Evaluation of Dynamic Voltage and Frequency Scaling as a Differential Power Analysis Countermeasure

Karthik Baddam, Mark Zwolinski
School of Electronics and Computer Science, University of Southampton, Southampton, UK. SO17 1BJ.
Email: kb04r, mz@ecs.soton.ac.uk

Abstract— **Differential Power Analysis (DPA) attack is a major concern for secure embedded devices [1]–[3]. Currently proposed countermeasures [4]–[10] to prevent DPA imposes significant area, power and performance overheads. In addition they either require special standard cell library and design flows or algorithmic modifications. Recently, Random Dynamic Voltage and Frequency Scaling (RDVFS) has been proposed [11] as a DPA countermeasure, which has less area, power and performance overheads and it does not require special cell library nor design flows nor algorithmic modifications. However, in a synchronous digital circuit, the operating frequency can be detected by monitoring glitches on the power line. In this paper, we show that using this information, it is possible to mount a DPA attack on circuits employing RDVFS countermeasure. We propose an alternative technique which only varies the supply voltage randomly. Experimental results on AES core with SPICE level simulations show that our proposed method significantly weakens the DPA attack by reducing the correlation of power to processed data.**

I. Introduction

Security is becoming an important metric along with cost, performance and power consumption in embedded systems such as smart-cards, PDAs and pay TV [1]. A typical cryptographic algorithm is used to implement the secure part, usually refereed to as a cryptographic device. A cryptographic device can be part of an embedded system (pay TV, PDA) or a system on its own (smart card). In either case, the whole system has to be secure and protect its contents - mainly its data and secret keys.

Traditional cryptanalysis (attempt to circumvent the security of a cryptographic algorithm) is based on observation of inputs and outputs of the cryptographic device. The cryptanalyst (usually referred to as 'attacker') would attempt to extract the 'secret key' based on these observations and some knowledge of the implemented algorithms. This has led to the development of mathematically more 'secure' algorithms, such as AES [12], where extracting the secret keys based on the input-output relation is extremely difficult.

Even though the algorithm is secure from a mathematical point of view, its hardware implementation leaks some information through power consumption, time of execution, electromagnetic radiation, etc. that can be utilised in extracting the secret key. In the jargon of the cryptography, such information is known as 'side channel information' and the attacks based on this are called Side Channel Attacks. One such type of side channel information is the power consumption of the cryptographic device. Attacks based on the power consumption are known as Power Analysis Attacks. Differential Power Analysis (DPA), first published by Kocher [2], is one type of Power Analysis Attack where statistical techniques are used to find the secret key. DPA attacks can be successful and DPA countermeasures are a major concern for secure embedded systems [3]. As a result, researchers have developed several DPA countermeasures [4]–[10], [13]. Although some of these countermeasures have been reported successful, their implementation incurs high area and power overheads [4]–[10]. In this paper, we investigate area and power efficient countermeasures employing Random Dynamic Voltage and Frequency Scaling proposed in [11]. Using SPICE simulations, we find serious limitations for this approach. We propose an alternative Random Voltage Scaling approach and evaluate our method on a test circuit by implementing DPA attack.

The rest of this paper is organised as follows: Section II discusses previous work. Section III introduces our DPA flow and test circuit. In this section we implement a DPA attack on test circuit and use these results to compare countermeasures. In Section IV we show that by finding the operating frequency, one can still successfully attack an algorithm employing Random Dynamic Voltage and Frequency Scaling. In Section V we propose to keep the frequency constant and randomly vary voltage and show its effectiveness against DPA. In Section VI we discuss conclusions and future work.

II. Previous Work

Successful DPA attacks on cryptographic implementation were reported in [3], [14]. As a result, a number of countermeasures to DPA have been proposed. DPA countermeasures on the algorithmic level include random masking of intermediate variables [4], [13]. These are platform-dependent countermeasures and require a substantial processing time overhead, increased power consumption and area.

