Eavesdropper-Blind Remote State Preparation and Applications to Quantum Public-Key Encryption

Kaniuar Bacho* Alexandru Cojocaru†

Abstract

Remote state preparation (RSP) is a central primitive in quantum cryptography, enabling classical parties to remotely construct quantum states using only classical communication. As a result, RSP serves as a key building block in numerous protocols involving classical clients and quantum servers, allowing classical parties to leverage the advantages offered by powerful quantum computers. All known constructions of RSP rely on strong cryptographic assumptions, typically variants of trapdoor claw-free functions (TCFs).

In this work, we initiate the study of a weaker form of remote state preparation, which we call *eavesdropper-blind remote state preparation* (EB-RSP). Informally, EB-RSP requires blindness only against external observers who see the transcript of the honest protocol, rather than against the quantum server itself. Despite this relaxed adversarial model, the resulting notion remains sufficient for useful cryptographic applications. In particular, we show that two-message EB-RSP already suffices to construct quantum public-key encryption with classical public keys and quantum ciphertexts. We then construct two-message EB-RSP protocols from specific one-way group actions, yielding a first step toward RSP-type primitives based on assumptions that do not rely on trapdoors. Finally, we observe that existing RSP constructions are likely naturally adaptable to the two-message EB-RSP notion; we demonstrate this explicitly for a concrete TCF-based RSP construction.

*University of Edinburgh. Email: k.bacho@sms.ed.ac.uk
†University of Edinburgh. Email: a.cojocaru@ed.ac.uk

Contents

1 Introduction **3**
1.1 Main Results and Technical Overview 5
1.1.1 Eavesdropper-Blind Remote State Preparation 5
1.1.2 Quantum Public-Key Encryption with Classical Public Keys 9
1.2 Discussions 10

2 Preliminaries **12**
2.1 One-Way Group Actions 12
2.2 Quantum Fourier Transform over Finite Abelian Groups 13
2.3 Quantum Goldreich-Levin Theorem for Large Fields 15

3 Eavesdropper-Blind Remote State Preparation **15**
3.1 Definition 16
3.2 Construction from One-Way Group Actions 18

4 Quantum Public-Key Encryption with Classical Public Keys **22**
4.1 Definition 23
4.2 Black-Box Construction from Eavesdropper-Blind Remote State Preparation 23

A Eavesdropper-Blind Remote State Preparation from Trapdoor Claw-Free Functions **30**

1 Introduction

Remote state preparation (RSP) is a central quantum cryptographic primitive that enables a classical party to remotely prepare quantum states on a quantum device using only classical communication. As a result, RSP plays a fundamental role in the study of the *Quantum-Computation Classical-Communication* (QCCC) model [ACC+22], whose goal is to enable classical parties to leverage the advantages provided by powerful quantum computers. RSP serves as a key building block in numerous protocols in the QCCC setting, including delegated and verifiable quantum computation [GV19, BK25, BKM+25, Zha25], proofs of quantumness [AMMW22, BK25], quantum fully homomorphic encryption [GV24], quantum public-key encryption [BK25], and unclonable cryptography [GMP23].

An RSP protocol [CCKW19, GV19, CCKW21] is an interactive protocol between a classical verifier (or client) and a quantum prover (or server). At the end of the protocol, the prover should hold a quantum state from a prescribed family of states, while the verifier obtains a classical description of the output quantum state. Existing RSP constructions differ along two main axes:

1. The family of quantum states that can be remotely prepared, and
2. The security guarantees provided by the protocol.

These two aspects largely determine the types of applications for which a given RSP protocol is suitable. Most existing constructions prepare BB84 states [BK25], generalized BB84 states [CCKW19, GV19, AMMW22, BKM+25, Zha25], or EPR pairs [GV24]. On the security side, two central notions are *blindness* and *verifiability*. Informally, blindness requires that the prover learns essentially no information about the prepared quantum state, while verifiability guarantees that a successful prover has prepared a valid state consistent with the verifier's classical description.

There are also several possible threat models for blindness. One of the weakest notions is *honest-but-curious blindness* (or *semi-honest blindness*), where the prover follows the protocol honestly but later attempts to infer information about the hidden state. Stronger notions consider *malicious-server blindness*, where the prover may arbitrarily deviate from the protocol and still should not learn information about the prepared state. Existing RSP constructions typically aim to achieve such strong malicious-server security notions.

However, different applications may require different levels of security. This motivates the investigation of weaker forms of remote state preparation that may still suffice for meaningful cryptographic applications while potentially admitting constructions from weaker assumptions.

A long line of work has sought to understand which cryptographic assumptions suffice to realize remote state preparation. Existing constructions typically rely on trapdoor cryptographic primitives, notably trapdoor claw-free functions (TCFs) or variations thereof, while reducing the required assumptions has remained a major open problem. On the other hand, recent impossibility results suggest that one-way functions alone are unlikely to suffice for constructing certain families of RSP protocols [BK25].

This naturally raises the question of whether weaker forms of remote state preparation may still suffice for meaningful cryptographic applications while admitting constructions from weaker assumptions. More concretely, two closely related questions emerge:

> (1) *Can useful cryptographic applications still be derived from RSP protocols that satisfy weaker security notions?*

(2) *Can such weaker forms of RSP be constructed from trapdoor-free cryptographic assumptions?*

This work investigates both questions. We first introduce a weaker notion of remote state preparation, called *eavesdropper-blind remote state preparation* (EB-RSP), and show that despite its relaxed security guarantees, it still suffices for meaningful cryptographic applications. We then show that such protocols can be constructed from *specific* one-way group actions[1], yielding a first step toward RSP-type primitives that do not rely on trapdoor assumptions.

The importance of the first question lies in understanding whether meaningful cryptographic applications can already be obtained from weaker forms of remote state preparation. Such weaker notions may potentially admit constructions based on qualitatively different or weaker cryptographic assumptions.

Our first contribution addresses the question of whether weaker notions of remote state preparation can still support meaningful cryptographic applications. We introduce a new primitive called *eavesdropper-blind remote state preparation* (EB-RSP), based on what we argue is one of the weakest natural security notions for remote state preparation: blindness only against an external eavesdropper observing the honest transcript of the interaction between the verifier and the prover. Concretely, the security guarantee ensures that, given the transcript of the protocol, any quantum polynomial-time eavesdropper cannot infer any information about the classical description of the prepared quantum state. Unlike standard blindness notions for RSP, EB-RSP does not require hiding the prepared state from the prover itself. A central message of this work is that such a relaxed adversarial model may nevertheless suffice for useful cryptographic applications.

In particular, we show that any two-message EB-RSP protocol implies quantum public-key encryption (QPKE) with classical public keys and quantum ciphertexts. In the classical setting, [IR89] showed that classical public-key encryption cannot be constructed from one-way functions in a black-box manner. However, when allowing quantum public keys and quantum communication, it is known that one-way functions suffice to construct quantum public-key encryption [BGH+23, BMW23, KMNY24]. Nevertheless, quantum public keys introduce substantial challenges compared to classical public-key infrastructures, where public keys can be freely copied, stored, and distributed through classical communication channels.

These limitations motivate the study of QPKE with classical public keys. Previous work [HMY23] constructed such schemes from non-abelian pseudorandom group actions. In contrast, our work identifies two-message EB-RSP as an intermediate primitive that suffices for constructing QPKE in a black-box manner. As we show later, two-message EB-RSP itself can be instantiated from specific one-way group actions and can also be obtained by adapting existing TCF-based RSP protocols. By combining these ingredients, we obtain constructions of QPKE from certain one-way group actions and from TCFs.

Our second main contribution addresses the possibility of constructing RSP-type primitives without relying on trapdoor cryptographic assumptions. From a foundational perspective, this question is particularly compelling, as all existing RSP constructions rely on cryptographic primitives that admit a trapdoor in order to allow the classical verifier to efficiently recover a classical description of the prepared quantum state. In contrast, we show that EB-RSP protocols can be constructed from specific one-way group actions.

At a conceptual level, our proposed construction replaces the role traditionally played by the

[1]The *specific* one-way group action can be found in Theorem 3.3.

trapdoor with algebraic structure arising from the group action. More specifically, we exploit the algebraic properties of the group action to eliminate parameters unknown to the verifier from the description of the output quantum state, while still preserving security. To the best of our knowledge, this is the first construction of an RSP-type primitive with meaningful cryptographic applications that does not rely on any trapdoor primitive.

More broadly, our results suggest that algebraic cryptographic assumptions may provide an alternative route toward quantum cryptographic primitives in the QCCC model. While existing constructions of RSP rely heavily on trapdoor claw-free functions, one-way group actions arise from a fundamentally different framework rooted in group-based and isogeny-based cryptography.

Group actions have long served as a versatile abstraction in cryptography, starting with the seminal work of Brassard and Yung [BY91], by generalizing Diffie–Hellman-type constructions [MMR07] and playing a central role in isogeny-based cryptography [JD11, CLM+18, ADMP20]. Group-action-based assumptions have also found applications in quantum cryptography. For instance, stronger assumptions such as pseudorandom group actions have been used to construct QPKE with classical public keys [HMY23], while related assumptions have enabled constructions of quantum money and quantum lightning schemes [MS24, Zha24, BNZ25]. More recently, several works introduced *quantum group actions* [MX24, MZ25], extending group actions to quantum settings and enabling additional applications, including pseudorandom quantum states and quantum key distribution.

Our work therefore provides evidence that algebraic techniques based on group actions may be useful for constructing QCCC cryptographic primitives beyond the trapdoor-based paradigm. A naturally arising open question is whether stronger forms of remote state preparation, such as standard blind or verifiable RSP, can also be constructed from trapdoor-free assumptions.

1.1 Main Results and Technical Overview

In this section, we describe our main contributions and the key ideas underlying these results. We first introduce a new family of remote state preparation protocols, called *eavesdropper-blind remote state preparation* (EB-RSP), and show how to construct a *two-message* version of EB-RSP from certain one-way group actions (OWGAs) and, as a side result, also from plain trapdoor claw-free functions (TCFs). We then explain the role of EB-RSP and, in particular, show that the two-message version is sufficient for constructing quantum public-key encryption (QPKE) schemes with classical public keys and quantum ciphertexts. By combining these two results, we obtain a construction of QPKE from specific OWGAs and from TCFs.

1.1.1 Eavesdropper-Blind Remote State Preparation

We introduce a new primitive called *eavesdropper-blind remote state preparation*, which is a variant of RSP between a classical verifier V and a quantum prover P. Loosely speaking, it ensures that, at the end of the protocol, P holds a single-qubit state from a very large family of states that we call *root of unity states*, while V efficiently learns the classical description of that state. The security guarantee ensures that any QPT eavesdropper given the transcript of the classical communication between an honest V and an honest P learns no information about the prepared quantum state.[2]

[2]We emphasize that the definition of eavesdropper blindness differs from the well-known notion of *honest-but-curious blindness*: in our setting, we require blindness only against a malicious third party that has access to the transcript generated by the honest verifier and honest prover, rather than against the honest prover participating in

Definition 1.1 (EB-RSP, Informal)**.** *An* eavesdropper-blind remote state preparation *protocol is an interactive protocol between a PPT verifier V and a QPT prover P that satisfies the two properties:*

- (Correctness) *At the end of the protocol, the honest prover P holds the state*

$$|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle),$$

  for some angle $\theta \in \Theta_N := \left\{k \cdot \frac{2\pi}{N} \mid 0 \leq k \leq N-1\right\}$. On the other hand, the verifier V holds the classical description of the state, namely θ.

