Password Authentication Schemes: Current Status and Key Issues

Chwei-Shyong Tsai[§] Cheng-Chi Lee[†, ‡] Min-Shiang Hwang[§]

Department of Management Information Systems[§]
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan
Email: tsaics, mshwang@nchu.edu.tw

Department of Computer Science[†]
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan

Department of Computer & Communication Engineering[‡]
Asia University
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan

October 31, 2012

[§]Responsible for correspondence: Prof. Min-Shiang Hwang

Password Authentication Schemes: Current Status and Key Issues

Abstract

Password authentication scheme is one of the simplest and the most convenient authentication mechanisms over insecure networks. It is more frequently required in areas such as computer networks, wireless networks, remote login, operation systems, and database management systems. In this paper, we survey all related password authentication schemes and classify them with different properties. Previous schemes were vulnerable to various attacks and did not achieve goals of password authentication schemes. In order to compare related password authentication schemes with different properties, we define all attacks and goals of password authentication schemes that an ideal password authentication scheme should withstand and achieve. According to the ideal password authentication scheme, researchers should aim to propose a further password authentication scheme in which withstand all attacks and achieve all goals.

Keywords: Cryptography, ElGamal, one-way hash function, password authentication, RSA.

1 Introduction

To access the resources of the remote system, the users should have the access rights. One of the simplest and the most convenient security mechanism is password authentication scheme. For example, many applications, such as remote login, private corporations, ATM, PDA, and database management systems, etc., based on password authentication schemes are developed. To access theses resources, each user has an identifier (ID) and a password (PW).

ID and PW are maintained by the remote system. It provides the legal users to access the resources of the remote system. When a user wants to login to a remote server, he/she submit his/her ID and PW to the server. Once receiving the login message, the remote server will identify it with his stored password (verification) table. The password table including users' IDs and PWs are maintained by the remote system. If the submitted ID and PW match the corresponding pair stored in the server's password table, the user will be granted to access the server.

Two problems are found in this traditional mechanism. One is the revelation of the passwords can be seen by the administrator of the server because of the plain-text form of password table. The other is an intruder can impersonate a legal user by stealing the user's ID and PW from the password table. Additionally, the current Internet is vulnerable to various attacks such as denial of service attacks, forgery attacks, forward secrecy, server spoofing attacks, parallel session attacks, password guessing attacks, replay attacks, smart card loss attacks, and stolen-verifier attacks. These attacks are described and defined in Section 1.2.

1.1 Previous Researches

Hashed or encrypted of password can solve the above two problems [14, 37]. Then, Lamport proposed one-time password using one-way hash function against replay attacks [28]. However, three drawbacks of Lamport's scheme are as follows [31]: 1) it has high hash overhead. 2) it is the necessity for password resetting. 3) a password (verification) table should be stored in the server. Therefore, future researchers aim to solve the three drawbacks. To prevent the password table from stealing or modifying by others, researchers proposed solutions in which the password table is no longer required in the server [10, 18, 24]. To solve the drawback 1 and 2 of Lamport's scheme, Shimizu proposed CINON protocol [43]. Later, Shimizu et al. proposed PERM protocol [44] to solve the random number memorizing problem of CINON protocol.

From the Lamport's method, Haller derived the famous S/KEY one-time password for an Internet draft RFC 1760 [16, 17]. However, some researchers pointed out that S/KEY scheme does not protect against replay attacks, server spoofing attacks, and password guessing attacks [35, 53, 54]. Sandirigama et al. and Lin et al. proposed SAS [40] and OSPA protocol [33], respectively, which are superior to the Lamport's protocol, CINON protocol, and PERM protocol, in terms of storage utilization, computing time, and transmission overhead. However, Chen and Ku proposed two stolen-verifier attacks on SAS and OSPA prtocol [7].

Recently, a number of password authentication schemes using smart cards have been proposed by some articles [1, 2, 5, 6, 9, 10, 11, 15, 21, 22, 23, 24, 27, 29, 31, 32, 41, 42, 46, 47, 48, 51, 52, 55]. We classify them with different properties. The different properties will be introduced in next section. We brief three types password authentication schemes as follows. Here, we omit some papers [5, 6, 24, 48, 49] in which are based on the cryptography technics.

RSA-based Password Authentication Schemes

Yang and Shieh [52] proposed two password authentication schemes with smart cards. The two schemes are based on RSA public key cryptosystem [39]. They do not store passwords or verification tables in the server, and let users freely change their own passwords. However, some papers [3, 15, 42, 45] pointed out that Yang and Shieh's schemes have a drawback in that an intruder is able to impersonate a legal user by constructing a valid login request from an intercepted login request. Therefore, Yang and Shieh's schemes cannot prevent forgery attacks. Fan et al. [15] proposed a simple improved schemes to remedy the forgery attacks. The improved scheme limit ID with a strict form. In authentication phase, the remote system will check the ID's form. However, Chen et al. [8] and Wang et al. [47] showed that Fan et al.'s scheme cannot also withstand forgery attacks respectively.

Shen et al. [42] also proposed an enhancement of Yang-Shieh scheme. The proposed scheme can withstand forgery attacks and provide mutual authentication to withstand server spoofing attacks. However, Yang et al. [50] pointed out that Shen et al.'s scheme is still vulnerable to forgery attacks. Sun et al. [45] pointed out that [3]'s cryptanalysis was unreasonable and proposed the forgery attacks on Yang-Shieh scheme. To resist Sun et al.'s attack, Yang et al. [51] proposed an improvement of the Yang-Shieh scheme.

ElGamal-based Password Authentication Schemes

Hwang and Li [23] proposed a ElGamal-based remote user authentication scheme using smart cards. This scheme is based on ElGamal's public key cryptosystem [13]. Hwang-Li scheme does not need a password table to check the validity of the login request. Additionally, it can withstand replay attacks. However, some papers [1, 2, 4, 41] showed that Hwang-Li scheme cannot withstand forgery attacks. Shen et al. [41] and Awasthi et al. [1] proposed an improved scheme to remedy forgery attacks respectively. Besides, Awasthi et al.'s scheme can achieve forward secrecy. Forward secrecy ensures that the previously generated user's passwords are secure even if the system's secret key is stolen or has been public by accident. In the same year, Leung et al. [30] also showed that Shen et al.'s [41] scheme cannot withstand forgery attacks. Later, Kumar [27] proposed a new remote user authentication scheme using smart cards. This scheme is the modified form of the Shen et al.'s [41] and uses one more function C_K to generate the check digit for each registered identity.

