جامعة البليدة 1
UNIVERSITE BLIDA 1

LINEACT cesi

A Low-Cost Authentication Protocol Using Arbiter-PUF

Fahem Zerrouki, Samir Ouchani, and Hafida Bouarfa

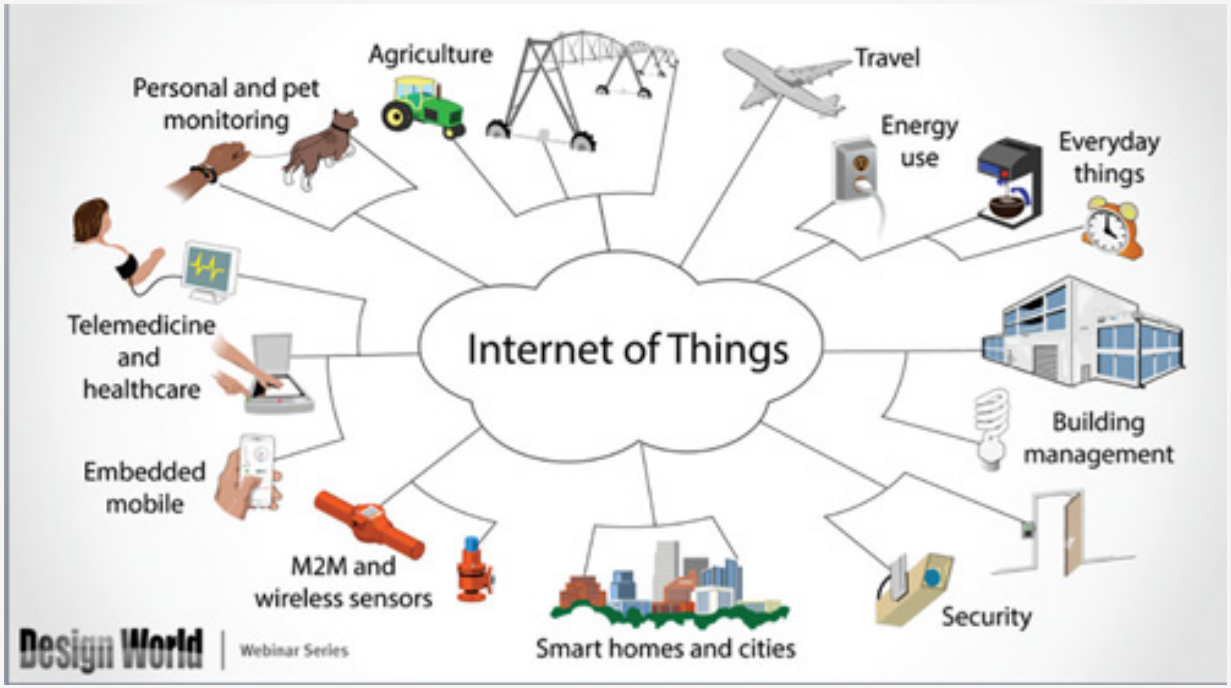
MEDI2021, June 21-23, 2021, Tallinn, Estonia.

21th June 2021

Contents

Introduction

- Internet of Things (IoT) is revolutionizing our daily lives.
- IoT is the future for many sectors: hospitals, schools, transportation, etc.
  - It is estimated that there will be 75 billion IoT devices by 2025.
  - Every second, around 127 devices are connected to internet.



Introduction (cont'd)

Security Issues

- Secure booting
- Authentication
- Privacy protection
- Data integrity
- User profiling and tracking
- Access control
- Digital forgetting

Authentication protocol

- Is the process of identifying devices
- Confirms the identity of each individual registered entity in an entrusted network
- Is the first step towards establishing a session after a secure boot of the IoT device and must be done in a secure and an efficient way

Claim

- Any solution and authentication protocol should satisfy the existing and recommended "IoT" cryptographic primitives
  1. should be **lightweight** occupying a little area on the device and have a very low power consumption
  2. **uniquely** identified on the network
  3. The used secret key by IoT devices has to resist to **physical attacks**
  4. Do not store **any** secrets on the device.

Conventional security for IoT

Conventional cryptographic schemes are designed for main-powered, high processing and large memory devices

- Encryption-based authentication: the IoT device uses symmetric and asymmetric algorithms [1]–[3]
- Localization-based authentication uses the information about the IoT device location or those of its neighboring devices or a communication link's characteristics [4], [5]

Does traditional authentication schemes feasible and applicable for IoT?

