otimes \mathbf{I}$) and Colspan($\mathbf{I} \otimes \mathbf{A}_2$) have significant non-overlap (linearly independent columns) and right multiplication by an invertible matrix preserves this non-overlap. We will show that this non-overlap enables a linear independence argument, involving a small number of carefully chosen linearly independent vectors, that shows that we can recover $\mathbf{A}_1$ and $\mathbf{A}_2$ up to a unique representation. More precisely, we show how to recover a normal form of $\mathbf{A}_i$, given by $\mathbf{U}_i = \mathbf{A}_i \cdot \mathbf{A}_{i,T}^{-1}$, where $\mathbf{A}_{i,T} \in \mathbb{Z}_q^{w \times w}$ denotes the top $w \times w$ block of $\mathbf{A}_i$ for $i \in \{1, 2\}$ (these inverses exist with high probability).

2. Consider a random matrix $\mathbf{P}$ with $M$ rows and $N$ columns. We conjecture that, with overwhelming probability over the choice of a random matrix $\mathbf{P}$, for any set of vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_T\}$ of linearly independent vectors, where $T \ll M$ and $T \leq N$, the set of vectors $\{\mathbf{P} \cdot \mathbf{v}_1, \ldots, \mathbf{P} \cdot \mathbf{v}_T\}$ is linearly independent. We demonstrate how to use the conjecture to prove the uniqueness of solutions and compute the rank of relevant matrices as we shortly explain. The parameter settings relevant to the DQVWW construction consider matrices $\mathbf{P}$ that are only slightly dimension shrinking and for which the conjecture is applicable ($M$ is still sufficiently large with respect to the sets of vectors we consider). In this setting, we cannot use matrices $\mathbf{P}$ with a very small number of rows $M$ because we require certain expansion properties for $i\mathcal{O}$.
3. Using the conjecture, we can show that left-multiplication by a random matrix $\mathbf{P}$ fails to destroy the tensor structure present if it is insufficiently dimension shrinking. For example, we show that we can still recover the matrices $\mathbf{A}_1, \mathbf{A}_2$ above up to a unique representation from the equation,

$$\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I} \| \mathbf{I} \otimes \mathbf{U}_2\right] = \mathbf{Y}$$

   where $\mathbf{P} \in \mathbb{Z}_q^{m^{3/2} \times m^2}$ is a known matrix, and where the matrix $\mathbf{Y}$ is generated as $\mathbf{Y} \leftarrow \mathbf{P} \cdot \left[\mathbf{A}_1 \otimes \mathbf{I} \| \mathbf{I} \otimes \mathbf{A}_2\right] \cdot \mathbf{R}$, differing from the above generation process only by the left-multiplication by $\mathbf{P}$. Our main observation here is that the linear independence of the same small set of linearly independent vectors identified above will be preserved by $\mathbf{P}$, enabling the same argument to show the recovery of a unique representation for $\mathbf{A}_1$ and $\mathbf{A}_2$.
   While many previous linear-algebraic cryptanalytic works present attacks from a matrix point of view, we show that considering column spans instead allows us to better analyze the tensor structure especially in the presence of the structure destroying matrix $\mathbf{P}$ and the randomizing matrix $\mathbf{R}$.
4. Finally, we give a technique for proving the uniqueness of solutions to $\mathbf{X}$ (when such uniqueness exists) in the equation

$$\mathbf{AX} + \mathbf{BY} = \mathbf{C}$$

   where $\mathbf{A}, \mathbf{B}, \mathbf{C}$ are known coefficient matrices such that the column span of $\mathbf{A}$ has a sufficient amount of non-overlap with the column span of $\mathbf{B}$, and $\mathbf{X}$ and $\mathbf{Y}$ are unknown matrices. By considering the homogeneous version of the above equation, in which $\mathbf{C} = \mathbf{0}$ and which corresponds to taking the difference of two solutions for the inhomogeneous version, and by identifying how many columns in $\mathbf{A}$ do not overlap with Colspan($\mathbf{B}$), we can isolate an equation of the form $\mathbf{A}'\mathbf{X} = \mathbf{0}$ for some matrix $\mathbf{A}'$. This allows us to use standard rank arguments that depend on the shape of $\mathbf{A}'$ to show that the only solution to $\mathbf{X}$ in the homogeneous equation is $\mathbf{0}$, which implies that there is a unique solution to $\mathbf{X}$ in the inhomogeneous equation. Here, the conjecture above also extends our technique to the setting of proving the uniqueness of solutions to $\mathbf{X}$ (when such uniqueness exists) in equations of

the form

$$\mathbf{PAX} + \mathbf{PBY} = \mathbf{C}.$$

In particular, if we can compute the size of the overlap of Colspan($\mathbf{A}$) and Colspan($\mathbf{B}$), then the conjecture allows us to compute the size of the overlap of Colspan($\mathbf{PA}$) and Colspan($\mathbf{PB}$).

*Related Works.* There is a huge body of other works [1,2,5,7,10,13,19,20,23,24,28,27,26,30,32,35,39,41,47,48,50,53,43] that construct $i\mathcal{O}$ candidates from plausible post-quantum assumptions (some of which are subject to prior cryptanalysis). This list includes constructions based on candidate multi-linear maps [31,32,34], from noisy linear functional encryption [1,2] and affine determinant programs [13]. Similarly, cryptanalysis was performed to better understand these assumptions [9,12,17,19,23,24,26,39,40,41,51,53,54]. Our work does not consider these lines of constructions.

*Organization of the Paper* The technical overview is nearly complete in of itself. Due to space constraints we place the proof of uniqueness for recovering $\mathbf{V}_1$ in the Supplementary Materials in Section 4.1. We also place the extension to the $T$-sum case in the Supplementary Materials in Section 4.2. Basic linear algebraic facts and proofs about the tensor structure are found in the Supplementary Materials in Section 4.4 and Section 4.5 (resp.). A full version can be found as a separate supplementary file.

## 2 Technical Overview

We start by reviewing the construction idea of [29]. The work is built upon [56], which was a follow up of [18]. The works [56,29] construct $i\mathcal{O}$ by constructing a non-trivial obfuscation $xi\mathcal{O}$. The works of [4,16,14,49] showed that, under a subexponential security loss, an $xi\mathcal{O}$ scheme can be generically lifted to a construction of an indistinguishability obfuscation scheme further assuming LWE. Recall that in an $xi\mathcal{O}$ scheme, the goal is to obfuscate circuits $C : \{0,1\}^n \to \{0,1\}^m$, where the size of the obfuscation must be marginally better than the size of the truth-table for $C$ i.e. bounded by $2^{\epsilon \cdot n}\,\mathsf{poly}(\lambda, |C|)$ for some constant $\epsilon < 1$, whereas the running time could be as large as $2^n\,\mathsf{poly}(\lambda, |C|)$.

*The Overall Approach of [56,29]* The main starting observation of the works [56,29] is the following. Consider a function $f : \{0,1\}^\ell \to \{0,1\}^{M \times K}$ where $M \cdot K = 2^n \cdot m$ (the size of the truth table for $C$). We intend the function $f$ to take as input the bit description of a circuit $C$, and output its truth table. Now consider ciphertexts encrypting bits of the circuit $C$, encrypted using the dual GSW variant of homomorphic encryption scheme [36] $\{\mathsf{CT}_i = \mathbf{AS}_i + \mathbf{E}_i + C_i\mathbf{G}\}_{i \in [\ell]}$ where $\mathbf{A} \in \mathbb{Z}_q^{M \times w}$ and $\mathbf{S}_i \in \mathbb{Z}_q^{w \times M \log q}$ and $\mathbf{G}$ is the gadget matrix defined by [52] and $w \ll M, K$. Then the idea is that, one can homomorphically evaluate on these ciphertexts to compute an encoding:

$$\mathsf{CT}_f = \mathbf{AS}_f + \mathbf{E}_f + \mathbf{M}_f \left\lceil \frac{q}{2} \right\rfloor$$

where $\mathbf{S}_f \in \mathbb{Z}_q^{w \times K}$ and $\mathbf{M}_f$ is a matrix of dimension $M \times K$, that arranges outputs of $f(C)$ in a matrix form, and $\mathbf{E}_f$ is a matrix with $\ell_2$ norm much smaller than $q$. This is a ciphertext that has an opening that is much shorter in size than $M \cdot K$. The opening is simply $\mathbf{S}_f$ which is of the size $w \cdot K \log q \ll M \cdot K$.

Thus, a first candidate could be one in which the obfuscator gives out $\{\mathsf{CT}_i\}_{i \in [\ell]}$ along with $\mathbf{S}_f$. Unfortunately, this is easily attackable, because this let's one learn $\mathbf{E}_f$, which lies in a linear subspace which is some function of the circuit $C$. Thus given $\mathbf{E}_f$ one can test if the ciphertexts encrypt $C_0$ or $C_1$.

*Relying on fresh LWE samples with large error.* To address this issue, [18,56] observed that access to fresh LWE samples $\mathbf{D} = \mathbf{AR} + \mathbf{F}$ where $\mathbf{R} \in \mathbb{Z}_q^{w \times K}$ and $\mathbf{F} \in \chi_{\mathsf{flood}}^{M \times K}$ from some distribution $\chi_{\mathsf{flood}}$ can drown out $\mathbf{E}_f$. Then, one can give out $\mathbf{S}_f + \mathbf{R}$ (in addition to $\mathbf{D}, \{\mathsf{CT}_i\}$) which lets one learn $\mathbf{E}_f + \mathbf{F} + \mathbf{M}_f \lceil \frac{q}{2} \rceil$. In fact, this system can be proven secure under LWE. Unfortunately, now the problem is that $\mathbf{D}$ is too big! We don't obtain any compression if we give such a matrix out. To address this issue, [56] suggested pseudorandomly generating LWE samples, motivating a source of new hardness assumptions in [56] as well as the paper under consideration in our work [29].

*Pseudorandomly sampling LWE* To obtain compression, [56] suggested that we come up with a way where one uses a small set of encryptions (encrypting say a PRF key) $\{\mathsf{CT}'_i = \mathbf{AS}'_i + \mathbf{E}'_i + k_i \mathbf{G}\}_{i \in [\ell']}$ and then using this compute a larger number of LWE samples of the same kind as $\mathbf{D}$. The work showed that by homomorphically evaluating PRF and relying on packing techniques, one could generate a larger sample of the required form $\mathbf{D} = \mathbf{AR}' + \mathbf{F}'$. Now one could give out $\mathbf{S}_f + \mathbf{R}'$ and this could effectively replace the role of a fresh LWE sample $\mathbf{D}$. Unfortunately, this assumption is heuristic in nature, and is contingent on the exact specification of the circuit implementation of the PRF used. The work of [40] pointed out that for every PRF, if the circuit implementation is not chosen carefully, the assumption could be attacked.

*Simplifying Assumption.* The main contribution of [29] is a significantly simpler scheme that involves computation of a fully specified structured constant-degree polynomials rather than a PRF. The purpose is to identify the simplest possible assumption that suffices to build $i\mathcal{O}$, and can be reasoned with respect to broad classes of cryptanalysis algorithms. In order to generate "LWE" type samples, the work of [29] gives out $d$ LWE matrices for some constant $d \in \mathbb{N}$:

$$\mathbf{B}_i = \mathbf{A}_i \mathbf{S}_i + \mathbf{E}_i \mod q,$$

for $i \in [d]$ where $\mathbf{A}_i \leftarrow \mathbb{Z}_q^{m \times w}$ and $\mathbf{S}_i \leftarrow \mathbb{Z}_q^{w \times k}$ and $\mathbf{E}_i \leftarrow \chi^{m \times k}$. Here $w \ll m \ll k$

The point of this is that now one can compute $\mathbf{B}' = \mathbf{B}_1 \otimes \ldots \otimes \mathbf{B}_d$ given these matrices resulting in a matrix of much larger dimension. This matrix can be expressed as:

$$\mathbf{B}_1 \otimes \ldots \otimes \mathbf{B}_d = \mathbf{A}' \cdot \mathbf{S}' + \mathbf{E}',$$

where,

$$\mathbf{A}' = (\mathbf{A}_1 \otimes \mathbf{I}_m \otimes \ldots \mathbf{I}_m \| \mathbf{I}_m \otimes \mathbf{A}_2 \otimes \ldots \mathbf{I}_m \| \ldots \| \mathbf{I}_m \otimes \mathbf{I}_m \otimes \ldots \mathbf{A}_d),$$

$$\mathbf{S}' = \begin{pmatrix} \mathbf{S}_1 \otimes \mathbf{B}_2 \otimes \mathbf{B}_3 \otimes \ldots \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \mathbf{E}_1 \otimes \mathbf{S}_2 \otimes \mathbf{B}_3 \otimes \ldots \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \vdots \\ \mathbf{E}_1 \otimes \mathbf{E}_2 \otimes \mathbf{E}_3 \otimes \ldots \mathbf{E}_{d-1} \otimes \mathbf{S}_d \end{pmatrix},$$

$$\mathbf{E}' = \mathbf{E}_1 \otimes \ldots \otimes \mathbf{E}_d.$$

At this point it is tempting to use $\mathbf{B}'$ to instantiate the template above. Indeed the dimension of $\mathbf{S}'$ is much smaller than the dimension of $\mathbf{B}'$. Unfortunately, this can be attacked using the sum-of-squares algorithm. The sample $\mathbf{E}' + \mathbf{M}_f \lceil \frac{q}{2} \rceil + \mathbf{E}_f$ does not hide $\mathbf{E}_f$. $\mathbf{E}'$ consists of all degree $d$ monomials of $\mathbf{E}_1, \ldots, \mathbf{E}_d$, and if $\|\mathbf{E}_f\|_2 \ll \|\mathbf{E}'\|_2$, using ideas similar to [12] we can recover $\{\mathbf{E}_i\}$ uniquely with high probability in polynomial time. For ruling out such attacks, we require that for any system of polynomials of degree $d$ over $n$ variables, the number of equations be less than $n^{d/2}$, whereas in this case we are giving out $n^d$ equations.

Thus, [29] suggested multiplying $\mathbf{B}'$ by matrices $\mathbf{P}$ and $\mathbf{P}'$ (which are both a part of some $\mathsf{crs}$) with integer Gaussian entries to compute $\mathbf{B}^* = \mathbf{P}\mathbf{B}'\mathbf{P}'$ where $\mathbf{P} \in \mathbb{Z}^{M \times m^d}$ and $\mathbf{P}' \in \mathbb{Z}^{k^d \times K}$. This yields $\mathbf{B}^* = \mathbf{A}^* \cdot \mathbf{S}^* + \mathbf{E}^*$ where $\mathbf{S}^* = \mathbf{S}' \cdot \mathbf{P}'$ and $\mathbf{E}^* = \mathbf{P}(\mathbf{E}_1 \otimes \ldots \otimes \mathbf{E}_d)\mathbf{P}'$. We can now use $\mathbf{E}^*$ as the smudging polynomial. The dimension $M$ and $K$ are set so that $M \cdot K \ll (m \cdot k)^{d/2}$ to resist sum-of-squares attacks and at the same time also give the compression needed to give rise to $i\mathcal{O}$.

While this is the main idea, there are several additional ideas that are needed to turn the intuition above into a scheme. Observe that in $\mathbf{B}^* = \mathbf{P}\mathbf{A}'\mathbf{S}'\mathbf{P}' + \mathbf{E}^*$, $\mathbf{A}'$ and $\mathbf{S}'$ are highly structured. Instead of releasing matrices $\overline{\mathbf{A}}^* = \mathbf{P}\mathbf{A}'$ in the clear, one gives out Kilian randomized version of $\overline{\mathbf{A}}^*$, which we denote by $\mathbf{A}^*$ with the same column span as that of $\mathbf{P}\mathbf{A}'$. Still, several issues remain: For example, the construction is in the CRS model, and the assumption is associated with a CRS. We now describe the assumption below and then give a sketch of our attack.

*Succinct LWE Sampling Assumption.* The assumption on a broad level roughly says that for some constant $d \in \mathbb{N}$:

$$(\{\mathbf{A}_i\mathbf{S}_i + \mathbf{E}_i\}_{i\in[d]}, \mathbf{A}^*, \bar{Q}, \bar{Q}(\mathbf{E}_1, \ldots, \mathbf{E}_d) + \mathsf{Z}_0, \mathsf{aux}_0) \approx_c$$
$$(\{\mathbf{A}_i\mathbf{S}_i + \mathbf{E}_i\}_{i\in[d]}, \mathbf{A}^*, \bar{Q}, \bar{Q}(\mathbf{E}_1, \ldots, \mathbf{E}_d) + \mathsf{Z}_1, \mathsf{aux}_1)$$

where $\bar{Q}$ is a fully specified degree-$d$ polynomial map over the integers chosen at random from some distribution which we will specify below. For $b \in \{0, 1\}$, $\mathsf{Z}_b$ is a distribution that needs to be smudged and $\mathsf{aux}_b$ is auxiliary information about the distribution. On a very high level, the assumption has a structure that is reminiscent of the assumptions made by [3,43]. However, there are differences in what set of polynomials that $\bar{Q}$ can be supported and the auxiliary

information. As described above, the polynomial map that [29] considers is of the form: $\bar{Q}(\mathbf{E}_1, \ldots, \mathbf{E}_d) = \mathbf{P}(\mathbf{E}_1 \otimes \ldots \mathbf{E}_d)\mathbf{P}'$ where the polynomial first computes multilinear degree $d$ monomials by computing $\mathbf{E}_1 \otimes \ldots \otimes \mathbf{E}_d$ and then multiplies it on both sides by matrices $\mathbf{P}, \mathbf{P}'$ of appropriately chosen dimensions where the entries are chosen from a discrete Gaussian distribution. Our attacks do not apply to the assumptions made in [3,43], which are structurally similar on a very high level. The reason for this is that our attack uses the structure of the polynomial $\bar{Q}$ in a crucial way. Our results, in fact, suggest that there are distributions of polynomials $\bar{Q}$, such that $\bar{Q}(\mathbf{E}_1, \ldots, \mathbf{E}_d)$ may be secure to release (from the point of view of $\mathsf{SoS}$, linearizations and other attacks) but together with the LWE samples, might end up being invertible. This conclusion suggests that these types of assumptions of LWE sampling with polynomial leakage on the errors need to be thoroughly investigated.

We now describe the assumption in full specification below.

### 2.1 The DQVWW Assumption implying $i\mathcal{O}$

We now describe the assumption of [29] implying $i\mathcal{O}$. The assumption appears as the "final assumption" on page 7 as well as Conjecture 2 in [29]. We emphasize unlike previous works in this line, the assumption of [29] is *fully-specified*, meaning all parameters/implementations are fully specified.

We first set some parameters that will be used to define the conjecture.

- $d \geq 3$ is a constant integer.
- $w$ is a security/dimension parameter,
- $m, n, k, M, N, W$ are other dimension parameters which are polynomials in $w$.
- In their candidate, $M = m^{d-1/2}$ and $K = m^{d+1/2}$, $m \geq w^3$ and $m^3 \leq k \leq m^{2d-7/6}$ and $W = O(dwm^{d-1})$.
- $q$ is a prime, $\chi, \bar{\chi}, \chi_{\mathsf{flood}}$ are LWE error distributions with different parameters. We note that there is a bound of $q \leq 2^{O(m)}$ for LWE security to hold, a point which we expound on in Remark 1.

The assumption is regarding indistinguishability of two distributions $\mathcal{D}_b$ for $b \in \{0, 1\}$. We describe both the distributions below.

*Distribution $\mathcal{D}_b$.*

- For $i \in [d]$, sample $\mathbf{A}_i \leftarrow \mathbb{Z}_q^{m \times w}$, $\mathbf{S}_i \leftarrow \mathbb{Z}_q^{w \times k}$, $\mathbf{E}_i \leftarrow \chi^{m \times k}$. Set $\mathbf{B}_i = \mathbf{A}_i \cdot \mathbf{S}_i + \mathbf{E}_i$. Visually, the $\mathbf{A}_i$'s are tall, the $\mathbf{S}_i$'s are wide, and the $\mathbf{B}_i$'s and the $\mathbf{E}_i$'s are wide.
- Sample $\mathbf{P} \leftarrow \chi^{M \times m^d}$ and $\mathbf{P}' \leftarrow \chi^{k^d \times K}$. Visually, $\mathbf{P}$ is a wide matrix and $\mathbf{P}'$ is a tall matrix.
- Set $\bar{\mathbf{A}}^* = \mathbf{P} \cdot \Big( \mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \mathbf{A}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \ldots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d \Big) \in Z_q^{M \times dwm^{d-1}}$. Visually, $\bar{\mathbf{A}}^*$ is a tall matrix.

– Set $\bar{\mathbf{S}}^* = \begin{pmatrix} \mathbf{S}_1 \otimes \mathbf{B}_2 \otimes \mathbf{B}_3 \otimes \ldots \otimes \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \mathbf{E}_1 \otimes \mathbf{S}_2 \otimes \mathbf{B}_3 \otimes \ldots \otimes \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \vdots \\ \mathbf{E}_1 \otimes \mathbf{E}_2 \otimes \mathbf{E}_3 \otimes \ldots \otimes \mathbf{E}_{d-1} \otimes \mathbf{S}_d \end{pmatrix} \cdot \mathbf{P}' \in \mathbb{Z}_q^{dwm^{d-1} \times K}$ Visually, $\bar{\mathbf{S}}^*$ is a wide matrix.
– (Killian Randomization) Find random full rank matrices $\mathbf{A}^* \in \mathbb{Z}_q^{M \times W}, \mathbf{S}^* \in \mathbb{Z}_q^{W \times K}$ such that $\mathbf{A}^* \cdot \mathbf{S}^* = \bar{\mathbf{A}}^* \cdot \bar{\mathbf{S}}^*$. Visually, $\mathbf{A}^*$ is a tall matrix and $\mathbf{S}^*$ is a wide matrix.
– Observe that if one sets $\mathbf{B}^* = \mathbf{P} \cdot (\mathbf{B}_1 \otimes \ldots \otimes \mathbf{B}_d) \cdot \mathbf{P}'$ and $\mathbf{E}^* = \mathbf{P} \cdot (\mathbf{E}_1 \otimes \ldots \otimes \mathbf{E}_d) \cdot \mathbf{P}'$, then it holds that $\mathbf{B}^* - \mathbf{A}^*\mathbf{S}^* = \mathbf{E}^*$. Set $\mathsf{seed} = \{\mathbf{B}_i\}_{i \in [d]}, \mathbf{A}^*, \mathbf{S}^*$.
– Set $\hat{\mathbf{B}} = \mathbf{A}^*\mathbf{S}_0 + \mathbf{F}$, where $\mathbf{S}_0 \leftarrow \mathbb{Z}_q^{W \times K}$ and $\mathbf{F} \leftarrow \chi_{\mathsf{flood}}^{M \times K}$.
– Set $\mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - b\mathbf{G}$, where $\mathbf{R} \leftarrow \mathbb{Z}_q^{W \times M \log q}$ and $\mathbf{E} \leftarrow \bar{\chi}^{M \times M \log q}$.

Output of $\mathcal{D}_b$ consists of the following tuple:

$$\Delta_b = (\mathbf{P}, \mathbf{P}', \mathbf{A}^*, \{\mathbf{B}_i\}_{i \in [d]}, \hat{\mathbf{B}}, \mathbf{C}, \mathbf{E}^* + \mathbf{E}\mathbf{G}^{-1}(\hat{\mathbf{B}}) - b\mathbf{F})$$

We note that $\mathbf{E}^* + \mathbf{E}\mathbf{G}^{-1}(\hat{\mathbf{B}}) - b\mathbf{F}$ let's one derive $\mathbf{A}^* \cdot (\mathbf{S}^* + \mathbf{R}\mathbf{G}^{-1}(\hat{\mathbf{B}}) - b\mathbf{S}_0)$. This is because $\mathbf{B}^* + \mathbf{C}\mathbf{G}^{-1}(\hat{\mathbf{B}}) = \mathbf{A}^*(\mathbf{S}^* + \mathbf{R}\mathbf{G}^{-1}(\hat{\mathbf{B}}) - b\mathbf{S}_0) + \mathbf{E}^* + \mathbf{E}\mathbf{G}^{-1}(\hat{\mathbf{B}}) - b\mathbf{F}$.

**The Assumption of [29].** For the distribution $\mathcal{D}_0, \mathcal{D}_1$ defined above, $\mathcal{D}_0$ is computationally indistinguishable to $\mathcal{D}_1$.

*Remark 1.* For simplicity, consider the LWE error distribution $\chi$ to be uniform over $[0, B-1]$. In general, the security of LWE itself requires that $B/q \geq 2^{-w}$ where $w$ is the security parameter (It's also the length of the secret, observe that each matrix $\mathbf{S}_i$ is of dimension $w \times k$ and every column, say $\mathbf{s}_{i,j} \in \mathbb{Z}_q^w$ of $\mathbf{S}_i$ defines a fresh LWE sample given by $\mathbf{A}_i\mathbf{s}_{i,j} + \mathbf{e}_{i,j}$, where $\mathbf{e}_{i,j} \in \mathbb{Z}_q^k$ is the $j$th column of $\mathbf{E}_i$). Moreover, we know that the total entropy in a LWE matrix is upper bounded by $wk \log q + mk \log B$ and this total entropy must be upper bounded by the entropy in a truly random matrix of dimension $m \times k$, so we have $mk \log q \geq wk \log q + mk \log B$. Substituting the constraint on the noise-to-modulus ratio into the entropy bound gives us that $m \geq \log q$, so $q \leq 2^{O(m)}$ so that LWE security holds. An analogous constraint holds on Gaussian distributions with respect to the width.

