Quantum Proofs of Deletion for Learning with Errors

Alexander Poremba[*]

California Institute of Technology

March 3, 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). This results in a new and powerful cryptographic notion called fully homomorphic encryption 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 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. We introduce an encoding based on *Gaussian coset states* which is highly generic and suggests that essentially *any* LWE-based cryptographic primitive admits a classically-verifiable quantum proof of deletion.

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. In terms of security, we distinguish between two types of attack scenarios: a semi-honest adversary that follows the protocol exactly, and a fully malicious adversary that is allowed to deviate arbitrarily from the protocol. In the former case, we achieve *indistinguishable ciphertexts*, even if the secret key is later revealed after deletion has taken place. In the latter case, we provide *entropic uncertainty relations for Gaussian cosets* which limit the adversary's ability to *guess* the delegated ciphertext once deletion has taken place. 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

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 private machine learning 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.

Formalizing quantum proofs of deletion. In this work, we present a formal definition of *quantum proofs of deletion* as an interactive protocol between a quantum prover and a classical verifier, which is inspired by so-called *agree-and-prove* schemes [BJM19, VZ21] in the context of proofs of knowledge. In contrast with the notion of certified deletion of ciphertexts by Broadbent and Islam [BI20], our definition of deletion relies on *entropies* and instead considers samples from *arbitrary* probability distributions. We introduce the notion of a *quantum proof-of-deletion protocol* which can be seen as a basic cryptographic primitive in the context of privacy-preserving quantum cloud applications; in particular, it gives rise to much stronger cryptographic notions such as *(public-key) quantum encryption with certified deletion*.

Entropic uncertainty relations for Gaussian cosets. We introduce a family of so-called *Gaussian coset states* which enable a client to encode samples from the *Learning with Errors* (LWE) distribution [Reg05] for the purpose of certifying deletion while simultaneously preserving their full cryptographic functionality. Our quantum proofs of deletion exploit the fact that it is impossible *simultaneously* measure a Gaussian coset state in two complementary bases – a property we establish using *entropic uncertainty relations*.

Quantum proofs of deletion for LWE. Using our encoding based on Gaussian coset states, we construct a quantum proof-of-deletion protocol which allows a client to be convinced that a sample from the LWE distribution has been deleted by an untrusted party. Our protocol achieves a notion we call *pseudoentropic deletion*, which implies that any efficient (possibly malicious) prover can recover the encoded LWE sample with at most negligible probability once deletion has taken place. We highlight that our quantum proof of deletion protocol can be generically applied to essentially *any* LWE-based cryptographic primitive.

Dual-Regev public-key encryption with certified deletion. Using Gaussian coset states, we construct a public-key encryption scheme with certified deletion which is based on the *Dual-Regev* scheme introduced by Gentry, Peikert and Vaikuntanathan [GPV07]. We prove that our construction has indistinguishable ciphertexts in the *semi-honest adversarial model*, even if the secret key is later revealed after deletion has taken place. In this attack scenario, we assume that the adversary *honestly* performs the correct deletion procedure when asked to prove erasure of the quantum ciphertext. However, after the experiment is over, the adversary may carefully analyze any additional data collected throughout the protocol. In the fully malicious setting, we rely on entropic uncertainty relations for Gaussian cosets which help further restrict the ability of a malicious adversary to guess the delegated ciphertext once deletion has taken place.

(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 due to Mahadev [Mah18b], which is a variant of the FHE scheme by Gentry, Sahai and Waters [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. Our security relies entirely on the quantum (subexponential) hardness of the LWE problem.

1.2 Overview

Let us now proceed with a technical overview.

Quantum proofs of deletion. 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* unconditionally using the principle of complementarity [CRW19, BI20]. We can formalize the task of certifying deletion as an interactive protocol between a quantum prover and a classical verifier who seeks to certify the erasure of data handed to the prover in the form of a quantum state[1]. The crucial idea that enables this task is the fact that we can encode information in two mutually unbiased bases. To illustrate the idea, we consider the *computational basis* $\{|0\rangle, |1\rangle\}$ and the *Hadamard basis* $\{|+\rangle, |-\rangle\}$ which present us with a simple case of incompatible bases that cannot be measured at the same time. Here, the two states $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ are the result of the Hadamard operation, which is specified by the map

$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

It is straightforward to see that two bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ are mutually unbiased. Denoting by $\{M^x\}_{x\in\{0,1\}}$ and $\{N^y\}_{y\in\{0,1\}}$ the measurements in the computational basis and the Hadamard basis, respectively, we find that their *overlap* c is precisely the inverse of the dimension of the Hilbert space,

$$\mathsf{c} = \max_{x,y} \left\| \sqrt{M^x}\sqrt{N^y} \right\|_\infty^2 = \frac{1}{2}.$$

Coiteux-Roy and Wolf [CRW19], and subsequently Broadbent and Islam [BI20], proposed simple certified deletion protocols based on Wiesner's *conjugate coding* [Wie83] and the BB84 protocol due to Bennett and Brassard [BB84]. The main idea behind their protocols is that it is possible to *hide* a string $r \in \{0,1\}^m$ by making m uniformly random choices of basis (either computational or Hadamard) which we denote by $\theta \in \{0,1\}^m$. Using the compact notation $H^0 = \mathbb{1}$ and $H^1 = H$, this results in the m-qubit state given by

$$|\boldsymbol{r}^\theta\rangle = H^{\theta_1} |r_1\rangle \otimes \cdots \otimes H^{\theta_m} |r_m\rangle. \tag{1}$$

Going back to the setting of an interactive protocol between a prover and a verifier, how can a prover who is given $|\boldsymbol{r}^\theta\rangle$ prove deletion to a classical verifier who knows both r and θ? The idea is rather simple. The verifier simply asks the prover for the measurement outcome $\pi \in \{0,1\}^m$ of a Hadamard basis measurement, where π serves as the classical proof (or *witness*) of deletion. For the sake of argument, let us assume that the prover is honest and does in fact perform the correct measurement, as requested. Then, for $i \in [m]$, the measurement outcome π_i matches r_i whenever $\theta_i = 1$, and is otherwise uniformly random. Hence, it appears that the prover has successfully deleted precisely the qubits of $|\boldsymbol{r}^\theta\rangle$ that coincide with the value $\theta_i = 0$. In other words, the prover has deleted the substring of r that corresponds to $\theta_i = 0$, which we can think of as the *private classical data* that is hidden from the prover. For the purpose of verification, it is then sufficient to check whether π_i matches r_i whenever $\theta_i = 1$. This essentially marks the approach taken by Coiteux-Roy and Wolf [CRW19] whose protocol ultimately cannot make malicious eavesdropping impossible – it merely makes it possible for a verifier to be convinced that deletion has taken place.

Building on the protocol of Coiteux-Roy and Wolf, Broadbent and Islam [BI20] construct a private-key quantum encryption scheme with a rigorous notion of certified deletion in a fully malicious adversarial

[1] Here, we imagine that a trusted third party prepares any auxiliary inputs handed to the classical verifier and the quantum prover at the beginning of the protocol.

setting by following a protocol that more closely resembles the standard QKD protocol [TL17]. Broadbent and Islam prove that the quantum encryption scheme achieves the notion of *instinguishable ciphertexts* in the context of certified deletion, even if the private key is later revealed once deletion has taken place.

In this work, we give a formal definition of *quantum proofs of deletion* as an interactive protocol between a quantum prover and a classical verifier, which is inspired by so-called *agree-and-prove* schemes [BJM19, VZ21] in the context of proofs of knowledge. In contrast with the notion of certified deletion by Broadbent and Islam [BI20], our definition is not limited to ciphertexts but instead considers *samples from an arbitrary probability distribution* which we call Samp. In a nutshell, we define deletion of a sample x generated by Samp as the prover's "inability to guess x" (in an information-theoretic sense) once the verifier is convinced that deletion has taken place. We formalize the task of *proving deletion* of a sample x as an interactive protocol between a classical verifier $\mathcal{V}$ (who receives as input a verification key vk and seeks to certify the erasure of x) and a quantum prover $\mathcal{P}$ (who receives as input a quantum state ϱ_P that depends on x). Here, we assume that the auxiliary inputs vk and ϱ_P which are handed to $\mathcal{V}$ and $\mathcal{P}$ at the beginning of the protocol are generated by a procedure Setup (for example, a trusted third party). For some additional flexibility, we also allow the auxiliary input generation procedure Setup and the prover $\mathcal{P}$ to receive a public key.

Our definition of quantum proof-of-deletion protocols (formally defined in Definition 16) is as follows.

A *(public-key) quantum proof-of-deletion* (QPD) protocol with respect an ensemble $\mathcal{X} = \{\mathcal{X}_\lambda\}$ is the following tuple of efficient (interactive) algorithms $(\mathsf{Samp}, \mathsf{Setup}, \mathcal{V}, \mathcal{P})$ given by:

- A sampling procedure $\mathsf{Samp}(1^\lambda)$ which takes as input a unary encoding 1^λ of the security parameter λ and outputs a pair (pk, x), where pk is a public key and $x \in \mathcal{X}_\lambda$ is sample.

- An auxiliary input generation procedure $\mathsf{Setup}(1^\lambda, \mathsf{pk}, x)$ which takes as input 1^λ, pk and $x \in \mathcal{X}_\lambda$, and outputs a pair (vk, ϱ_P) of auxiliary inputs for the verifier $\mathcal{V}$ (who receives a verification key vk) and the prover $\mathcal{P}$ (who receives a quantum state ϱ_P which depends on pk, vk and x).

- An (honest) classical verifier $\mathcal{V}(1^\lambda, \mathsf{vk}, \pi)$ which takes as input a unary encoding of the security parameter λ, an auxiliary input vk and a witness π, and outputs 1 (accept) or 0 (reject).

- An (honest) quantum prover $\mathcal{P}(1^\lambda, \mathsf{pk}, \varrho_P)$ which takes as input a unary encoding of the security parameter λ, a public key pk and a quantum state ϱ_P, and produces a classical deletion witness π.

We also define the following properties (see Definition 17 and Definition 19), *informally* stated below:

1. (*Completeness*): For any $\lambda \in \mathbb{N}$, $x \in \mathcal{X}$, the verifier $\mathcal{V}(1^\lambda, \mathsf{vk}, \pi)$ outputs 1 with overwhelming probability, for any honestly generated proof $\pi \leftarrow \mathcal{P}(1^\lambda, \mathsf{pk}, \varrho_P)$ with $(\mathsf{vk}, \varrho_P) \leftarrow \mathsf{Setup}(1^\lambda, \mathsf{pk}, x)$.

2. (*Entropic deletion*): Let X denote the random variable associated with the sample $x \leftarrow \mathsf{Samp}(1^\lambda)$. Then, for any (possibly malicious) prover $\widetilde{\mathcal{P}}(1^\lambda, \mathsf{pk}, \varrho_P)$ that receives an auxiliary input ϱ_P (which depends on x, pk and vk) and produces an outcome $|\pi\rangle\langle\pi|_\Pi \otimes \varrho_E$, where π is a witness and ϱ_E denotes the prover's quantum side information, at least *one* of the following two conditions applies:

   (1) the min-entropy of X given the public-key pk and the leftover quantum system E is large, **or**

   (2) the verification of π fails, and $\mathcal{V}(1^\lambda, \mathsf{vk}, \pi)$ outputs 0.

   In other words, the probability that a (possibly malicious) prover $\widetilde{\mathcal{P}}$ correctly guesses the random variable X with outcome x *and* simultaneously produces a proof π that passes verification is very low. We make this trade-off more precise in Definition 19, where we characterize entropic deletion in terms of the min-entropy of X. As a complementary notion, we also define *pseudoentropic deletion* which holds for all computationally bounded and possibly malicious provers. In this context, we replace the information-theoretic notion of *min-entropy* with *computational pseudoentropy* (see Definition 5).

The conjugate coding scheme of Broadbent and Islam [BI20] presents us with an example of a quantum proof-of-deletion protocol, as it is implicitly shown that the scheme satisfies the notion of entropic deletion. Namely, once deletion has taken place, the prover's uncertainty about the substring $r_{\mathcal{I}}$ that coincides with the set $\mathcal{I} = \{i \in [m] : \theta_i = 0\}$ of the quantum state $|\boldsymbol{r}^\theta\rangle$ in Eq. (1) must necessarily be large.

Quantum proofs of deletion for Learning with Errors. 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. More concretely, the problem is the following. Let $n \in \mathbb{N}$, $q \geq 2$ and $m \geq n$ be integers, and let $\alpha \in (0,1)$ be a noise ratio parameter. In its decisional formulation, the $\mathsf{LWE}^m_{n,q,\alpha q}$ problem asks to distinguish between the samples $(\boldsymbol{A}, \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}_0 \pmod q)$ and $(\boldsymbol{A}, \boldsymbol{u})$, where $\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$ and $\boldsymbol{s} \xleftarrow{\$} \mathbb{Z}_q^n$ are random, where $\boldsymbol{e}_0 \sim D_{\mathbb{Z}^m,\alpha q}$ is a noise vector, and where $\boldsymbol{u} \xleftarrow{\$} \mathbb{Z}_q^m$ is a uniformly random string. Here, $D_{\mathbb{Z}^m,r}$ is the discrete Gaussian distribution with parameter $r > 0$ that assigns probability proportional to $\varrho_r(\boldsymbol{x}) = e^{-\pi\|\boldsymbol{x}\|^2/r^2}$ to every lattice point $\boldsymbol{x} \in \mathbb{Z}^m$. Our work assumes the hardness of $\mathsf{LWE}^m_{n,q,\alpha q}$ with subexponential parameter $1/\alpha$, and thus relies on the worst-case hardness of approximating short vector problems (e.g. the shortest independent vectors problem, SIVP) in lattices to within a subexponential factor in n [Reg05, PRSD17].

How can we certify that a (possibly malicious) prover has deleted a sample from the $\mathsf{LWE}^m_{n,q,\alpha q}$ distribution? The main technical insight of our work is that one can use Gaussian superpositions to encode samples from the $\mathsf{LWE}^m_{n,q,\alpha q}$ distribution for the purpose of certified deletion while simultaneously preserving their cryptographic functionality. Let us now describe the idea behind our quantum proof-of-deletion protocol $(\mathsf{Samp}, \mathsf{Setup}, \mathcal{V}, \mathcal{P})$ for the LWE distribution (formally defined in Protocol 1) in more detail.

To encode a sample $(\boldsymbol{A}, \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}_0 \pmod q) \sim \mathsf{LWE}^m_{n,q,\alpha q}$ with a public matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$, we sample a random vector $\boldsymbol{v} \xleftarrow{\$} \mathbb{Z}_q^m$ and consider the Gaussian superposition with parameter $\beta > 0$ defined by

$$|\mathcal{D}^{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}_0,\boldsymbol{v}}_{\beta q}\rangle = \sum_{\boldsymbol{e}\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,\beta q}(\boldsymbol{e})} \cdot e^{-\frac{2\pi i}{q}\langle \boldsymbol{e},\boldsymbol{v}\rangle} \, |\boldsymbol{A}\cdot\boldsymbol{s} + \boldsymbol{e}_0 + \boldsymbol{e} \pmod q\rangle \,. \tag{2}$$

Here, we use the truncated discrete Gaussian $D_{\mathbb{Z}_q^m,\beta q}$ with support $\{\boldsymbol{x} \in \mathbb{Z}_q^m : \|\boldsymbol{x}\|_\infty \leq \sqrt{m}\beta q\}$. Note that we frequently denote the finite cube $\mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$ as $\mathbb{Z}_q^m$ in slight abuse of notation. The quantum state in Eq. (2) is essentially just a superposition of LWE samples over noise terms from the shifted distribution $(D_{\mathbb{Z}_q^m,\beta q} + \boldsymbol{e}_0)(x) = D_{\mathbb{Z}_q^m,\beta q}(\boldsymbol{x} - \boldsymbol{e}_0)$, except for an additional phase which depends on $\boldsymbol{v} \in \mathbb{Z}_q^m$. While the additional Gaussian shift $\boldsymbol{e}_0 \sim D_{\mathbb{Z}^m,\alpha q}$ in the encoding seems redundant, we choose to include it as it serves an important purpose in our security analysis. Fortunately, the shifted Gaussian $D_{\mathbb{Z}_q^m,\beta q} + \boldsymbol{e}_0$ is statistically close to the regular Gaussian $D_{\mathbb{Z}_q^m,\beta q}$ if β/α is superpolynomial (see Lemma 10). Therefore, a simple computational basis measurement of the state in Eq. (2) allows us to approximately reconstruct a sample from the distribution $\mathsf{LWE}^m_{n,q,\beta q}$. We remark that the security of our protocol depends on the hardness of the $\mathsf{LWE}^m_{n,q,\alpha q}$ distribution, whereas the parameters of the distribution $\mathsf{LWE}^m_{n,q,\beta q}$ (in particular, $\beta > 0$) are relevant for cryptographic applications of our encoding, such as homomorphic encryption. Superpositions of LWE samples have also 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- and Ring-LWE-based cryptosystems.

The crucial idea behind our quantum proof-of-deletion protocol $(\mathsf{Samp}, \mathsf{Setup}, \mathcal{V}, \mathcal{P})$ for LWE (formally defined in Protocol 1) lies in the fact that we can use the vector $\boldsymbol{v} \in \mathbb{Z}_q^m$ in order to *prove deletion*. In other words, we require that the (honest) prover $\mathcal{P}$ measures the state in Eq. (2) in the *Fourier basis* to erase the LWE sample encoded in the computational basis. Applying the Fourier transform to the *primal* Gaussian coset in Eq. (2) results in a state which is within trace distance $2^{-\Omega(m)}$ of the so-called *dual* Gaussian coset,

$$|\mathcal{D}_{1/2\beta}^{\boldsymbol{v},-(\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}_0)}\rangle = \sum_{\boldsymbol{e}\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,1/2\beta}(\boldsymbol{e})} \cdot e^{\frac{2\pi i}{q}\langle \boldsymbol{e}, \boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}_0\rangle} \, |\boldsymbol{v}+\boldsymbol{e} \pmod{q}\rangle \,. \tag{3}$$

We make this fact more precise in the so-called *Gaussian Switching Lemma* (see Lemma 11), which we derive using the *Poisson summation formula* (Lemma 9). The *primal* Gaussian coset in Eq. (2) and the *dual* Gaussian coset in Eq. (3) can be associated with a primal and dual integer lattice – a relationship we explore in greater detail in Section 4. Notice that a Fourier basis measurement of the state in Eq. (2) yields a sample $\pi \sim D_{\mathbb{Z}_q^m - \boldsymbol{v},1/2\beta}$ from the shifted Gaussian with parameter $1/2\beta$ centered around $\boldsymbol{v} \in \mathbb{Z}_q^m$. Hence, it is possible for the classical verifier $\mathcal{V}$ to check whether a sample $\pi = \boldsymbol{v} + \boldsymbol{e} \pmod{q}$ with $\boldsymbol{e} \sim D_{\mathbb{Z}_q^m,1/2\beta}$ is sufficiently close to $\boldsymbol{v}$ by checking whether the difference is a *short vector* in $\mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$.

Theorem (informal): *There exists a quantum proof-of-deletion protocol* $(\mathsf{Samp}, \mathsf{Setup}, \mathcal{V}, \mathcal{P})$ *for the Learning with Errors* (LWE) *distribution (formally defined in Protocol 1) which has completeness and pseudoentropic deletion against all (possibly malicious) provers that pass verification with overwhelming probability (assuming the quantum hardness of the* LWE *problem).*

In order to show that our protocol has *entropic deletion*, we have to argue that, if the prover produces an outcome which is highly correlated with an outcome associated with the Fourier basis, it is unlikely that the prover also succeeds at guessing the outcome of a hypothetical computational basis measurement.

To show this property, we shift our analysis to perfectly *random Gaussian cosets*. Here, we use the fact that $(\boldsymbol{A}, \boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}_0 \pmod{q})$ and $(\boldsymbol{A}, \boldsymbol{u})$ are computationally indistinguishable under the $\mathsf{LWE}_{n,q,\alpha q}^m$ assumption, where $\boldsymbol{u} \xleftarrow{\$} \mathbb{Z}_q^m$ is a random vector. This allows us to argue that the Gaussian coset in Eq. (2) is computationally indistinguishable from a random Gaussian coset with parameter $r = \beta q > 0$ given by

$$|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle = \sum_{\boldsymbol{e}\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{e})}\, e^{-\frac{2\pi i}{q}\langle \boldsymbol{e},\boldsymbol{v}\rangle} \, |\boldsymbol{u}+\boldsymbol{e} \pmod{q}\rangle \,. \tag{4}$$

Our quantum proofs of deletion rely on the fact that it is impossible *simultaneously* measure a Gaussian coset state in two complementary bases – a fact we establish using *entropic uncertainty relations*.

Uncertainty relations for Gaussian coset states. Suppose that a (possibly malicious) prover receives a random Gaussian coset state and is asked to prove deletion via an appropriate Fourier basis measurement. How can a classical verifier certify that the prover has indeed deleted all information associated with a complementary computational basis measurement? Because quantum measurement is an inherently destructive process, we expect that a Fourier basis immediately renders the result of a hypothetical computational basis measurement impossible to predict.

We prove *entropic uncertainty relations* which capture the intuitive property that it is impossible to simultaneously measure a Gaussian coset state in two incompatible bases. Let $r > 0$. To model the prover's uncertainty about the uniformly random vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_q^m$ encoded in the Gaussian coset state in Eq. (4), we consider the following classical-classical-quantum (CCQ) state given by

$$\sigma_{UVB} = \sum_{\boldsymbol{u} \in \mathbb{Z}_q^m} q^{-m} |\boldsymbol{u}\rangle \langle \boldsymbol{u}|_U \otimes \sum_{\boldsymbol{v} \in \mathbb{Z}_q^m} q^{-m} |\boldsymbol{v}\rangle \langle \boldsymbol{v}|_V \otimes |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle \langle \mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B \,. \tag{5}$$

Here, we imagine that the verifier has access to the classical systems U and V, whereas the prover receives the quantum system B. In Theorem 3, we prove the following uncertainty relation for Gaussian coset states.

Theorem (informal): *Let σ_{UVB} be the CCQ state in Eq. (5) and $\Phi_{B \to WE}$ an arbitrary quantum channel with outcome $\sigma_{UVWE} = (\mathbb{1}_A \otimes \Phi_{B \to WE})(\sigma_{UVB})$. Then, the marginals σ_{UE} and σ_{VW} satisfy*

$$H_{\min}^{\varepsilon}(U \mid E)_\sigma + H_{\max}^{\bar{\varepsilon}}(V \mid W)_\sigma \geq m \cdot \log(q).$$

where $\varepsilon > 0$ and $\bar{\varepsilon} := \varepsilon/2$ are smoothing parameters which represent the probability of failure and where $H_{\min}^{\varepsilon}(U \mid E)$ and $H_{\max}^{\bar{\varepsilon}}(V \mid W)$ are the (smooth) min- and max-entropies (Definition 8).

The intuition behind the uncertainty relation above is the following. Suppose that a (possibly malicious) prover maps a random Gaussian coset state in system B into registers W and E using an arbitrary quantum channel $\Phi_{B \to WE}$. Then, if register W is correlated with the verifier's system V (which is associated with a *Fourier basis* measurement outcome), the auxiliary system E must reveal close to no information about the verifier's system U (associated with a *computational basis* measurement outcome). In particular, from an upper bound on the max-entropy (which we can easily obtain as a consequence of the strong correlation between V and W, see Lemma 16), we are able to deduce a lower bound on the min-entropy of U given E.

The main idea behind the proof of our uncertainty relations for Gaussian coset states is to switch to an *entanglement-based setting* when interacting with a prover. This gives us a precise handle on the measurements performed by the prover and allows us to state uncertainty relations much more conveniently. To this end, we consider a *purification* of the uniformly random Gaussian coset state given by

$$\sigma_B = \mathrm{tr}_{UV}[\sigma_{UVB}] = q^{-2m} \sum_{\boldsymbol{u},\boldsymbol{v} \in \mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle \langle \mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B \,. \tag{6}$$

Namely, we introduce a joint system AB and consider the *entangled Gaussian cosets pair* given by

$$|\mathcal{D}_r\rangle_{AB} \propto \sum_{\boldsymbol{u},\boldsymbol{v} \in \mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},-\boldsymbol{v}}\rangle_A \otimes |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle_B \,. \tag{7}$$

The bipartite state $|\mathcal{D}_r\rangle_{AB}$ is indeed a purification of $\sigma_B = \mathrm{tr}_{UV}[\sigma_{UVB}]$, which we show in Lemma 13. Whenever we trace out one half of the state, say system A, the other half of the state in system B immediately collapses to a random Gaussian coset, as required.

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 $x \cdot \frac{q}{2}$ that depends on the plaintext $x \in \{0, 1\}$. Using Gaussian coset states, we can encode Dual-Regev ciphertexts for the purpose of certified deletion while simultaneously preserving their cryptographic functionality.

We sketch our scheme (formally defined in Construction 2) below.

Dual-Regev public-key encryption with certified deletion. Let n, m be integers with $m \geq n$, let $q \geq 2$ be a power of 2 modulus and $\alpha \in (0,1)$. The scheme consists of the following efficient algorithms:

- To generate a pair of keys $(\mathsf{sk}, \mathsf{pk})$, we sample a random string $\boldsymbol{e}_{\mathsf{sk}} \xleftarrow{\$} \{0,1\}^m$ and a random matrix $\bar{\boldsymbol{A}} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$ and output $\mathsf{sk} = (-\boldsymbol{e}_{\mathsf{sk}}, 1) \in \mathbb{Z}_q^{m+1}$ and $\mathsf{pk} = \boldsymbol{A} \in \mathbb{Z}_q^{(m+1)\times n}$ which is a matrix composed of $\bar{\boldsymbol{A}}$ (the first m rows) and $\bar{\boldsymbol{A}}^T \cdot \boldsymbol{e}_{\mathsf{sk}} \pmod q$ (the last row).
- To encrypt a bit $x \in \{0,1\}$ using the public-key pk, we choose random vectors $\boldsymbol{s} \xleftarrow{\$} \mathbb{Z}_q^n$ and $\boldsymbol{v} \xleftarrow{\$} \mathbb{Z}_q^{m+1}$, sample an error vector $\boldsymbol{e}_0 \sim D_{\mathbb{Z}^{m+1},\alpha q}$, and output the ciphertext $|\mathsf{ct}\rangle$ given by
$$|\mathsf{ct}\rangle = \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} \sqrt{D_{\mathbb{Z}_q^{m+1},\beta q}(\boldsymbol{e})}\, \omega_q^{-\langle \boldsymbol{e}, \boldsymbol{v} \rangle} \, |\boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}_0 + \boldsymbol{e} + (0, \dots, 0, x \cdot q/2) \pmod q \rangle .$$
- To decrypt a ciphertext $|\mathsf{ct}\rangle$, we measure in the computational basis to obtain an outcome $\boldsymbol{c}$, compute $\tilde{c} = \mathsf{sk}^T \cdot \boldsymbol{c} \in \mathbb{Z}_q$ and output 0, if $\tilde{c}$ is closer to 0 than to $\frac{q}{2} \pmod q$, and we output 1, otherwise.

Notice that $|\mathsf{ct}\rangle$ is a Gaussian coset that resembles the ciphertext of the classical Dual-Regev encryption scheme, except for a phase that depends on the verification key $\boldsymbol{v}$. To delete the ciphertext $|\mathsf{ct}\rangle$, the prover simply measures each qudit in the q-ary Fourier basis to obtain a proof $\pi \in \mathbb{Z}_q^{m+1}$, similar to our quantum proof-of-deletion protocol for LWE. According to the Gaussian Switching Lemma (Lemma 11), we have

$$\mathsf{FT}_q \, |\mathsf{ct}\rangle \;\approx \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} \sqrt{D_{\mathbb{Z}_q^{m+1},1/2\beta}(\boldsymbol{e})}\, \omega_q^{\langle \boldsymbol{e}, \boldsymbol{A}\cdot \boldsymbol{s} + \boldsymbol{e}_0 + (0,\dots,0,x\cdot q/2)\rangle} \, |\boldsymbol{v} + \boldsymbol{e} \pmod q\rangle . \tag{8}$$

Hence, a measurement of $|\mathsf{ct}\rangle$ in the Fourier basis yields a sample $\pi \sim D_{\mathbb{Z}_q^{m+1}-\boldsymbol{v},1/2\beta}$ from the shifted Gaussian with parameter $1/2\beta$ centered around $\boldsymbol{v} \in \mathbb{Z}_q^{m+1}$. To verify π, the verifier simply checks whether the vectors π and $\boldsymbol{v}$ are sufficiently correlated.

Our first observation is that an honest prover collapses the ciphertext $|\mathsf{ct}\rangle$ to a measurement outcome π that is completely *independent* of the LWE sample (as well as the plaintext $x \in \{0,1\}$). This is due to the fact that the Fourier transform maps the LWE sample into the phase of the Gaussian coset in Eq. (8). Therefore, we can conclude that our scheme $\mathsf{DualPKE}_{\mathsf{CD}}$ satisfies the notion of *indistinguishable ciphertexts* (formally defined in Definition 30) in the semi-honest adversarial model (in which the adversary is honest) even if the secret key is later revealed once deletion has taken place. We prove the following result:

Theorem (informal): *The Dual-Regev* PKE *scheme with certified deletion (see Construction 2) is* IND-CPA-CD*-secure in the semi-honest adversarial model.*

Unfortunately, proving security in the plain adversarial model is highly non-trivial. This is mainly due to the fact that we have to perform a reduction from (decisional) LWE to the IND-CPA-CD security (formally defined in Definition 30) of our $\mathsf{DualPKE}_{\mathsf{CD}}$ scheme. But in order to simulate the IND-CPA-CD game successfully, we have to eventually forward the LWE secret key in order to run the adversary once deletion has taken place. Notice, however, that reduction has no way of knowing the LWE secret key, as it is trying to break the underlying (decisional) LWE problem 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 a *fake* secret key. In our case, we cannot rely on similar techniques involving RNC encryption as it seems difficult to reconcile with homomorphic encryption, which is the main focus of this work.

Our second observation is that our entropic uncertainty relations for Gaussian cosets help limit the ability of a malicious adversary to guess the delegated ciphertext once deletion has taken place. Because the ciphertext $|\mathsf{ct}\rangle$ in our construction is indistinguishable from a random Gaussian coset, any adversary that obtains a measurement outcome associated with the Fourier basis is unlikely to guess the outcome of a hypothetical computational basis measurement. We formalize this using the notion of *quantum guessing pseudoentropy* – a computational analogue of *quantum min-entropy*. [CCL+17] (see Definition 10).

Fully homomorphic encryption with certified deletion. Our (leveled) FHE scheme with certified deletion is based on the (classical) Dual-Regev leveled FHE scheme introduced by Mahadev [Mah18b] which is a variant of the scheme due to Gentry, Sahai and Waters [GSW13].

Dual-Regev leveled fully homomorphic encryption. Let n, m be integers with $m \geq n$, let $q \geq 2$ be a power of 2 modulus, and let $\alpha \in (0,1)$ be the noise ratio. Let $N = (m+1)\log(q)$ and let $\boldsymbol{G} \in \mathbb{Z}_q^{(m+1)\times N}$ denote the *gadget matrix* (defined in Section 9.1) that converts a binary representation of a vector back to its ring representation over $\mathbb{Z}_q$. The scheme consists of the following efficient algorithms:

- To encrypt a bit $x \in \{0,1\}$, parse the public key as $\boldsymbol{A} \leftarrow \mathsf{pk}$, sample random vectors $\boldsymbol{S} \xleftarrow{\$} \mathbb{Z}_q^{n\times N}$ and $\boldsymbol{E}_0 \sim D_{\mathbb{Z}^{(m+1)\times N}, \alpha q}$, and output $\mathsf{ct} = \boldsymbol{A}\cdot\boldsymbol{S} + \boldsymbol{E}_0 + x\boldsymbol{G} \pmod{q} \in \mathbb{Z}_q^{(m+1)\times N}$.
- To apply a NAND gate on ciphertexts ct_0 and ct_1, output the ciphertext $\boldsymbol{G} - \mathsf{ct}_0 \cdot \boldsymbol{G}^{-1}(\mathsf{ct}_1) \pmod{q}$.
- To decrypt a ciphertext ct, compute $c = \mathsf{sk}^T \cdot \mathsf{ct}_N \in \mathbb{Z}_q$, where $\mathsf{ct}_N \in \mathbb{Z}_q^{m+1}$ is the N-th column of ct, and then output 0, if c is closer to 0 than to $\frac{q}{2} \pmod{q}$, and output 1, otherwise.

The 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 $x \cdot \boldsymbol{G}$ that depends on the plaintext $x \in \{0,1\}$. This property allows us to extend the Dual-Regev PKE scheme with certified deletion towards a (leveled) FHE scheme.

Our leveled fully homomorphic encryption scheme with certified deletion. Let us now briefly sketch our scheme which we denote by $\mathsf{DualFHE}_{\mathsf{CD}}$ (formally defined in Construction 3). To encrypt a bit $x \in \{0,1\}$, we first generate a verification key vk by sampling a random matrix $\boldsymbol{V} \xleftarrow{\$} \mathbb{Z}_q^{(m+1)\times N}$ with $\mathsf{vk} \leftarrow \boldsymbol{V}$ and output the *quantum* ciphertext $|\mathsf{ct}\rangle$ with $\boldsymbol{A} \leftarrow \mathsf{pk}$ and $\boldsymbol{S} \xleftarrow{\$} \mathbb{Z}_q^{n\times N}$ given by

$$|\mathsf{ct}\rangle = \sum_{\boldsymbol{E}\in\mathbb{Z}_q^{(m+1)\times N}} \sqrt{D_{\mathbb{Z}_q^{(m+1)\times N}, \beta q}(\boldsymbol{E})}\, \omega_q^{-\mathrm{tr}[\boldsymbol{E}^T\boldsymbol{V}]}\, |\boldsymbol{A}\cdot\boldsymbol{S} + \boldsymbol{E}_0 + \boldsymbol{E} + x\boldsymbol{G} \pmod{q}\rangle\,. \tag{9}$$

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 ct_0 and ct_1 are ciphertexts that encrypt two bits x_0 and x_1, respectively, then the outcome $\mathsf{ct} = \boldsymbol{G} - \mathsf{ct}_0 \cdot \boldsymbol{G}^{-1}(\mathsf{ct}_1) \pmod{q}$ is an encryption of $\mathsf{NAND}(x_0, x_1) = 1 - x_0 \cdot x_1$. 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 still allows for the decryption of the ciphertext 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_{NAND} in Definition 36 which allows us to apply a NAND gate directly onto Gaussian cosets as in Eq. (9). Consider two ciphertexts $|\mathsf{ct}_0\rangle$ and $|\mathsf{ct}_1\rangle$ in systems C_0 and C_1, respectively. Applying the homomorphic NAND gate via the unitary U_{NAND} results in an output state ct in systems $C_0 C_1 C_{\mathsf{out}}$ such that

$$U_{\mathsf{NAND}}: \quad |\mathsf{ct}_0\rangle_{C_0} \otimes |\mathsf{ct}_1\rangle_{C_1} \otimes |\mathbf{0}\rangle_{C_{\mathsf{out}}} \quad \rightarrow \quad |\mathsf{ct}\rangle_{C_0 C_1 C_{\mathsf{out}}}. \tag{10}$$

Just as in the (classical) Dual-Regev FHE scheme, the basis states of the state $|\mathsf{ct}\rangle$ in system C_{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_{out} in order to learn the ciphertext that corresponds to an encryption of $\mathsf{NAND}(x_0, x_1) = 1 - x_0 \cdot x_1$. Notice, however, that the new ciphertext $|\mathsf{ct}\rangle$ is now a highly entangled state since the unitary operation U_{NAND} induces entanglement between the Gaussian noise terms with distribution $D_{\mathbb{Z}_q^{(m+1)\times N}, \beta q}$. 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 coset 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_{NAND} gates starting from the ciphertext $|\mathsf{ct}\rangle = |\mathsf{ct}_1\rangle \otimes \dots \otimes |\mathsf{ct}_\ell\rangle$ in system C_{in} which corresponds to an encryption of $x = (x_1, \dots, x_\ell) \in \{0,1\}^\ell$, the prover simply sends the quantum system C_{out} containing an encryption of $C(x)$ to the verifier. Then, using the secret key sk (or, a trapdoor for the public matrix pk), it is possible for the verifier to *extract* the outcome $C(x)$ from the system C_{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_{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_{aux}) which mark intermediate applications of the gate U_{NAND}. In order to allow for a quantum proof of deletion, the verifier must now return the system C_{out} to the prover. Having access to all three systems $C_{\mathsf{in}} C_{\mathsf{aux}} C_{\mathsf{out}}$, 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_{in} (up to negligible trace distance). Since the ciphertext in the prover's possession is now approximately a simple product of Gaussian cosets, the prover can perform a Fourier basis measurement of systems C_{in}, as required. Once the protcol 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 11.

