International Journal of Security and Its Applications
Vol. 1, No. 1, July, 2007

A Proposal of Key Management Scheme and Its Operation Using Anonymous Biometrics on ID-based Infrastructure

Akitoshi Izumi
Dept. of Computer Science and Communication Engineering, Kyushu University
izumi@itslab.csce.kyushu-u.ac.jp

Yoshifumi Ueshige
Information Media Center, Nagasaki University
yueshige@nagasaki-u.ac.jp

Kouichi Sakurai
Dept. of Computer Science and Communication Engineering, Kyushu University
sakurai@itslab.csce.kyushu-u.ac.jp

Abstract

In the information exchange through network, the security risks always exist, that is eavesdropping, defacing, and spoofing by the attacker. PKI (Public Key Infrastructure) will prevent such attacks. But key management is very serious problem in PKI. The public key certificate is issued and distributed by certificate authority, but we think that the updating of expired certificate etc. are very costly for users. And secret key management is more serious problem. In order to solve above problems, we propose the scheme that stores protected secret key which is made by combination of biometrics and secret key in the smartcard in ID-based cryptography system. The user can restore the secret key from protected secret key by presenting his fingerprint to smartcard that has protected secret key and helper data. In our scheme, the template is not need for authentication. So, the problem of the template leakage won't arise. Lastly, we proposed the concrete operation scheme in which our scheme is used and how to make signature or authentication by applying our scheme. We show that the cost of the public key and secret key management will be reduced by using this operation scheme.

1. Introduction

We can exchange the information through the network fast thanks to rapid growth of internet. It is expected to be going to spread more and more in the future. However, when we exchange the information through the network, eavesdropping, defacing, and spoofing by the attackers exist and we must worry about such security risks.

PKI (Public Key Infrastructure) is spreading against such security risks. In PKI, the public key certificate is used to verify the validity of the public key. Generally, this public key certificate is issued and distributed by certificate authority, but interoperability of certificate authority among the different domain is indicated as one problem. Also we think that the updating of expired certificate is very costly for the user. The user must get the CRL (Certificate Revocation List) from CA.

The management of secret key is more serious problem than that of certificate for the user. For example, for assuring of validity of the digital document, the digital signature is used

which the function is provided by PKI. The validity of digital signature depends on the fact that the secret key which made that signature is held by only possessor. Consequently, theft or loss of the secret key means the collapse off validity of the digital signature made by that secret key so far.

As above, in the public key cryptography, the public key and the secret key must be managed by safe and proper procedure. The cost for user who uses public key cryptography will be reduced by the attempt on efficiency of that management. For this reason, we propose the scheme that stores protected secret key which is made by combination of biometrics and secret key in the smart card in the system which used ID-based cryptography. By using user's biometrics information, we can protect the user's secret key.

