Reconfigurable switched capacitor DC-DC converter for improved security in IoT devices

Ruzica Jevtic
Escuela Politecnica Superior,
Universidad San Pablo-CEU, CEU Universities
Madrid, Spain
Email: ruzica.jevtic@ceu.es

Marko Ylitolva and Lauri Koskinen
Department of Future Technologies,
University of Turku
Finland
Email: marko.ylitolva@utu.fi and lauri.koskinen@utu.fi

***Abstract*—With the ever increasing number of IoT devices, security and energy efficiency have become critical constraints in circuit design. To achieve small size and energy efficiency, devices need to be supplied by on-chip regulators. The power line generates the strongest signal in the circuit, and it is exploited for both, power and electromagnetic, side-channel attacks. In this work we propose to improve the security of the on-chip switched capacitor DC-DC converters by randomly switching between different converter topologies. Random ripple size and maximum supply voltage modulate the circuit current and power consumption, making the circuit more robust against side-channel attacks. We analyze the most common converter topologies and propose reconfigurable switched-capacitor cell for the efficient implementation in CMOS technology. The results show that power and time entropy of the proposed cell are increased significantly when compared to the commonly used DC-DC converter cell. There is around 6% variation in the DC-DC switching frequency for the constant load, and additional noise is observed in the frequency spectrum of the measured signal, thus, increasing the difficulty of the attack.**

I. Introduction

The world is on the brink of a massive breakthrough of Cyber-Physical Systems: the connected swarm of the Internet of Things (IoT). The IoT nodes need to be secured against security threats known as hacking. IoT hacking ranges from nuisances (tampering with home appliances, such as air conditioners or lights) and thefts (hacking into home security) to dangerous (hacking into cars or pace makers), to name but a few examples. Consequently, security is becoming a critical constraint, along with cost, power consumption and performance. Since the majority of the IoT devices will be battery operated and stay unattended for months or even years, a real challenge lies in securing these devices without increasing excessively their power consumption.

Cyber attacks that extract sensitive information by measuring physical signals of the chip are called side-channel attacks. They use physical leakage from the device under attack such as: power consumption, execution time, electromagnetic (EM) emanations, etc. In this work, we focus on the power attacks, also known as power analysis attacks. Additionally, we argue that the proposed technique can improve the robustness against EM attacks too.

In order to perform a power attack, the attacker first measures the actual power consumption of cryptographic device for different inputs [7]. From these test measurements, the attacker annotates the relative difference between the power consumption for each possible key. The attacker can then deduce which key is being processed by measuring the power of the real device under attack, and finding the highest correlation between the measured power signal and the initial test power measurements.

Many of the countermeasures for the power attacks of IoT devices are based on on-chip voltage regulation. Voltage regulators need to adapt the battery voltage to the power supply of the chip and are also used for dynamic voltage scaling to improve the energy efficiency of the system [2], [3], [5].

Inductive converters have bulky inductive components off chip that increase the size of the chip and are therefore not suitable for small IoT nodes. Only two circuits currently provide on-chip voltage regulation: linear regulators and switched-capacitor circuits. Although linear regulators are a mature technology, they are incapable of achieving high efficiency across a wide range of output voltages. Additionally, they seem to offer limited protection against side-channel attacks since the only tuning knob for introducing randomness in the power profile of the circuit is to scale the voltage randomly [6].

In this work, we consider switched-capacitor voltage regulators. Their benefits include full on-chip integration, no bulky inductive elements, and they can be reconfigured to achieve multiple output voltage levels without a significant loss in efficiency [2], [15]. They also have several tuning knobs to randomize the output voltage and de-correlate the chip activity from the physical leakages of the chip including both power consumption and EM emanations.

Our work is targeting low power IoT devices operating under changeable power supply voltage. Achieving low-energy operation is inherently also a security measure. The smaller the energy consumption, the harder it is to reliably measure the power consumption. Additionally, relaxing the output voltage ripple specifications of the DC-DC converter has proven to save a considerable amount of energy [2], [5]. In order to successfully protect the circuits from the functional errors that might arise as a consequence of changeable power supply, special error-protection technology and/or adaptive clocking can be used. The error-protection circuits guarantee correct functionality when the device is operating in the subthreshold

region, while the adaptive clocking has been used for the dynamic and voltage scaling. The voltage ripple adds an element of entropy to the system both in the time and voltage domains. This entropy also serves as additional security against side-channel attacks.