### 2.2 Overview of the Attack

We begin by describing a recovery algorithm for the error term $\mathbf{E}_1$ in the case that $b = 0$. To break the assumption, the algorithm is given a tuple

$$(\mathbf{P}, \mathbf{P}', \mathbf{A}^*, \{\mathbf{B}_i\}_{i \in [d]}, \hat{\mathbf{B}}, \mathbf{C}, \mathbf{E}^* + \mathbf{E}\mathbf{G}^{-1}(\hat{\mathbf{B}}) - b\mathbf{F})$$

for some $b \in \{0, 1\}$, and the algorithm needs to identify the value of $b \in \{0, 1\}$. We show that in the case of $b = 0$, we can construct an algorithm $\mathcal{A}$ that recovers the matrices $\mathbf{A}_1, \ldots, \mathbf{A}_d$ up to a unique representation, and then recovers the

secret $\mathbf{S}_1$ up to a unique representation. If we recover $\mathbf{A}_1$ and $\mathbf{S}_1$ up to a unique representation, then we can recover $\mathbf{E}_1$ from $\mathbf{B}_1$. The same attack can then iteratively recover $\mathbf{E}_i$ for all $i \in [d]$. This recovery algorithm for the case that $b = 0$ heuristically gives rise to a distinguisher which we explain in Section 3.1.

*A unique representation* Observe that if one was to naively solve for $\mathbf{A}_i, \mathbf{S}_i$, there could be many solutions simultaneously satisfying all the constraints. In particular, there are many possible values of $\mathbf{U}_i, \mathbf{V}_i$ that satisfy $\mathbf{B}_i = \mathbf{U}_i \cdot \mathbf{V}_i + \mathbf{E}_i$ where $\mathbf{U}_i \in \mathbb{Z}_q^{m \times w}$, $\mathbf{V}_i \in \mathbb{Z}_q^{w \times k}$ and $\mathbf{A}^* = \mathbf{P} \left[ \mathbf{U_1} \otimes \mathbf{I}^{\otimes(d-1)} \| \cdots \| \mathbf{I}^{\otimes(d-1)} \otimes \mathbf{U}_d \right] \mathbf{T}$ for a matrix $\mathbf{T} \in \mathbb{Z}_q^{dwm^{d-1} \times W}$. This large solution space, for example, contains all solutions of the form $\mathbf{U}_i = \mathbf{A}_i \mathbf{R}$ and $\mathbf{V}_i = \mathbf{R}^{-1} \mathbf{S}_i$ for any invertible matrix $\mathbf{R} \in \mathbb{Z}_q^{w \times w}$. Any such choice of $\mathbf{U}_i$ and $\mathbf{V}_i$ also gives rise to a solution of $\mathbf{A}^* \mathbf{S}^* = \bar{\mathbf{U}}^* \bar{\mathbf{V}}^*$ where

$$\bar{\mathbf{U}}^* = \mathbf{P} \left[ \mathbf{U_1} \otimes \mathbf{I}^{\otimes(d-1)} \| \cdots \| \mathbf{I}^{\otimes(d-1)} \otimes \mathbf{U}_d \right]$$

$$\bar{\mathbf{V}}^* = \begin{bmatrix} \mathbf{V}_1 \otimes \mathbf{B}_2 \otimes \mathbf{B}_3 \otimes \ldots \otimes \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \mathbf{E}_1 \otimes \mathbf{V}_2 \otimes \mathbf{B}_3 \otimes \ldots \otimes \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \vdots \\ \mathbf{E}_1 \otimes \mathbf{E}_2 \otimes \mathbf{E}_3 \otimes \ldots \otimes \mathbf{E}_{d-1} \otimes \mathbf{V}_d \end{bmatrix} \cdot \mathbf{P}'.$$

In order to make a *unique* search possible, we observe that for any LWE sample,

$$\mathbf{B}_i = \mathbf{A}_i \cdot \mathbf{S}_i + \mathbf{E}_i$$

for a planted $\mathbf{A}_i \in \mathbb{Z}_q^{m \times w}$, $\mathbf{S}_i \in \mathbb{Z}_q^{w \times k}$ and $\mathbf{E}_i \leftarrow \chi^{m \times k}$, with high probability, can be uniquely written as:

$$\mathbf{B}_i = \mathbf{U}_i \cdot \mathbf{V}_i + \mathbf{E}_i$$

where we insist that $\mathbf{U}_i$ is uniquely structured, namely in its Hermite normal form (reduced echelon form). That is, we set $\mathbf{U}_i = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_i \end{bmatrix}$, by setting the top $w \times w$ submatrix of $\mathbf{U}_i$ to be identity. The purported solution value of $\mathbf{U}_i$ is supposed to be $\mathbf{A}_i \cdot \mathbf{A}_{i,T}^{-1}$ where $\mathbf{A}_{i,T}^{-1}$ is the top $w \times w$ submatrix of $\mathbf{A}_i$. Similarly, the intended solution for $\mathbf{V}_i$ is supposed to be $\mathbf{A}_{i,T} \cdot \mathbf{S}_i$. Note that if this happens, then we still have the desired relation:

$$\mathbf{A}_i \cdot \mathbf{S}_i = \mathbf{U}_i \cdot \mathbf{V}_i$$

*Our algorithm* We now state our recovery algorithm that recovers $\mathbf{E}_1$ in two simple steps:

**Main Recovery Algorithm $\mathcal{A}$**

Input: $(\mathbf{P}, \mathbf{P}', \mathbf{A}^*, \{\mathbf{B}_i\}_{i \in [d]}, \hat{\mathbf{B}}, \mathbf{C}, \mathbf{E}^* + \mathbf{E}\mathbf{G}^{-1}(\hat{\mathbf{B}})$.
Output: $\mathbf{V}_1, \mathbf{E}_1$.

1. **Recover** $\mathbf{U}_1, \ldots, \mathbf{U}_d$: Solve the affine system of equations defined by

$$\mathbf{P} \cdot \left[ \mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d \right] = \mathbf{A}^* \cdot \mathbf{M} \tag{1}$$

   where $\mathbf{U}_i = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_i \end{bmatrix}$, for $i \in [d]$, and the variables are given by the entries of $\tilde{\mathbf{A}}_1, \ldots, \tilde{\mathbf{A}}_d \in \mathbb{Z}_q^{(m-w)\times w}$ and the entries of $\mathbf{M} \in \mathbb{Z}_q^{W \times dwm^{d-1}}$. Even more precisely, every entry of the matrix

$$\mathbf{P} \cdot \left[ \mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d \right] - \mathbf{A}^* \cdot \mathbf{M}$$

   defines an equation in the above described variables, where the coefficients are given by the entries of $\mathbf{A}^*$ and $\mathbf{P}$. We will show there is a unique solution for $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$, namely the fact that there is only one possible solution for all the entries of $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$ regardless of the solution found for the entries of $\mathbf{M}$.
2. **Recover** $\mathbf{V}_1$: Having recovered the unique matrices $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$, our algorithm now aims to recover $\mathbf{V}_1$ such that $\mathbf{U}_1 \cdot \mathbf{V}_1 = \mathbf{A}_1 \cdot \mathbf{S}_1$. To do this, our algorithm computes

$$\mathbf{Y} = \mathbf{A}^* \cdot (\mathbf{S}^* + \mathbf{R} \cdot \mathbf{G}^{-1}(\hat{\mathbf{B}}))$$

   by subtracting off the error $\mathbf{E}^* + \mathbf{E} \cdot \mathbf{G}^{-1}(\hat{\mathbf{B}})$ from $\mathbf{B}^* + \mathbf{C} \cdot \mathbf{G}^{-1}(\mathbf{B})$. Then it computes, via standard linear algebra, a full rank annihilator matrix $\mathbf{Q} \in \mathbb{Z}_q^{K \times (K - M \log q)}$ such that $\mathbf{G}^{-1}(\hat{\mathbf{B}}) \cdot \mathbf{Q} = \mathbf{0}$, obtaining the equation,

$$\mathbf{A}^* \cdot \mathbf{S}^* \cdot \mathbf{Q} = \mathbf{Y} \cdot \mathbf{Q}.$$

   Finally, it solves the linear system of equations defined by

$$\mathbf{P} \left[ \mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d \right] \begin{bmatrix} \mathbf{V}_1 \otimes \mathbf{B}_2' \\ \mathbf{Z} \end{bmatrix} \mathbf{P}' \cdot \mathbf{Q} = \mathbf{Y} \cdot \mathbf{Q} \tag{2}$$

   where $\mathbf{B}_2' = \mathbf{B}_2 \otimes \ldots \otimes \mathbf{B}_d$ and where the variables are the entries of $\mathbf{V}_1$ and $\mathbf{Z}$ and the coefficients are given by the entries of $\mathbf{P}$, $\mathbf{P}'$, $\mathbf{Q}$, $\mathbf{Y}$, $\mathbf{U}_i$, for $i \in [d]$, and $\mathbf{B}_2'$. We will show that $\mathbf{V}_1$ has a unique solution, namely the fact that there is only one possible solution for the entries of $\mathbf{V}_1$ regardless of the solution found for the entries of $\mathbf{Z}$. Finally, $\mathbf{E}_1$ is now recovered by computing $\mathbf{B}_1 - \mathbf{U}_1 \cdot \mathbf{V}_1$.

Observe that in each of the two steps above, our algorithm sets up a simple, explicit affine (linear in Step 2) system of equations. Correctness of the algorithm is entirely determined by showing, for Step 1, the uniqueness of the solution to $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$, and showing, for Step 2, the uniqueness of the solution to $\mathbf{V}_1$. This

analysis is intricate and benefits from being viewed in a specific lens as we shortly explain.

*Remark 2.* We will place basic linear algebra facts and linear algebraic statements about the tensor structure used in the DQVWW construction in a shaded box. This is done to minimize the number of distractions the reader encounters. A reference to the corresponding statement in the Appendix will be included. A compendium of these facts and their proofs is found in Appendix 4.4 and Appendix 4.5.

### 2.3 The Importance of Column Spans

To show uniqueness in Step 1, we will analyze column spans instead of analyzing matrix equations. There are two reasons for analyzing the column spans: First, reasoning about column spans allows us to disregard the matrix $\mathbf{M}$ in Equation 1 by taking advantage of the fact that the column span of $\mathbf{A}^* \cdot \mathbf{M}$ is contained in the column span of $\mathbf{A}^*$, a fact which we will recall shortly.

Our second, and principal, reason for analyzing column spans is that it allows us to continue to see the tensor structure even after left-multiplication by the matrix $\mathbf{P}$. If $\mathbf{P}$ were not present, then we observe that a straightforward linear independence argument, which uses the tensor structure of the matrix in the LHS of the below equation, shows that there is a unique choice of $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$ that satisfies the equation

$$\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right] = \mathbf{A}^* \cdot \mathbf{M}.$$

We will explicitly analyze this case without $\mathbf{P}$ later in this overview as a simple example to build intuition. Under a reasonable conjecture about random matrices being injective on subspaces of small dimension, we can directly extend this linear independence argument for the simple example to the general case when we have left-multiplication by $\mathbf{P}$. This extension reveals that left-multiplication by $\mathbf{P}$ does not sufficiently destroy, nor scramble, the tensor structure of the LHS above. Yet, this observation is completely hidden from view when considering the matrix view

$$\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]$$

Since $\mathbf{P}$, in general, is not decomposable into a tensor product, directly analyzing the matrix product makes the tensor structure appear to be completely lost!

From a column span view, however, this tensor structure is still very much accessible. Extending the above mentioned linear independence argument to the general case, in which $\mathbf{P}$ is present, turns out to exactly require analyzing the column span $\text{Colspan}\left(\mathbf{P}\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)$. A more detailed overview is given below.

**Framework for Column Spans** To analyze the column span of the following matrix

$$\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right].$$

where the matrices $\mathbf{U}_i \in \mathbb{Z}_q^{m \times w}$ are of the stipulated form (with a top $w \times w$ identity block, so of full column rank $w$), it is useful to make the following extension of each $\mathbf{U}_i$ to a full basis for $\mathbb{Z}_q^m$. The column span of this matrix is some subspace of the vector space over $\underbrace{\mathbb{Z}_q^m \otimes \cdots \otimes \mathbb{Z}_q^m}_{d \text{ times}}$. Considering $\mathbb{Z}_q^m$ as a vector space, we consider the following bases for $\mathbb{Z}_q^m$. For $i \in [d]$, let $\mathcal{B}_i$ be a basis for $\mathbb{Z}_q^m$ obtained by extending the set of column vectors in $\mathbf{U}_i = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_i \end{bmatrix}$ to the following full rank, lower-triangular matrix

$$\mathcal{B}_i \triangleq \begin{bmatrix} \mathbf{I}_w & \mathbf{0}_{w \times (m-w)} \\ \tilde{\mathbf{A}}_i & \mathbf{I}_{m-w} \end{bmatrix} \in \mathbb{Z}_q^{m \times m},$$

and let $(\mathbf{e}_1^{(i)}, \ldots, \mathbf{e}_m^{(i)})$ denote the columns of $\mathcal{B}_i$ (the basis vectors).

### 2.4 Correctness of Step 1

We aim to build simple intuition about the correctness of our algorithm in this overview and leave the full details to the main technical content. Our overview first shows the existence of one solution to $\{\mathbf{U}_i\}_{i \in [d]}$ in Equation 1, namely a solution to $\mathbf{U}_i$ is the Hermite normal form of $\mathbf{A}_i \in \mathbb{Z}_q^{m \times w}$, which has full column rank with overwhelming probability by property of random matrices. Then we explain why this is the only solution with overwhelming probability.

**(Step 1) Existence of a structured solution**: First, there exists at least one solution to $\{\mathbf{U}_i\}_{i \in [d]}$ and $\mathbf{M}$ in Equation 1 in which for all $i \in [d]$, we have $\mathbf{U}_i \leftarrow \mathbf{A}_i \cdot \mathbf{A}_{i,T}^{-1}$, where we recall that $\mathbf{A}_{i,T} \in \mathbb{Z}_q^{w \times w}$ is defined to be the top $w \times w$ block of $\mathbf{A}_i$. Put equivalently, a solution to $\mathbf{U}_i$ is the Hermite normal form of $\mathbf{A}_i$. To see why, for $i \in [d]$, define the invertible matrix $\mathbf{N}_i = \mathbf{I}_m^{\otimes(i-1)} \otimes \mathbf{A}_{i,T}^{-1} \otimes \mathbf{I}_m^{\otimes(d-i)}$ and use the following two linear algebraic facts.

**Lemma 1.** *For any matrices $\mathbf{M}_1, \mathbf{M}_2$, there exists a matrix $\mathbf{N}$ such that $\mathbf{M}_1 \cdot \mathbf{N} = \mathbf{M_2}$ if and only if* $\mathrm{Colspan}(\mathbf{M_2}) \subseteq \mathrm{Colspan}(\mathbf{M_1})$.

**Corollary 1.** *For any matrices $\mathbf{M}_1, \mathbf{M}_2$ and for any invertible matrices $\mathbf{N}_1, \mathbf{N}_2$ of the appropriate dimensions, we have that*

$$\mathrm{Colspan}\left(\left[\mathbf{M}_1 \| \mathbf{M}_2\right]\right) = \mathrm{Colspan}\left(\left[\mathbf{M}_1\mathbf{N}_1 \| \mathbf{M}_2\mathbf{N}_2\right]\right).$$

These statements and their proofs can be found in Appendix 4.4, under Lemma 12 and Corollary 6.

By Corollary 1 we have,

$$\begin{aligned}
&\text{Colspan}\left(\mathbf{P}\cdot\left[\mathbf{A}_1\otimes\mathbf{I}_m^{\otimes(d-1)}\|\cdots\|\mathbf{I}_m^{\otimes(d-1)}\otimes\mathbf{A}_d\right]\right)\\
&\quad=\text{Colspan}\left(\mathbf{P}\cdot\left[\left(\mathbf{A}_1\otimes\mathbf{I}_m^{\otimes(d-1)}\right)\cdot\mathbf{N}_1\|\cdots\|\left(\mathbf{I}_m^{\otimes(d-1)}\otimes\mathbf{A}_d\right)\cdot\mathbf{N}_d\right]\right)\\
&\quad=\text{Colspan}\left(\mathbf{P}\cdot\left[\mathbf{A}_1\cdot\mathbf{A}_{1,T}^{-1}\otimes\mathbf{I}_m^{\otimes(d-1)}\|\cdots\|\mathbf{I}_m^{\otimes(d-1)}\otimes\mathbf{A}_d\cdot\mathbf{A}_{d,T}^{-1}\right]\right).
\end{aligned}$$

By definition of the scheme,

$$\mathbf{A}^*=\mathbf{P}\cdot\left[\mathbf{A}_1\otimes\mathbf{I}_m^{\otimes(d-1)}\|\cdots\|\mathbf{I}_m^{\otimes(d-1)}\otimes\mathbf{A}_d\right]\cdot\mathbf{K}$$

for some matrix $\mathbf{K}\in\mathbb{Z}_q^{dwm^{d-1}\times W}$ that preserves the column span of

$$\mathbf{P}\cdot\left[\mathbf{A}_1\otimes\mathbf{I}_m^{\otimes(d-1)}\|\cdots\|\mathbf{I}_m^{\otimes(d-1)}\otimes\mathbf{A}_d\right].$$

Since the column span is preserved by $\mathbf{K}$,

$$\text{Colspan}(\mathbf{A}^*)=\text{Colspan}\left(\mathbf{P}\cdot\left[\mathbf{A}_1\cdot\mathbf{A}_{1,T}^{-1}\otimes\mathbf{I}_m^{\otimes(d-1)}\|\cdots\|\mathbf{I}_m^{\otimes(d-1)}\otimes\mathbf{A}_d\cdot\mathbf{A}_{d,T}^{-1}\right]\right)$$

which implies, by Lemma 1, that there exists some matrix $\mathbf{M}$ that satisfies Equation 1 when we consider $\mathbf{U}_i\leftarrow\mathbf{A}_i\cdot\mathbf{A}_{i,T}^{-1}$ for all $i\in[d]$.

**(Step 1) Uniqueness when P is absent**: To build intuition for the full uniqueness argument, we present it in the simpler setting in which $\mathbf{P}$ is entirely absent from the scheme in the DQVWW assumption. Let us also consider the simple case when $d=2$. In this toy case, there is no matrix $\mathbf{P}$ used to generate $\mathbf{A}^*$, so for this simple case we instead consider when the algorithm is given a matrix of the form $\mathbf{T}^*=\left[\mathbf{A}_1\otimes\mathbf{I}_m\|\mathbf{I}_m\otimes\mathbf{A}_2\right]\mathbf{K}$ for some column span preserving Kilian matrix $\mathbf{K}$. We show the following claim.

**Lemma 2 (Simple case without P).** *For matrices* $\mathbf{U}_1=\begin{bmatrix}\mathbf{I}_w\\ \tilde{\mathbf{A}}_1\end{bmatrix},\mathbf{U}_2=\begin{bmatrix}\mathbf{I}_w\\ \tilde{\mathbf{A}}_2\end{bmatrix},\mathbf{U}_1'=\begin{bmatrix}\mathbf{I}_w\\ \tilde{\mathbf{A}}_1'\end{bmatrix},\mathbf{U}_2'=\begin{bmatrix}\mathbf{I}_w\\ \tilde{\mathbf{A}}_2'\end{bmatrix}\in\mathbb{Z}_q^{m\times w}$*, if*

$$\text{Colspan}\left(\left[\mathbf{U}_1\otimes\mathbf{I}_m\|\mathbf{I}_m\otimes\mathbf{U}_2\right]\right)=\text{Colspan}\left(\left[\mathbf{U}_1'\otimes\mathbf{I}_m\|\mathbf{I}_m\otimes\mathbf{U}_2'\right]\right).\qquad(3)$$

*then* $\tilde{\mathbf{A}}_i=\tilde{\mathbf{A}}_i'$ *for* $i\in[2]$ *so that* $\mathbf{U}_1=\mathbf{U}_1'$ *and* $\mathbf{U}_2=\mathbf{U}_2'$.

Before we show how to prove Lemma 2, let us show that Lemma 2 implies uniqueness. In particular, we now explain why it is reasonable to require in the statement of Lemma 2 that the column spans are *equal*.

Recall that the algorithm finds a solution to $\{\tilde{\mathbf{A}}_i\}_{i\in[2]}$ and $\mathbf{M}$ in Equation 1 which is of the following form in the simplified setting:

$$\left[\mathbf{U}_1\otimes\mathbf{I}_m\|\mathbf{I}_m\otimes\mathbf{U}_2\right]=\mathbf{T}^*\cdot\mathbf{M}.$$

Then, by Lemma 1, any solution to $\{\tilde{\mathbf{A}}_i\}_{i\in[2]}$ satisfies the set *containment* $\text{Colspan}\left(\left[\mathbf{U}_1\otimes\mathbf{I}_m\|\mathbf{I}_m\otimes\mathbf{U}_2\right]\right)\subseteq\text{Colspan}(\left[\mathbf{A}_1\otimes\mathbf{I}_m\|\mathbf{I}_m\otimes\mathbf{A}_2\right])$.

**Corollary 2.** *With overwhelming probability over the choice of random* $\mathbf{A}_i \in \mathbb{Z}_q^{m \times w}$*, for* $i \in [d]$*, if*

$$\begin{aligned}&\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)\\ &\quad\subseteq \text{Colspan}\left(\left[\mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d\right]\right)\end{aligned}$$

*then*

$$\begin{aligned}&\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)\\ &\quad= \text{Colspan}\left(\left[\mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d\right]\right)\end{aligned}$$

The proof sketch can be found in Supp. Materials Section 4.5 under Corollary 11.

By Corollary 2, with overwhelming probability over the choice $\mathbf{A}_1, \mathbf{A}_2$, set containment in this setting actually implies set *equality*:

$$\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m \| \mathbf{I}_m \otimes \mathbf{U}_2\right]\right) = \text{Colspan}(\left[\mathbf{A}_1 \otimes \mathbf{I}_m \| \mathbf{I}_m \otimes \mathbf{A}_2\right]).$$

Therefore, any solution found for the simplified version of Equation 1 satisfies the above set equality, and our new Lemma 2 implies that there is only one such choice of $\{\tilde{\mathbf{A}}_i\}_{i\in[2]}$ that satisfies this equality.

*Proof (Proof of Lemma 2).* Proving this fact is done by a linear independence argument enabled by the structure of matrices $\mathbf{U}_i$ and by the tensor construction.

We now give a direct argument for uniqueness by showing that $\mathbf{U}_1 = \mathbf{U}_1'$ column-by-column. To show, for example, that the first column $\mathbf{v} = \mathbf{e}_1^{(1)}$ of $\mathbf{U}_1 = \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_1\end{bmatrix}$ is equal to the first column of $\mathbf{v}'$ of $\begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_1'\end{bmatrix}$, we perform the following steps.

- We observe that $\mathbf{v}'$ can expressed in the basis $\mathcal{B}_1$ in a special linear combination: $\mathbf{v}' = \mathbf{e}_1^{(1)} + \sum_{j\in\{w+1,\ldots,m\}} \alpha_j' \mathbf{e}_j^{(1)}$ for some coefficients $\alpha_j'$.
- We consider the vector $\mathbf{v}' \otimes \mathbf{e}_m^{(2)}$ which is in both the LHS and RHS of Equation 3. Because it is in both column spans, this vector can be written as

$$\mathbf{v}' \otimes \mathbf{e}_m^{(2)} = \sum_{i\le w \text{ or } j \le w} \lambda_{i,j} \cdot \mathbf{e}_i^{(1)} \otimes \mathbf{e}_j^{(2)}.$$

On the other hand, substituting for $\mathbf{v}'$ and rearranging gives

$$0 = (\lambda_{1,m} - 1) \cdot \mathbf{e}_1^{(1)} \otimes \mathbf{e}_m^{(2)} - \sum_{j \in \{w+1,\ldots,m\}} \alpha'_j \cdot \mathbf{e}_j^{(1)} \otimes \mathbf{e}_m^{(2)} + \sum_{i \leq w \text{ or } j \leq w} \lambda_{i,j} \cdot \mathbf{e}_i^{(1)} \otimes \mathbf{e}_j^{(2)}. \quad (4)$$

– $\mathcal{B}_1 \otimes \mathcal{B}_2 = \{\mathbf{e}_i^{(1)} \otimes \mathbf{e}_j^{(2)}\}_{i,j \in [m]}$ is a basis for $\mathbb{Z}_q^m \otimes \mathbb{Z}_q^m$. Therefore, the vectors in each of the terms above are linearly independent. This implies that for $j \in \{w+1, \ldots, m\}$, $\alpha'_j = 0$, and $\lambda_{1,m} = 1$, and for all other values of $i, j$ we have $\lambda_{i,j} = 0$.

The same outline of steps can be repeated column-by-column.

While this argument suffices to handle the case when $\mathbf{P}$ is absent, when $\mathbf{P}$ is present we exploit the following observation. In the argument above for the case of $d = 2$, we needed the linear independence of $m^2-(m-w)^2+(m-w)+1$ many vectors (given by each of the terms in Equation 4, although note that the first term will vary depending on which of the $w$ columns we are considering) which is a much smaller set of vectors than the total size of the basis for $\mathbb{Z}_q^m \otimes \mathbb{Z}_q^m$, which is $m^2$. For the argument to continue to hold when $\mathbf{P}$ is present, $\mathbf{P}$ only needs to preserve the linear independence of this small set of vectors. A formal statement and proof of this uniqueness is found in Theorem 2.

**(Step 1) Uniqueness in the general case**: Having seen the uniqueness argument in the simple case above without $\mathbf{P}$, we now address the general case where $\mathbf{P}$ is present.

In the general case, we introduce a single, reasonable conjecture about $\mathbf{P}$ being rank preserving on low-dimensional subspaces. Namely, we conjecture that with overwhelming probability over the choice of $\mathbf{P}$ whose entries are sampled from $\chi$ where $\mathbf{P}$ has $M$ rows, for $T \ll M$, and for any set of $T$ linearly independent vectors $\{\mathbf{v}_i\}_{i \in [T]}$, the set $\{\mathbf{P} \cdot \mathbf{v}_i\}_{i \in [T]}$ remains linearly independent. This conjecture enables us to firstly show that all solutions satisfy a column span set equality and secondly enable the same linear independence argument that shows that this set equality implies unique solutions.

