2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) | 979-8-3503-8199-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/TrustCom60117.2023.00233

LPA: A Lightweight PUF-based Authentication Protocol for IoT System

Vikash Kumar Rai
SCSDF
National Forensic Sciences University, Goa
Goa, India
vikash.rai_goa@nfsu.ac.in

Somanath Tripathy
Dept. of CSE
Indian Institute of Technology Patna
Patna, India
som@iitp.ac.in

Jimson Mathew
Dept. of CSE
Indian Institute of Technology Patna
Patna, India
jimson@iitp.ac.in

***Abstract*—With the emergence of the Internet of Things (IoT), there come opportunities to connect people, data, and objects, bringing dynamic changes in our way of living. At the same time, the presence of sensors and other devices around us has created a leaky ecology that is webbed. It has turned into a risk for the users and causes worry about how widely it could be adopted. Numerous projects have been put up in a similar vein, creating innovations to improve security. But, conventional cryptographic solutions are difficult to embed as these IoT devices have limited resources. Physical unclonable functions (PUFs), particularly in resource-restraining devices, have shown to be valuable for developing authentication protocols. In this work, we propose a PUF-based authentication mechanism for IoT devices. This authentication protocol also performs the key exchange between the two nodes, with the server in between. The security features of the proposed mechanism are verified using AVISPA tool.**

***Index Terms*—IoT Security, Authentication, Physical Unclonable Function (PUF)**

I. Introduction

IoT devices have seen a rapid increase over the past decade, surpassing humans by 1.5:1 as of 2014. It has emerged as an enabling technology for smart cities, power grids, health care, and control systems, which most suit crucial installments and infrastructure. Increased control and interaction of devices with the fact that IoT systems transfer large amounts of data over the public network makes them vulnerable to attacks. IoT security is tied to human safety, which has made network and internet security an active research area over the last two decades. The existing security mechanisms look imperfect, with significant security breaches. Secure booting, authentication, privacy protection, data integrity, user profiling and tracking, access control, and digital forgetting are the critical areas of concern in IoT systems. Apart from that, many IoT devices are very much resource constraint; sometimes, few devices operate without a battery or power source with the help of some harvesting of energy. So it is challenging to design a security protocol for an IoT environment with less resource overhead.

The conventional security protocol will not be feasible in the IoT environment because IoT nodes have limited energy and power sources. The second assumption making it infeasible to adopt conventional security protocols in the IoT domain is that devices are physically well protected. Rather, the devices are deployed in various geographical locations where an attacker or adversary can control them. So, the physical security of an IoT device is a challenging task. For instance, a memory of an IoT device may be physically controlled and tampered with to read sensitive information like keys to break the security and launch an attack. We use the physical unclonable functions to address such issues. The physical unclonable functions work on the challenge-response mechanism and exploit the manufacturing process variation of the chip to generate a device-specific signature, which is called a response, based on the applied challenge. The manufacturing process variations produce random behavior for different integrated circuits (ICs). So each device has a unique response, even for the same set of challenges. This ensures that no two copies of the same PUF are possible. Authentication is one of the prominent security features in the IoT environment. A user or device should be able to verify whether the data it receives is coming from the intended user or device. We have mentioned earlier that such authentication should be done as if no data should be stored in the memory of the device.

In this work, we propose a secure authentication for IoT devices using physical unclonable functions. The presented scheme accomplishes the required efficiency and security using a physical unclonable function (PUF). This paper achieves two important goals in the context of data security. First, it provides authentication between two IoT devices and between IoT devices and servers. Second, the proposed protocol can also be used to exchange the key between the two IoT nodes.

The major contributions of this work are as follows:

1) We present a robust and secure authentication protocol for IoT devices, employing physical unclonable functions to ensure security.
2) The proposed protocol establishes a robust authentication mechanism among interconnected IoT devices, ensuring their mutual trustworthiness.
3) It extends this formidable authentication to encompass the interactions between IoT devices and servers, thus fortifying the overall security of the IoT ecosystem.
4) The security evaluation and formal security verification for the proposed protocol using AVISPA give theoretical and formal guarantees.
5) We provide performance analysis and a comparison of

2324-9013/23/$31.00 ©2023 IEEE
DOI 10.1109/TrustCom60117.2023.00233

the proposed protocol with existing PUF-based authentication protocols. The empirical results show a shred of evidence, justifying the efficiency and efficacy of the proposed protocol.

