INT J COMPUT COMMUN, ISSN 1841-9836
9(1):79-84, February, 2014.

Efficiency of a Combined Protection Method against Correlation Power Analysis Side-Attacks on Microsystems

H.-N. Teodorescu, E.-F. Iftene

Horia-Nicolai Teodorescu*, Emanuel-Florin Iftene
1. "Gheorghe Asachi" Technical University of Iasi Romania, Iasi, 8 Bd. Carol I, and
2. Institute of Computer Science of the Romanian Academy, Romania, Iasi
*Corresponding author:hteodor@etti.tuiasi.ro

Abstract: We analyze the efficiency of the masking of instruction patterns using a chaotic driven clock and power supply, in front of a side attack intruding the power supply of a microsystem. The differential analysis is supposedly conducted by correlation power analysis. We demonstrate that the use of a chaotically-driven masking based on relatively simple circuits may be a significant candidate for the protection of embedded systems.

Keywords: physical security, protection, hardware, side attack, chaos, control signal, security evaluation.

1 Introduction

With a field less than 20 year old (the first paper, by Paul C. Kocher [1], was published in 1998, with the first significant expansion published in 2000, [2]), the protection against hardware-level attacks of the information in microsystems, including embedded systems is fast developing, due to the huge interest of the banks, security companies, card manufacturers, and military, moreover due to the interest in power minimization [3]. Citing [4], 'Side Channel Analysis is a [$\cdots$] form of attack [$\cdots$] that uses information that leaks, unintentionally, from the real-world implementations of cryptographic hardware.' Side-channel attacks (SCA) extract and decode the executed instructions and the manipulated data in microsystems, bypassing the cryptographic protections [1], [2]. The basic methods of attack were named simple power analysis (SPA), respectively differential power analysis (DPA), depending on the details of the attack. For various approaches of DPA, see [5].

While the literature includes numerous papers on the attacks and on the sibling topic of power analysis for software optimization [3], understandably fewer papers present hardware methods of mitigating these attacks. Several manufacturers include various solutions against side attacks. For example, Newell and Juliano [4] cite FreeScale Inc., who uses 'patented DPA functions, licensed from Cryptography Research.' Other manufacturers, as MAXIM Inc. and INFINEON also use various protection means, but details on them are not public. For example, the 32 RISC 'DeepCover Secure Microcontroller' MAX32590 released in 2013 by MAXIM includes on the chip, according to the manufacturer data- sheet, a 'tamper detection controller' that 'monitors voltage, frequency, temperature, die shield, and external sensors', erasing essential information when any type of suspicious external activity is detected.

In [6], [7], and [8] we introduced the masking of the instructions using a chaotically-driven clock and power supply. However, a detailed analysis of the masking efficiency under DPA has not been performed for that method. In this paper, we provide results of the analysis of differential power attacks, when the chaotic masking as above is used to protect the system. The protection method proposed in [6], [7], and [8] and further analyzed here is, at the hardware level, more of a proof of concept of the capabilities of the method, not a blueprint solution ready to put into silicon.

