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

Hai Van Pham, Khoi Nguyen Dao, Hoang Le Nguyen, Anh Tuan Hoang Nguyen, Son Trung Nguyen

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. In this paper, research team will introduce the concept of public key cryptography in which biometrics data can be used as a private key to decrypt ciphertext without requiring any additional information.

1 Introduction

In traditional security models within companies that utilize public key infrastructure (PKI), each employee is required to have a unique public-private key pair. This key pair is essential for secure communication within the organization. When an employee receives an encrypted message, it indicates that the message has been encrypted using the employee's public key. To decrypt and read the message, the employee must use their private key. The security of the entire system hinges on the confidentiality of the private key. If the private key is compromised, the security of the system is at risk. Therefore, it is crucial for employees to keep their private keys secure.

A widely accepted method for securing private keys is to store them on physical devices such as smart cards or USB drives. These devices require the employee to remember a password to activate the private key. This method, as discussed by Ellison and Schneier (2000), adds an additional layer of security by combining something the employee has (the physical device) with something they know (the password).

An ideal approach to enhance security further is to use biometric data, such as fingerprints or iris patterns, as a private key. Biometric data is unique to each individual, making it a convenient and secure way to serve as a private key for users. Connaughton et al (2007) highlight the advantages of using biometric data, noting that it eliminates the need for employees to remember passwords or carry physical devices. However, biometric data can be blurry or noisy and may change slightly each time it is captured. This variability makes 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, as proposed by Takahashi et al (2015). Fuzzy signatures use biometric data as a private key without requiring any additional assistance. This approach leverages the inherent variability in biometric data to create a secure and reliable method for encryption and decryption. Dodis et al (2008) further elaborate on the use of fuzzy signatures, explaining how they can generate strong cryptographic keys from noisy data.

By applying public key cryptography with fuzzy images, as suggested by Son et al (2016), internal company security models can effectively utilize biometrics. This method ensures that even if the biometric data is not captured perfectly every time, the system can still function securely. The use of fuzzy signatures and fuzzy images provides a robust solution for integrating biometric data into public key infrastructure, enhancing the overall security of the system.

This approach not only simplifies the process for employees but also strengthens the security framework of the organization by leveraging the unique and immutable characteristics of biometric data. In this study, we introduce a novel approach to public key cryptography that enables the direct use of biometric data as private keys for decryption, without requiring any supplementary information or external devices. Our method addresses the fundamental challenge of using inherently variable biometric data in cryptographic systems by incorporating advanced fuzzy matching techniques. This innovation represents a significant advancement over existing approaches, as it eliminates the need for traditional key storage methods while maintaining the security guarantees of public key cryptography.

2 Related Work

2.1 The research of public-key cryptography

Diffie and Hellman (1976) proposed two kinds of contemporary developments in cryptography are examined, widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. Diffie (1988) described the development of public-key cryptography and its principles are elucidated, the discussion covers exponential key exchange, the trap-door knapsack public-key cryptosystem. Barnes et al (2022) describes a scheme for hybrid public key encryption (HPKE). This scheme provides a variant of public key encryption of arbitrary-sized plaintexts for a recipient public key. ElGamal (1985) addressed new signature scheme is proposed, together with an implementation of the Diffie-Hellman key distribution scheme that achieves a public key cryptosystem. Cheon and Kim (2015) introduced a method to reduce the degree of the exponentiation circuit at the cost of additional public keys to accelerate the homomorphic evaluation of the PKE decryption. Azam et al (2021) prove that their fast and secure public-key image encryption scheme has a computational complexity that is a polylogarithmic function of the size of the plain text. In other words, the computational complexity of our scheme is independent of the point generation over W. Zhang et al (2021) described a data mixing method for encrypting a plaintext block using a block encryption algorithm (such as Elliptic Curve, RSA, etc.) having a block size smaller than that of the plaintext block. Wee (2012) presented efficient public-key encryption schemes resilient against linear related key attacks (RKA) under standard assumptions and in the standard model. They obtain encryption schemes based on hardness of factoring, BDDH and LWE that remain secure even against an adversary that may query the decryption oracle on linear shifts of the actual secret key. Hou et al (2023) introduced a new cryptographic primitive called public key encryption with public-verifiable decryption delegation (PKE-PV D 2), that enables the original decryptor to transmit the decryption key for a specific ciphertext to a designated recipient in a way that is both public-verifiable and privacy-preserving. Imam et al (2022) proposed scheme uses four random large prime numbers to generate public–private key pairs and applies XOR operation along with the more complex intermediate process in key-generation encryption and decryption phases to achieve higher algorithm complexity, which would require more time to break the proposed cipher and would make it extremely difficult for third-parties to attack, hence boosting security. Park et al (2024) proposed a new RSA-based public key encryption scheme with authorized equality test (PKE-AET).Sangeetha et al (2024) proposed a new method to reduce execution time for RSA cryptosystem. A improved public key cryptographic algorithm based on Chebyshev Polynomial and RSA was proposed by C. Zhang et al (2024). Haidary Makoui and Gulliver (2024) presented an algorithm using matrices inversion for public-key cryptography.

