2023 International Conference on IC Design and Technology (ICICDT) | 979-8-3503-1931-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICICDT59917.2023.10332396

Invited Talk #5

Challenges in generating true random numbers considering the variety of corners, aging, and attacks

Sylvain Guilley
Secure-IC, France

***Abstract*—** True Random Number Generators (TRNGs) are sensitive Intellectual Property blocks involved in the creation of cryptographic keys, initialization vectors, nonces, etc. They must behave within a large environmental spectrum, including multiple corners, chip properties change owing to aging, and intentional attacks aiming at lowering the TRNGs entropy. We review normative and technical landscape in this respect, and propose a pre-silicon verification methodology to assess TRNGs resilience.

Biography

Dr. Sylvain Guilley (Member, IEEE) has been organized the PROOFS workshop, which brings together researchers whose objective is to increase the trust in the security of embedded systems, since 2012. He is currently the General Manager and the CTO with Secure-IC, a French company offering security for embedded systems. Secure-IC's flagship product is the multi-certified SECURYZR integrated Secure Element (iSE). He is also a Professor with TELECOM Paris, a Research Associate with École Normale Supérieure (ENS), and an Adjunct Professor with the Chinese Academy of Sciences (CAS), Beijing. His research interests are trusted computing, cyber-physical security, secure prototyping in FPGA and ASIC, and formal/mathematical methods. He is also a Lead Editor of international standards, such as ISO/IEC 20897 (Physically Unclonable Functions), ISO/IEC 20085 (Calibration of non-invasive testing tools), and ISO/IEC 24485 (White Box Cryptography). He is a High Level Principles for Design/Architecture Team Leader of the drafting of Singapore TR68 standard on Cyber-Security of Autonomous Vehicles. He is also an Associate Editor of the Journal of Cryptography Engineering (JCEN) (Springer). He has coauthored more than 250 research articles and filed more than 40 invention patents. He is member of the IACR and a Senior Member of the CryptArchi club. He is an alumnus from École Polytechnique and TELECOM-Paris.