We develop reconfigurable switched capacitor cell that switches between different topologies for the same conversion ratio. The cell has only two additional switches compared to the standard switched capacitor cell. The power trace entropy (PTE) of the converter is increased due to the different ripple size produced by the topologies, and thus, different measured power for the same load. Furthermore, due to the variation in the voltage slope for the constant load, there is around 6% variation in the DC-DC switching frequency, and additional noise can be observed in the frequency spectrum of the measured signal. By increasing both, timing and power, entropy, the security features of the circuits are significantly improved. Although we do not directly analyze the effect of the proposed technique on the EM attacks, it seems that the robustness of the circuit against this type of the attacks improves too. The DC-DC converter generates the strongest signal in the circuit and consequently, has the highest EM emanations. Thus, the less correlated the DC-DC signal is from the workload, the better it masks the chip activity.

This paper is organized as follows. In section II we present the related work. In section III we describe the most commonly used switched capacitor topologies. In Section IV we propose the reconfigurable switched capacitor cell for efficient implementation in CMOS technology. In section V, we present the experimental results. Finally, section VI concludes this work.

II. Related work

Countermeasures based on chip voltage regulation are currently gaining attention since the voltage regulator is a block that is already present in embedded devices and security features added to the regulator produce less area and power overhead. The work in [10] presents a buck converter with control logic based on pseudo random hysteresis in order to enhance security against power side-channel attacks. Although it is oriented towards IoT devices, the converter needs to be implemented off-chip, so it is not suitable for small IoT sensors and per-core DVFS schemes in many-core systems.

In [6], the authors propose to randomly scale the output voltage. Randomizing the output voltage will lead to the corresponding scaling in the output current disabling the attacker to perform one-on-one mapping of the power consumption and particular secret key computation. The methodology is applied to on-chip voltage regulators.

In [8], the authors propose a methodology to randomly change the pattern for activating switched-capacitor cells. They are targeting multi-stage interleaved switched-capacitor converter. Their technique is applied to DVFS, and the number of activated switched capacitor cells depends on the workload. Consequently, the presented methodology is still vulnerable to power side-channel attacks that are syncronized with the converter switching frequency. The same authors in [9] improve their security technique by utilizing flying capacitors to withold random amount of charge for a random period of time.

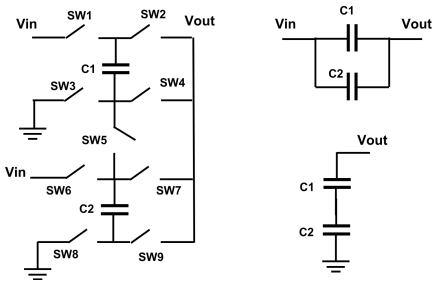

Fig. 1. Series parallel reconfigurable converter

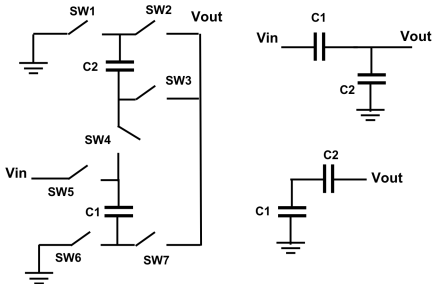

Fig. 2. Dickson 1:3 converter

III. DC-DC converter topologies

We analyze down-converters that are capable of converting battery voltage of 1.5V down to the range of [0.5V - 1V]. The most commonly used topologies found in the literature include series-parallel, ladder, dickson and fractional topology [11].

The reconfigurable cell for series parallel converter is presented in Fig. 1. This converter is capable of achieving three different input-output ratios: 1:3, 2:3 and 1:2 [15]. In this work we will use 1:3 and 2:3 configurations. When the converter is operating in 2:3 configuration, the flying capacitors are connected in parallel between input node and output node in the first switching phase, while the capacitors are discharged in series to the output in the second phase . The left hand side of the Fig. 1 shows the entire topology while the right hand side shows the configurations during both switching phases. For 1:3 configuration, the flying capacitors are connected in series between the input and the output voltage, while in the second phase, they are connected in parallel and discharged to the output.

The ladder converter consists of two series-capacitor strings that slide along each other while charging from the supply and discharging towards the load [11]. The dickson converter has a similar structure to the ladder topology in that it has two ladders of capacitors [12]. However, both ladders move with respect to the ground. Dickson topology also has the advantage of using fewer capacitors compared to the ladder topology for the same input-output voltage ratio [13]. The dickson converter used in this work is similar to the one used in [5]. The topology for both switching phases are presented in Fig. 2.

