PUF based Lightweight Authentication and Key Exchange Protocol for IoT

Sourav Roy[a], Dipnarayan Das[b], Anindan Mondal[c], Mahabub Hasan Mahalat[d], Suchismita Roy and Bibhash Sen[e]

Department of Computer Science and Engineering, National Institute of Technology Durgapur, Durgapur, WB, India

Keywords: Internet of Things (IoT), Physically Unclonable Function (PUF), Hardware Security, Lightweight, Authentication, One-Time Pad (OTP), Proverif.

Abstract: Internet-of-Things (IoT), an integral part of today's smart society, is facing tremendous challenges of different security and interoperability attacks. Also, IoT device works in resource-constrained environments with limited storage. Conventional cryptography is not suitable for low-cost IoTs, and also they are susceptible to physical attacks. This work proposes a lightweight authentication and key exchange protocol utilizing the physically unclonable function (PUF) as security primitive. A single PUF challenge-response pair (PUF-CRP) is utilised to overcomes the server's storage overhead in the proposed protocol. Also, this protocol ensures the secret message passing using the lightweight XOR function. The proposed protocol authenticates the end-user successfully as well as maintains the security of the shared secret. The two-pass approach of the proposed method builds confidence in communicating entities. Formal analysis by automated Proverif tool validates its security. Performance evaluation advocates the superiority of the proposed protocol over the existing methods upholding its strong security and lightweight feature.

1 INTRODUCTION

The Internet of Things (IoT) has emerged as the core technology for making smart cities, building automation, automotive engineering, cyber-physical systems, smart homes, e-healthcare, agriculture monitoring, etc. IoT has also become the backbone of the current century's industrial automation, referred to as Industry 4.0 or industrial IoT (IIoT). Besides the ease of accessibility of IoT, researchers face challenges like interoperability, security, and connectivity to resolve. Also, in a conventional network, only internet users face privacy concerns. But in the context of IoTs, those who are unaware of technology also join the rally.

Components of an IoT (i.e., sensors, actuators, nodes, RFID tags, mobile phones, etc.) connected with a particular server can easily be deployed solitary even in extreme environments, and chances arose to be attacked by an adversary. IoT devices are susceptible to unauthorized physical access by an intruder due to limited or no protection in a diverse environment.Again, a tiny battery-backed IoT device has limited hardware resources that prevent the usage of expensive classical cryptographic algorithms.Hence, alternative approaches require addressing those limitations.

In this direction, physically unclonable function (PUF), which extracts the fabrication variation to provide a unique identity, has emerged as a viable solution(Rührmair and van Dijk, 2013; Aman et al., 2020). The security achieved through the use of PUFs is in the full range of scalable security while maintaining low power system operation in a small footprint. PUF-based low-cost authentication requires less area, power, and mask layers than any traditional approach.

Several works on PUF based security protocol have been developed for the IoT security framework (Chatterjee et al., 2018). However, very few of these PUF based protocols are available to address the challenges of resource-limitation, largely distributed wireless heterogeneous nature of IoT network. Also,

[a] https://orcid.org/0000-0003-1885-3995
[b] https://orcid.org/0000-0002-7185-2978
[c] https://orcid.org/0000-0002-6175-1380
[d] https://orcid.org/0000-0003-3047-236X
[e] https://orcid.org/0000-0003-4803-3074

Roy, S., Das, D., Mondal, A., Mahalat, M., Roy, S. and Sen, B.
PUF based Lightweight Authentication and Key Exchange Protocol for IoT.
DOI: 10.5220/0010550906980703
In *Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021)*, pages 698-703
ISBN: 978-989-758-524-1

these protocols suffer from various overheads, such as NVM use in IoT devices, costly MAC and excess CRP storage in servers. Moreover, lack of formal security analysis for these protocols makes them very hostile.

