On the Statistical Leak of the GGH13 Multilinear Map and Some Variants

Léo Ducas[1] and Alice Pellet-Mary[2(✉)]

[1] Cryptology Group, CWI, Amsterdam, The Netherlands
leo.ducas@cwi.nl
[2] Univ Lyon, CNRS, ENS de Lyon, Inria, UCBL, LIP, Lyon, France
alice.pellet___mary@ens-lyon.fr

Abstract. At EUROCRYPT 2013, Garg, Gentry and Halevi proposed a candidate construction (later referred as GGH13) of cryptographic multilinear map (MMap). Despite weaknesses uncovered by Hu and Jia (EUROCRYPT 2016), this candidate is still used for designing obfuscators.

The naive version of the GGH13 scheme was deemed susceptible to averaging attacks, i.e., it could suffer from a statistical leak (yet no precise attack was described). A variant was therefore devised, but it remains heuristic. Recently, to obtain MMaps with low noise and modulus, two variants of this countermeasure were developed by Döttling et al. (EPRINT:2016/599).

In this work, we propose a systematic study of this statistical leakage for all these GGH13 variants. In particular, we confirm the weakness of the naive version of GGH13. We also show that, among the two variants proposed by Döttling et al., the so-called conservative method is not so effective: it leaks the same value as the unprotected method. Luckily, the leakage is more noisy than in the unprotected method, making the straightforward attack unsuccessful. Additionally, we note that all the other methods also leak values correlated with secrets.

As a conclusion, we propose yet another countermeasure, for which this leakage is made unrelated to all secrets. On our way, we also make explicit and tighten the hidden exponents in the size of the parameters, as an effort to assess and improve the efficiency of MMaps.

Keywords: Cryptanalysis · Multilinear maps · Statistical leakages
Ideal lattices

1 Introduction

Since their introduction in cryptographic constructions by Joux in 2000 [25], cryptographic bilinear maps, as provided by pairings on elliptic curves, have enabled the construction of more and more advanced cryptographic protocols, starting with the Identity-Based Encryption scheme of Boneh and Franklin [8]. More abstractly, a group equipped with an efficient bilinear map, and on which

T. Peyrin and S. Galbraith (Eds.): ASIACRYPT 2018, LNCS 11272, pp. 465–493, 2018.
https://doi.org/10.1007/978-3-030-03326-2_16

some discrete-logarithm like problems are hard (such as the bilinear Diffie-Hellmann problem), provides foundation for a whole branch of cryptography. A natural open question is whether it can be generalized to degrees higher than 2 while ensuring hardness of generalizations of the Diffie-Hellmann problem. Such hypothetical objects are referred to as *Cryptographic Multilinear Maps* (or, for short, MMaps).

In 2013, Garg, Gentry and Halevi [17] proposed a candidate construction for MMaps related to ideal-lattices, yet without a clearly identified underlying hard lattice problem. It differs from the pairing case in the sense that elements in the low-level groups have no canonical representation, and that the representation is noisy. Yet, these differences are not too problematic on the functionality front.

On the security front, it rapidly turned out that this construction was insecure, at least in its original set-up. In particular, the natural one-round k-partite protocol based on this MMap was broken by the zeroizing attack of Hu and Jia [24]: this construction fails to securely mimic the tripartite protocol of [25]. More generally, the mere knowledge of a non-trivial representative of 0 tends to make constructions based on this MMap insecure. Orthogonally, it has been discovered that solving over-stretched versions of the NTRU problem (whose intractability is necessary for the security of the GGH MMap) was significantly easier than previously thought, due to the presence of an unusually dense sublattice [1,12,26], yet this can be compensated at the cost of increasing parameters. Also, due to recent algorithms for the Principal Ideal Problem [6,7] and Short generator recovery [10,14], the GGH MMap can be broken[1] in quantum polynomial time, and classical subexponential time $\exp(\tilde{O}(\sqrt{n}))$, where n is the dimension of the used ring.

Nevertheless, this candidate MMap was still considered in a weaker form,[2] to attempt realizing indistinguishability obfuscation (or, for short, iO). Several iO candidates were broken by attacks that managed to build low-level encodings of zero even if no such encodings were directly given (this is referred to as zeroizing attacks, see e.g. [11,13]). To try to capture and prevent such attacks, a Weak MMap model was devised in [18,34].

Some iO constructions come with a security proof based on assumptions in the standard model [2,29,30], but cannot be securely instantiated with the GGH13 MMap as they require low-level encodings of 0. Others are proved secure in a non-standard model (the Generic MMap model [4,9] or the Weak MMap Model [15,18]). These models remain not fully satisfactory, as they imply Virtual-Black-Box Obfuscation [9,18], a provably impossible primitive [5]. The latest candidate of Lin and Tessaro [31] did escape these pitfalls by relying on pairings, but it required special Pseudo-Random Generators that were rapidly proved not to exist [3,32].

[1] The secret value h can be recovered exactly, allowing in particular to construct zero-tester at larger levels.

[2] Without providing any low-level encoding of 0, and keeping the order of the multilinear group secret.

Statistical leaks in lattice-based cryptography. Early signature schemes based on lattices [21–23] suffered from statistical leaks, which led to devastating attacks [20,35]. Those leaks can be fixed in a provably secure way using a *Gaussian Sampling* algorithm from Klein [27], as proven in [19]: the samples available to the adversary are made statistically independent from the secret key.

Similar leaks are a worry in the original construction of [17], and therefore, a candidate countermeasure was developed, making use of Klein's sampling procedure. Nevertheless, no formal statement was made on what this countermeasure prevents: the countermeasure is heuristic. This particular countermeasure turned out to be a difficulty when considering variants of the original scheme, as done in [15]. This candidate obfuscator aims at reaching polynomially small errors and modulus (in order to improve both efficiency and security of the GGH map, especially in the light of the dense sublattice attacks [1,12,26]) and hence cannot use the original sampling methods from [17]. Two modified versions of [17] are then proposed in [15], a so-called conservative one, leading to quite efficient parameters, and a so-called aggressive one.

Ideally, one wishes to make provable statements about those four variants, as done in other contexts [19]. Unfortunately, in the context of MMaps, it is not even clear what the statement should exactly be. The next best guarantee is a precise understanding of what can be done from a cryptanalytic point of view, as initiated in [17].

The analysis of the leak of [17] focuses on the covariance of products of encodings of zero. One can (informally) argue that this analysis captures all the information of the leakage. Indeed, up to discretization, such a product is the product of several centered Gaussian distributions (non necessary spherical), and such a distribution is fully identified by its covariance. The countermeasure proposed in Sect. 6.4 of [17] attempts to make this covariance proportional to the identity matrix (and therefore unrelated to all secrets) by sampling each element of the product according to a spherical distribution, that is a distribution whose covariance is proportional to the identity matrix. As we shall see, this attempt is unsuccessful, as one of the factors of the product (namely, the one related to the zero-testing parameter) is fixed. Obtaining several independent multiples of it, with covariance proportional to the identity matrix, then reveals an approximation of this factor.

Contributions. Our main contribution is to give a systematic study of the statistical leakage in the GGH13 scheme and its variants, in a simple framework we define. We first suggest a common formalism that encompasses all the variants at hand, by parametrising the sampling procedure for encodings by an arbitrary covariance matrix. Following the nomenclature of [15,17], except for the second one that had no clear name, we consider:

1. The simplistic method: the GGH MMap without countermeasure [17, Sect. 4.1]. This method was only given for simplicity of exposition and was already highly suspected to be insecure;

2. The exponential method:[3] the GGH MMap with countermeasure [17, Sect. 6.4];
3. The conservative method, proposed in [15]—which we partly revisit to tackle some of its limitations;
4. The aggressive method, proposed in [15]—we note that this method is specific to the iO construction of [15], and is not applicable to all constructions over the GGH MMap.

In order to formalize our study of the leakage, we propose a simple setting of the GGH multilinear map. Indeed, due to the attacks in presence of encodings of zero, the exact set-up for the analysis of the leakage in [17] is not relevant anymore. We adjust their setting to not provide low-level encodings of zero directly. Still, some relations between encodings are needed for the MMaps to be non-trivial; to ensure that those relations do not allow zeroizing attacks, we provide a security proof in the weak multilinear map model of [15,18,34]. For ease of exposure, we restrict ourselves to degree $\kappa = 2$, yet our analysis easily extends to higher degrees.

Using this framework, we are able to analyse a particular averaging attack against the GGH multilinear map. On the one hand, our analysis shows that Method 3 leads to the same leakage as Method 1. We also prove that with Method 1, a polynomial-time attack can be mounted using the leakage. Interestingly, it does not require the Gentry-Szydlo algorithm [20], unlike the approach discussed in [17, Sects. 6.3.2 and 7.6]. Nevertheless, we did not manage to extend the attack to Method 3: while the same quantity is statistically leaked, the number of samples remains too low for the attack to go through completely. On the other hand, we show that the statistical leakage of Method 4 is similar to the one of Method 2: perhaps surprisingly the aggressive method seems more secure than the conservative one.

Finally, having built a better understanding of which information is leaked, we devise a countermeasure that we deem more adequate than all the above:

5. The compensation method.

This method is arguably simpler, and provides better parameters. More importantly, applying the same leakage attack than above, one only obtains a distribution whose covariance is independent of all secrets. We wish to clarify that this is in no way a formal statement of security. The statistical attacks considered in this work are set up in a minimalistic setting, and extensions could exist beyond this minimalistic setting. For example, one could explore what can be done by varying the zero-tested polynomial, or by keeping certain encodings fixed between several successful zero-tests.

As a secondary contribution, we also make explicit and tighten many hidden constants present in the previous constructions, in an effort to evaluate and improve the efficiency of GGH13-like MMaps.

[3] The naming reflects the fact that this method leads to a modulus q which is exponential in the number ℓ of so-called *atoms*.

Impact. This result may be useful in pursuit of an underlying hard problem on which one could based the GGH multilinear map. Indeed, we show here that it is possible to recover some information about secret elements, for all the previously proposed sampling methods. Hence, an underlying hard problem (or the security reduction) should capture this leak. This enables us to get a bit more insight into what could be (or could not be) an underlying hard problem for the GGH map. In that regard, finding such a hard underlying problem could be easier with our new method, since one specific leak has been sealed. Again, we *do not* claim that no other leaks exist.

Further, our analysis shows that the weak multilinear map model does not capture averaging attacks. This is not surprising, as the weak multilinear map model only allows to evaluate polynomials in the post-zero-test values, while we need to average on them for this attack. But proving that averaging cannot be achieved by evaluating polynomials is not so immediate. Interestingly, our results prove it. Indeed, using averaging techniques, we were able to mount a polynomial time attack against our setting when using the simplistic sampling method (Method 1), but we also proved that in the weak multilinear map model, no polynomial time attacks could be mounted. This proves that the weak multilinear map model does not capture averaging attacks.[4]

Finally, our new method severely decreases the length of encodings in the GGH13 multilinear map, which substentially contribute to their practical feasibility.

Outline of the article. In Sect. 2, we recall some mathematical background about cyclotomic number fields and statistics. We also describe the GGH multilinear map and detail the size of its parameters. In Sect. 3, we describe different sampling methods for the GGH multilinear map, which come from [15,17], using a common formalism so as to factor the later analysis. We describe our simple setting and analyse the leakage in Sect. 4. The security proof of this simple setting in the weak multilinear map model can be found in the full version of this article [16]. Finally, we discuss the design of sampling methods in Sect. 5, and propose a design we deem more rational.