Hash-based Password Authentication Schemes

Recently, lots of password authentication schemes based on one-way hash function are proposed because the computation cost is less than RSA-based and ElGamal-based password authentication schemes. Sun [46] proposed an efficient and practical remote user authentication. No password table is required to keep in his system and the communication and computation costs is reduced. However, this scheme did not allow users to choose and change freely their passwords and cannot achieve mutual authentication to authenticate the system [11]. Hwang et al. [22] and Chien et al. [11] proposed a simple remote user authentication scheme respectively. In those schemes, the authors claimed that their schemes can achieve the following goals: the verification or password tables are not required in the server; the communication cost and the computational cost is very low; the replay attack problem is completely solved; and users can freely choose their passwords. However, in [22], their scheme can not achieve mutual authentication. And in [11], their scheme did not let users freely change their passwords. Furthermore, Yoon et al. [55] pointed out that [22] is insecure if the secret key of the server is leaked or stolen. And Hsu [19, 20] showed that [11] is vulnerable to the parallel session attacks. Later, Lee et al. [29] proposed an improved efficient scheme to remedy the parallel session attacks.

Chen et al. [9] proposed two secure SAS-like password authentication schemes with lower storage, processing, and transmission overheads. The two schemes can withstand the stolen-verifier attacks of SAS and OSPA prtocol. Until to now, all password authentication schemes are based on static login ID. The static ID is vulnerable to leak partial information about the user's login message. Hence, Das et al. [12] proposed a dynamic ID-based remote user authentication scheme using smart cards. However, their scheme has some security flaws shown in [32]. Hence, Liao et al. [32] proposed an improved scheme to remedy these security flaws. Later, Liao et al. [31] further proposed a new scheme to achieve all of the proposed requirements. This scheme can agree a session key to encrypt/decrypt their communicated messages using the symmetric cryptosystem.

Although there are so many schemes proposed to authenticate a legitimate user, none of them can solve all problems and withstand all of the attacks. We define an ideal password authentication scheme which satisfies all of the security requirements and achieves all of the goals. Next, we will describe them.

1.2 Security Requirements and Definitions

In this section, we describe the security requirements and definitions to examine an ideal password authentication scheme. All previous researches cannot withstand all of the attacks. They can only show that their scheme can withstand one or more attacks. In this section, we introduce all of the attacks that an ideal password authentication scheme should withstand. We sort them as follows:

SR1. *Denial of Service Attacks*

An attacker can update the false verification information of a legal user for the next login phase. Afterwards, the legal user will not login successfully anymore.

SR2. *Forgery Attacks (Impersonation Attacks)*

An attacker attempts to modify the intercepted communications to masquerade the legal user to login the system.

SR3. *Forward Secrecy*

It ensures that the previously generated passwords in the system are secure even if the system's secret key has been public by accident or is stolen.

SR4. *Mutual Authentication*

The user and the server can authenticate each other. Not only can server verify the legal users, but users can verify the legal server. Mutual authentication can withstand the *server spoofing attacks* that an attacker wants to fake servers to manipulate the sensitive date of legal users.

SR5. *Parallel Session Attacks*

Without knowing user's password, an attacker can masquerade as the legal user by creating a valid login message from the eavesdropped communication between the suer and the server.

SR6. *Password Guessing Attacks*

Most passwords have low entropy so that it is vulnerable to password guessing attacks. An attacker intercepts authentication messages and stores them locally. Then he/she attempts to use a guessed password to verifies the correctness of his/her guess using theses authentication messages.

SR7. *Replay Attacks*

Intercepting the previous communications, an attacker can impersonate the legal user to login the system. The attacker can replay the intercepted messages.

SR8. *Smart Card Loss Attacks*

When the smart card is loss or stolen, unauthorized users can easily change new password of the smart card, or can guess the password of the user using password guessing attacks, or can impersonate the user to login the system.

SR9. *Stolen-verifier Attacks*

An attacker who steals the password-verifier (e.g., hashed passwords) from the server can use the stolen-verifier to impersonate a legal user to login the system.

1.3 An Ideal Password Authentication Scheme

An ideal password authentication scheme should withstand all of the above attacks. Besides, it should achieve the following goals:

G1. The passwords or verification tables are not stored in the system.

G2. The passwords can be chosen and changed freely by the users.

G3. The passwords cannot be revealed by the administrator of the server.

G4. The passwords are not transmitted in plain text on network.

G5. The length of a password must be appropriate for memorization.

G6. The scheme must be efficient and practical.

G7. The unauthorized login can be fast detected when a user inputs wrong password.

G8. A session key is established during password authentication process to provide confidentiality of communication.

G9. The ID should be dynamic for each login to avoid leaking partial information about the user's login message to the adversary.

G10. The proposed scheme is secure if the secret key of the server is leaked or stolen.

To propose an ideal password authentication scheme, it should withstand all of the above attacks and achieve the above goals. Unfortunately, none of the password authentication schemes can meet the two purposes. Comparisons of some important schemes are given in Section 4.

1.4 Organization

The remainder of this paper is organized as follows. In Section 2, we introduce the related theories, such as RSA scheme, ElGamal scheme, and one-way hash function. In Section 3, we sort password authentication schemes by three type, which are RSA-based, ElGamal-based, and Hash-based schemes. In Section 4, we shall give the comparisons in terms of security requirements, goals, and performance. Finally, in Section 5 and 6, we indicate some future research directions, and conclude this paper, respectively.

2 Related Theories

The proposed password authentication schemes employ some basic concepts, such as RSA scheme [39], ElGamal scheme [13], and one-way hash function [36, 38]. We brief these basic concepts as follows.

2.1 RSA Scheme

RSA public-key cryptosystem is proposed by Rivest, Shamir, and Adleman in 1978. The RSA scheme can be used for both digital signature and encryption. Its security is based on the difficulty of factoring large numbers. Here, we briefly review the RSA 's digital signature scheme as follows. p and q are two large primes. Compute $n = p \times q$ and choose e and d such that $e \times d \bmod (p-1)(q-1) \equiv 1$. Each user has a key pair, private key and public key. d denotes user's private key. (e, n) denotes user's public key. When Alice wants to sign a message M and sends it and its digital signature to Bob, Bob can verify the signed message is really signed by Alice. The processes is as:

Sign:

1. Alice computes $s = M^d \bmod n$, where d is Alice's private key.

2. The value s is Alice's signature on M. Then Alice sends Bob (M, s).

Verify:

When Bob receives theses messages from Alice, he can verify s whether is Alice's signature on M by checking $s^e =?M \bmod n$, where e is Alice's public key.

2.2 ElGamal Scheme

ElGamal public-key cryptosystem is proposed by ElGamal in 1985. The ElGamal scheme can be used for both digital signature and encryption. Its security is based on the difficulty of calculating discrete logarithms in finite field. Here, we briefly review the ElGamal's digital signature scheme as follows. To perform this scheme, each user has a key pair, private key and public key. Firstly, choose a prime p and two random numbers, g and x, such that two numbers are less than p. x denotes user's private key. y, g, and p denote user's public key, where $y = g^x \bmod p$. When Alice wants to sign a message M and sends it and its digital signature to Bob, Bob can verify the signed message is really signed by Alice. The processes is as:

Sign:

1. Alice selects a random number $k \in Z_{p-1}$.
2. Alice calculates $r = g^k \bmod p$.
3. Alice solves for s in the equation: $M = xr + ks \bmod (p-1)$, where x is Alice's private key.
4. The pair values r and s are Alice's signature on M. Then Alice sends Bob (M, r, s).

