A 54μW Design-Agnostic Clock, Voltage, and EM-Pulse Fault-Injection Attack Detection using Time-to-Voltage Conversion

Yudhajit Ray, Archisman Ghosh, Sarthak Antal, Shreyas Sen

Purdue University, IN, USA

Fault Injection Attacks (FIAs) exploit faults to reveal sensitive information or extract keys from secured crypto algorithms (e.g. AES, Kyber, ASCON)[1-5]. Clock, voltage, and EM pulse (EMP) based FIAs are widespread due to the availability of cheap attack hardware [4]. Such glitches exploit digital designs by creating timing failures in the data path, leading to bit-flips, stuck-at-faults, etc. [3,4] (Fig. 1), which are exploited using algorithms such as Differential Faults Attacks [6]. In recent years, a few FIA detector ASICs have emerged, including design-specific attack detectors [7] and design-agnostic detectors[8,9]. [7] implements an error-checking-based FIA detector for AES with a 40% area overhead. Oversampling the clock to detect glitches[8] restricts timing sensitivity and consumes high power and area (0.8mW, 4800μm2 in 5nm). [9] utilizes a delay-locked-loop (DLL) to determine the duty cycle deviation in the presence of clock glitches, consuming 300μW at 50MHz. Though [8,9] did not include a crypto core, the power consumption of the clock-glitch detector is >50-200% of a typical crypto core (e.g. AES 256 65nm 50MHz is 590μW[10]), calling for an order-of-magnitude improvement in the power of FIA detectors. Moreover, there have been no dedicated voltage or EM Pulse glitch detector ASICs. Relying on a clock-glitch detector for voltage glitch detection, as in [9], may miss a voltage/EM Pulse glitch that creates a fault in the data path but not a clock glitch, causing true negatives.

Noting the fundamental nature of an effective clock glitch, which has fixed amplitude (V_{pp}) but varies in time (Δt) (Fig. 1), an integration-based solution promises to be highly sensitive and power efficient. Conversely, voltage/EMP glitch, i.e. small in amplitude (Δv) and time (Δt) calls for a differentiator for optimum detection. Utilizing these fundamentals, we introduce 1) an integrating clock glitch detector, to convert time information to voltage information that supports more efficient detection of all types of clock glitches (T1-T12), enabling a 4x benefit in glitch detection window and 33x power reduction over [9], 2) a differentiating voltage glitch/EMP detector consuming only 1.27μW power (<0.5%) with 3) an example newly standardized lightweight crypto-core ASCON, to investigate the effect of FIA, as highlighted in the overall system architecture in Fig. 2.

The system comprises two clock glitch detector units (26.5 μW each) operating at opposite levels to provide full coverage of all clock glitch types (odd and even), utilizing the inversion property among different types of clock glitches (Fig. 1). The voltage glitch detector also helps in EMP detection as it creates voltage glitches without tampering with the IC. Internal and external clock glitch generation modalities are designed in for extensive testability. As clock and voltage glitch detectors consume minimal area and power, multiple monitors can be placed in the IC to detect localized attacks.

The clock glitch detector is composed of one integrating amplifier and two differential double-tail samplers with slightly different threshold voltages (TH1/2) to define the acceptable window for normal clock operation (Fig. 2). The differential variant of double-tail sampler provides better performance in terms of power and input-referred noise. During normal clock operation, the sampler outputs (OUT1/2) will always be 0 and 1, respectively. In the presence of clock glitch, the deviation from normal operation of the positive detector (1A), as shown in Fig. 2-bottom left, ensures detection of glitches that affect the high state of the clock. Simultaneously operating the negative detector (1B) ensures detection of glitches that affect the low state of the clock. Clock glitches trip the detector circuit outside the acceptance window and create an output flag. Given that clock glitches are anomalies in time and detecting fine time leads to high power consumption, this architecture converts time anomalies to voltage anomalies and detects them in the voltage domain. A discrete-time integrating amplifier (Fig. 3) enables current-efficient time-to-voltage conversion. The output differential voltage is proportional to the clock high duration (TINT) and the transconductance (Gm) of the input nMOS pair. An nMOS cross-coupled integrating amplifier with cascading [11] enhances the current efficiency (Gm/Id), thereby reducing power consumption. Time-multiplexed operation further reduces the power consumption of each integrator by keeping them off for 50% of the clock period. Integration also reduces the impact of supply or input voltage noise at the differential output, enabling the detection of sharper clock glitches.

