# Post-quantum PKE from Unstructured Noisy Linear Algebraic Assumptions: Beyond LWE and Alekhnovich's LPN

Riddhi Ghosal[1(✉)], Aayush Jain[2], Paul Lou[1(✉)], Amit Sahai[1], and Neekon Vafa[3]

[1] UCLA, Los Angeles, CA, USA
{postboxriddhi,paul96lou}@gmail.com
[2] CMU, Pittsburgh, PA, USA
[3] MIT, Cambridge, MA, UK

**Abstract.** Noisy linear algebraic assumptions with respect to random matrices, in particular Learning with Errors (LWE) and Alekhnovich Learning Parity with Noise (Alekhnovich LPN), are among the most investigated assumptions that imply post-quantum public-key encryption (PKE). They enjoy elegant mathematical structure. Indeed, efforts to build post-quantum PKE and advanced primitives such as homomorphic encryption and indistinguishability obfuscation have increasingly focused their attention on these two assumptions and their variants.

Unfortunately, this increasing reliance on these two assumptions for building post-quantum cryptography leaves us vulnerable to potential quantum (and classical) attacks on Alekhnovich LPN and LWE. Quantum algorithms is a rapidly advancing area, and we must stay prepared for unexpected cryptanalytic breakthroughs. Just three decades ago, a short time frame in the development of our field, Shor's algorithm rendered most then-popular number theoretic and algebraic assumptions quantumly broken. Furthermore, within the last several years, we have witnessed major classical and quantum breaks on several assumptions previously introduced for post-quantum cryptography. Therefore, we ask the following question:

*In a world where both* LWE *and Alekhnovich* LPN *are broken, can there still exist noisy linear assumptions that remain plausibly quantum hard and imply PKE?*

To answer this question positively, we introduce two natural noisy-linear algebraic assumptions that are both with respect to random matrices, exactly like LWE and Alekhnovich LPN, but with different error distributions. Our error distribution combines aspects of both small norm and sparse error distributions. We design a PKE from these assumptions and give evidence that these assumptions are likely to still be secure even in a world where both the LWE and Alekhnovich LPN assumptions are simultaneously broken. We also study basic properties of these assumptions, and show that in the parameter settings we employ to build PKE, neither of them are "lattice" assumptions in the sense that we don't see


S. Fehr and P.-A. Fouque (Eds.): EUROCRYPT 2025, LNCS 15602, pp. 64–93, 2025.
https://doi.org/10.1007/978-3-031-91124-8_3

a way to attack them using a lattice closest vector problem solver, except via NP-completeness reductions.

## 1 Introduction

Constructing post-quantum public-key encryption (PKE) is of the utmost concern due to the possibility of practical quantum computing in the near future. Over the past two decades, there has been growing interest in post-quantum PKE from noisy linear algebraic assumptions, namely assumptions of the form $(\mathbf{A}, \mathbf{As}+\mathbf{e})$ being computationally indistinguishable from $(\mathbf{A}, \mathbf{u})$ for polynomial-time adversaries, where $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ is a uniform random expanding matrix $(m > n)$, $\mathbf{s}$ is uniform over $\mathbb{F}_q^n$, $\mathbf{u}$ is uniform over $\mathbb{F}_q^m$, and $\mathbf{e} \in \mathbb{F}_q^m$ is "noise" that satisfies some structural constraint. Two key assumptions in this category are (1) Learning with Errors (LWE) [29] where the error vector $\mathbf{e}$ has small integer entries from a discrete gaussian distribution centered at zero, and (2) Alekhnovich's setting for Learning Parity with Noise [1] (Alekhnovich LPN) where $\mathbf{e}$ is a sparse vector with roughly $mn^{-\frac{1}{2}}$ many non-zero entries that are uniform over $\mathbb{F}_q$. In general, LPN is said to be $\delta$-dense if the probability of non-zero entries is $n^{-\delta}$, and Alekhnovich's LPN is the special case of $\delta = \frac{1}{2}$. The simple mathematical structure of these two noisy linear algebraic assumptions, involving only *unstructured* noisy linear equations over finite fields is versatile for designing cryptographic primitives (see, e.g. [3–5,13–16,19,28,35,36]).

How worried should we be about a (quantum) break on assumptions such as LWE and Alekhnovich LPN? The short history of modern cryptography teaches us that it is vital to prepare ourselves against unexpected cryptanalytic breakthroughs. Only 30 years ago, a minuscule time-frame in the development of a scientific field, Shor's algorithm [33] single-handedly quantumly broke the two most centrally used cryptographic assumptions at the time, the hardness of factoring and the hardness of discrete logarithm. More surprisingly, there have even been classical attacks on isogeny [30] and multivariate quadratic [2] based assumptions that were initially believed to be quantum safe. Therefore, as things stand, we have very few well-studied assumptions that are potentially quantum safe, let alone being suitable for constructing PKE. Moreover, in recent times, there have been some serious (albeit failed) attempts to break LWE quantumly [8,12] and quantum speed-ups against certain LPN type assumptions [17,32]. At the same time, noisy linear algebraic assumptions have proven extremely versatile. Given that our understanding of quantum algorithms is nascent and that quantum algorithms is a rapidly advancing area of study, it is imperative to explore new presumably quantum safe noisy linear algebraic assumptions beyond LWE and LPN. In the context of this discussion, we address the following primary question in this work:

*In a world where both* LWE *and Alekhnovich* LPN *are polynomially broken, are there noisy linear assumptions that remain plausibly quantum polynomially-hard and imply PKE?*

In this work, we provide evidence that the answer is yes, indeed for assumptions that only assume polynomial hardness. We introduce two noisy linear algebraic assumptions that *together* imply PKE in a parameter regime in which *both* assumptions are potentially quantum-secure even if *both* LWE and Alekhnovich LPN are (quantum)-broken.

Indeed for our two new assumptions, we give evidence that they are not subject to complexity-theoretic reductions to lattice assumptions nor to typical cryptanalytical strategies applicable to lattice assumptions. On the other hand, we also give evidence that only by decoding random linear codes from sparse errors that are well beyond the Alekhnovich barrier ($\delta = \frac{1}{2}$) in terms of density, can our new assumptions be plausibly attacked.

Moreover, exactly like LWE and LPN as described above, our assumptions are also defined with respect to polynomial-time adversaries and truly random and *unstructured* matrices $\mathbf{A}$, differing only in the noise model. This is in contrast to structured variants of LWE and LPN such as sparse [7,10,11], ring [9,18,21,22,27] and McEliece's [23] variants of these assumptions, which have previously leveraged their structure, or $2^{\omega(n^{1/2})}$-subexponentially strong LPN assumptions [37] to give PKE constructions beyond the Alekhnovich barrier [1].

Furthermore, our construction of PKE from our new assumptions is natural and exploits a new kind of asymmetry, as we will describe shortly. We now describe both of our assumptions:

1. The **Learning with Two Errors (LW2E)** assumption consists of unstructured linear equations perturbed by both an LWE error term and an LPN sparse error term (over $\mathbb{F}_q$), i.e., it has the form $\mathbf{As} + \mathbf{e}$ where $\mathbf{e} = \mathbf{e}_1 + \mathbf{e}_2$. Here $\mathbf{e}_1$ is the short LWE error and $\mathbf{e}_2$ is the sparse LPN error. The aggregate error term is therefore neither sparse nor small. From a complexity-theoretic viewpoint, we prove that this assumption is at least as hard as both LWE and Alekhnovich LPN, while intuitively being strictly harder than both. We concretely support this intuition in Sect. 5, where we provide strong evidence that hardness would be preserved even in the presence of oracles that could break both LWE and Alekhnovich LPN.
2. The **Denser-than-Alekhnovich Learning with Short and Sparse Errors assumption (LWSSE)** consists of perturbing uniform random linear equations by a sparse error $\mathbf{e}$ that has a small $\ell_2$-norm error but that is denser than the Alekhnovich regime. We introduce the assumption in the parameter regime where the matrix $\mathbf{A} \in \mathbb{F}_q^{(m-n)\times m}$ is nearly square, that is with secret dimension $(m-n)$ and sample count $m$. It is convenient to think of the density parameter as 0.1 (much denser than the Alekhnovich 0.5 setting); that is, with probability $(m-n)^{-0.1}$ an error coordinate is non-zero. The parameters used to construct our PKE have been chosen particularly to ensure that they are (1) beyond the Alekhnovich regime and (2) outside of the regime in which LWSSE reduces to LW2E or LWE.

   We also introduce an equivalent dual form of this assumption called the Inhomogeneous Short and Sparse Integer Solution (ISSIS) which is inspired from the dual analogue of the LWE problem, namely that Inhomogeneous

Shortest Integer Solution (ISIS). As a decision problem, ISSIS states that $(\mathbf{A}^\perp, \mathbf{e}^\top \mathbf{A}^\perp)$ is computationally indistinguishable from $(\mathbf{A}^\perp, \mathbf{u})$ for uniform random $\mathbf{u} \in \mathbb{F}_q^n$ and $\mathbf{A}^\perp : \mathbf{A}\mathbf{A}^\perp = 0$. Similar to ISIS, this problem also has a "total" regime where the decision problem is information theoretically hard. However, as we detail shortly, we will always operate with parameters in the "planted" regime where the decision problem is only computationally hard.

A more detailed overview on the hardness and complexity-theoretic relations of these two assumptions will be discussed in Sect. 1.2. We now elaborate on how we combine the two assumptions to construct our PKE.

### 1.1 PKE from LW2E and LWSSE Beyond LWE and Alekhnovich

The well-known PKE constructions from LWE due to Regev [29] and from LPN due to Alekhnovich [1] follow a similar template. Typically, these constructions rely on the special structure of the error vector. In particular, the crucial property that ensures decryption correctness is the following: (1) In the case of LWE, the inner product of two vectors with small entries is small compared to the prime modulus $q$, and (2) In the case of LPN, when you take the inner product of two sparse vectors, the non-zero entries of one vector are likely to coincide with the zero entries of the other, if the sparsity parameters are chosen carefully, thereby resulting in 0. The following is a general blueprint that we follow as well:

- Key Generation: Sample a random $\mathbf{A} \in \mathbb{F}_q^{m \times n}$, a random $\mathbf{s} \in \mathbb{F}_q^n$ and an error vector $\mathbf{e} \in \mathbb{F}_q^m$ as per the distribution defined by a noisy linear assumption. Set $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ as the public key $\mathsf{pk}$ and set $\mathbf{s}, \mathbf{e}$ as the secret key $\mathsf{sk}$.
- Encryption: To encrypt a 1, sample a uniform random $\mathbf{u}_1 \in \mathbb{F}_q^n$ and $u_2 \in \mathbb{F}_q$ and output $(\mathbf{u}_1, u_2)$. To encrypt a 0, sample a another random $\mathbf{r}$ from *the error distribution of a noisy linear assumption* and output $(\mathsf{ct}_1^\top = \mathbf{r}^\top \mathbf{A}, \mathsf{ct}_2 = \mathbf{r}^\top \mathbf{b})$.
- Decryption: Compute $\mathsf{ct}_2 - \mathsf{ct}_1^\top \mathbf{s}$. If the result is below some pre-determined threshold, then output 0; otherwise output 1.

Correctness of this construction intuitively works because $\mathsf{ct}_2 - \mathsf{ct}_1^\top \mathbf{s}$ is going to be uniform random over $\mathbb{F}_q$ if 1 was encrypted. On the other hand, if 0 was encrypted, then $\mathsf{ct}_2 - \mathsf{ct}_1^\top \mathbf{s} = \mathbf{r}^\top \mathbf{e}$. Now if $\mathbf{r}$ and $\mathbf{e}$ are either both small or both sufficiently sparse, then we expect their inner product to be small or zero, respectively, and we can set an appropriate threshold to detect this gap.

The security proof typically has two phases: First to replace $\mathbf{b}$ in the public key to uniform random, i.e., replace $\mathbf{b}$ with a uniform random $\mathbf{u} \in \mathbb{F}_q^m$. At this point, the view of the adversary is of the form $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \mathbf{A}, \mathbf{r}^\top \mathbf{u})$. At a high level, we then need to argue that we can replace $(\mathbf{A} \| \mathbf{u}, \mathbf{r}^\top (\mathbf{A} \| \mathbf{u}))$ with $(\mathbf{A} \| \mathbf{u}, \mathbf{y}^\top)$, where $\mathbf{y}$ is a uniform random vector over $\mathbb{F}_q^n$.

*A First Failed Attempt to Set the Stage.* Since both of our assumptions have the same overarching structure as LWE and LPN, we can of course try to instantiate the above template with either LW2E or ISSIS. Let us begin with the LW2E assumption. In particular, we can replace $\mathbf{e}$ and $\mathbf{r}$ in the above template with $\mathbf{e}_1 +$

$\mathbf{e}_2$ and $\mathbf{r}_1 + \mathbf{r}_2$, respectively, where $\mathbf{e}_1$, $\mathbf{r}_1$ will be from the $\mathsf{LWE}$ error distribution and $\mathbf{e}_2$, $\mathbf{r}_2$ will be from the sparse-but-large error distribution. Immediately, we can see an issue with the decryption correctness. In particular, decryption in the above construction exploits the fact that the inner product of $\mathbf{r}$ with $\mathbf{e}$ will result in some small value. However in the case of $\mathsf{LW2E}$, both $\mathbf{e}_1 + \mathbf{e}_2$ and $\mathbf{r}_1 + \mathbf{r}_2$ are neither small or sparse. Therefore their inner product will likely not be a small value and we cannot get any appropriate threshold that will guarantee decryption with overwhelming probability.