We first note that the application of Lemma 1 on Equation 1, which we now restate,

$$\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right] = \mathbf{A}^* \cdot \mathbf{M}$$

shows that any solution to $\{\mathbf{U}_i\}_{i \in [d]}$ in Equation 1, satisfies the set *containment*

$$\text{Colspan}\left(\mathbf{P}\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right) \subseteq \text{Colspan}\left(\mathbf{A}^*\right). \quad (5)$$

To extend the uniqueness argument from above, we desire to show that any solution to $\{\mathbf{U}_i\}_{i \in [d]}$ in Equation 1 in fact satisfies the set *equality*:

$$\text{Colspan}\left(\mathbf{P}\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right) = \text{Colspan}(\mathbf{A}^*). \quad (6)$$

To see that the set containment implies set equality, we first observe that Corollary 2 gives us

$$\begin{aligned}&\mathrm{rk}\left(\left[\mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d\right]\right)\\&\quad = \mathrm{rk}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right).\end{aligned}$$

Then we use the assumption that $\mathbf{P}$ preserves the rank of low-dimensional subspaces. This assumption implies firstly that

$$\begin{aligned}&\mathrm{rk}\left(\mathbf{P}\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)\\&\quad = \mathrm{rk}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)\end{aligned}$$

and, recalling that $\mathbf{A}^* = \mathbf{P} \cdot \left[\mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d\right] \cdot \mathbf{K}$ for some column span preserving matrix $\mathbf{K}$, the assumption implies secondly that

$$\mathrm{rk}\left(\mathbf{A}^*\right) = \mathrm{rk}\left(\left[\mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d\right]\right)$$

Then we apply the following linear algebraic fact,

**Lemma 3.** *For any matrices* $\mathbf{M}, \mathbf{N}$ *with finitely many rows and columns such that* $\mathrm{Colspan}(\mathbf{M}) \subseteq \mathrm{Colspan}(\mathbf{N})$*, if* $\mathrm{rk}(\mathbf{M}) = \mathrm{rk}(\mathbf{N})$*, then* $\mathrm{Colspan}(\mathbf{M}) = \mathrm{Colspan}(\mathbf{N})$*.*

The proof can be found in Appendix 4.4 under Lemma 13.

to see that any solution $\{\mathbf{U}_i\}_{i\in[d]}$ that satisfies the set containment in Equation 5, also satisfies the set equality found in Equation 6. A formal statement of the conjecture on $\mathbf{P}$ and is given in Section 3.2.

Now that we've established this set equality, we return to our previous linear independence argument.

**Lemma 4 (Simple case with P).** *For matrices* $\mathbf{U}_1 = \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_1\end{bmatrix}, \mathbf{U}_2 = \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_2\end{bmatrix}$*,* $\mathbf{U}_1' = \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_1'\end{bmatrix}, \mathbf{U}_2' = \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_2'\end{bmatrix} \in \mathbb{Z}_q^{m\times w}$*, if*

$$\mathrm{Colspan}\left(\mathbf{P}\cdot\left[\mathbf{U}_1 \otimes \mathbf{I}_m \| \mathbf{I}_m \otimes \mathbf{U}_2\right]\right) = \mathrm{Colspan}\left(\mathbf{P}\cdot\left[\mathbf{U}_1' \otimes \mathbf{I}_m \| \mathbf{I}_m \otimes \mathbf{U}_2'\right]\right). \quad (7)$$

*then* $\tilde{\mathbf{A}}_i = \tilde{\mathbf{A}}_i'$ *for* $i \in [2]$ *so that* $\mathbf{U}_1 = \mathbf{U}_1'$ *and* $\mathbf{U}_2 = \mathbf{U}_2'$*.*

We leave the formal proof to the technical section and instead take the opportunity to demonstrate how the conjecture naturally extends the proof above

(proof of Lemma 2) to this setting in which $\mathbf{P}$ is present. To show, for example, that the first column $\mathbf{v} = \mathbf{e}_1^{(1)}$ of $\mathbf{U}_1 = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_1 \end{bmatrix}$ is equal to the first column of $\mathbf{v}'$ of $\begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}'_1 \end{bmatrix}$, we perform the almost identical steps as done before. We observe that $\mathbf{v}'$ can expressed in the basis $\mathcal{B}_1$ in a special linear combination: $\mathbf{v}' = \mathbf{e}_1^{(1)} + \sum_{j \in \{w+1,\ldots,m\}} \alpha'_j \mathbf{e}_j^{(1)}$ for some coefficients $\alpha'_j$. Then, using the set equality we showed above, we see that the vector $\mathbf{P} \cdot (\mathbf{v}' \otimes \mathbf{e}_m^{(2)})$, is in both Colspan $\left(\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)$ and in Colspan$(\mathbf{A}^*)$ where $\mathbf{A}^*$ was generated in a process that left-multiplied by $\mathbf{P}$. Therefore, it can also be expressed as

$$\mathbf{P} \cdot \mathbf{v}' \otimes \mathbf{e}_m^{(2)} = \mathbf{P} \cdot \left(\mathbf{e}_1^{(1)} \otimes \mathbf{e}_m^{(2)}\right) + \sum_{j \in \{w+1,\ldots,m\}} \alpha'_j \cdot \mathbf{P} \cdot \left(\mathbf{e}_j^{(1)} \otimes \mathbf{e}_m^{(2)}\right)$$

or as

$$\mathbf{P} \cdot \left(\mathbf{v}' \otimes \mathbf{e}_m^{(2)}\right) = \sum_{i \le w \text{ or } j \le w} \lambda_{i,j} \cdot \mathbf{P} \cdot \left(\mathbf{e}_i^{(1)} \otimes \mathbf{e}_j^{(2)}\right).$$

Taking the difference gives us the equation,

$$\begin{aligned} 0 = (\lambda_{1,m} - 1) \cdot \mathbf{P} \cdot \left(\mathbf{e}_1^{(1)} \otimes \mathbf{e}_m^{(2)}\right) &- \sum_{j \in \{w+1,\ldots,m\}} \alpha'_j \cdot \mathbf{P} \cdot \left(\mathbf{e}_j^{(1)} \otimes \mathbf{e}_m^{(2)}\right) \\ &+ \sum_{i \le w \text{ or } j \le w} \lambda_{i,j} \cdot \mathbf{P} \cdot \left(\mathbf{e}_i^{(1)} \otimes \mathbf{e}_j^{(2)}\right). \end{aligned}$$

For us to finish arguing that all the coefficients $\alpha'_j = 0$, for $j \in \{w+1, \ldots, m\}$, we need the linearly independence of the following set of vectors

$$\left\{\mathbf{P} \cdot \left(\mathbf{e}_1^{(1)} \otimes \mathbf{e}_m^{(2)}\right)\right\} \cup \left\{\mathbf{P} \cdot \left(\mathbf{e}_j^{(1)} \otimes \mathbf{e}_m^{(2)}\right)\right\}_{j \in \{w+1,\ldots,m\}} \cup \left\{\mathbf{P} \cdot \left(\mathbf{e}_i^{(1)} \otimes \mathbf{e}_j^{(2)}\right)\right\}_{i \le w \text{ or } j \le w}.$$

The proposed conjecture above that $\mathbf{P}$ preserves the linear independence of this small number of vectors directly addresses this.

### 2.5 Correctness of Step 2

In Step 2, we assume that the algorithm has already recovered the unique solution for $\{\tilde{\mathbf{A}}_i\}_{i \in [d]}$ (therefore, it has also recovered a unique solution for $\{\mathbf{U}_i\}_{i \in [d]}$) in Step 1. We claim that in Step 2 of the algorithm above, there exists a unique solution for $\mathbf{V}_1$ in Equation 2, which is restated below:

$$\mathbf{P} \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right] \begin{bmatrix} \mathbf{V}_1 \otimes \mathbf{B}'_2 \\ \mathbf{Z} \end{bmatrix} \mathbf{P}' \cdot \mathbf{Q} = \mathbf{Y} \cdot \mathbf{Q}.$$

To show uniqueness in Step 2, we consider the homogeneous version (when the RHS is $\mathbf{0}$) of Equation 2:

$$\mathbf{P} \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right] \begin{bmatrix} \mathbf{V}_1 \otimes \mathbf{B}'_2 \\ \mathbf{Z} \end{bmatrix} \mathbf{P}' \cdot \mathbf{Q} = \mathbf{0}.$$

Any solution for $\mathbf{V}_1$ and $\mathbf{Z}$ in the homogeneous version is exactly the difference of two solutions for $\mathbf{V}_1$ and $\mathbf{Z}$ in the inhomogeneous version. Therefore, by showing that the only solution for $\mathbf{V}_1$ in the homogeneous system is the zero matrix, we show that there is a unique solution for inhomogeneous version.

Intuitively, one sees that uniqueness is possible by observing that in the block $\mathbf{V}_1 \otimes \mathbf{B}'_2$ is linear in the entries of $\mathbf{V}_1$ and there are only $wk$ unknowns but many equations (as many as the number of entries in $\mathbf{V}_1 \otimes \mathbf{B}'_2$). On the other hand, in terms of uniqueness, one should be concerned about the unknown matrix $\mathbf{Z}$ in Equation 2. However, we show how to isolate a linear equation in only $\mathbf{V}_1$ (removing $\mathbf{Z}$) thereby revealing that $\mathbf{V}_1$ must have a unique solution with high probability. The proof of uniqueness then proceeds by a rank argument. We present an overview of this proof in three steps: firstly, we show that there always exists a solution, secondly we give a simple observation for when $\mathbf{P}$ is not present, and finally we give the high level argument for when $\mathbf{P}$ is present.

**(Step 2) Existence of a solution**: By definition of the scheme, $\mathbf{A}^* \cdot \mathbf{S}^* = \bar{\mathbf{A}}^* \cdot \bar{\mathbf{S}}^*$ where,

$$\bar{\mathbf{A}}^* = \mathbf{P}(\mathbf{A_1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{A}_d),$$

$$\bar{\mathbf{S}}^* = \begin{pmatrix} \mathbf{S}_1 \otimes \mathbf{B}_2 \otimes \mathbf{B}_3 \otimes \ldots \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \mathbf{E}_1 \otimes \mathbf{S}_2 \otimes \mathbf{B}_3 \otimes \ldots \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \vdots \\ \mathbf{E}_1 \otimes \mathbf{E}_2 \otimes \mathbf{E}_3 \otimes \ldots \mathbf{E}_{d-1} \otimes \mathbf{S}_d \end{pmatrix} \cdot \mathbf{P}'$$

Thus, due to the properties of tensor products $\mathbf{A}^* \cdot \mathbf{S}^* = \mathbf{L}_1 \cdot \mathbf{L}_2$, where,

$$\mathbf{L}_1 = \mathbf{P}(\mathbf{A}_1 \cdot \mathbf{A}_{1,T}^{-1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{A}_d \cdot \mathbf{A}_{d,T}^{-1}),$$

$$\mathbf{L}_2 = \begin{pmatrix} \mathbf{A}_{1,T} \cdot \mathbf{S}_1 \otimes \mathbf{B}_2 \otimes \mathbf{B}_3 \otimes \ldots \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \mathbf{E}_1 \otimes \mathbf{A}_{2,T}\mathbf{S}_2 \otimes \mathbf{B}_3 \otimes \ldots \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \vdots \\ \mathbf{E}_1 \otimes \mathbf{E}_2 \otimes \mathbf{E}_3 \otimes \ldots \mathbf{E}_{d-1} \otimes \mathbf{A}_{d,T}\mathbf{S}_d \end{pmatrix} \cdot \mathbf{P}'$$

Therefore, there is a solution to Equation 2 where $\mathbf{V}_1 = \mathbf{A}_{1,T} \cdot \mathbf{S}_1$.

**(Step 2) Uniqueness when P is absent**: Uniqueness is argued by considering the homogeneous version of Equation 2 (obtained by taking the difference of two candidate solutions) and arguing that the only solution is the zero solution (the difference is zero, so the two solutions are equal). Consider the homogeneous equation when $\mathbf{P}$ is absent:

$$\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right] \begin{bmatrix} \mathbf{V}'_1 \otimes \mathbf{B}'_2 \\ \mathbf{Z}' \end{bmatrix} \mathbf{P}' \cdot \mathbf{Q} = \mathbf{0} \tag{8}$$

where the entries of $\mathbf{V}'_1, \mathbf{Z}'$ are the unknowns. In this case, it easy to see that $\mathbf{V}'_1 = \mathbf{0}$ since we can remove $\mathbf{Z}'$ by left multiplying both sides of Equation 8 by the matrix

$$\mathbf{U}^{\perp} \triangleq \left[\mathbf{I}_m \otimes \mathbf{U}_2^{\perp} \otimes \cdots \mathbf{U}_d^{\perp}\right]$$

where $\mathbf{U}_i^{\perp} \in \mathbb{Z}_q^{(m-w)\times m}$ are full rank annihilators of $\mathbf{U}_i$, that is $\mathbf{U}_i^{\perp}\mathbf{U}_i = \mathbf{0}$. Moreover, observe that if $\mathbf{U}_i$ are the Hermite normal forms of $\mathbf{A}_i$, then $\mathbf{U}_i^{\perp}$ also annihilates $\mathbf{A}_i$. Left multiplying both sides of Equation 8 by $\mathbf{U}^{\perp}$ and expanding $\mathbf{B}'_2 = \mathbf{B}_2 \otimes \cdots \otimes \mathbf{B}_d$ where $\mathbf{B}_i = \mathbf{A}_i\mathbf{S}_i + \mathbf{E}_i$ gives:

$$\left(\mathbf{U}_1 \cdot \mathbf{V}'_1 \otimes \mathbf{U}_2^{\perp} \cdot \mathbf{E}_2 \otimes \cdots \otimes \mathbf{U}_d^{\perp} \cdot \mathbf{E}_d\right) \cdot \mathbf{P}' \cdot \mathbf{Q} = \mathbf{0}. \tag{9}$$

This equation implies that $\mathbf{V}'_1 = \mathbf{0}$ with high probability. Observe that the error terms $\mathbf{E}_i$, the matrix $\mathbf{P}'$, and the matrix $\mathbf{Q}$ are independently produced. Moreover, with high probability over the choice of error terms $\mathbf{E}_i$, we have $\mathbf{U}_i^{\perp} \cdot \mathbf{E}_i \neq \mathbf{0}$. If $\mathbf{V}'_1$ is non-zero then $\mathbf{U}_1 \cdot \mathbf{V}'_1 \neq \mathbf{0}$, since $\mathbf{U}_1$ has full column rank, which would imply that the LHS of Equation 9 is non-zero, a contradiction. Therefore, $\mathbf{V}'_1 = \mathbf{0}$ with high probability and we have uniqueness for a solution to $\mathbf{V}_1$ when $\mathbf{P}$ is absent.

**(Step 2) Uniqueness when P is present**: Now we consider the homogeneous equation with $\mathbf{P}$:

$$\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right] \begin{bmatrix} \mathbf{V}'_1 \otimes \mathbf{B}'_2 \\ \mathbf{Z}' \end{bmatrix} \mathbf{P}' \cdot \mathbf{Q} = \mathbf{0} \tag{10}$$

where $\mathbf{V}'_1$ and $\mathbf{Z}'$ are the unknowns. Here, from the matrix point of view the tensor structure is destroyed by the action of $\mathbf{P}$, for example consider $\mathbf{P} \cdot (\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)})$, obstructing us from using the simple argument for uniqueness above. An argument using column spans is also inhibited because the matrix of interest $\begin{bmatrix} \mathbf{V}'_1 \otimes \mathbf{B}'_2 \\ \mathbf{Z}' \end{bmatrix}$ is left-multiplied by the matrix

$$\mathbf{P}\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right].$$

The key insight from the simple argument above is that it allowed us to isolate $\mathbf{V}'_1$ in a simple homogeneous equation where $\mathbf{Z}'$ is absent. Therefore, we aim to again isolate $\mathbf{V}'_1$ in a simple homogeneous equation to prove uniqueness in this general setting, we first expand Equation 10:

$$\begin{aligned} &\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right] (\mathbf{V}'_1 \otimes \mathbf{B}'_2) \cdot \mathbf{P}' \cdot \mathbf{Q} \\ &\quad + \mathbf{P} \cdot \left[\mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right] \mathbf{Z}' \cdot \mathbf{P}' \cdot \mathbf{Q} = \mathbf{0} \end{aligned}$$

Applying the principle of wishful thinking, if the columns of $\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right]$ were linearly independent from those of $\mathbf{P} \cdot \left[\mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]$ then the first term alone must satisfy $\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right] (\mathbf{V}'_1 \otimes \mathbf{B}'_2) \cdot \mathbf{P}' \cdot \mathbf{Q} = \mathbf{0}$, thereby isolating $\mathbf{V}'_1$ in a new homogeneous equation without the presence of $\mathbf{Z}'$. This independence, however, is false. The two column spans certainly overlap.

To make this approach work, a simple modification suffices: we can take a submatrix of $\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right]$ and remove from consideration all the columns of $\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right]$ contained in

$$\text{Colspan}\left(\mathbf{P} \cdot \left[\mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right).$$

Moreover, we can compute the exact rank of this submatrix combinatorially as $w(m-w)^{d-1}$. Leaving the exact details to the main technical body, this observation leads us to an equation of the form

$$\mathbf{X}_1 \cdot (\mathbf{V}_1' \otimes \mathbf{B}_2') \cdot \mathbf{P}' \cdot \mathbf{Q} = 0.$$

for some matrix $\mathbf{X}_1$ that has a nullspace of dimension $O(w^2 m^{d-2})$. On the other hand, we will observe that when $\mathbf{V}_1' \neq \mathbf{0}$, $\mathbf{V}_1' \otimes \mathbf{B}_2'$ has rank at least $O(m^{d-1})$. Therefore, it must be the case that $\mathbf{V}_1' = \mathbf{0}$ if $m = \omega(w^2)$ and we observe that the initial work of [29] sets $m \geq w^3$. In a nutshell, the significant amount of non-overlap of the column span of $\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right]$ with the column span $\text{Colspan}\left(\mathbf{P} \cdot \left[\mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)$ is still enough to argue uniqueness of $\mathbf{V}_1$. The full details of this uniqueness claim can be found in Section 4.1.

## 3 Our Attack

**Theorem 1.** *Under Conjecture 1, there exists a polynomial time probabilistic algorithm that recovers $\{\mathbf{E}_i\}_{i\in[d]}$ for $i \in [d]$ when given an input from $\mathcal{D}_0$.*

*Proof.* We construct an algorithm $\mathcal{A}$ that takes an input

$$\Delta_0 = (\mathbf{P}, \mathbf{P}', \mathbf{A}^*, \{\mathbf{B}_i\}_{i\in[d]}, \hat{\mathbf{B}}, \mathbf{C}, \mathbf{E}^* + \mathbf{E} \cdot G^{-1}(\hat{\mathbf{B}})),$$

and outputs $\{\mathbf{E}_i\}_{i\in[d]}$. In a nutshell, the algorithm will be able to compute matrices $\mathbf{V}_1 \in \mathbb{Z}_q^{m\times w}$ and $\mathbf{U}_1 \in \mathbb{Z}_q^{w\times k}$ such that $\mathbf{B}_1 \in \mathbb{Z}_q^{m\times k}$ such that $\mathbf{B}_1 = \mathbf{U}_1 \cdot \mathbf{V}_1 + \mathbf{E}_1 \in \mathbb{Z}_q^{m\times k}$ such that $\mathbf{E}_1 \in \mathbb{Z}_q^{m\times k}$ has a small norm. Our attack recovers all the errors $\mathbf{E}_i$ for $i \in [d]$, giving a full recovery algorithm.

As described in the overview, there are only two steps where each step only uses Gaussian Elimination on polynomial sized systems of equations.

**Algorithm for Recovery of $\mathbf{E}_1$**

Input: $(\mathbf{P}, \mathbf{P}', \mathbf{A}^*, \{\mathbf{B}_i\}_{i\in[d]}, \hat{\mathbf{B}}, \mathbf{C}, \mathbf{E}^* + \mathbf{E}\mathbf{G}^{-1}(\hat{\mathbf{B}})$.
Output: $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}, \mathbf{V}_1, \mathbf{E}_1$.

1. **Recover $\mathbf{U}_1, \ldots, \mathbf{U}_d$**: Solve the affine system of equations defined by

$$\mathbf{P} \cdot \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right] = \mathbf{A}^* \cdot \mathbf{M}$$

where $\mathbf{U}_i = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_i \end{bmatrix}$, for $i \in [d]$, and the variables are given by the entries of $\tilde{\mathbf{A}}_1, \ldots, \tilde{\mathbf{A}}_d \in \mathbb{Z}_q^{(m-w)\times w}$ and the entries of $\mathbf{M} \in \mathbb{Z}_q^{W \times dwm^{d-1}}$ and the coefficients are given by the entries of $\mathbf{A}^*$ and $\mathbf{P}$. We discuss this step in detail in Section 3.2.

2. **Recover $\mathbf{V}_1$**: Having recovered the unique matrices $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$, our algorithm now aims to recover $\mathbf{V}_1$ such that $\mathbf{U}_1 \cdot \mathbf{V}_1 = \mathbf{A}_1 \cdot \mathbf{S}_1$. To do this, our algorithm computes

$$\mathbf{Y} = \mathbf{A}^* \cdot (\mathbf{S}^* + \mathbf{R} \cdot \mathbf{G}^{-1}(\hat{\mathbf{B}}))$$

by subtracting off the error $\mathbf{E}^* + \mathbf{E} \cdot \mathbf{G}^{-1}(\hat{\mathbf{B}})$ from $\mathbf{B}^* + \mathbf{C} \cdot \mathbf{G}^{-1}(\mathbf{B})$. Then it computes, via standard linear algebra, a full rank annihilator matrix $\mathbf{Q} \in \mathbb{Z}_q^{K\times(K-M\log q)}$ such that $\mathbf{G}^{-1}(\hat{\mathbf{B}}) \cdot \mathbf{Q} = \mathbf{0}$, obtaining the equation,

$$\mathbf{A}^* \cdot \mathbf{S}^* \cdot \mathbf{Q} = \mathbf{Y} \cdot \mathbf{Q}.$$

Finally, it solves the linear system of equations defined by

$$\mathbf{P}\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right] \begin{bmatrix} \mathbf{V}_1 \otimes \mathbf{B}_2' \\ \mathbf{Z} \end{bmatrix} \mathbf{P}' \cdot \mathbf{Q} = \mathbf{Y} \cdot \mathbf{Q}$$

where $\mathbf{B}_2' = \mathbf{B}_2 \otimes \ldots \otimes \mathbf{B}_d$ and where the variables are the entries of $\mathbf{V}_1$ and $\mathbf{Z}$ and the coefficients are given by the entries of $\mathbf{P}$, $\mathbf{P}'$, $\mathbf{Q}$, $\mathbf{Y}$, $\mathbf{U}_i$, for $i \in [d]$, and $\mathbf{B}_2'$. Finally, $\mathbf{E}_1$ is now recovered by computing $\mathbf{B}_1 - \mathbf{U}_1 \cdot \mathbf{V}_1$. We discuss this step in Section 4.1.

The above two steps details the main step of the algorithm. Having recovered $\mathbf{U}_1, \mathbf{V}_1$, we can now recover $\mathbf{E}_1$ from $\mathbf{B}_1$. We now describe how to extend the same recovery algorithm to $\mathbf{E}_2, \ldots, \mathbf{E}_d$. First consider the case of recovering $\mathbf{E}_2$.

**Extension to $\mathbf{E}_2$**: The algorithm described above allows us to learn recover $\mathbf{V}_1$ and $\mathbf{E}_1$ where $\mathbf{B}_1 - \mathbf{U}_1\mathbf{V}_1 = \mathbf{E}_1$. The idea is that we can repeat this process to learn $\mathbf{E}_2, \ldots, \mathbf{E}_d$. Note that in the equation

$$\mathbf{P}(\mathbf{U_1} \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d) \cdot \begin{bmatrix} \mathbf{V}_1 \otimes \mathbf{B}^{(2,\ldots,d)} \\ \mathbf{Z} \end{bmatrix} \mathbf{P}'\mathbf{Q} = \mathbf{Y}\mathbf{Q},$$

once $\mathbf{V}_1$ is known, we can begin exploiting the structure of a candidate solution to $\mathbf{Z}$. In particular, there exists a solution for $\mathbf{Z}$ which is of the form:

$$\bar{\mathbf{Z}} = \begin{pmatrix} \mathbf{E}_1 \otimes \mathbf{A}_{2,T} \cdot \mathbf{S}_2 \otimes \mathbf{B}_3 \otimes \ldots \otimes \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \vdots \\ \mathbf{E}_1 \otimes \mathbf{E}_2 \otimes \mathbf{E}_3 \otimes \ldots \otimes \mathbf{E}_{d-1} \otimes \mathbf{A}_{d,T}\mathbf{S}_d \end{pmatrix} \cdot \mathbf{P}'.$$

This form allows us to solve for $\mathbf{V}_2, \mathbf{Z}_2$, once we have $\mathbf{V}_1, \mathbf{E}_1$, by setting up the system of affine equations given by:

$$\mathbf{P}(\mathbf{U_1} \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d) \cdot \begin{bmatrix} \mathbf{V}_1 \otimes \mathbf{B}^{(2,\ldots,d)} \\ \mathbf{E}_1 \otimes \mathbf{V}_2 \otimes \mathbf{B}_3 \otimes \ldots \otimes \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \mathbf{Z}_2 \end{bmatrix} \mathbf{P'Q} = \mathbf{YQ}$$

for which we know a candidate solution for $\mathbf{V}_2$ is $\mathbf{A}_{2,T}\mathbf{S}_2$. Here the unknowns are the entries of $\mathbf{V}_2, \mathbf{Z}_2$ and the coefficients are given by all the other matrices' entries. We solve for $\mathbf{V}_2$ as the equation is now linear in $\mathbf{V}_2$. Proving that this solution is unique will use the exact same ideas as above, except on a smaller system of equations which are affine instead of linear. We will continue this way for all remaining indices $i \in [d]$. We prove this uniqueness formally for the case of $i = 1$ in Section 4.1 and remark here that uniqueness in the other cases follow similarly.

