International Journal of Scientific & Engineering Research, Volume 7, Issue 1, January-2016
ISSN 2229-5518

ELECTRONIC COMMERCE ACCOUNTABILITY USING ELLIPTIC CURVE CRYPTOGRAPHY

Shamsherullah[1], Asmarullah[2], Ijaz Ul Haq[3], Nadeem Ahmad[4]
Department of Information Technology, Hazara University Mansehra, KPK Pakistan[1]
Government Degree College Mir Ali NWA, KPK Pakistan [2]
Department of Chemical Engineering Balochistan University of Information Technology, Engineering and Management Sciences[3]
Department of ICES University of Science and Technology Bannu KPK, Pakistan[4]
*shamsherdawar33@yahoo.com, asmarullah5@gmail.com, engineerijazulhaq@gmail.com, musawerdawar@gmail.com

***Abstract:* -** Accountability is used for a fair use in electronic services (e-services), which keep secret the ownership of the message m from un-authority. The construction of this scheme is valuable in the areas of electronic commerce (e-commerce) and electronic voting (e-voting) systems. We have proposed blind signature scheme for e-commerce accountability using Elliptic Curve Cryptography (ECC). It satisfies the properties of Confidentiality, Anonymity, Integrity, Unforgeability, Authenticity as well as Non-repudiation. The security of our proposed scheme is based on ECDLP, because ECC provide strong processing power, less storage space and less power consumptions.

Keywords: E-Commerce, Blind Signature, Accountability, Accountability Design, Elliptic Curve Cryptography

1 Introduction

ACCOUNTABILITY has been widely used in different perspectives and has many different terms and definitions like accountability in management, accountability in health care and accountability in internet transactions and accountability in e-commerce etc. Accountability mechanism is used to consistently identify an entity that can be held accountable for sending a packets / transactions. Unattractive costs of this omission include in-ability to attribute attacks of various kinds to higher level users. We used accountability in traditional business activities like electronic service (e-service) and e-commerce. It is used to deliver support, experience, utility and other intellectual content to its customer / client over internet. The important issue of accountability is the construction of a successful e-service provider in e-society and it is trust dependent and very quality sensitive. Accountability has a major concern for electronic business (e-business) around the world. In a business it provides a responsibility to someone or for some activity. To enhance the performance of e-business B. Meng [1] proposed research on accountability in electronic transaction**.** It gives conditions of money accountability and goods accountability in the e-payment protocol and also easily judge the e-payment have the goods and money accountabilities or not [1]. J. Gao [2] proposed design for accountability in multi-core networks, author says without accountability who is responsible for a certain traffic system will suffer from two extremes of security. So the possible extreme is the deficiency of legitimate responsibility for all the traffic. M. Sellami [3] says that accountability having the property, in which an entity is responsible for its acts, provides such kind of grantee and also promotes the use of the services. S. Chakrabarti [4] proposed efficient blind signatures for accountability; it is traditionally constructed from heavy weight cryptographic techniques and their performances are more suitable than traditional blind signature schemes. Therefore, we concern about the privacy and anonymity of the owner and signer in accountability services like e-services. The main goal of this paper is to conceal the privacy of owner and signer, we proposed e-commerce accountability based on EC.

The cryptographic application is the set of $E_p(a,b)$,which define an Abelian group, its calculation are accurately execute the occurrence of round off errors are dis-allowed [18].

Under the rules of addition the set of elliptic curve (EC) points in the form of commutative finite group are satisfies the following rules:

1. $O + P = P \text{ and } P + O = P$, where O is additive identity.
2. $-O = O$.
3. $P + (-P) = (-P) + P = O$, Where $-P$ is the -ve point of P.
4. $(P + Q) + R = P + (Q + R)$.
5. $P + Q = Q + P$.

