Remote login password authentication scheme using tangent theorem on circle

Shipra Kumari* and Hari Om

Department of Computer Science and Engineering,
Indian School of Mines,
Dhanbad, Jharkhand, India
Email: shiprakumari18jan@gmail.com
Email: hariom4india@gmail.com
*Corresponding author

Abstract: In this paper, we propose a remote password authentication scheme based on geometry. We use some simple tangent theorems of a circle, RSA encryption technique, and a strong one-way function to mutually authenticate the user and the server. It has a facility for a legal user to freely choose and change his password using his smart card. The security of this scheme depends on the tangent points located in a plane associated with the circle and the tangent line itself. In this scheme, the user anonymity is preserved and the communication cost is also reduced due to checking the correctness of the password before sending any authentication message.

Keywords: authentication; RSA cryptosystem; tangent theorem; circle; smart card.

Reference to this paper should be made as follows: Kumar, S. and Om, H. (2016) 'Remote login password authentication scheme using tangent theorem on circle', *Int. J. Convergence Computing*, Vol. 2, No. 1, pp.93–106.

Biographical notes: Shipra Kumari is currently working as a full time Research Scholar in the Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, India. She received her Bachelor in Computer Application and Master in Computer Application from Indira Gandhi Open University. Her research interest includes cryptography.

Hari Om is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, India. He did his PhD in Computer Science from Jawaharlal Nehru University, New Delhi. He received his MTech in Computer Science and Engineering from Kurukshetra University, Kurukshetra (Haryana). He also received his MSc in Mathematics from Institute of Basic Sciences (I.B.S.), Khandari Agra, Dr. B.R. Ambedkar University (formerly Agra University) Agra. He has around 12 years of teaching and research experiences, and contributed a number of research papers in several journals and conference proceedings of national and international reputes. He is a member of Indian Society for Technical Education, Indian Mathematical Society, Indian Society of Mathematics and Mathematical Sciences, Cryptology Research Society of India, Institute of Electronics and Telecommunication Engineers. His main research interest includes data mining, network security, and image processing. He has a specialisation in video-on-demand, cryptography.

This paper is a revised and expanded version of a paper entitled 'Remote login password authentication scheme using tangent theorem on circle' presented at FICTA 2014, Bhubaneswar, India, 14–15 Novenber 2014.

1 Introduction

Since the inception of computer networks, their necessity has been very high. Almost all the people in the world depend on the computer networks for different purposes. In a network environment, a person can access resources or services remotely and to access resources remotely we depend on a communication channel. The communication channels may not secure all the time due to an opponent who always tries to collect the information from the communication channels and wants to use for own benefit or to harm someone. The unauthorised access and unauthorised services are the major problems for remote login mechanism. Therefore, an appropriate security mechanism is required that can verify the legitimacy of a legal user and the service provider as well, before the actual exchange of services. A remote login authentication scheme, especially in a distributed environment affects all users for different purposes. So there is always a need to have secure algorithms and several researchers are involved in developing secure methods to achieve all the security goals and requirements. These methods prevent the hampering of information travelling on an insecure channel. Since the first remote login authentication mechanism (Lamport, 1981), many researchers have developed very secure schemes that have numerous features using various approaches. However, almost all the schemes have some security breach due to the lack of some feature or some design issue.

2 Related work

Among the different approaches (Wu, 1995; Chien et al., 2001; Wang, 2003; Kumar et al., 2010; Liaw, 1995; Liaw and Lei, 1995; Das et al., 2004; Wang et al., 2004, 2009; Wen and Li, 2012; Juan and Zou, 2013; Chaturvedi et al., 2013; Zhang et al., 2014; Leu and Hsieh, 2014; Ramesh and Bhaskaran, 2014; Karuppiah and Saravanan, 2014; Kumari and Om, 2015; Lee et al., 2013), some researchers have developed the remote login schemes using geometric approach, which was first discussed by Wu (1995) with simple implementation in the Euclidean plane. The Wu's scheme was modified by Chien et al. (2001) in 2001. In 2003, Wang (2003) proposed a scheme using a circle in n-dimensional space. In 2004, Wang et al. (2004) pointed out that the scheme (Chien et al., 2001) was vulnerable to the replaying attack and dictionary attack. In 2010, Kumar et al. proposed an authentication scheme based on sphere (Kumar et al., 2010). This scheme, however lacks some features like use anonymity, earlier detection of wrong password. Meanwhile, different schemes have been proposed using geometry (Liaw, 1995; Liaw and Lei, 1995; Wang, 2003), but all of them do not provide all requirements. In 2004, Das et al. (2004) presented a dynamic ID-based remote user authentication scheme using smart cards. They pointed out that their scheme did not maintain any verifier table and could resist the replay attack, forgery attack, guessing attack, and insider attack. However, in 2009, Wang