On the hardware side, system level techniques include adding noise to the device power consumption through additional logic [5], which need circuit-level modifications and requires more area. Bucci et al [6] proposed a random pre-charging countermeasure to prevent DPA which adds noise to the device power consumption through random pre-charging and showed that this countermeasure was able to reduce the

20th International Conference on VLSI Design (VLSID'07)
0-7695-2762-0/07 $20.00 © 2007 IEEE

correlation of power consumption to data but not completely prevent DPA. However this countermeasure has less area, power and processing overheads when compared to other methods and is an attractive method to integrate with other countermeasures to prevent DPA.

Gate level countermeasures are based on masking at gate-level. These gate-level cells can be made available through a library of masked standard cells. These cell's power consumption will be uncorrelated to processed data [7], however these countermeasures have large area, power consumption and performance overheads.

A transistor level approach to prevent DPA is based on the adoption of a logic family whose power consumption is independent of the processed data such as [8]–[10]. Countermeasures based on logic design styles (transistor-level) have good security characteristics, but they tend to be expensive in terms of area, performance and power consumption. Moreover countermeasures based on logic design styles need a custom design approach thus increasing design time and costs.

Yang et al [11] proposed Dynamic Voltage and Frequency Scaling as a countermeasure to prevent DPA by altering voltage and frequency randomly, thus reducing the correlation of input data to the power consumed. We call the technique used in [11] Random Dynamic Voltage Scaling (RDVFS) to avoid confusion with normal Dynamic Voltage and Frequency Scaling (DVFS) technique [15]. The difference between RDVFS and DVFS is that RDVFS randomly scales voltage and frequency to randomise the power consumption, whereas DVFS scales voltage and frequency to save power consumption. In both DVFS and RDVFS the voltage and frequency $\{V_{dd}, f\}$ pairs are same, i.e. if f is changed V_{dd} is changed accordingly.

The main advantage of RDVFS as a DPA countermeasure is that it does not need the cryptographic algorithm to be altered nor its implementation design flow. As RDVFS does not process random data (like masking countermeasure) nor includes complementary logic styles (like transistor-level countermeasures) to prevent DPA, its area and power overhead are less. However Yang et al [11] did not verify the effectiveness of RDVFS by implementing a DPA attack. In Section IV we evaluate RDVFS by implementing DPA attack on a test circuit.

It is well know fact that security comes at a price. Every countermeasure so far presented has some overhead. Some of them higher than other. Although transistor level countermeasures are shown to be very secure, they require special design flows and require special attention to routing, to balance the routing capacitance on both the complementary outputs. Similarly gate level countermeasures need special standard cells and hence require a semi custom design flow. Algorithmic countermeasures only modify the algorithm and do not require special design flow, but these solutions are specific and are not portable. Designers of secure devices have to trade-off security against device cost (implementation and overhead costs). For some applications combining more than one low implementation cost countermeasure might be attractive than using a high implementation cost countermeasure.

III. DPA Attack flow and Test Circuit

To perform a DPA attack, the attacker first chooses 'N' plain_text (inputs to the cryptographic device), then measures the actual power consumption of cryptographic device in operation for 'N' ($round\_limit$) encryption rounds and stores this information with respect to $plain\_text$ or $cipher\_text$ $[P_1, P_2, ...P_N]$. Here encryption round or round is referred to as one plain_text (input) to cipher_text (output) operation, not AES internal rounds. Then he/she predicts the power consumption for each possible key for the same $plain\_text$, refered to as Hypothetical power consumption. For example, $[H1_1, H1_2, ...H1_N]$ for key 1, $[H2_1, H2_2, ...H2_N]$ for key 2 and so on. Note that the Hypothetical (predicted) power consumption does not necessarily represent exact values, it is the relative difference between them that is important [16]. The attacker then correlates the Hypothetical power consumption ($[Hi_1, Hi_2, ...Hi_N]$) of each key to that of the actual power consumption ($[P_1, P_2, ...P_N]$). Correlation for the actual key would be higher than the other keys. The detailed theory behind the Power analysis attacks has been presented in [2], [16]. As DPA relies on statistical analysis, the quality of analysis increases with 'N' (number of encryptions).

