An Entire Chaos-Based Biometric Remote User Authentication Scheme on Tokens Without Using Password

Eun-Jun YOON[1], Kee-Young YOO[2]

[1]*School of Electrical Engineering and Computer Science, Graduate School*
Kyungpook National University, 1370 Sankyuk-dong, Buk-gu, Daegu 702-701, Republic of Korea
e-mail: ejyoon@knu.ac.kr

[2]*School of Computer Science and Engineering, College of IT Engineering*
Kyungpook National University, 1370 Sankyuk-dong, Buk-gu, Daegu 702-701, Republic of Korea
e-mail: yook@knu.ac.kr

Received: October 2009; accepted: April 2010

Abstract. This paper presents an entire chaos-based biometric remote user authentication scheme on tokens without using passwords. The proposed scheme is based on the chaotic hash function and chaotic pseudo-random number generator to provide secure mutual authentication over an insecure channel between the user and remote server. Compared with the related biometric authentication schemes, the proposed scheme does not require the user password to provide convenience to users. It also does not require time synchronization or delay-time limitations between the user and remote server to resolve time synchronization problems.

Keywords: chaos theory, cryptography, biometric, authentication, security, protocol.

1. Introduction

A remote user authentication scheme (Lin *et al.*, 2003; Yoon *et al.*, 2005a, 2005b, 2007; Chen *et al.*, 2007, 2008; Khan *et al.*, 2008; Tseng *et al.*, 2008; Yoon and Yoo, 2009; Popescu *et al.*; Li *et al.*) mainly employs the possession of a token (smart cards, cell phones, personal digital assistant (PDA), and notebook computers, etc.) and/or the knowledge of a secret (password, etc.) in order to establish the identity of an individual. However, a token can be lost, stolen, misplaced, or willingly given to an unauthorized user; and a secret can be forgotten, guessed, and willingly or unwillingly be disclosed to an unauthorized user (Hsieh *et al.*, 2003; Chang *et al.*, 2003, 2005; Ku *et al.*, 2005; Yoon *et al.*, 2005c). Therefore, biometric techniques have emerged as a powerful tool for remote user authentication to resolve these problems. Since it is based on the physiological and behavioral characteristics of an individual, biometrics does not suffer from disadvantages found in traditional authentication methods (Yoon and Yoo, 2007; Khan *et al.*, 2008; Li *et al.*, 2010; Rila *et al.*, 2003). Also, biometrics and tokens have the potential to be a very useful combination. First, the security and convenience of biometrics allow for the implementation of high-security applications regarding tokens. Second, tokens represent a secure and portable way of storing biometric templates, which would otherwise need to be stored in a central database.

Chaos (Dachselt *et al.*, 2001; Kocarev *et al.*, 2001) is a universal, random-like and robust phenomenon in nonlinear systems. Chaotic systems are characterized by sensitive dependence on initial conditions and similarity to random behavior. They have been used to design and analyze secure communication systems. Hash function and pseudo-random number sequences are especially useful in many applications including user authentication, watermarking for image authentication and cryptography. For cryptographic applications, several algorithms such as MD5 and SHA-1 for hash functions, and ANSI X9.17 and FIPS 186 for pseudo-random number generation are found to be popular (Menezes *et al.*, 1997). In recent times, several researchers have been exploring the idea of using chaotic dynamical systems for these purpose (Xiao *et al.*, 2005; Sun *et al.*, 2009) because of the random-like, unpredictable dynamics of chaotic systems.