2 Preliminaries

2.1 Mathematical Background

Rings. We denote by R the ring of integers $\mathbb{Z}[X]/(X^n+1)$ for some n which is a power of 2 and $K = \mathbb{Q}[X]/(X^n+1)$ its fraction field. We denote by $\sigma_j : K \to \mathbb{C}$, with $1 \leq j \leq n$, the complex embeddings of K in $\mathbb{C}$. We also denote $K_{\mathbb{R}} = \mathbb{R}[X]/(X^n+1)$ the topological closure of K. For $x \in K_{\mathbb{R}}$, we denote $x_i \in \mathbb{R}$ its i-th coefficient, so that $x = \sum_{i=0}^{n-1} x_i X^i$. For $g \in K$ (or even $K_{\mathbb{R}}$) we denote gR the ideal generated by g: $gR = \{gx | x \in R\}$. The complex conjugation over R

[4] The precise component of the attack which is not captured by the weak multilinear map model is the rounding operation performed at the end.

and K is denoted $\bar{\cdot}$. It is the automorphism of R sending X to X^{-1}. We denote S the subring of $K_{\mathbb{R}}$ of symmetric elements, that is $S = \{x \in K_{\mathbb{R}} | x = \bar{x}\}$. We set S^+ the subset of symmetric positive elements of S, defined by $S^+ = \{x\bar{x} | x \in K_{\mathbb{R}}\}$. Alternatively, S is the completion of the real subfield of K, and S^+ is (the completion of) the set of elements of K whose embeddings are all non-negative real numbers. Note that S^+ is closed under addition, multiplication, division, but not under subtraction. The elements of S^+ also admit one and exactly one square root (resp. k-th root) in S^+, which we denote $\sqrt{\cdot}$ (resp. $\sqrt[k]{\cdot}$) . Finally, we call $x\bar{x} \in S^+$ the autocorrelation[5] of $x \in K_{\mathbb{R}}$, and denote it $A(x)$. For $\Sigma \in S^+$ it holds that $A(\sqrt{\Sigma}) = \Sigma$. We also define equivalence over S^+ up to scaling by reals, and write $x \sim y$ for invertible elements $x, y \in S^+$ if $x = \alpha y$ for some positive real $\alpha > 0$. Let q be a prime congruent to 1 modulo $2n$. We denote by R_q the quotient ring $R/(qR)$. For $x \in R$, we denote by $[x]_q$ (or $[x]$ when there is no ambiguity) the coset of the element x in R_q. We will often lift back elements from R_q to R, in which case we may implicitly mean that we choose the representative with coefficients in the range $[-q/2, q/2]$. To avoid confusion, we will always write x^{-1} for the inversion in R_q, and keep the fraction symbols $1/x$ and $\frac{1}{x}$ for inversion in K and $K_{\mathbb{R}}$.

Geometry. Because we work in the ring $\mathbb{Z}[X]/(X^n + 1)$, the canonical geometry of the coefficients embeddings is equivalent, up to scaling, to the geometry of the Minkowski embeddings. We stick with the former, following the literature on multilinear maps. More precisely, the inner product of two elements $x, y \in K$ is defined by $\langle x, y \rangle = \sum x_i y_i$. The Euclidean norm (or ℓ_2-norm) is defined by $\|x\| = \sqrt{\langle x, x \rangle}$. The ℓ_∞-norm is noted $\|x\|_\infty = \max |x_i|$.

We recall the following inequalities:

$$\|xy\| \leq \sqrt{n} \cdot \|x\| \cdot \|y\| \tag{1}$$

$$\|x\|_\infty \leq \|x\| \leq \sqrt{n} \cdot \|x\|_\infty \tag{2}$$

$$\|x\|^2 \leq \|x\bar{x}\|_\infty \tag{3}$$

$$\|\bar{x}\| = \|x\| \text{ and } \|\bar{x}\|_\infty = \|x\|_\infty. \tag{4}$$

Statistics. We denote by $\Pr[E]$ the probability of an event E. For a random variable x over $K_{\mathbb{R}}$, we denote by $\mathbb{E}[x]$ the expectation of x, and by $\mathbb{V}[x] = \mathbb{E}[x\bar{x}] - \mathbb{E}[x]\mathbb{E}[\bar{x}]$ its variance. It should be noted that $\mathbb{V}[x] \in S^+$ for any random variable x over $K_{\mathbb{R}}$. A random variable x is said centered if $\mathbb{E}[x] = 0$, and isotropic if $\mathbb{V}[x] \sim 1$. We recall Hoeffding's inequality.

Theorem 1 (Hoeffding's inequality). *Let $Y_1, \cdots, Y_m$ be independent random variables in $\mathbb{R}$ with the same mean $\mu \in \mathbb{R}$ and such that $|Y_i| \leq B$ for all i's.*

[5] In an algebraic context, this would be more naturally described as the norm of x relative to the maximal real subfield of K, yet for our purposes it is more adequate to use the vocabulary of statistics.

Then for all $t > 0$,

$$Pr\left[\left|\frac{1}{m}\sum_{i=1}^{m} Y_i - \mu\right| \geq t\right] < 2e^{-\frac{mt^2}{2B^2}}.$$

Hoeffding's inequality, as given above, applies to random variables in $\mathbb{R}$. In this article, we will be interested in random variables in R. We will then see our elements in R as vectors in $\mathbb{R}^n$ and apply Hoeffding's inequality coefficient-wise.

Corollary 1 (Hoeffding's inequality in R). *Let $Y_1, \cdots, Y_m$ be independent random variables in R with the same mean $\mu \in K_{\mathbb{R}}$ and such that $\|Y_i\|_\infty \leq B$ for all i's. Let $\varepsilon > 0$, then*

$$Pr\left[\left\|\frac{1}{m}\sum_{i=1}^{m} Y_i - \mu\right\|_\infty \geq B\sqrt{\frac{2(\ln n - \ln \varepsilon)}{m}}\right] < 2\varepsilon.$$

Proof. For $1 \leq i \leq m$ and $0 \leq j \leq n-1$, define $Y_{i,j}$ to be the j-th coefficient of the variable $Y_i \in R$ and μ_j to be the j-th coefficient of μ. For a fixed j, the variables $Y_{i,j}$ (where only i varies) are independent random variables in $\mathbb{R}$ of mean μ_j. Moreover, as $\|Y_i\|_\infty \leq B$ for all i's, the coefficients $Y_{i,j}$ are also bounded by B. We can then apply Hoeffding's inequality (Theorem 1) to them. We obtain

$$\begin{aligned}
&\Pr\left[\left\|\frac{1}{m}\sum_{i=1}^{m} Y_i - \mu\right\|_\infty \geq B\sqrt{\frac{2(\ln n - \ln \varepsilon)}{m}}\right] \\
&= \Pr\left[\exists j : \left|\frac{1}{m}\sum_{i=1}^{m} Y_{i,j} - \mu_j\right| \geq B\sqrt{\frac{2(\ln n - \ln \varepsilon)}{m}}\right] \\
&\leq \sum_{j=0}^{n-1} \Pr\left[\left|\frac{1}{m}\sum_{i=1}^{m} Y_{i,j} - \mu_j\right| \geq B\sqrt{\frac{2(\ln n - \ln \varepsilon)}{m}}\right] \\
&< \sum_{j=0}^{n-1} 2e^{-\frac{2mB^2(\ln n - \ln \varepsilon)}{2B^2 m}} = \sum_{j=0}^{n-1} 2\frac{\varepsilon}{n} = 2\varepsilon.
\end{aligned}$$

We used the union bound and Hoeffding's inequality with $t = B\sqrt{\frac{2(\ln n - \ln \varepsilon)}{m}}$. □

Discrete Gaussians. For $\Sigma \in S^+$ and $x_0 \in K_{\mathbb{R}}$, we define the *Gaussian weight function* on $K_{\mathbb{R}}$ as

$$\rho_{\sqrt{\Sigma},x_0} : x \mapsto \exp\left(-\frac{1}{2}\left\|\frac{x - x_0}{\sqrt{\Sigma}}\right\|^2\right).$$

For any shifted ideal $I+c$, $I \subset K$, $c \in K_{\mathbb{R}}$, we define the *discrete Gaussian distribution* over $I+c$ of parameter $\sqrt{\Sigma}$, centered in x_0 by:

$$\forall x \in I+c,\ D_{I+c,\sqrt{\Sigma},x_0}(x) = \frac{\rho_{\sqrt{\Sigma},x_0}(x)}{\rho_{\sqrt{\Sigma},x_0}(I+c)}.$$

For concision, we write $D_{I+c,\sqrt{\Sigma}}$ instead of $D_{I+c,\sqrt{\Sigma},0}$ and $\rho_{\sqrt{\Sigma}}$ instead of $\rho_{\sqrt{\Sigma},0}$.

Theorem 2 (Reformulation of [19, Theorem 4.1.]**).** *There exists a PPT algorithm that given $g \in R$, $c \in K_{\mathbb{R}}$ and a parameter Σ such that $\|g/\sqrt{\Sigma}\| \leq o(1/\sqrt{\log n})$, outputs x from a distribution negligibly close to $D_{gR+c,\sqrt{\Sigma}}$.*

This reformulation simply relies on the identity $D_{gR+c,\sqrt{\Sigma}} = \frac{\sqrt{\Sigma}}{\sigma} \cdot D_{(gR+c)/\sqrt{\Sigma},\sigma}$. We also recall that, above the smoothing parameter [33], a discrete Gaussian resembles the continuous Gaussian, in particular it is almost centered at 0, and of variance almost Σ.

Lemma 1. *For any $g \in K$, $\Sigma \in S^+$, $c \in K_{\mathbb{R}}$ such that $\|g/\sqrt{\Sigma}\| \leq o(1/\sqrt{\log n})$, if $x \leftarrow D_{gR+c,\sqrt{\Sigma}}$, then $\|\mathbb{E}[x]\| \leq \varepsilon \cdot \|\sqrt{\Sigma}\|$ and $\|\mathbb{V}[x] - \Sigma\| \leq \varepsilon \cdot \|\Sigma\|$ for some negligible function $\varepsilon(n)$.*

The proof of this result, using [33, Lemma 4.2], can be found in the full version [16].

2.2 The GGH13 Multilinear Map

We describe in this section the GGH13 multilinear map [17], in its asymmetric setting. The GGH13 multilinear map encodes elements of a ring of integers R, modulo a secret small element $g \in R$. More concretely, an authority generates the following parameters:

- an integer n which is a power of 2 (serving as the security parameter).
- a (small) element g in R. We denote by $I = gR$ the ideal generated by g in R.
- a (large) positive integer q such that $q \equiv 1 \mod 2n$. Originally, q was chosen exponentially large in n [17], but variants were proposed for polynomially sized q [15,28].
- ℓ invertible elements $[z_i] \in R_q^{\times}$, for $1 \leq i \leq \ell$, chosen uniformly at random in $R_q^{\times}$.
- a zero-testing parameter $[p_{zt}] = [hz^* g^{-1}]$ where $[z^*] = [\prod_{1\leq i\leq \ell} z_i]$ and h is a random element in R, generated according to a Gaussian distribution of standard deviation approximately $\sqrt{q}$.

We detail in Sect. 2.2 the size of the parameters described above (we will choose them to ensure the correctness of the scheme). The elements n, q and p_{zt} are public while the parameters h, g and the z_i's are kept secret.

Encoding of an element. The GGH13 multilinear map allows to encode cosets of the form $a + I$ for some element a in R. Let $\boldsymbol{v} \in \{0,1\}^\ell$ be a vector of size ℓ. An encoding of the coset $a + I$ at level $\boldsymbol{v}$ is an element of R_q of the form

$$u = \left[(a + rg) \cdot z_{\boldsymbol{v}}^{-1}\right]$$

where $[z_{\boldsymbol{v}}] = [\prod_{i, \boldsymbol{v}[i]=1} z_i]$ and $a + rg$ is a small element in the coset $a + I$. We call $\boldsymbol{v}$ the level of the encoding.[6] We abuse notation by saying that u is an encoding of a (instead of an encoding of the coset $a + I$).

An encoding generated by the authority is called a fresh encoding, by opposition to encodings that are obtained by adding or multiplying other encodings. The precise distribution of $a + rg$ for a fresh encoding will be a discrete Gaussian distribution over the coset $a + I$, but not necessarily a spherical one: $a + rg \leftarrow D_{a+I, \sqrt{\Sigma_{\boldsymbol{v}}}}$. The shape $\Sigma_{\boldsymbol{v}}$ of this Gaussian is essentially what distinguishes the variants that we will discuss in Sect. 3.

