Adaptive Hardcore Bit and Quantum Key Leasing over Classical Channel from LWE with Polynomial Modulus

Duong Hieu Phan[1], Weiqiang Wen[1], Xingyu Yan[2], and Jinwei Zheng[1]

[1] LTCI, Telecom Paris, Institut Polytechnique de Paris.
hieu.phan@telecom-paris.fr; weiqiang.wen@telecom-paris.fr; jinwei.zheng@telecom-paris.fr
[2] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China.
yanxy2020@bupt.edu.cn

Abstract. Quantum key leasing, also known as public key encryption with secure key leasing (PKE-SKL), allows a user to lease a (quantum) secret key to a server for decryption purpose, with the capability of revoking the key afterwards. In the pioneering work by Chardouvelis et al (arXiv:2310.14328), a PKE-SKL scheme utilizing classical channels was successfully built upon the noisy trapdoor claw-free (NTCF) family. This approach, however, relies on the superpolynomial hardness of learning with errors (LWE) problem, which could affect both efficiency and security of the scheme.

In our work, we demonstrate that the reliance on superpolynomial hardness is unnecessary, and that LWE with polynomial-size modulus is sufficient to achieve the same goal. Our approach enhances both efficiency and security, thereby improving the practical feasibility of the scheme on near-term quantum devices. To accomplish this, we first construct a *noticeable* NTCF (NNTCF) family with the adaptive hardcore bit property, based on LWE with polynomial-size modulus. To the best of our knowledge, this is the first demonstration of the adaptive hardcore bit property based on LWE with polynomial-size modulus, which may be of independent interest. Building on this foundation, we address additional challenges in prior work to construct the first PKE-SKL scheme satisfying the following properties: (*i*) the entire protocol utilizes only classical communication, and can also be lifted to support homomorphism. (*ii*) the security is solely based on LWE assumption with polynomial-size modulus.

As a demonstration of the versatility of our noticeable NTCF, we show that an efficient proof of quantumness protocol can be built upon it. Specifically, our protocol enables a classical verifier to test the quantumness while relying exclusively on the LWE assumption with polynomial-size modulus.

Keywords: Trapdoor claw-free functions · Adaptive hardcore bit · Secure key leasing · Proofs of quantumness · Learning with errors.

1 Introduction

In this article, we mainly focus on a fundamental primitive with a key-revocation capability – public key encryption with secure key leasing (PKE-SKL). Specifically, PKE-SKL refers to the realization of key-revocable PKE functionality, allowing the user/lessor to delegate decryption capability to the server/lessee in the form of a quantum decryption key, whereby once the key is revoked, the lessee loses the ability to decrypt. The PKE-SKL scheme is particularly effective in interactive cryptographic settings involving classical users and quantum servers.

Recently, inspired by secure software leasing in [ALP21], the notion of PKE-SKL was concurrently introduced by Agrawal et al in [AKN+23] and Ananth et al in [APV23]. Based on the PKE-SKL scheme, these works subsequently investigated the notion of secure key leasing for several extensions, like identity-based encryption (IBE), attribute-based encryption (ABE), functional encryption (FE), fully homomorphic encryption (FHE), and pseudorandom functions (PF). These key-revocable schemes based on the quantum no-cloning principle enable delegation and revocation of privileges, which is crucial in many cryptographic applications. Unfortunately, both recent works in [AKN+23,APV23] for constructing PKE-SKL have two shortcomings:

- The user and the server must have both quantum capabilities, and the key generation process has to require quantum communication;
- The construction requires *subexponential* hardness of the LWE assumption with superpolynomial modulus.

To address the former issue, Chardouvelis et al [CGJL23] recently introduced a semi-quantum PKE-SKL scheme, transforming their approach into a scheme with merely classical communication between a classical client and a quantum server. Their work is inspired by the work of classical verification of quantumness from LWE in [BCM+18]. Their construction is mainly based on a powerful cryptographic tool called the LWE-based noisy trapdoor claw-free functions (NTCF) with an adaptive hardcore bit (AHB) property.

However, the PKE-SKL scheme by Chardouvelis et al [CGJL23] does not address the second issue. Their construction still requires the subexponential hardness of LWE with a superpolynomial modulus. One of the main reasons for this is that their construction relies on NTCF with the AHB property, which in turn depends on the superpolynomial hardness of LWE assumption. This significantly affects the security and the efficiency of PKE-SKL, even making it unfriendly for implementation on near-term quantum devices. Thus, building on these, our main open question is the following:

Can efficient PKE-SKL with completely classical communication be based on the polynomial hardness of standard LWE over polynomially large modulus ?

1.1 Our Results

In this work, we affirmatively solve the above question. Main contributions are summarized in Fig. 1.

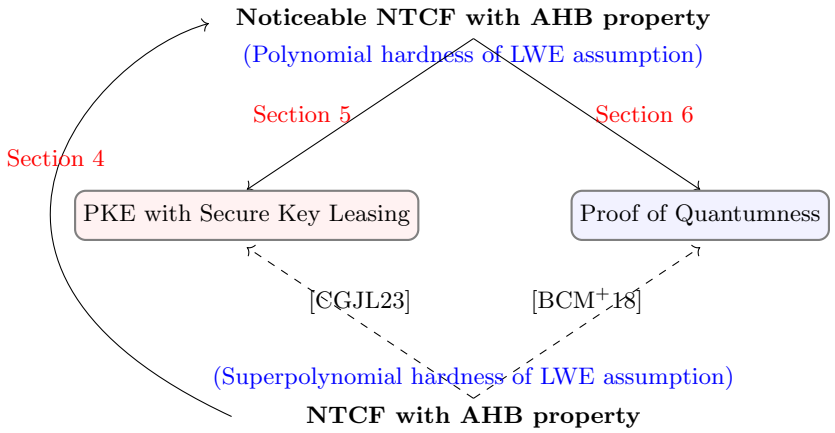

Fig. 1. Outline of main contributions in our work. To achieve a PKE-SKL scheme with a polynomially large modulus, we first improve the NTCF from [BCM+18] and propose a cryptographic primitive called noticeable NTCF (NNTCF). This primitive serves as the core tool for constructing PKE-SKL and can be constructed based on the polynomial hardness of LWE while still retaining the AHB property. We believe that NNTCF may have independent interests. In addition to constructing PKE-SKL schemes using NNTCF with AHB, as an example, we demonstrate a NNTCF-based proof of quantumness protocol to illustrate its versatility.

We show that a modified version of the PKE-SKL scheme [CGJL23] with merely classical communication can be constructed based on the hardness of LWE with polynomial modulus. Informally, we first obtain the following result.

Theorem 1 (Informal). *There exists a secure key leasing scheme for public key encryption with a completely classical lessor, assuming the hardness of LWE with polynomial modulus.*

Specifically, based on LWE with polynomial modulus, we can achieve PKE-SKL introduced in [CGJL23] with the following properties:

1. The protocol only uses polynomial-sized modulus q. This improves both efficiency and security.
2. The protocol executed between a classical lessor and a quantum lessee involves only classical communication, and all deletion certificates are classical.
3. The protocol satisfies a stronger PKE-SKL security described in [CGJL23]. We show that any quantum polynomial-time adversary can only simultaneously provide a valid classical deletion certificate and distinguish ciphertexts with at most negligible probability.

To achieve this target, we realize the ***adaptive hardcore bit property from the hardness of LWE with polynomial modulus***, which reduces the modulus from superpolynomial size in [BCM+18] to polynomial size. Besides this, we introduce an important primitive named the noticeable NTCF (NNTCF) family with this property.

Theorem 2 (Informal). *Assuming the hardness of the LWE problem with polynomial modulus, there exists a noticeable NTCF (NNTCF) family with the amplified adaptive hardcore bit property.*

To the best of our knowledge, prior to our work, the NTCF family with adaptive hardcore bit property can only be constructed based on superpolynomial modulus. We believe this noticeable version of NTCF using a smaller modulus may be of independent interest, such as enhancing the security[3] and improving the implementation efficiency of NTCF-based quantum cryptographic protocols: revocable quantum digital signatures [MPY23], proofs of quantumness [BCM+18,BKVV20], quantum delegated computation [Mah18b], certifiable randomness generation [BCM+18] etc. To illustrate this, we present a new proof of quantumness protocol based on NNTCF as an example.

Theorem 3 (Informal). *Assuming the polynomial hardness of the LWE with polynomial modulus, there exists a polynomial-sized proof of quantumness protocol from the NNTCF family.*

Specifically, our NNTCF-based proof of quantumness protocol circumvents the need for a superpolynomial modulus as required in [BCM+18], and fully satisfies both quantum completeness and classical soundness. Namely, the protocol ensures that a quantum polynomial-time prover can succeed with high probability (quantum completeness), while no classical polynomial-time prover can achieve comparable success probability (classical soundness). The soundness relies on the adaptive hardcore bit property of the NNTCF.

1.2 Related Works

Noisy Trapdoor claw-free functions The concept of noisy trapdoor claw-free functions (NTCF) was first introduced by Brakerski et al in the proofs of quantumness and certifiable quantum randomness generator [BCM+18], and was further developed by Mahadev within the realms of delegated quantum computing [Mah18b] and quantum homomorphic encryption [Mah18a]. Conceptually, trapdoor claw-free functions (TCFs) consist of a pair of injective functions f_0 and f_1 that share the same image. With access to a secret trapdoor td, it becomes easy to determine the two preimages $\mathbf{x}_0$ and $\mathbf{x}_1$ of the same image $\mathbf{y}$, such that $f_0(\mathbf{x}_0) = f_1(\mathbf{x}_1) = \mathbf{y}$. However, it is computationally difficult to invert f_0, f_1 without the trapdoor td. Such a pair of $(\mathbf{x}_0, \mathbf{x}_1)$ is known as a claw,

[3] Improving the security from the subexponential hardness of LWE assumption to polynomial hardness of LWE assumption.

hence the name is claw-free. This useful cryptographic tool constructed based on the LWE assumption plays a crucial role in quantum-classical interactive proof systems, especially in constraining, describing, and verifying the behavior of untrusted quantum devices. Inspired by these works, LWE-based NTCFs have been applied to many intriguing quantum cryptographic schemes, such as remote state preparation [GV19,GMP23], tests of quantumness [BKVV20,BGKM$^+$23], quantum money [RS19,Shm22], secure quantum extraction [ALP20], public-key deniable encryption [CGV22], quantum copy-protection [CHV23], quantum certified deletion [HMNY21], secure key leasing [AKN$^+$23,APV23,CHV23,MPY23], and secure software leasing [KNY21], etc.

More importantly, the security of LWE-based NTCF requires a very important property – the adaptive hardcore bit (AHB) property, which is widely used in constructing the above cryptographic schemes. The AHB property states that whenever $f_0(\mathbf{x}_0) = f_1(\mathbf{x}_1)$, it is difficult to hold both single preimage $(b, \mathbf{x}_b)$, as well as a random $\mathbf{d}$ and a bit c such that $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) \bmod 2$. So far, The LWE-based NTCF in [BCM$^+$18,Mah18b] is the only known TCF instance with AHB property, but its security is based on LWE with superpolynomial modulus. In this work, we will consider a noticeable version of NTCF with AHB property that only requires a polynomially large modulus.

Secure key leasing/revocable cryptography The notion of secure key leasing (SKL) or key-revocable cryptography is inspired by secure software leasing in [ALP21]. Secure key leasing can be viewed as secure software leasing for decryption algorithms but with stronger security guarantees that the adversary is not restricted from running the software honestly after it is returned. Similar to quantum copy protection schemes, the core idea of SKL is to encode the secret key into a quantum state to prevent it from being copied based on the no-cloning principle. Recently, a couple of works have built PKE-SKL (or called key-revocable PKE) and DSIG-SKL from lattices.

In [AKN$^+$23], Agrawal et al proposed the notion of public key encryption with secure key leasing. In [APV23], Ananth et al concurrently introduced the same concept of key-revocable public key encryption. In these two works, key-revocable PKE schemes are constructed based on standard LWE assumption[APV23] or even the mere existence of any PKE scheme [AKN$^+$23]. Independently, for the digital signature primitive, Morimae et al [MPY23] studied the notions of digital signature with revocable signing keys and digital signature with revocable signatures, assuming the sub-exponential hardness of LWE.

However, the above PKE-SKL works require both the user and the server to possess quantum capabilities and utilize quantum communication. Thus, an interesting question is whether it is possible to transform their schemes into one with classical user and classical communication. To solve this problem and further reduce quantum resources, Chardouvelis et al [CGJL23] introduced a semi-quantum PKE-SKL scheme in which the user is classical and interacts solely through a classical communication with the quantum server. However, as the construction of this scheme heavily relies on the trapdoor claw-free functions

with AHB property introduced in [BCM+18], the security of the scheme still depends on the sub-exponential time hardness of LWE assumption, necessitating a sub-exponentially large modulus.

To date, all previous works that imply PKE-SKL are designed to achieve quantum/semi-quantum key-revocable cryptography and almost rely on the sub-exponential hardness of LWE. In this paper, inspired by the work of Chardouvelis et al [CGJL23], our goal is to achieve a PKE-SKL scheme that requires only minimal quantum capabilities (only with classical communication), more desirably from the polynomial hardness of LWE assumption.

NTCF-based proofs of quantumness. A cryptographic proof of quantumness is an interactive protocol that enables classical verifiers to determine whether provers (potentially quantum) is non-classical. To achieve this, [BCM+18] introduced the first groundbreaking proof of quantumness system. This scheme is constructed based on LWE-based NTCF, and its soundness is guaranteed by the adaptive hardcore bit (AHB) property of NTCF. However, a major drawback of this scheme is that the AHB property must rely on the sub-exponential hardness of LWE, requiring the modulus of the scheme to be superpolynomially large. Since then, many methods have been proposed to further simplify NTCF-based proof systems by circumventing the AHB property. For example, [BKVV20] introduced a simple proof of quantumness scheme based on a random oracle model, assuming only the existence of trapdoor claw-free functions. [YZ22] demonstrated a non-interactive quantumness test in the random oracle model. Furthermore, other schemes [KMCVY22,KLVY23,BGKM+23] incorporate NTCF with Bell's inequality to get rid of dependence on AHB property.

In this work, to avoid relying on the random oracle model or Bell's inequality, we aim to achieve the AHB property solely based on the polynomial hardness of LWE. This approach will fundamentally and directly enhance the efficiency of the protocol described in [BCM+18]. To the best of our knowledge, no prior research has accomplished this.

1.3 Organization

The remainder of the paper is organized as follows. In Section 2 we give the technical overview for our main results. In Section 3 we provide cryptographic preliminaries used throughout this work. In Section 4 we formalize our definition of noticeable noisy trapdoor claw-free family (NNTCF) and show that its construction can be built from standard LWE assumption with polynomial modulus. Furthermore, we prove our NNTCF still satisfies the adaptive hardcore bit (AHB) property. In Section 5, we describe the construction of the NNTCF-based PKE-SKL scheme, assuming the polynomial hardness of LWE with polynomial modulus. In Section C.4, we give the security analysis for our SKL-PKE scheme. In Section 6, we describe the construction of the NNTCF-based proof of quantumness scheme, assuming the polynomial hardness of LWE.

2 Technical Overview

In this section, we will provide a technical overview of our works described in Fig. 1. We first slightly extend the original NTCF from [BCM+18] to define our noticeable NTCF (NNTCF) in subsection 2.1. Notably, our NNTCF family with adaptive hardcore bit property can be built upon LWE with polynomial modulus. In subsection 2.2, we will explain how the NNTCF primitive can be used to optimize the PKE-SKL scheme in [CGJL23] such that its ciphertexts' modulus q can be reduced to polynomial size and the security is based on the LWE with polynomial modulus. Finally, in subsection 2.3, we will present the main idea of constructing a new proof of quantumness protocol based on our NNTCF. In particular, our scheme is solely based on LWE with polynomial modulus and does not need to rely on random oracle model [BKVV20] or Bell's inequality [KMCVY22,KLVY23,BGKM+23].

Throughout this section, we will try to be consistent with prior works about the notation of parameters for easier comparison and comprehension.

2.1 Noticeable NTCF from Polynomial Hardness of LWE

Before explaining this approach, we need to recall how the LWE can be employed to construct a NTCF in [BCM+18] and why this original LWE-based NTCF requires a superpolynomial-sized modulus.

Recap: LWE-based NTCF and its two superpolynomial gaps. Given function $f_{k,b}(\mathbf{x}) = \mathbf{A}\mathbf{x} + \mathbf{e} + b \cdot \mathbf{A}\mathbf{s}$ defined with standard LWE samples $k = (\mathbf{A}, \mathbf{t} = \mathbf{A}\mathbf{s} + \mathbf{e}_0) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$, a NTCF can be informally defined by $f'_{k,b}(\mathbf{x}) = \mathbf{A}\mathbf{x} + \mathbf{e} + b \cdot (\mathbf{A}\mathbf{s} + \mathbf{e}_0)$ for $b \in \{0, 1\}$. We can see that if $\mathbf{e}_0$ were 0, $f'_{k,b}(\mathbf{x})$ is the same as $f_{k,b}(\mathbf{x})$, such that $f_{k,1}(\mathbf{x}) = f_{k,0}(\mathbf{x} + \mathbf{s})$. But in fact, $\mathbf{e}_0$ really won't be 0. In this case, to ensure that $f'_{k,1}(\mathbf{x})$ and $f'_{k,0}(\mathbf{x} + \mathbf{s})$ still appear to be the same, we must strictly constrain the norm of $\mathbf{e}$. Typically, we can sample $\mathbf{e}$ from a Gaussian distribution with width superpolynomially larger than the Gaussian distributed noise $\mathbf{e}_0$, implying that $f'_{k,1}(\mathbf{x})$ is statistically close to $f'_{k,0}(\mathbf{x} + \mathbf{s})$.

Specifically, if $\mathbf{e}_0 \hookleftarrow D_{\mathbb{Z}_q^m, B_V}$, $\mathbf{e} \hookleftarrow D_{\mathbb{Z}_q^m, B_P}$ and B_P/B_V is superpolynomial in security parameter λ, the Hellinger statistical distance between $f'_{k,b}(\mathbf{x})$ and $f_{k,b}(\mathbf{x})$, $1 - \exp(-2\pi m B_V/B_P)$, can be bounded by $1 - \mathsf{negl}(\lambda)$. Therefore, $\mathbf{e}$ can be viewed as a flooding noise for $\mathbf{e}_0$, which incurs the first superpolynomial gap B_P/B_V.

Next, we explain the second superpolynomial gap B_V/B_L. This gap is incurred by noise flooding used to ensure the adaptive hardcore bit (AHB) property of NTCF, which is briefly introduced below. Given a description of a NTCF described as above, a quantum device can easily set up a claw superposition as $\frac{1}{\sqrt{2}}(|0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle)$ by creating the state $\sum_{b,\mathbf{x}} |b\rangle |\mathbf{x}\rangle |f'_{k,b}(\mathbf{x})\rangle$ and measuring the last register, where $f'_{k,0}(\mathbf{x}_0) = f'_{k,1}(\mathbf{x}_1)$ and $\mathbf{x}_1 = \mathbf{x}_0 - \mathbf{s} \bmod q$. For the generated state $\frac{1}{\sqrt{2}}(|0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle)$, performing a computational basis measurement will yield a preimage $(b, \mathbf{x}_b) \in \{0, 1\} \times \mathbb{Z}_q^n$. On the other hand, performing a

Hadamard basis measurement will yield a pair $(c, \mathbf{d}) \in \{0,1\} \times \{0,1\}^{n \log q}$ such that $\mathbf{d}$ is uniform random and $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) \mod 2$ [4].

The AHB property asserts that it is not possible to simultaneously obtain both $(b, \mathbf{x}_b)$ and $(c, \mathbf{d})$ under the LWE assumption. From the Lemma 2, Brakerski et al. have proven that if $(b, \mathbf{x}_b, c, \mathbf{d})$ are given, there exists an efficiently computable function $I_{b,\mathbf{x}_b}(\mathbf{d})$ for random $\mathbf{d}$ can compute a string $\widehat{\mathbf{d}}$ such that $\mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) = \widehat{\mathbf{d}}^\top \cdot \mathbf{s}$, where $\widehat{\mathbf{d}} \in \{0,1\}^n \setminus \{0^n\}$ and $\mathbf{s} \in \{0,1\}^n$. Thus, the AHB property can be reformulated as stating that it is hard to produce a pair $(c, \widehat{\mathbf{d}})$ such that $c = \widehat{\mathbf{d}}^\top \cdot \mathbf{s} \bmod 2$. In other words, the AHB property holds if the distribution $\widehat{\mathbf{d}}^\top \cdot \mathbf{s} \bmod 2$ is statistically close to a uniformly random bit, where $\widehat{\mathbf{d}}$ is conditioned on LWE sample.

To prove this, [BCM+18] used the leakage resilience of LWE: Given an LWE instance, any given bit of $\mathbf{s}$ is computationally indistinguishable from a uniformly random bit. This approach replaces the matrix $\mathbf{A}$ with a computationally indistinguishable lossy matrix $\tilde{\mathbf{A}} = \mathbf{BC} + \mathbf{F} \leftarrow \text{LOSSY}(1^n, 1^m, 1^\ell, q, D_{\mathbb{Z}_q, L})$, where $\mathbf{C} \in \mathbb{Z}_q^{\ell \times n}$ has a large kernel and $\mathbf{F} \hookleftarrow D_{\mathbb{Z}_q^{m \times n}, B_L}$ is small. Now, the LWE instance $(\mathbf{A}, \mathbf{As} + \mathbf{e}_0)$ is replaced by $(\mathbf{BC} + \mathbf{F}, \mathbf{BCs} + \mathbf{Fs} + \mathbf{e}_0)$. As we know, the choice of $\widehat{\mathbf{d}}$ indeed depends upon the LWE sample, which corresponds in the leakage resilience argument to $\widehat{\mathbf{d}}$ depending on $\mathbf{Cs}$. Thus, the core proof of AHB property is to argue that given a sample of the form $(\mathbf{BC} + \mathbf{F}, \mathbf{BCs} + \mathbf{Fs} + \mathbf{e}_0)$, for any fixed $\widehat{\mathbf{d}}$, the distribution $\widehat{\mathbf{d}}^\top \cdot \mathbf{s} \bmod 2$ is still statistically close to uniform distribution with overwhelming probability. In other words, we need to show for any fixed $\widehat{\mathbf{d}}$ and $\mathbf{C}$, the joint distribution $(\mathbf{Cs}, \widehat{\mathbf{d}} \cdot \mathbf{s} \mod 2)$ is statistically close to uniform.

To achieve this, their solution relies on $\mathbf{s}$ being a computationally random binary vector, but now the $\mathbf{s}$ is subject to $\mathbf{Fs}$ information leakage. To solve this, they choose $\mathbf{e}_0$ from a Gaussian distribution with a width sufficiently larger than Gaussian distributed noise $\mathbf{F}$ (i.e., B_V/B_L also be superpolynomial). Since $\mathbf{e}_0 \hookleftarrow D_{\mathbb{Z}^m, B_V}$ and $\|\mathbf{Fs}\| \leq nB_L\sqrt{m}$, this ensures that $\mathbf{e}_0$ statistically "floods" the term $\mathbf{Fs}$. Then, this noise flooding technology could efficiently ensure that $(\mathbf{Cs}, \widehat{\mathbf{d}}^\top \cdot \mathbf{s} \bmod 2)$ is statistically close to uniform.

Noticeable NTCF from polynomial LWE assumption. To circumvent the above two superpolynomial flooding noises, we develop a family of noticeable NTCF (NNTCF) endowed with the AHB property from the hardness of standard LWE. The formal definition and construction are described in Section 4. Below we elaborate on the high-level idea of reducing B_P/B_V and B_V/B_L to polynomial size, respectively.

- *Circumvent superpolynomial B_P/B_V*: We introduce the concept of a noticeable version of NTCF (NNTCF). Intuitively, "noticeable" here means

[4] In fact, the bit c is evaluated by $c = \mathbf{d}^\top \cdot (\mathcal{J}(\mathbf{x}_0) \oplus \mathcal{J}(\mathbf{x}_1))$ in [BCM+18], where $\mathcal{J}(\cdot)$ is the binary representation function. For simplicity, we omit this function in the expression.

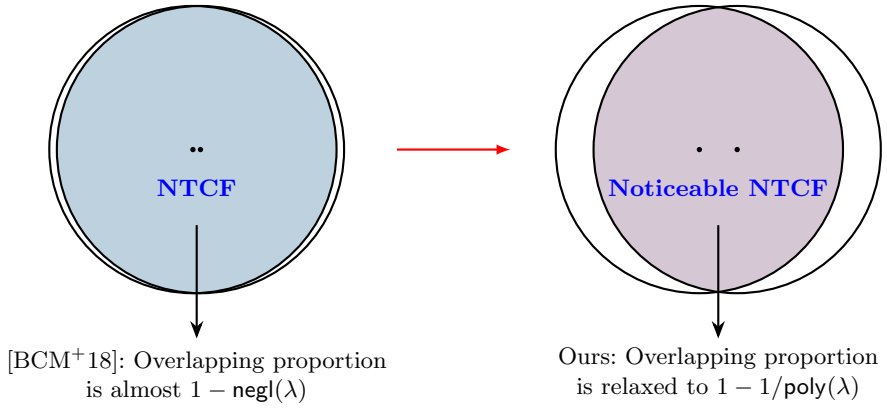

Fig. 2. Schematic representation of noticeable NTCF from original NTCF. The term "noticeable NTCF" emphasizes that the distance we consider is not negligible but noticeable (inverse polynomially small).

that we can slightly relax the statistical distance between the two distributions, $f'_{k,1}(\mathbf{x})$ and $f_{k,1}(\mathbf{x})$, in the NTCF. Specifically, we relax the Hellinger distance between $f'_{k,1}(\mathbf{x})$ and $f_{k,1}(\mathbf{x})$ from $\mathsf{negl}(\lambda)$ to $1/\mathsf{poly}(\lambda)$, as shown in Fig. 2. This relaxation allows us to naturally reduce B_P/B_V to a polynomial size. In fact, this relaxation has already been implicitly used in [BKVV20] to simplify the proof of quantumness. Here, we decide to explicitly define this concept to emphasize that the statistical distance between the two aforementioned distributions is not necessarily negligible.

– *Circumvent superpolynomial B_V/B_L*: We illustrate the high-level idea in Fig. 3. To ensure that distribution $(\mathbf{Cs}, \widehat{\mathbf{d}}^\top \cdot \mathbf{s} \bmod 2)$ is statistically close to the uniform distribution $U(\mathbb{Z}_q^l \times \mathbb{Z}_2)$, [BCM+18] uses the superpolynomial flooding noise $\mathbf{e}_0$ hides the term $\mathbf{Fs}$. This method is very straightforward, however, we observe that it is not necessary to completely hide the $\mathbf{Fs}$ information, but only to obscure the $\mathbf{s}$ information well. Intuitively, there is no need to hide $\mathbf{s}$ perfectly. We argue that if there is sufficiently high entropy left in $\mathbf{s}$, then the argument $(\mathbf{Cs}, \widehat{\mathbf{d}}^\top \cdot \mathbf{s} \bmod 2) \approx_s U(\mathbb{Z}_q^l \times \mathbb{Z}_2)$ still holds. Specifically, we use the refined flooding technique, also known as the gentle flooding approach in [BD20]. The main solution is to apply refined noise flooding to replace the error $\mathbf{e}_0$ with term $\mathbf{F}\mathbf{e}_0^{(1)} + \mathbf{e}_0^{(2)}$. Refer to [BD20], we set $\mathbf{e}_0^{(1)}$ and $\mathbf{e}_0^{(2)}$ as independent random variables with polynomially large width. Consequently, the term $\mathbf{Fs} + \mathbf{e}_0$ is reformulated as $\mathbf{F}(\mathbf{s} + \mathbf{e}_0^{(1)}) + \mathbf{e}_0^{(2)}$. Building on this, we prove that the AHB property still holds in the NNTCF family. The heart of the proof lies in the fact that we can directly argue that the distribution $(\mathbf{Cs}, \widehat{\mathbf{d}}^\top \cdot \mathbf{s} \bmod 2)$, conditioned on $\mathbf{v} = \mathbf{s} + \mathbf{e}_0^{(1)}$ for any fixed $\mathbf{v}$, is statistically indistinguishable from the uniform distribution $U(\mathbb{Z}_q^l \times \mathbb{Z}_2)$ (See Lemma 6).

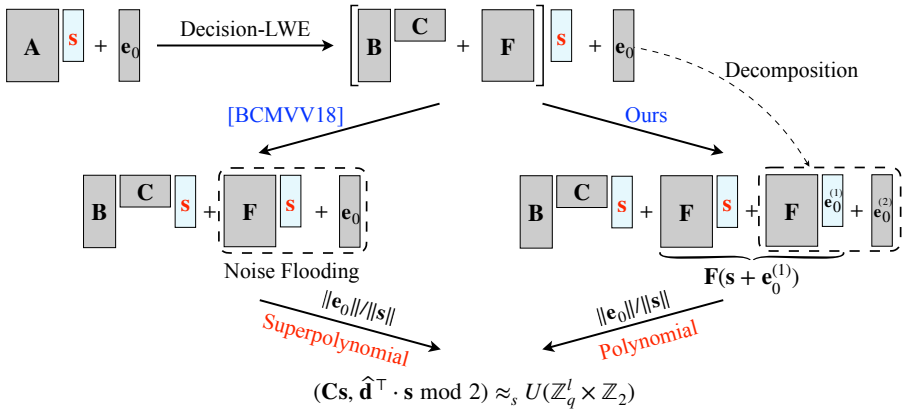

Fig. 3. Summary of circumventing superpolynomial flooding noise in the proof of AHB property of NTCF. $U(\mathbb{Z}_q^l \times \mathbb{Z}_2)$ denotes the density of the uniform distribution over $\mathbb{Z}_q^l \times \mathbb{Z}_2$.

Therefore, both B_P for $\mathbf{e}$ and B_V for $\mathbf{e}_0$ can be polynomially large, thereby ensuring the LWE-based NNTCF only relies on polynomial hardness of LWE assumption.

2.2 Secret Key Leasing for PKE from LWE-based NNTCF

Building on the NNTCF family with AHB property, we show how to construct a PKE-SKL scheme with a polynomial modulus. We first review the PKE-SKL scheme described in [CGJL23] from the LWE-based NTCF with AHB property.

Recap: NTCF-based PKE-SKL in [CGJL23]. Their construction is inspired by the "proof of quantumness" construction in [BCM+18]. To obtain a key leasing scheme, the idea is to use the claw superposition in their construction as a quantum decryption key. We describe (a slightly simplified version of) Chardouvelis's PKE-SKL scheme based on Regev's two-key PKE and LWE-based NTCF, as illustrated in Fig. 4.

