Secure and Efficient Protocol for Transmission of Multi Digital Documents Using Blind Signcryption

Fazlullah, Noor Ul Amin, Jawaid Iqbal, Arif Iqbal Umar and Muhammad Shahid

Department of Information Technology Hazara University Mansehra,K-P, Pakistan

Abstract

recently, the implementation of blind signcryption has become essential in various application such as (e- voting process, e-payment system, digital content safety policies, credential-based access mechanism and e-bidding). Blind signcryption enables the signer to generate the signcrypted text blindly without revealing the original contents of a message. All the existing blind signcryption schemes are based on bilinear pairing, RSA and elliptic curve cryptography which suffer from high computational power and communication overhead. The implementation of blind signcryption in our scheme using HECC covers the gape of high cost due to shorter key size (public key, private key, certificate and signature) in key processing and exchange. The proposed scheme meets all the security requirement of blind signcryption with additional properties like public verifiability, forward secrecy and provides resistance against replay attack. Similarly, secure communication of multiple digital documents requires multiple signatures, thus signing each digital document is over burdening the system resources. In our scheme signing multiple digital documents simultaneously with single signature decreases the bandwidth and processing cost. Further, we validate our proposed scheme security services through well-known security validation tool AVISPA.

Key words:

Blind Signcryption, Hyper Elliptic Curve Cryptosystem (HECC), Hash function, public verifiability, multi digital documents.

1. Introduction

In Modern communication society, people communicate through the public network, which requires security services such as authentication, privacy/confidentiality integrity and non-repudiation there are primary and significant functions in the security criteria. On the other hand, an application like e-payment [1, 2] and e-voting [3, 4] require sender privacy or anonymity. Because, sender privacy or anonymity in such type of applications is very important, if sender sends some sensitive data over public networks and don’t want to disclose his identity.

Digital signature [26, 27, 28, 29] are one of the most important mathematical scheme of modern cryptography used for authenticity, integrity and non-repudiation. The receiver satisfied by a valid digital signature to be believed that the known sender have sent the message. The property of authentication is the procedure of proving one's identity and assured by digital signature, Integrity is a major property of digital signature, which gives the guarantee of message to the receiver that the data has not be altered or modified during the transmission and non-repudiation technique used to confirm that the sender truly sent the message, or the signer cannot deny from his singed message. Various types of digital signature have been suggested such as blind signature, proxy signature, group signature etc.

Chum [5] suggested the procedure of blind signature which provides the sender anonymity/privacy. Blind signature technique is a type of digital signature scheme, whenever the signer sign the message the contents of documents is blinded from signer. Anonymity of sender refers to the condition where the identity of sender is not known to the enrolled parties or to the participants. Therefore it is an exigency in diverse applications like electronic voting and digital cash systems to protect the privacy/anonymity of sender from unauthorized access, Privacy of sender is extremely assistive when somebody wants to send significant data and expect to save his/her identity.

Signcryption scheme first introduced by Yu Liang Zheng [30] in 1997. Signcryption technique fulfills two fundamental functions public key encryption and digital signature simultaneously in one step. At less computation and communication costs than encrypting and signing individually. Many applications need for hard security therefore both encryption and digital signature executing simultaneously.

Blind signcryption technique is the combination of two function alities, encryption and blind digital signature executed simultaneously in single step. It presents two special properties un-linkability or untraceability which provides sender anonymity. The signer blindly signs the documents and the signer is powerless and cannot access and observe the contents of the message. This can be applied in dispatcher anonymous communication such as electronic voting and payment systems. To achieve and obtain security criteria in public key cryptography, it is needed to use fundamental security mechanisms in public key cryptography, as when the sender sends the message, the sender use his private key and computes the hash or signature of the message then utilize the recipient public key and encrypts the message and digital signature. When the recipient receives the message, first he decrypts the message then verifies the signature of the sender with his public key. The process of these two steps called signature-then-

Manuscript received June 5, 2018
Manuscript revised June 20, 2018

encryption technique. As per the study of the existing literature review, the existing blind signcryption schemes are based on bilinear pairing, RSA and elliptic curve cryptography, which suffer from high computational power and communication overhead. Similarly, secure communication of multiple documents requires multiple signatures, thus signing each document is over burdening the system resources. We present blind signcryption scheme based on hyper elliptic curves for transmission of multi digital documents that improves overall efficiency of the system. In security perspective hyper elliptic curve provides same level of security as compared to elliptic curve and reduces the storage cost, transmission cost and computational power. Our scheme meets all the basic security features like data confidentiality, data Integrity, unforgeability, blindness, non-repudiation, public-verifiability, and anonymity. In our proposed scheme we will treat the high computing power and bandwidth consumption problems by the application of hyper elliptic curve lower parameters size and by signing multi digital documents with single signature simultaneously. Finally, we will validate our proposed scheme security services through well-known security validation tool AVISPA.

