Supply Chain and IoT PUF-based Authentication

Wenjie Che, Goutham Pocklassery, Venkata K. Kajuluri and and Jim Plusquellic
ECE, Univ. of New Mexico
Albuquerque, NM
wjche@unm.edu, gouthamp@unm.edu, jimp@ece.unm.edu

Fareena Saqib
ECE, Florida Institute of Technology
Melbourne, FL
(fsaqib@fit.edu)

This poster demonstrates a privacy-preserving, mutual PUF-based authentication protocol using a set of wirelessly connected devices representing tokens, e.g., chips moving through the supply chain, electronic voting machines, credit cards, etc. A laptop is used to represent the secure server and a router (or handheld wireless transmitter) represents an intermediary between the secure server and wirelessly connected tokens. A Hardware Embedded Delay PUF called HELP is implemented entirely in VHDL on low cost Xilinx FPGAs. HELP communicates with the host system using the Microblaze embedded microcontroller connected to HELP using a register interface on the FPGA and to the secure server using a wireless interface. Authentication will be both privacy-preserving and mutual (2-way), followed by session encryption. Dynamic partial reconfiguration will be used to save resources on the token by replacing the HELP engine with a hardware instantiation of the Advanced Encryption Standard for session encryption.

1. INTRODUCTION

Authentication is the process between a prover, e.g., a hardware token or smart card, and a verifier, a secure server or bank, that confirms the identities, using corroborative evidence, of one or both parties. With the Internet-of-things (IoT), there are a growing number of applications that require low cost authentication. Physical unclonable functions (PUFs) are hardware security and trust primitives that can address issues related to low cost because they can potentially eliminate the need for NVM. Moreover, the special class of so-called 'strong PUFs' can also reduce area and energy overheads by reducing the number and type of cryptographic primitives and operations.

Most proposed PUF architectures require the insertion of a dedicated array of identically-designed test structures and are classified as 'weak PUFs'. Although weak PUFs can be used for authentication, they require cryptographic functions, e.g., secure hash and encryption, to exponentially expand the input/output space of challenge-response-based authentication protocols. A strong PUF, on the other hand, can generate, ideally, an exponential number of challenge-response-pairs (CRPs), and can potentially be configured to allow direct, unprotected access from outside the chip. This is true because it is infeasible for an adversary to apply all 2^n CRPs in an attempt to read-out and store all of the response bitstrings. Strong PUFs with unprotected interfaces, however, must be able to withstand model-building attacks which attempt to machine learn (ML) the relationship among the much smaller number of random circuit elements, from which the 2^n response bits are generated.

The HELP PUF is used as the basis for a novel strong-PUF-based authentication protocol. The entropy source of HELP is based on path delay variations that occur in the structural paths of an on-chip macro. In particular, we use data path components from a hardware implementation of the AES algorithm as the source of delay variations. Fig. 1 provides a illustration of the within-die (WID) delay variations leveraged by HELP using data collected from 500 chip-instances on a Xilinx FPGA. The range of WID is approx. 25 launch-capture-intervals (LCI), with each LCI equal to approx. 18 ps. Therefore, WID for this path is approx. 450 ps. Temperature and supply

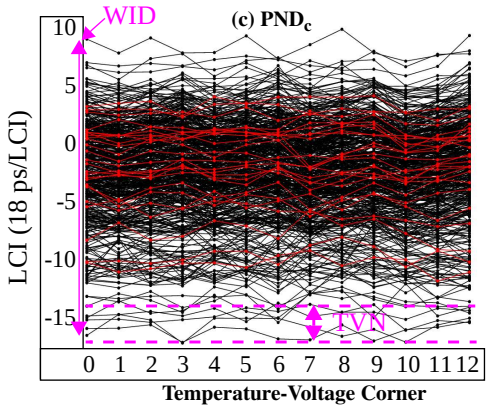

Fig. 1. (a) Within-die variations (WID) temperature-voltage noise (TVN) illustration from data collected from 500 FPGA chip-instances.

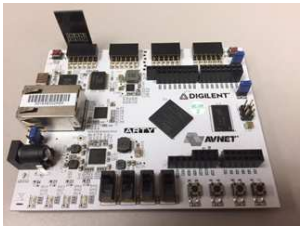

Fig. 2. (a) Xilinx Artix FPGA representing the tokens in the hardware demo.

voltage noise (TVN) is also illustrated, with the x-axis plotting the delays from the same path measured under different corners, ranging from enrollment at 25^{o}C, 1.00V through all combinations of temperatures -40^{o}C to 85^{o}C and voltages 0.95V to 1.05V for regeneration. TVN is approx. 5x smaller than WID.

2. Observeables in Hardware Demonstration

A set of Xilinx Artix FPGAs with wireless interfaces (shown in Fig. 2) will be used as the tokens, while a laptop with attached 'transmitter' (not shown) will be used as a secure server to demonstrate, in real time, the processing of simultaneous authentication requests. A short encryption session will be carried out immediately after mutual authentication. Both authentication and encryption will use bitstrings generated by the HELP PUF. A graphical-user-interface running on the laptop will show the results of authentication and encryption, in real time, reporting runtime specifications including authentication failures and elapsed time.