Provably Secure Nested One-Time Secret Mechanisms for Fast Mutual Authentication and Key Exchange in Mobile Communications

Speaker: Pei-Hsiu Ho

Advisor: Prof. Chun-I Fan

The final publication is available at http://ieeexplore.ieee.org
Outline

• Introduction
• Hwang and Chang's Protocol
• Our Idea
• The Proposed Scheme
• Security Definitions
• Security Proofs
• Performance Comparisons
• Conclusions
Introduction (1/2)

• Mobile communication plays an important role in personal communication activities.
• Global System for Mobile Communications (GSM) is a common standard issued by European Telecommunication Standards Institute (ETSI).
• Some schemes for GSM have similar drawbacks
  – High bandwidth consumption between VLR and HLR
  – Storage overhead in VLR
  – Lack of VLR authentication
Introduction (2/2)

- Hwang-Chang scheme is more efficient than other protocols.
- Not only does our scheme achieve mutual authentication, but also it reduces the computation and communication cost of mobile users.
- We formally prove that the proposed scheme is secure based on some hard problems.
Hwang and Chang's Protocol (1/3)

- The notations used in Hwang-Chang scheme

<table>
<thead>
<tr>
<th>Notation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U_i$</td>
<td>The identity of user $i$</td>
</tr>
<tr>
<td>$V$</td>
<td>The identity of some VLR</td>
</tr>
<tr>
<td>$H$</td>
<td>The identity of the HLR</td>
</tr>
<tr>
<td>$K_{uh}$</td>
<td>A common secret key kept by $U_i$ and $H$</td>
</tr>
<tr>
<td>$K_{vh}$</td>
<td>A common secret key kept by $V$ and $H$</td>
</tr>
<tr>
<td>$K_{auth}$</td>
<td>An authentication key kept by $U_i$ and $V$</td>
</tr>
<tr>
<td>$E_{K_x}$</td>
<td>A symmetric encryption function with a secret key $K_x$</td>
</tr>
<tr>
<td>$|$</td>
<td>The concatenation operator</td>
</tr>
</tbody>
</table>
Hwang and Chang's Protocol (2/3)

- The authentication protocol for $U_i$ and the system

<table>
<thead>
<tr>
<th>$U_i$</th>
<th>$V$</th>
<th>System</th>
<th>$H$</th>
</tr>
</thead>
</table>
| \begin{align*}
(1) & \text{Generate } r_0 \\
(2) & \{U_i \}, E_{K_{uh}} (K_{uh} \ || \ r_0) \\
(4) & E_{K_{uh}} (r_0 \ || \ r_1) \\
(5) & \text{Check } r_0, \text{ Set } K_{auth} = r_1 \\
\end{align*} | \begin{align*}
(2) & \text{Generate } r_1 \\
(4) & E_{K_{uh}} (r_0 \ || \ r_1) \\
(6) & \text{Check } K_{auth} \\
\end{align*} | \begin{align*}
(3) & \text{Check } t \\
(3) & E_{K_{uh}} (r_1) \\
\end{align*} | 

System:
- $H = \{E_{K_{uh}} (K_{uh} \ || \ r_0) , E_{K_{uh}} (U_i \ || \ r_1 \ || \ t) \}$
- $V = \{E_{K_{uh}} (r_1) , E_{K_{uh}} (r_0 \ || \ r_1) \}$

Equations:
- $0^r_1 auth Kr_1 auth = 1 auth$
Hwang and Chang's Protocol (3/3)

- The authentication protocol for $U_i$ and $V$

\[
\begin{align*}
U_i & \quad \text{(1) Generate } r_0' \\
\text{(3) Check } r_0' \\
V & \quad \text{(1) } \{U_i, E_{K_{auth}}(K_{auth} \parallel r_0')\} \\
\text{(2) } C' \\
\text{(3) } E_{K_s}(K_s) \\
\end{align*}
\]

System

\[
\begin{align*}
V & \quad \text{(2) Check } K_{auth} \\
\text{Generate } K_s \\
\text{(4) Check } K_s \\
H & \\
\end{align*}
\]
Our Idea (1/4)

- The comparisons of the three authentication mechanisms

<table>
<thead>
<tr>
<th>Assumptions:</th>
<th>Timestamps</th>
<th>One-Time Secrets</th>
<th>Nonces</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Clock synchronization</td>
<td>1. Clock synchronization</td>
<td>The previous authentication must be successfully finished</td>
<td>None</td>
</tr>
<tr>
<td>2. Stable transmission time</td>
<td>2. Stable transmission time</td>
<td></td>
<td>Better</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performance:</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The most efficient solution</td>
<td>Slightly less efficient</td>
<td>Much less efficient</td>
</tr>
<tr>
<td></td>
<td>Better</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Suitable for:                 | The authentication between     | The authentication between a user and the system for the authentication processes after the initial one | The initial authentication between a user and the system |
|-------------------------------| VLR and HLR                     |                                                     |                 |
Our Idea (2/4)

- The initial authentication between a mobile user and the system (VLR and HLR)
Our Idea (3/4)

- The $j$th authentication between a mobile user and the system (VLR and HLR) after the initial one where $j \geq 1$
Our Idea (4/4)

- The proposed nested one-time secret mechanism

**Mobile User** $i$  
**The System (VLR+HLR)**

The initial authentication with the system (based on nonces)

Based on a one-time secret (the outer one):

- The 1st authentication with the system
- The 2nd authentication with the system
  ...
- The $j$th authentication with the system

*<The user does not leave the service area of the current VLR>*

The initial authentication with the VLR only (based on nonces)

