

Quantum Proofs of Deletion for Learning with Errors

Alexander Poremba   

California Institute of Technology, Pasadena, CA, USA

Abstract

Quantum information has the property that measurement is an inherently destructive process. This feature is most apparent in the principle of complementarity, which states that mutually incompatible observables cannot be measured at the same time. Recent work by Broadbent and Islam (TCC 2020) builds on this aspect of quantum mechanics to realize a cryptographic notion called *certified deletion*. While this remarkable notion enables a classical verifier to be convinced that a (private-key) quantum ciphertext has been deleted by an untrusted party, it offers no additional layer of functionality.

In this work, we augment the proof-of-deletion paradigm with fully homomorphic encryption (FHE). We construct the first fully homomorphic encryption scheme with certified deletion – an interactive protocol which enables an untrusted quantum server to compute on encrypted data and, if requested, to simultaneously prove data deletion to a client. Our scheme has the desirable property that verification of a deletion certificate is *public*; meaning anyone can verify that deletion has taken place. Our main technical ingredient is an interactive protocol by which a quantum prover can convince a classical verifier that a sample from the Learning with Errors (LWE) distribution in the form of a quantum state was deleted. As an application of our protocol, we construct a *Dual-Regev* public-key encryption scheme with certified deletion, which we then extend towards a (leveled) FHE scheme of the same type. We introduce the notion of *Gaussian-collapsing* hash functions – a special case of collapsing hash functions defined by Unruh (Eurocrypt 2016) – and we prove the security of our schemes under the assumption that the Ajtai hash function satisfies a certain *strong* Gaussian-collapsing property in the presence of leakage.

2012 ACM Subject Classification Theory of computation → Computational complexity and cryptography

Keywords and phrases Learning with errors, certified deletion, fully homomorphic encryption

Digital Object Identifier 10.4230/LIPIcs.ITCS.2023.90

Related Version *Full Version*: <https://eprint.iacr.org/2022/295>

Funding *Alexander Poremba*: Partially supported by AFOSR YIP award number FA9550-16-1-0495 and the Institute for Quantum Information and Matter (an NSF Physics Frontiers Center; NSF Grant PHY-1733907).

Acknowledgements I would like to thank Urmila Mahadev, Thomas Vidick, Prabhanjan Ananth and Vinod Vaikuntanathan for many insightful discussions.

1 Introduction

Data protection has become a major challenge in the age of cloud computing and artificial intelligence. The European Union, Argentina, and California recently introduced new data privacy regulations which grant individuals the right to request the deletion of their personal data by *media companies* and other *data collectors* – a legal concept that is commonly referred to as the *right to be forgotten* [12]. While new data privacy regulations have been put into practice in several jurisdictions, formalizing data deletion remains a fundamental challenge for cryptography. A key question, in particular, prevails:

How can we certify that user data stored on a remote cloud server has been deleted?



© Alexander Poremba;
licensed under Creative Commons License CC-BY 4.0
14th Innovations in Theoretical Computer Science Conference (ITCS 2023).
Editor: Yael Tauman Kalai; Article No. 90; pp. 90:1–90:14



Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Without any further assumptions, the task is clearly impossible to realize in conventional cloud computing. This is due to the fact that there is no way of preventing the data collector from generating and distributing additional copies of the user data. Although it is impossible to achieve in general, *proofs-of-secure-erasure* [25, 11] can achieve a limited notion of data deletion under *bounded memory assumptions*. Recently, Garg, Goldwasser and Vasudevan [12] proposed rigorous definitions that attempt to formalize the *right to be forgotten* from the perspective of classical cryptography. However, a fundamental challenge in the work of Garg et al. [12] lies in the fact that the data collector is always assumed to be *honest*, which clearly limits the scope of the formalism.

A recent exciting idea is to use quantum information in the context of data privacy [10, 7]. Contrary to classical data, it is fundamentally impossible to create copies of an unknown quantum state thanks to the *quantum no-cloning theorem* [31]. Building on the work of Coiteux-Roy and Wolf [10], Broadbent and Islam [7] proposed a quantum encryption scheme which enables a user to certify the deletion of a quantum ciphertext. Unlike classical proofs-of-secure-erasure, this notion of certified deletion is achievable unconditionally in a fully malicious adversarial setting [7]. All prior protocols for certified deletion enable a client to delegate data in the form of plaintexts and ciphertexts with no additional layer of functionality. A key question raised by Broadbent and Islam [7] is the following:

Can we enable a remote cloud server to compute on encrypted data, while simultaneously allowing the server to prove data deletion to a client?

This cryptographic notion can be seen as an extension of fully homomorphic encryption schemes [27, 13, 5] which allow for arbitrary computations over encrypted data. Prior work on certified deletion makes use of very specific encryption schemes that seem incompatible with such a functionality; for example, the private-key encryption scheme of Broadbent and Islam [7] requires a classical *one-time pad*, whereas the authors in [18] use a particular *hybrid encryption* scheme in the context of public-key cryptography. While homomorphic encryption enables a wide range of applications including private queries to a search engine and machine learning classification on encrypted data [4], a fundamental limitation remains: once the protocol is complete, the cloud server is still in possession of the client's encrypted data. This may allow adversaries to break the encryption scheme retrospectively, i.e. long after the execution of the protocol. This potential threat especially concerns data which is required to remain confidential for many years, such as medical records or government secrets.

Fully homomorphic encryption with certified deletion seeks to address this limitation as it allows a quantum cloud server to compute on encrypted data while simultaneously enabling the server to prove data deletion to a client, thus effectively achieving a form of *everlasting security* [24, 17].

2 Main results

Our approach for certified deletion deviates from the hybrid encryption paradigm of previous works [7, 17]. The main technical ingredient of our schemes is an interactive protocol by which a quantum prover can convince a classical verifier that a sample from the *Learning with Errors* [26] distribution in the form of a quantum state was deleted. Our techniques are inspired by the quantum reduction from the *Short Integer Solution* (SIS) problem to the *Learning with Errors* (LWE) problem [26, 29]. We use Gaussian superposition states to encode LWE samples for the purpose of certified deletion while simultaneously preserving their full cryptographic functionality. Because verification of a deletion certificate amounts to checking whether it is a solution to the (inhomogenous) SIS problem, our encoding results

in encryption schemes with certified deletion which are publicly verifiable – in contrast to prior work based on hybrid encryption and BB84 states [7, 17]. Our results suggest a generic template for *certified deletion* protocols which can be applied to many other cryptographic primitives based on LWE.

2.1 Gaussian-collapsing hash functions

To analyze the security of our quantum encryption schemes based on Gaussian states, we introduce the notion of *Gaussian-collapsing* hash functions – a special class of so-called *collapsing* hash functions defined by Unruh [30]. Informally, a hash function h is *Gaussian-collapsing* if it is computationally difficult to distinguish a superposition of Gaussian-weighted pre-images under h from a single (measured) Gaussian pre-image. We prove that the *Ajtai collision-resistant hash function* [1] is Gaussian-collapsing assuming the quantum subexponential hardness of the decisional LWE problem.

