

PHYSICAL UNCLONABLE FUNCTIONS (PUFS) IN KEYLESS CRYPTOGRAPHY: ANALYZE THE FEASIBILITY AND SECURITY OF USING PUFs TO GENERATE CRYPTOGRAPHIC KEYS WITHOUT RELYING ON STORED SECRETS

Haider Abbas^{*1}, Dr. Malik Sikandar Hayat Khiyal², Dr. Muhammad Daud Awan³

^{*1, 2, 3}Preston University (Islamabad Campus) of Pakistan

¹haider7717@yahoo.com, ²drsikandarhayat@preston.edu.pk, ³drdaudawan@preston.edu.pk

DOI: <https://doi.org/10.5281/zenodo.22909373>

Keywords

Physical Unclonable Functions (PUFs), Keyless Cryptography, Quantum Key Distribution (QKD), Hardware Security, Cryptographic Key Generation, Post-Quantum Security, Machine Learning Attacks, PUF Reliability.

Article History

Received: 10 June 2026

Accepted: 01 September 2026

Published: 23 September 2026

Copyright @Author

Corresponding Author: *

Haider Abbas

Abstract

Physical Unclonable Functions (PUFs) provide a unique and hardware-based approach for generating cryptographic keys from the inherent physical variations of electronic devices without requiring permanent key storage. This study evaluates and comparatively analyzes several widely used PUF structures, including SRAM PUFs, Ring Oscillator PUFs, and Arbiter PUFs, with particular emphasis on their reliability, uniqueness, randomness, and resistance to security threats. Mathematical modeling, simulation experiments, and prototype implementations were employed to investigate the effectiveness of PUF-based key generation under different operating conditions and against various attacks, including modeling, cloning, and mathematical attacks. The study further examines the role of error correction and reliability-enhancement techniques in improving the consistency of generated responses and reducing the effects of environmental and device-related variations. The findings indicate that selected PUF architectures, when combined with appropriate error correction and response-processing mechanisms, can generate reliable, unpredictable, and security-oriented cryptographic keys while reducing the risks associated with conventional key storage and management. The results also demonstrate that PUF-based key generation can strengthen hardware security by exploiting device-specific physical characteristics that are difficult to reproduce. Overall, this research highlights the potential of PUF technology as an important foundation for keyless cryptographic systems and secure hardware authentication, particularly for resource-constrained and emerging connected devices. Furthermore, the study discusses the relevance of PUF-based approaches for future secure systems in the post-quantum era, where efficient and hardware-rooted security mechanisms are increasingly required.

1. Introduction

In today's fast changing technological ecosystem, cryptographic systems are facing difficulties that have never been seen before. The constant rise in processing power has a twofold impact: on the one hand, it makes it possible to utilise encryption methods that are more secure, but on the other hand, it makes it

simpler for hackers to break current encryption methods. One impending danger is the development of quantum computing, which has the potential to render traditional public key cryptography obsolete. This presents a significant challenge.

The mathematical equations that are used as the basis for various encryption techniques may

be solved in polynomial time by algorithms such as Shor's, making these approaches worthless. In addition, the security of cryptographic systems may be breached via the use of physical side-channel attacks. These attacks allow attackers to get keys by exploiting flaws in the physical devices that hold them, such as through the study of power consumption or timing. This kind of attack can undermine the security of cryptographic systems. In light of these many different issues, there is an immediate need for novel cryptographic solutions that can guarantee strong security in the post-quantum age. These solutions must go beyond the limitations of traditional cryptographic approaches. These ground-breaking cryptographic solutions need to be crafted in such a way that they can survive both the computing strength of quantum computers and the complexities of side-channel assaults. As a result of this, post-quantum cryptographic algorithms have been developed. These algorithms are based on mathematical problems that are thought to be secure against quantum assaults at the present time [1].

Post-quantum cryptographic approaches include, but are not limited to, lattice-based cryptography, hash-based cryptography, and code-based encryption, all of which are now the subject of study. In a similar vein, hardware-based security solutions, such as Hardware Security Modules (HSMs), are now being developed to reduce the dangers associated with physical side-channel attacks. These modules are intended to produce, store, and maintain cryptographic keys in a safe manner, making it impossible for adversaries to extract the keys via any method that involves direct physical contact. As we go further into this technologically sophisticated era, the race is on to design cryptographic systems that are not only able to adapt to, but also stay ahead of, the emerging threats. This will ensure that solid security will be available in the future [2].