*Idea 1. Exploit Asymmetry:* $\mathbf{r}$ *and* $(\mathbf{e}_1 + \mathbf{e}_2)$ *Need Not be from the Same Distribution!* What if we choose $\mathbf{r}$ from a distribution which is both short and sparse, i.e., the indices where $\mathbf{r}$ is non-zero are sparse and each non-zero entry is $B$-bounded for some $B \ll q$. The hope is that decryption correctness will now work because both $\mathbf{r}$ and $\mathbf{e}_2$ are sparse, as was the case in Alekhnovich, and therefore will likely cancel out, and therefore $\mathbf{r}^\top(\mathbf{e}_1 + \mathbf{e}_2)$ will be equal to $\mathbf{r}^\top \mathbf{e}_1$. Now, it is easy to see that $\mathbf{r}^\top \mathbf{e}_1$ will result in a small value as both vectors individually have small entries. A concern at this point is that we want to do *better* than Alekhnovich – but if we are using sparsity to ensure correctness, how will we surpass the Alekhnovich barrier? As we will see below, asymmetry will save us again! But before we tackle that, let's first consider security.

First we can appeal to the hardness of decisional $\mathsf{LW2E}$ and replace $\mathsf{pk} = (\mathbf{A}, \mathbf{As} + \mathbf{e}_1 + \mathbf{e}_2), \mathsf{ct} = (\mathbf{r}^\top \mathbf{A}, \mathbf{r}^\top(\mathbf{As} + \mathbf{e}_1 + \mathbf{e}_2)))$ with $\mathsf{pk}' = (\mathbf{A}, \mathbf{u}), \mathsf{ct}' = (\mathbf{r}^\top \mathbf{A}, \mathbf{r}^\top \mathbf{u}))$ for some uniform random $\mathbf{u} \in \mathbb{F}_q^m$.

Now, what about the ciphertext? Since $m > n$, can we hope to appeal to the Leftover Hash Lemma as per Regev [29]? If so, we could conclude that $((\mathbf{A} \| \mathbf{u}), \mathbf{r}^\top(\mathbf{A} \| \mathbf{u}))$ is statistically indistinguishable from $((\mathbf{A} \| \mathbf{u}), \mathbf{y}^\top)$ where $\mathbf{y}^\top$ is chosen uniformly. However to achieve correctness and security simultaneously, there are two crucial properties that need to be satisfied simultaneously:

1. Increasing the sparsity of $\mathbf{r}$ increases the number of 0 entries, and therefore reduces the entropy of $\mathbf{r}$. If we make the sparsity high enough then we cannot have enough entropy to apply the Leftover Hash Lemma. Thus, we desire $\mathbf{r}$ to be dense enough.
2. On the other hand, increasing the density of $\mathbf{r}$ reduces the chances that $\mathbf{r}^\top \mathbf{e}_2 = 0$. So to ensure decryption correctness, we need the sparsity of $\mathbf{r}$ to be more than a certain threshold.

Unfortunately it turns out that there are no settings of parameters that allow us to achieve both decryption correctness and use the Leftover Hash Lemma. Indeed, a similar issue arises in Alekhnovich [1] as well, and this is exactly where the Alekhnovich $n^{-0.5}$ barrier on density comes from.

*Idea 2. Let's Use Computational Hardness via LWSSE/ISSIS Instead!* This is where the $\mathsf{LWSSE}/\mathsf{ISSIS}$ assumption comes into the picture. Observe that $\mathbf{r}$ here has the same distribution as the secret distribution of $\mathsf{ISSIS}$. Rather than trying to argue statistical indistinguishability of $((\mathbf{A} \| \mathbf{u}), \mathbf{r}^\top(\mathbf{A} \| \mathbf{u}))$ and $((\mathbf{A} \| \mathbf{u}), \mathbf{y}^\top)$ via

the Leftover Hash Lemma, we will appeal to the hardness of decisional ISSIS to assert that the above distributions are computationally indistinguishable, completing the proof of security!

*Idea 3. Beyond the Alekhnovich Barrier via Asymmetry!* Now that we have taken care of security, the immediate question to ask is how can we proceed beyond the Alekhnovich barrier? It seems like we relied on the sparsity of $\mathbf{r}$, and certainly if this vector is $\gamma$-dense for $\gamma \geq 0.5$, then we will be again be stuck in the Alekhnovich regime. In fact, we do show a reduction from LWSSE to LPN with comparable parameter in Lemma 8, therefore it is crucial that we choose $\gamma < 0.5$. But is it possible to do so in our case?

For Alekhnovich LPN-based PKE, one needs to use the LPN assumption twice, i.e., once to replace the public key with random and then to replace the ciphertext with random. Say that the density parameter of the LPN error $\mathbf{e}$ used in the public key is $\delta$. It was shown in [1] that decryption is possible only when $\gamma + \delta \geq 1$, and therefore one cannot hope for anything better than setting $\gamma = \delta = 0.5$. In particular, this *symmetry* in our choice for $\gamma$ and $\delta$ is the optimal choice, since both the dual and primal forms of the LPN assumption are equivalent.

However, in our case the error $\mathbf{e}_1 + \mathbf{e}_2$ in the LW2E assumption is *already* dense due to the presence of the LWE error $\mathbf{e}_1$, which is not at all sparse. Since we do not have any evidence of how to use an LPN breaker to attack noisy linear equations where the noise is very dense, this error distribution seems completely outside the reach of any LPN-based attacks. Therefore we can actually afford to have $\mathbf{e}_2$ that is quite sparse, and specifically we can pick $\delta > 0.5$. This then gives us the freedom to pick $\gamma < 0.5$. In particular there are no other restrictions on the choice of $\gamma$ and $\delta$ beyond $\gamma + \delta \geq 1$, so $\delta = 0.9$ and $\gamma = 0.1$ are perfectly valid choices that move the LWSSE assumption to a density setting far beyond Alekhnovich's LPN. In fact, it is natural to conjecture that any attack that breaks LWSSE with density parameter 0.1 might have consequences on LPN with density parameter 0.1 as well.

And what about lattice attacks? In fact, as we argue below, our choice of parameters will be such that actually there will exist exponentially many vectors that solve the ISSIS equation that are *much smaller* than $\mathbf{r}$, but these "decoy" vectors will be very dense! As a result, even a huge breakthrough in (quantum) lattice-based attacks would discover these "decoy" vectors instead the actual $\mathbf{r}$ vector needed to break our PKE system[1]!

To summarize, in this work, we achieve the following theorem:

**Theorem 1.** *(Informal) Assuming the hardness of the (1) Decisional Learning with Two Errors Problem and (2) Decisional Inhomogeneous Short and Sparse Solutions assumptions, the Public Key Encryption constructed in Sect. 3 is statistically correct and semantically secure.*

We refer to Sect. 3 for a formal and parameterized theorem statement.

[1] A similar situation arises in the context of our LW2E assumption, rendering lattice attacks ineffective.

### 1.2 Parameters and the Hardness of LW2E and LWSSE

Additionally, we also perform a systematic study of the hardness of both assumptions and provide evidence that under our parameter setting, LW2E and LWSSE are potentially hard even in the presence of oracles that can break both LWE and LPN. We first formally restate the hardness assumptions with all the parameters.

**Definition 1 (Decisional Learning With Two Errors Assumption (LW2E)).** *For all $n \in \mathbb{N}$, $m = \mathsf{poly}(n)$, prime $q \in \mathbb{N}$, $\sigma = \mathsf{poly}(n)$, $\delta \in (0,1)$, the decisional learning with two errors assumption (decisional-LW2E), formally parameterized by $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$, states that the following distributions are computationally indistinguishable:*

1. $\left(\mathbf{A} \xleftarrow{\$} \mathbb{F}_q^{m\times n}, \mathbf{As} + \mathbf{e}^{(1)} + \mathbf{e}^{(2)} \pmod q\right)$ *where* $\mathbf{s} \xleftarrow{\$} \mathbb{F}_q^n$, $\mathbf{e}^{(1)} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^m$, *and* $\mathbf{e}^{(2)} \leftarrow \mathcal{S}_{n,q,\delta}^m$.
2. $\left(\mathbf{A} \xleftarrow{\$} \mathbb{F}_q^{m\times n}, \mathbf{b} \xleftarrow{\$} \mathbb{F}_q^m\right)$.

*Here,*

- *$\mathcal{D}_{\mathbb{Z},\sigma}$: For $\sigma \in \mathbb{R}^+$, we let $\mathcal{D}_{\mathbb{Z},\sigma}$ denote the discrete Gaussian distribution over the integer lattice $\mathbb{Z}$ with mean 0 and scale parameter $\sigma > 0$.*
- *$\mathcal{S}_{n,q,\delta}$: For $n, q \in \mathbb{N}, \delta \in (0,1)$, we define $\mathcal{S}_{n,q,\delta}$ to be the distribution samples 0 with probability $1 - n^{-\delta}$ or a uniformly random element from $\mathbb{F}_q$ with probability $n^{-\delta}$.*

**Definition 2 (Decisional Learning With Short and Sparse Errors Assumption (LWSSE)).**

*For all $n \in \mathbb{N}$, $m = \mathsf{poly}(n) > n$, prime $q \in \mathbb{N}$, $\xi = \mathsf{poly}(n)$, $\gamma \in (0,1)$, the decisional learning with short and sparse errors assumption (decisional-LWSSE), formally parameterized by $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$, states that the following distributions are computationally indistinguishable:*

1. $\left(\mathbf{A}^\perp \xleftarrow{\$} \mathbb{F}_q^{(m-n)\times m}, \mathbf{s}^\top\mathbf{A}^\perp + \mathbf{e}^\top \pmod q\right)$ *where* $\mathbf{s} \xleftarrow{\$} \mathbb{F}_q^{m-n}$, $\mathbf{e} \leftarrow \mathcal{E}_{m,n,\xi,\gamma}^m$.
2. $\left(\mathbf{A}^\perp \xleftarrow{\$} \mathbb{F}_q^{(m-n)\times m}, \mathbf{b}^\top \xleftarrow{\$} \mathbb{F}_q^m\right)$.

*Here, we define $\mathcal{E}_{m,n,\xi,\gamma}$ for $m, n, \xi \in \mathbb{N}$, $\gamma \in (0,1)$, with $m > n$, to be the distribution over $\mathbb{Z}$ which samples 0 with probability $1-(m-n)^{-\gamma}$ or a random element from the distribution $\mathcal{D}_{\mathbb{Z},\xi}$ with probability $(m-n)^{-\gamma}$.*

*Our Parameter Settings for* LW2E *and* LWSSE*, for Building PKE.* We will now describe how we set the parameters for our assumptions, in ways that are sufficient for constructing PKE. While these are not the only possible setting of parameters that would achieve the security desired from our PKE, this setting of parameters is easy to understand and achieve all the goals we desire to achieve. We will think of the dimension $n$ as a security parameter, and we will also make use of an arbitrarily small constant $\gamma \in (0, \frac{1}{2})$. Then, we set parameters for LW2E and LWSSE as follows:

– Secret dimension of LW2E: $n = n$.
– ISSIS sparsity parameter: $\gamma = \gamma$.
– Smallness parameter for LW2E noise $\mathbf{e}_1$: $\sigma = n$.
– Sparsity parameter for LW2E noise $\mathbf{e}_2$: $\delta = 1 - \gamma$.
– Dimension of ISSIS secret or number of LW2E samples: $m = 20n$.
– Prime modulus $q \in [m^{10}, 2m^{10}]$.
– ISSIS smallness parameter: $\xi = n^{0.5+\gamma}$.

*Understanding Our Assumptions More Broadly.* In Sect. 4 and Sect. 5, we perform a careful evaluation of the hardness of our newly introduced assumptions. We do so via two general approaches: (1) Show reductions to other lattice problems or LPN with parameters that we **do not use** in our PKE and (2) Explore some natural approaches to attack our assumptions using cryptanalysis of LWE and show why they do not apply to the parameter settings that we do use. We summarize the reductions in Fig. 1 that apply for all settings of parameters, including those that we use in our PKE.

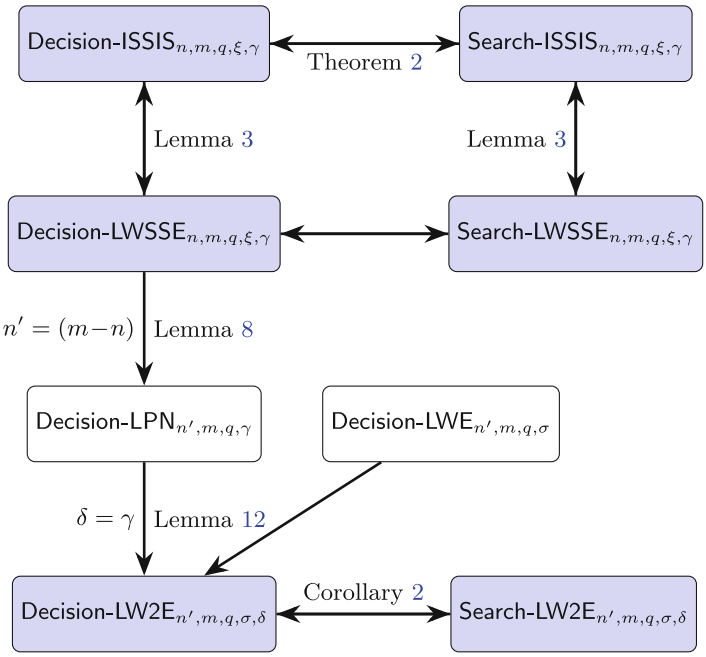


**Fig. 1.** Reductions between the assumptions when we are in the setting of parameters that we use for our PKE. An arrow from assumption $A$ to $B$ implies that an adversary breaking assumption $B$ can be used to break assumption $A$, i.e., reduction from $A$ to $B$. The new assumptions we introduce in this paper are highlighted with a blue background.

