High Efficiency Power Side-Channel Attack Immunity using Noise Injection in Attenuated Signature Domain

Debayan Das1, Shovan Maity1, Saad Bin Nasir2, Santosh Ghosh3, Arijit Raychowdhury2, Shreyas Sen1

1School of Electrical and Computer Engineering, Purdue University, USA
2School of Electrical and Computer Engineering, Georgia Institute of Technology, USA
3Intel Labs, Hillsboro, Oregon, USA
{das60, shreyas}@purdue.edu

Abstract—With the advancement of technology in the last few decades, leading to the widespread availability of miniaturized sensors and internet-connected things (IoT), security of electronic devices has become a top priority. Side-channel attack (SCA) is one of the prominent methods to break the security of an encryption system by exploiting the information leaked from the physical devices. Correlational power attack (CPA) is an efficient power side-channel attack technique, which analyses the correlation between the estimated and measured supply current traces to extract the secret key. The existing countermeasures to the power attacks are mainly based on reducing the SNR of the leaked data, or introducing large overhead using techniques like power balancing. This paper presents an attenuated signature AES (AS-AES), which resists SCA with minimal noise current overhead. AS-AES uses a shunt low-drop-out (LDO) regulator to suppress the AES current signature by 400× in the supply current traces. The shunt LDO has been fabricated and validated in 130 nm CMOS technology. System-level implementation of the AS-AES along with noise injection, shows that the system remains secure even after 50K encryptions, with 10× reduction in power overhead compared to that of noise addition alone.

Keywords—Side Channel Attack (SCA), Cryptographic Hardware, Power Analysis Attack, Countermeasure, Attenuated Signature AES, Shunt LDO, Noise Injection.

I. INTRODUCTION

The rapid proliferation of mobile devices and wireless communications has enhanced the need for stronger encryption algorithms. However, hardware implementations of these computationally-secure cryptographic algorithms provide sufficient "side-channel" information for the attackers to decipher the secret key. Side-channels include power consumption [1], [2], electromagnetic emanations [3], [4], acoustic vibrations [5], or the timing of various encryption operations [6], [7].

A. Motivation

For an attacker, the power monitoring attack is one of the most common side-channel attacks on modern computer systems. The attacker measures the power consumption of the encryption device under test (DUT), and performs subsequent simple (SPA) [8] or differential power analysis (DPA) [1] of the obtained traces to decipher the secret key.

In this article, we focus on the correlational power analysis (CPA) attack [9] on a 128-bit Advanced Encryption Standard (AES) engine. However, the proposed AS-AES is a generic technique to resist power attacks, and can be applied to other encryption algorithms. Figure 1 gives an overview of the proposed signature attenuating AES (AS-AES). The underlying idea is to embed the AES in a signature attenuating hardware, such that the variations in the AES current is highly suppressed and is not reflected in the supply current traces, thereby requiring much lower noise current injection to decorrelate the measured supply traces.

B. Contribution

This paper proposes a new hardware-based technique for cryptographic devices to resist power analysis attacks (PAA). Specific contributions of this paper are:

- Demonstrated the relation between only noise injection vs. correlation (for CPA with correct key), both mathematically and through simulation results. This highlighted the inefficiency of only noise injection leading to a 370% power overhead requirement for achieving Minimum Traces to Disclosure (MTD) > 50K.

- Proposed a new generic DPA/CPA countermeasure that can be applied to any cryptographic algorithm. This is achieved by embedding the cryptographic engine within a high-efficiency signature attenuation hardware, to reduce (> 400×) the secret signature on power pin. Injection of noise to mask SCA in the Attenuated-Signature AES (AS-AES) domain, reduces noise-injection overhead (~1 mA) for SCA immunity by 70×, compared to standalone noise injection.