Verify:

When Bob receives theses messages from Alice, he can verify (r, s) whether is Alice's signature on M using the following equation:

$$g^M \quad = \quad g^{xr+ks \bmod (p-1)} \bmod p,$$

$$\begin{aligned} &= g^{xr} g^{ks} \bmod p, \\ &= y^r r^s \bmod p, \end{aligned} \tag{1}$$

where y is Alice's public key.

2.3 One-Way Hash Function Scheme

A one-way hash function $h : x \to y$ is a function, $y = h(x)$, which takes an arbitrary-length message x as the input and it returns a fixed-length hash value y. One-way hash function have the following properties that make them one-way:

- Given x, it is easy to compute $h(x) = y$. However, given y, it is hard to compute $h^{-1}(y) = x$. This property is one-way.
- Given x, it is computationally infeasible to find x' such that $x' \neq x$, but $h(x') = h(x)$.
- It is computationally infeasible to find any pair x and x' such that $x' \neq x$, but $h(x') = h(x)$.

Hash functions are aimed at high-speed software implementations and are currently in the public domain. In recent years, to strengthen the efficiency of cryptosystems, more and more cryptosystems can be used a one-way hash function to develop. We can see that many password authentication schemes are developed based on this hash function.

3 Related Works

In this section, we review three types password authentication schemes, such as RSA-based, ElGamal-based, and hash-based password authentication schemes. We just survey some important schemes for each type password authentication scheme. First, some notations are defined in Table 1. The all notations are used throughout this paper.

Each type password authentication scheme is composed of three phases, namely, registration phase, login phase, and authentication phase. In the registration phase, the user U sends a request registration to the remote server. Then the server issues a smart card and a password to U through a secure channel. In login phase, when U wants to login S for using resources of S, he/she inserts his/her smart card to a terminal and keys in his/her identity ID and password PW to access services. In authentication phase, S verifies the validity of the login request. Next, we review three types password authentication schemes below.

Table 1: Notations

U	the user
S	the remote system
ID	the user's identity
PW	the password of U
$h(\cdot)$	a one-way hash function
$Red(\cdot)$	a shadowed identity of the device which is only possessed with the S
$C_K(\cdot)$	a function to generate check digit for the registered identity, which is only possessed with the S
$\bigoplus$	XOR operation
x	the long secret key of S
y	the S's secret number stored in each user's smart card
$\|\|$	Concatenation
p, q	large prime numbers
g	the primitive element in Galois field GF(p)
T, T'	time-stamp
T_{RT}	the user's registered timestamp
N, N'	nonce
r, r', a, w	random numbers

3.1 RSA-based Password Authentication Schemes

3.1.1 Yang-Shieh Scheme [52]

Yang and Shieh proposed two password authentication schemes with smart cards. One is timestamp-based scheme. The other is nonce-based scheme.

Here, we introduced the firs one scheme. This scheme consists of three phases as follows:

Registration Phase

A Key Information Center(KIC) is necessary to issue a smart card to U. U submits his/her ID and a chosen PW to KIC. Then KIC performs the following steps:

1. Generate RSA key pair, private key d and public key (e, n). KIC publishes (e, n) and keeps d privately.

2. Find an integer g, which is a primitive in both GF(p) and GF(q).

3. Calculate the user's secret information W as $W = ID^d \bmod n$.

4. Generate the smart card's identifier CID of U and compute V by $V = g^{PW \times d} \bmod n$.

5. Write n, e, g, ID, CID, W, V to the memory of the smart card and issue the card to U.

Login Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and enters ID and PW. The smart card will perform the following steps:

1. Generate a random number r and calculate $X = g^{r \times PW} \bmod n$, and $Y = W \times V^{r \times h(CID,T)} \bmod n$.

2. Send the login request messages $(ID, CID, X, Y, n, e, g, T)$ to S.

Authentication Phase

Upon receipt of the login request messages, S performs the following steps:

1. Check whether ID is a valid user identity and CID is a legal smart card identity.

2. Check whether T is a validity of timestamp.

3. Check whether the equation $Y^e = ID \times X^{h(CID \times T)} \bmod n$ holds.

One of the above checks is no, the login request is rejected, otherwise the login request is accepted.

Furthermore, Yang-Shieh scheme allows users to freely change their passwords at will. A user can submit his/her smart card and a newly PW' to KIC over a secure channel. KIC replaces V with $V' = g^{PW' \times d} \bmod n$ and sends the card to the user.

3.1.2 Fan-Li-Zhu Scheme [15]

The scheme is same as the Yang-Shieh Scheme. The only difference is that this scheme limits ID with a strict form.

3.1.3 Yang-Wang-Chang Scheme [51]

Registration Phase

This phase also needs a Key Information Center(KIC) to issue a smart card to U. U submits his/her ID and a chosen PW to KIC. Then KIC performs the registered steps. The only different steps with Yang-Shieh scheme in this phase are step 3 and step 4 as follows.

Step 3. Generate the smart card's identifier CID of U and calculate the user's secret information W as $W = ID^{CID \times d} \bmod n$.

Step 4. Compute V by $V = g^{PW \times d} \bmod n$.

Login Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1. Generate a random number r and calculate $X = g^{PW \times r} \bmod n$, and $Y = W \times V^{r \times T} \bmod n$.

2. Send the login request messages $(ID, CID, X, Y, n, e, g, T)$ to S.

Authentication Phase

Upon receipt of the login request messages, S performs the following steps:

1. Check whether ID is a valid user identity and CID is a legal smart card identity.

2. Check whether T is a validity of timestamp.

3. Check whether the equation $Y^e = ID^{CID} \times X^T \bmod n$ holds.

One of the above checks is no, the login request is rejected, otherwise the login request is accepted.

3.2 ElGamal-based Password Authentication Schemes

3.2.1 Hwang-Li Scheme [23]

Registration Phase

U submits his/her ID to S for registration. S computes a password PW for the user as $PW = ID^x \bmod p$. S issues a smart card, which contains public parameters $(h(), p)$, and delivers PW to U through a secure channel.

Login Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1. Generate a random number r and calculate $C_1 = ID^r \bmod p$.