To compare the effectiveness of a countermeasure, we implemented DPA on a AES [12] test circuit without any countermeasures. Our AES architecture was similar to the one in [3]. Our AES circuit was implemented on AMS 0.35μm technology. Simulations have been done on a SPICE netlist without routing parasitics (to increase simulator speed) using the fast spice simulator Nanosim from Synopsys [17]. To limit the time spent on simulation, encryption rounds of 10,000 ($round\_limit$) has been chosen. This simulation, which was run on a workstation running RHEL4 on AMD Opetron 246 with 1Gb memory, took about 25 hours of CPU time.

The simulated data is then processed through software developed by the authors to implement a DPA attack. As shown in Fig 1, this software has three main modules: 1) A pre-processing and partitioning tool which can pre-process and partition the simulation results 2) A generic test bench with customisable key hypothesis, when simulated with RTL/Gate level model of circuit under test generates hypothetical power consumption, and finally 3) The Statistical analysis module which can perform 'Pearson Correlation' analysis [3] and 'Difference of Mean' analysis [2]. Although this flow is presently targeted towards the AES algorithm, because of its generic and modular nature it can be adopted to any algorithm and design flow. Particularly, DPA check can be done before and after place & route, enabling us to check for DPA resistance early in the design flow.

The DPA attack on the above AES circuit was targeted on the 8 MSB's (most significant bits) and the corresponding hypothetical power consumption was generated. The power analysis attack we implemented was similar to the one described in [3]. As expected the correct 8 key bits, 167 in our case, were found. The DPA result plot for two different numbers of encryption rounds (round_limit), 1000 and 10,000,

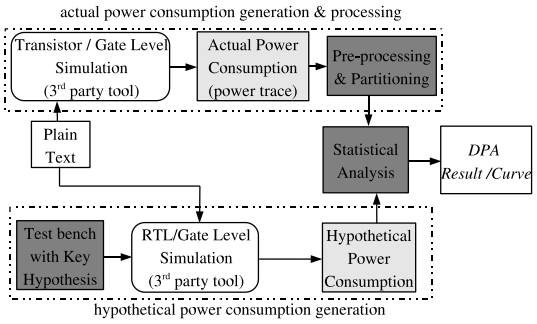


Fig. 1. Our DPA software flow.

is shown in Fig 2. The X-axis represents all possible key values (0 to 255) and the Y-axis represents correlation of a particular key's hypothetical power consumption to the actual power consumption. The key with highest correlation represents the correct key. It is also important to note that the absolute value of correlation for the correct key is not important, it is the relative value from other possible keys. As it can be seen in Fig 2, the correct key value was detected for 10,000 encryption rounds but not for 1000 encryption rounds. For our AES test circuit a minimum of 2500 rounds was needed to differentiate the correct key, i.e. for the correlation of correct key to be significantly higher than the correlation of other possible keys.

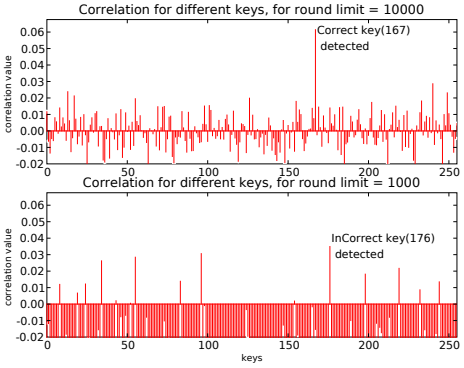


Fig. 2. DPA result of AES for 10,000 and 1000 encryption rounds, based on SPICE simulation using Nanosim

