Quantum Proofs of Deletion for Learning with Errors

Alexander Poremba∗

California Institute of Technology

August 23, 2022

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.

Our results enable a form of everlasting cryptography and give rise to new privacy-preserving quantum cloud applications, such as private machine learning on encrypted data with certified data deletion.

∗aporemba@caltech.edu
## Contents

1 Introduction ................................................. 3  
   1.1 Main results ........................................... 4  
   1.2 Overview ............................................... 4  
   1.3 Applications .......................................... 11  
   1.4 Related work ........................................... 12  

2 Preliminaries ............................................... 12  
   2.1 Quantum computation .................................... 13  
   2.2 Classical and quantum entropies ....................... 15  
   2.3 Fourier analysis ....................................... 16  
   2.4 Generalized Pauli operators ............................. 17  
   2.5 Lattices and the Gaussian mass ......................... 18  
   2.6 Cryptography .......................................... 21  
   2.7 The Short Integer Solution problem .................... 22  
   2.8 The Learning with Errors problem ...................... 23  

3 Primal and Dual Gaussian States .............................. 23  
   3.1 Transference lemma .................................... 24  
   3.2 Efficient state preparation ............................. 25  
   3.3 Invariance under Pauli-Z dephasing ..................... 26  

4 Uncertainty Relation for Fourier Basis Projections .......... 28  
   4.1 Fourier basis projections ............................... 28  
   4.2 Uncertainty relation .................................... 28  

5 Gaussian-Collapsing Hash Functions .......................... 30  
   5.1 Ajtaj’s hash function ................................... 32  
   5.2 Strong Gaussian-collapsing conjecture .................. 34  

6 Public-Key Encryption with Certified Deletion ................ 36  
   6.1 Definition .............................................. 36  
   6.2 Certified deletion security ................................ 37  

7 Dual-Regev Public-Key Encryption with Certified Deletion .... 37  
   7.1 Construction ............................................. 38  
   7.2 Proof of security ....................................... 39  

8 Fully Homomorphic Encryption with Certified Deletion ....... 43  
   8.1 Definition ............................................... 43  
   8.2 Certified deletion security .............................. 45  

9 Dual-Regev Fully Homomorphic Encryption with Certified Deletion 45  
   9.1 Construction ............................................. 46  
   9.2 Rewinding lemma ....................................... 50  
   9.3 Proof of security ....................................... 54
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 [GGV20]. 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?*

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 impossible to achieve in general, *proofs-of-secure-erasure* [PT10, DKW11] can achieve a limited notion of data deletion under *bounded memory assumptions*. Recently, Garg, Goldwasser and Vasudevan [GGV20] 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. [GGV20] 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 [CRW19, BI20]. Contrary to classical data, it is fundamentally impossible to create copies of an unknown quantum state thanks to the *quantum no-cloning theorem* [WZ82]. Building on the work of Coiteux-Roy and Wolf [CRW19], Broadbent and Islam [BI20] 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 [BI20]. 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 [BI20] 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 [RAD78, Gen09, BV11] 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 [BI20] requires a classical *one-time pad*, whereas the authors in [HMNY21b] 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 [BPTG14], 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* [MQU07, HMNY21a].
1.1 Main results

Our contributions are the following.

**Quantum superpositions of LWE samples.** We use Gaussian states to encode samples from the Learning with Errors (LWE) distribution \([\text{Reg05}]\) 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) short integer solution problem \([\text{Ajt96}]\), 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 \([\text{BI20, HMNY21a}]\). Our technique suggests a generic template for certified deletion protocols which can be applied to many other cryptographic primitives based on LWE.

**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 \([\text{Unr15}]\). 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) pre-image. We prove that the Ajtai collision-resistant hash function \([\text{Ajt96}]\) is Gaussian-collapsing assuming the quantum subexponential hardness of decisional LWE.

**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 \([\text{GPV07}]\). We prove the security of our scheme under the assumption that Ajtai’s hash function satisfies a certain strong Gaussian-collapsing property in the presence of leakage.

**(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 \([\text{Mah18}]\), which is a variant of the FHE scheme by Gentry, Sahai and Waters \([\text{GSW13}]\). 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.

1.2 Overview

How can we certify that sensitive information stored on a remote cloud server has been deleted? Remarkably, quantum information allows us to achieve the notion of certified deletion using the principle of complementarity; in other words, by encoding information in two mutually incompatible bases.

Broadbent and Islam \([\text{BI20}]\) construct a private-key quantum encryption scheme with a rigorous notion of certified deletion using a BB84-type protocol that closely resembles the standard quantum key distribution protocol \([\text{BB84, TL17}]\). There, the ciphertext (without the optional quantum error correction part) consists of random BB84 states \(|x_{i}\rangle = H^{\Theta_{i}} |x_{1}\rangle \otimes \cdots \otimes H^{\Theta_{n}} |x_{n}\rangle\) together with a one-time pad encryption of the form \(f(x_{|\Theta_{i}=0}) \oplus m \oplus u\), where \(u\) is a random string (i.e. a one-time pad key), \(f\) is a two-universal hash function and \(x_{|\Theta_{i}=0}\) is the substring of \(x\) to which no Hadamard gate is applied. The main idea behind the scheme is that the information which is necessary to decrypt is encoded in the computational basis, whereas deletion requires a Hadamard basis measurement. Therefore, if the verification of a deletion certificate is successful, \(x_{|\Theta_{i}=0}\) must have high entropy, and thus \(f(x_{|\Theta_{i}=0})\) is statistically close to uniform (i.e. \(f\) serves
as an extractor). The scheme in [BI20] achieves the notion of certified deletion security: once the ciphertext is successfully deleted, the plaintext $m$ remains hidden even if the private key $(\theta, f, u)$ is later revealed.

Using a standard hybrid encryption scheme, Hiroka, Morimae, Nishimaki and Yamakawa [HMNY21b] extended the scheme in [BI20] to both public-key and attribute-based encryption with certified deletion via the notion of receiver non-committing (RNC) encryption [JL00, CFGN96]. For example, in order to obtain a public-key encryption scheme with certified deletion, one simply outputs a ciphertext of the [BI20] scheme together with a classical (non-committing) public-key encryption of its private key, i.e.

$$\text{CT} \leftarrow \left( |x^\theta\rangle, f(x_{\theta_i=0}) \oplus m \oplus u, \text{RNC.Enc}_{pk}(\theta || f || u) \right).$$

Given access to the RNC secret key $sk$, it is therefore possible to decrypt CT in order to obtain the plaintext $m$. Crucially, the hybrid encryption scheme also inherits the certified deletion property of the [BI20] scheme; namely, once deletion has taken place, $m$ remains hidden even if the RNC secret key $sk$ is later revealed. The security proof in [HMNY21b] relies heavily on the fact that the classical public-key encryption is non-committing, i.e. it comes with the ability to equivocate ciphertexts to encryptions of arbitrary plaintexts. As a complementary result, the authors also gave a public-key encryption scheme with certified deletion which is publicly verifiable assuming the existence of one-shot signatures and extractable witness encryption. This property enables anyone to verify a deletion certificate using a publicly available verification key.

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. In this work, we answer a question raised by Broadbent and Islam [BI20] affirmatively, namely whether it is possible to construct a homomorphic quantum encryption scheme with certified deletion. This cryptographic notion is remarkably powerful as it would allow a quantum cloud server to compute on encrypted data, while simultaneously enabling the server to prove data deletion to a client. So far, however, none of the encryption schemes with certified deletion can enable such a functionality. Worse yet, the hybrid encryption paradigm appears fundamentally insufficient in order to construct homomorphic encryption with certified deletion: once we instantiate the (non-committing) public-key encryption scheme with a (classical) fully homomorphic encryption (FHE) encryption scheme instead, anyone can simply run the following homomorphic evaluation procedure (in superposition) to compute

$$\left( |x^\theta\rangle, f(x_{\theta_i=0}) \oplus m \oplus u, \text{FHE.Enc}_{pk}(\theta || f || u) \right) \xrightarrow{\text{Eval}} \text{FHE.Enc}_{pk}(m).$$

Assuming that the FHE scheme is correct, this step can be performed without disturbing the BB84 state $|x^\theta\rangle$ in the process.\footnote{For example, by relying on the so-called Almost As Good As New Lemma [Aar16].} Notice that the classical ciphertext $\text{FHE.Enc}_{pk}(m)$ is now completely decoupled from everything else. In particular, since the BB84 state $|x^\theta\rangle$ remains intact, it is possible to prove deletion and to simultaneously recover $m$ once the secret key is revealed. Because homomorphic encryption schemes are malleable by design, it seems fundamentally impossible for an encryption scheme to be homomorphic and non-committing at the same time. Therefore, to construct a truly homomorphic encryption scheme with certified deletion, an entirely new approach is necessary. Our techniques deviate from the hybrid encryption paradigm of previous works [BI20, HMNY21a] and allow us to construct the first homomorphic quantum encryption scheme with certified deletion which has the desirable feature of being publicly verifiable.

Quantum superpositions of LWE samples. The Learning with Errors (LWE) problem was introduced by Regev [Reg05] and serves as the primary basis of hardness for post-quantum cryptosystems, mainly due to its tight connection with worst-case approximation problems over Euclidean lattices.
The problem is described as follows. Let \( n, m, q \in \mathbb{N} \) and \( q \geq 2 \) be a prime modulus, and \( \alpha \in (0, 1) \) be a noise ratio parameter. In its decisional formulation, the LWE\(_{n, \alpha q}^m\) problem asks to distinguish between a sample \((A \leftarrow \mathbb{Z}_q^{n \times m}, sA + e \mod q)\) from the LWE distribution and a uniformly random sample \((A \leftarrow \mathbb{Z}_q^{n \times m}, u \leftarrow \mathbb{Z}_q^m)\). Here, \( s \leftarrow \mathbb{Z}_q^n \) is chosen uniformly random and \( e \sim D_{\mathbb{Z}_q^m, \alpha q} \) is an error vector which is sampled according to the discrete Gaussian distribution \( D_{\mathbb{Z}_q^m, \alpha q} \). The latter distribution assigns probability proportional to \( q_r(x) = e^{-|\pi||x|^2/\alpha^2} \) to every lattice point \( x \in \mathbb{Z}_q^m \), for \( r = \alpha q > 0 \).

How can we certify that a (possibly malicious) prover has deleted a sample from the LWE distribution? The main technical insight of our work is that one can encode LWE values which are sampled according to the discrete Gaussian distribution \( D_{\mathbb{Z}_q^m, \alpha q} \) using the Gaussian superposition, for the purpose of certified deletion while simultaneously preserving their full cryptographic functionality.

Throughout this work, we will refer to SIS-based cryptosystems. A standard tail bound shows that the discrete Gaussian \( D_{\mathbb{Z}_q^m, \alpha q} \) is essentially only supported on \( \{x \in \mathbb{Z}_q^m : ||x||_\infty \leq \sigma \sqrt{m}\} \). We choose \( \sigma \ll q / \sqrt{m} \) and consider the domain \( \mathbb{Z}_q^m \cap \left(-\frac{q}{2}, \frac{q}{2}\right]^m \) instead. For simplicity, we also ignore that \( \hat{\psi} \) is not normalized.

Our quantum encryption schemes with certified deletion exploit the fact measurement of \(|\hat{\psi}_Y\rangle\) in the Fourier basis yields a short solution to the ISIS problem specified by \((A, y)\), whereas information which is necessary to decrypt is encoded using LWE samples in the (incompatible) computational basis.
**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 (PKE) scheme introduced by Gentry, Peikert and Vaikuntanathan [GPV07]. Unlike Regev’s original PKE scheme in [Reg05], the Dual-Regev PKE scheme has the property that the ciphertext takes the form of a regular sample from the LWE distribution together with an additive shift \( b \cdot \lfloor \frac{q}{2} \rfloor \) that depends on the plaintext \( b \in \{0, 1\} \). Using Gaussian states, we can encode Dual-Regev ciphertexts for the purpose of certified deletion while simultaneously preserving their cryptographic functionality. The scheme consists of the following efficient algorithms:

- To generate a pair of keys (\( sk, pk \)), sample a random matrix \( A \in \mathbb{Z}_{q}^{n \times (m+1)} \) together with a short trapdoor vector \( t = (\bar{x}, -1) \in \mathbb{Z}^{m+1} \) such that \( A \cdot t = 0 \ (\text{mod } q) \), and let \( pk = A \) and \( sk = t \).
- To encrypt \( b \in \{0, 1\} \) using the public key \( pk = A \), choose a random \( y \in \mathbb{Z}_{q}^{n} \) and output the pair
  \[
  vk \leftarrow (A, y), \quad |CT| \leftarrow \sum_{s \in \mathbb{Z}_{q}^{n}} \sum_{e \in \mathbb{Z}_{q}^{m}} \theta \omega_{q}^{- (s,y)} |sA + e + (0, \ldots, 0, b \cdot \lfloor \frac{q}{2} \rfloor)\rangle,
  \]
  where \( vk \) is a public verification key and \( |CT| \) is the quantum ciphertext.
- To decrypt a ciphertext \( |CT| \) using the secret key \( sk \), measure in the computational basis to obtain an outcome \( c \in \mathbb{Z}_{q}^{m+1} \), and output 0, if \( c^T \cdot sk \in \mathbb{Z}_{q} \) is closer to 0 than to \( \lfloor \frac{q}{2} \rfloor \), and output 1, otherwise.

To delete the ciphertext \( |CT| \), we simply perform measurement in the Fourier basis. In Corollary 1, we show that the Fourier transform of the ciphertext \( |CT| \) results in the quantum state

\[
|\hat{CT}| = \sum_{x \in \mathbb{Z}_{q}^{m+1}: Ax = y \ (\text{mod } q)} \theta \omega_{q}^{(x, 0, \ldots, 0, b \cdot \lfloor \frac{q}{2} \rfloor)} |x\rangle.
\]  

Notice that a Fourier basis measurement of \( |CT| \) 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 \( A \cdot \pi = y \ (\text{mod } q) \). In other words, to verify a deletion certificate we can simply check whether it is a solution to the ISIS problem specified by the verification key \( vk = (A, y) \). Our scheme has the desirable property that verification of a certificate \( \pi \) is public; meaning anyone in possession of \( (A, y) \) can verify that \( |CT| \) has been successfully deleted. Moreover, due to the tight connection between worst-case lattice problems and the average-case ISIS problem [MR07, GPV07], it is computationally difficult to produce a valid deletion certificate from \( (A, y) \) alone.

To formalize security, we use the notion of certified deletion security (i.e. IND-CPA-CD security) [BI20, HMNY21a] which roughly states that, once deletion of the ciphertext is successful, the plaintext remains hidden even if the secret key is later revealed (see Definition 23).

Unfortunately, proving security from standard assumptions, such as LWE (or ISIS), is highly non-trivial. The problem emerges when we attempt to reduce the IND-CPA-CD security of our Dual-Regev public-key encryption scheme with certified deletion to the LWE (or ISIS) problem. In order to simulate the IND-CPA-CD game successfully, we have to eventually forward a short trapdoor vector \( t \in \mathbb{Z}^{m+1} \) (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 \( t \) such that \( A \cdot t = 0 \ (\text{mod } q) \) as it is trying to break the underlying LWE (or ISIS) problem with respect to \( A \) in the first place (!) Recently, Hiroka, Morimae, Nishimaki and Yamakawa [HMNY21a] managed to overcome similar technical difficulties using the notion of receiver non-committing (RNC) encryption [JL00, CFGN96] in the context of hybrid encryption in order to produce
The computational indistinguishability property holds under the (subexponential) quantum hardness of the (decisional) LWE assumption (Definition 15). Here, \( \Lambda^X_q(A) = \{ x \in \mathbb{Z}^m : A \cdot x = y \pmod{q} \} \) denotes a particular coset of the \( q \)-ary lattice \( \Lambda^\perp_q(A) = \{ x \in \mathbb{Z}^m : A \cdot x = 0 \pmod{q} \} \) defined in Section 2.5.

**Gaussian-collapsing hash functions.** Unruh [Unr15] 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. \( \sum_{x : h(x) = y} ^\rho x |x \rangle \), and a single measured pre-image \( |x_0 \rangle \) such that \( h(x_0) = y \). 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 \( \sigma \)-Gaussian-collapsing (formally defined in Definition 19), for some \( \sigma > 0 \), if the following states are computationally indistinguishable:

\[
\sum_{x : h(x) = y} ^\rho x |x \rangle \approx_c |x_0 \rangle, \text{s.t. } h(x_0) = y.
\]

Here, \( x_0 \) is the result of a computational basis measurement of 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 [LZ19] implicitly showed that the Ajtaj hash function \( h_A(x) = A \cdot x \pmod{q} \) is collapsing – and thus Gaussian-collapsing – via the notion of lossy functions by assuming the superpolynomial hardness of (decisional) LWE. In Theorem 4, we give a simple and direct proof that the Ajtaj hash function is Gaussian-collapsing assuming (decisional) LWE, which might be of independent interest.

The fact Ajtaj’s hash function is Gaussian-collapsing has several implications for the security of our Dual-Regev public-key encryption scheme with certified deletion. Because our Dual-Regev ciphertext \( |\text{CT} \rangle \)
corresponds to the Fourier transform of the dual Gaussian state in Eq. (3), the Gaussian-collapsing property immediately implies the semantic (i.e., IND-CPA) security under the hardness of decisional LWE (see Theorem 5). We refer to Figure 1 for an overview of the primal and dual 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 \( t \) in the kernel of \( A \)) is later revealed. In other words, it is sufficient to show that Ajtaj’s hash function satisfies a particular strong Gaussian-collapsing property in the presence of leakage; namely, once a computationally bounded adversary \( \mathcal{A} \) produces a valid short certificate \( \pi \) with the property that \( A \cdot \pi = y \pmod{q} \), 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 \( t \) in the kernel of \( A \). Here, it is crucial that \( \mathcal{A} \) receives the trapdoor vector \( t \) only after \( \mathcal{A} \) provides a valid pre-image witness \( \pi \), otherwise \( \mathcal{A} \) could trivially distinguish the two states by applying the Fourier transform and using the trapdoor \( t \) to check whether the outcome corresponds to a superposition of LWE samples (rather than a uniform superposition). Unfortunately, we currently do not know how to prove the strong Gaussian-collapsing property of the Ajtaj hash function from standard assumptions (such as LWE or ISIS); instead, we choose to formalize it as a simple and falsifiable conjecture in Conjecture 5.2.

To see why Conjecture 5.2 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 sample\(^3\) 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 were to succeed without disturbing the initial quantum state, we could potentially provide a valid certificate \( \pi \) and also distinguish the auxiliary system with access to the trapdoor. However, by shifting the initial state by another LWE sample, we have necessarily entangled the two systems in a way that prevents us from obtaining a valid certificate via the required Fourier basis measurement. We make this fact more precise in Section 4, where we prove a general uncertainty relation for Fourier basis projections (Theorem 3) that rules out a large class of attacks, including the shift-by-LWE-sample attack described above.

We prove the following result in Theorem 7 (assuming that Conjecture 5.2 holds):

**Theorem** (informal): The Dual-Regev PKE scheme with certified deletion (see Construction 1) is IND-CPA-CD-secure under the strong Gaussian-collapsing assumption in Conjecture 5.2.

Next, we extend our Dual-Regev public-key encryption scheme with certified deletion towards a (leveled) FHE scheme of the same type.

**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 [Mah18] – a variant of the scheme due to Gentry, Sahai and Waters [GSW13]. 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 \( G \in \mathbb{Z}_q^{(m+1) \times N} \) denote the gadget matrix (defined in Section 9.1) 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 (sk, pk), sample a random matrix \( A \in \mathbb{Z}_q^{(m+1) \times n} \) together with a short

---

\(^3\)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.
trapdoor vector \( t = (x, -1) \in \mathbb{Z}^{m+1} \) such that \( t \cdot A = 0 \pmod{q} \), and let \( pk = A \) and \( sk = t \).

- To encrypt a bit \( x \in \{0, 1\} \) using the public key \( A \in \mathbb{Z}^{(m+1) \times n}_q \), choose random matrix \( Y \in \mathbb{Z}^{n \times N}_q \) composed of rows \( y_1, \ldots, y_N \in \mathbb{Z}^{n}_q \) and output a public verification key and ciphertext pair

\[
\text{vk} \leftarrow (A, Y), \quad |\text{CT}| \leftarrow \sum_{S \in \mathbb{Z}^{N \times N}_q} \sum_{E \in \mathbb{Z}^{(m+1) \times N}_q} q_{g/s}(E) \omega_q^{-\text{Tr}[S]Y} \langle A \cdot S + E + x \cdot G \rangle,
\]

where \( (g_1, \ldots, g_N) \) are the rows of the gadget matrix \( G \in \mathbb{Z}^{(m+1) \times N}_q \).

- To decrypt a quantum ciphertext \(|\text{CT}|\) using the secret key \( sk \), measure in the computational basis to obtain an outcome \( C \in \mathbb{Z}^{(m+1) \times N}_q \) and compute \( c = sk^T \cdot e_N \in \mathbb{Z}_q \), where \( e_N \in \mathbb{Z}_q^{m+1} \) is the \( N \)-th column of \( C \), 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.

Let us now describe how to perform homomorphic operations on the encrypted data. Our FHE scheme supports the evaluation of polynomial-sized Boolean circuits consisting entirely of NOT-AND (NAND) gates, which are universal for classical computation. Recall that the (classical) Dual-Regev FHE scheme supports the homomorphic evaluation of a NAND gate in the following sense. If \( \text{CT}_0 \) and \( \text{CT}_1 \) are ciphertexts that encrypt two bits \( x_0 \) and \( x_1 \), respectively, then the outcome \( \text{CT} = G - \text{CT}_0 \cdot G^{-1}(\text{CT}_1) \pmod{q} \) is an encryption of NAND\((x_0, x_1) = 1 - x_0 \cdot x_1 \). Moreover, the new ciphertext \( \text{CT} \) maintains the form of an LWE sample with respect to the same public key \( pk \), albeit for a new LWE secret and a new (non-necessarily Gaussian) noise term of bounded magnitude. This property is crucial, as knowledge of the secret key \( sk \) still allows for the decryption of the ciphertext \( \text{CT} \) once a NAND gate has been applied (see Section 9.1).

Inspired by the classical homomorphic NAND operation, we define an analogous quantum operation \( U_{\text{NAND}} \) in Definition 28 which allows us to apply a NAND gate directly onto Gaussian states. Consider two ciphertexts \(|\text{CT}_0\rangle\) and \(|\text{CT}_1\rangle\) in systems \( C_0 \) and \( C_1 \), respectively. Applying the homomorphic NAND gate via the unitary \( U_{\text{NAND}} \) results in an output state \( \text{CT} \) in systems \( C_0 C_1 \) out such that

\[
U_{\text{NAND}} : |\text{CT}_0\rangle_{C_0} \otimes |\text{CT}_1\rangle_{C_1} \otimes |0\rangle_{C_{\text{out}}} \mapsto |\text{CT}\rangle_{C_0 C_1 C_{\text{out}}}. \tag{4}
\]

Just as in the (classical) Dual-Regev FHE scheme, the basis states of the state \(|\text{CT}\rangle\) in system \( C_{\text{out}} \) maintain the form of an LWE sample with a new bounded noise vector. Therefore, in principle, it should be possible to measure the outcome in system \( C_{\text{out}} \) in order to learn the ciphertext that corresponds to an encryption of NAND\((x_0, x_1) = 1 - x_0 \cdot x_1 \). Notice, however, that the new ciphertext \(|\text{CT}\rangle\) is now a highly entangled state since the unitary operation \( U_{\text{NAND}} \) induces entanglement between the LWE secrets and Gaussian error terms of the superposition. This raises the following question: How can a quantum server perform homomorphic computations and, if requested, to 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 makes it impossible to perform the correct Fourier basis measurement required for a proof of deletion.

Our solution to the problem involves a single additional round of interaction between the quantum server (the prover) and the client (the verifier) in order to prove deletion. After performing the Boolean circuit \( C \) via a sequence of \( U_{\text{NAND}} \) gates starting from the ciphertext \(|\text{CT}\rangle = |\text{CT}_1\rangle \otimes \cdots \otimes |\text{CT}_\ell\rangle\) in system \( C_{\text{in}} \) which corresponds to an encryption of \( x = (x_1, \ldots, x_\ell) \in \{0, 1\}^\ell \), the prover simply sends the quantum system \( C_{\text{out}} \) containing an encryption of \( C(x) \) to the verifier. Then, using the secret key \( sk \) (i.e., a trapdoor for the public matrix \( pk \)), it is possible for the verifier to extract the outcome \( C(x) \) from the system \( C_{\text{out}} \).
with overwhelming probability without significantly damaging the state. By the Almost As Good As New Lemma [Aar16] (see Lemma 1), 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 $C_{\text{out}}$. At this step of the protocol, the verifier has learned the outcome of the homomorphic application of the circuit $C$ while the prover is still in possession of a large number of auxiliary systems (denoted by $C_{\text{aux}}$) which mark intermediate applications of the gate $U_{\text{NAND}}$. In order to allow for a quantum proof of deletion, the verifier must now return the system $C_{\text{out}}$ to the prover. Having access to all three systems $C_{\text{in}}C_{\text{aux}}C_{\text{out}}$, the prover is then able to undo the sequence of homomorphic NAND gates in order to return to the original product state in system $C_{\text{in}}$ (up to negligible trace distance). Since the ciphertext in the prover’s possession is now approximately a simple product of Gaussian states, the prover can perform a Fourier basis measurement of systems $C_{\text{in}}$, 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.

In terms of security, our FHE scheme with certified deletion inherits the same security guarantees as our Dual-Regev PKE scheme with certified deletion. We prove the following in Theorem 10.

**Theorem** (informal): Our Dual-Regev (leveled) FHE scheme with certified deletion (Construction 3) is IND-CPA-CD-secure under the strong Gaussian-collapsing assumption in Conjecture 5.2.

**Open problems.** Our results leave open many interesting future research directions. For example, is it possible to prove Conjecture 5.2 – and thus the IND-CPA-CD security of our constructions – from the hardness of LWE or ISIS? Another interesting direction is the following. Since the verification of our proofs of deletion only requires classical computational capabilities, this leaves open the striking possibility that all communication that is required for fully homomorphic encryption with certified deletion can be dequantized entirely, similar to work of Mahadev [Mah18] on delegating quantum computations, as well as recent work on classically-instructed parallel remote state preparation by Gheorghiu, Metger and Poremba [GMP22].

