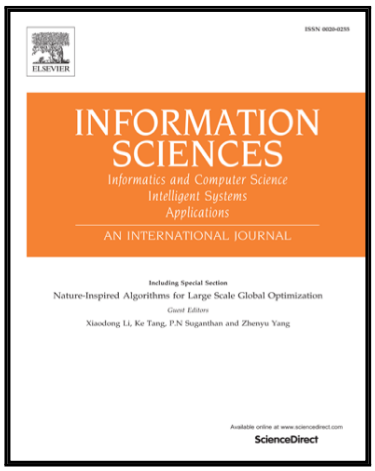

Provably Secure Certificate-Based Proxy Blind Signature Scheme from Pairings

Girraj Kumar Verma, B.B. Singh, Harendra Singh

PII: S0020-0255(18)30634-0
DOI: https://doi.org/10.1016/j.ins.2018.08.031
Reference: INS 13875

To appear in: *Information Sciences*

Received date: 7 September 2017
Revised date: 25 June 2018
Accepted date: 12 August 2018

Please cite this article as: Girraj Kumar Verma, B.B. Singh, Harendra Singh, Provably Secure Certificate-Based Proxy Blind Signature Scheme from Pairings, *Information Sciences* (2018), doi: https://doi.org/10.1016/j.ins.2018.08.031

Provably Secure Certificate-Based Proxy Blind Signature Scheme from Pairings

Girraj Kumar Verma[a,*], B. B. Singh[b], Harendra Singh[c]

[a] *Hindustan College of Science and Technology Farah, Mathura, India*
[b] *Government K. R. G. (P.G.) College Gwalior, India*
[c] *Hindustan College of Science and Technology Farah, Mathura, India*

Abstract

In 2003, C. Gentry introduced the paradigm of certificate-based encryption (CBE) to combine the merits of public key cryptography (PKC) and identity-based PKC (ID-PKC). The invention of CBE also remove the key escrow as well as secret key distribution problem in ID-PKC and the third party queries problem of PKC. This article presents the first short and efficient provably secure certificate-based proxy blind signature (CB-PBS) scheme from pairing over elliptic curves. The proposed CB-PBS scheme is proven secure under adaptively chosen message and ID attack in the random oracle model. Through efficiency comparison with existing related efficient PBS schemes, it is shown that the proposed CB-PBS scheme is the most efficient and short signature scheme. Due to the shortest length, it is the most appealing to implement in low bandwidth communication systems to design e-cash, e-voting, etc.

Keywords: Proxy Signature, Blind Signature, Bilinear Pairing, Certificate-Based Signature, e-cash.
2010 MSC: 94A60

*Corresponding author
Email address: girrajv@gmail.com (Girraj Kumar Verma)