International Journal of Innovative Computing, Information and Control
Volume **8**, Number **3(A)**, March **2012**

ICIC International ©2012 ISSN 1349-4198
pp. 1541–1555

PASSWORD-BASED AUTHENTICATED KEY EXCHANGE PROTOCOL WITHOUT TRUSTED THIRD PARTY FOR MULTI-SERVER ENVIRONMENTS

Chien-Lung Hsu[1,2], Tzong-Sun Wu[3] and Han-Yu Lin[3,*]

[1]Department of Information Management
Chang Gung University
No. 259, Wen-Hwa 1st Road, Kwei-Shan, Taoyuan 333, Taiwan
daniel.cl.hsu@gmail.com

[2]Taiwan Information Security Center at NTUST
No. 43, Sec. 4, Keelung Road, Taipei 106, Taiwan

[3]Department of Computer Science and Engineering
National Taiwan Ocean University
No. 2, Pei-Ning Road, Keelung 20224, Taiwan
ibox456@gmail.com
*Corresponding author: hanyu.cs94g@nctu.edu.tw

Received November 2010; revised April 2011

Abstract. *With the rapid development of Internet, lots of transactions are conducted on-line without interactions face to face. A critical issue is to keep these transactions secure and confidential. Since the Internet is a virtual and insecure world, it is rather important to authenticate each other for providing a secure environment. A password-based authenticated key exchange protocol not only allows a user to login remote servers with an easily rememberable password, but also achieves mutual authentication as well. A shared session key is then established for subsequent communication. However, if such protocols are applied in multi-server environments, the system is often vulnerable to password guessing attacks and impersonation attacks. Besides, each user has to remember multiple passwords due to the security concern. In this paper, we propose an efficient password-based authenticated key exchange protocol with smart cards for multi-server environments. The proposed protocol enables a user to utilize a single password for registration and requesting services of different remote servers. Each server is also unnecessary to maintain a verification table. Moreover, our protocol can dynamically add or remove servers without the assistance of registration center. Compared with previous works, ours not only has better efficiency, but also provides more capabilities.*

Keywords: Authentication, Key exchange, Password, Multi-server, Smart card

1. **Introduction.** In traditional password-based authentication protocols, a user first registers to remote servers and then becomes a legitimate member associated with an identifier (ID for short) and his corresponding password (PW for short). Remote servers also store the same information in the verification table. When a user requests services or resources of a remote server, he first enters his ID and PW and then sends the information to the remote server via network transmission. The remote server will check whether the received ID is identical to the one stored in the verification table, which is referred to as user identification. After that, the server verifies if the entered PW matches the correct one with respect to his ID in the verification table, which is referred to as authentication. As ID and PW are transmitted via network channels, such information is easily to be eavesdropped by any malicious adversary.

To deal with the above problem, in 1981, Lamport [1] proposed an authentication protocol based on one-way hash functions. In his protocol, remote servers store hashed passwords in the verification table such that any attacker having the knowledge of verification table cannot learn any legitimate user's password. In 1990, Shimizu [2] introduced the concept of dynamic password/one-time password. In his system, each user keeps his short password while remote servers store another authenticated one in the verification table. A user first employs his short password to generate the authenticated one and then logins remote servers. Nevertheless, these passwords all belong to weak passwords [3-6] which cannot resist off-line password guessing attacks. In 2000, Sandirigama et al. [7] addressed the notion of strong password-based authentication protocol. Since then, lots of related researches and improvements [8-14] have been proposed. Yet, these protocols require remote servers to maintain a verification table. In 2000, Sun et al. proposed a remote user authentication scheme without verification tables. However, their scheme cannot allow a user to freely choose his password.

With the development of Internet, a user might register to several remote servers for requesting different services. Accordingly, each user usually has to remember many identifiers and passwords, which is considered to be inconvenient for users. If a user only chooses one single password for registration in multiple remote servers, a malicious registration center (RC) of these servers can easily impersonate the legitimate user to login another remote server. To simultaneously obtain the user convenience and ensure the security of users' passwords, some researchers [15-18] proposed authentication protocols for multi-server environments. In these protocols, a user can employ one single password to login different remote servers.

In previous multi-server authentication protocols, a registration center (RC) must be trusted or else he can impersonate any legitimate user, since he knows shared private keys between users and remote servers. In addition, a remote server has to maintain a verification table and users cannot change their passwords at will. For guaranteeing the security and confidentiality of subsequent transmissions, a shared session key will be established after authentication processes are performed, which is referred to as a password-based authenticated key exchange protocol. In this paper, we propose an efficient and secure password-based authenticated key exchange protocol solving all above mentioned problems.

The rest of this paper is organized as follows: Section 2 briefly reviews related works; we introduce the proposed protocol in Section 3; some security analyses and comparisons are detailed in Section 4; finally, a conclusion is made in Section 5.

2. Review of Previous Works.

In this section, we briefly review Juang's [17], the Chang-Kuo [15] and the Hwang-Shiau [16] protocols for multi-server environments.

2.1. Juang's protocol.

Juang's protocol is divided into three phases: the user registration, the authenticated key exchange and the shared session key query phases. Some used notations are defined as Table 1. We describe each phase as follows:

User registration phase: In the user registration phase, each user U_i first registers to RC with his chosen password. Figure 1 depicts the process of user registration phase.

Authenticated key exchange phase: In the authenticated key exchange phase, U_i logins the remote server S_j to acquire provided services. Figure 2 depicts the process of authenticated key exchange phase.

