DESIGN OF RING OSCILLATOR BASED PUF WITH ENHANCED CHALLENGE RESPONSE SET AND ERROR CORRECTING CAPABILITY

Suchismita Batabyal; A A Bazil Raj*
Electronics Engineering, Defence Institute of Advanced Technology,
Pune, India-411025
suchi_mee18@diat.ac.in; brazilraj.a@diat.ac.in
* Corresponding author

Abstract: Modern cryptographic protocols are based on the premise that only authorized persons can obtain secret keys and access to information systems. However, various kinds of tampering methods exist that can extract secret keys from conditional access systems such as smart cards and ATM's. In today's world hardware security is of utmost importance and hence new methods have to be devised to make them more resistant to invasive attacks. A physical unclonable function (PUF) is a promising solution to many security issues due to its ability to generate a die unique identifier that can resist cloning attempts as well as physical tampering. PUF's make use of the measurable intrinsic randomness of physical systems to establish signature for those systems. A PUF is like a fingerprint for a particular physical object, it is based on many manufacturing variabilities that occur during IC fabrication or the propagation delays that are present in the wires and interconnects. The main advantage of PUF's is that no extra circuit is needed to be added as it can be generated from the IC itself. Various kind of PUF structures exist such as SRAM based PUF'S, which is based on the variability of the power ON value when the SRAM is first switched ON that is we do not know what value was previously stored either a '0' or a '1' in the feedback path. A delay based ring oscillator PUF is another structure that is a special challenge response entity, embedded in a physical device and are used as hardware primitives in the field of hardware oriented security. These challenge response pairs are unclonable, unpredictable, and permanent for each hardware. These delay based PUF design exploits the characteristics of silicon IC manufacturing process variations which caused random delay characteristics in wires and transistors that differ from chip to chip. In this paper we propose a new ring oscillator based PUF with enhanced challenge response set and better error correcting capability.

keywords: physical unclonable function (PUF), fingerprint, die unique identifier, manufacturing variability, ring oscillator, hardware oriented security, challenge response pair, error correcting capability