Statistical Zeroizing Attack: Cryptanalysis of Candidates of BP Obfuscation over GGH15 Multilinear Map

Jung Hee Cheon[1], Wonhee Cho[1], Minki Hhan[1], Jiseung Kim[1], and Changmin Lee[2]

[1] Seoul National University, Republic of Korea
{jhcheon,wony0404,hhan_,tory154}@snu.ac.kr
[2] ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), France
changmin.lee@ens-lyon.fr

Abstract. We introduce a new type of cryptanalytic algorithm on the obfuscations based on the branching programs. Applying this algorithm to two recent general-purpose obfuscation schemes one by Chen *et al.* (CRYPTO 2018) and the other by Bartusek *et al.* (TCC 2018), we can show that they do not have the desired security. In other words, there exist two functionally equivalent branching programs whose obfuscated programs can be distinguished in polynomial time.

Our strategy is to reduce the security problem of indistinguishability obfuscation into the distinguishing problem of two distributions where polynomially many samples are given. More precisely, we perform the obfuscating process ourselves with randomly chosen secret values to obtain identical and independent samples according to the distribution of evaluations of obfuscations. We then use the variance of samples as a new distinguisher of two functionally equivalent obfuscated programs.

This statistical attack gives a new perspective on the security of the indistinguishability obfuscations: We should consider the shape of distributions of the evaluations of obfuscations to ensure the security. In other words, while most of the previous (weak) security proofs have been studied with respect to algebraic attack model or ideal model, our attack shows that this algebraic security is not enough to achieve indistinguishability obfuscation.

Keywords: Cryptanalysis, indistinguishability obfuscation, multilinear map

Disclaimer

The authors of BGMZ obfuscation [4] (TCC'18) report that there are flaws of cryptanalysis of BGMZ obfuscation in Section 5. In particular, the current optimal parameter choice of BGMZ obfuscation is robust against our attack, while the attack lies outside the provable security of BGMZ obfuscation.

The flaws in the analysis in Section 5 are as follows:

- ν is chosen to $\mathsf{poly}(\lambda)$ in this paper whereas the original paper [4] chooses $\nu = 2^{\lambda}$ (or at least super-polynomial of λ).
- The analysis of our attack claims that $\left(1+\frac{2}{g}\right)^{h}$ is polynomial of λ, but it is not true since $g = 5$ is constant.

We remark that our attack gives a constraint on the parameters; BGMZ obfuscation with $\sigma = \exp(\lambda)^{a}$ can be broken in the same manner with slightly modified proof. We will update the paper as soon as possible.

[a] Interestingly, this choice gives a countermeasure of CVW obfuscation.

1 Introduction

Indistinguishability obfuscation (iO) is one of the most powerful tools used to construct many cryptographic applications such as multiparty key exchange and functional encryption [6, 21, 34]. While to construct a general-purpose of iO has been posed as an longstanding open problem, Garg *et al.* [21] firstly proposed a plausible candidate general-purpose iO based on a multilinear map in

2013. Starting from this work, many subsequent studies have proposed the iO design method using a multilinear map [1–3, 8, 21, 22, 30, 31].

Most of the general-purpose obfuscation are built upon the multilinear maps. Thus the multilinear maps rise as an essential building block to construct the obfuscations; However, all of the currently known candidates, so-called GGH13, CLT13 and GGH15 [19, 20, 23], are not known to have the desired security of multilinear map under the standard assumptions. Indeed, when the encodings of zero are given to adversary, theses candidates were broken due to *the first class of zeroizing attacks*, such as the CHLRS attack and Hu-Jia attack [13, 17, 27], which exploits the existence of public low level encodings of zero. Due to these attacks, many of their applications such as the multi-party key exchange cannot be instantiated by known candidates multilinear map.

Fortunately, many iO candidates are robust against the first class of zeroizing attack since iOs do not publish low level encodings of zero. However, it does not imply the security of the current constructions of iO. Indeed, it turned out that most of candidates iO are failed to achieve the desired security by *the second class of zeroizing attacks* [11,12,14–16,18,32], which employs algebraic relations from the top level encodings of zero. Thus, many researches focus on the algebraic security of obfuscation in the weak multilinear map models [4, 22, 28].

Recently, GGH15 multilinear map has been in the spotlight because it is shown that GGH15 and its variants can be exploited to construct the provable secure special-purpose obfuscations and other cryptographic applications including constraint pseudorandom function under the hardness of LWE and its variants [9, 10, 12, 26, 35]. Therefore, GGH15 multilinear map has been believed to the most plausible candidate for constructing the general-purpose obfuscation.

In this respect, Chen *et al.* [12] proposed a new iO candidate over GGH15, called CVW obfuscation, to be secure against all known attacks. On the other hand, Bartusek *et al.* [4] provided a new candidate over GGH15, called BGMZ obfuscation, which is provably secure against generalized zeroizing attacks. The security of these two schemes remains as an open problem.

1.1 Our Result

We give a new polynomial time cryptanalytic algorithm, *statistical zeroizing attack*, on candidates of iO. Our algorithm shows that the recent candidates iO suggested by Chen *et al.* and Bartusek *et al.* constructed upon GGH15 multilinear map do not satisfy the desired security. Our attack leads a new direction to the study of iO: our cryptanalysis shows that the distribution of evaluations should be (almost) the same regardless of the choice of target branching program. Previously, most of attacks and constructions focus only on the algebraic structure of evaluations.

Overview of Attack and Technique. We briefly describe our attack which consists of three steps. Assume that the adversary has two functionally equivalent branching programs $\mathbf{M}$ and $\mathbf{N}$, and an obfuscated program $\mathcal{O}(\mathbf{P})$ where $\mathbf{P} = \mathbf{M}$ or $\mathbf{N}$. The purpose of adversary is to determine whether $\mathbf{P} = \mathbf{M}$ or $\mathbf{N}$. Two branching programs which have the different distribution of the obfuscated program evaluations are in the scope of the attack. Intuitive description of each step of the attack is as follows:

1. As the first step of the attack, the adversary implements sampling algorithms for distributions of evaluation of obfuscated program $\mathcal{O}(\mathbf{M})$ and $\mathcal{O}(\mathbf{N})$ by *mimicking* whole obfuscating process, where the probability of sampling is over every secret values used in obfuscating process. More precisely, the adversary samples every secret and error values used in the construction process of obfuscator and the obfuscating process of program. Then the adversary constructs obfuscator and obfuscates targeted programs $\mathbf{M}$ and $\mathbf{N}$ itself using the sampled errors and secrets, and then evaluates the new obfuscated programs at a fixed input x. Since the obfuscation and evaluation process is done in polynomial time, the adversary obtains the polynomial time sampling procedure for evaluations of obfuscation.
2. The adversary then applies a well-known theorem: If one can sample two distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ in polynomial time, then one-sample indistinguishability of $\mathcal{D}_1$ and $\mathcal{D}_2$ implies polynomially many sample indistinguishability of $\mathcal{D}_1$ and $\mathcal{D}_2$.
   In other words, if the adversary can distinguish two distribution when polynomially many sample are given, then the adversary can distinguish two distribution even when only one sample is

given. Thanks to this theorem the adversary can reduce the distinguishing problem of evaluations of obfuscation $\mathcal{O}(\mathbf{M})$ and $\mathcal{O}(\mathbf{N})$ into the distinguishing problem of two distributions $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$ which follow the evaluations of $\mathcal{O}(\mathbf{M})$ and $\mathcal{O}(\mathbf{N})$, respectively, where the polynomially many samples are given.

3. At last, the adversary computes the variance of samples, which serves as a distinguisher of two distribution $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$. In other words, we estimate the confidence intervals of sample variances using Chebyshev inequality with high probability, say 99%. In our choice of $\mathbf{M}$ and $\mathbf{N}$, two intervals are disjoint thus the adversary can distinguish two distribution by checking the sample variance is included in which interval.

Though the last step is conceptually simple, it is difficult to verify that the conditions of attack hold well, and this verification requires several complex computational tasks. Thus we give the sufficient conditions that attack works well for the simpler description of the attack. And then we assign most of papers including appendix to deal with many random variables that might be dependent themselves. We derive many lemmas to deal with such intertwined random variables.

Applicability and Limitation of Statistical Zeroizing Attack. We discuss the applicability and limitation of our attack. First of all, our attack refutes the open problem suggested in [12] (as well as the same question of the BGMZ obfuscation): the CVW obfuscation is not secure even when only the honest evaluations (as matrices product) are given as oracle outputs.

The class of branching programs constructed from CNF formulas, which is suggested in [12, Construction 6.4], is in the range of our attack. For example, if we choose two branching programs $\mathbf{N} = \{\mathbf{N}_{i,b}\}$ and $\mathbf{M} = \{\mathbf{M}_{i,b}\}$ as follows: $\mathbf{N}_{1,b}$ as an identity matrix with $w \times w$ size and all other matrices of $\mathbf{M}$ and $\mathbf{N}$ as zero matrix. These two branching programs $\mathbf{M}$ and $\mathbf{N}$ are corresponding to some CNF formulas following the construction. This is exactly the same to the branching programs described in Section 4.2 as attack example.

On the other hand, there is a class of the branching programs that are robust against our attack: permutation matrix branching programs. For this class of branching programs, the distributions of evaluations except bookend vectors are always the same for any choice of permutation branching program $\mathbf{M}$ in many obfuscation constructions. Interestingly, the first candidate iO [21] has targeted such branching programs so it is robust against our attack.

Counter Measures. Unfortunately, CVW and BGMZ obfuscations in the suggested form are not appropriate to obfuscate the permutation branching programs, which are robust against our attack. More precisely, though there is a general transformation from permutation branching program (or Type II branching programs) into Type I branching program [12, Claim 6.2], this transformation induces the Type I branching program with bookend vector $(\mathbf{v}|-\mathbf{v})$, which does not coincide to $\mathbf{1}^{1\times w}$ that is the implicitly supposed bookend vector of CVW obfuscation.[3] In other words, slight modifications are required to obfuscate the permutation branching program and its transformed forms. The similar problem also appears in BGMZ obfuscation.

On the other hand, fortunately, we can modify CVW obfuscation to obfuscate the Type II branching programs; this modified construction is secure against all existing attacks including the attack suggested in this paper. This can be done by choosing the bookends $\mathbf{J}$ and $\mathbf{L}$ appropriately for such branching program. Namely, change the $\mathbf{1}^{1\times w}$ and $\mathbf{1}^{w\times 1}$ in $\mathbf{J}$ and $\mathbf{L}$ by repeated random vectors, and *do not* make public the choice of them; they are hid in the output matrices. More precise description is placed in Appendix A. The similar modification works well in BGMZ obfuscation, and we believe that the security of this modified scheme can be proven in more generalized model.

Open Questions. We also leave some open problems:

1. The modified candidates as in Appendix A are at least secure against all known attacks, including the attack suggested in this paper. Can we prove the security of those construction under the standard or plausible assumption? How about the same question if the only evaluations are given as oracle outputs?

[3] We write *bookend vector* to denote the vector $\mathbf{v}$ in [12, Definition 6]. In [12, Section 11.1], $\mathbf{1}^{1\times w}$ part of $\mathbf{J}$ means that the bookend vector $\mathbf{v}$ is in fact $\mathbf{1}^{1\times w}$.

2. Our attack is still a zeroizing attack in spite of brand-new, therefore the class of *evasive* functions is out of the range of attack.
3. The candidate witness encryption constructed in [12] shares almost same structure to obfuscation construction in [12] but we do not know whether it is (provably) secure or not.
4. The attack presented in this paper shows some weakness of obfuscation for non-permutation branching program, while this class of branching program is known to have several advantages compared to permutation branching programs including efficiency [12]. Can we avoid this attack without choosing the permutation branching programs?

Organization. In Section 2, we introduce preliminary information related to the branching program, iO, and lattices. We describe the statistical zeroizing attack in Section 3. In Section 4, we briefly describe CVW obfuscation and its cryptanalysis. In addition, we review BGMZ obfuscation and its cryptanalysis in Section 5.

2 Preliminaries

Notations. $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ denote the sets of natural numbers, integers, and real numbers, respectively. For an integer $q \geq 2$, $\mathbb{Z}_q$ is the set of integers modulo q. Elements are in $\mathbb{Z}_q$ are usually considered as integers in $[-q/2, q/2)$. We denote the set $\{1, 2, \cdots, h\}$ by $[h]$ for a natural number h.

Lower bold letters means row vectors and capital bold letters denote matrices. In addition, capital italic letters denote random matrices or random variables. For a random variable X, we let $E(X)$ be the expected value of X, $Var(X)$ the variance of X.

The n-dimensional identity matrix is denoted by $\mathbf{I}^{n\times n}$. For a row vector $\mathbf{v}$, a i-th component of $\mathbf{v}$ is denoted by v_i, and for a matrix $\mathbf{A}$, a (i,j)-th entry of a matrix $\mathbf{A}$ is denoted by $a_{i,j}$, respectively. A notation $\mathbf{1}^{a\times b}$ means a $a \times b$ matrix such that all entries are 1. The ℓ_p norm of a vector $\mathbf{v} = (v_i)$ is denoted by $\|\mathbf{v}\|_p = (\sum_i |v_i|^p)^{1/p}$. We denote $\|\mathbf{A}\|_\infty$ by the infinity norm of a matrix $\mathbf{A}$, $\|\mathbf{A}\|_\infty = \max_{i,j} a_{i,j}$ with $\mathbf{A} = (a_{i,j})$.

We use a notation $\mathbf{x} \leftarrow \chi$ to denote the operation of sampling element $\mathbf{x}$ from the distribution χ. Especially, if χ is the uniform distribution on a finite set $\mathbf{X}$, we denote $\mathbf{x} \leftarrow U(\mathbf{X})$.

For two square[4] matrices $\mathbf{A} = (a_{i,j}) \in \mathbb{R}^{n\times n}$, $\mathbf{B} \in \mathbb{R}^{n\times n}$, the tensor product of matrix $\mathbf{A}$ and $\mathbf{B}$ is defined as

$$\mathbf{A} \otimes \mathbf{B} := \begin{pmatrix} a_{1,1}\cdot\mathbf{B} & \cdots & a_{1,n}\cdot\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{n,1}\cdot\mathbf{B}, & \cdots, & a_{n,n}\cdot\mathbf{B} \end{pmatrix}.$$

Moreover, for four matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D} \in \mathbb{R}^{n\times n}$, the equation $(\mathbf{A}\otimes\mathbf{B})\cdot(\mathbf{C}\otimes\mathbf{D}) = (\mathbf{A}\cdot\mathbf{C})\otimes(\mathbf{B}\cdot\mathbf{D})$ holds.

2.1 Matrix Branching Program

A matrix branching program (BP) is the set which consists of an index-to-input function and several matrix chains.

Definition 2.1 *A width w, length h, and a s-ary matrix branching program $\mathbf{P}$ over a ℓ-bit input is a set which consists of an index-to-input map $\{\mathsf{inp}_\mu : [h] \to [\ell]\}_{\mu\in[s]}$, sequences of matrices, and two disjoint sets of target matrices*

$$\mathbf{P} = \{(\mathsf{inp}_\mu)_{\mu\in[s]}, \{\mathbf{P}_{i,\boldsymbol{b}} \in \{0,1\}^{w\times w}\}_{i\in[h],\boldsymbol{b}\in\{0,1\}^s}, \mathcal{P}_0, \mathcal{P}_1 \subset \mathbb{Z}^{w\times w}\}.$$

The evaluation of $\mathbf{P}$ on input $\mathbf{x} = (\mathbf{x}^\mu)_{\mu\in[s]} \in \{0,1\}^{\ell\times s}$ is computed by

$$\mathbf{P}(\mathbf{x}) = \begin{cases} 0 & \textit{if } \prod_{i=1}^{h} \mathbf{P}_{i,(x^\mu_{\mathsf{inp}_\mu(i)})_{\mu\in[s]}} \in \mathcal{P}_0 \\ 1 & \textit{if } \prod_{i=1}^{h} \mathbf{P}_{i,(x^\mu_{\mathsf{inp}_\mu(i)})_{\mu\in[s]}} \in \mathcal{P}_1 \end{cases}.$$

[4] The tensor product can be defined for arbitrary matrices, however, we only need the tensor product of square matrices.

When $s = 1$ ($s = 2$), the BP is called a single-input (dual-input) BP. In this paper, we usually use $\mathcal{P}_0 = \mathbf{0}^{w \times w}$ and $\mathcal{P}_1$ is the set of all nonzero matrices in $\mathbb{Z}^{w \times w}$. Also, we call $\{\mathbf{P}_{i,b}\}_{\boldsymbol{b} \in \{0,1\}^s}$ the i-th layer of the BP. Remark that CVW obfuscation and BGMZ obfuscation take as input different BP type (e.g. single and dual BP) and the required properties of BP for each obfuscation are different. Therefore, we mention the required properties used to construct an obfuscation again before describing each obfuscation.

2.2 Indistinguishability Obfuscation

Definition 2.2 (Indistinguishability Obfuscation) *A probabilistic polynomial time machine $\mathcal{O}$ is an indistinguishability obfuscator for a circuit class $\mathcal{C}$ if the following conditions are satisfied:*

- *For all security parameters $\lambda \in \mathbb{N}$, for all circuits $C \in \mathcal{C}$, for all inputs $\mathbf{x}$, the following probability holds:*
$$\Pr\left[C'(\mathbf{x}) = C(\mathbf{x}) : C' \leftarrow \mathcal{O}(\lambda, C)\right] = 1.$$
- *For any p.p.t distinguisher D, there exists a negligible function α satisfying the following statement: For all security parameters $\lambda \in \mathbb{N}$ and all pairs of circuits C_0, $C_1 \in \mathcal{C}$, $C_0(\mathbf{x}) = C_1(\mathbf{x})$ for all inputs $\mathbf{x}$ implies*
$$|\Pr\left[D(\mathcal{O}(\lambda, C_0)) = 1\right] - \Pr\left[D(\mathcal{O}(\lambda, C_1)) = 1\right]| \leq \alpha(\lambda).$$

2.3 Lattice Background

A lattice $\mathcal{L}$ of dimension n is a discrete additive subgroup of $\mathbb{R}^n$. If $\mathcal{L}$ is generated by the set $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$, all elements in $\mathcal{L}$ are of the form $\sum_{i=1}^n x_i \cdot \mathbf{b}_i$ for some integers x_i's. In this case, the lattice $\mathcal{L}$ is called the full rank lattice. Throughout this paper, we only consider the full rank lattice. Now we give several definitions and lemmas used in this paper.

For any $\sigma > 0$, the Gaussian function on $\mathbb{R}^n$ centered at $\mathbf{c}$ with parameter σ is defined as
$$\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp^{-\pi\|\mathbf{x}-\mathbf{c}\|/\sigma^2} \text{ for all } \mathbf{x} \in \mathbb{R}^n.$$

Definition 2.3 (Discrete Gaussian Distribution on Lattices) *For any element $\mathbf{c} \in \mathbb{R}^n$, $\sigma > 0$ and any full rank lattice $\mathcal{L}$ of $\mathbb{R}^n$, the discrete Gaussian distribution over $\mathcal{L}$ is defined as*
$$D_{\mathcal{L},\sigma,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{\sigma,\mathbf{c}}(\mathbf{x})}{\rho_{\sigma,\mathbf{c}}(\mathcal{L})} \text{ for all } \mathbf{x} \in \mathcal{L}$$
where $\rho_{\sigma,\mathbf{c}}(\mathcal{L}) = \sum_{\mathbf{x} \in \mathcal{L}} \rho_{\sigma,\mathbf{c}}(\mathbf{x})$.

Definition 2.4 (Decisional Learning with Errors (LWE) [33]) *For integers $n, m \in \mathbb{N}$ and modulus $q \geq 2$, let θ, π, and χ over $\mathbb{Z}$ be a distribution for secret vectors, public matrices, and error vectors, respectively. Then, an LWE sample is defined as $(\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T \mod q)$ where $\mathbf{s} \leftarrow \theta^n$, $\mathbf{A} \leftarrow \pi^{n \times m}$, $\mathbf{e} \leftarrow \chi^m$. If there exists an algorithm that distinguishes the LWE sample from one that is uniformly sampled from $\pi^{n \times m} \times U(\mathbb{Z}^{1 \times m})$ with probability non-negligibly greater than 1/2, then we say an algorithm can solve $\mathsf{LWE}_{n,m,q,\theta,\pi,\chi}$.*

Lemma 2.5 (Hardness of LWE [7,33]) *Given $n \in \mathbb{N}$, for any $m = \mathsf{poly}(n)$, $q \geq 2^{\mathsf{poly}(n)}$. Let θ and π be an uniform distribtuion over $\mathbb{Z}_q$ and χ the Gaussian distribution $D_{\mathbb{Z},\sigma}$ with $\sigma \geq 2\sqrt{n}$. If there exists an efficient (possibly quantum) algorithm that breaks $\mathsf{LWE}_{n,m,q,\theta,\pi,\chi}$, then there exists an efficient (possible quantum) algorithm for approximate SIVP and GapSVP in the ℓ_2 norm, in the worst case, to within $\tilde{O}(nq/\sigma)$ factors.*

Lemma 2.6 (LWE with Small Public Matrices [5]) *Given $n \in \mathbb{N}$, for $m = \mathsf{poly}(n)$, $q \leq 2^{\mathsf{poly}(n)}$ with $n' \geq 2n \log q$, $\mathsf{LWE}_{n',m,q,U(\mathbb{Z}_q),D_{\mathbb{Z},\sigma},D_{\mathbb{Z},\sigma}}$ is hard as $\mathsf{LWE}_{n,m,q,U(\mathbb{Z}_q),U(\mathbb{Z}_q),D_{\mathbb{Z},\sigma}}$.*

Theorem 2.7 ([29]) *There is a p.p.t algorithm $\mathsf{TrapSam}(1^n, 1^m, q)$ for any integers $n \geq 1$, modulus $q \geq 2$, and $m \geq 2n \log q$, outputs a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a trapdoor τ such that the distribution of $\mathbf{A}$ is statistically indistinguishable in n with a uniform distribution $\mathbb{Z}_q^{n \times m}$. Moreover, there is a p.p.t algorithm Invert that with overwhelming probability over all random choices, do the following:*

– *For* $\mathbf{b}^T = \mathbf{s}^T \cdot \mathbf{A} + \mathbf{e}^T$*, where* $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$ *and either* $\|\mathbf{e}\| < q/O(\sqrt{n \log q})$ *or* $\mathbf{e} \leftarrow D_{\mathbb{Z}^m, \alpha q}$ *for* $1/\alpha \geq \sqrt{n \log q} \cdot \omega(\sqrt{\log n})$*, the deterministic algorithm* $\mathsf{Invert}(\tau, \mathbf{A}, \mathbf{b})$ *outputs* $\mathbf{s}$ *and* $\mathbf{e}$*.*

Lemma 2.8 (Lemma 3.11 in [12]) *There is a p.p.t. algorithm that for* $\sigma \geq 2\sqrt{n \log q}$*, given* $(\mathbf{A}, \tau) \leftarrow \mathsf{TrapSam}(1^n, 1^m, q)$*,* $\mathbf{y} \in \mathbb{Z}_q^n$*, outputs a vector* $\mathbf{d}$ *from* $D_{\mathbb{Z}^m, \sigma}$ *conditioned on* $\mathbf{Ad} \equiv \mathbf{y} \mod q$*.*

Lemma 2.9 ([24]) *There is a p.p.t. algorithm* $\mathsf{Sample}(\mathbf{A}, \tau, \mathbf{y}, \sigma)$ *that outputs a vector* $\mathbf{d}$ *from a distribution* $D_{\mathbb{Z}^m, \sigma}$*. Moreover, if* $\sigma \geq 2\sqrt{n \log q}$*, then with all but negligible probability, we have*

$$\{\mathbf{A}, \mathbf{d}, \mathbf{y} : \mathbf{y} \leftarrow U(\mathbb{Z}_q^n), \mathbf{d} \leftarrow \mathsf{Sample}(\mathbf{A}, \tau, \mathbf{y}, \sigma)\} \approx_s \{\mathbf{A}, \mathbf{d}, \mathbf{y} : \mathbf{d} \leftarrow D_{\mathbb{Z}^m, \sigma}, \mathbf{Ad} = \mathbf{y}\}.$$

3 Statistical Zeroizing Attack

We introduce our attack, *statistical zeroizing attack*, in this section. We give an abstract model for branching program obfuscation and the attack on this model. In this attack, we are given two functionally equivalent branching programs $\mathbf{M}$ and $\mathbf{N}$, which will be decided later, and an obfuscated program $\mathcal{O}(\mathbf{P})$. Our purpose is to distinguish whether $\mathbf{P} = \mathbf{M}$ or $\mathbf{P} = \mathbf{N}$. The targeted branching programs of obfuscation output 0 when the product corresponding to input is zero. The obfuscated program $\mathcal{O}(\mathbf{P})$ consists of

$$\left\{\mathbf{S}, \{\mathbf{D}_{i,\boldsymbol{b}}\}_{1 \leq i \leq h, \boldsymbol{b} \in \{0,1\}^s}, \mathbf{T}, \mathsf{inp} = (\mathsf{inp}_1, \cdots, \mathsf{inp}_s) : [h] \to [\ell]^s, B\right\}$$

where every element is a matrix over $\mathbb{Z}_q$ (possibly identity) except the input function inp. The output of the obfuscated program at $\mathbf{x} = (x_1, \cdots, x_\ell) \in \{0,1\}^\ell$ is computed by considering the value

$$\mathcal{O}(\mathbf{P})(\mathbf{x}) = \mathbf{S} \cdot \prod_{i=1}^{h} \mathbf{D}_{i, \boldsymbol{x}_{\mathsf{inp}(i)}} \cdot \mathbf{T}$$

where $\boldsymbol{x}_{\mathsf{inp}(i)} = (x_{\mathsf{inp}_1(i)}, \cdots, x_{\mathsf{inp}_s(i)})$. Note that $\mathcal{O}(\mathbf{P})(\mathbf{x})$ can be a matrix, vector or an element (over $\mathbb{Z}_q$). Regard it as matrix/vector/integer over $\mathbb{Z}$ and check the value: If $\|\mathcal{O}(\mathbf{P})(\mathbf{x})\|_\infty < B < q$ then it outputs 0, otherwise outputs 1. We note that we call $\mathcal{O}(\mathbf{P})(\mathbf{x})$ the *evaluation* of obfuscated program (at $\mathbf{x}$) in this section. We also call $\mathcal{O}(\mathbf{P})(\mathbf{x})$ evaluation of zero if $\mathbf{P}(\mathbf{x}) = 0$ in the plain program. We stress that we do *not* say the *output* value of $\mathbf{P}(\mathbf{x})$ as an evaluation of obfuscated program in this section and Section 4 and 5.

