Chapter 19
Implementation of Algorithms for Identity Based Encryption and Decryption

Kannan Balasubramanian
Mepco Schlenk Engineering College, Sivakasi, India

M. Rajakani
Mepco Schlenk Engineering College, Sivakasi, India

ABSTRACT

Identity-based cryptosystems were introduced to overcome one of the main problems in public key encryption, the generation of public and private keys. In the identity-based cryptosystem, an identifier such as an e-mail address of a user can be used to generate public and private keys by a trusted third party. The trusted third party uses a system-wide master secret to provide private keys to a user. Identity-based cryptosystems can be constructed using the idea of pairings. This article discusses four different identity-based cryptosystems: the Boneh-Franklin scheme, the Cock's scheme, the Authenticated IBE scheme and the Hierarchical IBE scheme. This article also discusses the security notions considered for the identity-based cryptosystem. The security notions considered are: one-wayness, indistinguishability, semantic security and non-malleability. An architecture consisting of a public parameter server and private key generator for the implementation of the identity-based cryptosystems is also discussed.

INTRODUCTION

The concept of Identity Based Cryptography was proposed in (Shamir, 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, 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 make use of the public key of the intended recipient which has a number of advantages. While

DOI: 10.4018/978-1-7998-5351-0.ch019

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, 2010) and Boneh (Boneh et al., 2007) were not based on mathematics of pairings. The term Identity based cryptosystem (the term Identity Based Cryptography refers to the 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 IBE schemes and compares them based on the implementation efficiency. An extension to the basic IBE scheme is the Hierarchical IBE proposed by Horwitz and Lynn (Horwitz et al., 2001) is also discussed.

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 Trusted Authority 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 a 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 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.

Due to their unique nature, keys in public-key cryptography 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 provide equivalent security. Keys in asymmetric cryptography are also more vulnerable to brute force attacks than in secret-key cryptography (Halevi 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