Nova Scientia
Revista de Investigación de la Universidad De La Salle Bajío

Revista Electrónica Nova Scientia

Dynamic ID-based remote user authentication scheme using ElGamal encryption system
Esquema de autenticación de usuario remoto basado en un identificador dinamico utilizando el sistema de cifrado ElGamal

Rafael Martínez Peláez[1], Yesica Saavedra Benitez[2], Pablo Velarde Alvarado[3] y Jacek Pomykala[4]

[1]Facultad de Tecnologías de Información, Universidad De La Salle Bajío, León
[2]División de Estudios de Posgrado e Investigación, Instituto Tecnológico de Toluca, Toluca
[3]Ciencias Básicas e Ingenierías, Universidad Autónoma de Nayarit, Nayarit
[4]Faculty of Mathematics Informatics and Mechanics, University of Warsaw, Warsaw

Mexico - Poland

Rafael Martinez Pelaez. E-mail: rmartinezp@delasalle.edu.mx

Resumen

Se propone un nuevo esquema de autenticación de usuario remoto basado en un identificador dinámico, utilizando tarjetas inteligentes. Se utiliza una función unidireccional, criptosistema de clave pública ElGamal, y un número aleatorio. El esquema propuesto cumple con los siguientes requerimientos de seguridad: 1) los usuarios pueden seleccionar y cambiar su contraseña libremente, 2) autenticación mutua entre el usuario y el servidor, 3) el usuario y el servidor establecen una clave de sesión después de concluir exitosamente el proceso de autenticación, 4) el servidor no mantiene una tabla de verificación, 5) el mensaje de inicio de sesión no contiene la identidad del usuario, y 6) la fase de autenticación no requiere sincronización de tiempo. Además, el esquema puede resistir ataques bien conocidos, haciéndolo más seguro que otros trabajos relacionados. Con el fin de verificar las características de seguridad del protocolo propuesto, se ha modelado y analizado utilizando HLPSL y la herramienta AVISPA. Los resultados demuestran que el protocolo introducido ofrece mayores requisitos de seguridad que trabajos anteriores.

Palabras claves: criptografía, seguridad en redes, logaritmo discreto, autenticación mutua, contraseña, tarjetas inteligentes, herramienta AVISPA

Recepción: 22-08-2016 *Aceptación: 13-09-2016*

Abstract

We propose a new dynamic ID-based remote user authentication scheme using smart cards, which it is based on one-way hash function, ElGamal's public key cryptosystem and nonce. The scheme achieves the following security requirements: 1) users can choose and change their password freely, 2) mutual authentication between the user and the server, 3) the user and the server establish a session key after successful authentication process, 4) the server does not

maintain a verification table, 5) the login request message does not contain the user's identity, and 6) the authentication phase does not require time-synchronization, making it more secure than previous schemes. In order to verify the security characteristics of our protocol, we have modelled and analysed the proposal using High-level Protocol Specification Language (HLPSL) and Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The results demonstrate that our protocol achieves more security requirements than previous works.

Keywords: cryptography, computer network, discrete logarithm, mutul authentication, password, smart cards, AVISPA tool

Introduction

Remote user authentication scheme is a key security component for electronic services and it must provide the following security requirements (Madhusudhan and Mittal, 2012): 1) no verification table, the server should not store any information about the user in a database; 2) users can choose and change their password freely, users should have the option to create and to modify their password without assistance; 3) mutual authentication, user and server must be authenticated by each other; 4) password dependent, the user's smart card should not compute a login request message without the previous verification of user's identity; 5) session key agreement, after the successful authentication phase, the user and the server should share a session key; and 6) user's anonymity, the login request message should not contain the user's identity.

In 1981, Lamport (1981) proposed the first remote user authentication scheme based on one-way hash function. However, the server needs to maintain a verification table, making it susceptible to steal or to modify information stored in a database (Chang and Wu, 1991; Hwang and Li, 2000). Later, Hwang, Chen and Laih (1990) introduced the use of smart cards. They proposed the first remote user authentication scheme without the existence of verification table.

