opoSoM: A Modular Measurement Platform for Dynamic Power Consumption of SoCs

Kristóf Kanics, Meinhard Kissich
Graz University of Technology
Graz, Austria
{kristof.kanics,
meinhard.kissich}@tugraz.at

Gerhard Wirrer
Infineon Technologies AG
Neubiberg, Germany
Gerhard.Wirrer@infineon.com

Tobias Scheipel, Marcel Baunach
Graz University of Technology
Graz, Austria
{tobias.scheipel,
baunach}@tugraz.at

Abstract—**Software can have a significant impact on the electrical characteristics of the executing integrated circuit. The analysis of minor current consumption changes in a System-on-Chip reveals details about the executed instructions or the hardware's internal logic, potentially exposing sensible information. Despite careful design, glitches pose a further challenge that needs to be handled at hardware and software level.**

This paper introduces the concept of the open-source, modular *opoSoM* measurement platform that captures the dynamic power characteristics of System-on-Chips featuring external and on-chip measurement techniques. Due to the configurable measurement range and synchronous sampling at up to 250 MS/s, the platform provides valuable measurement data for investigating countermeasures against side-channel attacks and optimizing hardware and software towards lower dynamic power consumption.

***Index Terms*—System-on-Chip, measurement, supply voltage, power consumption, side-channel attacks**

I. Introduction

The externally observable dynamic power consumption may reveal valuable and sensitive information about the behavior of a processor core. Kocher et al. [1] showed very early that it is possible to extract information (e.g., cryptographic keys) from electronic devices based on power consumption measurements. Voltage sensors can be integrated into the implementation of a digital design [2] for Field Programmable Gate Arrays (FPGAs). Existing on-chip voltage sensors use the physical effect that the signal propagation depends on the device's supply voltage: Time-to-Digital Converters (TDCs) sample an input signal in a delay line with configurable length to probe how fast a signal transition propagates. Ring Oscillators (ROs) change their oscillation frequency depending on the delay in its individual stages, converting supply voltage transients into frequency deviations. Integrating on-chip voltage sensors into a device poses a significant threat when, e.g., an FPGA is shared among multiple users in cloud systems [3]. While service providers try to counteract attacks, by e.g., prohibiting combinatorial loops [4], such ROs have been used to crash an FPGA due to excessive power consumption by using only 12% of its lookup table resources [5]. As the power estimation of computer-aided design tools can significantly underestimate the power consumption [6] of such structures, a versatile and highly accurate research platform is required to detect and analyze malicious circuits.

Independent of their potentially malicious nature, fast transients in the dynamic power consumption (e.g., load jumps caused by unwanted signal activity) can compromise the device's own operation. The voltage on the supply pin might not be able to follow a rapid change in the current consumption due to the supply trace's parasitic inductance. Such supply anomalies can potentially cause device malfunctions or resets [7]. Optimizing the dynamic power consumption by e.g., minimizing the switching activity [8], is crucial when designing for side-channel attack resilience.

In this paper, we present a modular measurement platform that consists of a carrier board and pluggable modules that carry the System-on-Chips (SoCs) under test: ***opoSoM*** (optimizing power consumption for System on Modules) allows for cycle-accurate on-chip and external voltage measurements to analyze the dynamic power consumption of SoCs. It is designed to

- map voltage transients to instructions,
- compare voltage measurements that correspond to code sequences running on different implementations of the same architecture,
- investigate how the dynamic power consumption can be reduced by optimizing the hardware architecture, its implementation, and the software as a whole, and
- elaborate on the effectiveness of countermeasures against side-channel attacks.

When writing this paper, the first pluggable module is available, and the carrier board and further modules are under development.

The paper is structured as follows: **Section II** presents related work. **Section III** and **Section IV** describe the architecture of the carrier board and the necessary components of the modules, respectively. The suggested measurement techniques are presented in **Section V**, and **Section VI** closes with an outlook to future work.