Theorem (informal): *Our Dual-Regev (leveled)* FHE *scheme with certified deletion (formally defined in Construction 4) is* $\mathsf{IND\text{-}CPA\text{-}CD}$*-secure in the semi-honest adversarial model.*

As in our Dual-Regev PKE scheme with certified deletion, we can use entropic uncertainty relations to additionally argue that, if the adversary obtains a measurement outcome associated with the Fourier basis, the adversary is unlikely to guess the outcome of a hypothetical computational basis measurement.

1.3 Open problems

Our results leave open many interesting future research directions. For example, is it possible to prove the IND-CPA-CD security of our (leveled) Dual-Regev FHE scheme with certified deletion in the standard adversarial model? One possible direction is to use *receiver non-committing* (RNC) encryption, similar to the work of Hiroka, Morimae, Nishimaki and Yamakawa [HMNY21a] in the context of public-key encryption with certified deletion. 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 [Mah18b] on delegating quantum computations, as well as recent work on classically-instructed parallel remote state preparation by Gheorghiu, Metger and Poremba [GMP22].

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* originally 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. Building on the conjugate coding protocol of Coiteux-Roy and Wolf [CRW19], Broadbent and Islam [BI20] were able to construct a quantum encryption scheme with certified deletion whose security proof is similar to that of QKD [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] were able to extend 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] and *noisy trapdoor claw-free* (NTCF) functions, which were first introduced in [BCM$^+$21] in the context of certifiable randomness. The encryption schemes proposed by Hiroka, Morimae, Nishimaki and Yamakawa [HMNY21b] enjoy very strong security guarantees at the expense of functionality; in particular, none of the constructions are known to support computations on encrypted data. Hiroka et al. [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 crytography in a way that loosely resembles our use of *Gaussian coset states*.

1.5 Acknowledgments

The author would like to thank Thomas Vidick for many useful discussions and suggestions on this draft. The author is partially supported by AFOSR YIP award number 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. The author is also grateful for many useful comments and suggestions made by anonymous reviewers.

2 Preliminaries

Notation. All logarithms are always with respect to base 2. For $x \in \{0,1\}^n$, we denote the Hamming weight of x by $\omega(x)$. For $\boldsymbol{A} \in \mathbb{C}^{n\times n}$, we denote the operator norm by $\|\boldsymbol{A}\|_\infty$. For $x \in \mathbb{C}^n$, we denote the ℓ^2 norm by $\|\boldsymbol{x}\|_2$. For $\boldsymbol{x} \in \mathbb{Z}^n$, we occasionally also use the max norm $\|\boldsymbol{x}\|_\infty = \max_i |x_i|$. 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 $x \xleftarrow{\$} \mathcal{X}$ denotes sampling of an element 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 $p(n)$.

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 $|\psi\rangle \in \mathcal{H}$ over the finite-dimensional complex Hilbert space $\mathcal{H}$ is denoted as $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$. 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 $\mathcal{H} = \left(\mathbb{C}^2\right)^{\otimes n}$ 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 $\mathcal{H}$. We define the space of positive semidefinite operators over a Hilbert space $\mathcal{H}$ with trace norm not exceeding 1 as $\mathcal{S}_{\leq}(\mathcal{H})$.

Let $q \geq 2$ be an integer modulus. When $n \in \mathbb{N}$ is clear out of context, we use the following notation for the q-ary maximally entangled state $|\phi_q^+\rangle_{AB} \in \mathcal{H}_{AB}$ on n-qudits,

$$|\phi_q^+\rangle_{AB} = \sqrt{q^{-n}} \sum_{\boldsymbol{x}\in\mathbb{Z}_q^n} |\boldsymbol{x}\rangle_A \otimes |\boldsymbol{x}\rangle_B \,.$$

For $q = 2$, the state is equal to the standard n-qubit Einstein-Podolsky-Rosen (EPR) pair [EPR35]. The *trace distance* of two density matrices $\varrho, \sigma \in \mathcal{D}(\mathcal{H})$ is given by

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

We make use of the following inequality between the trace distance and the ℓ^2 distance over $(\mathbb{C}^q)^{\otimes m}$,

$$\| \, |\psi\rangle - |\phi\rangle \, \|_{\mathrm{tr}} \leq \| \, |\psi\rangle - |\phi\rangle \, \|_2, \qquad \forall \, |\psi\rangle \, , |\phi\rangle \in (\mathbb{C}^q)^{\otimes m}.$$

We define the *purified distance* as $P(\varrho,\sigma) = \sqrt{1 - F(\varrho,\sigma)^2}$, where $F(\varrho,\sigma) = \|\sqrt{\varrho}\sqrt{\sigma}\|_1$ denotes the fidelity. We denote by $\mathcal{B}^\varepsilon(\mathcal{H},\varrho)$ the ε-ball of density matrices in $\mathcal{D}(\mathcal{H})$ with purified distance at most ε with respect to ϱ. Sometimes, we use the compact notation $\varrho \approx_\varepsilon \sigma$ which means that $\|\varrho - \sigma\|_{\mathrm{tr}} \leq \varepsilon$, for some $\varepsilon \in [0,1]$. 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 $P_\mathcal{X}$ over the set $\mathcal{X}$, then all possible joint states ϱ_{XB} can be expressed as

$$\varrho_{XB} = \sum_{x \in \mathcal{X}} P_\mathcal{X}(x) |x\rangle\langle x|_X \otimes \varrho_B^x.$$

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 Φ 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 $\mathrm{Tr}[\Phi(X)] = \mathrm{Tr}[X]$, for all $X \in L(\mathcal{H})$. A quantum channel that is both completely positive and trace-preserving is called a quantum CPTP channel. A simple example of a CPTP channel which we consider in this work is the so-called *classical* channel $\mathcal{N} : L(\mathcal{H}_X) \to L(\mathcal{H}_Y)$ of the form

$$\mathcal{N}_{X \to Y}(\varrho) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P(x\,|\,y)\ |y\rangle\langle y| \cdot \mathrm{tr}\Big[|x\rangle\langle x|\varrho\Big], \qquad \forall \varrho \in L(\mathcal{H}_X).$$

Let $\mathcal{X}$ be a set. A *generalized measurement* on a system A is a set of linear operators $\{M_A^x\}_{x \in \mathcal{X}}$ such that

$$\sum_{x \in \mathcal{X}} (M_A^x)^\dagger (M_A^x) = \mathbb{1}_A.$$

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

$$\mathcal{M}_{A \to X} : \quad \varrho_{AB} \quad \mapsto \quad \sum_{x \in \mathcal{X}} |x\rangle\langle x|_X \otimes \mathrm{tr}_A \left[M_A^x \varrho_{AB} {M_A^x}^\dagger\right],$$

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 $\{M_A^x\}_{x \in \mathcal{X}}$ such that

$$\sum_{x \in \mathcal{X}} M_A^x = \mathbb{1}_A.$$

Oftentimes, we identify a POVM $\{M_A^x\}_{x \in \mathcal{X}}$ with an associated generalized measurement $\{\sqrt{M_A^x}\}_{x \in \mathcal{X}}$. The *overlap* c of two POVMs $\{M_A^x\}_{x \in \mathcal{X}}$ and $\{N_A^y\}_{y \in \mathcal{X}}$ acting on a quantum system A is defined by

$$\mathsf{c} = \max_{x,y} \left\| \sqrt{M_A^x} \sqrt{N_A^y} \right\|_\infty^2.$$

We say that two measurements are *mutually unbiased*, if the overlap satisfies $\mathsf{c} = 1/d$, 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 $\mathcal{C} = \bigcup_{n \in \mathbb{N}} C_n$, where each circuit $C \in \mathcal{C}$ 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 $\Pr[\mathcal{A}(1^\lambda) = 1]$ for a QPT algorithm $\mathcal{A}$, it is implicit that $\mathcal{A}$ 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 $\varrho \in \mathcal{H}_{A_\lambda}$,*

$$\Phi_\lambda(\varrho_\lambda) = \mathrm{Tr}_{A_\lambda C_\lambda}[C_\lambda(\varrho_\lambda \otimes |0\rangle\langle 0|_{B_\lambda C_\lambda})].$$

Definition 2 (Indistinguishability of ensembles of random variables). *Let $\lambda \in N$ 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 $\mathcal{D}$ which output a single bit, it holds that*

$$\big|\Pr[\mathcal{D}(1^\lambda, X_\lambda) = 1] - \Pr[\mathcal{D}(1^\lambda, Y_\lambda) = 1]\big| \leq \mathrm{negl}(\lambda)\,.$$

Definition 3 (Indistinguishability of ensembles of quantum states, [Wat06]). *Let $p : \mathbb{N} \to \mathbb{N}$ be a polynomially bounded function, and let ϱ_λ and σ_λ 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 $\mathcal{D}$ with single-bit output, any polynomially bounded $q : \mathbb{N} \to \mathbb{N}$, any family of $q(\lambda)$-qubit auxiliary states $\{\nu_\lambda\}_{\lambda\in\mathbb{N}}$, and every $\lambda \in \mathbb{N}$,*

$$\big|\Pr[\mathcal{D}(1^\lambda, \varrho_\lambda \otimes \nu_\lambda) = 1] - \Pr[\mathcal{D}(1^\lambda, \sigma_\lambda \otimes \nu_\lambda) = 1]\big| \leq \mathrm{negl}(\lambda)\,.$$

We say that $\mathcal{D}$ is a (T, ε) distinguisher if it runs in time $T(\lambda)$ and succeeds with probability at most $\varepsilon(\lambda)$.

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 $(\Pi_0, \Pi_1 = \mathbb{1} - \Pi_0)$ be projectors acting on $\mathcal{H} \otimes \mathcal{H}_{\mathsf{aux}}$. We interpret (U, Π_0, Π_1) as a measurement performed by appending an ancillary system in the state $|0\rangle\langle 0|_{\mathsf{aux}}$, 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 Π_0 occurs with probability $1 - \varepsilon$, for some $\varepsilon \in [0, 1]$. In other words, it holds that $\mathrm{Tr}[\Pi_0(U\varrho \otimes |0\rangle\langle 0|_{\mathsf{aux}} U^\dagger)] = 1 - \varepsilon$. Then,*

$$\|\widetilde{\varrho} - \varrho\|_{\mathrm{tr}} \leq \sqrt{\varepsilon},$$

where $\widetilde{\varrho}$ is the state after performing the measurement and applying $U^\dagger$, and after tracing out $\mathcal{H}_{\mathsf{aux}}$:

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

2.2 Classical and quantum entropies

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

$$H_{\min}(X) = -\log\left(\max_{x\in\mathcal{X}} \Pr_{X\sim P_{\mathcal{X}}}[X = x]\right).$$

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

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

Computational entropies. We use the following computational analogue of min-entropy.

Definition 4 (Computational pseudoentropy, [HILL99])**.** *Let $\lambda \in \mathbb{N}$. We say that an ensemble of random variables $\{X_\lambda\}$ has computational (*HILL*) pseudoentropy at least $k(\lambda)$, denoted by $H_{\mathsf{HILL}}(X_\lambda) \geq k(\lambda)$, if $\{X_\lambda\}$ and $\{Y_\lambda\}$ are computationally indistinguishable, i.e. $X_\lambda \approx_c Y_\lambda$, and $H_{\min}(Y_\lambda) \geq k(\lambda)$.*

Similar to the notion of *conditional min-entropy*, we also define the following computational analogue.

Definition 5 (Conditional computational pseudoentropy, [HILL99])**.** *Let $\lambda \in \mathbb{N}$. Let $\{X_\lambda\}$ and $\{Y_\lambda\}$ be ensembles of jointly distributed random variables. $\{X_\lambda\}$ has computational (*HILL*) pseudoentropy conditioned on $\{Y_\lambda\}$ at least $k(\lambda)$, denoted by $H_{\mathsf{HILL}}(X_\lambda|Y_\lambda) \geq k(\lambda)$, if there exists an ensemble of random variables $\{X'_\lambda\}$ jointly distributed with $\{Y_\lambda\}$ such that $(X_\lambda, Y_\lambda) \approx_c (X'_\lambda, Y_\lambda)$ and $H_{\min}(X'_\lambda|Y_\lambda) \geq k(\lambda)$.*

Quantum entropies.

Definition 6 (Min-entropy)**.** *Let A and B be two quantum systems and let $\varrho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ be any bipartite state. The min-entropy of A conditioned on B of the state ϱ_{AB} is defined as*

$$H_{\min}(A\,|\,B)_\varrho = \max_{\sigma \in \mathcal{S}_{\leq}(\mathcal{H}_B)} \sup \left\{ \lambda \in \mathbb{R} \,:\, \varrho_{AB} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B \right\}.$$

Definition 7 (Max-entropy)**.** *Let A and B be two quantum systems and let $\varrho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ be any bipartite state. The max-entropy of A conditioned on B of the state ϱ_{AB} is defined as*

$$H_{\max}(A\,|\,B)_\varrho = -H_{\min}(A\,|\,C)_\varrho$$

where $\varrho_{ABC} \in \mathcal{S}_{\leq}(\mathcal{H}_{ABC})$ is a purification with $\mathrm{Tr}_C[\varrho_{ABC}] = \varrho_{AB}$, for some quantum system C.

Definition 8 (Smooth min- and max-entropies)**.** *Let A and B be quantum systems and let $\varrho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$. Let $\varepsilon \geq 0$. We define the ε-smooth min- and max-entropies of A conditioned on B of ϱ_{AB} as*

$$\begin{aligned} H^\varepsilon_{\min}(A\,|\,B)_\varrho &= \sup_{\substack{\tilde{\varrho}_{AB} \\ P(\tilde{\varrho}_{AB}, \varrho_{AB}) \leq \varepsilon}} H_{\min}(A\,|\,B)_{\tilde{\varrho}}, \\ H^\varepsilon_{\max}(A\,|\,B)_\varrho &= \inf_{\substack{\tilde{\varrho}_{AB} \\ P(\tilde{\varrho}_{AB}, \varrho_{AB}) \leq \varepsilon}} H_{\max}(A\,|\,B)_{\tilde{\varrho}}. \end{aligned}$$

Lemma 2 ([TSSR11])**.** *Let $\varepsilon > 0$ and $\varrho \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_B)$ be a CQ state with a classical register X, where*

$$\varrho_{XB} = \sum_{x \in \mathcal{X}} P_{\mathcal{X}}(x)\, |x\rangle\langle x|_X \otimes \varrho^x_B.$$

Then, the state $\varrho^*_{XB} \in \mathcal{B}^\varepsilon(\mathcal{H}_X \otimes \mathcal{H}_B, \varrho)$ that optimizes the smooth min-entropy, i.e. where

$$H^\varepsilon_{\min}(X\,|\,B)_\varrho = H_{\min}(X\,|\,B)_{\varrho^*},$$

is of the same CQ form as the quantum state ϱ_{XB}.

Theorem 1 (Data-processing inequality, [Tom13])**.** *Let $\varrho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be any bipartite state. Let $\mathcal{E}_{A \to A'}$ and $\mathcal{F}_{B \to B'}$ be arbitrary* CPTP *maps and let $\sigma_{A'B'} = (\mathcal{E}_{A \to A'} \otimes \mathcal{F}_{B \to B'})(\varrho_{AB})$. Let $\varepsilon \geq 0$. Then,*

$$H^\varepsilon_{\min}(A\,|\,B)_\varrho \leq H^\varepsilon_{\min}(A'\,|\,B')_\sigma \quad \textit{and} \quad H^\varepsilon_{\max}(A\,|\,B)_\varrho \leq H^\varepsilon_{\max}(A'\,|\,B')_\sigma.$$

Lemma 3 ([TL17])**.** *Let ϱ_{AX} be a CQ state with a classical register X, and let $\Omega : X \to \{0,1\}$ be an event with $\Pr[\Omega]_\varrho = \varepsilon < \mathrm{Tr}[\varrho_{AX}]$. Then, there exists a CQ state $\tilde{\varrho}_{AX}$ with $\Pr[\Omega]_{\tilde{\varrho}} = 0$ and $P(\varrho_{AX}, \tilde{\varrho}_{AX}) \leq \sqrt{\varepsilon}$.*

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

Definition 9 (Guessing probability)**.** *Let $\varrho_{XB} \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_B)$ 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*

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

Moreover, if $\mathcal{A}$ is a quantum algorithm with access to system B, where $\mathcal{A}$ is characterized by a particular set of generalized measurements $\{M_B^x\}$, we occasionally use the notation $p_{\text{guess},\mathcal{A}}(X|B)_\varrho$.

Computational notions of quantum min-entropy. Let us now introduce computational variants of the quantum entropies we defined previously, similar to the classical notion of *pseudoentropy* in Definition 5.

Proposition 1. *Let ϱ_{XB} be a CQ state, where X is classical. Suppose that ϱ_{XB} is (T, ε)-indistinguishable from a state σ_{XB} that is of the same CQ form. Then, for every quantum circuit $\mathcal{A}$ of size at most T:*

$$|p_{\text{guess},\mathcal{A}}(X|B)_\varrho - p_{\text{guess},\mathcal{A}}(X|B)_\sigma| \leq \varepsilon.$$

Proof. Fix an adversary $\mathcal{A}$ running in time T that tries to guess the outcome X given as input a quantum system B. Consider the following distinguisher $\mathcal{D}$:

1. $\mathcal{D}$ receives as input a CQ state on XB, measures the classical system X in the computational basis and records the outcome as x. $\mathcal{D}$ then runs the algorithm $\mathcal{A}$ with system B as input.
2. $\mathcal{A}$ generates a guess x' by performing an appropriate measurement on system B.
3. $\mathcal{D}$ outputs 1 if $x' = x$.

Since $\mathcal{A}$ runs in quantum time T, so does the distinguisher $\mathcal{D}$. Further, by construction we have that

$$|p_{\text{guess},\mathcal{A}}(X|B)_\varrho - p_{\text{guess},\mathcal{A}}(X|B)_\sigma| = |\Pr[\mathcal{D}(\varrho_x) = 1] - \Pr[\mathcal{D}(\sigma_x) = 1]|. \tag{11}$$

By the assumption that ϱ_{XB} and σ_{XB} are (T, ε)-indistinguishable, we conclude that the advantage of the distinguisher $\mathcal{D}$ in Eq. (11) is at most ε for every $x \in \mathcal{X}$. This proves the claim. □

Lemma 4. *Let ϱ_{XB} be a CQ state, where X is classical, and suppose that ϱ_{XB} is (T, ε)-indistinguishable from a state σ_{XB} that is of the same CQ form. Then, for every quantum circuit $\mathcal{A}$ of size at most T:*

$$p_{\text{guess},\mathcal{A}}(X|B)_\varrho \leq 2^{-H_{\min}(X|B)_\sigma} + \varepsilon.$$

Proof. This follows immediately from Proposition 1. □

The following notion of quantum guessing pseudoentropy is implicit in Proposition 1 and Lemma 4.

Definition 10 (Quantum guessing pseudoentropy, [CCL+17])**.** *Let ϱ_{XB} be a CQ state, where X is classical. We say that X conditioned on B has (T, ε) quantum guessing pseudoentropy $H^{T,\varepsilon}_{\text{guess}}(X|B)_\varrho \geq \kappa$ if, for all quantum circuits $\mathcal{A}$ running in time T, it holds that*

$$p_{\text{guess},\mathcal{A}}(X|B)_\varrho \leq 2^{-\kappa} + \varepsilon.$$

Lemma 5. *Let $\varrho_{XB}, \sigma_{XB} \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_B)$ be CQ states with a classical register X and suppose that $\|\varrho_{XB} - \sigma_{XB}\|_{\text{tr}} \leq \varepsilon$, for some $\varepsilon \in [0, 1]$. Then,*

$$|p_{\text{guess}}(X|B)_\varrho - p_{\text{guess}}(X|B)_\sigma| \leq \varepsilon.$$

Proof. By the assumption that $\|\varrho_{AB} - \sigma_{AB}\|_{\text{tr}} \leq \varepsilon$, we obtain

$$\begin{aligned}
|p_{\text{guess}}(X|B)_\varrho - p_{\text{guess}}(X|B)_\sigma| &= \left| \sup_{\{\mathcal{M}^x_B\}} \sum_x p_x \text{Tr}[\mathcal{M}^x_B \varrho_B] - \sup_{\{\mathcal{N}^x_B\}} \sum_x q_x \text{Tr}[\mathcal{N}^x_B \sigma_B] \right| \\
&\leq \sup_{\{\mathcal{E}^x_B\}} \sum_x \text{Tr}[\mathcal{E}^x_B (p_x \varrho_B - q_x \sigma_B)] \\
&= \sum_x \|p_x \varrho_B - q_x \sigma_B\|_{\text{tr}} \\
&= \|\varrho_{XB} - \sigma_{XB}\|_{\text{tr}} \quad \leq \quad \varepsilon.
\end{aligned}$$

□

Lemma 6. *Let $\varrho, \sigma \in \mathcal{D}(\mathcal{H})$ be two quantum states with the property that $\|\varrho - \sigma\|_{\text{tr}} \leq \varepsilon$, for some $\varepsilon > 0$. Let Π be an arbitrary matrix acting on $\mathcal{H}$ such that $0 \leq \Pi \leq \mathbb{1}$. Then,*

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

Proof. From the standard identity $\|\varrho - \sigma\|_{\text{tr}} = \max_{0 \leq \Lambda \leq \mathbb{1}} \text{Tr}[\Lambda(\sigma - \varrho)]$, we obtain

$$|\text{Tr}[\Pi\varrho] - \text{Tr}[\Pi\sigma]| \;\leq\; \max_{0 \leq \Lambda \leq \mathbb{1}} \text{Tr}[\Lambda(\sigma - \varrho)] \;=\; \|\varrho - \sigma\|_{\text{tr}} \;\leq\; \varepsilon.$$

□

We use the following entropic uncertainty relation due to Tomamichel [Tom13].

Proposition 2 ([Tom13])**.** *Let $\varrho_{ACE} \in \mathcal{S}_{\leq}(\mathcal{H}_{ACE})$ be a tripartite quantum state, and let $\{M^x_A\}_{x \in \mathcal{X}}$ and $\{N^y_A\}_{y \in \mathcal{Y}}$ be* POVM*s. Let $\varepsilon \geq 0$. Then, the post-measurement CQ states*

$$\varrho_{XCE} = \sum_x |x\rangle\langle x| \otimes \text{Tr}_A \left[\sqrt{M^x_A} \varrho_{ACE} \sqrt{M^x_A} \right],$$

and

$$\varrho_{YCE} = \sum_y |y\rangle\langle y| \otimes \text{Tr}_A \left[\sqrt{N^y_A} \varrho_{ACE} \sqrt{N^y_A} \right],$$

satisfy the entropic uncertainty relation

$$H^\varepsilon_{\min}(X \,|\, C)_\varrho + H^\varepsilon_{\max}(Y \,|\, E)_\varrho \geq \log(1/\mathsf{c}),$$

where the overlap c *is defined by:*

$$\mathsf{c} = \max_{x,y} \left\| \sqrt{M^x_A} \sqrt{N^y_A} \right\|_\infty.$$

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 $f : \mathbb{Z}^m \to \mathbb{C}$ and produces a function $\hat{f} : \mathbb{Z}_q^m \to \mathbb{C}$ (the Fourier transform of f) defined by

$$\hat{f}(\boldsymbol{y}) = \sum_{\boldsymbol{x} \in \mathbb{Z}^m} f(x) \cdot e^{\frac{2\pi i}{q}\langle \boldsymbol{y}, \boldsymbol{x} \rangle}.$$

For brevity, we oftentimes write $\omega_q = e^{\frac{2\pi i}{q}} \in \mathbb{C}$ 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,

$$\mathsf{FT}_q : \quad |\boldsymbol{x}\rangle \quad \mapsto \quad \sqrt{q^{-m}} \sum_{\boldsymbol{y} \in \mathbb{Z}_q^n} e^{\frac{2\pi i}{q}\langle \boldsymbol{y}, \boldsymbol{x} \rangle} |\boldsymbol{y}\rangle, \qquad \forall \boldsymbol{x} \in \mathbb{Z}_q^m.$$

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

$$|\Psi\rangle = \sum_{\boldsymbol{x} \in \mathbb{Z}^m} f(x) |\boldsymbol{x}\rangle \quad \text{with} \quad \sum_{\boldsymbol{x} \in \mathbb{Z}^m} |f(x)|^2 = 1,$$

for a function $f : \mathbb{Z}^m \to \mathbb{C}$, results in the state (the Fourier transform of $|\Psi\rangle$) given by

$$\begin{aligned} \mathsf{FT}_q |\Psi\rangle &= \sqrt{q^{-m}} \sum_{\boldsymbol{y} \in \mathbb{Z}_q^n} \Big(\sum_{\boldsymbol{x} \in \mathbb{Z}^m} f(x) \cdot e^{\frac{2\pi i}{q}\langle \boldsymbol{y}, \boldsymbol{x} \rangle} \Big) |\boldsymbol{y}\rangle \\ &= \sqrt{q^{-m}} \sum_{\boldsymbol{y} \in \mathbb{Z}_q^n} \hat{f}(\boldsymbol{y}) |\boldsymbol{y}\rangle. \end{aligned}$$

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 7 (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 $x, y \in \mathbb{Z}_q$:*

$$\sum_{v \in \mathbb{Z}_q} \omega_q^{v \cdot x} \omega_q^{-v \cdot y} = q \ \delta_{x,y}.$$

2.4 Lattices and the Gaussian mass

A *lattice* $\Lambda \subset \mathbb{R}^m$ is a discrete subgroup of $\mathbb{R}^m$. More formally, suppose that $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^m$ are linearly independent vectors. Then, the lattice $\Lambda(\boldsymbol{B}) \subset \mathbb{R}^m$ generated by the *basis* $\boldsymbol{B} = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n]$ consists of all integer linear combinations of $\boldsymbol{B}$ and is given by

$$\Lambda(\boldsymbol{B}) = \Lambda(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) = \left\{ \sum_{i=1}^m x_i \boldsymbol{b}_i \ : \ x_i \in \mathbb{Z} \right\}.$$

The *dual* of a lattice $\Lambda \subset \mathbb{R}^m$, denoted by Λ^*, is the lattice of all vectors $y \in \mathbb{R}^m$ that satisfy $\langle \boldsymbol{y}, \boldsymbol{x} \rangle \in \mathbb{Z}$, for all vectors $\boldsymbol{x} \in \Lambda$. In other words, we define

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

It is straightforward to show that for any $\boldsymbol{B} \in \mathbb{R}^{m\times m}$ it holds that $\Lambda(\boldsymbol{B})^* = \Lambda((\boldsymbol{B}^{-1})^T)$. The rank of a lattice $\Lambda(\boldsymbol{B})$, denoted by $\mathsf{rank}(\Lambda)$, is defined as $\mathsf{rank}(\boldsymbol{B})$. Given a lattice $\Lambda \subset \mathbb{R}^m$ and a vector $\boldsymbol{t} \in \mathbb{R}^m$, we define the *shifted lattice* $\Lambda - \boldsymbol{t}$ as the (right) coset of Λ as a group under addition with $\boldsymbol{t}$. To avoid handling matters of precision, we will only consider integer lattices $\Lambda \subseteq \mathbb{Z}^m$ throughout this work.

The *Gaussian measure* ϱ_r with parameter $r > 0$ is defined as the function

$$\varrho_r(\boldsymbol{x}) = \exp(-\pi\|\boldsymbol{x}\|^2/r^2), \qquad \forall \boldsymbol{x} \in \mathbb{R}^m.$$

Let $\Lambda \subset \mathbb{R}^m$ be a lattice and let $\boldsymbol{t} \in \mathbb{R}^m$ be a shift. We define the *Gaussian mass* of $\Lambda - \boldsymbol{t}$ as the quantity

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

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

$$D_{\Lambda-\boldsymbol{t},r}(\boldsymbol{x}) = \frac{\varrho_r(\boldsymbol{x}-\boldsymbol{t})}{\varrho_r(\Lambda-\boldsymbol{t})}, \qquad \forall \boldsymbol{x} \in \Lambda.$$

The discrete Gaussian is an essential tool in the literature on lattices and has found numerous applications in computer science, most notably in factoring polynomials [LLL82], in solving integer programming [Len83], and in attacking cryptosystems [Odl90].

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 Λ and shift $\boldsymbol{t} \in \Lambda$ and for all $r > 0$, $c \geq (2\pi)^{-\frac{1}{2}}$ it holds that*

$$\varrho_r\left((\Lambda - \boldsymbol{t}) \setminus \mathcal{B}^m(\boldsymbol{0}, c\sqrt{m}r)\right) \leq (2\pi e c^2)^{\frac{m}{2}} e^{-\pi c^2 m} \varrho_r(\Lambda),$$

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

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 $f(\Lambda) = \det(\Lambda^*)\hat{f}(\Lambda^*)$. We use the following Gaussian variant of the formula.

Lemma 9 (Poisson summation formula)**.** *Let $\Lambda \subseteq \mathbb{Z}^m$ be a full-rank lattice, let $r > 0$ and $\boldsymbol{v} \in \mathbb{Z}^m$. Then,*

$$\sum_{\boldsymbol{x}\in\Lambda+\boldsymbol{v}} \varrho_r(\boldsymbol{x}) = \det(\Lambda^*)\ r^m \sum_{\boldsymbol{y}\in\Lambda^*} e^{2\pi i\langle \boldsymbol{y},\boldsymbol{v}\rangle} \varrho_{1/r}(\boldsymbol{y}).$$

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

$$D_{\mathbb{Z}_q^m,B}(\boldsymbol{x}) = \frac{e^{-\pi\|\boldsymbol{x}\|^2/B^2}}{\displaystyle\sum_{\boldsymbol{y}\in\mathbb{Z}_q^m, \|\boldsymbol{y}\|_\infty\leq\sqrt{m}B} e^{-\pi\|\boldsymbol{y}\|^2/B^2}}.$$

The following result allows us to bound the total variation distance between a truncated discrete Gaussian $D_{\mathbb{Z}_q^m,B}$ and its perturbation by a fixed vector $\boldsymbol{e}_0 \in \mathbb{Z}^m$.

Lemma 10 (Lemma 3.3, [Mah18b])**.** *Let $q \geq 2$ be a modulus, $m \in \mathbb{N}$ and $B > 0$. Then, for any $\boldsymbol{e}_0 \in \mathbb{Z}^m$,*

$$\|D_{\mathbb{Z}_q^m,B} - (D_{\mathbb{Z}_q^m,B} + \boldsymbol{e}_0)\|_{\mathsf{TV}} \leq 2 \cdot \left(1 - e^{\frac{-2\pi\sqrt{m}\|\boldsymbol{e}_0\|}{B}}\right).$$

2.5 Cryptography

In this section, we review several definitions in cryptography.

Public-key encryption.

Definition 11 (Public-key encryption)**.** *A public-key encryption* (PKE) *scheme* $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *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.

$\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$: *takes as input the parameter* 1^λ *and outputs a public key* pk *and secret key* sk.

$\mathsf{Enc}(\mathsf{pk}, m) \to \mathsf{ct}$: *takes as input the public key* pk *and a plaintext* $m \in \mathcal{M}$, *and outputs a ciphertext* ct.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to m'$ **or** $\perp$: *takes as input the secret key* sk *and ciphertext* ct, *and outputs* $m' \in \mathcal{M}$ *or* $\perp$.

Definition 12 (Correctness of PKE)**.** *For any* $\lambda \in \mathbb{N}$, *and for any* $m \in \mathcal{M}$*:*

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \neq m \;\middle|\; \substack{(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)}\right] \leq \mathrm{negl}(\lambda).$$

Definition 13 ($\mathsf{IND\text{-}CPA}$ security)**.** *Let* $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be a* PKE *scheme and let* $\mathcal{A}$ *be a* QPT *adversary. We define the security experiment* $\mathsf{Exp}^{\mathsf{ind\text{-}cpa}}_{\Sigma,\mathcal{A},\lambda}(b)$ *between* $\mathcal{A}$ *and a challenger as follows:*

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

We say that the scheme Σ *is* $\mathsf{IND\text{-}CPA}$*-secure if, for any* QPT *adversary* $\mathcal{A}$, *it holds that*

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

2.6 The Learning with Errors problem

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

Definition 14 ("Search" LWE, [Reg05])**.** *Let* n *and* $m \geq n$ *be integers, let* $q \geq 2$ *be an integer modulus and let* $\alpha \in (0,1)$ *be a parameter. The Learning with Errors* (LWE) *problem is to find a secret vector* $\boldsymbol{s}$ *given as input a sample* $(\boldsymbol{A}, \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e} \pmod q)$ *from the distribution* $\mathsf{LWE}^m_{n,q,\alpha q}$, *where* $\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$, $\boldsymbol{s} \xleftarrow{\$} \mathbb{Z}_q^n$ *and where* $\boldsymbol{e} \sim D_{\mathbb{Z}^m, \alpha q}$ *is sampled from the discrete Gaussian distribution. We say that an algorithm solves the ("search")* $\mathsf{LWE}^m_{n,q,\alpha q}$ *problem if it runs in (classical or quantum) time* $\mathrm{poly}(n \log q)$ *and finds* $\boldsymbol{s}$ *with probability at least* $1/\mathrm{poly}(n \log q)$.

Definition 15 ("Decisional" LWE, [Reg05])**.** *Let* n *and* $m \geq n$ *be integers, let* $q \geq 2$ *be an integer modulus and let* $\alpha \in (0,1)$ *be a parameter. The "decision" Learning with Errors* (dLWE) *problem is to distinguish between an instance of* $\mathsf{LWE}^m_{n,q,\alpha q}$ *and a uniform sample* $(\boldsymbol{A}, \boldsymbol{u})$, *where* $\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$ *and* $\boldsymbol{u} \xleftarrow{\$} \mathbb{Z}_q^m$. *We say that an algorithm solves the* $\mathsf{dLWE}^m_{n,q,\alpha q}$ *problem if it runs in (classical or quantum) time* $\mathrm{poly}(n \log q)$ *and succeeds with probability at least* $\frac{1}{2} + 1/\mathrm{poly}(n \log q)$.

As shown in [Reg05], the $\mathsf{LWE}^m_{n,q,\alpha q}$ 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 $\gamma = \widetilde{O}(n/\alpha)$ in worst case lattices of dimension n. In this work we assume the subexponential hardness of $\mathsf{LWE}^m_{n,q,\alpha q}$ which relies on the worst case hardness of approximating short vector problems in lattices to within a subexponential factor.

3 Quantum Proofs of Deletion

In this section, we present a formal definition of *quantum proofs of deletion* as an interactive protocol between a quantum prover $\mathcal{P}$ and a classical verifier $\mathcal{V}$, which is inspired by so-called *agree-and-prove* schemes [BJM19, VZ21] in the context of proofs of knowledge. Specifically, we imagine that there exists a trusted third party (a procedure which we call Setup) which prepares any auxiliary inputs handed to the verifier $\mathcal{V}$ and the prover $\mathcal{P}$ at the beginning of the protocol. In contrast with the notion of certified deletion by Broadbent and Islam [BI20], our definition is not limited to ciphertexts but instead considers *samples from an arbitrary probability distribution* which we call Samp. We remark that we define deletion of a sample x generated by Samp as the prover's "inability to guess x" (in an information-theoretic sense) once the verifier is convinced that deletion has taken place. For some additional flexibility, we also allow a quantum proof-of-deletion protocol to depend on a public key. Our definition is as follows.