The rest of the paper is organized as follows. Section II discusses some existing works on this topic. The system model and assumption are provided in Section III. Section IV presents the proposed authentication protocol. Section V provides a security evaluation of the proposed protocol. The performance analysis is provided in Section VI. We also compare our proposed protocol with some recent PUF-based authentication protocols in that Section. Section VII provides the summary of this paper.

II. Related Work

The different challenges and advice for Internet of Things (IoT) systems are presented in [1]. This paper suggests using the physical unclonable function for the security of IoT systems. An authentication protocol that uses a one-time password (OTP) is proposed in [2]. This scheme has to perform several iterations and compute OTPs using the public and private keys. This enhances the computational cost and complexity of the complete protocol. The other authentication protocol is presented in [3], which is a group authentication. The main disadvantage of this protocol is that all nodes would be at risk, even if a single node is attacked or compromised. Another lightweight protocol for authentication, which is based on PUF, is presented in [4]. In this work, the authors presented two authentication protocols. One protocol is designed when IoT devices want to communicate with the server, and the second protocol is designed when the two IoT devices want to communicate with each other. PUFs have been previously used in authentication protocols for wireless sensor networks (WSNs) and radio-frequency identification (RFID) systems [5]–[9].

Moreover, some of the PUF-based authentication protocols require a trusted party to store a large number of challenge response pairs (CRPs) for each IoT device [11], [12]. Given the increasing number of IoT devices, these protocols are not scalable. One of the most interesting PUF-based protocols is discussed in [10]. In this, the authors proposed an authentication protocol that is based on PUF and uses the zero-knowledge proof (ZKP) for the discrete logarithm. The main advantage of this protocol is that it does not need to reveal the CRP pair in any communication messages, so it achieves a high level of security, but the major drawback of this protocol is that the user always needs to input the password to the system or device every time when it requires authentication. This drawback limits the efficacy of this protocol. Another drawback of this protocol is that it can only be used to authenticate the server and the device. It can not be used in the authentication between the device to devices. Also, the ZKP of discrete logarithm makes it a more complex protocol.

In [11], the author says that normal PUF-based authentication is dependent on CRP pairs, introducing an overhead to retrieve each time when the device needs authentication. So they proposed a protocol based on the PUF model to make available the whole CRP set and then use encryption to protect the CRP set from the attack. A lightweight PUF-based authentication protocol is presented in [12]. This is based on a neural network model-based PUF. This model of PUF may learn PUF behavior when it is provided with all the CRP set for training to solve the key problem of the normal PUF-based authentication. In [13], The authors use the secret-sharing methodology with PUF to authenticate the two devices in an efficient and effective manner. This protocol does not use the traditional CRP set for authentication, which normally other PUF-based protocols do; rather, it uses secret shares to authenticate the devices.

III. System Model

Figure **??** describes a scenario of the system model with the IoT devices connected to the internet through the border router element. Each node tries to authenticate to a server or with another node. Each IoT device is equipped with a PUF and capable of performing multiplication and hash operations. The IoT devices communicate the information to a server. The server can also perform some multiplication and hash computations.

A. Assumptions

In this thesis work, we make the following assumptions regarding the system:

1) An IoT device consists of an embedded system equipped with a PUF. Any attempt to separate PUF from the embedded system by physical tampering will destroy it.
2) The IoT device micro-controller and the PUF are a system on-chip with secure communication.
3) The server is the trusted party with no limitation of resources. However, IoT devices have resource-constrained.

B. Attack Model

IoT devices transmit data to the central server using the standard or compressed TCP/IP protocol suite (e.g., 6LoWPAN). The packets follow various paths and pass through multiple transmission links. The adversary may negotiate with one or more network entities to gain access to an IoT device. The adversary can also monitor, insert packets, simulate other devices, start a session, and replay older messages to gain authentication into IoT devices without getting detected to launch various attacks to cause physical or economic damage.

IV. Proposed Authentication Protocol

Here, we propose a PUF based authentication scheme for the authentication of two IoT nodes using a server node. In the proposed scheme, the server performs the authentication of both IoT nodes. The proposed scheme contains two IoT devices $node_1$ and $node_2$ and a server S. This authentication protocol has two phases. The first phase is called the enrollment phase, and the second phase is the authentication phase.
Enrollment Phase: In the enrollment phase, each device is

enrolled at the server. The server sends a random challenge to the IoT devices, and the IoT devices use this challenge as input to the PUF and generate the PUF response for this particular challenge. Further, the device sends back this response to the server. The server stores this challenge-response pair for each device and uses it further in the authentication phase.