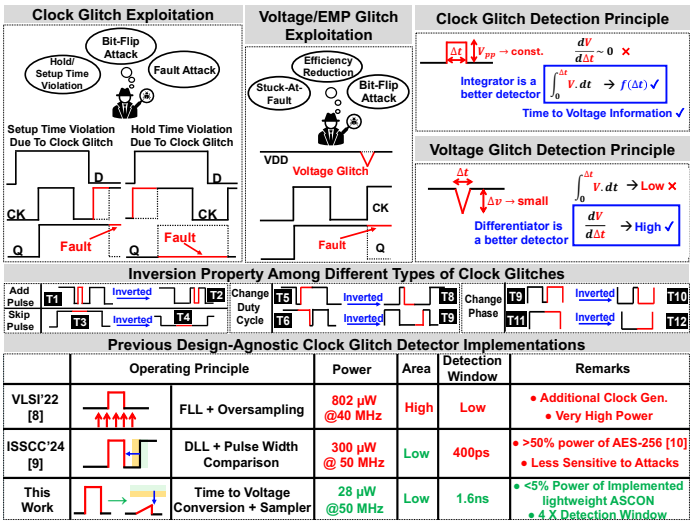
Voltage glitch detection (Fig. 3) operates on the principle of extracting maximum information through differentiation (dV/dΔt) and filtering out other sources that can interfere with the detection. The self-biased inverter is used as the differentiator due to its low power consumption, followed by a current starved inverter to provide an adjustable threshold voltage, rejecting supply noise in an amplified domain and creating a digital glitch flag. An RC-filter on the inverter supply ensures glitches only go to the detector input and not to the supply, which helps in avoiding missing alerts. A capacitive divider at the input aids in AC-coupled biasing while preventing direct supply to the ground path. The voltage glitch detector's normally off state only consumes active power in the presence of voltage or electromagnetic interference (EMP). As a result, the total power consumption of voltage glitch detector is only 1.27μW, <0.58% of power of implemented NIST lightweight crypto core ASCON. We utilize 320-bit data-path ASCON implementation for 80-bit security[12]. Load characterization for different supply voltages and frequencies shows power consumption ranging from 12μW at 0.8V supply, 500KHz to 850μW at 1V supply, 50MHz.

Fig. 4 presents the measured output waveform from the 65nm CMOS IC, illustrating the glitch flag generated when a periodic voltage fault of 200mV depth and 4ns width is introduced every 500ns. The IC glitch flag operates in two modes: continuous multi-glitch detection and single-glitch detection. In Mode 1, the IC can detect continuous incoming glitches to ensure the absence of false-positives or false-negatives. In Mode 2, the flag output can latch to VDD in the presence of a single voltage glitch, resulting in a total latency of 900ps from the onset of the fault. The voltage glitch detection Shmoo plot demonstrates the detector's performance under various voltage glitch depths and widths. A high-performance AWG is employed to generate voltage glitches with depths ranging from 100mV to 300mV and widths varying from 400ps to 8ns. Additionally, we present the impact of an electromagnetic pulse (EMP) attack on the supply rail of the IC and demonstrate the successful detection of an EMP attack using an on-chip detector for the first time. A 1.5W EMP generates a multi-peak glitch waveform on the IC supply, which the detector perceives as three concurrent glitches in Mode 1 (continuous detection mode) without any missed alerts. The EMP glitch detection Shmoo plot illustrates the detector's performance with varying EMP glitch generation power and the distance of the inductor from the supply. The overall implementation of the voltage glitch/EMP detector occupies an area of 1500μm2 and 1.27μW power.