The formal scheme is a parallel repetition of the above scheme. Recall the AHB property of NTCF that no quantum polynomial-time adversary can obtain both $(b, \mathbf{x}_b)$ and $(c, \mathbf{d})$. This property will guarantee the security of the PKE-SKL scheme of Fig. 4, i.e., any adversary cannot both provide a valid classical deletion certificate and distinguish ciphertexts (the latter corresponds to the ability to extract $\mathbf{x}_b$).

Now, we explain why the PKE-SKL construction in Fig. 4 requires a superpolynomial modulus. The primary reason is the presence of four superpolynomial gaps: all ratios B_V/B_L, B_P/B_V, $B_{P'}/B_P$, B_X/B_S need to be superpolynomial in λ. The first two superpolynomial gaps B_V/B_L, B_P/B_V are caused by LWE-based NTCF with AHB property, which has been explained in Section 2.1.

Fig. 4. Core subroutine of PKE-SKL in [CGJL23]

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{sk})$:
  - Generate a NTCF pair $k = (\mathbf{A}, \mathbf{t} = \mathbf{A}\mathbf{s} + \mathbf{e}_0)$ where $\mathbf{s} \xleftarrow{\$} [B_s]^n$ and $\mathbf{e}_0 \hookleftarrow D_{\mathbb{Z}_q^m, B_V}$, along with a trapdoor td, send just the k.
  - Output the master public-key and the trapdoor as $(\mathsf{mpk}, \mathsf{sk}) = (k, \mathsf{td})$.
- $\mathsf{KeyGen}(\mathsf{mpk}) \to (\rho_{\mathsf{sk}}, \mathsf{pk})$:
  - Create a state $|\psi\rangle = \sum_{b,\mathbf{x}} |b\rangle\,|\mathbf{x}\rangle\,|f'_{k,b}(\mathbf{x})\rangle$. Measure the last register.
  - Obtain an image $\mathbf{y}$, where $\mathbf{y} = \mathbf{A}\mathbf{x}_b + \mathbf{e} + b\mathbf{t}$, $\mathbf{e} \hookleftarrow D_{\mathbb{Z}_q^m, B_P}, \mathbf{x}_b \in [B_X]^n$. Generate a claw state: $|\phi\rangle = \frac{1}{\sqrt{2}} \sum_{b\in\{0,1\}} |b, \mathbf{x}_b\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|\mathbf{x}_0\rangle + |1\rangle\,|\mathbf{x}_1\rangle)$.
  - Output public key $\mathsf{pk} = \{k, \mathbf{y}\}$ and quantum decryption key $\rho_{\mathsf{sk}} = |\phi\rangle$.
- $\mathsf{Enc}(\mathsf{pk}, \mu) \to \mathsf{ct}$: For a message $\mu \in \{0, 1\}$:
  - Sample a binary random vector $\mathbf{r} \in \mathbb{Z}_q^{m\times 1}$ and computes $\mathsf{ct}_1 = \mathbf{r}^\top\mathbf{A}$, $\mathsf{ct}_2 = \mathbf{r}^\top\mathbf{t}$ and $\mathsf{ct}_3 = \mathbf{r}^\top\mathbf{y} + \mathbf{e}' + \mu \cdot \lceil q/2 \rceil$, where $\mathbf{e}' \hookleftarrow D_{\mathbb{Z}_q^m, B_{P'}}$.
  - Let $\mathsf{ct} := (\mathsf{ct}_1, \mathsf{ct}_2, \mathsf{ct}_3)$ and output ciphertext ct.
- $\mathsf{Dec}(\rho_{\mathsf{sk}}, \mathsf{ct}) \to (\mu, \rho_{\mathsf{sk}})$:
  - Coherently compute $\mathsf{ct}_3 - \mathsf{ct}_1 \cdot \mathbf{x}_b - b \cdot \mathsf{ct}_2$ on the ancilla register, obtain $|\phi\rangle \otimes |\mathsf{ct}_3 - \mathsf{ct}_1 \cdot \mathbf{x}_b - b \cdot \mathsf{ct}_2\rangle \approx |\phi\rangle \otimes |\mu \cdot q/2\rangle$.
  - Measure the last register, return $\mu = 0$ if the outcome is less than $q/4$; Return $\mu = 1$ otherwise. The ρ_{sk} in the first register remains intact.
- $\mathsf{Del}(\rho_{\mathsf{sk}}) \to \mathsf{cert}$:
  - Take in the decryption key $|\phi\rangle$, measure it in the Hadamard basis, resulting in $\mathsf{cert} = (c, \mathbf{d})$ as the deletion certificate.
- $\mathsf{VerDel}(\mathsf{sk}, \mathsf{pk}, \mathsf{cert}) \to \top/\bot$:
  - Use td to compute claw $(\mathbf{x}_0, \mathbf{x}_1)$. Check if $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) \bmod 2$ holds.
  - If this check passes, output $\top$; Otherwise output $\bot$.

The $B_{P'}/B_P$ must be superpolynomial because the ct_3 in ciphertext needs a flooding noise $\mathbf{e}' \hookleftarrow D_{\mathbb{Z}_q^m, B_{P'}}$ to flood the term $\mathbf{r}^\top\mathbf{e}$. In the PKE-SKL security game (refer to Supplementary Materials C), the $\mathbf{y} = \mathbf{A}\mathbf{x}_0 + \mathbf{e}$ is given by the adversary who plays the role of the user, hence $\mathbf{e}$ can be related to $\mathbf{A}$. Therefore we cannot apply a general leftover hash lemma directly to $\mathbf{r}^\top\mathbf{A}$ conditioned on $\mathbf{r}^\top\mathbf{e}$. To make $\mathbf{r}^\top\mathbf{A}$ independently random, they use smudging noise $\mathbf{e}'$ with superpolynomially larger width $B_{P'} \gg B_P$ to flood the term $\mathbf{r}^\top\mathbf{e}$, thereby ensuring $\mathbf{r}^\top\mathbf{A}$ to be independently random under the entropy of $\mathbf{r}$. This is crucial for the (quantum) extractor to work given a (quantum) distinguisher for distinguishing encryptions of 0 and 1. Due to the AHB property, the successful construction of such an extractor will ensure that any lessee can not decrypt anymore after submitting a deletion certificate, which proves the PKE-SKL security.

Finally, regarding B_X, it is required to be either superpolynomially larger than B_S or equal to modulus q. This condition is to ensure that the two distributions $U([B_X])$ and $U([B_X] + B_S)$ are statistically close, which is crucial for ensuring correct generation of claw superposition as $\frac{1}{\sqrt{2}}(|0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle)$. Later, when we resolve all three primary gaps B_V/B_L, B_P/B_V and $B_{P'}/B_P$, the mod-

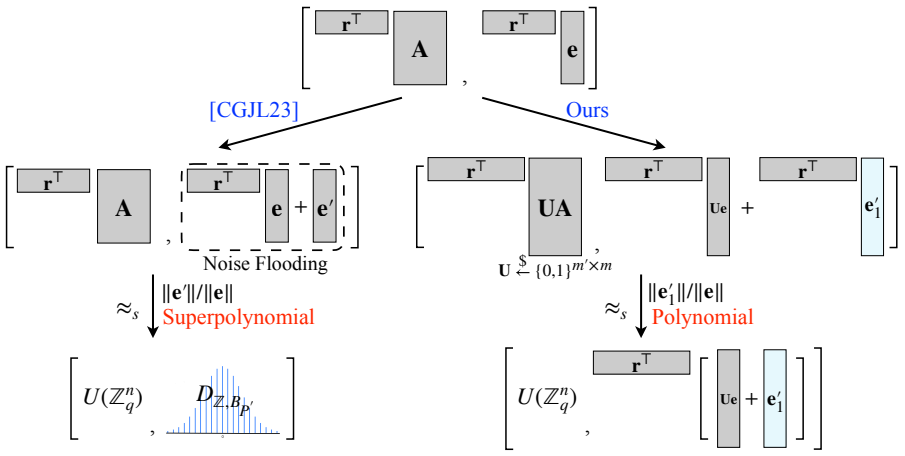

Fig. 5. Summary of circumventing superpolynomial $B_{P'}/B_P$. $U(\mathbb{Z}_q^n)$ denotes the density of the uniform distribution over $\mathbb{Z}_q^n$.

ulus can then be reduced to be polynomial-size. As a result, we can set $B_X{=}q$ and the gap B_X/B_S also becomes polynomial.

Therefore, to achieve polynomial-size modulus in the PKE-SKL [CGJL23], it suffices to address the three gaps: B_V/B_L, B_P/B_V and $B_{P'}/B_P$.

Solving superpolynomial gaps in NTCF-based PKE-SKL. Below, we provide high-level ideas for circumventing these gaps.

- *The gaps B_V/B_L and B_P/B_V*: Firstly, we can replace the NTCF with the NNTCF family described in Section 2.1, thereby immediately avoiding two superpolynomial gaps B_V/B_L, B_P/B_V. The security of PKE-SKL will then be based on the AHB property of our NNTCF.
- *The gap $B_{P'}/B_P$*: Intuitively, to make $\mathbf{r}^\top\mathbf{A}$ independently random, it is not necessary to completely hide the $\mathbf{r}^\top\mathbf{e}$ information, but only to obscure the $\mathbf{r}$ well. Furthermore, there is no need to statistically hide $\mathbf{r}$, we only need to properly hide enough information in $\mathbf{r}$ to ensure that $\mathbf{r}^\top\mathbf{A}$ appears independently random, as shown in Fig. 5.
  In order to remove the superpolynomially large $\mathbf{e}'$, our key idea is to perturb $\mathbf{e}$ with another vector $\mathbf{e}_1 \in [-\|\mathbf{e}\|_\infty, \|\mathbf{e}\|_\infty]^m$ before its product with $\mathbf{r}$. The hope is that many entries of $\mathbf{e}{+}\mathbf{e}_1$ indexed by some set $\mathcal{Z}$ will become 0's after the random perturbation. As explained before, the $\mathbf{e}$ can be related to $\mathbf{A}$. Therefore, it is crucial to argue that the set $\mathcal{Z}$ is random and independent from $\mathbf{e}$, in which case the remaining entropy of $\mathbf{r}$ given $\mathbf{r}^\top(\mathbf{e}{+}\mathbf{e}_1)$ is sufficient to make $\mathbf{r}^\top\mathbf{A}$ independently random.
  Unfortunately, the length of $\mathbf{e}$ is smaller than the infinity norm of $\mathbf{e}$, so we cannot expect a high probability that $\mathbf{e}{+}\mathbf{e}_1$ has many 0's. To address this, we need to modify the scheme such that the public key contains more samples.

We apply a standard technique that can help increase the number of samples (i.e., $m' > m$), but will also slightly increase the error size. Concretely, we select $\mathbf{U} \xleftarrow{\$} \{0,1\}^{m' \times m}$ and derive more samples $(\mathbf{A}', \mathbf{y}')$ with the same secret $\mathbf{x}_0$, where $\mathbf{A}' = \mathbf{U}\mathbf{A}$ and $\mathbf{y}' = \mathbf{U}\mathbf{y} = \mathbf{U}(\mathbf{A}\mathbf{x}_0 + \mathbf{e}) = \mathbf{A}'\mathbf{x}_0 + \mathbf{U}\mathbf{e}$. We let $\mathbf{e}'' = \mathbf{U}\mathbf{e}$ denote the new error. Now we can guess $\mathbf{e}''$ with $\mathbf{e}'_1$ from $[-\|\mathbf{e}''\|_\infty, \|\mathbf{e}''\|_\infty]^{m'}$ of a larger length. For an appropriate choice of m', we can ensure that $\mathbf{e}'' + \mathbf{e}'_1$ has sufficiently many 0's. Under this condition, sufficient randomness in $\mathbf{r}$ will be preserved, which allows us to argue that $\mathbf{r}^\top \mathbf{A}'$ is independently random.

Next, we discuss why the decryption functionality and security of the PKE-SKL scheme can still be maintained when switching from NTCF to NNTCF.

Decryption functionality. For the ciphertext in the PKE-SKL scheme, the correctness of decryption depends on the quantum decryption key ρ_{sk}. As we know, in the NTCF-based PKE-SKL scheme, the decryption key ρ_{sk} is the uniform claw superposition $\frac{1}{\sqrt{2}}(|0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle)$ quantumly generated by the NTCF.

When we switch from NTCF to NNTCF, the generated claw state may exhibit slight variations. In NNTCF, we relax the Hellinger distance between distributions $f'_{k,b}(\mathbf{x})$ and $f_{k,b}(\mathbf{x})$ from $1 - \mathsf{negl}(\lambda)$ to $1 - 1/\mathsf{poly}(\lambda)$. In this case, once the quantum device measures the last register of state $\sum_{b,\mathbf{x}} |b\rangle |\mathbf{x}\rangle |f'_{k,b}(\mathbf{x})\rangle$, the first two registers will not always produce a uniform claw superposition.

However, we must point out that even if the generated claw state is not a perfect uniform superposition of $(\mathbf{x}_0, \mathbf{x}_1)$, the state can still successfully decrypt with a probability of $1 - \mathsf{negl}(\lambda)$. This is because the decryption operation $\rho_{sk} \otimes |\mathsf{ct}_3 - \mathsf{ct}_1 \cdot \mathbf{x}_b + b \cdot \mathsf{ct}_2\rangle$ is performed coherently. As long as the claw state generated by the NNTCF is still over the two preimages $(0, \mathbf{x}_0)$ and $(1, \mathbf{x}_1)$, regardless of whether their amplitudes differ from $1/\sqrt{2}$, decryption will be successful.

Key leasing security. The core of key leasing security is to ensure that the lessee cannot perform decryption after deleting the quantum decryption state ρ_{sk}. The deletion operation requires the lessee to perform a Hadamard measurement on ρ_{sk} to produce a valid deletion certificate $(c, \mathbf{d})$ such that $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) \bmod 2$. Since the decryption capability corresponds to obtaining the information $(b, \mathbf{x}_b)$, the security of PKE-SKL will ultimately be guaranteed by the AHB security property of the NTCF. However, as shown in [CGJL23], a single valid deletion certificate is insufficient. For example, the adversary can forge a certificate $(c, \mathbf{d})$ by randomly picking $\mathbf{d}$ and c. Therefore with $1/2$ probability, the adversary can produce a valid certificate. In this case, the adversary does not need to run a Hadamard measurement on its state and can continue to decrypt ciphertext successfully. Therefore, the security of key leasing needs to be further amplified through a parallel repetition mechanism.

In the parallel repeated NTCF-based PKE-SKL scheme, the lessor is required to prepare many (say, N) independent LWE instances $\{k_i = (\mathbf{A}_i, \mathbf{t}_i = \mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i})\}_{i \in [N]}$. Correspondingly, the lessee generates its public key $\mathsf{pk} =$

$\{k_i, \mathbf{y}_i\}_{i\in N}$ and secret key $\rho_{\mathsf{sk}} = \otimes_{i=1}^{N}\rho_{\mathsf{sk},i}$, where $\rho_{\mathsf{sk},i} = \frac{1}{\sqrt{2}}\sum_{b_i\in\{0,1\}}|b_i, \mathbf{x}_{i,b_i}\rangle = \frac{1}{\sqrt{2}}(|0, \mathbf{x}_{i,0}\rangle + |1, \mathbf{x}_{i,1}\rangle)$. The deletion certificate now consists of a collection of N responses $\{(c_i, \mathbf{d}_i)\}_{i\in[N]}$ certifying the deletion of ρ_{sk}. The ciphertext is revised as $\mathsf{ct} := (\mathbf{ct}_1, \mathbf{ct}_2, \mathbf{ct}_3)$, where $\mathbf{ct}_1 = [\mathbf{r}^\top\mathbf{A}_1, \ldots, \mathbf{r}^\top\mathbf{A}_N]^\top$, $\mathbf{ct}_2 = [\mathbf{r}^\top\mathbf{t}_1, \ldots, \mathbf{r}^\top\mathbf{t}_N]^\top$ and $\mathbf{ct}_3 = \langle\mathbf{r}, \sum_{i=1}^{N}\mathbf{y}_i\rangle + \mathbf{e}' + \mu\cdot\lceil q/2\rceil$. Then, the decryption is performed in a coherent way as

$$\rho_{\mathsf{sk}}\otimes|\mathbf{ct}_3 - [\mathbf{x}_{1,b_1}, \ldots, \mathbf{x}_{N,b_N}]\cdot\mathbf{ct}_1 - [b_1, \ldots, b_N]\cdot\mathbf{ct}_2\rangle \approx \rho_{\mathsf{sk}}\otimes|\mu\cdot\lceil q/2\rceil\rangle\,.$$

Thus the security of the parallel repeated scheme will naturally depend on an amplified AHB property, i.e., the probability that the adversary can simultaneously obtain $\{(c_i, \mathbf{d}_i)\}_{i\in[N]}$ and $\{(b_i, \mathbf{x}_{i,b_i})\}_{i\in[N]}$ can be approximately bounded by 2^{-N}.

As mentioned previously, our main concern now is whether the security previously based on amplified AHB can be ensured if we replace NTCF with NNTCF. On the positive aspect, our NNTCF still enjoys the AHB property under the polynomial hardness of LWE assumption. On the negative side, the claw state generated with our NNTCF will sometimes lead to failure in the verification. In more detail, by using the NNTCF family, the claw state $\rho_{\mathsf{sk},i}$ corresponding to some $\mathbf{y}_i$ may no longer be a uniform superposition state as $\frac{1}{\sqrt{2}}(|0, \mathbf{x}_{i,0}\rangle + |1, \mathbf{x}_{i,1}\rangle)$. For such a non-uniform superposition claw state, performing a Hadamard measurement will no longer produce a valid certificate $(c_i, \mathbf{d}_i)$ that satisfies $c_i = \mathbf{d}_i^\top\cdot(\mathbf{x}_{i,0}\oplus\mathbf{x}_{i,1}) \bmod 2$, thereby causing the certificate verification algorithm to fail. Here, we need to point out that the generation of non-uniform superposition claw states, as described above, does not affect the overall security of our NNTCF-based PKE-SKL scheme.

Intuitively, the Hellinger distance between the distributions $f'_{k,b}(\mathbf{x})$ and $f_{k,b}(\mathbf{x})$ in NNTCF is $1 - 1/\mathsf{poly}(\lambda)$. Although this is not $1 - \mathsf{negl}(\lambda)$, it is still sufficiently close. Therefore, while we cannot generate a uniform superposition claw state with $1 - \mathsf{negl}(\lambda)$ probability every time, in N independent events, we can use the Chernoff bound to ensure that there are at least $0.78N$ valid deletion certificates. We further show that it suffices to verify a major (e.g., the carefully chosen 78%) proportion of the certificate for the security guarantee. Now suppose it requires passing verification of all certificates over a prefixed size-$0.78N$ set of indices i's. Under the amplified AHB, one can claim that the advantage of any adversary passing the verification without losing decryption capability is approximately $2^{-0.78N}$. However, in the real protocol, the adversary is available to choose any size-$0.78N$ set of indices, and there are $\binom{N}{0.78N}$ many choices over a set of N indices. Up to a union bound, the advantage of a successful adversary can still be properly bounded.

2.3 Proof of quantumness from LWE-based NNTCF

In this subsection, we introduce how to use the NNTCF to construct a proof of quantumness protocol based on the polynomial hardness of LWE problem.

Fig. 6. Polynomial-sized proof of quantumness from NNTCF (Simple version)

Repeat the following 1-4 steps N times:

1. $\mathcal{V} \to \mathcal{P}$: Generate a NNTCF pair $k = (\mathbf{A}, \mathbf{As} + \mathbf{e}_0)$, along with a trapdoor td, send just the k.
2. $\mathcal{P} \to \mathcal{V}$: Create the state $|\psi\rangle = \sum_{b,\mathbf{x}} |b\rangle |\mathbf{x}\rangle |f'_{k,b}(\mathbf{x})\rangle$ then measure the last register. Return a string $\mathbf{y}$.
3. $\mathcal{V} \to \mathcal{P}$: Send a uniformly random challenge $r \xleftarrow{\$} \{0,1\}$.
4. $\mathcal{P} \to \mathcal{V}$: Take in r, perform preimage test ($r = 0$) or equation test ($r = 1$):
   - $r = 0$: Perform standard measurement and return proof $\sigma_0 = (b, \mathbf{x}_b)$.
   - $r = 1$: Perform Hadamard measurement and return proof $\sigma_1 = (c, \mathbf{d})$.
5. $\mathcal{V}$: Take in $\{(\mathbf{y}_i, r_i, \sigma_{r,i})\}_{i\in[N]}$, use each td_i to compute $\{(\mathbf{x}_{0,i}, \mathbf{x}_{1,i})\}_{i\in[N]}$. Initialize $\mathsf{count} = 0$. For each proof $\sigma_{r,i}$, perform the following check:
   - If $r = 0$, check the validity of $(b_i, \mathbf{x}_{b_i,i})$; If $r = 1$, check $\mathbf{d}_i$ is non-zero and $c_i = \mathbf{d}_i^\top \cdot (\mathbf{x}_{0,i} \oplus \mathbf{x}_{1,i}) \bmod 2$.
   - If above check passes for $r = 1$, increment the value of count by 1. We let N_1 denote the total number of equation tests. If $N_1 > \frac{1}{4}N$ and the final $\mathsf{count} > 0.75N_1$, output 1, else output $\perp$.

Fix a security parameter λ and a LWE-based NNTCF family. Let $\mathcal{P}$ denote a quantum prover and $\mathcal{V}$ denote a classical verifier. The NNTCF-based proof of quantumness protocol is described in Fig. 6. Our NNTCF-based proof of quantumness protocol can be viewed as a revised version of the works in [BCM+18] and [BKVV20], while the security is solely based on the AHB property of the NNTCF. Compared to [BCM+18], the protocol construction no longer requires a superpolynomial LWE modulus; compared to [BKVV20], the protocol construction no longer requires the random oracle model (ROM).

Quantum completeness. Regarding the preimage test, as long as the claw state generated by the NNTCF is still over the two preimages $(0, \mathbf{x}_0)$ and $(1, \mathbf{x}_1)$ with any amplitude, any one of the two measured values will certainly pass the verification. As shown in Fig. 6, there are almost half of the NNTCF instances devoted to the preimage test instead of the equation test. Therefore, we need to correspondingly adapt the number of valid equation tests such that an honest quantum prover can pass the equation test except with negligible probability. Overall, the probability that the quantum prover can successfully pass the protocol described in Fig. 6 is $1 - \mathsf{negl}(\lambda)$.

Classical soundness. Intuitively, any malicious classical prover will be ruled out as it is required to pass a majority of the equation tests in our protocol. In particular, under the AHB property, conditioned on always passing the preimage test, any classical PPT prover should not be able to subsequently win in the equation test with probability noticeably larger than $\frac{1}{2}$.[5] As a result, the cheating

[5] Refer to Supplementary Materials D.2 for more details.

advantage of any classical PPT adversary to pass a major proportion (say, 75%) of the equation tests should be negligible.

2.4 Open Problems

Our work opens several promising avenues for future research, particularly concerning the NNTCF construction and its potential applications. While we focused primarily on quantum key leasing due to its compatibility with NNTCF, numerous other NTCF-based applications, particularly those involving the adaptive hardcore bit property, could benefit from our findings. We identify significant unexplored directions to extend and generalize our results, which could inspire further advancements in the field. They can be mainly divided into the following three categories.

The first category is about applications based on standard NTCF over classical channels. Within this category, we have successfully improved both the proof of quantumness scheme in [BCM+18] and the key leasing scheme in [CGJL23]. As far as we know, there are more applications within this category such as the certifiable randomness generation protocol [BCM+18] and the semi-quantum money [RS19]. However, these adaptations appear to be more involved and we leave them as future work.

The second category concerns the tasks based on variants of NTCF over classical channels. An example is the quantum delegated computation in [Mah18b], which is based on the extended TCF. It seems more effort would be needed to properly adapt these applications, which can also be interesting for future work.

The last category includes all applications based on (variants of) NTCF that require quantum channels. One example is the revocable quantum digital signature [MPY23]. In this work, to start, we tried to focus on the applications solely over classical channels. However, we believe that the adaptation for this category can be an interesting direction for future research.

3 Preliminaries

3.1 Notions

In this paper, we use λ to denote the security parameter. For positive integer N, let $[N]$ denote the set $\{1, 2, \ldots, N\}$. Let $\mathbb{Z}$ be the set of integers and $\mathbb{N}$ be the set of natural numbers. For any $q \geq 2 \in \mathbb{N}$, we let $\mathbb{Z}_q$ denote the ring of integers modulo q. The vectors are denoted by bold lowercase letters (e.g., $\mathbf{x} \in \mathbb{Z}^n$), matrices by bold uppercase letters (e.g., $\mathbf{A} \in \mathbb{Z}^{m \times n}$). We write $\mathsf{negl}(\lambda)$ for any function $f : \mathbb{N} \to \mathbb{R}_+$ such that for any polynomial p, $\lim_{\lambda \to \infty} p(\lambda) f(\lambda) = 0$. Let $\mathsf{poly}(n)$ be a polynomial in n.

Let $\mathcal{B}(\mathbf{c}, R)$ denote the ball with center $\mathbf{c}$ and radius R. Let the letter D denote a distribution over a finite domain X and f for a density on X, i.e., a function $f : X \to [0, 1]$ s.t. $\sum_{x \in X} f(x) = 1$. $x \leftarrow D$ indicates that x is sampled from the distribution D, and $x \xleftarrow{\$} X$ indicates that x is sampled uniformly from

the set X in random. Let D_X for the set of all densities on X. For any $f \in D_X$, $\textsc{Supp}(f)$ is denoted the support of f, $\textsc{Supp}(f) = \{x \in X | f(x) > 0\}$.

3.2 Lattices and lattice problems

We give some background on lattice in this section. Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\} \subset \mathbb{R}^n$, where $m \leq n$ consist of m linearly independent vectors. The m-dimensional lattice generated by the basis $\mathbf{B}$ is

$$\Lambda = \mathcal{L}(\mathbf{B}) = \{\mathbf{x} = \sum_{i \in [m]} c_i \mathbf{b}_i, c_i \in \mathbb{Z}\}.$$

In the following part, we will introduce discrete Gaussian distribution over a lattice Λ and some properties of discrete Gaussian distribution. For a full-rank, symmetric, positive definite $n \times n$ matrix Σ, we define the n-dimension Gaussian function of deviation parameter $\sqrt{\Sigma}$ as $\rho_{\sqrt{\Sigma}}(\mathbf{x}) = \exp(-\pi \cdot (\mathbf{x})^T \Sigma^{-1}(\mathbf{x}))$, for any $\mathbf{x} \in \mathbb{R}^n$. Particularly, if Σ is a diagonal matrix and each non-zero term equals r^2, Gaussian function can be simplified as $\rho_r(\mathbf{x}) = \exp(-\pi \cdot \|\mathbf{x}\|^2 / r^2)$.

We recall the discrete Gaussian distribution on the integer lattice $\mathbb{Z}^n$.

Definition 1 (Discrete Gaussian Distribution). *For a full-rank, symmetric, positive definite $n \times n$ matrix Σ, we define the n-dimension discrete Gaussian distribution over the lattice $\mathbb{Z}^n$, $D_{\mathbb{Z}^n, \sqrt{\Sigma}}$ of standard deviation parameter matrix $\sqrt{\Sigma}$ by*

$$\forall x \in \mathbb{Z}^n : \quad D_{\mathbb{Z}^n, \sqrt{\Sigma}}(\boldsymbol{x}) = \rho_{\sqrt{\Sigma}}(\boldsymbol{x}) / \rho_{\sqrt{\Sigma}}(\mathbb{Z}^n),$$

where $\rho_{\sqrt{\Sigma}}(\mathbb{Z}^n) = \sum_{\boldsymbol{x} \in \mathbb{Z}^n} \rho_{\sqrt{\Sigma}}(\boldsymbol{x})$.

Now we recall the following lemma about the approximate upper bounds of the vectors selected from discrete Gaussian distribution.

Lemma 1 ([Ban93, Lemma 1.4]). *Let $n \in \mathbb{N}, r > 0$, then it holds that*

1) For any $k > 0$, $Pr[|x| > kr; x \hookleftarrow \mathcal{D}_{\mathbb{Z},r}] \leq 2e^{\frac{-k^2}{2}}$;
2) for any $k > 1$, $Pr[\|\mathbf{x}\| > kr\sqrt{n}; \mathbf{x} \hookleftarrow \mathcal{D}_{\mathbb{Z}^n,r}] < k^n e^{\frac{n}{2}(1-k^2)}$.

We can now define bounded discrete Gaussian distribution.

Definition 2 (Bounded Gaussian Distribution). *For the integer lattice $\mathbb{Z}^n$, the bound B and the derivation parameter r, the bounded discrete Gaussian distribution is defined by:*

$$D_{\mathbb{Z}^n,r,B}(\mathbf{x}) = \begin{cases} \frac{\rho_r(\mathbf{x})}{\sum_{\|\mathbf{x}\| \leq B} \rho_r(\mathbf{x})} & , \text{ if } \|x\| \leq B, \\ 0 & , \text{ otherwise.} \end{cases}$$

Due to the Lemma 1, when $B > r\sqrt{n}$, the bounded discrete Gaussian distribution $D_{\mathbb{Z}^n,r,B}$ is statistically closed to the discrete Gaussian distribution $D_{\mathbb{Z}^n,r}$.

Definition 3 (LWE Problem). *For a security parameter λ, let $n, m, q \in \mathbb{N}$ be integer functions of λ. Let $\chi = \chi(\lambda)$ be a distribution over $\mathbb{Z}$. The $\mathsf{LWE}_{n,m,q,\chi}$ problem is to distinguish between the distributions $(\mathbf{A}, \mathbf{As}+\mathbf{e} \mod q)$ and $(\mathbf{A}, \mathbf{u})$, where $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \chi^m$, and $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^m$. Often we consider the hardness of solving LWE for any function m such that m is at most a polynomial in $n \log q$. This problem is denoted $\mathsf{LWE}_{n,q,\chi}$.*

4 Noticeable Noisy Trapdoor Claw-Free Function Family

In this section, we will describe our construction of a noticeable noisy trapdoor claw-free function (NNTCF) family and prove its properties including the adaptive hardcore bit. We refer the reader to Supplementary Materials B for our proper definition of NNTCF.

4.1 Construction of NNTCF from LWE with polynomial modulus

Our construction of NNTCF is similar to the one in [BCM+18]. Let λ be the security parameter All other parameters are functions of λ as follows: $l = \mathcal{O}(\lambda)$, $n \geq \lambda \cdot l \cdot \lceil \log q \rceil$, $m \geq n \cdot \lceil \log q \rceil$ and $m > 500$, $w = n\lceil \log q \rceil$, $q \geq 8\sigma\sqrt{m}$, and q is a prime, $\sigma_0 \geq n^{\frac{3}{2}}\sqrt{m}$, $150 \cdot m \cdot \sigma_0 \leq \sigma \leq \frac{q}{C_T\sqrt{mn\log q}}$.

