Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **4**, July **2015**

A Simple and Robust Biometrics-based One-Time Identity-Password Authenticated Key Agreement Scheme

Tianhua Liu
Shenyang Normal University, Dean's Office
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
liutianhua@sina.com

Received June, 2014; revised January, 2015

Abstract. *Authenticated key agreement protocols plays an important role in solving the issues over public internet, it sets up secure scheme to finish authentication of users and confidentiality of information transmission. As we know, more and more authenticated protocols put its heart into efficiency, security and user friendly. Biometrics-based algorithm can make the scheme more high-secure and user high-friendly. What is more, the one-time password-authenticated algorithms take advantage of the hash chain capturing the secure bit of the tip, improve the efficiency. Everyone has its advantage, so in my opinion, combining the mentioned algorithms could receive a high-level scheme. According to the approach, firstly we propose the new concept of one-time identity-password, importantly, the identity and the password could be used only once. Then the new robust biometrics-based one-time identity-password (OTIP) authenticated key agreement protocol is given. Because of the biometrics authentication and the function with the hash chain, the protocols stay away from the danger. The protocols of we proposed owns so much excellent advantages, such as refrain from some consuming algorithms robust to some attacks and so on. Lastly, we support the security and efficiency analysis about our scheme.*
Keywords: Authentication, Biometrics, Key agreement, One-time identity-password

1. **Introduction.** With the quicking pace of the mobile internet, many services such as internet shopping, stocking, banking and so on, take an action, so more and more key agreement protocols get to work. However, most of the authentication key agreement protocols used in M-commerce would consume so much communication rounds and computation cost that we can not afford it. Therefore, in order to satisfy user experience, security efficiency and user friendly, in particular, we propose a authenticated key agreement scheme which can get high-level service.

Nowadays, One time password (OTP) has been more popular and widely used in financial career, online shopping, internet game, and the OTP could be used only once. As a whole, the security of the traditional password, could be easily attacked due to Trojan horse and keylogger program. On the other hand, adversary could impersonate the legal user if he spends so much time, then communicate the service server, and even change the right password, on the contrary, legal user could not log in the servers. As a result, OTP has been attached great importance to solve the danger and protect the security of the users. Lamport [1] firstly proposes an approach of password authentication in 1981. Many schemes [2-9] have been proposed because of the high-level security, efficiency and user

friendly. In 2000, based on the discrete logarithm assumption, Tang [2] proposed an excellent directed OTP authentication protocol. In 2010, password-authentication key exchange (PAKE), which use the use the OTP, can support mutual authentication, session key exchange, and stand up to phish attacks, Paterson et al. [3] proposed a general technique scheme which allows for the secure use of pseudorandomly generated and time-dependent passwords, T.Y.Wu and Y.M.Tseng [4] proposed an efficient method that user achieve authentication and key exchange in mobile client-server environments, in addition, they [5] proposed an ID-based mutual authentication and key exchange protocol, making the scheme high-secure and the mobile devices low-power. In 2011, Fuglerud et al. [6] proposed a feasible and secure authentication method, which used a talking mobile OTP client rather than dedicated OTP generators to log in to a banking server. Then, Li et al. [7] proposed a two-layer authentication protocol with anonymous way on small Ad-hoc devices. In 2012, Mohan et al. [8] proposed an advanced idea using OTP to ensure that authenticating to services successfully, such as online shopping with a secure manner. In 2013, Huang et al. [9] proposed a valid simple OTP way that produce a unique passcode for each use. In Huangs scheme, OTP calculation used time stamps and sequence numbers. What is more, the mobile phones a two-factor authentication prototype using Huangs scheme has been used in practice for a year. In 2014, Xu et al. [10] proposed a self-updating OTP mutual authentication method based on a hash chain, which is unlimited used without establishing a new hash chain for Ad hoc network.

However, these literatures [1-10] just care about one-time password. As a matter of fact, the identity information is extraordinary significant. Because the adversary can search for much useful information according to the static identity by using illegal means. On the base of these motivations, the paper proposes a new simple biometrics-based one-time identity-password (OTIP) authenticated with key agreement protocol for mobile device between server and user to t mobile internet communication environment. Compared with previous connected protocols, the scheme of this paper proposed has the following more realistic advantages: (1) it firstly comes up with the concept of one-time identity-password. (2) it offers a kind of the secure and efficient biometric authentication [11, 12] , (3) it takes advantage of the one-time identity-passowrd to receive simple and robust session key agreement, (4) it provides secure one-time identity-password and biometric authentication and Seed update function by using biometrics update protocol, (5) it can reduce the whole calculated quantity and communication rounds because of the hash chain and Xored operation, (6) it can guard against many kinds of well-known attacks and guarantee the security.

The organization of the article is described as follows: Some preliminaries are given in Section 2. Next, a biometrics-based one-time password-authenticated with key agreement scheme is described in Section 3. Then, the security analysis and efficiency analysis are given in Section 4 and Section 5. This paper is finally concluded in Section 6.

2. **Preliminaries.**

2.1. **Biometric authentication.**

Each user has their unique biometric characteristics, such as voice, fingerprints, iris recognition and so on. These biometric characteristics have irreplaceable advantages: reliability, availability, non-repudiation and less cost. Therefore, biometric authentication has widely used. Fig.1 is the flow diagram of biometric characteristics collection and authentication. During the biometric collection phase, a biometric sample is collected, processed by a smart device, and stored which prepared for subsequent comparison (Fig.1). During the biometric authentication phase, the biometric system compares the stored sample with a newly captured sample (Fig.1). Obviously,

smart device has powerful information confidentiality and flexible portability. When performing a biometric authentication process, a user inputs a smart device, and utilizes a simple finger touch or a glance at a camera to authenticate himself/herself [9, 11, 12].

