Secure authentication and communication for embedded systems using a PUF/TRNG combined circuit

S. Buchovecká, R. Lórencz, J. Buček, F. Kodýtek
Czech Technical University of Prague
Czech Republic

Abstract

In our contribution we would like to present the protocol for simple authentication and encryption for embedded systems using a PUF/TRNG combined circuit. The goal is to show the possibilities of securing communication and authentication of the embedded systems, using PUF and TRNG for secure key generation, without requirement to store secrets on the device itself, thus allowing to significantly simplify the problem of key management and key establishment for symmetric and asymmetric cryptography. The proposed solution enables implementation on resource-limited hardware devices such as remote controlled sensors connected in a networks. A case study using a ring oscillator-based combined PUF/TRNG circuit is presented.

Keywords - TRNG, PUF, Key Generation, Key Management, Embedded Systems Security