A Novel Key Sharing Fuzzy Vault Scheme

Lin You[1], Yuna Wang[1], Yulei Chen[1], Qi Deng[1], and Huanhuan Zhang[1]
[1] School of Cmmunication Engineering, Hangzhou Dianzi University,
Hangzhou 310018, China
[e-mail: youlin@hdu.edu.cn;yunai1990@163.com; hdu_cyl@qq.com;307285568@qq.com; 917691965@qq.com]
*Corresponding author: Yuna Wang

Received March 19, 2015; revised January 9, 2016; revised April 20, 2016; accepted July 23, 2016; published September 30, 2016

Abstract

A novel key sharing fuzzy vault scheme is proposed based on the classic fuzzy vault and the Diffie-Hellman key exchange protocol. In this proposed scheme, two users cooperatively build their fuzzy vault for their shared key using their own biometrics. Either of the users can use their own biometrics to unlock the fuzzy vault with the help of the other to get their shared key without risk of disclosure of their biometrics. Thus, they can unlock the fuzzy vault cooperatively. The security of our scheme is based on the security of the classic fuzzy vault scheme, one-way hash function and the discrete logarithm problem in a given finite group.

Keywords: Fuzzy vault, Diffie-Hellman key exchange, finite group, biometrics, polynomial interpolation

This work is partially supported by the National Science Foundation of China (No. 61272045, No. 61328207), Zhejiang Qianjiang Talents Project (No. 2013R10071) and Zhejiang Province Science and Technology Innovation Program (2013TD03).

http://dx.doi.org/10.3837/tiis.2016.09.030 **ISSN : 1976-7277**

1. Introduction

Biometric-based authentication can enhance the security of users' identity and has been widely applied to various fields now. Since the compromise of the data will be permanent, the security of biometric data itself is particularly important. Taking this into account, we need to store such data in a non-invertible transformed version to block unauthorized access. Fuzzy vault is a cryptographic construction proposed by Juels and Sudan in 2002 [1] to secure critical data with biometric data. In their fuzzy vault scheme, they used user's unique biometric data set to bind his/her secure data within a vault based on Reed-Solomon codes. Legitimate users can recover their secure data by providing a biometric data set that overlaps to a definable amount with the original set. An attacker cannot obtain the user's secure data or the biometric data set even if they were able to obtain the vault itself. Diffie-Hellman key exchange scheme is a cryptographic protocol which provides users an authentic way who have no prior knowledge about each other to produce a shared key without their security being compromised. In some cases, the key is available only if both users' biometric data were presented. We propose a novel key sharing fuzzy vault based on the classical fuzzy vault and the Diffed-Hellman key exchange scheme. Only shall two users cooperate with each other, their shared fuzzy vault with a shared key will be built by using their own biometrics, and either user could use his/her biometrics to unlock the fuzzy vault with the help of the other to get their shared key. Neither user can obtain the shared key independently. The security of our proposed fuzzy vault scheme is based on the security of the classical fuzzy vault scheme, one-way hash function and the discrete logarithm problem in a given finite group.

In Section 2, several versions of fuzzy vault scheme are introduced. Our proposed novel key sharing fuzzy vault scheme is specified in Section 3. Its simulation results and the security analysis of our proposed scheme are given in Section 4. Section 5 discusses our findings and some applications of our proposed scheme.

2. Several Fuzzy Vault Schemes

The classic fuzzy vault scheme was proposed by Juels and Sudan in 2002 and was revised in 2006 [2]. The fuzzy vault is a scheme for the secure protection of personal data (which we will call a key) using a private message set which generally comes from the user's unique biometrics. A fuzzy vault scheme includes the Locking Algorithm and the Unlocking Algorithm.

A fuzzy vault scheme includes a finite field $\mathbb{F}_q$ with q a power of a prime and a Reed-Solomon decoding algorithm (RSDECODE). The most practical choice for RSDECODE is the Reed-Solomon decoding algorithm based on Newton's interpolation [3] or Lagrange interpolation polynomial. The following two algorithms for the fuzzy vault scheme are from the revised work of Juels and Sudan [2] with some minor changes. Its security is based on a polynomial reconstruction problem.

2.1 Locking Algorithm

INPUT: Parameters n, t, and r such that $n \le t \le r \le q$, a pre-selected secret key $k \in \mathbb{F}_q$, a set $A = \{a_i\}_{i=1}^{t}$, where $a_i \in \mathbb{F}_q$ is distinct.

OUTPUT: A fuzzy vault with $V = \{R, (n, r, q)\}$.

1. X, R, $V \leftarrow \varnothing$;

2. $P \leftarrow k$, that is, k is block-encoded into the polynomial of degree n in $\mathbb{F}_q$ as its coefficients;

3. For $i = 1$ to t, do

   (1) $(x_i, y_i) \leftarrow (a_i, P(a_i))$;

   (2) $X \leftarrow X \bigcup \{x_i\}$;

   (3) $R \leftarrow R \bigcup \{(x_i, y_i)\}$.

4. For $i = t+1$ to r, do

   (1) $x_i \in_U \mathbb{F}_q \setminus X$;

   (2) $X \leftarrow X \bigcup \{x_i\}$;

   (3) $y_i \in_U \mathbb{F}_q \setminus \{P(x_i)\}$;

   (4) $R \leftarrow R \bigcup \{(x_i, y_i)\}$.

5. Output R or $V = \{R, (n, r, q)\}$.

To make sure that the information about the order of x_i is safely chosen, the set R should be output in a pre-determined order, e.g., the points in R may be arranged in order of ascending x-coordinates, or in a random order. For security, the chaff points in the locking algorithm should be selected to intersect neither A nor the polynomial P. Generally, V combining R and (n, r, q) is called a fuzzy vault.

2.2 Unlocking Algorithm

INPUT: A fuzzy vault V, comprising parameter set (n, r, q), such that $n \le r << q$, and a set R of r points with their two-dimensional coordinates belong to $\mathbb{F}_q$. A query set $B = \{b_i\}_{i=1}^{t}$ with $b_i \in \mathbb{F}_q$.

OUTPUT: An element $k' \in \mathbb{F}_q^n \bigcup \{'null'\}$.

1. $Q \leftarrow \varnothing$;

2. For $i = 1$ to t, do

   (1) If there exists some $y_i \in \mathbb{F}_q$ such that $(b_i, y_i) \in R$, $Q \leftarrow Q \bigcup (b_i, y_i)$;

   (2) Set $k' \leftarrow null$ if Q has less than n points;

   (3) Otherwise, set $k' \leftarrow RS_{DECODE}(n, Q)$;

3. Output k'.

Suppose that the fuzzy vault V is created by Alice, and Bob tries to unlock V to recover the key k. Bob uses his set B to determine the codeword which encoded k to get a possible key k'. The set A specifies the x-coordinates of the correct points that lie on the

polynomial P. If B is close enough to A, it may identify a majority of these correct points. However, any divergence between A and B will bring error. This error or noise may be removed by a Reed-Solomon decoding algorithm if a majority of the points overlap.

