Innovative ATMEGA8 Microcontroler Static Authentication Based on SRAM PUF

Pascal Urien
Telecom ParisTech
19 Place Marguerite Perey 91120 Palaiseau, France
Pascal.Urien@Telecom-Paristech.fr

***Abstract*—In this paper we demonstrate physical static & dynamic authentication for ATMEGA8 microcontrollers used in USB tokens. This authentication is based on SRAM PUF dealing with 5184 bits. We present an original SRAM PUF-Extractor based on software and hardware components, such as SRAM probe software and waveform generator for power supply. We highlight the influence of the supply voltage rising time on the content of SRAM cells used for PUF authentication. Finally we observe that the power supply signal may act as a physical challenge (8-10 bits entropy in our experiment) for SRAM PUF generation, which could be used for dynamic authentication.**

***Keywords*—** PUF; SRAM*;* SPI; Security

I. INTRODUCTION

Physical integrity of electronic devices is a critical challenge for emerging cyber physical systems (CPS). This paper demonstrates static and dynamic authentication, for the ATMEGA8 MCU, used by USBASP tokens detailed in [5].

II. ABOUT SRAM PUF (PHYSICAL UNCLONABLE FUNCTION)

A SRAM memory (see figure 1) is designed with 6 CMOS transistors, and includes two inverters (i_1 and i_2) connected in series (i.e. head to tail). According to [2], if the PMOS transistors are not identical a latching effect occurs as soon as the first of them starts to provide current. Because "biased" memory cells are randomly distributed during the manufacturing process, they may be used for authentication purposes [2]. The paper [4] demonstrates that SRAM cells pattern is dependant from the power supply rising time. Dynamic effects involving transistor capacitance may flip output of "biased" memory. Other physical parameters, such as temperature [3], can also modified PUF parameters.

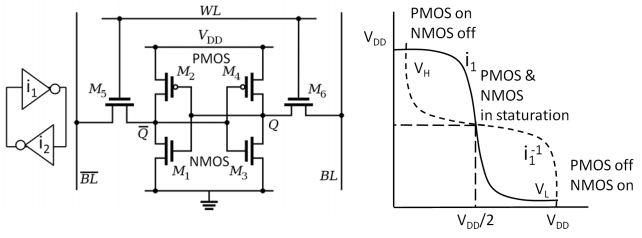

Fig. 1. SRAM cell with 6 CMOS transistors.

III. DESIGNING A SRAM PUF EXTRACTOR

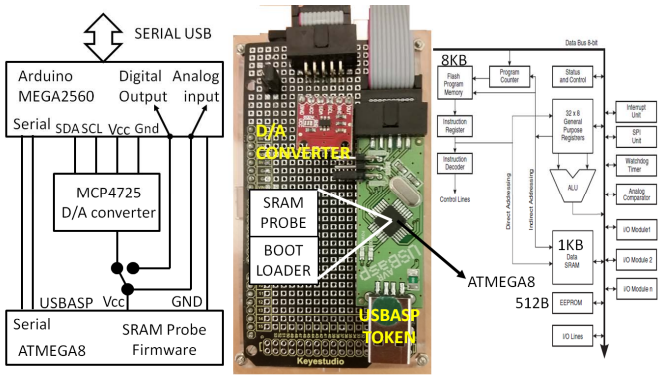

Fig. 2. A SRAM PUF extractor, based on Arduino ATMEGA2560 platform

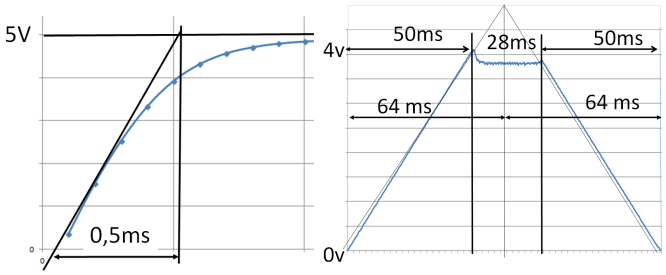

Fig. 3. Power supply voltage waveform. Left using an arduino ATMEGA2560 digital output pin. Right using a D/A converter