Based on another one-time secret (the inner one):

- The 1st authentication with the VLR only
- The 2nd authentication with the VLR only
  ...
- The last authentication with the VLR only

*<The user leaves the service area of the current VLR>*

The $(j+1)$th authentication with the system
The Proposed Scheme

- The definition of notations in the proposed scheme

<table>
<thead>
<tr>
<th>Notation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U_i$</td>
<td>The identity of user $i$</td>
</tr>
<tr>
<td>$V_c$</td>
<td>The identity of some VLR $c$</td>
</tr>
<tr>
<td>$K_{uh}$</td>
<td>A common secret key kept by $U_i$ and the HLR</td>
</tr>
<tr>
<td>$K_{vh}$</td>
<td>A common secret key kept by $V_c$ and the HLR</td>
</tr>
<tr>
<td>$E_{K_x}$</td>
<td>A symmetric encryption function with a secret key $K_x$</td>
</tr>
<tr>
<td>$F_K$</td>
<td>A one-way function with key $K$</td>
</tr>
<tr>
<td>$Sync$</td>
<td>The signal for the request of synchronization with authentication produced by $U_i$</td>
</tr>
</tbody>
</table>
Overview of Our Scheme

The protocol (1)

The protocol (2)

The protocol (3)

The protocol (4)
The Proposed Protocol (1)

- The initial authentication protocol for mobile user $U_i$ and the system

\[ A = E_{K_{uh}}(r + 1) \]

\[ B = E_{K_{vh}}(A, U_i, t_v) \]

\[ C = E_{K_{vh}}(x, y, w, t_h, D) \]

\[ D = E_{K_{vh}}(r, x, y, w) \]

\[ R_0 = r \]
The Proposed Protocol (2)

- The $j$th authentication protocol for a user and the system

\begin{align*}
(1) & \quad \text{Generate } y, w \\
R_j &= F_{K_{uh}} (R_{j-1}, w) \\
A &= E_{K_{uh}} (y, w, R_j) \\
(2) & \quad B = E_{K_{vh}} (A, U_i, t_v) \\
(3) & \quad \text{Check } t_v \\
R_j & = F_{K_{uh}} (R_{j-1}, w) \\
(4) & \quad \text{Check } t_h \\
(5) & \quad \text{Check } R_j
\end{align*}
The Proposed Protocol (3)

- The initial authentication protocol for a user and the current VLR

\[ U_i \]

1. Generate \( s \)
   \[ A = E_w(s+1) \]

2. \( \{A, U_i\} \)
3. Check \( s \)
   \[ S_0 = s \]

\[ V_c \]

1. \( x, y \)
2. \( D = E_w(x, y, s) \)
3. \( x \)
4. Check \( x \)
   \[ S_0 = s \]

\[ \text{System} \]

\[ \text{HLR} \]
The Proposed Protocol (4)

- The $k$th authentication protocol for a user and the current VLR

\begin{align*}
U_i & \quad \text{(1)} \quad \text{Generate } y \\
& \quad \quad S_k = F_w(S_{k-1}, y) \\
& \quad \quad A = E_w(y, S_k) \\
& \quad \text{(3)} \quad \text{Check } S_k
\end{align*}

\begin{align*}
V_c & \quad \text{(1)} \quad \{A, U_i\} \\
& \quad \text{(2)} \quad S_k? = F_w(S_{k-1}, y)
\end{align*}
The protocol of Chapter 4.1
\((U_i, \text{The system})\)

No

Visit a new VLR?

Yes

\(j = 0\)

\(j = 1\)

The \(j\)th protocol of Chapter 4.2
\((U_i, \text{The system})\)

No

Visit a new VLR?

Yes

\(j = j + 1\)

The protocol of Chapter 4.3
\((U_i, \text{current VLR})\)

No

Visit a new VLR?

Yes

\(k = 1\)

\(j = j + 1\)

The \(k\)th protocol of Chapter 4.4
\((U_i, \text{current VLR})\)

\(k = k + 1\)

No

Visit a new VLR?

Yes

\(j = j + 1\)

If failed

If failed

If failed

If failed

If failed

If failed

If failed

If failed

If failed

If failed

If failed

If failed

If failed

If failed
Security Definition (1/21)

- $\Pi^g_{\eta, \varpi}$: a player $\eta$ attempts to authenticate a player $\varpi$ in session $g$ of the protocol $\Pi$, where $\eta, \varpi \in I$, $g \in N$

- $I$: the set of the identities of the players

- $N$: the set of positive integers
Security Definition (2/21)

- An adversary can capture the following queries:
  - \(\text{Execute}(\Pi^g_{\eta,\varpi}, \Pi^p_{\varpi,\eta})\): This query models all kinds of passive attacks, where a passive adversary can eavesdrop all data transmitted between \(\Pi^g_{\eta,\varpi}\) and \(\Pi^p_{\varpi,\eta}\).
  - \(\text{Send}(\Pi^g_{\eta,\varpi}, m)\): This query models active attacks where an adversary sends a message \(m\) to \(\Pi^g_{\eta,\varpi}\).
Security Definition (3/21)

• \( \text{Reveal}(\Pi^g_{\eta,\varpi}) \)

  – This query models the exposure of the session key that \( \Pi^g_{\eta,\varpi} \) accepted.

  – The acceptance means that \( \Pi^g_{\eta,\varpi} \) and the other oracle run the protocol \( \Pi \) successfully and hold the same session key.
• \textit{Test}(\Pi^g_{\eta,\omega})
  
  – When an adversary makes a \textit{Test} query to \Pi^g_{\eta,\omega}, it will return a real session key or a random string to the adversary according to the value of a random bit.
  
