HAL open science

Sub-Space Modeling: An Enrollment Solution for XOR Arbiter PUF using Machine Learning

Amir Ali Pour, David Hely, Vincent Beroulle, Giorgio Di Natale

To cite this version:

Amir Ali Pour, David Hely, Vincent Beroulle, Giorgio Di Natale. Sub-Space Modeling: An Enrollment Solution for XOR Arbiter PUF using Machine Learning. International Symposium on Quality Electronic Design (ISQED 2022), Apr 2022, Virtual event, United States. 10.1109/ISQED54688.2022.9806267 . hal-03599356

HAL Id: hal-03599356

https://hal.science/hal-03599356v1

Submitted on 7 Mar 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

Sub-Space Modeling: An Enrollment Solution for XOR Arbiter PUF using Machine Learning

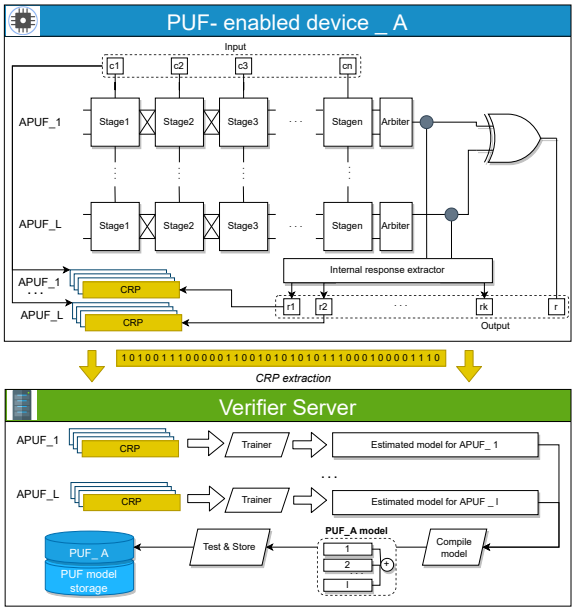
Amir Ali-pour*, David Hely†, Vincent Beroulle‡ and Giorgio Di Natale§
(*,†, ‡) Univ. Grenoble Alpes, Grenoble INP, LCIS, 26000 Valence, France
§ Univ. Grenoble Alpes, CNRS, Grenoble INP, TIMA, 38000 Grenoble, France,
(*,†, ‡, §) Email: firstname.lastname@univ-grenoble-alpes.fr

***Abstract*—In this work we present sub-space modeling of XOR Arbiter PUF as a cost efficient solution for enrollment for the designers' community. Our goal is to demonstrate a method which can reduce the overall cost in terms of number of CRPs required for training, training time and memory. Here we propose to reduce the complexity of the modeling target by dividing the PUF into smaller sub-components and model each sub-component of the PUF independently. Our early experimental assessment show that our sub-space modeling can significantly reduce the cost of training compared to some of the latest works, thus it is potentially a cost-efficient solution to enroll strong PUF with high complexity.**

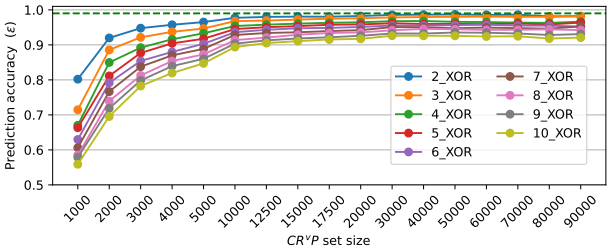
***Index Terms*—Physically Unclonable Function (PUF), XOR Arbiter PUF, PUF Enrollment, Machine Learning (ML)**

I. Introduction & Proposed Method

Our proposed solution can be used in emerging authentication and key generation protocols which demand to generate an equivalent predictive model of a target XOR arbiter PUF on a trusted third party (TTP) verifier server [1]–[3]. This solution should collectively reduce the number of CRPs in order to obtain an accurate model of XOR Arbiter PUF with large XOR size. A schematic of our proposed method is shown in Fig. 1a. Here the illustration shows sub-space modeling of n-bit L-XOR Arbiter PUF (n is the challenge size and k is the XOR size). As shown in Fig. 1a, the internal data from each internal Arbiter PUF ($r1$ to rL), in conjunction to their corresponding challenge values (e.g. $\{c1 \ldots cn\}$ + $\{r1\}$ for APUF_1, $\{c1 \ldots cn\}$ + $\{r2\}$ for APUF_2, etc.) are fed separately to trainer functions to discretely generate estimation models of each Arbiter PUF. After the trainer functions provide accurate estimated models, we merge the sub-models into forming a whole model which represents the whole PUF. An early demonstration of the prediction accuracy of the models generated with our method for variant XOR sizes are shown in Fig. 1b. Collectively, our generated models use considerably lower number of CRPs for modeling, compared to the conventional techniques for modeling XOR Ariber PUF [4].



(a) Schematics of the proposed sub-space modeling method for n-bit L-XOR Arbiter PUF.



(b) Convergence of prediction accuracy (ϵ) with respect to training set size (CR^vP) in modeling PUFs with various XOR sizes.

Fig. 1: Schematics and performance of our proposed method.

References

[1] T. Idriss and M. Bayoumi, "Lightweight highly secure puf protocol for mutual authentication and secret message exchange," in *2017 IEEE International Conference on RFID Technology Application (RFID-TA)*, 2017, pp. 214–219.

[2] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, "Slender puf protocol: A lightweight, robust, and secure authentication by substring matching," in *2012 IEEE Symposium on Security and Privacy Workshops*, 2012, pp. 33–44.

[3] A. Alipour, V. Beroulle, B. Cambou, J. Danger, G. D. Natale, D. Hely, S. Guilley, and N. Karimi, "Puf enrollment and life cycle management: Solutions and perspectives for the test community," in *2020 IEEE European Test Symposium (ETS)*, 2020, pp. 1–10, ISSN: 1558-1780.

[4] N. Wisiol, K. T. Mursi, J.-P. Seifert, and Y. Zhuang, "Neural-network-based modeling attacks on xor arbiter pufs revisited." *IACR Cryptol. ePrint Arch.*, vol. 2021, p. 555, 2021.

This material is based upon the work supported by the French National Research Agency in the framework of the "Investissements d'avenir" program (ANR-15-IDEX-02).