An Extended PUF-based Protocol

Francesco Berti
EnICS, Selecsys Labs
Bar-Ilan University
Ramat-Gan, Israel
francesco.berti@biu.ac.il

Itamar Levi
EnICS, Selecsys Labs
Bar-Ilan University
Ramat-Gan, Israel
itamar.levi@biu.ac.il

***Abstract*—We extend a PUF-based authentication protocol with key refresh, hierarchical groups, and revocation. Our framework enables secure communication among enrolled devices without server interaction, allowing group leaders to derive subordinate keys and the server to exclude compromised parties through controlled key updates.**

***Index Terms*—PUF**

I. Introduction

Kerckhoffs' principle states that the security of a cryptographic scheme should depend solely on the secrecy of its key [1]. Ensuring secure key generation, storage, and usage remains challenging [2].

Physically Unclonable Functions (PUFs) offer a hardware-based solution: a piece of unclonable hardware serving as a key. PUFs can be implemented in deep manometric silicon technologies within application specific integrated circuits, ASICs, or systems on a chip SoCs designs by various low-abstraction circuitry mechanisms, e.g., ring oscillators or SRAM cells metastability, race-conditions etc. [2]–[4]. They are designed to maintain a device (or user) specific signature like an ID or fingerprint, which is robust to noise and other adversarial scenarios. Therefore manometric PUFs are highly important. In commercial devices they are already wide spread and technologically mature. They are widely used in the Internet of Things (IoT) and Internet of Vehicles (IoV) due to their low footprint [5].

PUFs are usually used in two ways. In the first, *enrollment*, the PUF interacts securely with a server before being deployed. The server then provides the necessary information to other parties that wishes to interact with the PUF. In the second, *handover* [2] phase, one party has temporary access to the PUF, performs computations with it, and then transfers it to another party. The second party can then use the PUF to communicate securely with the first party [6].

The security of PUF-based protocols has been analyzed in the universal composability (UC) framework. Protocols often integrate passwords [7] or support group-based communication [5]. Surveys covering PUF protocols include [8]–[10].

Our contributions: We extend Maes' protocol [11] by supporting three features: (i) key refresh, (ii) hierarchical groups where leaders can access all subordinate messages, and (iii) party revocation. A trusted server manages enrollment and group permissions. The cost of these additions in communications is minimal (only the communication necessary to refresh), and in computation is little (only for groups and it is proportional to the depth of the group).

I. Levi and F. Berti funded by Israel Science Foundation, ISF grant 2569/21.

II. Preliminaries

Let $\{0,1\}^n$ be the set of n-bit strings and $\{0,1\}^*$ the set of all finite strings. Sampling x uniformly from $\mathcal{X}$ is denoted $x \xleftarrow{\$} \mathcal{X}$. We use a hash function $\mathsf{H} : \{0,1\}^* \to \{0,1\}^n$, modeled as a random oracle [1].

Physically Unclonable Functions (PUF): Mathematically, a PUF is a function $\mathsf{PUF} : \{0,1\}^n \to \{0,1\}^m$ producing unpredictable outputs [12]. A *strong* PUF supports many challenges, while a *weak* PUF supports few or a single challenge [13]. Thus, a PUF can be viewed as a circuit providing unpredictable challenge-response pairs.

III. Protocol

a) Enrollment framework: A trusted server enrolls all devices and defines communication permissions. Once deployed, devices communicate without server intervention. Sec. IV explains hierarchical group organization.

b) Enrollment without groups.: The server interacts securely with a PUF, assigning identity id, querying challenge c to obtain response $y = \mathsf{PUF}(c)$, and storing (id, c, y). The communication key with party A is $k = \mathsf{H}(id_{\mathsf{PUF}}, id_A, c, y, r)$, where r is current randomness. The server provides the PUF the keys $(id_1, c_{id_1}, k_{id_1}), \ldots, (id_N, c_{id_N}, k_{id_N})$ of the parties it is authorized to communicate, and the current randomness. See Fig. 1.

c) Double authentication and key derivation.: Party A selects random $x \xleftarrow{\$} \{0,1\}^n$ and sends (c, x, id_A) to the PUF. The PUF computes $y = \mathsf{PUF}(c)$, $k = \mathsf{H}(id_{\mathsf{PUF}}, id_A, c, y, r)$, $h = \mathsf{H}(k, x, r)$, selects $x' \xleftarrow{\$} \{0,1\}^n$, and sends (h, x') to A. Party A verifies $h = \mathsf{H}(k, x, r)$ and responds with $h' = \mathsf{H}(k, x, x', r)$. The PUF verifies h' and both parties derive the shared key $k' = \mathsf{H}(k, h, h')$ for secure communication. We depict this in Fig. 2.

This follows Maes' protocol [11]. Security relies on the preimage resistance of h due to the random oracle.

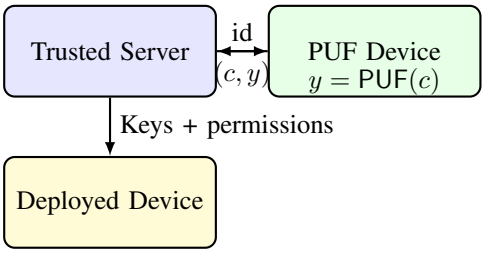

Fig. 1. Enrollment phase: the server securely queries the PUF and provisions the deployed device.