  – This query is only available when the real session key has not been revealed.
Security Definition (5/21)

- **Definition 1**: Matching Conversations

\[ \Pi_{\eta, \omega}^g \]

\[ \lambda \]

\[ \alpha_1 \]

\[ \beta_1 \]

\[ \alpha_2 \]

\[ \text{time } \tau_0 \]

\[ \text{time } \tau_1 \]

\[ \text{time } \tau_2 \]

\[ \Pi_{\omega, \eta}^p \]

\[ \alpha_1 \]

\[ \beta_1 \]

\[ \alpha_2 \]

\[ \text{time } \tau_3 \]

\[ * \]
Security Definition (6/21)

• **Definition 2**: \( No - Matching_E(k) \)

  \( No - Matching_E(k) \) is the event that there exists \( \eta, \varpi, g \) such that \( \Pi^g_{\eta, \varpi} \) accepted but there is no \( \Pi^p_{\varpi, \eta} \) which engaged in a matching conversation under the presence of a polynomial time adversary \( E \).
Security Definition (7/21)

- **Definition 3**: $Distinguish_{sk_E}(k)$
  
  - $Distinguish_{sk_E}(k)$ is the event that an adversary $E$ can distinguish whether she/he is given the real session key or a random number after the protocol is performed and terminates successfully.
Security Definition (8/21)

• **Definition 4**: A secure mutual authentication protocol

  – A protocol $\Pi$ is a secure mutual authentication protocol if the following properties are satisfied:

    • **Matching conversations (implies acceptance)**
    
    • **Acceptance implies matching conversations**: The probability of $\text{No} - Matching_E(k)$ is negligible.
Security Definition (9/21)

• **Definition 5**: A secure mutual authentication and key exchange protocol

  - A protocol $\Pi$ is a secure mutual authentication and key exchange protocol if the following properties are satisfied:

    • $\Pi$ is a secure mutual authentication protocol.
    
    • $\Pi^{g}_{\eta,\omega}$ and $\Pi^{p}_{\omega,\eta}$ hold the same session key after running $\Pi$ successfully.
    
    • Indistinguishability: The probability of $Distinguish_{sk_E}(k) - \frac{1}{2}$ is negligible.
• **Definition 6**: The game for INDistinguishability under the Chosen-Ciphertext Attack (IND-CCA).
  
  – A challenger $\psi$ and a polynomial time adversary $\Gamma$ play the following game with a symmetric cryptosystem $\Pi$. 

  Security Definition (10/21)
Security Definition (11/21)

- $E_{sk}$: an encryption oracle with key $sk$
- $D_{sk}$: a decryption oracle with key $sk$

\[ \psi \]

\[ \Gamma \]

\[ \text{Setup} \]

\[ \text{Challenge} \]

\[ \pi^* = E_{sk}(m^*) \]

\[ m^* = D_{sk}(\pi^*) \]

\[ \theta \in \{0,1\} \]

\[ \pi = E_{sk}(m_\theta) \]

\[ \text{Guess: } \theta' \in \{0,1\} \]
Security Definition (12/21)

• Such an adversary $\Gamma$ is referred to as an IND-CCA adversary.

• We define that the guessing advantage of the IND-CCA adversary $\Gamma$ in the game is

\[
Adv^{IND-CCA}_\Pi (\Gamma) = |Pr[\theta = \theta'] - \frac{1}{2}|.
\]
Security Definition (13/21)

• **Definition 7: IND-CCA Security**
  
  - A symmetric cryptosystem $\Pi$ is said to be with $(t, \varepsilon)$-IND-CCA security if no polynomial time adversary $\Gamma$, within running time at most $t$, has guessing advantage $\text{Adv}^{\text{IND-CCA}}_{\Pi}(\Gamma) \geq \varepsilon$ after performing the game of **Definition 6**.
• **Definition 8**: The game for indistinguishability under a pseudorandom function and a random function.

  – A challenger $\psi$ and a polynomial time adversary $\Gamma$ play the following game with a pseudorandom function $\mathcal{G}$. 
Security Definition (15/21)

- $\mathcal{S}_k$: a pseudorandom function with key $k$
- $\mathcal{R}$: a random function

$\psi$

$\Gamma$

Setup

$\mathcal{S}_k$

$\pi^* = \mathcal{S}_k(\gamma^*)$

If $\theta = 0$

$\pi = \mathcal{S}_k(\gamma)$

Else

$\pi = \mathcal{R}(\gamma)$

Guess: $\theta' \in \{0, 1\}$
Security Definition (16/21)

• Such an adversary $\Gamma$ is referred to as a PRF adversary.

• We define that the guessing advantage of the PRF adversary $\Gamma$ in the game is

$$Adv_{S}^{PRF}(\Gamma) = |Pr[\Gamma^{S_k} = 1] - Pr[\Gamma^{R} = 1]|$$

$$=|Pr[\theta' = \theta] - \frac{1}{2}|.$$
Security Definition (17/21)

- **Definition 9**: PseudoRandom Function Security (PRF Security)
  
  We say that \( \mathcal{F} \) is a \((t, \varepsilon)\)-secure pseudorandom function if no polynomial time adversary \( \Gamma \), within running time \( t \), has the advantage \( \text{Adv}^{\text{PRF}}_{\mathcal{F}}(\Gamma) \geq \varepsilon \) after performing the game of **Definition 8**.
• **Definition 10**: The game for indistinguishability under a pseudorandom permutation and a random permutation.

