PCA-CIA Ensemble-based Feature Extraction for Bio-Key Generation

Aeyoung Kim[1], Changda Wang[2], and Seung-Hyun Seo[3*]
[1] Research Institute of Engineering & Technology, Hanyang University Erica
Ansan, Gyeonggi-do 15588 - Korea
[e-mail: aeyoung@hanyang.ac.kr]
[2] School of Computer Science and Communication Engineering, Jiangsu University
Zhenjiang 212013 - China
[e-mail: changda@ujs.edu.cn]
[3] Devision of Electrical Engineering, Hanyang University
Ansan, Gyeonggi-do 15588 - Korea
[e-mail: seosh77@hanyang.ac.kr]
*Corresponding author: Seung-Hyun Seo

Received December 9, 2019; revised April 4, 2020; accepted May 13, 2020; published July 31, 2020

Abstract

Post-Quantum Cryptography (PQC) is rapidly developing as a stable and reliable quantum-resistant form of cryptography, throughout the industry. Similarly to existing cryptography, however, it does not prevent a third-party from using the secret key when third party obtains the secret key by deception, unauthorized sharing, or unauthorized proxying. The most effective alternative to preventing such illegal use is the utilization of biometrics during the generation of the secret key. In this paper, we propose a biometric-based secret key generation scheme for multivariate quadratic signature schemes, such as Rainbow. This prevents the secret key from being used by an unauthorized third party through biometric recognition. It also generates a shorter secret key by applying Principal Component Analysis (PCA)-based Confidence Interval Analysis (CIA) as a feature extraction method. This scheme's optimized implementation performed well at high speeds.

Keywords: Face Image-based Seed, Feature Extraction Ensemble, Bio-Key Generation, Biometric Cryptography, Multivariate Quadratic-based Post-Quantum Cryptography

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1A6A3A01013588), by the National Research Foundation of Korea through the Korea Government under Grant 2018R1A2B6006903, and by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2020-2018-0-01417) supervised by the IITP (Institute for Information & Communications Technology Promotion).

http://doi.org/10.3837/tiis.2020.07.011 **ISSN : 1976-7277**

1. Introduction

High speed Post-Quantum Cryptography (PQC) is the latest cryptographic technique to have been actively studied regarding the emergence of quantum computers, which threaten the security of the industry's existing cryptosystems [1]. Existing cryptographic algorithms such as RSA (Rivest-Shamir-Adleman) and ECDSA (Elliptic Curve Digital Signature Algorithm) are no longer secure, because they are based on the difficulty of factorization or discrete logarithm problems, which can be decrypted by quantum computers [2]. Therefore, there is a growing need for a new public key cryptography techniques that are resistant to the quantum computation of quantum computers, and quantum resistant cryptographic algorithms are being actively researched.

In particular, National Institute of Standards and Technology (NIST) is conducting a competition to create the standard for quantum resistant cryptosystems, which would be safer and more secure for quantum computation, to provide stable and reliable quantum-resistant cryptography throughout the industry [3-4]. NIST has classified into three detailed algorithms for quantum resistant cryptosystems: encryption, key exchange, and signature. The basic building blocks for designing quantum resistant cryptographic algorithms are lattice, code, hash, and multivariable quadratic (MQ). Among building blocks, the MQ signature algorithm shows faster performance than that of the existing RSA and ECDSA [5-6]. The representative MQ signature algorithm, the rainbow signature scheme (with Quantum Security Level 128-bit), is 145 times faster than RSA regarding signature generation, and is three times faster than ECDSA. It is also two and seven times faster for signature verification than these alternatives, respectively [7].

However, similarly to existing encryption algorithms, the quantum-resistant cryptographic algorithm does not prevent a third party from acquiring the encryption key by deception, unauthorized sharing, or unauthorized proxying of the key. The most effective alternative to prevent unauthorized third-party use of cryptographic key-based security solutions, such as digital signatures and encryption algorithms, is the utilization of biometrics within existing crypto systems [8-10].

Biometrics such as face, iris, and fingerprints, can be used for user authentication because they are unique characteristics that cannot be separated from the original user. However, biometrics consist of unstable information obtained with different values from noise images. This is true even though the same part of the same person is repeatedly acquired many times at short intervals, using the same device, under the same conditions. In conventional cryptosystems, as input values having a difference of one-bit can lead to a very large difference for authentication, the most important problem for generating the key from the biometrics is finding a scheme that can stably reproduce the exact bit string that looks random using the noisy input [11-13].

The fuzzy extractor proposed by Dodis et al., comprises one of the representative studies for solving this problem. It generates a key from biometrics such as face images, so that it can be applied to any cryptographic algorithm [12]. However, the proposed fuzzy extractor has high computational complexity for getting a (P, f (R)) pair, and requires a very large space (units of Giga- or Tera-) to store the P and f(R), which are extracted from biometrics as helper data (R is the key) [14]. Given these biometrics, generating a key that is both sufficiently long and strong from biometrics is a major problem; in our proposed scheme it is referred to as the entropy loss problem. To solve this problem, Fuller et al. proposed a model using the learning with error

(LWE) problem [15]. Cheon et al. also applied the LWE problem to the model proposed by Canetti et al. to solve this problem, creating models with more acceptable P and $f(R)$ storage sizes [14], [16-17]. In addition to the fuzzy extractor, there is another way, which uses quantization based on intervals to map a continuous set, as biometrics, to a countable smaller set, as indexes of each interval. However, the key generation schemes based on this quantization are not as feasible as those of the fuzzy extractor approach.

Unlike a general biometric-based key generation model that can be applied to any cryptographic algorithms, Conti, et al. proposed BiometricRSA, which is a model for generating private keys from some images of two fingerprints stored on smart cards. This model maps a prepared large prime number list for targeting RSA [18]. Thus, models for generating a secret key for a specific cryptographic algorithm, like RSA, have been proposed. Most of these models are simple mapping or linking methods, similar to BiometricRSA. It is not easy to find a representative study because their proposals do not provide a reasonable and concrete method [18-21]. Minhye Seo et al. proposed a new biometric-based key derivation function for enhancement of the authentication system by the replacement of password-based key derivation functions [22]. Some researchers have tried to use other noise sources such as Physical Unclonable Function and image link, but these results are also insignificant [23].

As a result, out of these biometric-based key generation schemes, fuzzy extractor schemes have been attracted significant attention. However, they are still difficult to realize, due to noise and error elimination problems, computation problems, and storage size problems for helper data [24-26].

In this paper, we propose a PCA-CIA ensemble-based seed extraction scheme and a biometric-based secret key generation scheme for targeting a specific cryptographic algorithm. It can effectively apply biometrics, and can satisfy a certain level of security, such as quantum security level in 128-bit. Our target cryptographic algorithm is the Rainbow signature scheme, which is a kind of MQ public key cryptography. This scheme can also be quantum-resistant and can be implemented in resource-constrained IoT devices, capable of performing at high speeds. The proposed scheme prevents the use of the secret key by an unauthorized user through biometric recognition schemes. It then provides a key reduction and a practical storage size for the helper data, which is called bio-seed.

The main contributions of this paper are as follows:

- We described the basic idea of the bio-seed extraction, which is suitable for MQ signature schemes such as Rainbow, through image processing. Considering the specific security parameters of Rainbow, we designed a PCA-CIA ensemble-based feature extraction scheme and extracted the bio-seed from face images.
- We proposed the bio-seed-based MQ signature model with a bio-seed key generation method. After a signer is authorized with the bio-seed as a feature of the recognition process, the signer can generate a secret key and public key pair $\{SK, PK\}$ with the bio-seed.
- We implemented our bio-seed-based MQ signature scheme and optimized it by using single instruction multiple data (SIMD). Then, we evaluated the performance of our scheme in terms of storage size for bio-seed and the CPU clock usage for key generation, signature generation, and signature verification.

The remainder of the paper consists of the following: in Section 2, we review some related literature for our work. In Section 3, we explain how to extract the feasible bio-seed for the MQ signature schemes. In Section 4, we describe how to apply the proposed bio-seed to an

MQ signature scheme, such as Rainbow. Section 5 presents the experimental results, to prove the feasibility of the biosignature scheme. In Section 6, we summarize the proposed scheme.

