# A Forward-Secure User Authentication Scheme with Smart Cards

Bin Wang and Zheng-Quan Li
*(Corresponding author: Bin Wang)*

Department of Electronics and Communication Engineering, Information Engineering College of Yangzhou University
No. 36 Middle JiangYang Road Yangzhou City, Jiangsu Province 225009, P.R. China (E-mail: xiaobinw@yahoo.com )

*(Received Sept. 4, 2005; revised and accepted Oct. 11, 2005)*

## Abstract

In 2004, Yoon et al. proposed a user authentication scheme based on generalized ElGamal signature scheme using smart cards. In their scheme, the previous session keys will be compromised if the secret key of the system is leaked. In this paper, we propose a new scheme which can offer forward secrecy. Our scheme is also secure against forgery attack while keeping the merits of the scheme proposed by Yoon et al.

*Keywords: Authentication, forward secrecy, password, smart card*

## 1 Introduction

With the rapid growth of computer networks, the achievement of secrecy and authentication has become increasingly important. User authentication can prevent unauthorized network access. For this reason, various kinds of authentication schemes have been developed [2, 8]. In 1981, Lamport [5] proposed a password authentication scheme for insecure communication. The scheme requires the remote server to maintain a password table for purpose of verification. In 2000, Hwang and Li [4] proposed a new scheme using smart cards. The advantage of the Hwang-Li's scheme is that it does not need any password table. Later, Yoon et al. [9] proposed a mutual authentication scheme based on generalized ElGamal signature scheme, which is more efficient than Hwang and Li's scheme in terms of computation and communication cost. In addition, the Yoon-Ryu-Yoo's scheme provides the function of key exchange.

However, this paper will point out a security leak of the Yoon-Ryu-Yoo's scheme. In their authentication protocol, an intruder is able to reveal previous session keys by means of the disclosed secret parameters. Then we will present a forward-secure scheme. Finally, we will analyze the security of our improved scheme and conclude this paper.

## 2 Review of the Yoon-Ryu-Yoo's Scheme

The Yoon-Ryu-Yoo's scheme can be divided into three phase: registration, login and authentication. In addition, user can change their passwords freely and securely without the help of a remote system.

**Registration:** The user $U_i$ submits his identifier $ID_i$ and chosen password $PW_i$ to the remote system. Then the remote system performs the following steps:

1) Compute $VPW_i = g^{x_s} \bmod p$, where $x_s$ is a secret key hold by the remote system, $p$ is a large prime number with bit size 1024–2048, $q$ is a prime divisor of $p-1$ with bit size 160, and $g$ is an element of order $q$ in the finite field $GF(p)$ .

2) Compute $R_i = h(ID_i, x_s)$ $X_i = R_i \oplus h(ID_i, PW_i)$, where $\oplus$ denotes an exclusive operation, and $h(\cdot)$ is a secure one-way function. The bit size of the output of $h(\cdot)$ is $|q|$.

3) Write $ID_i, VPW_i, R_i, X_i, h(\cdot), p, q, g$ to the memory of the smart card and issue the card to $U_i$.

**Login:** If the user $U_i$ wants to log in to a remote system, he must insert his smart card into a card reader and keys in his identifier $ID_i$ and password $PW_i$. Then the smart card performs the following steps:

1) Generate a random number $r \in Z_q^*$;

2) Compute $k = (VPW_i)^r \bmod p$;

3) Compute $t = h(k, T)$, where $T$ is the current timestamp;

4) Compute $V_i = X \oplus h(ID_i, PW_i)$;

5) Compute $s = r - V_i t \bmod q$;

6) Sends a message $C_1 = \{ID_i, t, s, T\}$ to the remote system.

**Authentication:** Upon receiving the authentication request message $C_1$, the remote system and the smart card will perform the following steps for mutual authentication between the user and the remote system.