II. Related Work

Fast voltage transients in an SoC have been investigated in several works, focusing on the current consumption of entire processes [9], [10], often using the built-in Analog-to-Digital Converters (ADCs) of the device under test [9], [11]. ChipWhisperer [12] offers a hardware and software environment to emulate and analyze side-channel attacks on

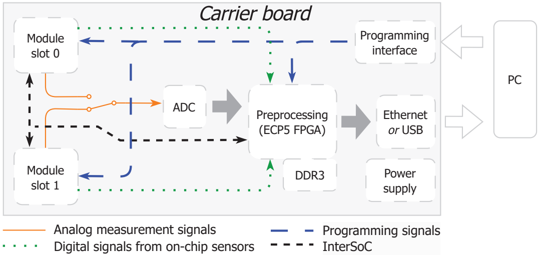


Fig. 1: Architecture of the *opo**SoM*** measurement platform.

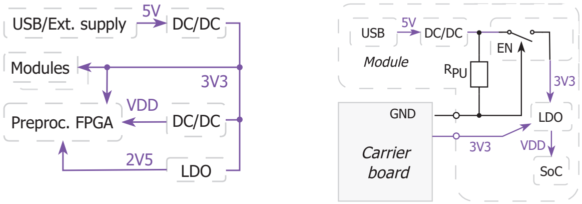
different circuit boards, using an external resistor as a current sensor. Voltage transients are often not easy to measure outside of an SoC since the on-chip and external decoupling capacitors flatten the transients. Therefore, *opo**SoM*** extends ChipWhisperer's approach by additionally applying on-chip sensor topologies with high voltage resolution and nanoscale range [13], [14], [15]. In contrast to the previously mentioned works [9], [10], [11], we are interested in how single instructions or short instruction sequences in Application Specific Integrated Circuit (ASIC) or FPGA-based soft processors can cause significant changes in the power consumption. We aim to perform cycle-accurate on-chip and external measurements to map voltage transients to executed instructions. Guiding the place and route tools enables to place sensors at different locations in the SoC to gather information about where exactly the voltage transients originate from or how different implementations of an architecture influence the measurement results. The measurement data is preprocessed in a separate device to avoid influencing the device under test itself. Localizing power peak sources at software and hardware levels helps to implement appropriate countermeasures to prevent side-channel attacks and optimize the system to reduce voltage drops that can lead to device malfunctions.

III. Carrier Board Architecture

The carrier board (cf. Fig. 1) has two slots for pluggable System-on-Modules (SoMs) that are built around the SoCs under test (cf. Section IV.). The measurement components are placed on the carrier board to provide an identical measurement environment for all SoCs. A Lattice ECP5 FPGA [16] is used to buffer and preprocess the measured sensor data. The data is then forwarded to a PC through Ethernet or USB. By generating a clock signal using the on-board ECP5 or an external clock source, the ADC and the SoC under test on a module can be clocked synchronously. Synchronous clocking is essential to keep track of code execution and voltage transients simultaneously. The following sections describe the individual building blocks of the carrier board in more detail.

A. Power supply

Fig. 2a summarizes the power supply scheme. The carrier board can be powered either via USB or by an external power supply, in case USB is insufficient to operate the on-board components *and* the plugged modules. An on-board step-down DC/DC converter provides the necessary 3V3 I/O voltage for the preprocessing FPGA and the plugged modules. The 1V2 core voltage of the preprocessing FPGA is generated by a second



a, *opo**SoM*** platform b, module

Fig. 2: Power supply scheme.

step-down converter. The 2V5 voltage level with low current flow is provided by a Low Drop-Out (LDO) regulator.

B. Programming interface

To avoid using multiple USB cables, the on-board FPGA and the SoCs on the modules can be programmed via an on-board USB hub and a subsequent JTAG converter. Configuration data are stored in each SoC's corresponding flash memory.

C. Data preprocessing and PC interface

For data preprocessing (e.g., filtering, compression) and buffering, the board features 1 GiB of DDR3 memory. The preprocessed data can be transmitted to a PC via Gigabit Ethernet or using a 5 Gbps USB peripheral controller.

D. Analog-to-digital converter

The analog signals from the modules are fed into a two-channel differential ADC. The two ADC channels are driven by two fully differential amplifiers. The amplifier circuits provide linearity in a wider frequency range compared to baluns. For conversion, an ADS4229 [17] converter was selected based on its 250 MS/s maximum sample rate, 550 MHz analog input bandwidth, and moderate price. To be compliant with the Nyquist-Shannon sampling theorem, the frequency of the input signal must not be higher than 125 MHz. An anti-aliasing filter ensures the band-limitation of the input signal.

