Mitigating Power Supply Glitch based Fault Attacks with Fast All-Digital Clock Modulation Circuit

Arvind Singh[1], Monodeep Kar[2], Nikhil Chawla[1], and Saibal Mukhopadhyay[1]
Georgia Institute of Technology[1], and Intel Labs[2]
rathorearvind19@gatech.edu, monodeep.kar@intel.com, nikhilchawla@gatech.edu, saibal.mukhopadhyay@ece.gatech.edu

***Abstract*—This paper experimentally demonstrates that an on-chip integrated fast all-digital clock modulation (F-ADCM) circuit can be used as a countermeasure against supply glitch and temperature variations-based fault injection attacks (FIA). The F-ADCM circuit modulates clock edges in presence of DC/transient supply glitches and temperature variations to ensure correct operation of the underlying cryptographic circuit. With a testchip manufactured in 130nm CMOS process, we first demonstrate an inexpensive methodology to conduct a fault attack on hardware implementation of a 128-bit advanced encryption standard (AES) engine using externally controlled supply glitches. Next, we show that with F-ADCM circuit, it is no longer possible to inject supply/temperature glitch-based faults even after 10 million encryptions across varying operating conditions. Moreover, in extreme operating conditions, the F-ADCM circuit doesn't generate any clock edges, leading to complete failure of the AES encryption, indicating no exploitable faults are present.**

Keywords— differential fault analysis, cryptography, advanced encryption standard, fault injection attack, supply glitch, clock modulation, error resilience, PVT variations.

I. Introduction

Cryptographic algorithms are increasingly integrated with modern embedded systems, e.g., smartphones, internet-of-everything (IoE) devices, smartcards, personal computers, and servers, to meet increasing demand for secure transmission of sensitive information. Although, these cryptographic algorithms are proven secure against cryptanalysis/brute-force attacks, their software and hardware implementations exhibit security vulnerabilities via various side channels, e.g., fault injection attacks (FIA) [1-4], power side channel analysis, etc. These attacks, especially FIA, can be conducted inexpensively in a non-invasive manner. FIA relies on injection of a precisely timed/located fault during the cryptographic operation. Differential fault analysis (DFA) is subsequently performed between correct and faulty output to reveal secret information.

Several fault injection techniques, such as variations in power supply, irregularities in clock input, X-ray or electromagnetic (EM) emissions, temperature variations and directed laser beams [5-7], can be employed to deliberately modify an integrated circuit's (IC) operating conditions to alter its computation. FIA based on supply, clock or temperature modification is low cost and easier to implement, therefore is highly practical. However, in most cases, clock is not accessible to an adversary, therefore clock glitch-based FIA cannot be conducted. Supply glitches, on the other hand, are easy to generate externally which then propagate to chip internal circuits resulting in timing failures.

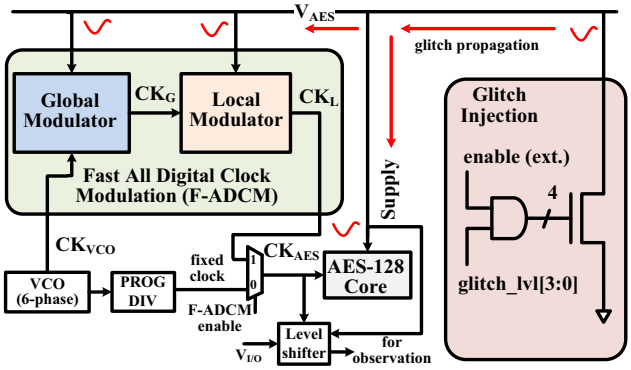


Fig. 1. System architecture of F-ADCM circuit to prevent supply glitch and temperature variations-based fault attacks for a 128-bit AES encryption core.

Software/hardware level countermeasures are incorporated to detect and correct faults as well as to increase tolerance to FIA to ensure data privacy/integrity [8-13]. This work demonstrates that an on-chip integrated fast all-digital clock modulation (F-ADCM) circuit can be used as a countermeasure against FIA. F-ADCM adapts to both DC and AC variations in power supply to generate an output clock for the target digital core implementing 128-bit AES (AES-128) algorithm (Fig. 1). With a testchip manufactured in 130nm CMOS technology, we first present a methodology to inject supply glitches without any assumption about accurate timing (cycle-by-cycle) of the AES operations. We then demonstrate that with F-ADCM circuit, one can no longer inject faults with supply glitches even after 10-million encryptions across varying operating conditions (voltage and VCO frequency, temperature variations). We further show that in extreme operating conditions, F-ADCM stops generating any clock edges leading to complete failure of AES operation, therefore no exploitable faults can be injected.

