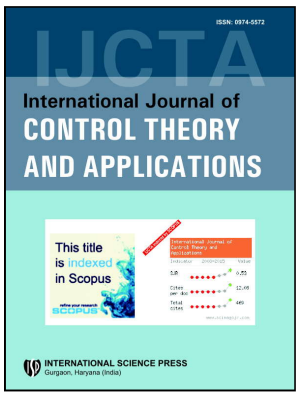

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 15 • 2017

A New Blind Signature Scheme Using Identity-Based Technique

Mahender Kumar[1], C.P. Katti[1] and P. C. Saxena[1]

[1] *School of Computer & Systems Sciences Jawaharlal Nehru University Delhi, India, Emails: mahendjnu1989@gmail.com, cpkatti@mail.jnu.ac.in, Premchand_saxena@yahoo.com*

Abstract: Blind Signature is a type of digital signature that allows a requester to request the signer such that signer only signs the message but could not able to see to message's content. At present, many blind signature based on the traditional PKC has been presented. Solving the problem of key management with traditional PKC, ID-based technique using pairing have been proposed. With the advantage of ECC that its operation on elliptic curve takes less time than operations of bilinear pairing, we proposed a new Blind Signature scheme using ID-based cryptosystem based on the difficulty to solve the GDH and ECDL problem and meets the security requirements of blind signature such as untraceability, Non-Forgeability, completeness, and non- deniability. Also, we present comparative results showing that proposed scheme is considerably more efficient, in terms of computational cost and bandwidth cost, than other schemes which are based on bilinear pairing. Assuming the ID and message attacks, proposed system is secure against one-more forgery and achieves blindness property.

Keywords: Blind Signature; Identity-Based Cryptosystem; Elliptic Curve Cryptosystem; Bilinear Pairing

1. INTRODUCTION

Blind signature, introduced by Chaum in [1],[2], is a cryptographic primitive that allows a requester to get a signature on message without leaking any information about message to signer. With sufficient security against blindness and Untraceability, blind signature have enough capability to implementing in e-commerce applications where user's anonymity is the main concern such as e-payment system, e-wallet [3],[4]. Several papers on blind signature based on the traditional public key cryptosystem has been presented in [2],[5],[6]. Unfortunately, public key infrastructure have disadvantage that it requires certificate which binds the user's public key with his Identity and overhead of managing those certificates. In order to solve the this issues, Shamir [7] introduce a concept of identity based cryptosystem (IBC) but did not implement it. Identity-based cryptosystem maps the user's pubic key directly from his unique identity. Boneh [8] practically implement the encryption using based on user's identity using bilinear pairing.

Using the technology of IBC, blind signature scheme based on user's identity is first presented by Zhang et al [9]. This scheme achieves the blindness property and the security is based on ROS problem. Their scheme is inefficient and impractical because security can be broken in sub-exponential time. Zhang et. al.

[10] presented a new IBBS scheme free from ROS problem and gives no proof against one-more signature forgery. Huang et. al. in [11] gives the new scheme that is secure under the ROS model. This scheme have been proven unforgeablity attack. Gao et. al. in [12] proposed the optimal rounds IBBS scheme. Assuming the parallel chosen message and given ID attack, this scheme is secure against one-more forgery attack and achieves blindness property. Kalkan et. al. in [13] extended the ElGamal signature to blind signature which has property of blindness and cannot have proof of one-more signature forgery. Rao et. al. [14] proposed scheme using Hess's ID-based signature scheme. This scheme acheives blindness property and secure against unforgeability. All schemes [9],[10],[11],[12],[13],[14] uses the pairing based cryptography. It is claimed in [15] that point multiplication on Elliptic Curve is much times faster than a pairing on two group points on elliptic curve. ECC takes less power consumption and less storage space than other cryptographic techniques, for example, bilinear pairing, RSA etc. Additionally, ECDLP is considered a harder problem as compared to the integer factorization and DLP. Vanstone [15] claimed that system using 128-bit ECC key achieved the same security as using the 1024-bit RSA key. In short, ECC takes less power consumption and less storage space which provides strong processing time.

