Cryptology ePrint Archive: Report 2011/131

Trapdoor oneway functions associated with exponentiation

Virendra Sule

Abstract: This paper shows that if exponentiation $b=X^{k}$ in groups of finite field units or $B=[k]X$ in elliptic curves is considered as encryption of X with exponent k treated as symmetric key, then the decryption or the computation of X from b (respectively B) can be achieved in polynomial time with a high probability under random choice of k. Since given X and b or B the problem of computing the discrete log k is not known to have a polynomial time solution, the exponentiation has a trapdoor property associated with it. This paper makes this property precise. Further the decryption problem is a special case of a general problem of solving equations in groups. Such equations lead to more such trapdoor one way functions when solvable in polynomial time. The paper considers single and two variable equations on above groups and determines their solvability.

Category / Keywords: secret-key cryptography / Exponential function, elliptic curves, division polynomials

Date: received 15 Mar 2011

Contact author: vrs at ee iitb ac in

Available formats: PDF | BibTeX Citation

Version: 20110318:122933 (All versions of this report)

Discussion forum: Show discussion | Start new discussion