2. Compute $t = h(T \oplus PW) \bmod (p - 1)$.

3. Compute $M = ID^t \bmod p$.

4. Compute $C_2 = M(PW)^r \bmod p$.

5. Send the login request messages (ID, C_1, C_2, T) to S.

Authentication Phase

Upon receipt of the login request messages, S performs the following steps:

1. Check whether ID is a valid user identity.
2. Check whether T is a validity of timestamp.
3. Compute $PW = ID^x \bmod p$ and $t = h(T \oplus PW) \bmod (p-1)$.
4. Check whether the equation $C_2(C_1^x)^{-1} \bmod p = ID^t \bmod p$ holds.

One of the above checks is no, the login request is rejected, otherwise the login request is accepted.

3.2.2 Awasthi-Lal Scheme [1]

The scheme can provide forward secrecy which ensures the previously passwords in the system are secure even if the secret key of the system is stolen. This scheme is similar to Hwang-Li scheme. The only different phase is registration phase. We brief this different phase as follows.

Registration Phase

U submits his/her ID to S for registration. S computes $m = h(ID \oplus T_{RT})$, and $PW = m^x \bmod p$, where T_{RT} is the user's registered timestamp. S issues a smart card, which contains public parameters $(h(), p, T_{RT})$, and delivers PW to U through a secure channel.

Our New Attack

Awasthi and Lal pointed out that previously passwords in the system are secure even if x is public. When an attacker wants to obtain some previous password, he/she has to compute $PW = [h(ID \oplus T_{RT})]^x \bmod p$, where T_{RT} is postdated timestamp that prevents him/her to compute PW. However, this scheme cannot provide forward secrecy if smart card is lost or stolen. An attacker can derive the T_{RT} from the smart card and then compute $PW = [h(ID \oplus T_{RT})]^x \bmod p$ if he/she also have x. Hence, all previously passwords may be known by the attacker.

3.2.3 Kumar's Scheme [27]

Registration Phase

U submits his/her identity string J, which consists the name, a unique identification number of U, to S for registration. S computes $S_{ID} = Red(J), C_{ID} = C_K(S_{ID})$, and $PW = (S_{ID})^x \bmod p$. S issues a smart card, which contains public parameters $(h(), p)$, and delivers $(S_{ID} \parallel C_{ID}, PW)$ to U through a secure channel.

Login Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and keys in $S_{ID} \parallel C_{ID}$ and PW. The smart card will perform the following steps:

1. Generate a random number r and calculate $C_1 = (S_{ID})^r \bmod p$.
2. Compute $t = h(T \oplus PW) \bmod (p-1)$.
3. Compute $m = (S_{ID})^t \bmod p$.
4. Compute $C_2 = m(PW)^r \bmod p$.
5. Send the login request messages $(S_{ID} \parallel C_{ID}, C_1, C_2, T)$ to S.

Authentication Phase

Upon receipt of the login request messages, S performs the following steps:

1. Check whether S_{ID} is the specific format.
2. Check whether the equation $C_{ID} = C_K(S_{ID})$ holds.
3. Check whether T is a validity of timestamp.
4. Compute $PW = (S_{ID})^x \bmod p$ and $t = h(T \oplus PW) \bmod (p-1)$.
5. Check whether the equation $C_2 = (C_1^x)(S_{ID})^t \bmod p$ holds.

One of the above checks is no, the login request is rejected, otherwise the login request is accepted.

3.3 Hash-based Password Authentication Schemes

Due to the efficiency and one-way property, more and more cryptosystems including password authentication systems can be used a one-way function to develop. Recently, lots of password authentication schemes based on one-way hash function are proposed because the computation cost is less than RSA-based and ElGamal-based password authentication schemes.

3.3.1 Sun's Scheme [46]

Registration Phase

U submits his/her identity ID to S for registration. S computes a password $PW = h(ID, x)$. S issues a smart card, which contains public parameter $h()$, and delivers PW to U through a secure channel.

Login Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1. Compute $C_1 = h(T \oplus PW)$.

2. Send the login request messages (ID, C_1, T) to S.

Authentication Phase

Upon receipt of the login request messages, S performs the following steps:

1. Check whether ID is the specific format.

2. Check whether T is a validity of timestamp.

3. Compute $PW = h(ID, x)$ and $C_1' = h(T \oplus PW)$.

4. Check whether the equation $C_1 = C_1'$ holds.

One of the above checks is no, the login request is rejected, otherwise the login request is accepted.

3.3.2 Hwang-Lee-Tang Scheme [22]

Registration Phase

U chooses freely PW, and then computes $h(PW)$. U submits his/her identity ID and $h(PW)$ to S for registration over a secure channel. S computes $A = h(ID \oplus x) \oplus h(PW)$. S issues a smart card, which contains $(ID, A, h())$, to U through a secure channel.

Login Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1. Compute $B = A \oplus h(PW)$ and $C_1 = h(B \oplus T)$.

2. Send the login request messages (ID, C_1, T) to S.

Authentication Phase

Upon receipt of the login request messages, S performs the following steps:

1. Check whether ID is the specific format.

2. Check whether T is a validity of timestamp.

3. Compute $B' = h(ID \oplus x)$ and $C_1' = h(B' \oplus T)$.

4. Check whether the equation $C_1 = C_1'$ holds.

One of the above checks is no, the login request is rejected, otherwise the login request is accepted.

Furthermore, Hwang-Lee-Tang scheme allows users to freely change their passwords at will. A user can insert his/her smart card and key in a newly PW' to device. The smart card will compute $B = A \oplus h(PW) = h(ID \oplus x), h(PW')$, and $A' = B \oplus h(PW')$. Then the smart card replaces A with A'.

3.3.3 Chien-Jan-Tseng Scheme [11]

Registration Phase

U chooses freely PW, and submits his/her identity ID and PW to S for registration over a secure channel. S computes $R = h(ID \oplus x) \oplus PW$. S issues a smart card, which contains $(R, h())$, to U through a secure channel.

Login Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1. Compute $C_1 = R \oplus PW$ and $C_2 = h(C_1 \oplus T)$.
2. Send the login request messages (ID, C_2, T) to S.

Authentication Phase

Upon receipt of the login request messages, S performs the following steps:

1. Check whether ID is the specific format.
2. Check whether T is a validity of timestamp.
3. Compute $C_1' = h(ID \oplus x)$.
4. Check whether the equation $C_2 = h(C_1' \oplus T)$ holds.

One of the above checks is no, the login request is rejected, otherwise the login request is accepted. Furthermore, the user can authenticate the system. S should compute $C_3 = h(C_1' \oplus T')$, where T' is current timestamp. And S sends back the message (T', C_3). Upon receiving the message, U can verify the system as follows:

1. Check whether T' is a validity of timestamp.
2. Check whether the equation $C_3 = h(C_1 \oplus T')$ holds.

If the above checks hold, U believes that S is legal system and the mutual authentication is done; otherwise, U disconnects the connection.