et al. (2009) pointed out that the Das et al.'s scheme could not resist the impersonation attack and also did not achieve mutual authentication. In 2012, Wen and Li pointed out that the Wang et al.'s scheme was vulnerable to the impersonation attack. Just through intercepting and modifying the messages transmitted on public networks, an adversary could impersonate the legal user to login the server. Moreover, an insider user who has registered with the remote server can reveal some secret information of the server and other users. They improved that scheme so that it could resist impersonation attack, avoiding partial information leakage and providing anonymity for the users (Wen and Li, 2012). In 2013, Juan and Zou pointed out that the Wen and Li's scheme could not withstand the insider attack and forward secrecy and the user can be traced out though eavesdropping the user's login request message on the public networks. They also proposed secure dynamic-ID remote user authentication scheme using ECC (Juan and Zou, 2013).

In 2013, Chaturvedi et al. (2013) proposed a scheme based on the exponential computation, which makes it costly as it needs more bits for authentication message. In 2014, Zang et al. (2014) proposed the first authentication scheme with anonymity for SIP, but its login and password change phase was not so efficient. In the same year, Leu and Hsieh (2014) proposed a dynamic ID-based remote user authentication scheme for distributed environment using the smart cards. After some time of the development of this scheme, Ramesh and Bhaskaran (2014) pointed out that the Leu et al.'s scheme was vulnerable to the impersonation attack, leak verifier attack, stolen smart card attack. In the same year, Karuppiah and Saravanan (2014) proposed a secure scheme; however its communication cost was high due to exponentiation. In this paper, we propose a scheme using geometry that fulfills all the security requirements. We also enhance the security and computational cost of the scheme (Kumari and Om, 2015) by providing the user anonymity and using a hash function to compute the points on the plane instead of the exponential function.

3 Proposed scheme

Our scheme has four phases: initialisation, registration, login, authentication and password change phases.

3.1 Initialisation phase

Let RS be a remote server that performs the following actions.

Choose two distinct very large prime numbers p and q and compute the following:

$$n = p \times q$$

$$\Phi(n) = (p-1) \times (q-1)$$

Choose an integer e such that $gcd(e, \Phi(n)) = 1$ and $1 < e\Phi(n)$.

Then compute a secret key d such that $e.d = 1 \bmod \Phi(n)$.

RS keeps the secret key d.

3.2 Registration phase

Assume that the new user U_i wants to register with the server. For this following steps are performed.

- new user chooses his own identity ID_i and password PW_i and selects a number b_i
- he sends ID_i and $f(PW_i \oplus b_i)$ to remote server (RS)
- RS calculates the pairs of points on XY-plane: $C = (C_{x_i}, C_{y_i})$ and $D = (D_{x_i}, D_{y_i})$, where

$$C_{x_i} = f(ID_i \| e) \bmod n,$$

$$C_{y_i} = f(ID_i \| d) \bmod n,$$

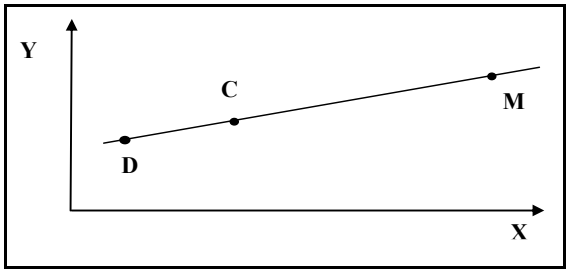
$$D_{x_i} = f(ID_i \oplus e) \bmod n,$$

$$D_{y_i} = f(f(PW_i \oplus b_i) \| e) \bmod n$$

- RS constructs a line L_i passing through the points C and D
- RS randomly chooses a point $M_i = (M_{x_i}, M_{y_i})$ on line L_i
- RS computes $HPW_i = f(f(PW_i) \| C_{y_i}) \bmod n$
- RS stores $\{M_i, HPW_i, e, n\}$ message in the smart card and delivers it to user U_i
- user inserts b_i into the smart card.

