عنوان مقاله:

Security and Speed Improvement of GGH based on polynomial rings, quaternion algebra and Gaussian method

محل انتشار:

دومین کنفرانس ملی ایده های نو در مهندسی برق (سال: 1392)

تعداد صفحات اصل مقاله: 8

نویسندگان:

,Massoud Sokouti - *Faculty of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran*

,Ali Zakerolhosseini - *Faculty of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran*

Babak Sokouti - *Biotechnology Research Center Tabriz University of Medical Sciences, Tabriz, Iran*

خلاصه مقاله:

We propose a probabilistic and multi-dimensional public key cryptosystem based on the GGH public key cryptosystem using polynomial rings and quaternion algebra.The new method encrypts four data vectors in each encryption session using quaternion algebraic structure and polynomialrings. The new method is faster than GGH in producing publickey but it is slow in encryption and decryption since it uses quaternion algebraic structure and polynomial rings. The newmethod strengths the GGH cryptosystem while using quaternion algebraic structure. Quaternion algebra is a non-commutativealgebra and it makes this cipher much more resistant to some lattice based attacks. For key generation in Quaternion GGHwe need sixteen multiplications which makes its calculationsslow. By using Gaussian and Brent equations we reduce the number of multiplications into twelve . For this reason we willuse Multiplicative Complexity for optimizing algebraic computations in non-commutative rings. As a result, the efficiency of Quaternion GGH has been increased and calculated in less time

کلمات کلیدی:

GGH, Polynomial rings, Public key cryptography, Lattice attacks, Encryption, Quaternion algebra, Gaussian