Accepted Manuscript

An elliptic curve cryptography based lightweight authentication scheme for smart grid communication

Khalid Mahmood, Shehzad Ashraf Chaudhry, Husnain Naqvi, Saru Kumari, Xiong Li, Arun Kumar Sangaiah

PII: S0167-739X(17)30926-3
DOI: http://dx.doi.org/10.1016/j.future.2017.05.002
Reference: FUTURE 3450

To appear in: *Future Generation Computer Systems*

Received date : 19 January 2017
Revised date : 12 April 2017
Accepted date : 5 May 2017

Please cite this article as: K. Mahmood, et al., An elliptic curve cryptography based lightweight authentication scheme for smart grid communication, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.05.002

- We have designed an authentication scheme for smart grid communication.
- The proposed scheme does not require the trusted third party during authentication phase.
- The scheme along with traditional security requirements also provides anonymity and privacy.
- Proposed scheme is secure under threat model of automated tool ProVerif.

An Elliptic Curve Cryptography based Lightweight Authentication Scheme for Smart Grid Communication

Khalid Mahmood[1], Shehzad Ashraf Chaudhry[2], Husnain Naqvi[2], Saru Kumari[3], Xiong Li[4], Arun Kumar Sangaiah[5]

[1] *COMSATS Institute of Information Technology, Sahiwal, Pakistan*

[2] *Department of Computer Science and Software Engineering, International Islamic University, Islamabad, Pakistan*

[3] *Department of Mathematics, Ch. Charan Singh University, Meerut, Uttar Pradesh, India*

[4] *School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China*

[5] *School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu, India*

Abstract

An evolved grid system, Smart Grid, enables appropriate adjustments in the amount of electricity generation by providing the capability to monitor the consumption behavior of customers. This advance grid system can help to promote cultural heritage because it is responsible to provide un-interruptable and reliable power supply in smart way. Smart grid is one of the key component for enabling smart cities and obviously, any city with more smart amenities will ultimately attract visitors to come and visit rich heritage. In smart grid, Supervisory Control and Data Acquisition (SCDA) system is responsible for keeping the underlying communication secure between substations and corresponding control center. While communication between customers and substations needs more enhancements as the existing protocols do not meet the comprehensive security requirements of smart grid. Due to the complex nature of smart grid and diverse security requirements, designing a suitable authentication scheme is a challenging task. For delay sensitive networks like smart grid, an ideal authentication scheme should withstand against all known security attacks, involving lightweight operations with trivial computations. ECC provides same security level with much less key sizes as compared with other security techniques such as RSA, DSA and DH. Keeping in mind the complex and delay sensitive nature of smart grid, a lightweight ECC based authentication scheme is proposed here. The proposed scheme not only provides mutual authentication with low computation and communication cost but also withstand against all known security attacks.

Keywords: Smart Grid, Authentication, Elliptic Curve Cryptography, Lightweight Cryptography, BAN Logic, ProVerif

---

1. Introduction

Cultural heritage can be expressed as the norms, values or the valuable traits of the locality or group of peoples that are acquired from the past generations. These valuable traits are preserved or observed for the prosperity of the current and future generations. Moreover, cultural heritage encompasses natural heritage (natural beauty or landscape etc.), tangible culture (temples, buildings or work of artistry etc.) and intangible culture (values, traditions, power etc.). People from all over the world visit such valuables assets to exchange and inherent healthy culture. Promotion of rich cultures can only be achieved through attracting more visitors. The more amenities provided in the vicinity of cultural landmark attracts more visitors to such places. The idea of smart city environment is to leverage the life of the citizens for their comfort and convenience through pervasive and smart technologies. Smart grid is one of the key enabling solution for transforming conventional cities into smart ones. Therefore, smart city environments with the help of secure smart grid will not only enhance the quick access of cultural heritage but it will also entice more visitors [1, 2, 3].

Making cities smarter is a challenging task to do because diverse technologies needs to be integrated to bring the smartness. More importantly city itself needs to be perceived as a substantial tangled system. Cities are uniquely recognized by their cultural heritage and it is a challenging task to maintain it during smart city development process. Smart grid has a major role in enabling smart cities. Moreover, secure, efficient and fault tolerant power grid can only guarantee desire-able platform for the smart city, which can also help to preserve cultural heritage. Smart grid is responsible to generate and distribute power from the utility to consumer and vice versa as renewable energy sources can also be integrated with the smart grid. Smart grid also provide two-way communication between utility and consumer. Smart grid utilizes diverse communication technologies in order to facilitate communication and this public communication is vulnerable to security breach. Therefore, secure authentication schemes can useful for maintaining the desired privacy and confidentiality. Hence, secure smart grid will set the suitable stage for establishing smart cities and empowering cultural heritage [4, 5].

Smart grid (SG) is the emerging electricity generation infrastructure, capable of monitoring the consumption behavior of customers in order to enable suitable adjustments in the amount of electricity generation, accordingly. Smart grid not only bridges the gap between customers and power producers but it also ensures un-interruptible power supply as a result of efficient controlling and monitoring of the customer's power usage. Generally, smart grid network is comprised of three distinct entities: smart appliances, substations and control center. Smart meters are utilized by smart appliances to exchange information with substations. Customer's requests are communicated with the help of smart meters to substation. Substations then forward these requests to corresponding control center. The control center respond to incoming request accordingly in order to facilitate the remote customers. Communications between control center and corresponding substations is kept secure by the Supervisory Control and Data Acquisition (SCDA) system. The conceptual model of SG to understand the security requirements of it can visualized in Figure. 1. On the other hand security of communication between the customers and substations still demand more attention [6, 7, 8, 9]. Even though numerous security mechanism have been designed in recent years to protect communication between smart appliances and substations but these protocols are not reliable to prevent common attacks [10]. Therefore, a reliable and decisive authentication scheme is inevitable to protect the intermediate communication between smart appliances and substation.