IV. Module Architecture

Each module features an SoC that contains an arbitrary analog or digital design to be evaluated. The effects on the dynamic power consumption of an instruction sequence are measured utilizing the on-chip voltage sensors and the on-board passive components. The measurement signals are routed directly to the module's interface connectors, and are not processed by the SoC under test to avoid negative effects on the signal quality. The modules can be plugged onto the carrier board described in the previous section. As a second option, the modules are designed to be operable in stand-alone mode when no measurements are performed, allowing to work on different modules simultaneously.

When using the module plugged onto the carrier board, it is supplied via the carrier board's 3V3 power rail, and the on-module step-down converter is disabled to eliminate its switching noise. The ground potential of the carrier board is used as a disable signal for a power switch (cf. Fig. 2b), preventing reverse current flow into the output of the step-down converter of the module. In the absence of the carrier board, R_{PU} pulls the enable pin of the power switch high to keep the switch on. The core voltage of the SoC under test and other necessary voltage levels are generated directly on the module. For this purpose, LDOs are preferred over switched-mode regulators to produce less noise. The USB signals of the module are accessible by the carrier board, which allows to program the module via the carrier board's USB connector and hub. The modules connect to the carrier board via a specifically tailored interface (InterSoC) and using Serializer/Deserializer (SerDes) if available on the SoC under test. SerDes signals are directly accessible on the module via four SMA connectors as the example design shows (Fig. 3).

In stand-alone mode, the modules are supplied via USB and the on-board voltage regulators (cf. Fig. 2b). The modules can be programmed via the same USB connector and an on-module USB-to-JTAG converter.

V. Measurement Concept

Fig. 4 sketches the measurement concept of the *opo**SoM*** platform. To capture fast transients of the core supply, techniques *A.* to *C.* are applied:

A. Voltage drop on current-sense resistor

The voltage drop on a current-sense resistor R_S is proportional to the current consumption *I*. Small (10 nF to 100 nF) noise filtering capacitors placed close to the device pin are not depicted in Fig. 4. Depending on the SoC under test, they may or may not be necessary for a normal SoC operation. On each module, we populate as few of them as required to keep the device operational while not absorbing the transients. Decoupling capacitors C_{dec} (100 nF to 10 µF) are placed in front of R_S so that the current flowing from them into the device pin can be captured. With fast signal changes, package parasitics become more significant. The capacitor C_{comp} is placed in parallel to R_S to compensate for the parasitic inductance of R_S. For evaluating the measurements with an external oscilloscope and for calculating the compensation afterwards, the potential difference on R_S is accessible on SMA connectors. To the measurement signals on R_S, an anti-aliasing (AA) filter is applied, and the signals are amplified on the carrier board before feeding them into the ADC.

Current sensing on a serial resistor is a common measurement technique [10] but it requires a current-sense resistor (and eventually a compensation capacitor) as close as possible to the SoC's supply pins. The optimal position is under the device, on the back of the circuit board, which is already a component-dense area due to decoupling capacitors. The value of R_S has to be chosen based on the current consumption of the SoC under test. The higher the resistor value and the current consumption, the larger the induced voltage drop and therefore the easier it is to capture. On the other hand, a high voltage drop can reduce the supply voltage on the device pin below the device's specification.

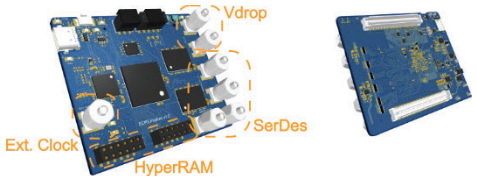


Fig. 3: 3D view of an example module with an ECP5 FPGA.

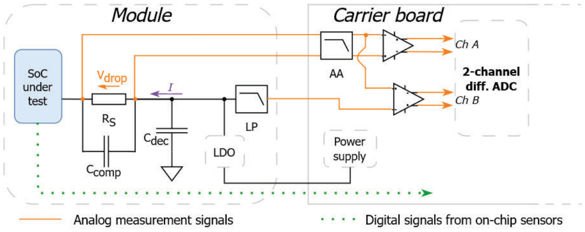


Fig. 4: Measurement concept.