- Demonstrated that with the proposed AS-AES, none of its secret key blocks have been disclosed (MTD > 50K) with...
II. RELATED WORK

Immunity to power analysis attack could be improved by modifying the encryption hardware module such that the power consumption of the device is independent of the signal transitions. The existing protection schemes for the hardware encryption engines against power analysis attacks can be classified into three major categories. The first category reduces the SNR of the leaked information by injecting noise into the supply traces [10]. However, solely noise addition is not an optimum technique to make a power attack infeasible. A statistical analysis for this technique is presented in Section III. Also, the effect of power delivery network (PDN) on SNR has been studied and a frequency-dependent noise injection circuit was implemented by Wang et al. [11].

The second category reduces side-channel leakage by balancing the power consumption of the rising and falling transitions. Power balancing logic implementations include the sense-amplifier based logic (SABL) [12], dual-rail circuits [13], [14], and wave dynamic differential logic (WDDL) [15]. The WDDL structure appears to be the first power attack resistant power-balancing circuit validated in silicon with a Measurements to Disclosure (MTD) of ~21K. However, the increased protection consumed 4× power overhead, 3× area, and a 4× performance degradation.

The third category of protection reduces the power side-channel leakage information by isolating the supply from the encryption engine. It includes switched capacitor techniques [16], [17], [18] and integrated voltage regulator (IVR) based implementations [19], [20], [21], [22]. The switched capacitor current equalizer module proposed by Tokunaga et al. [17] demonstrated Power SCA immunity, however, it resulted in 2× performance degradation and 33% power overhead. The impact of package parasitic and integrated buck converters on power SCA vulnerability have been analyzed in [11], [19]. Another concept is to degrade the performance of IVR such that supply current has lesser correlation with the AES current. Implementations of this concept could be found using Analog LDO [20], Digital LDO (resolution is traded off, droop increases) [21] and a buck converter [22]. The above described techniques exhibit a fundamental trade-off between system performance (e.g. dynamic loop response) and reduction in side-channel vulnerability.

In this work, the proposed AS-AES effectively combines the first and third categories of protection to achieve SCA immunity with high power efficiency and no performance degradation. Figure 2 shows a block diagram representing the CPA attack on the AES engine of the device under attack (DUT). The traditional AES-128 core revealed one byte (1st byte in this example) of the secret key with only 1K traces, while the same attack applied to the modified AS-AES core could not extract the key byte even with 50K traces.

III. POWER SIDE-CHANNEL IMMUNITY USING NOISE INSERTION

Noise injection into power consumption measurements is a convenient approach to defend against power side-channel attacks [23]. The correlation ($\rho_{TH}$) between the estimated hamming weight matrix ($H$) and the obtained power traces ($T$) can be given as,

$$\rho_{TH} = \frac{Cov(T,H)}{\sigma_T \sigma_H}$$

where, $Cov$ denotes the covariance matrix, and $\sigma_T, \sigma_H$ represents the standard deviation of $T$ and $H$ respectively.

Now, the main goal is to add enough random noise to resist a side-channel attack, yet introducing a minimal power overhead in the system. If $N$ denotes the amount of random noise added into the circuit, and $T' = T + N$ denote the modified traces, the modified correlation factor $\rho_{T'H}$ can be written as,

$$\rho_{T'H} = \frac{Cov(T' + N, H)}{\sigma_{T+N} \sigma_H}$$

$$= \frac{E[(T' + N)^2 - E(T' + N)E(H)]}{\sigma_{T+N} \sigma_H}$$

$$= \frac{E(T')^2 + E(N)^2 - E^2(T) - E^2(N) + \sigma_H^2}{\sigma_{T+N} \sigma_H}$$

$$= \frac{\sqrt{\sigma_T^2 + \sigma_H^2}}{\sigma_T \sigma_H}$$

$E$ represents the expectation or mean of the corresponding variable. The independence of the variables $N$ and $H$ has been utilized in this expression. Thus, we see that, higher is its

Figure 2: Power Side-Channel attack on unprotected 128-bit AES

> 10× lower power overhead compared to parallel noise incorporation.
variance $\sigma_{\hat{t}_l}^2$ and lower is the correlation $\rho_{\hat{t}_l \hat{\mu}}$. However, noise insertion alone introduces a significant current overhead.