To distinguish two different obfuscated programs, we see the distribution of valid evaluations of zero of $\mathcal{O}(\mathbf{M})$ and $\mathcal{O}(\mathbf{N})$. For the evaluation of zero, the size of these products is far small compared to q (or B) and thus we can obtain the integer value rather than the element in $\mathbb{Z}_q$. Now, if the evaluation is of the form matrix or vector, we consider only the first entry, namely (1,1) entry of the matrix or the first entry of the vector, in the whole procedure of the attack. We call all of these entries by *the first entry* of the evaluation, including the case of the evaluation is just a real value. Our strategy is to compute the sample variance of the first entries of many independent evaluations which follow the same distribution. The key of the attack is that this variance depends on the plain program of the obfuscated program and the variance is sufficiently different for two certain programs. Therefore, from the variance of the independent evaluations follow the same distribution, we can decide the obfuscated program is from which program.

Three natural questions arise for this strategy, which are stated as follows:

1. How can we use the given obfuscation $\mathcal{O}(\mathbf{P})$?
2. How can we sample *independent* evaluations of obfuscated programs $\mathcal{O}(\mathbf{M})$ and/or $\mathcal{O}(\mathbf{N})$?
3. How does the message part affects the variance of evaluations?

The first two questions are resolved by *mimicking* the obfuscator along with a well-known theorem about one-sample and multiple-sample indistinguishability, which is discussed in Section 3.1. The last question is rather complex to give a simple answer. What we need is that this effect suffices to distinguish two obfuscated programs. In Section 3.1 and 3.2, we give the detailed answers of these questions respectively. To illustrate the behavior of the obfuscation in practice, we place a simple obfuscation and the attack on that in Section 3.3. We recommend the readers to read the description of the attack while comparing the abstract description and the simple example.

3.1 Independent Multiple Sampling of Evaluations

Now we give a *mimicking* technique, which allow us to sample identical independent samples of evaluations. We begin with a simple but failed method for sampling to explain the obstacle of using $\mathcal{O}(\mathbf{P})$ itself. In other words, we can obtain multiple samples of evaluation at zero by evaluating several different zeros on the obfuscated program $\mathcal{O}(\mathbf{P})$. Unfortunately, this way cannot ensure that we obtain *independent* samples.

Our strategy to bypass this issue is to mimic the *whole process* of obfuscation, which resolves the second question. More precisely, we re-sample *every* secret values of obfuscation (such as errors or bundling matrices) and construct a new obfuscator, obfuscated program and its evaluation ourselves. The i-th sampling for $2 \leq i \leq \kappa$ of evaluation for obfuscation of $\mathbf{M}$ proceeds as follows:

1. randomly sample all secrets following the specified distribution of given obfuscation process.
2. construct obfuscator $\mathcal{O}^{(i)}$ ourselves using the sampled secrets and errors.
3. obfuscate the program $\mathbf{M}$ using $\mathcal{O}^{(i)}$ and obtain $\mathcal{O}^{(i)}(\mathbf{M})$.
4. compute $\mathcal{O}^{(i)}(\mathbf{M})(\mathbf{x})$ for a fixed $\mathbf{x}$ satisfying $\mathbf{M}(\mathbf{x}) = \mathbf{0}$.

In other words, we compute $\mathcal{O}^{(i)}(\mathbf{M})(\mathbf{x})$ by doing whole obfuscating procedure, instead of using the given obfuscated program $\mathcal{O}(\mathbf{P})$ to obtain several evaluations. Note that all of these $\mathcal{O}^{(i)}(\mathbf{M})(\mathbf{x})$ follow the same distribution, whose samples are computed as in the above procedure. We write the distributions of the first entry of $\mathcal{O}^{(i)}(\mathbf{M})(\mathbf{x})$ by $\mathcal{D}_{\mathbf{M}}$ and define $\mathcal{D}_{\mathbf{N}}$ similarly.

In this setting, we can consider the first entry of $\mathcal{O}(\mathbf{P})(\mathbf{x}) = \mathcal{O}^{(1)}(\mathbf{P})(\mathbf{x})$ as a sample from $\mathcal{D}_{\mathbf{M}}$ or $\mathcal{D}_{\mathbf{N}}$. Further, both sampling procedure of $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$ can be done in polynomial time since the sampling can be done by initializing obfuscation, obfuscating branching program and evaluating obfuscated program which all can be done in polynomial time by definition. Now the following lemma gives the answer for the first question. Namely, this lemma enable us to assume that polynomially many independent evaluations of obfuscation are given.

Proposition 3.1 (Theorem 3.2.6 in [25], adapted) *Let $\mathcal{X}$ and $\mathcal{Y}$ be two distributions from which one can sample in polynomial time. Then (one sample) indistinguishability of $\mathcal{X}$ and $\mathcal{Y}$ implies polynomial-sample indistinguishability of $\mathcal{X}$ and $\mathcal{Y}$.*

The corresponding algorithm that transforms the $\kappa = \mathsf{poly}(\lambda)$-sample distinguisher into one sample distinguisher as follows: sample k samples from $\mathcal{X}$ and $\kappa - k - 1$ samples from $\mathcal{Y}$ with probability $1/\kappa$ and then apply the κ-sample indistinguishability adversary with new samples plus the given sample. For more detailed proof we refer [25, Section 3.2] to readers.

We recall that we can sample two distributions $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$ in polynomial time. By combining the fact that two distributions $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$ can be sampled in polynomial time with Proposition 3.1, we can transform the distinguishing problem of obfuscation into the distinguishing problem of distributions with given polynomially many samples. In the remainder of the paper, we assume that we can obtain polynomially many samples from one of two distributions $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$ and try to solve the polynomial-sample distinguishing problem on the given distributions, instead of the distinguishing problem with one obfuscated program $\mathcal{O}(\mathbf{P})$. Note that, for each sampling, we re-sample every secrets and errors so that all samples are independent of each other.

3.2 Distinguishing Distributions Using the Sample Variance

Now we describe the distinguishing attack algorithm, assuming that we have polynomially many samples. The targeted branching programs are chosen as follows:

$$\mathbf{M} = \left(\mathbf{M}_{i,\boldsymbol{b}} = \mathbf{0}^{w\times w} \textit{ for } i = 1\right),$$
$$\mathbf{N} = \left(\mathbf{N}_{i,\boldsymbol{b}} = \mathbf{0}^{w\times w} \textit{ for } i = 2\right),$$

where $\mathbf{0}^{w\times w}$ means the w by w matrix with all zero entries. The other matrices will be determined later, appropriately for each case. Note that the valid evaluation of both branching programs is always $\mathbf{0}^{w\times w}$ so they are functionally equivalent. We fix the input $\mathbf{x} = \mathbf{x}_0$, which is used to construct distributions. We write $X_{\mathbf{N}}$ and $X_{\mathbf{N}}$ to denote the random variables that follow the distribution $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$, respectively. We remark that this choice (and choice of other matrices) make a difference on two distributions $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$. The example in Section 3.3 exemplifies the difference of two distributions.

Now we compute the variance of the samples, and check whether the distance between the sample variance we computed and the expected variance of $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$. If the distance from the sample variance to the variance of $\mathcal{D}_{\mathbf{M}}$ is less than the distance to the variance of $\mathcal{D}_{\mathbf{N}}$, we decide the given samples are from $\mathcal{D}_{\mathbf{M}}$. Otherwise we decide the samples are from $\mathcal{D}_{\mathbf{N}}$. The result of this method is stated in the following proposition.

Proposition 3.2 *Suppose that two random variables $X_{\mathbf{M}}$ and $X_{\mathbf{N}}$ that follow distributions $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$, and have the variances $\sigma_{\mathbf{N}}^2$ and $\sigma_{\mathbf{M}}^2$, respectively. For the security parameter λ and polynomials $p, q, r = \mathsf{poly}(\lambda)$, there is a polynomial time algorithm that determines $\mathcal{D}_{\mathbf{P}} = \mathcal{D}_{\mathbf{M}}$ or $\mathcal{D}_{\mathbf{N}}$ with non-negligible probability when $O(p \cdot (\sqrt{q} + \sqrt{r})) = poly(\lambda)$ independent samples from $\mathcal{D}_{\mathbf{P}}$ are given as input of the algorithm and the following conditions hold with overwhelming probability:*

$$\left| \frac{\max(E[X_{\mathbf{N}}^2], E[X_{\mathbf{M}}^2])}{\sigma_{\boldsymbol{N}}^2 - \sigma_{\boldsymbol{M}}^2} \right| \le p(\lambda), \quad \left| \frac{E[X_{\mathbf{N}}^4]}{E[X_{\mathbf{N}}^2]^2} \right| \le q(\lambda), \text{ and } \left| \frac{E[X_{\mathbf{M}}^4]}{E[X_{\mathbf{M}}^2]^2} \right| \le r(\lambda).$$

In other words, if two known distributions satisfy the conditions, we can solve the distinguishing problem of two distribution with multiple samples. Combining this result with Proposition 3.1 or the corresponding algorithm, we obtain the statistical zeroizing attack to solve the distinguishing problem of the obfuscations. Thus to cryptanalyze the concrete obfuscation schemes, it suffice to show the conditions in Proposition 3.2. We conclude this section by giving the proof of Proposition 3.2.

Proof (Proposition 3.2). We call two useful lemmas first.

Lemma 3.3 (Chebyshev's inequality) *Let X be a random variable with a finite expected value μ and a finite variance $\sigma^2 > 0$. Then, it holds that*

$$\Pr[|X - \mu| \ge k\sigma] \le 1/k^2$$

for any real number $k > 0$.

Lemma 3.4 *Let S^2 be the variance of with replacement samples of size κ from a distribution $\mathcal{D}$. The variance of S^2 satisfies*

$$Var(S^2) = \frac{1}{\kappa}\left(\mu_4 - \frac{\kappa - 3}{\kappa - 1}\mu_2^2\right)$$

where $\mu_n = E[X^n]$, X is random variable that follow a distribution $\mathcal{D}$.

Suppose that all of the conditions hold for polynomials $p, q, r \in \mathsf{poly}(\lambda)$. We compute the 99% confidence interval of variance of S^2. By Lemma 3.3 and 3.4,

$$\Pr\left[|S^2 - \sigma_{\boldsymbol{P}}^2| \ge 10 \cdot \sqrt{\frac{1}{\kappa} \cdot \left(E[X_{\boldsymbol{P}}^4] - \frac{\kappa - 1}{\kappa - 3} \cdot E[X_{\boldsymbol{P}}^2]^2\right)}\right] \le \frac{1}{100}$$

with κ number of samples. If two intervals (for $\mathbf{M}$ and $\mathbf{N}$) are disjoint, we can distinguish two distribution with the probability $\ge \left(\frac{99}{100}\right)^2$. More precisely, when $\kappa \ge 100 \cdot (p(\lambda) \cdot \sqrt{q(\lambda)} + p(\lambda) \cdot \sqrt{r(\lambda)})$ that is $\mathsf{poly}(\lambda)$, we can distinguish two random variables with probability more than or equal to $\left(\frac{99}{100}\right)^2$ since $\sigma_{\boldsymbol{M}}^2 + 10 \cdot \sqrt{\frac{1}{\kappa} \cdot \left(E[X_{\mathbf{M}}^4] - \frac{\kappa-1}{\kappa-3} \cdot E[X_{\mathbf{M}}^2]^2\right)} < \sigma_{\boldsymbol{N}}^2 - 10 \cdot \sqrt{\frac{1}{\kappa} \cdot \left(E[X_{\mathbf{N}}^4] - \frac{\kappa-1}{\kappa-3} \cdot E[X_{\boldsymbol{N}}^2]^2\right)}$ holds. □

3.3 Example of the Statistical Zeroizing Attack

In this section, we give a simple example of the statistical zeroizing attack. First, we briefly review the construction of single input BP obfuscation based GGH15 without safeguard.

For an index to input function $\mathsf{inp} : [h] \to [\ell]$, let

$$\mathbf{P} = \left\{\{\mathbf{P}_{i,b} \in \{0,1\}^{w \times w}\}_{i \in [h], b \in \{0,1\}}, \mathcal{P}_0 = \mathbf{0}^{w \times w}, \mathcal{P}_1 = \mathbb{Z}^{w \times w} \setminus \mathcal{P}_0\right\}$$

be a single input BP.

For parameters $w, m, q, B \in \mathbb{N}$ and $\sigma \in \mathbb{R}^+$,[5] the BP obfuscation based GGH15 consists of the matrices and input function, namely

$$\mathcal{O}(\mathbf{P}) = \left\{\mathsf{inp}, \mathbf{A}_0, \{\mathbf{D}_{i,b} \in \mathbb{Z}^{m\times m}\}_{i\in[h], b\in\{0,1\}}\right\}.$$

In this case, the matrix $\mathbf{T}$ in the abstract model is the identity matrix and $\mathbf{S} = \mathbf{A}_0$. The output of the obfuscation at $\mathbf{x}$ is computing as follows: compute the matrix $\mathbf{A}_0 \cdot \prod_{i=1}^{h} \mathbf{D}_{i,x_{\mathsf{inp}(i)}}$ and compare its $\|\cdot\|_\infty$ to a zerotest bound B. If it is less than B, outputs zero. Otherwise, outputs 1.

More precisely, the algorithm to construct an obfuscated program $\mathcal{O}(\mathbf{P})$ proceeds as follows:

- Sample matrices $(\mathbf{A}_i, \tau_i) \leftarrow \mathsf{TrapSam}(1^w, 1^m, q)$ for $i = 0, 1, \cdots, h-1$, $\mathbf{A}_h \leftarrow U(\mathbb{Z}_q^{w\times m})$ and $\mathbf{E}_{i,b} \leftarrow \chi^{w\times m}$.
- By using the trapdoor τ_i, sample matrices

$$\mathbf{D}_{i,b} \in \mathbb{Z}^{m\times m} \leftarrow \mathsf{Sample}(\mathbf{A}_{i-1}, \tau_{i-1}, \mathbf{P}_{i,b}\cdot\mathbf{A}_i + \mathbf{E}_{i,b}, \sigma) \text{ with } 1 \le i \le h.$$

- Output matrices $\{\mathbf{A}_0, \{\mathbf{D}_{i,b} \in \mathbb{Z}^{m\times m}\}_{i\in[h], b\in\{0,1\}}\}$.

Then, we observe the product $\mathcal{O}(\mathbf{P})(\mathbf{x}) = [\mathbf{A}_0 \cdot \prod_{i=1}^{h} \mathbf{D}_{i,x_{\mathsf{inp}(i)}}]_q$ is equal to

$$\prod_{i=1}^{h} \mathbf{P}_{i,x_{\mathsf{inp}(i)}} \cdot \mathbf{A}_h + \sum_{j=1}^{h} \left(\left(\prod_{i=1}^{j-1} \mathbf{P}_{i,x_{\mathsf{inp}(i)}} \right) \cdot \mathbf{E}_{j,x_{\mathsf{inp}(j)}} \cdot \prod_{k=j+1}^{h} \mathbf{D}_{i,x_{\mathsf{inp}(k)}} \right)$$

over $\mathbb{Z}_q$. If $\prod_{i=1}^{h} \mathbf{P}_{i,x_{\mathsf{inp}(i)}} = \mathbf{0}^{w\times w}$, then $\mathcal{O}(\mathbf{P})(\mathbf{x})$ can be regarded as a summation of matrices over integers instead of $\mathbb{Z}_q$ under the certain choice of parameters as follows

$$\mathcal{O}(\mathbf{P})(\mathbf{x}) = \left[\mathbf{A}_0 \cdot \prod_{i=1}^{h} \mathbf{D}_{i,x_{\mathsf{inp}(i)}}\right]_q = \sum_{j=1}^{h} \left(\left(\prod_{i=1}^{j-1} \mathbf{P}_{i,x_{\mathsf{inp}(i)}} \right) \cdot \mathbf{E}_{j,x_{\mathsf{inp}(j)}} \cdot \prod_{k=j+1}^{h} \mathbf{D}_{i,x_{\mathsf{inp}(k)}} \right)$$

since the infinity norm of the above matrix is less than $B \ll q$. Note that the evaluation values only rely on the matrices $\mathbf{P}_{i,b}$, $\mathbf{E}_{i,b}$ and $\mathbf{D}_{i,b}$. Thus, the evaluation result depends on the message matrices $\mathbf{P}_{i,b}$.

Suppose that we have two functionally equivalent BPs $\mathbf{M} = \{\mathbf{M}_{i,b}\}_{i\in[h],b\in\{0,1\}}$ and $\mathbf{N} = \{\mathbf{N}_{i,b}\}_{i\in[h],b\in\{0,1\}}$ satisfies

$$\mathbf{M}_{i,b} = \mathbf{0}^{w\times w} \text{ for all } i, b \text{ and } \mathbf{N}_{i,b} = \begin{cases} \mathbf{I}^{w\times w} & \text{if } i = 1 \\ \mathbf{0}^{w\times w} & \text{otherwise} \end{cases},$$

and an obfuscated program $\mathcal{O}(\mathbf{P})$. Our goal is to determine whether $\mathbf{P}$ is $\mathbf{M}$ or not. For all $\mathbf{x} \in \{0,1\}^\ell$, the evaluation of the obfuscation is of the form

$$\mathcal{O}(\mathbf{M})(\mathbf{x}) = \mathbf{E}_{1,x_{\mathsf{inp}(1)}} \cdot \prod_{k=2}^{h} \mathbf{D}_{k,x_{\mathsf{inp}(k)}} \text{ and}$$
$$\mathcal{O}(\mathbf{N})(\mathbf{x}) = \mathbf{E}_{1,x_{\mathsf{inp}(1)}} \cdot \prod_{k=2}^{h} \mathbf{D}_{k,x_{\mathsf{inp}(k)}} + \mathbf{I}\cdot\mathbf{E}_{2,x_{\mathsf{inp}(2)}} \cdot \prod_{k=3}^{h} \mathbf{D}_{k,x_{\mathsf{inp}(k)}}.$$

Note that they correspond to the distributions $\mathcal{D}_\mathbf{M}$ and $\mathcal{D}_\mathbf{N}$ for a fixed vector $\mathbf{x}$. These equations show the difference of two distributions in this case.

Our first strategy of the statistical zeroizing attack is mimicking obfuscated program. We know how to sample matrices $\mathbf{A}_i, \mathbf{E}_{i,b}$ and $\mathbf{D}_{i,b}$. Thus we can construct the obfuscated program by running the algorithms as the same way, and obtain independent and identical samples.

More precisely, we can obtain the imitation pairs $(\mathbf{A}'_i, \tau'_i)$ by implementing a $\mathsf{TrapSam}$ algorithm and similarly get the mimicked matrices $\mathbf{E}'_{i,b}$ and $\mathbf{D}'_{i,b}$ from the distribution $\chi^{w\times m}$ and the Sample

[5] We do not discuss the size of parameters for the simplicity of the description.

algorithm. Therefore, we can construct $\mathsf{poly}(\lambda)$ obfuscated program $\mathcal{O}^{(i)}(\mathbf{M})$ and $\mathcal{O}^{(i)}(\mathbf{N})$. If we denote $\mathcal{D}_{\mathbf{M}}$ by a distribution of the (1,1) entry of $\mathcal{O}^{(i)}(\mathbf{M})$ and use the notation $\mathcal{D}_{\mathbf{N}}$ similarly, the one sample indistinguishable problem is converted into $\mathsf{poly}(\lambda)$ sample indistinguishable problem by employing Proposition 3.1.

Lastly, we compute the range of sample variances of the two distributions $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$ using the Chebyshev's inequality with a parameter $k = 10$. If the two distributions satisfy the conditions of Proposition 3.2, the two ranges do not overlap with non-negligible probability. It implies that the $\mathcal{D}_{\mathbf{M}}$ distribution and the $\mathcal{D}_{\mathbf{N}}$ distribution with polynomially many samples can be distinguished. The remainder of this paper, in Section 4 and 5, we show that there are distributions that satisfy the Proposition 3.2 in the CVW and BGMZ obfuscations, respectively.

4 Cryptanalysis of CVW Obfuscation

In this section, we briefly describe the construction of CVW obfuscation scheme and show that the statistical zeroizing attack works well for CVW obfuscation.

4.1 Construction of CVW Obfuscation

Chen, Vaikuntanathan and Wee proposed a new candidate of iO which is robust against all existing attacks. We give a brief description of the candidate scheme here. For more details, we refer to original paper [12].

First, we start with the description of BPs they used. The authors use single-input binary BPs, *i.e.*, $\mathsf{inp} = \mathsf{inp}_1$. They employ a new function, called an input-to-index map $\bar{\omega}$: $\{0,1\}^\ell \to \{0,1\}^h$ such that $\bar{\omega}(\mathbf{x})_i = \mathbf{x}_{\mathsf{inp}(i)}$ for all $i \in [h]$, $\mathbf{x} \in \{0,1\}^\ell$. As used in the paper [12], we denote the $\prod_{i=1}^{h} \mathbf{M}_{i,\bar{\omega}(\mathbf{x})_i}$ by $\mathbf{M}_{\bar{\omega}(\mathbf{x})}$ for the product of array of matrices

A target BP $\mathbf{P} = \{\mathsf{inp}, \{\mathbf{P}_{i,b}\}_{i\in[h],b\in\{0,1\}}, \mathcal{P}_0, \mathcal{P}_1\}$, which is called *Type I* BP in the paper, satisfies the following conditions.