2. Related Work

2.1 Multivariate Quadratic-based Public Key Cryptography

Multivariate Quadratic Public Key Cryptography (MPKC) is one of the main approaches for secure communication in a post-quantum world. The Principal idea is to choose a multivariate system, Q, of quadratic polynomials that can be easily inverted to a central map. The idea is based on the MQ problem over finite fields known as the NP-hard problem. After that, one chooses two affine linear invertible maps S and T to hide the structure of Q. The public key of the cryptosystem is the composed map $P = S \circ Q \circ T$ which is difficult to invert. The private key consists of S^{-1}, T^{-1} and Q and therefore allows us to invert P. There are several models based on how to build Q and to select parameters to prevent various attacks [27-29]. A lot of work has been done to study the security of multivariate schemes, but it is still an open problem. To date, Rainbow, a major MPKC proposed by Ding and Schmidt, has a structure and the specific parameters that have survived numerous attacks [29-30]. The MQ polynomials with Q in Rainbow(q, v_1, o_1, o_2) are defined in n variables x_1, …, x_n (m=o_1+o_2, n=v_1+m, k=1, ..., m) as shown in Eq (1). Rainbow, with Eq (1), is generally composed of three algorithms, a key generation algorithm, a signature generation algorithm, and a signature verification algorithm.

$$F_{x(x)} = \sum_{i \subset O_l, j \subset S_l} a_{i,j}^k x_i x_j + \sum_{i,j \subset S_l, i \leq j} \beta_{i,j}^k x_i x_j + \sum_{i \subset S_l \cup O_l} \gamma_i^k x_i + \eta^k \quad (1)$$

- *Private Key Generation*: The private key consists of $S : F^m \rightarrow F^m$, T: $F^n \rightarrow F^n$, and $Q = (f_{v1+1}(x), \ldots, f_n(x))$, where $m = n - v_1$ and the field is F.
- *Public Key Generation*: The public key consists of $P(x) = S \circ Q \circ T(x)$: $F^n \rightarrow F^m$.
- *Signature Generation*: A signer generates the signature *sig* by computing $T^{-1} \circ Q^{-1} \circ S^{-1}(H(msg))$, where $H(\,) \subset F^n$ is a hash function and *msg* is a message to be signed. Q^{-1} is to solve $f_k(x)$ with Q and $S^{-1}(H(msg))$.
- *Signature Verification*: The receiver verifies the signature by checking if $P(sig) = H(msg)$. If $P(sig) \neq H(msg)$, the received signature *sig* is fake.

Table 1. Security Level Comparison among cryptographic schemes (bit)

Scheme	Security Parameters	Quantum Security Level	Classic Security Level	Size of PK	Size of SK
AES	128	64	128	-	128
AES	256	128	256	-	256
RSA	3,072	0	128	24,576	3,072
ECDSA	256	0	128	-	256
ECDSA	384	0	256	-	384
UOV	(256,56,28)	80	-	99×10^6	95×10^6
Rainbow	(256,19,18,19)	80	-	59×10^6	42×10^6

Zhiniang, Peng and Tang analyzed the security of several major schemes, including Rainbow [28]. The observed parameters of Rainbow for 80-bit and 100-bit security are

(GF(256),19,18,19) and (GF(256),26,23,23), respectively. The length of the public key, *PK*, and the secret key, *SK* (a private key stored in safe area), are 59.7 KB and 42 KB, respectively given (GF(256),19,18,19) as shown in **Table 1**. Zhiniang, Peng and Tang also proposed a new Rainbow variant scheme with rotating relations, called circulant rainbow [28]. They analyzed rotating relation attacks, as well as other major attacks, for rainbow-based schemes. They concluded that rotating relations are hard to exploit regarding the cryptanalysis of MPKC, and that their proposed scheme with rotating relations can withstand all attacks, providing that the parameters are chosen properly [28], [30-32].

2.2 PCA-based Feature Extraction

PCA (Principal Component Analysis) is one of the most popular multivariate statistical techniques that uses an orthogonal transformation. It has been broadly applied to multivariate data analysis, pattern recognition, and signal processing, and has driven variants of PCA usch as Quanternion PCA, L1-norm PCA, patch PCA, and $(2D)^2$ PCA, in various aspects [33-37].

These PCA variants have been widely used in the field of biometrics. In Particular, PCA has been applied to face images, an approach that has been termed eigenfaces [38]. This was first developed by Sirovich and Kirby for recognition, and was used by Turk and Pentland for face classification [39-40]. They tried to find a lower-dimensional space for the simplest approach to recognize faces as a template matching problem. They considered PCA for faces, and introduced their main idea behind eigenfaces as follows:

- Let Γ be an $\mathrm{N}^2 \times 1$ vector for an $N \times N$ face image I.
- Γ is represented into $\hat{\Gamma}$ in a low-dimensional space, where $\Phi = \Gamma - \Psi$ (a mean face Ψ, a represented face Φ, $K \ll N^2$): $\hat{\Gamma} = \hat{\Phi} - \hat{\Psi} = w_1 u_1 + w_2 u_2 + \cdots + w_k u_k$

For face recognition with PCA, the steps are as follows: first, the eigenface generation step, with K eigenvectors corresponding to K largest eigenvalues;then, the face representation step as a linear combination of the eigenvectors; and finally the distance calculation step, within the eigenspace [36], [40-42].

2.3 CIA based on PCA and T-test

CI(Confidence Interval) is also major statistical analysis technique and can be applied to ensemble methodology in various domain [43-44]. CIA (Confidence Interval Analysis) for face images is based on a set of this confidence interval generated by using the *PRE_TCI_GENERATE* algorithm in [45]. The algorithm includes steps for calcuating $pc_{i(j)}$ as i-th principal component of j-th face image, taking a T-test value t, and generating a confidence interval ci_i as a return value where $1 < i <$ m and $1 < j < n$.

3. Bio-Seed Extraction Scheme from Biometrics

In this section, we describe the proposed bio-seed *BS* extraction scheme, which extracts a seed from noisy data such as biometrics to apply MPKC. This *BS* is used as a secret key to generate a private key in MPKC. In order to design the *BS* extraction scheme, we consider some properties of an MPKC scheme such as Rainbow, as follows:

- The MQ signature scheme can be applied over GF(256), as well as many other signals - including images that can be represented in 8 bits.
- The private key consists of the central map, Q, and two affine transformations, S^{-1} and T^{-1}. These are made of random numbers over GF(256), as well as the acquired biometrics, which also appear as random numbers because of their variance noise.
- The central map is a subspace of an $n \times n \times m$ matrix where n and m are the security parameters; this appears as a subspace of the K^3 matrix simply in terms of size, where $k \geq n > m$ and K is the number of principal components.
- Various biometrics can be applied for the proposed scheme if we can use the biometrics to generate a *k*-dimensional subspace where $k \geq n > m$.

The basic idea of the proposed scheme, as shown in **Fig. 1**, is to generate biometric-based secret information, *BS*, from $F^{N \cdot N \cdot M}$ to F^{3k}, using signal processing. The *BS* can be used to derive a map from F^{3k} to $F^{N \cdot N \cdot M}$, and to replace the existing central map with the *BS*-based central map in the private key in the Key Generation Algorithm in Section 4. The basic process of this scheme includes the inclusion of output types (*Ot*), determining whether to save (*Sv*), and the stabilization of the state (*Ss*) of the output data in each stage (*St*), as shown in **Fig. 1**. The first stage, the *Acquisition Stage*, simply involves taking the signals or pictures as sources to generate *BS*. They are converted into grayscale in the second stage, the *Grayscale Stage*, if they are not already grayscale signals. The third stage, the *Dimension Reduction Stage*, involves reducing the higher dimensional grayscale images into *K*-dimensional images. The fourth stage, the *Bio-Seed Extraction Stage*, comprises representing the dimension reduced data into *K* groups.

