Lattice-Based Quantum Advantage from Rotated Measurements

Yusuf Alnawakhtha[1], Atul Mantri[1], Carl A. Miller[1,2], and Daochen Wang[1]

[1] Joint Center for Quantum Information and Computer Science (QuICS), 3100 Atlantic Building, University of Maryland, College Park, MD 20742, USA
[2] Computer Security Division, National Institute of Standards and Technology (NIST), 100 Bureau Dr., Gaithersburg, MD 20899, USA

Abstract. Trapdoor claw-free functions (TCFs) are immensely valuable in cryptographic interactions between a classical client and a quantum server. Typically, a protocol has the quantum server prepare a superposition of two-bit strings of a claw and then measure it using Pauli-X or Z measurements. In this paper, we demonstrate a new technique that uses the entire range of qubit measurements from the XY-plane. We show the advantage of this approach in two applications. First, building on (Brakerski et al. 2018, Kalai et al. 2022), we show an optimized two-round proof of quantumness whose security can be expressed directly in terms of the hardness of the LWE (learning with errors) problem. Second, we construct a one-round protocol for blind remote preparation of an arbitrary state on the XY-plane up to a Pauli-Z correction.

1 Introduction

The field of quantum cryptography has its origins [BB14,Wie83] in the idea that quantum states can be transmitted between two parties (e.g., through free space or through an optical fiber) to perform cryptographic tasks. Properties of the transmitted states, including no-cloning and entanglement, are the basis for interactive protocols that enable a new and qualitatively different type of security. However, a recent trend in the field has shown that quantum cryptography can be done even when quantum communication is not available. If one or more parties involved in a protocol possess a sufficiently powerful quantum computer, then certain cryptographic tasks can be performed — while still taking advantage of uniquely quantum properties — using strictly classical communication. This approach relieves the users of the difficulties associated with reliable quantum communication, and puts the focus instead on the problem of building a more powerful quantum computer, a goal that has seen tremendous investments during the past several years [Nat19].

At the center of this new type of quantum cryptography are cryptographic hardness assumptions. Certain problems, such as factoring numbers, are believed to be difficult for classical computers but not for quantum computers. Other problems, such as finding the shortest vector in a lattice, are believed to be hard for both types of computers. These hardness assumptions are used to prove soundness claims for quantum interactive protocols.

Two of the seminal papers in quantum cryptography with classical communication [Mah18,BCM+21] used *trapdoor claw-free functions* [GMR84] as the basis for their protocol designs, and created a model that has been followed by many other authors. A trapdoor claw-free function (TCF), roughly speaking, is a family of triples (f_0, f_1, t), where f_0 and f_1 are injective functions with the same domain and same range, and t is a trapdoor that allows efficient inversion of either function. To say that this family is *claw-free* means that without the trapdoor t, it is believed to be hard for any (quantum or classical) adversary to find values x_0 and x_1 such that $f_0(x_0) = f_1(x_1)$.

The TCF construction illustrates how a cryptographic hardness assumption that is made for both quantum and classical computers can nonetheless permit a quantum computer to show its unique capabilities. A quantum computer can perform an efficient process that will output a random element y in the range of f_0, f_1 together with a *claw state* of the form

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|x_0\rangle |0\rangle + |x_1\rangle |1\rangle \right), \tag{1}$$

where $f_0(x_0) = f_1(x_1) = y$ (see section 2 of [Mah18]). If this state is measured in the Z-basis, one obtains a pair (x, c) such that $f_c(x) = y$. Alternatively, assuming that x_0 and x_1 are expressed as bit strings of length ℓ, and thus $|\psi\rangle$ is an $(\ell + 1)$-qubit state, one can measure in the X-basis to obtain a bit string d that must satisfy

$$d \cdot (x_0 \oplus x_1 || 1) = 0. \tag{2}$$

(Here, $||$ denotes string concatenation.) This equation is significant because we have used a quantum process to obtain information about both x_0 and x_1, even though we have assumed that it would be impossible for any efficient computer to recover x_0 and x_1 entirely. This fact is the basis for using TCFs to verify that a server that one is interacting with is able to perform quantum computation [BCM+21,KMCVY22]. The same concept was also used in cryptographic constructions that delegate the preparation of a quantum state to a server without revealing its classical description [CCKW19,GV19] and in other cryptographic protocols [MV21,Mah18].

The majority of papers utilizing TCFs in their cryptographic constructions have applied only Pauli measurements and classical operations to the state $|\psi\rangle$.[3] What would happen if we considered the full range of single-qubit measurements on the state $|\psi\rangle$? We note that since single-qubit rotation gates are physically native in some platforms (for example, ion traps [NC10,DLF+16,Mas17]), realizing a continuous single-qubit rotation is not much more difficult than realizing a single-qubit Clifford gate, and so this direction is a natural one to study.

[3] Two exceptions are as [GV19] and [CCKW21]. In [GV19], the server applies Fourier transforms to the quantum state $|\psi\rangle$. In [CCKW21], the server applies measurements from a small set in the XY-plane and the protocol only provides security against honest-but-curious adversaries. See Section 1.2 for a comparison.

In this work, we use an infinite family of qubit measurements to prove new performance and security claims for quantum server protocols. We discuss two applications: proofs of quantumness and blind remote state preparation.

1.1 Our Contribution

Proof of Quantumness. With increasing efforts in recent years towards building quantum computers, the task of verifying the quantum behavior of such computers is particularly important. Integer factorization, one of the oldest theoretical examples of a quantum advantage [Sho94], is one possible approach to this kind of verification. However, building quantum computers that are able to surpass classical computers in factoring is experimentally difficult and a far-off task. Hence, it is desirable to find alternative *proofs of quantumness*[4] that are easier for a quantum computer to perform.

The authors of [BCM+21] did groundbreaking work in this direction by offering an interactive proof of quantumness based on the hardness of LWE (learning with errors). Follow-up work [BKVV20,KMCVY22,KLVY22] used their technical ideas to optimize some aspects or provide trade-offs under different assumptions. In this work we provide a proof of quantumness that utilizes rotated measurements on claw states (Eq. (1)) to achieve some new tradeoffs. The advantage achieved in our protocol by a quantum device is described in the following theorem.

Theorem 1 (Informal). *Let λ denote the security parameter. Suppose that n, m, q, σ, τ are functions of λ that satisfy the constraints given in Fig. 1 from Section 3, and suppose that the $\mathrm{LWE}_{n,q,G(\sigma,\tau)}$ problem is hard. Then, there exists a two round interactive protocol between a verifier and a prover such that the following holds:*

- *For any efficient classical prover, the verifier accepts with probability at most $\frac{3}{4} + \mathrm{negl}(\lambda)$.*
- *For any quantum prover that follows the protocol honestly, the verifier accepts with probability at least $\cos^2\left(\frac{\pi}{8}\right) - \frac{5m\sigma^2}{q^2} - \frac{m\sigma}{2\tau}$.*

The protocol for this theorem is referred to as Protocol **Q** and is given in Fig. 4. Noting that $\cos^2(\pi/8) > 0.85 > \frac{3}{4}$, we deduce that as long as the error term $\frac{5m\sigma^2}{q^2} + \frac{m\sigma}{2\tau}$ vanishes as $\lambda \to \infty$, a constant gap is achieved between the best possible quantum winning probability and the best possible classical winning probability. In Section 3.3, we show that this vanishing condition can be achieved while taking the modulus q to be only slightly asymptotically larger than $n^2\sigma$ (where the parameter n is the dimension of the LWE problem, and σ is the noise parameter). Our approach thus allows us to base the security of our protocol on the LWE problem for a broad range of parameters, including

[4] By proof of quantumness, we mean a specific test, administered by a classical verifier, which an efficient quantum device can pass at a noticeably higher rate than any efficient classical device.

parameters that are comparable to those used in post-quantum lattice-based cryptography. (For example, in the public-key cryptosystem in [Reg09], the modulus is taken to be on the order of n^2.) Previous works on interactive lattice-based proofs of quantumness have tended to use a modulus that is either very large or not explicitly given.

Our proof builds on recent previous work, and most directly builds on [KLVY22]. In comparison to [KLVY22], our protocol involves preparing and measuring only one TCF claw state at each iteration, whereas [KLVY22] requires preparing and measuring three TCF claw states (while maintaining quantum memory throughout). Additionally, whereas [KLVY22] requires the use of quantum homomorphic encryption schemes proved by other authors, our proof is self-contained and directly relates the security of our protocol to the hardness of the underlying LWE problem. At the same time, our approach inherits the following merits from [KLVY22]: our protocol involves only 2 rounds of interaction, it requires only one qubit to be stored in memory in between rounds, and it does not require any cryptographic assumptions beyond LWE.

As far as we are aware, the combination of features in our work has not been achieved before (see Section 1.2), and our results thus bring the community closer to establishing the minimal requirements for a lattice-based proof of quantumness. As experimental progress continues [ZKML+21], there is good reason to think that these proofs of quantumness may be realizable in the near future.

Remote State Preparation. Remote state preparation (RSP) is a protocol where a computationally weak client delegates the preparation of a quantum state to a remote server. An RSP protocol is blind if the server does not learn a classical description of the state in the process of preparing it [DKL12]. Recently, [CCKW19] and [GV19] introduced blind RSP with a completely classical client, based on the conjectured quantum hardness of the LWE problem. Blind RSP has become an essential subroutine to *dequantize* the quantum channel in various quantum cryptographic applications including blind and verifiable quantum computations [BFK09,GV19,BCC+20], quantum money [Rad19], unclonable quantum encryption [GMP22], quantum copy protection [GMP22], and proofs of quantumness [MY22].

All previous RSP protocols prepare a single-qubit state $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$, where θ belongs to some fixed set $S \subseteq [0, 2\pi)$. However, a common feature among all the schemes is that either the size of S must be small, or the basis determined by θ is not fixed a priori. Therefore, a natural question in this context is:

> *Can a completely classical client delegate the preparation of arbitrary single-qubit states to a quantum server while keeping the basis fixed?*

Ideally, we would like to achieve this task in a single round of interaction. Note that the previous RSP protocols along with *computing on encrypted data* protocols such as [BFK09,FBS+14] can realize this task in two rounds of interaction. In this work, we provide a simple scheme for *deterministic* blind RSP that achieves this task without incurring any additional cost

compared to previous *randomized* RSP schemes. Our protocol only requires one round of interaction to prepare any single qubit state in the XY-plane (modulo a phase flip). This is particularly helpful for applications which require a client to delegate an encrypted quantum input, as it gives the client more control over the state being prepared. The correctness and blindness of the protocol are summarized in the theorem below.

Theorem 2 (Informal). *Let λ denote the security parameter. Suppose that n, m, q, σ, τ are functions of the security parameter λ that satisfy the constraints given in Fig. 1 from Section 3 and $\tau \geq 2m\sigma$, and suppose that the $\mathrm{LWE}_{n,q,G(\sigma,\tau)}$ problem is hard. Then there exists a one-round client-server remote state preparation protocol such that for any $\alpha \in \mathbb{Z}_q$, the client can delegate the preparation of the state $|\alpha\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\,2\pi\alpha/q}\,|1\rangle\right)$ with the following guarantees:*

- *(Correctness) If the server follows the protocol honestly, then they prepare a state $|\beta\rangle$ such that*
$$\left\| |\alpha\rangle\langle\alpha| - Z^b\,|\beta\rangle\langle\beta|\,Z^b \right\|_1 \leq \frac{4\pi m\sigma}{q},$$
where $\|\cdot\|_1$ denotes the trace norm and $b \in \{0,1\}$ is a random bit that the client can compute after receiving the server's response.
- *(Blindness) The server gains no knowledge of α from interacting with the client.*

1.2 Related Works

Proof of quantumness. The study of proofs of quantumness based on LWE was initiated by Brakerski et al. [BCM+21] who proposed a four-message (two-round) interactive protocol between a classical verifier and a prover. Their protocol also involves constructing only a single TCF claw state (like in our protocol), although it requires holding the entire claw state in memory between rounds, and it uses an exponentially large modulus.[5] Later, [BKVV20] gave a two-message (one-round) proof of quantumness with a simpler and more general security proof, but at the cost of requiring the random oracle assumption. More recently, [KMCVY22] introduced a proof of quantummness with some of the same features as [BKVV20] without the random oracle assumption, but they require up to 6 messages in their protocol (3 rounds of interaction). Both [AGKZ20] and [YZ22] present constructions of *publicly verifiable* proofs of quantumness, albeit with different assumptions or models. More recently, [KLVY22] presented a generic compiler that turns any non-local game into a proof of quantumness and gave an explicit scheme that only requires 4 messages (2 rounds of interaction). Our proof of quantumness builds on [KLVY22] —

[5] One effect of using an exponentially large modulus is on hardness assumptions. If we phrase our hardness asssumptions in terms of the shortest vector problem in a lattice, then [BCM+21] assumes the hardness of sub-exponential approximation of the shortest vector, while in the current work we only assume that polynomial approximation is hard. See Section 3.3.

see Section 2. Further works have based proofs of quantumness on different assumptions [MY22], optimized the depth required for implementing TCFs [LG22,HLG21], and even achieved prototype experimental realization [ZKML+21].