- (Eavesdropper Blindness) *After the execution of the EB-RSP protocol (between the honest verifier V and the honest prover P), no QPT eavesdropper $\mathcal{A}$ that receives the transcript of the execution can distinguish the real θ from a uniformly random sample drawn from Θ_N.*

We also consider a *two-message* version of this definition, in which the communication consists of a message from the verifier followed by a message from the prover.

Our main theorem is that specific OWGAs are sufficient to realize two-message EB-RSPs. Before stating this result, we first introduce the definitions of a group action and the one-wayness property.

Definition 1.2 (Group Action)**.** *Let G be an arbitrary group and X be a non-empty set. A* group action *is a map*

$$\begin{aligned} \star : G \times X &\to X \\ (g, x) &\mapsto g \star x, \end{aligned}$$

such that the following conditions hold:

1. *$1 \star x = x$ for all $x \in X$, where 1 is the identity element of G;*
2. *$g \star (h \star x) = (gh) \star x$ for all $g, h \in G$ and all $x \in X$.*

Note that we use multiplicative notation for statements and definitions concerning arbitrary, potentially non-abelian groups. However, we consistently use additive notation for the abelian groups appearing in the construction.

We call a group action *free* (or *semiregular*) if the condition $g \star x = x$ for some $x \in X$ already implies that $g = 1$ (which intuitively corresponds to injectivity). Moreover, to place this mathematical object on cryptographic foundations, we assume, loosely speaking, that we work with finite objects and that all main operations on the group can be carried out efficiently. The one-wayness property states that, if a QPT adversary is given $(x, s \star x)$, where $x \leftarrow X$ and $s \leftarrow G$, it is hard to output an s' such that $s' \star x = s \star x$; that is, it is hard to find a preimage of $s \star x$ under the group action with respect to x.

Equipped with these definitions, we can now state our main result:

Theorem 1.3 (OWGA implies EB-RSP, Informal)**.** *The existence of a free OWGA $\star : G \times X \to X$, where $G = \mathbb{Z}_p^\lambda$ for a prime p, implies the existence of a two-message EB-RSP.*

the RSP protocol itself. The key distinction is therefore that the eavesdropper does not obtain access to the internal state of the honest prover, and hence also not to the prepared state, making this definition strictly weaker.

Let us first describe the protocol at a high level, and afterwards provide intuitive explanations for why correctness and security hold. At a high level, our construction proceeds as follows:

1. **Verifier**: Samples $x_0 \leftarrow X$ and $r, s \leftarrow G$, and computes $x_1 := (-s) \star x_0$. Sends (x_0, x_1, r) to the prover.
2. **Prover**:
   (a) Prepares the state $\sum_{b\in\{0,1\},g\in G} |b, g\rangle$.
   (b) Given x_0 and x_1, computes the state:
   $$\sum_{b\in\{0,1\},g\in G} |b, g, g \star x_b\rangle \,.$$
   (c) Measures the third register in the standard basis and uses r to prepare the state:
   $$|0, g_0, \langle g_0, r\rangle\rangle + |1, g_0 + s, \langle g_0 + s, r\rangle\rangle \,.$$
   (d) Measures the last two registers in the QFT basis, resulting in outcomes g and z. Sends (g, z) to verifier.
   (e) Outputs $|+_\theta\rangle$, where $\theta := \langle s, z \cdot r + g\rangle$.
3. **Verifier**: Uses s, r, z, g to compute θ.

Correctness. Let us start by explaining why this procedure intuitively yields our desired quantum state. We basically rely on two properties of the free OWGA: the freeness and the algebraic properties of the group action. After measuring the last register in step (b) of the prover, the state collapses to a *claw state* of the form

$$|0, g_0\rangle + |1, g_0 + s\rangle \,,$$

because the group action is, by assumption, free (which translates roughly to being injective in some sense). Later, in step (d), we measure this quantum state in the Fourier basis to push the appearing terms in the state into a relative phase. Because of the algebraic properties of the group action, unknown parameters like g_0 cancel out, and we are left with $\theta := \langle s, z \cdot r + g\rangle$, which can be efficiently computed by the verifier.

Security. Let us now move on to the intuitive explanation of the security. This follows relatively immediately, since g is a uniform element in G and independent of everything (as the prover behaves honestly). Thus, θ essentially consists of a secret s, unknown to the adversary, and a uniformly random quantity $z \cdot r + g$, which is independent of everything. This is exactly the setting of the quantum version of the Goldreich-Levin theorem for large fields given in Theorem 2.6, which states that this quantity is computationally indistinguishable from uniform.

Protocol Simplification. After completing the first version of the current paper, we realized that the presented protocol can be further simplified, as also pointed out independently by an anonymous Asiacrypt reviewer. Concretely, the protocol can be simplified by removing r and the measurement outcome z from the construction altogether, which has the same effect as setting

$r = 0$, i.e., the all-zero string. Completeness remains unchanged, as it holds for every value of r. For eavesdropper blindness, observe that, for any fixed verifier randomness r and any outcome of the inner product register measurement, the Fourier outcome g is uniformly distributed over G. In particular, g is uniform and independent of the verifier's first message. And now one can use the Goldreich-Levin argument for $\langle s, g\rangle$ as before.

Family of Output States. Our EB-RSP is more general than most existing protocols in terms of the family of states it can remotely prepare. We consider N states equally spaced on the (X, Y)-plane of the Bloch sphere, which we call *root of unity states*, since they are $|+\rangle$ states with relative phases given by the N-th roots of unity. Most prior RSP protocols cover only special cases of this family, such as BB84 states [BK25] and generalized BB84 states [CCKW19, GV19, AMMW22, BKM+25, Zha25].

Moreover, the presented protocol is for states with $N = p$ being a prime, but it also extends to $N = p_1 \cdots p_m$ for pairwise distinct primes p_i by combining the above EB-RSP in parallel. View the presented EB-RSP as a subroutine in which the verifier inputs p and the prover inputs a one-qubit state. At the end of the subroutine, a relative phase is included on the prover's input qubit, while the verifier knows this relative phase. Then run the subroutine for all p_i, yielding a state $|+_\theta\rangle$ with $\theta = \theta_1 + \ldots + \theta_m$ and $\theta_i \in \Theta_{p_i}$. Note that, in the end, $\theta = \theta_1 + \ldots + \theta_m \in \Theta_N$ by simply extending the fractions, which gives the desired EB-RSP for more general N. Security follows from the independence of the subroutines, the security for each θ_i, and the distinctness of the primes. However, how to extend this idea to powers of primes remains unclear.

No requirement of trapdoor. As we can see, the EB-RSP protocol presented here does not require the verifier V to use a trapdoor to compute the classical description of the quantum state, i.e. V does not have to invert a function using secret information, since we exploit only the algebraic properties of the group action to cancel out parameters unknown to the verifier. This ensures that only parameters known to the verifier appear in the quantum state while still maintaining security. To the best of our knowledge, this is the first RSP-type primitive with useful applications that does not rely on any trapdoor. The techniques used here could enable the blind preparation of more specific quantum states with stronger security properties without relying on a trapdoor primitive, thereby taking a step toward reducing the cryptographic assumptions underlying many protocols, as RSP protocols form the backbone of many quantum cryptographic schemes. This is an important goal, as reducing complexity assumptions remains a major ongoing work in cryptography.

This new primitive will ultimately be used in Section 4 to construct a quantum public-key encryption (QPKE) scheme with classical public keys in a black-box fashion. We also want to highlight that since our EB-RSP includes a wide range of output states, together with a relatively weak security definition, we can hope for relatively simple constructions from different cryptographic assumptions, allowing the QPKE to be instantiated from a wider range of assumptions. It might also be the case that many known RSPs already fall into our category of EB-RSP, such as the protocol presented in [BKM+25] (described in Section A), after a few suitable modifications, yielding the following result:

Theorem 1.4 (TCF implies EB-RSP, Informal)**.** *The existence of a plain TCF implies the existence of a two-message EB-RSP.*

1.1.2 Quantum Public-Key Encryption with Classical Public Keys

Our main result about QPKE is the black-box construction from two-message EB-RSP.

Theorem 1.5 (EB-RSP implies QPKE, Informal)**.** *The existence of a two-message EB-RSP implies the existence of a QPKE scheme with classical public keys and quantum ciphertexts.*

Before presenting the high-level description of the construction, we list the corollaries obtained from the above theorem by combining it with the previous theorems.

Corollary 1.6 (OWGA implies QPKE, Informal)**.** *The existence of a free OWGA $\star : G \times X \to X$, where $G = \mathbb{Z}_p^\lambda$ for a prime p, implies the existence of a QPKE scheme with classical public keys and quantum ciphertexts.*

Corollary 1.7 (TCF implies QPKE, Informal)**.** *The existence of a plain TCF implies the existence of a QPKE scheme with classical public keys and quantum ciphertexts.*

Remark 1.8. *The assumption-level conclusions of Corollaries 1.6 and 1.7 can also be obtained by specializing the framework of [HMY23]. Concretely, for the free group actions considered here, define $f_b(h) := h \star x_b$, for $b \in \{0,1\}$. Freeness implies that each f_b is injective, while one-wayness of the group action implies that the pair (f_0, f_1) is claw-free. Since injective functions are collapsing, [HMY23] shows that claw-freeness together with collapsingness implies conversion hardness, which in turn suffices for constructing an IND-CPA-secure QPKE scheme with classical public keys and quantum ciphertexts. Likewise, a TCF gives a swap-trapdoor function pair: trapdoor inversion recovers the unique matching preimage in the other branch, and the branch functions are injective and claw-free. Consequently, the two assumption-level QPKE corollaries above should be viewed as alternative modular derivations rather than new feasibility results relative to [HMY23].*

Let us now describe how the QPKE scheme from two-message EB-RSP looks at a high level, and afterwards give intuitive explanations of why correctness and security hold. For this, we first present the main ingredients of the definition of a QPKE scheme with classical public keys for classical one-bit messages. How to extend the message space is explained in Section 4.1. Such a QPKE scheme consists of the algorithms $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$:

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$. This is a PPT algorithm that takes the security parameter 1^λ as input and outputs a classical public key pk and a classical secret key sk.
- $\mathsf{Enc}(\mathsf{pk}, b) \to ct$. This is a QPT algorithm that takes a public key pk and a message $b \in \{0,1\}$ as input and outputs a quantum ciphertext ct.
- $\mathsf{Dec}(\mathsf{sk}, ct) \to b' / \perp$. This is a QPT algorithm that takes a secret key sk and a ciphertext ct as input and outputs a message $b' \in \{0,1\}$ or $\perp$.

For security, we follow the standard IND-CPA security definition. Note that our main theorem concerns the construction of QPKE from *any* two-message EB-RSP. For the sake of understanding, we focus in this section on the concrete protocol presented above and give a simplified version here.

At a high level, our construction works as follows.

- KeyGen: We define the public key $\mathsf{pk} := (x_0, x_1, r)$ to be the first message sent by the verifier, and the secret key $\mathsf{sk} := s$ to be the internal state of the verifier after sending the first message. It is essentially the information that the verifier does not reveal and later uses to compute the secret angle.

- Enc: To encrypt a bit $b \in \{0,1\}$, one goes through all the steps the prover performs in the EB-RSP, after receiving the message from the verifier, until obtaining a quantum state $|+_\theta\rangle$ and the two outcomes (z, g). One then applies a unitary $U_b := R_z(b \cdot \left\lfloor \frac{N}{2} \right\rfloor \cdot \frac{2\pi}{N})$, which encodes the information about b, to the state, and outputs $ct := (U_b |+_\theta\rangle, z, g)$ as the ciphertext. Thus, the ciphertext consists of the messages sent by the prover in the EB-RSP together with a unitary, depending on b, applied to the output state.

