Optimizing Trust-Centric Authentication in Matter-enabled IoT Devices with PUF and PKI

Chandranshu Gupta
Computer Science and Engineering
IIT Jammu
Jammu, India
chandranshu.gupta@iitjammu.ac.in

Gaurav Varshney
Computer Science and Engineering
IIT Jammu
Jammu, India
gaurav.varshney@iitjammu.ac.in

***Abstract*—The Internet of Things (IoT) ecosystem is rapidly expanding, connecting resource-constrained devices that require lightweight and efficient security mechanisms. The *Matter protocol* standardizes secure communication in smart homes, relying on X.509 certificates for device authentication. While effective, the management of these certificates—including creation, storage, distribution, and revocation—is cumbersome and resource-intensive for IoT devices. Additionally, Matter's reliance on private key storage increases vulnerability to key compromise. This paper proposes an improved lightweight authentication protocol combining Physical Unclonable Functions (PUFs) and Public Key Infrastructure (PKI) tailored for Matter-compliant IoT devices. By dynamically generating device-unique keys during operation, PUFs eliminate the need to store private keys, mitigating key extraction threats. The protocol reduces certificate storage overhead and simplifies the pairing process. Performance evaluations demonstrate significant reductions in computational overhead while maintaining robust security. By addressing Matter-specific challenges, the proposed approach optimizes device authentication, supports Perfect Forward Secrecy (PFS), and is well-suited for large-scale IoT deployments.**

I. Introduction

The Internet of Things (IoT) represents a groundbreaking technology that has turned conventional appliances and everyday items into intelligent devices capable of network communication [1]. However, the existence of different proprietary protocols and standards has led to a fragmented ecosystem, limiting compatibility across devices from diverse manufacturers and inhibiting the development of a seamless and cohesive smart home environment [2]. Therefore to address the above mentioned issue, the Connectivity Standards Alliance (CSA-IoT) developed Matter, an open-source, royalty-free connection framework for smart homes [2]. Standardizing communication amongst smart home devices is its main objective in order to increase interoperability across various platforms and ecosystems. By establishing a common networking standard, Matter, backed by industry titans like Apple, Google, Amazon, and the Zigbee Alliance, streamlines the development of IoT devices. Regardless of the manufacturer or brand, the standard guarantees safe, reliable, and simple interactions between devices [3]. Every Matter device that joins the network must be authenticated, and all communications are secured using strong, high-entropy cryptographic techniques. Furthermore, all approved devices must offer secure Over-the-Air Device Firmware Updates according to Matter [4].

Matter makes use of proven secure communication frameworks, such as certificate-based authenticated session setup and Public Key Infrastructure (PKI) [5]. By protecting the secrecy and integrity of device-to-device communication, these technologies guarantee secure device authentication [6]. During the Authentication process all Matter devices must display a Device Attestation Certificate (DAC), which is produced by the Product Attestation Intermediate (PAI), under the manufacturer's authority. PAI itself is certified by the Product Attestation Authority (PAA), thereby establishing the PAA as the foundation of system confidence. The CSA, which oversees the Matter protocol, manages the Distributed Compliance Ledger (DCL), a blockchain-based database that Matter utilizes to keep track of a list of reliable PAAs. The commissioner receives the device's DAC containing the product and vendor Id's of the devices during the commissioning process and verifies that the root certificate (PAA) is present in the DCL [7], [8].

Although Matter envisions a future where IoT devices from various manufacturers integrate seamlessly within a smart home ecosystem, the increased connectivity inevitably broadens the attack surface, exposing devices to potential security threats [6]. Furthermore, the authentication process, which relies on certificate-based PKI mechanisms, poses significant challenges for resource-constrained IoT devices due to the computational, management and storage overhead it demands [9]. Additionally, the current implementation does not offer Perfect Forward Secrecy (PFS), meaning that if a device's private key is compromised, past communications may also be at risk. These limitations highlight the need for more efficient and secure authentication methods to address the unique constraints of IoT environments.

