Global Journal of Computer Science and Technology: G Interdisciplinary
Volume 15 Issue 1 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Authentication Algorithm for Portable Embedded Systems using PUFs

By Sunil Devidas Bobade & Dr. Vijay R. Mankar

S.G.B. Amravati University, India

Abstract - Physical Unclonable Functions (PUFs) are circuits that exploit chip-unique features to be used as signatures which can be used as good silicon biometrics. These signatures are based on semiconductor fabrication variations that are very difficult to control or reproduce. These chipunique signatures together with strong challenge-response authentication algorithm can be used to authenticate and secure chips. This paper expands the security avenues covered by PUF and FPGAs by introducing a new class of concept called "Soft PUFs." This scheme propose robust challenge- response authentication solution based on a PUF device that provides stronger security guarantees to the user than what previously could be achieved. By exploiting the silicon uniqueness of each FPGA device and incorporating a special authentication algorithms in existing FPGA fabric, FPGA based embedded systems can be used for new security-oriented and network- oriented applications that were not previously possible or thought of.

Keywords: trapdoor function, soft PUF, physical unclonable functions, challenge–response authentication.

GJCST-G Classification: D.4.7, C.3

Authentication Algorithm for Portable Embedded Systems using PUFs

Sunil Devidas Bobade [α] & Dr. Vijay R. Mankar [σ]

Abstract- Physical Unclonable Functions (PUFs) are circuits that exploit chip-unique features to be used as signatures which can be used as good silicon biometrics. These signatures are based on semiconductor fabrication variations that are very difficult to control or reproduce. These chip-unique signatures together with strong challenge-response authentication algorithm can be used to authenticate and secure chips. This paper expands the security avenues covered by PUF and FPGAs by introducing a new class of concept called "Soft PUFs." This scheme propose robust challenge- response authentication solution based on a PUF device that provides stronger security guarantees to the user than what previously could be achieved. By exploiting the silicon uniqueness of each FPGA device and incorporating a special authentication algorithms in existing FPGA fabric, FPGA based embedded systems can be used for new security-oriented and network- oriented applications that were not previously possible or thought of.

Keywords: trapdoor function, soft PUF, physical unclonable functions, challenge–response authentication.

I. Introduction

PUF, is a trap door function physically blended or inscribed deep in system during manufacturing process and is easy to evaluate but hard to clone. Because of random process variations, no two Integrated Circuits even with the same layouts are identical.Variation is inherent in fabrication process or in areas environmental variations such as temperature, supply voltage and Electromagnetic interference, which can affect their performance and is hard to remove or predict. An untrusted foundry cannot create a copy of the circuit as it is impossible to control the manufacturing process variations. PUFs are highly secure and there are no need for trusted programming and are found to be inexpensive as there is no need of special fabrication technique PUF can enable a secure, low-cost authentication without crypto.

"Security engineers face the seemingly contradictory challenge of providing lightweight cryptographic algorithms for strong authentication, encryption and other cryptographic services that can perform on a speck of dust." [1]. Most of the traditional authentication schemes and encryption algorithms relies on a unique ID or a secret key. They are usually generated and stored in a secure manner in non volatile storage on chip either in fuses or EEPROMs, protecting them from malicious attackers. However, these are susceptible to invasive and non invasive attacks like side channel attacks.

Side channel attacks instead of testing the strength of the cryptographic algorithms and extract the information presented due to implementation weaknesses, instead extract vital information from the electrical characteristics of a chip such as power and timing which are data dependent. Hence, any hardware mechanism aiming to be robust should tackle and counter invasive and non invasive attacks.

PUFs basically work on concept of challenge–response authentication. When a physical stimulus is applied to the structure, it reacts in an unique way as a result of complex interaction of the stimulus with the physical microstructure of the device. This exact microstructure depends on physical factors introduced during manufacturing process. The device's identity is established and hidden in microstructure itself. As this structure is not directly revealed by the challenge-response mechanism such a device is resistant to spoofing attacks.

Unclonability means that each PUF device has a unique and unpredictable yet unique response to challenges. It is infeasible to construct a PUF with the same challenge–response behavior as another given PUF because exact control over the manufacturing process is infeasible. The combination of physical and mathematical unclonability renders a PUF truly unclonable.

A distinction is made between PUFs in which physical randomness is explicitly introduced and used as an unique identification code. PUFs uses this very inherent to thwart attacks.

