Ph.D. Project - IsoFPGA - A Novel CMOS Galvanic Isolation for Remote Physical Attacks in Multi-tenant Cloud FPGA

Muhammed Kawser Ahmed and Christophe Bobda
Electrical and Computer Engineering, University of Florida
Email: muhammed.kawsera@ufl.edu and cbobda@ece.ufl.edu

2024 IEEE 32nd Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM) | 979-8-3503-7243-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/FCCM60383.2024.00041

***Abstract*—Although FPGAs in cloud applications facilitate customized hardware acceleration, they also introduce new security challenges that demand attention. Granting cloud users, the capability to reconfigure hardware designs after deployment may create potential vulnerabilities for malicious users, thereby jeopardizing entire cloud platforms. Multi-tenant FPGA services, where a single FPGA is divided spatially among multiple users, are highly vulnerable to such attacks such as remote power side channel attacks, Denial of Service (DoS) attacks and Fault Injection attacks. Security solutions are limited by the architectural design of existing FPGAs. We propose a novel power distribution network for cloud FPGA security using physical CMOS-based galvanic isolation. In this architecture, each tenant is isolated spatially, providing protection against voltage spikes, ground loops, and electrical noise, the key premises of remote physical attacks. The isolation technique is carried out by using reconfigurable MoM (Metal-over-Metal) capacitors and switch banks, along with Power Management and Configuration Controller Unit. By implementing a Custom Configuration Memory (CCM), we aim to provide a dynamic and customizable solution that allows FPGA designers to selectively interconnect or isolate groups of Configurable Logic Blocks (CLBs). This approach involves the formation of distinct regions within the FPGA, each capable of sourcing power either from a dedicated CMOS isolation power supply or the standard FPGA voltage power supply. Our approach, leveraging physical isolation, can successfully prevent such attacks and can be established as the first line of defense for cloud FPGA security.**

***Index Terms*—Security, FPGA, SoC, Remote Voltage Attack, Multi-tenant**

I Problem and Motivation

As FPGA designs often underutilize the entire programmable logic available on a board, there have been academic research proposals exploring methods to share a single FPGA fabric among multiple cloud users. This involves leveraging the partial reconfigurable characteristics of FPGAs to maximize utilization. The crucial property of FPGAs allowing reconfiguration in specific regions during runtime without affecting others enables this sharing. Since all tenants share the same FPGA fabric and its power distribution network (PDN), malicious attackers could extract sensitive information such as voltage and total current consumption and launch various hardware-based attacks, including remote FPGA power side-channel attacks , Denial-of-Service (DoS) attacks, remote fault-injection attacks, and covert channel communications [1], .

In this context, we propose a novel physical isolation mechanism called IsoFPGA which can resist remote physical attacks (power side channel, fault injections, and denial-of-service) with physical CMOS-based galvanic isolation. Our proposed solution extends the current FPGA architecture with the addition of IsoFPGA to protect tenants' circuits on the same FPGA at various level of granularity. Figure 1 illustrates the high-level overview of the proposed model. In the general architecture depicted in Figure 1 (a), all tenant logic blocks are placed in the same **Vdd** and *ground* of FPGA metal layers as part of a single PDN. In Figure 1 (b), the proposed isolation model is presented. Tenant logic blocks are spatially isolated by a physically separated CMOS voltage source and ground. The control of this isolation is managed by custom configuration memory.

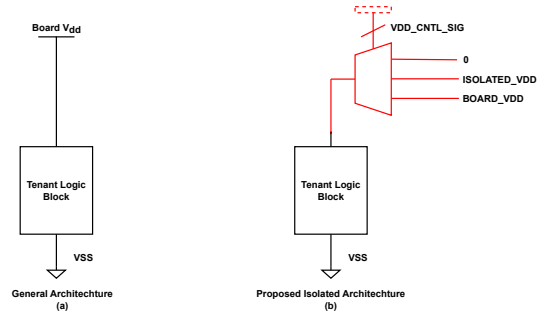

Fig. 1: High level overview of the proposed CMOS based physical isolation model.