2. Related Work

In the proposed carmenisch et al [6] blind signature scheme the security of this scheme is based on discrete logarithm problem DLP. Pointcheval and Stern [7] designed another blind signature scheme based on the factorization problem. Due to large module, the suggested scheme was not suitable for smart devices. So Harn [8] analyzed the scheme and claimed that this scheme [6] doesn’t provide the property of Un-traceability. Actually the hoster [9] wasn’t, agree with scheme [8] cryptanalysis. Therefore he claimed that the signer cannot trace the blind signature. Later lee et al [10] claims that the cryptanalysis of hoster [9] was not correct. They clarified that, during the request of requester for blind digital signature a signer stores the related parameter and trace the requester and finally they proposed a new scheme for the fulfillments of security requirements. Ting and Wang [11] demonstrate to the lee et al scheme [10] and claim that it doesn’t provide reasonable proof for the correctness of Un-traceability. The cost of this scheme was also high than the scheme [6]. S.A. Brands [12] proposed a restrictive blind signature scheme to blind the message with some limitation on the requester and some rules also described for selection and restriction of message. In blind signature the identity of user place and protected as well as the scheme is well-organized for offline electronic cash systems. To provide un-traceability property Nikooghadam and Zakerolhosseini [13] Contrivance a blind signature scheme based on elliptic curves. Both of communication and computation costs of suggested scheme are significantly decreased with comparison of existing schemes which is based on DLP. As well to improve the security Chakraborty and Mehta [14] also suggested another blind digital signature scheme they used hash function and elliptic curves, first the message is blinded from the selected singer, every user place two locks with each and every message, the first lock will be released by the selected singer and the second lock will be released by the requester, this process will be done to blind the content of message. Dhanashree and agrawal [15] projected well-organized scheme based on elliptic curve for electronic voting systems and used hash function as a blinding factor to blind the vote from the signer. Jena et al [16] contrivanced another blind signature scheme by using elliptic curve. The proposed scheme has love computation and communication over head as compare to RSA. Yu and He [17] recommend another effective DLP based blind signcryption convention to improve security objectives, for example, obscurity, untraceability, and unlinkability. Ullah et al. [18] additionally exhibit an ECC-based blind signcryption conspire that is fits for providing the properties of classification, trustworthiness, unforgeability, and non-repudiation for low-power or asset compelled gadgets. Over that, rather than utilizing elliptic curve cryptography, Ch et al. [19, 20] and Nizamuddin et al. [21] present an option paradigm for signcryption estimations that depend on the thought of hyper elliptic curve cryptography, and their papers propose a more lightweight signcryption display having open unquestionable status and forward mystery to lessen the quantity of bits and get preferable execution over the current ECC-based plans. In any case, every one of the three of the strategies don't utilize a security and blinding system, however a non-blind cryptographic crude to offer the help of open unquestionable status, and hyper elliptic curve cryptography in class that requires numerous more field activities in each gathering task can possibly be aggressive with its elliptic curve cryptography partner [22,23].Its merits calling attention to that a recently divulged blind signcryption idea (by consolidating blind mark and signcryption algorithm) is acquired from Shamsher-ullah et al. [24] and Sadat et al. [25]; their exploration is centered around redone outlines on electronic payment frameworks and an intermediary approach, individually, offering solid security prerequisites to encourage the advance of conveying and getting to data in complex systems. Chien-Hua Tsai and Pin-Chang Su [26] have exhibited another intermediary blind signcryption conspire by thinking of the countermeasure for numerous computerized messages preparing in view of the ECDLP trouble. To improve the security of messages marked in the interest of the first underwriter as the intermediary is printed, having the signcryption-stage strategy alongside the cryptographic natives is completely consolidated into the intermediary blind signature work. They depicted how the joined ideas of encryption and visually impaired signcryption can help build up an intermediary blind signcryption convention, demonstrating that the proposed conspire is equipped for having the advantages of handling numerous intermediary blind signcrypted data in both security and productivity contrasted with the other existing arrangements. They guarantee that the present plan gives huge improvements high security settings and low correspondence overheads for intermediary blind marks and their applications, for example, e-voting, e-money and web based business frameworks, and this model is extremely advantageous especially in versatile processing situations when these gadgets may have constrained correspondence capacities and influence supplies. However, their plan can be additionally altered to all the more less computational cost and correspondence overhead. In proposed scheme [27] blind signcryption based on ECC is used for the secure communication of multiple digital documents. This scheme still suffers from huge computation and communication resources and does not provide resistance against replay attack. Overall literature review reveals that the existing blind signcryption schemes are based on bilinear pairing, RSA and elliptic curve cryptography, which suffer from high computational power and communication overhead. Similarly, secure communication of multiple documents requires multiple signatures, thus signing each document is over burdening the system resources. Thus a blind signcryption scheme is required to improve overall efficiency of the system in terms of cost and security.

3. Proposed Scheme

The main objective of our proposed scheme is to design a secure and efficient protocol for transmission of multi digital documents using blind signcryption with HECC that consume less resources of the system and provide higher degree of security. The proposed scheme has three different participants Singer, Bob and Alice. This plays three different rules of signer, sender and receiver in three different phases.

Our scheme comprises in the following three phases:

i. Keys Generation Phase
ii. Blind Signcryption Phase
iii. Un-signcryption Phase

Now the following algorithms explain every phase in detail.

Algorithm (1): Keys Generation

In this first phase of keys generation Alice, Signer and Bob Initially select private keys and then compute their public keys using below steps.

```
Signer
{
    Step1. Select an integer $\mathcal{P}_s \in \{0,1,2,\dots\dots.n-1\}$ as for his private key
    Step2. Signer computes his public key $\mathcal{B}_s$ as:
                $\mathcal{B}_s = \mathcal{P}_s.\mathcal{D}$
}
Alice
{
    Step3. Alice choose an integer $\mathcal{P}_r \in \{0,1,2,\dots\dots.n-1\}$as for his private key
    Step4. Alice computes his public key $\mathcal{B}_r$ as:
                $\mathcal{B}_r = \mathcal{P}_r.\mathcal{D}$
}
Bob
{
Step5. Bob chooses an integer $\mathcal{P}_v \in \{0,1,2\,,\dots\dots.n-1\}$ for his private key
Step6. Bob computes his public key $\mathcal{B}_v$ as:
            $\mathcal{B}_v = \mathcal{P}_v.\mathcal{D}$
}

{

Step7.To obtain public key certificate every user will request to the certificate authority (CA)
}
```

Algorithm (2): Multi-Document Blind Signcryption

Suppose Alice assumes that he wants to send a vector of message$m_j \mathcal{E}\mathcal{M}$, blindly over public network to maintain their privacy to Bob. For generating a blind Signcrypted text $(\mathcal{C}_j, r,\ \mathcal{S},\ \mathcal{Z})$, the following steps will be executed.

```
Singer
{
        Step1. Signer first Pick a Random number $\mathcal{V}\ \boldsymbol{\mathcal{E}}\{0,1,2,\dots\dots.n-1\}$
        Step2. Then Computes $\mathcal{T} = \mathcal{V}.\mathcal{D}\ modn$
        Step3. Then Send $\mathcal{T}$ to the Alice
}
Alice (Where, $\mathcal{B}_v$ is the public key of a Bob, $m_j$ is the vector of multi messages and $\mathcal{D}$ is the divisor) {
        Step4. After receiving $\mathcal{T}$ Alice randomly pick a three blinding factors $\mathfrak{f}, \mathfrak{g}$ and $\mathfrak{h} \in \{0,1,2,\dots\dots.n-1\}$
        Step5. Computes $\mathcal{K} = h\ (\mathfrak{h}.\mathcal{B}_v \text{mod n})$
        Step6. Split $\mathcal{K}$ in two pats $(\mathcal{K}_1 \parallel \mathcal{K}_2)$
        Step7. Computes $r = \mathcal{K}\hbar_{\mathcal{K}_2}(m_j \parallel \mathcal{K}_1)$
        Step8. Computes $\mathcal{C}_j = \mathcal{E}_{\mathcal{K}_1}(m_j\,.\text{NS})$
        Step9. Computes $\boldsymbol{\mathcal{Z}}$
                    $= ((\boldsymbol{\mathfrak{h}} + \boldsymbol{\mathfrak{g}}).\boldsymbol{\mathcal{T}} + \boldsymbol{\mathfrak{f}}.\boldsymbol{\mathcal{D}})\textbf{mod n}$
        Step10. Computes $\bar{r} = (r + \mathfrak{g})\textbf{mod n}$
        Step11. Then Send $\bar{r}$ to the signer
}
Singer (Where, $\mathcal{P}_s$ is the private key of signer)
{
        Step12. When signer receiving $\bar{r}$ then
        **Step13**. Anonymous signer generate
                $\overline{\mathcal{S}} = (\mathcal{P}_s + \bar{\mathscr{r}}.\mathcal{V}) \bmod n$
        **Step14**.Send $\bar{\mathcal{S}}$ to the Alice
}
**Alice**
{
        **Step15**. Alice receive $\bar{\mathcal{S}}$ then
        **Step16**.Compute $\mathcal{S} = \frac{\mathfrak{h}}{\mathscr{r} + \bar{\mathcal{S}} + \mathfrak{f}} \bmod n$
        **Step17**. Send ( $\mathcal{C}_j, \mathscr{r}, \mathcal{S}, \mathcal{Z}$) to the Bob
}
```

Algorithm (3): Multi-Document Un-signcryption

Bob verifies all the signcrypted multi documents text, once he received the $(\mathcal{C}_j, \mathscr{r}, \mathcal{S}, \mathcal{Z})$ and accepts if valid or else reject.

