Dynamic Frequency Scaling as a countermeasure against simple power analysis attack in RISC-V processors

Ba-Anh Dao*, Anh-Tien Le*, Trong-Thuc Hoang*†, Akira Tsukamoto†, Kuniyasu Suzaki‡†, Cong-Kha Pham*
*The University of Electro-Communications (UEC), Tokyo, Japan
†National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan
‡Technology Research Association of Secure IoT Edge application based on RISC-V Open architecture (TRASIO)
Email: {daobaanh,leanhtien,thuc}@vlsilab.ee.uec.ac.jp, {akira.tsukamoto,k.suzaki}@aist.go.jp, phamck@uec.ac.jp

***Abstract*—Dynamic Frequency Scaling (DFS) is a technique related to dynamically changing the clock frequency of hardware modules during their operation. This paper demonstrates integrating DFS technique into an open-source RISC-V processor and used it as a simple, cost-effective countermeasure against Simple Power Analysis attack. The integrated processor is implemented in Sakura-X FPGA board [1] for experiments. Results from experiments show that the DFS module can cover up sensitive information in measured power traces while hardware resources requirements of the processor are virtually unchanged.**

***Index Terms*—DFS, RISC-V processor, SPA, SCA**

I. Introduction

Embedded systems are becoming more and more popular, especially with applications that require security. In these systems, general purpose processors are widely used due to matured and useful software. However, general purpose processors are extremely vulnerable to side channel attacks, which use leaked information from heat, sound, time, electromagnetic radiations or power consumption to retrieve secret keys used in cryptographic operations [2]. The most effective side channel attacks are Power Analysis attacks. They include Simple Power Analysis (SPA) attack, Differential Power Analysis (DPA) attack [3] and Correlation Power Analysis (CPA) attack [4]. Practically, SPA relates to visual observation on the power traces of the processor when it executes cryptographic functions. It allows attackers to gather basic information about the type and timing of cryptography algorithms [5]. Based on that information, attackers can decide to deploy more complicate and powerful attacks such as DPA or CPA to compromise security of entire system.

Various software-based and hardware-based countermeasures against power analysis attack has been proposed. Hardware-based approaches tend to be more straightforward and applicable across different platforms since they try to solve the problems at physic-level of the systems. For example, some hardware-based countermeasures are increasing noise [6], flattening current consumption [7], adding filters [8]. However, these hardware-based solutions are often not available for embedded cryptosystems with general purpose processors since these processors typically are fixed, commercial products. Therefore, security of these systems can only rely on software-based countermeasures such as dummy code insertion [9] or intermediate data masking [10].

First International Workshop on Secure RISC-V Architecture Design Exploration (SECRISC-V'20). It is held in conjunction with the IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS) - August 23rd, 2020 in Boston, Massachusetts, USA.

Recently, the open-source hardware instruction set architecture (ISA) named RISC-V is freely published by RISC-V Foundation. Many open-source RISC-V processor designs are also available, which allows designers to improve security of their embedded systems with effective hardware-based countermeasures. As a consequence, the security feature of these systems will become more transparent with software developers or high-level users. Dynamic Frequency Scaling (DFS) is a hardware-based countermeasure used to counter power analysis attack. This technique involves distorting power traces measured in both time axis and amplitude axis. Results in [11] shows that it can blocks SPA and DPA attacks on DES algorithm executed by a crypto-processor. In this paper, DFS technique is applied to the U500-Freedom platform, an open-source general-purpose RISC-V processor. Special designed FPGA board for side channel attack is used for implementing the DFS integrated RISC-V processor and evaluating effectiveness of this countermeasure. As an early work, this paper only focuses on countering SPA attack.

The rest of the paper is organized as follows: Section II briefly describes the target RISC-V processor and implementation of DFS technique. Next, setup and measuring results of experiments on Sakura-X FPGA board [1] are shown in Section III. Section IV discusses some properties of the proposed solution. Finally, conclusion and future works are given in Section V.