In SG, different devices communicate with each other to exchange information. Prior to this information exchange between the diverse kinds of communicating devices, these devices must be authenticated to ensure secure communication with legitimate entities. The proposed scheme is designed to authenticate such communicating devices using lightweight authentication protocol that make use of elliptic curve cryptography. In this protocol each participant has to register itself with the Trusted Third Party. Then each registered participant can initiate authentication process with another participant to initiate secure session of communication after successful authentication. Authentication process is terminated after exchange of valid session keys between the authenticating participant. Thus, SG architecture is

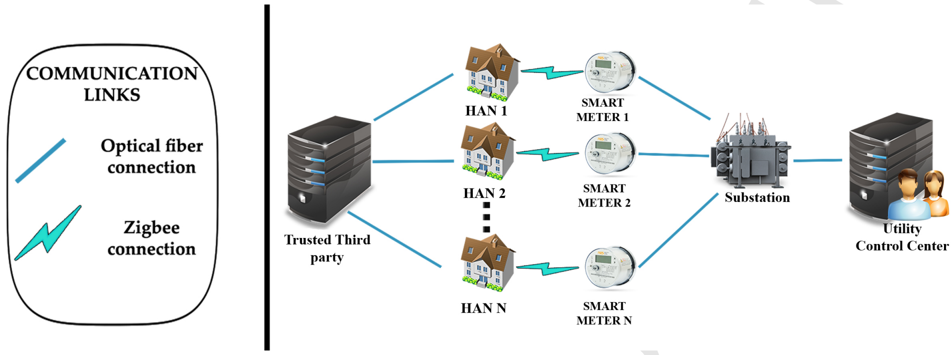

Figure 1: Smart Grid Interacting Entities

complex in nature and involves numerous interacting entities. So designing an appropriate authentication scheme is a tedious task to do due to its diversified security obligations as compared to any other kind of networks such as adhoc and VoIP networks. Ideal authentication schemes not only prevent the security attacks but it also involves lightweight operations with trivial computation for delay sensitive networks such as SG.

Various authentication schemes for communicating entities that are presented so far [11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] are briefly discussed as follows:

T.W. Chim et al. [11] presented an authentication scheme for fortifying the usage pattern of electricity. They utilized a specific device aka temper-resistance device and pseudo identity in order to fortify the customer's privacy for smart appliances and SG network, respectively. Although their scheme is insecure against impersonation attacks and doesn't offer key agreement function. Moreover, their scheme has utilized time-stamp during sign-in procedure that introduces problem of maintaining clock synchronization.

Mostafa et al. [12] introduced computational Diffie-Hellman based authentication scheme for SG network. Their scheme achieves key agreement and mutual authentication for distributed smart meters and smart appliances that are present in the entire SG network. Smart meters along with corresponding smart appliances authenticate each other using a joint session key and hash-based authentication scheme. Mostafa et al. declared that their scheme is lightweight but still its computational complexity is high due to exponential time complexity of some operations.

Li et el. [14] presented multicast scheme for authentication that also utilizes one-time signature in order to overcome the memory overhead and reduce the size of signature. Although computation complexity and authentication delay of the proposed scheme is very low but still it doesn't resolve the key agreement problem. Soohyun et al. [15] take another step to further improve the security for communications of SG. They proposed a key agreement and mutual authentication scheme for securing communication between intelligent devices and data concentration unit (DCU). The mutual authentication is achieved using long term pre-shared keys (PSK) and corresponding public key certificate of DCU. However, long-term sharing become the bottleneck for scalability of the proposed scheme and also make it impractical to be applicable. Gao et al. [18] attempted to incorporate biometric features like fingerprint for achieving tenacious authentication but it proved out to be non-trivial in terms of its computational complexity.

Vaidya et al. introduced a hybrid mechanism of attribute based authorization and multi-factor authentication for SG architecture. The proposed scheme is realized through zero knowledge, public key certificates and access control technologies. Their scheme also suffers due to high computational complexity in terms of public key certificate maintenance.

In order achieve improved security among interacting devices Nicanfar et al. [23] introduced password based authentication using key agreement. Their scheme has the potential to provide forward and backward stealth but again non-trivial operation leads towards hard and expensive implementation. Therefore, in order to reduce computational complexity, Nicanfar et al. presented another scheme using Elliptic Curve Cryptography (ECC) in [24]. Although use of ECC brought huge amount of reduction in computational complexity but restriction to preload the password between home area network and specific device prevents scalability and introduces overhead of maintaining a table for keeping the repository of password.

Lately, Li et al. [25] authentication architecture is designed for SG's advanced metering infrastructure (AMI) and it is proved to be fault-diagnosable. Although, key exchange is not considered along with authentication scheme. Schemes in [25, 12] do not prevent eavesdropping and also scheme in [11] fails to prevent impersonation attack due to absence of key agreement.

Even though few schemes proved to be good in performance but their security level is not up-to the mark. Whereas, some schemes are able to offer reasonable security but their performance doesn't meet the standards due to computational complexity, memory and communication overhead. Hence, the protocols discussed so far are not apt to be implemented and additionally do not protect privacy in SGs. All these reasons motivated us to design a lightweight ECC based authentication scheme. It is due to the fact that ECC offers similar security level with compact key size. It is also proved to be one of the efficient public key cryptosystem in terms of performance as compared to Diffie-Hellman. Moreover, it is observed that public key cryptosystems are more reliable and provide a remarkable trade-off between security and efficiency as compared to various other security techniques. Hence, ECC based authentication scheme can establish enhanced key agreement and it can also insulate privacy with lower computational complexity.

In this paper, ECC based lightweight authentication scheme is presented. Formal and informal analysis is done to assess the performance of the proposed scheme. Moreover, Burrows-Abadi-Needham (BAN) Logic [26] is utilized to investigate the integrity or completeness of the proposed protocol.

1.1. Roadmap of the Paper

Rest of the paper is organized as follows:
Preliminaries pertaining to this paper are presented in section 2. Section 3 elaborates the proposed ECC based lightweight authentication scheme for SG. In section 4 the security validation of the proposed scheme is formalized and proved using an automated tool ProVerif. Furthermore, security analysis of the proposed scheme is illustrated in section 5, whereas BAN logic is utilized to justify its completeness and integrity and this justification is presented in section 6. Performance evaluation of the proposed scheme is envisaged in section 7. Section 8 presents the concluding discussion at the end.

2. Preliminaries

This section elaborates the fundamentals of elliptic curve cryptography, primitive notations and customary adversarial blueprint.

2.1. Elliptic Curve Cryptography

Some fundamental concepts of elliptic curve cryptography (ECC), relevant to this paper are accommodated in this subsection. As compared with previous conventional cryptographic techniques such as DSA, RSA and DH, it has been proved that ECC is more efficient cryptographic technique for security [12-21]. ECC uses much less key size to provide same level of security, as compared with other techniques. The elliptic curve equation $E_p(a, b) : y^2 = x^3 + ax + b \ mod \ p$; is used to define the mathematical operations, where $a, b \in Zp$ and $4a^3 + 27b^2 \ \ mod \ \ p \neq 0$ such that p be a large prime number. The elliptic curve is defined by the values a and b, while the points (x, y) including a point at infinity lie on the elliptic curve, if it satisfies the previous given statement. Given Q as a point and $t \in F_P^*$ as an integer; then repeated addition is used to define as scalar multiplication i.e. $tQ = Q + Q + Q + Q + \ldots + Q(t \ \ times)$. The domain parameters are members of finite field $F_P^* i.e.(p, a, b, P, n, h) \in F_P^*$. E is an abelian group, the identity element of this group is the point which lies at infinity.