Under the above parameters, we describe the noticeable NTCF family $\mathcal{F}_{\mathsf{LWE}}$ based on LWE with polynomial modulus. Let $\mathcal{X} = \mathbb{Z}_q^n$ and $\mathcal{Y} = \mathbb{Z}_q^m$. The key space $\mathcal{K}_{\mathcal{F}_{\mathsf{LWE}}}$ is subset of $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$. For $b \in \{0,1\}$, $x \in \mathcal{X}$ and the key $k = (\mathbf{A}, \mathbf{As} + \mathbf{e}_0)$, the $f_{k,b}(\mathbf{x})$ is given as

$$\forall \mathbf{y} \in \mathcal{Y} : (f_{k,b}(\mathbf{x}))(\mathbf{y}) = D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{y} - \mathbf{Ax} - b \cdot \mathbf{As}), \tag{1}$$

Then we show that each of the properties of NNTCF holds. The first two properties are the same as that of LWE-based NTCF in [BCM+18], while the last two properties differ due to the use of polynomial-size modulus.

Efficient Function Generation. On input the security parameter λ, the procedure $\mathrm{GEN}_{\mathcal{F}_{\mathsf{LWE}}}$ samples a random $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$, together with trapdoor information $\mathbf{T_A}$. This is done using the procedure $\textsc{GenTrap}(1^n, 1^m, q)$ from Theorem 9 in Supplementary Materials A.2. Moreover, the distribution on matrices $\mathbf{A}$ returned by GenTrap is negligibly close to the uniform distribution on $\mathbb{Z}_q^{m\times n}$.

Next, the sampling procedure selects $\mathbf{s} \in \{0,1\}^n$ uniformly at random, and a vector $\mathbf{e}_0 \hookleftarrow D_{\mathbb{Z}^m,\sigma_0,\sigma_0\sqrt{m}}$. $\mathrm{GEN}_{\mathcal{F}_{\mathsf{LWE}}}$ returns $k = (\mathbf{A}, \mathbf{As} + \mathbf{e})$ and $\mathsf{td}_k = \mathbf{T_A}$.

Trapdoor Injective Pair.

(a) *Trapdoor.* For any key $k = (\mathbf{A}, \mathbf{As} + \mathbf{e}_0) \in \mathcal{K}_{\mathcal{F}_{\mathsf{LWE}}}$ and for all $\mathbf{x} \in \mathcal{X}$,

$$\textsc{Supp}(f_{k,0}(\mathbf{x})) = \left\{\mathbf{Ax} + \mathbf{e} \,|\, \|\mathbf{e}\| \leq \sigma\sqrt{m}\right\} , \tag{2}$$

$$\textsc{Supp}(f_{k,1}(\mathbf{x})) = \left\{\mathbf{Ax} + \mathbf{As} + \mathbf{e} \,|\, \|\mathbf{e}\| \leq \sigma\sqrt{m}\right\} . \tag{3}$$

The procedure $\text{INV}_{\mathcal{F}_{\mathsf{LWE}}}$ takes as input the trapdoor $\mathbf{T_A}$, $b \in \{0,1\}$, and $\mathbf{y}' \in \mathcal{Y}$, it uses the algorithm INVERT to determine $\mathbf{x}', \mathbf{e}'$ such that $\mathbf{y}' = \mathbf{A}\mathbf{x}' + \mathbf{e}'$, and returns the element $\mathbf{x}' - b \cdot \mathbf{s} \in \mathcal{X}$. Using Theorem 9, this procedure returns the unique correct outcome provided $\mathbf{y}' = \mathbf{A}\mathbf{x}' + \mathbf{e}'$ for some $\mathbf{e}'$ such that $\|\mathbf{e}'\| \leq \sigma\sqrt{m}$. This condition is satisfied for all $\mathbf{y}' \in \text{SUPP}(f_{k,b}(\mathbf{x}'))$ provided σ is chosen so that $\sigma \leq \frac{q}{C_T\sqrt{mn\log q}}$.

(b) *Injective Pair.* We let $\mathcal{R}_k$ be the set of all pairs $(\mathbf{x}_0, \mathbf{x}_1)$ such that $f_{k,0}(\mathbf{x}_0) = f_{k,1}(\mathbf{x}_1)$. By definition, this occurs if and only if $\mathbf{x}_1 = \mathbf{x}_0 - \mathbf{s} \bmod q$, and so $\mathcal{R}_k$ is a perfect matching.

Efficient Range Superposition. For $k = (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_0) \in \mathcal{K}_{\mathcal{F}_{\mathsf{LWE}}}, b \in \{0,1\}$ and $\mathbf{x} \in \mathcal{X}$, let

$$(f'_{k,b}(\mathbf{x}))(\mathbf{y}) \;=\; D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{y} - \mathbf{A}\mathbf{x} - b \cdot (\mathbf{A}\mathbf{s} + \mathbf{e}_0)) \,. \tag{4}$$

Note that $f'_{k,0}(\mathbf{x}) = f_{k,0}(\mathbf{x})$ for all $\mathbf{x} \in \mathcal{X}$. The distributions $f'_{k,1}(\mathbf{x})$ and $f_{k,1}(\mathbf{x})$ are shifted by $\mathbf{e}_0$. Given the key k and $\mathbf{x} \in \mathcal{X}$, the densities $f'_{k,0}(\mathbf{x})$ and $f'_{k,1}(\mathbf{x})$ are efficiently computable. For all $\mathbf{x} \in \mathcal{X}$,

$$\text{SUPP}(f'_{k,0}(\mathbf{x})) = \text{SUPP}(f_{k,0}(\mathbf{x})) \,, \tag{5}$$

$$\text{SUPP}(f'_{k,1}(\mathbf{x})) = \left\{\mathbf{A}\mathbf{x} + \mathbf{e} + \mathbf{A}\mathbf{s} + \mathbf{e}_0 \mid \|\mathbf{e}\| \leq 2\sigma\sqrt{m}\right\} \,. \tag{6}$$

(a) Using that $\sigma \geq \sigma_0 m$, it follows that the norm of the term $\mathbf{e}_0 + \mathbf{e}$ in Eqn. (6) is always at most $3\sigma\sqrt{m}$. Therefore, the inversion procedure $\text{INV}_{\mathcal{F}_{\mathsf{LWE}}}$ can be guaranteed to return $\mathbf{x}$ on input $\mathbf{T_A}$, $b \in \{0,1\}$, $\mathbf{y} \in \text{SUPP}(f'_{k,b}(x))$ if we strengthen the requirement on σ to $\sigma \leq \frac{q}{2C_T\sqrt{mn\log q}}$. This strengthened trapdoor requirement also implies that for all $b \in \{0,1\}$, $(\mathbf{x}_0, \mathbf{x}_1) \in \mathcal{R}_k$, and $\mathbf{y} \in \text{SUPP}(f'_{k,b}(\mathbf{x}_b)) \bigcap \text{SUPP}(f'_{k,b\oplus 1}(\mathbf{x}_{b\oplus 1}))$, $\text{INV}_{\mathcal{F}_{\mathsf{LWE}}}(t_{\mathbf{A}}, b \oplus 1, \mathbf{y}) = \mathbf{x}_{b\oplus 1}$.

(b) The procedure $\text{CHK}_{\mathcal{F}_{\mathsf{LWE}}}$ is identical to the one in [BCM+18]. On input $k = (\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e}_0)$, $b \in \{0,1\}$, $\mathbf{x} \in \mathcal{X}$, and $\mathbf{y} \in \mathcal{Y}$, if $b = 0$, it computes $\mathbf{e}' = \mathbf{y} - \mathbf{A}\mathbf{x}$. If $\|\mathbf{e}'\| \leq 2\sigma\sqrt{m}$, the procedure returns 1, and 0 otherwise. If $b = 1$, it computes $\mathbf{e}' = \mathbf{y} - \mathbf{A}\mathbf{x} - (\mathbf{A}\mathbf{s} + \mathbf{e}_0)$. If $\|\mathbf{e}'\| \leq 2\sigma\sqrt{m}$, it returns 1, and 0 otherwise.

(c) The procedure $\text{SAMP}_{\mathcal{F}_{\mathsf{LWE}}}$ is identical to the one in [BCM+18]. We bound the Hellinger distance between the densities $f_{k,b}(\mathbf{x})$ and $f'_{k,b}(\mathbf{x})$. If $b = 0$ they are identical. If $b = 1$, both densities are shifts of $D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}$, where the shifts differ by $\mathbf{e}_0$ and $\mathbf{e}_0 \hookleftarrow D_{\mathbb{Z}^m,\sigma_0,\sigma_0\sqrt{m}}$. Applying Lemma 11, it holds that $H^2(f_{k,1}(\mathbf{x}), f'_{k,1}(\mathbf{x})) \leq 1 - e^{\frac{-9\sqrt{m}\|\mathbf{e}_0\|}{4\sigma}}(1 - 2e^{-\frac{1}{2}m}) \leq 1 - e^{\frac{-9m\sigma_0}{4\sigma}}(1 - 2e^{-\frac{1}{2}m}) \leq 1 - e^{-\frac{3}{200}}(1 - 2e^{-\frac{1}{2}m})$. When $m > 500$, $1 - e^{-\frac{3}{200}}(1 - 2e^{-\frac{1}{2}m}) < \frac{1}{50}$. Therefore, the requirement $E_{x \xleftarrow{\$} \mathbb{Z}_q^n}[H^2(f_{k,1}(\mathbf{x}), f'_{k,1}(\mathbf{x}))] \leq \frac{1}{50}$ holds.

Finally, it remains to describe the procedure $\text{SAMP}_{\mathcal{F}_{\mathsf{LWE}}}$. At the first step, the procedure creates the following superposition

$$\sum_{\mathbf{e} \in \mathbb{Z}_q^m} \sqrt{D_{\mathbb{Z}_q^m,\sigma,2\sigma\sqrt{m}}(\mathbf{e})}\,|\mathbf{e}\rangle \;. \tag{7}$$

At the second step, the procedure creates a uniform superposition over $\mathbf{x} \in \mathcal{X}$, yielding the state

$$(2q)^{-\frac{n}{2}} \sum_{\substack{\mathbf{x}\in\mathcal{X} \\ b\in\{0,1\} \\ \mathbf{e}\in\mathbb{Z}_q^m}} \sqrt{D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{e})}\,|b,\mathbf{x}\rangle\,|\mathbf{e}\rangle \ . \tag{8}$$

At the third step, using the key $k = (\mathbf{A}, \mathbf{As}+\mathbf{e})$, the procedure computes

$$\begin{aligned} &(2q)^{-\frac{n}{2}} \sum_{\substack{\mathbf{x}\in\mathcal{X} \\ b\in\{0,1\} \\ \mathbf{e}\in\mathbb{Z}_q^m}} \sqrt{D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{e})}\,|b,\mathbf{x}\rangle\,|\mathbf{Ax}+\mathbf{e}+b\cdot(\mathbf{As}+\mathbf{e}_0)\rangle \\ =&(2q)^{-\frac{n}{2}} \sum_{\substack{\mathbf{x}\in\mathcal{X} \\ b\in\{0,1\} \\ \mathbf{y}\in\textsc{Supp}(f'_{k,b}(\mathbf{x}))}} \sqrt{f'_{k,b}(\mathbf{x})(\mathbf{y})}\,|b,\mathbf{x}\rangle\,|\mathbf{y}\rangle \end{aligned} \tag{9}$$

Adaptive Hardcore Bit. Now we show that our NNTCF family also enjoys the adaptive hardcore bit property. We start by providing some useful statements and lemmata. Recall that $\mathcal{X} = \mathbb{Z}_q^n$ and let $w = n\lceil \log q \rceil$. Let $\mathcal{J} : \mathcal{X} \to \{0,1\}^w$ be such that $\mathcal{J}(\mathbf{x})$ returns the binary representation of $\mathbf{x} \in \mathcal{X}$. For $b \in \{0,1\}$, $\mathbf{x} \in \mathcal{X}$, and $\mathbf{d} \in \{0,1\}^w$, let $I_{b,x}(\mathbf{d}) \in \{0,1\}^n$ be the vector whose each coordinate is obtained by taking the inner product mod 2 of the corresponding block of $\lceil \log q \rceil$ coordinates of $\mathbf{d}$ and of $\mathcal{J}(\mathbf{x}) \oplus \mathcal{J}(\mathbf{x} - (-1)^b\mathbf{1})$, where $\mathbf{1} \in \mathbb{Z}_q^n$ is the vector with all its coordinates equal to $1 \in \mathbb{Z}_q$. There is a useful claim in [BCM+18] that the inner product $\mathbf{d} \cdot \mathcal{J}(\mathbf{x}) \oplus \mathcal{J}(\mathbf{x} - (-1)^b\mathbf{1})$ is exactly equal to $I_{b,\mathbf{x}}(\mathbf{d}) \cdot \mathbf{s}$, which is recalled as follows.

Lemma 2 (Claim 4.5 in [BCM+18]). *For all $b \in \{0,1\}, \mathbf{x} \in \mathcal{X}, \mathbf{d} \in \{0,1\}^w$ and $\mathbf{s} \in \{0,1\}^n$ the following equality holds:*

$$\mathbf{d} \cdot (\mathcal{J}(\mathbf{x}) \oplus \mathcal{J}(\mathbf{x} - (-1)^b\mathbf{s})) \ = \ I_{b,x}(\mathbf{d}) \cdot \mathbf{s} \ . \tag{10}$$

Note that in [BCM+18], the $\mathbf{d}$ is only required to have one non-zero place in the first and second half as each bit of secret $\mathbf{s}$ is computationally indistinguishable from random. In our case, we consider a relaxed condition on $\mathbf{s}$, which then requires the string $\mathbf{d}$ to have more non-zero positions. Therefore, for $k = (\mathbf{A}, \mathbf{As}+\mathbf{e}_0), b \in \{0,1\}$ and $\mathbf{x} \in \mathcal{X}$, we define the set $G_{k,b,x}$ as $G_{k,b,\mathbf{x}} = \left\{\mathbf{d} \in \{0,1\}^w : \mathsf{HW}\left(I_{b,\mathbf{x}}(\mathbf{d})_{\mathcal{I}_b}\right) \geq \frac{n}{8}\right\}$, where $\mathsf{HW}(\cdot)$ represents the Hamming weight and $I_{b,\mathbf{x}}(\mathbf{d})_{\mathcal{I}_b}$ is the concatenation of all the entries indexed by $\mathcal{I}_b$, which satisfies $\mathcal{I}_b = \left\{b\frac{n}{2}, \cdots, b\frac{n}{2}+\frac{n}{2}\right\}$. Besides, we also divide $\mathbf{s} = (\mathbf{s}_0, \mathbf{s}_1)$. Here $\mathbf{s}_0$ is the vector containing the first $\frac{n}{2}$ entries and $\mathbf{s}_1$ contains the last $\frac{n}{2}$ entries. We define $\hat{G}_{\mathbf{s}_1,0,\mathbf{x}_0} = \hat{G}_{\mathbf{s}_0,1,\mathbf{x}_1} = G_{k,0,\mathbf{x}_0} \bigcap G_{k,1,\mathbf{x}_1}$.

Actually, for all $b \in \{0,1\}$ and $\mathbf{x} \in \mathcal{X}$, if $\mathbf{d}$ is sampled uniformly at random, $\mathbf{d} \notin \hat{G}_{\mathbf{s}_{b\oplus 1},b,\mathbf{x}_b}$ with probability $e^{-\frac{n}{32}+1}$. We refer to Lemma 19 in Supplementary Materials B.2 for this result.

First, note that membership in $G_{k,b,x}$ can be verified given only $b, \mathbf{x}$, which is sufficient for Condition (a) of the adaptive hardcore bit property as defined in Definition 11 in Supplementary Materials B.1. Next, we proceed to prove Condition (b) of adaptive hardcore bit. Note that our proof follows the proof structure of the adaptive hardcore bit in [BCM+18], except that our proof is based on LWE with a polynomial-size modulus.

Theorem 4 (Adaptive hardcore bit (Condition 4.(b))). *For m, n, q set the same as section 4.1 and $\sigma_0 \geq n^{\frac{3}{2}}\sqrt{m}$, assume the hardness assumption $\mathsf{LWE}^{m,n}_{q,\sigma_0}$ and $\mathbf{s} \in \{0,1\}^n$, we define two sets:*

$$\begin{aligned} H_{\mathbf{s}} &= \{(b, \mathbf{x}, \mathbf{d}, (\mathbf{d} \cdot (\mathcal{J}(\mathbf{x}) \oplus \mathcal{J}(\mathbf{x} - (-1)^b\mathbf{s})) \bmod 2) | b \in \{0,1\}, \mathbf{x} \in \mathbb{Z}_q^n, \\ &\qquad \mathbf{d} \in \hat{G}_{\mathbf{s}_{b\oplus 1}, b, \mathbf{x}}\}, \\ \overline{H}_{\mathbf{s}} &= \{(b, \mathbf{x}, \mathbf{d}, c) | (b, \mathbf{x}, \mathbf{d}, c \oplus 1) \in H_{\mathbf{s}}\}. \end{aligned}$$

For any quantum polynomial-time algorithm $\mathcal{A} : \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m \to \{0,1\} \times \mathbb{Z}_q^n \times \{0,1\}^{n\lceil log(q)\rceil} \times \{0,1\}$ and the any LWE sample $(\mathbf{A}, \mathbf{As}+\mathbf{e}_0) \hookleftarrow \boldsymbol{Gen}(1^\lambda, \mathbf{s}, m, n)$, the negligible difference always exists:

$$|\Pr[\mathcal{A}(\mathbf{A}, \mathbf{As} + \mathbf{e}_0) \in H_{\mathbf{s}}] - Pr[\mathcal{A}(\mathbf{A}, \mathbf{As} + \mathbf{e}_0) \in \overline{H}_{\mathbf{s}}]| \leq negl(\lambda)$$

Refer to [BCM+18, Section 4.4.1], it suffices to prove the following lemma, which implies the above theorem.

Lemma 3. *Under the hardness assumption $\mathsf{LWE}^{m,n}_{q,\sigma_0,\mathbf{s}}$, $\mathcal{A} : \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m \to \{0,1\} \times \mathbb{Z}_q^n \times \{0,1\}^{n\lceil log(q)\rceil} \times \{0,1\}$ is a quantum polynomial-time algorithm. The following two distributions are computationally indistinguishable:*

$$\begin{aligned} D_0 &= (k = (\mathbf{A}, \mathbf{As} + \mathbf{e}_0), (b, x, \mathbf{d}, c) \leftarrow \mathcal{A}(k), I_{b,\mathbf{x}}(\mathbf{d}) \cdot \mathbf{s} \bmod 2) \\ D_1 &= (k = (\mathbf{A}, \mathbf{As} + \mathbf{e}_0), (b, x, \mathbf{d}, c) \leftarrow \mathcal{A}(k), (\delta_{d\in\hat{G}_{\mathbf{s}_{b\oplus 1}, b, \mathbf{x}}} \cdot r) \oplus (I_{b,\mathbf{x}}(\mathbf{d}) \cdot \mathbf{s} \bmod 2)) \end{aligned}$$

where r is a random bit and $\delta_{d\in\hat{G}_{\mathbf{s}_{b\oplus 1}, b, \mathbf{x}}} = 1$ if $d \in \hat{G}_{\mathbf{s}_{b\oplus 1}, b, \mathbf{x}}$ and 0 otherwise.

Here, we recall some useful notions such as moderate vector and moderate matrix, together with the lemma of the lower bound of the probability for a uniformly selected matrix to be moderate from [BCM+18].

Definition 4. *For a vector $\mathbf{b} \in \mathbb{Z}_q^n$, we say $\mathbf{b}$ is moderate if there are at least $\frac{n}{4}$ entries of $\mathbf{b}$ has absolute value in the range $(\frac{q}{8}, \frac{3q}{8}]$. A matrix $\mathbf{C} \in \mathbb{Z}_q^{l\times n}$ is moderate if every vector in the spanning space of row vectors of $\mathbf{C}$, span($\mathbf{C}$), is moderate.*

Lemma 4 ([BCM+18, Lemma 4.8]). *Let q be prime and l, n be integers. Then*

$$\Pr_{\mathbf{C}\xleftarrow{\$}\mathbb{Z}_q^{m\times n}}[\mathbf{C} \text{ is moderate}] \geq 1 - q^l \cdot 2^{-\frac{n}{8}}.$$

Now suppose $\sigma \geq n$, we present our main lemma as follows.

Lemma 5. *Let $\mathbf{C} \in \mathbb{Z}_q^{l \times n}$ be an arbitrary moderate matrix and $\widehat{\mathbf{d}} \in \{0,1\}^n$ be an arbitrary non-zero binary vector satisfying that its hamming weight is at least $\frac{n}{4}$. Let $\mathbf{s} \xleftarrow{\$} \{0,1\}^n$ and $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^n,\sigma,\sigma\sqrt{n}}$, where $\sigma = n$. Consider the random variables $\mathbf{v} = \mathbf{C}\mathbf{s} \bmod q$ and $z = \langle \widehat{\mathbf{d}}, \mathbf{s} \rangle \bmod 2$ conditioned on $\mathbf{s} + \mathbf{e} = \mathbf{t}$ for any $\mathbf{t}$ fixed. Then statistical distance between the distribution of $(\mathbf{v}, z)$ and the distribution of $U(\mathbb{Z}_q^l \times \mathbb{Z}_2)$ is at most $q^{\frac{l}{2}} \cdot 2^{-\frac{n}{4}}$.*

Proof (Proof of Lemma 5). Let f be the probability density function of $(\mathbf{v}, z)$ and $\widehat{f}$ be the Fourier transform over $\mathbb{Z}_q^l \times \mathbb{Z}_2$. It's clear that $\widehat{f}(\mathbf{0}, 0) = 1$. Let U denote the density of the uniform distribution over $\mathbb{Z}_q^l \times \mathbb{Z}_2$. It's easy to see that $\widehat{U}(\mathbf{0}, 0) = 1$ and $\widehat{U}(\widehat{\mathbf{v}}, \widehat{z}) = 0$ for all $(\widehat{\mathbf{v}}, \widehat{z}) \neq (\mathbf{0}, 0)$. Then we can compute: $\frac{1}{2} \left\| f - U \right\|_1 \leq \sqrt{\frac{q^l}{2}} \left\| f - U \right\|_2 = \frac{1}{2} \left\| \widehat{f} - \widehat{U} \right\|_2 = \frac{1}{2} \left(\sum_{(\widehat{\mathbf{v}}, \widehat{z} \in \mathbb{Z}_q^l \times \mathbb{Z}_2 \setminus (\mathbf{0},0)} \left| \widehat{f}(\widehat{\mathbf{v}}, \widehat{z}) \right|^2 \right)^{1/2}$, where the first inequality follows from the Cauchy-Schwarz inequality and the second line follows from Parseval's identity. Denote $\omega_{2q} = e^{-\frac{2\pi\sqrt{-1}}{2q}}$, then we can write:$\widehat{f}(\widehat{\mathbf{v}}, \widehat{z}) = E_{\mathbf{s}} \left[\omega_{2q}^{(2\widehat{\mathbf{v}}^\intercal \mathbf{C} + q\widehat{z}\widehat{d}^\intercal)\mathbf{s}} \right] = E_{\mathbf{s}} \left[\omega_{2q}^{\mathbf{w}^\intercal \mathbf{s}} \right] = \Pi_{i \in [n]} E_{s_i}[\omega_{2q}^{w_i s_i}]$, where $\mathbf{w}^\intercal = 2 \cdot \widehat{\mathbf{v}}^\intercal \mathbf{C} + q \cdot \widehat{z} \cdot \widehat{\mathbf{d}}^\intercal \in \mathbb{Z}_{2q}^n$. To compute $\widehat{f}(\widehat{\mathbf{v}}, \widehat{z})$, we have:

$$
\begin{aligned}
&\Pr[s_i | e_i + s_i = t_i,\ t_i \text{ fixed},\ s_i \xleftarrow{\$} \{0,1\}, e_i \hookleftarrow D_{\mathbb{Z},\sigma}] \\
=&\frac{\rho_\sigma(t_i - s_i)}{\rho_\sigma(t_i) + \rho_\sigma(t_i - 1)} = \frac{e^{-\pi(-2s_i t_i + s_i^2)/\sigma^2}}{1 + e^{-\pi(-2t_i+1)/\sigma^2}}
\end{aligned}
$$

Therefore,

$$
\Pr[s_i | e_i + s_i = t_i,\ t_i \text{ fixed},\ s_i \xleftarrow{\$} \{0,1\}, e_i \hookleftarrow D_{\mathbb{Z},\sigma}] = \begin{cases} \frac{1}{e^{-\pi(-2t_i+1)/\sigma^2}+1} & , s_i = 0; \\ \frac{e^{-\pi(-2t_i+1)/\sigma^2}}{e^{-\pi(-2t_i+1)/\sigma^2}+1} & , s_i = 1. \end{cases}
$$

For $(\widehat{\mathbf{v}}, \widehat{z}) = (\mathbf{0}, 1)$, $E_{s_i}[\omega_{2q}^{w_i s_i}] = \begin{cases} \frac{1 - e^{-\pi(-2t_i+1)/\sigma^2}}{e^{-\pi(-2t+1)/\sigma^2}+1} & , d_i = 1; \\ 1 & , d_i = 0. \end{cases}$

When $d_i = 1$, $E_{s_i}[\omega_{2q}^{w_i s_i}] \leq \frac{1 - e^{(-2\pi\sigma\sqrt{n} - \pi)/\sigma^2}}{1 + e^{(-2\pi\sigma\sqrt{n} - \pi)/\sigma^2}} \leq \frac{1 - e^{-3\pi/\sqrt{n}}}{1 + e^{-3\pi/\sqrt{n}}} \leq \frac{1}{2}$. Since the hamming weight of $\widehat{\mathbf{d}}$ is at least $\frac{n}{4}$, $\widehat{f}(\mathbf{0}, 1) \leq (\frac{1}{2})^{\frac{n}{4}}$.

For $\widehat{\mathbf{v}} \neq \mathbf{0}$, $E_{s_i}[\omega_{2q}^{w_i s_i}] = 1 - \frac{e^{(2\pi t_i - \pi)/\sigma^2}}{1 + e^{(2\pi t_i - \pi)/\sigma^2}}(1 - e^{2\pi\sqrt{-1} w_i/(2q)})$, and for the second term of the formula above,

$$
\begin{aligned}
&\left| \frac{e^{(2\pi t_i - \pi)/\sigma^2}}{1 + e^{(2\pi t_i - \pi)/\sigma^2}} (1 - e^{2\pi\sqrt{-1} w_i/2q}) \right| \geq \frac{2e^{(2\pi t_i - \pi)/\sigma^2}}{1 + e^{(2\pi t_i - \pi)/\sigma^2}} \left| sin(\frac{\pi w_i}{2q}) \right| \\
\geq &\frac{2e^{(-2\pi\sigma\sqrt{n} - \pi)/\sigma^2}}{1 + e^{(-2\pi\sigma\sqrt{n} - \pi)/\sigma^2}} \left| sin(\frac{\pi w_i}{2q}) \right| \geq 2 \cdot sin(\pi/8),
\end{aligned}
$$

the last inequality exists for at least $\frac{n}{4}$, $i \in [n]$ because $\mathbf{C}$ is moderate. In this case $E_{s_i}(\omega_{2q}^{w_i s_i}) \leq 1-2\cdot sin(\pi/8)$. Hence for $\widehat{\mathbf{v}} \neq \mathbf{0}$, $\widehat{f}(\widehat{\mathbf{v}}, \widehat{z}) \leq (1-2\cdot sin(\pi/8))^{\frac{n}{4}} \leq (\frac{1}{4})^{\frac{n}{4}}$. Therefore, $\Delta(f,U) \leq \frac{1}{2}\sqrt{\left(\frac{1}{2}\right)^{\frac{n}{4}} + 2(q^l-1)\left(\frac{1}{4}\right)^{\frac{n}{4}}} \leq \frac{1}{2}\sqrt{2\cdot q^l \cdot \left(\frac{1}{2}\right)^{\frac{n}{2}}} \leq q^{\frac{l}{2}} 2^{-\frac{n}{4}}$ □

Based on the lemma above, the following lemma can be proved by following the same merit of the proof for [BCM+18, Lemma 4.6]. We provide the lemma below but defer the proof to Supplementary Materials B.2.

Lemma 6. *Let q be a prime, $l, n \geq 1$ integers, and $\mathbf{C} \in \mathbb{Z}_q^{l\times n}$ a uniformly random matrix. With probability at least $1 - q^l \cdot 2^{-\frac{n}{8}}$ over the choice of $\mathbf{C}$ the following holds. For a fixed $\mathbf{C}$, all $\mathbf{v} \in \mathbb{Z}_q^l$ and $\widehat{\mathbf{d}} \in \{0,1\}^n$ with hamming weight larger than $\frac{n}{4}$, the distance of $(\widehat{\mathbf{d}} \cdot \mathbf{s} \bmod 2)$, where $\mathbf{s}$ is uniform in $\{0,1\}^n$ conditioned on $\mathbf{Cs} = \mathbf{v}$ and $\mathbf{s} + \mathbf{e} = \mathbf{t}$ fixed, where $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^n,\sigma,\sigma\sqrt{n}}$ is within statistical distance $\mathcal{O}(q^{\frac{3l}{2}} \cdot 2^{-\frac{n}{4}})$ of the uniform distribution $\{0,1\}$.*

Our idea to circumvent noise flooding in the proof of [BCM+18, Lemma 4.4] is inspired by the Gaussian decomposition technique introduced in [BD20]. In short, to hide $\mathbf{s}$ in $\mathbf{Fs}$, one can decompose $\mathbf{e}_0 = \mathbf{F}\mathbf{e}_0^{(1)} + \mathbf{e}_0^{(2)}$ and use $\mathbf{e}_0^{(1)}$ to hide $\mathbf{s}$. We defer this Gaussian decomposition lemma as Lemma 13 to Supplementary Materials A.2.

Now we can prove the Lemma 3.

Proof (Proof of Lemma 3). We use hybrid arguments to prove the lemma. Here are the six hybrids we introduce.