*Remark 3.* Theorem 1 shows a full recovery attack for the case that the input is from $\mathcal{D}_0$ and can be extended via a heuristic argument to a distinguisher between $\mathcal{D}_0$ and $\mathcal{D}_1$ which we discuss in Section 3.1.

### 3.1 Distinguishing $\mathcal{D}_0$ from $\mathcal{D}_1$

To come up with a distinguisher which takes an instance from $\mathcal{D}_b$ for some $b \in \{0, 1\}$, we follow the following approach:

- We use the algorithm described in Theorem 1 to learn $\mathbf{E}_1, \ldots, \mathbf{E}_d$. As a remark, we note that equations solved for in the algorithm can be set up regardless of whether $b = 0$ or $b = 1$. What we show is that the recovery will succeed with high probability when $b = 0$.
- Once we have $\mathbf{E}_1, \ldots, \mathbf{E}_d$ we can compute $\mathbf{E}^* = \mathbf{P} \cdot (\mathbf{E}_1 \otimes \cdots \otimes \mathbf{E}_d) \cdot \mathbf{P'}$. Then, we can use the error leakage from the assumption $\mathbf{E}^* + \mathbf{E} \cdot G^{-1}(\hat{\mathbf{B}})$ to learn $\mathbf{E} \cdot G^{-1}(\hat{\mathbf{B}})$. We simply check that this is annihilated by multiplying by $\mathbf{Q}$. This will succeed in the case that $b = 0$.
- In the case when $b = 1$, the check will not pass because of the presence of a random error matrix $\mathbf{F}$, namely the leakage term is given by $\mathbf{E}^* + \mathbf{E} \cdot G^{-1}(\hat{\mathbf{B}}) - \mathbf{F}$ and even if we solve for $\mathbf{E}^*$ and attempt to annihilate the remaining terms, the term $\mathbf{E} \cdot G^{-1}(\hat{\mathbf{B}}) - \mathbf{F}$ cannot be annihilated because heuristically a random matrix $\mathbf{F}$ is unlikely to lie in the row span of $G^{-1}(\hat{\mathbf{B}})$ (noet that $G^{-1}(\hat{\mathbf{B}})$ is a wide matrix with a large right nullspace) .

### 3.2 Recovery of unique $\tilde{\mathbf{A}}_i$'s

Our first objective is to recover the matrices $\mathbf{A}_1, \ldots, \mathbf{A}_d$ up to a unique representation $\mathbf{U}_1 = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_1 \end{bmatrix}, \ldots, \mathbf{U}_d = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_d \end{bmatrix}$. The intuition for the below section is provided in detail in Section 2.4.

**Useful Claims and Conjectures**

*Conjecture 1 (Linear independence preservation under* $\mathbf{P}$*).* Let $m, w, d, k, K, M, q, \chi$ be parameters defined previously. If $\mathbf{v}_1, \ldots, \mathbf{v}_T$ are arbitrary linearly independent vectors in $\mathbb{Z}_q^{\otimes d}$, where $T = m^d - (m-w)^d + d \cdot m$ then with probability $1 - q^{-\Omega(w^2 m)}$ over the choice of $\mathbf{P} \leftarrow \chi^{M \times m^d}$, we have that $\mathbf{P} \cdot \mathbf{v}_1, \ldots, \mathbf{P} \cdot \mathbf{v}_T$ are linearly independent.

*Remark 4 (Limit on Modulus Size).* Naively using exponential modulus-to-noise ratios does not break the conjecture because the hardness of LWE puts a limit on this ratio. As a concrete attempt to break the conjecture, let us focus on the probability of sampling the zero-matrix, $\mathbf{P} \leftarrow \mathbf{0}$, given by $B^{-m^d \cdot M} = B^{-m^{2d-(1/2)}}$. The zero-matrix is not injective on any non-trivial subspace so to attempt to break the conjecture, we can set the modulus $q$ such that the probability of sampling the zero-matrix is larger than $q^{-\Omega(w^2 m)}$. For this attempt to be succeed, we require the relation $B^{-m^{2d-(1/2)}} \geq q^{-\Omega(w^2 m)}$ which implies that setting $q \geq B^{\Omega(m^{2d-3/2}/w^2)} \geq 2^{\Omega(m^{2d-3/2}/w^2)}$ (since $B \geq 2$) is enough to refute the conjecture. Since $d \geq 3$ and $m \geq w^3$, this setting of modulus $q$ is much too large for LWE security to hold as security requires $q \leq 2^{O(m)}$. In other words, in this setting, the distribution $\chi$ is *not* an LWE-friendly error distribution and is not an admissible choice of $\chi$ allowed in the original assumptions (see Section 2.1 and Remark 1).

*Remark 5.* If $\mathbf{P}$ is a uniformly random matrix over $\mathbb{Z}_q^{M \times m^d}$, a straightforward counting argument suffices to prove the above conjecture. If $\mathbf{P}$ is random, then $\mathbf{P}\mathbf{v}_1, \ldots, \mathbf{P}\mathbf{v}_T$ are jointly distributed as random vectors over $\mathbb{Z}_q^M$ provided $T \ll M$. For random vectors, the probability that they are linearly independent is at least $1 - O(T \cdot \frac{q^{T-1}}{q^M}) = 1 - O(q^{-M/2})$ when $T \ll M$.

Now we use the conjecture and express it in a notation useful to our proofs.

**Corollary 3 (Linear independence preservation under P, Useful Notation).** *Let* $m, w, d, k, K, M, q, \chi$ *be parameters defined previously. Let* $\mathbf{e}_j^{(i)}$ *denote the* $j$*th column of the matrix* $\mathcal{B}_i$*, which was defined in Section 2.3 so that for* $i \in [d]$*, the set* $\{\mathbf{e}_1^{(i)}, \mathbf{e}_2^{(i)}, \ldots, \mathbf{e}_m^{(i)}\}$ *is a basis for* $\mathbb{Z}_q^m$*. Then define*

$$\mathcal{B} \triangleq \left\{ \mathbf{e}_{i_1}^{(1)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)} : i_1, \ldots, i_d \in [m] \wedge \exists j \in [d], i_j \leq w, \right\} \cup \bigcup_{k=1}^{d} \left\{ \mathbf{e}_m^{(1)} \otimes \cdots \otimes \mathbf{e}_m^{(k-1)} \otimes \mathbf{e}_\ell^{(k)} \otimes \mathbf{e}_m^{(k+1)} \otimes \cdots \otimes \mathbf{e}_m^{(d)} : \ell \in [m] \right\}.$$

*Assuming Conjecture 1 and* $\mathbf{P}$ *is sampled from* $\chi^{M \times m^d}$ *, with probability* $1 - q^{-\Omega(w^2 m)}$*, the vectors in the set* $\mathcal{B}^{\mathbf{P}} \triangleq \{\mathbf{P} \cdot \mathbf{v} : \mathbf{v} \in \mathcal{B}\}$ *are linearly independent.*

*Proof.* Set $\mathbf{v}_1, \ldots, \mathbf{v}_T$ to the vectors in $\mathcal{B}$.

We now show that under Conjecture 1, for a random choice of $\mathbf{P}$ from $\chi$, with overwhelming probability there is no choice of matrices $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$ for which $\mathbf{P}$ does not preserve the linear independence of the set $\mathcal{B}$.

**Lemma 5.** *Let* $\mathbf{P} \leftarrow \chi^{M\times m^d}$ *and for* $i \in [d]$, *let* $\tilde{\mathbf{A}}_i \in \mathbb{Z}_q^{(m-w)\times w}$. *Assuming Conjecture 1,*

$$\Pr_{\mathbf{P}}\left[\exists\{\tilde{\mathbf{A}}_i\}_{i\in[d]} \text{ s.t. } \mathcal{B}^{\mathbf{P}} \text{ not linearly independent}\right] = q^{-\Omega(w^2m)} = \mathsf{negl}(w)$$

*Proof.* By Corollary 3, the probability over choice of $\mathbf{P}$ that $\mathbf{P}$ preserves the linear independence of $\mathcal{B}$ defined with respect to a fixed set of $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$ is $1 - q^{-\Omega(w^2m)}$. Taking a union bound over all possible values of $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$, for which there are $q^{dw(m-w)}$ many, we have

$$\Pr_{\mathbf{P}}[\exists\{\tilde{\mathbf{A}}_i\}_{i\in[d]} \text{ s.t. } \mathcal{B}^{\mathbf{P}} \text{ not linearly independent}] = q^{-\Omega(w^2m)+dw(m-w)} = q^{-\Omega(w^2m)}.$$

**Lemma 6.** *For* $i \in [d]$, *let* $\mathbf{L}_i \triangleq \mathbf{I}_m^{\otimes(i-1)} \otimes \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_i\end{bmatrix} \otimes \mathbf{I}_m^{\otimes(d-i)}$ *and let* $\tilde{\mathbf{A}} \triangleq \left[\mathbf{L}_1 \| \mathbf{L}_2 \| \cdots \| \mathbf{L}_d\right]$. *Under Conjecture 1, with overwhelming probability over the choice of* $\mathbf{P} \leftarrow \chi^{M\times m^d}$, *we have that the following holds for any set of matrices* $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$.

$$\forall i \in [d], \dim\left(\mathbf{P}\cdot\mathbf{L}_i\right) = wm^{d-1}$$

$$\dim\left(\text{Colspan}\left(\left[\mathbf{P}\cdot\mathbf{L}_1 \| \mathbf{P}\cdot\mathbf{L}_2 \| \ldots \| \mathbf{P}\cdot\mathbf{L}_d\right]\right)\right) = m^d - (m-w)^d = dwm^{d-1} - O\left(w^2m^{d-2}\right)$$

$$\dim\left(\text{Colspan}(\mathbf{P}\cdot\mathbf{L}_1) \cap \text{Colspan}\left(\left[\mathbf{P}\cdot\mathbf{L}_2 \| \ldots \| \mathbf{P}\cdot\mathbf{L}_d\right]\right)\right) = wm^{d-1} - w(m-w)^{d-1}$$

*Proof.* The proof can be found in the Supplementary Materials (under Lemma 18).

**Main Theorem for the Recovery of $\tilde{\mathbf{A}}_i$'s** The following theorem immediately gives rise to our recovery algorithm.

**Theorem 2 (Unique solutions for $\tilde{\mathbf{A}}_i$).** *Let* $M, m, w, k, d, q, \chi$ *be parameters as defined previously. Sample* $\mathbf{P} \leftarrow \chi^{M\times m^d}$. *Then with probability* $1 - \mathsf{negl}(m)$, *over the choice of* $\mathbf{P}$ *we have that for any choice of* $\tilde{\mathbf{A}}_i \in \mathbb{Z}_q^{(m-w)\times w}$ *for* $i \in [d]$ *and* $\tilde{\mathbf{A}}'_i$, *we have the following where we define*

$$\tilde{\mathbf{A}} \triangleq \left[\begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_1\end{bmatrix} \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_2\end{bmatrix} \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_d\end{bmatrix}\right]$$

$$\tilde{\mathbf{A}}' \triangleq \left[\begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}'_1\end{bmatrix} \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}'_2\end{bmatrix} \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}'_d\end{bmatrix}\right].$$

1. *If,* $\text{Colspan}\left(\mathbf{P}\tilde{\mathbf{A}}'\right) \subseteq \text{Colspan}\left(\mathbf{P}\tilde{\mathbf{A}}\right)$, *then* $\text{Colspan}\left(\mathbf{P}\tilde{\mathbf{A}}'\right) = \text{Colspan}\left(\mathbf{P}\tilde{\mathbf{A}}\right)$.
2. *Furthermore, if* $\text{Colspan}\left(\mathbf{P}\tilde{\mathbf{A}}'\right) = \text{Colspan}\left(\mathbf{P}\tilde{\mathbf{A}}\right)$ *for all* $i \in [d]$, *then* $\tilde{\mathbf{A}}_i = \tilde{\mathbf{A}}'_i$.

*Proof.* The proof of the first claim was fully addressed in Section 2.4 in *(Step 1) Uniqueness in the general case.*

We now address the second claim. The proof proceeds column-by-column of $\begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}'_i\end{bmatrix}$ for $i \in [d]$ and shows that each column of $\begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_i\end{bmatrix}$ is equal to its corresponding column in $\begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_i\end{bmatrix}$. We'll show that the first column of $\begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}'_1\end{bmatrix}$, say $\mathbf{d}_1^{(1)}$, is equal to the first column of $\begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_1\end{bmatrix}$.

First, for every $i \in [d]$ extend the columns of $\begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_i\end{bmatrix}$ to a basis for $\mathbb{Z}_q^m$ given by the columns of the matrix $\mathcal{B}_i$ below:

$$\mathcal{B}_i \triangleq \begin{bmatrix}\mathbf{I}_w & \mathbf{0}_{w\times(m-w)} \\ \tilde{\mathbf{A}}_i & \mathbf{I}_{m-w}\end{bmatrix} \in \mathbb{Z}_q^{m\times m}.$$

Let $\mathbf{e}_j^{(i)}$ denote the $j$th column in $\mathcal{B}_i$ and observe that for all the $j$th columns of $\mathcal{B}_i$ for $j \in [w+1, m]$ are all elementary vectors. That is, for $i \in [d]$ and for $j \in \{w+1, \ldots, d\}$, $\mathbf{e}_j^{(i)} = \mathbf{e}_j$ where $\mathbf{e}_j$ is the $j$th elementary vector. Now we aim to show that $\mathbf{d}_1^{(1)} = \mathbf{e}_1^{(1)}$.

Take a carefully chosen column of $\mathbf{P}\tilde{\mathbf{A}}'$, namely $\mathbf{P}\cdot\left(\mathbf{d}_1^{(1)} \otimes \mathbf{e}_m^{(2)} \otimes \cdots \otimes \mathbf{e}_m^{(d)}\right) \in \text{Colspan}\left(\mathbf{P}\tilde{\mathbf{A}}'\right) = \text{Colspan}\left(\mathbf{P}\tilde{\mathbf{A}}\right)$. Therefore, we can write an equation:

$$\begin{aligned}&\mathbf{P}\cdot\left(\mathbf{d}_1^{(1)} \otimes \mathbf{e}_m^{(2)} \otimes \cdots \otimes \mathbf{e}_m^{(d)}\right) \\ &\quad= \sum_{i_1,i_2,\ldots,i_d\in[m]\exists j\in[d] \text{ s.t. } i_j\in[w]} \lambda_{i_1,\ldots,i_d}\cdot\mathbf{P}\cdot(\mathbf{e}_{i_1}^{(1)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)}) \qquad (*)\end{aligned}$$

Now observe that, $\mathbf{d}_1^{(1)}$ has a special form. Namely, the first column $\mathbf{d}_1^{(1)}$ must be of the form $\mathbf{d}_1^{(1)} = \mathbf{e}_1^{(1)} + \sum_{w<j\le m}\alpha_j^{(1)}\mathbf{e}_j^{(1)}$ for some coefficients $\alpha_j^{(1)} \in \mathbb{Z}_q$, $j \in \{w+1, \ldots, m\}$. If we show that $\alpha_j^{(1)} = 0$ for all $j \in \{w+1, \ldots, m\}$, then $\mathbf{d}_1^{(1)} = \mathbf{e}_1^{(1)}$ and $\mathbf{e}_1^{(1)}$ is the first column of $\begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_1\end{bmatrix}$.

Substituting for $\mathbf{d}_1^{(1)}$, we have

$$\begin{aligned}&\mathbf{P}\cdot\left(\mathbf{d}_1^{(1)} \otimes \mathbf{e}_m^{(2)} \otimes \cdots \otimes \mathbf{e}_m^{(d)}\right) \\ &\quad= \mathbf{P}\cdot\left(\left(\mathbf{e}_1^{(1)} + \sum_{j>w}\alpha_j^{(1)}\mathbf{e}_j^{(1)}\right) \otimes \mathbf{e}_m^{(2)} \otimes \cdots \mathbf{e}_m^{(d)}\right) \\ &\quad= \mathbf{P}\cdot\left(\mathbf{e}_1^{(1)} \otimes \mathbf{e}_m^{(2)} \otimes \cdots \mathbf{e}_m^{(d)}\right) + \sum_{j>w}\alpha_j^{(1)}\mathbf{P}\cdot\left(\mathbf{e}_j^{(1)} \otimes \mathbf{e}_m^{(2)} \otimes \cdots \mathbf{e}_m^{(d)}\right) \qquad (**)\end{aligned}$$

Taking the difference of equation (*) and (**), we see that we have

$$\begin{aligned}0 =&(\lambda_{1,m,m,\ldots,m}-1)\cdot\mathbf{P}\cdot(\mathbf{e}_1^{(1)}\otimes\mathbf{e}_m^{(2)}\otimes\cdots\mathbf{e}_m^{(d)})\\&+\sum_{i_1\in\{w+1,\ldots,m\}}\alpha_j^{(1)}\cdot\mathbf{P}\cdot(\mathbf{e}_{i_1}^{(1)}\otimes\mathbf{e}_m^{(2)}\otimes\cdots\otimes\mathbf{e}_m^{(d)})\\&+\sum_{i_1,i_2,\ldots,i_d\in[m]\exists j\in[d]\text{ s.t. }i_j\in[w]}\lambda_{i_1,\ldots,i_d}\cdot\mathbf{P}\cdot(\mathbf{e}_{i_1}^{(1)}\otimes\cdots\otimes\mathbf{e}_{i_d}^{(d)})\end{aligned}$$

Now observe that every vector in this linear combination is linearly independent by Lemma 5 which states that

$$\begin{aligned}\mathcal{B}^{\mathbf{P}}=&\left\{\mathbf{P}\cdot\left(\mathbf{e}_{i_1}^{(1)}\otimes\cdots\otimes\mathbf{e}_{i_d}^{(d)}\right):i_1,\ldots,i_d\in[m]\wedge\exists j\in[d],i_j\le w,\right\}\\&\cup\bigcup_{k=1}^{d}\left\{\mathbf{P}\cdot\left(\mathbf{e}_m^{(1)}\otimes\cdots\mathbf{e}_m^{(k-1)}\otimes\mathbf{e}_\ell^{(k)}\otimes\mathbf{e}_m^{(k+1)}\otimes\cdots\otimes\mathbf{e}_m^{(d)}\right):\ell\in\{w+1,\ldots,m\}\right\}\end{aligned}$$

is a linearly independent set of vectors. Therefore, $\lambda_{1,m,m,\ldots,m}=1$ and $\alpha_j^{(1)}=0$ for all $j\in\{w+1,\ldots,d\}$. Therefore, $\mathbf{d}_1^{(1)}=\mathbf{e}_1^{(1)}$. To show that the $\ell$th column of $\begin{bmatrix}\mathbf{I}_w\\\tilde{\mathbf{A}}_i'\end{bmatrix}$, denoted $\mathbf{d}_\ell^{(i)}$, is the the $\ell$th column of $\begin{bmatrix}\mathbf{I}_w\\\tilde{\mathbf{A}}_i\end{bmatrix}$, denoted $\mathbf{e}_\ell^{(i)}$, apply the same argument on the vector $\mathbf{P}\cdot\left(\mathbf{e}_m^{\otimes(i-1)}\otimes\mathbf{d}_\ell^{(i)}\otimes\mathbf{e}_m^{\otimes(d-i)}\right)$.

## Acknowledgement

Aayush Jain is supported by the Computer Science Department, CMU and a seed grant from the CYLAB security and the privacy institute, CMU. Amit Sahai was supported in part from a Simons Investigator Award, DARPA SIEVE award, NTT Research, NSF Frontier Award 1413955, BSF grant 2012378, a Xerox Faculty Research Award, a Google Faculty Research Award, and an Okawa Foundation Research Grant. This material is based upon work supported by the Defense Advanced Research Projects Agency through Award HR00112020024. Huijia Lin was supported by NSF grants CNS-1936825 (CAREER), CNS-2026774, a JP Morgan AI research Award, a Cisco research award, and a Simons Collaboration on the Theory of Algorithmic Fairness. This work was done (in part) while Paul Lou was visiting the Simons Institute for the Theory of Computing.

We gratefully thank Hoeteck Wee for several extended technical discussions which greatly developed the presentation of our attack. We are also grateful to the anonymous TCC reviewers for graciously providing a thorough review process and giving us very useful feedback about our presentation.

## References

1. Agrawal, S.: Indistinguishability obfuscation without multilinear maps: New methods for bootstrapping and instantiation. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part I. LNCS, vol. 11476, pp. 191–225. Springer, Heidelberg (May 2019). https://doi.org/10.1007/978-3-030-17653-2_7

2. Agrawal, S., Pellet-Mary, A.: Indistinguishability obfuscation without maps: Attacks and fixes for noisy linear FE. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part I. LNCS, vol. 12105, pp. 110–140. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45721-1_5
3. Ananth, P., Jain, A., Lin, H., Matt, C., Sahai, A.: Indistinguishability obfuscation without multilinear maps: New paradigms via low degree weak pseudorandomness and security amplification. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part III. LNCS, vol. 11694, pp. 284–332. Springer, Heidelberg (Aug 2019). https://doi.org/10.1007/978-3-030-26954-8_10
4. Ananth, P., Jain, A.: Indistinguishability obfuscation from compact functional encryption. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015, Part I. LNCS, vol. 9215, pp. 308–326. Springer, Heidelberg (Aug 2015). https://doi.org/10.1007/978-3-662-47989-6_15
5. Ananth, P., Sahai, A.: Projective arithmetic functional encryption and indistinguishability obfuscation from degree-5 multilinear maps. In: Coron, J.S., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part I. LNCS, vol. 10210, pp. 152–181. Springer, Heidelberg (Apr / May 2017). https://doi.org/10.1007/978-3-319-56620-7_6
6. Badrinarayanan, S., Goyal, V., Jain, A., Sahai, A.: Verifiable functional encryption. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 557–587. Springer, Heidelberg (Dec 2016). https://doi.org/10.1007/978-3-662-53890-6_19
7. Badrinarayanan, S., Miles, E., Sahai, A., Zhandry, M.: Post-zeroizing obfuscation: New mathematical tools, and the case of evasive circuits. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 764–791. Springer, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49896-5_27
8. Ballard, L., Green, M., de Medeiros, B., Monrose, F.: Correlation-resistant storage via keyword-searchable encryption. Cryptology ePrint Archive, Report 2005/417 (2005), https://eprint.iacr.org/2005/417
9. Barak, B., Brakerski, Z., Komargodski, I., Kothari, P.: Limits on low-degree pseudorandom generators (or: Sum-of-squares meets program obfuscation). Electronic Colloquium on Computational Complexity (ECCC) **24**, 60 (2017)
10. Barak, B., Garg, S., Kalai, Y.T., Paneth, O., Sahai, A.: Protecting obfuscation against algebraic attacks. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 221–238. Springer, Heidelberg (May 2014). https://doi.org/10.1007/978-3-642-55220-5_13
11. Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S.P., Yang, K.: On the (im)possibility of obfuscating programs. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 1–18. Springer, Heidelberg (Aug 2001). https://doi.org/10.1007/3-540-44647-8_1
12. Barak, B., Hopkins, S.B., Jain, A., Kothari, P., Sahai, A.: Sum-of-squares meets program obfuscation, revisited. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part I. LNCS, vol. 11476, pp. 226–250. Springer, Heidelberg (May 2019). https://doi.org/10.1007/978-3-030-17653-2_8
13. Bartusek, J., Ishai, Y., Jain, A., Ma, F., Sahai, A., Zhandry, M.: Affine determinant programs: A framework for obfuscation and witness encryption. In: Vidick, T. (ed.) ITCS 2020. vol. 151, pp. 82:1–82:39. LIPIcs (Jan 2020). https://doi.org/10.4230/LIPIcs.ITCS.2020.82
14. Bitansky, N., Nishimaki, R., Passelègue, A., Wichs, D.: From cryptomania to obfustopia through secret-key functional encryption. In: Hirt, M., Smith, A.D. (eds.) TCC 2016-B, Part II. LNCS, vol. 9986, pp. 391–418. Springer, Heidelberg (Oct / Nov 2016). https://doi.org/10.1007/978-3-662-53644-5_15

