Descrambling of embedded SRAM using a laser probe

S. Chef[1], C.T. Chua[1, 2], J.Y. Tay[1], Y.W. Siah[1, 2], S. Bhasin[1], J. Breier[1] and C.L. Gan[1, 2*]
[1]Temasek Laboratories@NTU, Nanyang Technological University, 50 Nanyang Drive, 637553, Singapore.
[22]School of Material Science and Engineering, Nanyang Technological University, 50 Nanyang Avenue, 639798 Singapore.
[*]Email: CLGan@ntu.edu.sg

Abstract- **Understanding the organization of memory is a mandatory first step in various fields of applications such as failure analysis, defect localization, qualification and testing of space electronics, and security evaluation. For the last category, localization of specific addresses may be used for content estimation or encryption key recovery, with several techniques being reported for this task. In this paper, we discuss the application of laser probing for descrambling memory embedded in 8 bits microcontrollers designed and manufactured by different companies in various technology nodes.**

Keywords *– Laser probing, Descrambling, SRAM, 8 bits Microcontrollers*

I. INTRODUCTION

Microcontrollers are used in a wide range of applications such as automotive electronics, Internet of Things (IoT) and banking systems. For many of these applications, it is critical to ensure that these devices cannot be easily compromised, whether it is at the software or hardware level. In standard architecture, SRAM is used to store variables, data or intermediate computation results. Some microcontrollers even allow the execution of a program from the SRAM in order to fasten execution or minimize power consumption. In the context involving the manipulation of sensitive data such as encryption [1], this area becomes a target of choice for attackers.

During design, memory cells are usually reorganized to answer the need of optimizing required area, power consumption, access time and signal integrity. In addition, bits may be scrambled to avoid probing attacks [2].

Several techniques have been reported to identify the organization of memory, ranging from semi-invasive (e.g. photon emission [3], laser generated bit flip [4]) to destructive processes (e.g. laser thermal damage [5]). For obvious reasons, the latter cannot be considered in the context of security evaluation, where the objective is to bring as little modification to the device under test (DUT) as possible, while keeping it fully functional. For photon emission, as it arises from both dynamic switching of transistors and leakage current, one strategy is to toggle addresses of interest one after another and acquire signals for a long enough duration. The more switches occur during the acquisition time, the better the signal is. For the pulsed laser bit-flip process, the memory array is filled with a known value. A scan of the area of interest is then performed, and after each laser pulse irradiation, a check on the integrity of the data is performed. If a bit flip occurs, then the pixel is labeled with the matching address and bit rank.

We reported in [6] that it is possible that due to the technology and/or circuit architecture, these methods fail to provide accurate localization of the bits of interest. However, if the memory array is big, localization with this process may require several acquisitions as the full memory may not fit in the field of view. Furthermore, modern microcontrollers are designed for very low power consumption applications; meaning the required static and dynamic current consumption is very low. As a consequence, for some devices, emission signals from the memory cell may be too low to be detected, as reported in [6]. For such applications, alternative techniques must be found.

Laser fault injection may offer a more precise localization as charges are directly generated in the memory cell itself. As demonstrated in [6], other effects may also be triggered by this approach. For instance, it can trigger an erroneous detection flag (i.e. transient signal on the power lines [7]) or latch-up. The latter has the potential to be destructive to the DUT if not properly taken care of. Once again, an alternative has to be found to provide a precise localization of the bit cell without triggering side effects.

In the field of failure analysis, laser frequency mapping has been widely used to localize areas and nodes operating at known frequencies [8]. It has recently attracted the attention of the security analysis community thanks to its capabilities to extract periodic signals from complex devices, enabling the recovery of sensitive information such as encryption key or embedded design in FPGA [9, 10].

Most of the descrambling processes reported above relies on the capability to periodically activate SRAM bit cells (either by writing or reading). Considering the nature of the signals involved, it is quite natural to investigate if laser probing can provide a precise understanding of how SRAM is organized and operates.

In this paper, we report on the use of a laser probe as an alternative to precisely localize bits of interest in the SRAM. After giving some background, we first detail the approach and process to carry out the analysis. We then demonstrate proof of concept and discuss its application to different commercial 8 bits microcontrollers manufactured in different technologies. We also share some general consideration regarding the automated descrambling of a complete array.