For any two points $P = (x_P, y_P) \text{ and } Q = (x_Q, y_Q) \text{over } E_P(a,b)$

Now EC addition operation, which is written as $P + Q = R = (x_R, y_R)$, which fulfill the following rules:

$$\begin{bmatrix} x_R = \lambda_2 + x_P + x_Q \\ x_R = \lambda(x_P - x_R) - y_P \end{bmatrix}, \text{ Where}$$

$$\begin{cases} \lambda = \dfrac{y_Q - y_P}{x_Q - x_P} & if\ P \neq Q \\ \lambda = \dfrac{3x_P^2 + a}{2y_P} & if\ P = Q \end{cases}$$

International Journal of Scientific & Engineering Research, Volume 7, Issue 1, January-2016
ISSN 2229-5518

Elliptic curve point multiplication operation over an integer is $E_p(a, b)$, represented as $Q = kP$ and can be defined as repeated elliptic curve additions operations.

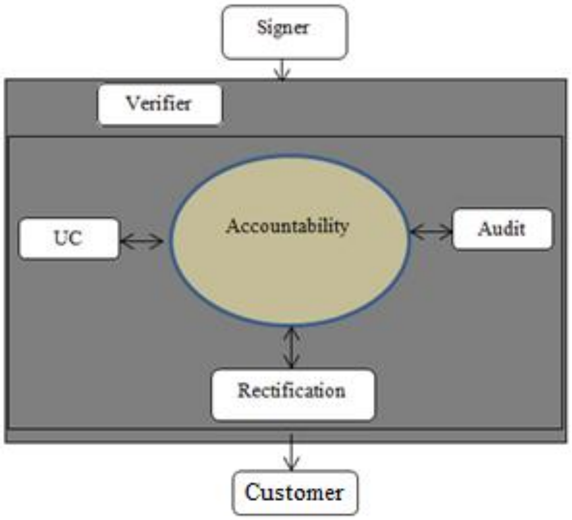

Fig. 1 Proposed Scheme Flow

There are three entities within accountability (usage control (UC), audit and rectification) and two out sider entities signer and customer, which are communicated to each other. From figure 1, it is clear that accountability is hiding from signer and customer, but it anonymously performs all the required function in needed instance. Now in accountability UC, Audit and Rectification are providing the following properties:

CU: It covers all access control with money distribution and transformation of e-payment in e-commerce.
Audit: It covers detection, judgment and evidences collection of all e-payments in e-commerce.
Rectification: It includes punishment for sanction remediation and compensation functionalities.

II LITERATURE REVIEW

D. Chaum [5] extend digital signature and introduced a new idea of blind signature with two additional properties such as blindness and un-linkability. Scheme [5] is well-organized for electronic payment and electronic voting system. A. C. Squicciarini [6] introduced a policy-based accountability tool for grid computing systems. In this scheme accountability agent, entities performing a wide range of information gathering and keeping track of submitted jobs and their users and also have the additional improvement of supporting a form of redundancy. W. Lou [7] proposed security, privacy and accountability in wireless access networks. The author proposes a novel authentication frame-work that accomplishes improved user privacy protection with suitable user/ customer accountability. J. Yao [8] proposed accountability as a service for the cloud. J. Yao propose a novel design to implement solid accountability in the SOA organized in cloud. Accountability, not only faults can always be guaranteed to their causers, this binding is permanently un-deniable as well as provable. K. J. Lin [9] proposed accountability computing for e-society, it presents an SOA research project, which is account-able service transfer in-frastructure to support the monitor, analyses and reconfiguration of service process. W. Lee [10] Proposed profile-based selection of accountability policies in grid computing systems, to solve such conflicts and get flexible accountability processes. M. Hirai [11] a chain of accountabilities in open system based on assured entrustments, it make consistence system of accountability in the "DEOS Process". C. Techapanupreeda [12] present accountability in internet transactions revisited. The author conducts a survey of different viewpoints of accountability to designate that the definition of accountability is limited in internet transactions. R. A. Cherrueau [13] scheme shown how the harness of the accountability schemes to tackle real world destructions of accountability properties rising from security vulnerabilities of oauth based authentication and authorization accountability policies in protocols. B. Meng [1] present practical detailed requirements of accountability and its application in electronic payment protocols, without logic reasoning and complex analysis whether e-payment protocols. J. L. Camenisch [14] scheme is provide guarantee the anonymity of the applicants. D. Pointcheval [15] proposed scheme avoid the forgery of a user signature without his secret key knowledge. A. Boldyreva [16] proposed threshold signature, multi-signatures as well as blind signatures based on the gap Diffie Hellman group signature scheme. This scheme is much simple and more efficient than existing schemes and also has useful characteristics. M. Abe [17] scheme provably secure from double spender traceable electronic cash system. Scheme [17] provably secure from double spender traceable e-cash system. Yang, XianFeng, and Changjiang Li. Limitation of this is not full fill the security properties like anonymity, unforgeability as well as authenticity [19].
We compare our proposed scheme with scheme [19, 4, 14, 17], its security is based on Discrete Logarithm Problem (DLP). The limitations of these schemes have high computation and communication costs. Our proposed scheme is simple and more efficient than existing schemes.

