Microcontroller Sensitivity to Fault-Injection Induced by Near-Field Electromagnetic Interference

Ludovic Claudepierre, Philippe Besnier

Microcontroller Sensitivity to Fault-Injection Induced by Near-Field Electromagnetic Interference

Ludovic Claudepierre
INRIA

F-35000 Rennes, France
ludovic.claudepierre@inria.fr

Philippe Besnier
INSA Rennes, CNRS, IETR - UMR 6164

F-35000 Rennes, France
philippe.besnier@insa-rennes.fr

***Abstract*—This communication deals with fault-injection induced by a source of radiated electromagnetic field at near-field distance of a microcontroller. We show that software execution is altered at targeted instructions if the radiating probe is located above the phase-locked loop device driving the clock tree. Furthermore, the fault-injection rate is analyzed for a pulse-modulated sine wave. The higher rate is obtained within a frequency range that likely corresponds to the upper spectrum associated to the rate of change of voltages / currents of the microcontroller associated with its semiconductor technology.**

***Index Terms*—fault-injection, near-field, radiated immunity**

I. Introduction

Fault injection is a classical technique used since the 60's. The original aim was to simulate the cosmic radiation and its effects on the embedded equipment in a space environment [1]. Using such a technique to attack cryptographic algorithms has been proposed in 1997 by Biham *et al.* [2] and by Boneh *et al.* [3].

Four different methods are commonly used to make fault injection. Firstly laser injection may be used. It requires to accurately point a laser on a precise location on the chip but allows a great control of the induced perturbation on the device, with the possibility in some cases to choose the transistor to pertubate. This is an invasive attack that requires the exposure of the silicon part of the chip. Secondly, direct injection of electrical perturbation within the circuit may be achieved. This technique is free of all coupling problems but requires direct access on the board to the electric lines which is hard to obtain without damaging the hardware. Moreover, this way of injection is far less precise, the perturbation effect is global. Thirdly, the clock glitch is a way to disturb circuit behaviour through the clock line. It can be realized by changing the duration of one clock period. This technique requires an access to the clock signal. Fourthly, the electromagnetic injection (EMI), which is the topic of this work, is a non-invasive way of attacking the chip.

In case of EMI, an electromagnetic probe is placed at close proximity of the chip (in the reactive near-field range), and a signal is generated at the precise time where a fault is desired. Moreover, the spatial location of the probe above the chip is crucial. The nature of the electromagnetic waveform plays a key role for the efficiency of the attack. The common parameter of all the previous physical attack techniques remains the need for timing accuracy of the disruptive emission in order to target the critical software instruction.

The rate of success of a fault injection can be crucial for an effective attack for two reasons: first, every injection is a risk for the attacker to be detected by some countermeasures. Second, in a personal identification number (PIN) code attack for example, the attacker has only three attempts to provide the right key, so every try has to be exploited for the attack.

This communication proposes several ways to improve the success rate of fault injection by electromagnetic radiation. The test bench used for those tests is described in section II. In section IV, explanations on the preferred location for an efficient EMI are given presuming on the phase-locked loop (PLL) high susceptibility to that disruption, proven in section III. Finally, through a parametric analysis on the waveform, key parameters are highlighted to optimize the injection efficiency.

II. Test bench description

A. Hardware

Fig. 1: Test bench for fault attacks by electromagnetic injection.

The targeted microcontroller is the STM32F100RB, embedding an ARM-cortex-M3 core running at 24 MHz. The test-bench (Figure 1) is composed of a generation chain with a Keysight 33509B pulse generator, a Keysight 81160A signal generator and a Milmega 80RF1000-175 power amplifier. The so produced signal, with high power, is radiated through a Langer R0.3-3 probe located just above the surface of the chip.

The communication between the computer and the application on the chip is realized by a UART (Universal Asynchronous Receiver Transmitter) connection. The JTAG (Joint

Test Action Group) interface ensures the debug access on the board and allows to upload the firmware.