II. DESCRAMBLING PROCESS USING A LASER PROBE

In this paper, we focus on the study of 8 bits microcontrollers. Depending on the applications, such devices may have a very limited number of I/Os and there is no way to directly access the signals coming in and out of the memory. However, this type of

circuit can be easily reconfigured and is usually designed to be "low-level" programming-friendly (e.g. assembly language). One can then easily consider a short loop program to periodically activate the SRAM. The question arising from this approach is how to activate single bytes of memory? Which mode (i.e. writing, reading, storing) may generate the strongest signal signature in laser frequency mapping? In order to answer these questions, it is mandatory to understand how the signal is generated in laser probing and how SRAM cells operate.

A. Background on laser probing in the field of security analysis

Laser probing, also named laser voltage probing/frequency mapping or electro-optical probing/frequency mapping, is a well-established technique in the field of failure analysis. A detailed presentation of the technique can be found in [8]. As a summary, this technique makes use of the change in the electro-optical properties of material due to a varying electric field. In terms of implementation, a laser irradiates an area of interest and the reflected wave, modulated in phase and amplitude by the change of properties, is acquired by the detection electronics. After conversion from light to an electrical signal, the signal is conveyed to either to a spectrum analyzer/lock-in amplifier or an oscilloscope/digitizer, depending on the domain of analysis (i.e. frequency or time). Due to the magnitude of the observed phenomenon, the signal to noise ratio (SNR) prevents from a single shot observation and periodic test loop coupled with an averaging process have to be implemented to generate observable signals. Some post-acquisition processing schemes have been reported in order to reduce the acquisition time and to improve SNR [11, 12]. However, in the following study we will only consider the standard averaging process for signal estimation.

B. Operating principle of SRAM

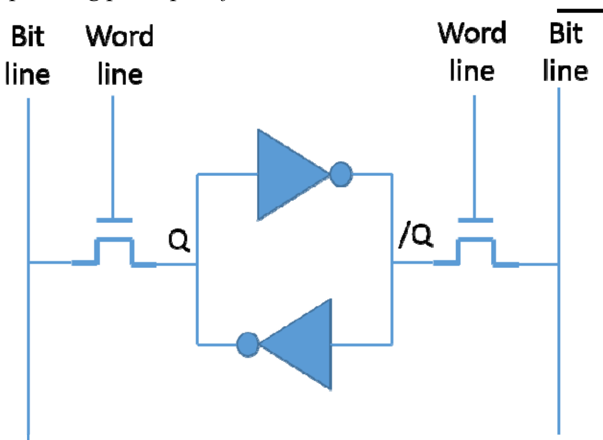


Fig. 1: Standard SRAM Bit Cell Schematic.

SRAM blocks are usually constituted of an array of individual cells with row and column decoders to access each cell and sense amplifier to read or write data. Regardless of the architecture (e.g. 4T, 6T), the cells are constituted of a bistable system (i.e. the double inverters in the Fig. 1) where the bit is stored. Two access transistors controlled by the word line signal enable the access to the bistable system. During a read operation, the bit line is pre-charged to a logic '1' and the word line is set to '1' to switch on the access transistor. Depending on the stored value, the voltage of the bit line on Q or /Q side slightly drops, due to a short circuit to Vss. This drop is then amplified by the sense amplifier to a logic level that can be understood by the remainder of the circuit. During a write operation, wordline enables once again to access the bistable system and the sense amplifiers drive the bit lines to the value to be stored in the cells at Q and /Q. A diagram of the operation process of a standard SRAM cell is shown in Fig. 2.

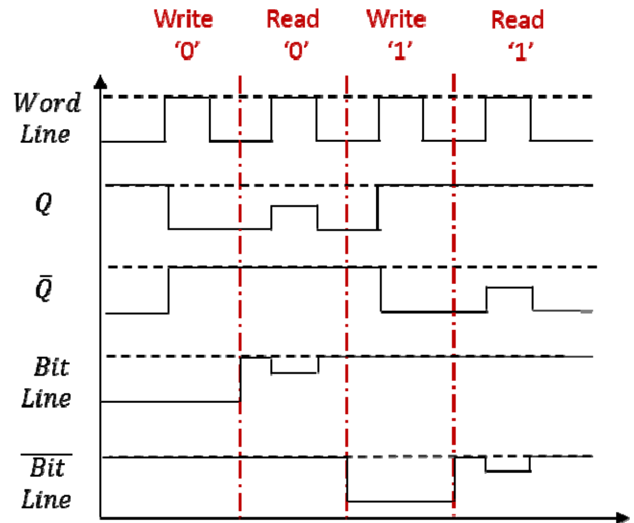


Fig. 2: Chronogram of standard SRAM operation

C. Choice of periodic activation process in SRAM

The bistable system usually involves several transistors. If we consider a standard 6T cell architecture, it consists of two CMOS pairs. During a write operation, the state of four transistors changes, in addition to the two access transistors connected to the word line signal. For the sake of power consumption, they do not stay 'on' once the write operation is completed. At the scale of a whole test loop, the time they are active is therefore very short. Frequency spectrum of such signals is spread among many odds and even harmonics, meaning there will be less energy at the fundamental frequency compared to a square wave with a duty cycle of 50%. On the other hand, if the bistable system state is changed once per loop iteration, each of its transistor exhibits this square wave behavior. The energy of the fundamental harmonic is then expected to be stronger when these transistors are probed. As a conclusion, if frequency mapping is performed while cells are switched once per loop, most of the signals are expected to come from the bistable system for which the energy at this frequency is stronger. Furthermore, since several transistors are involved in the signal generation process, the cumulative area where the optical modulation occurs is larger, generating a stronger signature.

In the case of a reading operation, a voltage switch occurs once again at the access transistors but little change occurs in the bistable system. Only a slight change on the drain voltage of transistors on either Q or /Q side. Similarly to what happens during the writing, the reading is achieved during a short period

of time to minimize power consumption. During this operation, the voltage changes are small, brief compared to the loop duration and impact only a few transistors. Energy at the frequency of interest is expected to be very little and more difficult to detect, as opposed to a write operation. As a conclusion, writing/toggling the content of a cell may offer a better detectability and should be selected for the descrambling process.

All these conclusions are drawn from a general thinking for designs commonly found in literature. If a device embeds a very specific architecture of bit cell, a dedicated analysis may be required in order to develop a more suitable process than the one reported in this study.

C. Descrambling process using a laser probe

Considering the conclusions from the previous section, periodically toggling the content of a SRAM cell may produce a signal with higher SNR in laser frequency mapping. Since there is no direct access to control the SRAM signals through the circuit I/Os, the only approach to perform the toggle is to program the target to do so. Modern microcontrollers can be easily reconfigured through in-situ programming or JTAG. They are also designed to be high-level programming language friendly like C/C++. If such type of language simplifies development, the compiling step may reorganize operations and the physical execution may not follow the exact sequence initially planned. For instance, with the use of “const” variable in the code, the compiler may store the variable in ROM instead of RAM. It is therefore more advisable to use low level language such as assembly.

As mentioned earlier, in laser frequency mapping, it is mandatory to have some knowledge of the operating frequency to be monitored. In order to estimate it, several options may be considered. First, using low-level language, information from the datasheet and knowledge of the clock frequency, one can formulate an estimation of the time required to execute a single writing loop. The SRAM toggle signal period then lasts twice this duration. Another simple solution is to include a trigger signal in the test loop. As this instruction extends the duration of execution of the loop, if the DUT operates at very low frequency, the detectability of the FM signal may be impacted. Indeed, the instrumentation used for detection has a limited bandwidth and the SRAM toggle frequency may fall out of the bandwidth. In such a case, detection scheme like the one reported in [13] may tackle this issue. Alternatively, one can use post acquisition processing such as reported in [14] with laser probe or in [15] with time resolved photon emission to gain some knowledge about the signals met in an area of interest. Finally, one can perform side channel analysis [16], either using an electrical or a magnetic probe.

Based on this, we suggest the following basic steps to localize the memory cells of specific addresses:

1. Write in low level language a loop to toggle specific addresses
2. Estimate time of execution of the loop and the frequency of toggling.
3. Perform frequency mapping at the toggle frequency and localize memory cells of interest.