Blind RSP. Remote state preparation over a classical channel comes in two security flavors — blind RSP and blind-verifiable RSP (in this work, we give a protocol for the former). Such a primitive was first introduced in [CCKW21] for honest-but-curious adversaries. This was later extended to fully malicious adversaries in [CCKW19], where the authors present two blind RSP protocols, one of which allows the client to delegate the preparation of a BB84 state ($\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$) and the other allows the client to delegate the preparation of one of 8 states in the XY-plane. The former protocol has the advantage of allowing the client to choose if the server is preparing a computational ($\{|0\rangle, |1\rangle\}$) or a Hadamard ($\{|+\rangle, |-\rangle\}$) basis state. However, it is not clear how to generalize the scheme to prepare quantum states from a large set while maintaining control over the choice of basis. Independently, [GV19] gives a blind-verifiable RSP scheme that generalizes [BCM+21], where the blindness is based on the adaptive hardcore bit property. The protocol in [GV19] can prepare one of 10 states: 8 in the XY-plane and the two computational basis states. There is a natural way to generalize [GV19] to prepare states of the form $\frac{1}{\sqrt{2}}(|0\rangle + \exp(i\,2\pi x/q)\,|1\rangle)$ with $x, q \in \mathbb{N}$. However, the naturally generalized protocol requires an honest quantum server to apply a Fourier transform over $\mathbb{Z}_q$ on the claw state, whereas we only require the server to perform single-qubit gates on the claw state for any q. Moreover, the quantity x in the prepared state is randomly chosen in [GV19] whereas our protocol allows the client to choose x. More recently, [MY22] constructs an RSP protocol from different cryptographic assumptions (full domain trapdoor permutations); however, the blindness is only shown against classical adversaries.

Previous RSP protocols have proven to be immensely useful in several cryptographic applications, ranging from proofs of quantumness [MY22] and verification of quantum computation [GV19,Zha22] to computing on encrypted data [BCC+20,GMP22], secure two-party quantum computation [CCKM20] and more. Finally, RSP protocols have been extended to self-testing protocols [MV21,MTH+22,FWZ22]. A self-testing protocol characterizes not only the state prepared but also the measurements made upon them.

1.3 Further Directions

In our results on RSP, we have focused on qubit states in the XY-plane. It would be interesting to explore whether other continuous families of encrypted states could be prepared using our technique.

In general, blind remote state preparation can be done via quantum fully homomorphic encryption (QFHE) schemes [Mah18,Bra18]. An area where QFHE-based remote state preparation has been helpful is quantum money over classical channels [Shm22a,Shm22b].

It would be interesting to see if quantum money schemes can be made more efficient when one uses our RSP protocol to delegate the state preparation.

The integration of rotated qubit measurements with [KLVY22] invites some further development. In particular, one could see if the optimization carried out in this paper could be applied to other non-local games besides the CHSH game, thus allowing a broader range of protocols and more flexibility in implementation.

2 Technical Overview

Our protocol involves performing rotated measurements on the claw states put forward by [BCM+21] to steer the final qubit of the claw state into a specific form, while keeping this form secret by hiding it using LWE. Suppose that n, m, q are positive integers. The *Learning With Errors* (LWE) hardness assumption implies that if a classical client chooses a uniformly random vector $s \in \mathbb{Z}_q^n$ and a uniformly random matrix $A \in \mathbb{Z}_q^{m\times n}$, and computes $v := As + e$ where $e \in \mathbb{Z}_q^m$ is a small noise vector, then a quantum server cannot recover s from (A, v). Following [BCM+21] the server can (for certain parameters) nonetheless approximately prepare a superposed *claw state* of the form

$$|\gamma\rangle = \frac{1}{\sqrt{2}}\big(|x_1\rangle\,|1\rangle + |x_0\rangle\,|0\rangle\big), \tag{3}$$

where $x_0 \in \mathbb{Z}_q^n$ and $x_1 = x_0 + s$, along with a vector $y \in \mathbb{Z}_q^m$ which is close to both Ax_0 and Ax_1. We will assume that x_0 and x_1 are written out in base-2 using little-endian order.

At this point, rather than having the server measure $|\gamma\rangle$ in the X-basis, we can go in a different direction: suppose that the client instructs the server to measure the k^{th} qubit of $|\gamma\rangle$ in the basis $(\cos\theta_k)X + (\sin\theta_k)Y$ where θ_k are real numbers for $k = 1, 2, \ldots, n\lceil\log q\rceil$, and report the result as a binary vector

$$u = (u_1, \ldots, u_{n\lceil\log q\rceil}). \tag{4}$$

Once this is done, the state of the final remaining qubit will be $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}\,|1\rangle)$, where

$$\phi := \langle\theta, [x_0]\rangle - \langle\theta, [x_1]\rangle + \langle u, [x_0] \oplus [x_1]\rangle \cdot \pi.$$

Here $\langle\cdot,\cdot\rangle$ denotes the dot product, and $[x_0]$ and $[x_1]$ denote the base-2 representations of x_0 and x_1. Since the quantum server cannot know both x_0 and x_1, they cannot compute ϕ from this formula. However, if the client possesses a trapdoor to the original matrix A, then they can recover x_0 and x_1 from y and compute ϕ.

We can go further: if the client chooses a vector $t = (t_1, \ldots, t_n) \in \mathbb{Z}_q^n$ and sets θ by the formula $\theta_{(i-1)n+j} := 2^j t_i \pi/q$ for $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, \lceil\log q\rceil\}$, then

$$\begin{aligned}\phi &= \langle t, x_0 - x_1\rangle \cdot (2\pi/q) + \langle u, [x_0] \oplus [x_1]\rangle \cdot \pi \\ &= -\langle t, s\rangle \cdot (2\pi/q) + \langle u, [x_0] \oplus [x_1]\rangle \cdot \pi.\end{aligned}$$

The server thus computes a qubit that encodes a prescribed linear function $\langle t, s\rangle$ of s, modulo a possible phase flip that is known to the client – see Section 4. At the same time, LWE-hardness guarantees that the vector s remains unknown to the server. (This can be seen an enhancement of the approach described in subsection 1.4 in [CCKW21]. We have used a different measurement strategy in order to gain more control over the prepared qubit.)

We summarize our two applications of this idea, starting with blind remote state preparation (blind RSP).

Blind RSP. We will denote the state that the client wants the server to prepare (modulo a phase flip) as $|\alpha\rangle := \frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\,2\pi\alpha/q}\,|1\rangle\big)$ for some $\alpha \in \mathbb{Z}_q$ of the client's choice. The way we will ensure blindness with respect to α is by encrypting it using Regev's encryption scheme, described in Section 3.4, and having the server use the ciphertext to prepare the state. To encrypt α as such the client requires, in addition to an LWE instance, a uniformly sampled random vector $f \leftarrow \{0,1\}^m$. The client then computes $f^\top(As+e)+\alpha$ and sends $(A, As+e)$ and $(a, w) := \big(f^\top A, f^\top(As+e)+\alpha\big)$ to the server.

The server uses $(A, As+e)$ to create a claw state, which also yields the image y of the claw, and then measures the claw state using the vector $a \in \mathbb{Z}_q^n$ as described above. Then the server rotates the final qubit around the Z-axis of the Bloch sphere by $2\pi w/q$. From the discussion above we see that the resulting state will be $\frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\beta}\,|1\rangle\big)$ where

$$\begin{aligned}\beta &:= -\langle a, s\rangle \cdot (2\pi/q) + \langle u, [x_0] \oplus [x_1]\rangle \cdot \pi + 2\pi w/q \\ &= -2\pi f^\top As/q + 2\pi\big(f^\top(As+e)+\alpha\big)/q + \langle u, [x_0] \oplus [x_1]\rangle \cdot \pi \\ &\approx 2\pi\alpha/q + b \cdot \pi,\end{aligned}$$

by denoting $b := \langle u, [x] \oplus [x_1]\rangle$ and letting e/q be small (a more explicit calculation is provided in Section 6.1). The final state held by the server is $Z^b\,|\alpha\rangle$, as desired. Finally, the server sends the measurements y and u to the client who can use them along with the trapdoor of A to learn b. Note that while the client has control over α, they do not have control over the bit b as it is a function of the server's measurements.

The blindness property of the protocol is derived from the security of Regev's encryption scheme, which is based on the hardness of LWE. The information that the server receives during the protocol is $(A, As+e)$ and $\big(f^\top A, f^\top(As+e)+\alpha\big)$. The first pair is the public key in Regev's encryption scheme and the second pair is the ciphertext encrypting the message α. Hence, if an adversary can guess α in our RSP protocol then they can break Regev's encryption scheme.

Proof of Quantumness. Our proof of quantumness is based on the CHSH game [CHSH69], which is a game played with a referee and two players (Charlie and David) who cannot communicate with each other. The referee sends bits b and b' chosen uniformly at random

to Charlie and David respectively. Charlie and David are required to return bits d and d' to the referee, who decides that they win if and only if $d \oplus d' = b \wedge b'$.

Recent work [KLVY22] has proposed a version of the nonlocal CHSH game that a single server (Bob) can play with a classical client (Alice) to prove the quantumness of the server. However, the protocol in [KLVY22] requires the server to evaluate a controlled-Hadamard gate under a homomorphic encryption scheme, which requires preparing and measuring three claw-states while maintaining qubits in quantum memory. By combining the ideas in [KLVY22] with our RSP protocol, we obtain the following proof of quantumness protocol that only requires preparing and measuring one claw-state.

Our central protocol (Fig. 4 and Fig. 5) is roughly the following. Alice begins by choosing bits b and b' uniformly at random. Then, Alice uses our RSP protocol to delegate to Bob the preparation of a state of the form $(I + (-1)^d X)/2$ (if $b = 0$) or of the form $(I + (-1)^d Y)/2$ (if $b = 1$). From the RSP process, Bob obtains an encryption of the bit d which he sends back to Alice for her to decrypt. Alice then sends b' to Bob, and he measures his state in the eigenbasis of $\frac{1}{\sqrt{2}}(X + (-1)^{b'} Y)$ and returns the outcome bit d' to Alice. Alice considers Bob to have won the game if and only if $d \oplus d' = b \wedge b'$.

It can be seen that the distribution over (b, b', d, d') in the procedure described above is approximately the same as the distribution in the nonlocal CHSH game when the two players implement the optimal quantum strategy. Therefore, a quantum Bob can win with probability approximately $\cos^2(\pi/8) \approx 0.85$ (Theorem 3). On the other hand, by adapting reasoning from [KLVY22], we show that an efficient classical Bob cannot do much better than the optimal classical winning probability for the CHSH game, which is 0.75 (Theorem 4). Therefore, with appropriate parameter choices (see Section 3.3), a constant gap is achieved between the best possible classical and quantum winning probabilities.

3 Preliminaries

Let $\mathbb{C}, \mathbb{Z}, \mathbb{N}$ denote, respectively, the field of complex numbers, the ring of integers, and the set of nonnegative integers. For any $c \in \mathbb{N}$, let $\mathbb{Z}_c$ denote the set $\{0, 1, \ldots, c-1\}$ with multiplication and addition defined modulo c. If $x \in \mathbb{Z}_c$, then $|x|$ denotes the quantity

$$|x| \coloneqq \min\{x, c - x\}. \tag{5}$$

If $v = (v_1, \ldots, v_s)$ is a vector with entries from any of $\mathbb{C}, \mathbb{Z}$, or $\mathbb{Z}_c$, we write $\|v\|_\infty$ for the infinity norm of v, defined by

$$\|v\|_\infty \coloneqq \max_i |v_i|. \tag{6}$$

We denote by $\{0,1\}^*$ the set of all finite-length bit strings. For $s \in \{0,1\}^*$ and $k \in \mathbb{N}$, let $s^k \in \{0,1\}^*$ denote s repeated k times. The symbol $||$ denotes string concatenation. We write MAJ for the function $\mathrm{MAJ}\colon \{0,1\}^* \to \{0,1\}$ defined by $\mathrm{MAJ}(s) = 1$ if and only if

the Hamming weight of s is at least half its length. If a, b are vectors of the same length, we may write either $\langle a, b\rangle$ or $a \cdot b$ for the dot product of a and b.

For a finite set S, we write $s \leftarrow S$ to mean s is sampled uniformly at random from S. If χ is a distribution on S, we write $s \leftarrow \chi$ to mean s is sampled from S according to χ. The expression χ^n denotes the distribution of n-length sequences of independent samples of χ.

The expression log always denotes the logarithm in base 2. If $k \in \mathbb{Z}_c$ (viewed as $\{0, 1, \ldots, c-1\}$), then $[k] \in \{0,1\}^{\lceil \log c \rceil}$ denotes the binary representation of k in little-endian order (i.e., with the least significant bits first). If $x \in \mathbb{Z}_c^d$, then $[x]$ denotes the concatenation of $[x_1], [x_2], \ldots, [x_d]$.

