A Survey of Identity-Based Cryptography

Joonsang Baek, Reihaneh Safavi-Naini and Willy Susilo

School of Information Technology and Computer Science
University of Wollongong

<{baek, rei, wsusilo}@uow.edu.au>

Jan Newmarch

School of Network Computing
Monash University

<jan.newmarch@infotech.monash.edu.au>

ABSTRACT

In this paper, we survey the state of research on identity-based cryptography. We start from reviewing the basic concepts of identity-based encryption and signature schemes, and subsequently review some important identity-based cryptographic schemes based on the bilinear pairing, a computational primitive widely used to build up various identity-based cryptographic schemes in the current literature. We also survey the cryptographic schemes such as a "certificate-based encryption scheme" and a "public key encryption scheme with keyword search", which were able to be constructed thanks to the successful realization of identity-based encryption. Finally, we discuss how feasible and under what conditions identity-based cryptography may be used in current and future environments and propose some interesting open problems concerning with practical and theoretical aspects of identity-based cryptography.

1. Introduction

In 1984, Shamir[30] proposed a concept of identity-based cryptography. In this new paradigm of cryptography, users' identifier information such as email or IP addresses instead of digital certificates can be used as public key for encryption or signature verification. As a result, identity-based cryptography significantly reduces the system complexity and the cost for establishing and managing the public key authentication framework known as Public Key Infrastructure (PKI).

Although Shamir[30] easily constructed an identity-based signature (IBS) scheme using the existing RSA[27] function, he was unable to construct an identity-based encryption (IBE) scheme, which became a long-lasting open problem. Only recently in 2001, Shamir's open problem was independently solved by Boneh and Franklin[8] and Cocks[15]. Thanks to their successful realization of identity-based encryption, identity-based cryptography is now flourishing within the research community.

2. Basic Concepts of Identity-Based Encryption and Signature

Basic Concept of IBE. As mentioned earlier, in the IBE scheme, the sender Alice can use the receiver's identifier information which is represented by any string, such as email or IP address, even a digital image[28], to encrypt a message. The receiver Bob, having obtained a private key associated with his identifier information from the trusted third party called the "Private Key Generator (PKG)", can decrypt the ciphertext.

Summing up, we describe an IBE scheme using the following steps. (Figure 1 illustrates a schematic outline of an IBE scheme).

- Setup: The PKG creates its master (private) and public key pair, which we denote by sk_{PKG} and pk_{PKG} respectively. (Note that pk_{PKG} is given to all the interested parties and remains as a constant system parameter for a long period.)
- Private Key Extraction: The receiver Bob authenticates himself to the PKG and obtains a private key $sk_{\mathrm{ID}_{Bob}}$ associated with his identity ID_{Bob}