The registration phase is graphically shown in Figure 1.

Figure 1 Registration phase



3.3 Login phase

When the user U_i wants to login to the server, he keys in his identity ID_i and password PW_i. Then, the smart card performs the following:

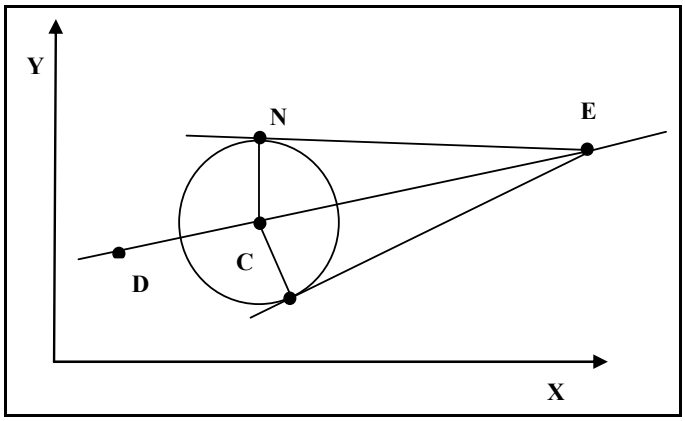
- Obtain current login time T from the system.
- Compute the point $D = (D_{x_i}, D_{y_i})$ as

  $D_{x_i} = f(ID_i \oplus e) \bmod n,$

  $D_{y_i} = f(f(PW_i \oplus b_i) \| e) \bmod n.$
- Redraw line L_c passing through the points D_i and M_i.
- Compute slope m_i of line L_c.
- Ccmpute $C_{x_i} = f(ID_i \| e) \bmod n.$
- Compute C_{y_i} by substituting C_{x_i} in the equation of line L_c.
- Compute $HPW_i^* = f(f(PW_i \oplus b_i) \| C_{y_i}) \bmod n.$
- Compare HPW_i^* with HPW_i that is already stored in smart card. They match, proceed; otherwise terminate the session.
- Compute $V_i = f(m_i \| C_{y_i} \| D_{y_i} \| T).$
- Choose a random number r_c.
- Compute $V_2 = V_1 \oplus r_c$.
- Compute $R_i = f(V_2 \| V_1) \bmod n$.
- Draw a circle in xy-plane using the point $C = (C_{x_i}, C_{y_i})$ as its centre and R_i as its radius.
- Take a random point E on line L_c.
- Through the point E, draw a tangent on a circle which touches the circle at point N.
- Draw a line from the centre C to the tangent point N. By tangent theorem, the line CN is perpendicular to the tangent line. Thus, < MTC = 90° (refer to Figure 2).
- By Pythagoras theorem

  $EN_i^2 = (EC_i^2 - CN_i^2) \bmod n,$ where $CN_i = R_i$
- Compute $V_3 = f(EN_i^2 \| r_c) \bmod n.$
- Compute $CID_i = (ID_i \oplus T)^e \bmod n$.
- Compute point $E^* = (E_{x_i} \oplus ID_i, E_{y_i} \oplus ID_i) \bmod n.$
- Send the authentication message $\{CID_i, V_2, V_3, E^*, T\}$ to server.

Figure 2 Login phase



3.4 Authentication phase

Upon receiving a login request at time T', the server RS performs the following:

- Check if the transmission time $(T' - T)$ is within the legal tolerant interval ΔT. If $(T' - T) < \Delta T$, then proceed; otherwise terminate the login request.
- Decrypt CID_i and compute ID_i as

  $$ID_i = \left((CID_i)^d \oplus T\right) \bmod n.$$

- Check the correctness of the format of ID_i to continue.
- Compute the point $E\,(E_x, E_y)$ as: $(E_x^* \oplus ID_i, E_x^* \oplus ID_i) \bmod n.$
- Compute $C_{x_i} = f(ID_i \,||\, e) \bmod n$ and $C_{y_i} = f(ID_i \,||\, d) \bmod n.$
- Using the points C and E, draw line L_s.
- Compute slope n_i of line L_s.
- Compute $D_{x_i} = f(ID_i \oplus e) \bmod n.$
- Compute D_{y_i} by substituting D_{x_i} in the equation of line L_s.
- Compute $V_i^* = f(n_i \,||\, C_{y_i} \,||\, D_{y_i} \,||\, T).$
- Compute $R_i^* = f(V_2^* \,||\, V_1^*) \bmod n.$
- Draw a circle in xy-plane using the point $C(C_{x_i}, C_{y_i})$ as centre and R_i^* as radius.