Ten years later, Chang and Wu (1991) proposed a scheme based on the Chinese Remainder Theorem. Their scheme was inspired from Shamir's identity-based signature scheme (Shamir, 1984). Later, Chang and Liao (1994) proposed the first remote user authentication scheme based on ElGamal's public key cryptosystem (ElGamal, 1985) and time-stamping. Since 1994, many schemes based on ElGamal's public key cryptosystem have been proposed (Awasthi and Lal, 2005; Chan and Cheng, 2000; Chang and Hwang, 2003; Hölbl and Welzer, 2009; Hwang and Li, 2000; Kumar, 2004; Lee and Chiu, 2005; Ramasamy and Munivandi, 2009; Rhee, Kwon and Lee, 2009; Shao, 2004; Shen, Lin and Hwang, 2003; Tseng, 2007; Wang and Chang, 1996; Yoon, Ryu and Yoo, 2004) to enhance security.

However, previous works do not maintain the user's anonymity during the login phase because each user sends its identity in clear text to the server, making the schemes susceptible to identity theft, impersonation attack, and forgery attack (Chan and Cheng, 2000; Das, Saxena and Gulati, 2004; Hölbl and Welzer, 2009; Leung et al., 2003; Shen, Lin and Hwang, 2003). Moreover, some schemes are based on time-synchronization which it is still a problem (Juang, 2004; Lee, Kim and Yoo, 2005a; Liaw, Lin and Wu, 2006) in existing networks environments because the data

transmission and processing delay is uncertain. Furthermore, previous works do not give the option to users to choose and to change their password freely (Lee, Kim and Yoo, 2005b).

In this paper, we point out that previous works are unsecured for electronic services because such works do not achieve the security requirements explained by Madhusudhan and Mittal (2012). For that reason, we propose a new scheme which provides all the security requirements for an ideal remote user authentication scheme (Madhusudhan and Mittal, 2012) and withstand very well known attacks to enhance the security. Moreover, we compare it with other related works in terms of security, demonstrating that the proposed scheme is more secure. Our scheme is inspired by the idea of Das, Saxena and Gulati (2004). The rest of this paper is organized as follows. In Section 2, we explain the proposed scheme. In Section 3, we carry out the security analysis and comparison of the proposed scheme with other related works. Finally, conclusions are given in Section 4.

Proposed scheme

Table 1 shows the notations used throughout this paper.

U	User
ID	Identity of U
PW	Password of U
SC	Smart card of U
S	Server
x, y, z	Secret numbers of S
$h( )$	One-way hash function
SK_{US}	Session key between U and S
$E_{SK}( )$	Symmetric encryption using SK
$D_{SK}( )$	Symmetric decryption using SK
N_U, N_S	Nonce of U and Nonce of S
Z_P^*	Multiplicative group
α	Generator of Z_P^*
a	Random exponente of U
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation
➔	Secure cannel
→	Open cannel

Source: Own elaboration

Our scheme is composed of the following phases:

Phase 1- Initialization. In this phase, S computes public parameters used by each user in the scheme.

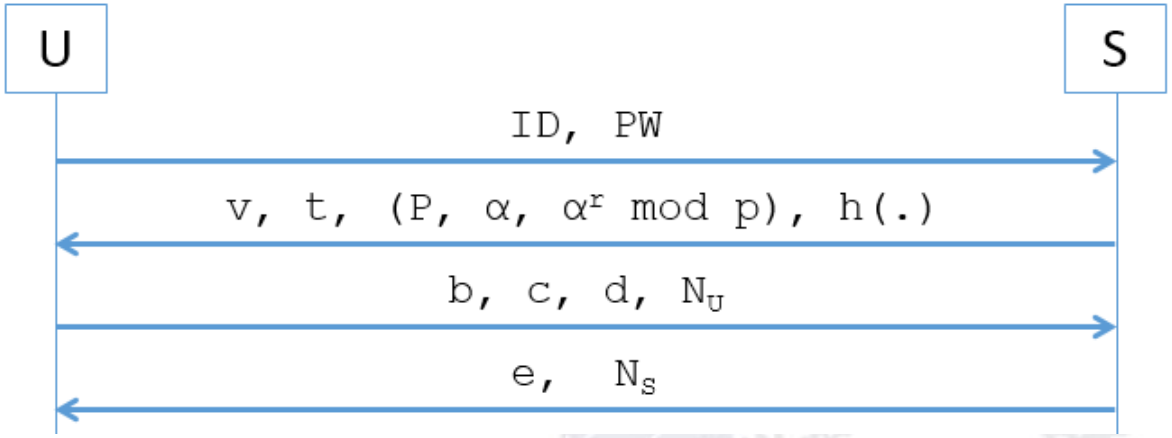
Phase 2- Registration. In this phase, U shares personal information with S to be part of the system. As a result, U obtains its smart card with security parameters (v, t, (P, α, α^r ($mod\ p$)), $h(.)$).