2.2. Notation Guide

The primitive notations pertaining to proposed scheme are demonstrated in Table 1.

2.3. Adversarial Model

In this paper, we consider the common adversarial model as mentioned in [27, 28, 29]. Where according to the capabilities of the adversary $\mathcal{A}$, following assumptions are made:

1. $\mathcal{A}$ can access the public communication channel. He can retrieve, modify, replay, inject new message and can discard any message.
2. The Trusted Third Party $\mathcal{T}$ is presumed to be protected, therefore $\mathcal{A}$ cannot obtain the secret key of $\mathcal{T}$.
3. $\mathcal{A}$ knows the public identities of all the users and the $\mathcal{T}$.
4. $\mathcal{A}$ can be an intruder or can be an insincere user of the underlying system.

3. Proposed Scheme

The proposed ECC based lightweight authentication scheme for SG is presented in this section. The scheme is explained in three phases and it is also depicted in Figure. 2.

3.1. Initialization

During initialization phase, the Trusted Third Party (TTP) designated as $\mathcal{T}$ assembles the preliminary parameters. Primarily, elliptic curve $E_p(a, b)$ is considered, then $\mathcal{T}$ picks up a random base point P along-with three one-way hash functions $h_1(.)$, $h_2(.)$ and $h_3(.)$. Thereafter, $\mathcal{T}$ engenders his secret key s and discloses the subsequent parameters $\{E_p(a, b)P, h_1(.), h_2(.), h_3(.)\}$.

Table 1: Notation guide

Notations	Description
$h_1(.),\ h_2(.),\ h_3(.)$	Three one-way hash functions
$\mathcal{T},\ \mathcal{U}_i$	Trusted Third Party, Particular User
ID_i	$\mathcal{U}_i$'s identity
$s,\ PK = s.P$	Private and Public key pair of $\mathcal{T}$
$\mathcal{A}$	An Adversary

3.2. Registration

This phase elaborates the registration procedure. The user $\mathcal{U}_i$ picks up his ID_i and sends it towards $\mathcal{T}$ through reliable medium. The $\mathcal{T}$ deduces $K_{ip} = a_i.P$ and $K_{is} = a_i + sH_1(ID_i, K_{ip})$, after getting the ID_i from the $\mathcal{U}_i$. The registration concludes when the $\mathcal{T}$ sends back these computed K_{ip} and K_{is} to $\mathcal{U}_i$ through reliable medium.

3.3. Authentication

In order to initiate communication with one another in the SG. Each participant or particular user needs to be authenticated with each other. Therefore, the authentication of the registered user $\mathcal{U}_i$ with another registered user $\mathcal{U}_j$ proceeds as follows:

Step 1: $\mathcal{U}_i \longrightarrow \mathcal{U}_j : \{X_i, Y_i, K_{ip}, ID_i, t_i\}$

The registered user $\mathcal{U}_i$, who has the K_{ip} and K_{is}, picks up $x_i \in Z_p$ and sets a time-stamp t_i. Then $X_i = x_i.P$ and $Y_i = x_i + K_{is}H_2(ID_j, X_i, t_i)$ are determined by the $\mathcal{U}_i$. $\mathcal{U}_i$ place an authentication entreaty by transmitting $X_i, Y_i, K_{ip}, ID_i, t_i$ towards $\mathcal{U}_j$

Step 2: $\mathcal{U}_j \longrightarrow \mathcal{U}_i : \{X_j, Y_j, K_{jp}, ID_j, t_j\}$

Against authentication request message from $\mathcal{U}_i$, $\mathcal{U}_j$ checks the freshness of the time-stamp. If the difference between the time-stamps is beyond a specific threshold then session is abruptly terminated, otherwise $\mathcal{U}_j$ proceeds to entertain the authentication request from $\mathcal{U}_j$. Then it corroborates $Y_i.P \stackrel{?}{=} (X_i + K_{ip} + H_1(ID_i, K_{ip})s.P).(H_2(ID_j, X_i, t_i))$, unsuccessful corroboration leads to session termination, otherwise $\mathcal{U}_j$ proceeds to next calculation. Therefore, $\mathcal{U}_j$ computes $X_j = x_j.P$ and $Y_j = x_j + K_{js}H_2(ID_i, X_j, t_j)$ and then determine the shared session key

$\mathcal{U}_i$	$TTP\ \mathcal{T}\ (s,\ PK = s.P)$
Registration Phase:	
Select identity ID_i	
$\xrightarrow{ID_i}$	
	Computes $K_{ip} = a_i.P$
	Computes $K_{is} = a_i + sH_1(ID_i, K_{ip})$
$\xleftarrow{K_{ip}, K_{is}}$	

$\mathcal{U}_i\ (K_{ip}, K_{is})$	$\mathcal{U}_j\ (K_{jp}, K_{js})$
Authentication Phase:	
Select $x_i \in Z_p$, t_i	
$X_i = x_i.P$	
$Y_i = x_i + K_{is}H_2(ID_j, X_i, t_i)$	
$\xrightarrow{X_i, Y_i, K_{ip}, ID_i, t_i}$	
	$T_i - T_j \leq \Delta T$, abort if not fresh
	$Y_i.P \stackrel{?}{=} (X_i + K_{ip} + H_1(ID_i, K_{ip})s.P).(H_2(ID_j, X_i, t_i))$
	$X_j = x_j.P$
	$Y_j = x_j + K_{js}H_2(ID_i, X_j, t_j)$
	$SKij = H_3(x_j.X_i)$
$\xleftarrow{X_j, Y_j, K_{jp}, ID_j, t_j}$	
$T_j - T_i' \leq \Delta T$, abort if not fresh	
$Y_j.P \stackrel{?}{=} (X_j + K_{jp} + H_1(ID_j, K_{jp})s.P).(H_2(ID_i, X_j, t_j))$	
$SKji = H_3(x_i.X_j)$	

Figure 2: Proposed Scheme

as $SKij = H_3(x_j.X_i)$. $\mathcal{U}_j$ then sends a challenge message containing $X_j, Y_j, K_{jp}, ID_j, t_j$.