- Equation of the circle is

$$\left(x - C_{x_i}\right)^2 + \left(y - C_{y_i}\right)^2 = \left(R_i^*\right)^2. \tag{1}$$

- Let line L_s cut the circle at the points: A and B.
- Equation of the line L_s passing through point C and has slope n_i is given by

$$y - C_{y_i} = n_i\left(x - C_{x_i}\right). \tag{2}$$

- From (1) and (2), we get two points: $A(A_{x_i}, A_{y_i})$ and $B(B_{x_i}, B_{y_i})$.
- Draw a tangent on the circle from the point E.
- If N is a tangent point on the circle, then by the secant tangent theorem

  $EN_i^2 = EA \times EB$, where AB is secant of circle that passes through the centre C. Thus, Ab is the diameter of circle (refer to Figure 2).

  Proof:

$$\begin{aligned} EN_i^2 &= EA_i \times EB_i = EA_i \times \left(EA_i + AB_i\right) \\ &= \left(EC_i - CA_i\right) \times \left(\left(EC_i + CA_i\right) + 2\left(CA_i\right)\right) \\ &= \left(EC_i - CA_i\right) \times \left(EC_i - CA_i\right) \\ &= EC_i^2 - CN_i^2, \quad \text{where } CN_i = R_i^*. \end{aligned}$$

- Compute $V_3 = f(EN_i^2 \,||\, (V_1^* \oplus V_2)) \bmod p$. If $V_3^* = V_3$, then user U_i is authenticated; otherwise the login request is rejected.
- Choose random number r_s.
- Compute $V_4 = V_1^* \oplus r_s$.
- Compute $SK = f(ID_i \,||\, C_{y_i} \,||\, D_{y_i} \,||\, r_s \,||\, (V_i^* \oplus V_2))$.
- Compute $V_5 = f(V_1^* \,||\, SK \,||\, T_1)$.
- Send message $\{V_4, V_5, T_1\}$ to user.
- Smart card computes

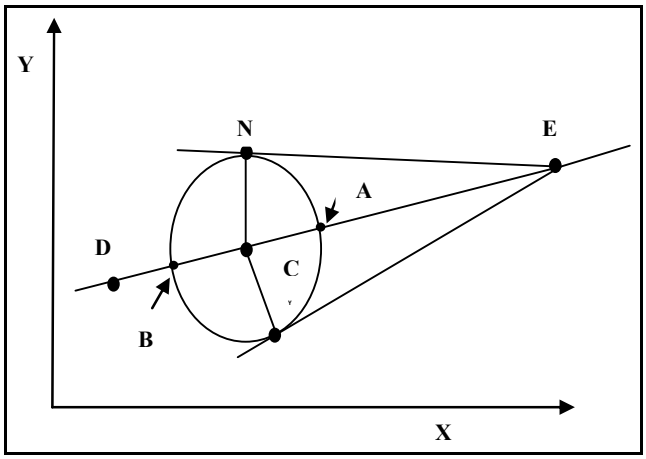
$$SK = f\left(ID_i \,||\, C_{y_i} \,||\, D_{y_i} \,||\, (V_4 \oplus V_1) \,||\, r_c\right)$$

$$V_5^* = f\left(V_1 \,||\, SK \,||\, T_1\right)$$

  If $V_5^* = V_5$, then the server is authenticated.

The authentication phase is shown graphically in Figure 3.

Figure 3 Authentication phase



3.5 Password change

To change the password, the user U_i first enters his smart card into the card reader and then types his identity ID_i and password PW_i. System performs the following.

