The MARK-B.L.U. Architecture: A Quantum Hash Function Framework for Research and Implementation of Security and Verification of Agent Identity Outputs

Bhavyadhirr V. Bharadwaj[1]

[1] GENORROW ENTERPRISES

Abstract. Quantum Computation & Artificial Intelligence have been progressing from mere theoretical promises to experimental realities, and the cryptographic primitives, more than anything else, must thereby adapt to the noisy and limited-scaled capabilities of current quantum processors and over that mitigate the increasing gap between the expansion and scaling of AI Infrastructure, and the mostly underdeveloped security aspects of the said autonomous ecosystem. In this work, or odyssey of sorts, is introduced MARK-B.L.U. (Base Layer Unification); a novel quantum hash function architecture constructed using parameterized quantum circuits explicitly designed for Secure Agent Identity and Verifiable Autonomous AI outputs. MARK-B.L.U. serves as both a research framework and a defense model, providing not only an understanding, but also a practical and interpretable blueprint for investigating entropy generation, randomness extraction, and quantum-based hash properties. Unlike classical hash functions or existing quantum proposals that assume fault-tolerant architectures, the MARK-B.L.U. operates within the practical limitations of current hardware, balancing circuit depth, gate fidelity, and entropy spread. Presented here is also a comprehensive evaluation of the proposed architecture's behavior under multiple classical-to-quantum input encodings, simulated randomness profile through entropy distribution, and sensitivity analysis through collision resistance, avalanche effect, and bit independence tests. Furthermore, the research positions this architectural framework within the broader landscape of quantum cryptography by contrasting it against classical and quantum hash proposals identifying the niche it fills — that of a modular, scalable, and pedagogically rich hash function for autonomous infrastructure, which is operable "today". Moreover, by providing reproducible code, empirical validation, and educational scaffolding, this research work aims to catalyze both further inquiry and implementation of quantum hashing on real quantum hardware, while offering a stepping stone towards future fault-tolerant cryptographic primitives.

Keywords: Quantum Cryptography, Quantum Hash Function, Cryptanalysis, Parameterized Quantum Circuits, AI and Autonomous Infrastructure.

1 Introduction

With the rapid maturation of quantum computing technologies, and proliferation of Artificial Intelligence Infrastructure, has also come the catalysis of a paradigm shift in cryptographic design, challenging long-standing assumptions underlying classical

information security. As quantum processors approach intermediate-scale capabilities — known as the Noisy Intermediate-Scale Quantum (NISQ) era, a growing need has arisen for cryptographic primitives that are not merely resistant to quantum attacks, but natively constructed to exploit quantum resources. Amongst these primitives, quantum hash functions have garnered an ever-increasing interest due to their potential applications in secure communications, quantum blockchains, proof-of-work systems, entropy amplification, verifiable randomness generation, and more.

Classical hash functions such as SHA-256 or SHA-3, though foundational to current cryptographic infrastructure, suffer from the inevitable vulnerabilities in the presence of quantum adversaries. Grover's algorithm, for example, reduces the effective search space for hash collisions quadratically, threatening the long-term viability of these classical schemes, especially when looked in the context of securing AI and Autonomous systems. While the research into post-quantum cryptography has proposed quantum-resistant algorithms, such approaches remain inherently classical in design and do not take advantage native quantum phenomena, thus continuing the susceptible status-quo of the entire cryptographic demography in totality.

Despite the theoretical proposals for quantum hash functions, a significant research gap lies in the practical realization of such function architectures on current hardware. Umpteen of these proposals rely on idealized quantum models, unscalable assumptions, or hardware features that are not yet accessible on today's NISQ devices. Further, it is only a select few frameworks that offer reproducible, interpretable, and scalable implementations that can be tested, refined, and applied in both research and actual security settings.

To address the aforementioned gap, this paper proposes MARK-B.L.U. (or Base Layer Unification), a parameterized quantum circuit architecture for hash generation designed explicitly for Security and a notch up, verification of AI Identity implementation within right now, the context of National Defense. The proposed architecture is an operationally simple yet functionally sound hash function prototype built using Qiskit and executable on IBM quantum backends, designed to accept classical inputs and output deterministic hash-like signatures derived from quantum state manipulations. It simulates a 16-qubit, 3-layered entangled quantum circuit that:

- Encodes classical input into rotation parameters,
- Entangles qubits in alternating block layers,
- Outputs signatures from the final statevector of the circuit.

The hash is derived from the real/imaginary parts of selected amplitudes in the final quantum state. It is also seminal to note here, that after all the critique of the facet of non-deployability on hardware of previous iterations of hash functions, these test phases of MARK-B.L.U. are of the initial simulated model, thus it is only a part of the entirety of the eventual architectural proceeding that will be hardware deployable on field. All in all, essentially, the architectural framework of MARK-B.L.U. leverages input-dependent gate parameterization, circuit-level entropy diffusion, and measurement-induced randomness to generate binary hash outputs from classical inputs. Beyond its practical utility, it also functions as a modular platform for evaluating cryptographic properties such as entropy distribution, collision resistance, avalanche behavior, and bit independence in quantum circuits.

In summary, this work contributes directly in terms of the value addition towards forwarding the horizon of the known, as is expanded over in the following table.

Table 1.MARK-B.L.U. contribution and value addition space.

S. No.	Contribution Headers
1.	Fully reproducible framework that integrates parameterized gate encoding and quantum measurement-based randomness harvesting.
2.	Architectural evaluations against cryptographic metrics and empirical results on entropy distribution, avalanche effect, and output collision behavior.
3.	Bridging theoretical design and NISQ-compatible quantum cryptography by the means of an open-source implementation of the framework for educational and research use.
4.	Identification of key limitations, discussion of the hash function's use-case in securing high-stake AI Infrastructure in the context of National Defense, and suggestions for future extensions including hybrid-classical improvements, randomness extractors, and robustness to adversarial noise.

In doing so, this work not only introduces a viable cryptographic primitive but also provides a sandbox environment for further exploration of entropy dynamics, randomness amplification, and secure function design within the constraints of the current quantum hardware, holistically ensuring the communications, decisions, and outputs from AI Infrastructure, like drones, robots, or autonomous AI systems remain cryptographically authentic, tamper-evident, and provably quantum-secured.