Zuowen Tan

Jiangxi University of Finance & Economics

An efficient biometrics-based authentication scheme for telecare medicine information systems

Abstract. *The telecare medical information system enables the patients gain health monitoring and access healthcare-related services over internet or mobile networks. Due to the open environment, the mutual authentication between the user and the telecare server will thus be in demand. Many smart card based authentication schemes for telecare medicine information systems have been proposed for the goals. However, most of the schemes are vulnerable to various attacks. Specially, some schemes require the exponential computation or public key cryptography which leads to very low efficiency for smart card. This paper proposes an efficient smart card based password authentication scheme by applying biometrics technique and hash function operations. It is shown to be more secure and practical for telecare medicine environments.*

Streszczenie. *W artykule opisano prostą metodę uwierzytelniania i identyfikacji użytkownika danych usług (np. medycznych) na podstawie kart typu Smart-Card. Proponowana struktura opiera się na technikach biometrycznych oraz funkcji skrótu (haszowanie). Rozwiązanie to zapewnia większe bezpieczeństwo i jest praktyczniejsze dla telefonicznych biur obsługi medycznej. (**Zastosowanie techniki biometrii w strukturze uwierzytelniania klienta dla telefonicznych biur obsługi ośrodków medycznych**).*

Keywords: Authentication; biometrics;smart card;information system
Słowa kluczowe: uwierzytelnianie, biometria, smart-card, system informacyjny.

Introduction

Recently, telecare is increasingly working as a valuable supplementary way of medicine care from traditional desktop telemedicine platforms [1]. Through a telecare medical information system (TMIS), patients send health message or use portals for health monitoring and healthcare-related services over internet or mobile networks. Since the patients apply TMISs to access the healthcare delivery services, the expense of the patients such as travel cost and the hospitalization time will be significantly reduced. In addition, the telecare server keeps the electronic medical records of registered users. Thus, TMIS helps the physicians make more comprehensive decision via the cooperation of some physicians in different places. Because wireless moblie telecommunications of TMIS are in the open environments, the security issue becomes a significant concern. A secure authentication scheme is essential to guarantee that only the authorized users can access the service from TMIS or the network[2,3,4].

Lamport proposed a password based authentication scheme to deal with the authentication of remote user access [3]. Nowadays, password is one of the most acceptable and widely used authentication mechanisms, e.g., telnet, Kerberos. However, Lamport's scheme is susceptible to dictionary attacks. Later, smart cards have been widely applied to construct the password based authentication schemes. Due to their low cost and portability, smart card based password authentication is one of the most convenient and commonly used authentication techniques [6,7].

Recently, Wu et al. [8] proposed an efficient smart card based password authentication scheme for TMIS. Wu et al. claimed that their scheme is secure and very suitable for TMIS via mobile devices with low computation. But He et al. [9] showed that Wu et al.'s scheme suffers from the impersonation attacks and insider's attacks. To remove the weaknesses, He et al. [9] proposed an improved authentication scheme for TMIS.

Unfortuantely, Wei et al.[10] found that both the schemes [8,9] for TMIS fail to achieve two factor authentication. The adversary can mount off-line password guessing attacks if the adversary has extracted the secret data from the smart card. Wei et al. also proposed an improved scheme for TMIS. Wei et al. claimed their scheme conquers those security weaknesses of the above two schemes.

Subsequently, Zhu [11] showed that Wei et al.'s scheme is also vulnerable to off-line password guessing attacks. Thus, Wei et al.'s scheme does not hold two-factor authentication.

Furthermore, the above mentioned authentication schemes [8-11] require no verification during the password change phase. Thus,if a malicious adversary can access the smart card temporarily, he can mount denial of service attacks by changing the password.

