An ECC Based Remote User Authentication Protocol

Akasha Shafiq[1], Izwa Altaf[1], Khalid Mahmood[1], Saru Kumari[2], Chien-Ming Chen[3]

[1] Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus, Pakistan
[2] Department of Mathematics, Chaudhary Charan Singh University, Meerut-250004, Utlar Pradesh
[3] College of Computer Science and Engineering, Shandong University of Science and Technology, China
akasha.shafiq75@gmail.com, izwaaltaf01@gmail.com, khalid.mahmood@cuisahiwal.edu.pk,
saryusiirohi@gmail.com, chienmingchen@ieee.org

Abstract

IoT has remarkably broaden the universal network of information barter, because millions of the communication devices have become the ingredients of global network. Apart from the abundant advantages of the expansion of global network, secure authentication and communication between global networking elements are posing numerous challenges. To expedite user authenticity with the help of elliptic curve cryptography a new efficient scheme is introduced in contrast to the previous schemes. Security analysis of proposed scheme is affirmed through random oracle model. Moreover, performance and security analysis show that the proposed scheme prevents the major attack and provides additional security features. The performance analysis is carried out by implementing the proposed protocol using python language in ubuntu. Thus, because of the better security and performance, proposed protocol is adequate for the resource constrained and security sensitive environments.

Keywords: Remote-User, ECC, Authentication, Ubuntu, Pycharm

1 Introduction

Rapid growth of wireless communication technologies has laid a very powerful impact on our life. A very large community in the world are getting the benefits of the wireless technology via wireless devices like mobile phones, notebooks and various other wireless devices. Due to these wireless devices, large amount of people at any location and at any time are enjoying the online services. There are various kinds of online services being provided, such as web browsing, video calls, telemedicine system and government assistance. An attacker can easily eavesdrop the information shared between legal users and can also change or intercept information. It is due to the fact that the Internet structure is still prone to attacks, as it is easily accessible to anyone. To make the shared messages secure between legal participants, we need an authentication protocol. Early on authentication protocol were based on single factor i.e. password. As the first attempt only, Lamport [1] introduced password based authentication protocol. Therefore, many people started working on password based authentication protocols and many password based protocols were developed by researchers [2-7].

Although, password based authentication attracted the researchers and provided a foundation for new protocols. Later on, it is realized that just password based authentication is not enough as it can easily be cracked. After that, researchers proposed two-factor authentication protocols [8-17] to bring more security. In two factor authentication protocols, smart card of the user is used as the additional factor along with password.

Though, two-factor authentication protocols provide more reliability and security but many systems are constrained in terms of resource utilization in communication technologies. However, these systems obliged two-factor authentication protocols that include lightweight computational operations like hash operations and arbitrary numbers. To accomplish reasonable security, a computationally effective and efficient protocol is proposed by Tsai et al. [18], which uses hash operations and arbitrary numbers. Many other lightweight protocols are also developed in [19-21], in which security has been compromised to a certain level by minimizing the computation cost. We determine that lightweight protocols does not provide enough security and reliability and thus these protocols are prone to attacks easily [22-23].

To decrease the cost of transmission and computation, Juang et al. [24] used the ECC based system for the session key exchange and authentication protocol. Xu et al. [25] observed that two protocols of Lee et al. [26-27] are not secure against password guessing and impersonation attacks, they proposed a more efficient two-factor based protocol against the described attacks. Further, Juang et al. demonstrates the enhanced security feature of their protocol by using the Diffie-Hellman protocol's assumption.

*Corresponding Author: Chien-Ming Chen; E-mail: chienmingchen@ieee.org
DOI: 10.3966/160792642020012101024

Later, Sood et al. [28] and Song [29] discovered that the Xu et al.'s protocol does not give much security against masquerading and privileged insider attacks. Therefore, they proposed an improved protocol that provides security against the expected security threats. After that, Chen et al. [30] performed the analysis of both the enhanced protocols and stated that Sood et al.'s protocol is not offering mutual authentication also Song et al.'s protocol does not resist password guessing and smart card stolen attack. Therefore, Chen et al. proposed a better scheme and claimed that their enhanced scheme provides security against many attacks. Afterwards, Jiang et al. identified that Chen et al.'s protocol does not resist offline dictionary attack, also does not maintain anonymity of the user.

Qu and Tan [31] then proposed two factor based key exchanging protocol for mutual authentication. However, Huang et al. [32] showed that Qu et al.'s scheme is still prone to smart card stolen and masquerading attack. Therefore, Huang et al. proposed an enhanced authentication and key exchanging protocol. Then, Chaudhry et al. [33] claimed that Huang et al.'s protocol does not resist user masquerading attack and also proposed an enhanced scheme that prevent this attack. Moreover, we have analyzed that Chaudhry et al. [32] scheme is still vulnerable to smart card stolen attack. In 2017, Nikooghadam et al. [34] presented a authentication protocol later which was cryptanalyzed by Limbasiya et al. [35] meanwhile many other RUA protocols were presented [36-46].

In this paper, we have presented more secure, efficient and lightweight remote user key exchanging protocol. Architecture for remote-user authentication is shown in Figure. 1.