In the **Hybrid 1**,

$$D^{(1)} = ((\widetilde{\mathbf{A}}, \widetilde{\mathbf{A}}\mathbf{s} + \mathbf{e}_0), (b, x, \mathbf{d}, c) \leftarrow \mathcal{A}(\widetilde{\mathbf{A}}, \widetilde{\mathbf{A}}\mathbf{s} + \mathbf{e}_0), I_{b,\mathbf{x}}(\mathbf{d}) \cdot \mathbf{s} \bmod 2),$$

where $\widetilde{\mathbf{A}} = \mathbf{BC} + \mathbf{F}$ and $\mathbf{B} \in \mathbb{Z}_q^{m\times l}$, $\mathbf{C} \in \mathbb{Z}_q^{l\times n}$ and $\mathbf{F}$ is selected from the distribution $D_{\mathbb{Z}_q^{m\times n},\sigma_{\mathbf{F}}}$, where $\sigma_{\mathbf{F}} = \sqrt{n}$. According to the hardness of $\mathsf{LWE}_{q,\sigma_{\mathbf{F}}}^{m,l}$ assumption, distribution D_0 and $D^{(1)}$ are computationally indistinguishable.

In the **Hybrid 2**,

$$D^{(2)} = ((\widetilde{\mathbf{A}}', \widetilde{\mathbf{A}}'\mathbf{s} + \mathbf{e}_0), (b, x, \mathbf{d}, c) \leftarrow \mathcal{A}(\widetilde{\mathbf{A}}', \widetilde{\mathbf{A}}'\mathbf{s} + \mathbf{e}_0), I_{b,\mathbf{x}}(\mathbf{d}) \cdot \mathbf{s} \bmod 2).$$

The only difference between distribution $D^{(1)}$ and $D^{(2)}$ is that we select $\widetilde{\mathbf{A}}' = \mathbf{BC} + \mathbf{F}$ with totally the same parameters with $\widetilde{\mathbf{A}}$ in $D^{(1)}$, but abort if $\|\mathbf{F}\| \geq \sigma_{\mathbf{F}}\sqrt{m}$. As the probability of aborting is negligible, the distributions of $D^{(1)}$ and $D^{(2)}$ are statistically indistinguishable.

In the **Hybrid 3**,

$$\begin{aligned} D^{(3)} = ((\widetilde{\mathbf{A}}', \mathbf{BCs} + \mathbf{F}(\mathbf{s} + \mathbf{e}_0^{(1)}) + \mathbf{e}_0^{(2)}),& \\ (b, \mathbf{x}, \mathbf{d}, c) \leftarrow \mathcal{A}(\widetilde{\mathbf{A}}', \mathbf{BCs} + \mathbf{F}(\mathbf{s} + \mathbf{e}_0^{(1)}) + \mathbf{e}_0^{(2)}), I_{b,\mathbf{x}}(\mathbf{d}) \cdot \mathbf{s} \bmod 2),& \end{aligned}$$

where $\mathbf{e}_0^{(1)} \hookleftarrow D_{\mathbb{Z}^n,\sigma_0^{(1)}}$ with $\sigma_0^{(1)} = n$ and $\mathbf{e}_0^{(2)} \hookleftarrow D_{\mathbb{Z}^m,\sqrt{\Sigma}}$ with $\Sigma = \sigma_0^2\mathbf{I}_m - (\sigma_0^{(1)})^2\mathbf{F}^\intercal\mathbf{F}$. The distributions of $D^{(3)}$ is identical to that of $D^{(2)}$, according to the Lemma 13 in Supplementary Materials A.2.

In the **Hybrid 4**,

$$\begin{aligned} D^{(4)} = ((\widetilde{\mathbf{A}}', \mathbf{BCs} + \mathbf{F}(\mathbf{s} + \mathbf{e}_0^{(1)}) + \mathbf{e}_0^{(2)}),\\ (b, \mathbf{x}, \mathbf{d}, c) \leftarrow \mathcal{A}(\widetilde{\mathbf{A}}', \mathbf{BCs} + \mathbf{F}(\mathbf{s} + \mathbf{e}_0^{(1)}) + \mathbf{e}_0^{(2)}),\\ (\delta_{\mathbf{d}\in\hat{G}_{\mathbf{s}_{b\oplus 1},b,\mathbf{x}}} \cdot r) \oplus (I_{b,\mathbf{x}}(\mathbf{d}) \cdot \mathbf{s} \bmod 2)). \end{aligned}$$

According to the Lemma 6, based on the condition of $(\mathbf{s} + \mathbf{e}_0^{(1)})$, $\mathbf{Cs}$ and the hamming weight of $I_{b,\mathbf{x}}(\mathbf{d})$ larger than $\frac{n}{4}$, the distribution of $I_{b,\mathbf{x}}(\mathbf{d}) \cdot \mathbf{s} \bmod 2$ is within statistical distance at most $q^{\frac{3l}{2}} \cdot 2^{-\frac{n}{4}}$ to the uniform distribution over $\mathbb{Z}_2$. Since $n = \lambda \cdot l \cdot \log q$, these two distributions are statistically close.

In the **Hybrid 5**,

$$\begin{aligned} D^{(5)} = ((\widetilde{\mathbf{A}}', \widetilde{\mathbf{A}}'\mathbf{s} + \mathbf{e}_0),\\ (b, \mathbf{x}, \mathbf{d}, c) \leftarrow \mathcal{A}(\widetilde{\mathbf{A}}', \widetilde{\mathbf{A}}'\mathbf{s} + \mathbf{e}_0),\\ (\delta_{\mathbf{d}\in\hat{G}_{\mathbf{s}_{b\oplus 1},b,\mathbf{x}}} \cdot r) \oplus (I_{b,\mathbf{x}}(\mathbf{d}) \cdot \mathbf{s} \bmod 2)). \end{aligned}$$

The distribution of $D^{(5)}$ is identical to that of $D^{(4)}$ according to the Lemma 13 in Supplementary Materials A.2.

In the **Hybrid 6**,

$$\begin{aligned} D^{(6)} = ((\widetilde{\mathbf{A}}, \widetilde{\mathbf{A}}\mathbf{s} + \mathbf{e}_0),\\ (b, \mathbf{x}, \mathbf{d}, c) \leftarrow \mathcal{A}(\widetilde{\mathbf{A}}, \widetilde{\mathbf{A}}\mathbf{s} + \mathbf{e}_0),\\ (\delta_{\mathbf{d}\in\hat{G}_{\mathbf{s}_{b\oplus 1},b,\mathbf{x}}} \cdot r) \oplus (I_{b,\mathbf{x}}(\mathbf{d}) \cdot \mathbf{s} \bmod 2)). \end{aligned}$$

The distribution of $D^{(6)}$ is statistically closed to that of $D^{(5)}$ since the probability of aborting due to the selection of $\widetilde{\mathbf{A}}'$ is negligible.

Finally, the distribution of $D^{(6)}$ is computationally indistinguishable with the distribution D_1, according to the hardness $\mathsf{LWE}^{m,l}_{q,\sigma_{\mathbf{F}}}$ assumption. This completes the proof of the lemma. □

5 Public Key Encryption with Secret Key Leasing from LWE with Polynomial Modulus

5.1 Our PKE-SKL Scheme Description

Here we describe our construction for PKE-SKL over classical channel with single-bit messages from NNTCF family.

Construction 1 (Parallel Repetition Version of our PKE-SKL protocol)

– $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{sk})$*:*

- *let* $l = \mathcal{O}(\lambda)$*;* $n = \omega(l \cdot \lceil \log q \rceil)$*;* q *is a poly*(λ)*-sized prime satisfying* $q > 8Bm'\lfloor \log q \rfloor$ *and* $m = n \cdot \lceil \log q \rceil$*.* $\sigma_0 = n^{\frac{3}{2}}\sqrt{m}$*,* $\sigma = 150 \cdot \sigma_0 \cdot m$*,* $B = m \cdot (\sigma + \sigma_0)\sqrt{\lambda}$*,* $m'/B = \omega(n \log q)$*,* $N = \lambda$*.*
- *Run* $(k_i, \mathsf{td}_i) \leftarrow \mathrm{GEN}_{\mathcal{F}}(1^\lambda)$*, return* $k_i = (\mathbf{A}_i, \mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i})$ *and* $\mathsf{td}_i = \mathbf{T}_{\mathbf{A}_i}$*.*
- *Output* $(\mathsf{mpk}, \mathsf{sk}) = (\{k_i\}_{i\in[N]}, \{\mathsf{td}_i\}_{i\in[N]})$*.*

– $\mathsf{KeyGen}(\mathsf{mpk}) \to (\rho_{\mathsf{sk}}, \mathsf{pk})$*:*

- *Take in* $\mathsf{mpk} = \{(\mathbf{A}_i, \mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i})\}_{i=1}^N$*. Run* $\mathrm{SAMP}_{\mathcal{F}}(k_i, \cdot)$ *on a uniform superposition of* b_i*'s, to obtain the state*

$$\bigotimes_{i=1}^{N} \frac{1}{\sqrt{2q^n}} \sum_{\substack{b_i\in\{0,1\},\\ \mathbf{x}_i\in\mathbb{Z}_q^n,\\ \mathbf{e}_i\in\mathbb{Z}_q^m}} \sqrt{D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{e}_i)}|b_i, \mathbf{x}_i\rangle|\mathbf{e}_i\rangle,$$

then compute the following state:

$$\bigotimes_{i=1}^{N} \frac{1}{\sqrt{2q^n}} \sum_{\substack{b_i\in\{0,1\},\\ \mathbf{x}_i\in\mathbb{Z}_q^n,\\ \mathbf{e}_i\mathbb{Z}_q^m}} \sqrt{D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{e}_i)}|b_i, \mathbf{x}_i\rangle|\mathbf{e}_i + \mathbf{A}_i\mathbf{x}_i + b_i \cdot (\mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i})\rangle,$$

- *Measure the last register to obtain* $\mathbf{y}_i = \mathbf{A}_i\mathbf{x}'_i + \mathbf{e}'_i$*, where* $\mathbf{x}'_i = \mathbf{x}'_{i,b_i} + b_i\mathbf{s}_i$*,* $\mathbf{e}'_i = \mathbf{e}_i + b_i \cdot \mathbf{e}_{0,i}$*. The resulting post-measurement state constitutes the quantum decryption key:*

$$\rho_{sk} = \bigotimes_{i=1}^{N} \frac{1}{\sqrt{2}} \sum_{b_i\in\{0,1\}} p_{b_i}(\mathbf{e}_{0,i}, \mathbf{e}'_i)|b_i, \mathbf{x}'_{i,b_i}\rangle,$$

where $\mathbf{x}'_{i,b_i} = \mathbf{x}'_i - b_i\mathbf{s}_i$ *and the value of* $p_{b_i}(\mathbf{e}_{0,i}, \mathbf{e}'_i)$ *satisfying:*
1) $p_0(\mathbf{e}_{0,i}, \mathbf{e}'_i) = \frac{1}{\sqrt{1+e^{(2\pi\langle \mathbf{e}'_i, \mathbf{e}_{0,i}\rangle - \pi\|\mathbf{e}_{0,i}\|^2)/\sigma^2}}}$,
$p_1(\mathbf{e}_{0,i}, \mathbf{e}'_i) = \frac{e^{(\pi\langle \mathbf{e}'_i, \mathbf{e}_{0,i}\rangle - \frac{\pi}{2}\|\mathbf{e}_{0,i}\|^2)/\sigma^2}}{\sqrt{1+e^{(2\pi\langle \mathbf{e}'_i, \mathbf{e}_{0,i}\rangle - \pi\|\mathbf{e}_{0,i}\|^2)/\sigma^2}}}$ *if* $\mathbf{e}'_i \in \mathcal{S}_0 \bigcap \mathcal{S}_1 \bigcap \mathbb{Z}^m$*;*
2) $p_0(\mathbf{e}_{0,i}, \mathbf{e}'_i) = 0$*,* $p_1(\mathbf{e}_{0,i}, \mathbf{e}'_i) = 1$ *if* $\mathbf{e}'_i \in (\mathcal{S}_0 \setminus \mathcal{S}_1) \bigcap \mathbb{Z}^m$*;*
3) $p_0(\mathbf{e}_{0,i}, \mathbf{e}'_i) = 1$*,* $p_1(\mathbf{e}_{0,i}, \mathbf{e}'_i) = 0$ *if* $\mathbf{e}'_i \in (\mathcal{S}_1 \setminus \mathcal{S}_0) \bigcap \mathbb{Z}^m$*,*
where $\mathcal{S}_0 = \mathcal{B}(0, \sigma\sqrt{m})$ *and* $\mathcal{S}_1 = \mathcal{B}(\mathbf{e}_0, \sigma\sqrt{m})$*.*
- *Output public key* $\mathsf{pk} = \{(\mathbf{A}_i, \mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i}, \mathbf{y}_i)\}_{i\in[N]}$ *and quantum decryption key* ρ_{sk}*.*

– $\mathsf{Enc}(\mathsf{pk}, \mu) \to \mathsf{ct}$*:*

- *Take in a message* $\mu \in \{0, 1\}$*. Select* $\mathbf{U}_i \xleftarrow{\$} \{0,1\}^{m'\times m}$*,* $\mathbf{R} \hookleftarrow \{0,1\}^{m'\times m'}$ *and* $\hat{\mathbf{e}}_{1,i} \xleftarrow{\$} [-B, B]^{m'}$*, where* $B = (\sigma + \sigma_0)\sqrt{\lambda} \cdot m$*.*

- *Let* $\hat{\mathbf{e}}_1 = \sum_{i\in[N]} \hat{\mathbf{e}}_{1,i}$. *The algorithm computes ciphertexts as follows:*

$$\mathsf{ct} = \mathbf{R}\mathbf{A} + \mathbf{R}\mathbf{E}_1 + \mu \cdot \mathbf{G}_{m',N(n+1)+1},$$

where $\mathbf{A} \in \mathbb{Z}_q^{m'\times N(n+1)+1}$ *is given as:*

$$\mathbf{A} = \left(\mathbf{U}_1(\mathbf{A}_1\mathbf{s}_1 + \mathbf{e}_{0,1}) \middle| \mathbf{U}_1\mathbf{A}_1 \cdots \mathbf{U}_N(\mathbf{A}_N\mathbf{s}_N + \mathbf{e}_{0,N}) \middle| \mathbf{U}_N\mathbf{A}_N \middle| \textstyle\sum_{i\in[N]} \mathbf{U}_i\mathbf{y}_i \right),$$

$\mathbf{E}_1 \in \mathbb{Z}_q^{m'\times N(n+1)+1}$ *is a matrix with all columns* $\mathbf{0}^{m'}$ *except the last column which equals* $\hat{\mathbf{e}}_1$. $\mathbf{G}_{m',N(n+1)+1}$ *is the Gadget matrix.*

- *Output ciphertext* ct.

– $\mathsf{Add}(\mathsf{ct}_1, \mathsf{ct}_2) \to \mathsf{ct}_{Add}$*: On input two ciphertexts* $\mathsf{ct}_1, \mathsf{ct}_2$*, output* $\mathsf{ct}_{Add} = \mathsf{ct}_1 + \mathsf{ct}_2$.

– $\mathsf{Mult}(\mathsf{ct}_1, \mathsf{ct}_2) \to \mathsf{ct}_{Mult}$*: On input two ciphertexts* $\mathsf{ct}_1, \mathsf{ct}_2$*, output* $\mathsf{ct}_{Mult} = \mathbf{G}^{-1}(\mathsf{ct}_1) \cdot \mathsf{ct}_2$.

– $\mathsf{Dec}(\rho_{\mathsf{sk}}, \mathsf{ct}) \to (\mu', \rho'_{\mathsf{sk}})$*:*

- *On the input quantum decryption key* ρ_{sk} *and ciphertext* ct*, run decryption algorithm in a coherent way as follows:*

$$(\bigotimes_{i=1}^{N} \frac{1}{\sqrt{2}} \sum_{b_i\in\{0,1\}} p_{b_i}(\mathbf{e}_{0,i}, \mathbf{e}'_i)|b_i, \mathbf{x}'_{b_i,i})\rangle|\underbrace{\mathbf{v}_{inv}\cdot\mathsf{ct}\cdot\mathbf{v}_{sk}}_{y'}\rangle|\lceil y'/\lfloor q/2\rfloor\rceil\rangle, \quad (11)$$

where $\mathbf{v}_{inv} = \mathbf{G}^{-1}\left(\mathbf{0}^{1\times(N(n+1))} \middle| \lfloor \frac{q}{2} \rfloor\right)$ *and* $\mathbf{v}_{sk} = (-b_1, -(\mathbf{x}'_{b_1,1})^\top, \cdots - b_N, -(\mathbf{x}'_{b_N,N})^\top, 1)^\top$ *is a column vector where* b_i*'s,* $\mathbf{x}'_{b_i,i}$*'s for* $\forall i \in [N]$ *are from the corresponding registers in the secret key* ρ_{sk}.

- *Measure the last register to obtain* μ'*. Uncompute the register* $|\mathbf{y}'\rangle$ *with the ciphertexts and* b_i, $\mathbf{x}'_{b_i}$*. Then the first* N *registers consist of* ρ'_{sk}*. Ideally,* $\rho'_{\mathsf{sk}} = \rho_{\mathsf{sk}}$ *holds.*

– $\mathsf{Del}(\rho_{\mathsf{sk}}) \to \mathsf{cert}$*:*

- *Take in the* ρ_{sk}*, perform Hadamard operations and obtain*

$$|\psi\rangle = \bigotimes_{i=1}^{N} 2^{-\frac{n\cdot\lceil log(q)\rceil+2}{2}} \sum_{\substack{\mathbf{d}_i\in\{0,1\}^{n\lceil\log(q)\rceil},\\ b_i\in\{0,1\},\\ u_i\in\{0,1\}}} (-1)^{\mathbf{d}_i\cdot\mathcal{J}(\mathbf{x}'_{b_i,i})\oplus u_i b_i} p_{b_i}(\mathbf{e}_{0,i}, \mathbf{e}'_i)|u_i\rangle|\mathbf{d}_i\rangle.$$

- *Measure this quantum state, thereby resulting in* $\mathsf{cert} = \{(u_i, \mathbf{d}_i)\}_{i=1}^N \in (\mathbb{Z}_2 \times \mathbb{Z}_2^{n\cdot\lceil\log(q)\rceil})^N$ *as the deletion certificate.*

– $\mathsf{VerDel}(\mathsf{sk}, \mathsf{pk}, \mathsf{cert}) \to \top/\bot$*:*

- *Compute* $\mathbf{x}'_{b',i} \leftarrow \textsc{Inv}_{\mathcal{F}}(\mathbf{T}_{\mathbf{A}_i}, b_i, \mathbf{y}_i)$ *for all* $i \in [N]$ *and both* $b' \in \{0,1\}$.
- *Check if* $\|\mathbf{y}_i - \mathbf{A}_i\mathbf{x}'_{b',i} - b'\cdot\mathbf{A}_i\mathbf{s}_i\|_2 \le (\sigma+\sigma_0)\sqrt{m}$ *for all* $i \in [N]$ *and* $b' \in \{0,1\}$*. If not, output invalid* $\bot$*. If yes, continue.*

- *Check if* $\mathbf{d}_i \in G_{k_i,0,\mathbf{x}'_{0,i}} \bigcap G_{k_i,1,\mathbf{x}'_{1,i}}$ *and* $u_i = \mathbf{d}_i^\top \cdot (\mathcal{J}(\mathbf{x}'_{0,i}) \oplus \mathcal{J}(\mathbf{x}'_{1,i})) \bmod 2$. *Count the number of the* i *that passes the checking step and denote this number as* N'. *If* $N' > 0.78N$, *output valid* $\top$. *Otherwise, output invalid* $\perp$.

The completeness of our protocol is given as follows.

Theorem 5. *The PKE-SKL scheme with classical lessor described in Construction 1 satisfies the correctness property given in Definition 12.*

The Theorem 5 follows immediately from the following Lemmata 7 and 8. We defer the proofs to Supplementary Materials C.2.

Lemma 7 (Correctness of Decryption). *The algorithm* Dec *in PKE-SKL Construction 1 satisfies decryption correctness, namely,*

$$\Pr\left[\begin{matrix}(\mathsf{mpk},\mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{Dec}(\rho_{\mathsf{sk}},\mathsf{ct}) = \mu : (\mathsf{pk},\rho_{\mathsf{sk}}) \leftarrow \mathsf{KeyGen}(\mathsf{mpk}) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk},\mu)\end{matrix}\right] \geq 1 - \mathsf{negl}(\lambda).$$

Lemma 8 (Correctness of Verifying Deletion). *For* $m > 500$, *honestly prepared* $\{\mathbf{y}_i\}_{i\in[N]}$ *and secret key* ρ_{sk}, *the probability passing the algorithm* VerDel *is overwhelming.*

To prove the security of our PKE-SKL scheme, we need to show that the lessee should not have any noticeable advantage to distinguish between ciphertexts of messages 0 and 1, after submitting the deletion certificate. We provide the security of our protocol as follows and defer the proof to Supplementary Materials C.4. Notably, to build a similar quantum search-to-decision reduction as shown in [CGJL23] but with polynomial-size modulus, we need to resolve a dependency issue (refer to Section 2 for the high-level idea and Supplementary Materials C.3 for the rigorous statement).

Theorem 6 (Security of our PKE-SKL). *For* $\sigma_0 = n^{\frac{3}{2}}\sqrt{m}$, *assuming the post-quantum hardness* $\mathsf{LWE}_{n,m,q,\sigma_0}$ *with polynomial modulus, the Construction 1 satisfies strong* γ*-SKL security defined in Definition 15 for any noticeable* γ.

6 Polynomial-Sized Proof of Quantumness

In this section, we present an NNTCF-based proof of quantumness protocol based on the polynomial hardness of LWE problem without reliance on a random oracle or Bell's inequality. Our proof of quantumness protocol can be viewed as an improved version of the work in [BCM+18], where the soundness is directly guaranteed by the AHB property of the NNTCF.

Let $\mathcal{P}$ denote a quantum prover and $\mathcal{V}$ denote a classical verifier, our proof of quantumness protocol is given in Construction 2.

Construction 2 (Proof of Quantumness based on LWE-based NNTCF)

1. $\mathsf{Setup}(1^\lambda)$*: Fix a security parameter* λ *and the NNTCF family* $\mathcal{F}$ *described by algorithms* $(\textsc{Gen}_{\mathcal{F}}, \textsc{Samp}_{\mathcal{F}}, \textsc{Inv}_{\mathcal{F}}, \textsc{Chk}_{\mathcal{F}})$*, assuming the polynomial hardness of LWE. Set* $l = \mathcal{O}(\lambda)$*,* $n = \omega(l\lceil \log q \rceil)$*,* $m \geq n \cdot \lceil \log q \rceil$ *and* $m > 500$*;* $w = n\lceil \log q \rceil$*,* $q \geq 8\sigma\sqrt{m}$ *a prime,* $\sigma_0 \geq n^{\frac{3}{2}}\sqrt{m}$*,* $150 \cdot m \cdot \sigma_0 \leq \sigma \leq \frac{q}{C_T\sqrt{mn\log q}}$*.* $N = \lambda$*. Output* $\mathsf{pp} = (n, m, w, q, \sigma_0, \sigma)$*.*
2. *For* $i = 1, \ldots, N$*,*
   - *i.1.* $\mathcal{V}$*: On input the parameters* pp*, the verifier runs* $(k_i = (\mathbf{A}_i, \mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i}), \mathbf{T}_{\mathbf{A}_i}) \leftarrow \textsc{Gen}_{\mathcal{F}_{\mathsf{LWE}}}(1^m, 1^n, \sigma_0, q)$*,where* $\mathbf{e}_{0,i} \hookleftarrow D_{\mathbb{Z}^m,\sigma_0,\sigma_0\sqrt{m}}$*, sends* k *to the prover and keeps the trapdoor* $\mathbf{T}_{\mathbf{A}_i}$ *private.*
   - *i.2.* $\mathcal{P}$*: On receive the key* $k_i = (\mathbf{A}_i, \mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i})$*, the prover will do the following steps:*
     - *Generate the following quantum state:*

$$\frac{1}{\sqrt{2q^n}} \sum_{\substack{b_i\in\{0,1\},\\ \mathbf{x}_i\in\mathbb{Z}_q^n,\\ \mathbf{e}_i\in\mathbb{Z}_q^m}} \sqrt{D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{e}_i)}|b_i, \mathbf{x}_i\rangle|\mathbf{e}_i\rangle$$

     and then compute with the key k_i *as below:*

$$\frac{1}{\sqrt{2q^n}} \sum_{\substack{b_i\in\{0,1\},\\ \mathbf{x}_i\in\mathbb{Z}_q^n,\\ \mathbf{e}_i\mathbb{Z}_q^m}} \sqrt{D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{e}_i)}|b_i, \mathbf{x}_i\rangle|\mathbf{e}_i + \mathbf{A}_i\mathbf{x}_i + b_i \cdot (\mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i})\rangle, \tag{12}$$

     - *Measure the last register to obtain* $\mathbf{y}_i = \mathbf{A}_i\mathbf{x}'_i + \mathbf{e}'_i$*, where* $\mathbf{x}'_{i,b_i} = \mathbf{x}'_i - b_i\mathbf{s}_i$ *and* $\mathbf{x}'_i = \mathbf{x}'_{i,0} + b_i\mathbf{s}_i$*,* $\mathbf{e}'_i = \mathbf{e}_i + b_i \cdot \mathbf{e}_{0,i}$ *for some fixed* $\mathbf{e}_i$*. The resulting post-measurement state is:*

$$|\varphi_i\rangle = \frac{1}{\sqrt{2}} \sum_{b_i\in\{0,1\}} p_{b_i}(\mathbf{e}_{0,i}, \mathbf{e}'_i)|b_i, \mathbf{x}'_{i,b_i}\rangle,$$

     where the value of $p_{b_i}(\mathbf{e}_{0,i}, \mathbf{e}'_i)$ *satisfying:*
     1) $p_0(\mathbf{e}_{0,i}, \mathbf{e}'_i) = \frac{1}{\sqrt{1+e^{(2\pi\langle\mathbf{e}'_i,\mathbf{e}_{0,i}\rangle - \pi\|\mathbf{e}_{0,i}\|^2)/\sigma^2}}}$*,*
     $p_1(\mathbf{e}_{0,i}, \mathbf{e}'_i) = \frac{e^{(\pi\langle\mathbf{e}'_i,\mathbf{e}_{0,i}\rangle - \frac{\pi}{2}\|\mathbf{e}_{0,i}\|^2)/\sigma^2}}{\sqrt{1+e^{(2\pi\langle\mathbf{e}'_i,\mathbf{e}_{0,i}\rangle - \pi\|\mathbf{e}_{0,i}\|^2)/\sigma^2}}}$ *if* $\mathbf{e}'_i \in \mathcal{S}_0 \bigcap \mathcal{S}_1 \bigcap \mathbb{Z}^m$*;*
     2) $p_0(\mathbf{e}_{0,i}, \mathbf{e}'_i) = 0$*,* $p_1(\mathbf{e}_{0,i}, \mathbf{e}'_i) = 1$ *if* $\mathbf{e}'_i \in (\mathcal{S}_0 \setminus \mathcal{S}_1) \bigcap \mathbb{Z}^m$*;*
     3) $p_0(\mathbf{e}_{0,i}, \mathbf{e}'_i) = 1$*,* $p_1(\mathbf{e}_{0,i}, \mathbf{e}'_i) = 0$ *if* $\mathbf{e}'_i \in (\mathcal{S}_1 \setminus \mathcal{S}_0) \bigcap \mathbb{Z}^m$*,*
     where $\mathcal{S}_0 = \mathcal{B}(0, \sigma\sqrt{m})$ *and* $\mathcal{S}_1 = \mathcal{B}(\mathbf{e}_0, \sigma\sqrt{m})$*.*
     - *Output the string* $\mathbf{y}_i$*.*
   - *i.3.* $\mathcal{V}$*: Reply with a uniformly random challenge bit* $c_i \xleftarrow{\$} \{0, 1\}$*.*
   - *i.4.* $\mathcal{P}$*: Take in the challenge* c_i*, do the following tests:*
     - *Preimage test (if* $c_i = 0$*): Perform a standard basis measurement onto* $|\varphi_i\rangle$*, return a pair* $(b_i, \mathbf{x}'_{i,b_i})$ *as the proof* σ_{c_i}*.*
     - *Equation test (if* $c_i = 1$*): Perform a Hadamard basis measurement onto* $|\varphi_i\rangle$*, return a pair* $(u_i, \mathbf{d}_i)$ *as the proof* σ_{c_i}*.*

3. $\mathcal{V}$: *Take in* $\{\mathbf{T}_{\mathbf{A}_i}, \mathbf{y}_i, c_i, \sigma_{c_i}\}_{i\in N}$, *do the following steps:*
   - *Compute* $\mathbf{x}'_{b',i} \leftarrow \text{INV}_{\mathcal{F}}(\mathbf{T}_{\mathbf{A}_i}, b_i, \mathbf{y}_i)$ *for all* $i \in [N]$ *and both* $b' \in \{0,1\}$.
   - *When* $c_i = 0$, *check if* $\text{CHK}_{\mathcal{F}_{\mathsf{LWE}}}(k_i, b_i, \mathbf{x}'_{i,b_i}, \mathbf{y}_i) = 1$ *holds for all* $i \in [N]$.
   - *When* $c_i = 1$, *check if* $\mathbf{d}_i \in G_{k_i,0,\mathbf{x}'_{0,i}} \bigcap G_{k_i,1,\mathbf{x}'_{1,i}}$ *and* $u_i = \mathbf{d}_i^{\mathrm{T}} \cdot (\mathcal{J}(\mathbf{x}'_{0,i}) \oplus \mathcal{J}(\mathbf{x}'_{1,i}))$ mod 2.
   - *Count the number of* i*'s that* $c_i = j$ *for* $j \in \{0,1\}$ *and denote this number as* N_j. *Count the number of the* i*'s that pass the Equation tests and denote this number as* N'. *If* $N_0 > \frac{1}{4}N$,$N_1 \geq \frac{1}{4}N$ *and* $N' > 0.75N_1$, *output valid* $\top$. *Otherwise, output invalid* $\bot$.

The correctness of our protocol is given as follows. We defer the proof to Supplementary Materials D.1.

Theorem 7 (Correctness of Our Proof of Quantumness). *Let* $\lambda \in \mathbb{N}$ *be the security parameter. A QPT prover* $\mathcal{P}$, *following the honest strategy in the Construction 2, is accepted with probability* $1 - \mathsf{negl}(\lambda)$.

In the following, we let p_{pre} denote the $\widetilde{\mathcal{P}}$'s success probability in the preimage test and p_{eqn} denote the $\widetilde{\mathcal{P}}$'s success probability in the equation test. We refer to the Lemma 28 in Supplementary Materials D.2 for the relation $p_{\mathsf{pre}} + 2p_{\mathsf{eqn}} - 2 \leq \mathsf{negl}(\lambda)$ between these two probabilities. Now we are ready to present the soundness of our protocol.