Rest of the paper is organized as below. Section II presents some background on FIA and surveys the related work. Section III presents system architecture. Section IV presents testchip, fault injection setup, DFA, fault mitigation with F-ADCM, compares F-ADCM with existing countermeasures and discusses design tradeoffs. Section V concludes the paper.

II. Background

A. Fault Injection Attacks (FIA)

In 1996, Boneh et. al. demonstrated fault attacks for the first time to extract cryptographic keys from public-key cryptosystem (RSA) [1]. Subsequently, fault-based attack models were applied to several block ciphers (DES [2], AES

[3]). Several works have presented fault models ranging from 1-bit to single-/multi- byte [3,4]. 1-bit faults are difficult to induce; therefore, byte faults are preferred. Additionally, fault models which require less number of faulty outputs are desired. Several works have shown supply/clock glitch-based FIA on FPGA or smartcards [7].

Existing works on clock/supply glitch-based fault attacks assume that glitches can be injected in a precise manner assuming an adversary has complete knowledge of the underlying cryptographic hardware in terms of exactly when round operations are computed. However, in absence of such knowledge, it is very difficult to inject faults at the desired locations. Authors of [5] demonstrated FIA for AES on a cryptographic LSI, however, the clock was generated externally using FPGA with precise control on the clock edges. Authors of [6] demonstrated an FIA on ARM-based android device. Underpowering, overclocking and temperature variations-based FIA relies on timing failures in the digital circuits. Under modified operating conditions, data may either arrive too late at a flipflop (FF) or too early leading to setup (Eq. 1) and hold (Eq. 2) failure, respectively [11-12]. Any fault mitigation technique attempts to detect these timing errors, masks the faulty output (under FIA) and performs the operation again.

$$t_{c2q,max} + t_{comb,max} + t_{setup} \leq t_{ck} + \Delta_{ck,min} \quad (1)$$

$$t_{c2q,min} + t_{comb,min} \geq t_{hold} + \Delta_{ck,max} \quad (2)$$

B. Related Work

Recently, there have been several countermeasures proposed to prevent FIA. Countermeasures can be categorized in - 1) detection and correction [8], and 2) infection: propagating difference in intermediate states to multiple bytes of the ciphertext making it unexploitable [9]. Since the primary mechanism for the fault injection is timing failures, error-resilient architectures such as duplicated complemented datapath [10], tunable replicas [11,12], glitch detector circuit [13], synchronous Razor [14] family can be used to detect and correct errors in presence of supply glitches. Additionally, instead of stalling the pipeline for an erroneous operation, the instantaneous clock frequency can be adapted in a pre-emptive manner to prevent the timing failures [15]. However, major drawback with most of the adaptive circuits is their complexity and slow response time. To prevent any fault propagating outside, the adaptive circuit must respond at cycle-by-cycle speed and for an easier integration with the current digital design flows, it must be fully synthesizable. The prior works to prevent FIA for a cryptographic ASIC hardware accelerator with timing error detection circuits are primarily based on simulation studies [11,12] and did not present experimental (hardware) results. This paper considers a high-speed and fully-synthesizable ASIC implementation of F-ADCM circuit [16] with 130nm CMOS and demonstrates fault mitigation with measured results.

III. System Architecture

The proposed system consists of an ASIC implementation of 128-bit AES and F-ADCM circuit.

A. Architecture of AES-128

AES encryption algorithm is the most common in modern security critical electronic devices. AES has several datapath architectures optimized for area, power, and/or performance. We have implemented an 8-bit datapath for AES which is optimized for area and power, however, offers lower performance. AES-128 algorithm consists of 10 rounds of operations and 1 initial round. Each round (except final round) consists of 4 round operations –1) Substitute Box (SBOX), 2) ShiftRow, 3) MixColumn, and 4) AddRoundKey [Fig. 2(a)]. Last round doesn't have MixColumn operation while initial round performs AddRoundKey only. Our design implements one SBOX circuit which is used iteratively for all SBOX operations for the encryption as well as key expansion. Similarly, a single 32-bit MixColumn circuit is used iteratively for all 128 bits. The design implements a unified datapath for encryption and decryption to minimize resources. The total latency for performing 1 encryption is 502 cycles. Fig. 2(b) shows the datapath for AES and timing diagram for each round.