15. Bitansky, N., Paneth, O., Rosen, A.: On the cryptographic hardness of finding a Nash equilibrium. In: Guruswami, V. (ed.) 56th FOCS. pp. 1480–1498. IEEE Computer Society Press (Oct 2015). https://doi.org/10.1109/FOCS.2015.94
16. Bitansky, N., Vaikuntanathan, V.: Indistinguishability obfuscation from functional encryption. In: Guruswami, V. (ed.) 56th FOCS. pp. 171–190. IEEE Computer Society Press (Oct 2015). https://doi.org/10.1109/FOCS.2015.20
17. Boneh, D., Wu, D.J., Zimmerman, J.: Immunizing multilinear maps against zeroizing attacks. Cryptology ePrint Archive, Report 2014/930 (2014)
18. Brakerski, Z., Döttling, N., Garg, S., Malavolta, G.: Candidate iO from homomorphic encryption schemes. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part I. LNCS, vol. 12105, pp. 79–109. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45721-1_4
19. Brakerski, Z., Gentry, C., Halevi, S., Lepoint, T., Sahai, A., Tibouchi, M.: Cryptanalysis of the quadratic zero-testing of GGH. Cryptology ePrint Archive, Report 2015/845 (2015), http://eprint.iacr.org/
20. Brakerski, Z., Rothblum, G.N.: Virtual black-box obfuscation for all circuits via generic graded encoding. In: TCC. pp. 1–25 (2014)
21. Brzuska, C., Farshim, P., Mittelbach, A.: Indistinguishability obfuscation and UCEs: The case of computationally unpredictable sources. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 188–205. Springer, Heidelberg (Aug 2014). https://doi.org/10.1007/978-3-662-44371-2_11
22. Canetti, R., Lin, H., Tessaro, S., Vaikuntanathan, V.: Obfuscation of probabilistic circuits and applications. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015, Part II. LNCS, vol. 9015, pp. 468–497. Springer, Heidelberg (Mar 2015). https://doi.org/10.1007/978-3-662-46497-7_19
23. Cheon, J.H., Han, K., Lee, C., Ryu, H., Stehlé, D.: Cryptanalysis of the multilinear map over the integers. In: EUROCRYPT (2015)
24. Cheon, J.H., Lee, C., Ryu, H.: Cryptanalysis of the new clt multilinear maps. Cryptology ePrint Archive, Report 2015/934 (2015), http://eprint.iacr.org/
25. Chung, K.M., Lin, H., Pass, R.: Constant-round concurrent zero-knowledge from indistinguishability obfuscation. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015, Part I. LNCS, vol. 9215, pp. 287–307. Springer, Heidelberg (Aug 2015). https://doi.org/10.1007/978-3-662-47989-6_14
26. Coron, J., Gentry, C., Halevi, S., Lepoint, T., Maji, H.K., Miles, E., Raykova, M., Sahai, A., Tibouchi, M.: Zeroizing without low-level zeroes: New MMAP attacks and their limitations. In: CRYPTO (2015)
27. Coron, J.S., Lepoint, T., Tibouchi, M.: Practical multilinear maps over the integers. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 476–493. Springer, Heidelberg (Aug 2013). https://doi.org/10.1007/978-3-642-40041-4_26
28. Coron, J.S., Lepoint, T., Tibouchi, M.: New multilinear maps over the integers. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015, Part I. LNCS, vol. 9215, pp. 267–286. Springer, Heidelberg (Aug 2015). https://doi.org/10.1007/978-3-662-47989-6_13
29. Devadas, L., Quach, W., Vaikuntanathan, V., Wee, H., Wichs, D.: Succinct LWE sampling, random polynomials, and obfuscation. pp. 256–287. LNCS, Springer, Heidelberg (2021). https://doi.org/10.1007/978-3-030-90453-1_9
30. Döttling, N., Garg, S., Gupta, D., Miao, P., Mukherjee, P.: Obfuscation from low noise multilinear maps. IACR Cryptology ePrint Archive **2016**, 599 (2016)

31. Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 1–17. Springer, Heidelberg (May 2013). https://doi.org/10.1007/978-3-642-38348-9_1
32. Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., Waters, B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: 54th FOCS. pp. 40–49. IEEE Computer Society Press (Oct 2013). https://doi.org/10.1109/FOCS.2013.13
33. Gay, R., Pass, R.: Indistinguishability obfuscation from circular security. pp. 736–749. ACM Press (2021). https://doi.org/10.1145/3406325.3451070
34. Gentry, C., Gorbunov, S., Halevi, S.: Graph-induced multilinear maps from lattices. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015, Part II. LNCS, vol. 9015, pp. 498–527. Springer, Heidelberg (Mar 2015). https://doi.org/10.1007/978-3-662-46497-7_20
35. Gentry, C., Jutla, C.S., Kane, D.: Obfuscation using tensor products. Electronic Colloquium on Computational Complexity (ECCC) **25**, 149 (2018)
36. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 75–92. Springer, Heidelberg (Aug 2013). https://doi.org/10.1007/978-3-642-40041-4_5
37. Goldreich, O.: Candidate one-way functions based on expander graphs. IACR Cryptol. ePrint Arch. **2000**, 63 (2000)
38. Goldwasser, S., Gordon, S.D., Goyal, V., Jain, A., Katz, J., Liu, F.H., Sahai, A., Shi, E., Zhou, H.S.: Multi-input functional encryption. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 578–602. Springer, Heidelberg (May 2014). https://doi.org/10.1007/978-3-642-55220-5_32
39. Halevi, S.: Graded encoding, variations on a scheme. IACR Cryptology ePrint Archive **2015**, 866 (2015)
40. Hopkins, S.B., Jain, A., Lin, H.: Counterexamples to new circular security assumptions underlying iO. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part II. LNCS, vol. 12826, pp. 673–700. Springer, Heidelberg, Virtual Event (Aug 2021). https://doi.org/10.1007/978-3-030-84245-1_23
41. Hu, Y., Jia, H.: Cryptanalysis of GGH map. IACR Cryptology ePrint Archive **2015**, 301 (2015)
42. Ishai, Y., Prabhakaran, M., Sahai, A.: Secure arithmetic computation with no honest majority. In: Theory of Cryptography Conference. pp. 294–314. Springer (2009)
43. Jain, A., Lin, H., Matt, C., Sahai, A.: How to leverage hardness of constant-degree expanding polynomials overa $\mathbb{R}$ to build $i\mathcal{O}$. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part I. LNCS, vol. 11476, pp. 251–281. Springer, Heidelberg (May 2019). https://doi.org/10.1007/978-3-030-17653-2_9
44. Jain, A., Lin, H., Sahai, A.: Indistinguishability obfuscation from well-founded assumptions. pp. 60–73. ACM Press (2021). https://doi.org/10.1145/3406325.3451093
45. Jain, A., Lin, H., Sahai, A.: Indistinguishability obfuscation from LPN over $\mathbb{F}_p$, dlin, and prgs in $\mathsf{nc}^0$. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13275, pp. 670–699. Springer (2022). https://doi.org/10.1007/978-3-031-06944-4_23, https://doi.org/10.1007/978-3-031-06944-4_23

46. Khurana, D., Rao, V., Sahai, A.: Multi-party key exchange for unbounded parties from indistinguishability obfuscation. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I. LNCS, vol. 9452, pp. 52–75. Springer, Heidelberg (Nov / Dec 2015). https://doi.org/10.1007/978-3-662-48797-6_3

47. Lin, H.: Indistinguishability obfuscation from constant-degree graded encoding schemes. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part I. LNCS, vol. 9665, pp. 28–57. Springer, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49890-3_2

48. Lin, H.: Indistinguishability obfuscation from SXDH on 5-linear maps and locality-5 PRGs. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part I. LNCS, vol. 10401, pp. 599–629. Springer, Heidelberg (Aug 2017). https://doi.org/10.1007/978-3-319-63688-7_20

49. Lin, H., Pass, R., Seth, K., Telang, S.: Indistinguishability obfuscation with non-trivial efficiency. In: Cheng, C.M., Chung, K.M., Persiano, G., Yang, B.Y. (eds.) PKC 2016, Part II. LNCS, vol. 9615, pp. 447–462. Springer, Heidelberg (Mar 2016). https://doi.org/10.1007/978-3-662-49387-8_17

50. Lin, H., Tessaro, S.: Indistinguishability obfuscation from trilinear maps and block-wise local PRGs. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part I. LNCS, vol. 10401, pp. 630–660. Springer, Heidelberg (Aug 2017). https://doi.org/10.1007/978-3-319-63688-7_21

51. Lombardi, A., Vaikuntanathan, V.: Limits on the locality of pseudorandom generators and applications to indistinguishability obfuscation. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017, Part I. LNCS, vol. 10677, pp. 119–137. Springer, Heidelberg (Nov 2017). https://doi.org/10.1007/978-3-319-70500-2_5

52. Micciancio, D., Peikert, C.: Hardness of SIS and LWE with small parameters. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 21–39. Springer, Heidelberg (Aug 2013). https://doi.org/10.1007/978-3-642-40041-4_2

53. Miles, E., Sahai, A., Zhandry, M.: Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over GGH13. In: Advances in Cryptology - CRYPTO (2016)

54. Minaud, B., Fouque, P.A.: Cryptanalysis of the new multilinear map over the integers. Cryptology ePrint Archive, Report 2015/941 (2015), http://eprint.iacr.org/

55. Sahai, A., Waters, B.: How to use indistinguishability obfuscation: deniable encryption, and more. In: Shmoys, D.B. (ed.) 46th ACM STOC. pp. 475–484. ACM Press (May / Jun 2014). https://doi.org/10.1145/2591796.2591825

56. Wee, H., Wichs, D.: Candidate obfuscation via oblivious LWE sampling. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part III. LNCS, vol. 12698, pp. 127–156. Springer, Heidelberg (Oct 2021). https://doi.org/10.1007/978-3-030-77883-5_5

# 4 Supplementary Materials

## 4.1 Recovery of a unique $\mathbf{V_1}$

Having recovered matrices $\mathbf{U}_1 = \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_1\end{bmatrix} = \mathbf{A}_1\mathbf{A}_{1,T}^{-1}, \ldots, \mathbf{U}_d = \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_d\end{bmatrix} = \mathbf{A}_d\mathbf{A}_{d,T}^{-1}$, we now aim to recover a secret matrix up to uniqueness $\mathbf{V}_1 = \mathbf{A}_{1,T} \cdot \mathbf{S}_1$ such that $\mathbf{B}_1 = \mathbf{U}_1 \cdot \mathbf{V}_1 + \mathbf{E}_1$ where $\mathbf{E}_1$ is a low-norm error matrix. We argue correctness for this procedure for $b = 0$. We reason about the case $b = 1$ in Section 3.1.

Observe that when $b = 0$, the algorithm can compute the matrix $\mathbf{Y} = \mathbf{A}^*(\mathbf{S}^* + \mathbf{R}G^{-1}(\hat{\mathbf{B}}))$ from its inputs and then it can annihilate the term $\mathbf{R}G^{-1}(\hat{\mathbf{B}})$ by computing a full rank matrix $\mathbf{Q} \in \mathbb{Z}_q^{K \times (K - M \log q)}$ from the right nullspace of $G^{-1}(\hat{\mathbf{B}})$. Now we have,

$$\mathbf{A}^* \cdot \mathbf{S}^* \cdot \mathbf{Q} = \mathbf{Y} \cdot \mathbf{Q}$$

By definition of the scheme,

$$\mathbf{A}^* \cdot \mathbf{S}^* = \bar{\mathbf{A}}^* \cdot \bar{\mathbf{S}}^*,$$

where,

$$\bar{\mathbf{A}}^* = \mathbf{P}(\mathbf{A_1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{A}_d),$$
$$\bar{\mathbf{S}}^* = \begin{pmatrix} \mathbf{S}_1 \otimes \mathbf{B}_2 \otimes \mathbf{B}_3 \otimes \ldots \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \mathbf{E}_1 \otimes \mathbf{S}_2 \otimes \mathbf{B}_3 \otimes \ldots \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \vdots \\ \mathbf{E}_1 \otimes \mathbf{E}_2 \otimes \mathbf{E}_3 \otimes \ldots \mathbf{E}_{d-1} \otimes \mathbf{S}_d \end{pmatrix} \cdot \mathbf{P}'$$

Thus, due to the properties of tensor products:

$$\mathbf{A}^* \cdot \mathbf{S}^* = \mathbf{L}_1 \cdot \mathbf{L}_2,$$

where,

$$\mathbf{L}_1 = \mathbf{P}(\mathbf{A}_1 \cdot \mathbf{A}_{1,T}^{-1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{A}_d \cdot \mathbf{A}_{d,T}^{-1}),$$
$$\mathbf{L}_2 = \begin{pmatrix} \mathbf{A}_{1,T} \cdot \mathbf{S}_1 \otimes \mathbf{B}_2 \otimes \mathbf{B}_3 \otimes \ldots \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \mathbf{E}_1 \otimes \mathbf{A}_{2,T}\mathbf{S}_2 \otimes \mathbf{B}_3 \otimes \ldots \mathbf{B}_{d-1} \otimes \mathbf{B}_d \\ \vdots \\ \mathbf{E}_1 \otimes \mathbf{E}_2 \otimes \mathbf{E}_3 \otimes \ldots \mathbf{E}_{d-1} \otimes \mathbf{A}_{d,T}\mathbf{S}_d \end{pmatrix} \cdot \mathbf{P}'$$

Therefore, there is a solution to the equation

$$\underbrace{\mathbf{P}(\mathbf{U_1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{U}_d)}_{\text{defined to be } \mathbf{M}} \cdot \begin{bmatrix} \mathbf{V}_1 \otimes \mathbf{B}_2 \otimes \cdots \otimes \mathbf{B}_d \\ \mathbf{Z} \end{bmatrix} \mathbf{P}'\mathbf{Q} = \mathbf{Y}\mathbf{Q} \tag{11}$$

Where everything is known except the variables $\mathbf{V}_1$ and $\mathbf{Z}$ and $\mathbf{M}$ is a known quantity obtained from the previous step of recovering $\tilde{\mathbf{A}}_i$'s. Essentially, what we show is that when seen as equation over just $\mathbf{V}_1$, the equations are actually uniquely solvable. There may be many solutions to $\mathbf{Z}$ but this is irrelevant to solving for $\mathbf{V}_1$.

For $b = 1$, observe that we will be solving

$$\underbrace{\mathbf{P}(\mathbf{U_1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{U}_d)}_{\text{defined to be } \mathbf{M}} \cdot \begin{bmatrix} \mathbf{V}_1 \otimes \mathbf{B}_2 \otimes \cdots \otimes \mathbf{B}_d \\ \mathbf{Z} \end{bmatrix} \mathbf{P}'\mathbf{Q} = \mathbf{Y}\mathbf{Q} \tag{12}$$

where $\mathbf{YQ} = (\mathbf{L}_1\mathbf{L}_2 - \mathbf{S}'_0)\mathbf{Q}$ where $\mathbf{S}'_0 = \mathbf{K}\mathbf{S}_0$ for a Kilian matrix $\mathbf{K}$. If $\mathbf{S}'_0$ was completely random and independent of everything else, then, we won't be able to recover $\mathbf{A}_{1,T}\mathbf{S}_1$ because $\mathbf{S}'_0$ will completely hide any information about $\mathbf{A}_{1,T}\mathbf{S}_1$. However, $\mathbf{S}'_0$ is correlated with $\mathbf{Q}$ and therefore we give a heuristic reason why the recovery will fail when $b = 1$, thereby giving a distinguisher.

The above approach explains how to setup a system of equations in the unknowns $\mathbf{V}_1$ and $\mathbf{Z}$ and it remains to explain why solving this system will give you a unique solution for $\mathbf{V}_1$.

To show uniqueness, we consider the following homogeneous equation and show that the only solution is $\mathbf{V}'_1 = \mathbf{0}$ (we treat $\mathbf{V}'_1, \mathbf{Z}'$ as the variables for the homogeneous equation).

$$\mathbf{P}(\mathbf{U_1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{U}_d) \cdot \begin{bmatrix} \mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)} \\ \mathbf{Z} \end{bmatrix} \mathbf{P}'\mathbf{Q} = 0$$

where $\mathbf{B}^{(2,\ldots,d)} = \mathbf{B}_2 \otimes \cdots \otimes \mathbf{B}_d$. We proceed in three steps. In any proofs corresponding to these three steps, we'll assume that the equations were setup with $\mathbf{B}_2, \ldots, \mathbf{B}_d, \hat{\mathbf{B}}$ are sampled uniform randomly as opposed to LWE matrices. If multiple solutions for this homogeneous equation exist when they are LWE matrices, then we have a distinguisher between LWE matrices and random matrices because the homogeneous equation does not require any secret information.

- **Step 1:** First, we expand the above equation.

  $$\mathbf{M}_1 \cdot \mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)} \cdot \mathbf{P}' \cdot \mathbf{Q} + \mathbf{M}_2 \cdot \mathbf{Z}' \cdot \mathbf{P}' \cdot \mathbf{Q} = \mathbf{0}$$

  where $\mathbf{M}_1 = \mathbf{P} \cdot (\mathbf{U}_1 \otimes \mathbf{I}^{\otimes(d-1)})$ and $\mathbf{M}_2 = \mathbf{P} \cdot (\mathbf{I} \otimes \mathbf{U}_2 \otimes \mathbf{I}^{\otimes(d-2)} \| \cdots \| \otimes \mathbf{I}^{\otimes(d-1)} \otimes \mathbf{U}_d)$.
- **Step 2:** In the second step, find $\mathbf{\Gamma}_2$ as linearly independent columns of $\mathbf{M}_2$ that span its column space. Then find additional linearly independent vectors from from columns of $\mathbf{M}_1$ so that $\left[\mathbf{\Gamma}_1 \| \mathbf{\Gamma}_2\right]$ have full column rank and generate the column space of $\left[\mathbf{M}_1 \| \mathbf{M}_2\right]$. Observe that, by Lemma 6, $\mathbf{\Gamma}_1$ will have at least $w(m-w)^{d-1}$ columns. Moreover, by the properties of column spans (see Lemma 1), we can write $\mathbf{M}_1 = \mathbf{\Gamma}_1\mathbf{X}_1 + \mathbf{\Gamma}_2\mathbf{X}_2$ and $\mathbf{M}_2 = \mathbf{\Gamma}_2\mathbf{X}_3$ for

some $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3$. In particular, the matrix $\mathbf{X}_1$ will be a permutation matrix that simply selects, or places, the columns of $\mathbf{\Gamma}_1$ into the their corresponding column in $\mathbf{M}_1$. Our equation becomes:

$$\mathbf{\Gamma}_1(\mathbf{X}_1 \cdot (\mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)}) \cdot \mathbf{P'} \cdot \mathbf{Q}) + \mathbf{\Gamma}_2(\mathbf{X}_2 \cdot (\mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)}) + \mathbf{X}_3 \cdot \mathbf{Z}')\mathbf{P'}\mathbf{Q} = \mathbf{0}$$

Now we use the linear independence of $\mathbf{\Gamma}_1$ and $\mathbf{\Gamma}_2$ to see that each of the terms must be equal to $\mathbf{0}$. Therefore,

$$\mathbf{X}_1 \cdot (\mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)}) \cdot \mathbf{P'} \cdot \mathbf{Q} = \mathbf{0}.$$

The first and second steps hold with high probability over the choice of $\mathbf{P}, \mathbf{A}_1, \ldots, \mathbf{A}_d$. Notably, they do not depend on $\mathbf{P'}$ nor $\mathbf{Q}$.

– **Step 3:** Our main theorem is that, with high probability over a random choice of $\mathbf{P'}, \mathbf{B}_2, \ldots, \mathbf{B}_d, \hat{\mathbf{B}}$, $\mathbf{V}'_1$ must be $\mathbf{0}$. If $\mathbf{V}'_1 \neq \mathbf{0}$ and satisfies the equation, then this implies $\mathbf{X}_1$ has a nullspace of dimension at least $O(m^{d-1})$. Namely, all columns of $\mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)} \cdot \mathbf{P'} \cdot \mathbf{Q}$ are in the nullspace, and this matrix has column rank $O(m^{d-1})$ when $\mathbf{V}'_1 \neq \mathbf{0}$. On the other hand, we know that $\mathbf{X}_1 \in \mathbb{Z}_q^{w(m-w)^{d-1} \times wm^{d-1}}$ from step 2 is of rank $w(m-w)^{d-1}$. This rank is due to the fact that if a given column $\gamma_i$ of $\mathbf{\Gamma}_1$ appears as $i$th column of $\mathbf{M}_1$ then it also appears as the $i^{th}$ column in $\mathbf{\Gamma}_1\mathbf{X}_1$, therefore $\mathbf{X}_1$ is a permutation matrix of rank $w(m-w)^{d-1}$ because $\mathbf{\Gamma}_1$ is of rank $w(m-w)^{d-1}$, ensuring that the rank of $\mathbf{X}_1$ is at least this much. We know the rank of $\mathbf{\Gamma}_1$ because Lemma 6 tells us there are $w(m-w)^{d-1}$ many such columns not in the column span of $\mathbf{M}_2$ with overwhelming probability over the choice of $\mathbf{P}, \mathbf{A}_1, \ldots, \mathbf{A}_d$.
Therefore, the right nullity of $\mathbf{X}_1$ is at most $wm^{d-1} - w(m-w)^{d-1} = O(w^2 m^{d-2})$ by rank-nullity. Therefore, the only way that the rank of $\mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)} \cdot \mathbf{P'} \cdot \mathbf{Q}$ can be consistent with the nullity of $\mathbf{X}_1$ is if $m \leq O(w^2)$. This parameter setting is in contrast to that in the paper which asks that $m \geq w^3$. This is what our main theorem attempts to prove.

**Useful Claims and Conjectures** We begin by proving multiple lemmas about rank of certain distributions of matrices in order to obtain a lower bound on the column rank of $\mathbf{V}_1 \otimes \mathbf{B}^{(2,\ldots,d)} \cdot \mathbf{P'} \cdot \mathbf{Q}$.

**Lemma 7.** *For $n, k \in \mathbb{N}$ such that $n \leq k$, a uniform random matrix $\mathbf{R} \in \mathbb{Z}_q^{n \times k}$ has rank at least $r$ with probability:*

$$\Pr_{\mathbf{R}}[\mathrm{rk}(\mathbf{R}) \leq r] \leq \frac{q^{(n+k)r}}{q^{nk}}$$

*Proof.* Note that if a matrix $\mathbf{M}$ has rank $r$ it can be factored also as $\mathbf{M} = \mathbf{M}'_1 \cdot \mathbf{M}'_2$ where $\mathbf{M}'_1 \in \mathbb{Z}_q^{n \times \ell}, \mathbf{M}'_2 \in \mathbb{Z}_q^{\ell \times k}$ for any $\ell \geq r$. Therefore, the number of matrices of rank at most $r$ is loosely bounded by $q^{(n+k)r}$. Then,

$$\Pr_{\mathbf{R}}[\mathrm{rk}(\mathbf{R}) \leq r] \leq \frac{q^{(n+k)r}}{q^{nk}}$$

**Lemma 8.** *For any $n, k \in \mathbb{N}$ such that $n \geq k$, if $\mathbf{M} \in \mathbb{Z}_q^{n \times n}$ is a full rank square matrix and $\mathbf{F} \in \mathbb{Z}_q^{k \times n}$ is a (wide) matrix sampled uniform randomly, then $\mathbf{F} \cdot \mathbf{M}$ is uniform randomly distributed.*

*Proof.* Let $\mathbf{M} \in \mathbb{Z}_q^{n \times n}$ be any full rank square matrix. Observe that for any fixed matrix $\mathbf{Y} \in \mathbb{Z}_q^{k \times n}$, the probability over the choice of $\mathbf{F}$ that $\mathbf{F} \cdot \mathbf{M} = \mathbf{Y}$ is uniform since $\mathbf{M}$ is invertible:

$$\Pr_{\mathbf{F}}[\mathbf{F} \cdot \mathbf{M} = \mathbf{Y}] = \Pr_{\mathbf{F}}\left[\mathbf{F} = \mathbf{Y} \cdot \mathbf{M}^{-1}\right] = q^{-kn}.$$

**Corollary 4.** *For any $n, k, \ell \in \mathbb{N}$ such that $n \geq k$, $n \geq \ell$, if $\mathbf{N} \in \mathbb{Z}_q^{n \times \ell}$ is a full column rank matrix and $\mathbf{F} \in \mathbb{Z}_q^{k \times n}$ is a (wide) matrix sampled uniform randomly, then $\mathbf{F} \cdot \mathbf{N}$ is uniform randomly distributed.*

*Proof.* Let $\mathbf{N} \in \mathbb{Z}_q^{n \times \ell}$ be any full rank column matrix. If $\ell = n$, then Lemma 8 already gives our desired statement. If $\ell < n$, then fix $\mathbf{N'} \in \mathbb{Z}_q^{n \times (n-\ell)}$ to be any matrix such that $\left[\mathbf{N} \| \mathbf{N'}\right]$ is a full rank square matrix (in other words, extend the columns of $\mathbf{N}$ to a basis for $\mathbb{Z}_q^n$). Then for any matrix $\mathbf{Y} \in \mathbb{Z}_q^{k \times \ell}$

$$\begin{aligned}
\Pr_{\mathbf{F}}[\mathbf{F} \cdot \mathbf{N} = \mathbf{Y}] &= \sum_{\mathbf{Y'} \in \mathbb{Z}_q^{k \times (n-\ell)}} \Pr_{\mathbf{F}}\left[\mathbf{F} \cdot \left[\mathbf{N} \| \mathbf{N'}\right] = \left[\mathbf{Y} \| \mathbf{Y'}\right]\right] \\
&= \sum_{\mathbf{Y'} \in \mathbb{Z}_q^{k \times (n-\ell)}} q^{-kn} \qquad \text{(by Lemma 8)} \\
&= q^{-k\ell}
\end{aligned}$$

**Lemma 9.** *Consider a fixed matrix $\mathbf{Q} \in \mathbb{Z}_q^{K \times D}$ be of rank $D = K - M \log q$ and a uniform random matrix $\mathbf{F} \in \mathbb{Z}_q^{m^{d-1} \times K}$ where $M = m^{d-1/2}$, and $K = m^{d+1/2}$. For all constants $c < 1$,*

$$\Pr_{\mathbf{F}}\left[\mathrm{rk}(\mathbf{F} \cdot \mathbf{Q}) \leq c \cdot m^{d-1}\right] < q^{-\Omega(K \cdot m^{d-1})}$$

*Proof.* By Corollary 4, $\mathbf{F} \cdot \mathbf{Q} \in \mathbb{Z}_q^{m^{d-1} \times D}$ is a uniform randomly distributed matrix. By Lemma 7,

$$\Pr_{\mathbf{F}}\left[\mathrm{rk}(\mathbf{F} \cdot \mathbf{Q}) \leq c \cdot m^{d-1}\right] \leq \frac{q^{(m^{d-1}+D)(c \cdot m^{d-1})}}{q^{m^{d-1} \cdot D}} = q^{m^{d-1}(c \cdot m^{d-1} - (1-c)D)} = q^{-\Omega(K \cdot m^{d-1})}.$$

.