For any finite set S, the expression $\mathbb{C}^S$ denotes the Hilbert space of functions from S to $\mathbb{C}$. Let $L(S)$ denote the set of linear maps from $\mathbb{C}^S$ to itself. A *quantum state* on S is an element of $L(S)$ that is trace-1 and positive semidefinite (i.e., a density operator on $\mathbb{C}^S$). A *pure quantum state* on S is a rank-1 quantum state. Any pure quantum state on S can be written as $\rho \coloneqq |\alpha\rangle\langle\alpha|$, where $|\alpha\rangle$ is a unit vector in $\mathbb{C}^S$, and we may also refer to $|\alpha\rangle$ as a pure quantum state. The *trace distance* between two quantum states ρ and σ on S is defined by $\|\rho - \sigma\|_1$, where $\|\cdot\|_1$ denotes the trace norm. When $\rho = |\alpha\rangle\langle\alpha|$ and $\sigma = |\beta\rangle\langle\beta|$ are pure, we have $\||\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta|\|_1 = 2(1 - |\langle\alpha|\beta\rangle|^2)^{1/2}$. If T is another finite set, then a *quantum operation* from S to T is a completely positive trace-preserving map from $L(S)$ to $L(T)$.

3.1 Models of Computation

We define terms related to quantum algorithms. A standard way to define a quantum circuit is as a composition of gates drawn from some specified finite set of primitive gates. Since we are concerned here with protocols that involve general single-qubit rotations, we will use a larger set of primitive gates. Let X, Y, and Z denote the Pauli operators

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \text{and} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{7}$$

A quantum circuit is then a composition of the following primitive operations:

1. Any single qubit gate of the form $e^{i\pi(p/q)R}$, where $p, q \in \mathbb{Z}$, $q \neq 0$, and $R \in \{X, Y, Z\}$.
2. The Toffoli gate $T\colon \left(\mathbb{C}^2\right)^{\otimes 3} \to \left(\mathbb{C}^2\right)^{\otimes 3}$, given by $T|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|z + xy\rangle$.
3. The gate which creates a single qubit in state $|0\rangle$.
4. The gate which measures a single qubit in the computational basis.

If a quantum circuit Q has m input qubits, and n output qubits, and ℓ intermediate primitive operations, then the size of Q is $n + m + \ell$. Such a circuit determines a function from $\{0,1\}^m$ to the set of probability distributions on $\{0,1\}^n$.

Throughout this work, $\lambda \in \mathbb{N}$ denotes the security parameter. A function $f\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ of λ is *negligible* if it is $O(\lambda^{-C})$ for all $C > 0$. For any $c \in \mathbb{N}$, a *register of size c* is a finite set Z with a fixed injection $Z \hookrightarrow \{0,1\}^c$. A *variable-sized register* (or simply a *register*) is an indexed family $\{Y_\lambda \mid \lambda \in \mathbb{N}\}$ of registers of sizes $\ell(\lambda)$, where $\ell\colon \mathbb{N} \to \mathbb{N}$ is a function. For a set A, $D(A)$ denotes the set of probability distributions on A.

Let $\mathcal{J} \coloneqq \{J_\lambda\colon A_\lambda \to B_\lambda \mid \lambda \in \mathbb{N}\}$ be a family of functions between registers. We say that $\mathcal{J}$ is *computable by a uniform deterministic polynomial-time algorithm* if there exists a poly(λ)-time classical Turing machine that on input 1^λ, where $\lambda \in \mathbb{N}$, outputs the description of a classical circuit (with a fixed gate set) $M_\lambda\colon A_\lambda \to B_\lambda$ such that $J_\lambda(x) = M(x)$ for all $x \in A_\lambda$. Let $\mathcal{F} \coloneqq \{F_\lambda\colon A_\lambda \to D(B_\lambda) \mid \lambda \in \mathbb{Z}\}$ be a family of functions. We say that $\mathcal{F}$ is *computable by a uniform probabilistic polynomial-time algorithm* if there exists a poly(λ)-time classical Turing machine that on input 1^λ, where $\lambda \in \mathbb{N}$, outputs the description of a classical circuit $M_\lambda\colon A_\lambda \to D(B_\lambda)$ with poly(λ) uniformly random bits as auxiliary input such that $\Pr[M_\lambda(x) = y] = \Pr[F_\lambda(x) = y]$ for all $\lambda \in \mathbb{N}$, $x \in A_\lambda$, and $y \in B_\lambda$. We say that $\mathcal{F}$ is *computable by a uniform quantum polynomial-time algorithm* if there exists a poly(λ)-time classical Turing machine that on input 1^λ, where $\lambda \in \mathbb{N}$, outputs the description of a quantum circuit $M_\lambda\colon A_\lambda \to D(B_\lambda)$ such that $\Pr[M_\lambda(x) = y] = \Pr[F_\lambda(x) = y]$ for all $\lambda \in \mathbb{N}$, $x \in A_\lambda$, and $y \in B_\lambda$. We also define computability by *non-uniform* {deterministic, probabilistic, quantum}-polynomial time algorithms in exactly the same way as their uniform counterparts, except we replace the requirement that the circuits M_λ be computable by a poly(λ)-time Turing machine by the requirement that M_λ is poly(λ)-sized. Note that we will often drop the index λ for simplicity — i.e., the expression $J\colon A \to B$ will be used to refer to the family of maps $\mathcal{J} = \{J_\lambda\colon A_\lambda \to B_\lambda \mid \lambda \in \mathbb{N}\}$.

3.2 Learning With Errors

For any real number $s > 0$, let $G(s)$ denote the discrete Gaussian probability distribution on $\mathbb{Z}$, defined as follows: if X is a random variable distributed according to $G(s)$, and $x \in \mathbb{Z}$, then

$$P(X = x) = \frac{e^{-x^2/(2s^2)}}{\sum_{y \in \mathbb{Z}} e^{-y^2/(2s^2)}}. \tag{8}$$

If $t > 0$, let $G(s,t)$ denote the distribution obtained from $G(s)$ by conditioning on the event $|X| \leq t$ (that is, the Gaussian distribution with standard deviation s truncated at t). To be explicit, if X is a random variable distributed according to $G(s,t)$, and $x \in \mathbb{Z}$, then

$$P(X = x) = \begin{cases} \frac{e^{-x^2/(2s^2)}}{\sum_{y \in \mathbb{Z}:|y| \leq t} e^{-y^2/(2s^2)}} & \text{if } |x| \leq t, \\ 0 & \text{if } |x| > t. \end{cases} \tag{9}$$

We will need the following lemma which gives some properties of $G(s)$.

Lemma 1 (Corollary 9 of [CKS20]). *Let X be distributed according to $G(s)$. Then $\mathrm{E}[X] = 0$ and $\mathrm{Var}[X] \leq s^2$. If C is a nonnegative real number, then $\Pr[X \geq C] \leq e^{-C^2/(2s^2)}$.*

In the following, χ denotes a probability distribution on $\mathbb{Z}$ (which in this paper will always be a Gaussian or truncated Gaussian distribution).

The $\mathrm{LWE}_{c,d,\chi}$ Problem: Let $\mathcal{D}_0$ denote the probability distribution of $(a, a \cdot s + e)$, where $a \leftarrow \mathbb{Z}_d^c$, $s \leftarrow \mathbb{Z}_q^n$, and $e \leftarrow \chi$. Let $\mathcal{D}_1$ denote the probability distribution of (a, v), where $a \leftarrow \mathbb{Z}_d^c$ and $v \leftarrow \mathbb{Z}_d$. Given oracle access to $\mathcal{D}_b$, where $b \leftarrow \{0, 1\}$, determine the value of b.

3.3 Parameters and assumptions

Throughout this paper, we will assume $m = m(\lambda), n = n(\lambda), q = q(\lambda), Q = Q(\lambda), \sigma = \sigma(\lambda), \tau = \tau(\lambda)$ are real-valued functions of the security parameter λ which satisfy all of the conditions in Fig. 1.

Parameter list:

q : modulus
Q : binary length of modulus
n, m : matrix dimensions
σ : standard deviation of Gaussian noise
τ : truncation factor for Gaussian noise

Assumptions:

- $\log q$ and $\log \sigma$ are polynomially bounded functions of λ
- $\sigma \geq 1$
- q is always an odd prime
- $Q = \lceil \log q \rceil$
- $n = \lambda$
- $m = n(2Q + 1)$
- $\tau = q/(4mQ)$

Fig. 1. Parameters and assumptions.

The rationale for the conditions in Fig. 1 is the following.

– The quantity m, which specifies the number of rows in the LWE matrix A that we will use, needs to be sufficiently large so that the single-bit encryption algorithm in Section 3.4 will be secure and that A can accommodate a trapdoor (Section 3.5). The formula $m = n(2Q + 1)$ accomplishes both purposes.
– The truncation factor τ is chosen sufficiently small to allow LWE samples involving the matrix A to be inverted, using a trapdoor, with probability 1.

We discuss more specific parameter choices in Section 5.3.

If we say that we assume that *the* $\mathrm{LWE}_{n,q,G(\sigma)}$ *problem is hard* for particular parameter functions $n = n(\lambda), q = q(\lambda), \sigma = \sigma(\lambda)$, we mean that we assume that any non-uniform quantum polynomial-time algorithm will solve the $\mathrm{LWE}_{n,q,G(\sigma)}$ problem with probability at most $\frac{1}{2} + \mathrm{negl}(\lambda)$. Note that if $\tau/\sigma = \omega(\log \lambda)$, then the distribution of $G(\sigma, \tau)$ is negligibly different from $G(\sigma)$ by Lemma 1, and so the hardness of $\mathrm{LWE}_{n,q,G(\sigma,\tau)}$ is equivalent to the hardness of $\mathrm{LWE}_{n,q,G(\sigma)}$.

As shown in [Reg09][6], we can assume that the $\mathrm{LWE}_{n,q,G(\sigma)}$ problem is hard for $n, q, \sigma = \alpha q$ with $\alpha \in (0, 1)$ and $\alpha q > \sqrt{2/\pi} \cdot \sqrt{n}$ if we assume that no non-uniform quantum polynomial-time algorithm can solve the Shortest Independent Vectors Problem (SIVP) in worst-case lattices of dimension n to within an approximation factor of $\tilde{O}(n/\alpha)$.

3.4 A Simple Encryption Algorithm

In Section 5 we will make use of a single-bit encryption algorithm which is very similar to the original lattice-based encryption algorithm proposed by Regev in [Reg09]. This algorithm is shown in Fig. 2, and consists of three algorithms: Gen (key generation), Encrypt, and Decrypt. Essentially, the public key is an LWE matrix $(A, v) := (A, As + e)$, where s is a secret vector and e is a Gaussian noise vector. Given a random bit b, a ciphertext ct is computed by summing up a random subset of the rows of $[A|v]$ and then adding a quantity (dependent on b) to the last coordinate of the sum. There is one important and unique feature of Protocol K: rather than adding $b\lfloor q/2 \rfloor$ to the final coordinate of the ciphertext (which would optimize decoding) we add $b\lfloor q/4 \rfloor$ instead, which will aid us in Section 5.

The following result asserts the IND-CPA security (that is, security against chosen-plaintext attacks) for Protocol K. The proof is standard and is given in Appendix B.

Proposition 1. *If the* $\mathrm{LWE}_{n,q,G(\sigma,\tau)}$ *problem is hard, then for any non-uniform quantum polynomial-time algorithm* $\mathcal{B}$*, we have*

$$\Pr[b' = b \mid pk \leftarrow \mathrm{Gen}_K(), b \leftarrow \{0,1\}, ct \leftarrow \mathrm{Encrypt}_K(pk, b), b' \leftarrow \mathcal{B}(pk, ct)] \leq \frac{1}{2} + \mathrm{negl}(\lambda)\,.$$

[6] Strictly speaking, the next statement does not immediately follow from [Reg09] because the error distributions $\bar{\Psi}_\alpha$ and Ψ_α defined there do not exactly correspond to discrete Gaussians. However, it does follow after we first apply [Pei10, Theorem 1] to reduce $\mathrm{LWE}_{n,q,\Psi_{\sqrt{2\pi}\alpha}}$ to $\mathrm{LWE}_{n,q,G(\sigma)}$, where $\sigma = \alpha q$.

$K = (\mathrm{Gen}_K, \mathrm{Encrypt}_K, \mathrm{Decrypt}_K)$

- $\mathrm{Gen}_K()$ samples vectors $s \leftarrow \mathbb{Z}_q^n, e \leftarrow G(\sigma,\tau)^m$, samples a matrix $A \leftarrow \mathbb{Z}_q^{m\times n}$, computes $v := As + e$, and returns (pk, s), where

$$pk := (A, v).$$

- $\mathrm{Encrypt}_K(pk, b)$ samples $f \leftarrow \{0,1\}^m$, computes $a := f^\top A$ and $w := f^\top v + b\lfloor q/4 \rfloor$, and returns ct, where

$$ct := (a, w).$$

- $\mathrm{Decrypt}_K(sk, ct)$ computes

$$\ell := \langle a, s\rangle - w,$$

and returns 1 if $|\ell + \lfloor q/4 \rfloor| \le |\ell|$, and returns 0 otherwise.

Fig. 2. The single-bit public-key encryption algorithm K. pk is the public key, s is the secret key, b is the message, and ct is the ciphertext.

