International Journal of Computer Science and Informatics

Volume 2 | Issue 3 Article 12

January 2013

Secure E-Tendering Using Identity Based Encryption from Bilinear Pairings

K. V. Ramana
CSE, CIST, Kakinada, India, kvramana.mtech09@gmail.com

K. Anantha Lakshmi
CSE, CIST, Kakinada, India, lakshmi_anantha2002@yahoo.co.in

D. Anusha
CSE, CIST, Kakinada, India, anushadv@gmail.com

Secure E-Tendering Using Identity Based Encryption from Bilinear Pairings

K. V. Ramana, K. Anantha Lakshmi & D. Anusha

CSE, CIST, Kakinada, India
E-mail : kvramana.mtech09@gmail.com, lakshmi_anantha2002@yahoo.co.in, anushadv@gmail.com

Abstract **-** An electronic tender system (e-tender) streamlines the tender process and thereby saves time and cost. Security requirements for e-tendering systems have not been closely scrutinized in the literature. In addition to the security concerns of conventional e-tender systems—authentication, integrity, privacy, and non-repudiation are provided.

This paper identifies key issues to be addressed in the design of secure e-tendering systems. Key issues are the privacy protection and verifiability. A new e-tendering architecture, based on Identity Based Encryption from bilinear pairings is proposed which may be suitable for secure large scale operations. A Encryption is a scheme that provides private and authenticated delivery of message between tenderer and tenderee. This is done in a more efficient manner than a straight forward composition of an encryption followed by signature scheme. An Identity based Cryptosystem is one in which the public key may be as String (E-mail Address, PAN No., etc).

We propose Identity based encryption for secure e-tendering system that satisfies all the requirements an ideal atomic system requires. The elegant design makes it efficient both in computation and in communication. Secure e-Tendering System is carrying out of the tendering process using electronic means, such as the internet and specialist e-tendering software applications with a secured scheme.

Keywords **-** *Identity Based encryption, e-tender, Bilinear Pairings, authentication, integrity, privacy, non-repudiation, tenderer, tenderee.*

I. INTRODUCTION

A tender process should provide proper degrees of privacy on the submitted proposals and on the identities of the tenderers at different stages during the whole process, and support adaptive public verifiability levels as to the published information at different stages in the process. Conventional cryptographic systems (like signature, encryption, and etc) and trivial composition of these systems cannot provide the privacy protection and verifiability property. Assume m to be a proposal for some tender, to submit the proposal m with non-repudiation, the tenderer may send the proposal m with his signature.

In a traditional PKC[4], the association between a user's identity and his public key is obtained through a digital certificate issued by a Certifying Authority (CA)[4]. The CA checks the credentials of a user before issuing a certificate to him. If tenderee[5] wants to send a signed proposal to tenderer, he obtains a digital certificate for her public key from a CA.

Tenderee then signs a proposal using his private key and sends the signed proposal along with his certificate to Tenderer[5].

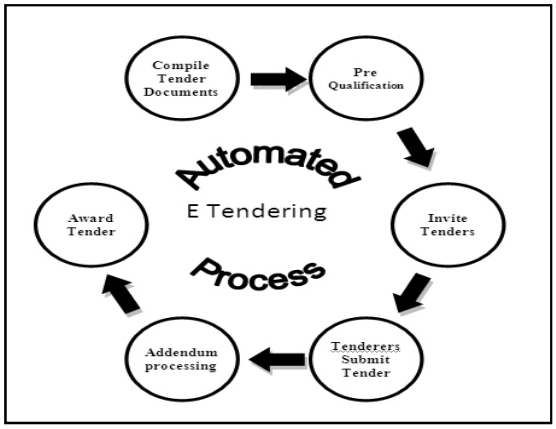

Fig. 1: E-Tendering Process.

Tenderer first verifies the validity of the certificate by checking the certificate revocation list published by the CA, then he verifies the signature using public key in the certificate. If many CAs are involved between Tenderee and Tenderer the entire certificate path has to be verified. Hence, the process of certificate management requires high computational and storage efforts.

The security requirements a general e-tender system should live up to as follows.