The ATMEGA8 8bits processor comprises 8KB FLASH, 1KB SRAM and 512B EEPROM. It has low power consumption; for 12 MHz clock and 5V supply voltage, the supply current is about 12mA. Therefore it is possible to feed the USBASP device from an ATMEGA256 digital output pin, which can deliver up to 40mA with 4,5V voltage. In that case we observe a rising time of about 0,5ms (see figure 3). In order to take into account the voltage rising time effect demonstrated in [4], we use a D/A converter with 12 bits resolution (see figure 2), which provides a maximum output current of 25mA. The Arduino board (see figure 2) manages the SRAM dump. It controls the USBASP device power feeding; it also sends commands over serial link to the SRAM probe application running in the USBASP device.

978-1-7281-3893-0/20/$31.00 ©2020 IEEE

IV. SRAM PUF AUTHENTICATION

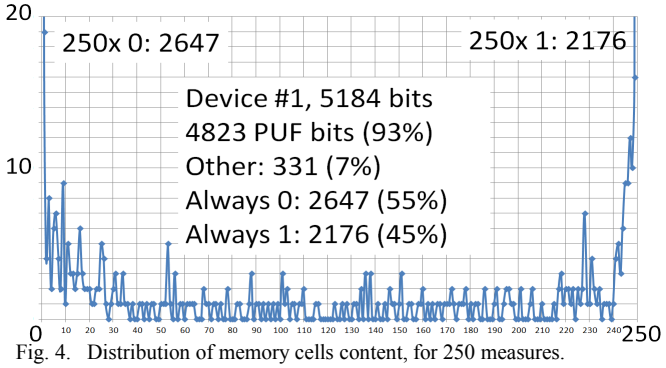

Fig. 4. Distribution of memory cells content, for 250 measures.

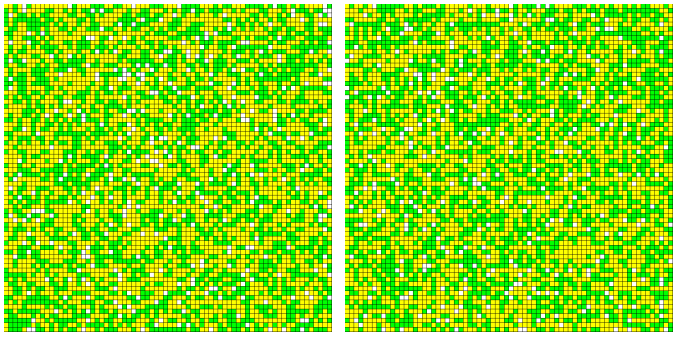

Fig. 5. SRAM-PUF (5184 bits) for two ATMEGA8 & 250 measures, left device #1 (0:2647, 1:2176), right device #2 (0: 2611, 1: 2245). Green points memory cells always seen at one. Yellow points memory cells always seen at zero. White points are noisy memory cells. Common PUF domain:has 2193 with cells distance 51%.

Figure 4 shows an example SRAM bits distribution after 250 measures; 2176 cells are always seen at one, 2647 cells are always seen at zero, and 361 have non constant values (noisy cells). So 93% of memory cells can be used as PUF material. For a device k we note $n(k, i, N) = ID_k^N(i)$ the result of N measures, i being a cell address, and n the number of observed one value ($n \varepsilon [0,N]$). We define three subsets from $ID^N(i)$: H_k^N the list of cell addresses always seen at one, L_k^N the list of cell addresses always seen at zero, and N_k^N the list of cell addresses seen either with zero or one value (noisy cells). We call ***PUF-Domain*** $D_k^N = H_k^N \cup L_k^N$ the set of cell addresses that have N identical values, either one or zero, whose number is noted $\#D_k^N$. Let's consider two PUF-Domains $D^{k1}{}_{N1}$ and $D^{k2}{}_{N2}$. Their common PUF-Domain (see figure 5) is:

$$(H_{k1}^{N1} \cap H_{k2}^{N2}) \cup (L_{k1}^{N1} \cap L_{k2}^{N2}) \cup (H_{k1}^{N1} \cap L_{k2}^{N2}) \cup (L_{k1}^{N1} \cap H_{k2}^{N2})$$