In this paper, we present an entire chaos-based biometric remote user authentication scheme on tokens without using password. The proposed scheme is based on the chaotic hash function (Xiao *et al.*, 2005) and chaotic pseudo-random number generator (Sun *et al.*, 2009) to provide secure mutual authentication over an insecure channel between user and remote server. In the proposed scheme, the user does not need to use his/her password to register and login in the remote server. This can give the user convenience. Moreover, the proposed scheme does not require time synchronization or delay-time limitations between the user and remote server in comparison with the related schemes. To resolve the time synchronization problem, the proposed scheme adopts nonce-based authentication method. As a result, the proposed scheme has several important features (Li *et al.*, 2010) as following: (1) it is designed to reduce the computation cost of each participant; (2) it achieves cryptographic goals using only bit-wise exclusive-OR (XOR) operations and collision-free chaotic one-way hash functions as the main cryptographic operations without additional requirements such as using the server's public key, digital signatures (Gao *et al.*, 2009; Wang *et al.*, 2009; Liu *et al.*, 2010; Sun *et al.*, 2010), and so on; (3) it not only is secure against well-known cryptographical attacks such as guessing attacks, replay attacks, stolen token attacks, insider attacks but also provides secure mutual authentication and session key agreement; (4) it provides functionality requirements for biometric and token-based authentication such as non-repudiation, without synchronized clocks, without storing password tables in the server. Thus, the proposed scheme is very useful in limited computation and communication resource environments to access remote information systems since it provides security, reliability, and efficiency.

This paper is organized as follows. Section 2 briefly reviews about chaotic map based hash function and chaotic map based pseudo-random sequence generation. Our proposed scheme is presented in Section 3, while Section 4 discusses the security and efficiency of the proposed scheme. Our conclusions are presented in Section 5.

2. Related Works

This section briefly reviews about chaotic map based hash function (Xiao *et al.*, 2005) and chaotic map based pseudo-random sequence generation (Sun *et al.*, 2009).

2.1. *Chaotic Map Based Hash Function*

The proposed scheme is based on the following chaotic one-way hash function (Xiao *et al.*, 2005). One dimension piecewise linear chaotic system is defined as

$$\begin{aligned} X(t+1) &= F_P(X(t)) \\ &= \begin{cases} X(t)/P, & \text{if } 0 \leqslant X(t) < P, \\ (X(t)-P)/(0.5P), & \text{if } P \leqslant X(t) < 0.5, \\ (1-X(t)-P)/(0.5-P), & \text{if } 0.5 \leqslant X(t) < 1-P, \\ (1-X(t))/P, & \text{if } 1-P \leqslant X(t) \leqslant 1, \end{cases} \end{aligned} \tag{1}$$

where $X \in [0,1],\ P \in (0,0.5)$. Let $X_i (0 \leqslant i \leqslant 3N)$ be the *chaining variable*. At the start of the hashing, the chaining variable has an *initial value* X_0 that is specified as part of the hash algorithm, where X_0 is chosen from $(0,1)$. H_0 is the *encryption key* for the pending message M. Given a pending message M, H_0 is a constant which is chosen from $(0,1)$. The 3-unit iterations, 1st to Nth, $(N+1)$th to $2N$th, $(2N+1)$th to $3N$th, ensure that each bit of the final hash value will be related to all bits of messages. The following brief refers to how to generate the hash value:

(1) translates the pending message to the corresponding ASCII numbers, then maps these ASCII numbers by means of linear transform into an array C, whose elements are numbers in $[0,1]$ and whose length N is the number of characters in the message;

(2) iterates the follows processes:
1st: $P_1 = (C_1 + H_0)/4 \in [0.05), X_1 = F_{P_1}(X_0) \in [0,1]$;
2nd to Nth: $P_i = (C_i + X_{i-1})/4 \in [0.05), X_i = F_{P_i}(X_{i-1}) \in [0,1]$;
$(N+1)$th: $P_{N+1} = (C_N + X_N)/4 \in [0.05), X_{N+1} = F_{P_{N+1}}(X_N) \in [0,1]$;
$(N+2)$th to $2N$th: $P_i = (C_{2N-i+1} + X_{i-1})/4 \in [0.05), X_i = F_{P_i}(X_{i-1}) \in [0,1]$;
$(2N+1)$th: $P_{2N+1} = (C_1 + H_0)/4 \in [0.05), X_{2N+1} = F_{P_{2N+1}}(X_{2N}) \in [0,1]$;
$(2N+2)$th to $3N$th: $P_i = (C_{i-2N} + X_{i-1})/4 \in [0.05), X_i = F_{P_i}(X_{i-1}) \in [0,1]$;

(3) transforms X_N, X_{2N}, X_{3N} to the corresponding binary format, extracts 40, 40, 48 bits after the decimal point, respectively, and juxtaposes them from left to right to get a 128-bit final hash value.

