# Lattice-Based Post-quantum iO from Circular Security with Random Opening Assumption

Yao-Ching Hsieh[1(✉)], Aayush Jain[2], and Huijia Lin[1]

[1] University of Washington, Seattle, USA
{ychsieh,rachel}@cs.washington.edu
[2] Carnegie Mellon University, Pittsburgh, USA
aayushja@andrew.cmu.edu

**Abstract.** Indistinguishability obfuscation (iO) stands out as a powerful cryptographic primitive but remains notoriously difficult to realize under simple-to-state, post-quantum assumptions. Recent works have proposed lattice-inspired iO constructions backed by new "LWE-with-hints" assumptions, which posit that certain distributions of LWE samples retain security despite auxiliary information. However, subsequent cryptanalysis has revealed structural vulnerabilities in these assumptions, leaving us without any post-quantum iO candidates supported by simple, unbroken assumptions.

Motivated by these proposals, we introduce the *Circular Security with Random Opening* (CRO) assumption—a new LWE-with-hint assumption that addresses structural weaknesses from prior assumptions, and based on our systematic examination, does not appear vulnerable to known cryptanalytic techniques. In CRO, the hints are random "openings" of zero-encryptions under the Gentry–Sahai–Waters (GSW) homomorphic encryption scheme. Crucially, these zero-encryptions are efficiently derived from the original LWE samples via a special, carefully designed procedure, ensuring that the openings are marginally random. Moreover, the openings do not induce any natural leakage on the LWE noises. These two features—*marginally random hints and the absence of (natural) noise leakage*—rule out important classes of attacks that had undermined all previous LWE-with-hint assumptions for iO. Therefore, our new lattice-based assumption for iO provides a qualitatively different target for cryptanalysis compared to existing assumptions.

To build iO under this less-structured CRO assumption, we develop several new technical ideas. In particular, we devise an *oblivious LWE sampling* procedure, which succinctly encodes random LWE secrets and smudging noises, and uses a tailored-made homomorphic evaluation procedure to generate secure LWE samples. Crucially, all non-LWE components in this sampler, including the secrets and noises of the generated samples, are independently and randomly distributed, avoiding attacks on non-LWE components.


Y. Tauman Kalai and S. F. Kamara (Eds.): CRYPTO 2025, LNCS 16006, pp. 3–38, 2025.
https://doi.org/10.1007/978-3-032-01907-3_1

# 1 Introduction

Indistinguishability obfuscation ($\mathsf{iO}$) for general polynomial-size circuits [10, 33, 42] requires that for any two circuits $\mathsf{C}_0$ and $\mathsf{C}_1$ of the same size and functionality—meaning $\mathsf{C}_0(x) = \mathsf{C}_1(x)$ for all inputs $x$—the obfuscated circuits $\mathsf{iO}(\mathsf{C}_0)$ and $\mathsf{iO}(\mathsf{C}_1)$ should be computationally indistinguishable. Moreover, the obfuscator $\mathsf{iO}$ must run in probabilistic polynomial time and output a circuit $\mathsf{C}'$ that preserves functionality with probability 1, i.e., $\mathsf{C}'(x) = \mathsf{C}(x)$ for all $x$.

Since its inception, $\mathsf{iO}$ has been a powerful cryptographic primitive, enabling a broad range of applications in cryptography and complexity theory (see, e.g., [13, 22, 26, 33, 34, 41, 46, 47, 55, 67]). However, constructing secure $\mathsf{iO}$ has remained a significant challenge. Following the first heuristic candidate [33], a long line of work [1, 3, 5–9, 12, 14, 17, 18, 24, 25, 27–29, 31–33, 35, 38, 39, 45, 50, 52, 56–58, 60, 61, 63–65] explored a diverse range of hardness assumptions, including multilinear maps, affine determinant programs, and block-local PRGs, before culminating in the first provably secure $\mathsf{iO}$ construction [53], based on four well-studied assumptions. This was later improved to rely on three assumptions [54, 66], namely, the Decisional Linear (DLin) assumption on symmetric bilinear maps, Learning Parity with Noise (LPN) over large fields, and constant-local PRGs or sparse LPN.

Despite these advancements, a grand challenge remains: constructing $\mathsf{iO}$ that is secure against quantum adversaries. Current state-of-the-art constructions [53, 54, 66] rely on bilinear maps, leaving them susceptible to quantum attacks. While some alternative approaches—such as those based on multilinear maps, or affine determinant programs, or random local mixing [23]—currently face no known quantum attacks, their security is not well understood, lacking reductions to simple-to-state hardness assumptions. This gap risks relying on "security by obscurity", limiting confidence in their approach. Besides post-quantum security, another important challenge is basing $\mathsf{iO}$ on simple-to-state hard problems w.r.t. a *single* mathematical structure, rather than *three* as the current state-of-the-art constructions do.

For both challenges, the ultimate long-term objective is to construct $\mathsf{iO}$ from a standard post-quantum assumption like Learning with Errors (LWE). However, our current understanding remains far from this goal. This raises the following natural and compelling question as an intermediate milestone toward that ultimate goal:

*Can we build post-quantum* $\mathsf{iO}$ *from a simple-to-state, principled, assumption?*

**Recent Attempts.** A recent exciting body of works have proposed lattice-inspired $\mathsf{iO}$ candidates [15, 16, 30, 36, 71], some of which are based on new, simple-to-state lattice assumptions. This includes the Circular Shielded Randomness Security (circ-SRL) assumption by [16, 36], the Homomorphic Pseudorandom LWE Samples (HPLS) conjecture by [71], and the Subspace Flooding assumption by [30]. In addition, two very recent works [2, 20] constructed $\mathsf{iO}$ for pseudorandom functionalities–termed Pseudorandom Obfuscation ($\mathsf{PrO}$)–where the

outputs of the circuits are pseudorandom, based on variants of private-coin evasive LWE assumptions, first introduced by [68–70] in the context of building attribute-based encryption and witness encryption.

Despite their differences, all these assumptions share a common structure:

> **LWE-with-hints assumptions** *posit that certain (circular) LWE samples retain some security (indistinguishability or pseudorandomness) even in the presence of specific* hints *that leak information about these samples.*

The presence of hints in these assumptions is crucial for achieving the functionality of iO, which requires revealing the outputs of the circuit evaluated on arbitrarily chosen inputs in the clear. Typically, these hints allow opening the output encoding derived via homomorphic evaluation from the original LWE samples. Then iO security requires the LWE samples to retain some security in the presence of hints, in order to argue that no information of the original circuit is revealed beyond the outputs. However, the hints introduce a delicate trade-off: do they leak too much information, possibly completely compromising LWE security? Prior works conjectured that the worst case does not happen.

Unfortunately, subsequent cryptanalysis [20,48,51] has demonstrated counterexamples or attacks against all aforementioned LWE-with-hint assumptions, leaving us without any iO constructions proven secure under simple, plausibly post-quantum assumptions.

**Our Contributions.** In this work, we show that even for the weaker notion of pseudorandom obfuscation, there are counterexamples to the private-coin evasive LWE assumptions underlying the recent constructions [2,20].

Moving beyond the attacks, we present a new iO construction based on a new, simple-to-state, post-quantum assumption, that we call the **Circular security with Random Opening (CRO) assumption**. CRO also has the LWE-with-hint format, and is falsifiable, instance-independent, and fully specified. Importantly, CRO avoids the structural vulnerabilities in prior assumptions that has been exploited in attacks, circumventing direct application of known attack strategies.

At a very high level, the CRO assumption considers real distributions consisting of circular LWE samples, denoted as encodings, together with hints $\mathbf{R}^*$ that are random "openings" of certain ciphertexts $\mathbf{C}^*$ of zeros under the Gentry-Sahai-Waters (GSW) homomorphic encryption scheme [40]. The opened zero-ciphertext $\mathbf{C}^*$ can be efficiently derived from the LWE samples, using a carefully crafted procedure $F$, and the opening satisfies the constraint that $\mathbf{C}^* = F(\mathsf{encodings}) = \mathsf{GSW.Enc}(\mathsf{GSW.hpk}, 0; \mathbf{R}^*)$, where the public key GSW.hpk is contained in encodings. The assumption postulates that the real distributions are indistinguishable to ideal distributions where the LWE samples are replaced with *random* samples, while the hints are sampled from a simulated distribution still satisfying the constraint.

We perform a systematic study of prior attack strategies, revealing that all prior LWE-with-hints assumptions suffer from *structural vulnerabilities* either

in their hints or in the leakage of LWE noises induced by the hint. Except for contrived counterexamples, all known attacks exploit these vulnerabilities by focusing solely on the hints or noise leakage, and are oblivious of the LWE samples otherwise. See Table 1 for a summary of the structural vulnerabilities in prior assumptions. We show that our CRO assumption introduces key structural differences, as highlighted below, that circumvent direct application of prior attacks.

1. *(Pseudo)Random Hints:* The *hints* in CRO are marginally random in the real distributions and pseudorandom in the ideal distributions, ensuring that the hints alone do not have any structural vulnerabilities.
2. *No Natural Noise Leakage:* Since our hints are "opening" of zero-ciphertexts that can be efficiently derived from the LWE samples available in the real distribution, it does not induce any natural noise leakage, circumventing zeroizing attacks. (See more discussion shortly below.)
3. *Pseudorandomness of LWE Samples Given Hints:* Different from prior LWE-with-hint assumptions underlying iO [16,30,36,71] which all postulate the indistinguishability security of LWE samples at the presence of hints, and *lack* natural pseudorandom variants of their assumptions, CRO gives a way to reason about the pseudorandomness of LWE samples, given hints that enable non-evasive and non-pseudorandom functionalities.
   We further formulate a weaker, but still sufficient, indistinguishability version, shorthanded as IND-CRO. We believe that the plausible pseudorandomness version, vetted against known cryptanalytic techniques, adds confidence to the security of CRO and IND-CRO.

In short, comparing with prior LWE-with-hint assumptions, CRO exhibits fewer structural vulnerabilities. As discussed in cryptanalysis in Sect. 2.3, the above features enable circumventing previous attack avenues in a principled way.

In order to base security on the less structured CRO assumption, our new iO construction develops several new ideas, building upon prior techniques especially [16,36]. We believe that these ideas might be instrumental for future constructions of iO and other advanced primitives.

Next, we describe the CRO assumption in more detail and provide a high-level overview of our construction. The formal definition and cryptanalysis of CRO are given in Sect. 2, while a detailed construction overview appears in Sect. 3.

## 1.1 Our Construction and Assumption in a Nutshell

It is well known that to construct iO, it suffices to build exponentially efficient iO, or xiO [59], assuming LWE. xiO is the simpler task of obfuscating circuits $\Pi$ that have polynomial-size truth tables TT. The obfuscator is allowed to run in time polynomial in the size of the entire truth table, with the only constraint that the resulting obfuscated circuit remains succinct – sublinear in the size of TT[1].

[1] Otherwise, a trivial construction would be to simply output the truth table as the obfuscated circuit.

The work of [15], followed by [16,30,36,71], proposed an appealing approach towards constructing xiO. The key idea is that, assuming (circular) LWE assumptions, one can hide a secret circuit $\Pi$ in a homomorphic encoding $\mathsf{HEnc}(\Pi)$, from which an encoded truth table $\mathsf{Enc}(\mathrm{TT})$ can be efficiently computed (possibly under a slightly different encoding). The core challenge in achieving xiO is devising a way to safely and succinctly "open" $\mathsf{Enc}(\mathrm{TT})$, revealing TT and hopefully nothing else. The overall paradigm is depicted below.

$$\left.\begin{array}{c}\mathsf{HEnc}_{\mathbf{s}}\left(\Pi \mid\mid f^{\mathrm{circ}}(\mathbf{s}) \mid\mid \cdots\right) \overset{\mathrm{HEval}}{\Longrightarrow} \mathsf{Enc}(\mathrm{TT}) \\ \text{succinct opening } \mathsf{open}\end{array}\right\} \Longrightarrow (\mathrm{TT}, \mathsf{leak})$$

We note that typically in these constructions, besides the original circuit $\Pi$, the homomorphic encoding also hides circular secret-dependent messages $f^{\mathrm{circ}}(\mathbf{s})$ to facilitate the final opening[2].

Prior works developed different encoding and succinct opening methods, and captured security of their scheme via different LWE-with-hint assumptions. Naturally, the LWE samples in the assumptions facilitate the homomorphic encoding $\mathsf{HEnc}(\Pi)$, while the hint $\mathsf{hint}$ facilitates opening $\mathsf{open}$. Inevitably, the final encoding $\mathsf{Enc}(\mathrm{TT})$ also consists of LWE samples (derived via homomorphic evaluation), and opening them reveals not only TT but also additional leakage $\mathsf{leak}$ of the LWE noises, as indicated in the paradigm above.

**Table 1.** Characterization for different information leakage beyond LWE samples for existing assumptions toward iO/PrO. In the table, ✗ stands for no such leakage exist, $ stands for the leakage is marginally random (from a well-defined distribution), *Attack* stands for that there exist adversary breaking the assumption by focusing on the leakage, and *Counterexample* stands for that there exist specific implementation for the assumption which can be broken by focusing on the leakage.

| Assumption | $\mathsf{hint}$ = LWE secret | LWE noise leakage | $\mathsf{hint}$ = GSW randomness | $\mathsf{hint}$ = Lattice trapdoor |
|---|---|---|---|---|
| circ-SRL ([36]) | ✗ | ✗ | Counterexample ([48]) | ✗ |
| HPLS ([71]) | Non-random | Counterexample ([48]) | ✗ | ✗ |
| Subspace Flooding ([30]) | Attack ([51]) | Non-random | ✗ | ✗ |
| Private-coin ELWE ([68,69]) | ✗ | Counterexample (This Work [49]) | ✗ | Non-random |
| CRO (Ours) | ✗ | ✗ | $ | ✗ |

[2] Sometimes more than one LWE secrets are involved and the key-dependent messages may depend on multiple secrets.

A key issue in prior LWE-with-hint assumptions is that the hints and/or the noise leakage exhibit structural vulnerabilities, which have been exploited in attacks. Notably, prior cryptanalysis efforts focused entirely on hints and leakage, without attacking the LWE samples directly. Specifically, as summarized in Table 1, [48] attacked the hints in the circ-SRL security assumption of [36], and the leakage in the HPLS conjecture [71]. Similarly, [51] attacked the hints in the subspace flooding assumption of [30]. Finally, in the full version of this work [49], we give attacks targeting leakage in private-coin evasive LWE assumptions underlying pseudorandom obfuscation [2,20].

**Our Assumption** CRO**:** Formally described in Fig. 3, our CRO assumption postulates that a real distribution of circular LWE samples with hints is indistinguishable to an ideal distribution consisting of random samples and simulated hints. In the real distribution the circular LWE samples contain a Gentry-Sahai-Waters (GSW) public key $\mathsf{GSW.hpk}$, GSW ciphertexts $\mathsf{GSW.hct}$, and other LWE samples $\mathbf{C}$, where the latter two hide secret-dependent messages. Their distribution is set up in such a way that, using a *special and carefully designed procedure* $F$, one can efficiently derive certain specific GSW ciphertexts of zeros, $\mathbf{C}^* = F(\mathsf{GSW.hpk}, \mathsf{GSW.hct}, \mathbf{C})$.

The key idea in CRO is that the hints are *random openings* $\mathbf{R}^*$ of $\mathbf{C}^*$. An opening of $\mathbf{C}^*$ is a random string $\mathbf{R}$ satisfying $\mathbf{C}^* = \mathsf{GSW.Enc}(\mathsf{GSW.hpk}, \mathbf{0}\,;\,\mathbf{R})$, which corresponds to a small-norm matrix in GSW. Then, a random opening $\mathbf{R}^*$ is sampled as a random small-norm Gaussian matrix satisfying the same constraint, that is, $\mathbf{R}^* \leftarrow \mathcal{D}|_{\mathbf{C}^* = \mathsf{GSW.Enc}(\mathsf{GSW.hpk}, 0\,;\,\mathbf{R}^*)}$, where $\mathcal{D}$ is the distribution of random Gaussian matrix of appropriate dimension and Gaussian width.

The CRO assumption postulates that the real distribution of LWE encodings and opening $\mathbf{R}^*$, is indistinguishable to random encodings, and an equivocated opening $\hat{\mathbf{R}}^*$.

$$\overbrace{\left(\mathsf{encodings} = (\mathsf{GSW.hpk}, \mathsf{GSW.hct}, \mathbf{C}),\ \mathbf{R}^*\right)}^{\text{Real}} \approx \overbrace{\left(\mathsf{encodings} = (\$, \$, \$),\ \mathbf{R}^*\right)}^{\text{Ideal}},$$

In the ideal distribution, $\mathbf{C}^* = F(\mathsf{encodings})$ is computed in the same way using procedure $F$ but evaluated on random encodings. $\mathbf{R}^*$ is also sampled in the same way w.r.t. $\mathbf{C}^*$, that is random small Gaussian matrix subject to constraint $\mathbf{C}^* = \mathsf{GSW.Enc}(\mathsf{GSW.hpk}, 0\,;\,\mathbf{R}^*)$. $\mathbf{R}^*$ is well-defined, corresponding to a "random opening" of $\mathbf{C}^*$ relative to a truly random "public key", owning to the equivocal properties of GSW when the public key is random.

**Key Features of the** CRO **Assumption:**

– *(Pseudo)random hints:* We prove that in the real distribution, $\mathbf{C}^*$ is, marginally, *a random GSW ciphertext of zeros*, and hence its random opening is, marginally, a truly random small-norm Gaussian matrix. In the ideal distribution, we show that $\mathbf{R}^*$ is pseudorandom. Therefore, no attacks focusing on hints alone can succeed. The (pseudo)randomness of $\mathbf{R}^*$ stems from the carefully designed distribution of LWE encodings and the procedure $F$ for evaluating $\mathbf{C}^*$ from them.

This stands in contrast to the structured hints in the circ-SRL assumption [36] and the subspace flooding assumption [30], which led to attacks [48, 51].

