Authentication Without Cryptography: Dynamic SRAM PUF Fingerprint

Pascal Urien – June 4th 2020

Certified: Ethereum 10762D67B0C8789AA63F80E2CE27F9EA75EFF89E, nonce 12

Summary: Dedicated power up waveforms creates flipping-bits in SRAM memory, at low voltage (a few hundred mV). Such signals define memory fingerprints, before the processor might work. They can be used as a reliable, low cost way, to perform dynamic authentication for micro-controller unit (MCU) without cryptography means. This effect could become a major technology for cyber security, especially in the IoT context.

When a SRAM is powered up, some bits take a non random value, i.e. they are always found at one or zero [2][3]. Figure 1 shows an example for the USBASP token (that costs about 1$) based on the ATMEGA8 processor embedding a 1KB (1024B) SRAM memory. We built a reference by collecting the SRAM content for 250 powers up. Green points are memory cells seen 250 times at 1, yellow points are memory cells seen 250 times at 0, and white points noisy cells (sometimes at 0 or 1). About 90% of SRAM cells have fix content at power up. So they can be used for static chip authentication purposes.

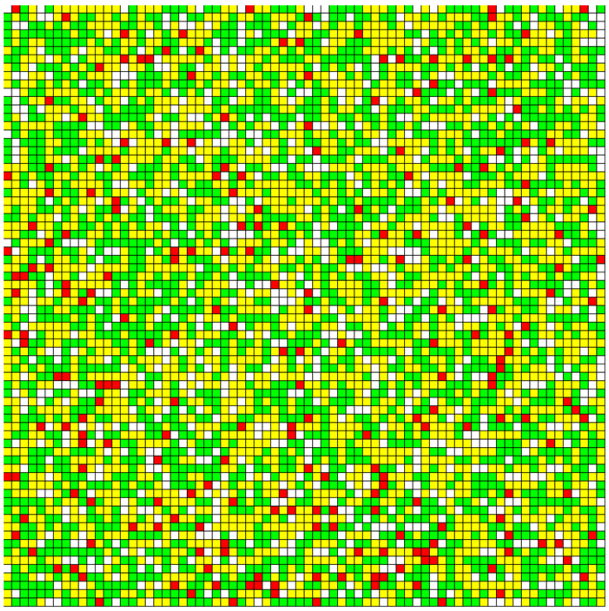

Figure 1. SRAM content after power up ($S^{250}64$ versus $S^{250}1024$)

The voltage waveform may modify the SRAM content. For example a voltage ramp modifies some (k) memory cells, whose content is b^0_k (either 0 or 1) for a slope S0, and $b^1k= (1-b^0_k)$ for slope S1. These cells, called flipping-bits, are colored in red in figure 1 (the slope is Vdd/64 V/ms, and the reference slope is Vdd/1024 V/ms). For our 1KB SRAM, about 200 flipping bits are observed.

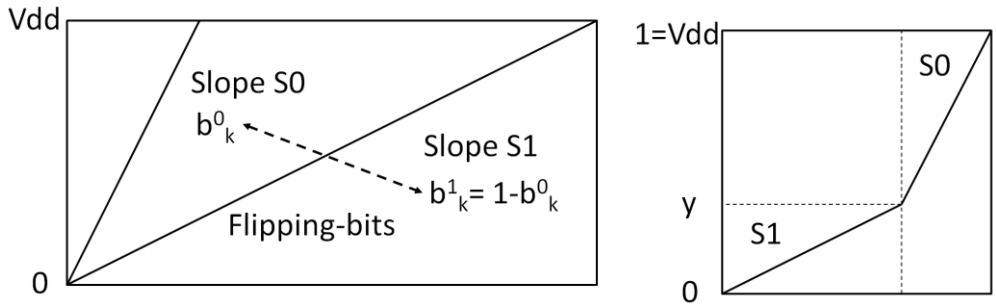

Figure 2. Voltage waveforms

Flipping-bits can be used for dynamics authentication. The voltage waveform (such as S0 or S1, left part of figure 2) is a physical challenge.