Theorem 8 (Soundness of Our Proof of Quantumness). *Based on the adaptive hardcore bit property of the NNTCF family* $\mathcal{F}$, *the probability for any classical* $\widetilde{\mathcal{P}}$ *to pass the verification in the Construction 2 is negligible.*

Proof (Proof of Lemma 8). In each round $c_i \xleftarrow{\$} \{0,1\}$, by Chernoff Bound, we have $\Pr[N_j \leq \frac{1}{4}N] \leq e^{-\frac{N}{8}} = e^{-\mathsf{poly}(\lambda)}$ for both $j \in \{0,1\}$. Assuming that we have $p_{\mathsf{pre}} \leq 1 - \xi(\lambda)$ for a non-negligible function $\xi(\lambda)$. Then the probability for the classical prover to pass all preimage tests is at most $(1 - \xi(\lambda))^{\frac{N_0}{4}}$, which is negligible and leads to a contradiction. Therefore we must have $p_{\mathsf{pre}} \geq 1 - \mathsf{negl}(\lambda)$. Basing on the Lemma 28 in Supplementary Materials D.2, this implies $p_{\mathsf{eqn}} \leq \frac{1}{2} + \mathsf{negl}(\lambda)$. By Chernoff Bound, we have $\Pr[N' > 0.75N_1] < e^{-\frac{N_1}{20}} < e^{-\frac{N}{80}}$, which is negligible. Therefore any classical prover $\widetilde{\mathcal{P}}$ cannot pass the verification in our protocol with a non-negligible probability. □

Acknowledgments

This work was supported in part by the National Key Research and Development Program of China (No. 2022YFB2702700), by the European Union's Horizon Europe research and innovation programme under the project "Quantum Secure Networks Partnership" (QSNP, No. 101114043). We thank the anonymous ASIACRYPT referees for corrections and suggestions that improved the presentation of the paper.

References

AKN+23. Shweta Agrawal, Fuyuki Kitagawa, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. Public key encryption with secure key leasing. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 581–610. Springer, 2023.

AKPW13. Joël Alwen, Stephan Krenn, Krzysztof Pietrzak, and Daniel Wichs. Learning with rounding, revisited. In Advances in Cryptology–CRYPTO 2013, pages 57–74. Springer, 2013.

ALL+21. Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. New approaches for quantum copy-protection. In Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41, pages 526–555. Springer, 2021.

ALP20. Prabhanjan Ananth and Rolando L La Placa. Secure quantum extraction protocols. In Theory of Cryptography Conference, pages 123–152. Springer, 2020.

ALP21. Prabhanjan Ananth and Rolando L. La Placa. Secure software leasing. In Anne Canteaut and François-Xavier Standaert, editors, Advances in Cryptology – EUROCRYPT 2021, pages 501–530, Cham, 2021. Springer International Publishing.

APV23. Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. In Guy Rothblum and Hoeteck Wee, editors, Theory of Cryptography, pages 93–122, Cham, 2023. Springer Nature Switzerland.

Ban93. Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. Mathematische Annalen, 296:625–635, 1993.

BCM+18. Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), pages 320–331. IEEE, 2018.

BD20. Zvika Brakerski and Nico Döttling. Hardness of lwe on general entropic distributions. In Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30, pages 551–575. Springer, 2020.

BGKM+23. Zvika Brakerski, Alexandru Gheorghiu, Gregory D Kahanamoku-Meyer, Eitan Porat, and Thomas Vidick. Simple tests of quantumness also certify qubits. In Annual International Cryptology Conference, pages 162–191. Springer, 2023.

BKVV20. Zvika Brakerski, Venkata Koppula, Umesh Vazirani, and Thomas Vidick. Simpler proofs of quantumness. In 15th Conference on the Theory of Quantum Computation, Communication and Cryptography, 2020.

CGJL23. Orestis Chardouvelis, Vipul Goyal, Aayush Jain, and Jiahui Liu. Quantum key leasing for pke and fhe with a classical lessor. arXiv preprint arXiv:2310.14328, 2023.

CGV22. Andrea Coladangelo, Shafi Goldwasser, and Umesh Vazirani. Deniable encryption in a quantum world. In Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing, pages 1378–1391, 2022.

CHV23. Céline Chevalier, Paul Hermouet, and Quoc-Huy Vu. Semi-quantum copy-protection and more. In Theory of Cryptography Conference, pages 155–182. Springer, 2023.

GMP23. Alexandru Gheorghiu, Tony Metger, and Alexander Poremba. Quantum cryptography with classical communication: Parallel remote state preparation for copy-protection, verification, and more. In 50th International Colloquium on Automata, Languages, and Programming (ICALP 2023). Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2023.

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`.

GSW13. Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Advances in Cryptology–CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I, pages 75–92. Springer, 2013.

GV19. Alexandru Gheorghiu and Thomas Vidick. Computationally-secure and composable remote state preparation. In 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS), pages 1024–1033. IEEE, 2019.

HMNY21. Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Quantum encryption with certified deletion, revisited: Public key, attribute-based, and classical communication. In Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part I 27, pages 606–636. Springer, 2021.

KLVY23. Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game. In Proceedings of the 55th Annual ACM Symposium on Theory of Computing, pages 1617–1628, 2023.

KMCVY22. Gregory D Kahanamoku-Meyer, Soonwon Choi, Umesh V Vazirani, and Norman Y Yao. Classically verifiable quantum advantage from a computational bell test. Nature Physics, 18(8):918–924, 2022.

KNY21. Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Secure software leasing from standard assumptions. In Theory of Cryptography Conference, pages 31–61. Springer, 2021.

LG22. Zhenning Liu and Alexandru Gheorghiu. Depth-efficient proofs of quantumness. Quantum, 6:807, 2022.

Mah18a. Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), pages 332–338. IEEE, 2018.

Mah18b. Urmila Mahadev. Classical verification of quantum computations. In 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), pages 259–267. IEEE, 2018.

MP13. Daniele Micciancio and Chris Peikert. Hardness of sis and lwe with small parameters. In Annual cryptology conference, pages 21–39. Springer, 2013.

MPY23. Tomoyuki Morimae, Alexander Poremba, and Takashi Yamakawa. Revocable quantum digital signatures. arXiv preprint arXiv:2312.13561, 2023.

RS19. Roy Radian and Or Sattath. Semi-quantum money. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT '19, page 132–146. Association for Computing Machinery, 2019.

Shm22. Omri Shmueli. Public-key quantum money with a classical bank. In Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing, pages 790–803, 2022.

YZ22. Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. In 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS), pages 69–74. IEEE, 2022.

Zha20. Mark Zhandry. Schrödinger's pirate: How to trace a quantum decoder. In Rafael Pass and Krzysztof Pietrzak, editors, Theory of Cryptography, pages 61–91, Cham, 2020. Springer International Publishing.

Supplementary Materials

A Supplementary materials for preliminary

A.1 Distance

We need to introduce some distances which are used to measure the difference between two distributions.

For two densities f_1 and f_2 on the discrete domain X, the Hellinger distance between f_1 and f_2 is

$$H^2(f_1, f_2) = 1 - \sum_{x \in X} \sqrt{f_1(x) f_2(x)}.$$

The statistical distance between f_1 and f_2 is defined by

$$\Delta(f_1, f_2) = \frac{1}{2} \sum_{x \in X} |f_1(x) - f_2(x)|.$$

and we can compute that $\Delta(f_1, f_2) \leq \sqrt{2H^2(f_1, f_2)}$.

Furthermore, referring to [BKVV20, Lemma 2.0.1], we can relate the Hellinger distance and the trace distance of superposition as below:

Lemma 9. *Let X be a finite set and f_1, f_2 two density functions on X. Let*

$$|\varphi_1\rangle = \sum_{x \in X} \sqrt{f_1(x)} |x\rangle, \text{ and } |\varphi_2\rangle = \sum_{x \in X} \sqrt{f_2(x)} |x\rangle.$$

Then

$$\| |\varphi_1\rangle - |\varphi_2\rangle \|_{tr} \leq \sqrt{1 - (1 - H^2(f_1, f_2))^2}.$$

Lemma 10 ([CGJL23, Claim C.1]). *Suppose there are three events A, B, C which all happen with inverse polynomial probability, and suppose $\Pr[A|B] \geq 1 - \mathsf{negl}(\lambda)$ and $\Pr[B \cap C] \geq 1/p$ for some polynomial p, we will have $\Pr[B \cap C] \geq 1/p - \mathsf{negl}'(\lambda)$ for some negligible $\mathsf{negl}'(\cdot)$.*

A.2 Lattices and lattice problems

Furthermore, we need to rely on the following lemmata and theorems in our work.

Lemma 11. *Let r be a positive number, and q, m be positive integers. $D_{\mathbb{Z}^n, r, 2r\sqrt{n}}$ is the bounded discrete Gaussian distribution with the derivation parameter r and the bound $2r\sqrt{n}$. Consider $\mathbf{e} \in \mathbb{Z}_q^n$ with 2-norm $\|\mathbf{e}\| \leq \frac{1}{2} r\sqrt{n}$. The shifted distribution $D_{\mathbb{Z}^n, r, 2r\sqrt{n}} + \mathbf{e}$ has the density of*

$$(D_{\mathbb{Z}^n, r, 2r\sqrt{n}} + \mathbf{e})(\mathbf{x}) = \begin{cases} \frac{\rho_r(\mathbf{x} - \mathbf{e})}{\sum_{\|\mathbf{y}\| \leq 2r\sqrt{n}} \rho_r(\mathbf{y})} & , \text{ if } \|\mathbf{x} - \mathbf{e}\| \leq 2r\sqrt{n}, \\ 0 & , \text{ otherwise.} \end{cases}$$

The Hellinger distance between the distribution $D_{\mathbb{Z}^n,r,2r\sqrt{n}}$ and the shifted distribution $D_{\mathbb{Z}^n,r,2r\sqrt{n}}+\mathbf{e}$ satisfies

$$H^2(D_{\mathbb{Z}^n,r,2r\sqrt{n}}, D_{\mathbb{Z}^n,r,2r\sqrt{n}}+\mathbf{e}) \leq 1-(e^{\frac{-9\sqrt{n}\|\mathbf{e}\|}{4r}}(1-2e^{-\frac{1}{2}n})).$$

Proof (Proof of Lemma 11). Let $\tau = \sum_{\|\mathbf{x}\|\leq 2r\sqrt{n}} e^{\frac{-\pi\|\mathbf{x}\|^2}{r^2}}$, $\mathcal{S} := \{\mathbf{y}\in\mathbb{Z}^n : \|\mathbf{y}\| \leq 2r\sqrt{n}\}$ and $\mathcal{S}' := \{\mathbf{y}\in\mathbb{Z}^n : \|\mathbf{y}-\mathbf{e}\| \leq 2r\sqrt{n}\}$.

$$\begin{aligned}
&\sum_{\mathbf{x}\in\mathbb{Z}^n}\sqrt{D_{\mathbb{Z}^n,r,2r\sqrt{n}}\cdot(D_{\mathbb{Z}^n,r,2r\sqrt{n}}+\mathbf{e})}\\
=&\frac{1}{\tau}\sum_{\mathbf{x}\in\mathcal{S}\bigcap\mathcal{S}'}\sqrt{e^{\frac{-\pi\|\mathbf{x}\|^2}{r^2}}\cdot e^{\frac{-\pi\|\mathbf{x}-\mathbf{e}\|^2}{r^2}}}\\
=&\frac{1}{\tau}\sum_{\mathbf{x}\in\mathcal{S}\bigcap\mathcal{S}'}e^{\frac{-\pi(\|\mathbf{x}\|^2+\|\mathbf{x}-\mathbf{e}\|^2)}{2r^2}}\\
\geq&\frac{1}{\tau}\sum_{\mathbf{x}\in\mathcal{S}\bigcap\mathcal{S}'}e^{\frac{-\pi\|\mathbf{x}\|^2}{r^2}}\cdot e^{\frac{-\pi(2\|\mathbf{x}\|\cdot\|\mathbf{e}\|)}{2r^2}}\cdot e^{\frac{-\pi\|\mathbf{e}\|^2}{2r^2}}\\
\geq&e^{\frac{-\pi(4r\sqrt{n}\|\mathbf{e}\|+\|\mathbf{e}\|^2)}{2r^2}}\frac{1}{\tau}\sum_{\mathbf{x}\in\mathcal{S}\bigcap\mathcal{S}'}e^{\frac{-\pi\|\mathbf{x}\|^2}{r^2}}\\
\geq&e^{\frac{-9\sqrt{n}\|\mathbf{e}\|}{4r}}\cdot\frac{\sum_{x\in\mathcal{S}\bigcap\mathcal{S}'}e^{\frac{-\pi\|\mathbf{x}\|^2}{r^2}}}{\sum_{x\in\mathcal{S}}e^{\frac{-\pi\|\mathbf{x}\|^2}{r^2}}}\\
\geq&e^{\frac{-9\sqrt{n}\|\mathbf{e}\|}{4r}}(1-\frac{\sum_{2r\sqrt{n}-\|\mathbf{e}\|\leq\|\mathbf{x}\|\leq 2r\sqrt{n}}e^{\frac{-\pi\|\mathbf{x}\|^2}{r^2}}}{\sum_{\|\mathbf{x}\|\leq 2r\sqrt{n}}e^{\frac{-\pi\|\mathbf{x}\|^2}{r^2}}})\\
\geq&e^{\frac{-9\sqrt{n}\|\mathbf{e}\|}{4r}}(1-\frac{\sum_{\frac{3}{2}r\sqrt{n}\leq\|\mathbf{x}\|\leq 2r\sqrt{n}}e^{\frac{-\pi\|\mathbf{x}\|^2}{r^2}}}{\sum_{\|\mathbf{x}\|\leq 2r\sqrt{n}}e^{\frac{-\pi\|\mathbf{x}\|^2}{r^2}}})\\
>&e^{\frac{-9\sqrt{n}\|\mathbf{e}\|}{4r}}(1-e^{(ln\frac{3}{2}-\frac{9}{4})n}(1+e^{(ln2-\frac{3}{2})n}))\\
>&e^{\frac{-9\sqrt{n}\|\mathbf{e}\|}{4r}}(1-2\cdot e^{(ln2-\frac{3}{2})n})\\
>&e^{\frac{-9\sqrt{n}\|\mathbf{e}\|}{4r}}(1-2e^{-\frac{1}{2}n})
\end{aligned}$$

The result follows immediately. □

Theorem 9 ([GPV07,MP13]). *There is an efficient algorithm* GenTrap *that, on input $1^n, q, m = \Omega(n\log q)$, outputs a matrix $\mathbf{A}$ distributed statistically close to uniformly on $\mathbb{Z}_q^{n\times m}$, and a $O(m)$-good lattice trapdoor* td *for $\mathbf{A}$. Moreover, there is an efficient algorithm* Invert *that, on input $\mathbf{A}$, td and $\mathbf{sA}+\mathbf{e}$ where $\|\mathbf{e}\| \leq q/(C_T\sqrt{n\log q})$ and C_T is a universal constant, returns $\mathbf{s}$ and $\mathbf{e}$ with overwhelming probability over $(\mathbf{A},\mathsf{td}) \leftarrow \textsc{GenTrap}(1^n, 1^m, q)$.*

Lemma 12 (Leftover Hash Lemma). *For a security parameter λ and n, m, q are polynomials over λ, the leftover hash lemma says that if $m \geq \omega(n \log q)$, then if you sample $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{x} \leftarrow \{0,1\}^m$ and $\mathbf{y} \leftarrow \mathbb{Z}_q^m$, we have:*

$$(\mathbf{A}, \mathbf{A} \cdot \mathbf{x}) \approx_{stat} (\mathbf{A}, \mathbf{y}).$$

Furthermore, the statistical distance between these distributions is at most $\frac{q^n}{2^m} = 2^{-\omega(n \log q)} = 2^{-poly(\lambda)}$, which is negligible.

Definition 5. *Let $\chi = \chi(\lambda)$ be an efficiently sampleable distribution over $\mathbb{Z}_q$. Define a lossy sampler $\tilde{\mathbf{A}} \leftarrow \text{LOSSY}(1^n, 1^m, 1^\ell, q, \chi)$ by $\tilde{\mathbf{A}} = \mathbf{BC} + \mathbf{F}$, where $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{m \times \ell}$, $\mathbf{C} \xleftarrow{\$} \mathbb{Z}_q^{\ell \times n}$, $\mathbf{F} \leftarrow \chi^{m \times n}$.*

Theorem 10 ([AKPW13, Lemma 3.2]). *Under the $\mathsf{LWE}_{\ell,q,\chi}$ assumption, the distribution of a random $\tilde{\mathbf{A}} \leftarrow \text{LOSSY}(1^n, 1^m, 1^\ell, q, \chi)$ is computationally indistinguishable from $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$.*

Lemma 13. *Let $\mathbf{F} \in \mathbb{Z}^{m \times n}$ be an arbitrary matrix with spectral norm $\sigma_{\mathbf{F}}$. Let $\sigma, \sigma_1 > 0$ s.t. $\sigma > \sigma_1 \sigma_{\mathbf{F}}$. Let $\mathbf{e}_1 \sim D_{\mathbb{Z}^n, \sigma_1}$ and let $\mathbf{e}_2 \sim D_{\mathbb{Z}^m, \sqrt{\Sigma}}$ for $\Sigma = \sigma^2 \mathbf{I}_m - \sigma_1^2 \mathbf{F}^\top \mathbf{F}$. Then the random variable $\mathbf{e} = \mathbf{F}\mathbf{e}_1 + \mathbf{e}_2$ is distributed according to $D_{\mathbb{Z}^m, \sigma}$.*

A.3 Parallel Repetition of the NTCF-based Protocol

We describe the single-instance game from [RS19,CGJL23]. The game is abstracted as a "1-of-2" puzzle with "2-of-2 soundness", where the verifier randomly asks the prover to output a preimage $\mathbf{x} \in \mathcal{X}$ or an adaptive hardcore bit for the same image $\mathbf{y} \in \mathcal{Y}$.

Definition 6 (1-of-2 Puzzle from NTCF [RS19]). *The protocol proceeds as follows.*

- *The verifier samples a key $(k, \mathsf{td}) \leftarrow \text{GEN}_{\mathcal{F}}(1^\lambda)$ and send k to the prover. The verifier keeps the trapdoors td*
- *The prover sends back a committed image value $\mathbf{y}$.*
- *The verifier samples a random bit $\delta \in \{0,1\}$ and sends δ to the prover.*
- *If $\delta = 0$, the prover sends back some $\mathbf{x} \in \mathcal{X}$; else if $b = 1$, the prover sends back a string $(c, \mathbf{d})$.*
- *The verifier does the following checks on each $(\mathbf{y}, \mathbf{x})$ or $(\mathbf{y}, c, \mathbf{d})$:*
  - *When $\delta = 0$: Check $\mathbf{x} \in \text{INV}(\mathsf{td}, b \in \{0,1\}, \mathbf{y})$ [6].*
  - *When $\delta = 1$: Find both $\mathbf{x}_0, \mathbf{x}_1$ using $\text{INV}(\mathsf{td}, b \in \{0,1\}, \mathbf{y})$. Check if $c = \mathbf{d} \cdot (\mathcal{J}(\mathbf{x}_0) \oplus \mathcal{J}(\mathbf{x}_1))$.*

[6] This step can also be performed publicly using $\text{CHK}_{\mathcal{F}}$.

[RS19] showed the following property for the above protocol using the LWE-based NTCF.

1-of-2 Completeness: Any BQP prover will answer one of the challenges for $\delta = 0$ or $\delta = 1$ with probability 1.

2-of-2 Soundness: The 2-of-2 soundness error in the above protocol is the probability that a prover can provide both the 1-challenge answer $\mathbf{x}$ and the 0-challenge answer $(c, \mathbf{d})$ correctly. The above protocol has 2-of-2 soundness $1/2$ for any BQP prover [RS19,BCM$^+$18,CGJL23].

Parallel Repetition We now describe a special type of parallel-repeated protocol based on the NTCF. In this protocol, we only consider the "2-of-2" setting: the verifier samples multiple keys independently; for every single key, the verifier simply asks the prover to provide both the answer to the 0-challenge and the answer to the 1-challenge.

Its parallel repetition soundness was shown in [RS19].

Definition 7 (Parallel-Repeated 2-of-2 NTCF-protocol)). *The protocol proceeds as follows.*

- *The verifier samples ℓ number of keys $(k_i, \mathsf{td}_i) \leftarrow \textsc{Gen}_{\mathcal{F}}(1^\lambda), i \in [\ell]$ independently and send $\{k_i\}_{i\in[\ell]}$ to the prover. The verifier keeps the trapdoors $\{\mathsf{td}_i\}_{i\in[\ell]}$*
- *The prover sends back ℓ tuple of values $\{(\mathbf{y}_i, \mathbf{x}_i, c_i, \mathbf{d}_i)\}_{i\in[\ell]}$.*
- *The verifier does the following checks on each $(\mathbf{y}_i, \mathbf{x}_i, c_i, \mathbf{d}_i)$ for $i \in [\ell]$:*
  - *Find both $\mathbf{x}_{i,0}, \mathbf{x}_{i,1}$ using $\textsc{Inv}(\mathsf{td}_i, b \in \{0,1\}, \mathbf{y}_i)$.*
  - *Check if $c_i = \mathbf{d}_i \cdot (\mathcal{J}(\mathbf{x}_{i,0}) \oplus \mathcal{J}(\mathbf{x}_{i,1}))$.*
- *If all the checks pass, the verifier outputs 1; else outputs 0.*

Lemma 14 (Parallel Repetition Soundness of NTCF-based Protocol, adapted from [RS19, Theorem 15]). *Let $\mathcal{Z}$ be an NTCF-based protocol with completeness η and hardness h. For a function $N(\lambda)$ that satisfies $N(\lambda) = \mathsf{poly}(\lambda)$, then a parallel-repeated NTCF-based protocol $\mathcal{Z}^N$ has completeness η^N and hardness h^N.*

In Lemma 14, we introduce the amplified adaptive hardcore bit property from the parallel repetition of an NTCF family [RS19,KNY21,CGJL23,MPY23]. We also make use of the following result.

Lemma 15 (Implicit in [RS19], [KNY21, Lemma 3.1]). *Any NTCF family with an adaptive hardcore property satisfies the amplified adaptive hardcore property.*

Since it has been proven that NNTCF has an adaptive hardcore bit property (Theorem 4), from the Lemma 15, we immediately have an amplified adaptive hardcore property by the parallel repetition of the NNTCF.

Corollary 1 (Amplified adaptive hardcore property). *The NNTCF family with an adaptive hardcore property satisfies the amplified adaptive hardcore property.*

A.4 GSW Homomorphic Encryption

Our PKE-SKL protocol in section 5 follows the design paradigm of GSW Homomorphic Encryption introduced in [GSW13], which supports both homomorphic addition and multiplication.

In GSW scheme, one needs to generate a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ together with a secret $\mathbf{s} \in \mathbb{Z}_q^n$ such that $m \geq n\lceil \log q \rceil$ and $\mathbf{As} = \mathbf{e} \in \mathbb{Z}_q^m$ where $\mathbf{e}$ has small norm. The scheme sets $\mathbf{A}$ as the public key and $\mathbf{s}$ as the secret key. In the encryption algorithm, it samples a random matrix $\mathbf{R} \in \mathbb{Z}_q^{m \times m}$ with a small norm and compute the ciphertext $\mathsf{ct} = \mathbf{RA} + \mu \mathbf{G}_{m,n}$, where $\mathbf{G}_{m,n}$ is the so-called Gadget matrix satisfying:

$$\mathbf{G}_{m,n} = \begin{pmatrix} \mathbf{I}_n \otimes \mathfrak{g} \\ \mathbf{0}^{(m-n\lceil \log q \rceil) \times m} \end{pmatrix},$$

and $\mathfrak{g} = (1, 2, \ldots 2^{\lfloor \log q \rfloor})^\top$ a column vector. Accordingly, the inverse operation $\mathbf{G}^{-1}$ is defined as: for any integer $k > 0$ and $\mathbf{B} \in \mathbb{Z}_q^{k \times n}$, $G^{-1}(\mathbf{B}) = \big(\mathsf{Bitdecomp}(\mathbf{B}) \big| \mathbf{0}^{k \times (m - n\lceil \log q \rceil)}\big)$, where $\mathsf{Bitdecomp}(\mathbf{B})$ is the concatenation of the binary representations in row vectors of all elements in $\mathbf{B}$. With this construction, it shows that $\mathsf{ct} \cdot \mathbf{s} \approx \mu \mathbf{G}_{m,n}\mathbf{s}$. Furthermore, for two ciphertexts $\mathsf{ct}_1 = \mathbf{R}_1\mathbf{A} + \mu_1 \mathbf{G}_{m,n}$ and $\mathsf{ct}_2 = \mathbf{R}_2\mathbf{A} + \mu_2 \mathbf{G}_{m,n}$, we have $(\mathsf{ct}_1 + \mathsf{ct}_2) \cdot \mathbf{s} \approx (\mu_1 + \mu_2)\mathbf{G}_{m,n}\mathbf{s}$ and $\mathbf{G}^{-1}(\mathsf{ct}_1) \cdot \mathsf{ct}_2 \mathbf{s} \approx \mu_1 \mu_2 \mathbf{G}_{m,n}\mathbf{s}$.

A.5 Quantum Measurements

We assume readers are familiar with fundamental concepts of quantum information. Below we review some quantum measurement techniques that will be used in the PKE-SKL security proof.

Definition 8 (Projective Implementation of a POVM). *Let $\mathcal{P} = (P, \mathbf{I} - P)$ be a binary outcome POVM. Let $\mathcal{D}$ be a finite set of distributions $(p, 1-p)$ over outcomes $\{0, 1\}$. Let $\mathcal{E} = \{E_p\}_{(p,1-p)\in\mathcal{D}}$ be a projective measurement with index set $\mathcal{D}$. Consider the following measurement procedure:*

(i) Apply the $\mathcal{E}$ and obtain as outcome a distribution $(p, 1-p)$ over $\{0, 1\}$;
(ii) Output a bit according to $(p, 1-p)$, i.e. output 1 w.p. p; output 0 w.p. $1-p$.

We say the above measurement procedure is a projective implementation of $\mathcal{P}$, which we denote by $\mathsf{ProjImp}(\mathcal{P})$, if it is equivalent to $\mathcal{P}$.

Definition 9 (Mixture of Projective Measurements). *Let $\mathcal{R}$, $\mathcal{I}$ be sets. Let $\{(P_i, Q_i)\}_{i\in I}$ be a collection of binary projective measurements $(P_i, Q_i))$ over the same Hilbert space $\mathcal{H}$ where $\mathcal{P}_i$ corresponds to output 0, and $\mathcal{Q}_i$ corresponds to output 1. We will assume we can efficiently measure the $\mathcal{P}_i$ for superpositions of i, meaning we can efficiently perform the following projective measurement over $\mathcal{I} \otimes \mathcal{H}$: $(\sum_i |i\rangle\langle i| \otimes P_i, \sum_i |i\rangle\langle i| \otimes Q_i)$. Let $\mathcal{D} : \mathcal{R} \to \mathcal{I}$ be some distribution.*

The mixture of projective measurements is the binary POVM $\mathcal{P}_{\mathcal{D}} = (P_{\mathcal{D}}, Q_{\mathcal{D}})$ defined as follows:

$$P_{\mathcal{D}} = \sum_{i \in \mathcal{I}} \Pr[i \leftarrow \mathcal{D}(R)]\, P_i, \qquad Q_{\mathcal{D}} = \sum_{i \in \mathcal{I}} \Pr[i \leftarrow \mathcal{D}(R)]\, Q_i.$$

Definition 10 (Threshold Implementation, [ALL+21]). *Let $\mathcal{P} = (P, Q)$ be a binary POVM. Let $\mathsf{ProjImp}(\mathcal{P})$ be a projective implementation of $\mathcal{P}$, and let $\mathcal{E}$ be the projective measurement in the first step of $\mathsf{ProjImp}(\mathcal{P})$. Let $\gamma > 0$. We refer to the following measurement procedure as a threshold implementation of $\mathcal{P}$ with parameter γ, and we denote it as $\mathsf{TI}_\gamma(\mathcal{P})$.*

- *Apply the $\mathcal{E}$ and obtain as outcome a vector $(p, 1-p)$;*
- *Output a bit according to the $(p, 1-p)$: output 1 if $p \geq \gamma$, and 0 otherwise.*

Lemma 16 (Approximating threshold implementation, [ALL+21, Corollary 1]). *For any $\epsilon, \delta, \gamma \in (0,1)$, any collection of projective measurements $\mathcal{P} = \{(P_i, Q_i)\}_{i \in \mathcal{I}}$, where $\mathcal{I}$ is some index set, and any distribution D over $\mathcal{I}$, there exists a measurement procedure $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma}$ that satisfies the following:*

1. *$\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma}$ implements a binary outcome measurement. For simplicity, we denote the probability of the measurement **outputting 1** on ρ by $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma}\, \rho]$.*
2. *For all quantum states ρ, $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma-\epsilon}\, \rho] \geq \mathrm{Tr}[\mathsf{TI}_\gamma(\mathcal{P}_D)\, \rho] - \delta$.*
3. *For all quantum states ρ, let ρ' be the post-measurement state after applying $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma}$ on ρ, and obtaining outcome 1. Then, $\mathrm{Tr}[\mathsf{TI}_{\gamma-2\epsilon}(\mathcal{P}_D)\, \rho'] \geq 1 - 2\delta$.*
4. *The expected running time is $O(T_{\mathcal{P},D} \cdot 1/\epsilon^2 \cdot 1/(\log \delta))$, where $T_{\mathcal{P},D}$ is the combined running time of sampling according to D, of mapping i to (P_i, Q_i), and of implementing the projective measurement (P_i, Q_i) [7].*

Lemma 17 ([Zha20, Corollary 6.9]). *Let ρ be an efficiently constructible, potentially mixed state, and let $\mathcal{D}_0, \mathcal{D}_1$ be two computationally indistinguishable distributions. Then for any inverse polynomial ϵ and any function δ, there exists a negligible $\mathsf{negl}(\cdot)$ such that:*

$$\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{D}_1,\mathcal{P},\gamma-3\epsilon}(\rho)] \geq \mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{D}_0,\mathcal{P},\gamma}(\rho)] - 2\delta - \mathsf{negl}(\lambda)$$

Lemma 18 ([CGJL23, Theorem 5.12]). *Suppose the statistical distance of $\mathcal{D}_0, \mathcal{D}_1$ is η. $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},1/2+\gamma}$ is the ATI for mixture of projections $\mathcal{P} = \mathcal{P}_{\mathcal{D}_0,\mathcal{D}_1}$, with parameters γ, ϵ, δ such that γ is inverse polynomial and $\epsilon < \gamma$. The distance η also satisfies $\eta < \epsilon/2$. We have the following properties, with probability $(1-\delta)$:*

- *For any input state ρ, let ρ' be the state after applying $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},1/2+\gamma}$ on ρ, we have $\|\rho - \rho'\|_{\mathrm{Tr}} \leq O(\eta \cdot \frac{\ln(4/\delta)}{\epsilon})$.*
- *$\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},1/2+\gamma}$ will output outcome 0.*

[7] In this paper, T is simply the running time of the quantum distinguisher algorithm ρ_{Del}.