Definition 16 (Quantum proof-of-deletion protocol)**.** *Let $\lambda \in \mathbb{N}$ denote the security parameter. A (public-key) quantum proof-of-deletion (QPD) protocol with respect an ensemble of alphabets $\mathcal{X} = \{\mathcal{X}_\lambda\}$ is a tuple consisting of the following four (interactive) algorithms* $\mathsf{QPD} = (\mathsf{Samp}, \mathsf{Setup}, \mathcal{V}, \mathcal{P})$ *given by:*

- *A* PPT *sampling procedure* $\mathsf{Samp}(1^\lambda)$ *which takes as input a unary encoding of the security parameter λ and outputs a pair (pk, x), where pk is a public key and $x \in \mathcal{X}_\lambda$ is an input.*

- *A* QPT *auxiliary input generation procedure* $\mathsf{Setup}(1^\lambda, \mathsf{pk}, x)$ *which takes as input a unary encoding of the security parameter λ together with a pair of inputs pk and $x \in \mathcal{X}_\lambda$ and outputs a CQ state ϱ_{VP} specifying the auxiliary inputs for the verifier (in the classical system V) and the prover (in the quantum system P), respectively, where we use the notation $\mathsf{vk} = \mathrm{tr}_P[\varrho_{VP}]$ and $\varrho_P = \mathrm{tr}_V[\varrho_{VP}]$.*

- *An (honest)* PPT *verifier $\mathcal{V}(1^\lambda, \mathsf{vk}, \pi)$ which takes as input a unary encoding of the security parameter λ, an auxiliary input vk and a witness π, and outputs 1 (accept) or 0 (reject).*

- *An (honest)* QPT *prover $\mathcal{P}(1^\lambda, \mathsf{pk}, \varrho_P)$ which takes as input a unary encoding of the security parameter λ, a public key pk and a quantum state ϱ_P, and outputs a classical witness π.*

3.1 Completeness

The first property we associate with a QPD protocol is *completeness*, which says that an honest prover is accepted with overwhelming probability by the verifier.

Definition 17 (Completeness)**.** *A quantum proof-of-deletion protocol* $\mathsf{QPD} = (\mathsf{Samp}, \mathsf{Setup}, \mathcal{V}, \mathcal{P})$ *with respect to an ensemble $\mathcal{X}$ is said to have completeness $c \geq 0$, if it holds that*

$$\Pr\left[\mathcal{V}(1^\lambda, \mathsf{vk}, \pi) = 1 \,\middle|\, \begin{array}{c} (\mathsf{pk}, x) \leftarrow \mathsf{Samp}(1^\lambda) \\ (\mathsf{vk}, \varrho_P) \leftarrow \mathsf{Setup}(1^\lambda, \mathsf{pk}, x) \\ \pi \leftarrow \mathcal{P}(1^\lambda, \mathsf{pk}, \varrho_P) \end{array}\right] \geq c(\lambda).$$

3.2 Entropic deletion

The second property we associate with a QPD protocol is *entropic deletion* which limits the prover's ability to guess the encoded sample x generated by Samp once the verifier is convinced that deletion has taken place. To formalize the notion of entropic deletion, we first define the following experiment.

Experiment 1 (Deletion experiment). *Let $\lambda \in \mathbb{N}$ be the security parameter and $\mathcal{X} = \{\mathcal{X}_\lambda\}$ an ensemble of alphabets. Let $\mathsf{QPD} = (\mathsf{Samp}, \mathsf{Setup}, \mathcal{V}, \mathcal{P})$ be a quantum proof-of-deletion protocol with respect to $\mathcal{X}$. The deletion experiment $\mathsf{Exp}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{\mathcal{P}}}$ is the following game between an (honest) verifier $\mathcal{V}$, a (possibly malicious) prover $\widetilde{\mathcal{P}}$ and an (honest) challenger who serves as a trusted third party:*

1. *The challenger executes the sampling procedure $\mathsf{Samp}(1^\lambda)$ which produces as output pair (pk, x), where pk is a public key and $x \in \mathcal{X}_\lambda$ is an input.*

2. *The challenger executetes the auxiliary input generation procedure $\mathsf{Setup}(1^\lambda, \mathsf{pk}, x)$ which outputs a CQ state ϱ_{VP} specifying the auxiliary inputs for the verifier $\mathcal{V}$ (in the classical system V) and the prover $\widetilde{\mathcal{P}}$ (in the quantum system P), where we let $\mathsf{vk} = \mathrm{tr}_P[\varrho_{VP}]$ and $\varrho_P = \mathrm{tr}_V[\varrho_{VP}]$.*

3. *The prover $\widetilde{\mathcal{P}}$ receives as input $(1^\lambda, \mathsf{pk}, \varrho_P)$, produces a classical witness π and sends it to $\mathcal{V}$.*

4. *The verifier $\mathcal{V}$ receives as input $(1^\lambda, \mathsf{vk}, \pi)$ and outputs a flag $F^{\mathsf{ver}} = 1$ (accept) or $F^{\mathsf{ver}} = 0$ (reject). If $\mathcal{V}$ accepts, the game continues. Otherwise, if $\mathcal{V}$ rejects, $\widetilde{\mathcal{P}}$ loses.*

5. *The prover $\widetilde{\mathcal{P}}$ generates an output x' as a guess for the sample $x \in \mathcal{X}_\lambda$ and sends it to the challenger.*

6. *The challenger outputs 1, if both $x' = x$ and $F^{\mathsf{ver}} = 1$, and 0 otherwise.*

We say that the prover $\widetilde{\mathcal{P}}$ wins the experiment $\mathsf{Exp}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{\mathcal{P}}}$ if the challenger outputs 1.

We also introduce the following definition which helps us represent a (possibly malicious) prover in terms of a pair of CPTP maps that are performed in Experiment 1.

Definition 18 (Characterization of a malicious prover). *Let $\lambda \in \mathbb{N}$ be the security parameter and let $\mathcal{X} = \{\mathcal{X}_\lambda\}$ be an ensemble of alphabets. Let $\mathsf{QPD} = (\mathsf{Samp}, \mathsf{Setup}, \mathcal{V}, \mathcal{P})$ be a quantum proof-of-deletion protocol with respect to $\mathcal{X}$. We say that a (possibly malicious) prover $\widetilde{\mathcal{P}}(1^\lambda, \mathsf{pk}, \varrho_P)$ is characterized by a pair of CPTP maps $\Phi = (\Phi^0, \Phi^1)$, if $\widetilde{\mathcal{P}}$ performs the following steps during $\mathsf{Exp}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{\mathcal{P}}}$ in Experiment 1:*

- *The prover $\widetilde{\mathcal{P}}$ receives as input a tuple $(1^\lambda, \mathsf{pk}, \varrho_P)$ and produces a classical witness π by performing a quantum channel $\Phi^0 : L(\mathcal{H}_P \otimes \mathcal{H}_K) \to L(\mathcal{H}_\Pi \otimes \mathcal{H}_E)$ on the auxiliary input ϱ_P in the quantum system P and the public key pk in the classical system K such that*

$$|\pi\rangle\langle\pi|_\Pi \otimes \varrho_E \leftarrow \Phi^{0,\mathsf{pk}}_{P\to\Pi E}(\varrho_P) \overset{\mathrm{def}}{=} \Phi^0_{PK\to\Pi E}(\varrho_P \otimes |\mathsf{pk}\rangle\langle\mathsf{pk}|_K),$$

where ϱ_E represents the prover's side information in a quantum system E.

- *The prover $\widetilde{\mathcal{P}}$ uses the state ϱ_E in system E and the public key pk in a classical system K, and produces an output x' by performing a quantum channel $\Phi^1 : L(\mathcal{H}_E \otimes \mathcal{H}_K) \to L(\mathcal{H}_{X'})$ with outcome*

$$|\boldsymbol{x}'\rangle\langle\boldsymbol{x}'|_{X'} \leftarrow \Phi^{0,\mathsf{pk}}_{E\to X'}(\varrho_E) \overset{\mathrm{def}}{=} \Phi^1_{EK\to X'}(\varrho_E \otimes |\mathsf{pk}\rangle\langle\mathsf{pk}|_K).$$

Based on the deletion experiment in Experiment 1 and our characterization of a malicious prover in Definition 18, we then introduce the following entropic notions of deletion.

Definition 19 (Entropic deletion)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter and $\mathcal{X} = \{\mathcal{X}_\lambda\}$ an ensemble of alphabets. Let* $\mathsf{QPD} = (\mathsf{Samp}, \mathsf{Setup}, \mathcal{V}, \mathcal{P})$ *be a quantum proof-of-deletion protocol with respect to $\mathcal{X}$. We say that* QPD *has κ-entropic deletion if there exists $\kappa(\lambda)$ such that, for any (possibly malicious) prover $\widetilde{\mathcal{P}}$ characterized by a pair of* CPTP *maps $\Phi = (\Phi^0, \Phi^1)$, the advantage in the deletion experiment* $\mathsf{Exp}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{\mathcal{P}}}$ *in Experiment 1 is at most*

$$\mathsf{Adv}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{\mathcal{P}}}(\lambda) = \Pr\left[\begin{array}{c|c} x'=x & (\mathsf{pk},x)\leftarrow\mathsf{Samp}(1^\lambda) \\ & (\mathsf{vk},\varrho_P)\leftarrow\mathsf{Setup}(1^\lambda,\mathsf{pk},x) \\ \wedge & |\pi\rangle\langle\pi|_\Pi\otimes\varrho_E\leftarrow\Phi^{0,\mathsf{pk}}_{P\to\Pi E}(\varrho_P) \\ & F^{\mathsf{ver}}\leftarrow\mathcal{V}(1^\lambda,\mathsf{vk},\pi) \\ F^{\mathsf{ver}}=1 & |x'\rangle\langle x'|_{X'}\leftarrow\Phi^{0,\mathsf{pk}}_{E\to X'}(\varrho_E) \end{array}\right] \leq 2^{-H_{\min}(X_\lambda|K_\lambda)+\kappa(\lambda)} + \mathrm{negl}(\lambda),$$

where $H_{\min}(X_\lambda|K_\lambda)$ corresponds to the min-entropy (see Section 2.2) of the random variable X_λ with outcome $x \in \mathcal{X}_\lambda$ conditioned on the random variable K_λ with outcome pk. *Note that both outcomes are generated by the sampling procedure* $\mathsf{Samp}(1^\lambda)$.

In the case of computationally bounded adversaries, we instead consider an efficient pair of CPTP maps $\Phi_\lambda = (\Phi^0_\lambda, \Phi^1_\lambda)$ which are parameterized by the security parameter $\lambda \in \mathbb{N}$ (as in Definition 1). This results in the following notion which we call *pseudoentropic deletion*.

Definition 20 (Pseudoentropic deletion)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter and $\mathcal{X} = \{\mathcal{X}_\lambda\}$ an ensemble of alphabets. Let* $\mathsf{QPD} = (\mathsf{Samp}, \mathsf{Setup}, \mathcal{V}, \mathcal{P})$ *be a quantum proof-of-deletion protocol with respect to $\mathcal{X}$. We say that* QPD *has κ-pseudoentropic deletion if there exists $\kappa(\lambda)$ such that, for any (possibly malicious)* QPT *prover $\widetilde{\mathcal{P}}$ characterized by a pair of efficient* CPTP *maps $\Phi_\lambda = (\Phi^0_\lambda, \Phi^1_\lambda)$, the advantage in* $\mathsf{Exp}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{\mathcal{P}}}$ *in Experiment 1 is at most*

$$\mathsf{Adv}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{\mathcal{P}}}(\lambda) = \Pr\left[\begin{array}{c|c} x'=x & (\mathsf{pk},x)\leftarrow\mathsf{Samp}(1^\lambda) \\ & (\mathsf{vk},\varrho_P)\leftarrow\mathsf{Setup}(1^\lambda,\mathsf{pk},x) \\ \wedge & |\pi\rangle\langle\pi|_\Pi\otimes\varrho_E\leftarrow\Phi^{0,\mathsf{pk}}_{P\to\Pi E}(\varrho_P) \\ & F^{\mathsf{ver}}\leftarrow\mathcal{V}(1^\lambda,\mathsf{vk},\pi) \\ F^{\mathsf{ver}}=1 & |x'\rangle\langle x'|_{X'}\leftarrow\Phi^{1,\mathsf{pk}}_{E\to X'}(\varrho_E) \end{array}\right] \leq 2^{-H_{\mathsf{HILL}}(X_\lambda|K_\lambda)+\kappa(\lambda)} + \mathrm{negl}(\lambda),$$

where $H_{\mathsf{HILL}}(X_\lambda|K_\lambda)$ corresponds to the conditional computational pseudoentropy (see Definition 4) of the random variable X_λ with outcome $x \in \mathcal{X}_\lambda$ conditioned on the random variable K_λ with outcome pk. *Note that both outcomes are generated by the sampling procedure* $\mathsf{Samp}(1^\lambda)$.

4 Entropic Uncertainty Relations for Gaussian Cosets

In this section, we develop a general theory for Gaussian coset states which are essential for our quantum proofs of deletion for Learning with Errors. In Section 4.1 we give a formal definition of primal and dual Gaussian coset states. Then, in Section 4.2, we prove an important technical lemma (which we call the *Gaussian Switching Lemma*) that relates the Fourier transform of a primal Gaussian coset with its dual Gaussian coset. Finally, in Section 4.3, we prove *entropic uncertainty relations* for Gaussian coset states which capture the intuitive property that it is impossible to simultaneously measure a Gaussian coset state in the computational as well as the Fourier basis.

Gaussian superpositions over lattices have found numerous applications in quantum cryptography [Reg05, Mah18a, Mah18a, Bra18, KNY21, HMNY21b]. Recall that a *lattice* $\Lambda \subset \mathbb{R}^m$ is a discrete subgroup of $\mathbb{R}^m$. To avoid handling matters of precision, one typically considers integer lattices $\Lambda \subseteq \mathbb{Z}^m$ in the context of quantum computation. The *Gaussian measure* ϱ_r with parameter $r > 0$ is defined as the function

$$\varrho_r(\boldsymbol{x}) = \exp(-\pi\|\boldsymbol{x}\|^2/r^2), \qquad \forall \boldsymbol{x} \in \mathbb{R}^m.$$

Let $\Lambda \subseteq \mathbb{R}^m$ be a lattice and let $\boldsymbol{t} \in \mathbb{R}^m$ be a shift. We define the *Gaussian mass* of $\Lambda - \boldsymbol{t}$ as the quantity

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

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

$$D_{\Lambda-\boldsymbol{t},r}(\boldsymbol{x}) = \frac{\varrho_r(\boldsymbol{x}-\boldsymbol{t})}{\varrho_r(\Lambda-\boldsymbol{t})}, \qquad \forall \boldsymbol{x} \in \Lambda.$$

We extend the discrete Gaussian distribution to superpositions over lattices as follows.

Definition 21 (Gaussian superpositions over lattices). *Let $\Lambda \subseteq \mathbb{Z}^m$ be an m-dimensional integer lattice and let $\mathbf{t} \in \mathbb{Z}^m$. Let $r > 0$. We define the Gaussian superposition $|\mathcal{D}_{\Lambda-\boldsymbol{t},r}\rangle$ over the shifted lattice $\Lambda - \boldsymbol{t}$ as*

$$|\mathcal{D}_{\Lambda-\boldsymbol{t},r}\rangle := \sum_{\boldsymbol{x}\in\Lambda} \sqrt{D_{\Lambda-\boldsymbol{t},r}(\boldsymbol{x})}\,|\boldsymbol{x}\rangle = \frac{1}{\sqrt{\varrho_r(\Lambda-\boldsymbol{t})}} \sum_{\boldsymbol{x}\in\Lambda} \varrho_{\sqrt{2}r}(\boldsymbol{x}-\boldsymbol{t})\,|\boldsymbol{x}\rangle\,.$$

We remark that the state in Definition 21 does not belong to a finite-dimensional Hilbert space. In practice, we typically replace $\Lambda = \mathbb{Z}^m$ with some finite set (namely, all lattice points that belong to some finite grid). The standard tail bound for the *Gaussian measure* ϱ_r in Lemma 8 reveals that

$$\varrho_r(\mathbb{Z}^m \setminus (-\sqrt{m}r, \sqrt{m}r]^m) \leq 2^{-\Omega(m)}\varrho_r(\mathbb{Z}^m), \qquad \forall r > 0.$$

In other words, the probability mass is almost entirely contained within the finite grid $\mathbb{Z}^m \cap (-\sqrt{m}r, \sqrt{m}r]^m$ up to a correction factor of $2^{-\Omega(m)}$ (see Lemma 8). This suggests the use of the *truncated* discrete Gaussian distribution $D_{\mathbb{Z}_q^m,r}$ over $\mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$ with support $\{\boldsymbol{x} \in \mathbb{Z}_q^m : \|\boldsymbol{x}\|_\infty \leq \sqrt{m}r\}$, where

$$D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}) = \frac{e^{-\pi\|\boldsymbol{x}\|^2/r^2}}{\sum\limits_{\boldsymbol{y}\in\mathbb{Z}_q^m, \|\boldsymbol{y}\|_\infty \leq \sqrt{m}r} e^{-\pi\|\boldsymbol{y}\|^2/r^2}}.$$

We adapt Definition 21 to the truncated discrete Gaussian distribution as follows.

Definition 22 (Truncated Gaussian superposition). *Let $m \in \mathbb{N}$ and let $q \geq 2$ be an integer modulus. Let $D_{\mathbb{Z}_q^m,r}$ be the truncated discrete Gaussian with parameter $r > 0$ over the finite cube $\mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$. Then, the truncated discrete Gaussian superposition state $|\mathcal{D}_{\mathbb{Z}_q^m,r}\rangle$ is defined as*

$$|\mathcal{D}_{\mathbb{Z}_q^m,r}\rangle = \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{x})}\,|\boldsymbol{x}\rangle\,.$$

We remark that the truncated Gaussian superposition state $|\mathcal{D}_{\mathbb{Z}_q^m,r}\rangle$ in Definition 22 can be efficiently approximated on a quantum computer via the Grover-Rudolph algorithm [GR02] (see also [GPV07, Bra18, BCM+21]) for the choice of parameter $r = \Omega(\sqrt{m})$ relevant to this work.

4.1 Gaussian coset states

Let us first give a formal definition of Gaussian coset states which are based on the truncated Gaussian superposition state $|\mathcal{D}_{\mathbb{Z}_q^m,r}\rangle$ we introduced in Definition 22.

Definition 23 (Gaussian coset states)**.** *Let $m \in \mathbb{N}$ and let $q \geq 2$ be an integer modulus. Let $D_{\mathbb{Z}_q^m,r}$ be the truncated discrete Gaussian with parameter $r > 0$ over the finite cube $\mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$. Then,*

- *(primal Gaussian coset:) for all $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_q^m$, we let*

$$|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle := \sum_{\boldsymbol{x} \in \mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{x})}\, \omega_q^{-\langle \boldsymbol{x},\boldsymbol{v}\rangle}\, |\boldsymbol{u} + \boldsymbol{x} \pmod{q}\rangle\,;$$

- *(dual Gaussian coset:) for all $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_q^m$, we let*

$$|\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle := \sum_{\boldsymbol{y} \in \mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,q/2r}(\boldsymbol{y})}\, \omega_q^{\langle \boldsymbol{y},\boldsymbol{u}\rangle}\, |\boldsymbol{v} + \boldsymbol{y} \pmod{q}\rangle\,,$$

where $\omega_q = e^{2\pi i/q}$ denotes the primitive q-th root of unity.

We now highlight an important connection between primal and dual Gaussian cosets in Definition 23.

4.2 Gaussian switching lemma

A key feature of Gaussian coset states lies in a property which we call *duality*. Namely, we can show that the Fourier transform of a primal Gaussian coset (approximately) results in its dual Gaussian coset. In particular, we show that Gaussian cosets can be associated with a primal and dual lattice, respectively.

Let $q \geq 2$ be an integer modulus and suppose that $r > 0$ is a parameter with $r \leq q/\sqrt{2m}$. Let $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_q^n$ be an arbitrary pair of vectors. Let $\Lambda = \mathbb{Z}^m$ be the trivial integer lattice. Notice that, according to the tail bound in Lemma 8, the *primal* Gaussian coset state $|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle$ restricted to the finite set $\mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$ is within ℓ^2 distance $2^{-\Omega(m)}$ of the state given by

$$|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle \approx \sum_{\boldsymbol{x} \in \Lambda} \sqrt{D_{\Lambda,r}(\boldsymbol{x})}\, \omega_q^{-\langle \boldsymbol{x},\boldsymbol{v}\rangle}\, |\boldsymbol{u} + \boldsymbol{x} \pmod{q}\rangle\,. \tag{12}$$

We prove the following result. Suppose we apply the q-ary quantum Fourier transform to the *primal* state given by $|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle$ in Eq. (12), where $r \geq \sqrt{m/2}$. Then, by the *Poisson summation formula* (Lemma 9) we have that the resulting state is within ℓ^2 distance $2^{-\Omega(m)}$ of the *dual* Gaussian coset,

$$|\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle \approx \sum_{\boldsymbol{y} \in \Lambda^*} \sqrt{D_{\Lambda^*,q/2r}(\boldsymbol{y})}\, \omega_q^{\langle \boldsymbol{y},\boldsymbol{u}\rangle}\, |\boldsymbol{v} + \boldsymbol{y} \pmod{q}\rangle\,. \tag{13}$$

We capture the duality property in the so-called *Gaussian Switching Lemma* (Lemma 11). Note that Λ^* in Eq. (13) denotes the *dual lattice* which is the lattice of all vectors $y \in \mathbb{R}^m$ that satisfy $\langle \boldsymbol{y}, \boldsymbol{x}\rangle \in \mathbb{Z}$, for all vectors $\boldsymbol{x} \in \Lambda$. For the trivial integer lattice $\Lambda = \mathbb{Z}^m$, the primal lattice and the dual lattice are identical. The duality of Gaussian cosets is captured by the following technical lemma which states that the Fourier transform of the primal coset is within trace distance $2^{-\Omega(m)}$ of its dual for appropriate choices of $r > 0$.

Lemma 11 (Gaussian Switching Lemma)**.** *Let $q \geq 2$ be a modulus, let $m \in \mathbb{N}$ and let $r \in \left[\frac{\sqrt{m}}{\sqrt{2}}, \frac{q}{\sqrt{2m}}\right]$. Then, for any $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_q^m$, the q-ary Fourier transform of the primal Gaussian coset satisfies*

$$\left\| |\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle - \mathsf{FT}_q \, |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle \right\|_{\mathrm{tr}} \leq 2\exp\left(-(\pi - \frac{1}{2}\left(\ln(2\pi)+1\right)\cdot m\right).$$

Proof. Let $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_q^m$ and $r \in \left[\frac{\sqrt{m}}{\sqrt{2}}, \frac{q}{\sqrt{2m}}\right]$. Recall that the primal Gaussian coset is given by

$$|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle \propto \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} \varrho_{\sqrt{2}r}(\boldsymbol{x}) \cdot e^{-\frac{2\pi i}{q}\langle \boldsymbol{x},\boldsymbol{v}\rangle} \, |\boldsymbol{u}+\boldsymbol{x} \pmod q\rangle \,. \tag{14}$$

Let $\Lambda = \mathbb{Z}^m$ be the trivial integer lattice. Since $r \leq q/\sqrt{2m}$, it follows from the Gaussian tail bound in Lemma 8 that the state in (14) is within ℓ^2 distance $(2\pi e)^{\frac{m}{2}} e^{-\pi m}$ of the quantum state

$$\sum_{\boldsymbol{x}\in\Lambda} \varrho_{\sqrt{2}r}(\boldsymbol{x}) \cdot e^{-\frac{2\pi i}{q}\langle \boldsymbol{x},\boldsymbol{v}\rangle} \, |\boldsymbol{u}+\boldsymbol{x} \pmod q\rangle \,. \tag{15}$$

Let us now consider the Fourier transform of (15). To this end, we define a function $f_r : \Lambda \to \mathbb{C}$ with

$$f_r(\boldsymbol{x}) \overset{\text{def}}{=} \varrho_{\sqrt{2}r}(\boldsymbol{x}) \cdot e^{-\frac{2\pi i}{q}\langle \boldsymbol{x},\boldsymbol{v}\rangle}, \qquad \forall \boldsymbol{x} \in \Lambda.$$

Then, applying the q-ary Fourier transform FT_q and re-arranging the roots of unity, we obtain the state

$$\begin{aligned} \sum_{\boldsymbol{z}\in\mathbb{Z}_q^m} \hat{f}_r(z)\,|\boldsymbol{z}\rangle &= \sum_{\boldsymbol{z}\in\mathbb{Z}_q^n} \Big(\sum_{\boldsymbol{x}\in\mathbb{Z}^m} f_r(x) \cdot e^{\frac{2\pi i}{q}\langle \boldsymbol{z},\boldsymbol{x}\rangle} \Big) |\boldsymbol{z}\rangle \\ &= \sum_{\boldsymbol{z}\in\mathbb{Z}_q^m} \sum_{\boldsymbol{x}\in\Lambda} \varrho_{\sqrt{2}r}(\boldsymbol{x}) \cdot e^{-\frac{2\pi i}{q}\langle \boldsymbol{x},\boldsymbol{z}-\boldsymbol{v}\rangle} \cdot e^{\frac{2\pi i}{q}\langle \boldsymbol{z},\boldsymbol{u}\rangle} \, |\boldsymbol{z}\rangle \,. \end{aligned} \tag{16}$$

Let $\Lambda^* = \mathbb{Z}^m$ denote the dual of $\Lambda = \mathbb{Z}^m$. Using the Poisson summation formula (Lemma 9), we obtain

$$\sum_{\boldsymbol{z}\in\mathbb{Z}_q^m} \sum_{\boldsymbol{w}\in\Lambda^*} \varrho_{1/\sqrt{2}r}\left(\boldsymbol{w} + \frac{\boldsymbol{z}-\boldsymbol{v}}{q}\right) \cdot e^{\frac{2\pi i}{q}\langle \boldsymbol{z},\boldsymbol{u}\rangle} \, |\boldsymbol{z}\rangle \,.$$

Let us now define $\boldsymbol{y} := q\cdot\boldsymbol{w} + \boldsymbol{z} - \boldsymbol{v} \in \mathbb{Z}^m$. A change of variables then yields the state

$$\sum_{\boldsymbol{y}\in\Lambda^*} \varrho_{q/\sqrt{2}r}(\boldsymbol{y}) \cdot e^{\frac{2\pi i}{q}\langle \boldsymbol{y}-q\cdot\boldsymbol{w}+\boldsymbol{v},\boldsymbol{u}\rangle} \, |\boldsymbol{v}+\boldsymbol{y}-q\cdot\boldsymbol{w} \pmod q\rangle \,. \tag{17}$$

The state above can be further simplified as follows. First, notice that by linearity

$$e^{-\frac{2\pi i}{q}\langle q\cdot\boldsymbol{w},\boldsymbol{u}\rangle} = e^{-2\pi i\langle \boldsymbol{w},\boldsymbol{u}\rangle} = 1, \qquad \forall \boldsymbol{w},\boldsymbol{u} \in \mathbb{Z}_q^m.$$

Then, using that $q\cdot\boldsymbol{w} \equiv \boldsymbol{0} \pmod q$ and omitting the global phase $e^{\frac{2\pi i}{q}\langle \boldsymbol{v},\boldsymbol{u}\rangle}$, we find that (17) equals

$$\sum_{\boldsymbol{y}\in\Lambda^*} \varrho_{q/\sqrt{2}r}(\boldsymbol{y}) \cdot e^{\frac{2\pi i}{q}\langle \boldsymbol{y},\boldsymbol{u}\rangle} \, |\boldsymbol{v}+\boldsymbol{y} \pmod q\rangle \,. \tag{18}$$

Since $r \geq \sqrt{m/2}$ we have by Lemma 8 that (18) is within ℓ^2 distance $(2\pi e)^{\frac{m}{2}} e^{-\pi m}$ of the dual coset

$$|\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle \propto \sum_{\boldsymbol{y}\in\mathbb{Z}_q^m} \varrho_{q/\sqrt{2}r}(\boldsymbol{y}) \cdot e^{\frac{2\pi i}{q}\langle \boldsymbol{y},\boldsymbol{u}\rangle} |\boldsymbol{v}+\boldsymbol{y} \pmod q\rangle .$$

Finally, we recall the following inequality which relates the trace distance and the ℓ^2 distance:

$$\| \, |\psi\rangle - |\phi\rangle \, \|_{\mathrm{tr}} \leq \| \, |\psi\rangle - |\phi\rangle \, \|_2, \qquad \forall \, |\psi\rangle , |\phi\rangle \in (\mathbb{C}^q)^{\otimes m}.$$

Putting everything together and applying the triangle inequality, we obtain the desired upper bound:

$$\begin{aligned}\big\| |\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle - \mathsf{FT}_q \, |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle \big\|_{\mathrm{tr}} &\leq \big\| |\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle - \mathsf{FT}_q \, |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle \big\|_2 \\ &\leq (2\pi e)^{\frac{m}{2}} \cdot \exp(-\pi m) + (2\pi e)^{\frac{m}{2}} \cdot \exp(-\pi m) \\ &= 2 \exp\Big(- (\pi - \frac{1}{2}\big(\ln(2\pi) + 1\big) \cdot m \Big).\end{aligned}$$

□

Next, we prove *entropic uncertainty relation* for Gaussian coset states.

4.3 Uncertainty relations

In this section, we formalize the intituitive property that it is impossible to simultaneously measure a Gaussian coset state in two incompatible bases (say the computational basis and the Fourier basis). Let us first consider a simple example. Consider the primal Gaussian coset,

$$|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle = \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{x})} \, \omega_q^{-\langle \boldsymbol{x},\boldsymbol{v}\rangle} \, |\boldsymbol{u}+\boldsymbol{x} \pmod q\rangle .$$

Our first observation is that a measurement in the computational basis yields a sample from the discrete Gaussian $D_{\mathbb{Z}_q^m-\boldsymbol{u},r}$ centered around the vector $\boldsymbol{u} \in \mathbb{Z}_q^m$. Because quantum measurement is an inherently destructive process, we expect that a computational basis immediately renders any measurement outcome of the Fourier basis impossible to predict. Note that, by the *Gaussian Switching Lemma* (Lemma 11), the Fourier transform of the primal state results in a state within trace distance $2^{-\Omega(m)}$ of the dual state,

$$|\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle = \sum_{\boldsymbol{y}\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,q/2r}(\boldsymbol{y})} \, \omega_q^{\langle \boldsymbol{y},\boldsymbol{u}\rangle} \, |\boldsymbol{v}+\boldsymbol{y} \pmod q\rangle ,$$

Hence, a measurement in the Fourier basis yields a sample from the discrete Gaussian $D_{\mathbb{Z}_q^m-\boldsymbol{v},q/2r}$ centered around the vector $\boldsymbol{v} \in \mathbb{Z}_q^m$. Therefore, it should be impossible to simultaneously produce samples from the discrete Gaussians $D_{\mathbb{Z}_q^m-\boldsymbol{u},r}$ and $D_{\mathbb{Z}_q^m-\boldsymbol{v},q/2r}$ given a single copy of the Gaussian coset state $|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle$.

In this section, we generalize this property even further. Namely, we show that any measurement that yields an outcome which is *highly correlated* with the vector $\boldsymbol{v} \in \mathbb{Z}_q^m$ associated with the q-ary Fourier basis immediately renders a hypothetical computational basis measurement impossible to predict.

For cryptographic purposes, we are primarily concerned with *random* Gaussian cosets, where $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_q^m$ are meant to be hidden (say, from the perspective of a prover) and are thus sampled uniformly at random from the set $\mathbb{Z}_q^m$. Thus, a random Gaussian coset, say in system B, corresponds to the mixture

$$\omega_B = q^{-2m} \sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle \langle \mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B . \tag{19}$$

In order to state entropic uncertainty relations for Gaussian cosets, it is convenient to work in an entanglement-based setting which gives us precise control over the different measurements performed on a Gaussian coset state. This motivates the following definition.

Definition 24 (Entangled Gaussian Cosets)**.** *Let $q \geq 2$ be a modulus, let $m \in \mathbb{N}$ be an integer, and let $r > 0$. We define the entangled Gaussian cosets pair $|\mathcal{D}_r\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ with respect to systems AB as*

$$|\mathcal{D}_r\rangle_{AB} = q^{-m}\sqrt{q^{-m}} \sum_{\boldsymbol{u},\boldsymbol{v} \in \mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},-\boldsymbol{v}}\rangle_A \otimes |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle_B .$$

The bipartite state $|\mathcal{D}_r\rangle_{AB}$ is indeed a purification of ω_B in Eq. (19), which we establish by means of the next two lemmas. Namely, whenever we trace out one half of the state, say system A, the other half of the state in system B immediately collapses to a random Gaussian coset, as required.

We first show the following technical lemma.

Lemma 12 (Partial trace identity for entangled Gaussian cosets)**.** *Let $q \geq 2$ be a modulus, $m \in \mathbb{N}$ and $r > 0$. Let $\omega_{AB} = |\mathcal{D}_r\rangle\langle\mathcal{D}_r|_{AB}$ be an entangled Gaussian coset in systems AB. Then, for any $\boldsymbol{x} \in \mathbb{Z}_q^m$,*

$$\mathrm{Tr}_A[(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|_A \otimes \mathbb{1}_B)\omega_{AB}] = q^{-2m} \sum_{\boldsymbol{u},\boldsymbol{v},\boldsymbol{e} \in \mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{e}) D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}-\boldsymbol{u})}\, \omega_q^{-\langle \boldsymbol{e},\boldsymbol{v}\rangle} \omega_q^{\langle \boldsymbol{x}-\boldsymbol{u},\boldsymbol{v}\rangle} \,|\boldsymbol{u}+\boldsymbol{e} \pmod q\rangle \langle \boldsymbol{x}|_B .$$

Proof. Let $\boldsymbol{x} \in \mathbb{Z}_q^m$. Expanding the partial trace with respect to system A, we get

$$\begin{aligned} \mathrm{Tr}_A[(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|_A \otimes \mathbb{1}_B)\omega_{AB}] &= \mathrm{Tr}_A[(\langle\boldsymbol{x}|_A \otimes \mathbb{1}_B)\omega_{AB}(|\boldsymbol{x}\rangle_A \otimes \mathbb{1}_B)] \\ &= (\langle\boldsymbol{x}|_A \otimes \mathbb{1}_B)|\mathcal{D}_r\rangle\langle\mathcal{D}_r|_{AB}(|\boldsymbol{x}\rangle_A \otimes \mathbb{1}_B). \end{aligned} \tag{20}$$

Hence, it suffices to analyze (20). Plugging in Definition 24 for entangled Gaussian cosets, we get

$$\begin{aligned} &(\langle\boldsymbol{x}|_A \otimes \mathbb{1}_B)|\mathcal{D}_r\rangle\langle\mathcal{D}_r|_{AB}(|\boldsymbol{x}\rangle_A \otimes \mathbb{1}_B) \\ &= q^{-3m} \sum_{\boldsymbol{u},\boldsymbol{v} \in \mathbb{Z}_q^m} \sum_{\boldsymbol{u}',\boldsymbol{v}' \in \mathbb{Z}_q^m} \langle \boldsymbol{x}|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle \langle \mathcal{D}_r^{\boldsymbol{u}',\boldsymbol{v}'}|\boldsymbol{x}\rangle \;\; |\mathcal{D}_r^{\boldsymbol{u},-\boldsymbol{v}}\rangle \langle \mathcal{D}_r^{\boldsymbol{u}',-\boldsymbol{v}'}|_B \\ &= q^{-3m} \sum_{\substack{\boldsymbol{u},\boldsymbol{v} \in \mathbb{Z}_q^m \\ \boldsymbol{u}',\boldsymbol{v}' \in \mathbb{Z}_q^m}} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}-\boldsymbol{u})}\sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}-\boldsymbol{u}')}\omega_q^{\langle \boldsymbol{x}-\boldsymbol{u},\boldsymbol{v}\rangle} \omega_q^{-\langle \boldsymbol{x}-\boldsymbol{u}',\boldsymbol{v}'\rangle} \;\; |\mathcal{D}_r^{\boldsymbol{u},-\boldsymbol{v}}\rangle \langle \mathcal{D}_r^{\boldsymbol{u}',-\boldsymbol{v}'}|_B \\ &= q^{-3m} \sum_{\substack{\boldsymbol{u},\boldsymbol{v} \in \mathbb{Z}_q^m \\ \boldsymbol{u}',\boldsymbol{v}' \in \mathbb{Z}_q^m}} \sum_{\boldsymbol{e},\boldsymbol{e}' \in \mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}-\boldsymbol{u})}\sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}-\boldsymbol{u}')}\sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{e})}\sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{e}')}\cdot \\ &\qquad \omega_q^{\langle \boldsymbol{x},\boldsymbol{v}\rangle}\omega_q^{-\langle \boldsymbol{u},\boldsymbol{v}\rangle}\omega_q^{-\langle \boldsymbol{x},\boldsymbol{v}'\rangle}\omega_q^{\langle \boldsymbol{u}',\boldsymbol{v}'\rangle}\omega_q^{-\langle \boldsymbol{e},\boldsymbol{v}\rangle}\omega_q^{\langle \boldsymbol{e}',\boldsymbol{v}'\rangle} \,|\boldsymbol{u}+\boldsymbol{e} \pmod q\rangle \langle \boldsymbol{u}'+\boldsymbol{e}' \pmod q|_B . \end{aligned}$$

We will now apply Lemma 7 to simplify the summation over $\boldsymbol{v}' \in \mathbb{Z}_q^m$. We have the identity,

$$\sum_{\boldsymbol{v}' \in \mathbb{Z}_q^m} \omega_q^{\langle \boldsymbol{u}'+\boldsymbol{e}',\boldsymbol{v}'\rangle} \cdot \omega_q^{-\langle \boldsymbol{x},\boldsymbol{v}'\rangle} = \prod_{i \in [m]} \sum_{v_i' \in \mathbb{Z}_q} \omega_q^{(u_i'+e_i')\cdot v_i'} \cdot \omega_q^{-x_i \cdot v_i'} = \prod_{i \in [m]} q \cdot \delta_{u_i'+e_i',x_i} = q^m \delta_{\boldsymbol{u}'+\boldsymbol{e}',\boldsymbol{x}}. \tag{21}$$

In other words, Eq. (21) implies $\boldsymbol{x} \equiv \boldsymbol{u}' + \boldsymbol{e}' \pmod q$. Note also that $D_{\mathbb{Z}_q^m-\boldsymbol{x},r}$ is normalized, since

$$\sum_{\boldsymbol{u}' \in \mathbb{Z}_q^m} D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}-\boldsymbol{u}') = 1. \tag{22}$$

Therefore, using Eq. (21) and Eq. (22) we obtain the desired identity

$$\mathrm{Tr}_A[(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|_A \otimes \mathbb{1}_B)\omega_{AB}] = q^{-2m} \sum_{\boldsymbol{u},\boldsymbol{v},\boldsymbol{e}\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{e})D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}-\boldsymbol{u})}\omega_q^{-\langle \boldsymbol{e},\boldsymbol{v}\rangle}\omega_q^{\langle \boldsymbol{x}-\boldsymbol{u},\boldsymbol{v}\rangle} |\boldsymbol{u}+\boldsymbol{e} \pmod q\rangle \langle \boldsymbol{x}|_B\,.$$

This proves the claim. □

The following lemma shows that the bipartite state $|\mathcal{D}_r\rangle_{AB}$ is indeed a purification of ω_B in Eq. (19).