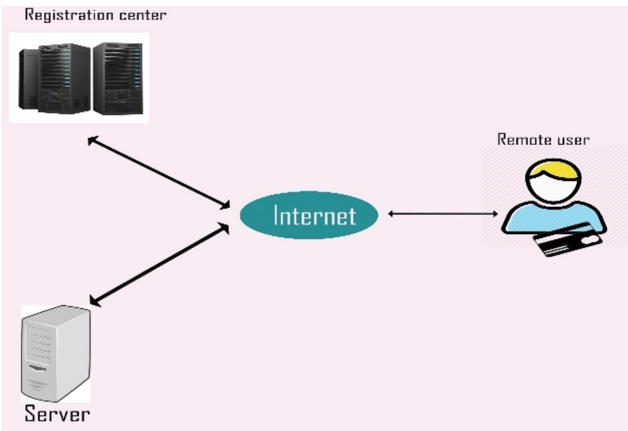


Figure 1. Remote-user authentication

1.2 Motivation and our Contribution

The protocols for authentication of user should be lightweight and secure. Several protocols are presented in recent time but those protocols not provides enough security also they are not lightweight. To remove above described flaws we proposed, a new ECC based remote user authentication scheme. Our presented scheme has several advantages which are as follows:

1. By sharing the session key, the server and user can validate each other.
2. Presented protocol secures identity of user from the attacker/adversary.
3. Attacker/adversary is unable to calculate the session key if he has the smart card of the user.
4. Presented scheme provides security against major attacks.
5. Protocol is efficient in terms of resource utilization.

1.3 Paper Structure

This paper is divided into the following sections: Sect.1 presents introduction. In Sect.2 , preliminaries are demonstrated. In Sect.3, our proposed protocol is described. Sect.4, describes the formal security analysis of proposed scheme. In Sect.5, there is performance and security comparison. In Sect.6, presented work is concluded.

2 Preliminaries

In this section, the major basics of the commonly used adversarial model, ECC, hash function and several notations used in this paper are described. Some commonly used notations are shown in Table 1.

2.1 Proposed Architecture for Remote User Authentication

Figure 2 shows that U_r through his smart card register himself on the server via a secure channel whereas an attacker has no access of the secure channel. Figure 3 depicts the login and authentication phase U_r send login request to server via a public channel, however adversary has the access to public channel and can eavesdrop, intercept, and modify the message.

Figure 2. Remote user registration

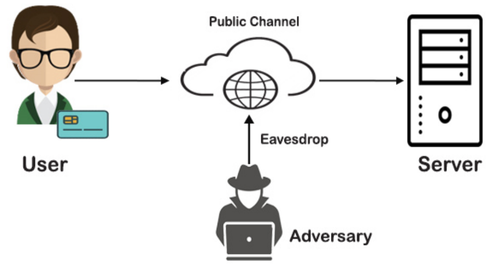


Figure 3. Remote user login and authentication

2.2 Elliptic Curve Cryptography (ECC)

The equation of Elliptic curve has defined in the form $E_P(a,b): x^2 = y^3 + ax + b$ over a prime finite field $(x,y) \in W_P^* \times W_P, a, b$ and $4a^3 + 27b^2 \neq 0 (\bmod P)$ in which P is a selected huge prime number, the size of P is ≥ 160 bits. Scalar product is gained by repeated addition e.g., $nt = t + t + t + ... + t$ (*n times*), over a determined t a point on $E_P(e,f)$ and the multiplier n. The variables (*e, f, t, P, n*) should be the member of limited field F_P. The E is supposed to be the abelian group, whereas O is stated as the *ID*'s infinity point.

Table 1. Notation table

Symbols	Details
U_r	r^{th} Legitimate user
ID_r	User identity
PW_r	User password
S	Legitimate server
ssk	Server's private key
spk	Server's public key
SC_r	User's Smart card
SK	Session Key
a_r	Random number chosen by U_r during registration phase
$\oplus$	XOR operator
$\|\|$	Concatenation operator
h	Hash function

Definition 1 (Logarithmic issues in ECDLP)

ECDLP: Given two specified points over $R, V \in E_P(e,f)$, calculate n a scalar so that $R = nV$. The chances that attacker A can find n in the polynomial time (T) are described as $Adv_X^{ECDLP}(T) = pr[(X(R,V) = x : xx \in W_P)]$. ECDLP assumption concludes that $Adv_X^{ECDLP}(T) \leq \in$.

2.3 Hash Function

By taking an input string $O = H(String)$ of random size, a fixed size output is generated by hash. Generated output is called hash code. A little change in the value of string can cause a huge difference. Whereas, a secure hash function has following specifications.

- If the string is described, it's easy to compute $O = H(String)$.
- If $O = H(String)$ is described, it is impossible to find out the string.
- It is tedious task to distinguish input of *String*1 and *String*2 so that *H*(*String*1) = *H*(*String*2). This property is named as collision resistance.

Definition (Characteristics of Collision Resistance)

Secure hash function H(.) is predetermined for collision resistance. The possibility that an attacker A can find a pair ($String_1 \neq String_2$) as $H(String_1) = H(String_2)$ is separated as $Adv_A^{HASH}(t) = prb[(String_1, String_2) \Leftarrow_r A : (String_1 \neq String_2), \ H(String_1) = H(String_2)]$, where attacker is allowed to choose a pair ($String_1$, $String_2$) randomly. Attacker's perk is calculated against the random selections taken with-in polynomial time (t). Further, Collision resistance conclude that $Adv_A^{HASH}(t) \leq \in$ whereas $\in <0$, is an enough tiny amount.

2.4 Adversarial Model

The basic adversarial model as stated in [44-46] is described in this paper. Following steps were taken up according to the ability of the attacker A:

(1) A has control over all the communication channels which are public. A can extract, replay, update, abolish or communicate a new replicated message.

(2) A, through power analysis, can get or leak out [47-50] the stored information in a smart card.

(3) A may be a deceitful or intruder user or the server.

(4) The identities of servers and users are not private but familiar to insiders.

(5) A cannot instigate attack on the server as it is thought to be secure.