Authentication Phase In this phase, the two IoT devices are authenticated by a server. In, this phase when a node $node_1$ initiates the authentication process, it sends its identification id_1 to the identification of $node_2$, id_2 and a nonce n_1, time stamp TS and computes $H(r_1, TS, n_1)$ and sends the following to the server.

$$id_1, id_2, n_1, TS, H(r_1, TS, n_1) \tag{1}$$

Then the server searches in its database for the $node_1$ entry and verifies $H(r_1, TS, n_1)$. If the verification is successful, it continues the authentication process; otherwise, it stops. Now the server generates random nonce n_s and a random number P, which is a base point on an elliptic curve. Further, the server calculates the following:

$$\alpha = r_2.n_s.P \tag{2}$$

$$\beta = r_1.n_s.P \tag{3}$$

$$H(r_1||\alpha||n_1) \tag{4}$$

$$H(r_2||\beta||n_1||id_1||TS') \tag{5}$$

Now server sends $H(r_1||\alpha||n_1), c_1, \alpha$ to the $node_1$ and $H(r_2||\beta||n_1||id_1||TS'), c_2, \beta, n_1, id_1, TS'$ to $node_2$, where TS' is TS+Δ. Now the $node_1$ generates r_1 using challenge c_1 and PUF module. Further, $node_1$ calculates $H(r_1||\alpha||n_1)$ and verifies the received hash value with the computed hash value. Then, the $node_1$ computes the following:

$$\gamma = \alpha.r1 \tag{6}$$

$$k1 = H(\gamma|id1||id2||n1) \tag{7}$$

Furthermore, $node_1$ encrypt the $(id_1, id_2, n1)$ with key k_1 and send $E_{k1}(id_1, id_2, n1)$ to server. Similarly, the $node_2$ generates r_2 using challenge c_2 and PUF module. Further, $node_2$ calculates $H(r_2||\beta||n_1||id_1TS')$ and verifies the received hash value with the computed hash value. Then, the $node_2$ computes the following:

$$\delta = \beta.r2 \tag{8}$$

$$k2 = H(\delta|id1||id2||n1) \tag{9}$$

Furthermore, $node_2$ encrypt the $id_1, id_2, n1$ with key k_2 and send $E_{k2}(id_1, id_2, n1)$ to server. The server decrypts the received messages using key k= k_1 = k_2 and authenticates both the nodes $node_1$ and $node_2$.

V. Security Evaluation

The security proof of the proposed authentication protocol is discussed here. Generally, the authentication protocol is secure if the identity id_1 and id_2 are unique and an adversary can not able to guess the identity id_1 and id_2 for the challenge c_1, c_2, and TS chosen randomly. It can be formulated by providing an adversary with c_1 and c_2 and TS' and check whether the adversary can successfully guess the identity for the given challenges. To prove the security of the proposed protocol, it has to be shown that breaking the protocol is as difficult as solving the 2-Decisional Uniqueness Problem. The 2-Decisional Uniqueness Problem assumption is that the probability with which an adversary guesses the bit correctly, that is, $t = t'$, is more than 1/2 by only a negligible quantity. In other words, if the proposed protocol is breakable, then the 2-Uniqueness Problem has a solution. To prove this, we present an experiment. Let the adversary is $\mathbf{Atk}$, which is probabilistic and polynomial time, and the PUF response bit size be n. Now, the experiment is as under:

The Eavesdropping Authentication Experiment $Auth_{\mathbf{Atk},\upsilon}$(n,$\phi$, $PUF_{\mathbf{Atk}}, id_1, id2_2$):

1) The adversary $\mathbf{Atk}$ is provided:
   a) ϕ= $\langle c_1, c_2, TS' \rangle$ where TS' = (PUF(c_1)) $\bigoplus$ TS),
   b) A PUF instance $PUF_{\mathbf{Atk}}$, and
   c) Two identities id_1 and id_2, which are calculated as follows: a random bit tϵ 0, 1 is chosen and the following has been calculated: id_t = H1(PUF(c_1)||TS)
2) The adversary $\mathbf{Atk}$ will output a value t'.

If the adversary $\mathbf{Atk}$ successfully distinguishes between the "correct" and the random identity, then she or he succeeds in the experiment. Further, the proof of the theorem is given below.