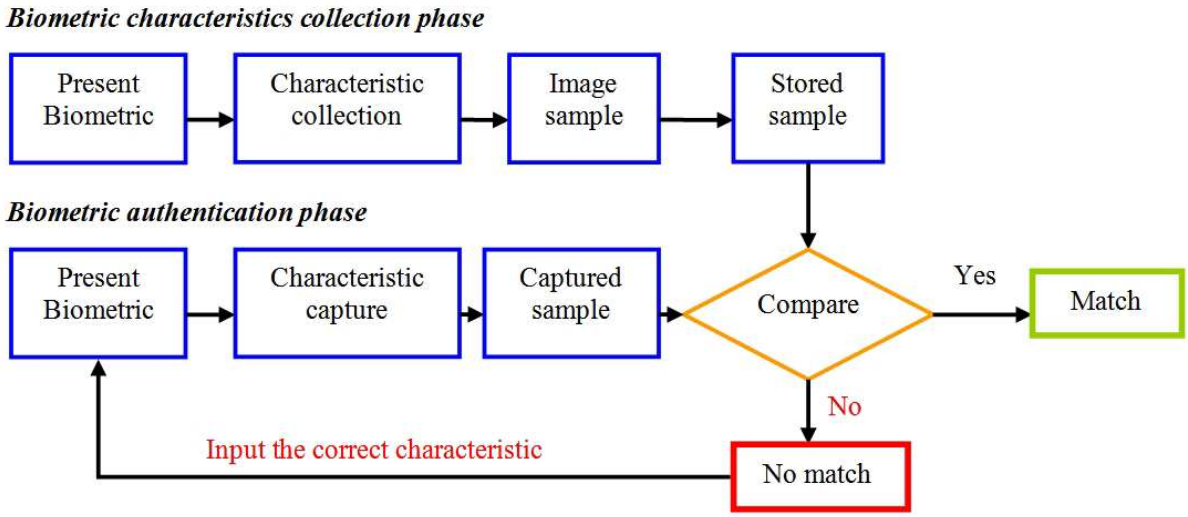

FIGURE 1. The flow diagram of Biometric characteristics collection and authentication

2.2. **One-way Hash Function.** A secure cryptographic one-way hash function $h : a \to b$ has four main properties:
(1) The function h takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output;
(2) The function h is one-way in the sense that given a , it is easy to compute $h(a) = b$.However, given b, it is hard to compute $h^{-1}(b) = a$;
(3) Given a , it is computationally infeasible to find a' such that $a' \neq a$,but $h(a') = h(a)$;
(4) It is computationally infeasible to find any pair a,a' such that $a' \neq a$,but $h(a') = h(a)$.

2.3. **Hard-Core Predicate.** General speaking, a polynomial-time predicate b is called a hard-core of a function f if each efficient algorithm, given $f(x)$,can guess $b(x)$ with success probability that is only negligibly better than one-half.

Definition 2.1. (Hard-Core Predicate) *A polynomial-time-computable predicate* $b : \{0,1\}^* \to \{0,1\}^n$ *is called a hard-core of a function* f *for each probabilistic polynomial-time algorithm* $A^{\sim}$*, each positive polynomial* $p(\cdot)$*, and all sufficiently large* n *has* $\Pr[A^{\sim}(f(U_n)) = b(U_n)] \leq \frac{1}{2} + \frac{1}{p(n)}$. U_n *is a random variable uniformly distributed in* $\{0,1\}^n$.

2.4. **Hash Chain.**

Definition 2.2. (Hash Chain) *Select a cryptographic secure hash function* h *with secure parameter* $k : \{0,1\}^* \to \{0,1\}^k$. *Pick a seed* s *randomly and apply* h *recursively* N *times to an initial seed* s *to generate a hash chain. The tip* ω *of the chain equals* $h^N(s)$.
$\omega = h^N(s) = h(h^{N-1}(s)) = \underbrace{h(h(h(...h(s))))}_{N \quad Times}$

3. **The Proposed Protocol.** In this section, biometrics-based one-time identity-password authenticated key agreement scheme is proposed which consists of three phases: the user registration phase, authenticated key agreement phase and the Seed and one-time password update phase (because the temporary identity is updated in every authenticated

key agreement phase). But firstly some notations are given which used in the proposed scheme.

3.1. **Notations.** The concrete notation used hereafter is shown in Table 1.

TABLE 1. Notations

Symbol	Definition
ID_A ID_S	The identity of a user and the server, respectively
TID_{A_t}	The temporary identity of Alice
R_{A_x}, R_{S_x}, r	nonces
B	the biometric sample of user
τ	predetermined threshold for biometric verification
$d()$	symmetric parametric function
h	A secure one-way hash function
$Seed$	An initial seed s to generate a hash chain by the server
$\|\|$	concatenation operation
$\oplus$	XORed operation
t	the reverse counter of the chosen hash chain by the server

3.2. **User registration phase.** Concerning the fact that the proposed scheme mainly relies on the design of one-time identity-password, it is assumed that the user can register at his appointed server in some secure way or by secure channel. The same assumption can be set up for the TTP server. Fig.2 illustrates the user registration phase.