Shared session key query phase: If a remote server chooses not to maintain a verification table, i.e., the server does not store a_{ij} in the user registration phase, it will ask

Table 1. Notations of Juang's protocol

Notation	Description
RC	Registration center (RC)
UID_i	User U_i' identity
SID_j	Remote server S_j' identity
$\oplus$	Exclusive OR (XOR) operation
$H(\cdot)$	Collision-resistant one-way hash function
PW_i	User U_i' password
X_j	Remote server S_j's secret
X	Registration center's secrect
k	Encryption/decryption key
$E_k(\cdot)/D_k(\cdot)$	Symmetric encryption/decryption with key k
$\|\|$	Concatenation

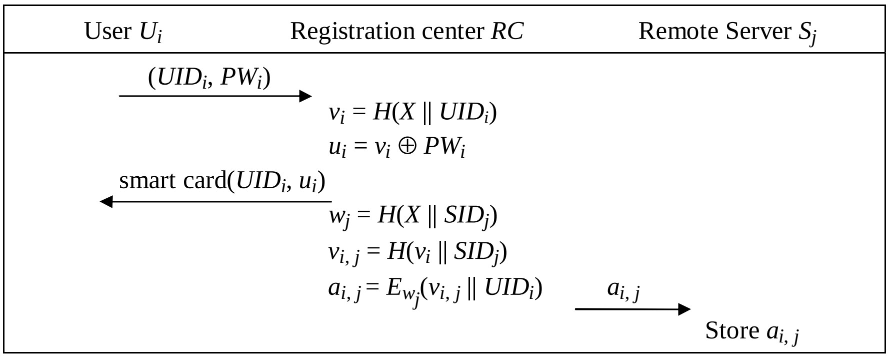

Figure 1. Diagram of the user registration phase in Juang's protocol

the assistance of RC to verify a shared session key. Figure 3 depicts the process of shared session key query phase.

2.2. **The Chang-Kuo protocol.** The Chang-Kuo protocol is divided into three phases: the user registration, the authenticated key exchange and the service update phases. Some used notations are defined as Table 2. We describe each phase as follows:

Table 2. Notations of the Chang-Kuo protocol

Notation	Description
RC	Registration center (RC)
UID_i	User U_i' identity
SID_j	Remote server S_j' identity
$\oplus$	Exclusive OR (XOR) operation
$H(\cdot)$	Collision-resistant one-way hash function
PW_i	User U_i' password
X_j	Remote server S_j's secret
X	Registration center's secrect
k	Encryption/decryption key
$E_k(\cdot)/D_k(\cdot)$	Symmetric encryption/decryption with key k
$\|\|$	Concatenation
a_{ij}	Access right of U_i in the remote server S_j

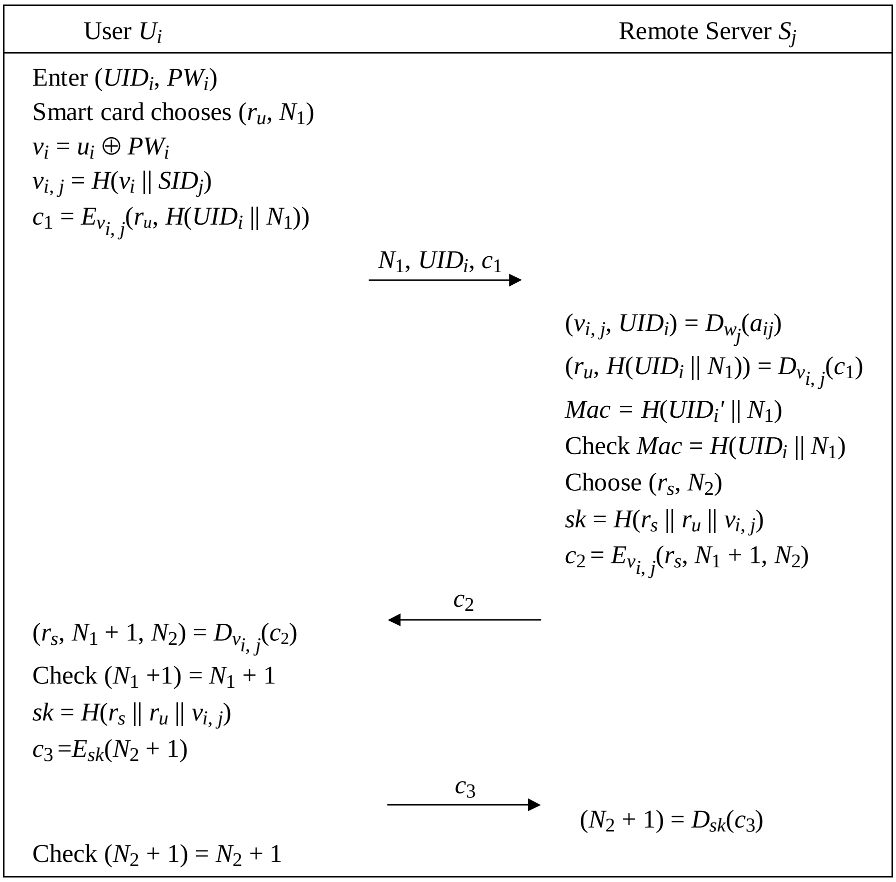

FIGURE 2. Diagram of the authenticated key exchange phase in Juang's protocol

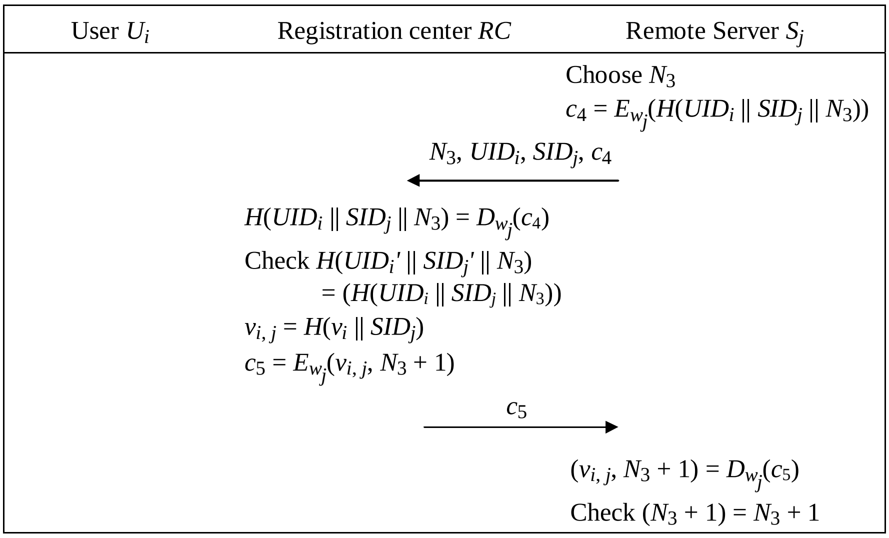

FIGURE 3. Diagram of the shared session key query phase in Juang's protocol

User registration phase: In the user registration phase, each user U_i first registers to RC with his chosen password. Figure 4 depicts the process of user registration phase.
Authenticated key exchange phase: In the authenticated key exchange phase, a user U_i logins the remote server S_j to acquire the access of provided services. Figure 5 depicts the process of authenticated key exchange phase.

