عنوان مقاله:

A Provably Secure Variant of ETRU Based on Extended Ideal Lattices Over Direct Product of Dedekind Domains

محل انتشار:

مجله محاسبات و امنیت, دوره 5, شماره 1 (سال: 1397)

تعداد صفحات اصل مقاله: 22

نویسندگان:

.Reza Ebrahimi Atani - *Department of Computer Engineering, University of Guilan, P. O. Box ۳۷۵۶, Rasht, Iran*

.Shahabaddin Ebrahimi Atani - *Department of Mathematics, University of Guilan, P. O. Box ۱۹۱۴, Rasht, Iran*

.Amir Hassani Karbasi - *Department of Mathematics, University of Guilan, P. O. Box ۱۹۱۴, Rasht, Iran*

خلاصه مقاله:

Jarvis and Nevins presented ETRU in 2013 which has applausive performance with moderate key-sizes and conjectured resistance to quantum computers. ETRU, as an efficient NTRUEncrypt-like cryptosystem, is over the ring of Eisenstein integers that is faster with smaller keys for the same or better level of security than does NTRUEncrypt which is a desirable alternative to public-key cryptosystems based on factorisation and discrete logarithm problem. However, because of its construction, doubts have regularly arisen on its security. In this paper, we propose how to modify ETRU to make it provably secure, under our modified assumption of quantum hardness of standard worst-case lattice problems, restricted to extended ideal lattices related to some extensions of cyclotomic fields structures. We describe the structure of all generated polynomial rings of quotient over direct product of Dedekind domains Z and Z[ζ3], where ζ3 is complex cube root of unity. We give a detailed description to show that if the private key polynomials of the ETRU are selected from direct product of some Dedekind domains using discrete Gaussians, then the public key, which is their ratio, is statistically indistinguishable from uniform over its range. The security then .proves for our main system from the already proven hardness of the R-SIS and R-LWE problems by their extensions

کلمات کلیدی:

Lattice-Based Cryptography, ETRU, Ideal Lattices, Dedekind Domains, Provable Security

لینک ثابت مقاله در پایگاه سیویلیکا: