

## PROTECTION OF TELE CARE INFORMATION FOR STRONG ROBUSTNESS WITH REMOTE THREE-FACTOR AUTHENTICATION

D.Saranya<sup>1</sup> - (PG)Scholar<sup>1</sup>, [saranyadayalraj@gmail.com](mailto:saranyadayalraj@gmail.com);  
Dr.S.Chakaravarthi<sup>1</sup> Assistant Professor-III, [Chakra2603@gmail.com](mailto:Chakra2603@gmail.com) ;  
Masters of Engineering,  
Department of Computer Science and Engineering,  
Velammal Engineering College, Chennai, India.

### Abstract—

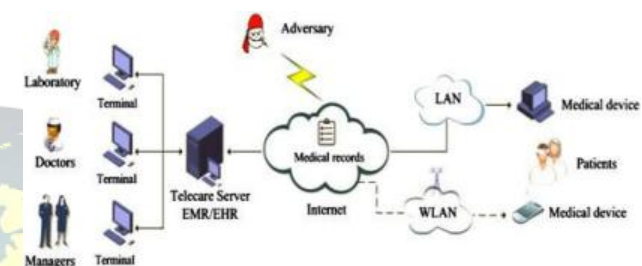
Telecare medicine information systems (TMIS) provide flexible and convenient e-health care. However, the medical records transmitted in TMIS are exposed to unsecured public networks, so TMIS are more vulnerable to various types of security threats and attacks. To provide privacy protection for TMIS, a secure and efficient authenticated key agreement scheme is urgently needed to protect the sensitive medical data. In the existing paper, the demonstration of Mishra *et al.*'s scheme suffers from replay attacks, man-in-the-middle attacks and fails to provide perfect forward secrecy. If the server fails, the transfer of information to another multi server may lead to robustness problem. To overcome this problem, we propose the remote three-factor authentication protocol by the efficient algorithm which provide the robustness. This also provide the Security analysis demonstrate, that the proposed scheme resists various attacks and provides several attractive security properties. Performance evaluation shows that the proposed scheme increases efficiency in comparison with other related schemes. The secure three-factor authentication protocol for multi-server environment based on Chebyshev chaotic map and secure sketch algorithm. To verify the security of the proposed scheme, we simulate our scheme using BAN logic and ProVerif tool. Through a thorough analysis, we can see that the proposed scheme not only has stronger security but also has less computation cost than the existing one.

**KEYWORDS:**—Secure three-factor authentication, Chebyshev chaotic maps, secure sketch, BAN logic, ProVerif, telecare medicine information systems(TMIS).

### 1.INTRODUCTION

ADVANCES in information technology and environmental concerns boost the rapid development of electronic medical record/electronic health record (EHR) systems, collect, store, manage, and share patient's healthcare associated information. Compared with traditional paper-based method, EMR/EHR provides low cost, high quality, and more flexible medical records. Owing to this transmission, telecare medicine information systems (TMIS) have been deployed to provide healthcare delivery services by accessing EMR/EHR via the public network like Internet. In a typical medical application scenario of TMIS, patients submit their healthcare data to a telecare server via wired/wireless medical devices in their home. After receiving the patient's medical records, the doctors perform the diagnosis at their clinical center, and then, transform the final clinical decisions and treatments to the patients through the Internet. Since the TMIS realizes

geographical distance, it attracts great attention and spreads into the market quickly



### Typical medical application scenario of TMIS

The sensitive medical records transmitted over the Internet are not protected in most TMIS environments, and various attacks could be launched successfully by malicious adversaries. To protect patient's medical records, TMIS-based healthcare should satisfy fundamental security and privacy requirements such as authentication, confidentiality, integrity, and user anonymity. As the authentication mechanism can prevent the medical resources from being accessed by malicious attackers and the session key used to encrypt the packets can ensure the confidentiality of EMR/HER, many authenticated key agreement schemes have been developed to protect medical records security and preserve patient's privacy. For example, the authentication schemes for HIPAA privacy and security regulations.

To enhance the security while still preserve the efficiency of Mishra *et al.*'s scheme in this study, we develop an improved authenticated key agreement scheme for TMIS, which enables the patients to enjoy the remote healthcare services securely and anonymously. Although Amin *et al.* presented an improvement scheme based on Mishra *et al.*'s scheme, their scheme suffered from the known session specific temporary information attack and increase the computational costs. In order to achieve a delicate balance between performance and security, chaotic map-based cryptography is employed in the proposed scheme. Since chaotic map operations possess the semigroup property, it is more efficient than modular exponential computation and point multiplication operations of elliptic curve. The proposed three-factor authentication scheme not only achieves mutual authentication and key agreement by using Chebyshev chaotic map but also enhances the performance in comparison with other related schemes.

However, this case may lead to other security problems such as attacker or the administrator of RC can delete user's information stored in data table and then register to RC by the victim's identity. In our scheme, we introduce timestamps to



authentication phase, we can complete the authentication between the user and the application without the participation of the RC. This case can increase greatly the robustness of the whole system. In order to solve the problem of fuzzy character of biometrics, we introduce the secure sketch scheme. From the analysis, we can see that secure sketch scheme consume less computational work than fuzzy extractors scheme.

## **2.RELATED WORKS**

### **2.1. Design and implementation of a telecare information platform:**

For the aging population and for people with dominant chronic diseases, countries all over the world are promoting an "Aging in Place" program with its primary focus on the implementation of telecare. In 2009, Taiwan held a "Health Care Value-Added Platinum Program" with the goal of promoting the development of "Telecare" services by integrating medical treatment, healthcare, information communication, medical equipments and materials and by linking related cross-discipline professions to enable people to familiarize themselves with preventive healthcare services offered in their household and community environments. In addition, this program can be utilized to effectively provide diversified healthcare service benefitting society as a whole. This study aims to promote a diversified telecare service network in Taiwan's household and community environments, establish telecare information platforms, build an internal network of various healthcare service modes, standardize externally interfacing telecare information networks, effectively utilize related healthcare service resources, and complete reasonable service resource links forming an up-to-date health information exchange network. To this end, the telecare information platform based on service oriented architecture (SOA) is designed to promote an open telecare information interface and sharing environment to assist in such tasks as developing healthcare information exchange services, integrating service resources among various different healthcare service modes, accessing externally complex community affairs information, supporting remote physiological information transmissions, and providing diversified remote innovative services. Information system architecture and system monitoring indices of various types of healthcare service modes are used for system integrations for future development and/or expansions.

### **2.2. An event-based notification approach for the delivery of patient medical information**

Data sharing is pivotal in current medical practice so as to better treat patients by taking the best medical decisions, and to optimize healthcare costs by reducing the need to repeat unnecessary medical tests and by better managing healthcare structures. To improve the delivery of treatment outcomes and test results, the request-triggered retrieval of clinical documents provided by current Health Information Systems is not sufficient. The addition of a notification solution is necessary to inform users as soon as their clinical documents

of interest have been produced so that they can retrieve them by means of the traditional Health Information Systems. In addition, this notification solution also has to implement the event-based information exchange patterns, which characterize the current attempts at integrating heterogeneous Health Information Systems in a seamless manner.

### **2.3 Electronic health records implementation: An evaluation of information system impact and contingency factors:**

A systematic literature review was conducted from peer-reviewed scholarly journal publications from the last 10 years (2001–2011). The search was conducted using various publication collections including: Scopus, Embase, Informit, Medline, Proquest Health and Medical Complete. This paper reports on our analysis of previous empirical studies of EHR implementations. We analysed data based on an extension of DeLone and McLean's information system (IS) evaluation framework. The extended framework integrates DeLone and McLean's dimensions, including information quality, system quality, service quality, intention of use and usage, user satisfaction and net benefits, together with contingent dimensions, including systems development, implementation attributes and organisational aspects, as identified by Van der Meijden and colleagues.

### **2.4 Three-Factor Anonymous Authentication and Key Agreement Scheme for Telecare Medicine Information Systems**

Nowadays, with comprehensive employment of the internet, healthcare delivery services is provided remotely by telecare medicine information systems (TMISs). A secure mechanism for authentication and key agreement is one of the most important security requirements for TMISs. Recently, a user anonymity preserving three-factor authentication scheme for TMIS. The present paper shows that Tan's scheme is vulnerable to replay attacks and Denial-of-Service attacks. In order to overcome these security flaws, a new and efficient three-factor anonymous authentication and key agreement scheme for TMIS is proposed. Security and performance analysis shows superiority of the proposed scheme in comparison with previously proposed schemes that are related to security of TMISs.