III PROPOSED SCHEME

This section presents a novel blind signature scheme for accountability using elliptic curve cryptography. Proposed

International Journal of Scientific & Engineering Research, Volume 7, Issue 1, January-2016
ISSN 2229-5518

scheme has three participants: Customer, Signer and Verifier, and also have four phases: Pre- Requisite Phase, Key Generation, Blind Signature as well as Verification. Each participants and phases are described one by one below:

- **Pre-requisite Phase**

In this phase, the domain parameters, which are used in our proposed scheme, are define and given below in Table1.

TABLE 1
PARAMETERS

Symbols	Description
$\boldsymbol{q}$	A large prime Number where $q > 2^{160}$
$\boldsymbol{F_q}$	A finite field of order q
$\boldsymbol{E}$	Elliptic curve over finite fields $F_q: y^2 = (x^3 + ax + b) mod\ q$
$\boldsymbol{n}$	A large Prime number where $n > 2^{160}$
$\boldsymbol{G}$	A base point of elliptic curve F_q with order n
$\boldsymbol{h/hk}$	One way / key hash function

- **Key Generation Phase**

All these three parties are randomly generate private keys and compute their public keys. Signer chooses d_s and computes his public key d_s as $p_s = d_s.G$. Customer selects d_c as a private key and computes his public p_c as $p_c = d_c.G$. And verifier also selects d_v as a private key and computes his public key $p_v = d_v$.G

- **Blind Signature Phase**

This phase contains two participants like, signer and customer.

Signer

Signe sign electronic service (e-service) transactions and send to customer.

(1) Randomly Generate $w \in \{0, 1, 2, \ldots . n-1\}$
(2) Compute $z = w.G\ mod\ n$
(3) Send z to customer

Customer

Now customer computes keys $(k_1||k_2)$, signature (r), blind signature $(\bar{r})$ and send again it to signer.

(1) Generate Blinding Factors $\alpha, \beta, \gamma\{0, 1, 2 \ldots\ldots n-1\}$
(2) Compute $r = \alpha.G\ mod\ n$
(3) Compute $(k_1||k_2) = h(r.p_v\ mod\ n)$
(4) Compute $r = kh_{k_2}(m||k_2)$
(5) $T = ((\gamma + \beta).z + \alpha.G) mod\ n$
(6) $\bar{r} = (\gamma + \beta) mod\ n$
(7) Send $\bar{r}$ to Signer

Signer

Again signer checks the validity of the blind signature, which is send by the customer.

(1) Compute $\bar{s} = (\mathrm{p_s} + \bar{r}.w) mod\ n$
(2) Send $\bar{s}$ to customer

Customer

Customer gets some cipher text and sends it to verifier, for verification.

(1) Compute $s = \frac{\gamma}{r+\bar{s}+\alpha} mod\ n$
(2) Send (r, s, T) to verifier

- **Verification Phase**

In this phase verifier verify that $r' = r$. It show the validity, If r' and r are equal together.

Verifier

Verifier check validity of the key, messages as well as blind signature. If valid accept otherwise reject.