In this paper, we are presenting a new ID-based Blind signature scheme based on the hardness of computing ECDLP problem and GDH problem that satisfy all security properties of generic blind signature and secure against one-more forgery attack under the adaptive chosen message and ID attacks. Proposed scheme found less numbers of pairing operations as compared to others scheme.

The arrangement of paper is as follows: preliminaries about the elliptic curve, bilinear pairing, mathematical problem and required security constraints are given in section II. Section III states the new ID-based blind signature system and security definition. The security, in terms of efficiency and computational cost are analyzed in section IV, finally conclusion is shown in section V.

2. PRELIMINARIES

2.1. Elliptic curve cryptosystem

Suppose the elliptic curve equation $y^2 = (x^2 + mx + n) mod p$, where $x, y \in F_p$ and $4m^2 + 27n^2 mod p \neq 0$. Formally, points group (x, y) is said to be elliptic curve, if these points satisfies the above equation and forming additive abelian group having point 0 is identity element. The condition $4m^2 + 27n^2 mod p \neq 0$ tells that $y^2 = (x^2 + mx = n) mod p$ has a finite abelian group that can be defined based on the set of points $E_p(m, n)$ on elliptic curve. Consider points $A = (x_A, y_A)$ and $B = (x_B, y_B)$ over $E_p(m, n)$, the addition operation of elliptic curve is represented as $A + B = C = (x_C, y_C)$, defined as following:

$$x_C = (u^2 - x_A - x_B) mod p$$

$$y_C = (u(x_A - x_C) - y_A) mod p$$

where

$$\mu = \begin{cases} \left(\frac{y_B - y_A}{x_B - x_A}\right) \bmod p, & if\ A \neq B \\ \left(\frac{3x_A^2 + m}{2y_a}\right) \bmod p, & if\ A = B \end{cases}$$

Based on the elliptic curve, Neal Koblitz [16] and Victor Miller [17] proposed a new kind of Public Key Cryptosystem called the elliptic curve cryptosystem(ECC). In order to have an ability to improve the traditional cryptosystem concerning the parameters (such as having smaller key size, smaller system parameter, lower

bandwidth and power requirements, and smaller hardware requirements), ECC is recommendable for the sake of high security and efficient computation. Those readers who are more familiar with traditional public key cryptosystem, it is noted that addition operation and multiplication operation in ECC are equivalent to modular multiplication and modular exponentiations in RSA respectively.

2.2. Bilinear Pairing

Suppose two cyclic groups having same order q are G_1 (additive) and G_2 (multiplicative) with and generator of G_1 be P. A map, e: G_1 X $G_1 \rightarrow G_2$ is a bilinear map if satisfies the following three properties:

1. Bilinearity: For every X, Y $\in G_1$, and x, y $\in$ Zq

   $e(xX, yY) = e(X, Y)^{xy} = e(x.y.X, Y)$

2. Non-Degeneracy: If X is a generator of G_1 then e(X, X) is generator of G_2 that means if there exist X $\in G_1$ such that $e(X, X) \neq 1$, where 1 is the identity element of G_2.

3. Computability: There must exist an algorithm that can efficiently compute e(X, Y) for every X, Y $\in G_1$.

2.3. Mathematical Problem

Elliptic Curve Discrete logarithm problem (ECDLP). Consider $Y = x.X$ where X, $Y \in E_p(a, b)$, and x $\in Z_q$, it is computationally easy to compute Y from X and x. But it is very difficult to compute x from Y and X.

Computational Diffie-Hellman Problem (CDH). Given $x, y \in Z_q$, $X \in G_1$ and $<X, x.X, y.X>$, compute xyX.

Decision Diffie-Hellman problem (DDH). Given $x, y, z \in Z_q$, $X \in G_1$ and $< X, x.X, y.X, z.X >$ check whether $z = x.y \bmod q$.

Gap Diffie-Hellman problem (GDH). Group of problem where *DDHP* is easy while CDHP is hard.