To achieve user anonymity, Wang et al. [12] proposed an authentication and key agreement scheme with user anonymity based on ECC. But Pu et al. [13] demonstrated that in Wang et al.'s scheme, the long-term private key stored in the mobile device will be revealed if an adversary gets the device. Moreover, their scheme needs a smart card producing center to maintain the certificates for users' public keys. Pu et al. propose a generic construction of smart card based password authentication scheme [13]. Their scheme does not need to store or verify others' certificates. However, Pu et al.'s scheme requires the high computation cost. Furthermore, the mutual authentication during the key agreement phase applies a password-based two-party authenticated key agreement scheme to establish a secure high-entropy session key. Therefore, the user and the server must share a password beforehand. Khan et al. [14] also found that Wang et al.'s scheme cannot provide user's anonymity and the user's free choice of a password. In addition, Wang et al.'s scheme suffers from the following security issues: vulnerability to insider attack and no provision for a session key agreement. To address these security flaws, Khan et al. proposed an enhanced authentication scheme. But Chen et al. [15] found that Khan et al.'s scheme still can not protect the user's anonymity. So far, to design an efficient smart card based authentication scheme with anonymity preserving is still a challenging issue.

Based on these motivations, this paper proposes a biometrics-based authentication scheme with key agreement for TMIS by using the smart card. The proposed scheme reduces significantly the execution time of two participants in TMIS. Compared with previous schemes [8-11], the proposed scheme has the following merits: (1) it provides a stronger user authentication function by adopting biometics technique. (2) It provides secure and efficient key

agreement function. (3) It provides free secure password and biometics update function.

The remainder of this paper is organized as follows. Section 2 presents a new password authentication scheme for TMIS using biometics. In Section 3, we analyze its security properties and performance. Finally, conclusion will be given in Section 4.

An authenticated key agreement scheme

In the section, we propose an authentication scheme with key agreement. Notations used in the scheme are defined in Table 1.

Table 1. Notations

U_i	i-th user	S	the telecare server
x	master key of S	$\|\|$	concatenation
ID_i	U_i's identity	$h(\ )$	hash function
PW_i	U_i's Password	$\rightarrow$	message transmission
N_i	random number	B_i	biometric information

The remote telecare server S selects a master key x and a secure one-way hash function $h()$. The authentication scheme is composed of four phases, i.e. registration, login, authentication and key agreement, and password and biometrics update.

1. Registration phase

Step 1. $U_i \rightarrow S$: $\{ID_i, \overline{pw}\}$

The user U_i selects an identity ID_i, a password PW_i and a random number N_i. Then U_i imprints her biometric information B_i and computes $\overline{pw}=h(ID_i||PW_i||B_i||N_i)$, $Z_i=h(N_i||B_i)$.

U_i sends $\{ID_i, \overline{pw}\}$ to the telecare server S through a secre channel.

Step 2. $S \rightarrow U_i$: Smart card

S computes $X_i=h(ID_i||x)$, $Y_i=X_i \oplus h(\overline{pw})$ and stores $\{Y_i,h()\}$ to a smart card. Then S issues the smart card to the user U_i through a secure channel.

Step 3. $U_i \rightarrow$Smart card: $\{N_i,Z_i\}$

U_i inputs $\{N_i,Z_i\}$ to her smart card.

2. Login phase

U_i inserts his smart card into a card reader, keys his identity ID_i and password PW_i and imprints biometric B_i at the sensor. Then the smart card compares $h(N_i||B_i)$ with Z_i. If they are not the same, it outputs rejection message. Otherwise, it outputs acceptance message.

Then the smart card chooses a random nonce r_i and calculates

$$\overline{pw}=h(ID_i||PW_i||B_i||N_i),\ X_i=Y_i \oplus h(\overline{pw}),$$

$$C_i = En_{X_i}(h(r_i \oplus ID_i)||ID_i||r_i),$$

where $En_{X_i}()$ is a symmetric encryption with key X_i.

Next, the smart card sends $\{ID_i, C_i\}$ to S.

3. Authentication and key agreement phase

Step 1. $S \rightarrow U_i$: $\{r_s, a_i\}$

S first decrypts the ciphertext C_i and parses the plaintext into three parts like this:

$$De_{X_i}(C_i)=h_i||ID_i||r_i.$$

And S checks if $h_i=h(r_i \oplus ID_i)$. If the equation does not hold, S refuses the login request. Otherwise, it accepts the login request. Next, S chooses a random nonce r_s and computes

$a_i=h(ID_i||r_i||r_s)$.