Adding and multiplying encodings. If u_1 and u_2 are two encodings of elements a_1 and a_2 at the same level $\boldsymbol{v}$ then $u_1 + u_2$ is an encoding of $a_1 + a_2$ at level $\boldsymbol{v}$.

If u_1 and u_2 are two encodings of elements a_1 and a_2 at levels $\boldsymbol{v}$ and $\boldsymbol{w}$ with $\boldsymbol{v}[i] \cdot \boldsymbol{w}[i] = 0$ for all $1 \leq i \leq \ell$, then $u_1 \cdot u_2$ is an encoding of $a_1 \cdot a_2$ at level $\boldsymbol{v} + \boldsymbol{w}$ (where the addition is the usual addition on vectors of size ℓ).

Zero-testing. We denote by $\boldsymbol{v}^* = (1, \ldots, 1)$ the maximum level of an encoding. The zero testing parameter allows us to test if an encoding u at level $\boldsymbol{v}^*$ is an encoding of zero, by computing

$$[w] = [u \cdot p_{zt}].$$

If w is small compared to q (the literature usually requires its coefficients to be less than $q^{3/4}$), then u is an encoding of zero. Otherwise, it is not.

Size of the parameters and correctness. We define Q such that $q = n^Q$ and L such that $\ell = n^L$ (the elements Q and L are not necessarily integers). The bounds below on the size of g and h come from [17]. The secret generator g is sampled so that:

$$\|g\| = O(n), \quad \|1/g\| = O(n^2). \tag{5}$$

Remark. There seems to be some inconsistencies in [17] about the size of g, which is on page 10 sampled with width $\sigma = \tilde{O}(\sqrt{n})$, while on page 13 the width σ is set to $\sqrt{n\lambda}$ to ensure the smoothing condition $\sigma \geq \eta_{2^{-\lambda}}(\mathbb{Z}^n)$ (where $\lambda = O(n)$ denote the security parameter). Yet, according to [33, Lemma 3.3], it holds that $\eta_{2^{-\lambda}}(\mathbb{Z}^n) \leq O(\sqrt{\lambda} + \log n)$, so $\sigma = O(\sqrt{n})$ is sufficient, and we do have $\|g\| \leq O(n)$ with overwhelming probability by [33, Lemma 4.4].

[6] Remark that we could define encodings of level $\boldsymbol{v}$ even if $\boldsymbol{v}$ is not binary (but still has non negative integer coefficients). This is not necessary for a honest use of the GGH13 map, but we will use it in Sect. 4 for our attack.

The numerator $c = a + rg$ of a fresh encoding of $a + I$ at level $\boldsymbol{v}$ is sampled such that

$$\|c\| = \Theta(n^{\gamma+\eta\cdot\|\boldsymbol{v}\|_1+\nu L}), \tag{6}$$

where γ, η and ν are positive reals, and depend on the sampling method, such as the ones proposed in [15] (depending on the method, η and ν may be zero). We describe later the different sampling methods and the values of γ, η and ν associated to each method. When we do not need to focus on the dependence on $\|\boldsymbol{v}\|_1$ and L, we just call $E := \Theta(n^{\gamma+\eta\cdot\|\boldsymbol{v}\|_1+\nu L})$ the bound above. For each sampling method described below, we choose this bound to be as small as possible under the specific constraints that will arise with the sampling method.

The mildly large element h is sampled so that

$$\|h\| = \Theta(\sqrt{nq}). \tag{7}$$

Remark. In the second variant proposed in [17, Sect. 6.4] to try to prevent averaging attacks, the authors generate h according to a non spherical Gaussian distribution. However, as h is sampled only once, its distribution does not matter for the attack we analyze in this article. This is why we only specify here the size of h, and not its distribution.

We now give a condition on the modulus q to ensure correctness of the GGH13 multilinear map. This condition will depend on the number κ of fresh encodings that we have to multiply in order to obtain a top level encoding. A natural upper bound for κ is ℓ, the number of levels of the multilinear map. However, in the following, we will be interested in cases where we are provided with fresh encodings at a somewhat high level and we only need to multiply a small number of them (much smaller than ℓ) to obtain a top level encoding. Choosing a small degree κ is motivated by the fact that we want to obtain a small modulus q. We will see below that q should be at least exponential in κ. Hence, in order to achieve a polynomial modulus q, it should be that κ is at most logarithmic in the security parameter (while ℓ can be much larger). In the simple setting we describe in Sect. 4.1, we choose $\kappa = 2$, which enables q to be polynomial (if we use the good sampling methods).

Correctness of zero-testing a homogeneous polynomial of degree κ, whose absolute sum of the coefficients is bounded by n^B and evaluated in fresh encodings, is guaranteed if $n^B \cdot \|\frac{h}{g}\prod_{i=1}^{\kappa} c_i\| \leq q^{3/4}$. It is then sufficient to have

$$B + \frac{\kappa+1}{2} + \frac{Q+1}{2} + 2 + \kappa(\gamma + \nu L) + \eta\ell \leq \frac{3}{4}Q. \tag{8}$$

The term $\frac{\kappa+1}{2}$ appears from applying inequality (1) $\kappa+1$ times. One should also note that $\sum_{i=1}^{\kappa}\|\boldsymbol{v}_i\|_1 = \|\boldsymbol{v}^*\|_1 = \ell$, because we can only zero test at level $\boldsymbol{v}^*$ (where $\boldsymbol{v}_i$ is the level of encoding c_i). More compactly, correctness holds if:

$$B + 3 + \kappa(1/2 + \gamma + \nu L) + \eta\ell \leq Q/4. \tag{9}$$

In our simple setting of the GGH multilinear map defined in Sect. 4.1, we will only query the zero-testing procedure on encodings of this form, with $\kappa = 2$

and $B = \log(m)/\log(n)$, for some constant m we will define later. Hence, taking $4 + 2\gamma + 2\nu L + \eta\ell + \log(m)/\log(n) \leq Q/4$ will be sufficient in our setting to ensure correctness of the zero-testing procedure.

Remark. We note that the bound $q^{3/4}$ for positive zero-tests is somewhat arbitrary and could very well be replaced by $q/4$, allowing to square-root the parameter q. Indeed, the probability of a false positive during zero-testing would remain as small as 2^{-n}. This would have a serious impact on concrete efficiency and security.

3 Sampling Methods

We describe in this section different sampling methods that can be used to generate the fresh encodings of the GGH multilinear map and we give the values of γ, η and ν that correspond to these methods. As said above, we will be interested in cases where (at least some of) the fresh encodings have a somewhat high degree and we just have to multiply a constant number of them (say 2) to obtain an encoding at maximal level $\boldsymbol{v}^*$. We denote by $\mathcal{A}$ the set of "atoms", that is the set of levels $\boldsymbol{v} \in \{0,1\}^\ell$ at which we want to encode fresh encodings. In our simple setting of the GGH multilinear map (see Sect. 4.1 for a full description of our setting), we will chose $\mathcal{A}$ to be the set of levels $\boldsymbol{v} \in \{0,1\}^\ell$ that have weight exactly 1 or $\ell - 1$, where the weight of $\boldsymbol{v}$ is the number of its non-zero coefficients. For all $\boldsymbol{v} \in \mathcal{A}$, we denote by $\tilde{\boldsymbol{v}} = \boldsymbol{v^*} - \boldsymbol{v}$ the complement of $\boldsymbol{v}$. We note that $\mathcal{A}$ is closed by complement.

In all the following sampling methods except the first one, one chooses a representative $z_{\boldsymbol{v}} \in R$ of $[z_{\boldsymbol{v}}] \in R_q$ for all $\boldsymbol{v} \in \mathcal{A}$. This representative will not necessarily be the canonical one, with coefficients in $[-q/2, q/2]$. Then, we will take $\Sigma_{\boldsymbol{v}} = \sigma_{\boldsymbol{v}}^2 z_{\boldsymbol{v}} \bar{z_{\boldsymbol{v}}}$, with $\sigma_{\boldsymbol{v}} = \Theta(n^2 \|1/z_{\boldsymbol{v}}\|)$. Using Inequalities (3) and (4), we can see that $\|1/\sqrt{\Sigma_{\boldsymbol{v}}}\| \leq 1/\sigma_{\boldsymbol{v}} \cdot n^{1/4} \cdot \|1/z_{\boldsymbol{v}}\|$. Hence, with our choice of $\sigma_{\boldsymbol{v}}$ and the fact that $\|g\| = O(n)$, we obtain

$$\left\| \frac{g}{\sqrt{\Sigma_{\boldsymbol{v}}}} \right\| \leq \sqrt{n} \cdot \|g\| \cdot \left\| \frac{1}{\sqrt{\Sigma_{\boldsymbol{v}}}} \right\| = O\left(\frac{1}{n^{1/4}}\right) = o\left(\frac{1}{\sqrt{\log n}}\right).$$

We can therefore apply Theorem 2 to sample the numerators of fresh encodings at level $\boldsymbol{v}$, according to a Gaussian distribution of parameter $\Sigma_{\boldsymbol{v}}$. Using tail-cut of Gaussian distributions, we have that if c is the numerator of a fresh encoding, then $\|c\| \leq n\|\sqrt{\Sigma_{\boldsymbol{v}}}\| \leq n^{1.5}\sigma_{\boldsymbol{v}}\|z_{\boldsymbol{v}}\|$ with overwhelming probability. This means that we can take

$$E \leq \Theta(n^{3.5} \cdot \|1/z_{\boldsymbol{v}}\| \cdot \|z_{\boldsymbol{v}}\|). \tag{10}$$

Hence, in the following methods (except the simplistic one), we will focus on the size of $\|1/z_{\boldsymbol{v}}\| \cdot \|z_{\boldsymbol{v}}\|$ to get a bound on the value of E.

Remark. Inequality (10) above is not tight. We could at least improve it to $E \leq \Theta(n^{3+\varepsilon} \cdot \|1/z_{\boldsymbol{v}}\| \cdot \|z_{\boldsymbol{v}}\|)$ for any $\varepsilon > 0$, by taking $\sigma_{\boldsymbol{v}} = \Theta(n^{1.75+\varepsilon}\|1/z_{\boldsymbol{v}}\|)$ (it still satisfies the condition of Theorem 2) and by noticing that $\|c\| \leq n\|\sqrt{\Sigma_{\boldsymbol{v}}}\| \leq n^{1.25}\sigma_{\boldsymbol{v}}\|z_{\boldsymbol{v}}\|$ for the numerator of a fresh encoding. This ensures statistical closeness to the desired distribution up to $\exp(-n^{2\varepsilon})$. Considering that there are already classical attacks in time $\exp(\tilde{O}(\sqrt{n}))$ (namely, using [6,14] to recover h from the ideal hR), one may just choose $\varepsilon = 1/4$.

3.1 The Simplistic Method

The simplistic method consists in always choosing $\Sigma_{\boldsymbol{v}} \sim 1$, independently of $\boldsymbol{v}$ and $z_{\boldsymbol{v}}$. This is done by applying Klein's algorithm [27], and requires for correctness [19, Theorem 4.1] that $\Sigma_{\boldsymbol{v}} = \sigma^2$ for a positive scalar $\sigma \in \mathbb{R}$, where $\sigma \geq \|g\| \cdot \omega(\sqrt{\log n})$. So by taking $\sigma = \Theta(n^{1+\varepsilon})$ with $\varepsilon > 0$, one may have $E = \Theta(\sqrt{n}\sigma) = \Theta(n^{1.5+\varepsilon})$, that is $\gamma = 1.5 + \varepsilon$ and $\eta = \nu = 0$.

This method was deemed subject to averaging attacks and hence less secure than the following one in [17], but the authors claim that their attack attempts failed because all recovered elements were larger that $\sqrt{q}$, and that averaging attacks would need super-polynomially many elements.[7] We make explicit an attack, and will show that this attack is possible even for exponential q, as long as E^κ remains polynomial: in other words, the presence of the mildly large factor h (of size $\sqrt{q}$) can be circumvented.

