An IBE-Based Authenticated Key Transfer Protocol on Elliptic Curves

Daya Sagar Gupta
https://orcid.org/0000-0001-5401-7287
Shershah College of Engineering Sasaram Bihar, India

INTRODUCTION

The twentieth century grew with the rapid development in the area of Internet and Mobile Communications Technologies/Applications, called Information and Communication Technology (ICT). ICT services have grown exponentially and become beneficial to the world in different ways. However, these technologies are changing very frequently, and several services with multimedia applications are growing through various real-life applications. In these regards, the security protection to various services becomes essential and challenging as well, and different security mechanism for different encryption, authentication, and integrity easy data availability technologies are being developed in a rapid pace. In order to design different security mechanisms and meet the challenges, different cryptographic primitives are used in their convenient waysIn the era of Internet technology; key transfer protocols are playing a crucial role in the network and information security field. These protocols are mainly incorporated to transfer a common session key among different user. The key exchanged using these protocols is generally used for symmetric key encryption where this key is known as private key and used for both encryption as well as decryption. As we all know, many key transfer protocols including basic Diffie-Hellman protocol, are proposed in the literature. However, many of these key transfer protocols either are proven insecure or had a burden of communication and computational cost. Therefore, a more secure and efficient key transfer protocol is needed. In this paper, the author proposes an authenticated key transfer protocol, which securely and efficiently negotiates a common session key between two end users. He calls this protocol as IBE-TP-AKE. This proposal is based on the elliptic-curve cryptography (ECC) and uses the idea of identity-based encryption (IBE) with pairing. The security of the proposed work is based on the hard problems of elliptic curve and their pairing extensions discussed in Gupta & Biswas (2015a), Gupta & Biswas (2015c) etc. Further, the author has shown the security of his proposed protocol and proved it using the security properties discussed later. All security properties of key exchange protocol is possessed by our proposed protocol. As we know, cryptography is a branch of science and it is an art to use security primitives in a way to deal with the security challenges and meet the solutions. Data encryption in cryptography is divided into two major categories namely, symmetric/private-key and asymmetric/public-key techniques in which the latter one has greater research impact than the former. However, the useful public-key cryptographic techniques like RSA, ElGamal etc. have some disadvantage as they require extensive public key management overheads. Thus, new technique called, identity-based encryption (IBE) is introduced recently and is used by researchers to design efficient cryptographic tools for different security applications. In this article, the author has formulated the idea of this technique to implement his protocol. Shamir (1984) has firstly proposed the novel idea of IBE by choosing the known identity of a user as public-key. This known identity may be Email, Ph. No, IP address etc. Using the

DOI: 10.4018/978-1-5225-9715-5.ch076

identity of a user as public-key, Shamir removed the overhead of certificate management from public-key cryptography. In addition, a trusted third party Private Key Generator (PKG) is considered to generate user's private key. However, the practical implementation of IBE is considered in Boneh & Franklin (2001). This proposed IBE-TP-AKE protocol includes the properties of a pairing technique as defined in Gupta & Biswas (2015b). This bilinear map relates two members of a group to a member of another group. For this particular paper, a bilinear mapping technique takes two members (points) of an elliptic curve group and maps it to a member of another multiplicative group. However, authentication to our proposed IBE-TP-AKE scheme is provided by means of the ECC. The elliptic curve hard assumptions are the hard problems which are used to efficient secure the presented protocol. The security provided by the ECC is efficient than that of RSA. A 160-bit key in ECC provides the same level of security provided by a 1024-bit key size in RSA as Gupta & Biswas (2017). The points of the elliptic curve group generate an abelian group which is used to generate the cryptographic algorithms.

BACKGROUND

Diffie and Hellman (1976) were the first who gave a new idea of having two separate keys; one for encipherment and other for decipherment. This proposal gave the birth to the key exchange protocol which is named as Diffie and Hellman (DH) key exchange protocol. Their idea was to exchange a common secret key between two authentic entities. But unfortunately, their proposal is vulnerable to a number of attacks which includes well known man-in-the-middle (MIMT) attack. To eliminate these difficulties, research has grown in this direction and many researchers have proposed different type of key transfer protocols like Liu et al. (2012), Gupta & Biswas (2016), Gupta & Biswas (2017a), Cheng et al. (2013), Gupta et al. (2018a) etc. Jeong et al. (2004) designed many two party key agreement protocols which are executed in one round of communication. They claim that the proposed protocols are authenticated and resist many attacks. McCullagh & Barreto (2005) proposed a key agreement protocol for two parties which were developed in IBE framework. They showed that their protocol is efficient and secure that other existed state-of-the-arts. They also presented the comparative analysis for their proposed key agreement scheme. Choo (2005) reviewed McCullagh & Barreto (2005) and showed that their protocols are vulnerable if the attacker has sent the *Reveal* query. Hölbl et al. (2012) devised an identity-based key exchange scheme for two parties. For their proposal, they used the pairing technique and also derived a variant of signature schemes which confirms the security of their proposal. They also claimed that their protocol is comparatively secure and cost efficient. Gupta & Biswas (2017b) proposed two secure bi-partite key agreement protocols using the IBE and pairing. The first protocol is based on the DH key agreement protocol; however the later is based on the elliptic curve group. They further extended their two party key exchange protocol for three party key exchange protocols. They showed that their protocols are secure against many attacks and claimed that these protocols exhibits better security and efficiency than other similar literatures. Tseng (2007) proposed an identity based key agreement protocol based on the hard problem of discrete logarithm. It was claimed that the computation and communication cost of his protocol is better than other competing protocols. His protocol is secure and resistance to many possible attacks. Gupta & Biswas (2018b) devised two authenticated key exchange protocol using signature and signcryption authenticators. The security of their protocols is based on the lattice hard problems. They claimed that their protocols resist the quantum attack.