3.3.4 Chen-Lee-Horng Scheme [9]

Registration Phase

U chooses freely PW and computes $h^2(PW \oplus N)$. Then U submits his/her identity ID, $h^2(PW \oplus N)$, and N to S for registration over a secure channel. S stores $h^2(PW \oplus N)$ into the verification table. S computes $h(x \parallel ID)$ and issues a smart card, which contains $(N, h(x \parallel ID))$, to U through a secure channel.

Login Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The steps of login are shown as follows:

1. U sends ID, r' to S.

2. S checks the format of ID, and returns $r \oplus h(x \parallel ID)$ and $h(r \parallel r')$.

3. Upon receiving $r \oplus h(x \parallel ID)$ and $h(r \parallel r')$, U can extract r from $r \oplus h(x \parallel ID)$. Then, with r, U verifies whether $h(r \parallel r')$ contains r' to authentication S.

4. With r, the smart card can compute $c_1 = h(PW \oplus N) \oplus h(h^2(PW \oplus N) \oplus r)$, $c_2 = h^2(PW \oplus N') \oplus h(PW \oplus N)$, and $c_3 = h^3(PW \oplus N')$.

5. U sends the login request messages (c_1, c_2, c_3) to S.

Authentication Phase

Upon receipt of the login request messages, S performs the following steps:

1. With r and $h^2(PW \oplus N)$, S can extract $h(PW \oplus N)$ from c_1.

2. Using $h(PW \oplus N)$, S can extract $h^2(PW \oplus N')$ from c_2.

3. Check whether the hash value of the extracted $h(PW \oplus N)$ is equal to that of the stored $h^2(PW \oplus N)$. If it holds, this login request is accepted; otherwise, it is rejected.

4. Check whether the hash value of the extracted $h^2(PW \oplus N')$ is equal to the received c_3. If it holds, S updates the verification table by replacing $h^2(PW \oplus N)$ with $h^2(PW \oplus N')$.

3.3.5 Liao-Lee-Hwang Scheme [32]

All previous schemes are based on static login identity. Liao, Lee, and Hwang proposed a dynamic ID-based remote user authentication scheme. The scheme is divided into three phases as follows: registration, authentication, and password change phases.

Registration Phase

U chooses freely PW and computes $h(PW)$. Then U submits his/her identity ID and $h(PW)$ to S for registration over a secure channel. S computes $L = h(PW) \oplus h(x \parallel ID)$ and issues a smart card, which contains $(L, y, h(\cdot))$, to U through a secure channel.

Authentication Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The steps of this phases are shown as follows:

1. The smart card computes a dynamic ID as $CID = h(PW) \oplus h(L \oplus y \oplus T)$, $B = h(CID \oplus h(PW))$, and $C = h(T \oplus L \oplus B \oplus y)$.

2. U sends the login request messages (CID, L, C, T) to S.

3. S checks whether T is a validity of timestamp.

4. S computes $h(PW) = CID \oplus h(L \oplus y \oplus T)$, and $B = h(CID \oplus h(PW))$.

5. S checks whether the equation $C = h(T \oplus L \oplus B \oplus y)$ holds. If it holds, S accepts U to login the ssytem; otherwise, rejects it.

6. S computes $D = h(T' \oplus L \oplus B \oplus y)$ and sends (D, T') to U.

7. Upon receiving (D, T'), U can check whether T' is a validity of timestamp and computes $h(T' \oplus L \oplus B \oplus y)$. Then, U compare it with the received D. If it holds, S is authenticated by U.

Password Change Phase

This scheme allows users to freely change their passwords at will. A user can insert his/her smart card and key in a newly PW' to device. The smart card will compute $L' = L \oplus h(PW) \oplus h(PW')$. Then the smart card replaces L with L'.

3.3.6 Yoon-Ryu-Yoo Scheme [55]

Registration Phase

U chooses freely PW, and submits his/her identity ID and PW to S for registration over a secure channel. S computes $V = h(ID, T_{RT}, x)$ and $A = h(ID, T_{RT}, x) \oplus PW$. S issues a smart card, which contains $(ID, V, A, h())$, to U through a secure channel.

Login Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1. Compute $B = A \oplus PW$ and verify whether B is equal to the stored V. If it holds, compute $C_1 = h(B \oplus T)$.

2. Send the login request messages (ID, C_1, T) to S.

Authentication Phase

Upon receipt of the login request messages, S and the smart card perform the following steps for mutual authentication between U and S.

1. S checks whether ID is the specific format.

2. S checks whether T is a validity of timestamp.

3. S computes $B' = h(ID, T_{RT}, x)$ and $C_1' = h(B', T)$. S compares C_1 and C_1'. If it holds, S accepts the login request; otherwise, S rejects it.

4. S computes $C_2 = h(B', C_1', T')$ and sends back the message (C_2, T').

5. Upon receiving (C_2, T'), U checks whether T' is a validity of timestamp. Then, compute $C_2' = h(B, C_1, T')$ and compare it with the received C_2. If it holds, U believes that the responding part is the real system.

One of the above checks is no, the login request is rejected, otherwise the login request is accepted.

Furthermore, Yoon-Ryu-Yoo scheme allows users to freely change their passwords at will. A user can insert his/her smart card and key in a newly PW' to device. The smart card will compute $B = A \oplus PW = h(ID, T_{RT}, x)$, and compare B with the stored V. If they are equal, compute $A' = B \oplus PW'$. Then the smart card replaces A with A'.

3.3.7 Lee-Kim-Yoo Scheme [29]

The registration phase and login phase are the same as Chien-Jan-Tseng scheme. The only difference between this scheme and Chien-Jan-Tseng scheme is in the authentication phase as follows:

Authentication Phase

The only difference between this phase of this scheme and this phase of Chien-Jan-Tseng scheme is in C_3. S compute $C_3 = h(h(C_1' \oplus T'))$, which is different from $C_3 = h(C_1' \oplus T')$ of Chien-Jan-Tseng scheme. And S sends back the message (T', C_3). Upon receiving the message, U can verify the system as follows:

1. Check whether T' is a validity of timestamp.

2. Check whether the equation $C_3 = h(h(C_1 \oplus T'))$ holds.

If the above checks hold, U believes that S is legal system and the mutual authentication is done; otherwise, U disconnects the connection.

Furthermore, Lee-Kim-Yoo scheme allows users to freely change their passwords at will. A user can insert his/her smart card and key in a newly PW' to device. The smart card will compute $R' = R \oplus PW \oplus PW'$. Then the smart card replaces R with R'.

3.3.8 Liao et al.'s Scheme [31]

Registration Phase

U chooses freely PW, and then computes $h(PW)$. U submits his/her identity ID and $h(PW)$ to S for registration over a secure channel. S computes $B = g^{h(x\|ID)+h(PW)} \bmod p$. S issues a smart card, which contains $(ID, B, p, g, h())$, to U through a secure channel.

