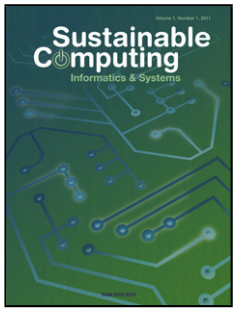

Title: A Certificateless Aggregate Signature Scheme for Healthcare Wireless Sensor Network

Authors: Pankaj Kumar, Saru Kumari, Vishnu Sharma, Arun Kumar Sangaiah, Jianghong Wei, Xiong Li

PII: S2210-5379(17)30022-7
DOI: http://dx.doi.org/10.1016/j.suscom.2017.09.002
Reference: SUSCOM 187

To appear in:

Received date: 4-2-2017
Revised date: 4-8-2017
Accepted date: 6-9-2017

Please cite this article as: Pankaj Kumar, Saru Kumari, Vishnu Sharma, Arun Kumar Sangaiah, Jianghong Wei, Xiong Li, A Certificateless Aggregate Signature Scheme for Healthcare Wireless Sensor Network, Sustainable Computing: Informatics and Systemshttp://dx.doi.org/10.1016/j.suscom.2017.09.002

A Certificateless Aggregate Signature Scheme for Healthcare Wireless Sensor Network

Pankaj Kumar[1], Saru Kumari[2], Vishnu Sharma[3], Arun Kumar Sangaiah[4], Jianghong Wei[5], Xiong Li[6]

[1,3]School of computing Science and engineering, Galgotias University
{pkumar240183, vishnusharma97}@gmail.com
[2]Department of Mathematics, Ch. Charan Singh University, Meerut, India
saryusiirohi@gmail.com
[4]School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu,India
arunkumarsangaiah@gmail.com
[5]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China.
jianghong.wei.xxgc@gmail.com
[6]School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
lixiongzhq@163.com

Highlights

- This paper presents a certificateless aggregate signature scheme for green Healthcare Wireless Sensor Network.
- The proposed scheme does not require certification and is free from key escrow problem.
- We have used batch verification technique for speedy verification of signatures. Security of the proposed scheme is proved using Random Oracle Model.

Abstract

Healthcare industry is one of the areas where wireless sensor network provides a lot of opportunities. Online data sharing in healthcare industry not only increases the efficiency but also reduces the time constraints. In the healthcare wireless sensor network, patient's report is available online for health professionals without any delay after patient's checkup. Data privacy becomes an important issue in healthcare industry due to direct involvement of personal health related data of patients. Modified data may become a serious cause of casualty for patient. Digital signature scheme is a technique of public key cryptography that is widely accepted in digital world to retain privacy and integrity. Certificateless public key cryptography was proposed to remove the complication of certificate management in public key cryptography as well as the key escrow problem inherited in identity based cryptography. An aggregate signature scheme is a many to one map which maps different signatures on different messages to a single signature. This feature is very beneficial in an environment which is constrained by limited bandwidth and low computational time/effort, such as wireless sensor network, vehicular ad-hoc network and Internet of things. Our proposed certificateless aggregate signature enjoys the goodness of both the concepts, certificateless and aggregate. We construct a certificateless aggregate signature scheme and prove the security of constructed scheme by using widely-accepted Random Oracle Model under the computationally hard Diffie-Hellman assumption.