Key Reconciliation Protocols: an Alternative for Lightweight Authentication of Integrated Circuits

Brice Colombier (1), Lilian Bossuet (1),
David Hely (2), Viktor Fischer (1)

(1) Univ. Lyon, UJM-Saint-Etienne, CNRS, Laboratoire Hubert Curien UMR 5516, F-42023, Saint-Etienne, France

(2) Univ. Grenoble Alpes, LCIS, F-26000, Valence, France

Abstract

Physical Unclonable Functions (PUFs) are promising primitives for lightweight authentication. 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, but need to be corrected first. This is currently achieved using error correcting codes, which generate helper data through a one-time process. 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 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 few logic resources on the device side, at least three times fewer than existing error correcting codes. The leakage caused by the key reconciliation process is limited and easily computable. Results of implementation on various FPGA targets are presented.