B. Direct voltage measurement

In contrast to the current-sense method, this technique is prone to noise coupling and ground bouncing. Short, impedance-controlled traces mitigate these issues. High resolution can be achieved by reducing the measured voltage range to the range of interest using the voltage regulator's low-pass (LP) filtered output as a potential reference. Single-ended voltage measurement does not require additional components, and a higher current consumption does not lead to a more difficult transient capture. If the evaluation of this measurement technique results in a comparable accuracy as the current-sense technique, further modules can be designed implementing only this technique, reducing manufacturing costs. The accuracy of this technique is high due to the differential signaling and is limited by package and trace parasitics.

C. Measurement with on-chip sensors

On-chip voltage level sensors (TDCs or ROs) can be implemented close to the source of transients, directly inside a target FPGA, to provide the most accurate measurement data among techniques *A.* to *C.* The sensors' nanoscale resolution allows the detection of transients even above the device's operation frequency due to the FPGA's internal power delivery network parasitics [15]. The carrier board receives signals from two 10-bit on-chip sensors of each plugged module. Since these sensors are directly implemented in the device under test, this measurement technique is not applicable for hard cores (e.g., microcontrollers) unless the sensors are already part of the implemented design. The on-chip sensors' resolution depends on their implementation (e.g., sampling rate).

D. Additional considerations

The carrier board can accommodate two pluggable SoMs with one SoC under test on each of them. The analog interfaces are multiplexed in a way that the ADC can process two arbitrary analog interfaces coming from any of the modules simultaneously. The external techniques' measurement range strongly depends on the static *and* dynamic current consumption of the SoC under test, and it has to be calibrated for each SoC under test by selecting an appropriate R_S. To log the temperature while performing measurements, the carrier board can read the module's temperature using external temperature sensors attached onto the SoC under test.

Synchronizing the ADC's sampling clock and the device's clock allows for the detection of transients that occur aligned with the clock edge. Without synchronous sampling, the detection requires a sampling rate far over the device's operation frequency. ChipWhisperer [12] shows that the results of synchronous sampling at 96 MS/s are comparable to those of an asynchronous sampling at 2 GS/s. With 250 MS/s synchronous sampling, our platform is designed to detect voltage transients on devices running at maximum 250 MHz. Synchronous sampling also provides a reliable timestamp that allows for an efficient mapping of voltage transients to executed instructions.

VI. Conclusion and Future Work

In this paper, we presented the architecture of a modular measurement platform to track the dynamic power consumption of a wide range of SoCs in the same measurement environment. The external and on-chip measurement techniques provide a flexible measurement range for devices running at up to 250 MHz. The requirements for further modules with new SoCs to be evaluated and the corresponding interfaces between a module and the carrier board are described.

On each module, a calibration process needs to be performed: We have to determine the values of the noise filtering capacitors on the SoC's supply pins and the value of the current-sense resistor R_S experimentally. Current-sense and direct voltage measurements need to be compared using an external oscilloscope to cancel out package parasitics for R_S. If the comparison yields a significant difference between the two measurement techniques, the worse-performing technique can be optimized out for further modules in order to reduce manufacturing costs.

Future research demands a measurement dataset that we can obtain via running benchmark code on an open architecture that we have full control of. Suitable candidates are RISC-V soft cores due to their growing popularity and a number of existing implementations (e.g., CV32E40P [18], VexRiscv [19], FazyRV [20]). These first datasets help to identify which instructions or instruction sequences influence the dynamic power characteristics the most. Based on the gathered knowledge, we aim to develop software techniques to detect ambiguous instruction sequences at compile time and improve the digital logic to mitigate the effect of specific instructions (e.g., via adjusting the soft core's pipeline [21]). We are also interested in how the voltage transients differ from core to core, especially from a soft core to a hard core of the same architecture implementation. Another interesting research question is how these transients can be attenuated by applying different place-and-route techniques. Finally, we aim to explore other optimization strategies to mitigate side-channel attacks originating both within and outside of an SoC.