– *No natural noise leakage:* The GSW public key and ciphertext have the form $\bar{\mathbf{B}}^T = (\mathbf{B}^T, \mathbf{B}^T\mathbf{r} + \mathbf{e})$ and $(\mathbf{C}^*)^T = (\mathbf{P}^T, \mathbf{P}^T\mathbf{r} + \mathbf{e}^*)$, and a random opening $\mathbf{R}^*$ satisfies $\bar{\mathbf{B}} \cdot \mathbf{R}^* = \mathbf{C}^*$. $\mathbf{R}^*$ may appear similar to a lattice trapdoor $\mathbf{R} \leftarrow \mathbf{B}^{-1}(\mathbf{P})$, satisfying $\mathbf{B} \cdot \mathbf{R} = \mathbf{P}$ [62], but there is a crucial distinction. A trapdoor $\mathbf{R} \leftarrow \mathbf{B}^{-1}(\mathbf{P})$ yields an approximate equality $\bar{\mathbf{B}}\mathbf{R} \approx \mathbf{C}^*$ and thus leaks LWE noises $\mathbf{e}^* - \mathbf{e}\mathbf{R}$, whereas an opening $\mathbf{R}^*$ yields an exact equality $\bar{\mathbf{B}}\mathbf{R}^* = \mathbf{C}^*$, leaking no information about LWE noises.

This distinguishes CRO from evasive LWE-type assumptions where the hints are lattice trapdoors. It also rules out attacks that only combine encodings and hint in the most natural way – multiplying $\overline{\mathbf{B}}$ and $\mathbf{R}^*$ yields $\mathbf{C}^* = \overline{\mathbf{B}}\mathbf{R}^*$ which can already be efficiently computed from the original LWE encodings in the assumption, giving no additional information.

In contrast, in the full version of this paper [49] we describe new attacks on private-coin evasive LWE assumptions underlying recent construction of pseudorandom obfuscation [2,20]. Unlike prior attacks on private-coin evasive LWE [21,69], our attack exploits structure in the noise leakage obtained after computing $\bar{\mathbf{B}} \cdot \mathbf{R}$. Hence, our attack is similar in principle to previous zeroizing attacks (e.g., [33]), and falsifies prior intuition that evasive LWE assumptions are not subject to zeroizing attacks.

The attacks of [48] on the HPLS conjecture [71] also focus on noise leakage only, though their hints are different, and are functions of the LWE secrets.

– *Pseudorandom vs Indistinguishability Assumptions:* The distribution of encodings in CRO follow the same principle behind circular-security of LWE and key-dependent-message security of GSW. Therefore, attacks on the encodings *alone* would undermine widely adopted circular security assumptions (e.g., [19,40]). When combined with the opening $\mathbf{R}^*$, there is an efficiently verifiable constraint $\mathbf{C}^* = F(\mathsf{encodings}) = \mathsf{GSW.Enc}(\mathsf{GSW.hpk}, 0\,;\, \mathbf{R}^*)$. CRO gives a new way to reason about the pseudorandomness of the LWE encodings at the presence of hint, stating that the real LWE encodings can be switched to random in an indistinguishable way, if $\mathbf{R}^*$ is simultaneously equivocated to maintain the constraint.

As discussed before, prior LWE-with-hint assumptions underlying iO [16, 30,36,71] postulate only indistinguishability security[3]. At first glance, indistinguishability may appear weaker and more preferable. The subtle issue, however, is that these assumptions *do not have* a natural stronger pseudorandom variant. In our view, the lack of a pseudorandom variant is precarious: *can LWE samples that lack pseudorandomness still retain any security*? This seems to be at odds with the common intuition that security of LWE-based schemes typically relies on pseudorandomness.

Therefore, we view the plausible pseudorandomness of CRO, vetted against

[3] Private-coin evasive LWE assumptions are pseudorandomness type assumptions. However, they only enable pseudorandom functionalities.

known cryptanalytic techniques, as a strength of the assumption. At the same time we formulate a weaker (but sufficient) indistinguishability-based variant IND-CRO (described formally in the full version [49]).

– *Remaining Challenge in Cryptanalysis:* The above three features entail that attacks on CRO must combine encodings and hint in ways more sophisticated than simply computing $\bar{\mathbf{B}} \cdot \mathbf{R}^*$. However, to the best of our knowledge, it is unclear how to extend current cryptanalytic techniques (e.g., lattice attacks) to leverage $\mathbf{R}^*$ in a non-trivial way. In the literature, such behavior has only arisen in contrived counterexamples – for instance, in prior cryptanalysis of private-coin evasive LWE [21,69], the attacker receives auxiliary information (an obfuscated circuit) that helps leverage the trapdoors. By contrast, CRO does not provide auxiliary information and instead features a natural distribution of encodings and hint.

**Highlights of Our Construction** In order to base security on CRO, our construction of xiO, building upon [16,36], carefully combines several new ideas. The main component is *oblivious LWE sampling*, whose goal is to generate LWE samples $\tilde{\mathbf{s}}\mathbf{A} + \tilde{\mathbf{e}}$, where $\tilde{\mathbf{s}} \in \mathbb{Z}_q^n$ and $\mathbf{A} \in \mathbb{Z}_q^{n \times \ell}$, from a *succinct* encoding that is much shorter than the bit length $\ell \log q$ of generated samples. Crucially, the security guarantee is that the secrets $\tilde{\mathbf{s}}$ and $\tilde{\mathbf{e}}$ remain pseudorandom and can be used to re-randomize other LWE samples. Let us briefly highlight some key ideas in our construction; we refer the reader to Sect. 3 for a detailed overview of how these ideas are implemented.

(1) We introduce new ways of encoding random LWE secrets $\mathbf{s}$ and smudging noises $\mathbf{e}$ inside the oblivious LWE sampler or xiO encoding. Specifically, the encoding contains GSW ciphertexts of $\mathbf{s}$, along with LWE samples using noises $\mathbf{e}$ modulo a *small* modulus $\Delta \ll q$. This encoding differs from prior approaches, which either store $\mathbf{s}$ and $\mathbf{e}$ in the CRS, derive them from a PRF, or expand them from $\mathbf{sB} + \mathbf{e}$ and a trapdoor $\mathbf{B}^{-1}(\mathbf{P})$.

(2) We design a carefully crafted homomorphic evaluation procedure to derive a GSW ciphertext $\mathsf{hct}'$ encrypting $(\mathbf{sA} + \mathbf{e}) \bmod q$. This special procedure is crucial to ensure that the $\mathsf{hint} = \mathbf{R}^*$ in CRO has a random marginal distribution in the real distribution and pseudorandom in the ideal distribution, thereby avoiding certain attacks. In contrast, prior constructions rely on generic homomorphic evaluation procedure, which ended up leading to counterexamples [48].

(3) Next, the GSW ciphertext $\mathsf{hct}'$ of $(\mathbf{sA} + \mathbf{e}) \bmod q$ is homomorphically decrypted using the dual GSW scheme (a.k.a. the packed dual-Regev encryption), producing the final samples $\tilde{\mathbf{s}}\mathbf{A} + \tilde{\mathbf{e}}$. Owing to (1) and (2), we can show that $\tilde{\mathbf{s}}$ and $\tilde{\mathbf{e}}$ are both *truly random* in their marginal joint distribution. This allows the security reduction to CRO to internally emulate $\tilde{\mathbf{s}}$ and $\tilde{\mathbf{e}}$ by sampling them randomly. As a result, the CRO assumption itself only contains an opening $\mathbf{R}^*$ and does not incur natural noise leakage.

(4) Finally, it is essential to *rerandomize* the GSW ciphertext $\mathsf{hct}'$ before performing homomorphic decryption. We achieve this using public randomness

$\mathbf{R}^*$ in the CRS by setting $\mathsf{hct}' = \mathsf{hct}' + \bar{\mathbf{B}}\mathbf{R}^*$, following the approach of [36]. Rerandomization is key to achieving *simulation-based* security for oblivious LWE sampler and xiO (instead of mere indistinguishability). Indeed, the simulator can "program" the truth table TT into $\mathbf{R}^*$ in the CRS.

Recall that CRO conjectures the *pseudorandomness* of the LWE samples when the hint is simultaneously equivocated. Intuitively, (as typically is the case when using pseudorandom assumptions) to maintain the correctness of the oblivious LWE sampler/xiO when the LWE samples switch to random, we need to "program" the outputs (fresh LWE samples or TT) into the CRS. The stronger simulation security of xiO is interesting on its own.

# 2 Circular Security with Random Opening (CRO)

## 2.1 Preliminaries

We define our abstraction of GSW FHE scheme, which hides most details of the construction and highlights the properties that are crucial for understanding the assumption structure. Note that GSW supports evaluating mixed circuits $f : \{0,1\}^k \to \mathbb{Z}_q^\ell$ which first computes the bitwise representation of the output and then packs the bits into $\mathbb{Z}_q$ elements. We therefore consider function class $\mathcal{F}$ mapping to $\mathbb{Z}_q$ vectors and define approximate correctness for decryption.

**Definition 2.1 (Homomorphic Encryption.).** *Let $n$ be a positive integer, and all other parameters are implicitly dependent on $n$. A homomorphic encryption scheme with message space $\mathcal{M}$, key space $\mathcal{K}$, and encryption space $\mathcal{C}$, supporting function class $\mathcal{F}$ mapping vectors over $\mathcal{M}$ to vectors over a ring $\mathcal{R}$ that is contained in $\mathcal{M}$, consists of the following algorithms:*

- $\mathsf{PKGen}(\mathbf{r})$ *takes as input a randomly sampled secret key $\mathbf{r} \leftarrow \mathbb{Z}_q^n$ and outputs a public key $\mathsf{hpk} \in \mathcal{K}$.*
- $\mathsf{Enc}(\mathsf{hpk}, \mathbf{m}; \mathbf{R})$ *takes as input a public key $\mathsf{hpk}$, a message $\mathbf{m} \in \mathcal{M}^k$ for some dimension $k$, and encryption randomness $R \leftarrow \mathcal{D}_{\mathrm{enc}}^k$ sampled according to $\mathcal{D}_{\mathrm{enc}}$, outputs a ciphertext $\mathsf{hct}$ which is a vector over $\mathcal{C}^k$. (Sometimes the notation $\mathsf{hct}(\mathbf{m})$ is used in order to explicitly indicate the encrypted message.)*
- $\mathsf{Eval}(\mathsf{hct}(\mathbf{m}), f)$ *takes as input a ciphertext $\mathsf{hct}(\mathbf{m})$, a circuit $f \in \mathcal{F}$, and outputs a ciphertext $\mathsf{hct}_f$ of the output $f(\mathbf{m})$.*
- $\mathsf{Dec}(\mathsf{hsk}, \mathsf{hct})$ *takes as input a secret key $\mathsf{hsk}$ and a ciphertext $\mathsf{hct}$, and outputs a message $\mathbf{m} \in \mathcal{M}^k \cup \{\perp\}$.*

*We require a homomorphic encryption scheme to be correct and secure as defined below.*

**$\alpha(n)$-Approximate Decryption Correctness:** *For every $k \in \mathbb{Z}$, message $m \in \mathcal{M}^k$, and function $f \in \mathcal{F}$ taking inputs of $k$ elements, the output cipher-*

*text of the homomorphic encryption decrypts to some message that is $\alpha(n)$-close to the correct evaluation outcome $f(\mathbf{m})$ under the Euclidean norm.*

$$\Pr\left[\|\mathsf{Dec}(\mathsf{hsk},\mathsf{hct}_f) - f(\mathbf{m})\| \le \alpha(n) \;\middle|\; \begin{array}{r} \mathbf{r} \leftarrow \mathbb{Z}_q^n \\ \mathsf{hpk} \leftarrow \mathsf{PKGen}(\mathbf{r}) \\ \mathbf{R} \leftarrow \mathcal{D}_{\mathrm{enc}}^k \\ \mathsf{hct} = \mathsf{Enc}(\mathsf{hpk},\mathbf{m};\mathbf{R}) \\ \mathsf{hct}_f = \mathsf{Eval}(\mathsf{hct},f) \end{array}\right] = 1$$

**$\epsilon(n)$-Pseudorandom Public Key and Ciphertext:** *For every polynomial $k = k(n)$, every ensemble of messages $\{\mathbf{m} \in \mathcal{M}^k\}_n$, the following ensembles are $\epsilon(n)$-indistinguishable to all polynomial-sized adversaries:*

$$\left\{(\mathsf{hpk},\mathsf{hct}) \;\middle|\; \begin{array}{r} \mathbf{r} \leftarrow \mathbb{Z}_q^n \\ \mathsf{hpk} \leftarrow \mathsf{PKGen}(\mathbf{r}) \\ \mathbf{R} \leftarrow \mathcal{D}_{\mathrm{enc}}^k \\ \mathsf{hct} = \mathsf{Enc}(\mathsf{hpk},\mathbf{m};\mathbf{R}) \end{array}\right\}_n \approx_c^{\epsilon} \left\{(\mathsf{hpk},\mathsf{hct}) \;\middle|\; \begin{array}{r} \mathsf{hpk} \leftarrow \mathcal{K} \\ \mathsf{hct} \leftarrow \mathcal{C}^k \end{array}\right\}_n$$

We also formulate the following additional properties, which are satisfied by the GSW scheme.

**Definition 2.2.** *A homomorphic encryption scheme is statistically $(\mathcal{D}_{\mathrm{rand}}, \epsilon(n))$* **-rerandomizable**, *if for every polynomial $k = k(n)$, polynomial $\ell = \ell(n)$, ensemble of function-message pairs $\{\mathbf{m} \in \mathcal{M}^k, f \in \mathcal{F}_{k,\ell}\}_n$, where $\mathcal{F}_{k,\ell}$ is the subset of function class $\mathcal{F}$ that maps $\mathcal{M}^k$ to $\mathcal{R}^\ell$, it holds that for sufficiently large $n \in \mathbb{Z}$,*

$$\Pr\left[\mathsf{SD}\left(\begin{array}{r}\left(\mathsf{hct}_f \boxplus (-f(\mathbf{m})) \boxplus \mathsf{Enc}(\mathsf{hpk},\mathbf{0}^\ell;\mathcal{D}_{\mathrm{rand}})\right), \\ \left(\mathsf{Enc}(\mathsf{hpk},\mathbf{0}^\ell;\mathcal{D}_{\mathrm{rand}})\right)\end{array}\right) \le \epsilon(n) \;\middle|\; \begin{array}{r} \mathbf{r} \leftarrow \mathbb{Z}_q^n \\ \mathsf{hpk} \leftarrow \mathsf{PKGen}(\mathbf{r}) \\ \mathbf{R} \leftarrow \mathcal{D}_{\mathrm{enc}}^k \\ \mathsf{hct} = \mathsf{Enc}(\mathsf{hpk},\mathbf{m};\mathbf{R}) \\ \mathsf{hct}_f = \mathsf{Eval}(\mathsf{hct},f) \end{array}\right] = 1$$

*where $\mathbf{0}$ denotes the zero element in ring $\mathcal{R}$, and $\boxplus$ is the homomorphic addition operation over two ciphertexts or over a ciphertext and a constant, implicitly defined by* Eval*, and* $\mathsf{SD}(A,B)$ *denotes the statistical distance between two distributions.*

**Definition 2.3.** *A homomorphic encryption scheme has $\epsilon(n)$-***equivocal mode** *if there are two additional algorithms:*

- $\mathsf{TDGen}(1^n, q)$ *samples a public key* hpk *together with a trapdoor* $\mathbf{T}$.
- $\mathsf{TDSamp}(\mathsf{hpk},\mathbf{T},\mathsf{hct})$ *on input a public key* hpk *with a trapdoor* $\mathbf{T}$*, and a target ciphertext* $\mathsf{hct} \in \mathcal{C}^\ell$*, samples a matching encryption randomness* $\mathbf{R}$ *satisfying* $\mathsf{Enc}(\mathsf{hpk},\mathbf{0}^\ell\ ;\ \mathbf{R}) = \mathsf{hct}$.

*These two algorithms satisfy the following two statistical properties:*

$$\left\{\ \mathsf{hpk} \;\middle|\; \begin{array}{r}\mathbf{r} \leftarrow \mathbb{Z}_q^n \\ \mathsf{hpk} \leftarrow \mathsf{PKGen}(\mathbf{r})\end{array}\right\}_n \approx_s^{\epsilon} \left\{\ \mathsf{hpk} \;\middle|\; (\mathsf{hpk},\mathbf{T}) \leftarrow \mathsf{TDGen}(1^n,q)\ \right\}_n$$

*For every polynomial $\ell = \ell(n)$, every ensemble of ciphertexts $\{\mathsf{hct} \in \mathcal{C}^\ell\}_n$,*

$$\begin{aligned}&\left\{\ (\mathsf{hpk},\mathbf{R}^*)\ \middle|\ (\mathsf{hpk},\mathbf{T}) \leftarrow \mathsf{TDGen}(1^n,q), \mathbf{R}^* \leftarrow \mathcal{D}_{\mathrm{rand}}\big|_{\mathsf{Enc}(\mathsf{hpk},\mathbf{0}^\ell;\mathbf{R}^*)=\mathsf{hct}}\right\}_n \\ \approx_s^{\epsilon} &\left\{\ (\mathsf{hpk},\mathbf{R}^*)\ \middle|\ (\mathsf{hpk},\mathbf{T}) \leftarrow \mathsf{TDGen}(1^n,q), \mathbf{R}^* \leftarrow \mathsf{TDSamp}(\mathsf{hpk},\mathbf{T},\mathsf{hct})\right\}_n\end{aligned}$$

## 2.2 Assumption Formulation

In this section, we present our assumption. In order to ease the exposition and build intuition towards our assumption, we introduce it in two stages. Each stage will be associated with a key concept central to our assumption.

### Building Intuition via Abstract Formulation

We will first describe our assumption in two stages, in an abstract way w.r.t. a homomorphic encryption scheme according to Definition 2.1. We believe the abstract versions better convey the rationale (without the burden of concrete algebra). We emphasize that the abstract versions are only for exposition, our actual assumption is w.r.t. the concrete GSW HE scheme [40].

**Stage 1: Circular Security.** Our first stage is simply a variant of well-studied circular security of the Homomorphic Encryption (HE) scheme in the context of Bootstrapping [37]. The assumption $f^{\text{circ}}$-circular security is described in Fig. 1. The assumption posits indistinguishability between a real and an ideal distribution. Let $\mathbb{Z}_q$ be the ambient space of the HE ciphertexts and the LWE samples, and $n$ the dimension of HE secret keys and LWE secret vectors. In the real distribution, we have two main components. The first component consists of an honestly homomorphic encryption public key $\mathsf{hpk}$ generated using secret key $\mathbf{r} \in \mathbb{Z}_q^n$, a circularly encrypted ciphertext $\mathsf{hct}$ encrypting the secret key $\mathbf{r}$ and a fresh encryption $\mathsf{hct}_0$ of zeros. The second component simply consists of LWE samples with respect to random matrices $\mathbf{A}$ and $\mathbf{D}$ encoding secret related terms. The first LWE sample $\mathsf{ct}_1$ with respect to $\mathbf{A}$ uses independent secret $\mathbf{U}$ and encodes a matrix $\mathbf{I}_\ell \otimes \mathbf{G}_n^\intercal \mathbf{r}$ that depends on $\mathbf{r}$, where $n$ is the dimension of the secret key $\mathbf{r}$ and $\ell$ is an integer parameter polynomial in $n$ and should be thought of as much larger than $n$. The second sample $\mathsf{ct}_2$ with respect to $\mathbf{D}$ uses $\mathbf{r}$ as the secret vector and encodes a $\mathbb{Z}_q$-vector-valued function $f^{\text{circ}}$ on $\mathbf{U}$ and $\mathsf{hct}_0$. The distribution outputs $(\mathsf{hpk}, \mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_1, \mathsf{ct}_2)$.