B. Architecture of Fast All-Digital Clock Modulation Circuit

A fast all-digital clock modulation (F-ADCM) circuit is designed to respond to DC/transient glitches in power supply. F-ADCM consists of global modulator (GM) and local modulator (LM) circuits [16] (Fig. 3). GM circuit consists of 2 critical path replicas of the timing critical path for the AES-128 core. GM is clocked with a high-speed clock (600MHz) generated from a 6-stage differential delay-cell based voltage-controlled-oscillator (VCO). It generates an output clock (CK_G) with time-period (T_{CKG}) an integer multiple of source (VCO) clock period. GM responds to any global noise or DC changes

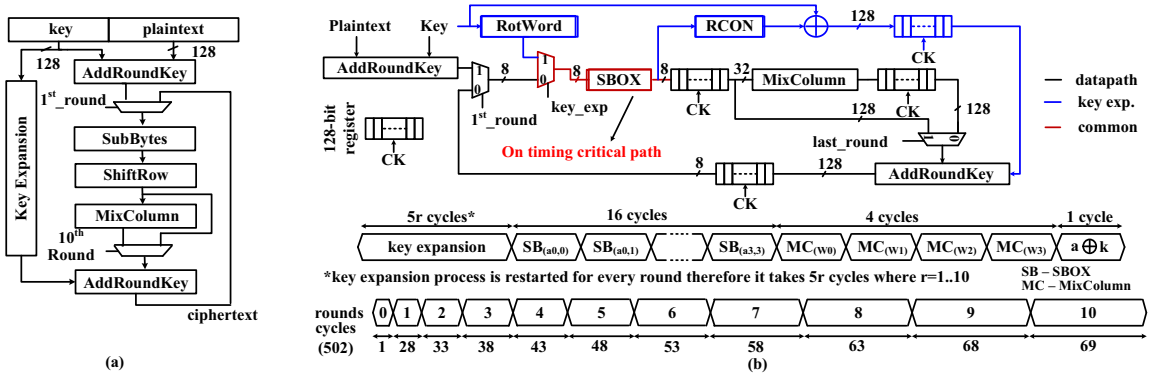


Fig. 2. ASIC implementation of 128-bit AES: (a) AES algorithm, and (b) hardware for a single round which is used iteratively for low area/power operation.

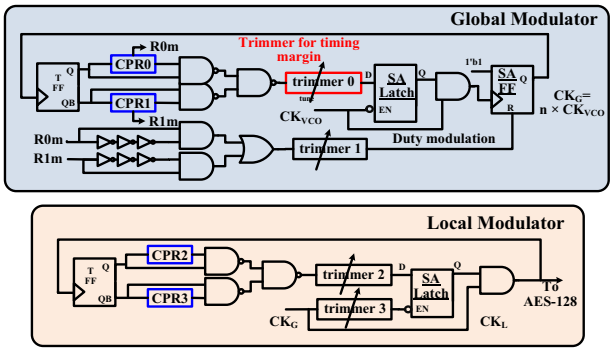


Fig. 3. F-ADCM circuit with global and local modulators [16, 17].

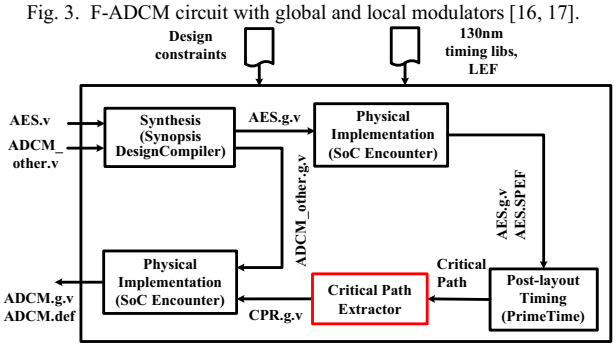


Fig. 4. Fully synthesizable design flow to implement F-ADCM circuit.

in the supply. A 32-tap programmable trimmer (trimmer 0) controlled with 5-bit SEL_TM signal adds some margin for timing in addition to critical path delay while another programmable trimmer (trimmer 1) is used to get the desired duty cycle. LM circuit, clocked by GM output (CK_G) also utilizes two critical path replicas and responds to any local transient glitch in power supply by delaying the next clock edge (rise) with up to trimmer 3 delay (duty modulation mode) or by skipping next clock edge (clock gating mode). Both GM and LM use sense-amplifier (SA) based flip-flops and latches to minimize metastability conditions.

Unlike existing timing error prevention circuits [14, 15], F-ADCM circuit (GM) can respond to DC changes in supply voltages making it ideal for implementing dynamic voltage and frequency scaling algorithms on-chip [17, 18]. The entire logic for GM and LM is fully synthesizable. Gate-level netlist for all critical path replicas (CPR0..3) is extracted using a critical path extractor script from post-layout static-timing-analysis (STA)

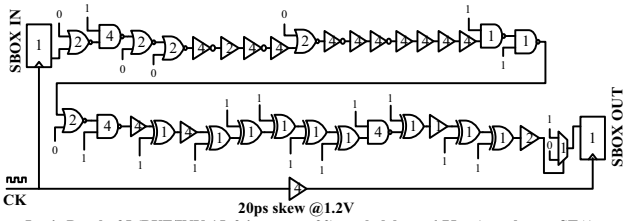


Fig. 5. Timing critical path for AES-128 extracted from post-layout STA.