A process similar to step 3 was reported in FA for the localization of defects in data input/output latches/registers (DQ) [17]. However, the scheme discussed here aims at identifying cells directly in the memory array, not getting signals in the surrounding circuitry and so without any knowledge of the circuit design. Furthermore, the device executes itself the electrical test loop, not an external tester. The process is therefore different in, aims, context and applications.

III. APPLICATION AND RESULTS

A. Experimental Setup

For the following experiments, all the acquisitions have been performed using a Semicaps LTP1100. The system is equipped with a 1319 nm CW laser for laser probing applications. A detailed presentation of the system is available in [18]. The frequency domain analysis is achieved through a Rohde & Schwarz FSL3 spectrum analyzer and the time domain analysis with a Lecroy Wavemaster 808 Zi-B. The objective lens available on the system and the matching estimated spot sizes (FWHM) for a 1319 nm irradiation are reported in Tab. 1.

Tab. 1: Objective lens and theoretical laser spot size at 1319 nm.

Objective Lens	5X	20X	50X	SIL
NA	0.16	0.35	0.4	3.0
Spot size (FWHM) (µm)	6.18	2.83	2.47	0.33
Area (FWHM) (μm^2)	30.0	6.29	4.79	8.55×10^{-2}

B. Application to ATMega 328P embedded on Arduino board

```
EStart :
        SBI 0x05, 5  ;set output to ‘1’
        COM r16
        STS 0x0300,r16 ;Write SRAM
        CBI 0x05, 5   ;set output to ‘0’
        JMP EStart
```

Fig. 3: Test loop program for localizing SRAM bytes in ATMega328P.

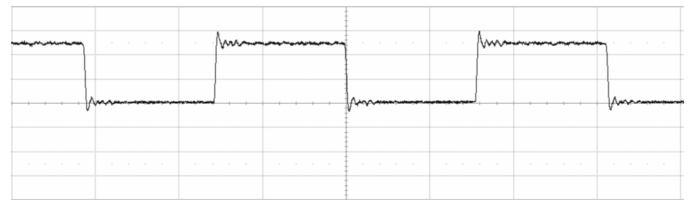
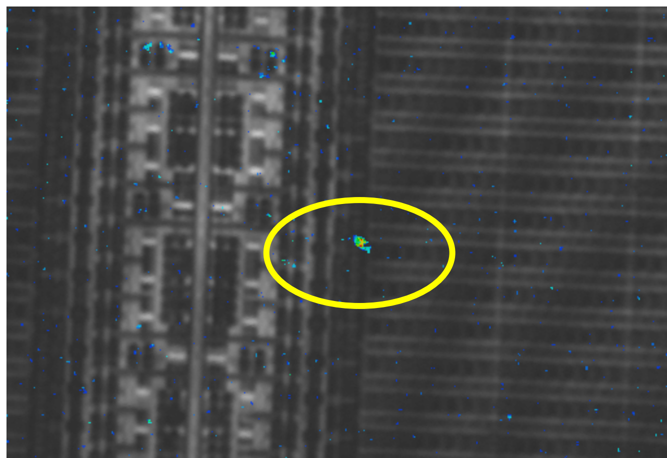
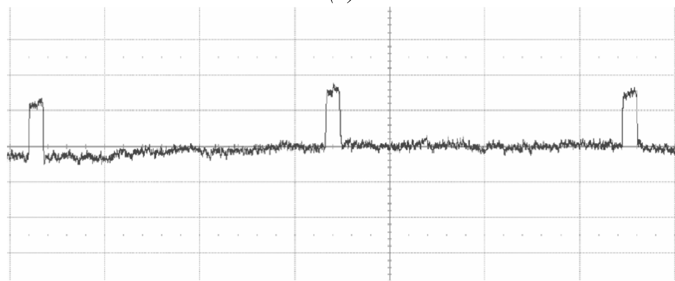


Fig. 4: Flag signal to monitor the duration of the test loop. Time Scale: 200 ns/div. Vertical Scale: 2 V/div.

The process was first tested on an ATMega328P embedded on an Arduino Uno board. The device was reverse soldered to access from the backside. The embedded code was written in AVR assembly to execute a toggle at the address 0x300 (assembly code in Fig. 3). At the beginning of the loop, one output was switched to '1' before the writing operation. The output was released once the writing was completed. A screen copy of the output signal is available in Fig. 4. The duration of execution of one loop is estimated to be close to 620 ns (equivalent frequency 1.6 MHz) when a clock frequency of 16 MHz was provided to the circuit, so the SRAM toggle frequency is estimated to be 800 kHz.