3.2 The Exponential Method

We present here the countermeasure of [17, Sect. 6.4], generalized to multi-dimensional universe, as done in [15, Sect. 2.1]. For $1 \leq i \leq \ell$, set z_i to be the canonical representative of $[z_i]$ in R (with coefficients in the range $[-q/2, q/2]$). Using rejection sampling when choosing z_i, assume that $\|z_i\| \cdot \|1/z_i\| \leq Z$; this is efficient for Z as small as $n^{5/2}$ using [15], and can even be improved to $Z = n^{3/2}$ using Lemma 3 below and its corollary.

For $\boldsymbol{v}$ in $\mathcal{A}$, set $z_{\boldsymbol{v}} = \prod z_i^{v_i}$ over R. Recall that Inequality (10) gives us: $E \leq \Theta(n^{3.5}\|1/z_{\boldsymbol{v}}\| \cdot \|z_{\boldsymbol{v}}\|)$. But we have $\|z_{\boldsymbol{v}}\| \leq n^{(\|v\|_1-1)/2}\prod_{i\in\boldsymbol{v}}\|z_i\|$ and $\|1/z_{\boldsymbol{v}}\| \leq n^{(\|v\|_1-1)/2}\prod_{i\in\boldsymbol{v}}\|1/z_i\|$. Hence we can take

$$E = \Theta(n^{2.5+\|v\|_1} \cdot Z^{\|v\|_1}) = \Theta(n^{2.5+2.5\|v\|_1}).$$

This means that we have $\gamma = 2.5, \eta = 2.5$ and $\nu = 0$.

Correctness is guaranteed for $q \geq n^{\Omega(\ell)}$ (because $\eta \neq 0$), and because ℓ is much larger than the constant degree κ in [15], this is not a satisfying solution, as we aim at decreasing q to polynomial. Two alternatives (conservative and aggressive) are therefore developed in [15].

[7] Recall that the original proposal was setting E and therefore q to be super-polynomial even for bounded degree ℓ because of the drowning technique for publicly sampling encodings. Since then, attacks using encodings of zero [13,24,34] have restricted encodings to be private, allowing polynomially large E.

3.3 The Conservative Method [15]

The first alternative suggested is to do as above, but reducing the $z_{\boldsymbol{v}}$ modulo q, that is, set $z_{\boldsymbol{v}}$ to be the representative of $[\prod z_i^{v_i}]$ with coefficients in $[-q/2, q/2]$. One then ensures, by rejection of all the z_i's together, that $\|z_{\boldsymbol{v}}\| \cdot \|1/z_{\boldsymbol{v}}\| \leq n^{2.5}$ for all $\boldsymbol{v} \in \mathcal{A}$. This leads to $E = \Theta(n^{3.5} \cdot n^{2.5}) = \Theta(n^6)$ (i.e., $\gamma = 6,\ \eta = \nu = 0$) and therefore allows correctness for q as small as $n^{O(\kappa)}$, which is polynomial for constant degree κ.

Using [15, Lemma 8] restated below, the authors conclude that this method is quite inefficient because for the above bound to hold simultaneously for all $\boldsymbol{v} \in \mathcal{A}$ with good probability, n must increase together with ℓ. Indeed, using Lemma 2, we can bound the probability that one of the $z_{\boldsymbol{v}}$ does not satisfy $\|z_{\boldsymbol{v}}\| \cdot \|1/z_{\boldsymbol{v}}\| \leq n^{2.5}$ by $2|\mathcal{A}|/n = 4\ell/n$. So if we want this probability to be small (say less than 1/2) in order for the sampling procedure to be efficient, we should increase n with ℓ.

Lemma 2 (Lemma 8 from [15]). *Let $[z]$ be chosen uniformly at random in R_q and z be its canonical representative in R (i.e., with coefficients in $[-q/2, q/2]$). Then it holds that*

$$Pr\left[\|1/z\| \geq n^2/q\right] \leq 2/n.$$

In the following section, we revisit the conservative method by generalizing this lemma.

3.4 The Conservative Method Revisited

In the following lemma, we introduce an extra degree of freedom c compared to the lemma of [15], but also improve the upper bound from $O(n^{1-c})$ to $O(n^{1-2c})$.

Lemma 3. *Let $[z]$ be chosen uniformly at random in R_q and z be its representative with coefficients between $-q/2$ and $q/2$. Then, for any $c \geq 1$, it holds that*

$$Pr[z = 0 \vee \|1/z\| \geq n^c/q] \leq 4/n^{2c-1}.$$

Corollary 2. *Let $[z]$ be chosen uniformly at random in $R_q^\times$ and z be its representative with coefficients between $-q/2$ and $q/2$. Then, for any $c \geq 1$, it holds that*

$$Pr[\|1/z\| \geq n^c/q] \leq 8/n^{2c-1}.$$

We can use this corollary to compute the probability that one of the $z_{\boldsymbol{v}}$ does not satisfy $\|1/z_{\boldsymbol{v}}\| \leq n^c/q$ when the $[z_i]$'s are independent and chosen uniformly at random in $R_q^\times$. Indeed, the $[z_{\boldsymbol{v}}]$'s are uniform in $R_q^\times$ because they are a product of uniform invertible elements, and, by union bound, we have

$$\begin{aligned}\Pr\left[\exists \boldsymbol{v} \in \mathcal{A} \text{ s.t. } \|1/z_{\boldsymbol{v}}\| > n^c/q\right] &\leq \sum_{\boldsymbol{v} \in \mathcal{A}} \Pr\left[\|1/z_{\boldsymbol{v}}\| > n^c/q\right] \\ &\leq \frac{8|\mathcal{A}|}{n^{2c-1}}.\end{aligned}$$

If we want this probability to be less than 1/2, in order to re-sample all the z_i's only twice on average, we should take

$$|\mathcal{A}| \leq \frac{n^{2c-1}}{16}. \tag{11}$$

But we also have $\|z_{\boldsymbol{v}}\| \leq \sqrt{n}\|z_{\boldsymbol{v}}\|_\infty \leq \sqrt{n}q$, hence $\|1/z_{\boldsymbol{v}}\| \cdot \|z_{\boldsymbol{v}}\| \leq n^{c+0.5}$. In order to minimize E, we wish to minimize c, under (11). By taking the minimal value of c that satisfies this constraint, and recalling that $|\mathcal{A}| = 2\ell$, we obtain

$$E = \Theta(n^{4.5+L/2}).$$

This means that $\gamma = 4.5$, $\nu = 0.5$ and $\eta = 0$. This conservative method revisited is the same as the original one, except that we improve on the encodings size bound E.[8] In the following, we will then only focus on the conservative method revisited and not on the original one.

Proof (Proof of Lemma 3). The proof of this lemma uses the same ideas as the one of [36, Lemma 4.1], but here, the element z is sampled uniformly modulo q instead of according to a Gaussian distribution. Let $[z]$ be chosen uniformly at random in R_q and z be its representative with coefficients between $-q/2$ and $q/2$. Recall that we denote $\sigma_j : K \to \mathbb{C}$ the complex embeddings of K in $\mathbb{C}$, with $1 \leq j \leq n$. We know that the size of z is related to the size of its embeddings. Hence, if we have an upper bound on the $|\sigma_j(1/z)|$, we also have an upper bound on $\|1/z\|$. Moreover, the σ_j's are morphisms, so $\sigma_j(1/z) = 1/\sigma_j(z)$, and it suffices to have a lower bound on $|\sigma_j(z)|$.

Let $j \in \{1, \cdots, n\}$, there exists a primitive $2n$-th root of unity ζ such that

$$\sigma_j(z) = \sum_{i=0}^{n-1} a_i \zeta^i,$$

where the a_i's are the coefficients of z, and so are sampled uniformly and independently between $-q/2$ and q/2. As ζ is a primitive 2^k-th root of unity for some k, there exists i_0 such that $\zeta^{i_0} = I$, where I is a complex square root of -1. So we can write

$$\sigma_j(z) = a_0 + I a_{i_0} + \tilde{z},$$

for some $\tilde{z} \in \mathbb{C}$ that is independent of a_0 and a_{i_0}. Now, we have that

$$\begin{aligned}\Pr\left[|\sigma_j(z)| < \frac{q}{n^c}\right] &= \Pr\left[a_0 + I a_{i_0} \in B(-\tilde{z}, \frac{q}{n^c})\right] \\ &\leq \frac{\mathrm{Vol}(B(-\tilde{z}, \frac{q}{n^c}))}{q^2} \\ &\leq \frac{4}{n^{2c}},\end{aligned}$$

[8] We also change a bit the point of view by fixing n first and then obtaining an upper bound on ℓ (which will appear because $\nu \neq 0$ in E), while the authors of [15] first fix ℓ and then increase n consequently.

where $B(-\tilde{z}, q/n^c)$ is the ball centered in $-\tilde{z}$ of radius q/n^c. A union bound yields that

$$\Pr\left[\exists j,\ |\sigma_j(z)| < \frac{q}{n^c}\right] \leq n \cdot \frac{4}{n^{2c}} = \frac{4}{n^{2c-1}}.$$

Which in turns implies

$$\Pr\left[\forall j,\ \left|\sigma_j\left(\frac{1}{z}\right)\right| \leq \frac{n^c}{q}\right] \geq 1 - \frac{4}{n^{2c-1}}.$$

To complete the proof, we use the fact that for cyclotomic fields of power-of-two order, we have $\|1/z\| \leq \max_j(|\sigma_j(1/z)|)$. This gives the desired result. □

Proof (Proof of Corollary 2). First, note that sampling $[z]$ uniformly in $R_q^\times$ is the same as sampling $[z]$ uniformly in R_q and re-sampling it until $[z]$ is invertible. We denote by $U(R_q)$ (resp. $U(R_q^\times)$) the uniform distribution in R_q (resp. $R_q^\times$). We then have that

$$\Pr_{[z]\leftarrow U(R_q^\times)}[\|1/z\| \geq n^c/q] = \Pr_{[z]\leftarrow U(R_q)}[\|1/z\| \geq n^c/q \mid [z] \in R_q^\times].$$

But using the definition of conditional probabilities, we can rewrite

$$\Pr_{[z]\leftarrow U(R_q)}[\|1/z\| \geq n^c/q \mid [z] \in R_q^\times] = \frac{\Pr_{[z]\leftarrow U(R_q)}[[z] \in R_q^\times \text{ and } \|1/z\| \geq n^c/q]}{\Pr_{[z]\leftarrow U(R_q)}[[z] \in R_q^\times]}.$$

The numerator of this fraction is less than $\Pr_{[z]\leftarrow U(R_q)}[\|1/z\| \geq n^c/q]$, which is less than $\frac{4}{n^{2c-1}}$ using Lemma 3. And at least half of the elements of R_q are invertible (if q is prime, we can even say that the proportion of non invertible elements is at most n/q, because $q \equiv 1 \mod 2n$). Hence, $\Pr_{[z]\leftarrow U(R_q)}[[z] \in R_q^\times] \geq 1/2$ and we obtain the desired result

$$\Pr_{[z]\leftarrow U(R_q^\times)}[\|1/z\| \geq n^c/q] \leq \frac{8}{n^{2c-1}}.$$

□

3.5 The Aggressive Method

This aggressive method was proposed by Döttling et al. in [15] in order to instantiate the GGH multilinear map for their obfuscator. This method cannot be used for any set of atoms $\mathcal{A}$, as it relies on the fact that the levels at which we encode fresh encodings have a specific structure. Indeed, for each $\boldsymbol{v} \in \mathcal{A}$, we have either $[z_{\boldsymbol{v}}] = [z_i]$ for some $i \in \{1, \cdots, \ell\}$ or $[z_{\boldsymbol{v}}] = [z^* \cdot z_i^{-1}]$. Using this remark, the secret $[z_i]$'s are generated in the following way.

For i from 1 to ℓ do:

- *sample a uniformly random invertible element $[z_i]$ in R_q. Let z_i be the representative of $[z_i]$ in R with coefficients between $-q/2$ and $q/2$, and $\widetilde{z}_i$ be the representative of $[z_i^{-1}]$ in R with coefficients between $-q/2$ and* q/2.
- *until both following conditions are satisfied, re-sample $[z_i]$:*

$$\|1/z_i\| \leq n^3/q \tag{12}$$
$$\|1/\widetilde{z}_i\| \leq n/q. \tag{13}$$

- *if $i = \ell$, we also re-sample $[z_i]$ until this third condition is met*

$$\|1/z^*\| \leq n/q, \tag{14}$$

where z^* is the representative of $[\prod_{1 \leq i \leq \ell} z_i]$ with its coefficients between $-q/2$ and q/2.