Bob (where $\mathcal{P}_v$ is the private key of a Bob and $\mathcal{B}_s$ is the public key of a signer)

```
{
        **Step1**. Bob computes $\mathscr{w} = \mathcal{P}_v.\mathcal{S}$
        **Step2**. Compute s $\mathcal{K} = \left(\mathscr{w}.(\mathcal{B}_s + \mathcal{Z} + \mathscr{r}.\mathcal{D})\right)$
        **Step2**. Computes $\mathcal{K} = (\mathcal{K}_1 \parallel \mathcal{K}_2)$
        **Step3**. Computes $\mathscr{m}_j = D_{\mathcal{K}_1}(\mathcal{C}_j)$
**Step3**. Computes $\mathscr{r}' = \mathcal{K}\mathscr{h}_{\mathcal{K}2}(\mathscr{m}_j \parallel \mathcal{K}_1)$
**Step4**. Accept $\mathscr{m}_j$ as a valid and original message if $\mathscr{r}' = \mathscr{r}$ otherwise reject
}
```

A. Proposed Model

The proposed scheme model is shown in below figurer.1.

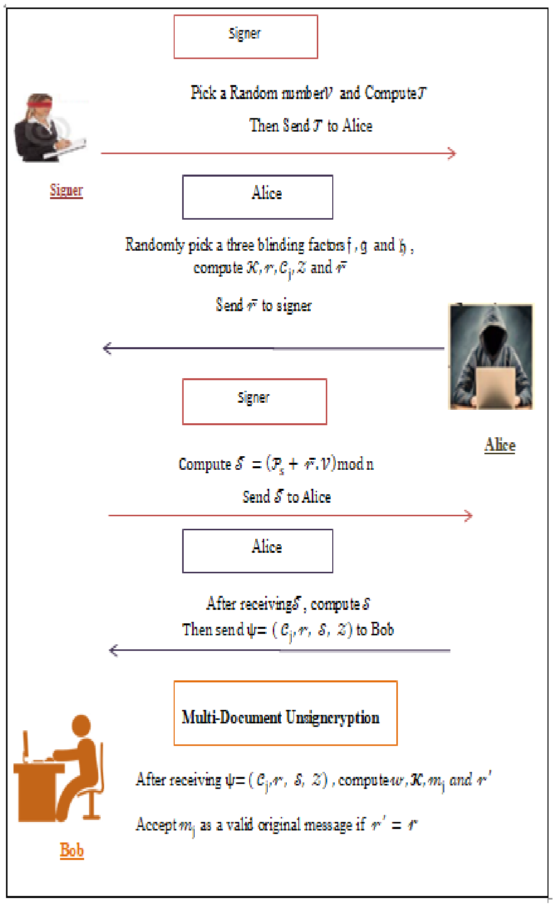

Signer
Pick a Random number$\mathcal{V}$ and Compute$\mathcal{T}$
Then Send $\mathcal{T}$ to Alice
Signer
Alice
Randomly pick a three blinding factors $\mathfrak{f}$, $\mathfrak{g}$ and $\mathfrak{h}$,
compute $\mathcal{K}, \mathscr{r}, \mathcal{C}_j, \mathcal{Z}$ and $\bar{\mathscr{r}}$
Send $\bar{\mathscr{r}}$ to signer
Signer
Alice
Compute $\bar{\mathcal{S}} = (\mathcal{P}_s + \bar{\mathscr{r}}.\mathcal{V}) \bmod n$
Send $\bar{\mathcal{S}}$ to Alice
Alice
After receiving$\bar{\mathcal{S}}$, compute $\mathcal{S}$
Then send ψ= ($\mathcal{C}_j, \mathscr{r}, \mathcal{S}, \mathcal{Z}$) to Bob
Multi-Document Unsigncryption
After receiving ψ= ($\mathcal{C}_j, \mathscr{r}, \mathcal{S}, \mathcal{Z}$) , compute$\mathscr{w}, \mathcal{K}, \mathscr{m}_j$ and $\mathscr{r}'$
Accept $\mathscr{m}_j$ as a valid original message if $\mathscr{r}' = \mathscr{r}$
Bob

Fig. 1 Structure of Proposed Model

4. Security Analysis

This phase include the detail discussion about security services of our designed scheme. Our designed scheme provides the security services such as Integrity, unforgeability, confidentiality, message integrity, message unforgeability, message integrity. SPAN aids our scheme to prove the secrecy and authentication. SPAN is a security protocol animator for AVISPA [27].The AVISPA tool is based on push-down automata techniques that can perform automated validations over internet security protocols and applications [28]. HLPSL is basically a language that is used to specify cryptographic protocols for the AVISPA tool [29]. The language can be explained in terms of: Modular, Role-base, Expressive and Formal language [30]. Where it is used for the specification of control flow patterns, cryptographic operators, alternative adversary models as well as complex security properties.

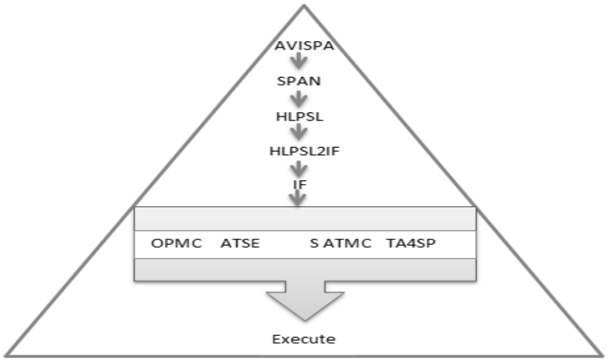


Fig. 2 Structure of AVISPA tool

A. Confidentiality

The propose multi document blind signcryption scheme ensures a requirement of confidentiality. It is a significant goal of communication when if two or more user want to communicate securely means data will be kept secret from unauthorized access. In our proposed scheme when the attacker/adversary wants to access the contents of a message then he/she needs to get the secret key. Thus, to get the secret key he/she can pass through the following cases:

1. Case (A): adversary/ attacker can obtain the secret key $\mathcal{K}$ if he/she solves the equation (1). Hence to calculate the adversary must need the random private number $\mathfrak{h}$. Thus solving the equation (1) gets $\mathcal{K}$ is infeasible and equals to computing hyper elliptic curve discrete logarithm problem.

$$\mathcal{K}=\text{h}\ (\mathfrak{h}.\mathcal{B}_{\text{v}})\text{mod n} \qquad (1)$$

