Key Reconciliation Protocols for Error Correction of Silicon PUF Responses

Abstract:

Physical Unclonable Functions (PUFs) are promising primitives for the lightweight authentication of an integrated circuit (IC). Indeed, by extracting an identifier from random process variations, they allow each instance of a design to be uniquely identified. However, the extracted identifiers are not stable enough to be used as is, and hence need to be corrected first. This is currently achieved using error-correcting codes in secure sketches, that generate helper data through a one-time procedure. As an alternative, we propose key reconciliation protocols. This interactive method, originating from quantum key distribution, allows two entities to correct errors in their respective correlated keys by discussing over a public channel. We believe that this can also be used by a device and a remote server to agree on two different responses to the same challenge from the same PUF obtained at different times. This approach has the advantage of requiring very few logic resources on the device side. The information leakage caused by the key reconciliation process is limited and easily computable. Results of implementation on FPGA targets are presented, showing that it is the most lightweight error-correction module to date.

Existing system

Physical Unclonable Functions (PUFs) have emerged in the last two decades as a root of trust and a way to provide identifiers for integrated circuits (ICs). They rapidly gained attention thanks to their lightweight and tamper-evident nature. Indeed, they usually require only a small area on the device and do not require a dedicated technology process, compared to nonvolatile memory which could be used to store a unique identifier. Two responses obtained at different times from the same PUF using an identical challenge are different. This instability is caused by environmental parameters, aging of the device, PUF architecture, etc. For that reason, PUF responses are not reliable enough to be directly used as cryptographic keys and require error-correction.
Proposed system

We propose to use a key reconciliation protocol instead. This interactive method, proposed and improved, is called the CASCADE protocol. It is the main protocol for key reconciliation in a quantum key distribution context. It allows two parties who exchanged a stream of bits through an insecure and noisy quantum channel to discuss about it publicly and derive a secret key from it. We believe that this protocol can also be used to reconcile two PUF responses obtained from the same challenge but at a different time. The CASCADE protocol mainly consists in interactively exchanging parity values of different blocks of the responses. Therefore, only parity computations need to be carried out on-chip, which requires very few logic resources. This minimal area overhead comes at the cost of heavy communication between the IC and the server. The parity values are then exploited to modify the response bits on the server side, like the reverse fuzzy extractor. When the protocol terminates, it is highly probable that the two parties will own an identical response. These two identical responses could then be further processed to generate a cryptographically strong secret key.

Applications

1) Communications
2) Digital signal processing

Advantages

Area, delay and power reduced

System Configuration:

In the hardware part a normal computer where Xilinx ISE 14.3 software can be easily operated is required, i.e., with a minimum system configuration

HARDWARE REQUIREMENT
Processor - Pentium –III

Speed - 1.1 GHz

RAM - 1 GB (min)

Hard Disk - 40 GB

Floppy Drive - 1.44 MB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

SOFTWARE REQUIREMENTS


- Front End: Modelsim 6.3 for Debugging and Xilinx 14.3 for Synthesis and Hard Ware Implementation

This software’s where Verilog source code can be used for design implementation.