Identity-Based Cryptography

Chunming Rong
Department of Electrical and Computer Engineering, University of Stavanger, Norway

Abstract

We review briefly about identity-based encryption and decryption. In 1984 Adi Shamir requested a solution for a novel public-key encryption scheme, called identity-based encryption. The original motivation for identity-based encryption was to help the deployment of a public-key infrastructure. The idea of an identity-based encryption scheme is that the public key can be any arbitrary string, for example, an email address, a name or a role. Several solutions were proposed in the following years. In 2001 the first practical and efficient scheme was proposed by Boneh and Franklin. Their encryption scheme was based on the Weil pairing on elliptic curves and proved secure in the random oracle model. In 2005, a new promising suggestion due to Waters was proposed, this time as an efficient solution without random oracles. An identity-based encryption (IBE) scheme does not need to download certificates to authenticate public keys as in a public-key infrastructure (PKI). A public key in an identity-based cryptosystem is simply the receiver's identity, e.g. an email address.

Introduction

The concept of identity-based cryptography was first proposed in 1984 by Adi Shamir [1]. In his paper, Shamir presented a new model of asymmetric cryptography in which the public key of any user is a characteristic that uniquely identifies himself/herself, like an e-mail address. In such a scheme there are four algorithms: (1) setup generates global system parameters and a master-key, (2) extract uses the master-key to generate the private key corresponding to an arbitrary public key string $ID \in \{0, 1\}^*$ (3) encrypt encrypts messages using the public key ID, and (4) decrypt decrypts messages using the corresponding private key.

Shamir's original motivation for identity-based encryption was to simplify certificate management in e-mail systems. When Alice sends mail to Bob at bob@company.com she simply encrypts her message using the public key string "bob@company.com". There is no need for Alice to obtain Bob's public key certificate. When Bob receives the encrypted mail he contacts a third party, which we call the Private Key Generator (PKG). Bob authenticates himself to the PKG in the same way he would authenticate himself to a Center of Authentication (CA) and obtains his private key from the PKG. Bob can then read his e-mail. Note that unlike the existing secure e-mail infrastructure, Alice can send encrypted mail to Bob even if Bob has not yet setup his public key certificate. Also note that key escrow is inherent in identity-based e-mail systems: the PKG knows Bob's private key.

The distinguishing characteristic of identity-based encryption is the ability to use any string as a public key. The functions that compose a generic IBE are thus specified as follows.

Setup: takes a security parameter t_s and returns t_g (system parameters) and *master-key*. The system parameters include a description of a finite message space *M*, and a description of a finite ciphertext space *C*. Intuitively, the system parameters will be publicly known, while the *master-key* will be known only to the Private Key Generator (PKG).

Extract: takes as input t_g, *master-key*, and an arbitrary $ID \in \{0, 1\}^*$, and returns a private key *K*. Here *ID* is an arbitrary string that will be used as a public key,

This paper was presented at the NIK 200x conference. For more information see http://www.nik.no/

and K is the corresponding private decryption key. The Extract algorithm extracts a private key from the given public key.

Encrypt: takes as input t_g, ID, and $m \in M$. It returns a ciphertext $c \in C$.

Decrypt: takes as input t_g, $c \in C$, and a private key K. It return $m \in M$. These algorithms must satisfy the standard consistency constraint, namely when K is the private key generated by algorithm Extract when it is given ID as the public key, then $\forall\ m \in M$: Decrypt(t_g, c, K) = m where c = Encrypt(t_g, ID, c)

The Boneh-Franklin IBE scheme

Boneh and Franklin suggested the first practical and efficient identity-based encryption scheme from the Weil pairing on elliptic curves [4]. This solution came after several not-fully satisfactory proposals [2, 3]. Some previous solutions required users not to collude, others that the Private Key Generator (PKG) spent a long time for each private key generation request. Some solutions even required tamper resistant hardware. In the same paper Boneh and Franklin also showed how an IBE scheme immediately could be converted into a signature scheme. Use of IBE was now suggested by different research communities for many different purposes [5,6,7,8].

The future is bright for the applications using Identity-Based Cryptography (IBC). We believe that IBC will help us to solve some of the problem associated with the deployment of traditional PKI. There are several more recent developments in the research of IBC, for instance the involvement of the user in generating the private-key so that the PKG may not have full access to the private-key. However, we will limit ourselves with space.

REFERENCES

[1] A. Shamir, "Identity-based cryptography and signature schemes," *Advances in Cryptology*, CRYPTO'84, *Lecture Notes in Computer Science*, vol. 196, pp. 47-53, 1985.

[2] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity", *J. Cryptology*, vol. 1, pp. 77-94, 1988.

[3] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems", In *Proceedings of CRYPTO'86*, pp. 186-194, 1986.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology*, CRYPTO 2001, *Lecture Notes in Computer Science*, vol. 2139, pp. 213-229,2001.

[5] X. Boyen, "Multipurpose Identity-based signcryption, a Swiss army knife for identity-based cryptography", in *Proceedings of the 23rd Interna. Conf. On Advances in Cryptology, Lecture Notes in Computer Science, vol.* 2729, pp. 383-399, 2003.

[6] L. Chen and C. Kudla, "Identity-based authenticated key agreement protocols from pairings", *Cryptology ePrint Archive*, Report 2002/184, http://eprint.iacr.org/2002/184, 2002.

[7] B. Lynn, "Authenticated identity-based encryption", *Cryptology ePrint Archive*, Report 2002/072, http://eprint.iacr.org/2002/072, 2002.

[8] B. R. Waters, "Efficient Identity-Based Encryption Without Random Oracles", *Cryptology ePrint Archive*, Report 2004/180, http://eprint.iacr.org/2004/180, 2004.