July - Sep © 2015 Transactions; 2(7): 321-329

International Journal of Research and Applications

ISSN (online): 2349-0020 ISSN (print): 2394-4544 http://www.ijraonline.com/

DRIVEN BY doi

Research Article

An upgraded signcryption scheme using forward secrecy

Varun Kumar Chennuri [1] and Dr. Sadanandam Manchala (Supervisor) [2]

Corresponding Author:
kumarvarun501@gmail.com

DOI:
http://dx.doi.org/
10.17812/IJRA.2.7(56)2015

Manuscript:
Received: 7th July, 2015
Accepted: 21st Aug, 2015
Published: 17th Sep, 2015

Publisher:
Global Science Publishing Group, USA
http://www.globalsciencepg.org/

ABSTRACT

SignCryption is a different prototype in public key cryptography technique to provide confidentiality and authentication in a single logical stride at the lowest computation cost and communication overhead compared to the traditional signature-then-encryption mechanism [1]. In this paper, we intend a new technique to the superior scheme is an ameded version of existing mechanism followed in Bao & Deng, in which publicly verifiable signcryption is to be deliberated [3]. But this scheme refers to providing the security feature of forward secrecy from the existing signcryption, without an escalation in computational cost. Also, this new signcryption procedure delivers the security services of message confidentiality and Authentication with public verifiability.

Keywords: SignCryption, Public Key Cryptography technique, Signature-then-Encryption, Public Verifiability, Forward Secrecy.

[1] [2] Department of Computer Science and Engineering, KUCE & T
[1] [2] Kakatiya University, Warangal, Telangana, India.

IJRA - Year of 2015 Transactions:
Month: July - September
Volume – 2, Issue – 7, Page No's:321-329
Subject Stream: Computers

Paper Communication: Author Direct

Paper Reference Id: IJRA-2015: 2(7)321-329