Fig. 5 presents detailed measurements of the clock-glitch detector. The clock glitch generation circuit employs an internal counter to generate a configurable sharp pulse of 160ps to 1.2ns every 32 cycles of the input clock. This pulse can be added or subtracted to generate T1/T2 and T5-T12 clock glitches for continuous testing of clock glitch attacks. T3/T4 and broader clock glitch attacks are generated externally. The clock glitch Shmoo plot illustrates the detection performance. The detector can detect all tested glitch widths for T1-T4. For the remaining glitch widths, depending on the type of glitch, the crypto core is more susceptible to narrow glitch widths for T5-T6, T9-T10, and to wide glitch widths for T7-T8, T11-T12, respectively. In both ranges where the glitch is more effective, the detector successfully detects with zero errors. The clock glitch detector design offers a 4x improvement in the largest detectable glitch width (400ps in [9] to 1.6ns) for glitches where higher width is more challenging to detect. An operation frequency-independent comparison of glitch detectors is more suitable when compared in terms of duty-cycle deviation. The accurate detection window is improved from 4/50 [9] to 16-28/50 duty cycle deviation, depending on the type of clock glitch. Periodic detection (Fig. 5 top right) of all major types of clock glitches is tested while ensuring there are no missing alerts. In comparison to previous implementations of clock glitch detectors, the overall power consumption is significantly reduced by a factor of 33x at 2.5MHz and 28x at 40MHz, as demonstrated in [9] and [8], respectively. Furthermore, duty-cycled operation of the detector further reduces the power consumption to 6μW at 2.5MHz and 53μW at 100MHz.

Fig. 6 illustrates the accuracy and power consumption of the clock glitch detector across a range of supply voltages, demonstrating its wide operational range from 0.85 V to 1.4 V. The complete clock glitch detector has an active area of 2250 μm2. The impact of clock glitch faults on the ASCON crypto core has been investigated, revealing that while the absence of clock glitches results in consistent ciphertext generation, the presence of glitches at different clock cycles enables successful fault injection, leading to diverse ciphertext outputs. The comparison table demonstrates a power improvement of 3.6x to 33x over state-of-the-art clock detectors while simultaneously expanding the detection window by 4x. Additionally, the performance and power consumption of a dedicated on-chip voltage/EMP glitch detector are presented for the first time. Although the FIA detectors are design-agnostic, when compared to the example ASCON core (216 μW at 10 MHz), the overhead of the voltage/EMP and clock-glitch detectors is negligible, comprising only 0.58% and 5% respectively. The die micrograph, power, and area breakdowns of the implemented IC are presented in Fig. 7.

2025 IEEE Custom Integrated Circuits Conference (CICC) | 979-8-3315-1745-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/CICC63670.2025.10983804



Previous Design-Agnostic Clock Glitch Detector Implementations					
	Operating Principle	Power	Area	Detection Window	Remarks
VLSI'22 [8]	FLL + Oversampling	802 µW @40 MHz	High	Low	• Additional Clock Gen. • Very High Power
ISSCC'24 [9]	DLL + Pulse Width Comparison	300 µW @ 50 MHz	Low	400ps	• >50% power of AES-256 [10] • Less Sensitive to Attacks
This Work	Time to Voltage Conversion + Sampler	28 µW @50 MHz	Low	1.6ns	• <5% Power of Implemented lightweight ASCON • 4 X Detection Window

Fig. 1. Clock, voltage, and EMP glitch exploitations on digital designs, optimal operating principles for detecting clock and voltage glitch, inversion property of different types of clock glitches, previous design-agnostic clock glitch detectors.