► **Theorem 1** (informal). *The Ajtai hash function is Gaussian-collapsing assuming the quantum subexponential hardness of the LWE problem.*

We conjecture that the Ajtai hash function also satisfies a stronger variant of the Gaussian-collapsing property in the presence of leakage (formally defined in Section 5.2).

2.2 Dual-Regev public-key encryption with certified deletion

Using Gaussian superpositions, we construct a public-key encryption scheme with certified deletion which is based on the *Dual-Regev* scheme introduced by Gentry, Peikert and Vaikuntanathan [14]. We prove the security of our scheme under the assumption that Ajtai’s hash function satisfies the strong Gaussian-collapsing property in the presence of leakage.

► **Theorem 2** (informal). *There exists a secure Dual-Regev public-key encryption scheme with certified deletion (and public verification) under the strong Gaussian-collapsing assumption.*

2.3 (Leveled) fully homomorphic encryption with certified deletion

We construct the first (leveled) fully homomorphic encryption (FHE) scheme with certified deletion based on our aforementioned *Dual-Regev* encryption scheme with the identical security guarantees. Our FHE scheme is based on the (classical) *dual homomorphic encryption* scheme used by Mahadev [22], which is a variant of the FHE scheme by Gentry, Sahai and Waters [15]. Our protocol supports the evaluation of polynomial-sized Boolean circuits on encrypted data and, if requested, also enables the server to prove data deletion to a client.

► **Theorem 3** (informal). *There exists a secure Dual-Regev (leveled) FHE scheme with certified deletion (and public verification) under the strong Gaussian-collapsing assumption.*

3 Applications

Data retention and the right to be forgotten. The European Union, Argentina, and California recently introduced new data privacy regulations – often referred to as the *right to be forgotten* [12] – which grant individuals the right to request the deletion of their personal data by media companies. However, formalizing data deletion still remains a fundamental challenge for cryptography. Our fully homomorphic encryption scheme with certified deletion achieves a rigorous notion of *long-term data privacy*: it enables a remote quantum cloud server to compute on encrypted data and – once it is deleted and publicly verified – the client’s data remain safeguarded against a future leak that reveals the secret key.

Private machine learning on encrypted data. Machine learning algorithms are used for wide-ranging classification tasks, such as medical predictions, spam detection and face recognition. While homomorphic encryption enables a form of privacy-preserving machine learning [4], a fundamental limitation remains: once the protocol is complete, the cloud server is still in possession of the client’s encrypted data. This threat especially concerns data which is required to remain confidential for many years. Our results remedy this situation by enabling private machine learning on encrypted data with certified data deletion.

Everlasting cryptography. Assuming that the server has not broken the computational assumption before data deletion has taken place, our results could potentially transform a long-term LWE assumption [26] into a temporary one, and thus effectively achieve a form of *everlasting security* [24, 17].

4 Technical Summary

The *Learning with Errors* (LWE) problem was introduced by Regev [26] and has given rise to numerous cryptographic applications, including public-key encryption [14], homomorphic encryption [6, 15] and attribute-based encryption [3]. Let $n, m \in \mathbb{N}$ and $q \geq 2$ be a prime modulus, and $\alpha \in (0, 1)$ be a noise ratio parameter. In its decisional formulation, the $\text{LWE}_{n,q,\alpha}^m$ problem asks to distinguish between a sample $(\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}, \mathbf{s} \cdot \mathbf{A} + \mathbf{e} \pmod{q})$ from the LWE distribution and a uniformly random sample. Here, $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$ is a uniformly random row vector and $\mathbf{e} \sim D_{\mathbb{Z}^m, \alpha q}$ is a row vector which is sampled according to the discrete Gaussian distribution $D_{\mathbb{Z}^m, \alpha q}$. The latter distribution assigns probability proportional to $\rho_r(\mathbf{x}) = e^{-\pi \|\mathbf{x}\|^2 / r^2}$ to every lattice point $\mathbf{x} \in \mathbb{Z}^m$, for $r = \alpha q > 0$.

How can we certify that a (possibly malicious) party has deleted a sample from the LWE distribution? The main technical insight of our work is that one can encode LWE samples as *quantum superpositions* for the purpose of certified deletion while simultaneously preserving their full cryptographic functionality. Superpositions of LWE samples have been considered by Grilo, Kerenidis and Zijlstra [16] in the context of quantum learning theory and by Alagic, Jeffery, Ozols and Poremba [2], as well as by Chen, Liu and Zhandry [9], in the context of quantum cryptanalysis of LWE-based cryptosystems.

Let us now describe the main idea behind our constructions. Consider the Gaussian superposition,¹

$$|\hat{\psi}\rangle_{XY} = \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle_X \otimes |\mathbf{A} \cdot \mathbf{x} \pmod{q}\rangle_Y.$$

Here, we let $\sigma = 1/\alpha$ and use \mathbb{Z}_q^m to represent $\mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$. By measuring system Y in the computational basis with outcome $\mathbf{y} \in \mathbb{Z}_q^n$, the state $|\hat{\psi}\rangle$ *collapses* into the quantum superposition

$$|\hat{\psi}_{\mathbf{y}}\rangle = \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^m: \\ \mathbf{A}\mathbf{x} = \mathbf{y} \pmod{q}}} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle. \quad (1)$$

¹ A standard tail bound shows that the discrete Gaussian $D_{\mathbb{Z}^m, \sigma}$ is essentially only supported on $\{\mathbf{x} \in \mathbb{Z}^m : \|\mathbf{x}\| \leq \sigma\sqrt{m}\}$. We choose $\sigma \ll q/\sqrt{m}$ and consider the domain $\mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$ instead. For simplicity, we also ignore that $|\hat{\psi}\rangle$ is not normalized.

Note that the state $|\hat{\psi}_{\mathbf{y}}\rangle$ is now a superposition of *short* Gaussian-weighted solutions $\mathbf{x} \in \mathbb{Z}_q^m$ subject to the constraint $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \pmod{q}$. In other words, by measuring the above state in the computational basis, we obtain a solution to the so-called (*inhomogenous*) *short integer solution* (ISIS) problem specified by (\mathbf{A}, \mathbf{y}) . The quantum state $|\hat{\psi}_{\mathbf{y}}\rangle$ in Eq. (1) has the following *duality property*; namely, by applying the (inverse) q -ary quantum Fourier transform we obtain the state

$$|\psi_{\mathbf{y}}\rangle = \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \rho_{\frac{q}{\sigma}}(\mathbf{e}) \omega_q^{-\langle \mathbf{s}, \mathbf{y} \rangle} |\mathbf{sA} + \mathbf{e} \pmod{q}\rangle, \quad (2)$$

where $\omega_q = e^{2\pi i/q}$ is the primitive q -th root of unity. Throughout this work, we will refer to $|\psi_{\mathbf{y}}\rangle$ and $|\hat{\psi}_{\mathbf{y}}\rangle$ as the *primal* and *dual* Gaussian state, respectively. Notice that the resulting state $|\psi_{\mathbf{y}}\rangle$ is now a quantum superposition of samples from the LWE distribution. This relationship was first observed in the work of Stehlé et al. [29] who gave quantum reduction from SIS to LWE based on Regev's reduction [26], and was later implicitly used by Roberts [28] and Kitagawa et al. [20] to construct quantum money and secure software leasing schemes.

