Extended Abstract: Covert Channels and Data Exfiltration From FPGAs

Ilias Giechaskiel
Independent Researcher
United Kingdom
ilias.giechaskiel@gmail.com

Ken Eguro
Microsoft Research
Redmond, WA, USA
eguro@microsoft.com

Kasper Rasmussen
University of Oxford
Oxford, United Kingdom
kasper.rasmussen@cs.ox.ac.uk

***Abstract*—In complex FPGA designs, implementations of algorithms and protocols from third-party sources are common. However, the monolithic nature of FPGAs means that all subcircuits share common on-chip infrastructure, such as routing resources. This presents an attack vector for all FPGAs that contain designs from multiple vendors, especially for FPGAs used in multi-tenant cloud environments, or integrated into multi-core processors: hardware imperfections can be used to infer high-level state and break security guarantees. In this paper, we demonstrate how "long" routing wires present can be used to for covert communication between disconnected cores, or by a malicious core to exfiltrate secrets. The information leakage is measurable for both static and dynamic signals, and that it can be detected using small on-board circuits. In our prototype we achieved $6\,\mathrm{kbps}$ bandwidth and 99.9% accuracy, and a side channel which can recover signals kept constant for only 128 cycles, with an accuracy of more than 98.4%.**

The high cost of FPGA design and development has led to an increase in outsourcing, making it common to have designs from different contractors on the same FPGA chip [1], [8]. Such designs often include protocol and data structure implementations, or more sophisticated circuits, like radio front-ends or soft processors. This practice raises concerns about the malicious inclusion of circuits (cores) that have additional backdoor functionality [5], [6], especially when FPGAs are integrated in multi-tenant cloud environments, or multi-core processors [3], [7], [9].. Although third-party implementations can be functionally validated before being included in the overall design, it is not always possible to detect unintentional information leakage or intentional covert channels [4]. It is thus important to identify sources of information leakage and protect against any resulting channels exploiting those sources.

In this work, we show that the value driven onto certain types of FPGA routing resources, called "long" wires, influences the delay of nearby wires, *even when the driven value remains constant*. This distinguishes our approach from prior work which depends on fast-changing signals [2], [5], and thus local voltage drops or inductive crosstalk. Specifically, we find that if a long wire carries a logical 1, the delay of nearby long lines will be slightly lower than when it carries a logical 0. This difference in delay allows cores sharing the same reconfigurable FPGA fabric to communicate, even when they are not directly connected.

We demonstrate how this phenomenon is measurable within the device by small circuits even in the presence of environmental noise, and without any modifications to the FPGA. We show how this phenomenon can be used to create a communication channel between circuits that are not physically connected. As designs often incorporate circuits from multiple third-parties, this channel can break separation of privilege between IP cores of different trust levels, or enable communication between distinct cores in multi-user setups. Such use-cases are increasingly common as FPGAs and CPUs become integrated, and as FPGAs become available on public cloud infrastructures. The same mechanism can also be used to eavesdrop and recover keys with high probability even when the signals change during the period of measurement. In our prototype implementation, the channel has a bandwidth of up to $6\,\mathrm{kbps}$, and we can recover 99.9% of the transmitted bits correctly using a Manchester encoding scheme. We can also recover signals which are kept constant for as low as 128 cycles, with an accuracy of more than 98.4%. The phenomenon is present in four generations of Xilinx FPGAs, and the channel is present regardless of the arrangement, location, or orientation of the cores, and with multiple transmitting circuits present. The strength of the phenomenon scales linearly with the number of wires used, and also dominates a competing effect caused by switching activity.

References

[1] R. S. Chakraborty, I. Saha, A. Palchaudhuri, and G. K. Naik. Hardware trojan insertion by direct modification of FPGA configuration bitstream. *IEEE Design Test*, 30(2):45–54, April 2013.

[2] M. Gag, T. Wegner, A. Waschki, and D. Timmermann. Temperature and on-chip crosstalk measurement using ring oscillators in FPGA. In *Design and Diagnostics of Electronic Circuits Systems (DDECS)*, 2012.

[3] Ilias Giechaskiel, Ken Eguro, and Kasper Rasmussen. Leakier wires: Exploiting FPGA long wires for covert- and side-channel attacks. *Transactions on Reconfigurable Technology and Systems (TRETS)*, 2019.

[4] T. Huffmire, B. Brotherton, T. Sherwood, R. Kastner, T. Levin, T. D. Nguyen, and C. Irvine. Managing security in FPGA-based embedded systems. *IEEE Design Test of Computers*, 25(6):590–598, Nov 2008.

[5] Shane Kelly, Xuehui Zhang, Mohammed Tehranipoor, and Andrew Ferraiuolo. Detecting hardware trojans using on-chip sensors in an ASIC design. *Journal of Electronic Testing*, 31(1):11–26, 2015.

[6] M. Lecomte, J. J. A. Fournier, and P. Maurine. Thoroughly analyzing the use of ring oscillators for on-chip hardware trojan detection. In *ReConFigurable Computing and FPGAs (ReConFig)*, 2015.

[7] Chethan Ramesh, Shivukumar B. Patil, Siva Nishok Dhanuskodi, George Provelengios, Sébastien Pillement, Daniel Holcomb, and Russell Tessier. FPGA side channel attacks without physical access. In *Field-Programmable Custom Computing Machines (FCCM)*, 2018.

[8] M. Tehranipoor and F. Koushanfar. A survey of hardware trojan taxonomy and detection. *IEEE Design Test of Computers*, 27(1):10–25, Jan 2010.

[9] M. Zhao and G. E. Suh. FPGA-based remote power side-channel attacks. In *IEEE Symposium on Security and Privacy (SP)*, 2018.

978-3-9819263-5-4/DATE21/©2021 EDAA