  - A challenger $\psi$ and a polynomial time adversary $\Gamma$ play the following game with a pseudorandom permutation $\Omega$.
- $\Omega_k, \Omega_k^{-1}$: a pseudorandom permutation and its inverse
- $\mathcal{U}_k, \mathcal{U}_k^{-1}$: a random permutation and its inverse

\[
\begin{align*}
\Psi & \quad \Omega_k \\
\text{Setup} & \quad \pi^* = \Omega_k(\rho^*) \\
\text{params} & \quad \rho^* \\
\rho^* & \quad \Omega_k^{-1} \\
\pi^* & \quad \rho^* \\
\pi^* & \quad \pi^* \\
\rho \neq \rho^* & \quad \pi \neq \pi^* \\
\text{Challenge} & \\
\theta \in \{0, 1\} & \\
\text{If } \theta = 0 & \pi = \Omega_k(\rho) \\
\text{Else} & \pi = \mathcal{U}(\rho) \\
\text{Guess: } \theta' \in \{0, 1\}
\end{align*}
\]
Security Definition (20/21)

• Such an adversary $\Gamma$ is referred to as a PRP adversary.

• We define that the guessing advantage of the PRP adversary $\Gamma$ in the game is

$$Adv^{\mathcal{PRP}}_S(\Gamma) = |Pr[\Gamma^\Omega, \Omega^{-1} = 1] - Pr[\Gamma^\mathcal{U}, \mathcal{U}^{-1} = 1]| = |Pr[\theta' = \theta] - \frac{1}{2}|$$
Security Definition (21/21)

• **Definition 11**: Pseudo Random Permutation Security (PRP Security)

  – We say that $\Omega$ is a $(t, q, \varepsilon)$-secure pseudorandom permutation if no polynomial time adversary $\Gamma$, making at most $q$ queries within running time $t$, has the advantage $Adv^{PRP}_\Omega(\Gamma) \geq \varepsilon$ after performing the game of **Definition 10**.
Security Proof of Protocol (1)

• **Theorem 1**: The protocol (1) is a secure mutual authentication and key exchange protocol under the assumption that the adopted underlying symmetric cryptosystem is with the IND-CCA security and the pseudorandom permutation is secure.
Security Proof of Protocol (1)

• Lemma 1: The proposed protocol (1) is a \((t, q_{se}, q_{ex}, \varepsilon)\)-secure mutual authentication protocol for \(V_c\) and \(H\) under the assumption that the underlying pseudorandom permutation \(\Omega\) is with \((t', \varepsilon')\)-PRP security where \(\varepsilon' \geq \frac{\varepsilon}{8 \cdot q_{se} \cdot \Pi(\cdot, \omega)}\) or \(\varepsilon' \geq \frac{\varepsilon}{8 \cdot q_{se} \cdot \Pi(\cdot, \omega)}\), \(t' \approx t + q_{se} \mathcal{O}(t_{se}) + q_{ex} \mathcal{O}(t_{ex}) + \mathcal{O}(1)\).
Security Proof of Protocol (1)

- $q_{se}$, $q_{ex}$: the number of queries to $Send(\cdot, \cdot)$ and $Execute(\cdot, \cdot)$, respectively
- $q_{se-\Pi^{(\cdot)}_{\eta, \infty}}$, $q_{se-\Pi^{(\cdot)}_{\infty, \eta}}$: the number of queries to $Send(\Pi^{(\cdot)}_{\eta, \infty}, \cdot)$ and $Send(\Pi^{(\cdot)}_{\infty, \eta}, \cdot)$, respectively
- $t_{se}$, $t_{ex}$: the computing time of queries to $Send(\cdot, \cdot)$ and $Execute(\cdot, \cdot)$, respectively
Security Proof of Protocol (1)
If $t_h'$ is legal
output $\theta' = 0$
else
output $\theta' \in \{0, 1\}$ randomly
\begin{itemize}
  \item \( Pr[No\text{-}Matching}_E(k)] = \tau \geq \varepsilon \)
  \item \( Pr[\theta' = \theta] \)
    \begin{equation}
      = Pr[\theta' = \theta = 0]Pr[\theta = 0] + Pr[\theta' = \theta = 1]Pr[\theta = 1]
      = ((\tau + (1 - \tau) \frac{1}{2^k} + (1 - \tau)(1 - \frac{1}{2^k}) \frac{1}{2}) \frac{1}{2}
      + (\tau \frac{1}{2}(1 - \frac{1}{2^k}) + (1 - \tau)(1 - \frac{1}{2^k}) \frac{1}{2}) \frac{1}{2}) \frac{1}{q^{s_e - \Pi^\eta, \omega}} q^{s_e - \Pi^\eta, \omega} - 1
      + ((\frac{1}{2^k} + (1 - \frac{1}{2^k}) \frac{1}{2}) \frac{1}{2} + ((1 - \frac{1}{2^k}) \frac{1}{2}) \frac{1}{2}) \frac{1}{q^{s_e - \Pi^\eta, \omega}}
      = \frac{\tau - \tau \frac{1}{2^k}}{4q^{s_e - \Pi^\eta, \omega}} + \frac{1}{2} \geq \frac{\varepsilon}{8q^{s_e - \Pi^\eta, \omega}} + \frac{1}{2}
    \end{equation}
  \item \( (Pr[\theta' = \theta] - \frac{1}{2}) \geq \frac{\varepsilon}{8q^{s_e - \Pi^\eta, \omega}} \)
\end{itemize}
Security Proof of Protocol (1)

\[ E \xrightarrow{\{B,V_c,\text{Sync}\}} \Pi^\delta_{\omega,\eta} \xrightarrow{B} \]

\[ \begin{align*}
\theta = 0 &: \Omega_{K_{vh}}^{-1}(B) \\
\theta = 1 &: \Omega^{-1}(B) \\
(\delta, U_\delta, t_\delta) &
\end{align*} \]