- Dec: One uses the secret key $\mathsf{sk} = s$ and the classical information within the ciphertext, to recover θ. One then applies the unitary $R_z(-\theta)$ to the quantum state, yielding the state $U_b |+\rangle$. Lastly, one measures this state in the Hadamard basis to obtain the initial message b.

Correctness. As mentioned, we consider only a simplified version here in order to understand the mechanics of the QPKE scheme. In the decryption phase, we measure the state $U_b |+\rangle$ in the Hadamard basis. This state is precisely $|+\rangle$ for $b = 0$, and is a state very close to $|-\rangle$ for $b = 1$. Hence, correct decryption occurs with relatively high probability. In the actual scheme, this probability is amplified by encrypting many states and taking the majority vote of the outcomes.

Security. For security, the adversary essentially has access to the public key pk and the ciphertext $ct = (U_b |+_\theta\rangle, z, g)$. We may even imagine giving the adversary the classical description of the state, which can only increase the adversary's advantage, yet it remains negligible, as we will see. This classical description can essentially be written as $\theta + b \cdot \left\lfloor \frac{N}{2} \right\rfloor \cdot \frac{2\pi}{N}$. Since θ is computationally indistinguishable from uniform due to the eavesdropper blindness of the EB-RSP, this classical information hides b, giving the adversary no non-negligible advantage in guessing b.

On the Security of the EB-RSP for QPKE. Our EB-RSP security definition considers the full angle $\theta = k \cdot \frac{2\pi}{N}$ with $k \in \mathbb{Z}_N$ to be computationally indistinguishable from uniform. When N is a power of 2, this means that every bit of k is hidden.

But note that for IND-CPA security, we only need the most significant bit of k to be computationally indistinguishable, since our encryption essentially flips the most significant bit of k within the quantum state when N is a power of 2. For general N, this translates to effectively hiding the single bit of information corresponding to whether $0 \leq k < \left\lfloor \frac{N}{2} \right\rfloor$ or $\left\lfloor \frac{N}{2} \right\rfloor \leq k < N$, that is, whether θ lies on the upper half or the lower half of the unit circle. Thus, requiring only that this information be hidden would be sufficient to ensure IND-CPA security. This is exactly equivalent to hiding the most significant bit of k when N is a power of 2. An interesting fact is that all other known RSPs do it the other way around: they try to hide all but the most significant bit (since it is impossible to hide everything while allowing the prover itself to be malicious).

1.2 Discussions

In this section, we discuss related work and outline several future directions.

Related Work. A long line of work on remote state preparation has focused on achieving strong notions of blindness and verifiability from trapdoor-based cryptographic assumptions, most notably variants of trapdoor claw-free functions [CCKW19, GV19, AMMW22, GV24, BK25, BKM+25, Zha25]. In contrast, our work studies whether weaker forms of remote state preparation may still suffice for meaningful cryptographic applications while admitting constructions from qualitatively

different assumptions. More concretely, our work introduces EB-RSP, a weaker RSP-type primitive satisfying only blindness against eavesdroppers. Conceptually, our approach differs from prior RSP constructions in two ways. First, we relax the blindness requirement compared to standard malicious-server blindness notions. Second, rather than relying on trapdoor cryptographic primitives, our construction exploits algebraic properties of one-way group actions to obtain a classical description of the prepared state.

Group actions and related algebraic assumptions have previously appeared in several quantum cryptographic constructions. In particular, [HMY23] constructs QPKE with classical public keys and quantum ciphertexts through the abstraction of conversion-hard swap-trapdoor function pairs. Their general group-action instantiation is analyzed under a *pseudorandomness* assumption to obtain the QPKE construction. However, as discussed in Remark 1.8, it can also be shown that their framework also yields the OWGA-to-QPKE consequence for the free group actions considered here: freeness makes the associated branch functions injective and hence collapsing, while one-wayness of the action implies claw-freeness; their conversion-hardness result then yields QPKE. Our work pursues a complementary objective. We introduce two-message EB-RSP as an abstract state-preparation functionality that already suffices for QPKE, establish a generic black-box transformation from any two-message EB-RSP to QPKE and construct such an EB-RSP from free OWGAs without relying on a trapdoor. This modular route separates the construction of the remote state preparation primitive from its use in encryption and, to the best of our knowledge, yields the first trapdoor-free RSP-type primitive with a concrete cryptographic application.

The idea of constructing QPKE from RSP has also appeared in prior work. In particular, [BK25] showed how to construct QPKE with classical public keys and classical ciphertexts from RSPs based on dual-mode trapdoor claw-free functions. In contrast, our work shows that even weaker forms of RSP already suffice for constructing QPKE with classical public keys, albeit with quantum ciphertexts. Furthermore, we observe that existing RSP constructions appear naturally adaptable to our two-message EB-RSP notion. We demonstrate this explicitly for a concrete TCF-based RSP construction, immediately yielding a construction of QPKE from plain TCFs.

Future Directions. Our work suggests several directions for future research. A first conceptual direction is to better understand the landscape of weaker RSP-type primitives and their cryptographic applications. In this work, we showed that even the relatively weak notion of EB-RSP already suffices to construct QPKE with classical public keys and quantum ciphertexts. This raises the broader question of which security properties of remote state preparation are truly necessary for various quantum cryptographic tasks. For instance, it would be relevant to identify additional applications that can already be realized from the security notion of eavesdropper-blindness, particularly in the QCCC model.

Another interesting direction is to investigate whether similar ideas can be extended to obtain stronger notions of remote state preparation, such as blind or verifiable RSP, from trapdoor-free assumptions.

Towards stronger RSP and proofs of quantumness. A natural direction is to investigate whether the algebraic phase-generation mechanism developed here can be combined with additional techniques to obtain stronger notions of remote state preparation, such as blindness against a malicious prover or verifiable RSP, while retaining trapdoor-free assumptions. Furthermore, several RSP and proof-of-quantumness protocols exploit closely related tools, including coherent claw states and measurements in complementary or Fourier bases. Therefore, a closely related target would be the construction of proofs of quantumness from group-action-based assumptions.

Finally, several technical questions remain open. One natural direction is whether our OWGA-based construction can be generalized beyond the current classes of groups considered in this work. Another is whether similar techniques could eventually yield QPKE schemes with classical public keys and classical ciphertexts, as in [BK25], while still avoiding trapdoor assumptions.

Disclosure on the use of AI. The authors declare that no AI tools were used at any stage of the research process. All intellectual and written contributions to the study were made by the authors without AI assistance.

2 Preliminaries

We denote the security parameter by $\lambda \in \mathbb{N}$. A function negl is called *negligible* if it vanishes faster than the absolute value of any inverse polynomial. We denote by $\omega_n = e^{2\pi i/n}$ the n-th root of unity. We define the set

$$\Theta_N := \left\{ k \cdot \frac{2\pi}{N} \mid 0 \leq k \leq N-1 \right\}$$

for any positive integer N, as we will work with it extensively. We also define the rotated $|+\rangle$ state

$$|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle),$$

which is defined for any $\theta \in \mathbb{R}$. Lastly, for any $\theta \in \mathbb{R}$, we define the *rotation operator about the z-axis* with respect to the Bloch sphere as follows:

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix},$$

which is equivalent to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{smallmatrix}\right)$ up to a global phase.

2.1 One-Way Group Actions

We briefly lay the mathematical foundation of this work by recalling the definition of an abstract group action in the mathematical sense. We then place this mathematical object on cryptographic grounds by requiring that certain operations are efficient, together with equipping it with a cryptographic assumption: the *one-wayness*, as in the seminal work of Brassard and Yung [BY91].

Let us now fix the notation used for groups throughout this work. For abelian groups G, we use additive notation to denote the group operation, i.e., $g + h$ for elements $g, h \in G$. Moreover, the neutral element is denoted by 0, and the inverse of an element $g \in G$ by $-g$. For general groups G that may not be abelian, we use multiplicative notation to denote the group operation, i.e., $g \cdot h$ or gh for elements $g, h \in G$. Moreover, the neutral element is denoted by 1, and the inverse of an element g by g^{-1}. In the remaining of the paper we will use multiplicative notation for statements and definitions concerning arbitrary, potentially non-abelian groups. However, we consistently use additive notation for the abelian groups appearing in the constructions later on.

Definition 2.1 (Group Action)**.** *Let G be an arbitrary group and X be a non-empty set. A* group action *is a map*

$$\star : G \times X \to X$$

$$(g, x) \mapsto g \star x,$$

such that the following conditions hold:

1. $1 \star x = x$ *for all* $x \in X$*;*
2. $g \star (h \star x) = (gh) \star x$ *for all* $g, h \in G$ *and all* $x \in X$*.*

We now introduce some common terminology used when working with group actions. Let $x \in X$ be any element. We call

$$G_x := \{g \in G \mid g \star x = x\}$$

the *stabilizer group* of x. The group action is called *free* (or *semiregular*) if the statement that $g \star x = x$ for some $x \in X$ already implies that $g = 1$. Or in other words, the stabilizer group of each x is trivial.

Next, we place this mathematical object on cryptographic grounds. To do this, we essentially assume that we work with finite objects and that all important operations we need to perform can be carried out efficiently. We follow (more or less) the definition given in [HMY23, Definition 4.13], but we do not require all the properties they list.

Definition 2.2 (Effective Group Action)**.** *A group action* $\star : G \times X \to X$ *is called an* effective group action (EGA) *if the following properties hold:*

(i) G *and* X *are finite.*

(ii) *There are classical deterministic polynomial-time algorithms that compute the multiplication* $g \cdot h$*, the inverse* g^{-1}*, and the group action* $g \star x$ *for all* $g, h \in G$ *and* $x \in X$*.*

(iii) *There are PPT algorithms that sample uniformly at random from* G *and* X*.*

(iv) *There is a QPT algorithm that generates a uniform superposition over all elements* $g \in G$*.*

Such EGAs can now be endowed with cryptographic hardness assumptions, and researchers always come up with new hardness assumptions for cryptographic group actions to prove the security of their protocols. We will focus on one of the weakest such assumptions among all assumptions currently in circulation.

Definition 2.3 (One-Way Group Action)**.** *An effective group action* $\star : G \times X \to X$ *is called an* one-way group action (OWGA) *if, for any QPT adversary* $\mathcal{A}$*, we have*

$$\Pr_{\substack{s \leftarrow G \\ x \leftarrow X}}\left[s' \star x = s \star x \ : \ s' \leftarrow \mathcal{A}(1^\lambda, x, s \star x)\right] = \mathsf{negl}(\lambda).$$

Note that for a free group action, the QPT adversary has to find s itself.

2.2 Quantum Fourier Transform over Finite Abelian Groups

Let G be a finite abelian group. By the well-known Fundamental Theorem of Finite Abelian Groups, we know that every finite abelian group G is isomorphic to a direct sum of cyclic groups

$$\mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k},$$

for some non-negative integer k and specific N_i, each of which is a power of a (not necessarily distinct) prime. For simplicity, we assume that G equals such a group, that is, $G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$. For an element $g \in G$, we denote its i-th component by g_i, that is, $g = (g_1, \ldots, g_k)$. Moreover, we define the map $\chi : G \times G \to \mathbb{C}$ by

$$\chi(h, g) := \omega_{N_1}^{h_1 g_1} \cdots \omega_{N_k}^{h_k g_k}.$$

We are now ready to define the quantum Fourier transform.