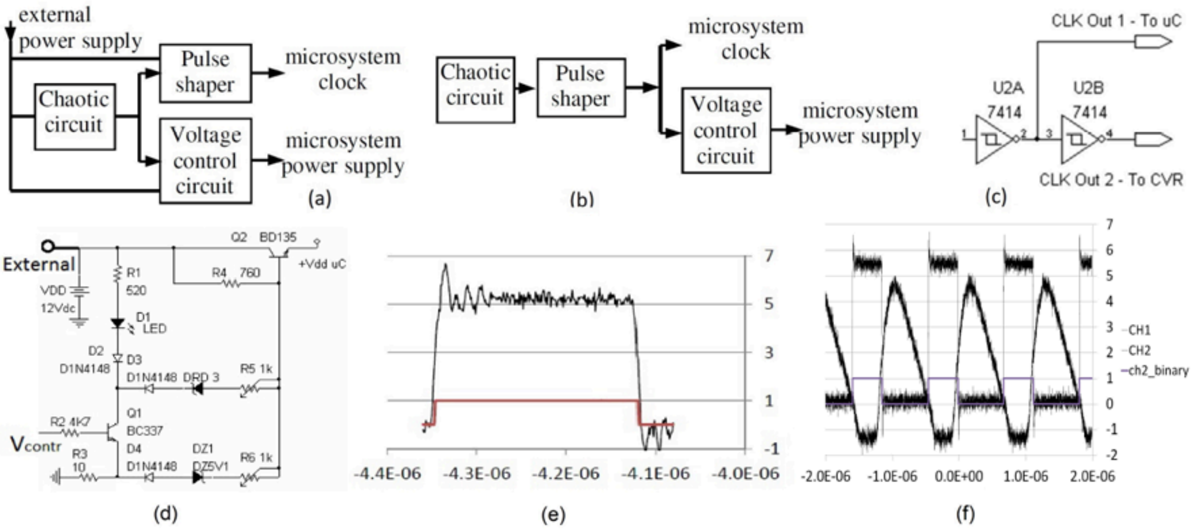

Figure 1: Block diagram for the hardware for protection against SCA. (a) Diagram with analog control of the voltage. (b) Both the clock and the voltage control are digital signals. (c) Pulse forming circuit. (d) Controlled voltage regulator. (e) Example of noisy control pulse. (f) Waveforms from the chaotic circuit and the corresponding pulses generated for control

2 The proposed protection method

Beyond software protection methods, such as specific algorithms, hardware protection methods play an essential role today in data and code security, as proved by several specific chips produced by companies as the ones quoted in Section 1.

We present in this paper an operation principle demonstrator of the protection method. We assume that only the external power supply is available to the intruder for monitoring with a series resistor. While the proposed method is similar to the typical injection of (pseudo-)random pulses on the power supply line, in this type of protection the random signal produced by the chaotic circuit is used to drive a controlled voltage regulator (CVR), which modifies the voltage that powers the microcontroller, moreover is used to generate the clock signal of the system. The protection circuits include a chaotic signal generator, a pulse shaper, and the CVR, as shown in Fig. 1 (a-c). The CVR designed and used in this research is shown in Fig. 1 (d) and an example of control pulse in Fig. 1 (e). The circuits where described in [9] and [8]. More than one level of voltage jump can be produced with such a scheme, provided that multiple loops with different Zener diodes are used in parallel on the lower branch of the circuit in Fig. 1 (d).

The random character of the pulses produced by the pulse shaper refers to the variation of their duration, especially on the long run, due to the change of operation condition of the chaotic circuit (changes in the ambient temperature, fluctuations of the power supply of the chaotic circuit.) For recordings spaced in time by about 10 minutes, under apparently unchanged laboratory conditions, variations of the number of samples per pulse were of more than 20 % for measurements performed during the same day. On the other hand, changes from one pulse to the other were less than 0.5 %. The slow change of the pulse duration due to the change of the chaotic regime produced by ambient factors is beneficial for the protection because it makes difficult the learning of the patterns of the instruction, as they continuously and unpredictably change. Notice in Fig. 1 (f) that the control pulses remain noisy with an amplitude of the noise of about 0.5 V (peak amplitude more than 1 V). This high frequency noise makes the masking process more effective, therefore we have not tried to reduce the noise. The evaluation of the randomicity of the clock signal, as produced by the pulse shaper of the chaotic clock generator proposed in [8] was performed by determining the fluctuations of the width of the pulses. For this purpose, the time between two successive up-down impulse edges was determined for all pulses during a long period of time. The analysis showed that the width of the pulses varies by about 0.1 to 2% over short periods (less than 1 ms), but with almost 40% over longer periods (minutes to hours). The presented circuits serve only to illustrate the operation principle and the feasibility. These circuits are not designs for on-chip implementations. On the other hand, the hardware-level protection discussed in this paper assumes that the protection circuits are built on the same chip as the protected microsystem (SoC - system on chip technology), or at least that they are on a chip included in the same package (multi-chip technology).