Step 1. When a user Alice wants to be a new legal user, she chooses her identity ID_A at liberty and sends it to the trusted third party TTP with some her necessary information.

Step 2. Upon receiving the request from Alice, S selects a Seed, a random number R_{S_0} and setting a secure parameter N.Then S initialize the temporary identity TID_{A_0} and sends $\{N, Seed, TID_{A_0}\}$ to Alice via a secure channel.

Step 3. Upon receiving the message $\{N, Seed, TID_{A_0}\}$, Alice inputs her personal biometric image sample B at the mobile device. Then Alices mobile device chooses a random r and computes $p_t = h^{N-t}(h(B) \oplus Seed \oplus h(ID_A||ID_S||r))$ and submits $\{p_0\}$ to server S via a secure channel. Finally Alices mobile device stores $\{TID_{A_0}, Seed, B, r, h, d(), \tau, p_t(0 \leq t < N)\}$ securely, where $d(\cdot)$ is a symmetric parametric function and τ is predetermined threshold for biometric authentication. The parameter t is the reverse counter of the chosen hash chain: when $t = 0$, the $h^N()$ of hash chain is the first instance used in the proposed protocol. When $t = N - 1$, the $h^{N-(N-1)}() = h()$ of hash chain is the last used instance in our proposed protocol.

Step 4. Upon receiving the message $\{p_0\}$, S stores $\{ID_A, TID_{A_0}, Seed, p_0\}$ securely.

3.3. **Authenticated key agreement phase.** Without loss of generality, the paper sets Alice as a user, Server S as a service server. The public information of this instance is h . Alice has the biometric sample B*, and her mobile device (Seed, B, r, h, d(), pt,$\tau, TID_{A_{t-1}}$). S securely kept the secret information Seed, pt-1,$TID_{A_{t-1}}$. This concrete process is presented in the following Fig. 3.

Step 1. If Alice wishes to establish a session key with S, she imprints biometric B^* obile device. Then the biometric authentication process of mobile device compares the newly captured B^* with the stored B. If $d(B^*, B) \geq \tau$, that means Alice will get a connection refused response. If $d(B^*, B) < \tau$, that means Alice will get a connection accepted response. Then the mobile device selects random R_{A_t} (the same length with Seed) and compute: $R_{A_t} \oplus Seed$. After that, the mobile device sends $m_1 = \{TID_{A_{t-1}}, R_{A_t} \oplus Seed\}$ to the servers service server S.

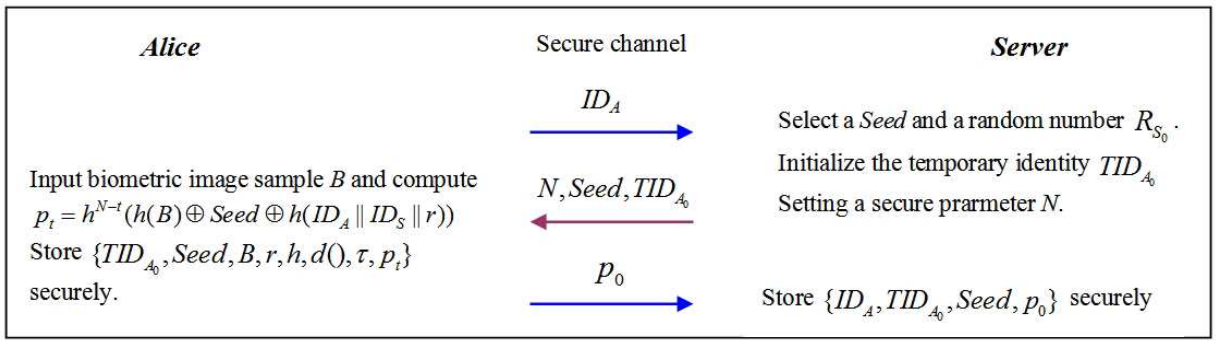

FIGURE 2. User registration phase

Step 2. After receiving the message $m_1 = \{TID_{A_{t-1}}, R_{A_t} \oplus Seed\}$ from Alice, S will do the following tasks:
(1)Compute $R_{A_t} = R_{A_t} \oplus Seed \oplus Seed$;
(2)Selects random R_{S_t} and computes $M_{t_1} = N - t, M_{t_2} = Seed \oplus h(R_{A_t}||R_{S_t}), M_{t_3} = h(h(R_{A_t}||R_{S_t})) \oplus p_{t-1}$ and $M_{t_4} = h(h(R_{A_t}||R_{S_t})||TID_{A_{t-1}}) \oplus TID_{A_t}$.
Finally S sends the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}\}$ to Alice.
Step 3. After receiving the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}\}$, Alice will check if $h(M_{t_2} \oplus Seed) \oplus p_{N-M_{t_1}-1} = M_{t_3}$. If the equation does not hold, Alice terminates it simply. Otherwise that means Alice authenticates S in this instance. Then Alice computes $m_3 = p_t \oplus h(R_{A_t}||R_{S_t})$, $TID_{A_t} = M_{t_4} \oplus h((M_{t_2} \oplus Seed)||TID_{A_{t-1}})$, $SK = h(h(R_{A_t}||R_{S_t})||ID_A||ID_S)$ and deletes p_t.Next Alice replaces $TID_{A_{t-1}}$ byTID_{A_t} and sends $m_3 = p_t \oplus h(R_{A_t}||R_{S_t})$ to server S . Finally Alice sets $SK = h(h(R_{A_t}||R_{S_t})||ID_A||ID_S)$ as the session key in this instance.