### **2.5 Cryptanalysis of crypt-analysis and improvement of Yan et al. biometric-based authentication scheme for TMIS:**

Remote user authentication is critical requirement in Telecare Medicine Information System (TMIS) to protect the patient personal details, security and integrity of the critical medical records of the patient as the patient data is transmitted over insecure public communication channel called Internet. In 2013, Yan proposed a biometric based remote user authentication scheme and claimed that his scheme is secure. Recently, Dheerendra et al. demonstrated some drawbacks in Yan et al scheme and proposed an improved scheme to erase the drawbacks of Yan et al scheme. We analyze Dheerendra et al scheme and identify that their scheme is vulnerable to off-



line identity guessing attack, and on successfully mounting it, the attacker can perform all major cryptographic attacks.

**2.6 Cryptanalysis and improvement of Yan et al.'s biometric-based authentication scheme for telecare medicine information systems:**

Remote user authentication is desirable for a Telecare Medicine Information System (TMIS) for the safety, security and integrity of transmitted data over the public channel. In 2013, Tan presented a biometric based remote user authentication scheme and claimed that his scheme is secure. Recently, Yan et al. demonstrated some drawbacks in Tan's scheme and proposed an improved scheme to erase the drawbacks of Tan's scheme. We analyze Yan et al.'s scheme and identify that their scheme is vulnerable to off-line password guessing attack, and does not protect anonymity. Moreover, in their scheme, login and password change phases are inefficient to identify the correctness of input where inefficiency in password change phase can cause denial of service attack. Further, we design an improved scheme for TMIS with the aim to eliminate the drawbacks of Yan et al.'s scheme. [11] discussed about a system, In this proposal, a neural network approach is proposed for energy conservation routing in a wireless sensor network. Our designed neural network system has been successfully applied to our scheme of energy conservation. Neural network is applied to predict Most Significant Node and selecting the Group Head amongst the association of sensor nodes in the network. After having a precise prediction about Most Significant Node, we would like to expand our approach in future to different WSN power management techniques and observe the results. In this proposal, we used arbitrary data for our experiment purpose; it is also expected to generate a real time data for the experiment in future and also by using adhoc networks the energy level of the node can be maximized. The selection of Group Head is proposed using neural network with feed forward learning method. And the neural network found able to select a node amongst competing nodes as Group Head.

**2.7 A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity:**

Telecaremedical information system (TMIS) makes an efficient and convenient connection between patient(s)/user(s) and doctor(s) over the insecure internet. Therefore, data security, privacy and user authentication are enormously important for accessing important medical data over insecure communication. Recently, many user authentication protocols for TMIS have been proposed in the literature and it has been observed that most of the protocols cannot achieve complete security requirements. In this paper, we have scrutinized two (Mishra et al., Xu et al.) remote user authentication protocols using smart card and explained that both the protocols are suffering against several security weaknesses. We have then presented three-factor user authentication and key agreement protocol usable

for TMIS, which fix the security pitfalls of the above mentioned schemes. The informal cryptanalysis makes certain that the proposed protocol provides well security protection on the relevant security attacks. Furthermore, the simulator AVISPA tool confirms that the protocol is secure against active and passive attacks including replay and man-in-the-middle attacks. The security functionalities and performance comparison analysis confirm that our protocol not only provide strong protection on security attacks, but it also achieves better complexities along with efficient login and password change phase as well as session key verification property.

**2.8 Robust ECC-based authenticated key agreement scheme with privacy protection for telecare medicine information systems:**

To protect the transmission of the sensitive medical data, a secure and efficient authenticated key agreement scheme should be deployed when the healthcare delivery session is established via Telecare Medicine Information Systems (TMIS) over the insecure public network. Recently, Islam and Khan proposed an authenticated key agreement scheme using elliptic curve cryptography for TMIS. They claimed that their proposed scheme is provably secure against various attacks in random oracle model and enjoys some good properties such as user anonymity. In this paper, however, we point out that any legal but malicious patient can reveal other user's identity. Consequently, their scheme suffers from server spoofing attack and off-line password guessing attack. Moreover, if the malicious patient performs the same time of the registration as other users, she can further launch the impersonation attack, man-in-the-middle attack, modification attack, replay attack, and strong replay attack successfully. To eliminate these weaknesses, we propose an improved ECC-based authenticated key agreement scheme. Security analysis demonstrates that the proposed scheme can resist various attacks and enables the patient to enjoy the remote healthcare services with privacy protection. Through the performance evaluation, we show that the proposed scheme achieves a desired balance between security and performance in comparisons with other related schemes.

