Application of Public Key Encryption on Fuzzy Images in a Company's Security Model

SadNguyen, Bonten, Khoi Nguyen, Hoang Le

Abstract This report presents an approach to addressing the implementation of a security model in companies by using picture fuzzy public key encryption, with a more detailed focus on utilizing user biometric data as a secret key. Since biometric data is blurred or noisy and changes with each collection, traditional public key encryption models cannot be used; instead, a picture fuzzy public key encryption model must be employed. This study introduces the concept of picture fuzzy public key encryption (PFPKE), a public encryption model that accepts a portion of blurred data (a noisy version of the original biometric data) as a private key for decrypting the ciphertext. Unlike traditional public key encryption models, where the private key is typically stored on devices (e.g., on USB drives), the picture fuzzy public key encryption model does not require any device to store the private key

Key words: Picture fuzzy public key encryption, fuzzy data, biometrics

1 Introduction

In traditional security models within companies using public key infrastructure, each employee must have a public-private key pair. If an employee receives an encrypted message, it means the message has been encrypted using that employee's public key, and they will decrypt it with their private key. The most important aspect for the employee is to keep their private key secure, as a leak of this key would compromise the system's security. A widely accepted method is to store the private key on a physical device like a smart card or USB drive and require the employee to remember a password to activate it (Ellison & Schneier, 2000). An ideal approach is to use biometric data (e.g., fingerprints or iris patterns) (Connaughton et al., 2007) as a private key since biometric data is unique to each individual, providing a convenient and secure way to serve as a private key for users. However, biometric data can be

Hanoi University of Science of Technology

blurry or noisy and may change every time it is captured, making it unsuitable for use as a private key in traditional public key encryption schemes. To address this issue, this paper introduces the concept of fuzzy signatures (Takahashi et al., 2015) ,which use biometric data as a private key without requiring any assistance (Dodis et al., 2008) . Thus, it applies public key cryptography with fuzzy images (Son et al., 2016) in internal company security models utilizing biometrics.

2 Symbols and definitions

(i) Let $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$ denote the sets of natural numbers, integers, and real numbers, respectively. If $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$. If $a \in \mathbb{R}$, then $\lfloor a \rceil$ denotes the nearest integer to a. Additionally, if $a = (a_1, a_2, \ldots)$, let $\lfloor a \rceil := (\lfloor a_1 \rceil, \lfloor a_2 \rceil, \ldots)$.

(ii) The notation $x \leftarrow y$ denotes that y is assigned to x. If S is a finite set, $|S|$ represents its size, and $x \leftarrow_R S$ means that x is chosen randomly from S. If Φ is a distribution over some set, $x \leftarrow_R \Phi$ denotes that x is chosen according to distribution Φ. Let $f : D \to R$ be a function and $y \in R$ a value; $f^{-1}(y)$ represents the set of pre-images of y under f, i.e., $f^{-1}(y) = \{x \in D \mid f(x) = y\}$. If x and y are bitstrings, then $|x|$ denotes the bit length of x, and $(x||y)$ represents the concatenation of x and y.

(iii) A function $f(.) : \mathbb{N} \to [0,1]$ is called negligible if for every positive polynomial $p(.)$ and every sufficiently large λ then $f(\lambda) < \dfrac{1}{p(\lambda)}$.

(iv) How to set the open key:
1 open key setting $\mathscr{F}$ includes $((d,X),t,\mathscr{X},\Phi,\varepsilon)$ with (d,X) being the spatial data with X being the space containing the values of the fuzzy set of the picture A and $d : X^2 \to \mathbb{R}$ being the corresponding distance function. $t \in \mathbb{R}$ is the threshold value determined by the security parameter λ, $\mathscr{X}$ is the distribution of the fuzzy data on X, Φ is the error distribution and $\varepsilon \in [0,1]$ is an error parameter representing the false rejection rate. The False Acceptance Rate (FAR) and False Rejection Rate (FRR) are determined based on the threshold value t.

Requirement: FAR $:= \Pr[x, x' \leftarrow_R \mathscr{X} : d(x,x') < t]$ is negligible in the security parameter λ. Also for all fuzzy data parts of $x \in X$, FRR $:= \Pr[e \leftarrow_R \Phi :$ $\mathrm{d}(x, x+e) \geq t] \leq \varepsilon$

(v) The definition of picture fuzzy set (PFS) is an extension of fuzzy set and intuitionistic fuzzy set. Picture fuzzy set is based on a complete model in situations where we have human opinions: yes, no, neutral.