- Compute the point $D = (D_{x_i}, D_{y_i})$ as

  $D_{x_i} = f(ID_i \oplus e) \bmod n,$

  $D_{y_i} = f(f(PW_i \oplus b_i) \| e) \bmod n.$

- Redraw line L_c passing the points D and M.
- Compute $C_{x_i} = f(ID_i \| e) \bmod n.$
- Compute C_{y_i} by substituting C_{x_i} in the equation of line L_c.
- Compute $HPW_i^* = f(f(PW_i \oplus b_i) \| C_{y_i}) \bmod n.$
- Compare HPW_i^* with HPW_i that is already stored in smart card. If equal, then proceed; otherwise, terminate the session.
- Enter new password PW_i^{new}.
- Compute $HPW_i^{new} = f(f(PW_i^{new} \oplus b_i) \| C_{yi}) \bmod n.$
- Compute the point $D^{new} = (D_{x_i}, D_{y_i})$. as

  $D_{x_i} = f(ID_i \oplus e) \bmod n,$

  $D_{y_i} = f(f(PW_i^{new} \oplus b_i) \| e) \bmod n.$

- Construct line L_i^{new} passing through the points C and D^{new}.
- Smart card chooses a point M_i^{new} on line L_i.
- Smart card replaces HPW_i by HPW_i^{new} and M_i with M_i^{new}. Hence, the password is changed successfully.

4 Security analysis of our scheme

In this section, we analyse the security of our scheme for proving that it provides strong security protection on the relevant security attacks. In the following, we justify several security attacks protection approach.

a *Replay attack:* The replay attack cannot work on our scheme because of the renewal of $V_1 = f(mi \| C_{y_i} \| D_{y_i} \| T)$ and $V_2 = V_1 \oplus r_c$ at different timestamps T and a fresh random number r_c for every login session.

If an adversary sends a same message $\{CID_i, V_2, V_3, E^*, T\}$, then the maximum time limit exceeds and the server rejects the request.

If an adversary sends the same message at the current time as $\{CID_i, V_2, V_3, E^*, T\}$, then the server computes

$$IDi = \left((CID_i)^d \oplus T_i\right) \bmod n.$$

Here, the server gets the incorrect ID_i. Server can also get incorrect values of points C and E. Moreover, the server gets the incorrect V_1^* and R_i^*. Thus, the correct value of radius cannot be computed. Therefore, an adversary cannot pass the verification process of the server.

b *Stolen smart card attack:* An attacker can try to use the stolen smart card of a valid user after extracting the stored parameters $\{M_i, HPW_i, b_i, e, n\}$ by monitoring the power consumption (Kocher et al., 1999; Messerges et al., 2002). To login successfully to the server, the attacker has to make a valid login message $\{CID_i, V_2, V_3, E^*, T\}$. However, the attacker cannot compute the valid ID_i from CID_i. Computing the rest of the parameters require V_1, which is also protected by the non-invertible cryptographic one-way hash function and is dependent on C_{y_i} and D_{y_i}.

The parameter ID_i is encrypted before transmission on an insecure channel. The smart card of U_i does not store ID_i. Moreover, the attacker cannot extract C_{y_i} and D_{y_i} from the transmitted login message and the known smart card parameters. Therefore, our scheme provides strong security on the smart card stolen attack.

c *Insider attack:* In registration phase, the user submits $y = f(PW_i \oplus b_i)$ to server. Since computing PW_i from y involves the one-way property of the hash function $f(.)$, the insider cannot know the password of the user. Hence, our scheme is secured against the insider attack.

d *Secure in password guessing attack:* If the adversary extracts the secured data from the smart card though physically monitoring its power consumption. He can also get the authentication message. Let the adversary guess the password PW_i. To check the correctness of the password, the adversary needs the point D as

$$D_{x_i} = f(ID_i \oplus e) \bmod n,$$

$$D_{y_i} = f(f(PW_i \oplus b_i) \| e) \bmod n.$$

To compute the point D, user ID_i is also required. However, guessing the ID_i and PW_i in polynomial time is not possible. Therefore, our scheme is secure against the password guessing attack.

e *Mutual authentication:* In our scheme, the user and server mutually authenticate each other, which increase the security of the scheme. The server and user use their own secret keys to compute the authentication messages, which are used to verify the authenticity of each other.

f *User-server impersonation attack:* In this attack, upon receiving the transmitting messages, the attacker may try to impersonate as a legitimate user or server after generating valid messages. However, our scheme has strong security protection on the transmitted messages which are justified below:

At first, the attacker tries to compute valid login message $\{CID_i, V_2, V_3, E^*, T\}$, which will be authenticated by the server. However, the attacker cannot compute valid login parameters V_2, V_3, as they require the knowledge of C_{y_i} and D_{y_i}. Therefore, our scheme provides strong security on the login message.