Our quantum encryption schemes with certified deletion exploit the fact that a measurement of $|\psi_{\mathbf{y}}\rangle$ in the *Fourier basis* yields a short solution to the ISIS problem specified by (\mathbf{A}, \mathbf{y}) , whereas ciphertext information which is necessary to decrypt is encoded using LWE samples in the *computational basis*.

4.1 Dual-Regev public-key encryption with certified deletion

The key ingredient of our homomorphic encryption scheme with certified deletion is the *Dual-Regev* public-key encryption scheme introduced by Gentry, Peikert and Vaikuntanathan [14]. Using Gaussian states, we can encode Dual-Regev ciphertexts for the purpose of certified deletion while simultaneously preserving their full cryptographic functionality. Our scheme Dual-Regev scheme with certified deletion consists of the following efficient algorithms:

- To generate a pair $(\mathbf{sk}, \mathbf{pk})$, sample $\mathbf{A} \in \mathbb{Z}_q^{n \times (m+1)}$ together with a particular short trapdoor vector $\mathbf{t} \in \mathbb{Z}^{m+1}$ such that $\mathbf{A} \cdot \mathbf{t} = \mathbf{0} \pmod{q}$, and let $\mathbf{pk} = \mathbf{A}$ and $\mathbf{sk} = \mathbf{t}$.
- To encrypt $b \in \{0, 1\}$ using the public key $\mathbf{pk} = \mathbf{A}$, generate for a random $\mathbf{y} \in \mathbb{Z}_q^n$:

$$\mathbf{vk} \leftarrow (\mathbf{A}, \mathbf{y}), \quad |\mathbf{CT}\rangle \leftarrow \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^{m+1}} \rho_{\frac{q}{\sigma}}(\mathbf{e}) \omega_q^{-\langle \mathbf{s}, \mathbf{y} \rangle} |\mathbf{sA} + \mathbf{e} + b \cdot (0, \dots, 0, \lfloor \frac{q}{2} \rfloor)\rangle,$$

where \mathbf{vk} is a public verification key and $|\mathbf{CT}\rangle$ is the quantum ciphertext for $\sigma = 1/\alpha$.

- To decrypt a ciphertext $|\mathbf{CT}\rangle$ using the secret key \mathbf{sk} , measure in the computational basis to obtain an outcome $\mathbf{c} \in \mathbb{Z}_q^{m+1}$, and output 0, if $\mathbf{c}^T \cdot \mathbf{sk} \in \mathbb{Z}_q$ is closer to 0 than to $\lfloor \frac{q}{2} \rfloor$, and output 1, otherwise.

To delete the ciphertext $|\mathbf{CT}\rangle$, we simply perform measurement in the Fourier basis. We show that the Fourier transform of the ciphertext $|\mathbf{CT}\rangle$ results in the *dual* quantum state

$$|\widehat{\mathbf{CT}}\rangle = \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^{m+1}: \\ \mathbf{Ax} = \mathbf{y} \pmod{q}}} \rho_{\sigma}(\mathbf{x}) \omega_q^{\langle \mathbf{x}, b \cdot (0, \dots, 0, \lfloor \frac{q}{2} \rfloor) \rangle} |\mathbf{x}\rangle. \quad (3)$$

Notice that a Fourier basis measurement of $|\mathbf{CT}\rangle$ necessarily erases all information about the plaintext $b \in \{0, 1\}$ and results in a *short* vector $\pi \in \mathbb{Z}_q^{m+1}$ such that $\mathbf{A} \cdot \pi = \mathbf{y} \pmod{q}$. In other words, to verify a deletion certificate we can simply check whether it is a solution

$$\begin{array}{ccc}
 \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^m \\ \mathbf{A}\mathbf{x} = \mathbf{y} \pmod{q}}} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle & \approx_c & |\mathbf{x}_0\rangle, \quad \mathbf{x}_0 \sim D_{\Lambda_q^\perp(\mathbf{A}), \frac{\sigma}{\sqrt{2}}} \\
 \uparrow \text{FT}_q & & \uparrow \text{FT}_q \\
 \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \rho_{\frac{q}{\sigma}}(\mathbf{e}) \omega_q^{-\langle \mathbf{s}, \mathbf{y} \rangle} |\mathbf{s}\mathbf{A} + \mathbf{e}\rangle & \approx_c & \sum_{\mathbf{u} \in \mathbb{Z}_q^m} \omega_q^{-\langle \mathbf{u}, \mathbf{x}_0 \rangle} |\mathbf{u}\rangle
 \end{array}$$

■ **Figure 1** Overview of the Gaussian superposition states and their properties shown in this work. The computational indistinguishability property holds under the (decisional) LWE assumption. Here, FT_q denotes the q -ary Fourier transform and $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A} \cdot \mathbf{x} = \mathbf{0} \pmod{q}\}$ denotes a particular coset of the q -ary lattice $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A} \cdot \mathbf{x} = \mathbf{0} \pmod{q}\}$.

to the ISIS problem specified by the verification key $\text{vk} = (\mathbf{A}, \mathbf{y})$. Our scheme has the desirable property that verification of a certificate π is public; meaning anyone in possession of (\mathbf{A}, \mathbf{y}) can verify that $|\text{CT}\rangle$ has been successfully deleted. Moreover, due to the tight connection between worst-case lattice problems and the average-case ISIS problem [23, 14], it is computationally difficult to produce a valid deletion certificate from (\mathbf{A}, \mathbf{y}) alone.

To formalize security, we use the notion of *certified deletion security* (formally, IND-CPA-CD security) [7, 17] which roughly states that, once deletion of the ciphertext is successful, the plaintext remains hidden even if the secret key is later revealed. We prove the security of our schemes under the assumption that the Ajtai *collision-resistant* hash function $h_{\mathbf{A}}(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x} \pmod{q}$ satisfies a certain strong *collapsing property* in the presence of leakage.