The ideal distribution is exactly the same except that all the components are now replaced with randomly chosen vectors of appropriate size over $\mathbb{Z}_q$.

We note that by inspection, only looking at the HE component corresponds to the standard circular security assumption used for bootstrapping GSW homomorphic encryption. Similarly, examining the LWE components independently (ignoring the dependence on the public ciphertext $\mathsf{hct}_0$ for the time-being) is close to the standard 2-circular security assumption. Our assumption posits indistinguishability of these two components together. We discuss cryptanalysis of this shortly in Sect. 2.3.

**Stage 2: Security with Re-randomized Opening.** As such, the first assumption is not useful for $\mathsf{iO}$ because one can never use these circularly encrypted ciphertexts to learn outputs securely in the clear. Our next assumption modifies the circular security assumption in a way that allows us to securely learn the outputs.

**$f^{\text{circ}}$-circular security**

| $\mathcal{D}_0$: **Real distribution** | $\mathcal{D}_1$: **Ideal distribution** |
|---|---|
| **HE Components:**<br>– Secret key $\mathbf{r} \leftarrow \mathbb{Z}_q^n$<br>– Public key $\mathsf{hpk} \leftarrow \mathsf{KeyGen}(\mathbf{r})$<br>– Ciphertext $\mathsf{hct} \leftarrow \mathsf{HE.Enc}(\mathsf{hpk}, \mathbf{r}; \mathcal{D}_{\text{enc}})$<br>– Mask $\mathsf{hct}_0 \leftarrow \mathsf{HE.Enc}(\mathsf{hpk}, \mathbf{0}^{M'}; \mathcal{D}_{\text{rand}})$ | **HE Components:**<br>– Public key $\mathsf{hpk} \leftarrow \$$<br>– Ciphertext $\mathsf{hct} \leftarrow \$$<br>– Mask $\mathsf{hct}_0 \leftarrow \$$ |
| **LWE Components:**<br>– Public matrices $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times\ell}, \mathbf{D} \leftarrow \mathbb{Z}_q^{n\times M}$<br>– $\mathsf{ct}_1 \leftarrow \underbrace{\mathbf{U}^\intercal\mathbf{A} + \mathbf{I}_\ell \otimes \mathbf{G}_n^\intercal\mathbf{r}}$, where $\mathbf{U} \leftarrow \mathbb{Z}_q^{n\times\ell\lceil\log q\rceil}$<br>– $\mathsf{ct}_2 \leftarrow \underbrace{\mathbf{r}^\intercal\mathbf{D} + f^{\text{circ}}(\mathbf{U}, \mathsf{hct}_0)}$ | **LWE Components:**<br>– Public matrices $\mathbf{A}, \mathbf{D} \leftarrow \$$<br>– $\mathsf{ct}_1 \leftarrow \$$<br>– $\mathsf{ct}_2 \leftarrow \$$ |
| **Output:** $(\mathsf{hpk}, \mathsf{enc})$, where encoding $\mathsf{enc} = (\mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_0, \mathsf{ct}_1)$ | |

**Fig. 1.** $f^{\text{circ}}$-circular security of HE scheme. The assumption is parameterized by a polynomial-sized circuit $f^{\text{circ}}$ with domain/codomain implicitly defined. We use the curly notation $\underbrace{\cdots}$ to hide the noise terms.

We consider the assumption, denoted as $\mathsf{CRO}$, to be the $f^{\text{circ}}$-circular security (Fig. 1) with an additional *opening* component described in Fig. 2. Since we work with the GSW encryption scheme, we provide a concrete version of this assumption in Fig. 3.

In this assumption, we consider a function $f$ (with potentially $\mathbb{Z}_q$-vector outputs) to be homomorphically evaluated. One computes $\mathsf{hct}_f = \mathsf{Eval}(f, \mathsf{hct})$. The assumption aims to securely open the randomness to $\mathsf{hct}_f$ that allows one to learn $f(\mathbf{r})$.

One intuitive way to achieve this would be to release randomness $\mathbf{R}_f$ such that $\mathsf{hct}_f = \mathsf{HE.Enc}(\mathsf{hpk}, f(\mathbf{r}); \mathbf{R}_f)$. Such a randomness can be computed as a deterministic function of the randomness used in the initial ciphertexts used to compute $\mathsf{hct}_f$ relying on the well-known randomness homomorphism structure in the GSW encryption scheme. Unfortunately, leaking $\mathbf{R}_f$ this was could jeopardize security as it might have a structure that enables leaking sensitive information. In fact, leveraging the prior attack techniques developed in [48] one might be able to show explicit attacks. Alternatively, one might try to release a random Gaussian opening $\tilde{\mathbf{R}}_f$ subject to the equation $\mathsf{hct}_f = \mathsf{HE.Enc}(\mathsf{hpk}, f(\mathbf{r}); \tilde{\mathbf{R}}_f)$, hoping that the additional randomness helps with security. This can be done, for example, by relying on a trapdoor matrix for the LWE coefficient matrix used to generate $\mathsf{hpk}$. Unfortunately, here too, one could find structural vulnerabilities enabling explicit attacks.

A reasonable approach to handle this is to introduce some sort of shield (as also considered by Gay and Pass [36]). Namely, we consider a fresh cipher-

text $\mathsf{hct}_0$ that encrypts 0, encrypted with randomness sampled from a special re-randomizing randomness distribution $\mathcal{D}_{\text{rand}}$ capable of smudging the evaluated randomness inside $\mathsf{hct}_f$ (see the rerandomizability property of HE, Definition 2.2). For GSW, the distribution $\mathcal{D}_{\text{rand}}$ consists of i.i.d. samples from a wide enough Gaussian distribution. Then, one can release an opening of the re-randomized ciphertext $\mathsf{hct}_f^* = \mathsf{hct}_f + \mathsf{hct}_0$. The opening is simply $\mathbf{R}^* = \mathbf{R}_f + \mathbf{R}_0$.

If the function $f(\star)$ did not depend on the secret, and in addition there were no circular encryptions of the secrets in the real distribution, the security of such a distribution can be proved under LWE (see [36] for details). Note that however, since the ciphertext $\mathsf{hct}$ encrypts the secret $\mathbf{r}$, one has to be careful on which functions $f(\star)$ should be allowed to learn. Therefore, for the assumption to make sense, we consider functions $f(\star)$ whose output can be computed publicly. We capture this by the safety constraint in eq. (1), where we require that in the real distribution, with high probability $f(\mathbf{r}) = \tilde{f}(\mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_1, \mathsf{ct}_2)$ for an efficient function $\tilde{f}$. This means revealing the function output is benign, since it can already be computed efficiently from the encodings themselves.

This describes the *real* distribution in Fig. 3. Namely, the distribution consists of HE and LWE encodings along with fresh encryption $\mathsf{hct}_0$ and the opening $\mathbf{R}^*$. We note that $f(\star)$ is a function that satisfies a safety constraint outlined in Fig. 2. Namely, the constraint requires that with overwhelming probability $f(\mathbf{r}) = \tilde{f}(\mathsf{enc})$ where $\mathsf{enc}$ contains $(\mathsf{hpk}, \mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_1, \mathsf{ct}_2)$ for some efficient functions $f, \tilde{f}$. One can also observe that instead of releasing $\mathbf{R}^* = \mathbf{R}_0 + \mathbf{R}_f$, we release $\mathbf{R}^*$ subject to $\mathsf{hct}_f^* = \mathsf{HE.Enc}(\mathsf{hpk}, \mathbf{0}; \mathbf{R}^*) \boxplus f(\mathbf{r}) \overset{\text{w.h.p.}}{=} \mathsf{HE.Enc}(\mathsf{hpk}, \mathbf{0}; \mathbf{R}^*) \boxplus \widetilde{f}(\mathsf{enc})$. For the GSW encryption scheme, the distribution of the openings generated deterministically as $\mathbf{R}_0 + \mathbf{R}_f$ and through random sampling are statistically close so long as $\mathcal{D}_{\text{rand}}$ is a wide-enough Gaussian. This choice is made as it syntactically unifies our presentation of the real and ideal distributions.

At this point, we remark that Gay and Pass also proposed an assumption that gave rise to similar structures, but there are major differences. Notably, in our case the function $f(\star)$ is independent of $\mathsf{hct}_0$. This causes $\mathbf{R}_f$ and $\mathbf{R}_0$ to be independent. As a consequence $\mathbf{R}^* = \mathbf{R}_f + \mathbf{R}_0$ behaves like a standard Gaussian matrix over integers. In the assumption proposed by Gay and Pass, homomorphic evaluation of $f$ can depend on $\mathsf{hct}_0$, leading $\mathbf{R}^*$ to have an extractable bias, allowing for an efficient distinguisher in the assumption for a properly chosen $f$ [48].

We now describe the *ideal* distribution in our assumption. Correspondingly, the new ideal distribution contains $(\mathsf{hpk}, \mathsf{enc}) \leftarrow \mathcal{D}_1$ together with $\mathbf{R}^* \leftarrow \mathsf{Open}(f, \widetilde{f}, (\mathsf{hpk}, \mathsf{enc}))$. Here, both $\mathsf{hpk}, \mathsf{enc}$ are sampled as uniformly random matrices in their co-domains as opposed to being generated honestly. While we do this, we make sure that the $\mathsf{Open}$ procedure is still well defined. In the case, the intermediate ciphertexts $\mathsf{hct}_f$ and $\mathsf{hct}_f^*$ are now computed efficiently from random public key $\mathsf{hpk}$ and random encodings $\mathsf{enc}$ by using the homomorphic evaluation procedures. The opening $\mathbf{R}^*$ is now sampled so that it satisfies the equation $\mathsf{hct}_{f^*} = \mathsf{HE.Enc}(\mathsf{hpk}, \mathbf{0}; \mathbf{R}^*) \boxplus \tilde{f}(\mathsf{enc})$. One might wonder why can this be done? We note that when the public keys are random, GSW enjoys an

**Opening procedure** $\mathsf{Open}(f, \widetilde{f}, \cdot)$

**Constraint:** The opening is parameterized with two efficiently computable function $f$ and $\widetilde{f}$ where $f$ is in the function class supported by $\mathsf{HE}$. $f$ maps tuple $(\mathbf{r}, \mathbf{A}, \mathbf{D})$ to $\mathcal{R}^{M'}$, while $\widetilde{f}$ maps $\mathsf{enc}$ to $\mathcal{R}^{M'}$. The procedure is only defined if $(f, \widetilde{f})$ satisfies the following constraint.

$$\textbf{safety constraint:} \quad \Pr[f(\mathbf{r}, \mathbf{A}, \mathbf{D}) = \widetilde{f}(\mathsf{enc})] \geq 1 - \epsilon(\lambda), \tag{1}$$

where the probability is taken over the sampling of $(\mathbf{r}, \mathbf{A}, \mathbf{D}, \mathsf{enc})$ according to distribution $\mathcal{D}_0$. We require $\epsilon$ to be negligible when considering polynomial security of $\mathsf{CRO}$, and require $\epsilon = 2^{-\lambda^\delta}$ when considering sub-exponential security.

**Procedure** $\mathsf{Open}(f, \widetilde{f}, (\mathsf{hpk}, \mathsf{enc}))$:
Parse $\mathsf{enc} = (\mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_0, \mathsf{ct}_1)$, the opening is computed as follow.

- Perform homomorphic evaluation over $\mathsf{hct}$ to get $\mathsf{hct}_f = \mathsf{HE.Eval}(\mathsf{hct}, f_{\mathbf{A},\mathbf{D}})$, where function $f_{\mathbf{A},\mathbf{D}}(\cdot) = f(\cdot, \mathbf{A}, \mathbf{D})$.
  *Comment: When* $\mathsf{enc}$ *follows the real distribution* $\mathcal{D}_0$*, since* $\mathsf{hct}$ *is an honest encryption of* $\mathbf{r}$*, by correctness of* $\mathsf{HE}$*,* $\mathsf{hct}_f$ *is a valid encryption of* $f_{\mathbf{A},\mathbf{D}}(\mathbf{r}) = f(\mathbf{r}, \mathbf{A}, \mathbf{D})$*. Following the safety constraint (Equation (1)),* $\mathsf{hct}_f$ *is with overwhelming probability a valid encryption of* $\widetilde{f}(\mathsf{enc})$*.*
- Rerandomize ciphertext using the mask $\mathsf{hct}^*_f = \mathsf{hct}_f + \mathsf{hct}_0 \boxminus \widetilde{f}(\mathsf{enc})$.
  *Comment: When* $\mathsf{enc}$ *follows the real distribution* $\mathcal{D}_0$*, by the rerandomizable property of* $\mathsf{HE}$ *(Definition 2.2), the distribution of* $\mathsf{hct}^*_f$ *is statistically close to* $\mathsf{HE.Enc}(\mathsf{hpk}, \mathbf{0}^{M'}; \mathcal{D}_{\mathrm{rand}})$*.*
- Sample a random opening $\mathbf{R}^*$ of $\mathsf{hct}^*_f$ with respect to $\mathsf{hpk}$, i.e.,

$$\mathbf{R}^* \leftarrow \mathcal{D}_{\mathrm{rand}}|_{\mathsf{hct}^*_f = \mathsf{HE.Enc}(\mathsf{hpk}, \mathbf{0}^{M'}; \mathbf{R}^*)}.$$

  *Comment: When* $\mathsf{enc}$ *follows the real distribution* $\mathcal{D}_0$*, by the above discussion, the marginal distribution of* $\mathbf{R}^*$ *is statistically close to* $\mathcal{D}_{\mathrm{rand}}$ *(Theorem 2.6). When* $\mathsf{enc}$ *follows the ideal distribution* $\mathcal{D}_1$*, by the equivocation property of* $\mathsf{HE}$ *(Definition 2.3) and the* $f^{\mathrm{circ}}$*-circular security of HE (Figure 1), the marginal distribution of* $\mathbf{R}^*$ *is pseudorandom (Theorem 2.7).*

**Fig. 2.** $(f, \widetilde{f})$-opening for $f^{\mathrm{circ}}$-circularly secure HE scheme. We note that though the opening procedure is not necessarily efficient, it is possible to efficiently sample its output $\mathbf{R}^*$ together with $\mathcal{D}_0$ or $\mathcal{D}_1$.

equivocal mode as defined in Definition 2.3 which guarantees such pre-images that can be sampled using a trapdoor matrix for $\mathsf{hpk}$. We also ensure that $\mathbf{R}^*$ is sampled according to a discrete Gaussian of the same width as in the case of real distribution.

**Concrete Assumptions**

We consider circular security with random opening assumption specifically with respect to the GSW encryption scheme. We formulate three versions. First, a parameterized assumption w.r.t. some appropriate tuple $(f^{\text{circ}}, f, \widetilde{f})$, referred to as the $(f^{\text{circ}}, f, \widetilde{f})$-$\mathsf{CRO}$ assumptions. Next, in quest of identifying a fully-specified assumption sufficient for $\mathsf{iO}$, we provide a completely specified single assumption with concrete $(f^{\text{circ}}, f, \widetilde{f})$ needed for our $\mathsf{iO}$ construction later. Throughout, this is referred to as the $\mathsf{CRO}$ assumption that we use.

**The $(f^{\text{circ}}, f, \widetilde{f})$-$\mathsf{CRO}$ assumptions** For a tuple of appropriate functions $(f^{\text{circ}}, f, \widetilde{f})$, with appropriate domains/co-domains, and satisfying the safety constraint (Eq. (1)), the abstract assumption instantiated with GSW, which is an HE scheme satisfying all needed properties , gives the following assumption.

**Definition 2.4 ($(f^{\text{circ}}, f, \widetilde{f})$-Circular Security with Random Opening (CRO) Assumption).** *Let $\lambda$ be the security parameter. Let $n, m, d, k, \ell, M, \sigma$ be integer parameters that are polynomial in $\lambda$, and $q, \sigma_0$ be (potentially super-polynomial) integer parameters where $m = \Omega(n \log q)$ and $\sigma_0 = 2^{\lambda} m^{\Omega(d)}$ are sufficiently large. Let $f \in \mathcal{F}_{d,M}$ be a bounded depth packed circuit which parses its input as bits and have depth bound $d$ and output length $M$, where $M$ w.l.o.g. is a multiple of $(n+1)\lceil \log q \rceil$[4], and $f^{\text{circ}}$ and $\widetilde{f}$ be efficiently computable functions with domain/codomain implicitly defined in Fig. 3.*

*We say that the (subexponential) $(f^{\text{circ}}, f, \widetilde{f})$-CRO assumption holds if $\mathcal{D}_0$ and $\mathcal{D}_1$ in Fig. 3 are (sub-exponentially) indistinguishable to all polynomial time attackers.*

$$\{(\mathsf{hpk}, \mathsf{enc} = (\mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_1, \mathsf{ct}_2), \mathsf{hint} = \mathbf{R}^*) \mid (\mathsf{hpk}, \mathsf{enc}, \mathsf{hint}) \leftarrow \mathcal{D}_0\}_\lambda$$
$$\approx \{(\mathsf{hpk}, \mathsf{enc} = (\mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_1, \mathsf{ct}_2), \mathsf{hint} = \mathbf{R}^*) \mid (\mathsf{hpk}, \mathsf{enc}, \mathsf{hint}) \leftarrow \mathcal{D}_1\}_\lambda$$

Next, we provide the fully-specified version (referred to as the $\mathsf{CRO}$ assumption) that is needed for our $\mathsf{iO}$ construction. The main difference between these assumptions is that this assumption is a particular instantiation of the previous assumption working with specific parameters (such as modulus, dimension, etc.) and specific functions $(f^{\text{circ}}, f, \widetilde{f})$ satisfying the safety constraint, as needed by our $\mathsf{iO}$ construction. Note that our $\mathsf{iO}$ construction needs to use this assumption for a *single* choice of $(f^{\text{circ}}, f, \widetilde{f})$. These functions do not depend on which circuit is being obfuscated, but only on the input/output length and the circuit size.

