

Hybrid Bio-Digital Cryptosystem: Simulation and Analysis of DNA-XOR Encryption Algorithm

Luka Khanjaladze, Ilia Makharadze, Saba Sidamonidze

luka.khanjaladze233@ens.tsu.edu.ge

Department of Computer Science, Faculty of Exact and Natural Sciences, Tbilisi State University, 11 University St., Tbilisi.

As the era of quantum computing approaches, traditional cryptographic standards such as RSA and AES face real threats of obsolescence and breach, as they rely on mathematical problems that quantum algorithms can easily solve. This project presents the development and simulation of a "Hybrid Bio-Digital Cryptosystem" that utilizes a DNA-XOR architecture to achieve post-quantum security. The primary challenge discussed in this paper is the vulnerability of existing DNA encoding methods. Early approaches relied on simple substitution (for example, mapping binary 00 to Adenine), which preserves the statistical patterns of the plaintext and leaves the system vulnerable to frequency analysis. To solve this problem, a multi-stage encryption algorithm is proposed that combines the speed of digital logic with the complexity of molecular biology. The presented method uses a chaotic private key to perform a Boolean "DNA-XOR" operation, followed by biological manipulation techniques: strand complementation and sequence reversal. The project includes the creation of a software simulation for logic validation and security auditing. Expected results demonstrate that this hybrid approach creates a "Cipher-DNA" that is chemically stable yet statistically indistinguishable from biological "noise" (random sequences). By erasing digital traces within a biological environment, the system achieves "information-theoretic security," rendering it impenetrable to brute-force attacks and modern cryptanalysis.