Energizing the Advanced Encryption Standard (AES) for Better Performance

Arif Sari[1], Behnam Rahnama[2], Ibukun Eweoya[3], Zafer Agdelen[4]

[1, 4]Girne American University, Turkey, arifsari@gau.edu.tr,zagdelen@gau.edu.tr

[2]Scale DB. Inc. Silicon Valley, USA, behnam.rahnama@gmail.com

[3]Covenant University, Nigeria, ibukun.eweoya@covenantuniversity.edu.ng

Abstract— *Security is a never ending challenge. The security researchers must be steps ahead to avoid attacks and threats, thereby keeping businesses running and avoiding calamities. The Advanced Encryption Standard (AES) is to this rescue after its official acceptance and recommendation by National Institute of Standards and Technology (NIST) in 2001. However, timing attacks have called for a modification to it to retain its potency and effectiveness. This research boosts the Rijndael by incorporating an invented playfair ciphering into the algorithm using 256 ASCII codes. The concept counters possible leakages from the S-box lookups from the cache. The research introduces mixcolumn in the last round against the standard to make it a constant time algorithm. The encryption and decryption were validated. Previous researches implemented Architectural and operating system modifications, placing all the lookup tables in CPU registers, Parallel Field Programmable Gate Array (FPGA) implementation , Application Specific Integrated Circuits (ASIC) implementation, the Dynamic Cache Flushing Algorithm but none keeps AES assets of good speed and memory conservation; most especially in embedded systems.*