Post-Quantum Security: Bridging Quantum Mechanics and Cryptographic Proofs

Suprita TALNIKAR[1,2] Anandarup ROY[1,3] Kouichi SAKURAI[1]

Abstract: We examine key post-quantum proof techniques, emphasising their theoretical foundations and security implications. In particular, we explore the O2H lemma in the Quantum Random Oracle Model (QROM), adaptive reprogramming methods by GHHM and Unruh, and oracle-based abstractions like Quantum OneWay Puzzles (OWPuzz) and Quantum Advantage Samplers (QAS). Techniques such as Quantum One-Time Memories (OTMs), Measure-and-Reprogram 2.0, and the Arbitrary Reprogramming Lemma are also analysed. A discussion on finding relationships between these various proof techniques follows, concluding with a mathematical proof of some of these relations.

Keywords: Quantum Memories, Post-Quantum Proof Techniques, QROM

1. Introduction

The advent of large-scale quantum computers poses a profound and existential threat to the cryptographic foundations underpinning modern digital security. While the primary focus often rests on the vulnerability of classical public-key cryptography to Shor's algorithm for factoring integers and computing discrete logarithms [1], the implications extend significantly to symmetric key cryptography. Grover's algorithm, for instance, offers a quadratic speed-up to brute-force attacks on symmetric ciphers, effectively halving their security strength [2]. This necessitates a re-evaluation of current security margins and parameter choices for symmetric primitives. For example, a symmetric key scheme designed to offer 128-bit classical security would, under a quantum attack utilising Grover's algorithm, effectively provide only 64-bit security. This subtle yet critical distinction underscores the urgent requirement for cryptographic schemes that demonstrably resist both classical and quantum adversaries. The development of robust post-quantum proof techniques is therefore not merely an academic pursuit but a foundational requirement for establishing trust in future cryptographic systems [3].

1.1 Significance of Provable Security in the Quantum Era

Provable security, a cornerstone of modern cryptography, involves reducing the security of a cryptographic scheme to the assumed hardness of a well-known computational problem. This paradigm is even more critical in the quantum realm, where classical security intuitions can be profoundly misleading. The capabilities of quantum adversaries, such as querying cryptographic functions in superposition, entangling their internal states with an oracle, and performing measurements that collapse quantum states, introduce complexities that classical proof techniques cannot adequately capture. The very definition of security and the methodologies for proving it must be re-imagined to incorporate the principles of quantum mechanics. This represents a fundamental shift in the adversarial model, moving beyond an incremental update to a complete paradigm change. Consequently, the development of new, quantum-specific proof techniques is not just an academic exercise but a foundational requirement for building confidence and trust in post-quantum systems [3].

1.2 Overview of Scope and Structure

In this paper, we systematically analyse the landscape of post-quantum symmetric key cryptographic provable security proof techniques. The discussion commences with the foundational Quantum Random Oracle Model (QROM) and its pivotal One-Way to Hiding (O2H) Lemma. Subsequently, we delve into advanced quantum reprogramming methods, including those by GHHM and Unruh, Measure-and-Reprogram 2.0, and the Arbitrary Reprogramming Lemma. A dedicated section explores various quantum cryptographic elements and oracle-based abstractions, such as Quantum One-Way Puzzles (OWPuzz), Quantum Advantage Samplers (QAS), and Quantum One-Time Memories (OTMs), alongside fundamental quantum mechanical principles. We then elucidate integration methodologies, including semi-

[1] Department of Advanced Informatics, Kyushu University, Fukuoka, Japan
[2] Applied Statistics Unit, Indian Statistical Institute, Kolkata, India
[3] Dr. ROY is supported by the National Institute of Information and Communications Technology(NICT), Japan, under the NICT International Invitational Program.

direct programming and Fourier analysis, demonstrating how these quantum elements can be incorporated into security proofs. Finally, we draw explicit relations and identify common underlying principles among these diverse techniques, concluding with a discussion on open challenges and future research directions.