- An IoT device has many limitations: memory capacity, processing power, and energy resources
- They are exposed to physical attacks (installed in locations where an adversary can easily capture and intercept them)

Claim

Any authentication mechanism shaped to IoT system has to consider the different communication ways while satisfying the "IoT" cryptographic primitives, security requirements and making it resilient to physical attacks

Related Work

1. PUF's response is used to guarantee data integrity in the authentication process by proposing two mutual authentication schemes: server-IoT and IoT-IoT devices (Aman et al.[6],2017)
2. PUF's response and timestamp of an authentication session are used to provide the identity of the IoT device (Chatterjee *et al.*[7], 2017)
3. PUF is used as authentication factors that allow an anonymously to communicate between the IoT device and the trusted server (Gope *et al.* [8], 2018)
4. The database is used as a third party in device authentication scheme for Internet-of-Medical-Things (IoMT). They store the device information in the server where the generated response by the server is used as the challenge of the IoMT device (Yanambaka *et al.* [9], 2019)

Limitations

1. The existing PUF based protocols ignores noise during the authentication steps
2. The noise elimination is guaranteed by the device which make it vulnerable to helper data manipulation
3. The protocols supporting noise elimination could be compromised since they transmit the helper data with the extracted secret key to the server

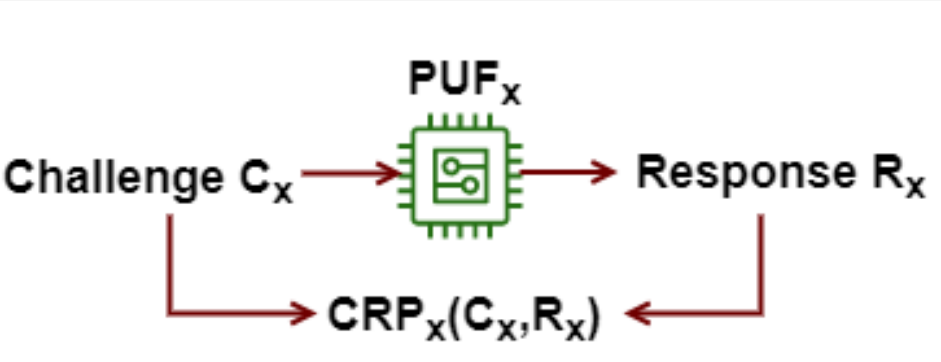
Definition

Physical unclonable functions (PUFs) are a primitive cryptosystem that exploits the intrinsic randomness found in ICs to generate a **non-uniform**, random, unique, unpredictable, and reproducible string that is used as a cryptographic key.

IC fingerprint

How PUF work ?

- Current manufacturing processes do not have the control at the nanoscale level
- Variation is inherent in fabrication process, hard to remove or predict and it is unique for each physical object
- Rather than storing the secrets in digital memory, PUFs exploit this randomness to derive the unique digital fingerprint



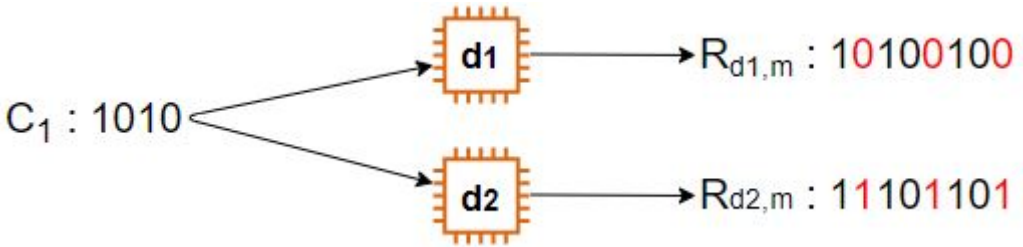
Challenge Response Behavior

Why PUF is suitable for IoT authentication ?

- PUF give to a device a **unique** identifier like a human fingerprint.
- PUF generate a secret key **without** storing any digital information on the device.
- It is difficult, or **impossible**, to build or to clone a given PUF.
- The produced key from PUF can be generated **only** when required.
- **No** battery or other permanent power source is required.
- PUF is a **low-cost** security primitive.

Uniqueness

$$Uniqueness = \frac{2}{D(D-1)} \frac{1}{P} \sum_{d_1=1}^{D-1} \sum_{d_2=d_1+1}^{D} HD(R_{d_1,m}, R_{d_2,m})$$



