

Mechanism-based PKI

- A real-time key generation from fingerprints -

Yoichi Shibata
Graduate School of
Science and Engineering
Shizuoka University
Hamamatsu-shi,
Shizuoka, JAPAN
cs9042@s.inf.shizuoka.
ac.jp

Masahiro Mimura
Hitachi, Ltd.,
System Development
Lab., Kawasaki-shi,
Kanagawa, JAPAN
mmimura@sdl.hitachi.
co.jp

Kenta Takahashi
Hitachi, Ltd.,
System Development
Lab., Kawasaki-shi,
Kanagawa, JAPAN
kenta@sdl.hitachi.co.jp

Masakatsu Nishigaki
Graduate School of Science
and Technology
Shizuoka University
Hamamatsu-shi, Shizuoka,
JAPAN
nishigaki@inf.shizuoka.ac.jp

Abstract - *This paper proposes a "mechanism-based PKI", in which only a mechanism for generating user's private keys is installed on a smart card. The private key is generated inside the smart card at the event that the legitimate user gives a "seed of private key" to his/her smart card in order to sign a message. The key exists nowhere except while users are signing a message. Thus, users no longer need to pay considerable attention to their smart cards. In addition, this paper also proposes a "statistical A/D conversion", which is an effective scheme to convert fingerprint to just one and the same ID in real-time. The statistical A/D conversion enables us to use fingerprint as a seed of private key. We construct an example system for real-time key generation from fingerprint. From some basic experiments that we carried out, the availability of the system is confirmed.*

Keywords: biometrics, fingerprint, key generation, PKI, digital signature

1 Introduction

With the advancement in information technology, e-commerce and e-banking have become an integral part of our life. In particular, various e-commerce services using mobile phone are becoming very hot topic in the business world now.

In e-commerce, where any consensual validation by face-to-face interaction is impossible, the validity of contract has to be certified by digital signature based on Public Key Infrastructure (PKI). Here, the length of private key that is used in digital signature is too long to memorize, for example more than 1024 bits for RSA encryption, and the key should be updated at suitable intervals. Therefore, we need private keys to be stored in a secure device in some form.

This means that user authentication over PKI is not based on "who he/she is" but "what he/she has". In other words, if an attacker could steal someone's device which keeps user's private key, the attacker can impersonate the

someone. In addition, if a user loses his/her device, the user will get into a serious problem.

This paper proposes a "Mechanism-based PKI" in which only a mechanism to generate user's private key is installed on a smart card. The private key is generated inside the smart card at the event that the legitimate user gives a "seed of private key" to his/her smart card in order to sign a message. The key exists nowhere except while users are signing a message. Thus, users no longer need to pay considerable attention to their smart cards.

In this paper, as an example, user's fingerprints are used as the "seed of private key", and a prototype system for real-time key generation from fingerprint is shown. Here, this paper also proposes a "statistical A/D conversion", which is an effective scheme to convert fingerprint to just one and the same ID in real-time.

2 Mechanism-based PKI

2.1 Digital signature without keeping private key

Generally, a pair of private key and public key is generated by a certificate authority (CA) in advance, and then the private key is securely kept in user's mobile device. Here, private keys are so important that the mobile devices need to be tamper-resistant and protected with password/biometrics. For instance, the literature [1] has proposed to protect private keys in a smart card by fingerprint. The private key will not be activated unless the authentic fingerprint is given to the smart card.

However, some studies have recently reported that information in smart cards could be readable with high precision by side-channel attacks [2]. Although we could harden the resistance of smart cards against the side-channel attacks, attackers may also refine their techniques or even find new vulnerability. As long as a private key is kept in the device, there will be possibility that it is

analyzed. Hence, it is desirable that digital signature can be generated without keeping private key in any device.

To achieve that, this paper proposes a "Mechanism-based PKI" in which only a mechanism to generate user's private key is installed on a smart card. In the Mechanism-based PKI, digital signature is carried out by the following steps:

- (1) When a user signs a message, the user inputs his/her "seed of private key" to his/her device.
- (2) His/her private key is generated inside the device.
- (3) The message is signed with the private key in the device.
- (4) Immediately, the private key is removed from the device.

