Cryptology ePrint Archive: Report 2011/690

A New Class of Multivariate Public Key Cryptosystem Constructed on the Basis of Message-Dependent Transformation

Masao KASAHARA

Abstract: In this paper, a new class of Public-Key Cryptosystem(PKC) based on Random Simultaneous Equation of degree g (RSE(g)PKC) is presented. The proposed scheme uses a new class of trap-doors based on two classes of transformation, i.e. random transformation and message-dependent random transformation. For constructing the proposed scheme,random transformations X and Ψ are used. The transformation Ψ would yield a breakthrough to a ﬁeld of multivaliate cryptosystem in a sense that the transformation is dependent on a message. Namely it is a message-dependent transformation on the basis of random coding. We show that the proposed PKC's, can be secure against the various excellent attacks such as the attack based on the Gr¨obner bases calculation(Gröbner bases attack, GB attack), Patarin's attack and Braeken-Wolf-Preneel attack, due to the random transformations using new trap-doors.

Category / Keywords: public-key cryptography /

Publication Info: Faculty of Informatics, Osaka Gakuin University, Suita-shi, 564-8511 Japan.

Date: received 20 Dec 2011

Contact author: kasahara at ogu ac jp