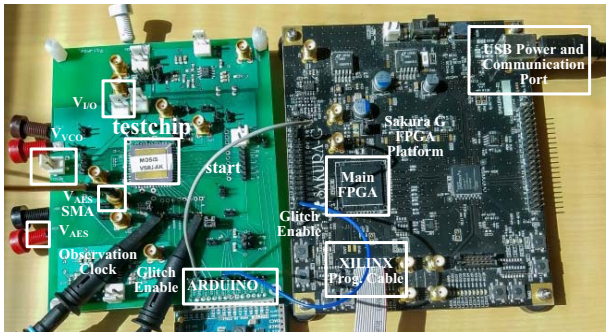


Fig. 6. Measurement setup with testchip and PCB integrated with Sakura-G FPGA platform and Arduino Due.

and is integrated with rest of the GM/LM gate-level netlist before it is placed and routed using standard physical design tools (Fig. 4 and Fig. 5).

IV. Measurement Results

A testchip, *previously presented in [18]*, was used to carry out FIA experiments. It consists of F-ADCM and AES-128 circuits [Fig. 7(c)]. Table 1 provides a summary for the testchip. Fig. 6 shows the measurement setup. An external start signal starts the encryption and ciphertext is read back for validation and DFA [Fig. 6(a)].

An on-chip circuit with 4 NMOS's (binary sized - W, 2W, 4W, 8W) is used to induce supply glitches (Fig. 1). All NMOS's can be turned on/off with a 4-bit external glitch level (glitch_lvl[3:0]) signal to modulate the height of the induced supply glitch. Additionally, a glitch enable control is used to send narrow pulses to enable/disable these NMOS's to induce supply glitch with varying height and width (glitch profile depends on width of narrow pulse and on-chip decoupling capacitor). The clock for the test-chip is generated internally using a free-running VCO. The AES can operate in the

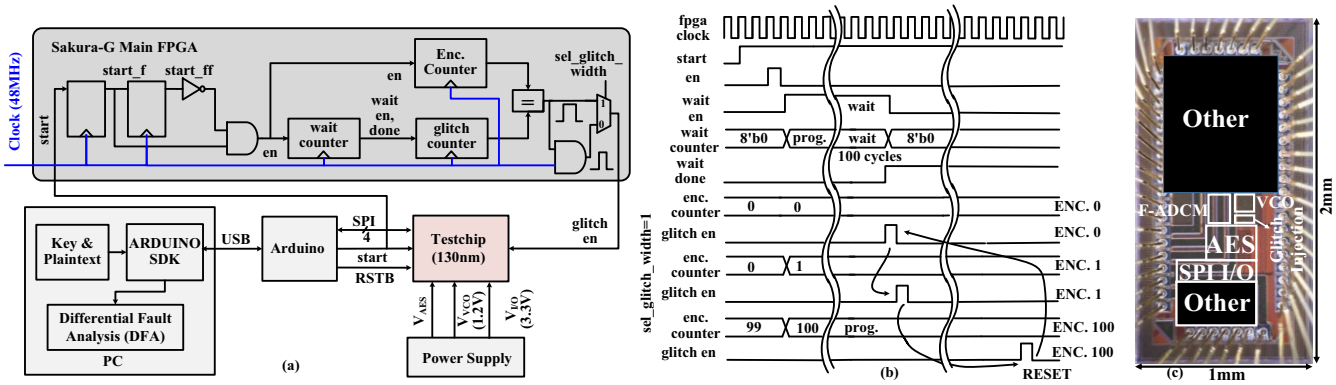


Fig. 7. Measurement setup for fault injection: (a) Sakura-G platform integrated with testchip to generate programmable glitch enable signal once every encryption, (b) timing diagram for glitch enable generation with respect to AES-128 encryption, and (c) testchip manufactured in 130nm CMOS.

Table. 1. Testchip summary

AES-128 Core	Area	320µm×360µm (6592 gates)
	Perf.	Latency: 502 cycles, Throughput: 28.1Mbps @1V, 110MHz
	Op. Range	0.58V (9.6MHz) - 1.25V (169.6MHz)
	Power	3.9mW @110MHz, 1V
F-ADCM	Area	100µm×145µm (1451 gates)
	Power	129µW @600MHz input, 110MHz output, 1V
	Freq. (VCO)	600MHz
	Op. Range	0.58V-1.25V @600MHz VCO clock
VCO	Freq. Range	93MHz - 600MHz
	V_{CTRL}	0 – 0.56V

standalone mode with a fixed frequency clock generated from the VCO. The AES can also operate in a *protected mode*, where the AES clock comes from the F-ADCM circuit. In the protected mode, the F-ADCM circuit takes the VCO clock as the input and generates the AES clock as the output (Fig. 8).

