Cryptanalysis on 'Robust Biometrics-Based Authentication Scheme for Multi-server Environment'

Vanga Odelu [1,⋆], Ashok Kumar Das [2], and Adrijit Goswami [3]

[1] Department of Mathematics
Indian Institute of Technology, Kharagpur 721 302, India
odelu.phd@maths.iitkgp.ernet.in, odelu.vanga@gmail.com
[2] Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad 500 032, India
iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in
[3] Department of Mathematics
Indian Institute of Technology, Kharagpur 721 302, India
goswami@maths.iitkgp.ernet.in

Abstract. Authentication plays an important role in an open network environment in order to authenticate two communication parties among each other. Authentication protocols should protect the sensitive information against a malicious adversary by providing a variety of services, such as authentication, user credentials' privacy, user revocation and re-registration, when the smart card is lost/stolen or the private key of a user or a server is revealed. Unfortunately, most of the existing multi-server authentication schemes proposed in the literature do not support the fundamental security property such as the revocation and re-registration with same identity. Recently, in 2014, He and Wang proposed a robust and efficient multi-server authentication scheme using biometrics-based smart card and elliptic curve cryptography (ECC). In this paper, we analyze the He-Wang's scheme and show that He-Wang's scheme is vulnerable to a known session-specific temporary information attack and impersonation attack. In addition, we show that their scheme does not provide strong user's anonymity. Furthermore, He-Wang's scheme cannot support the revocation and re-registration property. Apart from these, He-Wang's scheme has some design flaws, such as wrong password login and its consequences, and wrong password update during password change phase.

Keywords: Security, Credentials privacy, Smart card, Revocation and re-registration, Authentication.

1 Introduction

With the rapid development of the wireless communication networks and e-commerce applications, such as e-banking and transaction-oriented services [1], there is a growing demand to protect the user credentials' privacy and provide a variety of services. In the recent couple of decades, more and more transactions for the mobile devices have been implemented on the Internet or wireless networks due to the portability property of mobile devices, such as laptops, smart cards and smart phones [2]. Thus, the authentication protocols become the trusted components in a communication system in order to protect the sensitive information against a malicious adversary, by means of providing confidentiality as well as authentication. We consider the following two real-life scenarios for the smart card based authentication schemes in which the registered users may revoke and re-register with the same identity:

– when unexpectedly the secret token of a legal user is revealed [3].
– if the smart card of a legal user is stolen or lost [4].

Hence, the authentication schemes must support the user revocation [5] and re-registration with the same identity [6]. The user revocation and re-registration with the same identity may cause the user impersonation attack, when an authentication scheme distributes the static secret tokens [7], [8]. Therefore, designing an efficient approach to tackle the problem of user revocation while supporting a strong user untraceability becomes a challenging problem [9]. As a result, the user revocation and re-registration with the same identity is identified as a fundamental security functionality for the smart card-based authentication schemes.

After conception of Lamport's seminal authentication scheme in 1981 [26], several two-party authentication schemes have been proposed in the literature (for example, [1],[4]-[9]). In a single-server environment, a user needs to register with each server separately. However, it is impossible to apply two-party authentication methods in a single server environment directly to a multi- server environment. To handle this problem, several multi-server authentication schemes [27]-[39] have been proposed in the literature. Yoon and Yoo [40] proposed a multi-server authentication scheme using the biometrics-based smart card and ECC. However, Kim et al. [41] pointed out that if the smart card is lost, Yoon-Yoo's scheme cannot prevent the offline password guessing attack. Further, they proposed an enhanced scheme in order to withstand the security flaw found in Yoon-Yoo's scheme. Later, He [42] proved that Yoon-Yoo's scheme is also insecure against the privileged insider attack and impersonation attack. He [42] showed that their proposed attacks are also valid for Kim et al.'s scheme. Recently, He and Wang [11] proposed a robust biometrics-based authentication scheme for multi-server environment in order to withstand these security issues, and claimed that their scheme is secure against all possible known attacks. However, in this paper, we show that He-Wang's scheme fails to prevent known session temporary information attack, and as a result, their scheme cannot prevent the reply attack and impersonation attack. In addition, we show that their scheme cannot provide the strong users' anonymity.

