LETTER

A Biometric Authenticated Key Agreement Protocol for Secure Token

Eun-Jun YOON[†a)] ***and*** **Kee-Young YOO**[†b)]**,** ***Members***

SUMMARY This letter proposes a robust biometric authenticated key agreement (BAKA) protocol for a secure token to provide strong security and minimize the computation cost of each participant. Compared with other related protocols, the proposed BAKA protocol not only is secure against well-known cryptographical attacks but also provides various functionality and performance requirements.

key words: *biometric, token, authentication, password, security*

1. Introduction

Generally, there exist three kinds of approaches for user authentication. (1) Password-based user authentication ("what you know"): Passwords and PINs are examples of this approach. (2) Token-based user authentication ("what you have"): This approach includes physical keys, ATM or smart cards, photo ID cards, mobile devices (cell phones, PDA, RFID, sensor nodes) and so on. (3) Biometric-based user authentication ("what you are"): Voice, fingerprints, retinal scans, and keystrokes are included in this approach.

Due to their cryptographic capacity and portability, tokens have been widely used in many network applications. Moreover, biometrics hold the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications. Biometric authentication requires comparing a registered or enrolled biometric sample against a newly captured biometric sample, e.g., a fingerprint captured during a login. During enrollment procedure, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison (see Fig. 1). For biometric recognition, the biometric system authenticates a person's claimed identity from their previously enrolled pattern in verification procedure (see Fig. 1). For token-based biometrics authentication, a user inserts a token such as a smart card, a simple touch with a finger or a glance at a camera is enough to authenticate the user.

Recently, some research works [1], [2], [6]–[8] proposed biometrics-based remote user authentication protocols using smart cards. However, these protocols are insecure against some attacks or inefficiently designed because of high computation costs. Moreover, these protocols do not provide key agreement function which can provide two or more specified entities communicating over an open network with a shared secret key which may subsequently be used to achieve some cryptographic goal such as confidentiality or data integrity.

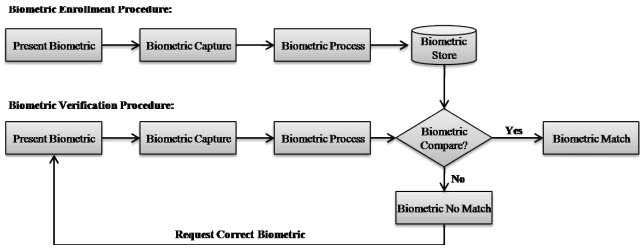

Fig. 1 The flowchart of biometric authentication.

Based on this motivation, this letter proposes a robust biometric authenticated key agreement (BAKA) protocol for a secure token to provide strong security and minimize the computation cost of each participant. The proposed BAKA protocol have several important features as follows: (1) It is designed to reduce the computation cost of each participant by using a small number of exponentiations. (2) It achieves cryptographic goals only using bitwise exclusive-OR (XOR) operation, exponentiations and collision-free one-way hash functions as main cryptographic operations without additional requirements such as using server's public key, digital signatures, 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 mutual authentication, perfect forward secrecy and secure password update phase. (4) It provides functionality requirements for biometric and token-based authentication such as provide non-repudiation, without synchronized clocks, without storing password tables in the server, allow users to freely choose and change the password and the biometrics without helping of the server, and so on. Thus, the proposed BAKA protocol is very useful in limited computations and communication resource environments to access remote information systems since it provides security, reliability, and efficiency.

2. The Proposed BAKA Protocol

The proposed protocol is composed of three steps, which are registration, authentication and key agreement, and password and biometrics update. Some of the notations used in

Manuscript received January 12, 2010.
Manuscript revised May 3, 2010.

