The diophantine equation hard problem (DEHP) as an asymmetric primitive - is it possible?

ABSTRACT

We put forward a probable hard problem based on a Diophantine equation that has characteristics to become an asymmetric primitive. Motivated by rearranging the equation representing the RSA modulus, N together with its Euler-phi function, (N) we define the Diophantine Equation Hard Problem (DEHP) on a definitive setting. Relation between the RSA factorization problem, RSA's e-th root problem and the DEHP is also discussed. A proposed asymmetric cryptosystem that manipulates DEHP together with the difficulty of factoring a product of strong primes is presented.