2. Foundations of Provable Security in the Quantum Random Oracle Model (QROM)

2.1 Introduction to the Quantum Random Oracle Model (QROM)

The Random Oracle Model (ROM) serves as an idealised abstraction for hash functions in classical cryptography, positing the hash function as a truly random, publicly accessible oracle. The Quantum Random Oracle Model (QROM) extends this idealisation to the quantum domain, modelling the oracle as a quantum black box capable of accepting quantum superpositions of inputs and returning superpositions of outputs [3]. In the classical ROM, an adversary queries $H(x)$ to obtain y. In contrast, a quantum adversary in the QROM can query a superposition state, such as $\sum_x \alpha_x|x\rangle$, and receive a superposition of outputs, $\sum_x \alpha_x|x, H(x)\rangle$. This capability fundamentally alters how an oracle can be interacted with and, consequently, how its ideal properties can be leveraged in a security proof. The ability of a single quantum query to simulate many classical queries simultaneously invalidates numerous classical ROM proofs that rely on counting distinct queries or assuming sequential, non-adaptive interactions. The QROM was thus developed as a direct response to these limitations, providing a necessary framework to capture the quantum advantage inherent in such queries, particularly for symmetric key primitives like hash functions and block ciphers. This represents a fundamental shift in the adversarial model, demanding new approaches to provable security.

2.2 Detailed Exposition of the One-Way to Hiding (O2H) Lemma and its Variants

The One-Way to Hiding (O2H) Lemma is a foundational tool for proving security in the QROM, particularly for constructions involving hash functions and pseudo-random functions (PRFs) [3]. Formally, the O2H Lemma states that if a quantum adversary can distinguish a quantum random oracle from a truly random function with a non-negligible advantage, then one can efficiently extract information about the oracle's internal state or a pre-image of a specific output. This principle provides a quantum analogue to classical "one-wayness," linking the ability to distinguish an oracle to the ability to extract hidden information.

The significance of O2H lies in its capacity to formalise the concept of "quantum indistinguishability" in the context of random oracles. It often serves as a crucial initial step or a sub-lemma within more complex QROM proofs, particularly those involving adaptive adversaries or scenarios where some "secret" information needs to be extracted from the adversary's interactions. Its simplicity belies its power as a primitive for quantum security reductions. For instance, while a classical adversary's query x directly reveals x, a quantum adversary's superposition query $\sum_x \alpha_x|x\rangle$ does not immediately reveal which x the adversary is "interested" in without measurement. The O2H Lemma provides a mechanism to argue that if an adversary gains a significant advantage in distinguishing, then some classical information can indeed be extracted from their quantum interaction. This extraction capability is then leveraged in reductions to break an underlying hard problem. Key variants and improvements, such as the "Fixed Permutation O2H" [4], have been developed to apply this lemma to specific cryptographic primitives, such as permutation-based constructions common in symmetric key cryptography. The proof structure of O2H typically involves a hybrid argument coupled with a carefully designed quantum measurement strategy to facilitate this information extraction [3].

3. Advanced Quantum Reprogramming Techniques

3.1 Adaptive Reprogramming Methods (GHHM and Unruh)

Reprogramming is a well-established technique in the classical Random Oracle Model, where the oracle's behaviour is altered during a security reduction to simulate different scenarios or to extract information from an adversary. However, the advent of quantum adversaries, whose subsequent queries can depend on prior quantum measurement outcomes, poses significant challenges to classical reprogramming techniques. The inherent adaptivity of quantum adversaries, where their quantum queries and measurements can influence their subsequent actions, directly necessitated the development of advanced reprogramming methods. Classical reprogramming often assumes non-adaptive or limited adaptive queries, which is insufficient for quantum settings.

Grilo, Hövelmanns, Hülsing, and Majenz (GHHM) [5], building upon the foundational work by Dominique Unruh [6], have made significant contributions to developing methods for handling such adaptive adversaries in the QROM [3]. Their techniques often involve sophisticated strategies for "rewinding" the adversary's quantum state or meticulously managing the oracle's state to maintain consistency throughout the simulation. Unlike classical rewinding, where an adversary's state can be simply reset, quantum rewinding is complicated by the no-cloning theorem and the collapse of superposition upon measurement. GHHM and Unruh's work provides ingenious solutions to these issues, often by carefully controlling the oracle's state or employing techniques that simulate rewinding without actually "rewinding" the adversary's quantum state in a problematic manner. This progression from classical reprogramming to adaptive quantum reprogramming reflects the increasing sophistication of quantum adversarial models and demonstrates a clear trend towards more robust and realis-

tic security analyses. Pan and Zeng have also contributed to this area, further refining adaptive reprogramming in the QROM [7]. This evolution is critical for proving the security of schemes where adversaries can learn and adapt their attacks based on quantum interactions.

