Journal of Cryptographic Engineering (2011) 1:71-77
DOI 10.1007/s13389-011-0004-0

Synchronization Method for SCA and Fault Attacks

Sergei Skorobogatov

Received: 15 November 2010 / Accepted: 16 January 2011

Abstract This paper shows how effectiveness of side-channel and fault attacks can be improved for devices running from internal clock sources. Due to frequency instability of internally clocked chips, attacking them was always a great challenge. A significant improvement was achieved by using a frequency injection locking technique via the power supply line of a chip. As a result, the analysis of a semiconductor chip can be accomplished with less effort and in shorter time. Successful synchronization was demonstrated on a secure microcontroller and a secure FPGA. This paper presents research into limits for synchronization and discusses possible countermeasures against frequency injection attacks.

Keywords side-channel attacks · hardware security · frequency injection locking · power analysis

1 Introduction

Side-channel attacks, especially in the form of differential power analysis (DPA) [1] and electro-magnetic analysis (EMA) [2] became a serious concern for the semiconductor industry since their introduction a decade ago. These attacks proved to be very effective against many implementations of cryptographic algorithms and authentication schemes [3–5]. However, for some devices, carrying out such attacks was quite a challenging task, even when no special countermeasures were in place. This was because there were no means of effective synchronization of the internal device operation, which made comparison of power traces an extremely difficult task. Although there are several ways such a comparison can be made, it takes a lot of effort and a significant time penalty. Various outcomes should be considered. First, the beginning of the operation can be unknown; hence, longer acquisition will be necessary, resulting in more expensive equipment. Second, variable frequency during the acquisition will inevitably result in a higher phase noise and possibly an incorrect result. This can be overcome by using multiple acquisitions and averaging the result or via post processing alignment [6, 7]. Both will result in a longer time required to get the result. Recently introduced optical emission analysis attacks [8, 9] will also benefit from a synchronously run chip. These attacks require precise timing synchronization for effective separation of data words present for a short period of time on a data bus or within a memory control circuit. Without such synchronization it is hard to correlate the emission with processed data.

There was a publication on a successfully implemented frequency injection attack on ring oscillators used for random number generators in secure chips [10]. This paper focuses on the possibility of frequency injection locking attacks on internal RC oscillators widely used for clocking secure chips. If such injections become practical, carrying out power analysis attacks will become easier as the externally supplied clock could be used as a precise timing reference. Not only side-channel attacks will benefit, but also fault injection attacks [11] that disrupt the normal operation of a chip at a precise time. Successful frequency injection would be highly useful for security testing of various chips as it offers a faster and less expensive solutions.

The research presented in this paper demonstrates the effectiveness of frequency injection attacks on a secure microcontroller and a highly secure FPGA chip.

S. Skorobogatov
University of Cambridge Computer Laboratory
15 JJ Thomson Avenue, Cambridge, CB3 0FD, UK
E-mail: sps32@cam.ac.uk

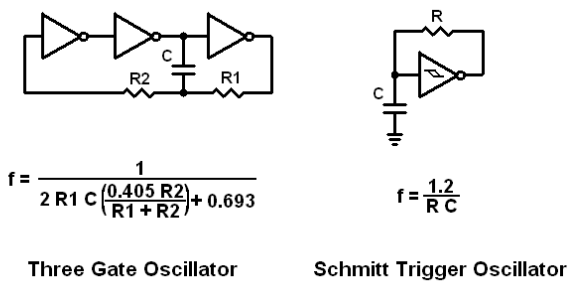

C
R2
R1
f = 1 / (2 R1 C (0.405 R2 / (R1 + R2)) + 0.693)
Three Gate Oscillator
R
C
f = 1.2 / R C
Schmitt Trigger Oscillator

Fig. 1 Examples of CMOS RC oscillators

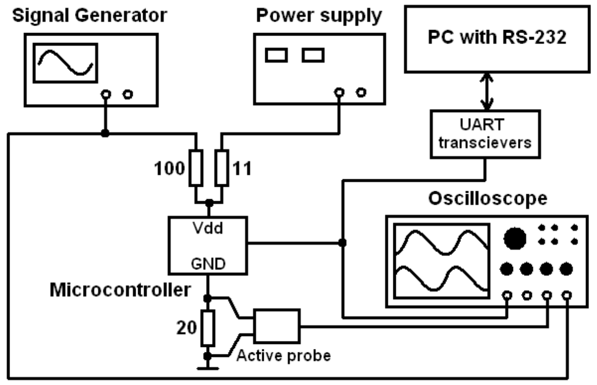


Fig. 2 Measurement setup

This paper is organized as follows. Sect. 2 describes the underlying physics of the frequency injection locking. Sect. 3 introduces the experimental setup, while Sect. 4 shows the results. Sect. 5 discusses limits, improvements and future work. Countermeasures are presented in Sect. 6.

