2025 Cryptographic Hardware and Embedded Systems (CHES)

A Lightweight PUF-based Mutual Authentication Protocol Using a Modeling-Resistant Dynamic Refresh Strategy

Jiang Li, Yijun Cui, Chenghua Wang, and Weiqiang Liu

College of Integrated Circuit, Key Laboratory of Aerospace Integrated Circuits and Microsystem Ministry of Industry and Information Technology
Nanjing University of Aeronautics and Astronautics, Nanjing, China
Email: lijiang@nuaa.edu.cn

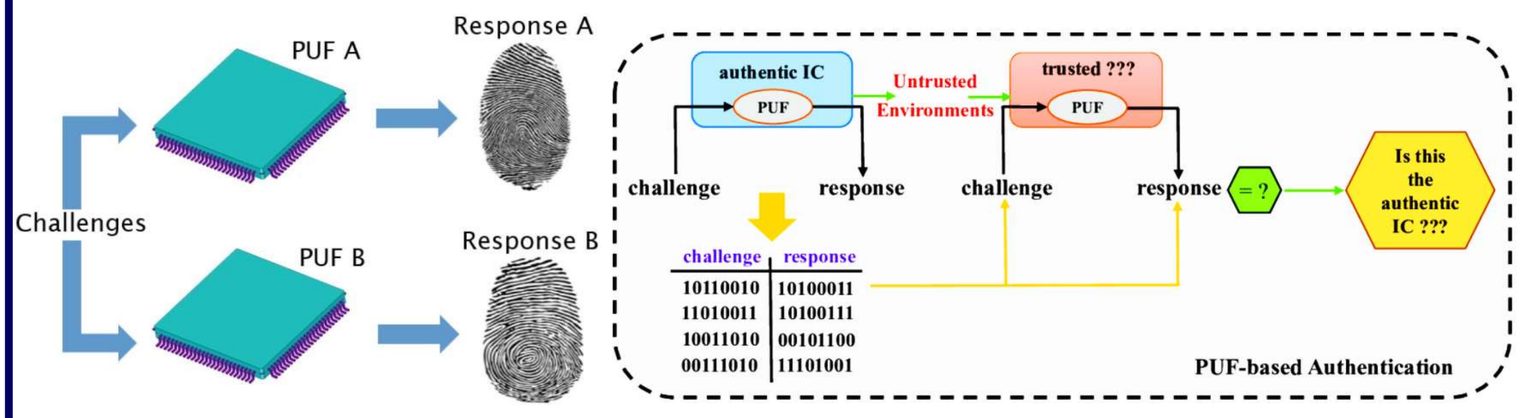
Background

1. Resource-constrained IoT devices
- Small calculation capacity
- Limited storage space
- Battery powered
- Outdoor Deployment

2. Conventional software encryption
- High cost
- Need to store keys
- High power consumption
- Can be copied

Introduction

Physical Uncloanble Function (PUF) is increasingly used in authentication and key generation due to its low cost and high security.



Unilateral protocol that vulnerable to machine learning attacks.

Lightweight Mutual Authentication Protocol

Device j — Server

$(ID_j, c_a) \leftarrow TRNG$

$ID_j \,||\, c_a$ ←

$<c_0, c_1, c_4> \leftarrow PRNG(c_a)$

$(r_0, r_1, r_4) \leftarrow PUF(<c_0, c_1, c_4>)$

Store ID_j

$r_0 \,||\, r_1 \,||\, r_4$ →

Store (c_a, r_0, r_1, r_4)

Enrolment phase: Only three CRPs are required.

Device j — Server

(c_a, r_0, r_1, r_4)

c_a ←

$E_i' \leftarrow r_i' \oplus Q', i \in \{0, 1, 2, 3, 5\}$

$N \leftarrow N + 1$

if $(N > N_{th})$ Lockdown

$ID_j \,||\, c_b \,||\, E_i'$ →

E_4 ←

Abort if $(T_2 < T_{th})$, else successful

if $(N > N_{th})$ fresh PUF

$N \leftarrow 0$

Refresh strategy against ML attacks.

