Design of Lightweight Buffer-free SRAM and Robust Ring Oscillator Based Physical Unclonable Functions

Abstract

Physical unclonable function (PUF) is an emerging security primitive to address vulnerability of the traditional data protection scheme that stores the secret keys in non-volatile memories. Static Random Access Memory (SRAM) and Ring Oscillator (RO) are two popular candidates to be designed as PUFs.

The most compelling issue in designing a good SRAM-based PUF (SPUF) is to maximize the mismatches between the transistors in the cross-coupled inverters but doing so will increase the memory read-write failures. For this reason, the memory cells of existing SPUFs cannot be reused as storage elements, which increases the overheads of cryptographic system where long signatures and high-density storage are both required. The traditional SPUF also has some other issues. First, it has limited entropy of only one response bit per cell. Second, as power-up reset has a global effect, extra storage is needed to temporarily buffer the original SRAM content before switching to PUF mode. This process has introduced extra area-power overhead as well as potential security leakage. The responses of RO-based PUF has the susceptibility issue to changes in operating conditions and device aging. Current solutions either incur large hardware overhead or require sophisticated RO selection algorithms to increase its reliability.

This report presents the solutions to the above problems with SRAM and RO PUFs. A novel design methodology to optimize an SRAM cell for dual application modes has been proposed and the design conflicts are resolved. The emerging dual-port (DP) SRAM cell offers attractive multiple access capability for low-power and high-speed memory transfer. By levering the forbidden contention state in one of its four multiple access modes, a new DP-SRAM based PUF is proposed to generate two independent response bits per cell and limit data buffering to only those cell content addressed by the challenge. The optimal biasing of current starved (CS) inverter is exploited for the design of RO PUF with very high reliability against both temperature and voltage variations. With two additional transistors, the CS inverter can be adaptively biased at idle time and in active mode to significantly reduce the overall stress, making the proposed CS RO PUF robust against both environmental condition variations and aging. Without using error correction code, the reliability is further improved by a low-cost proximity detector circuit with a small sacrifice on CRP space. The correlation between successive RO pairs of different input challenges is also broken by an irregular clocking of the linear feedback shift register used to encipher the input challenges.