# Cryptology ePrint Archive: Report 2011/187

## Accelerating ID-based Encryption based on Trapdoor DL using Pre-computation

*Hyung Tae Lee and Jung Hee Cheon and Jin Hong*

**Abstract:** The existing identity-based encryption (IBE) schemes based on pairings require pairing computations in encryption or decryption algorithm and it is a burden to each entity which has restricted computing resources in mobile computing environments. An IBE scheme (MY-IBE) based on a trapdoor DL group for RSA setting is one of good alternatives for applying to mobile computing environments. However, it has a drawback for practical use, that the key generation algorithm spends a long time for generating a user's private key since the key generation center has to solve a discrete logarithm problem.

In this paper, we suggest a method to reduce the key generation time of the MY-IBE scheme, applying modified Pollard rho algorithm using significant pre-computation (mPAP). We also provide a rigorous analysis of the mPAP for more precise estimation of the key generation time and consider the parallelization and applying the tag tracing technique to reduce the wall-clock running time of the key generation algorithm.

Finally, we give a parameter setup method for an efficient key generation algorithm and estimate key generation time for practical parameters from our theoretical analysis and experimental results on small parameters. Our estimation shows that it takes about two minutes using pre-computation for about 50 days with 27 GB storage to generate one user's private key using the parallelized mPAP enhanced by the tag tracing technique with 100 processors.

**Category / Keywords:** Identity-based Encryption, Trapdoor DL Groups, Discrete Logarithm, Pre-computation

**Date:** received 12 Apr 2011, last revised 11 Jan 2012

**Contact author:** htsm1138 at snu ac kr

**Available formats:** PDF | BibTeX Citation

**Version:** 20120112:021951 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

[ Cryptology ePrint archive ]