The strength of a PUF is determined by three important parameters namely uniqueness, reliability and security. Uniqueness indicates the ability to distinguish between different ICs, measured by determining hamming distance between the responses obtained from different PUF instances. Reliability indicates that PUF circuit should be capable of reproducing CRPs in presence of noise and environmental variations. The security in PUFs indicates a PUF's susceptibility to different types of modeling attacks. It should be

Author α: Research Scholar, S.G.B. Amravati University Amravati, India.
e-mail: sunilbobade73@gmail.com
Author σ: Deputy Secretary, R.B.T.E. Pune Region Pune, India.
e-mail: vr_mankar@rediffmail.com

impossible to construct an exact replica of a PUF instance even with complete knowledge of the design.

In the case of ASIC implementations, Hard PUFs are implemented directly into the ASIC silicon. By comparison, in the case of FPGAs, Soft PUFs are implemented using a small amount of the FPGA's standard programmable resources, such as Lookup Tables, Registers, and Memories.

II. Related Work

Generally, there are three classes of PUF architectures namely cover-based PUF, delay-based PUF, and memory-based PUF. The first mention of PUF in the literature is that of optical PUF [2] which is cover-based PUF, exploits the randomness in the light scattering particles and the complexity of the interaction between the laser and the particles. After that, several PUF hardware structures have been proposed [2–5]. Most PUFs use conventional silicon techniques so that they do not require any special fabrication process or treatment and can be easily integrated into IC chips. Silicon PUFs exploits manufacturing delay variation of wire to generate a unique challenge-response mapping for each IC. These unique properties of each IC are easy to measure through the circuits but hard to copy without. Unfortunately, recent analysis has demonstrated that those PUF structures are vulnerable to several attack methods including emulation, replay (man-in-the-middle attack), and reverse engineering [7]. Therefore, a dynamic PUF that can alter the CRPs every time the data is modified to prevent the hidden information leaked out is very desirable. Memory-based PUFs exploit the vulnerable balance of SRAM cross-coupled transistors. Uncontrollable random SRAM contents can be generated during power-up. The random contents are then used as PUF signature [6] [7]. The drawback of memory-based PUF is that every memory element generates a fixed one bit signature. Multi-factor authentication protocols, which often use a password and a mobile device, have been explored in prior literature [8,9,10].

III. Proposed Soft PUF Scheme

In this paper we describe authentication solution based on a PUF device that provide stronger security environment. Each user is issued a PUF that aids in authentication and cannot be copied or cloned. The scheme works on three underlying principle that anyone with complete access to the authentication data at the server side and the device itself is still unable to impersonate the user.

There are three principal entities in the scheme: server *S* (or another entity authenticating the user on behalf of the server), user *U,* and device *D.* Before authentication can take place, the user obtains a device with a PUF built into it and enrols himself with the aid of Register protocol with the server. Once the registration is complete, the user will be able to authenticate with the help of the device.

a) *Register:* is a process between *S* and *U,* where the user *U* registers with the server with the aid of *D.* If enrolment is successful, the server obtains and stores a token cred*U* that can be used in subsequent authentications.

Register :

1. Server *S* sends challenge *c* to user *U* along with description of the group G*q*, consisting of a pair (*p*,*q*), and its generator *g*.

2. User *U* sends *H*(c||*pwd*), G*q*, *g*, where *pwd* is a user password, to device *D* for a modified Gen protocol.

3. Device *D* calculates a challenge *d* = *H*(*H*(c||*pwd*), G*q*, *g*) and runs Gen on this

value to obtain response *r*,*P*, *D* then sends to the user (*gr*,*P*).

b) *Authentication:* is a process between *S* and *U*, where *U* uses *D* and *S* uses its stored credentials cred*U* to make its decision to either accept or reject the user.

Authentication :
1. Server *S* sends challenge *c*, G*q*, *g*, *P*, and a nonce *N* to the user *U*.
2. *U* sends (*H*(c||*pwd*), G*q*_,*g*,*P*,*N*) to device *D* for Rep protocol.
3. Device*D* calculates a challenge *d* =*H*(*H*(c||*pwd*),*g*, *p*) and runs Rep on this value
to obtain response *r*. *D* chooses a random value $v \in \mathbf{Z}_q$ and calculates $t = gv$. *D*
then calculates $c\_ = H(g,gr, t,N)$ and $w = v-c\_r \bmod q$, and sends *c*_,*w* to the *U*.
4. User *U* sends these values to the server *S*. *S* calculates $t\_ = gwgrc\_$
and accepts the authentication if $c\_ = H(g,gr, t\_,N)$, and otherwise rejects the value.

