Direct Chosen-Ciphertext Secure Hierarchical ID-Based Encryption Schemes*

Jong Hwan Park and Dong Hoon Lee

Center for Information Security Technologies(CIST),
Korea University, Seoul, Korea
{decartian,donghlee}@korea.ac.kr

Abstract. We describe two Hierarchical Identity Based Encryption (HIBE) schemes which are selective-ID chosen ciphertext secure. Our constructions are based on the Boneh-Boyen and the Boneh-Boyen-Goh HIBE schemes respectively. We apply the signature-based method to their HIBE schemes. The proposed l-level HIBE schemes are directly derived from l-level HIBE schemes secure against chosen plaintext attacks without padding on identities with one-bit. This is more compact than the known generic transformation suggested by Canetti et al..

Keywords: Hierarchical Identity Based Encryption, Chosen Ciphertext Security.

1 Introduction

Hierarchical Identity Based Encryption (HIBE) [17,16,4,5] is a generalization of Identity Based Encryption (IBE) [18,7,19,15] which allows a sender to encrypt a message for a receiver using the receiver's identity as a public key. In an l-level HIBE scheme, an identity is represented as ID-vectors of length at most l, and a private key for identity at depth $k(< l)$ can be used to derive private keys of its descendant identities. HIBE schemes could be applied to design forward-secure encryption schemes [12,20], and to convert a broadcast encryption scheme in the symmetric key setting into a public key broadcast encryption scheme [14]. Recently, Boyen et al. [11] suggested an anonymous HIBE scheme which mainly gives several application in the public key encryption with keyword search [1].

To prove the security for HIBE schemes without random oracles, Canetti et al. [12] defined a weaker security model called selective-ID security model, and proposed a HIBE scheme. Their scheme is selective-ID secure without random oracles, but that is not efficient. Later, Boneh and Boyen [4] provided an efficient HIBE (denoted by BB_1) scheme, and thereafter Boneh, Boyen, and Goh [5] presented an improved HIBE (denoted by BBG) scheme where the number of

* This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)(IITA-2006-(C1090-0603-0025)).

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 94–109, 2007.

ciphertext elements and pairing operations are independent of the hierarchy depth. These two HIBE schemes suggested by Boneh et al. were provably secure in the selective-ID model without random oracles. More recently, the techniques of constructing the BB_1 and BBG schemes were combined with a public key broadcast encryption scheme [8] in order to achieve the forward security [2].

Chosen ciphertext security of the BB_1 and BBG schemes are obtained from the generic transformation, proposed by Canetti, Halevi, and Katz [13]. The CHK transformation enables construction of an l-level HIBE scheme selective-ID secure against chosen ciphertext attacks based on any $(l+1)$-level HIBE scheme selective-ID secure against chosen plaintext attacks. The CHK transformation, improved upon by [9,10], is generic and extended to the case of adaptive-ID security model (i.e., the full security model) [6].

The CHK transformation requires one-time signature scheme to check the consistency of ciphertext. The important point is that a verification key associated with the one-time signature needs to be embedded into ciphertext in encryption procedure. For this, the authors [13] add one level to an identity hierarchy and set the verification key as an identity. Thus, the CHK transformation considered an $(l+1)$-level HIBE scheme as a subroutine in constructing an l-level HIBE scheme secure against chosen ciphertext attacks. We notice that the CHK transformation needs extra one-bit padding on identities, due to their security proof.

In this paper we construct two HIBE schemes which are provably secure against chosen ciphertext attacks in the selective-ID model. Two schemes are based on the the BB_1 and BBG schemes respectively. We apply the idea of the CHK transformation to their schemes, using one-time signature. At first sight, our constructions appear to apply the CHK transformation to the BB_1 and BBG schemes, but we obtain chosen ciphertext security of l-level HIBE schemes from l-level HIBE schemes secure against chosen plaintext attacks *directly*, without padding on identities with one-bit. Though our approach is not generic, that could be also applied to the concrete schemes [2] with structures of the BB_1 and BBG schemes.

The important algebraic property for security proofs is the one introduced by Boneh et al. [4]. Briefly speaking, for random elements g_1 and g_2 in $\mathbb{G}$ (where $\mathbb{G}$ is generated by a generator g), and random elements r_1, r_2, and r_3 in $\mathbb{Z}_p$ (where r_1 must be non-zero), we have that

$$g_2^{-r_2/r_1}(g_1^{r_1}g^{r_2})^{r_3} = g_2^{u}(g_1^{r_1}g^{r_2})^{r_3 - v/r_1}$$

where $u = \log_g g_1$ and $v = \log_g g_2$. For example, if we let $g_1 = g^a$ and $g_2 = g^b$, the value g_2^u becomes g^{ab}, and if we let $g_1 = g^\alpha$ and $g_2 = g^{\alpha^l}$, the value g_2^u becomes $g^{\alpha^{l+1}}$. The former plays a central role of proving the security of our first construction based on the BB_1 scheme, and the latter does in proving the security of our second construction based on the BBG scheme.