Phase 3- Login. In this phase, U computes the login request message (b, c, d, N_U).

Phase 4- Mutual authentication and session key. In this phase, U and S verifies the identity of each other and creates a session key (SK_{US}).

Phase 5- Password change. In this phase, U can choose a new password whenever and wherever it wants.

The protocol is presented in Figure 1.



Source: Own elaboration

Now, we describe each phase of the proposed protocol.

Phase 1: S generates two public parameters P and α, where P is a large prime number and α is a primitive root in Galois Field $GF(P)$. Then, S chooses three numbers (x, y, z) with a length of 256 bits. Next, S computes $r = h(x||y||z)$ creating its secret key. Later, S computes α^r ($mod\ p$) creating its publick key. In this scenario, the triplet (P, α, α^r (mod p)) are the public parameters of S. Moreover, S publishes the one-way hash function $h(\ )$ used in the scheme.

Phase 2: S creates the security parameters of U as follows:

Step 1 U → S: ID, PW

Step 2 S: $v = h(ID||PW) \oplus r \oplus h(ID||x||y||z)$

Step 3 S: $t = h(r \oplus h(ID||x||y||z) \oplus h(PW))$

Step 4 S → U: $v, t, (P, \alpha, \alpha^r \pmod p), h(.)$

U sends ID and PW to S through a secure channel. Afterthat, S calculates v computing two hash functions and two XOR operations. S uses the information received from U, the three numbers (x, y, z) and secret key r. Then, S calculates v computing two hash functions and one XOR operation. Finally, S stores the security parameters $(v, t, (P, \alpha, \alpha^r \pmod p))$ and one-way hash fuction $h( )$ in U's SC.

Phase 3: This phase is invoked whenever U wants to login S. First, U inserts its SC into the smart card reader and keys its ID and PW. Then, SC carries out the following steps:

Step 1 SC: $h(ID||PW), h(PW)$

Step 2 SC: $r^* \oplus h(ID||x||y||z)^* = h(ID||PW) \oplus v$

Step 3 SC: $t^* = h(r^* \oplus h(ID||x||y||z)^* \oplus h(PW))$

Step 4 SC: $t^* \stackrel{?}{=} t$

Step 5 SC: a

Step 6 SC: $b \equiv \alpha^a \pmod p$

Step 7 SC: $c \equiv ID \times (\alpha^r)^a \pmod p$

Step 8 SC: N_U

Step 9 SC: $d = h(h(ID)||r||h(ID||x||y||z)||N_U)$

Step 10 U → S: b, c, d, N_U

After U keys its ID and PW, its SC computes the following hash values: $h(ID||PW)$ and $h(PW)$. Then, SC recovers $r^* \oplus h(ID||x||y||z)^*$ from v as follows:

$$h(ID||PW) \oplus v = h(ID||PW) \oplus h(ID||PW) \oplus r \oplus h(ID||x||y||z)$$
$$= r^* \oplus h(ID||x||y||z)^*$$
$$= h(x||y||z)^* \oplus h(ID||x||y||z)^*$$

Later, SC verifies the identity of U by means of the comparison between t^* and t. If the verification is positive, the identity of U is verified and the process continues; otherwise, SC closes the session. Next, SC generates the secret key a, and it computes b and c using ElGamal cryptosystem. Then, SC generates a random number N_U. Later, SC computes d using the information recovered in step 2 and the U's ID. Finally, U sends the login request message (b, c, d, N_U) to S through an open channel.

