CCA2-Secure Threshold Broadcast Encryption with Shorter Ciphertexts

Vanesa Daza[1], Javier Herranz[2], Paz Morillo[3], and Carla Ràfols[3]

[1] Dept. D'Enginyeria Informàtica i Matemàtiques,
Universitat Rovira i Virgili
Av. Països Catalans 26, E-43007 Tarragona, Spain
vanesa.daza@urv.cat
[2] IIIA, Artificial Intelligence Research Institute
CSIC, Spanish National Research Council
Campus UAB s/n, E-08193 Bellaterra, Spain
jherranz@iiia.csic.es
[3] Dept. Matemàtica Aplicada IV,
Universitat Politècnica de Catalunya
C. Jordi Girona 1-3, E-08034 Barcelona, Spain
{paz,crafols}@ma4.upc.edu

Abstract. In a threshold broadcast encryption scheme, a sender chooses (ad-hoc) a set of n receivers and a threshold t, and then encrypts a message by using the public keys of all the receivers, in such a way that the original plaintext can be recovered only if at least t receivers cooperate. Previously proposed threshold broadcast encryption schemes have ciphertexts whose length is at least $n + \mathcal{O}(1)$. In this paper, we propose new schemes, for both PKI and identity-based scenarios, where the ciphertexts' length is $n - t + \mathcal{O}(1)$. The constructions use secret sharing techniques and the Canetti-Halevi-Katz transformation to achieve chosen-ciphertext security. The security of our schemes is formally proved under the Decisional Bilinear Diffie-Hellman (DBDH) Assumption.

1 Introduction

In a threshold public key encryption scheme a message is encrypted and sent to a group of receivers, in such a way that the cooperation of at least t of them (where t is the threshold) is necessary in order to recover the original message. Such schemes have many applications in situations where one wants to avoid that a single party has all the power/responsibility to protect or obtain some critical information. The usual strategy to implement this idea is the following: the set of receivers, which is decided on from the beginning, runs an interactive setup protocol which takes as input a threshold (chosen by themselves) and outputs a public key for the set and shares of the matching secret key.

The fact that the set of receivers and the threshold are set from the beginning can limit the applications of these schemes in real life. One can imagine that the sender of the message, who wants to protect some information, may want

W. Susilo, J.K. Liu, and Y. Mu. (Eds.): ProvSec 2007, LNCS 4784, pp. 35–50, 2007.

to decide who will be the designated receivers in an ad-hoc way, just before encrypting the message, and also decide the threshold of receivers which will be necessary to recover the information (e.g. depending on the secrecy level desired for the message). With this motivation in mind, a scheme for this situation would have the following properties:

1. There is no setup phase or predefined groups. Each potential receiver has his own pair of secret/public keys.
2. The sender chooses (ad-hoc) the set of receivers $\mathcal{P}$ and the threshold t for the decryption. Then he encrypts the message by using the public keys of all the receivers in $\mathcal{P}$.
3. A ciphertext corresponding to the pair $(\mathcal{P}, t)$ can only be decrypted if at least t members of $\mathcal{P}$ cooperate by using their secret keys. Otherwise, it is computationally infeasible to obtain any information about the plaintext.

Note that, when $t = 1$, the resulting scheme will be a *broadcast encryption scheme* [15], where a sender encrypts a message in such a way that any member of the set of receivers can decrypt it. For this reason, we have decided to use the name *threshold broadcast encryption scheme* (TBE scheme, for short) to refer to this kind of schemes. Other possible names could be dynamic threshold encryption (as used in [16]) or ad-hoc threshold encryption. To the best of our knowledge, very few works have dealt with this extension of the concept of broadcast encryption. In [16] the authors propose a scheme based on RSA; even if the authors claim that the length of the ciphertexts is constant, the ciphertext contains an integer modulo N, where N is the product of all the RSA moduli of the receivers. Therefore, the actual length of the ciphertext is $\mathcal{O}(n)$, where n is the number of receivers. A different scheme where the length of the ciphertexts is again $n + \mathcal{O}(1)$ is included in [17]. In [12], the authors propose a TBE scheme for identity-based scenarios; again, the length of the ciphertexts is $n + \mathcal{O}(1)$. In this same work [12], and previously in [10], a naive solution to the problem of threshold broadcast encryption was sketched: the sender distributes the message m into n pieces m_i, by using a threshold secret sharing scheme [19], and then encrypts each m_i by using the public key of the i-th receiver. The length of the ciphertext is also $\mathcal{O}(n)$.

In this paper we propose two new threshold broadcast encryption schemes, one for PKI-based scenarios and one for identity-based scenarios, where the length of the ciphertexts is $n - t + \mathcal{O}(1)$, being n the number of receivers and t the threshold for the decryption. We do not include the description of the set of receivers when we measure the length of the ciphertext; such a description can be quite short (for example, if the receivers are all the members of a company) or can be $\mathcal{O}(n)$-long, if the best/only way to describe the set is by including all the public keys of the receivers.

The idea in the design of our schemes is to combine the following tools: (1) a chosen plaintext selective-ID secure identity-based encryption scheme; (2) some secret sharing techniques to create, for each encryption, an ad-hoc master public key whose matching master secret key will be distributed among the receivers