2 Background

Many CMOS integrated circuits have internal oscillators based on RC circuits [12]. The basic idea behind such oscillators is phase shifting with amplification. As a CMOS inverter acts as an amplifier at input voltages close to its threshold, a simpler circuit can be used in microcontrollers [13]. Fig. 1 shows examples of some RC oscillators. However, despite the simplicity of such circuits, they all share the same disadvantage of having inaccurate and unstable frequencies. This is because values of the internal components, like resistors and capacitors, cannot be produced with better than a few percent accuracy with existing IC fabrication processes. In addition, temperature fluctuations and electronic noise influence frequency stability. Chip manufacturers use some methods of increasing the stability of internal oscillators including post-production calibration. However, this does not eliminate the problem of oscillator instability over time, temperature and power supply.

Two frequency-related effects take place when another oscillator is coupled with the original one. One is called injection locking [14] and refers to the situation when the frequencies of both oscillators become synchronized. Another effect is called injection pulling [15] and occurs when the interfering frequency source does not have enough power to injection lock it.

The effect of injection locking was originally observed by Christian Huygens, the inventor of the pendulum clock. He was surprised by the fact that two pendulum clocks, which originally had slightly different time, became perfectly synchronized when hung from a common beam. Later research confirmed that the pendulums were coupled by tiny vibrations in the wooden beam.

Not only the frequency of the oscillator can change, but there might be uncertainty in the timing of transitions. This effect is called jitter noise. As injection locking has the effect of low-pass filtering on the oscillator, the jitter should be expected to reduce [15].

3 Experimental Method

For the first set of experiments I chose a common secure microcontroller, the Texas Instruments MSP430F1121A [16], with secure bootloader that allows firmware updating. The bootloader runs from internal clock and verifies a 32-byte-long password before allowing access to the internal data. It was found that power analysis attacks can be used to distinguish between correct and incorrect guesses for each byte of the password. Theoretically, only 256 guesses are necessary to find the correct password as each byte is verified independently. However, as in the secure bootloader mode the chip can only run from its unstable internal clock, it is not easy to correlate the guesses for each value. Even if the beginning of the serial communication was aligned, the changes in the operating frequency makes comparison a hard task.

The measurement setup is presented in Fig. 2. The microcontroller was supplied with 3.3 V from a laboratory power supply. For power analysis measurements, a 20 Ω resistor was inserted in its ground supply line. Measurements were done with a digital storage oscilloscope using an active probe at 100 Msps. For reference and triggering, the oscilloscope was also connected to the signal generator and computer-controlled bootloader interface. Frequency injection was performed with

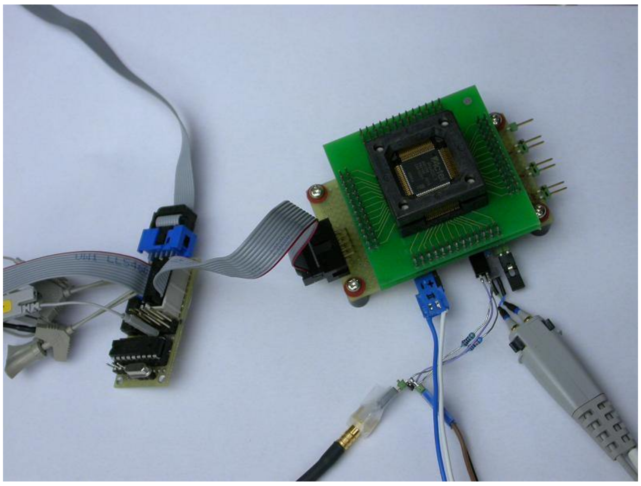
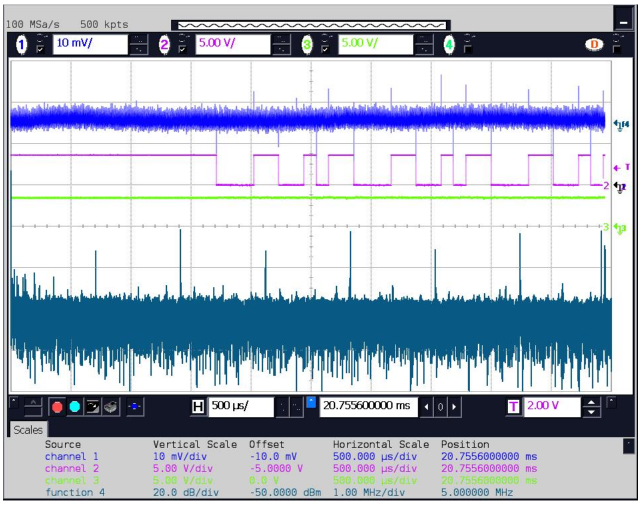


Fig. 3 Frequency injection setup for the FPGA



100 MSa/s 500 kpts

```
Source       Vertical Scale  Offset          Horizontal Scale  Position
channel 1    10 mV/div       -10.0 mV        500.000 µs/div    20.7556000000 ms
channel 2    5.00 V/div      -5.0000 V       500.000 µs/div    20.7556000000 ms
channel 3    5.00 V/div      0.0 V           500.000 µs/div    20.7556000000 ms
function 4   20.0 dB/div     -50.0000 dBm    1.00 MHz/div      5.000000 MHz
```