Up next, in Fig. 2, we provide reductions from LW2E and LWSSE to various lattice problems that hold only for a very **restricted set of parameters**. The

goal then is to construct our PKE relying on the hardness of $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ and $\mathsf{ISSIS}_{n,m,q,\xi,\gamma}$ with parameters that **do not** allow these reductions to go through.

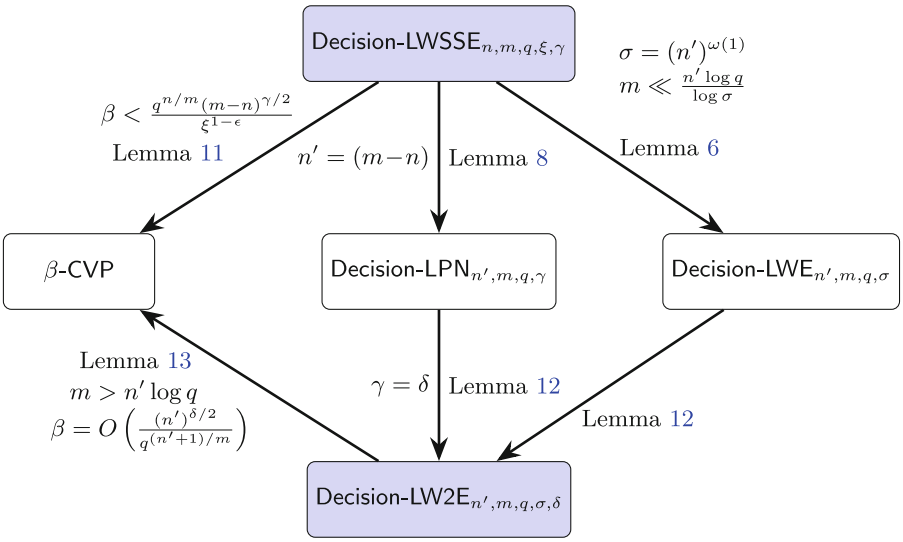


**Fig. 2.** Reductions between various assumptions that work for restricted parameter settings. An arrow from assumption $A$ to $B$ implies that an adversary breaking assumption $B$ can be used to break assumption $A$, i.e., reduction from $A$ to $B$. The parameters for which these reductions hold have are mentioned with the arrows. The new assumptions we introduce in this paper are highlighted with a blue background.

*Discussion on the Reductions.*

- Figure 1 seems to suggest that there is reduction from decision-LWSSE to decision-LW2E via decision-LPN with parameters that we use in our PKE. However, there is a parameter mismatch here. It is true that $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ reduces to $\mathsf{LPN}_{m-n,m,q,\gamma}$, However the next reduction, i.e., from $\mathsf{LPN}_{m-n,m,q,\gamma}$ to $\mathsf{LW2E}_{m-n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\gamma}$ only works when $m < \frac{n \log q}{\log \sigma}$. Outside these parameters, decision $\mathsf{LW2E}_{m-n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\gamma}$ is information theoretically secure and search $\mathsf{LW2E}_{m-n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\gamma}$ has exponentially many solutions, and therefore this reduction fails to work. However, there is indeed a reduction outside of the PKE regime which is consistent with the direct reduction from LWSSE to LW2E.
- Although we do not have a reduction from LWE to search-ISSIS, in Sect. 4 we give a moral argument about how can one use a search-ISSIS breaker to solve LWE. Such an argument only works when $m = \tilde{\Omega}(n^{\frac{1}{1-\gamma}})$ i.e., the total ISSIS regime. Unfortunately, we cannot afford to pick $m$ to be so big in our PKE as we will end up losing decryption correctness.

– With regards to proving a separation between LWE and LW2E, we do not, as a community, even know how to separate factoring from LWE. Note that an oracle separation is meaningless here, because neither LWE nor LW2E are defined with respect to oracles. What we are able to argue is this: LWE is broken given a $\sqrt{n}$-$\mathsf{CVP}$ oracle, whereas we do not know how to use a $\sqrt{n}$-$\mathsf{CVP}$ oracle to break LW2E. We furthermore explore under what circumstances a $\sqrt{n}$-$\mathsf{CVP}$ oracle could possibly be used to break LW2E, and we find that natural approaches would not work unless the sparse error components are *extremely sparse* and the field size q is also limited with respect to the dimension n. Note that if we were able to actually prove that no efficient algorithm given a $\sqrt{n}$-$\mathsf{CVP}$ oracle can break LW2E, this would imply that no efficient algorithm that does not use $\sqrt{n}$-$\mathsf{CVP}$ oracle can break LW2E, implying $\mathsf{P} \neq \mathsf{NP}$. Nevertheless, our work does motivate a further deep exploration of such separation questions.

*Relating Noisy Linear Algebraic Assumptions.* If we adopt the perspective of best-known *current* attack algorithms, LWE and LW2E share similar tools and might appear to be "similar assumptions" as a result. On the other hand, if we adopt the complexity-theoretic/cryptographic perspective, these two assumptions have clearly different complexity-theoretic standing and cryptographic utility. In this paper, we take the latter perspective of complexity-theoretic/cryptographic evidence, but we believe both perspectives are important. We hope that in studying this question, both perspectives converge in deeper insight about the landscape of computational assumptions necessary for PKE. Indeed, our results also further motivate the algorithmic study of "mixed-error" assumptions.

*Preliminaries:* Some notation and standard results about lattices, along with the formal definition of LWE and LPN have can be found in the full version.

## 2 Dual Form of LWSSE

We also define a "dualized", equivalent version of $\mathsf{LWSSE}$ that looks more like an $\mathsf{SIS}$-style assumption, as opposed to an $\mathsf{LWE}$-style one.

**Definition 3 (The Inhomogeneous Short and Sparse Decision Assumption (ISSIS)).**

*For all $n \in \mathbb{N}$, $m = \mathsf{poly}(n) > n$, prime $q \in \mathbb{N}$, $\xi = \mathsf{poly}(n)$, $\gamma \in (0, 1)$, the decisional inhomogeneous short and sparse assumption (decisional-ISSIS), formally parameterized as $\mathsf{ISSIS}_{n,m,q,\xi,\gamma}$, states that the following distributions are computationally indistinguishable:*

1. $\left(\mathbf{A} \xleftarrow{\$} \mathbb{F}_q^{m\times n}, \mathbf{r}^\top \mathbf{A} \pmod q\right)$ *where* $\mathbf{r} \leftarrow \mathcal{E}^m_{m,n,\xi,\gamma}$.
2. $\left(\mathbf{A} \xleftarrow{\$} \mathbb{F}_q^{m\times n}, \mathbf{u}^\top \xleftarrow{\$} \mathbb{F}_q^n\right)$.

*Remark 1 (Statistical Indistinguishability).* Note that the sparsity of the secret in the decisional-ISSIS assumption makes it *statistically distinguishable* from uniform random for certain choice of parameters. By the leftover hash lemma, only when $m = \Omega\left((n\log q)^{\frac{1}{1-\gamma}}\right)$, the decisional-ISSIS is information-theoretically hard. Refer to Sect. 4 for details. In fact, in this work, we will only use the decisional-ISSIS assumption in the computational regime.

*Remark 2.* We can analogously define the search version of ISSIS where a PPT adversary is required to output a "short and sparse" secret upon given a sample from the ISSIS distribution. Refer to Definition 4 for the formal definition.

We prove in Lemma 3 that the decisional (search)-ISSIS hardness assumption is equivalent to the decisional (search)-LWSSE assumption with identical parameters.

## 3 Public Key Encryption from LW2E and ISSIS

*Suggested Parameters:* We suggest the following choices of parameters. Assume that the security parameter is $n$:

- Decryption threshold parameter: $\zeta \in \mathbb{N}$.
- Secret dimension of LW2E: $n$.
- ISSIS sparsity parameter: $\gamma < \frac{1}{2}$.
- Smallness parameter for LW2E noise $\mathbf{e}_1$: $\sigma = n$.
- Sparsity parameter for LW2E noise $\mathbf{e}_2$: $\delta = 1 - \gamma$.
- Dimension of ISSIS secret or number of LW2E samples: $m = 20n$.
- Prime modulus $q > n^{11}$.
- ISSIS smallness parameter: $\xi = n^{0.5+\gamma}$.

More generally, we want to choose the parameters such that they satisfy the following constraints simultaneously: Pick any suitable constant $\varepsilon < \gamma$ such that

- Dimension of ISSIS secret or number of LW2E samples: $m < \frac{2(n+1)\log q}{\delta \log n}$.
- Define $B = \xi^{1-\frac{\varepsilon}{3}}$: $B > q^{\frac{n}{m}} m^{\frac{\gamma}{2}+\varepsilon}$.
- Prime modulus $q > \zeta m \sigma^{1+\frac{\varepsilon}{3}} \xi^{1+\frac{\varepsilon}{3}}$.

For example, the following can be choices of parameters:

$$\gamma = 0.1, \delta = 0.9, \varepsilon = 0.0001, \sigma = n, m = 20n, \text{ prime } q > n^{11}, \xi = n^{0.6}.$$

**Parameters**: $n, m, q, \delta, \gamma, \xi, \sigma, \zeta$.

**Error Distributions**:

1. **Sparse Error for LW2E.** Let $S_{n,q,\delta}$ be a distribution over $\mathbb{F}_q$ such that sampling results in 0 with probability $1 - n^{-\delta}$ and a uniform random element from $\mathbb{F}_q$ with probability $n^{-\delta}$.
2. **Gaussian Error for LW2E.** Let $\mathcal{D}_{\mathbb{Z},\sigma}$ be a discrete Gaussian with width $\sigma$.
3. **Small and Sparse Error for ISSIS.** Let $\mathcal{E}_{m,n,\xi,\gamma}$ be a distribution over $\mathbb{F}_q$ such that sampling results in 0 with probability $1 - (m-n)^{-\gamma}$ and in a random value from $\mathcal{D}_{\mathbb{Z},\xi}$ with probability $(m-n)^{-\gamma}$.

**Algorithms:**

- $\star$ $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$:
  1. Sample a uniform random matrix $\mathbf{A} \in \mathbb{F}_q^{m \times n}$.
  2. Sample uniform random $\mathbf{s} \in \mathbb{F}_q^n$, sample $\mathbf{e}_1 \sim \mathcal{D}_\sigma^m$, sample $\mathbf{e}_2 \sim S_{n,q,\delta}^m$.
  3. Set $\mathsf{pk} \leftarrow (\mathbf{A}, \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2)$. Set $\mathsf{sk} \leftarrow \mathbf{s}$.
  4. Output $(\mathsf{pk}, \mathsf{sk})$.
- $\star$ $\mathsf{ct} \leftarrow \mathsf{Enc}(1^\lambda, \mathsf{pk}, b \in \{0,1\})$:
  1. Parse $\mathsf{pk}$ as $(\mathbf{A}, \mathbf{y})$.
  2. Sample $\mathbf{r} \sim \mathcal{E}_{m,n,\xi,\gamma}^m$.
  3. If $b = 0$, output $(\mathbf{r}^\top \mathbf{A}, \langle \mathbf{r}, \mathbf{y} \rangle)$.
  4. If $b = 1$, output $(\mathbf{u}_1^\top, u_2)$ for uniform randomly sampled $\mathbf{u}_1 \in \mathbb{F}_q^n$, and $u_2 \in \mathbb{F}_q$.
- $\star$ $b' \leftarrow \mathsf{Dec}(1^\lambda, \mathsf{sk}, \mathsf{ct})$:
  1. Parse $\mathsf{sk}$ as $\mathbf{s}$, and parse $\mathsf{ct}$ as $(\mathsf{ct}_1 \in \mathbb{F}_q^n, \mathsf{ct}_2 \in \mathbb{F}_q)$
  2. $x \leftarrow (\mathsf{ct}_2 - \langle \mathsf{ct}_1, \mathbf{s} \rangle) \bmod q$
  3. If $x \leq \lfloor \frac{q}{\zeta} \rfloor$, then output $b' = 0$, otherwise output $b' = 1$.

*Correctness.*

**Lemma 1.** *Let $\lambda \in \mathbb{N}$ be the security parameter. Then there exists a constant $c > 0$, such that for all $n = n(\lambda) = \mathsf{poly}(\lambda) \in \mathbb{N}$, $m = O(n)$, $\delta \in (0,1)$, $\gamma = 1 - \delta$, $b \in \{0,1\}$, $\zeta \in \mathbb{N}, \zeta \geq 2$, $\mu, \nu > 0$, $\sigma = \sigma(\lambda) > 0$, $\xi = \xi(\lambda) > 0$ prime $q = q(\lambda) > \zeta m \xi^{1+\nu} \sigma^{1+\mu}$,*

$$\Pr[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda) \wedge \mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, b)) = b)] \geq c.$$

*Proof.* We proceed by analyzing the decryption error for the cases of $b = 1$ and $b = 0$ separately.