II. Proposed Solution

A. U500-Freedom Platform

The U500-Freedom platform is an open-source RTL design of a 64-bit RISC-V multicore CPU. It is created by SiFive. U500-Freedom platform source code is available on their github page. Initially, the U500-Freedom platform is designed to be mapped into Xilinx Virtex-7 VC707 FPGA Evaluation Kit for customization, development and evaluation. The platform is capable of booting Linux autonomously and can be controlled via an external debug. It also supports multicore, cache coherence architecture, various high speed and basic peripherals.

Fig. 1 described the block diagram of the U500-Freedom platform. With default configuration, the platform includes four 64-bit Rocket cores [12], private L1 caches for each core. Each core and its private caches are wrapped into a module called RocketTile. Besides, the platform also consisted of many other modules such as shared L2 cache, memories, peripherals. All of them can communicate with each other by using a free and open chip-scale interconnect standard

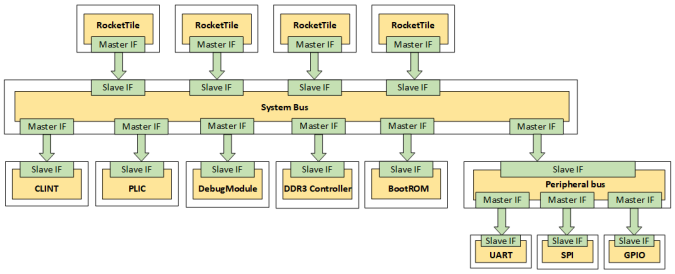


Fig. 1: Block diagram of U500-Freedom platform with default configuration.

named TileLink. This standard provides multi-master, multi-slaves communication interfaces and was designed for RISC-V System-on-Chip. As illustrated in Fig. 1, TileLink connections between modules are indicated by arrows from Master to Slave. By using TileLink, the platform is classified as a physically addressed, share-memory system.

When implemented into Xilinx Virtex-7 VC707 FPGA Evaluation Kit, the whole platform is synchronized and fed by a PLL generated clock signal. Actual test results on Xilinx Virtex-7 VC707 FPGA Evaluation Kit show that the frequency of the system clock can reach up to maximum value of 150MHz.

B. Integrating DFS technique into U500-Freedom

Since not only the RTL design of U500-Freedom platform but also its interconnect standard implementation is open sources, the platform can be easily modified. The proposed system architecture is shown in Fig. 2. DFS Control Reg and Clock Divider module are added to the platform. DFS Control Reg module contains several registers which are addressed in shared-memory space. The outputs of these registers are used as input of Clock Divider module so that Rocket cores are capable of tuning operating mode and settings of Clock Divider module. Clock Divider module receives settings from DFS Control Reg and generates output clock signals from its input clock. Each of these output clock signals are fed to a RocketTile. Different colored dashed boxes in Fig. 2 indicate different clock domains and which modules are included in them. The TileLink interconnects between RocketTiles and system bus are changed from Synchronous Crossing to Asynchronous Crossing since they are connecting modules from different clock domains. Since each core utilizes an independent TileLink connection to system bus, operating clock frequencies of all cores are independent of each other.

The Clock Divider module is designed to operate in manual or autonomous mode. In manual mode, clock output for any specific RocketTile could be scaled down from PLL generated clock. Scaling ratio, output selection values are stored in DFS Control Reg and could be dynamically updated by any Rocket core. Scaling ratio is designed to be integer so that output clock frequency is a factor of input clock frequency. In autonomous mode, output clock frequencies are alternately changed between predefined states every fixed period of time. A predefined state is a combination of n independent clock frequencies, where n is number of Rocket cores. Each frequency is applied to a output clock port. Since TileLink connections between cores and system bus are asynchronous, clock frequencies for any core of a predefined state could be any factor of the input clock signal.