If \( t_\delta \) is legal,
\[ \text{output } \theta' = 0 \]
else
\[ \text{output } \theta' \in \{0,1\} \text{ randomly} \]
Security Proof of Protocol (1)

• **Lemma 2:** The proposed protocol (1) is a \((t, q_{se}, q_{ex}, \varepsilon)\)-secure mutual authentication protocol for \(U_i\) and the system (\(V_c\) and \(H\)) under the assumption that the underlying symmetric cryptosystem is with \((t', \varepsilon')\)-IND-CCA security where 
\[
\varepsilon' \geq \frac{\varepsilon}{8 \cdot q_{se - \Pi(\cdot)}}, \quad \text{or} \quad \varepsilon' \geq \frac{\varepsilon}{8 \cdot q_{se - \Pi(\cdot)_{\Pi}}, \eta},
\]

\[
t' \approx t + q_{se} \mathcal{O}(t_{se}) + q_{ex} \mathcal{O}(t_{ex}) + \mathcal{O}(1).
\]
Security Proof of Protocol (1)
\( (r_0 + 1) \)
\( (r_1 + 1) \)

\[ \begin{align*}
\theta = 0 : A &= E_{K_{uh}} (r_0 + 1) \\
\theta = 1 : A &= E_{K_{uh}} (r_1 + 1) 
\end{align*} \]

If \( r' = r_0 \)
output \( \theta' = 0 \)
else
output \( \theta' \in \{0, 1\} \) randomly
$(r', x_0, y, w)$
$(r', x_1, y, w)$

$\theta = 0 : D = E_{K_{uh}}(r', x_0, y, w)$
$\theta = 1 : D = E_{K_{uh}}(r', x_1, y, w)$

$D$

$\Pi^\delta_{\omega, \eta}$

$\{A, U_i, Sync\}$

$D$

$x'$

$A$

$D_{K_{uh}}$

$r'$

If $x' = x_0$
output $\theta' = 0$
else
output $\theta' \in \{0, 1\}$ randomly
Security Proof of Protocol (1)

• **Lemma 3**: If there is a polynomial time adversary $E$ who has the advantage

\[
\left( \Pr[Distinguish_{sk_E}(k)] - \frac{1}{2} \right) \geq \varepsilon
\]

that the underlying symmetric cryptosystem is with $(t', \varepsilon')$-IND-CCA security, then we have that $\varepsilon' \geq \frac{\varepsilon}{2q_{ex}}$ and

\[
 t' \approx t + q_{ex}O(t_{ex}) + q_{se}O(t_{se}) + q_{rel}O(t_{rel}) + O(t_{te}) + O(1).
\]
Security Proof of Protocol (1)

- $q_{se}$: the number of queries to $Send(\cdot, \cdot)$
- $q_{ex}$: the number of queries to $Execute(\cdot, \cdot)$
- $q_{rel}$: the number of queries to $Reveal(\cdot)$
Security Proof of Protocol (1)

\[ \Gamma \]

- Execute
- Send
- Reveal
- Challenge

\[ E \]

- \( E_{K_{uh}} \)
- \( D_{K_{uh}} \)
$r, x, y_0, y_1, w \rightarrow \theta = 0 : D = E_{K_{uh}}(r, x, y_0, w) \theta = 1 : D = E_{K_{uh}}(r, x, y_1, w)$

$(r + 1)$

$E_{K_{uh}}$

$A$

$K = y_0$

If $E$ outputs “Yes”

guess $\theta' = 0$

else

guess $\theta' \in \{0, 1\}$

$(A, U_i, \text{Sync})$

$E$

$D$

$x$

Test

$K$

Yes/No

$(A, U_i, \text{Sync})$

$E$

$D$

$x$

Test

$K$

Yes/No
\[ (\Pr[Distinguish_{sk_E}(k)] - \frac{1}{2}) = \tau \geq \varepsilon \]

\[ \Pr[\theta' = \theta] \]
\[ = (((\frac{1}{2} + \tau) + (\frac{1}{2} - \tau) \cdot \frac{1}{2}) \cdot \frac{1}{2} + ((\frac{1}{2} + \tau) \cdot \frac{1}{2}) \cdot \frac{1}{2}) \cdot \frac{1}{q_{ex}} + \left(\frac{1}{2}\right) \cdot \frac{q_{ex} - 1}{q_{ex}} \]
\[ \geq \frac{\varepsilon}{2q_{ex}} + \frac{1}{2} \]

\[ (\Pr[\theta' = \theta] - \frac{1}{2}) \geq \frac{\varepsilon}{2q_{ex}} \]
Security Proof of Protocol (2)

• **Theorem 2**: The protocol (2) is a secure mutual authentication and key exchange protocol under the assumption that the adopted underlying symmetric cryptosystem is with the IND-CCA security, the pseudorandom permutation and the pseudorandom function are secure.
Security Proof of Protocol (2)