Step 3: $\mathcal{U}_i \longrightarrow \mathcal{U}_j : \{SKij\}, \mathcal{U}_j \longrightarrow \mathcal{U}_i : \{SKji\}$

The challenge message is entertained by determining the freshness of the time-stamp. If the difference between the time-stamps is beyond a specific threshold then session is immediately terminated, otherwise $\mathcal{U}_i$ determines and verify $Y_j.P \stackrel{?}{=} (X_j + K_{jp} + H_1(ID_j, K_{jp})s.P).(H_2(ID_i, X_j, t_j))$. Unsuccessful verification leads to session termination, otherwise $\mathcal{U}_j$ determines and accept the shared session key $SKji = H_3(x_i.X_j)$. Hence, successful exchange of shared session helps the registered participants to communicate with each other securely.

4. Formal Security Validation Using ProVerif

This section presents the scrutiny about security of proposed scheme through automated protocol verifier tool ProVerif [30, 31, 32]. It is used to develop prototypes for various cryptographic relations or functions such as encryption/decryption, hash functions and signatures etc. The role of the ProVerif is to demonstrate equivalence-based security characteristics for verifying the security strength of concerned protocol. ProVerif utilizes applied Π calculus to rectify authenticity and secrecy [33]. The prototype of proposed scheme illustrated in Figs. 3(a), 3(b) and 3(c) is developed in ProVerif. The prototype is composed of three segments, namely declaration, process and main segment. Declaration segment delineate variables, names and channels besides cryptographic functions. Definition of processes and sub-processes are elaborated in process segment, whereas blueprint of evaluating scheme is established in main segment. Couple of channels, constants and variables besides cryptographic functions delineated as constructors and equations are presented in declaration segment.

Main segment defines the initiation and termination of participating users. Processes of participating users execution is kept parallel. At the end, three queries are executed in order to rectify the correctness and secrecy of the proposed scheme. The results of the queries are as under:

1. RESULT inj-event(endUserUi(id)) ==> inj-event(beginUserUi(id)) is true.

2. RESULT inj-event(endUserUj(id)) ==> inj-event(beginUserUj(id)) is true.

3. RESULT not attacker(SK[]) is true.

The correctness of the proposed scheme is substantiated as first two queries are executed successfully. Whereas, its secrecy is confirmed due to unsuccessful query attack on session key SK.

5. Security Analysis

This section presents the security analysis of proposed authentication technique under the adversarial model discussed in subsection 2.3. The subsequent subsections substantiate the robustness against familiar attacks.

5.1. Mutual Authentication

As per proposed scheme, $\mathcal{U}_i$ determines $X_i = x_i.P$ and $Y_i = x_i + K_{is}H_2(ID_j, X_i, t_i)$ and sends $\{X_i, Y_i, K_{ip}, ID_i, t_i\}$. The computation of Y_i involves secret key K_{is} of $\mathcal{U}_i$. If public key infrastructure is not insecure then only legitimate user can determine $Y_i.P$. $\mathcal{U}_j$ authenticates $\mathcal{U}_i$ by verifying $Y_i.P \stackrel{?}{=} (X_i + K_{ip} + H_1(ID_i, K_{ip})s.P).(H_2(ID_j, X_i, t_i))$, where $\mathcal{A}$ cannot find $H_1(ID_i, K_{ip})$ without secret key s of $\mathcal{T}$. Morever, the use of public key K_{ip} of $\mathcal{U}_i$ guarantees that request is made by legitimate user. On the other hand $\mathcal{U}_i$ authenticates $\mathcal{U}_j$ by verifying $Y_j.P \stackrel{?}{=} (X_j + K_{jp} + H_1(ID_j, K_{jp})s.P).(H_2(ID_i, X_j, t_j))$. Hence, both $\mathcal{U}_i$ and $\mathcal{U}_j$ mutually authenticate each other.

5.2. Replay Attack

Authentication request contains time stamp t_i, which is not only sent in plaintext, but it is also concealed in $Y_i = x_i + K_{is}H_2(ID_j, X_i, t_i)$. Therefore, if an $\mathcal{A}$ replays a former message from $\mathcal{U}_i$, $\mathcal{U}_j$ can identify it by checking the recentness/freshness of t_i. However, if $\mathcal{A}$ sends a fresh time stamp t_a, even then authentication request fails to verify $Y_i.P \stackrel{?}{=} (X_i + K_{ip} + H_1(ID_i, K_{ip})s.P).(H_2(ID_j, X_i, t_i))$. Replay attack over challenge message is also prevented in the similar fashion due to t_j that is not only sent in the plaintext, but it is also concealed in $Y_j.P \stackrel{?}{=} (X_j + K_{jp} + H_1(ID_j, K_{jp})s.P).(H_2(ID_i, X_j, t_j))$.

```
(******************Channels*****************)
free SCh:channel [private].      (*Secure Channel*)
free PCh:channel.                (*Public Channel*)
(************Constants & Variables***********)
const P:bitstring.
free IDi:bitstring.
free IDj:bitstring.
free PK:bitstring.
free s:bitstring [private].
(*****************Constructor****************)
fun H1(bitstring,bitstring):bitstring.
fun H2(bitstring,bitstring,bitstring):bitstring.
fun H3(bitstring):bitstring.
fun ECPM(bitstring,bitstring):bitstring.
fun MULT(bitstring,bitstring):bitstring.
fun CONCAT(bitstring,bitstring):bitstring.
```

(a) Declarations

```
(*****************processes*****************)
(*******************User Ui******************)
let UserUi=
(****************Registration****************)
out(SCh,IDi);
in(SCh,(xKip:bitstring,xKis:bitstring));
(**********Login and Authentication**********)
event beginUserUi(IDi);
new xi:bitstring;
new ti:bitstring;
let Xi = ECPM(xi,P) in
let Yi = CONCAT(xi,MULT(xKis,H2(IDj,Xi,ti))) in
out(PCh,(Xi,Yi,xKip,IDi,ti));
in(PCh,(xXj:bitstring,xYj:bitstring,xKjp:bitstring,
xIDj:bitstring,xtj:bitstring));
let YjP = ECPM(xYj,P) in
let YjP' = MULT(CONCAT(xXj,(xKjp,MULT(H1(xIDj,xKjp)
    ,
ECPM(s,P)))),H2(IDi,xXj,xtj)) in
if (YjP = YjP') then
let SK = H3(MULT(xi,xXj)) in
event endUserUi(IDi)
else 0.
(*******************User Uj*******************)
let UserUj=
(****************Registration****************)
out(SCh,IDj);
in(SCh,(xKjp:bitstring,xKjs:bitstring));
(**********Login and Authentication**********)
event beginUserUj(IDj);
in(PCh,(xXi:bitstring,xYi:bitstring,xKip:bitstring,
xxIDi:bitstring,xti:bitstring));
let YiP = ECPM(xYi,P) in
let YiP'= MULT(CONCAT(xXi,(xKip,MULT(H1(xxIDi,xKip)
    ,
ECPM(s,P)))),H2(IDj,xXi,xti)) in
if (YiP = YiP') then
new xj:bitstring;
new tj:bitstring;
let Xj = ECPM(xj,P) in
let Yj =  CONCAT(xj,MULT(xKjs,H2(xxIDi,Xj,tj))) in
let SK = H3(MULT(xj,xXi)) in
out(PCh,(Xj,Yj,xKjp,IDj,tj));
event endUserUj(IDj)
else 0.
(********************TTP*********************)
let TTP=
(****************Registration****************)
in(SCh,xIDi:bitstring);
new ai:bitstring;
let Kip  = ECPM(ai,P) in
let Kis  = CONCAT(ai,MULT(s,H1(xIDi,Kip))) in
out(SCh,(Kip,Kis));
in(SCh,xIDj:bitstring);
new aj:bitstring;
let Kjp  = ECPM(aj,P) in
let Kjs  = CONCAT(aj,MULT(s,H1(xIDj,Kjp))) in
out(SCh,(Kjp,Kjs));
0.
process ((!UserUi) | (!TTP) | (!UserUj) )
```