We call flipping cells $F^{k1,k2}{}_{N1,N2}$ the elements of the common PUF-Domain with different values, i.e. whose hamming distance is not null :

$$F^{k1,k2}{}_{N1,N2} = (H_{k1}^{N1} \cap L_{k2}^{N2}) \cup (L_{k1}^{N1} \cap H_{k2}^{N2})$$

We note (1-ε) the probability of a biased cell to get a zero or one value, ε being a small value. Let assume N2 <= N1, N1 being a reference. The number of flipped cells should be about $\varepsilon^{N2} \times \#D^{k1}{}_{N1}$ and therefore decreases rapidly with N2. Consequently a simple algorithm to identify a device ID_{k2}^{N2} according to an ID_{k1}^{N1} reference is the following:

1) take $\varepsilon = 1/N1$, $N2 << N1$ (for example N2=1); 2) check that $\#D^{k1}{}_{N1} < \#D^{k2}{}_{N2}$; 3) the number of flipped cells should be less than $\varepsilon^{N2} \times \#D^{k1}{}_{N1}$.

V. EFFECT OF POWER SUPPLY RAMP

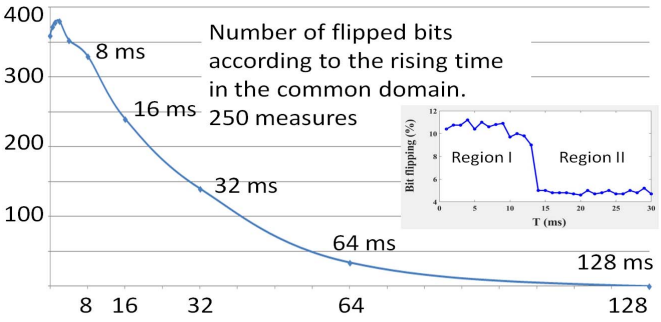

Fig. 6. Relationship between the power supply voltage rising time and the number of fillped bits (device #1), and similar effect (left) from [4].

The paper [4] demonstrated that SRAM cells have two different regions, relying on the supply voltage rising time.. Figure 6 presents our results with different power supply rising time. The number of flipping bits decreases with the rising time. Therefore we fix the reference domain at 1024ms. The transition region is between 8ms and 64ms, the flipping range is about 10% (about 8 bits of entropy). So a rising of one second gives more stable SRAM PUF material.

We build a power supply signal as an odd set of increasing and decreasing ramps. Figure 7 illustrates experiments performed with 64 ms rising/falling time, and power supply signal comprising 1,3,5,7,9 and 11 ramps. We observed no flipping bits, but the number of elements in the common domain decreases. This effect induces a four bits entropy (1,3,5,7 ramps) for the PUF-Domain.

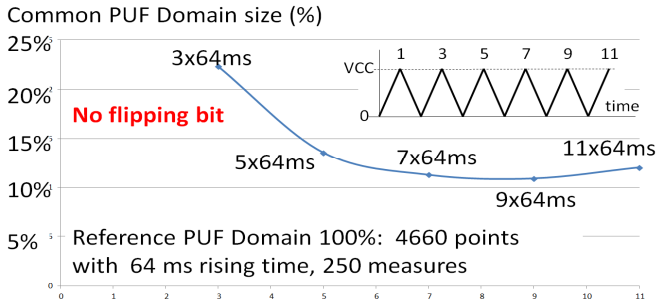

Fig. 7. Relationship between triangular power supply waveform and PUF domain.

VI. REFERENCES

[1] De Holcomb et all, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags", RFID Security, 2007

[2] Herder, C et all, "Physical Unclonable Functions and Applications: A Tutorial", in IEEE Volume 102, Issue: 8, Aug. 2014

[3] Chayanika Roy Chaudhuri, "Effects of Temporal Variations on Delay based Physical Unclonable Functions", Master's Thesis, 2016

[4] Abdelrahman T. Elshafiey et all, "The effect of power supply ramp time on SRAM PUFs", IEEE MWSCAS 2017.

[5] Urien, P; " Integrity Probe: Using Programmer as Root Of Trust For Bare Metal Blockchain Crypto Terminal", Fifth International Conference On Mobile And Secure Services, MobiSecServ2019