B Supplementary materials for NNTCF

B.1 Definition of NNTCF family

Here we formally define the noticeable NTCF family.

Definition 11 (Noticeable NTCF family). *Let λ be a security parameter. Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. Let $\mathcal{K}_{\mathcal{F}}$ be a finite set of keys. A family of functions*

$$\mathcal{F} = \left\{ f_{k,b} : \mathcal{X} \to \mathcal{D}_{\mathcal{Y}} \right\}_{k \in \mathcal{K}_{\mathcal{F}}, b \in \{0,1\}}$$

is called a noticeable noisy trapdoor claw-free (NNTCF) family if the following conditions hold:

1. ***Efficient Function Generation.*** *There exists an efficient probabilistic algorithm $\textsc{Gen}_{\mathcal{F}}$ which generates a key $k \in \mathcal{K}_{\mathcal{F}}$ together with a trapdoor td:*

$$(k, \mathsf{td}) \leftarrow \textsc{Gen}_{\mathcal{F}}(1^{\lambda}) \ .$$

2. ***Trapdoor Injective Pair.***
   (a) *Trapdoor: There exists an efficient deterministic algorithm $\textsc{Inv}_{\mathcal{F}}$ such that with overwhelming probability over the choice of $(k, \mathsf{td}) \leftarrow \textsc{Gen}_{\mathcal{F}}(1^{\lambda})$, the following holds:*

$$\text{for all } b \in \{0,1\}, x \in \mathcal{X} \text{ and } y \in \textsc{Supp}(f_{k,b}(x)), \textsc{Inv}_{\mathcal{F}}(\mathsf{td}, b, y) = x.$$

   (b) *Injective pair: For all keys $k \in \mathcal{K}_{\mathcal{F}}$, there exists a perfect matching $\mathcal{R}_k \subseteq \mathcal{X} \times \mathcal{X}$ such that $f_{k,0}(x_0) = f_{k,1}(x_1)$ if and only if $(x_0, x_1) \in \mathcal{R}_k$.*
3. ***Efficient Range Superposition.*** *For all keys $k \in \mathcal{K}_{\mathcal{F}}$ and $b \in \{0,1\}$ there exists a function $f'_{k,b} : \mathcal{X} \to \mathcal{D}_{\mathcal{Y}}$ such that the following hold.*
   (a) *For all $(x_0, x_1) \in \mathcal{R}_k$, $y \in \textsc{Supp}(f'_{k,0}(x_0)) \bigcap \textsc{Supp}(f'_{k,1}(x_1))$, it holds that $\textsc{Inv}_{\mathcal{F}}(\mathsf{td}, b, y) = x_b$ and $\textsc{Inv}_{\mathcal{F}}(\mathsf{td}, b \oplus 1, y) = x_{b \oplus 1}$.*
   (b) *There exists an efficient deterministic procedure $\textsc{Chk}_{\mathcal{F}}$ that, on input k, $b \in \{0,1\}$, $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, returns 1 if $y \in \textsc{Supp}(f'_{k,b}(x))$ and 0 otherwise. Note that $\textsc{Chk}_{\mathcal{F}}$ is not provided the trapdoor td.*
   (c) *For every k and $b \in \{0,1\}$,*

$$E_{x \leftarrow \mathcal{X}} \left[H^2(f_{k,b}(x),\, f'_{k,b}(x)) \right] \ \leq \ 1/50 \ .^{8}$$

   Here H^2 is the Hellinger distance. Moreover, there exists an efficient procedure $\textsc{Samp}_{\mathcal{F}}$ that on input k, it prepares the state

$$\frac{1}{\sqrt{2|\mathcal{X}|}} \sum_{\substack{x \in \mathcal{X} \\ b \in \{0,1\}}} \sum_{y \in \textsc{Supp}(f'_{k,b}(x))} \sqrt{(f'_{k,b}(x))(y)}\, |b\rangle_{\mathsf{B}} |x\rangle_{\mathsf{X}} |y\rangle_{\mathsf{Y}} \ . \tag{13}$$

[8] 1/50 can be replaced by an arbitrarily constant, unlike NTCF defined in [BCM+18], we will no longer require it to be negligible in the definition of noticeable NTCFs.

4. ***Adaptive Hardcore Bit.*** *For all keys $k \in \mathcal{K}_{\mathcal{F}}$ the following conditions hold, for some integer w that is a polynomially bounded function of λ.*
   (a) *For all $b \in \{0,1\}$ and $x \in \mathcal{X}$, there exists a set $G_{k,b,x} \subseteq \{0,1\}^w$ such that $\Pr_{d \xleftarrow{\$} \{0,1\}^w}[d \notin G_{k,b,x}]$ is negligible, and moreover there exists an efficient algorithm that checks for membership in $G_{k,b,x}$ given k, b, x and the trapdoor td.*
   (b) *There is an efficiently computable injection $\mathcal{J} : \mathcal{X} \to \{0,1\}^w$, such that $\mathcal{J}$ can be inverted efficiently on its range, and such that the following holds. If*

$$\begin{aligned} H_k = \big\{ & (b, x_b, d, d \cdot (\mathcal{J}(x_0) \oplus \mathcal{J}(x_1))) \mid b \in \{0,1\}, (x_0, x_1) \in \mathcal{R}_k, \\ & d \in G_{k,0,x_0} \bigcap G_{k,1,x_1} \big\}, \\ \overline{H}_k = \big\{ & (b, x_b, d, c) \mid (b, x, d, c \oplus 1) \in H_k \big\}, \end{aligned}$$

then for any quantum polynomial-time procedure $\mathcal{A}$ there exists a negligible function $\mu(\cdot)$ such that

$$\left| \Pr_{(k,\mathsf{td}) \leftarrow \mathrm{GEN}_{\mathcal{F}}(1^\lambda)}[\mathcal{A}(k) \in H_k] - \Pr_{(k,\mathsf{td}) \leftarrow \mathrm{GEN}_{\mathcal{F}}(1^\lambda)}[\mathcal{A}(k) \in \overline{H}_k] \right| \leq \mu(\lambda). \quad (14)$$

B.2 Supplementary proofs for adaptive hardcore bit property

Lemma 19. *For any $b, \mathbf{x}$ fixed, $\mathbf{d}$ is selected randomly from the set $\{0,1\}^{n \cdot \lceil log(q) \rceil}$. Then the vector $I_{b,\mathbf{x}}(\mathbf{d})$ is uniformly random in $\{0,1\}^n$ and the probability that the Hamming weight of $I_{b,\mathbf{x}}(\mathbf{d})_{\mathcal{I}_b}$ is at least $\frac{n}{8}$ is at least $1 - e^{-\frac{n}{32}}$. Furthermore, the probability that $\mathbf{d} \in \hat{G}_{\mathbf{s}_{b\oplus 1}, b, \mathbf{x}}$ for both $b \in \{0,1\}$ is at least $1 - e^{-\frac{n}{32}+1}$.*

Proof (Proof of Lemma 19). For each x_i, we have:

$$\mathcal{J}(x_i) \oplus \mathcal{J}(x_i + (-1)^b 1) = \begin{cases} (0, \ldots, 0, 1, \ldots, 1) & , x_i \text{ is odd, } b = 0; \\ (0, \ldots, 0, 1) & , x_i \text{ is odd, } b = 1; \\ (0, \ldots, 0, 1) & , x_i \text{ is even, } b = 0; \\ (0, \ldots, 0, 1, \ldots, 1) & , x_i \text{ is even, } b = 1. \end{cases}$$

Here the 1's in the vector $(0, \ldots, 0, 1 \ldots, 1)$ represent all the bits that are different between x_i and $x_i + (-1)^b 1$. We split the $\mathbf{d}$ into n vectors in $\{0,1\}^{\lceil log(q) \rceil}$ and $\mathbf{d}_i$ is the ith vector among them. Since $\mathbf{d}_i$ is randomly selected from the set $\{0,1\}^{\lceil log(q) \rceil}$, $\langle \mathbf{d}_i, \mathcal{J}(x_i) \oplus \mathcal{J}(x_i + (-1)^b) \rangle$ is uniformly random in $\{0,1\}$. Therefore, $I_{b,\mathbf{x}}(\mathbf{d})$ is uniformly random in the set $\{0,1\}^n$. By Chernoff bound, we have $\Pr[\mathsf{HW}(I_{b,\mathbf{x}}(\mathbf{d})_{\mathcal{I}_b}) \leq \frac{n}{8}] \leq e^{-\frac{n}{32}}$. The result follows. □

Proof (Proof of Lemma 6). We assume $\mathbf{C}$ is moderate. By Lemma 4, the $\mathbf{C}$ is moderate with probability at least $1 - q^l \cdot 2^{-\frac{n}{8}}$. Let $\mathbf{s}$ be uniform over $\{0,1\}^n$, $D'_1 = (\mathbf{Cs}, \widehat{\mathbf{d}} \cdot \mathbf{s} \bmod 2)$, conditioned on $\mathbf{s} + \mathbf{e} = \mathbf{t}$ where $\mathbf{t}$ fixed, and D'_2 uniformly

distributed over $\mathbb{Z}_q^l \times \{0,1\}$. Using that $\mathbf{C}$ is moderate, it follows from Lemma 5 that the statistical distance satisfies

$$\varepsilon = \|D_1' - D_2'\|_{ST} \leq q^{\frac{l}{2}} \cdot 2^{-\frac{n}{4}}.$$

For fixed $\mathbf{v}_0 \in \mathbb{Z}_q^l$ and let

$$\Delta = \frac{1}{2} \sum_{b \in \{0,1\}} \left| \Pr_{\mathbf{s} \leftarrow \{0,1\}^n} \left(\widehat{\mathbf{d}} \cdot \mathbf{s} \bmod 2 = b | \mathbf{C}\mathbf{s} = \mathbf{v}_0, \mathbf{s} + \mathbf{e} = \mathbf{t} \right) - \frac{1}{2} \right|.$$

We use the following formula to prove the lemma:

$$\begin{aligned}
\varepsilon &= \|D_1' - D_2'\|_{ST} \\
&= \frac{1}{2} \sum_{b \in \{0,1\}, \mathbf{v} \in \mathbb{Z}_q^l} \left| \Pr(\mathbf{C}\mathbf{s} = \mathbf{v} | \mathbf{s} + \mathbf{e} = \mathbf{t}) \Pr\left(\widehat{\mathbf{d}} \cdot \mathbf{s} \bmod 2 = b | \mathbf{C}\mathbf{s} = \mathbf{v}, \mathbf{s} + \mathbf{e} = \mathbf{t} \right) - \frac{1}{2q^l} \right| \\
&\geq \frac{1}{2} \sum_{b \in \{0,1\}} \left| \Pr\left(\mathbf{C}\mathbf{s} = \mathbf{v}_0 | \mathbf{s} + \mathbf{e} = \mathbf{t} \right) \Pr\left(\widehat{\mathbf{d}} \cdot \mathbf{s} \bmod 2 = b | \mathbf{C}\mathbf{s} = \mathbf{v}_0, \mathbf{s} + \mathbf{e} = \mathbf{t} \right) - \frac{1}{2q^l} \right| \\
&= \frac{1}{2} \sum_{b \in \{0,1\}} \left| \Pr\left(\mathbf{C}\mathbf{s} = \mathbf{v}_0 | \mathbf{s} + \mathbf{e} = \mathbf{t} \right) \left(\frac{1}{2} + (-1)^b \Delta \right) - \frac{1}{2q^l} \right|
\end{aligned}$$

Applying the triangle inequality,$|a| + |b| \geq max(|a-b|, |a+b|)$, it follows that

$$\Pr(\mathbf{C}\mathbf{s} = \mathbf{v}_0 | \mathbf{s} + \mathbf{e} = \mathbf{t}) \cdot \Delta \leq \varepsilon \text{ and } \Pr(\mathbf{C}\mathbf{s} = \mathbf{v}_0 | \mathbf{s} + \mathbf{e} = \mathbf{t}) \geq \frac{1}{q^l} - 2\varepsilon.$$

If $q^{3l/2} 2^{-\frac{n}{4}} > \frac{1}{3}$, the lemma is trivial. If $q^{3l/2} 2^{-\frac{n}{4}} \leq \frac{1}{3}$, it follows that $\Delta \leq 3q^l \varepsilon$, and the result follows immediately. □

C Supplementary materials for key leasing

C.1 Definition: PKE-SKL with Classical Lessor

We recall the notion of PKE-SKL over a classical channel.

Definition 12 (PKE-SKL, [CGJL23, Definition 8.1]). *A PKE-SKL scheme with a classical lessor consists of algorithms (*Setup, KeyGen, Enc, Dec, Del, VerDel*) defined as follows:*

- $\mathsf{Setup}(1^\lambda)$*: take input a security parameter* λ*, output a classical master public key* mpk *and a classical trapdoor* td*.*
- $\mathsf{KeyGen}(\mathsf{mpk})$*: take as input a classical master public key* mpk*, output a quantum decryption key* ρ_{sk} *and a classical public key* pk*.*
- $\mathsf{Enc}(\mathsf{pk}, \mu)$*: given a public key* pk *and a plaintext* $\mu \in \{0,1\}$*, output a classical ciphertext* ct*.*
- $\mathsf{Dec}(\rho_{\mathsf{sk}}, \mathsf{ct})$*: given a quantum decryption state* ρ_{sk} *and a ciphertext* ct*, output the message* μ *and the state* ρ'_{sk}*.*
- $\mathsf{Del}(\rho_{\mathsf{sk}})$*: given the quantum state* ρ_{sk}*, output a classical deletion certificate* cert*.*
- $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert})$*: given a public key* pk*, a classical certificate* cert *and the trapdoor* td*, output* Valid *or* $\mathsf{Invalid}$*.*

Correctness A PKE-SKL scheme over a classical channel described by the algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Del}, \mathsf{VerDel})$ satisfies correctness if the following hold.

Decryption Correctness: There exists a negligible function $\mathsf{negl}(\cdot)$, for all $\lambda \in \mathbb{N}$, for all $\mu \in \mathcal{M}$:

$$\Pr\left[\begin{matrix}(\mathsf{mpk},\mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)\\ \mathsf{Dec}(\rho_{\mathsf{sk}},\mathsf{ct}) = \mu : (\mathsf{pk},\rho_{\mathsf{sk}}) \leftarrow \mathsf{KeyGen}(\mathsf{mpk})\\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk},\mu)\end{matrix}\right] \geq 1 - \mathsf{negl}(\lambda).$$

Reusability: The above decryption correctness should hold for an arbitrary polynomial number of uses.

Verifying Deletion Correctness: There exists a negligible function $\mathsf{negl}(\cdot)$, for all $\lambda \in \mathbb{N}$:

$$\Pr\left[\begin{matrix}(\mathsf{mpk},\mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)\\ \mathsf{Valid} \leftarrow \mathsf{VerDel}(\mathsf{pk},\mathsf{td},\mathsf{cert}) : (\mathsf{pk},\rho_{\mathsf{sk}}) \leftarrow \mathsf{KeyGen}(\mathsf{mpk})\\ \mathsf{cert} \leftarrow \mathsf{Del}(\rho_{\mathsf{sk}})\end{matrix}\right] \geq 1 - \mathsf{negl}(\lambda).$$

Strong PKE-SKL Security In our work, we consider the strong PKE-SKL security defined in [CGJL23]. First, we specify the criteria for evaluating the success probability of a quantum decryptor.

Definition 13 (Testing a quantum decryptor). *Let $\gamma \in [0,1]$. Let pk be a public key and μ be a message. We refer to the following procedure as a test for a γ-good quantum decryptor with respect to pk and μ used in the following sampling procedure:*

- *The procedure takes as input a quantum decryptor ρ.*
- *Let $\mathcal{P} = (P, Q)$ be the following mixture of projective measurements (in terms of Definition 9) acting on some quantum state ρ:*
  - *Compute $\mathsf{ct}_0 \leftarrow \mathsf{Enc}(\mathsf{pk}, \mu)$, the encryption of message $\mu \in \{0,1\}$.*
  - *Compute $\mathsf{ct}_1 \leftarrow \mathcal{C}$, a random ciphertext from the possible space of all ciphertexts for 1-bit messages.*
  - *Sample a uniform $c \leftarrow \{0,1\}$.*
  - *Run the quantum decryptor ρ on input ct_c. Check whether the outcome is c. If so, output 1, otherwise output 0.*
- *Let $\mathsf{TI}_{1/2+\gamma}(\mathcal{P})$ be the threshold implementation of $\mathcal{P}$ with threshold value $\frac{1}{2}+\gamma$, as defined in Definition 10. Run $\mathsf{TI}_{1/2+\gamma}(\mathcal{P})$ on ρ, and output the outcome. If the output is 1, we say that the test passed, otherwise the test failed.*

Given that every binary outcome POVM $\mathcal{P} = (P, Q)$ possesses a threshold implementation $\mathsf{TI}_\gamma(\mathcal{P})$ for any γ, according to [ALL+21, Lemma 5.2], the following corollary holds.

Corollary 2 (γ-good Decryptor). *Let $\gamma \in [0,1]$. Let ρ be a quantum decryptor. Let $\mathsf{TI}_{1/2+\gamma}(\mathcal{P})$ be the test for a γ-good decryptor defined above. Then, the post-measurement state conditioned on output 1 is a mixture of states which are in the span of all eigenvectors of P with eigenvalues at least $1/2+\gamma$.*

Now we recall the definition of the strong γ-anti-piracy game.

Definition 14 (γ-Strong Secure Key Leasing Security Game). *Let $\lambda \in \mathbb{N}^+$, and $\gamma \in [0,1]$. The strong γ-PKE-SKL game is defined as the following game between a challenger and an adversary $\mathcal{A}$.*

1. *The challenger runs $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{td})$. It sends mpk to the adversary $\mathcal{A}$. $\mathcal{A}$ computes $(\mathsf{pk}, \rho_{\mathsf{sk}}) \leftarrow \mathsf{KeyGen}(\mathsf{mpk})$ and publishes pk.*
2. *The challenger requests that $\mathcal{A}$ runs the deletion algorithm $\mathsf{Del}(\rho_{\mathsf{sk}})$. $\mathcal{A}$ returns a deletion certificate cert to the challenger.*
3. *The challenger runs $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert})$ and continues if $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert})$ returns Valid; else it outputs $\perp$ and aborts, if $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert})$ returns $\mathsf{Invalid}$.*
4. *$\mathcal{A}$ outputs a message μ and a (possibly mixed) state ρ_{Del} as a quantum decryptor.*
5. *The challenger runs the test for a γ-good decryptor on ρ_{Del} with respect to pk and μ. The challenger outputs 1 if the test passes, otherwise outputs 0.*

We let $\mathsf{StrongSKL}(1^\lambda, \gamma, \mathcal{A})$ denote the output of the game.

Definition 15 (Strong PKE-SKL Security). *Let $\gamma : \mathbb{N}^+ \to [0,1]$. A secure key leasing scheme satisfies strong γ-SKL security, if for any QPT adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for all $\lambda \in \mathbb{N}$:*

$$\Pr\left[b = 1, b \leftarrow \mathsf{StrongSKL}(1^\lambda, \gamma(\lambda), \mathcal{A})\right] \leq \mathsf{negl}(\lambda) \tag{15}$$

C.2 Correctness Analysis

In this subsection, we prove the correctness of our PKE-SKL scheme described in Construction 1.

Proof (Proof of Lemma 7). In the quantum state Eqn.(11), we consider

$$\begin{aligned} y' =& \mathbf{v}_{inv} \cdot \mathsf{ct} \cdot \mathbf{v}_{sk} \\ =& \underbrace{\mathbf{v}_{inv} \left(\mathbf{R} \sum_{i \in [N]} \mathbf{U}_i \mathbf{e}'_i + \mathbf{R}\hat{\mathbf{e}}_1 \right)}_{e_{Dec}} + \mu \lfloor \frac{q}{2} \rfloor \end{aligned}$$

Since $|e_{Dec}| \leq 2B \cdot m' \cdot \lfloor \log q \rfloor \leq \frac{q}{4}$, The result follows directly. □

We now proceed with the proof of verifying deletion correctness for algorithm VerDel in Construction 1.

Proof (Proof of Lemma 8). Consider the quantum state in the procedure of KeyGen:

$$|\varphi_i\rangle = \frac{1}{\sqrt{2q^n}} \sum_{\substack{b_i\in\{0,1\},\\ \mathbf{x}_i\in\mathbb{Z}_q^n,\\ \mathbf{e}_i\mathbb{Z}_q^m}} \sqrt{D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{e}_i)}|b_i,\mathbf{x}_i\rangle|\mathbf{e}_i+\mathbf{A}_i\mathbf{x}_i+b_i\cdot(\mathbf{A}_i\mathbf{s}_i+\mathbf{e}_{0,i})\rangle.$$

and the quantum state below:

$$|\varphi_i'\rangle = \frac{1}{\sqrt{2q^n}} \sum_{\substack{b_i\in\{0,1\},\\ \mathbf{x}_i\in\mathbb{Z}_q^n,\\ \mathbf{e}_i\mathbb{Z}_q^m}} \sqrt{D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{e}_i)}|b_i,\mathbf{x}_i\rangle|\mathbf{e}_i+\mathbf{A}_i\mathbf{x}_i+b_i\cdot\mathbf{A}_i\mathbf{s}_i\rangle.$$

The trace distance between these two quantum states can be bounded according to the Lemma 9 by $\sqrt{1-(1-H^2(D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}},D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}+\mathbf{e}_{0,i})^2}$. Referring to our selection of parameters, $H^2(D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}},D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}+\mathbf{e}_{0,i})\leq\frac{1}{50}$, hence the distance between these two quantum states is at most 0.199.

On the other hand, for the quantum state

$$|\varphi_i'\rangle = \frac{1}{\sqrt{2q^n}} \sum_{\substack{b_i\in\{0,1\},\\ \mathbf{x}_i\in\mathbb{Z}_q^n,\\ \mathbf{e}_i\mathbb{Z}_q^m}} \sqrt{D_{\mathbb{Z}^m,\sigma,2\sigma\sqrt{m}}(\mathbf{e}_i)}|b_i,\mathbf{x}_i\rangle|\mathbf{e}_i+\mathbf{A}_i\mathbf{x}_i+b_i\cdot\mathbf{A}_i\mathbf{s}_i\rangle.$$

After measuring the last register and obtaining measurement $\mathbf{y}_i' = \mathbf{A}_i\mathbf{x}_i' + \mathbf{e}_i'$, the quantum state collapses to

$$|\varphi_i''\rangle = \frac{1}{\sqrt{2}}(|0,\mathbf{x}_i'\rangle + |1,\mathbf{x}_i'-\mathbf{s}_i\rangle) = \frac{1}{\sqrt{2}}\sum_{b_i\in\{0,1\}}|b_i,\mathbf{x}_{i,b_i}'\rangle.$$

Consider $\mathbf{x}_i'$ and $\mathbf{x}_i'-\mathbf{s}_i$ as $n\lceil\log q\rceil$-dimensional binary vectors and apply a Hadamard transform to all $n\lceil\log q\rceil+1$ qubits in the first two registers. The quantum state will turn into:

$$\begin{aligned}|\varphi_i'''\rangle =& 2^{-\frac{n\lceil\log q\rceil+2}{2}} \sum_{\substack{\mathbf{d}\in\{0,1\}^{n\lceil\log q\rceil}\\ b_i\in\{0,1\}\\ u\in\{0,1\}}} (-1)^{\mathbf{d}\cdot\mathcal{J}(\mathbf{x}_{b_i}')\oplus ub_i}|u\rangle|\mathbf{d}\rangle \\ =& 2^{-\frac{n\lceil\log q\rceil}{2}} \sum_{\mathbf{d}\in\{0,1\}^{n\lceil\log q\rceil}} (-1)^{\mathbf{d}\cdot\mathcal{J}(\mathbf{x}_0)}|\mathbf{d}^{\mathrm{T}}\cdot(\mathcal{J}(\mathbf{x}_i')\oplus\mathcal{J}(\mathbf{x}_i'-\mathbf{s}_i))\rangle|\mathbf{d}\rangle\end{aligned}$$

Measure the two registers and get a pair $(u,\mathbf{d})\in\mathbb{Z}_2\times\mathbb{Z}_2^{n\lceil\log q\rceil}$, it must satisfy that $u=\mathbf{d}\cdot(\mathcal{J}(\mathbf{x}_i')\oplus\mathcal{J}(\mathbf{x}_i'-\mathbf{s}_i)$. Therefore if we do the same procedure on the quantum state $|\varphi_i\rangle$ and get another pair $(\bar{u},\bar{\mathbf{d}})\in\mathbb{Z}_2\times\mathbb{Z}_2^{n\lceil\log q\rceil}$, the probability that $(\bar{u},\bar{\mathbf{d}})$ satisfies $\bar{u}=\bar{\mathbf{d}}^{\mathrm{T}}\cdot(\mathcal{J}(\mathbf{x}_i')\oplus\mathcal{J}(\mathbf{x}_i'-\mathbf{s}_i)$ is at least 0.801. Applying the Chernoff bound, for all $i\in[N]$, the number of i such that $|\varphi_i\rangle$ pass the

test, which we can simply denote as N' and its expectation can be denoted as $pN \geq 0.8N$, satisfying that:

$$\begin{aligned}\Pr[N' \leq 0.78N] =& \Pr[N' \leq (1-(1-\frac{0.78}{p})pN)] \\ \leq& e^{-\left(1-\frac{0.78}{p}\right)^2 \frac{pN}{2}} \\ \leq& \left. e^{-\left(1-\frac{0.78}{p}\right)^2 \frac{pN}{2}} \right|_{p=0.8},\end{aligned}$$

where the last probability is less than $e^{-0.01N} = e^{-0.01\lambda}$. Therefore, with the proper parameter selection and honestly prepared $\{\mathbf{y}_i\}_{i\in[N]}$ and secret key ρ_{sk}, the probability passing the algorithm VerDel is overwhelming. □

C.3 Resolution of the dependency issue

In this subsection, we address another noise flooding issue appearing in [CGJL23], which is used for statistically hiding $\mathbf{Re}$ to ensure the term $\mathbf{RA}$ to be independently random. To avoid noise flooding, we first perturb $\mathbf{e}$ by a random $\mathbf{e}_1$ with the same size of $\mathbf{e}$ such that $\mathbf{e}+\mathbf{e}_1$ could have many (random) positions of 0's. Then the corresponding components in $\mathbf{R}$ will not be leaked by $\mathbf{R}(\mathbf{e}+\mathbf{e}_1)$ and the term $\mathbf{RA}$ will again be promised to be random, but without a noise flooding.

For a finite set $\mathcal{S}$, we denote $\mathcal{P}(\mathcal{S})$ the power set of the set $\mathcal{S}$, which is the set containing all subsets of $\mathcal{S}$. We first show that the positions of 0's in $\mathbf{e}+\mathbf{e}_1$ are independent from $\mathbf{e}$.

Lemma 20. *φ is an arbitrary distribution over $[-B,B]^{m'}$, $\mathbf{e} \hookleftarrow \varphi$ and $\mathbf{e}_1 \xleftarrow{\$} [-B,B]^{m'}$ uniformly selected from the set $[-B,B]^{m'}$. Let $\mathcal{Z} \subset [m']$ the biggest set that for all $j \in \mathcal{Z}$, $(\mathbf{e}+\mathbf{e}_1)^{(j)} = 0$, where we use $\mathbf{a}^{(j)}$ to denote the j-th entry of the vector $\mathbf{a}$. We denote the distribution of $\mathcal{Z}$ over $\mathcal{P}([m'])$ as $\mathcal{V}_{\mathcal{Z}}$. Then $\mathcal{Z}$ is independent from $\mathbf{e}$.*

Proof (Proof of Lemma 20). In order to prove the independence between variable $\mathbf{e}$ and variable $\mathcal{Z}$, we only need to prove for $\mathbf{e} \hookleftarrow \varphi$ and $\mathcal{Z} \hookleftarrow \mathcal{V}_{\mathcal{Z}}$, $\Pr[\mathbf{e} = \mathbf{a}, \mathcal{Z} = \mathcal{Z}_1] = \Pr[\mathbf{e} = \mathbf{a}] \cdot \Pr[\mathcal{Z} = \mathcal{Z}_1]$.

$$\begin{aligned}&\Pr[\mathcal{Z} = \mathcal{Z}_1, \text{ where } \mathcal{Z} \hookleftarrow \mathcal{V}_{\mathcal{Z}}] \\ =& \sum_{\mathbf{a}\in[-B,B]^{m'} \bigcap \mathbb{Z}^{m'}} \Pr[\mathbf{e}_{1,\mathcal{Z}_1} = -\mathbf{a}_{\mathcal{Z}_1} \& \mathbf{e}_1^{(j)} \neq \mathbf{a}^{(j)} \text{ for } \forall j \in \overline{\mathcal{Z}}_1] \cdot \Pr[\mathbf{e} = \mathbf{a}] \\ =& \sum_{\mathbf{a}\in[-B,B]^{m'}} \frac{1}{(2B+1)^{\#\mathcal{Z}_1}} \cdot \frac{(2B)^{m'-\#\mathcal{Z}_1}}{(2B+1)^{m'-\#\mathcal{Z}_1}} \cdot \Pr[\mathbf{e} = \mathbf{a}] \\ =& \frac{1}{(2B+1)^{\#\mathcal{Z}_1}} \cdot \frac{(2B)^{m'-\#\mathcal{Z}_1}}{(2B+1)^{m'-\#\mathcal{Z}_1}} \cdot \sum_{\mathbf{a}\in[-B,B]^{m'}} \Pr[\mathbf{e} = \mathbf{a}] \\ =& \frac{1}{(2B+1)^{\#\mathcal{Z}_1}} \cdot \frac{(2B)^{m'-\#\mathcal{Z}_1}}{(2B+1)^{m'-\#\mathcal{Z}_1}}.\end{aligned}$$

Therefore, for $\mathbf{e} \hookleftarrow \varphi$ and $\mathcal{Z} \hookleftarrow \mathcal{V}_{\mathcal{Z}}$, we have

$$\begin{aligned}
&\Pr[\mathbf{e} = \mathbf{a} \,\&\mathcal{Z} = \mathcal{Z}_1, \text{ where } \mathbf{e} \hookleftarrow \varphi \text{ and } \mathcal{Z} \hookleftarrow \mathcal{V}_{\mathcal{Z}}] \\
=& \Pr[\mathbf{e} = \mathbf{a} \& \mathbf{e}_{1,\mathcal{Z}_1} = -\mathbf{a}_{\mathcal{Z}_1} \& \mathbf{e}_1^{(j)} \neq \mathbf{a}^{(j)} \text{ for } \forall j \in \overline{\mathcal{Z}}_1] \\
=& \Pr[\mathbf{e} = \mathbf{a}] \cdot \Pr[\mathbf{e}_{1,\mathcal{Z}_1} = -\mathbf{a}_{\mathcal{Z}_1} \& \mathbf{e}_1^{(j)} \neq \mathbf{a}^{(j)} \text{ for } \forall j \in \overline{\mathcal{Z}}_1] \\
=& \Pr[\mathbf{e} = \mathbf{a}] \cdot \Pr[\mathbf{e}_{1,\mathcal{Z}_1} = -\mathbf{a}_{\mathcal{Z}_1}] \cdot \Pr[\mathbf{e}_1^{(j)} \neq \mathbf{a}^{(j)} \text{ for } \forall j \in \overline{\mathcal{Z}}_1] \\
=& \Pr[\mathbf{e} = \mathbf{a}] \cdot \frac{1}{(2B+1)^{\#\mathcal{Z}_1}} \cdot \frac{(2B)^{m' - \#\mathcal{Z}_1}}{(2B+1)^{m' - \#\mathcal{Z}_1}} \\
=& \Pr[\mathbf{e} = \mathbf{a}] \cdot \Pr[\mathcal{Z} = \mathcal{Z}_1].
\end{aligned}$$

In other words, the variable $\mathbf{e}$ over the distribution φ and the variable $\mathcal{Z}$ over the distribution $\mathcal{V}_{\mathcal{Z}}$ are independent of each other. □

For a clearer proof of the following lemma, we define the submatrix of any matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ as follows: For $\mathcal{S}_1 \subset [m]$ and $\mathcal{S}_2 \subset [n]$, define $\mathbf{A}_{\mathcal{S}_1 \times \mathcal{S}_2}$ as the concatenation of all elements $A_{i,j}$ of $\mathbf{A}$ satisfying $i \in \mathcal{S}_1$ and $j \in \mathcal{S}_2$. Now we are ready to prove the main lemma, which is heavily used in the proof for the security of our PKE-SKL scheme.