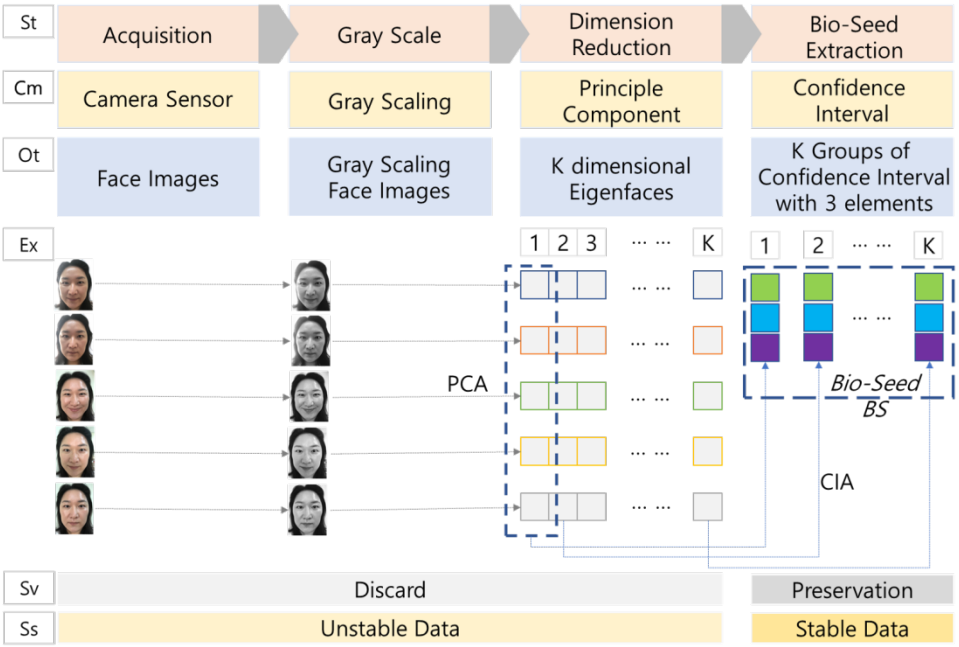

Fig. 1. The proposed bio-seed extraction process

The inputs of the first to third stages are deleted after they are used. *BS* is the only information that has to be kept in a secure area as *SK*, as it is impossible for it to be regenerated without using the same biometrics. *BS* is stable data for the mid-term. Our chosen methods

(*Cm*) for each stage are camera for acquisition, gray-scaling for transforming into the gray-scale, PCA for dimension reduction, and confidence interval analysis (CIA) for *BS* extraction.

1) *Acquisition Stage*: The $N \times N$ face images $I = [I_1, \dots, I_M]$ are acquired using a camera.

2) *Gray-scaling Stage*: Gray-scaling is the process of converting a continuous-tone image into an image that a computer can manipulate. After gray-scaling, the gray-scale image $GI = [GI_1, \dots, GI_M]$ is represented by 8 bits, so that each pixel is the same as an unsigned byte in various computer programming languages, such as C. Each pixel has 256 difference values {0, ... 255} and can be applied for operations over GF(256).

3) *Dimension Reduction Stage*: We used PCA for the dimension reduction of the gray-scale face image, GI, by projecting it from an N^2-dimensional space to a K-dimensional space, where $K \ll N^2$ and $K \geq n$. For the dimension reduction of face images using PCA, the face images must be centered and must be of the same size. In this paper, the PQC model that was used to fuse the face images is Rainbow, and the central map is replaced with a *BS*-based central map. Therefore, we need at least n dimensions, where n is a parameter in the MQ signature scheme. As a result, it is possible to use any reduction method to obtain K dimensions. To the best of our knowledge, this is the first time that such a fusion model has been proposed. PCA appears to be the most suitable choice to demonstrate the effectiveness of the proposed scheme, based on previous experimental cases that include the results of recognition based on PCA and CIA, although we do not focus on recognition here.

4) *Bio-Seed Extraction Stage*: We consider that the $n \times n \times m$ central map is a subspace of a larger K^3 cube, as a candidate of the new central map. To use this to generate the cube in the key generation stage, we represent the dimension-reduced faces into K groups, including their upper bound, median, and lower bound, using CIA. We call them *BS* as SK for generating a private key map to sign, and a public key map to verify. Similarly, at this stage, another method could also be applied, providing that it can represent or generate K groups with three or more elements, for an ensemble of Rainbow and biometrics.

Algorithm 1. Bio-Seed Generation Algorithm

Input: grayscale face images $GI = \{GI_1, GI_2, \dots, GI_M\}$
Output: bio-seed *BS*

1 $\mathrm{t} \leftarrow \mathrm{t}_{0.001}(M-1)$
2 Represent every image GI_i as a vector Γ
3 Compute the average face vector Ψ: $\Psi = \frac{1}{M}\sum_{i=1}^{M} \Gamma_i$
4 Subtract the mean face Φ_i from the represented face images Γ: $\Phi_i = \Gamma_i - \Psi$
5 Compute the covariance matrix C: $C = \frac{1}{M}\sum_{i=1}^{M} \Phi_i \Phi_i^T = AA^T$ where $A = [\Phi_1 \Phi_2 \dots \Phi_M]$
6 Compute the eigenvectors U_j of AA^T including the largest K eigenvalues
7 Represent Φ_i as $\Omega_i^T = [\omega_{i,1}, \dots, \omega_{i,j}, \dots, \omega_{i,k}]$: $\omega_{i,j} = U_j^T \times \Phi_{\mathrm{i}}$
8 Compute the average $\bar{X} = [\overline{X_1} \dots \overline{X_j} \dots \overline{X_K}]$: $\overline{X_j} = \frac{1}{M}\sum_{i=1}^{M} \omega_{i,j}$ for $j = 1, \dots, K$
9 Compute a variance vector $V = [V_1 \dots V_j \dots V_K]$:
$V_j = \frac{1}{M-1}\sum_{i=1}^{M} \omega_{i,j}^2 - \overline{X_j}$ for $j = 1, \dots, K$
10 Generate confidence interval CI_j: $CI_j = \overline{X_j} \pm t \cdot V_j \cdot M^{-1/2}$ for $j = 1, \dots, K$
11 Represent CI, which is divided into a set of K groups (upper bound *ub*, median *md*, lower bound *lb*), as bio-seed *BS*: $BS = \{(ub_1, md_1, lb_1), \dots, (ub_K, md_K, lb_K)\}$
12 Return *BS*

Algorithm 1 shows how *BS* is extracted in the dimension reduction stage with PCA, and in the bio-seed extraction stage with CIA. The main purpose of this algorithm is to represent each $N \times N$ face image, GI_i, into $N \times 1$ vector $\Omega_i = [\omega_1, \dots, \omega_j, \dots, \omega_k]$, whose weight corresponds to an eigenvector $U_i = [U_1, \dots, U_k]$ for $i = 1, \dots, M$ through lines 1 to 7, and to produce $CI_i = [CI_1, \dots, CI_k]$ through lines 8 to 10. For example, if $M = 5$, all faces CI_i are represented as Ω_i^T for $i = 1, \dots, 5$: $\Omega_1^T = [\omega_{1,1}, \dots, \omega_{1,j}, \dots, \omega_{1,k}]$, $\Omega_2^T = [\omega_{2,1}, \dots, \omega_{2,j}, \dots, \omega_{2,k}]$, ..., $\Omega_5^T = [\omega_{5,1}, \dots, \omega_{5,j}, \dots, \omega_{5,k}]$ and CI_1 is the 1st confidence interval for $\{\omega_{1,1}, \omega_{2,1}, \omega_{3,1}, \omega_{4,1}, \omega_{5,1}\}$. Here, CI_5 is the 5th confidence interval for $\{\omega_{1,K}, \omega_{2,K}, \omega_{3,K}, \omega_{4,K}, \omega_{5,K}\}$. Then, $BS = \{CI_1 = (ub_1, md_1, lb_1), \dots, CI_K = (ub_K, md_K, lb_K)\}$ is generated with CI in line 11.