**The $\mathsf{CRO}$ assumption** In fact, for our construction of $\mathsf{iO}$, it suffices to assume the CRO assumption for specific tuples of functions. By default, $\mathsf{CRO}$-assumption refers to this version.

[4] One can always append zeros to the function output to make $M$ a multiple of $(n+1)\lceil \log q \rceil$. This is a technicality due to the interface of GSW that we formalized in accordance with the abstract definition of HE, requiring that when encrypting a $\mathbb{Z}_q$ vector, the length of the vector is $(n+1)\lceil \log q \rceil$.

**$(f^{\text{circ}}, f, \widetilde{f})$-Circular Security with Random Opening**

**Real Distribution $\mathcal{D}_0$ / Ideal Distribution $\mathcal{D}_1$**

**HE (GSW) Components (Real):**

- $\mathbf{r} \leftarrow \mathbb{Z}_q^n$.
- $\mathsf{hpk} = \overline{\mathbf{B}} = \begin{pmatrix} \mathbf{B} \\ \mathbf{r}^\intercal \mathbf{B} + \mathbf{e}^\intercal \end{pmatrix}$, $\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}$, $\mathbf{e} \leftarrow \mathcal{D}_\sigma^m$.
- $\mathsf{hct} = \overline{\mathbf{B}}\mathbf{R} + \mathsf{bits}(\mathbf{r})^\intercal \otimes \mathbf{G}_{n+1}$, $\mathbf{R} \leftarrow \{0,1\}^{m \times n(n+1)\lceil \log q \rceil^2}$.
- $\mathsf{hct}_0 = \overline{\mathbf{B}}\mathbf{R}_0$, $\mathbf{R}_0 \leftarrow \mathcal{D}_{\sigma_0}^{m \times M}$.

**LWE Components (Real):**

- $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times \ell}$, $\mathbf{D} \leftarrow \mathbb{Z}_q^{n \times k}$.
- $\mathsf{ct}_1 = \mathbf{U}^\intercal \mathbf{A} + \mathbf{E}_\mathbf{A} + \mathbf{I}_\ell \otimes \mathbf{G}_n^\intercal \mathbf{r}$, $\mathbf{U} \leftarrow \mathbb{Z}_q^{n \times \ell n \lceil \log q \rceil}$, $\mathbf{E}_\mathbf{A} \leftarrow \mathcal{D}_\sigma^{\ell n \lceil \log q \rceil \times \ell}$.
- $\mathsf{ct}_2 = \mathbf{r}^\intercal \mathbf{D} + \mathbf{e}_\mathbf{D}^\intercal + f^{\text{circ}}(\mathbf{U}, \mathsf{hct}_0)$, $\mathbf{e}_\mathbf{D} \leftarrow \mathcal{D}_\sigma^k$

**HE (GSW) Components (Ideal):**

- $\mathsf{hpk} \leftarrow \mathbb{Z}_q^{(n+1) \times m}$
- $\mathsf{hct} \leftarrow \mathbb{Z}_q^{(n+1) \times n(n+1)\lceil \log q \rceil^2}$.
- $\mathsf{hct}_0 \leftarrow \mathbb{Z}_q^{(n+1) \times M}$.

**LWE Components (Ideal):**

- $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times \ell}$, $\mathbf{D} \leftarrow \mathbb{Z}_q^{n \times k}$.
- $\mathsf{ct}_1 \leftarrow \mathbb{Z}_q^{\ell n \lceil \log q \rceil \times \ell}$.
- $\mathsf{ct}_2 \leftarrow \mathbb{Z}_q^{1 \times k}$.

$\mathsf{Open}(f, \widetilde{f}, (\mathsf{hpk}, \mathsf{enc} = (\mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_1, \mathsf{ct}_2)))$:
Functions $(f, \widetilde{f})$ satisfies the safety constraint eq. (1), i.e., with overwhelming probability over the sampling of $(\mathsf{hpk}, \mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_1, \mathsf{ct}_2)$ according to $\mathcal{D}_0$, it holds that $f(\mathbf{r}, \mathbf{A}, \mathbf{D}) = \widetilde{f}(\mathsf{enc})$.

1. $\mathsf{hct}_f = \mathsf{HE.Eval}(\mathsf{hct}, f_{\mathbf{A},\mathbf{D}}) \overset{\text{in } \mathcal{D}_0}{=} \overline{\mathbf{B}}\mathbf{R}_f \boxplus f(\mathbf{r}, \mathbf{A}, \mathbf{D})$ , where function $f_{\mathbf{A},\mathbf{D}}(\cdot) = f(\cdot, \mathbf{A}, \mathbf{D})$.
2. $\mathsf{hct}_f^* = \mathsf{hct}_f \boxplus (-\widetilde{f}(\mathsf{enc})) \boxplus \mathsf{hct}_0 \overset{\text{in } \mathcal{D}_0}{\approx_s} \overline{\mathbf{B}}(\mathbf{R}_f + \mathbf{R}_0)$.
3. $\mathbf{R}^* \leftarrow \mathcal{D}_{\sigma_0}^{m \times k} \Big|_{\mathsf{hct}_f^* = \overline{\mathbf{B}}\mathbf{R}^*}$.

**Output:** $(\mathsf{hpk}, \mathsf{enc} = (\mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_1, \mathsf{ct}_2), \mathbf{R}^*)$.

**Fig. 3.** $n, m, q, d, k, \ell, M, \sigma, \sigma_0$ are $\lambda$-dependent parameters where $n, m, d, k, \ell, M, \sigma$ are polynomials in $\lambda$, while $q, \sigma_0$ may be superpolynomial in $\lambda$ satisfying $(n+1)\lceil \log q \rceil | M$, $m = \Omega(n \log q)$, and $\sigma_0 = 2^\lambda m^{\Omega(d)}$, where $m, \sigma_0$ are sufficiently large. Circuit $f \in \mathcal{F}_{d,M}$ is a bounded depth packed circuit with depth bound $d$ and output length $M$. We assume that $f$ parses its input as bits.

**Assumption 1 (Circular Security with Random Opening (CRO) Assumption)** *Let $\lambda$ be the security parameter, and $n, q, \sigma$ be LWE parameters dependent on $\lambda$, where $n = \mathsf{poly}(\lambda)$, $\sigma = \mathsf{poly}(\lambda)$, $q \leq 2^{n^\delta}$ for some constant $\delta \in (0,1)$, $q$ is a multiple of $\Delta$ such that $q/\Delta \geq 2^\lambda$, and $\Delta \geq (2n \log q)^\lambda$. The (subexponential) CRO assumption with parameters $(n, q, \sigma, \Delta)$ states that for an appropriate $m = \Theta(n \log q)$, $\sigma_0 = \Delta/2^{\Theta(\lambda)}$, and every efficiently computable*

*polynomials $Q : \mathbb{Z} \to \mathbb{Z}$ and $\ell : \mathbb{Z} \to \mathbb{Z}$, the (subexponential) $(f^{\mathrm{circ}}, f, \widetilde{f})$-CRO assumption holds for the following function tuple.*

$$\mathsf{hct}_0 = \begin{pmatrix} \overline{\mathsf{hct}}_{0,i} \in \mathbb{Z}_q^{n\times\ell} \\ \underline{\mathsf{hct}}_{0,i} \in \mathbb{Z}_q^{1\times\ell} \end{pmatrix}_{i\in[Q]} \qquad \mathbf{D} = \left(\mathbf{D}_i \in \mathbb{Z}_q^{n\times n\lceil\log q\rceil}\right)_{i\in[Q]}$$

$$\mathsf{ct}_2 = \left(\mathsf{ct}_{2,i} = \mathbf{r}^\intercal\mathbf{D}_i + \mathbf{e}_{\mathbf{D},i} + f_i^{\mathrm{circ}}(\mathbf{U}, \mathsf{hct}_{0,i})\right)_{i\in[Q]} \quad (f^{\mathrm{circ}}, f, \widetilde{f}) = \left(f_i^{\mathrm{circ}}, f_i, \widetilde{f}_i\right)_{i\in[Q]}$$

$$f_i^{\mathrm{circ}}(\mathbf{U}, \mathsf{hct}_0) = -\mathsf{vec}(\mathbf{G}^{-1}(-\overline{\mathsf{hct}}_{0,i}))^\intercal \cdot (\mathbf{U}^\intercal\mathbf{G}) \in \mathbb{Z}_q^{1\times n\lceil\log q\rceil}$$

$$f_i(\mathbf{r}, \mathbf{A}, \mathbf{D})^\intercal = \Delta \left\lfloor \frac{\mathbf{r}^\intercal\mathbf{D}_i \cdot \mathbf{G}^{-1}(\mathbf{A})}{\Delta} \right\rceil \in \mathbb{Z}_q^{1\times\ell}$$

$$\widetilde{f}_i(\mathsf{hct}, \mathsf{hct}_0, \mathbf{A}, \mathbf{D}, \mathsf{ct}_1, \mathsf{ct}_2)^\intercal = \Delta \left\lfloor \frac{\mathsf{ct}_{2,i} \cdot \mathbf{G}^{-1}(\mathbf{A}) + \mathsf{vec}(\mathbf{G}^{-1}(-\overline{\mathsf{hct}}_{0,i}))^\intercal\mathsf{ct}_1 + \underline{\mathsf{hct}}_{0,i}}{\Delta} \right\rceil \in \mathbb{Z}_q^{1\times\ell}$$

*Note that $f$ is computable by a packed circuit of depth $d = O(\log(n \log q))$. The corresponding distributions $\mathcal{D}_0$, $\mathcal{D}_1$ in Fig. 3 have parameters $(n, m = \Theta(n \log q), q, d, k = Qn\lceil\log q\rceil, \ell, M = Q\ell, \sigma, \sigma_0)$.*

The CRO assumption is almost fully specified modulo the circuit that implements $f_{\mathbf{A},\mathbf{D}}$ . The circuit hard-codes $\mathbf{G}^{-1}(\mathbf{A})$ and $\mathbf{D}$, and performs matrix multiplication, tensor products, modulo $q$, and rounding. We simply choose canonical circuits implementing these operations.

We show below that $f, \widetilde{f}$ considered in the CRO assumption indeed satisfies the safety constraint. A reader can safely skip the proof of this lemma below without affecting the understanding about the assumption or our construction:

**Lemma 2.5.** *The following safety constraint holds w.r.t. the distribution $\mathcal{D}_0$ and functions $(f^{\mathrm{circ}}, f, \widetilde{f})$ specified in Assumption 1.*

$$\textbf{safety constraint}: \quad \Pr[f(\mathbf{r}, \mathbf{A}, \mathbf{D}) = \widetilde{f}(\mathsf{enc})] \geq 1 - 2^{-\Omega(\lambda)}, \tag{2}$$

*where the probability is taken over the sampling of $(\mathbf{r}, \mathbf{A}, \mathbf{D}, \mathsf{enc})$ according to $\mathcal{D}_0$.*

A reader might find some superficial similarities between CRO and two assumptions considered in prior works: Evasive LWE [68–70] and 2-Circ SRL security [36]. We stress that there are many important differences in our assumptions that are crucial. It is these differences that make our assumptions provably robust against natural applications of all known attacks applicable to Evasive LWE and 2-Circ SRL security. In the full version [49], we give a detailed comparison between CRO and the two assumptions.

## 2.3 Cryptanalysis

In this section, we discuss natural avenues to break our assumption, including prior cryptanalytic attempts on related assumptions implying iO and PrO.

As mentioned previously, our assumption falls into the category of **LWE-with-hints** assumptions. Indeed, as described in Fig. 3 we have HE and LWE components, in addition to opening $\mathbf{R}^*$ that is referred to as hint in this case. We start by characterizing/summarizing the state of attacks by discussing what parts of the assumption these attacks focus on as well as cryptanalytic techniques. Then, we will understand our assumption in light of this characterization.

**Characterization of Prior Attacks**

Broadly speaking, all known prior attacks on assumptions fitting into **LWE-with-hints** framework [2,4,16,20,30,36,52,71] could be characterized into three categories:

- **Type 1 Attacks:** These are attacks that only exploit the structure present in the hints or any immediately derivable leakage from the hint. These typically are the most worrisome kinds of attacks. Most of the previous attacks such as [48,51] and even the attacks in this work [49], on private-coin evasive LWE are of this kind.
- **Type 2 Attacks:** These are attacks that exploit only the structure present in the (circularly encrypted) samples but do not make use of any additional hint.
- **Type 3 Attacks:** These are attacks that make use of hints, together with samples, as well as any auxiliary information, if any, present in the assumption.

These attacks can also be characterized on the basis of cryptanalytic techniques:

- **Algebraic Attacks:** These attacks entail setting up systems of equations and solving them algebraically to recover various secrets involved in the assumption. The attack described by [51] on the assumption in [30] was a **Type 1** attack that set linear equations based on the provided hint and recovered the secrets involved.
- **Correlation Attacks:** These are attacks that examine the hint or immediately derivable leakage from the hint. These attacks extract a biased bit of information either correlated with secrets or that enables an efficient distinguisher. Attacks on the assumptions considered in previous schemes [16,36,71] described in [48] and the attack on private-coin evasive LWE underlying pseudorandom obfuscation [2,20] in this work are **Type 1** correlation attacks. Finally, we note that there were simple-to-state, instance-independent and falsifiable **LWE-with-hints** assumptions that implied $i\mathcal{O}$ together with Bilinear maps [1,4,52]. Earlier versions of these assumptions also had **Type 1** correlation based attacks based on sum-of-squares [11].
- **Corner Cases:** Often, a family of assumptions is meant to capture certain security heuristic, such as the evasive LWE assumption family, or the circular

security assumption family. An important type of cryptanalysis is searching for corner cases, which are attacks that exploit the freedom in the assumption family, or in coming up with variants of the assumption family, to find broken corner cases. When the corner cases are contrived and/or unnatural, they do not completely invalidate the security heuristic especially in "natural" applications (reminiscent of the random oracle heuristic). Nevertheless, they show how robust a security heuristic is, and we would ideally like to have assumptions that do not have broken corner cases.

So far, all direct attacks on **LWE-with-hints** assumptions underlying iO or PrO are of **Type 1**. For the broader class of private-coin evasive LWE assumptions which allows for general auxiliary information, there had been **Type 3** attacks [21,69] that designed complex auxiliary information containing obfuscated programs. The obfuscated programs can for example help utilize the matrix trapdoors in the post-conditions of evasive LWE in a way that cannot be matched in the pre-condition without matrix trapdoors. Note our CRO and IND-CRO assumptions do not allow any auxiliary input.

Furthermore, there had been attacks on circular security of lattice-based schemes that feature unnatural distributions [43,44,72]. In a nutshell, these encryption schemes rely on the cycle-tester framework typically instantiated using lockable/compute-and-compare obfuscation. However, these corner cases are not known to be applicable to prior assumptions towards iO or PrO, nor to our CRO and IND-CRO assumptions, which contain (circular) LWE samples that follow natural distributions, unlike these in the corner cases.

Finally, typically the more freedom an assumption family allows, or the more under-specified an assumption is, the more prone it can be to existence of corner cases. Our CRO and IND-CRO assumptions are fully-specified, thereby, reducing the room for such corner cases.

– **Lattice-Based Attacks:** Finally, an important class of attacks are lattice-based attacks. The goal here is to somehow translate the problem of LWE samples with hints into an efficiently solvable lattice problem. This is an important potential class of attacks, however, when the hints are matrix trapdoors (as in evasive LWE) or openings (as in this work) it is unclear how to use them in lattice attacks beyond the straightforward way – simply using the hints to obtain new LWE samples by multiplying $\overline{\mathbf{B}}$ with the hint, and then attacking the original LWE samples together with these new samples, ignoring the hints. Recall that in CRO and IND-CRO, using the openings in this way only gives $\overline{\mathbf{B}}\mathbf{R}^*$ which can already be efficiently computed from the original LWE encodings, reducing to **Type 2** attacks that ignore the hints.

  In fact, the question whether there are lattice techniques that can significantly speed up attacks on LWE encodings by using matrix trapdoors in a non-straightforward way is a question implicitly posted by the evasive LWE assumptions. Despite various attacks on private coin evasive LWE, no such lattice techniques have been developed so far. We believe that this is a highly important question to investigate.

**Security Against Attacks**

Armed with the characterization of previous attacks and types of attacks, we now discuss the plausibility of our assumption with respect to these attacks.

**Resistance against Type - 1 Attacks.** Perhaps a major silver lining in our assumption is that one can show provable resistance against **Type 1** attacks. These are typically the most devastating attacks as witnessed in most attacks to recent **LWE-with-hints** assumptions [11,48,51].

As it turns out, our hint $\mathbf{R}^*$ (in the real distribution) as seen in Fig. 3 is statistically closely distributed to a canonical discrete Gaussian distribution.

**Theorem 2.6.** *In the real distribution $\mathcal{D}_0$ of the $(f^{\text{circ}}, f, \widetilde{f})$-CRO assumption (Figure fig. 3), if $f, \widetilde{f}$ satisfies the (subexponential) safety condition (Eq. 1), then the marginal distribution of the opening $\mathbf{R}^*$ in $\mathcal{D}_0$ is (subexponentially) statistically-close to a fresh discrete Gaussian $\mathcal{D}_{\sigma_0}^{m \times M}$.*

Furthermore, we can also prove that in the ideal distribution, the hints $\mathbf{R}^*$ are computationally indistinguishable to the same Gaussian distribution, assuming the $f^{\text{circ}}$-circular security assumption described in Fig. 1.

**Theorem 2.7.** *In the ideal distribution $\mathcal{D}_1$ of the $(f^{\text{circ}}, f, \widetilde{f})$-CRO assumption (Figure fig. 3), if $f, \widetilde{f}$ satisfies the (subexponential) safety condition (Eq. 1), then assuming the (subexponential) $f^{\text{circ}}$-circular assumption [5], the marginal distribution of the opening $\mathbf{R}^*$ in $\mathcal{D}_1$ is (subexponentially) indistinguishable to a fresh discrete Gaussian $\mathcal{D}_{\sigma_0}^{m \times M}$ for all polynomial-sized adversaries.*

Moreover, in our assumption there is no additional"immediate natural leakage" enabled by the hint. If $\mathbf{R}^*$ is used in the straightforward way, one can only compute:

$$\mathsf{hct}_f^* = \overline{\mathbf{B}}\mathbf{R}^* = \mathsf{hct}_f \boxplus \mathsf{hct}_0 \boxminus \widetilde{f}(\mathsf{enc}),$$

which is a known function of the LWE/HE encodings. In that sense, our assumption does not produce additional natural leakage, unlike some of the prior assumptions [30,71], and like [36].

