New Paradigms for Access Control in Constrained Environments

Abdelkarim Cherkaoui, Lilian Bossuet, L. Seitz, G. Selander, R. Borgaonkar

New Paradigms for Access Control in Constrained Environments

A. Cherkaoui*, L. Bossuet*, L. Seitz†, G. Selander‡ and R. Borgaonkar§
Hubert Curien Lab* (France), SICS Swedish ICT† (Sweden), Ericsson Research‡ (Sweden), TU Berlin / T-Labs§ (Germany)
Emails: abdelkarim.cherkaoui@univ-st-etienne.fr, lilian.bossuet@univ-st-etienne.fr, ludwig@sics.se,
goran.selander@ericsson.com, ravii@sec.t-labs.tu-berlin.de

***Abstract*—The Internet of Things (IoT) is here, more than 10 billion units are already connected and five times more devices are expected to be deployed in the next five years. Technological standarization and the management and fostering of rapid innovation by governments are among the main challenges of the IoT. However, security and privacy are the key to make the IoT reliable and trusted. Security mechanisms for the IoT should provide features such as scalability, interoperability and lightness. This paper adresses authentication and access control in the frame of the IoT. It presents Physical Unclonable Functions (PUF), which can provide cheap, secure, tamper-proof secret keys to authentify constrained M2M devices. To be successfully used in the IoT context, this technology needs to be embedded in a standardized identity and access management framework. On the other hand, Embedded Subscriber Identity Module (eSIM) can provide cellular connectivity with scalability, interoperability and standard compliant security protocols. The paper discusses an authorization scheme for a constrained resource server taking advantage of PUF and eSIM features. Concrete IoT uses cases are discussed (SCADA and building automation).**

I. Introduction

We evolve because we communicate. Data is interpreted as information, from which we derive a knowledge that translates into wisdom. Considering the impact the Internet already has had on education, communication, business and science, it certainly appears to be one of the most important creations in human history. Now, the evolution of the Internet is leading to a global network of objects, which is commonly refered to as the Internet of Things (IoT). The IoT enables the Internet to reach out to the real world of physical objects by combining their ability to sense, collect data, transmit it, analyze it, and distribute it on a massive scale.

Ultimately, everything would be connected anytime, at anyplace. This convergence of virtual and physical worlds can drastically improve the user's experience, but it also presents several challenges regarding security and privacy, which are among the main barriers for the deployment of IoT on a broad scale [1]. IoT security needs to be garanteed on several levels. Communication with the IoT needs to be encrypted with proven algorithms using keys with high entropy that are securely exchanged between the user and the IoT. The communication channel is usually secured using a symmetric encryption algorithm like AES, while public key encryption is prefered for low data rate communication (*e.g.* key exchange). Ideally, an IoT chip would embed a crypto-processor which performs the encryption tasks and provides secure key management (key generation, key storage, etc).

978-1-4799-5810-8/14/$31.00

Authentication using secret keys stored in non volatile memories presents nowadays many vulnerabilities, principaly due to the development of active attacks (*e.g.* probing) and passive attacks (*e.g.* differential power analysis). Protection mechanisms against these attacks are expensive and not adapted to devices with constrained size and energy. On the other hand, future IoT scenarios would involve billions of heterogeneous devices which some of them maybe reprogrammable. In many cases, non expert users would define policy and permissions for the use of their own resources. Therefore, security mechanisms for the IoT should also provide features such as scalability, interoperability while still being sufficiantly light.

This paper discusses two technologies that, combined together, provide most of the building blocks that meet these requirements: Physical Unclonable Functions (PUF) provide secure, low-cost authentication means in constrained devices while eSIM provide cellular connectivity with the flexibility to change operator or late binding of subscription needed in many IoT use cases. Section II presents the PUF technology and discusses a few design candidates that seem suitable for the IoT use cases. Section III presents eSIM and its features. Section IV describes the identity and access management framework to show how these technologies fit together in a security architecture for IoT devices. Finally, Section V concludes the paper.

II. Physical Unclonable Functions - PUF

Privacy is an important prerequisite in most IoT use cases, especially when the managed data is sensitive. This is true even for a simple device like a sensor: the consequences of a compromised temperature sensor in a power plant can range from costly to disastrously. PUF provide a promising framework for authentication in IoT architectures especially in reconfigurable and/or constrained devices.