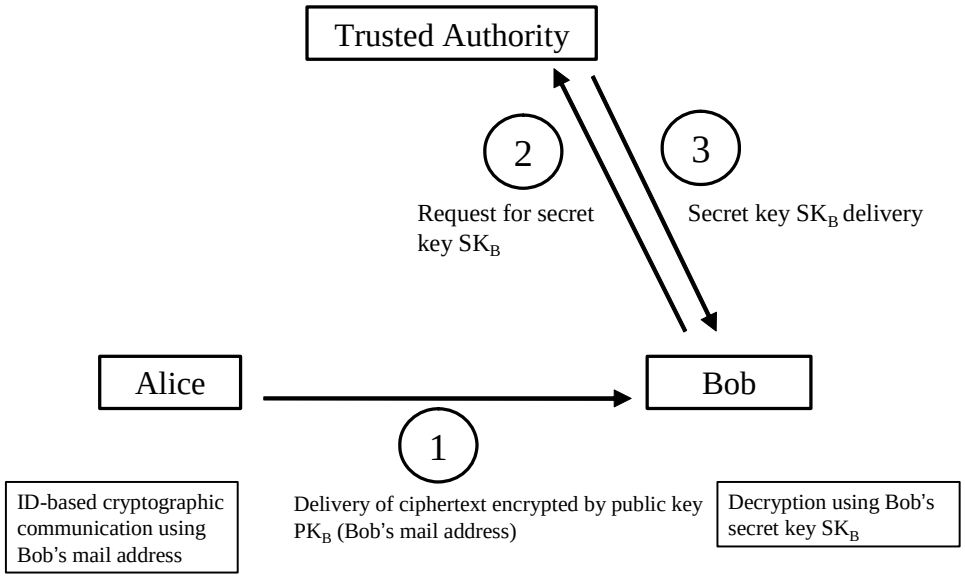


Figure1. ID-based cryptography communication

The ID-based cryptography is a scheme that can use ID of receiver as a public key. So, if the receiver's ID can be easily guessed or already known, we can verify the validity of receiver's public key and reduce the cost of user's key management without using the public key certificate that that traditional PKI has used. In the ID-based cryptography, user's secret key is deposited with the organization that is called TA (Trusted Authority). Therefore the user authentication and the secret key delivery must be done safety and the proper procedure when the user needs his secret key. We propose the ID-based cryptography infrastructure scheme which delivers the secret key using the smart card which has protected secret key protected by user's biometrics information and helper data which is used to correct the error of biometrics information.

In our scheme the template is not stored as reiterated information in smart card at authentication, so a template leakage problem to a biometrics authentication can be solved. In

the use of the above-mentioned method, we try to reduce the cost of management of public key and private key.

The composition of this paper is as follows. In the second section, the ID-based cryptography which is used in our scheme as public key infrastructure is outlined, in the third section, after showing a general biometrics authentication, we introduce the token type fingerprint authentication device and anonymous biometrics for a helper data as a relation research. And in the fourth section, we propose our scheme and compare our scheme with a traditional token type scheme. In the fifth section, we propose the operating a concrete public key infrastructure that uses our proposal scheme. In sixth section, I propose signature and authentication scheme using our scheme. Lastly, we conclude this paper at the section7.

2. Verification of public key validity

In the cryptosystem that uses the public key cryptography, it is extremely important to guarantee that the public key is really owners. For example, we assume that Alice communicates with Bob by using the public key cryptography. Here, Bob(s public key is PKB. Alice should obtain Bob's public key PKB before the cryptographic communication is started. However, the Bob's public key PKB might be replaced with the Charlie's public key PKC by attacker Charlie. If Alice doesn't notice this fact, the message encrypted with Charlie's public key PKC will be read by attacker Charlie. In PKI that uses a traditional public key cryptography, to prevent such a man-in-the middle attack, the certificate authority is set. The validity of the public key is guaranteed by issuing the public key certificate that is added digital signature of certificate authority.

Thus, the validity of the public key can be proven by using the public key certificate. The expiration date is generally installed in the certificate, and the updating of the certificate will force the load on the user. Moreover, there is a case where the certificate is revoked by losing the secret key at the expiration date. In such a case, confirmation of certificate revocation list distributed by certificate authority by user or, confirmation with OCSP (Online Certificate Status Protocol) is needed. Such tasks become a load of the user. And operation cont of certificate authority or interoperation of certificate authority among the different domain is indicated as one problem. The management of the certificate becomes a large cost for the user. For this reason, the ID-based cryptography is advocated as a cryptography that guarantees the validity of the public key without using the certificate.

2.1. Public key management using ID-based cryptography

The concept of the ID-based cryptography was proposed by A.Shamia in 1984 [1], and a concrete scheme was proposed by D.Boneh and M.Franklin in 2001 [2]. The ID-based cryptography is a cryptography that can use arbitrary ID like receiver's e-mail address directly as a public key. Therefore, the relation of the public key and the owner can be guaranteed, it is not necessary to use the certificate, and the cost of certificate management can be gone away.

Generally, TA (Trusted Authority) that generates user’s secret key is set up (Figure 1). Therefore, when the user needs his secret key, it is necessary to demand the delivery of his secret key from TA. For example, we think about the ID-based cryptography situation which Alice uses Bob’s ID as public key. Alice can transmit the ciphertext encrypted by using Bob’s

ID to Bob. After receiving the ciphertext from Alice, Bob demands his secret key SKB to TA for decrypting that ciphertext. After user's authentication is appropriately done by some methods, it is necessary to delver his secret key by the safe procedure. Thus, it is called an escrow problem to deposit the secret key with the third party. It is a very difficult problem to authenticate by proper procedure and to deliver the secret key by safe way for TA when the infrastructure that uses the ID-based cryptography is actually operated. The concrete authentication and the delivery method when the secret key is delivered are proposed in our scheme.