Given a background set $X = \{x_1, x_2, \ldots, x_n\}$, a picture fuzzy set A on X is defined by

$$A = \{\langle x, \mu_A(x), \eta_A(x), \nu_A(x)\rangle \mid x \in X\}$$

Where:

$$\mu_A : X \to [0,1] \quad \text{is a positive function}$$

$$\eta_A : X \to [0,1] \quad \text{is a neutral function}$$

$$\nu_A : X \to [0,1] \quad \text{is a negative function}$$

Satisfy the condition:

$$\mu_A(x) + \eta_A(x) + \nu_A(x) < 1 \quad \forall x \in X$$

Apply the $L-R$ fuzzy number formula to calculate $\mu(x) = \langle b, c \rangle$, where b is the average value in set X, and c is the maximum value in set X:

$$\mu(x) = \begin{cases} 0 & \text{if } x \leq c \\ \dfrac{x-b}{c-b} & \text{if } b < x \leq c \end{cases}$$

Apply the triangular fuzzy number formula to calculate $\eta(x) = \langle a, b, c \rangle$, where b is the average value in the set X:

$$a = \frac{b + \min(X)}{2}$$

$$c = \frac{b + \max(X)}{2}$$

$$\eta(x) = \begin{cases} 0 & \text{if } x \geq c \text{ or } x < a \\ \dfrac{c-x}{c-b} & \text{if } b \leq x < c \\ \dfrac{x-a}{b-a} & \text{if } a \leq x < b \end{cases}$$

Apply the $L-R$ fuzzy number formula to calculate $\nu(x) = \langle a, b \rangle$, where b is the average value in set X, and a is the minimum value in set X:

$$\nu(x) = \begin{cases} 0 & \text{if } x \geq a \\ \dfrac{b-x}{b-a} & \text{if } a \leq x < b \end{cases}$$

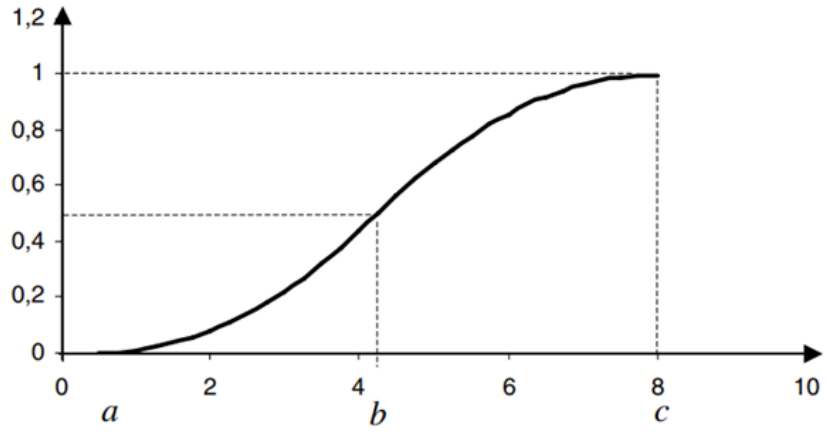

Fig. 1: Membership functions applied to high level of security of fuzzy sets of pictures

3 Famework and security model of public key cryptography of watermark

A. Framework of Public Key Cryptography for Watermark

The public key cryptography scheme consists of the following six algorithms: Key Extraction, Setup Algorithm, Key Generation Algorithm, Encrypt Algorithm, and Decrypt Algorithm:

- **Extract the fuzzy picture (Bio)**

$$\{\langle x, \mu_A(x), \eta_A(x), \nu_A(x)\rangle \mid x \in X\}$$

When entering the user's biometric information, the algorithm will output the fuzzy picture data.