2. Case (B): adversary/ attacker also can get the secret key $\mathcal{K}$ if he computes $\mathfrak{h}$ from equation (2). For this purpose he/she must need the two private random number $\mathfrak{g}$ and $\mathfrak{f}$ which are infeasible to get. Hence, it is hard for adversary to compute the equation with three unknown number.

$$\mathcal{Z} = \ ((\mathfrak{h} + \mathfrak{g}).\mathcal{T} + \mathfrak{f}.\mathcal{D}) \qquad (2)$$

B. Integrity

Our proposed multi-document blind signcryption scheme provides the property of integrity of multi-massages. The proposed multi document scheme enables the multi document signcrypter to make the hash of messages and after this it will be transmitted. In our designed multi document scheme, if the attacker wants to change $\boldsymbol{\mathcal{C}}$ into $\acute{\mathcal{C}}$ then the message will be changed from m_{j} to m_{j}', thus according to the collision residence service of one way hash if the attacker changed $\boldsymbol{\mathcal{C}}$ then it will be automatically detected.

C. Unforgeability

Unforgeability describes an important term to protect the associated message only the signer is able to offer a valid signature on the message. Our proposed scheme resists against the forgeability of signature because the signcrypter generate the signature by using his private key. Though, if the attacker exercised to generate a forge signature like eq (3) then it further requires $\mathcal{V}$ from eq (4), hence it is not possible for forger and equivalents to solve a hyper elliptic curve discrete logarithm problem. Furthermore, for solving eq (3) the forger needs $\bar{\mathcal{S}}$ from eq (5), for this forger requires the private key of signer from eq (6) and $\mathcal{V}$ from eq (4). Thus, solving the equation with two unknown variables is infeasible for forger.

$$\mathcal{S} = \ \frac{\mathcal{V}}{r + \ \bar{\mathcal{S}} + \mathfrak{f}} \qquad (3)$$

$$\mathcal{T} = \ \mathcal{V}.\mathcal{D} \qquad (4)$$

$$\bar{\mathcal{S}} \ = (\mathcal{P}_{\text{s}} + \ \bar{r}.\mathcal{V}) \qquad (5)$$

$$\mathcal{B}_{\text{s}} = \mathcal{P}_{\text{s}}.\mathcal{D} \qquad (6)$$

D. Blindness

Our proposed multi-document scheme ensures the security property of blindness against signer. In our scheme, Alice picks three random blind factors $\mathfrak{f}$, $\mathfrak{g}$ and $\mathfrak{h}$ for to blind the message. Therefore, without these blind factors the signer cannot see the message contents. Moreover, if the signer wants to see the contents of a message, then it requires three blind factors like $\mathfrak{f}$, $\mathfrak{g}$ and $\mathfrak{h}$ which is private to Alice.

E. Non-repudiation

The proposed multi document blind signcryption assures the security property of non-repudiation. Though, before sending the messages to un-signcrypter the signcrypter generate the digital signature by using the private key of it's on a message. Hence, in this way, if the signcrypter wants to repudiate from there sends messages the trusted third party can easily identify the source by using the public key of signcrypter.

F. Forward secrecy

Our designed multi document blind signcryption meets the service of security forward secrecy. In our scheme, even if the private key of a signcrypter is compromised the attacker cannot decrypt the messages because we used the secret key. Therefore, to generate the secret key $\mathcal{K}_1$ like eq (7), the attacker needs the random number $\mathfrak{h}$ which is private to the Alice. Thus, to generate $\mathcal{K}_1$ by using eq (7) is infeasible and equivalent for attacker to solve hyper elliptic curve discrete logarithm problem. Further, we refresh the secret key at each and every session. In this way, our scheme strongly satisfies the forward secrecy property.

$$\mathcal{K}=\text{h}\ (\mathfrak{h}.\mathcal{B}_{\text{v}}) = (\mathcal{K}_1 \parallel \mathcal{K}_2) \qquad (7)$$

G. Anonymity

The aim of anonymity when a user wants to send data to each other no one know their actual identity. For example a person can't tell from a group signature who signed a message, Even if anyone knows about the clandestine data of the user and can request group manager to disclose the identity for further more signatures.
It can also be possible that an adversary can interrupt or snoop (eavesdrop) the blinded message α but it's impossible to gain a valid pair (α,(R,S)) to carry out the process of signature generation exclusive of designated signer B, holding private key nB. Likewise if the signer B endeavour to intentionally produce two more legal signature after to interact by the requester A once, it's virtually difficult for B for to guess a random signature (R, S) besides, the verifier.

H. Computational Cost

The elementary thought of computational cost includes calculating the computation cost occur between sender and receiver. Computational cost is measured in terms of major operations like Elliptic Curve Point Multiplication ($\mathcal{EPM}$) and Hyper Elliptic Curve Divisors Scalar Multiplication ($\mathcal{HEDM}$). Table 1 dipicts the comparison of existing schemes with projected scheme in standings of $\mathcal{HEDM}$ (most expensive operation)

Table 1: Computational cost in term of major operations

Schemes	Blind Signcryption	Blind Un-Signcryption	Total Cost
Riaz et al[18]	$8\mathcal{EPM}$	$2\ \mathcal{EPM}$	$10\ \mathcal{EPM}$
Chien and pin [26]	$3\ \mathcal{EPM}$	$3\ \mathcal{EPM}$	$6\ \mathcal{EPM}$
Proposed	$3\ \mathcal{HEDM}$	$2\ \mathcal{HEDM}$	$5\ \mathcal{HEDM}$

Elliptic curve point multiplication (ECPM) takes 4.24 ms and hyper elliptic curve divisors scalar multiplication (HECDM) consumes 2.2 ms.

Table 2: Computational cost in term of milliseconds

Schemes	Blind Signcryption	Blind Un-Signcryption	Total Cost	Total Cost reduction from Riaz et al	Total Cost reduction from Chien and pin
Riaz et al[18]	33.92	8.48	42.4	$\frac{42.4-11}{42.4}*$ 100=74 %	$\frac{25.44-11}{25.44}*$ 100=56 %
Chien& pin [26]	12.72	12.72	25.44		
Proposed	6.6	4.4	11		

I. Communication Cost

The most important factor in wireless communication media to be considered is communication overhead whereas to design cryptographic techniques, the feature of low communication overhead is needed for constrained of bandwidth in wireless media. Minimum communication overhead is the most important issue of a cryptographic technique for wireless networks. The alternative of parameters will have an effect on the communication cost for the proposed system and the quantity of information to be transmitted. For example we suppose that $\boldsymbol{\mathscr{p}}$ is a large prime number $\geq 2^{160}$ for elliptic curve $|\boldsymbol{\mathcal{F}}|\triangleq=|\boldsymbol{\mathscr{p}}|$ and $\boldsymbol{\mathscr{g}}$ is a large prime number $\geq 2^{80}$ for hyper elliptic curve $|\boldsymbol{\mathcal{F}}| \triangleq |\boldsymbol{\mathscr{g}}|$. Table 3 elaborate the comparisons of in term of cipher text size and additional parameters. The [Riaz et al, Chien & Pin [18, 26] schemes communication cost is $\boldsymbol{\mathcal{C}}+|\boldsymbol{\mathcal{F}}|+2|\boldsymbol{\mathscr{p}}|$ which is similar between them. As well the [Elkamchouchi] scheme communication cost is $\boldsymbol{\mathcal{C}}+|\boldsymbol{\mathcal{F}}\ |+3|\boldsymbol{\mathscr{p}}|$ and proposed scheme is $\boldsymbol{\mathcal{C}}+|\boldsymbol{\mathcal{F}}\ |+2|\boldsymbol{\mathscr{g}}\ |$.