III. Experiment

A. Experiment Setup

U500-Freedom platform with integrated DFS modules is mapped into Sakura-X FPGA board [1] for further experiments. A Xilinx Kintex-7 XC7K160T FPGA and probe points for measuring its power supply for internal logic gates are available on Sakura-X board. Therefore, the power consumption of the U500-Freedom platform which is side channel information can be easily observed. The number of Rocket cores is reduced to maximum of 2 cores in order to fit the proposed platform into XC7K160T FPGA chip.

Experiment setup are shown in Fig. 3. Kintex-7 XC7K160T FPGA is loaded with the modified U500-Freedom platform. External SPI MicroSD Card and UART modules are connected with the platform via header CN8. An open-source implementation of AES-128 written in C [13] is compiled, stored in MicroSD Card while UART module is used to print out boot log, softwares output to an UART terminal on another monitoring PC. A GPIO pin of U500-Freedom platform is also mapped to header CN8 and used as trigger signal. It indicates whether platform is executing AES encryption or not. Power consumption waveform can be measured by oscilloscope. Channel 3 of oscilloscope is connected to J19 of Sakura-X board via a SMA-BNC 50Ω cable. J19 is the SMA jack that connected to VCCINT1V, the voltage supply of FPGAs internal logic cells. Channel 2 grabs trigger signal via a typical

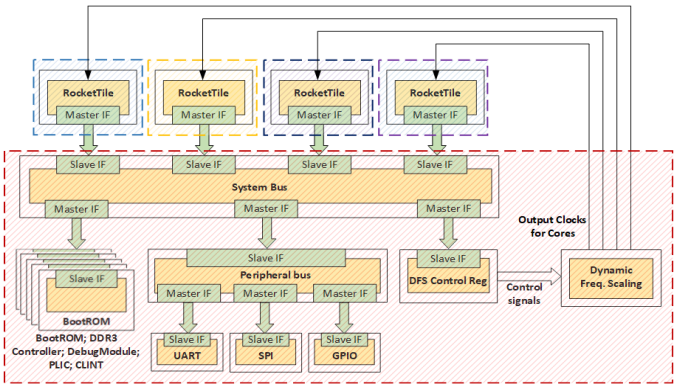


Fig. 2: Block diagram of DFS-integrated platform.

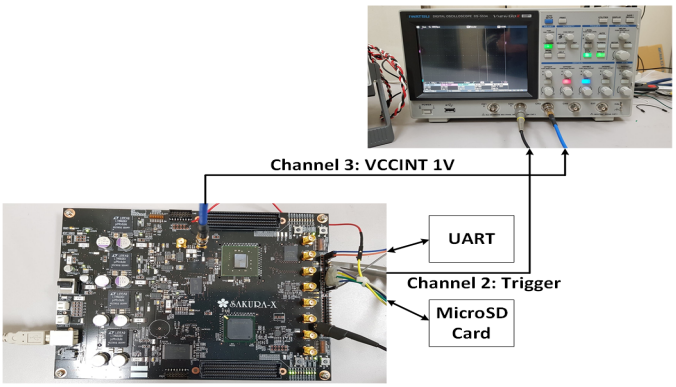
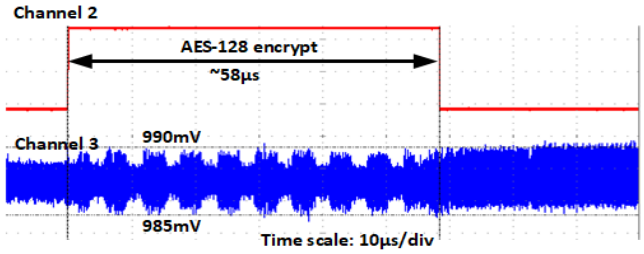
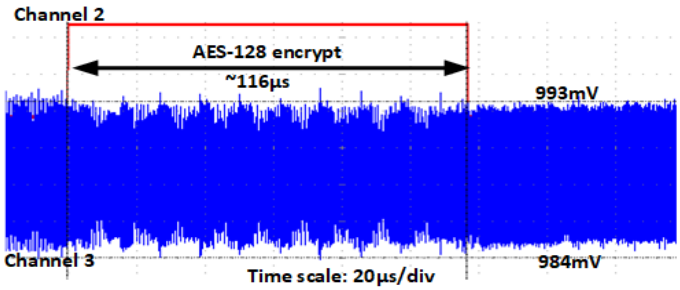


