Cryptology ePrint Archive: Report 2013/180

A New Class of Product-sum Type Public Key Cryptosystem,K(V)$\Sigma\Pi$ PKC,Constructed Based on Maximum Length Code

Masao KASAHARA

Abstract: The author recently proposed a new class of knapsack type PKC referred to as K(II)$\Sigma\Pi$PKC [1]. In K (II)$\Sigma\Pi$PKC with old algorithm DA[I], Bob randomly constructs a very small subset of Alice's set of public key whose order is very large, under the condition that the coding rate ρ satisfies $0.01 < \rho < 0.2$. In K(II) $\Sigma\Pi$PKC, no secret sequence such as super-increasing sequence or shifted-odd sequence but the sequence whose components are constructed by a product of the same number of many prime numbers of the same size, is used. In this paper we present a new algorithm, DA(II) for decoding K(II)$\Sigma\Pi$PKC.We show that with new decoding algorithm, DA(II), K(II)$\Sigma\Pi$PKC yields a higher coding rate and a smaller size of public key compared with K(II)$\Sigma\Pi$PKC using old decoding algorithm, DA(I). We further present a generalized version of K(II) $\Sigma\Pi$PKC, referred to as K(\v) $\Sigma\Pi$PKC. We finally present a new decoding algorithm DA(III) and show that, in K(V)$\Sigma\Pi$PKC with DA (III), the relation, $r_F\simeq 0, \rho \simeq \frac{2}{3}$ holds, where r_F is the factor ratio that will be defined in this paper. We show that K(V)$\Sigma\Pi$PKC yields a higher security compared with K(II) $\Sigma\Pi$PKC.

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

Date: received 30 Mar 2013

Contact author: kasahara at ogu ac jp