4.2 Gaussian-collapsing hash functions.

Unruh [30] introduced the notion of collapsing hash functions in his seminal work on computationally binding quantum commitments. Informally, a hash function h is called *collapsing* if it is computationally difficult to distinguish between a superposition of pre-images, i.e. $\sum_{\mathbf{x}: h(\mathbf{x})=\mathbf{y}} \alpha_{\mathbf{x}} |\mathbf{x}\rangle$, and a single measured pre-image $|\mathbf{x}_0\rangle$ such that $h(\mathbf{x}_0) = \mathbf{y}$. Motivated by the properties of the dual Gaussian state in Eq. (1), we consider a special class of hash functions which are *collapsing* with respect to Gaussian superpositions. We say that a hash function h is σ -*Gaussian-collapsing*, for some $\sigma > 0$, if the following states are computationally indistinguishable:

$$\sum_{\mathbf{x}: h(\mathbf{x})=\mathbf{y}} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle \approx_c |\mathbf{x}_0\rangle, \quad \text{s.t. } h(\mathbf{x}_0) = \mathbf{y}.$$

Here, \mathbf{x}_0 is the result of a computational basis measurement of the the Gaussian superposition (on the left). Notice that any collapsing hash function h is necessarily also *Gaussian-collapsing*, since a superposition of Gaussian-weighted vectors constitutes a special class of inputs to h . Liu and Zhandry [21] implicitly showed that the *Ajtai hash function* $h_{\mathbf{A}}(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x} \pmod{q}$ is

collapsing – and thus *Gaussian-collapsing* – via the notion of *lossy functions* and (decisional) LWE. In this work, we give a simple and direct proof of the Gaussian-collapsing property assuming (decisional) LWE, which might be of independent interest.

The fact Ajtai’s hash function is Gaussian-collapsing has several implications for the security of our schemes. Because our Dual-Regev ciphertext corresponds to the Fourier transform of the state in Eq. (3), the Gaussian-collapsing property immediately implies the semantic (i.e., IND-CPA) security under decisional LWE. We refer to Fig. 1 for an overview of our Gaussian states and their properties.

To prove the stronger notion of IND-CPA-CD security of our Dual-Regev scheme with certified deletion, we have to show that, once deletion has taken place, the plaintext remains hidden even if the secret key (i.e., a short trapdoor vector \mathbf{t} in the kernel of \mathbf{A}) is later revealed. In other words, it is sufficient to show that Ajtai’s hash function satisfies a particular *strong Gaussian-collapsing property* in the presence of leakage; namely, once an adversary \mathcal{A} produces a valid short certificate π with the property that $\mathbf{A} \cdot \pi = \mathbf{y} \pmod{q}$, then \mathcal{A} cannot tell whether the input at the beginning of the experiment corresponded to a Gaussian superposition of pre-images or a single (measured) pre-image, even if \mathcal{A} later receives a short trapdoor vector \mathbf{t} in the kernel of \mathbf{A} . Here, it is crucial that \mathcal{A} receives the trapdoor vector \mathbf{t} only *after* \mathcal{A} provides a valid pre-image witness π , otherwise \mathcal{A} could trivially distinguish the two states by applying the Fourier transform and using the trapdoor \mathbf{t} to distinguish between a superposition of LWE samples and a uniform superposition.

Unfortunately, we currently do not know how to prove the *strong* Gaussian-collapsing property of the Ajtai hash function from standard assumptions (such as LWE or ISIS). The problem emerges when we attempt to give a reduction between the IND-CPA-CD security of our Dual-Regev public-key encryption scheme with certified deletion and the LWE (or ISIS) problem. In order to simulate the IND-CPA-CD game successfully, we have to eventually forward a short trapdoor vector $\mathbf{t} \in \mathbb{Z}^{m+1}$ (i.e. the secret key) to the adversary once deletion has taken place. Notice, however, that the reduction has no way of obtaining a short trapdoor vector \mathbf{t} such that $\mathbf{A} \cdot \mathbf{t} = \mathbf{0} \pmod{q}$ as it is trying to break the underlying LWE (or ISIS) problem with respect to \mathbf{A} in the first place (!) Recently, Hiroka, Morimae, Nishimaki and Yamakawa [17] managed to overcome similar technical difficulties using the notion of *receiver non-committing* (RNC) encryption [19, 8] in the context of *hybrid encryption* in order to produce a *fake* secret key. In our case, we cannot rely on similar techniques involving RNC encryption as it seems difficult to reconcile with homomorphic encryption, which is the main focus of this work. Instead, we choose to formalize the strong Gaussian-collapsing property of the Ajtai hash function as a simple and falsifiable conjecture. To see why the conjecture is plausible, consider the following natural attack. Given as input either a Gaussian superposition of pre-images or a single (measured) pre-image, we perform the quantum Fourier transform, reversibly shift the outcome by a fresh LWE sample² and store the result in an auxiliary register. If the input corresponds to a superposition, we obtain a separate LWE sample which is *re-randomized*, whereas if the input is a single (measured) pre-image, the outcome remains random. Hence, if the aforementioned procedure succeeded without disturbing the initial quantum state, we could potentially provide a valid certificate π and also distinguish the auxiliary system with access to the trapdoor. However, by shifting the state by another LWE sample, we have necessarily entangled the two systems in a way that prevents us from finding a valid certificate via a Fourier basis measurement. We make

² To *smudge* the Gaussian error of the initial superposition, we can choose an error from a discrete Gaussian distribution which has a significantly larger standard deviation.

this fact more precise by proving a general *uncertainty relation for Fourier basis projections* that rules out a large class of attacks, including the *shift-by-LWE-sample* attack described above. Next, we extend our Dual-Regev scheme towards a (leveled) FHE scheme with certified deletion.

4.3 Dual-Regev fully homomorphic encryption with certified deletion.

Our (leveled) FHE scheme with certified deletion is based on the (classical) Dual-Regev leveled FHE scheme used by Mahadev [22] – a variant of the scheme due to Gentry, Sahai and Waters [15]. Let $n, m \in \mathbb{N}$, let $q \geq 2$ be a prime modulus, and let $\alpha \in (0, 1)$ be the noise ratio with $\sigma = 1/\alpha$. Let $N = (n + 1)\lceil \log q \rceil$ and let $\mathbf{G} \in \mathbb{Z}_q^{(m+1) \times N}$ denote the *gadget matrix* designed to convert a binary representation of a vector back to its \mathbb{Z}_q representation. The scheme consists of the following efficient algorithms:

- To generate a pair of keys $(\mathbf{sk}, \mathbf{pk})$, sample $\mathbf{A} \in \mathbb{Z}_q^{(m+1) \times n}$ together with a particular short trapdoor vector $\mathbf{t} \in \mathbb{Z}^{m+1}$ such that $\mathbf{t} \cdot \mathbf{A} = \mathbf{0} \pmod{q}$, and let $\mathbf{pk} = \mathbf{A}$ and $\mathbf{sk} = \mathbf{t}$.
- To encrypt a bit $x \in \{0, 1\}$ using the public key $\mathbf{A} \in \mathbb{Z}_q^{(m+1) \times n}$, generate the following pair consisting of a verification key and ciphertext for a random $\mathbf{Y} \in \mathbb{Z}_q^{n \times N}$ with columns $\mathbf{y}_1, \dots, \mathbf{y}_N \in \mathbb{Z}_q^n$:

$$\text{vk} \leftarrow (\mathbf{A}, \mathbf{Y}), \quad |\text{CT}\rangle \leftarrow \sum_{\mathbf{S} \in \mathbb{Z}_q^{n \times N}} \sum_{\mathbf{E} \in \mathbb{Z}_q^{(m+1) \times N}} \rho_{q/\sigma}(\mathbf{E}) \omega_q^{-\text{Tr}[\mathbf{S}^T \mathbf{Y}]} |\mathbf{A} \cdot \mathbf{S} + \mathbf{E} + x \cdot \mathbf{G}\rangle,$$

where $\mathbf{G} \in \mathbb{Z}_q^{(m+1) \times N}$ denotes the *gadget matrix* and where $\sigma = 1/\alpha$.