1) The remote system verifies that $ID_i$ is correct. If not, the login request is rejected;
2) Let $T'$ be the time that the system receives $C_1$. The system compares $T$ and $T'$. If the difference between $T$ and $T'$ is within a valid time interval $\triangle T$, $C_1$ is considered as a valid message;
3) The system computes $V_i' = h(ID_i, x_s)$;
4) The system computes $k' = (g^s g^{v_i' t})^{x_s} \bmod p$;
5) The system compares $t$ with $h(k', t)$. If they are equal, then the system accepts the login request and proceeds to the next step, otherwise rejects the login request;
6) The system acquires the current time-stamp $T''$ and computes $C_2 = h(k', V_i', T'')$. The system sends back the message $\{C_2, T''$ to $U_i$;
7) Upon receiving the message $\{C_2, T''$, $U_i$ verifies the validity of the time interval between $T''$ and the current time-stamp $T'''$, then computes $C_2' = h(k, V_i, T'')$ and compares $C_2'$ with $C_2$. If they are equal, the mutual authentication is complete. After the mutual authentication, $k = k' = g^{x_s r} \bmod p$ is used as the session key between the user $U_i$ and the remote system.

# 3 A Security Leak of the Yoon-Ryu-Yoo's Scheme

A protocol offers forward secrecy if compromise of a long-term secret key(s) cannot result in the compromise of past session keys [1]. In this section, we will point out that the Yoon-Ryu-Yoo's scheme is not forward-secure.

Initially, we can assume that an intruder intercepted a legitimate login request message $C_1 = \{ID_i, t_0, s_0, T_0\}$. Then suppose the intruder acquires the long-term secret parameters $x_s, h(\cdot), g, p$ and $q$ for some reason. Thereafter, the intruder can reveal previous session keys by means of the intercepted login request messages. At this point, the intruder can compute $V_i = h(ID_i, x_s)$ and we know that the following equation holds:

$$s_0 = r_0 - V_i t_0 \bmod q. \quad (1)$$

From Equation 1, the intruder will obtain the correct value of $r_0$ since $r_0$ is an element in $Z_q^*$. Hence the intruder can reveal the previous session key $k_0$ by computing

$$k_0 = g^{x_s r_0} \bmod p.$$

Now the intruder is able to decrypt data encrypted with . Consequently, the Yoon-Ryu-Yoo's scheme violates the security requirement of forward secrecy.

# 4 Our Scheme

At this point, we will present a remote user authentication scheme with forward secrecy. Similarly, our scheme can be divided into three phase: registration, login and authentication.

**Registration:** The user $U_i$ submits his identifier $ID_i$ and $PW_i$ to the remote system, where $PW_i$ is the chosen password. Initially, the remote system performs the following steps:

1) Chooses a secure one-way function $h(\cdot), p, q$ and $g$, where $p$ is a large prime number with bit size 1024, $q$ is a prime divisor of $p-1$ with bit size 160, and $g$ is an element of order $q$ in the finite field $GF(p)$. The bit size of the output of $h(\cdot)$ is $|q|$;
2) Computes $R_i = h(ID_i||x_s)$, $X_i = R_i \oplus h(ID_i||PW_i)$, where $||$ denotes a concatenation operation;
3) Writes $ID_i, R_i, X_i, h(\cdot), p, q, g$ to the memory of the smart card and issue the card to $U_i$. Note that $h(\cdot), p, q$ and $g$ are public parameters, while $R_i$ and $X_i$ are kept secret.

**Login:** If the user $U_i$ wants to log in to a remote system, he must insert his smart card into a card reader and keys in his identifier $ID_i$ and password $PW_i$. Then the smart card performs the following steps:

1) Generates a random number $r \in Z_q^*$;
2) Computes $t = g^r \bmod p$;
3) Computes $V_i = X_i \oplus h(ID_i||PW_i)$. Then the smart card computes $W_i = h(V_i \oplus T)$, where $T$ is the current time-stamp;
4) Computes $s = h(t||W_i)$;
5) Sends a message $C_1 = \{ID_i, t, s, T\}$ to the remote system.

