Security implications of simultaneous dynamic and leakage power analysis attacks on nanoscale cryptographic circuits

Weize Yu and Selçuk Köse

The implications of simultaneous differential power analysis (DPA) and leakage power analysis (LPA) attacks are investigated on nanoscale cryptographic circuits which employ dynamic voltage scaling (DVS) or aggressive voltage scaling (AVS) techniques. As compared to individually performing a DPA or an LPA attack on the corresponding cryptographic circuits, the number of required plaintexts to disclose the key with a 0.9 success rate reduces by 93.5% (as compared to DPA attacks) and 93.06% (as compared to LPA attacks), respectively, when the variance of supply voltage is 0.0833 V^2.

Introduction: Power analysis attacks are non-invasive side-channel attacks (SCA) to obtain critical information from cryptographic circuits [1]. Differential power analysis (DPA) attacks are typically performed through monitoring the dynamic power consumption of cryptographic circuits [1]. As the size of cryptographic circuits scales to nanometer level, the leakage power consumption becomes comparable to the dynamic power consumption [2]. Owing to the increased leakage power consumption in modern circuits, Alioto *et al.* [2] proposed leakage power analysis (LPA) attacks to exploit the leakage power dissipation of nanoscale cryptographic circuits as a side-channel attack.

Dynamic voltage scaling (DVS) and aggressive voltage scaling (AVS) techniques are proposed in [3], [4] as a countermeasure against power analysis attacks. These countermeasures randomly vary the supply voltage level and thereby generate random fluctuations in the power consumption profile. These fluctuations act as noise to mask the actual power consumption profile.

Both dynamic power consumption and leakage power consumption contain critical information of nanoscale cryptographic circuits. Although DPA and LPA attacks have previously been studied thoroughly [2],[5],[6], to the best of our knowledge, the implications of the joint DPA and LPA attacks on the nanoscale cryptographic circuits have not yet been investigated. Our hypothesis is that if DPA and LPA attacks can be utilized together, the number of required plaintexts to disclose critical information would be greatly reduced.

In this letter, the implications of joint DPA and LPA attacks on the nanoscale cryptographic circuits which employ dynamic voltage scaling (DVS) or aggressive voltage scaling (AVS) technique are investigated. It is analytically demonstrated that the number of plaintexts required to achieve a 0.9 success rate (SR) reduces over 93%.

DPA attacks on nanoscale cryptographic circuits with DVS or AVS technique: If an attacker inputs two different *data* (*data1* and *data2*) to a nanoscale cryptographic circuit sequentially, the dynamic power consumption of the circuit P_{dyn1} is

$$P_{dyn1} = \alpha_{0\to1} C_L f_c V_{dd}^2, \tag{1}$$

where C_L is the gate to load capacitance, f_c is the clock frequency, V_{dd} is the supply voltage, and $\alpha_{0\to1}$ is the number of transitions from 0 to 1 when input *data* switch from *data1* to *data2*. If an attacker inputs *data2* and *data1* sequentially (input *data2* first), the dynamic power consumption P_{dyn2} is

$$P_{dyn2} = \alpha_{1\to0} C_L f_c V_{dd}^2, \tag{2}$$

where $\alpha_{1\to0}$ is the number of transitions from 1 to 0 when input *data* switch from *data1* to *data2*.

The differential dynamic power dissipation $P_{dyn2} - P_{dyn1}$ can be obtained as

$$P_{dyn2} - P_{dyn1} = (\alpha_{1\to0} - \alpha_{0\to1}) C_L f_c V_{dd}^2. \tag{3}$$

After taking the logarithm of both sides, (3) can be written as

$$log_2^{|P_{dyn2}-P_{dyn1}|} = log_2^{|\alpha_{1\to0}-\alpha_{0\to1}|} + log_2^{C_L f_c} + 2log_2^{V_{dd}}, \tag{4}$$

where $log_2^{|\alpha_{1\to0}-\alpha_{0\to1}|}$ is the signal that carries critical information related to the input data and $2log_2^{V_{dd}}$ is the noise which is induced by randomly scaling the supply voltage V_{dd}. The SNR of DPA attacks SNR_{DPA} on a circuit employing DVS or AVS technique can be defined as

$$SNR_{DPA} = \frac{Var(log_2^{|\alpha_{1\to0}-\alpha_{0\to1}|})}{Var(2log_2^{V_{dd}})} = \frac{Var(log_2^{|\alpha_{1\to0}-\alpha_{0\to1}|})}{Var(N_1(V_{dd}))}, \tag{5}$$

where Var represents the variance operation.

