II Encuentro Matemático del Caribe

Universidad Tecnológica de Bolívar & Universidad del Sinú Seccional Cartagena

Septiembre 09 - 12, 2020, Cartagena de Indias - Colombia

New Trapdoor Functions for Public Key Cryptohraphy

Tipo: (ponencia)

Autores: Moises Delgado *

Resumen

Trapdoor functions over finite fields are the security components of multivariate cryptographic systems for public key cryptography (PKC). PKC systems use two keys, a public key and a private key. A public key used for encryption while the private key is used for decryption. It is almost impossible the decryption without knowing the private key. Public key systems are fundamental security ingredients in modern electronic communications and data storage. Current PKC systems, based on number theory principles, could be obsolete provided the emergence of quantum computers and quantum attacks. In this talk we propose new candidates for trapdoor functions of high degree for PKC. This high degree promises high resistance against algebraic attacks because of the difficulty for solving a system of multivariate polynomial equations.

Palabras & frases claves: .

Trapdoor function, public key cryptography, quantum cryptography, algebraic attacks, Matsumoto-Imai system, Hidden Field Equation system.

1. Introducción

Current cryptographic algorithms for information security are becoming unsafe the last years because of the growing computer technology, the increasing number of hackers, and the multiple types of attacks. Trapdoor functions over

*Universidad de Puerto Rico en Cayey, e-mail: moises.delgado@upr.edu

Finite Fields are functions that are easy to evaluate but very hard to invert, then promises multiple applications digital communications systems, in particular in public key cryptography (PKC). The most principal cryptographic algorithm in PKC is the well-known RSA algorithm. As it is well known, RSA security is based on the difficulty of factoring very large prime numbers and some results of number theory. This algorithm will be probably obsolete with the new coming age of quantum computing as showed by Peter Shor. So, it is extremely important to start testing new designs and new algorithms for safer cryptographic systems. In this talk, by using almost permutations, we will design new high degree trapdoor functions over finite fields of characteristic two with high resistance against algebraic attacks. Current systems are based in classical Matsumoto-Imai and Hidden Field Equation systems which use quadratic degrees trapdoor functions, so they are sensitive to these attacks.

Referencias

[1] Ding, J., Gower, J. E., Schmidt, D. S. (2006). Multivariate public key cryptosystems (Vol. 25). Springer Science Business Media.

[2] Ding, J., Yang, B. Y. (2009). Multivariate public key cryptography. In Post-quantum cryptography (pp. 193-241). Springer, Berlin, Heidelberg.