National Conference on Advancements of Science, Technology, Engineering, and Management

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A PUF-based Lightweight and Secure Mutual Authentication System for Remote Keyless Entry Mechanisms

Rajath .K, Sahana S Hegde, Shreya .S, Swetha .M, Supriya Suresh

(Student, Student, Student, Student, Assistant Professor)

*(Dept of CSE, KS School of Engineering and Management, and Banglore

Rajathnaik3@gmail.com ,sahanahegde467@gmail.com ,shreyashivamurthy@gmail.com ,swethamurugesh1@gmail.com, supriyasuresh@kssem.edu.in)

****

Abstract:

The work aims to present a strong security approach of systems for Remote Keyless Entry (RKE) by introducing a lightweight a mutual authentication mechanism employing Physical Unclonable Functions (PUFs). RKE systems are susceptible to various threats like replay attacks and Roll Jam attacks, posing risks to vehicle security. By incorporating PUFs into the authentication process, this method seeks to address these vulnerabilities. Through comprehensive analysis, which includes security assessments and comparative evaluations of computational efficiency, this work is proposed. The work contributes to enhancing security measures within RKE systems, offering a dependable defense against evolving threats.

.

Keywords — **Mutual authentication, System for Remote Keyless Entry (RKE), Replay attack, RollJam attack, Physical Unclonable Function (PUF),SRAM PUF**

****

I. INTRODUCTION

This Keyless entry systems operated remotely are now commonly found in modern vehicles, offering convenience and ease of access. However, along with their convenience comes the risk of security vulnerabilities, which can compromise the safety of the vehicle. Attacks such as replay attacks and Roll Jam attacks have been shown to exploit weaknesses in RKE systems, highlighting he pressing requirement for improved security measures .When tackling these obstacles, this study suggests a novel approach to enhance the protection of RKE systems. The work focuses on implementing a lightweight mutual the system of authentication that leverages Physical Unclonable Functions (PUFs). PUFs offer unique physical characteristics inherent in each device, providing a robust foundation for authentication .By integrating PUFs into the authentication process, the method aims to fortify RKE systems in opposition to a range of potential attacks. Through the utilization of PUFs, is applied an additional layer of security that enhances the resilience of the confirmation process.

This paper presents a detailed exploration of the suggested solution, including its design, implementation, and evaluation. Physically Unclonable Functions (PUFs) are cryptographic primitives used for hardware authentication and security. PUFs exploit the inherent variations in physical properties of hardware components to generate unique identifiers or cryptographic keys. They are resistant to cloning and tampering, making them valuable in secure authentication systems and anti-counterfeiting measures. Ultimately, the research contributes to advancing the security measures within RKE systems, offering a reliable defense against emerging threats in the automotive

II. RELATED WORKS

A Secure and Lightweight PUF-Based Similar authentication Process over Remote Keyless Entry Systems**,** Rohini Poolat Parameswarath, and Biplab Sikdar

Department of Electrical and Computer Engineering at the College of Design and Engineering, National University of Singapore, located in Singapore. Contact: rohini.p@nus.edu.sg. Also, part of the Department of Electrical and Computer Engineering at the College of Design and Engineering, National University of Singapore, Singapore. Contact: bsikdar@nus.edu.sg

.In 2022, keyless ignition vehicles allow passengers to open the windows without using physical keys. RollJams can be launched by attackers with RKE structures that employ rolling codes rather than fixed codes. The proposed system is shown to be resistant to multiple common attacks by the researchers through a formal security analysis.[1]

Designing Physical Unclonable Functions for Key Generation in the AES Encryption Algorithm

Pallavi K, Bhoomika B, Thanmay M. Shetty, and Pramila B,*Associate Professor, ECE Department, East West Institute of Technology, Bengaluru, India, bjpramila@gmail.com Student, ECE Department, East West Institute of Technology, Bengaluru, India, tanmayamshetty@gmail.com Student, ECE Department, East West Institute of Technology, Bengaluru, India, bhoomikadevraj725@gmail.com Student, ECE Department, East West Institute of Technology, Bengaluru, India, pallavikpallu03@gmail.com*

Algorithms for cryptography that are frequently stored on hardware devices are vulnerable to hacking because the keys required for encryption or interpret data must be kept on hardware in addition to the design .This emphasises how essential it is to find a solution for the key storing problem. A physical function that cannot be replicated is proposed as a fix.[2]

A security solution using cryptography for Systems on Chip in IoT, leveraging Physical Unclonable Functions.

Alexandra Balan, Titus Balan1, Marcian Cirstea and Florin Sandu. *titus.balan@unitbv.ro Transilvania University of Brasov, Brașov, Romania*

A major security issue with IoT multiprocessor systems-on-chip (SoC) proved brought to light. This issue was the use of multicore processors and peripherals from different intellectual property fundamental sources as hardware parts. The writers talk about the idea of SoC protection and its advantages.[3]

Implementing timestamping and XOR logic as protective measures against replay attacks in remote keyless entry systems.

Kyle Greene, Deven Rodgers, Henry Dykhuizen, Quamar Niyaz, Khair Al Shamaileh, and Vijay Devabhaktu. *Bachelor of Science in Electrical Engineering earned at Purdue University Northwest in Indiana, USA. Bachelor of Science in Computer Engineering contact: hdykhuiz@pnw.edu. Both are affiliated with the Engineering Department at Purdue University Northwest, IN, USA. Contact qniyaz@pnw.edu for Electrical and Computer Engineering inquiries*.

By safeguarding authentication codes even when transmission between transmitters and receivers is impeded, this novel system improves security. This updated RKE system protects itself against popular attack vectors by timestamping and XOR encoding, guaranteeing resilience and robustness against possible breaches. This defence mechanism's effectiveness is proven by extensive real-world testing and validation, which also highlights its superiority over traditional RKE systems.[4]

On Vehicular Security for RKE and Cryptographic Algorithms

Furthermore, Chinese researchers demonstrated their ability to remotely activate the brakes of a Tesla Model S. Wi-Fi networking plays a crucial role in realizing ubiquitous computing. Integrating network devices into various environments ensures constant connectivity and improves overall quality of life. Radio Frequency Identification (RFID) services connect devices through unique serial numbers stored in tags. This technology employs radio frequency for communication between an RFID reader and a tagged device, facilitating tracking and identification of various implanted objects.[5]

Security and Privacy of PUF-Based RFID Systems

Ferucio Laurenţiu Ţiplea, Cristian Andriesei, and Cristian Hristea

Alexandru Ioan Cuza University of Iasi, Iasi, Romania Gheorghe Asachi Technical University, Iasi, Romania Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest,Romania ,SC AT&C Technology SRL, Iasi, RomaniaAddress all correspondence to: fltiplea@gmail.com.

In 2020, a particular focus was placed on stressing the importance of integrating formal models for evaluating the security and privacy of RFID systems relying on PUFs. The authors delve into the concept of the tag corruption oracle and identify potential threats to the security and privacy of such systems, underscoring the critical role of formal models. Additionally, they highlight the necessity of formally analyzing the cryptographic properties of PUFs to offer verifiable evidence of security and privacy assurances. [6]

III. Methodology:

The methods listed below methods are used to accomplish the work's objectives:

Methodology 1: Careful consideration of security measures and strategies to prevent attackers from reusing captured communication data is necessary when designing a protocol that is resistant to replay attacks in keyless remote systems.

Methodology 2: A security scenario involving both A and the car can be employed to simulate the RollJam attack targeting the key fob

Methodology 3: Attacker A attempts to authenticate as a genuine key fob in this game.

Methodology 4: The proposed mutual authentication mechanism for remote keyless entry (RKE) systems, which relies on PUFs, provides all essential security features. This suggested authentication approach boasts exceptional computational efficiency..

Methodology 5: The proposed method defends against impersonation, replay attacks, and RollJam attacks on RKE systems. It incorporates a mutual authentication mechanism for remote keyless entry (RKE) systems utilizing PUFs, which offers all necessary security functionalities. This authentication approach is highly computationally efficient.

IV. DESIGN

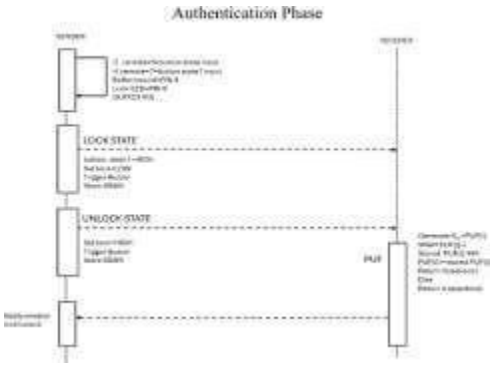


Fig 1:Sequence Diagram

1. Hardware Setup:

Connect RF remote, buzzer, lock, and SRAM to the Arduino board centered on the defined pin configurations in the code.Ensure proper power supply to all components.

2. Software Setup:

Install the necessary libraries, such as SPI.h if not already included.Set up the Arduino Integrated Development Environment (IDE) or your preferred code editor.

4. SRAM Initialization:-

SRAM PUF has a potential to become the main player in hardware security. Here, SRAM PUF technology using off-the-shelf SRAM. The

present testing results on off-the-shelf SRAMs quality to be a PUF component Microchip 23LC1024. Furthermore, there is a secure data and key storage scheme using SRAM PUF. The proposed scheme is influenced by multi- factor authentication. Using a combination of a PUF- generated key and user's password, a derived key is produced and utilized as the final key to protect user's data or/and user's key.