The key exists nowhere except while users are signing a message. Thus, users no longer need to pay considerable attention to their smart cards, and attackers can not obtain any information about the private key from the smart card.

It is noted that the algorithm (mechanism) to generate private keys must be public. In other words, any private key generated by the algorithm is supposed not to be revealed as long as the seed of private key is kept secret.

2.2 A seed of private key

Although we guess that we could use anything as a seed of private key, we are thinking of biometrics as one of suitable candidates. Especially, this paper describes to use fingerprints as a seed of private key.

However, most of biometric characteristics are analog quantities. Hence, measurement errors are inescapable when biometric data are scanned. When the noisy measurement data are quantized into discrete values, the outcome of quantization may differ from scanning. In particular, if some biometric data are values close to a quantization threshold, minor amounts of noise can change the outcome. For instance, the literature [3] has reported that when 2,048 bits iris code is extracted, about 172 bits are noisy. Also, in the literature [4], the keys generated from pen input information are not completely the same. To realize the mechanism-based PKI, a scheme to convert biometrics to just one and the same private key is essential.

The literature [5] has studied a private key generation from DNA. DNA would be easier to convert a private key since DNA itself is a digital code. But, a real-time DNA extraction is infeasible so far. Unless a real-time key generation is impossible, we can not use it as a seed of private key. The real-timeness is one more important issue in the mechanism-based PKI.

3 Digital signature in Mechanism-based PKI

This section shows a concrete system of digital signature in the Mechanism-based PKI. The system described here is one example.

3.1 Specifications

The specifications for this example system are given below:

- User's fingerprints are used as a seed of private key.
- It is assumed that the images of fingerprints are not easily stolen.
- There are storage area and working area in a smart card. The data in working area are removed as soon as used.
- The mechanism to generate private keys from fingerprints is installed in the smart card.
- Signature algorithm is implemented in the smart card. When a message and the authentic fingerprint are fed to the smart card, the smart card then outputs the signed message.
- ElGamal signature scheme is used, which means that random number generator is implemented in the smart card.
- There are CAs based on the existing PKI.

3.2 Fingerprint registration

First of all, the legitimate user is required to register his/her fingerprint. In the registration, a private key is generated from user's fingerprint and then the corresponding public key is made from the private key. The user needs to register the public key along with the user information to a CA. If the CA can verify the authenticity of the user, the CA issues a public key certificate to the user. The procedures in the registration phase is described as below, and depicted in Fig.1. In the following explanation, all data are stored in the working area in the smart card and removed as soon as used, unless described as "stored in storage area".

- (1) A user inputs his/her finger to a smart card. The smart card scans the fingerprint.
- (2) The fingerprint is converted to an ID by the statistical A/D conversion. (The detailed explanation of the statistical A/D conversion is addressed in Section 4.)
- (3) The user inputs random number PN to the smart card. The number is stored as the pass number in storage area in the smart card.
- (4) ID and PN are concatenated to yield $ID|PN$, where "|" stands for concatenation.
- (5) The user's private key x is generated by feeding $ID|PN$ to a hash function H . That is, $x=H(ID|PN)$. The user can generate a different private key from the same

fingerprint by changing the pass number.

- (6) The public key is generated by $y = g^x \text{ mod } p$.
- (7) The smart card sends the public key y , p and g along with the user information to a CA.
- (8) The CA verifies the authenticity of the user. If OK, the CA issues a public key certificate to the user's smart card.
- (9) The smart card stores the public key certificate in the storage area.

Now the legitimate user is ready to sign a message.

When the public key certificate has been expired, the user is required to renew his/her private key by changing the pass number and to updated public key certificate.

