FROM RING OSCILLATORS TO READOUTS: DISCOVERING USER-SPACE POWER PROXIES ON PYNQ/ZYNQ-7000

Marianne Ninet[1], Yehya Nasser[1],Eliott Quere[2], Ruben Salvador[2]
[1]*IMT Atlantique, Plouzané,* [2]*CentraleSupélec, IRISA, Inria, Cesson-Sévigné*

Abstract

Modern ARM–SoC FPGAs expose numerous hardware blocks whose timing drifts are induced by power supply fluctuations, enabling software-based power side-channel observation without external measurement equipment.

This work investigate power proxy areas and focuses on whether network packet timing can serve as a remotely-accessible, user-space proxy on Zynq-7000 platforms, leveraging the relationship between power delivery network (PDN) current fluctuations and signal propagation delays. We generate controlled power stress using ring-oscillator (RO) farms in the programmable logic, while concurrently capturing UDP packet timestamps under high network traffic conditions. Unlike existing approaches that rely on specialized sensors, privileged register access, or custom FPGA circuits, our method uses only application-layer network timing and ROs, requiring no privileges and is accessible remotely. Statistical analysis is then applied to correlate network timing variations with known power stress patterns, assessing the feasibility of power monitoring for side-channel attack analysis.

Keywords : Side-Channel Attacks (SCA);Remote Power Analysis;FPGA;Power Proxies;Network Timing.

I INTRODUCTION

The Xilinx Zynq-7000 family of System-on-Chip (SoC) FPGAs has become omni-present in critical embedded systems due to the tight integration of an ARM Processing System (PS) and high-throughput Programmable Logic (PL). This architecture exposes sensitive applications to Side-Channel Attacks (SCA) [1], particularly those leveraging power consumption fluctuations to reconstruct cryptographic secrets.

Historically, SCAs required intrusive physical access and specialized equipment (oscilloscopes, probes..). Modern research on Non-Invasive Side-Channel Attacks (NISCA) eliminates physical probes by measuring micro-architectural artifacts like cache timing or voltage regulator droop. In multi-tenant cloud FPGA environments attacks like FPGADefender [2] demonstrate how unprivileged users can generate significant power stress using malicious Ring-Oscillator circuits in the PL creating new defense challenges.

This work investigates a novel vector: network packet timing as an indirect power proxy. Unlike approaches requiring specialized sensors (INA226 [3]) or privileged register access (DLL states [4]), we use only user-space network timestamps. High-throughput network flows are measured via timestamp analysis while the system is subjected to controlled power stress generated by ring oscillators (RO) activity.

This article is organized as follows: Section II reviews background and related work. Section III presents our aims. Section IV details the experimental methodology and setup. Finally, Section V discusses expected results and Section VI concludes this paper.

II BACKGROUND AND RELATED WORK

Power Side-Channel Attacks exploit the correlation between power consumption in the power delivery network (PDN) and processed data to extract cryptographic secrets. Recent work has demonstrated that various on-chip sensing mechanisms can be weaponized as SCA tools without external measurement equipment.

AmpereBleed [3] leveraged dedicated INA226 current sensors, exposed via the Linux hwmon interface, to perform circuit-free power analysis, highlighting the risk of vendor-provided telemetry.

SideLine [4] showed that Delay-Locked Loop (DLL) and delay-line (DL) states within memory controllers drift measurably with voltage noise, transforming them into software-readable voltage sensors capable of enabling Correlation Power Analysis (CPA) on SoCs like the Zynq-7000.

On the FPGA fabric itself, Time-to-Digital Converters (TDCs), Routing Delay Sensors (RDS) and 1-LUT sensors [5] measure voltage variations but require embedding crafted circuits.

Our work explores a fundamentally different observation channel: network packet timing. The hypothesis is that power stress in the PL perturbs the shared VCCINT supply rail, causing voltage fluctuations. The supply voltage fluctuations affect propagation delays throughout the PS, from CPU instruction timing to memory controller and Ethernet MAC/PHY latency. These accumulated micro-delays manifest as measurable jitter in packet reception timestamps.

Unlike existing approaches that requires specialized hardware sensors, privileged access to system registers or custom sensing circuits, network timestamps require no special privileges and are universally available in networked embedded systems. This makes them particularly relevant for cloud FPGA scenarios, where physical access is restricted but network connectivity is inherent to the system's function.

III AIM

This work addresses two key questions:

- Signal detectability: Can pseudo-random power variations generated by ROs stress introduce measurable timing perturbations that exceed the baseline jitter of the Linux network stack and Ethernet physical layer ?