A. Privacy by design

Nowadays, traditionnal authentication methods based on secret digital keys often require additionnal protection mechanisms for the key storage. In fact, numerous active and passive attacks which aim at extracting these keys have been developed and reported over the past several years. On the other hand,

FPGA-based reconfigurable devices are increasingly growing in the market of embedded and mobile applications. Integrating secure non-volatile memories in FPGA significantly raises the fabrication overhead and production costs: in fact, most commercial FPGA do not include it. The storage of secret keys in FPGA therefore requires external memory with additionnal contermeasures to protect it against attacks.

The concept of PUF was first introduced by Pappu in [2]. PUF introduce a new paradigm shift from explicitely programmed digital identity to unclonable physical identity. They are mostly electrical constructions that extract a unique secret key from physical parameters of the device: the challenge/response procedure is based on a physical interaction which is theoretically unclonable. Entropy is derived from a physical random variable as the mismatch in transistor attributes (length, width, oxide thickness, etc) due to manufacturing process variability (MPV). The founding principle is that MPV are not controllable (they are not predictable) and not reproducible. Therefore and ideally (if the extraction mechanism is properly designed), a PUF extracts secret keys which are unique (each device has a unique, non reproducible ID based on its unique physical characteristics), random (it is impossible to predict the response of a device to a given challenge), reliable (each device reproduces the same response to a give challenge) and tamper resistant (probing the PUF changes its physical behavior and thus the obtained response). Therefore, a PUF can be seen as a function returning a fingerprint of the device in which it is implemented, or even of a specific part inside the device.

B. A closer look at PUF designs

Traditionnally, silicon based PUF rely on manufacturing process variability (MPV) to generate unique, reliable and unpredictable identifiers. There exist many silicon PUF architectures, but there are two main approaches to extract secrets from MPV: methods based on delay measurements and other methods related to the resolution of a metastability situation. SRAM-PUF [4] and butterfly PUF [5] rely on the settling state of a couple of cross-coupled elements. At the initialization of an SRAM, most cells outputs are biased toward '1' or '0' depending on MPV. The arbiter PUF [3] relies on the race of two events (electrical transitions) in two symmetrical delay lines. The Ring Oscillator based PUF [6] (RO-PUF) leverages the frequency mismatch between several identically designed ring oscillators (RO). Most recent PUF architectures are based on differential measurements in order to improve the responses stability against environmental changes (mainly temperature and voltage). PUF designs are often characterized in terms of intra-device variation (a value close to 0% means that PUF responses are reliable) and inter-device variation (a value close to 50% means that PUF responses are unique). Some PUF designs can provide an additionnal True Random Number Generator (TRNG) function with little design overhead since the entropy extraction methods are very similar to those used usually in PUF, the variable being the source of entropy targetted (MPV for PUF against noise for TRNG). This feature is particulary interesting in constrained devices because it allows to provide high entropy keys for encryption mechanisms with very little design effort (implementing each feature independently would be much more expensive). Table I presents a comparison between four PUF designs in terms of uniqueness, reliability, mathematical unclonability, the ability to provide an additionnal TRNG function and their implementation effort. Intra-device and inter-device variations are provided in [7] for ASIC and FPGA implementations.

TABLE I
COMPARISON OF THE MAIN PUF ARCHITECTURES IN DIGITAL DEVICES (*INTRA-DEVICE AND INTER-DEVICE VARIATIONS HAVE BEEN CHARACTERIZED IN [7], PP = REQUIRES HEAVY POST-PROCESSING, DO = INVOLVES AN IMPORTANT DESIGN OVERHEAD)

	Butterfly PUF	SRAM PUF	Arbiter PUF	RO PUF
Challenge	cell selection	SRAM adress	delay path selection	RO selection
Response	settling state	memory state	delay length	oscillation frequency
Inter-dev. var.*	50%	50%	38%	46%
Intra-dev. var.*	6%	12%	10%	0.5%
Math. clonability	no	no	yes	possible
TRNG	DO and PP	DO and PP	no	DO
Implementation	easy	easy	difficult	easy