Definition 2.4 (Quantum Fourier Transform over Finite Abelian Groups)**.** *The* quantum Fourier transform (QFT) over finite abelian groups G *is the unitary operator* QFT_G *defined by*

$$\mathsf{QFT}_G \left|g\right\rangle = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \chi(h, g) \left|h\right\rangle.$$

Note that the QFT decomposes as

$$\mathsf{QFT}_G = \mathsf{QFT}_{\mathbb{Z}_{N_1}} \otimes \ldots \otimes \mathsf{QFT}_{\mathbb{Z}_{N_k}},$$

and can therefore be implemented efficiently.

Next, we introduce some notation to make the expressions appearing later in this work more concise. Define $M := \mathrm{lcm}(N_1, \ldots, N_k)$ to be their least common multiple. For each $1 \leq i \leq k$, set $R_i := M/N_i$. Consider the following two maps:

$$\begin{aligned} f_1 : G \times G &\to G \\ (h, g) &\mapsto (h_1 g_1, \ldots, h_k g_k), \end{aligned}$$

where each multiplication is performed with respect to the corresponding modulus, and

$$\begin{aligned} f_2 : G &\to \mathbb{Z}_M \\ e &\mapsto \sum_{i=1}^{k} e_i R_i, \end{aligned}$$

where the multiplication and summation are performed modulo M. Both maps are clearly well defined. Lastly, we define the map

$$\langle \cdot, \cdot \rangle : G \times G \to \mathbb{Z}_M$$

via $\langle \cdot, \cdot \rangle = f_2 \circ f_1$, which is the composition of the two maps defined above. It is easy to see that $\langle \cdot, \cdot \rangle$ is symmetric and homomorphic in both components; that is, $\langle h, g \rangle = \langle g, h \rangle$ and $\langle h + g, e \rangle = \langle h, e \rangle + \langle g, e \rangle$. Now, to draw the connection to χ, we observe that

$$\chi(h, g) = \omega_{N_1}^{h_1 g_1} \cdots \omega_{N_k}^{h_k g_k} = \omega_M^{h_1 g_1 R_1} \cdots \omega_M^{h_k g_k R_k} = \omega_M^{\langle h, g \rangle}.$$

Hence, the newly established notation allows us to express χ more concisely. Moreover, this immediately shows that χ is also symmetric in h and g, that is, $\chi(h, g) = \chi(g, h)$, and bilinear; that is, $\chi(h + g, e) = \chi(h, e) \cdot \chi(g, e)$, with a similar property holding for the second component. In this work, we focus on the case where $N_1 = \ldots = N_k = p$ for a prime p. Consequently, $M = p$, and every operation is performed modulo p.

2.3 Quantum Goldreich-Levin Theorem for Large Fields

We recall generalized Goldreich-Levin theorems over large fields, one for classical adversaries and one for quantum adversaries. We begin with the classical version.

Theorem 2.5 (Classical Goldreich-Levin Theorem for Large Fields [DGK+10, Theorem 1])**.** *Let p be prime, and let H be an arbitrary subset of $\mathbb{Z}_p$. Let $f : H^\lambda \to \{0,1\}^*$ be any (possibly randomized) function. If there is a distinguisher $\mathcal{D}$ that runs in time t such that*

$$\left| \Pr_{\substack{x\leftarrow H^\lambda \\ y\leftarrow f(x) \\ r\leftarrow \mathbb{Z}_p^\lambda}}[\mathcal{D}(y,r,\langle r,x\rangle)=1] - \Pr_{\substack{x\leftarrow H^\lambda \\ y\leftarrow f(x) \\ r\leftarrow \mathbb{Z}_p^\lambda \\ u\leftarrow \mathbb{Z}_p}}[\mathcal{D}(y,r,u)=1] \right| = \varepsilon,$$

then there is an inverter $\mathcal{A}$ that runs in time $t' = t \cdot \mathsf{poly}(\lambda, |H|, 1/\varepsilon)$ such that

$$\Pr_{\substack{x\leftarrow H^\lambda \\ y\leftarrow f(x)}}[\mathcal{A}(y)=x] \geq \frac{\varepsilon^3}{512\cdot\lambda\cdot p^2}.$$

Now, we want to obtain a quantum version of the above theorem. To do this, we use the same idea explained in [APV23] by applying [APV23, Theorem 4.1], an adapted version of [BBK22, Theorem 7.1], to Theorem 2.5. This converts classical reductions into post-quantum reductions.

Theorem 2.6 (Quantum Goldreich-Levin Theorem for Large Fields)**.** *Let p be prime, and let H be an arbitrary subset of $\mathbb{Z}_p$. Let $\Phi : \mathcal{L}(\mathcal{H}_p^{\otimes\lambda}) \to \mathcal{L}(\mathcal{H}_{\mathsf{Aux}})$ be any CPTP map with auxiliary system $\mathcal{H}_{\mathsf{Aux}}$, where $\mathcal{H}_p$ is p-dimensional. If there is a quantum distinguisher $\mathcal{D}$ that runs in time t such that*

$$\left| \Pr_{\substack{x\leftarrow H^\lambda \\ \mathsf{aux}\leftarrow\Phi(|x\rangle\langle x|) \\ r\leftarrow \mathbb{Z}_p^\lambda}}[\mathcal{D}(\mathsf{aux},r,\langle r,x\rangle)=1] - \Pr_{\substack{x\leftarrow H^\lambda \\ \mathsf{aux}\leftarrow\Phi(|x\rangle\langle x|) \\ r\leftarrow \mathbb{Z}_p^\lambda \\ u\leftarrow \mathbb{Z}_p}}[\mathcal{D}(\mathsf{aux},r,u)=1] \right| = \varepsilon,$$

then there is a quantum extractor $\mathcal{E}$ that runs in time $t' = t \cdot \mathsf{poly}(\lambda, |H|, 1/\varepsilon)$ such that

$$\Pr_{\substack{x\leftarrow H^\lambda \\ \mathsf{aux}\leftarrow\Phi(|x\rangle\langle x|)}}[\mathcal{E}(\mathsf{aux})=x] \geq \mathsf{poly}(\varepsilon, 1/\lambda, 1/p).$$

We will work with this theorem in the setting where p is polynomial in λ, $H = \mathbb{Z}_p$, Φ computes the output of a quantumly secure one-way function f, and $\mathcal{D}$ is a QPT algorithm. In this setting, the advantage ε of $\mathcal{D}$ is negligible, i.e., the hardcore predicate $\langle r, x\rangle$ looks uniformly random from the adversary's view.

3 Eavesdropper-Blind Remote State Preparation

In this section, we present a new type of *remote state preparation* (RSP) protocol for *root of unity states*, which generalize the BB84 states,

$$|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle),$$

where

$$\theta \in \Theta_N := \left\{ k \cdot \frac{2\pi}{N} \mid 0 \leq k \leq N-1 \right\},$$

from free OWGAs associated with certain groups. We consider a weaker security notion for RSP than the standard ones, which we call *eavesdropper blindness*, shifting the focus from the server to an external eavesdropper. We emphasize that the definition of eavesdropper blindness differs from the well-known notion of *honest-but-curious blindness*: in our setting, we require blindness only against a malicious third party that has access to the transcript generated by the honest verifier and honest prover, rather than against the honest prover participating in the RSP protocol itself. The key distinction is therefore that the eavesdropper does not obtain access to the internal state of the honest prover, and hence also not to the prepared state, making this definition strictly weaker.

A *two-message version* of this new primitive will ultimately be used in Section 4.2 to construct a quantum public-key encryption (QPKE) scheme with classical public keys in a black-box fashion. Although this section provides a concrete instantiation based on certain OWGAs, we later adopt a modular approach to the QPKE construction that relies only on the abstract definition of a two-message eavesdropper-blind RSP (EB-RSP) protocol, rather than on any specific instantiation. This allows any two-message EB-RSP protocol to be used within the QPKE scheme. Nevertheless, the protocol presented here may be of independent interest. In particular, we construct this two-message EB-RSP from a cryptographic primitive in such a way that the verifier does not require a trapdoor, since the construction exploits only the algebraic properties of the group action. To the best of our knowledge, this is the first RSP-type primitive that does not rely on any trapdoor. The techniques used here could enable the blind preparation of more specific quantum states with stronger security properties without relying on a trapdoor primitive, thereby taking a step toward reducing the cryptographic assumptions underlying many protocols, as RSP protocols form the backbone of many quantum cryptographic schemes. This is an important goal, as reducing complexity assumptions remains a major ongoing work in cryptography.

3.1 Definition

We start by providing a formal definition of this new primitive and will later explain in more detail its functionality and how it compares to other common RSP definitions.

Definition 3.1 (Eavesdropper-Blind Remote State Preparation)**.** *An* eavesdropper-blind remote state preparation (EB-RSP) *protocol consists of a pair of interactive algorithms* (V, P)*, with the security parameter in unary* 1^λ *as input: A classical probabilistic polynomial-time algorithm* V*, called the* verifier*, and a quantum polynomial-time algorithm* P*, called the* prover*. We require the protocol to satisfy the following properties:*

- (Correctness) *The protocol terminates successfully with probability at least* $1 - \mathsf{negl}(\lambda)$*. Furthermore, upon successful completion, the honest prover* P *holds the state*

$$|+_\theta\rangle$$

for an angle $\theta \in \Theta_N := \left\{ k \cdot \frac{2\pi}{N} \mid 0 \leq k \leq N-1 \right\}$*, where* $N = N(\lambda)$ *is a positive integer that depends on* λ*. The verifier, on the other hand, holds the classical description of the state, i.e.* θ*. Denote the transcript of the classical communication by* trans*.*

- (Eavesdropper Blindness) *Consider the following experiment* $\mathrm{Exp}(1^\lambda, V, P, \mathcal{A})$ *played between an honest verifier* V*, an honest prover* P*, and an eavesdropper* $\mathcal{A}$*.*[3]

  – V *and* P *engage in the interactive EB-RSP protocol. If the protocol does not terminate successfully, the experiment outputs* 1 *with probability* $\frac{1}{2}$ *and* 0 *with probability* $\frac{1}{2}$*. If the protocol does terminate successfully, it continues as follows:*

  – *Let* $|+_\theta\rangle$ *be the output state held by* P*, and* θ *the output of* V*. Send the EB-RSP transcript* trans *to* $\mathcal{A}$*.*

  – *Flip a coin* $c \leftarrow \{0,1\}$*. If* $c = 0$*, set* $\theta_{\mathsf{chal}} := \theta$*, otherwise sample* $\theta_{\mathsf{chal}} \leftarrow \Theta_N$ *uniformly at random. Send* θ_{chal} *to* $\mathcal{A}$*, who returns a bit* c'*.*

  – *The experiment outputs* 1 *if* $c' = c$ *and* 0 *otherwise.*

  We require that for all QPT adversaries $\mathcal{A}$ *there exists a negligible function* negl *such that for all sufficiently large* $\lambda \in \mathbb{N}$*:*

$$|\Pr\Big[\mathrm{Exp}(1^\lambda, V, P, \mathcal{A}) = 1\Big] - \frac{1}{2}| \leq \mathsf{negl}(\lambda).$$

We call it a two-message EB-RSP *if it additionally consists of exactly two messages: one from the verifier, followed by one from the prover. In this case, we use the following notation to describe the algorithms within the protocol:*

- $\mathsf{EB\text{-}RSP.Setup}(1^\lambda) \to (\mathsf{msg}_V, \mathsf{st}_V)$*. The verifier takes as input the security parameter* 1^λ *and outputs a message* msg_V *and a state* st_V*.*

- $\mathsf{EB\text{-}RSP.QComp}(\mathsf{msg}_V) \to (|+_\theta\rangle, \mathsf{msg}_P)$*. The prover takes as input the verifier's message and outputs the state* $|+_\theta\rangle$ *and a message* msg_P*.*

- $\mathsf{EB\text{-}RSP.Dec}(\mathsf{st}_V, \mathsf{msg}_P) \to \theta$*. The verifier takes as input its state* st_V *and the prover's message* msg_P*, and outputs* θ*.*

Family of Output States. First, our EB-RSP is more general than other known RSP protocols in terms of the family of states being remotely prepared. In our case, we consider N states that lie equidistantly on the (X, Y)-plane of the Bloch sphere, which we call *root of unity states*, as they correspond to the $|+\rangle$ state with a relative phase described by the N-th roots of unity. Most existing RSP constructions work with a special case of this family of states, including BB84 states [BK25] and generalized BB84 states [CCKW19, GV19, AMMW22, BKM+25, Zha25]. However, there is also at least one other known RSP protocol that does not fall into this category and instead prepares EPR pairs [GV24].

