Journal of King Saud University – Computer and Information Sciences xxx (2018) xxx–xxx

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

A forward secure signcryption scheme with ciphertext authentication for e-payment systems using conic curve cryptography

Renu Mary Daniel *, Elijah Blessing Rajsingh, Salaja Silas

Department of Computer Sciences Technology, Karunya Institute of Technology and Sciences, Tamil Nadu 641114, India

ARTICLE INFO

Article history:
Received 10 November 2017
Revised 22 January 2018
Accepted 10 February 2018
Available online xxxx

Keywords:
Signcryption
Conic curve cryptography
Forward secrecy
Ciphertext authentication
E-commerce
ProVerif

ABSTRACT

Signcryption is an authenticated encryption technique that concurrently establishes message confidentiality, authenticity, integrity and non-repudiation. In this paper, we propose an efficient signcryption scheme, based on the hardness of RSA assumption and discrete logarithm problem on conic curves over a ring Z_n. The protocol ensures forward secrecy, in case the sender's secret keys are exposed and supports ciphertext authentication by an external entity, without full decryption. The protocol remains secure, as long as, either one of the hardness assumptions hold. The scheme is implemented over conic curves, which facilitates effective message encoding and decoding, as well as, efficient point operations and inverses. Conic-based RSA assumption offers resistance to low public key and low private key exponent attacks, prevalent in the original RSA cryptosystem. The proposed protocol is used to design a Business to Customer (B2C) e-commerce system, with security against replay attacks, man-in-the-middle attacks, impersonation attacks, server spoofing and double spending. The protocol is validated using automated cryptographic verification tool ProVerif.

1. Introduction

In public key cryptosystems, message confidentiality, integrity, authenticity and non-repudiation is ensured by first signing the message with the sender's private key and then encrypting the message-signature pair using an ephemeral session key. Subsequently, the session key is encrypted using the receiver's public key before transmission. On receiving the randomized session key and the encrypted message-signature pair, the receiver retrieves the session key using his private key. Then, the receiver decrypts the encrypted message-signature pair using the session key. Finally, the receiver confirms the authenticity and integrity of the message by verifying the signature using the sender's public key. To reduce the cost of the conventional "signature then encryption" approach, Zheng (1997) proposed an authenticated encryption primitive called signcryption, which combines the functionalities of both encryption and digital signature in a single logical step. Zheng's signcryption scheme was based on Discrete Logarithm Problem (DLP) over a finite field. Later, a variant of the scheme based on the elliptic curve analog of DLP (ECDLP), was proposed by Zheng and Imai (1998). Ideally, a signcryption scheme must ensure the following security attributes:

- *Public verifiability* – Public verifiability implies that given the original message, the ciphertext components and some optional information, an external entity can verify the message authenticity, without the recipient's private key (Ahmed et al., 2010).
- *Ciphertext authentication* – Ciphertext authentication implies that the external judge can authenticate the message origin from the ciphertext components and some intermediate decryption results provided by the receiver. The receiver need not reveal the original message or the private key to an external judge, to ensure non-repudiation.
- *Public ciphertext authentication* – Public ciphertext authentication implies that an external entity can verify the message origin solely from the ciphertext components, without any intervention of the recipient.
- *Ciphertext anonymity* – Ciphertext anonymity ensures that no useful information about the sender can be derived from the ciphertext components. It is to be noted that, public ciphertext authentication and ciphertext anonymity cannot be attained simultaneously.

* Corresponding author.
E-mail addresses: renumarydaniel@karunya.edu.in (R.M. Daniel), elijahblessing@karunya.edu (E.B. Rajsingh), salaja_cse@karunya.edu (S. Silas).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2018.02.004
1319-1578/

Please cite this article in press as: Daniel, R.M., et al. A forward secure signcryption scheme with ciphertext authentication for e-payment systems using conic curve cryptography. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.02.004

- *Forward secrecy* – Forward secrecy property deters an adversary in possession of the sender's secret keys, from decrypting previously encrypted messages.