A. Fault Injection and Analysis for Standalone AES

Fault Injection: To inject glitches in a controllable fashion, the testchip is supplied glitch enable signal from Sakura-G based FPGA board. The FPGA chip runs at 48MHz with 67% duty cycle. Glitch widths of 21ns/14ns are generated using full and high pulse period for the clock [Fig. 7(a)]. With the assumption that we only have approximate information about AES-128 rounds of operations, faults are injected towards the last few rounds only. The "start" signal used to start AES encryption is also used by the FPGA chip to generate glitch enable signal approximately in the proximity to the target rounds. In our experiments, to ensure the inclusion of target operation(s) for fault injection, the faults are injected over a longer duration (about 50% of total encryption duration - to approximately cover round 5 to round 10). When the encryption is started, a glitch counter circuit, after initial wait time is used to generate glitch enable at incremented clock cycles [Fig. 7(b)]. Glitch counter circuit is reset after a programmable duration and whole process restarts. The wait, encryption (enc.) and glitch counters are reconfigured to inject faults at different AES clock frequencies (F_{AES}). Since the AES clock and FPGA clock are asynchronous, the timing of fault injection with respect to AES clock is random during each iteration of glitch counter. Also, since width of the glitch enable signal is larger than the AES clock period, the supply glitch may affect multiple bytes during AES operation.

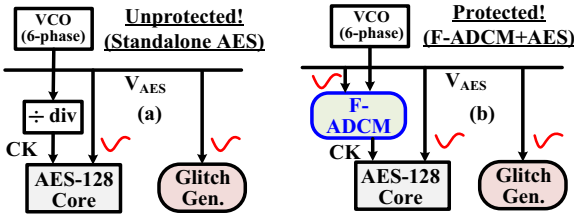


Fig. 8. (a) Unprotected standalone AES and (b) AES protected with on-chip F-ADCM circuit are analyzed with respect to FIA.

Table 2. Summary of fault injection experiments.

Glitch Level	Glitch Width=T_{FPGA_CLK}(21ns)					Glitch Width=T_{FPGA_CLKP}(14ns)				
	ΔV (mV)	Total Faults	16-Byte Faults			ΔV (mV)	Total Faults	16-Byte Faults		
			Total	Unique	Explo-itable			Total	Unique	Explo-itable
0001	111	0	0	0	0	90	0	0	0	0
0011	160	1188	1173	112	11	157	282	275	29	5
0100	207	2727	2622	731	43	215	1518	1415	206	28
0111	274	2965	2752	1430	52	267	2594	2450	653	60
1000	321	2966	2786	1599	28	320	2798	2624	1067	53
1111	384	2972	2796	1721	0	374	2958	2752	1329	28

Fault Model Selection: Since the faults are injected in a random fashion without accurate information/control on timing of the faults, the faulty ciphertexts will consist of both exploitable and unexploitable faults. To reduce the DFA time and computation complexity, we chose fault model proposed by Piret and Quisquater [4] for AES which is based on single-byte fault injection between MixColumn operation of round 7 and 8 and requires only 2 faulty ciphertexts to find correct key.

Fault Characterization and Analysis: Supply glitches are injected with different width (14ns and 21ns, controlled with glitch enable generation circuit on FPGA chip) and different height (90mV to 384mV with several intermediate levels, controlled with glitch_lvl signal) at nominal operating conditions (V_{AES}=1V and F_{AES}=110MHz). Fig. 9 shows measured glitch height and width for few cases. Under large glitch, the level shifter between V_{AES} and $V_{I/O}$ cannot support high speed, therefore, observed clock waveform is distorted. Table 2 summarizes all the faults that are injected out of total 10,000 encryptions. Total number of faults increase with increased glitch width/height. Most of the faults injected are all (16) byte faults indicating a single-byte fault is induced before round 8 MixColumn or multi-byte faults are injected.

It is observed that at smaller drop in supply voltage, the unique 16-byte faults are less compared to higher drop where most of the 16-byte faults injected are unique. For the fault attack, all unique 16-byte faults are filtered out and 2 faulty

