

# Analysis on Imai-Shin's LR-AKE Protocol for Wireless Network Security

**Wang Yingjie**  
**Beijing Remote Sensing**  
**Institution, Beijing, China**

- **THREE PARTS:**
- **Imai-Shin's AKE(authenticated key exchange) Protocol for Wireless Network Security**
- **Cryptanalysis on the Protocol**
- **Conclusion**

- **Imai-Shin's Protocol:**
- In 2005 Imai and Shin proposed authenticated key exchange protocol for wireless network security. It is based on password authentication for simplicity. Here we show the scheme is vulnerable to client/server impersonation attacks. And to provide strong security, improvement work is needed.

# IMAI-SHIN'S PROTOCOL

Client  $\mathcal{C}$

Server  $\mathcal{S}_i$  ( $i \geq 1$ )

[Initialization]

$$p_i(x) = \boxed{\alpha_{i1}} \cdot x + pw \bmod q \xrightarrow{h^{p_i(1)}}$$

$$\boxed{h^{p_i(1)}}$$

[Protocol Execution]

$$p_i(x) = \boxed{\alpha_{i1}} \cdot x + pw \bmod q$$

$$r_1 \xleftarrow{R} (\mathbb{Z}/q\mathbb{Z})^*$$

$$y_1 = g^{r_1} \cdot h^{-p_i(1)} \bmod p \xrightarrow{(\mathcal{C}, y_1)}$$

$$r_2 \xleftarrow{R} (\mathbb{Z}/q\mathbb{Z})^*$$

$$y_2 = g^{r_2} \cdot \boxed{h^{p_i(1)}} \bmod p$$

$$MK_{\mathcal{S}_i} = (y_1 \cdot h^{p_i(1)})^{r_2} \bmod p$$

$$Ver_2 = \text{MAC}(SID || MK_{\mathcal{S}_i} || 01)$$

$$MK_{\mathcal{C}} = (y_2 \cdot h^{-p_i(1)})^{r_1} \bmod p \xleftarrow{(\mathcal{S}_i, y_2, Ver_2)}$$

If  $Ver_2 \neq \text{MAC}(SID || MK_{\mathcal{C}} || 01)$ ,

Stop the protocol.

Otherwise,  $Ver_1 = \text{MAC}(SID || MK_{\mathcal{C}} || 10)$

and  $SK_{\mathcal{C}} = \text{MAC}(SID || MK_{\mathcal{C}} || 11)$ .  $Ver_1 \xrightarrow{\quad}$

If  $Ver_1 \neq \text{MAC}(SID || MK_{\mathcal{S}_i} || 10)$ ,

stop the protocol.

Otherwise,  $SK_{\mathcal{S}_i} = \text{MAC}(SID || MK_{\mathcal{S}_i} || 11)$ .

- **Imai-Shin's protocol consists of four phases:**
  - ***Initialization***
  - ***Secrecy amplification***
  - ***Verification***
  - ***Session-key generation***

# Initialization

- *Client choose a number  $a_{i1}$ , compute*

$$p_i(x) = a_{i0} + a_{i1} \cdot x \bmod q$$

- *where  $a_{i0} = pw$*
- *Client register securely the value  $h^{p_i(1)}$  to server  $S_i$*

$$S_i \leftarrow h^{p_i(1)}$$

- Client stores

$$p_i'(x) = p_i(x) - pw = a_{i1} \cdot x \bmod q$$

- And keep  $pw$  in mind.