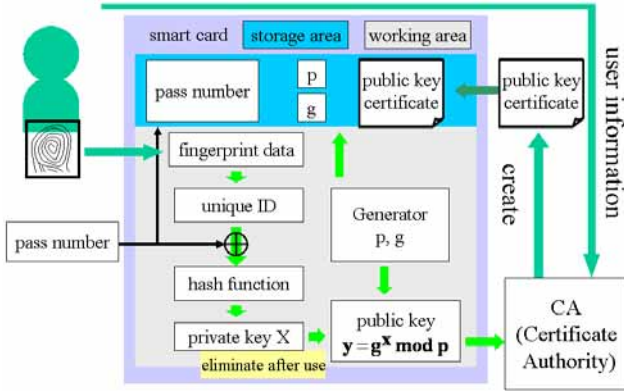


Figure 1. Key registration in Mechanism-based PKI

3.3 Message signing

When a user is going to sign a message, the user inputs his/her fingerprint and the message to his/her smart card. In the smart card, the user's private key is generated and the message is signed with the private key. The message signing is described as below, and depicted in Fig.2. In the following explanation, all data are stored in the working area in the smart card and removed as soon as used, unless described as "stored in storage area".

- (1) A user inputs his/her finger to his/her smart card. The smart card scans the fingerprint.
- (2) The fingerprint is converted to an ID by the statistical A/D conversion. (The detailed explanation of the statistical A/D conversion is addressed in Section 4.)
- (3) The ID is concatenated with a pass number PN stored in the storage area in the smart card to yield $ID|PN$.
- (4) The user's private key x is generated by feeding $ID|PN$ to a hash function H . Here, we can obtain the same private key $x=H(ID|PN)$ every time, since the statistical A/D conversion can always convert the legitimate user's fingerprint to the same ID.
- (5) A random number r is generated in the smart card. Then, the smart card calculates $a = g^r \text{ mod } p$ and $s = x^{-1} (H(m)a - r) \text{ mod } p-1$, where m is a message to be signed, g and p are the public parameters listed in the

public key certificate stored in the storage area, and $H(-)$ is a hash function. The a and s are the digital signature of the message m .

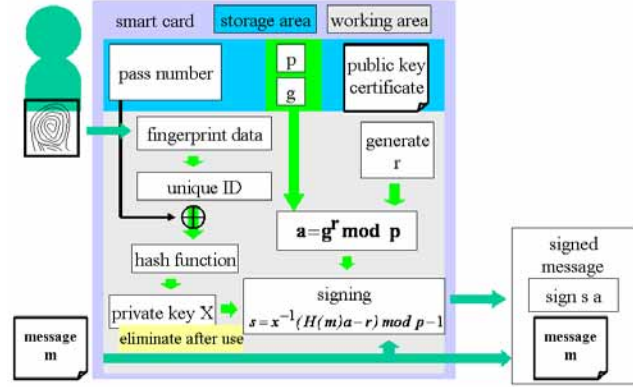


Figure 2. Message signing in Mechanism-based PKI

3.4 Signature verification

Anyone who receives the signed message (m, s, a) and the public key certificate (y, g, p) from the user can verify the authenticity of the message, by checking $y^s a = g^{h(m)a} \text{ mod } p$.

3.5 Remarks

In the proposed system, any smart card keeps only the public key certificate and the pass number. The private key exists nowhere except while users are signing a message. In addition, the compatibility of the Mechanism-based PKI with the existing PKI is one more big advantage. Thus, the benefits below are obtained:

- (1) Even if the smart card is stolen and the pass number is revealed by an attacker, the attacker can not sign a message without the legitimate user's fingerprint.
- (2) The user no longer needs to pay considerable attention to his/her smart card. Even if the card is lost or stolen, the user can buy a new smart card and regenerate his/her private key just by carrying out again the registration procedure with another pass number.
- (3) The public key certificate in the proposed system is identical to that of the existing PKI.
- (4) When a public key certificate is revoked or expired, the user can obtain new certificate just by remaking his/her private key with another pass number and registering it to a CA.