**2.9 Two-factor remote authentication protocol with user anonymity based on elliptic curve cryptography:**

In order to provide secure remote access control, a robust and efficient authentication protocol should realize mutual authentication and session key agreement between clients and the remote server over public channels. Recently, Chun-Ta Li proposed a password authentication and user anonymity protocol by using smart cards, and they claimed that their protocol has satisfied all criteria required by remote authentication. However, we have found that his protocol cannot provide mutual authentication between clients and the remote server. To realize 'real' mutual authentication, we propose a two-factor remote authentication protocol based on elliptic curve cryptography





in this paper, which not only satisfies the criteria but also bears low computational cost. Detailed analysis shows our proposed protocol is secure and more suitable for practical application.

### 2.10 Cryptanalysis of a chaotic map-based password-authenticated key agreement protocol using smart cards:

Chaotic maps have been applied in the design of authenticated key agreement protocols, which allow communication parties to exchange session keys in an authentic and secure manner. Guo and Chang recently proposed a novel password-authenticated key agreement protocol using smart card based on chaotic maps. They claimed that the protocol achieves the security goal of mutual authentication, as well as other essential security requirements. We show that this protocol is susceptible to key-compromise impersonation and parallel session attacks. We also identify two weaknesses in the password change phase of the protocol that leads to authentication with old password and denial of service, respectively. [7] discussed about a method, Optimality results are presented for an end-to-end inference approach to correct (i.e., diagnose and repair) probabilistic network faults at minimum expected cost. One motivating application of using this end-to-end inference approach is an externally managed overlay network, where we cannot directly access and monitor nodes that are independently operated by different administrative domains, but instead we must infer failures via end to-end measurements. We show that first checking the node that is most likely faulty or has the least checking cost does not necessarily minimize the expected cost of correcting all faulty nodes. In view of this, we construct a potential function for identifying the candidate nodes, one of which should be first checked by an optimal strategy. Due to the difficulty of finding the best node from the set of candidate nodes, we propose several efficient heuristics that are suitable for correcting fault nodes in large-scale overlay networks. We show that the candidate node with the highest potential is actually the best node in at least 95% of time, and that checking first the candidate nodes can reduce the cost of correcting faulty nodes as compared to checking first the most likely faulty nodes.

## 3. TECHNIQUE USED :

### 3.1 The robustness of the scheme:

Compared with the Odelu-Das-Goswami's scheme, our scheme doesn't need the RC to participate in the login and authentication phase. This design can greatly improve the robustness of our scheme because improper work has slightest effect on the whole scheme.

### 3.2 BAN LOGIC:

In this section, we adopt Burrows-Aba-di-Needham (BAN) logic [25-26] to prove that the proposed scheme can achieve a session key between user and application server.

- (I) A believes a statement  $X$
- (II) The key  $K$  is shared between user and server
- (III)  $X$  is fresh
- (IV) A sees or receives  $X$
- (V) A said or sent  $X$
- (VI) The value of  $X$  and  $Y$  are encrypted by the key  $k$
- (VII) The value of  $X$  and  $Y$  are hashed by the key  $k$
- (VIII)  $X$  is XORed with the key  $K$

### 3.3 Formal security validation using proverif :

In this section, we prove the security of our proposed scheme using ProVerif which is an automated formal tool [27]. ProVerif is based on applied calculus and can be used to verify authentication and secrecy properties [28]. There are three parts in the ProVerif: (1) declaration part; (2) process part; and (3) main part. We perform the ProVerif code in the online demo for ProVerif (<http://proverif.rocq.inria.fr/index.php>). The performance results as shown in the Fig 5. From the experimental results, we can see that our proposed scheme is security.