These issues motivate us to propose a lightweight authentication and key exchange protocol for IoT security comprising PUF as a hardware fingerprint to prevent physical attacks, like tampering, MAC spoofing, etc. This protocol reduces the overhead of cryptographic engines in resource-constrained IoT devices, reducing the authentication overhead between an IoT device and server. The contribution of the proposed work are as follows:

- A PUF based lightweight two-pass authentication protocol which allows secure authentication between an IoT node and server.
- The proposed protocol stores a single CRP into the serve to reduce storage overhead and improve efficiency in a large-scale heterogeneous IoT network.
- Formal security analysis using the automated Proverif tool validates the security of the proposed protocol.
- Finally, the performance analysis signifies the superiority of the proposed protocol.

2 BASICS OF PHYSICALLY UNCLONABLE FUNCTION (PUF)

Physically Unclonable Function (PUF) extracts the unique inherent fabrication variation of a device to provide it a unique identity. The physical system of a PUF maps a set of input (i.e., challenge) into an output set (i.e., response) which is hard to characterize (i.e., unique), model, or reproduce (i.e., unclonable). This system is unique for every hardware instance, and the static mapping is random in nature. A PUF has its application in low-cost authentication and cryptographic key generation, keyless authentication, IC anti-counterfeiting, device identification, etc. (Mukhopadhyay, 2016).A *weak PUF* has its linear or polynomial set of CRPs, whereas a *strong PUF* can go with exponential scaling of CRPs production. For an ideal strong PUF, CRPs are infeasible to fully readout or make a computer model predict its output because of its complex features.

Mathematically a PUF can be expressed as:

$$f_{PUF} : C \rightarrow R$$

Where, $C_i \in C, R_i \in R$ for any $i \in \mathbb{N}$.
C and R represent the set of challenges and generated responses by a PUF instance f_{PUF}.

- **Uniqueness Property of PUF.** Uniqueness measures the difference between the response of two similar PUF instance generated against the same challenge. An ideal PUF should have uniqueness of 50%.
- **Reliability of PUF Response.** Reliability measures the stability of a PUF response for a fixed challenge in different environmental conditions. Ideally, the reliability is 100%. An efficient ECA can be accessed in (Gao et al., 2018), which has very low hardware overhead.

Without loss of generality, we consider an ideally reliable strong PUF for the proposed protocol.

3 RELATED WORKS

The PUF concept was first introduced in (Pappu et al., 2002). The IoT protocol in (Aman et al., 2016) reports PUF as security primitive against physical and side-channel attacks with the help of cryptographic message authentication code (MAC) for integrity preserving and entity authentication. A PUF based authentication and key exchange protocol for IoT is proposed in (Chatterjee et al., 2018). Another PUF based authentication scheme in (Muhal et al., 2018) is applicable for secure interaction among IoT devices. Security achieves from these conventional cryptographic MAC, ECC, Key-ed hash, and encryption-decryption schemes are causes overhead for resource-constrained IoT. Lightweight PUF based WiFi protocol between IoT and router in (Mahalat et al., 2018) utilize three sets of PUF-CRPs. The use of cryptographic XOR reduces computation overhead. However, any large WiFi-connected system router incurs the overhead for holding three CRPs for each entity authentication and reduces the scalability. These factors motivate us to design a lightweight protocol for secure authentication and key exchange for rapidly growing heterogeneous IoT devices.

4 DESIGN OF THE LIGHTWEIGHT PROTOCOL

Here, we first describe a generic threat model for the application of the proposed protocol, and then introduced the proposed lightweight PUF embedded mutual authentication protocol for IoT networks.

Table 1: Notation Description Table.

Notation	Description
id_{node}	Unique identity of the IoT device
C_i	PUF challenge for any i^{th} iteration
R_i	PUF responses for C_i
nonce	A random number
f_{PUF}	Function to represent PUF-CRP mapping
$\oplus$	Cryptographic XOR operation
H	Instance variable of hashing
$\mathbb{N}$	Set of natural numbers
LFSR	Linear feedback shift register

4.1 Protocol Threat Model

The following premises are taken into account for the proposed protocol.