**Lemma 10.** [1] *Consider a fixed matrix $\mathbf{Q} \in \mathbb{Z}_q^{K \times D}$ of full rank $D$ where $D = K - M \log q$, $M = m^{d-1/2}$, and $K = m^{d+1/2}$. Then let $\mathbf{F}_i \in \mathbb{Z}_q^{m^{d-1} \times K}$ for $i \in [k]$ denote uniform random matrices. Let $\mathbf{s} \in \mathbb{Z}_q^k$ where $m^3 \leq k \leq m^{2d-7/6}$. Then for all constants $c < 1$ such that*

$$\Pr_{\mathbf{F}_i}\left[\exists \mathbf{s} \neq \mathbf{0} \text{ such that } \mathrm{rk}\left(\left(\sum_{i=1}^{k} s_i \cdot \mathbf{F}_i\right) \cdot \mathbf{Q}\right) \leq c \cdot m^{d-1}\right] < q^{-\Omega(K \cdot m^{d-1})}$$

[1] In Lemma 10, the values of (lowercase) $k$ are specified on page 24 of [29].

*Proof.* For a fixed non-zero $\mathbf{s} \in \mathbb{Z}_q^k$,

$$\Pr_{\{\mathbf{F}_i\}_{i=1}^k}\left[\mathrm{rk}\left(\left(\sum_{i=1}^k s_i \cdot \mathbf{F}_i\right)\cdot \mathbf{Q}\right) \leq cm^{d-1}\right] = \Pr_{\mathbf{F}}\left[\mathrm{rk}\left(\mathbf{F}\cdot\mathbf{Q}\right) \leq cm^{d-1}\right] \leq q^{-\Omega(K\cdot m^{d-1})}$$

where the inequality above is given by Lemma 9. Then there are $q^k$ possible $\mathbf{s}$ so by the union bound,

$$\Pr_{\{\mathbf{F}_i\}_{i=1}^k}\left[\exists \mathbf{s} \neq \mathbf{0} \text{ such that } \mathrm{rk}\left(\left(\sum_{i=1}^k s_i \cdot \mathbf{F}_i\right)\cdot \mathbf{Q}\right) \leq c\cdot m^{d-1}\right] < q^k \cdot q^{-\Omega(K\cdot m^{d-1})} = q^{-\Omega(K\cdot m^{d-1})}$$

*Remark 6.* We require that a uniform matrix $\mathbf{F} \in \mathbb{Z}_q^{m\times k}$ extracts $m$ random field elements from $\chi^k$. A uniform matrix $\mathbf{F}$ is a 2-universal hash function because for a fixed non-zero vector $\mathbf{x}$ the probability over a random choice of $\mathbf{F}$ that $\mathbf{F}\cdot\mathbf{x} = 0$ is exactly $q^{-m}$. To apply the Leftover Hash Lemma and obtain the extraction property, we require that $k\cdot\mathbb{H}_\infty(\chi) \geq m\log q + 2\log(\epsilon^{-1})$ where $\mathbb{H}_\infty(\cdot)$ denotes min-entropy. For a discrete Gaussian, $\mathbb{H}_\infty(\chi)$ is some constant $c$. Therefore, we require that $c\cdot k \geq m\log q + 2\log(\epsilon^{-1})$. Per Remark 1, for the security of LWE to hold we require that $q \leq 2^{O(m)}$, so $\log q = O(m)$. Then since $k \geq m^3$, there exists some $\epsilon$ that is negligible in $k$ such that this condition is satisfied.

**Lemma 11.** *Assume parameters for $m, k, \epsilon, q, \mathbb{H}_\infty(\chi)$ are as stated in Remark 6. Let $\mathbf{F}_i \in \mathbb{Z}_q^{m\times k}$ for $i \in \{1,\ldots,d\}$ be sampled uniformly at random. Define $\mathbf{F}^{(1,\ldots,d)} \triangleq \mathbf{F}_1 \otimes \ldots \otimes \mathbf{F}_d$. Let $\mathbf{P}' \leftarrow \chi^{k^d\times 1}$. Then $\mathbf{F}^{(1,\ldots,d)}\cdot\mathbf{P}'$ is $\left(k^{O(d^2)}\cdot\epsilon\right)$-statistically close to uniform.*

*Proof.* The induction is on the index $d$. In the base case, $d = 1$, we have that $\mathbf{F}_1\cdot\mathbf{P}'$ for $\mathbf{P}' \leftarrow \chi^{k\times 1}$ is $\epsilon$-close to uniform from Remark 6. Assume the statement holds for $d-1$, we show the statement holds for $d$. Let $\mathbf{P}' \leftarrow \chi^{k^d\times 1}$. Split $\mathbf{P}'$ into $k$ blocks of dimension $k^{d-1}\times 1$:

$$\mathbf{P}' = \begin{bmatrix}\mathbf{P}'_1\\ \vdots \\ \mathbf{P}'_k\end{bmatrix}.$$

Observe that

$$\begin{aligned}\mathbf{F}^{(1,\ldots,d)}\cdot\mathbf{P}' &= \begin{bmatrix}\mathbf{F}_1[1,1]\cdot\mathbf{F}^{(2,\ldots,d)} & \cdots & \mathbf{F}_1[1,k]\cdot\mathbf{F}^{(2,\ldots,d)}\\ \vdots & \ddots & \vdots \\ \mathbf{F}_1[m,1]\cdot\mathbf{F}^{(2,\ldots,d)} & \cdots & \mathbf{F}_1[m,k]\cdot\mathbf{F}^{(2,\ldots,d)}\end{bmatrix}\cdot\mathbf{P}'\\ &= \begin{bmatrix}\sum_{j\in[k]}\mathbf{F}_1[1,j]\cdot\mathbf{F}^{(2,\ldots,d)}\cdot\mathbf{P}'_j\\ \vdots \\ \sum_{j\in[k]}\mathbf{F}_1[m,j]\cdot\mathbf{F}^{(2,\ldots,d)}\cdot\mathbf{P}'_j\end{bmatrix}.\end{aligned}$$

where $\mathbf{F}_\ell[i,j]$ denotes the $(i,j)$th entry of $\mathbf{F}_\ell$. Now apply the induction hypothesis on so that for $i \in [k]$, $\{\mathbf{F}^{(2,\ldots,d)} \cdot \mathbf{P}'_i\}_{i\in[k]}$ is $k \cdot \epsilon_{d-1}$ statistically close to $k$ random vectors $\{\mathbf{v}_i\}_{i\in[k]}$ where $\mathbf{v}_i \in \mathbb{Z}_q^{k^{d-1}\times 1}$. Therefore

$$\begin{bmatrix} \sum_{j\in[k]} \mathbf{F}_1[1,j] \cdot \mathbf{F}^{(2,\ldots,d)} \cdot \mathbf{P}'_j \\ \vdots \\ \sum_{j\in[k]} \mathbf{F}_1[m,j] \cdot \mathbf{F}^{(2,\ldots,d)} \cdot \mathbf{P}'_j \end{bmatrix} \approx_{k\cdot\epsilon_{d-1}} \begin{bmatrix} \sum_{j\in[k]} \mathbf{F}_1[1,j] \cdot \mathbf{v}_j \\ \vdots \\ \sum_{j\in[k]} \mathbf{F}_1[m,j] \cdot \mathbf{v}_j \end{bmatrix}.$$

Now observe that the entries of the above matrix are equivalently a rearrangement of the following quantities:

$$\mathbf{F}_1 \cdot \left[\mathbf{v}[1]\ \mathbf{v}[2] \cdots\ \mathbf{v}[k^{d-1}]\right]$$

where for $i \in [k^{d-1}]$, we define the column vector $\mathbf{v}[i] \triangleq (\mathbf{v}_1[i], \ldots, \mathbf{v}_k[i])^\top \in \mathbb{Z}_q^{k\times 1}$. Apply the leftover hash lemma $k^{d-1}$ times to replace every column with a random vector in $\mathbb{Z}_q^m$. This implies a further statistical distance of $k^{d-1}\epsilon$. Therefore we have that $\epsilon_d \le \epsilon_{d-1} \cdot k + k^{d-1}\epsilon = O(k^{d-1} \cdot \epsilon_{d-1})$. Setting $\epsilon_1 = \epsilon$, we have that $\epsilon_d = k^{O(d^2)}\epsilon$.

**Recovering $\mathbf{V_1}$** We now use the above rank lemmas to show that the only solution for $\mathbf{V}'_1$ in the homogeneous equation above is $\mathbf{0}$. This is step 3 in the outline described above.

**Theorem 3.** *Let $\mathbf{X}_1 \in \mathbb{Z}_q^{w(m-w)^{d-1}\times wm^{d-1}}$ be of rank $w(m-w)^{d-1}$. Let $\mathbf{B}_2, \ldots, \mathbf{B}_d$ be uniform randomly sampled from $\mathbb{Z}_q^{m\times k}$. Let $\mathbf{B}^{(2,\ldots,d)} \triangleq \mathbf{B}_2 \otimes \cdots \otimes \mathbf{B}_d$ and let $\mathbf{P}' \leftarrow \chi^{k^{d-1}\times K}$ and let $\mathbf{Q} \in \mathbb{Z}_q^{K\times(K-M\log q)}$ be of full rank $K - M\log q$. Then with probability $1-\mathsf{negl}(w)$ over the choice of $\mathbf{P}'$, $\mathbf{B}_2, \ldots, \mathbf{B}_d$, if $m = \omega(w^2)$ and $\mathbf{X}_1 \cdot (\mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)}) \cdot \mathbf{P}' \cdot \mathbf{Q} = \mathbf{0}$, then $\mathbf{V}'_1 = \mathbf{0}$.*

*Proof.* If $\mathbf{V}'_1$ is non-zero than it has a non-zero row. Suppose WLOG that the first row of $\mathbf{V}'_1$ is some non-zero vector $\mathbf{v}_1 = (v_{1,1}, \ldots, v_{1,k}) \neq \mathbf{0}$. Split

$$\mathbf{P}' = \begin{bmatrix} \mathbf{P}'_1 \\ \vdots \\ \mathbf{P}'_k \end{bmatrix},$$

into $k$ blocks of shape $\mathbf{P}'_i \in \mathbb{Z}_q^{k^{d-1}\times K}$, for $i \in [k]$. Then observe that the top $m^{d-1} \times (K - M\log q)$ block of $(\mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)}) \cdot \mathbf{P}' \cdot \mathbf{Q} \in \mathbb{Z}_q^{wm^{d-1}\times(K-M\log q)}$ is given by

$$\left(\sum_{i=1}^{k} v_{1,i} \cdot \mathbf{B}^{(2,3,\ldots,d)} \cdot \mathbf{P}'_i\right) \cdot \mathbf{Q}$$

where $v_{1,i}$ denotes the $(1,i)$th entry of $\mathbf{V}_1$. Lemma 11 argues that $\mathbf{B}^{(2,3,\ldots,d)}$ extracts a row vector from a single column of $\mathbf{P}'_i$ that is some $\epsilon' = \mathsf{negl}(w)$-statistically close to uniform. Applying Lemma 11 on $K$ columns of $k$ many

fresh $\mathbf{P}'_i$, we have

$$\left(\sum_{i=1}^{k} v_{1,i} \cdot \mathbf{B}^{(2,3,\ldots,d)} \cdot \mathbf{P}'_i\right) \cdot \mathbf{Q} \approx_{\mathsf{stat}, k \cdot K \cdot \epsilon'} \left(\sum_{i=1}^{k} v_{1,i} \cdot \mathbf{F}_i\right) \cdot \mathbf{Q}.$$

where $kK\epsilon'$ remains negligible in $w$. $\mathbf{P}'_i$ having $K$ column Then by Lemma 10,

$$\Pr_{\mathbf{F}_i}\left[\exists \mathbf{v}_1 \neq \mathbf{0} \text{ such that } \mathrm{rk}\left(\left(\sum_{i=1}^{k} v_{1,i} \cdot \mathbf{F}_i\right) \cdot \mathbf{Q}\right) \leq m^{d-1}/2\right] < q^{-\Omega(Km^{d-1})}.$$

Therefore with probability $1 - q^{-\Omega(Km^{d-1})} - kK\epsilon'$ over the choice of $\mathbf{P'}$ and $\mathbf{B}_1, \ldots, \mathbf{B}_d$, $(\mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)}) \cdot \mathbf{P'} \cdot \mathbf{Q}$ is of rank at least $m^{d-1}/2$ since the top $m^{d-1} \times (K - M \log q)$ block already has rank above $m^{d-1}/2$.

On the other hand, the right nullity of $\mathbf{X}_1$ is $wm^{d-1} - w(m-w)^{d-1} = O\left(w^2 m^{d-2}\right)$. This is only possible if $m \leq O(w^2)$. In the parameter regime proposed by [29], $m \geq w^3$.

Note that Theorem 3 is the key ingredient in Step 3.

**Corollary 5 (Uniqueness of $\mathbf{V}_1$).** *Let $d, m, w, k, K, M, q, \chi$ be parameters as defined in Section 2.1. Then the homogeneous system of equations*

$$\mathbf{P}(\mathbf{U_1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{U}_d) \cdot \begin{bmatrix} \mathbf{V}'_1 \otimes \mathbf{B}^{(2,\ldots,d)} \\ \mathbf{Z} \end{bmatrix} \mathbf{P'Q} = 0$$

*has a unique solution $\mathbf{V}'_1 = 0$ with $1 - \mathsf{negl}(w)$ probability over the choice of randomness used in generating the distribution $\mathcal{D}_0$.*

*Proof.* As specified, $m = w^3 = \omega(w^2)$. Setting up the matrix $\mathbf{X}_1 \in \mathbb{Z}_q^{w(m-w)^{d-1} \times wm^{d-1}}$ exactly as specified in Step 2 in Section 4.1, and assuming that the equations were set up with $\mathbf{B}_2, \ldots, \mathbf{B}_d, \hat{\mathbf{B}}$ that are sampled uniform randomly as opposed to being LWE matrices, Theorem 2 implies that there is a unique solution $\mathbf{V}'_1 = 0$ with $1 - \mathsf{negl}(w)$ probability over the choice of randomness used in generating the distribution $\mathcal{D}_0$. If multiple solutions for this homogeneous equation exist when this equation is set up where $\mathbf{B}_2, \ldots, \mathbf{B}_d, \hat{\mathbf{B}}$ as LWE matrices, then we have a distinguisher between LWE matrices and random matrices because setting up the the homogeneous equation does not require any secret information. Therefore, we have the intended statement.

### 4.2 Extending the Attack to the T-sum Candidate

On page 26 of [29], an alternate candidate construction that builds upon the previous candidate is proposed. In particular, this alternate candidate fixes a single set of matrices $\{\mathbf{A}_i\}_{i=1}^d$, and reuses them to build $T$ copies of the original candidate, and sums the $T$ copies. More specifically we have the following candidate:

*Distribution $\mathcal{D}_b$.*

- Let $d, m, w, k, \chi, M, K, q$ be the same parameters as defined in Section 2.1.
- For $i \in [d]$, sample $\mathbf{A}_i \leftarrow \mathbb{Z}_q^{m \times w}$. For $i \in [d], j \in [T]$, sample $\mathbf{S}_i^{(j)} \leftarrow \mathbb{Z}_q^{w \times k}$, $\mathbf{E}_i^{(j)} \leftarrow \chi^{m \times k}$. Compute $\mathbf{B}_i^{(j)} = \mathbf{A}_i \cdot \mathbf{S}_i^{(j)} + \mathbf{E}_i^{(j)} \in \mathbb{Z}_q^{m \times k}$. Visually, the $\mathbf{A}_i$'s are tall, the $\mathbf{S}_i$'s are wide, and the $\mathbf{B}_i$'s and the $\mathbf{E}_i$'s are wide.
- Sample $\mathbf{P} \leftarrow \chi^{M \times m^d}$ and $\mathbf{P'} \leftarrow \chi^{k^d \times K}$. Visually, $\mathbf{P}$ is a wide matrix and $\mathbf{P'}$ is a tall matrix.
- Set $\bar{\mathbf{A}}^* = \mathbf{P} \cdot (\mathbf{A}_1 \otimes \mathbf{I}_m \otimes \ldots \mathbf{I}_m \| \mathbf{I}_m \otimes \mathbf{A}_2 \otimes \ldots \mathbf{I}_m \| \ldots \| \mathbf{I}_m \otimes \mathbf{I}_m \otimes \ldots \mathbf{A}_d) \in Z_q^{M \times dwm^{d-1}}$. Visually, $\bar{\mathbf{A}}^*$ is a tall matrix.
- For $j \in [T]$, set $\bar{\mathbf{S}}^{*^{(j)}} = \begin{pmatrix} \mathbf{S}_1^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \mathbf{B}_3^{(j)} \otimes \ldots \mathbf{B}_{d-1}^{(j)} \otimes \mathbf{B}_d^{(j)} \\ \mathbf{E}_1^{(j)} \otimes \mathbf{S}_2^{(j)} \otimes \mathbf{B}_3^{(j)} \otimes \ldots \mathbf{B}_{d-1}^{(j)} \otimes \mathbf{B}_d^{(j)} \\ \vdots \\ \mathbf{E}_1^{(j)} \otimes \mathbf{E}_2^{(j)} \otimes \mathbf{E}_3^{(j)} \otimes \ldots \mathbf{E}_{d-1}^{(j)} \otimes \mathbf{S}_d^{(j)} \end{pmatrix} \cdot \mathbf{P'} \in \mathbb{Z}_q^{dwm^{d-1} \times K}$. Then set
$$\bar{\mathbf{S}}^* = \sum_{j=1}^{T} \bar{\mathbf{S}}^{*^{(j)}} \cdot \mathbf{P'}.$$
Visually, $\bar{\mathbf{S}}^*$ is a wide matrix.
- (Killian Randomization) Find random full rank matrices $\mathbf{A}^* \in \mathbb{Z}_q^{M \times W}, \mathbf{S}^* \in \mathbb{Z}_q^{W \times K}$ such that $\mathbf{A}^* \cdot \mathbf{S}^* = \bar{\mathbf{A}}^* \cdot \bar{\mathbf{S}}^*$. Visually, $\mathbf{A}^*$ is a tall matrix and $\mathbf{S}^*$ is a wide matrix.
- Set $\mathbf{B}^* = \mathbf{P} \cdot (\sum_{j=1}^{T} \mathbf{B}_1^{(j)} \otimes \ldots \otimes \mathbf{B}_d^{(j)}) \cdot \mathbf{P'}$ and $\mathbf{E}^* = \mathbf{P} \cdot (\sum_{j=1}^{T} \mathbf{E}_1^{(j)} \otimes \ldots \otimes \mathbf{E}_d^{(j)}) \cdot \mathbf{P'}$, so that $\mathbf{B}^* - \mathbf{A}^*\mathbf{S}^* = \mathbf{E}^*$. Set $\mathsf{seed} = \{\mathbf{B}_i^{(j)}\}_{i \in [d], j \in [T]}, \mathbf{A}^*, \mathbf{S}^*$.
- Set $\hat{\mathbf{B}} = \mathbf{A}^*\mathbf{S}_0 + \mathbf{F}$, where $\mathbf{S}_0 \leftarrow \mathbb{Z}_q^{W \times K}$ and $\mathbf{F} \leftarrow \chi_{\mathsf{flood}}^{M \times K}$.
- Set $\mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - b\mathbf{G}$, where $\mathbf{R} \leftarrow \mathbb{Z}_q^{W \times M \log q}$ and $\mathbf{E} \leftarrow \bar{\chi}^{M \times M \log q}$.

The output of $\mathcal{D}_b$ consists of the following tuple:

$$\Delta_b = (\mathbf{P}, \mathbf{P'}, \mathbf{A}^*, \{\mathbf{B}_i^{(j)}\}_{i \in [d], j \in [T]}, \hat{\mathbf{B}}, \mathbf{C}, \mathbf{E}^* + \mathbf{E}\mathbf{G}^{-1}(\hat{\mathbf{B}}) - b\mathbf{F})$$

*Remark 7.* Note that the number of field elements in the seed is $T \cdot m \cdot k$. This seed is expanded to $M \cdot K$ elements by the tensor construction above. Per the parameters proposed in [29], we have $M \cdot K = m^{2d}$. Therefore if $T < m^{2d-1}/k$, then there is sufficient expansion to be useful for construction $i\mathcal{O}$.

### 4.3 Extending the attack

We show that our attack on the original candidate directly extends to all interesting settings of $T$ that imply $i\mathcal{O}$ under a reasonable assumption about the randomness of certain matrix distributions. Namely, we will show that for all the same algorithm extends to the $T$-sum case for $T = O(m^{2d-(1/2)} \cdot w/k)$.

Our attack proceeds in the same main overall steps as the original $T = 1$ case. We detail the algorithm in two steps below.

– **Step 1:** Exactly as before, the algorithm recovers matrices $\mathbf{A}_1, \ldots, \mathbf{A}_d$ up to unique representation $\mathbf{U}_1 = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_1 \end{bmatrix} = \mathbf{A}_1 \cdot \mathbf{A}_{1,T}^{-1}, \ldots \mathbf{U}_1 = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_1 \end{bmatrix} = \mathbf{A}_d \cdot \mathbf{A}_{d,T}^{-1}$ where $\mathbf{U}_i \in \mathbb{Z}_q^{m \times w}$ for $i \in [d]$.
– **Step 2:** Having recovered $\mathbf{U}_1, \ldots, \mathbf{U}_d$, the algorithm now aims to recover the secrets up to unique representation $\{\mathbf{V}_1^{(j)} = \mathbf{A}_{1,T} \cdot \mathbf{S}_1^{(j)}\}_{j \in [T]}$ where $\mathbf{V}_i^{(j)} \in \mathbb{Z}_q^{w \times k}$ for $j \in [T], i \in [d]$.

The algorithm now sets up a system of equations to solve for $\{\mathbf{V}_1^{(j)}\}_{j \in [T]}$. As in the original setting, an algorithm given the inputs from the distribution $\mathcal{D}_b$ can compute the matrix $\mathbf{Y} = \mathbf{A}^*(\mathbf{S}^* + \mathbf{R} \cdot G^{-1}(\hat{\mathbf{B}}) - b \cdot \mathbf{S}_0) \in \mathbb{Z}_q^{M \times K}$. An algorithm can then annihilate the term $\mathbf{R} \cdot G^{-1}(\hat{\mathbf{B}}) \in \mathbb{Z}_q^{W \times K}$ by computing a full column rank matrix $\mathbf{Q} \in \mathbb{Z}_q^{K \times (K - M \log q)}$ from its right nullspace. Now we have,

$$\mathbf{A}^*(\mathbf{S}^* - b \cdot \mathbf{S}_0) \cdot \mathbf{Q} = \mathbf{Y} \cdot \mathbf{Q}.$$

As in the original setting, when $b = 1$, the matrix $\mathbf{S}_0$ heuristically hides information about $\mathbf{A}_{1,T} \cdot \mathbf{S}_1^{(j)}$ for all $j \in [T]$ so no recovery is possible of these matrices. We refer the reader to Section 4.1 for a longer discussion about the case where $b = 1$.
From now on we focus on the case where $b = 0$ so that

$$\mathbf{A}^* \cdot \mathbf{S}^* \cdot \mathbf{Q} = \mathbf{Y} \cdot \mathbf{Q}.$$

By the definition of the $T$-sum scheme and properties of the tensor product we have,

$$\mathbf{A}^* \cdot \mathbf{S}^* = \bar{\mathbf{A}}^* \cdot \bar{\mathbf{S}}^* = \mathbf{L}_1 \cdot \mathbf{L}_2$$

where

$$\mathbf{L}_1 = \mathbf{P}(\mathbf{A}_1 \cdot \mathbf{A}_{1,T}^{-1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{A}_d \cdot \mathbf{A}_{d,T}^{-1}),$$

$$\mathbf{L}_2 = \begin{pmatrix} \sum_{j \in [T]} \left( \mathbf{A}_{1,T} \cdot \mathbf{S}_1^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \mathbf{B}_3^{(j)} \otimes \ldots \mathbf{B}_{d-1}^{(j)} \otimes \mathbf{B}_d^{(j)} \right) \\ \sum_{j \in [T]} \left( \mathbf{E}_1^{(j)} \otimes \mathbf{A}_{2,T} \cdot \mathbf{S}_2^{(j)} \otimes \mathbf{B}_3^{(j)} \otimes \ldots \mathbf{B}_{d-1}^{(j)} \otimes \mathbf{B}_d^{(j)} \right) \\ \vdots \\ \sum_{j \in [T]} \left( \mathbf{E}_1^{(j)} \otimes \mathbf{E}_2^{(j)} \otimes \mathbf{E}_3^{(j)} \otimes \ldots \mathbf{E}_{d-1}^{(j)} \otimes \mathbf{A}_{d,T} \cdot \mathbf{S}_d^{(j)} \right) \end{pmatrix} \cdot \mathbf{P}'.$$

Therefore, when $b = 0$, there is a solution to the equation

$$\underbrace{\mathbf{P}(\mathbf{U_1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{U}_d)}_{\text{defined to be } \mathbf{M}} \cdot \begin{bmatrix} \sum_{j \in [T]} \left( \mathbf{V}_1^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)} \right) \\ \mathbf{Z} \end{bmatrix} \mathbf{P}'\mathbf{Q} = \mathbf{Y}\mathbf{Q}$$

where all values are known except for the variables $\{\mathbf{V}_1^{(j)}\}_{j \in [T]}$ and $\mathbf{Z}$. Here $\mathbf{M}$ is a known quantity computed in Step 1. We show that when this equation is viewed as an equation over just the variables $\{\mathbf{V}_1^{(j)}\}_{j \in [T]}$, the equation is uniquely solvable. Again, there may be many solutions to $\mathbf{Z}$, but this will be irrelevant to solving for $\{\mathbf{V}_1^{(j)}\}_{j \in [T]}$.