Security. The main difference between our EB-RSP and others lies in the security notion. Standard RSP security definitions aim to hide the angle θ from the quantum prover. Moreover, these

[3]Note that, for our security definition, in the experiment we consider indistinguishability-type security for θ. One might think that a search-type security definition, in which the adversary is asked to output the correct θ from the search space Θ_N, would generally be sufficient, but this is not the case. In fact, if the search space, parameterized here by N, is polynomial in the security parameter λ, then the two definitions are equivalent. However, for general N, and in particular when N is exponential in λ, indistinguishability-type security is strictly stronger and necessary for our QPKE construction. Loosely speaking, search-type security may reveal bits of θ that must remain hidden from the eavesdropper in the QPKE construction.

definitions typically allow the prover to deviate arbitrarily from the protocol while still requiring that θ remains hidden, with the disadvantage of introducing an undesired *byproduct bit*[4], over which the verifier has no control and for which one usually has no security guarantees. By contrast, our security notion concerns hiding the angle only from an external third party that passively intercepts the communication between an honest verifier and an honest prover, and no undesired byproduct bit appears in this construction. More precisely, eavesdropper blindness means that the protocol is blind only with respect to a passive third-party observer of the communication channel, and not with respect to the server itself. Crucially, this security notion is still sufficient for our QPKE application, which motivates our introduction of eavesdropper blindness.

Before presenting our concrete instantiation based on certain OWGAs, we emphasize that suitable instantiations already exist. For example, the RSP protocol of [BKM+25], based on plain TCFs, already provides such an instantiation. A full description of the RSP is given in Section A. With only minor modifications, that protocol can be transformed into a two-message EB-RSP protocol by merging the verifier's messages into a single message and likewise merging the prover's messages. This transformation has no drawback on security. Note that their RSP prepares quantum states of the form

$$Z^b \left|+_\theta\right\rangle = \left|+_{(\theta+b\pi)}\right\rangle,$$

where $\theta \in \Theta_N$ with $N = 8$, and b is a single bit representing the undesired byproduct bit, while security holds only with respect to θ and not the entire angle $\theta + b\pi$, when the quantum prover is considered to be the adversary. With respect to eavesdropper blindness, however, one can verify, after a few algebraic manipulations, that from the eavesdropper's perspective, the angle $\theta + b\pi$ remains computationally indistinguishable from uniform, by an argument similar to the Goldreich-Levin argument used in their work. The intuitive reason for this is that, in the honest execution of the protocol, b is independent of θ, which may not be the case when the quantum prover behaves maliciously. Hence, we obtain the following result.

Theorem 3.2. *The existence of a plain TCF implies the existence of a two-message EB-RSP.*

This indicates that there may exist even more RSP protocols that can likewise be transformed into two-message EB-RSP protocols and subsequently used to construct QPKE schemes.

3.2 Construction from One-Way Group Actions

We now present a two-message EB-RSP protocol that uses a free OWGA associated with a certain group. The interesting aspect of this EB-RSP construction is that it does not rely on any trapdoor that would give the verifier a complete classical description of the state held by the prover. Instead, we exploit the algebraic properties of the group action to cancel out parameters unknown to the verifier, ensuring that only parameters known to the verifier appear in the quantum state while still maintaining security. This approach may be of independent interest, as the techniques used here could enable the blind preparation of more specific quantum states with stronger security properties without relying on a trapdoor primitive (as most RSPs rely on variants of TCFs).

We will first describe our two-message EB-RSP construction in Protocol 1. Afterwards, we show the correctness and the eavesdropper blindness of the protocol.

[4]The byproduct bit intuitively refers to a single bit from the entire description of θ, as we will see later in the discussion about the RSP from [BKM+25].

Protocol 1 Two-Message EB-RSP

Let

- λ be the security parameter
- $\star : G \times X \to X$ be a free OWGA
- $G = \mathbb{Z}_p^\lambda$ for a prime p, which is poly-sized in the security parameter λ

Protocol Steps:

1. V samples $x_0 \leftarrow X$ and $r, s \leftarrow G$. V computes $x_1 := (-s) \star x_0$, and sends (x_0, x_1, r) to P.
2. P proceeds as follows:
   (a) Prepare the state $\sum_{b\in\{0,1\},g\in G} |b, g\rangle$.
   (b) Evaluate in superposition the function $f(b, g) = g \star x_b$, resulting in the state
   $$\sum_{b\in\{0,1\},g\in G} |b, g, g \star x_b\rangle .$$
   (c) Measure the last register in the standard basis, resulting in outcome y and the state
   $$|0, g_0\rangle + |1, g_0 + s\rangle .$$
   (d) Evaluate in superposition the function $h(g) = \langle g, r\rangle$, resulting in the state
   $$|0, g_0, \langle g_0, r\rangle\rangle + |1, g_0 + s, \langle g_0 + s, r\rangle\rangle .$$
   (e) Apply QFT over $\mathbb{Z}_p$ to last register and measure to obtain a measurement outcome z.
   (f) Apply QFT over G to second register and measure to obtain a measurement outcome g.
   (g) Send (z, g) to V.
3. V outputs $\theta := \langle s, z \cdot r + g\rangle \cdot \frac{2\pi}{p}$, and P outputs the post-measurement state $|+_\theta\rangle$.

The main result of this section shows that Protocol 1 is a two-message EB-RSP (as defined in Definition 3.1):

Theorem 3.3. *The existence of a free OWGA $\star : G \times X \to X$, where $G = \mathbb{Z}_p^\lambda$ for a prime p, which is poly-sized in the security parameter λ, implies the existence of a two-message EB-RSP with $N = p$.*

Proof. We will break the proof into two parts: we will first show that Protocol 1 satisfies correctness in Theorem 3.4 and then show it achieves security, i.e. eavesdropper blindness, in Theorem 3.5. □

Theorem 3.4. *The two-message EB-RSP in Protocol 1 satisfies correctness.*

Proof. We will now describe carefully, step by step, the interaction between the classical verifier V and the quantum prover P as well as how the state of P evolves in the protocol. For simplicity, we drop normalization factors in quantum states.

- (Verifier 1st Message) Sample $x_0 \leftarrow X$ and $r, s \leftarrow G$. Compute $x_1 := (-s) \star x_0$, and send (x_0, x_1, r) to P.
- (Prover 1st Message) Prepare the state

$$|+\rangle \otimes \sum_{g \in G} |g\rangle = \sum_{b \in \{0,1\}, g \in G} |b, g\rangle .$$

Then apply the isometric mapping that lets g act on x_0 and x_1, respectively, controlled on the first register, to obtain the state

$$\sum_{b \in \{0,1\}, g \in G} |b, g, g \star x_b\rangle .$$

Measure the last register in the standard basis to obtain some $y \in X$, with the residual state being

$$|0, g_0\rangle + |1, g_0 + s\rangle ,$$

where $g_0 \star x_0 = y$, since the group action is free. Apply another isometric mapping that computes the inner product between r and the second register, to obtain the state

$$|0, g_0, \langle g_0, r\rangle\rangle + |1, g_0 + s, \langle g_0 + s, r\rangle\rangle = |0, g_0, z_0\rangle + |1, g_0 + s, z_1\rangle ,$$

where we define $z_0 := \langle g_0, r\rangle \in \mathbb{Z}_p$ and $z_1 := \langle g_0 + s, r\rangle \in \mathbb{Z}_p$. Note that $z_1 = z_0 + \langle s, r\rangle \mod p$. Now, apply the QFT over $\mathbb{Z}_p$ to the last register to obtain

$$\sum_{z \in \mathbb{Z}_p} (\chi(z, z_0) |0, g_0\rangle + \chi(z, z_1) |1, g_0 + s\rangle) |z\rangle ,$$

and measure the last register to obtain some $z \in \mathbb{Z}_p$, with the residual state being

$$\begin{aligned} &\chi(z, z_0) |0, g_0\rangle + \chi(z, z_1) |1, g_0 + s\rangle \\ &= |0, g_0\rangle + \chi(z, \langle s, r\rangle) |1, g_0 + s\rangle \\ &= |0, g_0\rangle + \omega_p^{z \cdot \langle s, r\rangle} |1, g_0 + s\rangle \\ &= |0, g_0\rangle + \omega_p^{\langle s, z \cdot r\rangle} |1, g_0 + s\rangle , \end{aligned}$$

where $z \cdot r$ means that each component of r is multiplied by z. Lastly, apply the QFT over G to the second register to obtain

$$\sum_{g \in G} (\chi(g, g_0) |0\rangle + \omega_p^{\langle s, z \cdot r\rangle} \chi(g, g_0 + s) |1\rangle) |g\rangle ,$$

and measure again the last register to obtain some $g \in G$, with the residual state being

$$\begin{aligned} &\chi(g, g_0) |0\rangle + \omega_p^{\langle s, z \cdot r\rangle} \chi(g, g_0 + s) |1\rangle \\ &= \chi(g, g_0) |0\rangle + \omega_p^{\langle s, z \cdot r\rangle} \chi(g, g_0) \chi(g, s) |1\rangle \\ &= |0\rangle + \omega_p^{\langle s, z \cdot r\rangle} \chi(g, s) |1\rangle \\ &= |0\rangle + \omega_p^{\langle s, z \cdot r\rangle + \langle g, s\rangle} |1\rangle \\ &= |0\rangle + \omega_p^{\langle s, z \cdot r + g\rangle} |1\rangle . \end{aligned}$$

Send (z, g) to V.

- (Verifier Output) Compute $k := \langle s, z \cdot r + g \rangle \in \mathbb{Z}_p$ and output $\theta = k \cdot \frac{2\pi}{p}$.

As a result, this shows that the protocol obviously terminates successfully with probability 1. Furthermore, upon successful completion, the honest prover P holds the state $|+_\theta\rangle$ for an angle $\theta \in \Theta_p$ known to the verifier. □

Theorem 3.5. *The two-message EB-RSP in Protocol 1 satisfies eavesdropper blindness.*

Proof. By the definition of eavesdropper blindness security, we have to show that the distribution of θ in Protocol 1 is computationally indistinguishable from the uniform distribution over Θ_N for $N = p$, from the eavesdropper's view. In other words, we have to show that $k := \langle s, z \cdot r + g \rangle \in \mathbb{Z}_p$ is computationally indistinguishable from the uniform distribution over $\mathbb{Z}_p$.