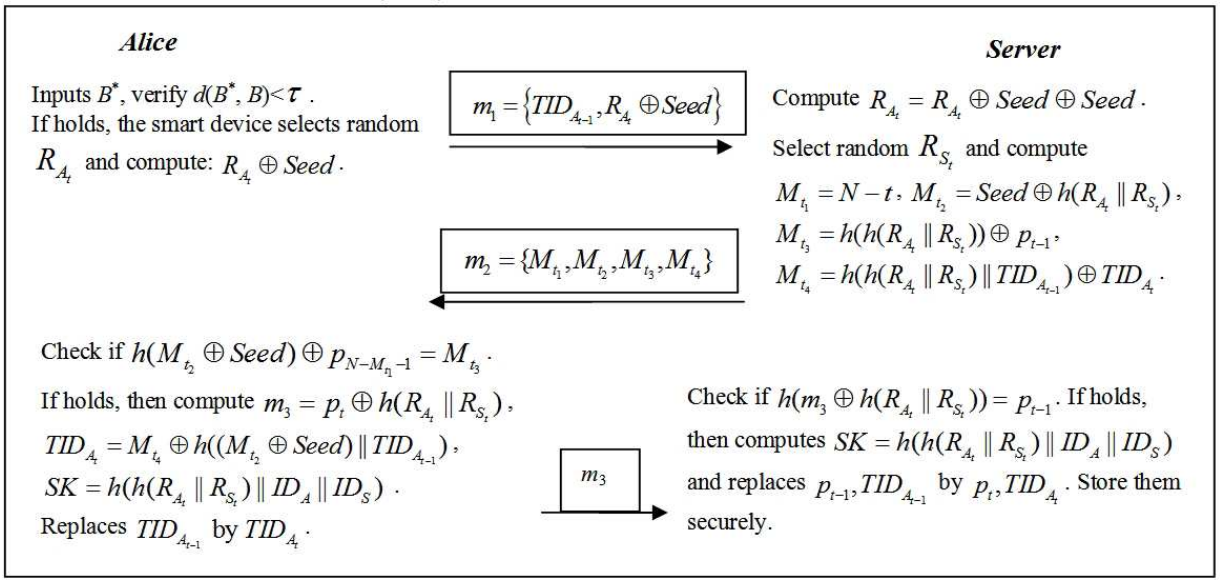

FIGURE 3. The process of the t th time authentication and key exchange phase

Step 4. When S obtains m_3, S computes $p'_{t-1} = h(m_3 \oplus h(R_{A_t}||R_{S_t}))$ and verifies whether $p'_{t-1} = p_{t-1}$ or not. If it does not hold, S terminates it. Otherwise, S computes $SK = h(h(R_{A_t}||R_{S_t})||ID_A||ID_S)$ as the session key in this instance and replaces p_{t-1} by p_t to store p_t securely.

3.4. **The Seed and one-time password update phase.** Fig.4 illustrates biometrics and password update phase. The public information of this instance is h. Alice has the biometric sample B^*, and her mobile device ($Seed$, B,r, h, $d()$,p_t, τ ,$TID_{A_{t-1}}$). S securely kept the secret information ($Seed$, p_{t-1}, $TID_{A_{t-1}}$).The steps are performed during the Seed and one-time password update phase as follows.

Step 1. When t = N-1, Alice and the Server S need to update the Seed and one-time password at the same time. Alice imprints biometric B^* at the mobile device. Then the biometric authentication process of mobile device compares the newly captured B^* with the stored B. If $d(B^*, B) \geq \tau$, that means Alice will get a connection refused response. If $d(B^*, B) < \tau$, that means Alice will get a connection accepted response. Then Alice inputs her ID_A, and the mobile device selects random $R_{A_{N-1}}$ (the same length with Seed) and compute: $R_{A_{N-1}} \oplus Seed$. After that, the mobile device sends $m_1 = \{TID_{A_{N-2}}, R_{A_{N-1}} \oplus Seed\}$ to the servers service server S.

Step 2. After receiving the message $m_1 = \{TID_{A_{N-2}}, R_{A_{N-1}} \oplus Seed\}$from Alice, S will do the following tasks:

(1) Compute $R_{A_{N-1}} = R_{A_{N-1}} \oplus Seed \oplus Seed$;

(2) Selects random $R_{S_{N-1}}$, $Seed'$ and computes $M_{t_1} = N-t$,$M_{t_2} = Seed \oplus h(R_{A_{N-1}}||R_{S_{N-1}})$, $M_{t_3} = h(h(R_{A_{N-1}}||R_{S_{N-1}})) \oplus p_{t-1}$, $M_{t_4} = h(h(R_{A_{N-1}}||R_{S_{N-1}})||TID_{A_{N-2}}) \oplus TID'_{A_0}$ and $M_{t_5} = Seed \oplus Seed'$. Finally S sends the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}, M_{t_5}\}$ to Alice.

