SRAM-PUF Based on Selective Power-Up and Non-Destructive Scheme

Mohd Syafiq Mispan, Basel Halak, Mark Zwolinski
Electronics and Computer Science, University of Southampton, United Kingdom

Abstract. Research in hardware security, particularly on Physical Unclonable Functions (PUF) has attracted a lot of attention in recent years. PUFs provide primitives for implementing encryption/decryption and device fingerprinting. Though a wide range of solutions exists for PUF-based CMOS devices, the most investigated solutions today for weak PUF implementation are based on the use of random start-up values of SRAM, which offers the advantage of reusing memories that already exist in many designs. However, the start-up value availability is compromised during memory write access which causes a limitation in using SRAM as both memory and PUF. Although using a dedicated SRAM as PUF could overcome the problem, it comes with high extra overhead. In this work, we propose a new scheme called ‘selective power-up and non-destructive’ scheme to enable SRAM as memory and PUF. A case study of generating a 128-bit key shows that the area overhead of proposed scheme is approximately 12.5_ smaller than for a dedicated SRAM-PUF