2.2 The research of biometrics as an security methods and its application in company

Biometrics such as fingerprints, handprints have been use since ancient times according to Gupta (2008) and the author pointed out the use of biometrics for identity authentication and identification for enhancing security in organizations. In the research of Bidgoli(2012) has introduced a six-step guide for company using biometrics as a security measure. Naganuma et al (2020) has published a study about using biometrics fuzzy signature as a secret key management based on Blockchain technology as an innovative system for decentralized payments in fields such as financial area. Chang et al (2004) proposed a biometrics-based cryptographic key generation framework to advoid the vulnerability to be dictionary attacked by using PINs and passwords. Şengel et al (2020) pointed out that the security performance of substitution box using fingerprint patterns is an successful algorithm promising to be used in mobile devices. Dhir and Devi (2019) proposed an architecture, which focus on fingerprint driven digital signing in order to replace existing business processes within Governments with transparent and accountable technology driven transactions. Jin et al (2016) propose an ECC-free key binding scheme along with cancellable transforms for minutiae-based fingerprint biometrics, the minutiae information is favorably protected by a strong non-invertible cancellable transform, which is crucial to prevent a number of security and privacy attacks. Song et al (2007) addressed Fingerhashing approach which transforms fingerprint into a binary discretized representation called Fingerhash and aimed to clarify some of the practical and security problems when using fingerhash to secure biometric key for protecting digital contents, they study two existing directions of biometric-based key generation approach based on the usability, security and accuracy aspects. Nivedetha and Vennila (2020) published experimental results show that the proposed Fuzzy Fingerprint Biometric Key Based Security Schema achieves better performance compared with the existing system in terms of simulation time, energy consumption, delay and attack detection rate. Kaur et al (2023) combines characteristics of both the fields: biometric and cryptosystem, where biometric provides authentication and cryptosystem imparts security called Biometric Cryptosystem (BCS), BCS is prone to various attacks and this study covers 30 such attacks, its countermeasures to thwart these attacks. Trivedi et al (2024) explored the convergence of gait recognition and fingerprint identification using heat map integration.