Suppose that the attacker traps the transmitting message $\{V_4, V_5, T_1\}$ between the server and user and tries to impersonate as a valid server to user. The attacker fails to validate the above mentioned message, as he cannot compute valid V_4, V_5 parameters because of unknown parameters C_{y_i} and D_{y_i}.

Therefore, the attacker fails to impersonate as a legitimacy entity in our scheme.

g *Session key agreement and verification:* It is confirmed that the U_i and the RS both compute the same session key $SK = f(ID_i \| C_{y_i} \| D_{y_i} \| (V_4 \oplus V_1) \| r_c)$ and $SK = f(ID_i \| C_{y_i} \| D_{y_i} \| r_s \| (V_i^* \oplus V_2))$, respectively, our scheme during the authentication phase. The RS computes $V_5 = f(V_1^* \| SK \| T_1)$ and transmits it to U_i through a public channel. Then, the U_i verifies the authenticity of V_5 parameter, which ensures that the session key is verified. Thus, our scheme provides the session key agreement and verification.

h *User anonymity:* In our scheme, the anonymity of a user is preserved. The smart card sends $CID_i = (ID_i \oplus T)^e$ instead of plain ID_i. Due to the discrete logarithm problem, it is hard to derive ID_i from CID_i. Decrypting the message is also not possible without knowing the secret key d of the server.

i *Stolen verifier:* Since the server, neither saves any verification table, nor stores any entry in its database, no question arises for an attacker to make a way inside the scheme.

j *Security against denial of service attack:* Our scheme prevents an unauthorised modification of the password verification information by enabling the smart card to check the validity of a user before updating. It is impossible to correctly guess ID_i and PW_i both at the same time even after getting the smart card of the legitimate user. The administrator cannot modify the password information in the database, since there is no server database.

k *Prompt detection of wrong password:* If the user inputs a wrong password, it will perform unnecessary computation and communication. In our scheme, when a user inputs ID_i, PW_i, in login and password phases, the smart card computes $HPW_i^* = f(f(PW_i) \| C_{y_i})$ and compares with the stored HPW_i in the smart card. If someone has entered a wrong password, then the smart card terminates the session; otherwise, the smart card performs the remaining steps. Hence, entry of wrong password is detected at the beginning of the login phase by the smart card that reduces the wastage of communication cost.

l *Friendly and efficient password change:* In our scheme, to change the password, server is not involved to check the validity of the user. However, the smart card first checks the validity of the original password PW_i. To check the correctness of the password, the smart card computes D_{x_i}, D_{y_i} and C_{y_i} using the line DM. Then it computes $HPW_i^* = f(f(PW_i \oplus b_i) \| C_{y_i}) \bmod n$ and compares HPW_i* with HPW_i that is stored in the smart card. If equal, then the password is valid, i.e. the wrong password is detected before communication. After checking the correctness of password, the user can input a new password and the smart card computes M_i^{new} and HPW_i^{new} and replaces old value with new one, to complete the password change. Therefore, the password change phase is efficient and there is no chance of denial of service because the server is not involved in this phase. It also saves the communication cost between the smart card and server.

m *Known session key security:* A unique secret session key is used in each run of the scheme. If any session key is compromised, it should not have an impact on other session keys. In our scheme, knowing the session key $SK = f(ID_i \| C_{y_i} \| D_{y_i} \| r_s \| r_c)$ and the random numbers r_c and r_s, it is of no use to compute the other session keys. Since it is impossible to compute the session key without knowing the correct random values in another session. Extracting any value from the session key is also not possible due to the security of one-way function. Therefore, our scheme can provide the known session key security.

5 Performance analysis

In this section, we provide a comparison of our scheme with different related schemes. The measures of our comparisons are communication cost (Table 1) and security features (Table 2). For fair comparisons, we assume the following:

- the identifications and the timestamp can be represented with 32 bits
- a point in an elliptic curve can be represented with 163 × 2 = 326 bits

- the output size of the secure one-way hash functions is 160 bits
- the size of a random number is 64 bits
- the size of an exponent result 1,024 bits.

