INTISARI

Kriptografi Berdasar Multivariat:

Skema Tanda Tangan Digital

***Hidden Product of Polynomial Composition* (HPPC)**

Oleh

Saifullah Ali

22/495968/PPA/06323

Skema tanda tangan digital *Hidden Product of Polynomial Composition* (HPPC) merupakan salah satu partisipan pada kompetisi *post-quantum cryptography* yang diselenggarakan oleh NIST sejak tahun 2023 dengan fokus pada pencarian skema tanda tangan digital yang pendek, efisien dan aman. Skema tanda tangan digital yang diusulkan pada kompetisi ini perlu ditinjau oleh publik terhadap teori ataupun praktik. Pada penelitian ini, dilakukan tinjauan teori terhadap teori-teori aljabar yang mendasari skema HPPC dengan kajian pustaka dan pemaparan mendetail skema HPPC. Skema HPPC merupakan skema yang didasari oleh pintu jebakan HFE dengan memanfaatkan repreresentasi matriks sehingga kunci public berupa matriks di berukuran $n \times n^2$ atas $\mathbb{F}_q$. Skema HPPC memberikan cara konstruksi pemetaan pusat HFE menggunakan dua polinomial dilinearisasi dengan menghitung produk dari komposisi polinomial. Pada penelitian ini, skema HPPC juga diaplikasikan untuk enkripsi.

Skema HPPC memanfaatkan permasalahan multivariat kuadrat untuk keamanannya. Walaupun demikian, penggunaan representasi matriks dan pembentukan pemetaan pusat pada HPPC memberikan kemudahan dalam menghitung pintu jebakan HFE. Skema tanda tangan digital HPPC merupakan skema dengan teori aljabar yang kuat dan bervariasi tetapi mudah dihitung. Namun, skema HPPC tidak direkomendasikan untuk skema enkripsi karena tidak ada jaminan ketunggalan akar suatu polinomial univariat.

ABSTRACT

Multivariate-based Cryptography:

Digital Signature Scheme

Hidden Product of Polynomial Composition (HPPC)

By

Saifullah Ali

22/495968/PPA/06323

The Hidden Product of Polynomial Composition (HPPC) digital signature scheme is one of the participants in the post-quantum cryptography competition organized by NIST since 2023 to find digital signature schemes that are short, efficient, and secure. The digital signature schemes proposed in the competition must be reviewed by the public in theory and application. In this research, we conduct a theoretical review of the algebraic theories underlying the HPPC scheme with a literature review and a detailed study of the HPPC scheme. The HPPC scheme is based on the HFE trapdoor by utilizing a matrix representation of size $n \times n^2$ over $\mathbb{F}_q$. The HPPC scheme provides a way of constructing the HFE center map using two linearized polynomials by computing its product and composition. In this research, we also applied the HPPC scheme for encryption.

The HPPC Scheme is based on a quadratic multivariate problem. However, the use of matrix representation and the way of constructing a center map makes the HFE trapdoor calculate easily. The HPPC scheme has strong and varied algebraic theory but keeps it easy to compute. However, the applications of the HPPC scheme for encryption are not recommended because the uniqueness of the root for a univariate polynomial is not guaranteed.