Device j — Server

(c_a, r_0, r_1, r_4)

c_a ←

$<c_0, c_1, c_4> \leftarrow PRNG(c_a)$

$(r_0', r_1') \leftarrow PUF(<c_0, c_1>)$

$(c_b, Q') \leftarrow TRNG$

$<c_2, c_3, c_5> \leftarrow PRNG(c_b)$

$(r_2', r_3', r_5') \leftarrow PUF(<c_2, c_3, c_5>)$

$E_i' \leftarrow r_i' \oplus Q', i \in \{0, 1, 2, 3, 5\}$

$ID_j \,||\, c_b \,||\, E_i'$ →

Abort if ID_j is invalid

$(Q_0, Q_1) \leftarrow E_i' \oplus r_i, i \in \{0, 1\}$

$T \leftarrow match\ (Q_0, Q_1)$

Abort if $(T_1 < T_{th})$, else successful

$(r_2, r_3) \leftarrow E_i' \oplus Q_0, i \in \{2, 3\}$

$(c_a, r_0, r_1) \leftarrow (c_b, r_2, r_3)$

$E_4 \leftarrow r_4 \oplus Q_0$

E_4 ←

$(r_4') \leftarrow PUF(<c_4>)$

$E_4' \leftarrow r_4' \oplus Q'$

$T_2 \leftarrow match\ (E_4', E_4)$

Abort if $(T_2 < T_{th})$, else successful

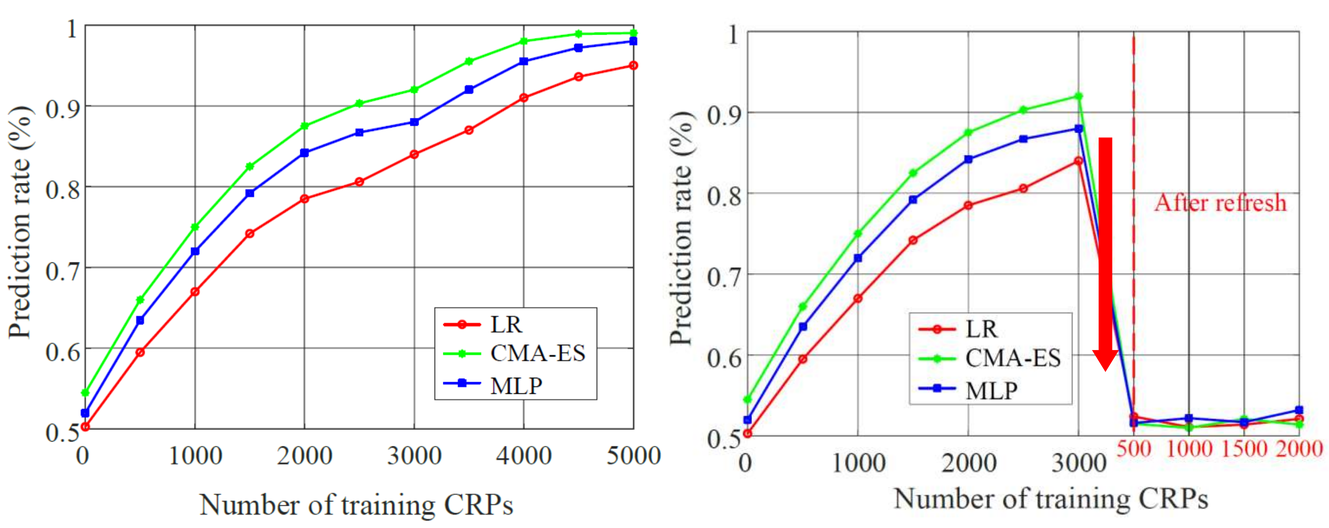
$r_5 \leftarrow E_5' \oplus Q_0$

$r_4 \leftarrow r_5$

Store (c_a, r_0, r_1, r_4)

Authentication phase: The enroll-while-authenticate mechanism allows simultaneous enrollment and authentication.

Performance



Conclusion

- This work presents a lightweight mutual authentication protocol that integrates a novel modeling-resistant dynamic refresh strategy.
- An enroll-while-authenticate mechanism is proposed, which significantly reduces server-side storage and computation overhead.
- Experimental results demonstrate that the proposed approach achieves strong resilience to modeling attacks.