A Novel Fuzzy Vault Scheme for Secret Key Exchange

Lin You[1] and Jie Lu[2]
[1]Institute of Cryptography and Information Security, Hangzhou Dianzi University, Hangzhou 310018, China
[2]Zhejiang Wellcom Technology Co., Ltd, Hangzhou 310012, China

Keywords: Fuzzy Vault, Secret Key Exchange, Finite Group, Biometrics, Polynomial Interpolation.

Abstract: Based on the classical fuzzy vault and the Diffie-Hellman key exchange scheme, a novel fuzzy vault scheme for the secret key exchange is proposed. In this fuzzy vault scheme, the two users can respectively use their biometric features to unlock the fuzzy vault to get their shared secret key without running the risk of disclosure of their biometric features. The security of our scheme is based on the polynomial reconstruction problem and the discrete logarithm problem in a given finite group.

1 INTRODUCTION

In a cryptosystem, one of the most important procedure is to securely store the secret key. Generally, the secret key is stored in the user's computer, a smart card or other storage medias by using a password for accessing, but it will run the risks that the storage medias be lost or stolen, or the password will suffer from the exhaustive search attack. A better way is to use the user's biometric features as the access control measure, while the user's biometric feature or secret key may also be disclosed if his biometric template and key are separately stored. Therefore, to ensure their safety simultaneously, the user's biometric feature and secret key should be completely blended into one set or a data. A classical solution is the fuzzy vault proposed by A. Juels and M. Sudan in 2002 (Juels and Sudan, 2002). In their fuzzy vault scheme, they used the user's unique set to blend his secret into a vault based on Reed-Solomon codes, and the user can recover his secret by providing a set that overlaps largely with the original set. Even if an attacker can get the vault he cannot obtain the the user's secret or the information about the set.

The secret sharing scheme or Diffie-Hellman key exchange scheme is a key cryptographic protocol, and how to safely store the shared key between the users is also a thorny problem. Based on the ideal of A. Juels and M. Sudan's fuzzy vault, a fuzzy vault scheme for the secret key exchange is proposed in this work. The security of this fuzzy vault scheme is based on both the discrete logarithm problem and that the users'biometric features are not illegally exposed.

In Section 2, the classical fuzzy vault scheme is introduced, and our novel fuzzy vault scheme for the secret key exchange is proposed in Section 3. Finally, some conclusions are presented in Section 4.

2 THE CLASSICAL FUZZY VAULT SCHEME

Essentially, the classical fuzzy vault is a scheme for the secure protection of one's secret (value or key) by the use of his some private message set which generally comes from his unique biometrics. A fuzzy vault is composed of two algorithms, one is called 'Locking Algorithm', and the other is called 'Unlocking Algorithm'. The security of this scheme is based on the polynomial reconstruction problem.

A fuzzy vault scheme includes two public parameters, one is a finite field $\mathbb{F}_q$ with q a power of a prime, and the other is a Reed-Solomon decoding algorithm (denoted as $\mathrm{RS}_{\mathrm{DECODE}}$ for short). The best practical choice for $\mathrm{RS}_{\mathrm{DECODE}}$ is the Reed-Solomon decoding algorithm based on Newton's interpolation (Sorger, 1993). The following two algorithms for the fuzzy vault scheme comes originally from the revised work of A. Juels and M. Sudan (Juels and Sudan, 2006) except for some minor changes.

Locking Algorithm

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

You L. and Lu J..
A Novel Fuzzy Vault Scheme for Secret Key Exchange.
DOI: 10.5220/0004125404260429
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 426-429
ISBN: 978-989-8565-24-2

```
Output: A fuzzy vault $V = \{R, (n,r,q)\}$ with $R$ being
    a set of points $\{(x_i,y_i)\}_{i=1}^{r}$ such that $x_i, y_i \in \mathbb{F}_q$ and
    all $x_i$ being distinct.
1. $X, R, V \leftarrow Ø$;
2. $P \leftarrow k$, that is, $k$ is block-encoded into the coefficients of a polynomials of degree $n$ in $\mathbb{F}_q$;
3. For $i = 1$ to $t$ do
    • $(x_i,y_i) \leftarrow (a_i, P(a_i))$;
    • $X \leftarrow X \bigcup \{x_i\}$;
    • $R \leftarrow R \bigcup \{(x_i,y_i)\}$;
   for $i = t+1$ to $r$ do
    • $x_i \in_U \mathbb{F}_q \backslash X$;
    • $X \leftarrow X \bigcup \{x_i\}$;
    • $y_i \in_U \mathbb{F}_q \backslash \{P(x_i)\}$;
    • $R \leftarrow R \bigcup \{(x_i,y_i)\}$.
4. Output $R$ or $V = \{R, (n,r,q)\}$.
```