Phase 4. After the login request message (b, c, d, N_U) is received, S performs the following operations:

Step 1 S: $ID \equiv b^{-r} \times c \pmod p$

Step 2 S: $d^* = h(h(ID)||h(x||y||z)||h(ID||x||y||z)||N_U)$

Step 3 S: $d^* \stackrel{?}{=} d$

Step 4 S: N_S

Step 5 S: $SK_{US} = h(h(ID)||h(x||y||z)||h(ID||x||y||z)||N_U||N_S)$

Step 6 S: $e = E_{SK}(N_U + N_S)$

Step 7 S → U: e, N_S

S decrypts ID as follows:

$$b^{-r} \times c \bmod p \equiv (\alpha^a)^{-r} \times ID \times (\alpha^r)^a \bmod p$$
$$\equiv \alpha^{-ra} \times ID \times \alpha^{ra} \pmod p$$
$$\equiv ID \pmod p$$

Then, S computes d^* and uses it to verify the identity of U comparing d^* and d. If they are equal, U is a legal user; otherwise, the session is closed. Next, S computes the session key SK_{US} using secret information known only by it $h(x||y||z)||h(ID||x||y||z)$, information received from U $(h(ID))$ and information generated by each other during the current session N_U and N_S. Later, S encrypts N_U and N_S using the session key $E_{SK}(N_U + N_S)$ as verification proof. Finally, S sends the login response message (e, N_S) to U through an open channel.

Upon receiving the login response message (e, N_S), U performs the following operations:

Step 1 U: $SK_{US} = h(h(ID)||h(x||y||z)||h(ID||x||y||z)||N_U||N_S)$

Step 2 U: $(N_U + N_S)^* = D_{SK}(e)$

Step 3 U: $(N_U + N_S)^* ?= (N_U + N_S)$

U computes the session key SK_{US} and decrypts e. As result, U knows $(N_U + N_S)^*$ and verifies the validity of the session key by means of the comparison between $(N_U + N_S)^*$ and $(N_U + N_S)$. If the comparison is correct, the session key is accepted and the legitimacy of S is validated.

Note: U and S can exchange messages using the session key SK_{US}.

Phase 5. When U wants to change its PW with a new password PW_{new}, it needs to carry out the following process.

Step 1 U: ID, PW

Step 2 SC: h(ID||PW), h(PW)

Step 3 SC: $r^* \oplus h(ID||x||y||z)^* = h(ID||PW) \oplus v$

Step 4 SC: $t^* = h(r^* \oplus h(ID||x||y||z)^* \oplus h(PW))$

Step 5 SC: $t^* ?= t$

Step 6 SC: PW_{new}

Step 7 SC: $v_{new} = h(ID||PW_{new}) \oplus r^* \oplus h(ID||x||y||z)^*$

Step 8 SC: $t_{new} = h(r^* \oplus h(ID||x||y||z)^* \oplus h(PW_{new}))$

Step 9 SC: REPLACE v and t with v_{new} and t_{new}

Security Analysis

In this section, we discuss the security features of the proposed scheme. The security analysis corroborates the security advantages of the proposed scheme.

Resist off-line guessing attack: in the proposed scheme, U's smart card contains $(v, t, (P, \alpha, \alpha^r \pmod p), h( ))$ after registration phase. Assuming that an adversary is a legal user of the system, it can obtain $r \oplus h(ID||x||y||z)$ from $v = h(ID||PW) \oplus r \oplus h(ID||x||y||z)$ because the attacker knows ID and PW. Unfortunately for the adversary, $r \oplus h(ID||x||y||z)$ does not provide any sensitive information. In this case, S uses four pieces of secret information instead of one. Moreover, $h(ID||x||y||z)$ is personalized by ID, making it unique in the scheme.

Resist impersonation attack: if the adversary knows the login request message $(b, c, d,$

N_U), the attacker cannot compute a valid login request message (b^*, c^*, d^*, N_U^*) without knowing the correct ID and $h(ID||x||y||z)$ because c and d requires the knowledge of both values. Moreover, S checks the validity of d in the mutual authentication and session key agreement phase.