Login Phase

When U wants to login S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card and S will perform the following steps:

1. U sends ID to S for login the system.
2. After receiving the login ID, S computes $B" = g^{h(x\|ID)r} \bmod p$. Then S computes $h(B")$ and sends back the message $(h(B"), r)$ to U.
3. Upon receiving $(h(B"), r)$, U computes $B' = (Bg^{-h(PW)})^r \bmod p$. Then U can verify the validity of server S by checking whether the received $h(B")$ is equal to hashed B'. If it holds, U computes $C = h(T\|B')$; otherwise, S is rejected. To overcome the replaying $(h(B"), r)$, in point 8 of Section 2.5, they pointed out we can add timestamp to it.
4. U sends the login request messages (ID, C, T) to S.

Modified Login Phase to Key agreement

The steps of login phase are modified as follows:

1. U sends ID to S for login the system.

2. After receiving the login ID, S computes $B" = g^{h(x\|ID)r} \bmod p$ and $A = g^a \bmod p$. Then S computes $h(B"\|A)$ and sends back the message $(h(B"\|A), r, A)$ to U.

3. Upon receiving $(h(B"\|A), r, A)$, U computes $B' = (Bg^{-h(PW)})^r \bmod p$. Then U can verify the validity of server S by checking whether the received $h(B"\|A)$ is equal to hashed $(B'\|A)$. If it holds, U computes $W = g^w \bmod p$ and $C = h(T\|B'\|W)$; otherwise, S is rejected. To overcome the replaying $(h(B"\|A), r, A)$, in point 8 of Section 2.5, they pointed out we can add timestamp to it.

4. U sends the login request messages (ID, C, W, T) to S.

Finally, U and S can agree the session key $K = A^w \bmod p = W^a \bmod p = g^{aw} \bmod p$.

Authentication Phase

Upon receipt of the login request messages (ID, C, T), S performs the following steps:

1. Check whether ID is the specific format.

2. Check whether T is a validity of timestamp.

3. Compute $C' = h(T\|B")$.

4. Check whether the equation $C = C'$ holds.

One of the above checks is no, the login request is rejected, otherwise the login request is accepted.

Furthermore, Liao et al.'s scheme allows users to freely change their passwords at will. A user can insert his/her smart card and key in a newly PW' to device. The smart card will compute $Y = g^{h(PW')} \bmod p$, $Z =$

$Bg^{-h(PW)} \bmod p$, and $\beta = YZ \bmod p$. Then the smart card replaces B with β.

4 Comparisons

In this section, we give the comparisons in terms of security requirements, goals, and performance. An ideal password authentication scheme is defined in Introduction that should meet the all security requirements and goals. Below, we check out recently papers whether it is an ideal password authentication scheme.

4.1 Security Requirements

Table 2, Table 3, and Table 4 show the comparisons in security requirements for three types schemes. In Table 2, Yang et al.'s scheme is the best scheme because their scheme can withstand most attacks. In Table 3, Awasthi-Lal and Kumar's scheme are the best schemes because of the same above reason. In Table 4, most schemes are the best schemes. Their schemes can withstand most various attacks. However, we can seen that none of the password authentication schemes among the three types is an ideal password authentication scheme.

Table 2: Comparisons of security requirements among the RSA-based schemes

	SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9
Yang-Shieh[52]	Y	N	Y	N	Y	Y	Y	Y	Y
Fan et al.[15]	Y	N	Y	N	Y	Y	Y	Y	Y
Yang et al.[51]	Y	Y	Y	N	Y	Y	Y	Y	Y

SRi: Proposed Security Requirements in Section 1, Y: Supported, N: Not supported.

4.2 Goals

Table 5, Table 6, and Table 7 show the comparisons in goals for three types schemes. In Table 5, all schemes cannot achieve most goals. These schemes

Table 3: Comparisons of security requirements among the ElGamal-based schemes

	SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9
Hwang-Li[23]	Y	N	N	N	Y	Y	Y	Y	Y
Awasthi-Lal[1]	Y	Y	Y	N	Y	Y	Y	Y	Y
Kumar[27]	Y	Y	Y	N	Y	Y	Y	Y	Y

SRi: Proposed Security Requirements in Section 1, Y: Supported, N: Not supported.

Table 4: Comparisons of security requirements among the hash-based schemes

	SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9
Sun[46]	Y	Y	N	N	Y	Y	Y	Y	Y
Hwang et al.[22]	Y	Y	Y	N	Y	Y	Y	N	Y
Chien et al.[11]	Y	Y	Y	Y	N	Y	Y	N	Y
Chen et al.[9]	Y	Y	Y	Y	Y	Y	Y	N	Y
Liao et al.[32]	Y	Y	Y	Y	Y	Y	Y	N	Y
Yoon et al.[55]	Y	Y	Y	Y	Y	Y	Y	N	Y
Lee et al.[29]	Y	Y	Y	Y	Y	Y	Y	N	Y
Liao et al.[31]	Y	Y	Y	Y	Y	Y	Y	N	Y

SRi: Proposed Security Requirements in Section 1, Y: Supported, N: Not supported.

are not good. In Table 6, these schemes are also not good because they cannot achieve most goals. In Table 7, Liao's scheme is the best scheme because their scheme can achieve most goals. However, we can seen that none of the password authentication schemes among the three types is an ideal password authentication scheme.

Table 5: Comparisons of goals among the RSA-based schemes

	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
Yang-Shieh[52]	Y	N	N	Y	Y	Y	N	N	N	N
Fan et al.[15]	Y	N	N	Y	Y	Y	N	N	N	N
Yang et al.[51]	Y	N	N	Y	Y	Y	N	N	N	N

Gi: Proposed Goals in Section 1, Y: Achieved, N: Not Achieved.

Table 6: Comparisons of goals among the ElGamal-based schemes

	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
Hwang-Li[23]	Y	N	N	Y	N	Y	N	N	N	N
Awasthi-Lal[1]	Y	N	N	Y	N	Y	N	N	N	N
Kumar[27]	Y	N	N	Y	N	Y	N	N	N	N

Gi: Proposed Goals in Section 1, Y: Achieved, N: Not Achieved.

Table 7: Comparisons of goals among the hash-based schemes

	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
Sun[46]	Y	N	N	Y	Y	Y	N	N	N	N
Hwang et al.[22]	Y	Y	Y	Y	Y	Y	N	N	N	N
Chien et al.[11]	Y	N	N	Y	Y	Y	N	N	N	N
Chen et al.[9]	N	N	Y	Y	Y	Y	N	N	N	N
Liao et al.[32]	Y	N	Y	Y	Y	Y	N	N	Y	N
Yoon et al.[55]	Y	Y	N	Y	Y	Y	Y	N	N	Y
Lee et al.[29]	Y	Y	N	Y	Y	Y	N	N	N	N
Liao et al.[31]	Y	Y	Y	Y	Y	Y	N	Y	N	N

Gi: Proposed Goals in Section 1, Y: Achieved, N: Not Achieved.