3.5 Trapdoors for LWE matrices

Both of the applications in this paper will rely on trapdoors for LWE samples. The following is a slightly modified version of Theorem 2 from [MP12]. (The main difference is that we bound the noise vector using the infinity-norm rather than the Euclidean norm.)

Proposition 2. *There is a probabilistic polynomial-time algorithm* GenTrap() *and a deterministic polynomial-time algorithm* $\mathrm{Invert}(A, v, t)$ *satisfying the following.*

1. GenTrap() *accepts no input and returns a pair* (A, t)*, where* A *is an* $m \times n$ *matrix with entries in* $\mathbb{Z}_q$*. The matrix* A *is within statistical distance* $nQ2^{-n/2}$ *from a uniformly random matrix.*
2. *Given a pair* (A, t) *obtained from* GenTrap() *and vectors* $s \in \mathbb{Z}_q^n$ *and* $e \in \mathbb{Z}_q^m$ *satisfying* $\|e\|_\infty \le 2\tau$*, the algorithm* $\mathrm{Invert}(A, As + e, t)$ *returns the value* s*.*

Proof. See Appendix C. □

We make note of the following, which is an easy consequence of Proposition 2.

Proposition 3. *If* (A, t) *is a sample obtained from* GenTrap()*, then for any nonzero vector* $v \in \mathbb{Z}_q^n$*, we must have* $\|Av\|_\infty > 4\tau$*.*

Proof. Suppose that $v \neq 0$ were such that $\|Av\|_\infty \leq 4\tau$. Then, we can find vectors e, e' of infinity norm less than or equal to 2τ such that $Av = e + e'$. We have

$$0 = \text{Invert}(A, 0 + e, t) = \text{Invert}(A, Av - e', t) = v, \tag{10}$$

which is a contradiction. □

$J = (\text{Gen}_J, \text{Encrypt}_J, \text{Decrypt}_J)$

- $\text{Gen}_J()$ samples $s \leftarrow \mathbb{Z}_q^n, e \leftarrow G(\sigma, \tau)^m$, $(A, t) \leftarrow \text{GenTrap}()$, computes $v := As + e$, and returns (pk, s, t), where

$$pk := (A, v).$$

The algorithms Encrypt_J and Decrypt_J are the same as the algorithms Encrypt_K and Decrypt_K in Fig. 2.

Fig. 3. The single-bit public-key encryption algorithm J.

For the results in Section 5, it will be important to have a version of the encryption algorithm from Fig. 2 that has a trapdoor for the encoding matrix A. See Fig. 3. (Only the Gen() algorithm is different. The trapdoor is not used for encryption or decryption.) The following proposition follows directly from Propositions 1 and 2.

Proposition 4. *If the* $\text{LWE}_{n,q,G(\sigma,\tau)}$ *problem is hard, then for any non-uniform quantum polynomial-time algorithm* $\mathcal{B}$*, we have*

$$\Pr[b' = b \mid pk \leftarrow \text{Gen}_J(), b \leftarrow \{0,1\}, ct \leftarrow \text{Encrypt}_J(pk, b), b' \leftarrow \mathcal{B}(pk, ct)] \leq \frac{1}{2} + \text{negl}(\lambda)\,.$$

4 Rotated Measurements on Generalized GHZ States

The purpose of this section is to prove Proposition 5, which shows how rotated measurements behave when applied to states that generalize GHZ states [GHZ89], defined below.

Definition 1 (Generalized GHZ state). *Let* d *be a positive integer. A generalized GHZ state on* $d + 1$ *qubits is a state of the form*

$$\frac{1}{\sqrt{2}}(|x\rangle\,|1\rangle + |y\rangle\,|0\rangle), \tag{11}$$

where $x, y \in \{0,1\}^d$.

Given any sequence of real numbers $\theta_1, \ldots, \theta_n$, we make use of an associated sequence of real numbers $r_1, \ldots, r_{nQ}$ defined by

$$\begin{array}{lllll} r_1 = \theta_1 & r_2 = 2\theta_1 & r_3 = 4\theta_1 & \ldots & r_Q = 2^{Q-1}\theta_1 \\ r_{Q+1} = \theta_2 & r_{Q+2} = 2\theta_2 & r_{Q+3} = 4\theta_2 & \ldots & r_{2Q} = 2^{Q-1}\theta_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{nQ-Q+1} = \theta_n & r_{nQ-Q+2} = 2\theta_n & r_{nQ-Q+3} = 4\theta_n & \ldots & r_{nQ} = 2^{Q-1}\theta_n. \end{array} \tag{12}$$

Proposition 5. *Let $x, y \in \mathbb{Z}_q^n$, let $|\psi\rangle$ denote the $(nQ+1)$-qubit generalized GHZ state*

$$|\psi\rangle := \frac{1}{\sqrt{2}}\big(|[x]\rangle \otimes |1\rangle + |[y]\rangle \otimes |0\rangle\big), \tag{13}$$

and let $\theta_1, \ldots, \theta_n \in \mathbb{Z} \cdot (2\pi/q)$. Let $r_1, \ldots, r_{nQ}$ be the sequence defined in Eq. (12). Suppose that for each $i \in \{1, 2, \ldots, nQ\}$, the i^{th} qubit of $|\psi\rangle$ is measured in the eigenbasis of

$$(\cos r_i)X + (\sin r_i)Y \tag{14}$$

and that the outcome is $(-1)^{u_i} \in \{-1, 1\}$. Then the state of the remaining qubit is

$$\frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\theta}\,|1\rangle\big), \tag{15}$$

where

$$\theta := \sum_{i=1}^{n}(y_i - x_i)\theta_i + \pi \sum_{i=1}^{n}\sum_{j=1}^{Q}([y_i]_j - [x_i]_j)u_{(i-1)Q+j}. \tag{16}$$

Proof. The eigenvectors of the matrix in Eq. (14) are given by

$$|+_{r_i}\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{ir_i}\,|1\rangle) \quad \text{and} \quad |-_{r_i}\rangle := \frac{1}{\sqrt{2}}(|0\rangle - e^{ir_i}\,|1\rangle), \tag{17}$$

where $|+_{r_i}\rangle$ is the $+1$ eigenvector and $|-_{r_i}\rangle$ is the -1 eigenvector. For a string $s \in \{0,1\}^{nQ}$ and $t \in \{1, 2, \ldots, nQ\}$, let $s_{\geq t}$ denote the suffix of s starting at index t (when $t > |s|$, $s_{\geq t}$ denotes the empty string). Define ϕ_t by

$$\phi_t := \begin{cases} \sum_{j=1}^{t-1}([y]_j - [x]_j)(r_j + \pi u_j) & \text{if } t > 1, \\ 0 & \text{if } t = 1. \end{cases} \tag{18}$$

We want to show that measuring the first qubit of the $nQ - t + 2$ qubit state

$$|\psi_t\rangle := \frac{1}{\sqrt{2}}\big(e^{i\phi_t}\,|[x]_{\geq t}\rangle\,|1\rangle + |[y]_{\geq t}\rangle\,|0\rangle\big)$$

in the eigenbasis of $\cos(\theta_t)X + \sin(\theta_t)Y$ yields the state $|\psi_{t+1}\rangle$. The description of the post-measurement state is given by

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\langle \pm_{r_t}|_1 \left(e^{i\phi_t}|[x]_{\geq t}\rangle|1\rangle + |[y]_{\geq t}\rangle|0\rangle\right) \\
=&\frac{1}{\sqrt{2}}(e^{i\phi_t}\langle \pm_{r_t}|[x]_t\rangle|[x]_{\geq t+1}\rangle|1\rangle + \langle \pm_{r_t}|[y]_t\rangle|[y]_{\geq t+1}\rangle|0\rangle) && (19)\\
=&\frac{1}{\sqrt{2}}\left(e^{-i[y]_t(r_t+\pi u_t)}|[y]_{\geq t+1}\rangle|0\rangle + e^{i\phi_t}e^{-i[x]_t(r_t+\pi u_t)}|[x]_{\geq t+1}\rangle|1\rangle\right) && (20)\\
=&\frac{1}{\sqrt{2}}\left(|[y]_{\geq t+1}\rangle|0\rangle + e^{i(\phi_t+([y]_t-[x]_t)(r_t+\pi u_t))}|[x]_{\geq t+1}\rangle|1\rangle\right) && (21)\\
=&\frac{1}{\sqrt{2}}\left(|[y]_{\geq t+1}\rangle|0\rangle + e^{i\phi_{t+1}}|[x]_{\geq t+1}\rangle|1\rangle\right). && (22)
\end{aligned}$$

Since $|\psi_1\rangle = |\psi\rangle$, then after performing all of the nQ measurements described in the proposition statement we are left with the state $|\psi_{nQ+1}\rangle$. It remains to show that $\phi_{nQ+1} = \theta$:

$$\begin{aligned}
\phi_{nQ+1} =& \sum_{j=1}^{nQ}([y]_j - [x]_j)(r_j + \pi u_j) && (23)\\
=& \sum_{i=1}^{n}\sum_{j=1}^{Q}([y_i]_j - [x_i]_j)(r_{(i-1)Q+j} + \pi u_{(i-1)Q+j}) && (24)\\
=& \left(\sum_{i=1}^{n}\sum_{j=1}^{Q}([y_i]_j - [x_i]_j)2^{j-1}\theta_i\right) + \left(\pi\sum_{i=1}^{n}\sum_{j=1}^{Q}([y_i]_j - [x_i]_j)u_{(i-1)Q+j}\right) && (25)\\
=& \left(\sum_{i=1}^{n}(y_i - x_i)\theta_i\right) + \left(\pi\sum_{i=1}^{n}\sum_{j=1}^{Q}([y_i]_j - [x_i]_j)u_{(i-1)Q+j}\right) = \theta. && (26)
\end{aligned}$$

This completes the proof. □

5 An Optimized Proof of Quantumness

This section constructs a proof of quantumness based on the assumed hardness of the LWE problem. Our central protocol in this section, Protocol **Q** in Fig. 4, follows the form of the CHSH protocol from [KLVY22], although [KLVY22] uses a quantum homomomorphic encryption scheme and we instead use the encryption scheme J from Fig. 3. First the single prover is given an encrypted version of the first input bit b, and returns an encrypted version of the first output bit d (steps 1–2). Then, the prover is given the second input bit b' as plaintext and returns d' (steps 3–4). Finally, the verifier decrypts d (step 5) and scores the result (step 6).

Protocol Q:

1. Alice samples $(pk = (A, v), s, t) \leftarrow \mathrm{Gen}_J()$, $b \leftarrow \{0,1\}$, and computes

$$ct = (a, w) \leftarrow \mathrm{Encrypt}_J(pk, b).$$

   Alice broadcasts (pk, ct) to Bob.
2. Bob returns a pair (y, u) where $y \in \mathbb{Z}_q^m$ and $u \in \{0,1\}^{nQ}$.
3. Alice samples $b' \leftarrow \{0,1\}$ and broadcasts b' to Bob.
4. Bob returns a bit d'.
5. Alice computes $x_0 \coloneqq \mathrm{Invert}(A, y, t)$ and $x_1 \coloneqq \mathrm{Invert}(A, y + v, t)$ and

$$d \coloneqq u \cdot ([x_0] \oplus [x_1]). \tag{27}$$

6. If $d \oplus d' = b \wedge b'$, then Bob succeeds. If $d \oplus d' \neq b \wedge b'$, then Bob fails.

Fig. 4. The proof of quantumness protocol, including the behavior of the verifier (Alice).

5.1 Completeness

The ideal behavior for the prover (Bob) is given in Fig. 5. The primary difference between Bob's strategy in Fig. 5 when compared to [BCM+21,KMCVY22,KLVY22] is the use of rotated measurements to compute u.

The optimal quantum score for the ordinary CHSH game is $\cos^2(\pi/8) = (1/2 + \sqrt{2}/4)$. The next theorem implies that an honest quantum prover will approach that score, provided that certain ratios between the parameters q, m, σ and τ vanish as λ tends to infinity.

Theorem 3. *If Alice and Bob follow the process given in Figs. 4 and 5, then*

$$\Pr[\text{success}] \geq \cos^2\left(\frac{\pi}{8}\right) - \frac{5m\sigma^2}{q^2} - \frac{m\sigma}{2\tau}. \tag{32}$$

Proof. Let $T \coloneqq \{e \in \mathbb{Z}_q \mid |e| \leq \tau\}$. Consider the map

$$S \colon \mathbb{Z}_q^n \times \{0,1\} \times T^m \to \mathbb{Z}_q^m \tag{33}$$

defined by

$$S(x, c, g) = Ax - cv + g. \tag{34}$$

Proposition 3 implies that any y can have at most one pre-image in the set

$$\mathbb{Z}_q^n \times \{0\} \times T^m \tag{35}$$

Step 2. Bob prepares the state

$$|\phi\rangle \coloneqq \frac{1}{\sqrt{2q^n(2\tau+1)^m}} \sum_{x\in\mathbb{Z}_q^n} \sum_{c\in\{0,1\}} \sum_{\substack{g\in\mathbb{Z}_q^m \\ \|g\|_\infty \leq \tau}} |x\rangle\,|c\rangle\,|Ax - cv + g\rangle \tag{28}$$

Bob measures the third register of this state to obtain a state of the form $|\psi\rangle\,|y\rangle$.