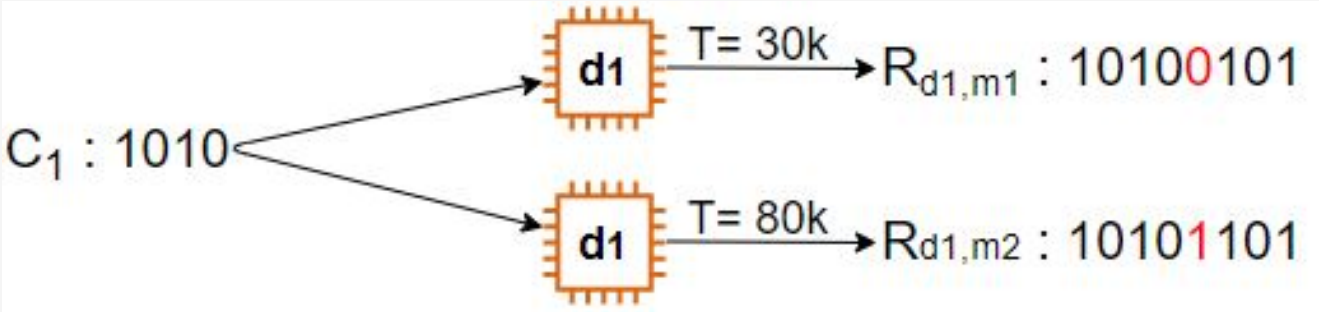
Uniformity

$$Uniformity = \frac{1}{P} \sum_{p=1}^{P} (r_{p,d,m})$$

The HW of of '01010101' $\longrightarrow$ uniformity is the optimal value 50%

Environmental effects

- Environmental variation or variability in the environmental conditions plays an important and significant role in the circuit operating conditions
- It has a major impact on the stability and the reliability of the output of the PUF
- The factors that caused this variation can be temperature, power supply, or even by the aging of the IC



Noise vs Cryptographic

- Environmental effects create noise in the output of the PUFs
- This noise resulting in an incorrect and unusable output because it is not the same as the original key
- The response cannot directly be used as a cryptographic key

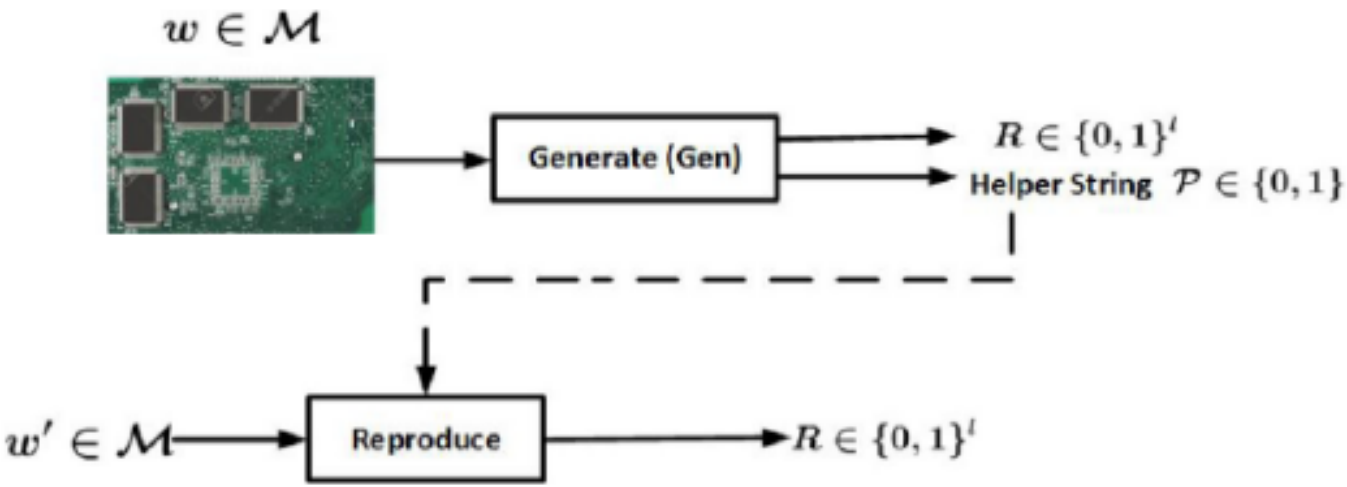
Problematic 2

To exploit PUF as cryptographic key generation process, two problems should be solved:

- Clean the noise or errors found in data when reading multiple times is known as information-reconciliation
- Uniforming data and this process is known as privacy amplification