(a)



(b)

Fig. 5: a) Frequency mapping at ATMega328P at the frequency of execution of a loop. Image acquired with the 50X objective lens equipped, (b) Laser timing probing signal at the spot circled in yellow. Time scale: 200 ns/div. Vertical Scale: 100 µV/div.

In order to have an idea of the area where the byte of the address 0x300 is located, a first scan was performed at 1.6 MHz. If the hypothesis formulated in the section II.C is correct, some node related to the word line signal should show some signal in the periphery of the array. It is supposed to be switched on and off at every iteration of the loop. We can see from Fig. 5 (a) a spot of signal at the center of the image, circled in yellow. Time domain analysis performed with the laser probe shows that this node is active during approximately 30 ns (Fig. 5 (b)). This value matches with half-a-clock period and demonstrates how brief the execution of an operation is. This confirms that only focusing on the signals related to the wordline signal (e.g. like during a read operation) may be more difficult to detect than a change of the bistable state.

A second frequency mapping was performed at 800 kHz. Fig. 6 shows the overlay of the frequency mapping signal over the device micrograph. Memory cells localized by laser probing are circled in yellow. Due to the limited field of view and the architecture of array, not all of the bits from a single byte fit into the image. This demonstrates that the process developed in the previous section works in this case.

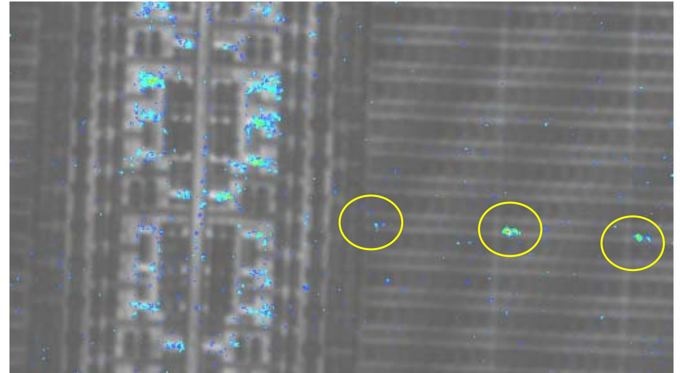


Fig. 6: Overlay of frequency mapping signal at 800 kHz on device micrograph while the ATMega328P was clocked at 4 MHz. Images acquired with the 50x objective lens, during a toggle operation at the address 0x300. Only the first three bits are shown (Circled in yellow).

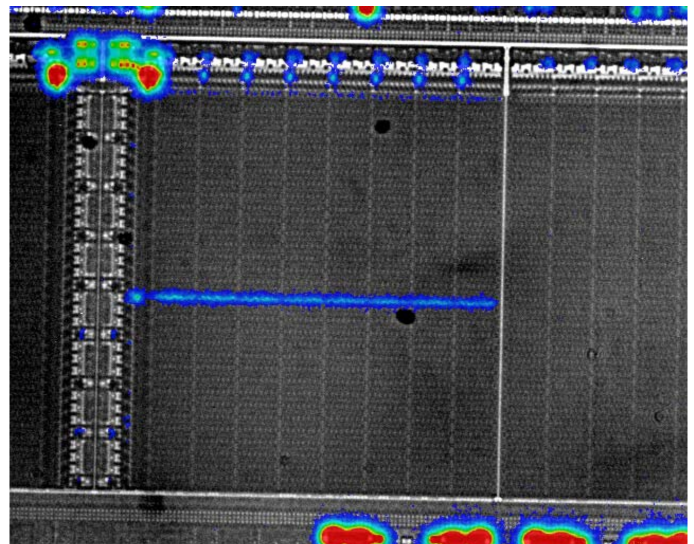


Fig. 7: Photon emission signal superimposed over device micrograph while toggle was performed at the address 0x300 in ATMega328. Acquisition was performed using the 20X objective of the Semicaps SOM 1100, device biased at 5 V, clock frequency = 20 MHz.