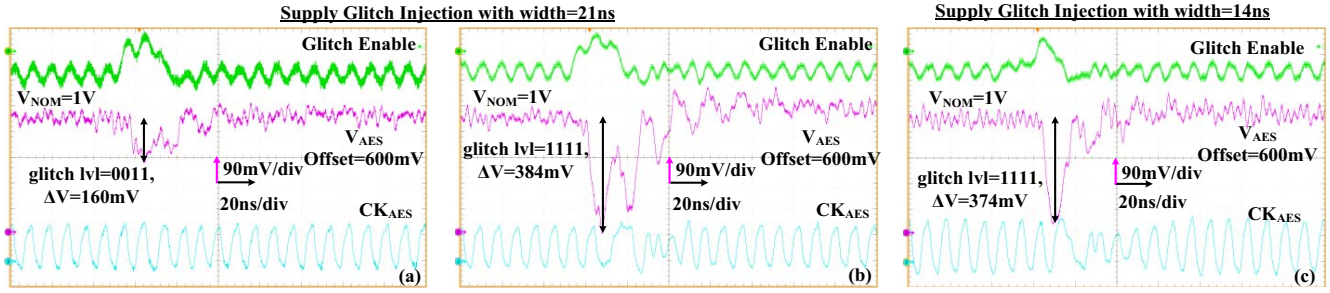


Fig. 9. Glitch injection under nominal conditions (V_{AES}=1V, F_{AES}=110MHz) with programmable glitch height and width: (a) glitch level=0011, width=21ns, (b) glitch level=1111, width=21ns, (c) glitch level=1111, width=14ns.

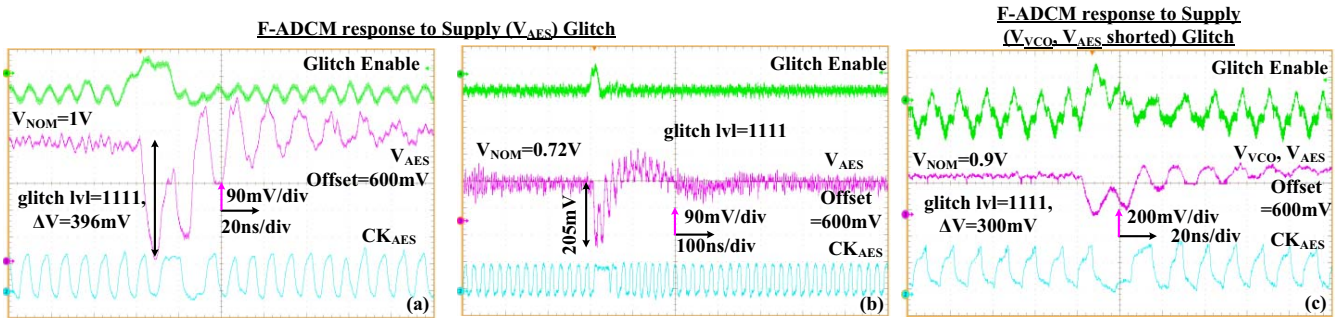


Fig. 10. F-ADCM responds to supply glitches: (a) at nominal conditions (V_{AES}=1V, F_{AES}=110MHz) with the highest glitch level, (b) at V_{AES}=0.72V with the highest glitch level, and (c) effect of glitch on VCO supply voltage when V_{AES} and V_{VCO} are shorted. F-ADCM still operates reliably under glitches.

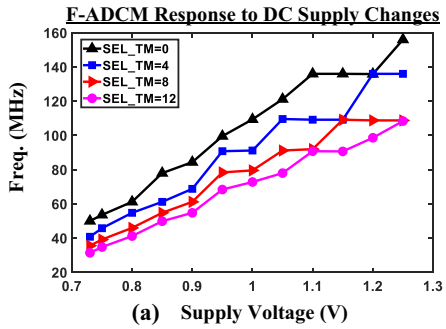
ciphertexts are randomly chosen for DFA until the key is recovered. The number of exploitable faults injected increase initially with increasing drop in supply voltage as more unique faults are injected, however as drop is increased further, exploitable faults decrease, mainly due to multi-byte faults injected with higher drop. At highest drop (384mV), none of the faulty ciphertexts were exploitable for a glitch width of 21ns. However, for same drop but 14ns glitch width, 28 exploitable faults were injected. The experiment indicates the importance of controlling glitch height and width, even when we inject glitches randomly during the encryption.

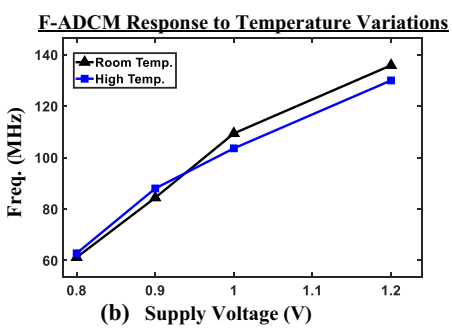
B. Fault Mitigation with F-ADCM (Protected AES Mode)

Supply Glitch @V_{AES}: In presence of supply drops, GM inside F-ADCM modulates CK_G to prevent timing failures. Since in our design, GM is in proximity to AES-128, it can modulate the clock even in presence of local supply noise, therefore, LM doesn't play a big role. Fig. 10(a) and (b) show operation of F-ADCM under highest glitch level (1111) at 1V and 0.72V. F-ADCM generates rising clock edges only when entire critical path is traversed under supply glitch (the output clock period is significantly increased at higher glitch levels). No faults could be injected at nominal operating conditions even after 10 million encryptions under all glitch profiles (width and level). However, when power supply is decreased to 0.8V and 0.72V, faults could be injected (1 fault @0.8V and 168758 faults @0.72V, though only 1 unique fault which is same at both supply conditions) even when F-ADCM is on. This could be caused by slight mismatch between critical path replicas and actual critical path circuit at low supply voltages or a very different path may be critical, not the one implemented with critical path replicas as digital gates have very different behavior under extreme levels of supply noise which is not observed with simulation/STA.