(b) Processes

```
(*******************Events*******************)
event beginUserUi(bitstring).
event endUserUi(bitstring).
event beginUserUj(bitstring).
event endUserUj(bitstring).
(*******************Queries******************)
free SK:bitstring [private].
query attacker(SK).
query id:bitstring; inj event(endUserUi(id)) ==>
      inj event(beginUserUi(id)).
query id:bitstring; inj event(endUserUj(id)) ==>
      inj event(beginUserUj(id)).
```

(c) Main

Figure 3: ProVerif Code

5.3. Impersonation Attack

$\mathcal{A}$ can impersonate himself as $\mathcal{U}_i$ by engendering valid login request $\{X_i, Y_i, K_{ip}, ID_i, t_i\}$. Likewise, $\mathcal{A}$ can impersonate himself as $\mathcal{U}_j$ by engendering valid response message $\{X_j, Y_j, K_{jp}, ID_j, t_j\}$. Valid login solicitation is produced by computing X_i and Y_i, where computation of Y_i involves secret K_{is} of $\mathcal{U}_i$ and $H_2(ID_j, X_i, t_i)$. Valid response is also produced in the similar fashion. Thus proposed scheme withstands impersonation attack.

5.4. Privileged Insider Attack

$\mathcal{T}$ and interacting users do not maintain any verifier repository. Server and interacting users utilize their respective secret keys for authentication process. Hence, proposed scheme withstands stolen verifier and insider attacks.

5.5. Man-in-the-middle Attack

It is difficult for an $\mathcal{A}$ to successfully pass authentication at both ends without secret credentials. Subsection 5.1, proves that only legitimate users can successfully authenticate each. Therefore, the proposed scheme prevents man-in-the-middle Attack.

5.6. Perfect Forward Secrecy

If $\mathcal{A}$ is able to get secret keys of participating users, even then the previous session keys are not compromised. This characteristic of authentication scheme is designated as perfect forward secrecy. The random numbers x_i and x_j are exclusively engendered by the clients $\mathcal{U}_i$ and $\mathcal{U}_j$, respectively. Therefore, it is hard for $\mathcal{A}$ to guess previous session keys without having multiple session parameters. The $\mathcal{A}$ has to resolve Elliptic Curve Discrete Logarithm Problem (ECDLP) in order to extract x_i, x_j from $X_i = x_i.P$ and $X_j = x_j.P$, respectively. It is almost strenuous for $\mathcal{A}$ to get previous session keys based on such current session keys that are somehow compromised. Hence, proposed scheme maintains perfect forward secrecy.

At the end of the security analysis, security characteristics of proposed scheme is compared against security features of analogous schemes. The comparison is depicted in Table 2. It shows that the proposed has more security features as compared to its counterparts.

Table 2: Comparison of Security Characteristics

Scheme:	Proposed	[11]	[12]	[34]
Provides Mutual Authentication and key agreement	Yes	No	Yes	Yes
Withstands Replay attack	Yes	Yes	Yes	Yes
Withstands Impersonation attack	Yes	No	Yes	Yes
Withstands Privileged Insider Attack	Yes	No	No	No
Withstands Man-in-the-middle Attack	Yes	Yes	Yes	Yes
Provides Perfect Forward secrecy	Yes	No	No	No

6. BAN logic based authentication proof

This section elaborates the integrity or completeness of the proposed scheme using BAN logic [26]. BAN logic is a prominent formal method for the assessment of the authentication scheme. The concerned assessment is as follows:

Principals (U and V) indicate general instances participating in a protocol

Keys are meant for symmetric message encryption

Public keys are used in pairs, and used for asymmetric message encryption

Timestamps are time-synchronized and never repeated

Primitive syllabaries for BAN logic analysis are presented in Table 3

$U \mid\equiv M$:	U believes the statement M
$U \triangleleft M$:	U sees M
$U \mid\sim M$:	U once said M, sometime ago
$U \Rightarrow M$:	U has got jurisdiction over M
$\sharp(M)$:	The message M is to be taken as fresh
$\langle M \rangle_N$:	The formulae M is used in combination with formulae N
(M, N) :	M or N being the part of message (M, N)
$\{M, N\}_K$:	M or N is encrypted with symmetric key K
$\langle M, N \rangle_K \mapsto U$:	M or N is encrypted with the public key K of U
$(M, N)_K$:	M or N is hashed using the key K
$U \xleftrightarrow{K} V$	U and V can securely contact using the shared key K

Table 3: Notations

Fundamental rules for BAN logic analysis are delineated as under:

RBL 1: Message meaning rule: $\frac{U|\equiv U \overset{K}{\longleftrightarrow} V, U \triangleleft \langle M \rangle_N}{U|\equiv V|\sim M}$

RBL 2: Nonce verification rule: $\frac{U|\equiv \sharp(M), U|\equiv V|\sim M}{U|\equiv V|\equiv M}$

RBL 3: Jurisdiction rule: $\frac{U|\equiv V \Rightarrow M, U|\equiv V|\equiv M}{U|\equiv M}$

RBL 4: Freshness conjuncatenation rule: $\frac{U|\equiv \sharp(M)}{U|\equiv \sharp(M,N)}$

RBL 5: Belief rule: $\frac{U|\equiv (M), U|\equiv (N)}{U|\equiv (M,N)}$

RBL 6: Session key rule: $\frac{U|\equiv \sharp(M), U|\equiv V|\equiv M}{U|\equiv U \overset{K}{\longleftrightarrow} V}$

RBL 7: Public key encryption rule: $\frac{U|\equiv_K \mapsto V, U \triangleleft \{M\}_{K-1}}{U|\equiv V|\sim M}$

The subsequent goals must be satisfied using above-mentioned rules in order to validate the security of the proposed protocol under BAN logic.

