International Journal of Information Security and Privacy
Volume 13 • Issue 4 • October-December 2019

An Efficient and Secure Certificateless Aggregate Signature From Bilinear Maps

Pankaj Kumar, School of Computing Science and Engineering, Galgotias University, Delhi, India

Vishnu Sharma, Amity School of Engineering, Amity University, Noida, India

Gaurav Sharma, Départment d'Informatique, Université Libre de Bruxelles, Bruxelles, Belgium

Tarunpreet Bhatia, Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Punjab, India

ABSTRACT

Certificateless signature schemes are a very intriguing aspect in information security because of its capability of removing the well-known key escrow problem predominately in ID-based cryptography. He et al. proposed an efficient certificateless aggregate signature scheme and proved that their scheme is secure against all possible types of security attacks. However, the authors still managed to find loopholes in the form of insecurities against 'honest but curious' and 'malicious but passive' attacks during cryptanalysis of He et al.'s scheme. The authors propose an efficient certificateless aggregate signature scheme which fills the security gaps in He et al.'s scheme and demonstrate the security in their scheme via a mathematical proof, and reinforce the fact that their scheme is much more efficient in a thorough performance comparison of their scheme against the previous schemes.

KEYWORDS

Certificateless Signature, Cryptanalysis, Cryptography, Digital Signature

1. INTRODUCTION

Digital signature is an imperative and an indispensable constituent in public key cryptography which covers authenticity, integrity and non-repudiation. In a public key infrastructure, a user uses a pair of keys namely, private/public key pair for communication. Public key is widely spread across the participants of the communication process whereas private key is kept secret by the user. A certificate is needed in order to bind the public key and private key to avoid the authentication problem. A third entity is also required in the system for binding the public key with the corresponding private key, that leads to the certification management problem. In order to overpower the certificate management problem Shamir (1984) introduced an ID-based public key cryptography which does not need certification. In the ID-based cryptography, public key is chosen by user such as an address, phone number, driving license or any other identity and the private key is generated by the third party called private key generator (PKG). Since private key is generated by the PKG, hence in case the PKG itself becomes malicious then security is inherently compromised, and it is this issue that has been termed as key

DOI: 10.4018/IJISP.2019100106

escrow problem. ID-based public key cryptography falls prey to the key escrow problem. Al Riyami (2003) provided the solution to key escrow problem for the first time where certificateless signature scheme was enumerated in which the interested third party say key generation center (KGC) generates the partial private key of user instead of private key and the private key is in turn generated by the user with the help of partial private key. KGC does not know the private key directly. Aggregate signature scheme was incentivized by Boneh (2003). Aggregation is very efficient technique that collects all the n individual signatures of n different users corresponding to n different messages and aggregates them into short single signature. Aggregate signatures can significantly reduce computational and communication overhead. The single aggregate signature can easily convince verifier that n different users have really signed n messages individually.

Wireless Sensor Networks, Vehicular networks, Internet of Things (IoT) have been utilized for target tracking, remote location monitoring, environment monitoring, patient monitoring etc. in the real-world but data can be easily compromised by various attacks such as fabrication, tampering etc. Certificateless aggregate signatures can be used to ensure data integrity and to reduce computational and communication overhead.

Related work: Many researchers have successfully accomplished a lot of work in the area of certificateless Signature scheme. Al Riyami (2003) have proposed for the first time, the CLS scheme. Gorantla (2005) proposed an efficient CLS scheme and later Cao (2006) found certain insecurities in their scheme against some concrete security attacks. Li (2005) and Zhang (2006) used elliptic curve verification algorithms in their CLS scheme which was improved by Yap (2006) by reducing the bilinear pairing operation. Au (2007) suggested a malicious-but-passive KGC attack where adversary may be a malicious KGC. Huang (2007) proposed two new short CLS schemes and proved that both CLS schemes are secure against type 1 and type 2 adversary but Shim (2011) proved that the first scheme proposed (Shim, 2009) was found insecure against type I adversary. Tsai (2014) proposed a certificateless signature scheme without pairing. Sharma (2013) found in their security analysis of proposed scheme (Tsai, 2014) that it failed to resist the malicious-but-passive attacks. Huang (2012) categorized the adversary A_1 and adversary A_2 according to their attacking power say, Super type, Strong type and Normal type. Since the introduction of Boneh et al.'s aggregate signature scheme and certificateless cryptography, their integration i.e. certificateless aggregate signature schemes have also attracted much attention of researchers (Castro, 2007; Gong, 2007; Zhang, 2009; Zhang, 2010; Shim, 2011; Xiong, 2013; He, 2014; Cheng, 2015; Zhang, 2014; Tu, 2014). Castro (2007) introduced first certificateless aggregate signature scheme and developed its security model. Thereafter, Gong (2007) designed two certificateless aggregate signature schemes. First scheme reduces communication and computation cost but compromises with storage space and second minimizes storage but compromises communication cost. The schemes (Gong, 2007; Zhang, 2009; Zhang, 2010) involve heavy pairing computations in signing process and it varies linearly with increasing number of signers. Other schemes (Zhang, 2009; Zhang, 2010) require synchronization among all signers while generating aggregated signature which is difficult to achieve in real time.In a cryptanalysis of CLAS scheme (Zhang, 2009), Shim (2011) proved that their scheme was not safe against the collision resistant attack by testing against some concrete attacks. Xiong (2013) proposed a certificateless aggregate signature scheme with constant pairing computations which is convenient for Ad-hoc Networks and claimed to be secure with the computational Diffie-Hellman problem in random oracle, but their scheme is found insecure by He (2014) and Cheng (2012) by demonstrations and they further provided an improvement for their CLS scheme. Zhang (2014) applies four types of attacks, malicious but passive attack, honest but curious attack on CLS scheme (Xiong, 2013) and proved it insecure. Tu (2014) proved that Xiong (2013) CLAS scheme is forgeable under Type II adversary and proposed an improvement over their scheme.

The Nature, Extent, Causes, and Consequences of Cyberbullying
Michelle F. Wright (2019). *Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics (pp. 138-150).*
www.igi-global.com/chapter/the-nature-extent-causes-and-consequences-of-cyberbullying/213646?camid=4v1a

Control Mechanism of Identity Theft and Its Integrative Impact on Consumers' Purchase Intention in E-Commerce
Mahmud A. Shareef, Vinod Kumar and Uma Kumar (2014). *Analyzing Security, Trust, and Crime in the Digital World (pp. 121-161).*
www.igi-global.com/chapter/control-mechanism-of-identity-theft-and-its-integrative-impact-on-consumers-purchase-intention-in-e-commerce/103814?camid=4v1a