AN ONLINE BIOMETRICS-BASED SECRET SHARING SCHEME FOR MUL TIPARTY CRYPTOSYSTEM USING SMART CARDS

CHUN-TA LI
Department of Information Management
Tainan University of Technology
529 Jhong Jheng Road, Yongkang, Tainan, Taiwan 710, R.O.C.
th0040@mail.tut.edu.tw

MIN-SHIANG HWANG1
Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
mshwang@nchu.edu.tw

ABSTRACT. In this article, we propose an online \((t, n)\) threshold secret sharing scheme, in which the system will disperse a primary secret sharing key \(K\) for \(n\) users, and at least \(t\) users together can reconstruct the secret \(K\). The security of our scheme is based on biometric verification and threshold password authentication. Therefore, the scheme is not only secure against several common attacks, but is also appropriate to be applied to other applications such as entrance guard systems and treasury management systems.

Keywords: Biometrics, cryptosystem, threshold password authentication, secret sharing, smart cards, network security.

1. Introduction. In general, a system manager is assigned to protect momentous resources (for instance, encrypted secret information etc.) in the cryptosystem with a master key. However, in practice, some drawbacks may occur. The circumstances of these drawbacks are briefly described as follows:

1. A system manager is only allowed to recover the secrets with the master key. So he or she is required to participate in person every time.
2. If accidents happen to the system manager, the master key might be lost. The idea of managing resources by a system manager is quite risky due to single-point-failure. With the result that will hinder a user from accessing the system.
3. If the system manager is capable of betraying the master key, this kind of compromised attack will damage the security of the system.

According to the previously-mentioned drawbacks, the concept of \((t, n)\) threshold scheme [1, 2, 6, 22, 23, 24] is proposed, so that scattering a primary secret to a group of \(n\) participants and at least \(t\) authorized participants can reconstruct the primary secret, where \(1 \leq t \leq n\). Hence, the idea of sharing a key among multiple authentication system managers may reduce the risk of key exposure and can prevent an unfaithful system manager from holding all of the important resources to seek private gain at public expense. Moreover, in order to provide secure communication in an open network, some security services such as user authentication mechanisms and key distribution protocols are necessary in communication network environments [3, 4, 5].

1Responsible for correspondence: Prof. Min-Shiang Hwang.
Traditionally, password-based protocols [9, 20, 25] have been widely used for user authentication because they permit users to freely choose the passwords they want. However, storing password tables in the system may suffer from compromised, stolen-verifier. Also, modification attacks and most passwords are so simple that they can be easily broken by guessing and dictionary attacks [5, 11, 12, 13, 14, 16, 17]. Furthermore, passwords are unable to provide non-repudiation if they are disclosed to others. There is no way to prove who the actual user is. For this reason, the biometrics-based authentication will be applied for security enhancement in this article. Biometrics [8, 26] are based on physiological and behavioral characteristics of persons, such as fingerprints, palm prints, iris, human-written signatures, gait, voice and hand geometry etc. In contrast with password-based solutions, biometric authentication is inherently more reliable because biometric characteristics cannot be lost or forgotten. In addition, they are possible to provide non-repudiation because they are difficult to copy, share, guess, forge or distribute. This advantage could increase the feasibility of current multiparty cryptosystems such as entrance guard systems and treasury management systems. Taking all the above requirements and problems into consideration, we shall present a biometrics-based \((t, n)\) threshold authentication scheme based on the Lagrange interpolating polynomial proposed by Shamir [23]. To the best of our knowledge, this work is the first attempt to provide a secure authentication model with mutual authentication, threshold secret sharing, and biometrics-based verification for multiparty cryptosystem.

The remainder of this article is organized as follows. In Section 2, we show the notations used in our proposed scheme and security requirements. In Section 3, our scheme is proposed and its security is analyzed in Section 4. Finally, our conclusion is shown in Section 5.

2. Notations and Security Requirements. In this section, the notations used in our proposed scheme are defined in Table 1 and we shall present several common attacks including man-in-middle attacks, replay attacks, masquerade attacks, stolen-verifier attacks, and attacks from the legal user’s smart card is lost.

- **Man-in-middle attack:** This attack occurs because the communication parties have no way to verify each other.
- **Replay attack:** In this attack, an intruder would try to intercept communication messages between the communicating parties and impersonate another legal party to replay the fake messages for further deceptions, such as guessing attacks.
- **Collusion attack:** In this attack, some dishonest participants may collaborate to reconstruct the system’s primary secret sharing key.
- **Stolen-verifier attack:** In general, a remote system uses a password table to verify the legitimacy of a user. However, storing the password table in the system always puts it at the risk of modification, compromised, and stolen-verifier attacks and this way lays a heavy burden on system when the number of legal users grows large.
- **Attacks from the legal users lost smart card:** If the legal user loses his or her smart card, the intruder may derive the secret information stored on the smart card or masquerade as a legal user to access the system illegally.