2.2. *Chaotic Map-Based Pseudo-Random Sequence Generation*

The following spatially generalized 2D logistic systems can be used in the proposed scheme to generate a pseudo-random binary sequence (Sun *et al.*, 2009):

$$x_{m+1,n} + \omega x_{m,n+1} = 1 - \big(\mu(1+\omega)x_{m,n}\big)^2. \tag{2}$$

Here, $x_{m,n}$ is the spatial state of the system, ω is a real constant and μ is a positive parameter. Research shows that when $2 > \mu \geqslant 1.55$ and $\omega(-1,1)$, the system is in chaotic state.

Generating a pseudo-random binary sequence from the orbit of a chaotic map essentially requires mapping the state of the system to $\{0,1\}$. A simple way to generate a bit sequence from a chaotic real valued signal is as follows:

$$b_x = \begin{cases} 1, & \text{if } x_{m,n} > c, \\ 0, & \text{if } x_{m,n} < c. \end{cases} \tag{3}$$

Here, c is an appropriately chosen threshold value for state-variables $x_{m,n}$. The c chosen such that the likelihood of $x_{m,n} > c$ is equal to that of $x_{m,n} \leqslant c$.

In the proposed scheme, it takes and uses a 128-bit block or higher bit block length from the output bits of the pseudo-random sequence generation to compliance with FIPS 140-2 and NIST SP800-90 which satisfy cryptographically secure and security strength of n bits (Sun *et al.*, 2009; Jean *et al.*, 2007; Elaine *et al.*, 2007). That is, a 128-bit block or higher bit block length based pseudo-random number generator is cryptographically secure because there is no polynomial-time algorithm that on the first n output-sequences can predict the $n+1$th bit with probability greater than 0.5.

3. The Proposed Scheme

The proposed scheme is composed of two phases: registration and authentication. Some of the notations used in the proposed scheme are defined as follows:

- U, S: user (client) and remote server;
- ID: identifier of U;
- B: biometric template of U;
- X: strong secret key of S;
- $h(\cdot)$: collision resistant secure one-way chaotic hash function;
- $prng(\cdot)$: chaotic map based pseudo-random sequence generation function which can generate 128-bit or higher bit block length as AES or SHA-1 (Kazlauskas *et al.*, 2009);
- $\oplus$: bit-wise exclusive-OR (XOR) operation;
- r_u, r_s: fresh chaotic random nonces $\in prng(\cdot)$ chosen by U and S.

3.1. *Registration Phase*

Before a user logs into the remote server, the user needs to perform the following steps (see Fig. 1).

R.1 $U \rightarrow S$: $\{ID, h(ID, B), B \oplus N\}$.
User U freely chooses his/her identity ID and a random number $N \in prng(\cdot)$. U also imprints his/her personal biometric impression B at the sensor. U then interactively submits $\{ID, h(ID, B), B \oplus N\}$ to the server S. This private data must be sent in person or over a secure channel.

R.2 $S \rightarrow U$: {Token containing $(ID, w, B \oplus N, d(\cdot), \tau)$}.
S computes $v = h(ID, X)$ and $w = v \oplus h(ID, B)$, where X is a secret key of S. Then, S writes the secure information $\{ID, w, B \oplus N, d(\cdot), \tau\}$ to the memory of U's token and issues it to U through a secure channel, where $d(\cdot)$ is a symmetric parametric function and τ is a predetermined threshold for biometric verification (Lumini *et al.*, 2007; Tulyakov *et al.*, 2007; Kisel *et al.*, 2008; Ribaric *et al.*, 2008; Inuma *et al.*, 2009; Ziauddin *et al.*, 2010).

R.3 Upon receiving the token from S, U inputs the chosen random number N into the received token. Then, U's token extracts the biometric impression B by computing $(B \oplus N) \oplus N$ and then replaces the stored $B \oplus N$ with B.

3.2. *Authentication Phase*

In this phase, after getting the token from the server S, the user U can use it when he/she securely communicates with S (see Fig. 2).