3 Proposed Scheme

This section discusses the proposed protocols for remote user authentication. Proposed protocol provides desired security to make it invincible against major security attacks and is more efficient than previous remote user authentication schemes.

3.1 Registration Phase

For registering the user, each user U_r chooses his ID_r, PW_r and a_r. After that U_r calculate RP_r by applying functions of one way hash that is embedded with the concatenation of PW_r and a_r. Then U_r sends, $\{ID_r, RP_r\}$ to S, via a protected channel. On receiving these values, S calculates:

$$\alpha_r = h(ID_r \| ssk)$$
$$\beta_r = RP_r \oplus \alpha_r$$
$$\lambda_r = h(ID_r \| RP \| \alpha_r)$$

S via a protected channel, then reserve the β_r and λ_r in U_r's smart card. The U_r then inserts a_r in smart card after receiving it from server S. Now, the smart card contains these values $\{\beta_r, \lambda_r, a_r\}$.

3.2 Login Phase

Step LO 1: U_r inserts the smart card in the card reader and enters his unique ID_r and PW_r. Smart card SC_r then calculates:

$$RP_r = h(PW_r \| a_r)$$
$$\alpha_r = RP_r \oplus \beta_r$$
$$\lambda_r \overset{?}{=} h(ID_r \| \alpha_r \| RP_r)$$

Then, U_r checks that the λ_r equals to value stored in smart card. If both of these values are equal then the unique ID_r and PW_r is considered valid, else the session will be terminated.

Step LO 2: Smart card capitulates q_r and calculates $Q_r = q_r.p$ whereas, p is a point on elliptic curve. Moreover, computes:

$$M_r = q_r.spk$$
$$PID_r = ID_r \oplus M_r$$
$$\tau_r = h(ID_r \| \alpha_r \| Q_r \| M_r)$$

After calculating these values, user U_r sends $\{PID_r, \tau_r, Q_r\}$ towards S.

U_r **S**

Registration Phase

Choose ID_r, PW_r, a_r

$RP_r = h(PW_r \| a_r)$

$\xrightarrow{\{ID_r, RP_r\}}$

$\alpha_r = h(ID_r \| ssk)$

$\beta_r = RP_r \oplus \alpha_r$

$\lambda_r = h(ID_r \| RP \| \alpha_r)$

Store $\{\lambda_r, \beta_r\}$

$\xleftarrow{SC_r}$

Stores a_r *in smart card*

U_r **S**

Login and Authentication phase

Input ID_r, PW_r

Calculate $RP_r = h(PW_r \| a_r)$

$\alpha_r = RP_r \oplus \beta_r$

$\lambda_r \overset{?}{=} h(ID_r \| \alpha_r \| RP_r)$

Generate q_r and $Q_r = q_r.p$

$M_r = q_r.spk$

$PID_r = ID_r \oplus M_r$

$\tau_r = h(ID_r \| \alpha_r \| Q_r \| M_r)$

$\xrightarrow{\{PID_r, \tau_r, Q_r\}}$

Compute $M_r^{'} = ssk.Q_r$

$ID_r^{'} = PID_r \oplus M_r^{'}$

$\tau_r^{'} = h(ID_r^{'} \| \alpha_r \| Q_r \| M_r^{'})$

Check $\tau_r^{'} \overset{?}{=} \tau_r$

Generate q_s

Compute $Q_s = q_s.Q_r$

$N_s = Q_s \oplus M_r$

$\tau_s = h(\alpha_r \| ID_r \| Q_s)$

$\xleftarrow{\{N_S, \tau_S\}}$

$Q_s^{'} = N_s \oplus M_r$

$\tau_s^{'} = h(\alpha_r \| ID_r \| Q_s)$

$\tau_s^{'} = \tau_s$

$SK = h(ID_r \| Q_r \| Q_s \| M_r)$

Proposed Scheme

3.3 Authentication Phase

For authenticating, S performs following steps against login entries that the user Ur sends.

Step AU 1: After receiving login request server computes:

$$M_r^{'} = ssk.Q_r$$
$$ID_r^{'} = PID_r \oplus M_r^{'}$$
$$\tau_r^{'} = h(ID_r^{'} \| \alpha_r \| Q_r \| M_r^{'})$$

After that S inspects either $\tau_r^{'} \overset{?}{=} \tau_r$ if the condition does not hold true then session will be aborted, otherwise U_r is supposed as legitimate user. Then server S generates arbitrary number q_s and further computes:

$$Q_s = q_s.Q_r$$
$$N_s = Q_s \oplus M_r$$
$$\tau_s = h(\alpha_r \| ID_r \| Q_s)$$

Server then sends $\{N_s, \tau_s\}$ against the login request from the user U_r.

Step AU 2: U_r then calculates

$$Q_s^{'} = N_s \oplus M_r$$
$$\tau_s^{'} = h(\alpha_r \| ID_r \| Q_s)$$

U_r checks the condition $\tau_s^{'} = \tau_s$. Session will abort if this condition does not hold true, else U_r computes session key as follows:

$$SK = h(ID_r \| Q_r \| Q_s \| M_r)$$

4 Security Analysis

4.1 Informal Security Analysis

In this portion the proposed protocols of security analysis has explained.The security analysis demonstrates that our proposed scheme prevents all the major possible attacks. Detailed analysis is given below.

4.1.1 Smart Card Stolen Attack

Let's suppose an adversary *A* steals the U_r's smart card and retrieves values β_r, λ_r and an arbitrary number a_r. Still *A* can not extract ID_r because, to calculate correct value of β_r , *A* needs to server's private key ssk. To calculate the value of λ_r , he needs RP_r which includes PW_r of U_r. That's why it is not beneficial for *A*, even if he steals the smart card of U_r.