2.4. Security property

ID-based blind signature achieves the property of blindness and under parallel chosen message and ID attacks proposal is secure against non-forgeability of additional signature. Reader may refers [18] for more details. An ID-based blind signature scheme is considered as secure if it fulfils the following two conditions:

Blindness: Blindness property is defined in terms of following game playing between the challenger C and PPT adversary A.

- *Setup*: The challenger C chooses a security parameter k and executes the *Setup* algorithm to compute the published parameter *PARAM* and master key s. Challenger C sends *PARAM* to A.
- *Phase1*: A selects two distinct message M_0 and M_1 and an ID_i, and sends them to C.
- *Challenge*: C uniformly chooses a random bit $b \in \{0, 1\}$ and ask A for signature on M_b and M_{1-b}. Finally, C strips both the Signatures and gives the original signatures (σ_b, σ_{1-b}) to A.
- *Response*: A guesses bit b' $\in \{0, 1\}$ on tuple (M_0, M_1, σ_b, σ_{1-b}). A wins the game if $b = b'$ holds with probability $Pr[b = b'] > 1/2 + k^n$.

To define the Non-forgeability, let us introduce the following game playing between the Adversary A, who act as Requester and the Challenger C, who act as honest SA.

- *Setup*: On random Security parameter k, the challenger C execute the *Setup* algorithm and computes the parameter *PARAM* and master key s. Challenger C sends *PARAM* to A.

- *Queries*: Adversary *A* can performs numbers of queries as follows:
  - *Hash function queries*: For requested input, challenger *C* computes the hash function values and sends it to the attacker *A*.
  - *Extract queries*: *A* selects an Identity *ID* and ask for S_{ID} to *A*.
  - *BlindSig queries*: *A* selects an *ID* and Message *M*, blindly requested the Signature from *C*. *C* compute signature on Message *M* with respect to *ID*.
- *Forgery*: Game is in favor of A, if against on identity ID*, A response with n valid Message-Signature $(M_1, \sigma_1 = (S'_1, M'_1, y_1))$,. $(M_2, \sigma_2 = (S'_2, M'_2, y_2))$….. $(M_n, \sigma_n = (S'_n, M'_n, y_n))$ such that
  - Each message M_i is distinct from other Message M_j in given Message-Signature $(M_1, \sigma_1 = (S'_1, M'_1, y_1))$,. $(M_2, \sigma_2 = (S'_2, M'_2, y_2))$….. $(M_n, \sigma_n = (S'_n, M'_n, y_n))$ set.
  - *Adversary A* is restricted to ask an extract query on Identity *ID**.
  - Execution of BlindSig algorithm is bounded by n.

Non-forgeability: An ID-based blind signature scheme is break by an Adversary A (t, q_E, q_B, k^n), if *A* runs no more than *t*, *A* make Extract queries no more than q_E and runs *BlindSig* phase no more than q_B, with an advantage more than equal to k^n. Under the adaptive chosen message and ID attacks, our ID-based blind signature scheme is said to secure against one-more forgery, if no adversary *A* (t, q_E, q_B, k^n)-breaks the scheme.

Other important security constraints of blind signature scheme include: *Integrity* (Unauthorized Requester cannot alter the Message M),*Authenticity* (only an authentic signer can sign on Blinded Message),*Non-repudiation* (signer cannot deny having signed on a Blinded Message) and *Non-re-usability* (Signature generated for one Blinded Message cannot be applied to another Blinded Message).

3. PROPOSED ID- BASED BLIND SIGNATURE SCHEME

In this section, we present ID-based blind signature scheme as given in Fig. 1. Suppose *P* be the generator of group G_1 of prime order *q*. Bilinear map $e: G_1 \times G_1 \rightarrow G_2$. Let the Four cryptographic hash function $H_1: \{0,1\}^* \rightarrow G_1$, $H_2: \{0,1\}^* \rightarrow Z_q$, $H_3: \{0,1\}^* \times G_1 \rightarrow Z_q$ and $H_4: G_2 \rightarrow \{0,1\}^*$. Let the private key of signer and requester is denoted as S_{IDS} and S_{IDR} respectively, where $Q_{IDR} = H_1(ID_R)$, $S_{IDR} = s.Q_{IDR} \in G_1$, $Q_{IDS} = H_1(ID_S)$ *and* $S_{IDS} = s.Q_{IDS} \in G_1$. Let T_S denotes the timestamp.