The rest of the paper is sketched as follows. In Section 2, we briefly discuss some mathematical preliminaries to review and analyze He-Wang's scheme [11]. We then review the recently proposed He-Wang's scheme in Section 3. In Section 4, we show that He-Wang's scheme is vulnerable to various attacks. We also point out some design flaws of He-Wang's scheme in this section. Finally, we conclude the paper in last section.

2 Mathematical preliminaries

In this section, we briefly discuss the following mathematical preliminaries to review and analyze He-Wang's scheme [11].

2.1 Elliptic curve over a prime field $GF(p)$

A non-singular elliptic curve $y^2 = x^3 + ax + b$ over the finite field $GF(p)$ is the set E_p of solutions $(x, y) \in Z_p \times Z_p$ to the congruence $y^2 = x^3 + ax + b \,(\bmod\, p)$, where $a, b \in Z_p$ are constants such that $4a^3 + 27b^2 \neq 0 \,(\bmod\, p)$, together with a special point $\mathcal{O}$ called the point at infinity or zero point, $Z_p = \{0, 1, \ldots, p-1\}$ and $p > 3$ be a prime. The set of elliptic curve points E_p forms an abelian group under addition modulo p operation [45].

Let G be the base point on $E_p(a, b)$, whose order be n, that is, $nG = G + G + \ldots + G(n\, times) = \mathcal{O}$. Assume that $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are two points on elliptic curve $y^2 = x^3 + ax + b \,(\bmod\, p)$. Then $R = (x_R, y_R) = P + Q$ is computed as follows [45]:

$$x_R = (\delta^2 - x_P - x_Q)(\bmod\, p),$$
$$y_R = (\delta(x_P - x_R) - y_P)(\bmod\, p),$$
$$\text{where } \delta = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} \,(\bmod\, p), \text{if } P \neq Q \\ \frac{3{x_P}^2 + a}{2y_P} \,(\bmod\, p), \text{if } P = Q. \end{cases}$$

In elliptic curve cryptography, multiplication is defined as the repeated additions. For example, if $P \in E_p(a, b)$, then $4P$ is computed as $4P = P + P + P + P \,(\bmod\, p)$.

Definition 1 (Elliptic curve discrete logarithm problem (ECDLP)). *Computing $Q = kP$ is relatively easy for given $k \in Z_p$ and $P \in G$. However, given P and Q, it is computationally hard to compute the scalar k such that $Q = kP$.*

Definition 2 (Computational Diffie-Hellman problem (CDHP)). *Given $P, xP, yP \in G$, it is computationally hard to compute $xyP \in G$ without the knowledge of $x \in Z_p^*$ or $y \in Z_p^*$, where $Z_p^* = \{a | 0 < a < p, \gcd(a, p) = 1\} = \{1, 2, 3, \ldots, p-1\}$.*

Definition 3 (Collision-resistant one-way hash function). *A collision-resistant one-way hash function $H : X \to Y$, where $X = \{0, 1\}^*$ and $Y = \{0, 1\}^n$, is considered as a deterministic algorithm that takes an input as an arbitrary length binary string $x \in \{0, 1\}^*$ and outputs a binary string $y \in \{0, 1\}^n$ of fixed-length n [42], [43]. If $Adv_{\mathcal{A}}^{HASH}(t)$ is an adversary (attacker) $\mathcal{A}$'s advantage in finding collision, we then have*

$$Adv_{\mathcal{A}}^{HASH}(t) = Pr[(x, x') \Leftarrow_R \mathcal{A} : x \neq x' \text{ and } H(x) = H(x')],$$

where $Pr[E]$ denotes the probability of a random event E, and $(x, x') \Leftarrow_R \mathcal{A}$ denotes the pair (x, x') is selected randomly by $\mathcal{A}$. In this case, the adversary $\mathcal{A}$ is allowed to be probabilistic and the probability in the advantage is computed over the random choices made by the adversary $\mathcal{A}$ with the execution time t. A hash function $H(\cdot)$ is called collision-resistant, if $Adv_{\mathcal{A}}^{HASH}(t) \leq \epsilon$, for any sufficiently small $\epsilon > 0$.