We have presented the total communication cost needed for a scheme to authenticate the user and server (refer to Table 1).

Table 1 Communication cost in login and authentication phases

Schemes	*User → Server*	*Server → User*	*Total comm. cost (in bits)*
Lee et al. (2003)	(32 + 32 + 326 + 326 + 326) + (32 + 160)	(326 + 160)	1,720
Chaturvedi et al. (2013)	(1,024 + 160 + 1,024 + 32)	(160 + 1,024 + 32)	3,456
Chaturvedi et al. (2013)	(1,024 + 160 + 1,024 + 32)	(160 + 1,024 + 32)	3,456
Karuppiah and Saravanan (2014)	(1,024 + 160 + 1,024) + (1,024 + 32)	(160 + 64 + 32)	3,520
Proposed scheme	(1,024 + 160 + 160 + 320 + 32) + (160 + 160 + 32)	(2,048)	2,048

Table 2 Security features

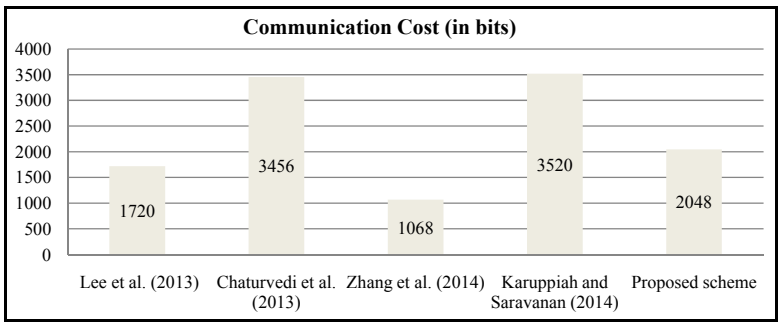
Schemes	*Lee et al. (2003)*	*Chaturvedi et al. (2013)*	*Zhang et al. (2014)*	*Karuppiah and Saravanan (2014)*	*Proposed scheme*
Mutual authentication	Y	Y	Y	Y	Y
Efficient login phase	N	Y	N	Y	Y
Efficient password change phase	N	Y	N	Y	Y
Resist replay attack	Y	Y	Y	Y	Y
Resist insider attack	Y	Y	Y	Y	Y
Resist user impersonation attack	Y	Y	Y	Y	Y
Resist server impersonation attack	Y	Y	Y	Y	Y
Resist stolen verifier attack	Y	Y	Y	Y	Y
User anonymity	N	Y	Y	Y	Y
Withstand offline password guessing attack	Y	Y	Y	Y	Y
Session key agreement	N	Y	Y	Y	Y

Notes: Y = yes, N = no.

We have presented security functionality comparison of our scheme with other related schemes under consideration and we have found that our scheme provides maximum security (refer to Table 2). After comparing the results from both Tables 1 and 2, we have found that the schemes (Chaturvedi et al., 2013; Karuppiah and Saravanan, 2014) have

same security features, however they have more communication cost to achieve theses requirement. This makes our scheme better than other schemes.

Figure 4 Graphical representation of communication cost of various schemes



6 Conclusions

In this paper, we have discussed a new remote user authentication scheme based on the tangent theorem of a circle with RSA cryptosystem. In this scheme we have used points on a circle to authenticate the user. The radius and centre of the circle are not same for every user in every login session that provides the unpredictability and prevents different attacks. It provides freedom to choose and change password to a user at any time. A user and the sever both authenticate each other to enhance its security. No wastage of communication cost takes place if the wrong password is entered. The communication cost is also saved during the password change phase as the server is not involved in password change scenario. Thus, our scheme provides various security requirements and saves the communication cost as well.

References

Chaturvedi, A., Mishra, D. and Mukhopadhyay, S. (2013) 'Improved biometric-based three-factor remote user authentication scheme with key agreement using smart card', *Lecture Notes in Computer Science*, Vol. 8303, pp.63–77, DOI: 10.1007/978-3-642-45204-8_5.

Chien, H.Y., Jan, J.K. and Tseng, Y.M. (2001) 'A modified remote login authentication scheme based on geometric approach', *The Journal of Systems and Software*, Vol. 55, No. 3, pp.287–290.