A.1 $U \rightarrow S$: ID, M_1. If U wants to negotiate a session key with S, he/she opens the login application software into his/her token, and imprints biometric B^* at the sensor. Then, a biometric verification process of U's token compares the imprinted biometric value B^* with the stored biometric value B. If $d(B^*, B) < \tau$, then it

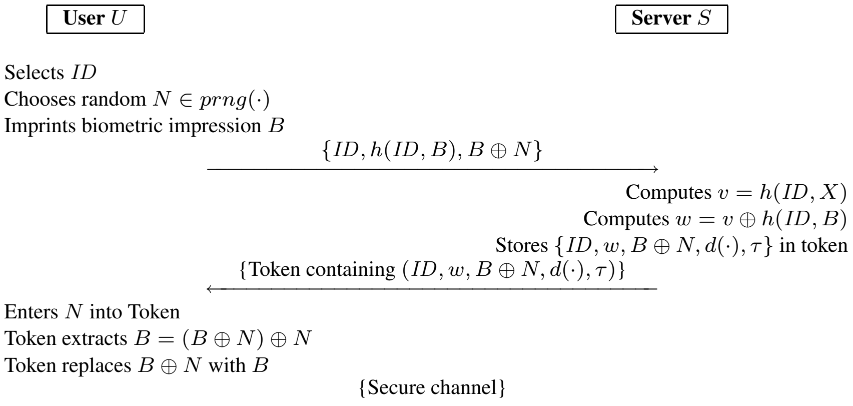
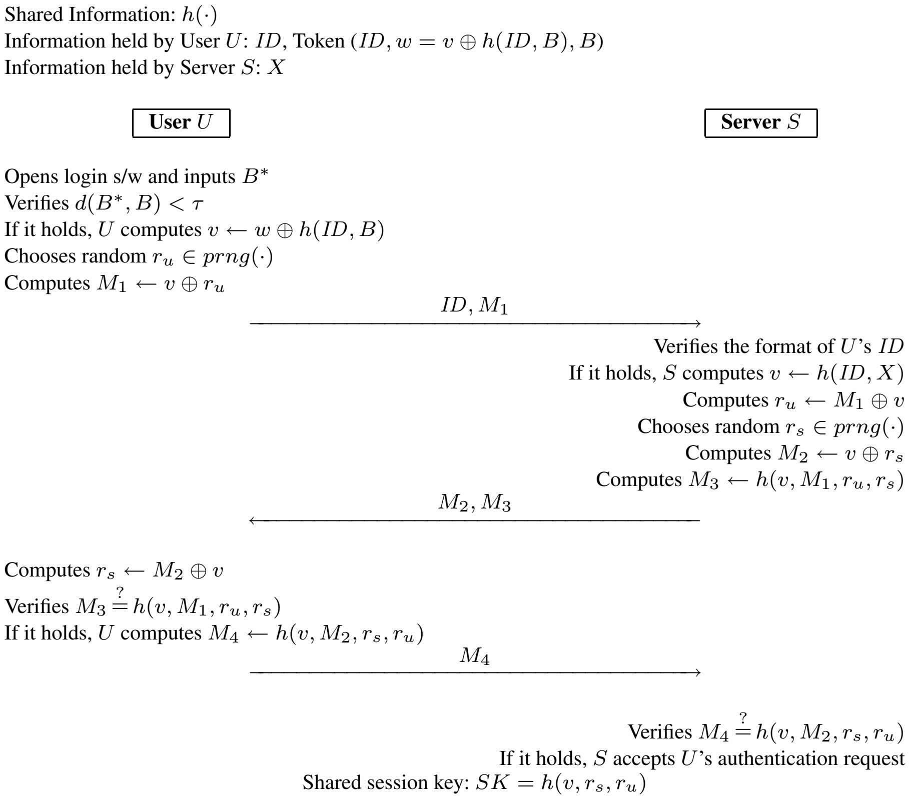

