Contribution ID: **136** Type: **Oral**

Enhancing DES Architecture by Replacing XOR with NAND in the Feistel Network

The Data Encryption Standard (DES) has historically been a fundamental symmetric-key cryptographic algorithm, distinguished by its sixteen-round Feistel network that combines substitution via S-boxes, permutation by P-boxes, and a mixing function rooted in bitwise XOR operations, delivering a balance of operational efficiency and security suitable for its time. However, the fixed 56-bit key length and advances in computational power have exposed DES's vulnerability to brute-force attacks, pressing the need for alternative approaches to enhance or rethink its core mechanisms. This research introduces a novel adaptation to the DES framework by replacing the traditional XOR operation in the Feistel round function with the NAND logical gate, a universal gate known for its functional completeness and inherent non-linearity. By embedding NAND into the mixing stage, the design aims to infuse stronger non-linear transformations into the encryption process while preserving the established structure of key scheduling, expansion, S-box substitution, and permutation layers. The modified algorithm retains the fundamental Feistel symmetry and operates over sixteen rounds where the right half of the plaintext undergoes expansion, subkey mixing via NAND, substitution, permutation, and subsequent NAND-based combination with the left half. This substitution introduces a distinctly different bitwise transformation compared to standard DES, resulting in ciphertext outputs that markedly deviate from traditional patterns and thereby potentially augmenting resistance to certain cryptanalytic attacks, including linear and differential methods. Experimentally, the system demonstrates consistent and reversible encryption-decryption cycles for fixed plaintext-key pairs, substantiating the feasibility of NAND as a viable alternative logical operator within the Feistel context. Moreover, the use of NAND is particularly promising for lightweight cryptographic applications, especially in hardware-constrained environments such as Internet of Things (IoT) devices, given NAND gates' efficiency and dominance in digital circuit design. Nonetheless, the transition from XOR to NAND alters diffusion properties and error propagation dynamics, necessitating thorough cryptanalytic evaluation to assess possible vulnerabilities, biases, or novel strength characteristics introduced by this logical shift. This study thus underscores the adaptability of classical cryptographic frameworks to alternative algebraic primitives, encourages broader exploration of logical operations in cipher construction, and lays groundwork for future development of hardware-optimized, secure encryption systems that balance practical efficiency with cryptographic robustness.

Keywords: Data Encryption Standard (DES), symmetric-key cryptography, Feistel network, NAND gate, logical mixing, XOR replacement, block cipher, S-box, lightweight cryptography, encryption-decryption cycle, cryptanalysis, IoT security, hardware-efficient cryptography.

Author: AJAI, Alwin (JAIN (Deemed-to-be University))

Co-author: Mr NATARAJAN, VISHNU VENKATESH (JAIN (Deemed-to-be University))

Presenter: AJAI, Alwin (JAIN (Deemed-to-be University))

Track Classification: Forensic Sciences