LPA attacks on nanoscale cryptographic circuits with DVS or AVS technique: The leakage power dissipation of the corresponding nanoscale cryptographic circuit P_{leak1} and P_{leak2} while processing, respectively, *data1* and *data2* can be denoted as follows [2],

$$P_{leak1} = V_{dd} I_{leak1} = V_{dd}[w_1 I_H + (m - w_1) I_L], \tag{6}$$

$$P_{leak2} = V_{dd} I_{leak2} = V_{dd}[w_2 I_H + (m - w_2) I_L], \tag{7}$$

where I_{leak1} and I_{leak2} are the total leakage current induced, respectively, by *data1* and *data2*. I_H and I_L are, respectively, the high level (input bit is high) and low level (input bit is low) leakage current. w_1 and w_2 are, respectively, the Hamming weight of *data1* and *data2*. m is the total number of input bits for *data1* and *data2*. The relationship between the Hamming weight (w_1, w_2) and the parameters ($\alpha_{0\to1}$, $\alpha_{1\to0}$) satisfies the following equation

$$w_1 - w_2 = \alpha_{1\to0} - \alpha_{0\to1}. \tag{8}$$

Using (6) and (7), the differential leakage power dissipation $P_{leak1} - P_{leak2}$ can be written as

$$\begin{aligned}
&P_{leak1} - P_{leak2} = V_{dd}[(w_1 - w_2) I_H + (w_2 - w_1) I_L] \\
&= V_{dd}(\alpha_{1\to0} - \alpha_{0\to1})(I_H - I_L) \\
&= V_{dd}(\alpha_{1\to0} - \alpha_{0\to1})[I_{0,P} W_P e^{\frac{V_{gs}-(V_{t0,P}-\eta_P V_{dd}-\gamma_P V_{bs,P})}{n_P V_T}} - \\
&I_{0,N} W_N e^{\frac{V_{gs}-(V_{t0,N}-\eta_N V_{dd}-\gamma_N V_{bs,N})}{n_N V_T}}](1 - e^{\frac{-V_{dd}}{V_T}}),
\end{aligned} \tag{9}$$

where $I_{0,P}$ ($I_{0,N}$) is the process dependent leakage current for PMOS (NMOS), W_P (W_N) is the gate width of PMOS (NMOS), V_{gs} is the gate to source voltage (*i.e.,* V_{gs} is equal to 0 if the transistor is in off-state). n_P (n_N) is the sub threshold slope factor of PMOS (NMOS), $V_{t0,P}$ ($V_{t0,N}$) is the threshold voltage of PMOS (NMOS), $\gamma_P V_{bs,P}$ ($\gamma_N V_{bs,N}$) is the substrate bias voltage of PMOS (NMOS), η_P (η_N) is the drain induced barrier lowering (DIBL) coefficient of PMOS (NMOS), and V_T is the thermal voltage. Note that V_T is equal to $k_B T/q$. As $V_{dd} \gg V_T = k_B T/q \approx 26mV (T = 300K)$ [4], then $(1 - e^{-V_{dd}/V_T}) \approx 1$. (9) can therefore be approximated as

$$\begin{aligned}
&P_{leak1} - P_{leak2} \approx V_{dd}(\alpha_{1\to0} - \alpha_{0\to1})(I_{0,P} W_P e^{A V_{dd}} \times \\
&e^{\frac{-V_{t0,P}+\gamma_P V_{bs,P}}{n_P V_T}} - I_{0,N} W_N e^{B V_{dd}} e^{\frac{-V_{t0,N}+\gamma_N V_{bs,N}}{n_N V_T}}) \\
&= (\alpha_{1\to0} - \alpha_{0\to1}) V_{dd} (I_H' e^{A V_{dd}} - I_L' e^{B V_{dd}}),
\end{aligned} \tag{10}$$

where $A = \eta_P/(n_P V_T)$ and $B = \eta_N/(n_N V_T)$. After taking the logarithm of both sides, (10) becomes

$$log_2^{|P_{leak1}-P_{leak2}|} \approx log_2^{|\alpha_{1\to0}-\alpha_{0\to1}|} + log_2^{V_{dd}|I_H' e^{A V_{dd}} - I_L' e^{B V_{dd}}|}. \tag{11}$$

The SNR of LPA attacks SNR_{LPA} on circuits employing DVS or AVS technique can be written as

$$\begin{aligned}
SNR_{LPA} &\approx \frac{Var(log_2^{|\alpha_{1\to0}-\alpha_{0\to1}|})}{Var(log_2^{V_{dd}} + log_2^{|I_H' e^{A V_{dd}} - I_L' e^{B V_{dd}}|})} \\
&= \frac{Var(log_2^{|\alpha_{1\to0}-\alpha_{0\to1}|})}{Var(N_2(V_{dd}))}.
\end{aligned} \tag{12}$$

Simultaneous DPA and LPA attacks on nanoscale cryptographic circuits with DVS or AVS technique: Both dynamic and leakage power consumption strongly depend on the input data pattern and supply voltage. If the input data information can be eliminated by analyzing the dynamic power data and leakage power data, an attacker can estimate the variations of supply voltage. Alternatively, the uncertain noise that is induced by randomly scaling the supply voltage is greatly reduced.