User U
Server S
Selects ID
Chooses random $N \in prng(\cdot)$
Imprints biometric impression B
$\{ID, h(ID, B), B \oplus N\}$
Computes $v = h(ID, X)$
Computes $w = v \oplus h(ID, B)$
Stores $\{ID, w, B \oplus N, d(\cdot), \tau\}$ in token
{Token containing $(ID, w, B \oplus N, d(\cdot), \tau)$}
Enters N into Token
Token extracts $B = (B \oplus N) \oplus N$
Token replaces $B \oplus N$ with B
{Secure channel}

Fig. 1. Registration phase



Shared Information: $h(\cdot)$
Information held by User U: ID, Token $(ID, w = v \oplus h(ID, B), B)$
Information held by Server S: X

User U **Server** S

Opens login s/w and inputs B^*
Verifies $d(B^*, B) < \tau$
If it holds, U computes $v \leftarrow w \oplus h(ID, B)$
Chooses random $r_u \in prng(\cdot)$
Computes $M_1 \leftarrow v \oplus r_u$

$$\xrightarrow{ID, M_1}$$

Verifies the format of U's ID
If it holds, S computes $v \leftarrow h(ID, X)$
Computes $r_u \leftarrow M_1 \oplus v$
Chooses random $r_s \in prng(\cdot)$
Computes $M_2 \leftarrow v \oplus r_s$
Computes $M_3 \leftarrow h(v, M_1, r_u, r_s)$

$$\xleftarrow{M_2, M_3}$$

Computes $r_s \leftarrow M_2 \oplus v$
Verifies $M_3 \overset{?}{=} h(v, M_1, r_u, r_s)$
If it holds, U computes $M_4 \leftarrow h(v, M_2, r_s, r_u)$

$$\xrightarrow{M_4}$$

Verifies $M_4 \overset{?}{=} h(v, M_2, r_s, r_u)$
If it holds, S accepts U's authentication request
Shared session key: $SK = h(v, r_s, r_u)$

Fig. 2. Authentication phase.

generates *accept* message. If $d(B^*, B) \geqslant \tau$, then it generates *reject* message. If *reject*, it means U does not pass the biometric verification and the phase is terminated. On the contrary, if *accept*, U's token extracts v by computing $w \oplus h(ID, B)$ and chooses a random number $r_u \in prng(\cdot)$. In here, v will be successfully retrieved because B is the original biometric information which stored into the token in the registration phase. Finally, U's token computes $M_1 = v \oplus r_u$ and sends it with ID to S.

A.2 $S \rightarrow U$: M_2, M_3.
S first checks whether the format of ID is valid or not. If the identity is not valid, S rejects this request. If ID is valid, S then computes $v = h(ID, X)$ using its master secret key X and decrypts the received message M_1 by computing $M_1 \oplus v$ to obtain r_u. Then, S chooses a random number $r_s \in prng(\cdot)$, and computes $M_2 = v \oplus r_s$ and $M_3 = h(v, M_1, r_u, r_s)$. Finally, S sends M_2 and M_3 to U.

A.3 $U \rightarrow S$: M_4.
U first decrypts the received message M_2 by computing $M_2 \oplus v$ to obtain r_s. Then, U verifies whether $M_3 \overset{?}{=} h(v, M_1, r_u, r_s)$. If it holds, U believes that S is authen-

ticated and then computes $M_4 = h(v, M_2, r_s, r_u)$ and sends it to S to provide mutual authentication between S and U.

A.4 S verifies whether $M_4 \overset{?}{=} h(v, M_2, r_s, r_u)$. If it holds, S accepts U's authentication request.

To protect (e.g., encrypt) further information exchanged in the session, U and S compute a one-time session key $SK = h(v, r_s, r_u)$.

4. Security Analysis

This section provides the proof of correctness of the proposed scheme. First, the security terms (Menezes *et al.*, 1997) needed for the analysis of the proposed scheme are defined as follows.

DEFINITION 1. A strong secret key (X) has a value of high entropy, which cannot be guessed in polynomial time.

DEFINITION 2. A secure chaotic one-way hash function $y = h(x)$ is where given x to compute y is easy and given y to compute x is hard.

Here, five security properties: guessing attacks, replay attacks, stolen token attacks, insider attacks, and mutual authentication, will be considered for the proposed scheme.