**1.3 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 [GGV20] – 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 remains safeguarded even in the case of 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 [BPTG14], 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 [Reg05] into a temporary one, and thus effectively achieve a form of everlasting security [MQU07, HMNY21a].
1.4 Related work

The first work to formalize a notion resembling certified deletion is due to Unruh [Unr13] who proposed a quantum timed-release encryption scheme that is revocable. The protocol allows a user to return the ciphertext of a quantum timed-release encryption scheme, thereby losing all access to the data. Unruh’s security proof exploits the monogamy of entanglement in order to guarantee that the quantum revocation process necessarily erases all information about the plaintext. Subsequently, Coladangelo, Majenz and Poremba [CMP20] adapted this property to revocable programs in the context of secure software leasing, a weaker notion of quantum copy-protection which was proposed by Ananth and La Placa [AP20].

Fu and Miller [FM18] gave the first quantum protocol that proves deletion of a single bit using classical interaction alone. Subsequently, Coiteux-Roy and Wolf [CRW19] proposed a QKD-like conjugate coding protocol that enables certified deletion of a classical plaintext, albeit without a complete security proof. Coiteux-Roy and Wolf also coined the term privacy delegation as the means to delegate information to a remote quantum server in a way that prevents the leakage of user data. By design, privacy delegation cannot make eavesdropping impossible – it merely makes it possible for a verifier to be convinced that deletion has taken place. Broadbent and Islam [BI20] construct a quantum encryption scheme with certified deletion whose security proof is similar to that of QKD protocol [BB84, TL17]. The notion of certified deletion proposed by Broadbent and Islam is information-theoretic and does not take computational assumptions into account. Subsequently, Hiroka, Morimae, Nishimaki and Yamakawa [HMNY21b] extended the scheme in [BI20] to public-key and attribute-based encryption by using a hybrid encryption scheme in combination with receiver non-committing (RNC) encryption [JL00, CFGN96]. Hiroka, Morimae, Nishimaki and Yamakawa [HMNY21a] studied certified everlasting zero-knowledge proofs for QMA via the notion of everlasting security which was first formalized by Müller-Quade and Unruh [MQU07]. A recent paper by Coladangelo, Liu, Liu and Zhandry [CLLZ21] introduces subspace coset states in the context of unclonable cryptography in a way that loosely resembles our use of primal and dual Gaussian states.

Acknowledgments. The author would like to thank Urmila Mahadev for pointing out an attack on an earlier version of our protocols, and for the idea behind the proof of Theorem 4. The author would also like to thank Thomas Vidick and Vinod Vaikuntanathan for many insightful discussions. The author is also grateful for many useful comments and suggestions made by anonymous reviewers. The author is 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), and is also grateful for the hospitality of the Simons Institute for the Theory of Computing, where part of this research was carried out.

2 Preliminaries

Notation. For $x \in \mathbb{C}^n$, we denote the $\ell^2$ norm by $\|x\|_2$. For $x \in \mathbb{Z}^n$, we occasionally also use the max norm $\|x\|_{\infty} = \max_i |x_i|$. We denote the expectation value of a random variable $X$ which takes values in $\mathcal{X}$ by $\mathbb{E}[X] = \sum_{x \in \mathcal{X}} x \Pr[X = x]$. The notation $x \overset{\$}{\leftarrow} \mathcal{X}$ denotes sampling of $x$ uniformly at random from $\mathcal{X}$, whereas $x \sim D$ denotes sampling of an element $x$ according to the distribution $D$. We call a non-negative real-valued function $\mu : \mathbb{N} \to \mathbb{R}^+$ negligible if $\mu(n) = o(1/p(n))$, for every polynomial $p(n)$. Given an integer $m \in \mathbb{N}$ and modulus $q \geq 2$, we represent elements in $\mathbb{Z}_q^m$ as integers $\mathbb{Z}_q^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$. 

12
2.1 Quantum computation

For a comprehensive overview of quantum computation, we refer to the introductory texts [NC11, Wil13]. We denote a finite-dimensional complex Hilbert space by \( \mathcal{H} \), and we use subscripts to distinguish between different systems (or registers). For example, we let \( \mathcal{H}_A \) be the Hilbert space corresponding to a system \( A \). The tensor product of two Hilbert spaces \( \mathcal{H}_A \) and \( \mathcal{H}_B \) is another Hilbert space denoted by \( \mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B \). The Euclidean norm of a vector \( \| \psi \| = \sqrt{\langle \psi | \psi \rangle} \). Let \( L(\mathcal{H}) \) denote the set of linear operators over \( \mathcal{H} \). A quantum system over the 2-dimensional Hilbert space \( \mathcal{H} = \mathbb{C}^2 \) is called a qubit. For \( n \in \mathbb{N} \), we refer to quantum registers over the Hilbert space \( \mathcal{H} = (\mathbb{C}^2)^\otimes n \) as \( n \)-qubit states. More generally, we associate qudits of dimension \( d \geq 2 \) with a \( d \)-dimensional Hilbert space \( \mathcal{H} = \mathbb{C}^d \). We use the word quantum state to refer to both pure states (unit vectors \( |\psi\rangle \in \mathcal{H} \)) and density matrices \( \varrho \in \mathcal{D}(\mathcal{H}) \), where we use the notation \( \mathcal{D}(\mathcal{H}) \) to refer to the space of positive semidefinite matrices of unit trace acting on \( \mathcal{H} \). For simplicity, we frequently consider subnormalized states, i.e. states in the space of positive semidefinite operators over \( \mathcal{H} \) with trace norm not exceeding 1, denoted by \( \mathcal{S}_{\leq 1}(\mathcal{H}) \). The trace distance of two density matrices \( \varrho, \sigma \in \mathcal{D}(\mathcal{H}) \) is given by

\[
\| \varrho - \sigma \|_{tr} = \frac{1}{2} \text{Tr} \left[ \sqrt{(\varrho - \sigma)^\dagger (\varrho - \sigma)} \right].
\]

We frequently use the compact notation \( \varrho \approx \sigma \) which means that there exists some \( \varepsilon \in [0, 1] \) such that \( \| \varrho - \sigma \|_{tr} \leq \varepsilon \). The purified distance is defined as \( P(\varrho, \sigma) = \sqrt{1 - F(\varrho, \sigma)^2} \), where \( F(\varrho, \sigma) = \| \sqrt{\varrho} \sqrt{\sigma} \|_1 \) denotes the fidelity. The trace distance and the \( \ell^2 \) distance over \((\mathbb{C}^d)^\otimes m\) are related via the inequality,

\[
\| |\psi\rangle \langle \psi| - |\phi\rangle \langle \phi| \|_{tr} \leq \| |\psi\rangle - |\phi\rangle \|_2, \quad \forall |\psi\rangle, |\phi\rangle \in (\mathbb{C}^d)^\otimes m.
\]

A classical-quantum (CQ) state \( \varrho \in \mathcal{D}(\mathcal{H}_{XB}) \) depends on a classical variable in system \( X \) which is correlated with a quantum system \( B \). If the classical system \( X \) is distributed according to a probability distribution \( P_X \) over the set \( \mathcal{X} \), then all possible joint states \( \varrho_{XB} \) can be expressed as

\[
\varrho_{XB} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle \langle x| \otimes \varrho^x_B.
\]

Quantum channels and measurements. A quantum channel \( \Phi : L(\mathcal{H}_A) \to L(\mathcal{H}_B) \) is a linear map between linear operators over the Hilbert spaces \( \mathcal{H}_A \) and \( \mathcal{H}_B \). Oftentimes, we use the compact notation \( \Phi_{A \to B} \) to denote a quantum channel between \( L(\mathcal{H}_A) \) and \( L(\mathcal{H}_B) \). We say that a channel \( \Phi \) is completely positive if, for a reference system \( R \) of arbitrary size, the induced map \( \mathbb{1}_R \otimes \Phi \) is positive, and we call it trace-preserving if \( \text{Tr}[\Phi(X)] = \text{Tr}[X] \), for all \( X \in L(\mathcal{H}) \). A quantum channel that is both completely positive and trace-preserving is called a quantum CPTP channel. Let \( \mathcal{X} \) be a set. A generalized measurement on a system \( A \) is a set of linear operators \( \{ M^x_A \}_{x \in \mathcal{X}} \) such that

\[
\sum_{x \in \mathcal{X}} (M^x_A)^\dagger (M^x_A) = \mathbb{1}_A.
\]

We can represent a measurement as a CPTP map \( \mathcal{M}_{A \to \mathcal{X}} \) that maps states on system \( A \) to measurement outcomes in a register denoted by \( \mathcal{X} \). For example, let \( \varrho \in \mathcal{D}(\mathcal{H}_{AB}) \) be a bipartite state. Then,

\[
\mathcal{M}_{A \to \mathcal{X}} : \varrho_{AB} \mapsto \sum_{x \in \mathcal{X}} |x\rangle \langle x| \otimes \text{tr}_A \left[ M^x_A \varrho_{AB} M^x_A \right]^\dagger,
\]
yields a normalized classical-quantum state. A positive-operator valued measure (POVM) on a quantum system \( A \) is a set of Hermitian positive semidefinite operators \( \{M^x_A\}_{x \in \mathcal{X}} \) such that
\[
\sum_{x \in \mathcal{X}} M^x_A = 1_A.
\]

Oftentimes, we identify a POVM \( \{M^x_A\}_{x \in \mathcal{X}} \) with an associated generalized measurement \( \{\sqrt{M^x_A}\}_{x \in \mathcal{X}} \). The overlap \( c \) of two POVMs \( \{M^x_A\}_{x \in \mathcal{X}} \) and \( \{N^y_A\}_{y \in \mathcal{X}} \) acting on a quantum system \( A \) is defined by
\[
c = \max_{x, y} \left\| \sqrt{M^x_A} \sqrt{N^y_A} \right\|_\infty^2.
\]
We say that two measurements are mutually unbiased, if the overlap satisfies \( c = 1/d \), where \( d = \dim(\mathcal{H}_A) \) is the dimension of the associated Hilbert space.

**Quantum algorithms.** By a polynomial-time quantum algorithm (or QPT algorithm) we mean a polynomial-time uniform family of quantum circuits given by \( C = \bigcup_{n \in \mathbb{N}} C_n \), where each circuit \( C \in C \) is described by a sequence of unitary gates and measurements. Similarly, we also define (classical) probabilistic polynomial-time (PPT) algorithms. A quantum algorithm may, in general, receive (mixed) quantum states as inputs and produce (mixed) quantum states as outputs. Occasionally, we restrict QPT algorithms implicitly. For example, if we write \( \Pr[A(1^A) = 1] \) for a QPT algorithm \( A \), it is implicit that \( A \) is a QPT algorithm that outputs a single classical bit.

We extend the notion of QPT algorithms to CPTP channels via the following definition.

**Definition 1** (Efficient CPTP maps). A family of CPTP maps \( \{\Phi_\lambda : L(\mathcal{H}_{A_\lambda}) \to L(\mathcal{H}_{B_\lambda})\}_{\lambda \in \mathbb{N}} \) is called efficient, if there exists a polynomial-time uniformly generated family of circuits \( \{C_\lambda\}_{\lambda \in \mathbb{N}} \) acting on the Hilbert space \( \mathcal{H}_{A_\lambda} \otimes \mathcal{H}_{B_\lambda} \otimes \mathcal{H}_{C_\lambda} \) such that, for all \( \lambda \in \mathbb{N} \) and for all \( \varrho \in \mathcal{H}_{A_\lambda} \),
\[
\Phi_\lambda(\varrho_\lambda) = \text{Tr}_{A_\lambda C_\lambda}[C_\lambda(\varrho_\lambda \otimes |0\rangle\langle0|_{B_\lambda C_\lambda})].
\]

**Definition 2** (Indistinguishability of ensembles of random variables). Let \( \lambda \in \mathbb{N} \) be a parameter. We say that two ensembles of random variables \( X = \{X_\lambda\} \) and \( Y = \{Y_\lambda\} \) are computationally indistinguishable, denoted by \( X \approx_c Y \), if, for all QPT distinguishers \( D \) which output a single bit, it holds that
\[
|\Pr[D(1^X, X_\lambda) = 1] - \Pr[D(1^Y, Y_\lambda) = 1]| \leq \text{negl}(\lambda).
\]

**Definition 3** (Indistinguishability of ensembles of quantum states, [Wat06]). Let \( p : \mathbb{N} \to \mathbb{N} \) be a polynomially bounded function, and let \( \varrho_\lambda \) and \( \sigma_\lambda \) be \( p(\lambda) \)-qubit quantum states. We say that \( \{\varrho_\lambda\}_{\lambda \in \mathbb{N}} \) and \( \{\sigma_\lambda\}_{\lambda \in \mathbb{N}} \) are quantum computationally indistinguishable ensembles of quantum states, denoted by \( \varrho_\lambda \approx_c \sigma_\lambda \), if, for any QPT distinguisher \( D \) with single-bit output, any polynomially bounded \( q : \mathbb{N} \to \mathbb{N} \), any family of \( q(\lambda) \)-qubit auxiliary states \( \{v_\lambda\}_{\lambda \in \mathbb{N}} \), and every \( \lambda \in \mathbb{N} \),
\[
|\Pr[D(1^X, \varrho_\lambda \otimes v_\lambda) = 1] - \Pr[D(1^X, \sigma_\lambda \otimes v_\lambda) = 1]| \leq \text{negl}(\lambda).
\]

**Lemma 1** ("Almost As Good As New" Lemma, [Aar16]). Let \( \varrho \in \mathcal{D}(\mathcal{H}) \) be a density matrix over a Hilbert space \( \mathcal{H} \). Let \( U \) be an arbitrary unitary and let \( \{\Pi_0, \Pi_1 = 1 - \Pi_0\} \) be projectors acting on \( \mathcal{H} \otimes \mathcal{H}_{\text{aux}} \). We interpret \( (U, \Pi_0, \Pi_1) \) as a measurement performed by appending an ancillary system in the state \( |0\rangle\langle0|_{\text{aux}} \), applying the unitary \( U \) and subsequently performing the two-outcome measurement \( \{\Pi_0, \Pi_1\} \) on the larger
system. Suppose that the outcome corresponding to $\Pi_0$ occurs with probability $1 - \varepsilon$, for some $\varepsilon \in [0, 1]$. In other words, it holds that $\text{Tr}[\Pi_0 (U_0 \otimes |0\rangle \langle 0|_{\text{aux}} U_t^\dagger)] = 1 - \varepsilon$. Then,

$$\|\tilde{\varrho} - \varrho\|_{\text{tr}} \leq \sqrt{\varepsilon},$$

where $\tilde{\varrho}$ is the state after performing the measurement and applying $U_t^\dagger$, and after tracing out $H_{\text{aux}}$:

$$\tilde{\varrho} = \text{Tr}_{\text{aux}} \left[ U_t^\dagger (\Pi_0 U (\varrho \otimes |0\rangle \langle 0|_{\text{aux}}) U_t \Pi_0 + \Pi_1 U (\varrho \otimes |0\rangle \langle 0|_{\text{aux}}) U_t^\dagger \Pi_1) U_t \right].$$

We also use the following lemma on the closeness to ideal states:

**Lemma 2** ([Unr13], Lemma 10). Let $\Pi$ be an arbitrary projector and let $|\psi\rangle$ be a normalized pure state such that $\|\Pi |\psi\rangle\|^2 = 1 - \varepsilon$, for some $\varepsilon \geq 0$. Then, there exists a (pure) ideal state $|\bar{\psi}\rangle = \Pi |\psi\rangle / \|\Pi |\psi\rangle\|$, with the property that $\| |\psi\rangle \langle \psi| - |\bar{\psi}\rangle \langle \bar{\psi}| \|_{\text{tr}} \leq \sqrt{\varepsilon}$ and $|\bar{\psi}\rangle \in \text{im}(\Pi)$. In other words, the state $|\bar{\psi}\rangle$ is within trace distance $\varepsilon > 0$ of the state $|\psi\rangle$ and lies in the image of $\Pi$.

We also use the following elementary lemma.

**Lemma 3** ([CMP20], Lemma 23). Let $\varrho, \sigma \in D(H)$ be two states with the property that $\|\varrho - \sigma\|_{\text{tr}} \leq \varepsilon$, for some $\varepsilon \geq 0$. Let $\Pi$ be an arbitrary matrix acting on $H$ such that $0 \leq \Pi \leq 1$. Then,

$$|\text{Tr}[\Pi \varrho] - \text{Tr}[\Pi \sigma]| \leq \varepsilon.$$

### 2.2 Classical and quantum entropies

**Classical entropies.** Let $X$ be a random variable with an arbitrary distribution $P_X$ over an alphabet $\mathcal{X}$. The *min-entropy* of $X$, denoted by $H_{\text{min}}(X)$, is defined by the following quantity

$$H_{\text{min}}(X) = -\log \left( \max_{x \in \mathcal{X}} \text{Pr}_{X \sim P_X} [X = x] \right).$$

The *conditional min-entropy* of $X$ conditioned on a correlated random variable $Y$ is defined by

$$H_{\text{min}}(X|Y) = -\log \left( \mathbb{E}_{y \sim Y} \left[ \max_{x \in \mathcal{X}} \text{Pr}_{X \sim P_Y} [X = x|Y = y] \right] \right).$$

**Lemma 4** (Leftover Hash Lemma, [HILL88]). Let $n, m \in \mathbb{N}$ and $q \geq 2$ a prime. Let $P$ be a distribution over $\mathbb{Z}_q^m$ and suppose that $H_{\text{min}}(X) \geq n \log q + 2 \log(1/\varepsilon) + O(1)$ for $\varepsilon > 0$, where $X$ denotes a random variable with distribution $P$. Then, the following two distributions are within total variance distance $\varepsilon$:

$$(A, A \cdot x \pmod{q}) \approx_{\varepsilon} (A, u) : A \overset{\$}{\leftarrow} \mathbb{Z}_q^{n \times m}, u \overset{\$}{\leftarrow} \mathbb{Z}_q^n.$$
Quantum entropies.

**Definition 4** (Quantum min-entropy). Let $A$ and $B$ be two quantum systems and let $\varrho_{AB} \in S_{\leq}(\mathcal{H}_{AB})$ be any bipartite state. The min-entropy of $A$ conditioned on $B$ of the state $\varrho_{AB}$ is defined as

$$H_{\text{min}}(A \mid B)_{\varrho} = \max_{\sigma_B} \sup \left\{ \lambda \in \mathbb{R} : \varrho_{AB} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B \right\}.$$  

**Definition 5** (Smooth quantum min-entropy). Let $A$ and $B$ be quantum systems and let $\varrho_{AB} \in S_{\leq}(\mathcal{H}_{AB})$. Let $\varepsilon \geq 0$. We define the $\varepsilon$-smooth quantum min-entropy of $A$ conditioned on $B$ of $\varrho_{AB}$ as

$$H_{\varepsilon \text{min}}(A \mid B) = \sup_{\tilde{\varrho}_{AB}, \varrho_{AB}} \Pr[\tilde{\varrho}_{AB} \leq \varepsilon] \cdot \text{Tr} \left[ M_B^* \varrho_B M_B^{\dagger} \right].$$

The conditional min-entropy of a CQ state $\varrho_{XB}$ captures the difficulty of guessing the content of a classical register $X$ given quantum side information $B$. This motivates the following definition.

**Definition 6** (Guessing probability). Let $\varrho_{XB} \in D(\mathcal{H}_X \otimes \mathcal{H}_B)$ be a CQ state, where $X$ is a classical register over an alphabet $\mathcal{X}$ and $B$ is a quantum system. Then, the guessing probability of $X$ given $B$ is defined as

$$p_{\text{guess}}(X \mid B)_{\varrho} = \sup_{M_X} \sum_{x \in \mathcal{X}} \Pr[X = x]_{\varrho} \cdot \text{Tr} \left[ M_B^* \varrho_B M_B^{\dagger} \right].$$

The following operational meaning of min-entropy is due to Koenig, Renner and Schaffner [KRS09].

**Theorem 1** ([KRS09], Theorem 1). Let $\varrho_{XB} \in D(\mathcal{H}_X \otimes \mathcal{H}_B)$ be a CQ state, where $X$ is a classical register over an alphabet $\mathcal{X}$ and $B$ is a quantum system. Then, it holds that

$$H_{\text{min}}(X \mid B)_{\varrho} = - \log \left( p_{\text{guess}}(X \mid B)_{\varrho} \right).$$

### 2.3 Fourier analysis

Let $q \geq 2$ be an integer modulus and let $m \in \mathbb{N}$. The $q$-ary (discrete) Fourier transform takes as input a function $f : \mathbb{Z}_m \rightarrow \mathbb{C}$ and produces a function $\hat{f} : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ (the Fourier transform of $f$) defined by

$$\hat{f}(y) = \sum_{x \in \mathbb{Z}_m} f(x) \cdot e^{2\pi i (y,x) / q}.$$

For brevity, we oftentimes write $\omega_q = e^{2\pi i / q} \in \mathbb{C}$ to denote the primitive $q$-th root of unity. The $m$-qudit $q$-ary quantum Fourier transform over the ring $\mathbb{Z}_q^m$ is defined by the operation,

$$\text{FT}_q : \left| \mathbf{x} \rightangle \mapsto \sqrt{q^{-m}} \sum_{y \in \mathbb{Z}_q^m} e^{2\pi i (\mathbf{y}, \mathbf{x}) / q} \left| \mathbf{y} \rightangle, \quad \forall \mathbf{x} \in \mathbb{Z}_q^m.$$  

It is well known that the $q$-ary quantum Fourier transform can be efficiently performed on a quantum computer for any modulus $q \geq 2$ [HH00]. Note the quantum Fourier transform of a normalized quantum state

$$\left| \Psi \rightangle = \sum_{x \in \mathbb{Z}_m} f(x) \left| x \rightangle \quad \text{with} \quad \sum_{x \in \mathbb{Z}_m} |f(x)|^2 = 1,$$
for a function $f : \mathbb{Z}^m \to \mathbb{C}$, results in the state (the Fourier transform of $|\Psi\rangle$) given by

$$\text{FT}_q |\Psi\rangle = \sqrt{q^{-m}} \sum_{y \in \mathbb{Z}^m_q} \left( \sum_{x \in \mathbb{Z}^m} f(x) \cdot e^{\frac{2\pi i}{q} y x} \right) |y\rangle \equiv \sqrt{q^{-m}} \sum_{y \in \mathbb{Z}^m_q} f(y) |y\rangle.$$ 

Notice that the Fourier transform of $|\Psi\rangle$ is unitary if $\text{supp}(f) \subseteq \mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2})^m$. We frequently make use of the following standard identity for Fourier characters.

**Lemma 5** (Orthogonality of Fourier characters). Let $q \geq 2$ be any integer modulus and let $\omega_q = e^{\frac{2\pi i}{q}} \in \mathbb{C}$ denote the primitive $q$-th root of unity. Then, for arbitrary $x, y \in \mathbb{Z}_q$:

$$\sum_{x \in \mathbb{Z}_q} \omega_{q,x}^{x y} \omega_{q,y} = q \delta_{x,y}.$$ 

### 2.4 Generalized Pauli operators

**Definition 7** (Generalized Pauli operators). Let $q \geq 2$ be an integer modulus and $\omega_q = e^{\frac{2\pi i}{q}}$ be the primitive $q$-th root of unity. The generalized $q$-ary Pauli operators $\{X^b_q\}_{b \in \mathbb{Z}_q}$ and $\{Z^b_q\}_{b \in \mathbb{Z}_q}$ are given by

$$X^b_q = \sum_{a \in \mathbb{Z}_q} |a + b \text{ (mod } q)\rangle \langle a|,$$

$$Z^b_q = \sum_{a \in \mathbb{Z}_q} \omega_{q,a}^{a b} |a\rangle \langle a|.$$ 

For $b = (b_1, \ldots, b_m) \in \mathbb{Z}_q^m$, we use the notation $X^b_q = X^{b_1}_q \otimes \cdots \otimes X^{b_m}_q$ and $Z^b_q = Z^{b_1}_q \otimes \cdots \otimes Z^{b_m}_q$.

**Lemma 6.** Let $q \geq 2$ be an integer modulus. Then, for all $b \in \mathbb{Z}_q$, it holds that

$$Z^b_q = \text{FT}_q X^b_q \text{FT}_q^*$$

$$X^b_q = \text{FT}_q^* Z^b_q \text{FT}_q.$$ 

**Proof.** It suffices to show the first identity only as the second identity follows by conjugation with $\text{FT}_q$. Using the orthogonality of Fourier characters over $\mathbb{Z}_q$ (Lemma 5), we find that

$$Z^b_q = \sum_{x \in \mathbb{Z}_q} \omega_{q,x}^{x b} |x\rangle \langle x|$$

$$= \sum_{x, y' \in \mathbb{Z}_q} \omega_{q,x}^{x b} \left( \frac{1}{q} \sum_{a \in \mathbb{Z}_q} \omega_{q,a}^{a x} \omega_{q,-a y'} \right) |x\rangle \langle y'|$$

$$= \frac{1}{q} \sum_{x, y' \in \mathbb{Z}_q} \sum_{a \in \mathbb{Z}_q} \omega_{q,x}^{x y'} \omega_{q,-y'} \langle y|a + b \text{ (mod } q)\rangle \cdot \langle a|x'\rangle |x\rangle \langle y'|$$

$$= \frac{1}{q} \left( \sum_{x, y' \in \mathbb{Z}_q} \omega_{q,x}^{x y'} |x\rangle \langle y| \right) \sum_{a \in \mathbb{Z}_q} |a + b \text{ (mod } q)\rangle \langle a| \left( \sum_{x', y' \in \mathbb{Z}_q} \omega_{q,-y'} \langle x'| \langle y'| \right)$$

$$= \text{FT}_q X^b_q \text{FT}_q^*.$$ 

\[\square\]
**Definition 8** (Pauli-Z dephasing channel). Let \( q \geq 2 \) be an integer modulus and let \( m \in \mathbb{N} \). Let \( p \) be a probability distribution over \( Z^m_q \). Then, the Pauli-Z dephasing channel with respect to \( p \) is defined as

\[
Z_p(\varrho) = \sum_{z \in Z^m_q} p_z Z_q^z \varrho Z_q^{-z}, \quad \forall \varrho \in L((\mathbb{C}^q)^\otimes m).
\]

We use \( Z \) to denote the uniform Pauli-Z channel for which \( p \) is the uniform distribution over \( Z^m_q \).