4.1.2 User's Privacy and Anonymity

U_r identity is not transferred in plain text in proposed protocol. Further, the smart card leaves no traces of U_r's identity. Moreover, the calculation of $Q_r=q_r.p$ consists of random number q_r, whereas the random number is session specific. Therefore, it is hard to extract ID_r of legal U_r and to find out that either same U_r has initiated the two or more different sessions.

4.1.3 Mutual Authentication

In our proposed protocol, *S* authenticates U_r by checking whether $\tau_r' \stackrel{?}{=} \tau_r$. If an adversary wants to compute τ_r correctly, he has to compute $h(ID_r' \parallel \alpha_r \parallel Q_r \parallel M_r')$ which requires U_r's smart card. Moreover, *S* is authenticated by U_r by checking $\tau_s' \stackrel{?}{=} \tau_s$ whereas, $\tau_s = h(\alpha_r \parallel ID_r \parallel Q_s)$ and it requires server's private key *ssk* to extract ID_r of legal U_r. Thus, our proposed protocol ensures mutual authentication.

4.1.4 Server and User Impersonation Attack

For authenticating the login request $\{PID_r, \tau_r, Q_r\}$ and challenge message $\{PID_r, \tau_r, Q_r\}$, it is important to know that legal challenge message can only be generated by the legal *S* as it includes RP_r and to calculate it PW_r is required. On the other hand, only the legal *S* can answer to the authentication message via the challenge message $\{N_s, \tau_s\}$.

4.1.5 Stolen Verifier and Insider Attack

Our proposed protocol doesn't maintain any table in the database. Moreover, *S* also does not maintains any parameter or data related to the PW_r of U_r. that may helps to null and void stolen verifier attack. Also, PW_r of U_r is not being exposed because it not sent in the plain text. So, any insider can't misuse the password of U_r.

4.1.6 Password Guessing Attack

Password PW_r of U_r is protected with the random number a_r. Moreover, the hash is being implemented on the concatenation of the PW_r and random number a_r. Further, the smart card is secured in such a way that it doesn't provide any kind of hint of U_r's password PW_r validity. Therefore, it's impossible for an adversary *A* to launch this attack in proposed scheme.

4.1.7 Replay Attack

Consider *A* can intercepts U_r's request message and replays it after some time, but *A* will not able to answer the challenge message that comes from *S.* As the calculation of PID_r includes random number that makes it session specific. That's why, on proposed protocol replay attack is not possible.

4.1.8 Perfect Forward Secrecy

SK which is calculated among *S* and U_r encompasses Q_r and Q_s consisting of random numbers from both participants reciprocally. Thus, if *A* can get previous secret keys of any promoter, still *A* will not be able to find that two different sessionsare initiated by same user. So, proposed scheme offers perfect forward secrecy.

4.1.9 No Clock Synchronization

No time stamp is used by both participants, user and server, rather they generate their own random numbers. Therefore, precious resources are being saved by avoiding clock synchronization.

4.2 Formal Security Analysis

To show that our proposed protocol is protected, we have adopted same analysis mechanism which is mentioned in [33]. For the analysis purpose, below oracles are described:

- ***Reveal:*** The purpose of this oracle is to output a string *Z* through one way hash function as *Y* = *h*(*Z*).
- ***Extract:*** For a given input at a point *O* = *kU* and *U* this oracle returns a scalar *k*.

Theorem 1. Proposed protocol is absolutely protected against an adversary A for the perseverance of the U_r's identity (ID_r), secret key (ssk) of S, calculated SK among U_r and S under hard supposition of ECDLP and random oracle protected hash functions.

Proof 1. Suppose A has abilities to extract U_r's identity ID_r, S's private key ssk and calculates SK. For this purpose A performs $EXPE1_{A,PRUSAS}^{ECDLP,HASH}$ algorithmic experiment authentication protocol PRUAS against solicited remote-user through simulating oracles Reveal and Extract.We have defined probability achieved of above mentioned analysis as $Suce_1 = |\Pr b[EXPE1_{A,PRUSAS}^{ECDLP,HASH} = 1] - 1|$. Benefits taken by adversary A is described as $\max_A(Suce_1) = A1_{A,TFBAMS}^{HASH,ECDLP}(t_e, q_{ex}, q_{rv})$,

Algorithm 1. $\mathrm{EXPE1}_{\mathrm{A,\ PRUSAS}}^{\mathrm{ECDLP,\ HASH}}$

Intercept log*in* message $\{PID_r, \tau_r, Q_r\}, \tau_r = \mathrm{h}(\mathrm{ID}_r \| \alpha_r \| \mathrm{Q}_r \| \mathrm{M}_r), \mathrm{Q}_r = q_r.P$
Call the Reveal on oracle τ_r and get $\mathrm{h}(\mathrm{ID}_r \| \alpha_r \| \mathrm{Q}_r' \| \mathrm{M}_r) \leftarrow$ Reveal(τ_r)
Call the Reveal on oracle $\mathrm{h}(\mathrm{ID}_r \| \mathrm{M}_r)'$ and get $(\mathrm{ID}_r' \| \mathrm{M}_r'') \leftarrow$ Reveal $(\mathrm{h}(\mathrm{ID}_r \| \mathrm{M}_r)')$
if $(\mathrm{M}_r'' = \mathrm{M}_r')$ then
  Compute $\tau_r' = h(ID_r' \| \alpha_r' \| Q_r \| M_r')$
  if $(\tau_r = \tau_r')$ then
    Accept ID_r'
    Compute $\mathrm{ssk}' = (ssk \oplus ID_r') \oplus ID_r'$
    Eavesdrop the challenge message $\{\mathrm{N}_s, \tau_s\}$, Where $\mathrm{N}_s = Q_s \oplus M_r$, $\tau_s = h(\alpha_r \| ID_r \| Q_s)$
    Compute $\mathrm{Q}_s' = N_s \oplus M_r$
    Compute $\tau_s' = h(\alpha_r \| ID_r \| Q_s)$
    if $(\tau_s' = \tau_s)$ then
      Accept ssk
      Calculate $\mathrm{SK} = \mathrm{h}(\mathrm{ID}_r \| \mathrm{Q}_r \| \mathrm{Q}_s \| \mathrm{M}_r)$
    else
      return Fail
    end if
  else
    return Fail
  end if
else
  return Fail
end if