**Case 1:** If $b = 1$, in Step 2 of the decryption procedure,

$$x = \mathsf{ct}_2 - \langle \mathsf{ct}_1, \mathbf{s} \rangle = u_2 - \sum_{i \in [m]} s_i u_{1,i} \bmod q.$$

Since, each $u_{1,i}$ and $s_i$ are independent and uniformly sampled from $\mathbb{F}_q$, $y$ is also distributed uniformly over $\mathbb{F}_q$, thus

$$\Pr\left[x \geq \lfloor \frac{q}{\zeta} \rfloor\right] \geq 1 - \frac{1}{\zeta}.$$

Thus,

$$\Pr[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda) \wedge \mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, 1)) = 1)] = 1 - \frac{1}{\zeta}.$$

**Case 2:** If $b = 0$, then in Step 2 of the decryption procedure,

$$x = (\mathsf{ct}_2 - \langle \mathsf{sk}_1, \mathsf{ct}_1 \rangle) \bmod \ \mathrm{q} = \left(\mathbf{r}^\top \mathbf{e}_1 + \mathbf{r}^\top \mathbf{e}_2\right) \bmod q.$$

We first compute the probability that the event $\mathbf{r}^\top \mathbf{e}_2 = 0$ occurs that relies on the sparsity of $\mathbf{e}_2$.

To do so, first observe that the expected number of non-zero entries in $\mathbf{r} \sim \mathcal{E}^m_{m,n,\xi,\gamma}$ is $m(m-n)^{-\gamma}$. By a standard Chernoff bound, with an all but negligible probability in $n$ over the choice of $\mathbf{r}$, the number of non-zero entries in $\mathbf{r}$ is at most $2m(m-n)^{-\gamma}$. Clearly $\mathbf{r}^\top \mathbf{e}_2 = 0$ if $\mathbf{r}$ has $2m(m-n)^{-\gamma}$ non-zero elements in the worst case, and all the corresponding entries in $\mathbf{e}_2$ at these indices are 0. Therefore, the probability that $\mathbf{r}^\top \mathbf{e}_2 = 0$ is upper bounded by the probability that $\mathbf{e}_2$ has 0 at the $2m(m-n)^{-\gamma}$ many non-zero entries of $\mathbf{r}$. The probability of this is

$$(1 - n^{-\delta})^{2\, m(m-n)^{-\gamma}} = (1 - n^{-\delta})^{c' n^\delta} = \Theta(1)$$

for some constant $c' \in \mathbb{N}$, $m = O(n)$ and $\gamma + \delta = 1$.

Conditioning on the event that $\mathbf{r}^\top \mathbf{e}_2 = 0$, we have that $x = \mathbf{r}^\top \mathbf{e}_1 \bmod q$. For correctness to hold, we need to show that this value of $x$ will be sufficiently small with high probability. First, we note that the entries of $\mathbf{e}_1$ will all be upper bounded by $\sigma^{1+\mu}$ with overwhelming probability. Let $e_{1,i}$ denote the $i^{th}$ coordinate of the vector $\mathbf{e}_1$. Using standard facts about lattices (see full version), for a fixed $e_{1,i}$ and small constant $\mu > 0$,

$$\Pr\left[e_{1,i} > \sigma^{1+\mu}\right] \leq 2e^{-\pi\sigma^{2\mu}}.$$

Taking a union bound,

$$\Pr\left[\exists i \in [m] : e_{1,i} > \sigma^{1+\mu}\right] \leq 2\, m \cdot e^{-\pi\sigma^{2\mu}}.$$

Similarly applying the same lemma on $\mathbf{r}$ gives us

$$\Pr\left[\exists i \in [m] : r_i > \xi^{1+\nu}\right] \leq 2\, m \cdot e^{-\pi\sigma^{2\nu}}.$$

Therefore it must be that $\mathbf{r}^\top \mathbf{e}_1 \leq m\xi^{1+\nu}\sigma^{1+\mu}$ with probability at least $1 - 2m \cdot e^{-\pi\sigma^{2\mu}} - 2m \cdot e^{-\pi\sigma^{2\nu}}$. Since we have chosen $q > \zeta m \xi^{1+\nu}\sigma^{1+\mu}$, $x$ must be less than $\lfloor \frac{q}{\zeta} \rfloor$.

Then,

$$\Pr[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda) \wedge \mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, 0)) = 0)] \geq c.$$

Combining Case 1 and Case 2 gives us our desired correctness statement. □

*Remark 3.* While we achieve only constant decryption error in the above lemma, correctness can be amplified to achieve negligible decryption error by considering an encryption process that outputs several fresh encryptions for a single bit and a decryption process that outputs the majority value of their decryptions.

*Semantic Security.*

**Lemma 2 (Semantic Security).** *Let $\lambda$ be the security parameter. Then for every $n = \mathsf{poly}(\lambda)$, $m = \mathsf{poly}(\lambda)$, prime $q(\lambda)$, $\xi = \mathsf{poly}(\lambda)$, $\gamma \in (0, 1)$, and for all polynomial-sized adversaries $\mathcal{A}$, assuming the hardness of the Decisional-$\mathsf{LW2E}_{n,m,q,\sigma\delta}$ problem (Assumption 1) and the hardness of the Decisional-$\mathsf{ISSIS}_{n,m,q,\xi,\gamma}$ problem (Assumption 3), there exists a negligible function $\mu(\cdot) : \mathbb{N} \rightarrow [0, 1]$ such that*

$$\Big| \Pr\left[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda); \mathcal{A}(\mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, 0)) = 1, \right] - \Pr\left[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda); \mathcal{A}(\mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, 1)) = 1\right] \Big| \leq \mu(\lambda)$$

*where the probability statement is over the coins of* Gen*, the coins of* Enc*, and the coins of $\mathcal{A}$.*

The proof follows standard hybrid arguments. Refer to the full version for formal details.

*Remark 4 (Achieving CCA Security).* Note that one can achieve CCA security by combining our CPA secure encryption scheme together with a non-interactive zero knowledge (NIZK) proof system using the Naor-Yung paradigm [26,31]. Such a NIZK can even be constructed unconditionally in the random oracle model, implying a CCA secure PKE from our assumptions. We do not explore the possibility of constructing a direct CCA secure PKE and leave this for future work.

## 4 Analysis of the ISSIS Assumption

*Convention.* As shown in the proof of Lemma 1, we know that when $r_i \xleftarrow{\$} \mathcal{E}_{m,n,\xi,\gamma}$, the probability that $r_i > \xi^{1+\nu}$ for some positive constant $\nu$ is negligible. Sometimes in this section, for notational convenience, we will use $B := \xi^{1+\nu}$. We will refer to any vector $\mathbf{r} \xleftarrow{\$} \mathcal{E}^m_{m,n,\xi,\gamma}$ as being $B$-bounded while ignoring the fact that it might not be so with a negligible probability. This is solely done for ease of exposition in this section and does not impact any of the analysis.

*Necessary Condition for Totality.* Totality is the regime where for all $\mathbf{b} \in \mathbb{F}_q^n$, there will exist a "short and sparse" $\mathbf{r} \leftarrow \mathcal{E}_{m,n,\xi,\gamma}$ such that $\mathbf{r}^\top \mathbf{A} = \mathbf{b}$ with overwhelming probability over the choice of $\mathbf{A} \in \mathbb{F}_q^{m \times n}$. In computing the sufficient asymptotic condition for totality, it suffices to consider the number of $B$-bounded, exactly $m(m-n)^{-\gamma}$-sparse vectors in $\mathbb{F}_q^m$. This number is exactly $B^{m(m-n)^{-\gamma}} \cdot \binom{m}{m(m-n)^{-\gamma}}$. A necessary condition for totality, in other words surjectivity from the domain of $B$-bounded $m(m-n)^{-\gamma}$-sparse vectors in $\mathbb{F}_q^m$ to the codomain of $\mathbb{F}_q^n$, is that $B^{m(m-n)^{-\gamma}} \cdot \binom{m}{m(m-n)^{-\gamma}} > q^n$. A lower bound of the LHS is given by $(B(m-n)^\gamma)^{m(m-n)^{-\gamma}}$ and therefore $(B(m-n)^\gamma)^{m(m-n)^{-\gamma}} > q^n$, then totality is possible. This happens when $m > \left(\frac{n \log q}{\log B}\right)^{\frac{1}{1-\gamma}}$.

*For our PKE construction, we will not be in the ISSIS total regime because the parameter setting is that $\gamma = 1 - \delta \in (0,1)$ for which the correctness of our PKE requires $m = O(n)$. A natural question is whether we could avoid the usage of LWSSE/ISSIS and only obtain PKE from LW2E via the usage of the leftover hash lemma. This would be possible if there were a parameter setting in which we were in the ISSIS total regime.*

### 4.1 ISSIS Search-to-Decision Reduction

**Definition 4 (The Search Inhomogeneous Short and Sparse Decision Assumption (ISSIS)).** *Let $\lambda$ be the security parameter. The search inhomogeneous short and sparse assumption (search-ISSIS), formally parameterized as search-$\mathsf{ISSIS}_{n,m,q,\xi,\gamma}$, states that for all PPT adversaries $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that*

$$\Pr\Big[\mathbf{r'}^\top \mathbf{A} = \mathbf{r}^\top \mathbf{A} \text{ and } \max_i(\mathbf{r'}_i) \leq B \text{ and } \mathsf{hw}(\mathbf{r'}) \leq 2\,m(m-n)^{-\gamma} \\ \big|\mathbf{r'} \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{r}^\top \mathbf{A}), \mathbf{A} \xleftarrow{\$} \mathbb{F}_q^{m \times n}, \mathbf{r} \xleftarrow{\$} \mathcal{E}_{m,n,\xi,\gamma}^m\Big] \leq \mathsf{negl}(\lambda).$$

*Here, $\mathsf{hw}(\mathbf{r'}) = |i : \mathbf{r}'_i \neq 0|$, $n < m$ and $\mathcal{E}_{m,n,\xi,\gamma}$ is a distribution over $\mathbb{Z}$ which samples 0 with probability $1 - (m-n)^{-\gamma}$ or a random element from $\mathcal{D}_{\mathbb{Z},\xi}$ with probability $(m-n)^{-\gamma}$.*

**Theorem 2 (Decision ISSIS is at least as hard as search ISSIS).** *If there exists a PPT algorithm $\mathcal{A}$ that has non-negligible distinguishing advantage $\varepsilon : \mathbb{N} \to [0,1]$ for the decisional $\mathsf{ISSIS}_{n,m,q,\xi,\gamma}$ assumption, then there exists a PPT algorithm $\mathcal{B}$ that inverts the search $\mathsf{ISSIS}_{n,m,q,\xi,\gamma}$ assumption with non-negligible inversion advantage.*

The core idea behind this reduction are the techniques used to achieve a *sample-preserving* search-to-decision reduction as done by Micciancio and Mol [25]. See the full version for details.

### 4.2 Equivalence of ISSIS and LWSSE

Here, we show that (decisional) ISSIS and LWSSE are equivalent assumptions. The same holds for the search versions of the assumptions, but for simplicity we state the proof for the decisional versions.

**Lemma 3 (Primal and Dual Equivalence).** *For any $m \geq n + \omega(\log n)$ , there are polynomial time reductions in both directions between $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ and $\mathsf{ISSIS}_{n,m,q,\xi,\gamma}$.*

The proof can be found in the full version.

### 4.3 Reduction Between LWSSE and LW2E

Intuitively, LW2E seems harder than LWSSE because the structure of LWSSE resembles that of LPN (we will see that LWSSE indeed reduces to LPN with the same sparsity). Whereas the lack of sparsity or smallness (in the $\ell_2$ norm) of the LW2E error resembles neither the structure of LPN or LWE.

We are not aware of a reduction from distinguishing LW2E (respectively, recovering the secret), to the problem of distinguishing LWSSE (resp. recovering the planted short and sparse solution in LWSSE). In the other direction, however, we now show a natural reduction idea from LWSSE to LW2E using noise smudging.

**Lemma 4 (Gaussian Smudging Lemma [20]).** *Let $n \in \mathbb{N}$, $\forall \sigma > \omega(\sqrt{\log n})$, for any $\mathbf{c} \in \mathbb{Z}^n$,*

$$\Delta(\mathcal{D}_{\mathbb{Z}^n,\sigma}, \mathcal{D}_{\mathbb{Z}^n,\sigma,\mathbf{c}}) \leq \frac{\|\mathbf{c}\|_2}{\sigma}.$$

*LWSSE to LW2E.* Using an algorithm $\mathcal{A}$ that distinguishes the decisional-LW2E assumption $\mathsf{LW2E}_{m-n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ for $q = (m-n)^{\omega(1)}$, with non-negligible advantage $\varepsilon$, we construct an algorithm $\mathcal{B}$ that distinguishes the decisional-LWSSE assumption $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ for $\xi = \frac{\sigma}{(m-n)^{\omega(1)}}$ and for any value of $\gamma$ with non-negligible advantage $\varepsilon'$.