1.1. Previous work

The initial signcryption scheme proposed by Zheng (1997) lacked public verifiability. Hence, in Zheng's scheme, the receiver had to reveal his private key to the external verifier, to ensure non-repudiation. Bao and Deng (1998) modified Zheng's protocol so that, the recipient's private key is no longer required for signature verification. Instead, the recipient must produce the original message along with the ciphertext components to the external entity. The property is termed as public verifiability. The protocol was implemented in finite field, based on strong Gap Diffie-Hellman (Gap-DH) assumption. However, public verifiability property is unsuitable for applications requiring content filtering by firewalls, since, verification by an external entity is not possible until the decryption of the ciphertext, by the intended recipient. Gamage et al. (1999) proposed the first signcryption scheme with public ciphertext authentication property. In Gamage's scheme, any external entity can verify the signature solely from the ciphertext components, without the intervention of the recipient. The protocol is based on standard Computational Diffie-Hellman (CDH) assumption. Apparently, the protocol lacks ciphertext anonymity, since, an adversary can perform random checks to detect the message origin (Chow et al., 2003). Hence, public ciphertext authentication property is undesirable for applications like e-commerce, where the sender's identity has to be preserved. None of the above mentioned protocols provide forward secrecy property. Chow et al. proposed a forward secure signcryption scheme with public ciphertext authentication property, under Modified Decisional Bilinear Diffie-Hellman (MDBDH) assumption on elliptic curves. However, the protocol incurs higher computational complexity due to expensive bilinear pairing operations. Later, Han et al. (2004) proposed a forward secure signcryption scheme with ciphertext authentication and ciphertext anonymity based on Elliptic Curve Discrete Logarithm Problem (ECDLP). The protocol offers better efficiency than Chow et al.'s scheme, since it does not involve bilinear pairing computations. Subsequently, several forward secure elliptic curve based protocols with public verifiability were proposed (Bala et al., 2013; Hwang et al., 2005; Hwang and Sung, 2011; Toorani and Shirazi, 2009; Xiang-Xu et al., 2005). Mohamed and Elkamchouchi (2009) proposed a forward secure, signcryption scheme with public ciphertext authentication based on ECDLP, without any pairing computations. Subsequently, similar constructions with forward secrecy and public ciphertext authentication were proposed (Iqbal and Afzal, 2013; Mohapatra, 2010). Recently, Chaudhry et al. (2016) designed an efficient e-commerce system using signcryption based on ECDLP, however, the protocol lacks forward secrecy, as well as, basic public verifiability.

1.2. Motivation

The intractability of private keys and ephemeral secrets in an algorithm, can be reduced to the intractability of the underlying hardness assumptions. The security of all the previously discussed signcryption schemes depends on individual hardness assumptions. If an attacker successfully solves the hardness assumption, he can trivially compute the private keys of individual users in the system (Gutub et al., 2017). Elkamchouchi, Nasr and Ismail (2009) proposed a forward secure proxy signcryption scheme with public verifiability, based on a combination of hard problems such as, Integer Factorization Problem (IFP) and DLP in finite fields. However, the protocol was designed using a composite modulus comprising of four primes, rendering it inefficient. The modulus size must be at least 4096 bits, to resist factoring attacks by elliptic curve method (Ciet et al., 2002; Hinek, 2008). Moreover, the protocol lacks ciphertext authentication, hence, the original message must be revealed to the external verifier for dispute redressal. In this paper, we propose a novel efficient signcryption scheme based on Conic Based RSA (CBRSA) assumption, as well as, Conic Curve DLP (CCDLP) that ensures public verifiability, ciphertext authentication, ciphertext anonymity and forward secrecy, in addition to confidentiality, authenticity, non-repudiation and integrity. Each user has a pair of private keys corresponding to CBRSA and CCDLP, respectively. An encrypted ephemeral session key can only be retrieved by the authorized recipient in possession of both the private keys. Also, a valid signature can be created only by a user in possession of both the private keys. The probability that an adversary simultaneously solves two hardness assumptions is negligible, hence, the protocol offers better security. A comparison of the security attributes of the proposed scheme with the existing protocols in the literature, is provided in Table 1. The proposed scheme is implemented on conic curves, which facilitates effective message encoding and decoding, as well as, efficient point operations and inverses, when compared to elliptic curves. We derive theorems to substantiate the security of the proposed scheme against low exponent attacks prevalent in the original RSA cryptosystem.

Table 1
Comparison of the security attributes of the proposed scheme with other signcryption schemes in the literature.

Scheme	Forward Secrecy	Public Verifiability	Ciphertext Authentication	Ciphertext Anonymity■	Public Ciphertext Authentication	Assumption
(Bao'98)	No	Yes	No	Yes	No	Gap-DH
(Gamage'99)	No	Yes	Yes	No	Yes	CDH
(Chow'03)	Yes	Yes	Yes	No	Yes	MDBDH
(Han'04)	Yes	Yes	Yes	Yes	No	ECDLP
(Hwang'05)	Yes	Yes	No	Yes	No	ECDLP
(Xiang-Xu'05)	No	Yes	No	Yes	No	ECDLP
(Xiang-Xu'05)	Yes	No	No	Yes	No	ECDLP
(Toorani'09)	Yes	Yes	No	Yes	No	ECDLP
(Elkam'09)	Yes	Yes	No	Yes	No	IFP, DLP
(Moham'09)	Yes	Yes	Yes	No	Yes	ECDLP
(Mohapat'10)	Yes	Yes	Yes	No	Yes	ECDLP
(Ahmed'10)	No	Yes	No	Yes	No	CDH
(Hwang'11)	Yes	Yes	No	Yes	No	CDH
(Bala'13)	Yes	Yes	No	Yes	No	ECDLP
(Iqbal'13)	Yes	Yes	Yes	No	Yes	ECDLP
(Chaudhry'16)	No	No	No	Yes	No	ECDLP
Our Scheme	Yes	Yes	Yes	Yes	No	CBRSA, CCDLP

■ Ciphertext anonymity and public ciphertext authentication are mutually exclusive properties.

Please cite this article in press as: Daniel, R.M., et al. A forward secure signcryption scheme with ciphertext authentication for e-payment systems using conic curve cryptography. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.02.004