Remark. As we sample the $[z_i]$'s from $i = 1$ to ℓ, when we generate $[z_\ell]$ all other $[z_i]$'s are already fixed, so we can define $[z^*]$.

Note that with this method, we re-sample each z_i an expected constant number of times, independently of ℓ. Indeed, all $[z_i]$'s for $i \leq \ell - 1$ are sampled independently. And the two conditions we want are satisfied except with probability at most $\frac{8}{n}$ for each condition (using Corollary 2 with $[z_i]$ and $[z_i^{-1}]$ that are uniform in $R_q^\times$ and with $c = 3$ or $c = 1$). So, applying a union bound, the probability that we have to re-sample $[z_i]$ is at most $\frac{16}{n}$, which is less than 1/2 if $n \geq 32$. The idea is the same for $[z_\ell]$ except that we also want $\|1/z^*\|$ to be small. But all $[z_i]$ for $i < \ell$ are already fixed, so $[z^*]$ only depends on $[z_\ell]$ and is uniform in $R_q^\times$. Hence this last condition is also satisfied except with probability $\frac{8}{n}$ from Corollary 2. And the probability that the three conditions are met for $[z_\ell]$ is at least 1/2 as long as $n \geq 48$.

To conclude, if $n \geq 48$, the procedure described above will sample each $[z_i]$ at most twice in average, independently of the choice of ℓ. So we can choose ℓ arbitrarily large and the sampling procedure will take time $O(\ell) \cdot \mathrm{poly}(n)$.

It remains to choose our representative $z_{\boldsymbol{v}} \in R$ of $[z_{\boldsymbol{v}}] \in R_q$ and to get a bound on $\|1/z_{\boldsymbol{v}}\| \cdot \|z_{\boldsymbol{v}}\|$ for all $\boldsymbol{v} \in \mathcal{A}$, in order to get the value of E. We will show that $\|z_{\boldsymbol{v}}\| \cdot \|1/z_{\boldsymbol{v}}\| \leq n^4$ for some choice of the representative $z_{\boldsymbol{v}}$ we detail below.

First case. If $\boldsymbol{v}$ has weight 1, that is $[z_{\boldsymbol{v}}] = [z_i]$ for some i, then we take $z_{\boldsymbol{v}} = z_i$. With our choice of $[z_i]$, we have that $\|1/z_{\boldsymbol{v}}\| \leq n^3/q$. And as $\|z_{\boldsymbol{v}}\|$ has its coefficients between $-q/2$ and $q/2$ we have that $\|z_{\boldsymbol{v}}\| \leq \sqrt{n}q$ and hence $\|z_{\boldsymbol{v}}\| \cdot \|1/z_{\boldsymbol{v}}\| \leq n^{3.5} \leq n^4$.

Second case. If $\boldsymbol{v}$ has weight $\ell - 1$, then there exists $i \in \{1, \cdots, \ell\}$ such that $[z_{\boldsymbol{v}}] = [z^* \cdot z_i^{-1}]$. We choose as a representative of $[z_{\boldsymbol{v}}]$ the element $z_{\boldsymbol{v}} = z^* \cdot \widetilde{z}_i \in R$, with z^* and $\widetilde{z}_i$ as above (with coefficients between $-q/2$ and $q/2$). We then have

$$\|1/z_{\boldsymbol{v}}\| = \|1/z^* \cdot 1/\widetilde{z}_i\| \leq \sqrt{n} \cdot \|1/z^*\| \cdot \|1/\widetilde{z}_i\| \leq n^{2.5}/q^2.$$

Further, we have that $\|z_{\boldsymbol{v}}\| = \|z^* \cdot \widetilde{z_i}\| \leq \sqrt{n} \cdot \sqrt{n}q \cdot \sqrt{n}q = n^{1.5}q^2$. This finally gives us

$$\|z_{\boldsymbol{v}}\| \cdot \|1/z_{\boldsymbol{v}}\| \leq n^4.$$

To conclude, this method gives us

$$E = \Theta(n^{7.5}).$$

This means that $\gamma = 7.5$ and both η and ν are zero.

Remark. For all methods with $\Sigma_{\boldsymbol{v}} \sim z_{\boldsymbol{v}} \bar{z_{\boldsymbol{v}}}$ (i.e., all methods except the simplistic one), if $c \leftarrow D_{I+a, \sqrt{\Sigma_v}}$ is sampled using a Gaussian distribution of standard deviation $\sqrt{\Sigma_{\boldsymbol{v}}}$, we can rewrite $c = c^* z_{\boldsymbol{v}}$ with $c^* \leftarrow D_{\frac{I+a}{z_{\boldsymbol{v}}}, \sigma_{\boldsymbol{v}}}$ for some $\sigma_{\boldsymbol{v}} \in \mathbb{R}$. Note that c^* is now a following a spherical Gaussian distribution but its support depends on $z_{\boldsymbol{v}}$. In addition to this remark, one can observe that in all the methods described above, there exists a real σ such that $\sigma_{\boldsymbol{v}} \sigma_{\tilde{\boldsymbol{v}}} = \sigma$ for all $\boldsymbol{v} \in \mathcal{A}$ (in fact, $\sigma_{\boldsymbol{v}}$ only depends on the weight of $\boldsymbol{v}$ in all the methods above). This means that for every fresh encodings $[c_{\boldsymbol{v}} z_{\boldsymbol{v}}^{-1}]$ and $[c_{\tilde{\boldsymbol{v}}} z_{\tilde{\boldsymbol{v}}}^{-1}]$ at level $\boldsymbol{v}$ and $\tilde{\boldsymbol{v}}$ generated independently, we have an element $c^* \in K$, following an isotropic distribution[9] of variance σ^2 such that $c_{\boldsymbol{v}} c_{\tilde{\boldsymbol{v}}} = c^* z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$ in R. Again, we note that the support of c^* depends on $z_{\boldsymbol{v}}$ and $z_{\tilde{\boldsymbol{v}}}$, but as σ is larger than the smoothing parameter, this has no influence on the variance of c^* (by Lemma 1).

A summary of the different values of γ, η and ν for the different sampling methods can be found in Table 1.

4 Averaging Attack

4.1 Our Simple Setting of the GGH Multilinear Map

To study the leakage of the GGH multilinear map, we need to make reasonable assumptions on what is given to the adversary. It has been shown in [24] that knowing low level encodings of zero for the GGH13 multilinear map leads to zeroizing attacks that completely break the scheme. So our setting should not provide any, yet we will provide enough information for some zero-tests to pass. To this end, we will prove our setting to be secure in the weak multilinear map model, which supposedly prevents zeroizing attacks.

This setting is inspired by the use of multilinear maps in current candidate obfuscator constructions, and more precisely the low noise candidate obfuscator of [15]. Yet, for easier analysis, we tailored this setting to the bare minimum. We will assume the degree of the multilinear map to be exactly $\kappa = 2$, and will provide the attacker with elements that pass zero-test under a known polynomial. The restriction $\kappa = 2$ can easily be lifted but it would make the exposition of the model and the analysis of the leakage less readable.

[9] c^* is isotropic as it is the product of two independent isotropic Gaussian variables.

More precisely, we fix a number $m > 1$ of monomials, and consider the homogeneous degree-2 polynomial:

$$H(x_1, y_1, \ldots, x_m, y_m) = \sum x_i y_i.$$

Recall that we chose the set of "atoms" $\mathcal{A}$ to be the set of levels $\boldsymbol{v} \in \{0,1\}^\ell$ that have weight exactly 1 or $\ell - 1$, where the weight of $\boldsymbol{v}$ is the number of its non-zero coefficients. For all $\boldsymbol{v} \in \mathcal{A}$, we let $\tilde{\boldsymbol{v}} = \boldsymbol{v}^* - \boldsymbol{v}$ (we say that $\tilde{\boldsymbol{v}}$ is the complement of $\boldsymbol{v}$). We assume that for each $\boldsymbol{v} \in \mathcal{A}$ of weight 1, the authority reveals encodings $u_{\boldsymbol{v},1}, \ldots, u_{\boldsymbol{v},m}$ at level $\boldsymbol{v}$ of random values $a_{\boldsymbol{v},1}, \ldots, a_{\boldsymbol{v},m}$ modulo I, and encodings $u_{\tilde{\boldsymbol{v}},1}, \ldots, u_{\tilde{\boldsymbol{v}},m}$ at level $\tilde{\boldsymbol{v}}$ of random values $a_{\tilde{\boldsymbol{v}},1}, \ldots, a_{\tilde{\boldsymbol{v}},m}$ modulo I, under the only constraint that

$$H(a_{\boldsymbol{v},1}, a_{\tilde{\boldsymbol{v}},1}, \ldots, a_{\boldsymbol{v},m}, a_{\tilde{\boldsymbol{v}},m}) = 0 \bmod I.$$

We remark that generating almost uniform values $a_{\cdot,\cdot}$ under the constraint above is easily done, by choosing all but one of them at random, and setting the last one to

$$a_{\tilde{\boldsymbol{v}},m} = -a_{\boldsymbol{v},m}^{-1} \sum_{i=1}^{m-1} a_{\boldsymbol{v},i} a_{\tilde{\boldsymbol{v}},i} \bmod I.$$

In the weak multilinear map model [15,18,34], we can prove that an attacker that has access to this simple setting of the GGH multilinear map cannot recover a multiple of the secret element g, except with negligible probability. The definition of the weak multilinear map model and the proof that an attacker cannot recover a multiple of g can be found in the full version [16].[10] This weak multilinear-map model was used to prove security of candidate obfuscators in [15,18], as it is supposed to capture zeroizing attacks, like the ones of [11,34]. In the weak multilinear map model, recovering a multiple of g is considered to be a successful attack. This is what motivates our proof that no polynomial time adversary can recover a multiple of g in our simple setting, under this model.

4.2 Analysis of the Leaked Value

We describe in this section the information we can recover using averaging attacks, depending on the sampling method. We will see that depending on the sampling method, we can recover an approximation of $A(z^*h/g)$, or an approximation of $A(h/g)$ or even the exact value of $A(h/g)$. In order to unify notation, we introduce the leakage $\mathfrak{L}$, which will refer to $A(z^*h/g)$ or $A(h/g)$ depending the method. We explain below what is the value of $\mathfrak{L}$ for the different methods, and how we can recover an approximation of it. In the case of the simplistic method, we also explain how we can recover the exact value of $\mathfrak{L}$ from its approximation and how to use it to create a zero-testing parameter at level $2\boldsymbol{v}^*$.

[10] The idea of the proof is the same as in [15,18], in a much simpler context (this is based on a generalized version of the Schwartz-Zippel lemma from [34]).