THEOREM 1: The authentication protocol υ is secure in the presence of eavesdroppers if the 2-Decisional Uniqueness Problem Assumption is true.

PROOF: To justify the security of the protocol υ, it has to be shown that the adversary gets success in the experiment $Auth_{\mathbf{Atk},\upsilon}$ with a probability negligibly greater than 1/2. So, there exists a negligible function negl($\cdot$) such that $Pr[Auth_{\mathbf{Atk},\upsilon} = 1] \leq 1/2 + negl(n)$
for every probabilistic polynomial-time adversary $\mathbf{Atk}$.

Assuming the adversary $\mathbf{Atk}$ has some non-negligible advantage θ in breaking the protocol υ. An algorithm η can be constructed having an advantage θ in breaking the 2-Uniqueness problem. Further, the algorithm η takes a random 2-Uniqueness Problem tuple as input $(c_1, c_2, PUF_{\mathbf{Atk}}, m_1, m_2)$, (where m_1 = PUF(c_1) and m_2 = PUF(c_2) or two random string belongs to $0, 1^*$) and proceeds as follows:

1) SetUp: Provide $\mathbf{Atk}$ with $PUF_{\mathbf{Atk}}$.
2) Input Tuple:
   a) Initially, it chooses the TS.
   b) Then, it calculates TS' = $(m_1||m_2,)$ $\bigoplus TS$