(1) *Guessing attacks*. The password guessing attack will not work against the proposed scheme since the proposed scheme does not require the password for protecting the corresponding token. Also, the secret $w = v \oplus h(ID, B)$ is stored in the user U's token. Only the legal user U which has his/her biometrics B can authenticate and compute the secret $v = w \oplus h(ID, B)$ on his/her token. In addition, an attack may try to derive S's secret key X from the intercepted messages M_1, M_2, M_3 and M_4. But it is computationally infeasible because of the property of the one-way hash function and random values. Therefore, the proposed scheme can prevent guessing attacks.

(2) *Replay attacks*. The replay attacks fail because the freshness of the messages transmitted in the authentication phase is provided by the random nonces r_u and r_s. Except for U (or S), only S (or U) who can embed the secret value v and two random nonces in the hashed message $M_3 = h(v, M_1, r_u, r_s)$ of Step A.2 (or $M_4 = h(v, M_2, r_s, r_u)$ of Step A.3), respectively. Therefore, the proposed scheme can prevent replay attacks.

(3) *Stolen token attacks*. Although the token of legal user U is lost or stolen, it is difficult for any attacker to derive the stored value w or extract v from w because he/she cannot pass the biometric verification. On comparing attacker's biometric template with the biometric template stored on the token, the illegal request will be rejected immediately. In addition, tamper-resistant microprocessors can be used to store and process private or sensitive information, such as private keys w or biometric information B, in the proposed scheme. To prevent an attacker from retrieving

or modifying the information, the tamper-resistant chips (e.g., IBM 4758) are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures. Therefore, the proposed scheme can prevent stolen token attacks.

(4) *Insider attacks*. In the proposed registration phase, the token of U will generate his/her biometric impression B and compute $h(ID, B)$ and $B \oplus N$, where N is a random number. Then, the token sends them to the server S for registration request. Hence, S cannot get the correct biometric B from $h(ID, B)$ and $B \oplus N$ because of the property of the one-way hash function. Therefore, the proposed scheme can prevent insider attacks.

(5) *Secure mutual authentication*. In Steps A.3 and A.4, both U and S will check if the hashed message M_3 or M_4 contains the secret value v, its computed M_1 or M_2, and the random nonces r_u and r_s, respectively. Since the hashed messages included two random nonces r_u and r_s, both U and S will believe the ith random nonce r_u or r_s was originally sent from S and U, respectively. U and S agree a one-time session key $SK = h(v, r_s, r_u)$ to protect (e.g., encrypt) further information exchanged in the session. By adopting Diffie–Hellman key agreement algorithm (e.g., $g^{r_u}, g^{r_s}, g^{r_u r_s}, SK = h(v, g^{r_u r_s})$; Diffie *et al.*, 1976), where g is a generator), the proposed scheme can also provide perfect forward secrecy. Therefore, the proposed scheme can provide secure mutual authentication and session key agreement.

5. Performance Comparisons

The comparisons of our scheme and other related schemes are summarized in Table 1. From Table 1, the computation costs of Khan *et al.*'s (2008), Li and Hwang's (2010), and the proposed schemes are very low because only a few hashing function computations are needed. Therefore, this feature makes our scheme effective. Both Khan *et al.*'s and

Table 1

Comparison with other related schemes

	Khan *et al.* (2008)	Li and Hwang (2010)	Our scheme
Computational costs in registration phase	3H	3H	2H
Computational costs in authentication phase	7H	7H	6H
Change password	Need	Need	No need
Mutual authentication	Yes	Yes	Yes
Without synchronized clocks	No	Yes	Yes
Provide non-repudiation	Yes	Yes	Yes
Prevent insider attack	No	No	Yes
Prevent stolen token attack	No	No	Yes

H: chaotic one-way hashing operation.

Li–Hwang's schemes use passwords during the registration and authentication phases. However, the proposed scheme does not require passwords. Thus, the user does not need to perform the password change phase to change the password. Moreover, the proposed scheme provides the same security level without using the password. In addition, the proposed scheme is secure to insider attacks and stolen token attacks. However, Khan *et al.*'s and Li–Hwang's schemes cannot withstand these attacks. As a result, the proposed scheme is more secure compared to both schemes.