3.1.1 Memory-Tight Security in the QROM

Xagawa [8] introduces the notion of *memory-tight security* within the Quantum Random Oracle Model (QROM), addressing adversaries constrained by quantum memory. This refinement is particularly relevant for signature schemes, where adversaries may exploit quantum memory to parallelise oracle queries or simulate rewinding. The techniques proposed offer a pathway to more realistic post-quantum security proofs, especially when modelling adversaries with bounded quantum storage.

3.2 Measure-and-Reprogram 2.0

Measure-and-Reprogram 2.0 [9] represents a significant advancement in quantum reprogramming techniques, specifically designed to achieve "tight" quantum rewinding. In the context of security reductions, "tightness" refers to the minimisation of security loss when translating an attack on a cryptographic scheme to an attack on the underlying hard problem. Earlier quantum security reductions frequently suffered from substantial security loss factors, meaning that if an adversary could break a scheme with probability p, the reduction might only demonstrate that the underlying hard problem could be broken with a probability of p/N, where N is a large factor related to the number of queries. Such loose reductions can lead to impractically large key sizes or parameters for post-quantum schemes, rendering them unusable in real-world applications.

Measure-and-Reprogram 2.0 specifically addresses this issue by reducing this loss, thereby making the reduction "tight." This is achieved through a meticulous control over the quantum state of the oracle and the adversary's interaction. The technique involves performing measurements at opportune times and reprogramming the oracle's behaviour based on the outcomes of these measurements, all while preserving the adversary's advantage. This methodological refinement is a critical step towards practical post-quantum cryptography, enabling more efficient parameter choices and bridging the gap between theoretical security proofs and deployable cryptographic systems [3].

3.2.1 Quantum Attacks on the Even-Mansour Cipher

Alagic et al. [10] revisit the Even-Mansour cipher under quantum adversarial models, demonstrating vulnerabilities to superposition attacks. Their generalised reprogramming lemma provides a robust framework for analysing symmetric constructions in the QROM. This work is foundational for extending oracle programmability and adaptive reprogramming techniques in post-quantum proofs, especially for symmetric primitives.

3.3 The Arbitrary Reprogramming Lemma

The Arbitrary Reprogramming Lemma [11] signifies a further maturation of the field, offering a generalisation of existing reprogramming techniques. This lemma aims to provide a unified framework for various reprogramming scenarios, moving towards more abstract and general principles for quantum security proofs rather than relying on ad-hoc techniques tailored for specific situations. As the number of quantum reprogramming techniques expanded, researchers sought a more encompassing framework. The Arbitrary Reprogramming Lemma provides such a framework, specifying general conditions under which an oracle can be reprogrammed, irrespective of the particular cryptographic primitive or attack scenario. This is akin to developing a "master theorem" for reprogramming, which can simplify and streamline future QROM proofs by providing a powerful, ready-to-use tool. Its application, for instance, to quantum attacks on Even-Mansour constructions [11], demonstrates its practical utility and potential for abstracting common reprogramming patterns, thereby enhancing the efficiency and clarity of security analyses [3].

3.3.1 Security of CRYSTALS-Dilithium in the QROM

Jackson et al. [12] analyse the security of CRYSTALS-Dilithium under quantum adversaries using the QROM. Their adaptation of the Measure-and-Reprogram technique reveals subtle vulnerabilities in the Fiat-Shamir transformation applied to lattice-based schemes. This case study underscores the importance of tight reductions and careful oracle modelling in post-quantum signature schemes, and validates the relevance of QROM-based analysis for standardised primitives.

3.4 Comparative Analysis of Reprogramming Techniques

The evolution of quantum reprogramming techniques, from Unruh's initial work [6] to GHHM's contributions [5], then to tight reductions like Measure-and-Reprogram 2.0 [9], and finally to the general Arbitrary Reprogramming Lemma [11], illustrates a clear trajectory. Early methods focused on establishing the feasibility of quantum reprogramming, demonstrating that such complex operations were possible despite the inherent challenges of quantum mechanics. Subsequent developments prioritised tightness, aiming to minimise the security loss in reductions to yield more practical cryptographic parameters. The most recent advancements, exemplified by the Arbitrary Reprogramming Lemma, have focused on generality and abstraction, seeking unified frameworks that can encompass and simplify diverse reprogramming scenarios. This progression indicates a field that is rapidly maturing, moving from demonstrating "can we prove it?" to "can we prove it tightly and generally?" Each technique addresses specific challenges: Unruh and GHHM provide the foundational methods for handling adaptive adversaries, Measure-and-Reprogram 2.0 refines this for tighter bounds, and the Arbitrary Reprogramming Lemma offers

a meta-approach for broader applicability. This continuous refinement is essential for building robust and efficient post-quantum cryptographic schemes.

4. Quantum Cryptographic Elements and Oracle-Based Abstractions

4.1 Quantum One-Way Puzzles (OWPuzz)

Quantum One-Way Puzzles (OWPuzz) are conceptualised as a quantum analogue of classical one-way functions. In this context, the "puzzle" involves quantum states or operations, where it is computationally easy to generate a puzzle and its solution, but computationally hard to find the solution given only the puzzle, even for a quantum computer. The study of OWPuzz implies that new forms of computational difficulty, inherently arising from quantum mechanics, could underpin future cryptographic security. Their proposed role is significant either as a potential foundation for quantum-secure primitives or as a hardness assumption within security proofs [13]. The exploration of OWPuzz highlights active research into fundamental quantum hardness assumptions, which are crucial for constructing new cryptographic primitives or rigorously proving the security of existing ones against quantum adversaries.

4.2 Quantum Advantage Samplers (QAS)

Quantum Advantage Samplers (QAS) formalise the notion that a quantum computer can efficiently sample from a distribution that a classical computer cannot, thereby providing a quantifiable computational advantage. This concept is directly relevant to defining quantum-specific computational assumptions and has potential applications in constructing quantum-secure primitives or demonstrating quantum supremacy. The existence of QAS suggests that certain cryptographic tasks might inherently be easier for quantum computers, leading to new security models where quantum adversaries possess a distinct and measurable advantage [14]. This is a more nuanced concept than simply "breaking" a classical problem; it pertains to leveraging a unique quantum computational capability as a basis for cryptographic security or as a measure of adversarial power.

4.3 Quantum One-Time Memories (OTMs)

Quantum One-Time Memories (OTMs) represent a fascinating quantum primitive that leverages fundamental quantum mechanical principles, such as the no-cloning theorem, to achieve functionalities impossible in classical cryptography. An OTM allows information to be written once and read once, with the quantum properties preventing multiple reads or copies of the stored quantum state. This exemplifies how quantum mechanics can be directly exploited to create novel cryptographic functionalities beyond merely resisting quantum attacks. OTMs hold theoretical significance and potential applications in secure hardware, uncloneable tokens, or as building blocks for other quantum primitives [15]. While not a proof technique in itself, OTMs represent a class of quantum resources whose unique properties may need to be considered in future security proofs, either as underlying assumptions or as components within a larger cryptographic system.

Stambler [16] constructs quantum one-time memories (QOTMs) using stateless hardware and random access codes, framed within a nonconvex optimisation paradigm. This work bridges physical assumptions with cryptographic abstractions, enabling QOTMs without trusted setup. These primitives are instrumental in secure computation and commitment schemes, and their abstraction aligns with the survey's exploration of quantum memory models and minimal hardware assumptions.

4.3.1 Quantum Proofs of Knowledge

Unruh [17] formalises quantum proofs of knowledge (QPoK), extending classical definitions to quantum settings. His quantum rewinding technique preserves soundness and zero-knowledge under superposition attacks. This foundational work underpins modern QROM techniques such as Measure-and-Reprogram and adaptive reprogramming, and is essential for constructing sound post-quantum zero-knowledge protocols.

4.4 Other Relevant Quantum Cryptographic Elements

Beyond specific abstractions like OWPuzz, QAS, and OTMs, the fundamental building blocks of quantum mechanics themselves constitute critical quantum cryptographic elements. These include:

- **Quantum States:** Superposition and entanglement are fundamental properties defining the quantum computational model and adversarial capabilities [18]. Adversaries can leverage superposition to query a cryptographic function on many inputs simultaneously, effectively exploring a vast input space in a single operation. Entanglement allows for correlations between different parts of a quantum system, which can be exploited to gain information or coordinate attacks.
- **Quantum Measurements:** The probabilistic and state-collapsing nature of quantum measurements profoundly impacts security proofs [18]. While measurements yield classical outcomes, they destroy the underlying superposition, which must be carefully accounted for in proofs, particularly in rewinding arguments. Measurements can be used to extract information, but their irreversible nature also imposes limitations on an adversary.
- **Quantum Algorithms:** Algorithms such as Shor's [1] and Grover's [2] are not merely threats to classical cryptography but also serve as concrete examples of quantum capabilities that define the power of the quantum adversary model against which proofs must hold. They establish the computational limits for quantum adversaries in specific problem domains.
- **Quantum Oracles:** While the QROM is a specific

Table 1: Key Post-Quantum Proof Techniques Overview

Technique Name	Core Concept	Primary Application	Key Advantage(s)	Key Reference(s)
One-Way to Hiding (O2H) Lemma	Links distinguishing an oracle to extracting hidden information from quantum queries.	Hash functions, PRFs, foundational QROM reductions.	Foundational, enables information extraction from quantum adversaries.	[3], [4]
Adaptive Reprogramming (Unruh)	Enables oracle reprogramming against adaptive quantum adversaries by managing oracle state consistency.	General QROM proofs for schemes with adaptive queries.	Handles adaptivity, laid groundwork for quantum reprogramming.	[6]
Adaptive Reprogramming (GHHM)	Extends Unruh's work, providing more general methods for adaptive oracle reprogramming in QROM.	General QROM proofs, particularly for hash-based schemes.	Improved generality for adaptive adversaries.	[5], [7]
Measure-and-Reprogram 2.0	Achieves "tight" quantum rewinding by careful measurement and reprogramming, minimising security loss.	Symmetric key schemes requiring tight security bounds.	Achieves tighter reductions, leading to more practical parameters.	[9]
Arbitrary Reprogramming Lemma	Generalises various reprogramming techniques, providing a unified framework for diverse scenarios.	Simplifying and streamlining future QROM proofs, general attacks.	High generality, abstracts common reprogramming patterns.	[11]

type of quantum oracle, more general quantum oracles might represent specific functionalities or attack models. These oracles define the interface through which an adversary interacts with a cryptographic primitive in a quantum setting.

These fundamental quantum elements are not merely theoretical curiosities; they form the very fabric of the quantum adversarial model. Any robust post-quantum security proof must implicitly or explicitly account for how an adversary can manipulate and exploit these properties. Understanding these "atoms" of quantum computation is essential for defining the adversary's power and, consequently, for shaping the landscape of provable security.

5. Integration Methodologies: Bridging Quantum Elements and Proof Techniques

5.1 General Principles for Incorporating Quantum Elements into Security Proofs

Adapting classical proof techniques to the quantum setting necessitates a set of overarching strategies that account for the unique properties of quantum mechanics. The core challenge lies in the fact that classical proof techniques often rely on assumptions that are invalid in the quantum realm, such as the ability to copy a state or the deterministic nature of interactions. Therefore, new principles are required. Foremost among these is the need to accurately model quantum adversaries, typically as quantum circuits or oracles, capable of performing superposition queries, entanglement, and measurements. This leads to the concept of quantum indistinguishability, which extends the classical notion of indistinguishability to quantum states and operations. Security proofs must demonstrate that an adversary cannot distinguish between an ideal and a real cryptographic system, even with quantum queries. Furthermore, quantum reductions must be designed to map quantum attacks on a scheme to quantum-hard problems. The complexities of "rewinding" quantum adversaries, due to the no-cloning theorem and measurement-induced state collapse, represent a significant hurdle, requiring sophisticated techniques to circumvent or manage these limitations. These integration methodologies represent the mathematical and conceptual tools required to translate the abstract principles of quantum mechanics into concrete, rigorous cryptographic security proofs.

5.2 Application of Semi-Direct Programming in Post-Quantum Proofs

Semi-direct programming, conceptually adapted from the mathematical notion of a semi-direct product in group theory or algebra, offers a structured approach for manipulating quantum oracles within security proofs. This methodology involves constructing a composite system or operation where one part acts on another in a structured manner, thereby enabling controlled simulation or reprogramming. It provides