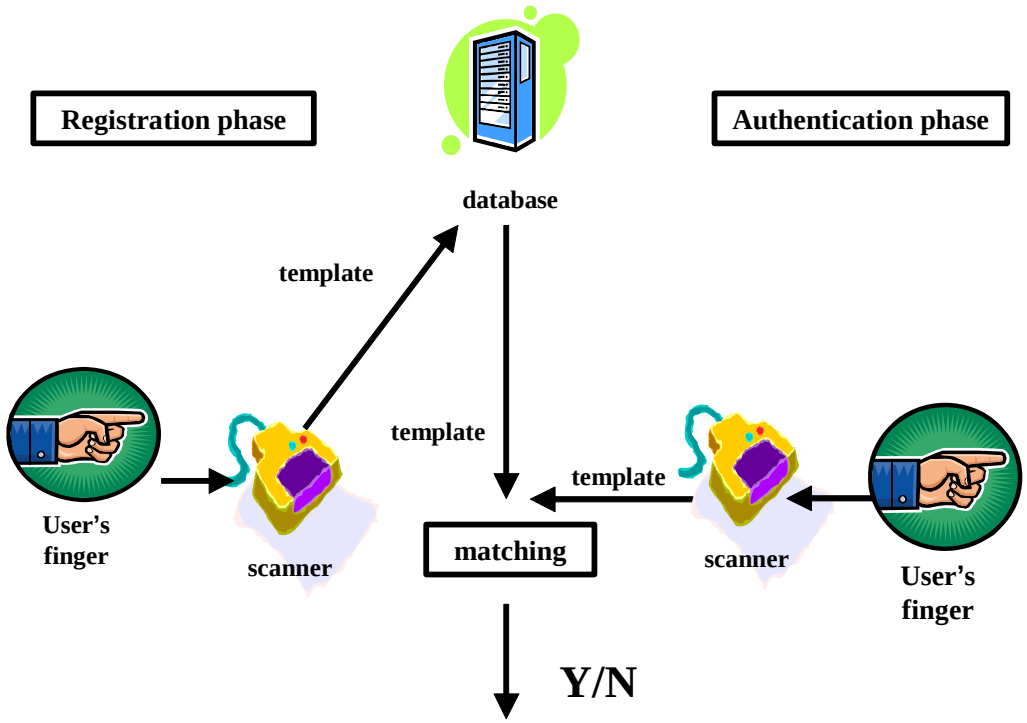


Figure2. Biometrics authentication

3. Biometrics

In the biometrics authentication, after extracting features (from fingerprint, iris, voice, etc.), the similarity is evaluated between data bases of the feature (template) registered in advance. If the similarity is high enough, it is attested the person in question Figure 2.

In this paper, we propose the authentication and the private key management system that uses the fingerprint authentication token system applied anonymous biometrics [5].

3.1. Fingerprint authentication token system

The fingerprint authentication token system is researched and developed as a password keeping tool only for the individual [3],[4]. This token has the fingerprint sensing and authentication function.

The fingerprint authentication is recognized as a standard keyboard when it connected with the USB connector of PC, and the fingerprint data obtained through fingerprint sensing is compared with the registration fingerprint data which is kept in the token in advance. If the similarity is high enough, the token transmits the password from token to PC.