Resist server spoofing attack: in this case, the adversary cannot compute a valid login response message (e, N_S) because the attacker needs to know the secret numbers of S. Moreover, the attacker cannot compute a valid session key $SK_{US} = h(h(ID)||h(x||y||z)||h(ID||x||y||z)||N_U||N_S)$ because it does not know the values of ID, $h(x||y||z)$ and $h(ID||x||y||z)$ corresponding to the legal U.

Resist recovers private data attack: if the adversary tries to recover encrypted information, it needs to compute the correct SK_{US}. In this case, the attacker cannot compute the correct session key because it does not know the correct values of ID, $h(x||y||z)$ and $h(ID||x||y||z)$. Moreover, the adversary can find a if it can compute a discrete log in the large prime $modulus\ p$, where in practical situation is a hard problem.

Avoids inefficiency for error password login: in the proposed scheme, U's smart card verifies the identity of U by means of two process: 1) knowledge of ID and PW to recover $r \oplus h(ID||x||y||z)$ and 2) knowledge of PW to compute a valid $t = h(r \oplus h(ID||x||y||z) \oplus h(PW))$ in order to validate the identity of U.

Provides user's anonymity: in the proposed scheme, U's anonymity is preserved at each login request because U does not send its ID in clear over an open network. The login request message (b, c, d, N_U) does not provide information about the U's identity. Moreover, the value of d is dynamic every time because this value is computed using a nonce N_U. Hence, the adversary cannot identify the victim trying to login into the server.

Formal security analysis

In order to verify the security goals of the proposed protocol - mutual authentication and secrecy of the session key – we have modelled and analysed it using High-Level Protocol Specification Languange (HLPSL) (Chevalier, 2004) and Automated Validation of Internet Security Protocols and Applications (AVISPA) tool (Armando, 2005). HLPSL is a modelling language to write specifications for security protocols based on roles. Each role contains a set of actions of a single

agent, which its transitions is indicated as a state. On the other hand, AVISPA tool consists of four back-ends called: Constraint-Logic-Based Attack Searcher (CL-AtSe), On-the-Fly Model-Checker (OFMC), SAT-Based Model-Checker (SATMC), and Tree Automata-Based Protocol Analyser (TA4SP).

We have considered two players – user (A) and server (B) –, symmetric key (Kab) and one-way function (H) knowledge by each player, and communication channels – user (SA, RA) and server (SB, RB) –, where each communication channel assumes the presence of a Dolev-Yao Intruder (Dolev and Yao, 1983). The Dolev-Yao Intruder (dy) implies the following assumptions: 1) the adversary or attacker can capture any message in the network; 2) the adversary or attacker can impersonate any legitimate user in the system; and 3) the adversary or attacker can execute many concurrent instances of the protocol. Under this circunstances, we have modelled the role of user and server as follows:

```
role user (A, B : agent,Kab : symmetric_key,H : function,Snd, Rcv : channel(dy))
played_by A
def=
local
State : nat,
C, W, Z, Y, X, R, Pw, Na, Nb : text,
Kab1 : message
const server_user_kab1, server_user_n : protocol_id
init  State := 0
transition
1. State   = 0 /\ Rcv(start) =|>
   State' := 1 /\ Pw' := new() /\ Snd(A.Pw')
2. State   = 1 /\Rcv(xor(H(A'.Pw').R'.H(A'.X'.Y'.Z')).xor(H(R'.H(A'.X'.Y'.Z').H(Pw')))) =|>
   State' := 2 /\ C' := new() /\ W' := new() /\ Na' := new()
               /\ Snd(H(C'.W'.H(H(A).R.H(A.X.Y.Z).Na')))
3. State   = 2 /\ Rcv({Na.Nb'}_Kab1'.Nb') =|>
   State' := 3 /\ Kab1' := H(H(A).H(X.Y.Z).H(A.X.Y.Z).Na.Nb')
               /\ witness(A, B, server_user_n, Na.Nb')
               /\ witness(A, B, server_user_kab1, Kab1')
end role
```

```
role server (B, A : agent,Kab : symmetric_key,H: function,Snd, Rcv: channel(dy))
played_by B
def=
local
State : nat,
C, W, Z, Y, X, R, Pw, Na, Nb : text,
Kab1 : message
init  State := 0
transition
1. State   = 0 /\ Rcv(A'.Pw') =|>
   State' := 1 /\ X' := new() /\ Y' := new() /\ Z' := new() /\ R' := new()
               /\ Snd(xor(H(A'. Pw').R'.H(A'.X'.Y'.Z')).xor(H(R'.H(A'.X'.Y'.Z').H(Pw'))))
2. State   = 1 /\ Rcv(H(C'.W'.H(H(A).R.H(A.X.Y.Z).Na'))) =|>
   State' := 2 /\ Nb' := new() /\ Kab1' := H(H(A).H(X.Y.Z).H(A.X.Y.Z).Na.Nb')
               /\ Snd({Na.Nb'}_Kab1'.Nb')
               /\ witness(B, A, server_user_n, Na.Nb')
               /\ witness(B, A, server_user_kab1, Kab1')
               /\ secret(Kab1', kab1, {A, B})
end role
```