- Any physical tampering of the device immediately affects the PUF, i.e., the PUF based IoT device is tamper-resistive.
- Once the PUF embedded nodes are deployed in operation, the PUF response can only be accessed through the existing communication protocol.
- Database of the server that holds CRPs is secure enough against adversarial attacks.
- Considering large IoT network, a resource constrained IoT node is chosen. On the other hand, a server is considerably resourceful.

4.2 Proposed Protocol Design

The protocol consists of two modules. First, *i. one-time enrollment* phase to enroll a newly connected IoT node with the server. Second, *ii.* device *authentication* phase The notations used throughout the paper are summarized in "Table 1".

4.2.1 One-time Enrollment Phase

Enrolling the PUF-CRP for secure authentication is done in a secure environment without any access to the adversary. In this phase, server generates a random challenge (C_i) for the PUF, embedded in IoT (id_{node}) and collect the generate response (R_i) and stored in a secure database of the server as CRP, shown in "Figure 1".

$$R_i = f_{PUF}(C_i)$$

4.2.2 Authentication Phase

Authentication starts with 'Message 1' i.e. connection initialization phase of "Figure 2", where the IoT node sends connection request to the server after successful completion of *one-time enrollment*.

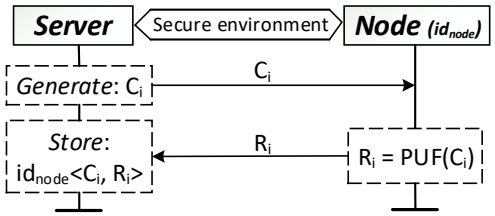

Figure 1: PUF embedded one-time enrollment.

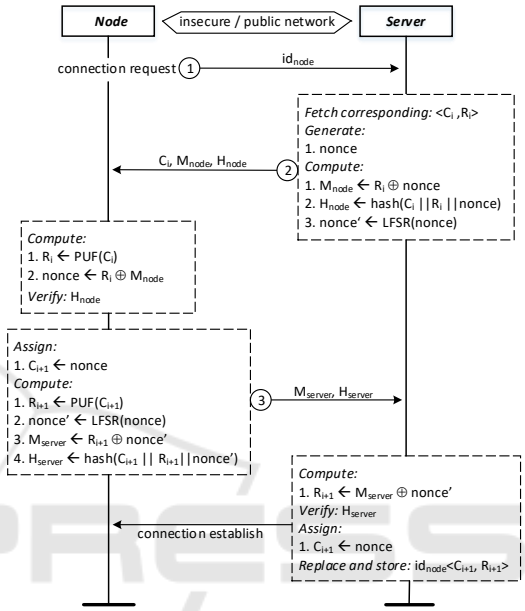

Figure 2: Proposed PUF embedded authentication protocol for IoT.

- Server searches for id_{node} in its secure database and fetches corresponding C_i, R_i to perform the authentication.
- Sever generates a random number *nonce*. This *nonce* is then masked with R_i using XOR as OTP to get the message M_{node}.

$$M_{node} \leftarrow R_i \oplus nonce$$

- This *nonce* act as a trusted freshness to prevent replaying older messages.
- Hash value H_{node} is calculated by concatenating C_i, R_i and *nonce*. Then it is forwarded to the node for verification.

$$H_{node} \leftarrow hash(C_i||R_i||nonce)$$

The server sends 'Message 2' to the node.

a. **Server Authentication.** Upon receiving 'Message 2' from the server, the communicating node having id_{node} first feed the C_i to its embedded PUF. Then produce a response R_i similar to its previously stored response in the server's secure database.