In order not to leak information about the order in which the x_i are 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 else in a random order. Note that the chaff points in the locking algorithm should be selected so as to intersect neither the set A nor the polynomial P. This is for technical reasons, namely to simplify our security proofs. Generally, the set R together with the parameter pair (n,q) is called a fuzzy vault.

Unlocking Algorithm

```
Input : A fuzzy vault $V$ comprising a parameter pair
    $(n,r,q)$ such that $n \leq r \ll q$ and a set $R$ of $r$ points
    with their two coordinations in $\mathbb{F}_q$. A query set
    $B = \{b_i\}_{i=1}^{t}$ with $b_i \in \mathbb{F}_q$.
Output : An element $k' \in \mathbb{F}_q^n \bigcup \{\text{'null'}\}$.
1. $Q \leftarrow Ø$;
2. For $i = 1$ to $t$ do
    • If there exists some $y_i \in \mathbb{F}_q$ such that $(b_i,y_i) \in R$, set $Q \leftarrow Q \bigcup \{(b_i,y_i)\}$;
    • $k' \leftarrow$ 'null' if $Q$ has less than $n$ points;
    • $k' \leftarrow \text{RS}_{\text{DECODE}}(n,Q)$;
3. Output $k'$.
```

Suppose that V is created by Alice and Bob tries to unlock V to recover the secret key k, Bob has to use his set B to determine the codeword that encodes the secret key k to get a possible secret key k'. Since the set A specifies the x-coordinates of "correct" points that lie on the polynomial P. Thus, if B is close to A, then B will identify a large majority of these "correct" points. Any divergence between B and A will introduce a certain amount of error. Provided that there is a sufficient overlap, however, this noise may be removed by means of a Reed-Solomon decoding algorithm.

The most convenient and unique features to the user is his biometric feature set, such as the fingerprint features, iris features, retinal features and etc. In 2005, U. Uludag and *et al.*(Uludag et al., 2005) proposed a fingerprint-based fuzzy vault. One can also use our other biometric features to construct fuzzy vault schemes.

3 A NOVEL FUZZY VAULT SCHEME FOR A SECRET KEY EXCHANGE

The most popular and classical secret key exchange scheme is the Diffie-Hellman key exchange scheme (Diffie and Hellman, 1976) which is a specific method for the exchanging secret keys between two parties, and it is one of the earliest practical examples of secret key exchange scheme implemented within the field of cryptography. The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This established shared secret key can then be used in a symmetric key algorithm.

In practical applications, the multiplicative group G is generally chosen to be multiplicative group $\mathbb{F}_p^*$ of the Galois field $\mathbb{F}_p$ with p a large prime, and g is selected to be a primitive element of $\mathbb{F}_p^*$. To increase its security strength, we can set up the shared secret key scheme on a (hyper)elliptic curve rational point group since the discrete logarithm problem is much harder than the discrete logarithm problem in the multiplicative group of a Galois field.

In this section, we will put out a novel fuzzy vault scheme for secret key exchange based on the classical fuzzy vault and a multiplicative group, here we denote this scheme as FV-DH scheme.

We suppose that Alice and Bob want to establish a shared secret key for their future cryptographic uses by using their biometric features (such as fingerprint features, iris features, or other part features of their bodies), then they agree on a finite multiplicative group $G = \mathbb{F}_q^*$ with q a power of a large prime and a cyclic subgroup $< g >$ of G with g an element of some large prime p order. Here, G, q, g and p are assumed to be public parameters.