Bob computes $r_1, \ldots, r_{nQ}$ via the formulas

$$r_{(i-1)Q+j} \coloneqq 2^j \pi a_i / q \quad \text{for } i \in \{1,\ldots,n\}, j \in \{1,\ldots,Q\}, \tag{29}$$

and measures the kth qubit of $|\psi\rangle$ in the eigenbasis of

$$(\cos r_k)X + (\sin r_k)Y \tag{30}$$

to obtain outcomes $(-1)^{u_1}, (-1)^{u_2}, \ldots, (-1)^{u_{nQ}}$. Bob rotates the remaining qubit (which we denote by L) by the unitary operator $|0\rangle \mapsto |0\rangle\,, |1\rangle \mapsto e^{2\pi i w/q}\,|1\rangle$.

Bob broadcasts $(y, u_1, \ldots, u_{nQ})$ to Alice.

Step 4. Bob sets $\xi = (-1)^{b'}(\pi/4)$, measures L in the eigenbasis of

$$(\cos\xi)X + (\sin\xi)Y, \tag{31}$$

obtains outcome $(-1)^{d'}$, and broadcasts d' to Alice.

Fig. 5. The behavior of an honest quantum prover in Protocol **Q** in Fig. 4.

and at most one pre-image in the set

$$\mathbb{Z}_q^n \times \{1\} \times T^m. \tag{36}$$

Moreover, when y has two pre-images $(x_0', 0, g_0)$ and $(x_1', 1, g_1)$ under S, we have

1. $x_0' = x_0$ by Proposition 2 since $\|Ax_0' - y\|_\infty = \|g_0\|_\infty \leq \tau$.
2. $x_1' = x_1$ by Proposition 2 since $\|Ax_1' - (y + v)\|_\infty = \|g_1\|_\infty \leq \tau$.
3. $x_1' = x_0' + s$ by Proposition 3 since $\|A(x_1' - (x_0' + s))\|_\infty \leq 2\tau + \|v - As\|_\infty \leq 3\tau$.

Let U_0 denote the set of all values of $y \in \mathbb{Z}_q^m$ that have a pre-image under S in (35) and let U_1 denote the set of all values of $y \in \mathbb{Z}_q^m$ that have a pre-image under S in set (36). A simple counting argument shows that, conditioned on the value of $e \coloneqq v - As \in \mathbb{Z}_q^m$, we have

$$\Pr[y \in U_0 \cap U_1 \mid e] = \frac{\prod_{i=1}^m (2\tau + 1 - |e_i|)}{(2\tau+1)^m}. \tag{37}$$

Therefore we have the following, in which we apply Lemma 5.

$$\begin{aligned}
\Pr[y \in U_0 \cap U_1] &= E\left[\frac{\prod_{i=1}^m (2\tau + 1 - |e_i|)}{(2\tau+1)^m} \;\middle|\; e \leftarrow G(\sigma,\tau)^m\right] \\
&= E\left[\prod_{i=1}^m \left(1 - \frac{|e_i|}{(2\tau+1)^m}\right) \;\middle|\; e \leftarrow G(\sigma,\tau)^m\right] \\
&\geq E\left[1 - \sum_{i=1}^m \frac{|e_i|}{(2\tau+1)} \;\middle|\; e \leftarrow G(\sigma,\tau)^m\right] \\
&= 1 - \frac{E\left[\sum_{i=1}^m |e_i| \mid e \leftarrow G(\sigma,\tau)^m\right]}{(2\tau+1)} \\
&\geq 1 - \frac{m\sigma}{2\tau+1} \geq 1 - \frac{m\sigma}{2\tau}.
\end{aligned} \tag{38}$$

The following lemma upper bounds the probability of failure when $y \in U_0 \cap U_1$.

Lemma 2. *If Alice and Bob follow the process in Figs. 4 and 5, then*

$$\Pr[\text{failure} \mid y \in U_0 \cap U_1] \leq \sin^2\left(\frac{\pi}{8}\right) + \frac{5m\sigma^2}{q^2} + \frac{1}{q}. \tag{39}$$

Proof. When $y \in U_0 \cap U_1$, by arguments made earlier in the proof, we have

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|x_1\rangle\,|1\rangle + |x_0\rangle\,|0\rangle), \tag{40}$$

where $x_1 = x_0 + s$.

After Bob measures qubits $1, 2, \ldots, nQ$ of $|\psi\rangle$ to obtain outcomes

$$(-1)^{u_1}, (-1)^{u_2}, \ldots, (-1)^{u_{nQ}}, \tag{41}$$

the remaining qubit L (by Proposition 5) is in state

$$\frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\theta}\,|1\rangle\big), \tag{42}$$

where

$$\begin{aligned}\theta &\coloneqq \frac{2\pi a \cdot (x_0 - x_1)}{q} + \pi([x_0] - [x_1]) \cdot (u_1, \ldots, u_{nQ}) \\ &= -\frac{2\pi(a \cdot s)}{q} + \pi([x_0] \oplus [x_1]) \cdot (u_1, \ldots, u_{nQ}) \mod 2\pi.\end{aligned} \tag{43}$$

Bob then rotates this state by the unitary operator $|0\rangle \mapsto |0\rangle, |1\rangle \mapsto e^{i\,2\pi w/q}\,|1\rangle$, where $w = a \cdot s + f^\top e + b\lfloor q/4 \rfloor$, to obtain the state

$$\frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\beta}\,|1\rangle\big), \tag{44}$$

where

$$\beta \coloneqq \frac{2\pi(f^\top e + b\lfloor q/4 \rfloor)}{q} + \pi([x_0] \oplus [x_1]) \cdot (u_1, \ldots, u_{nQ}). \tag{45}$$

Measuring this qubit with the observable $(\cos\gamma)X + (\sin\gamma)Y$, for any $\gamma \in \mathbb{R}$, yields outcome $+1$ with probability $\cos^2((\gamma - \beta)/2)$ and outcome -1 with probability $\sin^2((\gamma - \beta)/2)$. We therefore obtain the following formula for the failure probability:

$$\begin{aligned}&\Pr[\text{failure} \mid y \in U_0 \cap U_1] \\ &= \frac{1}{4}\,\mathrm{E}\left[\sin^2\left(\frac{\pi f^\top e}{q} - \frac{\pi}{8}\right) + \sin^2\left(\frac{\pi f^\top e}{q} + \frac{\pi}{8}\right)\right. \\ &\quad \left. + \sin^2\left(\frac{\pi(f^\top e + \lfloor q/4 \rfloor)}{q} - \frac{\pi}{8}\right) + \cos^2\left(\frac{\pi(f^\top e + \lfloor q/4 \rfloor)}{q} + \frac{\pi}{8}\right)\right],\end{aligned} \tag{46}$$

where the expectation is over $e \leftarrow G(\sigma, \tau)^m$ and $f \leftarrow \{0,1\}^m$. For the rest of this proof, we consider all expectations to be over the conditions $e \leftarrow G(\sigma, \tau)^m$ and $f \leftarrow \{0,1\}^m$.

We can obtain an upper bound on the above expression for Pr[failure] by replacing both instances of $\lfloor q/4 \rfloor$ with $q/4$, and adding a term at the end of the expression to account for any increase that these replacements may cause. Since the derivative of $\sin^2(\cdot)$ is always

between -1 and 1, inserting the term $(1/q)$ suffices. Therefore,

$$\begin{aligned}\Pr[\text{failure} \mid y \in U_0 \cap U_1] &\leq \frac{1}{4} E\left[\sin^2\left(\frac{\pi f^\top e}{q} - \frac{\pi}{8}\right) + \sin^2\left(\frac{\pi f^\top e}{q} + \frac{\pi}{8}\right)\right. \\ &\quad \left. + \sin^2\left(\frac{\pi f^\top e}{q} + \frac{\pi}{8}\right) + \cos^2\left(\frac{\pi f^\top e}{q} + \frac{3\pi}{8}\right)\right] + \frac{1}{q} \qquad (47) \\ &= 4 \cdot \frac{1}{4} E\left[\sin^2\left(\frac{\pi f^\top e}{q} + \frac{\pi}{8}\right)\right] + \frac{1}{q}.\end{aligned}$$

Using Lemma 7, we get that

$$\Pr[\text{failure} \mid y \in U_0 \cap U_1] \leq \sin^2\left(\frac{\pi}{8}\right) + \sin\left(\frac{\pi}{4}\right) E\left[\frac{\pi f^\top e}{q}\right] + E\left[\left(\frac{\pi f^\top e}{q}\right)^2\right] + \frac{1}{q}. \qquad (48)$$

It is clear that $\mathrm{E}[f^\top e] = 0$, while

$$\mathrm{E}[(f^\top e)^2] = \sum_{i=1}^{m} \mathrm{E}[(f_i e_i)^2] = \sum_{i=1}^{m} \frac{1}{2} \mathrm{E}[e_i^2] \leq m\sigma^2/2, \qquad (49)$$

where the first equality follows from Lemma 8 and the last inequality follows from Lemma 4.

Therefore,

$$\Pr[\text{failure} \mid y \in U_0 \cap U_1] \leq \sin^2\left(\frac{\pi}{8}\right) + \frac{\pi^2\sigma^2 m}{2q^2} + \frac{1}{q} \leq \sin^2\left(\frac{\pi}{8}\right) + \frac{5\sigma^2 m}{q^2} + \frac{1}{q}, \qquad (50)$$

as desired. □

Now we conclude the proof of Theorem 3. When the event $(y \in U_0 \cap U_1)$ does not occur, Bob merely measures a computational basis state on $nQ + 1$ qubits using $nQ + 1$ observables of the form $(\cos\gamma)X + (\sin\gamma)Y$. Therefore, the bits $u_1, \ldots, u_{nQ}$ and d' that Bob returns to Alice are distributed uniformly at random, and Bob thus succeeds at Protocol **Q** with probability 1/2. Therefore, by Lemma 2 and inequality (38), the overall probability that Bob fails in the protocol is upper bounded by

$$\sin^2\left(\frac{\pi}{8}\right) + \frac{5m\sigma^2}{q^2} + \frac{1}{q} + \frac{1}{2} \cdot \frac{m\sigma}{2\tau}. \qquad (51)$$

Since $\tau \leq q/4$ and $m\sigma \geq 1$, we can combine the last two summands above to obtain

$$\Pr[\text{failure}] \leq \sin^2\left(\frac{\pi}{8}\right) + \frac{5m\sigma^2}{q^2} + \frac{m\sigma}{2\tau}, \qquad (52)$$

which implies the desired result. □

5.2 Soundness

The goal of this subsection is to put an upper bound on the probability that a classical prover could succeed at Protocol **Q** in Fig. 4. We model the behavior of a classical prover in Fig. 6. Bob responds to Alice's queries in two rounds using efficient classical algorithms while holding a private register p in memory between the two rounds.

Step 2. Bob receives input (pk, ct) and computes

$$(y, u, p) \leftarrow \text{FirstResponse}(pk, ct),$$

where FirstResponse is a non-uniform probabilistic polynomial-time algorithm.

Step 4. Bob receives b' from Alice and computes

$$d' \leftarrow \text{SecondResponse}(b', p),$$

where SecondResponse is a non-uniform probabilistic polynomial-time algorithm.

Fig. 6. A model of a classical adversary for Protocol **Q** in Fig. 4. The register p denotes internal memory held by the adversary between the rounds of communication.

Theorem 4. *Suppose that the* $\text{LWE}_{n,q,G(\sigma,\tau)}$ *problem is hard. If Alice and Bob follow the process in Figs. 4 and 6, then*

$$\Pr[\text{success}] \leq \frac{3}{4} + \text{negl}(\lambda)\,. \tag{53}$$

Our proof method comes from subsection 3.1 of [KLVY22]. We first make the following elementary observation. Suppose that $T()$ is a non-uniform probabilistic polynomial-time algorithm that outputs a single bit, and that one wishes to optimally guess the output of $T()$. Clearly, the highest probability with which this can be done is

$$\kappa := \max\{\xi, 1-\xi\}\,, \tag{54}$$

where ξ denotes the expected value of $T()$. Consider the following procedure, which uses the majority function (see Section 3).

1. Sample $z_1, z_2, \ldots, z_\lambda \leftarrow T()$.
2. Output $\text{MAJ}(z_1, z_2, \ldots, z_\lambda)$.

The Chernoff bound implies that if z is obtained from this procedure and $z' \leftarrow T()$ is a new sample, then $P(z = z')$ is within $\exp\big(-\Omega(\lambda^{1/2})\big)$ of the optimal guessing probability κ.