Fig. 4 Power trace (top) and FFT (bottom) for MSP430 microcontroller

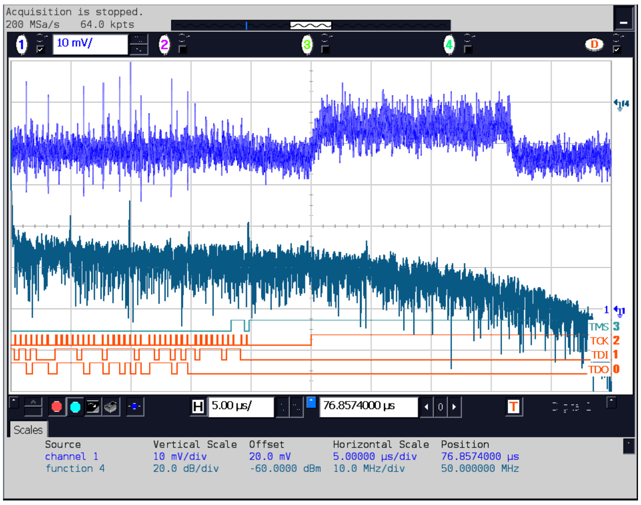
a function generator in sine mode via a 1:10 resistor divider.

The next set of experiments was done on a highly secure FPGA, the Actel ProASIC3 A3P060 [17], with secure AES-encrypted firmware updating via JTAG. Without the knowledge of the AES key it is virtually impossible to reprogram the FPGA. One possibility for extracting the AES key is by using side-channel attacks. However, as the JTAG control circuit always runs from the internal clock source, synchronization could be a very challenging task.

The measurement setup for the FPGA was similar to the one used for the microcontroller, with some difference at the PC control side. A special JTAG control board was built for communication and a differential probe was used on a core power supply due to multiple power supply rings present on the chip (see Fig. 3).

The MSP430F1121A microcontroller was initially programmed with a test pattern in its EEPROM and Flash areas including the bootloader password. All measurements were done during password verification operation. The FPGA was programmed with a test design, and the secure AES bitstream update feature was activated. It was also initialized with a test AES key. All measurements were done during the AES key scheduling operation.

For comparison, frequency injection experiments were carried out on the Microchip PIC16F628 microcontroller [18] running from an internal 4 MHz RC oscillator and from an external 4 MHz crystal quartz oscillator. It was programmed with a simple test code that was changing the state of one I/O port pin in a permanent loop.



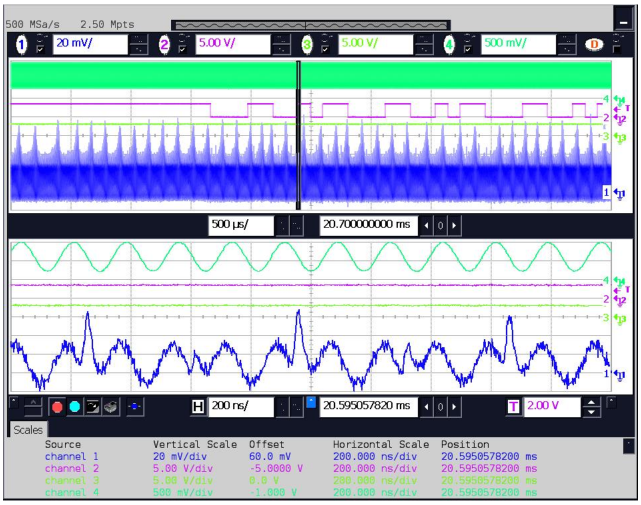
Acquisition is stopped.
200 MSa/s 64.0 kpts

```
Source       Vertical Scale  Offset          Horizontal Scale  Position
channel 1    10 mV/div       20.0 mV         5.00000 µs/div    76.8574000 µs
function 4   20.0 dB/div     -60.0000 dBm    10.0 MHz/div      50.000000 MHz
```