Finally, S sends $\{r_s, a_i\}$ back to the smart card.

Step 2. $U_i \rightarrow S$: $\{b_i\}$

Upon receiving the message from the remote telecare server S, the smart card checks if $a_i=h(ID_i||r_i||r_s)$. If the equation holds, the smart card computes $b_i=h(ID_i||r_s||r_i)$.

Then the smart card computes the session key $sk=h(r_i||r_s||ID_i)$ and sends the message $\{b_i\}$ to S.

Step 3. S checks if $b_i=h(ID_i||r_s||r_i)$. If the equation holds, S computes the session key $sk=h(r_i||r_s||ID_i)$.

4. Password and biometrics update phase

If U_i wants to change his password, U_i inserts his smart card and keys his identity ID_i and password PW_i. Then U_i imprints her biometric information B_i. The smart card compares $h(N_i||B_i)$ with Z_i. If they are not the same, it outputs rejection message. Otherwise, U_i carries out the following operations.

(1). U_i selects a random number N_i', keys a new password PW_i' and imprints her biometric information B_i'.

(2). The smart card computes

$$\overline{pw}=h(ID_i||PW_i||B_i||N_i),$$

$$\overline{\overline{pw}}=h(ID_i||PW_i'||B_i'||N_i'),$$

$$Z_i'=h(N_i'||B_i'),\ Y_i'=Y_i \oplus h(\overline{pw}) \oplus h(\overline{\overline{pw}}).$$

(3). The smart card replaces $\{N_i,Y_i,Z_i\}$ with $\{N_i', Y_i', Z_i'\}$,respectively.

Analyses on the proposed scheme

1. Security analyses

In the following, we analyze the security of our scheme. We demonstrate that our scheme resists against some well-known security threats.

We first consider the adversarial model of smart card based authentication scheme for TMIS. Assume that an adversary A gets the full control over the communication channel between the user U_i and the telecare server S (except the registration phase). Thus, A could obtain all the messages transmitted between U_i and S (except the registration message). Of all the four phases in a smart card based authentication scheme for TMIS, only the registration phase requires a secure channel between U_j and S. For other phases, there could be various kinds of passive and active adversaries in the communication channel between U_i and S. The adversary can eavesdrop on the communication, modify messages, remove messages or insert messages into the communication channel. Its objective is to compromise mutual authentication between U_i and S. For example, the adversary even impersonates U_i to access S, or the adversary impersonates S to provide U_i with false service. To simulate the insider attack, if a user is under attack, A is allowed to obtain the passwords and extract the information stored in the smart-cards of all the users except the user under attack.

For a smart card based authentication scheme, one basic security property is that the user is required to have both the smart-card and the password, which is often called two-factor authentication. Since Messerges et al. [16] and Kocher et al. [17] pointed out that the smart-cards cannot prevent the information stored in them from being extracted by monitoring their power consumption [18], their security is always discussed in the case that the smart card is stolen. In other words, when a user is under attack, we also allow the adversary A to either compromise the password or the smart-card of the user under attack, but not both.

Theorem 1. *The proposed scheme provides user authentication*.
Proof: In the proposed scheme, the smart card identifies the validity of the user by checking if $h(N_i||B_i)=Z_i$. Due to the one-wayness and collision resistance of hash function, only the user U_i can imprint B_i.

Next, S authenticates the user by checking if $h_i=h(r_i \oplus ID_i)$. The random nounce r_i is contained in the ciphertext C_i. Although ID_i is transmitted over the open channel, even if h_i is obtained, it is computationally infeasible to generate a random nounce r_i which satisfies $h_i=h(r_i \oplus ID_i)$. In essence, h_i is also contained in the ciphertext C_i. Only the entity who knows X_i can decrypt C_i and further get h_i. Since an adversary does not have the master key x, he has to compute the encryption key X_i through $X_i = Y_i \oplus h(ID_i||PW_i||B_i||N_i)$. Suppose that the adversary has stolen the smart card, he obtains the message $\{Y_i, N_i\}$ stored in the card and ID_i .The adversary still cannot work out X_i. This is because the adversary does not know $\{PW_i, B_i\}$ while X_i also depends on $\{PW_i, B_i\}$.

