Password Authenticated Key Exchange Protocols

Xun Yi, Victoria University
Raylin Tso, National Cheng Chi University
Eiji Okamoto, University of Tsukuba

Abstract

- Scenario: client/server model
- Application: password-authenticated key exchange (PAKE)
- Proposals: client/server PAKE protocol from IBE, group PAKE protocol from IBE and IBS
Outline

- Backgrounds
- Client/server PAKE from IBE
- Group PAKE from IBE and IBS
- Security and performance analysis
- Conclusion

What is PAKE?

Password

\[ E \quad E_k(M) \quad D \]

Password
Dictionary Attack

First PAKE


\[
\begin{align*}
A, \ E_{PW}(g^a) \\
E_{PW}(g^b), \ E_K(\text{ChallengeB}) \\
E_K(\text{ChallengeA}, \text{ChallengeB}) \\
E_K(\text{ChallengeA}) \\
PW, \ a \\
PW, \ b
\end{align*}
\]

\[
\begin{align*}
K = g^{ab}
\end{align*}
\]
First Formal Model of Security for PAKE

- Random oracle model versus standard model

\[ \text{Adv}_{A,P}(k) \leq Q(k)/N + \epsilon(k) \]

First Practical PAKE without Random Oracles

- Built on Cramer-Shoup cryptosystem (1998)

\[ \begin{align*}
PK & \quad SK \\
\varepsilon = g_1^{x_1} g_2^{x_2} & \quad x_1, x_2 \\
\delta = g_1^{y_1} g_2^{y_2} & \quad y_1, y_2 \\
n = g_1^z & \quad z \in \mathbb{Z}_q \\
\end{align*} \]

\[ \begin{align*}
E & : k \in \mathbb{Z}_q \\
u_1 = g_1^k & \\
u_2 = g_2^k & \\
e = h^k & \\
S & : u_1, u_2, v, e \\
a = H(u_1, u_2, e) & \\
v = \varepsilon \cdot \varepsilon^{k_0} & \\

R & : D: a = H(u_1, u_2, e) \\
u_1 x_1 u_2 x_2 (u_1 y_1 u_2 y_2)^e = v? \\
m = e / u_1^z & \\
\end{align*} \]
**KOY PAKE**

**Client**

\[
(VK, SK), r_1 \in \mathbb{Z}_q
\]

\[
A = g_1^{r_1}, B = g_2^{r_1}
\]

\[
C = H(g_1^{r_1})
\]

\[
r_1 A = g_1, \quad B = g_2
\]

\[
C = h_1 g_1
\]

\[
pw x_2, y_2, z_2, w_2, r_2 \in \mathbb{Z}_q
\]

\[
a = H(client, VK, A, B, C)
\]

\[
d = (ça)^{-1}
\]

\[
\text{Client, VK, A, B, C, D}
\]

\[
E = g_1^{x_2} g_2^{y_2} h_2^{z_2} (cd)^{w_2}
\]

\[
F = g_1^{r_2}, G = g_2^{r_2}
\]

\[
I = h_2 g_1
\]

\[
pw
\]

\[
sks = Er_1 F x_1 g_1 \quad I' z_1 J w_1
\]

\[
\text{If VerifyVK}(b, K, Sig) = 1
\]

\[
C' = C / g_1
\]

\[
sks = K^{e^2} A^{x_2} B^{y_2} C'^2 D^{w_2}
\]

**Server**

\[
x_2, y_2, z_2, w_2, r_2 \in \mathbb{Z}_q
\]

\[
a' = H(client, VK, A, B, C)
\]

\[
D = (cd)^{-1}
\]

\[
\text{Server, E, F, G, I, J}
\]

\[
b' = H(server, E, F, G, H)
\]

\[
K = g_1^{x_1} g_2^{y_1} h_1^{z_1} (cd)^{w_1}
\]

\[
Sig = \text{Sign}_{SK}(b', K)
\]

\[
I' = I / g_1
\]

\[
sks = E^2 F x_1 G y_1 I' z_1 J w_1
\]

**Motivations**

- Common reference model versus IBE
- Implicit authentication versus explicit authentication
- PAKE security model versus ID-based PAKE security model
Security Model for PAKE from IBE