Fig. 5 Power trace (top) and FFT (bottom) for the FPGA

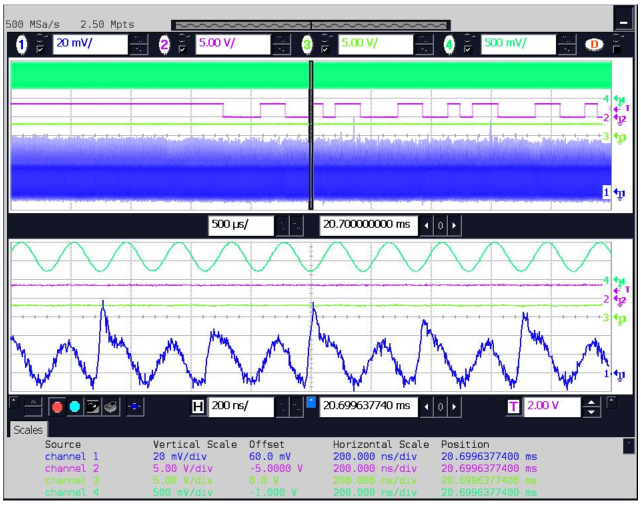
4 Results

Initial power analysis measurements were done on the MSP430F1121A microcontroller to determine the frequency of its internal clock. The FFT spectrum of the power analysis waveform revealed peaks at 1.4 MHz, 2.8 MHz, 4.3 MHz, 5.7 MHz, 7.1 MHz, 8.5 MHz and 9.9 MHz, with higher peaks at 2.8 MHz, 5.7 MHz and 8.5 MHz (see Fig. 4). The power trace signal has very good signal-to-noise ratio (SNR) of about 20 dB, suggesting a very good probability of instruction flow detection from a single power trace. For the A3P060 FPGA, the FFT spectrum showed peaks at 10 MHz, 20 MHz, 30 MHz and 40 MHz, with higher peaks at 20 MHz and 40 MHz (see Fig. 5). However, with very poor SNR of about −15 dB, substantial signal averaging will be required for tracing any data dependency.



```
Source       Vertical Scale  Offset      Horizontal Scale  Position
channel 1    20 mV/div       60.0 mV     200.000 ns/div    20.5950578200 ms
channel 2    5.00 V/div      -5.0000 V   200.000 ns/div    20.5950578200 ms
channel 3    5.00 V/div      0.0 V       200.000 ns/div    20.5950578200 ms
channel 4    500 mV/div      -1.000 V    200.000 ns/div    20.5950578200 ms
```

Fig. 6 Frequency pulling on the microcontroller with zoom



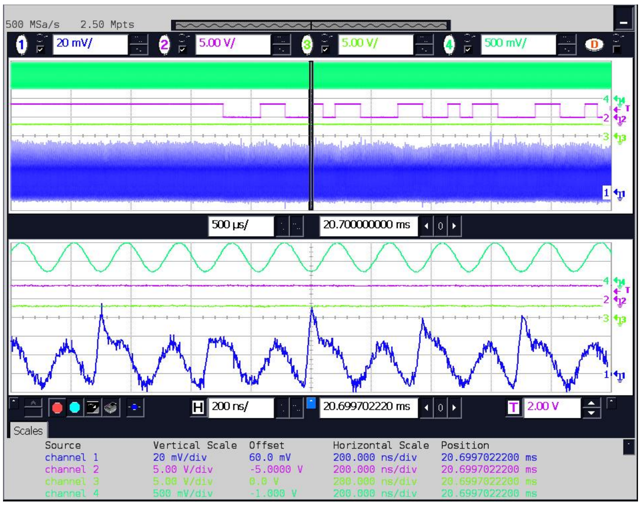
```
Source       Vertical Scale  Offset      Horizontal Scale  Position
channel 1    20 mV/div       60.0 mV     200.000 ns/div    20.6996377400 ms
channel 2    5.00 V/div      -5.0000 V   200.000 ns/div    20.6996377400 ms
channel 3    5.00 V/div      0.0 V       200.000 ns/div    20.6996377400 ms
channel 4    500 mV/div      -1.000 V    200.000 ns/div    20.6996377400 ms
```

Fig. 7 Frequency locking on the microcontroller with zoom

The first set of experiments on the microcontroller was carried out with an injection frequency around 2.8 MHz with a 2 V amplitude from the signal generator. That way, the power supply voltage was fluctuating between 3.1 V and 3.3 V. The locking happens at frequencies between 2.852 MHz and 2.856 MHz. For frequencies around 5.7 MHz, the locking took place between 5.665 MHz and 5.735 MHz. However, no locking was observed at other frequencies. The typical oscilloscope waveform for frequency pulling is presented in Fig. 6 (Channel 1 – power trace, Ch2&3 – UART, Ch4 – signal generator). The interference and instability of the oscillator frequency can be seen. Typical frequency locking results both in stable frequency and in constant phase between the injection frequency and the power trace signal (see Fig. 7).

Table 1 Frequency injection dependency for MSP430

Modulation amplitude V	Fundamental frequency MHz	2nd harmonic MHz	3rd harmonic MHz
0.03	no effect	pulling only	no effect
0.04	no effect	5.702–5.708	no effect
0.05	pulling only	5.700–5.714	no effect
0.10	pulling only	5.696–5.720	pulling only
0.20	2.852–2.856	5.665–5.735	pulling only



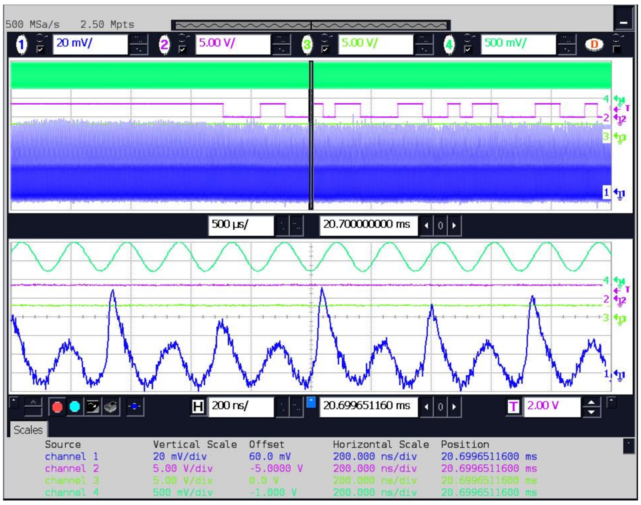
```
Source       Vertical Scale  Offset      Horizontal Scale  Position
channel 1    20 mV/div       60.0 mV     200.000 ns/div    20.6997022200 ms
channel 2    5.00 V/div      -5.0000 V   200.000 ns/div    20.6997022200 ms
channel 3    5.00 V/div      0.0 V       200.000 ns/div    20.6997022200 ms
channel 4    500 mV/div      -1.000 V    200.000 ns/div    20.6997022200 ms
```

