Algebraic Cryptanalysis pada Algoritma NTRU-HPS dan NTRU-HRSS = Algebraic Cryptanalysis on NTRU-HPS and NTRU-HRSS

Fadila Paradise, author

Abstrak

NTRU adalah sebuah lattice-based public key cryptosystem yang didesain oleh Hoffstein, Pipher, dan Silverman pada tahun 1996. NTRU dipublikasikan pada Algorithmic Number Theory Symposium (ANTS) pada tahun 1998. Pada tahun 2008 NTRU ANTS'98 ditetapkan sebagai standar dalam IEEE untuk teknik public key cryptography berbasis hard problem pada lattice. NTRU kemudian dikembangkan kembali oleh NTRU Inc. sejak tahun 2018 dan menjadi salah satu finalis pada round 3 kompetisi pemilihan standar post-quantum cryptography yang diselenggarakan oleh NIST pada tahun 2020. Secara umum terdapat 2 jenis algoritma yang diajukan oleh NTRU dalam proses seleksi round 3 jika diklasifikasikan berdasarkan penentuan parameternya, yaitu NTRU-HPS (Hoffstein, Pipher, Silverman) dan NTRU-HRSS (Hulsing, Rijnveld, Schanck, Schwabe). Percobaan algebraic cryptanalysis terhadap NTRU ANTS'98 sudah pernah dilakukan pada tahun 2009 dan 2012.

Dalam penelitian ini, dilakukan algebraic cryptanalysis terhadap NTRU-HPS dengan, (ntruhps2048509) serta NTRU-HRSS dengan (ntruhrss701). Tujuan dari penelitian ini adalah untuk mengevaluasi ketahanan algoritma NTRU-HPS dan NTRU-HRSS terhadap algebraic cryptanalysis dengan melakukan rekronstruksi nilai private key. Dari hasil penelitian didapatkan bahwa NTRU-HPS dan NTRU-HRSS tahan terhadap algebraic cryptanalysis.
.....NTRU is a lattice-based public-key cryptosystem designed by Hoffstein, Pipher, and Silverman in 1996. NTRU published on Algorithmic Number Theory Symposium (ANTS) in 1998. The ANTS'98 NTRU became the IEEE standard for public key cryptographic techniques based on hard problems over lattices in 2008. NTRU was later redeveloped by NTRU Inc. since 2018 and became one of the finalists in round 3 of the PQC (Post-Quantum Cryptography) standardization process organized by NIST in 2020. There are two types of NTRU algorithms proposed by NTRU Inc., which are classified based on parameter determination, NTRU-HPS (Hoffstein, Pipher, Silverman) and NTRU-HRSS (Hulsing, Rijnveld, Schanck, Schwabe). Algebraic cryptanalysis on ANTS'98 NTRU had previously been carried out in 2009 and 2012.

In this paper, algebraic cryptanalysis is performed on NTRU-HPS with, (ntruhps2048509) and NTRU-HRSS with (ntruhrss701). This study aims to evaluate the resistance of NTRU-HPS and NTRU-HRSS algorithms against algebraic cryptanalysis by reconstructing the private key value. As a result, NTRU-HPS and NTRU-HRSS are resistant to algebraic cryptanalysis.