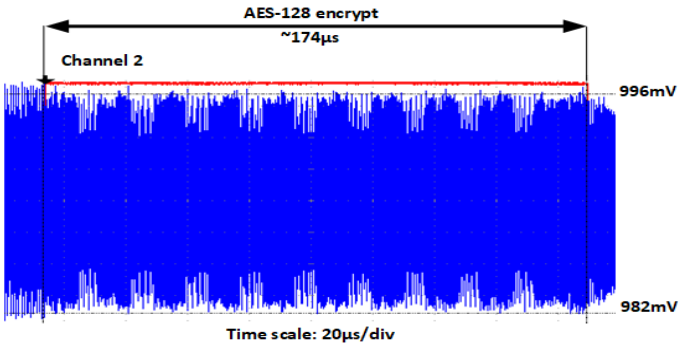
Fig. 3: Experiment setup to measure power traces.



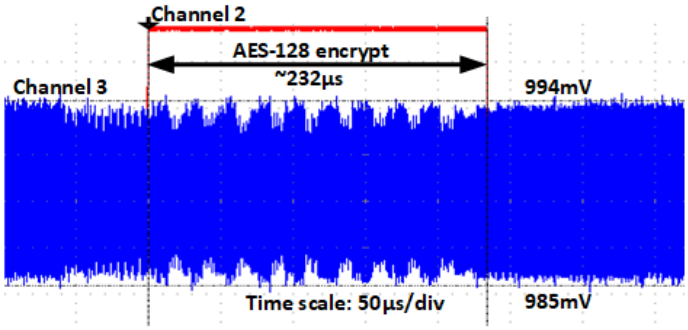
(a) Measured power trace when Rocket core clock is 100MHz.



(b) Measured power trace when Rocket core clock is 50MHz.



(c) Measured power trace when Rocket core clock is 33.33MHz.



(d) Measured power trace when Rocket core clock is 25MHz.

Fig. 4: Measured power traces when Rocket core clock is fixed at various frequencies.

passive probe. At rising edge of trigger signal, power traces from channel 3 are captured and saved for later evaluation. For channel 2, vertical scale is set to 1V/div and offset is set to 820mV. For channel 3, vertical scale is set to 2mV/div and offset is set to -990mV.