The following lemma shows that the uniform Pauli-Z channel on input \( \varrho \) returns a diagonal state which consists of diagonal elements of \( \varrho \) encoded in the standard basis.

**Lemma 7.** Let \( q \geq 2 \) be a modulus and \( m \in \mathbb{N} \). Then, the uniform Pauli-Z dephasing channel satisfies,

\[
Z(\varrho) = q^{-m} \sum_{z \in Z^m_q} Z_q^z \varrho Z_q^{-z} = \sum_{x \in Z^m_q} \text{Tr}[|x\rangle\langle x| |\varrho|] |x\rangle\langle x|, \quad \forall \varrho \in L((\mathbb{C}^q)^\otimes m).
\]

**Proof.** Suppose that the state \( \varrho \) has the following form in the standard basis,

\[
\varrho = \sum_{x,y \in Z^m_q} \alpha_{xy} |x\rangle \langle y| \in L((\mathbb{C}^q)^\otimes m).
\]

Using the orthogonality of Fourier characters over \( Z_q \) (Lemma 5), we obtain

\[
Z(\varrho) = q^{-m} \sum_{z \in Z^m_q} Z_q^z \varrho Z_q^{-z} \\
= q^{-m} \sum_{z \in Z^m_q} \sum_{x,y \in Z^m_q} \alpha_{xy} Z_q^z |x\rangle \langle y| Z_q^{-z} \\
= \sum_{x,y \in Z^m_q} \alpha_{xy} \left( q^{-m} \sum_{z \in Z^m_q} \omega_q^{|x|} \omega_{q}^{-|y|} \right) |x\rangle \langle y| \\
= \sum_{x \in Z^m_q} \alpha_{xx} |x\rangle \langle x| \\
= \sum_{x \in Z^m_q} \text{Tr}[|x\rangle \langle x| \varrho] |x\rangle \langle x|.
\]

\[\Box\]

### 2.5 Lattices and the Gaussian mass

A **lattice** \( \Lambda \subset \mathbb{R}^m \) is a discrete subgroup of \( \mathbb{R}^m \). To avoid handling matters of precision, we will only consider integer lattices \( \Lambda \subset \mathbb{Z}^m \) throughout this work. The **dual** of a lattice \( \Lambda \subset \mathbb{R}^m \), denoted by \( \Lambda^* \), is the lattice of all vectors \( y \in \mathbb{R}^m \) that satisfy \( \langle y, x \rangle \in \mathbb{Z} \), for all vectors \( x \in \Lambda \). In other words, we define

\[
\Lambda^* = \{ y \in \mathbb{R}^m : \langle y, x \rangle \in \mathbb{Z}, \text{ for all } x \in \Lambda \}.
\]

Given a lattice \( \Lambda \subset \mathbb{R}^m \) and a vector \( t \in \mathbb{R}^m \), we define the coset with respect to \( t \) as the lattice shift \( \Lambda - t = \{ x \in \mathbb{R}^m : x + t \in \Lambda \} \). Note that many different shifts \( t \) can define the same coset.

The **Gaussian measure** \( \varrho_\sigma \) with parameter \( \sigma > 0 \) is defined as the function

\[
\varrho_\sigma(x) = \exp(-\pi \|x\|^2 / \sigma^2), \quad \forall x \in \mathbb{R}^m.
\]
Let $\Lambda \subseteq \mathbb{R}^m$ be a lattice and let $t \in \mathbb{R}^m$ be a shift. We define the Gaussian mass of $\Lambda - t$ as the quantity

$$q_v(\Lambda - t) = \sum_{y \in \Lambda} q_v(y - t).$$

The discrete Gaussian distribution $D_{\Lambda - t,c}$ is the distribution over the lattice $\Lambda - t$ that assigns probability proportional to $e^{-\pi||x-t||^2/c^2}$ to every lattice point $x \in \Lambda$. In other words, we have

$$D_{\Lambda - t,c}(x) = \frac{q_v(x - t)}{q_v(\Lambda - t)}, \quad \forall x \in \Lambda.$$

We make use of the following tail bound for the Gaussian mass of a lattice [Ban93, Lemma 1.5 (ii)].

**Lemma 8.** For any $m$-dimensional lattice $\Lambda$ and shift $t \in \Lambda$ and for all $r > 0$, $c \geq (2\pi)^{-\frac{1}{2}}$ it holds that

$$q_v((\Lambda - t) \setminus B^m(0, c \sqrt{mr})) \leq (2\pi e c^2)^{m} r e^{-\pi c^2 r} q_v(\Lambda),$$

where $B^m(0, s) = \{x \in \mathbb{R}^m : ||x||_2 \leq s\}$ denotes the $m$-dimensional ball of radius $s > 0$.

**q-ary lattices.** In this work, we mainly consider q-ary lattices $\Lambda$ that that satisfy $q\mathbb{Z}^m \subseteq \Lambda \subseteq \mathbb{Z}^m$, for some integer modulus $q \geq 2$. Specifically, we consider lattices generated by a matrix $A \in \mathbb{Z}^{n \times m}_q$ for some $n, m \in \mathbb{N}$. The first lattice consists of all vectors which are perpendicular to the rows of $A$, namely

$$\Lambda_q^\perp(A) = \{x \in \mathbb{Z}^m : A \cdot x = 0 \mod q\}.$$

Note that $\Lambda_q^\perp(A)$ contains $q\mathbb{Z}^m$; in particular, it contains the identity $0 \in \mathbb{Z}^m$. For any syndrome $y \in \mathbb{Z}^n_q$ in the column span of $A$, we also consider the lattice coset $\Lambda_q^y(A)$ given by

$$\Lambda_q^y(A) = \{x \in \mathbb{Z}^m : A \cdot x = y \mod q\} = \Lambda_q^\perp(A) + \bar{x},$$

where $\bar{x} \in \mathbb{Z}^m$ is an arbitrary integer solution to the equation $A\bar{x} = y \mod q$.

The second lattice is the lattice generated by $A^T$ and is defined by

$$\Lambda_q(A) = \{y \in \mathbb{Z}^m : y = A^T \cdot s \mod q\}, \text{ for some } s \in \mathbb{Z}^n.$$

The $q$-ary lattices $\Lambda_q(A)$ and $\Lambda_q^\perp(A)$ are dual to each other (up to scaling). Specifically, we have

$$q \cdot \Lambda_q^\perp(A)^* = \Lambda_q(A) \quad \text{and} \quad q \cdot \Lambda_q(A)^* = \Lambda_q^\perp(A).$$

We use the following facts due to Gentry, Peikert and Vaikuntanathan [GPV07].

**Lemma 9 ([GPV07], Lemma 5.1).** Let $n \in \mathbb{N}$ and let $q \geq 2$ be a prime modulus with $m \geq 2n \log q$. Then, for all but a $q^{-n}$ fraction of $A \in \mathbb{Z}^{n \times m}_q$, the subset-sums of the columns of $A$ generate $\mathbb{Z}^n_q$. In other words, a uniformly random matrix $A \subseteq \mathbb{Z}^{n \times m}_q$ is full-rank with overwhelming probability.

**Lemma 10 ([GPV07], Corollary 5.4).** Let $n \in \mathbb{N}$ and $q \geq 2$ be a prime with $m \geq 2n \log q$. Then, for all but a $2q^{-n}$ fraction of $A \in \mathbb{Z}^{n \times m}_q$ and $\sigma = \omega(\sqrt{\log m})$, the distribution of the syndrome $A \cdot e = u \mod q$ is within negligible total variation distance of the uniform distribution over $\mathbb{Z}^n_q$, where $e \sim D_{m,\sigma}$.

The following lemma is a consequence of [MR04, Lemma 4.4] and [GPV07, Lemma 5.3].
Lemma 11. Let \( n \in \mathbb{N} \) and let \( q \geq 2 \) be a prime modulus with \( m \geq 2n \log q \). Let \( A \in \mathbb{Z}_q^{n \times m} \) be a matrix whose columns generate \( \mathbb{Z}_q^n \). Then, for any \( \sigma = \omega(\sqrt{\log m}) \) and for any syndrome \( y \in \mathbb{Z}_q^n \),

\[
\Pr_{x \sim D_{\Lambda_q}(A, \sigma)} \left[ \|x\| \geq \sqrt{mq} \right] \leq \text{negl}(n).
\]

Definition 9 (Periodic Gaussian). Let \( m \in \mathbb{N} \), let \( q \geq 2 \) be a modulus and let \( \sigma > 0 \). The \( q \)-periodic Gaussian \( \varrho_{q, \sigma} \) function is the periodic continuation of the Gaussian measure \( \varrho_\sigma \), where

\[
\varrho_{q, \sigma}(x) = \varrho_\sigma(x + q\mathbb{Z}^m), \quad \forall x \in \mathbb{R}^m.
\]

For any function \( f : \mathbb{Z}^m \to \mathbb{C} \) and lattice \( \Lambda \subseteq \mathbb{Z}^m \), the well-known Poisson summation formula states that \( f(\Lambda) = \det(\Lambda^*) \tilde{f}(\Lambda^*) \). We use the following Gaussian variant of the formula [Bra18, Corollary 2.14].

Lemma 12 (Poisson summation formula). Let \( q \geq 2 \) be a prime modulus and let \( A \in \mathbb{Z}_q^{n \times m} \) be any matrix whose columns generate \( \mathbb{Z}_q^n \). Let \( v, w \in \mathbb{Z}_q^m \) and \( \sigma > 0 \) be arbitrary. Then, it holds that

\[
\sum_{x \in \Lambda_q(A)} \varrho_\sigma(x) \cdot e^{-\frac{2\pi i}{q} (w, x)} = \frac{\sigma^m}{q^m} \cdot \sum_{y \in \mathbb{Z}_q^m} \varrho_{q, \sigma}(w + yA) \cdot e^{\frac{2\pi i}{q} (y, v)}.
\]

For \( x \in \mathbb{Z}^m \), let \( [x]_q \) denote the unique representative \( \bar{x} \in \mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2})^m \) such that \( x \equiv \bar{x} \pmod{q} \). The following lemma due to Brakerski [Bra18] says that, whenever \( \sigma \) is much smaller than the modulus \( q \), the periodic Gaussian \( \varrho_{q, \sigma} \) is close to the non-periodic (but truncated) Gaussian.

Lemma 13 ([Bra18], Lemma 2.6). Let \( q \geq 2 \), \( x \in \mathbb{Z}^m \) such that \( \|x\| < q/4 \) and \( \sigma > 0 \). Then,

\[
1 \leq \frac{\varrho_{q, \sigma}(x)}{\varrho_\sigma([x]_q)} \leq 1 + 2^{-\left(\frac{1}{2}(q/\sigma)^2 - m\right)}.
\]

A simple consequence of the tail bound in Lemma 8 is that the discrete Gaussian \( D_{\mathbb{Z}^m, \sigma} \) distribution is essentially only supported on the finite set \( \{ x \in \mathbb{Z}^m : \|x\|_\infty \leq \sigma \sqrt{m} \} \), which suggests the use of truncation. Given a modulus \( q \geq 2 \) and \( \sigma > 0 \), we define the truncated discrete Gaussian distribution \( D_{\mathbb{Z}^m_q, \sigma} \) over the finite set \( \mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2})^m \) with support \( \{ x \in \mathbb{Z}^m_q : \|x\|_\infty \leq \sigma \sqrt{m} \} \) as the density

\[
D_{\mathbb{Z}^m_q, \sigma}(x) = \sum_{y \in \mathbb{Z}^m_q, \|y\|_\infty \leq \sigma \sqrt{m}} \frac{\varrho_\sigma(x)}{\varrho_\sigma([y]_q)}.
\]

We define the analogous periodic discrete Gaussian distribution \( D_{\mathbb{Z}^m_q, \sigma, A} \) as

\[
D_{\mathbb{Z}^m_q, \sigma, A}(x) = \sum_{y \in \mathbb{Z}^m_q, \|y\|_\infty \leq \sigma \sqrt{m}} \frac{\varrho_{q, \sigma}(x)}{\varrho_{q, \sigma}([y]_q)}.
\]

Lemma 14. Let \( m \in \mathbb{N} \), \( q \geq 2 \) a modulus and let \( \sigma \in (0, q/\sqrt{8m}) \). Consider the quantum states,

\[
|\psi\rangle = \sum_{x \in \mathbb{Z}_q^n} \sqrt{D_{\mathbb{Z}_q^n, \sigma}(x)} \ket{x} \quad \text{and} \quad |\phi\rangle = \sum_{x \in \mathbb{Z}_q^n} \sqrt{D_{\mathbb{Z}_q^n, \sigma, A}(x)} \ket{x}.
\]

Then, it holds that

\[
\|\langle \psi | \psi \rangle - \langle \phi | \phi \rangle\|_{\text{tr}} \leq \sqrt{1 - \left(1 + 2^{-\left(\frac{1}{2}(q/\sigma)^2 - m\right)}\right)^{-1}}.
\]
To this end, we define two normalization factors

\[ Z_{\sigma} = \sum_{y \in Z_q^m, \|y\|_\infty \leq \sqrt{m}\sigma} \varphi(y) \quad \text{and} \quad Z_{\sigma,\eta} = \sum_{y \in Z_q^m, \|y\|_\infty \leq \sqrt{m}\sigma} \varphi_{\sigma,\eta}(y). \]  

From Lemma 13, it follows for any \( x \in Z_q^m \cap (-\frac{q}{2} \leq x \leq \frac{q}{2})^m \) with \( \|x\| < q/4 \) that

\[ \varphi_{\sigma,\eta}(x) \cdot \left(1 + 2^{-\left(\frac{1}{2}(q/\sigma)^2-m\right)}\right)^{-1} \leq \varphi_\sigma(x) \cdot \varphi_{\sigma,\eta}(x). \]  

Recall also that the truncated discrete Gaussian is supported on the finite set

\[ \text{supp}(D_{Z_q^m}) = \{ x \in Z_q^m : \|x\|_\infty \leq \sqrt{m}\sigma \} \].

Plugging in Eq. (7), we can bound the Hellinger distance as follows:

\[
H^2(D_{Z_q^m}, D_{Z_q^m}) = 1 - \sum_{x \in Z_q^m} \sqrt{D_{Z_q^m}(x) \cdot D_{Z_q^m}(x)} \\
= 1 - \sqrt{Z_{\sigma}^{-1} \cdot Z_{\sigma,\eta}^{-1}} \sum_{x \in Z_q^m, \|x\|_\infty \leq \sqrt{m}\sigma} \sqrt{\varphi_{\sigma}(x) \cdot \varphi_{\sigma,\eta}(x)} \\
\leq 1 - \sqrt{\frac{Z_{\sigma}^{-1} \cdot Z_{\sigma,\eta}^{-1}}{1 + 2^{-\left(\frac{1}{2}(q/\sigma)^2-m\right)}}} \sum_{x \in Z_q^m, \|x\|_\infty \leq \sqrt{m}\sigma} \varphi_{\sigma,\eta}(x) \\
\leq 1 - \left(1 + 2^{-\left(\frac{1}{2}(q/\sigma)^2-m\right)}\right)^{-1/2}.
\]

Therefore, it holds that

\[
\|\psi\rangle\langle\psi| - |\psi\rangle\langle\psi|\|_{\text{tr}} \leq \sqrt{1 - \left(1 - H^2(D_{Z_q^m}, D_{Z_q^m})\right)^2} \\
\leq \sqrt{1 - \left(1 + 2^{-\left(\frac{1}{2}(q/\sigma)^2-m\right)}\right)^{-1}}.
\]

The following result allows us to bound the total variation distance between a truncated discrete Gaussian \( D_{Z_q^m} \) and its perturbation by a fixed vector \( e_0 \in Z^m \).

**Lemma 15** ([BCM+21], Lemma 2.4). Let \( q \geq 2 \) be a modulus, \( m \in \mathbb{N} \) and \( \sigma > 0 \). Then, for any \( e_0 \in Z^m \),

\[
\|D_{Z_q^m} - (D_{Z_q^m} + e_0)\|_{\text{TV}} \leq 2 \cdot \left(1 - e^{-2\sigma \sqrt{\|e_0\|^2}}\right). \]

### 2.6 Cryptography

In this section, we review several definitions in cryptography.
Public-key encryption.

**Definition 10** (Public-key encryption). A public-key encryption (PKE) scheme $\Sigma = (\text{KeyGen}, \text{Enc}, \text{Dec})$ with plaintext space $\mathcal{M}$ is a triple of PPT algorithms consisting of a key generation algorithm KeyGen, an encryption algorithm Enc, and a decryption algorithm Dec.

- **KeyGen**$(1^\lambda) \rightarrow (pk, sk)$: takes as input the parameter $1^\lambda$ and outputs a public key $pk$ and secret key $sk$.
- **Enc**$(pk, m) \rightarrow CT$: takes as input the public key $pk$ and a plaintext $m \in \mathcal{M}$, and outputs a ciphertext $CT$.
- **Dec**$(sk, CT) \rightarrow m$ or $\perp$: takes as input the secret key $sk$ and ciphertext $CT$, and outputs $m'$ or $\perp$.

**Definition 11** (Correctness of PKE). For any $\lambda \in \mathbb{N}$, and for any $m \in \mathcal{M}$:

$$\Pr \left[ \text{Dec}(sk, CT) \neq m \right| \text{KeyGen}(1^\lambda) \right) \leq \text{negl}(\lambda).$$

**Definition 12** (IND-CPA security). Let $\Sigma = (\text{KeyGen}, \text{Enc}, \text{Dec})$ be a PKE scheme and let $A$ be a QPT adversary. We define the security experiment $\text{Exp}_{\Sigma,A,\lambda}^{\text{ind-cpa}}(b)$ between $A$ and a challenger as follows:

1. The challenger generates a pair $(pk, sk) \leftarrow \text{KeyGen}(1^\lambda)$, and sends $pk$ to $A$.
2. $A$ sends a plaintext pair $(m_0, m_1) \in \mathcal{M} \times \mathcal{M}$ to the challenger.
3. The challenger computes $CT_b \leftarrow \text{Enc}(pk, m_b)$, and sends $CT_b$ to $A$.
4. $A$ outputs a bit $b' \in \{0, 1\}$, which is also the output of the experiment.

We say that the scheme $\Sigma$ is IND-CPA-secure if, for any QPT adversary $A$, it holds that

$$\text{Adv}_{\Sigma,A}(\lambda) := |\Pr[\text{Exp}_{\Sigma,A,\lambda}^{\text{ind-cpa}}(0) = 1] - \Pr[\text{Exp}_{\Sigma,A,\lambda}^{\text{ind-cpa}}(1) = 1]| \leq \text{negl}(\lambda).$$

### 2.7 The Short Integer Solution problem

The (inhomogenous) SIS problem was introduced by Ajtai [Ajt96] in his seminal work on average-case lattice problems. The problem is defined as follows.

**Definition 13** (Inhomogenous SIS problem, [Ajt96]). Let $n, m \in \mathbb{N}$ be integers, let $q \geq 2$ be a modulus and let $\beta > 0$ be a parameter. The Inhomogenous Short Integer Solution problem (ISIS) problem is to find a short solution $x \in \mathbb{Z}^m$ with $\|x\|_2 \leq \beta$ such that $Ax \equiv y \pmod q$ given as input a tuple $(A \leftarrow \mathbb{Z}_q^{n \times m}, y \leftarrow \mathbb{Z}_q^n)$. The Short Integer Solution (SIS) problem is a homogenous variant of ISIS with input $(A \leftarrow \mathbb{Z}_q^{n \times m}, 0 \in \mathbb{Z}_q^n)$.

Micciancio and Regev [MR07] showed that the average-case SIS problem is as hard as approximating worst-case lattice problems to within small factors. Gentry, Peikert and Vaikuntanathan [GPV07] subsequently gave an improved reduction showing that, for any $m = \text{poly}(n)$, $\beta = \text{poly}(n)$, and prime $q \geq \beta \cdot \omega(\sqrt{n \log q})$, the average-case problems $\text{SIS}_{n,m,\beta}$ and $\text{ISIS}_{n,m,\beta}$ are as hard as approximating the shortest independent vector problem (SIVP) problem in the worst case to within a factor $\gamma = \beta \cdot \tilde{O}(\sqrt{n})$. 

22
2.8 The Learning with Errors problem

The Learning with Errors problem was introduced by Regev [Reg05] and serves as the primary basis of hardnness of post-quantum cryptosystems. The problem is defined as follows.

**Definition 14** (“Search” LWE, [Reg05]). Let \( n, m \in \mathbb{N} \) be integers, let \( q \geq 2 \) be a modulus and let \( \alpha \in (0, 1) \) be a parameter. The Learning with Errors (LWE) problem is to find a secret vector \( \mathbf{s} \) given as input a sample \((\mathbf{A}, \mathbf{sA} + \mathbf{e} \pmod{q})\) from the distribution \( \text{LWE}_{n, q, \alpha q}^m \) where \( \mathbf{A} \leftarrow \mathbb{Z}_{q}^{n \times m} \) and \( \mathbf{s} \leftarrow \mathbb{Z}_q^n \) are uniformly random, and where \( \mathbf{e} \sim D_{\mathbb{Z}_q^{m, \alpha q}} \) is sampled from the discrete Gaussian distribution.

**Definition 15** (“Decisional” LWE, [Reg05]). Let \( n, m \in \mathbb{N} \) be integers, let \( q \geq 2 \) be a modulus and let \( \alpha \in (0, 1) \) be a parameter. The “decision” Learning with Errors (DLWE) problem is to distinguish between

\[
(\mathbf{A} \leftarrow \mathbb{Z}_{q}^{n \times m}, \mathbf{sA} + \mathbf{e} \pmod{q}) \quad \text{and} \quad (\mathbf{A} \leftarrow \mathbb{Z}_{q}^{n \times m}, \mathbf{u} \leftarrow \mathbb{Z}_q^n),
\]

where \( \mathbf{s} \leftarrow \mathbb{Z}_q^n \) is uniformly random and where \( \mathbf{e} \sim D_{\mathbb{Z}_q^{n, \alpha q}} \) is a discrete Gaussian noise vector.

As shown in [Reg05], the \( \text{LWE}_{n, q, \alpha q}^m \) problem with parameter \( \alpha q \geq 2\sqrt{n} \) is at least as hard as approximating the shortest independent vector problem (SIVP) to within a factor of \( \gamma = \tilde{O}(n / \alpha) \) in worst case lattices of dimension \( n \). In this work we assume the subexponential hardness of \( \text{LWE}_{n, q, \alpha q}^m \) which relies on the worst case hardness of approximating short vector problems in lattices to within a subexponential factor.

3 Primal and Dual Gaussian States

Our Dual-Regev-type encryption schemes with certified deletion in Section 7 and Section 9 rely on two types of Gaussian superpositions, which we call primal and dual Gaussian states. The former (i.e., primal) state corresponds to a quantum superposition of LWE samples with respect to a matrix \( \mathbf{A} \in \mathbb{Z}_{q}^{n \times m} \), and (up to a phase) can be thought of as a superposition of Gaussian balls around random lattice vectors in \( \Lambda_q(\mathbf{A}) \). The latter (i.e., dual) state corresponds to a Gaussian superposition over a particular coset,

\[
\Lambda_q^\perp(\mathbf{A}) = \{ \mathbf{x} \in \mathbb{Z}^m : \mathbf{A} \cdot \mathbf{x} = \mathbf{y} \pmod{q} \},
\]

of the \( q \)-ary lattice \( \Lambda_q^\perp(\mathbf{A}) = \{ \mathbf{x} \in \mathbb{Z}^m : \mathbf{A} \cdot \mathbf{x} = \mathbf{0} \pmod{q} \} \) defined in Section 2.5.

Our terminology regarding which state is primal and which state is dual is completely arbitrary. In fact, the \( q \)-ary lattices \( \Lambda_q(\mathbf{A}) \) and \( \Lambda_q^\perp(\mathbf{A}) \) are both dual to each other (up to scaling), and satisfy

\[
q \cdot \Lambda_q^\perp(\mathbf{A})^* = \Lambda_q(\mathbf{A}) \quad \text{and} \quad q \cdot \Lambda_q(\mathbf{A})^* = \Lambda_q^\perp(\mathbf{A}).
\]

We choose to refer to the quantum superposition of LWE samples as the primal Gaussian state because it corresponds directly to the ciphertexts of our encryption scheme, whereas the dual Fourier mode is only used in order to prove deletion. Gaussian superpositions first appeared in Regev’s quantum reduction from worst-case lattice problems to LWE, and have also been used by Stehlé et al. [SSTX09] who gave a quantum reduction from SIS to LWE. Roberts [Rob19] and Kitagawa et al. [KNY21] used similar (dual) Gaussian states to construct quantum money and secure software leasing schemes. Various other forms of superpositions of LWE samples have been considered by Grilo, Kerenidis and Zijlstra [GKZ19] in the context of quantum learning theory and by Alagic, Jeffery, Ozols and Poremba [AJOP20], as well as by Chen, Liu and Zhandry [CLZ21], in the context of quantum cryptanalysis of LWE-based cryptosystems.

We define primal and dual Gaussian states as follows.
Definition 16 (Gaussian states). Let \( m \in \mathbb{N} \), \( q \geq 2 \) be an integer modulus and \( \sigma > 0 \). Then,

- (primal Gaussian state:) for all \( A \in \mathbb{Z}_q^{n \times m} \) and \( y \in \mathbb{Z}_q^m \), we let
  \[
  |\psi_{A,y}\rangle = \sum_{s \in \mathbb{Z}_q^n} \sum_{e \in \mathbb{Z}_q^m} \frac{\rho_q}{\sigma} (e) \left( s_y^{(s,y)} \right) |sA + e \ (\text{mod } q)\rangle ;
  \]

- (dual Gaussian state:) for all \( A \in \mathbb{Z}_q^{n \times m} \) and \( y \in \mathbb{Z}_q^m \), we let
  \[
  |\hat{\psi}_{A,y}\rangle = \sum_{x \in \mathbb{Z}_q^m \atop Ax = y \ (\text{mod } q)} \rho_\sigma (x) |x\rangle .
  \]

For simplicity, we oftentimes drop the subscript on \( A \) and write \( |\psi_y\rangle \) and \( |\hat{\psi}_y\rangle \), respectively.