3. Our Scheme. An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards is proposed in this section. The security of our scheme is based on a public key cryptosystem, discrete logarithms, biometrics verification and uses a trusted registration center as an authority. There are two phases in our scheme including registration phase and reconstruction phase. The detailed steps of the registration phase and reconstruction phase are described in the following subsections.

3.1. Registration Phase. In this section, we show the registration phase in Figure 1 and the detailed steps are described as follows:

**Step 1:** A group of \(n\) managers in \(\Omega\) input his/her personal biometrics \(B_i\) on the specific device and offer the password \(PW_i\), identify of the user \(ID_i\) to the trusted registration center \(R\) via a secret channel, where \(i = 1\) to \(n\).
### Table 1. Notations used in the proposed scheme

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U_i$</td>
<td>A manager in $\Omega$, where $i = 1, \ldots, n$.</td>
</tr>
<tr>
<td>$S$</td>
<td>The system.</td>
</tr>
<tr>
<td>$R$</td>
<td>A trusted registration center.</td>
</tr>
<tr>
<td>$\Omega$</td>
<td>A collection of $n$ managers.</td>
</tr>
<tr>
<td>$ID_i$</td>
<td>Identity of $U_i$.</td>
</tr>
<tr>
<td>$PW_i$</td>
<td>A password chosen by $U_i$.</td>
</tr>
<tr>
<td>$B_i$</td>
<td>Biometric template of $U_i$.</td>
</tr>
<tr>
<td>$H(\cdot)$</td>
<td>One-way hashing function.</td>
</tr>
<tr>
<td>$P$</td>
<td>A large prime.</td>
</tr>
<tr>
<td>$R_S$</td>
<td>A random number generated by $S$.</td>
</tr>
<tr>
<td>$R_{c_i}$</td>
<td>A random number generated by $U_i$.</td>
</tr>
<tr>
<td>$PK_S$</td>
<td>Public key of $S$.</td>
</tr>
<tr>
<td>$</td>
<td></td>
</tr>
<tr>
<td>$\oplus$</td>
<td>XOR operation.</td>
</tr>
<tr>
<td>$E_{PK}(\cdot)$</td>
<td>Asymmetric encryption with the public key $PK$.</td>
</tr>
<tr>
<td>$E_x[\cdot]$</td>
<td>Symmetric encryption with the key $x$.</td>
</tr>
<tr>
<td>$K$</td>
<td>Primary secret key shared by all managers in $\Omega$.</td>
</tr>
</tbody>
</table>

Step 2: Then, the registration center generates a Lagrange interpolating polynomial $(y_i = K + a_1x_1^i + a_2x_2^i + \cdots + a_{t-1}x_{t-1}^i \mod P)$ with degree $t-1$ ($1 \leq t \leq n$), where the values from $a_1$ to $a_{t-1}$ and the primary secret sharing key $K$ are randomly chosen by $R$. After generating the Lagrange interpolating polynomial, $R$ computes secret shadows $y_1, y_2, \cdots, y_n$ with distinct $x_i$, where $x_i = H(ID_i||f_i) \mod P$ and $f_i = H(B_i)$. 

Step 3: Next, $R$ computes $e_i$ and $g_i$ as follows:

$$
\begin{align*}
    e_i &= H(ID_i||x) \oplus H(PW_i) \mod P \\
    g_i &= H(ID_i||x) \oplus x_i \oplus y_i \mod P.
\end{align*}
$$

where $x$ is a secret value protected by $S$.

Step 4: Finally, $R$ sends the corresponding smart cards to every manager, $U_i$ ($i = 1$ to $n$), over a secret channel, with $ID_i$, $P$, $H(\cdot)$, $f_i$, $e_i$ and $g_i$ stored on the card.

#### 3.2. Reconstruction Phase. Whenever the users want to login to the cryptosystem, at least $t$ participants are sufficient to reconstruct the primary secret sharing key, $K$. If there are only $t-1$ or fewer participants, they cannot use Lagrange interpolating polynomial to reconstruct the secret by $S$. If the $t$ legal users would like to reconstruct the secret to access the resources of the system, they must perform the following steps shown in Figure 2 and the detailed steps are briefly described as follows:

Step 1: At least $t$ users are sufficient to reconstruct the secret. Every participant $U_i$ ($i = 1$ to $t$) inserts his/her smart card to the card reader and offers his/her own biometrics on the specific device to capture $U_i$’s biological characteristics.

Step 2: After capturing $U_i$’s biometrics, $B_i$, $U_i$ must pass the biometric verification with the biometric template stored on the smart card ($H(B_i) = f_i$). If it does not hold, $U_i$ may be an intruder and the illegal access will be rejected.