Lemma 21. *For an integer $k \leq q$, a random matrix $\mathbf{A} \in \mathbb{Z}_q^{m' \times n}$ and a vector $\mathbf{e} \in \mathbb{Z}_q^{m'}$ related to $\mathbf{A}$ and satisfying $\|\mathbf{e}\|_\infty \leq B$, select $\mathbf{e}_1 \xleftarrow{\$} [-B, B]^{m'}$ satisfying $m'/B = \omega(n \log q)$, $\mathbf{R} \xleftarrow{\$} \{0,1\}^{k \times m'}$. The distribution of $(\mathbf{A}, \mathbf{RA}, \mathbf{R}(\mathbf{e} + \mathbf{e}_1))$ is statistically close to $(\mathbf{A}, \mathbf{B}, \mathbf{R}(\mathbf{e} + \mathbf{e}_1))$, where $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{k \times n}$. Furthermore the statistical distance is at most $k \cdot 2^{-\omega(n \log q)} = 2^{-\omega(n \log q)}$.*

Proof (Proof of Lemma 21). We use the hybrid argument to argue the lemma.

In **Hybrid 0**, the distribution is:

$$\mathcal{D}_0 = \left\{ (\mathbf{A}, \mathbf{RA}, \mathbf{R}(\mathbf{e} + \mathbf{e_1})) \;\middle|\; \begin{array}{l} \mathbf{A} \xleftarrow{\$} \mathbf{Z}_q^{m' \times n}, \mathbf{e} \hookleftarrow \mathcal{D}_{\mathbf{A}}, \\ \mathbf{R} \xleftarrow{\$} \{0,1\}^{k \times m'}, \mathbf{e}_1 \xleftarrow{\$} [-B, B] \end{array} \right\},$$

where $\mathbf{e} \hookleftarrow \mathcal{D}_{\mathbf{A}}$ means the distribution of $\mathbf{e}$ is dependent on the value of matrix $\mathbf{A}$.

This distribution is identical to the first distribution in the lemma. If we want to replace $\mathbf{RA}$ with a real random matrix $\mathbf{B} \in \mathbb{Z}_q^{k \times n}$, we cannot apply the general leftover hash lemma directly because $\mathbf{e} \hookleftarrow \mathcal{D}_{\mathbf{A}}$ is related to the matrix $\mathbf{A}$. Therefore we need to consider the influence of $\mathbf{e}$ in the third term.

As to the vector $\mathbf{e} + \mathbf{e}_1$, for a selected $\mathbf{A}$, we denote $\mathbf{e}' = \mathbf{e} + \mathbf{e}_1$ and $\mathcal{Z} \subset [m']$ the biggest set that for all $j \in \mathcal{Z}$, $(\mathbf{e} + \mathbf{e}_1)^{(j)} = 0$, where we use $\mathbf{a}^{(j)}$ to denote the j-th entry of the vector $\mathbf{a}$. Since $\mathbf{e}_1 \xleftarrow{\$} [-B, B]^{m'}$, each $i \in [m']$ has the same probability that $(\mathbf{e} + \mathbf{e}_1)^{(i)} = 0$, which is equal to $\frac{1}{2B+1}$. According to the Chernoff bound,

$$\Pr[\#\mathcal{Z} \leq \frac{m'}{4B+2}] \leq e^{-\frac{m'}{16B+8}} = e^{-\omega(n \log q)} = \mathsf{negl}(\lambda),$$

and

$$\Pr[\#\mathcal{Z} \geq \frac{3m'}{4B+2}] \leq e^{-\frac{m'}{20B+10}} = e^{-\omega(n\log q)} = \mathsf{negl}(\lambda),$$

where $\#\mathcal{Z}$ is the size of this finite set. Therefore the probability that $\#\mathcal{Z} \geq \frac{m'}{4B+2}$ and $\#\mathcal{Z} \leq \frac{3m'}{4B+2}$ is overwhelming.

We denote $\overline{\mathcal{Z}}$ as the complementary set of $\mathcal{Z}$ in $[m']$, and it follows directly that $\mathcal{D}_0$ can be rewritten as

$$\mathcal{D}_0 = \left\{ \begin{array}{l} (\mathbf{A}, \mathbf{R}_{[k]\times\mathcal{Z}}\mathbf{A}_{\mathcal{Z}\times[n]} + \mathbf{R}_{[k]\times\overline{\mathcal{Z}}}\mathbf{A}_{\overline{\mathcal{Z}}\times[n]}, \\ \mathbf{R}_{[k]\times\overline{\mathcal{Z}}}(\mathbf{e}+\mathbf{e_1})_{\overline{\mathcal{Z}}\times[1]}) \end{array} \middle| \begin{array}{l} \mathbf{A} \xleftarrow{\$} \mathbf{Z}_q^{m'\times n}, \mathbf{e} \hookleftarrow \mathcal{D}_{\mathbf{A}}, \\ \mathbf{R} \xleftarrow{\$} \{0,1\}^{k\times m'}, \mathbf{e}_1 \xleftarrow{\$} [-B,B] \end{array} \right\},$$

and according to Lemma 20, $\mathcal{Z}$ is independent from $\mathbf{e}$, therefore we can use leftover hash lemma directly on the term $\mathbf{R}_{[k]\times\mathcal{Z}}\mathbf{A}_{\mathcal{Z}\times[n]}$, and this term can be replaced by a random matrix $\mathbf{B}$. It follows that the distribution $\mathcal{D}_0$ is statistically close to the distribution below:

$$\mathcal{D}_0' = \left\{ \begin{array}{l} (\mathbf{A}, \mathbf{B} + \mathbf{R}_{[k]\times\overline{\mathcal{Z}}}\mathbf{A}_{\overline{\mathcal{Z}}\times[n]}, \\ \mathbf{R}_{[k]\times\overline{\mathcal{Z}}}(\mathbf{e}+\mathbf{e_1})_{\overline{\mathcal{Z}}\times[1]}) \end{array} \middle| \begin{array}{l} \mathbf{A} \xleftarrow{\$} \mathbf{Z}_q^{m'\times n}, \mathbf{e} \hookleftarrow \mathcal{D}_{\mathbf{A}}, \mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{k\times n} \\ \mathbf{R} \xleftarrow{\$} \{0,1\}^{k\times m'}, \mathbf{e}_1 \xleftarrow{\$} [-B,B] \end{array} \right\}.$$

Furthermore, according to Leftover Hash Lemma, the statistical distance between these two distributions is at most $k\frac{q^n}{2^{\#\overline{\mathcal{Z}}}} \leq \frac{q^{n+1}}{2^{\#\overline{\mathcal{Z}}}} = 2^{-\omega(n\log q)}$.

Since $\mathbf{B}$ is selected independently from $\mathbf{Z}_q^n$, the influence of the term $\mathbf{R}_{[k]\times\overline{\mathcal{Z}}}\mathbf{A}_{\overline{\mathcal{Z}}\times[n]}$ will be dismissed and the distribution above will be identical to the following distribution $\mathcal{D}_2$.

In **Hybrid 2**, the distribution is:

$$\mathcal{D}_2 = \left\{ (\mathbf{A}, \mathbf{B}, \mathbf{R}(\mathbf{e}+\mathbf{e_1})) \middle| \begin{array}{l} \mathbf{A} \xleftarrow{\$} \mathbf{Z}_q^{m'\times n}, \mathbf{e} \hookleftarrow \mathcal{D}_{\mathbf{A}}, \mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{k\times n} \\ \mathbf{R} \xleftarrow{\$} \{0,1\}^{k\times m'}, \mathbf{e}_1 \xleftarrow{\$} [-B,B] \end{array} \right\},$$

which is identical to the second distribution in this lemma. Therefore two distribution $\mathcal{D}_0$ and $\mathcal{D}_2$ are statistically close and the statistical distance is at most $k \cdot 2^{-\omega(n\log q)} = 2^{-\omega(n\log q)}$. □

C.4 Security Analysis for SKL-PKE

The proof of Theorem 6 directly follows by combining Lemmata 22 and 23, which we state and prove next.

Note that the $\mathbf{Hybrid}_0$ described in Fig. 7 corresponds to the real security game whereas $\mathbf{Hybrid}_1$ described in Fig. 8 is a corresponding modified game.

Lemma 22. *The following* $\mathbf{Hybrid}_0$ *and* $\mathbf{Hybrid}_1$ *are indistinguishable and the winning probability in these two hybrids is negligibly close.*

Fig. 7. Hybrid 0

Hybrid 0

In this hybrid, the adversary and the challenger play the security game as in Definition 14.

1. The challenger runs $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{td})$. It sends mpk to the adversary $\mathcal{A}$. $\mathcal{A}$ computes $(\mathsf{pk}, \rho_{\mathsf{sk}}) \leftarrow \mathsf{KeyGen}(\mathsf{mpk})$ and publishes pk.
2. The challenger requests that $\mathcal{A}$ runs the deletion algorithm $\mathsf{Del}(\rho_{\mathsf{sk}})$. $\mathcal{A}$ returns a deletion certificate cert to the challenger.
3. The challenger runs $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert})$ and continues if $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert})$ returns Valid; else it outputs $\perp$ and aborts, if $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert})$ returns $\mathsf{Invalid}$.
4. $\mathcal{A}$ outputs a message μ and a (possibly mixed) state ρ_{Del} as a quantum decryptor.
5. The challenger runs the test for a γ-good decryptor on ρ_{Del} with respect to pk and μ (using $\mathsf{TI}_{1/2+\gamma}(\mathcal{P}_{\mathcal{D}})$). The challenger outputs 1 if the test passes, otherwise outputs 0.

Proof (Proof of Lemma 22). This lemma follows from Lemma 16. If the inefficient γ-good decryptor test outputs 1 with probability p on a state ρ, then the efficient $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D},1/2+\gamma-\epsilon}$ will output 1 on the state ρ with probability $p - \delta$. Since δ is negligible, $\mathcal{A}$'s overall winning probability will have a negligible difference. □

According to Lemma 22, if we can demonstrate that the winning probability for $\mathbf{Hybrid}_1$ is negligible, then we can infer that the winning probability for$\mathbf{Hybrid}_0$ is negligible. Thus, the key to proving Theorem 6 is to show that $\Pr[\mathbf{Hybrid}_1 = 1] \leq \mathsf{negl}(\lambda)$ for some negligible $\mathsf{negl}(\lambda)$, as described in the following Lemma 23.

Lemma 23. *Assuming post-quantum hardness of* $\mathsf{LWE}_{n,m,q,\sigma_0}$ *with parameter choice in Construction 1, we have* $\Pr[\mathbf{Hybrid}_1 = 1] \leq \mathsf{negl}(\lambda)$ *for some negligible* $\mathsf{negl}(\cdot)$.

C.5 Proof for Lemma 23

Similar to [CGJL23], to prove the Lemma 23, we first make a few notations for the events that take place in $\mathbf{Hybrid}_1$:

- **Event** CertPass: We denote the event that the adversary hands in a valid deletion certificate $\mathsf{cert} = \{(u_i, \mathbf{d}_i)\}_{i=1}^N$ such that $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert}) = \mathsf{Valid}$, as CertPass.
- **Event** GoodDecryptor: We denote the event that test $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma+1/2}(\rho_{\mathsf{Del}})$ outputs 1 with respect to μ and pk, as GoodDecryptor. When this event happens, we say that an adversary could produce a state ρ_{Del} for which

Fig. 8. Hybrid 1

Hybrid 1

In this hybrid, we replace the check for γ good decryptor with an efficient check $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma}$ where we set δ and ϵ to be $\lambda^{-\omega(1)}$ for a tiny super-constant $\omega(1)$, e.g. we can set δ to be exponentially small and $\epsilon = \frac{\gamma}{100Nnq}$ [a].

1. The challenger runs $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{td})$. It sends mpk to the adversary $\mathcal{A}$. $\mathcal{A}$ computes $(\mathsf{pk}, \rho_{\mathsf{sk}}) \leftarrow \mathsf{KeyGen}(\mathsf{mpk})$ and publishes pk.
2. The challenger requests that $\mathcal{A}$ runs the deletion algorithm $\mathsf{Del}(\rho_{\mathsf{sk}})$. $\mathcal{A}$ returns a deletion certificate cert to the challenger.
3. The challenger runs $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert})$ and if $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert})$ returns Valid it outputs z; else it outputs $\perp$ if $\mathsf{VerDel}(\mathsf{pk}, \mathsf{td}, \mathsf{cert})$ returns $\mathsf{Invalid}$.
4. $\mathcal{A}$ outputs a message μ and a (possibly mixed) state ρ_{Del} as a quantum decryptor.
5. The challenger runs the test $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma+1/2-\epsilon}(\rho_{\mathsf{Del}})$ with respect to μ and pk. The challenger sets $z = 1$ if the test passes, otherwise it sets $z = 0$.

[a] Here, we can choose $\epsilon = \frac{\gamma}{cNnq}$ for any constant $c > 6$. Looking ahead, this is to ensure that after $2Nnq$ times of measurements, the advantage is still at least $\gamma - 3\epsilon \cdot 2Nnq = (1 - \frac{6}{c})\gamma$, where 3ϵ is due to Lemma 16. To ease comparison, we set $c = 100$, as used in [CGJL23].

the test of good decryptor $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma+1/2}$ for some noticeable γ passes with inverse-polynomial probability. Namely, a successful attacker can distinguish ciphertexts from randomly chosen ciphertexts.

– **Event** Ext: We denote Ext as the event where we can obtain the preimages $\{\mathbf{x}_{i,b_i}\}_{i\in[N]} \in \{\mathrm{INV}(\mathsf{td}_i, b_i \in \{0,1\}, \mathbf{y}_i)\}_{i\in[N]}$(from the remaining state of measurement $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma+1/2}(\rho_{\mathsf{Del}})$).

We will prove Lemma 23 by contradiction. Suppose the probability that final output 1 in $\mathbf{Hybrid}_1$ is some noticeable ϵ, i.e. $\Pr[\mathbf{Hybrid}_1 = 1] \geq \epsilon$, this means we must have $\Pr[\mathsf{CertPass} \wedge \mathsf{GoodDecryptor}] \geq \epsilon_1$ for noticeable ϵ_1. The main proof is to build a reduction that breaks the amplified adaptive hardcore bit security of parallel repeated NNTCF. In other words, we need the following statement to hold: $\Pr[\mathsf{CertPass} \wedge \mathsf{Ext}] \geq \epsilon'$ for some noticeable ϵ' when $\Pr[\mathsf{CertPass} \wedge \mathsf{GoodDecryptor}] \geq \epsilon_1$. In this case, the reduction can efficiently obtain both the deletion certificates $\{u_i, \mathbf{d}_i\}_{i\in[N]}$ and the preimages $\{\mathbf{x}_{i,b_i}\}_{i\in[N]}$, which allows it to break the amplified adaptive hardcore property of NNTCF.

The outline of our proof of Lemma 23 is as follows. Assume that $\Pr[\mathbf{Hybrid}_1 = 1] \geq \epsilon$ for noticeable ϵ, namely the adversary wins the γ-strong SKL-PKE game in Definition 15. This means $\Pr[\mathsf{CertPass} \wedge \mathsf{GoodDecryptor}] \geq \epsilon_1$ for noticeable ϵ_1. To prove $\Pr[\mathsf{CertPass} \wedge \mathsf{Ext}] \geq \epsilon'$, we need an important intermediate argument:

$$\Pr[\mathsf{Ext}|\mathsf{GoodDecryptor}] \geq 1 - \mathsf{negl}(\lambda), \tag{16}$$

which means when $\mathsf{GoodDecryptor}$ happens, Ext *always happens* except with negligible probability. If this event holds, by a simple probability calculation (Lemma 10), it holds that, for any noticeable ϵ_1,

$$\begin{aligned}\Pr[\mathsf{CertPass} \wedge \mathsf{Ext}] &\geq \Pr[\mathsf{Ext}|\mathsf{GoodDecryptor}] \cdot \Pr[\mathsf{CertPass} \wedge \mathsf{GoodDecryptor}] \\ &= (1 - \mathsf{negl}(\lambda)) \cdot \epsilon_1 = \epsilon_1 - \mathsf{negl}(\lambda).\end{aligned}$$

According to the amplified Adaptive Hardcore Bit property, for any LWE instance $(\mathbf{A}, \mathbf{As} + \mathbf{e}_0)$, if it is accessible to the preimage $(b, \mathbf{x}_b)$ for either $b \in \{0, 1\}$, the probability to give a pair $(u, \mathbf{d}) \in \mathbb{Z}_2 \times \mathbb{Z}_2^{n\lceil \log q \rceil}$ satisfying $u = \mathbf{d} \cdot \mathcal{J}(\mathbf{x}_0) \otimes \mathcal{J}(\mathbf{x}_1)$ is at most $\frac{1}{2} + \mathsf{negl}(\lambda)$. First, we consider the case that $0.78N$ is an integer, and hence in this case $\lceil 0.78N \rceil = 0.78N$. For a prefixed set of size-$0.78N$ indices, the probability to pass all tests over this prefixed set of indices is at most $(\frac{1}{2} + \mathsf{negl}(\lambda))^{0.78N}$. There are $\binom{N}{0.78N}$ choices of size-$0.78N$ set from N indices. Canonically, by union bound, we have:

$$\Pr[\mathsf{CertPass} \wedge \mathsf{Ext}] \leq \binom{N}{0.78N} \cdot (\frac{1}{2} + \mathsf{negl}(\lambda))^{0.78N}, \tag{17}$$

and

$$\begin{aligned}\log \binom{N}{\lceil 0.78N \rceil} =& \log(N!) - \log((0.78N)!) - \log((0.22N)!) \\ =& N \log N - N \log e + \mathcal{O}(\log N) \\ & -0.78N \log(0.78N) + 0.78N \log e + \mathcal{O}(\log N) \\ & -0.22N \log(0.22N) + 0.22 \log e + \mathcal{O}(\log N) \\ =& (-0.78 \log 0.78 - 0.22 \log 0.22)N + \mathcal{O}(\log N) \\ \leq& 0.761N + \mathcal{O}(\log N)\end{aligned}$$

Hence it follows:

$$\begin{aligned}\text{Eqn. (17)} \leq& c_{ce} 2^{0.761N} \cdot N \cdot ((\frac{1}{2})^{0.99})^{0.78N} \\ =& c_{ce} 2^{-0.0112N} N \\ =& \mathsf{negl}(\lambda),\end{aligned} \tag{18}$$

where c_{ce} is a constant.

Then we consider the case that $0.78N$ is not an integer. Since $\lceil 0.78N \rceil \leq 0.79N$ so there's an α such that $0.78 \leq \alpha \leq 0.79$ and $\lceil 0.78N \rceil = \alpha N$. The function $f(\alpha) = -\alpha \log_2 \alpha - (1 - \alpha) \log_2(1 - \alpha) - 0.99\alpha$ is illustrated in Fig. 9.

For $0.78 \leq \alpha \leq 0.79$, $f(\alpha) < 0$ and decrease strictly monotonically. Therefore in general case,

$$\begin{aligned}\Pr[\mathsf{CertPass} \wedge \mathsf{Ext}] \leq& \binom{N}{\lceil 0.78N \rceil} \cdot (\frac{1}{2} + \mathsf{negl}(\lambda))^{\lceil 0.78N \rceil} \\ \leq& c_{ce} \cdot N \cdot 2^{(-0.78 \log 0.78 - 0.22 \log 0.22 - 0.99 \times 0.78)N} \\ \leq& c_{ce} \cdot N \cdot 2^{-0.012N} \\ =& \mathsf{negl}(\lambda).\end{aligned}$$

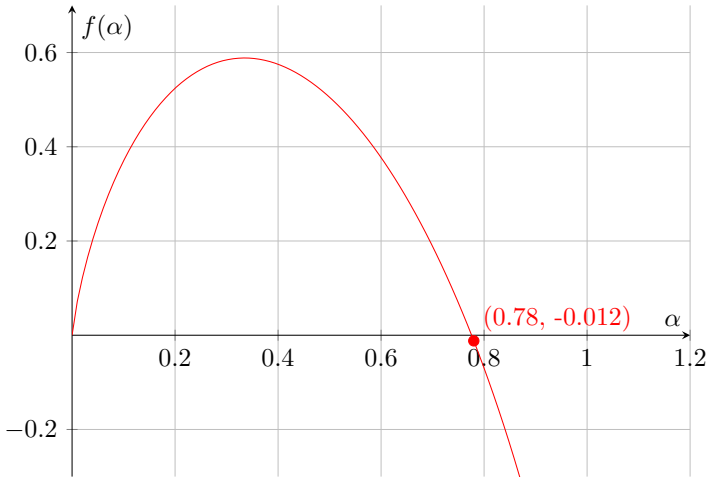

Fig. 9. Illustration for the function $f(\alpha) = -\alpha \log_2 \alpha - (1-\alpha)\log_2(1-\alpha) - 0.99\alpha$.

It leads to contradiction and proves the Lemma 23.

Next, we describe the event described in Eqn. (16) in a new world of $\mathbf{Hybrid}_1$, where the challenger does not perform the check on the deletion certificate and lets the adversary pass all the time, as shown in the following Game 0.

Game 0. This is an experiment the same as the one in $\mathbf{Hybrid}_1$, using the Construction 1, except that *the challenger does not perform the check on the deletion certificate*.

1. The challenger runs $\mathsf{Setup}(1^\lambda)$: the challenger prepares $\mathsf{mpk} = \{(\mathbf{A}_i, \mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i})\}_{i=1}^N$, where $(\mathbf{A}_i, \mathsf{td}_i) \leftarrow \textsc{GenTrap}(1^n, 1^m, q), \forall i \in [N]$ and sends it to $\mathcal{A}$. The challenger keeps $\mathsf{td} = \{\mathsf{td}_i\}_{i\in[N]}$.
2. $\mathcal{A}$ receives mpk and obtains the classical public key $\mathsf{pk} = \{(\mathbf{A}_i, \mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i}, \mathbf{y}_i)\}_{i\in[N]} \leftarrow \mathsf{KeyGen}(\mathsf{mpk})$ and one copy of quantum decryption key ρ_{sk}. $\mathcal{A}$ publishes pk.
3. $\mathcal{A}$ outputs a message μ and a (possibly mixed) state ρ_{Del} as a quantum decryptor.
4. The challenger runs the (efficient) test $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma+1/2}(\rho_{\mathsf{Del}})$ with respect to μ and pk. The challenger outputs 1 if the test passes, otherwise it outputs 0.

Next, we argue that in Game 0, if the game outputs 1, then there exists an extractor that extracts all preimages $\{\mathbf{x}_{i,b_i}\}_{i\in[N]}, b_i = 0$ or 1 for $\{\mathbf{y}_i\}_{i\in[N]}$. Let us denote $\mathcal{D}_0$ as the distribution used in ATI of Game 0, we have

Theorem 11. *Assume that post-quantum hardness of* $\mathsf{LWE}_{n,m,q,\sigma_0}$ *with parameter choice in Construction 1. In the Game* 0*, if we have* $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_0,1/2+\gamma}(\rho_{\mathsf{Del}}) = 1$*, for some noticeable* γ*, then there exists an polynomial-time extractor* Ext *such*

that there is a negligible function $\mathsf{negl}(\cdot)$*:*

$$\Pr\left[\begin{array}{c}\mathsf{Ext}(\rho_{\mathsf{Del}},\mathsf{pk})\to\{\mathbf{x}_{i,b_i}\}_{i\in[N]}\\ \mathbf{x}_{i,b_i}\in\mathrm{INV}(\mathsf{td}_i,b_i,\mathbf{y}_i)\end{array}:|\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_0,1/2+\gamma}(\rho_{\mathsf{Del}})=1\right]\geq 1-\mathsf{negl}(\lambda).$$

C.6 Proof for Theorem 11

To prove the Theorem 11, we show other games that are indistinguishable from game 0 as follows.

Game 1. This is the same as Game 0 except that all $\mathbf{A}_i$ are sampled uniformly at random, without a trapdoor.

1. The challenger runs $\mathsf{Setup}(1^\lambda)$: the challenger prepares $\mathsf{mpk}=\{(\mathbf{A}_i,\mathbf{A}_i\mathbf{s}_i+\mathbf{e}_{0,i})\}_{i=1}^N$, where $\mathbf{A}_i\xleftarrow{\$}\mathbb{Z}_q^{m\times n},\forall i\in[N]$ and sends it to $\mathcal{A}$.
2. $\mathcal{A}$ receives mpk and obtains the classical public key $\mathsf{pk}=\{(\mathbf{A}_i,\mathbf{A}_i\mathbf{s}_i+\mathbf{e}_{0,i},\mathbf{y}_i)\}_{i\in[N]}\leftarrow\mathsf{KeyGen}(\mathsf{mpk})$ and one copy of quantum decryption key ρ_{sk}. $\mathcal{A}$ publishes pk.
3. $\mathcal{A}$ outputs a message μ and a (possibly mixed) state ρ_{Del} as a quantum decryptor.
4. The challenger runs the (efficient) test $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma+1/2}(\rho_{\mathsf{Del}})$ with respect to μ and pk. The challenger outputs 1 if the test passes, otherwise it outputs 0.

Game 2.j. For $j=1,\cdots,N$, this is the same as Game 0 except for the following:

1. During $\mathsf{Setup}(1^\lambda)$,
   - For $i\leq j$: the challenger prepares $\mathsf{mpk}_i=(\mathbf{A}_i,\mathbf{u}_i)$, where $\mathbf{A}_i\xleftarrow{\$}\mathbb{Z}_q^{m\times n}$ and $\mathbf{u}_i\xleftarrow{\$}\mathbb{Z}_q^{m\times 1}$ uniformly random.
   - For $i>j$: the challenger prepares $\mathsf{mpk}_i=(\mathbf{A}_i,\mathbf{u}_i=\mathbf{A}_i\mathbf{s}_i+\mathbf{e}_{0,i})$ the same as in Game 0.
2. $\mathcal{A}$ receives mpk and obtains the classical public key $\mathsf{pk}=\{(\mathbf{A}_i,\mathbf{u}_i,\mathbf{y}_i)\}_{i\in[N]}$ and one copy of quantum decryption key ρ_{sk}. $\mathcal{A}$ publishes pk.
3. $\mathcal{A}$ outputs a message μ and a (possibly mixed) state ρ_{Del} as a quantum decryptor.
4. The challenger runs the (efficient) test $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma+1/2}(\rho_{\mathsf{Del}})$ with respect to μ and pk. The challenger outputs 1 if the test passes, otherwise it outputs 0.

Similar to [CGJL23], we have the following Lemma:

Lemma 24. *Assuming the hardness of* $\mathsf{LWE}_{n,m,q,\sigma_0}$*, Game 0 and Game* $2.N$ *are indistinguishable.*

The above lemma follows immediately from the following two claims.

Claim 1. *Given the property of* GenTrap *algorithm in Theorem 9, Game 0 and Game 1 are statistically indistinguishable.*

Claim 2. *Assuming the hardness of* $\mathsf{LWE}_{n,m,q,\sigma_0}$*, Game 1 and Game* $2.N$ *are indistinguishable.*

Proof (Proof of Claim 2). The claim holds because each pair in (Game 1, Game 2.1), (Game 2.1, Game 2.2) ... (Game 2.$(N-1)$, Game 2.N) is indistinguishable, assuming the hardness of LWE assumption. □

Let us denote $\mathcal{D}_{2.N}$ as the distribution used in ATI of Game 2.N. Building on the Lemma 24, it is known that the distribution $\mathcal{D}_0$ and distribution $\mathcal{D}_{2.N}$ are computationally indistinguishable. Thus, to prove the Theorem 11, we only need to prove the following theorem for Game 2.N.

Theorem 12. *In the last Game 2.N, if we have* $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma}(\rho_{\mathsf{Del}})$ *outputs 1, for some noticeable γ, then there exists an efficient extractor* Ext *such that there is a negligible function* $\mathsf{negl}(\cdot)$*:*

$$\Pr\left[\begin{array}{c}\mathsf{Ext}(\rho_{\mathsf{Del}},\mathsf{pk})\to\{\mathbf{x}_{i,b_i}\}_{i\in[N]}:\\ \mathbf{x}_{i,b_i}\in \mathrm{INV}(\mathsf{td}_i,b_i,\mathbf{y}_i)\end{array}\middle|\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma}(\rho_{\mathsf{Del}})=1\right]\geq 1-\mathsf{negl}(\lambda).$$

Claim 3. *By Lemma 17, due to the property of computationally indistinguishable* ATI*, Theorem 12 implies Theorem 11.*

C.7 Proof of Theorem 12 via "Noisy" Quantum Search-to-Decision Reduction

Similar to [CGJL23, Section 11], we prove the Theorem 12 by a "noisy" quantum search-to-decision reduction algorithm.