- Correlation strength: Do inter-arrival jitter variance, kernel-to-userspace delay, and packet loss rates exhibit statistically significant correlation with known PRBS stress patterns across varying traffic loads (50k–300k packets per second)?

If validated, this would establish network timing as a novel, remotely-accessible power side-channel requiring no specialized hardware, privileges, or FPGA circuits.

IV. METHODS

We evaluate network packet timing as a potential covert channel by correlating controlled power stress patterns with observable timing variations in UDP traffic. Our experimental setup consists of a PYNQ-Z1 board (Zynq-7000 XC7Z020, ARM Cortex-A9) as the receiver and a Raspberry Pi 5 as the UDP packet generator.

To generate controlled power stress, we deploy 256 Flip-Flop Ring Oscillators in the FPGA programmable logic (PL), oscillating at approximately 500 MHz. This frequency was chosen because it provides significant dynamic power without violating timing constraints, additional frequencies may be tested in future work. These oscillators are modulated by a Pseudo-Random Binary Sequence generator, as in prior work [2]. It creates pseudo-random stress patterns that avoid fixed-frequency tones, which could be attenuated by on-chip power delivery networks. By toggling RO activity synchronously with network traffic injection, we can search for statistical correlations between known stress patterns and observed timing perturbations. User-space software toggles the entire RO bank between active (high current draw) and idle states via a memory-mapped AXI GPIO register, enabling precise synchronization with network traffic patterns. Concurrently, the Raspberry Pi transmits high UDP traffic at configurable rates (50k–300k packets per second). Each packet contains a sequence number and nanosecond-resolution send timestamp, allowing precise loss detection and one-way delay measurement. The PYNQ receiver runs a custom C program (`rx_logger.c`) that uses `recvmmsg()` for batch reception with kernel timestamps.

An automated shell script orchestrates: (1) deploy and launch the receiver on the PYNQ board, (2) initiate UDP traffic from the Raspberry Pi (3) toggle the RO stress in a periodic pattern (OFF,ON) for 15 complete cycles, (4) terminate traffic and retrieve the timestamped log file.

Statistical analysis will focus on inter-arrival jitter variance which is expected to increase during stress-ON periods due to clock frequency modulation and Ethernet MAC timing drift. Also, packet loss rates should correlate with stress state due to degraded timing margins in the network stack or hardware buffers.

V EXPECTED RESULTS

If network timing correlates with power stress, we anticipate a measurable increase in variance and distribution shifts during stress periods. Even a weak correlation would validate the principle of remotely-accessible power leakage. A potential limitation is that timing noise sources (kernel jitter, network congestion, or buffering effects) may dominate under high traffic rates, limiting the detectability of PDN-induced timing variations.

VI CONCLUSION

By correlating PRBS-modulated ring-oscillator stress with UDP packet timestamps, this work determines whether network timing can serve as a remotely-accessible power proxy on Zynq-7000 SoCs, without specialized sensors, privileges, or custom FPGA circuits. If validated, this would show that even in cloud FPGA or IoT scenarios where physical access is impossible, an attacker with network connectivity alone may observe side-channel leakage. This expands the SCA threat model for heterogeneous SoC platforms, motivating further research into network-level countermeasures and timing-resilient architectures.

Future work could extend to real cryptographic workloads and explore countermeasures such as traffic shaping and timestamp fuzzing.

References

[1] F.-X. Standaert, 'Introduction to Side-Channel Attacks', in *Secure Integrated Circuits and Systems*, I. M. R. Verbauwhede, Ed., Boston, MA: Springer US, 2010, pp. 27–42. doi: 10.1007/978-0-387-71829-3_2.

[2] Tuan Minh La, Kaspar Matas, Nikola Grunchevski, Khoa Dang Pham, and Dirk Koch, 'FPGADefender: Malicious Self-oscillatorScanning for Xilinx UltraScale+FPGAs'. ACM Trans.Reconfigurable Technol. Syst. 13, 3,Article 15, english.

[3] Xin Zhang et al., 'Amperebleed : Exploiting On-chip Current Sensors for Circuit-Free Attacks on ARM-FPGA SoCs'. 2025.

[4] Joseph Gravellier, Jean-Max Dutertre, Yannick Teglia, and Philippe Loubet Moundi, 'SideLine: How Delay-Lines (May) Leak Secrets from your SoC'. 2020.

[5] David Spielmann, Ognjen Glamočanin and Mirjana Stojilović, ‘RDS: FPGA Routing Delay Sensors for Effective Remote Power Analysis Attacks’.