In order to request one blind signature on message, proposed scheme requires four phases (Setup, Extract, BlindSig and Verify) and four entities (PKG, Signer, Requester and Verifier). The algorithm is given as follows:

Setup: PKG select a random integer $s \in Z_q$ and computes public key $P_{Pub} = s.P$. Publishes $PARAMS = \{G_1, q, e, P, P_{Pub}, H_1, H_2, H_3, H_4\}$, and s should be kept secretly.

Extract: Using signer's ID_S, requester's identity ID_R and his master key *s*, PKG computes $S_{IDS} = s.Q_{IDS}$, where $Q_{IDS} = H_1(ID_S)$ and $S_{IDR} = s.Q_{IDR}$, where $Q_{IDR} = H_1(ID_R)$ and sends S_{IDS} and S_{IDR} to the signer and requester respectively.

BlindSig: This phase consists of four sub-phases that runs between signer and requester as follows:

Commitment: Signer chooses a secret random integer $r \in Z_q$. Compute pair (k, R) where, $k = H_4(e(S_{IDS}, rH_2(T_S)Q_{IDR}))$ *and* $R = rH_2(T_S)Q_{IDS}$ and delivers R to requester.

Authenticating & Blinding: On given input R and his private key S_{IDR}, requester compute $K = H_4(e(S_{IDR}, R))$. If any forger wants to compute k with his private key S_{IDf}, he couldn't compute next step correctly because $k \neq K$. Only an authenticate requester can proceed to next. Now, requester chooses two random number $a, b \in Z_q$