[†]The authors are with the School of Electrical Engineering and Computer Science, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702–701, South Korea.
a) E-mail: ejyoon@knu.ac.kr
b) E-mail: yook@knu.ac.kr (Corresponding Author)

DOI: 10.1587/transinf.E93.D.2311

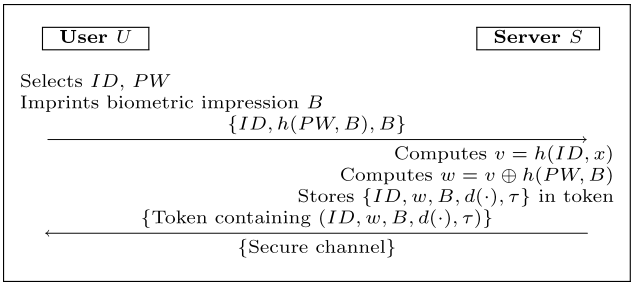

Fig. 2 Registration phase.

the proposed BAKA are defined as follows:

- U, S: User (client) and remote server.
- ID, PW: Identifier and password of U.
- B: Biometric template of U.
- x: Strong secret key of S.
- p: Large prime (usually at least 1024 or 2048 bits).
- q: Relatively small prime (typically of 160 bits) with $q|p-1$.
- g: Generator g of Z_q.
- a, b: Session-independent random exponents chosen by U and S.
- sk: Shared fresh session key computed by U and S.
- $h(\cdot)$: Collision resistant secure one-way hash function, e.g. SHA-512.
- $\oplus$: Bit-wise exclusive-OR (XOR) operation.

2.1 Registration Phase

Before a remote user login to the remote server, the user needs to perform the following steps (see Fig. 2).

R.1 $U \rightarrow S$: $\{ID, h(PW, B), B\}$

User U freely chooses his/her ID and password PW, and also imprints his/her personal biometric impression B at the sensor. U then interactively submits $\{ID, h(PW, B), B\}$ to the server S. These private data must be sent in person or over a secure channel.

R.2 $S \rightarrow U$: {Token containing $(ID, w, B, d(\cdot), \tau)$}

S computes $v = h(ID, x)$ and $w = v \oplus h(PW, B)$, where x is a secret key of S. Then, S writes the secure information $\{ID, w, B, d(\cdot), \tau\}$ 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 [9] for biometric verification.

2.2 Authentication and Key Agreement 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. 3).

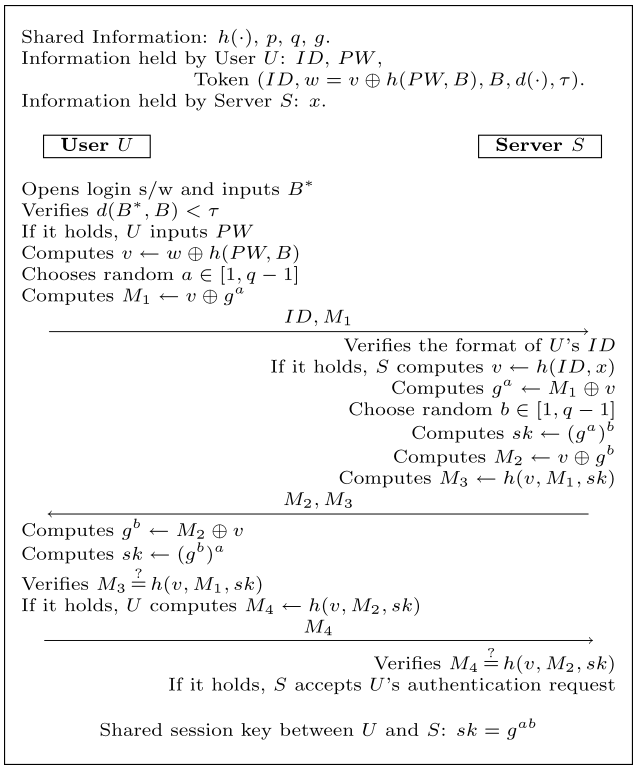

Fig. 3 Authentication and key agreement phase.

