Multi-receiver Identity-Based Key Encapsulation with Shortened Ciphertext

Sanjit Chatterjee[1] and Palash Sarkar[2]

[1] Indian Institute of Science Education and Research
HC VII, Sector III, Salt Lake City
(IIT Kharagpur Kolkata Campus)
India 700106
[2] Applied Statistics Unit
Indian Statistical Institute
203, B.T. Road, Kolkata
India 700108
palash@isical.ac.in

Abstract. This paper describes two identity based encryption (IBE) protocols in the multi-receiver setting. The first protocol is secure in the selective-ID model while the second protocol is secure in the full model. The proofs do not depend on the random oracle heuristic. The main interesting feature of both protocols is that the ciphertext size is $|S|/N$, where S is the intended set of receivers and N is a parameter of the protocol. To the best of our knowledge, in the multi-receiver IBE setting, these are the first protocols to achieve sub-linear ciphertext sizes. There are three previous protocols for this problem – two using the random oracle heuristic and one without. We make a detailed comparison to these protocols and highlight the advantages of the new constructions.

Keywords: Multi-receiver encryption, identity based encryption, bilinear pairing.

1 Introduction

In a multi-recipient public key encryption scheme [4,21,5] all users use a common public key encryption system. Suppose there are n users indexed by $1, \ldots, n$; user i having public and private key pair (pk_i, sk_i). A sender who wants to send messages $M_1, \ldots, M_n$ to users $1, \ldots, n$, where M_i is intended for the user i, encrypts M_i using pk_i and sends the resulting ciphertexts $C_1, \ldots, C_n$. This general setting is referred to as multi-plaintext, multi-recipient public key encryption scheme in the literature [21]. If a single message is encrypted, i.e., $M_1 = \cdots = M_n = M$, then we get a single-plaintext, multi-recipient public key encryption scheme. In terms of functionality the later is same as a public key broadcast encryption [17,18].

Alternatively, one can send an encapsulated session key K to multiple parties, whereas the original message M is encrypted through a symmetric encryption scheme using K. In this case, the ciphertext consists of the encapsulation of K,

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 394–408, 2006.

together with an encryption of M using K. Smart [24] considered this notion of mKEM, i.e., an efficient key encapsulation mechanism for multiple parties in the KEM-DEM philosophy.

In the identity-based setting [22,9], the public key corresponding to each user is her/his identity. Given an identity v, a trusted private key generator (PKG) creates the secret key corresponding to v using its own master secret. Now consider the problem of encrypting the same message M for a large set of identities, for example in a group mail. One can either directly encrypt M or use a key-encapsulation mechanism. A trivial solution would be to encrypt (resp. encapsulate) M (resp. K) separately for each individual identities and then transmit them separately. Let the set of identities be S. Then one has to perform $|S|$ many independent encryptions/encapsulation, where $|S|$ denotes the cardinality of S. This solution is clearly too expensive in terms of bandwidth requirement as well as pairing computation.

Baek, Safavi-Naini and Susilo considered this problem in [1]. Along with a formal definition and security model for MR-IBE, they proposed a construction based on the Boneh-Franklin IBE using bilinear pairing. This protocol was proved secure in the selective-ID model *using* the random oracle heuristic. Independent of this work, Barbosa and Farshim [2] proposed an identity-based key encapsulation scheme for multiple parties. This is an extension of the concept of mKEM of Smart [24] to the identity-based setting. Their construction was inspired by the "OR" construction of Smart for access control [23] using bilinear pairing. Security of this scheme also uses the random oracle heuristic, though in the full model. A construction without using the random oracle heuristic has been described in [14]. The construction is based on the Boneh-Boyen (H)IBE [6].

Our contribution: One common limitation of all the above protocols – be it encryption or key encapsulation and whether they use the random oracle heuristic or not – is that the ciphertext size becomes large as the set S of intended recipients increase. For all three protocols, the ciphertext consists of approximately $|S|$ many elements of an elliptic curve group of suitable order.

The context of the current work is based on the following scenario.

- The sender uses a broadcast channel for transmission. Each receiver picks out the part relevant to him/her from the entire broadcast.
- Each recipient gets to know the entire set of receivers. In other words, each receiver knows who are the other persons receiving the same message.

In a broadcast transmission, it is of interest to lower the amount of data to be transmitted. Secondly, since each receiver gets to know the entire set of receivers, this set has to be broadcast along with the message. Thus, the only way of reducing the amount of transmission is by reducing the size of the ciphertext (or the encapsulation of the secret key).

In this work, we concentrate on the problem of reducing the ciphertext size in multi-receiver identity based key encapsulation (mID-KEM). We give constructions where the expected ciphertext size is a fraction of $|S|$. This, comes at