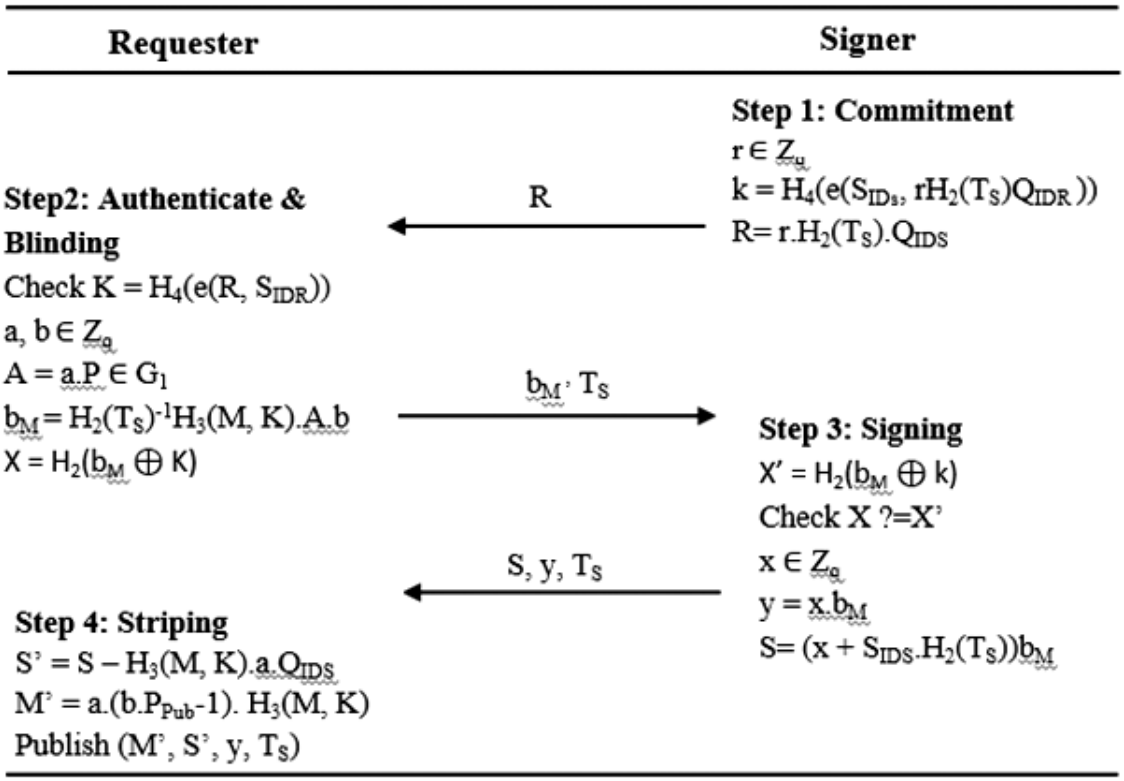

Figure 1: Proposed ID-based blind signature scheme

as blinding factor and timestamp T_S. Compute $A = a.P$, blinded message $b_M = H_2(T_S)^{-1}H_3(M, K).A.b$ and $X = H_4(b_M \oplus K)$, then the requester sends b_M, T_S and X to signer.

S*igning*: On given blinded message (b_M, X, T_S), the signer computes $X' = H_4(b_M \oplus k)$. If $X' = X$ holds, signer selects $x \in Z_q$ and computes signature $y = x.b_M$ *and* $S = (x + S_{IDS}.H_2(T_S))b_M$ and sends S, y and T_S to the requester.

Stripping: On receiving the blinded signature (S, y, T_S), requester strips it and computes the originial signature (S', M'), where

$$S' = S - H_3(M, K).a.Q_{IDS}$$

$$M' = a.(b.P_{Pub}-1).H_3(M, K)$$

Finally, requester publishes (M', S', y, T_S) for verification

Verify: On given (M', S', y, c), verifier with signer ID_S and accept the signature is valid if and only if

$$y = S' - M'.Q_{IDS}$$

4. ANALYSIS OF OUR SCHEME

This section gives the analysis of our proposed scheme in terms of security and computational efficiency.

4.1. Security Analysis

Correctness. The correctness of proposed scheme is verifies from this following equations:

$$
\begin{aligned}
y &= S' - M'.Q_{IDS} \\
&= S - H_3(M, K).a.Q_{IDS} - M'.Q_{IDS} \\
&= S - H_3(M, K).a.Q_{IDS} - a.(b.P_{Pub}\text{-}1).H_3(M, K).Q_{IDS} \\
&= S - H_3(M, K).a.Q_{IDS} - a.b.P_{Pub}.H_3(M, K).Q_{IDS} + a.H_3(M, K).Q_{IDS} \\
&= S - a.b.P_{Pub}.H_3(M, K).Q_{IDS} \\
&= (x + S_{IDS})b_M - a.b.P_{Pub}.H_3(M, K).Q_{IDS} \\
&= x.b_M + S_{IDS}.H_2(T_s)b_M - a.b.P_{Pub}.H_3(M, K).Q_{IDS} \\
&= x.b_M + S_{IDS}.H_2(T_s).H_2^{-1}(T_s)H_3(M, K).A.b - a.b.P_{Pub}.H_3(M, K).Q_{IDS} \\
&= x.b_M + s.Q_{IDS}.H_3(M, K).a.P.b - a.b.P_{Pub}.H_3(M, K).Q_{IDS} \\
&= x.b_M + Q_{IDS}.H_3(M, K).a.P_{Pub}.b - a.b.P_{Pub}.H_3(M, K).Q_{IDS} \\
&= x.b_M = y
\end{aligned}
$$