(1) Compute $u = d_v.s$
(2) Compute $k = h(u.(p_s + T + r.G))$
(3) Compute $r' = kh_{k_2}(m||k_2)$
(4) If $r' = r$ accept, otherwise reject

International Journal of Scientific & Engineering Research, Volume 7, Issue 1, January-2016
ISSN 2229-5518

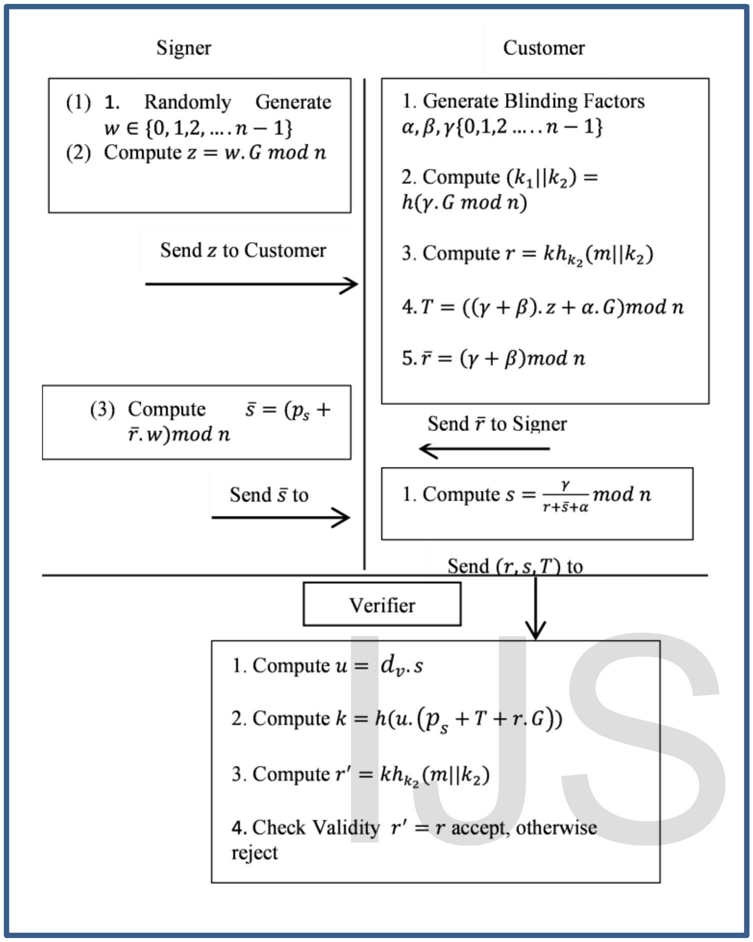

Fig. 2 Flow of Proposed Algorithm

IV SECURITY ANALYSIS

In security analysis we present all the security properties of the proposed scheme.

- **Confidentiality**

Let d_s is private keys of Signer and d_c customer are compromised to each other, the attacker cannot reveal the original transaction of the customers.

- **Anonymity**

An anonymous communication customer used α belongs to blind factor and G Elliptic curve for computing a blind signature. To find α from equation (1) is hard because α is selected from the set of anonymous factor.

$$r = \alpha.G \bmod n \qquad (1)$$

- **Integrity**

Verifier verifies that the message m which is send by the customer is original or not. If he obtained m' instead of m. For collision resistant, we used the property $r' = kh_{k_2}(m||k_2) \neq r = kh_{k_2}(m||k_2)$.In which detect eavesdropper activities.

- **Authenticity**

Signer use his own private key d_s to generate $\bar{s} = (d_s + \bar{r}.w) \bmod n$, compute d_s from $p_s = d_s.G$ is computationally hard equivalent to solve ECDLP.

- **Unforgeability**

Without know private key $s_{pr}$of the signer and his randomly generated parameter w. such as $\bar{s} = (d_s + \bar{r}.w) \bmod n$. If third party want to compute $\bar{s}$ he/she need to find p_s and w. To compute $p_s$from equation $p_s = d_s.G$. is computationally hard due to ECDLP and w from equation $z = w.G \bmod n$ is also computationally hard for third party, equivalent to solve ECDLP.