Step 3: If Step 2 holds, $U_i$ inputs his/her password and the smart card will perform the following operations:

$$
\begin{align*}
    x_i^* &= ID_i^t \mod P \\
    M_{i1} &= e_i \oplus H(PW_i) \mod P = H(ID_i||x) \mod P
\end{align*}
$$
Step 4: Each $U_i$ generates a random number $Rc_i$ and keeps it secret. Then, $U_i$ computes his/her message $M_{i2} = E_{PK_S}(ID_i||M_{i3}||g_i||Rc_i)$ and transmits it to the system.

Step 5: After receiving $U_i$’s message, $S$ decrypts $E_{PK_S}(ID_i||M_{i3}||g_i||Rc_i)$ with its private key corresponding to the public key $PK_S$ and checks whether the format of $U_i$’s $ID_i$ is correct or not. If it does not hold, $S$ rejects the login request.

Step 6: If Step 5 holds, $S$ will compute the following message:

$$M_{i3} = H(ID_i||x) \mod P.$$  

Step 7: Then, $S$ verifies $(M_{i3})^{y_i}_w = M_{i4}$. If it is not successful, $S$ rejects the login request.

Step 8: If Step 7 holds, $S$ computes $M_{i4} = g_i \oplus H(x||ID_i) \mod P$ and $M_{i5} = E_{Rc_i}(ID_i||R||g_i||Rc_i)$ and sends $M_{i5}$ to $U_i$, where $R$ is a random number. Note that the random number $R$s in the encrypted messages $M_{i5}$ $(i = 1$ to $t)$ for every participating manager are all the same value.

Step 9: After receiving $S$’s message, $U_i$ decrypts $E_{Rc_i}(ID_i||R||g_i||Rc_i)$ with $Rc_i$ and computes $M_{i6} = M_{i4} \oplus x_i = y_i \mod P$. Then, $U_i$ checks the validity of $M_{i4}^{y_i}_w = x_i^w \oplus M_{i6}$. If it does not hold, the communicating parties may suffer from the malicious attack and the reconstruction phase is terminated.

Step 10: If it holds, $U_i$ encrypts $(ID_i, x_i^w, M_{i6})$ with $S$’s random number $R_S$ and transmits the encrypted message $M_{i7} = E_{R_S}(ID_i||x_i^w||M_{i6})$ to $S$.

Step 11: $S$ decrypts the message $E_{R_S}(ID_i||x_i^w||M_{i6})$ with $R_S$ to get $U_i$’s secret shadow $M_{i6} = y_i$ with distinct $x_i^w$.

Step 12: After receiving all the set of $t$ tuples $(x_i^w, y_i)$ from the $t$ managers, the shared secret $K$ can be reconstructed by $S$.

4. **Discussions.** In the section, we discuss the essential properties and security of the proposed scheme and show a performance analysis of our scheme in terms of the computational and communicative costs.

4.1. **Property Discussion.** According to the aforementioned biometric-based secret sharing scheme in Section 3, in the following, we describe how our proposed scheme achieves the security-related properties.
1. Every participant, $U_i$ (i=1 to t), inserts his/her smart card and inputs $B_i$ into a specific biometric capture device.

2. Verifies $H(B_i) = f_i$.

3. If Step2 holds, $U_i$ inputs $PW_i$ and computes the following messages:
   \[ x_i' = ID_i || x \mod P \]
   \[ M_{i1} = e_i \oplus H(PW_i) \mod P \]

4. Every $U_i$ sends his/her
   \[ M_{i2} = E_{PK_S}(ID_i || M_{i1} || g_i || Rc_i) \] to $S$.

5. $S$ decrypts $M_{i2}$ and checks the format of $U_i$'s $ID_i$.

6. If Step5 holds, $S$ computes
   \[ M_{i3} = H(ID_i || x) \mod P \]

7. Then, $S$ verifies $M_{i3} = M_{i1}$.

8. If Step7 holds, $S$ sends
   \[ M_{i5} = E_{Rs_i}(ID_i || Rs || M_{i4}) \] to $U_i$.

9. $U_i$ decrypts $M_{i5}$ and verifies $M_{i4} = x_i' \oplus M_{i6}$.

10. If Step9 holds, $U_i$ sends
    \[ M_{i7} = E_{Rs_i}(ID_i || x_i' || M_{i6}) \] to $S$.

11. $S$ decrypts $M_{i7}$ to get the secret shadow $M_{i6} = y_i$ with distinct $x_i'$.

12. After receiving the set of $t$ tuples, $(x_i', y_i)$ the secret, $K$ can be reconstructed by $S$.
Table 2. Property comparisons between our scheme and other related schemes

<table>
<thead>
<tr>
<th>Property/Scheme</th>
<th>Ours</th>
<th>Lin et al. [18]</th>
<th>Chai et al. [2]</th>
<th>Raimonodo et al. [22]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without password table</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Threshold secret sharing</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

and compare it with other related schemes [2, 18, 22]. The results of a comparison of property between our scheme, Lin et al.’s scheme [18], Chai et al.’s scheme [2], and Raimonodo et al.’s scheme [22] are shown in Table 2.

