INTISARI

CRYSTALS-KYBER SEBAGAI ALGORITMA POST-QUANTUM CRYPTOGRAPHY PADA APLIKASI MOBILE

Chrissandy Sapulete
22/502093/06414

Dalam era digital yang terus berkembang, efisiensi aplikasi pesan instan memegang peranan krusial dalam komunikasi sehari-hari. Kemajuan teknologi komputasi kuantum menimbulkan ancaman terhadap keamanan kriptografi klasik, memicu kebutuhan akan algoritma kriptografi yang tahan terhadap serangan kuantum. Dalam menanggapi hal tersebut *National Institute of Standards and Technology* (NIST) mengembangkan standar kriptografi melalui kompetisi *Post-Quantum Cryptography* (PQC) dengan algoritma CRYSTALS-Kyber sebagai pemenang. Penelitian ini berfokus pada implementasi dan pengujian kinerja waktu pembangkit kunci, *Key Encapsulation Mechanism* (KEM), enkripsi, dan dekripsi dari algoritma PQC, khususnya N^{th} *Degree Truncated Polynomial Ring Units* (NTRU) dan CRYSTALS-Kyber (Kyber512, Kyber768, dan Kyber1024), dalam aplikasi pesan instan pada perangkat mobile. Hasil penelitian menunjukkan bahwa Kyber768 menghasilkan kinerja terbaik dalam hal waktu operasional keseluruhan, dengan waktu rata-rata 67.34×10^{-4} detik, secara signifikan lebih efisien dibandingkan dengan NTRU yang menghasilkan waktu rata-rata 419.27×10^{-4} detik. Penelitian ini memberi pengetahuan mengenai algoritma CRYSTALS-Kyber, yang relatif baru dalam dunia kriptografi, dan merekomendasikan penggunaan algoritma CRYSTALS-Kyber varian Kyber768 sebagai pilihan yang efisien untuk diterapkan dalam aplikasi pesan instan pada perangkat mobile.

Kata Kunci: *Post-Quantum Cryptography,* Aplikasi Pesan Instan, Perangkat Mobile, NTRU, CRYSTALS-Kyber.

ABSTRACK

CRYSTALS-KYBER AS A POST-QUANTUM CRYPTOGRAPHY ALGORITHM IN MOBILE APPLICATIONS

Chrissandy Sapulete
22/502093/06414

In the ever-growing digital era, the efficiency of instant messaging applications plays a crucial role in daily communication. Advances in quantum computing technology pose a threat to the security of classical cryptography, triggering the need for cryptographic algorithms that are resistant to quantum attacks. In response to this, the National Institute of Standards and Technology (NIST) developed cryptographic standards through the Post-Quantum Cryptography (PQC) competition, with the CRYSTALS-Kyber algorithm as the winner. This research focuses on implementing and testing the time performance of key generation, Key Encapsulation Mechanism (KEM), encryption, and decryption of PQC algorithms, especially N^{th} *Degree Truncated Polynomial Ring Units* (NTRU) and CRYSTALS-Kyber (Kyber512, Kyber768, and Kyber1024), in instant messaging applications on mobile devices. The results showed that Kyber768 produced the best performance in terms of overall operational time, with an average time of 67.34×10^{-4} seconds, significantly more efficient compared to NTRU, which produced an average time of 419.27×10^{-4} seconds. This research provides knowledge about the CRYSTALS-Kyber algorithm, which is relatively new in the world of cryptography, and recommends the use of the Kyber768 variant of the CRYSTALS-Kyber algorithm as an efficient choice for implementation in instant messaging applications on mobile devices.

Keywords: Post-Quantum Cryptography, Instant Messaging Applications, Mobile Devices, NTRU, CRYSTALS-Kyber.