The source files of the *opo**SoM*** platform are available open source on *https://github.com/EAS-DSD/opoSoM*.

Acknowledgment

This work has been supported by the FFG under contract No.881844: "Pro2Future" (Products and Production Systems of the Future), Graz University of Technology (TU Graz), and Infineon Technologies AG in the joint research project CompEAS.

References

[1] P. Kocher et al., "Differential Power Analysis," Springer Berlin Heidelberg, 1999.

[2] K. M. Zick et al., "Sensing nanosecond-scale voltage attacks and natural transients in FPGAs," in *Proceedings of the ACM/SIGDA International Symposium on Field Programmable Gate Arrays*, Monterey, 2013.

[3] O. Glamočanin et al., "Are Cloud FPGAs Really Vulnerable to Power Analysis Attacks?," in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2020.

[4] aws/aws-fpga, *AWS EC2 FPGA HDK+SDK Errata, GitHub,* 2021. (accessed 2024-04-26).[Online]. Available: https://github.com/aws/aws-fpga/blob/master/ERRATA.md

[5] D. R. E. Gnad et al., "Voltage drop-based fault attacks on FPGAs using valid bitstreams," in *2017 27th International Conference on Field Programmable Logic and Applications (FPL)*, 2017.

[6] K. Matas et al., "Power-hammering through Glitch Amplification – Attacks and Mitigation," in *IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, 2020.

[7] A. Boutros et al., *Neighbors From Hell: Voltage Attacks Against Deep Learning Accelerators on Multi-Tenant FPGAs,* 2020.

[8] M. Kubica et al., "Logic Synthesis Strategy Oriented to Low Power Optimization," *Applied Sciences,* vol. 11, 2021.

[9] Feinstein, David Y. et al., "System-on-Chip Power Consumption Refinement and Analysis," in *6th IEEE Dallas Circuits and Systems Workshop on System-on-Chip*, 2007.

[10] T. Doebbert et al., "Precision measurement of the application-dependent current consumption of a wireless transceiver chip in the time and frequency domain," *Journal of Sensors and Sensor Systems,* 2022.

[11] Nakutis, Žilvinas, "A consumption current measurement approach for FPGA based embedded systems," in *IEEE International Instrumentation and Measurement Technology Conference Proceedings*, 2012.

[12] O'Flynn, Colin and Chen, Zhizhang, "ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research," in *Lecture Notes in Computer Science*, Springer International Publishing, 2014.

[13] X. Xu et al., "A High-Resolution Nanosecond-Scale On-Chip Voltage Sensor for FPGA Applications," *IEEE Transactions on Instrumentation and Measurement,* vol. 72, 2023.

[14] S. Moini et al., "Understanding and Comparing the Capabilities of On-Chip Voltage Sensors against Remote Power Attacks on FPGAs," in *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2020.

[15] J. Gravellier et al., "High-Speed Ring Oscillator Based Sensors for Remote Side-Channel Attacks on FPGAs," *2019 International Conf. on ReConFigurable Computing and FPGAs (ReConFig),* 2019.

[16] Lattice Semiconductor, *ECP5 and ECP5-5G Family, Datasheet*

[17] Texas Instruments, *ADS4229 Dual-Channel, 12-Bit, 250-MS/S Ultralow-Power ADC,* June 2011 – Revised May 2015.

[18] OpenHW Group, *cv32e40p,* GitHub, (accessed 2024-05-23). [Online]. Available: https://github.com/openhwgroup/cv32e40p.

[19] C. Papon, *VexRiscv,* 2018., GitHub, 2018, (accessed 2024-05-16). [Online]. Available: https://github.com/SpinalHDL/VexRiscv

[20] M. Kissich and M. Baunach, "FazyRV: Closing the Gap between 32-Bit and Bit-Serial RISC-V Cores with a Scalable Implementation," in *Proc. of the 21st ACM International Conference on Computing Frontiers (CF '24)*, 2024.

[21] T. Scheipel et al., "moreMCU: A Runtime-reconfigurable RISC-V Platform for Sustainable Embedded Systems," in *2022 25th Euromicro Conference on Digital System Design (DSD)*.