- **Mutual authentication:**
  Our scheme copes with this requirement by introducing a verification mechanism, as described in Section 3. During the reconstruction phase, the manager $U_i$ is authenticated based on its preloaded password and $M_{i1}$ in the sense that the system verifies that $U_i$ is indeed legal and authorized. In addition, the system is authenticated to $U_i$ by showing the knowledge of $H(x||ID_i)$.

- **Non-repudiation:**
  Based on the biometric verification, an attack has no way to masquerade a legal user to login in the system. By comparing attacker’s biometrics minutiae with the minutiae template stored in the smart card, the masquerade attacks will be detected. So that it may enhance the security for our proposed scheme.

- **Protection of secret sharing key:**
  For internal attacks, even if a malicious manager can break into up to $t-1$ managers, he/she still cannot derive any information about the primary secret key $K$. On the other hand, for external attacks, an attacker has no way to derive a user’s secret information or passwords from collecting messages in the reconstruction phase because he/she cannot decrypt $M_{i2}$ from Step 4 in the reconstruction phase. Moreover, in Step 8 and 10 of reconstruction phase, the proposed scheme generates two one-time random numbers $Rc_i$ and $Rs$ to secure the transmission messages $M_{i5}$ and $M_{i7}$, respectively.

4.2. **Security Analysis.** According to the aforementioned security requirements in Section 2, we shall show how our proposed scheme resists the following attacks:

- **Man-in-middle Attack:**
  In our scheme, the communicating parties use the messages $M_{i1}$ and $M_{i4}$ to provide user authentication. Therefore, the communicating parties can verify each other and our scheme is immune to man-in-middle attacks.

- **Replay Attack:**
  Considering our scheme, an attack can replay fake messages in $M_{i2}$, $M_{i5}$ and $M_{i6}$ respectively. However, in $M_{i2}$ and $M_{i5}$, we used the random numbers $Rc_i$ and $Rs$ to resist this problem. Furthermore, it is also difficult to guess the encrypted messages $M_{i5}$ and $M_{i7}$ without knowing the random numbers $Rc_i$ and $Rs$ respectively.

- **Collusion Attack:**
  In our secret sharing scheme, at least $t$ participants are needed to reconstruct the secret. However, if $t-1$ dishonest participants would like to reconstruct the secret $K$ in private without notifying the system, it is computationally infeasible due to the security of Shamir secret sharing scheme. Therefore, the collusion attack cannot work against our scheme.

- **The Smart Card is Lost:**
  In our scheme, if the legal users lose their smart cards, the attacker cannot derive the secret information stored on the smart card because he/she cannot pass the biometric verification first.
4.3. Performance Analysis. In this subsection, we evaluate the performance of the proposed scheme in terms of the total number of cryptographic operations performed during the reconstruction phase. To evaluate performance, we define some computational parameters as follows:

- $T_{Exp}$: The time of modular exponentiation.
- $T_{Ha}$: The time of hashing operation.
- $T_{XOR}$: The time of exclusive OR operation.
- $T_{Sym}$: The time of symmetric encryption/decryption operation.
- $T_{Asym}$: The time of asymmetric encryption/decryption operation.

As shown in Table 3, the most time-consuming operations are asymmetric encryption/decryption $T_{Asym}$. We can adopt a lightweight asymmetric encryption/decryption algorithm to perform those operations. For example, Elliptic Curve Cryptography (ECC) [10, 21] is widely being adopted to provide public key cryptography (PKC) support in resource-constrained environments so that the existing PKC-based solutions can be exploited. In addition, it has been shown that ECC computations need less computation time than modular exponentiation computations, and ECC with a 160-bit key size can be instead 1024-bit key size in ElGamal or RSA solutions [7]. In 2008, TinyECC [19], a software package, is being introduced to provide ECC-based PKC operations that can be quickly configured and integrated into limited-resource lightweight devices. Therefore, we can choose TinyECC to provide a ready-to-use and publicly available software package for ECC-based PKC operations in multiparty cryptosystem applications. We believe that the performance of our proposed secret sharing is acceptable for participant nodes and can be practically applied over insecure networks.

5. Conclusions. In this article, a new on-line biometrics-based secret sharing scheme for multiparty cryptosystem is proposed. The concepts of $(t,n)$ threshold secret sharing, biometrics verification and user authentication are integrated. Based on the difficulty of the personal biometrics and public key cryptosystem problems, several kinds of attacks such as man-in-middle attacks, replay attacks, collusion attacks and attacks from the user who lost the smart card were solved to show the security of our proposed scheme.

REFERENCES