2.2 Biometrics and fuzzy extractor

A fuzzy extractor $(\Upsilon, m, l, t, \epsilon)$ extracts a nearly random string σ from its biometric characteristic input ω in an error-tolerant way [22]. If an input changes but it remains close to ω, then the extracted σ remains the same. To assist in recovering σ from the biometric characteristic input ω', a fuzzy extractor outputs an auxiliary string θ. However, σ remains uniformly random for a given θ. The fuzzy extractor is given by the following two procedures, called Gen and Rep:

– Gen is a probabilistic generation procedure, which on (biometric characteristic) input $\omega \in \Upsilon$, outputs an extracted string $\sigma \in \{0,1\}^l$ and auxiliary string θ. For any distribution W on metric space Υ of mini-entropy m, if $\langle \sigma, \theta \rangle \leftarrow Gen(W)$, the static distance $SD(\langle \sigma, \theta \rangle, \langle U_l, \theta \rangle) \leq \epsilon$, where U_l denotes the uniform distribution on l-bit binary strings.
– Rep is a deterministic reproduction procedure that allows to recover σ from the corresponding auxiliary string θ and any vector ω' close to ω. For all $\omega, \omega' \in \Upsilon$ satisfying $dis(\omega, \omega') \leq t$, if $\langle \sigma, \theta \rangle \leftarrow Gen(W)$, then $Rep(\omega', \theta) = \sigma$.

The uniqueness property of a biometric allows its applications in authentication protocols. As compared to the low-entropy password, the biometric keys has more advantages [12]-[14] such as biometric keys cannot be lost or forgotten, hard to forge or distribute, difficult to copy or share, and as a result, guessing the biometric keys is a hard problem.

3 Review of He-Wang's scheme

In this section, we review the recently proposed He-Wang's scheme [11]. For the convenience, in this paper we use the notations listed in Table 1.

3.1 Registration phase

This phase consists of the server registration phase and the user registration phase.

Server registration phase In this phase, server S_j chooses its identity SID_j and sends it to RC via a secure channel. Upon receiving the request, RC computes $k_j = H(SID_j||k)$ and then sends it to S_j via a secure channel. After receiving k_j from RC, S_j keeps it secret.

User registration phase In this phase, U_i sends a request and obtains the smart-card SC_i with authentication parameter as follows:

Step R1. U_i chooses his/her identity ID_i, password pw_i and imprints his personal biometric impression B_i at the sensor. Then U_i computes $(\sigma_i, \theta_i) = Gen(B_i)$ and sends the registration request $Reg = \{ID_i, H(pw_i||\sigma_i)\}$ to RC via a secure channel.

Table 1. Notations used in this paper

Symbol	Description
RC	The registration center
k	The secret of RC
P_{pub}	The public key of RC, where $P_{pub} = kP$
S_j	The j^{th} server
SID_j	Identity of server S_j
k_j	Private key of S_j
U_i	The i^{th} user
ID_i and pw_i	Identity and password of U_i
k_i	Authentication factor of U_i
SC_i	Smart card of the user U_i
Ω	Symmetric-key cryptography
$E_k(\cdot)/D_k(\cdot)$	Symmetric enc/decryption with key k
$H(\cdot)$	A secure one-way hash function
n, p	Two sufficiently large prime number
F_p	A finite field of order p
E_p	A non-super singular elliptic curve over a field F_p
G	The additive group consisting of points on E
P	A generator of G with order n
$M_1 \| M_2$	Data M_1 concatenates with data M_2
$M_1 \oplus M_2$	XOR operation of M_1 and M_2
$X \rightarrow Y : \langle M \rangle$	X sends message M to Y

Step R2. After receiving the registration request Reg from U_i, RC computes $k_i = H(ID_i||k)$, $z_i = k_i \oplus H(pw_i||\sigma_i)$ and stores z_i into a smart-card SC_i. Finally, RC issues SC_i to U_i face to face.

Step R3. After receiving SC_i, U_i stores θ_i in it.

3.2 Authentication and key establishment phase

In this phase, U_i and S_j mutually authenticate each other and establish the session key as follows:

Step A1. U_i inserts SC_i into a card reader and inputs pw_i, ID_i and imprints personal biometrics B_i' at the sensor. U_i then generates a random number $x \in Z_n^*$ and computes $Rep(B_i', \theta_i) = \sigma_i$, $k_i = z_i \oplus H(pw_i||\sigma_i)$, $X = xP$, $K_1 = xP_{pub}$, $CID_i = ID_i \oplus H(K_1)$, and $h_1 = H(ID_i\,||SID_j||k_i||X||K_1)$. Finally, U_i sends the message $M_1 = \{CID_i, X, h_1\}$ to S_j via a public channel.

Step A2. After receiving message M_1, S_j randomly chooses $y \in Z_n^*$ and computes $Y = yP, K_2 = yP_{pub}, h_2 = H(CID_i||X||h_1||SID_j||k_j||Y||K_2)$, and $CSID_j = SID_j \oplus H(K_2)$. Finally, S_j sends the message $M_2 = \{CID_i, X, h_1, CSID_j, Y, h_2\}$ to RC via a public channel.

Step A3. Upon receiving M_2 from S_j, RC computes $K_3 = kY\ (= K_2)$, $SID_j = CSID_j \oplus H(K_2)$, and $k_j = H(SID_j||k)$. Then RC checks whether $h_2 = H(CID_i\,||X||h_1||SID_j||\,k_j||Y||K_3)$ holds or not. If it dose not hold, the RC terminates the session. Otherwise, RC computes $K_4 = kX\ (= K_1)$, $ID_i = CID_i \oplus H(K_4)$, and $k_i = H(ID_i||k)$. RC then checks whether $h_1 = H(ID_i\ ||SID_j||\ k_i||X||K_4)$ holds or not. If it does not hold, it terminates the session. Otherwise, RC computes $TID_i = ID_i \oplus H(Y||K_3||k_j)$, $h_3 = H(ID_i||\ TID_i||X||SID_j\ ||Y||k_j)$, $TSID_j = SID_j \oplus H(X||K_4||k_i)$, and $h_4 = H(ID_i||X||K_4||SID_j||Y\ ||k_i)$. Finally, RC sends the message $M_3 = \{TID_i,\ h_3, TSID_j, h_4\}$ to S_j via a public channel.

Step A4. After receiving M_3 from RC, S_j computes $ID_i = TID_i \oplus H(Y||K_2||k_j)$ and checks whether ID_i is valid or not. If it is not valid, S_j terminates the session. Otherwise, S_j checks whether the condition $h_3 = H(ID_i||TID_i||X||SID_j||Y||k_j)$ holds or not. If it does not hold, S_j terminates the session. Otherwise, S_j computes the session key $SK = yX = xyP$ and $h_5 = H(ID_i||SID_j||X||Y||SK||h_4)$. Finally, S_j sends $M_4 = \{TSID_j, Y, h_4, h_5\}$ to U_i via a public channel.

Step A5. Upon receiving M_4 from S_j, U_i computes $SID_j = TSID_j \oplus H(X||K_1||k_i)$ and then checks whether $h_4 = H(ID_i||X||K_4||SID_j||Y\ ||k_i)$ holds or not. If it does not hold, U_i stops the session. Otherwise, U_i computes the session key $SK = xY = xyP$, and checks whether $h_5 = H(ID_i||SID_j||X||Y||SK||h_4)$ holds or not. If it does not hold, U_i terminates the session. Otherwise, U_i computes $h_6 = H(SID_j||ID_i||X||Y||SK||h_4)$ and sends $M_5 = \{h_6\}$ to S_j.

Step A6. After receiving M_5 from U_i, S_j checks whether the condition $h_6 = H(SID_j\ ||ID_i||X||Y||SK||h_4)$ holds or not. If it holds true, S_j confirms that U_i is legitimate. Otherwise, S_j stops the session immediately.

3.3 Password change phase

In this phase, U_i changes his/her password as follows:

Step P1. U_i inserts SC_i into a card reader and inputs pw_i, ID_i and imprints personal biometrics B_i' at the sensor. U_i also inputs the new password pw_i^{new}.

Step P2. SC_i then computes $Rep(B_i', \theta_i) = \sigma_i$, $k_i = z_i \oplus H(pw_i||\sigma_i)$, and $z_i^{new} = k_i \oplus H(pw_i^{new}||\sigma_i)$. Finally, SC_i replaces z_i with z_i^{new}.

4 Cryptanalysis on He-Wang's scheme

In this section, we show that He-Wang's scheme [11] is vulnerable to various well-known attacks, which are outlined in the following subsections.

4.1 Known session-specific temporary information attack

According to [16]-[20], all the session keys must be secured even if the session random numbers of the user are compromised to an adversary $\mathcal{A}$. Assume that the session random number x chosen by U_i is unexpectedly revealed to an attacker $\mathcal{A}$. Then, He-Wang's scheme has the following drawback:

- Since U_i and S_j computes a session key SK as $SK = xY = xyP$, an attacker $\mathcal{A}$ can compute the session key SK using known session random number x.

- Adversary $\mathcal{A}$ intercepts the message $M_1 = \{CID_i, X, h_1\}$ sent to the server S_j (in Step A1 of the authentication and key establishment phase), and checks whether xP matches with X. If it matches, $\mathcal{A}$ confirms that x corresponds to M_1 and computes K_1 and ID_i as $K_1 = xP_{pub}$ and $ID_i = CID_i \oplus H(K_1)$ (this may cause user anonymity violation). The adversary $\mathcal{A}$ sends reply message M_1 to S_j without any modifications. In this case, neither S_j nor RC can identify the message M_1 as a replied one. From the message $M_4 = \{TSID_j, Y, h_4, h_5\}$, the adversary $\mathcal{A}$ knows Y and h_4, and he/she can compute SK as $SK = xY$ using x and then compute the valid $h_6 = H(SID_j||ID_i||X||Y||SK||h_4)$ for S_j without knowledge of U_i's authentication parameter k_i. As a result, $\mathcal{A}$ can successfully impersonate the legal user U_i.
- One more drawback is that RC cannot identify the user U_i and the server S_j separately when they want to establish the session key. In this case, a legal server S_j may act as legal user [10] and enjoy the services from the other servers S_l's.

4.2 Impersonation attack

In He-Wang's scheme [11], during the registration phase of a user U_i, the registration center RC computes the authentication parameter k_i of U_i using the identity ID_i of U_i and secret key k of RC as $k_i = H(ID_i||k)$. Clearly, the authentication parameter is static and the registration phase has no ability to detect re-registration with old identity. Thus, the user U_i can not re-register with the same identity ID_i in future for the following two genuine cases:

- when U_i's smart-card SC_i is lost/stolen, and
- unexpectedly U_i's authentication parameter k_i is revealed.

Hence, an adversary $\mathcal{A}$ can easily obtain the authentication parameter by performing re-registration with the legal user U_i's identity ID_i because RC does not maintain any user identity information table. Moreover, the servers' authentication parameter are also static and RC does not maintain any identity information of the servers. Therefore, the second case is also applicable to the servers. As a result, an attacker $\mathcal{A}$ can obtain the authentication parameter of a legal user (or a server), and then successfully impersonate the user (or a server). Moreover, the server is a semi-trusted party and He-Wang's authentication scheme cannot protect the user's identity from the server. It also causes the user's anonymity violation. As a result, He-Wang's scheme fails to protect user impersonation attack.

4.3 Wrong password login and its consequences

According to Khan and Kumari [8], during the authentication and key establishment phase if a legal user U_i enters his/her wrong password, the authentication test will fail and then it causes denial of service to the legal user U_i. In the login phase of He-Wang's [11] scheme, the smart cart SC_i sends the message M_1 without verifying the correctness of the user U_i's credentials ID_i, pw_i and biometrics B_i'. Even if U_i mistakenly enters his/her wrong password, say pw_i' $(pw_i' \neq pw_i)$, then SC_i still computes

$k_i' = z_i \oplus H(pw_i'||\sigma_i)$ instead of $k_i = z_i \oplus H(pw_i\ ||\sigma_i)$. In this case, U_i will send a wrong login request message M_1' instead of valid message M_1. Thus, the authentication test fails and as a result, He-Wang's scheme [11] falls under the denial-of-service (DoS) to the legal user U_i, which must not happen in sensitive applications. Moreover, an adversary can create denial of service problem by keep on sending the login request message using the legal user U_i's smart-card SC_i and wrong credentials.

4.4 Drawback in password change phase

In the password change phase of He-Wang's [11] scheme, a legal user U_i inputs ID_i, old password pw_i^{old}, biometrics B_i^* and new password pw_i^{new} into the smart card SC_i. As discussed in Section 4.3, even if U_i enters his/her wrong password pw_i' instead of old correct password pw_i^{old} ($pw_i' \neq pw_i^{old}$), SC_i still computes $r_i' = z_i \oplus H(pw_i'\ ||\sigma_i)$ and updates z_i with $z_i' = r_i' \oplus H(pw_i^{new}\ ||\sigma_i)$, where $r_i' \neq r_i$, using the wrong computed r_i' without verifying the validity of old password pw_i^{old}. After updating SC_i with wrong password entry, U_i will never pass the authentication test and the repetition of authentication may cause prolonged/permanent failures to login. As a result, the wrong password update may also cause the denial-of-service to the legal users in such a specific case.

4.5 No provision for revocation and re-registration

In order to provide the strong security to the user, revocation of lost/stolen smart-card is one of the fundamental security requirement of smart-card based authentication schemes. If a legal user U_i's smart-card SC_i is lost or stolen, there must be some mechanism to prevent the misuse of lost/stolen smart-card SC_i. Otherwise, an adversary $\mathcal{A}$ can impersonate the legal user U_i as the registration phase has no ability to detect the re-registration with old identity. To cope with this problem, the smart-card based authentication schemes need to store the identity information table in the RC's database, based on which the invalid smart-card will be detected [3]-[9]. However, most of the existing multi-server authentication schemes including the He-Wang's scheme do not consider the fundamental security feature for revocation and re-registration in their schemes in the multi-server environment.

5 Conclusion

In this paper, we have first reviewed the recently proposed He-Wang's scheme. We have then showed that their scheme is vulnerable to the known session-specific temporary information attack and user impersonation attack. Further, their scheme cannot provide strong user's anonymity property. Also, we have demonstrated the drawbacks in He-Wang's scheme when distributing the static authentication parameters and wrong password entry. In future, we aim to design a novel and more secure multi-server authentication protocol using biometric-based smart card and ECC in order to withstand the security flaws found in He-Wang's scheme.