Because of the circuit complexity (and hence time) to simulate the entire AES circuit we choose a part of AES, the Sbox shown in Fig 3, to experiment on. Sbox is designed in combinational logic as described in [18]. Hypothetical power consumption is chosen as a function of toggling activity at the register R2. 'N' (encryption rounds) of 10,000 input plain texts have been applied to check DPA proof. Here encryption round refers to one input to output operation. This number has been arbitrarily chosen so that the encryption rounds should be large enough to get accurate results without dramatically increasing the simulation time. Although this circuit is trivial when compared to the complete AES system, it enables us to see the effectiveness of a countermeasure in a shorter simulation time. Moreover as the there is no other logic (circuit) operating in parallel in the Sbox circuit, the power consumption observed would have less noise than in AES circuit (as there is more logic operating at a given time in AES), thus any countermeasure proved against this circuit should work for the entire AES as well. The effect of noise can be clearly seen in Fig 4, the correct key detected for Sbox has much higher correlation value when compared to the DPA result on the entire AES in Fig 2.

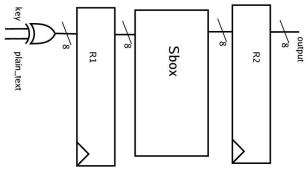


Fig. 3. Test Circuit 2 - AES Sbox.

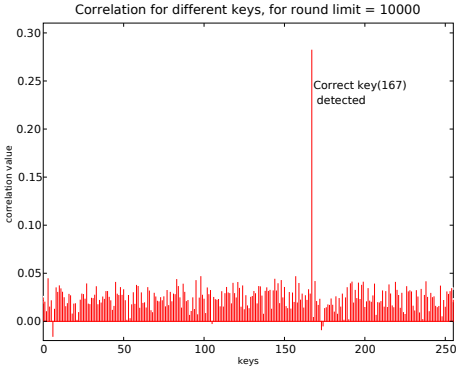


Fig. 4. DPA result for 10000 rounds on AES Sbox without any countermeasure.

IV. DPA ON CIRCUITS EMPLOYING RDVFS

Dynamic Voltage and Frequency Scaling (DVFS) is an effective approach to reduce energy [15]. DVFS utilises the fact that the power P is directly proportional to the clock frequency f and to the square of the supply voltage V_{dd}. $P \propto f \cdot V_{dd}^2$. In DVFS, scaling of supply voltage and clock frequency takes place dynamically to adjust to performance demand. Each such power-performance mode has a $\{V_{dd}, f\}$-pair, which are predetermined. It is important to note that frequency and voltage are both changed together as a pair and both these values are related. Yang et al [11] proposed to randomly vary voltage V_{dd} and frequency f to prevent DPA (RDVFS). This technique is similar to DVFS in that both vary voltage and frequency dynamically. Except RDVFS aim is to prevent DPA whereas DVFS aim is to reduce energy.

DVFS has been generally used with microprocessors to reduce overall power consumption, in the DPA context RDVFS as a DPA countermeasure is of interest to both microprocessors and ASICs. In order to check the effect of RDVFS on DPA, we implemented RDVFS on AES Sbox. Although our circuit is trivial when compared to a microprocessor, it enables us to

check the effectiveness of RDVFS as a DPA countermeasure. The $\{V_{dd}, f\}$-pairs have been arbitrarily chosen to bring in randomness. We assumed frequency and voltage change values instantly and are modelled as piecewise linear source in our SPICE simulations. We implemented a DPA attack as discussed in Section III and found that we could not find the key, this DPA result is shown in Fig 5.