In 2012, Lin and Jie [4] combined the Diffie-Hellman key exchange scheme with fuzzy vault scheme and proposed a fuzzy vault scheme for key exchange, the FV-DH scheme. In that scheme, the two users used the Diffie-Hellman key exchange protocol to produce a shared key, either of them may use their private biometrics to build a fuzzy vault separately with real and chaff points mixed, and store their different vaults, including the shared key, on their own computers. Lin and Jie considered the users' fingerprints as the input biometrics in the fuzzy vault. If either user wants to unlock the fuzzy vault and obtain the key, they need to use their own fingerprints. The locking algorithm and unlocking algorithm for the FV-DH scheme is shown in **Fig. 1** and **Fig. 2**.

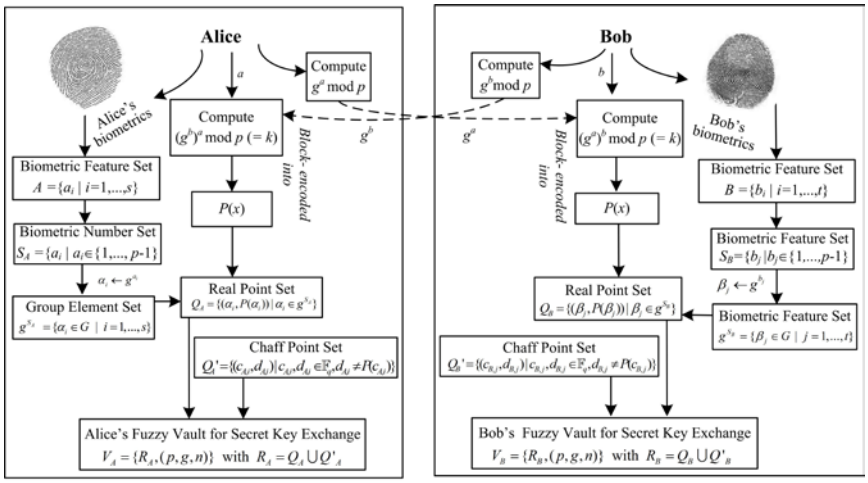


Fig. 1. FV-DH locking algorithm

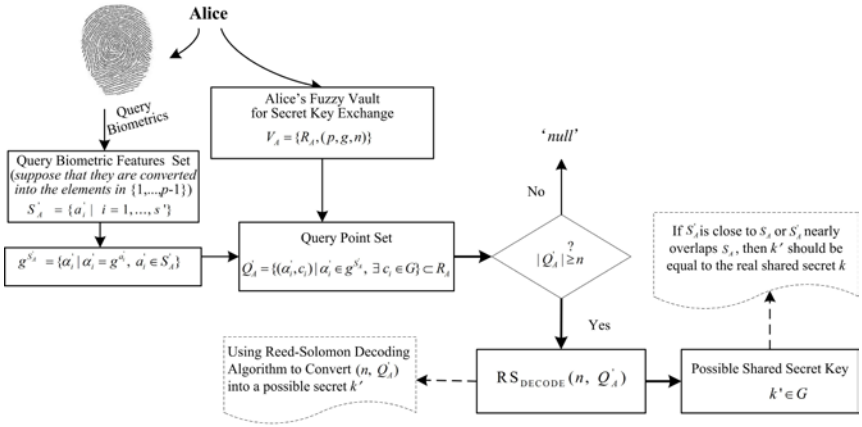


Fig. 2. FV-DH unlocking algorithm (for Alice)

A key sharing fuzzy vault scheme, the KSFV scheme was also proposed by Lin and Mengsheng [5]. The scheme is that the users cooperatively built their shared fuzzy vault based on a Diffie-Hellman key exchange scheme. The two users can independently use their

personal biometrics to unlock the fuzzy vault to obtain the shared key. That article provides the motivation for the work reported here. The locking algorithm and unlocking algorithm for the FV-DH scheme is shown in **Fig. 3** and **Fig. 4**.

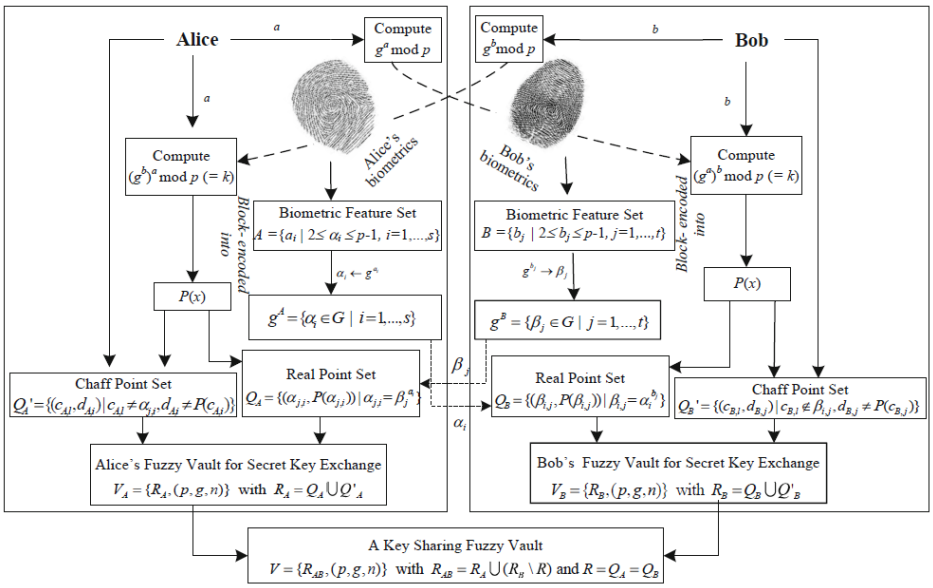


Fig. 3. KSFV-locking algorithm

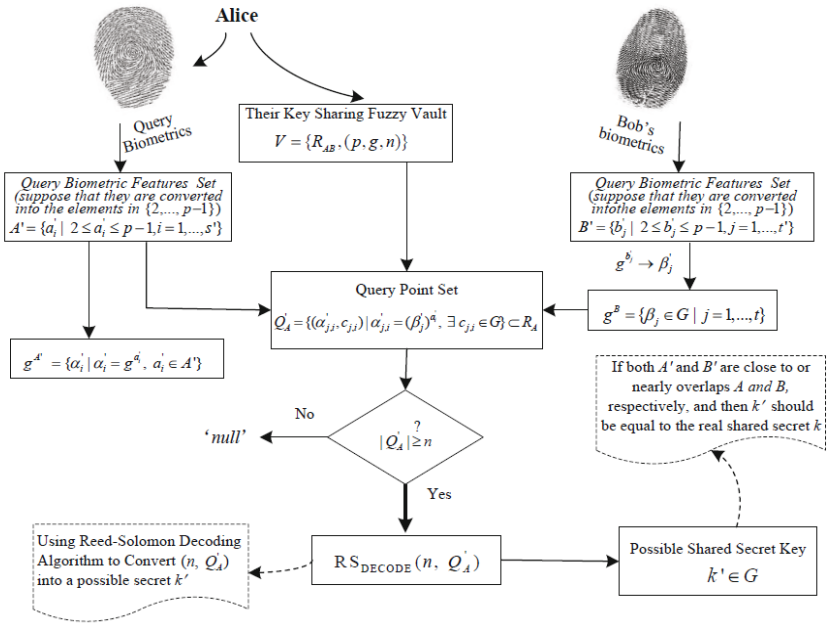


Fig. 4. KSFV-unlocking algorithm (for Alice)

In 2013, Thi Hanh Nguyen and Yi Wang [6] proposed and employed a chaff point generation algorithm to improve the performance and security of fingerprint fuzzy vault scheme. In 2014, Thi Thuy Linh Vo, Tran Khanh Dang and Josef Küng [7] proposed a method for storing the biometric fuzzy vault based on hash mapping and the method helps to prevent attacks via record multiplicity and stolen key attacks.