References

1. J. L. Tsai and N. W. Lo and T. C. Wu, “Novel Anonymous Authentication Scheme Using Smart Cards”, IEEE Transactions on Industrial Informatics, vol. 9, no. 4, pp. 2004–2013, 2013.
2. S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani and R. Buyya, “Cloud-Based Augmentation for Mobile Devices: Motivation, Taxonomies, and Open Challenges”, IEEE Communications Survey & Tutorial, vol. 16, no. 1, 2014.
3. E. Brickell and J. Li, “Enhanced Privacy ID : A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities”, IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 3, PP. 345-360, 2012.
4. X. Huang, X. Chen, J. Li, Y. Xiang and L. Xu, “Further Observations on Smart-Card-Based Password-Authenticated Key Agreement in Distributed Systems”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp.1767-1175, 2014.
5. D. Wang, D. He, P. Wang and C. H. Chu, “Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment”, IACR Cryptology ePrint Archive, vol. 2014, pp. 135, 2014. This paper appeared at IEEE Transactions on Dependable and Secure Computing, pp. 1-15, Aug. 24, 2014.
6. S. Wu, Y. Zhu and Q. Pu, “Robust smart-cards-based user authentication scheme with user anonymity”, Security and Communication Networks, vol. 5, no. 2, pp. 236-248, 2012.
7. S. Kumari and M. K. Khan, “Cryptanalysis and improvement of a robust smart-card-based remote user password authentication scheme”, International Journal of Communication Systems, 2013. DOI: 10.1002/dac.2590.
8. M. K. Khan and S. Kumari, “Cryptanalysis and Improvement of An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems”, Security and Communication Networks, vol. 7, no. 2, pp. 399-408, 2014.
9. D. He, J. Bu, S. Chan, C. Chen and M. Yin, “Privacy-Preserving Universal Authentication Protocol for Wireless Communications”, IEEE Transactions on Wireless Communications, vol. 10, no. 2, pp. 431-436, 2011.
10. R. C. Wang, W. S. Juang and C. L. Lei, “User Authentication Scheme with Privacy-Preservation for Multi-Server Environment”, IEEE communication letters, vol. 13, no. 2, pp. 157–159, 2009.
11. D. He and D. Wang, “Robust Biometrics-Based Authentication Scheme for Multi-server Environment”, IEEE System journal, pp. 1-8, 2014.
12. A. Jain, L. Hong and S. Pankanti, “Biometric identification”, ACM Communications, vol. 43, no. 2, pp. 90-98, 2000.
13. N. K. Ratha, J. H. Connell and R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems”, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.
14. A. K. Das, “Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards”, IET Information Security, vol. 5, no. 3, pp. 145-151, 2011.
15. K. Lauter, “The advantages of elliptic curve cryptography for wireless security”, IEEE Wireless Communications, vol. 11, no. 1, pp. 62-67, 2004.
16. S. H. Islam, “Design and analysis of an improved smartcard-based remote user password authentication scheme”, International Journal of Communication Systems, 2014. DOI: 10.1002/dac.2793.
17. D. He, N. Kumar, M. K. Khan and J. H. Lee, “Anonymous Two-factor Authentication for Consumer Roaming Service in Global Mobility Networks Anonymous”, IEEE Transactions on Consumer Electronics, vol. 59, no. 4, pp.811-817, 2013.
18. R. Canetti and H. Krawczyk, “Analysis of key exchange protocols and their use for building secure channels”, In Advances in Cryptology-EUROCRYPT 2001, pp. 453-474, 2001.