4. Bio-Seed-based Key Generation Applied to A MQ Signature Scheme

4.1 Overview of Bio-Seed-based MQ Signature Scheme

Fig. 2 shows the overall steps of the bio-signature scheme. The proposed bio-signature scheme is designed by weaving together greyscale image process schemes with the MPKC signature scheme, over GF(256). Grayscale images are commonly stored with 8 bits per pixel. Moreover, this scheme can be directly applied via operations over GF(256) including mod for reduction, Exclusive Or (XOR) operation for addition and subtraction, and lookup tables for multiplication, inversion, and division.

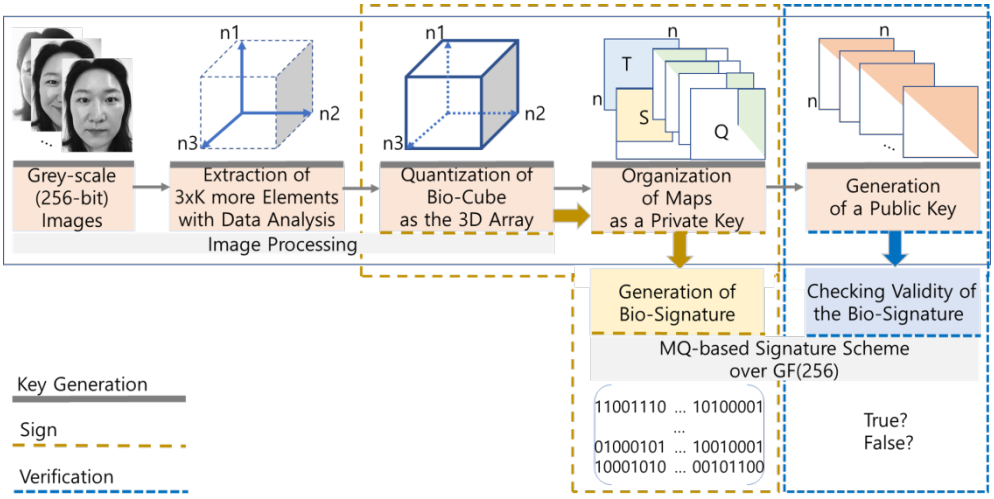

Fig. 2. Bio-Seed-based signature model showing the the proposed key generation scheme

A common signature scheme basically includes three stages: key generation, signature generation, and signature verification. While these basic stages are almost the same, there are differences in the methods used for processing biometrics to generate keys and apply them into a signature scheme. The first stage, the *key generation stage*, includes either acquiring grey images or converting images into grey images, extracting a bio-seed *BS*, which consists of *3K* elements extracted from noisy data (i.e. face images), quantizing *BS* in the three-dimensional (3D) array (called the bio-cube), organizing maps for a private key with the bio-cube, and generating a public key (*PK*) with the bio-cube. Unlike *PK*, the important information that needs to be kept safe for a period is *BS*, which is used as a secret key, *SK*. The second stage, the

signature generation stage, includes loading *BS* in a secure area, quantizing the bio-cube as coefficient maps with *BS*, and generating a biometric-based signature, *sig*. However, only authenticated user can access the *BS* and use it for generating *sig*. The authentication procedure is based on image processing in **Fig. 2** and steps 1-7 in **Algorithm 1** with grayscale face image GI_{now}. After checking whether $ub_i < \omega_{now,i}$ and $\omega_{now,i} < lb_i$ for each feature $\omega_{now,i}$ $(i = 1, \dots, k)$ in PCA-based features $\Omega_{now}^{T} = [\omega_{now,1}, \dots, \omega_{now,k}]$ generated from GI_{now}, the number of passed $\omega_{now,i}$ can determine the user's access for *BS*. The third stage, the *signature verification stage*, includes loading *PK* as coefficients in the MQ polynomial, *P*(*sig*), and checking the validity of *sig* by evaluating it via *P*(*sig*).

4.2 Key Generation Algorithm

This section presents the proposed biometric key generenation scheme with *BS* for the RAINBOW signature scheme. The basic idea is that a private key map for signature generation is made by transforming *BS* into a cube in the form of a 3D array, whereas the MQ signature scheme is usually made by filling the cube with random numbers.

The process of this key generation scheme with *BS* is as shown in **Fig. 3**. The *BS* of *K* groups are used to make *PK*, and are stored as *SK*. First, *BS* is represented by the bio-cube by quantization. The bio-cube, is aligned with the two-dimensional (2D) planes consisting of the *X* axis and *Y* axis, with respect to the *Z* axis. The first and second 2D planes must be two invertible affine maps, as S^{-1} and T^{-1}. Therefore, part S^{-1} of the first plane and part T^{-1} of the second plane are checked to see if they are invertible - if this is not the case they are swapped with another plane, after the third plane. Swapping planes here refers to changing the order of the pairs in *BS*. The resulting *BS*, with this adjusted order, is kept as *SK* in a safe place for the MQ signature scheme, and is used to generate the private key in the signature generation stage. The adjusted *BS* is also used to generate *PK*, using calculations based on $P(sig) = S \circ Q \circ T(sig)$. The bio-cube reflects the adjusted *BS*; it includes S^{-1}, T^{-1}, and *Q*. The public map, *Pc*, which is calculated using the bio-cube and *P*(*sig*), is symmetrical, and all of the 2D planes are arranged in the form of triangles for computational efficiency. Finally, in this key generation process, the *PK* consists of the reshaped *Pc*.

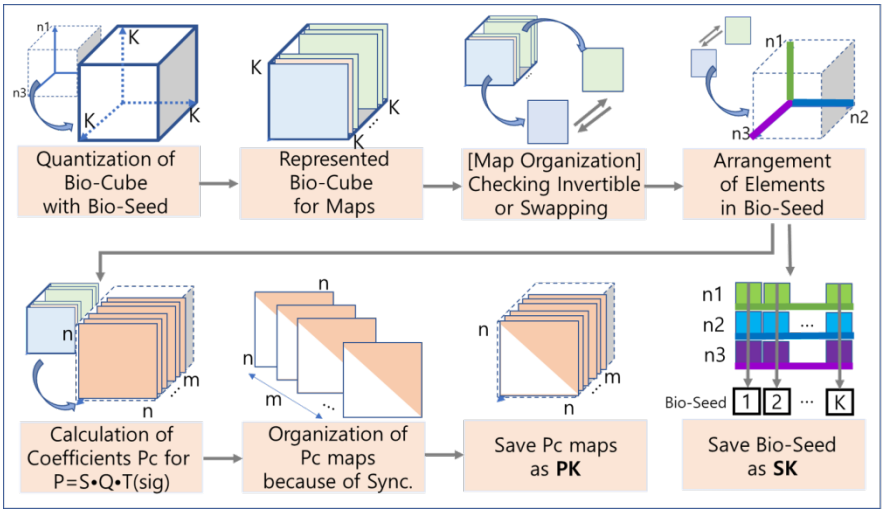

Fig. 3. Key generation process with the bio-seed

Algorithm 2. Bio-Seed-based Key Generation Algorithm

Input: bio-seed $BS = \{(ub_1, md_1, lb_1), \dots, (ub_K, md_K, lb_K)\}$
Output: a secret key *SK* and a public key *PK*
1 Rearrange *BS* to $X = [ub_1, \dots, ub_K]$, $Y = [md_1, \dots, md_K]$, and $Z = [lb_1, \dots, lb_K]$
2 Calcurate $C_{i,j,k} = X_i \times Y_i \times Z_i$ for $i, j, k = 1, \dots, K$
3 $idx \leftarrow K$
4 **while** $C_{1:m,1:m,1}$ *is not invertible*. **do**
5 swap((Z_1, Z_{idx})
6 $idx \leftarrow idx - 1$
7 **end**
8 **while** $C_{1:n,1:n,2}$ *is not invertible*. **do**
9 swap((Z_2, Z_{idx})
10 $idx \leftarrow idx - 1$
11 **end**
12 Reassign X, Y, Z to $BS = \{(ub_1, md_1, lb_1), \dots, (ub_K, md_K, lb_K)\}$
13 Assign the secret key: $SK \leftarrow BS$
14 Calcurate the public key with S^{-1}, T^{-1}, Q:
$S^{-1} \leftarrow Invt(C_{1:m,1:m,1})$, $T^{-1} \leftarrow Invt(C_{1:n,1:n,2})$, $T^{-1} \leftarrow Invt(C_{„3:m+2})$
$PK \leftarrow Pc \leftarrow S \circ Q \circ T$
15 **Return** *SK* and *PK*

Algorithm 2 shows this process in more detail. We use *BS* as the input, which consists of confidence intervals based on the largest K eigenvalues. *BS* consists of K groups $\{BS_1, BS_2, \dots, BS_K\}$, and a group includes the upper bound, ub_i, the median bound, md_i, and the lower bound, lb_i, where $i = (1, 2, \dots, K)$. *BS* is used to generate the biometric-based *SK* and *PK* in the signature scheme, after setting the three vectors $X = [ub_1, ub_2, \dots, ub_K]$, $Y = [md_1, md_2, \dots, md_K]$, and $Z = [lb_1, lb_2, \dots, lb_K]$ with $ub_i, md_i,$ and lb_i, respectively.