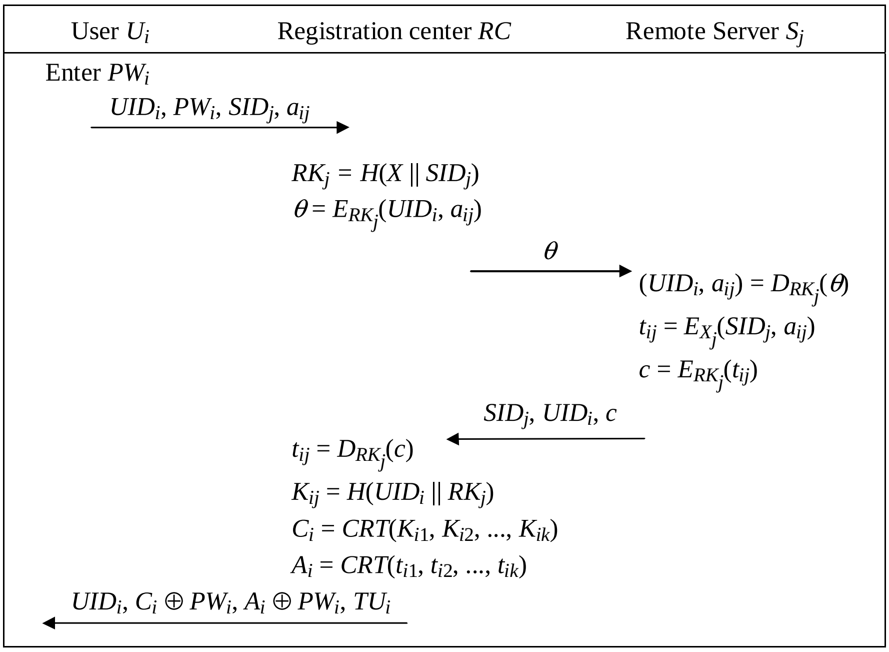

FIGURE 4. Diagram of the user registration phase in the Chang-Kuo protocol

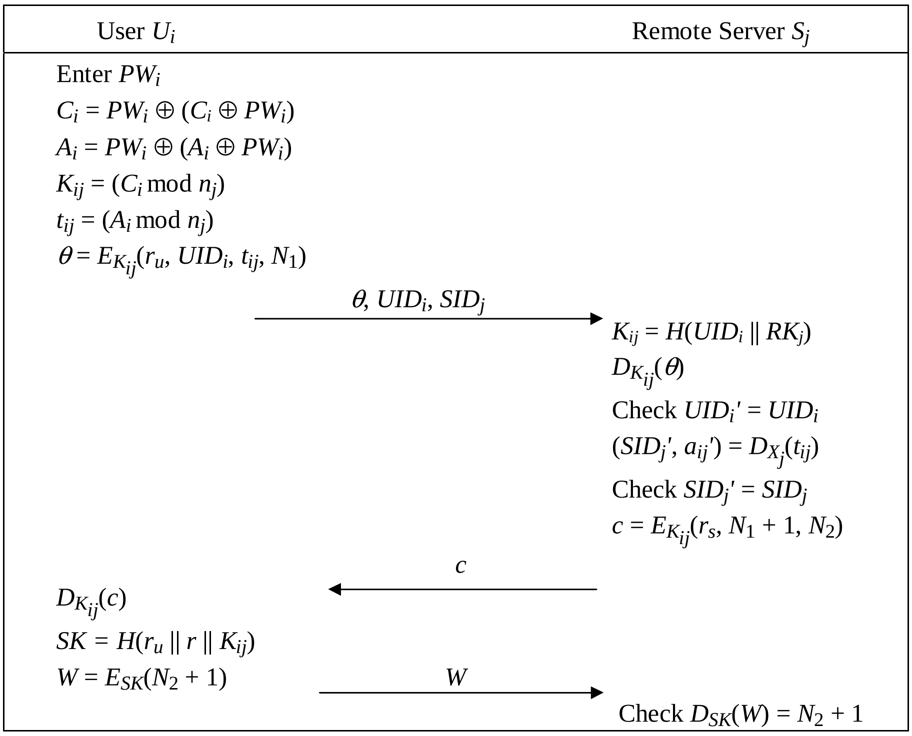

FIGURE 5. Diagram of the authenticated key exchange phase in the Chang-Kuo protocol

Service update phase: To update the services provided by a remote server, a user has to enter his password to obtain a new authentication value from a registration center. Figure 6 depicts the process of service update phase.