4 ID extraction from fingerprint

4.1 Key generation from fingerprint

In this paper, user's fingerprint is used as a seed of private key. However the features extracted from the fingerprint could not be identical from scanning to scanning, since measurement errors are inescapable when the fingerprint is scanned. In particular, if some feature of

fingerprint is a value close to a quantization threshold, minor amounts of noise can change the outcome of quantization. Even one bit change in the cryptographic key will result in an entirely different output of encryption. This makes it difficult to make any cryptographic key from fingerprint. Fingerprint will never be used as a seed of private key unless we can convert fingerprint to just one and the same ID in real-time.

4.2 Statistical A/D conversion

Value of a feature extracted from a fingerprint, V , would not be identical from scanning to scanning. However, it is expected that the distribution of V for the legitimate user is probably localized to a certain authentic region, while the distribution of V for all users is usually widespread. This paper proposes to exploit this property to convert fingerprint to just one and the same ID in real-time. That is, authentic feature distribution analysis is introduced into A/D conversion. We refer this modified A/D conversion as “statistical A/D conversion”. The followings are outline of the statistical A/D conversion.

- Template generation (Registration of fingerprint)
 - (1) Legitimate user A is required to have A's fingerprint scanned more than once. In this paper, user's fingerprint is scanned 10 times. The 10 fingerprint images of the one finger would differ from scanning to scanning.
 - (2) Value of feature V is extracted from each fingerprint images.
 - (3) Mean \bar{e} and standard deviation $\tilde{\sigma}$ of V over 10 fingerprints of the finger of the legitimate user A are calculated.
 - (4) Authentic region of V over 10 fingerprints, $[\bar{e} - n\tilde{\sigma}, \bar{e} + n\tilde{\sigma}]$, is determined, where n is a security parameter. If we can assume that V is normally distributed, the authentic region may include about 99.7% of V when $n = 3$.
 - (5) All the feature space is divided into regions with the same size as the authentic region. This gives the regions $\{[\bar{e} - (2i - 1)n\tilde{\sigma}, \bar{e} + (2i + 1)n\tilde{\sigma}] \mid i = 0, \pm 1, \pm 2, \dots\}$.
 - (6) For $i = 0, \pm 1, \pm 2, \dots$, random number r_i is generated and assigned to every regions $[\bar{e} - (2i - 1)n\tilde{\sigma}, \bar{e} + (2i + 1)n\tilde{\sigma}]$ as “region-ID”.
 - (7) The region boundaries $\{\dots, \bar{e} - 5n\tilde{\sigma}, \bar{e} - 3n\tilde{\sigma}, \bar{e} - n\tilde{\sigma}, \bar{e} + n\tilde{\sigma}, \bar{e} + 3n\tilde{\sigma}, \bar{e} + 5n\tilde{\sigma}, \dots\}$ and region-IDs $\{r_i \mid i = 0, \pm 1, \pm 2, \dots\}$ are stored in the A's smart card as template $T(V^A)$.
- A/D conversion (Extracting ID from fingerprint)
 - (1) Legitimate user A is required to have A's fingerprint scanned once. Note that only registration phase requires the user of multiple scanning of one finger to generate template by the authentic feature distribution

analysis.

- (2) Value of feature V is extracted from the fingerprint image.
- (3) The region including V is searched from template $T(V^A)$. Now suppose that V is included in the region $[\bar{e} - (2L - 1)n\tilde{\sigma}, \bar{e} + (2L + 1)n\tilde{\sigma}]$. Then the corresponding region-ID, r_L , is recognized as the authentic region-ID. Actually, for the legitimate user A, it is highly expected that V falls within the authentic region $[\bar{e} - n\tilde{\sigma}, \bar{e} + n\tilde{\sigma}]$, thus r_0 would be almost always extracted as authentic region-ID. On the other hand, the authentic region-ID would not be obtained when someone else tries to extract ID using A's template, since the feature value V for the someone else's fingerprint could be different from that for A. Even if the value of a feature for someone else's fingerprint is close to that of A, the value of another feature could be different each other.