Whereas adversary A can take maximum of q_{rv} Reveal and q_{ex} Extract inquiries. According to analysis adversary A can calculate ID_r, ssk and SK if and only if he can inverse 1 the protected hash function and 1 breach ECDLP. Therefore, cited to the Definition 1, to inverse the protected hash function is infeasible to calculate in polynomial time, as by the Definition 1 to breach ECDLP is impossible to calculate. Thus, we have $A1_{A,PRUAS}^{HASH,ECDLP}(t, q_{ex}, q_{rv}) \leq \varepsilon$. Hence, improved authentication of remote user protocol is invulnerable A to calculate U_r's ID_r, S's private key ssk and calculate SK.

5 Performance and Security Comparisons

This section demonstrates the security and performance analysis of proposed protocol. Performance of the proposed scheme has verified by using following tools which are described as, cryptographic functions used in proposed scheme were implemented using inbuilt PyCrypto library in Ubuntu 19.04, with system specifications, 16.0 GB RAM and 3.60 GHZ processing power with core i7 using python programming language. The proposed protocol was implemented various times under similar conditions to get the average time. The amount of time require for XOR and concatenation is negligible that's why these values are not considered. Moreover, hash operation, point multiplication and point addition takes 0.00093 ms, 0.00037 ms and 0.00028 ms, respectively. Values for identity, password, time stamp, random number, XOR and P are supposed to be 160 bits. Whereas, hash value is considered 256 bits and encryption/decryption, server public key and private key value is considered as 512 bits. The following notations are used to describe computation cost:

t_h time for calculating hash function.
t_m time for calculating the dot product.
p_a time for calculating point addition.
$t_\oplus$ time for calculating XOR.
$t_\|$ time for calculating concatenation.

5.1 Cost of Storage

This section describes the storage cost of proposed protocol in comparison of other protocols. Storage cost is basically the storage required for credentials stored in SC_r and database.

The total storage cost of our protocol is 672. Moreover, cost of storage for Qu and Tan's [31], Huang et al.'s [32] and Chaudhry et al.'s [33] are 928 bits, 672 bits and 928 bits, respectively. Storage cost is described in Table 2 and Figure 4. The number of bits are represented on Y-axis and protocols are represented on X-axis, shown in Figure 4. It demonstrates that the storage cost of proposed protocol is less than [31, 33] and almost equal to [32] protocol.

Table 2. Storage cost

Protocols	Storage cost
Qu et al. [31]	928
Huang et al. [32]	672
Chaudhry et al. [33]	928
Proposed	672

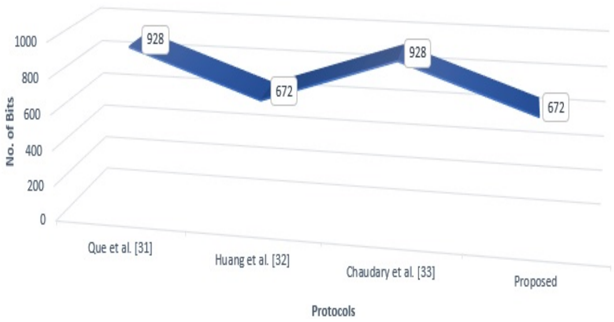


Figure 4. Storage cost comparison

5.2 Cost of Communication

Comparison and analysis of communication cost of the proposed scheme in compare to the other protocols are carried out in this section. Proposed protocol requires 211 bits for communication. Likewise, communication cost of Qu et al.'s, Huang et al.'s and Chaudhry et al.'s protocol are 3392 bits, 3136 bits, 2880 bits, respectively shown in Figure 5 and Table 3. Whereas, Figure 5 states that the communication cost of proposed protocol is less than all related protocols [31-33].

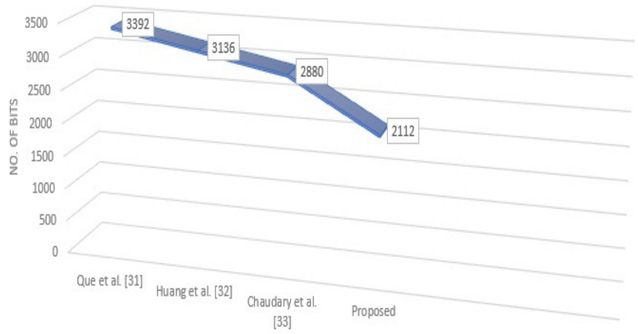


Figure 5. Communication cost comparison

Table 3. Communication cost

Protocols	Cost of Registration (in bits)	Cost of login and Authentication (in bits)	Total Cost (in bits)
Qu and Tan [31]	1184	2208	3392
Huang et al. [32]	928	2208	3136
Chaudhry et al. [33]	928	1952	2880
Proposed	928	1184	2112

5.3 Cost of Computation

In this section, we compare and analyze computation cost of proposed protocol with related protocols shown in Table 4 Proposed protocol carries out, 9 one way hash functions and 4 point of multiplications whereas, the computation cost is calculated in milliseconds(ms).