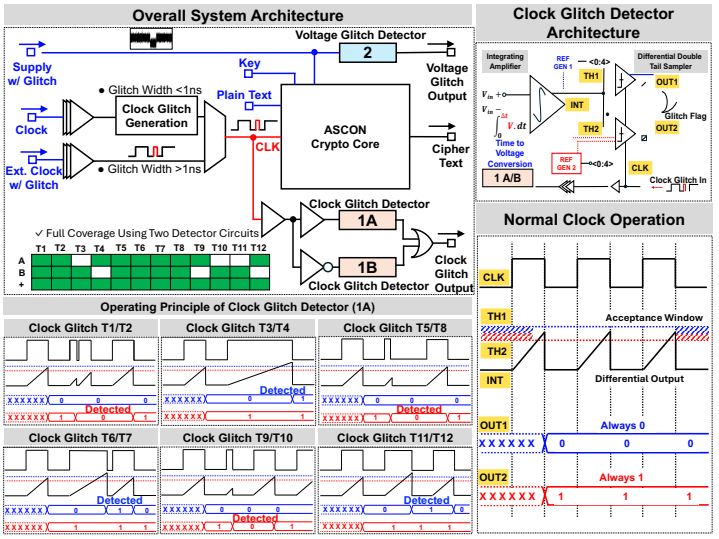


Fig. 2. Overall system architecture of the implemented IC, clock glitch detector architecture; normal clock operation and deviation from it in the presence of clock glitch, affecting high state of the clock.

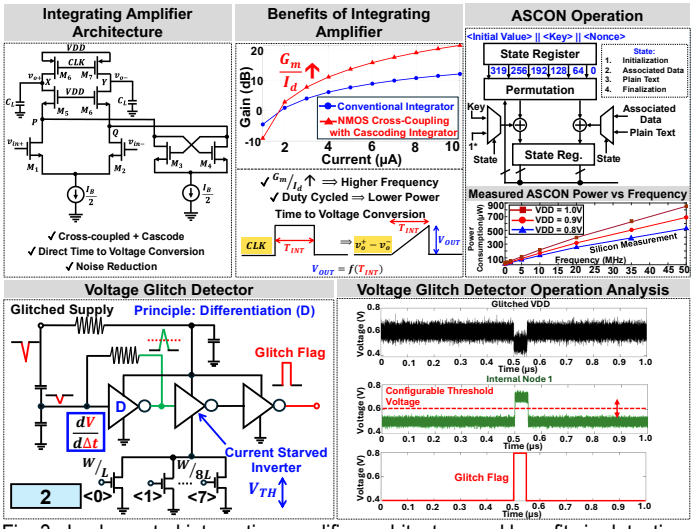
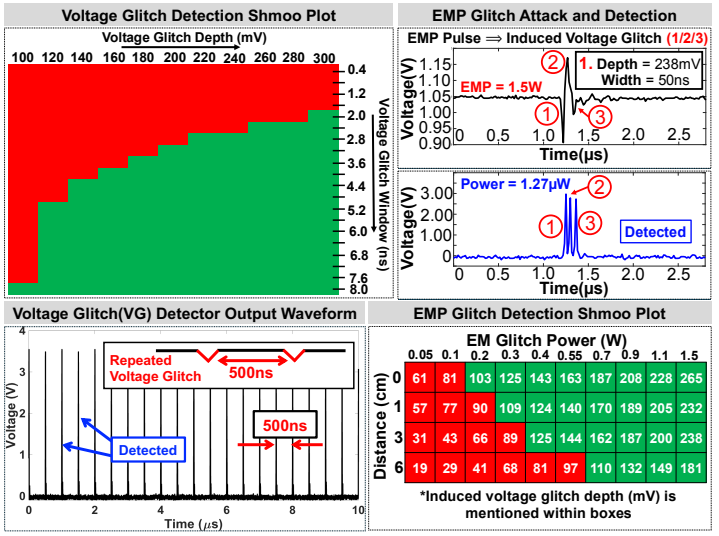
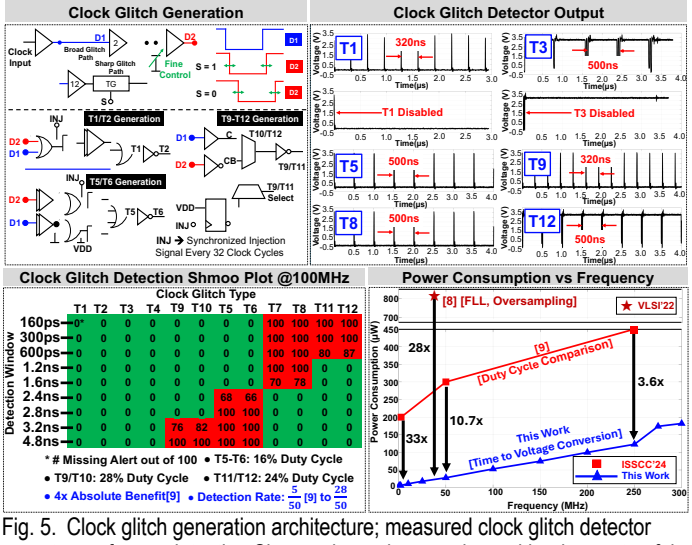