Goal 1: $U_j|\equiv U_j \overset{SK}{\longleftrightarrow} U_i$

Goal 2: $U_j|\equiv U_i|\equiv U_j \overset{SK}{\longleftrightarrow} U_i$

Goal 3: $U_i|\equiv U_j \overset{SK}{\longleftrightarrow} U_i$

Goal 4: $U_i|\equiv U_j|\equiv U_j \overset{SK}{\longleftrightarrow} U_i$

Idealized transformation of proposed protocol is as follows:

IM 1: $U_i \to U_j : X_i, Y_i, K_{ip}, ID_i, t_i : \{x_i.P, \langle ID_j, x_i.P, t_i \rangle_{(a_i + sH_1(ID_i, a_i.P))}, a_i.P, ID_i, t_i\}$

IM 2: $U_j \to U_i : X_j, Y_j, K_{jp}, ID_j, t_j : \{x_j.P, \langle ID_i, x_j.P, t_j \rangle_{(a_j + sH_1(ID_j, a_j.P))}, a_j.P, ID_j, t_j\}$

Assumptions regarding preliminary state of the scheme are presented below, in order to evaluate the proposed protocol:

A 1: $U_i|\equiv \sharp t_i$

A 2: $U_j|\equiv \sharp t_j$

A 3: $U_i|\equiv sP \mapsto T$

A 4: $U_j|\equiv sP \mapsto T$

A 5: $U_i|\equiv U_j \Rightarrow X_j$

A 6: $U_j|\equiv U_i \Rightarrow X_i$

Where $sP \mapsto T$ is designated as the public key of T (trusted third party), which is believed by U_i and U_j. Considering the $IM1$ of the idealized form:

$IM1 : U_i \rightarrow U_j : X_i, Y_i, K_{ip}, ID_i, t_i :$
$\{x_i.P, \langle ID_j, x_i.P, t_i\rangle_{(a_i+sH_1(ID_i,a_i.P))}, a_i.P, ID_i, t_i\}$

By applying seeing rule, we get:

$S1 : U_j \triangleleft X_i, Y_i, K_{ip}, ID_i, t_i :$
$\{x_i.P, \langle ID_j, x_i.P, t_i\rangle_{(a_i+sH_1(ID_i,a_i.P))}, a_i.P, ID_i, t_i\}$

According to $S1$, $A4$ and RBL 7, we have:

$S2 : U_j|\equiv U_i \sim \{x_i.P, \langle a_i.P, ID_i, ID_j, x_i.P, t_i\rangle_{sP\mapsto T}, t_i\}$

Using $S2$, $A1$, RLB 2 and RLB 4, we have:

$S3 : U_j|\equiv U_i|\equiv \{x_i.P, \langle a_i.P, ID_i, ID_j, x_i.P, t_i\rangle_{sP\mapsto T}, t_i\}$

Using $S3$, $A6$ and RLB 3, we have:

$S4 : U_j|\equiv \{x_i.P, \langle a_i.P, ID_i, ID_j, x_i.P, t_i\rangle_{sP\mapsto T}, t_i\}$

Using $SK = x_j.x_i.P$, $S4$, $A1$ and RLB 6, we have:

$S5 : U_j|\equiv U_j \xleftrightarrow{\text{SK}} U_i$ **Goal 1**

According to $S5$, $A6$ we apply RLB 6 as:

$S6 : U_j|\equiv U_i|\equiv U_j \xleftrightarrow{\text{SK}} U_i$ **Goal 2**

Now, we consider the second message $IM2$ in idealized form:

$IM2 : U_j \rightarrow U_i : X_j, Y_j, K_{jp}, ID_j, t_j :$
$\{x_j.P, \langle ID_i, x_j.P, t_j\rangle_{(a_j+sH_1(ID_j,a_j.P))}, a_j.P, ID_j, t_j\}$

By applying seeing rule, we get:

$S7 : U_i \triangleleft X_j, Y_j, K_{jp}, ID_j, t_j :$
$\{x_j.P, \langle ID_i, x_j.P, t_j\rangle_{(a_j+sH_1(ID_j,a_j.P))}, a_j.P, ID_j, t_j\}$

According to $S7$, $A3$ and RLB 7, we have:

$S8 : U_i|\equiv U_j \sim \{x_j.P, \langle a_j.P, ID_j, ID_i, x_j.P, t_j\rangle_{sP\mapsto T}, t_j\}$

Using $S8$, $A2$, RLB 2 and RLB 4, we have:

$S9 : U_i|\equiv U_j|\equiv \{x_j.P, \langle a_j.P, ID_j, ID_i, x_j.P, t_j\rangle_{sP\mapsto T}, t_j\}$

Using $S9$, $A5$ and RLB 3, we have:

$S10 : U_i|\equiv \{x_j.P, \langle a_j.P, ID_j, ID_i, x_j.P, t_j\rangle_{sP\mapsto T}, t_j\}$

Using $SK = x_i.x_j.P$, $S10$, $A2$ and RLB 6, we have:

$S11 : U_i|\equiv U_j \xleftrightarrow{\text{SK}} U_i$ **Goal 3**

According to $S11$, $A5$ we apply RLB 6 as:

$S12 : U_i| \equiv U_j| \equiv U_j \overset{SK}{\longleftrightarrow} U_i$ **Goal 4**

The above BAN logic analysis formally proves that the proposed protocol achieves mutual authentication and the session key SK is mutually established between U_i and U_j.

7. Performance Evaluation

Performance evaluation of proposed scheme is presented here beside analogous schemes [11, 12, 34]. The primitive metrics used for the performance comparison, namely computational complexity, communication and memory overheads. The results are derived at the core $i5$ machine with processing capability of 2.50 GHz and installed internal memory of 4.0 GB. The system has utilized Windows 7 Professional as an operating system. Time of each primitive operation is used as presented in the [35].

