A Challenge Code for Maximizing the Entropy of PUF Responses

Olivier Rioul[1], Patrick Solé[1],
Sylvain Guilley[1,2] and Jean-Luc Danger[1,2]

[1] LTCI, CNRS, Télécom ParisTech,
Université Paris-Saclay, 75 013 Paris, France.
Email: firstname.lastname@telecom-paristech.fr

[2] Secure-IC S.A.S., 15 Rue Claude Chappe, Bât. B,
ZAC des Champs Blancs, 35510 Cesson-Sévigné, France.
Email: firstname.lastname@secure-ic.com

A physically unclonable function (PUF) is a hardware device that can generate intrinsic responses from challenges (one bit response per challenge). The responses serve as unique identifiers and it is required that they be as little predictable as possible. A loop-PUF [1] is an architecture where n single-bit delay elements are chained.

In this talk, we introduce a *stochastic model* for the loop-PUF using Gaussian random variables and give a closed-form expression of the total entropy of the responses. It is shown that n bits of entropy can be obtained with n challenges if and only if the challenges constitute a Hadamard code.

Furthermore, contrary to a previous belief, it is shown that adding more challenges results in an entropy strictly greater than n bits. A greedy code construction is provided for this purpose. When n is a power of two, heuristic results indicate the challenge code is constituted of additional challenges from several nonorthogonal Hadamard matrices. A challenging problem is to find a tight upper bound on the generated entropy.

This is an preliminary presentation of a work to be presented at ISIT 2016, in July 10-15 at Barcelona, Spain.

References

[1] Zouha Cherif, Jean-Luc Danger, Sylvain Guilley, and Lilian Bossuet. An easy-to-design PUF based on a single oscillator: The loop PUF. In *15th Euromicro Conference on Digital System Design, DSD 2012, Çeşme, Izmir, Turkey, September 5-8, 2012*, pages 156–162. IEEE Computer Society, 2012.