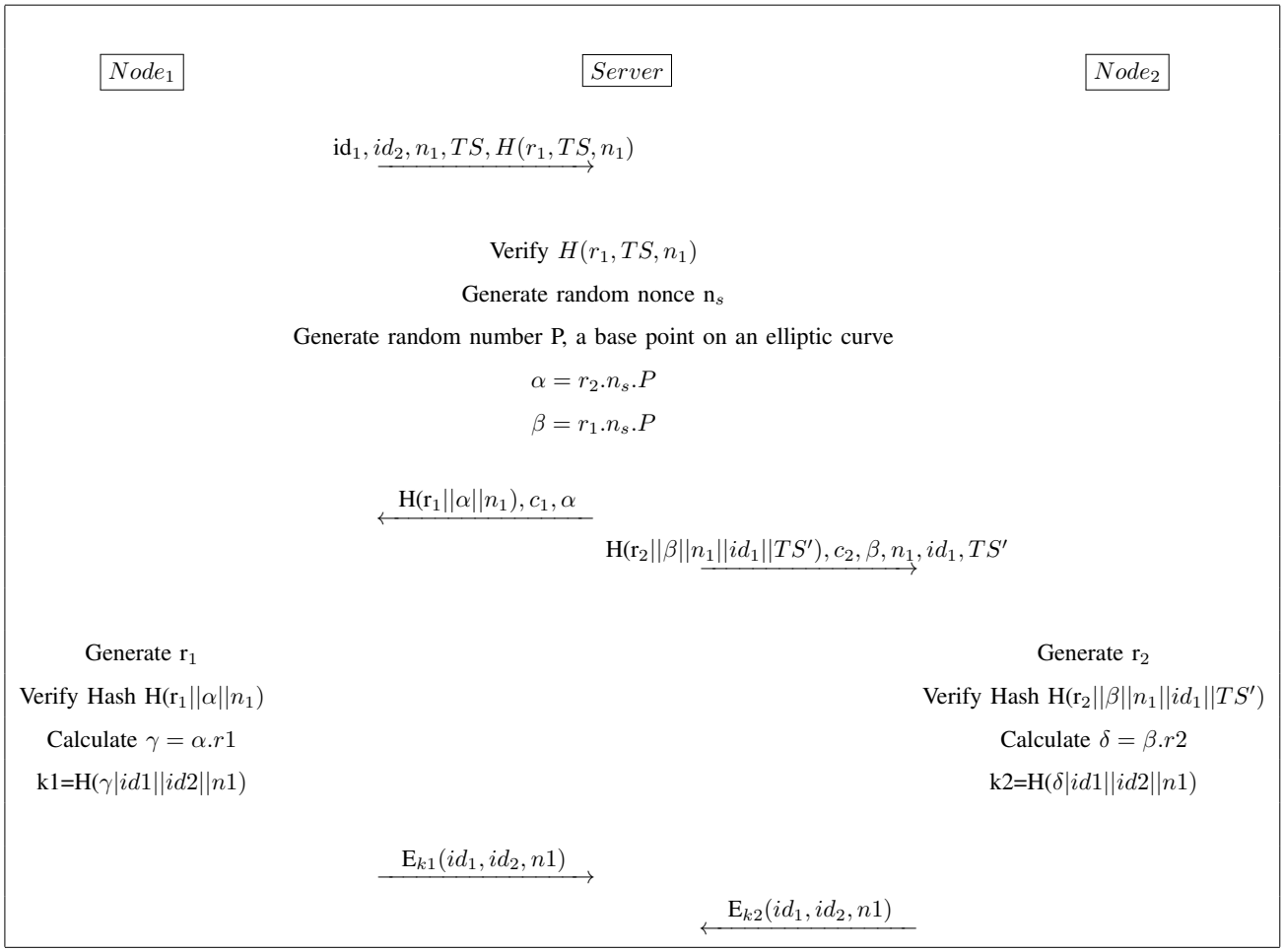

Fig. 1: Authentication and Key Exchange protocol

c) Then it sets $\phi = \langle c_1, c_2, TS' \rangle$, which is perfectly random to the adversary $\mathbf{Atk}$.
d) Now, it randomly chooses t ϵ 0,1
e) Then it calculates id_t = H1(PUF(m_1)||TS)
f) Now the η provides $\mathbf{Atk}$ the tuple ϕ, id_1, id_2. Now, if (m_1 = PUF(c_1) and m_2 = PUF(c_2), then id_t will be equal to H1(PUF(c_1)||TS), and it will be a valid input tuple. Otherwise, id_1, id_2 will be some random element of G_1^*.

3) Guess: The adversary $\mathbf{Atk}$ returns t', a guess of t. If $t = t'$, then the algorithm η returns 1, implying that m_1, m_2 are the correct responses of c_1,c_2. Otherwise, it returns 0. Hence, it is proved that the adversary $\mathbf{Atk}$ has the same advantage θ as the η. But, due to the hardness 2-Uniqueness Problem, θ should be negligible. Hence, $Pr[Auth_{\mathbf{Atk},\upsilon} = 1] \leq 1/2 + negl(n)$

Since the nodes locally calculate its key k_1 and communicate it to the server. Considering the complexity of the Computational Discrete Log Problem, the probability that the adversary $\mathbf{Atk}$ can retrieve the value of response r_1 from k_1 is negligible. Hence, the adversary $\mathbf{Atk}$ fails to guess the exact value of the key k_1.

A. Formal Security Verification

The proposed PUF-based authentication protocol is validated through the existing AVISPA tool [14].

The agents' roles in the proposed scheme are specified in the HLPSL language. Further, we defined the security goals for the proposed scheme. We performed the security analysis using the AVISPA and verified that the proposed scheme is safe, provides mutual authentication, and can authenticate nodes. The role of the first node is presented in Figure 2, the role of the second node is presented in Figure 3, and the role of the server is presented in Figure in 4. The results shown in Figure 5 indicate that the proposed scheme is safe and achieves the security goals.

The proposed protocol achieves the following security goals:

1) **Integrity:** Every step of the protocol computes the hash of the messages since every message contains a hash, which can be used to verify the integrity of the message.

```
role role_A(A:agent,B:agent,C:agent,SND,RCV:channel(dy))
played_by A
def=
local
State:nat,
H:hash_func,
Id1,Id2,N1,R1,TS,HAB,HBA,Non:text

init State := 0
transition
1.    State=0 /\ RCV(start) =|> State':=1 /\ Id1':=new()/\ Id2':=new()
/\ N1':=new()/\R1':=new()/\ TS':=new() /\ G':=new() /\ HAB':=H(R1'.TS'.N1')/\SND(R1'.Id1'.Id2'.N1'.TS'.HAB')
2. State =1 /\ RCV(HBA'.Non') =|> State':=2 /\request(A,B,a_b_hba,HBA')/\ witness(B,A,a_b_hba,HBA')
/\ KAB':=H(G.Id1.Id2.N1)  /\ SND({Id1.Id2.N1_KAB'})

end role
```

Fig. 2: Role of node A

```
role role_C(C:agent,B:agent,A:agent,SND,RCV:channel(dy))
played_by
C def=
local
State:nat,
H:hash_func,
Id1,Id2,N1,HAB,HBA,HBC,Non,Bon,TS2,R2:text
init
State := 0
transition
1.    State=0 /\ RCV(HBC'.Bon'.N1',Id1',TS2'.R2)=|> State':=1
/\request(C,B,c_b_hbc,HBC')/\ witness(B,C,c_b_hbc,HBC') /\ D' :=new()
/\ KBC':=H(D.Id1.Id2.N1) /\ SND({Id1.Id2.N1_KBC'})
end role
```

Fig. 3: Role of node C

In AVISPA, the roles of all three participants (two nodes and a server) are defined. Each participant sends the message hash value, and the recipient of the message verifies the hash value. So, the integrity is verified by the AVISPA tool.