Arbiter PUF seem nowadays obsolete considering their low uniqueness and reliability. Their main flaws are the difficulty to place and route identical delay lines which results in a low entropy in the subsequent responses, and therefore a high vulnerability to modeling attacks. This is more especially the case in FPGA in which routing circuitery is often complex and uses active elements such as multiplexors. SRAM and butterfly PUF have remarkable uniqueness properties while being fairly reliable. They can be easily embedded in most targets (using SRAM, flip-flops, latches, bus keepers, etc) and are known to be resistant to modeling attacks. Additional TRNG function can be obtained but at a high cost. In fact, very few memory cells would have unpredictable behavior and there is no prior way to determine which cells should be used for the TRNG. Also, one main barrier for their usage in many of the IoT use cases is their low number of challenge/response pairs.

RO-PUF is reliable and has good uniqueness. Its implementation is straightforward since inverter ring oscillators integrate very well in all ASIC and FPGA design flows. The number of pair of challenge/response is potentially very large (2^n where n is the number of oscillators) although some of them may be correlated. An additionnal TRNG feature can be implemented by integrating a XOR tree at the outputs of the ring oscillators (the size of the design is approximately doubled in the case of rings of tens of elements). Until recent years, RO-PUF was considered as a promising candidate for large scale usage of PUF. Yet, recent studies highlighted two security issues that may change this status: the mutual influence of RO frequencies through supply lines (locking phenomenon) which can be

maliciously exasperated to fault the PUF behavior, and even worse, the possibility of extracting the RO frequencies through contactless electromagnetic charecterization [8] without affecting the PUF behavior. The first case would be simply a denial of service, while the latter could possibly allow to mathematically clone the identifier (even though such attack has not been performed yet).

C. TERO-PUF: a promising PUF candidate ?

The Transient Element Ring Oscillator based PUF (TERO-PUF) is a delay based PUF which has been recently proposed in [9]. The main argument of TERO-PUF is that it reproduces most of RO-PUF features (good uniqueness and reliability, straightforward implementation, large number of challenge/response pairs) while presenting considerably less security flaws and providing the TRNG feature with a very low design effort.

A full TERO-PUF architecture is composed of several TERO loops, whose architecture is described in Fig. 1. Each TERO loop consists of a bistable circuit composed of two intialization stages and 2 branches (ideally symmetrical) of an odd number of inverters. After the initilization, two events (electrical transitions) start propagating across the TERO loop which provokes a periodic oscillation of the output. Due to the charge and discharge phenomena, there occurs a drafting effect where one event closes the distance to the other until they ultimately collide which stops the oscillation. Since the number of oscillations in each TERO loop depends on manufacturing process variability that affects individually each logic cell in the device, it appears natural to use a counter as an entropy extractor. An 8-bit counter is placed at the output of each TERO loop. Challenges consist of selecting two TERO loops. Multiplexors allows to select pairs of TERO-loops whose number of oscillation is compared to provide the subsequent response to the challenge.

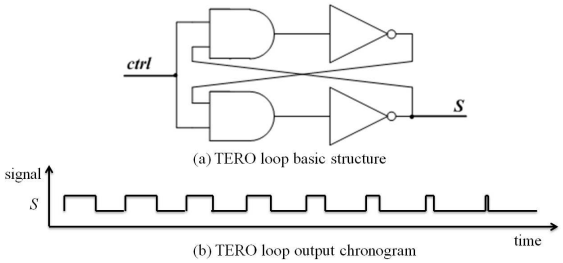

Fig. 1. TERO-PUF basic cell architecture

The number of oscillations in each TERO loop depends on three parameters:

Intrinsic noise: The effective number of oscillations is directly affected by intrinsic noise fluctuations (white noise, flicker noise, etc) in each logic cell of the TERO loop. Therefore, the reliability of each bit of the output comparison decreases from most significant bits (MSB) to least significant bits (LSB).

Manufacturing process variability: The mean number of oscillations depends on manufacturing process variability, it is independent of noise fluctuations.