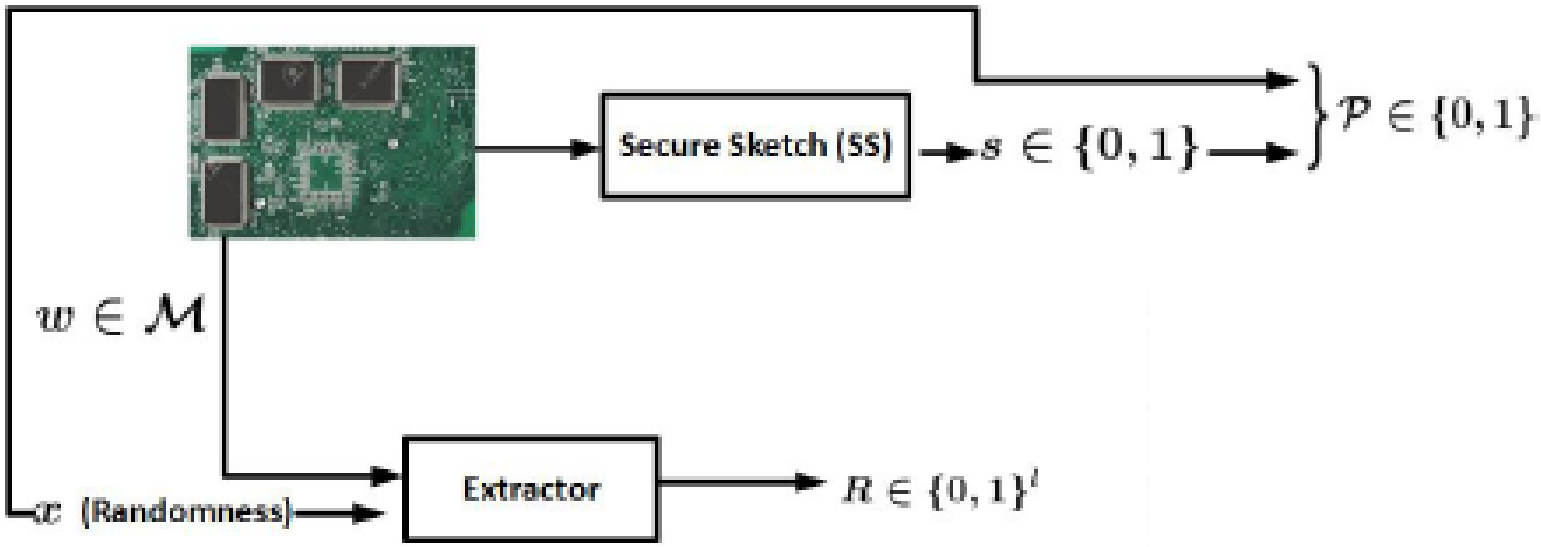
Fuzzy Extractor

FE is a solution used to extract uniformly random string from noisy and not uniformly random data. It is consists of a pair of efficient algorithms (Gen,Rep)



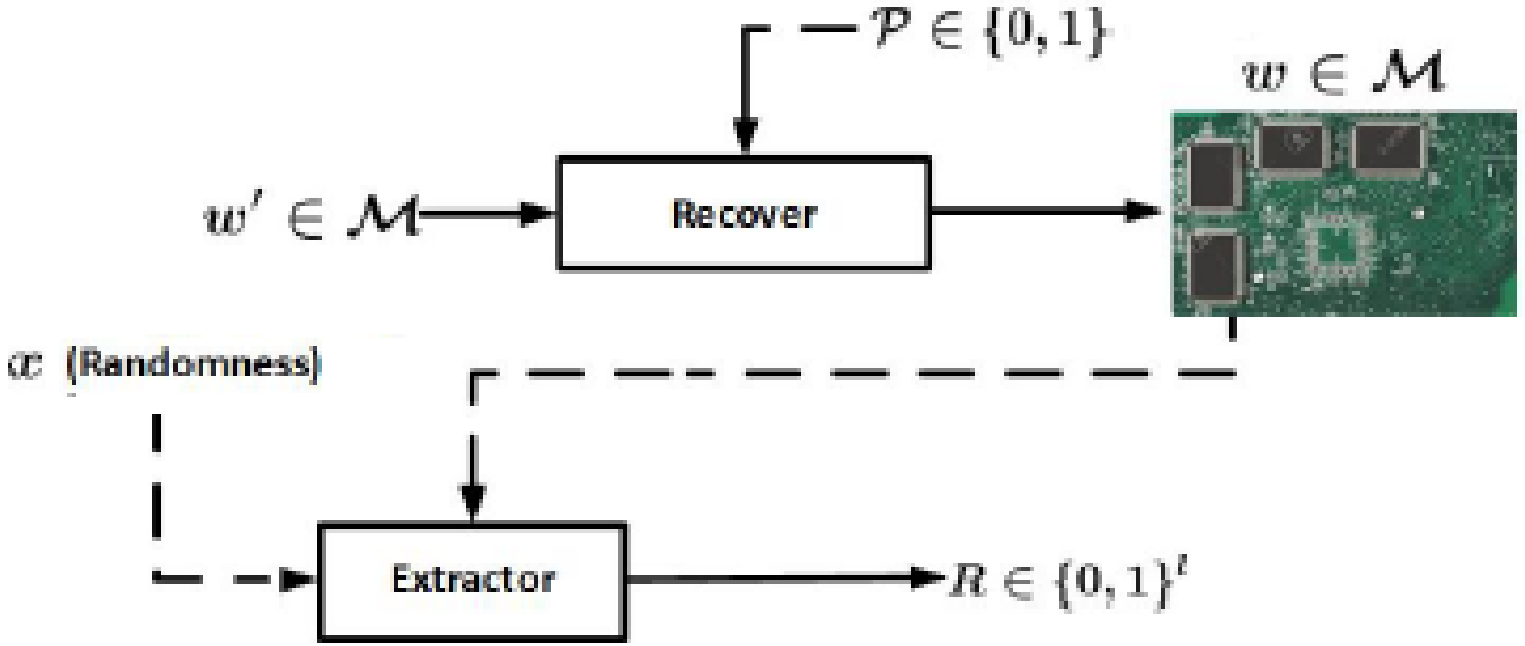
Key Generation

Gen takes as input the initial reading w from a noisy source and produces a uniformly random string R, which is used as a cryptographic key, and a non-secret string P (Public helper data)