7.1. Computation Complexity Comparison

Comparison of computational complexity of the proposed scheme beside analogous schemes is discoursed here. Prior to presenting comparison, important notations are listed as under:

- T_{ME} : appertains to execution time for operation of modular exponentiation
- T_{SM} : appertains to execution time for operation of ECC Scalar multiplication
- T_H : appertains to time incurred during one-way hash function
- T_{PA} : appertains to time incurred during point addition
- T_{SE} : appertains to time incurred during execution of symmetric key encryption
- T_{SD} : appertains to time incurred during execution of symmetric key decryption
- T_{AE} : refers to execution time incurred during execution of asymmetric key encryption
- T_{AD} : refers to execution time incurred during execution of asymmetric key decryption

Table 4: Performance Analysis

Scheme: ↓	Computation Cost	Communication Cost	Memory Overhead
Chim et al. [11]	$2T_{AE} + 2T_{AD} + 2T_{HMAC} = 15.4092\ ms$	4448 *bits*	3232 *bits*
Fouda et al. [12]	$2T_{AE} + 2T_{AD} + 2T_{H} + 4T_{ME} + T_{HMAC} = 30.8092\ ms$	3744 *bits*	320 *bits*
Zhang et al. [34]	$T_{AE} + T_{AD} + 2T_{H} + 2T_{SM} + 2T_{SE} + 2T_{SD} = 19.8658\ ms$	608 *bits*	3200 *bits*
Proposed	$5T_{SM} + 5T_{H} + 1T_{PA} = 11.1703\ ms$	576 *bits*	320 *bits*

- T_{HMAC} : appertains to execution time incurred during execution of Hash-based Message Authentication Code (HMAC) operation

Computation complexity of the proposed scheme and analogous schemes are evaluated by identifying the primitive operations and their frequency in the respective schemes. Time of each primitive operation is used as presented in the [35]. Whereas, communication and storage overhead comparison is performed by selecting 64 bits long ID. Time stamp length is considered as 32 bits, public/private keys and ECC operation size is taken up as 160 bits. Table 4 depicts that proposed scheme outperforms rest of the analogous schemes [11, 12, 34] in terms of computational complexity. The computation cost of the proposed scheme is just 11.1703 ms, which is substantially less than the analogous schemes. It is due to the fact that expansive operations (in terms of computation) are eradicated in the proposed scheme. So, proposed scheme is capable to achieve same level of security against various well-known attacks using lightweight primitive operations.

7.2. Communication and Memory overhead Comparison

Comparison of communication and memory overhead of the proposed scheme beside analogous schemes is presented here. This comparison reveals that the proposed scheme outperforms analogous or relevant schemes in terms of communication overhead. The communication cost of the proposed scheme is 576 *bits*, which is obviously less than the communication cost of the analogous schemes. Similarly, memory overhead is just 320 *bits*, which is less than the rest of the analogous schemes. Although, memory overhead of the proposed scheme is similar to Fouda et al.'s [12] scheme but it is proved that proposed scheme is able to prevent additional security attacks as compared to other relevant schemes including Fouda et al.'s scheme. Hence, Table 4 highlights that the proposed scheme is resource efficient as far as the communication cost and memory overhead is concerned.

8. Conclusion

For enabling smart city environment to entice more visitors towards cultural heritage, secure SG is considered as the vital component. In this paper, we have proposed an ECC based lightweight authentication scheme for SG system. The proposed scheme is best suited for SG system due to its lightweight operations as SG is a complex network with delay sensitive nature. The scheme provides mutual authentication with protection against all known security attacks. Automated protocol verifier tool ProVerif is used to analyze the security of the proposed scheme. Integrity and completeness of the scheme is proved through BAN logic. Furthermore, the proposed technique is informally analyzed under a given adversarial model to confirm its robustness against known security attacks. Performance analysis of the proposed scheme in comparison with contemporary related authentication schemes shows that our scheme requires lowest computational overhead as well as least communication overhead.

[1] A. Chianese, F. Piccialli, A smart system to manage the context evolution in the cultural heritage domain, Computers and Electrical Engineering 55 (2016) 27–38. doi:10.1016/j.compeleceng.2016.02.008.

[2] A. Chianese, F. Marulli, F. Piccialli, P. Benedusi, J. Jung, An associative engines based approach supporting collaborative analytics in the internet of cultural things, Future Generation Computer Systems 66 (2017) 187–198. doi:10.1016/j.future.2016.04.015.

[3] A. Chianese, F. Marulli, F. Piccialli, P. Benedusi, J. E. Jung, An associative engines based approach supporting collaborative analytics in the internet of cultural things, Future generation computer systems 66 (2017) 187–198.

[4] A. Chianese, F. Piccialli, A smart system to manage the context evolution in the cultural heritage domain, Computers & Electrical Engineering 55 (2016) 27–38.

[5] M. Hong, J. J. Jung, F. Piccialli, A. Chianese, Social recommendation service for cultural heritage, Personal and Ubiquitous Computing 1–11.

[6] M. S. Thomas, J. D. McDonald, Power System SCADA and Smart Grids, CRC Press, 2015.

[7] B. Vaidya, D. Makrakis, H. Mouftah, Secure communication mechanism for ubiquitous smart grid infrastructure, The Journal of Supercomputing 64 (2) (2013) 435–455.

[8] C.-I. Fan, S.-Y. Huang, W. Artan, Design and implementation of privacy preserving billing protocol for smart grid, The Journal of Supercomputing 66 (2) (2013) 841–862.

[9] B. Vaidya, D. Makrakis, H. Mouftah, Secure and robust multipath routings for advanced metering infrastructure, The Journal of Supercomputing 66 (2) (2013) 1071–1092.

[10] S. Al-Agtash, Electricity agents in smart grid markets, Computers in Industry 64 (3) (2013) 235–241.

[11] T. W. Chim, S.-M. Yiu, L. C. Hui, V. O. Li, Pass: Privacy-preserving authentication scheme for smart grid network, in: Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, IEEE, 2011, pp. 196–201.

[12] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, X. Shen, A lightweight message authentication scheme for smart grid communications, Smart Grid, IEEE Transactions on 2 (4) (2011) 675–685.

[13] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, H. F. Ahmad, A lightweight message authentication scheme for smart grid communications in power sector, Computers & Electrical Engineering.

[14] Q. Li, G. Cao, Multicast authentication in the smart grid with one-time signature, Smart Grid, IEEE Transactions on 2 (4) (2011) 686–696.

[15] S. Oh, J. Kwak, Mutual authentication and key establishment mechanism using dcu certificate in smart grid, Applied Mathematics & Information Sciences. Mag. S 1 (2012) 257–264.

[16] J. Nam, K.-K. R. Choo, S. Han, M. Kim, J. Paik, D. Won, Efficient and anonymous two-factor user authentication in wireless sensor networks: achieving user anonymity with lightweight sensor computation, PloS one 10 (4) (2015) e0116709.

[17] D. He, N. Kumar, N. Chilamkurti, A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks, Information Sciences 321 (2015) 263–277.

[18] Q. Gao, Biometric authentication in smart grid, in: Energy and Sustainability Conference (IESC), 2012 International, IEEE, 2012, pp. 1–5.