### 3.4 Performance analysis:

The length of identity is 32bits[21];  $L_H$ : The length of hash function is 160bits[21];  $L_M$ : The output size of chaotic maps is 128 bits because it is long enough if we select the prime number  $p$  as 128bits in the proposed scheme;  $L_T$ : The length of time is 128bits because it can be considered as a random number [21];  $L_E$ : The length of symmetric encryption/decryption is 128bits [21];  $L_P$ : The output size of an elliptic curve point  $P=(P_x, P_y)$  is 320bits [21];  $L_B$ : The length of biometrics is 128bits [31];  $L_{key}$ : The length of key is about 1024bits[31].

S1: Server Registration Phase; U2: User Registration Phase; C3: Login And Authentication Phase; C4: Total

We measure the consumption time Fuzzy Extractors algorithm, Secure Sketch algorithm, MD5 and DES algorithm on an Intel Core i5-3470 platform. The details are

*Comparison of computational cost in the registration phase*

	Odelu [21]	Irshad [29]	Chuang [30]	Proposed scheme
C1	$T_{Gen}+T_h$	$T_h$	$2T_h$	$T_{SS}+2T_h$
C2	0	0	0	0
C3	$T_x+5T_h$	$3T_h$	$3T_h+2T_M+T_X$	$3T_h+T_X+T_M$
C4	0.78679 sec	0.00388 sec	0.34435 sec	0.95557 sec



#### Comparison of computational cost in the login and authentication phase

	Odelu [21]	Irshad [29]	Chuang [30]	Proposed scheme
$T_x + 7T_h + T_{operator} + T_{meRe}$				
C1	$5T_x + 8T_h$	$2T_x + 5T_h + 4T_M$	$3T_x + 8T_h + T_{Rec} + 4T_M$	
C2	$T_D + 6T_h + T_E + 2T_{PM}$	$2T_x + 8T_h$	$T_x + 4T_h + 4T_M$	$2T_x + 6T_h + 4T_M$
C3	$2T_D + 11T_h + T_E + T_{PM}$	0	0	0
C4	0.28958 sec	0.01552 sec	1.36673 sec	1.55158 sec

#### Comparison of performance

	Odelu [21]	Irshad [29]	Chuang [30]	Proposed scheme
S1	$L_{ID} + 2L_H$	$L_{key}$	$L_{ID} + L_H + L_M$	$L_{ID} + L_T + L_H + L_M$
U2	$L_{ID} + 3L_H$	$L_{ID} + L_H$	$L_{ID} + 2L_H$	$L_{ID} + L_T + 2L_H$
C3	$3L_P + 4L_E + 6L_H$	$3L_{ID} + 5L_H + 2L_{key} + L_B$	$2L_M + 3L_H + 2L_T$	$L_T + 4L_H + 2L_M$
C4	3080 bits	8428 bits	1664 bits	1952 bits

#### 4. CONCLUSION:

we have presented some flaws of the Odelu-Das-Goswami's scheme. In order to solve these problems, secure biometric-based remote three-factor authentication with Chebyshev chaotic map and secure sketch scheme has been proposed. From the analysis, we can see that the proposed scheme has higher security and deals with biometric more appropriately compared with Odelu-Das-Goswami's scheme and other similar schemes. What's more, the proposed scheme has less computation cost than Odelu-Das-Goswami's scheme. At the same time, our scheme can achieve session key agreement and has stronger robustness than Odelu-Das-Goswami's scheme also.

In the future, we will continue to further study three-factor schemes in multi-server environment. These schemes should

become more reasonable and more effective compared with the proposed scheme in this paper. More-over, we will build a biometric-based authentication tested and extend our scheme for body area and the network.