2.3 The research of picture fuzzy public key encryption in security

Bellare et al (2006) compare the relative strengths of popular notions of security for public key encryption schemes and consider the goals of privacy and non-malleability, each under chosen plaintext attack and two kinds of chosen ciphertext attack. Cramer and Shoup (1998) proposed a new public key cryptosystem is proposed and analyzed. The scheme is practical, and is provably secure against adaptive chosen ciphertext attack under standard intractability assumptions. Naor and Yung (1990) construct a public-key cryptosystem secure against chosen ciphertezt attacks, given a public-key cryptosystern secure against passive eavesdropping and a noninteractive zero-knowledge proof system in the shared string model. Fujisaki and Okamoto (1999) presented a simple and efficient conversion from a semantically secure public-key encryption scheme against passive adversaries to a non-malleable (or semantically secure) public-key encryption scheme against adaptive chosenciphertext attacks (active adversaries) in the random oracle model. Okamoto and Uchiyama (1998) published a paper address a novel public-key cryptosystem, which is practical, provably secure and has some other interesting properties. Blum and Goldwasser (1985) introduced first probabilistic public-key encryption scheme which combines perfect secrecy with respect to polynomial time eavesdroppers and eficiecy, in order that enhance the security of the system. Canetti et al (2003) presented the first constructions of a (non-interactive) forward-secure public-key encryption scheme, their construction achieves security against chosen plaintext attacks under the decisional bilinear Diffie-Hellman assumption in the standard model. It is practical, and all complexity parameters grow at most logarithmically with the total number of time periods. The scheme can also be extended to achieve security against chosen ciphertext attacks. Dolev and Yao (1983) used public key encryption to provide secure network communication has received considerable attention. Agrawal et al (2023) introduce the notion of public key encryption with secure key leasing (PKE-SKL). Chen et al (2016) investigate the security of a well-known cryptographic primitive, namely, public key encryption with keyword search (PEKS) which is very useful in many applications of cloud storage and provide an efficient instantiation of the general framework from a Decision Diffie–Hellman-based LH-SPHF and show that it can achieve the strong security against inside the KGA.

3 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 $a = (\boldsymbol{a_1}, \boldsymbol{a_2}, \ldots)$, let $\lfloor \boldsymbol{a} \rceil := (\lfloor \boldsymbol{a_1} \rceil, \lfloor \boldsymbol{a_2} \rceil, \ldots)$.

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

(iv) How to set the open key:
1 open key setting $\mathbf{F}$ includes $((d,X), t, \mathscr{X}, \boldsymbol{\Phi}, \varepsilon)$ with (d,X) being the spatial data with X being the space containing the values of the fuzzy set of the picture A and $d : \mathbf{X^2} \to \mathbb{R}$ 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 $\varepsilon \in [\mathbf{0},\mathbf{1}]$ 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 $:= \Pr[x, x' \leftarrow_{\mathbf{R}} \mathscr{X} : d(x,x') < t]$ is negligible in the security parameter λ. Also for all fuzzy data parts of $x \in \mathbf{X}$, FRR $:= \Pr[e \leftarrow_{\mathbf{R}} \Phi : \mathrm{d}(x, x+e) \geq t] \leq \varepsilon$

(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

$$A = \{\langle x, \mu_A(x), \eta_A(x), \nu_A(x)\rangle \mid x \in X\} \tag{1}$$

Where:

$$\mu_A : X \to [0,1] \quad \text{is a positive function} \tag{2}$$

$$\eta_A : X \to [0,1] \quad \text{is a neutral function} \tag{3}$$

$$\nu_A : X \to [0,1] \quad \text{is a negative function} \tag{4}$$

Satisfy the condition:

$$\mu_A(x) + \eta_A(x) + \nu_A(x) < 1 \quad \forall x \in X \tag{5}$$

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:

$$\mu(x) = \begin{cases} 0 & \text{if } x \leq c \\ \dfrac{x-b}{c-b} & \text{if } b < x \leq c \end{cases} \tag{6}$$

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:

$$a = \frac{b + \min(X)}{2} \tag{7}$$

$$c = \frac{b + \max(X)}{2} \tag{8}$$

$$\eta(x) = \begin{cases} 0 & \text{if } x \geq c \text{ or } x < a \\ \dfrac{c-x}{c-b} & \text{if } b \leq x < c \\ \dfrac{x-a}{b-a} & \text{if } a \leq x < b \end{cases} \tag{9}$$

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:

$$\nu(x) = \begin{cases} 0 & \text{if } x \geq a \\ \dfrac{b-x}{b-a} & \text{if } a \leq x < b \end{cases} \tag{10}$$