Non-forgeability. Consider an Adversary A supposed to forge the signature, he should compute the correct value of $k = H_4(e(S_{IDS}, rH_2(T_s)Q_{IDR}))$. But private key is known only to the signer so he must choose random S_{IDA} as the private key or k_A as the share information to compute $k_A = H_4(e(S_{IDA}, r_A.H_2(T_s)Q_{IDR}))$ and subsequently compute $y_A = x_A.b_M$ and $S_A = (x_A + S_{IDA}.H_2(T_s))b_M$ with random choose r_A and x_A. finally, $S_A' = S_A - H_3(M, K).a.Q_{IDS}$ and $M' = a.(b.P_{Pub}\text{-}1).H_3(M, K)$ are computed on requester side. The recipient can check the verification of signature through following equation:

$$
\begin{aligned}
S_A' - M_A'.Q_{IDA} &= S_A - H_3(M, K).a.Q_{IDA} - M_A'.Q_{IDA} \\
&= S_A - H_3(M, K).a.Q_{IDA} - a.(b.P_{Pub}\text{-}1).H_3(M, K).Q_{IDA} \\
&= S_A - H_3(M, K).a.Q_{IDA} - a.b.P_{Pub}.H_3(M, K).Q_{IDA} + a.H_3(M, K).Q_{IDA} \\
&= S_A - a.b.P_{Pub}.H_3(M, K).Q_{IDA} \\
&= (x_A + S_{IDA})b_M - a.b.P_{Pub}.H_3(M, K).Q_{IDA} \\
&= x_A.b_M + S_{IDA}.H_2(T_s)b_M - a.b.P_{Pub}.H_3(M, K).Q_{IDA} \\
&= x.b_M + S_{IDA}.H_2(T_s).H_2^{-1}(T_s)H_3(M, K).A.b - a.b.P_{Pub}.H_3(M, K).Q_{IDA} \\
&= x_A.b_M + S_{IDA}.H_3(M, K).a.P.b - S_{IDA}.H_3(M, K).a.P.b \\
&= x_A.b_M = y_A \neq y
\end{aligned}
$$

To forge the signature, adversary must know S_{IDS}, r_A and x_A. Otherwise, the adversary could not forge the blinded signature on M.

Suppose adversary wants to replace the original message M with forged message M', he should forge the value of k, which is equivalent to solve the GDP problem and computes $A_A = a_A.P$ and $b_{MA} = H_2(T_s)^{-1}H_3(M_A, K_A).A_A.b_A$ and $X_A = H_4(b_{MA} \oplus K_A) \neq X$. Due to the inconsistency, signer will refuse to sign on forged blinded signature b_{MA}. Therefore, our scheme is secure against one-more forgeable attack.

Blindness. In *blinding* phase, requester introduces two integers *a* and *b* as the blinding factor to blind a message *M*. So, signer could not know about the content of message *M*. Additionally, the original Signature *(S', M')* could not reveal any information and also know the original signature as it would obtained by eliminating the blinding factor *a* and *b*, which is equivalent to solve the ECDLP. Hence, our scheme achieves the blindness property of generic blind signature.

Non-Repudiation. In signing phase, Signer signs on blinded message with his private key and the pre-computed information k is required to obtain the blinded signature in *BlindSig* Phase. Corresponding Public key of the signer is required in verify phase. Thus, the signer could not refuse the signature on message *M*.

4.2. Computational Analysis

In this section, proposed Identity-based based blind signature is compared with existing scheme [11],[13],[14]. Table 1 compared our scheme with other existing schemes in terms of computational cost, where P: pairing, M: scalar and G_1 elements multiplication, A: addition of two G_1 elements, H: hash function H: $\{0,1\}^* \rightarrow G_1$, M_s: two scalar multiplication, I_s: scalar inversion, C_s: comparison of two scalar, H_s: hash function H_s: $\{0,1\}^* x G_2 \rightarrow Z_q$, E_p: exponentiation of pairing, M_p: multiplication of two pairing, C_p: comparison of two pairing elements, P: publish stage, S: signer, R: requester, V: verifier and Pb: public, $\sum$: total operations at signer, requester and verifier side. Table 2 compared our scheme with other in terms of bandwidth cost, where G_1: points from first group, G_2: points from second group, s: scalar value, C: commitment, B: blinding, Sg: signing.

Table 1
Comparison of proposed scheme in term of computation cost.