1. All the matrices $\mathbf{P}_{i,b}$ are $w \times w$ matrices.
2. For a vector $\mathbf{v} = \mathbf{1}^{1\times w}$, the target sets $\mathcal{P}_0, \mathcal{P}_1$ satisfies $\mathbf{v} \cdot \mathcal{P}_0 = \{\mathbf{0}^{1\times w}\}$, $\mathbf{v} \cdot \mathcal{P}_1 \neq \{\mathbf{0}^{1\times w}\}$.[6]
3. An index length h is set to $(\lambda + 1) \cdot \ell$.
4. An index-to-input function satisfies $\mathsf{inp}(i) = (i \mod \ell)$. Thus, index-to-input function iterates $\lambda + 1$ times.

Construction. CVW obfuscation is a probabilistic polynomial time algorithm which takes as input a BP $\mathbf{P}$ with an input length ℓ, and outputs an obfuscated program with the same functionality. The algorithm process consists of the following steps. Here we use new parameters $n, m, q, t := (w + 2n\ell) \cdot n, \sigma$ for the construction. We will specify the parameter settings later.

- Sample bundling matrices $\{\mathbf{R}_{i,b} \in \mathbb{Z}^{2n\ell\times 2n\ell}\}_{i\in[h],b\in\{0,1\}}$ such that $(\mathbf{1}^{1\times 2\ell}\otimes \mathbf{I}^{n\times n})\cdot \mathbf{R}_{\mathbf{x}'}\cdot(\mathbf{1}^{2\ell\times 1}\otimes \mathbf{I}^{n\times n}) = \mathbf{0} \iff \mathbf{x}' \in \bar{\omega}(\{0,1\}^\ell)$ for all $\mathbf{x}' \in \{0,1\}^h$. More precisely, $\mathbf{R}_{i,b}$ is a block diagonal matrix $\mathsf{diag}(\mathbf{R}_{i,b}^{(1)}, \mathbf{R}_{i,b}^{(2)}, \cdots, \mathbf{R}_{i,b}^{(\ell)})$. Each $\mathbf{R}_{i,b}^{(k)} \in \mathbb{Z}^{2n\times 2n}$ is one of the following three cases.

$$\mathbf{R}_{i,b}^{(k)} = \begin{cases} \mathbf{I}^{2n\times 2n} & \text{if } \mathsf{inp}(i) \neq k \\ \begin{pmatrix} \tilde{\mathbf{R}}_{i,b}^{(k)} & \\ & \mathbf{I}^{n\times n} \end{pmatrix}, \tilde{\mathbf{R}}_{i,b}^{(k)} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{n\times n} & \text{if } \mathsf{inp}(i) = k \text{ and } i \leq \lambda\ell \\ \begin{pmatrix} -\mathbf{I}^{n\times n} & \\ & \prod_{j=0}^{\lambda-1} \tilde{\mathbf{R}}_{k+j\ell,b}^{(k)} \end{pmatrix} & \text{if } \mathsf{inp}(i) = k \text{ and } i > \lambda\ell \end{cases}$$

[6] As noted in the remark of introduction, it is assumed implicitly that $\mathbf{v} = \mathbf{1}^{1\times w}$ for the targeted BP, while the definition of Type I BP uses $\mathbf{v} \in \{0,1\}^{1\times w}$.

- Sample matrices $\{\mathbf{S}_{i,b} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{n\times n}\}_{i\in[h],b\in\{0,1\}}$ and compute

$$\mathbf{J} := (\mathbf{1}^{1\times(w+2n\ell)} \otimes \mathbf{I}^{n\times n}) \in \mathbb{Z}^{n\times t}$$
$$\hat{\mathbf{S}}_{i,b} := \begin{pmatrix} \mathbf{P}_{i,b} \otimes \mathbf{S}_{i,b} & \\ & \mathbf{R}_{i,b} \otimes \mathbf{S}_{i,b} \end{pmatrix} \in \mathbb{Z}^{t\times t}$$
$$\mathbf{L} := (\mathbf{1}^{(w+2n\ell)\times 1} \otimes \mathbf{I}^{n\times n}) \in \mathbb{Z}^{t\times n}$$

- Sample $(\mathbf{A}_i, \tau_i) \leftarrow \mathsf{TrapSam}(1^t, 1^m, q)$ for $0 \le i \le h-1$, $\mathbf{A}_h \leftarrow U(\mathbb{Z}_q^{n\times n})$, $\{\mathbf{E}_{i,b} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{t\times m}\}_{i\in[h-1],b\in\{0,1\}}$ and $\{\mathbf{E}_{h,b} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{t\times n}\}_{b\in\{0,1\}}$.
- Run Sample algorithms to obtain

$$\mathbf{D}_{i,b} \in \mathbb{Z}^{m\times m} \leftarrow \mathsf{Sample}(\mathbf{A}_{i-1}, \tau_{i-1}, \hat{\mathbf{S}}_{i,b} \cdot \mathbf{A}_i + \mathbf{E}_{i,b}, \sigma) \text{ for } 1 \le i \le h-1,$$
$$\mathbf{D}_{h,b} \in \mathbb{Z}^{m\times n} \leftarrow \mathsf{Sample}(\mathbf{A}_{h-1}, \tau_{h-1}, \hat{\mathbf{S}}_{h,b} \cdot \mathbf{L} \cdot \mathbf{A}_h + \mathbf{E}_{h,b}, \sigma).$$

- Define $\mathbf{A}_{\mathbf{J}}$ as a matrix $\mathbf{J} \cdot \mathbf{A}_0 \in \mathbb{Z}^{n\times m}$ and outputs matrices

$$\left\{\mathsf{inp}, \mathbf{A}_{\mathbf{J}}, \{\mathbf{D}_{i,b}\}_{i\in[h],b\in\{0,1\}}\right\}.$$

Evaluation. Evaluation process consists of two steps. The first step is to compute a matrix $\mathbf{A}_{\mathbf{J}} \cdot \mathbf{D}_{\bar{\omega}(\mathbf{x})}$. The last step is size comparison: If $\|\mathbf{A}_{\mathbf{J}} \cdot \mathbf{D}_{\bar{\omega}(\mathbf{x})}\|_\infty \le B$, output 0 for some fixed B. Otherwise, output 1.

Parameters and Zerotest Functionality. Due to Lemma 2.4 and 2.5, $n = \Omega(\lambda \log q)$ and $\chi = D_{\mathbb{Z},2\sqrt{\lambda}}$. Moreover, for the trapdoor functionality, $m = \Omega(t \log q)$ and $\sigma = \Omega(\sqrt{t \log q})$ due to Lemma 2.7 and 2.8. From the construction of the obfuscation, the following equality always holds, which is essentially what we need.

$$[\mathbf{A}_{\mathbf{J}}\mathbf{D}_{\bar{\omega}(\mathbf{x})}]_q = \left[\mathbf{J}\left(\prod_{i=1}^{h} \hat{\mathbf{S}}_{i,x_i}\right) \cdot \mathbf{A}_h + \mathbf{J}\sum_{j=1}^{h}\left(\left(\prod_{i=1}^{j-1} \hat{\mathbf{S}}_{i,x_i}\right) \cdot \mathbf{E}_{j,x_j} \cdot \prod_{k=j+1}^{h} \mathbf{D}_{k,x_k}\right)\right]_q$$

The honest evaluation with $\mathbf{P}_{\mathbf{x}} = \mathbf{0}^{w\times w}$ gives $\hat{\mathbf{S}}_{\mathbf{x}} = \mathbf{0}^{t\times t}$ due to the construction of $\mathbf{R}_{i,b}$ is zero for the valid evaluation. Then, the following inequality holds:

$$\begin{aligned} \|[\mathbf{A}_{\mathbf{J}} \cdot \mathbf{D}_{\bar{\omega}(\mathbf{x})}]_q\|_\infty &= \left\|\left[\mathbf{J} \cdot \sum_{j=1}^{h}\left(\left(\prod_{i=1}^{j-1} \hat{\mathbf{S}}_{i,x_i}\right) \cdot \mathbf{E}_{j,x_j} \cdot \prod_{k=j+1}^{h} \mathbf{D}_{k,x_k}\right)\right]_q\right\|_\infty & (1) \\ &\le \left\|\mathbf{J} \cdot \sum_{j=1}^{h}\left(\left(\prod_{i=1}^{j-1} \hat{\mathbf{S}}_{i,x_i}\right) \cdot \mathbf{E}_{j,x_j} \cdot \prod_{k=j+1}^{h} \mathbf{D}_{k,x_k}\right)\right\|_\infty & (2) \\ &\le h \cdot \left(\max_{i,b} \|\hat{\mathbf{S}}_{i,b}\| \cdot \sigma \cdot m\right)^h & (3) \end{aligned}$$

for all but negligible probability. Therefore, the upper bound B of the error needs to be larger than

$$(w + 2n\ell) \cdot h \cdot \left(m \cdot \sigma^2 \cdot \sqrt{n(2 + 2n\ell)\sigma}\right)^h.$$

If $\mathbf{P}_{\mathbf{x}}$ is not the zero matrix, then $\hat{\mathbf{S}}_{\mathbf{x}}$ is also not the zero matrix with overwhelming probability. It implies that $\|[\mathbf{A}_{\mathbf{J}} \cdot \mathbf{D}_{\bar{\omega}(\mathbf{x})}]_q\|_\infty$ is larger than B with overwhelming property because of $\mathbf{A}_h \leftarrow U(\mathbb{Z}_q^{n\times n})$. Lastly, q is larger than $B \cdot \omega(\mathsf{poly}(\lambda))$ for the correctness of the evaluation, and $q \le (\sigma/\lambda) \cdot 2^{\lambda^{1-\epsilon}}$ for a fixed $\epsilon \in (0, 1)$ due to the security, Lemma 2.4.

4.2 Cryptanalysis of CVW Obfuscation

We apply the statistical zeroizing attack to the CVW obfuscation. As we stated in Section 3, it is enough to show that the conditions of Proposition 3.2 hold.

We stress that *every* choice of secret elements is determined by the same way as the construction of an obfuscation scheme in this section. We also note that we call all unknown matrices such as $\mathbf{E}_{i,b}, \mathbf{A}_i$ and $\mathbf{S}_{i,b}$ by *secret elements.*

Our targeted two functionally equivalent BPs $\mathbf{M} = \{\mathbf{M}_{i,b}\}_{i\in[h],b\in\{0,1\}}$ and $\mathbf{N} = \{\mathbf{N}_{i,b}\}_{i\in[h],b\in\{0,1\}}$ are of the form

$$\mathbf{M}_{i,b} = \mathbf{0}^{w\times w} \text{ for all } i,b \text{ and } \mathbf{N}_{i,b} = \begin{cases} \mathbf{1}^{w\times w} & \text{if } i=1 \\ \mathbf{0}^{w\times w} & \text{otherwise} \end{cases}.$$

Suppose that we have an obfuscated program $\mathcal{O}(\mathbf{P})$ for $\mathbf{P} = \mathbf{M}$ or $\mathbf{P} = \mathbf{N}$. Our main goal is to determine whether the program $\mathcal{O}(\mathbf{P})$ is an obfuscation of $\mathbf{M}$ or $\mathbf{N}$.

By applying Proposition 3.1, we can assume that we have polynomially many samples from the one of two distributions $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$, where $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$ denotes the distributions of the (1,1) entry of evaluation at a fixed vector $\mathbf{x}$ of the obfuscated program of $\mathbf{M}$ or $\mathbf{N}$, respectively. The probability of samples of distribution is over the choice of *all* secrets to construct obfuscation, including secrets for obfuscator.

Now our purpose is changed to deciding whether the samples comes from $\mathcal{D}_{\mathbf{M}}$ or $\mathcal{D}_{\mathbf{N}}$. To exploit Proposition 3.2, we transform the CVW construction into the language of random variables. We denote the random matrix by the capital italic words, whose entry follows a distribution that corresponds to the distribution of entry of the bold matrix. For example, the entry of random matrix $E_{i,b}$ follows the distribution $\mathcal{D}_{\mathbb{Z},\sigma}$ since the matrix $\mathbf{E}_{i,b}$ is chosen from $\mathcal{D}_{\mathbb{Z},\sigma}^{t\times m}$ in the CVW construction. More precisely, we define random matrices $\tilde{R}_{i,b}^{(k)}$ following $\mathcal{D}_{\mathbb{Z},\sigma}^{n\times n}$, $S_{i,b}$ following $\mathcal{D}_{\mathbb{Z},\sigma}^{n\times n}$ and A_i as in the trapdoor sampling algorithm. Then we obtain random matrices $\hat{S}_{i,b}^{(\mathbf{P})}$, $R_{i,b}^{(\mathbf{P})}$, $E_{i,b}^{(\mathbf{P})}$ and $D_{i,b}^{(\mathbf{P})}$ as in the construction of CVW obfuscation for the branching programs $\mathbf{P} = \mathbf{M}$ or $\mathbf{N}$. We note that only $\hat{S}_{i,b}^{(\mathbf{P})}$ and $D_{i,b}^{(\mathbf{P})}$ depend on the choice of branching program, but we put $\mathbf{P}$ in some other random variables for convenience of distinction.

Under this setting, it suffices to show the following proposition.

Proposition 4.1 *Let $X_{\mathbf{M}}$ and $X_{\mathbf{N}}$ be random variables satisfying*

$$X_{\mathbf{M}} = \left[\left(\mathbf{J}\cdot A_0 \cdot D_{\bar{\omega}(\mathbf{x})}^{(\mathbf{M})}\right)_{(1,1)}\right]_q, \quad X_{\mathbf{N}} = \left[\left(\mathbf{J}\cdot A_0 \cdot D_{\bar{\omega}(\mathbf{x})}^{(\mathbf{N})}\right)_{(1,1)}\right]_q.$$

Let $\sigma_{\mathbf{M}}^2$ and $\sigma_{\mathbf{N}}^2$ be variance of the random variables of $X_{\mathbf{M}}$ and $X_{\mathbf{N}}$, respectively.

Then, it holds that

$$\left|\frac{\max(E[X_{\mathbf{N}}^2], E[X_{\mathbf{M}}^2])}{\sigma_{\boldsymbol{N}}^2 - \sigma_{\boldsymbol{M}}^2}\right| \le p(\lambda), \quad \left|\frac{E[X_{\mathbf{N}}^4]}{E[X_{\mathbf{N}}^2]^2}\right| \le q(\lambda), \text{ and } \left|\frac{E[X_{\mathbf{M}}^4]}{E[X_{\mathbf{M}}^2]^2}\right| \le q(\lambda).$$

for some $p, q = \mathsf{poly}(\lambda)$.

The honest evaluation of the CVW obfuscation $[\mathbf{A}_{\mathbf{J}} \cdot \mathbf{D}_{\bar{\omega}(\mathbf{x})}^{(\mathbf{P})}]_q$ is the matrix of the form

$$\mathbf{J}\cdot\sum_{j=1}^{h}\left(\left(\prod_{i=1}^{j}\hat{\mathbf{S}}_{i,x_i}\right)\cdot\mathbf{E}_{j+1,x_{j+1}}\cdot\prod_{k=j+2}^{h}\mathbf{D}_{k,x_k}^{(\mathbf{P})}\right),$$

which does not contain the term including the trapdoor matrices $\mathbf{A}_i$ for $i = 0, \cdots, h-1$. Thus, to establish the statistical properties including a variance in Proposition 4.1, it suffices to analyze the statistical properties of the random matrices $\hat{S}_{i,b}^{(\mathbf{P})}$, $E_{i,b}^{(\mathbf{P})}$, $D_{i,b}^{(\mathbf{P})}$ and their products.

To approximate the statistical values of the evaluations, we consider random variables $\tilde{D}_{i,b}^{(\mathbf{P})}$'s whose columns correspond to $\mathcal{D}_{\mathbb{Z}^m,\sigma}$ instead of the $D_{i,b}^{(\mathbf{P})}$'s in the following lemmas. Since the corresponding distributions of $D_{i,b}^{(\mathbf{P})}$'s and $\tilde{D}_{i,b}^{(\mathbf{P})}$'s are statistically close, it is enough to show the lemmas and conditions of Proposition 3.2 using $\tilde{D}_{i,b}^{(\mathbf{P})}$'s.[7]

More precisely, we consider the random variable

$$Z_{\mathbf{P}} = \mathbf{J} \cdot \sum_{j=1}^{h} \left(\left(\prod_{i=1}^{j} \hat{S}_{i,x_i} \right) \cdot E_{j+1,x_{j+1}} \cdot \prod_{k=j+2}^{h} \tilde{D}_{k,x_k}^{(\mathbf{P})} \right)$$

for $\mathbf{P} = \mathbf{M}$ or $\mathbf{N}$. The lemmas are stated with the random variables $Z_{\mathbf{M}}$ and $Z_{\mathbf{N}}$, but the statistical closeness of two distribution $\tilde{D}_{i,b}^{(\mathbf{P})}$ and $D_{i,b}^{(\mathbf{P})}$ induces that the same results hold for $X_{\mathbf{M}}$ and $X_{\mathbf{N}}$ with overwhelming probability.

Now we give the lemmas to prove Proposition 4.1. The proofs of lemmas are placed in Appendix D and sub-lemmas in Appendix C. The proof of Proposition 4.1 using the lemmas is placed in the concluding part of this section.

For the convenience of the statement, let $(Z_{1,1}^{(\mathbf{M})})_j$ be random variables of $(1,1)$-th entry of the random matrices

$$\mathbf{J} \cdot \prod_{i=1}^{j} \hat{S}_i^{(\mathbf{M})} \cdot E_{j+1}^{(\mathbf{M})} \cdot \prod_{k=j+2}^{h} \tilde{D}_k^{(\mathbf{M})}$$

for $j = 0, 1, \cdots, h-1$. In this notation, $Z_{\mathbf{M}}$ be the summation of $(Z_{1,1}^{(\mathbf{M})})_j$ for $j \in \{0, 1, \cdots, h-1\}$. Similarly, we define $(Z_{1,1}^{(\mathbf{N})})_j$ for all $j = 0, \cdots, h-1$ and $Z_{\mathbf{N}}$.

Lemma 4.2 $E[(Z_{1,1}^{(\mathbf{M})})_{\mu_1} \cdot (Z_{1,1}^{(\mathbf{M})})_{\mu_2}] = E[(Z_{1,1}^{(\mathbf{N})})_{\mu_1} \cdot (Z_{1,1}^{(\mathbf{N})})_{\mu_2}] = 0$ *for* $\mu_1 \neq \mu_2$.

Lemma 4.3 **($j = 0$)** *It holds that*

$$Var[(Z_{1,1}^{(\mathbf{M})})_0] = Var[(Z_{1,1}^{(\mathbf{N})})_0] = (w + 2n\ell) \cdot m^{h-1} \cdot \sigma^{2h} \text{ and}$$
$$\left| \frac{E[(Z_{1,1}^{(\mathbf{M})})_0^4]}{Var[(Z_{1,1}^{(\mathbf{M})})_0]^2} \right|, \left| \frac{E[(Z_{1,1}^{(\mathbf{N})})_0^4]}{Var[(Z_{1,1}^{(\mathbf{N})})_0]^2} \right| \leq 3 \cdot (w + 2n\ell)^2 \cdot (1 + \frac{2}{m})^{h-1} = \mathsf{poly}(\lambda).$$

Lemma 4.4 **($j = 1$)** *It holds that*

$$Var[(Z_{1,1}^{(\mathbf{M})})_1] = \Big(n^3\sigma^2 + (2\ell - 1) \cdot n^2\Big) \cdot m^{h-2}(\sigma^2)^h,$$
$$Var[(Z_{1,1}^{(\mathbf{N})})_1] = \Big(w^3 \cdot n + n^3 \cdot \sigma^2 + (2\ell - 1) \cdot n^2\Big) \cdot m^{h-2}(\sigma^2)^h$$
$$\left| \frac{E[(Z_{1,1}^{(\mathbf{M})})_1^4]}{Var[(Z_{1,1}^{(\mathbf{M})})_1]^2} \right|, \left| \frac{E[(Z_{1,1}^{(\mathbf{N})})_1^4]}{Var[(Z_{1,1}^{(\mathbf{N})})_1]^2} \right| \leq 27(w + 2n\ell)^4 n^2 (1 + \frac{2}{n})^{j_1+j-1}(1 + \frac{2}{m})^{h-j-1}$$
$$= \mathsf{poly}(\lambda).$$

Lemma 4.5 **($1 < j \leq \lambda \cdot \ell$)** *Let j be a fixed integer such that $j = \ell \cdot j_1 + j_2 > 1$ for $0 \leq j_2 < \ell$ such that $2 \leq j \leq \lambda \cdot \ell$. Then, it holds that*

$$Var[(Z_{1,1}^{(\mathbf{M})})_j] = Var[(Z_{1,1}^{(\mathbf{N})})_j]$$
$$= \Big(j_2 n^{j+j_1+2}(\sigma^2)^{j_1+1} + (\ell - j_2) n^{j+j_1+1}(\sigma^2)^{j_1} + \ell n^{j+1}\Big) m^{h-j-1}(\sigma^2)^h.$$

Moreover, it holds that

$$\left| \frac{E[(Z_{1,1}^{(\mathbf{M})})_j^4]}{Var[(Z_{1,1}^{(\mathbf{M})})_j]^2} \right|, \left| \frac{E[(Z_{1,1}^{(\mathbf{N})})_j^4]}{Var[(Z_{1,1}^{(\mathbf{N})})_j]^2} \right| \leq 27(w + 2n\ell)^4 \cdot n^2 \left(1 + \frac{2}{n}\right)^{j_1+j-1} \left(1 + \frac{2}{m}\right)^{h-j-1}$$
$$= \mathsf{poly}(\lambda).$$

[7] We remark that there is a subtle gap in this argument. In fact this argument already used in the correctness of the obfuscation and many statistical analysis on the trapdoor samplings in spite of the presence of the gap. We discuss this problem in Appendix B.

Lemma 4.6 ($j > \lambda \cdot \ell$)) *Let j be a fixed integer such that $j > \lambda \cdot \ell$. Then, it holds that*

$$\begin{aligned} Var[(Z^{(\mathbf{M})}_{1,1})_j] &= Var[(Z^{(\mathbf{N})}_{1,1})_j] \\ &= \Big((\ell + j_2) \cdot n^{\lambda+j+1} \cdot (\sigma^2)^{\lambda} + (\ell - j_2) \cdot n^{j+1}\Big) \cdot m^{h-j-1} \cdot (\sigma^2)^h. \end{aligned}$$

In addition, it holds that

$$\begin{aligned} \left|\frac{E[(Z^{(\mathbf{M})}_{1,1})^4_j]}{Var[(Z^{(\mathbf{M})}_{1,1})_j]^2}\right|, \left|\frac{E[(Z^{(\mathbf{N})}_{1,1})^4_j]}{Var[(Z^{(\mathbf{N})}_{1,1})_j]^2}\right| &\le 27(w + 2n\ell)^4 n^2 \left(1 + \frac{2}{n}\right)^{\lambda+j-2} \left(1 + \frac{2}{m}\right)^{h-j-1} \\ &= \mathsf{poly}(\lambda). \end{aligned}$$

Now we give a proof of the proposition 4.1 using above lemmas.

Proof (of Proposition 4.1). Using the results of lemmas, we can prove the proposition by analyzing the summation of random matrices in the above lemmas. We first verify the results for $Z_{\mathbf{M}}$. The same result holds for $Z_{\mathbf{N}}$ since the bounds of lemmas are the same.