To mitigate these faults, timing margin is added with the help of programmable trimmer inside GM (trimmer 0, configurable from 0-31 in increments of 1) with SEL_TM=2. With additional timing margin (SEL_TM=2), no faults could be injected at 0.8V/0.72V. Fig. 11(a) shows F-ADCM output clock freq. characterized with DC changes in supply voltage (0.72V-1.25V) for a few SEL_TM settings. When the supply voltage is further reduced, the level shifter (Fig. 1) between core (V_{AES}) and I/O (3.3V) domains fails and internal clock can no longer be observed. However, AES correctly operates up to 0.58V. We couldn't inject any faults at 0.58V even with highest glitch level. When supply is further reduced, F-ADCM and AES circuits completely fail and generate 16-byte unexploitable faults.

Temperature Variations: The delay of CMOS gates changes under temperature variations. To study the effect of temperature on injected faults and F-ADCM generated output clock frequency, testchip was subjected to hot air flow for 30 seconds with a 120V/300W heat gun from about 3cm. Fig. 11(b) shows the response of F-ADCM at room temperature and high temperature. Inverse temperature dependence is observed in the output clock frequency. Therefore, FIA becomes critical at higher voltages under overheating. At nominal operating conditions (F_{AES}=110MHz, V_{AES}=1V), only one fault could be injected at room temperature after 100K encryptions while number of faults increase to 3376 at high temperature [Fig. 11(c)]. A skilled adversary can control the testchip temperature to induce temperature dependent faults during the last few rounds for FIA. With F-ADCM turned on, no faults are injected with 100K encryptions at room temperature or high temperature.





Fault Injection with Temperature Variations @V_{AES}=1V, F_{AES}=110MHz

	# of Faults (Total, Unique, Exploitable)	
	Room Temperature	High Temperature
Standalone AES	1,1,0	3376,1,0
F-ADCM +AES	0,0,0	0,0,0

(c)

Fig. 11. (a) Characterization of F-ADCM for DC supply voltage ranging from 0.72-1.25V, (b) effect of increased temperature on F-ADCM output clock freq., and (c) more faults are injected at high temperature at nominal conditions (V_{AES}=1V, F_{AES}=110MHz) however with F-ADCM turned ON, all faults are prevented.

Supply Glitch @V_{VCO}: Since an adversary doesn't have access to internal clock when F-ADCM is ON, he/she may still alter VCO supply clock to modify the operation of F-ADCM itself. We shorted VCO supply (V_{VCO}) with V_{AES} to investigate the effect of supply glitch on VCO and therefore F-ADCM. Under nominal conditions, we couldn't inject any faults however at V_{VCO}=0.9V [Fig. 10(c)], we were able to inject same fault as observed for V_{AES}=0.72V in previous section. This fault goes away for SEL_TM=2. When V_{VCO} is further reduced, both VCO and F-ADCM operate reliably at reduced DC supply however under supply glitch, it is no longer operational.

C. Discussion

Traditionally error-resilient circuits have been designed to tolerate and correct for timing errors under small supply glitch to increase performance. Exploiting these timing error detection/correction and prevention (F-ADCM) circuits to mitigate fault attack is an interesting research direction as an adversary will try all possible methods to make the circuit fail even with abnormal operating conditions, e.g. high supply glitches. Additionally, the error-resilient circuits may themselves fail giving rise to a possible path to inject faults in the cryptographic hardware. We observed the need to build timing margin to account for any layout mismatches or in case some other path is activated under certain conditions. Design flow in [19] can be used to minimize these mismatches. Additionally, parasitics of on-chip power delivery network will create small mismatches in the exact timing of injected glitch at F-ADCM and AES. A proficient adversary may be able to exploit these differences to inject faults. However, for a large design, it is recommended to have distributed local modulator circuits to respond to local supply noise. Additionally, F-ADCM cannot prevent timing errors due to hold failures [11]. With large +ve spikes in supply voltage, short paths in AES-128 (primarily related to control/finite state machines) can be activated. However, a guardband can be built into the design to tackle hold issues at small area and power overheads without any impact on performance. Moreover, since proposed F-ADCM generated output clock period is a multiple of source clock period, input data-dependent fluctuations in critical path delay (may lead to an unintentional timing side channel) are only minimally reflected in the generated clock.

