ABSTRACT

This study discusses the implementation of the NTRU algorithm with compressed parameters using a hybrid Number Theoretic Transform (NTT)–Karatsuba approach in the polynomial multiplication process. The purpose of this research is to evaluate the performance impact of parameter modification on the computational speed of key generation, encryption, and decryption processes, without reducing the algorithm's security level, which is standardized at 128-bit. The implementation was carried out using compressed parameter sets of $n = 1024, q = 83969$ *and* $n = 2048, q = 166657$*. The experimental results indicate that the compressed parameters are capable of maintaining, and even slightly enhancing, the security level beyond 128-bit. Furthermore, parameter compression effectively reduces the key size from 3.75 Kb to 2.1 Kb, and the ciphertext size from 3,840 B to 2,176 B. Bandwidth utilization measurements also show a significant reduction—from 3.072 Kb/s to 1.741 Kb/s for parameters* $n = 1024, q = 83969$*, and from 11.878 Kb/s to 3.686 Kb/s for parameters* $n = 2048, q = 166657$*. In terms of computational performance, the hybrid approach achieved a key generation time of 0.000372 s, encryption time of 0.006684 s, and decryption time of 0.005858 s for parameters* $n = 1024, q = 83969$*. Meanwhile, for parameters* $n = 2048, q = 166657$*, the key generation, encryption, and decryption times were 0.000975 s, 0.020263 s, and 0.017821 s, respectively. However, a decryption failure occurred at* $n = 2048, q = 166657$*, resulting in the ciphertext being unable to be restored to its original plaintext form.*

Keywords: *Hybrid, Karatsuba, NTRU, Number Theoretic Transform, Polynomial.*

ABSTRAK

Penelitian ini membahas penerapan algoritma NTRU dengan parameter hasil kompresi menggunakan pendekatan hibrid Number Theoretic Transform (NTT)–Karatsuba dalam proses perkalian polinomial. Tujuan dari penelitian ini adalah untuk mengukur performa perubahan nilai parameter terhadap kecepatan waktu pembangkitan kunci (*key generation*), enkripsi, dan dekripsi, tanpa mengurangi tingkat keamanan algoritma yang berada pada standar 128-bit. Implementasi dilakukan dengan menggunakan parameter hasil kompresi, yaitu $n = 1024, q = 83969$dan $n = 2048, q = 166657$. Hasil pengujian menunjukkan bahwa penggunaan parameter hasil kompresi mampu mempertahankan bahkan sedikit meningkatkan tingkat keamanan algoritma di atas 128-bit. Selain itu, kompresi parameter terbukti dapat menurunkan ukuran kunci dari semula 3,75 Kb menjadi 2,1Kb, serta mengurangi ukuran *ciphertext* dari 3.840B menjadi 2.176B. Pengukuran terhadap penggunaan bandwidth juga menunjukkan penurunan yang signifikan, yaitu dari 3,072Kb/s menjadi 1,741Kb/s untuk parameter $n = 1024, q = 83969$, dan dari 11,878Kb/s menjadi 3,686Kb/s untuk parameter $n = 2048, q = 166657$. Dari sisi performa waktu komputasi, pendekatan yang digunakan menghasilkan waktu key generation sebesar 0,000372 s, enkripsi sebesar 0,006684 s, dan dekripsi sebesar 0,005858 s pada parameter $n = 1024, q = 83969$. Sementara itu, pada parameter $n = 2048, q = 166657$diperoleh waktu key generation sebesar 0,000975s, enkripsi sebesar 0,020263s, dan dekripsi sebesar 0,017821s. Namun demikian, pada parameter $n = 2048, q = 166657$ditemukan kegagalan proses dekripsi yang menyebabkan *ciphertext* tidak dapat dikembalikan menjadi *plaintext* semula.

Kata Kunci: Hibrid, Karatsuba, NTRU, Number Theoretic Transform, Polinomial.