B. Software

The targeted firmware, uploaded on the chip for the experiments, send a signal on an output pin of the board to trigger the injection. The clock signal is outed on another pin of the board and displayed on the oscilloscope. This firmware is a dedicated program where a single instruction, the one under investigation, is isolated to ensure no side effect.

Listing 1: Assembly code for the targeted instruction

```
asm_ldr:
nop
nop
nop
nop
nop
nop
ldr R2,[R0,#4] ;/* load value in R2 from the address R0+4*/
nop
nop
nop
nop
nop
nop
mov R0,R2 ;/* copy R2 in R0, output of the function*/
bx lr
```

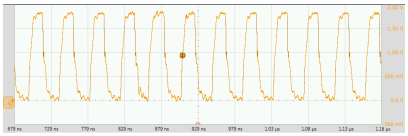
The software managing the testbench communicates with the two generators to monitor the delay and the shape of the injected signal. These capabilities make parametric study possible and enable us to find optimized parameterization for the injection.

III. Identification of the PLL as a vulnerable device with regard to radiated immunity

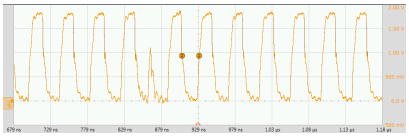
PLL are well known components designed to produce stabilized clock signals for receiving systems and microcontroller chips. Classically PLL are composed of a voltage controlled oscillator (VCO) which provides the clock signal, a frequency divider, a filter, a reference signal (classically a crystal), and a phase comparator. Since the clock signal is distributed in the whole system, its distortion could affect every part of the chip and induce errors during data processing.

It has been previously demonstrated that PLLs become unstable in presence of EMI [4]. Exposure to strong electromagnetic waves can cause sub-harmonic oscillations [5], [6]. More specifically, such an EMI can cause amplitude modulation of the voltage control of the VCO, inducing phase modulation of the VCO output.

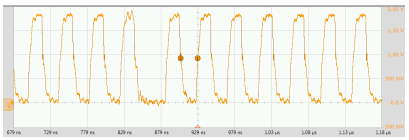
In the specific case of a microchip, EMI provokes clock glitches. In Figure 2 (a), the normal clock signal is pictured (a) and two captures of the clock signal when a fault occurs are presented in Figure 2 (b) and (c). This outline the strong influence of an EMI on the clock signal for one cycle and advance the global timing of a half clock period. In Figure 2 (b), the beginning of a clock edge appears but suddenly goes back to the low state instead of reaching the high state. We assume it enables to activate part of the circuit but not the whole chip. In Figure 2 (c), a clock edge does not appear. If the edge had just been deleted, there would be no fault, just a



(a) Clock signal without fault



(b) Clock signal with fault: starting edge



(c) Clock signal with fault: no edge

Fig. 2: Normal clock signal (a) vs faulted clock signals (b) and (c).

delay on the global timing of the software. As there is a fault, we can assume that in some part of the clock tree, an edge is present and sufficiently perceptible to induce a software effect.

Listing 2: Interpreted code for Pin verification.

```
if (myPinIsVerified())
 then{
 //do_something_securely
  test=1;}
 else{
    test=0;//throw_exception_condition_not_satisfied}
```

Listing 3: Assembly code for Pin verification.

```
80004b6: f000 f8aeb1  8000616 <myPinIsVerified>
80004ba: 4603 mov  r3,r0 /*move output to R3*/
80004bc: 2b00 cmp  r3,#0 /*compare R3 to 0*/
80004be: d003 beq.n 80004c8 <main+0x218>  /* branch if
    ↪ unequal*/
80004c0: 4b24 ldr  r3,[pc, #144];(8000554 <main+0x2a4>)
80004c2: 2201 movs r2, #1
80004c4: 601a str  r2, [r3, #0] /* store value */
80004c6: e002 b.n  80004ce <main+0x21e> /* branch */
80004c8: 4b22 ldr  r3, [pc, #136];(8000554 <main+0x2a4>)
80004ca: 2200 movs r2, #0
80004cc: 601a str  r2, [r3, #0]
```

Listing 4: Interpreted code for faulted Pin verification.

```
 //do_something_securely
  test=1;}
```

Such a disruption can provoke a fault or a crash in the software. A fault happens when a part of the program is in an unexpected state but still runs. A crash happens when the disruption leads the program to an exception branch or requires it to be reset.