3 Analysis of the strength of the protection method

Various attack methods and related countermeasures were presented in the literature, see [5], [10], [11], [12]. Attacks based on correlation analysis are among the most common. The intercorrelation function for two sequences, $\{x(n)\}$ and $\{y(n)\}$, is defined as $C_{x,y}(\tau) = \frac{1}{N}\sum_{n=0}^{N-1} x[n]y$ $[n+\tau]$, where τ is the delay. Let $V_k = (s_N, s_{N+1}, , s_{N+T})$ be the expected (average) vector standing for the pattern of an unperturbed (unmasked) instruction k. Let $X = (x_M, x_{M+1}, , x_{M+T})$ be the vector of an instantiation of a masked, unknown instruction. The duration (number of samples) is taken the same as for V_k, when the clock can be determined independently and the number of clock periods for an instruction is known. The purpose of the attack is to identify the instruction from its signature, X. Several approaches for the attack are possible, among others the determination of the distance between X and all the patterns of the instructions, V_k, $k = 1 \cdots n$, the computation of the inter-correlations between all V_k and X, or determining the distances between the Fourier transforms of the unknown, masked sequence X, $F(X)$, and the Fourier transform of the sequence of the instructions, $F(V_k)$. Some authors, e.g. [5], consider the correlation power analysis (CPA) a distinct, more advanced method than DPA.

When using correlation functions, attackers may try to determine the instruction in various ways, depending on the information they can acquire about the microsystem. When the attackers are able to determine the patterns of the unmasked instructions, they could proceed as follows. The attackers may compute in the first place the intercorrelation functions between the ‘clean’ patterns of instructions and segments of the waveform that correspond to one machine cycle (m.c.), assuming the instructions take one m.c. The attackers may reason that the true instruction is there where the intercorrelation is the greatest. Denote the ‘clean’ pattern of the instruction $\#k$ by X_k^0. We denote an instance of the masked instruction $\#j$ by X_j^m. The correlation between them is denoted by $C_{X_k^0,X_j^m}(t)$. In the simplest (ideal) case, $max_t C_{X_k^0,X_k^m}(t) \ggg max_t C_{X_k^0,X_j^m}(t), j \neq k$. Then, the instructions are easily identifiable. If, instead, there is some index j such that $max_t C_{X_k^0,X_k^m}(t) < max_t C_{X_k^0,X_j^m}(t), j \neq k$, confusion appears between the instructions $\#k$ and $\#j$.

In the next Section, we demonstrate that a key sub-set of the instruction set of the microcontrollers in the 16FXXX series is securely masked by the method we proposed in [7], [8] against CPA analysis. For this purpose, we compute the correlation functions between the waveforms produced by various instructions when they are masked, respectively unmasked.

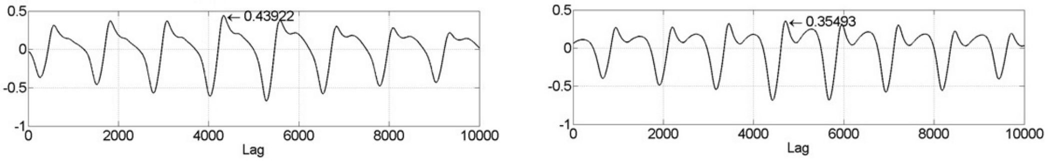

Figure 2: Examples of intercorrelations with masked instructions

4 Results and assessment of the robustness against CPA-SCA

The main results refer to the efficiency of the masking as determined by the lack of correlation between the unmasked pattern of the instruction and the masked ones. The results are summarized in Tables I and II. Table I shows that the maximal values of the self-correlations of unmasked instruction waveforms is (almost) 1 for all the instructions, as expected, while the maximal values of the intercorrelations between unmasked instructions is less than 0.8. This allows the easy discovery of the unknown instruction by performing the correlation of its waveform with the waveforms of the other instructions. In our case, as Table II shows, seven out of eight instructions have maximal values of intercorelations with other instructions than with themselves. For example, the instruction **movlw**, when masked, better intercorrelates with **addwf**, **andwf**, **movf**, **rrf**, and **btfss** than with itself (larger correlation values, see Table II).