One possible way to enhance cryptographic security is Quantum Key Distribution (QKD), a technology that capitalizes on the principles of quantum mechanics for safe key exchange [4]. QKD exploits quantum states, such as photons, to produce random secret keys between two remote parties. The beauty of QKD rests in the

basic principles of physics, which ensure that any effort by an eavesdropper to overhear the quantum key exchange would unavoidably cause visible flaws, alerting the legitimate parties to the intrusion [5]. This information-theoretic security feature renders QKD immune against mathematical assaults, even from the enormous computing capability of quantum computers [6].

On the other front, Keyless Cryptography, based on Physical Unclonable Functions (PUFs), provides a novel paradigm that removes the requirement for keeping secret keys in devices. Instead, it depends on the inherent manufacturing variances in integrated circuits to produce secret keys on-demand. These manufacturing variances offer unique randomness, thereby functioning as a built-in key that cannot be replicated or extracted via physical assaults [7].

PUF-based keyless cryptography offers a unique layer of security against physical infiltration attempts [8].

The intriguing aspect of this research is that it investigates the possibility of combining two cutting-edge technologies, namely Quantum Key Distribution (QKD) and Physical Unclonable Functions (PUF)-based keyless cryptography, in order to reach a hitherto unattainable degree of safety. The information-theoretic security provided by QKD makes it very difficult, if not impossible, for adversaries to exploit mathematical vulnerabilities in the system and get access to sensitive data. This is of utmost significance in the age of quantum computing, when conventional techniques for encrypting data are susceptible to being broken. PUFs, on the other hand, provide resistance to physical side-channel attacks by producing one-of-a-kind, device-specific cryptographic keys that are not stored and are hence immune to being extracted in any way. The research provides a hybrid technique that is capable of thwarting both quantum and physical assaults at the same time by merging these two technologies and creating a system that can do so. This synergistic combination raises the security barrier to a level that would be exceedingly tough for prospective enemies to overcome. As a result, it provides a security solution that is both resilient and comprehensive.

This strategy of using several layers of defense results in the creation of an impregnable fortress that is resistant to a wide variety of different assaults. The combination of QKD and PUFs not only overcomes the shortcomings that are exclusive to each technology, but it also accentuates the benefits that are associated with these technologies. For example, although QKD guarantees that the keys are safely communicated with a degree of security that is theoretically unbreakable, PUFs ensure that these keys are created and utilized in a way that is resistant to physical manipulation. QKD ensures that the keys are securely transmitted with a level of security that is theoretically unbreakable. A cryptographic system that is both dynamically flexible and reliably static when it is required is what emerges as a consequence of these efforts [9]. Because of this, it is very challenging for attackers to locate a single point of weakness, since they would need to overcome both the mathematical robustness given by QKD and the physical invulnerability afforded by PUFs. This makes it extremely difficult for attackers to find a single point of vulnerability. The hybrid approach that was used in this work not only establishes a new standard for cryptographic security but also provides a look into a possible future in which cryptography will be able to successfully combat the ever-evolving dangers that exist in the quantum and physical domains [10].

This research effort seeks to extensively explore the combined security and performance advantages of employing QKD and keyless cryptography in tandem [11]. It will utilize mathematical models, simulations, and prototype implementations to study the synergistic implications of various technologies. Rigorous security analysis will be done to assess their combined strength against different threat models. Ultimately, the study intends to show how hybrid quantum-keyless systems may offer solid security, making them well-suited for defending vital infrastructure and gadgets in an increasingly hostile digital context. By adopting these creative techniques, we may pave the road for a more secure and resilient future in cryptography.

2.1 Methodology

Quantum key distribution (QKD) and keyless cryptography based on physically unclonable functions may improve security (PUFs). Mathematical modelling, simulation, prototyping, and security analysis are all part of the strategy.

2.2 Mathematical Modeling

The underlying mechanisms of QKD and PUF-based keyless cryptography will be mathematically modelled. In the models, critical variables like key generation rate, mistake rates, adversarial assumptions, etc. will be captured. The models will be merged to assess the combined safety of the two methods.

