A Pairing-free and Provably Secure Certificateless Signature Scheme

Arijit Karati[1], SK Hafizul Islam[2], G. P. Biswas[3]

Abstract

Certificateless Signature (CLS) scheme is a notable cryptographic technique for solving the key escrow problem in identity-based cryptosystem (IBC). In the CLS, the private key is computed collectively by both the key generation center (KGC) and the signer which ensures that no vindictive KGC masquerades the actual signer. Recently, a number of CLS schemes have been proposed using bilinear pairing and show their immunity under standard security model. It is well known that one such pairing operation requires significantly more computational cost than the other cryptographic operations. In this paper, we propose a new CLS scheme using elliptic curve cryptography (ECC), which does not require bilinear pairing operation. Our CLS scheme is analyzed formally and found to be provably secure against both the Type-I and Type-II attacks based on the intractability of elliptic curve discrete logarithm problem (ECDLP) under the random oracle model. Performance evaluation demonstrates that the proposed CLS scheme outperforms than other competitive CLS schemes.

Keywords: Digital signature, Elliptic curve, Certificateless cryptography, Random oracle model, Provable security.

1. Introduction

Traditional public key cryptography (PKC) needs additional support which is known as public key infrastructure (PKI). The authenticity of users' public key is an essential aspect and therefore, it is necessary to be satisfied prior to the secure communication. Hence, to achieve the key authenticity, PKI maintains certificates by ensuring that the user's public key is not tampered by any malicious entity. A trusted entity called certificate authority (CA) is assumed to issue and distribute the certificates by binding users' identity with their public keys. However, PKI is considered as a high computational infrastructure in the real-life scenarios due to the certificate management overhead (e.g., storage, distribution, verification, and revocation). A novel concept of IBC was proposed by Shamir [23] in 1984 to solve the aforementioned problem. The motive of that proposal was to choose a unique identity (e.g., email-id, phone-no, IP-address, etc.) of each party as their public key without being certified by the trusted authority. Besides, a trusted entity called key generation center (KGC) is considered to compute and send the participant's secret key over the secure channel. Since the KGC computes users' private key, it has all the potentials that a party can perform during the signature generation. Therefore, the KGC could act as a target entity for any attacker. This is commonly known as key-escrow problem. To resolve the aforementioned deficiency in IBC, a new cryptosystem known as certificateless public key cryptography (CL-PKC) was devised by Al-Riyami and Paterson [1]. This cryptosystem inherits the benefits of PKC as well as IBC. The CL-PKC introduced a unique idea of computing the key pair (public and private keys) by utilizing both the user's and KGC's private keys. The CL-PKC allows every user to have a private key, which is a pair of keys. One component of the pair is called secret value whereas another component is known as the partial-private-key. The secret value is selected at random by the user itself while the partial-private-key is computed by the KGC using its master secret key. In order to authenticate a message, the signature generation algorithm requires

[*] Corresponding author. (SK Hafizul Islam)

Email addresses: `arijit.karati@gmail.com` (Arijit Karati), `hafi786@gmail.com` (SK Hafizul Islam), `gpbiswas@gmail.com` (G. P. Biswas)

[1] Department of Computer Science and Engineering, NIIT University, Neemrana-301705, Rajasthan, India.

[2] Department of Computer Science and Engineering, Indian Institute of Information Technology Kalyani, West Bengal 741235, India.

[3] Department of Computer Science and Engineering, Indian Institute of Technology (ISM), Dhanbad, Jharkhand 826004, India.