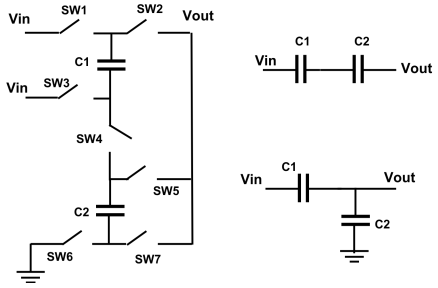

Fig. 3. Fractional 2:3 converter

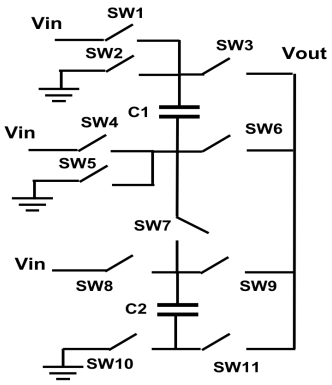

Fig. 4. Proposed reconfigurable switched capacitor cell

The fractional converter [14] is presented in Fig. 3. This type of converter is connected to the input voltage in both switching phases. Right hand-side of the Fig. 3 shows the converter in both switching phases. The ratio used for this converter is 2:3.

In this work we choose to combine series-parallel converter and the fractional converter for 2:3 conversion ratio and series-parallel converter and the dickson converter for 1:3 conversion ratio. Due to the different dynamics of the switching phases, both the ripple size and the discharging time will differ between the two topologies. This will cause a change in the amplitude of the current and its time dependence. The chosen topologies are presented as a proof-of-concept. The methodology can be applied to any two combinations of the above mentioned topologies, as long as the charging and discharging phases differ in the impedance sufficiently enough as to generate output waveforms with different ripple size and timing characteristics.

IV. Reconfigurable switched capacitor cell structure

Fig. 4. presents reconfigurable switched capacitor cell that is capable of achieving three different conversion ratios: 1:2, 2:3 and 1:3 and three different converter topologies: series-parallel, dickson and fractional. Two MIM flying capacitors of equal size are used for the implementation. The proposed cell has only two additional switches compared to the reconfigurable cell used for DVFS in [15]. If thin-oxide devices are used for the switches, two additional switches are needed to connect in series with the switches SW2 and SW5 to protect them from the high overdrive voltage. Even though the series-parallel configuration with 1:2 conversion ratio is not combined with any other topology, it can be useful when DVFS methodology is applied to the circuit.

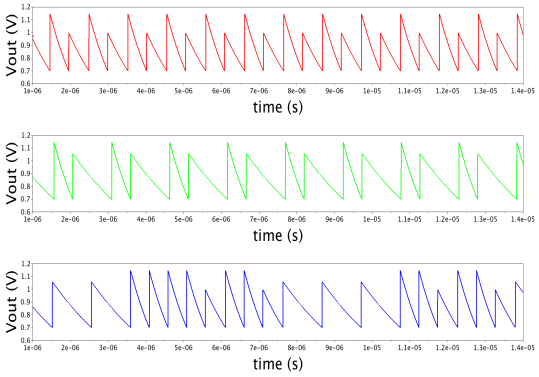

Fig. 5. Output voltage waveforms for 2:3 series parallel (red), 2:3 fractional (green) and combination of the two topologies (blue)

The configuration of the switches is shown in Table 1. For the series parallel topology, the output impedance of the converter will depend on the parallel connection of the two flying capacitors in one switching phase, while this connection will be serial in the other switching phase. As a result, the ripple size in both phases will not be equivalent. Following the same reasoning, it can be seen that the output impedance for the Dicskon and the fractional topology will change in a similar fashion. However, due to the different connections to the output and input voltage, both ripple size and the voltage slope will be different when compared to the series-parallel topology.

V. Experimental results

We have implemented the reconfigurable DC-DC converter in 28nm FDSOI technology. In order to accelerate the simulations for many different topologies, we have built a simulation flow in Matlab. The functionality of the DC-DC converter has been described by using differential equations and the veracity of the flow has been confirmed by Cadence simulations.

We choose 1.5V as an input voltage that corresponds to most battery voltage levels. Each switched-capacitor topology has two identical flying capacitors equal to 1nF. In all simulations, we apply constant resistive load of 1KΩ as to separate the effect that random voltage has on the security features of the chip. The load value and the flying capacitor size was chosen to match the mircroprocessor design presented in [5]. When the load is constant, the side-channel attacks are easier. Therefore, the analysis presented here should provide a fair insight in the improvement of the chip security.