**Authentication:** Upon receiving the authentication request message $C_1$, the remote system and the smart card will perform the following steps for mutual authentication between the user and the remote system.

1) The remote system verifies that $ID_i$ is correct. If not, the login request is rejected;
2) Let $T'$ be the time that the system receives $C_1$. The system compares $T$ and $T'$. If the difference between$T$ and $T'$ is within a valid time interval $\triangle T$, $C_1$ is considered as a valid message;
3) The system computes $V_i' = h(ID_i||x_s)$ as well as $W_i' = h(V_i' \oplus T)$;
4) The system compares $h(t||W_i')$ with $s$. If they are equal, then the system accepts the login request and proceeds to the next step, otherwise rejects the login request;

Table 1: Performance comparison of related schemes and our scheme

| | Juang | S.W.Lee et al. | Yoon-Ryu-Yoo | Our Scheme |
|---|---|---|---|---|
| Computation of Registration phase | 1hash | 1hash | 1 Exp +2 hash | 2hash |
| Computation of Login phase | 1 Sym +1 hash +1 Exp | 1hash | 1 Exp +2 hash | 1 Exp +3 hash |
| Computation of Authentication phase | 5 Sym +3 hash +3 Exp | 3hash | 2 Exp +4 hash | 3 Exp +7 hash |
| Computation of Password change | Not Supported | Not Supported | 2 hash | 2 hash |
| Communication cost | $\approx 3*1024$ bits | $\approx 5*128$ bits | $\approx 3*160$ bits | $\approx 2*(1024+160)$ bits |
| **Hash: hashing operations; Exp: exponentiation operations; Sym: Symmetric encryption or decryption.** | | | | |

5) The system picks a random number $\bar{r} \in Z_q^*$ and computes the session key $k = t^{\bar{r}} \bmod p$;

6) The system acquires the current time-stamp $T''$ and computes $w = h(V_i' \oplus T'')$, $u = g^{\bar{r}} \bmod p$, $v = h(u||w)$. The system sends back the message $C_2 = \{u, v, T''\}$ to $U_i$;

7) Upon receiving the message $\{u, v, T''\}$, the smart card verifies the validity of the time interval between $T''$ and the current time-stamp $T'''$, then computes $w' = h(V_i \oplus T'')$. If $v = h(u||W')$, the mutual authentication is complete. Then $k = g^{\bar{r}r} \bmod p$ is used as the session key between the user $U_i$ and the remote system.

Our scheme also enables user to change their password freely and securely. In fact, our strategy is similar to the method described in [9].

**Password change:** If the user $U_i$ wants to change his password from $PW_i$ to $PW_i^{'}$, he should insert his smart card into a card reader and keys in his identifier $ID_i$ and password $PW_i$. Then the smart card performs the following steps:

1) Computes $V_i = X_i \oplus h(ID_i||PW_i)$ and compares $V_i$ with $R_i$. If they are equal, then the smart card proceeds to the next step, otherwise rejects the password change request;

2) The user $U_i$ keys in a new password $PW_i'$;

3) The smart card computes $X_i' = V_i \oplus h(ID_i||PW_i')$ and stores $X_i'$ in place of $X_i$.

# 5 Security Analysis

In this section, the security of the proposed scheme is analyzed as follows:

1) The secure one-way function $h(\cdot)$ protects $x_s$ since it is computationally infeasible to invert a one-way function. The secret $R_i = h(ID_i||x_s)$ s stored in the smart card. A legal user must keys in his correct password in order that the correct value of $R_i$ can be computed by the smart card for the purpose of authentication.

2) It is impossible for an adversary to forge a valid login request message $\bar{C}_1 = \{ID_i, \bar{t}, \bar{s}, \bar{T}\}$, where $\bar{T}$ is the current time-stamp chosen by the intruder. The intruder must obtain the correct value of $\bar{W} = h(V_i \oplus \bar{T})$ to pass the remote system verification. However, there is no way for the intruder to compute $\bar{W}_i$ without the knowledge of the secret parameters $R_i$ or $x_s$. Similarly, a masqueraded server must obtain the correct $\bar{w}' = h(V_i \oplus \bar{T}'')$ to construct a valid message $\bar{C}_2$. Obviously, it is equivalent to obtaining the secret parameters $R_i$ or $x_s$.

