Secure Encryption and Key Exchange using Arbiter PUF

Raja Adhithan Radhakrishnan
r.rajaadhithan@gmail.com
Society For Electronic Transactions and Security(SETS)

Abstract. This paper introduces a novel approach to enhancing cryptographic security. It proposes the use of one-time message sharing combined with Physically Unclonable Functions (PUF) to securely exchange keys and generate an S-subbyte-box for encryption. This innovative technique aims to elevate the security standards of cryptographic applications.

Keywords: PUF · Key exchange· modeling · S-box

1 Proposed one time message share machnism to exchange key securely multiple time using PUF between two device or network

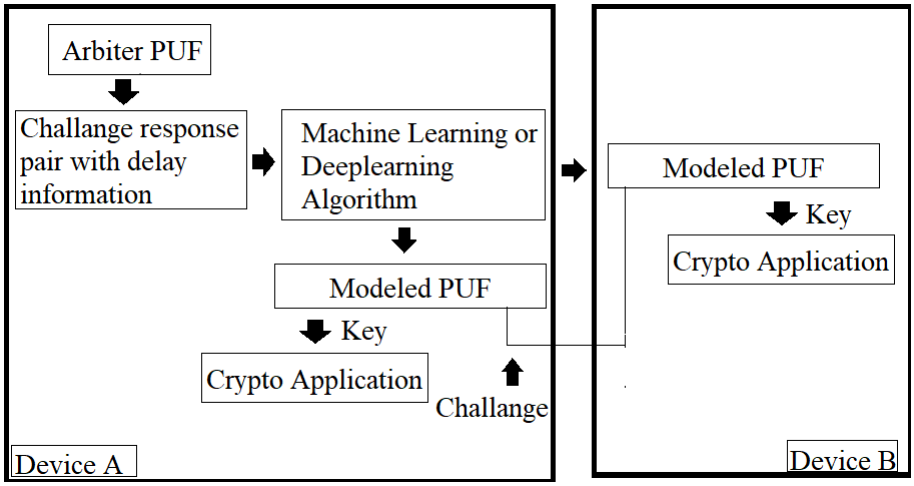

Fig. 1. Key exchange using PUF

In this approach, an arbiter Physically Unclonable Function (PUF) is modeled using machine learning or deep learning algorithms [1] in Device A and

subsequently transferred to Device B as shown in Fig.1. Both devices are provided with identical challenges to their respective modeled PUFs, resulting in the generation of a shared secret key. This shared secret key finds application in various secure data transfer scenarios. Moreover, in this scheme, the PUF can be modeled in either Device A or Device B and then transferred to the other side. Alternatively, a common server can be employed to generate the modeled PUF and share it with both Device A and Device B."message sharing mechanism integrated with Physically Unclonable Functions (PUF) serves to elevate the security standards of cryptographic applications." Note : This modeled PUF can be obfuscated and securely stored, leveraging the inherent security of PUF technology.

The benefits of this scheme are twofold: it offers uniqueness and flexibility in generating multiple private keys on both sides while also providing robust protection against computational attacks.""

2 Proposed Scheme is using PUF to generate S(sub-byte)Box for unique Encryption

In this approach, the S-BOX for encryption is created through PUF technology as shown in Fig.2, ensuring a unique encryption process, leading to device-specific, unpredictable computations. This, in turn, reduces the implementation complexity of Hardware Security Modules (HSMs). Moreover, employing a one-time message sharing mechanism with PUF enables distinct encryption and decryption for each device.Further I can use this PUF for unique key generation and side channel resistance [2].

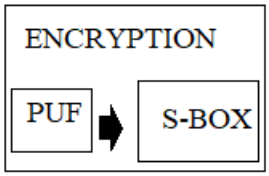

Fig. 2. S-BOX using PUF

3 Proof for this approachs

3.1 First approach

From [1] one of my research shown that Arbiter PUF can be modelled using artificial intelligent(AI)and its has large challenge response pairs.So this can shared onetime to securely generate mutilpe private key on both side.Therby side channel attacks [2] and Plain text attack [3] is become much harder.