Proof of Theorem 4. Suppose, for the sake of contradiction, that there exists a classical adversary

$$\mathcal{A} = (\text{FirstResponse}, \text{SecondResponse})$$

that achieves a success probability at Protocol **Q** that is non-negligibly higher than $\frac{3}{4}$. Consider Experiment **C**, shown in Fig. 7, in which two parties play a modified version of the CHSH game. The Referee encrypts the first input bit b using the scheme from Figure 3, and transmits the resulting encryption to both Charlie and David while also giving Charlie the trapdoor t. Then, Charlie and David play the CHSH game by doing a simulation of the behavior of the adversary $\mathcal{A}$. The winning probability in Experiment **C** is the same as the success probability for $\mathcal{A}$ in Protocol **Q**.

Experiment C:

Participants: Referee, Charlie, David

1. Referee chooses input bits $b, b' \leftarrow \{0,1\}$. She computes $(pk, s, t) \leftarrow \text{Gen}_J()$ and $ct \leftarrow \text{Encrypt}_J(pk, b)$ and sends (pk, ct) to Charlie and David. The referee also sends the trapdoor t to Charlie.
2. David computes $(y, u, p) \leftarrow \text{FirstResponse}(pk, ct)$ and shares (y, u, p) with Charlie.
3. Referee transmits b to Charlie and transmits b' to David.
4. David computes $d' \leftarrow \text{SecondResponse}(b', p)$ and transmits d' back to the Referee.
5. Charlie computes $x_0 \coloneqq \text{Invert}(A, y, t)$ and $x_1 \coloneqq \text{Invert}(A, y - v, t)$ and
$$d = u \cdot ([x_0] \oplus [x_1]). \tag{55}$$
Charlie transmits d to the Referee.
6. If $d \oplus d' = b \wedge b'$, then Charlie and David win; if not, they lose.

Fig. 7. Two players (Charlie and David) play a modified version of the CHSH game using procedures FirstResponse and SecondResponse from Fig. 6.

Next consider Experiment **C′**, shown in Fig. 8, which has two changes from Experiment **C**. First, Charlie is not given the trapdoor t at step 1. Also, at step 5, rather than

attempt to compute the output bit d directly, Charlie performs a sampling procedure to estimate the response d that will maximize Charlie and David's winning probability. The winning probability in Experiment $\mathbf{C}'$ can be at most negligibly lower (specifically, no more than $\exp\left(-\Omega(\lambda^{1/2})\right)$ lower) than that of Experiment $\mathbf{C}$. Therefore, the winning probability in Experiment $\mathbf{C}'$ is also non-negligibly higher than $\frac{3}{4}$.

Experiment $\mathbf{C}'$:

Participants: Referee, Charlie, David

1. Referee chooses input bits $b, b' \leftarrow \{0,1\}$. She computes $(pk, s, t) \leftarrow \mathrm{Gen}_J()$ and $ct \leftarrow \mathrm{Encrypt}_J(pk, b)$ and sends (pk, ct) to Charlie and David.
2. David computes $(y, u, p) \leftarrow \mathrm{FirstResponse}(pk, ct)$ and shares (y, u, p) with Charlie.
3. Referee transmits b to Charlie and transmits b' to David.
4. David computes $d' \leftarrow \mathrm{SecondResponse}(b', p)$ and transmits d' back to the Referee.
5. Charlie samples $b'_1, \ldots, b'_\lambda \leftarrow \{0,1\}$, samples $d'_k \leftarrow \mathrm{SecondResponse}(b'_k, p)$ for each $k \in \{1, 2, \ldots, \lambda\}$, and computes

$$d \coloneqq \mathrm{MAJ}\left\{d'_k \oplus (b \wedge b'_k) \mid k \in \{1, 2, \ldots, \lambda\}\right\}. \tag{56}$$

   Charlie transmits d to the referee.
6. If $d \oplus d' = b \wedge b'$, then Charlie and David win; if not, they lose.

Fig. 8. Experiment $\mathbf{C}'$ is the same as Experiment $\mathbf{C}$, except for steps 1 and 5.

Lastly, let Experiment $\mathbf{C}''$ denote a modified version of the Experiment $\mathbf{C}'$ in which, at step 1, the Referee generates ct via the procedure $ct \leftarrow \mathrm{Encrypt}_J(pk, 0)$ instead of $ct \leftarrow \mathrm{Encrypt}_J(pk, b)$. In Experiment $\mathbf{C}''$, Charlie and David are playing the original version of the CHSH game, in which both must compute their own outputs without any information about the other player's inputs. In this case, we know that Charlie and David cannot win with probability more than $\frac{3}{4}$. Therefore, the winning probabilities in Protocol $\mathbf{C}'$ and Protocol $\mathbf{C}''$ are non-negligibly different. But this is a contradiction, because it provides an efficient way to distinguish the probability distributions

$$[(b, ct, pk) \mid (pk, s, t) \leftarrow \mathrm{Gen}_J(), b \leftarrow \{0,1\}, ct \leftarrow \mathrm{Encrypt}_J(pk, b)] \tag{57}$$

and

$$[(b, ct, pk) \mid (pk, s, t) \leftarrow \mathrm{Gen}_J(), b \leftarrow \{0,1\}, ct \leftarrow \mathrm{Encrypt}_J(pk, 0)] \tag{58}$$

which violates Proposition 4. □

5.3 Parameter Choices

Let c, ϵ be constant positive real numbers, and let the functions $q = q(\lambda)$ and $\sigma = \sigma(\lambda)$ be as follows:

- σ is equal to n^c.
- q is an odd prime number between $n^{2+\epsilon}\sigma$ and $2n^{2+\epsilon}\sigma$.

(See Fig. 1 for the definitions of the other parameters.) Then,

$$q = \Theta(n^{2+\epsilon+c}), \quad Q = \Theta(\log n), \quad m = \Theta(n \log n), \quad \text{and} \quad \tau = \Theta(n^{1+c+\epsilon}/(\log n)^2).$$

The lower bound (32) from the previous completeness theorem for Protocol **Q** then satisfies

$$\begin{aligned}\cos^2\left(\frac{\pi}{8}\right) - \frac{5m\sigma^2}{q^2} - \frac{m\sigma}{2\tau} &\geq \cos^2\left(\frac{\pi}{8}\right) - O\left(\frac{(n\log n)(n^{2c})}{n^{4+2c+2\epsilon}}\right) - O\left(\frac{(n\log n)(n^c)}{n^{1+c+\epsilon}(\log n)^{-2}}\right) \\ &= \cos^2\left(\frac{\pi}{8}\right) - O\left(\frac{\log n}{n^{3+2\epsilon}}\right) - O\left(\frac{(\log n)^3}{n^\epsilon}\right),\end{aligned}$$

which tends to $\cos^2(\pi/8)$ as n tends to infinity. Meanwhile, assuming that $\mathrm{LWE}_{n,q,G(\sigma)}$ is hard (noting that $G(\sigma,\tau)$ is negligibly different from $G(\sigma)$ with these parameters), the upper bound in inequality (53) applies and tends to $\frac{3}{4}$ as n tends to infinity. Therefore, a constant gap is achieved between the best quantum success probability and our upper bound on the classical success probability.

6 Blind Single-Qubit State Preparation

This section constructs Protocol **P** in Fig. 9 which allows a classical client to instruct a quantum server to prepare a single-qubit state of the form $\frac{1}{\sqrt{2}}Z^b(|0\rangle + e^{i\,2\pi\alpha/q}\,|1\rangle)$, where $\alpha \in \mathbb{Z}_q$ and $b \in \{0,1\}$. Here, α is chosen by the client but kept hidden from the server while b is a random bit that depends on the outcomes of the server's measurements. The client can compute b after receiving the server's response.

To prepare the desired state in a secure manner, a classical client, Alice, interacts with the quantum server, Bob, in the following way. First, Alice sends an encoding of the (partial) classical description of the quantum state to Bob. As in Section 5, we use ideas from the LWE-based public key encryption scheme introduced by Regev [Reg09] to design an encoding. Upon receiving the public key and the encoded message, Bob performs a quantum circuit and a series of measurements on the resulting state to steer the final qubit as described in Section 4. Bob rotates the last qubit, according to the information sent by Alice, to prepare the desired state up to a Pauli-Z pad. The Pauli-Z padding

is partially determined by the measurement outcomes on Bob's end. Finally, Bob sends the measurement outcomes to Alice and she computes the full classical description of the prepared state. Namely, Bob's message allows Alice to learn b.

Throughout this section, we assume $\tau \geq 2m\sigma$, which is required to bound the completeness error of Protocol **P**. In terms of the parameters n, q, σ, this means we require $q/\sigma \geq 8n^2(2\lceil \log q \rceil + 1)^2 \lceil \log q \rceil$ (see Fig. 1), which can be satisfied for, e.g., $q = \Omega(n^3)$ and $\sigma = O(1)$.

6.1 Completeness

The purpose of this subsection is to prove Theorem 5 which shows that the state $|\beta\rangle$ produced by Protocol **P** in Fig. 9 is close to the state $|\alpha, b\rangle$, whose classical description is held by Alice. We first prove a technical lemma.

Lemma 3. *If Alice and Bob follow the process in Fig. 9, then*

$$\mathrm{E}[\|e\|_1 \mid \text{no abort}] \leq 2m\sigma, \tag{62}$$

where the expectation is over the distribution on (A, t, s, e, f, y) defined by Fig. 9.

Proof. x Since $e \leftarrow G(\sigma, \tau)^m$, by Lemma 5, we have that $\mathrm{E}[\|e\|_1] = \mathrm{E}[\sum_{i=1}^m |e_i|] \leq m\sigma$. But,

$$\begin{aligned} \mathrm{E}[\|e\|_1] &= \mathrm{E}[\|e\|_1 \mid \text{abort}] \Pr[\text{abort}] + \mathrm{E}[\|e\|_1 \mid \text{no abort}] \Pr[\text{no abort}] \\ &\geq \mathrm{E}[\|e\|_1 \mid \text{no abort}] \Pr[\text{no abort}] \\ &\geq \left(1 - \frac{m\sigma}{2\tau}\right) \mathrm{E}[\|e\|_1 \mid \text{no abort}], \end{aligned} \tag{63}$$

where the last inequality uses inequality (38) from Section 5.

Therefore, as $\tau \geq 2m\sigma$, we obtain $\mathrm{E}[\|e\|_1 \mid \text{no abort}] \leq m\sigma(1 - \frac{1}{4})^{-1} \leq 2m\sigma$, as required. □

Theorem 5. *If Alice and Bob follow the process given in Fig. 9, then the expected trace distance between $|\alpha, b\rangle$ and $|\beta\rangle$, conditioned on Alice not aborting, satisfies*

$$\mathrm{E}[\||\alpha, b\rangle\langle\alpha, b| - |\beta\rangle\langle\beta|\|_1 \mid \text{no abort}] \leq \frac{4\pi m\sigma}{q}, \tag{64}$$

where the expectation is over the distribution on (A, t, s, e, f, y) defined by Fig. 9.

Proof. Throughout this proof, we use the notation defined in Fig. 9. In step 3, by using arguments similar to those in our proof of Theorem 3, we see that

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(|x_1\rangle\,|1\rangle + |x_0\rangle\,|0\rangle\big), \tag{65}$$

Protocol P:

Input: Alice: $\alpha \in \mathbb{Z}_q$.
Output: Alice: classical description of $|\alpha, b\rangle$. Bob: $|\beta\rangle$.

1. Alice samples $(A, t) \leftarrow \mathrm{GenTrap}()$, $s \leftarrow \mathbb{Z}_q^n, e \leftarrow G(\sigma,\tau)^m$, and $f \leftarrow \{0,1\}^m$. Then Alice broadcasts $(A, v) \coloneqq (A, As + e)$ and $(a, w) \coloneqq (f^\top A, f^\top v + \alpha)$ to Bob.
2. Bob prepares the state

$$|\phi\rangle \coloneqq \frac{1}{\sqrt{2}\sqrt{q^n(2\tau+1)^m}} \sum_{x\in\mathbb{Z}_q^n} \sum_{c\in\{0,1\}} \sum_{\substack{g\in\mathbb{Z}_q^m \\ \|g\|_\infty \le \tau}} |x\rangle\,|c\rangle\,|Ax - cv + g\rangle\,, \tag{59}$$

   Bob measures the third register of $|\phi\rangle$ to obtain a state of the form $|\psi\rangle\,|y\rangle$. Note that $|\psi\rangle$ is an $(nQ+1)$-qubit state.

   Bob computes $r_{(i-1)Q+j} \coloneqq 2^j \pi a_i / q$ for all $i \in \{1,\ldots,n\}$, $j \in \{1,\ldots,Q\}$, and $r \coloneqq 2\pi w/q$.

   For each $i \in [nQ]$, Bob measures the i^{th} qubit of the state $|\psi\rangle$ in the eigenbasis of $(\cos r_i)X + (\sin r_i)Y$ and obtains outcome $(-1)^{u_i}$.