3. A Novel Key Sharing Fuzzy Vault Scheme

The Diffie-Hellman key exchange scheme [8] is a popular key sharing scheme for two parties to establish a shared secret key without any prior knowledge over an insecure communications channel. This established shared key can be used in any symmetric key algorithm, so the Diffie-Hellman key exchange scheme could also be applied to our work.

Suppose that Alice and Bob want to establish a shared secret key for their future cryptographic applications using their biometrics, such as their fingerprints. They agree on a finite multiplicative group $G = \mathbb{F}_q^*$, where q is a power of a large prime; and a cyclic subgroup $< g >$ of G, where g is an element of some large prime order p. The parameters G, q, g, and p are assumed to be public. If Alice or Bob want to obtain the key, they use their biometrics to unlock the fuzzy vault with the other's help. Neither of them can open the fuzzy vault independently.

Our proposed scheme also consists of the locking and unlocking algorithms. The locking algorithm introduces a novel way to build the shared information by exchanging biometric data and binds the shared key to generate a shared fuzzy vault. The unlocking algorithm describes the method for recovering the shared key from the shared fuzzy vault by using users' biometrics.

3.1 Our Locking Algorithm

Our proposed scheme consists of a locking algorithm and an unlocking algorithm. The locking algorithm introduces a novel way to build the shared information by exchanging biometric data and binds the shared key with the shared information to generate a shared fuzzy vault. The unlocking algorithm describes the method for recovering the shared key from the shared fuzzy vault by using users' biometrics.

INPUT: A finite multiplicative group $G = \mathbb{F}_q^*$, where q is a prime power; and one of its cyclic subgroup $H =< g >$ with a large prime order p; positive integers n, s_1, s_2, r_A, and r_B, where $n \le \min\{s_1, s_2\} \le s_1 \cdot s_2 \le r_A$, $r_B << p$. All these parameters are made public.

OUTPUT: $V_{AB} = \{R_{AB}, (p, g, n)\}$, where R_{AB} is a set composed of much more than n points with their coordinates $\in \mathbb{F}_q^*$.

1. X, $\overline{X}$, G_A, G_B, $g^{F'_A}$, $g^{F'_B}$, Q_R, R_A, $R_B \leftarrow \varnothing$;
2. Alice and Bob produce their shared key based on Diffie-Hellman protocol:
   (1) Alice randomly selects a select key $a \in G$, computes $\alpha = g^a \bmod p$, and sends α to Bob;
   (2) Bob randomly selects a select key $b \in G$, computes $\beta = g^b \bmod p$, and sends β to Alice;
   (3) Alice computes $(\beta)^a$ and deletes a;

(4) Bob computes $(\alpha)^b$ and deletes b;

(5) $k = H((\beta)^a \bmod p) = H((\alpha)^b \bmod p)$ (Since $(g^b)^a = g^{ba} = g^{ab} = (g^a)^b \bmod p$, k can be regarded as Alice and Bob's shared key);

3. Alice and Bob construct a polynomial $P(x)$ using the shared key k. That is, k is divided into n sections $a_i (i = 0, \ldots, n-1)$, which construct the polynomial coefficients of $P(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$;
4. Alice does the following steps:

(1) Extract her private biometrics $F_A = \{(x_{Ai}, y_{Ai}, \theta_{Ai}, t_{Ai}) \mid i = 1, \ldots, s_1\}$. (A fingerprint minutia represented by $(x_i, y_i, \theta_i, t_i)$ is composed of four elements: x and y coordinates, *angle*, and *type*);

(2) For $i = 1, \ldots, s_1$, do

(i) $u_{Ai} = [x_{Ai} \| y_{Ai}]$;

(ii) $G_A \leftarrow G_A \bigcup \{a_{Ai} = (u_{Ai}, \theta_{Ai}, t_{Ai})\}$;

(iii) Compute $g^{u_{Ai}} \bmod p$, $g^{\theta_{Ai}} \bmod p$;

(iv) Set $\alpha_i = (g^{u_{Ai}}, g^{\theta_{Ai}}, t_{Ai})$;

(v) $g^{F'_A} \leftarrow g^{F'_A} \bigcup \{\alpha_i\}$;

(vi) Send $g^{F'_A}$ to Bob.

5. Bob performs the same process (Step 4) as Alice to obtain β_j and $g^{F'_B}$.
6. After receiving $g^{F'_B}$ from Bob, Alice does

(1) For $i = 1, \ldots, s_1$, $j = 1, \ldots, s_2$:

(i) Compute $\alpha_{j,i} = (\beta_j)^{a_{Ai}} \bmod p = (g^{u_{Bj}}, g^{\theta_{Bj}}, t_{Bj})^{(u_{Ai}, \theta_{Ai}, t_{Ai})} = (g^{u_{Bj}u_{Ai}}, g^{\theta_{Bj}\theta_{Ai}}, t_{Bj} \wedge t_{Ai})$;

(ii) $(x_{i,j}, y_{i,j}) \leftarrow (\alpha_{j,i}, P(\alpha_{j,i}))$;

(iii) $X \leftarrow X \bigcup \{x_{i,j}\}$;

(iv) $Q_R \leftarrow Q_R \bigcup \{(x_{i,j}, y_{i,j})\}$.

(2) For $l = s_1 \cdot s_2 + 1$ to r_A, do:

(i) $x_l \in_U < g > \backslash X$;

(ii) $\overline{X} \leftarrow \overline{X} \bigcup \{x_l\}$;

(iii) $y_l \in_U < g > \backslash P(x_l)$;

(iv) $R_A \leftarrow Q_R \bigcup \{(x_l, y_l)\}$;

(v) $X \leftarrow \varnothing$;

(3) Send R_A to Bob.

7. Bob does similar steps to generate R_B with the same real point set Q_R, and $r_B - s_1 \cdot s_2$ chaff points.
8. Set $R_{AB} = R_A \bigcup (R_B \setminus Q_R)$. (Note that $R_{AB} = (R_A \bigcup R_B) \setminus Q_R = R_B \bigcup (R_A \setminus Q_R)$).
9. Output $V_{AB} = \{R_{AB}, (p, g, n)\}$.