#### 6. REFERENCE :

- [1] Wang B, Ma M. "A smart card based efficient and secured multi-server authentication scheme". Wireless Personal Communications, vol.68, no. 2, pp. 361-378, 2013.
- [2] Li X, Xiong Y, Ma J, et al. "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards". Journal of Network and Computer Applications, vol. 35, no. 2, pp. 763-769, 2012.
- [3] Li X, Ma J, Wang W, et al. "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments". Mathematical and Computer Modelling, vol. 58, no. 1, pp. 85-95, 2013.
- [4] Yoon E J, Yoo K Y. "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem". The Journal of Supercomputing, vol. 63, no. 1, pp 235-255, 2013.
- [5] Shen H, Gao C, He D, et al. "New bio - metrics-based authentication scheme for multi-server environment in critical systems[J]. Journal of Ambient Intelligence and Humanized Computing", vol. 6, no. 6, pp. 825-834, 2015.
- [6] Tsai J L, Lo N W. "A chaotic map based anonymous multi-server authenticated key agreement protocol using smart card". International Journal of Communication Systems, vol. 28, no. 13, pp. 1955-1963, 2015.
- [7] Christo Ananth, Mona, Kamali, Kausalya, Muthulakshmi, P.Arthy, "Efficient Cost Correction of Faulty Overlay nodes", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1, Issue 1, August 2015, pp:26-28
- [8] Zhu H. "A Provable One-way Authentication Key Agreement Scheme with User Anonymity for Multi-Server Environment". TIIS, vol. 9, no. 2, pp 811-829, 2015.
- [9] Zhang M, Zhang J, Zhang Y. "Remote three factor authentication scheme based on Fuzzy extractors". Security and Communication Networks, vol. 8, no. 4, pp. 682-693, 2015.
- [10] Uludag U, Jain A K. "Attacks on biometric systems: a case study in fingerprints", Electronic Imaging 2004. International Society for Optics and Photonics, pp. 622-633, 2004;
- [11] Christo Ananth, A.Nasrin Banu, M.Manju, S.Nilofer, S.Mageshwari, A.Peratchi Selvi, "Efficient Energy Management Routing in WSN", International Journal of Advanced Research in Management, Architecture,



- Technology and Engineering (IJARMATE), Volume 1, Issue 1, August 2015, pp:16-19
- [12] C.-H. Lin and Y.-Y. Lai, "A flexible biometrics remote user authentication scheme," *Comput. Standards & Interfaces*, vol. 27, no. 1, pp. 19–23, nov 2004.
- [13] C.-C. Chang and I.-C. Lin, "Remarks on finger-print-based remote user authentication scheme using smart cards," *ACM SIGOPS Oper. Syst. Rev.* vol. 38, no. 4, pp. 91–96, Oct. 2004.
- [14] H.-S. Kim, S.-W. Lee, and K.-Y. Yoo, "ID-based password authentication scheme using smart cards and fingerprints," *ACM SIGOPS Oper. Syst. Rev.*, vol. 37, no. 4, pp. 32–41, Oct. 2003.
- [15] M. Scott, "Cryptanalysis of an ID-based pass-word authentication scheme using smart cards and fingerprints," *ACM SIGOPS Oper. Syst. Rev.*, vol. 38, no. 2, pp. 73–75, Apr. 2004.
- [16] C.-T. Li and M.-S. Hwang, "An efficient biomet-rics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 33, no. 1, pp. 1–5, Jan. 2010.
- [17] X . Li, J. Niu, J. Ma, W. Wang, and C. Liu, "Cryptanalysis and improvement of a biomet-rics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 73–79, Jan. 2011.
- [18] E. Yoon and K. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryp-tosystem," *J. Supercomput.*, vol. 63, no. 1, pp. 235–255, Jan. 2013.
- [19] D. He, Security flaws in a biometrics-based multi-server authentication with key agree-ment scheme, Tech. Rep. 2011/365, ePrint Archive. [On-line]. Available: <http://eprint.iacr.org/2011/365.pdf>.
- [20] He D, Wang D. Robust biometrics-based au-thentication scheme for multiserver environ-ment[J]. *Systems Journal*, IEEE, vol. 9, no. 3, pp. 816-823, 2015
- [21] Odelu V, Das A K, Goswami A. A secure biomet-rics-based multi-server authentication protocol using smart cards[J]. *Information Forensics and Security, IEEE Transactions on*, 2015, 10(9): 1953-1966.
- [22] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[C]//Advances in cryptolo-gy-Eurocrypt 2004. Springer Berlin Heidelberg, 2004: 523-540.
- [23] Kocarev, Ljupco, and ShiguoLian, eds. *Cha-os-based cryptography: Theory, algorithms and applications*. Vol. 354. Springer, 2011.
- [24] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.
- [25] Lu Y, Li L, Peng H, et al. "Robust and efficient biometrics based password authentication scheme for telecare medicine information sys-tems using extended chaotic maps". *Journal of medical systems*, vol. 39, no. 6, pp. 1-10, 2015. Burrow, M., Abadi, M., Needham, R., "A logic of authentication". *ACM Trans. Comp. Syst.* vol. 8 18–36, 1990.