Scheme		P	M	A	H	M_s	A_s	I_s	C_s	H_s	E_p	M_p	C_p
[11]	S	1	1				1				1		
	R	3	1	1	1	2					2	2	
	V	2			1						1	1	1
	$\sum$	**6**	**2**	**1**	**2**	**2**	**1**				**4**	**3**	**1**
[13]	S	1	2	1							1		
	R					1		2		1	3	2	1
	V	2						1		1	1		
	$\sum$	**3**	**2**	**1**		**1**		**3**		**2**	**4**	**2**	**1**
[14]	S	1	2	1							1		
	R	1	4	2			2			1			
	V	2						1	1	1	1	1	
	$\sum$	**4**	**6**	**3**			**2**	**1**	**1**	**2**	**2**	**1**	
Our	S	1	4	1	2				1				
	R	1	4	1	1		1		1				
	V		1	1									
	$\sum$	**2**	**9**	**3**	**3**		**1**		**2**				

Pairing of two points on elliptic curve is more time consuming operation as compared to addition of two points and point multiplication with scalar operation. Table 1 shows that proposed scheme takes only 2 pairing operation as compared to [11],[13],[14] schemes take 6, 8, 3 pairing operations respectively. Additionally, reader may notice that verification phase of our scheme consumes only one scalar multiplication, one addition operation and 0 pairing operations. As compared against other three schemes, our scheme claims that proposed scheme is more efficient. In order to examine the operation cost on elliptic curve, we use the results from panda project [19].

Table 2
Comparision of bandwidth cost of our scheme with exisiting scheme.

Scheme		G_1	G_2	s	*Cost*
[11]	C: S to R		1		384
	B: R to S			1	32
	S: S to R	1			32
	P: R to Pb	1	1		416
	Total				864
[13]	C: S to R		1		384
	B: R to S			1	32
	S: S to R	1			32
	P: R to Pb	1		1	64
	Total				512
[14]	C: S to R		1		384
	B: R to S			1	32
	S: S to R	1			32
	P: R to Pb	1		1	64
	Total				512
Our	C: S to R	1			32
	B: R to S	1			32
	S: S to R	2			64
	P: R to Pb	3		1	128
	Total				256

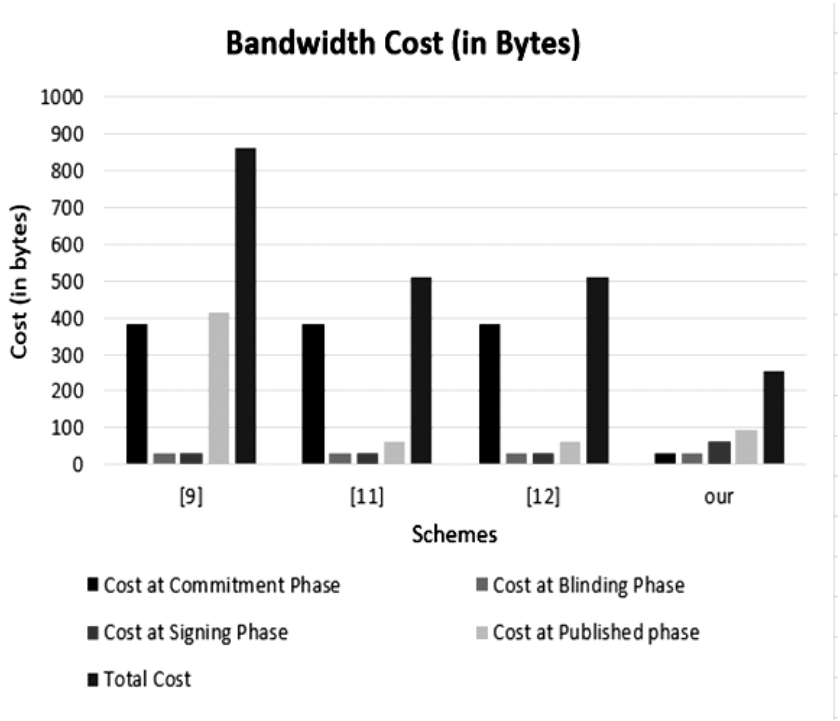

Figure 2: Comparison of bandwidth cost of our scheme against the existing scheme.