The output V_{AB} is regarded as the key sharing fuzzy vault owned by both Alice and Bob. If one of them wants to restore the shared key k they can use their own biometrics to restore the possible shared key with the help of the other by the following Unlocking Algorithm. This means that Alice or Bob cannot unlock the fuzzy vault if they do not cooperate with each other.

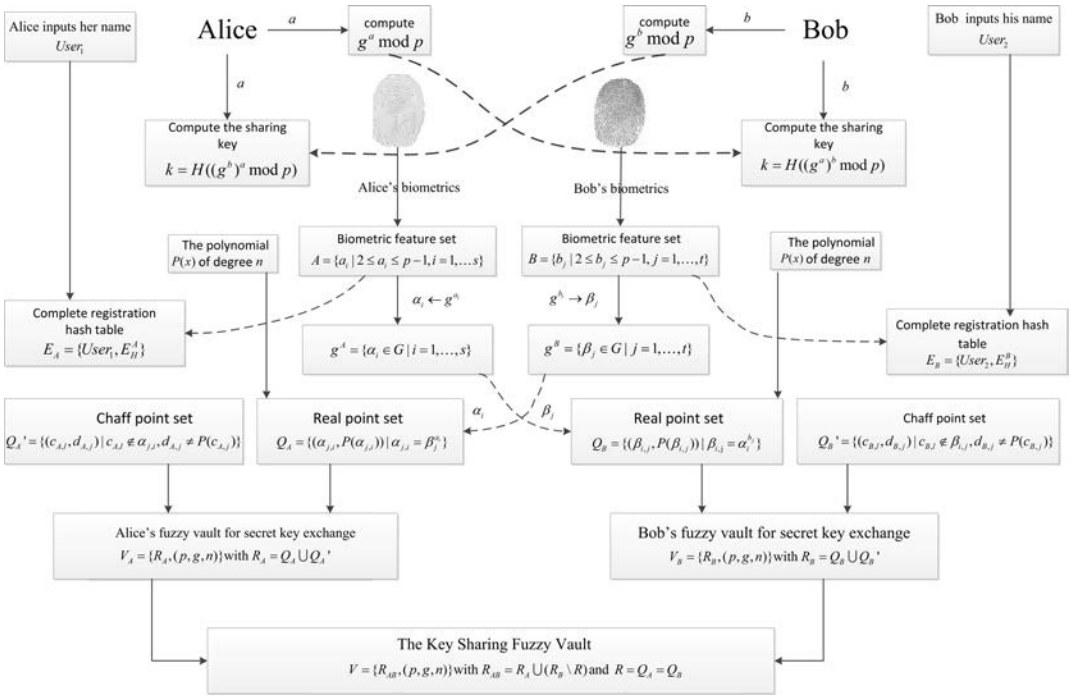


Fig. 5. Proposed locking algorithm

3.2 Our Unlocking Algorithm

INPUT: A finite multiplicative group $G = \mathbb{F}_q^*$, and one of its cyclic subgroup $< g >$ with large prime order p; Alice and Bob's biometric sets $Q'_A = \{x_w^A, y_w^A, \theta_w^A, t_w^A \mid w = 1, \ldots, |Q'_A|\}$ and $Q'_B = \{x_v^B, y_v^B, \theta_v^B, t_v^B \mid v = 1, \ldots, |Q'_B|\}$, respectively; A set $V_{AB} = \{R_{AB}, (p, g, n)\}$ satisfying $n \le \min\{s_1, s_2\} \le s_1, s_2 \le r_A, r_B << p$, and the all points in $R_{AB} \in \mathbb{F}_q^* \times \mathbb{F}_q^*$.

OUTPUT: An element $k' \in \mathbb{F}_q^* \bigcup \{'null'\}$.

1. $Q_R \leftarrow \varnothing$;
2. If Alice wants to recover the shared key k, she performs the steps:
   (1) Extract her private biometrics and get $Q'_A = \{x_w^A, y_w^A, \theta_w^A, t_w^A \mid w = 1, \ldots, |Q'_A|\}$;
   (2) For $w = 1, \ldots, |Q'_A|$:
      (i) $u_w^A = [x_w^A \,||\, y_w^A]$;
      (ii) $Q''_A \leftarrow Q''_A \bigcup \{a_{Aw} = (u_w^A, \theta_w^A, t_w^A)\}$;
   (3) Send her identity information and a request to Bob to release the shared key.

3. After receiving the request and identity information from Alice, Bob checks Alice's identity. If it is false, Bob does not reply. If it is Alice's fourth request, Bob does not send her information about his biometrics. Instead, Bob sends Alice a message warning that her identity might be stolen. If it is true, he performs the steps:

(1) Extract his private biometrics $Q'_B = \{x_v^B, y_v^B, \theta_v^B, t_v^B \mid v = 1, \ldots, |Q'_B|\}$ and compute $Q''_B = \{u_v^B, \theta_v^B, t_v^B \mid v = 1, \ldots, |Q'_B|\}$.

(2) Randomly select an element $(u_c^B, \theta_c^B, t_c^B)$ from Q''_B, and compute $\beta_1' = (g^{u_c^B}, g^{\theta_c^B}, t_c^B), c \in_R \{1, \ldots, |Q'_B|\}$.

(3) Send β_1' to Alice.

4. After receiving β_1' from Bob, Alice performs the steps:

(1) For each fixed $w \in \{1, \ldots, |Q'_A|\}$, compute $(\beta_j')^{a_{Aw}} = (g^{u_a^B}, g^{\theta_a^B}, t_a^B)^{(u_w^A, \theta_w^A, t_w^A)}$ and set it to α_w'.

(2) If there exists some $y \in \mathbb{F}_q^*$ such that $(\alpha_w', y) \in R_{AB}$, do

(i) $(x_{i,j}, y_{i,j}) \leftarrow (\alpha'_w, y)$;

(ii) $Q \leftarrow Q \bigcup \{(x_{i,j}, y_{i,j})\}$;

(iii) If Q has less than n points, $k'_1 \leftarrow 'null'$;

(iv) If Q has no less than n points, she uses Lagrange interpolation polynomial to get a key k'' and does CRC to check it. If the possible key has the same CRC code with k, $k'_1 \leftarrow k''$; Else, $k'_1 \leftarrow 'null'$.

(v) $k' \leftarrow k'_1$.

5. Bob does similar steps as Alice to recover the possible shared key k'.

6. Output k'.

Figures **Fig. 5** and **Fig. 6** describe the locking and unlocking algorithm, respectively, using fingerprints as the example of biometric data.

If Alice can provide biometrics Q'_A that is close to or sufficiently overlaps Q_A, or in other words, if Q'_A contains no less than n real points from her biometric features, she will recover their shared key successfully with Bob's assistance. Otherwise, she will fail to recover a correct shared key. From Guruswami and Sudan's polynomial reconstruction algorithm [9], if the query set Q_R contains at least $\min\{\sqrt{ns_1'}, \sqrt{ns_2'}\}$ real points, then there exists a polynomial time algorithm to reconstruct the correct polynomial $P(x)$, and it follows that the real shared key k can be successfully recovered.