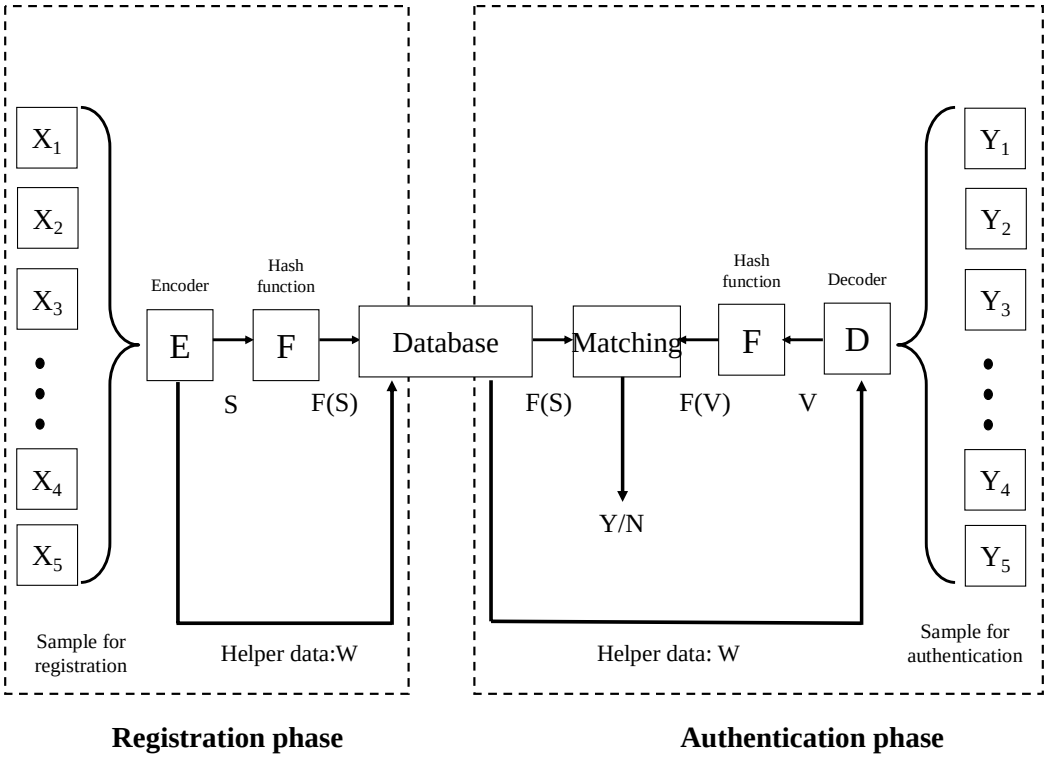


Figure3. The general form of anonymous biometrics

3.2. Anonymous biometrics

The template is generated from biometrics information through the feature extraction processing. The feature extraction processing is conversion into the template that extracts only a part of useful information from the biometrics information. It was thought impossible that the inversion of biometrics information from the template because it was not able to decide it uniquely so far [6]. However, it was shown to be able to generate the artificial finger that can be authenticated from the fingerprint template only [7]. The anonymous biometrics is from such a background as a research on the template protection.

The general form of anonymous biometrics that uses helper data is shown by Tuyles (Figure 3). When registering feature vector S and helper data W are generated from registration sample $X_i(i=1,...,N)$ with encoder E in Figure 3. The feature vector S is transformed into $F(S)$ through the hash function. It makes the presumption of S form $F(S)$ by using the hash function impossible.

Then, decoded result V can be the same data as feature vector S by the error correction of authentication sample Y by using helper data W. The same fingerprint data is needed in this proposal scheme when the protected private key is registered and the private key is extracted.

4. Registration of protected secret key and extraction of secret key using anonymous biometrics

In this chapter, we show the scheme of making protected private key and extracting secret key from protected secret key by applying anonymous biometrics to secret key management. Our scheme is composed of the protected secret key registration phase and the secret key registration phase, the input value is user's biometrics sample and user's secret key. The output value is the protected secret key and the helper data. In the secret key extraction phase, the input value is the protected secret key and the helper data and user's biometrics sample. The output value is user's secret key.

We compare our scheme with the traditional token type fingerprint authentication system; we show that the private key can be protected without depending on a tamper resistance.

4.1. Prerequisite

Smart card used in this model is assumed to have biometrics reading function, memory to store the helper data W and protected secret key $P(SK)$, operation function functions necessary for encoding, hash, XOR operation. Here, P is the function to protect user's secret key, and SK means user's secret key. And, it is assumed that an operation and biometrics reading are done in smart card in figure 4.

