Journal of King Saud University – Computer and Information Sciences (2014) **26**, 55–67

King Saud University

**Journal of King Saud University – Computer and Information Sciences**

www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

# A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings

**SK Hafizul Islam** [*], **G.P. Biswas**

*Department of Computer Science and Engineering, Indian School of Mines, Dhanbad 826004, Jharkhand, India*

Received 21 October 2012; revised 17 January 2013; accepted 17 March 2013
Available online 26 March 2013

**KEYWORDS**

Elliptic curve cryptography;
Identity-based cryptosystem;
Bilinear pairing;
Proxy signature;
Strong designated verifier;
AVISPA tool

**Abstract** The proxy signature, a variant of the ordinary digital signature, has been an active research topic in recent years; it has many useful applications, including distributed systems and grid computing. Although many identity-based proxy signature schemes have been proposed in the literature, only a few proposals for identity-based strong designated verifier proxy signature (ID-SDVPS) schemes are available. However, it has been found that most of the ID-SDVPS schemes that have been proposed to date are not efficient in terms of computation and security, and a computationally efficient and secured ID-SDVPS scheme using elliptic curve bilinear pairing has been proposed in this paper. The security of the scheme is mainly based on the hardness assumption of CDH and GBDH problems in the random oracle model, which is existentially unforgeable against different types of adversaries. Furthermore, the security of our scheme is simulated in the AVISPA (Automated Validation of Internet Security Protocols and Applications) software, a widely used automated internet protocol validation tool, and the simulation results confirm strong security against both active and passive attacks. In addition, because of a high processing capability and supporting additional security features, the scheme is suitable for the environments in which less computational cost with strong security is required.

## 1. Introduction

In a PKI (public key infrastructure)-based cryptosystem, the public key certificate that is generated and signed by a certificate authority (CA) is required for authentication of the public keys of the entities, and, as a result, it creates a heavy management burden for maintaining and using the public key certificate by developing a global infrastructure. As a remedy, Shamir (1984) proposed the concept of an identity-based cryptosystem (IBC) that supports the users' authentication through the use of a public identity. In other words, a user's public key in IBC is computed from an email identity, a social security number, a passport number or other identifiers and a private key generator (PKG); a trusted third party generates the user's private key by using the user's identity and his/her master private key. The private key generated by PKG is communicated to the user through a secure channel, for which its legitimacy can be verified by the user publicly. However, as such, no practical implementation for IBC was proposed by Shamir, and in 2001, Boneh and Franklin (2001) first proposed a bilinear pairing-based technique (Weil or Tate) that uses a super-singular elliptic curve based on the Bilinear Diffie

[*] Corresponding author. Tel.: +91 8797369160; fax: +91 326 2296563.
E-mail addresses: hafi786@gmail.com, hafizul.ism@gmail.com (SK H. Islam).

1319-1578 © 2013 Production and hosting by Elsevier B.V. on behalf of King Saud University.
http://dx.doi.org/10.1016/j.jksuci.2013.03.004

Hellman (BDH) assumption in the random oracle model (Bellare and Rogaway, 1993), which is called the identity-based encryption (IBE) technique. Subsequently, a number of IBE cryptosystems have been developed. In this paper, we have proposed an identity-based strong designated verifier proxy signature (ID-SDVPS) scheme that uses bilinear pairing for mapping from an elliptic curve additive cyclic group (Miller, 1985; Koblitz, 1987) to any multiplicative cyclic group of the same prime order. Next, the description of some signature schemes will be given.

In 1996, Jakobsson et al. (1996) first proposed a designated verifier signature (DVS) scheme for which the original signer *Alice* generates a signature, and only a designated verifier *Bob* can verify the signature. However, it can be seen that the signer's privacy protection is violated in DVS schemes because *Bob* can easily convince a third party that the message was signed by *Alice*. To remove this problem, Jakobsson et al. (1996) proposed another signature scheme, called the strong designated verifier signature (SDVS). In an SDVS scheme (Huang et al., 2008; Kang et al., 2009; Islam and Biswas, 2013), *Bob* cannot prove to an outsider that *Alice* is the original signer. This problem occurs because an identical signature can be generated by *Bob*, and it cannot be distinguished from the signatures of *Alice;* in addition, *Bob*'s private key is strictly required in the verification phase. Therefore, the SDVS scheme satisfies the *strongness* and *repudiable* properties. Since then, many SDVS schemes (Saeednia et al., 2004; Huang et al., 2008; Lee et al., 2010; Tang et al., 2011; Yoon, 2011) have been proposed by researchers for different applications of Network/Information Security.