A highly effective and resilient security feature for safeguarding IoT devices is the Physically Unclonable Function (PUF). Based on digital logic and integrated circuits (ICs),

Workshop on Security and Privacy in Standardized IoT (SDIoTSec) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-6-6
https://dx.doi.org/10.14722/sdiotsec.2025.23044
www.ndss-symposium.org

PUFs are recognized as a promising solution for enhancing hardware security [10]. PUFs create a unique identifier tied to the chip, leveraging manufacturing variability to ensure both security and resistance to cloning. The authentication process using PUFs operates through Challenge-Response Pairs (CRPs). When a challenge is presented to a PUF, it generates a corresponding response bit. This challenge-response mapping is influenced by the inherent variations in the PUF's fabrication [11]. Due to their unique, unclonable nature and resistance to tampering, PUFs offer robust security by eliminating the need for key storage in the device's memory, making them an excellent choice for IoT device protection. Several efforts have explored PUF-based methods for unique device identification, authentication, and key exchange across various IoT domains, such as wireless sensor networks, smart healthcare, vehicular technology, and drone networks [11], [12]. However, these approaches often fall short in security and do not address the integration of PKI with PUF to establish trust and enable authentication without relying on certificates. Since trust is essential for hardware security and devices must include all necessary protections against potential theft, this paper introduces an enhanced and highly secure PUF-based PKI authentication protocol for IoT devices. This protocol builds on traditional PKI concepts but eliminates the resource-intensive tasks of certificate generation, distribution, and revocation, making it suitable for resource-constrained IoT environments.

II. Background

This section delves into the device commissioning process within the Matter protocol, highlighting the associated security challenges and the inherent limitations of its authentication mechanism.

A. Key Steps in the Matter Device Commissioning Process

The commissioning process in the Matter protocol ensures the secure onboarding of IoT devices into a Matter fabric [4]. Below are the primary steps involved:

1) **Initiation:** The commissioner (e.g., mobile app or hub) starts the onboarding process. Device discovery is conducted via IP (if networked) or Bluetooth Low Energy (BLE) for offline devices.
2) **Setup Code Entry and Discovery:**
The onboarding payload, containing a unique setup code, identifies the device. The payload is provided through QR codes, NFC tags, or manual entry. The device broadcasts its identity, enabling discovery by the commissioner.
3) **Secure Session Establishment:**
The Password Authenticated Session Establishment (PASE) protocol establishes a secure session. Encryption keys are derived from the setup code to secure further communication.
4) **Device Attestation:**
The commissioner retrieves and verifies the DAC from the device. Verification is performed against the DCL to ensure authenticity.
5) **Operational Configuration:**
The commissioner installs the signed Node Operational Certificate (NOC) on the device. The NOC provides the device with a unique node identity within the Matter fabric.
6) **Network Commissioning:**
The device is provisioned with operational network credentials (e.g., Wi-Fi SSID and password). The device transitions from the commissioning network to the operational network.
7) **Post-Commissioning:**
The device is fully integrated into the fabric as a trusted node. Future communications within the fabric are secured using the Certificate Authenticated Session Establishment (CASE) protocol.

B. Limitations and Vulnerability in the existing Device Comissioning and Authentication process

The Matter protocol employs a dual PKI system to ensure security. The first PKI is used during device commissioning to authenticate the device as a certified Matter device by verifying its DAC. The second PKI is used to issue the NOC to end devices by a common comissioner, enabling mutual authentication and secure communication within the Matter fabric/network. While this dual PKI approach enhances security, it introduces significant computational overhead, which can be burdensome for resource-constrained IoT devices [13]. Additionally, the distribution, storage, and revocation of digital certificates in IoT devices is a resource-intensive task since these devices are resource-constrained [13]. Another notable limitation is that the commissioner/controller is not required to authenticate itself to the device. This lack of mutual authentication can allow a malicious controller to onboard non-certified matter devices, undermining the trust and security of the Matter fabric [6]. These challenges highlight areas requiring optimization for device authentication in the matter protocol.

III. Proposed Method

This paper introduces an efficient mutual authentication and key exchange protocol optimized for matter based IoT devices. Unlike conventional PKI systems, our proposed method eliminates several resource-heavy operations, including the creation, verification, storage and revocation of digital certificates. Typically, trust in PKI systems is established through a Certificate Authority (CA), which distributes digital certificates containing public keys to verify the identities of communicating parties. While highly secure and widely accepted in traditional computing systems, this approach can be too demanding for IoT environments, which often face constraints related to power consumption, processing time, and memory capacity. To address these limitations, our solution optimizes the trust model by introducing a system that relies on three main actors: the CA, the manufacturers, and the IoT devices themselves. Rather than employing digital certificates, our protocol makes use of PUFs for authentication. The system

utilizes CRPs generated by PUFs to offer a secure and unique method for device identification and authentication. A detailed architectural representation of the model is provided in Figure 1. Our System model consists of three entities as described below:

Certificate Authority (CA): The CA is a robust, secure entity with substantial storage capacity. It maintains a database of CRPs for each IoT device. This database is crucial for authenticating devices during communication. The CA ensures the integrity of the CRP data, facilitating reliable device identification and authentication.