- **Set** $(1^\lambda) \to par$: when entering the security parameter λ, this algorithm will output the public parameter *par*, including the fuzzy key setting

$$\mathscr{F} = ((d, X), t, X, \Phi, \varepsilon)$$

- **KeyGen** $(par, x) \to \mathrm{pk}_f$: when entering the public parameter *par* and the fuzzy picture data of $x \in X$, this algorithm outputs the public key pk_f.
- **Encryption** $(par, \mathrm{pk}_f, M) \to \mathrm{CT}$: When entering the public parameter *par*, the public key pk_f and the message M (in the message space), this algorithm outputs the ciphertext CT.
- **Extract the fuzzy picture (Bio)**

$$\{\langle x', \mu_A(x'), \eta_A(x'), \nu_A(x')\rangle \mid x' \in X\}$$

When entering the user's biometric information, the algorithm will output the fuzzy picture data.

- **Decrypt** $(par, \mathrm{pk}_f, x', \mathrm{CT}) \to M/\perp$: When entering the public parameter par, the public key pk_f, the fuzzy picture data of $x' \in X$, and the ciphertext CT, this algorithm outputs the message M or the error symbol $\perp$.

We say that the public key encryption scheme of a fuzzy picture with the fuzzy key setting $\mathscr{F}$ is correct, meaning that for every security parameter $\lambda \in \mathbb{N}$ with all fuzzy picture data of $x, x' \in X$ such that $\mathrm{d}(x,x') < t$, for all messages M in the message space, if:

$$par \leftarrow \mathrm{Set}(1^\lambda)$$

$$\mathrm{pk}_f \leftarrow \mathrm{KeyGen}(par, x)$$

$$\mathrm{CT} \leftarrow \mathrm{Encrypt}(par, \mathrm{pk}_f, M)$$

we get:

$$\mathrm{Decrypt}(par, \mathrm{pk}_f, x', \mathrm{CT}) = M$$

B. Security Model

Similar to the security definition of a public key cryptography scheme, a fuzzy public key cryptography scheme is required to be indistinguishable under universal faults of the fuzzy key setting $\mathscr{F}$. A fuzzy public key cryptography scheme in fuzzy key setting $\mathscr{F}$ is said to be indistinguishable under chosen ciphertext attacks (IND-CCA security) if for any adversary $\mathscr{A}$ we have an advantage function given by:

$$Adv^{ind-cca}_{\mathrm{FPKE},\mathscr{A}}(\lambda) = Pr\left[b' = b \;\middle|\; \begin{array}{c} par \leftarrow Init(1^\lambda) \\ x^* \leftarrow_R \mathscr{X}, b \leftarrow \{0,1\} \\ pk^*_f \leftarrow KeyGen(par, x^*) \\ (M_0, M_1, \mathrm{state}) \leftarrow \mathscr{A}^{O_{Dec(.)}}(par, pk^*_f) \\ CT^* \leftarrow Encrypt(par, pk^*_f, M) \\ b' \leftarrow \mathscr{A}^{O_{Dec(.)}}(par, pk^*_f, M_0, M_1, \mathrm{state}, CT^*) \end{array} \right] - \frac{1}{2}$$

This is negligible in the security parameter λ, with $|M_0| = |M_1|$ and $O_{\mathrm{DEC}(.)}$ being the decryption guess, taking the public parameter par, the public key pk^*_f, a fragment of the watermark data x^*, and a fragment of the ciphertext CT as input, and outputting the message $M \leftarrow \mathrm{Decrypt}(par, \mathrm{pk}^*_f, x^*, \mathrm{CT})$.

4 Construct algorithm for fuzzy public key encryption

- Encryption Algorithm

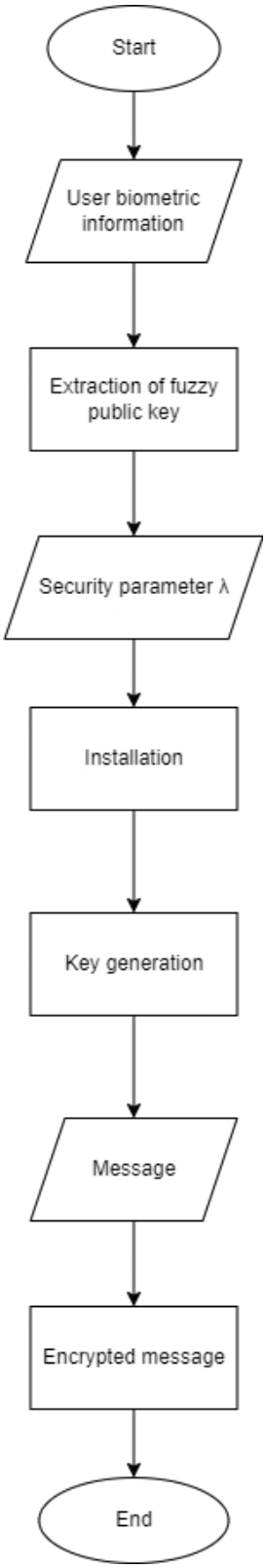

Fig. 2: Encryption Algorithm

Example of the Encryption Algorithm:

1. First, the algorithm will perform the extraction of the biometric information of the user that has been encoded into a vector $x = (5, 7, \ldots, 1)$.

2. Then, it will extract the information of the fuzzy public key $A = \langle 0.75, 0.1, 0.15 \rangle$.

3. After that, choose λ as a random number in the range $\{0, 2^{64} - 1\}$ as the input security parameter.

4. Execute the installation algorithm to obtain the output public parameter:
   par = "MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJQVu6lHAEtia3xc8fCEKd9dpt0jGt7FSiMz"

5. With *par* and fuzzy public key data obtained above through the key generation algorithm, the output public key
   $pk_f = (pk, c)$ = (MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKD/RZvqG4ocFdsCpVpUbgrlYlEumD9qebAIVm3gv1Y6XN7w6jf2B4V9soP9jbXcmwEDy/N6xognyuqKAEB81JUCAwEAAQ==, MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKNQ0UmtSE2dD6Mbx0Vd8GWcTYvqPJNTqyg7xtJAYWWGPmjScKH1VUZw0lIRve3mtlLoxa7mRntUm6iw94ZSCXcCAwEAAQ).

6. Input the message to be encrypted
   M = "PUBLIC ENCRYPTION OF FUZZY PUBLIC KEY" into the algorithm. From the message to be encrypted and the key obtained above through the encryption algorithm, we obtain the ciphertext:
   CT = "exhxWbrXSm7huDc/4LkAHnmk3i91K1FDBqUwpk01gLR0pY8Ow/SQe3xPLpdkSpoTLwm/T3KqI0qGs8HehzXHHw==".

- Decryption Algorithm

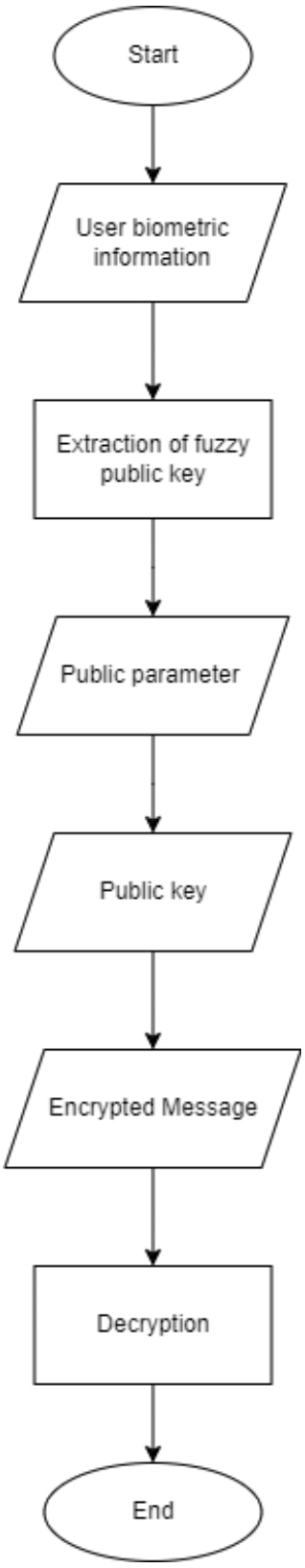

Fig. 3: Decryption Algorithm

Example of the Decryption Algorithm:

1. First, the algorithm will perform the extraction of the biometric information of the user that has been encoded into a vector $x' = (5, 6, \ldots, 1)$.

2. Then, it will extract the information of the fuzzy public key. The output will be the data of the fuzzy public key $A = \langle 0.74, 0.1, 0.15 \rangle$.