The algorithm $\mathcal{B}$ on input $\left(\mathbf{A} \in \mathbb{F}_q^{(m-n)\times m}, \mathbf{y} \in \mathbb{F}_q^{1\times m}\right)$, where either $\mathbf{y} = \mathbf{sA} + \mathbf{e}$ for $\mathbf{e} \in \mathbb{F}_q^{1\times m}$ sampled from $\mathcal{E}_{m,n,\xi,\gamma}$ or $\mathbf{y} \sim \mathsf{Unif}\left(\mathbb{F}_q^{1\times m}\right)$, performs the following computational steps:

1. Sample a vector $\mathbf{e}_{\mathsf{flood}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma}$ where $\sigma = (m-n)^{\omega(1)} \cdot \xi$.
2. Sample a vector $\mathbf{e}_{\mathsf{flood,sp}} \leftarrow \mathcal{S}^m_{m-n,q,\delta}$.
3. Output $\mathcal{A}(\mathbf{A}, \mathbf{y} + \mathbf{e}_{\mathsf{flood}} + \mathbf{e}_{\mathsf{flood,sp}})$.

**Lemma 5 (Correctness of Reduction to LW2E).** *If $\mathcal{A}$ is a polynomial-time algorithm that distinguishes $\mathsf{LW2E}_{m-n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ for $q = (m-n)^{\omega(1)}$, for $\xi = \mathsf{poly}(n)$, and for any $\delta \in [0,1]$ with advantage $\varepsilon$, then $\mathcal{B}$ is a polynomial-time algorithm that distinguishes $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ for $\xi = \frac{\sigma}{(m-n)^{\omega(1)}}$ and for any $\gamma \in [0,1]$ with advantage at least $\varepsilon - \frac{1}{(m-n)^{\omega(1)}}$.*

*Proof.* We know that $\mathbf{e}$ is $B$-bounded with all but negligible probability and therefore $\|\mathbf{e}\|_2 \leq B\sqrt{m}$ By Lemma 4, the distribution of $\mathbf{e}+\mathbf{e}_{\mathsf{flood}}$ has statistical distance bounded above by $\frac{B\sqrt{m}}{\sigma}$ from the distribution of $\mathbf{e}_{\mathsf{flood}}$, i.e. $\mathcal{D}_{\mathbb{Z}^n,\sigma}$. Therefore $\mathbf{e}+\mathbf{e}_{\mathsf{flood}}+\mathbf{e}_{\mathsf{flood,sp}}$ has statistical distance at most $\frac{B\sqrt{m}}{\sigma}$ from the distribution of $\mathbf{e}_{\mathsf{flood}}+\mathbf{e}_{\mathsf{flood,sp}}$, which is exactly the error distribution of $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$. □

*Remark 5 (Non-applicability of the Reduction for the PKE Parameter Setting).* If we are in the information-theoretically hard regime of the $\mathsf{LW2E}_{m-n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ assumption, then this reduction vacuously fails as the assumption that there exists an efficient algorithm $\mathcal{A}$ that distinguishes $\mathsf{LW2E}$ is false. In particular, as we elaborate in Sect. 5, we hit the information-theoretically hard regime when

$$m = o\left(\frac{(m-n)\log q}{\log q - \log \sigma}\right)$$

which occurs when $m > n \cdot \left(\frac{\log q}{\log \sigma}\right)$. In our PKE scheme, the parameters for the ISSIS problem, and its corresponding dualized form as a LWSSE problem, fall into this information-theoretically hard regime of the $\mathsf{LW2E}$ assumption.

*Remark 6.* As we will see later, there is another way to have an "indirect" reduction from $\mathsf{LWSSE}$ to $\mathsf{LW2E}$. Lemma 8 says that $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ reduces to $\mathsf{LPN}_{m-n,m,q,\gamma}$ and Lemma 12 says that $\mathsf{LPN}_{m-n,m,q,\gamma}$ reduces to $\mathsf{LW2E}_{m-n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\gamma}$. Therefore, together we can conclude that $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ reduces to $\mathsf{LW2E}_{m-n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\gamma}$. The catch here is that for most setting of parameters, i.e., $m > \frac{n\log q}{\log \sigma}$, $\mathsf{LW2E}_{m-n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\gamma}$ is information theoretically secure, and therefore this reduction vacuously fails.

### 4.4 Reduction Between LWSSE and LWE

The same idea of noise smudging gives a reduction from LWSSE to LWE. Using an algorithm $\mathcal{A}$ that distinguishes the decisional-LWE assumption $\mathsf{LWE}_{(m-n),m,q,\sigma}$ for $q = (m-n)^{\omega(1)}$, with non-negligible advantage $\varepsilon$, we construct an algorithm $\mathcal{B}$ that distinguishes the decisional-LWSSE assumption $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ for $\xi = \frac{\sigma}{(m-n)^{\omega(1)}}$ and for any value of $\gamma$ with non-negligible advantage $\varepsilon - \frac{1}{(m-n)^{\omega(1)}}$. The algorithm $\mathcal{B}$ on input $\left(\mathbf{A} \in \mathbb{F}_q^{(m-n)\times m}, \mathbf{y} \in \mathbb{F}_q^{1\times m}\right)$, where either $\mathbf{y} = \mathbf{s}\mathbf{A}+\mathbf{e}$ for $\mathbf{e} \in \mathbb{F}_q^{1\times m}$ sampled from $\mathcal{D}_{\mathbb{Z}^m,\sigma}$ or $\mathbf{y} \sim \mathsf{Unif}\left(\mathbb{F}_q^{1\times m}\right)$, performs the following computational steps:

1. Sample a vector $\mathbf{e}_{\mathsf{flood}} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^m$ where $\sigma = (m-n)^{\omega(1)} \cdot B$.
2. Output $\mathcal{A}(\mathbf{A}, \mathbf{y}+\mathbf{e}_{\mathsf{flood}})$.

**Lemma 6 (Correctness of Reduction to LWE).** *If $\mathcal{A}$ is a polynomial-time algorithm that distinguishes $\mathsf{LWE}_{(m-n),m,q,\sigma}$ for $q = (m-n)^{\omega(1)}$ , for $\sigma > \omega(\sqrt{\log m})$, and for any $\delta \in [0,1]$ with advantage $\varepsilon$, then $\mathcal{B}$ is a polynomial-time algorithm that distinguishes $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ for $\xi = \frac{\sigma}{(m-n)^{\omega(1)}}$ and for any $\gamma \in [0,1]$ with advantage at least $\varepsilon - \frac{1}{(m-n)^{\omega(1)}}$.*

*Proof.* The proof is immediate by application of Lemma 4. □

**Corollary 1 (ISSIS to LWE).** *If $\mathcal{A}$ is a polynomial-time algorithm that distinguishes $\mathsf{LWE}_{(m-n),m,q,\sigma}$ for $q = (m-n)^{\omega(1)}$, for $\xi > \mathsf{poly}(n)$, and for any $\delta \in [0,1]$ with advantage $\varepsilon$, then $\mathcal{B}$ is a polynomial-time algorithm that distinguishes $\mathsf{ISSIS}_{n,m,q,\xi,\gamma}$ for $\xi = \frac{\sigma}{(m-n)^{\omega(1)}}$ and for any $\gamma \in [0,1]$ with advantage at least $\varepsilon - \frac{1}{(m-n)^{\omega(1)}}$.*

*Proof.* This follows from Lemma 3 and Lemma 6. □

*Remark 7 (No Known Reduction Inside the Total SIS Regime).* In the $\mathsf{LWE}_{m-n,m,q,\sigma}$ problem, the parameter setting of $m = \Omega\left(n \cdot \frac{\log q}{\log \sigma}\right)$ is inside of the total SIS regime, which can be computed by a direct entropy calculation: $(m-n)\log q + m \log \sigma \gg m \log q$. In this parameter setting, there does not exist any efficient algorithm $\mathcal{A}$ that distinguishes (resp. solves) the corresponding decisional-LWE assumption as the decisional-LWE assumption is statistically hard to distinguish. Vacuously, then, there is no known reduction from decisional-LWSSE to decisional-LWE. Our PKE parameters have been set to be in this setting where the above reduction from decisional-LWSSE to decisional-LWE does not hold. Similarly, while there is a reduction from search-LWSSE to search-LWE, in the total SIS regime the corresponding search-LWE problem does not have a unique $\mathbf{s}$, so there's no guarantee that the search-LWE solver returns the correct $\mathbf{s}$.

*Remark 8 (Gap between Total SIS and Total ISSIS Regime).* Remark 7 and the totality computation for ISSIS show that there is a wide range of parameters for which we have both the conjectured computational hardness of decisional-ISSIS and no known reduction from decisional-ISSIS to decisional-LWE. That range of parameters are any parameters inside of the total SIS regime, namely when $m = \Omega\left(n \cdot \frac{\log q}{\log \sigma}\right)$, and outside of the total ISSIS regime, namely when $m = O\left(\left(n \cdot \frac{\log q}{\log \sigma}\right)^{1/(1-\gamma)}\right)$ where $\gamma < 1$.

*On a Potential Reduction from LWE to ISSIS.* We briefly note a potential reduction from decisional-LWE to search-ISSIS. Namely, a search-ISSIS breaker should be able to distinguish the LWE problem with suitable parameters. The same reduction idea from LWE to SIS should work to reduce LWE to search-ISSIS. The reduction starts with an instance of the form $(\mathbf{A}, \mathbf{b})$, uses the search-ISSIS breaker on $\mathbf{A}$ to find a short and sparse solution $\mathbf{r} \in \mathbb{Z}^m$, and computes $\langle \mathbf{b}, \mathbf{r} \rangle \bmod q$. In the case that $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, then the above inner product is small relative to $q$. Otherwise, if $\mathbf{b}$ is uniformly distributed, the above inner product is $O(q)$. This reduction can only be possible when a short and sparse $\mathbf{r}$ exists, i.e. in the total regime of ISSIS, for which we have computed a necessary condition above. While we computed a necessary condition for the total regime for ISSIS, we have not yet computed a *sufficient* condition for the existence of a short *and sparse* vector, which would give us our desired reduction. We can now observe two crucial points:

- The parameter regime for our PKE is in the non-total regime for ISSIS, so this reduction does not work, and we do not know a reduction from decision LWE to search ISSIS for such parameter settings.
- This *does not* imply a reduction from decision LWE to decision ISSIS because in the total ISSIS regime, the decisional ISSIS problem is information theoretically secure, hence there is no search-decision reduction.

This also implies that we do not know any relation between (decisional) LWE and (search) ISSIS in the parameter regime that implies PKE.

*Relation Between SIS and ISSIS.* Heuristically, there is a parameter regime for ISSIS in which a SIS oracle is unlikely to return a planted *short and sparse* vector. Consider an ISSIS instance of the form $(\mathbf{A} \in \mathbb{F}_q^{m \times n}, \mathbf{r}^\top \mathbf{A})$. For our choice of parameters for our PKE scheme, any SIS oracle that can possibly output $\mathbf{r}$ must select this $\mathbf{r}$ from exponentially many short integer solutions. That is, the expected $\ell_2$ norm of $\mathbf{r}$ is so large that there exists a positive $D$ such that $D^m \gg q^n$ and the $\ell_2$ norm of $\mathbf{r}$ is concentrated above $2D\sqrt{m}$. Since there are exponentially many short integer solutions that are shorter than $\mathbf{r}$, an SIS oracle that can possibly output $\mathbf{r}$ must somehow select $\mathbf{r}$ out of an exponential sized set of integer solutions that are shorter. Only the sparseness of $\mathbf{r}$ distinguishes it, which an SIS oracle is blind to.

### 4.5 Reducing LWSSE to LPN

We begin with a helpful lemma about the mass of discrete Gaussians on 0 (mod $q$).

**Lemma 7.** *For any $q \geq \xi \geq 2$, we have*

$$\Pr_{Z \leftarrow \mathcal{D}_{\mathbb{Z},\xi}}[Z = 0 \pmod q] = \Theta\left(\frac{1}{\xi}\right).$$

The proof can be found in the full version.

Now we give the reduction from LWSSE to LPN. Note that the additive difference between $\gamma$ and $\gamma'$ is sub-constant, while we typically consider $\gamma$ and $\gamma'$ set to be constants in $(0, 1)$, so this additive fudge factor is a lower order term for us. Moreover, the reason there is a difference between $\gamma$ and $\gamma'$ is due to the way we defined the error distributions: if with probability $(m-n)^{-\gamma}$ we were *guaranteed* that the error is non-zero (instead of drawn from a discrete Gaussian or from the uniform distribution over $\mathbb{F}_q$), then $\gamma' = \gamma$.

We emphasize that for $\gamma < 1/2$, this only reduces to LPN in a regime where $\gamma' < 1/2$, which is *not* the Alekhnovich regime for LPN.

**Lemma 8.** *For prime $q$ with $2 \leq \xi \leq q$, there is an efficient reduction from $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ to $\mathsf{LPN}_{m-n,m,q,\gamma'}$, for*

$$\gamma' = \gamma - \frac{\log\left(1 - \Theta\left(\frac{1}{\xi}\right)\right)}{\log(m-n)} - \frac{\log \frac{q}{q-1}}{\log(m-n)}.$$

*Proof.* Let $\left(\mathbf{A}^{\perp} \in \mathbb{F}_q^{(m-n)\times m}, \mathbf{b}^{\top} \in \mathbb{F}_q^m\right)$ be the $\mathsf{LWSSE}$ instance. Sample i.i.d. values $r_1, \cdots, r_m \leftarrow \mathbb{F}_q \setminus \{0\}$. Then, let $\mathbf{R} = \mathrm{diag}(r_1, \cdots, r_m) \in \mathbb{F}_q^{m\times m}$ be the diagonal matrix with $R_{i,i} = r_i$ for all $i \in [m]$. The reduction outputs (the transposes of)

$$\left(\mathbf{A}' := \mathbf{A}^{\perp}\mathbf{R} \in \mathbb{F}_q^{(m-n)\times m}, (\mathbf{b}')^{\top} := \mathbf{b}^{\top}\mathbf{R} \in \mathbb{F}_q^m\right)$$

as the $\mathsf{LPN}$ instance.