6. Conclusions

This paper proposed an entire chaos-based biometric remote user authentication scheme on tokens without using passwords to provide strong security and minimize the computation cost of each participant. The proposed scheme not only is secure against well-known cryptographical attacks such as guessing attacks, replay attacks, stolen token attacks, insider attacks but also provides secure mutual authentication. In addition, the proposed scheme does not need to use the user password to register or authenticate and also does not require time synchronization or delay-time limitations between the user and remote system. As a result, we believe that the proposed scheme is very useful in limited computation and communication resource environments to access remote information systems since it provides security, reliability, and efficiency.

Acknowledgements. We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. This work is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2010-0010106).

References

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

Chang, C.C., Lin, I.C. (2005). Cryptanalysis of the modified remote login authentication scheme based on a geometric approach. *Informatica*, 16(1), 37–44.

Chen, T., Horng, G., Wu, K. (2007). A secure YS-like user authentication scheme. *Informatica*, 18(1), 27–36.

Chen, T., Horng, G., Yang, C. (2008). Public key authentication schemes for local area networks. *Informatica*, 19(1), 3–16.

Dachselt, F., Schwarz, W. (2001). Chaos and cryptography. *IEEE Trans. Circuits Syst.-I, Fundam. Theory*, 48(12), 1498–509.

Diffie, W., Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.

Elaine, B., John, K. (2006). *NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. Elaine Barker and John Kelsey, National Institute of Standards and Technology.

Gao, W., Wang, G., Wang, X., Yang, Z. (2009). One-round ID-based threshold signature scheme from bilinear pairings. *Informatica*, 20(4), 461–476.

Jean, C., Randall, J.E. (2007). *Annex C: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*. US Department of Commerce/National Institute of Standards and Technology.

Hsieh, B.T., Sun, H.M., Hwang, T. (2003). On the security of some password authentication protocols. *Informatica*, 14(2), 195–204.

Inuma, M., Otsuka, A., Imai, H. (2009). Theoretical framework for constructing matching algorithms in biometric authentication systems. In: *Lect. Notes Comput. Sci.*, Vol. 5558, pp. 806–815.

Kazlauskas, K., Kazlauskas, J. (2009). Key-dependent s-box generation in aes block cipher system. *Informatica*, 20(1), 23–34.

Khan, M.K., Jiashu, Z., Wang, X.M. (2008). Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. *Chaos Solitons Fractals*, 35(3), 519–524.

Kisel, A., Kochetkov, A., Kranauskas, J. (2008). Fingerprint minutiae matching without global alignment using local structures. *Informatica*, 19(1), 31–34.

Kocarev, L. (2001). Chaos-based cryptography: a brief overview. *IEEE Circuits Syst. Mag.*, 1, 6–21.

Ku, W., Tsai, H. (2005). Weaknesses and improvements of Yang–Chang–Hwang's password authentication scheme. *Informatica*, 16(2), 203–212.

Li, C.T., Hwang, M.S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *J. Netw. Comput. Appl.*, 33(1), 1–5.

Lin, C.L., Hwang, T. (2003). A password authentication scheme with secure password updating. *Comput. Secur.*, 22(1), 68–72.

Liu, J., Huang, S. (2010). Identity-based threshold proxy signature from bilinear pairings. *Informatica*, 21(1), 41–56.

Lumini, A., Nanni, L. (2007). An improved BioHashing for human authentication. *Pattern Recogn.*, 40, 1057–1065.

Menezes, A.J., Oorschot, P.C., Vanstone, S.A. (1997). *Handbook of Applied Cryptograph*. CRC Press, New York.

Popescu, C. (2009). An anonymous mobile payment system based on bilinear pairings. *Informatica*, 20(4), 579–590.

Ribaric, S., Fratric, I., Kis, K. (2008). A novel biometric personal verification system based on the combination of palmprints and faces. *Informatica*, 19(1), 81–100.

Rila, L., Mitchell, C.J. (2003). Security protocols for biometrics-based cardholder authentication in smartcards. In: *Lect. Notes Comput. Sci.*, Vol. 2846, pp. 254–264.

