Formal Security Treatments for Signatures from Identity-Based Encryption

Yang Cui[1], Eiichiro Fujisaki[2], Goichiro Hanaoka[1],
Hideki Imai[1], and Rui Zhang[1]

[1] Research Center for Information Security (RCIS),
National Institute of Advanced Industrial Science and Technology (AIST), Japan
{y-cui,hanaoka-goichiro,h-imai,r-zhang}@aist.go.jp
[2] NTT Information Sharing Platform Laboratories, NTT Corporation, Japan
fujisaki.eiichiro@lab.ntt.co.jp

Abstract. In a seminal paper of identity based encryption (IBE), Boneh and Franklin [4] mentioned an interesting transform from an IBE scheme to a signature scheme, which was observed by Naor. In this paper, we give formal security treatments for this transform and discover several implications and separations among security notions of IBE and transformed signature. For example, we show for such a successful transform, one-wayness of IBE is an essential condition. Additionally, we give a sufficient and necessary condition for converting a semantically secure IBE scheme into an existentially unforgeable signature scheme. Our results help establish strategies on design and automatic security proof of signature schemes from (possibly weak) IBE schemes. We also show some separation results which strongly support that one-wayness, rather than semantic security, of IBE captures an essential condition to achieve secure signature.

1 Introduction

Identity-based encryption (IBE) [17,4] is a public key encryption scheme where a user's public key can be any bit string, such as an email address. Although IBE was originally advocated to simplify public key certificate management, it has now been shown a powerful tool constructing various cryptographic applications: key-insulated encryption, forward secure encryption and public key encryption with keyword search , etc. In this paper, we investigate another application of IBE, whose observation was attributed to Naor, saying that "*an IBE scheme can immediately be converted into a public key signature scheme*" [4].

In IBE, a *private key generator* (PKG) uses his master key msk to issue a decryption key d which corresponds to an arbitrary bit string "ID". Here, msk can also be seen as a signing key of the PKG, and by letting ID $= M$ (M is a message), d becomes the PKG's signature for M. The signature verification can be done by checking if d functions properly as a correct decryption key for identity "M" by encrypting a random plaintext and checking if the ciphertext can be decrypted to the original plaintext. We hereafter call this transformation

W. Susilo, J.K. Liu, and Y. Mu. (Eds.): ProvSec 2007, LNCS 4784, pp. 218–227, 2007.

the *Naor Transform* (NT), and denote $NT(\Pi)$ as a signature scheme derived from an IBE scheme Π via NT (A detailed description is give in Sec. 3).

1.1 IBE and Naor-Transformed Signatures

IBE. Boneh and Franklin [4] defined the security model and proposed the first full-fledged IBE, using bilinear maps and assuming random oracles. Independently, Cocks [9] also presented an IBE scheme based on the decisional quadratic residue assumption. Gentry and Silverberg [12] generalized the model of IBE with a hierarchical structure, and proposed hierarchical IBE (HIBE) schemes. Canetti, Halevi, and Katz [7] proposed an IBE whose security can be proven without random oracles but in a weaker security notion, called the selective-ID (sID) model [7]. Interestingly, sID IBE implies chosen ciphertext security (CCA) [15,16,8]. IBE The first fully secure (adaptively chosen ID secure) IBE system without random oracles was presented [3]. Waters [18] subsequently simplified the scheme from [3]. Recently, Gentry [11] presented a more efficient scheme with tight security reduction, relying on a stronger assumption.

Naor-Transfromed Signatures. Boneh, Lynn, and Shacham applied NT to the Boneh-Franklin IBE [4], and proposed the famous short signature [5]. Gentry and Silverberg proposed a hierarchical identity-based signature (HIBS) scheme from their HIBE scheme via NT [12]. Furthermore, Waters [18] presented the first (efficient) signature scheme whose security can be reduced to hardness of the computational Diffie-Hellman (CDH) problem. A subsequent paper [6] strengthened the Waters signature to have strong unforgeability.

Boneh and Franklin [4], and Waters [18] remarked (in an informal way) the security of Naor-transformed signatures: "*If IBE is semantically secure against adaptive chosen identity and adaptive chosen ciphertext attacks (*IND-ID-CCA*) [4], then the signature scheme is existentially unforgeable against adaptive chosen message attacks (*UF-CMA*) [14]*".

Posed a deeper consideration, the statement is *true*, yet with some subtle aspects that we later clarify. More importantly, since we are interested in "generic" applications of NT, we further wonder whether this statement admits of a broader interpretation. Namely, we would like to ask, for example, the following question: *What are sufficient and/or necessary conditions for underlying IBE to achieve* UF-CMA *signature*? Previous rich body of research on IBE seems not to have ready answers for such kind of "general questions". In particular, it should be noted that the security of signatures from [5,12,18,6] was analyzed individually and was very specific to their schemes.

1.2 Our Contributions

The main theoretical results are relations among security notions for IBE and signature, which are depicted in Figure 1. Our results help understand both primitive better, especially on the nature of a signature scheme with a randomized verification algorithm, which was rarely studied before. Throughout this paper,