

Secure Data-Binding in FPGA-based Hardware Architectures utilizing PUFs

Florian Frank, Martin Schmid, Felix Klement, Purushothaman Palani, Andreas Weber, Elif Bilge Kavun, Wenjie Xiong, Tolga Arul, Stefan Katzenbeisser

In this work, a novel FPGA-based data-binding architecture incorporating PUFs and a user-specific encryption key to protect the confidentiality of data on external non-volatile memories is presented. By utilizing an intrinsic PUF derived from the same memory, the confidential data is additionally bound to the device. This feature proves valuable in cases where software is restricted to be executed exclusively on specific hardware or privacy-critical data is not allowed to be decrypted elsewhere. To improve the resistance against hardware attacks, a novel method to randomly select memory cells utilized for PUF measurements is presented. The FPGA-based design presented in this work allows for low latency as well as small area utilization, offers high adaptability to diverse hardware and software platforms, and is accessible from bare-metal programs to full Linux kernels. Moreover, a detailed performance and security evaluation is conducted on five boards. A single read or write operation can be executed in $0.58 \mu\text{s}$ when utilizing the lightweight PRINCE cipher on an AMD Zync 7000 MPSoC. Furthermore, the entire architecture occupies only about 10% of the FPGA's available space on a resource-constrained AMD PYNQ-Z2. Ultimately, the implementation is demonstrated by storing confidential user data on new generations of network base stations equipped with FPGAs.

Full document at <https://doi.org/10.1145/3634737.3656996>