The candidate map, C, of $S^{-1}, T^{-1},$ and Q is generated by quantizing the vectors $X, Y,$ and Z in the 3D array, by calculating Eq. (2) in lines 4 to 10 of **Algorithm 2**, where $i, j,$ and $k = 1, 2, \dots, K$. This is one of the simplest ways to quantatize them. If $X, Y,$ and Z are placed on the *x*, *y*, and *z* axes, respectively, and they are used by this equation, the volume of the quantized data set is formed like a cube; we refer to it as bio-cube $C_{i,j,k}$. The parameters $x, y,$ and z in $C_{i,j,k}$ are the *i*-th *X*, *i*-th *Y*, and *i*-th *Z*, respectively.

$$C_{i,j,k} = X_i \times Y_i \times Z_i \tag{2}$$

We are now ready to generate *SK* and *PK* with $C_{x,y,z}$ from lines 11 to 26 of **Algorithm 2**. $C_{1:k,1:K,k}$ is assigned the k^{th} $K \times K$ 2-dimensional array by calculating $[X_1 X_2 \dots X_K]^T \times [Y_1 Y_2 \dots Y_K] \times Z_K$. This is used for generating S^{-1} or T^{-1}, which are invertible according to the definition of the rainbow signature scheme $RAINBOW(GF, v_1, o_1, o_2)$. First of all, S is defined as a subspace $C_{1:m,1:m,1}$ in $C_{„1}$, and we check whether or not it is invertible. Otherwise, $C_{„1}$ is reset by swapping it with $C_{„idx}$. The parameter idx, which is the initiallized index, K, of Z_K, is decremented by one after swapping. As T is a subspace $C_{1:n,1:n,2}$ in $C_{„2}$ according to our definition, it is also assigned by the algorithm after assigning the invertible S^{-1}. The central map, Q, is also a subspace in $C_{„3:m+2}$, and does not need any other processing for SK. Then, we set SK with the BS reasembled by X, Y, and Z. Such a SK needs to be kept in a secure area.

For generating $PK, S, T,$ and Q are set by using $C_{1:m,1:m,1}$, $C_{1:n,1:n,2}$, and $C_{„m+2}$, respectively. The PK is assigned with Pc, which is the coefficient map composed by calculating the composite function $P(sig) = S \circ Q \circ T(sig): F^n \rightarrow F^m$. This is similar to approaches in other MQ signature schemes. Looking at Q more closely, it can be seen that Q_k uses only some coefficients in a subspace in $C_{„3:m+2}$ for $P_k(sig)$.

4.3 Signature Generation Algorithm with Bio-Seed

To sign a hashed message $H(msg)$ with a length of m bytes, the signer quantizes the bio-cube as the 3D array with BS using Eq. (2), thus obtaining the private key T^{-1}, S^{-1}, and Q, and then inverts Q with the private key, as shown in **Fig. 4**. While inverting Q with the given y, the signer randomly guesses the vinegar variables v_1, and finds the solution by evaluating the secret quadratic equation using the secret values. The formal description of this process is shown in **Algorithm 3**.

A system that applies the MQ signature scheme with this proposed bio-seed-based key can use this BS in a secure area, before the signature generation. BS comprises useful data to verify (or deny) an authorized user for signature generation with BS. Given a new biometric input, B, the system checks whether pc_i in B is included in $ci_i = (u_i, v_i)$ of CI; it returns a result of 0 if it is not included, and a result of 1 if it is included. The sum of the results for K is the inclusion rate. This is a useful measure as a recognition or prediction result. As a result, the user becomes a signer to generate sig with BS.

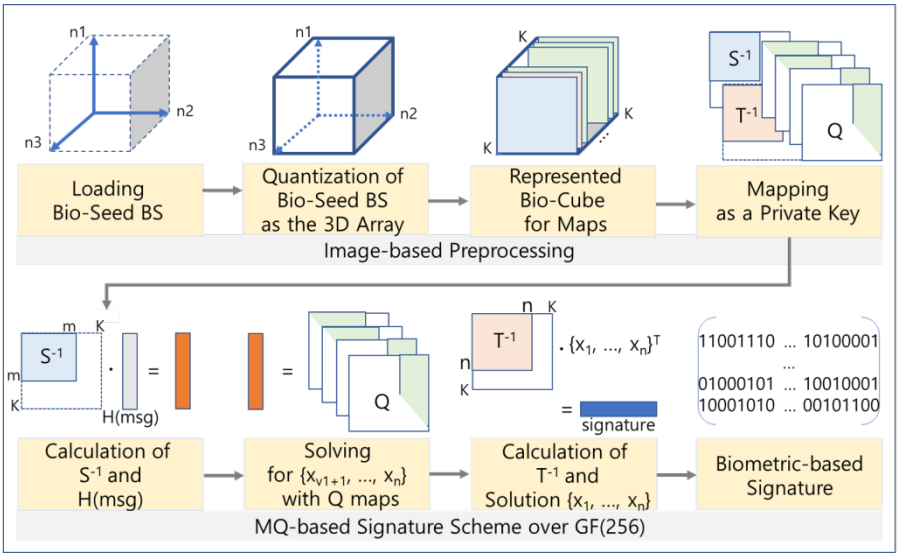

Fig. 4. Signature generation process with bio-seed

Algorithm 3. Signature Generation Algorithm

Input: Hashed message $\boldsymbol{msg} = \{msg_1, \ldots, msg_l\}$
Output: Signature $\boldsymbol{sig} = \{sig_1, \ldots, sig_n\} \subset K^n$

$w \subset K^m \leftarrow Hash(msg)$
$y = S^{-1}(w)$
$(s_1, \ldots, s_{v1}) \leftarrow rand(\ ) \ mod\ 256$
$(x_1, \ldots, x_{v1}) \leftarrow (s_1, \ldots, s_{v1})$
for $i \leftarrow 1$ **to** $t + 1$ **do**
    $(g_{v_i+1}, \ldots, g_{v_i+o_i}) \leftarrow (x_1, \ldots, x_{v1})$

7 **if** $(not\ IsRegualr(Lx = u))$
8 go back to line 3
9 $(s_{v_i+1}, \dots, s_{v_i+o_i}) \leftarrow Solve(Lx = u)$
10 $(x_{v_i+1}, \dots, x_{v_i+o_i}) \leftarrow (s_{v_i+1}, \dots, s_{v_i+o_i})$
11 **end**
12 **Return** $sig \leftarrow T^{-1}(x)$

4.4 Signature Verification Algorithm

To verify the authenticity of a signature that has a length of n bytes, the verifier evaluates $P(sig)$ with their signature and the biometric-based PK, as shown in **Fig. 5**. This process is the same as in any other verification process based on an MQ signature scheme, except that PK is generated by using BS based on biometrics. If the value of the signature projected on the polynomial $P(sig)$ by loading and evaluating PK using the bio-signature is the same as the hash value for the original message, the signature has been successfully verified.