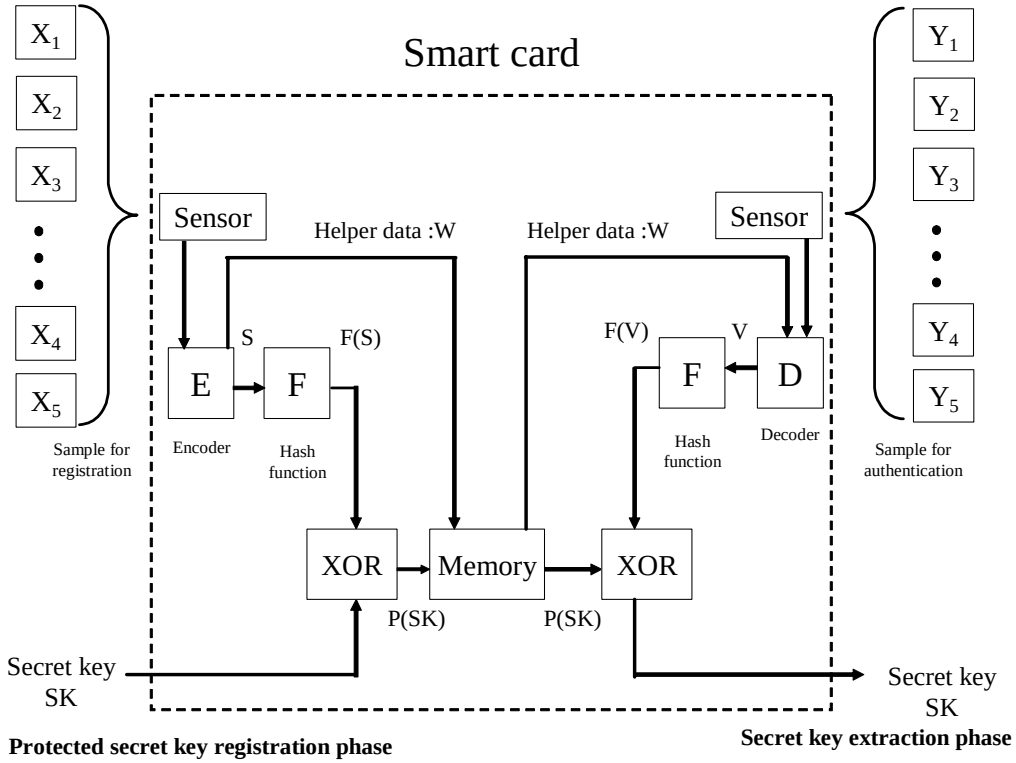


Figure 4. Registration of protected secret key and extraction of secret key using anonymous biometrics

4.2. Protected secret key registration

The input to smart card when the protected secret key is biometrics sample $X_i(i=1,...,N)$ and secret key $SK \in \{0,1\}^n$. Encoder E generates feature vector S and helper data W from the biometrics sample X_i. The feature vector S is transformed into $F(S) \in \{0,1\}^n$ by hash function F. It is impossible to presume S from $F(S)$ or W. Afterwards, exclusive-OR (XOR) of secret key SK and $F(S)$ is computed, the value is called protected secret key $P(SK)$ and this value is stored in memory with helper data W.

$$SK \oplus F(S) = P(SK) \tag{1}$$

Storage on smart card of protected secret key $P(SK)$ and helper data W ends by operating the above mentioned.

4.3. Secret key extraction

When the private key is extracted, the input to smart card is biometrics sample $Y_i(i=1,...,N)$. Decoder D generates feature vector V from helper data W stored in smart card and input value $Y_i(i=1,...,N)$. Feature vector V is transformed into $F(S) \in \{0,1\}^n$ by using hash function F which is same as when the protected secret key was registered. Afterwards, if $F(S)$ and $F(V)$ are same value, by computing exclusive-OR(XOR) of protected secret key $P(SK) \in \{0,1\}^n$ and $F(V) \in \{0,1\}^n$, the secret key SK is restored.

$$P(SK) \oplus F(V)(= F(S)) = SK \tag{2}$$

By operating the above-mentioned, the secret key can be extracted from protected secret key.

4.4. Security discussion

Here, we discuss about security of our scheme. We assume that the smart card is stolen by the attacker and he can access information inside of the token.

First, we discuss the attack to recover the biometrics information which can be authenticated validly and to extract some useful information from helper data. The mutual information between helper data and biometrics information is almost 0 [5]. Therefore, it is impossible for the attacker to recover some useful information or biometrics information which can be authenticated validly.

Secondly, we discuss the attack to recover the secret key from protected secret key. Making the protected secret key is synonymous with making the ciphertext by the Vijunel type cryptography with a key to the same length as the plaintext on $GF(2)$.Therefore, it is impossible to recover the secret key from protected secret key.