   Let $|\psi'\rangle$ denote the state of the last (unmeasured) qubit of $|\psi\rangle$. Bob prepares

$$|\beta\rangle \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & e^{ir} \end{bmatrix} |\psi'\rangle\,. \tag{60}$$

   Bob broadcasts the vector $y \in \mathbb{Z}_q^m$ and the bit string $u \in \{0,1\}^{nQ}$ to Alice.
3. Alice computes whether y belongs to the set

$$\{Ax + g \mid x \in \mathbb{Z}_q^n, g \in \mathbb{Z}_q^m, \|g\|_\infty \le \tau\} \cap \{Ax - v + g \mid x \in \mathbb{Z}_q^n, g \in \mathbb{Z}_q^m, \|g\|_\infty \le \tau\}.$$

   If not, Alice aborts. Otherwise, Alice computes $x_0 \coloneqq \mathrm{Invert}(A, y, t) \in \mathbb{Z}_q^n$, $x_1 \coloneqq x_0 + s \in \mathbb{Z}_q^n$, $z \coloneqq [x_0] \oplus [x_1] \in \{0,1\}^{nQ}$, and $b \coloneqq z \cdot u \in \{0,1\}$. Finally, Alice computes the classical description of the single-qubit state

$$|\alpha, b\rangle \coloneqq Z^b \frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\,2\pi\alpha/q}\,|1\rangle\big). \tag{61}$$

Fig. 9. The one-round (two-message) blind remote state preparation protocol, including the behavior of the client (Alice) and an honest server (Bob).

where $x_0, x_1 \in \mathbb{Z}_q^n$ and $x_1 = x_0 + s$, when Alice does not abort.

Then, using Proposition 5, we see that

$$\left|\psi'\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}\,|1\rangle\right), \tag{66}$$

where

$$\begin{aligned}\theta :=& \frac{2\pi a \cdot (x_0 - x_1)}{q} + \pi([x_0] - [x_1])u \\ =& -\frac{2\pi a \cdot s}{q} + \pi b \mod 2\pi.\end{aligned} \tag{67}$$

Then, since $r := 2\pi w/q = 2\pi(a \cdot s + f^\top e + \alpha)/q$, we deduce

$$|\beta\rangle := \begin{bmatrix} 1 & 0 \\ 0 & e^{ir} \end{bmatrix} \left|\psi'\right\rangle = Z^b \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}\,|1\rangle), \tag{68}$$

where

$$\phi := \frac{2\pi f^\top e}{q} + \frac{2\pi\alpha}{q}. \tag{69}$$

Therefore, the trace distance between $|\alpha, b\rangle$ and $|\beta\rangle$ is

$$\||\alpha,b\rangle\langle\alpha,b| - |\beta\rangle\langle\beta|\|_1 = 2(1 - |\langle\alpha,b|\beta\rangle|^2)^{1/2} = 2\left|\sin\left(\frac{1}{2}\cdot\frac{2\pi f^\top e}{q}\right)\right| \le \frac{2\pi\left|f^\top e\right|}{q}, \tag{70}$$

where the last inequality uses Lemma 6. Therefore,

$$\begin{aligned}\mathrm{E}[\||\alpha,b\rangle\langle\alpha,b| - |\beta\rangle\langle\beta|\|_1 \mid \text{no abort}] &\le \mathrm{E}\left[\frac{2\pi\left|f^\top e\right|}{q} \;\middle|\; \text{no abort}\right] \\ &\le \frac{2\pi}{q}\,\mathrm{E}\left[\|e\|_1 \mid \text{no abort}\right] \le \frac{4\pi m\sigma}{q},\end{aligned}$$

where the last inequality uses Lemma 3, as desired. □

6.2 Blindness

The purpose of this subsection is to prove Theorem 6, which shows that a non-uniform quantum polynomial-time adversary can compute the value of α in Protocol **P** in Fig. 9 with at most negligible advantage over random guessing. In other words, such an adversary is blind to the value of α. Intuitively, this is because the value $(a, w) = (f^\top A, f^\top v + \alpha)$ sent by Alice in her first message can be seen as an encryption of $\alpha \in \mathbb{Z}_q$ under the public key (A, v).

To state Theorem 6, we define the following distributions. For $x \in \mathbb{Z}_q$, we define $\mathcal{D}_x$ to be the distribution on $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m \times \mathbb{Z}_q^n \times \mathbb{Z}_q$ such that an element (A, v, a, w) is sampled as follows:

1. $(A, t) \leftarrow \mathrm{GenTrap}()$,
2. $v \coloneqq As + e$, where $s \leftarrow \mathbb{Z}_q^n$ and $e \leftarrow G(\sigma, \tau)^m$,
3. $a \coloneqq f^\top A$, where $f \leftarrow \{0,1\}^m$, and
4. $w \coloneqq f^\top v + x$.

We define $\tilde{\mathcal{D}}_x$ to be the same as $\mathcal{D}_x$ except with the first step replaced by $A \leftarrow \mathbb{Z}_q^{m \times n}$. We define $\mathcal{D}$ to be the distribution on $\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m \times \mathbb{Z}_q^n \times \mathbb{Z}_q$ such that an element (A, v, a, w) is sampled as follows:

$$A \leftarrow \mathbb{Z}_q^{m \times n}, \quad v \leftarrow \mathbb{Z}_q^n, \quad a \leftarrow \mathbb{Z}_q^n, \quad \text{and} \quad w \leftarrow \mathbb{Z}_q. \tag{71}$$

We can now state and prove Theorem 6. The proof is essentially the same as that of Proposition 1 but we include it for completeness.

Theorem 6 (Blindness with respect to α). *Let* $\mathrm{Guess} \colon \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m \times \mathbb{Z}_q^n \times \mathbb{Z}_q \to D(\mathbb{Z}_q)$ *be a non-uniform quantum polynomial-time algorithm. Suppose that the* $\mathrm{LWE}_{n,q,G(\sigma,\tau)}$ *problem is hard. Then for all* $x, y \in \mathbb{Z}_q$*, we have*

$$\begin{aligned} &|\Pr[\mathrm{Guess}(A, v, a, w) = x \mid (A, v, a, w) \leftarrow \mathcal{D}_y] \\ &\quad - \Pr[\mathrm{Guess}(A, v, a, w) = x \mid (A, v, a, w) \leftarrow \mathcal{D}]| \leq \mathrm{negl}(\lambda)\,. \end{aligned} \tag{72}$$

Proof. For two real functions of λ, $a = a(\lambda)$ and $b = b(\lambda)$, we write $a \simeq b$ to mean $|a - b| \leq \mathrm{negl}(\lambda)$. Then, we have

$$\begin{aligned} &\Pr[\mathrm{Guess}(A, v, a, w) = x \mid (A, v, a, w) \leftarrow \mathcal{D}_y] \\ &\simeq \Pr[\mathrm{Guess}(A, v, a, w) = x \mid (A, v, a, w) \leftarrow \tilde{\mathcal{D}}_y] \\ &\simeq \Pr[\mathrm{Guess}(A, v, a, w) = x \mid A \leftarrow \mathbb{Z}_q^{m \times n},\ v \leftarrow \mathbb{Z}_q^n,\ f \leftarrow \{0,1\}^m, a = f^\top A,\ w = f^\top v + y] \\ &\simeq \Pr[\mathrm{Guess}(A, v, a, w) = x \mid A \leftarrow \mathbb{Z}_q^{m \times n}, v \leftarrow \mathbb{Z}_q^n, a \leftarrow \mathbb{Z}_q^n, u \leftarrow \mathbb{Z}_q, w = u + y] \\ &= \Pr[\mathrm{Guess}(A, v, a, w) = x \mid (A, v, a, w) \leftarrow \mathcal{D}], \end{aligned}$$

where the first approximation follows from Proposition 2 (under our parameter settings in Fig. 1), the second approximation follows from the LWE hardness assumption and Guess being a non-uniform quantum polynomial-time algorithm, and the third approximation follows from the leftover hash lemma (see Lemma 2.1 in [AP11]). The theorem follows by the triangle inequality. □

Acknowledgements

We thank Gorjan Alagic, Alexandru Cojocaru, and Yi-Kai Liu for useful discussions and comments on an earlier version of this work. Y.A. acknowledges support from the Crown

Prince International Scholarship Program and the Arabian Gulf University. A.M acknowledges support from the U.S. Army Research Office under Grant Number W911NF-20-1-0015 and AFOSR MURI project "Scalable Certification of Quantum Computing Devices and Networks". D.W. acknowledges support from the Army Research Office (grant W911NF-20-1-0015); the Department of Energy, Office of Science, Office of Advanced Scientific Computing Research, Accelerated Research in Quantum Computing program; and the National Science Foundation (grant DMR-1747426). This paper is partly a contribution of the National Institute of Standards and Technology.

References

[AGKZ20] Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 255–268, 2020. iacr:2020/107. doi:10.1145/3357713.3384304. [p. 5]

[AP11] Joël Alwen and Chris Peikert. Generating shorter bases for hard random lattices. *Theory of Computing Systems*, 48(3):535–553, 2011. iacr:2008/521. doi:10.1007/s00224-010-9278-3. [pp. 30, 37, 38]

[BB14] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. arXiv:2003.06557. doi:10.1016/j.tcs.2014.05.025. [p. 1]

[BCC+20] Christian Badertscher, Alexandru Cojocaru, Léo Colisson, Elham Kashefi, Dominik Leichtle, Atul Mantri, and Petros Wallden. Security limitations of classical-client delegated quantum computing. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 667–696, 2020. arXiv:2007.01668. doi:10.1007/978-3-030-64834-3_23. [pp. 4, 6]

[BCM+21] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *J. ACM*, 68(5), August 2021. arXiv:1804.00640. doi:10.1145/3441309. [pp. 2, 3, 5, 6, 7, 18]

[BFK09] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Proceedings of the 50th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 517–526, 2009. arXiv:0807.4154. doi:10.1109/FOCS.2009.36. [p. 4]

[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 (TQC 2020)*, pages 8:1–8:14, 2020. arXiv:2005.04826. doi:10.4230/LIPIcs.TQC.2020.8. [pp. 3, 5]

[Bra18] Zvika Brakerski. Quantum FHE (almost) as secure as classical. In *Annual International Cryptology Conference*, pages 67–95, 2018. iacr:2018/338. doi:10.1007/978-3-319-96878-0_3. [p. 6]

[CCKM20] Michele Ciampi, Alexandru Cojocaru, Elham Kashefi, and Atul Mantri. Secure two-party quantum computation over classical channels, 2020. arXiv:2010.07925. [p. 6]

[CCKW19] Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. QFactory: classically-instructed remote secret qubits preparation. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 615–645, 2019. arXiv:1904.06303. doi:10.1007/978-3-030-34578-5_22. [pp. 2, 4, 6]

[CCKW21] Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. On the possibility of classical client blind quantum computing. *Cryptography*, 5(1):3, 2021. arXiv:1802.08759. doi:10.3390/cryptography5010003. [pp. 2, 6, 8]

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880, 1969. doi:10.1103/PhysRevLett.23.880. [p. 8]

[CKS20] Clément L Canonne, Gautam Kamath, and Thomas Steinke. The Discrete Gaussian for Differential Privacy. In *Advances in Neural Information Processing Systems*, volume 33, pages 15676–15688, 2020. arXiv:2004.00010. [p. 12]

[DKL12] Vedran Dunjko, Elham Kashefi, and Anthony Leverrier. Blind quantum computing with weak coherent pulses. *Physical Review Letters*, 108(20):200502, 2012. arXiv:1108.5571. doi:10.1103/PhysRevLett.108.200502. [p. 4]

[DLF+16] S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe. Demonstration of a small programmable quantum computer with atomic qubits. *Nature*, 536(7614):63–66, 2016. arXiv:1603.04512. doi:10.1038/nature18648. [p. 2]

[FBS+14] Kent A. G. Fisher, Anne Broadbent, L. K. Shalm, Z. Yan, Jonathan Lavoie, Robert Prevedel, Thomas Jennewein, and Kevin J. Resch. Quantum computing on encrypted data. *Nature Communications*, 5(1):1–7, 2014. arXiv:1309.2586. doi:10.1038/ncomms4074. [p. 4]

[FWZ22] Honghao Fu, Daochen Wang, and Qi Zhao. Computational self-testing of multi-qubit states and measurements, 2022. arXiv:2201.13430. [p. 6]

[GHZ89] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. *Going Beyond Bell's Theorem*, pages 69–72. Springer Netherlands, Dordrecht, 1989. arXiv:0712.0921. doi:10.1007/978-94-017-0849-4_10. [p. 15]

[GMP22] Alexandru Gheorghiu, Tony Metger, and Alexander Poremba. Quantum cryptography with classical communication: parallel remote state prepara-

tion for copy-protection, verification, and more, 2022. arXiv:2201.13445. [pp. 4, 6]

[GMR84] S. Goldwasser, S. Micali, and R. L. Rivest. A "paradoxical" solution to the signature problem. In *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 441–448, 1984. doi:10.1109/SFCS.1984.715946. [p. 2]

[GV19] Alexandru Gheorghiu and Thomas Vidick. Computationally-secure and composable remote state preparation. In *Proceedings of the 60th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 1024–1033, 2019. arXiv:1904.06320. doi:10.1109/FOCS.2019.00066. [pp. 2, 4, 6]

[HLG21] Shuichi Hirahara and François Le Gall. Test of quantumness with small-depth quantum circuits. In *46th International Symposium on Mathematical Foundations of Computer Science (MFCS 2021)*, 2021. arXiv:2105.05500. doi:10.4230/LIPIcs.MFCS.2021.59. [p. 6]