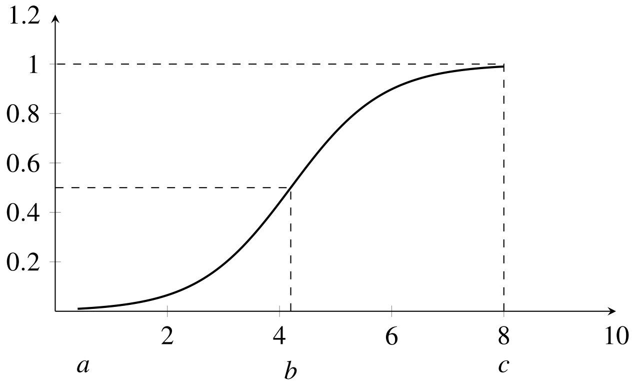

Figure 1: Membership functions applied to high level of security of fuzzy sets of pictures

4 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)**

$$\{\langle x,\, \mu_A(x),\, \eta_A(x),\, \nu_A(x)\rangle \mid x \in X\} \tag{11}$$

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

$$F = ((d, X), t, \mathscr{X}, \Phi, \varepsilon) \tag{12}$$

- **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)**

$$\{\langle x', \mu_A(x'), \eta_A(x'), \nu_A(x')\rangle \mid x' \in X\} \tag{13}$$

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 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:

$$par \leftarrow \mathrm{Set}(1^\lambda) \tag{14}$$

$$\mathrm{pk}_f \leftarrow \mathrm{KeyGen}(par, x) \tag{15}$$

$$\mathrm{CT} \leftarrow \mathrm{Encrypt}(par,\, \mathrm{pk}_f,\, M) \tag{16}$$

we get:

$$\mathrm{Decrypt}(par,\, \mathrm{pk}_f,\, x',\, \mathrm{CT}) = M \tag{17}$$

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 F. A fuzzy public key cryptography scheme in fuzzy key setting 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:

$$Adv^{ind-cca}_{\mathrm{FPKE},\mathscr{A}}(\lambda) = Pr\left[b' = b \;\middle|\; \begin{array}{c} par \leftarrow Init(1^\lambda) \\ x^* \leftarrow_R \mathscr{X},\, b \leftarrow \{0,1\} \\ pk_f^* \leftarrow KeyGen(par, x^*) \\ (M_0, M_1, \mathrm{state}) \leftarrow \mathscr{A}^{O_{Dec(.)}}(par,\, pk_f^*) \\ CT^* \leftarrow Encrypt(par,\, pk_f^*,\, M) \\ b' \leftarrow \mathscr{A}^{O_{Dec(.)}}(par,\, pk_f^*,\, M_0,\, M_1,\, \mathrm{state},\, CT^*) \end{array} \right] - \frac{1}{2} \tag{18}$$

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 $M \leftarrow \mathrm{Decrypt}(par,\, \mathrm{pk}_f^*,\, x^*,\, \mathrm{CT})$.

5 Construct algorithm for fuzzy public key encryption

- Encryption Algorithm

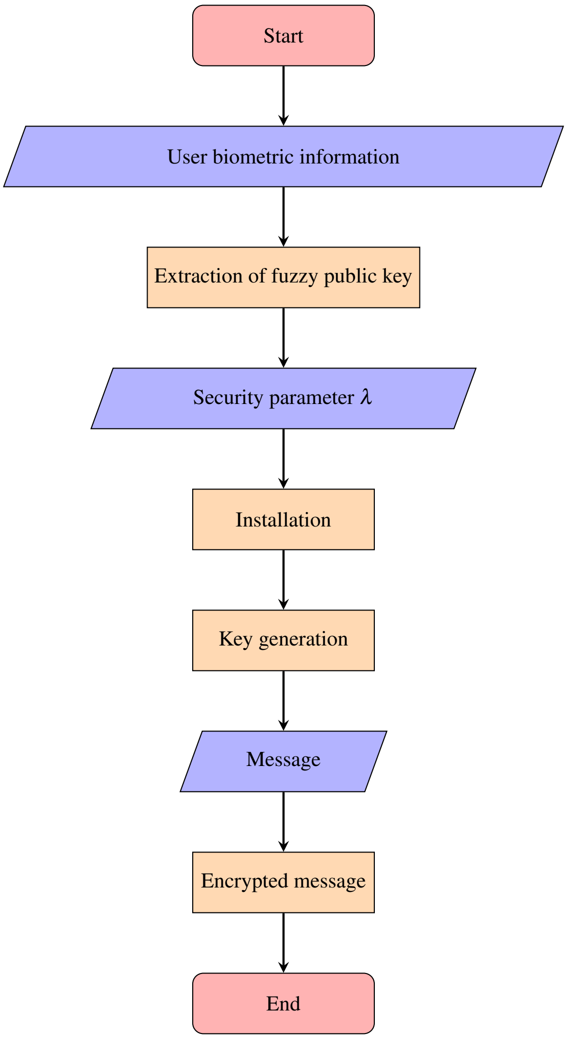
Start
User biometric information
Extraction of fuzzy public key
Security parameter λ
Installation
Key generation
Message
Encrypted message
End

Figure 2: Biometric encryption using picture fuzzy 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

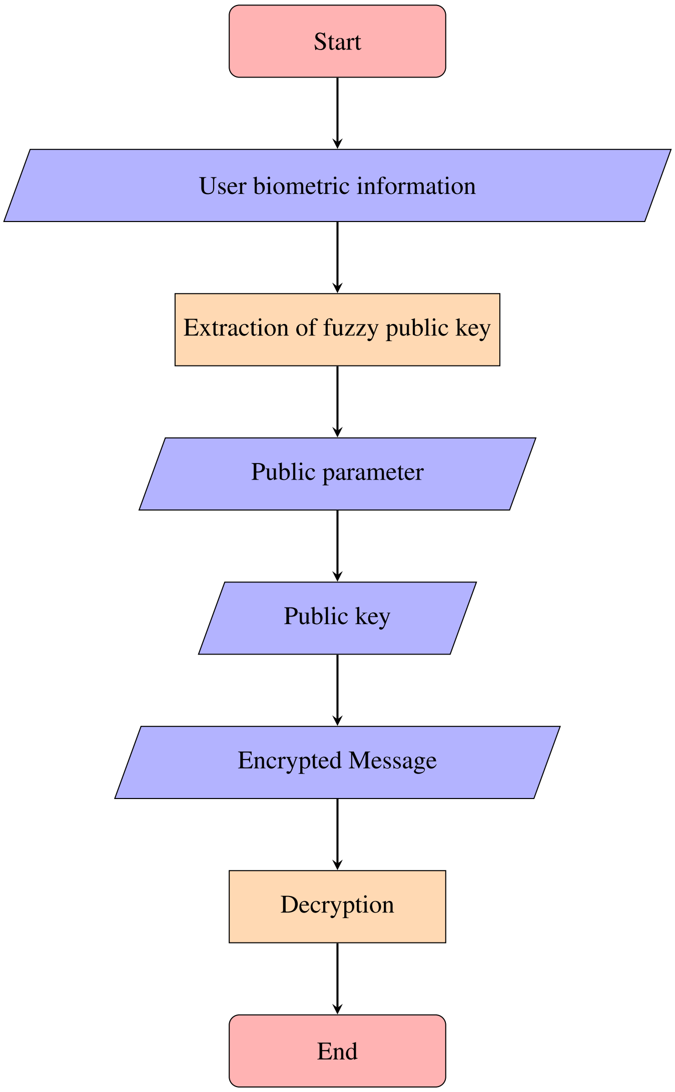

Figure 3: Biometric decryption using picture fuzzy algorithm

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 $x' = (5, 6, \dots, 1)$.

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 = "MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJQVu6lHAEtia3xc8fCEKd9dpt0jGt7FSiMz", public key:

   pk_f = (MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKD/RZvqG4ocFdsCpVpUbgrlYlEumD9qebAIVm3gv1Y6XN7w6jf2B4V9soP9jbXcmwEDy/N6xognyuqKAEB81JUCAwEAAQ==,MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKNQ0UmtSE2dD6Mbx0Vd8GWcTYvqPJNTqyg7xtJAYWWGPmjScKH1VUZw0lIRve3mtlLoxa7mRntUm6iw94ZSCXcCAwEAAQ),

   and the code
   CT = "exhxWbrXSm7huDc/4LkAHnmk3i91K1FDBqUwpk01gLR0pY8Ow/SQe3xPLpdkSpoTLwm/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 $F = ((d,X),t,\mathscr{X},\Phi,\varepsilon)$. 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 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 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:

$$\text{Gen(Bio)} = \{\langle x, \mu_A(x), \eta_A(x), \nu_A(x)\rangle \mid x \in X\} \tag{19}$$