Therefore, the proposed scheme provides the strong user authentication. The telecare server is sure that the service requestor is indeed a registered user as the user claims.

Theorem 2. *The proposed scheme provides server authentication*.
Proof: We first show that the proposed scheme prevents any adversary from obtaining the server's master secret key. The secret key x is hashed in the form $h(ID_i||x)$. Upon the assumptions of collision-resistant hash functions, an adversary cannot extract x from $h(ID_i||x)$.

Next, it is infeasible that an adversary cheats a user U_i by masquerading as S. Since the adversary does not have the master key x, the adversary cannot decrypt C_i. Thus, the adversary cannot obtain r_i. Therefore, it is infeasible to generate a valid pair $\{r_s,a_i\}$. When an adversary chooses randomly r_s and sends a response message back to the smart card, the smart card will find that the response is not from S. This is because the verification equation $a_i=h(ID_i||r_i||r_s)$ will not hold at probability 1.

Therefore, the proposed scheme can authenticate the server S. The user is sure that the server is indeed the one who the user wants to access. □

Theorem 1 and Theorem 2 imply that the proposed scheme also can resist against the man-in-the-middle attacks.

Theorem 3. *The proposed scheme provides secure password and biometrics update*.
Proof: Before the user updates the password and biometrics, the smart card will compares $h(N_i||B_i)$ with the stored Z_i. Only the valid user can continue the update phase. The verification prevents any malicious adversary from mounting denial of service attacks by changing the password and biometrics.

The password and biometrics can freely be updated by the smart card holder (a registered user U_i) at will without any interaction with the server. The server can be totally unaware of the password and biometrics change. □

Theorem 4. *The proposed scheme can resist the stolen verifier attacks.*
Proof: In the proposed scheme, the telecare server does not maintain a user verification table or a password table. No user verifiable information can be obtained from the server S. So the proposed scheme can prevent the stolen verifier attack.

Theorem 5. *The proposed scheme can resist off-line password guessing attacks.*
Proof: Without loss of generality, assume that an adversary obtains a smart card but the password of the user is kept secret to the adversary. Then the adversary can extract the information $\{Y_i,h(),N_i, Z_i\}$ stored in the smart card. The password is protected in the card as $h(ID_i||x) \oplus h(ID_i||PW_i||B_i||N_i)$. The message $\{ID_i,C_i\}$ is transmitted. The adversary cannot work out the key $h(ID_i||x)$ from the ciphtertext C_i which is changing with fresh random value r_i. Therefore, even if an adversary has extracted the message and intercepted the transmitted message, he still can not obtain a verification function about the password from the stored information $h(ID_i||x) \oplus h(ID_i||PW_i||B_i||N_i)$.

For a passive adversary, the adversary can not calculate $\{r_i, N_i, x, B_i\}$ to verify the candidate password through the transmitted messgage $\{ID_i,C_i\}$. This also makes off-line password attack impossible for a passive adversary.

The password is not applied to compute any authentication message. Thus, the undetectable on-line password guessing attack will not work.

The above analyses show that the proposed scheme can resist against password guessing attacks and achieve true two-factor authentication.□

Theorem 6. *The proposed scheme can resist impersonation attacks.*
Proof: If an adversary attempts to impersonate a legal user U_i, he has to generate a correct ciphtertext C_i. Since $X_i=Y_i \oplus h(ID_i||PW_i||B_i||N_i)$ or $X_i=h(ID_i||x)$, we know from the analysi of Theorem 1 and Theorem 2 that it is infeasible for the adversary to obtain X_i. Thus, the adversary chooses a random nonce r_i, a key X and encrypts $h(r_i \oplus ID_i)||ID_i||r_i$ with the key X. Next, he adversary sends the ciphertext and ID_i to the server S. Obviously, since two keys X and X_i are different, the server S decrypts the ciphtertext and will obtain a different hash function. Thus, the server S will identify that the service requester is not a registered user.