It is difficult for adversaries to guess the authentic region-ID, unless they obtain both of fingerprint and the template. Therefore, if we can assume that fingerprint could not be stolen, the template information can be opened. On the other hand, in the situation where adversaries could steal fingerprint, it is better to keep the template secret.

Actually, the number of the fingerprint features is more than one. Now suppose that we are using M features. Then, the feature values are expressed as a vector $\mathbf{V} = \{V_1, V_2, \dots, V_M\}$, and the template is as $\mathbf{T}(\mathbf{V}^A) = \{T(V_1^A), T(V_2^A), \dots, T(V_M^A)\}$, where $T(V_j^A)$ is composed of the boundary information for V_j , $\{\dots, \bar{e}_j - 5n_j\tilde{\sigma}_j, \bar{e}_j - 3n_j\tilde{\sigma}_j, \bar{e}_j - n_j\tilde{\sigma}_j, \bar{e}_j + n_j\tilde{\sigma}_j, \bar{e}_j + 3n_j\tilde{\sigma}_j, \bar{e}_j + 5n_j\tilde{\sigma}_j, \dots\}$, and the corresponding region-IDs, $\{\dots, r_{j-2}, r_{j-1}, r_{j0}, r_{j1}, r_{j2}, \dots\}$. Here, \bar{e}_j , $\tilde{\sigma}_j$ and n_j are the mean, standard deviation and security parameter of V_j , respectively. When the legitimate user A tries to extract ID, the values of every V_j usually fall within each authentic region $[\bar{e}_j - n_j\tilde{\sigma}_j, \bar{e}_j + n_j\tilde{\sigma}_j]$, thus the authentic ID, $r_{10}|r_{20}|r_{30}|\dots|r_{M0}$, would be almost always obtained, where “|” stands for concatenation.

The authentic ID is obtained from fingerprint only when all the authentic region-IDs, $\{r_{j0} \mid 1 \leq j \leq M\}$, can be extracted correctly. In other words, one wrong region-ID results in failure of fingerprint ID extraction. Therefore, if the number of the fingerprint features can be sufficiently large, it would be acceptable to set every security parameters $\{n_j \mid 1 \leq j \leq M\}$ as big as needed to achieve a small FRR (false rejection rate) of ID extraction. Of course bigger security parameters, which gives wider authentic regions $\{[\bar{e}_j - n_j\tilde{\sigma}_j, \bar{e}_j + n_j\tilde{\sigma}_j] \mid 1 \leq j \leq M\}$, will help to convert someone else's feature values to the authentic region-IDs. However, it is expected that if M becomes sufficiently large, the legitimate user A would be the only person who can obtain all the authentic region-IDs when

A's template is used for ID extraction. This means that FAR (false acceptance rate) would also be kept low. Larger M contributes to make the bit length of the extracted ID longer, too.

It is note that statistical A/D conversion would be applicable to ID extraction not only from fingerprint but also from any biometric data.

4.3 Related work

To our knowledge, there are two kinds of approaches to achieve extraction of just one and the same ID from biometrics. One of them is error-correction-based approach. Another scheme is statistical-analysis-based approach.

Fuzzy commitment proposed by Juels et al. [6] is an error correcting algorithm for ID extracted from biometric or other noisy data. Juels et al. have also proposed the subsequent study, fuzzy vault [7]. In general, error correcting code has the error correcting capability proportional to the size of parity bits, P . Therefore, these schemes could always convert the legitimate user's biometric data to the authentic ID with high accuracy, by using an error correcting code with P chosen to be large enough. However, a larger P would also help to correct IDs extracted from someone else's biometric data. This means that these schemes might give a higher FAR (False acceptance rate) when keeping FRR (False rejection rate) low.

A statistical-analysis-based approach is further classified into post-learning scheme and pre-analysis scheme.

Monrose et al. [8] have proposed a post-learning scheme that extracts ID from voice. The scheme determines region boundaries (thresholds) for voice feature vector quantization without any statistical analysis in enrollment phase. Every region contains a share of ID as produced by a secret sharing scheme [9]. Then, how often and which region each feature value falls within is measured in authentication phase. When we can find any region within which a feature never falls over time, the region is recognized as a junk legion. After that, the share for the junk region is replaced by a random value. These random values should disturb only impersonators.

