Provably Unclonable Functions for Future Internet Security Provisioning

Denis Trček

***Abstract*—Security on the internet is a hard issue already nowadays, but due to the proliferation of internet of things (IoT) objects these issues are going to become a real challenge because of their limited computing resources (according to Cisco the number of IoT devices in the internet is going to reach 50 billion by year 2020). Clearly, new approaches to security are therefore needed, and taking into account that authentication is a key service for any kind of security provisioning, provably unique identification is a priority. Moreover, key derivation protocols based on such unique identification techniques should be developed to bridge the gap that will enable new identification services to be put into practice. This paper therefore covers these issues and provides existing state of art in the field. On this basis it presents an improved solution based on PUFs that is suitable for energy constrained IoT devices.**

***Index Terms*—Security, internet of things, provably unclonable functions, lightweight protocols.**

I. Introduction

Security services provisioning starts with proper authentication of involved entities. This is done through verification of factors that may be knowledge based (like passwords), or possessed (like secure tags) or may be characteristics of an entity being authenticated (like biometric elements). These latter elements are the most "authentic" property - so the research in this area is intensively going on for years, and is already producing successful outputs. No wonder that an analog approach is looked for with physical (electronic) devices. But can this be achieved and if, how?

The answer to the first question is clearly "yes". Variability of engineered artefacts is a fact, even for those that are a result of the very same production process, and even the same batch. In case of electronic circuits this variability is due to numerous factors starting with integrated circuits technology and ending with application deployment. The integrated circuits technology related variability starts with local (random) defects in semiconductor wafers, going on with variability of masks and photoresist coating process, photolithography production step, chemical (or plasma) etch step, doping process, hardened resist removal and metal contacts bonding [1]. But then the variability comes also from a certain wiring of a particular IC, where parasitic delays can be identified (that is linked to the above mentioned variability) together with a stage effort delay. This kind of delay can be further broken into logical effort that captures gate's structure properties, and into electrical effort that captures load properties and transistor sizes (it should be noted that multistage networks have also path related efforts, but in order to preserve simplicity and clarity they will not be considered in further text) [2].

As to the second question, there exist various possibilities. A typical option that consists of four XOR gates cascade is given in Fig. 1.

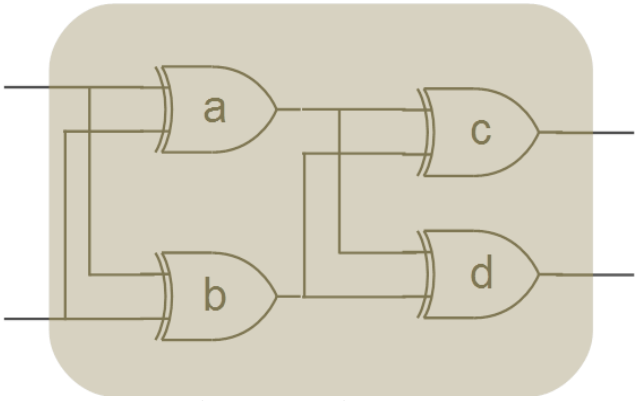

Fig. 1. An example of uniquely identifying timing delays – XOR gates ladder.

This basic structure can be further extended in length and width as needed, resulting in timing delays during switching that are characteristic for each such structure (it should be added that for current CMOS processes and NAND gates architectures these delays are in the range of pico seconds). Thus they are appropriate candidates for so called Provably Unclonable Functions, or PUFs for short.

Although the above ideas are not completely novel there are still many open issues (the first ideas have been published already in the eighties [3], while prototype implementations date some ten years back [4]). And this paper presents some new solutions for this purpose.

II. Overview of the Field

One basic definition for PUFs has been given by Naccache and Fremanteau: "A physically unclonable function is a function, which maps a set of challenges to a set of responses based on intractably complex physical characteristics" [5].

Thus, the whole process starts with finding appropriate intractably complex physical characteristics. And luckily, many possibilities exist for this purpose. One of them are delay-based PUFs like the XOR ladder mentioned above (and an excellent paper providing security services on this basis is [6]), while other PUFs are based on instability of volatile

Manuscript received December 15, 2015; revised May 25, 2016.

Denis Trček is with the Faculty of Computer and Information Science, University of Ljubljana, Večna pot 113, 1000 Ljubljana, Slovenia (e-mail: paper-author@fri.uni-lj.si).

memory cells like flip-flops and SRAMs, and so on. An extensive elaboration of PUFs with focus on RFIDs can be found in [7] – this paper provides also new authentication solution, while some more interesting solutions can be found in [8] (this latter paper gives a solution that can be implemented with less than 1000 gates while the whole structure gives resistance to tampering).