4.3 Performance

In the following, we compare the performance of the three types password authentication schemes. The performance evaluation of the all related works mainly concerns the time complexity. To evaluate these schemes, symbols are used to analyze the computational complexity as in Table 8. For simplification, we do not compare registration phase and change password among the three types schemes. Table 9, Table 10, and Table 11 show the comparisons in performance for three types schemes. It is seen that why more and more password authentication schemes are based on one-way hash function.

Table 8: Symbols

T_{mexp}	the time for executing a modular exponentiation operation
T_{mmul}	the time for executing a modular multiplication operation
T_{xor}	the time for executing a XOR operation
T_h	the time for executing a one-way hash function
T_{ck}	the time for executing a function $C_k()$

Table 9: The performance analysis of the RSA-based schemes

	Login Phase	Authentication Phase
Yang-Shieh[52]	$2T_{mexp} + 3T_{mmul} + 1T_h$	$2T_{mexp} + 1T_{mmul} + 1T_h$
Fan et al.[15]	$2T_{mexp} + 3T_{mmul} + 1T_h$	$2T_{mexp} + 1T_{mmul} + 1T_h$
Yang et al.[51]	$2T_{mexp} + 3T_{mmul}$	$3T_{mexp} + 1T_{mmul}$

Table 10: The performance analysis of the ElGamal-based schemes

	Login Phase	Authentication Phase
Hwang-Li[23]	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h$	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h$
Awasthi-Lal[1]	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h$	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h$
Kumar[27]	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h$	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h + 1T_{ck}$

Table 11: The performance analysis of the hash-based schemes

	Login Phase	Authentication Phase
Sun[46]	$1T_{xor} + 1T_h$	$1T_{xor} + 2T_h$
Hwang et al.[22]	$2T_{xor} + 2T_h$	$2T_{xor} + 2T_h$
Chien et al.[11]	$2T_{xor} + 1T_h$	$2T_{xor} + 2T_h$
Chen et al.[9]	$5T_{xor} + 8T_h$	$3T_{xor} + 3T_h$
Liao et al.[32]	x	$19T_{xor} + 9T_h$
Yoon et al.[55]	$2T_{xor} + 1T_h$	$4T_h$
Lee et al.[29]	$2T_{xor} + 1T_h$	$2T_{xor} + 4T_h$
Liao et al.[31]	$3T_{mexp} + 2T_{mmul} + 3T_h$	$1T_h$

5 Future Works

There are three types of identity authentication methods in the following [26]:

1. identity authentication of something known, such as password;
2. identity authentication of something possessed, such as smart cards;
3. identity authentication of some personal characteristics, such as fingerprint.

Most previous schemes use the first two methods to identify a user such as above reviewed schemes. In the future, combining these three methods can enhance the security level of a system. Expert researchers can attempt to propose an ideal password authentication scheme combining the three methods. The procedures of designing an ideal password authentication scheme is shown in Figure 1.

In addition, most proposed password authentication schemes are only designed for the single-server environment. Due to the scale of the networks becoming larger and larger, the password authentication schemes which only support single-server environment will insufficient for users' need. Therefore, some schemes [25, 34] are proposed for multi-server architecture. Users can register at the register center only once and access resources between different

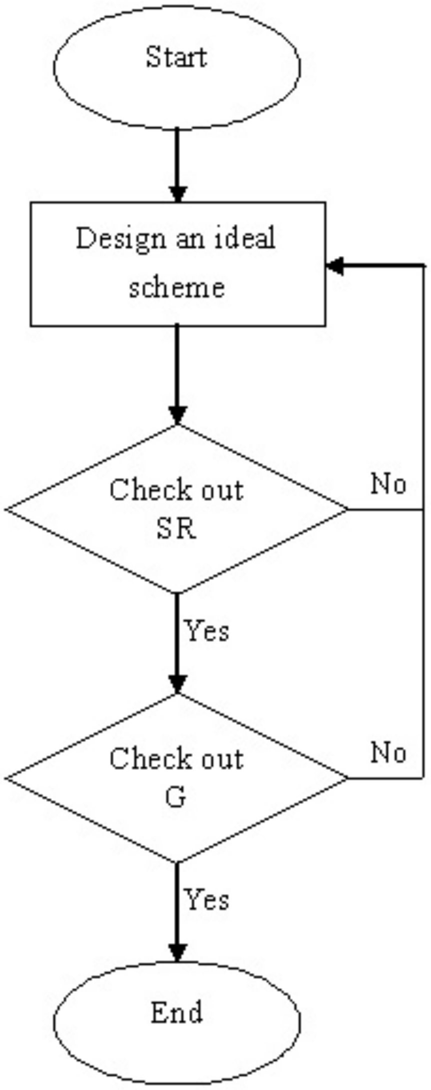

Figure 1: The procedures of designing an ideal password authentication scheme

servers efficiently. In the future, expert researchers can also attempt to propose an ideal password authentication scheme for multi-server architecture.

6 Conclusions

In this paper, we have surveyed all related password authentication schemes over insecure networks. Compare with these password authentication schemes, none of them can solve all problems and withstand all of the attacks. We define an ideal password authentication scheme which satisfies all of the security requirements and achieves all of the goals. In the future, an ideal password authentication scheme which meets all security requirements and goals is still an open problem. Expert researchers can attempt to propose a further password authentication scheme in which solve all problems.

References

[1] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1246–1248, 2003.

[2] Chi-Kwong Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, vol. 46, pp. 992–993, 2000.

[3] Chi-Kwong Chan and L. M. Cheng, "Cryptanlysis of timestamp-based password authentication scheme," *Computers & Security*, vol. 21, no. 1, pp. 74–76, 2002.

[4] C. C. Chang and K. F. Hwnag, "Some forgery attack on a remote user authentication scheme using smart cards," *Infomatics*, vol. 14, no. 3, pp. 189–194, 2003.

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

[6] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, pp. 165–168, May 1991.

[7] Chien-Ming Chen and Wei-Chi Ku, "Stolen-verifier attack on two new strong-password authentication protocols," *IEICE Transactions on Communications*, vol. E85-B, pp. 2519–2521, November 2002.

[8] K. F. Chen and S. Zhong, "Attacks on the (enhanced) Yang-Shieh authentication," *Computers & Security*, vol. 22, no. 8, pp. 725–727, 2003.

[9] Tzung-Her Chen, Wei-Bin Lee, and Gwoboa Horng, "Secure SAS-like password authentication schemes," *Computer Standards & Interfaces*, vol. 27, pp. 25–31, 2004.