The scheme proposed in this paper is a pre-analysis scheme. Coincidentally, the similar schemes have been studied also by Soutar et al. [10], Feng et al. [11] and Chang et al. [12]. Although the basic concept of them is identical, there exists the following difference to our scheme. Soutar's scheme, which was applied to extract ID from fingerprints, carries out authentic feature distribution analysis in frequency domain. Feng's scheme uses a shape matching as a preprocessing for ID extraction from on-line

handwritten signatures. This means that a hybrid-type algorithm of the conventional matching and a statistical-based matching could be effective to some biometric data. In Chang's scheme, to achieve ID extraction from face images, principal component analysis was performed on images to reduce the feature dimension, and then authentic feature distribution analysis was done.

5 Experimental results

In this section, we have constructed an example system for real-time key generation form fingerprint. We have carried out some basic experiments to evaluate the availability of our scheme.

5.1 Extraction of feature values

This system has used Veridicom 5th Sense as fingerprint reader. Fingerprint image is 300×300 pixels and gray scale. The system divides fingerprint image into small blocks, and uses ridge orientation of every blocks as features of fingerprint. The feature extraction is carried out as follows:

- (1) The position and orientation of fingerprint image are adjusted. In this system, alignment is done by maximizing the number of minutiae correspondences¹.
- (2) The fingerprint image is divided into blocks of size 16×16 pixels. This system uses the middle 8×8 blocks.
- (3) For $1 \leq p, q \leq 8$, ridge orientation of the (p, q) block is extracted as feature value V_{pq} . In this system, the algorithm described in Sec.2.4 in the literature [13] is used for extraction of ridge orientation.
- (4) By setting $j = 8p + q - 8$, the feature vector $\{V_j \mid 1 \leq j \leq 64\}$ is obtained from $\{V_{pq}\}$.

5.2 Extraction of ID

In this experiment, the followings have been evaluated.

- (1) FTAR: Failure to acquire rate.
- (2) FNMR: False non match rate.
- (3) FRR: False rejection rate (FNMR+FTAR).
- (4) FAR: False acceptance rate.
- (5) Length of ID: The bit length of ID extracted from a fingerprint. For instance, let us consider that the boundaries for V_j are $\{0^\circ, 45^\circ, 90^\circ, 135^\circ\}$. This means that V_j has four regions, $[0^\circ, 45^\circ)$, $[45^\circ, 90^\circ)$, $[90^\circ, 135^\circ)$ and $[135^\circ, 180^\circ)$. In this case, region-ID of V_j is 2 bits.

¹ Although no explanation was given in Sec.4.2, one fingerprint image is selected as a reference in the registration phase and the location data (x and y coordinates) of minutiae points for the reference fingerprint are stored in the legitimate user's smart card as well as the user's template. The position and orientation of fingerprint image are adjusted by using the location data.

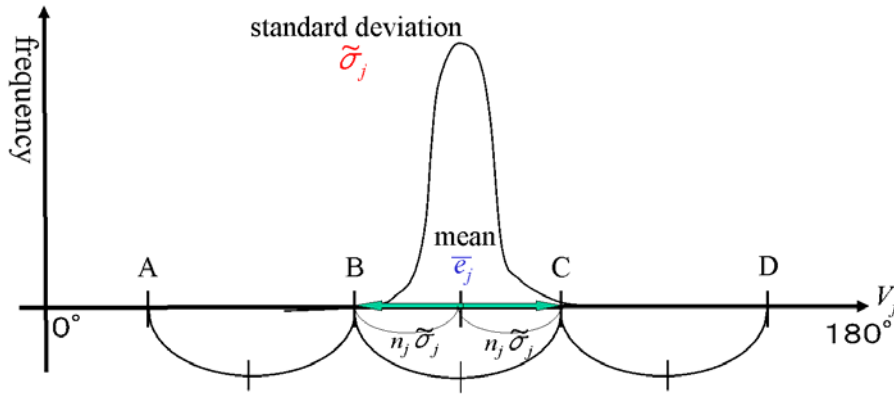


Figure 4. Authentic feature distribution analysis

When the bit length of ID extracted from V_j is d_j , the length of ID extracted from $V = \{V_1, V_2, V_3, \dots, V_M\}$ is