Step 3. After receiving the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}, M_{t_5}\}$, Alice will check if

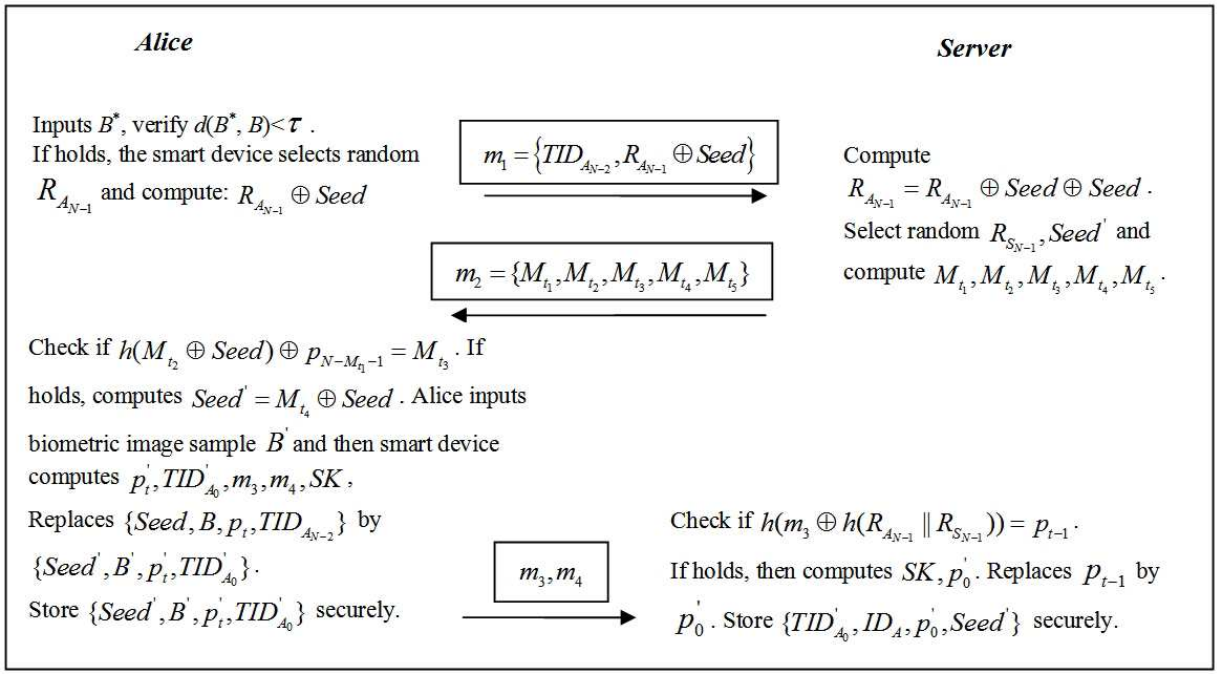

FIGURE 4. The Seed and one-time integrated information update phase

$h(M_{t_2} \oplus Seed) \oplus p_{N-M_{t_1}-1} = M_{t_3}$. If the equation does not hold, Alice terminates it simply. Otherwise that means Alice authenticates S in this instance. Alice inputs biometric image sample B' and then mobile device computes computes, $p'_t = hN - t(h(B') \oplus Seed' \oplus h(ID_A))$, $TID'_{A_0} = M_{t_4} \oplus h((M_{t_2} \oplus Seed)||TID_{A_{N-2}})$, $m_3 = p_t \oplus h(R_{A_{N-1}}||R_{S_{N-1}})$, $m_4 = p'_0 \oplus h(R_{A_{N-1}}||R_{S_{N-1}})$ and $SK = h(h(R_{A_t}||R_{S_t})||ID_A||ID_S)$. Next Alice sends m_3, m_4 to server S and sets $SK = h(h(R_{A_t}||R_{S_t})||ID_A||ID_S)$ as the session key in this instance. Finally Alices mobile device will replaces $\{Seed, B, p_t, TID_{A_{N-2}}\}$ by $\{Seed', B', p'_t, TID'_{A_0}\}$

and stores $\{Seed', B', p'_t, TID'_{A_0}\}$ securely.
Step 4. When S obtains m_3, m_4 , S computes $p'_{t-1} = h(m_3 \oplus h(R_{A_{N-1}}||R_{S_{N-1}}))$ and verifies whether $p'_{t-1} = p_{t-1}$ or not. If it does not hold, S terminates it. Otherwise, S computes $SK = h(h(R_{A_{N-1}}||R_{S_{N-1}})||ID_A||ID_S)$ as the session key in this instance and computes $p'_0 = m_4 \oplus h(R_{A_{N-1}}||R_{S_{N-1}})$ to replace p_{t-1} by p'_0 for storing $\{TID'_{A_0}, ID_A, p'_0, Seed'\}$ securely.

4. **Security Consideration.** The section analyzes the security of our proposed protocol. Let us assume that there are two secure components, including a secure one-way hash function and a secure symmetric encryption. Assume that the adversary has full control over the insecure channel including eavesdropping, recording, intercepting, modifying the transmitted messages. The definitions and analysis of the security requirements [13-17] will be illustrated in Appendix A. From Table 2, we can draw a conclusion that the proposed scheme provided One-time identity-password feature which can wipe out many attacks relating the static identity and static password. At the same time, our proposed protocol prevents the KCI attacks owing to OTP method.