# Secrecy amplification

- When client wants to share session key with server, on client end:

- First recover  $p_i(x)$  with  $pw$  and  $p_i'(x)$

- And compute  $h^{-p_i(1)}$  and  $y_1 \leftarrow g^{r_1} \cdot h^{-p_i(1)}$

- Then send  $y_1$  to server

On server end:

- Server compute

$$y_2 \leftarrow g^{r_2} \cdot h^{p_i(1)}$$

$$MK_{S_i} \leftarrow (y_1 \cdot h^{p_i(1)})^{r_2}$$

$$Ver_2 = MAC(SID \| MK_{S_i} \| 01)$$

- Server send  $y_2$  and  $Ver_2$  to Client
- Client compute

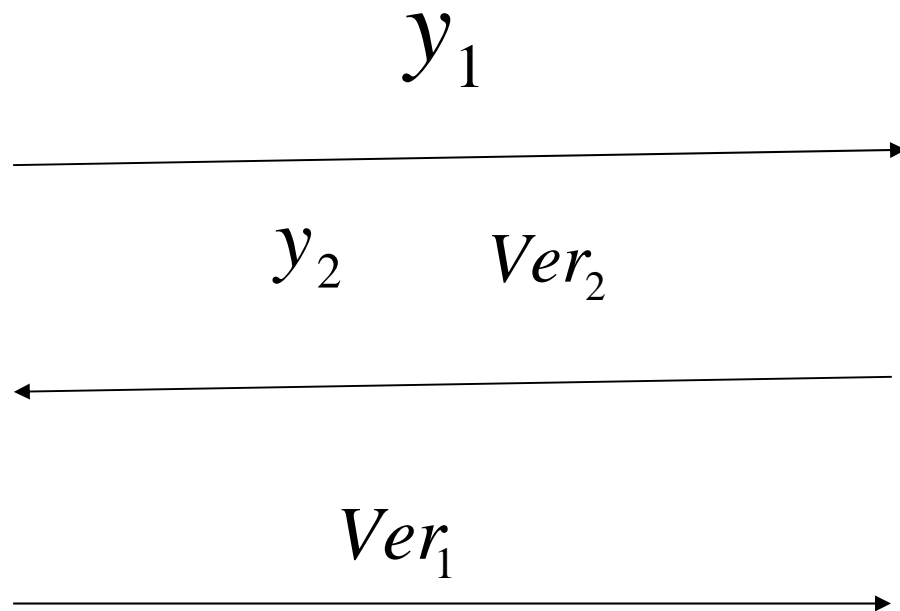
$$MK_C \leftarrow (y_2 \cdot h^{-p_i(1)})^{r_1}$$

$$Ver_1 = MAC(SID \| MK_C \| 10)$$

- And send  $Ver_1$  to Sever

# Message exchanges between client and server

- Client Server



# Verification

- Client verify

$$Ver_2 = ? MAC(SID \| MK_C \| 01)$$

- Server verify

$$Ver_1 = ? MAC(SID \| MK_{S_i} \| 10)$$

# Session-key Generation

- If the above verifications succeed, Client and Server compute the session key material respectively as

$$SK_C \leftarrow \text{MAC}(SID \| MK_C \| 11)$$

$$SK_{S_i} \leftarrow \text{MAC}(SID \| MK_{S_i} \| 11)$$

- Since  $MK_C = (y_2 \cdot h^{-p_i(1)})^{r_1} = g^{r_1 r_2} = (y_1 \cdot h^{p_i(1)})^{r_2} = MK_{S_i}$   
 $SID = C \| S_i \| y_1 \| y_2$ , at end of the protocol run they share a session key.

# CRYPTANALYSIS ON THE SCHEME

- 1) *Client Impersonation Attack*

Imai-Shin's protocol does not require secure server storage, an intruder can easily get access to the secrecy on the server ----- the value  $h^{p_i(1)}$ , then the intruder