Table 4. Computation cost

Protocols	Computation Cost	Cost (in ms)
Qu et al. [31]	$9t_m + 5p_a + 13t_h + 2t_{\oplus} + 17t_{\parallel}$	$= 0.01679$
Huang et al. [32]	$6t_m + 1p_a + 17t_h + 7t_{\oplus} + 24t_{\parallel}$	$= 0.01831$
Chaudhry et al. [33]	$6t_m + 1p_a + 12t_h + 5t_{\oplus} + 16t_{\parallel}$	$= 0.01366$
Proposed	$4t_m + 9t_h + 8t_{\oplus} + 17t_{\parallel}$	$= 0.00985$

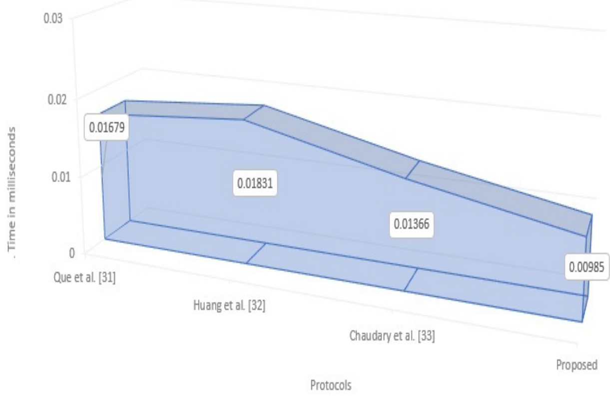


Figure 6. Computation cost comparison

The Figure 6 shows the time required for computation by the related and proposed protocols. The time required in ms is represented on vertical axis whereas, the protocols are represented on horizontal axis.

Whereas P= Provides and NP= Not Provides.

Table 5 shows the comparison of proposed and related protocols in terms of security features. After analyzing Table 3, Table 4 and Table 5 we conclude that the computation, storage and communication cost of proposed protocol is less and provides more security than other protocols.

Table 5. Comparison of security parameters

Protocols	[31]	[32]	[33]	Proposed
Prevents smart card Stolen attack	NP	P	NP	P
Impersonation Attack	NP	NP	P	P
Mutual Authentication	P	P	P	P
Perfect Forward Secrecy	P	P	P	P
Prevents Replay Attack	P	P	P	P
Privacy and Anonymity	P	P	P	P
Prevents Insider and Stolen Verifier Attack	P	P	P	P
Prevents Password Guessing Attack	NP	P	P	P
No Clock Synchronization	P	P	P	P

6 Conclusion

In this paper, using ECC, we have presented lightweight remote user authentication protocol. The extensive analysis has proved that all related protocols are costly and were also vulnerable to some major attacks. So, we have presented an enhanced scheme that proves to be more secure. Moreover, our proposed protocol is precisely analyzed through informal and formal analysis of security. Further, the analysis proved that our proposed protocol is more robust and lightweight in comparison of other related protocols. Thus, due to the enhanced performance and security features, our proposed protocol has proved to be more efficient, lightweight and practical.

References

[1] L. Lamport, Password Authentication with Insecure Communication, *Communications of the ACM*, Vol. 24, No. 11, pp. 770-772, November, 1981.

[2] D. Z. Sun, J. P. Huai, Z. J. Sun, J. X. Li, J. W. Zhang, Z. Y. Feng, Improvements of Juang's Password-Authenticated Key Agreement Scheme Using Smart Cards, *IEEE Transactions on Industrial Electronics*, Vol. 56, No. 6, pp. 2284-2291, June, 2009.

[3] D. He, D. Wang, Robust Biometrics-based Authentication Scheme for Multiserver Environment, *IEEE Systems Journal*, Vol. 9, No. 3, pp. 816-823, September, 2015.

[4] D. He, S. Zeadally, Authentication Protocol for an Ambient Assisted Living System, *IEEE Communications Magazine*, Vol. 53, No. 1, pp. 71-77, January, 2015.

[5] R. Lu, X. Lin, X. Liang, X. Shen, A Dynamic Privacy-Preserving Key Management Scheme for Location-based Services in Vanets, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 13, No. 1, pp. 127-139, March, 2012.

[6] Y. Lu, L. Li, H. Peng, Y. Yang, An Enhanced Biometric-based Authentication Scheme for Telecare Medicine Information Systems Using Elliptic Curve Cryptosystem, *Journal of Medical Systems*, Vol. 39, No. 3, p. 32, March, 2015.

[7] D. Zhao, H. Peng, L. Li, Y. Yang, A Secure and Effective Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks, *Wireless Personal Communications*, Vol. 78, No. 1, pp. 247-269, September, 2014.

[8] D. He, An Efficient Remote User Authentication and Key Agreement Protocol for Mobile Client-server Environment from Pairings, *Ad Hoc Networks*, Vol. 10, No. 6, pp. 1009-1016, August, 2012.

[9] M. S. Farash, M. A. Attari, A Secure and Efficient Identity-based Authenticated Key Exchange Protocol for Mobile Client-Server Networks, *The Journal of Supercomputing*, Vol. 69, No. 1, pp. 395-411, July, 2014.

[10] S.-Y. Chiou, Z. Ying, J. Liu, Improvement of a privacy Authentication Scheme Based on Cloud for Medical Environment, *Journal of Medical Systems*, Vol. 40, No. 4, pp. 101, April, 2016.