Client/Server PAKE from IBE
Practical IBE without Random Oracles

- C. Gentry: Practical identity-based encryption without random oracles (Eurocrypt 2006).
- Truncated decisional augmented bilinear Diffie-Hellman exponent (ABDHE) assumption

$q, g, g_1 = g^a, h_1, h_2, h_3, H, a$: MasterKey

\[ E : s \in \mathbb{Z}_q \ u = g^{s_{ID}} \]
\[ v = e(g, g)^s \]
\[ w = m \cdot e(g, h_1)^s \]
\[ b = H(u, v, w) \]
\[ Y = e(g, h_2)^s e(g, h_3)^{s_b} \]

\[ S \]

\[ \text{SecretKey} \]
\[ d_{ID} = \{(r_{ID, i}, h_{ID, i}) : i = 1, 2, 3\} \]
\[ h_{ID, i} = (h_ig^{r_{ID, i}})^{1/(a - ID)} \]

\[ R \]

Security of Client/Server PAKE from IBE without Random Oracles

- IBE is secure against the adaptive chosen ciphertext attack.
- A new decisional Diffie-Hellman (NDDH) assumption: given $g, g^a, g^b, Z \in G$, it is hard to decide if $Z = e(g, g)^{ba}$
- ABDHE: $(g', g_{q+2}, g, g_1, ..., g_q, Z)$, it is hard to decide if $Z = e(g_{q+1}, g')$ where $g_i = g^a$
- NDDH is harder than ABDHE because let $g_{(q+1)}/2 = g^x$, $g' = g^y$, then $e(g_{q+1}, g') = e(g, g)^{yx^2}$
KOY versus Client/Server
PAKE from IBE (Client side)

<table>
<thead>
<tr>
<th></th>
<th>KOY</th>
<th>YTO-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rounds</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Auth.</td>
<td>Implicit</td>
<td>Explicit</td>
</tr>
<tr>
<td>Comm.</td>
<td>12</td>
<td>10</td>
</tr>
<tr>
<td>Comp.</td>
<td>16 + 1 Sign</td>
<td>14 + 2 Pair</td>
</tr>
</tbody>
</table>

Extension to Group PAKE

\[ PW_{C1}, PW_{C2}, \ldots, PW_{Cn} \]

Server

"Honest but curious"

\[ K \]

\[ Client_1, \quad Client_2, \quad \ldots, \quad Client_n \]

\[ PW_{C1}, \quad PW_{C2}, \quad PW_{Cn} \]
Group PAKE from IBE

- Broadcasting communication model
- Clients run a group key exchange protocol $P$ to obtain $K$
- Authentication

\[
\text{IBE}_{\text{Server}}[H(msg|K)*H(msg|PW_{ci})]
\]

\[
\text{Sign}_{\text{Server}}[H(msg|clients,server),SK_s]
\]

- $PW_{ci}$
- $SK_s, PW_{ci}$

Security of Group PAKE from IBE and IBS

- Trust model
  - IBE is secure against the adaptive chosen ciphertext attack.
  - IBS is existential unforgeability under the chosen message attack.
- Group PAKE from IBE and IBS has been proved to be secure without random oracles.
### Abdalla et al’s Group PAKE versus ID-based Group PAKE

<table>
<thead>
<tr>
<th></th>
<th>Abdalla et al.</th>
<th>YTO-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compiler</td>
<td>2-party PAKE,</td>
<td>Group KE,</td>
</tr>
<tr>
<td></td>
<td>Burmester-Desmedt KE</td>
<td>Client/server PAKE</td>
</tr>
<tr>
<td>Trusted model</td>
<td>Each user is</td>
<td>Server is</td>
</tr>
<tr>
<td></td>
<td>honest</td>
<td>honest</td>
</tr>
<tr>
<td>Auth model</td>
<td>n pairs of users</td>
<td>All clients to server</td>
</tr>
<tr>
<td>Rounds</td>
<td>5</td>
<td>4</td>
</tr>
</tbody>
</table>

### Conclusion

- **Client/server model**
- **Client/server PAKE from IBE** is more efficient than existing 2-party PAKE without random oracles.
- **Group PAKE from IBE and IBS** is a new way to construct group PAKE protocols.
References