Hence, our authentication scheme for TMIS can resist against impersonation attacks. □

Theorem 7. *The proposed scheme can resist insider attacks.*
Proof: In the proposed scheme, since the user uses $h(ID_i||PW_i||B_i||N_i)$ instead of PW_i during the registration phase and $\{B_i, N_i\}$ is kept secret from the server, the server can never find out the user's password. Thus, some insider attacks are avoided.

Now, we consider the impersonation attack in the following case: a malicious user U_j attempts to impersonate a user U_i who has ever accessed the server S. In order to impersonate the user U_i to login the server, the malicious user chooses a random nonce r_i and calculates C_i. However, the message C_i is generated by encryption with the key X_i. Due to the one-wayness and collision resistance of hash function, the user U_j can not extract x from her secret value $X_j=h(ID_j||x)$. Thus the malicious user U_j can not compute X_i. By the similar anlysis in Theorem 6, it is infeasible for U_j to generate the valid login message $\{ ID_i, C_i\}$. □

Theorem 8. *The proposed scheme can resist replay attacks.*
Proof: The proposed scheme uses two fresh random values r_i and r_s to protect against replay attacks during the login phase and authentication and key agreement phase, respectively. Assume that an adversary intercepts the message $\{ID_i,C_i\}$ and attempts to impersonate U_i by replaying it. However, after receiving the message $\{r_s, a_i\}$,

since the adversary has no knowledge of r_i, he cannot compute the correct value $b_i=h(ID_i||r_s||r_i)$ with a fresh r_s. The value b_i is used by the server to confirm that the service requester has the right value of r_i. Then S can easily detect the replay attacks by checking if $b_i=h(ID_i||r_s||r_i)$.

2. Performance and functionality analyses

Due to the resource constraints of smart card, the password based smart card authentication scheme must take efficiency into consideration. In this section, we will evaluate the performance of the proposed scheme and make comparison with some authentication schemes for TMISs [8-11]. We evaluate the efficiency in terms of computation cost. A comparison of the efficiency and security features of our scheme with those schemes is given in Table 2.

To analyze the computational complexity of the schemes, we define T_s, t_e, t_{inv}, t_h, t_{sym} and t_m be the time cost of one scalar multiplication in a group, one modular exponentiation in Z_p, one inverse operation in Z_q, one hash operation, one symmetric encryption or decryption operation, and one modular multiplication in Z_q, respectively. According to [19-22], the time cost of all operations satisfies the following: $T_s \approx 29t_h$, $t_h \approx t_m$, and $t_e \approx t_{inv} \approx 240t_m$, $t_{sym} \approx 2.25t_h$.

The smart card based authentication schemes consist of four phases: registration, login, authentication and key agreement, and password and biometrics update. We list the computaion cost in all the phases in Table 2 of the smart card based authentication schemes [8-11] for the user (smart card) and the remote medical server,repectively.