**Resistance against Type - 2 Attacks.** Next, we discuss security of just the HE/LWE encodings, i.e., the $f^{\text{circ}}$-circular security. The non-standardness in our LWE samples comes from the fact that they are circularly encoded. If one is not careful with the dependency of various secrets and public matrices, it is easy to construct easy-to-attack distributions.

For example, if only one secret $\mathbf{s}$ is involved, it is problematic to consider samples with the pattern $\{\mathbf{s}\mathbf{A}_1 + f_1(\mathbf{s}, \mathbf{A}_2) + \mathbf{e}_1, \mathbf{s}\mathbf{A}_2 + f_2(\mathbf{s}, \mathbf{A}_1) + \mathbf{e}_2\}$, where $f_1, f_2$ are efficiently computable "circular" functions. The reason for this is that one could choose $f_1(\mathbf{s}, \mathbf{A}_2) = -\mathbf{s}\mathbf{A}_2$ and $f_2(\mathbf{s}, \mathbf{A}_1) = -\mathbf{s}\mathbf{A}_1$ producing samples that

[5] The formal description of the $f^{\text{circ}}$-circular assumption, along with the proofs of the two theorems, are provided in the full version [49].

add up to a small norm vector $\mathbf{e}_1+\mathbf{e}_2$. These counterexamples do not apply when one of $f_1, f_2$ becomes independent of the coefficient matrices. These problematic patterns would also be an issue in the two-secret settings. For instance, samples of the form $\{\mathbf{s}_1\mathbf{A} + f_1(\mathbf{s}_2, \mathbf{B}) + \mathbf{e}_1, \mathbf{s}_2\mathbf{B} + f_2(\mathbf{s}_1, \mathbf{A}) + \mathbf{e}_2\}$ is prone to the exact same counterexample.

It seems problematic when the dependency on the public matrix is also circular. In the above example, we have function of $\mathbf{B}$ encoded by LWE samples of matrix $\mathbf{A}$, and function of $\mathbf{A}$ circularly encoded by LWE samples of matrix $\mathbf{B}$.

Our assumption, on the other hand, follows a good circular security pattern in the two-secret setting, where the dependency on the public matrices is non-circular. As described in Assumption 1, we have samples of the form $\{\mathbf{s}_2\mathbf{A} + f_0(\mathbf{s}_2) + \mathbf{e}_0, \mathbf{s}_1\mathbf{B} + f_1(\mathbf{s}_2) + \mathbf{e}_1, \mathbf{s}_2\mathbf{C} + f_2(\mathbf{s}_1, \mathbf{A}) + \mathbf{e}_2\}$. Note that the only sample featuring a matrix in the encoded term is the third sample, but crucially, randomness $(\mathbf{C}, \mathbf{e}_2)$ used in this sample is not circularly encoded.

One can further generalize the above case into a circular encoding pattern that seems safe, without known counterexamples. In the single secret setting, one can assign an order to the encodings, such that, the $i$'th encoding encodes a function $f_i(\mathbf{s}, \{\mathbf{A}_j, \mathbf{e}_j\}_{j<i})$ of the secret $\mathbf{s}$ and randomness $(\mathbf{A}_j, \mathbf{e}_j)$ used in previous encodings $j < i$, using fresh and independent randomness $(\mathbf{A}_i, \mathbf{e}_i)$. That is, we have samples of form $\{\mathbf{s}\mathbf{A}_i + f_i(\mathbf{s}, \{\mathbf{A}_j, \mathbf{e}_j\}_{j<i})\}_{i\in[\ell]}$, where all $\mathbf{A}_i, \mathbf{e}_i$ are randomly sampled. In the case of multiple secrets, the circular functions $f_i$ can depend on all secrets. We leave it as an exciting open question to identify a set of efficient functions obeying this dependency pattern that leads to an efficient attack.

So far, the only circular security counterexamples on lattice-based schemes [44] make use of specific designs consisting of a cycle-tester framework containing lockable-obfuscation of carefully chosen programs. These structures are absent in our assumption.

**Resistance to Type-3 Attacks.** As mentioned above, currently there lack cryptanalytic techniques that can leverage the hint $\mathbf{R}^*$ in a non-straightforward way. The only exception is the corner cases of private-coin evasive LWE [68,69] that leverage complex auxiliary information depending on LWE matrices and/or secrets. Again, our assumption contains no auxiliary information. If $\mathbf{R}^*$ were used in the straightforward way, it produces encodings that can be efficiently computed from the original encodings in the assumption distributions, reducing security to the $f^{\text{circ}}$-circular security. We leave it as an exciting question to find such attacks on our assumption.

# 3 Overview for Functional Encoding Construction

**GSW and dual-GSW, through the Lens of Functional Encoding** Both the GSW and dual GSW homomorphic encryption scheme can be converted

into a functional encoding scheme[6] : To encode an input $\mathbf{x}$, simply encrypt it $\mathsf{hct} = \mathsf{Enc}(\mathbf{x}; \rho)$. To open the output of a function $g$, first perform homomorphic evaluation to obtain $\mathsf{hct}_g = \mathsf{Enc}(\mathbf{x}; \rho_g)$ and use the randomness $\rho_g$ underlying the output ciphertext as the opening. More specifically,

$$\overline{\mathbf{B}} = \begin{pmatrix} \mathbf{B} \\ \mathbf{r}^\mathsf{T}\mathbf{B} + \mathbf{e}_\mathbf{B}^\mathsf{T} \end{pmatrix}, \mathsf{GSW.hct}(\mathbf{x}) = \overline{\mathbf{B}}\mathbf{R} + \mathbf{x}^\mathsf{T} \otimes \mathbf{G} \Longrightarrow \mathsf{GSW.hct}_g = \overline{\mathbf{B}}\mathbf{R}_g + \begin{pmatrix} \mathbf{0} \\ g(\mathbf{x}) \end{pmatrix}$$
$$\mathsf{dGSW.hct}(\mathbf{x}) = \mathbf{U}^\mathsf{T}\mathbf{A} + \mathbf{x} \otimes \mathbf{G}^\mathsf{T} + \mathbf{E} \Longrightarrow \mathsf{dGSW.hct}_g = \mathbf{u}_g^\mathsf{T}\mathbf{A} + g(\mathbf{x}) + \mathbf{e}_g^\mathsf{T}$$

Both GSW and dual-GSW allow packing and $g(\mathbf{x})$ can be a $\mathbb{Z}_q$ vector of some dimension $\ell$, and bit length close to $L = \ell \log q$ (modulo low order bits). The GSW opening is not succinct, as $\rho_g = \mathbf{R}_g$ has size $n \log q \cdot \ell \cdot \log q$. But dual-GSW does have succinct openings, with $\rho_g = \mathbf{u}_g$ of size $n \cdot \log q$, which is sublinear in $L$. Note that GSW does not have noise leakage, whereas dual-GSW leaks $\mathbf{e}_g$.

The main issue is that their openings reveal more information than $g(\mathbf{x})$. In both cases, $\mathbf{R}_g, \mathbf{u}_g$ is a linear function (dependent on $\mathbf{x}, g, \mathsf{hct}$) of the original randomness $\mathbf{R}, \mathbf{U}$. The revelation of them could completely compromise security.

One way to create a safe opening is through re-randomization: If there is additionally a fresh ciphertext of zero $\mathsf{hct}_0$ generated using randomness from an appropriate distribution, we can instead open $\mathsf{hct}'_g = \mathsf{hct}_g + \mathsf{hct}_0$. The randomness of $\mathsf{hct}_0$ can ensure that the re-randomized opening and noise leakage reveals only $g(\mathbf{x})$. More specifically, in GSW, the randomness in $\mathsf{hct}_0$ is $\widetilde{\mathbf{R}}$, consisting of i.i.d. sufficiently wide discrete Gaussian samples, and the opening becomes $\mathbf{R}^* = \mathbf{R}_g + \widetilde{\mathbf{R}}$, while in dual-GSW, the randomness in $\mathsf{hct}_0$ consists of random $\mathbf{s}$ and smudging noise $\mathbf{e}$, and the opening becomes $\tilde{\mathbf{s}} = \mathbf{u}_g + \mathbf{s}$, leaking noise $\tilde{\mathbf{e}} = \mathbf{e}_g + \mathbf{e}$. The fact that they reveal only $g(\mathbf{x})$ can be proven using the standard simulation technique that "programs" the output $g(\mathbf{x})$ into $\mathsf{hct}_0$ (e.g., see [71] for such a proof). Interestingly, GSW admits an alternative simulation strategy that "programs" $g(\mathbf{x})$ into the opening $\mathbf{R}^*$ (e.g., see [36] for such a proof).

The problem is we need fresh and independent zero-ciphertexts $\{\mathsf{hct}_{0,i}\}_{i\in[Q]}$ for each functional opening for $g_i$. There is no place for these zero-ciphertexts: They are too large, larger than $Q \cdot L$ bits, to be put in the succinct functional encoding. On the other hand, leaving them in the CRS renders them useless, as giving re-randomized openings such as $\widetilde{\mathbf{R}}, \tilde{\mathbf{s}}$ requires knowing the secrets related to the CRS.

**Version 0: Combining GSW with dual-GSW** In this work, we will leverage both the succinct opening of dual-GSW and the GSW simulation strategy of programming into randomness $\mathbf{R}^*$ . A technique of combining them, introduced by [15,16,36], is to perform homomorphic evaluation using GSW, followed by homomorphic decryption using dual-GSW, as shown in Fig. 4.

An encoding of $\mathbf{x}$ contains a GSW public key $\mathsf{hpk} = \overline{\mathbf{B}}$ with secret $\mathbf{r} \in \mathbb{Z}_q^n$, and a ciphertext $\mathsf{hct}(\mathbf{x})$. It also contains a dual-GSW ciphertext $\mathsf{dct}$ using public matrix $\mathbf{A}$ and encrypting the GSW secret $\mathbf{r}$ in a special form $\mathbf{I}_\ell \otimes \mathbf{G}_n^\mathsf{T}\mathbf{r} \in \mathbb{Z}_q^{\ell \cdot n \cdot \log q \times \ell}$.

[6] Functional encoding, introduced by [71], is an intermediate primitive implying $\mathsf{xiO}$. Due to space constraints, we refer the readers to the full version [49] for the definition.

**Encoding of x:**

| GSW components | dGSW components |
|---|---|
| $\mathsf{hpk} = \overline{\mathbf{B}} = \begin{pmatrix} \mathbf{B} \\ \mathbf{r}^\intercal\mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal \end{pmatrix}$. | $\mathbf{A}$ |
| $\mathsf{hct}(\mathbf{x}) = \overline{\mathbf{B}}\mathbf{R} + \mathbf{x}^\intercal \otimes \mathbf{G}_{n+1}$ . | $\mathsf{dct} = \mathbf{U}^\intercal\mathbf{A} + \mathbf{E}_{\mathbf{A}} + \mathbf{I}_\ell \otimes \mathbf{G}_n^\intercal\mathbf{r}$. |

**Opening $\mathbf{u}_{g_i}$ for $g_i$:**

| (1) Evaluate $g_i$. | (2) Linear decryption of $\mathsf{hct}_{g_i}$ |
|---|---|
| $\mathsf{hct}_{g_i} = \mathsf{Eval}(\mathsf{hct}(\mathbf{x}), g_i)$, | $\mathbf{v}_{g_i} = \mathsf{vec}(\mathbf{G}^{-1}(-\overline{\mathsf{hct}}_{g_i}))$ |
| $\begin{pmatrix} \overline{\mathsf{hct}}_{g_i} \\ \underline{\mathsf{hct}}_{g_i} \end{pmatrix} = \begin{pmatrix} \mathbf{B}\mathbf{R}_{g_i} \\ (\mathbf{r}^\intercal\mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal)\mathbf{R}_{g_i} + g_i(\mathbf{x}) \end{pmatrix}$. | $= \mathsf{vec}(\mathbf{G}^{-1}(-\mathbf{B}\mathbf{R}_{g_i}))$ |
| | $\mathsf{dct}_{g_i} = \mathbf{v}_{g_i}^\intercal \cdot \mathsf{dct} = \mathbf{u}_{g_i}^\intercal\mathbf{A} + \mathbf{e}_{g_i}^\intercal - \mathbf{r}^\intercal(\mathbf{B}\mathbf{R}_{g_i})$. |

**Correctness:** $\underline{\mathsf{hct}}_{g_i} + \mathsf{dct}_{g_i} = \mathbf{u}_{g_i}^\intercal\mathbf{A} + g_i(\mathbf{x}) + (\mathbf{e}_{\mathbf{B}}^\intercal\mathbf{R}_{g_i} + \mathbf{e}_{g_i}^\intercal)$ (3)

**Fig. 4.** Combining GSW and dual-GSW. The matrix/vectors are sampled as $\mathbf{r} \leftarrow \mathbb{Z}_q^n$, $\mathbf{B} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{e}_{\mathbf{B}} \leftarrow \mathcal{D}_\sigma^m$, $\mathbf{R} \leftarrow \{0,1\}^{m\times(n+1)\lceil\log q\rceil\cdot|\mathbf{x}|}$, $\mathbf{U} \leftarrow \mathbb{Z}_q^{n\times\ell n\lceil\log q\rceil}$, $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times\ell}$, $\mathbf{E}_{\mathbf{A}} \leftarrow \mathcal{D}_\sigma^{\ell n\lceil\log q\rceil\times\ell}$. The function $g_i$ has outputs in $\mathbb{Z}_q^\ell$. Hence variables derived from the homomorphic evaluation have dimensions: $\mathbf{R}_{g_i} \in \mathbb{Z}_q^{m\times\ell}$, $\mathbf{u}_{g_i} \in \mathbb{Z}_q^n$, $\mathbf{e}_{g_i} \in \mathbb{Z}_q^\ell$. The opening $\mathbf{u}_{g_i}$ is succinct: $|\mathbf{u}_{g_i}| = n\log q \ll \ell\log q = |g_i(\mathbf{x})|$.

Opening the output of a function $g_i$ proceeds as described in bottom part of Fig. 4: Step 1) computes a GSW-ciphertext $\mathsf{hct}_{g_i}$ of $g_i(\mathbf{x})$, followed by Step 2) that homomorphically decrypts $\mathsf{hct}_{g_i}$ under dual-GSW by computing $\mathsf{dct}_{g_i}$.

$$\mathsf{dct}_{g_i} = \underbrace{\mathsf{vec}\big(\mathbf{G}^{-1}(-\overline{\mathsf{hct}}_{g_i})\big)^\intercal}_{\mathbf{v}_{g_i}=\mathsf{vec}(\mathbf{G}^{-1}(-\mathbf{B}\mathbf{R}_{g_i}))} \cdot \mathsf{dct} = \underbrace{\mathbf{v}_{g_i}^\intercal \cdot \mathbf{U}^\intercal}_{\mathbf{u}_{g_i}^\intercal} \cdot \mathbf{A} + \underbrace{\mathbf{v}_{g_i}^\intercal \cdot \mathbf{E}_{\mathbf{A}}}_{\mathbf{e}_{g_i}^\intercal} + \underbrace{\mathbf{v}_{g_i}^\intercal \cdot (\mathbf{I}_\ell \otimes \mathbf{G}^\intercal\mathbf{r})}_{-\mathbf{r}^\intercal\cdot\mathbf{B}\mathbf{R}_{g_i}} \quad (4)$$

Adding $\mathsf{hct}_{g_i}$ and $\mathsf{dct}_{g_i}$ gives a dual-GSW ciphertext of $g_i(\mathbf{x})$ as shown in Eq. (3), which can be succinctly opened by revealing $\mathbf{u}_{g_i}$. However, just as dual-GSW, revealing $\mathbf{u}_{g_i}$ and leaking $\mathbf{e}_{g_i}$ may completely compromise security.

**Version I: Special Encoding of Secrets $(\mathbf{s}, \mathbf{e})$ of Zero-Ciphertexts** In order to hide $\mathbf{u}_{g_i}, \mathbf{e}_{g_i}$, we attempt to re-randomize the final dual-GSW ciphertext. Since, as discussed above, there is no suitable place for storing zero-ciphertexts $\{\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal\}_{i\in[Q]}$, we instead encrypt their secrets as described in Fig. 5. Version I encrypts all $\mathbf{s}_i$'s using GSW, and hides all $\mathbf{e}_i$'s in LWE samples $\mathbf{c}_i^\intercal = (\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal \bmod \Delta)$ modulo *a much smaller modulus* $\Delta \ll q$. (The dual-GSW components stay the same.) Note that the LWE samples $\{\mathbf{c}_i\}_{i\in[Q]}$ are succinct, of size $Q \cdot \ell \cdot \log\Delta \ll Q \cdot \ell \cdot \log q \approx Q \cdot L$. This also shows we cannot afford, for succinctness, to encrypt all the smudging noises $\mathbf{e}_i$ in any regular ciphertexts mod $q$.