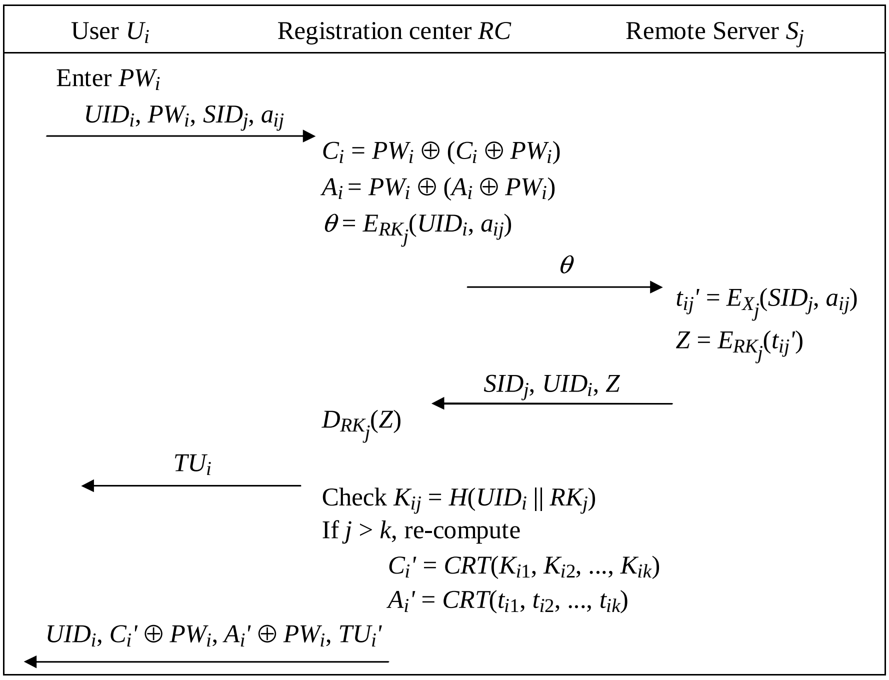

Figure 6. Diagram of the service update phase in the Chang-Kuo protocol

2.3. The Hwang-Shiau protocol.

The Hwang-Shiau protocol is divided into three phases: the user registration, the authenticated key exchange and the password changing phases. Some used notations are defined as Table 3. We describe each phase as follows:

Table 3. Notations of the Hwang-Shiau protocol

Notation	Description
RC	Registration center (RC)
ID_{U_i}	User U_i' identity
ID_{S_j}	Remote server S_j' identity
$\oplus$	Exclusive OR (XOR) operation
$H(\cdot)$	Collision-resistant one-way hash function
PW_i	User U_i' password
s	Registration center's secret
K_{M_j}	Private key between RC and S_j
$E_k(\cdot)/D_k(\cdot)$	Symmetric encryption/decryption with key k
$\|\|$	Concatenation
P	Large prime
T	Timestamp

User registration phase: In the user registration phase, each user U_i first registers to RC with his chosen password. Figure 7 depicts the process of user registration phase.

Authenticated key exchange phase: In the authenticated key exchange phase, a user U_i logins a remote server S_j to require the access of provided services. Figure 8 depicts the process of authenticated key exchange phase.

Password changing phase: To change the password, U_i and his smart card perform the steps of Figure 9.

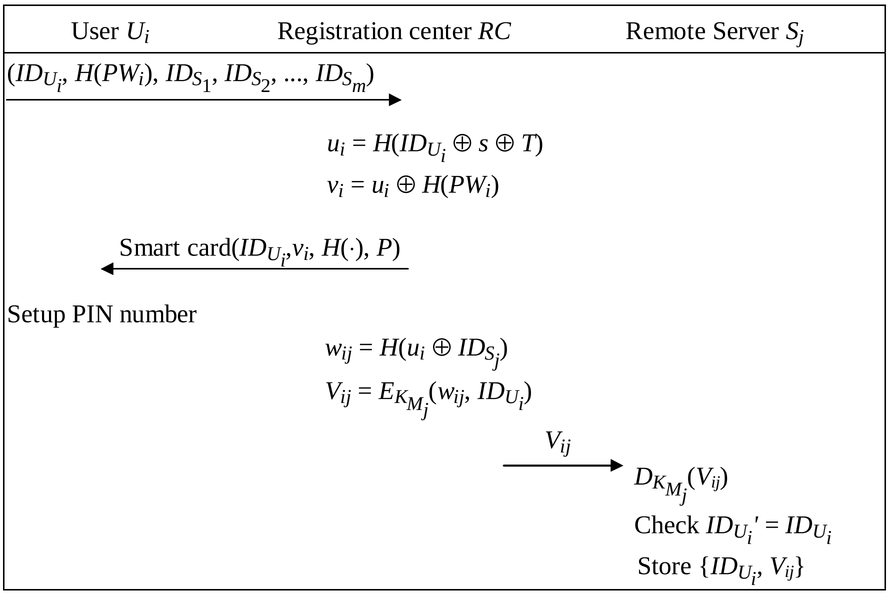

Figure 7. Diagram of the user registration phase in the Hwang-Shiau protocol

3. **The Proposed Protocol.**

The proposed protocol is divided into four phases: the system initialization, the user registration, the authenticated key exchange and the password changing phases. Some used notations in our protocol are defined as Table 4. We describe each phase as follows:

Table 4. Notations of the proposed protocol

Notation	Description
ID_{U_i}	User U_i' identity
ID_{S_j}	Remote server S_j' identity
$\oplus$	Exclusive OR (XOR) operation
$H(\cdot)$	Collision-resistant one-way hash function
PW_i	User U_i' password
X_j	Remote server S_j's secret
k	Encryption/decryption key
$E_k(\cdot)$	Symmetric encryption algorithm with key k
$D_k(\cdot)$	Symmetric decryption algorithm with key k
r	Random number
g, p, q	Parameters of Digital Signature Algorithm (DSA)
$\|\|$	Concatenation
T	Timestamp
USB	Portable USB device

System initialization phase: In this phase, each user first goes to the card center to obtain his smart card personally and then enters his identifier and password on the spot. Let remote servers generate the following parameters according to the Digital Signature Algorithm (DSA):

p, q: two large primes satisfying that $q \mid (p-1)$;

g: a generator of order q over GF(p).