Different from the FV-DH scheme proposed by Lin and Jie in which the users could unlock the vault, respectively, our scheme needs users' cooperation to unlock the vault. So, without the help of the other, neither can unlock the vault in our scheme. Compared to the KSFV scheme proposed by Lin and Mengsheng, our scheme binds the key $H(k)$ instead of k used in their KSFV scheme within the vault which makes the key k much safer. In addition, Bob randomly chooses an element from Q''_B and sends it to Alice in our scheme instead of

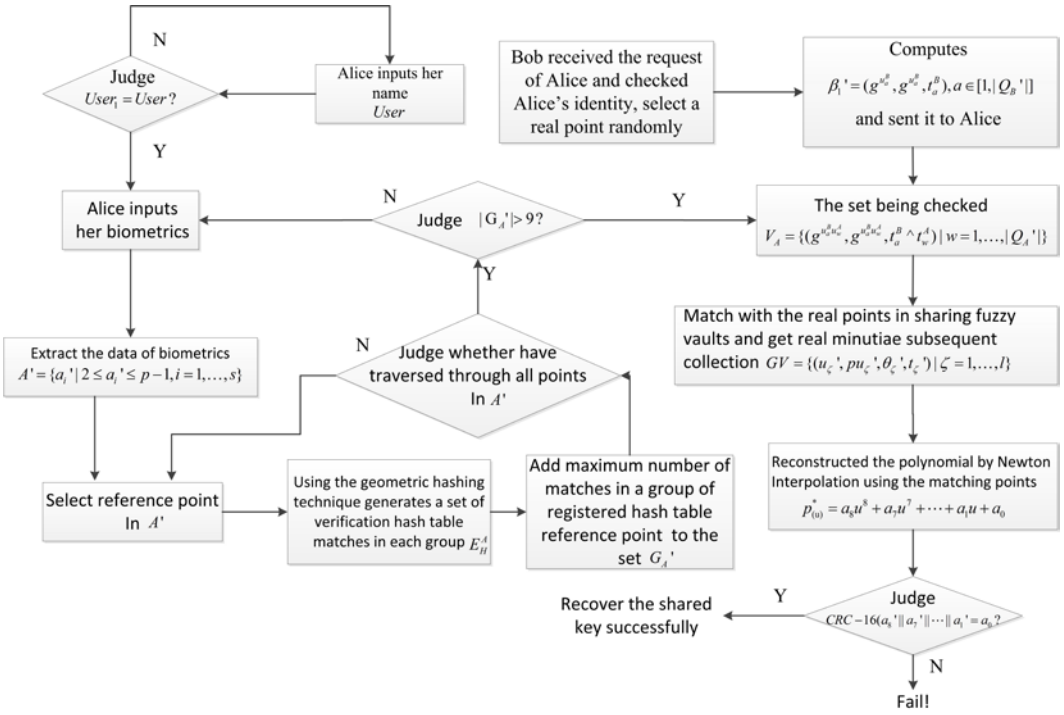


Fig. 6. Proposed unlocking algorithm (for Alice)

sending all the biometric information to Alice in KSFV scheme. If an attack produces one correct point, he will be able to obtain the true shared key in KSFV scheme. That is, the attacker could obtain n correct points by using the received n correct points and his own single correct point which is enough to unlock the vault. However, in our proposed scheme the attacker still could not unlock the vault even if he has one or two correct points. The comparison of our proposed scheme to FV-DH and KSFV scheme is shown in **Table 1**.

Table 1. Difference of the three schemes

Scheme	Locking Algorithm		Unlocking Algorithm		
	Key binding in the vault	The number of real points	The need of Bob's assitance	The number of elements received from Bob	The number of real points
Our proposed scheme	$H(k)$	$m+n$	No	0	n
FV-DH scheme	k	$m \cdot n$	Yes	n	$m \cdot n$
KSFV scheme	k	$m \cdot n$	Yes	1	n

4. Simulation and Security Analysis

In order to verify the correctness and feasibility of our proposed scheme, we use the C ++ program in Visual Studio 2010 platform to simulate the proposed scheme. The environment

used for our simulation is a HP pro 6300MT desktop computer with Intel i5-3470 3.2GHz, DDR3 1600MHz 4GB and Windows7 64-bit. The fingerprint database is created by us which is a pre-calibrated fingerprint database. The details of simulation are given as follows.

To increase the security of our proposed scheme, we incorporate a further check of the user's identity based on a hash table. If the user is an attacker, error would occur in this check and it would produce an error. The simulation picture for the proposed scheme is shown in **Fig. 7**.

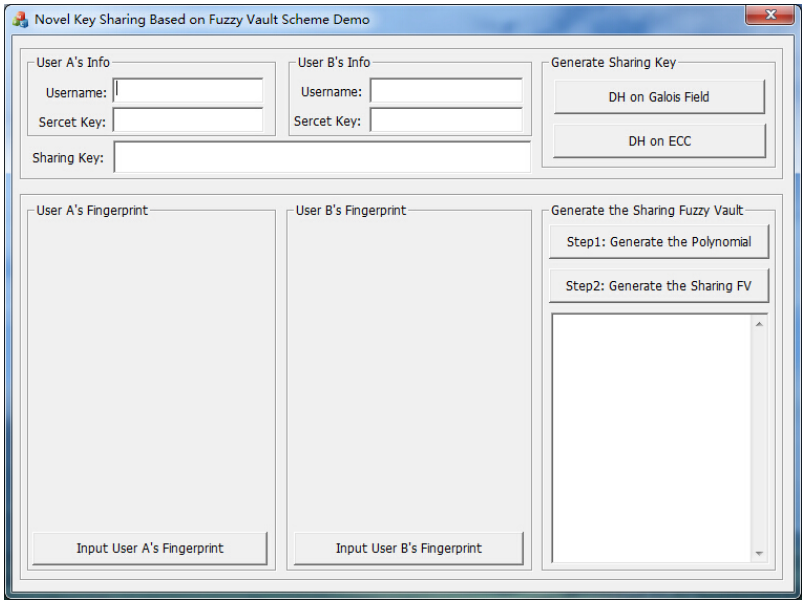


Fig. 7. Homepage of our proposed scheme

The simulation details are as follows: The system exchanges the information of the two users to produce a shared key based on Diffie-Hellman protocol. The shared key is divided into 9 parts as coefficients of the polynomial of degree 9, see **Fig. 8**.