Now to make PUFs operationally deployable, environmental factors (typically this is a temperature or EM interference, but also supply power variations) further influence PUFs, so fuzzy extractors are needed to provide the final authentication results. One such case that does a mapping from a dispersed set of (candidate) values to the final value is given in [9], while additional precision can be provided through extracting full-entropy strings of bits from a partially random source [10].

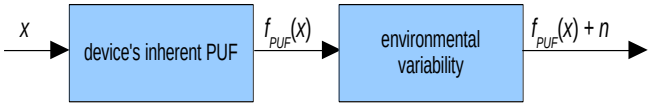

Fig. 2. Inherent PUF's response and PUF's response influenced by environmental variability (noise).

In the rest of the paper the work described in [6] will serve as a basis, while only the pre-environmentally influenced outputs will be considered (see Fig. 2). Let's start an analysis of XOR ladders and time delayed based PUFs by using a simple case presented in Fig. 3 (delays on the right side - the output - are in pico-seconds and they well correspond to major technological processes nowadays).

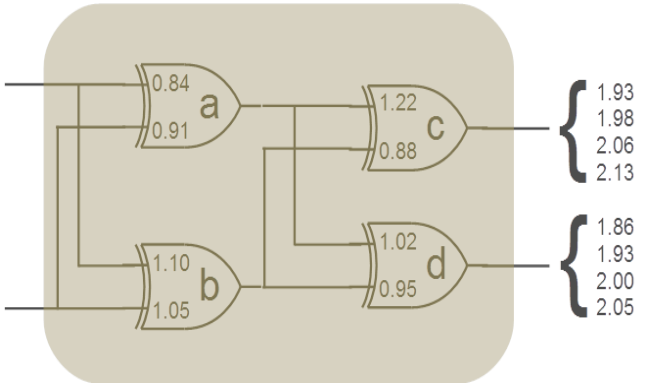

Fig. 3. An example of uniquely identifying timing delays (XOR gates ladder).

Suppose that the initial signal on the input side is 00, so the equilibrium output state is 0. Suppose further that at t = 0 ps the transition from 00 to 01 takes place (the lower line input changes to one). Consequently, the output values remain 00 at 1.86 ps, become momentarily undefined at 1.93 ps, become 11 at 1.98 ps, become 10 at 2.00 ps and remain so at 2.06 ps, go to 00 at 2.06 and finally remain 00 at 2.13 ps. There are 4 different inputs and for each of them there are 3 transitions, while each transition results in 8 output timings (with possible transitions). In total, for the structure in Fig. 3, four different inputs with each having three transitions, while each of these transitions has eight output transitions results, there are in total ninety-six possible transitions values.

If this 2-bit input ladder gets extended by another stage we get an output with time 16 variations for one transition (before reaching the equilibrium state). Again, for four different inputs each of them having three possible transitions this means 192 possible transitions. Adding another stage (and getting a 4 stages ladder) would give 12×32 possible transitions values. Thus a two inputs ladder with n stages has $12 \times 2^{n+1}$ (or $3 \times 2^{n+3}$) possible variations.

Clearly, with a linearly growing cascade of such kind the output grows exponentially when adding new stages, and this gives a good ground for an asymmetric mechanism. In addition, using this building block one can produce sufficiently complex circuits to ensure one-way properties that are needed for secret key derivation – such possible circuits are presented in Fig. 4a and Fig. 4b.

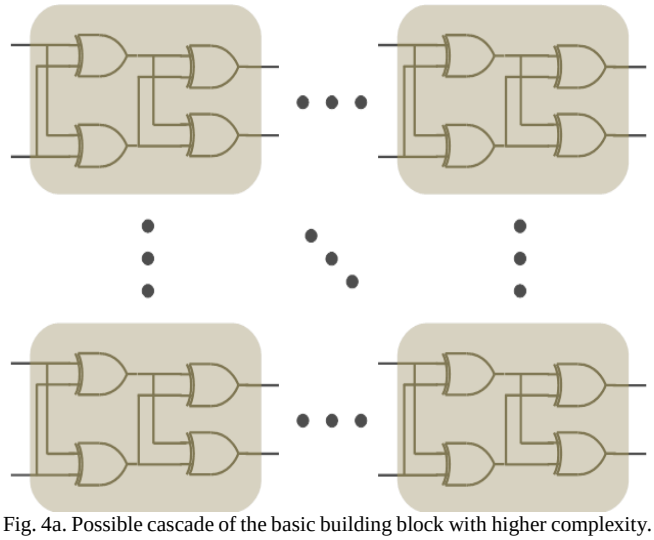

Fig. 4a. Possible cascade of the basic building block with higher complexity.