Figure 3 shows the effect of noise insertion on power attack (PAA) immunity. It can be seen that for the actual key, the traces correlate in absence of noise ($\rho_{\hat{t}_l \hat{\mu}} \approx 0.9$). For the AES-128 core under attack, the average current consumption of the sampled traces during the AES operations was found to be $\sim 18.89 \text{ mA}$. In order to provide high enough resistance to a DPA or CPA, noise insertion requires a current overhead of $\sim 70 \text{ mA}$ (refer MTD plots in Figure 12 (a-d)), which incurs a current overhead of approximately four times (370%) of the average AES current consumption. Thus, only noise insertion is not an optimized solution for power SCA immunity.

IV. PROPOSED ATTENUATED SIGNATURE AES (AS-AES)

In this section, we introduce the attenuated signature AES (AS-AES) with noise injection. The proposed AS-AES architecture (Figure 4) incorporates a shunt LDO, and an integrating load capacitor. As discussed earlier, to remove the correlation spikes for the actual key, the supply current needs to be independent of the AES current. As seen from Figure 4, the voltage across AES block ($V_{\text{reg}}$) needs to be regulated at a constant value, with minimum power overhead. Traditional LDOs, which are commonplace in ICs, aim to maintain a constant $V_{\text{reg}}$ however, the supply current reflects the changes in load (e.g. AES) current. In our design, the goal is to maintain a constant $V_{\text{reg}}$, as well as to make the supply current independent of the AES current during encryption operations.

A. Operation Principle

The proposed AS-AES operates using two control loops. Switched-mode control (SMC) is implemented using a low bandwidth slow loop to track large changes in the average AES current. The concept of SMC has been demonstrated in [24]. The SMC loop (Figure 5) regulates the current through an array of PMOS current sources, which are activated when the output voltage goes beyond $V_{\text{target}} \pm \Delta$. Here $\Delta$ acts as a guard-band and prevents the digitally controlled loop from being continuously ON. As soon as the output voltage is within $\Delta$, the digital loop is gated and the analog shunt regulator takes the output voltage to $V_{\text{reg}}$. For the AES-core under attack, it was verified that the average current ($\sim 18.89 \text{ mA}$) consumed by the AES engine for different inputs remain almost the same throughout the encryption operations, as it performs repetitive ten S-box operations for each input byte. SMC only engages to compensate for slow changes in the average AES current. Due to the almost-constant nature of the average AES current, the SMC loop stays disengaged and the PMOS (Figure 4) acts as a current source (CS), in saturation, with high drain to source impedance ($r_{ds}$).

Once the SMC loop is set, the CS current is fixed at a value higher ($I_{\text{ES}} = I_{\text{AES avg}} + I_{\text{av}}$) than the average load (AES current). The fast loop incorporates a shunt LDO with a NMOS bleed to sink any excess current from the supply, when the AES current consumption is lower than the average. Thus, the bleed restricts unnecessary charging of the load capacitor ($C_{\text{Load}}$), and thereby regulates the output voltage ($V_{\text{reg}}$). On the other hand, when the AES current requirement is more than the supply current, the capacitor provides the necessary extra current, thereby maintaining a constant supply current irrespective of the AES current variation, at the expense of an instantaneous droop in $V_{\text{reg}}$, which is reduced with increased $C_{\text{Load}}$ or $I_{\text{av}}$.

B. Steady State Analysis of the AS-AES

The parameters involved in the design of the fast control loop (steady state) of the AS-AES are the NMOS bleed size, the choice of integrating load capacitor, gain ($A_p$) and bandwidth of the operational amplifier (OP-AMP) in the shunt-LDO loop.
Gain (with its effect on different key parameters. AF increases as loop
plot of the attenuation factor (AF) with nominal design, along
OP-AMP, respectively. Figure 8 shows the magnitude Bode
represents the transconductance and the dominant pole of the
where, AF is the AES signature attenuation factor; $g_m$ and $a$
notes from these analysis is that for all cases, AS-AES provides
attenuation of $> 400 \times$ in the supply current.