Now, suppose we build a voltage waveform that mixes the two slopes (Sy). For voltage values ranging from 0 to y we use slope S1, and for voltage values ranging from y to 1 (1 meaning Vcc=5V) we use slope S0 (see figure 2, right part).

At the end of such power up, we observe a cell content b^y_k. Obviously for y=0 (slope S0) we should find b^0_k, and for y=1 (slope S1) we should find b^1_k (i.e. $1-b^0_k$). This waveform (Sy) is useful only for flipping-bits; otherwise the y parameter would have no effect on memory cells content.

The question we would like to answer is what is the threshold y value (Vth) for which a k SRAM cell content switches from S0 output to the S1 output?. Is there a distribution, in other word is a flipping-bit (k) associated to a pseudo unique threshold value?

We performed 250x25 measures, for y values starting from 1 bit resolution (y=1/4096) to 250 bits resolution (y=250/4096) with an increment step of one bit resolution (1/4096, about 1,2mV=5V/4096). So the same y is associated to N=25 measures, and we store the number of 1 occurrences, ranging from 0 to 25, in $B_k(y)$ records. The Figure 3 shows $B_k(y)$ curves for two flipping-bits. Obviously the region around the threshold is noisy; a small y interval is observed to decrease Bk(y) from 25 to 0. The two threshold points (Vth) are about 2,45% (=100 bits resolution) and 4.30% (=175 bits resolution).

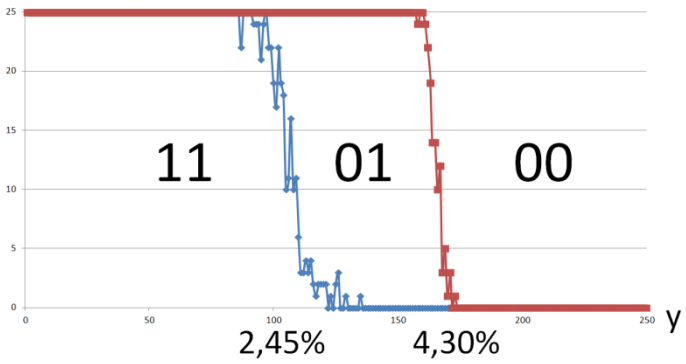

Figure 3. Threshold voltages for two flipping-bits

As illustrated by figure 3, flipping-bits are associated to different threshold values Vth;. n flipping bits, with distinct Vth defines n+1 areas. For example in figure 3 two flipping-bits define three regions from left to right: 11 01 and 00.