Note that during the quantum computation, g is sampled uniformly at random from G. Furthermore, g is independent of the measurement outcome z and V's randomness r. This implies that $z \cdot r + g$ is uniformly distributed over G.

As a result, we can now invoke the quantum version of the Goldreich-Levin theorem for large fields given in Theorem 2.6. More concretely, we instantiate it with $p = \mathsf{poly}(\lambda)$, $H = \mathbb{Z}_p$, and Φ computes $\star$ with respect to x_0. As a result, this shows that if the advantage ε of the eavesdropper to distinguish between $k := \langle s, z \cdot r + g \rangle$ and a uniform $u \in \mathbb{Z}_p$ would be non-negligible, then this would imply the existence of an efficient extractor for s, contradicting the one-wayness of the group action. Consequently, the advantage of the eavesdropper must be negligible, which concludes the security proof. □

Protocol Simplification. As also described in Section 1.1.1, the current protocol can be further simplified by removing r and the measurement outcome z from the construction altogether, which has the same effect as setting $r = 0$, i.e., the all-zero string. At a high-level, the completeness of the new protocol remains unchanged, as it holds for every value of r. On the other hand, for the eavesdropper blindness, observe that, for any fixed verifier randomness r and any outcome of the inner product register measurement, the Fourier outcome g is uniformly distributed over G. In particular, g is uniform and independent of the verifier's first message. And now one can use the Goldreich-Levin argument for $\langle s, g \rangle$ as before.

On Extending the Range of N. So far, we have shown how to construct such EB-RSPs for N being a prime p, which is poly-sized in the security parameter λ. We can, in fact, extend this to N of the form $N = p_1 \cdots p_m$, where the p_i are pairwise distinct poly-sized primes and m is also poly-sized in the security parameter. The idea of constructing such EB-RSPs for larger N is fairly simple: combine the above EB-RSP for different primes. More concretely, view the presented EB-RSP as a subroutine in which the verifier inputs p and the prover inputs a one-qubit state (in this case, it was $|+\rangle$). View the outcome of this subroutine as including a relative phase on the prover's input qubit, while the verifier obtains a classical description of this relative phase. The basic idea is now to run this in parallel for all primes p_i. Thus, if we want to construct this EB-RSP for $N = p_1 \cdots p_m$, the verifier simply sends the group action instances together with the randomness (x_0, x_1, r) for each p_i in parallel to the prover, while P performs the subroutine for each p_i sequentially on the same qubit. More precisely, the prover starts with the input $|+\rangle$ and follows the subroutine for p_1 to obtain the new one-qubit state $|+_{\theta_1}\rangle$ for $\theta_1 \in \Theta_{p_1}$. Next, the prover again follows the subroutine for p_2 by inputting this newly obtained one-qubit state and ends up with $\left|+_{(\theta_1+\theta_2)}\right\rangle$ for $\theta_2 \in \Theta_{p_2}$. This continues until the subroutine has been executed for all p_i. Note that in the end $\theta_1 + \ldots + \theta_m \in \Theta_N$

by simply extending the fractions. That this sum is computationally indistinguishable from uniform in Θ_N follows immediately from the independence of the subroutines, together with the previous security analysis showing that each $\theta_i \in \Theta_{p_i}$ is computationally indistinguishable from uniform, and, lastly, from the fact that all primes are distinct.

We note that how to extend this idea to powers of primes remains unclear. A naive approach, replacing the QFT over $\mathbb{Z}_p$ with the QFT over prime powers $\mathbb{Z}_{p^m}$, does not work, since correctness fails: the verifier V cannot recover θ because the phase depends on the term $z_1 - z_0$, and V must know its value modulo p^m. Writing $\delta := \langle s, r \rangle$, one has $z_1 - z_0 = \delta$ or $z_1 - z_0 = \delta - p$, depending on the unknown value of g_0. Although V can compute δ, it cannot determine which of the two cases holds, since this depends on g_0, about which V has no information. Consequently, V cannot compute $z_1 - z_0 \mod p^m$ in general. The case $m = 1$ is the exception, since both possibilities are congruent to δ modulo p.

On Extending to General Abelian One-Way Group Actions. Finally, we want to emphasize that it remains an open problem to construct such EB-RSPs from general abelian OWGAs. We construct them only for certain groups, since we rely on the Goldreich-Levin theorem for large fields. There are indeed generalizations of the Goldreich-Levin theorem to general abelian groups, but the authors are not familiar with the framework in which those theorems are stated. Thus, it may be plausible that more general Goldreich-Levin theorems could extend this construction to more general groups. Nevertheless, this work is still a step forward toward constructing RSP-type primitives without relying on trapdoor primitives, as we exploit the algebraic properties of the group action to compensate for the absence of a trapdoor. Another important aspect is that this EB-RSP has a useful application in QPKE, as we show in Section 4. It also remains open whether this type of EB-RSP has other useful applications.

4 Quantum Public-Key Encryption with Classical Public Keys

In this section, we present a new *quantum public-key encryption* (QPKE) construction with classical public keys and quantum ciphertexts that is IND-CPA secure. The protocol consists of a black-box construction from the previously defined two-message EB-RSP in Section 3 and can therefore ultimately be instantiated from the specific one-way group actions described in Section 3.2 or from plain TCFs.

There are many different types of QPKE, depending on whether the public keys and ciphertexts are classical or quantum [BGH+23, BMW23, HMY23, BK25]. As we said, we focus on the case where the public keys are classical and the ciphertexts are quantum, as this setting is still not well understood with respect to minimal cryptographic assumptions. In terms of near-future usability, this setting is also much more practical than having quantum public keys, since one would need to store an enormous number of quantum public keys, which would also be 'consumed' after each encryption, thereby creating a need to 'refill' them.

We also want to highlight that, since our EB-RSP includes a wide range of output states together with a relatively weak security definition, we can hope for relatively simple constructions from different cryptographic assumptions, thereby allowing the QPKE to be instantiated from a wider range of assumptions. As we have seen in Section 3.1, existing RSPs are likely naturally adaptable to the two-message EB-RSP notion and can therefore subsequently be used to construct QPKE schemes. This yields a QPKE construction from plain TCFs. To compare this result, in

some sense, with existing ones, the authors of [BK25] used a stronger notion of TCFs, namely *dual-mode TCFs*, to construct a QPKE, but with the advantage of having classical ciphertexts rather than quantum ones.

4.1 Definition

We start by providing a formal definition of QPKE with classical public keys and quantum ciphertexts. For this, we follow the definition in [HMY23, Definition 4.8].

As in their case, we will define this QPKE for classical one-bit messages for simplicity. The multi-bit message version can be defined analogously, and a simple parallel repetition suffices to expand the message length. Moreover, we can further extend the message space to *quantum states* via hybrid encryption by relying on the quantum one-time pad as in [BJ15]. That is, we encrypt a quantum message using a quantum one-time pad and then encrypt the key of the quantum one-time pad using our QPKE for classical messages.

Definition 4.1 (Quantum Public-Key Encryption)**.** *A* quantum public-key encryption (QPKE) *scheme (with single-bit messages) consists of the algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$*:*

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$*. This is a PPT algorithm that takes the security parameter* 1^λ *as input and outputs a classical public key* pk *and a classical secret key* sk*.*
- $\mathsf{Enc}(\mathsf{pk}, b) \to ct$*. This is a QPT algorithm that takes a public key* pk *and a message* $b \in \{0,1\}$ *as input and outputs a quantum ciphertext* ct*.*
- $\mathsf{Dec}(\mathsf{sk}, ct) \to b' / \perp$*. This is a QPT algorithm that takes a secret key* sk *and a ciphertext* ct *as input and outputs a message* $b' \in \{0,1\}$ *or* $\perp$*.*

We require the scheme to satisfy the following properties:

- (Correctness) *For any* $b \in \{0,1\}$*, we have*

$$\Pr\Big[b' = b : (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda), ct \leftarrow \mathsf{Enc}(\mathsf{pk}, b), b' \leftarrow \mathsf{Dec}(\mathsf{sk}, ct)\Big] = 1 - \mathsf{negl}(\lambda).$$

- (IND-CPA Security) *We say the QPKE scheme is* IND-CPA secure *if for any QPT adversary* $\mathcal{A}$*, we have*

$$|\Pr[b' = b : b' \leftarrow \mathcal{A}(\mathsf{pk}, ct_b)] - \frac{1}{2}| = \mathsf{negl}(\lambda),$$

where $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$*,* $b \leftarrow \{0,1\}$*, and* $ct_b \leftarrow \mathsf{Enc}(\mathsf{pk}, b)$*.*

Note that the security definition is given in *guess style*, where the game picks a random bit b and the adversary has to output a guess b' for the bit. Since it aligns more with our eavesdropper blindness security in Definition 3.1 that we want to reduce to, we use this formulation.

4.2 Black-Box Construction from Eavesdropper-Blind Remote State Preparation

We now present the QPKE scheme with classical public keys, built in a black-box fashion based on our two-message EB-RSP defined in Definition 3.1. Before going into the construction, we first prove a lemma that will later help us compute the probability for correctness.

Lemma 4.2. *For any $\theta_1, \theta_2 \in \mathbb{R}$, we have*

$$|\langle +_{\theta_2} | +_{\theta_1} \rangle|^2 = \tfrac{1}{2} + \tfrac{\cos(\theta_1 - \theta_2)}{2}.$$

Proof. We calculate:

$$\begin{aligned}\langle +_{\theta_2} | +_{\theta_1} \rangle &= \tfrac{1}{2}\Big(\langle 0| + e^{-i\theta_2} \langle 1|\Big)\Big(|0\rangle + e^{i\theta_1} |1\rangle\Big) \\ &= \tfrac{1}{2}\Big(1 + e^{i(\theta_1 - \theta_2)}\Big).\end{aligned}$$

Hence,

$$\begin{aligned}|\langle +_{\theta_2} | +_{\theta_1} \rangle|^2 &= \langle +_{\theta_2} | +_{\theta_1} \rangle \cdot \langle +_{\theta_1} | +_{\theta_2} \rangle \\ &= \tfrac{1}{4}\Big(1 + e^{i(\theta_1 - \theta_2)}\Big)\Big(1 + e^{i(\theta_2 - \theta_1)}\Big) \\ &= \tfrac{1}{4}\Big(1 + e^{i(\theta_2 - \theta_1)} + e^{i(\theta_1 - \theta_2)} + 1\Big) \\ &= \tfrac{1}{2} + \tfrac{\cos(\theta_1 - \theta_2)}{2}.\end{aligned}$$

□

The main result of this section is stated in the following theorem.