3) The time-stamp $T$ and $T''$ can be used to verify the validity of messages. Hence the replay attack is prevented.

4) Assume that the secret key $x_s$ is disclosed to the intruder for some reason, e.g., stolen by the intruder. Based on the difficulty of solving DH problem [3], it is computationally infeasible for the intruder to derive the exchanged session key $k = g^{\bar{r}r} \bmod p$ from the given $(g, g^{\bar{r}}, g^r)$. Consequently, the proposed scheme is forward-secure.

5) During the phase of changing password, the smart card will verify the correctness of the previous password by comparing $V_i$ with stored $R_i$. Even if the smart card is stolen, unauthorized users cannot change the password associated with the smart card.

# 6 Performance Analysis

In this section, we evaluate the performance of the proposed scheme and the related schemes proposed in [6, 7, 9]. We assume $p$ with bit size 1024 and $q$ with bit size 160 in order to make the DH problem infeasible

to solve. The block size of a secure symmetric cryptosystem should be 128 bits. The output of a secure one-way function is assumed to be 128 bits. To provide forward-secrecy, the DH key exchange algorithm must be used in the scheme proposed in [7] such that both the computational cost and the communicational cost will increase considerably. The result is stated in Table 1.

In spite of its efficiency, the scheme in [6] does not provide the functionality of session key agreement. The problem of changing password is not considered in [7] and the performance of it has no advantage over other schemes in order to provide forward secrecy. Although the Yoon-Ryu-Yoo's scheme is more efficient than our scheme, our scheme can offer forward secrecy. Hence our scheme is acceptable under the situation that compromise of a long-term secret key(s) should not result in the compromise of the past session keys.

## 7 Conclusion

In this paper, we point out a security leak of the Yoon-Ryu-Yoo's password authentication scheme with smart card and propose a new scheme to offer forward secrecy. The proposed scheme can withstand the forgery attack while keeping the merit of the Yoon-Ryu-Yoo's scheme, e.g., mutual authentication, key agreement as well as enabling legal users to update their passwords freely and securely without the help of remote system.

## References

[1] G. Ateniese, M. Steiner and G. Tsudik, "New multiparty authentication services and key agreement protocols," *IEEE Journal on Selected Areas in Communication*, vol. 18, no. 4, pp. 628-639, 2000.

[2] C. C. Chang and W. Y. Liao, "A remote password authentication scheme based upon ElGamal's signature scheme," *Computer &Security*, vol. 13, no. 2, pp. 137-144, 1994.

[3] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644-654, 1976.

[4] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28-30, 2000.

[5] L. Lamport, "Password authentication with insecure communication," *Communication of ACM*, vol. 24, pp. 770-772, 1981.

[6] S. W. Lee, H. S. Kim and K. Y. Yoo, "Improvement of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards &Interfaces*, vol. 27, no. 2, pp. 181-183, 2005.

[7] W. S. Juang, "Efficient password authenticated key agreement using smart cards," *Computer &Security,* vol. 23, no. 2, pp. 167-173, 2004.

[8] H. M. Sun and L. H. Li, "An efficient remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958-961, 2000.

[9] E. J. Yoon, E. K. Ryu and K. Y. Yoo, "Efficient remote user authentication scheme based on generalized ElGamal signature scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 568-570, 2004.

**Bin Wang** received his Ph.D.degree in the Shanghai Jiaotong University, Peoples Republic of China. He is now a member of Yangzhou University. His research interests include cryptography and network security.

**Zheng-quan Li** received his Ph.D.degree in the Shanghai Jiaotong University, Peoples Republic of China. He is now a member of Yangzhou University. His research interests include coding theory.