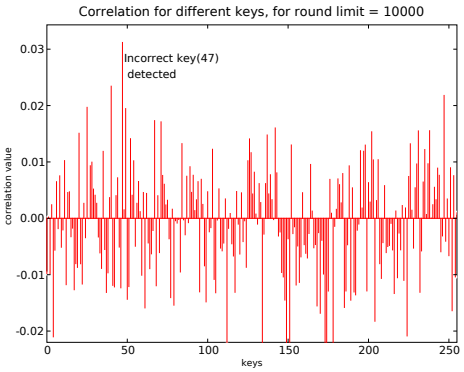


Fig. 5. DPA on Sbox with DVFS countermeasure

Most of the circuits used today are sequential, employing flip-flops and latches, i.e. circuit operation is synchronised to a single clock pulse. Thus at the rising (or falling) edge of a clock pulse, there will be a burst of operation (transistors switching) which will settle down towards the end of the clock period. Current consumed at the rising edge of clock pulse will thus be higher and goes down along with switching activity. This can be clearly observed in the Fig 6. From this it is clear that a change in frequency can be easily detected by observing the power consumption trace. Based on this, we observed the power consumption trace of Sbox employing RDVFS and recorded the circuit frequency for each input applied. By knowing the frequency, we found the voltage by looking at the voltage frequency $\{V_{dd}, f\}$-pairs. We changed our hypothetical power consumption to reflect the changes in frequency and voltage. With this new hypothetical power consumption we performed DPA attack on the same circuit, this time our attack was successful. Although we could not find an automated way to determine frequency from power consumption, this experiment shows that it is possible to implement DPA attack on systems employing the RDVFS countermeasure, where frequency and voltage values are related.

V. Random Supply Voltage Variation as DPA Countermeasure

As we showed in Section IV countermeasures that depend on varying the frequency are susceptible to DPA. Since frequency is easily detectable, one approach to overcome this would be to randomly change the supply voltage while keeping the frequency constant, such that the circuit is operational under all possible supply voltages as shown in 7(a). A simplified block diagram of the proposed method is shown in

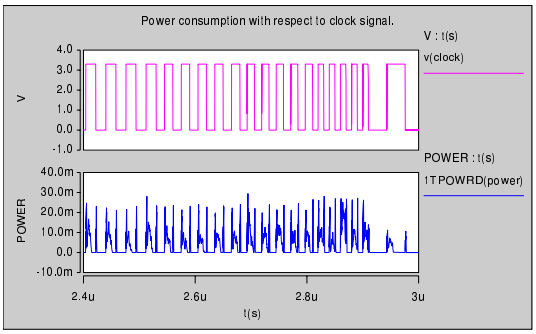
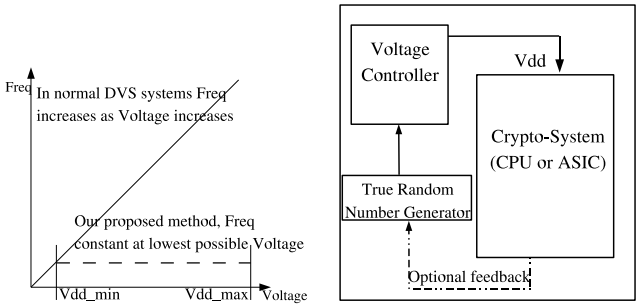


Fig. 6. Power consumption with respect to clock pulse

Fig 7(b). The additional blocks required are a true random number generator (RNG) and a voltage controller. RNGs already exists for secure smart card applications and are not additional overhead. A voltage controller is the only additional block required for this countermeasure. Benefit in this type of countermeasure is that it can be applied to a custom ASIC or a general Micro controller, without modification to the algorithm or its design flow (unlike masking countermeasures or gate level countermeasures). The main restriction of our proposed method is that the attacker should not have access to any of these blocks directly, i.e. if the connection between RNG and Voltage controller is cut off, then there would be no randomness in the power consumption.



(a) Voltage and Frequency relationship.

(b) Block diagram of our proposed method.

Fig. 7. Our proposed method.

As we propose to vary the voltage, the maximum limit of V_{dd} (V_{dd_max}), the minimum limit of V_{dd} (V_{dd_min}) and the frequency of change of V_{dd} (dvs_rate) affect the DPA result. This section discusses these parameters and their effect on DPA. For our countermeasure to work effectively, the change in power consumed ($\delta_{voltage}$) due to a change in Voltage (V_{dd}) should be close to change in power consumed ($\delta_{switching}$) due to a change in input (or switching activity). This is explained below.