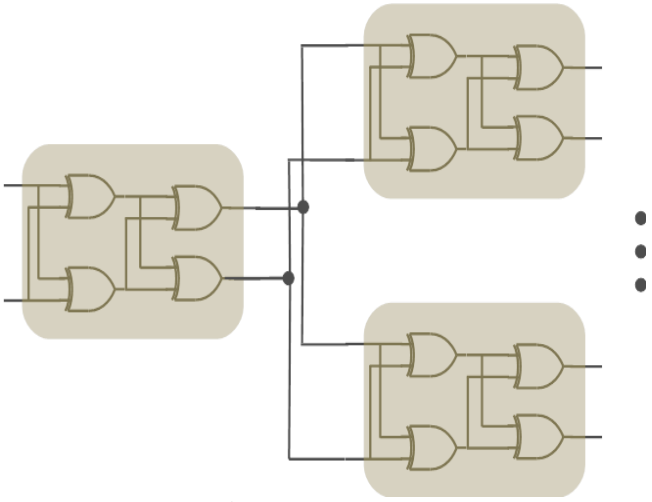

Fig. 4b. Possible cascade of the basic building block with higher complexity.

Now the application given in Fig. 4a is not really one that we would want. Although the number of input bits is increased, the "avalanche" effect (i.e., the diffusion of one bit change on the input and its affection of the output bits) is limited to outputs along the input bits (in pairs). The structure on Fig. 4b solves this problem more appropriately, and we should a principle like this, but take into account the fan-out limitations of a deployed technology. Following this kind of reasoning one can build a structure where the number of input bits is large enough to prevent systematic changes of input bits from 00…0, 00…1, to 11…1 and observe all timing variations of the output. Why is this needed?

Let us first explicitly state one-way properties that we want to implement:

1) Fast forward mapping, FFM, $f(x) = y$ meaning that this mapping can be done computationally fast (with a few resources).
2) Slow reverse mapping, SRM, $f^{-1}(y) = x$, meaning that this mapping is slow (requiring considerably more resources than with fast forward mapping).
3) Conditionally fast reverse mapping, CFRM, $f^{-1}(y)=x|_{known\ p}$, where knowledge of some (secret) parameter p enables fast reverse mapping (requiring only a few resources).

Now the basic protocol description follows. Using PUFs, it is possible to adhere to the above requirements. In principle, each element is physically unclonable due to its structural complexity. Further, its FFM simulation is feasible, while SRM mapping is infeasible except if one possesses the physical object to which a PUF belongs (which equals to knowledge of a secret parameter p), thus enabling CFRM.

Considering now structures from Figs. 4 it is rather straightforward to construct such a cascade that the above criteria are met, and that the following secret key exchange protocol can be implemented:

1) Alice owns a PUF device, while Bob knows the gates characteristics of this device and is able to simulate it. Bob uses certain input x_0 to reach equilibrium, and then makes a transition on the input to x_1, while at the same time he starts a timer. After a randomly chosen amount of time t this simulation yields a certain output y.
2) Bob sends to Alice x_0, t, and y. This way Alice is able to generate all possible values for x_1 (because running a PUF is in the range of pico-seconds), and looks for a match.
3) Next, Bob sends a random challenge r to Alice.
4) Alice encrypts the challenge with the obtained value x_1 and sends it to Bob.
5) Bob checks if the encrypted value r matches the received one. If not, Alice is instructed to go for the next value as long as the obtained secret value can enable proper decryption at Bob's side. This value presents a common secret key between Alice and Bob.

And the final, important remark – it should be ensured that every challenge is unique. This means uniqueness of x_0, t, y and r.

III. Discussion

If Eve is trying to attack the above protocol she has a clear disadvantage compared to Bob. Her calculations (i.e., simulations) require many orders of magnitude more time than those of Bob who has to perform only one simulation. Further, Eve has a significant disadvantage compared to Alice as Alice can run each check in the range of pico-seconds while Eve has to use a few orders of magnitude slower processor and is further pushed back by being forced to check (in the worst case) the whole space of possible values. So if the order of the input values x (and the length of cascades) is sufficiently large, then the gap becomes wider and wider for Eve (compared to Bob and Alice). Effectively, Eve is forced to deal with SRM.

