{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 165
-
Number 2

Year of Publication: 2017

Authors:

Roayat Ismail Abdelfatah

10.5120/ijca2017913804

{bibtex}2017913804.bib{/bibtex}

## Abstract

Proxy signcryption scheme allows an original signer to delegate his signing power to a proxy such that the latter can signcrypt a message on behalf of the former. In this paper, a new proxy signcryption scheme is proposed based on Discrete Logarithm Problem (DLP) and Diffie-Hellman Problem (DHP) with a reduced computational cost compared to other schemes in literature. The proposed scheme achieves public ciphertext authentication as the signcrypted message before being accepted, the receiver first verifies the signature. This property is very useful as the receiver can filter some incorrect ciphertext before decrypting it which achieves more efficient unsigncryption. Also, a variant of the main scheme that works over elliptic curves will be considered, since it has proven to provide better security with shorter keys and hence less storage requirements which makes it more suitable for resource constrained devices such as pagers and mobile phones. Numerical examples have been given with Mathematica to emphasize the ease of its practical use.

## References

1. Diffie W, Heliman M. New direction in cryptography. IEEE Transactions on Information Theory 1976; 22 (6): 644-654.
2. Mambo M, Usuda K, Okamoto E. Proxy signature: delegation of the power to sign messages. IEICE Transaction on Fundamentals 1996; E79-A (9): 1338-1353.
3. Kim S, Park S, Won D. Proxy signatures, revisited. In Proceedings of Information and Communications Security. (ICICS' 97), Han Y, Okamoto T, Qing S (eds), LNCS 1334. Springer-Verlag:Beijing, China, 1997; 223-232.
4. Lee B, Kim H, Kim K. Secure mobile agent using strong non-designated proxy signature. In Proceedings of Information Security and Privacy (ACISP'01), Varadharajan V, Mu Y (eds), LNCS 2119. Springer Verlag: Sydney, Australia, 2001; 474-486.
5. Lee B, Kim H, Kim K. Strong proxy signature and its applications, In Proceedings of the Symposium on Cryptography and Information Security (SCIS'01), Oiso, Japan,2001;603-608.
6. Kim S, Park S, and Won D. Proxy signatures, revisited. In Proceedings of ICICS 97, LNCS 1334, Springer-Verlag; 1997; 223-232.
7. Zheng Y. Digital Signcryption or How to Achieve Cost (Signature & Encryption)