Original Equipment Manufacturer (OEM): Manufacturers are responsible for producing IoT devices and conducting challenge-response interactions with them in a secure environment during the enrollment phase. They also establish a trust relationship with the CA using traditional TLS due to their computational and storage capabilities. Manufacturers forward each device's CRP to the CA and distribute the CA's public key to all IoT devices during enrollment.

IoT Devices: These are the end devices, ranging from temperature sensors to door locks. IoT devices are characterized by limited computational resources, storage capacity, and battery power. They rely on PUFs for secure authentication and key generation, leveraging the CA's public key distributed by the manufacturers.

A. Enrollment Phase

During the Enrollment phase, the OEM interacts with the manufactured IoT devices in a secure environment. The OEM sends a challenge to each IoT device, which then applies this challenge to its PUF to generate a CRP. This CRP is securely transmitted to the CA by the OEM via a TLS channel. Each OEM is responsible for sending the CRP of every IoT device it has manufactured to the CA. The CA stores these CRPs in its database, along with the corresponding IoT device IDs. Additionally, the OEM must send the CA's public key to each IoT device during this phase, which is then stored within the IoT device for future use.

B. Authentication and Key Exchange Phase

During the authentication phase, IoT devices that wish to communicate must first authenticate themselves as shown in Figure 1. The steps are as follows:

1) IoT device A or the Commissioner, desiring to communicate or register IoT device B to the fabric, sends the IDs of both devices, ID_A and ID_B, as well as the public keys of both devices, Pub_A and Pub_B.
2) The CA verifies the message's origin by fetching the stored challenge, Ch_A, for IoT device A from its database. The CA then sends this challenge to IoT device A. Both IoT device A and the CA derive the shared secret S_{AC} using the public keys.
3) Upon receiving the challenge, Ch_A, IoT device A applies it to its PUF to generate the corresponding response, $R_A = \text{PUF}_A(Ch_A)$. Device A then XORs Ch_A with R_A to create a new challenge, $Ch_A^{'} = Ch_A \oplus R_A$. Device A applies this new challenge to its PUF to generate a new response, $R_A^{'} = \text{PUF}_A(Ch_A^{'})$. Device A XORs R_A with its public key, resulting in $M_A = R_A \oplus Pub_A$ and sends this and the new response both encrypted with the shared secret, to the CA.
4) The CA verifies the authenticity of device A by fetching the stored response, R_A^{stored}, from its database and comparing it with the received response, R_A. If they match, the CA proceeds with the next steps. The CA also stores the new response $R_A^{'}$ in its database along with the corresponding challenge $Ch_A^{'} = Ch_A \oplus R_A$. The CA then sends A's public key and the challenge Ch_B fetched from its database, to device B. The CA also includes a hashed message of this data along with R_B to ensure integrity.
5) Upon receiving the messages from the CA, IoT device B applies the challenge Ch_B to its PUF, generating the response $R_B = \text{PUF}_B(Ch_B)$. Also, the received hashed message is recalculated to verify the integrity of the message. Device B then XORs Ch_B with R_B to create a new challenge, $Ch_B^{'} = Ch_B \oplus R_B$. Device B applies this new challenge to its PUF to generate a new response, $R_B^{'} = \text{PUF}_B(Ch_B^{'})$. Device B then XORs R_B with its public key, resulting in $M_A = R_B \oplus Pub_B$ and sends this and the new response both encrypted with the shared secret, to the CA.
6) The CA verifies the authenticity of device B by comparing the stored response, R_B^{stored}, with the received response, R_B. If they match, the CA sends the public key of B to A along with the hashed message of this data to ensure integrity. The CA also stores the new response $R_B^{'}$ in its database along with the corresponding challenge $Ch_B^{'} = Ch_B \oplus R_B$.
7) Device A, after receiving the public key of Device B and verifying the integrity of the message, generates a nonce, N_A, encrypts it with the shared secret S_{AB} that it derives using public key of B, and sends it to B.
8) Device B receives the nonce, N_A, generates its own nonce, N_B, concatenates it with N_A, and sends the concatenated nonce encrypted with the shared secret S_{BA} that it derives using public key of A.
9) Both devices use the Hash of concatenation of the nonces, $N_A \| N_B$, as the session key for secure communication.

