ELECTRONIC COMMERCE ACCOUNTABILITY USING ELLIPTIC CURVE CRYPTOGRAPHY

Shamsheerullah 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 unauthorized. 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 signature schemes 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. \( 0 + P = P \) and \( P + 0 = P \), 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 \( P = (x_p, y_p) \) and \( Q = (x_q, y_q) \) over \( E_p(a,b) \) Now EC addition operation, which is written as

\[
P + Q = (x_r, y_r),
\]

which fulfill the following rules:

\[
\begin{align*}
x_r &= \lambda x_p + x_q + \lambda^2 - a - x_p x_q, \\
x_r &= \lambda (x_p - x_q) - y_p, \\
\lambda &= \frac{y_q - y_p}{x_q - x_p} \quad \text{if } P \neq Q, \\
\lambda &= \frac{3x_p^2 + a}{2y_p} \quad \text{if } P = Q
\end{align*}
\]
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 causes, 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-rastructure 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. Cherueau [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
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>
<thead>
<tr>
<th>Symbols</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$q$</td>
<td>A large prime Number where $q &gt; 2^{160}$</td>
</tr>
<tr>
<td>$F_q$</td>
<td>A finite field of order $q$</td>
</tr>
<tr>
<td>$E$</td>
<td>Elliptic curve over finite fields $E_q: y^2 = (x^3 + ax + b)mod q$</td>
</tr>
<tr>
<td>$n$</td>
<td>A large Prime number where $n &gt; 2^{160}$</td>
</tr>
<tr>
<td>$G$</td>
<td>A base point of elliptic curve $E_q$ with order $n$</td>
</tr>
<tr>
<td>$h/hk$</td>
<td>One way / key hash function</td>
</tr>
</tbody>
</table>

- **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 $d_sG$ as $p_s = d_sG$. Customer selects $d_c$ as a private key and computes his public $p_c$ as $p_c = d_cG$. And verifier also selects $d_v$ as a private key and computes his public key $p_v = d_vG$.

- **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 $w \in \{0, 1, 2, ..., n - 1\}$
(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 ($\tilde{r}$) and send again it to signer.

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

**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 $r' = kh_k(m||k_2)$
(4) If $r' = r$ accept, otherwise reject

**Verification Phase**

In this phase verifier verify that $r' = r$. It show the validity, If $r'$ and $r$ are equal together.
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 $\alpha$ belongs to blind factor and $G$ Elliptic curve for computing a blind signature. To find $\alpha$ from equation (1) is hard because $\alpha$ is selected from the set of anonymous factor.

$$r = \alpha.G \mod n \quad (1)$$

• 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 $\bar{s} = (d_s + \bar{r}.w) \mod n$, 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 $\bar{s} = (d_s + \bar{r}.w) \mod n$. 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 $x = w.G \mod n$ 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 $(r', \bar{s}', T')$ to judge for checking, whether signature is generated by signer or not.

TABLE 2

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Confidentiality</th>
<th>Anonymity</th>
<th>Integrity</th>
<th>Non-repudiation</th>
<th>Unforgeability</th>
<th>Authenticity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed Scheme</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X. Yang and C. Li</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>S. Chakrabarti et al. [4]</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>J.L. Camenisch[14]</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>D. Pointcheval [10]</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Author</th>
<th>M-E</th>
<th>ECPM</th>
<th>Sc. M</th>
<th>Pairing Computation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed Scheme</td>
<td>G. Cost</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Veri. Cost</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X. Yang and C. Li [19]</td>
<td>G. Cost</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Veri. Cost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Veri. Cost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Veri. Cost</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Veri. Cost</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Communication Cost

In communication cost we compare different size of PK (Public Key) size and signature size [4] with existing schemes in Figure 1.

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