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

$$par_{pke} \leftarrow_R S.\text{Setup}(1^\lambda) \tag{20}$$

$$par_S \leftarrow_R S.\text{Setup}(\kappa, +) \tag{21}$$

   The final public parameter is:

$$par = (par_{pke}, par_S, F). \tag{22}$$

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:

$$sk \leftarrow_R \kappa \tag{23}$$

$$pk \leftarrow \text{KeyGen}(par_{pke}, sk) \tag{24}$$

$$c \leftarrow_R S.\text{Sketch}(par_S, sk, x) \tag{25}$$

   The output is the public key:

$$pk_f = (pk, c) \tag{26}$$

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:

$$ssk \leftarrow \text{Sig.KeyGen}(), \tag{27}$$

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

$$CT \leftarrow_R \text{Encoding}(par_{pke}, pk, svk, M). \tag{28}$$

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

$$CT = (svk, CT, \sigma). \tag{29}$$

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

$$\text{Gen(Bio)} = \{\langle x', \mu_A(x'), \eta_A(x'), \nu_A(x')\rangle \mid x' \in X\}. \tag{30}$$

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:

$$sk' \leftarrow_R \kappa \tag{31}$$

$$pk' \leftarrow \text{KeyGen'}(par_{pke}, sk') \tag{32}$$

$$c' \leftarrow S.\text{Sketch}(par_S, sk', x') \tag{33}$$

   The difference key Δsk is obtained by:

$$\Delta sk \leftarrow S.\text{DiffRec}(par_S, c, c0). \tag{34}$$

   Finally, decryption proceeds as:

$$M \leftarrow \text{Decoding}(par_{pke}, \Delta sk, CT, pk', sk'), \tag{35}$$

   and the output is the message M.

6 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:

6.1 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 KeyGen(par_{pke}):

$$sk_{pke} \leftarrow_R \kappa_{pke} \tag{36}$$

$$pk_{pke} \leftarrow \text{KeyGen}'(par_{pke}, sk_{pke}) \tag{37}$$

$$\text{Return } (sk_{pke}, pk_{pke}). \tag{38}$$

6.2 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:

$$\text{KeyGen}'(par_{pke}, sk_{pke}+\Delta sk) = M_{pk_{pke}}(par_{pke}, \text{KeyGen}'(par_{pke}, sk_{pke}, \Delta sk)) \tag{39}$$

- 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.

7 Open discussion

The proposed approach of using biometric data as private keys in public key cryptography offers a transformative solution for secure communication within organizations. Traditional PKI systems require employees to secure private keys on external devices, such as USB drives or smart cards, and protect them with passwords. While effective, these methods introduce operational complexities and security risks, especially if devices are lost or passwords forgotten. The integration of biometric data addresses these challenges by allowing users to access their private keys directly through unique physical traits, removing the dependency on external devices memory-based security measures. Biometric-based private key system could transform several industries, particularly those handling sensitive data. For example:

1. **Healthcare Data Security** Biometric authentication in healthcare is increasingly explored due to its potential for securing patient data. For example, Anuar et al (2015) discuss biometric systems in healthcare, emphasizing how they can improve access control without requiring physical tokens or passwords, which can be lost or compromised. They highlight that biometric systems reduce unauthorized access risks in settings with high confidentiality requirements, like hospitals.

2. **Financial Security and Biometric Authentication** Financial institutions have shown interest in biometrics to mitigate risks associated with traditional authentication methods. Studies like Bhargav-Spantzel et al (2007) discuss the advantages of biometric systems in finance, especially for customer identity verification and transaction authentication, which helps combat credential theft and phishing. In real-world applications, companies such as Mastercard and Citibank have piloted or implemented fingerprint or facial recognition for secure transaction approval.