Table 2: Quantum Elements and Their Role in Provable Security

Quantum Element	Description/Definition	Role in Provable Security	Key Reference(s)
Quantum Random Oracle (QROM)	An idealised quantum black box responding to superposition queries.	Security Model for proofs against quantum adversaries.	[3]
Quantum One-Way Puzzle (OWPuzz)	Quantum analogue of one-way functions, hard to invert even for quantum computers.	Potential Hardness Assumption for quantum-secure primitives.	[13]
Quantum Advantage Sampler (QAS)	A distribution from which a quantum computer can sample efficiently, but a classical computer cannot.	Basis for quantum-specific Computational Assumptions, demonstrating quantum advantage.	[14]
Quantum One-Time Memory (OTM)	A quantum memory that can be written once and read once, uncloneable due to quantum mechanics.	Novel Cryptographic Primitive leveraging quantum properties.	[15]
Quantum Superposition	A quantum state existing in multiple states simultaneously.	Fundamental Adversary Capability, enabling parallel queries.	[18]
Quantum Entanglement	A strong correlation between quantum particles, regardless of distance.	Fundamental Adversary Capability, enabling correlated attacks.	[18]
Quantum Measurement	The process of extracting classical information from a quantum state, causing state collapse.	Fundamental Property influencing proof strategies and information extraction.	[18]
Quantum Algorithms (e.g., Shor's, Grover's)	Algorithms demonstrating quantum computational power for specific problems.	Defines the power of the Quantum Adversary Model.	[1], [2]

a structured algebraic framework for precisely controlling the oracle's behaviour, which is essential for simulating different attack scenarios or extracting information from an adversary. For instance, one might define a "hybrid" oracle as a semi-direct product of the original oracle and a "reprogramming" operation, allowing for a rigorous analysis of how the adversary's view changes across different hybrids, a fundamental aspect of many security reductions.

Theorem 1 Consider a quantum oracle O_f for a function f, implemented as a unitary transformation U_f mapping $|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$. Suppose one needs to reprogram f to f' for a specific input x_0, while maintaining the oracle's behaviour for all other inputs. Semi-direct programming can involve constructing a new oracle $O_{f'}$ that behaves like O_f for inputs $x \neq x_0$ but yields $f'(x_0)$ for x_0. This can be achieved by applying a correction unitary U_{corr} only for the input x_0, such that $U_{corr}(|x_0\rangle|y\rangle) = |x_0\rangle|y \oplus f(x_0) \oplus f'(x_0)\rangle$. The challenge lies in ensuring this correction is undetectable by the adversary or consistent with the overall simulation. This technique is particularly useful when the oracle's behaviour needs subtle alteration for a few specific inputs without affecting the adversary's overall view, often employed in proofs for quantum-resistant hash functions or pseudo-random functions.

5.3 Application of Fourier Analysis in Post-Quantum Proofs

Fourier analysis, particularly the Quantum Fourier Transform (QFT), plays an indispensable role in quantum algorithms and their application to cryptographic proofs. The QFT is central to many quantum algorithms that pose a threat to classical cryptography, such as Shor's algorithm. Consequently, its inverse and properties are also crucial for analysing quantum systems within security proofs. Fourier analysis can be used to analyse properties of quantum states, bound probabilities, or demonstrate equivalences between different quantum distributions. It allows for the transformation of information between different bases (e.g., computational basis to Fourier basis), which can reveal hidden periodicities or correlations in quantum states. Its application in proofs signifies that the mathematical tools used to break classical cryptography are now essential for proving the security of post-quantum schemes.

Theorem 2 (Illustrative Example of Fourier Analysis in Pr Consider a proof requiring a demonstration that a quantum adversary cannot distinguish between two quantum

states, $|\psi_0\rangle$ and $|\psi_1\rangle$. If these states exhibit a relationship involving a phase shift or a periodic property, Fourier analysis can be instrumental. For instance, if the states are of the form $|\psi_k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} |j\rangle$ (a QFT basis state), distinguishing between $|\psi_k\rangle$ and $|\psi_{k'}\rangle$ might involve performing a QFT on the states and then measuring in the computational basis. Fourier analysis enables precise calculations of overlap and distinguishability in such scenarios. It is frequently employed in proofs related to quantum query complexity, period finding problems, or when analysing the properties of quantum functions in superposition. In a security proof, this can be used to show that an adversary's quantum queries, when transformed into the Fourier domain, do not reveal sufficient information to break the scheme, or conversely, that a successful attack implies a computationally hard Fourier analysis.

5.4 Other Relevant Methodologies

Beyond the specific applications of semi-direct programming and Fourier analysis, several other methodologies are crucial for bridging quantum elements and proof techniques:

- **Quantum Rewinding:** This is a general concept in quantum proofs, analogous to classical rewinding, but it faces significant challenges due to the no-cloning theorem and the collapse of quantum states upon measurement. Techniques like Measure-and-Reprogram 2.0 [9] are specifically designed to address these challenges, enabling effective rewinding in the quantum setting.