- **Non-repudiation**

When dispute occur, the verifier can send encrypted message, encrypted signature as well as signer digital signature (r', s', T') to judge for checking, whether signature is generated by signer or not.

TABLE 2

SECURITY ANALYSIS

Author(s)	Properties					
	Confidentiality	Anonymity	Integrity	Non-Repudiation	Unforgeability	Authenticity
Proposed Scheme	Yes	Yes	Yes	Yes	Yes	Yes
X. Yang and C. Li [19]	Yes	No	Yes	Yes	No	No
S. Chakrabarti et al. [4]	No	Yes	No	No	No	No
J.L. Camenisch[14]	No	Yes	No	No	No	No
D. Pointcheval [15]	No	Yes	No	Yes	No	No

International Journal of Scientific & Engineering Research, Volume 7, Issue 1, January-2016
ISSN 2229-5518

V COST ANALYSIS

1. Computational Cost

Computational cost comparisons of proposed scheme with existing scheme are given in table 1. Where in table 1 G. Cost is "generation cost", Veri. Cost is "verification cost", M-E is "Modular Exponentiation", ECPM is "Elliptic curve Point Multiplication" and Sc. M is "Scalar Multiplication".

TABLE 3

COMPUTATIONAL COST COMPARISON

Author	*Costs*	*Major Operation*			
		M-E	*ECPM*	*Sc. M*	*Pairing Computation*
Proposed Scheme	G. Cost	–	3	–	–
	Veri. Cost	–	1	–	–
X. Yang and C. Li [19]	G. Cost	2	4	–	–
	Veri. Cost	–	–	–	–
S. Chakrabarti et al. [4]	G. Cost	–	–		30
	Veri. Cost	–	–		20
J.L. Camenisch[14]	G. Cost	16	–	–	–
	Veri. Cost	8	–	–	–
D. Pointcheval [15]	G. Cost	–	–	3	–
	Veri. Cost	–	–	–	–

2. Communication Cost

In communication cost we compare different size of PK (Public Key) size and signature size [4] with existing schemes in Figure1.

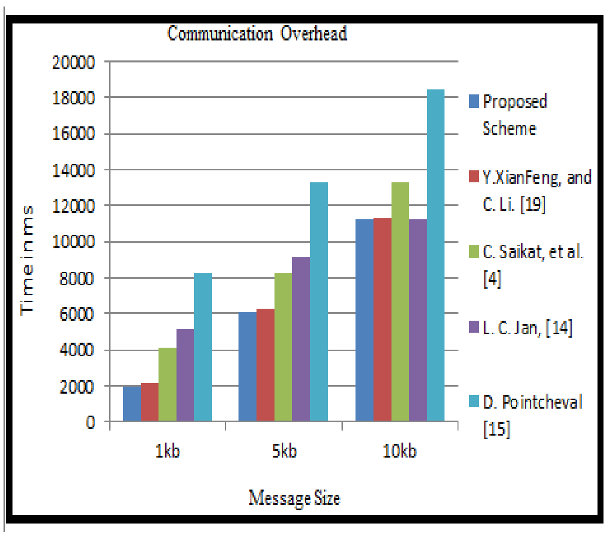

Fig. 3 Communication Costs

VI CONCLUSION

We proposed blind signature for E-Commerce accountability based on Elliptic Curve (EC). It satisfies the properties of Confidentiality, Anonymity Integrity, Unforgeability, Authenticity as well as Non-repudiation. The security of our proposed scheme is based on ECCDLP. Its key size is short as compare to existing schemes, which is based on Discrete Logarithm Problem (DLP), El-Gamal and RSA. It has low generating and verification costs as compared to existing schemes.

VII FUTURE WORK

In future, we more extend e-commerce accountability based on hyper elliptic curve.