Let $[In_1, In_2, In_3, In_4, In_5, In_6]$ be a set of input vectors and $[P1_1, P1_2, P1_3, P1_4, P1_5, P1_6]$ power consumed per input at voltage V_{dd1} and $[P2_1, P2_2, P2_3, P2_4, P2_5, P2_6]$

be the power consumed for same inputs at voltage V_{dd2} and $[P3_1, P3_2, P3_3, P3_4, P3_5, P3_6]$ for V_{dd3}. For a constant V_{dd}, the attacker can easily correlate the hypothetical power model and the actual power consumption to determine the key. But if the voltage was varied after input In_2 and In_4, then the resultant power consumption would be $[P1_1, P1_2, P2_3, P2_4, P3_5, P3_6]$ (assuming a change in supply voltage would take much less time when compared to the time to process each input). This would significantly reduce the correlation between input data and power consumption, as the difference in $P1_2 - P1_3$ is not same as $P1_2 - P2_3$. This can be seen as introducing randomness in power consumption. For this countermeasure to be effective, the difference in $P1_2 - P2_3$ should be equal to $P1_1 - P1_2$ or $P1_3 - P1_4$ or $P1_4 - P2_5$ or $P1_5 - P2_6$. i.e. a change in V_{dd} should manifest itself as a change in input. But finding V_{dd1}, V_{dd2} and V_{dd3} values to satisfy the above condition would be difficult as the inputs to the system can be any value (and are usually unknown). Moreover these values cannot be generalised, as the inputs (switching activity) and the voltage range vary from system to system.

The rate of change of voltage (dvs_rate) should be much less than the time to process the minimum number of inputs to successfully mount a DPA attack. For our test circuit AES, the minimum number of encryption rounds required to successfully implement a DPA attack was 2500. If dvs_rate is close to the above number, then the attacker could simply implement a DPA attack, before the randomness is introduced.

The amount of randomness in power consumption can be increased by increasing the available voltage range. i.e, if V_{dd_min} and V_{dd_max} are close to each other then the amount of randomness is less and if this range is more, randomness is more. Bo Zhai et al [15] discussed the limits of voltage scaling and showed that digital circuits can work even in the sub-threshold region. Since we propose to keep the frequency to the lowest possible, selecting the V_{dd_min} will be constrained by the expected circuit speed. However to overcome such a limitation, one could increase V_{dd_max} to increase the overall range at the expense of higher power consumption.

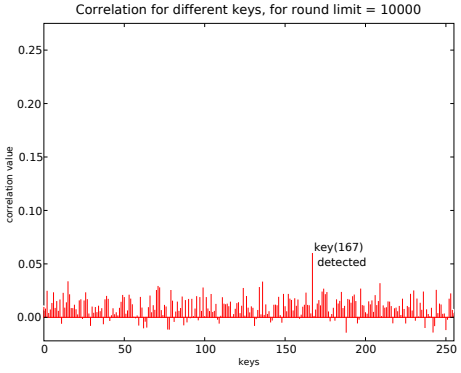


Fig. 8. DPA result for V_{dd_max} of 3.7v and V_{dd_min} of 1.6v for dvs_rate of 200.

To test the effect of voltage variation on DPA we first simulated AES Sbox (in Fig 3) with V_{dd_max} of 3.3v and V_{dd_min} of 3.0v and found that the correlation strength was lowered when compared to the Sbox without any countermeasure. When we increased the range, V_{dd_max} of 3.7v and V_{dd_min} of 1.6v, the correlation strength was lowered by at least 5 times, shown in Fig 8. We assumed that change in supply voltage is done instantly without any delay. While this assumption is not realistic, it quickly enables us to check the effectiveness of countermeasure, without affecting the quality of experiment. Fig 8 shows these results for dvs_rate of 10 to 1000. The X-axis represents dvs_rate and the Y-axis represents highest correlation value, second correlation value and their respective keys. From Fig 9 it is clear that the the correlation is reduced by 5 times for all the dvs_rate considered (10 to 1000). More importantly, the difference between the correct key's correlation and incorrect key's correlation has been reduced by 10 times.