In proposed scheme, nowhere it is required to place any sensitive information on the device, to eliminate any possibility of data compromise In fact, our protocols do not require the device to store any information not related to the PUF functionality, which strengthens our design.

There is a strong possibility that an adversary can clone the PUF by obtaining the PUFs response to a challenge, and then build a piece of software that impersonates the user. To mitigate this software cloning attack, proposed scheme requires the authenticator to always have physical access to the PUF in order to authenticate.

IV. New Application Areas

Wide spectrum of security oriented applications is now available for soft PUFs to be grabbed. Here are the few applications.

a) Deployment of Keyed Applications

Currently, in devices such as Xilinx Virtex-4 and Virtex-5, there exists battery-backed key that is used to store Bitstream decryption key. This key cannot be accessed from the programmable fabric. By incorporating Soft PUFs into these devices, system designer can now deploy cryptographic keys/seeds on FPGAs.

b) Activation or deactivation

Different features in FPGA-based can be activated, with activation rights blended in FPGA silicon die. Features like software / firmware running on FPGA-based systems, different modules or features within software / firmware, or remote commands that are directed for a particular FPGA-based system can be made chip specific. This is more secure than traditional anchoring methods such as use of USB dongle, MAC addresses, or similar technologies.

c) Cloning or Counterfeit Detection of FPGA Silicon

Soft PUFs can be used to counter chip counterfeiting or chip cloning. They can be used, for example, to make sure that FPGAs purchased through distributors or secondary markets are in fact authentic and are shipped by actual manufacturing firm.

V. Conclusion

With Soft PUFs, system designers have a new primitive to increase and enhance application space of FPGA-based designs. By having ability to authenticate FPGAs at device level, and ability to store "volatile" keys in these devices, FPGAs have the potential to venture into yet more security applications areas.

References Références Referencias

1. Clark, J., Hengartner, U.: Panic passwords: Authenticating under duress. In: USENIXWorkshop on Hot Topics in Security, Hot Sec 2008 (2008).
2. Guajardo, J., Kumar, S., Schrijen, G.J., Tuyls, P.: Physical unclonable functions and publickey crypto for fpga ip protection. In: International Conference on Field Programmable Logic and Applications, pp. 189–195 (2007).
3. Simpson, E., Schaumont, P.: Offline hardware/software authentication for reconfigurable platforms. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 311–323. Springer, Heidelberg (2006).
4. E. Ozturk, G. Hammouri, and B. Sunar, "Physical Unclonable Function with Tristate Buffers," in Proc. *ISCAS'08*, pp. 3194-3197, 2008.
5. Heike Busch, M. Sotakova, Stefan Katzenbeisser, and R. Sion. The PUF Promise. In 3rd International Conference on Trust and Trustworthy Computing (TRUST 2010), page 17.Springer Lecture Notes in Computer Science, 2010.
6. J. Guajardo, S. Kumar, G. Schrigen, P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection " in Proc. *CHES'07*, pp. 63-80, 2007.
7. Y. Su, J. Holleman and B. Otis, "A D igital 1.6 PJ/bit Chip Identification Circuit Using Process Variations" in Proc. *ISSCC'07*, pp. 15-17, 2007.
8. Park, Y.M., Park, S.K.: Two factor authenticated key exchange (TAKE) protocol in public wireless LANs. IEICE Transactions on Communications E87-B(5), 1382–1385 (2004).
9. Pietro, R.D., Me, G., Strangio, M.: A two-factor mobile authentication scheme for secure financial transactions. In: International Conference on Mobile Business (ICMB 2005), pp. 28–34 (2005).
10. Bhargav-Spantzel, A., Sqicciarini, A., Modi, S., Young, M., Bertino, E., Elliott, S.: Privacy preserving multi-factor authentication with biometrics. Journal of Computer Security 15(5), 529–560 (2007).
11. Stebila, D., Udupi, P., Chang, S.: Multi-factor password-authenticated key exchange. Technical Report ePrint Cryptology Archive 2008/214 (2008).

This page is intentionally left blank