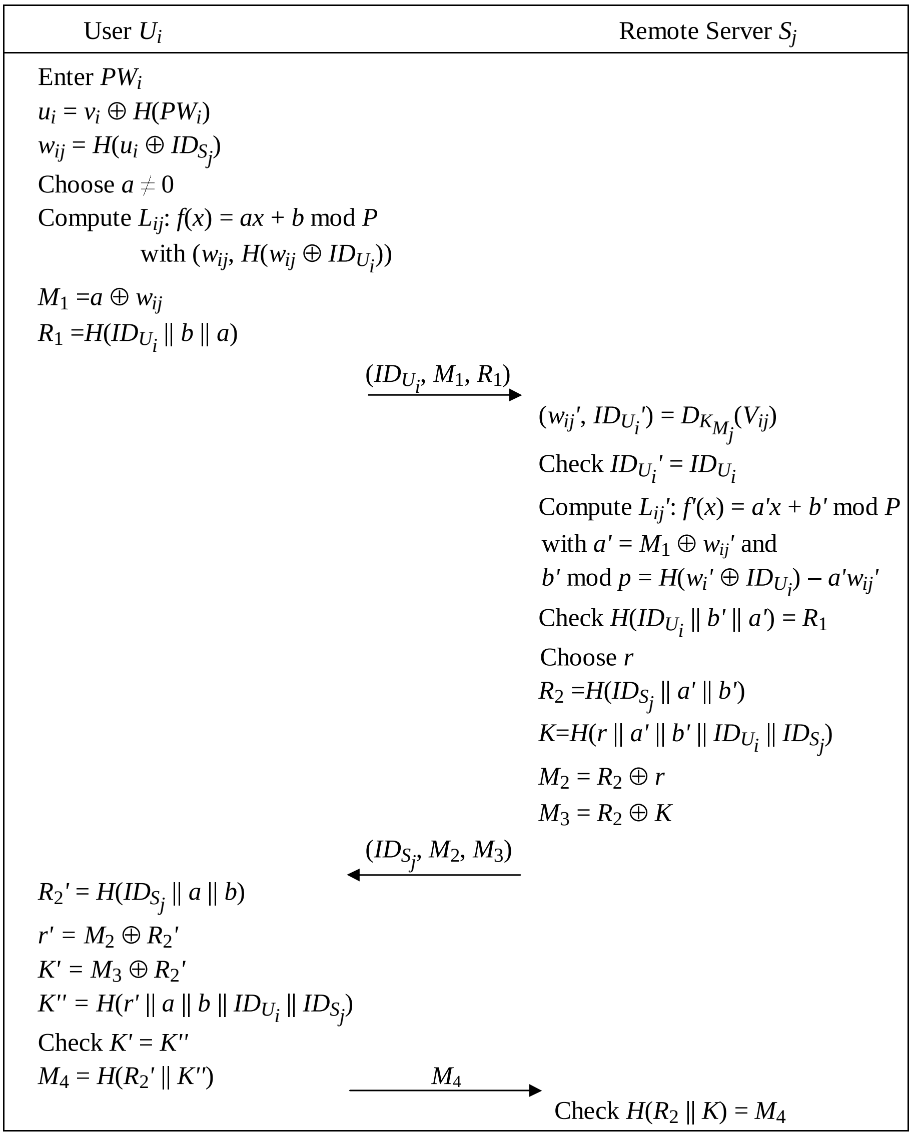

Figure 8. Diagram of the authenticated key exchange phase in the Hwang-Shiau protocol

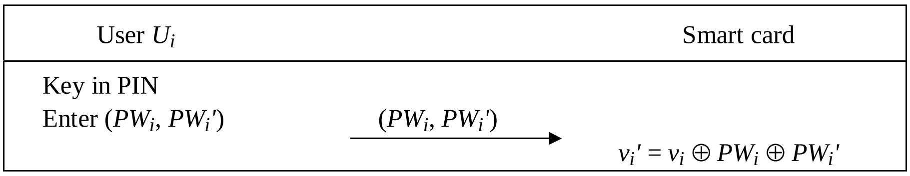

Figure 9. Diagram of the password changing phase in the Hwang-Shiau protocol

User registration phase: Figure 10 depicts how the user registration phase works. To become a legitimate member, each user U_i and a remote server S_j perform the following steps to complete the registration process:

Step 1 U_i enters his ID_{U_i} and PW_i.

Step 2 The smart card chooses a random number r to compute

$$A = H(PW_i) \oplus H\left(r \| ID_{S_j}\right), \tag{1}$$

and sends (ID_{U_i}, A) to the remote server S_j.

Step 3 After receiving (ID_{U_i}, A), the server S_j computes

$$u_i = H(ID_{U_i} \| X_j), \tag{2}$$
$$B = u_i \oplus A, \tag{3}$$

and then returns B to U_i.

Step 4 Upon receiving B, the smart card stores it along with r in the USB device.

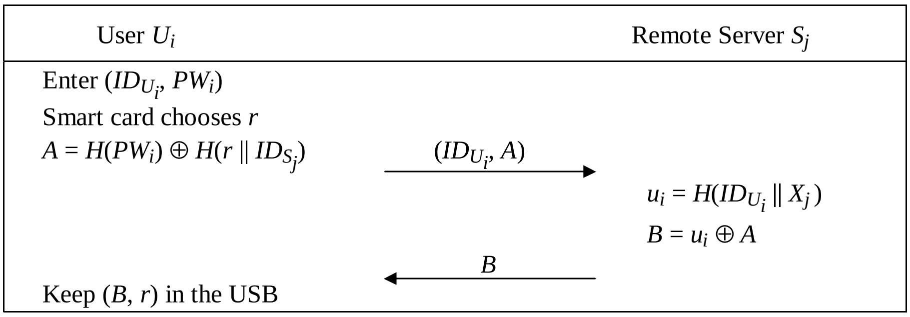

FIGURE 10. Diagram of the user registration phase in the proposed protocol

Authenticated key exchange phase: Figure 11 is the diagram of the authenticated key exchange phase. To achieve mutual authentication and obtain the server's services, a user U_i and a remote server S_j perform the following steps:

Step 1 U_i enters his ID_{U_i} and PW_i.

Step 2 The smart card first utilizes r to compute $A = H(PW_i) \oplus H(r \| ID_{S_j})$ and then retrieves B stored in the USB to recover

$$u_i = A \oplus B. \tag{4}$$

Step 3 The smart card and S_j separately compute

$$V_A = g^{u_i} \bmod p. \tag{5}$$

Step 4 The smart card chooses $a \in_R Z_p^*$ to compute

$$R_A = g^a \bmod p, \tag{6}$$
$$M_1 = (R_A \| ID_{U_i}), \tag{7}$$
$$X_A = (R_A \| H(M_1 \| T)) \oplus V_A, \tag{8}$$

and sends (ID_{U_i}, X_A) to the remote server S_j.