Theorem 4.3. *The existence of a two-message EB-RSP implies the existence of an IND-CPA secure QPKE scheme.*

QPKE Scheme. We first define

$$n = \begin{cases} 1, & \text{if } 2 \mid N, \\ 2\lambda + 1, & \text{if } 2 \nmid N. \end{cases}$$

The key generation, encryption, and decryption algorithms are given by:

- $\mathsf{KeyGen}(1^\lambda)$: Run $\mathsf{EB\text{-}RSP.Setup}(1^\lambda)$ exactly n times and output $\mathsf{pk} := (\mathsf{msg}_{V_1}, \ldots, \mathsf{msg}_{V_n})$ and $\mathsf{sk} := (\mathsf{st}_{V_1}, \ldots, \mathsf{st}_{V_n})$.
- $\mathsf{Enc}(\mathsf{pk}, b)$: Given a message bit $b \in \{0,1\}$, run $\mathsf{EB\text{-}RSP.QComp}(\mathsf{msg}_{V_i})$ for each i to obtain $(|+_{\theta_1}\rangle, \ldots, |+_{\theta_n}\rangle, \mathsf{msg}_{P_1}, \ldots, \mathsf{msg}_{P_n})$. Now apply $U := R_z(b \cdot \left\lfloor \frac{N}{2} \right\rfloor \cdot \frac{2\pi}{N})$ to all quantum states and output
$$ct := (U|+_{\theta_1}\rangle, \ldots, U|+_{\theta_n}\rangle, \mathsf{msg}_{P_1}, \ldots, \mathsf{msg}_{P_n}).$$
- $\mathsf{Dec}(\mathsf{sk}, ct)$: Recover the θ_i's by running $\mathsf{EB\text{-}RSP.Dec}(\mathsf{st}_{V_i}, \mathsf{msg}_{P_i})$ for each instance. Apply the unitary $U_i := R_z(-\theta_i)$ to the i-th qubit, which are now all in the state $U|+\rangle$. Measure all of them in the Hadamard basis, yielding outcomes 0 for $|+\rangle$ and 1 for $|-\rangle$. Finally, output the bit that appears most often using a majority vote.

Theorem 4.4. *The QPKE scheme as described above is correct.*

Proof. We perform a case distinction depending on the parity of N.

We start with the case where N is even. Note that in this case we have $\left\lfloor \frac{N}{2} \right\rfloor \cdot \frac{2\pi}{N} = \pi$. Hence $U = R_z(b\pi)$. Therefore the received qubit is in the state $\left|+_{(\theta_1 + b\pi)}\right\rangle$. In the decryption algorithm we remove θ_1, as $R_z(-\theta_1)$ is applied to the qubit. We are left with the state $|+_{b\pi}\rangle = H|b\rangle$. Measuring this in the Hadamard basis then yields b with probability 1.

Now consider the case where N is odd and the encrypted message was $b = 0$. In this case $U = I$ and all states in the decryption phase right before the measurement are in the $|+\rangle$ state, which all output 0 under a Hadamard measurement. By majority vote, 0 will be the output of the decryption. Hence the decryption again succeeds with probability 1.

Lastly, consider the case where N is odd and the encrypted message was $b = 1$. This case is the reason we included repetition within the encryption algorithm in order to boost the correctness probability. We observe that

$$b \cdot \left\lfloor \frac{N}{2} \right\rfloor \cdot \frac{2\pi}{N} = \pi - \frac{\pi}{N} =: \theta'.$$

Hence all qubits right before the Hadamard measurement are in the state $|+_{\theta'}\rangle$. We first compute the probability that one of the measurements yields the correct bit. Our measurement outcome must correspond to $|-\rangle$, since $b = 1$ was encrypted. The probability that we measure $|-\rangle$ is given by

$$\begin{aligned}
|\langle -|+_{\theta'}\rangle|^2 &= |\langle +_{\pi}|+_{\theta'}\rangle|^2 \\
&= \tfrac{1}{2} + \tfrac{\cos(\theta' - \pi)}{2} \\
&= \tfrac{1}{2} + \tfrac{\cos(\frac{\pi}{N})}{2} \\
&\geq \tfrac{1}{2} + \tfrac{\cos(\frac{\pi}{3})}{2} \\
&= 0.75,
\end{aligned}$$

where we used Lemma 4.2 for the second equality and lower-bounded the expression since N is odd and, without loss of generality, at least 3, and the cosine function is strictly monotonically decreasing on $[0, \frac{\pi}{2}]$. Since the probability that a single outcome is correct is at least 75%, a standard Chernoff bound argument implies that the probability that the majority vote decrypts correctly is $1 - \mathsf{negl}(\lambda)$. □

Theorem 4.5. *The QPKE scheme as described above is IND-CPA secure.*

Proof. We reduce the security of the QPKE scheme to the security of the EB-RSP. An adversary $\mathcal{A}$ against the QPKE security game receives the public key $\mathsf{pk} := (\mathsf{msg}_{V_1}, \ldots, \mathsf{msg}_{V_n})$ and the ciphertext ct_b, which encrypts a bit $b \in \{0, 1\}$. Instead of giving the adversary only the quantum states, we even provide $\mathcal{A}$ with the classical description of the quantum states given by

$$\theta_i + b \cdot \left\lfloor \frac{N}{2} \right\rfloor \cdot \frac{2\pi}{N} = \left(k_i + b \cdot \left\lfloor \frac{N}{2} \right\rfloor\right) \cdot \frac{2\pi}{N},$$

where $\theta_i = k_i \cdot \frac{2\pi}{N}$ with $k_i \in \mathbb{Z}_N$. This only increases the advantage of $\mathcal{A}$, and we show that it still remains negligible. Thus the adversary receives

$$\left(\mathsf{msg}_{V_i}, \mathsf{msg}_{P_i}, k_i + b \cdot \left\lfloor \frac{N}{2} \right\rfloor \mod N\right)_{1 \leq i \leq n}.$$

Note that the first two elements correspond exactly to the transcript of the two-message EB-RSP. Since the EB-RSP is eavesdropper-blind, we know that k_i is computationally indistinguishable from a uniform element of $\mathbb{Z}_N$. By a hybrid argument, the information above is computationally indistinguishable from

$$(\mathsf{msg}_{V_i}, \mathsf{msg}_{P_i}, u_i)_{1\leq i\leq n},$$

where $u_i \leftarrow \mathbb{Z}_N$, as all instances are independent of each other. Hence the information about b is completely hidden and the adversary has no non-negligible advantage. □

This concludes the proof that two-message EB-RSP implies IND-CPA secure QPKE with classical public keys. Combining this theorem with our construction of two-message EB-RSP from specific OWGAs yields the following corollary.

Corollary 4.6. *The existence of a free OWGA $\star : G \times X \to X$, where $G = \mathbb{Z}_p^\lambda$ for a prime p, which is poly-sized in the security parameter λ, implies the existence of an IND-CPA secure QPKE scheme.*

Proof. This follows immediately from Theorems 3.3 and 4.3. □

Furthermore, the relationship between two-message EB-RSP and IND-CPA secure QPKE yields additional constructions of QPKE from another well-studied assumption:

Corollary 4.7. *The existence of a plain TCF implies the existence of an IND-CPA secure QPKE scheme.*

Proof. This follows immediately from Theorems 3.2 and 4.3. □

On the Security of the EB-RSP for QPKE. Our EB-RSP security definition considers the full angle $\theta = k \cdot \frac{2\pi}{N}$ with $k \in \mathbb{Z}_N$ to be computationally indistinguishable from uniform. When N is a power of 2, this means that each individual bit of k should be computationally indistinguishable from uniform.

But note that for IND-CPA security, we only need the most significant bit of k to be computationally indistinguishable, since our encryption essentially flips the most significant bit of k within the quantum state when N is a power of 2. For general N, this translates to effectively hiding the single bit of information corresponding to whether $0 \leq k < \left\lfloor \frac{N}{2} \right\rfloor$ or $\left\lfloor \frac{N}{2} \right\rfloor \leq k < N$, that is, whether θ lies on the upper half or the lower half of the unit circle. Thus, requiring only that this information be hidden would be sufficient to ensure IND-CPA security. This is exactly equivalent to hiding the most significant bit of k when N is a power of 2. An interesting fact is that all other known RSPs do it the other way around: they try to hide all but the most significant bit (since it is impossible to hide everything while allowing the prover itself to be malicious).

Acknowledgments

The authors thank Tomoyuki Morimae for several helpful discussions at many different stages of the project and valuable feedback on drafts of this paper, the anonymous ASIACRYPT 2026 reviewers for their valuable comments and suggestions, and Giulio Malavolta for helpful discussions. The authors acknowledge support from the National Science Foundation grant CCF-1813814, from the AFOSR under Award Number FA9550-20-1-0108 and from the Quantum Advantage Pathfinder project.

References

[ACC+22] Per Austrin, Hao Chung, Kai-Min Chung, Shiuan Fu, Yao-Ting Lin, and Mohammad Mahmoody. On the impossibility of key agreements from quantum random oracles. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 165–194, Santa Barbara, CA, USA, August 15–18, 2022. Springer, Cham, Switzerland.

[ADMP20] Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis. Cryptographic group actions and applications. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 411–439, Daejeon, South Korea, December 7–11, 2020. Springer, Cham, Switzerland.

[AMMW22] Yusuf Alnawakhtha, Atul Mantri, Carl A. Miller, and Daochen Wang. Lattice-based quantum advantage from rotated measurements. Cryptology ePrint Archive, Report 2022/1497, 2022.

[APV23] Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. In Guy N. Rothblum and Hoeteck Wee, editors, *TCC 2023, Part IV*, volume 14372 of *LNCS*, pages 93–122, Taipei, Taiwan, November 29 – December 2, 2023. Springer, Cham, Switzerland.

[BBK22] Nir Bitansky, Zvika Brakerski, and Yael Tauman Kalai. Constructive post-quantum reductions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part III*, volume 13509 of *LNCS*, pages 654–683, Santa Barbara, CA, USA, August 15–18, 2022. Springer, Cham, Switzerland.

[BGH+23] Khashayar Barooti, Alex B. Grilo, Loïs Huguenin-Dumittan, Giulio Malavolta, Or Sattath, Quoc-Huy Vu, and Michael Walter. Public-key encryption with quantum keys. In Guy N. Rothblum and Hoeteck Wee, editors, *TCC 2023, Part IV*, volume 14372 of *LNCS*, pages 198–227, Taipei, Taiwan, November 29 – December 2, 2023. Springer, Cham, Switzerland.

[BJ15] Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 609–629, Santa Barbara, CA, USA, August 16–20, 2015. Springer Berlin Heidelberg, Germany.

[BK25] James Bartusek and Dakshita Khurana. On the power of oblivious state preparation. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part II*, volume 16001 of *LNCS*, pages 575–607, Santa Barbara, CA, USA, August 17–21, 2025. Springer, Cham, Switzerland.

[BKM+25] Kaniuar Bacho, Alexander Kulpe, Giulio Malavolta, Simon Schmidt, and Michael Walter. Compiled nonlocal games from any trapdoor claw-free function. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part II*, volume 16001 of *LNCS*, pages 642–673, Santa Barbara, CA, USA, August 17–21, 2025. Springer, Cham, Switzerland.

[BMW23] Khashayar Barooti, Giulio Malavolta, and Michael Walter. A simple construction of quantum public-key encryption from quantum-secure one-way functions. Cryptology ePrint Archive, Report 2023/306, 2023.

[BNZ25] John Bostanci, Barak Nehoran, and Mark Zhandry. A general quantum duality for representations of groups with applications to quantum money, lightning, and fire. In Michal Koucký and Nikhil Bansal, editors, *57th ACM STOC*, pages 201–212, Prague, Czechia, June 23–27, 2025. ACM Press.

[BY91] Gilles Brassard and Moti Yung. One-way group actions. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 94–107, Santa Barbara, CA, USA, August 11–15, 1991. Springer Berlin Heidelberg, Germany.

[CCKW19] Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. QFactory: Classically-instructed remote secret qubits preparation. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part I*, volume 11921 of *LNCS*, pages 615–645, Kobe, Japan, December 8–12, 2019. Springer, Cham, Switzerland.

[CCKW21] Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. On the possibility of classical client blind quantum computing. *Cryptography*, 5(1):3, January 2021.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427, Brisbane, Queensland, Australia, December 2–6, 2018. Springer, Cham, Switzerland.