In order to offer some reference, the photon emission signal of the toggle of the address 0x300 is reported in Fig. 7. In this picture, a strong emission signal can be seen in the memory array. The emission can be observed from the full row. At the top of the image, seven emission spots can be seen; they match with the activation of bit lines, the eighth one being covered by emission from its surrounding nodes. From this image, a rough estimation of the bits locations of the specific address can be achieved by looking at the intersection between wordline signal and bitline signals, but it is not as precise as the signal coming from the laser probe shown in Fig. 6.

IV. Discussion

A. Limits of applicability of laser probing

Commercial offers in the market of 8 bits microcontrollers is large and circuits vary in terms of technologies and architectures. In view of this, it is legitimate to wonder if the strategy mentioned above is valid for any microcontrollers or were the previous results specific? In other words, can it work on any circuit? In order to evaluate it, we applied the process to various devices.

Tab. 2: Characteristics of device tested in the comparative study. The bit cell area is estimated by dividing measured SRAM area by the number of bits.

Ref.	A	B	C	D
SRAM size (bytes)	68	256	2000	1000
SRAM area (μm^2)	122,500	95,400	486,400	36,000
Bit cell area (μm^2)	225	47	30	4.5

Four devices were selected (Tab. 2): A: Microchip PIC16F84A [19] and B: PIC16F688 [20], C: Atmel ATMega328/P [21], D: STMicroelectronics STM8S103F3 [22]. For each device, a specific testboard was designed for backside testing. Samples were prepared for backside analysis using a standard procedure (laser decapsulation + substrate thinning and polishing).

Since information about technology process is not always available, we estimated the level of integration by measuring the area of the SRAM array by IR imaging. Using the SRAM size from datasheet, we estimated the area occupied by one bit cell. It is important to note that this method is an over simplification since there will be room between bits cells to avoid coupling or to insert contact for signals routing (e.g. Vdd, Vss, etc). For instance, after delayering, we reported in [6] measuring a bit cell area of approximately 25 μm^2 for the PIC16F688 when we estimate here an area of 47 μm^2. Results are reported in Tab. 2 and show that for the four devices, there is a difference of scale. Sample A is the least integrated while D is the one with the smallest area per bit cell.

For the circuit A, B and C, toggle signal of single bit cell was detected. For the sake of space, image results are not reported in this paper. For circuit D, nothing was detected in frequency mapping, although photon emission showed signal from a full row (yellow square box in Fig. 8). At this stage, it is unclear why the approach failed for this particular device. There are several hypothesis such as:

- The cell architecture. As detailed in section II, the approach has been designed for standard cell. It is unknown if this device has a particular design working in a completely different way.
- Size of transistors generating the signal. Bit cells may be built with a few transistors and this device is the most integrated one (Tab. 2), offering the smallest area of electro-optical modulation. Furthermore, the bit cell area may be smaller than the spot size using standard objective lens (Tab. 1). Considering the size of the dice and package, SIL cannot be used here.

This result shows nonetheless that no technique is superior to all of the others for descrambling. It suggests on the contrary that all of them brings complementary information and successful analysis may rely on a combination of techniques.

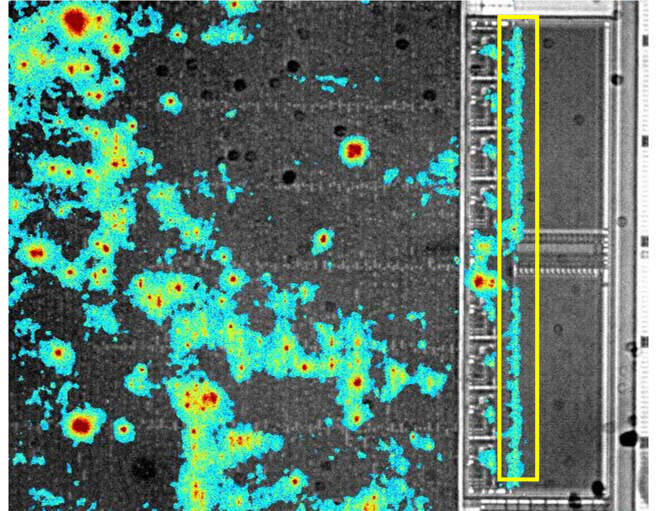


Fig. 8: Photon emission image from STM8S103F3 when the address 0x10 of the SRAM toggles. The yellow box highlights the area from SRAM emitting when the toggle is performed.