To calculate bandwidth cost shown in Table II, we use the results of pairing friendly elliptic curve introduced by Barretto-Naehrig [20], where the size of points in G_1 is 32 bytes, scalar element is 32 bytes and pairing points in G_2 is 384 bytes. From Fig. 2, reader can see that total bandwidth of proposed scheme is 256 bytes which is very less as compared to schemes [11], [13], [14] having bandwidth cost are 864, 512 and 512 bytes respectively.

5. CONCLUSION

With the incorporate benefits of Blind signature, IBC and ECC, a new ID-based blind signature system has been proposed. As comparison against three other ID-based blind signature schemes as shown in Table 1 and 2, proposed scheme gives less number of pairing operations and less bandwidth cost respectively, which allows less processing time for performing blind signature on message. Under the chosen message and ID attack, proposed system secure against one-more forgery and achieves blindness property. More significantly, the reported comparison given in Table 1 and 2 show that our scheme is far more efficient than other ID-based blind signature scheme that fully based on bilinear pairing which makes our scheme more favorable for implementing an E-commerce system where user's anonymity is the main concern.

ACKNOWLEDGEMENT

This research has been partially supported by the Council of Scientific and Industrial Research, a research and development organization in India, with sanctioned no. 09/263(1052)/2015EMR-I.

REFERENCES

[1] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[2] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*, 1983, pp. 199–203.

[3] H. Wang and Y. Zhang, "A protocol for untraceable electronic cash," in *International Conference on Web-Age Information Management*, 2000, pp. 189–197.

[4] J. Cao, Y. Zhang, and H. Wang, "An Electronic Cash Scheme and its Management," 2004.

[5] K. Alam, K. R. Alam, O. Faruq, and Y. Morimoto, "A comparison between RSA and ElGamal based untraceable blind signature schemes," in *2016 International Conference on Networking Systems and Security (NSysS)*, 2016, pp. 1–4.

[6] M.-S. Hwang, L. E. E. Cheng-Chi, and L. A. I. Yan-Chi, "An untraceable blind signature scheme," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 86, no. 7, pp. 1902–1906, 2003.

[7] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the Theory and Application of Cryptographic Techniques*, 1984, pp. 47–53.

[8] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Annual International Cryptology Conference*, 2001, pp. 213–229.

[9] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2002, pp. 533–547.

[10] F. Zhang and K. Kim, "Efficient ID-based blind signature and proxy signature from bilinear pairings," in *Australasian Conference on Information Security and Privacy*, 2003, pp. 312–323.

[11] Z. Huang, K. Chen, and Y. Wang, "Efficient identity-based signatures and blind signatures," in *International Conference on Cryptology and Network Security*, 2005, pp. 120–133.

[12] W. Gao, G. Wang, X. Wang, and F. Li, "One-round ID-based blind signature scheme without ROS assumption," in *International Conference on Pairing-Based Cryptography*, 2008, pp. 316–331.

[13] S. Kalkan, K. Kaya, and A. A. Selcuk, "Generalized ID-based blind signatures from bilinear pairings," in *Computer and Information Sciences, 2008. ISCIS'08. 23rd International Symposium on*, 2008, pp. 1–6.

[14] B. U. Rao, K. A. Ajmath, P. V. Reddy, and T. Gowri, "An ID-based Blind Signature Scheme from Bilinear Pairings," *Int. J. Comput. Sci. Secur.*, vol. 4, no. 1, p. 98, 2010.

[15] S. A. Vanstone, "Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments," *Inf. Secur. Tech. Rep.*, vol. 2, no. 2, pp. 78–87, 1997.

[16] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[17] S. MilierV, "Use ofelliptic curve in cryptography," *Advannce in Cryptology—CRYPTO*, vol. 85, pp. 417–426.

[18] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, 2000.

[19] C. Chuengsatiansup, M. Naehrig, P. Ribarski, and P. Schwabe, "PandA: Pairings and arithmetic," in *International Conference on Pairing-Based Cryptography*, 2013, pp. 229–250.

[20] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," in *International Workshop on Selected Areas in Cryptography*, 2005, pp. 319–331.