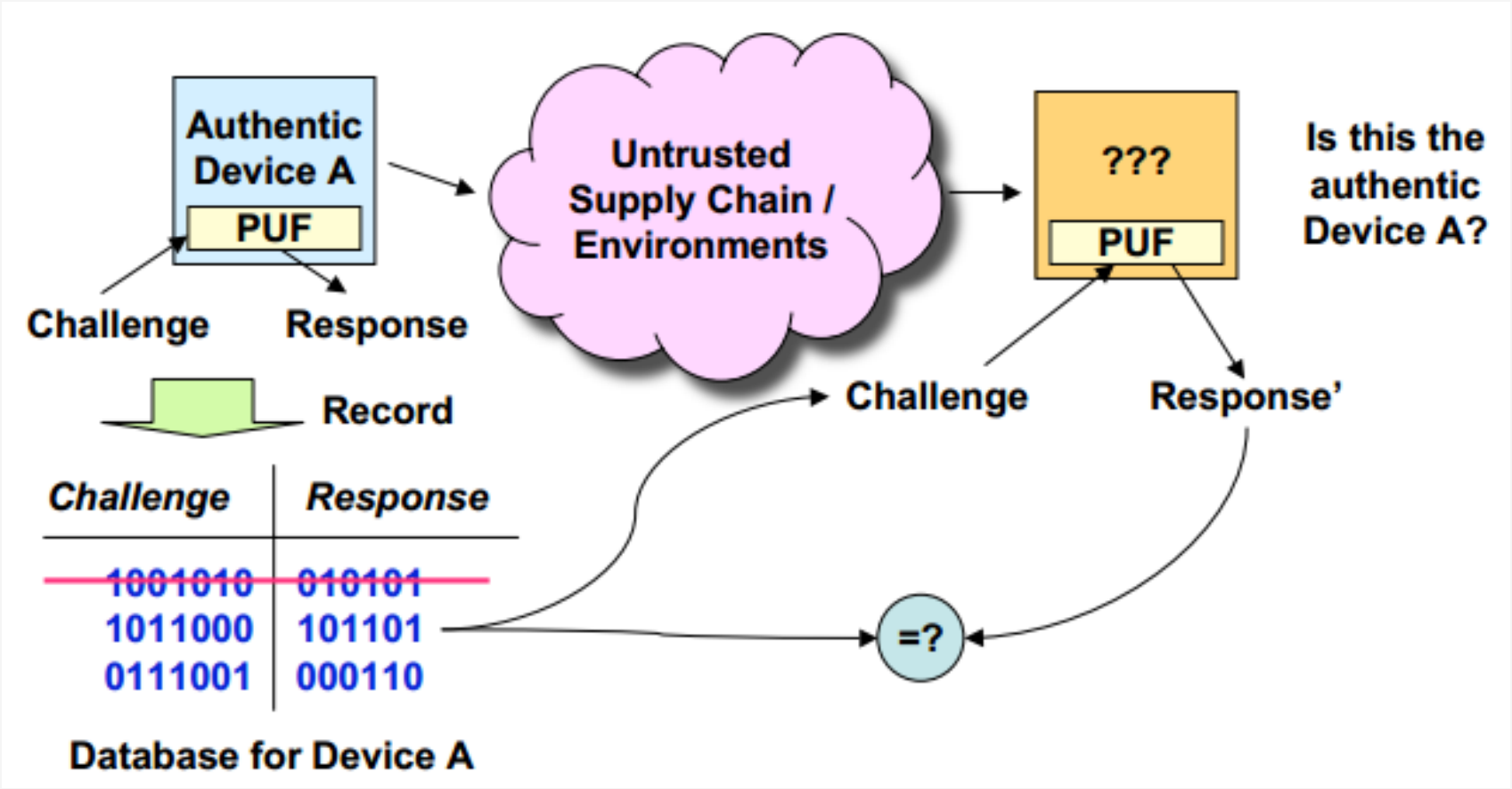


Key Reproduction

Rep takes two inputs: the public helper data P and w' which is a noisy version of w, *Rep* reproduces R if w and w are close enough