Step 5 After receiving (ID_{U_i}, X_A), the server S_j computes

$$R_A \,\|\, H(M_1 \| T) = X_A \oplus V_A, \tag{9}$$
$$M_1' = (R_A \| ID_{U_i}), \tag{10}$$
$$MAC = R_A \| H(M_1' \| T), \tag{11}$$

and then verifies if

$$MAC = R_A \| H(M_1 \| T). \tag{12}$$

If it holds, the server S_j authenticates the user U_i.

Step 6 For establishing a shared session key, the server S_j chooses $b \in_R Z_p^*$ to compute

$$V_B = g^b \bmod p, \tag{13}$$
$$K = (R_A)^b \bmod p, \tag{14}$$
$$\beta = H(K \| ID_{U_i} \| ID_{S_j}), \tag{15}$$
$$\theta = E_{R_A}(V_B, \beta), \tag{16}$$

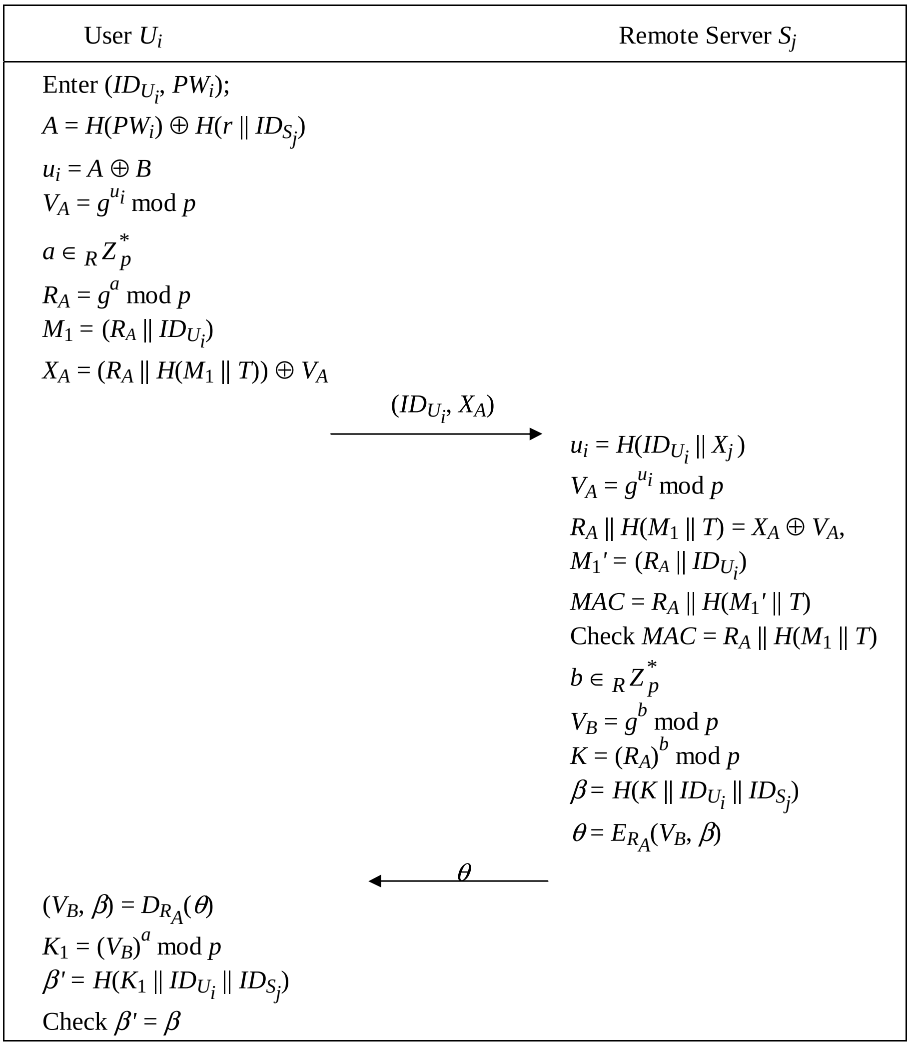

FIGURE 11. Diagram of the authenticated key exchange phase in the proposed protocol

and sends θ to the smart card.

Step 7 Upon receiving θ, the smart card computes

$$(V_B, \beta) = D_{R_A}(\theta), \tag{17}$$

$$K_1 = (V_B)^a \bmod p, \tag{18}$$

$$\beta' = H(K_1 \| ID_{U_i} \| ID_{S_j}), \tag{19}$$

and checks whether $\beta' = \beta$. If it holds, the mutually shared session key is correct.

Password changing phase: Figure 12 is the diagram of password changing phase. To complete the password changing process, U_i and the smart card cooperatively perform the following steps:

Step 1 U_i first enters the PIN number to start the smart card and then inputs his old PW_i and new PW_i'.

Step 2 The smart card updates

$$A' = H(PW_i) \oplus H(r \parallel ID_{S_j}), \tag{20}$$

and stores it.

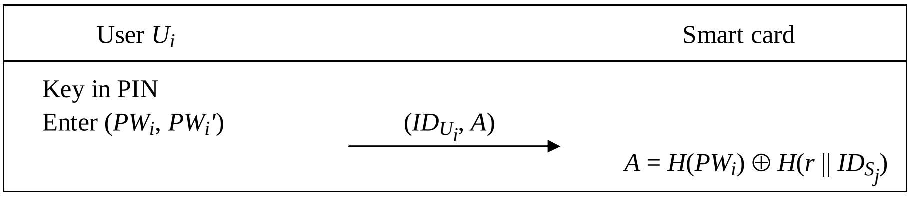

FIGURE 12. Diagram of the password changing phase in the proposed protocol

4. **Security Analyses and Comparisons.** In this section, we first analyze the security of our proposed protocol and then make a comparison with some previous works.

4.1. **Scurity analyses.** Generally speaking, an authenticated key exchange protocol achieving mutual authentication should satisfy the following three security requirements:

(a) ***Confidentiality***: Given the public information such as public keys and a message authentication code, it is computationally infeasible for any malicious adversary to derive related secret information including private keys of users/remote servers and mutually shared session keys.
(b) ***Authenticity***: A user and a remote server can authenticate each other. Besides, they cannot deny having generated session keys or encrypted messages.
(c) ***Unforgeability***: Any malicious adversary cannot forge valid information or impersonate legitimate users/remote servers to successfully complete the authenticated key exchange process with another legitimate party.