Cipher text size	Riaz et al[18]	Chien& pin [26]	Proposed	Total overhead reduction from Riaz et al[18]	Total overhead reduction from Chien& pin [26]
1KB	$\|1024\| + \|160\| + \|160\| + \|160\| = 1504$	$\|1024\| + \|160\| + \|160\| + \|160\| + \|160\| = 1664$	$\|1024\| + \|160\| + \|80\| + \|80\| = 1344$	$\frac{1504-1344}{1504}*$ 100=10.6 %	$\frac{1644-1344}{1644}*$ 100=18.24 %
5KB	$5 * \|1024\| + \|160\| + \|160\| + \|160\| = 5600$	$5 * \|1024\| + \|160\| + \|160\| + \|160\| = 5760$	$5 * \|1024\| + \|160\| + \|80\| + \|80\| = 5440$	$\frac{5600-5440}{5600}*$ 100=2.85 %	$\frac{5760-5440}{5760}*$ 100=5.55 %
10KB	$10 * \|1024\| + \|160\| + \|160\| + \|160\|=10720$	$10 * \|1024\| + \|160\| + \|160\| + \|160\| = 10880$	$10 * \|1024\| + \|160\| + \|80\| + \|80\| = 10560$	$\frac{10720-10560}{10720}*$ 100=1.49%	$\frac{10880-10560}{10880}*$ 100=2.94 %

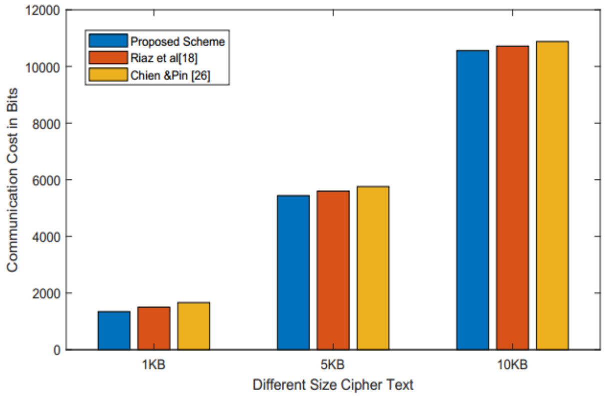


Fig. 3 Communication Cost

J. Generalized formulas for the Reduction of Communication Cost

The formula of lessening correspondence cost for the proposed scheme when contrasted with [18] is trailed by equation (2).

$$\frac{\mathcal{C}+|\mathcal{F}|+2|\wp|-\mathcal{C}+|\mathcal{F}|+|\mathcal{g}|}{\mathcal{C}+|\mathcal{F}|+2|\wp|} \qquad (2)$$

Also the formula of lessening correspondence cost for the proposed scheme when contrasted with [26] is trailed by equation (3).

$$\frac{\mathcal{C}+|\mathcal{F}|+|\wp|-\mathcal{C}+|\mathcal{F}|+|\mathcal{g}|}{\mathcal{C}+|\mathcal{F}|+|\wp|} \qquad (3)$$

In correspondence cost diminishment rely on the selection of parameters and the measure of information. Table clarify the correlations of correspondence cost of a different kind figure content and determination of curve of hyper elliptic curve scheme and existing schemes [18,26]. We select differing sizes of figure content like 128 bits, 256 bits and 1024 bits. In this way our proposed scheme claims in correspondence cost from [26] plots around 2.94 % to 18.24 %to 52.63% and from [18] is around 1.49 % to 10.6 %.

5. Conclusion

The use of blind signcryption for ensuring the users anonymity in various applications (e-voting process, e-payment system, digital content safety policies, credential-based access mechanism) is essential. We have addressed the shortcoming arose in the implementation of blind signcryption using RSA and ECC for best utilization of network resources. In our designed protocol we implemented blind signcryption using HECC. As a result cost is significantly decreased due to shorter key size. The result shows 14.42 % average reduction in communication cost in comparison to existing schemes in case of 1KB cipher text size, while for 5KB average reduction cost is 4.2 %. In our proposed scheme simultaneously signing multiple digital documents with single signature decreases the bandwidth and processing cost. Apart from others essential security services, our scheme provides additional security services by adding public verifiability, forward secrecy and protect the system from replay attack. Moreover, our scheme validate the security properties using well known security tool AVISPA along with SPAN.

6. Appendix

Renowned security simulation tool AVISPA [31, 32] is use for the validation of our protocol. HLPSL is basically a language that is used to specify cryptographic protocols for the AVISPA tool.

Notations

No	Symbols	Description
1	$\mathcal{h} \rightarrow$ HH	Hash functions
2	$m_j \rightarrow$ C	Is plain text or message
3	$\mathcal{C}_j \rightarrow$ C’	Is the cipher text
4	D	Is hyper elliptic curve point divisor
5	$\mathcal{B}_v \rightarrow$ Bv	public key of Un-Signcrypter
6	$\mathcal{P}_r \rightarrow$ inv (Br)	private key of Signcrypter
7	$\mathcal{P}_v \rightarrow$ inv (Bv)	private key of Un-Signcrypter
8	$\mathcal{B}_r \rightarrow$ Br	public key of Signcrypter
9	$\mathcal{P}_s \rightarrow$ inv (Bs)	Private key of signer.
10	$m_j \mathcal{EM}$	Vector of message blindly.

11	$\mathfrak{f}$, $\mathfrak{g}$ and $\mathfrak{h}$ → F, H, G	Three blinding factors.
12	$\bar{r}$→ (Signer. {HH(C).Bv.Ns.Ss''.H.G}_inv (Bs))	signed encrypted message with blind factor from signer to sender
13	$\mathcal{S}$→ ({HH(C).Bv.Ns.Ss'.H.Alice} _inv (Br)):	Signed encrypted message with added blind factors.
14	$\mathcal{T}$→T	Signing request of signer.
15	$\mathcal{Z}$→ Ss'	Signatures with blind factors.
16	$\mathcal{C}_j$→SND (Alice. {HH(C').Bv.Ns'.T'.F'.G'.H'}_inv (Br))	Encryption
17	m_j→RCV ({HH(C').Bv.Ns'.Ss'.H'.Alice}_inv(Br))	Decryption.
18	$\bar{\mathcal{S}}$→ Ss	Signature
19	$\mathcal{B}_s$→ Bs	Public key signer.