Lastly, we discuss the attack to recover the valid biometrics information from helper data and attacker's biometrics information. To make this attack succeed, the attacker's biometrics information must be similar enough to valid biometrics information. So, we can prevent such an attack by set the threshold as similarity. Furthermore, we can prevent this kind of attack

with high probability by making the authentication stop if the person failed his authentication once or twice. Therefore, attacker can't obtain the secret key or valid biometrics information from stolen smart card.

4.5. Comparison between fingerprint authentication systems with proposed method

The fingerprint authentication token system is template matching system which keeps the template as registration information in the memory of token. If input biometrics information and template are same enough, the token outputs the password registered in advance outside. This system depends on tamper resistance which makes it impossible to extract template from the token. However, it is not easy to achieve a perfect tamper resistance. Especially, the storage method that depends on a tamper resistance is undesirable if it sees from the viewpoint of long-term operation. Therefore, it is necessary to think of reconstruction of biometrics information from stolen template that can be used for authentication by the attacker when the token is lost or stolen. On the other hand, our method makes protected secret key from secret key by using biometrics information and makes helper data for biometrics information at registration, and stores them in smart card. When the secret key is extracted, we can recover the biometrics information which is same as the registration time by applying helper data to input. We can extract the secret key by computing the exclusive-OR of the protected secret key and the recovered biometrics information. In our scheme, the information stored in smart card is only helper data and the protected secret key. It is impossible to recover the biometrics information that can be used for authentication from helper data. Making the protected secret key is synonymous with making the ciphertext by the Vijunel type cryptography with a key to the same length as the plaintext on , so it is impossible to recover the secret key from protected secret key.

Therefore, in our scheme, from inside information, recovering of the data that can be authenticated and the secret key are impossible. To protect secret key, there is no need for depending on a tamper resistance like an existing method.

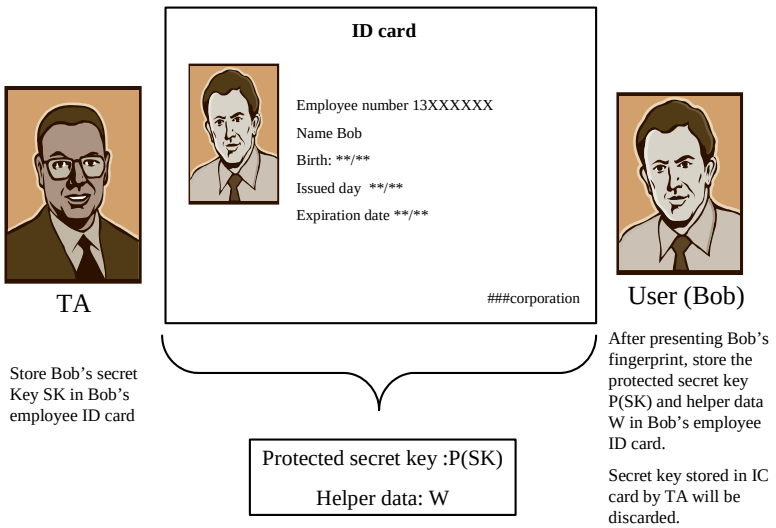


Figure 5. Making of a smart card by TA and registration of user's protected secret key

5. Proposal of concrete operation method

The user's secret key is made by TA in the infrastructure that uses the ID-based cryptography. Therefore user must deposit him secret key with TA. The problem concerning an appropriate authentication when the delivery of secret key is requested from TA and a safe delivery method is called an escrow problem.

In this section, in ID-based infrastructure, we propose a concrete scheme to register protected secret key and to extract secret key that uses the anonymous biometrics proposed in section 4. And, it is shown that the escrow problem of the ID-based infrastructure can be solved by using our scheme. Lastly, out scheme improves the efficiency of the public key and secret key management of the user.

In ID-based infrastructure, the public key and the receiver can be related without using the certificate because we use receiver's ID directly as a public key. Therefore, the cost concerning the management of the certificate by the user can be greatly reduced. The user's ID is used directly as a key in the infrastructure that used the ID-based cryptography, the environment in which we already know or easily guess ID is necessary.

Then, in this paper, we discuss about small network like a company in which we already know or easily guess ID is necessary.

The smart card used in this model has some functions which is biometrics reader and is memory to store the helper data W and protected secret key $P(SK)$, and is computation function to compute XOR and hash and encoding and decoding. We use this smart card as employee ID card.