- To decrypt a quantum ciphertext $|\text{CT}\rangle$ using the secret key \mathbf{sk} , measure in the computational basis to obtain an outcome $\mathbf{C} \in \mathbb{Z}_q^{(m+1) \times N}$ and compute $c = \mathbf{sk}^T \cdot \mathbf{c}_N \in \mathbb{Z}_q$, where $\mathbf{c}_N \in \mathbb{Z}_q^{m+1}$ is the N -th column of \mathbf{C} , and then output 0, if c is closer to 0 than to $\lfloor \frac{q}{2} \rfloor$, and output 1, otherwise.

We remark that deletion and verification take place as in our Dual-Regev scheme with certified deletion.

Our FHE scheme supports the evaluation of polynomial-sized Boolean circuits consisting entirely of NAND gates, which are universal for classical computation. Inspired by the classical homomorphic NAND operation of the Dual-Regev scheme [15, 22], we define an analogous quantum operation U_{NAND} which allows us to apply a NAND gate directly onto Gaussian states. When applying homomorphic operations, the new ciphertext maintains the form of an LWE sample with respect to the same public key \mathbf{pk} , albeit for a new LWE secret and a new (non-necessarily Gaussian) noise term of bounded magnitude. Notice, however, that the resulting ciphertext is now a highly entangled state since the unitary operation U_{NAND} induces entanglement between the LWE secrets and Gaussian error terms of the superposition. This raises the following question: How can a server perform homomorphic computations and, if requested, afterwards prove data deletion to a client? In some sense, applying a single homomorphic NAND gates breaks the structure of the Gaussian states in a way that prevents us from obtaining a valid deletion certificate via a Fourier basis measurement. Our solution to the problem involves a single additional round of interaction between the quantum server and the client in order to *certify deletion*.

After performing a Boolean circuit C via a sequence of U_{NAND} gates starting from the ciphertext $|\text{CT}\rangle = |\text{CT}_1\rangle \otimes \dots \otimes |\text{CT}_\ell\rangle$ in system C_{in} corresponding to an encryption of $x = (x_1, \dots, x_\ell) \in \{0, 1\}^\ell$, the server simply sends the quantum system C_{out} containing an encryption of $C(x)$ to the client. Then, using the secret key \mathbf{sk} (i.e., a trapdoor for the public matrix \mathbf{pk}), it is possible for the client to *extract* the outcome $C(x)$ from the system C_{out}

with overwhelming probability without significantly damaging the state. We show that it is possible to rewind the procedure in a way that results in a state which is negligibly close to the original state in system C_{out} . At this step of the protocol, the client has learned the outcome of the homomorphic application of the circuit C while the server is still in possession of a large number of auxiliary systems (denoted by C_{aux}) which mark intermediate applications of the gate U_{NAND} . We remark that this is where the standard FHE protocol ends. In order to enable *certified deletion*, the client must now return the system C_{out} to the server. Having access to all three systems $C_{\text{in}}C_{\text{aux}}C_{\text{out}}$, the server is then able to undo the sequence of homomorphic NAND gates in order to return to the original product state in system C_{in} (up to negligible trace distance). Since the ciphertext in the server's possession is now approximately a simple product of Gaussian states, the server can perform a Fourier basis measurement of systems C_{in} , as required. Once the protocol is complete, it is therefore possible for the client to know $C(x)$ and to be convinced that data deletion has taken place.

5 Gaussian-Collapsing Hash Functions

Unruh [30] introduced the notion of collapsing hash functions in his seminal work on computationally binding quantum commitments. Motivated by the properties of the dual Gaussian state, we consider a special class of hash functions which are *collapsing* with respect to Gaussian superpositions. Informally, we say that a hash function h is *Gaussian-collapsing* if it is computationally difficult to distinguish between a Gaussian superposition of pre-images and a single (measured) Gaussian pre-image (of h). We formalize this below.

► **Definition 4** (Gaussian-collapsing hash function). *Let $\lambda \in \mathbb{N}$ be the security parameter, $m(\lambda), n(\lambda) \in \mathbb{N}$ and let $q(\lambda) \geq 2$ be a modulus. Let $\sigma > 0$. A hash function family $\mathcal{H} = \{H_\lambda\}_{\lambda \in \mathbb{N}}$ with domain $\mathcal{X} = \mathbb{Z}_q^m$ and range $\mathcal{Y} = \mathbb{Z}_q^n$ is called σ -Gaussian-collapsing if, for every QPT adversary \mathcal{A} ,*

$$|\Pr[\text{GaussCollapseExp}_{\mathcal{H}, \mathcal{A}, \lambda}(0) = 1] - \Pr[\text{GaussCollapseExp}_{\mathcal{H}, \mathcal{A}, \lambda}(1) = 1]| \leq \text{negl}(\lambda).$$

Here, the experiment $\text{GaussCollapseExp}_{\mathcal{H}, \mathcal{A}, \lambda}(b)$ is defined as follows:

1. The challenger samples a random hash function $h \xleftarrow{\$} H_\lambda$ and prepares the quantum state

$$|\hat{\psi}\rangle_{XY} = \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle_X \otimes |h(\mathbf{x})\rangle_Y.$$

2. The challenger measures system Y in the computational basis, resulting in the state

$$|\hat{\psi}_{\mathbf{y}}\rangle_{XY} = \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^m: \\ h(\mathbf{x}) = \mathbf{y}}} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle_X \otimes |\mathbf{y}\rangle_Y.$$

3. If $b = 0$, the challenger does nothing. Else, if $b = 1$, the challenger measures system X of the quantum state $|\hat{\psi}_{\mathbf{y}}\rangle$ in the computational basis. Finally, the challenger sends the outcome state in systems X to \mathcal{A} , together with the string $\mathbf{y} \in \mathbb{Z}_q^n$ and a classical description of the hash function h .
4. \mathcal{A} returns a bit b' , which we define as the output of the experiment.

5.1 Ajtai's hash function

We give a simple and direct proof that the Ajtai hash function is Gaussian-collapsing assuming (decisional) LWE, which might be of independent interest.