Locking Algorithm

```
Input: A finite multiplicative group $G = \mathbb{F}_q^*$ ; positive integers $n$, $s$, $t$, $r_A$ and $r_B$ such that $n \le min\{s,t\} \le s+t \le r_A, r_B \ll q$ ; a cyclic subgroup $< g >$ of order $p$. These parameters are made public.
Output: $V_A = \{R_A, (p,g,n)\}$ and $V_B = \{R_B, (p,g,n)\}$ for Alice and Bob, respectively. Where $R_A$ and $R_B$ are two sets that are respectively composed of much more than $n$ points with their coordinations in $\mathbb{F}_p^*$.
1. $X, R, R_A, R_B \leftarrow \emptyset$;
2. Alice and Bob extract their private biometric features $A = \{a_i\}_{i=1}^s$ and $B = \{b_j\}_{j=1}^t$, respectively;
3. Mapping all $a_i$ and $b_j$ into the numbers in $\{1, \ldots, p-1\}$. For convenience, they are still respectively represented as $a_i$ and $b_j$, and they are supposed to be different from each others. The corresponding sets are denoted as $S_A$ and $S_B$, respectively;
4. Alice randomly selects a select key $a$: $1 \le a \le p-1$, computes $g^a$ and sends it to Bob;
5. Bob randomly selects a select key $b$: $1 \le b \le p-1$, computes $g^b$ and sends it to Alice;
6. Alice and Bob compute $(g^b)^a$ and $(g^a)^b$, respectively;
7. $k \leftarrow g^{ab}$ (Since $(g^b)^a = g^{ba} = g^{ab} = (g^a)^b$, $k$ can be regarded as the shared key of Alice and Bob);
8. Alice and Bob, respectively, set $P(x) \leftarrow k$. That is, $k$ is block-encoded into the coefficients of a polynomial of degree $n$ in $\mathbb{F}_p[x]$;
9. Alice does the following steps:
   (a) For $i = 1, \ldots, s$, computes $g^{a_i}$ and set it to $\alpha_i$;
   (b) For $i = 1$ to $s$ do
       • $(x_i, y_i) \leftarrow (\alpha_i, P(\alpha_i))$;
       • $X \leftarrow X \bigcup \{x_i\}$;
       • $R \leftarrow R \bigcup \{(x_i, y_i)\}$;
   (c) For $i = s+1$ to $r_A$ do
       • $x_i \in_U G \backslash X$;
       • $X \leftarrow X \bigcup \{x_i\}$;
       • $y_i \in_U G \backslash \{P(x_i)\}$;
       • $R_A \leftarrow R \bigcup \{(x_i, y_i)\}$.
10. Bob does the similar steps to generate $R_B$ with $t$ real points and $r_B - t$ chaff pints.
11. Output $V_A = \{R_A, (p,g,n)\}$ and $V_B = \{R_B, (p,g,n)\}$ respectively for Alice and Bob.
```

The V_A and V_B are the fuzzy vaults of the shared key k owned by Alice and Bob, respectively. If one of them wants to restore the shared key, he/she can independently use his/her own fuzzy vault to restore the possible shared sky k' by the following "Unlocking Algorithm".

Unlocking Algorithm

```
Input: A group $G = \mathbb{F}_q^*$ and a cyclic subgroup $< g >$ of order $p$; Alice and Bob's biometric sets $A' = \{a'_i\}_{i=1}^{s'}$ and $B' = \{b'_j\}_{j=1}^{t'}$ with $a'_i, b'_j \in G$, respectively; Two sets $V_A = \{R_A, (p,g,n)\}$ and $V_B = \{R_B, (p,g,n)\}$ satisfying that $n \le s', t' < s' + t' \ll q$, and the all points of the sets $R_A$ and $R_B$ are in $\mathbb{F}_p^* \times \mathbb{F}_p^*$.
Output: An element $k' \in \mathbb{F}_p \bigcup \{\text{'}null\text{'}\}$.
1. $Q_A, Q_B \leftarrow \emptyset$;
2. If Alice wants to recover the shared key $k$, she does the following:
   (a) For $i = 1$ to $s'$ do
       i. Convert her biometric set $A'$ into a subset of $\{1, \ldots, p-1\}$ which is still denoted as $A'$ for convenience;
       ii. $\alpha'_i \leftarrow g^{a'_i}$;
       iii. If there exists some $y \in \mathbb{F}_q$ such that $(\alpha'_i, y) \in R_A$, do
            • $(x_i, y_i) \leftarrow (\alpha'_i, y)$;
            • $Q_A \leftarrow Q_A \bigcup \{(x_i, y_i)\}$.
       iv. $k' \leftarrow$ '$null'$ if $Q_A$ has less than $n$ points;
       v. $k' \leftarrow \mathrm{RS}_{\mathrm{DECODE}}(n, Q_A)$ (that is, apply Newton's interpolation polynomial to get a possible key $k'$ if $Q_A$ has no less than $n$ points. );
       vi. $k' \leftarrow null$ if $Q_A$ has less than $n$ points.
   (b) $k' \leftarrow \mathrm{RS}_{\mathrm{DECODE}}(n, Q_A)$ or '$null$'.
3. Similarly, Bob can do the same steps as Alice does to recover the possible shared key $k'$.
4. Output $k'$.
```