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 B^* with the stored B. If $d(B^*, B) < \tau$, then it generates *accept* message. If $d(B^*, B) \geq \tau$, 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 enters his/her password PW, and then U's token extracts v by computing $w \oplus h(PW, B)$ and chooses a random number $a \in [1, q-1]$. Finally, U's token computes $M_1 = v \oplus g^a$ 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 g^a. Then, S chooses a random number $b \in [1, q-1]$, and computes g^b and the shared session key $sk = (g^a)^b$. Finally, S computes $M_2 = v \oplus g^b$ and $M_3 = h(v, M_1, sk)$, and sends them 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 g^b. Then, U computes the

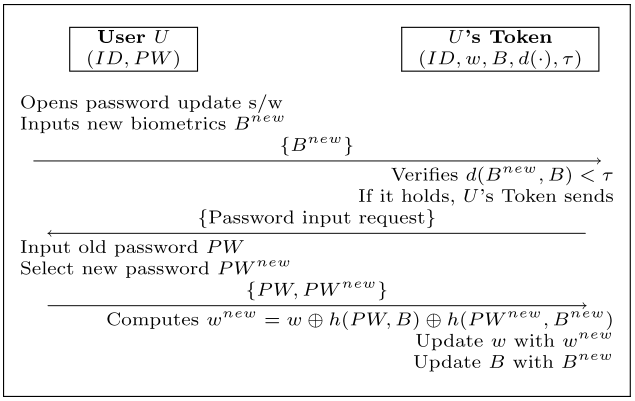

Fig. 4 Password and biometrics update phase.

shared session key $sk = (g^b)^a$ and verifies whether $M_3 \stackrel{?}{=} h(v, M_1, sk)$. If it holds, U believes that S is authenticated and then computes $M_4 = h(v, M_2, sk)$ and sends it to S to provide mutual authentication between S and U.

A.4 S verifies whether $M_4 \stackrel{?}{=} h(v, M_2, sk)$. If it holds, S accepts U's authentication and session key agreement request. Then, U and S can use the shared secret session key $sk = g^{ab}$ in private communication soon.

2.3 Password and Biometrics Update Phase

In this phase, the user U can freely and securely change the old password PW to a new password PW^{new} and the old biometrics B to a new biometrics B^{new} without helping of the server S (see Fig. 4). Because the old biometrics B has the problem of the aged deterioration, it needs to securely update the old biometrics B to a new biometrics B^{new}.

P.1 $U \rightarrow U$'s Token: $\{B^{new}\}$

U opens the password update application software into his/her token, and imprints new biometric B^{new} at the sensor.

P.2 U's Token $\rightarrow U$: {Password input request}

U's token first compares the imprinted B^{new} with the stored B by using the biometric verification process. If $d(B^{new}, B) \geq \tau$, it means U does not pass the biometric verification and the password and biometrics update phase is terminated. On the contrary, if $d(B^{new}, B) < \tau$, U passes the biometrics verification and then U's token shows a password input request message to the user.

P.3 $U \rightarrow U$'s Token: $\{PW, PW^{new}\}$

U enters his/her old password PW and inputs the new password PW^{new}.

P.4 U's token computes new $w^{new} = w \oplus h(PW, B) \oplus h(PW^{new}, B^{new})$ and then replaces the old w and the old B with new w^{new} and new B^{new} on the token, respectively.

3. Security Analysis

Here, seven security properties: guessing attacks, replay attacks, stolen token attacks, insider attacks, mutual authentication, perfect forward secrecy and secure password update phase, would be considered for the proposed BAKA.

1. *Guessing attacks*. The password guessing attack will not work against the proposed BAKA protocol since the password PW is only used for protecting the corresponding token, and no verifiable information is encrypted by passwords. Also, the secret $w = v \oplus h(PW, B)$ is stored in the user U's token. Only the legal user U which has his/her password PW and biometrics B can authenticate and compute the secret $v = w \oplus h(PW, B)$ 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.

2. *Replay attacks*. The replay attacks fail because the freshness of the messages transmitted in the authentication and key agreement phase is provided by the exponents a and b. Except for U (or S), only S (or U) who can compute the session key sk can embed the secret value v and the session key sk in the hashed message $M_3 = h(v, M_1, sk)$ of step A.2 (or $M_4 = h(v, M_2, sk)$ of step A.3), respectively.