We tested our protocol using OFMC and CL-ATSE models in order to verify that it achieves the

following goals:

```
goal
  secrecy_of kab1
  authentication_on server_user_kab1
  authentication_on server_user_n
end goal
```

As a result, the outputs returned a “SAFE” state under the OFMC model and “No Attack Found” under the CL-ATSE model.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\SPAN\testsuite\results\V4.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.03s
  visitedNodes: 16 nodes
  depth: 3 plies
```

```
----------------
  AtSe Summary
----------------
  Protocol file: C:\SPAN\testsuite\results\V4.if
  Attack found : NO

  Analysed   : 113 states
  Reachable  : 64 states
  Translation: 0.01 seconds
  Computation: 0.02 seconds
```

Security Comparison

We summarize the security and functionality of the proposed scheme, making comparison with related works in Table 2. It demonstrates that our scheme can achieve the essential security requirements mentioned in Section 1.

Table 2 demonstrates that users can choose and change their password whenever they want, in our proposed scheme, whereas the schemes proposed by Chang and Liao (1994), Hwang and Li (2000) and Ramasamy and Muniyandi (2009) do not provide this security requirement. Moreover, the schemes proposed by Chang and Liao (1994) and Hwang and Li (2000) do not provide mutual authentication and session key agreement, making their scheme unsecured for electronic services. The main advantage of the proposed scheme is based on the concept of dynamic identity introduced by Das et al. (2004), where the user does not send its ID, in clear,

over an open network.

Table 2. Comparison with related works

Security requirement	Chang and Liao, 1994	Hwang and Li, 2000	Yoon, Ryu and Yoo, 2004	Ramasamy and Muni-yandi, 2009	Our scheme
No verification table	Yes	Yes	Yes	Yes	Yes
User chooses and changes her password freely	No	No	Yes	No	Yes
Mutual authentication	No	No	Yes	Yes	Yes
Session key agreement	No	No	Yes	No	Yes
User's anonymity	No	No	No	No	Yes
No time-synchronization	No	No	Yes	No	Yes

Source: Own elaboration

Conclusions

In this paper, we proposed a secure remote user authentication scheme based on ElGamal Public Key Cryptosystem, one-way hash function and nonce. Security analysis proved that our scheme prevents very well-known attacks and maintains the user's anonymity. Moreover, we have carried out formal security analysis of our protocol using the popular automated tool AVISPA. The formal security analysis proved that our protocol is safe. Furthermore, security comparison between our protocol and previous works showed that our scheme is more secure, making it feasible for electronic services.

References

Armando, A., Basin, D., Boichut, Y., *et al*. (2005). The AVISPA tool for the automated validation of Internete security protocols and applications, Lecture Notes in Computer Science, Berlin.

Awasthi, A.-K. and Lal, S. (2005). A new remote user authentication scheme using smart cards with check digits, *CoRR*, vol. abs/cs/0504094.

Chan, C.-K. and Cheng, L.-M. (2000). Cryptanalysis of a remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, 46(4): 992-993.

Chang, C.-C. and Hwang, K.-F. (2003). Some forgery attacks on a remote user authentication scheme using smart cards, *Informatica*, 14(3): 289-294.

Chang, C.-C. and Liao, W.-Y. (1994). A remote password authentication scheme based upong ElGamal's signature scheme, *Computers & Security*, 13(2): 137-144.

Chang, C.-C. and Wu, T.-C. (1991). Remote password authentication with smart cards, *IEE Proceedings-E*, 138(3): 165-168.