90:10 Quantum Proofs of Deletion for Learning with Errors

► **Theorem 5.** Let $n \in \mathbb{N}$ and $q \geq 2$ be a prime with $m \geq 2n \log q$, each parameterized by $\lambda \in \mathbb{N}$. Let $\sigma \in (\sqrt{8m}, q/\sqrt{8m})$. Then, the Ajtai hash function family $\mathcal{H} = \{H_\lambda\}_{\lambda \in \mathbb{N}}$ with

$$H_\lambda = \{h_{\mathbf{A}} : \mathbb{Z}_q^m \rightarrow \mathbb{Z}_q^n \text{ s.t. } h_{\mathbf{A}}(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x} \pmod{q}; \mathbf{A} \in \mathbb{Z}_q^{n \times m}\}$$

is σ -Gaussian-collapsing assuming the quantum hardness of the decisional $\text{LWE}_{n,q,\alpha q}^m$ problem, for any noise ratio $\alpha \in (0, 1)$ with relative noise magnitude $1/\alpha = \sigma \cdot 2^{o(n)}$:

Proof. Let \mathcal{A} denote the QPT adversary in the experiment $\text{GaussCollapseExp}_{\mathcal{H},\mathcal{A},\lambda}(b)$ with $b \in \{0, 1\}$. To prove the claim, we give a reduction from the decisional $\text{LWE}_{n,q,\alpha q}^m$ assumption. We are given as input a sample (\mathbf{A}, \mathbf{b}) with $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$, where $\mathbf{b} = \mathbf{s}_0 \cdot \mathbf{A} + \mathbf{e}_0 \pmod{q}$ is either a sample from the LWE distribution with $\mathbf{s}_0 \xleftarrow{\$} \mathbb{Z}_q^n$ and $\mathbf{e}_0 \sim D_{\mathbb{Z}^m, \alpha q}$, or where \mathbf{b} is a uniformly random string $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^m$.

Consider the distinguisher \mathcal{D} that acts as follows on input 1^λ and (\mathbf{A}, \mathbf{b}) :

1. \mathcal{D} prepares a bipartite quantum state on systems X and Y with

$$|\hat{\psi}\rangle_{XY} = \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle_X \otimes |\mathbf{A} \cdot \mathbf{x} \pmod{q}\rangle_Y.$$

2. \mathcal{D} measures system Y in the computational basis, resulting in the state

$$|\hat{\psi}_{\mathbf{y}}\rangle_{XY} = \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^m \\ \mathbf{A}\mathbf{x} = \mathbf{y}}} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle_X \otimes |\mathbf{y}\rangle_Y.$$

3. \mathcal{D} applies the generalized Pauli- \mathbf{Z} operator $\mathbf{Z}_q^{\mathbf{b}}$ on system X , resulting in the state

$$(\mathbf{Z}_q^{\mathbf{b}} \otimes I_Y) |\hat{\psi}_{\mathbf{y}}\rangle_{XY} = \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^m \\ \mathbf{A}\mathbf{x} = \mathbf{y}}} \rho_\sigma(\mathbf{x}) (\mathbf{Z}_q^{\mathbf{b}} |\mathbf{x}\rangle_X) \otimes |\mathbf{y}\rangle_Y.$$

4. \mathcal{D} runs \mathcal{A} on input system X and classical descriptions of $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{y} \in \mathbb{Z}_q^n$.

5. \mathcal{D} outputs whatever bit $b' \in \{0, 1\}$ the adversary \mathcal{A} outputs.

Suppose that, for every $\lambda \in \mathbb{N}$, there exists a polynomial $p(\lambda)$ such that

$$|\Pr[\text{GaussCollapseExp}_{\mathcal{H},\mathcal{A},\lambda}(0) = 1] - \Pr[\text{GaussCollapseExp}_{\mathcal{H},\mathcal{A},\lambda}(1) = 1]| \geq \frac{1}{p(\lambda)}.$$

We now show that this implies that \mathcal{D} succeeds at the decisional $\text{LWE}_{n,q,\alpha q}^m$ experiment with advantage at least $1/p(\lambda) - \text{negl}(\lambda)$. We distinguish between the following two cases.

If (\mathbf{A}, \mathbf{b}) is a sample from the LWE distribution with $\mathbf{b} = \mathbf{s}_0 \cdot \mathbf{A} + \mathbf{e}_0 \pmod{q}$, then the adversary \mathcal{A} receives as input the following quantum state in system X :

$$\mathcal{Z}_{\text{LWE}_{n,q,\alpha q}^m} \left(|\hat{\psi}_{\mathbf{y}}\rangle \langle \hat{\psi}_{\mathbf{y}}|_X \right) = \sum_{\mathbf{s}_0 \in \mathbb{Z}_q^n} \sum_{\mathbf{e}_0 \in \mathbb{Z}^m} q^{-n} D_{\mathbb{Z}^m, \alpha q}(\mathbf{e}_0) \mathbf{Z}_q^{\mathbf{s}_0 \cdot \mathbf{A} + \mathbf{e}_0} |\hat{\psi}_{\mathbf{y}}\rangle \langle \hat{\psi}_{\mathbf{y}}|_X \mathbf{Z}_q^{-(\mathbf{s}_0 \cdot \mathbf{A} + \mathbf{e}_0)}.$$

Due to the invariance of (primal) Gaussian states under shifts from the $\text{LWE}_{n,q,\alpha q}^m$ distribution, it follows that there exists a negligible function $\varepsilon(\lambda)$ such that

$$\mathcal{Z}_{\text{LWE}_{n,q,\alpha q}^m} \left(|\hat{\psi}_{\mathbf{y}}\rangle \langle \hat{\psi}_{\mathbf{y}}|_X \right) \approx_\varepsilon |\hat{\psi}_{\mathbf{y}}\rangle \langle \hat{\psi}_{\mathbf{y}}|_X.$$

In other words, \mathcal{A} receives as input a state in system X which is within negligible trace distance of the dual Gaussian state $|\hat{\psi}_{\mathbf{y}}\rangle$, which corresponds precisely to the input in $\text{GaussCollapseExp}_{\mathcal{H},\mathcal{A},\lambda}(0)$.

If (\mathbf{A}, \mathbf{b}) is a uniformly random sample, where \mathbf{b} is a random string $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^m$, then the adversary \mathcal{A} receives as input the following quantum state in system X :

$$\mathcal{Z} \left(|\hat{\psi}_{\mathbf{y}}\rangle\langle\hat{\psi}_{\mathbf{y}}|_X \right) = q^{-m} \sum_{\mathbf{u} \in \mathbb{Z}_q^m} \mathbf{Z}_q^{\mathbf{u}} |\hat{\psi}_{\mathbf{y}}\rangle\langle\hat{\psi}_{\mathbf{y}}|_X \mathbf{Z}_q^{-\mathbf{u}}.$$

Because \mathcal{Z} corresponds to the uniform Pauli- \mathbf{Z} dephasing channel, it follows that

$$\mathcal{Z} \left(|\hat{\psi}_{\mathbf{y}}\rangle\langle\hat{\psi}_{\mathbf{y}}|_X \right) = \sum_{\mathbf{x} \in \mathbb{Z}_q^m} |\langle \mathbf{x} | \hat{\psi}_{\mathbf{y}} \rangle|^2 |\mathbf{x}\rangle\langle \mathbf{x}|_X.$$

In other words, \mathcal{A} receives as input a mixed state which is the result of a computational basis measurement of the Gaussian state $|\hat{\psi}_{\mathbf{y}}\rangle$. Note that this corresponds precisely to the input in $\text{GaussCollapseExp}_{\mathcal{H}, \mathcal{A}, \lambda}(1)$.