Fig. 8 Frequency locking at 5.696 MHz (phase shift −100°)

Further measurements were carried out at lower injection amplitudes to determine the dependency of the minimum injection amplitude from the injection frequency. The result is summarized in Table 1. The best synchronization is achieved at the second harmonic of the power analysis spectrum. However, even with a 10% modulation at the second harmonic, the frequency locking took place within just a 1% range of the internal frequency. This suggests that the frequency of the injecting signal must be very close to that of the internal oscillator.

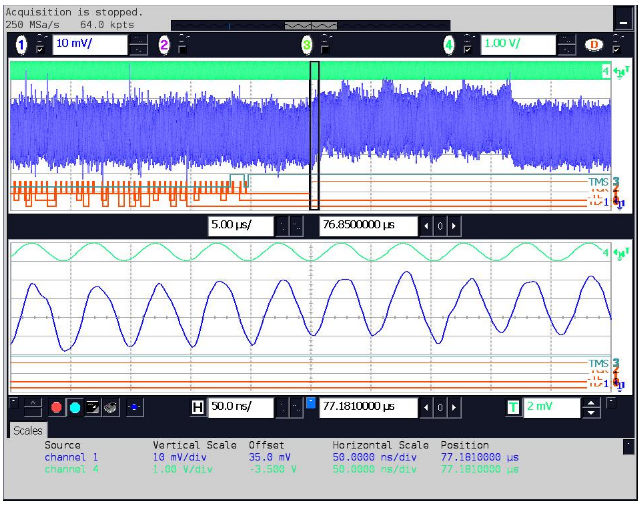
Another set of experiments revealed that the phase shift between the locking signal and the power trace signal have a strong correlation with the depth of injection. With very stable locking the peaks in the power trace are phase shifted by about −80 degrees from the injection signal, for example, at 5.700 MHz with 10% modulation (see Fig. 7). An example of less stable locking at 5.696 MHz and 5.720 MHz is presented in Fig. 8 and Fig. 9. If the phase shift is below −120 or above −40 degrees, it corresponds to the frequency pulling effect only, which is not useful for synchronization.

The FPGA frequency injection experiments started with signals around 10 MHz with 1 V amplitude. That corresponded to the power supply fluctuations between 1.4 V and 1.5 V. The locking was found at frequencies between 9.855 MHz and 9.860 MHz, 19.690 MHz and



```
Source        Vertical Scale  Offset      Horizontal Scale  Position
channel 1     20 mV/div       60.0 mV     200.000 ns/div    20.6996511600 ms
channel 2     5.00 V/div      -5.0000 V   200.000 ns/div    20.6996511600 ms
channel 3     5.00 V/div      0.0 V       200.000 ns/div    20.6996511600 ms
channel 4     500 mV/div      -1.000 V    200.000 ns/div    20.6996511600 ms
```

Fig. 9 Frequency locking at 5.720 MHz (phase shift −50°)

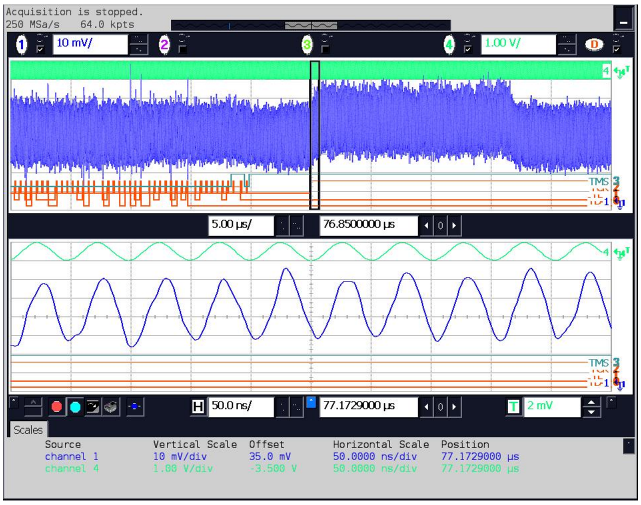


```
Source        Vertical Scale  Offset      Horizontal Scale  Position
channel 1     10 mV/div       35.0 mV     50.0000 ns/div    77.1810000 µs
channel 4     1.00 V/div      -3.500 V    50.0000 ns/div    77.1810000 µs
```

Fig. 10 Frequency pulling on the FPGA with zoom

19.710 MHz, 39.370 MHz and 39.440 MHz. An example of an oscilloscope waveform for frequency pulling with visible interference is presented in Fig. 10 (Ch1 – power trace, Ch4 – signal generator, D0–D3 – JTAG). A typical frequency locking waveform is presented in Fig. 11. The influence of the injection signal on the power trace is about an order of magnitude higher than the original power trace signal (see Fig. 5). However, as the injection signal has a very narrow spectrum, it can be easily filtered out later.