Statistical leakage. Let $\boldsymbol{v} \in \mathcal{A}$ be of weight 1. We denote by $[u_{\boldsymbol{v}}]$ the encoding $[H(u_{\boldsymbol{v},1}, u_{\tilde{\boldsymbol{v}},1}, \dots, u_{\boldsymbol{v},m}, u_{\tilde{\boldsymbol{v}},m})]$. Recall that we have $[u_{i,\boldsymbol{v}}] = [c_{i,\boldsymbol{v}} z_{\boldsymbol{v}}^{-1}]$, where $c_{i,\boldsymbol{v}} = a_{i,\boldsymbol{v}} + r_{i,\boldsymbol{v}} g$ for some $r_{i,\boldsymbol{v}} \in R$. So using the definition of H and the fact that $[u_{\boldsymbol{v}}]$ passes the zero test, we can rewrite

$$\begin{aligned}
[u_{\boldsymbol{v}} p_{zt}] &= [H(c_{\boldsymbol{v},1}, c_{\tilde{\boldsymbol{v}},1}, \dots, c_{\boldsymbol{v},m}, c_{\tilde{\boldsymbol{v}},m})(z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}})^{-1} \cdot z^* h g^{-1}] \\
&= [H(c_{\boldsymbol{v},1}, c_{\tilde{\boldsymbol{v}},1}, \dots, c_{\boldsymbol{v},m}, c_{\tilde{\boldsymbol{v}},m}) \cdot h g^{-1}] \\
&= H(c_{\boldsymbol{v},1}, c_{\tilde{\boldsymbol{v}},1}, \dots, c_{\boldsymbol{v},m}, c_{\tilde{\boldsymbol{v}},m}) \cdot h/g.
\end{aligned}$$

Note that the product of the last line is in R, as it is a product of small elements compared to q. Also, the first term is a small multiple of g so we can divide by g. We denote by $w_{\boldsymbol{v}} \in R$ the value above (i.e., the representative of $[u_{\boldsymbol{v}} p_{zt}]$ with coefficients in $[-q/2, q/2]$). The term h/g of the product is fixed, but the first factor $H(c_{\boldsymbol{v},1}, c_{\tilde{\boldsymbol{v}},1}, \dots, c_{\boldsymbol{v},m}, c_{\tilde{\boldsymbol{v}},m})$ depends on $\boldsymbol{v}$: we can average over it. We now analyze this first factor, depending on the method we choose for generating the fresh encodings of the GGH map. We will denote by $Y_{\boldsymbol{v}}$ the random variable $H(c_{\boldsymbol{v},1}, c_{\tilde{\boldsymbol{v}},1}, \dots, c_{\boldsymbol{v},m}, c_{\tilde{\boldsymbol{v}},m})$.

By definition of the polynomial H, we know that $Y_{\boldsymbol{v}} = \sum c_{i,\boldsymbol{v}} c_{i,\tilde{\boldsymbol{v}}}$. Moreover, all the $c_{i,\boldsymbol{v}}$ are independent when i or $\boldsymbol{v}$ vary. So the $c_{i,\boldsymbol{v}} c_{i,\tilde{\boldsymbol{v}}}$ are centered random variables of variance $\Sigma_{\boldsymbol{v}} \Sigma_{\tilde{\boldsymbol{v}}}$ (observe that the variance of a product of independent centered variables is the product of their variances) and $Y_{\boldsymbol{v}}$ is a centered random variable of variance $m \Sigma_{\boldsymbol{v}} \Sigma_{\tilde{\boldsymbol{v}}}$ (recall that H is a sum of m monomials). We now consider several cases, depending on the choice of $\Sigma_{\boldsymbol{v}}$.

Case 1 (the simplistic method). In this case, we have $\Sigma_{\boldsymbol{v}} = \sigma^2$ for all $\boldsymbol{v} \in \mathcal{A}$, for some $\sigma \in \mathbb{R}$. This means that the $Y_{\boldsymbol{v}}$ are centered isotropic random variables with the same variance. Let us call $\mu := \mathbb{E}[A(Y_{\boldsymbol{v}})] = m\sigma^2 \in \mathbb{R}^+$ this variance. If we compute the empirical mean of the $A(Y_{\boldsymbol{v}})$, this will converge to μ and we can bound the speed of convergence using Hoeffding's inequality. Going back to the variables $w_{\boldsymbol{v}} = Y_{\boldsymbol{v}} \cdot h/g$, we have that $\mathbb{E}[A(w_{\boldsymbol{v}})] = \mu \cdot A(h/g)$ for some μ in $\mathbb{R}^+$. Furthermore, all the $A(w_{\boldsymbol{v}})$, with $\boldsymbol{v}$ of weight 1, are independent variables with the same mean, so we can apply Hoeffding's inequality.

Case 2 (the conservative method). In this case, we chose $\Sigma_{\boldsymbol{v}} \sim z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$. We do not know the variance of the $Y_{\boldsymbol{v}}$ (because the $z_{\boldsymbol{v}}$ are secret) but we will be able to circumvent this difficulty, by averaging over the $z_{\boldsymbol{v}}$'s.

First, using the remark we made at the end of Sect. 3, we have that $Y_{\boldsymbol{v}} = \sum c_{i,\boldsymbol{v}} c_{i,\tilde{\boldsymbol{v}}} = \sum c^*_{i,\boldsymbol{v}} z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$, with the $c^*_{i,\boldsymbol{v}}$ being independent centered isotropic random variables with the same variance $\sigma^2 \in \mathbb{R}^+$. Hence, we can rewrite $Y_{\boldsymbol{v}} = X_{\boldsymbol{v}} z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$ with $X_{\boldsymbol{v}}$ a centered isotropic variable of variance $m\sigma^2$ (which is independent of $\boldsymbol{v}$). Unlike the previous case, we now have some $z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$ that contribute in Y_v. However, we will be able to remove them again by averaging.

Indeed, even if all the $z_{\boldsymbol{v}}$ satisfy $[z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}] = [z^*]$ in R_q, this is not the case in R, and that individually each $z_{\boldsymbol{v}}$ is essentially[11] uniform in the hypercube

[11] Up to the invertibility condition in R_q.

$[-q/2, q/2]^n$, in particular it is isotropic. For our analysis, let us treat the $z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$ as random variables in R, that are isotropic and independent when $\boldsymbol{v}$ varies. The isotropy follows from the fact that the two factors are isotropic. The independence assumption is technically incorrect, yet as the only dependence are of arithmetic nature over R_q and that the elements in question are large, one does not expect the correlation to be geometrically visible.

We will call $\mu_z := \mathbb{E}\left[A(z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}})\right]$ their variance. Recall that as the $z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$ are isotropic, μ_z is in $\mathbb{R}^+$. While the independence assumption may be technically incorrect, experiments confirm that the empirical mean $\mathbb{E}\left[A(z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}})\right]$ does indeed converge to some $\mu_z \in \mathbb{R}^+$ as the number of sample grows, and more precisely it seems to converge as $\mu_z \cdot (1 + \varepsilon)$ where $\varepsilon \in K_{\mathbb{R}}$ satisfies $\|\varepsilon\|_\infty = \tilde{O}(\sqrt{1/|\mathcal{A}|})$, as predicted by the Hoeffding bound (results of the experiments are given in the full version [16]).

Assuming that the $X_{\boldsymbol{v}}$ are independent of the $z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$,[12] we finally obtain

$$\mathbb{E}[A(Y_{\boldsymbol{v}})] = \mathbb{E}[A(X_{\boldsymbol{v}})]\mathbb{E}[A(z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}})] = m\sigma^2 \mu_z.$$

We denote by $\mu = m\sigma^2\mu_z$ this value. As in the previous case, the variables $A(w_{\boldsymbol{v}})$ are independent (when $\boldsymbol{v}$ has weight 1) and have the same mean

$$\mathbb{E}\left[A(w_{\boldsymbol{v}})\right] = \mu \cdot A(h/g),$$

with $\mu \in \mathbb{R}^+$.

Case 3 (the exponential and aggressive methods). In these methods, we can again write $Y_{\boldsymbol{v}} = X_{\boldsymbol{v}} z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$ with $X_{\boldsymbol{v}}$ a centered isotropic variable of variance $m\sigma^2$ for some $\sigma \in \mathbb{R}^+$, independent of $\boldsymbol{v}$. However, unlike the previous case, the $z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$ are not isotropic variables anymore and therefore the z's do not "average-out".

In the exponential method, the identity $z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}} = z^*$ holds over R (where $z^* = \prod_i z_i \in R$ is a representative of $[z^*]$), hence, $z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}}$ is constant when $\boldsymbol{v}$ varies, and we have

$$\mathbb{E}\left[A(w_{\boldsymbol{v}})\right] = \mu \cdot A(hz^*/g),$$

for some scalar $\mu \in \mathbb{R}^+$.

In the aggressive method, we have $z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}} = z^* \cdot \widetilde{z_i} \cdot z_i$ for some $1 \leq i \leq \ell$, with z^* the representative of $[z^*]$, z_i the representative of $[z_i]$ and $\widetilde{z_i}$ the representative of $[z_i^{-1}]$ with coefficients in $[-q/2, q/2]$. The element z^* is fixed, but, as in the conservative case, we can see the $\widetilde{z_i} \cdot z_i$ as isotropic variables. Assuming they are independent, we then have $\mathbb{E}\left[A(z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}})\right] = \mu_z A(z^*)$ for some scalar $\mu_z \in \mathbb{R}^+$. And we again have

$$\mathbb{E}\left[A(w_{\boldsymbol{v}})\right] = \mu \cdot A(hz^*/g),$$

for some scalar $\mu \in \mathbb{R}^+$.

[12] We can view the variables $c^*_{i,\boldsymbol{v}}$ as being independent of the variables $z_{\boldsymbol{v}}$ because the standard deviation of the Gaussian distribution is larger than the smoothing parameter (see Lemma 1).

Conclusion on the average. To conclude, we have argued that in all methods,

$$\mathbb{E}\left[A(w_{\boldsymbol{v}})\right] = \mu \cdot \mathfrak{L}$$

for some scalar $\mu \in \mathbb{R}^+$, where the leaked variable $\mathfrak{L}$ depends on the sampling method in the following way:

- $\mathfrak{L} = A(h/g)$ for the simplistic and the conservative methods.
- $\mathfrak{L} = A(hz^*/g)$ for the exponential and the aggressive methods.

Now, using the fact that the random variables $A(w_{\boldsymbol{v}})$ are independent for different $\boldsymbol{v} \in \mathcal{A}$ of weight 1, we can compute their empirical mean and Hoeffding's inequality will allow us to bound the distance to the theoretical mean. In the following we assume that we know μ.[13]

Relative error of the leakage. Compute

$$W = \frac{2}{|\mathcal{A}|} \sum_{\substack{\boldsymbol{v}\in\mathcal{A} \\ \boldsymbol{v} \text{ of weight } 1}} A(w_{\boldsymbol{v}})$$

the empirical mean of the random variables $A(w_{\boldsymbol{v}})$. This is an approximation of $\mu \cdot \mathfrak{L}$. We know that the coefficients of the random variable $w_{\boldsymbol{v}}$ are less than q, so the coefficients of $A(w_{\boldsymbol{v}})$ are less that nq^2. By applying Hoeffding's inequality in R (Corollary 1) with $\varepsilon = 1/n$, $B = nq^2$ and $m = |\mathcal{A}|/2$, we have that $\|W - \mu \cdot \mathfrak{L}\|_\infty < \frac{nq^2\sqrt{8 \ln n}}{\sqrt{|\mathcal{A}|}}$ (except with probability at most $2/n$). As the coefficients of $\mu\mathfrak{L}$ are of the order of nq^2, we have a relative error $\delta < \sqrt{8 \ln n/|\mathcal{A}|}$ for each coefficient of $\mu\mathfrak{L}$. As μ is known, this means that we know $\mathfrak{L}$ with a relative error at most $\sqrt{8 \ln n/|\mathcal{A}|}$.[14]

Unfortunately, we cannot directly recover the exact value of $\mathfrak{L}$ because its coefficients are not integers. When $\mathfrak{L} = A(hz^*/g)$, i.e., for the exponential and aggressive methods, we do not know how to use this approximation of $\mathfrak{L}$ to recover the exact value of $\mathfrak{L}$.[15] When $\mathfrak{L} = A(h/g)$, i.e., for the simplistic and conservatives methods, we can circumvent this difficulty. The idea is to transform our approximation of $\mathfrak{L}$ into an approximation of an element $r \in R$, with coefficients that are integers of logarithmic bit-size. Indeed, if we have an approximation of r with error less that $1/2$ we can round its coefficients and recover the exact value of r. And we can get such an approximation using a polynomial

[13] The value of the scalar μ can be obtained from the parameters of the multilinear maps. If we do not want to analyze the multilinear map, we can guess an approximation of μ with a sufficiently small relative error, by an exhaustive search.

[14] Again, if we do not know μ, we can guess an approximation of μ with relative error at most $\sqrt{8 \ln n/|\mathcal{A}|}$ (so that it has no influence on our approximation of $\mathfrak{L}$), with an exhaustive search.