The locking algorithm and unlocking algorithm can be described as the following Figure 1 and Figure 2, respectively. Here the used biometrics are supposed to be the users' fingerprints.

If Alice and Bob can provide their biometric sets A' and B' that sufficiently overlap A and B, respectively. That is, if their biometric sets A' and B' contain no less than n "correct" biometric features, then they will recover their real shared key k successfully, otherwise, they will fail.

Since the two users' biometric features are not directly stored in our novel fuzzy vault, any third party (attacker) who plan to get the users's features has to solve the discrete logarithm problems on the multiplicative group G. Therefore, if any third party (attacker) cannot solve the discrete logarithm problems,

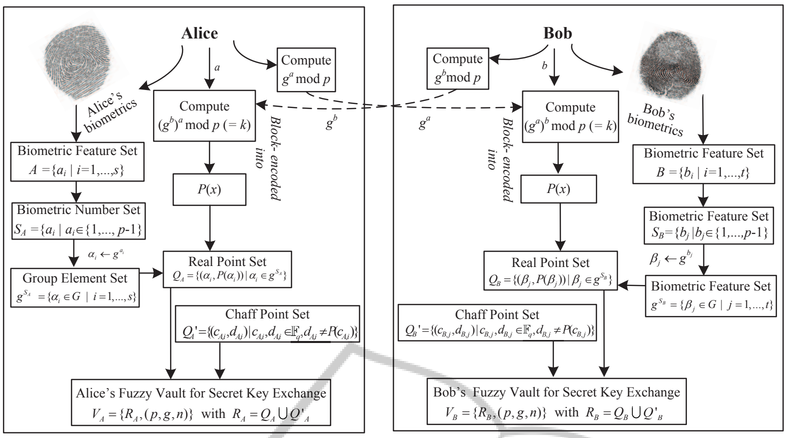
Alice
Bob
Alice's biometrics
Bob's biometrics
Compute $g^a \bmod p$
Compute $g^b \bmod p$
a
b
Compute $(g^b)^a \bmod p\ (=k)$
Compute $(g^a)^b \bmod p\ (=k)$
g^b
g^a
Block-encoded into
$P(x)$
Biometric Feature Set $A=\{a_i \mid i=1,\dots,s\}$
Biometric Number Set $S_A=\{a_i \mid a_i\in\{1,\dots,p-1\}$
$\alpha_i \leftarrow g^{a_i}$
Group Element Set $g^{S_A}=\{\alpha_i\in G \mid i=1,\dots,s\}$
Real Point Set $Q_A=\{(\alpha_i,P(\alpha_i)) \mid \alpha_i\in g^{S_A}\}$
Chaff Point Set $Q_A'=\{(c_{Ai},d_{Ai}) \mid c_{Ai},d_{Ai}\in\mathbb{F}_p,d_{Ai}\neq P(c_{Ai})\}$
Alice's Fuzzy Vault for Secret Key Exchange $V_A=\{R_A,(p,g,n)\}$ with $R_A=Q_A\cup Q'_A$
Biometric Feature Set $B=\{b_i \mid i=1,\dots,t\}$
Biometric Feature Set $S_B=\{b_j \mid b_j\in\{1,\dots,p-1\}$
$\beta_j \leftarrow g^{b_j}$
Biometric Feature Set $g^{S_B}=\{\beta_j\in G \mid j=1,\dots,t\}$
Real Point Set $Q_B=\{(\beta_j,P(\beta_j)) \mid \beta_j\in g^{S_B}\}$
Chaff Point Set $Q_B'=\{(c_{B,j},d_{B,j}) \mid c_{B,j},d_{B,j}\in\mathbb{F}_p,d_{B,j}\neq P(c_{B,j})\}$
Bob's Fuzzy Vault for Secret Key Exchange $V_B=\{R_B,(p,g,n)\}$ with $R_B=Q_B\cup Q'_B$