II Background and Related Work

A. Multi-tenant Cloud FPGA and Power Distribution Network (PDN)

FPGAs can be shared among multiple tenants through two sharing models: time and spatial. In the time-sharing scheme, the entire FPGA board is allocated to a user/tenant for a specific time period, during which the tenant has full control and access. In spatial sharing, the FPGA fabric is partitioned into different regions, granting concurrent tenants access to isolated regions for designated time periods. Spatial sharing offers several advantages, including optimal resource utilization, shorter wait times, and potential cost savings. In FPGA technology, a single Power Distribution Network (PDN) is responsible to supply and maintain necessary voltage level and current for all of the components in the board. Any small variation in the PDN network can cause a significant current drop and hence affect the voltage. By inserting a sensor, this voltage drop can be read and exploited to launch attacks.

B. Galvanic Isolation

Galvanic isolation is a technique used to separate electrical circuits from each other in order to prevent the flow of direct current (DC) between them [2]. It relies on the use of a physical barrier or an isolation device, such as transformers or optocouplers, to transmit signals or power across the isolation boundary. This isolation provides protection against electrical noise, voltage spikes, and ground loops that can occur in interconnected systems. Optocouplers and Transform isolation are the two most common methods applied for isolation in circuits. But they are still yet to be integrated in CMOS platforms due to their notoriously slow and poor performance issues [3] .

C. Related Work

Gnad et al. [4] proposed a bitstream checking technique, also known as FPGA antivirus, which checks for the signatures of malicious logic that might lead to electrical-level attacks. Similarly, FPGA Defender [5] proposes an antivirus technology that scans the

2576-2621/24/$31.00 ©2024 IEEE
DOI 10.1109/FCCM60383.2024.00041

Authorized licensed use limited to: University of Florida. Downloaded on February 02,2025 at 18:05:56 UTC from IEEE Xplore. Restrictions apply.

configuration blocks (CLBs), block RAM memories (BRAMs), and digital signal processing blocks (DSPs) of a bitstream to detect non-ring-oscillator-based attack circuits (self-oscillators). This technique can be handy because self-oscillating attacker circuits can hardly be detected by AWS or other major public cloud FPGA providers. However, a drawback of both two methods are, it flags all non-malicious true random number generator circuits (TRNG) that exploit self-oscillator technology. Masking strategies are typically achieved by applying cryptographic algorithms that help transform the base circuit into a logically different but functionally equivalent circuit [6]. Hiding strategies can be accomplished by reducing the Signal-to-Noise Ratio (SNR) at the computational stages of design cores, which mitigates the attacker's ability to leak sensitive information using different sensors [4].

III Proposed Approach

We propose a CMOS-based galvanically isolated power delivery mechanism that completely isolates the power supply of each tenant in the FPGA device which is proposed in Figure 2. In our proposed model we use reconfigurable capacitor-based galvanic isolation instead of inductors and optocouplers.By galvanically isolating the power supply of each tenant block, tenants are protected from any voltage drops or currents present in neighbouring tenants. The isolation technique is carried out by using reconfigurable MoM (Metal-over-Metal) capacitors and switch banks, along with the Power Management and Configuration Controller Unit. The capacitors act as an energy reservoir, and by utilizing the proper switching mechanisms it can isolate the attached power supply and separate it from the main voltage supply while still delivering the necessary current to the tenant. Reconfigurable Capacitor banks, with the help of power management unit, can isolate and deliver necessary current to a connected tenant region that is separate from main power supply VCC and VSS.

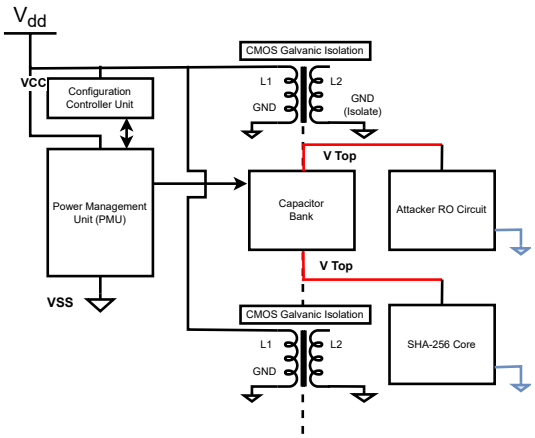

Fig. 2: Proposed capacitive galvanic isolation circuit for galvanic isolation of two tenant cores (RO and SHA-256 crypto).