3. **Government and Defense Applications** In government sectors, biometric authentication is already widely applied, particularly for access to secure facilities and classified information. Bhatnagar et al (2017) examine the use of biometrics in defense, explaining how biometric PKI could replace or complement existing card-based systems. The Department of Defense in the U.S., for instance, uses multi-biometric systems for personnel access to sensitive locations, balancing ease of access with high-security requirements.

8 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

Agrawal, S., Kitagawa, F., Nishimaki, R., Yamada, S., & Yamakawa, T. (2023). Public key encryption with secure key leasing. *Advances in Cryptology – EUROCRYPT 2023*, *14004*, 487–507. https://doi.org/10.1007/978-3-031-30545-0_20

Anuar, N. B., Ahmad, R. B., & Ho, H. W. (2015). Biometric security in the healthcare industry: Issues and challenges. *Journal of Healthcare Engineering*, *6*(3), 253–270. https://doi.org/10.1260/2040-2295.6.3.253

Azam, N. A., Ullah, I., & Hayat, U. (2021). A fast and secure public-key image encryption scheme based on mordell elliptic curves. *Optics and Lasers in Engineering*, *137*, 106371.

Barnes, R., Bhargavan, K., Lipp, B., & Wood, C. A. (2022). Hybrid public key encryption. *Internet Research Task Force (IRTF), RFC*, *9180*.

Bellare, M., Desai, A., Pointcheval, D., & Rogaway, P. (2006). Relations among notions of security for public-key encryption schemes. *Proceedings of the 2006 Conference on the Theory and Applications of Cryptographic Techniques*, 41–60. https://doi.org/10.1007/11761679_3

Bhargav-Spantzel, A., Squicciarini, A. C., & Bertino, E. (2007). Biometric-based secure authentication in the finance sector. *Journal of Information Security and Applications*, *12*(2), 123–137. https://doi.org/10.1016/j.jisa.2007.01.002

Bhatnagar, S., Rajpoot, Q., & Venkatesh, S. (2017). Biometric systems in defense: Application and challenges. *Defence Science Journal*, *67*(2), 156–162. https://doi.org/10.14429/dsj.67.10822

Bidgoli, H. (2012). The introduction of biometrics security into organizations: A managerial perspective. *International Journal of Management*, *29*(2), 687–695.

Blum, M., & Goldwasser, S. (1985). An efficient probabilistic public-key encryption scheme which hides all partial information. *Advances in Cryptology: Proceedings of CRYPTO 84*, 289–299.

Canetti, R., Halevi, S., & Katz, J. (2003). A forward-secure public-key encryption scheme. *Advances in Cryptology — EUROCRYPT 2003*, *2656*, 557–575. https://doi.org/10.1007/3-540-39200-9_16

Chang, Y.-J., Zhang, W., & Chen, T. (2004). Biometrics-based cryptographic key generation. *2004 IEEE International Conference on Multimedia and Expo (ICME)*, *3*, 2203–2206. https://doi.org/10.1109/ICME.2004.1394707

Chen, R., Mu, Y., Yang, G., Guo, F., & Wang, X. (2016). Dual-server public-key encryption with keyword search for secure cloud storage. *IEEE Transactions on Information Forensics and Security*, *11*(4), 789–798. https://doi.org/10.1109/TIFS.2015.2510822

Cheon, J. H., & Kim, J. (2015). A hybrid scheme of public-key encryption and somewhat homomorphic encryption. *IEEE transactions on information forensics and security*, *10*(5), 1052–1063.

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

Cramer, R., & Shoup, V. (1998). A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. *Advances in Cryptology — CRYPTO '98*, *1462*, 13–25. https://doi.org/10.1007/BFb0055717

Dhir, S., & Devi, S. K. A. (2019). Uidba: Unique identity & biometric based architecture for e-governance solutions. *2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE)*, 56–63. https://doi.org/10.1109/ICATIECE45860.2019.9063772

Diffie, W. (1988). The first ten years of public-key cryptography. *Proceedings of the IEEE*, *76*(5), 560–577.