Compared to other error-resilient architectures, F-ADCM prevents timing errors from occurring while other techniques, such as Razor [14], may completely stall the pipeline resulting in denial-of-service attacks. Additionally, unlike Razor which requires modifying the sequential elements, F-ADCM doesn't require any modification in the underlying hardware and therefore has very small overheads (12.5% area and 3.3% power – Table 1). Finally, F-ADCM doesn't require any complex glitch detection circuits like in [15].

V. Conclusion

This paper demonstrated that a F-ADCM circuit, normally designed to increase variation tolerance, can also prevent supply glitch and temperature variations-based fault injection attacks. Measurement results from a 130nm CMOS test-chip showed successful DFA attack on a standalone AES-128 digital core with externally controlled fault injections and programmable glitch width and height. However, when F-ADCM is turned on to provide clock to AES-128, no fault could be injected even after 10 million encryptions under wide range of operating conditions. F-ADCM can mitigate both supply glitch and temperature variation induced faults and incurs only 12.5% area and 3.3% power overheads and improves performance under supply transient noise.

Acknowledgment

This material is based on work supported in parts by Intel Corp. and Semiconductor Research Corporation through TxACE (#2810.002).

VI. References

[1] D. Boneh, R. A. Demillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," Advances in Cryptology - EUROCRYPT, 1997, LNCS, vol 1233, Springer.

[2] E. Biham, and A. Shamir, "Differential fault analysis of secret key cryptosystems," Advances in Cryptology - CRYPTO, 1997, LNCS, vol 1294, Springer.

[3] C. Giraud, "DFA on AES," Int. Conf. on AES, 2004, pp. 27-41.

[4] G. Piret, and J. J. Quisquater, "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad," CHES, 2003, LNCS, vol 2779, Springer.

[5] T. Fukunaga, and J. Takahashi, "Practical Fault Attack on a Cryptographic LSI with ISO/IEC 18033-3 Block Ciphers," Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009, pp. 84-92.

[6] A. Tang, S. Sethumadhavan, and S. Stolfo, "CLKSCREW: exposing the perils of security-oblivious energy management," USENIX Conference on Security Symposium (SEC), 2017, pp 1057-1074.

[7] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures," in Proceedings of the IEEE, vol. 100, no. 11, pp. 3056-3076, 2012.

[8] C. Yen, and B. Wu, "Simple error detection methods for hardware implementation of Advanced Encryption Standard," in IEEE Trans. on Computers, vol. 55, no. 6, pp. 720-731, 2006.

[9] B. Wang et al., "Exploration of Benes Network in Cryptographic Processors: A Random Infection Countermeasure for Block Ciphers Against Fault Attacks," in IEEE Trans. on Information Forensics and Security, vol. 12, no. 2, pp. 309-322, 2017.

[10] M. Doulcier-Verdier, J. Dutertre, J. Fournier, J. Rigaud, B. Robisson, and A. Tria, "A side-channel and fault-attack resistant AES circuit working on duplicated complemented values," IEEE ISSCC, 2011, pp. 274-276.

[11] K. Gomina, P. Gendrier, P. Candelier, JB Rigaud, and A. Tria, " Detecting positive voltage attacks on CMOS circuits," Cryptography and Security in Computing Systems (CS2), ACM, 2014, pp. 1-6.

[12] K. Gomina, J. Rigaud, P. Gendrier, P. Candelier and A. Tria, "Power supply glitch attacks: Design and evaluation of detection circuits," IEEE HOST, 2014, pp. 136-141.

[13] L. Zussa et al., "Efficiency of a glitch detector against electromagnetic fault injection," IEEE DATE, 2014, pp. 1-6.

[14] D. Ernst et al., "Razor: a low-power pipeline based on circuit-level timing speculation," IEEE/ACM MICRO, 2003, pp. 7-18.

[15] M. S. Floyd et al., "26.5 Adaptive clocking in the POWER9™ processor for voltage droop protection," IEEE ISSCC, 2017, pp. 444-445.

[16] K. Chae and S. Mukhopadhyay, "All-Digital Adaptive Clocking to Tolerate Transient Supply Noise in a Low-Voltage Operation," in IEEE Trans. on Circuits and Systems II, vol. 59, no. 12, pp. 893-897, 2012.

[17] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "Improved power side channel attack resistance of a 128-bit AES engine with random fast voltage dithering," IEEE ESSCIRC, 2017, pp. 51-54.

[18] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "Improved Power/EM Side-Channel Attack Resistance of 128-Bit AES Engines With Random Fast Voltage Dithering," in IEEE JSSC, 2018.

[19] M. Khairallah et al., "DFARPA: Differential fault attack resistant physical design automation," IEEE DATE, 2018, pp. 1171-1174.