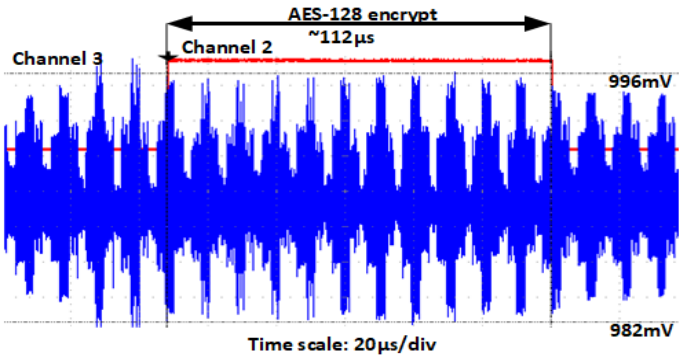
B. Measured Results

On Kintex-7 XC7K160T, PLL generates a 100MHz clock signal for U500-Freedom platform excluding the RocketTiles. In various cases of DFS setting, power traces of the U500-Freedom platform are captured and shown in Fig. 4 and Fig. 5. AES-128 encryption is executed sequentially by one Rocket core. Fig. 4a shows the power trace measured from oscilloscope when Rocket core uses 100MHz clock signal generated from Clock Divider module. Channel 2 signal shows that AES encryption executed in approximately 58μs or 5600 clock cycles. Only during encrypting time interval, there is pattern of 10 peaks appeared in power trace measured in Channel 3 that matched with 10 rounds of AES-128 encryption. There is no peak occurred outside that time interval. Voltage level of collected power trace varies in range from 985mV to 990mV. When Rocket core clock reduced to 50MHz, channel 3 measured power trace that shown in Fig. 4b. Similar to power trace shown in Fig. 4a, 10 peaks are easily observed. However, in this case, the voltage level is in range from 984mV to 993mV. The power traces measured when clock frequency of Rocket core is 33.33MHz and 25MHz also has similar properties as respectively illustrated in Fig. 4c and Fig. 4d. Fig. 4 indicates that changes in clock frequency of Rocket core cause significant changes in voltage level and peak to peak voltage swing of measured power traces. The peak to peak voltage swing would increase several times, for example 1.8 times when core clock frequency scaled down by 2 and 2.8 times when core clock frequency scaled down by 3. Therefore, when Clock Divider module operates in autonomous mode, voltage level and peak to peak voltage swing are also alternately changed according to Rocket core clock frequencies. Power trace of U500-Freedom platform measured in this case is shown in Fig. 5. As an example, in this experiment, Rocket core clock is periodically changed every 256 clock cycles of 100MHz system clock, alternately between 100MHz, 50MHz, 33.33MHz and 25MHz. The average core frequency of this example could be considered as 52.0833MHz. Peak pattern related to 10 rounds of AES-128 can not be visually observed in Fig. 5a whether channel 2 signal is triggered or not. Fig. 5b shows that power trace voltage level and voltage swing are also alternated every 2.56μs.

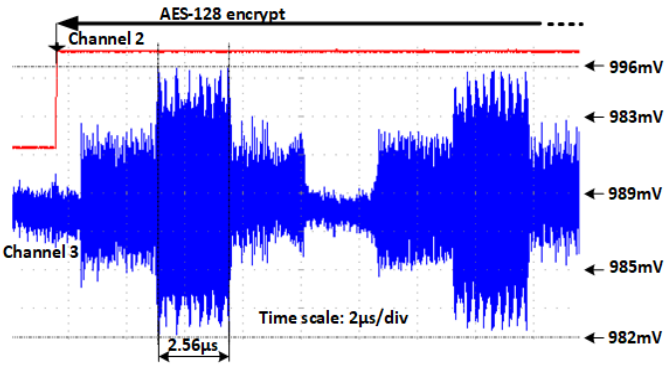
Resource utilization of the proposed platform is shown in Table I. The most critical resource is LUT. Entire proposed platform, which includes two Rocket cores, utilizes nearly 70% number of LUT available in Kintex-7 XC7K160T FPGA on Sakura-X board. Most of used LUT are spent on these cores, around 25% each. Meanwhile, the proposed Clock Divider module only requires 0.03% of available LUT and 0.01% of available FF.

IV. Discussions

Results from previous section is obtained by utilizing a specific, simple design of Clock Divider module. In its autonomous mode, the clock frequency alternation period is fixed to 256 clock cycles of system clock. However, this frequency alternation period can be flexible. System designers are free to design their own module with alternation period that suited their system requirements. Besides, the frequency



(a) Measured power trace of full AES-128 encrypting interval.



(b) Measured power trace at the start of AES-128 encrypting interval.

Fig. 5: Measured power trace when Clock Divider module operates in autonomous mode.

TABLE I: Post-implementation utilization.