2) **Authentication of Node:** The nodes are authenticated if the encrypted messages received by the server from both nodes can be decrypted by the server using the key k = $k1$=$k2$. Since the server could be able to generate a key k which is equal to $k1$=$k2$. In AVISPA, we define two goals for the nodes authentication, and the result shown in Figure 5 displays safe, which means the goals defined for the authentication are achieved; otherwise, the result would display unsafe.
3) **Authentication of Server:** The server is authenticated by the nodes from the message received by the server. The first message sent by the server to $node_1$ contains the hash of r_1. Due to the symmetry of the protocol, the same reasoning holds for Node 2. In AVISPA, we define two goals for server authentication, one for each node. The result shown in Figure 5 displays safe, which means the goals defined for the authentication are achieved; otherwise, the result would display unsafe.

VI. Performance Analysis

Here, we provide the proposed authentication protocol's performance based on performance measurement parameters like computational cost and storage requirement.

```
role role_B(B:agent,A:agent,C:agent,SND,RCV:channel(dy))
played_by B
def= local
State:nat,
H:hash_func,
R1,Id1,Id2,N1,TS,HAB,HBA,HBC,Non,Bon,TS2,R2:text
init
State := 0
transition
1.    State=0 /\ RCV(R1'.Id1'.Id2'.N1'.TS'.HAB) =|>
State':=1 /\Non':=new()/\Bon':=new()  /\ D':=new() /\TS2':=new()/\R2':=new()
          /\ G':=new()    /\HBA':=H(R1'.Non'.N1')/\SND(HBA'.Non')
               /\HBC':=H(R2'.Bon'.N1'.Id1',TS2)/\SND(HBC'.Bon'.N1',Id1',TS2'.R2')
          /\ KAB':=H(G.Id1.Id2.N1)  /\ KBC':=H(D.Id1.Id2.N1)
          /\RCV({Id1.Id2.N1}_KAB) /\RCV({Id1.Id2.N1}_KBC)
          /\request(B,A,b_A_kab,KAB')/\ witness(A,B,b_a_kab,KAB')
          /\request(B,C,b_c_kbc,KBC')/\ witness(C,B,b_c_kbc,KBC')
end role
```

Fig. 4: Role of Server B

```
% OFMC%
Version of 2006/02/13
SUMMARY
   SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL       /home/span/span/testsuite/results/pufauthentication2.if
GOAL
    as_specified
BACKEND
   OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.04s
visitedNodes: 8 nodes
depth: 3 plies
```

Fig. 5: Security verification result for the OFMC back-end

A. Computational Analysis

TABLE I: Computational Cost Comparison

Scheme	No. of Operations (IoT Devices)	Time (ms)
proposed Scheme	5 Hash +2 ENC +2 MUL	0.0325
[15]	8 Hash +4 MUL	0.0388
[16]	10 Hash + 4 MUL	0.0398
[17]	8 Hash + 6 ENC	0.0418

We have calculated the computational cost on the basis of a number of operations performed at the two IoT nodes and one server. The number of hash, encryption/decryption (ENC), and point multiplication (MUL) operations are measured for the proposed authentication protocol. These values can be directly obtained by counting the frequency of the corresponding operations. Our proposed authentication protocol involves five hash operations, two encryption, and two multiplication operations in IoT devices. The time required for one hash operation, one encryption, and one point multiplication is 0.0005 ms, 0.0063 ms, and 0.0087 ms, respectively. So the total time required for the proposed scheme is 0.0325 ms to complete these operations.

B. Storage Requirement

We have proposed an effective protocol in terms of memory usage. id_1,id_2,n_1 and c_1 are only cached and further erased during authentication. Further, only one CRP pair (c_i, r_i) and the respective id_i are kept for every node. On the other hand, most of the existing literature protocols require the following conditions storing secret information and the server storing a huge number of CRPs for each IoT device. One of the CRPs is used each time for authenticating an IoT device with the server. However, these protocols are not scalable with a large number of IoT devices. The proposed mutual authentication protocol does not impose these requirements and has meager storage requirements.