This marks the end of Authentication and Key exchange phase. Whenever new session is to be established, then the same procedure will be followed but the new Challenges will be sent encrypted.

C. Key Management and Revocation

Although our scheme does not utilize traditional digital certificates, it addresses key management and revocation issues. In the event that the long-term key of the CA is compromised, the OEM will facilitate the IoT devices by distributing the new public key of the CA through firmware updates. This approach

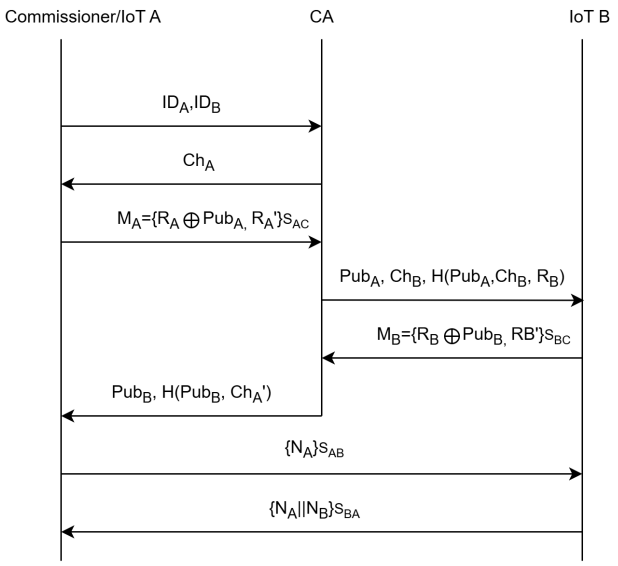

Fig. 1. Authentication and Key exchange

ensures continued secure communication and mitigates the risks associated with key compromise.

IV. Experimentation and Results

The testbed for the execution of the experiment includes two IoT devices and two local servers, one working as a CA and the other as the original equipment manufacturer. To evaluate the effectiveness of our proposed PUF-based PKI scheme for IoT environments, we ran experiments using a local server setup. Our experimental setup included the following components:

IoT Devices: We utilized two Raspberry Pi 3 Model B devices as the IoT devices in our proposed scheme. The PUF used is arbiter PUF. We also simulated the PUF behavior using the PyPuf library, which models the XOR Arbiter PUF.

OEM Server: A local machine simulated the OEM server. The OEM was responsible for initial interaction with IoT devices, generating and transmitting CRPs to the CA, and forwarding the CA's public key to the IoT devices. The server ran on an Intel Core i7 processor with 16 GB of RAM and used Python for implementing TLS communication. The OEM server setup involved running an Apache HTTP server to handle HTTP requests and a MySQL database to store CRPs and manage IoT device information.

CA Server: Another local machine simulated the CA server. The CA was responsible for storing CRPs, managing public keys, and facilitating authentication and key exchange between IoT devices. This server was also equipped with an Intel Core i7 processor with 16 GB of RAM and used Python along with OpenSSL for secure communication and cryptographic operations. The CA server setup involved running an Apache HTTP server to handle HTTP requests and a MySQL database to store CRPs and public keys.

Performance Evaluation: Now, we assess the performance of our proposed protocol in comparison with matter prtocol and the existing state-of-the-art schemes, specifically those utilizing either certificate-based or certificateless PKI approaches for IoT device authentication. Table I presents a performance comparison between our protocol and other contemporary schemes. Our evaluation focuses on the authentication and key exchange phases, emphasizing the computational cost incurred by the IoT devices when they are directly communicating, with each other. Specifically, we have accounted for the cost of cryptographic operations such as Elliptic Curve Point Multiplication (ECPM) and Hash performed by the IoT devices during these phases. The comparative analysis reveals that our proposed protocol demonstrates superior efficiency relative to the alternative schemes. In our scheme even if the initial phase with the CA is included for computation cost, the total ECPM operations increases to 4 which remains lower than other protocols. By contrast, in Matter we have excluded phases like PASE and device attestation verification, and including these would significantly increase its computation costs, making it far less efficient. Moreover, our scheme significantly reduces storage costs compared to the Matter protocol by eliminating the need to store X.509 certificates on IoT devices.