Charge and discharge parameters: The dependency of the number of oscillations on the charge and discharge parameters is maybe, unexpectedly, the most interesting feature of TERO-PUF. Probing the output signal of a TERO loop would necesseraly change its output capacitance, resulting in a change in its number of oscillations. This features makes the TERO-PUF strongly tamper evident and resistant against active attacks that aim at cloning the identifier. Moreover, TERO-PUF are non vulnerable to contacless electromagnetic characterization methods as for RO-PUF. In fact, these methods are based on frequency analysis, they cannot detect brief transient oscillations in the case of TERO-PUF.

The two MSB of the 8-bit counters were used to build 128-bit, 189-bit and 252-bit signatures which have been evaluated in terms of uniqueness in reliability in 36 PUF instances in Altera Cyclone II FPGA. Results are presented in Table II: they show that TERO-PUF has good uniqueness and reliability properties in FPGA implementations.

TABLE II
UNIQUENESS AND STABILITY OF IDS GENERATED USING A 64-LOOP TERO PUF IN AN ALTERA CYCLONE II FPGA

ID size (bits)	Intra-device variation (%)	Inter-device variation (%)
126	1.73	48.07 %
189	2.07	48.99 %
252	2.75	49.27 %

III. EMBEDDED SIM

Innovation regarding IoT is rapidely increasing, a wider adoption of the IoT requires pressing the capitals and reducing the operational costs. Classical removable SIM (Suscriber Identity Module) cards and their logistic are certainly a barrier for the development of M2M wireless communications. Changing SIM card is problematic in many business cases: many M2M devices are remotely deployed, often hermetically sealed, their after sale location is not known during production and furthermore their product life cycles are lengthy[1] (network operator may change during their life time).

To overcome these issues, the GSMA has developed the new embedded SIM (eSIM) standard to fullfill all the scalability, interoperability and over-the-air (OTA) connectivity requirements for an array of new connected products. eSIM is a non-removable, standard compliant, physical SIM specially designed for M2M devices and which can provide secure connectivity to the IoT. Its main features are:

Secure remote provisioning: provisioning of one or multiple operator credentials into a SIM, remote enablement/disablement of the operator credentials within the SIM (which enables a change of active operator), remote deletion of an operator credentials within a SIM. Remote provisioning can be performed OTA with encrypted packets or using SMS or https connection.

New network elements: Subscription Manager - Data Preparation (SM-DP) used to securely encrypt operator credentials and Subscription Manager - Secure Routing (SM-SR) used to securely deliver the credentials to the SIM and remotely

[1] http://www.gsma.com/connectedliving/embedded-sim/

manage the SIM once they are installed. These network elements make easier selecting and installing different mobile operator credentials once the M2M device has been deployed.

eSIM also provide tamper-proof key storage that can be used to authentify M2M devices, however at higher cost than PUF (especially when the other eSIM services are not required). Therefore, PUF seem suitable for a large number of constrained devices which does not need to be individually connected to the IoT (sensors, actuators, etc), while eSIM would be suitable for a smaller number of more powerful devices (*e.g.* control devices, gateways).

IV. Practical use cases in the frame of the IoT

While PUF can provide a cheap, tamper-proof, secret key which can be used for authentication, this technology needs to be embedded in a standardized identity and access management framework in order to reap its benefits. The target platform that would use PUF would be low cost, mass produced IoT devices with very constrained resources (battery driven, very small volatile and persistent memory, low processor power). These devices would typically interact with more powerful devices, such as gateways, client devices or control units that would be equipped with eSIM. Standardized authentication protocols would use the secret keys provided by either PUF or eSIM to authenticate the different IoT devices in such a framework. Based on that authentication, access control can be performed in order to secure access to the data and functions provided by the IoT devices.