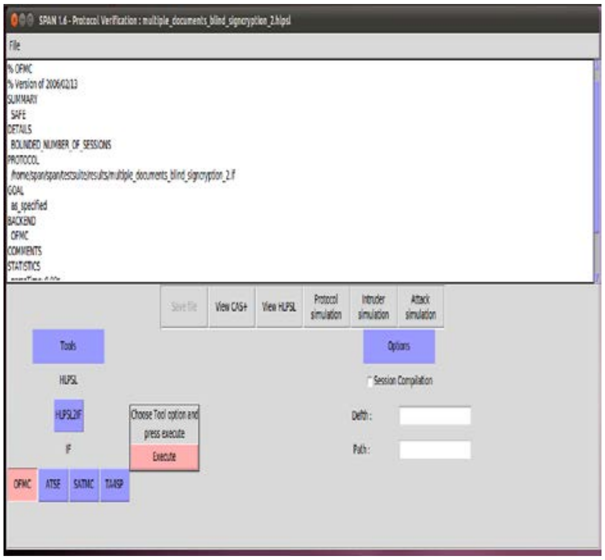
Scheme code

```
Role
%%start of the protocol knows Alice ,public keys and his own private
key
role_Signer(Signer:agent,Alice:agent,Bob:agent,Bs:public_key,Br:public
_key,Bv:public_key,SND,RCV:channel(dy))
played_by Signer
def=
local
State:nat,T:text,F:text,H:text,Ns:text,C:text,HH:hash_func,Ss:text,G:t
ext
init
State := 0
Transition
%% signer sends challenge to Alice his public key
           1. State=0 /\ RCV(Alice.Bob) =|> State':=1 /\ Ns':=new() /\
              T':=new() /\ SND(Signer.{T'.Ns'}_Bs)
%% signer receive message from Alice for signature and send back to
alice %%with his signatures
3. State=1 /\ RCV(Alice.{HH(C').Bv.Ns.T.F'.G'.H'}_inv(Br)) =|>
State':=2 /\ secret(C',sec_2,{Alice}) /\ Ss':=new() /\
SND(Signer.{HH(C').Bv.Ns.Ss'.H'.G'}_inv(Bs))
end role
role
%%defining the role played by Alice using his keys…
role_Alice(Signer:agent,Alice:agent,Bob:agent,Bs:public_key,Br:public_
key,Bv:public_key,SND,RCV:channel(dy))
played_by Alice
def=
local
State:nat,T:text,F:text,G:text,H:text,Ns:text,C:text,HH:hash_func,Ss:t
ext
init
State := 0
```

```
Transition
%%Alice sends challenge to signer and then send encrypted message
1. State=0 /\ RCV(start) =|> State':=1 /\ SND(Alice.Bob)
2. State=1 /\ RCV(Signer.{T'.Ns'}_Bs) =|> State':=2 /\ H':=new() /\
G':=new() /\ F':=new() /\ C':=new() /\ secret(C',sec_2,{Alice}) /\
witness(Alice,Bob,auth_1,C') /\
SND(Alice.{HH(C').Bv.Ns'.T'.F'.G'.H'}_inv(Br))
%%Alice receive signed encrypted message from signer
4. State=2 /\ RCV(Signer.{HH(C).Bv.Ns.Ss'.H.G}_inv(Bs)) =|> State':=3
/\ C':=new()/\ secret(C',sec_2,{Alice}) /\
SND({HH(C).Bv.Ns.Ss'.H.Alice}_inv(Br))
end role
role
%%defining the role played by Bob using his keys…
role_Bob(Signer:agent,Alice:agent,Bob:agent,Bs:public_key,Br:public_ke
y,Bv:public_key,SND,RCV:channel(dy))
played_by Bob
def=
local
State:nat,H:text,Ns:text,C:text,HH:hash_func,Ss:text
init
State := 0
Transition
%% Bob receive signed encrypted message from Alice which he have to
%%decrypt
5. State=0 /\ RCV({HH(C').Bv.Ns'.Ss'.H'.Alice}_inv(Br)) =|> State':=1
/\ request(Bob,Alice,auth_1,C') /\ secret(C',sec_2,{Alice})
end role
role
%%represents the commence of session1 between agents
session1(Signer:agent,Alice:agent,Bob:agent,Bs:public_key,Br:public_ke
y,Bv:public_key)
def=
local
```

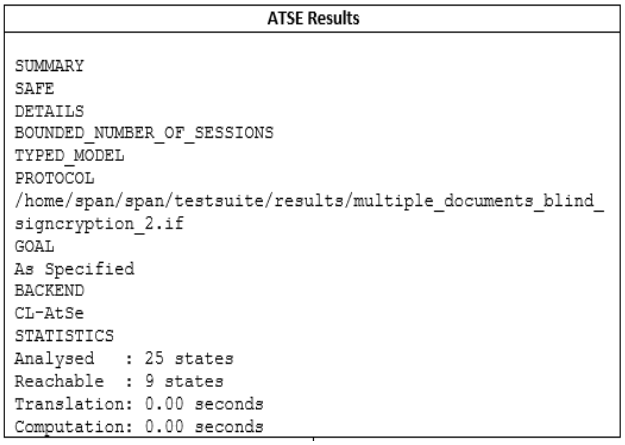
OFMC Results

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/multiple_documents_blind_
signcryption_2.if
GOAL
as specified
BACKEND
OFMC
COMMENTS
STATISTICS
Parse Time: 0.00s
search Time: 0.01s
visited Nodes: 8 nodes
depth: 6 plies
```



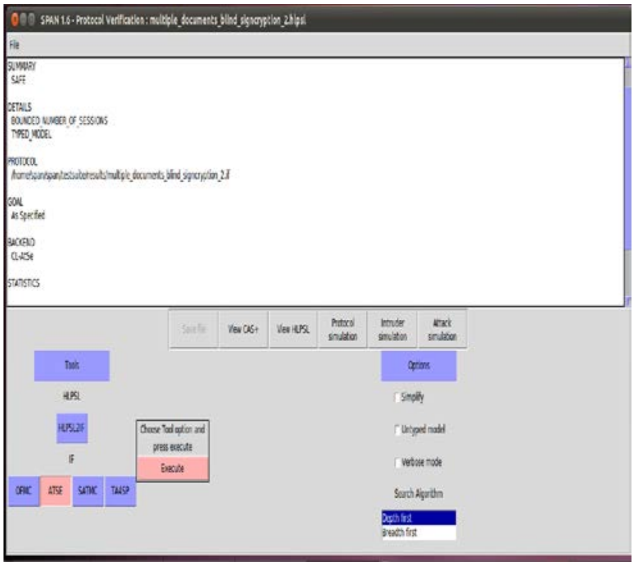
```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/multiple_documents_blind_signcryption_2.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
```

Fig. 4 OFMC summary for HLPSL code 1



ATSE Results

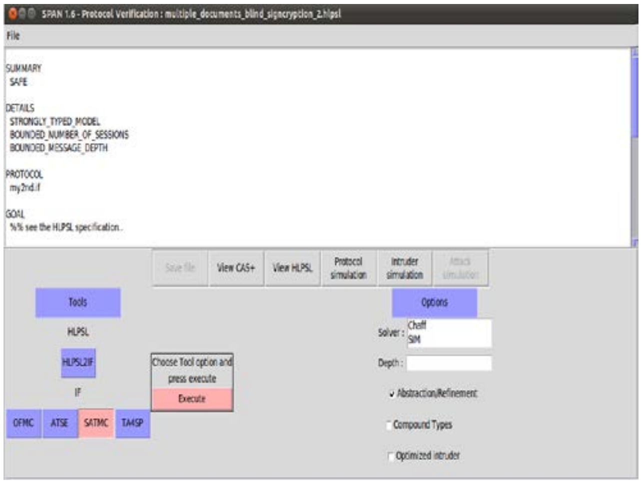
```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/multiple_documents_blind_
signcryption_2.if
GOAL
As Specified
BACKEND
CL-AtSe
STATISTICS
Analysed   : 25 states
Reachable  : 9 states
Translation: 0.00 seconds
Computation: 0.00 seconds
```



SPAN 1.6 - Protocol Verification : multiple_documents_blind_signcryption_2.hlpsl

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/multiple_documents_blind_signcryption_2.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS
```