$$R_i = f_{PUF}(C_i)$$

- Generated R_i is then used to get *nonce*, in the step
$$nonce \leftarrow R_i \oplus M_{node}$$
- Message integrity and authenticity is then ratified by verifying the H_{node} by the IoT node. The successful verification confirms that the communicated messages are not tampered in-between.
- The IoT node is then uses the collected *nonce* as C_{i+1} to update old challenge C_i. It foster a new response R_{i+1} from the updated C_{i+1}.
$$C_{i+1} \leftarrow nonce$$
$$R_{i+1} \leftarrow PUF(C_{i+1}))$$
- The IoT node improvises *nonce* to $nonce^{'}$ by passing the *nonce* into a linear feedback shift register (LFSR), same as the server does after sending 'Message 2' to the node (*in compute: step 3* of server).
$$nonce^{'} \leftarrow LFSR(nonce)$$
- Newly generated PUF R_{i+1} is then masked with $nonce^{'}$ and transferred as M_{server} to the server. Integrity preserving hash H_{server} for node authentication is also sent to the server (shown by 'Message 3') by the IoT node.
$$R_{i+1} \oplus nonce^{'}$$
$$H_{server} \leftarrow hash(c_{i+1}||R_{i+1}||nonce^{'})$$

b. **Node Authentication.** R_{i+1} is decrypted by the server from M_{server} of received 'Message 3'.
$$R_{i+1} \leftarrow M_{server} \oplus nonce^{'}$$
- The server verifies the received H_{server} by computing hash value with help of R_{i+1}, C_{i+1} and $nonce^{'}$. Trusted integrity and authenticity claimed by the node hold for successful verification. This authenticates the intended IoT device, and the use of OTP helps in the secure exchange of new volatile secret R_{i+1}.
- On confirmation, the server replaces the previous CRP with this newly acknowledged (C_{i+1}, R_{i+1}) of id_{node} in its secure database for the next iteration of communication.

Success of the proposed protocol ("Figure: 2)" depends on the PUF function having volatile secret R_i. The random number *nonce* masked with OTP eliminates the trust issue in key transportation scenarios as a cryptographic secret. For every generation of *nonce*, a new communication is initiated to preserve freshness.

Finally, after successful authentication, actual message transmission takes place between an IoT node and server. PUF response R_{i+1} is used as shared secret. This shared secret helps to establish *session key* after authentication to resist attack against *chosen plain text* and *chosen cipher text*. So, proper analysis is required to establish the validity of our claimed security.

5 SECURITY ANALYSIS

Analysis of security taxonomy for the proposed protocol is as follows:

Probabilistic Analysis. Repetition probability (P_{rep}) of *nonce* combined with a R_i is:
$$P_{rep}(M_{node}) = 1/(2^{2n})$$
where 2^n exemplify each outcomes for any n.

Similarly, repetition frequency of any $R_{i+1} \oplus nonce^{'}$ stored as M_{server} is 2^{2n}. So, in reality brute force attack is quite impossible for some sufficiently large n (i.e. 64 bits or 128 bits in practice).

CIA Triad. Encrypting R_i and R_{i+1} with cryptographic secure XOR along with equal length *nonce* and $nonce^{'}$ respectively preserve message *confidentiality* in communication. The hashing algorithm ensures that the data has not been modified in transit. It is to preserve message *integrity* between the intended sender and receiver of the message. The presence of tamper resistive and uniquely identifiable PUF in the IoT device and the PUF CRP in the server's secure database assists to *authenticate* both the sender and receiver.

Non-repudiation. The unclonability property of PUF, where each response is random in nature, and every PUF module is unique by its implementation. It works as a digital fingerprint for every device to safeguard against message repudiation, where denial of generated response carries the PUF feature. This non-repudiation with the mentioned CIA triad provides more robust security features for the proposed protocol.

5.1 Formal Security Verification using Proverif Tool

The security property of the protocol is formally verified using the ProVerif tool (Blanchet, 2013; Roy, 2021). Based on the proposed protocol, node and

Table 2: Comparison Study.