IV. Key refresh, Revocations and Groups

a) Key refresh and revocation.: The server can update randomness r' and distribute new keys $k = \mathsf{H}(id_{\mathsf{PUF}}, id_A, c, y, r')$. Parties without updates cannot communicate, enabling secure revocation. For this communication, the server can use as a key $k = \mathsf{H}(id_{\mathsf{PUF}}, c, y)$ (a key that the PUF can retrieve easily). See also Fig. 3.

b) Hierarchical groups.: Devices are organized in a tree. Each node can access communications of subordinate devices. For instance, in a bank, area managers supervise regional managers, who supervise operatives. Leaders can perform the functions of all subordinate nodes.

c) Identity vectors.: Each member receives an identity vector $id = (id_1, \ldots, id_I)$ with $id_i \in \{0,1\}^n$. Leaders have vectors of length I, while members share the first I components and extend them for subgroups. That is, the leader identity vector can be $id = (id_1, \ldots, id_I)$ while all the members of the group has identity vector $id = (id_1, \ldots, id_I, id_{I+1}, \ldots, id_{I'})$. Keys are derived iteratively: $k_i = \mathsf{H}(id_{\mathsf{PUF}}, id_i, c, k_{i-1}, r)$ with $k_0 = y$, allowing leaders to compute all subordinate keys.

V. Conclusions

We introduced a PUF-based authentication protocol supporting key refresh, hierarchical groups, and party revocation using a random oracle. Our framework enables secure and flexible communication among enrolled devices with minimal server interaction.

References

[1] J. Katz and Y. Lindell, *Introduction to Modern Cryptography, Second Edition*. CRC Press, 2014.

[2] R. Maes, *Physically Unclonable Functions - Constructions, Properties and Applications*. Springer, 2013.

[3] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A puf taxonomy," *Applied physics reviews*, vol. 6, no. 1, p. 011303, 2019.

[4] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electronics*, vol. 3, no. 2, pp. 81–91, 2020.

[5] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K. R. Choo, "Puf-based authentication and key agreement protocols for iot, wsns, and smart grids: A comprehensive survey," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8205–8228, 2022.

[6] M. van Dijk and U. Rührmair, "Physical unclonable functions in cryptographic protocols: Security proofs and impossibility results," *IACR Cryptol. ePrint Arch.*, p. 228, 2012.

[7] I. Ahmim, N. Ghoualmi-Zine, A. Ahmim, and M. Ahmim, "Security analysis on "three-factor authentication protocol using physical unclonable function for iov"," *Int. J. Inf. Sec.*, vol. 21, no. 5, pp. 1019–1026, 2022.

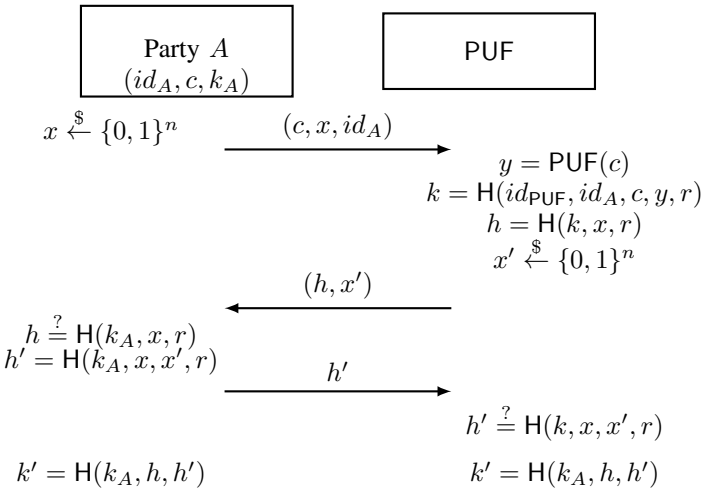

Fig. 2. Double authentication and shared key derivation between party A and the PUF.

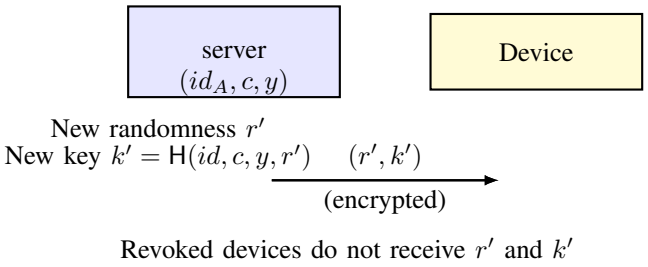

Fig. 3. Key refresh and revocation mechanism.

[8] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-K. R. Choo, "Puf-based authentication and key agreement protocols for iot, wsns, and smart grids: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8205–8228, 2022.

[9] R. A. Alhamarneh and M. Mahinderjit Singh, "Strengthening internet of things security: Surveying physical unclonable functions for authentication, communication protocols, challenges, and applications," *Applied Sciences*, vol. 14, no. 5, p. 1700, 2024.

[10] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (puf)-based security solutions for internet of things," *Computer Networks*, vol. 183, p. 107593, 2020.

[11] R. Maes, "Physically unclonable functions: Concept and constructions," in *Physically unclonable functions: constructions, Properties and applications*, pp. 11–48, Springer, 2013.

[12] C. Brzuska, M. Fischlin, H. Schröder, and S. Katzenbeisser, "Physically uncloneable functions in the universal composition framework," in *CRYPTO*, 2011.

[13] M. Barbareschi, V. Casola, A. Emmanuele, and D. Lombardi, "A lightweight puf-based protocol for dynamic and secure group key management in iot," *IEEE Internet Things J.*, vol. 11, no. 20, pp. 32969–32984, 2024.