*Arguing uniqueness* At this point, the overall algorithm has not changed at all. Having set up a linear system of equations in the variables $\{\mathbf{V}_1^{(j)}\}_{j\in[T]}$ and $\mathbf{Z}$, and having observed there is at least one solution, it remains to argue that with high probability over the choice of matrices $\mathbf{P}, \mathbf{P}', \{\mathbf{B}_i^{(j)}\}_{j\in[T],i\in[d]}, \hat{\mathbf{B}}$ that there is a unique solution to the variables $\{\mathbf{V}_1^{(j)}\}_{j\in[T]}$. To argue uniqueness, we again consider the homogeneous equation where the unknowns are denoted $\{\mathbf{V}_1'^{(j)}\}_{j\in[T]}$ and $\mathbf{Z}'$ and need to show that $\mathbf{V}_1'^{(j)} = 0$ for $j \in [T]$.

$$\underbrace{\mathbf{P}(\mathbf{U_1} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I} | \ldots | \mathbf{I} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{U}_d)}_{\text{defined to be } \mathbf{M}} \cdot \begin{bmatrix} \sum_{j\in[T]} \left(\mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)}\right) \\ \mathbf{Z}' \end{bmatrix} \mathbf{P}'\mathbf{Q} = \mathbf{0}$$

This overall argument is effectively identical except for a single step that differs from the original $T = 1$ case. We outline these steps in detail for analyzing the attack on the $T$-sum candidate analogously to what has been outlined for the original setting.

- **Step 1 (for uniqueness):** As done in the original setting, expand the above equation to obtain:

$$\mathbf{M}_1 \cdot \sum_{j\in[T]} \left(\mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)}\right) \cdot \mathbf{P}'\mathbf{Q} + \mathbf{M}_2\mathbf{Z}'\mathbf{P}'\mathbf{Q} = 0$$

  where $\mathbf{M}_1 = \mathbf{P} \cdot (\mathbf{U}_1 \otimes \mathbf{I}^{\otimes(d-1)})$ and $\mathbf{M}_2 = \mathbf{P} \cdot (\mathbf{I} \otimes \mathbf{U}_2 \otimes \mathbf{I}^{\otimes(d-2)} \| \cdots \| \otimes \mathbf{I}^{\otimes(d-1)} \otimes \mathbf{U}_d)$.
- **Step 2 (for uniqueness):** The second step here is identical to that in the uniqueness analysis for the attack on the original scheme. In the second step, set $\mathbf{\Gamma}_2$ as linearly independent columns of $\mathbf{M}_2$ that span its column space. Then set $\mathbf{\Gamma}_1$ as additional linearly independent columns of $\mathbf{M}_1$ so that $\left[\mathbf{\Gamma}_1 \| \mathbf{\Gamma}_2\right]$ has full column rank and generate the column space of $\mathbf{M}$. Observe that $\mathbf{\Gamma}_1$ will have at least $w(m-w)^{d-1}$ columns by Lemma 6 which allows us to compute

$$\dim\left(\text{Colspan}(\left[\mathbf{M}_1 \| \mathbf{M}_2\right])\right) - \dim\left(\text{Colspan}(\mathbf{M}_2)\right) + \dim\left(\text{Colspan}(\mathbf{M}_1) \cap \text{Colspan}(\mathbf{M}_2)\right) = w(m-w)^{d-1}.$$

  As a consequence, we can write this equation as $\mathbf{M}_1 = \mathbf{\Gamma}_1\mathbf{X}_1 + \mathbf{\Gamma}_2\mathbf{X}_2$ and $\mathbf{M}_2 = \mathbf{\Gamma}_2\mathbf{X}_3$ for some $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3$. Our equation becomes:

$$\mathbf{\Gamma}_1 \left(\mathbf{X}_1 \cdot \sum_{j\in[T]} \left(\mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)}\right) \cdot \mathbf{P}' \cdot \mathbf{Q}\right) + \mathbf{\Gamma}_2 \left(\mathbf{X}_2 \cdot \left(\sum_{j\in[T]} \left(\mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)}\right)\right) + \mathbf{X}_3 \cdot \mathbf{Z}'\right) \mathbf{P}'\mathbf{Q} = \mathbf{0}$$

  Now we use the linear independence of $\mathbf{\Gamma}_1$ and $\mathbf{\Gamma}_2$ to see that each of the terms must be equal to $\mathbf{0}$. Therefore,

$$\mathbf{X}_1 \cdot \sum_{j\in[T]} \left(\mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)}\right) \cdot \mathbf{P}' \cdot \mathbf{Q} = 0. \qquad (***)$$

The first and second steps hold with high probability over the choice of $\mathbf{P}, \mathbf{A}_1, \ldots, \mathbf{A}_d$. Notably, they do not depend on $\mathbf{P}'$ nor $\mathbf{Q}$.

– **Step 3 (for uniqueness):** Our main theorem is that, with high probability over a random choice of $\mathbf{P}', \mathbf{B}_2, \ldots, \mathbf{B}_d, \hat{\mathbf{B}}$, the matrices $\mathbf{V}_1'^{(j)} = \mathbf{0}$ for $j \in [T]$, if there exists any $j \in [T]$ such that $\mathbf{V}_1'^{(j)} \neq \mathbf{0}$, then $\sum_{j\in[T]} \left(\mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)}\right) \cdot \mathbf{P}' \cdot \mathbf{Q}$ is of rank $O(m^{d-1})$.
Namely, all columns of $\mathbf{V}_1' \otimes \mathbf{B}^{(2,\ldots,d)} \cdot \mathbf{P}' \cdot \mathbf{Q}$ has column rank $O(m^{d-1})$ when $\mathbf{V}_1' \neq \mathbf{0}$ and are in the nullspace of $\mathbf{X}_1$. On the other hand, we know that $\mathbf{X}_1 \in \mathbb{Z}_q^{w(m-w)^{d-1} \times wm^{d-1}}$ from step 2 is of rank at least $w(m-w)^{d-1}$. This rank is due to the fact that if a given column $\gamma_i$ of $\mathbf{\Gamma}_1$ appears as $i^{th}$ column of $\mathbf{M}_1$ then it also appears as the $i^{th}$ column in $\mathbf{\Gamma}_1\mathbf{X}_1$, therefore $\mathbf{X}_1$ is a permutation sub-matrix of rank $w(m-w)^{d-1}$ because $\mathbf{\Gamma}_1$ is of rank $w(m-w)^{d-1}$, ensuring that the rank of $\mathbf{X}_1$ is at least this much. We know the rank of $\mathbf{\Gamma}_1$ because Lemma 6 tell us there are $w(m-w)^{d-1}$ many columns of $\mathbf{M}_1$ not in the column span of $\mathbf{M}_2$ with overwhelming probability over the choice of $\mathbf{P}, \mathbf{A}_1, \ldots, \mathbf{A}_d$.
Therefore, the right nullity of $\mathbf{X}_1$ is at most $wm^{d-1} - w(m-w)^{d-1} = O(w^2 m^{d-2})$ by rank-nullity. Therefore, the only way that the rank of $\sum_{j\in[T]} \left(\mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)}\right) \cdot \mathbf{P}' \cdot \mathbf{Q}$ can be consistent with the nullity of $\mathbf{X}_1$ is if $m \leq O(w^2)$. This parameter setting is in contrast to that in the paper which asks that $m \geq w^3$. This is what our main theorem attempts to prove.

*Preparing a rank computation* In Step 3, we determined that analyzing the rank of

$$\sum_{j\in[T]} \left(\mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)}\right) \cdot \mathbf{P}' \cdot \mathbf{Q}$$

for some non-zero $\mathbf{V}_1'^{(j)}$ for $j \in [T]$ suffices to obtain a uniqueness theorem. To analyze this rank, we will massage the form of this matrix so that the rank is easier to analyze. We now describe how to rewrite this expression.

For convenience, for $j \in [T]$, define

$$\mathbf{B}'^{(j)} \triangleq \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)} \in \mathbb{Z}_q^{m^{d-1} \times k^{d-1}}.$$

1. Rewrite the following expression:

$$\sum_{j=1}^{T} \mathbf{V}_1'^{(j)} \otimes \mathbf{B}'^{(j)} = \left[\mathbf{V}_1'^{(1)} \otimes \mathbf{I}_{m^{d-1}} \| \mathbf{V}_1'^{(2)} \otimes \mathbf{I}_{m^{d-1}} \| \cdots \| \mathbf{V}_1'^{(T)} \otimes \mathbf{I}_{m^{d-1}}\right] \cdot \begin{bmatrix} \mathbf{I}_k \otimes \mathbf{B}'^{(1)} \\ \mathbf{I}_k \otimes \mathbf{B}'^{(2)} \\ \vdots \\ \mathbf{I}_k \otimes \mathbf{B}'^{(T)} \end{bmatrix}$$

$$= \left(\left[\mathbf{V}_1'^{(1)} \| \mathbf{V}_1'^{(2)} \| \cdots \| \mathbf{V}_1'^{(T)}\right] \otimes \mathbf{I}_{m^{d-1}}\right) \cdot \begin{bmatrix} \mathbf{I}_k \otimes \mathbf{B}'^{(1)} \\ \mathbf{I}_k \otimes \mathbf{B}'^{(2)} \\ \vdots \\ \mathbf{I}_k \otimes \mathbf{B}'^{(T)} \end{bmatrix}$$

2. Then open up the tensor structure of $\begin{bmatrix} \mathbf{I}_k \otimes \mathbf{B}'^{(1)} \\ \mathbf{I}_k \otimes \mathbf{B}'^{(2)} \\ \vdots \\ \mathbf{I}_k \otimes \mathbf{B}'^{(T)} \end{bmatrix}$ to see that for $j \in [T]$,

$$\mathbf{I}_k \otimes \mathbf{B}'^{(j)} = \begin{bmatrix} \mathbf{B}'^{(j)} & \mathbf{0}_{m^{d-1} \times k^{d-1}} & \mathbf{0}_{m^{d-1} \times k^{d-1}} & \cdots & \mathbf{0}_{m^{d-1} \times k^{d-1}} \\ \mathbf{0}_{m^{d-1} \times k^{d-1}} & \mathbf{B}'^{(j)} & \mathbf{0}_{m^{d-1} \times k^{d-1}} & \cdots & \mathbf{0}_{m^{d-1} \times k^{d-1}} \\ \vdots & \vdots & \ddots & \vdots & \\ \mathbf{0}_{m^{d-1} \times k^{d-1}} & \mathbf{0}_{m^{d-1} \times k^{d-1}} & \mathbf{0}_{m^{d-1} \times k^{d-1}} & \cdots & \mathbf{B}'^{(j)} \end{bmatrix} \in \mathbb{Z}_q^{km^{d-1} \times k^d}.$$

3. Then partition $\mathbf{P}'$ into $k$ blocks as before: $\mathbf{P}' = \begin{bmatrix} \mathbf{P}'_1 \\ \vdots \\ \mathbf{P}'_k \end{bmatrix}$ so that $\mathbf{P}' \cdot \mathbf{Q} = \begin{bmatrix} \mathbf{P}'_1 \cdot \mathbf{Q} \\ \vdots \\ \mathbf{P}'_k \cdot \mathbf{Q} \end{bmatrix}$ where $\mathbf{P}'_i \in \mathbb{Z}_q^{k^{d-1} \times K}$ is a tall matrix.
4. Then multiplying gives

$$\begin{bmatrix} \mathbf{I}_k \otimes \mathbf{B}'^{(1)} \\ \mathbf{I}_k \otimes \mathbf{B}'^{(2)} \\ \vdots \\ \mathbf{I}_k \otimes \mathbf{B}'^{(T)} \end{bmatrix} \cdot \mathbf{P}' \cdot \mathbf{Q} = \begin{bmatrix} \mathbf{W}_1 \\ \mathbf{W}_2 \\ \vdots \\ \mathbf{W}_T \end{bmatrix} \in \mathbb{Z}_q^{kTm^{d-1} \times (K - M \log q)}$$

where for $j \in [T]$ we define

$$\mathbf{W}_j \triangleq \begin{bmatrix} \mathbf{B}'^{(j)} \cdot \mathbf{P}'_1 \cdot \mathbf{Q} \\ \mathbf{B}'^{(j)} \cdot \mathbf{P}'_2 \cdot \mathbf{Q} \\ \vdots \\ \mathbf{B}'^{(j)} \cdot \mathbf{P}'_k \cdot \mathbf{Q} \end{bmatrix} \in \mathbb{Z}_q^{km^{d-1} \times (K - M \log q)}.$$

*Working with only the top block* We now recap the progress made so far in the analysis for Step 3 (for uniqueness). At this point, we can rewrite

$$\sum_{j \in [T]} \left( \mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)} \right) \cdot \mathbf{P}' \cdot \mathbf{Q}$$

$$= \left( \left[ \mathbf{V}_1'^{(1)} \| \mathbf{V}_1'^{(2)} \| \cdots \| \mathbf{V}_1'^{(T)} \right] \otimes \mathbf{I}_{m^{d-1}} \right) \cdot \begin{bmatrix} \mathbf{W}_1 \\ \mathbf{W}_2 \\ \vdots \\ \mathbf{W}_T \end{bmatrix} \in \mathbb{Z}_q^{wm^{d-1} \times (K - M \log q)}$$

Recall that for our uniqueness argument to proceed in Step 3, we need that this matrix is of relatively large rank, say $O(m^{d-1})$, with high probability for

any non-zero matrix $\left[\mathbf{V}_1'^{(1)}\|\mathbf{V}_1'^{(2)}\|\cdots\|\mathbf{V}_1'^{(T)}\right]$. The following key observation simplifies analyzing the rank of this matrix: If $\left[\mathbf{V}_1'^{(1)}\|\mathbf{V}_1'^{(2)}\|\cdots\|\mathbf{V}_1'^{(T)}\right]$ is non-zero, then there is some row that is non-zero.

Without loss of generality, suppose that this non-zero row is the first row. This first row of $\left[\mathbf{V}_1'^{(1)}\|\mathbf{V}_1'^{(2)}\|\cdots\|\mathbf{V}_1'^{(T)}\right]$ defines a submatrix of $\left(\left[\mathbf{V}_1'^{(1)}\|\mathbf{V}_1'^{(2)}\|\cdots\|\mathbf{V}_1'^{(T)}\right]\otimes\mathbf{I}_{m^{d-1}}\right)\cdot\begin{bmatrix}\mathbf{W}_1\\\mathbf{W}_2\\\vdots\\\mathbf{W}_T\end{bmatrix}$ formed by its first $m^{d-1}$ rows. If this submatrix has large rank $O(m^{d-1})$, then the whole matrix has rank $O(m^{d-1})$.

This top block is of a substantially simpler form amenable to rank analysis as we will show below. We now identify this submatrix.

1. First observe that we can rewrite one of the multiplicands as follows:

$$\left[\mathbf{V}_1'^{(1)}\|\mathbf{V}_1'^{(2)}\|\cdots\|\mathbf{V}_1'^{(T)}\right]\otimes\mathbf{I}_{m^{d-1}}=\begin{bmatrix}\mathsf{Top}\\*\end{bmatrix}\in\mathbb{Z}_q^{wm^{d-1}\times kTm^{d-1}}$$

   where $\mathsf{Top}\in\mathbb{Z}_q^{m^{d-1}\times k\cdot T\cdot m^{d-1}}$ is of the form

$$\mathsf{Top}=[\mathbf{R}_{1,1}\|\mathbf{R}_{2,1}\|\mathbf{R}_{3,1}\|\cdots\|\mathbf{R}_{k,1}\|\mathbf{R}_{1,2}\|\cdots\|\mathbf{R}_{k,2}\|\cdots\|\mathbf{R}_{1,T}\|\cdots\|\mathbf{R}_{k,T}]$$

   where for $i\in[k], j\in[T]$, $(\mathbf{V}_1'^{(j)})_{[1,i]}$ denotes the $(1,i)$th entry of $\mathbf{V}_1'^{(j)}$ and where we define the following matrix to be a scalar multiple of the identity matrix:

$$\mathbf{R}_{i,j}\triangleq\left[(\mathbf{V}_1'^{(j)})_{[1,i]}\cdot\mathbf{I}_{m^{d-1}}\right].$$

2. Then the top block $\mathsf{Top}'\in\mathbb{Z}_q^{m^{d-1}\times(K-M\log q)}$ of

$$\left(\left[\mathbf{V}_1'^{(1)}\|\mathbf{V}_1'^{(2)}\|\cdots\|\mathbf{V}_1'^{(T)}\right]\otimes\mathbf{I}_{m^{d-1}}\right)\cdot\begin{bmatrix}\mathbf{W}_1\\\mathbf{W}_2\\\vdots\\\mathbf{W}_T\end{bmatrix}=\begin{bmatrix}\mathsf{Top}'\\*\end{bmatrix}$$

   satisfies the following equation

$$\begin{aligned}\mathsf{Top}'=\mathsf{Top}\cdot\begin{bmatrix}\mathbf{W}_1\\\mathbf{W}_2\\\vdots\\\mathbf{W}_T\end{bmatrix}&=\sum_{j\in[T]}\left(\sum_{i\in[k]}\mathbf{R}_{i,j}\cdot\mathbf{B}'^{(j)}\cdot\mathbf{P}_i'\cdot\mathbf{Q}\right)\\&=\sum_{j\in[T]}\left(\sum_{i\in[k]}(\mathbf{V}_1'^{(j)})_{[1,i]}\cdot\mathbf{B}'^{(j)}\cdot\mathbf{P}_i'\cdot\mathbf{Q}\right)\end{aligned}$$

**Recovering secrets up to uniqueness for $T > 1$** Having rewritten our expression, to finish Step 3 of our uniqueness argument, it suffices to show that with high probability over the choice of $\mathbf{P}', \mathbf{B}_2^{(j)}, \ldots, \mathbf{B}_d^{(j)}, \hat{\mathbf{B}}$ for $j \in [T]$, the matrix

$$\mathsf{Top}' = \sum_{j \in [T]} \left( \sum_{i \in [k]} (\mathbf{V}_1'^{(j)})_{[1,i]} \cdot \mathbf{B}'^{(j)} \cdot \mathbf{P}_i' \cdot \mathbf{Q} \right)$$

has rank $O(m^{d-1})$ for all non-zero vectors of the form $\left( (\mathbf{V}_1'^{(j)})_{[1,i]} \right)_{i \in [k], j \in [T]} \in \mathbb{Z}_q^{kT \times 1}$. Moreover, the form of the summation above gives rise to the following conjecture about the randomness of the matrices $\mathbf{W}_j$ for $j \in [T]$ defined above during the simplification.

Previously for the case $T = 1$, we were dealing with a single copy $(\mathbf{B}_2 \otimes \mathbf{B}_3 \otimes \cdots \otimes \mathbf{B}_d)\mathbf{P}_i'\mathbf{Q}$ for $i \in [k]$. We then replaced $(\mathbf{B}_2 \otimes \mathbf{B}_3 \otimes \cdots \otimes \mathbf{B}_d)\mathbf{P}_i'$ with a random matrix $\mathbf{F}_i$, due to Lemma 11. The homogeneous equation we worked implies that all the columns of $\sum_i v_i \mathbf{F}_i \mathbf{Q}$, where $\mathbf{v} = (v_1, \ldots, v_k) \in \mathbb{Z}_q^k$ is any non-zero vector, will be in the null-space of $\mathbf{X}_1$ . We ruled this out by using a union bound. Unfortunately, this approach won't be enough for us to handle large $T$. Indeed, in Lemma 9, the probability of error grows as $q^{-O(K)}$ restricting the dimension of $\mathbf{v}$ and hence $T$ to be $O(K) = O(m^{d+1/2})$. For ruling out $i\mathcal{O}$, we need to rule out $T$ at least $m^{2d-1}$.

We take a different approach. We will conjecture that $\{\mathbf{B}'^{(j)} \cdot \mathbf{P}_i' \cdot \mathbf{Q}\}_{i \in [k], j \in [T]}$ are close $\{\mathbf{F}_{i,j}\}_{i \in [k], j \in [T]}$ where $\mathbf{F}_{i,j}$ are uniform. This conjecture is heuristically feasible because each $\mathbf{B}'^{(j)}$ can be viewed as a randomness extractor who extracts $m^{d-1}$ field from $k^{d-1}$ field elements. Therefore, $T$ such extractors can be equivalently viewed as extracting $T \cdot m^{d-1}$ field elements from $k^{d-1}$ $\chi$ elements. This is heuristically possible if $T \ll (\frac{k}{m})^{d-1} \frac{\mathcal{H}_\infty(\chi)}{\log q}$. If $k \geq m^3$ as suggested by [29], our attack can extend to $T = O(m^{2d-2}/(\log q))$.

*Conjecture 2.* Let $m, k, w, q, \chi, M, K$ be as specified in Section 2.1. For $T \leq m^{2d-3}$, there exists $\epsilon = \epsilon(w) = \mathsf{negl}(w)$ such that for uniform randomly sampled matrices $\mathbf{B}_2^{(j)}, \mathbf{B}_3^{(j)}, \ldots \mathbf{B}_d^{(j)} \in \mathbb{Z}_q^{m \times k}$ for $j \in [T]$, $\mathbf{P}' \leftarrow \chi^{k^d \times K}$, and $\mathbf{Q} \in \mathbb{Z}_q^{K \times (K - M \log q)}$ a random full column rank matrix generated from the right nullspace of $G^{-1}(\hat{\mathbf{B}})$ where $\hat{\mathbf{B}} \in \mathbb{Z}_q^{M \times K}$ is uniform randomly sampled, we have

$$\left( \mathbf{B}'^{(j)} \cdot \mathbf{P}_i' \cdot \mathbf{Q} \right)_{i \in [k], j \in [T]} \approx_{\mathrm{stat}, \epsilon} (\mathbf{F}_{i,j})_{i \in [k], j \in [T]}$$

where $\mathbf{F}_{i,j} \in \mathbb{Z}_q^{m^{d-1} \times (K - M \log q)}$ for $i \in [k], j \in [T]$ are uniformly sampled random matrices, and where for $j \in [T]$

$$\mathbf{B}'^{(j)} \triangleq \mathbf{B}_2^{(j)} \otimes \mathbf{B}_3^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)} \in \mathbb{Z}_q^{m^{d-1} \times k^{d-1}}$$

and define $\mathbf{P}_i' \in \mathbb{Z}_q^{k^{d-1} \times K}$ for $i \in [k]$ such that $\mathbf{P}' = \begin{bmatrix} \mathbf{P}_1' \\ \vdots \\ \mathbf{P}_k' \end{bmatrix}$.

**Theorem 4.** *Let $d, m, w, k, q, M, K, \chi$ be as defined in Section 2.1. Assume Conjecture 1 and Conjecture 2. Let $\mathbf{X}_1 \in \mathbb{Z}_q^{w(m-w)^{d-1} \times wm^{d-1}}$ be of rank at least $w(m-w)^{d-1}$. For $j \in [T]$, let $\mathbf{B}_2^{(j)}, \ldots, \mathbf{B}_d^{(j)}$ be uniformly sampled from $\mathbb{Z}_q^{m \times k}$. Let $\mathbf{P}' \leftarrow \chi^{k^{d-1} \times K}$. Let $\mathbf{Q} \in \mathbb{Z}_q^{K \times K - M \log q}$ be of full column rank generated randomly from the right nullspace of $G^{-1}(\hat{\mathbf{B}})$ where $\hat{\mathbf{B}} \in \mathbb{Z}_q^{M \times K}$ is uniform randomly sampled.*

*If $T < m^{2d-1}/k = O(m^{2d-3})$, $m = \omega(w^2)$, then with probability $1 - \mathsf{negl}(w)$ over the choice of $\mathbf{P}'$ and $\mathbf{B}_2^{(j)}, \ldots, \mathbf{B}_d^{(j)}$ for $j \in [T]$ we have that $\mathbf{X}_1 \cdot \sum_{j \in [T]} \left( \mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)} \right) \cdot \mathbf{P}' \cdot \mathbf{Q} = 0$ implies that $\mathbf{V}_1'^{(j)} = \mathbf{0}$ for all $j \in [T]$.*

*Proof.* If $\left[ \mathbf{V}_1'^{(1)} \| \mathbf{V}_1'^{(2)} \| \cdots \| \mathbf{V}_1'^{(T)} \right]$ has a non-zero element it has a non-zero row. WLOG assume that it is the first one. The top block of $\sum_{j \in [T]} \left( \mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)} \right) \cdot \mathbf{P}' \cdot \mathbf{Q}$ was computed above to be

$$\sum_{i=1}^{k} \sum_{j=1}^{T} (\mathbf{V}'^{(j)})_{[1,i]} \mathbf{B}'^{(j)} \mathbf{P}'_i \cdot \mathbf{Q}$$

where $\left( (\mathbf{V}_1'^{(j)})_{[1,i]} \right)_{i \in [k], j \in [T]} \in \mathbb{Z}_q^{kT \times 1}$ is the first row of $\left[ \mathbf{V}_1'^{(1)} \| \mathbf{V}_1'^{(2)} \| \cdots \| \mathbf{V}_1'^{(T)} \right]$. Conjecture 2 gives $\epsilon = \mathsf{negl}(w)$ such that this sum is $\epsilon$-statistically close to

$$\sum_{i=1}^{k} \sum_{j=1}^{T} (\mathbf{V}'^{(j)})_{[1,i]} \mathbf{F}_{i,j}$$

for uniform random $\mathbf{F}_{i,j} \in \mathbb{Z}_q^{m^{d-1} \times (K - M \log q)}$. For a fixed vector $\left( (\mathbf{V}_1'^{(j)})_{[1,i]} \right)_{i \in [k], j \in [T]} \in \mathbb{Z}_q^{kT \times 1}$, $\sum_{i=1}^{k} \sum_{j=1}^{T} (\mathbf{V}'^{(j)})_{[1,i]} \mathbf{F}_{i,j}$ is uniformly distributed over $\mathbb{Z}_q^{m^{d-1} \times (K - M \log q)}$. Therefore, by the proof of Lemma 9, for this fixed vector we have that

$$\Pr_{\mathbf{F}_{i,j}} \left[ \mathrm{rk} \left( \sum_{i=1}^{k} \sum_{j=1}^{T} (\mathbf{V}'^{(j)})_{[1,i]} \mathbf{F}_{i,j} \right) \geq m^{d-1}/2 \right] \geq 1 - q^{-\Omega(K \cdot m^{d-1})}.$$

Then by union bound over all vectors $\left( (\mathbf{V}_1'^{(j)})_{[1,i]} \right)_{i \in [k], j \in [T]} \in \mathbb{Z}_q^{kT \times 1}$, the probability that there exists any non-zero vector over the choice of random matrices $\mathbf{F}_{i,j}$ is

$$\Pr_{\mathbf{F}_{i,j}} \left[ \exists \left( (\mathbf{V}_1'^{(j)})_{[1,i]} \right)_{i \in [k], j \in [T]} \neq \mathbf{0} \text{ s.t. } \mathrm{rk} \left( \sum_{i=1}^{k} \sum_{j=1}^{T} (\mathbf{V}'^{(j)})_{[1,i]} \cdot \mathbf{F}_{i,j} \right) \leq m^{d-1}/2 \right] < q^{-\Omega(Km^{d-1})}$$

as long as $T = O(m^{2d-3})$. Therefore with probability $1 - q^{-\Omega(Km^{d-1})} - \epsilon$ over the choice of $\mathbf{P}'$ and $\mathbf{B}_2^{(j)}, \ldots, \mathbf{B}_d^{(j)}$ for $j \in [T]$, and $\hat{\mathbf{B}}$, the matrix $\sum_{j \in [T]} \left( \mathbf{V}_1'^{(j)} \otimes \mathbf{B}_2^{(j)} \otimes \cdots \otimes \mathbf{B}_d^{(j)} \right)$.