Chevalier, Y., Compagna, L., Cuellar, J., *et al.* (2004), presented at Workshop on Specification and Automated Processing of Security Requirements, Linz, Austria.

Das, M.-L., Saxena, A., and Gulati, V.-P. (2004). A Dynamic ID-based remote user authentication scheme, *IEEE Transactions on Consumer Electronics*, 50(2): 629-631.

Dolev, D., and Yao, A. (1983). On the security of public key protocols, IEEE Transactions on Information Theory, 29(2): 198-208.

ElGamal, T. (1985). A public-key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, 31(4): 469-472.

Hölbl, M. and Welzer, T. (2009). Two improved two-party identity-based authenticated key agreement protocols, *Computer Standards & Interfaces*, 31(6): 1056-1060.

Hwang, M.-S. and Li, L.-H. (2000). A new remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, 46(1): 28-30.

Hwang, T., Chen, Y. and Laih, C.-S. (1990). Non-interactive password authentication without password tables, presented at IEEE Region 10 Conference on Computer and Communication System, Hong Kong.

Juang, W.-S. (2004). Efficient password authenticated key agreement using smart cards, *Computers & Security*, 23(2): 167-173.

Kumar, M. (2004). New remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, 50(2): 597-600.

Lamport, L. (1981). Password authentication with insecure communication, *Communications of the ACM*, 24(11): 770-772.

Lee, N.-Y. and Chiu, Y.-C. (2005). Improved remote authentication scheme with smart card, *Computer Standards & Interfaces*, 27(2): 177-180.

Lee, S.-W., Kim, H.-S., and Yoo, K. Y. (2005a). Efficient nonce-based remote user authentication scheme using smart cards, *Applied Mathematics and Computation*, 167(1): 355-361.

Lee, S.-W., Kim, H.-S., and Yoo, K.-Y. (2005b). Improvement of Chien et al.'s remote user authentication scheme using smart cards, *Computer Standards & Interfaces*, 27(2): 181-183.

Leung, K.-C., Cheng, L.-M., Fong, A.-S., and Chan, C.-K. (2003). Cryptanalysis of a modified remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, 49(4): 1243-1245.

Liaw, H.-T., Lin, J.-F., and Wu, W.-C. (2006). An efficient and complete remote user authentication scheme using smart cards, *Mathematical and Computer Modelling*, 44(1-2): 223–228.

Madhusudhan, R. and Mittal, R.-C. (2012). Dynamic ID-based remote user password authentication schemes using smart cards: A review, *Journal of Network and Computer Applications*, 35(4): 1235-1248.

Ramasamy, R. and Muniyandi, A.-P. (2009). New remote mutual authentication scheme using smart cards, *Transactions on Data Privacy*, 2(2): 141-152.

Rhee, H.-S., Kwon, J.-L., and Lee, D.-H. (2009). A remote user authentication scheme without using smart cards, *Computer Standards & Interfaces*, 31(1): 6-13.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes, presented at *CRYPTO 84*.

Shao, Z. (2004). Efficient deniable authentication protocol based on generalized ElGamal signature scheme, *Computer Standards & Interfaces*, 26(5): 449-454.

Shen, J.-J., Lin, C.-W., and Hwang, M.-S. (2003). A modified remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, 49(2): 414-416.

Tseng, Y.-M. (2007). An efficient two-party identity-based key exchange protocol, *Informatica*, 18(1): 125-136.

Wang, S.-J. and Chang, J.-F. (1996). Smart card based secure password authentication scheme, *Computer & Security*, 15(3): 231-237.

Yoon, E.-J., Ryu, E.-K., and Yoo, K.-Y. (2004). Efficient remote user authentication scheme based on Generalized ElGamal Signature Scheme, *IEEE Transactions on Consumer Electronics*, 50(2): 568-570.