Since $Z_{\mathbf{M}}$ is equal to $\sum_{j=0}^{h-1} (Z^{(\mathbf{M})}_{1,1})_j$, we have

$$Var[Z_{\mathbf{M}}] = E\left[(\sum_{j=0}^{h-1} (Z^{(\mathbf{M})}_{1,1})_j)^2\right] = E\left[\sum_{j=0}^{h-1} (Z^{(\mathbf{M})}_{1,1})^2_j\right].$$

Applying the Cauchy-Schwarz inequality, it also holds

$$E[Z^4_{\mathbf{M}}] = E\left[(\sum_{j=0}^{h-1} (Z^{(\mathbf{M})}_{1,1})_j)^4\right] \le E\left[h^3 \cdot (\sum_{j=0}^{h-1} (Z^{(\mathbf{M})}_{1,1})^4_j)\right].$$

Diving both sides by $Var[Z_{\mathbf{M}}]^2$, we obtain the inequality

$$\begin{aligned} \left|\frac{E[Z^4_{\mathbf{M}}]}{Var[Z_{\mathbf{M}}]^2}\right| &\le \left|\frac{E[h^3 \cdot (\sum_{j=0}^{h-1} (Z^{(\mathbf{M})}_{1,1})^4_j)]}{Var[Z_{\mathbf{M}}]^2}\right| = h^3 \cdot \left|\frac{E[\sum_{j=0}^{h-1} (Z^{(\mathbf{M})}_{1,1})^4_j]}{Var[Z_{\mathbf{M}}]^2}\right| \\ &= h^3 \cdot \sum_{j=0}^{h-1} \left|\frac{E[(Z^{(\mathbf{M})}_{1,1})^4_j]}{Var[Z_{\mathbf{M}}]^2}\right| \le h^3 \cdot \sum_{j=0}^{h-1} \left|\frac{E[(Z^{(\mathbf{M})}_{1,1})^4_j]}{Var[(Z^{(\mathbf{M})}_{1,1})_j]^2}\right|. \end{aligned}$$

By Lemma 4.3,4.4,4.5 and 4.6, $\left|\frac{E[(Z^{(\mathbf{M})}_{1,1})^4_j]}{Var[(Z^{(\mathbf{M})}_{1,1})_j]^2}\right|$ is bounded by $\mathsf{poly}(\lambda)$ for all $i = 0, 1, \cdots, h-1$ regardless of $\mathbf{P} = \mathbf{M}$ or $\mathbf{P} = \mathbf{N}$. Therefore, the following inequality holds.

$$\left|\frac{E[Z^4_{\mathbf{M}}]}{Var[Z_{\mathbf{M}}]^2}\right| \le \mathsf{poly}(\lambda) =: q(\lambda)$$

Moreover, we can compute the exact values $E[Z^2_{\mathbf{M}}] = Var[Z_{\mathbf{M}}]^2 = \sum_{j=0}^{h-1} Var[(Z^{(\mathbf{M})}_{1,1})_j]^2$, the same for $Z_{\mathbf{N}}$ and the difference $Var[Z_{\mathbf{M}}]^2 - Var[Z_{\mathbf{N}}]$ using lemmas; these computations directly show that $\left|\frac{\max(E[Z^2_{\mathbf{N}}], E[Z^2_{\mathbf{M}}])}{Var[Z_{\mathbf{N}}]^2 - Var[Z_{\mathbf{M}}]^2}\right| = poly(\lambda)$ holds.

At last the statistical closeness of distributions completes the proof for $X_{\mathbf{M}}$ and $X_{\mathbf{N}}$. □

Remark 1. In the original paper [12], the authors give two different choice of the distributions of $\mathbf{E}_{i,b}$; $\mathcal{D}_{\mathbb{Z},\sigma}$ with corresponding dimension in Section 11, and $\chi = \mathcal{D}_{\mathbb{Z},2\sqrt{\lambda}}$ with appropriate dimension in Section 5. We analyze the obfuscation with distribution $\mathcal{D}_{\mathbb{Z},\sigma}$ stated in the construction but the result still holds for $\chi = \mathcal{D}_{\mathbb{Z},2\sqrt{\lambda}}$ with slight modification.

5 Crtypanalysis of BGMZ Obfuscation

In this section, we briefly review the BGMZ obfuscation and show the obfuscation fails to achieve the desired security.

5.1 Construction of BGMZ Obfuscation

Bartusek *et al.* proposed a new candidate of iO which is secure in the GGH15 zeroizing model. We briefly review the construction of this candidate scheme. For more detail, we refer to an original paper [4].

We start with the conditions of BP they used. The authors use a dual-input binary BP's. *i.e.*, $\mathsf{inp}(i) = (\mathsf{inp}_1(i), \mathsf{inp}_2(i))$. For simplicity, they use the notation $\boldsymbol{x}(i) = (x_{\mathsf{inp}_1(i)}, x_{\mathsf{inp}_2(i)})$. Moreover, they employ the new parameter $\eta = \mathsf{poly}(\ell, \lambda)$ with $\eta \geq \ell^4$ which decides the minimum number of the BP layer.

The targeted BP $\mathbf{P}$ also satisfies the following conditions.

1. All the matrices $\{\mathbf{P}_{i,\boldsymbol{b}}\}_{i\in[h],\boldsymbol{b}\in\{0,1\}^2}$ are $w \times w$ matrices.
2. $\prod_{i=1}^{h} \mathbf{P}_{i,\boldsymbol{x}(i)} = \mathbf{0}^{w\times w}$.
3. Each pair of input bits (j, k) is read in at least $4\ell^2$ different layers of branching program.
4. There exist layers $i_1 < i_2 < \cdots < i_t$ such that $\mathsf{inp}_1(i_1), \cdots, \mathsf{inp}_1(i_\eta)$ cycles η/ℓ times through $[\ell]$.

To obfuscate a branching program that does not satisfy the condition 3 or 4, we pad the identity matrices to satisfy the conditions while preserving the functionality. Moreover, they employ the asymmetric level construction to generate straddling sets used to enforce the honest evaluation.[8]

Construction. BGMZ obfuscation is a probabilistic polynomial time algorithm which takes as input a BP $\mathbf{P}$ with a length h, and outputs an obfuscated program with the same functionality. We use several parameter such as $n, m, q, t := (w+1)\cdot n, \sigma, \nu, g$ in the construction. We will describe the setting for new parameters such as g, ν later.

The obfuscation procedure consists of the following steps.

- Sample $(\mathbf{A}_i, \tau_i) \leftarrow \mathsf{TrapSam}(1^t, 1^m, q)$ for $0 \leq i \leq h-1$, $\mathbf{A}_h \leftarrow U(\mathbb{Z}_q^{t\times m})$, $\{\mathbf{E}_{i,\boldsymbol{b}} \leftarrow \chi_{\mathbb{Z},\sigma}^{t\times m}\}_{i\in[h-1],\boldsymbol{b}\in\{0,1\}^2}$ and $\mathbf{E}_h \leftarrow \chi_{\mathbb{Z},\sigma}^{t\times m}$ where $t := (w+1)\cdot n$.
- Sample matrices $\mathbf{B}_{i,\boldsymbol{b}} \in \mathbb{Z}_\nu^{g\times g}$ and invertible matrices $\mathbf{R}_i \in \mathbb{Z}_q^{(m+g)\times(m+g)}$ randomly.
- Sample matrices $\{\mathbf{S}_{i,\boldsymbol{b}} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{n\times n}\}_{i\in[h-1],\boldsymbol{b}\in\{0,1\}^2}$ and a final encoding $\mathbf{D}_h$ as

$$\mathbf{D}_h \in \mathbb{Z}^{m\times m} \leftarrow \mathsf{Sample}(\mathbf{A}_{h-1}, \tau_{h-1}, \begin{pmatrix} \mathbf{I}^{wn\times wn} & \\ & \mathbf{0}^{n\times n} \end{pmatrix} \cdot \mathbf{A}_h + \mathbf{E}_h, \sigma),$$

  and compute bookend vectors $\mathbf{v}$ and $\mathbf{w}$ as

$$\mathbf{v} = [\mathbf{v}' \cdot \mathbf{J} \cdot \mathbf{A}_0 \mid \mathbf{b}_v] \cdot \mathbf{R}_1,$$

$$\hat{\mathbf{S}}_{i,\boldsymbol{b}} := \begin{pmatrix} \mathbf{P}_{i,\boldsymbol{b}} \otimes \mathbf{S}_{i,\boldsymbol{b}} & \\ & \mathbf{S}_{i,\boldsymbol{b}} \end{pmatrix} \in \mathbb{Z}^{t\times t}$$

$$\mathbf{w}^T = \mathbf{R}_h^{-1} \cdot \begin{pmatrix} \mathbf{D}_h \cdot \mathbf{w}'^T \\ \mathbf{b}_w^T \end{pmatrix}$$

  where $\mathbf{v}' \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^n$, $\mathbf{w}' \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^m$, $\mathbf{b}_v, \mathbf{b}_w \leftarrow U(\mathbb{Z}_\nu^k)$ and $\mathbf{J} := [\mathbf{J}'|\mathbf{I}^{n\times n}]$ with a randomly chosen matrix $\mathbf{J}' \leftarrow \{0,1\}^{n\times wn}$.
- Compute matrices

$$\mathbf{D}_{i,} \in \mathbb{Z}^{m\times m} \leftarrow \mathsf{Sample}(\mathbf{A}_{i-1}, \tau_{i-1}, \hat{\mathbf{S}}_{i,\boldsymbol{b}} \cdot \mathbf{A}_i + \mathbf{E}_{i,\boldsymbol{b}}, \sigma) \text{ with } 1 \leq i \leq h-1,$$

$$\text{and } \mathbf{C}_{i,\boldsymbol{b}} = \mathbf{R}_i^{-1} \cdot \begin{pmatrix} \mathbf{D}_{i,\boldsymbol{b}} & \\ & \mathbf{B}_{i,\boldsymbol{b}} \end{pmatrix} \cdot \mathbf{R}_{i+1} \text{ with } i = 1, \cdots, h-1.$$

[8] We omitted the *straddling set* and *level parameters*, because they prohibit *invalid* evaluations and do not affect anything on the valid evaluations. Our attack only exploits the valid encodings.

Evaluation. Outputs 0 if $|\mathbf{v}\cdot\prod_{i=1}^{h-1}\mathbf{C}_{i,\boldsymbol{x}(i)}\cdot\mathbf{w}^T|\leq B$. Otherwise, outputs 1.

Parameters and Zerotest Functionality. Let λ_{LWE} and λ_{SZ} be security parameters depending on the hardness of LWE and the security of the model in the paper [4], respectively. Both parameters are $\mathsf{poly}(\lambda)$ for the security parameter λ, but $\lambda_{LWE}\gg\lambda_{SZ}$ for the zerotesting functionality. Due to Lemmas 2.4 and 2.5, they set $n=\Omega(\lambda_{LWE}\log q)$, $\chi=\mathcal{D}_{\mathbb{Z},s}$ with $s=\Omega(\sqrt{n})$. Moreover, for the trapdoor functionality, the authors set $m=\Omega(t\log q)$ and $\sigma=\Omega(\sqrt{t\log q})$ due to Lemma 2.7 and 2.8. In addition, they use parameters $g=5$ and $\nu=\mathsf{poly}(\lambda_{SZ})$.

Moreover, from the construction of obfuscation, the following equality always holds if $\mathbf{C}:=\prod_{i=1}^{h-1}\mathbf{C}_{i,\boldsymbol{x}(i)}$ is an encoding of zero computed by honest evaluation.

$$\begin{aligned}
&\|[\mathbf{v}\cdot\mathbf{C}\cdot\mathbf{w}^T]_q\|_\infty\\
&=\left\|\left[\mathbf{v}'\cdot\mathbf{J}\sum_{j=1}^{h}((\prod_{i=1}^{j-1}\hat{\mathbf{S}}_{i,\boldsymbol{x}(i)})\mathbf{E}_{j,\boldsymbol{x}(j)}\prod_{k=j+1}^{h}\mathbf{D}_{k,\boldsymbol{x}(k)}\cdot\mathbf{w}'^T+\mathbf{b}_v\cdot\prod_{i=1}^{h-1}\mathbf{B}_{i,x(i)}\cdot\mathbf{b}_w^T\right]_q\right\|_\infty\\
&\leq\left\|\mathbf{v}'\cdot\mathbf{J}\sum_{j=1}^{h}((\prod_{i=1}^{j-1}\hat{\mathbf{S}}_{i,\boldsymbol{x}(i)})\mathbf{E}_{j,\boldsymbol{x}(j)}\prod_{k=j+1}^{h}\mathbf{D}_{k,\boldsymbol{x}(k)}\cdot\mathbf{w}'^T+\mathbf{b}_v\cdot\prod_{i=1}^{h-1}\mathbf{B}_{i,x(i)}\cdot\mathbf{b}_w^T\right\|_\infty\\
&\leq\sigma^2\cdot m^2\cdot(m\cdot\beta\cdot\sigma\cdot\sqrt{t})^{h-1}+(k\cdot\nu)^{h+1}
\end{aligned}$$

Since $\|[\mathbf{v}\cdot\mathbf{C}\cdot\mathbf{w}^T]_q\|_\infty$ is bounded by $\sigma^2\cdot m^2\cdot(m\cdot\beta\cdot\sigma\cdot\sqrt{t})^{h-1}+(k\cdot\nu)^{h+1}$ for all but negligible probability, the zerotest bound is set to $B:=(m\cdot\beta\cdot\sigma\sqrt{t})^{h+1}$. Moreover, if $\prod_{i=1}^{h}\mathbf{P}_{i,\boldsymbol{x}(i)}$ is a nonzero matrix, then $\prod_{i=1}^{h}\hat{\mathbf{S}}_{i,\boldsymbol{x}(i)}$ is also nonzero matrix. Thus, $\|[\mathbf{v}\cdot\mathbf{C}\cdot\mathbf{w}^T]_q\|_\infty$ is larger than B with overwhelming probability because of $\mathbf{A}_h\leftarrow U(\mathbb{Z}_q^{t\times m})$.

Lastly, q is chosen so that

$$q\geq B\cdot\omega(\mathsf{poly}(\lambda_{SZ}))\text{ and }q\leq(\sigma/\lambda_{LWE})\cdot 2^{\lambda_{LWE}^{1-\epsilon}}$$

for some fixed $\epsilon\in(0,1)$.

5.2 Cryptanalysis of BGMZ Obfuscation

In this section, we analyze the conditions for the statistical zeroizing attack on the BGMZ obfuscation. As in Section 4.2, the notation written in the capital italic words are regarded as the random matrix whose entry follows a distribution that corresponds to the distribution of entry of the bold-written matrix.

The targeted BPs are $\mathbf{M}=\{\mathbf{M}_{i,\boldsymbol{b}}\}_{i\in[h],\boldsymbol{b}\in\{0,1\}^2}$ and $\mathbf{N}=\{\mathbf{N}_{i,\boldsymbol{b}}\}_{i\in[h],\boldsymbol{b}\in\{0,1\}^2}$ such that

$$\mathbf{M}_{i,\boldsymbol{b}}=\begin{cases}\mathbf{0}^{w\times w} & \text{if } i=1\\ \mathbf{I}^{w\times w} & \text{otherwise}\end{cases}\text{ and }\mathbf{N}_{i,\boldsymbol{b}}=\begin{cases}\mathbf{0}^{w\times w} & \text{if } i=2\\ \mathbf{I}^{w\times w} & \text{otherwise}\end{cases}.$$

Note that two branching programs always output zero. Now we suppose that we have polynomially many samples from the one of two distributions $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$, where $\mathcal{D}_{\mathbf{M}}$ and $\mathcal{D}_{\mathbf{N}}$ are the distributions of the evaluations of obfuscations of $\mathbf{M}$ and $\mathbf{N}$.

Then our purpose is to distinguish whether the samples come from $\mathcal{D}_{\mathbf{M}}$ or $\mathcal{D}_{\mathbf{N}}$ by applying Proposition 3.1 and 3.2. We obtain random matrices $S_{i,\mathbf{b}}^{(\mathbf{P})}$, $E_{i,\boldsymbol{b}}^{(\mathbf{P})}$, $D_{i,\boldsymbol{b}}^{(\mathbf{P})}$ and $C_{i,\boldsymbol{b}}^{(\mathbf{P})}$ as in the construction of BGMZ obfuscation for branching programs $\mathbf{P}=\mathbf{M}$ or $\mathbf{N}$. As in the CVW case, it suffices to prove Proposition 5.1.

Proposition 5.1 *Let $X_{\mathbf{M}}$ and $X_{\mathbf{N}}$ be random variables satisfying*

$$X_{\mathbf{M}}=\left[v\cdot\prod_{i=1}^{h-1}C_{i,\boldsymbol{x}(i)}^{(\mathbf{M})}\cdot w^T\right]_q\text{ and }X_{\mathbf{N}}=\left[v\cdot\prod_{i=1}^{h-1}C_{i,\boldsymbol{x}(i)}^{(\mathbf{N})}\cdot w^T\right]_q.$$

Let $\sigma_{\mathbf{M}}^2$ and $\sigma_{\mathbf{N}}^2$ be variance of the random variables of $X_{\mathbf{M}}$ and $X_{\mathbf{N}}$, respectively. Then, it holds that

$$\left|\frac{\max(E[X_{\mathbf{N}}^2], E[X_{\mathbf{M}}^2])}{\sigma_{\boldsymbol{N}}^2 - \sigma_{\boldsymbol{M}}^2}\right| \leq p(\lambda), \quad \left|\frac{E[X_{\mathbf{N}}^4]}{E[X_{\mathbf{N}}^2]^2}\right| \leq q(\lambda), \text{ and } \left|\frac{E[X_{\mathbf{M}}^4]}{E[X_{\mathbf{M}}^2]^2}\right| \leq q(\lambda).$$

for some $p, q = \mathsf{poly}(\lambda)$.

With the honest evaluation of the BGMZ obfuscation $\left[\mathbf{v}\cdot\prod_{i=1}^{h}\mathbf{C}_{i,\boldsymbol{x}(i)}\cdot\mathbf{w}^T\right]_q$, we obtain an integer of the form

$$\mathbf{v}'\cdot\mathbf{J}\sum_{j=1}^{h}((\prod_{i=1}^{j-1}\hat{\mathbf{S}}_{i,\boldsymbol{x}(i)})\mathbf{E}_{j,\boldsymbol{x}(j)}\prod_{k=j+1}^{h}\mathbf{D}_{k,\boldsymbol{x}(k)}\cdot\mathbf{w}'^T + \mathbf{b}_v\cdot\prod_{i=1}^{h-1}\mathbf{B}_{i,\boldsymbol{x}(i)}\cdot\mathbf{b}_w^T$$

which does not contain the term including the trapdoor matrices $\mathbf{A}_i$'s. Thus, similarly to the CVW obfuscation case, we need to analyze the statistical properties of the random vectors $v'^{(\mathbf{P})}$, $w'^{(\mathbf{P})}$, $b_v^{(\mathbf{P})}$, $b_w^{(\mathbf{P})}$ and random matrices $\hat{S}_{i,\boldsymbol{b}}^{(\mathbf{P})}$, $E_{i,\boldsymbol{b}}^{(\mathbf{P})}$, $D_{i,\boldsymbol{b}}^{(\mathbf{P})}$ and their products to prove the statistical properties including the variance in Proposition 5.1.

As stated in Section 4, we use new random variables $\tilde{D}_{i,\boldsymbol{b}}^{(\mathbf{P})}$ for $\mathbf{P} = \mathbf{M}$ or $\mathbf{N}$ whose columns are identical to $\mathcal{D}_{\mathbb{Z}^m,\sigma}$, instead of $D_{i,\boldsymbol{b}}^{(\mathbf{P})}$. Though our analysis focus on $\tilde{D}_{i,\boldsymbol{b}}^{(\mathbf{P})}$ cases, our attack still hold due to the statistical closeness of $D_{i,\boldsymbol{b}}^{(\mathbf{P})}$ and $\tilde{D}_{i,\boldsymbol{b}}^{(\mathbf{P})}$.

The proof of Proposition 5.1 is based on the following lemmas and placed in the concluding part of this section. All proofs of these lemmas are in Appendix E.

For the convenience of the statement, let $(Z^{(\mathbf{M})})_j$ be a random variable of the form

$$v'^{(\mathbf{M})}\cdot J^{(\mathbf{M})}\cdot\prod_{i=1}^{j}\hat{S}_{i,\boldsymbol{x}(i)}^{(\mathbf{M})}\cdot E_{j+1,\boldsymbol{x}(j+1)}^{(\mathbf{M})}\cdot\prod_{k=j+2}^{h}\tilde{D}_{k,\boldsymbol{x}(k)}^{(\mathbf{M})}\cdot w'^{(\mathbf{M})^T}$$

for $j = 0, 1, \cdots, h-1$. For the case of $j = h$, $(Z^{(\mathbf{M})})_h$ be a random variable of the form

$$b_v^{(\mathbf{M})}\cdot\prod_{i=1}^{h-1}B_{i,\boldsymbol{x}(i)}^{(\mathbf{M})}\cdot b_w^{(\mathbf{M})^T}.$$

Similarly, we define $(Z^{(\mathbf{N})})_j$ for $j = 0, 1, \cdots, h$ and $Z_{\mathbf{P}} = \sum_{i=0}^{h}(Z^{(\mathbf{P})})_j$ for $\mathbf{P} = \mathbf{M}$ and $\mathbf{N}$.

Lemma 5.2 *$E[(Z^{(\mathbf{M})})_{\mu_1}\cdot(Z^{(\mathbf{M})})_{\mu_2}] = 0$ for $\mu_1 \neq \mu_2$.*

Lemma 5.3 ($j = 0$) *It holds that*

$$Var[(Z^{(\mathbf{M})})_0] = Var[(Z^{(\mathbf{N})})_0] = nm\cdot(\frac{w}{2}+1)\cdot m^{h-1}\cdot(\sigma^2)^{h+1}\cdot s^2 \text{ and}$$

$$\left|\frac{E[(Z^{(\mathbf{M})})_0^4]}{Var[(Z^{(\mathbf{M})})_0]^2}\right|, \quad \left|\frac{E[(Z^{(\mathbf{N})})_0^4]}{Var[(Z^{(\mathbf{N})})_0]^2}\right| \leq 108\cdot(nm)^2\cdot(w+1)^2\cdot\left(1+\frac{2}{m}\right)^{h-1}$$
$$= \mathsf{poly}(\lambda).$$

Lemma 5.4 ($j = 1$) *It holds that*

$$Var[(Z^{(\mathbf{M})})_1] = nm\cdot n\cdot m^{h-2}\cdot(\sigma^2)^{h+1}\cdot s^2,$$
$$Var[(Z^{(\mathbf{N})})_1] = nm\cdot\left(\frac{1}{2}\cdot wn+1\right)\cdot n\cdot m^{h-2}\cdot(\sigma^2)^{h+1}\cdot s^2.$$

Moreover, it holds that

$$\left|\frac{E[(Z^{(\mathbf{M})})_1^4]}{Var[(Z^{(\mathbf{M})})_1]^2}\right| \leq 81\cdot(nm)^2\cdot n^2\cdot\left(1+\frac{2}{m}\right)^{h-2} = \mathsf{poly}(\lambda),$$
$$\left|\frac{E[(Z^{(\mathbf{N})})_1^4]}{Var[(Z^{(\mathbf{N})})_1]^2}\right| \leq 324\cdot(nm)^2\cdot\{(w+1)n\}^2\cdot n^2\cdot\left(1+\frac{1}{m}\right)^{h-2}$$
$$= \mathsf{poly}(\lambda).$$

Lemma 5.5 **($2 \leq j \leq h-1$)** *It holds that*

$$Var[(Z^{(\mathbf{M})})_j] = Var[(Z^{(\mathbf{N})})_j] = nm \cdot n^j \cdot m^{h-j-1} \cdot (\sigma^2)^{h+1} \cdot s^2.$$

Moreover, it holds that

$$\left|\frac{E[(Z^{(\mathbf{M})})_j^4]}{Var[(Z^{(\mathbf{M})})_j]^2}\right|, \left|\frac{E[(Z^{(\mathbf{N})})_j^4]}{Var[(Z^{(\mathbf{N})})_j]^2}\right| \leq 81(nm)^2 \cdot n^2 \left(1+\frac{2}{n}\right)^{j-1} \left(1+\frac{2}{m}\right)^{h-j-1}$$
$$= \mathsf{poly}(\lambda).$$

Lemma 5.6 **($j = h$)** *It holds that*

$$Var[(Z^{(\mathbf{M})})_h] = Var[(Z^{(\mathbf{N})})_h] = g^h \cdot \left\{\frac{1}{12} \cdot v(v+2)\right\}^{h+1}.$$

Moreover, it holds that

$$\left|\frac{E[(Z^{(\mathbf{M})})_h^4]}{Var[(Z^{(\mathbf{M})})_h]^2}\right|, \left|\frac{E[(Z^{(\mathbf{N})})_h^4]}{Var[(Z^{(\mathbf{N})})_h]^2}\right| \leq 27 \cdot (g^2)^2 \cdot \left(1+\frac{2}{g}\right)^{h-2}$$
$$= \mathsf{poly}(\lambda).$$

Now we give a proof of the proposition 5.1 using the above lemmas.