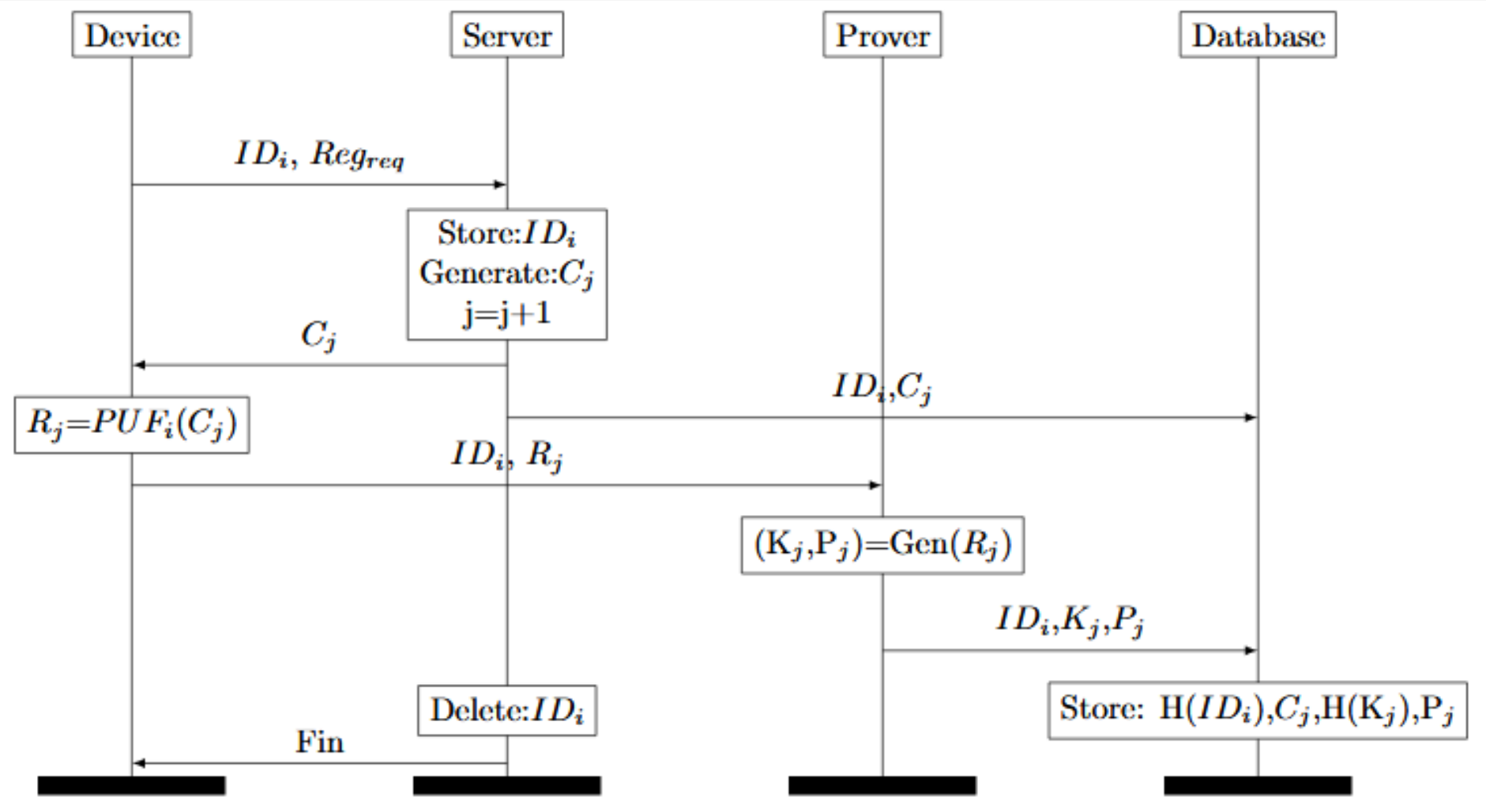
A Low-cost Authentication Protocol



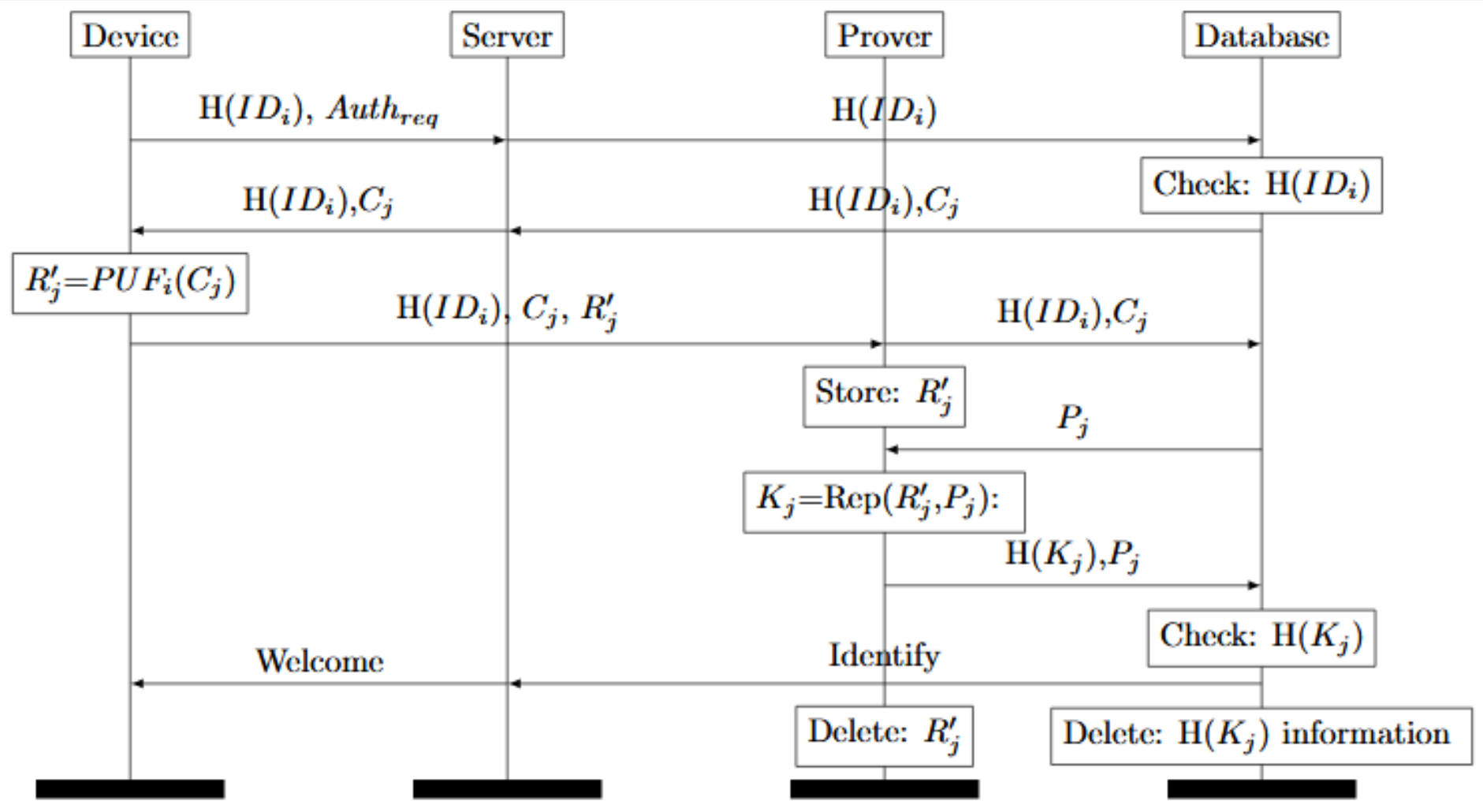
Communication Model

- Our **communication model** establishes a secure connection for an IoT device
- **Device** should integrates a PUF without storing any information
- **Server** does not store anything but it generates challenge generation. It is the first interface interfering with the device