$$\sum_{j=1}^M d_j \text{ bits.}$$

- (6) Number of the non-used blocks: In this system, each feature space (ridge orientation of every blocks) is from 0° to 180° . Hence, if $2\bar{e}_j\tilde{\sigma}_j$ is over 90° , it is easy for adversary to guess the authentic region-ID for V_j from template. So, such V_j is not used in this system.

At the beginning of the experiment, we have asked 12 university students to let us scan their fingerprints. We have scanned every finger of each student, and refer them as Finger 1 ~ 120. 90 scans for all fingers have been gotten. Thus totally 10,800 fingerprint images (12 students x 10 fingers x 90 scans) are obtained.

The experimental procedure is as follows. In this system, authentic feature distribution analysis in the template generation phase is done with 10 fingerprint images.

- (1) 90 fingerprint images of Finger 1 are divided into two groups. Group 1 includes 10 images for template generation. Group 2 includes 80 images for FRR evaluation.
- (2) Template for Finger 1 is generated from 10 fingerprint images in Group 1. Figures 3 and 4 depict the template generation and authentic feature distribution analysis. Here, to measure the effect of n_j , we generate seven templates with different value of n_j ; a template with $n_j=2.0$, a template with $n_j=3.0$, ..., a template with $n_j=8.0$, respectively.
- (3) To evaluate FRR for Finger 1, IDs are extracted from 80 fingerprint images in Group 2 of Finger 1 using each template generated in (2). The bit length of IDs and the number of non-used blocks are also calculated.
- (4) To evaluate FAR for Finger 1, IDs are extracted from all the fingerprint images of Finger 2 ~ 120 using each template generated in (2). Totally 10,710 fingerprint images (119 fingers x 90 scans) are checked. Figure 5

- depicts the ID extraction in (3) and (4).
 (5) (1) ~ (4) are repeated for Finger k , $2 \leq k \leq 120$.

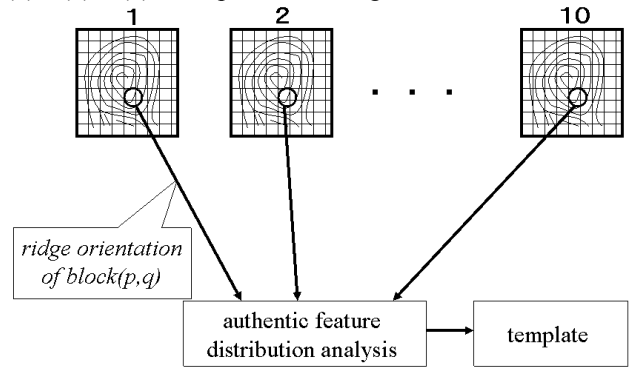


Figure 3. Template generation

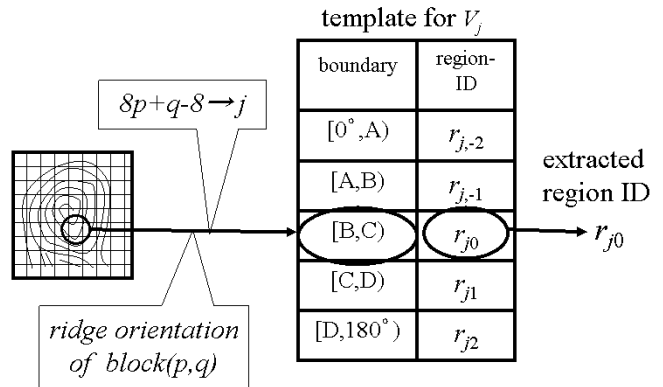


Figure 5. ID extraction

The results are shown in Table 1. For FRR, actually we have to keep both FTAR and FNMR low. However, immediate aim of this paper is to evaluate the availability of statistical A/D conversion. That is why, this paper excludes FTAR, which is the frequency of error that occurred in preprocessing phase (alignment phase in Sec.5.1), from the evaluation at the moment, and focuses on FNMR only. Judging from Table 1, it has been confirmed that when $n_j=6.0$ or 7.0 , both of FAR and FNMR become as low as around 5%.

