Efficient Identity-Based Encryption with Tight Security Reduction

Nuttapong Attrapadung[1], Jun Furukawa[1,2], Takeshi Gomi[1], Goichiro Hanaoka[3], Hideki Imai[3], and Rui Zhang[3]

[1] Institute of Industrial Science, University of Tokyo, Japan
{nuts, takego}@imailab.iis.u-tokyo.ac.jp
[2] NEC Corporation, Japan
j-furukawa@ay.jp.nec.com
[3] Research Center for Information Security, AIST, Japan
{hanaoka-goichiro, h-imai, r-zhang}@aist.go.jp

Abstract. In a famous paper at CRYPTO'01, Boneh and Franklin proposed the first fully functional identity-based encryption scheme (IBE), around fifteen years after the concept was introduced by Shamir. Their scheme achieves chosen-ciphertext security (*i.e.,* secure in the sense of IND-ID-CCA); however, the security reduction is far from being tight.

In this paper, we present an efficient variant of the Boneh-Franklin scheme that achieves a tight security reduction. Our scheme is basically an IBE scheme under two keys, one of which is randomly chosen and given to the user. It can be viewed as a continuation of an idea introduced by Katz and Wang; however, unlike the Katz-Wang variant, our scheme is quite efficient, as its ciphertext size is roughly comparable to that of the original full Boneh-Franklin scheme. The security of our scheme can be based on either the gap bilinear Diffie-Hellman (GBDH) or the decisional bilinear Diffie-Hellman (DBDH) assumptions.

1 Introduction

Identity Based Encryption (IBE) provides a public key encryption mechanism where an arbitrary string, such as recipient's identity, can be served as a public key. The ability to use identities as public keys avoids the need to distribute public key certificates. Such a scheme is largely motivated by many applications such as to encrypt emails using recipient's email address or to encrypt messages for users that have not their proper key at that moment.

Although the concept of identity based encryption was proposed two decades ago [21], it is only recently that the first fully functional schemes were proposed. Boneh and Franklin [5,6] defined a security model namely IND-ID-CCA and gave the first efficient construction provably secure in the random oracle model based on the bilinear Diffie-Hellman (BDH) assumption. A few years after, new schemes were proposed and shown to be secure without random oracles, but in a weaker model of security known as "Selective-ID" model [8,2]. Such schemes in this weaker model are known to be secure also in the sense of IND-ID-CCA, but the

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 19–36, 2006.

proofs use an inefficient security reduction [2], which degrades reduction costs by a factor of the size of identities' space, which is indeed not polynomial in the security parameter. Boneh and Boyen [3] subsequently proposed the first scheme which is provably secure in the sense of IND-ID-CCA with a polynomial time reduction in the absence of random oracles, which was then improved by Waters [23].

However, for each of the above schemes, the security as in the sense of IND-ID-CCA is reduced only *loosely* to its underlying intractability assumption. An inefficient security reduction would imply either a lower security level or the requirement of larger key and ciphertext sizes to obtain the same security level.

It had been an open problem (as posed in [23,12]) whether efficient IBE systems can exist with their security in the sense of IND-ID-CCA being reduced *tightly* (*i.e.,* the factor between the difficulty of the underlying problem and the security of the scheme being only a constant term, as close to 1 as possible) to some reasonable intractability assumption. In the standard model, this problem was partially solved recently by Gentry [13], which we will discuss below.

In the random oracle model, however, essentially it has been solved using a technique by Katz and Wang [16]. However, they only introduced the key technique at the end of their paper [16], of which main topic was regarding a different subject, namely, signature schemes; hence, some thoughts were left to the reader.

Towards Achieving Tightly IND-ID-CCA-secure IBE. As a prologue to our result, we will explain that by applying the Katz-Wang technique (in order to achieve tight reduction) and the generic Fujisaki-Okamoto [10,11] transforms (in order to achieve ID-CCA security) to the basic Boneh-Franklin scheme, one would already get such a tightly IND-ID-CCA-secure scheme (or to be more precise, tightly reduced to the Gap BDH problem). We note that the only thing that we have to take into account is that we should apply the Katz-Wang technique first and then apply the Fujisaki-Okamoto transform over it. Applying in the reverse order will yield an insecure scheme (*cf.* §3).

Unfortunately, it turns out that the ciphertexts in this scheme are roughly twice as much as in the *full* Boneh-Franklin scheme and the encryption time is twice long. Recall that efficiency is one of the important motivations for designing schemes with tight security reduction. Hence the above scheme is not really a desirable result. Therefore, an important problem left to solve is to construct a tightly IND-ID-CCA-secure IBE scheme of which efficiency does not degrade much, in particular, degrades only less than twice, from the original full Boneh-Franklin scheme.

Our Contribution. Our result is a new efficient IBE scheme with a tight reduction to either the gap bilinear Diffie-Hellman (GBDH) problem or the decisional bilinear Diffie-Hellman (DBDH) problem. This is done by first (tightly) reducing the security of our scheme to the list bilinear Diffie-Hellman (LBDH) problem, which itself can be shown to be tightly reduced to the GBDH or DBDH problem.