In the software point of view, it can induce a virtual nop. In fact, the EMI induces an uncontrolled alteration in the opcode which is the binary value of the instruction. The opcode of the targeted instruction (LDR in the example in Listing 1) is changed in the opcode of another instruction which most of the time has no side-effect [7]. Thus the effect is the same as

if the targeted instruction had been replaced by a nop. This action produces wrong values on the output of the function. In some specific cases, the attack can corrupt data while it is loaded in a register.

Skipping an instruction can be useful for example to bypass a code pin verification [8] or to evaluate the current status as shown in Listing 2. Such a code fragment is essentially an if...then...else structure. The corresponding assembly code is given in Listing 3. In the normal case, output of *myPinIsVerified* function is tested. If it is *True*, the variable *test* is set to 1, if not the variable *test* is set to 0. In case of fault on the conditional branch instruction (in blue) the pin is considered as correct and the red part of the code is executed automatically with no condition. Thus the verification is bypassed as shown in Listing 4.

A. Success rate of fault-injection vs probe position

Considering the PLL vulnerability to the EMI and the effects of a fault injection on the clock signal, we assume that the PLL is the sensitive part of the chip.

Mapping of injection efficiency has been realized on the chip. The probe is moved with steps of $0.5\,\mathrm{mm}$ above the surface of the chip. For each position 1000 EMI are achieved. The injected signal is a pulse modulated sinusoidal wave of 4 periods at $275\,\mathrm{MHz}$ frequency. The delay of injection is fixed and equal to $188.5\,\mathrm{ns}$. The phase is explored with a step of 20°. The best results for each location have been chosen for the plot in Figure 3. The hypothesis of a fix delay is due to the stability of the injection efficiency on a range of $5\,\mathrm{ns}$ around that delay value (see section IV).

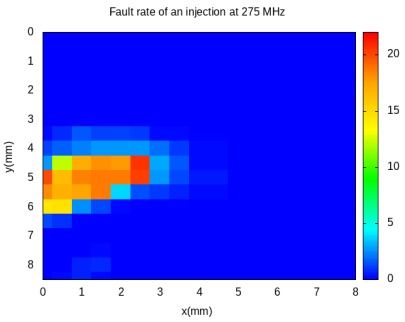
Comparing the most susceptible location to EMI to the pins mapping of the chip, this location is correlated to the V_{ssa} and V_{dda} pins used to feed analog peripheral. In particular, these signals feed the PLL.

Finally, when the PLL is disabled and the chip clock is directly plugged to the crystal, the fault rate induced by EMI is close to zero. Considering all those results, we confirm that the PLL is a vulnerable device to EMI within such a microcontrolller. Knowing this, the location of the probe for the attack can be reduced to an area around pins linked to the PLL.

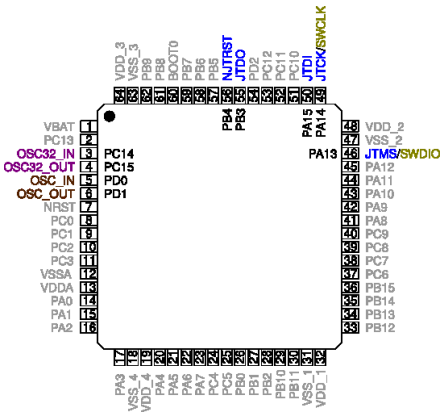
IV. Parametric influence of the waveform

