# TRNG Based Key Generation for Certificateless Signcryption

**Authors :** S.Balaji, R.Sujatha, M. Ramakrishnan

**Abstract :** Signcryption is a cryptographic primitive that fulfills both the functions of digital signature and public key encryption simultaneously in low cost when compared with the traditional signature-then-encryption approach. In this paper, we propose a novel mouse movement based key generation technique to generate secret keys which is secure against the outer and insider attacks. Tag Key Encapsulation Mechanism (KEM) process is implemented using True Random Number Generator (TRNG) method. This TRNG based key is used for data encryption in the Data Encapsulation Mechanism (DEM). We compare the statistical reports of the proposed system with the previous methods which implements TKEM based on pseudo random number generator

**Keywords :** pseudo random umber generator, signcryption, true random number generator, node deployment
**Conference Title :** ICCEIT 2015 : International Conference on Computer Engineering and Information Technology
**Conference Location :** Miami, United States
**Conference Dates :** March 09-10, 2015

Open Science Index, Computer and Information Engineering Vol:9, No:03, 2015 publications.waset.org/abstracts/15844.pdf