Table 2. Architecture and security of our proposed protocol

Category		Eun-Jun Yoon's Scheme [10] (2013)	Our Proposed Scheme
Security requirements	One-time identity-password	N/A	**Provided**
	Single registration	Provided	Provided
	Mutual authentication	Provided	Provided
	Impersonation attack	Provided	Provided
	Man-in-the-middle attack	Provided	Provided
	Replay attack	Provided	Provided
	Known-key security	Provided	Provided
	Perfect forward secrecy	Provided	Provided
	Data integrity	Provided	Provided
	Guessing attacks	Provided	Provided
	Session key security	Provided	Provided
	KCI attacks	N/A	**Provided**
	Stolen mobile device attack	Provided	Provided
	Biometrics authentication	Provided	Provided
Notes: N/A: "not available" or "not support".			

5. **Efficiency Analysis.** Compared to RSA and ECC, Chebyshev polynomial computation problem offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings. In our proposed protocol, no time-consuming modular exponentiation and scalar multiplication on elliptic curves are needed.
In this section, we will compare our scheme with Eun-Jun Yoons scheme of [10]. For convenience, some notations are defined as follows. Thash: The time for executing the hash function; TXOR: The time for executing the XOR operation; TECmul: The time for executing the elliptic curve point multiplication.
To be more precise, on an Intel Pentium4 2600 MHz processor with 1024 MB RAM, where N and P are 1024 bits long, the computational time of a one-way hashing operation and an elliptic curve point multiplication operation is 0.0005s and 0.063075s separately [18-20]. Moreover, the computational cost of XOR operation could be ignored when compared with other operations. Table 3 shows performance comparisons between our proposed scheme and Eun-Jun Yoons scheme of [10]. Therefore, as in Table 3, we can draw a conclusion that the proposed scheme has the lowest computational costs and is well suited to the mobile devices applications.

TABLE 3. Efficiency of our proposed scheme

Communication costs		Eun-Jun Yoon's Scheme [10] (2013)	Our Proposed Scheme
User registration phase		$1T_{hash}\approx 0.0005$s	$NT_{hash}\approx 0.0005N$s
Server registration phase		$1T_{hash}\approx 0.0005$s	-
Authentication and key agreement phase	*User*	$5T_{hash}+2T_{EC-mul}\approx 0.12715$s	$3T_{hash}\approx 0.0015$s
	S_i (server)	$5T_{hash}+2T_{EC-mul}\approx 0.12715$s	$5T_{hash}\approx 0.0025$s
	S_j (*RC*)	$7T_{hash}\approx 0.0035$s	-
secrets update phase		$2T_{hash}\approx 0.001$s	$10T_{hash}+NT_{hash}\approx 0.0005(10+N)$s
Random numbers		2	2
Rounds of Authentication phase		5	3
Note: **-: "no need".**			

Next, we will illustrates the concrete values with the N changing between our proposed scheme and Eun-Jun Yoons scheme of [10]. We devided the total computations into two steps:
(1) The first step including registration phase and authentication and key agreement phase which can only be used once. $(19T_{hash}+4T_{EC-mul})$ is the computations of [10] and $(8T_{hash}+NT_{hash})$ is the computations of our proposed scheme.
(2) The second step only including authentication and key agreement phase which can be used $(N-1)$ times. $(18T_{hash}+4T_{EC-mul})$ is the computations of [10] and $(6T_{hash})$ is the computations of our proposed scheme at a time. So the difference of total calculated amount between literature [10] and our proposed scheme is:

$$\begin{aligned} &Total_{time-difference} = Total_{\text{computationsof[10]}} - Total_{\text{computationsofourprotocol}} \\ &=(19T_{hash}+4T_{EC-mul})-(8T_{hash}+NT_{hash})+(N-1)[(18T_{hash}+4T_{EC-mul})-(6T_{hash})] \\ &=N(11T_{hash}+4T_{EC-mul})-1T_{hash}\approx 0.2578N-0.0005 \end{aligned}$$

That means our proposed scheme has much more efficient than Eun-Jun Yoons scheme of [10]. With the N increases linearly, our proposed schemes cost of computation will decrease linearly comparing with Eun-Jun Yoons scheme of [10].

6. **Conclusion.** The article firstly presents the concept about one-time identity-password which makes the security and efficiency more stronger than the previous project. Then, according to OTIP theory, we come up with the one-time identity-password authenticated key agreement scheme on the base of biometrics, not only it is simple and robust, but also secure and efficient. The centre ideas of the proposed scheme have many advantages in the mobile device and servers side, such as security, efficiency and so on, and the advantage in users side is user friendly. In brief, the scheme of we proposed has satisfied many aspects of requirements with security, efficiency and functionality. As a result, our schemes become the best choice to actual applications.

REFERENCES

[1] L. Lamport, Password Authentication with Insecure Communication. *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, November 1981.
[2] S. H. Tang, Directed one-time password authentication scheme based upon discrete logarithm. *Journal of Circuits, Systems and Compute*, vol. 10, no. 3, pp. 173-180, 2000.
[3] K. G. Paterson, G. Kenneth and D. Stebila, One-time-password-authenticated key exchange. *Information Security and Privacy: Proceedings of 15th Australasian Conference*, pp. 264-281, July 2010.
[4] T. Y. Wu and Y. M. Tseng, An efficient user authentication and key exchange protocol for mobile client-server environments. *Computer Network*, vol. 54, no. 9, pp 1520-1530, 2010.
[5] T. Y. Wu and Y. M. Tseng, An ID-based mutual authentication and key exchange protocol for low-power mobile devices. *The Computer Journal*, vol. 53, no. 7, 2010, pp 1062-1070.
[6] K. Fuglerud and O. Dale, Secure and inclusive authentication with a talking mobile one-time-password client. *Security and Privacy, IEEE*, vol. 9, no. 2, pp. 27-34, 2011.