3.1 Transference lemma

The following lemma states that, up to negligible trace distance, the primal and dual Gaussian states in Definition 16 are related via the \( q \)-ary quantum Fourier transform.

Lemma 16 (Transference lemma). Let \( m \in \mathbb{N} \), \( q \geq 2 \) be a prime modulus and let \( \sigma \in (\sqrt{8m}, q / \sqrt{8m}) \). Let \( A \in \mathbb{Z}_q^{n \times m} \) be a matrix whose columns generate \( \mathbb{Z}_q^n \) and let \( y \in \mathbb{Z}_q^m \) be arbitrary. Then, up to negligible trace distance, the primal and dual Gaussian states are related via the quantum Fourier transform:

\[
\text{FT}_q |\psi_y\rangle \approx \varepsilon |\hat{\psi}_y\rangle = \sum_{x \in \mathbb{Z}_q^m \atop Ax = y \ (\text{mod } q)} \rho_\sigma (x) |x\rangle ;
\]

\[
\text{FT}_q^\dagger |\hat{\psi}_y\rangle \approx \varepsilon \sum_{s \in \mathbb{Z}_q^n} \sum_{e \in \mathbb{Z}_q^m} \frac{\rho_q}{\sigma} (e) \left( s_y^{(s,y)} \right) |sA + e \ (\text{mod } q)\rangle ,
\]

where \( \varepsilon : \mathbb{N} \rightarrow \mathbb{R}^+ \) is a negligible function in the parameter \( m \in \mathbb{N} \).

Proof. Let \( y \in \mathbb{Z}_q^m \) be an arbitrary vector and recall that the dual Gaussian coset \( |\hat{\psi}_y\rangle \) is given by

\[
|\hat{\psi}_y\rangle = \sum_{x \in \mathbb{Z}_q^m \atop Ax = y \ (\text{mod } q)} \rho_\sigma (x) |x\rangle . \tag{8}
\]

We denote by \( \Lambda_y^\dagger (A) = \{ x \in \mathbb{Z}_q^m : Ax = y \ (\text{mod } q) \} \) be the associated coset of the lattice \( \Lambda_y^\dagger (A) \). Consider now the Gaussian superposition over the entire lattice coset \( \Lambda_y^\dagger (A) \) formally defined by

\[
|\hat{\psi}_y\rangle = \sum_{x \in \Lambda_y^\dagger (A)} \rho_\sigma (x) |x\rangle . \tag{9}
\]

Since \( \sigma < q / \sqrt{8m} \), it follows from the tail bound in Lemma 11 that the state in (8) is within negligible trace distance of the state in Eq. (9). Applying the (inverse) quantum Fourier transform, we get

\[
|\psi_y\rangle \overset{\text{def}}{=} \text{FT}_q^\dagger |\hat{\psi}_y\rangle = \sum_{z \in \mathbb{Z}_q^m} \left( \sum_{x \in \Lambda_y^\dagger (A)} \rho_\sigma (x) \cdot \omega_q^{-(x,z)} \right) |z\rangle . \tag{10}
\]

24
Because $\sigma > \sqrt{8m}$ it follows from Lemma 14 that there exists
\[
\kappa(m) = \sqrt{1 - (1 + 2^{-3m})^{-1}} \geq 0
\]
such that
\[
|\psi_y\rangle \approx_{\kappa} \sum_{s \in \mathbb{Z}_q^n \ e \in \mathbb{Z}_m^n} \psi_{q/s}(\sigma) \cdot \omega_{q}^{(s,y)} |sA + e \mod q\rangle.
\] (12)

Putting everything together, it follows from the triangle inequality that
\[
\text{FT}_q \hat{\psi}_y \approx \epsilon_{\kappa} \sum_{s \in \mathbb{Z}_q^n \ e \in \mathbb{Z}_m^n} \psi_{q/s}(\sigma) \cdot \omega_{q}^{(s,y)} |sA + e \rangle,
\]
where $\epsilon(m) = \text{negl}(m) + \kappa(m)$. Using that $\sqrt{1 - 1/(1 + x)} \leq \sqrt{x}$ for all $x > 0$, we have
\[
\epsilon(m) = \text{negl}(m) + \sqrt{1 - (1 + 2^{-3m})^{-1}} \\
\leq \text{negl}(m) + 2^{-3m/2}.
\]
Thus, we have that $\epsilon(m) \leq \text{negl}(m)$. This proves the claim.

Corollary 1. Let $m \in \mathbb{N}$, $q \geq 2$ be a prime and $\sigma \in (\sqrt{8m}, q/\sqrt{8m})$. Let $A \in \mathbb{Z}_q^{m \times m}$ be a matrix whose columns generate $\mathbb{Z}_q^n$ and let $y \in \mathbb{Z}_q^n$ be arbitrary. Then, there exists a negligible function $\epsilon(m)$ such that
\[
\text{FT}_q X_q^y |\psi_y\rangle \approx \epsilon \times \mathbb{Z}_q^n |\hat{\psi}_y\rangle, \quad \forall v \in \mathbb{Z}_q^n.
\]

Proof. From Lemma 6 it follows that $\text{FT}_q X_q^y = Z_q^y \text{FT}_q$, for all $v \in \mathbb{Z}_q^n$. Moreover, Lemma 16 implies that $\text{FT}_q |\psi_y\rangle$ is within negligible trace distance of $|\hat{\psi}_y\rangle$. This proves the claim.

3.2 Efficient state preparation

In this section, we give two algorithms that prepare the primal and dual Gaussian states from Definition 16. We remark that Gaussian superpositions over $\mathbb{Z}_q^m$ with parameter $\sigma = \Omega(\sqrt{m})$ can be efficiently implemented using standard quantum state preparation techniques, for example using rejection sampling and the Grover-Rudolph algorithm. We refer to [GR02, Reg05, Bra18, BCM+21] for a reference.

Our first algorithm (see Algorithm 1 in Figure 2) prepares the dual Gaussian state from Definition 16 with respect to an input matrix $A \in \mathbb{Z}_q^{n \times m}$ and parameter $\sigma = \Omega(\sqrt{m})$, and is defined as follows.

Our second algorithm (see Algorithm 2 in Figure 3) prepares the primal Gaussian state with respect to an input matrix $A \in \mathbb{Z}_q^{n \times m}$ and parameter $\sigma = \Omega(\sqrt{m})$. Here, in order for Lemma 16 to apply, it is crucial that the columns of $A$ generate $\mathbb{Z}_q^n$. Fortunately, it follows from Lemma 9 that a uniformly random matrix $A \sim \mathbb{Z}_q^{n \times m}$ satisfies this property with overwhelming probability.
Algorithm 1: GenDual(A, σ)

**Input:** Matrix $A \in \mathbb{Z}_q^{n \times m}$ and parameter $\sigma = \Omega(\sqrt{m})$.

**Output:** Gaussian state $|\hat{\psi}_y\rangle$ and $y \in \mathbb{Z}_q^n$.

1. Prepare a Gaussian superposition in system $X$ with parameter $\sigma > 0$:

   $$|\hat{\psi}\rangle_{XY} = \sum_{x \in \mathbb{Z}_q^m} \rho_{\sigma}(x) |x\rangle_X \otimes |0\rangle_Y.$$

2. Apply the unitary $U_A : |x\rangle |0\rangle \rightarrow |x\rangle |A \cdot x \pmod{q}\rangle$ on systems $X$ and $Y$:

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

3. Measures system $Y$ in the computational basis, resulting in the state

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

4. Output the state $|\hat{\psi}_y\rangle$ in system $X$ and the outcome $y \in \mathbb{Z}_q^n$ in system $Y$.

Figure 2: Quantum algorithm which takes as input a matrix $A \in \mathbb{Z}_q^{n \times m}$ and a width parameter $\sigma = \Omega(\sqrt{m})$, and outputs the dual Gaussian state in Definition 16.

### 3.3 Invariance under Pauli-Z dephasing

In this section, we prove a surprising property about the dual Gaussian state from Definition 16. We prove Theorem 2, which says that the Pauli-Z dephasing channel with respect to the LWE distribution leaves the dual Gaussian state approximately invariant.

**Theorem 2.** Let $n, m \in \mathbb{N}$ be integers and let $q \geq 2$ be a prime modulus, each parameterized by the security parameter $\lambda \in \mathbb{N}$. Let $\sigma \in (\sqrt{8m}, q / \sqrt{8m})$ be a function of $\lambda$. Let $y \in \mathbb{Z}_q^n$ be any vector and $A \in \mathbb{Z}_q^{n \times m}$ be any matrix whose columns generate $\mathbb{Z}_q^n$, and let $|\hat{\psi}_y\rangle$ be the dual Gaussian state,

   $$|\hat{\psi}_y\rangle = \sum_{x \in \mathbb{Z}_q^m : Ax = y \pmod{q}} \rho_{\sigma}(x) |x\rangle.$$

Let $\mathcal{Z}_{\text{LWE}_{n, A, q}^{m}}$ be the Pauli-Z dephasing channel with respect to the LWE distribution for $A \in \mathbb{Z}_q^{n \times m}$ and a noise ratio $\alpha \in (0, 1)$ with relative noise magnitude $\frac{q/\alpha}{q} = \lambda^{o(1)}$, i.e.

   $$\mathcal{Z}_{\text{LWE}_{n, A, q}^{m}}(\rho) = \sum_{s_0 \in \mathbb{Z}_q^m} \sum_{\mathbf{e}_0 \in \mathbb{Z}_q^m} q^{-n} D_{\mathbb{Z}_q^{m}, q}^{s_0, \mathbf{A} + \mathbf{e}_0} Z_q^{s_0, \mathbf{A} + \mathbf{e}_0} Z_q^{(s_0, \mathbf{A} + \mathbf{e}_0)} \rho Z_q^{s_0, \mathbf{A} + \mathbf{e}_0}, \quad \forall \rho \in L((\mathbb{C}^q)^{\otimes m}).$$
Algorithm 2: GenPrimal($A, \sigma$)

**Input:** Matrix $A \in \mathbb{Z}_q^{n \times m}$ whose columns generate $\mathbb{Z}_q^n$, and a parameter $\sigma = \mathcal{O} \left( \frac{q}{\sqrt{m}} \right)$.

**Output:** Gaussian state $|\psi_y\rangle$ and $y \in \mathbb{Z}_q^n$.

1. Run $\text{GenDual}(A, \sigma)$, resulting in the state
   \[
   |\hat{\psi}_y\rangle_{XY} = \sum_{x \in \mathbb{Z}_q^n} e^{i \langle x | x \rangle} |x\rangle_Y |y\rangle_Y .
   \]

2. Apply the quantum Fourier transform $\text{FT}_q$ to system $X$.

3. Output the state in system $X$, denoted by $|\psi_y\rangle$, and the outcome $y \in \mathbb{Z}_q^n$ in system $Y$.

Figure 3: Quantum algorithm which takes as input a matrix $A \in \mathbb{Z}_q^{n \times m}$ and a parameter $\sigma = \mathcal{O} \left( \frac{q}{\sqrt{m}} \right)$, and outputs the primal Gaussian state in Definition 16.

Then, there exists a negligible function $\varepsilon(\lambda)$ such that
\[
\mathcal{Z}_{LWE_{m,q,\lambda}} \left( |\hat{\psi}_y\rangle \langle \hat{\psi}_y| \right) \approx \varepsilon \ |\hat{\psi}_y\rangle \langle \hat{\psi}_y| .
\]

In other words, the Pauli-$Z$ dephasing channel with respect to the LWE distribution leaves the dual Gaussian state approximately invariant.

**Proof.** Let $y \in \mathbb{Z}_q^n$ be an arbitrary vector and recall that the dual Gaussian state $|\hat{\psi}_y\rangle$ is given by
\[
|\hat{\psi}_y\rangle \sum_{x \in \mathbb{Z}_q^n} e^{i \langle x | x \rangle} |x\rangle . \tag{13}
\]

Consider a sample $b = s_0 \cdot A + e_0 \pmod{q} \sim \mathcal{LWE}_{m,q,\lambda} \text{ with } s \sim \mathbb{Z}_q^n \text{ and } e_0 \sim D_{\mathbb{Z}_q^n, \lambda}$. Because $\sigma \in (\sqrt{8m}, q / \sqrt{8m})$ and $\frac{q}{\sigma} = \lambda^{\Omega(1)}$, there exist negligible $\eta(\lambda)$ and $\kappa(\lambda)$ such that
\[
\mathcal{Z}_{Z_{\rho}^S \cdot A + e_0}^S |\hat{\psi}_y\rangle = \mathcal{Z}_{\mathcal{LWE}_{m,q,\lambda}} \big( |\hat{\psi}_y\rangle \langle \hat{\psi}_y| \big) \approx \varepsilon \ |\hat{\psi}_y\rangle \langle \hat{\psi}_y| . \tag{Lemma 6}
\]

Here, $|\psi_y\rangle$ is the primal Gaussian state given by
\[
|\psi_y\rangle = \sum_{s \in \mathbb{Z}_q^n} \sum_{e \in \mathbb{Z}_q^n} e^{i \langle s | e \rangle} \omega_q^{(s,y)} |sA + e \pmod{q}\rangle .
\]

In other words, $|\hat{\psi}_y\rangle$ in Eq. (13) is an approximate eigenvector of the generalized Pauli operator $Z_{\rho}^S \cdot A + e_0$ with respect to the same matrix $A \in \mathbb{Z}_q^{n \times m}$. Note that we can simply discard $\omega_q^{(s,y)} \in \mathbb{C}$ because it serves
as a global phase. Hence, there exists a negligible function $\epsilon(\lambda)$ such that

$$Z_{\text{LWE}_{m,0,\alpha}}(\langle \hat{\psi}_y | \hat{\psi}_y \rangle) = \sum_{s_0 \in \mathbb{Z}_q^n} \sum_{e_0 \in \mathbb{Z}_q^m} D_Z^{s_0, -\alpha q}(e_0) \left| Z_{q - n}^{s_0 \cdot A + e_0} \langle \hat{\psi}_y | \hat{\psi}_y \rangle \right| \approx \epsilon \left( \sum_{s_0 \in \mathbb{Z}_q^n} q^{-n} \right) \cdot \left( \sum_{e_0 \in \mathbb{Z}_q^m} D_Z^{s_0, -\alpha q}(e_0) \right) \left| \hat{\psi}_y \rangle \langle \hat{\psi}_y \right| \approx \epsilon(\lambda).$$

## 4 Uncertainty Relation for Fourier Basis Projections

In this section, we prove an entropic uncertainty relation with respect to so-called Fourier basis projections. Informally, we say that a projector $\hat{\Pi}$ is a Fourier basis projection, if $\hat{\Pi}$ corresponds to a projector (onto a subset of $\mathbb{Z}_q^m$) which is conjugated by the $q$-ary Fourier transform $\text{FT}_q$. Notice that the deletion procedures of our encryption schemes with certified deletion in Section 7 and Section 9 require a Fourier basis projection onto a small set of solutions to the (inhomogenous) short integer solution (ISIS) problem. Another example can be found in the work of Aaronson and Christiano [AC12] who used Hadamard basis projections (a special case of the $q$-ary Fourier transform) onto small hidden subspaces to verify quantum money states.

Our uncertainty relation captures the following intuitive property: any system which passes a Fourier basis projection onto a small subset of $\mathbb{Z}_q^m$ (say, with high probability) must necessarily be unentangled with any auxiliary system. We formalize this statement using the (smooth) quantum min-entropy (Definition 5).

### 4.1 Fourier basis projections

**Definition 17 (Fourier basis projection).** Let $m \in \mathbb{N}$ and let $q \geq 2$ be an integer modulus. Let $S \subseteq \mathbb{Z}_q^m$ be an arbitrary set and let $\Pi_S$ be the associated projector onto $S$, where

$$\Pi_S = \sum_{x \in S} |x\rangle \langle x|.$$  

Then, we define the associated Fourier basis projection onto $S$ as the projector

$$\hat{\Pi}_S = \text{FT}_q^\dag \Pi_S \text{FT}_q.$$ 

### 4.2 Uncertainty relation

In this section, our main result is the following.

**Theorem 3** (Uncertainty relation for Fourier basis projections). Let $m \in \mathbb{N}$, $q \geq 2$ be a modulus, $\{|\psi^x\rangle\}_{x \in \mathbb{Z}_q^m}$ be any family of normalized auxiliary states, and let $|\psi\rangle_{AB}$ be any state of the form

$$|\psi\rangle_{AB} = \sum_{x \in \mathbb{Z}_q^m} a_x |x\rangle_A \otimes |\psi^x\rangle_B \quad \text{s.t.} \quad \sum_{x \in \mathbb{Z}_q^m} |a_x|^2 = 1.$$ 

Let $S \subseteq \mathbb{Z}_q^m$ be an arbitrary set and define the following projectors onto system $A$,

$$\Pi_S = \sum_{x \in S} |x\rangle \langle x| \quad \text{and} \quad \hat{\Pi}_S = \text{FT}_q^\dag \Pi_S \text{FT}_q.$$ 

28
Suppose that \( \| (\hat{\Pi}_S \otimes 1_B) \rho \|_2^2 = 1 - \varepsilon \), for some \( \varepsilon \geq 0 \). Then, it holds that

\[
H_{\min}^\varepsilon (X|B)_\rho \geq m \cdot \log q - 2 \cdot \log \| S \|.
\]

Here, \( q_{XB} \) results from a computational basis measurement of system \( A \) of the state \( \rho \langle \phi | AB \), i.e.

\[
q_{XB} = \sum_{x \in \mathbb{Z}_q^m} |x \rangle \langle x | \otimes \text{tr}_A \left[ (|x \rangle \langle x | A) \otimes 1_B \right] \langle \phi | AB \rangle.
\]

**Proof.** Suppose that \( |\phi \rangle_{AB} \) satisfies \( \| (\hat{\Pi}_S \otimes 1_B) |\phi \rangle_{AB} \|_2^2 = 1 - \varepsilon \), for some \( \varepsilon \geq 0 \). From Lemma 2, it follows that there exists an ideal pure state,

\[
|\bar{\phi} \rangle_{AB} = \frac{(\hat{\Pi}_S \otimes 1_B) |\phi \rangle_{AB}}{\| (\hat{\Pi}_S \otimes 1_B) |\phi \rangle_{AB} \|} = \sum_{x \in \mathbb{Z}_q^m} \alpha_x |x \rangle_A \otimes |\phi^x \rangle_B \quad \text{s.t.} \quad \sum_{x \in \mathbb{Z}_q^m} |\alpha_x|^2 = 1,
\]

with the property that

\[
\| |\phi \rangle \langle \phi | - |\bar{\phi} \rangle \langle \bar{\phi} | \|_\text{tr} \leq \sqrt{\varepsilon} \quad \text{and} \quad |\bar{\phi} \rangle \in \text{im}(\hat{\Pi}_S \otimes 1_B).
\]

Because \( |\bar{\phi} \rangle_{AB} \) lies in the image of the projector \( \hat{\Pi}_S \otimes 1_B \), we have

\[
|\bar{\phi} \rangle_{AB} = (\hat{\Pi}_S \otimes 1_B) |\bar{\phi} \rangle_{AB} = \sum_{x' \in \mathbb{Z}_q^m} \sum_{s \in S} \alpha_{x'} \cdot \omega_q^{\langle x,s \rangle} \omega_q^{-(x',s)} \langle x \rangle_A \otimes |\phi^x \rangle_B.
\]

Let us now analyze the ideal state \( \tilde{q}_{XB} \) which results from a computational basis measurement of system \( A \) of the state \( |\bar{\phi} \rangle \langle \bar{\phi} | AB \). In other words, we consider the CQ state given by

\[
\tilde{q}_{XB} = \sum_{x \in \mathbb{Z}_q^m} |x \rangle \langle x | \otimes \text{tr}_A \left[ (|x \rangle \langle x | A) \otimes 1_B \right] \langle \bar{\phi} | AB \rangle.
\]

By the definition of the guessing probability in Definition 6, we have

\[
p_{\text{guess}}(X|B)_\tilde{q} = \sup_{M_B} \sum_{x \in \mathbb{Z}_q^m} \left( \| (|x \rangle \langle x | A) \otimes M_B^x |\bar{\phi} \rangle_{AB} \| \right)^2
\]

\[
= \sup_{M_B} \sum_{x \in \mathbb{Z}_q^m} q^{-2m} \left( \sum_{x' \in \mathbb{Z}_q^m} \sum_{s \in S} \alpha_{x'} \cdot \omega_q^{\langle x,s \rangle} \omega_q^{-(x',s)} \langle x \rangle_A \otimes M_B^x |\phi^x \rangle_B \right)^2
\]

\[
= \sup_{M_B} \sum_{x \in \mathbb{Z}_q^m} q^{-2m} \left( \sum_{x' \in \mathbb{Z}_q^m} \alpha_{x'} \cdot \left( \sum_{s \in S} \omega_q^{\langle x,s \rangle} \omega_q^{-(x',s)} \right) \langle x \rangle_A \otimes M_B^x |\phi^x \rangle_B \right)^2.
\]
Using the Cauchy-Schwarz-inequality, we find that for any $x \in \mathbb{Z}_{mq}^n$:

$$\left\| \sum_{x' \in \mathbb{Z}_{mq}^n} \bar{\alpha}_{x'} \cdot \left( \sum_{s \in S} \omega_q^{(x,s)} \omega_q^{-(x',s)} \right) |x\rangle_A \otimes M^x_B |\psi^x\rangle_B \right\|$$

$$\leq \sqrt{\sum_{x' \in \mathbb{Z}_{mq}^n} |\bar{\alpha}_{x'}|^2 \cdot \left( \sum_{s \in S} \omega_q^{(x,s)} \omega_q^{-(x',s)} \right)^2} \sqrt{\sum_{x' \in \mathbb{Z}_{mq}^n} \left| |x\rangle_A \otimes M^x_B |\psi^x\rangle_B \right|^2}$$

$$\leq |S|^2 \sqrt{\sum_{x' \in \mathbb{Z}_{mq}^n} |\bar{\alpha}_{x'}|^2 \cdot \left( \sum_{s \in S} \omega_q^{(x,s)} \omega_q^{-(x',s)} \right)^2} \sqrt{\sum_{x' \in \mathbb{Z}_{mq}^n} \left| |x\rangle_A \otimes M^x_B |\psi^x\rangle_B \right|^2}$$

$$= |S| \cdot \left[ \sum_{x' \in \mathbb{Z}_{mq}^n} \left\| M^x_B |\psi^x\rangle_B \right\|^2 \right]. \quad (14)$$

Using the inequality in (14), we can now bound the guessing probability as follows:

$$p_{\text{guess}}(X|B)_{\bar{\rho}} \leq \left\| \sum_{x \in \mathbb{Z}_{mq}^n} \sum_{x' \in \mathbb{Z}_{mq}^n} M^x_B |\psi^x\rangle_B \right\|^2$$

$$= \left\| \sum_{x \in \mathbb{Z}_{mq}^n} \sum_{x' \in \mathbb{Z}_{mq}^n} M^x_B |\psi^x\rangle_B \right\|^2$$

$$= \left\| \sum_{x \in \mathbb{Z}_{mq}^n} \sum_{x' \in \mathbb{Z}_{mq}^n} M^x_B |\psi^x\rangle_B \right\|^2 \quad \text{(since } \sum_{x} M^x_B = 1)$$

Because the purified distance is bounded above by the trace distance, it follows that

$$P(\rho_{XB}, \bar{\rho}_{XB}) \leq \| \rho_{XB} - \bar{\rho}_{XB} \|_{\text{tr}} \leq \| |\psi\rangle \langle \psi| - |\bar{\psi}\rangle \langle \bar{\psi}| \|_{\text{tr}} \leq \sqrt{\varepsilon}.$$ 

Therefore, by the definition of (smooth) min-entropy (see Definition 5), we have

$$H_{\min}(X|B)_{\bar{\rho}} \leq \sup_{\rho_{XB}} H_{\min}(X|B)_{\rho} = H_{\min}^{\sqrt{\varepsilon}}(X|B)_{\rho}. \quad (15)$$

Putting everything together, it follows from (15) and Theorem 1 that

$$H_{\min}^{\sqrt{\varepsilon}}(X|B)_{\rho} \geq H_{\min}(X|B)_{\bar{\rho}}$$

$$= - \log p_{\text{guess}}(X|B)_{\bar{\rho}}$$

$$\geq m \cdot \log q - 2 \cdot \log |S|.$$ 

This proves the claim. \qed

5 Gaussian-Collapsing Hash Functions

Unruh [Unr15] introduced the notion of collapsing hash functions in his seminal work on computationally binding quantum commitments. This property is captured by the following definition.
**Definition 18** (Collapsing hash function, [Unr15]). Let \( \lambda \in \mathbb{N} \) be the security parameter. A hash function family \( \mathcal{H} = \{ H_\lambda \}_{\lambda \in \mathbb{N}} \) is called collapsing if, for every QPT adversary \( \mathcal{A} \),

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

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

1. The challenger samples a random hash function \( h \leftarrow H_\lambda \), and sends a description of \( h \) to \( \mathcal{A} \).
2. \( \mathcal{A} \) responds with a (classical) string \( y \in \{0,1\}^{n(\lambda)} \) and an \( m(\lambda) \)-qubit quantum state in system \( X \).
3. The challenger coherently computes \( h \) (into an auxiliary system \( Y \)) given the state in system \( X \), and then performs a two-outcome measurement on \( Y \) indicating whether the output of \( h \) equals \( y \). If \( h \) does not equal \( y \) the challenger aborts and outputs \( \bot \).
4. If \( b = 0 \), the challenger does nothing. Else, if \( b = 1 \), the challenge measures the \( m(\lambda) \)-qubit system \( X \) in the computational basis. Finally, the challenger returns the state in system \( X \) to \( \mathcal{A} \).
5. \( \mathcal{A} \) returns a bit \( b' \), which we define as the output of the experiment.