[10] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng, "A modified remote login authentication scheme based on geometric approach," *Journal of Systems and Software*, vol. 55, pp. 287–290, 2001.

[11] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers & Security*, vol. 21, pp. 372–375, 2002.

[12] Manik Lal Das, Ashutosh Saxena, and Ved P. Gulati, "A dynamid ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[13] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, July 1985.

[14] A. Jr. Evans, W. Kantrowitz, and E. Weiss, “A user authentication scheme not requiring secrecy in the computer,” *Communications of the ACM*, vol. 17, pp. 437–442, August 1974.

[15] L. Fan, J.H. Li, and H. W. Zhu, “An enhancement of timestamp-based password auhentication scheme,” *Computers & Security*, vol. 21, pp. 665–667, 2002.

[16] N. Haller, “The S/KEY one-time password system,” in *Proceedings of Internet Society Symposium on Network and Distributed System Security*, pp. 151–158, 1994.

[17] N. Haller, “The S/KEY one-time password system,” *RFC1760*, Feb. 1995.

[18] Gwoboa Horng, “Password authentication without using password table,” *Information Processing Letters*, vol. 55, pp. 247–250, 1995.

[19] C. L. Hsu, “Security of two remote user authentication schemes using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1196–1198, 2003.

[20] C. L. Hsu, “Security of Chien et al.’s remote user authentication scheme using smart cards,” *Computer Standards and Interfaces*, vol. 26, no. 3, pp. 167–169, 2004.

[21] Min-Shiang Hwang, “Cryptanalysis of remote login authentication scheme,” *Computer Communications*, vol. 22, no. 8, pp. 742–744, 1999.

[22] Min-Shiang Hwang, Cheng-Chi Lee, and Yuan-Liang Tang, “A simple remote user authentication scheme,” *Mathematical and Computer Modelling*, vol. 36, pp. 103–107, 2002.

[23] Min-Shiang Hwang and Li-Hua Li, “A new remote user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[24] J. K. Jan and Y. Y. Chen, “’paramita wisdom’ password authentication scheme without verification tables,” *The Journal of Systems and Software*, vol. 42, pp. 45–57, 1998.

[25] W. S. Juang, “Efficient multi-server password authentication key agreement using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 251–255, 2004.

[26] H. J. Kim, “Biometrics, is it a viable proposition for identity authentication and access control,” *Computers & Security*, vol. 14, pp. 205–214, 1995.

[27] Manoj Kumar, “New remote user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 597–600, 2004.

[28] L. Lamport, “Password authentication with insecure communication,” *Communications of the ACM*, vol. 24, pp. 770–772, November 1981.

[29] S. W. Lee, H. S. Kim, and K. Y. Yoo, “Improved efficient remote user authentication scheme using smart cards,” *IEEE Transactions on Communications*, vol. 50, pp. 565–567, May 2004.

[30] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, “Cryptanalysis of a modified remote user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1243–1245, 2003.

[31] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang, "A password authentication scheme over insecure networks," *accepted in Journal of Computer and System Sciences*, 2005.

[32] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang, "Security enhancemento for a dynamic id-based remote user authentication scheme," in *IEEE CS Press, International Conference on Next Generation Web Services Practices (NWeSP'05)*, pp. 437–440, Seoul, Korea, August 2005.

[33] C. L. Lin, H. M. Sun, and T. Hwang, "Attacks and solutions on strong-password authentication," *IEICE Transactions on Communications*, vol. E84-B, pp. 2622–2627, September 2001.

[34] I. C. Lin, M. S. Hwang, and L. H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, pp. 13–22, 2003.

[35] C. J. Mitchell and L. Chen, "Comments on the S/KEY user authentication secheme," *ACM Operating Systems Review*, vol. 30, pp. 12–16, Oct. 1996.

[36] NIST. "Secure hash standard,". Tech. Rep. FIPS 180-1, NIST, US Department Commerce, April 1995.

[37] G. B. Purdy, "A high security log-in procedure," *Communications of the ACM*, vol. 17, pp. 442–445, Aug. 1974.

[38] R. Rivest. "The MD5 message digest algorithm,". Tech. Rep. RFC 1321, IETF, April 1992.

[39] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[40] M. Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol (sas)," *IEICE Transactions on Communications*, vol. E83-B, pp. 1363–1365, June 2000.

[41] Jau-Ji Shen, Chih-Wei Lin, and Min-Shiang Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414–416, 2003.

[42] Jau-Ji Shen, Chih-Wei Lin, and Min-Shiang Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards," *Computers & Security*, vol. 22, no. 7, pp. 591–595, 2003.

[43] A. Shimizu, "A dynamic password authentication method by one-way function," *IEICE Transactions on Information and System*, vol. J73-D-I, pp. 630–636, July 1990.

[44] A. Shimizu, T. Horioka, and H. Inagaki, "A password authentication method for contents communication on the Internet," *IEICE Transactions on Communications*, vol. E81-B, pp. 1666–1763, Aug. 1998.

[45] H. M. Sun and H. T. Yeh, "Further cryptanalysis of a password authentication scheme with smart cards," *IEICE Transactions and Communications*, vol. E86-B, no. 4, pp. 1412–1415, 2003.

[46] Hung-Min Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958–961, 2000.

[47] B. Wang, J. H. Li, and Z. P. Tong, "Cryptanalysis of an enhanced timestamp-based password authentication scheme," *Computers & Security*, vol. 22, no. 7, pp. 643–645, 2003.

[48] T. C. Wu, "Remote login authentication scheme based on a geometric approash," *Computer Communications*, vol. 18, no. 12, pp. 959–963, 1995.

[49] S. Yamaguchi, K. Okayama, and H. Miyahara, "Design and implementation of an authentication system in WIDE Internet environment," in *Proceedings of IEEE Region Conference on Computer and Communication System*, 1990.

[50] C. C. Yang, H. W. Yang, and R. C. Wang, "Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 578–579, 2004.

[51] Chou-Chen Yang, Ren-Chiun Wang, and Ting-Yi Chang, "An improvement of the Yang-Shieh password authentication schemes," *Applied Mathematics and Computation*, vol. 162, pp. 1391–1396, 2005.

[52] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," *Computers & Security*, vol. 18, no. 8, pp. 727–733, 1999.

[53] Tzu-Chang Yeh, Hsiao-Yun Shen, and Jing-Jang Hwang, "A secure one-time password authentication scheme using smart cards," *IEICE Trans. on Communications*, vol. E85-B, pp. 2515–2518, Nov. 2002.

[54] S. M. Yen and K. H. Liao, "Shared authentication token secure against replay and weak key attacks," *Information Processing Letters*, vol. 62, pp. 77–80, 1997.

[55] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "An improvement of Hwang-Lee-Tang's simple remote user authentication schemes," *Computers & Security*, vol. 24, pp. 50–56, 2005.