Protocol	Application Area	TC1	TC2	TC3	TC4	TC5
(Aman et al., 2016)	IoT	N	N	XOR	1	high
(Muhal et al., 2018)	IoT	N	N	cipher	1	high
(Chatterjee et al., 2018)	IoT	N	Y	ecc	1	high
(Mahalat et al., 2018)	WiFi	N	N	XOR	3	high
(Alladi et al., 2020)	IoD	Y	N	XOR	1	low
Proposed Here	IoT	N	N	XOR	1	low

Note: TC1: PUF-CRP database in IoT, TC2: Explicit storage for key holding, TC3: Message transmission mode, TC4: Number of PUF-CRPs accessed for every authentication phase, TC5: Incurred hardware overhead.

server are the two roles, and their corresponding behaviors are defined in *ProVerif* as *eventA* and *eventB* respectively. $begin < event >$ defines the starting or initiation of authentication request and $end < event >$ defines the termination of the existing request. The occurrence of two events (*event A* and *event B*) in proverif result is described as follows:

i. *Server Authentication by IoT Node: eventB* will terminate the execution only when it has initiated the execution, which means if any attacker impersonate and initiate a authentication request, this proverif implication will return false value.

$$inj-event(endBfull(..)) ==> inj-event(beginBfull(..))$$

ii. *Node Authentication by the Server: eventA* will terminate the execution only when it has initiated the execution, which means if any attacker impersonate and initiate a authentication request, this proverif implication will return false value.

$$inj-event(endAfull(..)) ==> inj-event(beginAfull(..))$$

iii. *Secret Communication between Node and server:* The presence of an adversary in protocol communication through a public channel is incorporated as *attacker* in this security automation tool. Attacker query executes throughout the protocol's completion to eavesdrop on the shared secret between the node and the server.

$$\begin{aligned} query \quad & attacker(ARa); attacker(ARb) \\ & attacker(BRa); attacker(BRb) \\ & attacker(AR_{new}); attacker(BR_{new}) \end{aligned}$$

These attacker are inculcated in the execution query to check secrecy of *nonce* and $R_{(i+1)}$ with respect to node as well as server side.

This automated verification result shows that our proposed protocol is resistive against defined adversarial attack.

5.2 Modelling Robustness

In the proposed protocol, an adversary is able to obtain C_i from 'message 2' and 'message 3'. Corresponding R_i is also required to create a PUF model based on machine learning attacks. The XOR encrypted R_i is hard to guess for any sufficient large bit length. Hence, building a numerical model with an exact randomness feature is considered infeasible.

It is also convenient that, once the enrollment process is complete, PUF responses are accessible only through the proposed authentication protocol. So, the *one-time enrollment* immunises cloning attack from an adversary with physical access to the PUF enabled IoT. Hence, the proposed protocol can prevent physical attacks.

6 PERFORMANCE EVALUATION AND COMPARISON

"Table 2" represent the performance evaluation with existing literature in terms of the protocol architecture. It is evident from the table that this proposed protocol need not require storing PUF CRP in the IoT Node. Using a single PUF CRP for entity authentication and easy-to-implement cryptographic XOR has superior performance improvements over conventional cryptographic cipher message or ECC execution. The final column, 'TC5' concludes the overall overhead incurred by the different protocols in terms of hardware architectural dependency, and We restrict the proposed protocol design in lightweight. "Figure 3" compare the computation performance of different protocols along with the proposed here. "Figure 3(a)" shows the computation made by the IoT Node and "Figure 3(b)" for server. This comparison is made between different similarly performed protocols.

In IoT node side computation, the proposed protocol eliminates computationally expensive MAC with hash functions. But, even though the hash count sur-

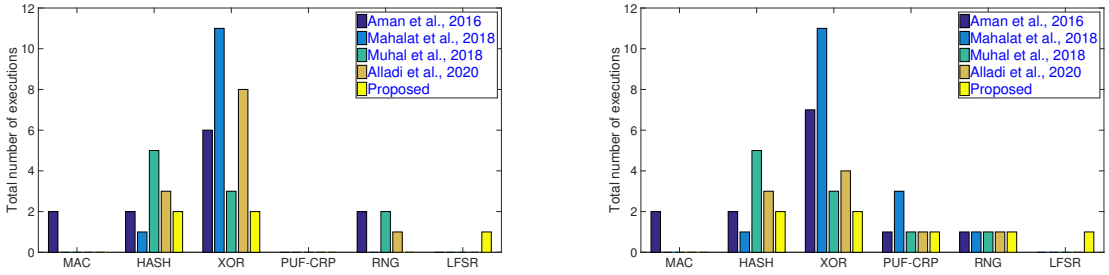

Figure 3: (a) Performance comparison of IoT device. (b) Performance comparison of Server.