A. Method of analysis

As the fault rate is essential for the success of a physical attack, optimization of injection parameters has been investigated. First of all, the dwell time of the injected signal must be strictly restricted so that the fault is limited to a single instruction. Second, we select a pulsed sinusoidal wave with moderate bandwidth rather than wideband pulses. Especially, the waveform is a pulse modulated sinus of 4 periods parameterized by three main criteria: the frequency, the delay of injection and the starting phase of that sinus. For these parametric studies, the location for the probe has been chosen in the most sensitive area (x=$0.05\,\mathrm{mm}$, y=$6\,\mathrm{mm}$). Seven frequency values are tested from $250\,\mathrm{MHz}$ to $300\,\mathrm{MHz}$.



(a) Fault rate (%) mapping



(b) PIN in/out mapping

Fig. 3: Comparison of fault injection mapping with STM32F100RB-LQFP64 PIN map.

Injection delay goes from $180\,\mathrm{ns}$ to $195\,\mathrm{ns}$ and the phase value is explored with a 20° step. In order to monitor the injection, one of the board pin is set to high state to start the injection. The time at which the EM near-field reaches the microcontroller is delayed with regard to the triggering signal. It mainly corresponds to the propagation delay within the hardware including the generator, amplifier and coaxial cables. Induced currents and voltages are only due to reactive near-field coupling with the probe The delay of injection as spoken in this section is the complementary delay added to the hardware intrinsic delay due to generators, amplifiers and wires. This additional delay is used to target precisely the instruction we want to disrupt. In Figure 4, the gain of the probe is plotted with respect to the frequency. This gain increases fastly from $0\,\mathrm{MHz}$ to $500\,\mathrm{MHz}$ and reaches its maximum -30 dB for a frequency of $1.5\,\mathrm{GHz}$. So the probe is used in the low range of its bandwidth.

B. Results

In Figure 5, the fault rate is plotted with respect to the frequency of the EMI. Only the best fault rate for every frequency is considered (among all (delay;phase) couples). The consequence of the fault is a nop on the LDR instruction. The fault rate start increasing till $270\,\mathrm{MHz}$. Then the maximum fault rate achieved with this configuration is 20%. It can be observed that there is a bandwidth from $270\,\mathrm{MHz}$ to $290\,\mathrm{MHz}$

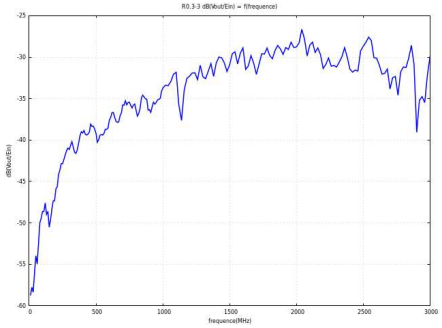


Fig. 4: Probe gain with respect to the frequency.

where the fault rate is maximum. Over 290 MHz, the fault rate decreases rapidly. On the one hand, the electromagnetic coupling increases linearly with frequency together with the probe gain. On the other hand, the limited bandwidth of the chip prevents high frequency propagation. Rising and falling time of the clock signal are 1.7 ns and 1.5 ns, respectively. The first cut-off frequency is around 206 MHz. The spectral envelope above this frequency decays with 20 dB per decade until it reaches 233 MHz and then decays with 40 dB / dec. We may therefore suppose that the increasing level of induced signal is overcompensated once the frequency is well above 233 MHz.

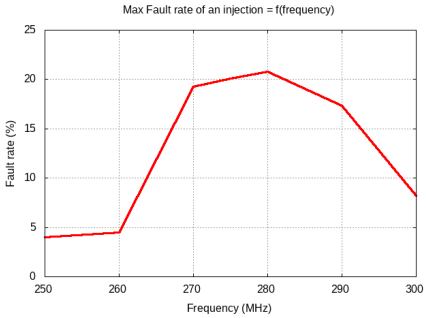


Fig. 5: Fault rate on LDR instruction with respect to the injection frequency.

