Security of Identity-Based Encryption Algorithms

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

M. Rajakani
Mepco Schlenk Engineering College, India

INTRODUCTION

The concept of Identity Based Cryptography was proposed in (Shamir,A., 1984) which introduced the idea of using arbitrary strings such as e-mail addresses and IP Addresses to form public keys with the corresponding private keys being created by the Trusted Authority(TA) who is in possession of a system-wide master secret (Srinivasan,S.,2010). Then a party, Alice who wants to send encrypted communication to Bob need only Bob's identifier and the system-wide public parameters. Thus the receiver is able to choose and manipulate the public key of the intended recipient which has a number of advantages. While Identity Based Cryptography (IBC) removes the problem of trust in the public key, it introduces trust in the TA. As the TA uses the system-wide master secret to compute private keys for users in the system, it can effectively recompute a private key for any arbitrary string without having to archive private keys. This greatly simplifies key management as the TA simply needs to protect its master secret.

Some of the earlier Identity Based Cryptosystems proposed such as the one by Cocks (Cocks, C., 2010) and Boneh (Boneh, et.al.,2007) were not based on mathematics of pairings. The Identity based cryptosystem (the term Identity Based Cryptography refers to this set of algorithms whereas the term Identity Based Cryptosystem refers to a specific algorithm) was introduced by Boneh and Franklin (Boneh, et.al.,2001). An Identity Based Encryption or IBE (the term IBE is used to denote a specific Identity Based Cryptosystem) scheme has the following four algorithms: Setup, KeyDer, Enc and Dec. This chapter discusses the algorithms of the IBE schemes and compares them based on the implementation efficiency. An extention to the basic IBE scheme is the Hierarchical IBE proposed by Horwitz and Lynn(Horwitz, et.al., 2001).

In contrast to the basic standard model of IBE, a Random Oracle Model (Bellare, et.al.,1993) may be used where proofs of security are obtained by replacing hash functions with "Random Oracles" that output truly random values for every distinct output. This chapter discusses IBE schemes based on the Random Oracle Model IBEs and compares them with the standard model IBE.

An extension of the above schemes with multiple Trusted Authorities(TAs) instead of a single TA is also possible. An architecture for the implementation of the IBE is discussed along with the security of the various schemes.

BACKGROUND

The public key encryption is a cryptographic system that uses two keys -- a *public key* known to everyone and a *private* or *secret key* known only to the recipient of the message. When user Alice wants to send a secure message to user Bob, she uses Bob's public key to encrypt the message, Bob then uses his private key to decrypt it. An important element to the public key system is that the public and private keys are related in

DOI: 10.4018/978-1-5225-2255-3.ch431

such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key. Users will exchange public keys; this transaction does not need to be done in a secure manner because the release of public keys does not threaten the security of any private information. After this swap, someone who wishes to send private information to another user will encrypt the data with the intended recipient's public key and then pass along the encrypted message. The recipient, who will keep his or her private key secure under any circumstance, can use the private key to decrypt the encoded message.

Keys in public-key cryptography, due to their unique nature, are more computationally costly than their counterparts in secret-key cryptography. Asymmetric keys must be many times longer than keys in secret-cryptography in order to boast equivalent security. Keys in asymmetric cryptography are also more vulnerable to brute force attacks than in secret-key cryptography (Halevi,S. et.al., 1987). Public-key cryptography also has vulnerabilities to attacks such as the man in the middle attack. In this situation, a malicious third party intercepts a public key on its way to one of the parties involved. The third party can then instead pass along his or her own public key with a message claiming to be from the original sender. An attacker can use this process at every step of an exchange in order to successfully impersonate each member of the conversation without any other parties having knowledge of this deception. In order to tackle the issues surrounding the generation, distribution and safekeeping of the private and public keys and also simplify the process of obtaining the public keys, the identity based Encryption was invented.

Many different Identity Based Cryptosystems have been proposed. Some of them use the concept of a Random Oracle. A popular methodology for designing cryptographic protocols consists of the following two steps. One first designs an ideal system in which all parties (including the adversary) have oracle access to a truly random function, and proves the security of this ideal system. Next, one replaces the random oracle by a "good cryptographic hashing function" (such as MD5 or SHA), providing all parties (including the adversary) with a succinct description of this function. Thus, one obtains an implementation of the ideal system in a "real-world" where random oracles do not exist. This methodology was formulated by Bellare and Rogaway (Bellare, M., et.al, 1993) and has been used in many works.

AN IBE SCHEME

An IBE scheme is defined in terms of four algorithms *Setup*, *KeyDer*, *Enc* and *Dec*:

- **Setup:** On input 1^k outputs a master public key *mpk* which includes system parameters *params*, and a master secret key *msk*. We assume that *params* contains descriptions of the message and ciphertext spaces, *MsgSp* and *CtSp*. This algorithm is randomized.
- **KeyDer:** A Key derivation algorithm that on input *mpk* and *msk* and identifier *id*, returns a private key usk_{id}. This algorithm may or may not be randomized.
- **Enc:** An encryption algorithm that on input *mpk*, identifier *id* and a message $m \in MsgSp$, returns a ciphertext $c \in CtSp$ and is written as $c = \text{Enc}(mpk,id,m)$. This algorithm is usually randomized and if randomness is emphazised it is written as $c = \text{Enc}(mpk,id,m:r)$.
- **Dec:** A decryption algorithm that on input *mpk*, a private key usk_{id} and a ciphertext $c \in CtSp$ returns either a message $m \in MsgSp$ or a failure symbol $\perp$.