B. Process automation for the mapping of complete array

In the application section, we only report on experiments performed with single address toggling. It showed that indeed the process can accomplish a precise detection of single bit cell. Moving forward from this, it is legitimate to wonder if the process can be applied to a full SRAM descrambling, similarly to what has been reported in [3] with photon emission. Experiments showed that using the standard detection process (averaging), several frames were required to distinguish the signal of interest from the background. A manual process, where users would change by "hand" the address to toggle may not be very realistic and this triggers the question of automation of the process.

From the scheme detailed in section II.C, a possible flow chart for process automation is introduced in Fig.9. It is basically constituted of the same steps except address to localize may change after each iteration. In case one acquisition does not provide any signal source, operator may wish to perform another mapping for the same address using a different set of parameters (e.g. laser energy, reference level on the spectrum analyzer, number of samples collected, number of frames to acquire, etc). This extra step adds a machine vision problem where one has to be able to classify images between the ones with signal and the ones where only noise can be seen. In addition, considering the number of parameters that can be modified in the acquisition setup, this task is not a trivial one

and relies on the experience of the operator. Finally, as long as acquisition duration is involved, several mechanical challenges and constraints may arise such as securing the DUT or minimizing vibrations or the drifting of the optical system (loss of focus). Regarding the latter, measure of focus as described in [23] may tackle this issue. As a conclusion, even if the process for SRAM descrambling is constituted of a few basic steps, a full automation for the mapping of a complete memory array is a more complex task requiring some R&D work in various fields of engineering.

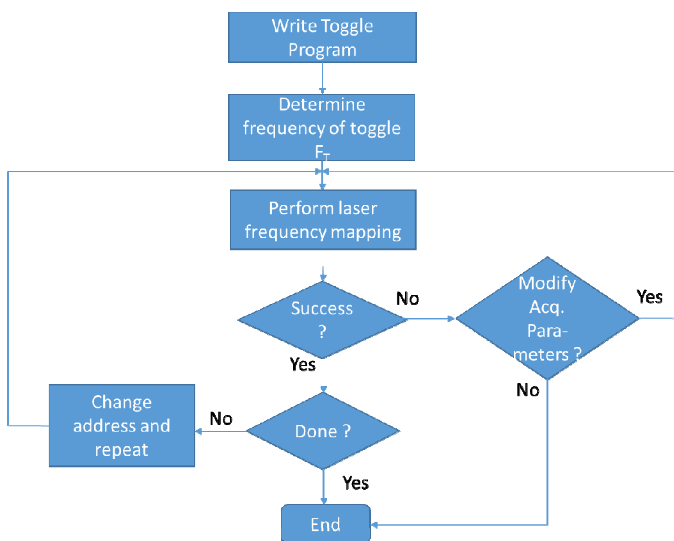


Fig.9: Flow chart of descrambling process using a laser probe.

V. Conclusion

Understanding how memory cells are organized is a non-trivial task and mandatory in many applications and analysis. In this paper, we demonstrated how frequency mapping using a laser probe can bring additional capabilities to perform this task. For several microcontrollers from various manufacturers, single bit cells have been localized. Experiments also showed that this technique may not necessarily provide results on any device and highlight complementarity between techniques. At this stage, the reason why the technique fails on certain devices is still under investigation. Finally, if laser probing allows to perform some precise localization, a full array descrambling appears to be challenging as it involves several more R&D work, especially in computer vision.

References

[1] J. Krämer, "Why Cryptography Should Not Rely on Physical Attack Complexity", *PhD Dissertation Thesis*, Technischen Universtät Berlin, 2015

[2] W. Rankl and W. Effing, "Smart Card Handcook", 4dn, Wiley, 2010

[3] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, J.P. Seifert, "Simple Photonics Emission Analysis of AES", *Journal of Cryptographic Engineering*, vol. 3, no. 1, pp. 3-15, 2013.

[4] S. Buchner, D. McMorrow, J. Melinger and A.B. Camdbell, "Laboratory Tests for Single Event Effects", *IEEE Transactions on Nuclear Science*, vol. 43, no. 2, pp. 678-686, 1996.