The formal description of this process is shown in **Algorithm 4**. PK is basically used for the coefficients $c_{i,j}$ to evaluate m quadratic polynomials:

$$P_k(x) = \sum_{i=1}^{n} \sum_{j=i}^{n} c_{i,j} x_j x_i \tag{3}$$

where $k = [1, \dots, m], x = [x_1, \dots, x_n]$, and $P_k(x) = [P_1, \dots, P_m]$ in the $MQ(gf, m, n)$ system. This equation can be represented as $P_k = (c_{1,1}x_1 + c_{1,2}x_2 + c_{1,3}x_3 + \cdots + c_{1,n}x_n)x_1 + (c_{2,2}x_2 + c_{2,3}x_3 + \cdots + c_{2,n}x_n)x_2 + \cdots + (c_{n,n}x_n)x_n$. Then, if $P(sig) = H(msg)$ holds, the signature is accepted; otherwise it is rejected.

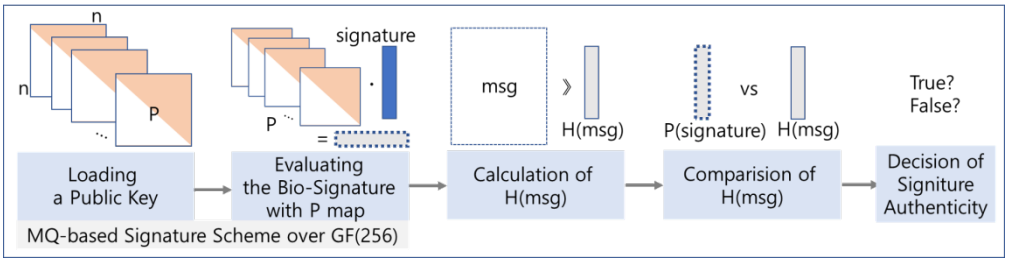

Fig. 5. Signature verification process

Algorithm 4. Signature Verification Algorithm

Input: Public key map PK, signature sig, and message msg
Output: 1, if sig is valid; 0 otherwise.
1 $auth \leftarrow 0$
2 **for** $k \leftarrow 1$ **to** m **do**
3 $hmsg'_k \leftarrow P_k(sig, PK)$
4 **end**
5 $hmsg \leftarrow SHA256(msg)$
6 **if** $(hmsg' == hmsg)$
7 $auth \leftarrow 1$
8 **Return** $auth$

5. Analysis of Rainbow Signature Scheme with Biometric-based Key

5.1 Parameters and Security

Security analysis of MQ Signature Schemes, including Rainbow, is generally performed by applying attacks of Direct, HighRank, Rainbow-Band-Separation (RBS), MinRank, UOV, and UOV-R (UOV-Reconciliation) [28]. These attacks are applied to the analysis of the target signature scheme, using the parameters and the multivariate quadratic structure.

1) *Attacks using similar biometric information*: Like in conventional cryptosystems, the proposed method results in a very large difference for different input values, even for one bit, because v1 generates and applies a random number at the beginning of the signature generation. Therefore, it is impossible to generate a signature with any other biometric samples. If an attacker wants to make the same signature as a secretly stored bio-seed, they must have the biometric samples that the user originally used, however these samples are discarded immediately after the bio-seed is generated.

2) *Attacks using estimated biometric information*: It is practically impossible to estimate the biometric information by using the whole investigation, such as the Bruce attack, on the password. The length of the bio-seed is $3n$ bytes over $GF(2^8)$, and the total number of cases to be examined is $(2^8)^{3n}$. If $n = 80$, the bio-seed to be stored as the secret key is 240 bytes, which is smaller than the 384 bytes of RSA, but larger than the 12 bytes of ECDSA. In this case, the total number of cases is $(2^8)^{240} = 2^{1920}$, which is practically impossible to estimate.

5.2 Storage space for Key or Helper data

As shown in **Table 2**, most biometric-based key generation techniques are not large enough to inspect security levels. In addition, there are many cases where the technique is proposed at the concept level, therefore no actual experiment is presented. Even the fuzzy extractor-based technique has a very large storage size of 1 GB for helper data generated from biometrics for extracting a key [14]. Unlike these methods, in our proposed method, the storage size, the security level, and the key size are LL practical. They are not related to the False Reject Rate (FRR) because they are stored using the secret key of the signature technique.

Table 2. Comparison of stroage space, quantum security level (QSLv.), key lengh, FRR, and False Acceptance Rate (FAR)

Scheme	**Storage Space** Byte	**QSLv.** bit	**Key Len** bit	**FRR** %	**FAR** %	**Database**
[46]	-	-	14	19	0.38	Fingerprint
[47]	-	-	29		0.00	Fingerprint
[48]	-	-	43 143	12.50 36.54	0.10 0.29	Fingerprint
[49]	-	-	40	-	-	Signature
[50]	-	-	15	-	-	Fingerprint
[51]	-	-	128	-	-	Face
[52]	-	-	130	-	-	Iris
[14]	1 T	80	128	50	-	Iris
[16]	1 T	80	128	50	-	Iris
Proposed	237	128	237	-	-	Face

Table 3. Length of signature, *PK*, and *SK*, with 128 bits in QSLv.

Scheme	QSLv. (bit)	Signature (byte)	PK (byte)	SK (byte)	PK+SK (byte)
RSA-3072	128	361	384	3,072	3,456
ECDSA-256^e	128	64	64	96	160
Rainbow($GF(2^8)$, 36,21,22)	128	79	139,320	105,006	244,326
Bio-Seed-based Rainbow	128	79	139,320	237	139,557

5.3 Size of Secret Key and Public Key

The target post-quantum cryptographic algorithm in this experiment is Rainbow. This algorithm is used to show how the proposed bio-seed-based key generation scheme can be applied to MQ signature schemes. The parameter set ($GF(2^8)$, 36,21,22 for Rainbow is considered to be the optimal secret key size at a 128-bit post-quantum security level [53]. The parameters for RSA and ECDSA are 3072 and 256^e respectively, they are also selected at the 128-bit post-quantum security level for comparison. When the QSLv. is 128 bits, as shown in **Table 3**, we can conclude the proposed algorithm-based scheme as follows:

- The signature is 79 bytes, as short as that of ECDSA (64 bytes). It is about 78.1% shorter than that of RSA.
- PK is 139,320 bytes, which is the same size as Rainbow. It is about 362.8 and 2,176.9 times longer than those of RSA and ECDSA, respectively.
- SK is 237 bytes, which is just as short as that of ECDSA (96 bytes). It is about 92.3% and 99.8% shorter than those of RSA and Rainbow.
- The total key size is 139,557 bytes, which is about 42.9% shorter than that of Rainbow.

5.4 Performance Through Experiments

We evaluated the performance of Rainbow based on the proposed bio-seed generation scheme. To assess its effectiveness in a system using such a signature scheme, we implemented the schemes on an Intel Core i5-7200U (2.5GHz), supporting AVX2 instructions, with a 512 GB SSD and 8 GB of RAM. The C and gcc compilers were used for the scheme's implementation. The AVX2 instructions used 256-bit registers YMM. They are Single Instruction Multiple Data (SIMD) and compile intrinsic. We basically used the AR Face Database to focus on applying bio-seed to Rainbow [40], [54].

In terms of speed, we found that the lower the value, the faster and better the performance was, as shown in **Table 4**. The proposed scheme is a more efficient signature scheme for various IoT devices with high speeds and short secret keys, despite the need to reduce the size of PK.

- The clock cycle for key generation is 8,200,840 cycles. It is about 95.5% lower than that of Rainbow.
- The clock cycle for signing is 38,245 cycles; this is faster than others. It is about 99.6%, 76.7%, and 40.8% lower than that of RSA, ECDSA, and Rainbow, respectively.
- The clock cycle for verification is 32,006 cycles, this is faster than others. It is about 74.8%, 92.9%, and 50.4% lower than that of RSA, ECDSA, and Rainbow, respectively.