To enhance clarity, we remove the index b_i from the vector $\mathbf{x}_{i,b_i}$, as the specific values of $\mathbf{x}_{i,0}$ or $\mathbf{x}_{i,1}$ do not impact our analysis. Henceforth, the subscripts i,j in $x_{i,j}$ denote the j-th entry of the i-th vector $\mathbf{x}_i$. Next, for simplicity, we will focus on encrypting the message $\mu=0$. The analysis for the case $\mu=1$ should follow symmetrically.

Firstly, given three ATI's for different distributions $(\mathcal{D}_{2.N},\mathcal{D}(g_{\ell,j}),\mathcal{D}_{\mathsf{unif}})$.

(1) ATI ***for*** $\mathcal{D}_{2.N}$*:* $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma}$ is the approximate threshold implementation algorithm for the following mixture of projections $\mathcal{P}_{\mathcal{D}_{\mathsf{ct}}}$, acting on the state ρ_{Del}:

- Compute $\mathsf{ct}_0\leftarrow\mathsf{Enc}(\mathsf{pk},0)$ *in Game* 2.N. Here $\mathsf{ct}_0=(\mathsf{ct}^{(1)}|\mathsf{ct}^{(2)}|\mathsf{ct}^{(3)})$ can be seen as column concatenation of the following three components:
  - $\mathsf{ct}^{(1)}=\{\mathbf{R}\mathbf{U}_i\mathbf{A}_i\}_{i\in[N]}$
  - $\mathsf{ct}^{(2)}=\{\mathbf{R}\mathbf{U}_i\mathbf{u}_i\}_{i\in[N]}$
  - $\mathsf{ct}^{(3)}=\sum_{i\in[N]}(\mathbf{R}\mathbf{U}_i\mathbf{e}'_i+\mathbf{R}\mathbf{U}_i\mathbf{A}_i\mathbf{x}_i+b_i\cdot\mathbf{R}\mathbf{U}_i\mathbf{u}_i)+\mathbf{R}\hat{\mathbf{e}}_1$

  where $\{\mathbf{A}_i,\mathbf{u}_i,\mathbf{y}_i\}_{i\in[N]}$ are given in the public key pk; $\mathbf{U}_i\xleftarrow{\$}\{0,1\}^{m'\times m}$, $\mathbf{R}\hookleftarrow\{0,1\}^{m'\times m'}$; $\hat{\mathbf{e}}_1=\sum_{i\in[N]}\hat{\mathbf{e}}_{1,i}$, and $\hat{\mathbf{e}}_{1,i}\xleftarrow{\$}[-B,B]^{m'}$ with $B=(\sigma+\sigma_0)\sqrt{\lambda}\cdot m$. Note that $b_i=0$ or 1, is an adversarially chosen bit that come in the $\mathbf{y}_i$ part of pk.
- Compute $\mathsf{ct}_1\leftarrow\mathcal{C}$, a random ciphertext from the possible space of all ciphertexts for 1-bit messages.
- Sample a uniform bit $c\leftarrow\{0,1\}$.
- Run the quantum decryptor ρ on input ct_c. Check whether the outcome is c. If so, output 1, otherwise output 0.

(2) ATI ***for*** $\mathcal{D}(g_{\ell,j})$*:* We then consider a second approximate threshold implementation $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}(g_{\ell,j}),1/2+\gamma}$. Here $\mathcal{P}_{\mathcal{D}(g_{\ell,j})}$ is the following mixture of measurements (we denote the following distribution we sample from as $\mathcal{D}(g_{\ell,j})$):

- Let $g_{\ell,j}$ be a guess for the j-th entry in vector $\mathbf{x}_\ell \in \{\mathbf{x}_1, \cdots, \mathbf{x}_N\}$.
- Sample a random $\mathbf{c} \leftarrow \mathbb{Z}_q^{m'}$, and let matrix $\mathbf{C} \in \mathbb{Z}_q^{m' \times n}$ be a matrix where the j-th column is $\mathbf{c}$ and the rest of rows are 0's.
- Prepare $\mathsf{ct}_0 = (\mathsf{ct}^{(1)}|\mathsf{ct}^{(2)}|\mathsf{ct}^{(3)})$ as follows:
  - $\mathsf{ct}^{(1)} = \{\mathbf{R}\mathbf{U}_1\mathbf{A}_1, \mathbf{R}\mathbf{U}_2\mathbf{A}_2, \ldots, \mathbf{R}\mathbf{U}_\ell\mathbf{A}_\ell + \mathbf{C}, \ldots, \mathbf{R}\mathbf{U}_N\mathbf{A}_N\}$
  - $\mathsf{ct}^{(2)} = \{\mathbf{R}\mathbf{U}_i\mathbf{u}_i\}_{i\in[N]}$
  - $\mathsf{ct}^{(3)} = \sum_{i\in[N]}(\mathbf{R}\mathbf{U}_i\mathbf{e}'_i + \mathbf{R}\mathbf{U}_i\mathbf{A}_i\mathbf{x}_i + b_i \cdot \mathbf{R}\mathbf{U}_i\mathbf{u}_i) + \mathbf{R}\hat{\mathbf{e}}_1 + g_{\ell,j} \cdot \mathbf{c}$

  where $\{\mathbf{A}_i, \mathbf{u}_i, \mathbf{y}_i\}_{i\in[N]}$ are given in the public key pk; $\mathbf{U}_i \xleftarrow{\$} \{0,1\}^{m'\times m}$, $\mathbf{R} \hookleftarrow \{0,1\}^{m'\times m'}$; $\hat{\mathbf{e}}_1 = \sum_{i\in[N]} \hat{\mathbf{e}}_{1,i}$, and $\hat{\mathbf{e}}_{1,i} \xleftarrow{\$} [-B, B]^{m'}$ with $B = (\sigma + \sigma_0)\sqrt{\lambda} \cdot m$. Note that $b_i = 0$ or 1, is an adversarially chosen bit that come in the $\mathbf{y}_i$ part of pk.
- Compute $\mathsf{ct}_1 \leftarrow \mathcal{C}$, a random ciphertext from the possible space of all ciphertexts for 1-bit messages.
- Flip a bit $c \leftarrow \{0,1\}$.
- Run the quantum distinguisher ρ on input ct_c. Check whether the outcome is c. If so, output 1, otherwise output 0.

(3) ATI ***for*** $\mathcal{D}_{\mathsf{unif}}$*:* We finally consider a third threshold implementation, we call $\mathsf{ATI}^{\epsilon,\delta}_{1/2+\gamma,\mathcal{P},\mathcal{D}_{\mathsf{unif}}}$:

- Compute both $\mathsf{ct}_0, \mathsf{ct}_1 \leftarrow \mathcal{C}$, as random ciphertexts from the possible space of all ciphertexts for 1-bit messages.
- Flip a bit $c \leftarrow \{0,1\}$.
- Run the quantum distinguisher ρ on input ct_c. Check whether the outcome is c. If so, output 1, otherwise output 0.

Extraction algorithm We build an extractor similar to the extraction algorithm via a quantum search-to-decision reduction in [CGJL23]. The extraction algorithm takes input $\mathsf{pk} = \{\mathbf{A}_i, \mathbf{u}_i\}_{i\in[N]}$ and a quantum state ρ_{Del}, as well as parameters: threshold (inverse polynomial) γ, range for each entry in the secret q, timing parameter (inverse exponential) δ. Note that the secret dimension $N \cdot n$ comes with pk.

- Let $\mathbf{x}'_{\ell,j}$ be the register that stores the final guess for the j-th entry of $\mathbf{x}_\ell$, initialized with all zeros.
- For $\ell = 1, \cdots, N$:
  - For $j = 1, 2, \cdots, n$:
    - For $g_{\ell,j} \in \mathbb{Z}_q$, as the possible value range for $\mathbf{x}_{\ell,j} \in \mathbb{Z}_q$:
      1. Let ρ_{Del} be the current state from the quantum distinguisher.
      2. Let $\gamma := \gamma - 3\epsilon$, where $\epsilon = \frac{\gamma}{100knq}$.

3. Run $\mathsf{ATI}^{\epsilon,\delta}_{1/2+\gamma,\mathcal{P},\mathcal{D}(g_{\ell,j})}$ on ρ_{Del} with respect to pk.
4. If $\mathsf{ATI}^{\epsilon,\delta}_{1/2+\gamma,\mathcal{P},\mathcal{D}(g_{\ell,j})}$ outputs 1, then set $\mathbf{x}'_{\ell,j} := g_{\ell,j}$ and move on to the next coordinate, let $j := j+1$ if $j < n$, else let $\ell := \ell+1, j = 1$.
5. If $\mathsf{ATI}^{\epsilon,\delta}_{1/2+\gamma,\mathcal{P},\mathcal{D}(g_{\ell,j})}$ outputs 0, the let $g_i := g_i + 1$ and go to step 1.

– Output $\mathbf{x}'$.

Analysis of the Extractor We show the following two lemmata.

Lemma 25. *When the guess $g_{\ell,j} = x_{\ell,j}$, the distributions $\mathcal{D}(g_{\ell,j})$ and $\mathcal{D}_{2.N}$ are statistically close by distance $\eta_0 = 2^{-\omega(n \log q)}$.*

Proof (Proof of Lemma 25). We know that these two distributions are identical, except for how they sample ct_0. By Leftover Hash Lemma (Lemma 12), the distribution of $\mathsf{ct}_0 = (\mathsf{ct}^{(1)}|\mathsf{ct}^{(2)}|\mathsf{ct}^{(3)})$ in $\mathcal{D}_{2.N}$ is statistically close ($2^{-\omega(n \log q)}$-close) to the following distribution of $(\widetilde{\mathsf{ct}}^{(1)}, \widetilde{\mathsf{ct}}^{(2)}, \widetilde{\mathsf{ct}}^{(3)})$.

– $\widetilde{\mathsf{ct}}^{(1)} = \{\mathbf{R}\mathbf{A}'_i\}_{i\in[N]}$,
– $\widetilde{\mathsf{ct}}^{(2)} = \{\mathbf{R}\mathbf{u}'_i\}_{i\in[N]}$,
– $\widetilde{\mathsf{ct}}^{(3)} = \sum_{i\in[N]}(\mathbf{R}\mathbf{U}_i\mathbf{e}'_i + \mathbf{R}\mathbf{A}'_i\mathbf{x}_i + b_i \cdot \mathbf{R}\mathbf{u}'_i) + \mathbf{R}\hat{\mathbf{e}}_1$,

where $\mathbf{A}'_i \xleftarrow{\$} \mathbb{Z}_q^{m'\times n}, \mathbf{u}'_i \xleftarrow{\$} \mathbb{Z}_q^{m'}$ are uniformly random; $b_i = 0$ or $1, i \in [k]$ are some arbitrary, adversarially chosen bits. Recall that $\mathbf{U}_i \xleftarrow{\$} \mathbb{Z}_q^{m'\times m}$, $\mathbf{R} \hookleftarrow \{0,1\}^{m'\times m'}$, $\mathbf{e}'_i \hookleftarrow D_{\mathbb{Z}_q^m,\sigma}$; $\hat{\mathbf{e}}_1 = \sum_{i\in[N]} \hat{\mathbf{e}}_{1,i}$, and $\hat{\mathbf{e}}_{1,i} \xleftarrow{\$} [-B, B]^{m'}$ with $B = (\sigma+\sigma_0)\sqrt{\lambda}\cdot m$. For clarity, let us denote $\tilde{\mathbf{e}}_i = \mathbf{U}_i\mathbf{e}'_i$ and $\tilde{\mathbf{e}} := \sum_{i\in[N]} \tilde{\mathbf{e}}_i$. Thus, we can rewrite $\widetilde{\mathsf{ct}}^{(3)}$ as $\sum_{i\in[N]}(\mathbf{R}\mathbf{A}'_i\mathbf{x}_i + b_i \cdot \mathbf{R}\mathbf{u}'_i) + \mathbf{R}(\tilde{\mathbf{e}} + \hat{\mathbf{e}}_1)$. From the Lemma 21, we can immediately prove the distribution of ct_0 in $\mathcal{D}_{2.N}$ is statistically close to the distribution of $(\widetilde{\mathsf{ct}}^{(1)}, \widetilde{\mathsf{ct}}^{(2)}, \widehat{\mathsf{ct}}^{(3)})$ as follows.

– $\widetilde{\mathsf{ct}}^{(1)} = \{\mathbf{A}''_i\}_{i\in[N]}$,
– $\widetilde{\mathsf{ct}}^{(2)} = \{\mathbf{u}''_i\}_{i\in[N]}$,
– $\widehat{\mathsf{ct}}^{(3)} = \sum_{i\in[N]}(\mathbf{A}''_i\mathbf{x}_i + b_i \cdot \mathbf{u}''_i) + \mathbf{R}(\tilde{\mathbf{e}} + \hat{\mathbf{e}}_1)$,

where $\mathbf{A}''_i \xleftarrow{\$} \mathbb{Z}_q^{m'\times n}, \mathbf{u}''_i \xleftarrow{\$} \mathbb{Z}_q^{m'}$ are uniform random. In addition, we will show that ct_0 in $\mathcal{D}(g_{\ell,j})$ is also close to this distribution $(\widetilde{\mathsf{ct}}^{(1)}, \widetilde{\mathsf{ct}}^{(2)}, \widehat{\mathsf{ct}}^{(3)})$. Similarly as above, we can also replace the first two ciphertext components $\mathbf{R}\mathbf{U}_i\mathbf{A}_i$ and $\mathbf{R}\mathbf{U}_i\mathbf{u}_i$ by Leftover Hash Lemma (Lemma 12) and Lemma 21 with random $\mathbf{A}''_i, \mathbf{u}''_i$. Then we can ignore $\sum_i b_i \cdot \mathbf{u}''_i$ in the last component from our distribution, since b_i is known to the adversary and they are the same in both distributions.

We can observe that when the guess $g_{\ell,j} = x_{\ell,j}$, we let $\mathbf{A}'''_\ell = \mathbf{A}''_\ell + \mathbf{C}$ where $\mathbf{C}$ is everywhere 0 except the j-th column being uniformly random $\mathbf{c}$. We also have $\mathbf{A}''_\ell \mathbf{x}_\ell + g_{\ell,j} \cdot \mathbf{c} + \mathbf{R}(\tilde{\mathbf{e}}_i + \hat{\mathbf{e}}_{1,i}) = [(a''_{\ell,1,j} + c_1) \cdot x_{\ell,j} + \sum_{i \neq j}(a''_{\ell,1,i} + 0) \cdot x_{\ell,i}, \cdots, (a''_{\ell,m',j} + c_{m'}) \cdot x_{\ell,j} + \sum_{i \neq j}(a''_{\ell,m',i} + 0) \cdot x_{\ell,i}] + \mathbf{R}(\tilde{\mathbf{e}}_i + \hat{\mathbf{e}}_{1,i}) = \mathbf{A}'''_\ell \mathbf{x}_\ell + \mathbf{R}(\tilde{\mathbf{e}}_i + \hat{\mathbf{e}}_{1,i})$, where $a'''_{\ell,x,y}$ denotes the entry in x-th row and y-th column of $\mathbf{A}'''_\ell$.

□

Lemma 26. *When the guess $g_{\ell,j} \neq x_{\ell,j}$, the distributions $\mathcal{D}(g_{\ell,j})$ and $\mathcal{D}_{\mathsf{unif}}$ are statistically close by distance $\eta_1 = 2^{-\omega(n \log q)}$.*

Proof (Proof of Lemma 26). the two distributions are the same except for how they sample ct_0. The ct_0 in $\mathcal{D}_{\mathsf{unif}}$ is uniformly sampled from the ciphertext space. It remains to show that ct_0 in $\mathcal{D}(g_{\ell,j})$ is close to this uniform distribution.

Similar to the proof of Lemma 25, we can replace the two components $\mathbf{R}\mathbf{U}_i\mathbf{A}_i$ and $\mathbf{R}\mathbf{U}_i\mathbf{u}_i$ by Leftover Hash Lemma (Lemma 12) and Lemma 21 with random $\mathbf{A}''_i, \mathbf{u}''_i$. We let $\mathbf{A}'''_\ell = \mathbf{A}''_\ell + \mathbf{C}$. The $\mathbf{A}'''_\ell$ is uniformly random because the only change is adding the uniform random vector $\mathbf{c}$ in its j-th column. Next, we can observe the case when the guess $g_{\ell,j} \neq x_{\ell,j}$. We can ignore the term $\sum_i b_i \cdot \mathbf{u}'_i$ in the $\mathsf{ct}^{(3)}$ from our distribution, because b_i is known to the adversary and they are the same in both distributions. We consider the vector $\mathbf{w} = \mathbf{A}'''_\ell \mathbf{x}_\ell + g_{\ell,j} \cdot \mathbf{c} + \mathbf{R}(\tilde{\mathbf{e}}_i + \hat{\mathbf{e}}_{1,i}) = [(g_{\ell,j} \cdot c_1 + \sum_i a'''_{\ell,1,i} \cdot x_{\ell,i}, \cdots, g_{\ell,j} \cdot c_{m'} + \sum_i a'''_{\ell,m',i} \cdot x_{\ell,i}] + \mathbf{R}(\tilde{\mathbf{e}}_i + \hat{\mathbf{e}}_{1,i})$, where $\tilde{\mathbf{e}}_i = \mathbf{U}_i \mathbf{e}_i$. Since $\mathbf{c}$ is uniformly random, the entire $\mathbf{w}$ now becomes uniformly random. Since the last component $\mathsf{ct}^{(3)}$ of ct_0 in $\mathcal{D}(g_{\ell,j})$ is $\sum_{i \neq \ell}(\mathbf{A}''_i \cdot \mathbf{x}_{i,b_i} + b_i \cdot \mathbf{u}''_i + \mathbf{R}(\tilde{\mathbf{e}}_i + \hat{\mathbf{e}}_{1,i})) + \mathbf{w}$, which becomes uniformly random due to the mask $\mathbf{w}$. □

Referencing Lemma 25 (resp. Lemma 26), we have proved that the statistical distance between distributions $\mathcal{D}_{2.N}$ and $\mathcal{D}(g_{\ell,j})$ (resp. $\mathcal{D}_{\mathsf{unif}}$ and $\mathcal{D}(g_{\ell,j})$) is exponentially small when applying with correct guesses $g_{\ell,j}$ (resp. incorrect guesses $g_{\ell,j}$). We summarize our reduction extractor as follows.

Invariant through measurements: Assume that the probability of the measurement **outputting 1** on ρ is denoted by $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D},1/2+\gamma}\,\rho]$. Accordingly $1 - \mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D},1/2+\gamma}\,\rho] := \Pr[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D},1/2+\gamma}\,\rho \to 0]$. We have the following claim.

Claim 4. *For any inverse polynomial $\gamma, \epsilon < \gamma$ and exponentially small δ, it holds that:*

- *When $g_{\ell,j} = \mathbf{x}_{\ell,j}$: If $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma}\,\rho] = 1$ and a leftover state ρ', then*

$$\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}(g_{\ell,j})),1/2+\gamma-3\epsilon}\,\rho'] \geq 1 - \mathsf{negl}(\lambda).$$

- *When $g_{\ell,j} \neq \mathbf{x}_{\ell,j}$: If $\Pr[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{\mathsf{unif}},1/2+\gamma}\,\rho \to 0] = 1 - \mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{\mathsf{unif}},1/2+\gamma}\,\rho] = 1 - \delta$ and a leftover state ρ', then*

$$\Pr[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{\mathsf{unif}},1/2+\gamma}\,\rho' \to 0] \geq 1 - \mathsf{negl}(\lambda)\,.$$

Proof (Proof of Claim 4). For the case $g_{\ell,j} = \mathbf{x}_{\ell,j}$: By Lemma 16, it is known that if $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma}\,\rho] = 1$, then $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma-3\epsilon}\,\rho'] \geq 1-\delta$. By Lemma 25, we know the statistical distance between $\mathcal{D}(g_{\ell,j})$ and $\mathcal{D}_{2.N}$ is $\eta_0 = 2^{-\omega(n\log q)}$. Then, by Lemma 17, we have $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}(g_{\ell,j})),1/2+\gamma-3\epsilon}\,\rho'] \geq \mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma}\,\rho'] - 2\delta - \mathsf{negl}(\lambda) - \eta_0$. Thus, overall we have $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}(g_{\ell,j})),1/2+\gamma-3\epsilon}\,\rho'] \geq 1-\mathsf{negl}(\lambda)$ since δ and η_0 are exponentially small. For the case $g_{\ell,j} \neq \mathbf{x}_{\ell,j}$: By Lemma 26, it is known that the statistical distance between $\mathcal{D}_{\mathsf{unif}}$ and $\mathcal{D}(g_{\ell,j})$ is $\eta_1 = 2^{-\omega(n\log q)}$. By Lemma 18, we have $\|\rho-\rho'\|_{\mathrm{Tr}} \leq O(\eta_1 \cdot \frac{\ln(4/\delta)}{\epsilon})$, then $\Pr[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{\mathsf{unif}},1/2+\gamma}\,\rho' \to 0] \geq \Pr[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{\mathsf{unif}},1/2+\gamma}\,\rho \to 0] - O(\eta_1 \cdot \frac{\ln(4/\delta)}{\epsilon}) \geq 1-\delta-O(\eta_1 \cdot \frac{\ln(4/\delta)}{\epsilon})$. Thus, overall we have $\Pr[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{\mathsf{unif}},1/2+\gamma}\,\rho' \to 0] \geq 1-\mathsf{negl}(\lambda)$ since δ and η_1 are exponentially small. □

Correctness: Indeed, the behavior of our extractor is similar to [CGJL23] and mainly depends on the ATI measurement properties. We conclude it as follows.

Lemma 27. *Given the extractor as shown in C.7, if* $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma}\,\rho] = 1$ *holds for some inverse polynomial* γ*, exponentially small* δ *and* $\epsilon = \frac{\gamma}{100Nnq}$*, then the extractor algorithm will output correct secret with probability* $(1-\mathsf{negl}(\lambda))$*, by our choice of parameters in Construction 1.*

Proof (Proof of Lemma 27). Assuming that the distinguisher ρ_{Del}, hereafter referred to as ρ, meets the condition where the measurement $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma}(\rho) \approx 1$, with δ being exponentially small and ϵ defined as $\epsilon = \frac{\gamma}{100Nnq}$, as proposed in Theorem 11.

Considering that the outcome has been realized, it implies that the measurement $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma}$ has already been applied to ρ, resulting in a subsequent state ρ'. It follows then that ρ' meets the condition $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},\mathcal{D}_{2.N},1/2+\gamma-3\epsilon}\rho'] \geq 1-3\delta$, as outlined in points 2 and 3 of Lemma 16.

In the algorithm described above, when we first apply $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D(g_{\ell,j}),1/2+\gamma-4\epsilon}$ (specifically when $\ell, j = 1$ and $g_{\ell,j}$ assumes the smallest value in $\mathbb{Z}_q$), let's assume that our guess of $g_{\ell,j}$ is correct. By Claim 4, we have $\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D(g_i),1/2+\gamma-4\epsilon}\,\rho] \geq 1-3\delta-\mathsf{negl}(\lambda) \geq 1-\mathsf{negl}(\lambda)$, where δ is exponentially small. Additionally, suppose the first time we preform $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D(g_{\ell,j}),1/2+\gamma-3\epsilon}$, the guess $g_{\ell,j}$ is incorrect, then from Claim 4 it holds that $1-\mathrm{Tr}[\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D(g_{\ell,j}),1/2+\gamma-3\epsilon}\,\rho'] \geq 1-\delta$. Furthermore, after applying the measurement $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D(g_{\ell,j}),1/2+\gamma-3\epsilon}$, the resulting state ρ'' is likely, with a probability of $(1-\delta)$, to exhibit a trace distance that differs by $O(\eta_1 \cdot \ln(4/\delta)/\epsilon)$ from the state ρ'.

Then we can continue with our algorithm: every time we make a measurement $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D(g_{\ell,j}),1/2+\gamma}$, we can then apply induction: suppose we get the desired measurement (outcome 1 if $g_{\ell,j}$ is correct and 0 if $g_{\ell,j}$ is incorrect) for all the first L-th measurements. We denote the state obtained after the L-th steps in the loop as ρ_L. When the $L+1$-th measurement takes in an incorrect $g_{\ell,j}$: suppose

L' is the number of times we obtain outcome 0(including L-th measurement) because the last time we obtain outcome 1, then with probability $(1 - L' \cdot \delta)$, the state is $1 - (1 - O(\eta_1 \cdot \ln(4/\delta)/\epsilon))^{L'} \leq L' \cdot O(\eta_1 \cdot \ln(4/\delta)/\epsilon)$ close in trace distance from the last time we measure with a correct $g_{\ell,j}$. When the $L+1$-th measurement $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D(g_{\ell,j}),1/2+\gamma}$ inputs a correct $g_{\ell,j}$, then we obtain outcome 1 with probability $(1 - L' \cdot O(\eta_1 \cdot \ln(4/\delta)/\epsilon))(1 - \mathsf{negl}(\lambda))$, where L' represents the number of times we obtain outcome 0 because the last time we obtain outcome 1, by the fact that $|\operatorname{Tr}(\mathcal{P}\rho_{L-L'}) - \operatorname{Tr}(\mathcal{P}\rho_L)| \leq \|\rho_{L-L'} - \rho_L\|_{\mathrm{Tr}}$ for all POVM measurements $\mathcal{P}$.

Due to Lemma 16, each measurement will at most differ γ by 3ϵ. Therefore after $2qNn$ times of measurements, the γ is still at least $\gamma - 3\epsilon \cdot 2qNn = 0.94\gamma$, which is still inverse polynomial. This ensures that during the whole process of extraction, the γ is always non-negligible.

The overall probability we extract all $N \cdot n$-entries of the LWE secret is bounded by $(1-\mathsf{negl}(\lambda))^{Nn} \cdot (1-\delta)^{O(Nnq)} \cdot (1-O(\eta_1 \cdot \ln(4/\delta)/\epsilon))^{O(Nnq)}$, where $(1-\mathsf{negl}(\lambda))^{Nn}$ denotes the total loss incurred by $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D(g_{\ell,j}),1/2+\gamma}$ with correct $g_{\ell,j}$'s, since we will make Nn such measurements. The error $(1-\delta)^{O(Nnq)} \cdot (1 - O(\eta_1 \cdot \ln(4/\delta)/\epsilon))^{O(Nnq)}$ is incurred by $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D(g_{\ell,j}),1/2+\gamma}$ with incorrect $g_{\ell,j}$'s, since we will make $O(Nnq)$ number of such measurements. Recall our parameter settings. η_1 and δ are exponentially small and N, n, q are polynomially large. Thus, the final success probability is:

$$(1 - \mathsf{negl}(\lambda))^{Nn} \cdot (1-\delta)^{O(Nnq)} \cdot (1 - O(\eta_1 \cdot \ln(4/\delta)/\epsilon))^{O(Nnq)} \geq 1 - Nn \cdot \mathsf{negl}(\lambda)$$

which indeed is $1 - \mathsf{negl}(\lambda)$. □

Running time: By Lemma 16, the running time of each $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P},D(g_{\ell,j})),1/2+\gamma}$ is $T \cdot O(1/\epsilon^2 \cdot 1/\log\delta) = T \cdot \mathsf{poly}(1/\epsilon \cdot 1/\log\delta)$ where T is the running of quantum algorithm ρ and thus polynomial, so the entire algorithm is $O(TnNq \cdot \mathsf{poly}(1/\epsilon, 1/\log\delta))$, where $\epsilon = O(\gamma/Nnq)$ is an inverse polynomial and δ can be an inverse exponential function. As the size of the secret (to extract) is polynomial in our case, the running time of our extractor is polynomial.

D Supplementary materials for proof of quantumness

D.1 Proof of Theorem 7

Proof (Proof of Theorem 7). Given each k_i for all $i \in [N]$, a honest QPT prover will always generate $|\varphi_i\rangle$ and $\mathbf{y}_i$. Thus, when $c_i = 0$, the QPT prover can pass the preimage test with probability $1 - \mathsf{negl}(\lambda)$ by honestly performing the standard basis measurement on $|\varphi_i\rangle$. In the other hand, when $c_i = 1$, the QPT prover performs Hadamard operations on the quantum state $|\varphi_i\rangle$ and obtain

$$|\psi_i\rangle = 2^{-\frac{n\cdot\lceil log(q)\rceil+2}{2}} \sum_{\substack{\mathbf{d}_i\in\{0,1\}^{n\lceil\log(q)\rceil},\\ b_i\in\{0,1\},\\ u_i\in\{0,1\}}} (-1)^{\mathbf{d}_i^{\mathrm{T}}\cdot\mathcal{J}(\mathbf{x}'_{b_i,i})\oplus u_i b_i} p_{b_i}(\mathbf{e}_{0,i}, \mathbf{e}'_i)|u_i\rangle|\mathbf{d}_i\rangle.$$

After measuring these registers and then the prover can get a pair $(u_i, \mathbf{d}_i)$. Similar to the analysis of Lemma 8, the $(u_i, \mathbf{d}_i)$ satisfies $u_i = \mathbf{d}_i \cdot (\mathcal{J}(\mathbf{x}'_{0,i}) \oplus \mathcal{J}(\mathbf{x}'_{1,i})) \bmod 2$ with probability at least 0.801. After applying the Chernoff bound, it is straightforward to argue that $\Pr[N' > 0.75N] = 1 - \mathsf{negl}(\lambda)$.

□

D.2 Proof of Lemma 8

Our proof of quantumness protocol follows the same design paradigm as the one in [BCM+18]. In particular, the verifier also picks the preimage test and the equation test equally to challenge the prover $\widetilde{\mathcal{P}}$. Next, we recall an explicit relation from [LG22] between the p_{pre} as the $\widetilde{\mathcal{P}}$'s success probability in the preimage test and p_{eqn} as the $\widetilde{\mathcal{P}}$'s success probability in the equation test for this specific type of protocols.

Lemma 28 ([LG22, Theorem 2.2]). *For any classical prover $\widetilde{\mathcal{P}}$, in each round of test, the two probability p_{eqn} and p_{pre} satisfies:*

$$p_{\mathsf{pre}} + 2p_{\mathsf{eqn}} - 2 \leq \mathsf{negl}(\lambda).$$