Construction of a Hybrid HIBE Protocol Secure Against Adaptive Attacks (Without Random Oracle)

Palash Sarkar and Sanjit Chatterjee

Applied Statistics Unit
Indian Statistical Institute
203, B.T. Road, Kolkata
India 700108
{palash,sanjit_t}@isical.ac.in

Abstract. We describe a hybrid hierarchical identity based encryption (HIBE) protocol which is secure in the full model without using the random oracle heuristic and whose security is based on the computational hardness of the decisional bilinear Diffie-Hellman (DBDH) problem. The new protocol is obtained by augmenting a previous construction of a HIBE protocol which is secure against chosen plaintext attacks (CPA-secure). The technique for answering decryption queries in the proof is based on earlier work by Boyen-Mei-Waters. Ciphertext validity testing is done indirectly through a symmetric authentication algorithm in a manner similar to the Kurosawa-Desmedt public key encryption protocol. Additionally, we perform symmetric encryption and authentication by a single authenticated encryption algorithm. A net result of all these is that our construction improves upon previously known constructions in the same setting.

1 Introduction

Identity based encryption [29,8] is a kind of public key encryption where the public key can be the identity of the receiver. The secret key corresponding to the identity is generated by a private key generator (PKG) and is securely provided to the relevant user. The notion of IBE simplifies the issues of certificate management in public key infrastructure. The PKG issues the private key associated with an identity. The notion of hierarchical IBE (HIBE) [21,19] was introduced to reduce the workload of the PKG. The identity of any entity in a HIBE structure is a tuple $(\mathsf{v}_1, \ldots, \mathsf{v}_j)$. The private key corresponding to such an identity can be generated by the entity whose identity is $(\mathsf{v}_1, \ldots, \mathsf{v}_{j-1})$ and which possesses the private key corresponding to this identity. The security model for IBE was extended to that of HIBE in [21,19].

The first construction of an IBE which can be proved to be secure in the full model without the random oracle heuristic was given by Boneh and Boyen in [5]. Later, Waters [31] presented an efficient construction of an IBE which is secure in

W. Susilo, J.K. Liu, and Y. Mu. (Eds.): ProvSec 2007, LNCS 4784, pp. 51–67, 2007.

the same setting. An extension of Waters' construction has been independently described in [13] and [26]. This leads to a controllable trade-off between the size of the public parameters and the efficiency of the protocol (see [13] for details).

A construction of a HIBE secure in the full model without using the random oracle heuristic was suggested in [31]. A recent work [14], describes a HIBE which builds on [31] by reducing the number of public parameters. The constructed HIBE is secure against chosen plaintext attacks (CPA-secure).

The Problem. We consider the problem of constructing a HIBE under the following conditions.

- Security is in the full model [8], i.e., the adversary can mount an adaptive chosen ciphertext attack and can choose the challenge identity adaptively.
- The reduction is from the decisional bilinear Diffie-Hellman problem.
- The security proof does not use the random oracle heuristic.

1.1 Our Contributions

We describe a hybrid HIBE protocol for the above setting. The new construction is obtained by augmenting the construction in [14]. The idea for this augmentation is based on the technique of [9] and algebraic ideas from the construction of IBE given in [4]. In addition, we make use of two new things. First, we incorporate information about the length of the identity into the ciphertext. Second, we use symmetric key authentication to verify ciphertext well formedness. We also show that the two tasks of symmetric key encryption and authentication can be combined by using an authenticated encryption (AE) protocol.

The idea of using symmetric authentication technique to verify the well formedness of the ciphertext is based on the PKE protocol due to Kurosawa-Desmedt (KD) [25]. To the best of our knowledge, this technique has not been earlier applied to the (H)IBE setting.

We can specialize the HIBE protocol described in this paper to obtain a PKE and an IBE. With some natural simplifications, the PKE turns out to be the key encapsulation mechanism (KEM) proposed by BMW [9] composed with a one-time secure data encapsulation mechanism (DEM). On the other hand, the IBE is different from previous work. Kiltz-Galindo [24] had proposed an IB-KEM. Composed with a suitable symmetric encryption algorithm, this provides an IBE. The decryption algorithm of our IBE is faster than the IBE obtained from the KEM given in [24].

Our construction has a security degradation of approximately q^h (where q is the number of queries and h is the number of levels). This is better than a degradation of q^{h+1} which is what one would obtain by a straightforward application of the known techniques. Another advantage is that by instantiating the AE protocol with a single pass algorithm [27,22,20,12], it is possible to obtain a speed-up by a factor of two for both encryption and decryption of the symmetric part of the hybrid encryption. Also, by using the authentication aspect of the AE protocol for verifying the well formedness of the ciphertext we can avoid a number of pairing based verifications. This leads to a faster decryption algorithm.