3. With the input parameters, including the fuzzy public key, the public parameter:

   par = "MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJQVu6lHAEtia3x c8fCEKd9dpt0jGt7FSiMz", public key:

   pk_f = (MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKD/RZvqG4ocFd sCpVpUbgrlYlEumD9qebAIVm3gv1Y6XN7w6jf2B4V9soP9jbXcmwEDy/N 6xognyuqKAEB81JUCAwEAAQ==,MFwwDQYJKoZIhvcNAQEBBQADS wAwSAJBAKNQ0UmtSE2dD6Mbx0Vd8GWcTYvqPJNTqyg7xtJAYWWG PmjScKH1VUZw0lIRve3mtlLoxa7mRntUm6iw94ZSCXcCAwEAAQ),

   and the code
   CT = "exhxWbrXSm7huDc/4LkAHnmk3i91K1FDBqUwpk01gLR0pY8Ow/S Qe3xPLpdkSpoTLwm/T3KqI0qGs8HehzXHHw==".

4. After the decryption algorithm, we obtain: *M* = "PUBLIC KEY ENCRYPTION OF THE FUZZY PUBLIC KEY".

- Detailed Implementation of the Algorithm

Install the fuzzy key $\mathscr{F} = ((d,X),t,\mathscr{X},\Phi,\varepsilon)$. The Public Fuzzy Public Key Encryption (PFPKE) includes extracting the fuzzy representation, installation, Keygen, key code, and decryption, ensuring IND-CCA security, with K being the space of private keys that determine the key characteristics and homomorphism.

Assume that $S = (\text{S.Setup}, \text{S.Sketch}, \text{S.DiffRec})$ is the probabilistic algorithm for installing the fuzzy key $\mathscr{F}$, and $\text{Sig} = (\text{Sig.KeyGen}, \text{Sig.Sign}, \text{Sig.Verify})$ is the one-time signature algorithm.

The public-key cryptographic scheme of the fuzzy representation (PFPKE) is linked to the installation of the fuzzy key $\mathscr{F}$, including the following steps:

1. **Extract the fuzzy representation**: This step takes the biometric information of the user as input. The output is the fuzzy representation data:

$$\text{Gen(Bio)} = \{\langle x, \mu_A(x), \eta_A(x), \nu_A(x)\rangle \mid x \in X\}.$$

2. **Installation**: The security parameter λ is taken as input. It defines the installation of the fuzzy key $\mathscr{F} = ((d, X), t, \mathscr{X}, \Phi, \varepsilon)$. The public parameter *par* is obtained:

$$par_{pke} \leftarrow_R S.\text{Setup}(1^\lambda), \quad par_S \leftarrow_R S.\text{Setup}(\kappa, +).$$

The final public parameter is:

$$par = (par_{pke}, par_S, \mathscr{F}).$$

3. **KeyGen**: Takes the public parameter par and a part of the fuzzy representation data of x as input. It parses $par = (par_{pke}, par_S)$, then runs:

$$sk \leftarrow_R \kappa, \quad pk \leftarrow \text{KeyGen}(par_{pke}, sk), \quad c \leftarrow_R S.\text{Sketch}(par_S, sk, x).$$

The output is the public key:

$$pk_f = (pk, c)$$

4. **Encryption**: Takes the public parameters par, the public key pk_f, and the message M as input. It parses $par = (par_{pke}, par_S)$ and $pk_f = (pk, c)$. The signature key generation algorithm is run:

$$ssk \leftarrow \text{Sig.KeyGen}(),$$

generating the signing key ssk and verification key svk. The ciphertext CT is obtained by running:

$$CT \leftarrow_R \text{Encoding}(par_{pke}, pk, svk, M).$$

The signature σ is created with the signing key ssk on CT, and the final output is the encoded message:

$$CT = (svk, CT, \sigma).$$

5. **Extract fuzzy representation**: This step takes the user's biometric information as input. The output is the fuzzy representation data:

$$\text{Gen}(\text{Bio}) = \left\{ \langle x', \mu_A(x'), \eta_A(x'), \nu_A(x') \rangle \mid x' \in X \right\}.$$