[DGK+10] Yevgeniy Dodis, Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Public-key encryption schemes with auxiliary inputs. In Daniele Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 361–381, Zurich, Switzerland, February 9–11, 2010. Springer Berlin Heidelberg, Germany.

[GMP23] Alexandru Gheorghiu, Tony Metger, and Alexander Poremba. Quantum cryptography with classical communication: Parallel remote state preparation for copy-protection, verification, and more. In Kousha Etessami, Uriel Feige, and Gabriele Puppis, editors, *ICALP 2023*, volume 261 of *LIPIcs*, pages 67:1–67:17, Paderborn, Germany, July 10–14, 2023. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik.

[GV19] Alexandru Gheorghiu and Thomas Vidick. Computationally-secure and composable remote state preparation. In David Zuckerman, editor, *60th FOCS*, pages 1024–1033, Baltimore, MD, USA, November 9–12, 2019. IEEE Computer Society Press.

[GV24] Aparna Gupte and Vinod Vaikuntanathan. How to construct quantum FHE, generically. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part III*, volume 14922 of *LNCS*, pages 246–279, Santa Barbara, CA, USA, August 18–22, 2024. Springer, Cham, Switzerland.

[HMY23] Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. From the hardness of detecting superpositions to cryptography: Quantum public key encryption and commitments. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part I*, volume 14004 of *LNCS*, pages 639–667, Lyon, France, April 23–27, 2023. Springer, Cham, Switzerland.

[IR89] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *21st ACM STOC*, pages 44–61, Seattle, WA, USA, May 15–17, 1989. ACM Press.

[JD11] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011*, pages 19–34, Tapei, Taiwan, November 29 – December 2 2011. Springer Berlin Heidelberg, Germany.

[KMNY24] Fuyuki Kitagawa, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Quantum public-key encryption with tamper-resilient public keys from one-way functions. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part VII*, volume 14926 of *LNCS*, pages 93–125, Santa Barbara, CA, USA, August 18–22, 2024. Springer, Cham, Switzerland.

[MMR07] Gérard Maze, Chris Monico, and Joachim Rosenthal. Public key cryptography based on semigroup actions. *Advances in Mathematics of Communications*, 1(4):489–507, 2007.

[MS24] Hart Montgomery and Shahed Sharif. Quantum money from class group actions on elliptic curves. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part IX*, volume 15492 of *LNCS*, pages 33–64, Kolkata, India, December 9–13, 2024. Springer, Singapore, Singapore.

[MX24] Tomoyuki Morimae and Keita Xagawa. Quantum group actions. Cryptology ePrint Archive, Report 2024/1578, 2024.

[MZ25] Saachi Mutreja and Mark Zhandry. Quantum state group actions. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part II*, volume 16001 of *LNCS*, pages 449–480, Santa Barbara, CA, USA, August 17–21, 2025. Springer, Cham, Switzerland.

[Zha24] Mark Zhandry. Quantum money from abelian group actions. In Venkatesan Guruswami, editor, *ITCS 2024*, volume 287, pages 101:1–101:23, Berkeley, CA, USA, January 30 – February 2, 2024. LIPIcs.

[Zha25] Jiayu Zhang. Formulations and constructions of remote state preparation with verifiability, with applications. In Raghu Meka, editor, *ITCS 2025*, volume 325, pages 96:1–96:19, New York, NY, USA, January 7–10, 2025. LIPIcs.

A Eavesdropper-Blind Remote State Preparation from Trapdoor Claw-Free Functions

In this section, we provide a description of the RSP protocol presented in [BKM+25], which relies solely on the existence of a plain trapdoor claw-free function. As described in the paragraph before Theorem 3.2, this RSP can be modified to obtain a two-message EB-RSP from plain trapdoor claw-free functions.

Their RSP constructs states of the form

$$|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle),$$

where $\theta \in \Theta := \{k \cdot \pi/4 \mid k = 0, \ldots, 7\}$, and achieves the standard blind security notion against any malicious quantum prover. More precisely, they construct states of the form $Z^b|+_\theta\rangle = \left|+_{(\theta+b\pi)}\right\rangle$, while the security guarantee is provided only for θ.

We first recall the definition of a trapdoor claw-free function.

Definition A.1 (Trapdoor Claw-Free Function)**.** *Let λ be the security parameter. A* trapdoor claw-free function (TCF) *consists of a family of injective function pairs $(f_{0,\lambda}, f_{1,\lambda})$ and finite sets $\mathcal{X}_\lambda$ and $\mathcal{Y}_\lambda$ with*

$$\{f_{b,\lambda} : \mathcal{X}_\lambda \to \mathcal{Y}_\lambda\}_{(b,\lambda)\in\{0,1\}\times\mathbb{N}},$$

where we omit the subscript λ when it is clear from the context. Additionally, a TCF pair is augmented with two algorithms.

- $\mathsf{Gen}(1^\lambda)$*: On input the security parameter in unary 1^λ, the polynomial-time generation algorithm outputs a function pair (f_0, f_1) and a trapdoor* td*.*
- $\mathsf{Invert}(\mathsf{td}, y)$*: On input an image $y \in \mathcal{Y}$ and the trapdoor* td*, the polynomial-time deterministic inversion algorithm returns two preimages (x_0, x_1).*

We require a TCF to satisfy the following properties:

- (Correctness) *For all $\lambda \in \mathbb{N}$, all $x \in \mathcal{X}$, and all $b \in \{0,1\}$, it holds that:*

  $$f_0(x_0) = f_1(x_1) = y,$$

  where $((f_0, f_1), \mathsf{td}) \leftarrow \mathsf{Gen}(1^\lambda)$ and $(x_0, x_1) \leftarrow \mathsf{Invert}(\mathsf{td}, f_b(x))$.

- (Efficient Superposition) *There exists a QPT algorithm that, on input the description of the functions (f_0, f_1), prepares the state*

  $$\frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x\in\mathcal{X}} |x\rangle.$$

- (Claw-Freeness) *For all QPT algorithms A^* there exists a negligible function* negl *such that for all $\lambda \in \mathbb{N}$ it holds that:*

  $$\Pr[(x_0^*, x_1^*) \leftarrow A^*(f_0, f_1) : f_0(x_0^*) = f_1(x_1^*)] \leq \mathsf{negl}(\lambda).$$

  where $((f_0, f_1), \mathsf{td}) \leftarrow \mathsf{Gen}(1^\lambda)$.

We also assume that there exists an embedding of the set $\mathcal{X}$ into the bitstrings $\{0,1\}^{p(\lambda)}$ for some fixed polynomial p.

Next, we present their main RSP protocol, assuming the existence of any TCF $(\mathsf{Gen}, \mathsf{Invert})$. They start with describing a subroutine that the prover P and the verifier V will run in their main protocol.

Subroutine. The input and output of the protocol are:

- (Input) The protocol is parameterized by the security parameter in unary 1^λ, an integer n and the prover P holds a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- (Output) At the end of the interaction, the verifier holds a pair $(b, \theta) \in \{0,1\} \times \{0,1,2\}$ and the prover holds the state $\alpha|0\rangle + \beta(-1)^b \omega_n^\theta |1\rangle$.

The interaction between P and V proceeds as follows:

- (Verifier 1st Message) Sample $((f_0, f_1), \mathsf{td}) \leftarrow \mathsf{Gen}(1^\lambda)$ and send (f_0, f_1) to P.
- (Prover 1st Message) Prepare the state

$$|\psi\rangle \otimes \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x \in \mathcal{X}} |x\rangle = \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x \in \mathcal{X}} \alpha|0,x\rangle + \beta|1,x\rangle .$$

  Then, apply the isometric mapping that evaluates f_b coherently on input the second register, with the function controlled on the first register, to obtain the state

$$\frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x \in \mathcal{X}} \alpha|0,x,f_0(x)\rangle + \beta|1,x,f_1(x)\rangle .$$

  Measure the last register to obtain some $y \in \mathcal{Y}$, with the residual state being

$$\alpha|0,x_0\rangle + \beta|1,x_1\rangle$$

  where $f_0(x_0) = f_1(x_1) = y$. Send y to V.
- (Verifier 2nd Message) Check if $y \in \mathcal{Y}$ and abort if not. Sample two strings $r_0, r_1 \leftarrow\!\!\$\ \{0,1\}^{p(\lambda)}$ uniformly at random. Send (r_0, r_1) to P.
- (Prover 2nd Message) Consider the isometric mapping

$$M : (b, x_b) \mapsto (b, x_b, (-1)^{1-b}(x_b \cdot r_b))$$

  where the inner product $z_b := x_b \cdot r_b \in \{0,1\}$ is computed over $\mathbb{Z}_2$ and then parsed as an element of $\mathbb{Z}_n$. Apply M to the current state to compute

$$\alpha|0,x_0,-(x_0 \cdot r_0)\rangle + \beta|1,x_1,x_1 \cdot r_1\rangle = \alpha|0,x_0,-z_0\rangle + \beta|1,x_1,z_1\rangle .$$

  Apply QFT_n to the last register to obtain

$$\frac{1}{\sqrt{n}} \sum_{d' \in \mathbb{Z}_n} (\omega_n^{-d' \cdot z_0} \alpha|0,x_0\rangle + \omega_n^{d' \cdot z_1} \beta|1,x_1\rangle)|d'\rangle ,$$

where $-d' \cdot z_0, d' \cdot z_1 \in \mathbb{Z}_n$. Measure the last register in the computational basis and abort if the output $d' \neq 1$. The state becomes

$$\omega_n^{-z_0}\alpha\,|0, x_0\rangle + \omega_n^{z_1}\beta\,|1, x_1\rangle \equiv \alpha\,|0, x_0\rangle + \omega_n^{z_0+z_1}\beta\,|1, x_1\rangle\,.$$

Conditioning on not aborting, measure the second register in the Hadamard basis to obtain some $d \in \{0,1\}^{p(\lambda)}$, and return the state

$$\alpha\,|0\rangle + \beta(-1)^{d\cdot(x_0\oplus x_1)}\omega_n^{z_0+z_1}\,|1\rangle\,.$$

Send d to V.

- (Verifier Output) Recompute $(x_0, x_1) \leftarrow \mathsf{Invert}(\mathsf{td}, y)$ and set $b := d \cdot (x_0 \oplus x_1)$ and $\theta := z_0 + z_1 = x_0 \cdot r_0 + x_1 \cdot r_1 \in \{0, 1, 2\}$, where the sum is computed over $\mathbb{Z}$.

Main Protocol. The main protocol uses the above defined subroutine and proceeds in three steps.

- Run the above protocol with $n = 2$ and set $|+\rangle$ to be P's input state. Let (b_1, θ_1) be the output of V, and let $|\psi_1\rangle$ be the output of P.
- Run the above protocol with $n = 4$ and set $|\psi_1\rangle$ to be P's input state. Let (b_2, θ_2) be the output of V, and let $|\psi_2\rangle$ be the output of P.
- Run the above protocol with $n = 8$ and set $|\psi_2\rangle$ to be P's input state. Let (b_3, θ_3) be the output of V, and let $|\psi_3\rangle$ be the output of P.

The prover P returns the final state $|\psi_3\rangle$, whereas the verifier V sets

$$b := b_1 \oplus b_2 \oplus b_3 \text{ and } \theta := 4\theta_1 + 2\theta_2 + \theta_3 \mod 8$$

and must multiply θ by $\pi/4$ to obtain the angle.

For a full analysis of the correctness and security of their protocol, we refer the reader to their paper [BKM+25].