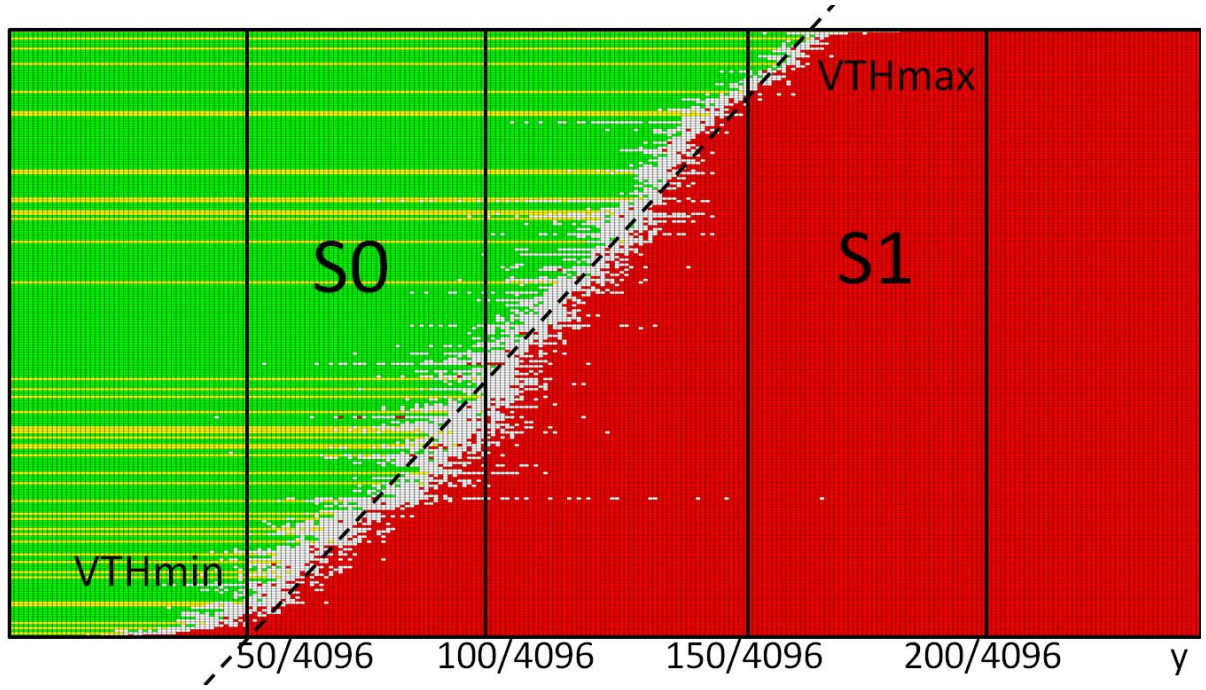

Figure 4. Threshold distribution

Figure 4 presents the threshold distribution. The S0 domain is on the left (green and yellow colors). The S1 domain is on the right (red color). The frontier between the two domains is noisy (white points). Roughly speaking, these domains are separated by a line, for y ranging from VTHmin to VTHmax. So for y within [VTHmin, VTHmax], the Sk signal selects a set of flipping-bits ($\{b^y_k\}$) either in the S0 ($\{b^0_k,\}$) or in the S1 ($\{b^1_k,\}$) domain.

The parameter y is on the abscissa. The memory cells are on the ordinate. A line represents the values of a flipping-bit k (1= b^0_k= green, 0= b^0_k = yellow, noisy= white, red= inverted= b^1_k) according to the parameter y, which varies from 1/4096 to 250/4096.

A column represents the values of the flipping-bits (1= b^0_k= green, 0= b^0_k = yellow, noisy= white, red= inverted= b^1_k) for a given y.

The addresses of the flipping-bits are sorted by increasing values of threshold voltage. Figure 4 shows a quasi-linear distribution for threshold voltages as function of y.

The average threshold value is about 225mV. So flipping-bits state is determined for low voltage values, less than 500mV. For such voltages the processor is not operational. In these conditions, we believe that it is very difficult to design clones, able to sample voltage, in order to set the flipping-bits content accordingly. Without the accurate knowledge of the Sk signal, the probability of selecting a right set of n flipping-bits is 1/(1+n) (as illustrated by figure 3), what enables to define many protocols able to detect cloned devices.

As illustrated by figure 5 the paper [1] confirms that flipping-bits switches at low voltage.

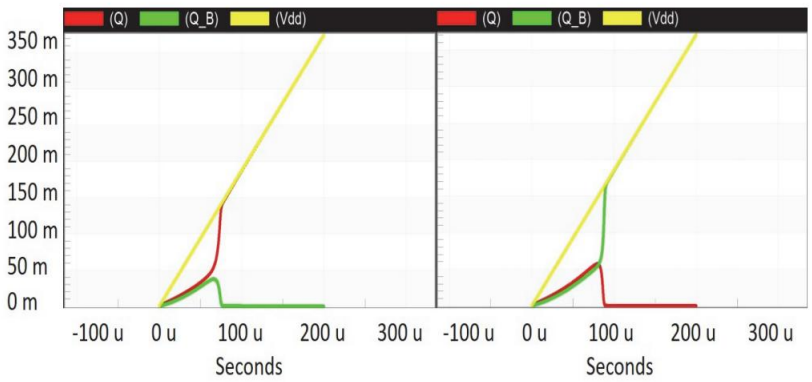

Figure 5. Illustration of Flipping-bits threshold voltage according to [1]

In our experiments we observe that flipping-bits threshold voltages are less than 500mV. At such low voltage, the processor is not working but the SRAM cell states are already set.