Das, M.L. Das, Saxena, A. and Gulati, V.P. (2004) 'A dynamic ID-based remote user authentication scheme', *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp.629–631.

Juan, Q. and Zou, L.M. (2013) 'An improved dynamic id-based remote user authentication with key agreement scheme', *Journal of Electrical and Computer Engineering*, Vol. 2013, pp.1–5 [online] http://dx.doi.org/10.1155/2013/786587.

Karuppiah, M. and Saravanan, R. (2014) 'A secure remote user mutual authentication scheme using smart cards', *Journal of Information Security and Application*, Vol. 19, No. 11, pp.282–294, Elsevier.

Kocher, P., Jaffe, J. and Jun, B. (1999) 'Differential power analysis', *Advances in Cryptology CRYPTO 99, Lecture Notes in Computer Science*, Vol. 1666, pp.388–397.

Kumar, M., Gupta, M.K. and Kumari, S.(2010) 'A remote login authentication scheme with smart cards based on unit sphere', *Indian Journal of Computer Science and Engineering*, Vol. 11, No. 3, pp.192–198.

Kumari, S. and Om, H. (2015) 'Remote login password authentication scheme using tangent theorem on circle', Springer, *Proceedings of 3rd International Conference on FICTA-2014, Advances in Intelligent Systems and Computing*, Vol. 328, pp.721–728.

Lamport, L. (1981) 'Password authentication with in secure communication', *Communications of the ACM*, Vol. 24, No. 11, pp.770–772.

Lee, C.C., Li, C.T., Weng, C.Y., Jheng, J.J., Zhang, X.Q. and Zhu, Y.R. (2013) 'Cryptanalysis and improvement of an ECC-based password authentication scheme using smart cards', *Lecture Note in Computer Science*, Springer, Vol. 8300, pp.338–348, DOI: 10.1007/978-3-319-03584-0_25.

Leu, J.S. and Hsieh, W.B. (2014) 'Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards', *IET Information Security*, Vol. 8, No. 2, pp.104–113.

Liaw, H.T. (1995) 'Password authentication using triangle and straight lines', *Computers & Mathematics with Applications*, Vol. 30, No. 9, pp.63–71, Elsevier.

Liaw, H.T. and Lei, C.L. (1995) 'An efficient password authentication scheme based on a unit circle', *Cryptologia*, Vol. 19, No. 2, pp.198–208.

Messerges, T.S., Dabbish, E.A. and Sloan, R.H. (2002) 'Examining smartcard security under the threat of power analysis attacks', *IEEE Trans. Comput*., Vol. 51, No. 5, pp.541–552.

Ramesh, S. and Bhaskaran, V.M. (2014) 'A secured and improved dynamic id based remote user authentication scheme using smart card and hash function for distributed systems', *International Journal on Computer Science and Engineering*, Vol. 6, No. 8, pp.305–320.

Wang, S., Bao, F. and Wang, J.(2004) 'Comments on yet another log-in authentication using n-dimensional construction', *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp.606–608.

Wang, S.J. (2003) 'Remote table based log-in authentication upon geometric triangle', *Computer Slandered and Interface*, Vol. 26, No. 2, pp.85–92.

Wang, S.J. (2003) 'Yet another login autentication using N-dimensional construction based on circle property', *IEEE Trans. on Comsumer Electionics*, Vol. 49, No. 2, pp.337–341.

Wang, Y., Liu, J., Xiao, F. and Dan, J. (2009) 'A more efficient and secure dynamic ID-based remote user authentication scheme', *Computer Communications*, Vol. 32, No. 4, pp.583–585.

Wen, F. and Li, X. (2012) 'An improved dynamic ID-based remote user authentication with key agreement scheme', *Computers and Electrical Engineering*, Vol. 38, No. 2, pp.381–387.

Wu, T.C. (1995) 'Remote login authentication shceme based on a geometric approach', *Computer Communications*, Vol. 18, No. 12, pp.959–963.

Zhang, Z., Qi, Q., Kumar, N., Chilamkurti, N. and Jeong, H.Y. (2014) 'A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography', *Multimedia Tools and Application*, Springer, Vol. 74, No. 10, DOI: 10.1007/s11042-014-1885-6.