C. Discussion

This paper presents a physical unclonable function (PUF) based secure authentication protocol for IoT devices. The proposed protocol accomplishes the required efficiency and security using a PUF. This scheme authenticates the IoT nodes with the help of a server node. The proposed protocol can also be used to exchange the key between the two IoT nodes. We compared the proposed protocol with some existing PUF-based authentication protocols as presented in [15]–[17], and the comparison is shown in Table I. The protocol discussed in [15] computes 8 hash and 4 multiplications. So, this scheme has three more hash operations than the proposed scheme. Also, it has no encryption or decryption operation and two more point multiplication operations compared to the proposed scheme. The total computation time taken in this scheme is 0.0388 ms. The protocol presented in [16] has 10 hash operations, five more than the proposed scheme, and four multiplication operations, which are also more than the proposed authentication protocol. The total computation time taken in this scheme is 0.0398 ms. The scheme presented in [17] has 8 hash functions and 6 encryption functions, which are more than the proposed scheme. The total computation time taken in this scheme is 0.0418 ms. So, the proposed scheme is more efficient in computation time than some existing schemes.

VII. Conclusion

This work presented a lightweight authentication protocol for an IoT system. The authentication mechanism is based on a challenge-response mechanism using PUFs. A session key is also established using the proposed protocol. No device is required to store a secret in memory, so difficult for an attacker to extract the secret from the device or clone the device. The analysis of the performance of the proposed protocol shows that it is secure and requires lesser computation.

References

[1] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of iot systems: Design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2014, pp. 417–423.

[2] V. Shivraj, M. Rajan, M. Singh, and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for internet of things (iot)," in *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*. IEEE, 2015, pp. 1–6.

[3] P. N. Mahalle, N. R. Prasad, and R. Prasad, "Threshold cryptography-based group authentication (tcga) scheme for the internet of things (iot)," in *2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*. IEEE, 2014, pp. 1–5.

[4] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in iot systems using physical unclonable functions," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1327–1340, 2017.

[5] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 9–14.

[6] P. Tuyls and L. Batina, "Rfid-tags for anti-counterfeiting," in *Cryptographers' Track at the RSA Conference*. Springer, 2006, pp. 115–131.

[7] P. F. Cortese, F. Gemmiti, B. Palazzi, M. Pizzonia, and M. Rimondini, "Efficient and practical authentication of puf-based rfid tags in supply chains," in *2010 IEEE International Conference on RFID-Technology and Applications*. IEEE, 2010, pp. 182–188.

[8] G. Hammouri, E. Öztürk, and B. Sunar, "A tamper-proof and lightweight authentication scheme," *Pervasive and mobile computing*, vol. 4, no. 6, pp. 807–818, 2008.

[9] Y. S. Lee, H. J. Lee, and E. Alasaarela, "Mutual authentication in wireless body sensor networks (wbsn) based on physical unclonable function (puf)," in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2013, pp. 1314–1318.

[10] K. B. Frikken, M. Blanton, and M. J. Atallah, "Robust authentication using physically unclonable functions," in *International Conference on Information Security*. Springer, 2009, pp. 262–277.

[11] M. Barbareschi, P. Bagnasco, and A. Mazzeo, "Authenticating iot devices with physically unclonable functions models," in *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*. IEEE, 2015, pp. 563–567.

[12] Y. Yilmaz, S. R. Gunn, and B. Halak, "Lightweight puf-based authentication protocol for iot devices," in *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*. IEEE, 2018, pp. 38–43.

[13] D. Naveen and K. Praveen, "Puf authentication using visual secret sharing scheme," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. IEEE, 2019, pp. 472–475.

[14] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani *et al.*, "The avispa tool for the automated validation of internet security protocols and applications," in *International conference on computer aided verification*. Springer, 2005, pp. 281–285.

[15] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A puf-based secure communication protocol for iot," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 3, pp. 1–25, 2017.

[16] A. Braeken, "Puf based authentication protocol for iot," *Symmetry*, vol. 10, no. 8, p. 352, 2018.

[17] R. De Smet, T. Vandervelden, K. Steenhaut, and A. Braeken, "Lightweight puf based authentication scheme for fog architecture," *Wireless Networks*, vol. 27, no. 2, pp. 947–959, 2021.