Proof (of Proposition 5.1). Note that elements $(Z^{(\mathbf{M})})_j$ in the above lemmas are of the form

$$(Z^{(\mathbf{M})})_j = v'^{(\mathbf{M})} \cdot J^{(\mathbf{M})} \cdot \prod_{i=1}^{j} \hat{S}^{(\mathbf{M})}_{i,\boldsymbol{x}(i)} \cdot E^{(\mathbf{M})}_{j+1,\boldsymbol{x}(j+1)} \cdot \prod_{k=j+2}^{h} \tilde{D}^{(\mathbf{M})}_{k,\boldsymbol{x}(k)} \cdot w'^{(\mathbf{M})^T} \quad \textit{for } j < h$$

$$(Z^{(\mathbf{M})})_h = b_v^{(\mathbf{M})} \cdot \prod_{i=1}^{h-1} B^{(\mathbf{M})}_{i,\boldsymbol{x}(i)} \cdot b_w^{(\mathbf{M})^T}$$

Let $Z_{\mathbf{M}}$ be the summation of $(Z^{(\mathbf{M})})_j$ for $j \in \{0, 1, \cdots, h\}$. We have

$$Var[Z_{\mathbf{M}}] = E\left[(\sum_{i=0}^{h}(Z^{(\mathbf{M})})_i)^2\right] = E\left[\sum_{i=0}^{h}(Z^{(\mathbf{M})})_i^2\right],$$

$$E[Z_{\mathbf{M}}^4] = E\left[(\sum_{i=0}^{h}(Z^{(\mathbf{M})})_i)^4\right] \leq E\left[(h+1)^3 \cdot (\sum_{i=0}^{h}(Z^{(\mathbf{M})})_i^4)\right].$$

Diving both sides by $Var[Z_{\mathbf{M}}]^2$, we obtain the inequality

$$\left|\frac{E[Z_{\mathbf{M}}^4]}{Var[Z_{\mathbf{M}}]^2}\right| \leq \left|\frac{E[(h+1)^3 \cdot (\sum_{i=0}^{h}(Z^{(\mathbf{M})})_i^4)]}{Var[Z_{\mathbf{M}}]^2}\right| = (h+1)^3 \cdot \left|\frac{E[\sum_{i=0}^{h}(Z^{(\mathbf{M})})_i^4]}{Var[Z_{\mathbf{M}}]^2}\right|$$
$$= (h+1)^3 \cdot \sum_{i=0}^{h}\left|\frac{E[(Z^{(\mathbf{M})})_i^4]}{Var[Z_{\mathbf{M}}]^2}\right| \leq (h+1)^3 \cdot \sum_{i=0}^{h}\left|\frac{E[(Z^{(\mathbf{M})})_i^4]}{Var[(Z^{(\mathbf{M})})_i]^2}\right|$$

By Lemma 5.3,5.4,5.5 and 5.6, $\left|\frac{E[(Z^{(\mathbf{M})})_i^4]}{Var[(Z^{(\mathbf{M})})_i]^2}\right|$ is bounded by $\mathsf{poly}(\lambda)$ for all $i = 0, 1, \cdots, h$ regardless of $\mathbf{P} = \mathbf{M}$ or $\mathbf{P} = \mathbf{N}$. Therefore, the following inequality holds.

$$\left|\frac{E[Z_{\mathbf{M}}^4]}{Var[Z_{\mathbf{M}}]^2}\right| \leq \mathsf{poly}(\lambda) =: q(\lambda)$$

Moreover, by the definition of $Z_{\mathbf{N}}$ and $Z_{\mathbf{M}}$, it holds that $E[Z_{\mathbf{N}}^2] = \sigma_{\mathbf{N}}^2$ and $E[Z_{\mathbf{M}}^2] = \sigma_{\mathbf{M}}^2$, respectively. Thus, it is clear that $\sigma_{\mathbf{M}}^2 \neq \sigma_{\mathbf{N}}^2$ and $\left|\frac{\max(E[Z_{\mathbf{N}}^2], E[Z_{\mathbf{M}}^2])}{\sigma_{\boldsymbol{N}}^2 - \sigma_{\boldsymbol{M}}^2}\right|$ is bounded by $\mathsf{poly}(\lambda)$. At last the statistical closeness of distributions completes the proof. □

References

1. Prabhanjan Ananth, Divya Gupta, Yuval Ishai, and Amit Sahai. Optimizing obfuscation: Avoiding barrington's theorem. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 646–658. ACM, 2014.
2. Saikrishna Badrinarayanan, Eric Miles, Amit Sahai, and Mark Zhandry. Post-zeroizing obfuscation: New mathematical tools, and the case of evasive circuits. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 764–791. Springer, 2016.
3. Boaz Barak, Sanjam Garg, Yael Tauman Kalai, Omer Paneth, and Amit Sahai. Protecting obfuscation against algebraic attacks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 221–238. Springer, 2014.
4. James Bartusek, Jiaxin Guan, Fermi Ma, and Mark Zhandry. Preventing zeroizing attacks on ggh15. accepted in TCC 2018.
5. Dan Boneh, Kevin Lewi, Hart Montgomery, and Ananth Raghunathan. Key homomorphic prfs and their applications. In *Advances in Cryptology–CRYPTO 2013*, pages 410–428. Springer, 2013.
6. Dan Boneh and Mark Zhandry. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. *Algorithmica*, 79(4):1233–1285, 2017.
7. Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 575–584. ACM, 2013.
8. Zvika Brakerski and Guy N Rothblum. Virtual black-box obfuscation for all circuits via generic graded encoding. In *Theory of Cryptography Conference*, pages 1–25. Springer, 2014.
9. Zvika Brakerski, Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. Obfuscating conjunctions under entropic ring lwe. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, pages 147–156. ACM, 2016.
10. Ran Canetti and Yilei Chen. Constraint-hiding constrained prfs for nc^1 from lwe. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 446–476. Springer, 2017.
11. Yilei Chen, Craig Gentry, and Shai Halevi. Cryptanalyses of candidate branching program obfuscators. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 278–307. Springer, 2017.
12. Yilei Chen, Vinod Vaikuntanathan, and Hoeteck Wee. Ggh15 beyond permutation branching programs: Proofs, attacks, and candidates. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018*, pages 577–607, Cham, 2018. Springer International Publishing.
13. Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the multilinear map over the integers. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 3–12. Springer, 2015.
14. Jung Hee Cheon, Minki Hhan, Jiseung Kim, and Changmin Lee. Cryptanalyses of branching program obfuscations over GGH13 multilinear map from the NTRU problem. In *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, pages 184–210, 2018.
15. Jung Hee Cheon, Minki Hhan, Jiseung Kim, and Changmin Lee. Cryptanalysis on the HHSS obfuscation arising from absence of safeguards. *IEEE Access*, 6:40096–40104, 2018.
16. Jean-Sébastien Coron, Craig Gentry, Shai Halevi, Tancrede Lepoint, Hemanta K Maji, Eric Miles, Mariana Raykova, Amit Sahai, and Mehdi Tibouchi. Zeroizing without low-level zeroes: New mmap attacks and their limitations. In *Advances in Cryptology–CRYPTO 2015*, pages 247–266. Springer, 2015.
17. Jean-Sébastien Coron, Moon Sung Lee, Tancrede Lepoint, and Mehdi Tibouchi. Cryptanalysis of ggh15 multilinear maps. In *Annual Cryptology Conference*, pages 607–628. Springer, 2016.
18. Jean-Sébastien Coron, Moon Sung Lee, Tancrede Lepoint, and Mehdi Tibouchi. Zeroizing attacks on indistinguishability obfuscation over clt13. In *IACR International Workshop on Public Key Cryptography*, pages 41–58. Springer, 2017.
19. Jean-Sébastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In *Advances in Cryptology–CRYPTO 2013*, pages 476–493. Springer, 2013.
20. Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *Eurocrypt*, volume 7881, pages 1–17. Springer, 2013.
21. Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 40–49. IEEE Computer Society, 2013.
22. Sanjam Garg, Eric Miles, Pratyay Mukherjee, Amit Sahai, Akshayaram Srinivasan, and Mark Zhandry. Secure obfuscation in a weak multilinear map model. In *Theory of Cryptography Conference*, pages 241–268. Springer, 2016.

23. Craig Gentry, Sergey Gorbunov, and Shai Halevi. Graph-induced multilinear maps from lattices. In *Theory of Cryptography*, pages 498–527. Springer, 2015.
24. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.
25. Oded Goldreich. *The Foundations of Cryptography - Volume 1, Basic Techniques*. Cambridge University Press, 2001.
26. Rishab Goyal, Venkata Koppula, and Brent Waters. Lockable obfuscation. In *Foundations of Computer Science (FOCS), 2017 IEEE 58th Annual Symposium on*, pages 612–621. IEEE, 2017.
27. Yupu Hu and Huiwen Jia. Cryptanalysis of ggh map. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 537–565. Springer, 2016.
28. Fermi Ma and Mark Zhandry. The mmap strikes back: obfuscation and new multilinear maps immune to clt13 zeroizing attacks. Technical report, Cryptology ePrint Archive, Report 2017/946, 2017.
29. Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 700–718. Springer, 2012.
30. Eric Miles, Amit Sahai, and Mor Weiss. Protecting obfuscation against arithmetic attacks. *IACR Cryptology ePrint Archive*, 2014:878, 2014.
31. Rafael Pass, Karn Seth, and Sidharth Telang. Indistinguishability obfuscation from semantically-secure multilinear encodings. In *International Cryptology Conference*, pages 500–517. Springer, 2014.
32. Alice Pellet-Mary. Quantum attacks against indistinguishablility obfuscators proved secure in the weak multilinear map model. In *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, pages 153–183, 2018.
33. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34, 2009.
34. Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 475–484. ACM, 2014.
35. Daniel Wichs and Giorgos Zirdelis. Obfuscating compute-and-compare programs under lwe. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 600–611. IEEE, 2017.

A Modified CVW Obfuscation

We give a modification of CVW obfuscation, which can obfuscate the permutation matrix branching programs. This modification is, as far as we know, robust against all existing attacks. We first describe the transformation of branching programs. Then, we give the modification of CVW obfuscation.

A.1 Transformation of Branching Programs

We first introduce the transformation on single-input permutation matrix branching programs. This transformation is applicable to BPs which outputs 0 when the product of BP matrices is the identity matrix. The output of transformation is a new branching program that outputs 0 when the product of BP matrices is the zero matrix. Through this transformation, the width of branching program is doubled. Note that this is adapted version of [12, Claim 6.2].

We are given a branching program with input size ℓ

$$\mathbf{P} = \left\{\{\mathbf{P}_{i,b} \in \{0,1\}^{w\times w}\}_{i\in[h],b\in\{0,1\}}, \mathsf{inp} : [h] \to [\ell]\right\}$$

where the evaluation of $\mathbf{P}$ at $x \in \{0,1\}^\ell$ is computed by

$$\mathbf{P}(x) = \begin{cases} 0 & \text{if } \prod_{i=1}^{h} \mathbf{P}_{i,(x_{\mathsf{inp}(i)})} = \mathbf{I}_w \\ 1 & \text{otherwise} \end{cases}$$

Then the transformation is done by changing branching program matrices as

$$\mathbf{P}' = \left\{\left\{\mathbf{P}'_{i,b} = \begin{bmatrix} \mathbf{P}_{i,b} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_w \end{bmatrix} \in \{0,1\}^{2w\times 2w}\right\}_{i\in[h],b\in\{0,1\}}, \mathsf{inp} : [h] \to [\ell]\right\}$$

and the evaluation is similar but uses new vectors $\mathbf{v}' = (\mathbf{v}| - \mathbf{v})$ and $\mathbf{w}' = (\mathbf{w}|\mathbf{w})$ for $\mathbf{v}, \mathbf{w} \in \mathbb{Z}^w$:

$$\mathbf{P}'(x) = \begin{cases} 0 & \text{if } \mathbf{v}' \cdot \prod_{i=1}^{h} \mathbf{P}'_{i,(x_{\mathsf{inp}(i)})} \cdot \mathbf{w}'^T = \mathbf{0} \\ 1 & \text{otherwise} \end{cases}$$

We will choose $\mathbf{v}$ and $\mathbf{w}$ as random Gaussian vectors. Note that the resulting branching program is also a permutation BP.

A.2 Modification of CVW Obfuscation

We give here how to modify the CVW obfuscation to be applicable to the resulting permutation BPs of the above transform. We also assume that the index length $h = (\lambda+1)\cdot\ell$ and the index-to-input function satisfies $\mathsf{inp}(i) = (i \mod \ell)$ as in the CVW obfuscation. We also assume that the BP is $(\lambda + 1)$-input repetition BP as in the original construction. The changed parts are written in red. Note that the targeted BPs have width $2w$. Thus we set $t := (2w + 2n\ell) \cdot n$.

- Sample bundling matrices $\{\mathbf{R}_{i,b} \in \mathbb{Z}^{2n\ell\times 2n\ell}\}_{i\in[h],b\in\{0,1\}}$ such that $(\mathbf{1}^{1\times 2\ell}\otimes\mathbf{I}^{n\times n})\cdot\mathbf{R}_{\mathbf{x}'}\cdot(\mathbf{1}^{2\ell\times 1}\otimes\mathbf{I}^{n\times n}) = \mathbf{0} \iff \mathbf{x}' \in \bar{\omega}(\{0,1\}^\ell)$ for all $\mathbf{x}' \in \{0,1\}^h$. More precisely, $\mathbf{R}_{i,b}$ is a block diagonal matrix $\mathsf{diag}(\mathbf{R}^{(1)}_{i,b}, \mathbf{R}^{(2)}_{i,b}, \cdots, \mathbf{R}^{(\ell)}_{i,b})$. Each $\mathbf{R}^{(k)}_{i,b} \in \mathbb{Z}^{2n\times 2n}$ is one of the following three cases.

$$\mathbf{R}^{(k)}_{i,b} = \begin{cases} \mathbf{I}^{2n\times 2n} & \text{if } \mathsf{inp}(i) \neq k \\ \begin{pmatrix} \tilde{\mathbf{R}}^{(k)}_{i,b} & \\ & \mathbf{I}^{n\times n} \end{pmatrix}, \tilde{\mathbf{R}}^{(k)}_{i,b} \leftarrow \mathcal{D}^{n\times n}_{\mathbb{Z},\sigma} & \text{if } \mathsf{inp}(i) = k \text{ and } i \leq \lambda\ell \\ \begin{pmatrix} -\mathbf{I}^{n\times n} & \\ & \prod_{j=0}^{\lambda-1} \tilde{\mathbf{R}}^{(k)}_{k+j\ell,b} \end{pmatrix} & \text{if } \mathsf{inp}(i) = k \text{ and } i > \lambda\ell \end{cases}$$

- Sample matrices $\{\mathbf{S}_{i,b} \leftarrow \mathcal{D}^{n\times n}_{\mathbb{Z},\sigma}\}_{i\in[h],b\in\{0,1\}}$, bookend vectors $\mathbf{v} \leftarrow \mathcal{D}^{w}_{\mathbb{Z},\sigma}$ and $\mathbf{w} \leftarrow \mathcal{D}^{w}_{\mathbb{Z},\sigma}$ and compute

$$\mathbf{J} := ((\mathbf{v}| - \mathbf{v}|\mathbf{1}^{1\times 2n\ell}) \otimes \mathbf{I}^{n\times n}) \in \mathbb{Z}^{n\times t}$$

$$\hat{\mathbf{S}}_{i,b} := \begin{pmatrix} \mathbf{P}_{i,b} \otimes \mathbf{S}_{i,b} & \\ & \mathbf{R}_{i,b} \otimes \mathbf{S}_{i,b} \end{pmatrix} \in \mathbb{Z}^{t\times t}$$

$$\mathbf{L} := ((\mathbf{w}|\mathbf{w}|\mathbf{1}^{1\times 2n\ell})^T \otimes \mathbf{I}^{n\times n}) \in \mathbb{Z}^{t\times n}$$

- Sample $(\mathbf{A}_i, \tau_i) \leftarrow \mathsf{TrapSam}(1^t, 1^m, q)$ for $0 \leq i \leq h-1$, $\mathbf{A}_h \leftarrow U(\mathbb{Z}_q^{n\times n})$, $\{\mathbf{E}_{i,b} \leftarrow \mathcal{D}^{t\times m}_{\mathbb{Z},\sigma}\}_{i\in[h-1],b\in\{0,1\}}$ and $\{\mathbf{E}_{h,b} \leftarrow \mathcal{D}^{t\times n}_{\mathbb{Z},\sigma}\}_{b\in\{0,1\}}$.
- Run Sample algorithms to obtain

$$\mathbf{D}_{i,b} \in \mathbb{Z}^{m\times m} \leftarrow \mathsf{Sample}(\mathbf{A}_{i-1}, \tau_{i-1}, \hat{\mathbf{S}}_{i,b}\cdot\mathbf{A}_i + \mathbf{E}_{i,b}, \sigma) \text{ for } 1 \leq i \leq h-1,$$
$$\mathbf{D}_{h,b} \in \mathbb{Z}^{m\times n} \leftarrow \mathsf{Sample}(\mathbf{A}_{h-1}, \tau_{h-1}, \hat{\mathbf{S}}_{h,b}\cdot\mathbf{L}\cdot\mathbf{A}_h + \mathbf{E}_{h,b}, \sigma).$$

- Define $\mathbf{A}_{\mathbf{J}}$ as a matrix $\mathbf{J}\cdot\mathbf{A}_0 \in \mathbb{Z}^{n\times m}$ and outputs matrices

$$\left\{\mathsf{inp}, \mathbf{A}_{\mathbf{J}}, \{\mathbf{D}_{i,b}\}_{i\in[h],b\in\{0,1\}}\right\}.$$

We omit the procedure and correctness of evaluation that are almost the same to the original one.

B Subtle Gap in the Argument using Statistical Indistinguishability

In this section, we give two subtle counter-intuitive problems which usually appear in arguments dealing with statistical indistinguishability, and how to subvert them. We remark that this problem is also found in many analysis related to the trapdoor sampling of lattice[9] but we cannot find the discussion on such problem in the literature. Since our attack and candidates obfuscations itself cannot be run in practical time, it is meaningful to address the theoretical backgrounds.

The problems are stated as follows:

[9] e.g. the correctness of GGH15 multilinear map

1. Statistical indistinguishability of two random variables does NOT imply that the statistical values of those variables such as the expectations or variances are negligibly close.
2. The sequences of (dependent) statistical indistinguishable random variables may NOT be statistically indistinguishable.

The following examples show the problems of the above arguments.

Expectations of two statistically indistinguishable distributions. Let X_λ, Y_λ be two random variables defined by

1. X_λ is always zero
2. $Y_\lambda = 0$ with probability $1 - 1/2^\lambda$ and 2^λ with probability $1/2^\lambda$

then this two distributions is clearly statistically indistinguishable but the expectations are differ; $E[X] = 0$ and $E[Y] = 1$.

Sequences of statistical indistinguishable random variables. Let A, B, X, Y be random variables which are defined by

1. A, B, Y are independent and uniformly distributed over $[0, 1]$
2. $X = 1 - A$

then clearly $A \approx_s B$ and $X \approx_s Y$. However, (A, X) and (B, Y) are not statistical indistinguishable; even worse, $(A, X) \not\approx_s (A, Y)$.

B.1 Detour by Sample Variance

Fortunately, the algorithm (in Theorem 3.2) works with only the variance of *samples* and those samples are *independent*. In this computation we do not compute the real variance of distribution that may be problematic. Instead we compute the *sample variance* which can be considered as a function of samples. More precisely, we sample random variables $X^{(i)}$ that follow the distribution $\mathcal{D}_{\mathbf{P}}$ of the first entry of evaluation. In the main body of paper we prove Proposition 3.2 for random variables $Z^{(i)}$ following $\tilde{\mathcal{D}}$, which is substituted D into $\tilde{D}$, rather than $\mathcal{D}$. We assume that $\mathcal{D} \approx_s \tilde{\mathcal{D}}$, which will be proven in the next subsection. Since all random variables are mutually independent, we have

$$\prod_i (X^{(i)}) \approx_s \prod_i (Z^{(i)}).$$

Note that the same function evaluations on two random variable decrease the statistical distance; this allows that the distributions of *sample variance* of $(X^{(i)})_i$ and $(Z^{(i)})_i$ are also statistically indistinguishable. Thus Proposition 3.2 hold as well for X's, that is, the inequality of sample variance for $\mathcal{D}$ holds with overwhelming probability when the same one for $\tilde{\mathcal{D}}$ holds.

B.2 How to deal $\tilde{D}$'s

The usual definition of statistical indistinguishability only consider the outputs of random variables and does not embrace the relations of several random variables. We can deal with this problem using the definition:

Definition B.1 (Ω-statistical distance) *Let $D, E : \Omega \to \mathbb{R}$ be two random variables on a set Ω. The Ω-statistical distance of D and E is defined by*

$$\Delta(D, E) = \max_{X \subset \Omega} \left| \Pr_D(X) - \Pr_E(X) \right|.$$

We say that D and E are Ω-statistical indistinguishable if the Ω-statistical distance is negligible and denote this case by $D \approx_s^\Omega E$.

In the usual cryptographic setting, we use $\mathit{\Omega}$ as outcomes of random variables such as $\mathbb{Z}$, lattice points or $\mathbb{Z}^n$. This choice does not ensure the dependency of random variables. However, if we choose $\mathit{\Omega}$ that embraces all dependencies of random variables then it is enough to overcome the second problem. That is, we choose $\mathit{\Omega}$ so that the every (conditional) events with respect to all random variables are included in $\mathit{\Omega}$, and $\tilde{D}^{(\mathbf{M})}_{i,x_i}$ entry-wise Gaussian distribution so that

$$(D^{(\mathbf{P})}_{i,x_i}, E^{(\mathbf{P})}_{i,x_i}, \hat{S}^{(\mathbf{P})}_{i,x_i}) \approx^{\mathit{\Omega}}_s (\tilde{D}^{(\mathbf{P})}_{i,x_i}, E^{(\mathbf{P})}_{i,x_i}, \hat{S}^{(\mathbf{P})}_{i,x_i})$$

holds. This choice of $\tilde{D}$ is possible because the only constraint of $\tilde{D}$ is that it is Gaussian distribution; the choice of specified distribution on each event is free except Gaussian.[10]

In this choice, we can obtain

$$\prod_i (D^{(\mathbf{P})}_{i,x_i}, E^{(\mathbf{P})}_{i,x_i}, \hat{S}^{(\mathbf{P})}_{i,x_i}) \approx^{\mathit{\Omega}}_s \prod_i (\tilde{D}^{(\mathbf{P})}_{i,x_i}, E^{(\mathbf{P})}_{i,x_i}, \hat{S}^{(\mathbf{P})}_{i,x_i})$$

since they are all independent except the random variables with the same index. Since the evaluation of function decrease the statistical distance, the first entries of obfuscations are statistically indistinguishable, i.e. $(X^{(i)})_i \approx_s (Z^{(i)})_i$ with the notation in the previous section.