Table 1. Experimental Results

n_j	3.0	4.0	5.0	6.0	7.0	8.0
FTAR	0.374	0.373	0.376	0.378	0.384	0.383
FNMR	0.177	0.116	0.072	0.063	0.050	0.039
FRR	0.485	0.446	0.421	0.417	0.415	0.408
FAR	0.006	0.013	0.031	0.046	0.061	0.073
Length of ID	151.407	132.435	102.098	95.949	75.094	70.843
non used block	58.708	56.283	53.892	51.367	48.917	46.567

6 Conclusions

This paper has proposed mechanism-based PKI, in which only mechanism for key generation and message signing is implemented in a smart card. The private key is generated inside the smart card at the event that the legitimate user gives a seed for private key to his/her smart card in order to sign a message. The key exists nowhere except while users are signing a message. Thus, users no longer need to pay considerable attention to their smart cards. In addition, we have proposed statistical A/D conversion, which is an effective scheme to convert biometric data to just one and the same ID in real-time. This paper has constructed an example system for real-time key generation from fingerprint. From some basic experiments that we carried out, the availability of the system has been confirmed.

7 References

- [1] Shuichi ISHIDA, Masahiro MIMURA, and Yoichi SETO, "Development of Personal Authentication Techniques Using Fingerprint Matching Embedded in Smart Cards," IEICE Trans. Inf. & Syst., Vol. E84-D, No.7 2001.
- [2] Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzer and Stephane Tinguely, "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards," IEEE Sym. on Security and Privacy, 2002.
- [3] John Daugman, "How Iris Recognition Works," IEEE Conf. on ICIP, 2002.
- [4] M. Akao, S. Yamanaka, G. Hanaoka and H. Imai, "Cryptographic Key Generation from Pen Input Information," SCIS2003 (Symposium on Cryptography and Information Security 2003), pp. 299-304, 2003. (in japanese)
- [5] Y. Itakura and S. Tsujii, "Proposal on Personal Identifiers Generated from the STR Information of DNA," IJIS (International Journal of Information Security) Vol.1 No.3, Springer, Berlin Heidelberg NewYork, 2002
- [6] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," ACM CCS 1999, 1999.
- [7] A. Juels and M. Sudan, "A fuzzy vault scheme," IEEE Int. Symp. Information Theory, p. 408, 2002.
- [8] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel. "Cryptographic Key Generation From Voice," IEEE Conf. on Security and Privacy, 2001.
- [9] Adi Shamir, "How to share a secret," Communications of the ACM, 22(1), pp. 612–613, 1979.
- [10] C. Soutar, D. Roverge, A. Stoianov, R. Gilroy and B. V. K. Vijaya Kumar, "Biometric Encryption™," Chapter 22 in ICSA Guide to Cryptography, edited by Randall K. Nicholls, pp. 649-675, 1999.
- [11] H. Feng and C. C. Wah, "Private Key Generation from On-line Handwritten Signatures," Information Management & Computer Security, vol. 10, no. 4, pp. 159-164, 2002.
- [12] Y. J. Chang, W. Zhang. and T. Chen, "Biometric-based cryptographic key generation," IEEE Conf. on Multimedia and Expo 2004 Taipei, Taiwan, 2004.
- [13] Lin Hong, Yifei Wan and Anil Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", IEEE Trans. on pattern analysis and machine intelligence, Vol.20, No.8, pp.777-789, 1998.