To see why this is correct, suppose we are in the "null" case where $\mathbf{b}^{\top}$ is uniformly random. Since $\mathbf{R}$ is clearly invertible (as $q$ is prime), the distribution exactly matches the $\mathsf{LPN}$ "null" distribution. Now suppose we are in the "planted" case, where

$$\mathbf{b}^{\top} = \mathbf{s}^{\top}\mathbf{A}^{\perp} + \mathbf{e}^{\top} \pmod q,$$

for $\mathbf{s} \xleftarrow{\$} \mathbb{F}_q^{m-n}$, $\mathbf{e} \leftarrow \mathcal{E}_{m,n,\xi,\gamma}^m$. Then,

$$(\mathbf{b}')^{\top} = \mathbf{b}^{\top}\mathbf{R} = \left(\mathbf{s}^{\top}\mathbf{A}^{\perp} + \mathbf{e}^{\top}\right)\mathbf{R} = \mathbf{s}^{\top}\mathbf{A}' + \mathbf{e}^{\top}\mathbf{R} = \mathbf{s}^{\top}\mathbf{A}' + (\mathbf{e}')^{\top},$$

where we define $(\mathbf{e}')^{\top} := \mathbf{e}^{\top}\mathbf{R}$. It suffices to show that the distributions of $(\mathbf{e}')^{\top}$ and $\mathbf{A}'$ are independent and have the correct marginals for a $\mathsf{LPN}$ instance. For $(\mathbf{e}')^{\top} = \mathbf{e}^{\top}\mathbf{R}$, observe that multiplying $\mathbf{e}^{\top}$ by $\mathbf{R}$ multiplicatively re-randomizes all non-zero entries of $\mathbf{e}^{\top}$ to be uniformly random in $\mathbb{F}_q$, since $q$ is prime, while preserving all 0 values of $\mathbf{e}^{\top}$. Let $p \in [0,1]$ denote the probability that a given entry of $\mathbf{e}^{\top}$ is non-zero (i.e., zero with probability $1-p$). This reduction produces $(\mathbf{e}')^{\top}$ where each entry is 0 with probability $1-p$, and every other element in $\mathbb{F}_q$ has probability $p/(q-1)$. Equivalently, this can be phrased as a mixture distribution of uniform over $\mathbb{F}_q$, with probability $pq/(q-1)$, and the singleton distribution $\{0\}$, with probability $1 - pq/(q-1)$. We need

$$(m-n)^{-\gamma'} = pq/(q-1). \tag{1}$$

If this holds, then this reduction maps $\mathcal{E}_{m,n,\xi,\gamma}$ to $\mathcal{S}_{m-n,q,\gamma'}$, making the marginal distribution of $\mathbf{e}^{\top}$ correct. We defer this setting of $\gamma'$ to later in the proof. For $\mathbf{A}'$, note that for any fixed, invertible $\mathbf{R}$, the distribution of $\mathbf{A}' = \mathbf{A}^{\perp}\mathbf{R}$ is uniformly random, by the randomness of $\mathbf{A}^{\perp}$. Therefore, $\mathbf{A}'$ and $\mathbf{e}^{\top}$ are independent, and the marginal distribution of $\mathbf{A}'$ is correct, as desired.

To set $\gamma'$, we now analyze this probability $p$. A given entry of $\mathbf{e}^{\top}$ is non-zero with probability

$$p = (m-n)^{-\gamma} \cdot \left(1 - \Pr_{Z \leftarrow \mathcal{D}_{\mathbb{Z},\xi}}[Z = 0 \pmod q]\right). \tag{2}$$

Applying Lemma 7 and plugging the result back into (2), we have

$$p = (m-n)^{-\gamma} \cdot \left(1 - \Pr_{Z \leftarrow \mathcal{D}_{\mathbb{Z},\xi}}[Z = 0 \pmod q]\right) = (m-n)^{-\gamma} \cdot \left(1 - \Theta\left(\frac{1}{\xi}\right)\right).$$

Plugging back into (1), we need

$$(m-n)^{-\gamma'} = p \cdot \frac{q}{q-1} = (m-n)^{-\gamma} \cdot \left(1 - \Theta\left(\frac{1}{\xi}\right)\right) \cdot \frac{q}{q-1}.$$

For $q \geq 2$ and $\xi \geq 1$, this becomes

$$(m-n)^{-\gamma'} = \Theta\left((m-n)^{-\gamma}\right).$$

Thus,

$$\gamma' = \gamma \pm O\left(\frac{1}{\log(m-n)}\right).$$

□

*Comparing with Alekhnovich's LPN.* The above lemma implies that our PKE scheme is broken in the presence of an LPN oracle. But, that is fine because we pick the sparsity parameter $\gamma$ to satisfy $\gamma < \frac{1}{2}$. This means that an adversary that breaks LPN in this parameter regime is stronger than one that breaks Alekhnovich's LPN. In particular, in the world where Alekhnovich's LPN is broken, i.e., there exists an adversary that solves LPN with $\gamma \geq \frac{1}{2}$, our assumption is still secure as the sparsity parameter is strictly less than $\frac{1}{2}$. In fact, we do not have any lower bound on the choice of $\gamma$ and it can as small as one wants, e.g., $\gamma = 0.01$, which should be beyond the reach of a breaker for Alekhnovich's LPN.

### 4.6 Reducing LWSSE to Lattice Problems

In this subsection, we show that for reasonable parameter choices in ISSIS/LWSSE, there is no (obvious) reduction to a lattice problem. We adopt a cryptanalytic approach here and attempt to rule out the obvious ways to interpret ISSIS/LWSSE as a lattice problem. We will assume some knowledge of the standard notion for the usual lattice parameters and standard bounds on random lattices, all of which can be found in the full version.

**Lemma 9 ([24]).** *There exists a universal constant $\delta \in (0,1)$ such that the following equations hold for all $q \geq m^{\max\left(\frac{m}{2n}, \frac{m}{2(m-n)}\right)}$:*

$$\Pr_{\mathbf{A}^\perp \xleftarrow{\$} \mathbb{F}_q^{(m-n)\times m}}\left[\lambda_1(\Lambda_q(\mathbf{A}^\perp)) \in \left[\delta\sqrt{m}\cdot q^{n/m}, \sqrt{m}\cdot q^{n/m}\right]\right] \geq 1 - \mathsf{negl}(n),$$

$$\Pr_{\mathbf{A}^\perp \xleftarrow{\$} \mathbb{F}_q^{(m-n)\times m}}\left[\lambda_1(\Lambda_q^\perp(\mathbf{A}^\perp)) \in \left[\delta\sqrt{m}\cdot q^{1-n/m}, \sqrt{m}\cdot q^{1-n/m}\right]\right] \geq 1 - \mathsf{negl}(m-n).$$

**Lemma 10 ([24]).** *There exists a universal constant $\delta \in (0,1)$ such that the following equation holds for all $q \geq m^{\frac{m}{2(m-n)}}$:*

$$\Pr_{\mathbf{A}^\perp \xleftarrow{\$} \mathbb{F}_q^{(m-n)\times m}}\left[\rho(\Lambda_q(\mathbf{A}^\perp)) \in \left[\delta\sqrt{m}\cdot q^{n/m}, \frac{1}{\delta}\sqrt{m}\cdot q^{n/m}\right]\right] \geq 1 - \mathsf{negl}(n),$$

The lower bounds on $q$ needed above, which our PKE parameter settings satisfy since $q \geq m^{10}$ and $m = 20n$, are to rule out trivial shortest vectors of the form $q\mathbb{Z}^m$. Therefore, we can assume $\lambda_1(\Lambda_q(\mathbf{A}^\perp)) = \Theta\left(\sqrt{m} \cdot q^{n/m}\right)$, $\lambda_1(\Lambda_q^\perp(\mathbf{A}^\perp)) = \Theta\left(\sqrt{m} \cdot q^{1-n/m}\right)$, and $\rho(\Lambda_q(\mathbf{A}^\perp)) = \Theta\left(\sqrt{m} \cdot q^{n/m}\right)$.

We now set up notation for $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$. In the planted case for $\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$, we have

$$\mathbf{b}^\top = \mathbf{s}^\top \mathbf{A}^\perp + \mathbf{e}^\top \pmod q,$$

for $\mathbf{s} \xleftarrow{\$} \mathbb{F}_q^{m-n}$, $\mathbf{e} \leftarrow \mathcal{E}_{m,n,\xi,\gamma}^m$.

**Closest Vector Problem and Bounded Distance Decoding.** The natural way to view this as a lattice problem is to phrase it as an instance of the closest vector problem (CVP) (or bounded distance decoding (BDD)), where $\mathbf{b}^\top$ is a target vector within the lattice $\Lambda_q(\mathbf{A}^\perp)$. The distance from $\mathbf{b}^\top$ to the lattice is at most $\mathbf{e}^\top$, which has expected squared norm

$$\mathbb{E}\left[\|\mathbf{e}\|_2^2\right] = \Theta\left(\xi^2 \cdot \frac{m}{(m-n)^\gamma}\right), \tag{3}$$

and this norm concentrates well by standard Chernoff and Gaussian bounds. We begin by observing that we can have a reduction to the $\mathsf{CVP}_\beta$ problem when $\xi = o(q^{n/m} \cdot (m-n)^{\gamma/2})$.

**Definition 5.** *The* $\mathsf{BDD}_\alpha$ *problem, parameterized by* $\alpha \in (0, 1/2)$*: Given an instance* $(\mathbf{A} \in \mathbb{Q}^{m\times m}, \mathbf{t} \in \mathbb{Q}^m)$ *where* $\mathbf{A}$ *is a basis for a lattice* $\mathcal{L} \subseteq \mathbb{Q}^m$ *and the promise that* $\|\mathcal{L} - \mathbf{t}\|_2 \leq \alpha \cdot \lambda_1(\mathcal{L})$*, find the unique lattice point* $\mathbf{x} \in \mathcal{L}$ *such that* $\|\mathbf{x} - \mathbf{t}\|_2 \leq \alpha \cdot \lambda_1(\mathcal{L})$*.*

**Definition 6.** *The* $\mathsf{CVP}_\beta$ *(or* $\beta$-CVP*) problem, parameterized by* $\beta \geq 1$*: Given an instance* $(\mathbf{A} \in \mathbb{Q}^{m\times m}, \mathbf{t} \in \mathbb{Q}^m)$ *where* $\mathbf{A}$ *is a basis for a lattice* $\mathcal{L} \subseteq \mathbb{Q}^m$*, output any lattice point* $\mathbf{x} \in \mathcal{L}$ *such that* $\|\mathbf{x} - \mathbf{t}\|_2 \leq \beta \cdot \|\mathcal{L} - \mathbf{t}\|_2$*.*

**Lemma 11.** *If* $\xi = o(q^{n/m} \cdot (m-n)^{\gamma/2})$*, then decisional-*$\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ *reduces to* $\mathsf{CVP}_\beta$ *for* $\beta > 1$ *where*

$$\beta = \frac{q^{n/m}(m-n)^{\gamma/2}}{\xi}.$$

*Proof.* The reduction $\mathcal{B}$ is given as input $(\mathbf{A}^\perp \in \mathbb{F}_q^{(m-n)\times m}, \mathbf{b}^\top = \mathbf{s}^\top \mathbf{A}^\perp + \mathbf{e}^\top)$ where $\mathbf{b}^\top = \mathbf{s}^\top \mathbf{A}^\perp + \mathbf{e}^\top$ or $\mathbf{b}^\top$ is uniform random. Let $\tilde{\mathbf{A}}^\perp$ be a basis for $\Lambda_q(\mathbf{A}^\perp)$. Recall that by Lemma 9, we have $\lambda_1(\Lambda_q(\mathbf{A}^\perp)) = \Theta(\sqrt{m}q^{n/m})$ with all but negligible probability. When $\xi = o(q^{n/m} \cdot (m-n)^{\gamma/2})$, then the expected squared error norm satisfies

$$\mathbb{E}\left[\|\mathbf{e}\|_2^2\right] = \Theta(m \cdot (m-n)^{-\gamma} \cdot \xi^2) = o(\lambda_1(\Lambda_q(\mathbf{A}^\perp))^2).$$

Observe that $\|\Lambda_q(\mathbf{A}^\perp) - \mathbf{b}^\top\|_2 \leq \|\mathbf{e}^\top\|_2$ when $\mathbf{b}^\top$ is planted. The reduction $\mathcal{B}$ obtains $\mathbf{y}^\top \leftarrow \mathsf{CVP}_\beta(\tilde{\mathbf{A}}^\perp, \mathbf{b}^\top)$, and outputs 1 if $\mathbf{y} \in \Lambda_q(\mathbf{A}^\perp)$ and $\|\mathbf{b}^\top - \mathbf{y}^\top\|_2 \leq \frac{1}{100} \cdot \sqrt{m} q^{n/m}$. The oracle guarantees that when $\mathbf{b}^\top$ is planted,

$$\|\mathbf{b}^\top - \mathbf{y}^\top\|_2 \leq \beta \cdot \|\mathbf{e}^\top\|_2 = o\left(\lambda_1(\Lambda_q(\mathbf{A}^\perp))\right).$$

On the other hand, when $\mathbf{b}^\top$ is not planted, with high probability, there does not exist any lattice vector $\mathbf{y} \in \Lambda_q(\mathbf{A}^\perp)$ such that $\|\mathbf{b}^\top - \mathbf{y}^\top\|_2 \leq \frac{1}{100} \cdot \sqrt{m} q^{n/m}$. This completes the reduction. □

*Remark 9.* Also, a bounded distance decoding solver can be used to solve search-$\mathsf{LWSSE}_{n,m,q,\xi,\gamma}$ with parameter $\alpha \in (0, 1/2)$ given by

$$\alpha = \omega\left(\frac{\xi}{q^{n/m}(m-n)^{\gamma/2}}\right).$$

The statement for the $\alpha$-bounded distance decoding follows from the last equation in the above proof for the reduction to CVP, in which we observe that since $\beta \cdot \|\mathbf{e}\|_2$ is asymptotically smaller than $\lambda_1(\Lambda_q(\mathbf{A}^\perp))$, we have $\|\mathbf{e}\|_2 \ll \frac{1}{2\beta}\lambda_1(\Lambda_q(\mathbf{A}^\perp))$, so solving is possible from using a $\alpha$-BDD solver for $\alpha = \omega(1/\beta)$.