3. *Stolen token attacks*. Although the token of legal user U is lost or stolen, it is difficult for any attacker to derive or change the password PW 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.

4. *Insider attacks*. In the proposed registration phase, the token of U will generate his/her biometric impression B and compute $h(PW, B)$. Then, the token sends them to the server S for registration request. Hence, S cannot directly get the correct password PW from $h(PW, B)$ because of the property of the one-way hash function. In addition, the legitimate user U cannot perform an insider attack to impersonate a legal server S because there is no way to directly obtain the strong secret key x of S. Although U can extract $v = h(ID, x)$ by computing $w \oplus h(PW, B)$ on his/her token, he/she still cannot obtain x because of the property of the one-way hash function. Thus, the proposed scheme can resist the insider attacks by the legitimate server S and the legitimate user U.

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,

Table 1 Performance comparisons with related protocols.

	Lin-Lai	Lee-Chiu	Yoon et al.	Chang et al.	Khan et al.	Li-Hwang	BAKA
Computations in registration phase	1H + 1E	2H + 1E	1H	2H	2H	3H	2H
Computations in authentication phase	3H + 4E	4H + 1E	5H	7H	7H	7H	6H + 4E
Change password	Yes	Yes	Yes	No	Yes	Yes	Yes
Change biometrics	No	No	No	No	No	No	Yes
Mutual authentication	No	No	Yes	Yes	Yes	Yes	Yes
Provide non-repudiation	Yes	No	No	No	Yes	Yes	Yes
Without synchronized clocks	No	No	No	Yes	No	Yes	Yes
Secure to stolen token attacks	No	No	No	No	No	No	Yes
Secure to insider attacks	No	No	No	No	No	No	Yes
Session key agreement	N/A	N/A	N/A	N/A	N/A	N/A	Yes
Perfect forward secrecy	N/A	N/A	N/A	N/A	N/A	N/A	Yes

H: one-way hashing operation, E: exponential operation, N/A: Not Applicable or Not Available

and the session key sk, respectively. Since the hashed messages included the shared session key sk between U and S, both U and S will believe the i-th random value g^b or g^a was originally sent from S and U, respectively.

6. *Perfect forward secrecy*. A disclosed long-lived secret key v, x or the password PW cannot derive the session key $sk = g^{ab}$ used before because without getting the used random exponents a and b, nobody can compute the used session key sk. If an attacker wiretaps all conversations of the medium, then he/she can derive some used random values g^a and g^b by computing $M_1 \oplus v$ and $M_2 \oplus v$, respectively. However, he/she could not compute the used session key sk from g^a and g^b. This problem is the Diffie-Hellman key exchange algorithm.

7. *Secure password and biometrics update phase*. In the proposed protocol, every user can select his/her password freely. Hence, the user can easily remember the password. Furthermore, we provide a secure password and biometrics update phase for users to change their old passwords PW and biometrics B. Because the old biometrics B has the problem of the aged deterioration, it needs to securely update the old biometrics B to a new biometrics B^{new}. In the proposed password and biometrics update phase, it is difficult for any attacker to change the password and biometrics because he/she cannot pass the biometric verification in P.2. Thus, the proposed password and biometrics update phase provides secure password and biometrics update function.

4. Performance Analysis and Comparisons

In this section, we will analyze the security of the proposed BAKA protocol and further compare Lin-Lai's protocol [2], Lee-Chiu's protocol [3], Yoon et al.'s protocol [4], Chang et al.'s protocol [5], Khan et al.'s protocol [7], Li-Hwang's protocol [8], and our BAKA protocol in terms of functionality and efficiency.

