Cryptology ePrint Archive: Report 2011/125

A Construction of A New Class of Knapsack-Type Public Key Cryptosystem, K(III)ΣPKC

Masao KASAHARA

Abstract: In this paper, we present a new class of knapsack type PKC referred to as K(III)ΣPKC. In a sharp contrast with the conventional knapsack type PKC's, in our proposed scheme, K(III)ΣPKC, no conventional secret sequence but the natural binary number with noise is used. We show that the coding rate, a more conservative measure for the security on knapsack PKC, can be made approximately 1.0.

In Appendix, we present K(II)ΣPKC.

Category / Keywords: public-key cryptography / Public-key cryptosystem(PKC), Knapsack type PKC, Subset-sum problem, LLL algorithm, PQC.

Date: received 10 Mar 2011

Contact author: kasahara at ogu ac jp