Resource	Available	Proposed U500-Freedom platform		RocketTile module		Clock Divider module	
		Utilization	*Utilization%*	*Utilization*	*Utilization%*	*Utilization*	*Utilization%*
LUT	101,400	68,124	67.18	25,557	25.20	27	0.03
LUTRAM	35,000	3,037	8.68	112	0.32	0	0
FF	202,800	42,585	21.00	14,403	7.10	22	0.01
BRAM	325	50	15.38	24	7.38	0	0
DSP	600	30	5.00	15	2.50	0	0
MMCM	8	2	25.00	0	0	0	0
PLL	8	1	12.50	0	0	0	0

alternation period can even be dynamically changed during system operations by using same design concept that allows dynamic changing of clock scaling ratio in proposed platform. Furthermore, since frequency alternation is independent with cryptographic encryption, applying DFS will cause severe misalignment, in both time and amplitude, between all measured power traces. This misalignment may not be enough to prevent DPA but it will significantly increase the number of power traces required to retrieve a secret key. Lastly, applying DFS does not affect the cache coherency of U500-Freedom platform. The cache coherence is maintained by the policies [14] and actual open-source implementation of TileLink interconnects between modules in platform.

V. Conclusion And Future Works

This article demonstrates using Dynamic Frequency Scaling technique as a countermeasure against Simple Power Analysis attack for RISC-V processor. Implementation results on FPGA show that simple DFS technique can cover sensitive operations of processor from visual observation on power consumption traces while hardware requirement is virtually unchanged. The drawback of applying DFS technique is that average clock frequency of RISC-V processor is significantly reduced. Future works will focus on minimizing this disadvantage and evaluate effectiveness of using DFS technique against more complicate power attack analysis, such as Differential Power Analysis attack.

Acknowledgment

This paper is based on results obtained from a project commissioned by the New Energy and Industrial technology Development Organization (NEDO).

References

[1] http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-X.html
[2] O. Lo, W. J. Buchanan and D. Carson, "Power analysis attacks on AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)," J. Cyber Security Technology, vol. 1, pp. 88-107, Sep. 2016.
[3] P. Kocher, J. Jaffle, B. Jun et al., "Introduction to differential power analysis," J. Cryptographic Engineering, vol. 1, pp. 5-27, Apr. 2011.
[4] J. S. Coron, P. Kocher and D. Naccache, "Statistics and secret leakage," , in Proc. of International Conference on Financial Cryptography, pp. 157-173, 2001.
[5] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," in Proc. of 19th annual international cryptology conference, pp. 388-397, 1999.
[6] L. Benini et al., ''Energy-aware design techniques for differential power analysis protection," in Proc. of the 40th Annual Design Automation Conference, pp. 36-41, Jun. 2003.
[7] E. Laohavaleeson and C. Patel, "Current flattening circuit for DPA countermeasure," in Proc. of 2010 IEEE International Symposium on Hardware-Oriented Security and Trust, pp. 118-123, Jun. 2006.
[8] M. Kar et al., "Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," in Proc. of 2017 IEEE International Solid-State Circuits Conference, pp. 1-4, Feb. 2017.
[9] J. Daeme, V. Rijmen, "Resistance Against Implementation Attacks: A Comparative Study of the AES Proposals," in Proc. of Second Advanced Encryption Standard Candidate Conference, pp. 122-132, Mar. 1999.
[10] T. S. Messerges, "Securing the AES Finalists Against Power Analysis Attacks," in Proc. of International Workshop on Fast Software Encryption, pp. 150-164, Jan. 2002.
[11] S. Yang et al., "Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach," in Proc. of the Conference Design, Automation and Test in Europe, pp. 1-6, Mar. 2005.
[12] K. Asanovic et al., "The rocket chip generator," Dept. Elect. Eng. Comput.Sci., Univ. California at Berkeley, Berkeley, CA, USA, Rep. UCB/EECS-2016, Apr, 2011.
[13] https://github.com/kokke/tiny-AES-c.
[14] Sifive Company., "SiFive TileLink Specication Version 1.8.1," 2020 [Online]. Available: https://sifive.cdn.prismic.io/sifive/7bef6f5c-ed3a-4712-866a-1a2e0c6b7b13_tilelink_spec_1.8.1.pdf [Accessed: 16-Mar-2020]