C Useful Tools for Computing the Variances

We introduce useful lemmas to help our computation. We note that we consider the random matrix A whose entries in the same columns are independent, while the other entries need not to be independent, that corresponds to the output of trapdoor sampling.[11]

Lemma C.1 *Let $A = (A_{i,j})$ be a $n \times n$ random matrix where $A_{i,t}$ and $A_{j,t}$ are independent for every $1 \leq i < j \leq n$ and $1 \leq t \leq n$. and $X = [X_1, X_2, \cdots, X_n]$ a n-dimensional random vector which is independent to A. Assume that the following conditions for all distinct $i, j, k, l \in [n]$:*

$$E[X_i \cdot X_j] = 0,\ E[X_i^3 \cdot X_j] = 0,$$
$$E[X_i^2 \cdot X_j \cdot X_k] = 0,\ \textit{and}\ E[X_i \cdot X_j \cdot X_k \cdot X_l] = 0.$$

Then, a n-dimensional random vector $Y = [Y_1, Y_2, \cdots, Y_n] = A \cdot X$ also satisfies the similar constraints

$$E[Y_i \cdot Y_j] = 0,\ E[Y_i^3 \cdot Y_j] = 0,$$
$$E[Y_i^2 \cdot Y_j \cdot Y_k] = 0,\ \textit{and}\ E[Y_i \cdot Y_j \cdot Y_k \cdot Y_l] = 0.$$

for all distinct $i, j, k, l \in [n]$.

Proof.

$$\begin{aligned} E[Y_i \cdot Y_j] &= E\left[\sum_{t=1}^{n}\sum_{s=1}^{n} A_{i,t} \cdot X_t \cdot A_{j,s} \cdot X_s\right] \\ &= \sum_{t=1}^{n}\sum_{s=1}^{n} E[A_{i,t} \cdot X_t \cdot A_{j,s} \cdot X_s] \\ &= \sum_{1 \leq t,s \leq n, t \neq s} E[A_{i,t} \cdot A_{j,s}] \cdot E[X_t \cdot X_s] + \sum_{t=1}^{n} E[A_{i,t}] \cdot E[A_{j,t}] \cdot E[X_t \cdot X_t] = 0 \end{aligned}$$

□

Lemma C.2 *Let $\{A_i = (A_i^{j,k})\}_{1 \leq i \leq t}$ be $n \times n$ random matrices where*

[10] This part is done by constructing $\tilde{D}$ so that the difference of $Pr[\tilde{D} = x|\text{condition}]$ and $Pr[D = x|\text{condition}]$ is sufficiently small and the entries of $\tilde{D}$ follow Gaussian.

[11] Since the trapdoor sampling uses some shared trapdoor, so we cannot ensure the independency of each columns. The somewhat complex conditions in the lemma are used to deal with such problem.

- $A_i^{j,k}$ *follow Gaussian distribution* $\mathcal{D}_{\mathbb{Z},\sigma}$ *for all* $1 \le j, k \le n$ *and* $1 \le i \le t$,
- $A_i^{j,s}$ *and* $A_i^{k,s}$ *are independent for every* $1 \le j < k \le n$, $1 \le s \le n$ *and* $1 \le i \le t$,
- $A_1^{i_1,j_1}, \cdots, A_t^{i_t,j_t}$ *are mutually independent for every* $1 \le i_k, j_k \le n$ *for all* k

and $X = (X_{i,j}) = \prod_{k=1}^t A_k$ $n \times n$ *random matrix. For all* $i, j, k \in [n]$, *it holds that*

$$E[X_{i,j}] = 0,\ Var[X_{i,j}] = n^{t-1} \cdot (\sigma^2)^t,$$
$$E[X_{i,j}^4] = 3\left(n(n+2)\right)^{t-1} \cdot (\sigma^2)^{2t},$$
$$E[X_{i,j}^2 \cdot X_{k,j}^2] = \left(n(n+2)\right)^{t-1} \cdot (\sigma^2)^{2t}$$

Proof. We apply mathematical induction on t. For $t = 1$, it is clear because of the property of Gaussian distribution.

We assume that the equations hold when $t = s$ and will show that the same results hold for $t = s+1$. Let $X' = \prod_{i=1}^{s} A_i$ and $Y = A_{s+1} \cdot X'$. Note that all entries of A_i follow Gaussian distribution $\mathcal{D}_{\mathbb{Z},\sigma}$ satisfy the same condition of the lemma. We denote $A_{s+1} = (A_{i,j})$ for brevity and $Y_{i,j} = \sum_{k=1}^{n} A_{i,k} \cdot X_{k,j}$. Note that the results of Lemma C.1 holds for every columns of X, which can be shown in the inductively applying Lemma C.1.

1. $E[Y_{i,j}] = 0$ is clear.

2. Since $E[Y_{i,j}] = 0$, $Var[Y_{i,j}]$ is the same to $E[Y_{i,j}^2]$. Note that we can obtain $E[X_{k,j} \cdot X_{l,j}] = 0$ and for $k \ne l$ by applying Lemma C.1 inductively, thus $E[A_{i,k} \cdot X_{k,j} \cdot A_{i,l} \cdot X_{l,j}] = E[A_{i,k} \cdot A_{i,l}] \cdot E[X_{k,j} \cdot X_{l,j}] = 0$ also holds. Now we obtain

$$\begin{aligned} Var[Y_{i,j}] = E[Y_{i,j}^2] &= E\left[(\sum_{k=1}^{n} A_{i,k} \cdot X_{k,j})^2\right] \\ &= E\left[\sum_{k=1}^{n} A_{i,k}^2 \cdot X_{k,j}^2\right] = \sum_{k=1}^{n} E[A_{i,k}^2] \cdot E[X_{k,j}^2] \\ &= n \cdot \sigma^2 \cdot n^{s-1} \cdot (\sigma^2)^s = n^s \cdot (\sigma^2)^{s+1} \end{aligned}$$

The last equality holds by the inductive hypothesis.

3. Note that $E[Y_{i,j}^4] = E[(\sum_{k=1}^n A_{i,k} \cdot X_{k,j})^4]$. It holds that, for $k \ne l$,

$$E[(A_{i,k} \cdot X_{k,j})^3 \cdot (A_{i,l} \cdot X_{l,j})] = E[A_{i,k}^3 \cdot A_{i,l}] \cdot E[X_{k,j}^3 \cdot X_{l,j}] = 0$$
$$E[(A_{i,k} \cdot X_{k,j})^2 \cdot (A_{i,l} \cdot X_{l,j}) \cdot (A_{i,m} \cdot X_{m,j})] = 0$$
$$E[(A_{i,k} \cdot X_{k,j}) \cdot (A_{i,l} \cdot X_{l,j}) \cdot (A_{i,m} \cdot X_{m,j}) \cdot (A_{i,u} \cdot X_{u,j})] = 0$$

for all for all distinct $k, l, m, u \in \{1, \cdots, n\}$. By the induction hypothesis, it holds that

$$E[A_{i,k}^4 \cdot X_{k,j}^4] = E[A_{i,k}^4] \cdot E[X_{k,j}^4] = 3\sigma^4 \cdot 3(n(n+2))^{s-1} \cdot (\sigma^2)^{2s}.$$

Therefore, we conclude that

$$E[(\sum_{k=1}^{n} A_{i,k} \cdot X_{k,j})^4] = 3(n(n+2))^s \cdot (\sigma^2)^{2(s+1)}.$$

4. Note that $E[Y_{i,j}^2 \cdot Y_{k,j}^2] = E[(\sum_{m=1}^n A_{i,m} \cdot X_{m,j})^2 \cdot (\sum_{u=1}^n A_{k,u} \cdot X_{u,j})^2]$. Then we obtain the similar result as follows:

$$\begin{aligned} E[(\sum_{m=1}^{n} A_{i,m} \cdot X_{m,j})^2 \cdot (\sum_{u=1}^{n} A_{i,u} \cdot X_{u,j})^2] &= E\left[(\sum_{m=1}^{n} A_{i,m}^2 \cdot X_{m,j}^2) \cdot (\sum_{u=1}^{n} A_{k,u}^2 \cdot X_{u,j}^2)\right] \\ = \sum_{u=1}^{n} \sum_{m=1}^{n} E[A_{i,m}^2 \cdot A_{k,u}^2] \cdot E[X_{m,j}^2 \cdot X_{u,j}^2] &= (n(n+2))^s \cdot (\sigma^2)^{2(s+1)}. \end{aligned}$$

□

Lemma C.3 *Let $A = (A_{i,j})$ be a $n \times m$ random matrix whose entries satisfy $E[A_{i,j}] = 0$, $E[A_{i,j}^2] = \sigma_1^2$ and $E[A_{i,j}^4] \leq C\sigma_1^4$ for all $i \in [n], j \in [m]$ with some constant C, where the entries of A need not to be independent. Let $v = [v_1, \cdots, v_n]$ and $w = [w_1, \cdots, w_m]$ be n-dimensional random vectors whose entries are mutually independent and follow the Gaussian distribution $\mathcal{D}_{\mathbb{Z},\sigma_2}$. If the entries of A are independent to the entries of v and w, then $Y = v \cdot A \cdot w^T$ satisfies the following condition:*

$$E[Y] = 0, \; E[Y^2] = nm \cdot \sigma_1^2 \cdot \sigma_2^4, \quad E[Y^4] \leq (nm)^4 \cdot (C\sigma_1^4) \cdot (3\sigma_2^4)^2.$$

Proof. Note that $Y = \sum_{j=1}^{m} \sum_{i=1}^{n} v_i \cdot A_{i,j} \cdot w_j$.

1. $E[Y] = E[\sum_{j=1}^{m} \sum_{i=1}^{n} v_i \cdot A_{i,j} \cdot w_j] = \sum_{j=1}^{m} \sum_{i=1}^{n} E[v_i]E[A_{i,j}]E[w_j] = 0.$
2. For all $i, k \in [n], j, l \in [m]$ satisfy $(i, j) \neq (k, l)$, $E[(v_i \cdot A_{i,j} \cdot w_j) \cdot (v_k \cdot A_{k,l} \cdot w_l)] = E[v_i \cdot v_k]E[A_{i,j} \cdot A_{k,l}]E[w_j \cdot w_l] = 0$ since one of $E[v_i \cdot v_k]$ or $E[w_j \cdot w_l]$ is zero. Then it holds that

$$\begin{aligned} E[Y^2] &= E[(\sum_{j=1}^{m} \sum_{i=1}^{n} v_i \cdot A_{i,j} \cdot w_j)^2] = E[\sum_{j=1}^{m} \sum_{i=1}^{n} v_i^2 \cdot A_{i,j}^2 \cdot w_j^2] \\ &= \sum_{j=1}^{m} \sum_{i=1}^{n} E[v_i^2]E[A_{i,j}^2]E[w_j^2] = nm \cdot \sigma_1^2 \cdot \sigma_2^4. \end{aligned}$$

3. By the Cauchy-Schwarz Inequality, it holds

$$\begin{aligned} E[Y^4] &= E[(\sum_{j=1}^{m} \sum_{i=1}^{n} v_i \cdot A_{i,j} \cdot w_j)^4] \leq E[(nm)^3 \cdot (\sum_{j=1}^{m} \sum_{i=1}^{n} v_i^4 \cdot A_{i,j}^4 \cdot w_j^4)] \\ &= (nm)^3 \cdot \sum_{j=1}^{m} \sum_{i=1}^{n} E[v_i^4]E[A_{i,j}^4]E[w_j^4] \leq (nm)^4 \cdot (C\sigma_1^4) \cdot (3\sigma_2^4)^2. \end{aligned}$$

□

D Analysis of CVW Obfuscation

In this seciton, we describe how to prove the lemmas in Section 4.2. We use the same notation as in Section 4. We re-use or abuse the some notations for the different proof for the convenience of the writing. Fix a $\mathbf{x}$ satisfying $\mathcal{O}(\mathbf{P})(\mathbf{x}) = \mathbf{0}$.

Note that the appeared random matrices are of the form

$$\mathbf{J} \cdot \prod_{i=1}^{j} \hat{S}_{i,x_i}^{(\mathbf{P})} \cdot E_{j+1,x_{j+1}}^{(\mathbf{P})} \cdot \prod_{k=j+2}^{h} \tilde{D}_{k,x_k}^{(\mathbf{P})}.$$

For the CVW obfuscation, all random matrices are independent except the tuples $(D_{i,x_i}^{(\mathbf{M})}, E_{i,x_i}^{(\mathbf{M})})$ and $(D_{i,x_i}^{(\mathbf{M})}, \hat{S}_{i,x_i}^{(\mathbf{M})})$. Though we use another random variable $\tilde{D}_{i,b}$ whose columns correspond to the distribution $\mathcal{D}_{\mathbb{Z}^m,\sigma}$ instead of $D_{i,b}$, we cannot ensure the independency of tuples $(\tilde{D}_{i,x_i}^{(\mathbf{M})}, E_{i,x_i}^{(\mathbf{M})})$ and $(\tilde{D}_{i,x_i}^{(\mathbf{M})}, \hat{S}_{i,x_i}^{(\mathbf{M})})$. Further, we also cannot ensure that the columns of trapdoor sampling matrices are independent. From now on, we drop the tilde in the trapdoor sampling.

We also remark that all distributions corresponding to random variables appeared in lemmas except $\left(Z_{1,1}^{(\mathbf{P})}\right)_1$ are not changed regardless of the choice of $\mathbf{P} = \mathbf{M}$ or $\mathbf{N}$, because the matrices of branching programs are all zero except the first matrix. Thus we consider the choice of the branching program only in Lemma 4.4, which discusses $\left(Z_{1,1}^{(\mathbf{P})}\right)_1$.

By Lemma 2.9, each column of the random matrix $D^{(\mathbf{P})}_{i,x_i}$ follows the distribution $\mathcal{D}_{\mathbb{Z}^m,\sigma}$ for all i. Note that since $\mathcal{D}_{\mathbb{Z}^m,\sigma}$ is equal to $\mathcal{D}^m_{\mathbb{Z},\sigma}$, entries of each column are mutually independent. Therefore, we can use Lemma C.1 and C.2 to analyze the product of $D^{(\mathbf{P})}_{i,x_i}$.

At last, we note that many inequalities can be improved. For example, the bounds in Lemma 4.3 and 4.5 can be tightened as constant upper bound. We omit those calculation because we only need the polynomial upper bounds.

Proof (of Lemma 4.2). We assume that $\mu_1 < \mu_2$ and only show the result for $\mathbf{M}$. Note that the random matrix $E^{(\mathbf{M})}_j$ is only (possibly) dependent to $\tilde{D}^{(\mathbf{M})}_j$ and the random variables $(Z^{(\mathbf{M})}_{1,1})_{\mu_1}$ and $(Z^{(\mathbf{M})}_{1,1})_{\mu_2}$ do not contain such random variables. Therefore, if we express $(Z^{(\mathbf{M})}_{1,1})_{\mu_1} \cdot (Z^{(\mathbf{M})}_{1,1})_{\mu_2}$ into the polynomials of random variables, then every monomial includes one entry of $E^{(\mathbf{M})}_{\mu_1+1}$ and does not include the entries of $\tilde{D}^{(\mathbf{M})}_{\mu_1+1}$. Since the expectation of every entry of $E^{(\mathbf{M})}_{\mu_1+1}$ is zero, the desired result holds. □

Proof (of Lemma 4.3). We suffice to show the result for $\mathbf{M}$. Let $(X^{(\mathbf{M})}_{u,v})$ be random variables of the (u,v)-th entry of the random matrix $E^{(\mathbf{M})}_{1,x_1} \cdot \prod_{k=2}^{h} D^{(\mathbf{M})}_{k,x_k}$. Then, for all $u \in [t], v \in [n]$, all random variables $X^{(\mathbf{M})}_{u,v}$ have the same variance $m^{h-1}(\sigma^2)^h$ by Lemma C.2. Moreover, it holds that $E[X^{(\mathbf{M})}_{u,v} \cdot X^{(\mathbf{M})}_{u',v}] = 0$ for distinct u, u' and $E[{X^{(\mathbf{M})}_{u,v}}^4] = 3\,(m(m+2))^{h-1} \cdot (\sigma^2)^{2h}$.

The random variables of the (u,v)-th entry of the random matrix $\mathbf{J} \cdot E^{(\mathbf{M})}_{1,x_1} \cdot \prod_{k=2}^{h} D^{(\mathbf{M})}_{k,x_k}$ are denoted by $(Z^{(\mathbf{M})}_{u,v})_0$. We observe $(Z^{(\mathbf{M})}_{1,1})_0 = \sum_{i=1}^{w+2n\ell} X^{(\mathbf{M})}_{n\cdot(i-1)+1,1}$. Then,

$$\begin{aligned} Var[(Z^{(\mathbf{M})}_{1,1})_0] &= E\left[\left(\sum_{i=1}^{w+2n\ell} X^{(\mathbf{M})}_{n\cdot(i-1)+1,1}\right)^2\right] \\ &= E\left[\sum_{i=1}^{w+2n\ell} {X^{(\mathbf{M})}}^2_{n\cdot(i-1)+1,1}\right] = (w+2n\ell)\cdot m^{h-1}(\sigma^2)^h. \end{aligned}$$

In addition, the upper bound of $E[(Z^{(\mathbf{M})}_{1,1})_0^4]$ can be computed as follows:

$$\begin{aligned} E[(Z^{(\mathbf{M})}_{1,1})_0^4] &= E[(\sum_{i=1}^{w+2n\ell} X^{(\mathbf{M})}_{n(i-1)+1,1})^4] \\ &\leq E[(w+2n\ell)^3 \cdot (\sum_{i=1}^{w+2n\ell} {X^{(\mathbf{M})}}^4_{n(i-1)+1,1})] \\ &= (w+2n\ell)^4 \cdot 3\{m(m+2)\}^{h-1} \cdot (\sigma^2)^{2h}. \end{aligned}$$

Combining them, we obtain the inequality $\left|\dfrac{E[(Z^{(\mathbf{M})}_{1,1})_0^4]}{Var[(Z^{(\mathbf{M})}_{1,1})_0]^2}\right| \leq 3\cdot(w+2n\ell)^2 \cdot \left(1+\dfrac{2}{m}\right)^{h-1} = \mathsf{poly}(\lambda)$. All arguments with respect to $\mathbf{N}$ also hold well. □

Proof (of Lemma 4.4). Only for this lemma, we give the proof of the two cases; $\mathbf{P} = \mathbf{M}$ and $\mathbf{P} = \mathbf{N}$.

Case 1: $\mathbf{J} \cdot \hat{S}^{(\mathbf{M})}_{1,x_1} \cdot E^{(\mathbf{M})}_{2,x_2} \cdot \prod_{k=3}^{h} D^{(\mathbf{M})}_{k,x_k}$.

Indeed, this case is a special case of Lemma 4.5. Readers refer to the proof of Lemma 4.5. In particular, we can obtain that

$$Var[(Z^{(\mathbf{M})}_{1,1})_1] = (n^3 \cdot \sigma + (2\ell-1)\cdot n^2)\cdot m^{h-2} \cdot (\sigma^2)^h$$

and

$$E[(Z^{(\mathbf{M})}_{1,1})_1^4] \leq (w+2n\ell)^4 \cdot (27n^8 \cdot (n(n+2))^{j_1+j-1} \cdot (m(m+2))^{h-j-1} \cdot (\sigma^2)^{2(h+j_1+1)}.$$

Combining this we obtain the inequality

$$\left|\frac{E[(Z_{1,1}^{(\mathbf{M})})_1^4]}{Var[(Z_{1,1}^{(\mathbf{M})})_1]^2}\right| \leq 27 \cdot (w+2n\ell)^4 \cdot n^2 \cdot \left(1+\frac{2}{n}\right)^{j_1+j-1} \cdot \left(1+\frac{2}{m}\right)^{h-j-1}.$$

Case 2: $\mathbf{J} \cdot \hat{S}_{1,x_1}^{(\mathbf{N})} \cdot E_{2,x_2}^{(\mathbf{N})} \cdot \prod_{k=3}^{h} D_{k,x_k}^{(\mathbf{N})}$.

Since $\hat{S}_{1,x_1}^{(\mathbf{N})}$ is $\mathsf{diag}(\mathbf{1}^{w\times w} \otimes S_{1,x_1}^{(\mathbf{N})}, \mathbf{0}^{n^2\times n^2}) + \mathsf{diag}(\mathbf{0}^{wn\times wn}, R_{1,x_1}^{(\mathbf{N})} \otimes S_{1,x_1})^{(\mathbf{N})}$, the random variable can be written as

$$\begin{aligned}\mathbf{J} \cdot \hat{S}_{1,x_1}^{(\mathbf{N})} \cdot E_{2,x_2}^{(\mathbf{N})} \cdot \prod_{k=3}^{h} D_{k,x_k}^{(\mathbf{N})} &= \mathbf{J} \cdot \mathsf{diag}(\mathbf{1}^{w\times w} \otimes S_{1,x_1}^{(\mathbf{N})}, \mathbf{0}^{n^2\times n^2}) \cdot E_{2,x_2}^{(\mathbf{N})} \cdot \prod_{k=3}^{h} D_{k,x_k}^{(\mathbf{N})} \\ &\quad + \mathbf{J} \cdot \mathsf{diag}(\mathbf{0}^{wn\times wn}, R_{1,x_1}^{(\mathbf{N})} \otimes S_{1,x_1}^{(\mathbf{N})}) E_{2,x_2}^{(\mathbf{N})} \cdot \prod_{k=3}^{h} D_{k,x_k}^{(\mathbf{N})}.\end{aligned}$$

By the lemma C.1, the variance of the random matrix $\mathbf{J} \cdot \hat{S}_{1,x_1}^{(\mathbf{N})} \cdot E_{2,x_2}^{(\mathbf{N})} \cdot \prod_{k=3}^{h} D_{k,x_k}^{(\mathbf{N})}$ is equal to summation of variances of two above two random matrices.

We only need to compute the variance of the first random matrix $\mathbf{J} \cdot \mathsf{diag}(\mathbf{1}^{w\times w} \otimes S_{1,x_1}^{(\mathbf{N})}, \mathbf{0}^{n^2\times n^2}) \cdot E_{2,x_2}^{(\mathbf{N})} \cdot \prod_{k=3}^{h} D_{k,x_k}^{(\mathbf{N})}$; the variance of the latter term is a special case of the Lemma 4.5 as the above case.

Let $S_{u,v}^{(\mathbf{N})}$ be the random variables of (u,v)-th entry of the random matrix $S_{1,x_1}^{(\mathbf{N})}$. We define $X_{u,v}^{(\mathbf{N})}$, $Y_{u,v}^{(\mathbf{N})}$ and $(Z_{u,v}^{(\mathbf{N})})_1$ be random variables of the (u,v)-th entry of the random matrix $E_{2,x_2}^{(\mathbf{N})} \cdot \prod_{k=3}^{h} D_{k,x_k}^{(\mathbf{N})}$, $\hat{S}_{1,x_1}^{(\mathbf{N})} \cdot E_{2,x_2}^{(\mathbf{N})} \cdot \prod_{k=3}^{h} D_{k,x_k}^{(\mathbf{N})}$ and $\mathbf{J} \cdot \hat{S}_{1,x_1}^{(\mathbf{N})} \cdot E_{2,x_2}^{(\mathbf{N})} \cdot \prod_{k=3}^{h} D_{k,x_k}^{(\mathbf{N})}$, respectively.