In our scheme, the user's secret key generated by TA will be delivered to user through the process similar to the method of delivering a usual employee ID after be stored in smart card. The authentication method to the employee ID card will be done in a usual company (photograph of face description and presentation of ID card, etc.)

The user received the employee ID card can generate protected secret key from secret key and can extract helper data,, and can store both with smart card by presenting fingerprint information in the employee ID card through the process similar to the protected secret key registration denoted in section 4.2. When the user extracts the secret key form smart card, the secret key can be extracted only by presenting fingerprint information to smart card that is stored his protected secret key and helper data. This operation is same as secret key extraction denoted in section 4.3.

The fingerprint authentication token system stores the template in the token, and outputs the password stored in advance by matching template and biometrics information if the tamper resistance was broken, so there was danger for which the artificial finger that able to be used to authenticate from template is made.

The information stored in smart card is only a protected secret key and helper date in our scheme. Making the artificial finger that can be authenticated and the extraction of the secret key are impossible.

6. Digital signature generation and authentication

In this chapter, we describe digital signature generation and authentication in our scheme.

6.1. Second-order headings

In general signature scheme, the signer makes a message digest through hash function and encrypts this digest by him secret key. This encrypted digest is digital signature.

We can generate the digital signature in our scheme if we attach a hash and encryption function to smart card. Figure 6 shows the signature generation procedure. Here f is the function to generate the message digest.

1. The message is inputted into smart card.
2. The signer present him biometrics sample $Y_i(i=1,...,N)$ to smartcard.
3. The decoder D generates the feature vector V from presented biometrics sample $Y_i(i=1,...,N)$ and helper data W stored in smart card in advance.
4. In the smart card, the feature vector V is inputted to the hash function F and hash function outputs $F(V)$.
5. The XOR value of $F(V)$ and protected secret key $P(SK)$ is computed. This is the user's secret key.
6. The digest message generated in (1) will be encrypted by secret key SK, and outputted as the digital signature.

The user's secret key must be discarded securely.

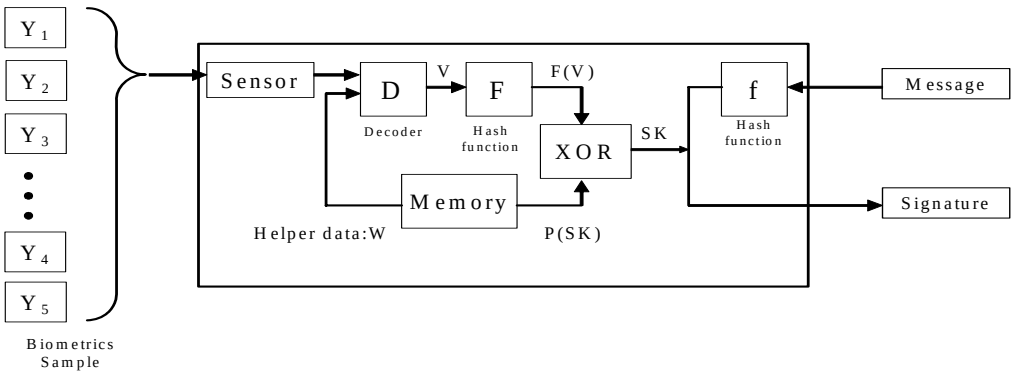


Figure 6. Digital signature generation in our scheme

6.2. Authentication

Authentication is the technique that can prevent impersonation. In this section, we present the authentication system in which we set different password to each computer.

Generally, it is difficult for users who use some computers to remember different passwords. In such a case, our secret key management scheme is very efficient for users. I show concrete example as follows.

First, the user presents the cipher text which is encrypted by his public key to the computer which he will make an authentication (Figure7). We define PW_n as a password to computer. The computer n stores $PK(PW_n)$. Here, $PK(PW_n)$ is encrypted PW_n by user's public key PK.

When the user makes an authentication to the computer, first, he presents the smart card to the computer. Then the computer passes $PK(PW_n)$ to the smart card. The user will present his biometrics sample to the smart card, and he can recover his secret key SK from protected secret key $P(SK)$. The ciphertext $PK(PW_n)$ will be decrypted in the smart card by the secret key SK. The authentication will be done by presenting PW_n to computer form smart card. Only the owner of smart card can make an authentication successfully because he is only the person to recover the secret key.