[11] L. Zhang, S. Tang, Z. Cai, Robust and Efficient Password Authenticated Key Agreement with User Anonymity for Session Initiation Protocol-based Communications, *IET Communications*, Vol. 8, No. 1, pp. 83-91, January, 2014.

[12] L. Wu, Y. Zhang, L. Li, J. Shen, Efficient and Anonymous Authentication Scheme for Wireless Body Area Networks, *Journal of Medical Systems*, Vol. 40, No. 6, pp. 134, June, 2016.

[13] C. Jin, C. Xu, X. Zhang, F. Li, A Secure ECC-based RFID Mutual Authentication Protocol to Enhance Patient Medication Safety, *Journal of Medical Systems*, Vol. 40, No. 1, pp. 12, January, 2016.

[14] Q. Jiang, J. Ma, Y. Tian, Cryptanalysis of Smart-card-based Password Authenticated Key Agreement Protocol for Session Initiation Protocol of Zhang et al., *International Journal of Communication Systems*, Vol. 28, No. 7, pp. 1340-1351, May, 2015.

[15] A. Irshad, M. Sher, E. Rehman, S. A. Ch, M. U. Hassan, A. Ghani, A Single Round-trip Sip Authentication Scheme for Voice over Internet Protocol Using Smart Card, *Multimedia Tools and Applications*, Vol. 74, No. 11, pp. 3967-3984, June, 2015.

[16] M. S. Farash, M. A. Attari, An Anonymous and Untraceable Password-based Authentication Scheme for Session Initiation Protocol Using Smart Cards, *International Journal of Communication Systems*, Vol. 29, No. 13, pp. 1956-1967, September, 2016.

[17] M. S. Farash, M. A. Attari, Cryptanalysis and Improvement of a Chaotic Map-based Key Agreement Protocol Using Chebyshev Sequence Membership Testing, *Nonlinear Dynamics*, Vol. 76, No. 2, pp. 1203-1213, April, 2014.

[18] J.-L. Tsai, Efficient Multi-server Authentication Scheme Based on One-way Hash Function without Verification Table, *Computers & Security*, Vol. 27, No. 3-4, pp. 115-121, June, 2008.

[19] R. Lu, X. Lin, H. Zhu, X. Liang, X. Shen, BECAN: A Bandwidth-efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, No. 1, pp. 32-43, January, 2012.

[20] Y.-P. Liao, 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, January, 2009.

[21] C.-C. Lee, T.-H. Lin, R.-X. Chang, A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment Using Smart Cards, *Expert Systems with Applications*, Vol. 38, No. 11, pp. 13863-13870, October, 2011.

[22] D. Wang, P. Wang, On the Anonymity of Two-factor Authentication Schemes for Wireless Sensor Networks: Attacks, Principle and Solutions, *Computer Networks*, Vol. 73, pp. 41-57, November, 2014.

[23] D. Wang, D. He, P. Wang, C. H. Chu, Anonymous Two-factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment, *IEEE Transactions on Dependable and Secure Computing*, Vol. 12, No. 4, pp. 428-442, July-August, 2015.

[24] W.-S. Juang, S.-T. Chen, H.-T. Liaw, Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards, *IEEE Transactions on Industrial Electronics*, Vol. 55, No. 6, pp. 2551-2556, June, 2008.

[25] J. Xu, W.-T. Zhu, D.-G. Feng, An Improved Smart Card Based Password Authentication Scheme with Provable Security, *Computer Standards & Interfaces*, Vol. 31, No. 4, pp. 723-728, June, 2009.

[26] S.-W. Lee, H.-S. Kim, K.-Y. Yoo, Improvement of Chien et al.'s Remote User Authentication Scheme Using Smart Cards, *Computer Standards & Interfaces*, Vol. 27, No. 2, pp. 181-183, January, 2005.

[27] N.-Y. Lee, Y.-C. Chiu, Improved Remote Authentication Scheme with Smart Card, *Computer Standards & Interfaces*, Vol. 27, No. 2, pp. 177-180, January, 2005.

[28] S. K. Sood, A. K. Sarje, K. Singh, An Improvement of Wang et al.'s Authentication Scheme Using Smart Cards, *National Conference On Communications (NCC)*, Chennai, India, 2010, pp. 1-5.

[29] R. Song, Advanced Smart Card Based Password Authentication Protocol, *Computer Standards & Interfaces*, Vol. 32, No. 5-6, pp. 321-325, October, 2010.

[30] B. L. Chen, W. C. Kuo, L. C. Wuu, Robust Smart-card-based Remote User Password Authentication Scheme, *International Journal of Communication Systems*, Vol. 27, No. 2, pp. 377-389, February, 2014.

[31] J. Qu, X.-L. Tan, Two-factor User Authentication with Key Agreement Scheme Based on Elliptic Curve Cryptosystem, *Journal of Electrical and Computer Engineering*, Vol. 2014, Article ID 423930, pp. 1-6, May, 2014.

[32] B. Huang, M. K. Khan, L. Wu, F. T. B. Muhaya, D. He, An Efficient Remote User Authentication with Key Agreement Scheme Using Elliptic Curve Cryptography, *Wireless Personal Communications*, Vol. 85, No. 1, pp. 225-240, November 2015.

[33] S. A. Chaudhry, H. Naqvi, K. Mahmood, H. F. Ahmad, M. K. Khan, An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography, *Wireless Personal Communications*, Vol. 96, No. 4, pp. 5355-5373, October, 2017.

[34] M. Nikooghadam, R. Jahantigh, H. Arshad, A Lightweight Authentication and Key Agreement Protocol Preserving User Anonymity, *Multimedia Tools and Applications*, Vol. 76, No. 11, pp. 13401-13423, June, 2017.