Motivated by the properties of the dual Gaussian state from **Definition 16**, 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 19** (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 \( \sigma \)-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 GaussCollapseExp\(_{\mathcal{H},\mathcal{A},\lambda}(b) \) is defined as follows:

1. The challenger samples a random hash function \( h \leftarrow H_\lambda \) and prepares the quantum state

\[
| \hat{\psi} \rangle_{XY} = \sum_{x \in \mathbb{Z}_q^m} q_\sigma(x) \, |x\rangle_X \otimes |h(x)\rangle_Y.
\]

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

\[
| \hat{\psi}_Y \rangle_{XY} = \sum_{\substack{x \in \mathbb{Z}_q^m: \ h(x) = y \}} q_\sigma(x) \, |x\rangle_X \otimes |y\rangle_Y.
\]

3. If \( b = 0 \), the challenger does nothing. Else, if \( b = 1 \), the challenger measures system \( X \) of the quantum state \( | \hat{\psi}_Y \rangle \) in the computational basis. Finally, the challenger sends the outcome state in systems \( X \) to \( \mathcal{A} \), together with the string \( y \in \mathbb{Z}_q^n \) 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.

The following follows immediately from the definition of Gaussian-collapsing hash functions, and the fact that the dual Gaussian state can be efficiently prepared using **Algorithm 1**.

**Claim 1.** Let \( \mathcal{H} = \{ H_\lambda \}_{\lambda \in \mathbb{N}} \) be a hash function family with domain \( \mathcal{X} = \mathbb{Z}_q^m \) and range \( \mathcal{Y} = \mathbb{Z}_q^n \), where \( m(\lambda), n(\lambda) \in \mathbb{N} \). If \( \mathcal{H} \) is collapsing, then \( \mathcal{H} \) is also \( \sigma \)-Gaussian-collapsing, for any \( \sigma = \Omega(\sqrt{m}) \).
5.1 Ajtaj’s hash function

Liu and Zhandry [LZ19] implicitly showed that the Ajtaj hash function \( h_A(x) = Ax \mod q \) is collapsing – and thus Gaussian-collapsing – via the notion of lossy functions and by assuming the superpolynomial hardness of (decisional) LWE. In this section, we give a simple and direct proof that the Ajtaj hash function is Gaussian-collapsing assuming (decisional) LWE, which might be of independent interest.

**Theorem 4.** Let \( n, m \in \mathbb{N} \) be integers and let \( q \geq 2 \) be a prime modulus, each parameterized by \( \lambda \in \mathbb{N} \). Let \( \sigma \in (\sqrt{8m}, q/\sqrt{8m}) \) be a function of \( \lambda \). Then, the Ajtaj hash function family \( \mathcal{H} = \{ H_\lambda \}_{\lambda \in \mathbb{N}} \) with

\[
H_\lambda = \left\{ h_A : \mathbb{Z}^m_q \to \mathbb{Z}^n_q \ \text{s.t.} \ h_A(x) = A \cdot x \mod q; \ A \in \mathbb{Z}^{n \times m}_q \right\}
\]

is \( \sigma \)-Gaussian-collapsing assuming the quantum hardness of the decisional \( \text{LWE}^m_{n,A,q} \) problem, for any parameter \( \alpha \in (0, 1) \) with relative noise magnitude \( q/\sigma = \lambda^\omega(1) \).

**Proof.** Let \( A \) denote the QPT adversary in the experiment \( \text{GaussCollapseExp}_{H,A,\lambda}(b) \) with \( b \in \{0, 1\} \). To prove the claim, we give a reduction from the decisional \( \text{LWE}^m_{n,A,q} \) assumption. We are given as input a sample \((A, b)\) with \( A \xleftarrow{\$} \mathbb{Z}^{m \times n}_q \), where \( b = s_0 \cdot A + e_0 \mod q \)) is either a sample from the LWE distribution with \( s_0 \xleftarrow{\$} \mathbb{Z}^m_q \) and \( e_0 \sim D_{\mathbb{Z}^n_q, A,q} \), or where \( b \) is a uniformly random string \( u \xleftarrow{\$} \mathbb{Z}^m_q \).

Consider the distinguisher \( D \) that acts as follows on input \( 1^\lambda \) and \( (A, b) \):

1. \( D \) prepares a bipartite quantum state on systems \( X \) and \( Y \) with

\[
|\hat{\psi}\rangle_{XY} = \sum_{x \in \mathbb{Z}^n_q} \psi_\sigma(x) |x\rangle_X \otimes |A \cdot x \mod q\rangle_Y.
\]

2. \( D \) measures system \( Y \) in the computational basis, resulting in the state

\[
|\hat{\psi}\rangle_{XY} = \sum_{x \in \mathbb{Z}^n_q: A\cdot x = y} \psi_\sigma(x) |x\rangle_X \otimes |y\rangle_Y.
\]

3. \( D \) applies the generalized Pauli-\( Z \) operator \( Z^b_q \) on system \( X \), resulting in the state

\[
(Z^b_q \otimes \mathbb{1}_Y) |\hat{\psi}\rangle_{XY} = \sum_{x \in \mathbb{Z}^n_q: A\cdot x = y} \psi_\sigma(x) \left(Z^b_q |x\rangle_X\right) \otimes |y\rangle_Y.
\]

4. \( D \) runs the adversary \( A \) on input system \( X \) and classical descriptions of \( A \in \mathbb{Z}^{m \times n}_q \) and \( y \in \mathbb{Z}^n_q \).

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

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

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

We now show that this implies that \( D \) succeeds at the decisional \( \text{LWE}^m_{n,q,A,q} \) experiment with advantage at least \( 1/p(\lambda) - \text{negl}(\lambda) \). We distinguish between the following two cases.
If \((A, b)\) is a sample from the LWE distribution with \(b = s_0 \cdot A + e_0 \pmod q\), then the adversary \(A\) receives as input the following quantum state in system \(X\):

\[
Z_{\text{LWE}_{n,q,aq}}^{m}(|\hat{\psi}_y\rangle\langle\hat{\psi}_y|_X) = \sum_{s_0 \in \mathbb{Z}_q^n} \sum_{e_0 \in \mathbb{Z}^m} q^{-n} D^{mq,aq}_{Z_0} (e_0) \ Z_q^{s_0 \cdot A + e_0} |\hat{\psi}_y\rangle\langle\hat{\psi}_y|_X Z_q^{-(s_0 \cdot A + e_0)}.
\]

From Theorem 2 it follows that there exists a negligible function \(\varepsilon(\lambda)\) such that

\[
Z_{\text{LWE}_{n,q,aq}}^{m}(|\hat{\psi}_y\rangle\langle\hat{\psi}_y|_X) \approx \varepsilon |\hat{\psi}_y\rangle\langle\hat{\psi}_y|_X.
\]

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

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

\[
Z(|\hat{\psi}_y\rangle\langle\hat{\psi}_y|_X) = q^{-m} \sum_{u \in \mathbb{Z}_q^m} Z_q^u |\hat{\psi}_y\rangle\langle\hat{\psi}_y|_X Z_q^{-u}.
\]

Because \(Z\) corresponds to the uniform Pauli-\(Z\) dephasing channel, it follows from Lemma 7 that

\[
Z(|\hat{\psi}_y\rangle\langle\hat{\psi}_y|_X) = \sum_{x \in \mathbb{Z}_q^m} |(x|\hat{\psi}_y\rangle|^2 |x\rangle\langle x|_X.
\]

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

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

**Theorem 5.** Let \(n \in \mathbb{N}\) and \(q \geq 2\) be a prime modulus with \(m \geq 2n \log q\), each parameterized by the security parameter \(\lambda \in \mathbb{N}\). Let \(\sigma \in (\sqrt{8m}, q/\sqrt{8m})\) be a function of \(\lambda\) and \(A \leftarrow \mathbb{Z}_q^{n \times m}\) be a matrix.

Then, the following states are computationally indistinguishable assuming the quantum hardness of decisional \(\text{LWE}_{n,q,aq}^m\) for any parameter \(\alpha \in (0,1)\) with relative noise magnitude \(\frac{q/\sigma}{\sigma} = \lambda^{\omega(1)}\):

- For any \((|\psi_y\rangle, y) \leftarrow \text{GenDual}(A, \sigma)\) in Algorithm 1:
  \[
  |\psi_y\rangle = \sum_{x \in \mathbb{Z}_q^m} q_\sigma(x) |x\rangle \approx_c |x_0\rangle : x_0 \sim D_{A^\perp}(A, q^{1/2}).
  \]

- For any \((|\psi_y\rangle, y) \leftarrow \text{GenPrimal}(A, \sigma)\) in Algorithm 2:
  \[
  |\psi_y\rangle = \sum_{s \in \mathbb{Z}_q^n} \sum_{e \in \mathbb{Z}_q^m} q_\sigma(e) \omega_q^{-(s,y)} |sA + e\rangle \approx_c \sum_{u \in \mathbb{Z}_q^m} \omega_q^{-(u,x_0)} |u\rangle : x_0 \sim D_{A^\perp}(A, q^{1/p}).
  \]

Moreover, the distribution of \(y \in \mathbb{Z}_q^n\) is negligibly close in total variation distance to the uniform distribution over \(\mathbb{Z}_q^n\). Here, \(\Lambda_q^+(A) = \{x \in \mathbb{Z}_q^m : Ax = y \pmod q\}\) denotes a coset of the lattice \(\Lambda_q^+(A)\).
Proof. Let \( A \sim Z_q^{n \times m} \) be a random matrix. From Lemma 9 it follows that the columns of \( A \) generate \( Z_q^n \) with overwhelming probability. Let us also recall the following simple facts about the discrete Gaussian.

According to Lemma 10, the distribution of the syndrome \( A \cdot x \equiv y \mod q \) is statistically close to the uniform distribution over \( Z_q^n \), whenever \( x \sim D_{Z_q^n, \sigma} \) and \( \sigma = \omega(\sqrt{\log m}) \). Moreover, the conditional distribution of \( x \sim D_{Z_q^n, \sigma} \) given the syndrome \( y \in Z_q^n \) is a discrete Gaussian distribution \( D_{\Lambda_q^\sigma(A), \sigma} \).

Let us now show the first statement. Recall that in Theorem 4 we show that the Ajtai hash function \( h_A(x) = A \cdot x \mod q \) is \( \sigma \)-Gaussian-collapsing assuming the decisional \( \text{LWE}_n, q, \alpha, q \) assumption and a noise ratio \( \frac{q}{\alpha} \leq \lambda^2 \). Therefore, for \( y \in Z_q^n \), the (normalized variant of the) dual Gaussian state,

\[
|\hat{\psi}_y\rangle = \sum_{x \in Z_q^n : Ax = y \mod q} \psi_{\sigma}(x) |x\rangle
\]

is computationally indistinguishable from the (normalized) classical mixture,

\[
\sum_{x \in Z_q^n} |\langle x| \hat{\psi}_y \rangle|^2 |x\rangle = \left( \sum_{Z_q^n} \sum_{Ax = y \mod q} \psi_{\sigma}(z) \right)^{-1} \sum_{x \in Z_q^n : Ax = y \mod q} \psi_{\sigma}(x) |x\rangle
\]

which is the result of a computational basis measurement of \( |\hat{\psi}_y\rangle \). Since \( \sigma \in (\sqrt{8m}, q/\sqrt{8m}) \), the tail bound in Lemma 11 implies that the above mixture is statistically close to the discrete Gaussian \( D_{\Lambda_q^\sigma(A), q} \).

The second statement follows immediately by applying the (inverse) Fourier transform to both of the states above. Note that in Lemma 16 we showed that the primal Gaussian state

\[
|\psi_y\rangle = \sum_{s \in Z_q^n} \sum_{e \in Z_q^n} \psi_s(e) \omega_q^{-s\langle y \rangle} |sA + e\rangle
\]

is within negligible trace distance of \( \text{FT}_q^\dagger |\psi_y\rangle \). This proves the claim.

\[\square\]

### 5.2 Strong Gaussian-collapsing conjecture

Our quantum encryption schemes with certified deletion in Section 7 and Section 9 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** (Strong Gaussian-Collapsing Conjecture).

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

\[
H_\lambda = \left\{ h_A : Z_q^n \rightarrow Z_q^n \text{ s.t. } h_A(x) = A \cdot x \mod q; A \in Z_q^{n \times m} \right\}.
\]

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

\[
\Pr[\text{StrongGaussCollapseExp}_{H_\lambda} \lambda (0) = 1] - \Pr[\text{StrongGaussCollapseExp}_{H_\lambda} \lambda (1) = 1] \leq \text{negl}(\lambda).
\]

**Here, the experiment** \( \text{StrongGaussCollapseExp}_{H_\lambda} \lambda (b) \) **is defined as follows:**

---

\(^4\text{Here, the additional factor } 1/\sqrt{2} \text{ arises from the normalization of the dual Gaussian state } |\hat{\psi}_y\rangle.\)
1. The challenger samples $\bar{A} \in \mathbb{Z}_q^\lambda$ and prepares the quantum state
\[ |\psi\rangle_{XY} = \sum_{x \in \mathbb{Z}_q^m} \varphi(x) |x\rangle_X \otimes |A \cdot x \pmod{q}\rangle_Y, \]

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

2. The challenger measures system $Y$ in the computational basis, resulting in the state
\[ |\psi_y\rangle_{XY} = \sum_{x \in \mathbb{Z}_q^m} \varphi(x) |x\rangle_X \otimes |y\rangle_Y. \]

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

4. $A$ sends a classical witness $w \in \mathbb{Z}_q^m$ to the challenger.

5. The challenger checks whether $A \cdot w = y \pmod{q}$ and $|w| \leq \sqrt{n} \varphi/\sqrt{2}$. If $w$ passes both checks, the challenger sends $t = (x, -1) \in \mathbb{Z}_q^m$ to $A$ with $A \cdot t = 0 \pmod{q}$. Else, the challenger aborts.

6. $A$ returns a bit $b'$, which we define as the output of the experiment.

**Remark.** We also consider an $N$-fold variant of $SGC_{n, m, A, \sigma}$, which we denote by $SGC_{n, m, A, \sigma}^N$, where the challenger prepares $N$ independent states $|\psi_{y_1}\rangle \otimes \cdots \otimes |\psi_{y_N}\rangle$ in Steps 1–2, for outcomes $y_1, \ldots, y_N \in \mathbb{Z}_q^n$. A simple hybrid argument shows that $SGC_{n, m, A, \sigma}^N$ is implied by $SGC_{n, m, A, \sigma}$, for any $N = \text{poly}(\lambda)$.

**Towards a proof of the strong-Gaussian-collapsing conjecture.** Unfortunately, we currently do not know how to prove Conjecture 5.2 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 $A \in \mathbb{Z}_q^{n \times m}$. In order to simulate the experiment StrongGaussCollapseExp_{H, A, \lambda}, with respect to an adversary $A$, we have to eventually forward a short trapdoor vector $t \in \mathbb{Z}_q^m$ in order to simulate the second phase of the experiment once $A$ has produced a valid witness. Notice, however, that the reduction has no way of obtaining a short vector $t$ in the kernel of $A$ as it is trying to break the underlying LWE (or ISIS) problem with respect to $A$ in the first place. Therefore, any successful security proof must necessarily exploit the fact that there is interaction between the challenger and the adversary $A$, and that a short trapdoor vector $t$ is only revealed after $A$ has already produced a valid short pre-image of $y \in \mathbb{Z}_q^n$.

When trying to distinguish between the state $|\psi_y\rangle$ and a single Gaussian pre-image $|x_0\rangle$ with the property that $A \cdot x_0 = y \pmod{q}$, it is useful to work with the Fourier basis. Without loss of generality, we can assume that $A$ instead receives one of the following states during in Step 2; namely
\[ \sum_{s \in \mathbb{Z}_q^n} \sum_{e \in \mathbb{Z}_q^m} \varphi(s) \omega_q^{-(s \cdot y)} |sA + e\rangle_X \quad \text{or} \quad \sum_{u \in \mathbb{Z}_q^n} \omega_q^{-(u \cdot x_0)} |u\rangle_X. \]

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 $t$ is revealed (ideally, without disturbing $X$ so as to allow for a Fourier basis measurement).
Because finding a valid witness \( w \) to the ISIS problem specified by \((A, y)\) now amounts to a Fourier basis projection (as in Definition 17), the entropic uncertainty relation in Theorem 3 immediately rules out large class of attacks, including the shift-by-LWE-sample attack we described in Section 1.2. 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 \( w \) and simultaneously distinguish the auxiliary system \( B \) with access to the trapdoor \( t \). 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 \((A, y)\). Intuitively, if the state in system \( X \) yields a short-pre image \( w \) with high probability via a Fourier basis measurement, then system \( X \) cannot be entangled with any auxiliary systems. Because the set \( S \) of valid short pre-images (i.e. the set of solution to the ISIS problem specified by \( A \) and \( y \)) is much smaller than the size of \( \mathbb{Z}_q^n \) (in particular, if \( \sigma \sqrt{m} \ll q \)), Theorem 3 tells us that the min-entropy of system \( X \) (once it is measured in the computational basis) 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 \( t \) 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 Conjecture 5.2, it captures the inherent difficulty in extracting information encoded in two mutually unbiased bases, i.e. the computational basis and the Fourier basis.

6 Public-Key Encryption with Certified Deletion

In this section, we formalize the notion of public-key encryption with certified deletion.

6.1 Definition

We first introduce the following definition.

**Definition 20** (Public-key encryption with certified deletion). A public-key encryption scheme with certified deletion \( (\text{PKE}_{\text{CD}}) \Sigma = (\text{KeyGen, Enc, Dec, Del, Vrfy}) \) with plaintext space \( \mathcal{M} \) consists of a tuple of QPT algorithms, a key generation algorithm \( \text{KeyGen} \), an encryption algorithm \( \text{Enc} \), and a decryption algorithm \( \text{Dec} \), a deletion algorithm \( \text{Del} \), and a verification algorithm \( \text{Vrfy} \).

\[
\text{KeyGen}(1^\lambda) \rightarrow (pk, sk) : \text{takes as input the parameter } 1^\lambda \text{ and outputs a public key } pk \text{ and secret key } sk.
\]

\[
\text{Enc}(pk, m) \rightarrow (vk, CT) : \text{takes as input the public key } pk \text{ and a plaintext } m \in \mathcal{M}, \text{ and outputs a classical verification key } vk \text{ together with a quantum ciphertext } CT.
\]

\[
\text{Dec}(sk, CT) \rightarrow m' \text{ or } \perp : \text{takes as input the secret key } sk \text{ and ciphertext } CT, \text{ and outputs } m' \in \mathcal{M} \text{ or } \perp.
\]

\[
\text{Del}(CT) \rightarrow \pi : \text{takes as input a ciphertext } CT \text{ and outputs a classical certificate } \pi.
\]

\[
\text{Vrfy}(vk, \pi) \rightarrow \top \text{ or } \perp : \text{takes as input the verification key } vk \text{ and certificate } \pi, \text{ and outputs } \top \text{ or } \perp.
\]

**Definition 21** (Correctness of \( \text{PKE}_{\text{CD}} \)). We require two separate kinds of correctness properties, one for decryption and one for verification.
(Decryption correctness:) For any \( \lambda \in \mathbb{N} \), and for any \( m \in \mathcal{M} \):
\[
\Pr \left[ \text{Dec}(sk, CT) \neq m \middle| \begin{array}{l}
(pk, sk) \leftarrow \text{KeyGen}(1^\lambda) \\
CT \leftarrow \text{Enc}(pk, m)
\end{array} \right] \leq \text{negl}(\lambda).
\]

(Verification correctness:) For any \( \lambda \in \mathbb{N} \), and for any \( m \in \mathcal{M} \):
\[
\Pr \left[ \text{Vrfy}(vk, \pi) = \bot \middle| \begin{array}{l}
(pk, sk) \leftarrow \text{KeyGen}(1^\lambda) \\
(vk, CT) \leftarrow \text{Enc}(pk, m) \\
\pi \leftarrow \text{Del}(CT)
\end{array} \right] \leq \text{negl}(\lambda).
\]

The notion of IND-CPA-CD security for public-key encryption was first introduced by Hiroka, Morimae, Nishimaki and Yamakawa [HMNY21b].

6.2 Certified deletion security

In terms of security, we adopt the following definition.

**Definition 22** (Certified deletion security for PKE). Let \( \Sigma = (\text{KeyGen, Enc, Dec, Del, Vrfy}) \) be a PKE_{CD} scheme and let \( A \) be a QPT adversary (in terms of the security parameter \( \lambda \in \mathbb{N} \)). We define the security experiment \( \text{Exp}_{\Sigma, A, \lambda}^{pk\text{-cert\text{-}del}(b)} \) between \( A \) and a challenger as follows:

1. The challenger generates a pair \( (pk, sk) \leftarrow \text{KeyGen}(1^\lambda) \), and sends \( pk \) to \( A \).
2. \( A \) sends a plaintext pair \( (m_0, m_1) \in \mathcal{M} \times \mathcal{M} \) to the challenger.
3. The challenger computes \( (vk, CT_b) \leftarrow \text{Enc}(pk, m_b) \), and sends \( CT_b \) to \( A \).
4. At some point in time, \( A \) sends the certificate \( \pi \) to the challenger.
5. The challenger computes \( \text{Vrfy}(vk, \pi) \) and sends \( sk \) to \( A \), if the output is \( \top \), and sends \( \bot \) otherwise.
6. \( A \) outputs a guess \( b' \in \{0, 1\} \), which is also the output of the experiment.

We say that the scheme \( \Sigma \) is IND-CPA-CD-secure if, for any QPT adversary \( A \), it holds that
\[
\text{Adv}_{\Sigma, A, \lambda}^{pk\text{-cert\text{-}del}(\lambda)} := |\Pr[\text{Exp}_{\Sigma, A, \lambda}^{pk\text{-cert\text{-}del}(0)} = 1] - \Pr[\text{Exp}_{\Sigma, A, \lambda}^{pk\text{-cert\text{-}del}(1)} = 1]| \leq \text{negl}(\lambda).
\]

7 Dual-Regev Public-Key Encryption with Certified Deletion

In this section, we consider the Dual-Regev PKE scheme due to Gentry, Peikert and Vaikuntanathan [GPV07]. Unlike Regev’s original PKE scheme in [Reg05], the Dual-Regev PKE scheme has the useful property that the ciphertext takes the form of a regular sample from the LWE distribution together with an additive shift which depends on the plaintext.
7.1 Construction

Parameters. Let $\lambda \in \mathbb{N}$ be the security parameter. We choose the following set of parameters for our Dual-Regev PKE scheme with certified deletion (each parameterized by $\lambda$).

- an integer $n \in \mathbb{N}$.
- a prime modulus $q \geq 2$.
- an integer $m \geq 2n \log q$.
- a noise ratio $\alpha \in (0, 1)$ such that $\sqrt{8(m+1)} \leq \frac{1}{\alpha} \leq \frac{q}{\sqrt{8(m+1)}}$.

Construction 1 (Dual-Regev PKE with Certified Deletion). Let $\lambda \in \mathbb{N}$. The Dual-Regev PKE scheme $\text{DualPKE}_{CD} = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Del}, \text{Vrfy})$ with certified deletion is defined as follows:

KeyGen$(1^\lambda) \rightarrow (pk, sk):$ sample a random matrix $A \leftarrow \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{x} \leftarrow \{0, 1\}^m$ and choose $A = [\mathbf{1}|A|\mathbf{x} \pmod{q}]$. Output $(pk, sk)$, where $pk = A \in \mathbb{Z}_q^{n \times (m+1)}$ and $sk = (-\mathbf{x}, 1) \in \mathbb{Z}_q^{m+1}$.

Enc$(pk, x) \rightarrow (vk, |CT|):$ parse $A \leftarrow pk$ and run $(|\psi_y\rangle, y) \leftarrow \text{GenPrimal}(A, 1/\alpha)$ in Algorithm 2, where $y \in \mathbb{Z}_q^n$. To encrypt a single bit $b \in \{0, 1\}$, output the pair

$$\left(\text{vk} \leftarrow (A \in \mathbb{Z}_q^{n \times (m+1)}, y \in \mathbb{Z}_q^n), \ |CT\rangle \leftarrow X_{b \in \{0,1\}}^{|\psi_y\rangle}\right),$$

where $vk$ is the public verification key and $|CT\rangle$ is an $(m + 1)$-qudit quantum ciphertext.

Dec$(sk, |CT\rangle) \rightarrow \{0, 1\}:$ to decrypt, measure the ciphertext $|CT\rangle$ in the computational basis with outcome $c \in \mathbb{Z}_q^m$. Compute $sk^T \cdot c \in \mathbb{Z}_q$ and output 0, if it is closer to 0 than to $\lfloor \frac{q}{2} \rfloor$, and output 1, otherwise.

Del$(|CT\rangle) \rightarrow \pi: \text{Measure } |CT\rangle \text{ in the Fourier basis and output the measurement outcome } \pi \in \mathbb{Z}_q^{m+1}$.

Vrfy$(vk, \pi) \rightarrow \{\top, \bot\}:$ to verify a deletion certificate $\pi \in \mathbb{Z}_q^{m+1}$, parse $(A, y) \leftarrow vk$ and output $\top$, if $A \cdot \pi = y \pmod{q}$ and $||\pi|| \leq \sqrt{m+1}/\sqrt{2\alpha}$, and output $\bot$, otherwise.

Proof of correctness. Let us now establish the correctness properties of DualPKE_{CD} in Construction 1.

Lemma 17 (Correctness of decryption). Let $n \in \mathbb{N}$ and $q \geq 2$ be a prime modulus with $m \geq 2n \log q$, each parameterized by the security parameter $\lambda \in \mathbb{N}$. Let $\alpha$ be a ratio with $\sqrt{8(m+1)} \leq \frac{1}{\alpha} \leq \frac{q}{\sqrt{8(m+1)}}$.