In the following, we will temporarily switch to the goal of oblivious LWE sampling, which captures the key ideas. Intuitively, we can think of computing the function $f_i$ with output $\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal \bmod q$, and the final dual-GSW ciphertext

**Encoding:**

| GSW components | Connecting components | dGSW components |
|---|---|---|
| $\mathsf{hpk} = \begin{pmatrix} \mathbf{B} \\ \mathbf{r}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal \end{pmatrix}$. $\{\mathsf{hct}(\mathbf{s}_i) = \overline{\mathbf{B}}\mathbf{R} + \mathsf{bits}(\mathbf{s}_i)^\intercal \otimes \mathbf{G}_{n+1}\}_i$. | $\{\mathbf{c}_i^\intercal = (\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal \bmod \Delta)\}_i$. | $\mathbf{A}$ $\mathsf{dct} = \mathbf{U}^\intercal\mathbf{A} + \mathbf{E} + \mathbf{I}_\ell \otimes \mathbf{G}_n^\intercal\mathbf{r}$. |

**Oblivious LWE Sampling:**

| (1) Evaluate $f_i(\mathbf{s}_i) = \Delta \left\lfloor \frac{\mathbf{s}_i^\intercal\mathbf{A}}{\Delta} \right\rceil$. | (2) Add $\mathbf{c}_i$ | (3) Linear decryption for $\mathsf{hct}_{f_i}$ |
|---|---|---|
| $\mathsf{hct}_{f_i} = \mathsf{Eval}(\mathsf{hct}(\mathbf{s}_i), f_i)$, $\overline{\mathsf{hct}}_{f_i} = \mathbf{B}\mathbf{R}_{f_i}$ $\underline{\mathsf{hct}}_{f_i} = (\mathbf{r}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal)\mathbf{R}_{f_i} + f_i(\mathbf{s}_i)$ | $\underline{\mathsf{hct}}_{f_i} + \mathbf{c}_i$ $= (\mathbf{r}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal)\mathbf{R}_{f_i} + \mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal$ | $\mathbf{v}_{f_i} = \mathsf{vec}(\mathbf{G}^{-1}(-\overline{\mathsf{hct}}_{f_i}))$ $\mathsf{dct}_{f_i} = \mathbf{v}_{f_i}^\intercal \cdot \mathsf{dct}$ $= \mathbf{u}_{f_i}^\intercal\mathbf{A} + \mathbf{e}_{f_i}^\intercal - \mathbf{r}^\intercal(\mathbf{B}\mathbf{R}_{f_i})$ |

**Correctness** : $\forall i \in [Q]$, $\underline{\mathsf{hct}}_{f_i} + \mathbf{c}_i^\intercal + \mathsf{dct}_{f_i} = \tilde{\mathbf{s}}_i^\intercal\mathbf{A} + \tilde{\mathbf{e}}_i^\intercal$ where $\tilde{\mathbf{s}}_i = \mathbf{u}_{f_i} + \mathbf{s}_i$, $\tilde{\mathbf{e}}_i^\intercal = \mathbf{e}_i^\intercal + \mathbf{e}_\mathbf{B}^\intercal\mathbf{R}_{f_i} + \mathbf{e}_{f_i}^\intercal$ (5)

**Fig. 5.** Version I: Encrypt secrets $(\mathbf{s}_i, \mathbf{e}_i)$ of zero-ciphertexts. Note that $\mathbf{e}_i$'s are encoded in LWE samples with modulus $\Delta$, where $\Delta \gg \|\mathbf{e}_i\|$. The output of $f_i$ has roughly bit length $L = \ell \log q$. By setting $\log \Delta \ll \log q$ and $\log q$ to be sublinear in $L$, each $\mathbf{c}_i$ is succinct with length $L^{1-\epsilon}$. The marginal distribution of $\{\tilde{\mathbf{e}}_i\}$ is statistically close to iid Gaussian.

$\tilde{\mathbf{s}}_i^\intercal\mathbf{A} + \tilde{\mathbf{e}}_i^\intercal = (\mathbf{u}_{g_i} + \mathbf{s}_i)^\intercal\mathbf{A} + (\mathbf{e}_{g_i} + \mathbf{e}_i)^\intercal$ will be the generated LWE samples. (Note we use $f_i$ to denote the functions related to oblivious LWE sampling, to not confuse with the functions $g_i$ computed using functional encoding.) Our goal is to ensure that LWE secrets $(\tilde{\mathbf{s}}_i, \tilde{\mathbf{e}}_i)$ are pseudorandom, given the encoding and CRS (currently empty) from which they are generated. Eventually, this will be shown via simulation – the encodings and CRS can be simulated from $\tilde{\mathbf{s}}_i^\intercal\mathbf{A} + \tilde{\mathbf{e}}_i^\intercal$ with truly random $\tilde{\mathbf{s}}_i, \tilde{\mathbf{e}}_i$.

To this end, our first attempt at generating $\tilde{\mathbf{s}}^\intercal\mathbf{A} + \tilde{\mathbf{e}}^\intercal$ is described in the bottom part of Fig. 5. Step 1) uses GSW to homomorphically evaluate the function $f_i(\mathbf{s}_i) = \Delta\lfloor \mathbf{s}_i^\intercal\mathbf{A}/\Delta \rceil$ to get $\mathsf{hct}_{f_i}$; Step 2) adds $\mathbf{c}_i = (\mathbf{s}_i\mathbf{A} + \mathbf{e}_i \bmod \Delta)$ to the last row of $\mathsf{hct}_{f_i}$ to obtain a GSW ciphertext of $f_i(\mathbf{s}_i) + \mathbf{c}_i = (\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal \bmod q)$; Step 3) homomorphically decrypts $\mathsf{hct}_{f_i}$ under dual-GSW as done in Eq. (4) to produce the final LWE samples $\tilde{\mathbf{s}}_i^\intercal\mathbf{A} + \tilde{\mathbf{e}}_i^\intercal$.

*Advantage and Drawbacks* The advantage of Version I is that the LWE noises $\{\tilde{\mathbf{e}}_i\}_i$ follow the distribution of iid Gaussian $\tilde{\mathbf{e}}_{i,j} \sim \mathcal{D}_{\sigma_0}$. This is because $\tilde{\mathbf{e}}_i = \mathbf{e}_i + \mathbf{e}_\mathbf{B}\mathbf{R}_{f_i} + \mathbf{e}_{f_i}$, note that both $\mathbf{e}_\mathbf{B}\mathbf{R}_{f_i}$ and $\mathbf{e}_{f_i}$ resulting from homomorphic evaluation in Step 1) and 3) have bounded norm and are independent of the smudging noise $\mathbf{e}_i$. By sampling $\mathbf{e}_i$ according to $\mathcal{D}_{\sigma_0}$ with sufficient width $\sigma_0 \gg ||\mathbf{e}_{f_i} + \mathbf{e}_\mathbf{B}\mathbf{R}_{f_i}||$, $\tilde{\mathbf{e}}_i$ distributes statistically closely to iid Gaussian $\mathcal{D}_{\sigma_0}$. This means the noises $\tilde{\mathbf{e}}_i$ alone are safe to reveal.

It may appear that the LWE secret $\tilde{\mathbf{s}}_i$ is random, because of the randomness in $\mathbf{s}_i$. This is false because $\mathbf{u}_{f_i}$ may be correlated with $\mathbf{s}_i$. Recall that $\mathbf{u}_{f_i}^\intercal = \mathbf{v}_{f_i}^\intercal \cdot \mathbf{U}^\intercal$ and $\mathbf{v}_{f_i} = \mathsf{vec}\big(\mathbf{G}^{-1}(-\overline{\mathsf{hct}}_{f_i})\big)$. Note the top part $\overline{\mathsf{hct}}_{f_i}$ of the GSW output ciphertext $\mathsf{hct}_{f_i}$ is correlated with the encrypted secret $\mathsf{bits}(\mathbf{s}_i)$, and so is $\mathbf{u}_{f_i}$. Therefore, revealing $\tilde{\mathbf{s}}_i$ may leak information $\mathbf{u}_{f_i}$ which may compromise security.

*Comparisons* In all prior constructions of $\mathsf{xiO}$ and pseudorandom random obfuscation [2,20,30,71], except for [16,36], the marginal distribution of noise leakage is far from random. The structure in the noise leakage was leveraged in showing counterexamples [48] against certain instances of [71] and in the attack in the full version [49] against private-coin evasive LWE [2,20].

The distinction lies in how the smudging noise $\mathbf{e}_i$ is encoded or generated. In prior works, they are generated either through homomorphic decryption of the CRS, or homomorphic evaluation of a PRF, or expanded from a few samples $(\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}^\intercal)$ using a trapdoor $\mathbf{K} = \mathbf{B}^{-1}(\mathbf{P})$. In these examples, the generated smudging noise $\mathbf{e}_i$ is not random. The key idea in Version I is that random $\mathbf{e}_i$ is directly encoded in LWE samples with small modulus, and added to $\mathbf{e}_{f_i}$.

**Version II: Special Homomorphic Evaluation Procedure** We now fix the drawback in Version I that $\tilde{\mathbf{s}}_i = \mathbf{u}_{f_i} + \mathbf{s}_i$ is not marginally random. To this end, we remove the correlation between $\mathbf{u}_{f_i}$ and $\mathbf{s}_i$, by carefully designing a special procedure for homomorphically evaluating $\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal$. Our key observation is as follows: Given LWE sample $\mathbf{c}_{\mathbf{s},i}^\intercal = \mathbf{r}^\intercal\mathbf{D}_i + \mathbf{s}_i\mathbf{G} + \mathbf{e}_{\mathbf{s},i}^\intercal$ together with $\mathbf{c}_i$ introduced above, we can obtain $\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal$ hidden by a pad $\mathsf{PAD}_i(\mathbf{r})$ dependent only on $\mathbf{r}$.

$$
\begin{aligned}
&\Delta \cdot \left\lfloor \frac{\mathbf{c}_{\mathbf{s},i}^\intercal\mathbf{G}^{-1}(\mathbf{A}) - \mathbf{c}_i^\intercal}{\Delta} \right\rceil + \mathbf{c}_i^\intercal \\
&= \Delta \cdot \left\lfloor \frac{\mathbf{r}^\intercal\mathbf{D}_i\mathbf{G}^{-1}(\mathbf{A}) + \mathbf{e}_{\mathbf{s},i}^\intercal\mathbf{G}^{-1}(\mathbf{A}) - \mathbf{e}_i^\intercal}{\Delta} + \frac{\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal - (\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal \bmod \Delta)}{\Delta} \right\rceil + \mathbf{c}_i^\intercal \\
&= \Delta \cdot \left\lfloor \frac{\mathbf{r}^\intercal\mathbf{D}_i\mathbf{G}^{-1}(\mathbf{A}) + \mathbf{e}_{\mathbf{s},i}^\intercal\mathbf{G}^{-1}(\mathbf{A}) - \mathbf{e}_i^\intercal}{\Delta} \right\rceil + \Delta \cdot \left\lfloor \frac{\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal}{\Delta} \right\rceil + (\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal \bmod \Delta) \\
&\overset{w.h.p}{=} \Delta \cdot \left\lfloor \frac{\mathbf{r}^\intercal\mathbf{D}_i\mathbf{G}^{-1}(\mathbf{A})}{\Delta} \right\rceil + \mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal = \mathsf{PAD}_i(\mathbf{r}) + \mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal
\end{aligned} \tag{6}
$$

where the second last equality holds with high probability when the noises $\mathbf{e}_{\mathbf{s},i}^\intercal\mathbf{G}^{-1}(\mathbf{A}) - \mathbf{e}_i$ are much smaller than $\Delta$.

The Version II encoding is described in Fig. 6. It includes a circular GSW ciphertext $\mathsf{hct}(\mathbf{r})$ and LWE samples $\mathbf{c}_{\mathbf{s},i}^\intercal = \mathbf{r}^\intercal\mathbf{D} + \mathbf{s}_i^\intercal\mathbf{G} + \mathbf{e}_{\mathbf{s},i}^\intercal$, in addition to $\mathbf{c}_i, \mathsf{dct}$ as before. The evaluation proceeds as follows. Step 1) uses GSW homomorphic evaluation to obtain a ciphertext $\mathsf{hct}_{f_i}$ encrypting the pad $f_i(\mathbf{r}) = -\mathsf{PAD}_i(\mathbf{r})$. Step 2) computes $\mathsf{PAD}_i(\mathbf{r}) + \mathbf{s}_i\mathbf{A} + \mathbf{e}_i$ as in Eq. (6), and Step 3) homomorphically decrypts the GSW ciphertext under dual-GSW to obtain the LWE sample $\tilde{\mathbf{s}}_i^\intercal\mathbf{A} + \tilde{\mathbf{e}}_i^\intercal$. The overall correctness is summarized in Eq. (7).

*Advantage* The advantage of Version II is that the joint distribution of the LWE secret $\tilde{\mathbf{s}}_i$ and noise $\tilde{\mathbf{e}}_i$ is, marginally, random. $\tilde{\mathbf{s}}_i$ is uniformly random over $\mathbb{Z}_q$ since $\mathbf{s}_i$ is random and independent of $\mathbf{u}_{f_i}$ (and $\tilde{\mathbf{e}}_i$ is iid random Gaussian as in

## Encoding

**GSW components**

$$\mathsf{hpk} = \begin{pmatrix} \mathbf{B} \\ \mathbf{r}^\intercal\mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal \end{pmatrix}.$$

$$\mathsf{hct}(\mathbf{r}) = \overline{\mathbf{B}}\mathbf{R} + \mathsf{bits}(\mathbf{r})^\intercal \otimes \mathbf{G}_{n+1}.$$

**Connecting components**

$$\{\mathbf{c}_i^\intercal = (\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal \mod \Delta)\}_i.$$

$$\{\mathbf{D}_i\}_{i\in[Q]}.$$

$$\{\mathbf{c}_{\mathbf{s},i}^\intercal = \mathbf{r}^\intercal\mathbf{D}_i + \mathbf{e}_{\mathbf{s},i} + \mathbf{s}_i^\intercal\mathbf{G}\}_i$$

**dGSW components**

$$\mathbf{A}$$

$$\mathsf{dct} = \mathbf{U}^\intercal\mathbf{A} + \mathbf{E} + \mathbf{I}_\ell \otimes \mathbf{G}^\intercal\mathbf{r}$$

## Oblivious LWE Sampling:

**(1)** Evaluate

$$f_i(\mathbf{r}) = -\Delta\left\lfloor \frac{\mathbf{r}^\intercal\mathbf{D}_i\mathbf{G}^{-1}(\mathbf{A})}{\Delta} \right\rceil.$$

$$\mathsf{hct}_{f_i} = \mathsf{Eval}(\mathsf{hct}(\mathbf{s}_i), f_i),$$

$$\overline{\mathsf{hct}}_{f_i} = \mathbf{B}\mathbf{R}_{f_i}$$

$$\underline{\mathsf{hct}}_{f_i} = (\mathbf{r}^\intercal\mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal)\mathbf{R}_{f_i} + f_i(\mathbf{s}_i)$$

**(2)** Round and Mult by $\Delta$ and Add $\mathbf{c}_i$.

$$\Delta\left\lfloor \frac{\mathbf{c}_{\mathbf{s},i}^\intercal\mathbf{G}^{-1}(\mathbf{A}) - \mathbf{c}_i^\intercal}{\Delta} \right\rceil + \mathbf{c}_i$$

$$= \Delta\left\lfloor \frac{\mathbf{r}^\intercal\mathbf{D}\mathbf{G}^{-1}(\mathbf{A})}{\Delta} \right\rceil + \mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal$$

**(3)** Linear decryption for $\mathsf{hct}_{f_i}$.

$$\mathbf{v}_{f_i} = \mathsf{vec}(\mathbf{G}^{-1}(-\overline{\mathsf{hct}}_{f_i}))$$

$$\mathsf{dct}_{f_i} = \mathbf{v}_{f_i}^\intercal \cdot \mathsf{dct}$$

$$= \mathbf{u}_{f_i}^\intercal\mathbf{A} + \mathbf{e}_{f_i}^\intercal - \mathbf{r}^\intercal(\mathbf{B}\mathbf{R}_{f_i})$$

**Correctness** :

$$\forall i \in [Q],\ \underline{\mathsf{hct}}_{f_i} + \Delta\left\lfloor \frac{\mathbf{c}_{\mathbf{s},i}^\intercal\mathbf{G}^{-1}(\mathbf{A}) - \mathbf{c}_i^\intercal}{\Delta} \right\rceil + \mathbf{c}_i^\intercal + \mathsf{dct}_{f_i} = \tilde{\mathbf{s}}_i^\intercal\mathbf{A} + \tilde{\mathbf{e}}_i^\intercal \tag{7}$$

$$\text{where } \tilde{\mathbf{s}}_i^\intercal = \mathbf{u}_{f_i}^\intercal + \mathbf{s}_i^\intercal,\ \tilde{\mathbf{e}}_i^\intercal = \mathbf{e}_i^\intercal + \mathbf{e}_{\mathbf{B}}^\intercal\mathbf{R}_{f_i} + \mathbf{e}_{f_i}^\intercal$$

**Fig. 6.** Version II: Special Homomorphic Evaluation Procedure for Computing GSW ciphertexts of $\mathbf{s}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal$. Each $\mathbf{c}_{\mathbf{s},i}$ has dimension $n \log q$ and bit length $n \log q \log q$, which is sublinear in $L = \ell \log q$ if $n \log q \ll \ell$.

Version I). Recall again that $\mathbf{u}_{f_i}^\intercal = \mathbf{v}_{f_i}^\intercal \cdot \mathbf{U}^\intercal$ and $\mathbf{v}_{f_i} = \mathsf{vec}\big(\mathbf{G}^{-1}(-\overline{\mathsf{hct}}_{f_i})\big)$ depends on the top part of the ciphertext $\mathsf{hct}_{f_i}$. Different from Version I, $\mathsf{hct}_{f_i}$ is now the result of evaluating $f_i(\mathbf{r})$ and hence is only correlated with $\mathsf{hct}(\mathbf{r})$ and $f_i$ which depends on matrices $\mathbf{D}, \mathbf{A}$, and hence independent of $\mathbf{s}_i$.

*Comparison* In prior constructions [30,71], the LWE secrets $\tilde{\mathbf{s}}$ produced in the scheme are far from random. In particular, this was leveraged by [51] to launch a polynomial-time attack on [30].

*Drawbacks* Now that $(\tilde{\mathbf{s}}_i, \tilde{\mathbf{e}}_i)$ is jointly random, can we reduce the security of Version II to some LWE-with-hints assumption with random hints? We show below that this could be done, however, the resulting assumption needs to postulate security of LWE-based encodings with an "unnatural" distribution, in particular, they are provably not pseudorandom given the hints.

We observe that there is a reduction $\mathcal{R}_2$ that given a sample from the following "smaller" distribution can emulate the distribution of Version II:

$$\mathsf{Real}_{\mathrm{v2}} : (\mathsf{hpk}, \mathsf{hct}(\mathbf{r}), \{\mathbf{D}_i, \widehat{\mathbf{c}}_i\}_i, \mathbf{A}, \mathsf{dct}), \text{ where } \widehat{\mathbf{c}}_i^\intercal = \mathbf{r}^\intercal\mathbf{D}_i - \mathbf{u}_{f_i}^\intercal\mathbf{G} + \widehat{\mathbf{e}}_i^\intercal$$

Above, components $\mathsf{hpk}, \mathsf{hct}(\mathbf{r}), \mathbf{D}, \mathbf{A}, \mathsf{dct}$ are sampled exactly as in Version II. Therefore, the reduction $\mathcal{R}_2$ just needs to emulate the missing components $(\tilde{\mathbf{s}}_i, \tilde{\mathbf{e}}_i, \mathbf{c}_i, \mathbf{c}_{\mathbf{s},i})$ in Version II. Leveraging that $(\tilde{\mathbf{s}}_i, \tilde{\mathbf{e}}_i)$ are random, $\mathcal{R}_2$ *can sample them internally*, which implicitly defines $\mathbf{s}_i^\intercal = \tilde{\mathbf{s}}_i^\intercal - \mathbf{u}_{f_i}^\intercal$ and $\mathbf{e}_i^\intercal = \tilde{\mathbf{e}}_i^\intercal - (\mathbf{e}_{f_i}^\intercal + \mathbf{e}_{\mathbf{B}}^\intercal\mathbf{R}_{f_i})$.