Table 4. Clock Cycles of Signature Schemes

Scheme	Key Gen.	Sig. Gen.	Sig. Ver.	Spec.
RSA-3072 [55]	-	8,802,000	87,360	i5 3.3 GHz
ECDSA-256^e [55]	-	163,996	310,048	i5 3.3 GHz
Rainbow $(GF(2^8), 36,21,22)$ [55]	183,000,000	64,658	44,397	i5 3.3 GHz
Bio-Seed-based Rainbow	8,200,840	38,245	32,006	i5 2.5 GHz

6. Conclusion

Here, we have proposed a new biometric-based key generation scheme for a multivariate quadratic-based signature scheme by using the PCA-based CIA, which is a suitable ensemble method for extracting the features from images. The proposed scheme generates PCA-CIA-based features from biometrics and saves them in secure area as same as the secret key in Rainbow. In the case of Rainbow, the private key to keep in secure area is equal to the secret key to generate the sign. On the other hand, the biometric-based key is the private key to keep and it can be used to derive the secret key for signature generation when the user is authorized via the biometric-based key. Through biometric recognition with this biometric-based key, the proposed scheme prevents a third-party from using the secret key obtained by deception, unauthorized sharing, or unauthorized proxying. Moreover, the PCA-CIA-based key is shorter, even though it is enough to generate the secret key for signature.

Our results regarding optimized implementation show that using the proposed scheme with Rainbow performs well at high speeds for signature generation and verification; the approach is five times faster regarding key generation than that of Rainbow alone. We believe that this proposed scheme is a practical biometric-based key generation scheme for quantum-resistant cryptography. We also expect that this practicality will be proven in the future by experimenting with more feature extraction methods, various biometric templates, and different biometric sensors.

References

[1] Kim-Kwang Raymond Choo, Stefanos Gritzalis, and Jong Hyuk Park, "Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3567-3569, May, 2018. Artilcle (CrossRefLink).

[2] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone, "Blockchain technology overview," *NISTIR 8202*, 2018. Article (CrossRef Link)

[3] Li Da Xu, Wu He, and Shancang Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233-2243, January, 2014. Article (CrossRef Link)

[4] Dustin Moody, "Let's Get Ready to Rumble. The NIST PQC "Competition"," in *Proc. of First PQC Standardization Conference*, April 11-13, 2018. Article (CrossRef Link)

[5] Cheol-Min Park, Aeyoung Kim, Namhun Koo, and Kyung-Ah Shim, "High Speed MQ Signature: HiMQ3," in *Proc. of First PQC Standardization Conf.*, April 11-13, 2018. Article (CrossRef Link)

[6] Jintai Ding and Dieter Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in *Proc. of Int. Conf. on Applied Cryptography and Network Security*, pp. 164-175, Jun 2005. Article (CrossRef Link)

[7] Kyung-Ah Shim, Cheol-Min Park, and Namhun Koo, "An existential unforgeable signature scheme based on multivariate quadratic equations," in *Proc. of Int. Conf. on the Theory and Application of Cryptology and Information Security*, pp. 37-64. December 3, 2017. Article (CrossRef Link)
[8] Christian Rathgeb and Andreas Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, pp. 3, December, 2011. Article (CrossRef Link)
[9] K. Xi and H. Jiankun, *Bio-Cryptography in Handbook of Information and Communication Security*, Peter Stavroulakis, Mark Stamp (Eds.), *Springer Berlin Heidelberg*, 2010. Article (CrossRef Link)
[10] S. P. Venkatachalam, P. M. Kannan, V. Palanisamy, "Combining Cryptography with Biometrics for Enhanced Security," in *Proc. of Int. Conf. on Control, Automation, Communication and Energy Conservation*, pp. 1-6, June 4, 2009. Article (CrossRef Link)
[11] Claude Crépeau, Rafael Dowsley, and Anderson CA Nascimento, "On the commitment capacity of unfair noisy channels," *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3745-3752, 2020. Article (CrossRef Link)
[12] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM journal on computing*, vol. 38, no. 1, pp. 97-139, March, 2008. Article (CrossRef Link)
[13] Fuchun Guo, Willy Susilo, and Yi Mu, "Distance-based encryption: How to embed fuzziness in biometric-based encryption," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 247-257, October, 2015. Article (CrossRef Link)
[14] Jung Hee Cheon, Jinhyuck Jeong, Dongwoo Kim, and Jongchan Lee, "A Reusable Fuzzy Extractor with Practical Storage Size: Modifying Canetti et al.'s Construction," in *Proc. of Australasian Conf. on Information Security and Privacy*, pp. 28-44, July 11, 2018. Article (CrossRef Link)
[15] Fuller Benjamin, Xianrui Meng, and Leonid Reyzin, "Computational Fuzzy Extractors," in *Proc. of Int. Conf. on the Theory and Application of Cryptology and Information Security*, pp. 174-193, December 1, 2013. Article (CrossRef Link)
[16] Canetti Ran, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam Smith, "Reusable Fuzzy Extractors for Low-entropy Distributions," in *Proc. of Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, pp. 117-146, May 8-12, 2016. Article (CrossRef Link)
[17] Wen Yunhua, and Shengli Liu, "Reusable Fuzzy Extractor from LWE," in *Proc. of Australasian Conf. on Information Security and Privacy*, pp. 13-27, July 11-13, 2018. Article (CrossRef Link)
[18] Conti Vincenzo, Salvatore Vitabile, and Filippo Sorbello, "Fingerprint Traits and RSA Algorithm Fusion Technique," in *Proc. of 2012 Sixth Int. Conf. on Complex, Intelligent and Software Intensive Systems*, pp. 351-356, July 4-6, 2012. Article (CrossRef Link)
[19] Evgeny A. Verbitskiy, Pim Tuyls, Chibuzo Obi, Berry Schoenmakers, and Boris Skoric, "Key extraction from general nondiscrete signals," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 269-279, March, 2010. Article (CrossRef Link)
[20] P. Y. Safnitha and K. S. Kurian, "Enhancing security with fingerprint combination using RSA algorithm," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 3, no. 4, pp. 61-65, 2014. Article (CrossRef Link)
[21] M. Marimuthu and A. Kannammal, "Dual Fingerprints Fusion for Cryptographic Key Generation," *International Journal of Computer Applications*, vol. 122, no. 23, pp. 20-25, January, 2015. Article (CrossRef Link)
[22] Minhye Seo, Jong Hwan Park, Youngsam Kim, Sangrae Cho, Dong Hoon Lee, and Jung Yeon Hwang, "Construction of a New Biometric-Based Key Derivation Function and Its Application," *Security and Communication Networks*, vol. 2018, 2018. Article (CrossRef Link)
[23] A. H. Sulaiman, I. F. T. Al-Shaikhli, M. R. Wahiddin, S. Houri, Norziana Jamil, and A. F. Ismail, "A novel secret key generation based on image link," *International Journal of Engineering and Technology (UAE)*, vol. 7, no. 2, pp. 23-26, January, 2018. Article (CrossRef Link)