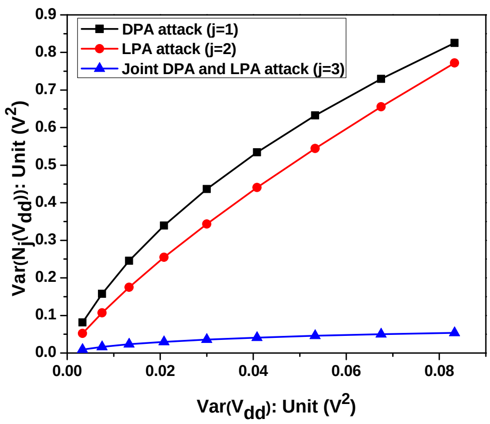

Fig. 1 *Variance of V_{dd} versus the variance of $N_j(V_{dd}), (j = 1, 2, 3)$ under three different attacks on nanoscale cryptographic circuits employing either DVS or AVS technique (Device parameter values are taken from [8]: $A = 1.75$, $B = 1.02$, $I_L^{'} = 26\mu A$ and $I_H^{'} = 0.26\mu A$).*

By substituting (3) into (10), the differential leakage power dissipation $P_{leak1} - P_{leak2}$ can also be written as

$$P_{leak1} - P_{leak2} \approx \frac{P_{dyn2} - P_{dyn1}}{C_L f_c V_{dd}} e^{AV_{dd}} (I_{0,P} W_P \times e^{\frac{-V_{t0,P}+\gamma_P V_{bs,P}}{n_P V_T}} - I_{0,N} W_N e^{\frac{-V_{t0,N}+\gamma_N V_{bs,N}}{n_N V_T}} e^{(B-A)V_{dd}}). \quad (13)$$

The approximated equation (13) can be further processed to simplify the estimation of supply voltage V_{dd} by the attackers as follows

$$\frac{P_{leak1} - P_{leak2}}{P_{dyn2} - P_{dyn1}} \times \frac{1}{AK} \approx \frac{1}{AV_{dd}} e^{AV_{dd}}, \quad (14)$$

$$where \quad K = \frac{I_{0,P} W_P e^{\frac{-V_{t0,P}+\gamma_P V_{bs,P}}{n_P V_T}}}{C_L f_c} - \frac{I_{0,N} W_N e^{\frac{-V_{t0,N}+\gamma_N V_{bs,N}}{n_N V_T}} e^{(B-A)V_{dd}}}{C_L f_c}. \quad (15)$$

Since an attacker would not know the values of A and B, K can be assumed constant (*i.e.,* $A = B$) by the attacker. The attacker can then get an approximated $AV_{dd}^{'}$ by solving (14) and (3) can be written as

$$P_{dyn2} - P_{dyn1} = \frac{1}{A^2}(\alpha_{1\to 0} - \alpha_{0\to 1}) C_L f_c (AV_{dd}^{'})^2 (\frac{AV_{dd}}{AV_{dd}^{'}})^2. \quad (16)$$

After taking the logarithm of (16), the $SNR_{DPA+LPA}$ of the joint DPA and LPA attacks on circuits with DVS or AVS technique can be written as

$$SNR_{DPA+LPA} = \frac{Var(log_2^{|\alpha_{1\to 0} - \alpha_{0\to 1}|})}{Var(2log_2^{V_{dd}} - 2log_2^{V_{dd}^{'}})} = \frac{Var(log_2^{|\alpha_{1\to 0} - \alpha_{0\to 1}|})}{Var(N_3(V_{dd}))}. \quad (17)$$

The next step is to calculate the possible variations of the intentional noise $Var(N_j(V_{dd})), (j = 1, 2, 3)$ which is induced by randomly scaling the supply voltage level with either DVS or AVS. Assuming that those cryptographic circuits employ true random DVS or AVS technique, the supply voltage V_{dd} would statistically have a uniform distribution. If the supply voltage V_{dd} can take n discrete values ranging from V_{DD1} to V_{DD2}, the $i^{th}, (i = 0, 1, 2, ..., n)$ supply voltage level $V_{dd,i}$ can be denoted as

$$V_{dd,i} = \frac{i \times (V_{DD2} - V_{DD1})}{n} + V_{DD1}. \quad (18)$$

The variance of $N_j(V_{dd})$ can be denoted as

$$Var(N_j(V_{dd})) = \frac{1}{n+1} \sum_{i=0}^{n} [N_j(V_{dd,i}) - \frac{1}{n+1} \sum_{i=0}^{n} N_j(V_{dd,i})]^2. \quad (19)$$