*Remark 10 (Discussion on Larger Values of $\xi$).* Comparing Lemma 9 to Eq. (3), we see that $\mathbf{e}^\top$ is *larger* than the shortest vector in $\Lambda_q(\mathbf{A}^\perp)$ and more so, the covering radius of $\Lambda_q(\mathbf{A}^\perp)$ iff

$$\xi \gg q^{n/m} \cdot (m-n)^{\gamma/2}. \tag{4}$$

If Eq. (4) holds, then solving $\mathsf{CVP}$ or $\mathsf{BDD}$ on $\Lambda_q(\mathbf{A}^\perp)$ with target $\mathbf{b}^\top$ would *not* necessarily yield $\mathbf{s}^\top\mathbf{A}^\perp$ or $\mathbf{e}^\top$, as the closest vector to $\mathbf{b}^\top$ would very likely not recover $\mathbf{e}$. In fact, there are likely exponentially many "decoy" values one could recover instead of $\mathbf{e}^\top$. For example, as in our suggested parameters for our PKE scheme, when we set $m$ as $m = n(1+\Theta(1))$, Eq. (4) becomes $\xi \gg q^{1-\Theta(1)} \cdot n^{\gamma/2}$—a feasible parameter setting.

*Discussion: The SIS Perspective.* Alternatively, one can look at the lattice $\mathcal{L} = \Lambda_q^\perp(\mathbf{A}^\perp)$, with the idea being that a short (nonzero) vector $\mathbf{x} \in \mathcal{L}$ can distinguish $\mathsf{LWSSE}$ by computing

$$\mathbf{b}^\top\mathbf{x} = \left(\mathbf{s}^\top\mathbf{A}^\perp + \mathbf{e}^\top\right)\mathbf{x} = \mathbf{e}^\top\mathbf{x} \pmod q,$$

where hopefully $|\mathbf{e}^\top\mathbf{x}| \ll q$. From the calculations above, the smallest non-zero $\mathbf{x} \in \mathcal{L}$ we can hope for has $\|\mathbf{x}\|_2 = \Theta(\sqrt{m} \cdot q^{1-n/m})$. By using independence of $\mathbf{x}$ and $\mathbf{e}$, we roughly have

$$|\mathbf{e}^\top\mathbf{x}| \approx \xi \cdot q^{1-n/m} \cdot \sqrt{\frac{m}{(m-n)^\gamma}}.$$

For the reduction to be *unsuccessful*, this would be above $q$. This holds when

$$\xi \gg q^{n/m} \cdot \sqrt{\frac{(m-n)^\gamma}{m}}. \tag{5}$$

Comparing Eqs. (4) and (5), the only difference is a $\sqrt{m}$ factor. Therefore, as long as Eq. (4) holds, none of these lattice reductions seem to work.

## 5 Analysis of the LW2E Assumption

*Information-Theoretically Secure Parameter Regime of LW2E.* Per standard lattice facts (see full version), with all but negligible probability, every entry of $\mathbf{e}_1$ is upper bound by $\sigma^{1+\mu}$, for non-negative constant $\mu \in (0,1)$.

Most of the mass of the distribution of $\mathbf{e}_1 + \mathbf{e}_2$ for $\mathbf{e}_1 \sim \mathcal{D}^m_{\mathbb{Z},\sigma}$ and $\mathbf{e}_2 \sim \mathcal{S}^m_{n,q,\delta}$ lies in a set of size $T = \binom{m}{n^{-\delta}m} q^{n^{-\delta}m} \sigma^{m(1+\mu)(1-n^{-\delta})}$. A straightforward entropic/combinatorial argument shows that Leftover Hash Lemma applies when $m \log q < n \log q + \log T$, and therefore, LW2E is information-theoretically hard. When $q = n^{O(1)}$, then standard algebraic manipulation shows that the above constraint gets satisfied when $m \ll \frac{n \log q}{\log q - \log \sigma}$.

### 5.1 Search-to-Decision Reduction of LW2E

Similar to ISSIS, we get a search-decision equivalence for LW2E as well. See full version for details.

**Corollary 2 (Decision LW2E is at least as hard as search LW2E).** *If there exists a PPT algorithm $\mathcal{A}$ that has non-negligible distinguishing advantage $\varepsilon : \mathbb{N} \to [0,1]$ for the decisional $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ assumption, then there exists a PPT algorithm $\mathcal{B}$ that inverts the search $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ assumption with non-negligible inversion advantage.*

### 5.2 Reduction from LPN and LWE

In this section, we prove that the learning with two errors assumption is at least as hard as both LWE and LPN with comparable parameters. Formally, we prove that the hardness of $\mathsf{LPN}_{n,m,q,\delta}$ and $\mathsf{LWE}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma}}$ can be reduced to the hardness of $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$. In other words, $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ is at least as hard as $\mathsf{LPN}_{n,m,q,\delta}$ and $\mathsf{LWE}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma}}$.

**Lemma 12.** *For all $n \in \mathbb{N}, m \in \mathbb{N}$, prime $q \in \mathbb{N}, \sigma > 0, \delta \in (0,1)$, if there exists a polynomial sized breaker for search[2]-$\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$, then there exists a polynomial sized breaker for search-$\mathsf{LPN}_{n,m,q,\delta}$ and search-$\mathsf{LWE}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma}}$.*

At a high level, given a LPN or LWE sample, one can simply add the error from the other distribution to generate a valid LW2E sample. The reduction is then straightforward. Refer to full version for formal details.

[2] The lemma and its proof works as it is even if we refer to the decisional variant of the respective assumptions.

### 5.3 Hardness of LW2E in the Presence of LWE and LPN Breaking Oracles

Having shown that LW2E is at least as hard as LWE and LPN, we provide some evidence that LW2E is a strictly harder problem. In particular, we show that it is unclear how to make use of an LWE or LPN breaking adversary in any natural ways to break LW2E.

*Conjecture 1.* $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ is secure even in the presence of an $\mathsf{LPN}_{n,m,q,\delta}$-breaking oracle or an $\mathsf{LWE}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma}}$-breaking oracle.

We believe that all the arguments here apply to both the search and decisional variant of the respective assumptions. However, to keep things succinct, we only talk explicitly about the search versions in the following discussion.

We strongly believe that this conjecture is true because of the very nature of the Learning With Two Errors assumption in which the error is neither small nor sparse. Recall that an $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ sample is of the form

$$\Big(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2\Big)$$

where $\mathbf{A} \xleftarrow{\$} \mathbb{F}_q^{m\times n}$, $\mathbf{s} \xleftarrow{\$} \mathbb{F}_q^t$, $\mathbf{e}_1 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z},\sigma}^m$, and $\mathbf{e}_2 \xleftarrow{\$} \mathcal{S}_{q,\delta}^m$. Here $\mathcal{D}_{\mathbb{Z},\sigma}$ is the small LWE error distribution, and $\mathcal{S}_{n,q,\delta}^m$ is the sparse but large LPN error distribution.

Let us assume that there is a $\mathsf{LPN}_{n,m,q,\delta}$-breaking oracle which can solve search-$\mathsf{LPN}_{n,m,q,\delta}$. Now say that we have received an $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ sample $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2)$. A direct use of the $\mathsf{LPN}_{n,m,q,\delta}$-breaking oracle to break LW2E is as follows:

- Since we know that as an Learning With Two Errors sample $\mathbf{b}$ must be of the form $\mathbf{u} + \mathbf{e}$ where $\mathbf{u}$ is a random vector in the column space of $\mathbf{A}$ and $\mathbf{e}$ is *some* error term. We can simply send $(\mathbf{A}, \mathbf{b})$ to the LPN breaking oracle.
- The oracle then sends us a response $(\mathbf{s}', \mathbf{e})$.
- We can now output $\mathbf{s}'$ which satisfies $\mathbf{A}\mathbf{s}' + \mathbf{e} = \mathbf{b}$ because of the correctness of LPN-breaking oracle.

However, observe that for the above algorithm to work, the number of non-zero elements in $\mathbf{e}$ must be less than the maximum number of non-zero error terms an $\mathsf{LPN}_{n,m,q,\delta}$ breaking oracle can handle, i.e., an expected number of non-zero entries of no more than $\frac{m}{n^\delta}$.

However, it is easy to see that $\mathbf{e}_1 + \mathbf{e}_2$ is very far from being sparse. In our case, $\mathbf{e}_1$ can have very few entries which are 0 and $\mathbf{e}_2$ already has $\frac{m}{n^\delta}$ many non-zero terms. Even with a few terms cancelling out over $\mathbb{F}_q$, it is definitely true that with an overwhelming (i.e., $1 - \mathsf{negl}$, where $\mathsf{negl}$ is a negligible function) probability, the number of non-zero entries in $\mathbf{e}$ i.e., $\mathbf{e}_1 + \mathbf{e}_2$ will be strictly greater than $\frac{m}{n^\delta}$ in which case there is no hope for a $\mathsf{LPN}_{n,m,q,\delta}$ breaking oracle to succeed in inverting $\mathbf{b}$.

But what about using a $\mathsf{LWE}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma}}$ oracle instead? Again, let us attempt to proceed by directly invoking the oracle. Observe that

– The error term $\mathbf{e}_1$ is sampled from $\mathcal{D}^m_{\mathbb{Z},\sigma}$. In such a case, as per standard lattice facts (see full version), for a small constant $\mu > 0$,

$$\Pr\left[e_{1,i} > \sigma^{1+\mu}\right] \leq 2e^{-\pi\sigma^{2\mu}}.$$

Since $\mathbf{e}_1$ has $m$ many entries, taking a union bound, we get

$$\Pr\left[\exists i \in [m] : e_{1,i} > \sigma^{1+\mu}\right] \leq 2\,m \cdot e^{-\pi\sigma^{2\mu}}.$$

This implies that with an overwhelming probability, there will be no entry in $\mathbf{e}_1$ which is more than $\sigma^{1+\mu}$.

– In the error term $\mathbf{e}_2$, the probability that an entry is greater than $\sigma^{1+\mu}$ and less than $q - \sigma^{1+\mu}$ is

$$\frac{1}{n^\delta} \cdot \frac{q - 2\sigma^{1+\mu}}{q}.$$

Therefore the expected number of entries in $\mathbf{e}_2$ which are greater than $\sigma^{1+\mu}$ and less than $q - \sigma^{1+\mu}$ is

$$\frac{m}{n^\delta} \cdot \frac{q - 2\sigma^{1+\mu}}{q}.$$

Here $n \leq m$ and $\delta \in (0, 1)$ and as per our choice of parameters $q > \zeta m B \sigma^{1+\mu}$ which makes the above expression $\Omega(m^{1-\delta})$.

The above two observations indicate that with an overwhelming probability there will be $\Omega(m^{1-\delta})$ many indices $i \in [m]$ in expectation such that

$$2\sigma^{1+\mu} < e_{1,i} + e_{2,i} < q.$$

Note that here the addition is over the integers.

On the other hand, clearly a $\mathsf{LWE}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma}}$-breaking oracle will only work if $\mathbf{e}$ is sampled from $\mathcal{D}^m_{\mathbb{Z},\sigma}$, in which case, with probability $1 - 2m \cdot e^{-\pi\sigma^{2\mu}}$ every entry of the error term must be less than $\sigma^{1+\mu}$. Thus an $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ sample has errors much larger than what a $\mathsf{LWE}$-breaking oracle can tolerate, indicating no clear way to use such an oracle to tackle the Learning With Two Errors assumption.

To summarize, a Learning With Two Errors error term is neither small nor sparse enough for either an $\mathsf{LPN}$-breaking oracle or an $\mathsf{LWE}$-breaking oracle to be useful. In fact, we conjecture that $\mathsf{LW2E}$ is secure even if we simultaneously had access to *both* an ISIS-breaking oracle and a $\mathsf{LPN}$-breaking oracle.