TABLE I. Maximal values of the inter-correlation functions for eight instructions; unmasked operation, at 4 MHz clock

	addwf#2	andwf#7	movf#4	rrf#3	btfsc#4	btfss#3	andlw#2	movlw#7
addwf#2	1	0.73801	0.73584	0.60686	0.39528	0.75491	0.66487	0.78685
andwf#7	0.73801	1	0.85923	0.60065	0.4209	0.77955	0.73043	0.8248
movf#4	0.73584	0.85923	1	0.5919	0.39232	0.76756	0.67754	0.80839
rrf#3	0.60686	0.60065	0.5919	1	0.81175	0.57169	0.5507	0.57
btfsc#4	0.39528	0.4209	0.39232	0.81175	1	0.40628	0.46722	0.38796
btfss#3	0.75491	0.77955	0.76756	0.57169	0.40628	1	0.85267	0.73405
andlw#2	0.66487	0.73043	0.67754	0.5507	0.46722	0.85267	1	0.68391
movlw#7	0.78685	0.8248	0.80839	0.57	0.38796	0.73405	0.68391	1

TABLE II. Maximal values of the inter-correlation functions between eight instructions, when one instruction is unmasked (first column in the table) and the other one is masked (first row).

	addwf#3	andwf#7	movf#3	rrf#6	btfsc#6	btfss#5	andlw#4	movlw#4
addwf#2	0.4508	0.30583	0.33292	0.27566	0.37544	0.37642	0.30343	0.44512
andwf#7		0.34256	0.36752	0.28884	0.41852	0.39059	0.30863	0.48923
movf#4			0.36011	0.29453	0.38931	0.40252	0.32866	0.45862
rrf#3				0.23007	0.47391	0.29884	0.27176	0.51101
btfsc#4					0.39219	0.22641	0.20155	0.40093
btfss#3						0.3588	0.28241	0.45588
andlw#2							0.21974	0.33482
movlw#7								0.44189

Notice that the first table is symmetrical with respect to the main diagonal (Hermitian). Tables I and II should be considered from the point of view of the identification of the instruction based on correlation functions. Each element of the tables (matrices) is the maximal value of the correlation function for specified execution instances of a first and second instructions. The instruction is identified when the correlation is 1, in Table I. The attacker is supposed here to have access to the true waveform of the instruction and to be able to directly or indirectly determine the clock frequency of the attacked system.

Assume that the attackers have acquired the waveforms of the non-masked instructions. The attackers can determine the true clock frequency of a system by running in a loop the correlation between an interpolated, respectively extrapolated version of the clean waveforms with the unknown, masked waveforms. For some value(s) of the interpolation, the correlation function exhibits the maximal highest value and a strong periodicity, due to the machine cycles in the waveform. In that case of interpolation, the time alignment between the known 'clean' waveform and the given waveform with unknown clock is the best and, therefore, the unknown clock period is found. We assume that the attackers have performed this determination. Next, the attackers can perform with a known interpolation factor all the intercorrelations, to extract the information on the instructions in the attacked program.

Figure 2 shows examples of self-correlations of unmasked and masked instructions and correlations between masked and unmasked instructions. As expected, in all cases the correlations exhibit the periods of the clock and of the machine cycles, but not the instruction patterns. Notice in Table II that values of selfcorrelation for a specified instruction that are lower than values of the correlation of the same instruction with others means that the criterion of maximal value of correlation will not work for the discovery of the instruction, based on correlations.

5 Discussion and conclusions

This paper synthesized partial and preliminary results reported in [6], [7], [8] and presented a thorough analysis of the masking efficiency under CPA attacks against a microsystem protected with the masking method proposed. The method is based on the randomization of both the clock and the supply voltage. The randomization uses an approach based on a simple chaotic system and the related circuitry.

The proposed protection can be effective only when the attacker has no access to the chaotic circuit, or to the controlled voltage regulator. These circuits should be included in the same package as the microsystem. Moreover, the electromagnetic radiation (EMR) from the CVR should not be easy measured, because it reveals to the attacker the control of the voltage (that is, the chaotic circuit output). With the chaotic signal known, the attacker would be able to demodulate the masked signal and the masking one. In addition to limiting the direct and indirect (EMR mediated) access to the chaotic signal, the protection must insure that the modulating signal and the protected one have similar characteristics, for example, similar amplitudes and heavily overlapping spectra. Only with all these conditions satisfied, could the protection be effective. We reported only on an idea demonstration, not on an effective circuit. Therefore, neither the condition on the amplitude of the swings of the VCR, nor the overlapping spectra condition is satisfied.

Concluding, we presented a method for instruction masking against CPA and showed that the method proves highly effective even with simple circuits for protection. The core of the method is the use of a chaotic circuit to alter at the same time the clock frequency and the supply voltage of the protected microsystem. The method is appropriate for integration either on the chip of the microsystem or in a multi-chip package.

Acknowledgment. This research was not supported by any institution; most of the conceptual work was benevolently performed by HNT. While there is a partial overlapping of this research with the project 'Cognitive Systems' of the Romanian Academy, there was no support from that project.

Authors' contributions. HNT proposed the protection method in Fig. 1, the schemes of the circuits for chaotic signal generation and power supply control, determined the tests and participated in the tests and experiments, performed part of the data processing, derived conclusions and wrote the paper. EFI built all the circuits based on the design and schemes provided by HNT, wrote the test programs based indicated by HNT, and made most of the experiments. Both authors discussed the paper and agreed with its final form. **Conflicts of interest.** The authors declare no conflict of interest.

Bibliography

[1] P. Kocher, J. Jaffe, B. Jun, (1998), Introduction to Differential Power Analysis and Related Attacks, Cryptography Research Inc, www.cryptography.com/public/pdf/DPATechInfo.pdf. Accessed Jan. 2012.

[2] P. Kocher, J. Jaffe, B. Jun, (2000), Differential Power Analysis, Cryptography Research Inc, www.cryptography.com/public/pdf/DPA.pdf. Accessed Jan. 2012.

[3] V. Tiwari, S. Malik, A. Wolfe, M. T.-C.Lee, Instruction Level Power Analysis and Optimization of Software, *J. VLSI Signal Processing*, 13(2-3):223-238, Aug 1996.

[4] R. Newell, F. Juliano, Protecting Sensitive Networked Embedded Systems from Aggressive Intrusion. EDN, Electronic Design News Magazine, May 5, 2013. www.edn.com/Pdf/ViewPdf?contentItemId=4413418

[5] T.-H. Le, M. Berthier, Mutual Information Analysis under the View of Higher-Order Statistics. In: Echizen, I., Kunihiro, N., Sasaki, R., (Eds.), Advances in Information and Computer Security, *LNCS*, Springer, Berlin Heidelberg, 6434: 285-300. 2010.

[6] H.-N. L. Teodorescu, E.-F. Iftene, Analysis of the Code Masking Efficiency of Chaotic Clocks in Microcontroller Applications, *3rd Int. Symposium on Electrical and Electronics Engineering (ISEEE2010), Sep 16-18, Galati*, 261-266, 2010.

[7] E.-F. Iftene, H.-N. L. Teodorescu, Masking the Instructions of a Microcontroller using a 'Chaotic' Power Supply, Bull. Polytechnic Inst. Iasi, E&E, LIX (LXIII), 1:21-28, 2013.

[8] E.-F. Iftene, H.-N. L. Teodorescu, Protecting the Code against Side Attacks using Chaotically Controlled Clock and Supply, *Proc. ECAI 2013 - 5th Int. Conf. Electronics, Computers and A.I., IEEE Conf. #20924, 27-29 June 2013, Pitesti, Romania*, 79-82, 2013.

[9] H.-N.L. Teodorescu, V. P. Cojocaru, Complex Signal Generators based on Capacitors and on Piezoelectric Loads. In: C. H. Skiadas, I. Dimotikalis and C. Skiadas (Eds), Chaos Theory: Modeling, Simulation and Applications. World Scientific Publishing Co., 423-430, 2011.

[10] E. Brier, C. Clavier, F. Olivier, Correlation Power Analysis with a Leakage Model. In M. Joye and J.J. Quisquater (Eds.), Cryptographic Hardware Embedded System, CHES 2004, Vol. 3156, LNCS, pp. 16-29, Springer-Verlag, 2004.

[11] Y. Zhang, A. Juels, M.K. Reiter, T. Ristenpart, Cross-VM Side Channels and Their Use to Extract Private Keys. ACM, 2012. Available at http://dx.doi.org/10.1145/2382196.2382230, 2012.

[12] R.E. Atani, S. Mirzakuchaki, S.E. Atani, W. Meier, On DPA-Resistive Implementation of FSR-based Stream Ciphers using SABL Logic Styles, *Int J Comput Commun*, ISSN 1841-9836, 3 (4):324-335, 2008.