Fine-tuning the Advanced Encryption Standard (AES)

Behnam Rahnama, Atilla Elci, Ibukun Eweoya

Fifth International Conference on Security of Information and Networks (SIN 2012)

The Advanced Encryption Standard has been playing a prominent role in embedded systems security for a decade after being announced by the National Institute of Standards and Technology (NIST). However, vulnerabilities have emerged, especially timing attacks, that challenges its security. This paper demonstrates the introduction of a unique diffusion and confusion scheme in Rijndael by incorporating ASCII codes manipulations using playfair ciphering into the algorithm; it is not dependent on the key and input thereby making it a constant time module in AES algorithm. The concept counters possible leakages from the S-box lookups; intermediary operations (SubstituteByte, ShiftRows, MixColumns, AddRoundKey) of the AES are still applicable but it becomes impossible for cryptanalysis discovery of enciphering method and ciphertext bits. Success of cracking efforts will be beyond human patience as it avoids statistical precision, thereby curbing timing attacks.