Measurements were carried out to find the dependency of the injection frequency from the injection amplitude. The result is summarized in Table 2. The best synchronization is achieved for the second harmonic of the power analysis spectrum. However, even with a 10% modulation at the fourth harmonic, the frequency locking took place within merely 0.2% of the internal frequency. This requires the frequency of the injected signal to be very close to that of the internal oscillator.



```
Source        Vertical Scale  Offset      Horizontal Scale  Position
channel 1     10 mV/div       35.0 mV     50.0000 ns/div    77.1729000 µs
channel 4     1.00 V/div      -3.500 V    50.0000 ns/div    77.1729000 µs
```

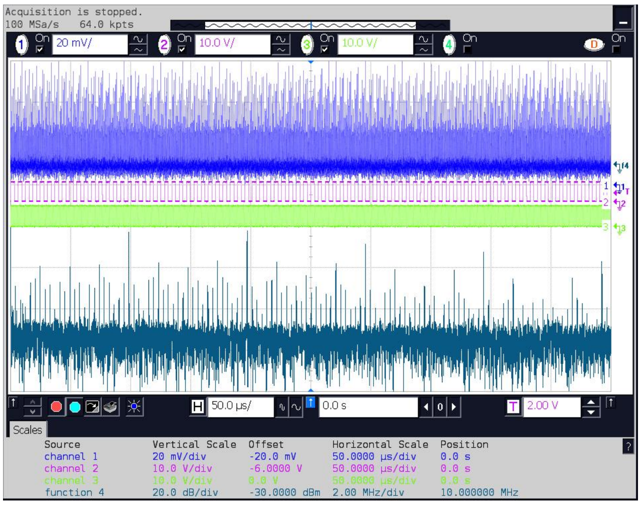
Fig. 11 Frequency locking on the FPGA with zoom

Table 2 Frequency injection dependency for A3P060

Modulation V	Fundamental MHz	2nd harmonic MHz	3rd harmonic MHz	4th harmonic MHz
0.01	no effect	no effect	no effect	pulling only
0.02	no effect	pulling only	no effect	39.403–39.408
0.03	pulling only	19.695–19.705	no effect	39.400–39.410
0.05	pulling only	19.690–19.715	no effect	39.390–39.420
0.10	9.855–9.860	19.680–19.730	pulling only	39.370–39.440

Pilot experiments were performed on the PIC16F628 microcontroller [18] running from the internal 4 MHz RC oscillator. The FFT spectrum of the power analysis waveform revealed higher peaks at 4 MHz, 8 MHz, 11.9 MHz, 15.8 MHz and 19.7 MHz (see Fig. 12). The power trace signal has a very good signal-to-noise ratio (SNR) of about 20 dB suggesting a very high probability of instruction flow detection from a single power trace as with the MSP430F1121A microcontroller.

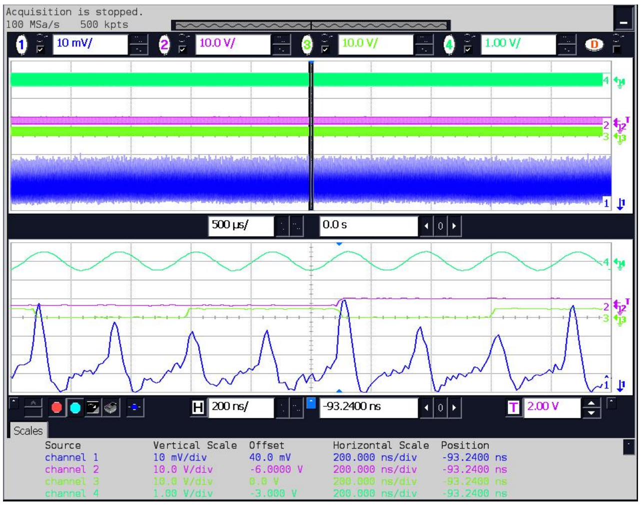
Frequency injection locking was achieved with a 2 V amplitude from the signal generator for frequencies around 3.93 MHz, 7.87 MHz and 15.75 MHz. That corresponded to the power supply fluctuations between 4.8 V and 5.0 V. An example of frequency locking at 3.93 MHz is presented in Fig. 13 (Ch1 – power trace, Ch2 – I/O trigger, CH3 – CLKOUT, Ch4 – signal generator). Results for other amplitudes are presented in Table 3. The best locking was achieved at around 7.87 MHz where as little as 10 mV modulation is enough



Acquisition is stopped.
100 MSa/s 64.0 kpts

```
Source      Vertical Scale  Offset         Horizontal Scale  Position
channel 1   20 mV/div       -20.0 mV       50.0000 µs/div    0.0 s
channel 2   10.0 V/div      -6.0000 V      50.0000 µs/div    0.0 s
channel 3   10.0 V/div      0.0 V          50.0000 µs/div    0.0 s
function 4  20.0 dB/div     -30.0000 dBm   2.00 MHz/div      10.000000 MHz
```

Fig. 12 Power trace (top) and FFT (bottom) for PIC microcontroller



Acquisition is stopped.
100 MSa/s 500 kpts

```
Source      Vertical Scale  Offset      Horizontal Scale  Position
channel 1   10 mV/div       40.0 mV     200.000 ns/div    -93.2400 ns
channel 2   10.0 V/div      -6.0000 V   200.000 ns/div    -93.2400 ns
channel 3   10.0 V/div      0.0 V       200.000 ns/div    -93.2400 ns
channel 4   1.00 V/div      -3.000 V    200.000 ns/div    -93.2400 ns
```

Fig. 13 Frequency locking on PIC microcontroller with zoom

for frequency locking. Stable locking was observed for phase shift between −90 and +30 degrees, for lower and higher frequency limits respectively.

When the PIC16F628 microcontroller was running from an external crystal quartz oscillator, it was impossible to achieve any form of frequency locking or pulling even with 10% modulation. At the same time, frequency locking to the internal RC oscillator can be done with just 2% modulation and within 1% frequency range. All the results of frequency injection locking experiments on the PIC16F628 microcontroller are presented in Table 3.

Table 3 Frequency injection dependency for PIC16F628

Modulation V	Fundamental MHz	2nd harmonic MHz	3rd harmonic MHz	4th harmonic MHz
0.005	no effect	pulling only	no effect	pulling only
0.01	no effect	7.871–7.876	no effect	pulling only
0.02	pulling only	7.868–7.880	pulling only	15.746–15.750
0.03	pulling only	7.866–7.884	pulling only	15.745–15.753
0.05	pulling only	7.857–7.890	11.809–11.811	15.742–15.757
0.10	3.934–3.938	7.838–7.904	11.806–11.811	15.730–15.764
0.20	3.927–3.936	7.793–7.928	11.793 11.805	15.705–15.778

5 Limitations and Further Improvements

Although the MSP430F1121A microcontroller tested in this paper is relatively old and was built with 0.35 μm technology with three metal layers, the internal RC oscillator will behave similarly in modern microcontrollers built with 0.18 μm technology. This assumption was proved with the 0.13 μm FPGA experiments. However, as it was observed in my experiments, the frequency locking happens within a very narrow range – usually within less than a 1% range from the internal clock frequency. This requires precision clock generators to be used for such experiments.

One way to improve the attack could be to build a more sophisticated generator with feedback from the chip. That way the frequency of the generator could be phase locked to the frequency of the internal oscillator of the chip, thus making the locking faster and more reliable.

The effectiveness of injection locking was verified with optical emission analysis experiments [9]. For that the Actel A3P060 chip was evaluated for side-channel leakage through optical emission during its three AES-related operations: key scheduling, authentication and decryption. The key scheduling operation computes round keys from the secret key, with the result placed into the internal secure SRAM. The SRAM data bus is a good source of data leakage via optical side channel. The FPGA chip was decapsulated from the rear side and placed under a microscope. A near-infrared sensitive CCD camera with a long exposure time was used to acquire the images. With the power supply voltage increased to 2.5 V, the exposure time was reduced to one hour. My measurements showed that the AES key scheduling takes 16 μs. Assuming that the data bus is 16 bits wide, the time during which unique data is present on the bus is less than 200 ns. Taking into account the transition time, the actual data holding time should be about 100 ns. Power analysis jitter time was measured on this chip and was estimated at 100 ns. Without proper synchronization, the data bus data will be overlapping, resulting in a blurred image. As a result, the time required for reliable data extraction is at least 16 hours per 16-bit block. The synchronization will be required for precise highlighting of the SRAM data bus values during the AES key scheduling operation. With the injection locking in place, the acquisition time was reduced down to four hours. This proved the effectiveness of synchronous side-channel attacks.

The next set of experiments was aimed at improving the effectiveness of optical bumping attacks – a certain class of fault attacks [19]. Compared to the published results where two months were required for full firmware extraction, less than three weeks was necessary for the full success using injection locked Actel A3P250 chip setup.

6 Conclusion

My experiments showed how effective the internal RC oscillators can be synchronized to the externally driven clock source. Two secure chips were tested and successfully frequency locked to the external clock. The most stable injection on the MSP430F1121A microcontroller happens at the second harmonic of its internal oscillation according to the FFT analysis. For the A3P060 FPGA, the best result was achieved at the fourth harmonic. However, it could well be the case that the initial RC oscillation frequency is divided by two for jitter improvement. As expected, the highly secure FPGA chip was more difficult to frequency lock than a microcontroller. Deeper modulation was necessary, and the frequency injection range was narrower. In addition, the FPGA offers much higher security protection against side-channel attacks due to very poor signal-to-noise ratio in the power trace signal. Still, the frequency injection locking offers significant improvement by allowing better synchronization and reducing the jitter noise of the internal RC oscillator. Pilot experiments carried out on the PIC16F628 microcontroller confirmed that the best result is achieved at the second harmonic of RC oscillator. However, even with a 10% modulation at the second harmonic, the frequency locking took place within just a 1% range of the internal frequency. This suggests that the frequency of the injecting signal must be very close to that of the internal oscillator. The phase shift between the locking signal and the power trace signal has a strong correlation with the depth of the injection and could be used to improve the locking.