Fig. 5 shows the output voltage for the series-parallel topology with 2:3 conversion ratio (red), the output voltage for the fractional 2:3 topology (green) and the output voltage when these two topologies are combined and we switch between them randomly. The reference voltage of 0.7V is chosen for this experiment. As mentioned before, we are targeting IoT

TABLE I
SWITCH CONFIGURATION FOR DIFFERENT TOPOLOGIES

Topology	Conv. ratio	F1	F2	always OFF
Series Parallel	1:2	sw1, sw6, sw8, sw11	sw3, sw5, sw9, sw10	sw2, sw4, sw7
Series Parallel	1:3	sw1, sw7, sw11	sw3, sw5, sw9, sw10	sw2, sw4, sw6
Series Parallel	2:3	sw1, sw6, sw8, sw11	sw3, sw7, sw10	sw2, sw4, sw9
Dickson	1:3	sw2, sw6, sw8, sw11,	sw3, sw7, sw10	sw1, sw4, sw5, sw9
Fractional	2:3	sw1, sw7, sw11	sw3, sw4, sw9, sw10	sw2, sw5, sw6, sw8

devices that are operating under changeable supply voltage and can withstand large ripple size. It can be seen from Fig. 5 that, if the attacker has no information on the actual implementation of the DC-DC converter, he or she may assume that different timing and ripple size occur due to the different load, making the circuit more robust against power side-channel attacks.

Similar to 2:3 conversion ratio topologies, the proposed reconfigurable cell allows for the combination of 1:3 series-parallel topology and 1:3 dickson topology.

In order to evaluate the effectiveness of the proposed method, we use a similar methodology to the one that is presented in [8]. First, we analyze power trace entropy (PTE). When there is a one-to-one relationship between the measured power and the load power, the entropy is equal to zero. However, if different measured power values (i.e. P_{in}^1, P_{in}^2, ... P_{in}^k) can be obtained for the same load, the PTE of the converter can be computed as:

$$PTE = -\sum_{l=1}^{k} p_l \cdot log_2 p_l \tag{1}$$

where p_l is the probability of the measured input power P_{in}^l.

We analyze the PTE when the load is constant, since this seems to be the lower bound for the power trace entropy. When the load is time-dependent, there will be and additional number of possible input power values and thus, the entropy will result in a higher value. Higher PTE value indicates better protection against power side-channel attacks.

We assume that the input power for the given load in the first switching phase of the series parallel and fractional converter are P_1 and P_2 respectively, while the input powers for the second switching phase are P_3 and P_4, respectively. Since the topology for each switching phase is chosen randomly between two possibilities (i.e. between P_1 and P_2 for the first switching phase, and between P_3 and P_4 for the second switching phase) the total number of equally probable different measured power values in one DC-DC switching cycle is four. Therefore, the PTE of the converter also becomes four (i.e. $PTE = -\sum_{l=1}^{4} 0.25 \cdot log_2 0.25 = 4$). It can be seen that, switching between different topologies produces non-zero PTE resulting in a circuit more robust against side-channel attacks. Moreover, the presented technique is compatible with any other security measure applied to the voltage regulators, such as random scaling of the reference voltage or random change in the pattern for activating different DC-DC stages.

In order to evaluate the entropy introduced in the time-domain, we plot Fast Fourier Transform (FFT) of the measured

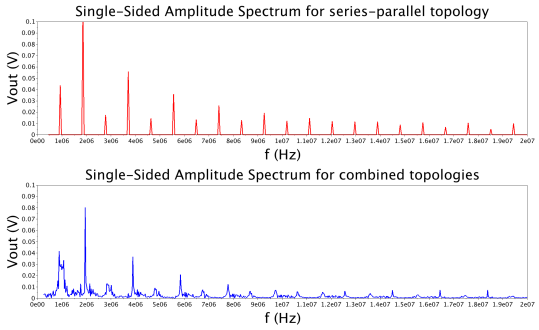

Fig. 6. FFT for the output voltages of 2:3 series-parallel topology and combination of 2:3 series-parallel and 2:3 fractional topology

output signal. The results are shown in Fig. 6. We have plotted the FFT without the DC component for the sake of clarity. It can be seen that the FFT of the power signal obtained when two different topologies are used, contains much more noise in the spectrum when compared to the FFT of the power signal when only one topology is used. It can also be seen that there is a variation in the frequency for the main harmonic around 2MHz that indicates the switching frequency of the converter. We found it to be around 6%. This change in the frequency is due to the different impedance of the converter in each switching phase. For example, it can be seen that the duration of the two switching phases differ for the series parallel topology. The same applies for the fractional topology. Additionally, the duration of the switching phases of one topology differs when compared to the duration of the switching phases of the other topology. When combined, the mean switching frequency gets shifted when compared to the single topology converter, thus adding time uncertainty to the DC-DC signal.