We give detailed security analyses with respect to the above three requirements as follows:

Confidentiality

(a) ***The confidentiality of user's transmission***: Consider the case that an attacker attempts to derive a user's secret information V_A from some eavesdropped messages. From the authenticated key exchange process, we know that the attacker will not make it unless he knows u_i. However, based on the discrete logarithm problem (DLP) [3,19,20], the attacker cannot obtain u_i from $V_A = g^{u_i} \bmod p$. Consequently, any malicious attacker cannot acquire a user's private information.
(b) ***The confidentiality of remote server's transmission***: To derive a shared session key K from intercepted (ID_{U_i}, X_A), an attacker has to recover R_A first. However, without the knowledge of V_A, the attacker cannot succeed in obtaining R_A. In addition, if the attacker tries to derive the secret u_i stored in the remote server, he will face the difficulty of DLP and fail. Hence, the confidentiality of remote server's transmission is ensured.

Authenticity

When acquiring services of remote servers, a user has to employ a shared session key to encrypt transmitted messages. It is computationally infeasible for any malicious attacker to intercept or replace the session key, since all transmitted messages are properly encrypted. Without the knowledge of user's password, the attacker cannot decrypt the eavesdropped messages. Moreover, a remote server will quickly detect illegal users when receiving unknown keys. Similarly, as a mutually shared session key is computed by a user and a remote server cooperatively, only the real user who owns the corresponding secret can derive it. Therefore, any attacker trying to cheat a remote server will be detected. The authenticity of the proposed protocol is satisfied.

Unforgeability

Consider the case that an attacker attempts to forge valid messages to impersonate a legitimate user for requesting a remote server's services without knowing the user's password. According to the equality, $X_A = (R_A \parallel H(M_1 \parallel T)) \oplus V_A$, the attacker will face the difficulty of DLP and fail to transmit valid (ID_{U_i}, X_A) to the remote server.

We further consider the following existential attacks against our proposed protocol:

(a) ***Password guessing attack***: To guess a user's password from some intercepted messages (ID_{U_i}, A), an attacker has to know the random number r stored in the smart card first. Even the attacker can successfully obtain the secret value r, he still faces the difficulty of one-way hash function (OHF) [3,19] and cannot make it.

(b) ***Impersonation attack***: To impersonate a legitimate user for requesting a remote server's service, an attacker has to transmit valid X_A passing the verification of remote server. However, without the user's password, he cannot compute valid X_A. The remote server will quickly terminate the authenticated key exchange process.

(c) ***Man-in-the-middle-attack***: It can be seen that in our proposed protocol, the message (V_B, β) is encrypted with a symmetric encryption algorithm under the key R_A and then sent to the user. Without the knowledge of the shared key R_A, any attacker cannot decrypt the ciphertext and obtain the transmitted messages.

(d) ***Forward secrecy***: Even an attacker successfully obtain a mutually shared session key between a user and a remote server, he cannot learn any information about the user's password or shared secret between the remote server. Consequently, the confidentiality of previous transmission is still fulfilled.

(e) ***Replay attack***: In the authenticated key exchange phase, a timestamp T is used to verify the login time of a smart card, so as to prevent any attacker from plotting replay attacks.

(f) ***Smart card loss attack***: The smart card only stores a random number r. In case the smart card is lost, anyone picking up this card cannot impersonate the legitimate user without knowing his corresponding password.

We summarize the security analyses and the capabilities of our proposed and other related protocols including Juang's (Jua for short) [17], the Chang-Kuo (CK for short) [15] and the Hwang-Shiau (HS for short) [16] ones as Table 5.

Table 5. Summarization of the proposed and related protocols in terms of the security and capabilities

Item	Jua [17]	CK [15]	HS [16]	Ours
Secure against password guessing attack	Yes	Yes	Yes	Yes
Secure against impersonation attack	Yes	Yes	Yes	Yes
Secure against man-in-the-middle-attack	Yes*	Yes*	Yes*	Yes
Forward secrecy	Yes	Yes	Yes	Yes
Secure against replay attack	Yes	Yes	Yes	Yes
Secure against smart loss attack	Yes	Yes	Yes	Yes
Changeable password	Yes	Yes	Yes	Yes
Mutual authentication	Yes	Yes	Yes	Yes
Explicit key validation	N.A.	N.A.	Yes	Yes
Without registration center (RC)	N.A.	N.A.	N.A.	Yes
Without verification table	N.A.	N.A.	N.A.	Yes
Dynamically add or remove servers	N.A.	N.A.	N.A.	Yes

Remark *: It should be assumed that the registration center (RC) is trusted.

4.2. **Comparisons.** In this subsection, we evaluate the computational costs and the communicational overheads of our proposed protocol. For facilitating the following comparisons, some used notations are defined below:

$|x|$: the bit-length of a parameter x;
T_H: the time for performing a one-way hash function;
T_{EK}: the time for performing a symmetric encryption/decryption algorithm;
T_{CRT}: the time for performing the Chinese reminder theorem.

Table 6. Comparisons of computational costs among the proposed and previous protocols

Item		User registration	Authenticated key exchange
Jua [17]	User	N.A.	$2T_H + 3T_{EK}$
	Registration center	$2T_H + T_{EK}$	N.A.
	Remote server	N.A.	$2T_H + 3T_{EK}$
	Total	$6T_H + 7T_{EK}$	
CK [15]	User	N.A.	$T_H + 2T_{EK}$
	Registration center	$2T_H + T_{EK} + T_{CRT}$	N.A.
	Remote server	T_{EK}	$T_H + T_{EK}$
	Total	$4T_H + 5T_{EK} + T_{CRT}$	
HS [16]	User	T_H	$6T_H$
	Registration center	$3T_H + T_{EK}$	N.A.
	Remote server	T_{EK}	$3T_H + T_{EK}$
	Total	$13T_H + 3T_{EK}$	
Ours	User	$2T_H$	$2T_H + T_{EK}$
	Remote server	T_H	$2T_H + T_{EK}$
	Total	$7T_H + 2T_{EK}$	