In the proposed scheme, each entity needs to carry out two hash function operations during the registration phase. During the login and authentication phases, the smart card requires one symmetric encryption and five hash function operations, while the telecare server requires one symmetric decryption operation and four hash function operations. During the password and biometrics update phase, the smart card takes three hash operations. Compared with the previous schemes above mentioned, the user or the smart card needs one more or two more hash operations. Since the password and biometrics update phase in our scheme can provide the verification function, the smart card needs one more hash operations to update password and biometrics than the schemes [10,11]. Although the schemes [8,9] cannot provide the verification during the password update phase, the smart card in [9] needs two hash operations, one inverse operation, one modular multiplication in Z_q, one modular exponentiation, while the smart card in [11] needs two inverse operations, two modular multiplications in Z_q, two modular exponentiation operations. In the proposed scheme, the total computation cost for smart card is equivalent to about 12 hash function opeations, while the total computation cost for smart card is equivalent to about 8 hash function opeations. By contrast, the total computation cost for smart card in [8-11] is equivalent to about 969 hash function opeations, 970 hash function opeations, 278 hash function opeations and 247 hash function opeations, respectively. The total computation cost for the telecare server in [8-11] is equivalent to about 1206 hash function opeations, 965 hash function opeations, 754 hash function opeations and 245 hash function opeations, respectively. The comparison in Table 2 clearly indicates that the proposed scheme achieves high efficiency. Both the user and the telecare server take much less computation to accomplish the mutual authentication and key agreement than the previous smart card based authentication schemes for TMIS [8-11].

We list the function features of the schemes present in [8-11] and the proposed scheme in Table 3. It demonstrates that our scheme can achieve the essential requirements for a secure authentication scheme for TMIS.Those smart card based authentication schemes for TMIS in [8-11] cannot provide the verification function during the password change phase. This will lead to the denial of service attacks by changing the password. In addtion, the schemes in [8-10] are vulnerable to offline password guessing attacks. Thus, they cannnot provide the two-factor authentication.

Table 2 Comparison of computation cost

		[8]	[9]	[10]	[11]	Proposed scheme
Registration phase	Smart card	0	t_h	t_h	t_h	$2t_h$
	Server	$3t_e+t_{inv}+2t_m \approx 962t_h$	$t_e+t_{inv}+t_h \approx 481t_h$	$t_e \approx 240t_h$	t_h	$2t_h$
Login and authentication phase	Smart card	$4t_h+3t_m \approx 7t_h$	$t_e+t_{inv}+5t_h+t_m \approx 486t_h$	$t_e+6t_h+T_s \approx 275t_h$	$t_e+4t_h \approx 244t_h$	$5t_h+t_{sym} \approx 7.25t_h$
	Server	$t_e+4t_h \approx 244t_h$	$t_e+t_{inv}+4t_h \approx 484t_h$	$t_e+t_{inv}+5t_h+T_s \approx 514t_h$	$t_e+4t_h \approx 244t_h$	$4t_h+t_{sym} \approx 6.25t_h$
Password update phase	Smart card	$2t_e+2t_{inv}+2t_m \approx 962t_h$	$t_e+t_{inv}+2t_h+t_m \approx 483t_h$	$2t_h$	$2t_h$	$3t_h$

Table 3 Comparison of function features

	[8]	[9]	[10]	[11]	Proposed scheme
Offline password guessing attack	×*	×*	×※	√	√
Two-factor authentication	×*	×*	×※	√	√
Impersonation attack	×△	√	√	√	√
Insider attack	×△	√	√	√	√
Verification in password update phase	×	×	×	×	√
Key agreement	√	√	√	×	√

Note: * denotes the attack is found in [10]; △ denotes the attack is found in [9]; ※ denotes the attack is found in [11].

Conclusions

In the paper, we have proposed an efficient biometrics-based authentication scheme for telecare medicine information systems. Security analyses have showed that the proposed scheme can withstand various possible attacks and achieve the stronger security. The functionality comparison shows that our scheme holds the advantages over the previous smart card based authentication schemes for TMIS. Our scheme is very efficient. Dynamic identity based authentication schemes can provide anonymity. However, Wang et al.'s scheme, Pu et al.'s scheme and Khan et al.'s scheme have some security issues. Future work is to design secure dynamic identity authentication schemes for TMIS with high efficiency.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China under Grant No. 61163053 and Natural Science Foundation of Jiangxi Province (20122BAB201035).