$\mathbf{P}' \cdot \mathbf{Q} = 0$, is of rank at least $m^{d-1}/2$ since the top $m^{d-1} \times (K - M \log q)$ block already has rank above $m^{d-1}/2$.

On the other hand, the right nullity of $\mathbf{X}_1$ is $wm^{d-1} - w(m-w)^{d-1} = O\left(w^2 m^{d-2}\right)$. This is only possible if $m \leq O(w^2)$. In the parameter regime proposed by [29], $m \geq w^3$.

*Remark 8.* As mentioned before, $i\mathcal{O}$ needs some expansion which is only possible if $T < m^{2d-1}/k \leq m^{2d-4}$. If $m = w^3$, then for some $T = \Omega(m^{2d-3})$ the attack proceeds, ruling out any value of $T$ for which there is meaningful expansion.

*Remark 9.* As mentioned before, in any proofs corresponding to these the three steps described for proving uniqueness, we assumed that the equations were set up with $\mathbf{B}_2, \ldots, \mathbf{B}_d, \hat{\mathbf{B}}$ that are sampled uniform randomly as opposed to being LWE matrices. If multiple solutions for this homogeneous equation exist when they are LWE matrices, then we have a distinguisher between LWE matrices and random matrices because the homogeneous equation does not require any secret information so any adversary can set up the homogeneous equation.

### 4.4 Useful Linear Algebraic Facts

First, we recall several useful linear algebraic facts used in the uniqueness analysis in both Step 1 and Step 2. While it is not necessary, we encourage the reader to review the following section to facilitate their understanding of the above algorithm's correctness.

**Lemma 12.** *For any matrices $\mathbf{M}_1, \mathbf{M}_2$, there exists a matrix $\mathbf{N}$ such that $\mathbf{M}_1 \cdot \mathbf{N} = \mathbf{M_2}$ if and only if* $\mathrm{Colspan}(\mathbf{M}_2) \subseteq \mathrm{Colspan}(\mathbf{M_1})$.

*Proof.* This fact immediately follows by the definition of column span and matrix multiplication.

**Corollary 6.** *For any matrices $\mathbf{M}_1, \mathbf{M}_2$ and for any invertible matrices $\mathbf{N}_1, \mathbf{N}_2$ of the appropriate dimensions, we have that*

$$\mathrm{Colspan}\left(\left[\mathbf{M}_1 \| \mathbf{M}_2\right]\right) = \mathrm{Colspan}\left(\left[\mathbf{M}_1\mathbf{N}_1 \| \mathbf{M}_2\mathbf{N}_2\right]\right).$$

*Proof.* Observe that $\left[\mathbf{M}_1 \| \mathbf{M}_2\right] = \left[\mathbf{M}_1\mathbf{N}_1 \| \mathbf{M}_2\mathbf{N}_2\right] \cdot \begin{bmatrix} \mathbf{N}_1^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{N}_2^{-1} \end{bmatrix}$ where $\begin{bmatrix} \mathbf{N}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{N}_2 \end{bmatrix}^{-1} = \begin{bmatrix} \mathbf{N}_1^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{N}_2^{-1} \end{bmatrix}$ and apply Lemma 12.

**Lemma 13.** *For any matrices $\mathbf{M}, \mathbf{N}$ with finitely many rows and columns such that* $\mathrm{Colspan}(\mathbf{M}) \subseteq \mathrm{Colspan}(\mathbf{N})$*, if* $\mathrm{rk}(\mathbf{M}) = \mathrm{rk}(\mathbf{N})$*, then* $\mathrm{Colspan}(\mathbf{M}) = \mathrm{Colspan}(\mathbf{N})$.

*Proof.* Recall that column and row ranks are always equivalent (consider the reduced echelon form) and recall that the dimension of the vector space $\mathrm{Colspan}(\mathbf{A})$ satisfies $\dim(\mathrm{Colspan}(\mathbf{A})) = \mathrm{rk}(\mathbf{A})$. Therefore, we have

$$\dim(\mathrm{Colspan}(\mathbf{M})) = \mathrm{rk}(\mathbf{M}) = \mathrm{rk}(\mathbf{N}) = \dim(\mathrm{Colspan}(\mathbf{N})).$$

Combining this equivalence with $\mathrm{Colspan}(\mathbf{M}) \subseteq \mathrm{Colspan}(\mathbf{N})$, implies $\mathrm{Colspan}(\mathbf{M}) = \mathrm{Colspan}(\mathbf{N})$.

**Lemma 14.** *For any matrices* $\mathbf{M}, \mathbf{N}$ *with finitely many rows and columns,* $\mathrm{Colspan}(\mathbf{M} \otimes \mathbf{N}) = \mathrm{Colspan}(\mathbf{M}) \otimes \mathrm{Colspan}(\mathbf{N})$.

*Proof.* Let $s$ be the number of columns of $\mathbf{M}$ and let $t$ be the number of columns of $\mathbf{N}$ and observe that $\mathbf{M} \otimes \mathbf{N}$ has $st$ columns. For $i \in [s]$, let $\mathbf{m}_i$ denote the $i$th column of $\mathbf{M}$ and for $j \in [t]$, let $\mathbf{n}_j$ denote the $j$th column of $\mathbf{N}$.

For $\ell \in [st]$, we can express $\ell$ uniquely as $\ell = (k-1) \cdot t + r$ for $k \in [s]$ and $r \in [t]$. By definition of the tensor product, for $\ell$th column of $\mathbf{M} \otimes \mathbf{N}$ is exactly $\mathbf{m}_k \otimes \mathbf{n}_r$. This relation establishes a direct equality between a spanning set for $\mathrm{Colspan}(\mathbf{M} \otimes \mathbf{N})$ given by the columns of $\mathbf{M} \otimes \mathbf{N}$ and a spanning set for $\mathrm{Colspan}(\mathbf{M}) \otimes \mathrm{Colspan}(\mathbf{N})$ given by $\{\mathbf{m}_i \otimes \mathbf{n}_j\}_{i \in [s], j \in [t]}$ so we obtain the desired set equality.

Finally, we recall the standard fact without proof.

**Lemma 15.** *Let* $\mathcal{I}, \mathcal{J}$ *be index sets. If* $\{\mathbf{b}_i : i \in \mathcal{I}\}$ *is a basis for some vector space* $\mathbf{W}_1$ *and* $\{\mathbf{c}_j : j \in \mathcal{J}\}$ *is a basis for some vector space* $\mathbf{W}_2$*, then* $\{\mathbf{b}_i \otimes \mathbf{c}_j\}_{i \in \mathcal{I}, j \in \mathcal{J}}$ *is a basis for the vector space* $\mathbf{W}_1 \otimes \mathbf{W}_2$.

### 4.5 Analyzing the Tensor Structure in the Construction

Having recalled certain linear algebraic facts, we first analyze the column span of the following matrix

$$\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \mathbf{I}_m \otimes \mathbf{U}_2 \otimes \mathbf{I}_m^{\otimes(d-2)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right].$$

where the matrices $\mathbf{U}_i \in \mathbb{Z}_q^{m \times w}$ are of the stipulated form (with a top $w \times w$ identity block, so of full column rank $w$). The column span of this matrix is some subspace of the vector space over $\underbrace{\mathbb{Z}_q^m \otimes \cdots \otimes \mathbb{Z}_q^m}_{d \text{ times}}$. Considering $\mathbb{Z}_q^m$ as a vector space, we consider the following bases for $\mathbb{Z}_q^m$. For $i \in [d]$, let $\mathcal{B}_i$ be a basis for $\mathbb{Z}_q^m$ obtained by extending the set of column vectors in $\mathbf{U}_i = \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_i \end{bmatrix}$ to the following full rank, lower-triangular matrix

$$\mathcal{B}_i \triangleq \begin{bmatrix} \mathbf{I}_w & \mathbf{0}_{w \times (m-w)} \\ \tilde{\mathbf{A}}_i & \mathbf{I}_{m-w} \end{bmatrix} \in \mathbb{Z}_q^{m \times m},$$

and let $(\mathbf{e}_1^{(i)}, \ldots, \mathbf{e}_m^{(i)})$ denote the columns (the basis vectors). We make the following straightforward observations:

**Lemma 16.** *The set* $\{\mathbf{e}_{i_1}^{(1)} \otimes \mathbf{e}_{i_2}^{(2)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)}\}_{i_1 \in [w], i_2, i_3, \ldots, i_d \in [m]}$ *forms a basis for* $\mathrm{Colspan}\left(\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right)$.

*Proof.* Lemma 14 implies that

$$\mathrm{Colspan}\left(\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right) = \mathrm{Colspan}\left(\mathbf{U}_1\right) \otimes \mathrm{Colspan}\left(\mathbf{I}_m\right)^{\otimes(d-1)} = \mathrm{Colspan}\left(\mathbf{U}_1\right) \otimes \mathbb{Z}_q^{\otimes(d-1)}.$$

Then observe that $\{\mathbf{e}_i^{(1)}\}_{i\in[w]}$ forms a basis for Colspan $(\mathbf{U}_1)$ and for each $j \in [d]$, the set $\{\mathbf{e}_i^{(j)}\}_{i\in[m]}$ forms a basis for $\mathbb{Z}_q^m$. Now apply Lemma 15 repeatedly with the above bases to obtain the desired result.

Lemma 16 readily implies the following two corollaries.

**Corollary 7.** *For all $j^* \in [d]$, the set $\{\mathbf{e}_{i_1}^{(1)} \otimes \mathbf{e}_{i_2}^{(2)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)}\}_{i_{j^*}\in[w],\forall\ j\in[d]\setminus\{j^*\},i_j\in[m]}$ forms a basis for* Colspan $\left(\mathbf{I}_m^{\otimes(j^*-1)} \otimes \mathbf{U}_{j^*} \otimes \mathbf{I}_m^{\otimes(d-j^*)}\right)$.

*Proof.* The proof follows exactly as that for Lemma 16.

**Corollary 8.** $\dim\left(\text{Colspan}\left(\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right)\right) = wm^{d-1}$.

*Proof.* The dimension is the number of elements in the basis.

Moreover, using the above corollaries, we can analyze the column space of the blockwise concatenation of these tensor matrices which we state in the following lemma.

**Lemma 17.** *The set*

$$\mathcal{B} \triangleq \{\mathbf{e}_{i_1}^{(1)} \otimes \mathbf{e}_{i_2}^{(2)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)}\}_{\forall j\in[d],i_j\in[m]\wedge\exists j^*\in[d]\ s.t.\ i_{j^*}\in[w]}$$

*forms a basis for the vector space* Colspan $\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)$.

*Proof.* For convenience, we use the shorthand notation

$$\mathbf{M} \triangleq \left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]$$
$$V \triangleq \text{Colspan}\,(\mathbf{M})$$

A subset of vectors in a linearly independent set of vectors is linearly independent. Therefore, the set $\mathcal{B}$ is linearly independent because it is a subset of

$$\{\mathbf{e}_{i_1}^{(1)} \otimes \mathbf{e}_{i_2}^{(2)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)}\}_{\forall j\in[d],i_j\in[m]}$$

which is a basis for $(\mathbb{Z}_q^m)^{\otimes d}$ by Lemma 15. Finally, we observe that $V = \text{span}(\mathcal{B})$.

1. $(V \subseteq \text{span}(\mathcal{B}))$ By the definition of column span, the columns of $\mathbf{M}$ form a spanning set for $V$. Therefore it suffices to show that each column $\mathbf{c}$ in $\mathbf{M}$ belongs in $\text{span}(\mathcal{B})$. This is easy to see because every column $\mathbf{c}$ is a column in some block of the form

   $$\mathbf{I}_m^{\otimes(j^*-1)} \otimes \mathbf{U}_{j^*} \otimes \mathbf{I}_m^{\otimes(d-j^*)}$$

   where $j^* \in [d]$. By Corollary 7, $\mathcal{B}_{\text{blk}_{j^*}} \triangleq \{\mathbf{e}_{i_1}^{(1)} \otimes \mathbf{e}_{i_2}^{(2)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)}\}_{i_{j^*}\in[w],\forall j\in[d]\setminus\{j^*\},i_j\in[m]}$ is a basis for this block and therefore $\mathbf{c} \in \text{span}(\mathcal{B}_{\text{blk}_{j^*}})$. Finally, observe that $\text{span}(\mathcal{B}_{\text{blk}_{j^*}}) \subseteq \text{span}(\mathcal{B})$ by construction of $\mathcal{B}$. This concludes showing the containment in this direction since every column of $\mathbf{M}$ is in $\text{span}(\mathcal{B})$.

2. ($V \supseteq \text{span}(\mathcal{B})$) It suffices to show that every element of $\mathcal{B}$ is contained in $V$. Pick any element of $\mathcal{B}$, say $\mathbf{e}_{i_1}^{(1)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)}$. By construction of $\mathcal{B}$, we know that at least one of the indices $i_1, \ldots, i_d$ is at most $w$. Without loss of generality assume that the first index $i_1 \leq w$. Then for $1 < j \leq d$ we can express $\mathbf{e}_{i_j}^{(j)} = \sum_{k_j \in [m]} \beta_{k_j}^{(j)} \mathbf{e}_{k_j}$ where $\beta_{k_j}^{(j)} \in \mathbb{Z}_q$ is some scalar and $\mathbf{e}_{k_j} \in \mathbb{Z}_q^m$ (without any superscripts) denotes the $k_j$-th standard elementary vector for $k_j \in [m]$. Observe that $\{\mathbf{e}_{i_1}^{(1)} \otimes \mathbf{e}_{i_2} \otimes \cdots \mathbf{e}_{i_d}\}_{i_1 \in [w], i_2, \ldots, i_d \in [m]}$ forms a basis for Colspan $\left(\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right)$. Substitute for $\mathbf{e}_{i_j}^{(j)}$, for $2 \leq j \leq d$, in the element $\mathbf{e}_{i_1}^{(1)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)}$ to obtain the expression:

$$\begin{aligned}\mathbf{e}_{i_1}^{(1)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)} &= \mathbf{e}_{i_1}^{(1)} \otimes \sum_{k_2 \in [m]} \beta_{k_2}^{(j)} \mathbf{e}_{k_2} \otimes \cdots \otimes \sum_{k_d \in [m]} \beta_{k_d}^{(j)} \mathbf{e}_{k_d} \\ &= \sum_{k_2, \ldots, k_d \in [m]} \left( \prod_{j \in \{2, \ldots, d\}} \beta_{k_j}^{(j)} \right) \mathbf{e}_{i_1}^{(1)} \otimes \mathbf{e}_{k_2} \otimes \cdots \otimes \mathbf{e}_{k_d}\end{aligned}$$

The above expression shows that $\mathbf{e}_{i_1}^{(1)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)} \in$ Colspan $\left(\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right)$. Finally, we observe that Colspan $\left(\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)}\right) \subseteq V$ by construction of $V$. Therefore, $\mathbf{e}_{i_1}^{(1)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)} \in V$. We conclude that $\mathcal{B} \subseteq V$.

**Corollary 9.** *For any choice of* $\{\tilde{\mathbf{A}}_i\}_{i \in [d]}$, $\dim\left(\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)\right) = m^d - (m-w)^d$.

*Proof.* The dimension is the number of elements in the basis given by Lemma 17. Straightforward counting gives $m^d - (m-w)^d$ many elements.

*Remark 10.* As a result of Corollary 9, we observe a rank deficiency of $O(w^2 m^{d-2})$ in

$$\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right].$$

Namely, the number of columns in $\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]$ is exactly $dwm^{d-1}$, but the rank is $m^d - (m-w)^d = dwm^{d-1} - O(w^2 m^{d-2})$.

The following corollary demonstrates why the special structure of the $\mathbf{U}_i$'s is so useful for proving uniqueness, and it plays a critical role in proving the uniqueness of the solution for $\{\tilde{\mathbf{A}}_i\}_{i \in [d]}$. In particular, we observed in Corollary 9 that the dimension of the concatenated blockwise tensor matrix is fixed regardless of the choice of matrices for $\{\tilde{\mathbf{A}}_i\}_{i \in [d]}$. This implies the following corollary.

**Corollary 10.** *For* $i \in [d]$, *let* $\mathbf{U}_i \triangleq \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_i \end{bmatrix}$ *and let* $\mathbf{U}_i' \triangleq \begin{bmatrix} \mathbf{I}_w \\ \tilde{\mathbf{A}}_i' \end{bmatrix}$. *For any choice of* $\{\tilde{\mathbf{A}}_i\}_{i \in [d]}$ *and* $\{\tilde{\mathbf{A}}_i'\}_{i \in [d]}$, *if*

$$\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right) \subseteq \text{Colspan}\left(\left[\mathbf{U}_1' \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d'\right]\right)$$

*then*

$$\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right) = \text{Colspan}\left(\left[\mathbf{U}'_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}'_d\right]\right)$$

*Proof.* By Corollary 9,

$$\begin{aligned}
&\dim\left(\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)\right) \\
&\quad = m^d - (m-w)^d \\
&\quad = \dim\left(\text{Colspan}\left(\left[\mathbf{U}'_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}'_d\right]\right)\right).
\end{aligned}$$

Therefore, by Lemma 13,

$$\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right) = \text{Colspan}\left(\left[\mathbf{U}'_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}'_d\right]\right)$$

**Corollary 11.** *With overwhelming probability over the choice of random* $\mathbf{A}_i \in \mathbb{Z}_q^{m\times w}$*, for* $i \in [d]$*, if*

$$\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right) \subseteq \text{Colspan}\left(\left[\mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d\right]\right)$$

*then*

$$\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right) = \text{Colspan}\left(\left[\mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d\right]\right)$$

*Proof (Proof Sketch).* For brevity, we provide a short proof sketch that shows the relationship between $\left[\mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d\right]$ and $\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]$ for some matrices $\mathbf{U}_i$ that are in a normal form with a top $w \times w$ identity block.

Note, that with overwhelming probability the matrices $\mathbf{A}_i \in \mathbb{Z}_q^{m\times w}$ generated in the scheme are of full column rank $w$. Since they are of full column rank, for each $i \in [d]$, there exists a well-defined invertible linear transformation $T'_i : \text{Colspan}(\mathbf{A}_i) \to \text{Colspan}(\mathbf{A}_i)$ that maps the columns of $\mathbf{A}_i$ to the columns of its reduced echelon form (the matrix form is exactly $\mathbf{A}_{i,T}^{-1}$). Every such invertible linear transformation $T'_i$ can be extended to a invertible linear transformation $T_i : \mathbb{Z}_q^m \to \mathbb{Z}_q^m$ by acting as the identity on a set of $m-w$ vectors in $\mathbb{Z}_q^m$ that extend the columns of $\mathbf{A}_i$ to a basis for $\mathbb{Z}_q^m$. Observe that $T_i(\mathbb{Z}_q^m) = \mathbb{Z}_q^m$. Then we observe that applying the invertible linear transformation $T_1 \otimes T_2 \otimes \cdots \otimes T_d$ on $\text{Colspan}\left(\left[\mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d\right]\right)$ gives us a vector space that is expressible as $\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)$ for some matrices $\{\mathbf{U}_i\}_{i\in[d]}$ of the desired form. By Corollary 9,

$$\dim\left(\text{Colspan}\left(\left[\mathbf{U}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{U}_d\right]\right)\right) = m^d - (m-w)^d.$$

Invertible linear transformations preserve the overall dimension, therefore, the original column span has the same dimension:

$$\dim\left(\text{Colspan}\left(\left[\mathbf{A}_1 \otimes \mathbf{I}_m^{\otimes(d-1)} \| \cdots \| \mathbf{I}_m^{\otimes(d-1)} \otimes \mathbf{A}_d\right]\right)\right) = m^d - (m-w)^d.$$

Finally if a subspace has the same dimension as the ambient space, then the subspace as a set must be equivalent to the ambient space (see Lemma 13).

**Lemma 18.** *For $i \in [d]$, let $\mathbf{L}_i \triangleq \mathbf{I}_m^{\otimes(i-1)} \otimes \begin{bmatrix}\mathbf{I}_w \\ \tilde{\mathbf{A}}_i\end{bmatrix} \otimes \mathbf{I}_m^{\otimes(d-i)}$ and let $\tilde{\mathbf{A}} \triangleq \left[\mathbf{L}_1 \| \mathbf{L}_2 \| \cdots \| \mathbf{L}_d\right]$. Under Conjecture 1, with overwhelming probability over the choice of $\mathbf{P} \leftarrow \chi^{M \times m^d}$, we have that the following holds for any set of matrices $\{\tilde{\mathbf{A}}_i\}_{i\in[d]}$.*

$$\forall i \in [d], \dim\left(\mathbf{P} \cdot \mathbf{L}_i\right) = wm^{d-1}$$

$$\dim\left(\text{Colspan}\left(\left[\mathbf{P} \cdot \mathbf{L}_1 \| \mathbf{P} \cdot \mathbf{L}_2 \| \ldots \| \mathbf{P} \cdot \mathbf{L}_d\right]\right)\right) = m^d - (m-w)^d = dwm^{d-1} - O\left(w^2 m^{d-2}\right)$$

$$\dim\left(\text{Colspan}(\mathbf{P} \cdot \mathbf{L}_1) \cap \text{Colspan}\left(\left[\mathbf{P} \cdot \mathbf{L}_2 \| \ldots \| \mathbf{P} \cdot \mathbf{L}_d\right]\right)\right) = wm^{d-1} - w(m-w)^{d-1}$$

*Proof.* By Corollary 3 and Lemma 5, the following vectors are linearly independent

$$\mathcal{B}^{\mathbf{P}} = \left\{\mathbf{P} \cdot \left(\mathbf{e}_{i_1}^{(1)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)}\right) : i_1, \ldots, i_d \in [m] \wedge \exists j \in [d], i_j \leq w\right\}$$
$$\cup \bigcup_{k=1}^{d} \left\{\mathbf{P} \cdot \left(\mathbf{e}_m^{(1)} \otimes \cdots \mathbf{e}_m^{(k-1)} \otimes \mathbf{e}_\ell^{(k)} \otimes \mathbf{e}_m^{(k+1)} \otimes \cdots \otimes \mathbf{e}_m^{(d)}\right) : \ell \in [m]\right\}.$$

Because of this, the first claim trivially holds.

For the second claim, observe that the following set of $m^d - (m-w)^d$ vectors

$$\left\{\mathbf{P} \cdot \left(\mathbf{e}_{i_1}^{(1)} \otimes \cdots \otimes \mathbf{e}_{i_d}^{(d)}\right) : i_1, \ldots, i_d \in [m] \wedge \exists j \in [d], i_j \leq w\right\}$$

spans Colspan$(\mathbf{P}\tilde{\mathbf{A}})$, therefore it is also a basis so $\dim\left(\text{Colspan}(\mathbf{P}\tilde{\mathbf{A}})\right) = m^d - (m-w)^d$.

For the third claim, we first claim that $\dim\left(\text{Colspan}\left(\mathbf{P}\mathbf{L}_2 \| \cdots \| \mathbf{P}\mathbf{L}_d\right)\right) = \dim\left(\text{Colspan}\left(\mathbf{L}_2 \| \cdots \| \mathbf{L}_d\right)\right) = m^d - m(m-w)^{d-1}$. The first equality is due to Lemma 5.

For the second equality follows from the proof of Lemma 17.

Now we have that

$$\begin{aligned}
&\dim\left(\text{Colspan}(\mathbf{P} \cdot \mathbf{L}_1) \cap \text{Colspan}\left(\left[\mathbf{P} \cdot \mathbf{L}_2 \| \ldots \| \mathbf{P} \cdot \mathbf{L}_d\right]\right)\right) \\
&\quad = \dim(\text{Colspan}(\left[\mathbf{P} \cdot \mathbf{L}_1\right])) + \dim(\text{Colspan}(\left[\mathbf{P} \cdot \mathbf{L}_2 \| \cdots \| \mathbf{P} \cdot \mathbf{L}_d\right])) \\
&\qquad - \dim\left(\text{Colspan}\left(\left[\mathbf{P} \cdot \mathbf{L}_1 \| \mathbf{P} \cdot \mathbf{L}_2 \| \ldots \| \mathbf{P} \cdot \mathbf{L}_d\right]\right)\right) \\
&= wm^{d-1} - w(m-w)^{d-1}.
\end{aligned}$$