Table 7. Comparisons of communicational overheads among the proposed and previous protocols

Item		User registration	Authenticated key exchange
Jua [17]	User	$\|ID\| + \|PW\|$	$\|N\| + \|ID\| + 2\|K\| + \|H\|$
	Registration center	$\|K\|$	N.A.
	Remote server	N.A.	$\|K\|$
	Total	$\|N\| + 2\|ID\| + 4\|K\| + \|H\| + \|PW\|$	
CK [15]	User	$2\|ID\| + \|PW\| + \|a\|$	$2\|ID\| + 2\|K\|$
	Registration center	$\|K\| + \|ID\| + 2\|PW\|$	N.A.
	Remote server	$2\|ID\| + \|K\|$	$\|K\|$
	Total	$\|a\| + 7\|ID\| + 5\|K\| + 3\|PW\|$	
HS [16]	User	$2\|ID\| + \|H\|$	$3\|H\| + \|ID\|$
	Registration center	$\|N\| + \|ID\| + 2\|K\| + \|H\|$	N.A.
	Remote server	N.A.	$\|ID\| + 2\|H\|$
	Total	$\|N\| + 5\|ID\| + 2\|K\| + 7\|H\|$	
Ours	User	$\|ID\| + 2\|H\|$	$\|ID\| + \|H\|$
	Remote server	$\|H\|$	$\|K\|$
	Total	$2\|ID\| + \|K\| + 4\|H\|$	

We demonstrate the detailed comparisons with previous works [15-17] in terms of computational costs and communicational overheads as Tables 6 and 7, respectively. As shown in Table 6, the computational costs of authenticated key exchange phase in our protocol are the lowest compared with the other three. Likewise, the communicational overheads of authenticated key exchange phase in our protocol are also the lowest among all compared ones.

5. **Conclusions.** To provide users with more convenience, in this paper, we have proposed an efficient password-based authenticated key exchange protocol for multi-server environments. In our proposed protocol, each user can utilize one single password to register and login different servers and change his password at will. At the same time, the remote server does not have to maintain a verification table. Besides, it does not need the assistance of registration center to dynamically add or remove servers. We also analyzed that the proposed protocol is secure against known existential active attacks. Compared with previous related works, ours not only has lower computational costs and communicational overheads, but also provides better capabilities. Therefore, the proposed protocol can benefit the practical implementation.

Acknowledgement. We would like to thank anonymous referees for their valuable suggestions. We thank Healthy Aging Research Center (HARC) of Chang Gung University for excellent technical assistance. This work was supported in part by the Chang Gung Memorial Hospital Grant CMRPD390032 and in part by National Science Council under the grant NSC 100-2628-H-182-001-MY3.

REFERENCES

[1] L. Lamport, Password authentication with insecure communication, *Communications of the ACM*, vol.24, no.11, pp.770-772, 1981.
[2] A. Shimizu, A dynamic password authentication method by one-way function, *IEICE Transactions on Communications*, vol.J73-D-I, no.7, pp.630-636, 1990.
[3] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 4th Edition, Pearson, 2005.
[4] K. Tan and H. Zhu, Remote user authentication scheme using smart cards, *Computer Communications*, vol.46, no.4, pp.390-393, 1999.
[5] S. J. Wang and J. F. Chang, Smart card based secure password authentication scheme, *Computers and Security*, vol.15, no.3, pp.231-237, 1996.
[6] W.-H. Yang and S.-P. Shieh, Password authentication schemes with smart cards, *Computers and Security*, vol.18, no.8, pp.727-733, 1999.
[7] M. Sandirigama, A. Shimizu and M. Noda, Simple and secure password authentication protocol (SAS), *IEICE Transactions on Communications*, vol.E83-B, no.6, pp.1363-1365, 2000.
[8] C.-M. Chen and W.-C. Ku, Stolen-verifier attack on two new strong-password authentication protocols, *IEICE Transactions on Communications*, vol.E85-B, no.11, pp.2519-2521, 2004.
[9] T.-H. Chen, An authentication protocol with billing non-repudiation to personal communication systems, *International Journal of Innovative Computing, Information and Control*, vol.5, no.9, pp.2657-2664, 2009.
[10] W.-C. Ku, H.-C. Tsai and S.-M. Chen, Two simple attack on Lin-Shen-Hwang's strong-password authentication protocol, *ACM Operating Systems Review*, vol.37, no.4, pp.26-31, 2003.
[11] C.-W. Lin, J.-J. Shen and M.-S. Hwang, Security enhancement for optimal strong-password authentication protocol, *ACM Operating Systems Review*, vol.37, no.2, pp.7-12, 2003.
[12] W.-G. Shieh and W.-B. Horng, Security analysis and improvement of the remote user authentication scheme without using smart cards, *ICIC Express Letters*, vol.4, no.6(B), pp.2431-2436, 2010.
[13] T. Tsuji, T. Kamioka and A. Shimizu, Simple and secure password authentication protocol. Ver.2. (SAS-2), *IEICE Technical Report*, vol.102, no.314, pp.7-11, 2002.
[14] T. Tsuji and A. Shimizu, An impersonation attack on one-time password authentication protocol OSPA, *IEICE Transactions on Communications*, vol.E86-B, no.7, pp.2182-2185, 2003.
[15] C.-C. Chang and J.-Y. Kuo, An efficient multi-server password authenticated key agreement scheme using smart cards with access control, *IEEE International Conference on Advanced Information Networking and Applications*, vol.2, no.56, pp.257-260, 2005.

[16] R.-J. Hwang and S.-H. Shiau, Provably efficient authenticated key agreement protocol for multi-servers, *The Computer Journal*, vol.50, no.5, pp.602-615, 2007.

[17] 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.

[18] J.-S. Lee, Y.-F. Chang and C.-C. Chang, A novel authentication protocol for multi-server architecture without smart cards, *International Journal of Innovative Computing, Information and Control*, vol.4, no.6, pp.1357-1364, 2008.

[19] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, Springer, 2002.

[20] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, vol.22, no.6, pp.644-654, 1976.