Since these effects are produced for the constant load, they will only intensify for the real-world case where the load is time-dependent, thus proving the effectiveness of the proposed method.

VI. CONCLUSION

In this paper we have presented a reconfigurable switched capacitor DC-DC converter that is used for improving the security features of the IoT devices. The converter is capable of achieving three different conversion ratios: 1:2, 1:3, and 2:3 making it also suitable for DVFS methodology. It can be reconfigured to implement three different topologies: series-parallel, dickson and fractional. By switching randomly between the topologies, we are able to increase both, power and

time entropy of the circuit, making it more secure from side-channel power attacks. The proposed methodology is compatible with the security techniques reported in the literature for the on-chip voltage regulators.

REFERENCES

[1] S. Guilley, et. al., *Evaluation of Power-Constant Dual-Rail Logic as a Protection of Cryptographic Applications in FPGAs*, Secure System Integration and Reliability Improvement, 2008. SSIRI'08, pg. 16-23.

[2] R. Jevtic et. al., *Per-Core DVFS for Many-Core Processors in 28nm FDSOI Technology*, IEEE Transactions on VLSI Systems, 2014.

[3] B. Zimmer et. al., *A RISC-V Vector Processor with Tightly-Integrated Switched-Capacitor DC-DC Converters in 28nm FDSOI*, Journal of Solid-State Circuits, 2016.

[4] M. Hiienkari et. al., *A 1.67pJ/cyc 32-bit RISC CPU with Timing-Error Prevention and Adaptive Clocking in 28nm CMOS*, the IEEE Custom Integrated Circuits Conference (CICC), 2014.

[5] M. Turnquist et. al., *Fully Integrated DC-DC Converter and a 0.4V 32-bit CPU with Timing-Error Prevention Supplied from a Prototype 1.55V Li-ion Battery*, VLSI Symposium 2015.

[6] D. Kamel et. al., *Towards securing Low-Power Digital Circuits with Ultra-Low-Voltage Vdd Randomizers*, International Conference on Security, Privacy, and Applied Cryptography Engineering, 2016.

[7] K. Baddam and M. Zwolinski, *Evaluation of Dynamic Voltage and Frequency Scaling as a Differential Power Analysis Countermeasure*

[8] O.A. Uzun and S. Kose, *Converter gating: A power efficient and secure on-chip power delivery system*, IEEE J. Emerging Sel. Topics Circuits Syst., vol. 4, no. 2, pp. 169179, Jun. 2014.

[9] Weize Yu and Selcuk Kose, *Charge-Witheld Converter Reshuffling: A Countermeasure Against Power Analysis Attacks*, IEEE Transactions on Circuits and Systems II, vol.63, no. 5, May 2016.

[10] L-C. Chu et. al., *An Enhanced Security Buck DC-DC Converter with True-Random-Number-Based Pseudo Hysteresis Controller for Internet of Everything (IoE) Devices*, International Solid-State Circuits Conference, Feb. 2018.

[11] T. Van Breussegem and M. Steyaert, *CMOS Integrated Capacitive DC-DC Converters*, Analog Circuits and Signal Processing, Springer 2013.

[12] M. Seeman, *Analytical and Practical Analysis of Switched-Capacitor DC-DC Converters*, Technical Report, UC Berkeley, September 2006.

[13] V. Wai-Shai Ng and S. Sanders, *Switched-Capacitor DC-DC Converter: Superior where the Buck Converter has dominated*, Technical Report, UC Berkeley, August 2011.

[14] Makowski and Maksimovic, *Performance limits of switched capacitor DC-DC converters*, 1995.

[15] H.P. Le, S. Sanders and E. Alon, "Design techniques for fully integrated switched-capacitor DC-DC converters, IEEE J. Solid-State Circuits, vol. 46, no. 9, pp. 21202131, Sep. 2011.