- **Hybrid Arguments in Quantum Settings:** The classical hybrid argument, which interpolates between an ideal system and a real system through a sequence of intermediate "hybrid" systems, is adapted for quantum states and operations. This adaptation requires careful management of quantum coherence and entanglement throughout the sequence of hybrids to ensure the validity of the reduction.

- **Mirror Theory Bounds:** Mirror Theory [19] represents a newer approach for deriving bounds in algebraic cryptanalysis. While its direct implications for quantum settings are still being explored, it offers an alternative mathematical lens focusing on algebraic properties, which could potentially complement or even replace existing QROM-based approaches for certain schemes.

The continuous development of new methodologies, including Mirror Theory, indicates that the field of quantum provable security is actively seeking more powerful and general mathematical tools to tackle the complexities of quantum interactions. This diversity of approaches underscores the ongoing quest for the most effective and rigorous proof techniques.

6. Interconnections and Relationships Among Proof Techniques

6.1 Hierarchical Dependencies and Building Blocks

The various post-quantum proof techniques are not isolated but form a sophisticated toolkit with clear hierarchical dependencies. The One-Way to Hiding (O2H) Lemma [3] often serves as a fundamental building block or a prerequisite for more complex adaptive reprogramming techniques. For instance, an adaptive reprogramming proof might rely on O2H to argue about the extractability of information from an adversary's queries. O2H provides a baseline for quantum indistinguishability that reprogramming techniques then strive to maintain. If an adversary gains a significant advantage in distinguishing a reprogrammed oracle, an O2H-like argument can often be invoked to extract information, thereby leading to a contradiction or a break of an underlying hard problem.

Furthermore, the generality of the Arbitrary Reprogramming Lemma [11] aims to encompass and abstract common patterns found in earlier adaptive reprogramming methods, such as those developed by GHHM [5] and Unruh [6]. The Arbitrary Reprogramming Lemma is a meta-technique, generalising the specific methods employed by its predecessors, providing a more abstract and reusable framework. This progression illustrates a clear evolutionary path in quantum provable security, where simpler techniques provide foundational lemmas upon which more complex, adaptive, and tighter methods are constructed.

6.2 Relationship Between Proof Techniques and Quantum Elements/Abstractions

A symbiotic relationship exists between quantum cryptographic elements and the proof techniques employed to establish security. Quantum elements such as Quantum One-Way Puzzles (OWPuzz) [13], Quantum Advantage Samplers (QAS) [14], and Quantum One-Time Memories (OTMs) [15] often serve as the hard problems or idealised primitives to which the security of a post-quantum scheme is reduced. These elements represent either new hardness assumptions or novel primitives that are inherently quantum.

The proof techniques, such as adaptive reprogramming in the QROM, are the methodologies used to perform these reductions. They demonstrate that if a cryptographic scheme is broken by a quantum adversary, then that adversary's capabilities can be leveraged to solve an OWPuzz, construct a QAS, or violate the ideal properties of an OTM. For example, a security proof for a post-quantum symmetric key scheme might employ adaptive reprogramming in the QROM to show that an adversary successfully breaking the scheme implies they can solve a quantum one-way puzzle. In essence, the quantum elements define the security goal (the "what"), while the proof techniques provide the means to achieve these reductions (the "how"). The QROM itself

functions as a fundamental quantum element, serving as the model within which these proofs operate [3].

6.3 Common Underlying Principles

Despite their diversity, all these post-quantum proof techniques converge on a set of fundamental quantum mechanical and mathematical principles. This convergence suggests a robust and internally consistent theoretical framework for post-quantum provable security. Key common principles include:

- **Quantum Indistinguishability:** This is the core objective across all techniques. Adversaries should not be able to distinguish between an ideal cryptographic system (e.g., a truly random oracle) and a real implementation, even when making quantum queries. This principle underpins the O2H Lemma and is maintained throughout various reprogramming strategies.

- **Quantum Query Complexity:** Analysing the number and type of quantum queries required for an adversary to succeed is crucial for quantifying the adversary's power and deriving security bounds. Proofs meticulously account for the efficiency of quantum queries.

- **Superposition and Entanglement Management:** Proofs must carefully account for and manage these fundamental quantum phenomena. Adversaries exploit superposition to query multiple inputs simultaneously and entanglement to correlate different parts of their attack. The proof techniques must demonstrate how these properties are either controlled, limited, or leveraged in the reduction.