Then, for $b \in \{0, 1\}$, the scheme DualPKE_{CD} = (KeyGen, Enc, Dec, Del, Vrfy) in Construction 1 satisfies:

$$\Pr \left[ \text{Dec}(sk, |CT\rangle) = b \left| (pk, sk) \leftarrow \text{KeyGen}(1^\lambda) \right. \right. \left. \left. (vk, |CT\rangle) \leftarrow \text{Enc}(pk, b) \right] \geq 1 - \text{negl}(\lambda).$$

Proof. By the Leftover Hash Lemma (Lemma 4), the distribution of $A = [\mathbf{1}|A|\mathbf{x} \pmod{q}]$ is within negligible total variation distance of the uniform distribution over $\mathbb{Z}_q^{n \times (m+1)}$. Moreover, from Lemma 9 it follows that the columns of $A$ generate $\mathbb{Z}_q^n$ with overwhelming probability. Since the noise ratio $\alpha \in (0, 1)$
satisfies $\sqrt{8(m+1)} \leq \frac{1}{\alpha} \leq \frac{q}{\sqrt{8(m+1)}}$, it then follows from Corollary 1 that the ciphertext $|\text{CT}\rangle$ is within negligible trace distance of the state

$$\sum_{s \in \mathbb{Z}_q^n} \sum_{e \in \mathbb{Z}^{m+1}_q} \varrho_{a_0}(e) \omega_q^{-(s,e)} |sA + e + (0, \ldots, 0, b \cdot \lfloor \frac{q}{2} \rfloor)\rangle$$

A measurement in computational basis yields an outcome $c$ such that

$$c = s_0A + e_0 + (0, \ldots, 0, b \cdot \lfloor \frac{q}{2} \rfloor) \in \mathbb{Z}^{m+1}_q,$$

where $s_0 \leftarrow \mathbb{Z}_q^n$ is random and where $e_0 \sim D_{\mathbb{Z}^{m+1}_q \cdot \frac{q}{2}}$ is a sample from the (truncated) discrete Gaussian such that $\|e_0\| \leq a\sqrt{\frac{m+1}{2}} < \lfloor \frac{q}{4} \rfloor$. Since $\text{Dec}(sk, |\text{CT}\rangle)$ computes $sk^T \cdot c \in \mathbb{Z} \cap (-\frac{q}{2}, \frac{q}{2}]$ and outputs 0, if it is closer to 0 than to $\lfloor \frac{q}{2} \rfloor$ over , and 1 otherwise, it succeeds with overwhelming probability.

\[\square\]

Let us now prove the following property.

**Lemma 18** (Correctness of verification). Let $n \in \mathbb{N}$ and $q \geq 2$ be a prime modulus with $m \geq 2n \log q$, each parameterized by the security parameter $\lambda \in \mathbb{N}$. Let $\alpha$ be a ratio with $\sqrt{8(m+1)} \leq \frac{1}{\alpha} \leq \frac{q}{\sqrt{8(m+1)}}$.

Then, for $b \in \{0, 1\}$, the scheme $\text{DualPKE}_{\text{CD}} = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Del}, \text{Vrfy})$ in Construction 1 satisfies:

$$\Pr\left[\text{Verify}(vk, \pi) = T \mid (pk, sk) \leftarrow \text{KeyGen}^{(1^\lambda)}, (vk, |\text{CT}\rangle) \leftarrow \text{Enc}(pk, b), \pi \leftarrow \text{Del}(|\text{CT}\rangle)\right] \geq 1 - \text{negl}(\lambda).$$

**Proof.** By the Leftover Hash Lemma (Lemma 4), the distribution of $A = [\bar{A} | \bar{A} \cdot \tilde{x} \pmod{q}]$ is within negligible total variation distance of the uniform distribution over $\mathbb{Z}_q^n \times (m+1)$. From Lemma 9 it follows that the columns of $A$ generate $\mathbb{Z}_q^n$ with overwhelming probability. Since $\alpha \in (0, 1)$ is a ratio parameter with $\sqrt{8(m+1)} \leq \frac{1}{\alpha} \leq \frac{q}{\sqrt{8(m+1)}}$, Corollary 1 implies that the Fourier transform of the ciphertext $|\text{CT}\rangle$ is within negligible trace distance of the state

$$|\hat{\text{CT}}\rangle = \sum_{x \in \mathbb{Z}_q^{m+1}; A x = y \pmod{q}} \varrho_{1/\alpha}(x) \omega_q^{D_{\Lambda_{\alpha}}(A) \cdot \frac{1}{\sqrt{2\alpha}}} |x\rangle.$$  

From Lemma 11, it follows that the distribution of computational basis measurement outcomes is within negligible total variation distance of $\pi \sim D_{\Lambda_{\alpha}}[A, \frac{1}{\sqrt{2\alpha}}]$ with $\|\pi\| \leq \sqrt{m+1} / \sqrt{2\alpha}$. This proves the claim.

\[\square\]

### 7.2 Proof of security

Let us now analyze the security of our Dual-Regev PKE scheme with certified deletion in Construction 1.
IND-CPA security of DualPKE_{CD}. We first prove that our public-key encryption scheme DualPKE_{CD} in Construction 1 satisfies the notion IND-CPA security according to Definition 12. The proof follows from Theorem 5 and assumes the hardness of (decisional) LWE (Definition 15). We add it for completeness.

**Theorem 6.** Let \( n \in \mathbb{N} \) and \( q \geq 2 \) be a prime modulus with \( m \geq 2n \log q \), each parameterized by the security parameter \( \lambda \in \mathbb{N} \). Let \( \alpha \in (0, 1) \) be a noise ratio parameter with \( \sqrt{8(m + 1)} \leq \frac{1}{\alpha} \leq \frac{q}{\sqrt{8(m + 1)}} \).

Then, the scheme DualPKE_{CD} in Construction 1 is IND-CPA-secure assuming the quantum hardness of the decisional LWE_{m,n,q,\beta} problem, for any \( \beta \in (0, 1) \) with \( \alpha / \beta = \lambda^{\omega(1)} \).

**Proof.** Let \( \Sigma = \text{DualPKE}_{CD} \). We need to show that, for any QPT adversary \( A \), it holds that

\[
\text{Adv}_{\Sigma, A}(\lambda) := |\text{Pr}[\text{Exp}^{\text{ind-cpa}}_{\Sigma, A, \lambda}(0) = 1] - \text{Pr}[\text{Exp}^{\text{ind-cpa}}_{\Sigma, A, \lambda}(1) = 1]| \leq \text{negl}(\lambda).
\]

Consider the experiment \( \text{Exp}^{\text{ind-cpa}}_{\Sigma, A, \lambda}(b) \) between the adversary \( A \) and a challenger taking place as follows:

1. The challenger generates a pair \((pk, sk) \leftarrow \text{KeyGen}(\lambda)\), and sends \( pk \) to \( A \).
2. \( A \) sends a distinct plaintext pair \((m_0, m_1) \in \{0, 1\} \times \{0, 1\}\) to the challenger.
3. The challenger computes \((vk, CT_b) \leftarrow \text{Enc}(pk, m_b)\), and sends \( CT_b \) to \( A \).
4. \( A \) outputs a guess \( b' \in \{0, 1\} \), which is also the output of the experiment.

Recall that the procedure \( \text{Enc}(pk, m_b) \) outputs a pair \((vk, CT_b)\), where \((A \in \mathbb{Z}_{q}^{n \times (m+1)}, y \in \mathbb{Z}_{q}^{n}) \leftarrow vk\) is the verification key and where the ciphertext \( CT_b \) is within negligible trace distance of

\[
\sum_{s \in \mathbb{Z}_{q}^{n}} \sum_{e \in \mathbb{Z}_{q}^{m+1}} \omega_{q}(e) \omega_{q}^{-1}(s, y) |sa + e + (0, \ldots, 0, m_b \cdot [q/2]) (\text{mod } q)|
\]  

(16)

Let \( \beta \in (0, 1) \) be such that \( \alpha / \beta = \lambda^{\omega(1)} \). From Theorem 5 it follows that, under the (decisional) LWE_{n,q,\beta} assumption, the quantum ciphertext \( CT_b \) is computationally indistinguishable from the state

\[
\sum_{u \in \mathbb{Z}_{q}^{n+1}} \omega_{q}^{-1}(u, x_0) |u\rangle, \quad x_0 \sim D_{A_{\lambda}}^{\lambda}(\lambda, \frac{1}{\sqrt{m}}).
\]

(17)

Because the state in Eq. (20) is completely independent of \( b \in \{0, 1\} \), it follows that

\[
\text{Adv}_{\Sigma, A}(\lambda) := |\text{Pr}[\text{Exp}^{\text{ind-cpa}}_{\Sigma, A, \lambda}(0) = 1] - \text{Pr}[\text{Exp}^{\text{ind-cpa}}_{\Sigma, A, \lambda}(1) = 1]| \leq \text{negl}(\lambda).
\]

This proves the claim.

IND-CPA-CD security of DualPKE_{CD}. In this section, we prove that our public-key encryption scheme DualPKE_{CD} in Construction 1 satisfies the notion of certified deletion security assuming the Strong Gaussian-Collapsing (SGC) Conjecture (see Conjecture 5.2). This is a strengthening of the Gaussian-collapsing property which we proved under the (decisional) LWE assumption (see Theorem 4).

**Theorem 7.** Let \( n \in \mathbb{N} \) and \( q \geq 2 \) be a prime modulus with \( m \geq 2n \log q \), each parameterized by \( \lambda \in \mathbb{N} \). Let \( \alpha \) be a ratio with \( \sqrt{8(m + 1)} \leq \frac{1}{\alpha} \leq \frac{q}{\sqrt{8(m + 1)}} \). Then, the scheme DualPKE_{CD} in Construction 1 is IND-CPA-CD-secure assuming the Strong Gaussian-Collapsing property SGC_{n,m+1,q,\beta} from Conjecture 5.2.
Proof. Let $\Sigma = \text{DualPKE}_{\text{CD}}$. We need to show that, for any QPT adversary $\mathcal{A}$, it holds that

$$\text{Adv}_{\Sigma, \mathcal{A}}^{\text{pk-cert-del}}(\lambda) := |\Pr[\text{Exp}_{\Sigma, \mathcal{A}}^{\text{pk-cert-del}}(0) = 1] - \Pr[\text{Exp}_{\Sigma, \mathcal{A}}^{\text{pk-cert-del}}(1) = 1]| \leq \text{negl}(\lambda).$$

We consider the following sequence of hybrids:

$\mathbf{H}_0$: This is the experiment $\text{Exp}_{\Sigma, \mathcal{A}}^{\text{pk-cert-del}}(0)$ between $\mathcal{A}$ and a challenger:

1. The challenger samples a random matrix $\bar{A} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n \times m}$ and a vector $\bar{x} \overset{\$}{\leftarrow} \{0, 1\}^m$ and chooses $A = [\bar{A}]\bar{x} \pmod{q}]$. The challenger chooses the secret key $sk \leftarrow (-\bar{x}, 1) \in \mathbb{Z}_q^{m+1}$ and the public key $pk \leftarrow A \in \mathbb{Z}_q^{n \times (m+1)}$.
2. $\mathcal{A}$ sends a distinct plaintext pair $(m_0, m_1) \in \{0, 1\} \times \{0, 1\}$ to the challenger. (Note: Without loss of generality, we can just assume that $m_0 = 0$ and $m_1 = 1$).
3. The challenger runs $(|\psi_y\rangle, y) \leftarrow \text{GenPrimal}(A, 1/\alpha)$ in Algorithm 2, and outputs
   $$\left(\nu_k \leftarrow (A \in \mathbb{Z}_q^{n \times (m+1)}, y \in \mathbb{Z}_q^n), \quad |\text{CT}_0\rangle \leftarrow |\psi_y\rangle\right).$$

4. At some point in time, $\mathcal{A}$ returns a certificate $\pi$ to the challenger.
5. The challenger verifies $\pi$ and outputs $T$, if $A \cdot \pi = y \pmod{q}$ and $||\pi|| \leq \sqrt{m+1}/\sqrt{2\alpha}$, and output $\perp$, otherwise. If $\pi$ passes the test with outcome $T$, the challenger sends $sk$ to $\mathcal{A}$.
6. $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$, which is also the output of the experiment.

$\mathbf{H}_1$: This is same experiment as in $\mathbf{H}_0$, except that (in Step 3) the challenger prepares the ciphertext in the Fourier basis rather than the standard basis. In other words, $\mathcal{A}$ receives the pair

$$\left(\nu_k \leftarrow (A \in \mathbb{Z}_q^{n \times (m+1)}, y \in \mathbb{Z}_q^n), \quad |\text{CT}_0\rangle \leftarrow \text{FT}_q |\psi_y\rangle\right).$$

$\mathbf{H}_2$: This is the experiment $\text{StrongGaussCollapseExp}_{\mathcal{H}, \mathcal{D}, \lambda}(0)$ in Conjecture 5.2:

1. The challenger samples a random matrix $\bar{A} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n \times m}$ and a vector $\bar{x} \overset{\$}{\leftarrow} \{0, 1\}^m$ and chooses $A = [\bar{A}]\bar{x} \pmod{q}]$. The challenger chooses $t = (-\bar{x}, 1) \in \mathbb{Z}_q^{m+1}$.
2. The challenger runs $(|\tilde{\psi}_y\rangle, y) \leftarrow \text{GenDual}(A, 1/\alpha)$ in Algorithm 1, where $y \in \mathbb{Z}_q^n$, and sends the triplet $(|\tilde{\psi}_y\rangle, A, y)$ to the adversary $\mathcal{A}$.
3. At some point in time, $\mathcal{A}$ returns a certificate $\pi$ to the challenger.
4. The challenger verifies $\pi$ and outputs $T$, if $A \cdot \pi = y \pmod{q}$ and $||\pi|| \leq \sqrt{m+1}/\sqrt{2\alpha}$, and output $\perp$, otherwise. If $\pi$ passes the test with outcome $T$, the challenger sends $t$ to $\mathcal{A}$.
5. $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$, which is also the output of the experiment.

$\mathbf{H}_3$: This is the experiment $\text{StrongGaussCollapseExp}_{\mathcal{H}, \mathcal{D}, \lambda}(1)$ in Conjecture 5.2; it is the same as $\mathbf{H}_2$, except that the state $|\tilde{\psi}_y\rangle$ (in Step 2) is measured in the computational basis before it is sent to $\mathcal{A}$.

$\mathbf{H}_4$: This is same experiment as $\mathbf{H}_3$, except that (in Step 2) the challenger additionally applies the Pauli operator $\mathbb{Z}_q^{(0, \ldots, 0, 1/2)}$ to the state $|\tilde{\psi}_y\rangle$ before it is measured in the computational basis.
$H_5$: This is same experiment as $H_4$, except that (in Step 2) $A$ receives the triplet
\[(Z_q^{(0,\ldots,0,\frac{2}{q})}|\hat{\psi}_y\rangle, \ A \in \mathbb{Z}_q^n \times (m+1), \ y \in \mathbb{Z}_q^n).\]

$H_6$: This is same experiment as $H_5$, except that (in Step 2) the challenger prepares the quantum state
\[Z_q^{(0,\ldots,0,\frac{2}{q})}|\hat{\psi}_y\rangle\] in the (inverse) Fourier basis instead. In other words, $A$ receives the triplet
\[(\text{FT}_q^+Z_q^{(0,\ldots,0,\frac{2}{q})}|\hat{\psi}_y\rangle, \ A \in \mathbb{Z}_q^n \times (m+1), \ y \in \mathbb{Z}_q^n).\]

$H_7$: This is the experiment $\text{Exp}^\text{pk-cert-del}_{\Sigma, A, \lambda}(1)$.

We now show that the hybrids are indistinguishable.

Claim 2.
\[
\Pr[\text{Exp}^\text{pk-cert-del}_{\Sigma, A, \lambda}(0) = 1] = \Pr[H_1 = 1].
\]

Proof. Without loss of generality, we can assume that $A$ applies the inverse Fourier transform immediately upon receiving the quantum ciphertext. Therefore, the success probabilities are identical in $H_0$ and $H_1$.

Claim 3.
\[
\Pr[H_1 = 1] = \Pr[H_2 = 1].
\]

Proof. Because the challenger in $H_1$ always sends the ciphertext $|CT_0\rangle$ corresponding to $m_0 = 0$ to the adversary $A$, the two hybrids $H_1$ and $H_2$ are identical.

Claim 4. Under the Strong Gaussian-Collapsing property $\text{SGC}_{n,m+1,q,\frac{1}{n}}$, it holds that
\[
|\Pr[H_2 = 1] - \Pr[H_3 = 1]| \leq \text{negl}(\lambda).
\]

Proof. This follows directly from Conjecture 5.2.

Claim 5.
\[
\Pr[H_3 = 1] = \Pr[H_4 = 1].
\]

Proof. Because the challenger measures the state $|\hat{\psi}_y\rangle$ in Step 2 in the computational basis, applying the phase operator $Z_q^{(0,\ldots,0,\frac{2}{q})}$ before the measurement does not affect the measurement outcome.

Claim 6. Under the Strong Gaussian-Collapsing property $\text{SGC}_{n,m+1,q,\frac{1}{n}}$, it holds that
\[
|\Pr[H_4 = 1] - \Pr[H_5 = 1]| \leq \text{negl}(\lambda).
\]

Proof. This follows from Conjecture 5.2 since, without loss of generality, we can assume that $A$ applies the phase operator $Z_q^{(0,\ldots,0,\frac{2}{q})}$ immediately upon receiving the state $|\hat{\psi}_y\rangle$.

Claim 7.
\[
\Pr[H_5 = 1] = \Pr[H_6 = 1].
\]

Proof. Without loss of generality, we can assume that $A$ applies the Fourier transform immediately upon receiving the state $Z_q^{(0,\ldots,0,\frac{2}{q})}|\hat{\psi}_y\rangle$. Therefore, the success probabilities are identical in $H_5$ and $H_6$.  

42
Claim 8.

\[ |\Pr[H_6 = 1] - \Pr[\text{Exp}_{\Sigma, A, \lambda}^{\text{pk-cert-del}}(1) = 1]| \leq \text{negl}(\lambda). \]

Proof. From Lemma 6, we have \( FT_q^* \psi y = Z_q^* FT_q \), for all \( v \in \mathbb{Z}_q^m \). Hence, in \( H_6 \), we can instead assume that the challenger runs \((|\psi y \rangle, y) \leftarrow \text{GenPrimal}(A, 1/\alpha) \) in Algorithm 2 and sends the following to \( A \):

\[
(vk \leftarrow (A \in \mathbb{Z}_q^{n \times (m+1)}, y \in \mathbb{Z}_q^n), \ \text{CT}_1) \leftarrow X_q^{(0, \ldots, 0, \lfloor \frac{q}{2} \rfloor)} |\psi y \rangle.
\]

From Corollary 1, we have that \( FT_q^* Z_q^* |\psi y \rangle \) and \( X_q^y |\psi y \rangle \) are within negligible trace distance, for all \( v \in \mathbb{Z}_q^m \).

Because the challenger in \( H_7 \) always sends the ciphertext \( |\text{CT}_1 \rangle \) corresponding to \( m_1 = 1 \) to the adversary \( A \), it follows that the distinguishing advantage between \( H_6 \) and \( H_7 = \text{Exp}_{\Sigma, A, \lambda}^{\text{pk-cert-del}}(1) \) is negligible. \( \square \)

Because the hybrids \( H_0 \) and \( H_7 \) are indistinguishable, this implies that

\[ \text{Adv}_{\Sigma, A}^{\text{pk-cert-del}}(\lambda) \leq \text{negl}(\lambda). \]

\( \square \)

Next, we show how to extend our Dual-Regev PKE scheme with certified deletion in Construction 1 to a fully homomorphic encryption scheme of the same type.

8 Fully Homomorphic Encryption with Certified Deletion

In this section, we formalize the notion of homomorphic encryption with certified deletion which enables an untrusted quantum server to compute on encrypted data and, if requested, to simultaneously prove data deletion to a client. We also provide several notions of certified deletion security.

8.1 Definition

We begin with the following definition.

Definition 23 (Homomorphic encryption with certified deletion). A homomorphic encryption scheme with certified deletion is a tuple \( \text{HECD} = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval}, \text{Del}, \text{Vrfy}) \) of QPT algorithms (in the security parameter \( \lambda \in \mathbb{N} \)), a key generation algorithm \( \text{KeyGen} \), an encryption algorithm \( \text{Enc} \), a decryption algorithm \( \text{Dec} \), an evaluation algorithm \( \text{Eval} \), a deletion algorithm \( \text{Del} \), and a verification algorithm \( \text{Vrfy} \).

\[ \text{KeyGen}(1^\lambda) \rightarrow (pk, sk) : \text{takes as input } 1^\lambda \text{ and outputs a public key } pk \text{ and secret key } sk. \]

\[ \text{Enc}(pk, x) \rightarrow (vk, \text{CT}) : \text{takes as input the public key } pk \text{ and a plaintext } x \in \{0,1\}, \text{ and outputs a classical verification key } vk \text{ together with a quantum ciphertext } CT. \]

\[ \text{Dec}(sk, CT) \rightarrow x' \text{ or } \perp : \text{takes as input a key } sk \text{ and ciphertext } CT, \text{ and outputs } x' \in \{0,1\} \text{ or } \perp. \]

\[ \text{Eval}(C, CT, pk) \rightarrow \hat{CT} : \text{takes as input a key } pk \text{ and applies a circuit } C : \{0,1\}^n \rightarrow \{0,1\} \text{ to a product of quantum ciphertexts } CT = CT_1 \otimes \cdots \otimes CT_n \text{ resulting in a state } \hat{CT}. \]

\[ \text{Del}(CT) \rightarrow \pi : \text{takes as input a ciphertext } CT \text{ and outputs a classical certificate } \pi. \]

\[ \text{Vrfy}(vk, \pi) \rightarrow \top \text{ or } \perp : \text{takes as input a key } vk \text{ and certificate } \pi, \text{ and outputs } \top \text{ or } \perp. \]
We remark that we frequently overload the functionality of the encryption and decryption procedures by allowing both procedures to take multi-bit messages as input, and to generate or decrypt a sequence of quantum ciphertexts bit-by-bit.

**Definition 24** (Compactness and full homomorphism). A homomorphic encryption scheme with certified deletion $\text{HE}_{\text{CD}} = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval}, \text{Del}, \text{Vrfy})$ is fully homomorphic if, for any efficiently (in $\lambda \in \mathbb{N}$) computable circuit $C : \{0, 1\}^L \rightarrow \{0, 1\}$ and any set of inputs $x = (x_1, \ldots, x_L) \in \{0, 1\}^L$, it holds that

$$\Pr \left[ \text{Dec}(sk, CT) \neq C(x_1, \ldots, x_L) \middle| \begin{array}{l}
(pk, sk) \leftarrow \text{KeyGen}(1^\lambda) \\
(vk, CT) \leftarrow \text{Enc}(pk, x) \\
CT \leftarrow \text{Eval}(C, CT, pk)
\end{array} \right] \leq \text{negl}(\lambda).$$

We say that a fully homomorphic encryption scheme with certified deletion ($\text{FHE}_{\text{CD}}$) is compact if its decryption circuit is independent of the circuit $C$. The scheme is leveled fully homomorphic if it takes $1^L$ as an additional input for its key generation procedure and can only evaluate depth $L$ Boolean circuits.

**Definition 25** (Correctness of verification). A homomorphic encryption scheme with certified deletion $\text{HE}_{\text{CD}} = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval}, \text{Del}, \text{Vrfy})$ has correctness of verification if the following property holds for any integer $\lambda \in \mathbb{N}$ and any set of inputs $x = (x_1, \ldots, x_L) \in \{0, 1\}^L$

$$\Pr \left[ \text{Vrfy}(vk, \pi) = \bot \middle| \begin{array}{l}
(pk, sk) \leftarrow \text{KeyGen}(1^\lambda) \\
(vk, CT) \leftarrow \text{Enc}(pk, x) \\
\pi \leftarrow \text{Del}(CT)
\end{array} \right] \leq \text{negl}(\lambda).$$

Recall that a fully homomorphic encryption scheme with certified deletion enables an untrusted quantum server to compute on encrypted data and to also prove data deletion to a client. In this context, it is desirable for the client to be able to extract (i.e., to decrypt) the outcome of the computation without irrevocably affecting the ability of the server to later prove deletion. We use the following definition.

**Definition 26** (Extractable FHE scheme with certified deletion). A fully homomorphic encryption scheme with certified deletion $\Sigma = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval}, \text{Extract}, \text{Del}, \text{Vrfy})$ is called extractable, if

- $\text{Eval}(C, CT_1, \ldots, CT_L, pk)$ additionally outputs a circuit transcript $t_C$ besides $CT$;
- $\text{Extract}(S(q, t_C), R(sk))$ is an interactive protocol between a sender $S$ (which takes as input a state $q$ and a circuit transcript $t_C$) and a receiver $R$ (which takes as input a key $sk$) with the property that, once the protocol is complete, $S$ obtains a state $\tilde{q}$ and $R$ obtains a bit $y \in \{0, 1\}$.

such that for any efficiently computable circuit $C : \{0, 1\}^L \rightarrow \{0, 1\}$ of depth $L$ and any input $x \in \{0, 1\}^L$

$$\Pr \left[ y \neq C(x_1, \ldots, x_L) \middle| \begin{array}{l}
(pk, sk) \leftarrow \text{KeyGen}(1^\lambda, 1^L) \\
(vk, CT) \leftarrow \text{Enc}(pk, x) \\
(CT, t_C) \leftarrow \text{Eval}(C, CT, pk) \\
\tilde{q} \leftarrow \text{Extract}(S(\tilde{q}, t_C), R(sk))
\end{array} \right] \leq \text{negl}(\lambda),$$

and

$$\Pr \left[ \text{Vrfy}(vk, \pi) = \bot \middle| \begin{array}{l}
(pk, sk) \leftarrow \text{KeyGen}(1^\lambda, 1^L) \\
(vk, CT) \leftarrow \text{Enc}(pk, x) \\
(CT, t_C) \leftarrow \text{Eval}(C, CT, pk) \\
\tilde{q} \leftarrow \text{Extract}(S(\tilde{q}, t_C), R(sk)) \\
\pi \leftarrow \text{Del}(\tilde{q})
\end{array} \right] \leq \text{negl}(\lambda).$$

**Remark** (Compactness of an extractable FHE scheme). Our notion of an extractable FHE scheme with certified deletion in Definition 26 requires the evaluator to keep a transcript of the circuit that is being applied, which at first sight seems to violate the usual notion of compactness in Definition 24. However, the action of the decryptor during the interactive protocol Extract is still independent of the circuit that is being applied, and so it is possible to recover an analogous form of compactness as before.
8.2 Certified deletion security

Our notion of certified deletion security for homomorphic encryption (HE) schemes is similar to the notion of IND-CPA-CD security for public-key encryption schemes in Definition 22.