Fig. 3. Implemented integrating amplifier architecture and benefits in detecting glitches; Operation and load-characteristics of on-chip ASCON crypto core; Voltage glitch detector and operation analysis



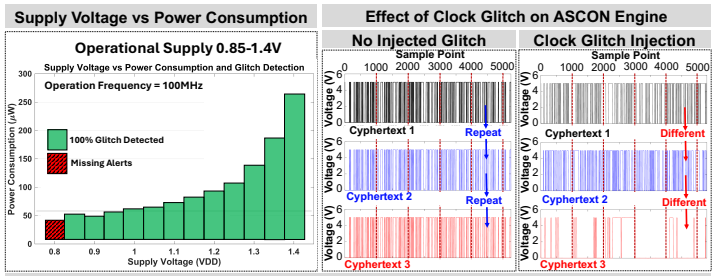
Distance (cm) \ EM Glitch Power (W)	0.05	0.1	0.2	0.3	0.4	0.55	0.7	0.9	1.1	1.5
0	61	81	103	125	143	163	187	208	228	265
1	57	77	90	109	124	140	170	189	205	232
3	31	43	66	89	125	144	162	187	200	238
6	19	29	41	68	81	97	110	132	149	181

Fig. 4. Implemented integrating amplifier architecture and benefits in detecting glitches; Operation and load-characteristics of on-chip ASCON crypto core; Voltage glitch detector and operation analysis



Clock Glitch Type → / Detection Window ↓	T1	T2	T3	T4	T9	T10	T5	T6	T7	T8	T11	T12
160ps	0*	0	0	0	0	0	0	0	100	100	100	100
300ps	0	0	0	0	0	0	0	0	100	100	100	100
600ps	0	0	0	0	0	0	0	0	100	100	80	87
1.2ns	0	0	0	0	0	0	0	0	100	100	0	0
1.6ns	0	0	0	0	0	0	0	0	70	78	0	0
2.4ns	0	0	0	0	0	0	68	66	0	0	0	0
2.8ns	0	0	0	0	0	0	100	100	0	0	0	0
3.2ns	0	0	0	0	76	82	100	100	0	0	0	0
4.8ns	0	0	0	0	100	100	100	100	0	0	0	0

Fig. 5. Clock glitch generation architecture; measured clock glitch detector output waveforms, detection Shmoo plot and comparison with other state of the art achieving 3.6x-33x benefit compared to [9].



Comparison Chart with Other State-Of-The-Art Voltage and Clock Glitch Detectors								
	Tech.	Operation Principle	Primary Glitch Detection	Crypto-Core	Power (µW)	Area (MF²)	Frequency Independent Detection Window	Detected Clock Glitch Width	Attack Type
ISSCC'23 [7]	4nm	Error Checking	NA	AES	-	244	-	-	Any FIA
VLSI'22 [8]	5nm	FLL + Oversampling	Clock	Agnostic	802 @ 40MHz	192	-	-	Low Freq. Clock
ISSCC'24[9]	65 nm	Pulse Width Comparison	Clock	Agnostic	487 @250MHz	0.355	5% Duty Cycle	400ps	Clock, Voltage, EMI
This Work	65 nm	Integration + Comparison	Clock	Design Agnostic	53 @100MHz	0.532	16-28% Duty Cycle	1.6ns	Clock
		Differentiation	Voltage / EMP		1.27	0.355	>100mV	-	Voltage, EMP

Fig. 6. Measured performance of Clock glitch detector for varied supply voltage; Effect of clock glitch on implemented ASCON core showing different ciphertext output, comparison with prior-art.

