Efficient Anonymous Identity-Based Broadcast Encryption without Random Oracles

Xie Li, School of Communication and Information Engineering, Shanghai University, Shanghai, China
Ren Yanli, School of Communication and Information Engineering, Shanghai University, Shanghai, China

ABSTRACT

Broadcast encryption provides a method of secure multi-receiver communications, where a broadcaster can encrypt a message for a set S of users who are listening to a broadcast channel. Most identity-based broadcast encryption (IBBE) schemes are not anonymous, which means the attacker can obtain the identities of all receivers from the ciphertext. In this paper, the authors propose an efficient anonymous IBBE scheme in bilinear groups of prime order, where any attacker cannot get the identities of the receivers from the ciphertext. The scheme has constant size ciphertext and achieves adaptive security based on the asymmetric decisional bilinear Diffie-Hellman Exponent (DBDHE) assumption without random oracles. The proposed scheme improves efficiency and security of anonymous IBBE schemes simultaneously.

Keywords: Anonymous, Bilinear Groups of Prime Order, Broadcast Encryption, Identity-Based, Without Random Oracles

INTRODUCTION

Different from the traditional encryption of point-to-point communication mode, the notion of broadcast encryption (BE) which was first realized by Fiat and Naor (1994), provides a method of secure multi-receiver communications. In a BE scheme, the sender is allowed to specify a set of receivers whoever he wants to transmit a message to, and broadcasts a corresponding ciphertext related to the specified set. A fundamental demand for a secure BE scheme is that only the specified receivers in the set can decrypt the ciphertext accurately, even if all the outside users collude (Boneh, Gentry & Waters, 2005). According to its intrinsic characteristic, BE scheme has its own application in some practical situation,
such as encrypted file sharing, digital media copyright protection, social network services (Malek & Miri, 2012; Lin, Sun, Ho & Shen, 2007; Jung, Nam, Kim, Jeon, Lee & Won, 2014) and so on.

Since the BE scheme was introduced in 1994, various BE schemes have been proposed (Zhao, 2012; Delerablée, Paillier & Pointcheval, 2007; Naor, Naor & Lotspiech, 2001). With the development of identity-based encryption (IBE) (Waters, 2005; Zhandry, 2012), the new concept of identity-based broadcast encryption (IBBE) appeared which can also be regarded as multi-receiver IBE. The IBBE construction in Baek, Safavi-Naini & Susilo (2005) achieves fast decryption in the random oracle model. Delerablée (2007) shortens the ciphertexts and private keys to constant size and proves that it is selectively secure in the random oracle model. Gentry and Waters (2009) achieves adaptive security with short ciphertexts without random oracles. Ren, Wang and Zhang (2012) proposes a dynamic IBBE scheme which realizes constant size ciphertexts and adaptive security.

To insure that all the users of the receiver set can decrypt exactly, most of the BE schemes design the set as a part of the ciphertext. It means that everyone knows all the receiver identities from the broadcasted ciphertexts. With the frequently use of digital technologies, privacy protection is gradually becoming people’s actual needs. More and more anonymous schemes appear in various fields of modern cryptography (Boyen & Waters, 2006; Li, Gu, Ren, Ding & Yuan, 2012; Katz, Sahai & Waters, 2008), and anonymous BE schemes are also included. Barth, Boneh and Waters (2006) first proposed a generic CCA recipient private construction and suggested it combine with IBE. Both of the proposed constructions reveal no information of message receivers. The decrypt time of the scheme which is secure without random oracles has a linear relation with the recipient number. Based on Barth et al (2006), Libert, Paterson and Quaglia (2012) proposes an anonymous BE scheme with efficient decryption without random oracles, but the ciphertexts is linear in the size of the receiver set.

To realize full anonymity meaning the recipient set should be removed from the ciphertext. However, it is difficult even for the legal users to decrypt without the set. Therefore, the existing schemes have to sacrifice ciphertexts length or computational costs to hide the receivers’ information in the ciphertexts. Otherwise, another compromised solution for resolving conflict between full anonymity and efficiency is outsider-anonymous schemes (Jarecki & Liu, 2007; Fazio & Perera, 2012). Outsider-anonymity means that except the users of the specified set can know the other legal receivers’ identities, all the person outside the set cannot learn any information about the receivers. Using the advantages of anonymity for better performance is the main trait of the schemes.

The similar situation also appears in IBBE schemes. Fan, Huang and Ho (2010) proposed an fully anonymous multi-receiver ID-based encryption
Image Forensics Using Generalised Benford's Law for Improving Image Authentication Detection Rates in Semi-Fragile Watermarking
www.igi-global.com/article/image-forensics-using-generalised-benford/43551?camid=4v1a

A Framework for Privacy Assurance and Ubiquitous Knowledge Discovery in Health 2.0 Data Mashups
www.igi-global.com/chapter/framework-privacy-assurance-ubiquitous-knowledge/60953?camid=4v1a