- Lemma 4: The proposed protocol (2) is a $(t, q_{se}, q_{ex}, \varepsilon)$-secure mutual authentication protocol for $V_c$ and $H$ under the assumption that the underlying pseudorandom permutation $\Omega$ is with $(t', \varepsilon')$-PRP security where $\varepsilon' \geq \frac{\varepsilon}{8\cdot q_{se-\Pi^{(\cdot)}_{\varnothing, \eta}}}$ or $\varepsilon' \geq \frac{\varepsilon}{8\cdot q_{se-\Pi^{(\cdot)}_{\varnothing, \eta}}}$, $t' \approx t + q_{se} \mathcal{O}(t_{se}) + q_{ex} \mathcal{O}(t_{ex}) + \mathcal{O}(1)$. 
Security Proof of Protocol (2)

\[ E \rightarrow \Gamma \]

- Execute
- Send
- Challenge

\[ \Omega_{K_{vh}} \quad \Omega_{K_{vh}}^{-1} \]
Security Proof of Protocol (2)

\[(A, U_i, t_v) \rightarrow \Omega_{K_{vh}} \rightarrow B \rightarrow (y', w', R'_j, t'_h) \]

\[\theta = 0 : \Omega_{K_{vh}}^{-1}(C') \]
\[\theta = 1 : \Omega_{K_{vh}}^{-1}(C') \]

\[\Pi^\delta_{\eta, \omega} \rightarrow E \rightarrow \{B, V_c\} \rightarrow C \]

If \(t'_h\) is legal
output \(\theta' = 0\)
else
output \(\theta' \in \{0, 1\}\) randomly
Security Proof of Protocol (2)

\[ E \xrightarrow{\{B, V_c\}} \Pi_{\omega, \eta}^{\delta} \xrightarrow{B} \]

\[ \theta = 0 : \Omega_{Kvh}^{-1}(B) \]

\[ \theta = 1 : \Omega^{-1}(B) \]

\[ (A', U'_{i'}, t'_{v'}) \]

If \( t'_{v} \) is legal
- output \( \theta' = 0 \)

else
- output \( \theta' \in \{0, 1\} \) randomly
Security Proof of Protocol (2)

- **Lemma 5**: The proposed protocol (2) is a \((t, q_{se}, q_{ex}, \varepsilon)\)-secure mutual authentication protocol for \(U_i\) and the system \((V_{ce} and H)\) under the assumption that the underlying pseudorandom permutation is with \((t', \varepsilon')\)-PRP security and the underlying pseudorandom function is with \((t'', \varepsilon'')\)-PRF security where \(\varepsilon' \geq \frac{\varepsilon}{8 \cdot q_{se - \Pi_{\eta, \omega}^{(\cdot)}}}\) and
\[
\varepsilon'' \geq \frac{\varepsilon}{8 \cdot q_{se - \Pi_{\omega, \eta}^{(\cdot)}}}\]
Security Proof of Protocol (2)

- $t' \approx t + q_{se} \mathcal{O}(t_{se}) + q_{ex} \mathcal{O}(t_{ex}) + \mathcal{O}(1)$

- $t'' \approx t + q_{se} \mathcal{O}(t_{se}) + q_{ex} \mathcal{O}(t_{ex}) + \mathcal{O}(1)$
Security Proof of Protocol (2)
Security Proof of Protocol (2)

\[ \theta = 0 : A = \Omega_{K_{uh}}(y, w, R_j) \]
\[ \theta = 1 : A = \mathcal{U}(y, w, R_j) \]

If \( R'_j = R_j \)
output \( \theta' = 0 \)
else
output \( \theta' \in \{0, 1\} \) randomly
Security Proof of Protocol (2)

\[ E \rightarrow \Pi_{\varnothing, \eta}^{\delta} \rightarrow A \rightarrow \Omega_{K_{uh}}^{-1} \rightarrow (y, w, R'_j) \rightarrow (R_{j-1}, w) \rightarrow \theta = 0 : R_j = \mathcal{S}_{K_{uh}}(R_{j-1}, w) \]

\[ \theta = 1 : R_j = \mathcal{R}(R_{j-1}, w) \rightarrow R_j \]

If \( R'_j = R_j \)

output \( \theta' = 0 \)

else

output \( \theta' \in \{0, 1\} \) randomly
Security Proof of Protocol (2)

- **Lemma 6**: If there is a polynomial time adversary \( E \) who has the advantage

\[
(\Pr[Distinguish_{sk_E}(k)] - \frac{1}{2}) \geq \varepsilon
\]

with running time \( t \), in the proposed protocol (2) under the assumption that the underlying symmetric cryptosystem is with \((t', \varepsilon')\)-IND-CCA security, then we have that

\[
\varepsilon' \geq \frac{\varepsilon}{2q_{ex}} \quad \text{and} \quad t' \approx t + q_{ex}O(t_{ex}) + q_{se}O(t_{se}) + q_{rel}O(t_{rel}) + O(t_{te}) + O(1).
\]
Security Proof of Protocol (2)

\[\Gamma\]

- Execute
- Send
- Reveal
- Challenge

\[E\]

\[E_{K_{uh}}\]
\[D_{K_{uh}}\]
\[S_{K_{uh}}\]
\((y_0, y_1, w, R_j) \rightarrow \begin{align*}
\theta = 0 : A &= E_{K_{uh}}(y_0, w, R_j) \\
\theta = 1 : A &= E_{K_{uh}}(y_1, w, R_j)
\end{align*}\)

\((R_{j-1}, w) \rightarrow \begin{array}{c}
\frown K_{uh} \\
\downarrow \\
R_j \\
\uparrow \\
K = y_0
\end{array}\)

If \(E\) outputs "Yes"

guess \(\theta' = 0\)

else

guess \(\theta' \in \{0, 1\}\)
Security Proof of Protocol (3)

• **Theorem 3**: The protocol (3) is a secure mutual authentication and key exchange protocol under the assumption that the adopted underlying symmetric cryptosystem is with the **IND-CCA security**.
Security Proof of Protocol (3)