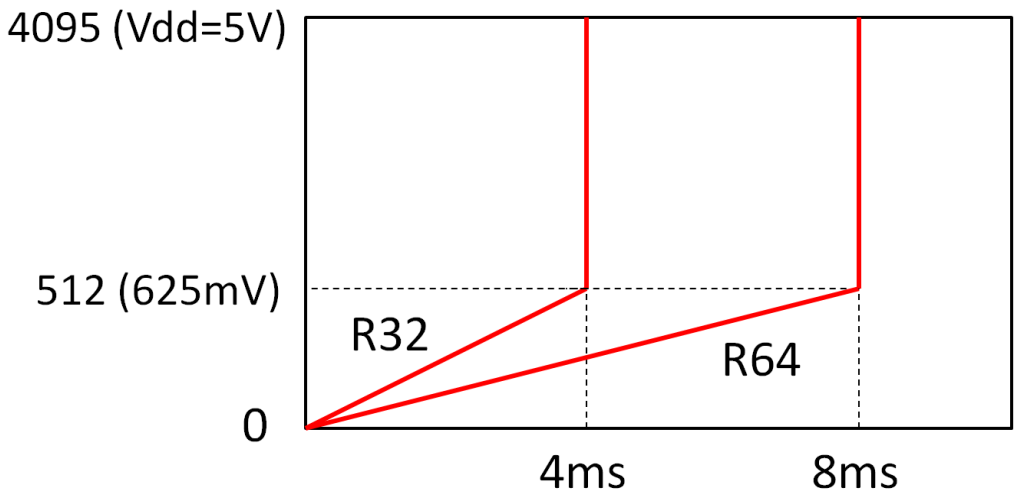

Figure 6. Rx power up waveforms

We use voltage waveforms (Rx) illustrated by figure 6, which comprise two parts: a slope from 0V to 625 mV (i.e. 4096/512 *Vdd), and then a fast rise from 625mV to Vdd. The x parameter is expressed in ms, and the associated slope is Vdd/x in Volt/ms.

We perform a single measure of SRAM content, powered by the Rx (R^1x) signal, and compare the results with references based on 250 measures ($S^{250}x$). For these references the voltage waveform is a single ramp, ranging from 0 to Vdd, whose slope is Vdd/x in Volt/ms (x in millisecond).