[19] B. Vaidya, D. Makrakis, H. T. Mouftah, Authentication and authorization mechanisms for substation automation in smart grid network, Network, IEEE 27 (1) (2013) 5–11.

[20] D. He, N. Kumar, M. K. Khan, L. Wang, J. Shen, Efficient privacy-aware authentication scheme for mobile cloud computing services, IEEE Systems Journal.

[21] D. He, N. Kumar, H. Shen, J.-H. Lee, One-to-many authentication for access control in mobile pay-tv systems, Science China Information Sciences 59 (5) (2016) 052108.

[22] D. He, S. Zeadally, Authentication protocol for an ambient assisted living system, Communications Magazine, IEEE 53 (1) (2015) 71–77.

[23] H. Nicanfar, V. Leung, Password-authenticated cluster-based group key agreement for smart grid communication, security and communication networks 7 (1) (2014) 221–233.

[24] H. Nicanfar, V. C. Leung, Multilayer consensus ecc-based password authenticated key-exchange (mcepak) protocol for smart grid system, Smart Grid, IEEE Transactions on 4 (1) (2013) 253–264.

[25] D. Li, Z. Aung, J. R. Williams, A. Sanchez, Efficient and fault-diagnosable authentication architecture for ami in smart grid, Security and Communication Networks 8 (4) (2015) 598–616.

[26] M. Burrows, M. Abadi, R. M. Needham, A logic of authentication, in: Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, Vol. 426, The Royal Society, 1989, pp. 233–271.

[27] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, M. Shalmani, On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme, in: D. Wagner (Ed.), Advances

in Cryptology, CRYPTO 2008, Vol. 5157 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2008, pp. 203–220. doi:10.1007/978-3-540-85174-5˙12.
URL http://dx.doi.org/10.1007/978-3-540-85174-5_12

[28] D. Dolev, A. C. Yao, On the security of public key protocols, Information Theory, IEEE Transactions on 29 (2) (1983) 198–208. doi:10.1109/TIT.1983.1056650.

[29] X. Cao, S. Zhong, Breaking a remote user authentication scheme for multi-server architecture, Communications Letters, IEEE 10 (8) (2006) 580–581. doi:10.1109/LCOMM.2006.1665116.

[30] M. Abadi, B. Blanchet, H. Comon-Lundh, Models and proofs of protocol security: A progress report, in: Computer Aided Verification, Springer, 2009, pp. 35–49.

[31] S. A. Chaudhry, M. S. Farash, H. Naqvi, M. Sher, A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography, Electronic Commerce Research (2015) 1–27doi:10.1007/s10660-015-9192-5.
URL http://dx.doi.org/10.1007/s10660-015-9192-5

[32] S. A. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, M. K. Khan, An enhanced privacy preserving remote user authentication scheme with provable security, Security and Communication Networks (2015) 1–13doi:10.1002/sec.1299.

[33] Q. Xie, B. Hu, N. Dong, D. S. Wong, Anonymous three-party password-authenticated key exchange scheme for telecare medical information systems, PloS one 9 (7) (2014) e102747.

[34] L. Zhang, S. Tang, H. Luo, Elliptic curve cryptography-based authentication with identity protection for smart grids, PloS one 11 (3) (2016) e0151253.

[35] H. H. Kilinc, T. Yanik, A survey of sip authentication and key agreement schemes, IEEE Communications Surveys & Tutorials 16 (2) (2014) 1005–1023.

Khalid Mahmood received the B.S. degree in Computer Science from Virtual University, Lahore, Pakistan and the M.S. degree in Computer Science from Riphah International University, Islamabad, Pakistan, respectively in 2007 and 2010. He is pursuing Ph.D. degree in Computer Science from International Islamic University, Islamabad, Pakistan. His research interests are in Smart Grid authentication and information security.

Shehzad Ashraf Chaudhry received distinction in his Masters and PhD from International Islamic University Islamabad, Pakistan in 2009 and 2016 respectively. He was awarded Gold Medal for achieving 4.0/4.0 CGPA in his Masters. Currently, he is working as an Assistant Professor at the Department of Computer Science & Software Engineering, International Islamic University, Islamabad. He authored more than 50 scientific publications appeared in different international journals and proceedings including 35 in SCI/E journals. His research interests include Lightweight Cryptography, Elliptic/Hyper Elliptic Curve Cryptography, Multimedia Security, E- Payment systems, MANETs, SIP authentication, Smart Grid Security, IP Multimedia sub-system and Next Generation Networks.

Husnain Abbas Naqvi received his Ph.D. from The University of Auckland, New Zealand. Currently he is working as Assistant Professor at the Department of Computer Science, International Islamic University, Islamabad. He authored more than 30 scientific publications published in different international journals and proceedings. His broad research interests include Sensor Networks, Collaborative Communications, Lightweight Cryptography, Beamforming and Space Time Block Codes.

Saru Kumari is currently an Assistant Professor with the Department of Mathematics, C.C.S. University, Meerut, U.P, India. She received Ph.D. degree in Mathematics in 2012 from C.C.S. University, Meerut, Uttar Pradesh, India. She has published 68 papers in international journals and conferences including 52 research publications in SCI indexed journals. Her research field is cryptology.

Xiong Li now is an associate professor at School of Computer Science and Engineering of the Hunan University of Science and Technology (HNUST), China. He received his masterâĂŹs degree in mathematics and cryptography from Shaanxi Normal University (SNNU), China in 2009 and Ph.D. degree in computer science and technology from Beijing University of Posts and Telecommunications (BUPT), China in 2012. He has published more than 40 referred journal papers in his research interests, which include cryptography and information security, etc. He has served on TPC member of several international conferences on information security and reviewer for more than 20 ISI indexed journals. He is a winner of the 2015 Journal of Network and Computer Applications Best Research Paper Award.

Arun Kumar Sangaiah has received his Master of Engineering (M.E.) degree in Computer Science and Engineering from the Government College of Engineering, Tirunelveli, Anna University, India. He had received his Doctor of Philosophy (Ph.D.) degree in Computer Science and Engineering from the VIT University, Vellore, India. He is presently working as an associate professor in School of Computer Science and Engineering, VIT University, India. His area of interest includes software engineering, computational intelligence, wireless networks, bio-informatics, and embedded systems. He has authored more than 100 publications in different journals and conference of national and international repute. His current research work includes global software development, wireless adhoc and sensor networks, machine learning, cognitive networks and advances in mobile computing and communications. He is an active member in Compute Society of India. Moreover, he has carried out a number of funded research projects for Indian government agencies. Also, he was registered a one Indian patent in the area of Computational Intelligence.