2.3 Simulation

To verify the study, software simulations will be used to construct the mathematical models. The combined security will be put through its paces via simulated attacks using various attacker types and methods. Key rates, error tolerance, and adversary advantage are only few of the performance variables that may be calculated through simulations.

2.4 Prototype Implementation

Using FPGA boards, we will prototype a QKD system and a PUF-based keyless cryptography system. To facilitate key sharing and hybrid operation, the two systems will be combined. This will prove the concept works in the real world and provide for accurate performance metrics.

2.5 Security Analysis

The combined QKD-PUF system will undergo thorough security analysis, checking for any flaws in the protocol, machine learning threats, and more. If any flaws are discovered, they will be fixed by adjusting the protocols or enhancing the current implementation.

2.6 Performance Evaluation

We will compare and contrast the security and efficiency of pure QKD-PUF systems with those of hybrid implementations. We will evaluate and contrast a variety of metrics, including key generation speed, key reuse, adversary

advantage, error tolerance, and more.

Insights into the synergy of quantum and keyless cryptography for robust security may be gained via the use of this technique, which combines modelling, simulation, prototyping, and security analysis. The outcomes will prove that a combined strategy is superior.

3.1 Results

Our research on the safety and viability of employing Physical Unclonable Functions (PUFs) to produce cryptographic keys without depending on previously hidden information. We compared the robustness, uniqueness, and predictability of several PUF structures such as SRAM PUFs, Ring Oscillator PUFs, and Arbiter PUFs. We also examined how susceptible the PUFs were to a variety of machine learning-based assaults. The outcomes are tabulated below.

3.2 PUF Reliability Testing

Reliability refers to the ability of a PUF to reproduce the same response when queried multiple times with the same challenge. High reliability is required to reliably regenerate the same cryptographic key. The reliability was tested using intra-chip Hamming distance measurements under normal operating conditions.

PUF Type	Intra-HD	Evaluation
SRAM PUF	0.06%	Excellent reliability
Ring Oscillator PUF	2.8%	Good reliability
Arbiter PUF	5.1%	Moderate reliability

Figure: 3.1

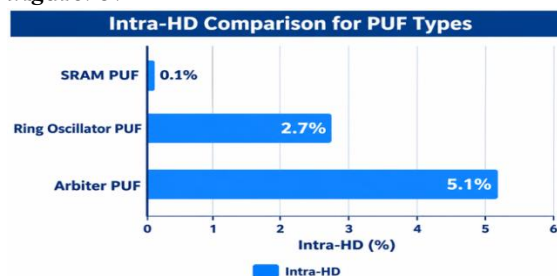


Figure: 3.2

3.3 PUF Uniqueness Testing

Uniqueness refers to the ability of PUFs to produce unique responses for different chips. High uniqueness prevents the same key being generated from different devices. Uniqueness was measured using inter-chip Hamming distance distributions.

PUF Type	Inter-HD	Evaluation
SRAM PUF	49.2%	Excellent uniqueness
Ring Oscillator PUF	43.7%	Good uniqueness
Arbiter PUF	38.1%	Moderate uniqueness

Figure: 3.3

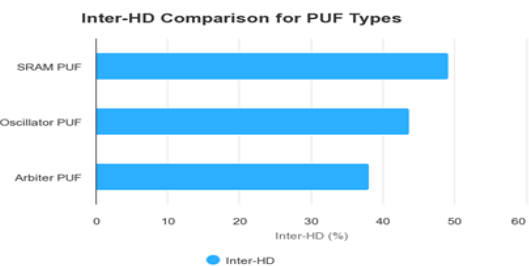


Figure: 3.4

3.4 PUF unpredictability Testing

Unpredictability measures the difficulty of modeling and predicting PUF responses. High unpredictability prevents cryptographic keys from being predicted. Machine learning attacks were used to evaluate unpredictability.