- Randomly choose  $r_1' \leftarrow_R (Z / qZ)^*$

- Compute  $y_1' \leftarrow g^{r_1'} \cdot h^{-p_i(1)}$

- Send  $(C, y_1')$  to Server

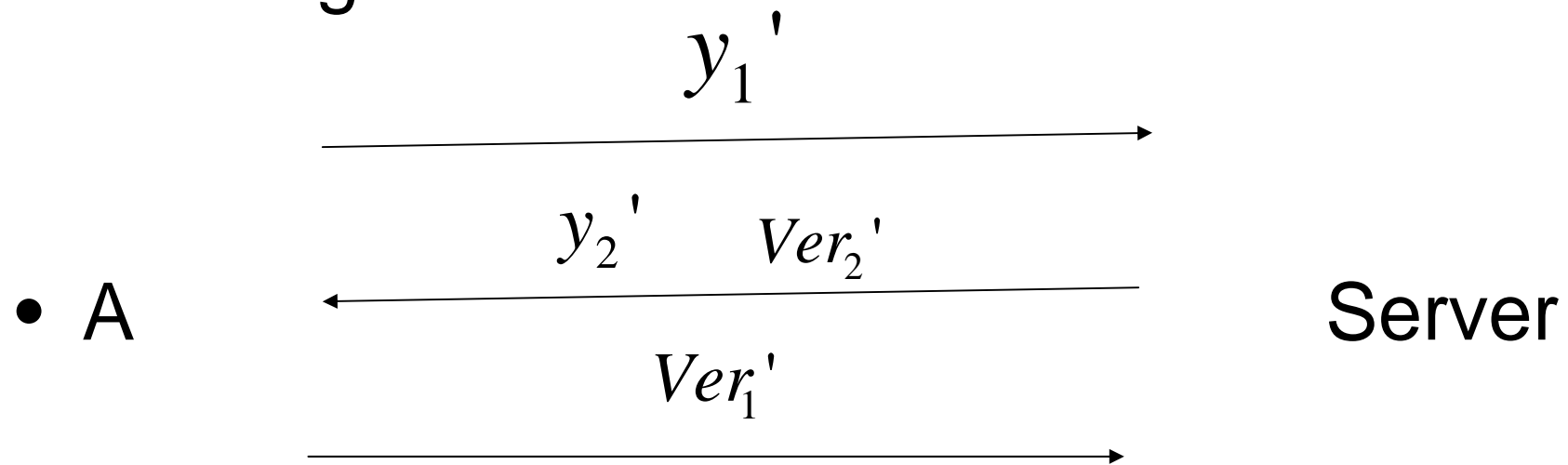
- Server randomly choose

$$r_2' \leftarrow_R (Z / qZ)^*$$

- Compute

$$y_2' \leftarrow g^{r_2'} \cdot h^{p_i(1)}$$

- Intruder(A) and Server exchange messages as below



- Where

$$Ver_1' = MAC(SID' \| MK_C' \| 10)$$

$$Ver_2' = MAC(SID' \| MK_{S_i}' \| 01)$$

$$MK_C' \leftarrow (y_2' \cdot h^{-p_i(1)})^{r_1'} = (g^{r_2'} h^{p_i(1)} h^{-p_i(1)})^{r_1'} = g^{r_1' r_2'}$$

$$MK_{S_i}' \leftarrow (y_1' \cdot h^{p_i(1)})^{r_2'} = (g^{r_1'} h^{-p_i(1)} h^{p_i(1)})^{r_2'} = g^{r_1' r_2'}$$

$$SID' = C \| S_i \| y_1' \| y_2'$$

It can be seen that  $MK_C' = MK_{S_i}'$ , so the adversary and the server can pass mutual authentication, and share a same session key at the end of the protocol.

- 2) *Server Impersonation Attack.*

When the adversary gets the secrecy  $h^{p_i(1)}$  on the server, he can also compute

$$y_2'' \leftarrow g^{r_2''} \cdot h^{p_i(1)}$$

by randomly choose  $r_2'' \leftarrow_R (Z / qZ)^*$

So he can communicate with the client as the server does. Similar to analysis in *client impersonation attack*, it is easy to see that the adversary and the client can authenticate each other successfully thus share a same session key in the end of the protocol.

# CONCLUSION

- Imai-Shin's scheme is not secure enough for most real world applications in wireless environment, it has weakness on client/server impersonation attacks.
- So far, few schemes based on password authentication can achieve strong security. Future research would be focused on how to achieve strong security as well as simplicity of the algorithm/protocol for authenticated key exchange in wireless environments.

# END

- THANK YOU!