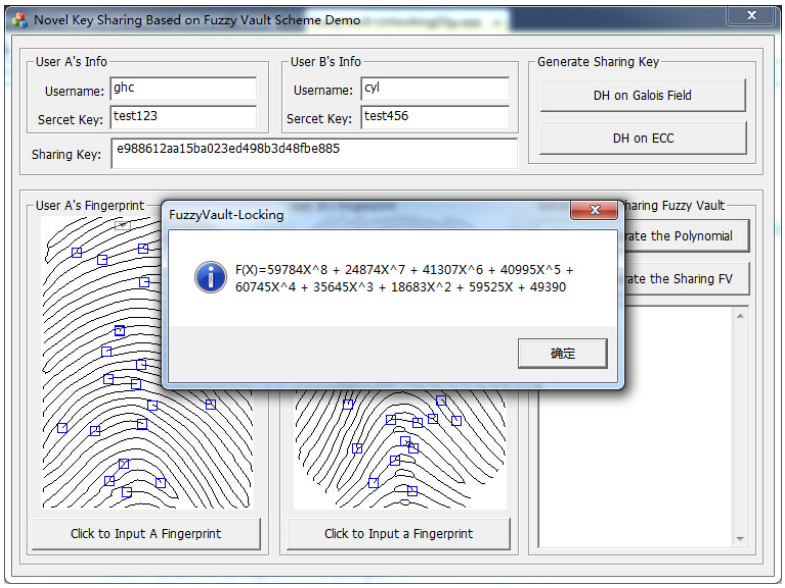


Fig. 8. Binding the shared key into the polynomial

The two users' fingerprints are registered as shown in **Fig. 9**, and we use our proposed scheme to produce a fuzzy vault based on the two users' biometrics (**Fig. 10**). Users' genuine fingerprint information will never be stored.

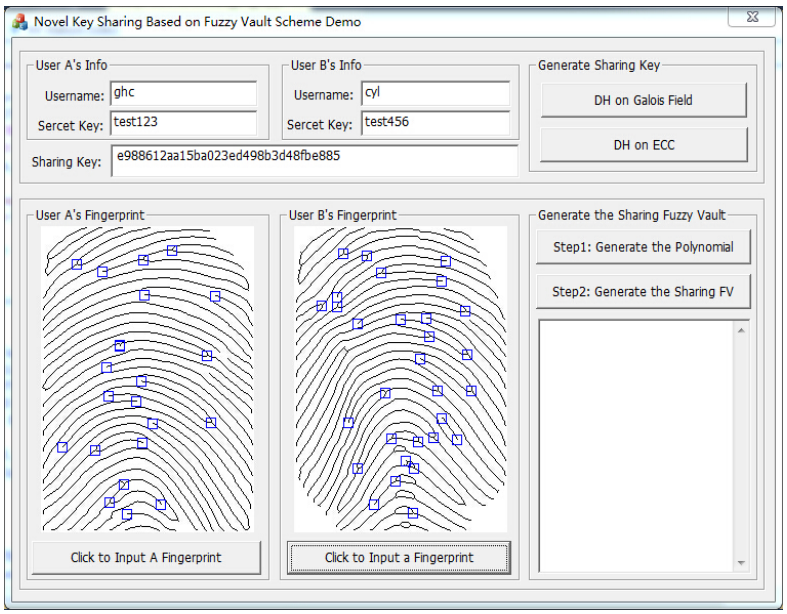


Fig. 9. Unlocking and release of the key

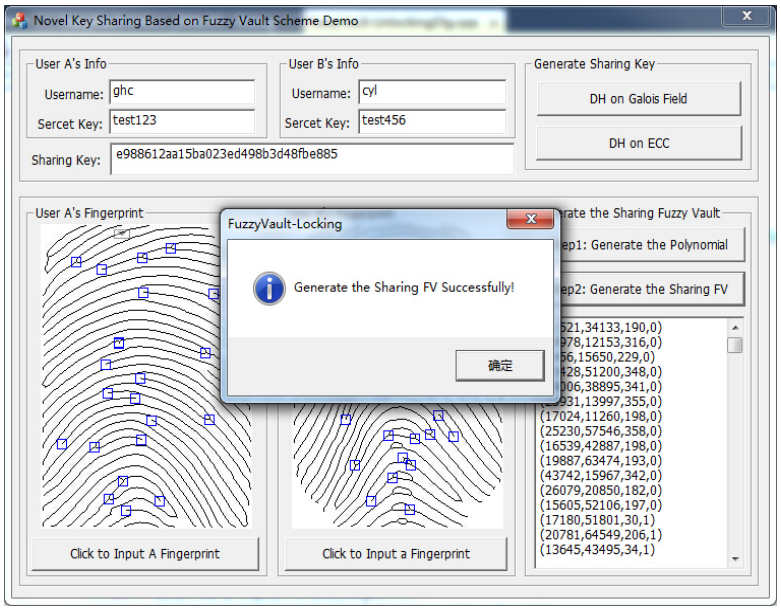


Fig. 10. Successful unlocking and release of the key

If one user wants to unlock the vault, they must ask for others' assistance. If the first user is valid, they unlock the vault and get the key (**Fig. 11**). Successful validation and key recovery steps are shown in **Fig. 12** and **Fig. 13**, respectively.