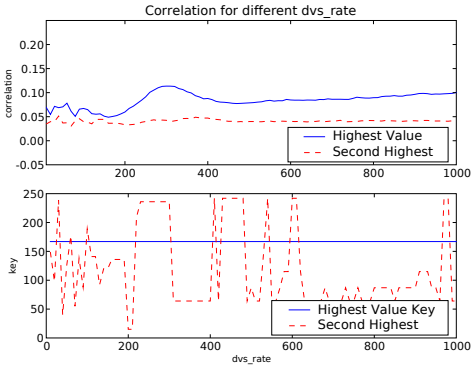


Fig. 9. DPA result for V_{dd_max} of 3.7v and V_{dd_min} of 1.6v for different dvs_rate.

Fig 10 shows the effect of the available V_{dd} range for dvs_step of 0.1v on DPA. It can be clearly seen that as this range (number of available V_{dd} to vary) increases, the correlation of the signal decreases. However for the set of experiments we conducted, the correlation of signal was never below a point where the secret key was undetectable.

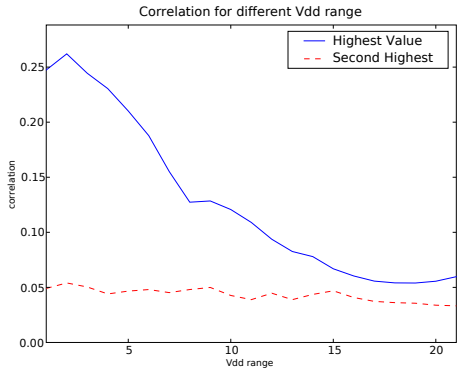


Fig. 10. DPA result for different V_{dd} ranges

All the above experiments were on a part of AES (Sbox) to reduce simulation time, however it is unlikely to be possible to observe only the power consumption of a part of the cryptosystem (circuit). To get a good estimate of our countermeasure on the entire AES, we simulated the entire AES with a V_{dd_min} of 2.8v, V_{dd_max} of 3.7v and a dvs_step of 0.1v for 10,000 encryptions ($round\_limit$). We found that for 10,000 encryptions the countermeasure was effective, the result is shown in Fig 11. However as DPA was successful on the Sbox circuit with our countermeasure, we conclude that our proposed method significantly increases the required number of encryptions rounds to mount DPA. As our method does not require the underlying algorithm or its logic to be altered, it is an ideal choice to be applied with other countermeasures to prevent DPA. Countermeasures such as Random pre-charging [6], which have been shown to have less overheads but are not entirely secure against DPA can be used with our proposed method to prevent DPA and can be a cost saving alternative than using a high overhead countermeasure such as [8], [10], which require custom design flows.

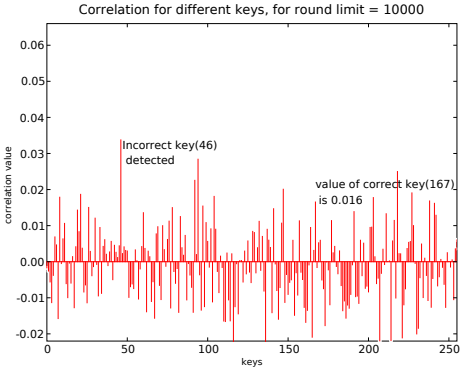


Fig. 11. DPA result of AES with a V_{dd_min} of 2.8v and V_{dd_max} of 3.7v

VI. Conclusion

We have discussed the limitations of RDVFS as a countermeasure for DPA. The operating frequency is detectable by monitoring glitches on the power supply. Our experiments indicate that this information can be successfully exploited by a DPA attacker and it severely compromises the the effectiveness of the proposed RDVFS countermeasure. We propose an alternative technique which randomly varies only the supply voltage while keeping the frequency constant. Our proposed method, when applied for encryption rounds of 10,000 to an AES Sbox, could lower the correlation strength by 10 times and when applied to the complete AES, the secret key was indistinguishable, and prevents the DPA attack. Our method does not require the underlying algorithm or its logic to be altered, which enables us to apply other countermeasures, such as [6], which have also been shown to reduce the correlation.