Lemma 13 (Purification of uniform mixture of Gaussian cosets)**.** *Let $q \geq 2$ be a modulus, $m \in \mathbb{N}$ and $r > 0$. Then, the entangled Gaussian coset state $|\mathcal{D}_r\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ (Definition 24) is a purification of the uniformly random mixture of Gaussian coset states in system B. In other words,*

$$\mathrm{Tr}_A\left[|\mathcal{D}_r\rangle\langle\mathcal{D}_r|_{AB}\right] = q^{-2m} \sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B\,.$$

Proof. Using the linearity of the partial trace and then Lemma 12, we obtain

$$\begin{aligned}\mathrm{Tr}_A\left[|\mathcal{D}_r\rangle\langle\mathcal{D}_r|_{AB}\right] &= \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} \mathrm{Tr}_A[(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|_A \otimes \mathbb{1}_B)|\mathcal{D}_r\rangle\langle\mathcal{D}_r|_{AB}] \\ &= q^{-2m} \sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_q^m}\sum_{\boldsymbol{e},\boldsymbol{x}\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{e})D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}-\boldsymbol{u})}\omega_q^{-\langle \boldsymbol{e},\boldsymbol{v}\rangle}\omega_q^{\langle \boldsymbol{x}-\boldsymbol{u},\boldsymbol{v}\rangle} |\boldsymbol{u}+\boldsymbol{e} \pmod q\rangle \langle \boldsymbol{x}|_B\,.\end{aligned}$$

Let us now define $\boldsymbol{e}' \equiv \boldsymbol{x}-\boldsymbol{u} \pmod q$. A change of variables $\boldsymbol{x} \mapsto \boldsymbol{u}+\boldsymbol{e}'$ then yields the desired equality,

$$\mathrm{Tr}_A\left[\,|\mathcal{D}_r\rangle\,\langle\mathcal{D}_r|_{AB}\,\right] = q^{-2m} \sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\,\langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B\,.$$

□

Next, we show that an entangled Gaussian coset pair $|\mathcal{D}_r\rangle_{AB}$ is equivalent to a q-ary EPR pair.

Lemma 14 (Equivalence with q-ary EPR pairs)**.** *Let $q \geq 2$ be a modulus, $m \in \mathbb{N}$ and let $r > 0$. Then,*

$$|\mathcal{D}_r\rangle_{AB} = |\phi_q^+\rangle_{AB}, \quad \textit{where} \quad |\phi_q^+\rangle_{AB} = \sqrt{q^{-m}} \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} |\boldsymbol{x}\rangle_A \otimes |\boldsymbol{x}\rangle_B\,.$$

Proof. Recall that $|\mathcal{D}_r\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ in Definition 24 is proportional to the state

$$\begin{aligned}|\mathcal{D}_r\rangle_{AB} &\propto \sum_{\boldsymbol{u}\in\mathbb{Z}_q^m}\sum_{\boldsymbol{v}\in\mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},-\boldsymbol{v}}\rangle_A \otimes |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle_B \\ &= \sum_{\boldsymbol{u}\in\mathbb{Z}_q^m}\sum_{\boldsymbol{e},\boldsymbol{e}'\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{e})}\sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{e}')} \sum_{\boldsymbol{v}\in\mathbb{Z}_q^m} \omega_q^{\langle \boldsymbol{v},\boldsymbol{e}-\boldsymbol{e}'\rangle} |\boldsymbol{u}+\boldsymbol{e} \pmod q\rangle_A \otimes |\boldsymbol{u}+\boldsymbol{e}' \pmod q\rangle_B\,.\end{aligned}$$

From the orthogonality of q-ary Fourier characters (Lemma 7)), we obtain the identity

$$\sum_{\boldsymbol{v}\in\mathbb{Z}_q^m} \omega_q^{\langle \boldsymbol{v},\boldsymbol{e}\rangle}\cdot\omega_q^{-\langle \boldsymbol{v},\boldsymbol{e}'\rangle} = \prod_{i\in[m]}\sum_{v_i\in\mathbb{Z}_q} \omega_q^{v_i\cdot e_i}\cdot\omega_q^{-v_i\cdot e_i'} = \prod_{i\in[m]} q\cdot\delta_{e_i,e_i'} = q^m\delta_{\boldsymbol{e},\boldsymbol{e}'}. \tag{23}$$

Plugging in Eq. (23) into previous expression, we find

$$\begin{aligned}
|\mathcal{D}_r\rangle_{AB} &\propto q^m \sum_{\boldsymbol{u}\in\mathbb{Z}_q^m} \sum_{\boldsymbol{e}\in\mathbb{Z}_q^m} D_{\mathbb{Z}_q^m,r}(\boldsymbol{e})\, |\boldsymbol{u}+\boldsymbol{e} \pmod q\rangle_A \otimes |\boldsymbol{u}+\boldsymbol{e} \pmod q\rangle_B \\
&= q^m \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} \sum_{\boldsymbol{u}\in\mathbb{Z}_q^m} D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}-\boldsymbol{u})\, |\boldsymbol{x}\rangle_A \otimes |\boldsymbol{x}\rangle_B && \text{(change of variables)} \\
&= q^m \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} |\boldsymbol{x}\rangle_A \otimes |\boldsymbol{x}\rangle_B\,,
\end{aligned}$$

where the last equality is due to the fact that the shifted Gaussian is normalized for any $\boldsymbol{x} \in \mathbb{Z}_q^m$. □

The following is a simple consequences of the previous lemma.

Corollary 1 (Gaussian ricochet property)**.** *Let $q \geq 2$ be a modulus, let $m \in \mathbb{N}$ be an integer and let $r > 0$. Let $|\mathcal{D}_r\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ be an entangled Gaussian cosets pair and $M \in L((\mathbb{C}^q)^{\otimes m})$ any matrix. Then,*

$$(M_A \otimes \mathbb{1}_B)\, |\mathcal{D}_r\rangle_{AB} = (\mathbb{1}_A \otimes M_B^T)\, |\mathcal{D}_r\rangle_{AB}\,.$$

Lemma 15 (Projection onto Fourier basis)**.** *Let $q \geq 2$ be a modulus, let $m \in \mathbb{N}$ be an integer and let $r > 0$. Let $|\mathcal{D}_r\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ be an entangled Gaussian cosets pair in systems A and B. Then,*

$$(\mathsf{FT}_q|\boldsymbol{y}\rangle\langle\boldsymbol{y}|_A\mathsf{FT}_q^\dagger \otimes \mathbb{1}_B)\, |\mathcal{D}_r\rangle_{AB} = \sqrt{q^{-m}}\mathsf{FT}_q\, |\boldsymbol{y}\rangle_A \otimes \mathsf{FT}_q^\dagger\, |\boldsymbol{y}\rangle_B\,, \qquad \forall \boldsymbol{y} \in \mathbb{Z}_q^m.$$

Proof. Let $\boldsymbol{y} \in \mathbb{Z}_q^m$. Using the Gaussian ricochet property (Corollary 1) and the equivalence between entangled Gaussian cosets and q-ary EPR pairs (Lemma 14) , we can verify the identity as follows.

$$\begin{aligned}
(\mathsf{FT}_q|\boldsymbol{y}\rangle\langle\boldsymbol{y}|_A\mathsf{FT}_q^\dagger \otimes \mathbb{1}_B)\, |\mathcal{D}_r\rangle_{AB} &= (\mathsf{FT}_q \otimes \mathbb{1}_B)(|\boldsymbol{y}\rangle\langle\boldsymbol{y}|_A \otimes \mathbb{1}_B)(\mathsf{FT}_q^\dagger \otimes \mathbb{1}_B)\, |\mathcal{D}_r\rangle_{AB} \\
&= (\mathsf{FT}_q \otimes \mathbb{1}_B)(|\boldsymbol{y}\rangle\langle\boldsymbol{y}|_A \otimes \mathbb{1}_B)(\mathbb{1}_A \otimes \mathsf{FT}_q^\dagger)\, |\mathcal{D}_r\rangle_{AB} \\
&= (\mathsf{FT}_q \otimes \mathbb{1}_B)(|\boldsymbol{y}\rangle\langle\boldsymbol{y}|_A \otimes \mathbb{1}_B)(\mathbb{1}_A \otimes \mathsf{FT}_q^\dagger)\, |\phi_q^+\rangle_{AB} \\
&= \sqrt{q^{-m}} \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} \mathsf{FT}_q\, |\boldsymbol{y}\rangle\, \langle y\,|\, x\rangle_A \otimes \mathsf{FT}_q^\dagger\, |\boldsymbol{x}\rangle_B \\
&= \sqrt{q^{-m}}\mathsf{FT}_q\, |\boldsymbol{y}\rangle_A \otimes \mathsf{FT}_q^\dagger\, |\boldsymbol{y}\rangle_B\,.
\end{aligned}$$

□

Before we state our entropic uncertainty relations for Gaussian cosets, let us first analyze the measurement outcomes in the entanglement-based setting. We are interested in the outcomes of two complementary observables, the computational basis and the q-ary Fourier basis, which we denote by $\{M_A^{0,x}\}$ and $\{M_A^{1,y}\}$. Suppose also that a CPTP map $\Phi : L(\mathcal{H}_B) \rightarrow L(\mathcal{H}_W \otimes \mathcal{H}_E)$ is applied to system B of the entangled Gaussian coset state ω_{AB}. The aforementioned measurements applied to system A are the following:

- (*Computational basis:*) The generalized set of measurement operators $\{M_A^{0,x}\}$ is applied which represent a computational basis measurement of system A and induces a measurement map $\mathcal{M}_{A\rightarrow X}$,

  $$\mathcal{M}_{A\rightarrow X}(\cdot) = \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} |\boldsymbol{x}\rangle_X \left(M_A^{0,x}\right) \cdot \left(M_A^{0,x}\right)^\dagger \langle\boldsymbol{x}|_X\,.$$

  As a result, we obtain the classical-quantum state $\omega_{XWE} = (\mathcal{M}_{A\rightarrow X} \otimes \mathbb{1}_{WE})(\omega_{AWE})$ given by

  $$\omega_{XWE} = \sum_{\boldsymbol{u}\in\mathbb{Z}_q^m} |\boldsymbol{x}\rangle\langle\boldsymbol{x}|_X \otimes \mathrm{Tr}_A\left[\sqrt{M_A^{0,x}}\omega_{AWE}\sqrt{M_A^{0,x}}\right]. \tag{24}$$

- (*Fourier basis:*) The generalized set of measurement operators $\{M_A^{1,y}\}$ is applied which represent a q-ary Fourier basis measurement of system A and induces a measurement map $\mathcal{M}_{A\to Y}$,

$$\mathcal{M}_{A\to Y}(\cdot) = \sum_{\boldsymbol{y}\in\mathbb{Z}_q^m} |\boldsymbol{y}\rangle_Y \left(M_A^{1,\boldsymbol{y}}\right)\cdot\left(M_A^{1,\boldsymbol{y}}\right)^\dagger \langle\boldsymbol{y}|_Y\,.$$

  As a result, we obtain the classical-quantum state $\omega_{YWE} = (\mathcal{M}_{A\to Y}\otimes\mathbb{1}_{WE})(\omega_{AWE})$ given by

$$\omega_{YWE} = \sum_{\boldsymbol{y}\in\mathbb{Z}_q^m} |\boldsymbol{y}\rangle\langle\boldsymbol{y}|_Y \otimes \mathrm{Tr}_A\left[\sqrt{M_A^{1,\boldsymbol{y}}}\,\omega_{AWE}\sqrt{M_A^{1,\boldsymbol{y}}}\right]. \tag{25}$$

Our first key result on Gaussian coset states is the following entropic uncertainty relation.

Theorem 2 (Uncertainty relation for Gaussian cosets I)**.** *Let $q\geq 2$ be an integer modulus and let $m\in\mathbb{N}$. Let $\omega_{AB} = |\mathcal{D}_r\rangle\langle\mathcal{D}_r|_{AB}\in\mathcal{D}(\mathcal{H}_A\otimes\mathcal{H}_B)$ be an entangled Gaussian coset pair in systems AB, where*

$$|\mathcal{D}_r\rangle_{AB} = q^{-m}\sqrt{q^{-m}}\sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},-\boldsymbol{v}}\rangle_A\otimes|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle_B\,, \qquad \textit{for } r>0.$$

Let $\mathcal{M}_{A\to X}$ and $\mathcal{M}_{A\to Y}$ the measurement channels corresponding to a computational and q-ary Fourier basis measurement of system A, respectfully. Let $\Phi: L(\mathcal{H}_B)\to L(\mathcal{H}_W\otimes\mathcal{H}_E)$ be an arbitrary CPTP *map with outcome $\omega_{AWE} = (\mathbb{1}_A\otimes\Phi_{B\to WE})(\omega_{AB})$. Let $\varepsilon\geq 0$. Then, it holds that*

$$H^\varepsilon_{\min}(X\,|\,E)_\omega + H^\varepsilon_{\max}(Y\,|\,W)_\omega \geq m\cdot\log(q),$$

where the states ω_{XE} and ω_{YW} refer to the marginals of the CQ states Eq. (24) and Eq. (25), respectively.

Proof. Let $\Phi_{B\to WE}$ be a an arbitrary CPTP map. To prove the statement, we apply the entropic uncertainty relation from Proposition 2 to the tripartite state $\omega_{AWE} = (\mathbb{1}_A\otimes\Phi_{B\to WE})(\omega_{AB})$, where $\omega_{AB} = |\mathcal{D}_r\rangle\langle\mathcal{D}_r|_{AB}$ is an entangled Gaussian coset pair in systems AB with

$$|\mathcal{D}_r\rangle_{AB} = q^{-m}\sqrt{q^{-m}}\sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},-\boldsymbol{v}}\rangle_A\otimes|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle_B\,, \qquad \text{for } r>0.$$

Denoting by $\{M_A^{0,x}\}$ and $\{M_A^{1,y}\}$ the POVMs for the computational and q-ary Fourier basis measurement of system A, respectfully, we first observe that their overlap c is given by

$$\mathsf{c} = \max_{x,y}\left\|\sqrt{M_A^{0,x}}\sqrt{M_A^{1,y}}\right\|_\infty^2 = q^{-m}.$$

In other words, the two measurement bases are mutually unbiased, since $\mathsf{c} = 1/q^m$, where $\dim(\mathcal{H}_A) = q^m$. Let us now analyze the post-measurement states after applying the two complementary POVMs $\{M_A^{0,x}\}$ and $\{M_A^{1,y}\}$. Recall that the tripartite state $\omega_{AWE} = (\mathbb{1}_A\otimes\Phi_{B\to WE})(\omega_{AB})$ is given by

$$\omega_{AWE} = q^{-3m}\sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_q^m}\sum_{\boldsymbol{u}',\boldsymbol{v}'\in\mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},-\boldsymbol{v}}\rangle\langle\mathcal{D}_r^{\boldsymbol{u}',-\boldsymbol{v}'}|_A\otimes\Phi_{B\to WE}\Big(|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\langle\mathcal{D}_r^{\boldsymbol{u}',\boldsymbol{v}'}|_B\Big). \tag{26}$$

Then, the computational basis measurement $\{M_A^{0,x}\}$ of system A of the tripartite state ω_{AWE} in Eq. (26) results in the CQ state $\omega_{XWE} = (\mathcal{M}_{A\to X}\otimes \mathbb{1}_B)(\omega_{AWE})$ given by

$$\omega_{XWE} = \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} |\boldsymbol{x}\rangle\langle\boldsymbol{x}|_X \otimes \mathrm{Tr}_A\left[\sqrt{M_A^{0,x}}\,\omega_{AWE}\sqrt{M_A^{0,x}}\right], \tag{27}$$

where we used the fact that the shifted discrete Gaussian distribution is normalized. Similarly, the q-ary Fourier basis measurement $\{M_A^{1,y}\}$ of ω_{AWE} in Eq. (26) results in $\omega_{YWE} = (\mathcal{M}_{A\to Y}\otimes \mathbb{1}_B)(\omega_{AWE})$, where

$$\omega_{YWE} = \sum_{\boldsymbol{y}\in\mathbb{Z}_q^m} |\boldsymbol{y}\rangle\langle\boldsymbol{y}|_Y \otimes \mathrm{Tr}_A\left[\sqrt{M_A^{1,y}}\,\omega_{AWE}\sqrt{M_A^{1,y}}\right]. \tag{28}$$

Let $\varepsilon \geq 0$. Then, applying Proposition 2 to the state ω_{AWE} and the POVMs $\{M_A^{0,x}\}$ and $\{M_A^{1,y}\}$ yields

$$H_{\min}^{\varepsilon}(X\,|\,E)_\omega + H_{\max}^{\varepsilon}(Y\,|\,W)_\omega \geq m\cdot\log(q),$$

where the above (smooth) min- and max-entropies refer to the marginals ω_{XE} and ω_{YW} of the CQ states in Eq. (27) and Eq. (28), respectively. This concludes the proof. □

Theorem 3 (Uncertainty relation for Gaussian cosets II)**.** *Let $q \geq 2$ be an integer, let $m \in \mathbb{N}$ and let $r \in \left[\frac{\sqrt{m}}{\sqrt{2}}, \frac{q}{\sqrt{2m}}\right]$. Let $\sigma \in \mathcal{D}(\mathcal{H}_U\otimes\mathcal{H}_V\otimes\mathcal{H}_B)$ be the Gaussian CCQ coset state defined by*

$$\sigma_{UVB} = \sum_{\boldsymbol{u}\in\mathbb{Z}_q^m} q^{-m}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|_U \otimes \sum_{\boldsymbol{v}\in\mathbb{Z}_q^m} q^{-m}|\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V \otimes |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\,\langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B\,.$$

Let $\Phi : L(\mathcal{H}_B) \to L(\mathcal{H}_W\otimes\mathcal{H}_E)$ be an arbitrary CPTP *map and let $\sigma_{UVWE} = (\mathbb{1}_A\otimes\Phi_{B\to WE})(\sigma_{UVB})$. Let $\varepsilon \geq 4e^{-(\pi-\frac{1}{2}(\ln(2\pi)+1))m}$ and $\bar{\varepsilon} := \frac{\varepsilon}{2}$. Then, the marginals σ_{UE} and σ_{VW} satisfy the uncertainty relation*

$$H_{\min}^{\varepsilon}(U\,|\,E)_\sigma + H_{\max}^{\bar{\varepsilon}}(V\,|\,W)_\sigma \geq m\cdot\log(q).$$

Proof. Let $\sigma \in \mathcal{D}(\mathcal{H}_U\otimes\mathcal{H}_V\otimes\mathcal{H}_B)$ be a Gaussian CCQ coset state and fix an arbitrary CPTP map $\Phi : L(\mathcal{H}_B) \to L(\mathcal{H}_W\otimes\mathcal{H}_E)$ with outcome $\sigma_{UVWE} = (\mathbb{1}_A\otimes\Phi_{B\to WE})(\varrho_{UVB})$. Define the (classical) discrete Gaussian transition channel $\mathcal{N}^r : L(\mathcal{H}_X) \to L(\mathcal{H}_Y)$ with parameter $r > 0$ as follows:

$$\mathcal{N}_{X\to Y}^r(\varrho) \overset{\text{def}}{=} \sum_{\boldsymbol{y}\in\mathbb{Z}_q^m}\sum_{\boldsymbol{x}\in\mathbb{Z}_q^m} D_{\mathbb{Z}_q^m,r}(\boldsymbol{x}-\boldsymbol{y})|\boldsymbol{y}\rangle\langle\boldsymbol{y}|_Y \cdot \mathrm{tr}\Big[|\boldsymbol{x}\rangle\langle\boldsymbol{x}|\varrho\Big], \quad \forall\varrho\in L(\mathcal{H}_X). \tag{29}$$

Let us also define the tripartite state $\omega_{AWE} = (\mathbb{1}_A\otimes\Phi_{B\to WE})(\omega_{AB})$ which is the result of applying the CPTP map Φ to an entangled Gaussian coset pair $\omega_{AB} = |\mathcal{D}_r\rangle\langle\mathcal{D}_r|_{AB}$ in systems AB with

$$|\mathcal{D}_r\rangle_{AB} = q^{-m}\sqrt{q^{-m}}\sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_q^m} |\mathcal{D}_r^{\boldsymbol{u},-\boldsymbol{v}}\rangle_A \otimes |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle_B\,, \quad \text{for } r > 0.$$

Let $\mathcal{M}_{A\to X}$ and $\mathcal{M}_{A\to Y}$ denote the measurement channels corresponding to a computational and q-ary Fourier basis measurement of system A, respectfully. Moreover, let $\omega_{XWE} = (\mathcal{M}_{A\to X}\otimes\mathbb{1}_{WE})(\omega_{AWE})$ and $\omega_{YWE} = (\mathcal{M}_{A\to Y}\otimes\mathbb{1}_{WE})(\omega_{AWE})$ be the resulting outcomes and let ω_{XE} and ω_{YW} be their marginals.

To prove the entropic uncertainty relation for the Gaussian CCQ coset σ_{UVB}, we relate the marginal states of σ_{UVB} to the marginal states ω_{XE} and ω_{YW}. Let $\sigma_{UE} = \mathrm{tr}_{VW}[\sigma_{UVWE}]$. Then,

$$
\begin{aligned}
\sigma_{UE} &= q^{-2m} \sum_{\boldsymbol{u}\in\mathbb{Z}_q^m} |\boldsymbol{u}\rangle\langle\boldsymbol{u}|_U \otimes \sum_{\boldsymbol{v}\in\mathbb{Z}_q^m} \mathrm{tr}_W\Big[\Phi_{B\to WE}\Big(\,|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\,\langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B\,\Big)\Big] && \text{(by definition)}\\
&= q^{-2m} \sum_{\boldsymbol{u}\in\mathbb{Z}_q^m} |\boldsymbol{u}\rangle\langle\boldsymbol{u}|_U \otimes \sum_{\boldsymbol{e},\boldsymbol{e}'\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{e})}\sqrt{D_{\mathbb{Z}_q^m,r}(\boldsymbol{e}')}\\
&\qquad\qquad \cdot\Big(\sum_{\boldsymbol{v}\in\mathbb{Z}_q^m} \omega_q^{-\langle\boldsymbol{e},\boldsymbol{v}\rangle}\cdot\omega_q^{\langle\boldsymbol{e}',\boldsymbol{v}\rangle}\Big)\ \mathrm{tr}_W\Big[\Phi_{B\to WE}\big(\,|\boldsymbol{u}+\boldsymbol{e}\rangle\,\langle\boldsymbol{u}+\boldsymbol{e}'|_B\,\big)\Big] && \text{(by linearity of }\Phi\text{)}\\
&= q^{-m} \sum_{\boldsymbol{u}\in\mathbb{Z}_q^m} |\boldsymbol{u}\rangle\langle\boldsymbol{u}|_U \otimes \sum_{\boldsymbol{e}\in\mathbb{Z}_q^m} D_{\mathbb{Z}_q^m,r}(\boldsymbol{e})\cdot\mathrm{tr}_W\Big[\Phi_{B\to WE}\big(|\boldsymbol{u}+\boldsymbol{e}\rangle\langle\boldsymbol{u}+\boldsymbol{e}|_B\big)\Big] && \text{(by Lemma 7)}\\
&= q^{-m} \sum_{\boldsymbol{x}\in\mathbb{Z}_q^m}\sum_{\boldsymbol{e}\in\mathbb{Z}_q^m} D_{\mathbb{Z}_q^m,r}(\boldsymbol{e})|\boldsymbol{x}-\boldsymbol{e}\rangle\langle\boldsymbol{x}-\boldsymbol{e}|_U\otimes\mathrm{tr}_W\Big[\Phi_{B\to WE}\big(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|_B\big)\Big] && \text{(change of variables)}\\
&= (\mathcal{N}_{X\to U}^r\otimes\mathbb{1}_E)\circ\mathrm{tr}_W\big[(\mathbb{1}_X\otimes\Phi_{B\to WE})\circ(\mathcal{M}_{A\to X}\otimes\mathbb{1}_B)(\omega_{AB})\big]\\
&= (\mathcal{N}_{X\to U}^r\otimes\mathbb{1}_E)\circ\mathrm{tr}_W\big[(\mathcal{M}_{A\to X}\otimes\mathbb{1}_{WE})\circ(\mathbb{1}_A\otimes\Phi_{B\to WE})(\omega_{AB})\big] && (\mathcal{M}\text{ and }\Phi\text{ commute})\\
&= (\mathcal{N}_{X\to U}^r\otimes\mathbb{1}_E)(\omega_{XE}).
\end{aligned}
$$

Here, we used that $\mathcal{M}_{A\to X}$ and $\Phi_{B\to WE}$ commute because they act on distinct systems. Let us now analyze the complementary marginal state $\sigma_{VW} = \mathrm{tr}_{UE}[\sigma_{UVWE}]$. Because FT_q is unitary, we have the identity

$$
\begin{aligned}
\sigma_{VW} &= q^{-2m}\sum_{\boldsymbol{v}\in\mathbb{Z}_q^m}|\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V\otimes\sum_{\boldsymbol{u}\in\mathbb{Z}_q^m}\mathrm{tr}_E\Big[\Phi_{B\to WE}\Big(\,|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\,\langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B\,\Big)\Big]\\
&= q^{-2m}\sum_{\boldsymbol{v}\in\mathbb{Z}_q^m}|\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V\otimes\sum_{\boldsymbol{u}\in\mathbb{Z}_q^m}\mathrm{tr}_E\Big[\Phi_{B\to WE}\Big(\,|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\,\langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B\,\Big)\Big]\\
&= q^{-2m}\sum_{\boldsymbol{v}\in\mathbb{Z}_q^m}|\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V\otimes\sum_{\boldsymbol{u}\in\mathbb{Z}_q^m}\mathrm{tr}_E\Big[\Phi_{B\to WE}\Big(\mathsf{FT}_q^\dagger(\mathsf{FT}_q\,|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\,\langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B\,\mathsf{FT}_q^\dagger)\mathsf{FT}_q\Big)\Big].
\end{aligned}
\tag{30}
$$

By assumption, we have that $r\in\big[\frac{\sqrt{m}}{\sqrt{2}},\frac{q}{\sqrt{2m}}\big]$. Thus, by Gaussian Switching Lemma (Lemma 11),

$$
\big\|\,|\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle - \mathsf{FT}_q\,|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\big\|_{\mathrm{tr}} \le 2\exp\left(-(\pi-\frac{1}{2}(\ln(2\pi)+1)\cdot m\right).
$$

Recall that $\mathrm{tr}_E : L(\mathcal{H}_W\otimes\mathcal{H}_E)\to L(\mathcal{H}_W)$ and $\Phi : L(\mathcal{H}_B)\to L(\mathcal{H}_W\otimes\mathcal{H}_E)$ are CPTP maps and that FT_q is unitary. By the contractivity of the trace distance it then follows that

$$
\begin{aligned}
&\Big\|\mathrm{tr}_E\circ\Phi_{B\to WE}\left(\mathsf{FT}_q^\dagger|\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle\langle\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}|\mathsf{FT}_q\right) - \mathrm{tr}_E\circ\Phi_{B\to WE}\left(\mathsf{FT}_q^\dagger(\mathsf{FT}_q|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|\mathsf{FT}_q^\dagger)\mathsf{FT}_q\right)\Big\|_{\mathrm{tr}}\\
&\le \Big\|\,|\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle\langle\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}| - \mathsf{FT}_q|\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|\mathsf{FT}_q^\dagger\Big\|_{\mathrm{tr}}\\
&\le 2\exp\left(-(\pi-\frac{1}{2}(\ln(2\pi)+1)\cdot m\right).
\end{aligned}
\tag{31}
$$

Using the inequality in (31), we can also conclude that

$$
\|\sigma_{VW}-\tilde{\sigma}_{VW}\|_{\mathrm{tr}} \le 2\exp\left(-(\pi-\frac{1}{2}(\ln(2\pi)+1)\cdot m\right).
\tag{32}
$$

where we let

$$\widetilde{\sigma}_{VW} = q^{-2m} \sum_{\boldsymbol{v} \in \mathbb{Z}_q^m} |\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V \otimes \sum_{\boldsymbol{u} \in \mathbb{Z}_q^m} \mathrm{tr}_E \left[\Phi_{B \to WE} \left(\mathsf{FT}_q^\dagger |\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle\langle\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}| \mathsf{FT}_q \right) \right]. \tag{33}$$

Let us now analyze the marginal state in (33). By linearity and by Lemma 7, it follows that

$$\begin{aligned}
\widetilde{\sigma}_{VW} &= q^{-2m} \sum_{\boldsymbol{v} \in \mathbb{Z}_q^m} |\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V \otimes \sum_{\boldsymbol{u} \in \mathbb{Z}_q^m} \mathrm{tr}_E \left[\Phi_{B \to WE} \left(\mathsf{FT}_q^\dagger |\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}\rangle\langle\mathcal{D}_r^{*\boldsymbol{u},\boldsymbol{v}}| \mathsf{FT}_q \right) \right] \\
&= q^{-2m} \sum_{\boldsymbol{v} \in \mathbb{Z}_q^m} |\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V \otimes \mathrm{tr}_E \Bigg[\Phi_{B \to WE} \Bigg(\mathsf{FT}_q^\dagger \Big(\sum_{\boldsymbol{e},\boldsymbol{e}' \in \mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m, q/2r}(\boldsymbol{e})} \sqrt{D_{\mathbb{Z}_q^m, q/2r}(\boldsymbol{e}')} \\
&\qquad \cdot \Big(\sum_{\boldsymbol{u} \in \mathbb{Z}_q^m} \omega_q^{\langle \boldsymbol{e},\boldsymbol{u} \rangle} \cdot \omega_q^{-\langle \boldsymbol{e}',\boldsymbol{u} \rangle} \Big) |\boldsymbol{v} + \boldsymbol{e}\rangle\langle\boldsymbol{v} + \boldsymbol{e}|_B \Big) \mathsf{FT}_q \Bigg) \Bigg] \\
&= q^{-m} \sum_{\boldsymbol{u} \in \mathbb{Z}_q^m} |\boldsymbol{u}\rangle\langle\boldsymbol{u}|_V \otimes \sum_{\boldsymbol{e} \in \mathbb{Z}_q^m} D_{\mathbb{Z}_q^m, q/2r}(\boldsymbol{e}) \cdot \mathrm{tr}_E \left[\Phi_{B \to WE} \left(\mathsf{FT}_q^\dagger |\boldsymbol{u} + \boldsymbol{e}\rangle\langle\boldsymbol{u} + \boldsymbol{e}|_B \mathsf{FT}_q \right) \right] \\
&= q^{-m} \sum_{\boldsymbol{y} \in \mathbb{Z}_q^m} \sum_{\boldsymbol{e} \in \mathbb{Z}_q^m} D_{\mathbb{Z}_q^m, q/2r}(\boldsymbol{e}) |\boldsymbol{y} - \boldsymbol{e}\rangle\langle\boldsymbol{y} - \boldsymbol{e}|_V \otimes \mathrm{tr}_E \left[\Phi_{B \to WE} \left(\mathsf{FT}_q^\dagger |\boldsymbol{y}\rangle\langle\boldsymbol{y}|_B \mathsf{FT}_q \right) \right] \\
&= (\mathcal{N}_{Y \to V}^{q/2r} \otimes \mathbb{1}_W) \circ \mathrm{tr}_E \left[(\mathbb{1}_Y \otimes \Phi_{B \to WE}) \circ (\mathcal{M}_{A \to Y} \otimes \mathbb{1}_B)(\omega_{AB}) \right] \\
&= \mathcal{N}_{Y \to V}^{q/2r} \otimes \mathbb{1}_W) \circ \mathrm{tr}_E \left[(\mathcal{M}_{A \to Y} \otimes \mathbb{1}_{WE}) \circ (\mathbb{1}_A \otimes \Phi_{B \to WE})(\omega_{AB}) \right] \\
&= (\mathcal{N}_{Y \to V}^{q/2r} \otimes \mathbb{1}_W)(\omega_{YW}).
\end{aligned}$$

Here, we used Lemma 15 and that $\mathcal{M}_{A \to Y}$ and $\Phi_{B \to WE}$ commute because they act on distinct systems.

Let $\varepsilon \geq 4e^{-(\pi - \frac{1}{2}(\ln(2\pi)+1))m}$ be a smoothing parameter and recall that the uncertainty relation smooth min- and max-entropies in Theorem 2 with respect to the entangled coset ω_{AB} yields

$$H_{\min}^{\varepsilon}(X \,|\, E)_\omega + H_{\max}^{\varepsilon}(Y \,|\, W)_\omega \geq m \cdot \log(q). \tag{34}$$

By the *data-processing inequality* (Theorem 1), we get that

$$H_{\min}^{\varepsilon}(X \,|\, E)_\omega \leq H_{\min}^{\varepsilon}(U \,|\, E)_{(\mathcal{N}_{X \to U}^{r} \otimes \mathbb{1}_E)(\omega)} = H_{\min}^{\varepsilon}(U \,|\, E)_\sigma \tag{35}$$

as well as

$$H_{\max}^{\varepsilon}(Y \,|\, W)_\omega \leq H_{\max}^{\varepsilon}(V \,|\, W)_{(\mathcal{N}_{Y \to V}^{q/2r} \otimes \mathbb{1}_W)(\omega)} = H_{\max}^{\varepsilon}(V \,|\, W)_{\widetilde{\sigma}}. \tag{36}$$

Let $\bar{\varepsilon} = \frac{\varepsilon}{2}$. Since the smoothing parameter satisfies $\varepsilon \geq 4e^{-(\pi - \frac{1}{2}(\ln(2\pi)+1))m}$, it follows from (32) that

$$\begin{aligned}
\|\sigma_{VW} - \widetilde{\sigma}_{VW}\|_{\mathrm{tr}} &\leq 2 \exp\left(-(\pi - \frac{1}{2}\left(\ln(2\pi) + 1\right) \cdot m \right) \\
&\leq \frac{\varepsilon}{2} = \bar{\varepsilon}.
\end{aligned}$$

Therefore, by the definition of the smooth max-entropy, we find

$$\begin{aligned}
H_{\max}^{\varepsilon}(V \,|\, W)_{\widetilde{\sigma}} &= \inf_{\substack{\varrho_{VW} \\ P(\widetilde{\sigma}_{VW}, \varrho_{VW}) \leq \varepsilon}} H_{\max}(V \,|\, W)_\varrho \\
&\leq \inf_{\substack{\varrho_{VW} \\ P(\sigma_{VW}, \varrho_{VW}) \leq \bar{\varepsilon}}} H_{\max}(V \,|\, W)_\varrho = H_{\max}^{\bar{\varepsilon}}(V \,|\, W)_\sigma.
\end{aligned} \tag{37}$$

Putting everything together, it follows from (34), (35),(36) and (37) that

$$H_{\min}^{\varepsilon}(U \,|\, E)_{\sigma} + H_{\max}^{\bar{\varepsilon}}(V \,|\, W)_{\sigma} \geq m \cdot \log(q).$$

This proves the claim. □

Entropic trade-off relations. In this section, we draw several conclusions from our entropic uncertainty relations for Gaussian coset states. Namely, we show that any measurement that yields an outcome which is *highly correlated* with a q-ary Fourier basis measurement outcome immediately renders a hypothetical computational basis measurement impossible to predict.