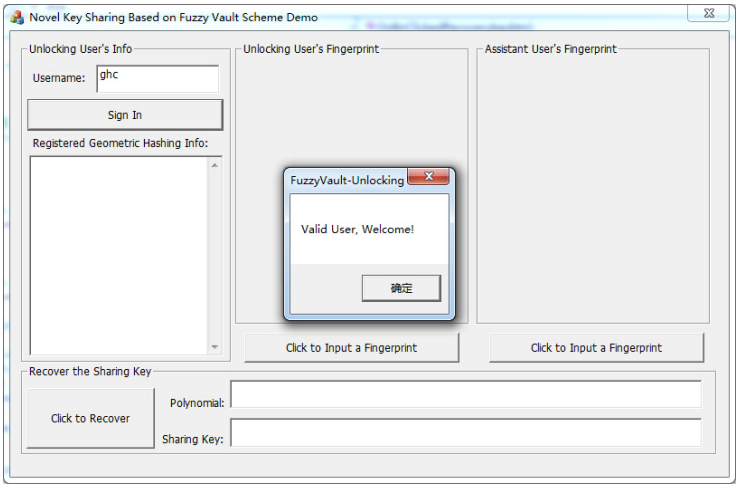


Fig. 11. Successful valid user access

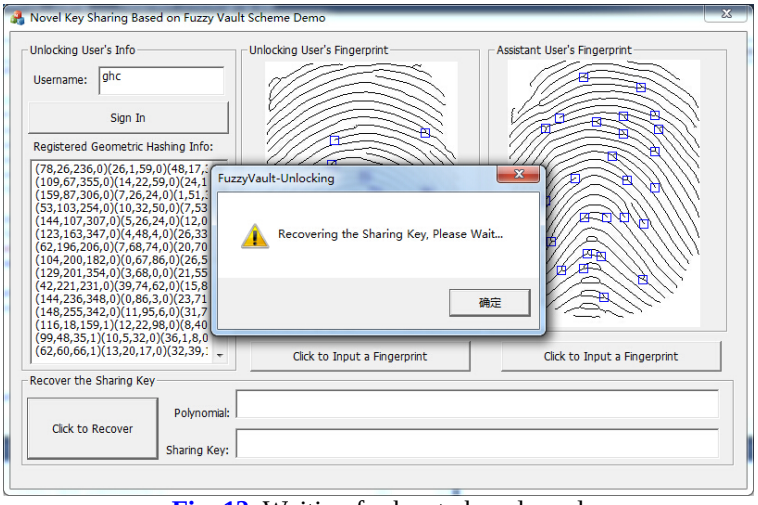


Fig. 12. Waiting for key to be released

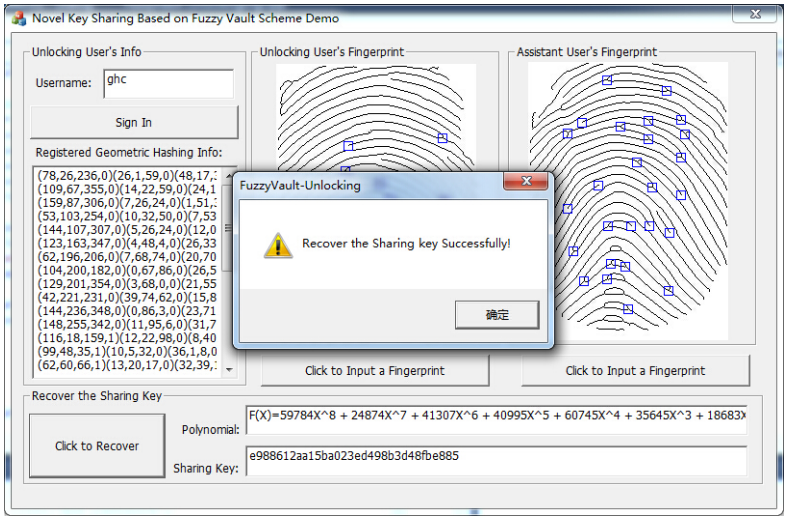


Fig. 13. Successful release of the key

If an attacker attempts to use his own fingerprints to obtain the shared key, it's impossible for him to pass the hash table test, hence he would be unable to unlock the fuzzy vault (see **Fig. 14**).

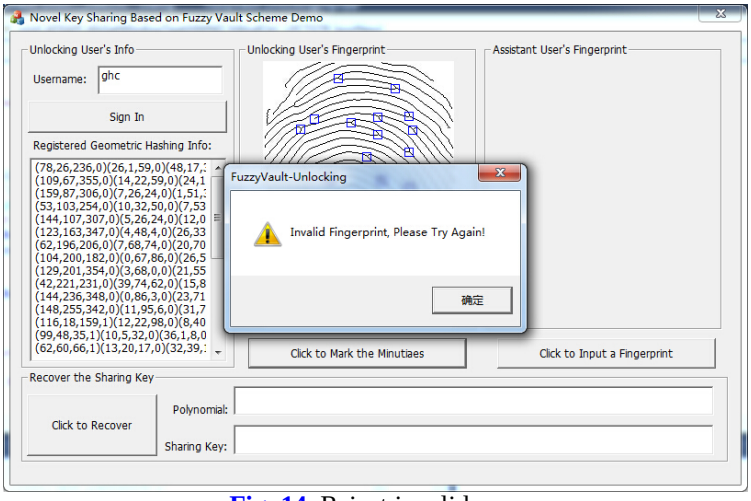


Fig. 14. Reject invalid user

As the FV-DH scheme proposed by Lin and Jie and the KSFV scheme proposed by Lin and Mengsheng are all just detailed models, and the simulation data were not given in their papers. So the comparison of the performance between our proposed scheme and the two schemes cannot be given here. However, the time costs of our locking algorithm and unlocking algorithm are less than 18 milliseconds and 460 milliseconds, respectively.

The pre-calibrated fingerprint database created by us contains 1000 fingerprint samples from 40 fingers, 25 samples per fingerprint. GAR (Genuine Acceptance Rate) and FAR (False Acceptance Rate) are used to evaluate the reliability of our scheme.

We divide the 1000 fingerprint samples into two parts, part A and part B. We design two experiments to evaluate the reliability of our scheme. In the first experiment, the fingerprint samples in Part A are used as user Alice's fingerprints and the fingerprint samples in Part B are used as Bob's fingerprints. In the second experiment, the fingerprint samples in Part B are used as user Alice's fingerprints and the fingerprint samples in Part A are used as Bob's fingerprints.

The simulation result of the first experiment shows that the GAR is 88% and the FAR is 0. The simulation result of the second experiment shows that the GAR is 85% and the FAR is 0. The GAR and FAR of the scheme proposed by Yanikoglu et al. in [10] is 100% and 98%, respectively. Compared with the scheme proposed by Vo et al. in [7], the simulation results of our scheme are better.

The security of our proposed scheme is based on the security of the classical fuzzy vault and the discrete logarithm problem. Since Bob will also check Alice's identity when he receives a request, the security is also based on the security of the hash table.

The security of our proposed scheme also depends on the number $r_A + r_B - 2s_1 \cdot s_2$ of chaff points included in the target set R_{AB} of a total of $r_A + r_B - s_1 \cdot s_2$ points. Since many chaff points are added to R_{AB}, there are many spurious polynomials which are similar to $P(x)$, but incorrect. Thus, the larger is the number of such chaff points, the more difficult will be the task to identify the correct polynomial.

Table 2. Average attack number of times

n \ $r_A + r_B$	160	180	200	220	240
8	7.7×10^{33}	5.9×10^{34}	3.3×10^{35}	1.4×10^{36}	4.9×10^{36}
16	1.2×10^{63}	8.9×10^{64}	2.6×10^{66}	4.4×10^{67}	4.9×10^{68}

Table 3. Average attack time cost (years)

n \ $r_A + r_B$	160	180	200	220	240
8	9.7×10^{25}	7.4×10^{26}	4.1×10^{27}	1.7×10^{28}	6.2×10^{28}
16	1.5×10^{57}	1.1×10^{58}	3.2×10^{58}	5.5×10^{59}	6.2×10^{60}

The probability an attacker can obtain the real polynomial is $\binom{n+1}{s_1 \cdot s_2} \Big/ \binom{n+1}{r_A + r_B - s_1 \cdot s_2}$ if they do not have any favorable information. This approximates to $\left(\frac{s_1 \cdot s_2}{r_A + r_B}\right)^n$ for large r_A and r_B.

If an attacker wants to unlock the fuzzy vault, the average attack numbers of times he should try are shown in **Table 2.** Here, the minutiae numbers of every user are chosen as 9 and the number of $s_1 \cdot s_2$ is 81. For convenience, we assume that an attempt of unlocking the vault costs 400 milliseconds. That means our computer can try 7.9×10^7 times to unlock the vault per year. The average attack time cost is shown in **Table 3.**

The shared key and shared transferred biometrics are produced based on Diffie-Hellman key exchange scheme on a cyclic group H of a large prime p. Thus, an attacker would obtain the key only if he could solve the discrete logarithm problem on H, and its complexity is about $O(\sqrt{p})$.