[35] T. Limbasiya, M. Soni, S. K. Mishra, Advanced Formal authentication Protocol Using Smart Cards for Network Applicants, *Computers & Electrical Engineering*, Vol. 66, pp. 50-63, February, 2018.

[36] P. Chandrakar, A Secure Remote User Authentication Protocol for Healthcare Monitoring Using Wireless Medical Sensor Networks, *International Journal of Ambient Computing and Intelligence (IJACI)*, Vol. 10, No. 1, pp. 96-116, January-March, 2019.

[37] S. Likitha, R. Saravanan, Cryptanalysis of a Multifactor Authentication Protocol, in: P. Sa, S. Bakshi, I. Hatzilygeroudis, M. Sahoo (Eds.), *Recent Findings in Intelligent Computing Techniques*, Springer, 2019, pp. 35-42.

[38] V. Odelu, An Efficient Two-Server Password-only User Authentication for Consumer Electronic Devices, *2019 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2019, pp. 1-2.

[39] S. F. Chiou, H. T. Pan, E. F. Cahyadi, M. S. Hwang, Cryptanalysis of the Mutual Authentication and Key Agreement Protocol with Smart Cards for Wireless Communications, *International Journal of Network Security*, Vol. 21, No. 1, pp. 100-104, January, 2019.

[40] X. Zhang, B. Wang, W. Zhang, A Robust Authentication Protocol for Multi-server Architecture Using Elliptic Curve Cryptography, *International Journal of Network Security*, Vol. 21, No. 2, pp. 191-198, March, 2019.

[41] C. M. Chen, L. Xu, K. H. Wang, S. Liu, T. Y. Wu, Cryptanalysis and Improvements on Three-party-authenticated Key Agreement Protocols Based on Chaotic Maps, *Journal of Internet Technology*, Vol. 19, No. 3, pp. 679-687, May, 2018.

[42] C. M. Chen, B. Xiang, K. H. Wang, Y. Zhang, T. Y. Wu, An Efficient and Secure Smart Card Based Authentication Scheme, *Journal of Internet Technology*, Vol. 20, No. 4, pp. 1113-1123, July, 2019.

[43] M. Barni, G. Droandi, R. Lazzeretti, T. Pignata, SEMBA: SEcure Multi-biometric Authentication, *IET Biometrics*, Vol. 8, No. 6, pp. 411-421, November, 2019.

[44] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, M. T. M. Shalmani, On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme, *Annual International Cryptology Conference*, Santa Barbara, CA, USA, 2008, pp. 203-220.

[45] D. Dolev, A. Yao, On the Security of Public Key Protocols, *IEEE Transactions on Information Theory*, Vol. 29, No. 2, pp. 198-208, March, 1983.

[46] X. Cao, S. Zhong, Breaking a Remote User Authentication Scheme for Multi-server Architecture, *IEEE Communications Letters*, Vol. 10, No. 8, pp. 580-581, August, 2006.

[47] P. Kocher, J. Jaffe, B. Jun, P. Rohatgi, Introduction to Differential Power Analysis, *Journal of Cryptographic Engineering*, Vol. 1, No. 1, pp. 5-27, April, 2011.

[48] T. S. Messerges, E. A. Dabbish, R. H. Sloan, Examining Smart-card Security under the Threat of Power Analysis Attacks, *IEEE Transactions on Computers*, Vol. 51 No. 5, pp. 541-552, May, 2002.

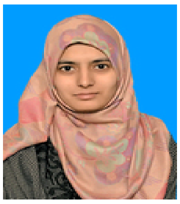
[49] C. M. Chen, B. Xiang, Y. Liu, K. H. Wang, A Secure Authentication Protocol for Internet of Vehicles, *IEEE ACCESS*, Vol. 7, pp. 12047-12057, January, 2019.

[50] C. M Chen, K. H. Wang, K. H. Yeh, B. Xiang, T. Y. Wu, Attacks and Solutions on a Three-party Password-based Authenticated Key Exchange Protocol for Wireless

Communications, *Journal of Ambient Intelligence and Humanized Computing*, Vol. 10, No. 8, pp. 3133-3142, August, 2019.

Biographies

Akasha Shafiq is currently pursuing her MS degree in Computer Science from COMSATS University Islamabad, Sahiwal campus, Pakistan. She received his BS in Computer Science degree with distinction from BZU, Sahiwal campus, Pakistan in 2018. Her research interests include Cloud computing and ECC based Remote-User Authentication.



Izwa Altaf is pursuing her MS degree in Computer Science from COMSATS University Islamabad, Sahiwal Campus, Pakistan**.** She is completed her BS (Honors) Computer Science from International Islamic University, Islamabad, Pakistan. Her research interests are in SIP authentication and information security.

Khalid Mahmood currently working at COMSATS University, Sahiwal Campus. He received Ph.D. degree in Computer Science from International Islamic University, Pakistan in 2018. The title of his Ph.D. dissertation is Secure Authenticated Key Agreement for Smart Grid Communication in Power Sector. His research interests include Lightweight Smart Grid Authentication.

Saru Kumari received Ph.D. degree in mathematics from Chaudhary Charan Singh University, India, in 2012. Currently working as Assistant Professor. She has published more than 133 research papers in reputed journals and conferences, including 115 publications in SCI journals. Her current research interests include information security and applied cryptography.

Chien-Ming Chen received Ph.D. degree from National Tsing Hua University, Taiwan. He is currently an Associate Professor of the Shandong University of Science and Technology, China. He also serves as Associate Editor of the IEEE ACCESS. His current research interests include network security, blockchain, mobile Internet, the IoT, and cryptography.