After the SNR of the power profile of a cryptographic circuit is obtained, the required number of plaintexts to disclose a secret key with a 0.9 success rate $N_{0.9}$ can be estimated as [7]

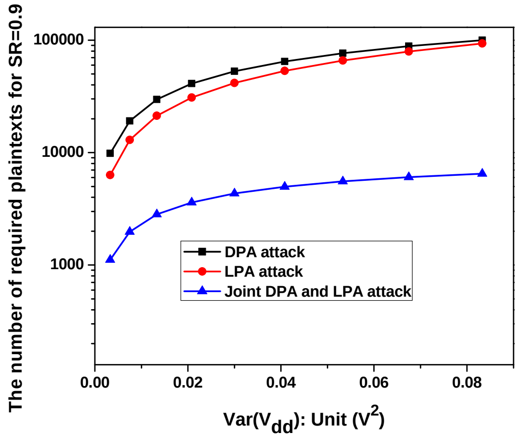

Fig. 2 *Variance of V_{dd} versus the number of required plaintexts to achieve a success rate (SR) of 0.9 under three different attacks on nanoscale cryptographic circuits employing either DVS or AVS technique.*

$$N_{0.9} \approx c \times \frac{1}{r_{P,M}^2}, \quad (20)$$

$$r_{P,M} = \frac{1}{\sqrt{1 + SNR}}, \quad (21)$$

where c is a success rate dependent constant which is approximately 10 when success rate is 0.9 [7].

As shown in Fig. 1, the joint DPA and LPA attack significantly reduces the variance of noise that is generated by randomly scaling the supply voltage with DVS or AVS. The number of required plaintexts to disclose the key with a 0.9 success rate reduces by 93.5% and 93.06% as compared to DPA and LPA attacks, respectively, when the variance of supply voltage is 0.0833 V^2, as shown in Fig. 2.

Conclusion: Security implications of simultaneous DPA and LPA attacks on nanoscale cryptographic circuits that employ DVS or AVS techniques are analytically investigated in this letter. The variance of noise that is inserted by DVS or AVS as a countermeasure against power analysis attacks is significantly reduced with simultaneous DPA and LPA. By utilizing the correlation between the dynamic and leakage power data, the number of required plaintexts to leak the secret key with a 90% success rate is reduced over 93%.

Acknowledgment: This work is supported in part by the National Science Foundation CAREER award under Grant CCF-1350451.

Weize Yu and Selçuk Köse (*Department of Electrical Engineering, University of South Florida, 4202 E. Fowler Avenue, Tampa, FL 33620.*)

E-mail: weizeyu@mail.usf.edu

References

1 Mangard, S., Oswald, E., and Popp, T.: 'Power analysis attacks revealing the secrets of smart cards (advances in information security)' (Springer, New York, 2007)

2 Alioto, M., Giancane, L., Scotti, G., and Trifiletti, A.: 'Leakage power analysis attacks: a novel class of attacks to nanometer cryptographic circuits', *IEEE Trans on Circuits And Systems-I: Regular Papers*, 2010, **57**, (2), pp. 355-367

3 Baddam, K., and Zwolinski, M.: 'Evaluation of dynamic voltage and frequency scaling as a differential power analysis attacks'. *Proc. VLSI design*, Jan 2007, pp. 854-862

4 Avirneni, N.-D.-P., and Somani, A.-K.: 'Countering power analysis attacks using reliable and aggressive designs', *IEEE Trans on Computers*, 2014, **63**, (6), pp. 1408-1420

5 Yang, S., Wolf, W., Vijaykrishnan, N., Serpanos, D.-N., and Xie, Y.: 'Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach'. *Proc. Design, Automation and Test in Europe*, March 2005, pp. 64-69

6 Tokunaga, C., Blaauw, D.: 'Securing encryption systems with a switched capacitor current equalizer', *IEEE journal of Solid-State Circuits*, 2010, **45**, (3), pp. 23-31

7 Standaert, F.-X., Peeters, E., Rouvroy, G., Quisquater, J.-J.: 'An overview of power analysis attacks against field programmable gate arrays', *Proceedings of the IEEE*, 2006, **94**, (2), pp. 383-394

8 Morsin, M.-B., Amriey, M.-K.: 'Designing and characterization of 60nm p-well MOSFET using sentaurus TCAD software', *Proc. ICECT*, May 2010, pp. 169-172