By assumption, the adversary \mathcal{A} succeeds with advantage at least $1/p(\lambda)$. Therefore, the distinguisher \mathcal{D} succeeds at the decisional $\text{LWE}_{n, q, \alpha}^m$ experiment with probability at least $1/p(\lambda) - \text{negl}(\lambda)$. This proves the claim. \blacktriangleleft

5.2 Strong Gaussian-collapsing conjecture

Our quantum encryption schemes with certified deletion rely on the assumption that Ajtai's hash function satisfies a strong Gaussian-collapsing property in the presence of leakage. We formalize the property as the following simple and falsifiable conjecture.

► Conjecture 6 (Strong Gaussian-Collapsing Conjecture).

Let $\lambda \in \mathbb{N}$ be the security parameter, $n(\lambda) \in \mathbb{N}$, $q(\lambda) \geq 2$ be a modulus and $m \geq 2n \log q$ be an integer. Let $\sigma = \Omega(\sqrt{m})$ be a parameter and let $\mathcal{H} = \{H_\lambda\}_{\lambda \in \mathbb{N}}$ be the Ajtai hash function family with

$$H_\lambda = \{h_{\mathbf{A}} : \mathbb{Z}_q^m \rightarrow \mathbb{Z}_q^n \text{ s.t. } h_{\mathbf{A}}(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x} \pmod{q}; \mathbf{A} \in \mathbb{Z}_q^{n \times m}\}.$$

The Strong Gaussian-Collapsing Conjecture ($\text{SGC}_{n, m, q, \sigma}$) states that, for any QPT \mathcal{A} ,

$$|\Pr[\text{StrongGaussCollapseExp}_{\mathcal{H}, \mathcal{A}, \lambda}(0) = 1] - \Pr[\text{StrongGaussCollapseExp}_{\mathcal{H}, \mathcal{A}, \lambda}(1) = 1]| \leq \text{negl}(\lambda).$$

Here, the experiment $\text{StrongGaussCollapseExp}_{\mathcal{H}, \mathcal{A}, \lambda}(b)$ is defined as follows:

1. The challenger samples $\bar{\mathbf{A}} \xleftarrow{\$} \mathbb{Z}_q^{n \times (m-1)}$ and prepares the quantum state

$$|\hat{\psi}\rangle_{XY} = \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle_X \otimes |\mathbf{A} \cdot \mathbf{x} \pmod{q}\rangle_Y,$$

where $\mathbf{A} = [\bar{\mathbf{A}} \mid \bar{\mathbf{A}} \cdot \bar{\mathbf{x}} \pmod{q}] \in \mathbb{Z}_q^{n \times m}$ is a matrix with $\bar{\mathbf{x}} \xleftarrow{\$} \{0, 1\}^{m-1}$.

2. The challenger measures system Y in the computational basis, resulting in the state

$$|\hat{\psi}_{\mathbf{y}}\rangle_{XY} = \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^m: \\ \mathbf{A}\mathbf{x} = \mathbf{y} \pmod{q}}} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle_X \otimes |\mathbf{y}\rangle_Y.$$

3. If $b = 0$, the challenger does nothing. Else, if $b = 1$, the challenger measures system X of the quantum state $|\hat{\psi}_{\mathbf{y}}\rangle$ in the computational basis. Finally, the challenger sends the outcome state in systems X to \mathcal{A} , together with the matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and the string $\mathbf{y} \in \mathbb{Z}_q^n$.
4. \mathcal{A} sends a classical witness $\mathbf{w} \in \mathbb{Z}_q^m$ to the challenger.

5. The challenger checks whether $\mathbf{A} \cdot \mathbf{w} = \mathbf{y} \pmod{q}$ and $\|\mathbf{w}\| \leq \sqrt{m}\sigma/\sqrt{2}$. If \mathbf{w} passes both checks, the challenger sends $\mathbf{t} = (\bar{\mathbf{x}}, -1) \in \mathbb{Z}_q^m$ to \mathcal{A} with $\mathbf{A} \cdot \mathbf{t} = \mathbf{0} \pmod{q}$. Else, the challenger aborts.
6. \mathcal{A} returns a bit b' , which we define as the output of the experiment.

Unfortunately, we currently do not know how to prove the conjecture from standard assumptions, such as LWE or ISIS. The difficulty emerges when we attempt to reduce the security to the LWE (or ISIS) problem with respect to the same matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. In order to simulate the experiment $\text{StrongGaussCollapseExp}_{\mathcal{H}, \mathcal{A}, \lambda}$ with respect to an adversary \mathcal{A} , we have to eventually forward a short trapdoor vector $\mathbf{t} \in \mathbb{Z}^m$ in order to simulate the second phase of the experiment once \mathcal{A} has produced a valid witness. Notice, however, that the reduction has no way of obtaining a short vector \mathbf{t} in the kernel of \mathbf{A} as it is trying to break the underlying LWE (or ISIS) problem with respect to \mathbf{A} in the first place. Therefore, any successful security proof must necessarily exploit the fact that there is *interaction* between the challenger and the adversary \mathcal{A} , and that a short trapdoor vector \mathbf{t} is only revealed *after* \mathcal{A} has already produced a valid short pre-image of $\mathbf{y} \in \mathbb{Z}_q^n$.

When trying to distinguish between the state $|\hat{\psi}_{\mathbf{y}}\rangle$ and a single Gaussian pre-image $|\mathbf{x}_0\rangle$ with the property that $\mathbf{A} \cdot \mathbf{x}_0 = \mathbf{y} \pmod{q}$, it is useful to work with the Fourier basis. Without loss of generality, we can assume that \mathcal{A} instead receives one of the following states during in Step 3; namely

$$\sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \rho_{\frac{q}{\sigma}}(\mathbf{e}) \omega_q^{-\langle \mathbf{s}, \mathbf{y} \rangle} |\mathbf{s}\mathbf{A} + \mathbf{e}\rangle_X \quad \text{or} \quad \sum_{\mathbf{u} \in \mathbb{Z}_q^m} \omega_q^{-\langle \mathbf{u}, \mathbf{x}_0 \rangle} |\mathbf{u}\rangle_X .$$