In order to quantify the correlation between two vectors in $\mathbb{Z}_q^m$, we introduce the following Boolean flag F^{corr} which is parameterized by two rounding parameters $0 \leq p < q$ and $\delta \in (0,1)$.

Definition 25 (Correlation flag)**.** *Let $q \geq 2$ be a modulus and let $m \in \mathbb{N}$. Let $0 \leq p < q$ and $\delta \in (0,1)$ be rounding parameters. We define the q-ary correlation flag $F^{\mathsf{corr}} : \mathbb{Z}_q^m \times \mathbb{Z}_q^m \to \{0,1\}$ as the function*

$$F^{\mathsf{corr}}(\boldsymbol{x}, \boldsymbol{y}) := \begin{cases} 1 & \text{if } \omega(\lfloor \boldsymbol{x} - \boldsymbol{y} \rceil_p) < m\delta \\ 0 & \text{otherwise.} \end{cases} \tag{38}$$

Here, ω denotes the Hamming weight of a bit string and, for vectors $x \in \mathbb{Z}_q$, we use the rounding function $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \{0,1\}$ such that $\lfloor x \rceil_p = 0$, if x as an element of $\mathbb{Z} \cap (-\frac{q}{2}, \frac{q}{2}]$ lies within $\mathbb{Z} \cap (-\frac{p}{2}, \frac{p}{2}]$, and $\lfloor x \rceil_p = 1$, otherwise. We extend it to vectors $\boldsymbol{x} \in \mathbb{Z}_q^m$ by defining $\lfloor \boldsymbol{x} \rceil_p = (\lfloor x_1 \rceil_p, \ldots, \lfloor x_m \rceil_p) \in \{0,1\}^m$.

Note that Definition 25 allows us to characterize the probability that two (classical) systems XY of a density matrix $\varrho \in \mathcal{D}(\mathcal{H}_{XY})$ are highly correlated. Defining the projector on the correlated subset of XY,

$$\Pi_{XY}^{\mathsf{corr}} = \sum_{\substack{\boldsymbol{x},\boldsymbol{y} \in \mathbb{Z}_q^m \text{ s.t.} \\ F^{\mathsf{corr}}(\boldsymbol{x},\boldsymbol{y}) = 1}} |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y,$$

we obtain the following identity for the probability that XY are correlated:

$$\Pr[F^{\mathsf{corr}} = 1]_{\varrho} = \mathrm{Tr}[\Pi_{XY}^{\mathsf{corr}} \varrho].$$

Lemma 16. *Let $\varrho_{XY} \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_Y)$ be classical state with $\dim(\mathcal{H}_X) = \dim(\mathcal{H}_Y) = q^m$, where $q \geq 2$ and $m \geq 1$. Let $0 \leq p < q$ and $\delta \in (0,1)$ be parameters. Suppose that $\Pr[F^{\mathsf{corr}} = 1]_{\varrho} = 1$. Then,*

$$H_{\max}(X \,|\, Y)_{\varrho} \leq m \cdot \log(p) + m \cdot h_2(\delta).$$

Proof. Using that $\Pr[F^{\mathsf{corr}} = 1]_\varrho = 1$, we can bound the max-entropy as in [Tom13, Sec. 4.3.2] to obtain

$$
\begin{aligned}
H_{\max}(X \,|\, Y)_\varrho = \log\Bigg(\sum_{\boldsymbol{y} \in \mathbb{Z}_q^m} \Pr[Y = \boldsymbol{y}]_\varrho \cdot 2^{H_{\max}(X \,|\, Y = y)_\varrho} \Bigg)
&\leq \max_{\substack{\boldsymbol{y} \in \mathbb{Z}_q^m \\ \Pr[Y = \boldsymbol{y}]_\varrho > 0}} H_{\max}(X \,|\, Y = \boldsymbol{y})_\varrho \\
&\leq \max_{\substack{\boldsymbol{y} \in \mathbb{Z}_q^m \\ \Pr[Y = \boldsymbol{y}]_\varrho > 0}} \log |\{\boldsymbol{x} \in \mathbb{Z}_q^m \,:\, \Pr[X = \boldsymbol{x} \,|\, Y = \boldsymbol{y}]_\varrho > 0\}| \\
&= \max_{\boldsymbol{y} \in \mathbb{Z}_q^m} \log |\{\boldsymbol{x} \in \mathbb{Z}_q^m \,:\, \Pr[X = \boldsymbol{x} \wedge Y = \boldsymbol{y}]_\varrho > 0\}| \\
&\leq \max_{\boldsymbol{y} \in \mathbb{Z}_q^m} \log |\{\boldsymbol{x} \in \mathbb{Z}_q^m \,:\, \omega(\lfloor \boldsymbol{x} - \boldsymbol{y} \rfloor_p) < m\delta\}| \\
&\leq \log\Bigg(\sum_{\gamma=0}^{\lfloor m\delta \rfloor} \binom{m}{\gamma} \; p^m \Bigg) \\
&\leq m \cdot \log(p) + m \cdot h_2(\delta).
\end{aligned}
$$

□

Theorem 4 (Entropic trade-off relation for Gaussian cosets)**.** *Let $q \geq 2$ be an integer, $m \in \mathbb{N}$ and $r > 0$. Let $\sigma \in \mathcal{D}(\mathcal{H}_U \otimes \mathcal{H}_V \otimes \mathcal{H}_B)$ be the Gaussian CCQ coset state defined by*

$$
\sigma_{UVB} = \sum_{\boldsymbol{u} \in \mathbb{Z}_q^m} q^{-m} |\boldsymbol{u}\rangle\langle\boldsymbol{u}|_U \otimes \sum_{\boldsymbol{v} \in \mathbb{Z}_q^m} q^{-m} |\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V \otimes |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle \, \langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B \,.
$$

Let $\Phi : L(\mathcal{H}_B) \to L(\mathcal{H}_W \otimes \mathcal{H}_E)$ be an arbitrary CPTP *map and let $\sigma_{UVWE} = (\mathbb{1}_A \otimes \Phi_{B \to WE})(\sigma_{UVB})$, where W is a classical system. Let $0 \leq p < q$ and $\delta \in (0,1)$ be rounding parameters. Suppose that*

$$
\Pr[F^{\mathsf{corr}} = 1]_{\sigma_{VW}} = 1 - \varepsilon,
$$

for some $\varepsilon \geq 4e^{-(\pi - \frac{1}{2}(\ln(2\pi)+1))m}$. Then, the marginal CQ state σ_{UE} satisfies

$$
H_{\min}^{\sqrt{\varepsilon}}(U \,|\, E)_\sigma \geq m \cdot \log(q) - m \cdot \log(p) - m \cdot h_2(\delta).
$$

Proof. By assumption, there exists $\varepsilon \geq 4e^{-(\pi - \frac{1}{2}(\ln(2\pi)+1))m}$ such that the marginal σ_{VW} of σ_{UVWE} satisfies

$$
\Pr[F^{\mathsf{corr}} = 1]_{\sigma_{VW}} = 1 - \varepsilon. \tag{39}
$$

Using Lemma 3, we can remove the possibility that $F^{\mathsf{corr}} = 0$ occurs with respect to σ_{VW} by instead considering the smoothed state $\tilde{\sigma}_{VW}$ with $\Pr[F^{\mathsf{corr}} = 1]_{\tilde{\sigma}_{VW}} = 1$, which satisfies

$$
P(\sigma_{VW}, \tilde{\sigma}_{VW}) \leq \sqrt{\varepsilon},
$$

where P denotes the purified distance. Note that, by the definition of the smooth max-entropy,

$$
H_{\max}^{\sqrt{\varepsilon}}(V \,|\, W)_\sigma = \inf_{\substack{\varrho_{VW} \\ P(\sigma_{VW}, \varrho_{VW}) \leq \sqrt{\varepsilon}}} H_{\max}(V \,|\, W)_\varrho \;\leq\; H_{\max}(V \,|\, W)_{\tilde{\sigma}}. \tag{40}
$$

Using that $\Pr[F^{\mathsf{corr}} = 1]_{\tilde{\sigma}_{VW}} = 1$, it then follows from (40) and Lemma 16 that

$$H_{\max}^{\sqrt{\varepsilon}}(V \mid W)_{\tilde{\sigma}} \leq m \cdot \log(p) + m \cdot h_2(\delta). \tag{41}$$

Recall that the uncertainty relation smooth min- and max-entropies in Theorem 3 yields

$$H_{\min}^{\sqrt{\varepsilon}}(U \mid E)_{\sigma} + H_{\max}^{\sqrt{\varepsilon}}(V \mid W)_{\sigma} \geq m \cdot \log(q).$$

Therefore, plugging in (40) and (41) into the inequality above, we can conclude that

$$H_{\min}^{\sqrt{\varepsilon}}(U \mid E)_{\sigma} \geq m \cdot \log(q) - m \cdot \log(p) - m \cdot h_2(\delta).$$

This proves the claim. □

Proposition 3 (Guessing probability trade-off relation for Gaussian cosets). *Let $q \geq 2$ be an integer, $m \in \mathbb{N}$ and $r > 0$. Let $\sigma \in \mathcal{D}(\mathcal{H}_U \otimes \mathcal{H}_V \otimes \mathcal{H}_B)$ be the Gaussian CCQ coset state defined by*

$$\sigma_{UVB} = \sum_{\boldsymbol{u} \in \mathbb{Z}_q^m} q^{-m} |\boldsymbol{u}\rangle\langle\boldsymbol{u}|_U \otimes \sum_{\boldsymbol{v} \in \mathbb{Z}_q^m} q^{-m} |\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V \otimes |\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}\rangle\,\langle\mathcal{D}_r^{\boldsymbol{u},\boldsymbol{v}}|_B\,.$$

Let $\Phi : L(\mathcal{H}_B) \rightarrow L(\mathcal{H}_W \otimes \mathcal{H}_E)$ be an arbitrary CPTP *map and let $\sigma_{UVWE} = (\mathbb{1}_A \otimes \Phi_{B \rightarrow WE})(\sigma_{UVB})$, where W is a classical system. Let $0 \leq p < q$ and $\delta \in (0,1)$ be rounding parameters. Suppose that the marginal state σ_{VW} satisfies $\Pr[F^{\mathsf{corr}} = 1]_{\sigma_{VW}} = 1 - \varepsilon$, for some $\varepsilon \geq 4e^{-(\pi - \frac{1}{2}(\ln(2\pi)+1))m}$. Then,*

$$p_{\text{guess}}(U|E)_{\sigma} \leq 2^{-m \cdot \log(q) + m \cdot \log(p) + m \cdot h_2(\delta)} + \sqrt{\varepsilon}.$$

Proof. From Theorem 4 it follows that the marginal σ_{UE} of the CCQ state σ_{UVWE} satisfies

$$H_{\min}^{\sqrt{\varepsilon}}(U \mid E)_{\sigma} \geq m \cdot \log(q) - m \cdot \log(p) - m \cdot h_2(\delta), \tag{42}$$

for $\varepsilon \geq 4e^{-(\pi - \frac{1}{2}(\ln(2\pi)+1))m}$. Using Lemma 2, we can argue that the state σ^* which optimizes the smooth min-entropy in (42), i.e. $H_{\min}(U \mid E)_{\sigma^*} = H_{\min}^{\sqrt{\varepsilon}}(U \mid E)_{\sigma}$, is of the same CQ form as σ. Therefore, by Lemma 5 and the simple fact that $\|\sigma - \sigma^*\|_{\text{tr}} \leq P(\sigma, \sigma^*)$, we obtain the following upper bound given by

$$p_{\text{guess}}(U|E)_{\sigma} \leq p_{\text{guess}}(U|E)_{\sigma^*} + \sqrt{\varepsilon}. \tag{43}$$

Putting everything together, we find that

$$\begin{aligned}
p_{\text{guess}}(U|E)_{\sigma} &\leq p_{\text{guess}}(U|E)_{\sigma^*} + \sqrt{\varepsilon} && \text{(by ineq. (43))}\\
&= 2^{-H_{\min}(U|E)_{\sigma^*}} + \sqrt{\varepsilon} && \\
&= 2^{-H_{\min}^{\sqrt{\varepsilon}}(U|E)_{\sigma}} + \sqrt{\varepsilon} && \text{(by definition)}\\
&\leq 2^{-m \cdot \log(q) + m \cdot \log(p) + m \cdot h_2(\delta)} + \sqrt{\varepsilon}. && \text{(by ineq. (42))}
\end{aligned}$$

□

5 Quantum Proofs of Deletion for Learning with Errors

In this section, we use our encoding based on Gaussian coset states from Section 4.1 to construct a quantum proof-of-deletion protocol which allows a client to be convinced that a sample from the LWE distribution has been deleted by a untrusted party. Our protocol achieves *pseudoentropic deletion* (Definition 20) which implies that any efficient (possibly malicious) prover can recover the encoded sample from the LWE distribution with at most negligible probability once deletion has taken place (assuming that the prover succeeds with sufficiently high probability during the verification step).

5.1 Protocol

Let us begin by introducing our construction.

Parameters. Let $\lambda \in \mathbb{N}$ be the security parameter and let $n \in \mathbb{N}$. We choose the following set of parameters for our QPD protocol for LWE (each parameterized by the security parameter λ).

- an integer modulus $q \geq 2$.
- an integer $m = \Omega(n \log q)$.
- noise ratios $\alpha, \beta \in (0,1)$ with $2\sqrt{n} \leq \alpha q < \beta q < q/\sqrt{2m}$ such that β/α is superpolynomial.
- a rounding parameter $p = \sqrt{m}/2\beta$ and arbitrary $\delta \in (0,1)$.

Protocol 1 (Quantum Proof-of-Deletion Protocol for Learning with Errors)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter. The quantum proof-of-deletion protocol* $\mathsf{QPD} = (\mathsf{Setup}, \mathsf{Samp}, \mathcal{V}, \mathcal{P})$ *for the Learning with Errors distribution* $\mathsf{LWE}^m_{n,q,\alpha q}$ *(Definition 14) consists of four efficient (interactive) algorithms:*

$\mathsf{Samp}(1^\lambda)$*: Outputs a sample* $(\boldsymbol{A}, \boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}_0 \pmod q) \sim \mathsf{LWE}^m_{n,q,\alpha q}$ *with* $\mathsf{pk} \leftarrow \boldsymbol{A}$.

$\mathsf{Setup}(1^\lambda, \mathsf{pk}, x)$*: Generates an auxiliary input pair* (vk, ϱ_P) *for* $\mathcal{V}$ *and* $\mathcal{P}$ *as follows:*

- *Sample a uniformly random vector* $\boldsymbol{v} \xleftarrow{\$} \mathbb{Z}_q^m$.
- *Parse the sample* $(\boldsymbol{A}, \boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}_0 \pmod q) \leftarrow (\mathsf{pk}, \boldsymbol{x})$.
- *Output* (vk, ϱ_P)*, where* $\mathsf{vk} \leftarrow \boldsymbol{v}$ *and* ϱ_P *is the quantum state given by*

$$|\mathcal{D}^{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}_0,\boldsymbol{v}}_{\beta q}\rangle_P = \sum_{\boldsymbol{e}\in\mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,\beta q}(\boldsymbol{e})}\,\omega_q^{-\langle \boldsymbol{e},\boldsymbol{v}\rangle}\,|\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}_0+\boldsymbol{e} \pmod q\rangle_P .$$

$\mathcal{V}(1^\lambda, \mathsf{vk}, \pi)$*: Verify a classical deletion witness* π *as follows:*

- *Parse the verification key as* $\boldsymbol{v} \leftarrow \mathsf{vk}$.
- *Output* $F^{\mathsf{corr}}(\boldsymbol{v}, \pi) \in \{0,1\}$ *(see Definition 25) with parameters* $0 \leq p < q$ *and* $\delta \in (0,1)$.

$\mathcal{P}(1^\lambda, \mathsf{pk}, \varrho_P)$*: Measure all qudits of* ϱ_P *in the* q*-ary Fourier basis to obtain a witness* $\pi \in \mathbb{Z}_q^m$.

5.2 Completeness

Let us now prove the completeness of Protocol 1 which says that an honest prover is always accepted with overwhelming probability by the verifier.

Proposition 4 (Completeness)**.** *Let $n \in \mathbb{N}$, let $q \geq 2$ be an integer modulus and let $m = \Omega(n \log q)$, each parameterized by $\lambda \in \mathbb{N}$. Let $\alpha, \beta \in (0,1)$ be noise ratios with $2\sqrt{n} \leq \alpha q < \beta q < q/\sqrt{2m}$ such that β/α is superpolynomial. Let $p = \sqrt{m}/2\beta$ and $\delta \in (0,1)$ be rounding parameters. Then, the quantum proof-of-deletion protocol $\mathsf{QPD} = (\mathsf{Setup}, \mathsf{Samp}, \mathcal{V}, \mathcal{P})$ for the $\mathsf{LWE}^m_{n,q,\alpha q}$ distribution in Protocol 1 has completeness $c(\lambda) = 1 - 2\exp\big(-(\pi - \frac{1}{2}\big(\ln(2\pi)+1\big)\cdot m\big)$. In other words, it holds that*

$$\Pr\left[\mathcal{V}(1^\lambda, \mathsf{vk}, \pi) = 1 \,\middle|\, \substack{(\mathsf{pk},x)\leftarrow\mathsf{Samp}(1^\lambda)\\ (\mathsf{vk},\varrho_P)\leftarrow\mathsf{Setup}(1^\lambda,\mathsf{pk},x)\\ \pi\leftarrow\mathcal{P}(1^\lambda,\mathsf{pk},\varrho_P)}\right] \geq 1 - 2^{-\Omega(m)}.$$

Proof. Fix $\lambda \in \mathbb{N}$ and consider an output $(\boldsymbol{A}, \boldsymbol{A}\cdot\boldsymbol{s} + \boldsymbol{e}_0 \pmod q) \leftarrow \mathsf{Samp}(1^\lambda)$ which is sampled from the $\mathsf{LWE}^m_{n,q,\beta q}$ distribution. Recall that the procedure $\mathsf{Setup}(1^\lambda, \boldsymbol{A}, \boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e})$ outputs a pair (vk, ϱ_P), where $\mathsf{vk} = \boldsymbol{v} \in \mathbb{Z}_q^m$ serves as the verification key (handed to $\mathcal{V}$) and where ϱ_P is a Gaussian coset state $|\mathcal{D}^{\boldsymbol{As}+\boldsymbol{e}_0,\boldsymbol{v}}_{\beta q}\rangle$ which is handed to $\mathcal{P}$. Because the (honest) prover $\mathcal{P}(1^\lambda, \mathsf{pk}, \varrho_P)$ measures each qudit of ϱ_P in the Fourier basis, we can now analyze the probability that $\mathcal{V}(1^\lambda, \mathsf{vk}, \pi) = 1$ as follows. Given our choice of $2\sqrt{n} \leq \alpha q < \beta q < q/\sqrt{2m}$, we can apply the Gaussian Switching Lemma (Lemma 11) and argue that a q-ary Fourier basis measurement yields a post-measurement state $\tilde{\tau}$ within distance,

$$\|\tilde{\tau} - \tau\|_{\mathrm{tr}} \leq 2\exp\Big(-\big(\pi - \frac{1}{2}\big(\ln(2\pi)+1\big)\cdot m\Big) = 2^{-\Omega(m)},$$

of the classical discrete Gaussian mixture defined by

$$\tau = \sum_{\boldsymbol{e}\in\mathbb{Z}_q^m} D_{\mathbb{Z}_q^m,1/2\beta}(\boldsymbol{e}) |\boldsymbol{v}+\boldsymbol{e} \pmod q\rangle\langle \boldsymbol{v}+\boldsymbol{e} \pmod q|. \tag{44}$$

Because the truncated discrete Gaussian $D_{\mathbb{Z}_q^m,1/2\beta}$ is supported on $\{\boldsymbol{x} \in \mathbb{Z}_q^m : \|\boldsymbol{x}\|_\infty \leq \sqrt{m}/2\beta\}$, it follows from Lemma 5 that verification is successful with overwhelming probability at least

$$\Pr\left[\mathcal{V}(1^\lambda, \mathsf{vk}, \pi) = 1 \,\middle|\, \substack{(\mathsf{pk},x)\leftarrow\mathsf{Samp}(1^\lambda)\\ (\mathsf{vk},\varrho_P)\leftarrow\mathsf{Setup}(1^\lambda,\mathsf{pk},x)\\ \pi\leftarrow\mathcal{P}(1^\lambda,\mathsf{pk},\varrho_P)}\right] \geq 1 - 2\exp\Big(-\big(\pi - \frac{1}{2}\big(\ln(2\pi)+1\big)\cdot m\Big)$$

for the choice of $p = \sqrt{m}/2\beta$. This proves the claim. □

5.3 Pseudoentropic deletion

Recall that in Proposition 4 we proved the completeness of Protocol 1. Specifically, we showed that an honest prover is always accepted with probability at least $1 - \xi(\lambda)$, where

$$\xi(\lambda) = 2\exp\Big(-\big(\pi - \frac{1}{2}\big(\ln(2\pi)+1\big)\cdot m\Big), \qquad \text{for } \lambda \in \mathbb{N}.$$

Let us now suppose that we have a (possibly malicious) prover that passes verification with probability $1 - \varepsilon(\lambda)$, where $\varepsilon(\lambda)$ is greater than $\xi(\lambda)$. What does that imply about the prover's ability to guess the encoded LWE sample once the verifier is convinced that deletion has taken place? We show the following.

Theorem 5 (Pseudoentropic deletion)**.** *Let $n \in \mathbb{N}$, let $q \geq 2$ be an integer modulus and let $m = \Omega(n \log q)$, each parameterized by the security parameter $\lambda \in \mathbb{N}$. Let $\alpha, \beta \in (0,1)$ be noise ratio parameters with $2\sqrt{n} \leq \alpha q < \beta q < q/\sqrt{m}$ such that the ratio β/α is superpolynomial. Let $p = \sqrt{m}/\beta$ and $\delta \in (0,1)$ be rounding parameters. Suppose that $\widetilde{\mathcal{P}}$ is a (possibly malicious) prover that passes verification with probability $1 - \varepsilon(\lambda)$, where $\varepsilon(\lambda) \geq 4e^{-(\pi - \frac{1}{2}(\ln(2\pi)+1))m}$. Then, the advantage in the deletion experiment $\mathsf{Exp}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{\mathcal{P}}}(\lambda)$ in Experiment 1 with respect to the prover $\widetilde{\mathcal{P}}$ is at most*

$$\mathsf{Adv}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{\mathcal{P}}}(\lambda) \leq 2^{-m(\lambda)\cdot\log q(\lambda) + m(\lambda)\cdot\log p(\lambda) + m(\lambda)\cdot h_2(\delta)} + \sqrt{\varepsilon(\lambda)} + \mathrm{negl}(\lambda).$$

Moreover, if $\varepsilon(\lambda)$ is negligible, the quantum proof-of-deletion protocol $\mathsf{QPD} = (\mathsf{Setup}, \mathsf{Samp}, \mathcal{V}, \mathcal{P})$ for the $\mathsf{LWE}^m_{n,q,\alpha q}$ distribution in Protocol 1 has κ-pseudoentropic deletion with respect to $\widetilde{\mathcal{P}}$ with parameter

$$\kappa(\lambda) = m(\lambda) \cdot \log p(\lambda) + m(\lambda) \cdot h_2(\delta).$$

Proof. Fix $\lambda \in \mathbb{N}$ and consider any (possibly malicious) QPT prover $\widetilde{P}$ characterized (according to Definition 18) by a pair $\Phi_\lambda = (\Phi^0_\lambda, \Phi^1_\lambda)$ of efficient CPTP maps $\Phi^0_\lambda : L(\mathcal{H}_P \otimes \mathcal{H}_K) \to L(\mathcal{H}_\Pi \otimes \mathcal{H}_E)$ and $\Phi^1_\lambda : L(\mathcal{H}_E \otimes \mathcal{H}_K) \to L(\mathcal{H}_{X'})$, where the classical system K contains the public key $\mathsf{pk} = \boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$. For simplicity, we use the compact notation $(\Phi^{0,\mathsf{pk}}_\lambda, \Phi^{1,\mathsf{pk}}_\lambda)$ to hide the dependence on the public key pk as in Definition 18. Suppose that the prover $\widetilde{P}$ passes verification with probability $1 - \varepsilon(\lambda)$, where $\varepsilon(\lambda) \geq 4e^{-(\pi - \frac{1}{2}(\ln(2\pi)+1))m}$. We show that the prover's advantage in $\mathsf{Exp}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{P}}$ (Experiment 1) is at most

$$\mathsf{Adv}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{P}}(\lambda) = \Pr\left[\begin{array}{c|c} \boldsymbol{x}'{=}\boldsymbol{x} & (\mathsf{pk},x){\leftarrow}\mathsf{Samp}(1^\lambda) \\ & (\mathsf{vk},\varrho_P){\leftarrow}\mathsf{Setup}(1^\lambda,\mathsf{pk},x) \\ \wedge & |\pi\rangle\langle\pi|_\Pi{\otimes}\varrho_E{\leftarrow}\Phi^{0,\mathsf{pk}}_{P\to\Pi E}(\varrho_P) \\ & F^{\mathsf{ver}}{\leftarrow}\mathcal{V}(1^\lambda,\mathsf{vk},\pi) \\ F^{\mathsf{ver}}{=}1 & |\boldsymbol{x}'\rangle\langle\boldsymbol{x}'|_{X'}{\leftarrow}\Phi^{1,\mathsf{pk}}_{E\to X'}(\varrho_E) \end{array}\right] \leq 2^{-H_{\mathsf{HILL}}(X_\lambda|K_\lambda)+\kappa(\lambda)} + \sqrt{\varepsilon(\lambda)} + \mathrm{negl}(\lambda),$$

where $H_{\mathsf{HILL}}(X_\lambda|K_\lambda)$ corresponds to the conditional computational pseudoentropy (see Definition 4) of the random variable X_λ with outcome $x \in \mathcal{X}_\lambda$ conditioned on the random variable K_λ with outcome pk. Note that both outcomes are generated by the procedure $\mathsf{Samp}(1^\lambda)$. We can model the prover's uncertainty about the sample $(\boldsymbol{A}, \boldsymbol{A}\cdot\boldsymbol{s} + \boldsymbol{e}_0 \pmod q) \sim \mathsf{LWE}^m_{n,q,\alpha q}$ by analyzing the following CCQ state ϱ_{UVB}, where U and V are classical and where the quantum system P contains the prover's auxiliary input, i.e.

$$\begin{aligned}\varrho_{UVP} = &\sum_{\boldsymbol{A}\in\mathbb{Z}_q^{m\times n}} q^{-(m+n)} \sum_{\boldsymbol{s}\in\mathbb{Z}_q^n} q^{-n} \sum_{\boldsymbol{e}_0\in\mathbb{Z}_q^m} D_{\mathbb{Z}_q^m,\alpha q}(\boldsymbol{e}_0)\, |\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}_0\rangle\langle\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}_0|_U \\ &\otimes \sum_{\boldsymbol{v}\in\mathbb{Z}_q^m} q^{-m}|\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V \otimes |\mathcal{D}^{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}_0,\boldsymbol{v}}_{\beta q}\rangle\langle\mathcal{D}^{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}_0,\boldsymbol{v}}_{\beta q}|_P.\end{aligned} \tag{45}$$

Under the $\mathsf{LWE}^m_{n,q,\alpha q}$ assumption (Definition 15), we have that the following states are indistinguishable

$$\varrho_{UVP} \quad \approx_c \quad \sigma_{UVP} \tag{46}$$

given the public key $\mathsf{pk} = \boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$. Here, σ_{UVP} is the Gaussian CCQ coset state given by

$$\sigma_{UVP} = \sum_{\boldsymbol{u}\in\mathbb{Z}_q^m} q^{-m}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|_U \otimes \sum_{\boldsymbol{v}\in\mathbb{Z}_q^m} q^{-m}|\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V \otimes |\mathcal{D}^{\boldsymbol{u},\boldsymbol{v}}_{\beta q}\rangle\langle\mathcal{D}^{\boldsymbol{u},\boldsymbol{v}}_{\beta q}|_P.$$

In addition, because the (possibly malicious) QPT prover $\widetilde{P}$ is characterized by a pair $(\Phi_\lambda^{0,\mathsf{pk}}, \Phi_\lambda^{1,\mathsf{pk}})$ of efficient CPTP maps, (46) also implies that the following states are indistinguishable,

$$\varrho_{UV\Pi E} = (\mathbb{1}_{UV} \otimes \Phi^{1,\mathsf{pk}}_{P\to\Pi E})(\varrho_{UVP}) \quad \approx_c \quad \sigma_{UV\Pi E} = (\mathbb{1}_{UV} \otimes \Phi^{1,\mathsf{pk}}_{P\to\Pi E})(\sigma_{UVP}). \tag{47}$$

By assumption, we have that the prover $\widetilde{P}$ passes verification with probability $1-\varepsilon(\lambda)$, where we assume that $\varepsilon(\lambda) \geq 4e^{-(\pi-\frac{1}{2}(\ln(2\pi)+1))m}$. In other words, the marginal state $\varrho_{V\Pi} = \mathrm{tr}[\varrho_{UV\Pi E}]$ has the property,

$$\Pr[F^{\mathsf{corr}} = 1]_{\varrho_{V\Pi}} = 1 - \varepsilon(\lambda).$$

From (47) it follows that the marginal state $\sigma_{V\Pi} = \mathrm{tr}[\sigma_{UV\Pi E}]$ satisfies,

$$\Pr[F^{\mathsf{corr}} = 1]_{\sigma_{V\Pi}} = 1 - \varepsilon(\lambda) - \mathrm{negl}(\lambda).$$

Using our entropic trade-off relations in Theorem 4 with smoothing parameter $\bar{\varepsilon}(\lambda) = \varepsilon(\lambda) + \mathrm{negl}(\lambda)$, we then obtain the following lower bound for the smooth min-entropy of the CQ state σ_{UE} given by

$$H_{\min}^{\sqrt{\bar{\varepsilon}}}(U \,|\, E)_\sigma \geq m \cdot \log(q) - m \cdot \log(p) - m \cdot h_2(\delta).$$

Recall that the QPT prover $\widetilde{P}$ is characterized by a pair $(\Phi_\lambda^{0,\mathsf{pk}}, \Phi_\lambda^{1,\mathsf{pk}})$ of efficient CPTP maps which are allowed to depend on the public key $\mathsf{pk} = \boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$ in a classical system K. However, because the CQ state σ_{UE} is completely independent of the public key, we must conclude that

$$H_{\min}^{\sqrt{\bar{\varepsilon}}}(U \,|\, EK)_\sigma = H_{\min}^{\sqrt{\bar{\varepsilon}}}(U \,|\, E)_\sigma \geq m \cdot \log(q) - m \cdot \log(p) - m \cdot h_2(\delta).$$

Because the CQ state ϱ_{UE} is computationally indistinguishable from the CQ state σ_{UE} given the auxiliary system K which contains $\mathsf{pk} = \boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$, we have according to the definition of quantum guessing pseudoentropy (Definition 10) with parameters $T = \mathrm{poly}(\lambda)$ and $\nu(\lambda) = \sqrt{\varepsilon(\lambda)} + \mathrm{negl}(\lambda)$ that

$$H_{\mathrm{guess}}^{T,\nu}(U \,|\, EK)_\varrho \;\geq\; m \cdot \log(q) - m \cdot \log(p) - m \cdot h_2(\delta). \tag{48}$$

Putting everything together, we can therefore bound the prover's advantage as follows:

$$\begin{aligned}\mathsf{Adv}^{\mathsf{del}}_{\mathsf{QPD},\widetilde{P}}(\lambda) &= \Pr\left[\begin{array}{c|c} \boldsymbol{x}'{=}\boldsymbol{x} & (\mathsf{pk},x){\leftarrow}\mathsf{Samp}(1^\lambda) \\ & (\mathsf{vk},\varrho_P){\leftarrow}\mathsf{Setup}(1^\lambda,\mathsf{pk},x) \\ \wedge & |\pi\rangle\langle\pi|_\Pi{\otimes}\varrho_E{\leftarrow}\Phi^{0,\mathsf{pk}}_{P\to\Pi E}(\varrho_P) \\ & F^{\mathsf{ver}}{\leftarrow}\mathcal{V}(1^\lambda,\mathsf{vk},\pi) \\ F^{\mathsf{ver}}{=}1 & |\boldsymbol{x}'\rangle\langle\boldsymbol{x}'|_{X'}{\leftarrow}\Phi^{1,\mathsf{pk}}_{E\to X'}(\varrho_E) \end{array}\right] \\ &\leq 2^{-m\cdot\log(q)+m\cdot\log(p)+m\cdot h_2(\delta)} + \sqrt{\varepsilon(\lambda)} + \mathrm{negl}(\lambda).\end{aligned}$$

Finally, suppose that $\varepsilon(\lambda)$ is negligible. Notice that under the $\mathsf{LWE}^m_{n,q,\alpha q}$ assumption, we have that $H_{\mathsf{HILL}}(X_\lambda|K_\lambda) = m \cdot \log(q)$, where (K_λ, X_λ) correspond to the jointly distributed sample given by $(\boldsymbol{A}, \boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}_0) \sim \mathsf{LWE}^m_{n,q,\alpha q}$ which is generated by the procedure $\mathsf{Samp}(1^\lambda)$. Thus, the QPD protocol $\mathsf{QPD} = (\mathsf{Setup}, \mathsf{Samp}, \mathcal{V}, \mathcal{P})$ for the Learning with Errors distribution in Protocol 1 has κ-pseudoentropic deletion for $\kappa(\lambda) = m(\lambda)\cdot\log p(\lambda) + m(\lambda)\cdot h_2(\delta)$. This proves the claim. □

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

$\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$: *takes as input the parameter* 1^λ *and outputs a public key* pk *and secret key* sk.

$\mathsf{Enc}(\mathsf{pk}, m) \to (\mathsf{vk}, \mathsf{ct})$: *takes as input the public key* pk *and a plaintext* $m \in \mathcal{M}$*, and outputs a classical verification key* vk *together with a quantum ciphertext* ct.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to m'$ **or** $\perp$: *takes as input the secret key* sk *and ciphertext* ct*, and outputs* $m' \in \mathcal{M}$ *or* $\perp$.

$\mathsf{Del}(\mathsf{ct}) \to \pi$: *takes as input a ciphertext* ct *and outputs a classical certificate* π.

$\mathsf{Vrfy}(\mathsf{vk}, \pi) \to \top$ **or** $\perp$: *takes as input the verification key* vk *and certificate* π*, and outputs* $\top$ *or* $\perp$.