**Definition 27 (Certified deletion security for HE).** Let \( \Sigma = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval}, \text{Del}, \text{Vrfy}) \) be a homomorphic encryption scheme with certified deletion and let \( A \) be a QPT adversary. We define the security experiment \( \text{Exp}^{\text{he-cert-del}}_{\Sigma, A, \lambda}(b) \) between \( A \) and a challenger as follows:

1. The challenger generates a pair \( (pk, sk) \leftarrow \text{KeyGen}(1^\lambda) \), and sends \( pk \) to \( A \).
2. \( A \) sends a distinct plaintext pair \( (m_0, m_1) \in \{0, 1\}^\ell \times \{0, 1\}^\ell \) to the challenger.
3. The challenger computes \( (vk, CT_b) \leftarrow \text{Enc}(pk, m_b) \), and sends \( |CT_b\rangle \) to \( A \).
4. At some point in time, \( A \) sends a certificate \( \pi \) to the challenger.
5. The challenger computes \( \text{Vrfy}(vk, \pi) \) and sends \( sk \) to \( A \), if the output is 1, and 0 otherwise.
6. \( A \) outputs a guess \( b' \in \{0, 1\} \), which is also the output of the experiment.

We say that the scheme \( \Sigma \) is IND-CPA-CD-secure if, for any QPT adversary \( A \), that
\[
\text{Adv}^{\text{he-cert-del}}_{\Sigma, A}(\lambda) := \left| \Pr[\text{Exp}^{\text{pk-cert-del}}_{\Sigma, A, \lambda}(0) = 1] - \Pr[\text{Exp}^{\text{he-cert-del}}_{\Sigma, A, \lambda}(1) = 1] \right| \leq \text{negl}(\lambda).
\]

9 Dual-Regev Fully Homomorphic Encryption with Certified Deletion

In this section, we describe the main result of this work. We introduce a protocol that allows an untrusted quantum server to perform homomorphic operations on encrypted data, and to simultaneously prove data deletion to a client. Our FHE scheme with certified deletion supports the evaluation of polynomial-sized Boolean circuits composed entirely of NAND gates (see Figure 4) – an assumption we can make without loss of generality, since the NAND operation is universal for classical computation. Note that, for \( a, b \in \{0, 1\} \), the logical NOT-AND (NAND) operation is defined by
\[
\text{NAND}(a, b) = \overline{a \land b} = 1 - a \cdot b.
\]

Recall also that a Boolean circuit with input \( x \in \{0, 1\}^n \) is a directed acyclic graph \( G = (V, E) \) in which each node in \( V \) is either an input node (corresponding to an input bit \( x_i \)), an AND (\( \land \)) gate, an OR (\( \lor \)) gate, or a NOT (\( \neg \)) gate. We can naturally identify a Boolean circuit with a function \( f : \{0, 1\}^n \rightarrow \{0, 1\} \) which it computes. Due to the universality of the NAND operation, we can represent every Boolean circuit (and the function it computes) with an equivalent circuit consisting entirely of NAND gates. In Figure 5, we give an example of a Boolean circuit composed of three NAND gates that takes as input a string \( x \in \{0, 1\}^4 \).
Figure 5: A Boolean circuit C made up of three NAND gates which takes as input a binary string of the form $x \in \{0,1\}^4$. The top-most NAND gate is the designated output node with outcome $C(x) \in \{0,1\}$.

### 9.1 Construction

In this section, we describe our fully homomorphic encryption scheme with certified deletion. In order to define our construction, we require a so-called flattenning operation first introduced by Gentry, Sahai and Waters [GSW13] in the context of homomorphic encryption and is also featured in the Dual-Regev FHE scheme of Mahadev [Mah18]. Let $n \in \mathbb{N}, q \geq 2$ be a prime modulus and $m \geq 2n \log q$. We define a linear operator $G \in \mathbb{Z}_q^{(m+1) \times N}$ called the gadget matrix, where $N = (n + 1) \cdot \lceil \log q \rceil$. The operator $G$ converts a binary representation of a vector back to its original vector representation over the ring $\mathbb{Z}_q$. More precisely, for any binary vector $\mathbf{a} = (a_{1,0}, \ldots, a_{1,l-1}, \ldots, a_{m+1,0}, \ldots, a_{m+1,l-1})$ of length $N$ with $\ell = \lceil \log q \rceil$, the matrix $G$ produces a vector in $\mathbb{Z}_q^{m+1}$ as follows:

\[
G(\mathbf{a}) = \left( \sum_{j=0}^{\lceil \log q \rceil - 1} 2^j \cdot a_{1,j}, \ldots, \sum_{j=0}^{\lceil \log q \rceil - 1} 2^j \cdot a_{m+1,j} \right).
\tag{18}
\]

We also define the associated (non-linear) inverse operation $G^{-1}$ which converts a vector $\mathbf{a} \in \mathbb{Z}_q^{m+1}$ to its binary representation in $\{0,1\}^N$. In other words, we have that $G^{-1} \cdot G = \mathbb{I}$ acts as the identity operation.

Our (leveled) FHE scheme with certified deletion is based on the (leveled) Dual-Regev FHE scheme introduced by Mahadev [Mah18] which is a variant of the LWE-based FHE scheme proposed by Gentry, Sahai and Waters [GSW13]. We base our choice of parameters on the aforementioned two works.

Let us first recall the Dual-Regev FHE scheme below.

**Construction 2** (Dual-Regev leveled FHE). Let $\lambda \in \mathbb{N}$ be the security parameter. The Dual-Regev leveled FHE scheme $\text{DualFHE} = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval})$ consists of the following PPT algorithms:

- **KeyGen**(1$^\lambda$) $\rightarrow$ (pk, sk) : sample a uniformly random matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and vector $\bar{x} \leftarrow \{0,1\}^m$ and let $\mathbf{A} = [\mathbf{A} | \check{\mathbf{A}} \cdot \bar{x} \pmod{q}]^T$. Output (pk, sk), where $\text{pk} = \mathbf{A} \in \mathbb{Z}_q^{(m+1) \times n}$ and $\text{sk} = (-\bar{x}, 1) \in \mathbb{Z}_q^{m+1}$.

- **Enc**(pk, x) : to encrypt $x \in \{0,1\}$, parse $\mathbf{A} \in \mathbb{Z}_q^{(m+1) \times n}$ $\leftarrow$ pk, sample $\mathbf{S} \leftarrow \mathbb{Z}_q^{n \times N}$ and $\mathbf{E} \sim D_{\mathbb{Z}_q^{(m+1) \times N}, a_\lambda}$ and output $\text{CT} = \mathbf{A} \cdot \mathbf{S} + \mathbf{E} + x \cdot G \pmod{q} \in \mathbb{Z}_q^{(m+1) \times N}$, where $G$ is the gadget matrix in Eq. (18).

- **Eval**(C, CT) : apply the circuit $C$ composed of NAND gates on a ciphertext tuple CT as follows:
• parse the ciphertext tuple as \((CT_1, \ldots, CT_i) \leftarrow CT\).
• repeat for every NAND gate in \(C\): to apply a NAND gate on a ciphertext pair \((CT_i, CT_j)\), parse matrices \(C_i \leftarrow CT_i\) and \(C_j \leftarrow CT_j\) with \(C_i, C_j \in \mathbb{Z}_q^{(m+1) \times N}\) and generate

\[
C_{ij} = G - C_i \cdot G^{-1}(C_j) \pmod{q}.
\]

Let \(CT_{ij} \leftarrow C_{ij}\) denote the outcome ciphertext.

\[
\text{Dec}(sk, CT) : \text{parse } C \in \mathbb{Z}_q^{(m+1) \times N} \leftarrow CT \text{ and compute } c = sk^T \cdot c_N \in \mathbb{Z} \cap (-\frac{q}{2}, \frac{q}{2}], \text{ where } c_N \in \mathbb{Z}_q^{n+1} \text{ is the } N\text{-th column of } C, \text{ and then output } 0, \text{ if } c \text{ is closer to } 0 \text{ than to } \left\lfloor \frac{q}{2} \right\rfloor, \text{ and output } 1, \text{ otherwise.}
\]

The Dual-Regev FHE scheme supports the homomorphic evaluation of a NAND gate in the following sense. If \(CT_0\) and \(CT_1\) are ciphertexts that encrypt two bits \(x_0\) and \(x_1\), respectively, then the resulting outcome \(CT = G - CT_0 \cdot G^{-1}(CT_1) \pmod{q}\) is an encryption of \(\text{NAND}(x_0, x_1) = 1 - x_0 \cdot x_1\), where \(G\) is the gadget matrix that converts a binary representation of a vector back to its original representation over the ring \(\mathbb{Z}_q\). Moreover, the new ciphertext CT maintains the form of an LWE sample with respect to the same public key \(pk\), albeit for a new LWE secret and a new (non-necessarily Gaussian) noise term of bounded magnitude. This property is crucial, as knowledge of the secret key \(sk\) (i.e., a short trapdoor vector) still allows for the decryption of the ciphertext CT once a NAND gate has been applied.

The following result is implicit in the work of Mahadev [Mah18, Theorem 5.1].

**Theorem 8** ([Mah18]). Let \(\lambda \in \mathbb{N}\) be the security parameter. Let \(n \in \mathbb{N}\), let \(q \geq 2\) be a prime modulus and \(m \geq 2n \log q\). Let \(N = (n+1) \cdot \lceil \log q \rceil\) be an integer and let \(L\) be an upper bound on the depth of the polynomial-sized Boolean circuit which is to be evaluated. Let \(\alpha \in (0, 1)\) be a ratio such that

\[
2\sqrt{n} \leq \alpha q \leq \frac{q}{4(m+1) \cdot N \cdot (N+1)^L}.
\]

Then, the scheme in Construction 2 is an IND-CPA-secure leveled fully homomorphic encryption scheme under the LWE\(_{n,q,\alpha q}\) assumption.

Note that the Dual-Regev FHE scheme is leveled in the sense that an apriori upper bound \(L\) on the NAND-depth of the circuit is required to set the parameters appropriately. We remark that a proper (non-leveled) FHE scheme can be obtained under an additional circular security assumption [BV11].

The leveled Dual-Regev FHE scheme inherits a crucial property from its public-key counterpart. Namely, in contrast to the FHE scheme in [GSW13], the ciphertext takes the form of a regular sample from the LWE distribution together with an additive shift \(x \cdot G\) that depends on the plaintext \(x \in \{0, 1\}\). In particular, if a Boolean circuit \(C\) of polynomial NAND-depth \(L\) is applied to the ciphertext corresponding to a plaintext \(x \in \{0, 1\}^L\) in Construction 2, then the resulting final ciphertext is of the form \(A \cdot S + E + C(x)G\), where \(S \in \mathbb{Z}_q^{n \times N}, E \in \mathbb{Z}_q^{(m+1) \times N}\) and \(\|E\|_{\infty} \leq \alpha q \sqrt{m+1}N \cdot (N+1)^L\) (see [GSW13] for details). Choosing \(1/\alpha\) to be sub-exponential in \(N\) as in [GSW13], we can therefore allow for homomorphic computations of arbitrary polynomial-sized Boolean circuits of NAND-depth at most \(L\). It is easy to see that the decryption procedure of the leveled Dual-Regev FHE scheme is successful as long as the cumulative error \(E\) satisfies the condition \(\|E\|_{\infty} \leq \frac{q}{4\sqrt{(m+1)N}}\).

This property is essential as it allows us to extend Dual-Regev PKE scheme with certified deletion towards a leveled FHE scheme, which we denote by FHE\(_{CD}\). Using Gaussian coset states, we can again encode Dual-Regev ciphertexts for the purpose of certified deletion while simultaneously preserving their cryptographic functionality.
**Dual-Regev leveled FHE with certified deletion.** Let us now describe our (leveled) FHE scheme with certified deletion. We base our choice of parameters on the Dual-Regev FHE scheme of Mahadev [Mah18] which is a variant of the scheme due to Gentry, Sahai and Waters [GSW13].

**Parameters.** Let $\lambda \in \mathbb{N}$ be the security parameter and let $n \in \mathbb{N}$. Let $L$ be an upper bound on the depth of the polynomial-sized Boolean circuit which is to be evaluated. We choose the following set of parameters for the Dual-Regev leveled FHE scheme (each parameterized by the security parameter $\lambda$).

- a prime modulus $q \geq 2$.
- an integer $m \geq 2n \log q$.
- an integer $N = (n + 1) \cdot \lceil \log q \rceil$.
- a noise ratio $\alpha \in (0, 1)$ such that
  \[ \frac{\sqrt{8(m + 1)N}}{q} \leq \frac{q}{\sqrt{8(m + 1) \cdot N \cdot (N + 1)^2}}. \]

**Construction 3** (Dual-Regev leveled FHE scheme with certified deletion). Let $\lambda \in \mathbb{N}$ be a parameter and DualFHE = (KeyGen, Enc, Dec, Eval) be the scheme in Construction 2. The Dual-Regev (leveled) FHE scheme DualFHE_{CD} = (KeyGen, Enc, Dec, Eval, Del, Vrfy) with certified deletion is defined by:

**KeyGen($1^\lambda$) → (pk, sk) : generate** (pk, sk) ← DualFHE.KeyGen($1^\lambda$) and output (pk, sk).

**Enc(pk, x) → (vk, |CT|) : to encrypt a bit** $x \in \{0, 1\}$, parse $A \in \mathbb{Z}_q^{(m + 1) \times n}$ ← pk and, for $i \in [N]$, run $(|\psi_{yi}|, y_i) \leftarrow \text{GenPrimal}(A^T, 1/\alpha)$ in Algorithm 2, where $y_i \in \mathbb{Z}_q^n$, and output the pair

\[
\left( vk \leftarrow (A \in \mathbb{Z}_q^{(m + 1) \times n}, (y_1, \ldots, y_N) \in \mathbb{Z}_q^{n \times N}), \ \ |CT| \leftarrow x^g |\psi_{y_1}| \otimes \cdots \otimes x^g |\psi_{y_N}| \right),
\]

where $(g_1, \ldots, g_N)$ are the rows of the gadget matrix $G \in \mathbb{Z}_q^{(m + 1) \times N}$ in Eq. (18).

**Eval(C, |CT|) → (|\widetilde{CT}|, t_C) : apply the Boolean circuit** $C$ composed of NAND gates to the ciphertext $|CT|$ in system $C_{in} = C_1 \cdots C_\ell$ as follows: For every gate $\text{NAND}_{ij}$ in the circuit $C$ between a ciphertext pair in systems $C_i$ and $C_j$, repeat the following two steps:

- apply $U_{\text{NAND}}$ from Definition 28 to systems $C_i C_j$ of the ciphertext CT by appending an auxiliary system $C_{ij}$. This results in a new ciphertext state $CT$ which contains the additional system $C_{ij}$.
- add the gate $\text{NAND}_{ij}$ to the circuit transcript $t_C$.

**Output** $(|\widetilde{CT}|, t_C)$, where $|\widetilde{CT}|$ is the final post-evaluation state in systems $C_{in} C_{aux} C_{out}$ and

- $C_{in} = C_1 \cdots C_\ell$ denotes the initial ciphertext systems of $|CT_1| \otimes \cdots \otimes |CT_\ell|$.
- $C_{aux}$ denotes all intermediate auxiliary ciphertext systems.
- $C_{out}$ denotes the final ciphertext system corresponding to the output of the circuit $C$.

**Dec(sk, |CT|) → \{0, 1\}^\mu or ⊥ : measure the ciphertext** $|CT|$ in the computational basis to obtain an outcome $C$ and output $x' \leftarrow \text{DualFHE.Dec}(sk, C)$.

48
Definition 28 (Homomorphic NAND gate). Let $q \geq 2$ be a modulus, and let $m$ and $N$ be integers. Let $X, Y, Z \in \mathbb{Z}_q^{(m+1) \times N}$ be arbitrary matrices. We define the homomorphic NAND gate as the unitary

$$U_{\text{NAND}} : \ket{X} \otimes \ket{Y} \otimes \ket{Z} \rightarrow \ket{X} \otimes \ket{Y} \otimes \ket{Z} + G \cdot G^{-1}(Y) \pmod{q},$$

where $G \in \mathbb{Z}_q^{(m+1) \times N}$ is the gadget matrix in Eq. (18).

To illustrate the action of our homomorphic NAND gate, we consider a simple example.
Example. Consider a pair of two ciphertexts $|\text{CT}_i\rangle \otimes |\text{CT}_j\rangle$ which encrypt two bits $x_i, x_j \in \{0, 1\}$ as in Construction 3. Let $U_{\text{NAND}_ij}$ denote the homomorphic NAND gate applied to systems $C_i$ and $C_j$. Then,

$$U_{\text{NAND}_ij} : |\text{CT}_i\rangle_{C_i} \otimes |\text{CT}_j\rangle_{C_j} \otimes |0\rangle_{C_{ij}} \rightarrow |\text{CT}_{ij}\rangle_{C_iC_jC_{ij}}.$$ 

Here, $|\text{CT}_{ij}\rangle$ is the resulting ciphertext in systems $C_iC_jC_{ij}$. Note that $U_{\text{NAND}_ij}$ is reversible in the sense that

$$U_{\text{NAND}_ij}^t : |\text{CT}_{ij}\rangle_{C_iC_jC_{ij}} \rightarrow |\text{CT}_i\rangle_{C_i} \otimes |\text{CT}_j\rangle_{C_j} \otimes |0\rangle_{C_{ij}}.$$ 

Let us now analyze how $U_{\text{NAND}}$ acts on the basis states of a pair of ciphertexts $|\text{CT}_i\rangle \otimes |\text{CT}_j\rangle$ that encode LWE samples as in Construction 3. In the following, $E_i, E_j \sim D_{\mathbb{Z}/q}^m$ have a (truncated) discrete Gaussian distribution as part of the superposition. Then,

$$U_{\text{NAND}_ij} : |\text{AS}_i + E_i + x_i\text{G}\rangle_{C_i} \otimes |\text{AS}_j + E_j + x_j\text{G}\rangle_{C_j} \otimes |0\rangle_{C_{ij}} \rightarrow |\text{AS}_i + E_i + x_i\text{G}\rangle_{C_i} \otimes |\text{AS}_j + E_j + x_j\text{G}\rangle_{C_j} \otimes |\text{AS}_i + E_j + (1 - x_i)x_j\text{G}\rangle_{C_{ij}},$$

where introduced the following matrices

$$S_{ij} := -S_i \cdot \text{G}^{-1}(\text{AS}_j + E_j + x_j\text{G}) - x_iS_i \pmod{q},$$

$$E_{ij} := -E_i \cdot \text{G}^{-1}(\text{AS}_j + E_j + x_j\text{G}) - x_iE_i \pmod{q}.$$

Because the initial error terms have the property that $\|E_i\|_{\infty}, \|E_j\|_{\infty} \leq aq\sqrt{(m+1)N/2}$, it follows that the resulting error after a single NAND gate is at most (see also [GSW13, Mah18] for more details)

$$\|E_{ij}\|_{\infty} \leq aq\sqrt{\frac{(m+1)N}{2}} \cdot (N + 1).$$

In other words, the cumulative error term remains short relative to the modulus $q$ after every application of a homomorphic NAND gate, exactly as in the Dual-Regev FHE scheme of Mahadev [Mah18].

### 9.2 Rewinding lemma

Notice that the procedure DualFHECD.Eval in Construction 3 produces a highly entangled state since the unitary operation $U_{\text{NAND}}$ induces entanglement between the Gaussian noise terms. In the next lemma, we show that it is possible to *rewind* the evaluation procedure to be able to prove data deletion to a client.

#### Lemma 19 (Rewinding lemma).

Let $\lambda \in \mathbb{N}$ be the security parameter. Let $n \in \mathbb{N}$, let $q \geq 2$ be a prime modulus and $m \geq 2n \log q$. Let $N = (n+1) \cdot \lceil \log q \rceil$ be an integer and let $L$ be an upper bound on the depth of the polynomial-sized Boolean circuit which is to be evaluated. Let $\alpha \in (0, 1)$ be a ratio such that

$$\sqrt{8(m+1)N} \leq aq \leq \frac{q}{\sqrt{8(m+1) \cdot N \cdot (N+1)L}}.$$ 

Let DualFHECD = (KeyGen, Enc, Dec, Eval, Del, Vrfy) be the Dual-Regev (leveled) FHE scheme with certified deletion in Construction 3 and let $\Pi$ be the interactive protocol in Protocol 1. Then, the following holds for any parameter $\lambda \in \mathbb{N}$, plaintext $x \in \{0, 1\}^2$ and any polynomial-sized Boolean circuit $C$:
Figure 6: Homomorphic evaluation of a Boolean circuit $C$ composed entirely of three NAND gates. Here, the input is the quantum ciphertext $|CT_1\rangle \otimes |CT_2\rangle \otimes |CT_3\rangle \otimes |CT_4\rangle$ which corresponds to an encryption of the plaintext $x = (x_1, \ldots, x_4) \in \{0, 1\}^4$ as in Construction 3. The resulting ciphertext $|CT_{12,34}\rangle$ lives on a system $C_{in} = C_{1}C_{2}C_{3}C_{4}C_{12}C_{34}C_{12,34}$ of which the last system $C_{12,34}$ contains an encryption of $C(x) \in \{0, 1\}$.

After the interactive protocol $\Pi = \langle S(\tilde{|CT}\rangle, t_C), R(sk) \rangle$ between the sender $S$ and receiver $R$ is complete, the sender $S$ is in possession of a quantum state $\varrho$ in system $C_{in}$ that satisfies

$$||\varrho - |CT\rangle\langle CT||_{tr} \leq \text{negl}(\lambda),$$

where $(\tilde{|CT}\rangle, t_C) \leftarrow \text{DualFHE}_{\text{CD}}.\text{Eval}(C, |CT\rangle)$ is the post-evaluation state $\tilde{|CT\rangle}$ in systems $C_{in}C_{aux}C_{out}$ and where $|CT\rangle \leftarrow \text{DualFHE}_{\text{CD}}.\text{Enc}(pk, x)$ is the initial state for $(pk, sk) \leftarrow \text{DualFHE}_{\text{CD}}.\text{KeyGen}(1^\lambda)$.

Proof: Let $\lambda \in \mathbb{N}$, $x \in \{0, 1\}^\ell$ be a plaintext and $C$ be any Boolean circuit of NAND-depth $L = \text{poly}(\lambda)$. Let $(\tilde{|CT\rangle}, t_C) \leftarrow \text{DualFHE}_{\text{CD}}.\text{Eval}(C, |CT\rangle)$ be the post-evaluation state $\tilde{|CT\rangle}$ in systems $C_{in}C_{aux}C_{out}$ with circuit transcript $t_C$ and let $\varrho$ be the outcome of the interactive protocol $\Pi = \langle S(\tilde{|CT\rangle}, t_C), R(sk) \rangle$. Recall that, in Lemma 20, we established that there exists a negligible $\epsilon(\lambda)$ such that $\text{DualFHE}_{\text{Dec}_{sk}}$ decrypts system $C_{out}$ of $|CT\rangle$ with probability at least $1 - \epsilon$. By the "Almost As Good As New Lemma" (Lemma 1), performing the operation $U_{\text{DualFHE}_{\text{Dec}_{sk}}},$ measuring the ancillary register $M$ and rewinding the computation, results in a mixed state $\tilde{\varrho}$ that is within trace distance $\sqrt{\epsilon}$ of the post-evaluation state $|CT\rangle$. Notice that, by reversing the sequence $U_{t_C}$ of homomorphic NAND gates according to the transcript $t_C$
with respect to $|\tilde{C}T\rangle$, we recover the initial ciphertext $|CT\rangle \langle CT| = U_{tC}^\dagger |CT\rangle \langle CT| U_{tC}$ in system $C_{in}$. By definition, we also have that $q = U_{tC}^\dagger q U_{tC}$. Therefore,
\[
\|q - |CT\rangle \langle CT||_{tr} = \|U_{tC}^\dagger q U_{tC} - U_{tC}^\dagger |\tilde{C}T\rangle \langle \tilde{C}T| U_{tC}\|_{tr} = \|\tilde{q} - |\tilde{C}T\rangle \langle \tilde{C}T||_{tr} \leq \sqrt{\varepsilon(\lambda)},
\]
where we used that the trace distance is unitarily invariant. Since $\varepsilon(\lambda) = \text{negl}(\lambda)$, this proves the claim. \hfill \Box

**Proof of correctness.** Let us now verify the correctness of decryption and verification of Construction 3.

**Lemma 20 (Compactness and full homomorphism of DualFHECD).** Let $\lambda \in \mathbb{N}$ be the security parameter. Let $n \in \mathbb{N}$, let $q \geq 2$ be a prime and $m \geq 2n \log q$. Let $N = (n + 1) \cdot \lceil \log q \rceil$ and let $L$ be an upper bound on the depth of the polynomial-sized Boolean circuit which is to be evaluated. Let $\alpha \in (0, 1)$ be a ratio with
\[
\sqrt{8(m + 1)N} \leq \alpha q \leq \frac{q}{\sqrt{8(m + 1) \cdot N \cdot (N + 1)^L}}.
\]

Then, the scheme DualFHECD = (KeyGen, Enc, Dec, Eval, Del, Vrfy) in Construction 3 is a compact and fully homomorphic encryption scheme with certified deletion. In other words, for any efficiently (in $\lambda \in \mathbb{N}$) computable circuit $C : \{0, 1\}^\ell \rightarrow \{0, 1\}$ and any set of inputs $x = (x_1, \ldots, x_\ell) \in \{0, 1\}^\ell$, it holds that:
\[
\Pr \left[ \text{DualFHECD}\text{-Dec}(sk, |\tilde{C}T\rangle) \neq C(x_1, \ldots, x_\ell) \bigg| (pk, sk) \leftarrow \text{DualFHECD}\text{-KeyGen}(1^\lambda), (vk, CT) \leftarrow \text{DualFHECD}\text{-Enc}(pk, x) \bigg( |\tilde{C}T\rangle, t_C \bigg) \leftarrow \text{DualFHECD}\text{-Eval}(C, |\tilde{C}T\rangle, pk) \right] \leq \text{negl}(\lambda).
\]