19. Z. Cheng, M. Nistazakis, R. Comley and L. Vasiu, “On the indistinguishability-based security model of key agreement protocols-simple cases”, Cryptology ePrint Archieve, Report 2005/129, 2005.
20. D. Mishra, A. K. Das and S. Mukhopadhyay, “A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards”, Expert Systems with Applications, vol. 41, no. 18, pp. 8129-8143, 2014. http://dx.doi.org/10.1016/j.eswa.2014.07.004.
21. M. Burrows, M. Abadi and R. Needham, “A logic of authentication”, ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36, 1990.
22. Y. Dodis, L. Reyzin, and A. Smith, “Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data”, In Advances in cryptology-Eurocrypt 2004, pp. 523-540. Springer Berlin Heidelberg, 2004.
23. T. A. ElGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, 1985.
24. H. Kilinc and T. Yanik, “A survey of SIP authentication and key agreement schemes”, IEEE Communications Surveys & Tutorials, pp. 1-19, 2013. DOI: 10.1109/SURV.2013.091513.00050.
25. X. Huang, Y. Xiang, A. Chonka, J. Zhou and R. H. Deng, “A generic framework for three-factor authentication: preserving security and privacy in distributed systems”, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 8, pp. 1390-1397, 2011.
26. L. Lamport, “Password authentication with insecure communication”, ACM Communications , vol. 24, pp. 28-30, 1981.
27. L. Li, I. Lin and M. Hwang, “A remote password authentication scheme for multi-server architecture using neural networks”, IEEE Transactions on Neural Networks, vol. 12, no. 6, pp. 1498-1504, 2001.
28. 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. 13-22, 2003.
29. W. S. Juang, “Efficient multi-server password authenticated key agreement using smart cards”, IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 251-255, 2004.
30. C. C. Chang and J. S. Lee, “An efficient and secure multi-server password authentication scheme using smart cards”, In International Conference on Cyberworlds, pp. 417-422. IEEE, 2004.
31. J. L. Tsai, “Efficient multi-server authentication scheme based on one-way hash function without verification table”, Computers & Security, vol. 27, no. 3, pp. 115-121, 2008.
32. Y. P. Liao and S. S. Wang, “A secure dynamic ID based remote user authentication scheme for multi-server environment”, Computer Standards & Interfaces, vol. 31, no. 1, pp. 24-29, 2009.
33. H. C. Hsiang and W. K. Shih, “Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment”, Computer Standards & Interfaces, vol. 31, no. 6, pp. 1118-1123, 2009.
34. X. Li, Y. Xiong, J. Ma and and W. Wang, “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.
35. Y. P. Liao and C. M. Hsiao, “A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients”, Future Generation Computer Systems, vol. 29, no. 3, pp. 886-900, 2013.
36. M. C. Chuang and C. C. Meng, “An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics”, Expert Systems with Applications 41, no. 4, pp. 1411-1418, 2014.

37. Y. Lee, J. Kim and D. Won, "Countermeasure on Password-Based Authentication Scheme for Multi-server Environments", In Multimedia and Ubiquitous Engineering, pp. 459-466. Springer Berlin Heidelberg, 2014.
38. X. Li, J. Niu, S. Kumari, J. Liao and W. Liang, "An Enhancement of a Smart Card Authentication Scheme for Multi-server Architecture", Wireless Personal Communications, pp. 1-18, 2014.
39. T. Y. Chen, C. H. Ling and M. S. Hwang, "Weaknesses of the Yoon-Kim-Yoo remote user authentication scheme using smart cards", In Electronics, Computer and Applications, 2014 IEEE Workshop on, pp. 771-774, 2014.
40. E. Yoon and K. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem", Journal of Supercomputing, vol. 63, no. 1, pp. 235-255, 2013.
41. H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, "Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme", In Computational Science and Its Applications (ICCSA 2012), pp. 391-406. Springer Berlin Heidelberg, 2012.
42. D. He, "Security flaws in a biometrics-based multi-server authentication with key agreement scheme", Tech. Rep. 2011/365, ePrint Archive. [On-line]. Available: http://eprint.iacr.org/2011/365.pdf
43. P. Sarkar, "A Simple and Generic Construction of Authenticated Encryption with Associated Data", ACM Transactions on Information and System Security (TISSEC), vol. 13, no. 4, 2010.
44. D. R. Stinson, "Some Observations on the Theory of Cryptographic Hash Functions", Designs, Codes and Cryptography, vol. 38, no. 2, pp. 259-277, 2006.
45. W. Stallings, *Cryptography and Network Security: Principles and Practices*, 3rd ed. Prentice Hall, 2003.