Definition 27 (Correctness of $\mathsf{PKE_{CD}}$)**.** *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* $m \in \mathcal{M}$*:*

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \neq m \,\middle|\, \substack{(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)}\right] \leq \mathrm{negl}(\lambda).$$

(Verification correctness:) For any $\lambda \in \mathbb{N}$*, and for any* $m \in \mathcal{M}$*:*

$$\Pr\left[\mathsf{Vrfy}(\mathsf{vk}, \pi) = \perp \,\middle|\, \substack{(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ (\mathsf{vk},\mathsf{ct}) \leftarrow \mathsf{Enc}(\mathsf{pk}, m) \\ \pi \leftarrow \mathsf{Del}(\mathsf{ct})}\right] \leq \mathrm{negl}(\lambda).$$

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

1. *The challenger generates a pair* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$*, and sends* pk *to* $\mathcal{A}$.
2. $\mathcal{A}$ *sends a plaintext pair* $(m_0, m_1) \in \mathcal{M} \times \mathcal{M}$ *to the challenger.*
3. *The challenger computes* $(\mathsf{vk}, \mathsf{ct}_b) \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$*, and sends* ct_b *to* $\mathcal{A}$.
4. *At some point in time,* $\mathcal{A}$ *sends the certificate* π *to the challenger.*

5. *The challenger computes* $\mathsf{Vrfy}(\mathsf{vk}, \pi)$ *and sends* sk *to* $\mathcal{A}$*, if the output is* $\top$*, and sends* $\perp$ *otherwise.*

6. $\mathcal{A}$ *outputs a guess* $b' \in \{0,1\}$*, which is also the output of the experiment.*

We say that the scheme Σ *is* IND-CPA-CD*-secure if, for any* QPT *adversary* $\mathcal{A}$*, it holds that*

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

As a complementary notion of certified deletion security, we also introduce a semi-honest variant in which we assume that the adversary honestly performs the correct deletion procedure when asked to prove erasure of the quantum ciphertext. However, after the experiment is over, the adversary may carefully analyze any additional data collected throughout the protocol.

Definition 29 (Semi-honest certified deletion security for PKE)**.** *Let* $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Del}, \mathsf{Vrfy})$ *be a* $\mathsf{PKE}_{\mathsf{CD}}$ *scheme and let* $\mathcal{A}$ *be a* QPT *adversary (in terms of the security parameter* $\lambda \in \mathbb{N}$*). The security experiment* $\mathsf{Exp}_{\Sigma,\mathcal{A},\lambda}^{\mathsf{pk\text{-}sh\text{-}cert\text{-}del}}(b)$ *between* $\mathcal{A}$ *and a challenger is defined as follows:*

1. *The challenger generates a pair* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$*, and sends* pk *to* $\mathcal{A}$*.*

2. $\mathcal{A}$ *sends a plaintext pair* $(m_0, m_1) \in \mathcal{M} \times \mathcal{M}$ *to the challenger.*

3. *The challenger computes* $(\mathsf{vk}, \mathsf{ct}_b) \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$*, and sends* ct_b *to* $\mathcal{A}$*.*

4. *At some point in time,* $\mathcal{A}$ *computes* $\pi \leftarrow \mathsf{Del}(\mathsf{ct}_b)$ *and sends the outcome* π *to the challenger.*

5. *The challenger computes* $\mathsf{Vrfy}(\mathsf{vk}, \pi)$ *and sends* sk *to* $\mathcal{A}$*, if the output is* $\top$*, and sends* $\perp$ *otherwise.*

6. $\mathcal{A}$ *outputs a guess* $b' \in \{0,1\}$*, which is also the output of the experiment.*

We say that the scheme Σ *is* IND-CPA-CD*-secure in the semi-honest adversarial model, if, for any* QPT *adversary* $\mathcal{A}$*, it holds that*

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

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. We borrow the presentation of the Dual-Regev scheme from the work of Mahadev [Mah18b].

7.1 Construction

Construction 1 (Dual-Regev PKE, [GPV07])**.** *Let* $\lambda \in \mathbb{N}$ *be the security parameter and let* n *and* $m \geq n$ *be integers, let* q *be a power of* 2 *integer modulus and let* $\alpha \in (0,1)$*. The Dual-Regev public-key encryption scheme given by* $\mathsf{DualPKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *consists of a triple of* PPT *algorithms defined as follows:*

$\mathsf{DualPKE.KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$: *Sample a random matrix* $\bar{\boldsymbol{A}} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$ *and let* $\boldsymbol{e}_{\mathsf{sk}} \xleftarrow{\$} \{0,1\}^m$*. The secret key is given by* $\mathsf{sk} = (-\boldsymbol{e}_{\mathsf{sk}}, 1) \in \mathbb{Z}_q^{m+1}$ *and the public key is given by* $\mathsf{pk} = \boldsymbol{A} \in \mathbb{Z}_q^{(m+1)\times n}$ *which is a matrix composed of* $\bar{\boldsymbol{A}}$ *(the first* m *rows) and* $\bar{\boldsymbol{A}}^T \cdot \boldsymbol{e}_{\mathsf{sk}} \pmod q$ *(the last row).*

$\mathsf{DualPKE.Enc}(\mathsf{pk}, x) \to \mathsf{ct}$: *to encrypt a bit* $x \in \{0,1\}$, *choose a random vector* $\boldsymbol{s} \xleftarrow{\$} \mathbb{Z}_q^n$, *sample* $\boldsymbol{e} \sim D_{\mathbb{Z}^{m+1},\alpha q}$, *and output* $\mathsf{ct} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e} + (0, \dots, 0, x \cdot \frac{q}{2}) \pmod q$.

$\mathsf{DualPKE.Dec}(\mathsf{sk}, \mathsf{ct}) \to \{0,1\}$: *to decrypt, compute* $c = \mathsf{sk}^T \cdot \mathsf{ct} \in \mathbb{Z}_q$ *and output* 0, *if* c *is closer to* 0 *than to* $\frac{q}{2} \pmod q$, *otherwise output* 1.

The following proof of (classical) IND-CPA security was shown by Gentry, Peikert and Vaikuntanathan [GPV07]. However, the proof for quantum adversaries is virtually identical under the LWE assumption.

Theorem 6 ([GPV07]). *Let* $n, m \in \mathbb{N}$ *and let* $q \geq 2$ *be a power of 2 with* $m = \Omega(n \log q)$. *Let* $\alpha q \geq 2\sqrt{n}$. *Then,* $\mathsf{DualPKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *in Construction 1 is* IND-CPA*-secure under the* LWE *assumption.*

As mentioned before, the Dual-Regev scheme due to Gentry, Peikert and Vaikuntanathan [GPV07] comes with a useful feature. Namely, 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 $\mathsf{LWE}_{n,q,\alpha q}^{m+1}$ distribution together with an additive shift $x \cdot \frac{q}{2}$ that depends on the plaintext $x \in \{0,1\}$. This property allows us to extend our privacy delegation protocol for LWE towards a fully-fledged PKE scheme with certified deletion. Using Gaussian coset states, we can encode Dual-Regev ciphertexts for the purpose of proving deletion while simultaneously preserving their cryptographic functionality.

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

- an integer modulus $q \geq 2$.
- an integer $m = \Omega(n \log q)$.
- noise ratios $\alpha, \beta \in (0,1)$ with $2\sqrt{n} \leq \alpha q < \beta q < q/\sqrt{2m+2}$ such that β/α is superpolynomial.
- a rounding parameter $p = \sqrt{m+1}/2\beta$ and arbitrary $\delta \in (0,1)$.

Construction 2 (Dual-Regev PKE with Certified Deletion). *Let* $\lambda \in \mathbb{N}$ *be the security parameter and let* $\mathsf{DualPKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be the scheme in Construction 1. The Dual-Regev public-key encryption scheme* $\mathsf{DualPKE}_{\mathsf{CD}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Del}, \mathsf{Vrfy})$ *with certified deletion is defined as follows:*

$\mathsf{DualPKE}_{\mathsf{CD}}.\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$: *Generate* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{DualPKE.KeyGen}(1^\lambda)$ *and output* $(\mathsf{pk}, \mathsf{sk})$.

$\mathsf{DualPKE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk}, x) \to (\mathsf{vk}, |\mathsf{ct}\rangle)$: *To encrypt a bit* $x \in \{0,1\}$, *generate a ciphertext* $|\mathsf{ct}\rangle$ *as follows:*

- *Parse the public key as* $\boldsymbol{A} \leftarrow \mathsf{pk}$, *where* $\boldsymbol{A} \in \mathbb{Z}_q^{(m+1)\times n}$.
- *Sample* $\boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}_0 + (0, \dots, 0, x \cdot q/2) \pmod q \leftarrow \mathsf{DualPKE.Enc}(\mathsf{pk}, x)$ *with* $\boldsymbol{e}_0 \sim D_{\mathbb{Z}^{m+1},\alpha q}$.
- *Sample a random vector* $\boldsymbol{v} \xleftarrow{\$} \mathbb{Z}_q^{m+1}$, *and let* $\mathsf{vk} \leftarrow \boldsymbol{v}$ *be the verification key.*
- *Generate the* $(m+1)$*-qudit quantum ciphertext given by*

$$|\mathsf{ct}\rangle = \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} \sqrt{D_{\mathbb{Z}_q^{m+1},\beta q}(\boldsymbol{e})}\, \omega_q^{-\langle \boldsymbol{e}, \boldsymbol{v}\rangle} \left| \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}_0 + \boldsymbol{e} + (0, \dots, 0, x \cdot q/2) \pmod q \right\rangle.$$

- *Output* $(\mathsf{vk}, |\mathsf{ct}\rangle)$, *where* vk *serves as the verification key and* $|\mathsf{ct}\rangle$ *is the quantum ciphertext.*

$\mathsf{DualPKE_{CD}.Dec}(\mathsf{sk}, |\mathsf{ct}\rangle) \to \{0,1\}$: *Measure the ciphertext* $|\mathsf{ct}\rangle$ *in the computational basis to obtain an outcome* $\boldsymbol{C} \in \mathbb{Z}_q^{m+1}$ *and output* $x' \leftarrow \mathsf{DualPKE.Dec}(\mathsf{sk}, \mathsf{ct}' = (\mathsf{pk}, \boldsymbol{C}))$.

$\mathsf{DualPKE_{CD}.Del}(|\mathsf{ct}\rangle) \to \pi$: *Measure each qudit of the ciphertext* $|\mathsf{ct}\rangle$ *in the* q*-ary Fourier basis, and output the measurement outcome denoted by* $\pi \in \mathbb{Z}_q^{m+1}$.

$\mathsf{DualPKE_{CD}.Vrfy}(\mathsf{vk}, \pi) \to \{0,1\}$: *To verify a certificate* π*, do the following:*

- *Parse* $\boldsymbol{v} \leftarrow \mathsf{vk}$ *as the verification key.*
- *Output* $F^{\mathsf{corr}}(\boldsymbol{v}, \pi) \in \{0,1\}$ *(see Definition 25) with parameters* $0 \leq p < q$ *and* $\delta \in (0,1)$.

Proof of correctness. Let us now establish the correctness properties of $\mathsf{DualPKE_{CD}}$ in Construction 2.

Lemma 17 (Correctness of decryption)**.** *Let* $n \in \mathbb{N}$*, let* $q \geq 2$ *be a modulus and let* $m = \Omega(n \log q)$*, each parameterized by* $\lambda \in \mathbb{N}$*. Let* $\alpha, \beta \in (0,1)$ *be noise ratios with* $2\sqrt{n} \leq \alpha q < \beta q < q/\sqrt{2m+2}$ *such that* β/α *is superpolynomial. Let* $p = \sqrt{m+1}/2\beta$ *and* $\delta \in (0,1)$ *be rounding parameters. Then, the scheme* $\mathsf{DualPKE_{CD}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Del}, \mathsf{Vrfy})$ *in Construction 2 satisfies the following for any* $x \in \{0,1\}$*:*

$$\Pr\left[\mathsf{DualPKE_{CD}.Dec}(\mathsf{sk}, |\mathsf{ct}\rangle) = x \,\middle|\, \begin{array}{c} (\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{DualPKE_{CD}.KeyGen}(1^\lambda) \\ (\mathsf{vk},|\mathsf{ct}\rangle) \leftarrow \mathsf{DualPKE_{CD}.Enc}(\mathsf{pk},x) \end{array}\right] \geq 1 - \mathrm{negl}(\lambda).$$

Proof. This follows immediately from the decryption correctness of the classical Dual-Regev scheme in Construction 1 and our choice of parameter $\beta \in (0,1)$ with $\beta q < q/\sqrt{2m+2}$, as in [Mah18b,GPV07]. □

Let us now prove the following property.

Lemma 18 (Correctness of verification)**.** *Let* $n \in \mathbb{N}$*, let* $q \geq 2$ *be a modulus and let* $m = \Omega(n \log q)$*, each parameterized by* $\lambda \in \mathbb{N}$*. Let* $\alpha, \beta \in (0,1)$ *be noise ratios with* $2\sqrt{n} \leq \alpha q < \beta q < q/\sqrt{2m+2}$ *such that* β/α *is superpolynomial. Let* $p = \sqrt{m+1}/2\beta$ *and* $\delta \in (0,1)$ *be parameters. Then, the scheme* $\mathsf{DualPKE_{CD}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Del}, \mathsf{Vrfy})$ *in Construction 2 satisfies the following for any* $x \in \{0,1\}$*:*

$$\Pr\left[\mathsf{DualPKE_{CD}.Verify}(\mathsf{vk}, \pi) = 1 \,\middle|\, \begin{array}{c} (\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{DualPKE_{CD}.KeyGen}(1^\lambda) \\ (\mathsf{vk},|\mathsf{ct}\rangle) \leftarrow \mathsf{DualPKE_{CD}.Enc}(\mathsf{pk},x) \\ \pi \leftarrow \mathsf{DualPKE_{CD}.Del}(|\mathsf{ct}\rangle) \end{array}\right] \geq 1 - \mathrm{negl}(\lambda).$$

Proof. Let $x \in \{0,1\}$ be an arbitrary plaintext bit and let $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{DualPKE_{CD}.KeyGen}(1^\lambda)$ denote the outcome of the key generation procedure. Recall that $\mathsf{DualPKE_{CD}.Enc}(\mathsf{pk}, x)$ outputs a pair $(\mathsf{vk}, |\mathsf{ct}\rangle)$, where $\mathsf{vk} = \boldsymbol{v} \in \mathbb{Z}_q^{m+1}$ and the ciphertext $|\mathsf{ct}\rangle$ corresponds to the Gaussian coset given by

$$|\mathsf{ct}\rangle = \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} \sqrt{D_{\mathbb{Z}_q^{m+1}, \beta q}(\boldsymbol{e})}\, \omega_q^{-\langle \boldsymbol{e}, \boldsymbol{v}\rangle} \left|\boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}_0 + \boldsymbol{e} + (0, \dots, 0, x \cdot q/2) \pmod q\right\rangle. \tag{49}$$

Recall that the deletion procedure measures each qudit of $|\mathsf{ct}\rangle$ in the q-ary Fourier basis. By Lemma 11 and that $2\sqrt{n} \leq \alpha q < \beta q < q/\sqrt{2m+2}$, we get that the Fourier transform of the Gaussian coset $|\mathsf{ct}\rangle$ in Eq. (49) results in a state within trace distance $\varepsilon = 2^{-\Omega(\lambda)}$ of the dual Gaussian coset, i.e.

$$\mathsf{FT}_q\, |\mathsf{ct}\rangle \;\approx_\varepsilon \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} \sqrt{D_{\mathbb{Z}_q^{m+1}, 1/2\beta}(\boldsymbol{e})}\, \omega_q^{\langle \boldsymbol{e}, \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}_0 + (0,\dots,0,x \cdot q/2)\rangle} \left|\boldsymbol{v} + \boldsymbol{e} \pmod q\right\rangle. \tag{50}$$

Hence, a measurement in the q-ary Fourier basis results in a classical state $\widetilde{\varrho}_P$ in a system P which is within distance $\|\widetilde{\varrho} - \varrho\|_{\mathrm{tr}} \leq 2^{-\Omega(\lambda)}$ of the classical Gaussian mixture ϱ_P centered around $\boldsymbol{v} \in \mathbb{Z}_q^{m+1}$, where

$$\varrho_P = \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} D_{\mathbb{Z}_q^m, 1/2\beta}(\boldsymbol{e}) |\boldsymbol{v} + \boldsymbol{e} \pmod q\rangle\langle \boldsymbol{v} + \boldsymbol{e} \pmod q|_P. \tag{51}$$

Recall that the q-ary correlation flag $F^{\mathsf{corr}} : \mathbb{Z}_q^{m+1} \times \mathbb{Z}_q^{m+1} \to \{0,1\}$ in Definition 25 is defined as

$$F^{\mathsf{corr}}(\boldsymbol{x}, \boldsymbol{y}) := \begin{cases} 1 & \text{if } \omega(\lfloor \boldsymbol{x} - \boldsymbol{y} \rceil_p) < (m+1)\delta \\ 0 & \text{otherwise.} \end{cases} \tag{52}$$

Let $\widetilde{\varrho}_{VP}$ and ϱ_{VP} be the associated states that include the verification key $|\boldsymbol{v}\rangle\langle\boldsymbol{v}|_V$ in a system V. We can model the verification with F^{corr} as applying a projector Π_{VP}^{corr} on the correlated subset of systems VP, for

$$\Pi_{VP}^{\mathsf{corr}} = \sum_{\substack{\boldsymbol{x},\boldsymbol{y} \in \mathbb{Z}_q^{m+1} \text{ s.t.} \\ F^{\mathsf{corr}}(\boldsymbol{x},\boldsymbol{y})=1}} |x\rangle\langle x|_V \otimes |y\rangle\langle y|_P.$$

Thus, by definition, we have that the probability of successful verification is given by

$$\mathrm{Tr}[\Pi_{VP}^{\mathsf{corr}} \widetilde{\varrho}_{VP}] = \Pr\left[\mathsf{DualPKE_{CD}.Verify}(\mathsf{vk}, \pi) = 1 \;\middle|\; \begin{array}{c} (\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{DualPKE_{CD}.KeyGen}(1^\lambda) \\ (\mathsf{vk}, |\mathsf{ct}\rangle) \leftarrow \mathsf{DualPKE_{CD}.Enc}(\mathsf{pk}, x) \\ \pi \leftarrow \mathsf{DualPKE_{CD}.Del}(|\mathsf{ct}\rangle) \end{array}\right].$$

Because the truncated discrete Gaussian $D_{\mathbb{Z}_q^{m+1}, 1/2\beta}$ is supported on $\{\boldsymbol{x} \in \mathbb{Z}_q^{m+1} : \|\boldsymbol{x}\|_\infty \leq \sqrt{m+1}/2\beta\}$ and $p = \sqrt{m+1}/2\beta$, it follows that $\mathrm{Tr}[\Pi_{VP}^{\mathsf{corr}} \varrho_{VP}] = 1$ for the classical Gaussian mixture ϱ_P centered around $\boldsymbol{v} \in \mathbb{Z}_q^{m+1}$. Therefore, using Lemma 6 and the fact that $\|\widetilde{\varrho} - \varrho\|_{\mathrm{tr}} \leq 2^{-\Omega(\lambda)}$, we have

$$\mathrm{Tr}[\Pi_{VP}^{\mathsf{corr}} \widetilde{\varrho}_{VP}] \geq 1 - 2^{-\Omega(\lambda)} = 1 - \mathrm{negl}(\lambda).$$

This proves the claim that $\mathsf{DualPKE_{CD}}$ satisfies correctness of verification. □

7.2 Proof of security

Let us now analyze the security of our Dual-Regev PKE scheme with certified deletion in Construction 2.

$\mathsf{IND\text{-}CPA}$ security of $\mathsf{DualPKE_{CD}}$. We first prove that our public-key encryption scheme $\mathsf{DualPKE_{CD}}$ in Construction 2 satisfies the notion $\mathsf{IND\text{-}CPA}$ security according to Definition 13. The proof follows immediately from the (decisional) LWE assumption (Definition 15). We add it for completeness.

Theorem 7. *Let $n \in \mathbb{N}$, let $q \geq 2$ be a modulus and let $m = \Omega(n \log q)$, each parameterized by $\lambda \in \mathbb{N}$. Let $\alpha, \beta \in (0,1)$ be noise ratios with $2\sqrt{n} \leq \alpha q < \beta q < q/\sqrt{m+1}$ such that β/α is superpolynomial. Then, the scheme $\mathsf{DualPKE_{CD}}$ in Construction 2 is $\mathsf{IND\text{-}CPA}$-secure under the $\mathsf{LWE}_{n,q,\alpha q}^{m+1}$ assumption.*

Proof. Let $\Sigma = \mathsf{DualPKE_{CD}}$. We need to show that, for any QPT adversary $\mathcal{A}$, it holds that

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

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

1. The challenger generates a pair $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{DualPKE}_{\mathsf{CD}}.\mathsf{KeyGen}(1^\lambda)$, and sends pk to $\mathcal{A}$.
2. $\mathcal{A}$ sends a distinct plaintext pair $(m_0, m_1) \in \{0,1\} \times \{0,1\}$ to the challenger.
3. The challenger computes $(\mathsf{vk}, \mathsf{ct}_b) \leftarrow \mathsf{DualPKE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk}, m_b)$, and sends $|\mathsf{ct}_b\rangle$ to $\mathcal{A}$.
4. $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$, which is also the output of the experiment.

Recall that the procedure $\mathsf{DualPKE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk}, m_b)$ outputs a pair $(\mathsf{vk}, |\mathsf{ct}_b\rangle)$, where $\mathsf{vk} = \boldsymbol{v} \in \mathbb{Z}_q^{m+1}$ is the verification key and where the quantum ciphertext $|\mathsf{ct}_b\rangle$ corresponds to the Gaussian coset given by

$$|\mathsf{ct}_b\rangle = \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} \sqrt{D_{\mathbb{Z}_q^{m+1},\beta q}(\boldsymbol{e})}\, \omega_q^{-\langle \boldsymbol{e}, \boldsymbol{v}\rangle} \, |\boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}_0 + \boldsymbol{e} + (0, \dots, 0, m_b \cdot q/2) \pmod q\rangle . \tag{53}$$

Under the (decisional) $\mathsf{LWE}_{n,q,\alpha q}^{m+1}$ assumption in Definition 15, we have that $|\mathsf{ct}_b\rangle$ is computationally indistinguishable from a random Gaussian coset $|\mathcal{D}_{\beta q}^{\boldsymbol{u},\boldsymbol{v}}\rangle$ with $\boldsymbol{u} \xleftarrow{\$} \mathbb{Z}_q^{m+1}$, where

$$|\mathcal{D}_{\beta q}^{\boldsymbol{u},\boldsymbol{v}}\rangle = \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} \sqrt{D_{\mathbb{Z}_q^{m+1},\beta q}(\boldsymbol{e})}\, \omega_q^{-\langle \boldsymbol{e}, \boldsymbol{v}\rangle} \, |\boldsymbol{u} + \boldsymbol{e} \pmod q\rangle .$$

Because the random Gaussian coset $|\mathcal{D}_{\beta q}^{\boldsymbol{u},\boldsymbol{v}}\rangle$ is completely indistinguishable from $b \in \{0,1\}$, it follows that

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

This proves the claim. □

$\mathsf{IND\text{-}CPA\text{-}CD}$ **security of** $\mathsf{DualPKE}_{\mathsf{CD}}$**.** In this section, we prove that our public-key encryption scheme $\mathsf{DualPKE}_{\mathsf{CD}}$ in Construction 2 satisfies the notion of *certified deletion security* in the semi-honest adversarial model (as in Definition 28). In other words, we analyze the security of our encryption scheme in the setting in which the adversary honestly follows the execution of the protocol, but may later maliciously analyze the data collected along the way. We remark that our scheme in Construction 2 achieves a form of *everlasting security* [MQU07, HMNY21a] in the semi-honest model. Here, we assume that the adversary honestly follows the execution of the protocol, but is later assumed to be unbounded once the protocol is over.

Theorem 8. *Let $n \in \mathbb{N}$, let $q \geq 2$ be a modulus and let $m = \Omega(n \log q)$, each parameterized by $\lambda \in \mathbb{N}$. Let $\alpha, \beta \in (0,1)$ be noise ratios with $2\sqrt{n} \leq \alpha q < \beta q < q/\sqrt{2m+2}$ such that β/α is superpolynomial. Let $p = \sqrt{m+1}/2\beta$ and $\delta \in (0,1)$ be rounding parameters. Then, the scheme $\mathsf{DualPKE}_{\mathsf{CD}}$ in Construction 2 is $\mathsf{IND\text{-}CPA\text{-}CD}$-secure in the semi-honest aversarial model according to Definition 28.*

Proof. Let $\Sigma = \mathsf{DualPKE}_{\mathsf{CD}}$. We need to show that, for any QPT adversary $\mathcal{A}$, it holds that

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

We will prove this statement in the honest-but-curious adversarial model. Hence, we assume that $\mathcal{A}$ behaves honestly during the execution of the protocol, but after the experiment is over, $\mathcal{A}$ may carefully analyze the data collected during the protocol. Let $\lambda \in \mathbb{N}$ be the security parameter and let $b \in \{0,1\}$. Consider the experiment $\mathsf{Exp}_{\Sigma,\mathcal{A},\lambda}^{\mathsf{pk\text{-}sh\text{-}cert\text{-}del}}(b)$ between the adversary $\mathcal{A}$ and a challenger which takes place as follows:

1. The challenger generates a pair $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{DualPKE}_{\mathsf{CD}}.\mathsf{KeyGen}(1^\lambda)$, and sends pk to $\mathcal{A}$.

2. $\mathcal{A}$ sends a distinct plaintext pair $(m_0, m_1) \in \{0,1\} \times \{0,1\}$ to the challenger.

3. The challenger computes $(\mathsf{vk}, \mathsf{ct}_b) \leftarrow \mathsf{DualPKE_{CD}.Enc}(\mathsf{pk}, m_b)$, and sends $|\mathsf{ct}_b\rangle$ to $\mathcal{A}$.

4. At some point in time, $\mathcal{A}$ computes $\pi \leftarrow \mathsf{DualPKE_{CD}.Del}(|\mathsf{ct}_b\rangle)$ and sends π to the challenger.

5. The challenger computes $\mathsf{DualPKE_{CD}.Vrfy}(\mathsf{vk}, \pi)$ and sends secret key sk to $\mathcal{A}$, if the output is 1, and sends 0 otherwise.

6. $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$, which is also the output of the experiment.

Let us now proceed by analyzing the ciphertext that is being deleted using the honest procedure $\mathsf{DualPKE_{CD}.Del}$ in more detail. Recall that $\mathsf{DualPKE_{CD}.Enc}(\mathsf{pk}, m_b)$ outputs a pair $(\mathsf{vk}, |\mathsf{ct}_b\rangle)$, where $\mathsf{vk} = \boldsymbol{v} \in \mathbb{Z}_q^{m+1}$ and the ciphertext $|\mathsf{ct}_b\rangle$ corresponds to the Gaussian coset given by

$$|\mathsf{ct}_b\rangle = \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} \sqrt{D_{\mathbb{Z}_q^{m+1}, \beta q}(\boldsymbol{e})}\, \omega_q^{-\langle \boldsymbol{e}, \boldsymbol{v}\rangle} \, |\boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}_0 + \boldsymbol{e} + (0, \dots, 0, m_b \cdot q/2) \pmod q\rangle . \tag{54}$$

Recall that the deletion procedure measures each qudit of $|\mathsf{ct}_b\rangle$ in the q-ary Fourier basis. By the Switching Lemma (Lemma 11) and that $\beta q < q/\sqrt{2m+2}$, we get that the Fourier transform of the Gaussian coset $|\mathsf{ct}_b\rangle$ in Eq. (54) results in a state within trace distance $\varepsilon = 2^{-\Omega(\lambda)}$ of the dual Gaussian coset, i.e.

$$\mathsf{FT}_q \; |\mathsf{ct}_b\rangle \;\; \approx_\varepsilon \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} \sqrt{D_{\mathbb{Z}_q^{m+1}, 1/2\beta}(\boldsymbol{e})}\, \omega_q^{\langle \boldsymbol{e}, \boldsymbol{A}\cdot \boldsymbol{s} + \boldsymbol{e}_0 + (0,\dots,0,m_b \cdot q/2)\rangle} \, |\boldsymbol{v} + \boldsymbol{e} \pmod q\rangle . \tag{55}$$

Hence, a measurement in the q-ary Fourier basis results in a classical state $\widetilde{\varrho}$ which is within distance $\|\widetilde{\varrho} - \varrho\|_{\mathrm{tr}} \leq 2^{-\Omega(\lambda)}$ of the classical Gaussian mixture ϱ centered around $\boldsymbol{v} \in \mathbb{Z}_q^{m+1}$, where

$$\varrho = \sum_{\boldsymbol{e} \in \mathbb{Z}_q^{m+1}} D_{\mathbb{Z}_q^m, 1/2\beta}(\boldsymbol{e}) |\boldsymbol{v} + \boldsymbol{e} \pmod q\rangle\langle \boldsymbol{v} + \boldsymbol{e} \pmod q| . \tag{56}$$

Because $\|\widetilde{\varrho} - \varrho\|_{\mathrm{tr}} \leq 2^{-\Omega(\lambda)}$, it follows that the post-measurement state $\widetilde{\varrho}$ is statistically close to a state ϱ which is completely independent of the Dual-Regev ciphertext encoding the plaintext $m_b \in \{0,1\}$. In other words, once deletion has taken place, the advantage of the adversary at distinguishing $b \in \{0,1\}$ is at most

$$\mathsf{Adv}_{\Sigma,\mathcal{A}}^{\mathsf{pk\text{-}sh\text{-}cert\text{-}del}}(\lambda) = |\Pr[\mathsf{Exp}_{\Sigma,\mathcal{A},\lambda}^{\mathsf{pk\text{-}sh\text{-}cert\text{-}del}}(0) = 1] - \Pr[\mathsf{Exp}_{\Sigma,\mathcal{A},\lambda}^{\mathsf{pk\text{-}sh\text{-}cert\text{-}del}}(1) = 1]| \leq 2^{-\Omega(\lambda)},$$

according to Lemma 6. This proves the claim. □

Next, we show how to extend our Dual-Regev PKE scheme with certified deletion in Construction 2 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 30 (Homomorphic encryption with certified deletion)**.** *A homomorphic encryption scheme with certified deletion is a tuple* $\mathsf{HE}_{\mathsf{CD}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Del}, \mathsf{Vrfy})$ *of* QPT *algorithms (in the security parameter* $\lambda \in \mathbb{N}$*), a key generation algorithm* KeyGen*, an encryption algorithm* Enc*, a decryption algorithm* Dec*, an evaluation algorithm* Eval*, a deletion algorithm* Del*, and a verification algorithm* Vrfy*.*

$\mathsf{HE}_{\mathsf{CD}}.\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$: *takes as input* 1^λ *and outputs a public key* pk *and secret key* sk*.*

$\mathsf{HE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk}, x) \to (\mathsf{vk}, \mathsf{ct})$: *takes as input the public key* pk *and a plaintext* $x \in \{0,1\}$*, and outputs a classical verification key* vk *together with a quantum ciphertext* ct*.*

$\mathsf{HE}_{\mathsf{CD}}.\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to x'$ **or** $\bot$: *takes as input a key* sk *and ciphertext* ct*, and outputs* $x' \in \{0,1\}$ *or* $\bot$*.*

$\mathsf{HE}_{\mathsf{CD}}.\mathsf{Eval}(C, \mathsf{ct}, \mathsf{pk}) \to \widetilde{\mathsf{ct}}$*: takes as input a key* pk *and applies a circuit* $C : \{0,1\}^\ell \to \{0,1\}$ *to a product of quantum ciphertexts* $\mathsf{ct} = \mathsf{ct}_1 \otimes \cdots \otimes \mathsf{ct}_\ell$ *resulting in a state* $\widetilde{\mathsf{ct}}$*.*

$\mathsf{HE}_{\mathsf{CD}}.\mathsf{Del}(\mathsf{ct}) \to \pi$: *takes as input a ciphertext* ct *and outputs a classical certificate* π*.*

$\mathsf{HE}_{\mathsf{CD}}.\mathsf{Vrfy}(\mathsf{vk}, \pi) \to \top$ **or** $\bot$: *takes as input a key* vk *and certificate* π*, and outputs* $\top$ *or* $\bot$*.*

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 31 (Compactness and full homomorphism)**.** *A homomorphic encryption scheme with certified deletion* $\mathsf{HE}_{\mathsf{CD}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Del}, \mathsf{Vrfy})$ *is fully homomorphic if, for any efficienty (in* $\lambda \in \mathbb{N}$*) computable circuit* $C : \{0,1\}^\ell \to \{0,1\}$ *and any set of inputs* $x = (x_1, \dots, x_\ell) \in \{0,1\}^\ell$*, it holds that*

$$\Pr\left[\mathsf{HE}_{\mathsf{CD}}.\mathsf{Dec}(\mathsf{sk}, \widetilde{\mathsf{ct}}) \neq C(x_1, \dots, x_\ell) \;\middle|\; \begin{array}{c} (\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{HE}_{\mathsf{CD}}.\mathsf{KeyGen}(1^\lambda) \\ (\mathsf{vk},\mathsf{ct}) \leftarrow \mathsf{HE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk},x) \\ \widetilde{\mathsf{ct}} \leftarrow \mathsf{HE}_{\mathsf{CD}}.\mathsf{Eval}(C,\mathsf{ct},\mathsf{pk}) \end{array}\right] \leq \operatorname{negl}(\lambda).$$

We say that a fully homomorphic encryption scheme with certified deletion $(\mathsf{FHE}_{\mathsf{CD}})$ *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 32 (Correctness of verification)**.** *A homomorphic encryption scheme with certified deletion* $\mathsf{HE}_{\mathsf{CD}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Del}, \mathsf{Vrfy})$ *has correctness of verification if the following property holds for any integer* $\lambda \in \mathbb{N}$ *and any set of inputs* $x = (x_1, \dots, x_\ell) \in \{0,1\}^\ell$

$$\Pr\left[\mathsf{HE}_{\mathsf{CD}}.\mathsf{Vrfy}(\mathsf{vk}, \pi) = \bot \;\middle|\; \begin{array}{c} (\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{HE}_{\mathsf{CD}}.\mathsf{KeyGen}(1^\lambda) \\ (\mathsf{vk},\mathsf{ct}) \leftarrow \mathsf{HE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk},x) \\ \pi \leftarrow \mathsf{HE}_{\mathsf{CD}}.\mathsf{Del}(\mathsf{ct}) \end{array}\right] \leq \operatorname{negl}(\lambda).$$

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 irreversibly affecting the ability of the server to later prove deletion. We use the following definition.

Definition 33 (Extractable FHE scheme with certified deletion)**.** *A fully homomorphic encryption scheme with certified deletion* $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Extract}, \mathsf{Del}, \mathsf{Vrfy})$ *is called extractable, if*

- $\Sigma.\mathsf{Eval}(C, \mathsf{ct}_1, \ldots, \mathsf{ct}_\ell, \mathsf{pk})$ *additionally outputs a circuit transcript* t_C *besides* $\widetilde{\mathsf{ct}}$*;*
- $\Sigma.\mathsf{Extract}\langle \mathcal{S}(\varrho, t_C), \mathcal{R}(\mathsf{sk})\rangle$ *is an interactive protocol between a sender* $\mathcal{S}$ *(which takes as input a state* ϱ *and a circuit transcript* t_C*) and a receiver* $\mathcal{R}$ *(which takes as input a key* sk*) with the property that, once the protocol is complete,* $\mathcal{S}$ *obtains a state* $\widetilde{\varrho}$ *and* $\mathcal{R}$ *obtains a bit* $y \in \{0,1\}$*;*

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

$$\Pr\left[y \neq \mathsf{C}(x_1, \ldots, x_\ell) \;\middle|\; \begin{array}{c} (\mathsf{pk},\mathsf{sk}) \leftarrow \Sigma.\mathsf{KeyGen}(1^\lambda, 1^L) \\ (\mathsf{vk},\mathsf{ct}) \leftarrow \Sigma.\mathsf{Enc}(\mathsf{pk}, x) \\ (\widetilde{\mathsf{ct}}, t_C) \leftarrow \Sigma.\mathsf{Eval}(C, \mathsf{ct}, \mathsf{pk}) \\ (\widetilde{\varrho}, y) \leftarrow \Sigma.\mathsf{Extract}\langle \mathcal{S}(\widetilde{\mathsf{ct}}, t_C), \mathcal{R}(\mathsf{sk})\rangle \end{array} \right] \leq \mathrm{negl}(\lambda), \quad \textit{and}$$

$$\Pr\left[\Sigma.\mathsf{Vrfy}(\mathsf{vk}, \pi) = \bot \;\middle|\; \begin{array}{c} (\mathsf{pk},\mathsf{sk}) \leftarrow \Sigma.\mathsf{KeyGen}(1^\lambda, 1^L) \\ (\mathsf{vk},\mathsf{ct}) \leftarrow \Sigma.\mathsf{Enc}(\mathsf{pk}, x) \\ (\widetilde{\mathsf{ct}}, t_C) \leftarrow \Sigma.\mathsf{Eval}(C, \mathsf{ct}, \mathsf{pk}) \\ (\widetilde{\varrho}, y) \leftarrow \Sigma.\mathsf{Extract}\langle \mathcal{S}(\widetilde{\mathsf{ct}}, t_C), \mathcal{R}(\mathsf{sk})\rangle \\ \pi \leftarrow \Sigma.\mathsf{Del}(\widetilde{\varrho}) \end{array} \right] \leq \mathrm{negl}(\lambda).$$

8.2 Certified deletion security

Our notion of certified deletion security for homomorphic encryption (HE) schemes is similar to the notion of $\mathsf{IND\text{-}CPA\text{-}CD}$ security for public-key encryption schemes in Definition 28.

