Cryptology ePrint Archive: Report 2011/467

Security Features of an Asymmetric Cryptosystem based on the Diophantine Equation Hard Problem

M.R.K. Ariffin, M.A. Asbullah and N.A. Abu

Abstract: The Diophantine Equation Hard Problem (DEHP) is a potential cryptographic problem on the Diophantine equation $U=\sum \limits_{i=1}^n {V_i x_{i}}$. A proper implementation of DEHP would render an attacker to search for private parameters amongst the exponentially many solutions. However, an improper implementation would provide an attacker exponentially many choices to solve the DEHP. The AA\,$_{\beta}$-cryptosystem is an asymmetric cryptographic scheme that utilizes this concept together with the factorization problem of two large primes and is implemented only by using the multiplication operation for both encryption and decryption. With this simple mathematical structure, it would have low computational requirements and would enable communication devices with low computing power to deploy secure communication procedures efficiently.

Category / Keywords: Diophantine equation hard problem (DEHP), integer factorization problem, asymmetric cryptography

Publication Info: Hope to be submitted

Date: received 28 Aug 2011, last revised 11 Jan 2012

Contact author: rezal at math upm edu my