Then, we observe $Y_{1,1}^{(\mathbf{N})} = \sum_{i=1}^{n} S_{1,i}^{(\mathbf{N})} \cdot X_{i,1}^{(\mathbf{N})} + \cdots + \sum_{i=1}^{n} S_{1,i}^{(\mathbf{N})} \cdot X_{i+(w-1)n,1}^{(\mathbf{N})}$ from the definition of Kronecker tensor properties. Then, using Lemma C.1, we can obtain

$$\begin{aligned}Var[Y_{1,1}^{(\mathbf{N})}] &= E[(\sum_{i=1}^{n} S_{1,i}^{(\mathbf{N})} \cdot X_{i,1}^{(\mathbf{N})} + \cdots + \sum_{i=1}^{n} S_{1,i}^{(\mathbf{N})} \cdot X_{i+(w-1)n,1}^{(\mathbf{N})})^2] \\ &= E[\sum_{i=1}^{n} S_{1,i}^{(\mathbf{N})^2} \cdot X_{i,1}^{(\mathbf{N})^2} + \cdots + \sum_{i=1}^{n} S_{1,i}^{(\mathbf{N})^2} \cdot X_{i+(w-1)n,1}^{(\mathbf{N})^2}] \\ &= wn \cdot (\sigma^2) \cdot m^{h-2} \cdot (\sigma^2)^{h-1} \\ &= wn \cdot m^{h-2} \cdot (\sigma^2)^h.\end{aligned}$$

Moreover, we can calculate an upper bound of $E[Y_{1,1}^{(\mathbf{N})^4}]$ as follows:

$$\begin{aligned}E[Y_{1,1}^{(\mathbf{N})^4}] &= E\left[(\sum_{i=1}^{n} S_{1,i}^{(\mathbf{N})} \cdot X_{i,1}^{(\mathbf{N})} + \cdots + \sum_{i=1}^{n} S_{1,i}^{(\mathbf{N})} \cdot X_{i+(w-1)n,1}^{(\mathbf{N})})^4\right] \\ &\leq E\left[(wn)^3 \cdot (\sum_{i=1}^{n} S_{1,i}^{(\mathbf{N})^4} \cdot X_{i,1}^{(\mathbf{N})^4} + \cdots + \sum_{i=1}^{n} S_{1,i}^{(\mathbf{N})^4} \cdot X_{i+(w-1)n,1}^{(\mathbf{N})^4})\right] \\ &= (wn)^4 \cdot 3(\sigma^2)^2 \cdot \{m(m+2)\}^{h-2} \cdot (\sigma^2)^{2(h-1)} \\ &= 3(wn)^4 \cdot \{m(m+2)\}^{h-2} \cdot (\sigma^2)^{2h}.\end{aligned}$$

Similarly, we can compute $Y_{i,1}^{(\mathbf{N})}$ for $i = 2, \cdots, wn$ in the exactly same way. The equations and inequalities are all equal to the $Y_{1,1}^{(\mathbf{N})}$ case. For $i > wn$, $Y_{i,1}^{(\mathbf{N})}$ is computed as in Case 1. In other words, it is the special case $j = 1$ of Lemma 4.5 and the result is equal to Case 1 as well. Thus, we omit the how to compute this value.

Note that $Y^{(\mathbf{N})}_{i,1} = Y^{(\mathbf{N})}_{i+(k-1)n,1}$ for all $k = 1, \cdots, wn$. Thus, we obtain the desired results as follows:

$$\begin{aligned}
Var[(Z^{(\mathbf{N})}_{1,1})_1] &= E[(\sum_{i=1}^{w+2n\ell} Y^{(\mathbf{N})}_{1+(i-1)n,1})^2] \\
&= E[w^2 \cdot {Y^{(\mathbf{N})}_{1,1}}^2 + \sum_{i=w+1}^{w+2n\ell} {Y^{(\mathbf{N})}_{1+(i-1)n,1}}^2] \\
&= (w^3 \cdot n + n^3 \cdot \sigma^2 + (2\ell - 1) \cdot n^2) \cdot m^{h-2} (\sigma^2)^h \\
E[(Z^{(\mathbf{N})}_{1,1})^4_1] &= E\left[(\sum_{i=1}^{w+2n\ell} Y^{(\mathbf{N})}_{1+(i-1)n,1})^4 \right] \\
&\leq E[(w+2n\ell)^3 \cdot (\sum_{i=1}^{w+2n\ell} {Y^{(\mathbf{N})}_{1+(i-1)n,1}}^4)] \\
&\leq (w+2n\ell)^4 \cdot (27n^8 \cdot (n(n+2)))^{j_1+j-1} \cdot (m(m+2))^{h-j-1} \cdot (\sigma^2)^{2(h+j_1+1)}
\end{aligned}$$

At last, with the two computations, we obtain

$$\left| \frac{E[(Z^{(\mathbf{N})}_{1,1})^4_1]}{Var[(Z^{(\mathbf{N})}_{1,1})_1]^2} \right| \leq 27 \cdot (w+2n\ell)^4 \cdot n^2 \cdot \left(1 + \frac{2}{n}\right)^{j_1+j-1} \cdot \left(1 + \frac{2}{m}\right)^{h-j-1} = \mathsf{poly}(\lambda).$$

□

Proof (of Lemma 4.5). We remark that, as noted in the above proof, this proof works for $j = 1$ as well and this case is used in the above proof. It suffice to prove the case $\mathbf{P} = \mathbf{M}$. Let $1 \leq j < \lambda \cdot \ell$ be an integer that $j = \ell \cdot j_1 + j_2$ and $X^{(\mathbf{M})}_{u,v}$ the random variables of the (u,v)-th entry of the random matrix $E^{(\mathbf{M})}_{j+1,x_{j+1}} \prod_{k=j+2}^{h} D^{(\mathbf{M})}_{k,x_k}$. Then, all random variables $X_{u,v}$ have the same variance $m^{h-j-1} \cdot (\sigma^2)^{h-j}$, and we have $E[X^{(\mathbf{M})}_{u,v} \cdot X^{(\mathbf{M})}_{u',v}] = 0$ for distinct u, u' and $E[{X^{(\mathbf{M})}_{u,v}}^4] = 3\,(m(m+2))^{h-j-1} \cdot (\sigma^2)^{2(h-j)}$.

Let $S^{(\mathbf{M})}_{u,v}$ be the random variable of (u,v)-th entry of the random matrix $\prod_{i=1}^{j} S^{(\mathbf{M})}_{i,x_i}$. Then, $Var[S^{(\mathbf{M})}_{u,v}] = n^{j-1} \cdot (\sigma^2)^j$, $E[S^{(\mathbf{M})}_{u,v} \cdot S^{(\mathbf{M})}_{u',v}] = 0$ for distinct u, u' and $E[{S^{(\mathbf{M})}_{u,v}}^4] = 3\{n(n+2)\}^{j-1} \cdot (\sigma^2)^{2j}$ hold.

By the construction of the matrix $R^{(\mathbf{M})}_{i,x_i}$, $\prod_{i=1}^{j} R^{(\mathbf{M})}_{i,x_i}$ is a block-diagonal matrix that consists of $\prod_{i=1}^{j} {R^{(k)}_{i,x_i}}^{(\mathbf{M})} \in \mathbb{Z}^{2n \times 2n}$ for $k \in [\ell]$. Note that $\prod_{i=1}^{j} {R^{(k)}_{i,x_i}}^{(\mathbf{M})}$ is of the form

$$\prod_{i=1}^{j} {R^{(k)}_{i,x_i}}^{(\mathbf{M})} = \begin{cases} \begin{pmatrix} \prod_{i=1}^{j_1+1} {\tilde{R}^{(k)}_{k+\ell(i-1),x_{k+\ell(i-1)}}}^{(\mathbf{M})} & \\ & \mathbf{I}^{n \times n} \end{pmatrix} & \text{if } k = 1, 2, \cdots, j_2 \\ \begin{pmatrix} \prod_{i=1}^{j_1} {\tilde{R}^{(k)}_{k+\ell(i-1),x_{k+\ell(i-1)}}}^{(\mathbf{M})} & \\ & \mathbf{I}^{n \times n} \end{pmatrix} & \text{if } k = j_2 + 1, \cdots, \ell \end{cases}$$

Let $R^{(\mathbf{M})}_{u,v}$ be the random variables of the (u,v)-th entry of the random matrix upper-left quadrant of $\prod_{i=1}^{j} {R^{(1)}_{i,x_i}}^{(\mathbf{M})}$. Then $Var[{R^{(\mathbf{M})}_{u,v}}^2] = n^{j_1} \cdot (\sigma^2)^{j_1+1}$, $E[R^{(\mathbf{M})}_{u,v} \cdot R^{(\mathbf{M})}_{u',v}] = 0$ and $E[{R^{(\mathbf{M})}_{u,v}}^4] = 3(n(n+2))^{j_1} \cdot (\sigma^2)^{2(j_1+1)}$.

Similarly, we consider the random variables of the (u,v)-th entry of the matrix $\left(\prod_{i=1}^{j} \hat{S}^{(\mathbf{M})}_{i,x_i}\right) \cdot E^{(\mathbf{M})}_{j+1,x_{j+1}} \cdot \left(\prod_{k=j+2}^{h} D^{(\mathbf{M})}_{k,x_k}\right)$ and denote it by $Y^{(\mathbf{M})}_{u,v}$. Then,

$$\begin{aligned}
Var[Y^{(\mathbf{M})}_{1+wn,1}] &= E[(R^{(\mathbf{M})}_{1,1} \sum_{i=1}^{n} S^{(\mathbf{M})}_{1,i} X^{(\mathbf{M})}_{i+wn,1} + \cdots + R^{(\mathbf{M})}_{1,n} \sum_{i=1}^{n} S^{(\mathbf{M})}_{1,i} X^{(\mathbf{M})}_{i+n(w+n-1),1})^2] \\
&= n^2 \cdot n^{j_1} \cdot (\sigma^2)^{j_1+1} \cdot n^{j-1} \cdot (\sigma^2)^j \cdot m^{h-j-1} \cdot (\sigma^2)^{h-j} \\
&= n^{j_1+j+1} \cdot (\sigma^2)^{j_1+j+1} \cdot m^{h-j-1} \cdot (\sigma^2)^{h-j}
\end{aligned}$$

because of Lemma C.1. Moreover, it holds that

$$\begin{aligned}
E[Y_{1+wn,1}^{(\mathbf{M})^4}] &= E[(R_{1,1}^{(\mathbf{M})}\sum_{i=1}^{n} S_{1,i}^{(\mathbf{M})} X_{i+wn,1}^{(\mathbf{M})} + \cdots + R_{1,n}^{(\mathbf{M})}\sum_{i=1}^{n} S_{1,i}^{(\mathbf{M})} X_{i+n(w+n-1),1}^{(\mathbf{M})})^4] \\
&\leq E[(n^2)^3(R_{1,1}^{(\mathbf{M})^4}\sum_{i=1}^{n} S_{1,i}^{(\mathbf{M})^4} X_{i+wn,1}^{(\mathbf{M})^4} + \cdots + R_{1,n}^{(\mathbf{M})^4}\sum_{i=1}^{n} S_{1,i}^{(\mathbf{M})^4} X_{i+n(w+n-1),1}^{(\mathbf{M})^4})] \\
&= 27n^8 \cdot (n(n+2))^{j_1+j-1} \cdot (m(m+2))^{h-j-1} \cdot (\sigma^2)^{2(h+j_1+1)}.
\end{aligned}$$

Therefore, we conclude that

$$\left| \frac{E[Y_{1+wn,1}^{(\mathbf{M})^4}]}{var[Y_{1+wn,1}^{(\mathbf{M})}]^2} \right| \leq 27 \cdot n^4 \cdot \left(1+\frac{2}{n}\right)^{j_1+j-1} \cdot \left(1+\frac{2}{m}\right)^{h-j-1}.$$

Similarly, we can compute all variances of $Y_{i,1}$ for each i.

$$Var[Y_{i,1}^{(\mathbf{M})}] = \begin{cases}
0 & \text{if } i \in [wn] \\
n^{j_1+j+1} \cdot (\sigma^2)^{j_1+j+1} \cdot m^{h-j-1} \cdot (\sigma^2)^{h-j} & \text{if } i = a \cdot n^2 + b + w \cdot n \text{ with } a/2 \in \{0\} \cup [j_2 - 1], b \in [n^2] \\
n^{j_1+j} \cdot (\sigma^2)^{j_1+j} \cdot m^{h-j-1} \cdot (\sigma^2)^{h-j} & \text{if } i = a \cdot n^2 + b + w \cdot n \text{ with } a/2 \in \{j_2, \cdots, \ell\}, b \in [n^2] \\
n^{j} \cdot (\sigma^2)^{j} \cdot m^{h-j-1} \cdot (\sigma^2)^{h-j} & \text{otherwise.}
\end{cases}$$

Thus, we can derive upper bounds of $E[Y_{i,1}^4]$ as follows:

$$E[Y_{i,1}^{(\mathbf{M})^4}] \leq \begin{cases}
0 \\
27n^8 \cdot \{n(n+2)\}^{j_1+j-1} \cdot \{m(m+2)\}^{h-j-1} \cdot (\sigma^2)^{2(h+j_1+1)} \\
27n^8 \cdot \{n(n+2)\}^{j_1+j-2} \cdot \{m(m+2)\}^{h-j-1} \cdot (\sigma^2)^{2(h+j_1)} \\
9n^4 \cdot \{n(n+2)\}^{j-1} \cdot \{m(m+2)\}^{h-j-1} \cdot (\sigma^2)^{2h}
\end{cases}$$

Let $(Z_{u,v}^{(\mathbf{M})})_j$ be random variable of (u,v)-th entry of the matrix $\mathbf{J} \cdot \left(\prod_{i=1}^{j} \hat{S}_{i,x_i}^{(\mathbf{M})}\right) \cdot E_{j+1,x_{j+1}}^{(\mathbf{M})} \cdot \left(\prod_{k=j+2}^{h} D_{k,x_k}^{(\mathbf{M})}\right)$. Then, we observe $(Z_{1,1}^{(\mathbf{M})})_j = \sum_{i=1}^{w+2n\ell} Y_{1+(i-1)n,1}^{(\mathbf{M})}$. Since, by Lemma C.1, $E[S_{u,v}^{(\mathbf{M})} \cdot S_{u',v}^{(\mathbf{M})}] = 0$, $E[R_{u,v}^{(\mathbf{M})} \cdot R_{u',v}^{(\mathbf{M})}] = 0$, and $E[X_{u,v}^{(\mathbf{M})} \cdot X_{u',v}^{(\mathbf{M})}] = 0$ hold for all distinct u, u', the equation $E[Y_{u,1}^{(\mathbf{M})} \cdot Y_{v,1}^{(\mathbf{M})}] = 0$ holds for all u, v.

With the similar method, we compute $Var[(Z_{1,1}^{(\mathbf{M})})_j]$ and upper bound of $E[(Z_{1,1}^{(\mathbf{M})})_j^4]$.

$$\begin{aligned}
Var[(Z_{1,1}^{(\mathbf{M})})_j] &= E[(\sum_{i=1}^{w+2n\ell} Y_{1+(i-1)n,1}^{(\mathbf{M})})^2] = E[\sum_{i=1}^{w+2n\ell} Y_{1+(i-1)n,1}^{(\mathbf{M})^2}] \\
&= j_2 n \cdot n^{j_1+j+1} \cdot (\sigma^2)^{j_1+j+1} \cdot m^{h-j-1} \cdot (\sigma^2)^{h-j} \\
&+ (\ell - j_2)n \cdot n^{j_1+j} \cdot (\sigma^2)^{j_1+j} \cdot m^{h-j-1} \cdot (\sigma^2)^{h-j} \\
&+ \ell n \cdot n^{j} \cdot (\sigma^2)^{j} \cdot m^{h-j-1} \cdot (\sigma^2)^{h-j} \\
&= \left(j_2 n^{j_1+j+2} \cdot (\sigma^2)^{j_1+1} + (\ell - j_2) n^{j_1+j+1} \cdot (\sigma^2)^{j_1} + \ell n^{j+1}\right) \cdot m^{h-j-1} \cdot (\sigma^2)^{h}
\end{aligned}$$

$$
\begin{aligned}
E[(Z^{(\mathbf{M})}_{1,1})^4_j] &= E[(\sum_{i=1}^{w+2n\ell} Y^{(\mathbf{M})}_{1+(i-1)n,1})^4] \\
&\le E[(w+2n\ell)^3 \cdot (\sum_{i=1}^{w+2n\ell} {Y^{(\mathbf{M})}}^4_{1+(i-1)n,1})] \\
&\le (w+2n\ell)^3 \cdot (j_2 n \cdot 27n^8 \cdot (n(n+2))^{j_1+j-1} \cdot (m(m+2))^{h-j-1} \cdot (\sigma^2)^{2(h+j_1+1)} \\
&+ (\ell - j_2)n \cdot 27n^8 \cdot (n(n+2))^{j_1+j-2} \cdot (m(m+2))^{h-j-1} \cdot (\sigma^2)^{2(h+j_1)} \\
&+ \ell n \cdot 9n^4 \cdot (n(n+2))^{j-1} \cdot \{m(m+2)\}^{h-j-1} \cdot (\sigma^2)^{2h}) \\
&\le (w+2n\ell)^4 \cdot (27n^8 \cdot (n(n+2))^{j_1+j-1} \cdot (m(m+2))^{h-j-1} \cdot (\sigma^2)^{2(h+j_1+1)}
\end{aligned}
$$

Overall, we obtain

$$
\left| \frac{E[(Z^{(\mathbf{M})}_{1,1})^4_j]}{Var[(Z^{(\mathbf{M})}_{1,1})_j]^2} \right| \le 27 \cdot (w+2n\ell)^4 \cdot n^2 \cdot \left(1 + \frac{2}{n}\right)^{j_1+j-1} \cdot \left(1 + \frac{2}{m}\right)^{h-j-1}.
$$

All arguments for $\mathbf{N}$ hold as well.

□

Proof (of Lemma 4.6). Let j be an integer that $j > \lambda \cdot \ell$ and $j = \ell \cdot \lambda + j_2$. This proof is very similar to Lemma 4.4. The difference only comes from a form of the random matrix $\prod_{i=1}^{j} R_{i,x_i}$. Thus, in this proof, we focus on the form of the matrix. Note that, because of the functionality, the matrices $R_{i,b}$ are completely different for $i \le \lambda \cdot \ell$ and for $i > \lambda \cdot \ell$. We also focus on $\mathbf{P} = \mathbf{M}$.

In this case, $\prod_{i=1}^{j} R_{i,x_i}$ is the block diagonal matrix

$$
\prod_{i=1}^{j} R_{i,x_i} = \mathsf{diag}(\prod_{i=1}^{j} R^{(1)}_{i,x_i}, \prod_{i=1}^{j} R^{(2)}_{i,x_i}, \cdots, \prod_{i=1}^{j} R^{(\ell)}_{i,x_i})
$$

where $\prod_{i=1}^{j} R^{(k)}_{i,x_i}$ is of the form

$$
\begin{cases}
\begin{pmatrix} -\prod_{i=1}^{\lambda} \tilde{R}^{(k)}_{k+\ell(i-1),x_{k+\ell(i-1)}} & \\ & \prod_{i=1}^{\lambda} \tilde{R}^{(k)}_{k+\ell(i-1),x_{k+\ell(i-1)}} \end{pmatrix} & \text{if } k = 1, 2, \cdots, j_2 \\
\begin{pmatrix} \prod_{i=1}^{\lambda} \tilde{R}^{(k)}_{k+\ell(i-1),x_{k+\ell(i-1)}} & \\ & \mathbf{I} \end{pmatrix} & \text{if } k = j_2 + 1, \cdots, \ell
\end{cases}
$$

Let $Y^{(\mathbf{M})}_{u,v}$ and $(Z^{(\mathbf{M})}_{u,v})_j$ be random variable of (u,v)-th entry of the matrix $\left(\prod_{i=1}^{j} \hat{S}^{(\mathbf{M})}_{i,x_i}\right) \cdot E^{(\mathbf{M})}_{j+1,x_{j+1}} \cdot \left(\prod_{k=j+2}^{h} D^{(\mathbf{M})}_{k,x_k}\right)$ and $\mathbf{J} \cdot \left(\prod_{i=1}^{j} \hat{S}^{(\mathbf{M})}_{i,x_i}\right) \cdot E^{(\mathbf{M})}_{j+1,x_{j+1}} \cdot \left(\prod_{k=j+2}^{h} D^{(\mathbf{M})}_{k,x_k}\right)$, respectively.

Similarly, we get

$$
\begin{aligned}
Var[(Z^{(\mathbf{M})}_{1,1})_j] &= E\left[(\sum_{i=1}^{w+2n\ell} Y^{(\mathbf{M})}_{1+(i-1)n,1})^2 \right] \\
&= E\left[\sum_{i=1}^{w+2n\ell} {Y^{(\mathbf{M})}}^2_{1+(i-1)n,1} \right] \\
&= \left((\ell + j_2)n^{\lambda+j+1} \cdot (\sigma^2)^{\lambda} + (\ell - j_2)n^{j+1}\right) \cdot m^{h-j-1} \cdot (\sigma^2)^h
\end{aligned}
$$

and

$$
\begin{aligned}
E[(Z^{(\mathbf{M})}_{1,1})^4_j] &= E[(\sum_{i=1}^{w+2n\ell} Y^{(\mathbf{M})}_{1+(i-1)n,1})^4] \\
&\le E[(w+2n\ell)^3 \cdot (\sum_{i=1}^{w+2n\ell} {Y^{(\mathbf{M})}}^4_{1+(i-1)n,1})] \\
&\le (w+2n\ell)^4 \cdot (27n^8 \cdot (n(n+2))^{\lambda+j-2} \cdot (m(m+2))^{h-j-1} \cdot (\sigma^2)^{2(h+\lambda)}
\end{aligned}
$$

Then, we have

$$\left|\frac{E[(Z_{1,1}^{(\mathbf{M})})_j^4]}{Var[(Z_{1,1}^{(\mathbf{M})})_j]^2}\right| \le 27(w+2n\ell)^4 n^2 \cdot \left(1+\frac{2}{n}\right)^{\lambda+j-2} \cdot \left(1+\frac{2}{m}\right)^{h-j-1}.$$

The arguments for $\mathbf{N}$ hold as well. □

E Analysis of BGMZ Obfuscation

In this section, we describe how to proof lemmas in Section 5.2. We modify the notation as in the CVW obfuscation case. We replace n', n with n, t. We re-use or abuse the some notations for the different proof for the convenience of the writing. For example, we omit the index j in the main body of the paper. Fix a $\mathbf{x} \in \{0,1\}^\ell$ satisfying $\mathcal{O}(\mathbf{P})(\mathbf{x}) = \mathbf{0}$.

By Lemma 2.9, each column of the random matrix $D_{i,\boldsymbol{x}_i}^{(\mathbf{P})}$ follows a distribution $\mathcal{D}_{\mathbb{Z}^m,\sigma}$ for all i. Since $\mathcal{D}_{\mathbb{Z}^m,\sigma}$ is equal to $\mathcal{D}_{\mathbb{Z},\sigma}^m$, entries of each column are mutually independent. Therefore, we can use Lemma C.1 and C.2 when we analyze product of $D_{i,\boldsymbol{x}_i}^{(\mathbf{P})}$. Note that all distributions are independent except the tuples related to trapdoor samplings as in the CVW obfuscation. We omit the proof of Lemma 5.2 since it is almost the same to the proof of Lemma 4.2.

Proof (of Lemma 5.3). Let $(X_{u,v}^{(\mathbf{M})})$ be random variables of the (u,v)-th entry of the random matrix $E_{\boldsymbol{x}(1)}^{(\mathbf{M})} \prod_{k=2}^h D_{k,\boldsymbol{x}(k)}^{(\mathbf{M})}$. Then, for all $u \in [t], v \in [n]$, all random variables $X_{u,v}^{(\mathbf{M})}$ have the same variance $m^{h-1}(\sigma^2)^{h-1} \cdot s^2$. Moreover, it holds that $E[X_{u,v}^{(\mathbf{M})} \cdot X_{u',v}^{(\mathbf{M})}] = 0$ for distinct u, u' and $E[{X_{u,v}^{(\mathbf{M})}}^4] = 3\,(m(m+2))^{h-1} \cdot (\sigma^2)^{2(h-1)} \cdot (s^2)^2$.

Similarly, the random variables of the (u,v)-th entry of the random matrix $J^{(\mathbf{M})} \cdot E_{1,\boldsymbol{x}(1)}^{(\mathbf{M})} \prod_{k=2}^h D_{k,\boldsymbol{x}(k)}^{(\mathbf{M})}$ are denoted by $Y_{u,v}^{(\mathbf{M})}$. J is defined by $[J'^{(\mathbf{M})} | \mathbf{I}^{n\times n}]$ and $J'^{(\mathbf{M})} \leftarrow \{0,1\}^{n\times wn}$. Let the random variables of the (u,v)-th entry of the random matrix $J'^{(\mathbf{M})}$ be denoted by $J'^{(\mathbf{M})}_{u,v}$. Then we can observe that $E[J'^{(\mathbf{M})}_{u,v}] = \frac{1}{2}$, $E[{J'^{(\mathbf{M})}_{u,v}}^2] = \frac{1}{2}$, $E[{J'^{(\mathbf{M})}_{u,v}}^4] = \frac{1}{2}$ for all u, v.

Since $Y_{1,1}^{(\mathbf{M})} = \sum_{i=1}^w J'^{(\mathbf{M})}_{1,n\cdot(t-1)+1} \cdot X_{n\cdot(t-1)+1,1}^{(\mathbf{M})} + X_{wn+1,1}^{(\mathbf{M})}$,

$$\begin{aligned} Var[Y_{1,1}^{(\mathbf{M})}] &= E\left[\left(\sum_{i=1}^w J'^{(\mathbf{M})}_{1,n\cdot(t-1)+1} \cdot X_{n\cdot(t-1)+1,1}^{(\mathbf{M})} + X_{wn+1,1}^{(\mathbf{M})}\right)^2\right] \\ &= E\left[\sum_{i=1}^w {J'^{(\mathbf{M})}_{1,n\cdot(t-1)+1}}^2 \cdot {X_{n\cdot(t-1)+1,1}^{(\mathbf{M})}}^2 + {X_{wn+1,1}^{(\mathbf{M})}}^2\right] \\ &= (\frac{w}{2}+1) \cdot m^{h-1} \cdot (\sigma^2)^{h-1} \cdot s^2. \end{aligned}$$

In addition, the upper bound of $E[{Y_{1,1}^{(\mathbf{M})}}^4]$ can be computed

$$\begin{aligned} E[{Y_{1,1}^{(\mathbf{M})}}^4] &= E[(\sum_{i=1}^w J'^{(\mathbf{M})}_{1,n(t-1)+1} \cdot X_{n(t-1)+1,1}^{(\mathbf{M})} + X_{wn+1}^{(\mathbf{M})})^4] \\ &\le E[(w+1)^3 \cdot (\sum_{i=1}^w {J'^{(\mathbf{M})}_{1,n(t-1)+1}}^4 \cdot {X_{n(t-1)+1,1}^{(\mathbf{M})}}^4 + {X_{wn+1}^{(\mathbf{M})}}^4)] \\ &\le (w+1)^4 \cdot 3\{m(m+2)\}^{h-1} \cdot (\sigma^2)^{2(h-1)} \cdot (s^2)^2. \end{aligned}$$

Similarly, we can derive the same results for $Y_{u,v}$ for all u, v. The variance of $(Z^{(\mathbf{M})})_0 = v'^{(\mathbf{M})} \cdot J^{(\mathbf{M})} \cdot E_{1,\boldsymbol{x}(1)}^{(\mathbf{M})} \prod_{k=2}^h D_{k,\boldsymbol{x}(k)}^{(\mathbf{M})} \cdot {w'^{(\mathbf{M})}}^T$ is computed by

$$Var[(Z^{(\mathbf{M})})_0] = nm \cdot (\frac{w}{2}+1) \cdot m^{h-1} \cdot (\sigma^2)^{h-1} \cdot s^2 \cdot \sigma^4 = nm \cdot (\frac{w}{2}+1) \cdot m^{h-1} \cdot (\sigma^2)^{h+1} \cdot s^2$$

We also have

$$\begin{aligned}E[(Z^{(\mathbf{M})})_0^4] &\le (nm)^4\cdot(w+1)^4\cdot 3\{m(m+2)\}^{h-1}\cdot(\sigma^2)^{2(h-1)}\cdot(s^2)^2\cdot(3\sigma^4)^2\\ &= 27\cdot(nm)^4\cdot(w+1)^4\cdot\{m(m+2)\}^{h-1}\cdot(\sigma^2)^{2(h+1)}\cdot(s^2)^2\end{aligned}$$

At last the upper bound is computed as

$$\left|\frac{E[(Z^{(\mathbf{M})})_0^4]}{Var[(Z^{(\mathbf{M})})_0]^2}\right| \le 108\cdot(nm)^2\cdot(w+1)^2\cdot\left(1+\frac{2}{m}\right)^{h-1} = \mathsf{poly}(\lambda)$$

For $\mathbf{N}$, all arguments are exactly same. □

Proof (of Lemma 5.4). In this proof we consider the two cases; $\mathbf{P}=\mathbf{M}$ and $\mathbf{P}=\mathbf{N}$.

Case 1: $v'^{(\mathbf{M})}\cdot J^{(\mathbf{M})}\cdot\hat{S}^{(\mathbf{M})}_{1,\boldsymbol{x}(1)}\cdot E^{(\mathbf{M})}_{2,\boldsymbol{x}(2)}\prod_{k=3}^{h} D^{(\mathbf{M})}_{k,\boldsymbol{x}(k)} w'^{(\mathbf{M})^T}$ **.** This is the special case $j=1$ of Lemma 5.5. Readers refer to the proof of Lemma 5.5. Based on this the following equation and inequalities hold:

$$\begin{aligned}Var[(Z^{(\mathbf{M})})_1] &= nm\cdot n\cdot m^{h-2}\cdot(\sigma^2)^{h+1}\cdot s^2\\ E[(Z^{(\mathbf{M})})_1^4] &\le 81\cdot(nm)^4\cdot n^4\cdot\{m(m+2)\}^{h-2}\cdot(\sigma^2)^{2(h+1)}\cdot s^4\\ \left|\frac{E[(Z^{(\mathbf{M})})_1^4]}{Var[(Z^{(\mathbf{M})})_1]^2}\right| &\le 81\cdot(nm)^2\cdot n^2\cdot\left(1+\frac{2}{m}\right)^{h-2}\end{aligned}$$

Case 2: $v'^{(\mathbf{N})}\cdot J^{(\mathbf{N})}\cdot\hat{S}^{(\mathbf{N})}_{1,\boldsymbol{x}(1)}\cdot E^{(\mathbf{N})}_{2,\boldsymbol{x}(2)}\cdot\prod_{k=3}^{h} D^{(\mathbf{N})}_{k,\boldsymbol{x}(k)}\cdot w'^{(\mathbf{N})^T}$**.** Let $S^{(\mathbf{N})}_{u,v}$ be random variables of (u,v)-th entry of the random matrix $S^{(\mathbf{N})}_{1,\boldsymbol{x}(1)}$. Similarly, we define $X^{(\mathbf{N})}_{u,v}$ and $Y^{(\mathbf{N})}_{u,v}$ are random variables of the (u,v)-th entry of the random matrix $E^{(\mathbf{N})}_{2,\boldsymbol{x}(2)}\prod_{k=3}^{h} D^{(\mathbf{N})}_{k,\boldsymbol{x}(k)}$ and $J^{(\mathbf{N})}\cdot\hat{S}^{(\mathbf{N})}_{1,\boldsymbol{x}(1)}\cdot E^{(\mathbf{N})}_{2,\boldsymbol{x}(2)}\cdot\prod_{k=3}^{h} D^{(\mathbf{N})}_{k,\boldsymbol{x}(k)}$, respectively. $J^{(\mathbf{N})}$ is defined by $[J'^{(\mathbf{N})}|\mathbf{I}^{n\times n}]$ and $J'^{(\mathbf{N})}\leftarrow\{0,1\}^{n\times wn}$. The random variables of the (u,v)-th entry of the random matrix $J'^{(\mathbf{N})}$ is denoted by $J'^{(\mathbf{N})}_{u,v}$.

Then, we observe

$$Y^{(\mathbf{N})}_{1,1} = \sum_{j=1}^{w}\sum_{i=1+n(j-1)}^{nj}(\sum_{k=1}^{n} J'^{(\mathbf{N})}_{k+n(j-1)}\cdot S^{(\mathbf{N})}_{k,i-n(j-1)})\cdot X^{(\mathbf{N})}_{i,1} + \sum_{k=1}^{n} S^{(\mathbf{M})}_{1,k}\cdot X^{(\mathbf{M})}_{wn+k,1}.$$

By Lemma C.1,

$$\begin{aligned}&Var[Y^{(\mathbf{N})}_{1,1}]\\ &= E\left[\left(\sum_{j=1}^{w}\sum_{i=1+n(j-1)}^{nj}(\sum_{k=1}^{n} J'^{(\mathbf{N})}_{k+n(j-1)}\cdot S^{(\mathbf{N})}_{k,i-n(j-1)})\cdot X^{(\mathbf{N})}_{i,1} + \sum_{k=1}^{n} S^{(\mathbf{N})}_{1,k}\cdot X^{(\mathbf{N})}_{wn+k,1}\right)^2\right]\\ &= E\left[\sum_{j=1}^{w}\sum_{i=1+n(j-1)}^{nj}(\sum_{k=1}^{n} J'^{(\mathbf{N})^2}_{k+n(j-1)}\cdot S^{(\mathbf{N})^2}_{k,i-n(j-1)})\cdot X^{(\mathbf{N})^2}_{i,1} + \sum_{k=1}^{n} S^{(\mathbf{N})^2}_{1,k}\cdot X^{(\mathbf{N})^2}_{wn+k,1}\right]\\ &= wn\cdot\left(\frac{n}{2}\cdot\sigma^2\right)\cdot m^{h-2}\cdot(\sigma^2)^{h-2}\cdot s^2 + n\cdot\sigma^2\cdot m^{h-2}\cdot(\sigma^2)^{h-2}\cdot s^2\\ &= \left(\frac{1}{2}\cdot wn+1\right)\cdot n\cdot m^{h-2}\cdot(\sigma^2)^{h-1}\cdot s^2\end{aligned}$$

In addition, the upper bound of $E[{Y_{1,1}^{(\mathbf{N})}}^4]$ can be computed

$$
\begin{aligned}
&E[{Y_{1,1}^{(\mathbf{N})}}^4] \\
&= E\left[\left(\sum_{j=1}^{w}\sum_{i=1+n(j-1)}^{nj}(\sum_{k=1}^{n} {J'}^{(\mathbf{N})}_{k+n(j-1)} \cdot S^{(\mathbf{N})}_{k,i-n(j-1)}) \cdot X^{(\mathbf{N})}_{i,1}) + \sum_{k=1}^{n} S^{(\mathbf{N})}_{1,k} \cdot X^{(\mathbf{N})}_{wn+k,1}\right)^4\right] \\
&\leq E\left[\{(w+1)n\}^3\left(\sum_{j=1}^{w}\sum_{i=1+n(j-1)}^{nj}(\sum_{k=1}^{n} {J'}^{(\mathbf{N})}_{k+n(j-1)} \cdot S^{(\mathbf{N})}_{k,i-n(j-1)})^4 \cdot {X^{(\mathbf{N})}_{i,1}}^4) + \sum_{k=1}^{n} {S^{(\mathbf{N})}_{1,k}}^4 \cdot {X^{(\mathbf{N})}_{wn+k,1}}^4\right)\right] \\
&\leq E\left[\{(w+1)n\}^3\left(\sum_{j=1}^{w}\sum_{i=1+n(j-1)}^{nj} n^3 \cdot (\sum_{k=1}^{n} {J'_{k+n(j-1)}}^{(\mathbf{N})^4} {S^{(\mathbf{N})}_{k,i-n(j-1)}}^4){X^{(\mathbf{N})}_{i,1}}^4) + \sum_{k=1}^{n} {S^{(\mathbf{N})}_{1,k}}^4 {X^{(\mathbf{N})}_{wn+k,1}}^4\right)\right] \\
&\leq \{(w+1)n\}^3\{wn \cdot n^4 \cdot (\frac{1}{2} \cdot 3\sigma^4) \cdot 3\{m(m+2)\}^{h-2} \cdot (\sigma^2)^{2(h-2)} \cdot (s^2)^2 \\
&+ n \cdot (\cdot 3\sigma^4) \cdot 3\{m(m+2)\}^{h-2} \cdot (\sigma^2)^{2(h-2)} \cdot (s^2)^2\} \\
&\leq 9 \cdot \{(w+1)n\}^4 \cdot n^4 \cdot \{m(m+2)\}^{h-2} \cdot (\sigma^2)^{2(h-1)} \cdot (s^2)^2
\end{aligned}
$$

The same results for $Y_{u,v}^{(\mathbf{N})}$ for all u, v can be shown in the same way. The variance of $(Z^{(\mathbf{N})})_1 = v'^{(\mathbf{N})} \cdot J^{(\mathbf{N})} \cdot \hat{S}_{1,\boldsymbol{x}(1)} \cdot E^{(\mathbf{N})}_{2,\boldsymbol{x}(2)} \prod_{k=3}^{h} D^{(\mathbf{N})}_{k,\boldsymbol{x}(k)} \cdot {w'^{(\mathbf{N})}}^T$ is computed as follows:

$$
\begin{aligned}
Var[(Z^{(\mathbf{N})})_1] &= nm \cdot \left(\frac{1}{2} \cdot wn + 1\right) \cdot n \cdot m^{h-2} \cdot (\sigma^2)^{h-1} \cdot s^2 \cdot \sigma^4 \\
&= nm \cdot \left(\frac{1}{2} \cdot wn + 1\right) \cdot n \cdot m^{h-2} \cdot (\sigma^2)^{h+1} \cdot s^2.
\end{aligned}
$$

Similarly, we have

$$
\begin{aligned}
E[(Z^{(\mathbf{N})})_1^4] &\leq (nm)^4 \cdot 9 \cdot \{(w+1)n\}^4 \cdot n^4 \cdot \{m(m+2)\}^{h-2} \cdot (\sigma^2)^{2(h-1)} \cdot (s^2)^2 \cdot (3\sigma^4)^2 \\
&= 81 \cdot (nm)^4 \cdot \{(w+1)n\}^4 \cdot n^4 \cdot \{m(m+2)\}^{h-2} \cdot (\sigma^2)^{2(h+1)} \cdot (s^2)^2
\end{aligned}
$$

Then, $\left|\dfrac{E[(Z^{(\mathbf{N})})_1^4]}{Var[(Z^{(\mathbf{N})})_1]^2}\right| \leq 324 \cdot (nm)^2 \cdot \{(w+1)n\}^2 \cdot n^2 \cdot \left(1 + \dfrac{1}{m}\right)^{h-2} = \mathsf{poly}(\lambda)$. □

Proof (of Lemma 5.5). Let $1 \leq j \leq h$ be an integer and $X_{u,v}$ the random variables of the (u,v)-th entry of the random matrix $E^{(\mathbf{M})}_{j+1,\boldsymbol{x}(j+1)} \prod_{k=j+2}^{h} D^{(\mathbf{M})}_{k,\boldsymbol{x}(k)}$. All random variables $X_{u,v}^{(\mathbf{M})}$ have the same variance $m^{h-j-1} \cdot (\sigma^2)^{h-j-1} \cdot s^2$, and $E[X_{u,v}^{(\mathbf{M})} \cdot X_{u',v}^{(\mathbf{M})}] = 0$ holds for distinct u, u' and $E[{X_{u,v}^{(\mathbf{M})}}^4] = 3\,(m(m+2))^{h-j-1} \cdot (\sigma^2)^{2(h-j-1)} \cdot (s^2)^2$.

We observe that

$$
\prod_{i=1}^{j} \hat{S}^{(\mathbf{M})}_{i,x_i} = \begin{pmatrix} \mathbf{0} \\ & \prod_{i=1}^{j} S^{(\mathbf{M})}_{i,x_i} \end{pmatrix}.
$$

Let $S_{u,v}^{(\mathbf{M})}$ be the random variable of (i,j)-th entry of the random matrix $\prod_{i=1}^{j} S^{(\mathbf{M})}_{i,x_i}$. Then, it hold that $Var[{S_{u,v}^{(\mathbf{M})}}^2] = n^{j-1} \cdot (\sigma^2)^j$, $E[S_{u,v}^{(\mathbf{M})} \cdot S_{u',v}^{(\mathbf{M})}] = 0$ for distinct u, u' and $E[{S_{u,v}^{(\mathbf{M})}}^4] = 3\{n(n+2)\}^{j-1} \cdot (\sigma^2)^{2j}$.

For a random variable of (u,v)-th entry of the random matrix $J^{(\mathbf{M})} \cdot \left(\prod_{i=1}^{j} \hat{S}^{(\mathbf{M})}_{i,\boldsymbol{x}(i)}\right) \cdot E^{(\mathbf{M})}_{j+1,\boldsymbol{x}(j+1)} \cdot \left(\prod_{k=j+2}^{h} D^{(\mathbf{M})}_{k,\boldsymbol{x}(k)}\right)$, we denote it by $Y_{u,v}^{(\mathbf{M})}$. Then a variance of $Y_{u,v}^{(\mathbf{M})}$ can be computed using

Lemma C.1.

$$\begin{aligned} Var[Y_{u,v}] &= E\left[\left(\sum_{k=1}^{n} S^{(\mathbf{M})}_{u,k}\cdot X^{(\mathbf{M})}_{wn+k,v}\right)^2\right] = E\left[\sum_{k=1}^{n} S^{(\mathbf{M})^2}_{u,k}\cdot X^{(\mathbf{M})^2}_{wn+k,v}\right] \\ &= n\cdot n^{j-1}\cdot(\sigma^2)^j\cdot m^{h-j-1}\cdot(\sigma^2)^{h-j-1}\cdot s^2 \\ &= n^j\cdot m^{h-j-1}\cdot(\sigma^2)^{h-1}\cdot s^2 \end{aligned}$$

Moreover, it holds that

$$\begin{aligned} E[Y^{(\mathbf{M})^4}_{u,v}] &= E\left[\left(\sum_{k=1}^{n} S^{(\mathbf{M})}_{u,k}\cdot X^{(\mathbf{M})}_{wn+k,v}\right)^4\right] \le E\left[n^3\cdot\left(\sum_{k=1}^{n} S^{(\mathbf{M})^4}_{u,k}\cdot X^{(\mathbf{M})^4}_{wn+k,v}\right)\right] \\ &= n^4\cdot 3\{n(n+2)\}^{j-1}\cdot(\sigma^2)^{2j}\cdot 3\,(m(m+2))^{h-j-1}\cdot(\sigma^2)^{2(h-j-1)}\cdot(s^2)^2 \\ &= 9\cdot n^4\cdot\{n(n+2)\}^{j-1}\cdot(m(m+2))^{h-j-1}\cdot(\sigma^2)^{2(h-1)}\cdot(s^2)^2 \end{aligned}$$

By Lemma C.3, we can compute $v'^{(\mathbf{M})}\cdot J^{(\mathbf{M})}\cdot\prod_{i=1}^{j}\hat{S}^{(\mathbf{M})}_{i,\boldsymbol{x}(i)}\cdot E^{(\mathbf{M})}_{j+1,\boldsymbol{x}(j+1)}\prod_{k=j+2}^{h}D^{(\mathbf{M})}_{k,\boldsymbol{x}(k)}\cdot w'^{(\mathbf{M})^T}$ which is denoted by $(Z^{(\mathbf{M})})_j$. Then it hold that

$$\begin{aligned} Var[(Z^{(\mathbf{M})})_j] &= nm\cdot n^j\cdot m^{h-j-1}\cdot(\sigma^2)^{h-1}\cdot s^2\cdot\sigma^4 = nm\cdot n^j\cdot m^{h-j-1}\cdot(\sigma^2)^{h+1}\cdot s^2 \\ E[(Z^{(\mathbf{M})})_j^4] &\le (nm)^4\cdot 9\cdot n^4\cdot\{n(n+2)\}^{j-1}\cdot\{m(m+2\})^{h-j-1}\cdot(\sigma^2)^{2(h-1)}\cdot(s^2)^2\cdot(3\sigma^4)^2 \\ &= 81\cdot(nm)^4\cdot n^4\cdot\{n(n+2)\}^{j-1}\cdot\{m(m+2)\}^{h-j-1}\cdot(\sigma^2)^{2(h+1)}\cdot(s^2)^2. \end{aligned}$$

Overall, $\left|\dfrac{E[(Z^{(\mathbf{M})})_j^4]}{Var[(Z^{(\mathbf{M})})_j]^2}\right| \le 81\cdot(nm)^2\cdot n^2\cdot\left(1+\dfrac{2}{n}\right)^{j-1}\cdot\left(1+\dfrac{2}{m}\right)^{h-j-1} = \mathsf{poly}(\lambda)$. All arguments hold as well for $\mathbf{N}$. □

Proof (of Lemma 5.6). Let $X^{(\mathbf{M})}_{u,v}$ be the random variables of the (u,v)-th entry of the random matrix $\prod_{i=1}^{h-1}B^{(\mathbf{M})}_{i,\boldsymbol{x}(i)}$. All random variables of entries of $B^{(\mathbf{M})}_{i,\boldsymbol{x}(i)}$ are mutually independent and follow a uniform distribution $[-\frac{\nu}{2},\frac{\nu}{2})$. For convenience, we assume random variables follow a uniform distribution $[-\frac{\nu}{2},\frac{\nu}{2}]$.[12]

We note that the similar computations as in Lemma C.2 hold as well for the uniform distributions. More precisely, for the random variable U_1, U_2 following the uniform distribution over $[-\frac{\nu}{2},\frac{\nu}{2}]$, it hold that $E[U_1]=0$, $E[U_1^2]=\dfrac{1}{12}\cdot\nu(\nu+2)$, $E[U_1^4]=\dfrac{1}{80}\cdot v(v+2)\{v(v+2)-\frac{4}{3}\}$.

Thus, the variance of $X^{(\mathbf{M})}_{u,v}$ is

$$Var[X^{(\mathbf{M})}_{u,v}] = g^{h-2}\cdot\left\{\frac{1}{12}\cdot v(v+2)\right\}^{h-1}.$$

We also have

$$E[X^{(\mathbf{M})^4}_{u,v}] \le 3\cdot\{g(g+2)\}^{h-2}\cdot\left\{\frac{1}{12}\cdot v(v+2)\right\}^{2(h-1)}.$$

By Lemma C.3, we can compute the variance and expectation of quadruple of $b^{(\mathbf{M})}_v\cdot\prod_{i=1}^{h-1}B^{(\mathbf{M})}_{i,\boldsymbol{x}(i)}\cdot b^{(\mathbf{M})^T}_w$ which is denoted by $(Z^{(\mathbf{M})})_h$.

$$\begin{aligned} Var[(Z^{(\mathbf{M})})_h] &= g^2\cdot g^{h-2}\cdot\left\{\frac{1}{12}\cdot v(v+2)\right\}^{h-1}\cdot\left\{\frac{1}{12}\cdot v(v+2)\right\}^2 \\ &= g^h\cdot\left\{\frac{1}{12}\cdot v(v+2)\right\}^{h+1}, \end{aligned}$$

[12] Our analysis can be applied without this assumption but the calculations are very tedious.

$$
\begin{aligned}
E[(Z^{(\mathbf{M})})_h^4] &\leq (g^2)^4 \cdot 3 \cdot \{g(g+2)\}^{h-2} \cdot \left\{\frac{1}{12} \cdot v(v+2)\right\}^{2(h-1)} \cdot \left[3\left\{\frac{1}{12} \cdot v(v+2)\right\}^2\right]^2 \\
&= 27 \cdot (g^2)^4 \cdot \{g(g+2)\}^{h-2} \cdot \left\{\frac{1}{12} \cdot v(v+2)\right\}^{2(h+1)}.
\end{aligned}
$$

As a result, $\left|\dfrac{E[(Z^{(\mathbf{M})})_h^4]}{Var[(Z^{(\mathbf{M})})_h]^2}\right| \leq 27 \cdot (g^2)^2 \cdot \left(1 + \dfrac{2}{g}\right)^{h-2} = \mathsf{poly}(\lambda)$. The same arguments hold as well for $\mathbf{N}$. □