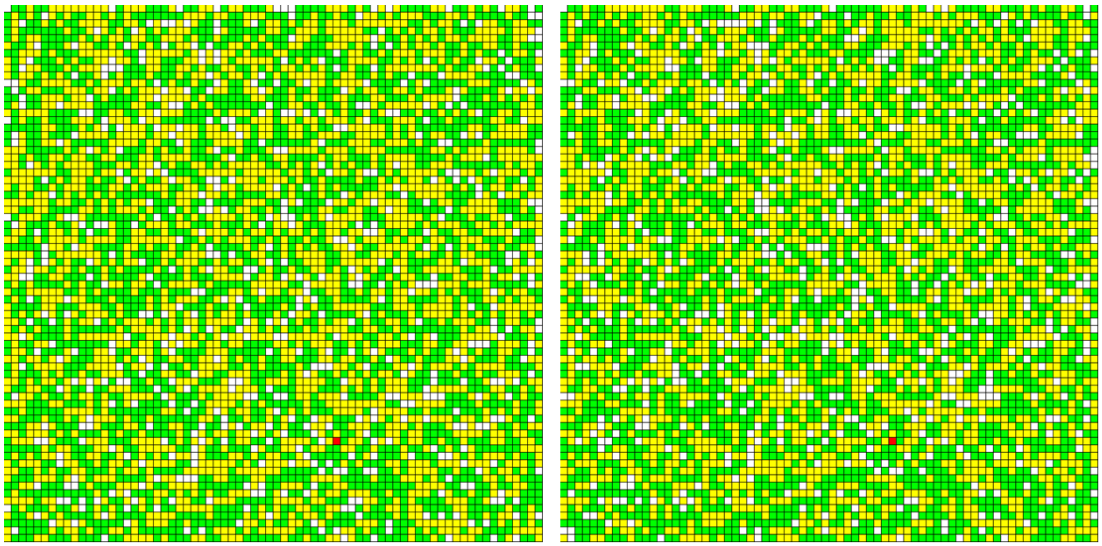

Figure 6. Memory fingerprints (1 measure) for to Rx signal compared to their references (250 measures)

If we compare R^1x to $S^{250}x$ for the same x (slope value) we find at the most one error (see figure 6).

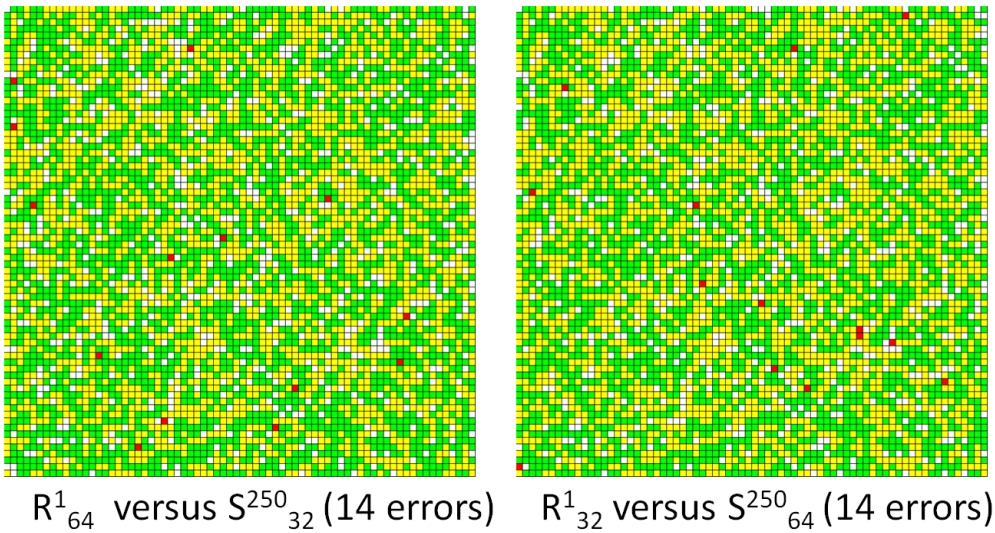

Figure 7. Memory fingerprints (1 measure) for to Rx signal compared to wrong references (250 measures)

If we compare $R^1$64 to S^{250}32 or $R^1$32 to S^{250}64 $R^1$32 we find about 14 errors (see figure 7).

In summary the Rx signal induces flipping-bits for low voltages(less than 500mV), and creates memory fingerprints before the processor might work.

References

[1] A. T. Elshafiey, P. Zarkesh-Ha and J. Trujillo, "The effect of power supply ramp time on SRAM PUFs," 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA, 2017, pp. 946-949, doi: 10.1109/MWSCAS.2017.8053081.

[2] P. Urien, "Innovative ATMEGA8 Microcontroler Static Authentication Based on SRAM PUF," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2020, pp. 1-2, doi: 10.1109/CCNC46108.2020.9045502.

[3] P. Urien, "Time Stamped Bijective MAC and Dynamic PUF Authentication New Directions For IoT Security : Invited Paper," 2020 Sixth International Conference on Mobile And Secure Services (MobiSecServ), Miami Beach, FL, USA, 2020, pp. 1-6, doi: 10.1109/MobiSecServ48690.2020.9042939.