In 1996, Mambo et al. (1996) proposed a proxy signature scheme in which the original signer (*Alice*) delegated his signing privilege to a proxy signer such that the proxy signer (*Bob*) on behalf of the original signer can sign some specific messages. An entity (*Cindy*) who receives a message with a proxy signature can easily check the correctness of the signature and be convinced about the agreement of the original signer. However, this proxy signature scheme allows public verification, which might not be suitable for applications in which the verification of the proxy signature for personal sensitive and/or important commercial documents must be performed by designated persons. Thus, a strong designated verifier proxy signature (SDVPS) scheme (Dai et al., 2003; Wang, 2004; Cao et al., 2005; Lin et al., 2011) is proposed for these environments. In this scheme, the proxy signer computes a proxy signature for the designated verifier, who only validates the signature but is unable to convince an outsider about the original signer and the proxy signer. The reason is that the designated verifier can also generate a simulated proxy signature that is intended for him, which is indistinguishable from the original proxy signature.

Proxy signatures have been suggested for many applications, including distributed systems (Neuman, 1993), grid computing (Foster et al., 1998), mobile agent systems (Kim et al., 2001), mobile communications (Park and Lee, 2001), and e-commerce (Dai et al., 2003; Wang, 2004). Based on the application areas, the proxy signature can be categorized into four types (Mambo et al., 1996; Wang, 2008; Yang, 2010; Islam and Biswas, 2012a), namely *full delegation*, *partial delegation*, *delegation by warrant* and *partial delegation by warrant*. Among these, the *partial delegation by warrant* satisfies all the security requirements of the proxy signatures. Additionally, the proxy signature is based on the proxy private key; the proxy signatures can be classified into two signature types, which are *proxy-unprotected* and *proxy-protected*. There is a repudiation dispute problem in the *proxy-unprotected* scheme because the proxy signature is created either by the original signer or the proxy signer. On the other hand, the repudiation dispute problem is absent in the *proxy-protected* scheme because only the proxy signer generates the proxy signature.

### *1.1. Recent studies*

A number of new identity-based strong designated verifier proxy signature (ID-SDVPS) schemes have been proposed recently (Cao et al., 2005; Lal and Verma, 2006; Kang et al., 2009; Lee et al., 2010), and a short discussion of each is provided here. In 2003, Dai et al. (2003) proposed a designated verifier proxy signature (DVPS) scheme that is suitable for e-commerce environments. In 2005, Cao et al. (2005) proposed an identity-based DVPS (ID-DVPS) scheme that is based on Cha and Cheon's signature scheme (Cha and Cheon, 2003) and uses bilinear pairing, and Gu and Zhu (2005) proposed a new computational model for a provably secure identity-based proxy signature scheme. In 2006, Lal and Verma (2006) proposed an ID-DVPS scheme using bilinear pairings. However, Kang et al. (2009) proved that the scheme was insecure; then, they proposed an efficient scheme and claimed that the scheme was unforgeable. Later, in 2008, Gu and Zhu (2008) proposed an efficient version of Zhang and Kim's scheme (2003), which was based on the security model proposed in (Gu and Zhu, 2005). In 2010, Lee et al. (2010) demonstrated that the scheme proposed in (Kang et al., 2009) is universally forgeable, which means that anyone can forge a valid ID-DVPS on an arbitrary message without the knowledge of the secret key of either the signer or the designated verifier.

A new proxy signature scheme was also proposed by Wu et al. (2007), which improves the security aspects of an identity-based proxy signature scheme. Wang (2008) gave a new identity-based proxy signature scheme, which is secure against the *proxy key exposure attack* in the random oracle model (Bellare and Rogaway, 1993). In general, an ID-DVPS scheme needs a trusted PKG unconditionally; otherwise, a dishonest PKG can compute the private key of any user and can forge its proxy signature. In 2010, Yang et al., as a solution of the problem, proposed an ID-DVPS scheme without a trusted party. Later on, Reddy et al. (2010) also proposed an identity-based directed proxy signature scheme using bilinear pairings and the concept of Hess's identity-based signature scheme (Hess, 2002). In 2012, Islam and Biswas (2012a) proposed an efficient ID-based Short DVPS (ID-ShDVPS) scheme using elliptic curve bilinear pairing, which is a short signature scheme and is applicable to the environments with limited bandwidth, computing power and storage space. However, it always generates the same proxy signature on the same message, and its security is proven only heuristically.

### *1.2. Our contributions*

Elliptic curve cryptography and bilinear pairing are two efficient tools that are used to design secure cryptographic protocols for various applications (Zhang and Kim, 2003; Dai et al., 2003; Cao et al., 2005; Farash et al., 2012; Das, 2012). In the literature, many ID-SDVPS schemes using elliptic curve