Next, the correctness constraint (Eq. (7)) gives a way to emulate $\mathbf{c}_i$ as follows:

$$\mathbf{c}_i \textbf{ emulation:} \quad \mathbf{c}_i^\intercal = (\tilde{\mathbf{s}}_i^\intercal \mathbf{A} + \tilde{\mathbf{e}}_i^\intercal) - \underline{\mathsf{hct}}_{f_i} - \mathsf{dct}_{f_i} \pmod{\Delta} \tag{8}$$

Finally, $\mathbf{c}_{\mathbf{s},i}$, which should encrypt $\mathbf{s}_i^\intercal \mathbf{G} = \tilde{\mathbf{s}}_i^\intercal \mathbf{G} - \mathbf{u}_{f_i}^\intercal \mathbf{G}$ can be emulated using $\widehat{\mathbf{c}}_i$:

$$\mathbf{c}_{\mathbf{s},i} \textbf{ emulation:} \quad \mathbf{c}_{\mathbf{s},i}^\intercal = \widehat{\mathbf{c}}_i^\intercal + \tilde{\mathbf{s}}_i^\intercal \mathbf{G} \tag{9}$$

Hence, any property of the distribution in Version II translates to some property of $\mathsf{Real}_{\mathrm{v2}}$, and vice versa.

Examining the distribution $\mathsf{Real}_{\mathrm{v2}}$, it contains circular LWE encodings – $\mathsf{hct}(\mathbf{r})$ circularly encrypts $\mathbf{r}$ under $\mathbf{r}$, $\mathsf{dct}$ encrypts $\mathbf{I}_\ell \otimes \mathbf{G}^\intercal \cdot \mathbf{r}$ under $\mathbf{U}$, and $\widehat{\mathbf{c}}_i$ encrypts $\mathbf{u}_{f_i}$ under $\mathbf{r}$. It appears that by the commonly used circular LWE security rationale, one could postulate the pseudorandomness of $\mathsf{Real}_{\mathrm{v2}}$, which would imply some form of the security of Version II.

However, this is false. $\mathsf{Real}_{\mathrm{v2}}$ is provably not pseudorandom, because the correctness condition (Eq. (7)) of Version II translates into an efficiently verifiable constraint on $\mathsf{Real}_{\mathrm{v2}}$ that truly random encodings do not satisfy.

To unravel the apparent contradiction, it is instrumental to note that the encoding $\widehat{\mathbf{c}}$ is not a "safe" circular encoding. In general, a circular encoding $\mathbf{t}^\intercal \mathbf{H} + f(\mathbf{t}) + \mathbf{e}^\intercal$ is only secure if the encrypted message $f(\mathbf{t})$ is independent of the encoding randomness $(\mathbf{H}, \mathbf{e})$ (a trivial counterexamples is $f(\mathbf{t}) = -\mathbf{t}^\intercal \cdot \mathbf{H}$). However, $\widehat{\mathbf{c}}$ violates this rule-of-thumb: The message $\mathbf{u}_{f_i}$ depends on the random matrix $\mathbf{D}_i$ used to encode it. The correlation exists because $\mathbf{u}_{f_i}$ depends on the function $f_i$, which computes $f_i(\mathbf{r}) = -\Delta \lfloor \mathbf{r}^\intercal \mathbf{D}_i \mathbf{G}^{-1}(\mathbf{A})/\Delta \rceil$ and is dependent on $\mathbf{D}_i$.

We distill a take-away message from the above discussion. For any assumption that contains LWE-based encodings, we view the lack of plausible pseudorandomness of the encodings problematic, as it stands at odds with our intuition that security based on LWE encodings relies on their pseudorandomness[7].

Therefore, our goal is to formulate an LWE-with-hint assumption, where the LWE encodings in the real distribution are switched to random in the ideal distribution. Towards this, in Version III we will introduce a URS (uniform random CRS), and show simulation security, namely, the encodings and URS can be simulated using $\tilde{\mathbf{s}}_i^\intercal \mathbf{A} + \tilde{\mathbf{e}}_i^\intercal$.

*Comparison* In all prior oblivious LWE sampler and $\mathsf{xiO}$ constructions [15,16,30,36,71], the underlying hardness / assumption postulates indistinguishability security, and lack natural pseudorandomness variants of their assumptions.

**Version III: GSW Rerandomization, Pseudorandom LWE-with-Hint, and Simulation Security** Towards the aforementioned goal of relying on pseudorandom LWE-with-hint assumption and achieving simulation security, Ver-

[7] This should be separated from LWE-based constructions, e.g., NIZK, where pseudorandomness does not hold but ZK or indistinguishability holds. Such behaviors are the result of careful design, whereas when formulating assumptions, we are considering LWE encodings that we do not fully know how to analyze.

## Encoding:

**Common reference string:** $\mathsf{crs} = \{\mathbf{R}_i^* \leftarrow \mathcal{D}_{\sigma_0}^{m\times\ell}\}_{i\in[Q]}$.

| **GSW components** | **Connecting components** | **dGSW components** |
|---|---|---|
| $\mathsf{hpk} = \begin{pmatrix}\mathbf{B}\\ \mathbf{r}^\intercal\mathbf{B}+\mathbf{e}_{\mathbf{B}}^\intercal\end{pmatrix}$<br>$\mathsf{hct}(\mathbf{r}) = \overline{\mathbf{B}}\mathbf{R} + \mathsf{bits}(\mathbf{r})^\intercal \otimes \mathbf{G}_{n+1}$ | $\{\mathbf{c}_i^\intercal = (\mathbf{s}_i^\intercal\mathbf{A}+\mathbf{e}_i^\intercal \mod \Delta)\}_i$<br>$\{\mathbf{D}_i\}_{i\in[Q]}$<br>$\{\mathbf{c}_{\mathbf{s},i}^\intercal = \mathbf{r}^\intercal\mathbf{D}_i + \mathbf{e}_{\mathbf{s},i}^\intercal + \mathbf{s}_i^\intercal\mathbf{G}\}_i$ | $\mathbf{A}$<br>$\mathsf{dct} = \mathbf{U}^\intercal\mathbf{A}+\mathbf{E}+\mathbf{I}_\ell\otimes\mathbf{G}^\intercal\mathbf{r}$ |

## Oblivious LWE Sampling:

**(1)** Evaluate
$f_i(\mathbf{r}) = -\Delta\left\lfloor\frac{\mathbf{r}^\intercal\mathbf{D}_i\mathbf{G}^{-1}(\mathbf{A})}{\Delta}\right\rceil$
$\mathsf{hct}_{f_i} = \mathsf{Eval}(\mathsf{hct}(\mathbf{s}_i), f_i)$,
**(2)** Rerandomize
$\mathsf{hct}_i' = \mathsf{hct}_{f_i} + \overline{\mathbf{B}}\mathbf{R}_i^*$
$\overline{\mathsf{hct}_i'} = \mathbf{B}\widetilde{\mathbf{R}}_i$
$\underline{\mathsf{hct}_i'} = (\mathbf{r}^\intercal\mathbf{B}+\mathbf{e}_{\mathbf{B}}^\intercal)\widetilde{\mathbf{R}}_i + f_i(\mathbf{r})$
where $\widetilde{\mathbf{R}}_i = \mathbf{R}_{f_i} + \mathbf{R}_i^*$

**(3)** Round and Mult by $\Delta$ and Add

$$\left\lfloor\frac{\mathbf{c}_{\mathbf{s},i}^\intercal\mathbf{G}^{-1}(\mathbf{A})-\mathbf{c}_i^\intercal}{\Delta}\right\rceil+\mathbf{c}_i^\intercal = \left\lfloor\frac{\mathbf{r}^\intercal\mathbf{D}\mathbf{G}^{-1}(\mathbf{A})}{\Delta}\right\rceil+\mathbf{s}_i^\intercal\mathbf{A}+\mathbf{e}_i^\intercal$$

**(4)** Linear decryption for $\mathsf{hct}_i'$

$$\begin{aligned}\mathbf{v}_i &= \mathsf{vec}(\mathbf{G}^{-1}(-\overline{\mathsf{hct}_i'}))\\ \mathsf{dct}_i &= \mathbf{v}_i^\intercal\cdot\mathsf{dct}\\ &= \mathbf{u}_i^\intercal\mathbf{A}+\mathbf{e}_i'^\intercal-\mathbf{r}^\intercal(\mathbf{B}\widetilde{\mathbf{R}}_i)\\ &(\mathbf{u}_i^\intercal=\mathbf{v}_i^\intercal\mathbf{U}^\intercal,\ \mathbf{e}_i'^\intercal=\mathbf{v}_i^\intercal\mathbf{E})\end{aligned}$$

**Correctness** : $\forall i\in[Q]$, $\underline{\mathsf{hct}_i'}+\Delta\left\lfloor\frac{\mathbf{c}_{\mathbf{s},i}^\intercal\mathbf{G}^{-1}(\mathbf{A})-\mathbf{c}_i^\intercal}{\Delta}\right\rceil+\mathbf{c}_i^\intercal+\mathsf{dct}_i = \tilde{\mathbf{s}}_i^\intercal\mathbf{A}+\tilde{\mathbf{e}}_i^\intercal$ (10)
where $\tilde{\mathbf{s}}_i = \mathbf{u}_i+\mathbf{s}_i$, $\tilde{\mathbf{e}}_i^\intercal = \mathbf{e}_i^\intercal+\mathbf{e}_{\mathbf{B}}^\intercal\widetilde{\mathbf{R}}_i+\mathbf{e}_i'^\intercal$, $\mathbf{e}_i'^\intercal = \mathbf{v}_i\mathbf{E}$

**Fig. 7.** Version III: Rerandomizing the GSW ciphertext.

sion III uses a technique introduced in [36] that re-randomizes the GSW ciphertext before dual-GSW homomorphic decryption, as described in Fig. 7. The re-randomization uses sufficiently wide random Gaussian matrices $\mathbf{R}^* = \{\mathbf{R}_i^*\}_{i\in[Q]}$ contained in the URS. In particular, after Step 1) obtaining the GSW ciphertext $\mathsf{hct}_{f_i}$, Step 2) "rerandomizes" the ciphertext to

$$\mathsf{hct}' = \mathsf{hct}_{f_i} + \overline{\mathbf{B}}\mathbf{R}_i^* = \begin{pmatrix}\mathbf{B}\widetilde{\mathbf{R}}_i\\ (\mathbf{r}^\intercal\mathbf{B}+\mathbf{e}_{\mathbf{B}}^\intercal)\widetilde{\mathbf{R}}_i + f_i(\mathbf{r})\end{pmatrix},\quad \text{where } \widetilde{\mathbf{R}}_i = (\mathbf{R}_{f_i}+\mathbf{R}_i^*)$$

Following that, evaluation proceeds identically as in Version II.

*Advantage* We first formulate a distribution $\mathsf{Real}_{\mathrm{v3}}$ from which Version III can be emulated, and show that the LWE encodings in $\mathsf{Real}_{\mathrm{v3}}$ now follow sound circular security rationale.

$$\mathsf{Real}_{\mathrm{v3}}:\ \mathsf{encodings} = \left(\mathsf{hpk}=\overline{\mathbf{B}},\ \mathsf{hct}(\mathbf{r}),\ \{\mathsf{hct}_{0,i}=\overline{\mathbf{B}}\widetilde{\mathbf{R}}_i\},\ \mathbf{D},\ \{\widehat{\mathbf{c}}_i\},\ \mathbf{A},\mathsf{dct}\right),\ \mathsf{hint}=\{\mathbf{R}_i^*\}$$
$$\text{where } \widetilde{\mathbf{R}}_i = \mathbf{R}_{f_i}+\mathbf{R}_i^*,\ \widehat{\mathbf{c}}_i = \mathbf{r}^\intercal\mathbf{D}_i+\widehat{\mathbf{e}}_i^\intercal-\mathbf{u}_i^\intercal\mathbf{G},\ \mathbf{u}_i^\intercal\mathbf{G} = \mathsf{vec}(\mathbf{G}^{-1}(-\mathbf{B}\widetilde{\mathbf{R}}))^\intercal\mathbf{U}^\intercal\mathbf{G} = f^{\mathrm{circ}}(\mathbf{U},\mathsf{hct}_0)\ .$$

Additionally, $(\mathsf{hpk},\mathsf{hct}(\mathbf{r}),\mathbf{D},\mathbf{A},\mathsf{dct},\mathbf{R}^*)$ are sampled, and $\mathbf{R}_{f_i},\mathbf{u}_i$ computed just as in Version III. To emulate the full distribution of Version III, a reduction $\mathcal{R}_3$ given a sample from $\mathsf{Real}_{\mathrm{v3}}$ needs to emulate the missing terms $(\tilde{\mathbf{s}}_i,\tilde{\mathbf{e}}_i,\mathbf{c}_i,\mathbf{c}_{\mathbf{s},i})$

similarly to $\mathcal{R}_2$. Because the distribution of $\tilde{\mathbf{s}}_i, \tilde{\mathbf{e}}_i$ are random and independent of all the components in $\mathsf{Real}_{\mathrm{v3}}$, they can be sampled by $\mathcal{R}_3$ internally, $\mathbf{c}_{\mathbf{s},i}$ is emulated by $\widehat{\mathbf{c}}_i + \tilde{\mathbf{s}}_i^{\mathsf{T}}\mathbf{G}$ as in Eq. (8), and $\mathbf{c}_i$ is emulated according to the new correctness condition (Eq. (10)):

$$\textbf{New } \mathbf{c}_i \textbf{ emulation:} \quad \mathbf{c}_i = (\tilde{\mathbf{s}}_i^{\mathsf{T}}\mathbf{A} + \tilde{\mathbf{e}}_i^{\mathsf{T}}) - \underline{\mathsf{hct}_{0,i}} - \mathsf{dct}_i \pmod{\Delta} \tag{11}$$

Thanks to re-randomization, the LWE encodings $\mathsf{encodings}$ in $\mathsf{Real}_{\mathrm{v3}}$ are now safe circular encoding. $\mathsf{hct}(\mathbf{r}), \mathsf{hct}_{0,i}, \mathsf{dct}$ are standard circular encodings. We further observe that $\widehat{\mathbf{c}}_i$ now encrypts a message $\mathbf{u}_i$ using *independent* randomness $(\mathbf{D}, \widehat{\mathbf{e}})$. This is because $\mathbf{u}_i$ depends on $\mathbf{U}$ and $\mathbf{B}\widetilde{\mathbf{R}}_i$. Thanks to smudging, $\widetilde{\mathbf{R}}_i = \mathbf{R}_{f_i} + \mathbf{R}_i^*$ is a random Gaussian matrix and hence $\mathbf{u}_i$ is independent of $\mathbf{D}$ and $\widehat{\mathbf{e}}$. Therefore, by circular security rationale, the $\mathsf{encodings}$ alone is pseudorandom. This overcomes the drawback of Version II.

*Our Pseudorandom LWE-with-hints Assumption:* We explore whether the LWE encodings $\mathsf{encodings}$ is still pseudorandom, at the presence of $\mathsf{hint}$, by formulating an LWE-with-hints assumption. While $\mathsf{encodings}$ alone is pseudorandom by circular security, and $\mathbf{R}_i^*$'s are marginally random, their joint distribution is subject to a constraint implied by the correctness condition of Version III. Hence, the main question is when $\mathsf{encodings}$ is switched to random in an ideal distribution, how should the distribution of $\mathbf{R}_i^*$ change accordingly to ensure that the constraint is still satisfied?

Let's examine the distribution of $\mathbf{R}_i^*$. In the real distribution $\mathsf{Real}_{\mathrm{v3}}$, it is a random Gaussian matrix subject to the following constraint:

$$\mathbf{R}_i^* \leftarrow \mathcal{D}_{\sigma_0}^{m\times\ell}, \ \textit{conditioned on } \mathsf{hct}_{f_i} + \overline{\mathbf{B}}\mathbf{R}_i^* = \mathsf{hct}_{0,i} + \begin{pmatrix} \mathbf{0} \\ f_i(\mathbf{r}) \end{pmatrix}$$

Furthermore, the correctness equality of Version III is equivalent to an equality showing that $f_i(\mathbf{r})$ can be computed publicly from existing LWE encodings $(\mathsf{hct}_{0,i}, \widehat{\mathbf{c}}_i, \mathsf{dct})$ with overwhelming probability.

We can now formulate our pseudorandom LWE-with-hints assumption:

$$\begin{aligned} \mathsf{encodings} &= \left( \mathsf{hpk} = \overline{\mathbf{B}},\ \mathsf{hct}(\mathbf{r}),\ \{\mathsf{hct}_{0,i} = \overline{\mathbf{B}}\widetilde{\mathbf{R}}_i\},\ \mathbf{D},\ \{\widehat{\mathbf{c}}_i\},\ \mathbf{A},\ \mathsf{dct} \right), \mathsf{hint} = \{\mathbf{R}_i^*\} \\ \approx \mathsf{encodings} &= \left( \$,\ \$,\ \{\$\},\ \$,\ \{\$\},\ \$,\ \$ \right), \mathsf{hint} = \{\mathbf{R}_i^*\} \end{aligned}$$

$$\text{where } \mathbf{R}_i^* \leftarrow \mathcal{D}_{\sigma_0}^{m\times\ell}, \ \textit{conditioned on } \mathsf{hct}_{f_i} + \overline{\mathbf{B}}\mathbf{R}_i^* = \mathsf{hct}_{0,i} + \begin{pmatrix} \mathbf{0} \\ \widetilde{f}_i(\mathsf{hct}_{0,i}, \widehat{\mathbf{c}}_i, \mathsf{dct}) \end{pmatrix}$$

Note that the constraint on $\mathbf{R}^*$ is efficiently verifiable. In the real distribution, the $\mathsf{encodings}$ contains honestly generated LWE encodings, and $\mathbf{R}^*$ follows the Gaussian distribution subject to the constraint, while in the ideal distribution, $\mathsf{encodings}$ is truly random and $\mathbf{R}^*$ is still Gaussian subject to the constraint. Furthermore, the marginal distribution of $\mathbf{R}_i^*$ is truly random Gaussian in the real distribution (Theorem 2.6), and is pseudorandom Gaussian in the ideal distribution (Theorem 2.7). Our assumption postulates that these two distributions

are indistinguishable. We show that it resists existing attacks and cryptanalytic techniques in Sect. 2.3.