Compared to [6] the presented solution is notably simpler. Clearly, there is a problem with uniform distribution of outputs y, and authors in [6] compensate this with deployment of one way hash functions. However, strong one way hash functions are inherently costly for hardware implementations, thus collisions are taken into account and compensated in our solution at the level of the protocol.

What is important to bear in mind is that practical implementations of solutions like the one above depend very much on precise timing in the range of pico-seconds. Therefore in case of PUFs this means additional timing circuitry will be needed that will enable reading of the ouputs at the specified times.

This is not a trivial task, but it is becoming doable – even network communications experiments nowadays already support timings that are in the range of pico seconds (see details of White Rabbit project in [11]). Traditionally, precision timings and acquisition of rapidly changing signals include techniques like Vernier's techniques (with delay lines, oscillators, time to digital conversion with tapped lines), then time to amplitude with A/D conversion, and interval stretching followed by digital counting [12].

Last but not least, PUFs are very promising technology due to the fact that side channel attacks are much harder than with traditional solutions and can be even prevented.

IV. Conclusions

Emerging internet technologies, in particular Internet of Things (IoT), require new and adapted solutions for security provisioning due to the lack of computational resources. One such approach is enabled through Provably Unclonable Functions, PUFs, which depend on physical characteristics of integrated circuits of IoT devices.

This paper gives an overview of PUFs, related issues, and provides a new solution that requires less computational resources than previously described ones. Such solutions will become an increasingly important approach as they disable also side channel attacks that are a problem with ordinary solutions, while, at the same time, become implementable at a price that makes them suitable even for such devices like radio-frequency identification tags (RFIDs).

Finally, the paper also paves the direction for future research in this area, especially with regard to XOR ladders based PUFs and their optimization in relation to fanout properties of CMOS gates (technology).

Acknowledgment

Author wants to thank ARRS (Slovene research agency) that is financing the research program P2-0359, called Ubiquitous computing, within which this research has been conducted. Further, collaboration within two EU projects should be mentioned: COST Cryptacus project, as well as COST CryptoAction project.

References

[1] C. H. Chenming, Modern Semiconductor Devices for Integrated Circuits, Prentice Hall, New York, 2009.

[2] I. E. Sutherland, B. F. Sproull, and L. D. Harris, *Logical Effort: Designing Fast CMOS Circuits*, Morgan Kaufmann Publishers, Burlington, 1999.
[3] D. Bauder, "An anti-counterfeiting concept for currency systems," Technical report, Sandia National Laboratories, Albuquerque, 1983.
[4] Y. Chen, M. Mihcak, and D. Kirovski, "Certifying authenticity via fiber-infused paper," *ACM SIGecom Exchanges*, vol. 5, no. 3, pp. 29–37, 2005.
[5] D. Naccache and P. Fremanteau, "Unforgeable identification device, identification device reader and method of identification," Patent-EP0583709, 1994.
[6] N. Beckmann and M. Potkonjak, "Hardware-based public-key cryptography with public physically unclonable functions," *Information Hiding*, Springer, 2009, pp. 206-220, LNCS 5806.
[7] S. Kardaş, S. Çelik, M. Yıldız, and A. Levi, "PUF-enhanced offline RFID security and privacy," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 2059-2067, 2012.
[8] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," *Topics in Cryptology* (CT-RSA 2006), Springer, 2006, pp. 115-131, LNCS 3860.
[9] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008.
[10] A. Herrewege *et al*., "Reverse fuzzy extractors: enabling lightweight mutual authentication for PUF-enabled RFIDs," *Financial Cryptography '12*, Springer, 2012, pp. 374-389, LNCS 7397.
[11] P. Moreira, J. Serrano, T. Wlostowski, P. Loschmidt, and G. Gaderer, "White rabbit: Sub-nanosecond timing distribution over Ethernet," in *Proc. 2009 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, 2009, pp. 1-5.
[12] J. Kalisz, "Review of methods for time interval measurements with picosecond resolution," *Metrologia*, vol. 41, no. 1, pp. 17–32, 2004.

Denis Trček is with the Faculty of Computer and Information Science, University of Ljubljana, where he heads the Laboratory of e-media. He has been involved in the field of computer networks and IS security and privacy for over twenty years. He has taken part in various EU and national projects in government, banking and insurance sectors (projects under his supervision total approx. one million EUR). His bibliography includes over one hundred titles, including a monograph published by renowned publisher Springer. He has served (and still serves) as a member of various international bodies and boards (MB of the European Network and Information Security Agency, etc.). His interests include security, trust management, privacy and human factor modeling.