Figure 3 shows a detailed view of the tenant logic block (TLB) and CLB cluster formation that is connected to a multiplexer which allows the TLB to be connected from either the general board power source or our proposed isolated capacitive source (Figure 3).

IV Expected Results and Contributions:

In this work, we have developed a novel CMOS-based capacitive galvanic isolation technique to prevent remote physical attacks in a multi-tenant cloud FPGA. The proposed design exploits charge

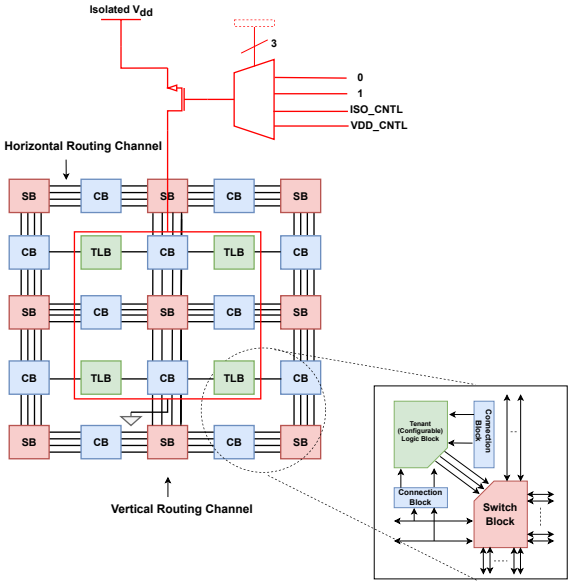

Fig. 3: A detailed view of the isolated tenant block source connection.

pump circuits using reconfigurable capacitors in the CMOS context to provide an isolated power supply for each tenant logic block. For preliminary evaluation, we conducted Differential Power Analysis (DPA) retrieving power variation data from Cadence Virtuoso platform. For both isolated and non-isolated SHA-256 core configurations, we collected 8000 traces. The physical isolation implemented in our proposed model makes it nearly impossible to recover any key from any round of computation due to the physical isolation of the core. The DPA attack fails to establish any relationship between voltage drop over time and the current isolation configuration. Also, the isolate modules was also successful against remote fault injection and denial of service attacks as there is no visible voltage drop in the supply line when the core is galvanically isolated using configuration process. In future work, we plan to perform in-depth work to facilitate the isolation transition with minimum overhead and time. Also, we plan to tape-out the proposed design to validate its effectiveness and electrical properties in a runtime scenario.

References

[1] I. Giechaskiel, S. Tian, and J. Szefer, "Cross-VM Information Leaks in FPGA-Accelerated Cloud Environments,"

[2] M. Wang, S. Xie, P. N. Li, A. Sayal, G. Li, V. V. Iyer, A. Thimmaiah, M. Orshansky, A. E. Yilmaz, and J. P. Kulkarni, "Galvanically isolated, power and electromagnetic side-channel attack resilient secure aes core with integrated charge pump based power management," in *2021 IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1–2, 2021.

[3] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Exploiting fully integrated inductive voltage regulators to improve side channel resistance of encryption engines," in *Proceedings of the 2016 International Symposium on Low Power Electronics and Design*, ISLPED '16, (New York, NY, USA), p. 130–135, Association for Computing Machinery, 2016.

[4] D. R. Gnad, S. Rapp, J. Krautter, and M. B. Tahoori, "Checking for Electrical Level Security Threats in Bitstreams for Multi-Tenant FPGAs," *Proceedings - 2018 International Conference on Field-Programmable Technology, FPT 2018*, pp. 289–292, 12 2018.

[5] T. L. Minh, K. Matas, N. Grunchevski, K. Dang Pham, D. Koch, T. Minh La, M. La, K. Matas, N. Grunchevski, K. D. Pham, and D. Koch, "FPGADefender," *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, vol. 13, p. 2020, 9 2020.

[6] Y. Ishai, A. Sahai, and D. Wagner, "Private Circuits: Securing Hardware against Probing Attacks,"

Authorized licensed use limited to: University of Florida. Downloaded on February 02,2025 at 18:05:56 UTC from IEEE Xplore. Restrictions apply.