[7] C. T. Li and M. S. Hwang, A lightweight anonymous routing protocol without public key en/decryptions for wireless Ad Hoc networks. *Information Sciences*, vol. 181, no. 23, pp. 5333-5347, December 2011.
[8] R. Mohan and N. Partheeban, Secure multimodal mobile authentication using one time password. *Informational Journal of Recent Technology and Engineering*, vol.1, no. 1, April 2012.
[9] Y. Huang, Z. Huang, H.R. Zhao and X.J. Lai, A new one-time password method. *Informational Conference on Electronic Engineering and Computer Science*, 2013, pp 32-37.
[10] F. Xu, X. Lv, Q. Zhou and X. Liu, Self-updating one-time password authentication protocol for ad hoc network. *Transactions on Internet and Information Systems*, vol. 8, no. 5, 2014.
[11] C. T. Li, M. S. Hwang, An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, vol. 33, np. 1, pp. 1-5, 2010.
[12] E. J. Yoon, K. Y. Yoo, Robust biometrics-based multi-server authentication with key agreement scheme for smart devices on elliptic curve cryptosystem. *J Supercomput*,vol. 63, pp. 235255, 2013.
[13] N. Y. Lee, Y. C. Chiu, Improved remote authentication scheme with smart card.[J]. *Computer Standards * Interfaces*, vol. 27, no. 2, pp. 177-180, January 2005.
[14] M. K. Khan, J. S. Zhang, Improving the security of a flexible biometrics remote user authentication scheme. *Computer Standards * Interfaces*, vol. 29, no. 1, pp. 82-85, January 2007.
[15] L. H. Li, I. C. Lin, and M. S. Hwang, A remote password authentication scheme for multi-server architecture using neural networks.*IEEE Transa. on Neural Networks*, vol. 12, no. 6, pp. 14981504, 2001.
[16] I. C. Lin, M. S. Hwang, and L. H. Li, A new remote user authentication scheme for multi-server architecture. *Future Generation Computer Systems*, vol. 19, no. 1, pp. 1322, 2003.
[17] J. L. Tsai, Efficient multi-server authentication scheme based on one-way hash function without verification table. *Comput Secur*, vol. 27, no. 34, pp.115121, 2008.
[18] S. P. Ravi, C. D. Jaidhar, T. Shashikala, Robust Smart Device Authentication Scheme for Multi-server Architecture. *Wireless Pers Commun*, vol. 72, pp.729745, 2013, DOI 10.1007/s11277-013-1039-6.
[19] B. Wang, M. Ma, A smart device based efficient and secured multi-server authentication scheme. *Wireless Personal Communications*, doi:10.1007/s11277-011-0456-7, 2012.
[20] L. Kocarev, S. Lian, Chaos-Based Cryptography: Theory, Algorithms and Applications, pp. 5354. Springer, 2011.
[21] W. Hsieh, J. Leu, Anonymous authentication protocol based on elliptic curve DiffieHellman for wireless access networks. *Wireless Communications and Mobile Computing*, 2012, doi:10.1002/wcm.2252.
[22] C. Li, M. Hwang, and Y. Chung, A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Computer Communication*, vol. 31, pp. 28032814, 2008.

Appendix A. **Security proof of the proposed scheme.** (1) Mutual authentication and key agreement

Definition A.1. Mutual authentication and key agreement refers to two parties authenticating each other suitably and getting the session key simultaneously.

Theorem A.1. The proposed protocol can achieve mutual authentication and key agreement.

Proof: If $h(M_{t_2} \oplus Seed) \oplus p_{N-M_{t_1}-1}$ equals M_{t_3}, which means that S was already authenticated by Alice. Because only S can retrive the Alices random number R_{A_t} by secret Seed. If $h(m_3 \oplus h(R_{A_t}||R_{S_t}))$ equals p_{t-1}, which means that Alice was already authenticated by S. Because only Alice can retrive the $h(R_{A_t}||R_{S_t})$ by the secret Seed.

As for the key agreement, after authenticating each other, the temporary R_{A_t}, R_{S_t} and the ID ID_A, ID_S were already authenticated by S. So finally Alice and S can make the key agreement simultaneously.

(2) Impersonation attack / Man-in-the-middle attack

Definition A.2. An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.

Definition A.3. The man-in-the-middle attack is a form of active eavesdropping in which

the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Theorem A.2. The proposed protocol can resist impersonation attack.

Theorem A.3. The proposed protocol can resist Man-in-the-middle attack.

Proof: An adversary cannot impersonate anyone of the Alice or S. The proposed scheme has already authenticated each other between Alice and S (in section Appendix A.(1)) based on the secrets $B, Seed$ and the nonces R_{A_t}, R_{S_t}. So there is no way for an adversary to have a chance to carry out impersonation attack.

Because $m_i (1 \leq i \leq 3)$ contain the secret Seed and the the nonces R_{A_t}, R_{S_t}, a man-in-the-middle attack cannot succeed.

(3) Replay attack

Definition A.4. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

Theorem A.4. The proposed protocol can resist replay attack.