We will direct our future work to implementing the entire circuit i.e. AES, random number generator and voltage regulator and to see the effect on DPA of combining our proposed method with other countermeasures.

References

[1] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *Trans. on Embedded Computing Sys.*, vol. 3, no. 3, pp. 461–491, 2004.

[2] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 1999, pp. 388–397.

[3] S. B. Örs, F. K. Gürkaynak, E. Oswald, and B. Preneel, "Power-analysis attack on an asic aes implementation," in *ITCC '04: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) Volume 2*. Washington, DC, USA: IEEE Computer Society, 2004, p. 546.

[4] N. Pramstaller, "An aes asic-implementation resistant to differential power analysis," IAIK, University of Technology Graz, Austria., 2004, http://www.iaik.tu-graz.ac.at/research/sca-lab/publications/abstracts/index.php Downloaded on 16 july 2005.

[5] L. Benini, A. Macii, E. Macii, E. Omerbegovic, F. Pro, and M. Poncino, "Energy-aware design techniques for differential power analysis protection," in *DAC '03: Proceedings of the 40th conference on Design automation*. New York, NY, USA: ACM Press, 2003, pp. 36–41.

[6] M. Bucci, M. Guglielmo, R. Luzzi, and A. Trifiletti, "A power consumption randomization countermeasure for dpa-resistant cryptographic processors," *Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation. 14th International Workshop, PATMOS 2004. Proceedings (Lecture Notes in Comput. Sci. Vol.3254)*, pp. 481 – 90, 2004.

[7] T. Popp and S. Mangard, "Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints," in *Cryptographic Hardware and Embedded Systems – CHES 2005, 7th International Workshop, Edinburgh, Scotland, August 29 - September 1, 2005, Proceedings*, ser. Lecture Notes in Computer Science, J. R. Rao and B. Sunar, Eds., vol. 3659. Springer, 2005, pp. 172–186.

[8] K. Tiri and I. Verbauwhede, "Securing encryption algorithms against dpa at the logic level: Next generation smart card technology." in *CHES*, 2003, pp. 125–136.

[9] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Design and analysis of dual-rail circuits for security applications," *IEEE Trans. Comput.*, vol. 54, no. 4, pp. 449–460, 2005.

[10] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure dpa resistant asic or fpga implementation," in *DATE '04: Proceedings of the conference on Design, automation and test in Europe*. Washington, DC, USA: IEEE Computer Society, 2004, p. 10246.

[11] S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach," in *DATE '05: Proceedings of the conference on Design, Automation and Test in Europe*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 64–69.

[12] *Advanced Encryption Standard*, National Institute of Standards and Technology, 2001, http://csrc.nist.gov/CryptoToolkit/aes/ Downloaded on 15 July 2005.

[13] E. Oswald, "On side-channel attacks and the application of algorithmic countermeasures," Ph.D. dissertation, IAIK, University of Technology Graz, Austria, 2003, http://www.iaik.tu-graz.ac.at/research/sca-lab/publications/abstracts/index.php Downloaded on 15 July 2005.

[14] T. S. Messerges, D. E.A, and S. R.H, "Examining smart-card security under the threat of power analysis attacks," vol. 51, 2002, pp. 541–552.

[15] B. Zhai, D. Blaauw, D. Sylvester, and K. Flautner, "Theoretical and practical limits of dynamic voltage scaling," in *DAC '04: Proceedings of the 41st annual conference on Design automation*. New York, NY, USA: ACM Press, 2004, pp. 868–873.

[16] S. Mangard, "Securing implementations of block ciphers against side-channel attacks," Ph.D. dissertation, IAIK, University of Technology Graz, Austria, 2004, http://www.iaik.tu-graz.ac.at/research/sca-lab/publications/abstracts/index.php Downloaded on 15 July 2005.

[17] *Nanosim user guide*, Synopsys, Inc, April 2006, http://www.synopsys.com.

[18] X. Zhang and K. K. Parhi, "High-speed vlsi architectures for the aes algorithm," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 12, no. 9, pp. 957–967, 2004.