TABLE I
Performance Comparison of Our Protocol Against State-of-the-Art Approaches

Protocol	ECPM	Hash Operations
[14]	6	6
[15]	6	4
Matter Protocol [5]	12	6
Proposed Scheme	2	3

V. Conclusion and Future Work

In this paper, we introduced a optimized mutual authentication and key exchange protocol designed for resource-constrained matter certified IoT devices. Our approach utilizes PUFs and CRPs to establish trust and manage keys without the need for traditional digital certificates. By circumventing the complexities and overhead associated with conventional PKI systems, our protocol significantly enhances computational efficiency and reduces resource consumption. Performance evaluation shows that our protocol requires fewer ECPM operations and Hash Operations, outperforming existing schemes in terms of computational efficiency. Additionally, our method incorporates firmware-based updates to address potential compromises of the CA long-term key, ensuring continued security. This lightweight, low-power approach is well-suited for large-scale IoT environments. Future research will focus on several key areas to enhance our protocol further. We plan to test different PUFs under various environmental conditions to determine the most effective PUF for diverse scenarios. Additionally, we will work on optimizing the firmware update mechanism to improve the efficiency and reliability of key distribution and updates. Exploring these aspects will help refine our protocol and ensure its robustness across a broad range of IoT applications.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] W. Li, T. Yigitcanlar, I. Erol, and A. Liu, "Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework," *Energy Research & Social Science*, vol. 80, p. 102211, 2021.

[3] S. Liao, J. Yan, and L. Cheng, "Wip: Hidden hub eavesdropping attack in matter-enabled smart home systems," in *Workshop on Security and Privacy in Standardized IoT (SDIoTSec)*, 2024.

[4] Infineon Technologies AG, "Can Matter finally crack the smart home?" Infineon Technologies AG, Tech. Rep., June 2022, accessed on 01/12/2024.

[5] "Matter: The Foundation for Connected Things," https://csa-iot.org/all-solutions/matter/, accessed on 01/12/2024.

[6] K. Shashwat, F. Hahn, X. Ou, and A. Singhal, "Security analysis of trust on the controller in the matter protocol specification," in *2023 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2023, pp. 1–6.

[7] G. Jiacheng. (2022, February) Matter security model. Espressif. Accessed on 01/12/2024. [Online]. Available: https://blog.espressif.com/matter-security-model-37f806d3b0b2

[8] Connectivity Standards Alliance, "Matter Specification Version 1.0," Connectivity Standards Alliance, Tech. Rep., October 2022, (visited on 10/12/2024). [Online]. Available: https://csa-iot.org/developer-resource/specifications-download-request/

[9] U. Ali, M. Y. I. B. Idris, J. Frnda, M. N. B. Ayub, M. A. Khan, N. Khan, A. A. Jasim, I. Ullah, M. Babar *et al.*, "Enhanced lightweight and secure certificateless authentication scheme (elwscas) for internet of things environment," *Internet of Things*, vol. 24, p. 100923, 2023.

[10] B. Sen, "Puf: A new era in iot security," *CSI Transactions on ICT*, vol. 8, no. 2, pp. 185–191, 2020.

[11] M. H. Mahalat, D. Karmakar, A. Mondal, and B. Sen, "Puf based secure and lightweight authentication and key-sharing scheme for wireless sensor network," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 18, no. 1, pp. 1–23, 2021.

[12] T. Alladi, G. Bansal, V. Chamola, M. Guizani *et al.*, "Secauthuav: A novel authentication scheme for uav-ground station and uav-uav communication," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 068–15 077, 2020.

[13] M. El-Hajj and P. Beune, "Lightweight public key infrastructure for the internet of things: A systematic literature review," *Journal of Industrial Information Integration*, p. 100670, 2024.

[14] P. Tedeschi, S. Sciancalepore, A. Eliyan, and R. Di Pietro, "Like: Lightweight certificateless key agreement for secure iot communications," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 621–638, 2019.

[15] C. Gupta and G. Varshney, "An improved authentication scheme for ble devices with no i/o capabilities," *Computer Communications*, vol. 200, pp. 42–53, 2023.