6. **Decryption**: Takes the public parameters par, the public key pk_f, the fuzzy representation data of $x' \in X$, and the encoded message CT as input. It parses $par = (par_{pke}, par_S)$, $pk_f = (pk, c)$, and $CT = (svk, CT, \sigma)$. If σ is the signature on CT with respect to the public key svk, it will run:

$$\begin{aligned} sk' &\leftarrow_R \kappa \\ pk' &\leftarrow \text{KeyGen'}(par_{pke}, sk') \\ c' &\leftarrow S.\text{Sketch}(par_S, sk', x') \end{aligned}$$

The difference key Δsk is obtained by:

$$\Delta sk \leftarrow S.\text{DiffRec}(par_S, c, c0).$$

Finally, decryption proceeds as:

$$M \leftarrow \text{Decoding}(par_{pke}, \Delta sk, CT, pk', sk'),$$

and the output is the message M.

5 Some additional properties

For the public key encryption scheme used to construct the public key encoding of the fuzzy representation, it is necessary to define some additional properties:

5.1 Key Determination Scheme

The decision key is the KeyGen algorithm that first randomly selects a key sk_{pke} (from the secret key space) and calculates the corresponding public key pk_{pke} (determined by the secret key sk_{pke}) during the key generation process. Formally, a public-key cryptographic scheme is a Key Determination Scheme if the public parameter par_{pke} is generated by a specified set algorithm, specifying the private key space κ_{pke}, and there exists a specified algorithm KeyGen' such that the algorithm to generate the key KeyGen can be defined as $\text{KeyGen}(par_{pke})$:

$$sk_{pke} \leftarrow_R \kappa_{pke}; \quad pk_{pke} \leftarrow \text{KeyGen}'(par_{pke}, sk_{pke}); \quad \text{Return } (sk_{pke}, pk_{pke}).$$

5.2 Homomorphism

The public key encryption scheme is homomorphic if it satisfies the following conditions:

- For the public parameters par_{pke} generated by the setup algorithm, there is an abelian group $(\kappa_{pke}, +)$ associated with the private key space κ_{pke}.
- There exists a deterministic algorithm denoted as $\kappa_{pk_{pke}}$ that takes the public parameters par_{pke}, the public key pk_{pke}, and an input $\Delta sk \in \kappa_{pke}$, and outputs a shifted public key pk'_{pke}. For every par_{pke} in the setup algorithm:

$$\text{KeyGen}'(par_{pke}, sk_{pke} + \Delta sk) = M_{pk_{pke}}(par_{pke}, \text{KeyGen}'(par_{pke}, sk_{pke}, \Delta sk))$$

- There exists an algorithm that determines M_{en}, taking the public parameters par_{pke}, public key pk_{pke}, ciphertext CT, and shifted private key $\Delta sk \in \kappa_{pke}$ as input, and outputs the shifted ciphertext message.

6 Conclusion

In the traditional method, messages encrypted using public key schemes rely on protecting the privacy of the user's private key by storing it in a physical device, such as a USB token carried by the user. However, it is not always practical for the user

to keep the device with them at all times. To solve this problem, using individual biometric data as the private key is a reasonable alternative.

However, biometric data can change every time it is collected, making it unsuitable for direct use as a private key. In this paper, the concept of public key cryptography with fuzzy data is introduced, where a part of the biometric data can be used as the private key to decrypt ciphertexts without requiring any additional information.

Compared to traditional public key encryption, the primary advantage of fuzzy public key encryption is that it does not require the user to carry any memory device or password to function as a private key. When using fuzzy public key encryption, attention should be paid to the value of the fuzzy set in the neutral degree, as these unclear points in system access allow potential vulnerabilities where hackers could access the system.

Acknowledgments

Acknowledgments section

References

Connaughton, R., Bowyer, K., & Flynn, P. (2007). Fusion of face and iris biometrics. In *Handbook of iris recognition*.

Dodis, Y., Ostrovsky, R., Reyzin, L., & Smith, A. D. (2008). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*.

Ellison, C., & Schneier, B. (2000). Ten risks of pki: What you're not being told about public key infrastructure. *Computer Security Journal*, *16*.

Son, L., Viet, P., & Hai, P. (2016). Picture inference system: A new fuzzy inference system on picture fuzzy set. *Applied Intelligence*.

Takahashi, K., Matsuda, T., Murakami, T., Hanaoka, G., & Nishigaki, M. (2015). A signature scheme with a fuzzy private key.