In the following, the comparisons of our BAKA protocol and other related protocols are summarized in Table 1. From Table 1, the proposed BAKA protocol requires some exponential operations in the authentication phase because the security of our BAKA protocol is based on solving discrete logarithm problems. These operations require to provide session key agreement and perfect forward secrecy unlike other related protocols. However, in terms of efficiency, the exponential computation is very high-powered and time-consuming. To provide the computational efficiency, we can change the the Diffie-Hellman key exchange algorithm with nonce-based key exchange algorithm in the proposed BAKA protocol. In this case, our BAKA protocol cannot provide the perfect forward secrecy. But, the computation costs are very low because only a few hashing function computations are needed like Yoon et al.'s, Chang et al.'s, Khan et al.'s, and Li-Hwang's protocols. In addition, other security requirements including session key agreement can still satisfied unlike other related protocols.

For functionality comparisons, though Chang et al.'s protocol allows users to freely choose the initial passwords during the registration phase, their protocol does not provide the functionality of change password in local. Thus, the user must notify the server if he/she wants to change the password. It will increase the communication overheads and some possible attacks between the user and the remote server over an insecure network. In addition, Lin-Lai's and Lee-Chiu's protocols do not provide mutual authentication between two communication parties. Lee-Chiu's, Yoon et al.'s, and Chang et al.'s protocols do not provide non-repudiation because of not employing personal biometrics. Lin-Lai's, Lee-Chiu's, Yoon et al.'s, and Khan et al.'s protocols required synchronized clocks between the user and the remote server because of using timestamps. In fact, it is fairly complicated to achieve time concurrency and some disadvantages exist such as the delivery latency and the different time zone, and so forth. From Table 1, we can see that our BAKA protocol not only provides session key agreement and perfect forward secrecy, but also prevents the stolen token attacks and insider attacks. As a result, our BAKA protocol is more secure and has many functionality compare with related protocols.

5. Conclusion

This letter proposed a robust biometric authenticated key

agreement (BAKA) protocol for a secure token to provide strong security and minimize the computation cost of each participant. Compared with other related protocols, the proposed BAKA protocol not only is secure against well-known cryptographical attacks such as guessing attacks, replay attacks, stolen token attacks, insider attacks but also provides mutual authentication, perfect forward secrecy and secure password update. In addition, it provides practical functionality requirements for biometric and token-based authentication.

Acknowledgment

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.2009-0073290).

References

[1] J.K. Lee, S.R. Ryu, and K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," Electron. Lett., vol.38, no.12, pp.554–555, June 2002.

[2] C.H. Lin and Y.Y. Lai, "A flexible biometrics remote user authentication scheme," Computer Standards and Interfaces, vol.27, no.1, pp.19–23, Nov. 2004.

[3] N.Y. Lee and Y.C. Chiu, "Improved remote authentication scheme with smart card," Computer Standards and Interfaces, vol.27, no.2, pp.177–180, Jan. 2005.

[4] E.J. Yoon, E.K. Ryu, and K.Y. Yoo, "An improvement of Hwang-Lee-Tang's simple remote user authentication scheme," Comput. Secur., vol.24, no.1, pp.50–56, Feb. 2005.

[5] Y.F. Chang, C.C. Chang, and Y.W. Su, "A secure improvement on the user-friendly remote authentication scheme with no time concurrency mechanism," Proc. 20th International Conference on Advanced Information Networking and Applications, IEEE CS, 2006.

[6] M.K. Khan and J. Zhang, "Improving the security of 'a flexible biometrics remote user authentication scheme'," Computer Standards and Interfaces, vol.29, no.1, pp.82–85, Jan. 2007.

[7] M.K. Khan, J. Zhang, and X. Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," Chaos, Solitons and Fractals, vol.35, no.3, pp.519–524, Feb. 2008.

[8] C.T. Li and M.S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," J. Network and Computer Applications, vol.33, no.1, pp.1–5, Jan. 2010.

[9] M. Inuma, A. Otsuka, and H. Imai, "Theoretical framework for constructing matching algorithms in biometric authentication systems," Proc. ICB 2009, LNCS 5558, pp.806–815, June 2009.