- **Prover** is responsible for information-reconciliation and privacy amplification using Fuzzy Extractor without any prior stored information
- **Database** stores challenges, the helper data, the device identifier and its secret key.

Enrolment phase.

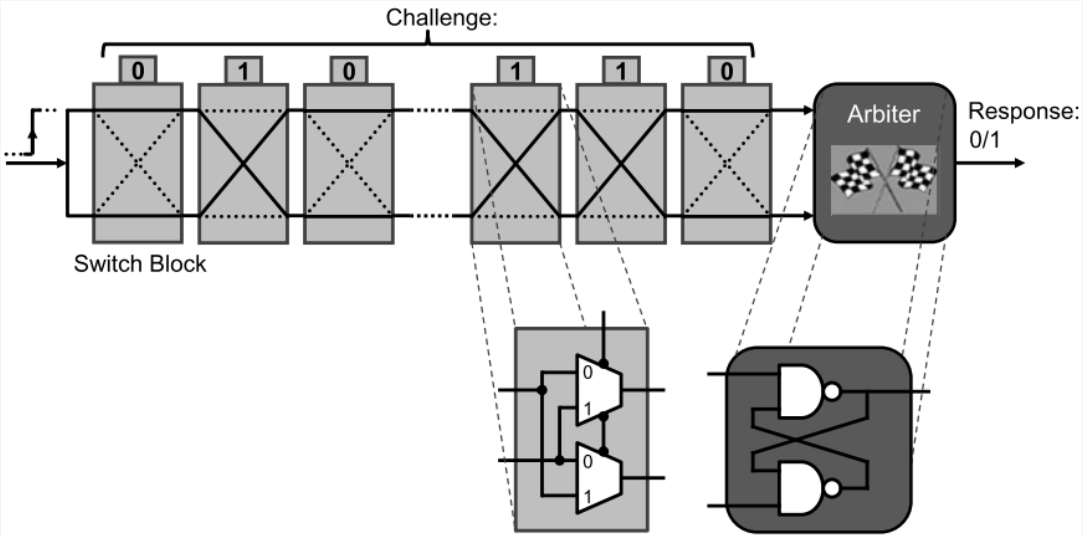


Authentication phase.