5. PUF Generation and Storage:

Implement the `generatePUF()` function to generate random PUF data.Implement the `storePUF()` function to store the generated PUF data in the SRAM chip.

6. Authentication Process:

The `authenticate()` function evaluates stored PUF data against generated PUF data to verify authentication. Depending on your security needs, you can adjust the authentication process by incorporating additional checks or algorithms for heightened security. For instance, you might introduce multi-factor authentication or integrate cryptographic hashing algorithms to strengthen the authentication process.

V. CODE AND IMPLEMENTATION

1. Enhance PUF Generation:

- Instead of random data generation, consider implementing a more sophisticated PUF generation method (e.g., Arbiter PUF, RO-PUF) for higher security.

2. PUF Storage:

- Encrypt the PUF data before storing it in SRAM to prevent easy extraction by unauthorized access.

3. Enhanced Authentication:

- Implement a challenge-response mechanism:

Challenge Generation: The system produces a random challenge (nonce) for each authentication attempt.

Response Calculation:

a. Combine the challenge with the PUF data using a secure algorithm (e.g., HMAC-SHA256) to generate a response.

b. Store this response in SRAM alongside the encrypted PUF data.

4. Authentication Process:

- When a user attempts authentication:
- The challenge is sent to the device.
- The device calculates the expected response using the stored PUF data and the challenge.
- If the received response matches the calculated response, authentication is successful.

4. **Anti-Replay Protection:**

- Include a timestamp or sequence number in the challenge to prevent replay attacks.

5. **Error Handling:**

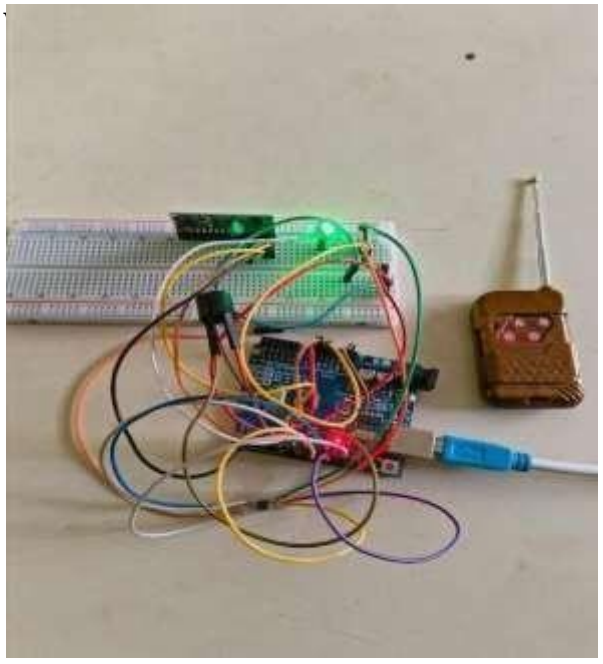
- Implement retry limits or cooldown periods for failed authentication attempts to deter brute-force attacks.

6. **Secure Communication:**

- Ensure secure communication channels (e.g., TLS for networked devices) to protect against eavesdropping and man-in-the-middle attacks.

VI. HARDWARE IMPLEMENTATION

- Arduino UNO-Through Arduino connect the following :
- RF 2262/2272
- LED BULB
- 23LC1024 Microchip
- Buzzer
- Jumper Wires



CONCLUSIONS

This paper examines attacks on RKE systems and presents a mutual authentication mechanism for RKE systems utilizing PUFs. The proposed mechanism is streamlined yet offers all essential security features. Analysis of its security and performance demonstrates the effectiveness of PUFs in creating an efficient authentication system for RKE systems..

VIII. ACKNOWLEDGMENT

We are grateful to Mrs. Supriya Suresh ,Assistant Professor ,for serving as our project guide and for her capable leadership in making this project works success

IX. REFERENCES

[1] Rohini Poolat Parameswarath and Biplab Sikdar published "A Lightweight and Secure Mutual Authentication Mechanism for Remote Keyless Entry Systems Based on PUFs" in 2022.

[2] A Physical Unclonable Design for Key Generation for AES Encryption Algorithm- Alexandra Balan and Florin Sandu-2022

[3] Alexandra Balan and Florin Sandu "A PUF-based cryptographic security solution for IoT systems on chip",2020

[4] Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic-Kyle Greene,Deven Rodgers, Henry Dykhuizen, Quamar Niyaz,Khair Al Shamaileh and Vijay Devabhakutuni,2021.

[5] On Vehicular Security for RKE and Cryptographic Algorithms-Kunal Karnik,Saurabh Kale,Manandeep,Ajinkya Medhekar,2020.

[6] Ferucio Laurenţiu Ţiplea, Cristian Andriesei and Cristian Hristea"Protection and Privacy of PUF-BasedRFID Systems",2020