*Simulation Security:* Our assumption immediately enables proving simulation security. Given $\tilde{\mathbf{s}}_i^\mathsf{T}\mathbf{A}+\tilde{\mathbf{e}}_i^\mathsf{T}$, a simulator simulates the LWE encodings and the CRS in Version III as follows: It samples $\mathsf{encodings}$ at random and $\mathbf{R}_i^*$ as in the ideal distribution. Note that sampling $\mathbf{R}_i^*$ as Gaussian with width $\sigma_0$ conditioned on $\overline{\mathbf{B}}\mathbf{R}_i^*$ being equal to a target matrix is efficient if $\overline{\mathbf{B}}$ in $\mathsf{encodings}$ is sampled together with a trapdoor. Then the simulator invokes $\mathcal{R}_3$ to simulate the rest components in Version III. We note that the output LWE samples $\tilde{\mathbf{s}}_i^\mathsf{T}\mathbf{A}+\tilde{\mathbf{e}}_i^\mathsf{T}$ are "programmed" in $\mathbf{R}_i^*$ in the CRS (note this is the alternative simulation strategy of GSW).

**Construction of Functional Encoding:** Once we have an oblivious LWE sampler, it becomes easy to construct a functional encoding. The high-level idea is that the CRS of the functional encoding is exactly the CRS of the oblivious LWE sampler, namely $\mathbf{R}^*$. The functional encoding of an input $\mathbf{x}$ includes all the encodings in the oblivious LWE sampler, and additionally a dual-GSW ciphertext of the binary input $\mathbf{x}$.

$$\mathsf{dct}(\mathbf{x}) = \mathbf{W}^\mathsf{T}\mathbf{A} + \mathbf{E}_\mathbf{x} + \mathbf{x}\otimes\mathbf{G}_\ell^\mathsf{T} \overset{\mathsf{dGSW\_Eval}}{\Longrightarrow} \mathsf{dct}_{g_i} = \mathbf{w}_{g_i}^\mathsf{T}\mathbf{A} + \mathbf{e}_{g_i}^\mathsf{T} + g_i(\mathbf{x})^\mathsf{T},\ \text{for } g_i(\mathbf{x}) \in \mathbb{Z}_q^\ell$$

Using the homomorphic evaluation of dual-GSW, we can obtain a ciphertext of the output $g_i(\mathbf{x}) \in \mathbb{Z}_q^\ell$. To reveal the output, instead of opening $\mathbf{w}_{g_i}$ which compromises security, we re-randomize $\mathsf{dct}_{g_i}$ using the obliviously sampled LWE samples and open $\mathbf{w}_{g_i}+\tilde{\mathbf{s}}_i$, which reveals $g_i(\mathbf{x})+\mathbf{e}_{g_i}+\tilde{\mathbf{e}}_i$ and hence the high order bits of $g_i(\mathbf{x})$. Thanks to the fact that $\tilde{\mathbf{s}}_i, \tilde{\mathbf{e}}_i$ are pseudorandom, $\mathbf{w}_{g_i}$ and $\mathbf{e}_{g_i}$ are now hidden. By a similar simulation strategy as above, we can show simulation security of the functional encoding.

As a remark, one can remove the connecting components $\{\mathbf{c}_i^\mathsf{T} = (\mathbf{s}_i^\mathsf{T}\mathbf{A}+\mathbf{e}_i^\mathsf{T} \bmod \Delta\}_i$ from the functional encoding construction by choosing appropriate parameters[8]. This slightly simplifies the construction and improves the efficiency. On the other hand, these connecting terms are crucial for constructing oblivious LWE sampling. In the full version [49], we also construct oblivious LWE sampler and functional encoding from a weaker indistinguishability variant of $\mathsf{CRO}$.

**Acknowledgment.** The authors would like to thank Hoeteck Wee for many insightful discussions about evasive LWE assumptions, and attacks on assumptions underlying lattice-based $\mathsf{iO}$ and $\mathsf{PrO}$ candidates. The authors also would like to thank the anonymous reviewers for insightful observations and comments. Yao Ching Hsieh and Huijia Lin were supported by NSF grant CNS-2026774, and a Simons Collaboration on the Theory of Algorithmic Fairness. Aayush Jain was supported by a Google Faculty Research Scholar 2023, a Stellar Foundation Grant, CYLAB of CMU, and an NSF CAREER CNS-2441647.

[8] We thank the anonymous reviewer for pointing out this observation.

# References


1. Agrawal, S.: Indistinguishability obfuscation without multilinear maps: new methods for bootstrapping and instantiation. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019. LNCS, vol. 11476, pp. 191–225. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17653-2_7
2. Agrawal, S., Kumari, S., Yamada, S.: Pseudorandom multi-input functional encryption and applications. Cryptology ePrint Archive, Paper 2024/1720 (2024). https://eprint.iacr.org/2024/1720
3. Agrawal, S., Pellet-Mary, A.: Indistinguishability obfuscation without maps: attacks and fixes for noisy linear FE. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12105, pp. 110–140. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45721-1_5
4. Ananth, P., Jain, A., Lin, H., Matt, C., Sahai, A.: Indistinguishability obfuscation without multilinear maps: new paradigms via low degree weak pseudorandomness and security amplification. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11694, pp. 284–332. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26954-8_10
5. Ananth, P., Jain, A., Sahai, A.: Indistinguishability obfuscation without multilinear maps: iO from LWE, bilinear maps, and weak pseudorandomness. Cryptology ePrint Archive, Report 2018/615 (2018). https://eprint.iacr.org/2018/615
6. Ananth, P., Sahai, A.: Projective arithmetic functional encryption and indistinguishability obfuscation from degree-5 multilinear maps. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10210, pp. 152–181. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56620-7_6
7. Ananth, P.V., Gupta, D., Ishai, Y., Sahai, A.: Optimizing obfuscation: avoiding Barrington's theorem. In: Ahn, G.J., Yung, M., Li, N. (eds.) ACM CCS 2014. pp. 646–658. ACM Press (2014). https://doi.org/10.1145/2660267.2660342
8. Badrinarayanan, S., Miles, E., Sahai, A., Zhandry, M.: Post-zeroizing obfuscation: new mathematical tools, and the case of evasive circuits. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 764–791. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_27
9. 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
10. Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S., Yang, K.: 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
11. Barak, B., Hopkins, S.B., Jain, A., Kothari, P., Sahai, A.: Sum-of-squares meets program obfuscation, revisited. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019. LNCS, vol. 11476, pp. 226–250. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17653-2_8
12. Bartusek, J., Ishai, Y., Jain, A., Ma, F., Sahai, A., Zhandry, M.: Affine determinant programs: a framework for obfuscation and witness encryption. In: Vidick, T. (ed.) ITCS 2020. vol. 151, pp. 82:1–82:39. LIPIcs (2020). https://doi.org/10.4230/LIPIcs.ITCS.2020.82

13. Bitansky, N., Paneth, O., Rosen, A.: On the cryptographic hardness of finding a Nash equilibrium. In: Guruswami, V. (ed.) 56th FOCS, pp. 1480–1498. IEEE Computer Society Press (2015). https://doi.org/10.1109/FOCS.2015.94
14. Boneh, D., Wu, D.J., Zimmerman, J.: Immunizing multilinear maps against zeroizing attacks. Cryptology ePrint Archive, Report 2014/930 (2014). https://eprint.iacr.org/2014/930
15. Brakerski, Z., Döttling, N., Garg, S., Malavolta, G.: Candidate iO from homomorphic encryption schemes. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12105, pp. 79–109. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45721-1_4
16. Brakerski, Z., Döttling, N., Garg, S., Malavolta, G.: Factoring and pairings are not necessary for IO: Circular-secure LWE suffices. In: Bojanczyk, M., Merelli, E., Woodruff, D.P. (eds.) ICALP 2022. LIPIcs, vol. 229, pp. 28:1–28:20. Schloss Dagstuhl (2022). https://doi.org/10.4230/LIPIcs.ICALP.2022.28
17. Brakerski, Z., Gentry, C., Halevi, S., Lepoint, T., Sahai, A., Tibouchi, M.: Cryptanalysis of the quadratic zero-testing of GGH. Cryptology ePrint Archive, Report 2015/845 (2015). https://eprint.iacr.org/2015/845
18. 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
19. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: Ostrovsky, R. (ed.) 52nd FOCS. pp. 97–106. IEEE Computer Society Press, October 2011. https://doi.org/10.1109/FOCS.2011.12
20. Branco, P., et al.: Pseudorandom obfuscation and applications. Cryptology ePrint Archive, Paper 2024/1742 (2024). https://eprint.iacr.org/2024/1742
21. Brzuska, C., Ünal, A., Woo, I.K.Y.: Evasive LWE assumptions: definitions, classes, and counterexamples. In: ASIACRYPT 2024. LNCS, vol. 15487, pp. 418–449. Springer, Cham (2024). https://doi.org/10.1007/978-981-96-0894-2_14
22. Brzuska, C., Farshim, P., Mittelbach, A.: Indistinguishability obfuscation and UCEs: the case of computationally unpredictable sources. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 188–205. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44371-2_11
23. Canetti, R., Chamon, C., Mucciolo, E.R., Ruckenstein, A.E.: Towards general-purpose program obfuscation via local mixing. In: Boyle, E., Mahmoody, M. (eds) Theory of Cryptography. TCC 2024. LNCS, vol. 15367, pp. 37–70. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-78023-3_2
24. Cheon, J.H., Han, K., Lee, C., Ryu, H., Stehlé, D.: Cryptanalysis of the multilinear map over the integers. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 3–12. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_1
25. Cheon, J.H., Lee, C., Ryu, H.: Cryptanalysis of the new CLT multilinear maps. Cryptology ePrint Archive, Report 2015/934 (2015). https://eprint.iacr.org/2015/934
26. Cohen, A., Holmgren, J., Nishimaki, R., Vaikuntanathan, V., Wichs, D.: Watermarking cryptographic capabilities. In: Wichs, D., Mansour, Y. (eds.) 48th ACM STOC, pp. 1115–1127. ACM Press, June 2016. https://doi.org/10.1145/2897518.2897651
27. Coron, J.-S., et al.: Zeroizing without low-level zeroes: new MMAP attacks and their limitations. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 247–266. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_12

28. Coron, J.-S., Lepoint, T., Tibouchi, M.: Practical multilinear maps over the integers. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 476–493. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_26
29. Coron, J.-S., Lepoint, T., Tibouchi, M.: New multilinear maps over the integers. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 267–286. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_13
30. Devadas, L., Quach, W., Vaikuntanathan, V., Wee, H., Wichs, D.: Succinct LWE sampling, random polynomials, and obfuscation. In: Nissim, K., Waters, B. (eds.) TCC 2021. LNCS, vol. 13043, pp. 256–287. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-90453-1_9
31. Döttling, N., Garg, S., Gupta, D., Miao, P., Mukherjee, P.: Obfuscation from low noise multilinear maps. In: Chakraborty, D., Iwata, T. (eds.) INDOCRYPT 2018. LNCS, vol. 11356, pp. 329–352. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-05378-9_18
32. 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
33. Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., Waters, B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: 54th FOCS, pp. 40–49. IEEE Computer Society Press, October 2013. https://doi.org/10.1109/FOCS.2013.13
34. Garg, S., Pandey, O., Srinivasan, A.: Revisiting the cryptographic hardness of finding a Nash equilibrium. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9815, pp. 579–604. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_20
35. Gay, R., Jain, A., Lin, H., Sahai, A.: Indistinguishability obfuscation from simple-to-state hard problems: new assumptions, new techniques, and simplification. In: Canteaut, A., Standaert, F.-X. (eds.) EUROCRYPT 2021. LNCS, vol. 12698, pp. 97–126. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77883-5_4
36. Gay, R., Pass, R.: Indistinguishability obfuscation from circular security. In: Khuller, S., Williams, V.V. (eds.) 53rd ACM STOC, pp. 736–749. ACM Press, June 2021. https://doi.org/10.1145/3406325.3451070
37. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Mitzenmacher, M. (ed.) 41st ACM STOC, pp. 169–178. ACM Press, May/June 2009. https://doi.org/10.1145/1536414.1536440
38. Gentry, C., Gorbunov, S., Halevi, S.: Graph-induced multilinear maps from lattices. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015. LNCS, vol. 9015, pp. 498–527. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46497-7_20
39. Gentry, C., Jutla, C.S., Kane, D.: Obfuscation using tensor products. Cryptology ePrint Archive, Report 2018/756 (2018). https://eprint.iacr.org/2018/756
40. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 75–92. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_5
41. Goldwasser, S., et al.: Multi-input functional encryption. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 578–602. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_32
42. Goldwasser, S., Kalai, Y.T., Rothblum, G.N.: One-time programs. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 39–56. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_3

43. Goyal, R., Koppula, V., Waters, B.: Lockable obfuscation. In: Umans, C. (ed.) 58th FOCS, pp. 612–621. IEEE Computer Society Press (Oct 2017). https://doi.org/10.1109/FOCS.2017.62
44. Goyal, R., Koppula, V., Waters, B.: Separating semantic and circular security for symmetric-key bit encryption from the learning with errors assumption. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10211, pp. 528–557. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56614-6_18
45. Halevi, S.: Graded encoding, variations on a scheme. Cryptology ePrint Archive, Report 2015/866 (2015). https://eprint.iacr.org/2015/866
46. Hofheinz, D., Jager, T., Khurana, D., Sahai, A., Waters, B., Zhandry, M.: How to generate and use universal samplers. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 715–744. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_24
47. Hohenberger, S., Sahai, A., Waters, B.: Full domain hash from (leveled) multilinear maps and identity-based aggregate signatures. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 494–512. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_27
48. Hopkins, S., Jain, A., Lin, H.: Counterexamples to new circular security assumptions underlying iO. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021. LNCS, vol. 12826, pp. 673–700. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-84245-1_23
49. Hsieh, Y., Jain, A., Lin, H.: Lattice-based post-quantum iO from circular security with random opening assumption (part II: zeroizing attacks against private-coin evasive LWE assumptions). Cryptology ePrint Archive, Paper 2025/390 (2025). https://eprint.iacr.org/2025/390
50. Hu, Y., Jia, H.: Cryptanalysis of GGH map. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9665, pp. 537–565. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49890-3_21
51. Jain, A., Lin, H., Lou, P., Sahai, A.: Polynomial-time cryptanalysis of the subspace flooding assumption for post-quantum $i\mathcal{O}$. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023. LNCS, vol. 14004, pp. 205–235. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-30545-0_8
52. Jain, A., Lin, H., Matt, C., Sahai, A.: How to leverage hardness of constant-degree expanding polynomials over $\mathbb{R}$ to build $i\mathcal{O}$. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019. LNCS, vol. 11476, pp. 251–281. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17653-2_9
53. Jain, A., Lin, H., Sahai, A.: Indistinguishability obfuscation from well-founded assumptions. In: Khuller, S., Williams, V.V. (eds.) 53rd ACM STOC, pp. 60–73. ACM Press, June 2021. https://doi.org/10.1145/3406325.3451093
54. Jain, A., Lin, H., Sahai, A.: Indistinguishability obfuscation from LPN over $\mathbb{F}_p$, DLIN, and PRGs in $NC^0$. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022. LNCS, vol. 13275, pp. 670–699. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-06944-4_23
55. Koppula, V., Lewko, A.B., Waters, B.: Indistinguishability obfuscation for Turing machines with unbounded memory. In: Servedio, R.A., Rubinfeld, R. (eds.) 47th ACM STOC, pp. 419–428. ACM Press, June 2015. https://doi.org/10.1145/2746539.2746614
56. 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 (May 2016). https://doi.org/10.1007/978-3-662-49890-3_2

57. 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
58. Lin, H., Matt, C.: Pseudo flawed-smudging generators and their application to indistinguishability obfuscation. Cryptology ePrint Archive, Report 2018/646 (2018). https://eprint.iacr.org/2018/646
59. Lin, H., Pass, R., Seth, K., Telang, S.: Indistinguishability obfuscation with non-trivial efficiency. In: Cheng, C.-M., Chung, K.-M., Persiano, G., Yang, B.-Y. (eds.) PKC 2016. LNCS, vol. 9615, pp. 447–462. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49387-8_17
60. Lin, H., Tessaro, S.: Indistinguishability obfuscation from trilinear maps and block-wise local PRGs. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 630–660. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_21
61. Lin, H., Vaikuntanathan, V.: Indistinguishability obfuscation from DDH-like assumptions on constant-degree graded encodings. In: Dinur, I. (ed.) 57th FOCS, pp. 11–20. IEEE Computer Society Press, October 2016. https://doi.org/10.1109/FOCS.2016.11
62. Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_41
63. 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. LNCS, vol. 9815, pp. 629–658. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_22
64. Minaud, B., Fouque, P.A.: Cryptanalysis of the new multilinear map over the integers. Cryptology ePrint Archive, Report 2015/941 (2015). https://eprint.iacr.org/2015/941
65. Pass, R., Seth, K., Telang, S.: Indistinguishability obfuscation from semantically-secure multilinear encodings. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 500–517. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44371-2_28
66. Ragavan, S., Vafa, N., Vaikuntanathan, V.: Indistinguishability obfuscation from bilinear maps and LPN variants. In: Boyle, E., Mahmoody, M. (eds) Theory of Cryptography. TCC 2024. LNCS, vol. 15367, pp. 3–36. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-78023-3_1
67. Sahai, A., Waters, B.: How to use indistinguishability obfuscation: deniable encryption, and more. In: Shmoys, D.B. (ed.) 46th ACM STOC, pp. 475–484. ACM Press, May/June 2014. https://doi.org/10.1145/2591796.2591825
68. Tsabary, R.: Candidate witness encryption from lattice techniques. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022. LNCS, vol. 13507, pp. 535–559. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-15802-5_19
69. Vaikuntanathan, V., Wee, H., Wichs, D.: Witness encryption and null-IO from evasive LWE. In: Agrawal, S., Lin, D. (eds.) ASIACRYPT 2022. LNCS, vol. 13791, pp. 195–221. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-22963-3_7
70. Wee, H.: Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022. LNCS, vol. 13276, pp. 217–241. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-07085-3_8

71. Wee, H., Wichs, D.: Candidate obfuscation via oblivious LWE sampling. In: Canteaut, A., Standaert, F.-X. (eds.) EUROCRYPT 2021. LNCS, vol. 12698, pp. 127–156. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77883-5_5
72. Wichs, D., Zirdelis, G.: Obfuscating compute-and-compare programs under LWE. In: Umans, C. (ed.) 58th FOCS, pp. 600–611. IEEE Computer Society Press, October 2017. https://doi.org/10.1109/FOCS.2017.61