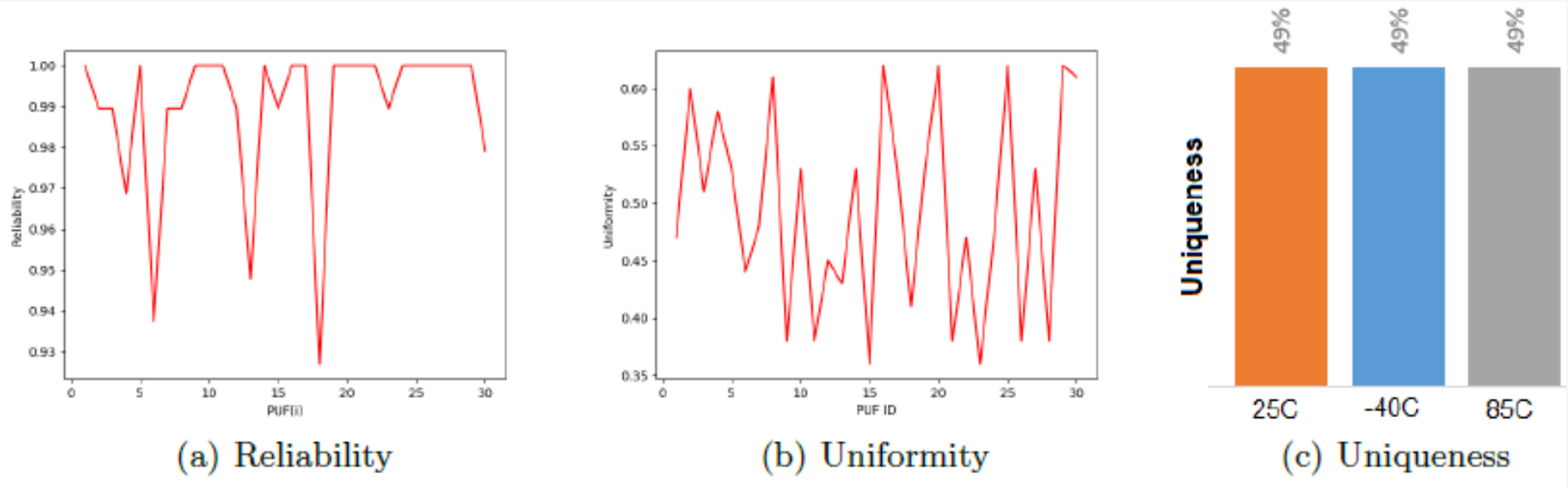


Experimental Results and Discussion

- Authentication between a device with an arbiter PUF and a server
- Check the performance of the used PUF
- Evaluate the correctness of the prover by extracting the uniform key from the response
- Recover the original one from the noisy response
- Prove the identity through a trusted server



Performance evaluation



(a) Reliability (b) Uniformity (c) Uniqueness

Key Extraction and Reconstruction

PUF_i	$R_{Reliability}(\%)$	$R_{Uniformity}$ (%)	$Error_{-40C}$	$Error_{85C}$	$K_{Uniformity}(\%)$	Correction
1	100	0.47	0	0	48	✓
2	99	0.6	1	0	45	✓
3	99	0.51	1	0	50	✓
4	97	0.58	1	2	54	✓
5	100	0.53	0	0	51	✓
6	94	0.44	1	5	50	✓
7	99	0.48	0	1	48	✓
8	99	0.61	0	1	48	✓
9	100	0.38	0	0	51	✓
10	100	0.53	0	0	50	✓
11	100	0.38	0	0	53	✓
12	99	0.45	1	0	47	✓
13	95	0.43	3	2	51	✓

Conclusion

Physically unclonable functions have a complete different system than any other one way function, especially with the challenge response pairs sets they provide a better reliability. Also, the level of defense is really good with PUFs, which make them a good security primitive for IoT field.

This work presents a low-cost protocol that exploits the randomness of the Arbiter PUF. We have used a fuzzy extractor as a prover in the protocol with the role to identify the trusted objects and correct the keys in the case of an allowed noise. The experiments were run on a benchmark related to the Arbiter PUF and showed good results.

Perspectives

1. Verify the security properties for the developed protocol: integrity, secrecy, availability, and confidentiality
2. Propose a mutual authentication and a session key protocol for IoT devices
3. Check possible vulnerabilities related to Denial-of-Service (DoS) and replay attacks, synchronization problems, token/server impersonation, and modeling attack
4. Simulate and deploy the proposed protocol on a real use case (autonomous vehicle)

Bibliography

[1] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for iot and cloud servers," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6428–6453, 2018.

[2] J. R. Naif, G. H. Abdul-Majeed and A. K. Farhan, "Secure iot system based on chaos-modified lightweight aes," in *2019 International Conference on Advanced Science and Engineering (ICOASE)*, IEEE, 2019, pp. 1–6.

[3] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon and H. F. Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Computers & Electrical Engineering*, vol. 52, pp. 114–124, 2016.

[4] P. Figueiredo e Silva, V. Kaseva and E. S. Lohan, "Wireless positioning in iot: A look at current and future trends," *Sensors*, vol. 18, no. 8, p. 2470, 2018.

Bibliography (cont'd)

[5] J. Zhang, Z. Wang, Z. Yang and Q. Zhang, "Proximity based iot device authentication," in *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*, IEEE, 2017, pp. 1–9.

[6] 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.

[7] 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.

[8] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580–589, 2018.

Bibliography (cont'd)

[9] V. P. Yanambaka, S. P. Mohanty, E. Kougianos and D. Puthal, "Pmsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

Thank you for your attention!

ze.fahem@gmail.com

Any Question