- **Lemma 7**: The proposed protocol (3) is a \((t, q_{se}, q_{ex}, \varepsilon)\) -secure mutual authentication protocol for \(U_i\) and \(V_c\) under the assumption that the underlying symmetric cryptosystem is with \((t', \varepsilon')\) -IND-CCA security where \(\varepsilon' \geq \frac{\varepsilon}{8 \cdot q_{se} \cdot \Pi(\cdot) \cdot \omega} \) or \(\varepsilon' \geq \frac{\varepsilon}{8 \cdot q_{se} \cdot \Pi(\cdot) \cdot \omega} \), \(t' \approx t + q_{se} \mathcal{O}(t_{se}) + q_{ex} \mathcal{O}(t_{ex}) + \mathcal{O}(1)\).
Security Proof of Protocol (3)
Security Proof of Protocol (3)

$D_w \rightarrow (x, y, s') \rightarrow D_w \rightarrow (s_0 + 1), (s_1 + 1) \rightarrow \Pi_{\eta, \varpi} \rightarrow \{A, U_i\} \rightarrow E \leftarrow D$

If $s' = s_0$

output $\theta' = 0$

else

output $\theta' \in \{0, 1\}$ randomly
The Security of Protocol (3)

\[
\begin{align*}
E & \xrightarrow[]{\{A, U_i\}} \Pi_{\omega, \eta}^\delta \\
\rightarrow & \quad D \\
\leftarrow & \quad x' \\
A & \downarrow \\
D_w & \\
\rightarrow & \quad s' \\
\rightarrow & \quad (x_0, x_1, y, s') \\
& \quad \theta = 0 : D = E_w(x_0, y, s') \\
& \quad \theta = 1 : D = E_w(x_1, y, s') \\
\rightarrow & \quad D \\
\text{If } x' = x_0 & \text{ output } \theta' = 0 \\
\text{else} & \text{ output } \theta' \in \{0, 1\} \text{ randomly}
\end{align*}
\]
Security Proof of Protocol (3)

• **Lemma 8**: If there is a polynomial time adversary $E$ who has the advantage 

$$\left( \Pr[Distinguish_{sk_E}(k)] - \frac{1}{2} \right) \geq \varepsilon$$

with running time $t$, in the proposed protocol (3) under the assumption that the underlying symmetric cryptosystem is with $(t', \varepsilon')$ -IND-CCA security, then we have that 

$$\varepsilon' \geq \frac{\varepsilon}{2q_{ex}}$$

and 

$$t' \approx t + q_{ex}\mathcal{O}(t_{ex}) + q_{se}\mathcal{O}(t_{se}) + q_{rel}\mathcal{O}(t_{rel}) + \mathcal{O}(t_{te}) + \mathcal{O}(1).$$
Security Proof of Protocol (3)
\[(x, y_0, y_1, s) \rightarrow \theta = 0 : D = E_w(x, y_0, s) \]
\[\theta = 1 : D = E_w(x, y_1, s)\]

\[
\begin{align*}
(s + 1) & \downarrow \\
E_w & \downarrow \\
A & \downarrow \\
K = y_0 & \\
\end{align*}
\]

If \(E\) outputs "Yes"

- guess \(\theta' = 0\)

else

- guess \(\theta' \in \{0, 1\}\)
Security Proof of Protocol (4)

- **Theorem 4**: The protocol (4) is a secure mutual authentication and key exchange protocol under the assumption that the adopted underlying symmetric cryptosystem is with the IND-CCA security, the pseudorandom permutation and the pseudorandom function are secure.
Security Proof of Protocol (4)

• Lemma 9: The proposed protocol (4) is a \((t, q_{se}, q_{ex}, \varepsilon)\)-secure mutual authentication protocol for \(U_i\) and \(V_c\) under the assumption that the underlying pseudorandom permutation is with \((t', \varepsilon')\)-PRP security and the underlying pseudorandom function is with \((t'', \varepsilon'')\)-PRF security where \(\varepsilon' \geq \frac{\varepsilon}{8 \cdot q_{se - \Pi^{(\cdot)}_{\eta, \varpi}}}\) and \(\varepsilon'' \geq \frac{\varepsilon}{8 \cdot q_{se - \Pi^{(\cdot)}_{\varpi, \eta}}}\).
Security Proof of Protocol (4)

- $t' \approx t + q_{se} \mathcal{O}(t_{se}) + q_{ex} \mathcal{O}(t_{ex}) + \mathcal{O}(1)$

- $t'' \approx t + q_{se} \mathcal{O}(t_{se}) + q_{ex} \mathcal{O}(t_{ex}) + \mathcal{O}(1)$
Security Proof of Protocol (4)

\[ E \quad \Gamma \]

- Execute
- Send
- Challenge

\[ \Omega_w \quad \mathcal{S}_w \]
Security Proof of Protocol (4)

\((S_{k-1}, y)\) \(\xrightarrow{} S_w\) \(\xrightarrow{} S_k\)

\((y, S_k)\) \(\xrightarrow{} \theta = 0 : A = \Omega_w(y, S_k)\) \(\theta = 1 : A = \mathcal{U}(y, S_k)\) \(\xrightarrow{} A\)

\(\Pi_{\eta, \varpi}^\delta\)

\(\{A, U_i\}\)

\(E\)