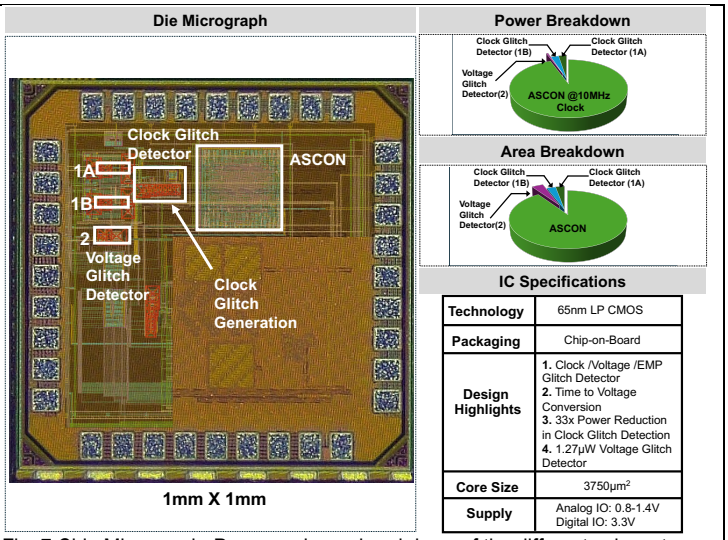


Fig. 7 Chip Micrograph; Power and area breakdown of the different sub-systems; IC specifications

Acknowledgements

<Acknowledgment placeholder>

References:

[1] K. Ramezanpour *et al.*, "A Statistical Fault Analysis Methodology for the Ascon Authenticated Cipher," HOST, 2019, https://doi.org/10.1109/HST.2019.8741029

[2] K. Murdock *et al.*, "Plundervolt: Software-based Fault Injection Attacks against Intel SGX," IEEE SP, 2020, https://doi.org/10.1109/SP40000.2020.00057

[3] M. Tunstall *et al.*, "Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault. In: Ardagna," WISTP, 2011, https://doi.org/10.1007/978-3-642-21040-2_15

[4] S. Kundu *et al.*, "Carry Your Fault: A Fault Propagation Attack on Side-Channel Protected LWE-Based KEM," CHES, 2024, https://doi.org/10.46586/tches.v2024.i2.844-869

[5] P. Mondal *et al.*, "A Practical Key-Recovery Attack on LWE-Based Key-Encapsulation Mechanism Schemes Using Rowhammer," ACNS, 2024, https://doi.org/10.1007/978-3-031-54776-8_11

[6] A. Ghosh *et al.*, "36.2 An EM/Power SCA-Resilient AES-256 with Synthesizable Signature Attenuation Using Digital-Friendly Current Source and RO-Bleed-Based Integrated Local Feedback and Global Switched-Mode Control," ISSCC, 2021, https://doi.org/10.1109/ISSCC42613.2021.9365978

[7] R. Kumar *et al.*, "15.5 A 100Gbps Fault-Injection Attack Resistant AES-256 Engine with 99.1-to-99.99% Error Coverage in Intel 4 CMOS," ISSCC, 2023, https://doi.org/10.1109/ISSCC42615.2023.10067715

[8] S. Song *et al.*, "An FLL-Based Clock Glitch Detector for Security Circuits in a 5nm FINFET Process," VLSI, 2022, https://doi.org/10.1109/VLSITechnologyandCir46769.2022.9830157

[9] Y. He *et al.*, " 16.5 A Synthesizable Design-Agnostic Timing Fault Injection Monitor Covering 2MHz to 1.26GHz Clocks in 65nm CMOS," ISSCC, 2024, https://doi.org/10.1109/ISSCC49657.2024.10454280

[10] A. Ghosh *et al.*, " Syn-STELLAR: An EM/Power SCA-Resilient AES-256 With Synthesis-Friendly Signature Attenuation," JSSC, 2022, https://doi.org/10.1109/JSSC.2021.3113335

[11] Y. Ray *et al.*, "Analysis of Discrete-Time Integrating Amplifiers as an Alternative to Continuous-Time Amplifiers in Broadband Receivers," OJCAS, 2023, https://doi.org/10.1109/OJCAS.2023.3338210

[12] C. Dobraunig *et al.*," Ascon v1.2: Lightweight Authenticated Encryption and Hashing, J Cryptol, 2021, https://doi.org/10.1007/s00145-021-09398-9