- **Hybrid Arguments:** The adaptation of classical hybrid arguments to quantum settings is a pervasive technique. This involves constructing a sequence of intermediate quantum systems (hybrids) that bridge the gap between an ideal and a real system, with each step being indistinguishable from the previous one. This often requires careful consideration of quantum state evolution and coherence.

7. Conclusion and Future Directions

This paper outlines the central role of the Quantum Random Oracle Model (QROM) in post-quantum provable security, tracing the refinement of proof techniques from the O2H Lemma to advanced reprogramming strategies. It highlighted the emergence of quantum constructs like OWPuzz, QAS, and OTMs as essential hardness assumptions. Integration methods such as semi-direct programming and Fourier analysis were shown to be vital in connecting quantum mechanics with cryptographic proofs. Despite progress, challenges remain in achieving tighter reductions, moving beyond idealised models, addressing quantum side-channels, and aligning theoretical security with practical constraints. The field is shifting towards more realistic and interdisciplinary approaches, essential for robust quantum-safe cryptography.

Acknowledgments We express our gratitude to the National Institute of Information and Communications Technology (NICT). This research was made possible through the support provided for Dr. Anandarup ROY's visit to Sakurai Lab at Kyushu University by the Foreign Researcher Invitation Program of NICT.

References

[1] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE, 1994.

[2] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pages 212–219. ACM, 1996.

[3] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum random oracle model and the one-way to hiding lemma. In *Advances in Cryptology – CRYPTO 2019*, pages 1–25. Springer, 2019.

[4] Joseph Jaeger. Nonadaptive one-way to hiding implies adaptive quantum reprogramming. Cryptology ePrint Archive, Report 2024/797, 2024.

[5] Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Tight adaptive reprogramming in the qrom. In *Advances in Cryptology – ASIACRYPT 2021*, pages 637–667. Springer, 2021.

[6] Dominique Unruh. Revocable quantum timed-release encryption. In *Advances in Cryptology – EUROCRYPT 2014*, pages 129–146. Springer, 2014.

[7] Jiaxin Pan and Runzhi Zeng. Selective opening security in the quantum random oracle model, revisited. In *Public-Key Cryptography – PKC 2024*, pages 92–122. Springer, 2024.

[8] Keita Xagawa. Signatures with memory-tight security in the quantum random oracle model. In *Cryptology ePrint Archive*, number 2023/1734, 2023.

[9] Jelle Don, Serge Fehr, and Christian Majenz. The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more. In *Advances in Cryptology – CRYPTO 2020*, pages 602–631. Springer, 2020.

[10] Gorjan Alagic, Chen Bai, Jonathan Katz, and Christian Majenz. Post-quantum security of the even-mansour cipher. In *Advances in Cryptology – EUROCRYPT 2022*, pages 458–487, 2022.

[11] Gorjan Alagic, Chen Bai, Jonathan Katz, and Christian Majenz. Post-quantum security of the even-mansour cipher. Cryptology ePrint Archive, Report 2021/1162, 2021.

[12] Kelsey Jackson, Carl Miller, and Daochen Wang. Evaluating the security of crystals-dilithium in the quantum random oracle model. In *Advances in Cryptology – EUROCRYPT 2024*, pages 418–446, 2024.

[13] Dakshita Khurana and Kabir Tomer. Commitments from quantum one-wayness. Cryptology ePrint Archive, Report 2023/1620, 2023.

[14] I. Rosset, M. Poremba, C. Majenz, A. Ambainis, A. Broadbent, J. F. Fitzsimons, V. Goyal, and A. Sahai. Quantum advantage samplers. *Quantum*, 7:1018, 2023.

[15] Anne Broadbent, Vinod Goyal, and Amit Sahai. Quantum one-time memories. In *Advances in Cryptology – CRYPTO 2013*, pages 636–653. Springer, 2013.

[16] Lev Stambler. Quantum one-time memories from stateless hardware, random access codes, and simple nonconvex optimization. *arXiv preprint arXiv:2501.04168*, 2025.

[17] Dominique Unruh. Quantum proofs of knowledge. *Cryptology ePrint Archive*, (2010/212), 2015.

[18] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition edition, 2010.

[19] Jacques Patarin, Olivier Cogliati, Jean-Philippe Aumasson, Itai Dinur, and Anne Canteaut. Mirror theory bounds in algebraic cryptanalysis. In *Advances in Cryptology – EUROCRYPT 2023*, pages 3–33. Springer, 2023.