[KLVY22] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game, 2022. arXiv:2203.15877v1. [pp. 3, 4, 5, 7, 9, 17, 18, 23]

[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. arXiv:2104.00687. doi:10.1038/s41567-022-01643-7. [pp. 2, 3, 5, 18]

[LG22] Zhenning Liu and Alexandru Gheorghiu. Depth-efficient proofs of quantumness. *Quantum*, 6:807, 2022. arXiv:2107.02163. doi:10.22331/q-2022-09-19-807. [p. 6]

[Mah18] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In *Proceedings of the 59th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 332–338, 2018. arXiv:1708.02130. doi:10.1109/FOCS.2018.00039. [pp. 2, 6]

[Mas17] Dmitri Maslov. Basic circuit compilation techniques for an ion-trap quantum machine. *New Journal of Physics*, 19(2):023035, 2017. arXiv:1603.07678. doi:10.1088/1367-2630/aa5e47. [p. 2]

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology – EUROCRYPT 2012*, pages 700–718, 2012. iacr:2011/501. doi:10.1007/978-3-642-29011-4_41. [pp. 14, 38, 39]

[MTH+22] Akihiro Mizutani, Yuki Takeuchi, Ryo Hiromasa, Yusuke Aikawa, and Seiichiro Tani. Computational self-testing for entangled magic states. *Physical Review A*, 106:L010601, 2022. arXiv:2111.02700. doi:10.1103/PhysRevA.106.L010601. [p. 6]

[MV21] Tony Metger and Thomas Vidick. Self-testing of a single quantum device under computational assumptions. *Quantum*, 5:544, 2021. arXiv:2001.09161. doi:10.22331/q-2021-09-16-544. [pp. 2, 6]

[MY22] Tomoyuki Morimae and Takashi Yamakawa. Proofs of quantumness from trapdoor permutations, 2022. arXiv:2208.12390. [pp. 4, 6]

[Nat19] National Academies of Sciences, Engineering, and Medicine. *Quantum Computing: Progress and Prospects*. The National Academies Press, 2019. doi:10.17226/25196. [p. 1]

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. [p. 2]

[Pei10] Chris Peikert. An efficient and parallel gaussian sampler for lattices. In *Advances in Cryptology – CRYPTO 2010*, pages 80–97, 2010. iacr:2010/088. doi:10.1007/978-3-642-14623-7_5. [p. 13]

[Rad19] Roy Radian. Semi-quantum money. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, pages 132–146, 2019. arXiv:1908.08889. doi:10.1145/3318041.3355462. [p. 4]

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009. doi:10.1145/1568318.1568324. [pp. 4, 13, 26]

[Shm22a] 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. iacr:2021/1427. doi:10.1145/3519935.3519952. [p. 6]

[Shm22b] Omri Shmueli. Semi-quantum tokenized signatures, 2022. iacr:2022/228. [p. 6]

[Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 124–134, 1994. arXiv:quant-ph/9508027. doi:10.1109/SFCS.1994.365700. [p. 3]

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. [p. 1]

[YZ22] Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure, 2022. arXiv:2204.02063. [p. 5]

[Zha22] Jiayu Zhang. Classical verification of quantum computations in linear time, 2022. arXiv:2202.13997. [p. 6]

[ZKML+21] Daiwei Zhu, Gregory D. Kahanamoku-Meyer, Laura Lewis, Crystal Noel, Or Katz, Bahaa Harraz, Qingfeng Wang, Andrew Risinger, Lei Feng, Debopriyo Biswas, Laird Egan, Alexandru Gheorghiu, Yunseong Nam, Thomas Vidick, Umesh Vazirani, Norman Y. Yao, Marko Cetina, and Christopher

Monroe. Interactive protocols for classically-verifiable quantum advantage, 2021. arXiv:2112.05156. [pp. 4, 6]

A Mathematical Lemmas

Lemma 4. *For any $\sigma \in \mathbb{N}, \tau > 0$,*

$$\mathrm{E}[X^2 \mid X \leftarrow G(\sigma, \tau)] \leq \sigma^2. \tag{73}$$

Proof. For notational convenience, for $x \in \mathbb{Z}$, we write

$$\Pr_1[x] \coloneqq \Pr[x \leftarrow G(\sigma)] \quad \text{and} \quad \Pr_2[x] \coloneqq \Pr[x \leftarrow G(\sigma, \tau)]. \tag{74}$$

We also write

$$Z \coloneqq \sum_{x \in \mathbb{Z} : |x| \leq \tau} \Pr_1[x] \quad \text{and} \quad L \coloneqq \mathrm{E}[X^2 \mid X \leftarrow G(\sigma, \tau)]. \tag{75}$$

Note that L is the quantity we need to upper bound and

$$L = \sum_{x \in \mathbb{Z} : |x| \leq \tau} x^2 \Pr_2[x] = \sum_{x \in \mathbb{Z} : |x| \leq \tau} x^2 \frac{\Pr_1[x]}{Z} \leq \tau^2. \tag{76}$$

We upper bound L as follows.

$$\begin{aligned}
L &= L(1 - Z) + LZ \\
&\leq \tau^2 (1 - Z) + \sum_{x \in \mathbb{Z} : |x| \leq \tau} x^2 \Pr_1[x] && \text{(by Eq. (76))} \\
&= \tau^2 \sum_{x \in \mathbb{Z} : |x| > \tau} \Pr_1[x] + \sum_{x \in \mathbb{Z} : |x| \leq \tau} x^2 \Pr_1[x] \\
&\leq \sum_{x \in \mathbb{Z} : |x| > \tau} x^2 \Pr_1[x] + \sum_{x \in \mathbb{Z} : |x| \leq \tau} x^2 \Pr_1[x] \\
&= \sum_{x \in \mathbb{Z}} x^2 \Pr_1[x] \\
&= \mathrm{E}[X^2 \mid X \leftarrow G(\sigma)],
\end{aligned}$$

but, by Lemma 1, we have

$$\mathrm{E}[X^2 \mid X \leftarrow G(\sigma)] = \mathrm{Var}[X \mid X \leftarrow G(\sigma)] \leq \sigma^2. \tag{77}$$

Therefore, $L \leq \sigma^2$, as required. □

Lemma 5. *For any $\sigma \in \mathbb{N}, \tau > 0$,*

$$\mathrm{E}[\,|X| \mid X \leftarrow G(\sigma, \tau)] \leq \sigma. \tag{78}$$

Proof. This lemma follows immediately from Lemma 4. We have

$$\mathrm{E}[\,|X| \mid X \leftarrow G(\sigma,\tau)] \leq \sqrt{\mathrm{E}[|X|^2 \mid X \leftarrow G(\sigma,\tau)]} \leq \sigma, \tag{79}$$

as desired. □

Lemma 6. *The following inequality holds for any real value t: $|\sin t| \leq |t|$.*

Proof. We have $\sin^2 t = \int_0^t \int_0^s 2\cos(2r)\,\mathrm{d}r\,\mathrm{d}s \leq \int_0^t \int_0^s 2(1)\,\mathrm{d}r\,\mathrm{d}s = t^2$. □

Lemma 7. *The following inequality holds for any real values t, s:*

$$\sin^2(t+s) \leq \sin^2 s + t\sin(2s) + t^2. \tag{80}$$

Proof. Let $f(x) = \sin^2(x+s)$. We have $f(0) = \sin^2 s$, $f'(0) = \sin 2s$, and $f''(x) = 2\cos(2x+2s)$. If we let

$$g(x) = \sin^2 s + x\sin 2s + x^2, \tag{81}$$

then $g(0) = f(0)$, $g'(0) = f'(0)$, and $g''(x) \geq f''(x)$ for all x, which yields $g(x) \geq f(x)$ for all x as desired. □

Lemma 8. *Suppose that $X_1, \ldots, X_\ell$ are independent real-valued random variables and that $\mathrm{E}[X_1] = \mathrm{E}[X_2] = \ldots = \mathrm{E}[X_{\ell-1}] = 0$. Then,*

$$\mathrm{E}[(X_1 + \ldots + X_\ell)^2] = \mathrm{E}[X_1^2] + \mathrm{E}[X_2^2] + \ldots + \mathrm{E}[X_\ell^2]. \tag{82}$$

Proof. We have

$$\mathrm{E}[(X_1 + \ldots + X_\ell)^2] = \sum_i \mathrm{E}[X_i^2] + \sum_{i \neq j} \mathrm{E}[X_i]\,\mathrm{E}[X_j]. \tag{83}$$

All terms in the second summation are clearly zero. □

B Proof of Proposition 1

Let $\mathrm{Gen}'()$ denote an algorithm that merely outputs a uniformly random pair $pk = (A, v)$ and does not output a secret key. By the LWE assumption, the quantity on the left-hand side of Proposition 1 is negligibly different from

$$\Pr[b' = b \mid pk \leftarrow \mathrm{Gen}'(), b \leftarrow \{0,1\}, ct \leftarrow \mathrm{Encrypt}_K(pk, b), b' \leftarrow \mathcal{B}(pk, ct)]$$

Meanwhile, the leftover hash lemma (see Lemma 2.1 in [AP11]) implies that the distribution of $(A, v, f^\top A, f^\top v)$, when $f \in \{0,1\}^m, A \in \mathbb{Z}_q^{m \times n}, v \in \mathbb{Z}_q^m$ are all sampled uniformly, is itself negligibly close to uniform. Therefore the quantity on the left-hand side of Proposition 1 is also negligibly close to

$$\Pr[b' = b \mid pk \leftarrow \mathrm{Gen}'(), ct \leftarrow \mathbb{Z}_q^{n+1}, b \leftarrow \{0,1\}, b' \leftarrow \mathcal{B}(pk, ct)].$$

Since ct and pk are independent of b in this expression, the quantity above is obviously equal to $\frac{1}{2}$. This completes the proof.

C Trapdoors for LWE matrices

Proof of Proposition 2. Our proof is essentially the same as the proof in [MP12]. The main difference is that we use the infinity norm, rather than the Euclidean norm, to bound error vectors. We define GenTrap() as follows.

Algorithm GenTrap():

1. Let

$$g = \begin{bmatrix} 1 \\ 2 \\ 4 \\ \vdots \\ 2^{Q-1} \end{bmatrix} \tag{84}$$

and let G be the $nQ \times n$ matrix

$$G = \begin{bmatrix} g & & & \\ & g & & \\ & & g & \\ & & & \ddots \\ & & & & g \end{bmatrix}. \tag{85}$$

2. Sample a matrix $M \in \mathbb{Z}_q^{(Q+1)n \times n}$ with entries chosen uniformly from $\mathbb{Z}_q$, and a matrix $N \in \mathbb{Z}_q^{Qn \times (Q+1)n}$ with entries chosen uniformly from $\{0,1\}$. Let

$$A = \left[\frac{G + NM}{M}\right]. \tag{86}$$

3. Let $t = N$. Return (A, t).

□

By the leftover hash lemma (see Lemma 2.1 in [AP11]) if $z \in \{0,1\}^{(Q+1)n}$ is chosen uniformly at random, then the distribution of

$$\left[\frac{M}{z^\top M}\right]$$

is within statistical distance $2^{-n/2}$ from uniformly random. Iterating this fact, we find that the matrix

$$\left[\frac{M}{NM}\right]$$

is within statistical distance $nQ2^{-n/2}$ from uniformly random, and the same applies to the matrix A. This proves the first claim of Proposition 2.

We sketch a method for the Invert algorithm (see [MP12] for more details). The algorithm Invert receives as input the matrix A, a vector $v := As + e$ where e satisfies $\|e\|_\infty \leq 2\tau$, and the trapdoor matrix N. Let v_1 denote the vector consisting of the first Qn entries of v, and let v_2 denote the vector consisting of the remaining entries of v. We have

$$v_1 = (G + NM)s + e_1 \quad \text{and} \quad v_2 = Ms + e_2, \tag{87}$$

where e_1, e_2 have infinity norm upper bounded by 2τ. Letting

$$v' := v_1 - Nv_2, \tag{88}$$

we find

$$v' = Gs + (e_1 - Ne_2). \tag{89}$$

Let $e' := e_1 - Ne_2$. Then, $v' = Gs + e'$, and $\|e'\|_\infty \leq \tau + (Q+1)n(2\tau) < q/(2Q)$. Let

$$S := \begin{bmatrix} 2 & -1 & & & \\ & 2 & -1 & & \\ & & \ddots & & \\ & & & 2 & -1 \\ [q]_1 & [q]_2 & [q]_3 & \cdots & [q]_Q \end{bmatrix} \tag{90}$$

and let Y be the $Q^2 \times Q^2$ matrix which consists of Q diagonal blocks, each equal to S. Then, $YG = 0$, and therefore if we compute $w := Yv'$, we have

$$w = Y(Gs + e') = Ye'. \tag{91}$$

Since each entry of e' has absolute value less than $q/(2Q)$ and each row of Y has trace-norm less than or equal to Q, the equation $Ye' = w$ can be solved for e' simply by inverting the matrix Y over the real numbers. Then, we compute $Gs = v' - e'$ and recover s. If no solution exists, we assume that Invert returns the vector 0^n.