[15] Note that if we recover the exact value of $A(hz^*/g)$, then its denominator is a multiple of g and this is considered as a success of the attacker in the weak multilinear map model.

number of samples because the coefficients we want to recover have logarithmic bit-size. This is what we explain in next subsection. Unfortunately, we will see that for the conservative method, the number of samples we need to be able to round r to its exact value is not compatible with the constraint we had on $|\mathcal{A}|$ for being able to generate the $z_{\boldsymbol{v}}$.

From the leakage to a complete attack against the GGH map. In this section, we explain how we can recover the exact value of $A(h/g)$, when $\mathfrak{L} = A(h/g)$ and we have enough samples. We then show how we can use this exact value to construct a zero-testing parameter at level $2\boldsymbol{v}^*$.

Recovering $\mathfrak{L}$ *exactly when* $\mathfrak{L} = A(h/g)$. In the following, we assume that we have an approximation of $A(h/g)$ with relative error $\delta < \sqrt{8 \ln n / |\mathcal{A}|}$ and we want to recover the exact value of $A(h/g)$. Let u be any encoding at level $\boldsymbol{v^*}$ that passes the zero test (we can take u to be one of the $[u_{\boldsymbol{v}}] = [H(u_{\boldsymbol{v},1}, u_{\tilde{\boldsymbol{v}},1}, \ldots, u_{\boldsymbol{v},m}, u_{\tilde{\boldsymbol{v}},m})]$). We have that $[u \cdot p_{zt}] = c \cdot h/g \in R$ for some small multiple c of g. In particular, the coefficients of c are somehow small[16] and are integers. Using our approximation W of $\mu \cdot A(h/g)$ with relative error δ plus the fact that we know μ and $c \cdot h/g$, we can recover an approximation of $A(c)$ with relative error at most $\delta \cdot n^2$ by computing $A(c \cdot h/g) \cdot \mu \cdot W^{-1}$.

The coefficients of $A(c)$ are integers and are less than $m^2 n^2 E^4$. Indeed, $c = H(c_{\boldsymbol{v},1}, c_{\tilde{\boldsymbol{v}},1}, \ldots, c_{\boldsymbol{v},m}, c_{\tilde{\boldsymbol{v}},m})$ for some $\boldsymbol{v}$ and we have $\|c_{\boldsymbol{v},i}\| \leq E$ for all $\boldsymbol{v}$'s and i's. So we know that $\|c\| \leq mn^{1/2}E^2$ and we get the desired bound on $\|A(c)\|_\infty$. Hence, if we have an approximation of the coefficients of $A(c)$ with relative error at most $\frac{1}{2m^2n^2E^4}$, the absolute error is less that $1/2$ and we can round the coefficients to recover $A(c)$ exactly. We can then recover $A(h/g)$ exactly by computing $A(c \cdot h/g)/A(c)$.

Putting together the conditions we got on the parameters, we have $\delta < \sqrt{\frac{8 \ln n}{|\mathcal{A}|}}$ and we want $\delta \cdot n^2 < \frac{1}{2m^2n^2E^4}$ to be able to recover $A(c)$. This is satisfied if $\sqrt{\frac{8 \ln n}{|\mathcal{A}|}} < \frac{1}{2m^2n^4E^4}$, i.e., $|\mathcal{A}| > 32E^8m^4n^8 \ln n$.

To conclude, if $|\mathcal{A}| > 32E^8m^4n^8 \ln n$, we can recover $A(g/h) \in K$ exactly.[17] In Sect. 4.3, we compare this constraint to the ones we had for the samplings methods. We will see that for the simplistic method, our constraints are compatible, so we can perform the attack. But this is not the case with the conservative method.

Using A(h/g) to create a zero testing parameter at a forbidden level. We present here a possible way of using the recovered value $A(h/g)$. Note that in current obfuscation model (for instance the weak multilinear map model of [18] or [15]), recovering $A(h/g)$ is already considered as a success for the attacker. Indeed, its denominator is a multiple of $A(g) = g\bar{g}$ so in particular we have recovered a

[16] Recall that q may be exponentially large but we assumed that the numerator of a top level encoding remains polynomial in n.

[17] Note that this bound does not depends on q but only on E. This is why our attack still works even if q is exponential in n, as long as E remains polynomial in n.

multiple of g, which is considered as a success of the attacker in these models.[18] Moreover, even if we do not consider that recovering a multiple of g is bad news, we present here a way of using $A(h/g)$ to create a zero-testing parameter at a higher level than $\boldsymbol{v}^*$ (here we create a zero-testing parameter at level $2\boldsymbol{v}^*$).

First, note that the complex conjugation $\bar{\cdot}$ in R is compatible with R_q. Indeed, let $c, r \in R$, we have $\overline{c+qr} = \bar{c} + \overline{qr} = \bar{c} + q\bar{r}$ (because $\bar{\cdot}$ is $\mathbb{R}$-linear). So $\overline{c+qr} \equiv \bar{c} \bmod q$ and we can define the operation $\bar{\cdot}$ in R_q by $\overline{[r]} = [\bar{r}]$. We will use this to construct our zero-testing parameter. Let again $[u]$ be an encoding of zero at level $\boldsymbol{v}^*$ and write $[u] = [c \cdot (z^*)^{-1}]$ where c is a small multiple of g. Compute

$$\begin{aligned} p'_{zt} &= [\bar{u} \cdot p_{zt}^2 \cdot \overline{p_{zt}} \cdot A(h/g)^{-1}] \\ &= \left[\frac{\bar{c}}{\overline{z^*}} \cdot \frac{(z^*)^2 h^2}{g^2} \cdot \frac{\overline{z^*}\,\bar{h}}{\bar{g}} \cdot \frac{g\bar{g}}{h\bar{h}} \right] \\ &= \left[\frac{(z^*)^2 \cdot (h\bar{c})}{g} \right]. \end{aligned}$$

As $h\bar{c}$ is small compared to q, this is likely to give us a zero-testing parameter at level $2\boldsymbol{v}^*$. To be sure that we can indeed zero-test at level $2\boldsymbol{v}^*$, we should check that the noise obtained at that level, when multiplied by $h\bar{c}$, does not become larger than q.

A sufficient condition for this attack to succeed is that

$$B + 3 + 3\kappa(1/2 + \gamma + \nu L) + \eta\ell \leq Q/4 \tag{15}$$

which is a variation on Inequality (9) where κ has been replaced by 3κ.

Note that the typical choice of q in [15,17] includes quite some extra margin compared to our condition (9). But even if q is chosen tightly following Inequality (9), it is not clear that the attack is prevented. Indeed, these conditions (9) and (15) are derived from the worst case inequality (1) ($\|xy\| \leq \sqrt{n} \cdot \|x\| \cdot \|y\|$), and may therefore be far from tight in the average case. In fact, $\|xy\|/(\|x\| \cdot \|y\|)$ can be arbitrarily small for well chosen x and y.

Determining whether there exist parameters that guarantee that legitimate zero-tests at level $\boldsymbol{v}^*$ almost always succeed while fraudulent zero-tests at level $\boldsymbol{2v}^*$ almost always fail would require a quite refined analysis of the distributions at hand, which is beyond the scope of this work. Indeed, we find it preferable to block this type of attacks by more robust means.

4.3 Noise Analysis of the Leakage

We sum up in this section the leakage that we can obtain and with which precision, depending on the sampling methods presented in Sect. 3.

[18] For this to be true, we need h and g to be co-prime. But as the ideal $\langle g \rangle$ is prime, this will be true unless h is a multiple of g. And the case where h is a multiple of g is not a problem, as we can easily recover multiples of h (and so multiples of g).

The simplistic method. In this method, we have $\mathfrak{L} = A(h/g)$. Recall that in this case, we can recover the exact value of $\mathfrak{L}$ if $\ell > 16E^8m^4n^8 \ln n$ (using the fact that $|\mathcal{A}| = 2\ell$). But in this method, we had $E = O(n^{1.5+\varepsilon})$, for any $\varepsilon > 0$. Hence, taking $\ell = \Theta(n^{20+8\varepsilon}m^4 \ln n)$ satisfies the conditions for generating the parameters plus our condition $\ell > 16E^8m^4n^8 \ln n$. To conclude, when using the simplistic method with some choice of the parameters, we can recover the exact value $A(h/g)$ and use it to construct a forbidden zero-testing parameter at level $2\boldsymbol{v}^*$. Note that recovering $A(h/g)$ also means that we recovered a multiple of g. However, we proved that in the weak multilinear map model, no polynomial time attacker could recover a multiple of g. This proves that the averaging attack described above is not captured by the weak multilinear map model.

Remark. For this sampling method, as $\Sigma_{\boldsymbol{v}} \sim 1$, we do not need to average over the $\boldsymbol{v}$, so we could also have $\ell = 2$ as long as we have enough samples for each $\boldsymbol{v}$.

The exponential method. In this method, we have $\mathfrak{L} = A(z^*h/g)$. We can recover an approximation of $\mu\mathfrak{L}$ with relative error at most $\sqrt{\frac{8 \ln n}{|\mathcal{A}|}}$. We do not know if it is possible to recover $\mathfrak{L}$ exactly.

The conservative method revisited. In this method, we have $\mathfrak{L} = A(h/g)$, we can recover an approximation of $\mu\mathfrak{L}$ with relative error at most $\sqrt{\frac{8 \ln n}{|\mathcal{A}|}}$ according to our heuristic analysis. While the independence condition between the $A(z_{\boldsymbol{v}} z_{\tilde{\boldsymbol{v}}})$ for applying Hoeffding's bound may not be satisfied, we show that this rate of convergence seems correct in practice (see the experiments in the full version [16]).

Recall that if $\ell > 16E^8m^4n^8 \ln n$, then we can recover $A(h/g)$ exactly. But for the sampling method to work, we need to take $E = \Theta(n^{4.5}\sqrt{\ell})$. Hence, the condition $\ell > 16E^8m^4n^8 \ln n$ can be rewritten

$$\ell > \Theta(n^{44}\ell^4m^4 \ln n).$$

This condition cannot be satisfied, so we cannot have enough samples for our attack when using this sampling method. And all we get is an approximation of $\mu A(h/g)$. Nevertheless, the only thing that prevents the full attack is the size of the parameters we have to choose in order to be able to generate the fresh encodings.

The aggressive method. In this method, we have $\mathfrak{L} = A(z^*h/g)$. We can recover an approximation of $\mu\mathfrak{L}$ with relative error at most $\sqrt{\frac{8 \ln n}{|\mathcal{A}|}}$. We do not know if it is possible to recover $\mathfrak{L}$ exactly.

4.4 Conclusion

We give in Table 1 a summary of the parameters used for the different sampling methods, and of the resulting leakage. The column'constraints' specifies possible constraints on the parameters or on the atoms set $\mathcal{A}$, that arise when using this sampling method. Recall that due to the correctness bound (9), there is always a constraint on the modulus q, so we do not mention it in the column ‘constraints’. This constraint on q can be obtained from the columns γ, η and ν, using the formula $\log q \geq 4\log(n)(3 + \kappa/2 + \kappa\gamma + \kappa\nu L + \eta\ell) + 4\log(m)$.

Table 1. Summary of the leakage analysis, depending on the sampling method. This includes our new method, sketched in Sect. 5. We recall that, according to correctness bound (9), the modulus q must satisfy $\log q \geq 4\log(n)(3+\kappa/2+\kappa\gamma+\kappa\nu L+\eta\ell)+4\log(m)$.

Sampling method	γ	η	ν	leakage $\mathfrak{L}$	full attack?	constraints
Simplistic [17]	$1.5 + \varepsilon$	0	0	$A(h/g)$	yes	none
Exponential [17]	2.5	2.5	0	$A(z^*h/g)$	no	none
Conservative [15]	6	0	0	$A(h/g)$	no	$n \geq 4\ell$
Conservative (revisited)	4.5	0	0.5	$A(h/g)$	no	none
Aggressive [15]	7.5	0	0	$A(z^*h/g)$	no	structure of $\mathcal{A}$
Compensation (Sec. 5)	$1.5 + 1/\kappa + \varepsilon$	0	0	1	no	none

We have seen that the leakage obtained in the conservative method is the same as the one of the unprotected scheme (the simplistic method). However, in the case of the conservative method, the number of available samples is not sufficient to complete the attack, as it is the case in the simplistic method. This limitation on the number of samples comes from some constraints in the sampling procedure and seems a bit accidental, we do not find this version of the countermeasure fully satisfactory.