Fig. 5 CL-ATSe summary for HLPSLC

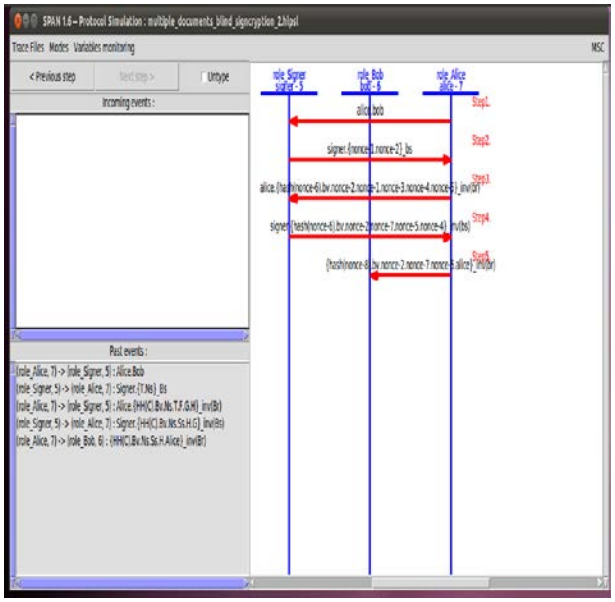


SPAN 1.6 - Protocol Verification : multiple_documents_blind_signcryption_2.hlpsl

```
SUMMARY
 SAFE

DETAILS
 STRONGLY_TYPED_MODEL
 BOUNDED_NUMBER_OF_SESSIONS
 BOUNDED_MESSAGE_DEPTH

PROTOCOL
 my2nd.if

GOAL
 %% see the HLPSL specification..
```

Fig. 6 SATMC summary for HLPSLC

Results of Protocol



SPAN 1.6 – Protocol Simulation : multiple_documents_blind_signcryption_2.hlpsl

```
(role_Alice, 7) -> (role_Signer, 5) : Alice.Bob
(role_Signer, 5) -> (role_Alice, 7) : Signer.{T.Ns}_Bs
(role_Alice, 7) -> (role_Signer, 5) : Alice.{HH(C).Bv.Ns.T.F.G.H}_inv(Br)
(role_Signer, 5) -> (role_Alice, 7) : Signer.{HH(C).Bv.Ns.Ss.H.G}_inv(Bs)
(role_Alice, 7) -> (role_Bob, 6) : {HH(C).Bv.Ns.Ss.H.Alice}_inv(Br)
```

Trace Files
Modes
Variables monitoring
MSC
< Previous step
Next step >
Untype
Incoming events :
Past events :
role_Signer signer - 5
role_Bob bob - 6
role_Alice alice - 7
Step1.
alice.bob
Step2.
signer.{nonce-1.nonce-2}_bs
Step3.
alice.{hash(nonce-6).bv.nonce-2.nonce-1.nonce-3.nonce-4.nonce-5}_inv(br)
Step4.
signer.{hash(nonce-6).bv.nonce-2.nonce-7.nonce-5.nonce-4}_inv(bs)
Step5.
{hash(nonce-8).bv.nonce-2.nonce-7.nonce-5.alice}_inv(br)

Fig. 7 Simulation of Scheme

References

[1] H. F. Huang and C. C. Chang, "An untraceable electronic cash system using fair blind signatures," In e-Business Engineering, IEEE International Conference, pp. 39–46, 2006.

[2] W. Qiu, K .Chen, and D. Gu, "A new offline privacy protecting e-cash system with revocable anonymity," In Proceedings of the 5th International Conference on Information Security, pp. 177–190, Springer-Verlag, 2008.

[3] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," Journal of cryptology, 13(3), pp.361-396, 2001.

[4] G. Qadah and R. Taha, "Electronic voting systems: Requirements, design, and implementation," Computer Standards Interfaces, 29(3), pp. 376–386, 2009.

[5] D. Chaum, "Blind signatures for untraceable payments," In Advances in cryptology Springer, Boston, pp. 199-203, 1983.

[6] D. Chaum, "Blind signatures for untraceable payments," In advances in Cryptology, Springer Verlag, vol -10, pp. 199-203, 1983.

[7] JL. Camenisch, JM. Piveteau, and MA. Stadler, "Blind signatures based on the discrete logarithm problem," In Advances in Cryptology - EUROCRYPT '94, pp. 428–432, 1994.

[8] D. Pointcheval, and J. Stern, "New blind signatures equivalent to factorization," In Proc. 4th ACM Conf. on Computer and Communication Security, pp. 92-99, 1997.

[9] L. Harn, "Cryptanalysis of blind signatures based on discrete logarithm problem," Electronic Letters, 31(14), pp. 1136–1137, 1995.

[10] M. Michels, P. Hoster and H. Petersen. "Comment: cryptanalysis of blind signatures based on discrete logarithm problem." Electronic Letters, 31(21):1827,1995.

[11] N. Sharma, and B. K. Sharma, “New Provably Secure Blind Signature Scheme with Weil Pairing,” International Journal of Advancements in Research & Technology, 3(5), May-2014.

[12] P. Yang, “A new blind signature based on the discrete logarithm problem for untraceability,” Applied Mathematics and Computation, 164(3), pp. 837–841, 2008.

[13] T. Wu and J.R Wang, “Comment: A new blind signature based on the discrete logarithm problem for untraceability,” Applied Mathematics and Computation,170(1) pp.999–1005, 2009.

[14] S.A. Brands, “Untraceable Off-line Cash in Wallets with Observer,” In Crypto 93, LNCS 773, pp: 302-318. Springer-Veral, 1994.