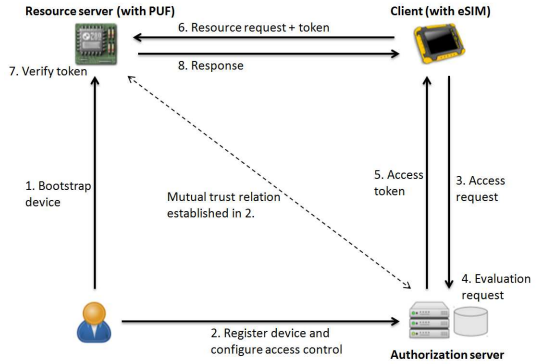

Fig. 2. Authentication and authorization scheme for constrained M2M devices using PUF and eSIM features

In Fig. 2 we present such a framework, which involves four parties: a constrained resource server (the IoT device) which authenticates using PUF, a client with an eSIM who wants to access the resource server, a back-end authorization server, and a resource owner, whose role is limited to the deployment steps which consist of bootstrapping the devices, registering them in the authorization server then setting the authorization policies (steps 1. and 2.). Making access control decisions has been offloaded to the authorization server (which is unconstrained), whereas the resource server only needs to enforce these decisions. This design allows to minimize the functionality that needs to be implemented on the constrained IoT devices. A more detailed description of this design is presented in [10]. This scheme can be applied for a number of uses cases such as building automation and SCADA (Supervisory Control And Data Acquisition). Table III illustrates how PUF and eSIM can be effectively utilized in both those use cases.

TABLE III
PUF and eSIM utilization in two IoT practical use cases

Use case	PUF	eSIM
Building automation	heaters, temperature sensors, smoke detectors, doorlocks, cameras	gateway, e-car
SCADA	sensors and actuators in a refinery, in an oil platform	gateway of the oil platform/rafinery, transport vehicules, petrol stations

V. Conclusion

Security protocols for the IoT need to be flexible and scalable while still being compliant with communication standards. This paper adresses authentication and access control (ACC) in constrained environments connected to the IoT. Two promising technologies are presented (PUF and eSIM) and an ACC framework and use cases are discussed. While PUF are appropriate to authenticate security critical constrained devices, eSIM provide all the credentials to securely connect to the IoT and communicate with it. The proposed setup takes fully advantage of eSIM standard compliance and flexibility features (remote provisionning, late binding, etc) and PUF lightness and security features (tamper evidence, the impossibility to physically clone identifiers, etc).

Acknowledgment

This research work is in the frame of the EIT (European Institute of innovation and Technology) ICT activity 14056.

References

[1] D. Miorandi, S. Sicari, F. Pellegrini, and I. Chlamtac. Internet of Things: Vision, Applications and Research Challenges. Ad Hoc Networks, 10(7):14971516, September 2012.
[2] Ravikanth S. Pappu. Physical one-way functions. PhD Thesis, MIT, 2001.
[3] B. Gassend, D. Lim, D. Clarke, M. Van Dijk, and S. Devadas. Identification and authentication of integrated circuits. Concurrency and Computation: Practice and Experience, 16(11):10771098, 2004.
[4] J. Guajardo, S.S. Kumar, G.J. Schrijen and P. Tulys. FPGA Intrinsic PUFs and Their Use for IP Protection. In Proc. of Int. Conf. on Cryptographic Hardware an Embedded Systems (CHES), Springer, LNCS, vol. 4727, pp. 63-80, 2010.
[5] S.S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen and P. Tulys. Extended Abstract: The Butterfly PUF Protecting IP on every FPGA. In Proc. of Int. Sym. on Hardware-Oriented Security and Trust (HOST), pp. 67-70, 2008.
[6] A. Maiti, J. Casarona, L. McHale and P. Schaumont. A large scale characterization of RO-PUF. In Proc. of Int. Sym. on Hardware-Oriented Security and Trust (HOST), IEEE, pp.94-99, 2010.
[7] Roel Maes, Ingrid Verbauwhede. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. Towards Hardware-Intrinsic Security 2010: 3-37.
[8] P. Bayon, L. Bossuet, A. Aubert, V. Fischer. EM leakage analysis on True Random Number Generator: Frequency and localization retrieval method. In Proc. of Asia-Pacific Int. Symp. And Exh. On Electromagnetic Compatibility (APEMC), 2013.
[9] L. Bossuet, X.T. Ngo , Z. Cherif, V. Fischer. A PUF based on transient effect ring oscillator and insensitive to locking phenomenon. IEEE Trans. Emerg. Top. Comput., 2013.
[10] L. Seitz, G. Selander, C. Gehrmann. Authorization Framework for the Internet-of-Things. In Proc. 4th IEEE International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN '13), 2013.