### 5.4 Hardness of $\mathsf{LW2E}$ in the Presence of $\mathsf{CVP}_\beta$ Oracles

We first show a reduction from $\mathsf{LW2E}$ to approximate $\mathsf{CVP}_\beta$, for appropriate approximation factor $\beta > 1$. While such a reduction exists for all choices of parameters that yield our PKE, we observe that the approximation factor required for the reduction is significantly smaller compared to what is sufficient to break $\mathsf{LWE}$. Formally, we prove the following lemma:

**Lemma 13.** *There exists a constant* $\kappa \in (0,1)$ *such that for all* $n \in \mathbb{N}$, $m = \mathsf{poly}(n)$, $\sigma = \mathsf{poly}(n)$, $q = \mathsf{poly}(n) > n^{0.5}\sigma^{1.1}$, $\delta \in (0,1)$, *decisional-*$\mathsf{LW2E}_{n,m,q,\sigma,\delta}$ *reduces to* $\mathsf{CVP}_\beta$ *where* $\beta = \frac{3\kappa n^{\delta/2}}{q^{\frac{n+1}{m}}}$.

*Proof.* Let $\mathcal{A}$ be the adversary that gets as input $(\mathbf{A} \in \mathbb{F}_q^{m\times n}, \mathbf{b} \in \mathbb{F}_q^m)$. It sends $(\mathbf{A}, \mathbf{b})$ to the $\mathsf{CVP}_\beta$ breaker $\mathcal{B}$ that then outputs some vector $\mathbf{t} \in \mathbb{F}_q^m$. If $\|\mathbf{b} - \mathbf{t}\|_2 \leq \kappa\sqrt{m}q^{1-\frac{n+1}{m}}$, then output 1, else output 0.

To prove the correctness of the reduction, it suffices to show that $\mathcal{B}$ outputs 1 with all but negligible probability when $\mathbf{b} = \mathbf{As} + \mathbf{e}_1 + \mathbf{e}_2$ where the errors are from the appropriate $\mathsf{LW2E}$ error distribution.

If $\mathbf{b}$ is of the form $\mathbf{As} + \mathbf{e}_1 + \mathbf{e}_2$. Then, $\|\Lambda_q(\mathbf{A}) - \mathbf{b}\|_2 = \|\mathbf{e}_1 + \mathbf{e}_2\|_2$. Our goal is to upper bound this norm first, $\|\mathbf{e}_1 + \mathbf{e}_2\|_2 \leq \|\mathbf{e}_1\|_2 + \|\mathbf{e}_2\|_2$.

By Chernoff, we know that $\mathbf{e}_2$ will have less than $2mn^{-\delta}$ many nonzero positions with all but negligible probability. Thus with all but negligible probability, it must be that $\|\mathbf{e}_2\|_2 \leq q\sqrt{2mn^{-\delta/2}}$. Similarly using the Gaussian tail bound, we know that every entry of $\mathbf{e}_1$ will be at most $\sigma^{1.1}$ with all but negligible probability, and therefore its norm will be upper bounded by $\sigma^{1.1}\sqrt{m}$. Thus with all but negligible probability

$$\|\mathbf{e}_1 + \mathbf{e}_2\|_2 \leq \sigma^{1.1}\sqrt{m} + q\sqrt{2\,mn}^{-\delta/2} \leq 3q\sqrt{mn}^{-\delta/2}.$$

The last inequality holds due to the lower bound on the choice of $q$.

Therefore, by the correctness of the $\mathsf{CVP}_\beta$ breaker, we know that with all but negligible probability, $\mathcal{B}$ returns $\mathbf{t}$ such that

$$\|\mathbf{b} - \mathbf{t}\|_2 \leq \beta \cdot 3q\sqrt{mn}^{-\delta/2} = \kappa\sqrt{m}q^{1-\frac{n+1}{m}},$$

and therefore $\mathcal{A}$ correctly outputs 1.

To complete the proof, we need to show that if $\mathbf{b}$ is uniform random, then $\|\Lambda_q(\mathbf{A}) - \mathbf{b}\|_2$ will be greater than $\kappa\sqrt{m}q^{1-\frac{n+1}{m}}$.

Observe that $\|\Lambda_q(\mathbf{A}) - \mathbf{b}\|_2$ is exactly equal the $\lambda_1$ of a random lattice generated by the $((n+1)\times m)$ dimensional matrix $\mathbf{A}\|\mathbf{b}$. $\kappa$ is exactly the value in Lemma 9 where with all but negligible probability $\lambda_1(\Lambda_q(\mathbf{A}\|\mathbf{b})) > \kappa\sqrt{m}q^{1-\frac{n+1}{m}}$ and therefore $\mathcal{A}$ must correctly output 0 in this case and we have the proof.

While we already show that our assumptions are unlikely to be broken using natural $\mathsf{LWE}$ and $\mathsf{AIe}$ breaking oracles, we would like to make a stronger claim. In particular we provide evidence that the $\mathsf{LW2E}$ assumption is potentially hard even upon given access to a approximate $\mathsf{CVP}_\beta$ for a wide range of parameters.

*Remark 11 (In-applicability of the reduction in the PKE parameter regime.).* Note that the above reduction is meaningless for $\beta < 1$. If we pick $m = 20n$ as in our PKE, $\delta = 0.9$, and $q = m^{10}$, then $q^{\frac{n+1}{m}} > q^{0.05} = \sqrt{m} > \sqrt{n} > n^{\delta/2}$, implying that $\beta < 1$.

*Discussion on larger values of $\beta$.*

*Conjecture 2.* For all $\beta > \omega\left(\frac{n^{\frac{\delta}{2}}}{q^{\frac{n+1}{m}}}\right)$, $\mathsf{LW2E}_{n,m,q,\mathcal{D}_{\mathbb{Z},\sigma},\delta}$ is secure even in the presence of a $\mathsf{CVP}_\beta$-breaking oracle when $q \gg \sigma^{1+\mu} n^{\delta/2}$, for some constant $\mu > 0$.

Observe that the above reduction works crucially because the choice of $\beta$ ensures that $\beta \cdot \|\mathbf{e}_1 + \mathbf{e}_2\|_2$ never exceeds $\kappa\sqrt{m}q^{1-\frac{n+1}{m}}$ with overwhelming probability. However if we picked $\beta \gg \frac{n^{\frac{\delta}{2}}}{q^{\frac{n+1}{m}}}$, then there is no more correctness guarantee as $\beta \cdot \|\mathbf{e}_1 + \mathbf{e}_2\|_2$ goes past the $\lambda_1$ of a random $m$-dimensional lattice spanned by an $n+1$ dimensional basis.

*Remark 12 (*$\mathsf{LW2E}$ *Harder than* $\mathsf{LWE}$ *Relative to a GapCVP Oracle.).* A back-of-the-envelope calculation shows that a $\mathsf{CVP}_\beta$ breaking oracle with $\beta = n^{\frac{1}{2}}$ will break $\mathsf{LWE}$ [6,34]. On the other hand, we have given the above heuristic evidence that a $\mathsf{CVP}_\beta$ breaking oracle with $\beta = \omega(n^{\delta/2})$ does not break the $\mathsf{LW2E}$ assumption. In our setting, we have set $\delta$ such that $\frac{1}{2} < \delta < 1$, which means that $\beta$ is strictly $o(n^{\frac{1}{2}})$.

**Acknowledgements.** This research was supported in part from a Simons Investigator Award, DARPA SIEVE award, NTT Research, NSF grant 2333935, BSF grant 2022370, a Xerox Faculty Research Award, a Google Faculty Research Award, an Okawa Foundation Research Grant, and the Symantec Chair of Computer Science. This material is based upon work supported by the Defense Advanced Research Projects Agency through Award HR00112020024. The second author is supported in part by a Google Faculty Research Scholarship, the CMU Cylab, and a Stellar Foundation Research Grant. The last author is supported in part by DARPA under Agreement No. HR00112020023, NSF CNS-2154149, NSF DGE-2141064, and a Simons Investigator Award.

## References

1. Alekhnovich, M.: More on average case vs approximation complexity. In: 44th FOCS, pp. 298–307. IEEE Computer Society Press (2003)
2. Beullens, W.: Breaking rainbow takes a weekend on a laptop. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022, Part II. LNCS, vol. 13508, pp. 464–479. Springer, Cham (Aug (2022)
3. Boneh, D., et al.: Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 533–556. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_30
4. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. In: Goldwasser, S. (ed.) ITCS 2012, pp. 309–325. ACM (2012)
5. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: Ostrovsky, R. (ed.) 52nd FOCS, pp. 97–106. IEEE Computer Society Press (2011)

6. Brakerski, Z., Vaikuntanathan, V.: Lattice-based the as secure as PKE. In: Proceedings of the 5th Conference on Innovations in Theoretical Computer Science, pp. 1–12 (2014)
7. Carrier, K., Debris-Alazard, T., Meyer-Hilfiger, C., Tillich, J.P.: Reduction from sparse LPN to LPN, dual attack 3.0. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024, Part VII. LNCS, vol. 14657, pp. 286–315. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-58754-2_11
8. Chen, Y.: Quantum algorithms for lattice problems. Cryptology ePrint Archive (2024)
9. Damgård, I., Park, S.: Is public-key encryption based on LPN practical? IACR Cryptol. ePrint Arch. p. 699 (2012). http://eprint.iacr.org/2012/699
10. Dao, Q., Ishai, Y., Jain, A., Lin, H.: Multi-party homomorphic secret sharing and sublinear MPC from sparse LPN. In: Handschuh, H., Lysyanskaya, A. (eds.) CRYPTO 2023, Part II. LNCS, vol. 14082, pp. 315–348. Springer, Cham (Aug (2023). https://doi.org/10.1007/978-3-031-38545-2_11
11. Dao, Q., Jain, A.: Lossy cryptography from code-based assumptions. In: Reyzin, L., Stebila, D. (eds.) CRYPTO 2024, Part III. LNCS, vol. 14922, pp. 34–75. Springer, Cham (Aug (2024). https://doi.org/10.1007/978-3-031-68382-4_2
12. Eldar, L., Shor, P.W.: An efficient quantum algorithm for a variant of the closest lattice-vector problem. arXiv preprint arXiv:1611.06999 (2016)
13. Gentry, C.: Toward basing fully homomorphic encryption on worst-case hardness. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 116–137. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_7
14. 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
15. Goldwasser, S., Kalai, Y.T., Popa, R.A., Vaikuntanathan, V., Zeldovich, N.: Reusable garbled circuits and succinct functional encryption. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) 45th ACM STOC. pp. 555–564. ACM Press (2013)
16. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Functional encryption with bounded collusions via multi-party computation. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 162–179. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_11
17. Hastings, M.B.: Classical and quantum bounded depth approximation algorithms. arXiv preprint arXiv:1905.07047 (2019)
18. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: a ring-based public key cryptosystem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0054868
19. 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 (2021)
20. Lai, Q., Liu, F.H., Wang, Z.: New lattice two-stage sampling technique and its applications to functional encryption - stronger security and smaller ciphertexts. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part I. LNCS, vol. 12696, pp. 498–527. Springer, Cham (Oct (2021). https://doi.org/10.1007/978-3-030-77870-5_18
21. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_1

22. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-LWE cryptography. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 35–54. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_3
23. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. The deep space network progress report 42-44, Jet Propulsion Laboratory, California Institute of Technology (1978). https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF
24. Micciancio, D.: The geometry of lattice cryptography. In: Aldini, A., Gorrieri, R. (eds.) FOSAD 2011. LNCS, vol. 6858, pp. 185–210. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23082-0_7
25. Micciancio, D., Mol, P.: Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 465–484. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_26
26. Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: 22nd ACM STOC, pp. 427–437. ACM Press (1990)
27. Peikert, C., Regev, O., Stephens-Davidowitz, N.: Pseudorandomness of ring-LWE for any ring and modulus. In: Hatami, H., McKenzie, P., King, V. (eds.) 49th ACM STOC, pp. 461–473. ACM Press (2017)
28. Peikert, C., Shiehian, S.: Noninteractive zero knowledge for NP from (Plain) learning with errors. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11692, pp. 89–114. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26948-7_4
29. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM (JACM) **56**(6), 1–40 (2009)
30. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 472–503. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-30589-4_17
31. Sahai, A.: Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In: 40th FOCS, pp. 543–553. IEEE Computer Society Press (1999)
32. Schmidhuber, A., O'Donnell, R., Kothari, R., Babbush, R.: Quartic quantum speedups for planted inference. arXiv preprint arXiv:2406.19378 (2024)
33. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: 35th FOCS, pp. 124–134. IEEE Computer Society Press (1994)
34. Stephens-Davidowitz, N.: Dimension-preserving reductions between lattice problems (2016). http://www.noahsd.com/latticeproblems.pdf
35. Vaikuntanathan, V., Wee, H., Wichs, D.: Witness encryption and null-IO from evasive LWE. In: Agrawal, S., Lin, D. (eds.) ASIACRYPT 2022, Part I. LNCS, vol. 13791, pp. 195–221. Springer, Cham (Dec (2022). https://doi.org/10.1007/978-3-031-22963-3_7
36. Wichs, D., Zirdelis, G.: Obfuscating compute-and-compare programs under LWE. In: Umans, C. (ed.) 58th FOCS, pp. 600–611. IEEE Computer Society Press (2017)
37. Yu, Yu., Zhang, J.: Cryptography with auxiliary input and trapdoor from constant-noise LPN. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 214–243. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53018-4_9