Studies on Identity-Based Fault-Tolerant Key Distribution Systems

Takeshi OKAMOTO

School of Information Science,
Japan Advanced Institute of Science and Technology

February 15, 1999

Keywords: ID-KDS, fault-tolerant, Diffie-Hellman, RSA, reducibility .

Cryptography is a strategy of information protection that dates back four thousand years. It is an ancient art that is taken on new significance in today's information society.

Through the ages, cryptography has protected communications while they were being transmitted through hostile environments - usually involving war or diplomacy. Especially, cryptography in World War II owed its biggest boom to the scientific mobilization. The world's first digital computers were built to crack codes at that time.

In 1949 the publication by C. E. Shannon of the paper, "Communication Theory of Secret Systems", ushered in the era of scientific secret key cryptography. Shannon provided a theory of secrecy systems almost as comprehensive as the theory of communications.

In 1977 Data Encryption Standard (DES) was published by National Bureau of Standards. The whole idea of a "standard" in cryptography is certainly revolutionary. Before the publication of DES, there apparently were no publications containing a complete algorithm for practical cryptographic usage.

The real breakthrough of the cryptography came with the publication in 1976 by W.Diffie and M.E.Hellman of their work "New Directions in Cryptography" [1]. In this paper, they proposed the concept of public key cryptography and showed that secret communication is possible without an exchange of secret key in advance, while usual symmetric cryptosystem was required for such preparations. Their splendid idea was to use two different keys, a public key for encryption and a private key for decryption. Based on this asymmetry, they further proposed the concept of digital signatures. Here, the private key is used to sign a message and the public key is used to verify a signature. However, they

did not provide realizations of the new concepts, but they proposed a protocol that allows two entities to share a common secret key only by exchanging information in public.

The concept of public key cryptography inspired many researchers, and it soon became a fast-growing and fascinating research theme. In the following years, although many realization of public key encryption and digital signature schemes were proposed, most notable one was RSA scheme. This scheme was introduced by three inventors R.L.Rivest, A.Shamir and L.Adleman who published the paper "A method for obtaining digital signatures and public key cryptosystems" [2] in 1978. This scheme was the first practical public-key encryption and digital signature schemes. Based on these primitives, more complex systems such as digital payment schemes or voting schemes were devised.

On the other hand, there are several problems in public key cryptosystems. That is, each user must have a file which contains users' public keys, and if one user wants to send a message to another, procurement of users' public keys is very costly.

To solve these problems, in 1984 A.Shamir [3] formulated the general idea of identity-based cryptosystem which is an asymmetric system employing users' identities instead of public keys, giving an example for ID-based signature system, and conceptual model for an ID-based encryption scheme. In this case, ID means information which is well-known to everyone. In ID-based systems, there are identity-based key distribution systems which are called ID-KDS for short. These systems have some advantages because they can be used not only for key distribution but also for authentication. In 1989, E.Okamoto and K.Tanaka [8] proposed a new ID-KDS which is based on the Diffie-Hellman key exchange scheme for key sharing, and which includes RSA-based authentication against impersonation.

In these days as a remarkable characteristic of modern cryptography, cryptography has been used for network security. Especially Internet which is a sort of network system, has enabled us to communicate with each other on networks which reach around the world. However, it has caused some problems such as wiretapping, forgery and impersonation, which have been getting terribly serious. Since the progress of cryptosystem is necessary to realize a secure communication, it is preferable that communication systems give users less burden and more secure environment. These things can establish practical infrastructures for network communications.

To solve these problems, we can adopt the technique of ID-KDS. Regarding this system, many useful schemes [8] - [12] are proposed up to now. These systems are efficient schemes for implementation, but they have certain drawbacks at the stage in which the center revokes and renews a user's secret information. That is, when the center revokes a user's secret information on the assumption that it is public for some reasons, the center must discard the user's ID and use the different one. To determine the ID information, it is preferable that the center adopts one uniform ID such as a user's name, an e-mail

address, or a social security number. In these systems, the user need to make a file which contains several pieces of ID for one user. Therefore, these systems impose a burden on users and lose the advantages of ID-based systems.

The concept of our proposal is as follows: Even after the center has revoked a user's secret information, the center generates a new one without any change of ID. This means that it keeps the one-to-one correspondence between users and ID's. Therefore, we must generate several pieces of secret information for a piece of ID. In this paper, we realize this concept by modifying the Okamoto-Tanaka key exchange scheme [8].

In this thesis we study the following themes:

1. We propose a new concept of identity-based cryptosystem and call this system "Identity-based fault-tolerant key distribution system".

2. To realize above concept, we propose a new scheme by modifying the Okamoto-Tanaka key exchange scheme.

3. We prove the security of the proposed scheme using reduction of functions.

4. We consider the applications of the proposed scheme to expand into other key management.

Our thesis is organized as follows.

Chapter 2 summarizes the public-key cryptosystem and shows several famous encryption and signature schemes.

Chapter 3 examines several aspects of the key management. One aspect is the importance of the keys employed by secure algorithms and methods. Another aspect is authorized key management methods.

Chapter 4 shows the overview of Turing machine at first, and indicates mathematically precise definitions for complexity classes, reductions and functions to break several protocols. This chapter also shows the ordering among difficulty of functions and finally, indicates reductions among functions. Each theorem in this chapter was proved by M.Mambo and H.Shizuya [17].

Chapter 5 shows a new concept of identity-based cryptosystem and proposes a new identity-based key distribution system. Security considerations of our proposed scheme are studied by using reductions among functions. The conceptual structure of our proposed scheme is also discussed.