We can also question the security of the other methods (exponential and aggressive), which leak an approximation of $A(hz^*/g)$, related to secret values. More precisely, one could wonder whether this noisy leakage could be combined with the knowledge of $p_{zt} = [hz^*g^{-1}]$ to mount an attack. As this problem does not look like any traditional (ideal) lattice problem, we fail to conclude beyond reasonable doubt that it should be intractable. We would find it more rational to make the leakage unrelated to secret parameters. In the following section, we propose such a design, which is simple, and leads to better parameters.

5 The Compensation Method

In this section, we propose a new sampling method which is designed so that the leakage $\mathfrak{L}$ that an attacker can recover by using the averaging attack described above, reveals no information about secret parameters of the GGH map. Nevertheless, we note that even if the attack described above does not apply directly to this method, other averaging attacks may be able to leak secret information. An idea could be to fix some encodings and average over the others.

Discussion on design. We have seen that choosing different covariance parameters $\Sigma_{\boldsymbol{v}}$ at different levels $\boldsymbol{v}$ can in fact make the leak *worse*, as the attacker can choose to average them out. We also remark that the parameters $[z_{\boldsymbol{v}}]$ can be *publicly re-randomized* without affecting anything else, in particular without affecting the covariance $\Sigma_{\boldsymbol{v}}$ of the numerator of the encodings. Indeed, we can choose random invertible elements $[\hat{z}_i] \in R_q^{\times}$, and apply the following transformation to all encodings $e_{\boldsymbol{v}}$ at level $\boldsymbol{v}$, as well as to the zero-testing parameter $[p_{zt}]$:

$$[e_{\boldsymbol{v}}] \mapsto \left[\prod_{i \in \boldsymbol{v}} \hat{z}_i^{-1}\right] \cdot [e_{\boldsymbol{v}}], \quad [p_{zt}] \mapsto \left[\prod_{i \in \boldsymbol{v}^\star} \hat{z}_i\right] [p_{zt}].$$

This means that the relation between the covariance $\Sigma_{\boldsymbol{v}}$ and the denominators $z_{\boldsymbol{v}}$ can be publicly undone while maintaining functionality.

The compensation method. We therefore proceed to set $\Sigma_{\boldsymbol{v}} = \Sigma$ for all levels $\boldsymbol{v}$, and to choose Σ independently of the $z_{\boldsymbol{v}}$. Doing so, we observe that the leakage $\mathfrak{L}$ will generically be:

$$\mathfrak{L} \sim \Sigma^{\kappa} \cdot A(h/g). \tag{16}$$

We then choose $\Sigma \sim A(g/h)^{1/\kappa}$, ensuring $\mathfrak{L} \sim 1$: the leakage is made constant, unrelated to any secret. We insist nevertheless that, as the previous methods, this method comes with no formal security argument. We also warn that we have not thoroughly explored more general leakage attacks, varying the zero-tested polynomials or keeping some encodings fixed.

It remains to see how short one can efficiently sample encodings following this choice. To get tighter bounds, we look at the conditioning number (or distortion) $\delta(\sqrt{\Sigma}) = \frac{\max(\sigma_i(\sqrt{\Sigma}))}{\min(\sigma_i(\sqrt{\Sigma}))}$, where σ_i runs over all embeddings. One easily verifies the following properties:

$$\delta(A(x)) = \delta(x)^2 \tag{17}$$

$$\delta(x^k) = \delta(x)^{|k|} \quad \text{for any } k \in \mathbb{R}, \tag{18}$$

$$\delta(xy) \leq \delta(x)\delta(y). \tag{19}$$

If a variable $x \in K_{\mathbb{R}}$ has independent continuous Gaussian coefficients of parameter 1, then its embeddings are (complex) Gaussian variables of parameter $\Theta(\sqrt{n})$, and it holds with constant probability that

$$\forall i, \quad \Omega(1) \leq |\sigma_i(x)| \leq O(\sqrt{n \log n}). \tag{20}$$

Indeed, the right inequality follows from classic tail bounds on Gaussian. For the left inequality, consider that $|\sigma_i(x)| \geq \max(|\Re(\sigma_i(x))|, |\Im(\sigma_i(x))|)$, where both the real and imaginary parts are independent Gaussian of parameter $\Theta(\sqrt{n})$: each part will be smaller than $\Theta(1)$ with probability at most $1/\sqrt{2n}$. By independence, $|\sigma_i(x)| \leq \Theta(1)$ holds with probability at most $1/2n$ for each i, and one may conclude by the union bound.

By scaling (and plausibly ignoring discreteness issues since g and h are sampled above the smoothing parameter of $\mathbb{Z}^n$) we can therefore assume, using rejection sampling over h and g, that $\delta(g), \delta(h) \leq O(\sqrt{n \log n})$, and therefore

$$\delta(\sqrt{\Sigma}) = \delta(A(g/h))^{1/2\kappa} \leq (\delta(g)\delta(h))^{1/\kappa} \leq O(n \log n)^{1/\kappa}.$$

This allows us to scale Σ so that:

- $\|g/\sqrt{\Sigma}\| \leq o(1/\sqrt{\log n})$, so that we can sample efficiently via Theorem 2.
- $E = \sqrt{n} \cdot \|\sqrt{\Sigma}\| \leq \sqrt{n} \cdot \|g\| \cdot \delta(\sqrt{\Sigma}) \cdot \omega(\sqrt{\log n}) = O(n^{1.5+1/\kappa+\varepsilon})$: the size of the numerators of the encodings is barely worse than in the simplistic method, and significantly better than in all other methods.

Acknowledgments. The authors are grateful to Alex Davidson, Nico Döttling and Damien Stehlé for helpful discussions. The first author was supported by a Veni Innovational Research Grant from NWO under project number 639.021.645. The second author was supported by an ERC Starting Grant ERC-2013-StG-335086-LATTAC.

References

1. Albrecht, M., Bai, S., Ducas, L.: A subfield lattice attack on overstretched NTRU assumptions. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 153–178. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53018-4_6
2. Ananth, P., Sahai, A.: Projective arithmetic functional encryption and indistinguishability obfuscation from degree-5 multilinear maps. Cryptology ePrint Archive, Report 2016/1097 (2016). http://eprint.iacr.org/2016/1097
3. Barak, B., Brakerski, Z., Komargodski, I., Kothari, P.K.: Limits on low-degree pseudorandom generators (or: Sum-of-squares meets program obfuscation). Cryptology ePrint Archive, Report 2017/312 (2017). http://eprint.iacr.org/2017/312
4. Barak, B., Garg, S., Kalai, Y.T., Paneth, O., Sahai, A.: Protecting obfuscation against algebraic attacks. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 221–238. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_13
5. Barak, B., et al.: On the (Im)possibility of obfuscating programs. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 1–18. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_1
6. Biasse, J.-F., Espitau, T., Fouque, P.-A., Gélin, A., Kirchner, P.: Computing generator in cyclotomic integer rings. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10210, pp. 60–88. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56620-7_3
7. Biasse, J.-F., Song, F.: Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In: Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 893–902. Society for Industrial and Applied Mathematics (2016)
8. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13

9. Brakerski, Z., Rothblum, G.N.: Virtual black-box obfuscation for all circuits via generic graded encoding. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 1–25. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54242-8_1
10. Campbell, P., Groves, M., Shepherd, D.: Soliloquy: a cautionary tale. In: ETSI 2nd Quantum-Safe Crypto Workshop, pp. 1–9 (2014)
11. Chen, Y., Gentry, C., Halevi, S.: Cryptanalyses of candidate branching program obfuscators. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10212, pp. 278–307. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56617-7_10
12. Cheon, J.H., Jeong, J., Lee, C.: An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low level encoding of zero. LMS J. Comput. Math. **19**(A), 255–266 (2016)
13. Coron, J.-S., et al.: Zeroizing without low-level zeroes: new MMAP attacks and their limitations. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015, Part I. LNCS, vol. 9215, pp. 247–266. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_12
14. Cramer, R., Ducas, L., Peikert, C., Regev, O.: Recovering short generators of principal ideals in cyclotomic rings. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 559–585. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_20
15. Döttling, N., Garg, S., Gupta, D., Miao, P., Mukherjee, P.: Obfuscation from low noise multilinear maps. Cryptology ePrint Archive, Report 2016/599 (2016). http://eprint.iacr.org/2016/599
16. Ducas, L., Pellet-Mary, A.: On the statistical leak of the GGH13 multilinear map and some variants. Cryptology ePrint Archive, Report 2017/482 (2017). http://eprint.iacr.org/2017/482
17. Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 1–17. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_1
18. Garg, S., Miles, E., Mukherjee, P., Sahai, A., Srinivasan, A., Zhandry, M.: Secure obfuscation in a weak multilinear map model. In: Hirt, M., Smith, A. (eds.) TCC 2016, Part II. LNCS, vol. 9986, pp. 241–268. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53644-5_10
19. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Ladner, R.E., Dwork, C. (eds.) 40th Annual ACM Symposium on Theory of Computing, pp. 197–206. ACM Press, May 2008
20. Gentry, C., Szydlo, M.: Cryptanalysis of the revised NTRU signature scheme. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 299–320. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_20
21. Goldreich, O., Goldwasser, S., Halevi, S.: Public-key cryptosystems from lattice reduction problems. In: Kaliski, B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 112–131. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0052231
22. Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J.H., Whyte, W.: NTRUSign: digital signatures using the NTRU lattice. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 122–140. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36563-X_9
23. Hoffstein, J., Pipher, J., Silverman, J.H.: NSS: an NTRU lattice-based signature scheme. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 211–228. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_14

24. Hu, Y., Jia, H.: Cryptanalysis of GGH map. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016, Part I. LNCS, vol. 9665, pp. 537–565. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49890-3_21
25. Joux, A.: A one round protocol for tripartite Diffie-Hellman. In: Bosma, W. (ed.) ANTS 2000. LNCS, vol. 1838, pp. 385–393. Springer, Heidelberg (2000). https://doi.org/10.1007/10722028_23
26. Kirchner, P., Fouque, P.-A.: Revisiting lattice attacks on overstretched NTRU parameters. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10210, pp. 3–26. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56620-7_1
27. Klein, P.N.: Finding the closest lattice vector when it's unusually close. In: Shmoys, D.B. (ed.) 11th Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 937–941. ACM-SIAM, January 2000
28. Langlois, A., Stehlé, D., Steinfeld, R.: GGHLite: more efficient multilinear maps from ideal lattices. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 239–256. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_14
29. Lin, H.: Indistinguishability obfuscation from constant-degree graded encoding schemes. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9665, pp. 28–57. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49890-3_2
30. Lin, H.: Indistinguishability obfuscation from SXDH on 5-linear maps and locality-5 PRGs. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 599–629. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_20
31. Lin, H., Tessaro, S.: Indistinguishability obfuscation from bilinear maps and block-wise local PRGs. Cryptology ePrint Archive, Report 2017/250 (2017). http://eprint.iacr.org/2017/250
32. Lombardi, A., Vaikuntanathan, V.: On the non-existence of blockwise 2-local PRGs with applications to indistinguishability obfuscation. Cryptology ePrint Archive, Report 2017/301 (2017). http://eprint.iacr.org/2017/301
33. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. In: 45th Annual Symposium on Foundations of Computer Science, pp. 372–381. IEEE Computer Society Press, October 2004
34. Miles, E., Sahai, A., Zhandry, M.: Annihilation attacks for multilinear maps: cryptanalysis of indistinguishability obfuscation over GGH13. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 629–658. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_22
35. Nguyen, P.Q., Regev, O.: Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 271–288. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_17
36. Stehlé, D., Steinfeld, R.: Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices. Cryptology ePrint Archive, Report 2013/004 (2013). http://eprint.iacr.org/2013/004