Definition 34 (Certified deletion security for HE)**.** *Let* $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Del}, \mathsf{Vrfy})$ *be a homomorphic encryption scheme with certified deletion and let* $\mathcal{A}$ *be a* QPT *adversary. We define the security experiment* $\mathsf{Exp}^{\mathsf{he\text{-}cert\text{-}del}}_{\Sigma,\mathcal{A},\lambda}(b)$ *between* $\mathcal{A}$ *and a challenger as follows:*

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

We say that the scheme Σ *is* $\mathsf{IND\text{-}CPA\text{-}CD}$*-secure if, for any* QPT *adversary* $\mathcal{A}$*, that*

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

As a complementary notion of certified deletion security, we also introduce a semi-honest variant in which we assume that the adversary honestly performs the correct deletion procedure when asked to prove erasure of the quantum ciphertext. However, after the experiment is over, the adversary may carefully analyze any additional data collected throughout the protocol. The definition is similar to Definition 29.

Definition 35 (Semi-honest certified deletion security for HE)**.** *Consider a homomorphic encryption scheme with certified deletion* $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Del}, \mathsf{Vrfy})$ *and let* $\mathcal{A}$ *be a* QPT *adversary. We define the security experiment* $\mathsf{Exp}^{\mathsf{he\text{-}sh\text{-}cert\text{-}del}}_{\Sigma,\mathcal{A},\lambda}(b)$ *between* $\mathcal{A}$ *and a challenger as follows:*

1. *The challenger generates a pair* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \Sigma.\mathsf{KeyGen}(1^\lambda)$*, and sends* pk *to* $\mathcal{A}$*.*

2. *$\mathcal{A}$ sends a distinct plaintext pair $(m_0, m_1) \in \{0,1\}^\ell \times \{0,1\}^\ell$ to the challenger.*

3. *The challenger computes $(\mathsf{vk}, \mathsf{ct}_b) \leftarrow \Sigma.\mathsf{Enc}(\mathsf{pk}, m_b)$, and sends $|\mathsf{ct}_b\rangle$ to $\mathcal{A}$.*

4. *$\mathcal{A}$ applies a Boolean circuit C by computing $(|\widetilde{\mathsf{ct}}\rangle, t_C) \leftarrow \Sigma.\mathsf{Eval}(C, |\mathsf{ct}\rangle)$.*

5. *At some point in time, $\mathcal{A}$ computes $\pi \leftarrow \Sigma.\mathsf{Del}(\mathsf{ct})$ and sends π to the challenger.*

6. *The challenger runs the verification procedure $\Sigma.\mathsf{Vrfy}(\mathsf{vk}, \pi)$ and sends secret key sk to $\mathcal{A}$, if the output is 1, and sends 0 otherwise.*

7. *$\mathcal{A}$ outputs a guess $b' \in \{0,1\}$, which is also the output of the experiment.*

We say that Σ is $\mathsf{IND\text{-}CPA\text{-}CD}$-secure in the semi-honest model if, for any QPT adversary $\mathcal{A}$, it holds that

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

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 1) – 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

$$\mathsf{NAND}(a,b) = \overline{a \wedge b} = 1 - a \cdot b.$$

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` $(\wedge)$ gate, an `OR` $(\vee)$ gate, or a `NOT` $(\neg)$ gate. We can naturally identify a Boolean circuit with a function $f : \{0,1\}^n \to \{0,1\}$ 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 2, we give an example of a Boolean circuit composed of three NAND gates that takes as input a string $x \in \{0,1\}^4$.

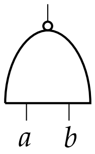

Figure 1: NAND gate.

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 *flattening* operation first introduced by Gentry, Sahai and Waters [GSW13] in the context of homomorphic encryption and is also featured in the Dual-Regev FHE

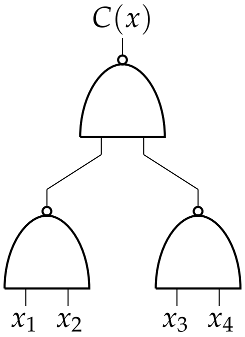

Figure 2: A Boolean circuit C made up of three NAND gates which takes as input a binary string of the form $x \in \{0,1\}^4$. The top-most NAND gate is the designated output node with outcome $C(x) \in \{0,1\}$.

scheme of Mahadev [Mah18b]. Let $q \geq 2$ be a power of two modulus, and let $n \in \mathbb{N}$ be an integer. We define a linear operator $\boldsymbol{G} \in \mathbb{Z}_q^{(n+1)\times N}$ called the *gadget matrix*, where $N = (n+1)\log(q)$. The operator $\boldsymbol{G}$ 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 $\boldsymbol{a} = (a_{1,0}, \ldots, a_{1,l-1}, \ldots, a_{m+1,0}, \ldots, a_{m+1,l-1})$ of length N, where $l = \log(q)$, the matrix $\boldsymbol{G}$ produces a vector in $\mathbb{Z}_q^{m+1}$ as follows:

$$\boldsymbol{G}(\boldsymbol{a}) = \left(\sum_{j=0}^{\log(q)-1} 2^j \cdot a_{1,j} \;, \ldots, \sum_{j=0}^{\log(q)-1} 2^j \cdot a_{m+1,j} \right). \tag{57}$$

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

Our (leveled) FHE scheme with certified deletion is based on the (leveled) Dual-Regev FHE scheme introduced by Mahadev [Mah18b] 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 3 (Dual-Regev leveled FHE, [Mah18a])**.** *Let $\lambda \in \mathbb{N}$ and let* DualPKE = (KeyGen, Enc, Dec) *be the Dual-Regev* PKE *scheme in Construction 1. The Dual-Regev leveled fully homomorphic encryption scheme* DualFHE = (KeyGen, Enc, Dec, Eval, Convert) *consists of the following* PPT *algorithms:*

DualFHE.KeyGen(1^λ) : *generate* (pk, sk) ← DualPKE.KeyGen(1^λ) *and output* (pk, sk).

DualFHE.Enc(pk, x) : *to encrypt a plaintext $x = (x_1, \ldots, x_\ell) \in \{0,1\}^\ell$, generate a ciphertext* ct *as follows. Fix $N = (m+1)\log(q)$ and parse $\boldsymbol{A} \leftarrow$* pk*, where $\boldsymbol{A} \in \mathbb{Z}_q^{(m+1)\times n}$. For $i \in [\ell]$, sample matrices $\boldsymbol{S}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times N}$ and $\boldsymbol{E}_i \sim D_{\mathbb{Z}^{(m+1)\times N}, \alpha q}$ and generate $\mathsf{ct}_i = \boldsymbol{A} \cdot \boldsymbol{S}_i + \boldsymbol{E}_i + x_i \boldsymbol{G} \pmod q \in \mathbb{Z}_q^{(m+1)\times N}$, where $\boldsymbol{G}$ is the gadget matrix in Eq. (57). Output the ciphertext $\mathsf{ct} = (\mathsf{ct}_1, \ldots, \mathsf{ct}_\ell)$.*

DualFHE.Eval(C, ct) : *apply the circuit C composed of* NAND *gates on the ciphertext* ct *as follows:*

- *parse the ciphertext tuple* $(\mathsf{ct}_1, \ldots, \mathsf{ct}_\ell) \leftarrow \mathsf{ct}$.

- *repeat for every* NAND *gate in* C*: to apply a* NAND *gate on a ciphertext pair* $(\mathsf{ct}_i, \mathsf{ct}_j)$*, parse matrices* $\boldsymbol{C}_i \leftarrow \mathsf{ct}_i$ *and* $\boldsymbol{C}_j \leftarrow \mathsf{ct}_j$ *with* $\boldsymbol{C}_i, \boldsymbol{C}_j \in \mathbb{Z}_q^{(m+1)\times N}$ *and generate* $\boldsymbol{C}_{ij} = \boldsymbol{G} - \boldsymbol{C}_i \cdot \boldsymbol{G}^{-1}(\boldsymbol{C}_j) \pmod q$*. Let* $\mathsf{ct}_{ij} \leftarrow \boldsymbol{C}_{ij}$ *denote the outcome ciphertext.*

$\mathsf{DualFHE.Convert}(\boldsymbol{M})$*: on input* $\boldsymbol{M} \in \mathbb{Z}_q^{(m+1)\times N}$*, output the* N*-th column of the matrix* $\boldsymbol{M}$*.*

$\mathsf{DualFHE.Dec}(\mathsf{sk}, \mathsf{ct})$ *: parse* $(\mathsf{ct}_1, \dots, \mathsf{ct}_\mu) \leftarrow \mathsf{ct}$ *with* $\mathsf{ct}_i \in \mathbb{Z}^{(m+1)\times N}$ *and, for every* $i \in [\mu]$*, generate* $x_i' = \mathsf{DualPKE.Dec}(\mathsf{sk}, \mathsf{DualFHE.Convert}(\mathsf{ct}_i))$ *and output a plaintext* $x' = (x_1', \dots, x_\mu') \in \{0,1\}^\mu$*.*

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 $\mathsf{ct} = \boldsymbol{G} - \mathsf{ct}_0 \cdot \boldsymbol{G}^{-1}(\mathsf{ct}_1) \pmod q$ is an encryption of $\mathsf{NAND}(x_0, x_1) = 1 - x_0 \cdot x_1$, where $\boldsymbol{G}$ 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 still allows for the decryption of the ciphertext ct once a NAND gate has been applied. The following result is due to Mahadev [Mah18b, Theorem 5.1].

Theorem 9 ([Mah18b]). *Let* $\lambda \in \mathbb{N}$ *be the security parameter. Let* $n \in \mathbb{N}$*,* $m = \Omega(n \log q)$ *and let* $q \geq 2$ *be a power of* 2 *integer modulus. Let* $N = (m+1)\log q$ *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 the noise ratio such that* $1/(\alpha\sqrt{m+1})$ *is sub-exponential in* N*, and it holds that*

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

Then, the scheme in Construction 3 is an $\mathsf{IND\text{-}CPA}$*-secure leveled fully homomorphic encryption scheme under the* $\mathsf{LWE}_{n,q,\alpha q}^{(m+1)\times N}$ *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 $x \cdot \boldsymbol{G}$ 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 $x \in \{0,1\}^\ell$ in Construction 3, then the resulting final ciphertext is of the form $\boldsymbol{A}\cdot\boldsymbol{S}+\boldsymbol{E}+C(x)\boldsymbol{G}$, where $\boldsymbol{S} \in \mathbb{Z}_q^{n\times N}$, $\boldsymbol{E} \in \mathbb{Z}_q^{(m+1)\times N}$ and $\|\boldsymbol{E}\|_\infty \leq \alpha q\sqrt{m+1}(N+1)^L$ (see [GSW13] for details). Choosing $1/(\alpha\sqrt{m+1})$ 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 $\boldsymbol{E}$ satisfies the condition $\|\boldsymbol{E}\|_\infty \leq \frac{q}{4\sqrt{m+1}}$.

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 $\mathsf{FHE}_{\mathsf{CD}}$. 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 [Mah18b] 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 λ).

- a power of 2 integer $q \geq 2$.
- an integer $m = \Omega(n \log q)$.
- an integer $N = (m+1)\log q$.
- noise ratios $\alpha, \beta \in (0,1)$ such that the parameter ratio β/α is superpolynomial in the parameter λ, the expression $1/(\beta\sqrt{m+1})$ is subexponential in the parameter N, and
$$2\sqrt{n} \leq \alpha q < \beta q \leq \frac{q}{4(m+1)\cdot(2N+2)^L}.$$
- a rounding parameter $p = \sqrt{N(m+1)}/2\beta$ and arbitrary $\delta \in (0,1)$.

Construction 4 (Dual-Regev leveled FHE scheme with certified deletion)**.** *Let $\lambda \in \mathbb{N}$ be a parameter and* $\mathsf{DualFHE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Convert})$ *be the scheme in Construction 3. The Dual-Regev (leveled)* FHE *scheme* $\mathsf{DualFHE}_{\mathsf{CD}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Del}, \mathsf{Vrfy})$ *with certified deletion is defined by:*

$\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{KeyGen}(1^\lambda) \rightarrow (\mathsf{pk}, \mathsf{sk})$: *generate* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{DualFHE}.\mathsf{KeyGen}(1^\lambda)$ *and output* $(\mathsf{pk}, \mathsf{sk})$.

$\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk}, x) \rightarrow (\mathsf{vk}, |\mathsf{ct}\rangle)$: *to encrypt $x = (x_1, \dots, x_\ell) \in \{0,1\}^\ell$, generate $|\mathsf{ct}\rangle$ as follows: For every index $i \in [\ell]$, generate $|\mathsf{ct}_i\rangle$ in system C_i by sampling a random vector $V_i \xleftarrow{\$} \mathbb{Z}_q^m$ with $\mathsf{vk}_i \leftarrow \boldsymbol{V}_i$, sampling $\boldsymbol{A} \cdot \boldsymbol{S}_i + \boldsymbol{E}_i + x_i \boldsymbol{G} \pmod q \leftarrow \mathsf{DualFHE}.\mathsf{Enc}(\mathsf{pk}, x)$ with $\boldsymbol{E}_i \sim D_{\mathbb{Z}^{(m+1)\times N}, \alpha q}$ and then preparing the $N(m+1)$-qudit quantum state given by*
$$|\mathsf{ct}_i\rangle = \sum_{\boldsymbol{E}^{(i)} \in \mathbb{Z}_q^{(m+1)\times N}} \sqrt{D_{\mathbb{Z}_q^{(m+1)\times N}, \beta q}(\boldsymbol{E}^{(i)})}\, \omega_q^{-\mathrm{tr}[\boldsymbol{E}^{(i)T}\boldsymbol{V}_i]}\, |\boldsymbol{A} \cdot \boldsymbol{S}_i + \boldsymbol{E}_i + \boldsymbol{E}^{(i)} + x_i \boldsymbol{G} \pmod q\rangle .$$

Output $(\mathsf{vk}, |\mathsf{ct}\rangle)$, *where* $\mathsf{vk} = (\mathsf{vk}_1, \dots, \mathsf{vk}_\ell)$ *and* $|\mathsf{ct}\rangle = |\mathsf{ct}_1\rangle \otimes \cdots \otimes |\mathsf{ct}_\ell\rangle$.

$\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Eval}(C, |\mathsf{ct}\rangle) \rightarrow (|\widetilde{\mathsf{ct}}\rangle, t_C)$: *apply the Boolean circuit C composed of* NAND *gates to the ciphertext $|\mathsf{ct}\rangle$ in system C_{in} as follows: For every gate NAND_{ij} in the circuit C between a ciphertext pair in systems C_i and C_j, repeat the following two steps:*

- *apply U_{NAND} from Definition 36 to systems $\mathsf{C}_i\mathsf{C}_j$ 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 NAND_{ij} to the circuit transcript t_C.*

Output $(|\widetilde{\mathsf{ct}}\rangle, t_C)$, where $|\widetilde{\mathsf{ct}}\rangle$ is the final post-evaluation state in systems $\mathsf{C}_{\mathsf{in}}\mathsf{C}_{\mathsf{aux}}\mathsf{C}_{\mathsf{out}}$ and

- *$\mathsf{C}_{\mathsf{in}} = \mathsf{C}_1 \cdots \mathsf{C}_\ell$ denotes the initial ciphertext systems of $|\mathsf{ct}_1\rangle \otimes \cdots \otimes |\mathsf{ct}_\ell\rangle$.*

- $\mathsf{C}_{\mathsf{aux}}$ *denotes all intermediate auxiliary ciphertext systems.*
- $\mathsf{C}_{\mathsf{out}}$ *denotes the final ciphertext system corresponding to the output of the circuit* C*.*

$\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Dec}(\mathsf{sk}, |\mathsf{ct}\rangle) \rightarrow \{0,1\}^{\mu}$ **or** $\perp$: *measures the state* $|\mathsf{ct}\rangle$ *in the computational basis with outcome* $\boldsymbol{C} = (\boldsymbol{C}_1, \dots, \boldsymbol{C}_{\mu})$*, where* $\boldsymbol{C}_i \in \mathbb{Z}_q^{(m+1)\times N}$ *and* $\mu \geq 1$*, and outputs* $x' \leftarrow \mathsf{DualFHE}.\mathsf{Dec}(\mathsf{sk}, \boldsymbol{C})$*.*

$\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Del}(|\mathsf{ct}\rangle) \rightarrow \pi$: *measures each qudit of* $|\mathsf{ct}\rangle$ *in the* q*-ary Fourier basis with outcome* π*.*

$\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Extract}\langle \mathcal{S}(|\widetilde{\mathsf{ct}}\rangle, t_C), \mathcal{R}(\mathsf{sk})\rangle \rightarrow (\varrho, y)$ *this is the following interactive protocol between a sender* $\mathcal{S}$ *with input* $|\widetilde{\mathsf{ct}}\rangle$ *in systems* $\mathsf{C}_{\mathsf{in}}\mathsf{C}_{\mathsf{aux}}\mathsf{C}_{\mathsf{out}}$ *and transcript* t_C*, and a receiver* $\mathcal{R}$ *with input* sk*:*

- $\mathcal{S}$ *and* $\mathcal{R}$ *run the rewinding protocol* $\Pi = \langle \mathcal{S}(|\widetilde{\mathsf{ct}}\rangle, t_C), \mathcal{R}(\mathsf{sk})\rangle$ *in* Protocol 2*.*
- *Once* Π *is complete,* $\mathcal{S}$ *obtains a state* ϱ *in system* C_{in} *and the receiver obtains a bit* $y \in \{0,1\}$*.*

$\mathsf{FHE}_{\mathsf{CD}}.\mathsf{Vrfy}(\mathsf{vk}, \pi) \rightarrow \{0,1\}$: *to verify a certificate* π*, do the following:*

- *parse* $(\pi_1, \dots, \pi_{\ell}) \leftarrow \pi$*, where* $\pi_i \in \mathbb{Z}_q^{(m+1)\times N}$ *for* $i \in [\ell]$*.*
- *parse the verification key as* $(\boldsymbol{V}_1, \dots, \boldsymbol{V}_{\ell}) \leftarrow \mathsf{vk}$*.*
- *Output* 1*, if* $F^{\mathsf{corr}}(\boldsymbol{V}_i, \pi_i) = 1$ *(see* Definition 25*) with parameters* $0 \leq p < q$ *and* $\delta \in (0,1)$ *for every index* $i \in [\ell]$*, and output* 0 *otherwise.*

Protocol 2 (Rewinding Protocol)**.** *Let* $\mathsf{DualFHE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Convert})$ *be the Dual-Regev* FHE *scheme in* Construction 3*. Consider the following interactive protocol* $\Pi = \langle \mathcal{S}(\varrho, t_C), \mathcal{R}(\mathsf{sk})\rangle$ *between a sender* $\mathcal{S}$ *which takes as input state* ϱ *in systems* $\mathsf{C}_{\mathsf{in}}\mathsf{C}_{\mathsf{aux}}\mathsf{C}_{\mathsf{out}}$ *and a transcript* t_C *of a Boolean circuit* C*, as well as a receiver* $\mathcal{R}$ *which takes as input a secret key* sk*.*

1. $\mathcal{S}$ *sends system* $\mathsf{C}_{\mathsf{out}}$ *of the state* ϱ *associated with the encrypted output of the circuit* C *to* $\mathcal{R}$*.*
2. $\mathcal{R}$ *runs* $U_{\mathsf{DualFHE}.\mathsf{Dec}_{\mathsf{sk}}}$ *(with the key* sk *hard coded) to reversibly decrypt system* $\mathsf{C}_{\mathsf{out}}$*, where*

$$U_{\mathsf{DualFHE}.\mathsf{Dec}_{\mathsf{sk}}}: \quad |\boldsymbol{C}\rangle_{\mathsf{C}_{\mathsf{out}}} \otimes |0\rangle_{M} \rightarrow |\boldsymbol{C}\rangle_{\mathsf{C}_{\mathsf{out}}} \otimes |\mathsf{DualFHE}.\mathsf{Dec}_{\mathsf{sk}}(\boldsymbol{C})\rangle_{M},$$

for any matrix $\boldsymbol{C} \in \mathbb{Z}_q^{(m+1)\times N}$*.* $\mathcal{R}$ *then measures system* M *to obtain a bit* $y \in \{0,1\}$ *(the supposed output of the Boolean circuit* C*). Afterwards,* $\mathcal{R}$ *applies* $U^{\dagger}_{\mathsf{DualFHE}.\mathsf{Dec}_{\mathsf{sk}}}$*, discards the ancillary system* M*, and sends back the post-measurement system* $\widetilde{\mathsf{C}_{\mathsf{out}}}$ *of the resulting ciphertext* $\widetilde{\varrho}$ *to* $\mathcal{S}$*.*

3. $\mathcal{S}$ *repeats the following two steps in order to uncompute the systems* $\mathsf{C}_{\mathsf{aux}}\widetilde{\mathsf{C}_{\mathsf{out}}}$ *from the state* $\widetilde{\varrho}$*: For every gate* $\mathsf{NAND}_{ij} \in t_C$*, where* i *and* j *denote the respective ciphertext systems* C_i *and* C_j*, in decreasing order starting from the last gate in the circuit transcript* t_C*:*
   - $\mathcal{S}$ *applies* $U^{\dagger}_{\mathsf{NAND}}$ *from* Definition 36 *to systems* $\mathsf{C}_i\mathsf{C}_j\mathsf{C}_{ij}$ *of* $\widetilde{\varrho}$ *to uncompute system* C_{ij}*.*
   - $\mathcal{S}$ *repeats the procedure starting from the new outcome state* $\widetilde{\varrho}$*.*

Let us now define how to perform the homomorphic NAND gate in Construction 4 in more detail.

Definition 36 (Homomorphic NAND gate)**.** *Let $q \geq 2$ be a modulus, and let m and N be integers. Let $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z} \in \mathbb{Z}_q^{(m+1)\times N}$ be arbitrary matrices. We define the homomorphic NAND gate as the unitary*

$$U_{\mathsf{NAND}}: \quad |\boldsymbol{X}\rangle_X \otimes |\boldsymbol{Y}\rangle_Y \otimes |\boldsymbol{Z}\rangle_Z \quad \rightarrow \quad |\boldsymbol{X}\rangle_X \otimes |\boldsymbol{Y}\rangle_Y \otimes |\boldsymbol{Z} + \boldsymbol{G} - \boldsymbol{X} \cdot \boldsymbol{G}^{-1}(\boldsymbol{Y}) \pmod q\rangle_Z\,,$$

where $\boldsymbol{G} \in \mathbb{Z}_q^{(m+1)\times N}$ is the gadget matrix in Eq. (57).

To illustrate the action of our homomorphic NAND gate, we consider a simple example.

Example. Consider a pair of two ciphertexts $|\mathsf{ct}_i\rangle \otimes |\mathsf{ct}_j\rangle$ which encrypt two bits $x_i, x_j \in \{0, 1\}$ as in Construction 4. Let $U_{\mathsf{NAND}_{ij}}$ denote the homomorphic NAND gate applied to systems C_i and C_j. Then,

$$U_{\mathsf{NAND}_{ij}}: \quad |\mathsf{ct}_i\rangle_{C_i} \otimes |\mathsf{ct}_j\rangle_{C_j} \otimes |\boldsymbol{0}\rangle_{C_{ij}} \quad \rightarrow \quad |\mathsf{ct}_{ij}\rangle_{C_iC_jC_{ij}}\,.$$

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

$$U^{\dagger}_{\mathsf{NAND}_{ij}}: \quad |\mathsf{ct}_{ij}\rangle_{C_iC_jC_{ij}} \quad \rightarrow \quad |\mathsf{ct}_i\rangle_{C_i} \otimes |\mathsf{ct}_j\rangle_{C_j} \otimes |\boldsymbol{0}\rangle_{C_{ij}}\,.$$

Let us now analyze how U_{NAND} acts on the basis states of a pair of ciphertexts $|\mathsf{ct}_i\rangle \otimes |\mathsf{ct}_j\rangle$ that encode LWE samples as in Construction 4. In the following, $\boldsymbol{E}_i, \boldsymbol{E}_j \sim D_{\mathbb{Z}^{(m+1)\times N}, \alpha q}$ are sampled from a discrete Gaussian, whereas $\boldsymbol{E}^{(i)}, \boldsymbol{E}^{(j)} \sim D_{\mathbb{Z}_q^{(m+1)\times N}, \beta q}$ have a Gaussian distribution as part of the superposition. Then,

$$\begin{aligned} U_{\mathsf{NAND}_{ij}}: \quad & |\boldsymbol{A}\boldsymbol{S}_i + \boldsymbol{E}_i + \boldsymbol{E}^{(i)} + x_i\boldsymbol{G}\rangle_{C_i} \otimes |\boldsymbol{A}\boldsymbol{S}_j + \boldsymbol{E}_j + \boldsymbol{E}^{(j)} + x_j\boldsymbol{G}\rangle_{C_j} \otimes |\boldsymbol{0}\rangle_{C_{ij}} \\ \rightarrow\ & |\boldsymbol{A}\boldsymbol{S}_i + \boldsymbol{E}_i + \boldsymbol{E}^{(i)} + x_i\boldsymbol{G}\rangle_{C_i} \otimes |\boldsymbol{A}\boldsymbol{S}_j + \boldsymbol{E}_j + \boldsymbol{E}^{(j)} + x_j\boldsymbol{G}\rangle_{C_j} \otimes |\boldsymbol{A}\boldsymbol{S}_{ij} + \boldsymbol{E}_{ij} + (1 - x_ix_j)\boldsymbol{G}\rangle_{C_{ij}}\,, \end{aligned}$$

where introduced the following matrices

$$\begin{aligned} &\boldsymbol{S}_{ij} := -\boldsymbol{S}_i \cdot \boldsymbol{G}^{-1}(\boldsymbol{A}\boldsymbol{S}_j + \boldsymbol{E}_j + \boldsymbol{E}^{(j)} + x_j\boldsymbol{G}) - x_i\boldsymbol{S}_i \pmod q \\ &\boldsymbol{E}_{ij} := -\boldsymbol{E}_i \cdot \boldsymbol{G}^{-1}(\boldsymbol{A}\boldsymbol{S}_j + \boldsymbol{E}_j + \boldsymbol{E}^{(j)} + x_j\boldsymbol{G}) - x_i\boldsymbol{E}_j - \boldsymbol{E}^{(i)} \cdot \boldsymbol{G}^{-1}(\boldsymbol{A}\boldsymbol{S}_j + \boldsymbol{E}_j + \boldsymbol{E}^{(j)} + x_j\boldsymbol{G}) - x_i\boldsymbol{E}^{(j)} \pmod q. \end{aligned}$$

Because the initial error terms have the property that $\|\boldsymbol{E}_i\|_\infty, \|\boldsymbol{E}_j\|_\infty \leq \alpha q\sqrt{m+1} \leq \beta q\sqrt{m+1}$, it follows that the resulting error after a single NAND gate is at most (see also [GSW13, Mah18b] for more details)

$$\|\boldsymbol{E}_{ij}\|_\infty \leq 2\beta q\sqrt{m+1}(N+1).$$

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 [Mah18b].

9.2 Rewinding lemma

Notice that the procedure $\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Eval}$ in Construction 4 produces a highly entangled state since the unitary operation U_{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.

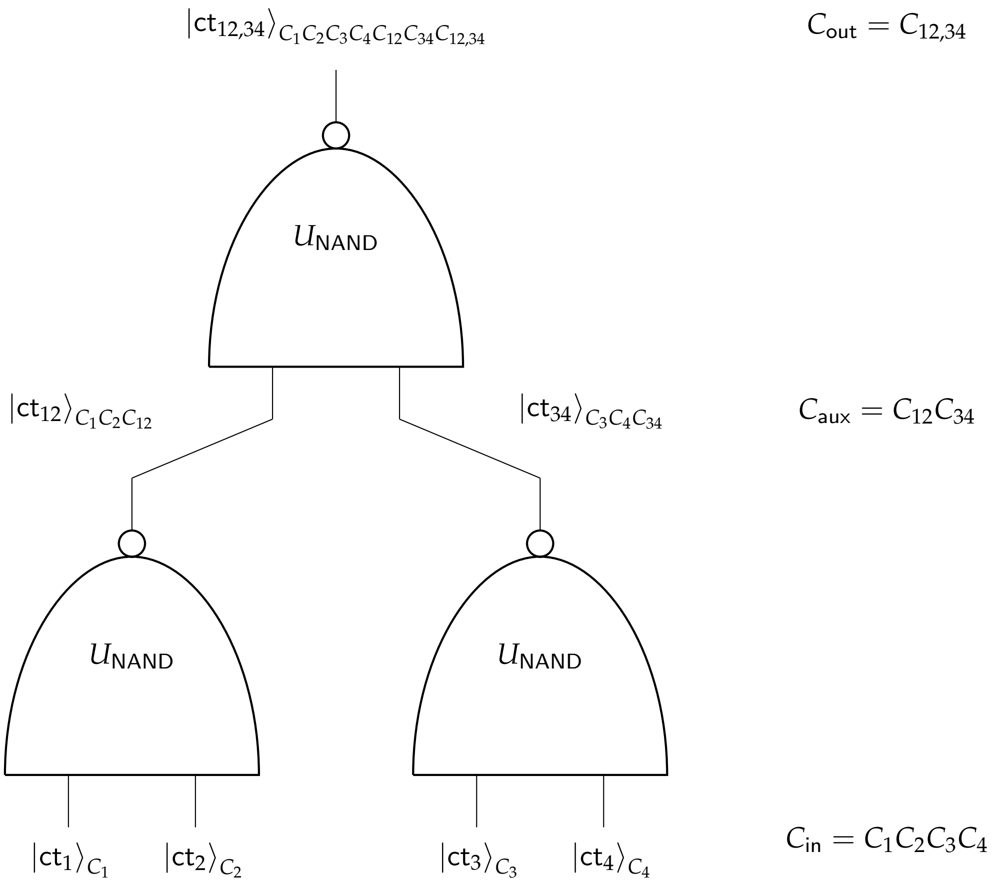
$|\mathsf{ct}_{12,34}\rangle_{C_1C_2C_3C_4C_{12}C_{34}C_{12,34}}$
$\mathsf{C}_{\mathsf{out}} = \mathsf{C}_{12,34}$
U_{NAND}
$|\mathsf{ct}_{12}\rangle_{C_1C_2C_{12}}$
$|\mathsf{ct}_{34}\rangle_{C_3C_4C_{34}}$
$\mathsf{C}_{\mathsf{aux}} = \mathsf{C}_{12}\mathsf{C}_{34}$
U_{NAND}
U_{NAND}
$|\mathsf{ct}_1\rangle_{C_1}$
$|\mathsf{ct}_2\rangle_{C_2}$
$|\mathsf{ct}_3\rangle_{C_3}$
$|\mathsf{ct}_4\rangle_{C_4}$
$\mathsf{C}_{\mathsf{in}} = \mathsf{C}_1\mathsf{C}_2\mathsf{C}_3\mathsf{C}_4$

Figure 3: Homomorphic evaluation of a Boolean circuit C composed entirely of three NAND gates. Here, the input is the quantum ciphertext $|\mathsf{ct}_1\rangle \otimes |\mathsf{ct}_2\rangle \otimes |\mathsf{ct}_3\rangle \otimes |\mathsf{ct}_4\rangle$ which corresponds to an encryption of the plaintext $x = (x_1, \dots, x_4) \in \{0,1\}^4$ as in Construction 4. The resulting ciphertext $|\mathsf{ct}_{12,34}\rangle$ lives on a system $C_1C_2C_3C_4C_{12}C_{34}C_{12,34}$ of which the last system $C_{12,34}$ contains an encryption of $C(x) \in \{0,1\}$.

Lemma 19 (Rewinding lemma)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter. Let $n \in \mathbb{N}$, $m = \Omega(n \log q)$ and let $q \geq 2$ be a power of 2 integer. Let $N = (m+1)\log q$ and let L be an upper bound on the depth of the polynomial-sized Boolean circuit C which is to be evaluated. Let $\alpha, \beta \in (0,1)$ be noise ratios such that $1/(\beta\sqrt{m+1})$ is subexponential in the parameter N, the ratio β/α is superpolynomial in λ and*

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

Let $\mathsf{DualFHE}_{\mathsf{CD}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Del}, \mathsf{Vrfy})$ be the Dual-Regev (leveled) FHE scheme with certified deletion in Construction 4 and let Π be the interactive protocol in Protocol 2. Then, the following holds for any parameter $\lambda \in \mathbb{N}$, plaintext $x \in \{0,1\}^\ell$ and any polynomial-sized Boolean circuit C:

After the interactive protocol $\Pi = \langle \mathcal{S}(\widetilde{\mathsf{ct}}, t_C), \mathcal{R}(\mathsf{sk})\rangle$ between the sender $\mathcal{S}$ and receiver $\mathcal{R}$ is complete, the sender $\mathcal{S}$ is in possession of a quantum state ϱ in system C_{in} that satisfies

$$\|\varrho - \mathsf{ct}\|_{\mathrm{tr}} \leq \mathrm{negl}(\lambda),$$

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

Proof. Let $\lambda \in \mathbb{N}$, $x \in \{0,1\}^\ell$ be a plaintext and C be any Boolean circuit of NAND-depth $L = \mathrm{poly}(\lambda)$. Let $(\widetilde{\mathsf{ct}}, t_C) \leftarrow \mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Eval}(C, |\mathsf{ct}\rangle)$ be the post-evaluation state $\widetilde{\mathsf{ct}}$ in systems $C_{\mathsf{in}} C_{\mathsf{aux}} C_{\mathsf{out}}$ with circuit transcript t_C and let ϱ be the outcome of the interactive protocol $\Pi = \langle \mathcal{S}(\widetilde{\mathsf{ct}}, t_C), \mathcal{R}(\mathsf{sk})\rangle$. Recall that, in Lemma 20, we established that there exists a negligible $\varepsilon(\lambda)$ such that $\mathsf{DualFHE}.\mathsf{Dec}_{\mathsf{sk}}$ decrypts system C_{out} of $\widetilde{\mathsf{ct}}$ with probability at least $1 - \varepsilon$. By the ”Almost As Good As New Lemma“ (Lemma 1), performing the operation $U_{\mathsf{DualFHE}.\mathsf{Dec}_{\mathsf{sk}}}$, measuring the ancillary register M and rewinding the computation, results in a mixed state $\widetilde{\varrho}$ that is within trace distance $\sqrt{\varepsilon}$ of the post-evaluation state $\widetilde{\mathsf{ct}}$. Notice that, by reversing the sequence U_{t_C} of homomorphic NAND gates according to the transcript t_C with respect to $\widetilde{\mathsf{ct}}$, we recover the initial ciphertext $\mathsf{ct} = U_{t_C}^\dagger \widetilde{\mathsf{ct}}\, U_{t_C}$ in system C_{in}. By definition, we also have that $\varrho = U_{t_C}^\dagger \widetilde{\varrho}\, U_{t_C}$. Therefore,

$$\|\varrho - \mathsf{ct}\|_{\mathrm{tr}} = \|U_{t_C}^\dagger \widetilde{\varrho}\, U_{t_C} - U_{t_C}^\dagger \widetilde{\mathsf{ct}}\, U_{t_C}\|_{\mathrm{tr}} = \|\widetilde{\varrho} - \widetilde{\mathsf{ct}}\|_{\mathrm{tr}} \leq \sqrt{\varepsilon(\lambda)},$$

where we used that the trace distance is unitarily invariant. Since $\varepsilon(\lambda) = \mathrm{negl}(\lambda)$, this proves the claim. □

Proof of correctness. Let us now verify the correctness of decryption and verification of Construction 4.