In Figure 6, fault rate is plotted with respect to the injection delay. The frequency of injection is 275 MHz and only the best fault rate for every delay value is considered (among the result for every phase value). Fault rate success increases progressively between 182 ns and 185 ns of delay to reach the maximum of 20% of fault. The fault rate is stable from 185 ns up to 193 ns and then decreases. For an injection of 15 ns duration (4 periods of a 275 MHz sinusoidal wave), a precision of 5 ns is expected in order to inject with the most probable fault success.

V. Conclusion

Electromagnetic injection is a non-invasive way to attack a chip. The large number of parameters that require to be properly tuned for such an attack limits its efficiency. In a first step, the PLL has been identified as a sensitive part of

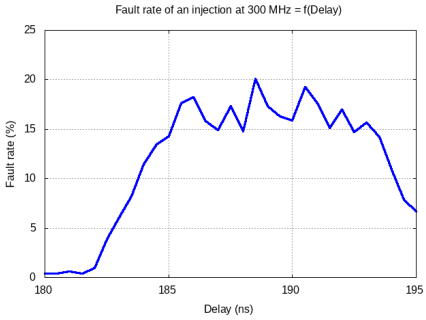


Fig. 6: Fault rate on LDR instruction with respect to the injection delay.

the chip. As a result, the preferential location for the EMI is reduced to a small area in the vicinity of the analog power supply feeding the PLL. In a second step, the influence of the frequency of the injected electromagnetic wave has been explored. The optimal fault rate is achieved in a bandwidth of 15 MHz, in the upper limit of the chip bandwidth. Then, it has been shown that for an optimal frequency that a precision of 5 ns is expected to reach the best fault rate. With this EMI technique, the achieved success rate reaches 15 to 20%. Such a fault can be used to retrieve the key of an cryptographic algorithm (for an Advanced Encryption Standard application for example [9]).

In further works, a deeper analysis of the PLL sensitivity could be realized. Having a better understanding of the real mechanism of such a disruption could lead to proposals for countermeasures to EMI on PLL to protect microcontrollers.

References

[1] D. H. Habing, "The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits," *IEEE Transactions on Nuclear Science*, vol. 12, no. 5, pp. 91–100, Oct. 1965.

[2] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in *Advances in Cryptology — CRYPTO '97*, B. S. Kaliski, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 513–525.

[3] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in *Advances in Cryptology — EUROCRYPT '97*, W. Fumy, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 37–51.

[4] S. Yuan, Y. Wu, R. Perdriau, S. Liao, and H. Ho, "Electromagnetic interference analysis using an embedded phase-lock loop," in *2012 Asia-Pacific Symposium on Electromagnetic Compatibility*, May 2012, pp. 189–192.

[5] M. F. Karsi and W. C. Lindsey, "Effects of cw interference on phase-locked loop performance," *IEEE Transactions on Communications*, vol. 48, pp. 886–896, May 2000.

[6] T. Dubois, J. Laurin, J. Raoult, and S. Jarrix, "Effect of low and high power continuous wave electromagnetic interference on a microwave oscillator system: From vco to pll to qpsk receiver," *IEEE Transactions on Electromagnetic Compatibility*, vol. 56, no. 2, pp. 286–293, April 2014.

[7] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz, "Electromagnetic fault injection: Towards a fault model on a 32-bit microcontroller," in *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Aug 2013, pp. 77–88.

[8] L. Rivière, "Securing software implementations against fault injection attacks on embedded systems," Ph.D. dissertation, TELECOM ParisTech - INFRES, 2015.

[9] A. Moradi, M. Manzuri, and M. Salmasizadeh, "A generalized method of differential fault attack against aes cryptosystem," 10 2006, pp. 91–100.