One natural approach is prepare an auxiliary system, say B , which could later help the adversary determine whether X corresponds to a superposition of LWE samples or a superposition of uniform samples once the trapdoor \mathbf{t} is revealed (ideally, without disturbing X so as to allow for a Fourier basis measurement). Because finding a valid witness \mathbf{w} to the ISIS problem specified by (\mathbf{A}, \mathbf{y}) now amounts to a Fourier basis projection, we give an entropic uncertainty relation which immediately rules out large class of attacks, including the *shift-by-LWE-sample attack* we described earlier. There, the idea is to reversibly shift system X by a fresh LWE sample into an auxiliary system B . If system X corresponds to a superposition of LWE samples, we obtain a separate LWE sample which is *re-randomized*, whereas, if X is a superposition of uniform samples, the outcome remains random. Hence, if the aforementioned procedure succeeded without disturbing system X , we could potentially find a valid witness \mathbf{w} and simultaneously distinguish the auxiliary system B with access to the trapdoor \mathbf{t} . As we observed before, however, such an attack must necessarily entangle the two systems X and B in a way that prevents it from finding a solution to the ISIS problem specified by (\mathbf{A}, \mathbf{y}) . Intuitively, if the state in system X yields a short-pre image \mathbf{w} *with high probability* via a Fourier basis measurement, then system X cannot be entangled with any auxiliary systems. Because the set \mathcal{S} of valid short pre-images (i.e. the set of solution to the ISIS problem specified by \mathbf{A} and \mathbf{y}) is much smaller than the size of \mathbb{Z}_q^m (in particular, if $\sigma\sqrt{m} \ll q$), our uncertainty relation tells us that the min-entropy of system X (once it is measured in the computational basis) given system B must necessarily be large. We remark that this statement holds *information-theoretically*, and does not rely on the hardness of LWE. This suggests that, even if the trapdoor \mathbf{t} is later revealed, system B cannot contain any relevant information about whether system X initially corresponded to a superposition of LWE samples, or to a superposition of uniform samples. While this argument is not sufficient to prove the conjecture, it captures the inherent difficulty in extracting information encoded in two mutually unbiased bases, i.e. the computational basis and the Fourier basis.

References

- 1 Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 99–108. ACM, 1996. doi:10.1145/237814.237838.
- 2 Gorjan Alagic, Stacey Jeffery, Maris Ozols, and Alexander Poremba. On quantum chosen-ciphertext attacks and learning with errors. *Cryptography*, 4(1), 2020. doi:10.3390/cryptography4010010.
- 3 Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit abe, and compact garbled circuits. Cryptology ePrint Archive, Paper 2014/356, 2014. URL: <https://eprint.iacr.org/2014/356>.
- 4 Raphael Bost, Raluca Ada Popa, Stephen Tu, and Shafi Goldwasser. Machine learning classification over encrypted data. *IACR Cryptology ePrint Archive*, 2014:331, 2014. URL: <https://eprint.iacr.org/2014/331>.
- 5 Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. In *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS '11*, pages 97–106, USA, 2011. IEEE Computer Society. doi:10.1109/FOCS.2011.12.
- 6 Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. Cryptology ePrint Archive, Paper 2011/344, 2011. URL: <https://eprint.iacr.org/2011/344>.
- 7 Anne Broadbent and Rabib Islam. Quantum encryption with certified deletion. *Lecture Notes in Computer Science*, pages 92–122, 2020. doi:10.1007/978-3-030-64381-2_4.
- 8 Ran Canetti, Uri Feige, Oded Goldreich, and Moni Naor. Adaptively secure multi-party computation. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96*, pages 639–648, New York, NY, USA, 1996. Association for Computing Machinery. doi:10.1145/237814.238015.
- 9 Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering, 2021. arXiv:2108.11015.
- 10 Xavier Coiteux-Roy and Stefan Wolf. Proving erasure. *2019 IEEE International Symposium on Information Theory (ISIT)*, July 2019. doi:10.1109/isit.2019.8849661.
- 11 Stefan Dziembowski, Tomasz Kazana, and Daniel Wichs. One-time computable self-erasing functions. In *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011*, volume 6597 of *Lecture Notes in Computer Science*, page 125. Springer, 2011. doi:10.1007/978-3-642-19571-6_9.
- 12 Sanjam Garg, Shafi Goldwasser, and Prashant Nalini Vasudevan. Formalizing data deletion in the context of the right to be forgotten. *IACR Cryptol. ePrint Arch.*, page 254, 2020. URL: <https://eprint.iacr.org/2020/254>.
- 13 Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009. URL: crypto.stanford.edu/craig.
- 14 Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. Cryptology ePrint Archive, Report 2007/432, 2007. URL: <https://eprint.iacr.org/2007/432>.
- 15 Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. Cryptology ePrint Archive, Report 2013/340, 2013. URL: <https://ia.cr/2013/340>.
- 16 Alex B. Grilo, Iordanis Kerenidis, and Timo Zijlstra. Learning-with-errors problem is easy with quantum samples. *Physical Review A*, 99(3), March 2019. doi:10.1103/physreva.99.032314.
- 17 Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Certified everlasting zero-knowledge proof for qma, 2021. arXiv:2109.14163.

- 18 Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Quantum encryption with certified deletion, revisited: Public key, attribute-based, and classical communication, 2021. [arXiv:2105.05393](https://arxiv.org/abs/2105.05393).
- 19 Stanisław Jarecki and Anna Lysyanskaya. Adaptively secure threshold cryptography: Introducing concurrency, removing erasures. In *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques, EUROCRYPT'00*, pages 221–242, Berlin, Heidelberg, 2000. Springer-Verlag.
- 20 Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Secure software leasing from standard assumptions, 2021. [arXiv:2010.11186](https://arxiv.org/abs/2010.11186).
- 21 Qipeng Liu and Mark Zhandry. Revisiting post-quantum fiat-shamir. Cryptology ePrint Archive, Paper 2019/262, 2019. URL: <https://eprint.iacr.org/2019/262>.
- 22 Urmila Mahadev. Classical verification of quantum computations, 2018. [arXiv:1804.01082](https://arxiv.org/abs/1804.01082).
- 23 Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007. doi:10.1137/S0097539705447360.
- 24 Jörn Müller-Quade and Dominique Unruh. Long-term security and universal composability. In Salil P. Vadhan, editor, *Theory of Cryptography*, pages 41–60, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.
- 25 Daniele Perito and Gene Tsudik. Secure code update for embedded devices via proofs of secure erasure. Cryptology ePrint Archive, Report 2010/217, 2010. URL: <https://ia.cr/2010/217>.
- 26 Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34:1–34:40, 2005. doi:10.1145/1568318.1568324.
- 27 R L Rivest, L Adleman, and M L Dertouzos. On data banks and privacy homomorphisms. *Foundations of Secure Computation, Academia Press*, pages 169–179, 1978.
- 28 Bhaskar Roberts. Toward secure quantum money. Princeton University Senior Thesis, 2019. URL: <http://arks.princeton.edu/ark:/88435/dsp01nc580q51r>.
- 29 Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. Cryptology ePrint Archive, Paper 2009/285, 2009. URL: <https://eprint.iacr.org/2009/285>.
- 30 Dominique Unruh. Computationally binding quantum commitments. Cryptology ePrint Archive, Paper 2015/361, 2015. URL: <https://eprint.iacr.org/2015/361>.
- 31 W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982. doi:10.1038/299802a0.