Lemma 20 (Compactness and full homomorphism of $\mathsf{DualFHE}_{\mathsf{CD}}$)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter. Let $n \in \mathbb{N}$, $m = \Omega(n \log q)$ and let $q \geq 2$ be a power of 2 integer. Let $N = (m+1)\log q$ and let L be an upper bound on the* NAND*-depth of the polynomial-sized Boolean circuit C which is to be evaluated. Let $\alpha, \beta \in (0,1)$ be noise ratios such that $1/(\beta\sqrt{m+1})$ is subexponential in the parameter N, the ratio β/α between the noise parameters is superpolynomial in λ and*

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

Then, the scheme $\mathsf{DualFHE}_{\mathsf{CD}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Del}, \mathsf{Vrfy})$ *in Construction 4 is a compact and fully homomorphic encryption scheme with certified deletion. In other words, for any efficiency (in $\lambda \in \mathbb{N}$) computable circuit $C : \{0,1\}^\ell \rightarrow \{0,1\}$ and any set of inputs $x = (x_1, \dots, x_\ell) \in \{0,1\}^\ell$, it holds that:*

$$\Pr\left[\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Dec}(\mathsf{sk}, \widetilde{\mathsf{ct}}) \neq C(x_1, \dots, x_\ell) \,\middle|\, \substack{(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{KeyGen}(1^\lambda, 1^L) \\ (\mathsf{vk},\mathsf{ct}) \leftarrow \mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk}, x) \\ (\widetilde{\mathsf{ct}}, t_C) \leftarrow \mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Eval}(C, \mathsf{ct}, \mathsf{pk})}\right] = \mathrm{negl}(\lambda).$$

Proof. Let $|\mathsf{ct}\rangle$ be the ciphertext output by $\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk}, x)$, where $x \in \{0,1\}^\ell$ denotes the plaintext, and let $(|\widetilde{\mathsf{ct}}\rangle, t_C) \leftarrow \mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Eval}(C, |\mathsf{ct}\rangle)$ 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 $D_{\mathbb{Z}_q^{(m+1)\times N}, \beta q}$ is supported on $\{\boldsymbol{X} \in \mathbb{Z}_q^{(m+1)\times N} : \|\boldsymbol{X}\|_\infty \leq \sqrt{N(m+1)}\beta q\}$. Recall that $\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Dec}(\mathsf{sk}, |\widetilde{\mathsf{ct}}\rangle)$ measures the ciphertext $|\widetilde{\mathsf{ct}}\rangle$ in the computational basis with outcome $\boldsymbol{C} = (\boldsymbol{C}_1, \dots, \boldsymbol{C}_\ell)$, where $\boldsymbol{C}_i \in \mathbb{Z}_q^{(m+1)\times N}$ is a matrix, and outputs $x' \leftarrow \mathsf{DualFHE}.\mathsf{Dec}(\mathsf{sk}, \boldsymbol{C})$. Therefore, it follows from our choice of parameters that

$$\|\boldsymbol{E}_i + \boldsymbol{E}^{(i)}\|_\infty \leq 2\beta q\sqrt{N(m+1)} < \frac{q}{4\sqrt{m+1}}, \quad \forall i \in [\ell].$$

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

$|\mathsf{ct}\rangle$. In this case, the cumulative error in system $\mathsf{C}_{\mathsf{out}}$ after L applications of U_{NAND} in Definition 36 is at most $\beta q \sqrt{m+1}(2N+2)^L$, which is less than $\frac{q}{4\sqrt{m+1}}$ by our choice of parameters. Therefore, the procedure $\mathsf{DualFHE.Dec}_{\mathsf{sk}}$ decrypts a computational basis state in system $\mathsf{C}_{\mathsf{out}}$ of the state $|\widetilde{\mathsf{ct}}\rangle$ correctly with probability at least $1-\mathrm{negl}(\lambda)$. Furthermore, because the procedure $\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Dec}$ is independent of the circuit C and its depth L, the scheme $\mathsf{DualFHE}_{\mathsf{CD}}$ is compact. This proves the claim. □

Let us now verify the correctness of verification of the scheme $\mathsf{DualFHE}_{\mathsf{CD}}$ in Construction 4 according to Definition 32. We show the following.

Lemma 21 (Correctness of verification)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter. Let $n \in \mathbb{N}$, $m = \Omega(n \log q)$ and let $q \geq 2$ be a power of 2 integer. Let $N = (m+1)\log q$ and let L be an upper bound on the depth of the polynomial-sized Boolean circuit C which is to be evaluated. Let $p = \sqrt{N(m+1)}/2\beta$ and arbitrary $\delta \in (0,1)$ be rounding parameters. Let $\alpha, \beta \in (0,1)$ be noise ratios such that $1/(\beta\sqrt{m+1})$ is subexponential in the parameter N, the ratio β/α is superpolynomial in λ and*

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

Then, the Dual-Regev FHE *scheme* $\mathsf{DualFHE}_{\mathsf{CD}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Del}, \mathsf{Vrfy})$ *with certified deletion in Construction 4 satisfies verification correctness. In other words, for any $\lambda \in \mathbb{N}$, any plaintext $x \in \{0,1\}^\ell$ and any polynomial-sized Boolean circuit C entirely composed of* NAND *gates:*

$$\Pr\left[\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Verify}(\mathsf{vk},\pi) = 1 \;\middle|\; \begin{smallmatrix}(\mathsf{pk},\mathsf{sk})\leftarrow\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{KeyGen}(1^\lambda)\\ (\mathsf{vk},|\mathsf{ct}\rangle)\leftarrow\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk},x)\\ \pi\leftarrow\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Del}(|\mathsf{ct}\rangle)\end{smallmatrix}\right] \geq 1-\mathrm{negl}(\lambda).$$

Proof. Let $|\mathsf{ct}\rangle$ be the ciphertext output by $\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk},x)$, where $x \in \{0,1\}^\ell$ denotes the plaintext, and let $(|\widetilde{\mathsf{ct}}\rangle, t_{\mathsf{C}}) \leftarrow \mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Eval}(\mathsf{C},|\mathsf{ct}\rangle)$ be the output of the evaluation procedure. Recall that $|\mathsf{ct}\rangle = |\mathsf{ct}_1\rangle \otimes \cdots \otimes |\mathsf{ct}_\ell\rangle$ is generated as follows: For every $i \in [\ell]$, the state $|\mathsf{ct}_i\rangle$ in system C_i is generated by sampling $V_i \xleftarrow{\$} \mathbb{Z}_q^m$ with $\mathsf{vk}_i \leftarrow \boldsymbol{V}_i$ and $\boldsymbol{A}\cdot\boldsymbol{S}_i + \boldsymbol{E}_i + x_i\boldsymbol{G} \pmod q \leftarrow \mathsf{DualFHE.Enc}(\mathsf{pk},x_i)$ with error $\boldsymbol{E}_i \sim D_{\mathbb{Z}^{(m+1)\times N},\alpha q}$, and then preparing the $N(m+1)$-qudit Gaussian coset given by

$$|\mathsf{ct}_i\rangle = \sum_{\boldsymbol{E}^{(i)} \in \mathbb{Z}_q^{(m+1)\times N}} \sqrt{D_{\mathbb{Z}_q^{(m+1)\times N},\beta q}(\boldsymbol{E}^{(i)})}\, \omega_q^{-\mathrm{tr}[\boldsymbol{E}^{(i)T}\boldsymbol{V}_i]}\, |\boldsymbol{A}\cdot\boldsymbol{S}_i + \boldsymbol{E}_i + \boldsymbol{E}^{(i)} + x_i\boldsymbol{G} \pmod q\rangle\,. \tag{58}$$

Recall that the deletion procedure $\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Del}(|\mathsf{ct}\rangle)$ measures each qudit of $|\mathsf{ct}\rangle$ in the q-ary Fourier basis. By the Switching Lemma (Lemma 11) and that $\beta q < q/\sqrt{2N(m+1)}$, we get that the Fourier transform of each Gaussian coset $|\mathsf{ct}_i\rangle$ in Eq. (58) results in a state within trace distance $\varepsilon = 2^{-\Omega(\lambda)}$ of the dual Gaussian coset, i.e.

$$\mathsf{FT}_q\, |\mathsf{ct}_i\rangle \;\approx_\varepsilon \sum_{\boldsymbol{E}^{(i)} \in \mathbb{Z}_q^{(m+1)\times N}} \sqrt{D_{\mathbb{Z}_q^{(m+1)\times N},1/2\beta}(\boldsymbol{E}^{(i)})}\, \omega_q^{-\mathrm{tr}[\boldsymbol{E}^{(i)T}(\boldsymbol{A}\cdot\boldsymbol{S}_i + \boldsymbol{E}_i + x_i\boldsymbol{G})]}\, |V_i + \boldsymbol{E}^{(i)} \pmod q\rangle\,. \tag{59}$$

Hence, a measurement in the q-ary Fourier basis results in a classical state $\widetilde{\sigma}^{(i)}$ in system P_i which is within distance $\|\widetilde{\sigma}^{(i)} - \sigma^{(i)}\|_{\mathrm{tr}} \leq 2^{-\Omega(\lambda)}$ of the Gaussian mixture $\sigma^{(i)}$ centered around $\boldsymbol{V}_i \in \mathbb{Z}_q^{(m+1)\times N}$, where

$$\sigma^{(i)} = \sum_{\boldsymbol{E}^{(i)} \in \mathbb{Z}_q^{(m+1)\times N}} D_{\mathbb{Z}_q^{(m+1)\times N},1/2\beta}(\boldsymbol{E}^{(i)})\, |\boldsymbol{V}_i + \boldsymbol{E}^{(i)} \pmod q\rangle\langle \boldsymbol{V}_i + \boldsymbol{E}^{(i)} \pmod q|. \tag{60}$$

Recall that the q-ary correlation flag $F^{\mathsf{corr}} : \mathbb{Z}_q^{(m+1)\times N} \times \mathbb{Z}_q^{(m+1)\times N} \to \{0,1\}$ in Definition 25 is defined as

$$F^{\mathsf{corr}}(\boldsymbol{X},\boldsymbol{Y}) := \begin{cases} 1 & \text{if } \omega(\lfloor \boldsymbol{X}-\boldsymbol{Y} \rceil_p) < N(m+1)\delta \\ 0 & \text{otherwise.} \end{cases} \tag{61}$$

Let $\widetilde{\sigma}^{(i)}_{V_iP_i}$ and $\sigma^{(i)}_{V_iP_i}$ be the associated states that include the verification keys $|\boldsymbol{V}_i\rangle\langle \boldsymbol{V}_i|_{V_i}$ in systems V_i. We can model the verification with F^{corr} as applying projectors $\Pi^{\mathsf{corr}}_{V_iP_i}$ on the correlated subset of systems V_iP_i, for

$$\Pi^{\mathsf{corr}}_{V_iP_i} = \sum_{\substack{\boldsymbol{X},\boldsymbol{Y}\in\mathbb{Z}_q^{(m+1)\times N} \text{ s.t.}\\ F^{\mathsf{corr}}(\boldsymbol{X},\boldsymbol{Y})=1}} |X\rangle\langle X|_{V_i} \otimes |Y\rangle\langle Y|_{P_i}, \qquad \forall i \in [\ell].$$

Thus, by definition, we have that the probability of successful verification is given by

$$\prod_{i=1}^{\ell} \mathrm{Tr}\left[\Pi^{\mathsf{corr}}_{V_iP_i}\widetilde{\sigma}^{(i)}_{V_iP_i}\right] = \Pr\left[\mathsf{DualFHE_{CD}.Verify}(\mathsf{vk},\pi) = 1 \,\middle|\, \begin{array}{c} (\mathsf{pk},\mathsf{sk})\leftarrow\mathsf{DualFHE_{CD}.KeyGen}(1^\lambda) \\ (\mathsf{vk},|\mathsf{ct}\rangle)\leftarrow\mathsf{DualFHE_{CD}.Enc}(\mathsf{pk},x) \\ (|\widetilde{\mathsf{ct}}\rangle,t_C)\leftarrow\mathsf{DualFHE_{CD}.Eval}(C,|\mathsf{ct}\rangle) \\ \pi\leftarrow\mathsf{DualFHE_{CD}.Del}\langle\mathcal{S}(|\widetilde{\mathsf{ct}}\rangle,t_C),\mathcal{R}(\mathsf{sk})\rangle \end{array}\right].$$

Because $p = \sqrt{N(m+1)}/2\beta$ and the truncated discrete Gaussian $D_{\mathbb{Z}_q^{(m+1)\times N},1/2\beta}$ is supported on the finite set $\{\boldsymbol{X} \in \mathbb{Z}_q^{(m+1)\times N} : \|\boldsymbol{X}\|_\infty \leq \sqrt{N(m+1)}/2\beta\}$, it holds for the classical Gaussian mixtures $\sigma^{(i)}$ that

$$\mathrm{Tr}[\Pi^{\mathsf{corr}}_{V_iP_i}\sigma^{(i)}_{V_iP_i}] = 1, \qquad \forall i \in [\ell]$$

Therefore, using Lemma 6 and the fact that $\|\widetilde{\sigma}^{(i)} - \sigma^{(i)}\|_{\mathrm{tr}} \leq 2^{-\Omega(\lambda)}$, we have

$$\mathrm{Tr}[\Pi^{\mathsf{corr}}_{V_iP_i}\widetilde{\sigma}^{(i)}_{V_iP_i}] \geq 1 - 2^{-\Omega(\lambda)} = 1 - \mathrm{negl}(\lambda), \qquad \forall i \in [\ell]. \tag{62}$$

Applying the union bound to Eq. (62) and using the fact that $\ell \cdot 2^{-\Omega(\lambda)} = \mathrm{negl}(\lambda)$, we get

$$\prod_{i=1}^{\ell} \mathrm{Tr}\left[\Pi^{\mathsf{corr}}_{V_iP_i}\widetilde{\sigma}^{(i)}_{V_iP_i}\right] \geq 1 - \ell\cdot 2^{-\Omega(\lambda)} = 1 - \mathrm{negl}(\lambda).$$

This proves the claim that $\mathsf{DualPKE_{CD}}$ satisfies correctness of verification. □

We now show that our scheme $\mathsf{DualFHE_{CD}}$ in Construction 4 is *extractable* according to Definition 33.

Lemma 22 (Extractability of $\mathsf{DualFHE_{CD}}$)**.** *Let $\lambda \in \mathbb{N}$ be a parameter. Let $n \in \mathbb{N}$, $m = \Omega(n \log q)$ and let $q \geq 2$ be a power of 2 integer. Let $N = (m+1)\log q$ and let L be an upper bound on the depth of the polynomial-sized Boolean circuit C which is to be evaluated. Let $p = \sqrt{N(m+1)}/2\beta$ and arbitrary $\delta \in (0,1)$ be rounding parameters. Let $\alpha,\beta \in (0,1)$ be noise ratios such that $1/(\beta\sqrt{m+1})$ is subexponential in the parameter N, the ratio β/α is superpolynomial in λ and*

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

Then, the Dual-Regev FHE *scheme $\Sigma = \mathsf{DualFHE_{CD}}$ with certified deletion in Construction 4 is extractable. In other words, for any efficiently computable circuit $\mathsf{C} : \{0,1\}^\ell \to \{0,1\}$ and any input $x \in \{0,1\}^\ell$:*

$$\Pr\left[y \neq \mathsf{C}(x_1,\dots,x_\ell) \,\middle|\, \begin{array}{c} (\mathsf{pk},\mathsf{sk})\leftarrow\Sigma.\mathsf{KeyGen}(1^\lambda,1^L) \\ (\mathsf{vk},\mathsf{ct})\leftarrow\Sigma.\mathsf{Enc}(\mathsf{pk},x) \\ (\widetilde{\mathsf{ct}},t_C)\leftarrow\Sigma.\mathsf{Eval}(C,\mathsf{ct},\mathsf{pk}) \\ (\varrho,y)\leftarrow\Sigma.\mathsf{Extract}\langle\mathcal{S}(\widetilde{\mathsf{ct}},t_C),\mathcal{R}(\mathsf{sk})\rangle \end{array}\right] \leq \mathrm{negl}(\lambda), \quad \textit{and}$$

$$\Pr\left[\Sigma.\mathsf{Vrfy}(\mathsf{vk},\pi)=\bot \;\middle|\; \begin{array}{c}(\mathsf{pk},\mathsf{sk})\leftarrow\Sigma.\mathsf{KeyGen}(1^\lambda,1^L)\\ (\mathsf{vk},\mathsf{ct})\leftarrow\Sigma.\mathsf{Enc}(\mathsf{pk},x)\\ (\widetilde{\mathsf{ct}},t_C)\leftarrow\Sigma.\mathsf{Eval}(C,\mathsf{ct},\mathsf{pk})\\ (\varrho,y)\leftarrow\Sigma.\mathsf{Extract}\langle\mathcal{S}(\widetilde{\mathsf{ct}},t_C),\mathcal{R}(\mathsf{sk})\rangle\\ \pi\leftarrow\Sigma.\mathsf{Del}(\varrho)\end{array}\right]\leq\operatorname{negl}(\lambda).$$

Proof. Let $C:\{0,1\}^\ell\rightarrow\{0,1\}$ be an efficiently computable circuit and let $x\in\{0,1\}^\ell$ be any input. Let $(\varrho,y)\leftarrow\Sigma.\mathsf{Extract}\langle\mathcal{S}(\widetilde{\mathsf{ct}},t_C),\mathcal{R}(\mathsf{sk})\rangle$ denote the outcome of the interactive protocol between the sender $\mathcal{S}$ and the receiver $\mathcal{R}$, where $(\widetilde{\mathsf{ct}},t_C)\leftarrow\Sigma.\mathsf{Eval}(C,\mathsf{ct},\mathsf{pk})$ is the post-evaluation state and $\mathsf{ct}\leftarrow\Sigma.\mathsf{Enc}(\mathsf{pk},x)$ is the initial ciphertext for $(\mathsf{pk},\mathsf{sk})\leftarrow\Sigma.\mathsf{KeyGen}(1^\lambda)$. Recall that the receiver $\mathcal{R}$ reversibly performs the decryption procedure $\Sigma.\mathsf{Dec}$ (with the secret key sk hard-coded) during the execution of $\Pi=\langle\mathcal{S}(\widetilde{\mathsf{ct}},t_C),\mathcal{R}(\mathsf{sk})\rangle$ in Protocol 2. Therefore, it follows that the measurement outcome y is equal to $C(x_1,\dots,x_\ell)$ 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 $\Pi=\langle\mathcal{S}(\widetilde{\mathsf{ct}},t_C),\mathcal{R}(\mathsf{sk})\rangle$ between the sender $\mathcal{S}$ and receiver $\mathcal{R}$ is complete, the sender $\mathcal{S}$ is in possession of a quantum state ϱ in system C_{in} that satisfies

$$\|\varrho-\mathsf{ct}\|_{\mathrm{tr}}\leq\operatorname{negl}(\lambda).$$

Therefore, the claim follows immediately from the verification correctness of Σ shown in Lemma 21. □

9.3 Proof of security

Let us now analyze the security of our FHE scheme with certified deletion in Construction 4. 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 $\mathsf{DualFHE}_{\mathsf{CD}}$. We first prove that our scheme $\mathsf{FHE}_{\mathsf{CD}}$ in Construction 4 satisfies the notion IND-CPA security according to Definition 13. The proof is identical to the proof of IND-CPA-security of our DualPKE scheme in Theorem 7. We add it for completeness.

Theorem 10. *Let $n\in\mathbb{N}$, let $q\geq 2$ be a modulus, let $m=\Omega(n\log q)$ and let $N=(m+1)\log q$, each parameterized by the security parameter $\lambda\in\mathbb{N}$. Let $\alpha\in(0,1)$ with $\alpha q\geq 2\sqrt{n}$. Then, the scheme $\mathsf{DualFHE}_{\mathsf{CD}}$ in Construction 4 is IND-CPA-secure under the $\mathsf{LWE}_{n,q,\alpha q}^{N(m+1)}$ assumption.*

Proof. Let $\Sigma=\mathsf{DualFHE}_{\mathsf{CD}}$. We need to show that, for any QPT adversary $\mathcal{A}$, it holds that

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

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

1. The challenger generates a pair $(\mathsf{pk},\mathsf{sk})\leftarrow\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{KeyGen}(1^\lambda)$, and sends pk to $\mathcal{A}$.
2. $\mathcal{A}$ sends a distinct plaintext pair $(m_0,m_1)\in\{0,1\}^\ell\times\{0,1\}^\ell$ to the challenger.
3. The challenger computes $(\mathsf{vk},\mathsf{ct}_b)\leftarrow\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk},m_b)$, and sends $|\mathsf{ct}_b\rangle$ to $\mathcal{A}$.
4. $\mathcal{A}$ outputs a guess $b'\in\{0,1\}$, which is also the output of the experiment.

Recall that the procedure $\mathsf{DualFHE}_{\mathsf{CD}}.\mathsf{Enc}(\mathsf{pk}, m_b)$ outputs a pair $(\mathsf{vk}, |\mathsf{ct}_b\rangle)$, where $\mathsf{vk} = (\mathsf{vk}_1, \dots, \mathsf{vk}_\ell)$ and $|\mathsf{ct}_b\rangle = |\mathsf{ct}_1\rangle \otimes \dots \otimes |\mathsf{ct}_\ell\rangle$, generated as follows: For $i \in [\ell]$, $|\mathsf{ct}_i\rangle$ in system C_i is generated by sampling $V_i \xleftarrow{\$} \mathbb{Z}_q^m$ with $\mathsf{vk}_i \leftarrow \boldsymbol{V}_i$ and $\boldsymbol{A} \cdot \boldsymbol{S}_i + \boldsymbol{E}_i + m_{b,i}\boldsymbol{G} \pmod q \leftarrow \mathsf{DualFHE}.\mathsf{Enc}(\mathsf{pk}, m_{b,i})$ with error $\boldsymbol{E}_i \sim D_{\mathbb{Z}^{(m+1)\times N}, \alpha q}$, and then preparing the $N(m+1)$-qudit Gaussian coset given by

$$|\mathsf{ct}_i\rangle = \sum_{\boldsymbol{E}^{(i)} \in \mathbb{Z}_q^{(m+1)\times N}} \sqrt{D_{\mathbb{Z}_q^{(m+1)\times N}, \beta q}(\boldsymbol{E}^{(i)})}\, \omega_q^{-\mathrm{tr}[\boldsymbol{E}^{(i)T}\boldsymbol{V}_i]} \, |\boldsymbol{A} \cdot \boldsymbol{S}_i + \boldsymbol{E}_i + \boldsymbol{E}^{(i)} + m_{b,i}\boldsymbol{G} \pmod q)\rangle .$$

Under the (decisional) $\mathsf{LWE}_{n,q,\alpha q}^{N(m+1)}$ assumption in Definition 15, we have that, for all $i \in [\ell]$, $|\mathsf{ct}_i\rangle$ is computationally indistinguishable from a random Gaussian coset $|\mathcal{D}_{\beta q}^{\boldsymbol{U}_i, \boldsymbol{V}_i}\rangle$ with $\boldsymbol{U}_i \xleftarrow{\$} \mathbb{Z}_q^{(m+1)\times N}$, where

$$|\mathcal{D}_{\beta q}^{\boldsymbol{U}_i, \boldsymbol{V}_i}\rangle = \sum_{\boldsymbol{E}^{(i)} \in \mathbb{Z}_q^{(m+1)\times N}} \sqrt{D_{\mathbb{Z}_q^{(m+1)\times N}, \beta q}(\boldsymbol{E}^{(i)})}\, \omega_q^{-\mathrm{tr}[\boldsymbol{E}^{(i)T}\boldsymbol{V}_i]} \, |\boldsymbol{U}_i + \boldsymbol{E}^{(i)} \pmod q)\rangle .$$

Because each Gaussian coset $|\mathcal{D}_{\beta q}^{\boldsymbol{U}_i, \boldsymbol{V}_i}\rangle$ is completely indistinguishable from $b \in \{0, 1\}$, it follows that

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

This proves the claim. □

$\mathsf{IND\text{-}CPA\text{-}CD}$ **security of** $\mathsf{DualFHE}_{\mathsf{CD}}$**.** In this section, we analyze the security of our Dual-Regev homomorphic encryption scheme $\mathsf{DualFHE}_{\mathsf{CD}}$ in Construction 4 and show that it satisfies the notion of *certified deletion security* in the semi-honest adversarial model (as in Definition 35). In other words, we analyze the security of our encryption scheme in the setting in which the adversary honestly follows the execution of the protocol, but may later maliciously analyze the data collected along the way.

We remark that our scheme in Construction 4 therefore achieves a form of *everlasting security* [MQU07, HMNY21a] in the semi-honest model. Here, we assume that the adversary honestly follows the execution of the protocol, but is later assumed to be unbounded once the protocol is over.

Theorem 11. *Let $\lambda \in \mathbb{N}$ be the security parameter. Let $0 \leq p < q$ and $\delta \in (0, 1)$ be rounding parameters. Let $n \in \mathbb{N}$, $m = \Omega(n \log q)$ and let $q \geq 2$ be a power of 2 integer. Let $N = (m + 1) \log q$ and let L be an upper bound on the NAND-depth of the polynomial-sized Boolean circuit C which is to be evaluated. Let $p = \sqrt{N(m + 1)}/2\beta$ and arbitrary $\delta \in (0, 1)$ be rounding parameters. Let $\alpha, \beta \in (0, 1)$ be noise ratios such that $1/(\beta\sqrt{m + 1})$ is subexponential in the parameter N, the ratio β/α is superpolynomial in λ and*

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

Then, the leveled fully homomorphic encryption scheme $\mathsf{DualFHE}_{\mathsf{CD}}$ with certified deletion in Construction 4 is $\mathsf{IND\text{-}CPA\text{-}CD}$-secure in the semi-honest adversarial model according to Definition 35.

Proof. Let $\Sigma = \mathsf{DualFHE}_{\mathsf{CD}}$. We need to show that, for any QPT adversary $\mathcal{A}$, it holds that

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

We will prove this statement in the honest-but-curious adversarial model. Hence, we assume that $\mathcal{A}$ behaves honestly during the execution of the protocol, but after the experiment is over, $\mathcal{A}$ may carefully analyze the data collected during the protocol. Let $\lambda \in \mathbb{N}$ be the security parameter and let $b \in \{0, 1\}$. Consider the experiment $\mathsf{Exp}_{\Sigma, \mathcal{A}, \lambda}^{\mathsf{he\text{-}sh\text{-}cert\text{-}del}}(b)$ between the adversary $\mathcal{A}$ and a challenger which takes place as follows:

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

Let $|\mathsf{ct}_b\rangle \leftarrow \mathsf{DualFHE_{CD}.Enc}(\mathsf{pk}, m_b)$, where $|\mathsf{ct}_b\rangle = |\mathsf{ct}_1\rangle \otimes \cdots \otimes |\mathsf{ct}_\ell\rangle$ is generated as follows: For every index $i \in [\ell]$, the state $|\mathsf{ct}_i\rangle$ in system C_i is generated by sampling a verification key $V_i \xleftarrow{\$} \mathbb{Z}_q^m$ with $\mathsf{vk}_i \leftarrow \boldsymbol{V}_i$ and $\boldsymbol{A} \cdot \boldsymbol{S}_i + \boldsymbol{E}_i + m_{b,i}\boldsymbol{G} \pmod q \leftarrow \mathsf{DualFHE.Enc}(\mathsf{pk}, m_{b,i})$ with error $\boldsymbol{E}_i \sim D_{\mathbb{Z}^{(m+1)\times N}, \alpha q}$, and then preparing the $N(m+1)$-qudit Gaussian coset given by

$$|\mathsf{ct}_i\rangle = \sum_{\boldsymbol{E}^{(i)} \in \mathbb{Z}_q^{(m+1)\times N}} \sqrt{D_{\mathbb{Z}_q^{(m+1)\times N}, \beta q}(\boldsymbol{E}^{(i)})}\, \omega_q^{-\mathrm{tr}[\boldsymbol{E}^{(i)T} \boldsymbol{V}_i]}\, |\boldsymbol{A} \cdot \boldsymbol{S}_i + \boldsymbol{E}_i + \boldsymbol{E}^{(i)} + m_{b,i}\boldsymbol{G} \pmod q\rangle\,. \tag{63}$$

Recall that the deletion procedure $\mathsf{DualFHE_{CD}.Del}(|\mathsf{ct}_b\rangle)$ measures each qudit of $|\mathsf{ct}_b\rangle$ in the q-ary Fourier basis. By the Switching Lemma (Lemma 11) and that $\beta q < q/\sqrt{2N(m+1)}$, we get that the Fourier transform of each Gaussian coset $|\mathsf{ct}_i\rangle$ in Eq. (63) results in a state within trace distance $\varepsilon = 2^{-\Omega(\lambda)}$ of the dual Gaussian coset, i.e.

$$\mathsf{FT}_q\, |\mathsf{ct}_i\rangle \;\approx_\varepsilon \sum_{\boldsymbol{E}^{(i)} \in \mathbb{Z}_q^{(m+1)\times N}} \sqrt{D_{\mathbb{Z}_q^{(m+1)\times N}, 1/2\beta}(\boldsymbol{E}^{(i)})}\, \omega_q^{-\mathrm{tr}[\boldsymbol{E}^{(i)T}(\boldsymbol{A}\cdot\boldsymbol{S}_i + \boldsymbol{E}_i + m_{b,i}\boldsymbol{G})]}\, |\boldsymbol{V}_i + \boldsymbol{E}^{(i)} \pmod q\rangle\,. \tag{64}$$

Hence, for every $i \in [\ell]$, a q-ary Fourier basis measurement of the Gaussian coset state $|\mathsf{ct}_i\rangle$ in system C_i results in a classical state $\widetilde{\sigma}^{(i)}$ in system P_i which is within distance $\|\widetilde{\sigma}^{(i)} - \sigma^{(i)}\|_{\mathrm{tr}} \leq 2^{-\Omega(\lambda)}$ of the classical Gaussian mixture $\sigma^{(i)}$ in system P_i centered around $\boldsymbol{V}_i \in \mathbb{Z}_q^{(m+1)\times N}$, where

$$\sigma^{(i)} = \sum_{\boldsymbol{E}^{(i)} \in \mathbb{Z}_q^{(m+1)\times N}} D_{\mathbb{Z}_q^{(m+1)\times N}, 1/2\beta}(\boldsymbol{E}^{(i)})\, |\boldsymbol{V}_i + \boldsymbol{E}^{(i)} \pmod q\rangle\langle \boldsymbol{V}_i + \boldsymbol{E}^{(i)} \pmod q|. \tag{65}$$

Therefore, the post-measurement state $\widetilde{\sigma} = \widetilde{\sigma}^{(1)} \otimes \cdots \otimes \widetilde{\sigma}^{(\ell)}$ is statistically close to the Gaussian mixture $\sigma = \sigma^{(1)} \otimes \cdots \otimes \sigma^{(\ell)}$ in Eq. (65). Note that the state σ is completely independent of the ciphertext which encodes the plaintext $m_b \in \{0,1\}^\ell$. Therefore, once deletion has taken place, the advantage of the adversary $\mathcal{A}$ at distinguishing $b \in \{0,1\}$ is at most

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

This proves the claim. □

References

[Aar16] Scott Aaronson. The complexity of quantum states and transformations: From quantum money to black holes, 2016.

[AJOP20] Gorjan Alagic, Stacey Jeffery, Maris Ozols, and Alexander Poremba. On quantum chosen-ciphertext attacks and learning with errors. *Cryptography*, 4(1), 2020.

[AP20] Prabhanjan Ananth and Rolando L. La Placa. Secure software leasing, 2020.

[Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–636, 1993.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.

[BCM$^+$21] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device, 2021.

[BI20] Anne Broadbent and Rabib Islam. Quantum encryption with certified deletion. *Lecture Notes in Computer Science*, page 92–122, 2020.

[BJM19] Christian Badertscher, Daniel Jost, and Ueli Maurer. Generalized proofs of knowledge with fully dynamic setup. Cryptology ePrint Archive, Report 2019/662, 2019. https://ia.cr/2019/662.

[BPTG14] Raphael Bost, Raluca Ada Popa, Stephen Tu, and Shafi Goldwasser. Machine learning classification over encrypted data. *IACR Cryptology ePrint Archive*, 2014:331, 2014.

[Bra18] Zvika Brakerski. Quantum fhe (almost) as secure as classical. Cryptology ePrint Archive, Report 2018/338, 2018. https://ia.cr/2018/338.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. In *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, FOCS '11, page 97–106, USA, 2011. IEEE Computer Society.

[CCL$^+$17] Yi-Hsiu Chen, Kai-Min Chung, Ching-Yi Lai, Salil P. Vadhan, and Xiaodi Wu. Computational notions of quantum min-entropy, 2017.

[CFGN96] Ran Canetti, Uri Feige, Oded Goldreich, and Moni Naor. Adaptively secure multi-party computation. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 639–648, New York, NY, USA, 1996. Association for Computing Machinery.

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography, 2021.

[CLZ21] Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering, 2021.

[CMP20] Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model, 2020.

[CRW19] Xavier Coiteux-Roy and Stefan Wolf. Proving erasure. *2019 IEEE International Symposium on Information Theory (ISIT)*, Jul 2019.

[DKW11] Stefan Dziembowski, Tomasz Kazana, and Daniel Wichs. One-time computable self-erasing functions. In *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011*, volume 6597 of *Lecture Notes in Computer Science*, page 125. Springer, 2011.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[FM18] Honghao Fu and Carl A. Miller. Local randomness: Examples and application. *Physical Review A*, 97(3), Mar 2018.

[Gen09] Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009. crypto.stanford.edu/craig.

[GGV20] Sanjam Garg, Shafi Goldwasser, and Prashant Nalini Vasudevan. Formalizing data deletion in the context of the right to be forgotten. *IACR Cryptol. ePrint Arch.*, page 254, 2020.

[GKZ19] Alex B. Grilo, Iordanis Kerenidis, and Timo Zijlstra. Learning-with-errors problem is easy with quantum samples. *Physical Review A*, 99(3), Mar 2019.

[GMP22] Alexandru Gheorghiu, Tony Metger, and Alexander Poremba. Quantum cryptography with classical communication: parallel remote state preparation for copy-protection, verification, and more, 2022.

[GPV07] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. Cryptology ePrint Archive, Report 2007/432, 2007. https://eprint.iacr.org/2007/432.

[GR02] Lov K. Grover and Terry Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions. *arXiv: Quantum Physics*, 2002.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. Cryptology ePrint Archive, Report 2013/340, 2013. https://ia.cr/2013/340.

[HH00] L. Hales and S. Hallgren. An improved quantum fourier transform algorithm and applications. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 515–525, 2000.

[HILL99] Johan HÅstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, March 1999.

[HMNY21a] Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Certified everlasting zero-knowledge proof for qma, 2021.

[HMNY21b] Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Quantum encryption with certified deletion, revisited: Public key, attribute-based, and classical communication, 2021.

[JL00] Stanisław Jarecki and Anna Lysyanskaya. Adaptively secure threshold cryptography: Introducing concurrency, removing erasures. In *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'00, page 221–242, Berlin, Heidelberg, 2000. Springer-Verlag.

[KNY21] Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Secure software leasing from standard assumptions, 2021.

[Len83] Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8(4):538–548, November 1983.

[LLL82] A. K. Lenstra, H. W. Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients. *MATH. ANN*, 261:515–534, 1982.

[Mah18a] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In Mikkel Thorup, editor, *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 332–338. IEEE Computer Society, 2018.

[Mah18b] Urmila Mahadev. Classical verification of quantum computations, 2018.

[MQU07] Jörn Müller-Quade and Dominique Unruh. Long-term security and universal composability. In Salil P. Vadhan, editor, *Theory of Cryptography*, pages 41–60, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, USA, 10th edition, 2011.

[Odl90] A. M. Odlyzko. The rise and fall of knapsack cryptosystems. pages 75–88, Cryptology and computational number theory, 42:75–88, 1990.

[PRSD17] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, page 461–473, New York, NY, USA, 2017. Association for Computing Machinery.

[PT10] Daniele Perito and Gene Tsudik. Secure code update for embedded devices via proofs of secure erasure. Cryptology ePrint Archive, Report 2010/217, 2010. https://ia.cr/2010/217.

[RAD78] R L Rivest, L Adleman, and M L Dertouzos. On data banks and privacy homomorphisms. *Foundations of Secure Computation, Academia Press*, pages 169–179, 1978.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34:1–34:40, 2005.

[TL17] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, July 2017.

[Tom13] Marco Tomamichel. A framework for non-asymptotic quantum information theory, 2013.

[TSSR11] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, Aug 2011.

[Unr13] Dominique Unruh. Revocable quantum timed-release encryption. Cryptology ePrint Archive, Report 2013/606, 2013. https://ia.cr/2013/606.

[VZ21] Thomas Vidick and Tina Zhang. Classical proofs of quantum knowledge, 2021.

[Wat06] John Watrous. Zero-knowledge against quantum attacks. In *Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '06, page 296–305, New York, NY, USA, 2006. Association for Computing Machinery.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

[Wil13] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, USA, 1st edition, 2013.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982.