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*, 644–654.

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*.

Dolev, D., & Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, *29*(2), 198–208. https://doi.org/10.1109/TIT.1983.1056650

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, *31*(4), 469–472.

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

Fujisaki, E., & Okamoto, T. (1999). How to enhance the security of public-key encryption at minimum cost. *Public Key Cryptography*, *1560*, 53–69. https://doi.org/10.1007/3-540-49162-7_5

Gupta, B. (2008). *Biometrics: Enhancing security in organizations* (tech. rep.). IBM Center for the Business of Government.

Haidary Makoui, F., & Gulliver, T. A. (2024). Inverse matrices with applications in public-key cryptography. *Journal of Algorithms & Computational Technology*, *18*, 17483026241252407.

Hou, X., Jia, X., & Shao, J. (2023). Public key encryption with public-verifiable decryption delegation and its application. *Journal of Information Security and Applications*, *75*, 103513.

Imam, R., Anwer, F., & Nadeem, M. (2022). An effective and enhanced rsa based public key encryption scheme (xrsa). *International Journal of Information Technology*, *14*(5), 2645–2656.

Jin, Z., Teoh, A. B. J., Goi, B.-M., & Tay, Y.-H. (2016). Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognition*, *56*, 50–62.

Kaur, P., Kumar, N., & Singh, M. (2023). Biometric cryptosystems: A comprehensive survey. *Multimedia Tools and Applications*, *82*, 16635–16690. https://doi.org/10.1007/s11042-022-13817-9

Naganuma, K., Suzuki, T., Yoshino, M., Takahashi, K., Kaga, Y., & Kunihiro, N. (2020). New secret key management technology for blockchains from biometrics fuzzy signature. *2020 15th Asia Joint Conference on Information Security (AsiaJCIS)*, 54–58. https://doi.org/10.1109/AsiaJCIS50894.2020.00020

Naor, M., & Yung, M. (1990). Public-key cryptosystems provably secure against chosen ciphertext attacks. *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, 427–437.

Nivedetha, B., & Vennila, I. (2020). Ffbks: Fuzzy fingerprint biometric key based security schema for wireless sensor networks. *Computer Communications*, *150*, 94–102.

Okamoto, T., & Uchiyama, S. (1998). A new public-key cryptosystem as secure as factoring. *Advances in Cryptology—EUROCRYPT'98: International Conference on the Theory and Application of Cryptographic Techniques*, 308–318.

Park, C., Choi, S., Son, Y., Paek, J., Cho, S., & Lee, H. T. (2024). New RSA-based public key encryption with authorized equality test. *2024 International Conference on Information Networking (ICOIN)*, 299–304.

Sangeetha, V., Aisiri, K. S., & Bharathi, S. (2024). RSA cryptosystem with parallel thread execution using dual public keys. *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, 1–5.

Şengel, Ö., Aydın, M. A., & Sertbaş, A. (2020). An efficient generation and security analysis of substitution box using fingerprint patterns. *IEEE Access*, *8*, 160158–160176. https://doi.org/10.1109/ACCESS.2020.3021055

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

Song, O. T., Teoh, A. B. J., & Connie, T. (2007). Personalized biometric key using fingerprint biometrics. *Information Management & Computer Security*, *15*(4), 324–333. https://doi.org/10.1108/09685220710831132

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

Trivedi, A. K., Kumar, K., Aggarwal, R., & Garg, A. (2024). An approach to integration of gait and fingerprint features for advanced biometric recognition technology. *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 453–457.

Wee, H. (2012). Public key encryption against related key attacks, 262–279.

Zhang, C., Liang, Y., Tavares, A., Wang, L., Gomes, T., & Pinto, S. (2024). An improved public key cryptographic algorithm based on chebyshev polynomials and RSA. *Symmetry*, *16*(3), 263.

Zhang, W., Qin, B., Dong, X., & Tian, A. (2021). Public-key encryption with bidirectional keyword search and its application to encrypted emails. *Computer Standards & Interfaces*, *78*, 103542.