Proof: An adversary cannot start a replay attack against our scheme because of the freshness of R_{A_t}, R_{S_t} in each session. If R_{A_t} and $h(R_{A_t}||R_{S_t})$ has appeared before or the status shows in process, any of the participants in instance protocol will reject the session request. If the adversary wants to launch the replay attack successfully, it must compute and modify R_{A_t}, $h(R_{A_t}||R_{S_t})$ and $m_i (1 \leq i \leq 3)$ correctly which is impossible.

(4) Known-key security

Definition A.5. Known-key security is that a protocol can protect the subsequent session keys from disclosing even if the previous session keys are revealed by the intendant user.

Theorem A.5. The proposed protocol can achieve known-key security.

Proof: Since the session key $SK = h(h(R_{A_t}||R_{S_t})||ID_A||ID_S)$ is depended on the random nonces R_{A_t}andR_{S_t} , and the generation of nonces is independent in all sessions, an adversary cannot compute the previous and the future session keys when the adversary knows one session key. And in the Seed and one-time password update phase, any session key is only used once, so it has known-key security attribute.

(5) Perfect forward secrecy

Definition A.6. An authenticated multiple key establishment protocol provides perfect forward secrecy if the compromise of both of the nodes secret keys cannot results in the compromise of previously established session keys [21].

Theorem A.6. The proposed protocol can achieve perfect forward secrecy.

Proof: In the proposed scheme, the session key $SK = h(h(R_{A_t}||R_{S_t})||ID_A||ID_S)$ is related with R_{A_t}andR_{S_t} , which were randomly chosen by Alice and the server S, respectively. So any session key has not related with the long secret key (such as) of each of participants. Furthermore because of the secure hash function, an adversary cannot compute the previously established session keys.

(6) Data integrity

Definition A.7. Authentication multiple key establishment protocol is said to achieve the property of data integrity, if there is no polynomial time algorithm that can alter or manipulate the transmitted messages.

Theorem A.7. The proposed protocol can achieve data integrity property.

Proof: While the each participant sends the sensitive data to another participant in the instance protocol by the communication channel, the adversary alter or manipulate the data and cheat one of the honest participants by relying on the wrong session keys.

If the adversary wants to alter or manipulate the message $m_1 = \{TID_{A_{t-1}}, R_{A_t} \oplus Seed\}$ of step1 for cheating S, the adversary will be detected in the step4. Because the adversary does not have the Seed , $TID_{A_{t-1}}$ and the personal biometric image sample B of Alice,

then the adversary cannot compute $m_3 = p_t \oplus h(R_{A_t}||R_{S_t})$, finally the adversary cannot pass the validation of S. If the adversary wants to alter or manipulate the message m2, the adversary will be detected in the step3 by Alice. Because the adversary does not have the Seed, p_{t-1} , he cannot get the Seed and compute M_{t_2}, M_{t_3}. As for m3, the adversary cannot alter or manipulate it because m3 is just a XORed value of a secure hash, S can verify m3 by the local information.

(7) Dictionary/Guessing attacks

Definition A.8. In an off-line dictionary/guessing attack, an attacker random chooses a word from a dictionary or guesses a password and verifies his choose or guess, but he does not need to participate in any communication phase because he has already downloaded the nessesary information.

Theorem A.8. The proposed protocol can resist Guessing attacks.

Proof: In our proposed scheme of the authenticated key exchange phase, the undetectable on-line guessing attack will not affect at all. Because there is no password at all. And the mobile device authenticated Alice only by Alices personal biometric image sample B. Therefore, the proposed scheme can resist guessing attacks.

(8) Session key security

Definition A.9. A communication protocol exhibits session key security if the session key cannot be obtained without any long-term secrets.

Theorem A.9. The proposed protocol can achieve session key security.

Proof: In the authenticated key agreement phase and one-time password and the Seed update phase, a session key SK is generated from R_{A_t}andR_{S_t}. These parameter values are different in each session, and each of them is only known by Alice and S. Whenever the communication ends between S and Alice, the session key will immediately self-destruct and will not be reused. Therefore, assuming the attacker has obtained a session key, Alice will be unable to use this session key to decode the information in other communication processes. Because the random point elements R_{A_t}andR_{S_t} are all generated randomly and are protected by the secure one-way hash function, a known session key cannot be used to calculate the value of the next session key. Additionally, since the values R_{A_t}andR_{S_t} of the random elements are very large, attackers cannot directly guess the values R_{A_t}andR_{S_t} of the random elements to generate session key. Therefore, the proposed scheme provides session key security.

(9) Key Compromise Impersonation Attacks (KCI attacks)

Definition A.10. An adversary is said to impersonate a party B to another party A if B is honest and the protocol instance at A accepts the session with B as one of the session peers but there exists no such partnered instance at B [22]. In a successful KCI attack, an adversary with the knowledge of the long-term private key of a party A can impersonate B to A.

Theorem A.10. The proposed protocol can resist KCI attack.

Proof: Because there is no password at all and the mobile device authenticated Alice only by Alices personal biometric image sample B, the key compromise impersonation attacks will fail.

(10) Stolen mobile device attacks

Definition A.11. Anyone gets the mobile device in some way to execute some kind of attacks.

Theorem A.11. The proposed scheme can resist stolen mobile device attacks.

Proof: It is very clear that the proposed scheme provides biometrics authentication. Anyone including an adversary cannot pass the biometric verification. Therefore, the proposed scheme can resist stolen mobile device attacks.