[5] W. C. H. Lee, L. Saku, W. K. Ong, Y.M. Kian, F.Y. Ren, "Memory Address Verification Using NIR Laser", *ISTFA 2014: Conference Proceedings from the International Symposium for Testing and Failure Analysis*, pp. 374-378, 2014.

[6] S. Chef, C.T. Chua, Y.W. Siah, P. Perdu, S. H. Tan, L.S. Koh and C.L. Gan, "VLSI for Space Applications: Single Event Effect Investigation and Optical Analysis on an Integrated Laser Platform ", *ISTFA 2017: Conference Proceedings from the International Symposium for Testing and Failure Analysis*, pp. 621-630, 2017.

[7] R.A.C. Viera, J.M. Dutertre, R. Possamai Bastos, P. Maurine, "Role of Laser Induced IR Drops in the occurrence of Faults: Assessment and Simulation", *2017 Euromicro Conference on Digital System Design (DSD)*, pp. 252-259, 2017.

[8] U. Kindereit, "Fundamental and Future Applications Laser Voltage Probing", 2014 *IEEE International Reliability Physics Symposium*, 3F.1.1-3F.1.11, 2014.

[9] H. Lohrke, S. Tajik, C. Boit, J.P. Seifert, "Contactless probing of Secret Data on FPGAs", *International Conference on Cryptographic Hardware and Embedded Systems*, pp. 147-167, 2016.

[10] S. Tajik, H. Lohrke, J.P. Seifert, C. Boit, "On the power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs", *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1661-1674, 2017.

[11] E. Matlin, N. Troy, D. Stoker, "Imaging Activity in Integrated Circuits" in 2014 *International Conference on Image Processing (ICIP)*, pp. 5821-5825, 2014.

[12] A. Boscaro, S. Jacquir, K. Sanchez, P. Perdu, S. Binczak, Improvement of Signal to Noise Ratio in Electro-Optical Probing Technique by Wavelet Filtering, *Microelectronics Reliability*, vol. 55, no. 9, pp. 1585-1591, 2015.

[13] K. Sanchez, K. Melendez, P.Perdu, "Method and device for extracting a low-frequency wave form from an electro-optical component", *Patent WO2015071582A1*, 2015.

[14] A. Boscaro, S. Jacquir, K. Melendez, K. Sanchez, P. Perdu, S. Binczak, "Automatic process for time-frequency scan of VLSI", *Microelectronics Reliability*, vol. 64, pp. 299-305, 2016.

[15] S. Chef, S. Jacquir, K. Sanchez, P. Perdu, S. Binczak, C.L. Gan, "Unsupervised learning for signal mapping in dynamic photon emission", *Microelectronics Reliability*, vol. 55, no.9-10, pp. 1564-1568, 2015.

[16] M. Joye, F. Olivier, "Side-Channel Analysis", *Encyclopedia of Cryptography and Security*, pp. 571-571, 2005.

[17] K.A. Serrels, A. Kalarikkal, A.M. Jakati, D. Dabney, "Fault Isolation of DQ Failure in 14 nm SRAM using Laser Voltage Imaging and Probing", *ISTFA 2016: Conference Proceedings from the 42nd International Symposium for Testing and Failure Analysis*, 2016.

[18] L.S. Koh, H. Marks, L.K. Ross, C.M. Chua, J.C.H. Phang, "Laser Timing Probe with Frequency Mapping for Locating Signal Maxima", *ISTFA 2009: Conference Proceedings from the 35th International Symposium for Testing and Failure Analysis*, pp. 33-37, 2009.

[19] Microchip Technology Inc, "PIC16F84A datasheet", Ver. DS35007C, 2001-2013.

[20] Microchip Technology Inc, "PIC16F688 datasheet", Ver. DS41203E, 2009.

[21] Atmel, "ATMega328/P datasheet", Ver. 42735B, 11/2016.

[22] STMicroelectronics, "STM8S103F2 STM8S103F3 STM8S103K3 datasheet", DocID 15441, Rev. 14, 02/2017.

[23] S. Chef, B. Billiot, S. Jacquir, K. Sanchez, P.Perdu, S. Binczak, "Pattern Image Enhancement by Extended Depth of Field", *Microelectronics Reliability*, vol. 54, no. 9-11, pp. 2099-2014, 2014.