[15] Morteza Nikooghadam, Ali Zakerolhosseini, “An efficient Blind Signature Scheme Based on the Elliptic Curve Discrete Logarithm Problem,” The ISC International Journal of Information Security 1(2), pp. 125-131, 2009.

[16] Chakraborty and J. Mehta, “A stamped blind signature scheme based on elliptic curve discrete logarithm problem," International Journal of Network Security, 14(6), pp. 316-319, 2012.

[17] M. Dhanashree and M.P.J. Agrawal, “Implementation of blind digital signature using ECC,”. International Journal of Computer Science and Network (IJCSN), 1(5), October 2012 www.ijcsn.org ISSN 2277-5420.

[18] R. Ullah, N. Uddin, A. I. Umar, and N. Amin, “Blind signcryption scheme based on elliptic curves,” In Proceedings of the Conference on Information Assurance and Cyber Security (CIACS ’14), pp. 51–54, IEEE Xplore Digital Library, Rawalpindi, Pakistan, June 2014.

[19] J. Debasish, S. Kumar Jena and B. Majhi, “A Novel Untraceable Blind Signature Based on Elliptic Curve Discrete Logarithm Problem,” IJCSNS International Journal of Computer Science and Network Security, 7(6), June 2007.

[20] X. Yu and D. He, “A new efficient blind signcryption,” Wuhan University, Journal of Natural Sciences, 13(6) , pp. 662–664, 2008.

[21] S. A. Ch, Nizamuddin, and M. Sher, “Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem,” Communications in Computer and Information Science, vol. 285, pp. 135–142, 2012.

[22] S. A. Ch, Nizamuddin, M. Sher, A. Ghani, H. Naqvi, and A. Irshad, “An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography,” Multimedia Tools and Applications, 74 (5), pp. 1711–1723, 2015.

[23] Nizamuddin, S. A. Ch, W. Nasar, and Q. Javaid, “Efficient signcryption schemes based on hyperelliptic curve ryptosystem,” In Proceedings of the 7th International Conference on Emerging Technologies (ICET ’11), September 2011.

[24] D. J. Bernstein and T. Lange, “Hyper-and-elliptic-curve cryptography,” LMS Journal of Computation and Mathematics, vol. 17, pp. 181–202, 2014.

[25] J. W. Bos, C. Costello, H. Hisil, and K. Lauter, “Fast cryptography in genus 2,” in Advances in Cryptology—EUROCRYPT 2013, vol. 7881 of LectureNotes in Computer Science, pp. 194–210, Springer, 2013.

[26] CH. Tsai, and PC. Su, “An ECC-based blind signcryption scheme for multiple digital documents,” Security and Communication Networks, 2017.

[27] Shamsherullah, Nizamudin, A. I. Umar, Noor-ul-Amin, R. Ullah, and I. Ullah, “Blind signcryption scheme based on hyper elliptic curve for untraceable payment system,” in Proceedings of the 13th International Conference on Statistical Sciences, vol. 28, pp. 337–344, Peshawar, Pakistan, 2015.

[28] A. Sadat, I. Ullah, H. Khattak, S. Ullah, and Amjad ur rehman, “Proxy blind signcrypion based on elliptic curve,” International Journal of Computer Science and Information Security, 14(3), pp. 257–262, 2016.

[29] http://www.avispaproject.org/participants.html.

[30] L .Vigano, "Automated security protocol analysis with the AVISPA tool," Electronic Notes in Theoretical Computer Science 155, pp. 61-86 2006.

[31] AVISPA. Deliverable 2.1: the High-Level Protocol Specification Language. Available at http://www.avispa-project.org, 2003.

[32] Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, J. Mantovani, S. M¨odersheim, and L. Vigneron, “A high level protocol specification language for industrial security-sensitive protocols,” In Proceedings of Workshop on Specification and Automated Processing of Security Requirements (SAPS), Linz, Austria, 2004.

Fazlullah was born on January 01, 1990 in Mansehra, KPK, Pakistan. He received the BS (Hons) degree from Hazara University Mansehra, Pakistan in 2015. He is currently enrolled in MS (Computer Science) at Hazara University Mansehra, Pakistan. He is the team member of smart Cryptography and networks research group in the department of Information technology, Hazara University Mansehra Pakistan from 2016 up to till date. His research interest includes Cryptography and Network Security. (E-mail: fazlullahumar@gmail.com)

Noor Ul Amin is Head Department of Telecommunication at Hazara University Mansehra. He completed his MSc in Computer Science at University of Peshawar in 1996 and his MS and PhD in Computer Sciences at International Islamic University Islamabad, Hazara University Mansehra subsequently. He has recently completed R & D project sponsored by Ministry of Science and Technology, Pakistan. He has been the session chair in the IEEE and Springer conferences. His research interests include Information Security, Wireless Sensor Networks, Steganography and Information-Centric Networking. He has authored more than 80 peer-reviewed journals articles and conference proceedings. (E-mail: namin@hu.edu.pk)

Jawaid Iqbal received the BS (Computer Science) degree from Institute of Business and Management Sciences (*IBMS*), Agriculture University Peshawar in 2010. He obtained the MS (Computer Science) degree with grade very good with honor from Department of Information Technology, Hazara University. Mansehra, K-P, Pakistan. He is currently PhD Scholar (Computer Science) at Department of Information Technology, Hazara University Mansehra, Pakistan. He is currently Lecturer in Department of information technology, Hazara University Mansehra Pakistan. He is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2012 up to till date. He believe in quality research in the area of Cryptography, Information and Network Security. He is currently active in Elliptic/Hyper Elliptic Curve Cryptography, Signcryption, Sensor Networks, Smart Grid and VANT Security. PhD thesis focused on secure communication of sensitive information in Wireless Body Area Networks (WBANs). (E-mail: jawaid5825@gmail.com)

Arif Iqbal Umar was born at district Haripur Pakistan. He obtained his MSc (Computer Science) degree from University of Peshawar Pakistan and PhD (Computer Science) degree from BeiHang University (BUAA) Beijing P.R. China. His research interests include Data Mining, Machine Learning, Information Retrieval, Digital Image Processing, Computer Networks Security and Sensor Networks. He has supervised 05 PhD candidates and 24 MS candidates. He has published more than 70 research publications in the leading research journals. He has at his credit 26 years' experience of teaching, research, planning and academic management. Currently he is working as Assistant Professor (Computer Science) Information Technology Department Hazara University Mansehra Pakistan.

He is Head Department of Information Technology at Hazara University Mansehra. (E-mail: arifiqbalumar@Yahoo.com & drarif@hu.edu.pk)

Muhammad Shahid received the BCS degree form Peshawar University Pakistan in 2014. He obtained the MCS degree from Hazara University Mansehra, Pakistan in 2017. He is currently enrolled in MS (Computer Science) at Hazara University Mansehra, Pakistan. He is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2017 up to till date. His research interest includes Information Security and Cryptography.

(E-mail: mshahidkhan32@gmail.com)