We transfer the users' biometrics into the corresponding fuzzy vault, containing all the chaff, etc., and it only store the transferred version. Hence, the original biometrics remain safe even if the transferred version were stolen.

In addition, when Bob receives the request, he randomly selects one element β'_1, and sends it to Alice. Hence, Alice could get at most 3 elements as β'_i from Bob, and could produce $3|Q'_A|$ correct points. She could unlock the vault since $3|Q'_A| \geq 3n \geq n$. If the attacker has one minutiae in common with Alice, the probability of which is 1/4900, he could produce only 3 correct points which would be insufficient for him to unlock the vault. Suppose that Bob sends all the elements $\{\beta'_w \mid w = 1, \ldots, |Q'_B|\}$ to Alice, rather than randomly selects one. Then if an attacker impersonated Alice's identity, he could receive $|Q'_B|$ correct points, and we know that if the attacker could provide one correct point, he would be able to obtain the true shared key, because he could obtain $|Q'_B|$ correct points by using the received $|Q'_B|$ correct points and his own single correct point. It is also possible, of course, some real points are in common between two different fingerprints.

Our proposed scheme ensures that the attacker cannot open the fuzzy vault if they do not have the right fingerprint, which in practice means less than n correct points. Our proposed scheme has strong security as the authentication based on hash table will be required when a request is received.

5. Conclusion

We proposed a novel key sharing fuzzy vault scheme based on the classic fuzzy vault and the Diffie-Hellman key exchange scheme. The shared biometric information is used to enhance the security, as well as a hash table check of any users' validity. The proposed scheme is very secure and reliable since the security is based on the classic fuzzy vault scheme, one-way hash function and the discrete logarithm problem in a given finite group.

Many information techniques have been applied in our daily life, the need for security of encryption and authentication mechanisms is vastly increasing. Biometrics are often used in encryption and authentication because it's difficult to copy. Our proposed scheme is designed for situations where two persons need to keep a secure key, and is based on their biometrics, such as fingerprints. Our proposed scheme would provide enhanced security in the following several scenarios.

Company financial records: such as safes, important assets and so on. For example, vaults which store the company's digital property require two persons to guard. The cashier and the finance manager could both make a fuzzy vault to keep the safe combination, or similar access information. Thus, neither can separately access to its details.

Personal information: Important information which means a lot to the users, such as bidding file(s), college examination papers, and so forth. College examinations are very important to the students, and should be kept securely. Our proposed scheme would ensure no illegal access to the papers.

In addition, our scheme can also be developed and applied for key distributions in wireless sensor networks [11].

References

[1] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. Of IEEE International Symposium on Information Theory (ISIT)*, pp. 408, June 30-July 5, 2002. Article (CrossRef Link)

[2] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes, and Cryptography*, vol. 38, no. 2, pp. 237-257, February, 2006. Article (CrossRef Link)

[3] U. K. Sorger, "A new reed-solomon code decoding algorithm based on newton's interpolation," *IEEE Transactions on Information Theory*, vol. 39, no. 2, pp. 358-365, March, 1993. Article (CrossRef Link)

[4] L. You and J. Lu, "A novel fuzzy vault scheme for secret key exchange," in *Proc. Of International Symposium Conference on Security & Cryptography (SECRYPT)*, pp. 426-429, July 24-27, 2012. Article (CrossRef Link)

[5] L. You, M. S. Fan, J. Lu, S. G. Wang and F. H. Li, "A key sharing fuzzy vault scheme," *Lecture Notes in Computer Science*, vol. 7618, pp. 453-460, October 29-31, 2012. Article (CrossRef Link)

[6] T. H. Nguyen, Y. Wang, T. N. Nguyen and R. Li, "A fingerprint fuzzy vault scheme using a fast chaff point generation algorithm," in *Proc. of IEEE Signal Processing, Communication and Computing*, pp. 1-6, Aug. 5-8, 2013. Article (CrossRef Link)

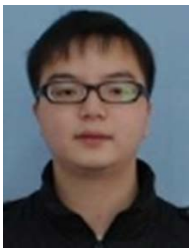
[7] T. T. L. Vo, T. K. Dang and J. Küng, "A hash-based index method for securing biometric fuzzy vaults. Trust, Privacy, and Security in Digital Business," *Lecture Notes in Computer Science*, vol. 8647, pp. 60-71, Sept. 2-3, 2014. Article (CrossRef Link)

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, November, 1976. Article (CrossRef Link)
[9] V. Guruswami and M. Sudan, "Improved deconding of reed-solomon and algebraic-geometric codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1757-1767, September, 1999. Article (CrossRef Link)
[10] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in *Proc. of ICPR-BCTP Workshop*, pp. 43-46, Aug. 5-8, 2004: 43-46. Article (CrossRef Link)
[11] N. T. T. Huyen, M. Jo, T. D. Nguyen and E. N. Huh, "A beneficial analysis of deployment knowledge for key distribution in wireless sensor networks," *Security and Communication Networks*, vol.5, no.5 pp.485-495, May 2012. Article (CrossRef Link)

Lin You received his B.S. degree (1985) and M.S. degree (1988) in mathematics from Wuhan University. He received his Ph.D. degree from Dalian University of Technology, Dalian, China, in 2003. He worked as postdoctoral research fellow at Beihang University from 2004 to 2007. He was a visiting scholar engaged in computational algebra and cryptography studies at Clemson University from Jan. 2010 to Feb. 2011 and from Jul. 2013 to Mar. 2014. He currently works as a professor at Hangzhou Dianzi University. His research interests include computational algebra, cryptography, biometrics recognition and their applications. Prof. You is a member of IEEE and IET, respectively, and he is also a council member of CACR.

Yuna Wang received her B.S. degree (2013), and M.S. degrees (2016) in School of Communication Engineering from Hangzhou Dianzi University，Hangzhou, China. She now works as an information security engineer in Zhejiang Dahua Technology Co., Ltd., China. Her research interests include information security, cryptography, biometrics recognition and their applications.

Yulei Chen received his B.S. degree (2013), and M.S. degrees (2016) in information security from Hangzhou Dianzi University，Hangzhou, China. He currently works as an information security engineer in China Zheshang Bank Co., Ltd., China. His research interests include information security, cryptography and biometrics recognition and their applications.



Qi Deng received his B.S. degree (2012) in communication engineering from Jiangxi University of Finance and Economics, Nanchang, China, and received his M.S. degrees (2016) in School of Communication Engineering from Hangzhou Dianzi University, Hangzhou, China. He now works as a software engineer in Zhejiang Sunny Intelligent Optical Technology Co Ltd., China. His research interests include image processing, cryptography and biometrics recognition.

Huanhuan Zhang is a M.S. candidate in the School of Communication Engineering (SCE), Hangzhou Dianzi University, Hangzhou, China. She received her B.S. degree (2014) in Communication Engineering from Anhui University of Technology, Ma'anshan, China. Her research interests include information security, cryptography and biometrics recognition.