passed mahalat et. al., the balanced use of single PUF CRP and LFSR in this protocol reduces down the number of XOR count at a certain optimal compared with by them. Similarly, in server-side computation, fast computing LFSR balances the performance of hash and XOR together. Here we have also eliminated the cryptographic MAC for faster and lightweight performance. Thus, the claimed authentication and lightweight key exchange in this proposed protocol is successfully established.

7 CONCLUSION

A single PUF CRP-based two-pass mutual authentication and key exchange protocol are presented in this paper. Comparison analysis makes the protocol lightweight in nature, and ease of implementation make the protocol suitable for heterogeneous WSN and the internet of connected things. Less computational functionality with adequate security raises the proposed protocol's acceptability while maintaining power consumption at its optimal level. The PUF based challenge-response mechanism helps in unique device identification and authentication resists any physical attack while maintaining communication security as the utmost priority.

ACKNOWLEDGMENT

This work is supported by DST-SERB under core research scheme (Formerly EMR) through grant No. EMR/2017/003206 and Young Faculty Research Fellow of Visvesvaraya PhD scheme through the grant No. MLA/MUM/GA/10(37)B.

REFERENCES

Alladi, T., Naren, N., Bansal, G., Chamola, V., and Guizani, M. (2020). Secauthuav: A novel authentication scheme for uav-base station scenario. *IEEE Transactions on Vehicular Technology*.

Aman, M. N., Basheer, M. H., and Sikdar, B. (2020). A lightweight protocol for secure data provenance in the internet of things using wireless fingerprints. *IEEE Systems Journal*.

Aman, M. N., Chua, K., and Sikdar, B. (2016). Position paper: Physical unclonable functions for iot security. In *2nd ACM international workshop on IoT privacy, trust, and security*, pages 10–13. ACM.

Blanchet, B. (2013). Automatic verification of security protocols in the symbolic model: The verifier proverif. In *Foundations of security analysis and design VII*, pages 54–87. Springer.

Chatterjee, U., Govindan, V., Sadhukhan, R., Mukhopadhyay, D., Chakraborty, R. S., Mahata, D., and Prabhu, M. M. (2018). Building puf based authentication and key exchange protocol for iot without explicit crps in verifier database. *IEEE transactions on dependable and secure computing*, 16(3):424–437.

Gao, Y., Su, Y., Xu, L., , and Ranasinghe, D. C. (2018). Lightweight (reverse) fuzzy extractor with multiple reference puf responses. *IEEE Transactions on Information Forensics and Security*, 14(7):1887–1901.

Mahalat, M. H., Saha, S., Mondal, A., and Sen, B. (2018). A puf based light weight protocol for secure wifi authentication of iot devices. In *2018 8th International Symposium on Embedded Computing and System Design (ISED)*, pages 183–187. IEEE.

Muhal, M. A., Luo, X., Mahmood, Z., and Ullah, A. (2018). Physical unclonable function based authentication scheme for smart devices in internet of things. In *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pages 160–165. IEEE.

Mukhopadhyay, D. (2016). Pufs as promising tools for security in internet of things. *IEEE Design & Test*, 33(3):103–115.

Pappu, R., Recht, B., Taylor, J., and Gershenfeld, N. (2002). Physical one-way functions. *Science*, 297(5589):2026–2030.

Roy, S. (2021). Github: Proverif scripts for node server authentication protocol. *GitHub repository: https://github.com/sourav-roy-git/Proverif_scripts*.

Rührmair, U. and van Dijk, M. (2013). Pufs in security protocols: Attack models and security evaluations. In *2013 IEEE symposium on security and privacy*, pages 286–300. IEEE.