**Proof.** Let $|CT\rangle$ be the ciphertext output by DualFHECD.Enc($pk, x$), where $x \in \{0, 1\}^\ell$ denotes the plaintext, and let $(|\tilde{C}T\rangle, t_C) \leftarrow \text{DualFHECD}\text{-Eval}(C, |\tilde{C}T\rangle)$ be the output of the evaluation procedure. Let us first consider the case when $t_C = \emptyset$, i.e. not a single NAND gate has been applied to the ciphertext. In this case, the claim follows from the fact that the truncated discrete Gaussian $D_{\mathbb{Z}_q^{(m+1)\times N}}$ is supported on
\[
\{ X \in \mathbb{Z}_q^{(m+1)\times N} : \|X\|_\infty \leq \alpha q \sqrt{N(m + 1)/2} \}. \text{ Recall that DualFHECD}\text{-Dec}(sk, |\tilde{C}T\rangle) \text{ measures the} \text{ ciphertext } |\tilde{C}T\rangle \text{ in the computational basis with outcome } C = (C_1, \ldots, C_\ell), \text{ where } C_i \in \mathbb{Z}_q^{(m+1)\times N} \text{ is a matrix, and outputs } x' \leftarrow \text{DualFHECD}\text{-Dec}(sk, C). \text{ By our choice of parameters, each error term satisfies}
\]
\[
\|E_i\|_\infty \leq \alpha q \sqrt{\frac{N(m + 1)}{2}} < \frac{q}{4\sqrt{(m + 1)N}}, \quad \forall i \in [\ell].
\]
Hence, decryption correctness is preserved if $t_C = \emptyset$. Let us now consider the case when $t_C \neq \emptyset$, i.e. the Boolean circuit $C$ consists of at least one NAND gate which has been applied to the ciphertext $|CT\rangle$. In this case, the cumulative error in system $C_{out}$ after $L$ applications of $U_{\text{NAND}}$ in Definition 28 is at most $\alpha q \sqrt{N(m + 1)/2(N + 1)^L}$, which is less than $\frac{q}{4\sqrt{(m + 1)N}}$ by our choice of parameters. Therefore, the procedure DualFHE.Dec$_{sk}$ decrypts a computational basis state in system $C_{out}$ of the state $|\tilde{C}T\rangle$ correctly with probability at least $1 - \text{negl}(\lambda)$. Furthermore, because the procedure DualFHECD.Dec is independent of the circuit $C$ and its depth $L$, the scheme DualFHECD is compact. This proves the claim. \hfill \Box

Let us now verify the correctness of verification of the scheme DualFHECD in Construction 3 according to Definition 25. We show the following.
Lemma 21 (Correctness of verification). Let $\lambda \in \mathbb{N}$ be the security parameter. Let $n \in \mathbb{N}$, let $q \geq 2$ be a prime modulus and $m \geq 2n \log q$. Let $N = (n + 1) \cdot \lceil \log q \rceil$ be an integer and let $L$ be an upper bound on the depth of the polynomial-sized Boolean circuit which is to be evaluated. Let $\alpha \in (0, 1)$ be a ratio with
\[
\sqrt{8(m + 1)N} \leq aq \leq \frac{q}{\sqrt{8(m + 1) \cdot N \cdot (N + 1)^L}}.
\]

Then, the Dual-Regev FHE scheme $\text{DualFHE}_{\text{CD}} = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval}, \text{Del}, \text{Vrfy})$ with certified deletion in Construction 3 satisfies verification correctness. In other words, for any $\lambda \in \mathbb{N}$, any plaintext $x \in \{0, 1\}^L$ and any polynomial-sized Boolean circuit $C$ entirely composed of NAND gates:
\[
\Pr \left[ \text{Verify}(vk, \pi) = 1 \mid \left( (pk, sk) \leftarrow \text{KeyGen}(\lambda) \right) \right. \left. \left( (vk, CT) \leftarrow \text{Enc}(pk, x) \right) \right] \geq 1 - \text{negl}(\lambda).
\]

Proof. Consider a bit $x \in \{0, 1\}$ and a public key $pk$ given by $A = [A|\tilde{A} \cdot \bar{x} \pmod{q}] \in \mathbb{Z}_q^{(m + 1) \times n}$, for $\bar{x} \leftarrow \mathbb{Z} \{0, 1\}^m$. By the Leftover Hash Lemma (Lemma 4), the distribution of $A$ is within negligible total variation distance of the uniform distribution over $\mathbb{Z}_q^{(m + 1) \times n}$. Lemma 9 implies that the columns of $A$ generate $\mathbb{Z}_q^n$ with overwhelming probability. We consider the ciphertext $|CT\rangle$ output by $\text{Enc}(pk, x)$, where
\[
|CT\rangle \leftarrow X_{\tilde{g}_1}^{x_{\tilde{g}_1}} |\tilde{\psi}_1\rangle \otimes \cdots \otimes X_{\tilde{g}_N}^{x_{\tilde{g}_N}} |\tilde{\psi}_N\rangle,
\]
and where $(g_1, \ldots, g_N)$ are the rows of the gadget matrix $G \in \mathbb{Z}_q^{(m + 1) \times N}$ in Eq. (18). Given our choice,
\[
\sqrt{8(m + 1)N} \leq aq \leq \frac{q}{\sqrt{8(m + 1) \cdot N \cdot (N + 1)^L}}.
\]

Corollary 1 implies that the Fourier transform of $|CT\rangle$ is within negligible trace distance of the state
\[
|\hat{C}T\rangle = \sum_{x_1 \in \mathbb{Z}_q^{m+1}} \omega_{\tilde{g}_1}^{x_1 \cdot \tilde{g}_1} |x_1\rangle \otimes \cdots \otimes \sum_{x_N \in \mathbb{Z}_q^{m+1}} \omega_{\tilde{g}_N}^{x_N \cdot \tilde{g}_N} |x_N\rangle.
\]

From Lemma 11, it follows that the distribution of computational basis measurement outcomes is within negligible total variation distance of the sample
\[
\pi = (\pi_1, \ldots, \pi_N) \sim D_{\Lambda_{n_1}}^{y_1}(A), \frac{1}{x_{n_1}} \times \cdots \times D_{\Lambda_{n_N}}^{y_N}(A), \frac{1}{x_{n_N}},
\]
where $\|\pi_i\| \leq \sqrt{m + 1} / \sqrt{2^{\alpha}}$ for every $i \in [N]$. This proves the claim. \hfill $\square$

We now show that our scheme $\text{DualFHE}_{\text{CD}}$ in Construction 3 is extractable according to Definition 26.

Lemma 22 (Extractability of DualFHECD). Let $\lambda \in \mathbb{N}$ be the security parameter. Let $n \in \mathbb{N}$, let $q \geq 2$ be a prime modulus and $m \geq 2n \log q$. Let $N = (n + 1) \cdot \lceil \log q \rceil$ and let $L$ be an upper bound on the depth of the polynomial-sized Boolean circuit which is to be evaluated. Let $\alpha \in (0, 1)$ be a noise ratio with
\[
\sqrt{8(m + 1)N} \leq aq \leq \frac{q}{\sqrt{8(m + 1) \cdot N \cdot (N + 1)^L}}.
\]
Then, the Dual-Regev FHE scheme \( \Sigma = \text{DualFHE}_{\text{CD}} \) with certified deletion in Construction 3 is extractable. In other words, for any efficiently computable circuit \( C : \{0, 1\}^\ell \to \{0, 1\} \) and any input \( x \in \{0, 1\}^\ell \):

\[
\Pr \left[ y \neq C(x_1, \ldots, x_\ell) \right] \leq \text{negl}(\lambda), \quad \text{and}
\]

\[
\Pr \left[ \text{Vrfy}(vk, \pi) = \perp \right] \leq \text{negl}(\lambda).
\]

**Proof.** Let \( C : \{0, 1\}^\ell \to \{0, 1\} \) be an efficiently computable circuit and let \( x \in \{0, 1\}^\ell \) be any input. Let \((\varrho, y) \leftarrow \text{Extract}(S(\uparrow CT), t_C), R(sk))\) denote the outcome of the interactive protocol between the sender \( S \) and the receiver \( R \), where \((\uparrow CT), t_C) \leftarrow \text{Eval}(C, |CT\rangle, pk)\) is the post-evaluation state and \( CT \leftarrow \text{Enc}(pk, x)\) is the initial ciphertext for \((pk, sk) \leftarrow \text{KeyGen}(1^\lambda)\). Recall that the receiver \( R \) reversibly performs the decryption procedure \( \text{Dec} \) (with the secret key \( sk \) hard-coded) during the execution of the protocol \( \Pi = \langle S(\uparrow CT), t_C), R(sk)\rangle \) in Protocol 1. Therefore, it follows that the measurement outcome \( y \) is equal to \( C(x_1, \ldots, x_\ell) \) with overwhelming probability due Lemma 20. This shows the first property.

To show the second property, we can use the Rewinding Lemma (Lemma 19) to argue that after the interactive protocol \( \Pi = \langle S(\uparrow CT), t_C), R(sk)\rangle \) between the sender \( S \) and receiver \( R \) is complete, the sender \( S \) is in possession of a quantum state \( \varrho \) in system \( C_{\text{in}} \) that satisfies

\[
\| \varrho - |CT\rangle\langle CT| \|_{\text{tr}} \leq \text{negl}(\lambda).
\]

Therefore, the claim follows immediately from the verification correctness of \( \Sigma \) shown in Lemma 21. \( \square \)

### 9.3 Proof of security

Let us now analyze the security of our FHE scheme with certified deletion in Construction 3. Note that the results in this section all essentially carry over from Section 7.2, where we analyzed the security of our Dual-Regev PKE scheme with certified deletion.

**IND-CPA security of DualFHE\(_{\text{CD}}\).** We first prove that our scheme \( \text{FHE}_{\text{CD}} \) in Construction 3 satisfies the notion IND-CPA security according to Definition 12. The proof is identical to the proof of IND-CPA-security of our DualPKE scheme in Theorem 6. We add it for completeness.

**Theorem 9.** Let \( n \in \mathbb{N} \), let \( q \geq 2 \) be a modulus, let \( m \geq 2n \log q \) and let \( N = (n + 1)\lceil \log q \rceil \), each parameterized by the security parameter \( \lambda \in \mathbb{N} \). Let \( \alpha \in (0, 1) \) be a noise ratio parameter such that \( \sqrt{8(m + 1)N} \leq \frac{1}{\alpha} \leq \frac{q}{\sqrt{8(m + 1)N}} \). Then, the scheme DualFHE\(_{\text{CD}} \) in Construction 3 is IND-CPA-secure assuming the quantum hardness of (decisional) \( \text{LWE}_{n,q,\chi q}^{(m+1)N} \), for any \( \beta \in (0, 1) \) with \( \alpha / \beta = \lambda^{\omega(1)} \).

**Proof.** Let \( \Sigma = \text{DualFHE}_{\text{CD}} \). We need to show that, for any QPT adversary \( A \), it holds that

\[
\text{Adv}_{\Sigma, A}(\lambda) := \left| \Pr[\text{Exp}_{\Sigma, A, \lambda}^{\text{ind-cpa}}(0) = 1] - \Pr[\text{Exp}_{\Sigma, A, \lambda}^{\text{ind-cpa}}(1) = 1] \right| \leq \text{negl}(\lambda).
\]

Consider the experiment \( \text{Exp}_{\Sigma, A, \lambda}^{\text{ind-cpa}}(b) \) between the adversary \( A \) and a challenger taking place as follows:
1. The challenger generates a pair \((pk, sk) \leftarrow \text{KeyGen}(1^\lambda)\), and sends \(pk\) to \(A\).
2. \(A\) sends a distinct plaintext pair \((m_0, m_1) \in \{0, 1\}^\ell \times \{0, 1\}^\ell\) to the challenger.
3. The challenger computes \((vk, CT_b) \leftarrow \text{DualFHE}_{\text{CD}}.\text{Enc}(pk, m_b)\), and sends \(|CT_b|\) to \(A\).
4. \(A\) outputs a guess \(b' \in \{0, 1\}\), which is also the output of the experiment.

Recall that the procedure \(\text{Enc}(pk, m_b)\) outputs a pair \((vk, |CT_b|)\), where

\[
\left( A \in \mathbb{Z}_q^{(m+1) \times n}, (y_1, \ldots, y_N) \in \mathbb{Z}_q^{n \times N} \right) \leftarrow vk
\]

is the verification key and where the ciphertext \(|CT_b|\) is within negligible trace distance of

\[
\sum_{s \in \mathbb{Z}_q^{n \times N}} \sum_{E \in \mathbb{Z}_q^{(m+1) \times N}} \theta_{aq}(E) \omega_q^{-\text{Tr}[S^T Y]} |A \cdot S + E + m_b \cdot G \mod q|.
\]

(19)

Here, \(Y \in \mathbb{Z}_q^{N \times N}\) is the matrix composed of the rows \(y_1, \ldots, y_N\). Let \(\beta \in (0, 1)\) be any parameter with \(a/\beta = \lambda^{\omega(1)}\). Then, it follows from Theorem 5 that, under the (decisional) LWE\(_{n, q, \beta q}^{(m+1)N}\) assumption, \(|CT_b|\) is computationally indistinguishable from the state

\[
\sum_{u \in \mathbb{Z}_q^{(m+1) \times N}} \omega_q^{\text{Tr}[U^T X]} |U|, \quad X = (\bar{x}_1, \ldots, \bar{x}_N) \sim D_{\Lambda_{\beta q}^{\frac{1}{\sqrt{n} \cdot \lambda}}(A), \frac{1}{\sqrt{\lambda} \cdot \lambda}} \times \cdots \times D_{\Lambda_{\beta q}^{\frac{1}{\sqrt{n} \cdot \lambda}}(A), \frac{1}{\sqrt{\lambda} \cdot \lambda}.
\]

(20)

Here \((\bar{x}_1, \ldots, \bar{x}_N)\) refer to the rows of the matrix \(X \in \mathbb{Z}_q^{(m+1) \times N}\). Finally, because the state in Eq. (20) is completely independent of the bit \(b \in \{0, 1\}\), it follows that

\[
\text{Adv}_{\Sigma_\lambda}(\lambda) := |\Pr[\text{Exp}_{\Sigma_\lambda}^{\text{ind-cpa}}(0) = 1] - \Pr[\text{Exp}_{\Sigma_\lambda}^{\text{ind-cpa}}(1) = 1]| \leq \text{negl}(\lambda).
\]

This proves the claim.

\[\square\]

**IND-CPA-CD security of DualFHE\(_{\text{CD}}\).** Let us now analyze the security of our Dual-Regev homomorphic encryption scheme DualFHE\(_{\text{CD}}\) in Construction 3. We prove that it satisfies certified deletion security assuming the Strong Gaussian-Collapsing (SGC) Conjecture (see Conjecture 5.2). This is a strengthening of the Gaussian-collapsing property which we proved under the (decisional) LWE assumption (see Theorem 4). The proof is similar to the proof of Theorem 7. We add it for completeness.

**Theorem 10.** Let \(\lambda \in \mathbb{N}\) be the security parameter. Let \(n \in \mathbb{N}\), let \(q \geq 2\) be a prime modulus and \(m \geq 2n \log q\). Let \(N = (n + 1) \cdot \lceil \log q \rceil\) be an integer and let \(L\) be an upper bound on the depth of the polynomial-sized Boolean circuit which is to be evaluated. Let \(\alpha \in (0, 1)\) be a noise ratio such that

\[
\sqrt{8(m+1)N} \leq \alpha q \leq \frac{q}{\sqrt{8(m+1) \cdot N \cdot (N+1)^L}}.
\]

Then, the Dual-Regev homomorphic encryption scheme DualFHE\(_{\text{CD}}\) in Construction 3 is IND-CPA-CD-secure assuming the Strong Gaussian-Collapsing property SGC\(_{n,(m+1)q,\frac{1}{2}}^N\) from Conjecture 5.2.
Proof. Let $\Sigma = \text{DualFHE}_{CD}$. We need to show that, for any QPT adversary $A$, it holds that

$$\text{Adv}^{\text{he-cert-del}}_{\Sigma,A}(\lambda) := |\Pr[\text{Exp}^{\text{he-cert-del}}_{\Sigma,A}(0) = 1] - \Pr[\text{Exp}^{\text{he-cert-del}}_{\Sigma,A}(1) = 1]| \leq \text{negl}(\lambda).$$

We consider the following sequence of hybrids:

**H$_0$**: This is the experiment $\text{Exp}^{\text{he-cert-del}}_{\Sigma,A}(0)$ between $A$ and a challenger:

1. The challenger samples a random matrix $\hat{A} \xleftarrow{\$} Z_q^{n \times m}$ and a vector $\hat{x} \xleftarrow{\$} \{0,1\}^m$ and chooses $A = [\hat{A}|\hat{A} - \hat{x} \pmod{q}]^T$. The challenger chooses the secret key $sk \leftarrow (-\hat{x},1) \in Z_q^{m+1}$ and the public key $pk \leftarrow A \in Z_q^{(m+1) \times n}$.
2. $A$ sends a distinct plaintext pair $(m_0,m_1) \in \{0,1\} \times \{0,1\}$ to the challenger. (Note: Without loss of generality, we can just assume that $m_0 = 0$ and $m_1 = 1$).
3. The challenger runs $(|\psi_i\rangle, y_i) \leftarrow \text{GenPrimal}(A^T, \sigma)$ in Algorithm 2, for $i \in [N]$, and outputs $$(vk \leftarrow (A \in Z_q^{(m+1) \times n}, (y_1,\ldots,y_N) \in Z_q^{n \times N}), \ |CT_0\rangle \leftarrow |\psi_1\rangle \otimes \cdots \otimes |\psi_N\rangle).$$
4. At some point in time, $A$ returns a certificate $\pi = (\pi_1,\ldots,\pi_N)$ to the challenger.
5. The challenger outputs $\top$, if $A^T \cdot \pi_i = y_i \pmod{q}$ and $||\pi_i|| \leq \sqrt{m+1}/\sqrt{2}\alpha$ for $i \in [N]$, and outputs $\bot$, otherwise. If $\pi$ passes the test with outcome $\top$, the challenger sends $sk$ to $A$.
6. $A$ outputs a guess $b' \in \{0,1\}$, which is also the output of the experiment.

**H$_1$**: This is same experiment as in $H_0$, except that (in Step 3) the challenger prepares the ciphertext in the Fourier basis rather than the standard basis. In other words, $A$ receives the pair $$(vk \leftarrow (A \in Z_q^{(m+1) \times n}, (y_1,\ldots,y_N) \in Z_q^{n \times N}), \ |CT_0\rangle \leftarrow FT_q |\psi_1\rangle \otimes \cdots \otimes FT_q |\psi_N\rangle).$$

**H$_2$**: This experiment is an $N$-fold variant of $\text{StrongGaussCollapseExp}_{H,D,A}(0)$ in Conjecture 5.2:

1. The challenger samples a random matrix $\hat{A} \xleftarrow{\$} Z_q^{n \times m}$ and a vector $\hat{x} \xleftarrow{\$} \{0,1\}^m$ and chooses $A = [\hat{A}|\hat{A} - \hat{x} \pmod{q}]$ and $t = (-\hat{x},1) \in Z_q^{m+1}$.
2. The challenger runs $(|\hat{\psi}_i\rangle, y_i) \leftarrow \text{GenDual}(A^T, \sigma)$ in Algorithm 1, for $i \in [N]$, and sends the following tiplet to the adversary $A$:

$$(|\hat{\psi}_1\rangle \otimes \cdots \otimes |\hat{\psi}_N\rangle, \ A^T \in Z_q^{n \times (m+1)}, \ Y = (y_1,\ldots,y_N) \in Z_q^{n \times N}).$$
3. At some point in time, $A$ returns a certificate $\pi$ to the challenger.
4. The challenger outputs $\top$, if $A^T \cdot \pi_i = y_i \pmod{q}$ and $||\pi_i|| \leq \sqrt{m+1}/\sqrt{2}\alpha$ for $i \in [N]$, and outputs $\bot$, otherwise. If $\pi$ passes the test with outcome $\top$, the challenger sends $sk$ to $A$.
5. $A$ outputs a guess $b' \in \{0,1\}$, which is also the output of the experiment.

**H$_3$**: This is an $N$-fold variant of the experiment in $\text{StrongGaussCollapseExp}_{H,D,A}(1)$ in Conjecture 5.2; it is the same as $H_2$, except that the states $|\hat{\psi}_1\rangle \otimes \cdots \otimes |\hat{\psi}_N\rangle$ (in Step 2) are measured in the computational basis before they are sent to $A$.  

56
**H₄**: This is same experiment as **H₃**, except that (in Step 2) the challenger additionally applies the Pauli operators \(Z_q^{g₁} \otimes \cdots \otimes Z_q^{g_N}\) to the states \(|\hat{ψ}_{y₁}\rangle \otimes \cdots \otimes |\hat{ψ}_{y_N}\rangle\) before they are measured in the computational basis, where \((g₁, \ldots, g_N)\) are the rows of the gadget matrix \(G \in \mathbb{Z}_{q}^{(m+1)\times N}\) in Eq. (18).

**H₅**: This is same experiment as **H₄**, except that (in Step 2) \(A\) receives the triplet
\[
\left( Z_q^{g₁} |\hat{ψ}_{y₁}\rangle \otimes \cdots \otimes Z_q^{g_N} |\hat{ψ}_{y_N}\rangle, \quad A^T \in \mathbb{Z}_q^{n \times (m+1)}, \quad y = (y₁, \ldots, y_N) \in \mathbb{Z}_q^{n \times N}\right).
\]

**H₆**: This is same experiment as **H₅**, except that (in Step 2) the challenger prepares the quantum states in the Fourier basis instead. In other words, \(A\) receives the triplet
\[
\left( FT_q Z_q^{g₁} |\hat{ψ}_{y₁}\rangle \otimes \cdots \otimes FT_q Z_q^{g_N} |\hat{ψ}_{y_N}\rangle, \quad A^T \in \mathbb{Z}_q^{n \times (m+1)}, \quad y = (y₁, \ldots, y_N) \in \mathbb{Z}_q^{n \times N}\right).
\]

**H₇**: This is the experiment \(\text{Exp}_{\Sigma, A, λ}^{\text{he-cert-del}}(1)\).

We now show that the hybrids are indistinguishable.

**Claim 9.**
\[
\Pr[\text{Exp}_{\Sigma, A, λ}^{\text{he-cert-del}}(0) = 1] = \Pr[H₁ = 1].
\]

**Proof.** Without loss of generality, we can assume that \(A\) applies the inverse Fourier transform immediately upon receiving the quantum ciphertext. Therefore, the success probabilities are identical in **H₀** and **H₁**.

**Claim 10.**
\[
\Pr[H₁ = 1] = \Pr[H₂ = 1].
\]

**Proof.** Because the challenger in **H₁** always sends the ciphertext \(|CT₀⟩\) corresponding to \(m₀ = 0\) to the adversary \(A\), the two hybrids **H₁** and **H₂** are identical.

**Claim 11. Under the Strong Gaussian-Collapsing property \(\text{SGC}_{n,m+1,q,λ}^{N}\), it holds that**
\[
|\Pr[H₂ = 1] − \Pr[H₃ = 1]| \leq \text{negl}(λ).
\]

**Proof.** This follows from **Conjecture 5.2**.

**Claim 12.**
\[
\Pr[H₃ = 1] = \Pr[H₄ = 1].
\]

**Proof.** Because the challenger measures the state \(|\hat{ψ}_{y₁}\rangle \otimes \cdots \otimes |\hat{ψ}_{y_N}\rangle\) in Step 2 in the computational basis, applying the phase operators \(Z_q^{g₁} \otimes \cdots \otimes Z_q^{g_N}\) before the measurement does not affect the outcome.

**Claim 13. Under the Strong Gaussian-Collapsing property \(\text{SGC}_{n,m+1,q,λ}^{N}\), it holds that**
\[
|\Pr[H₄ = 1] − \Pr[H₅ = 1]| \leq \text{negl}(λ).
\]

**Proof.** This follows from **Conjecture 5.2** since, without loss of generality, we can assume that \(A\) applies the phase operators \(Z_q^{g₁} \otimes \cdots \otimes Z_q^{g_N}\) immediately upon receiving the states \(|\hat{ψ}_{y₁}\rangle \otimes \cdots \otimes |\hat{ψ}_{y_N}\rangle\) as input.
Claim 14.

\[ \Pr[H_5 = 1] = \Pr[H_6 = 1]. \]

Proof. Without loss of generality, we can assume that \( \mathcal{A} \) applies the Fourier transform immediately upon receiving \( Z_{q}^{g_1} |\hat{\psi}_{y_1}\rangle \otimes \cdots \otimes Z_{q}^{g_N} |\hat{\psi}_{y_N}\rangle \). Therefore, the success probabilities in \( H_5 \) and \( H_6 \) are identical. \( \square \)

Claim 15.

\[ | \Pr[H_6 = 1] - \Pr[\text{Exp}_{\Sigma,\lambda}(1) = 1] | \leq \text{negl}(\lambda). \]

Proof. From Lemma 6, we have \( \text{FT}_{q} Z_{q}^{v} |\psi_{y}\rangle = Z_{q}^{v} \text{FT}_{q} |\psi_{y}\rangle \), for all \( v \in \mathbb{Z}_q^m \). Hence, in \( H_6 \), we can instead assume that the challenger runs \( (|\psi_{y_1}\rangle, y_1) \leftarrow \text{GenPrimal}(A^T, 1/\alpha) \) in Algorithm 2, for \( i \in [N] \), and then sends the following to \( \mathcal{A} \):

\[
(v_k \leftarrow (A \in \mathbb{Z}_q^{(m+1) \times n}, (y_1, \ldots, y_N) \in \mathbb{Z}_q^{n \times N}), \ |CT_1\rangle \leftarrow X_{q}^{g_1} |\psi_{y_1}\rangle \otimes \cdots \otimes X_{q}^{g_N} |\psi_{y_N}\rangle).
\]

From Corollary 1, it follows that the states \( \text{FT}_{q}^{-1} Z_{q}^{v} |\psi_{y}\rangle \) and \( Z_{q}^{v} |\psi_{y}\rangle \) are within negligible trace distance, for all \( v \in \mathbb{Z}_q^m \). Because the challenger in \( H_7 \) always sends \( |CT_1\rangle \) corresponding to \( m_1 = 1 \) to the adversary \( \mathcal{A} \), it follows that the distinguishing advantage between \( H_6 \) and \( H_7 = \text{Exp}_{\Sigma,\lambda}(1) \) is negligible. \( \square \)

Because the hybrids \( H_0 \) and \( H_7 \) are indistinguishable, this implies that

\[ \text{Adv}_{\Sigma,A}^{\text{he-cert-del}}(\lambda) \leq \text{negl}(\lambda). \]

\[ \square \]

References


Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography, 2021.