If \(S'_k = S_k\)

output \(\theta' = 0\)

else

output \(\theta' \in \{0, 1\}\) randomly
Security Proof of Protocol (4)

\[ E \]

\[ \{ A, U_i \} \]

\[ \Pi^\delta_{\omega, \eta} \]

\[ A \]

\[ (y, S'_k) \]

\[ \Omega^{-1}_w \]

\[ (S_{k-1}, y) \]

\[ \theta = 0 : S_k = \mathcal{S}_w(S_{k-1}, y) \]

\[ \theta = 1 : S_k = \mathcal{R}(S_{k-1}, y) \]

\[ S_k \]

If \( S'_k = S_k \)

output \( \theta' = 0 \)

else

output \( \theta' \in \{0, 1\} \) randomly
Security Proof of Protocol (4)

- Lemma 10: If there is a polynomial time adversary $E$ who has the advantage
  $\left( \Pr[Distinguish_{sk_E}(k)] - \frac{1}{2} \right) \geq \varepsilon$ with running time $t$ in the proposed protocol (4) under the assumption that the underlying symmetric cryptosystem is with $(t', \varepsilon')$-IND-CCA security, then we have that $\varepsilon' \geq \frac{\varepsilon}{2q_{ex}}$ and $t' \approx t + q_{ex}O(t_{ex}) + q_{se}O(t_{se}) + q_{rel}O(t_{rel}) + O(t_{te}) + O(1)$. 
Security Proof of Protocol (4)
\((y_0, y_1, S_k)\) →
\(\theta = 0 : A = E_w(y_0, S_k)\)
\(\theta = 1 : A = E_w(y_1, S_k)\)

\((S_k-1, y_0)\) →
\(S_k\)

\(K = y_0\)

If \(E\) outputs “Yes”
guess \(\theta' = 0\)
else
guess \(\theta' \in \{0, 1\}\)
Performance Comparisons (1/3)

• Assumptions
  – One-way hash function: SHA-256
  – The length of each user's identity: 128 bits
  – The length of every random number: 256 bits
  – The length of each timestamp: 60 bits
Performance Comparisons (2/3)

- The comparisons of the second protocol of Hwang-Chang scheme and the proposed protocol (4)

<table>
<thead>
<tr>
<th>For each user</th>
<th>Hwang-Chang scheme</th>
<th>Our scheme</th>
<th>Reduced by %</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communication cost</strong></td>
<td>1408 b</td>
<td>896 b</td>
<td>36%</td>
</tr>
<tr>
<td>(i) Encryption/Decryption</td>
<td>1280 b</td>
<td>512 b</td>
<td></td>
</tr>
<tr>
<td>(ii) Hashing</td>
<td>0</td>
<td>256 b</td>
<td></td>
</tr>
<tr>
<td>(iii) The generation for random strings</td>
<td>256 b</td>
<td>256 b</td>
<td></td>
</tr>
<tr>
<td><strong>Computation cost</strong></td>
<td>1536 b</td>
<td>1024 b</td>
<td>33%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The entire protocol</th>
<th>Hwang-Chang scheme</th>
<th>Our scheme</th>
<th>Reduced by %</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communication cost</strong></td>
<td>1408 b</td>
<td>896 b</td>
<td>36%</td>
</tr>
<tr>
<td>(i) Encryption/Decryption</td>
<td>2560 b</td>
<td>1024 b</td>
<td></td>
</tr>
<tr>
<td>(ii) Hashing</td>
<td>0</td>
<td>512 b</td>
<td></td>
</tr>
<tr>
<td>(iii) The generation for random strings</td>
<td>512 b</td>
<td>256 b</td>
<td></td>
</tr>
<tr>
<td><strong>Computation cost</strong></td>
<td>3072 b</td>
<td>1792 b</td>
<td>42%</td>
</tr>
</tbody>
</table>
Performance Comparisons (3/3)

- The comparisons of the first protocol of Hwang-Chang scheme and the proposed protocol (2)

<table>
<thead>
<tr>
<th>For each user</th>
<th>Hwang-Chang scheme</th>
<th>Our scheme</th>
<th>Reduced by %</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communication cost</strong></td>
<td>1408 b</td>
<td>896 b</td>
<td>36%</td>
</tr>
<tr>
<td>(i) Encryption/Decryption</td>
<td>1280 b</td>
<td>512 b</td>
<td></td>
</tr>
<tr>
<td>(ii) Hashing</td>
<td>0</td>
<td>256 b</td>
<td></td>
</tr>
<tr>
<td>(iii) The generation for random strings</td>
<td>256 b</td>
<td>256 b</td>
<td></td>
</tr>
<tr>
<td><strong>Computation cost</strong></td>
<td>1536 b</td>
<td>1024 b</td>
<td>33%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The entire protocol</th>
<th>Hwang-Chang scheme</th>
<th>Our scheme</th>
<th>Reduced by %</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communication cost</strong></td>
<td>3132 b</td>
<td>2296 b</td>
<td>27%</td>
</tr>
<tr>
<td>(i) Encryption/Decryption</td>
<td>3960 b</td>
<td>3568 b</td>
<td></td>
</tr>
<tr>
<td>(ii) Hashing</td>
<td>0</td>
<td>512 b</td>
<td></td>
</tr>
<tr>
<td>(iii) The generation for random strings</td>
<td>512 b</td>
<td>256 b</td>
<td></td>
</tr>
<tr>
<td><strong>Computation cost</strong></td>
<td>4472 b</td>
<td>4336 b</td>
<td>3%</td>
</tr>
</tbody>
</table>
Conclusions

• We have proposed a fast mutual authentication scheme for mobile communications based on a novel mechanism.

• Our proposed scheme is more efficient than Hwang and Chang's scheme.

• We have demonstrated the security of our scheme by formal proofs.