REFERENCES

[1] B. M. B. Meng and H. Z. H. Zhang, "Research on accountability in electronic transaction," *Proc. Ninth Int. Conf. Comput. Support. Coop. Work Des. 2005.*, vol. 2, pp. 745–749, 2005.

[2] J. Gao and H. Hall, "Design for Accountability in Multi-core Networks."

[3] Sellami, Mohamed, Jean-Claude Royer, and Walid Benghabrit. "Accountability for data protection." *Computational Intelligence for Multimedia Understanding (IWCIM), 2014 International Workshop on. IEEE*, 2014.

[4] Chakrabarti, Saikat, et al. "Efficient blind signatures for accountability." Secure Network Protocols, 2007. NPSec 2007. 3rd IEEE Workshop on. IEEE, 2007.

[5] D. Chaum. "Blind signatures for untraceable payments," Advances in Cryptology - Crypto '82 Springer-Verlag, vol. 10, 1983, pp. 199-203, 1983.

[6] A. C. Squicciarini, W. Lee, E. Bertino, and C. X. Song, "A policy-based accountability tool for grid computing systems," *Proc. 3rd IEEE Asia-Pacific Serv. Comput. Conf. APSCC 2008*, pp. 95–100, 2008.

[7] Lou, Wenjing, and Kui Ren. "Security, privacy, and accountability in wireless access networks." Wireless Communications, IEEE 16.4 (2009): 80-87.

[8] J. Yao, S. Chen, C. Wang, D. Levy, and J. Zic, "Accountability as a service for the cloud: From concept to implementation with BPEL," *Proc. - 2010 6th World Congr. Serv. Serv. 2010*, pp. 91–98, 2010.

[9] Lin, Kwei-Jay, Joe Zou, and Yan Wang. "Accountability Computing for E-society." *Advanced Information Networking and Applications (AINA), 2010, 24th IEEE International Conference*, 2010.

[10] W. Lee, A. C. Squicciarini, and E. Bertino, "Profile-based selection of accountability policies in grid computing systems,"

International Journal of Scientific & Engineering Research, Volume 7, Issue 1, January-2016
ISSN 2229-5518

Proc. - 2011 IEEE Int. Symp. Policies Distrib. Syst. Networks, POLICY 2011, pp. 145–148, 2011.

[11] Hirai, Makoto, Yoshifumi Yuasa, and Yoshiki Kinoshita. "A chain of accountabilities in open systems based on assured entrustments." *Software Reliability Engineering Workshops (ISSREW), 2013, IEEE International Symposium,* 2013.

[12] C. Techapanupreeda, et al. "Accountability in internet transactions revisited." Communications and Information Technologies (ISCIT), 2014 14th International Symposium on. IEEE, 2014.

[13] R.-A. Cherrueau and M. Sudholt, "Enforcing Expressive Accountability Policies," *2014 IEEE 23rd Int. WETICE Conf.*, pp. 333–338, 2014.

[14] Camenisch, Jan L., Jean-Marc Piveteau, and Markus A. Stadler. "Blind signatures based on the discrete logarithm problem." *Advances in Cryptology—Eurocrypt'94. Springer Berlin Heidelberg*, 1995.

[15] Pointcheval, David, and Jacques Stern. "Security arguments for digital signatures and blind signatures." *Journal of cryptology* 13.3 2000, pp. 361-396.

[16] Boldyreva, Alexandra. "Threshold signatures, multi-signatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme," Public key cryptography—PKC 2003. *Springer Berlin Heidelberg*, 2002. pp. 31-46, 2002.

[17] Abe, Masayuki. "A secure three-move blind signature scheme for polynomially many signatures." *Advances in Cryptology—Eurocrypt 2001. Springer Berlin Heidelberg*, 2001, pp. 136-151, 2010.

[18] Huang, Kuo-Hsuan, et al. "Efficient migration for mobile computing in distributed networks." *Computer Standards & Interfaces* 31.1 (2009): 40-47.
[19] Yang, XianFeng, and Changjiang Li. "Constructing E-Commerce Security System Based on ECC and PKI Technology." *Journal of Convergence Information Technology* 8.2 (2013).