Frequency injection locking can find very broad use in side-channel attacks and fault injection attacks. With the help of this technique, precise timing of the internal event can be predicted, thus making glitching attacks more feasible. Power analysis will benefit from low jitter noise, while optical emission analysis will be more effective with precise timing control.

Countermeasures can involve power stabilizing and filtering for internal oscillators. Another direction of improvement could be in spreading the spectrum of the internal oscillator, thus making injection less feasible. Other forms of protection against these attacks could involve using multiple oscillators and digital synthesizers rather than a simple RC oscillator. Crystal quartz oscillators proved to be very resilient to any frequency injection. However, they are significantly more expensive and much harder to integrate into small packages of modern semiconductor chips. Successful frequency injection locking might be useful for security testing of various chips as it offers a faster and less expensive solution for synchronization. Insertion of dummy cycles can help to deter side-channel and fault attacks, however, they cannot prevent injection locking. As a result, a higher quality power trace could still be acquired and the location of those dummy cycles can be found during the signal processing stage.

References

1. Kocher, P., Jaffe, J., Jun, B.: Differential Power Analysis. CRYPTO'99, LNCS, Vol. 1666, Springer-Verlag, pp. 388–397 (1999)
2. Quisquater, J.-J., Samyde, D.: ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smard Cards. Smart Card Programming and Security (E-smart 2001), Cannes, France, LNCS, Vol. 2140, Springer-Verlag, pp. 200–210 (2001)
3. Messerges, T., Dabbish, E., Sloan, R.: Investigations of Power Analysis Attacks on Smartcards. USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA, (1999)
4. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer (2007)
5. Sauvage, L., Guilley, S., Mathieu, Y.: Electromagnetic radiations of FPGAs: high spatial resolution cartography and attack of a cryptographic module. ACM Transactions on Reconfigurable Technology and Systems (TRETS), Vol. 2, Issue 1, (2009)
6. Real, D., Canovas, C., Clediere, J., Drissi, M.: Defeating Classical Hardware Countermesures: a New Processing for Side Channel Analysis. DATE2008, pp.1274–1279 (2008)
7. Kafi, M., Guilley, S., Marcello, S., Naccache, D.: Deconvolving Protected Signals. ARES2009, pp. 687–694 (2009)
8. Ferrigno, J., Hlavac, M.: When AES blinks: introducing optical side channel. IET Information Security, Vol. 2, No. 3, pp. 94–98 (2008)

9. Skorobogatov, S.: Using Optical Emission Analysis for Estimating Contribution to Power Analysis. 6th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC-2009), Lausanne, Switzerland, IEEE-CS Press, pp. 111–119 (2009)
10. Markettos, A.T., Moore, S.W.: The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators. Cryptographic Hardware and Embedded Systems Workshop (CHES-2009), LNCS, Vol. 5747, Springer, pp. 317–331 (2009)
11. Kommerling, O., Kuhn, M.G.: Design principles for tamper-resistant smartcard processors. USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA (1999)
12. RC Oscillator. Electronics-Tutorials. "http://www.electronics-tutorials.ws/oscillator/rc_oscillator.html", Last Accessed 21 January 2011
13. CMOS Oscillators. Fairchild Semiconductor. "http://www12.fairchildsemi.com/an/AN/AN-118.pdf", Last Accessed 21 January 2011
14. Adler, R.: A study of locking phenomena in oscillators. Proceedings IRE and Waves and Electrons, Vol. 34, pp. 351–357 (1946)
15. Razavi, B.: A study of injection pulling and locking in oscillators. IEEE Custom Integrated Circuits Conference, pp. 305–312 (2003)
16. Texas Instruments MSP430C11x1, MSP430F11x1A Mixed Signal Microcontroller. "http://focus.ti.com/lit/ds/symlink/msp430f1121a.pdf", Last Accessed 21 January 2011
17. Actel ProASIC3 Handbook. ProASIC3 Flash Family FPGAs. "http://www.actel.com/documents/PA3_DS.pdf", Last Accessed 21 January 2011
18. PIC16F62X Data Sheet. Flash-Based 8-Bit CMOS Microcontroller. "http://ww1.microchip.com/downloads/en/DeviceDoc/40300C.pdf", Last Accessed 21 January 2011
19. Skorobogatov, S.: Flash Memory 'Bumping' Attacks. Cryptographic Hardware and Embedded Systems Workshop (CHES-2010), LNCS, Vol. 6225, Springer, pp.158–172 (2010)