REFERENCES

[1] Al Ameen, M. Liu, J., Kwak,K., Security and privacy issues in wireless sensor networks for healthcare applications, *J Med Syst*,(36)(2012,93–101

[2] Adamsk, T., Winiecki, W., Entity identification algorithms for distributed measurement and control systems with asymmetry of computational power, *Prz Elektrotechniczn*,(2008),No. 05

[3] Cheng, X.R., Li, M.X., The authentication of the grid monitoring system for wireless sensor networks, *Prz Elektrotechniczn*, (2013),No.01a

[4] Pejaś, J., El Fray , I., Ruciński, A., Authentication protocol for software and hardware components in distributed electronic signature creation system, *Prz Elektrotechniczn*, (2012),No.10b

[5] Lamport, L., Password authentication with insecure communication, *Commun ACM*, 24(1981),28-30

[6] Hwang, M.S., Li, L.H., A new remote user authentication scheme using smart cards,*IEEE Trans. Consum. Electron*, 46(2000),No.1, 28-30

[7] Das, M.L., Saxena, A., Gulati, V.P. A dynamic id-based remote user authentication scheme,*IEEE T Consum Electr*, 50(2004),No.2, 629-631

[8] Wu, Z. Y., Lee, Y. C., Lai, F., Lee H. C., Chung, Y., A secure authentication scheme for telecare medicine information systems, *J. Med. Syst.* doi: 10.1007/s10916-010-9614-9, 2010.

[9] He, D. B., Chen, J. H., and Zhang, R., A more secure authentication scheme for telecare medicine information systems, *J.Med. Syst.* doi: 10.1007/s10916-011-9658-5, 2011

[10] Wei, J., Hu, X., Liu, W., An improved authentication scheme for telecare medicine information systems,*J. Med. Syst.* doi: 10.1007/s10916-012-9835-1, 2012

[11] Zhu,Z., An Efficient authentication scheme for telecare medicine information systems,*J. Med. Syst.* doi:10.1007/s10916-012-9856-9, 2012

[12] Wang, R.-C., Juang, W.-S., Lei, C.-L., Provably secure and efficient identification and key agreement protocol with user anonymity,*J Comput Syst Sci,* doi:10.1016/j.jcss.2010.07.004. 2010

[13] Pu, Q., Wang, J., Zhao, R.-Y., Strong authentication scheme for telecare medicine information systems, *J Med Syst*,36(2012),2609–2619

[14] Khan, M. K., et al., Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme,*Comput. Commun.* 34(2010), No.3, 305–309

[15] Chen, H.-M., Lo,J.-W., Yeh, C.-K., An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems, *J Med Syst*, DOI 10.1007/s10916-012-9862-y

[16] Messerges, T.S., Dabbish, E.A., Sloan, R.H., Examining smart-card security under the threat of power analysis attacks, *IEEE T Comput*, (51)2002.,No.5,541-552

[17] Kocher, P., Jaffe, J., Jun, B., Differential power analysis,*Advances in Cryptology-CRYPTO'99*, Santa Barbara, California, USA, August 15-19, 1999. Lecture Notes in Computer Science 1666, Springer, ISBN 3-540-66347-9, 388-397,1999

[18] Bayam, K. A., Ö rs, B., Differential power analysis resistant hardware implementation of the RSA cryptosystem, *Turk J Elec Eng & Comp Sci*, (18)2010,No.1, 129-140

[19] Fan, Ch.-I. Sun, Huang, W. Z., Vincent, S.-M.,Provably secure randomized blind signature scheme based on bilinear pairing,*Comput Math Appl*, 2010, No.60,285–293

[20] Koblitz, N., Menezes, A.J., Vanstone, S.A.,The state of elliptic curve cryptography, *Design Code Cryptogr*, (19)2000, No.2-3, 173–193

[21] Xue,K.M.,Hong, P.L., Security improvement on an anonymous key agreement protocol based on chaotic maps, *Commun Nonlinear Sci Numer Simulat*, 2012, No.17, 2969–2977

[22] Menezes, A., Van Oorschot, P. C., Vanstone, S. *Handbook of Applied Cryptography*, CRC Press, USA,1997.

***Authors**: Dr. Zuowen Tan, School of Information Technology, Jiangxi University of Finance & Economics,Nanchang, 30032, China, tanzyw@gmail.com*