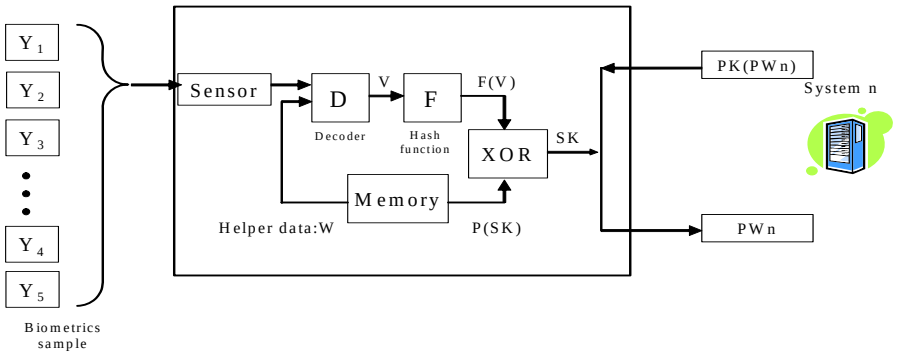


Figure 7. Authentication in our scheme

7. Summary and future work

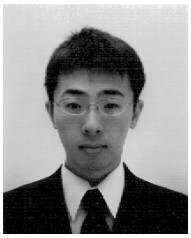
In this paper, we proposed the scheme to keep the protected secret key that is generated form user's biometrics information and secret key in the smart card. Also, we proposed concrete operation scheme. And we showed that the safety of the secret key is kept without depending on a tamper resistance and by using our scheme and showed that the system with high convenience of the key was able to be constructed. In the future works we examine whether the convenience of PKI in a large scale network can be enhanced by applying our scheme.

8. References

[1] A.Shamir,"Identity-Based Cryptography and Signature Schemes", Proceeding of CRYPTO'84, pp.4-53, 1984
[2] D.Boneh and M Franklin, "Identity-Based Encryption from the Weil Pairing", Proceedings of CRYPTO2001, pp.213-229, 2001
[3] Shutoh, Shigematsu, Hatano, Yamaguchi, Okazaki, Machida "Fingerprint authentication system", NTT Technological journal2003.12, pp43-46
[4] Sony fingerprint authentication system, http://www.sony.co.jp/Products/puppy/
[5] Tuyls P., Goseling J., "Capacity and examples of template-protecting biometrics authentication systems ", ECCC Workshop BioAW, no.77,2004
[6] International Biometric Group, "Generating Images from Templates", I.B.G. White Paper, 2002

[7] Hill C.J., "Risk of masquarade arising from the storage of biometrics", Bachelor thesis, Dept. of CS, Australian National University, 2002

Authors



Akitoshi Izumi

Received the B.E degrees from School of Engineering Kyushu University in 2007. From 2007 he is a student of master's course in Department of Computer Science and Communication Engineering, Kyushu University.

Yoshifumu ueshige

Received the B.E., M.E., and D.E. degrees from Kyushu Institute of Technology in 1992, 1994 and 1998, respectively. From 1997 to 2002 he worked at Kagoshima National College of Technology. In 2003 he was invited researcher at Kitakyushu Foundation for the Advancement of Industry, Science and Technology.
From 2004 to 2006 he worked at Institute of Systems & Information Technologies/KYUSHU as researcher.
From 2007 he works at Nagasaki University as associate professor. His research field includes image processing, and secure online biometric authentication. He is a member of IEICE, ITE, IPSJ, ACM, and IEEE.

Kouichi Sakurai

Received the B.S. degree in mathematics from Faculty of Science, Kyusyu University and the M.S. degree in applied science from the Faculty of Engineering, Kyushu University in 1986 and 1988, respectively. He had been engaged in the research and development on cryptography and information security at Computer and Information Systems Laboratory at Mitsubishi Electric Corporation from 1988 to 1994. He received the Dr. Degree in engineering from Faculty of Engineering, Kyushu University in 1993. Since 1994 he has been working for Department of Computer Science of Kyushu University as an associate professor, and now he is a full professor from 2002. His current research interests are in cryptography and information security. He is a member of the Information Processing Society of Japan, the Mathematical Society of Japan, ACM, IEEE and the International Association for Cryptologic Research.