Sun, L., Liu, S. (2009). Cryptographic pseudo-random sequence from the spatial chaotic map. *Chaos Solitons Fractals*, 41, 2216–2219.

Sun, X., Li, J., Yin, H., Chen, G. (2010). Delegatability of an identity based strong designated verifier signature scheme. *Informatica*, 21(1), 117–122.

Tseng, Y., Wu, T., Wu, J. (2008). A pairing-based user authentication scheme for wireless clients with smart cards. *Informatica*, 19(2), 285–302.

Tulyakov, S., Farooq, F., Mansukhani, P., Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recogn. Lett.*, 28, 2427–2436.

Wang, Z., Qian, H., Li, Z. (2009). Adaptively secure threshold signature scheme in the standard model. *Informatica*, 20(4), 591–612.

Xiao, D., Liao, X., Deng, S. (2005). One-way Hash function construction based on the chaotic map with changeable-parameter. *Chaos Solitons Fractals*, 24, 65–71.

Yoon, E.J., Yoo, K.Y. (2007). A secure chaotic hash-based biometric remote user authentication scheme using mobile devices. In: *Lect. Notes Comput. Sci.*, Vol. 4537, pp. 612–623.

Yoon, E.J., Yoo, K.Y. (2009). Robust key exchange protocol between set-top box and smart card in DTV broadcasting. *Informatica*, 20(1), 139–150.

Yoon, E.J., Kim, W.H., Yoo, K.Y. (2005a). Robust and simple authentication protocol for secure communication on the web. In: *Lect. Notes Comput. Sci.*, Vol. 3579, pp. 352–362.

Yoon, E.J., Ryu, E.K., Yoo, K.Y. (2005b). An improvement of Hwang–Lee–Tang's simple remote user authentication scheme. *Comput. Secur.*, 24, 50–56.

Yoon, E.J., Ryu, E.K., Yoo, K.Y. (2005c). Attacks and solutions of Yang *et al.*'s protected password changing scheme. *Informatica*, 16(2), 285–294.

Ziauddin, S., Dailey, M.N. (2010). Robust iris verification for key management. *Pattern Recogn. Lett.*, doi:10.1016/j.patrec.2009.12.028.

E.-J. Yoon received his MSc degree in computer engineering from Kyungil University in 2002 and the PhD degree in computer science from Kyungpook National University in 2006, Republic of Korea. From 2007 to 2008, he was a full-time lecturer at Faculty of Computer Information, Daegu Polytechnic College, Republic of Korea. He is currently a 2nd BK21 contract professor at the School of Electrical Engineering and Computer Science, Kyungpook National University, Republic of Korea. His current research interests are cryptography, authentication technologies, smart card security, network security, mobile communications security, and steganography.

K.-Y. Yoo received his BSc degree in education of mathematics from Kyungpook National University in 1976 and the MSc degree in computer engineering from Korea Advanced Institute of Science and Technology in 1978, Republic of Korea. He received the PhD degree in computer science from Rensselaer Polytechnic Institute in 1992, New York, USA. Currently, he is a professor at the School of Computer Science and Engineering, Kyungpook National University, Republic of Korea. His current research interests are cryptography, authentication technologies, smart card security, network security, DRM security, and steganography. He has published over a hundred technical and scientific international journals on a variety of information security topics.

Pilnu chaosu pagrįsta biometrinė nutolusio vartotojo autentifikacijos su požymiais nenaudojanti slaptažodžio schema

Eun-Jun YOON, Kee-Young YOO

Straipsnyje pasiūlyta pilnu chaosu pagrįsta biometrinė nutolusio vartotojo autentifikavimo su požymiais ir nenaudojanti slaptažodžių schema. Šioje schemoje naudojama chaotinė santraukos funkcija ir pseudoatsitiktinių skaičių generatorius, kurie užtikrina vartotojo ir serverio, bendraujančių neapsaugotu ryšio kanalu, saugią tarpusavio autentifikaciją. Palyginus su panašiomis biometrinėmis autentifikacijos schemomis, šioje schemoje nereikia naudoti vartotojo slaptažodžio.