3.2 Second approach

From [1] and [2] it state that PUF can be used to generate truly random number.Constant value of S-BOX is used in the every encryption.If we use the PUF to generate this constant value, then it is unique to the device [1] and computation become unknown(non-deterministic).

4 Conclusion

In conclusion, the integration of PUF technology in the one-time key sharing process, along with the generation of a unique S-BOX for encryption, significantly elevates the security of cryptographic applications. The use of PUF-generated keys adds an inherent layer of complexity, making them extremely challenging to compute or replicate.

5 Future Direction

From[4][5], current research utilizes quantum key exchange mechanisms to prevent eavesdropping on key exchanges. In the upcoming papers, I will detail discusses the advantage of Arbiter PUF model (APM) exchange over a quantum channel compared to the prior works.An overview is shown below.

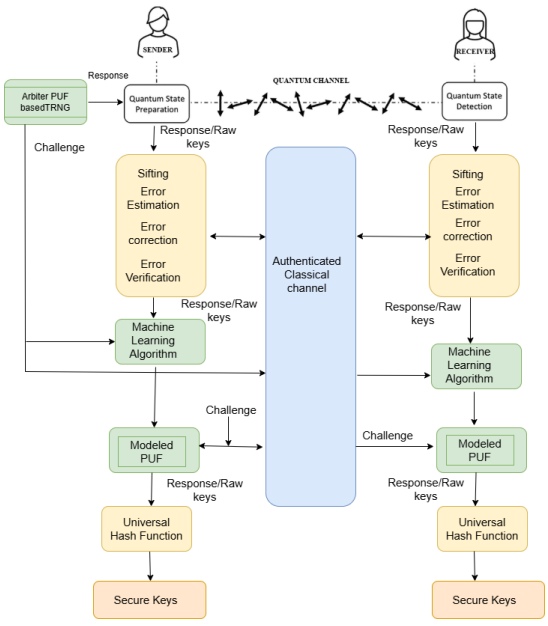

Fig. 3. Arbiter PUF Model exchange via quantum channel

In the above method, I propose using an Arbiter PUF-based True Random Number Generator (TRNG) to generate random numbers(Responses) on sender side(Alice), which are then converted into quantum signals and transmitted to the receiver side(Bob).On the receiver's side, the quantum signal is measured and converted back into classical bits.

The error-free bits are then isolated through post-processing, and the corresponding challenge is retrieved from the sender after error verification. Meanwhile, after error verification on the sender's side, an Arbiter PUF model(Modeled PUF) is constructed using random numbers and their corresponding challenges with the help of a machine learning algorithm, as shown in Fig.3. On the receiver side, using machine learning algorithms, the same Arbiter PUF is modeled(Modeled PUF) as on the sender's side, using the isolated error-free bits (response from error verification) and the challenge retrieved from the sender.

To generate the same keys on both sides, the same challenge is provided to the modeled PUF through exchange via a classical channel. Finally, a universal hash function is applied to increase the entropy of the keys on both sides, as shown in Fig. 3.

This approach enables secure sharing and periodic updates of the modeled PUF on both sides. Thus, the system can improve the throughput of quantum key exchange mechanisms and effectively address emerging threats.

References

1. R. Raja Adhithan, N. Nalla Anandakumar"Modeling Attacks and Efficient Countermeasures on Interpose PUF". FPS 2020: 149-162 pp. 396–401.
2. Raja Adhithan RadhaKrishnan ,Suganya annadurai "Side-Channel Resistant Implementation Using Arbiter PUF"Cryptology ePrint Archive, Paper 2023/047.
3. https://www.sciencedirect.com/topics/computer-science/plaintext-attack
4. Liu, Y., Sun, Z., Zhang, Y., Huang, C. (2020). Quantum Key Distribution Networks: A Survey. IEEE Communications Surveys Tutorials, 22(1), 593-604. https://doi.org/10.1109/COMST.2019.2958200