c. Noise Injection on AS-AES

The peak-to-peak variation in the supply current with different
was shown in Figure 7(b). Even designing a current source with output resistance in
the order of $M\Omega$ could reflect a variation in the order of $nA$, which can still be measured using an oscilloscope. Thus, a change in AES current in the order of $mA$ gets reflected in the supply current in an attenuated scale of the order few $\mu A$, depending on the impedance of the current source. Although the signature gets attenuated, the change in current will still be reflected in the power supply traces, and it cannot yet resist a CPA attack completely, resulting in some correlational peaks.

Note, though the signature is still present it is highly
attenuated. A small amount of random noise current is injected
(as shown in Figure 4) in order to decorrelate the traces with the estimated hamming weight matrix, and thereby provide significant immunity against CPA attack. The noise current generation circuit is a simple linear feedback shift register

Figure 9: Proof-of-concept shunt LDO design measured on a 130nm testchip.
Die-photo, key measurement results and the shunt LDO circuit is shown

Authorized licensed use limited to: Georgia Institute of Technology. Downloaded on June 28,2021 at 15:52:54 UTC from IEEE Xplore. Restrictions apply.
Effect of CS Output Resistance

The above results were obtained with 1000 traces, and gives a good sense of the choice of design parameters and its effects. To confirm the exact overheads and efficiency required, the CPA attack is run over significantly more traces. As the number of traces analyzed is increased, the correlation coefficients (ρ) are expected to be more accurate, and ρ for the correct key should be consistently higher than the ρ of the peak (absolute maximum) correlation of the incorrect keys.

C. SCA Immunity Verification with MTD Analysis

Figure 12(a-d) (noise addition alone) and Figure 12(e-h) (AS-AES + noise injection) shows the evolution of the correlation coefficient as the number of encryption runs increases for different noise injection. Figure 12(a-d) shows that noise addition alone, involves an overhead of 70 mA to achieve Measurements to Disclosure (MTD) >50K. As the AS-AES core is subjected to a CPA attack, it is seen that MTD
>50K is achieved, with only a noise current injection of 1 mA (Figure 12(h)). Also, the current consumed by the OP-AMP is 400 μA. Hence, the total overhead current (as discussed previously) is $I_{\text{op}} = I_{\text{peed}} + I_{\text{noise}} + I_{\text{pamp}} = 1.11 \text{ mA} + 1 \text{ mA} + 0.4 \text{ mA} = 2.51 \text{ mA}$, which is 28× lower than that of noise addition alone. The total overhead power for the AS-AES architecture is $(20 \text{ mA} + 1 \text{ mA} + 0.4 \text{ mA}) * 1.2 \text{ V} - 18.89 \text{ mA} * 1 \text{ V} = 6.79 \text{ mW}$. In case of solely noise insertion the power overhead required is $P_{\text{op}} = 70 \text{ mA} * 1 \text{ V} = 70 \text{ mW}$. Thus, AS-AES along with noise injection provides >10× improvement in the power overhead for iso-SCA immunity, compared to only noise addition, with $MTD > 50K$. Power efficiency for AS-AES is given as, $\eta = \frac{1.89 \text{ mA} * 1 \text{ V}}{21.4 \text{ mA} * 1.2 \text{ V}} = 73.56 \%$ (includes noise overhead). Hence, AS-AES consumes similar overhead as [17], but does not incur the performance penalty.

VI. CONCLUSION

Power Side Channel Attack is a prominent attack on cryptographic ICs. This work proposes low-overhead hardware modification that attenuates critical AES signature (AS) by >400× in the supply current which the attackers could observe from the periphery of an encryption ASIC. Noise injection in the AS domain achieves SCA immunity with extremely high-efficiency. Successful SCA immunity is demonstrated for a CPA side-channel attack, with up to 50 K traces. Power SCA immunity is achieved with 73.56 % power efficiency, and 10× lower power overhead, compared to only noise addition and more importantly without imposing any performance penalty.

REFERENCES