[24] Pragati Mahale, Sonali Alwani, Vaishnavi Borade, Shreya Dhanbar, and Pooja Suvarna Khandi, ”Securing System using Lossless Computational Fuzzy Extractor for IOT,” *International Journal of SRCSEIT*, pp.28-31, 2018. Article (CrossRef Link)
[25] Kenji Yasunaga and Kosuke Yuzawa, “On the Limitations of Computational Fuzzy Extractors,” *Cryptology ePrint Archive*, vol. 3, no. 1, pp. 7-9, March, 2018. Article (CrossRef Link)
[26] Benjamin Fuller and Lowen Peng, "When are Continuous-Source Fuzzy Extractors Possible?," *IACR Cryptology ePrint Archive*, vol. 2018, no. 461, pp.1-21, September, 2018. Article (CrossRef Link)
[27] Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann, “CyclicRainbow–a multivariate signature scheme with a partially cyclic public key,” in *Proc. of Int. Conf. on Cryptology in India*, pp. 33-48, December 12, 2010. Article (CrossRef Link)
[28] Zhiniang Peng and Shaohua Tang, "Circulant rainbow: A new rainbow variant with shorter private key and faster signature generation," *IEEE Access*, vol. 5, pp. 11877-11886, June, 2017. Article (CrossRef Link)
[29] J. Ding and D. Schmidt, ”Rainbow, A New Multivariable Polynomial Signature Scheme,” in *Proc. of Int. Conf. on Applied Cryptography and Network Security*, pp. 164-175, June 7, 2005. Article (CrossRef Link)
[30] Petzoldt Albrecht, Stanislav Bulygin, and Johannes Buchmann, ”Selecting Parameters for the Rainbow Signature Scheme,” in *Proc. of Int. Workshop on Post-Quantum Cryptography*, pp. 218-240, May 25, 2010. Article (CrossRef Link)
[31] A. Petzoldt, *Selecting and Reducing Key Sizes for Multivariate Cryptography*, Doctoral Dissertation, tuprints, 2013. Article (CrossRef Link)
[32] Albrecht Petzoldt and Stanislav Bulygin, ”Linear Recurring Sequences for the UOV Key Generation Revisited,” in *Proc. of Int. Conf. on Information Security and Cryptology*, pp.441-455, November 28, 2012. Article (CrossRef Link)
[33] Nova Hadi Lestriandoko, Luuk Spreeuwers, and Raymond Veldhuis, "The Behavior of Principal Component Analysis and Linear Discriminant Analysis (PCA-LDA) for Face Recognition," in *Proc. of 2018 Symposium on Information Theory and Signal Processing in the Benelux*, pp. 133-148, May 31-1, 2018. Article (CrossRef Link)
[34] Beijing Chen, Jianhao Yang, Byeungwoo Jeon, and Xinpeng Zhang, "Kernel quaternion principal component analysis and its application in RGB-D object recognition," *Neurocomputing*, vol. 266, pp. 293-303, November, 2017. Article (CrossRef Link)
[35] Panos P. Markopoulos, Sandipan Kundu, Shubham Chamadia, and Dimitris A. Pados, "Efficient L1-norm principal-component analysis via bit flipping," *IEEE Transactions on Signal Processing*, vol. 65, no. 16, pp. 4252-4264, May, 2017. Article (CrossRef Link)
[36] Tai-Xiang Jiang, Ting-Zhu Huang, Xi-Le Zhao, and Tian-Hui Ma, "Patch-based principal component analysis for face recognition," *Computational intelligence and neuroscience*, vol. 2017, 2017. Article (CrossRef Link)
[37] Shuisheng Zhou and Danqing Zhang, "Bilateral Angle 2DPCA for Face Recognition," *IEEE Signal Processing Letters*, vol. 26, no. 2, pp. 317-321, December, 2018. Article (CrossRef Link)
[38] Mrutyunjanya Sahani, Subhashree Subudhi, and Mihir Narayan Mohanty, "Design of Face Recognition based Embedded Home Security System," *KSII Transactions on Internet & Information Systems*, vol. 10, no. 4, April, 2016. Article (CrossRef Link)
[39] Lawrence Sirovich and Michael Kirby, "Low-dimensional procedure for the characterization of human faces," *Josa a*, vol. 4, no. 3, pp. 519-524, March, 1987. Article (CrossRef Link)
[40] Matthew Turk and Alex Pentland, "Eigenfaces for recognition," *Journal of cognitive neuroscience*, vol. 3, no. 1, pp. 71-86, January, 1991. Article (CrossRef Link)
[41] Kyungnam Kim, "Face recognition using Principal component analysis," in *Proc.* of *Int. Conf. on Computer Vision and Pattern Recognition*, vol. 586, pp. 591, 1996. Article (CrossRef Link)
[42] Marijeta Slavković and Dubravka Jevtić, "Face recognition using eigenface approach," *Serbian Journal of electrical engineering*, vol. 9, no. 1, pp.121-130, 2012. Article (CrossRef Link)

[43] Emily J. Huang, Ethan X. Fang, Daniel F. Hanley, and Michael Rosenblum, “Constructing a confidence interval for the fraction who benefit from treatment, using randomized trial data,” *Biometrics*, vol. 75, no. 4, pp. 1228-1239, 2019. Article (CrossRef Link)
[44] Soojeong Lee and Gaseong Lee, "Ensemble Methodology for Confidence Interval in Oscillometric Blood Pressure Measurements," *Journal of Medical Systems*, vol. 44, no. 5 pp. 1-9, 2020. Article (CrossRef Link)
[45] Aeyoung Kim and Sang-Ho Lee, "A scheme for predicting recognition performance by using confidence intervals," *IEICE Electronics Express*, vol. 9, no. 3, pp.133-139, February 2012. Article (CrossRef Link)
[46] K. B. Raja, "Fingerprint recognition using minutia score matching," *International Journal of Engineering Science and Technology*, vol. 1(2), pp.35-42, 2009. Article (CrossRef Link)
[47] George I. Davida, Yair Frankel, and Brian J. Matt, “On Enabling Secure Applications through Off-line Biometric Identification,” in *Proc of 1998 IEEE Symp. on Security and Privacy*, pp. 148-157, May 6, 1998. Article (CrossRef Link)
[48] T. Ramu and T. Arivoli, “Biometric Template Security: An Overview,” in *Proc. of Int. Conf. on Electronics*, vol. 65, November 2, 2012. Article (CrossRef Link)
[49] Hao Feng and Chan Choong Wah, "Private key generation from on-line handwritten signatures," *Information Management & Computer Security*, vol. 10, no. 4, pp. 159-164, October, 2002. Article (CrossRef Link)
[50] Yagiz Sutcu, Qiming Li, and Nasir Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 503-512, August, 2007. Article (CrossRef Link)
[51] Li Qiming, Muchuan Guo, and Ee-Chien Chang, “Fuzzy Extractors for Asymmetric Biometric Representations,” in *Proc. of IEEE Computer Society Conf. on Computer Vision and Pattern Recognition Workshops*, pp. 1-6, June 23, 2008. Article (CrossRef Link)
[52] Christian Rathgeb and Andreas Uhl, “An Iris-based Interval-mapping Scheme for Biometric Key Generation,” in *Proc. of the 6th Int. Symp. on Image and Signal Processing and Analysis*, pp. 511-516, September 16, 2009. Article (CrossRef Link)
[53] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. S. Tone, *Report on Post-Quantum Cryptography*, US Department of Commerce, National Institute of Standards and Technology, IR8105, 2016. Article (CrossRef Link)
[54] A. K. Jain and S. Z. Li, *Handbook of Face Recognition*, Springer-Verlag, New York, 2011. Article (CrossRef Link)
[55] Kyung-Ah Shim, Cheol-Min Park, and Namhun Koo, "An existential unforgeable signature scheme based on multivariate quadratic equations," in *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, pp. 37-64, 2017. Article (CrossRef Link)

Aeyoung Kim She is a research professor at Hanyang University. She received her B.S. degree in Computer Science & Statistics from Hanshin University, Korea in 2000, and the M.S. and Ph.D. degrees in Computer Science and Engineering from Ewha Womans University, Korea in 2003, 2012, respectively. Before joining the faculty at Hanyang University in 2018, she was a post-doctoral researcher and a research professor of Computer Science and Engineering at Ewha Womans University for four years and a researcher of cryptographic technology team for two years in NIMS (National Institute for Mathematical Sciences), Korea. Her research interests include optimization and quantum analysis of PQC (Post-Quantum Cryptography), lightweight cryptography for IoT and blockchain, authentication with biometrics, and privacy in body area networks.

Changda Wang was a Visiting Researcher with Carleton University and Purdue University. He is currently a Professor with the School of Computer Science and Communication Engineering, Jiangsu University. His recent research focuses on IoT security, network communication, and cloud computing. He is a member of CCF and serves in the Network and Data Communication Committee. He was a recipient of the Qinglan and Liuda Gaofeng Awards of Jiangsu Province.

Seung-Hyun Seo received the B.S. degree from the Department of Mathematics, Ewha Womans University, Seoul, South Korea, in 2000, and the M.S. and Ph.D. degrees in computer science from Ewha Womans University, in 2002 and 2006, respectively. She is currently a Professor at Hanyang University. Before joining the faculty at Hanyang University, in 2017, she was an Assistant Professor with Korea University Sejong campus for two years. Before that, she was a Postdoctoral Researcher of computer science with Purdue University for two and half years, a Senior Researcher of Korea Internet and Security Agency (KISA) for two years, and a Researcher for three years in Financial Security Agency (FSA), South Korea. Her main research interests include cryptography, the IoT security, mobile security, blockchain, and post-quantum cryptography.