Cryptology ePrint Archive: Report 2011/573

A New Class of Multivariate Public Key Cryptosystems Constructed Based on Random Pseudo Cyclic Codes, K (XIII)SE(2)PKC, Realizing Coding Rate of Exactly 1.0

Masao Kasahara

Abstract: In this paper, we present a new class of multivariate public-key cryptosystems, K(XIII)SE(2)PKC realizing the coding rate of exactly 1.0, based on random pseudo cyclic codes. The K(XIII)SE(2)PKC is constructed on the basis of K(IX)SE(1) PKC, formerly presented by the author. We show that K(XIII)SE(2)PKC is secure against the various attacks including the attack based on the Gröbner bases calculaion(GB attack) and the rank attack.

Category / Keywords: public-key cryptography / Public key cryptosystem, Error-correcting code, Code based PKC, Cyclic code, Multivariate PKC, Gröbner bases, Rank attack, PQC.

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

Date: received 23 Oct 2011

Contact author: kasahara at ogu ac jp