Symmetric Key Cryptographic Primitives Based on Pseudo-Randomness, Randomness and Dedicated Coding

Miodrag Mihaljevic

Power of Randomness for High Security and Low Implementation Complexity

Goal: Design of Cryptographic Primitives with Enhanced Security and Low Implementation Complexity

- Encryption - Compact Stream Ciphers
- Authentication Protocols for RFID and related applications

Design Components:
- Simple Finite State Machine for the Pseudo-Randomness
- Dedicated Coding: Linear Homophonic and Error-Correction
- Randomness

Effects:
- Enhanced Security Implied by Randomness
- Low Implementation Complexity

References:


