PUFs for hardware security

Sanu Mathew, Intel

Physically Unclonable Functions (PUFs) are root-of-trust circuit primitives that serve as the bedrock of security and confidentiality in modern computing platforms. PUFs raise the security bar vis-à-vis programmable fuses by generating volatile, tamper-proof IDs and encryption keys without requiring manual intervention by the manufacturer. PUFs harness the inherent static entropy of manufacturing variations to generate a static digital value that is repeatable and reliable in the presence of voltage/temperature variations and aging-induced process drift over die lifetimes. This short course gives an overview of the two broad categories of PUFs: (i) Weak PUFs used to produce device-unique keys/IDs (ii) Strong PUFs used for secure authentication using a device-unique challenge-response pairing. The course will also review the essential features required to qualify PUFs for reliable field operation. The various malicious attack mechanisms used to disrupt PUF operation will also be discussed.

Sanu Mathew is a Senior Principal Engineer with Circuits Research Lab, Intel Corporation, Hillsboro, Oregon, where he heads the Security Arithmetic Circuits Research group, responsible for developing arithmetic circuits and hardware accelerators for cryptography and security. He received a Ph.D. degree in electrical and computer engineering from the State University of New York at Buffalo in 1999. He received two Intel Achievement Awards for pioneering energy-efficient core datapaths circuits and developing AES-NI hardware for Intel products. He holds 110 issued/pending patents, has published 86 conference/journal articles and authored two book chapters. Sanu mentors Intel- and SRC-funded university research and has served on program committees of ARITH, ISLPED, DAC, SOCC conferences. He currently serves on the technical program committee at International Solid-State Circuits Committee (ISSCC). Sanu is a Fellow of the IEEE.