Figure 1: FV-DH's locking algorithm.

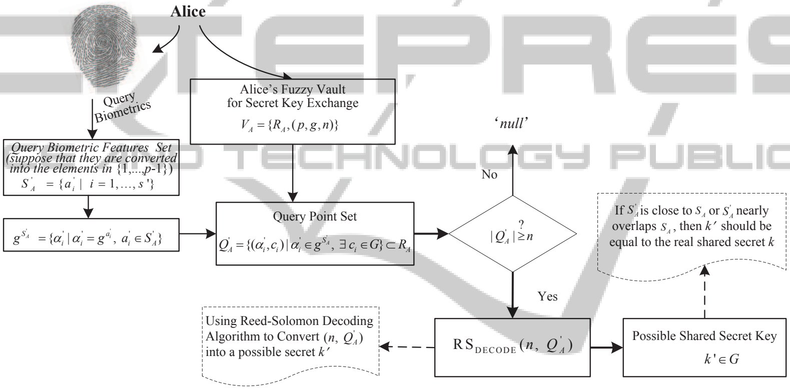
Alice
Query Biometrics
Alice's Fuzzy Vault for Secret Key Exchange $V_A=\{R_A,(p,g,n)\}$
Query Biometric Features Set (Suppose that they are converted into the elements in {1,...,p-1}) $S'_A=\{a'_i \mid i=1,\dots,s'\}$
$g^{S'_A}=\{\alpha'_i \mid \alpha'_i=g^{a'_i},\ a'_i\in S'_A\}$
Query Point Set $Q'_A=\{(\alpha'_i,c_i) \mid \alpha'_i\in g^{S'_A},\ \exists c_i\in G\}\subset R_A$
$|Q'_A|\overset{?}{\geq} n$
'null'
No
Yes
If S'_A is close to S_A or S'_A nearly overlaps S_A, then k' should be equal to the real shared secret k
$\mathrm{RS}_{\mathrm{DECODE}}(n,Q'_A)$
Using Reed-Solomon Decoding Algorithm to Convert (n,Q'_A) into a possible secret k'
Possible Shared Secret Key $k'\in G$

Figure 2: FV-DH's unlocking algorithm (for Alice).

he is unable to get enough biometric numbers to recover a possible real shared key.

4 CONCLUSIONS

A novel fuzzy vault secret key exchange scheme based on fuzzy vault scheme for the secret key exchange is proposed in this work. The security of this fuzzy vault scheme is based on both the discrete logarithm problem and the polynomial reconstruction problem. This fuzzy vault scheme is just a detailed model but it will be simulated for fingerprints in our future work. In addition, similar to our method, a fuzzy vault scheme for the multiparty secret key exchange can also be set up.

ACKNOWLEDGEMENTS

This work is partially supported by the Research Projects of Zhejiang Natural Science Foundations (No.R10900138) and The Key Laboratory of Information Assurance Technology (KJ-11-05).

REFERENCES

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

Juels, A. and Sudan, M. (2002). A fuzzy vault scheme. In *ISIT'02, International Symposium on Information Theory*. IEEE Press.

Juels, A. and Sudan, M. (2006). A fuzzy vault scheme. *Designs, Codes, and Cryptography*, 38:237–257.

Sorger, U. K. (1993). A new reed-solomon code decoding algorithm based on newton's interpolation. *IEEE Transactions on Information Theory*, 39:358–365.

Uludag, U., Pankanti, S., and Jain, A. K. (2005). Fuzzy vault for fingerprints. *Lecture Notes in Computer Science*, 3546:310–319.