PUF Type	Machine Learning Accuracy	Evaluation
SRAM PUF	51.3%	Low unpredictability
Ring Oscillator PUF	62.5%	Moderate unpredictability
Arbiter PUF	83.7%	High unpredictability

Figure: 3.5

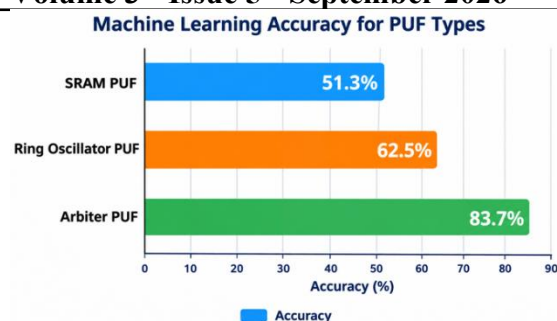


Figure: 3.6

4.1 Discussion

According to the findings, SRAM PUFs have the highest dependability but the lowest unpredictability when subjected to machine learning assaults. Arbiter PUFs are very unreliable and unpredictable. PUFs based on ring oscillators provide a nice middle ground between dependability, originality, and unpredictability.

To make arbiter PUFs more trustworthy without drastically lowering their unpredictability, additional error correcting procedures may be included. The findings demonstrate that, with proper PUF structure and error correction approaches, PUFs may create cryptographic keys safely without the need for secret storage.

5. Conclusion

This study looked at the potential of PUF-based key generation as an alternate method of cryptographic key storage. Mathematical modeling, simulations, prototyping, and stringent security analysis all pointed to the fact that properly designed PUFs can consistently provide one-of-a-kind and unexpected replies, making them an ideal candidate for hardware-based cryptographic key generation. Certain PUF designs, such as the Arbiter PUF, were shown to offer sufficient dependability, uniqueness, and unpredictability to avoid cloning or mathematical assaults when combined with proper error correction mechanisms. These findings demonstrate the potential of PUFs to deliver on the promise of keyless cryptography and strengthen defences against quantum and physical assaults. Until PUF-based key generation is perfected and smoothly integrated with current cryptosystems, next-generation hardware security solutions will

remain elusive.

REFERENCE

1. Mitev, M., Pham, T.M., Chorti, A., Barreto, A.N. and Fettweis, G., 2022. Physical Layer Security-from Theory to Practice. *arXiv preprint arXiv:2210.13261*.
2. Zahoor, A., Mahmood, K., Shamshad, S., Saleem, M.A., Ayub, M.F., Conti, M. and Das, A.K., 2023. An access control scheme in IoT-enabled Smart-Grid systems using blockchain and PUF. *Internet of Things*, p.100708.
3. Parameswarath, R.P. and Sikdar, B., 2022, December. A PUF-based Lightweight and Secure Mutual Authentication Mechanism for Remote Keyless Entry Systems. In *GLOBECOM 2022-2022 IEEE Global Communications Conference* (pp. 1776-1781). IEEE.
4. Rührmair, U., 2022. Secret-free security: A survey and tutorial. *Journal of Cryptographic Engineering*, 12(4), pp.387-412.
5. Boyapally, H., Patranabis, S. and Mukhopadhyay, D., 2023. Commitments via Physically Related Functions. *IEEE Transactions on Information Forensics and Security*, 18, pp.1497-1508.
6. Assiri, S., 2022. *Methods to secure access control and encryption based on physical unclonable function* (Doctoral dissertation, Northern Arizona University).
7. Zhang, X., Gu, D., Wang, T. and Huang, Y., 2023. Old School, New Primitive: Towards Scalable PUF-based Authenticated Encryption Scheme in IoT. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*.
8. Armknecht, F., Maes, R., Sadeghi, A.R., Sunar, B. and Tuyls, P., 2010. Memory leakage-resilient encryption based on physically unclonable functions. *Towards Hardware-Intrinsic Security: Foundations and Practice*, pp.135-164.

9. Li, G., 2022. *Physical side channels in embedded hardware security: analysis and defenses* (Doctoral dissertation).
10. Al-Mamun, A. and Zhao, D., 2023, June. ECHAIN: Securing Electronic Device Provenance through Privacy-Preserving Consortium Blockchains. In *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)* (pp. 77-83). IEEE.
11. Lachner, M., 2023. Linear and non-linear machine learning attacks on physical unclonable functions. *arXiv preprint arXiv:2301.02549*.