1. Authentication: Only registered tenderees can publish their tender documents, and only registered tenderers can submit their proposals.
2. Integrity: The integrity of the tender document and the submitted proposals should be preserved.
3. Non-repudiation: A tenderee cannot repudiate her/his published tender information, and a tenderer cannot repudiate her/his submitted proposal.
4. Adaptive privacy protection and adaptive verifiability: Through a tender process, a secure e-tender system should provide different degrees of privacy protection to the identities of the tenderers and their proposal contents and provide different verifiability levels to the published information at different stages in the process.

Up to the present time, though a number of e-tender systems have been put to use around the world with quite some research efforts focused on them, none of the e-tender systems developed so far has featured the property of privacy protection and verifiability.

In this paper, we shall propose a Secure E-Tender System based on encryption from Bilinear Pairings that satisfies all the requirements above. The contributions of our new system to this field of research are:

(1) It is the first study on secure e-tender system design that features the privacy protection and verifiability property;

(2) It is a secure system that satisfies the adaptiveness requirement based on a well-designed building block; and

(3) The design of an atomic system results in a very efficient scheme in terms of computations and communications.

II. METHODOLOGY

A. Bilinear Pairings

Let (G,+) and (V,.) denote cyclic groups of prime order q. Let P be a generator of G and let e: GxG→V be a pairing satisfying the condition below.

Bilinear: For all P,Q ∈G and all a,b∈Z we have $e(aP,bQ) = e(P,Q)^{ab}$ [1]. (1)

Such groups may be realized using supersingular elliptic curves and the Tate pairing.

Modified Tate pairing: Let p be a prime such that q|(p − 1) for a large prime q. Let G_1 and G_2 be two cyclic groups of order q. G_1 is a subgroup of finite field F∗p2 . The modified Tate pairing is a mapping $e : G_1 \times G_1 \rightarrow G_2$ which satisfies the following properties:

(i) Bilinear: $e(aP, bQ) = e(P,Q)^{ab}$, for all P,Q ∈G1 and all a, b ∈ Zq.

(ii) Non-degenerate: There exists a point P ∈ G1 such that $e(P,P) \neq 1$.

(iii) Computable: e(P,Q) can be computed in polynomial time.

The scheme also requires three hash functions:

$$H_1 : \{0,1\}^* \rightarrow G^*; H_2 : \{0,1\}^* \rightarrow Z_q^*; H_3 : Z_q^* \rightarrow \{0,1\}^n$$

B. Some Computational Complexity Assumptions

The security of proposed protocols is based on some well-studied problems that are assumed to be hard to compute efficiently.

Computational Diffie-Hellman assumption (CDH):

G_1 is a group of prime order q, $P \in G_1^*$ is the generator of G_1 , for ∀ a, b$\in Z_q^*$, given P, aP and bP , computing abP is hard.

Bilinear Diffie-Hellman assumption (BDH):

G_1 and G_2 are two cyclic groups of prime order q,P∈ G_1^* is the generator of G_1, ę is a bilinear map e: $G_1 \times G_1 \rightarrow G_2$ for ∀ a, b$\in Z_q^*$, given P, aP , bP and cP , computing $e(P, P)^{abc}$ is hard.

Decision Bilinear Diffie-Hellman assumption (DBDH):

G_1 and G_2 are two cyclic groups of prime order q, P∈ G_1^* is the generator of G_1 , ę is a bilinear map e: $G_1 \times G_1 \rightarrow G_2$ for ∀ a,b,c$\in Z_q^*$, given P, aP , bP and cP and w$\in G_2$, it is hard to decide whether $e(P, P)^{abc} = w$.

Gap Bilinear Diffie-Hellman assumption (Gap-BDH):

G_1 and G_2 are two cyclic groups of prime order q, P∈ G_1^* is the generator of G_1 , ę is a bilinear map e: $G_1 \times G_1 \rightarrow G_2$ for ∀ a,b,c$\in Z_q^*$, given P, aP , bP and cP and w$\in G_2$, it is hard to decide whether $e(P, P)^{abc} = w$.

C. Identity-Based encryption from Bilinear Pairings

The concept of encryption was proposed in 1997 by Zheng as a primitive that combines the functionality of a digital signature and encryption scheme at a much lower cost than separately conducting these operations one after the other. An ID-based encryption[1] scheme consists of four basic algorithms: Setup, Extract, encrypt, decrypt[1]. Position figures and tables at the tops and bottoms of columns.

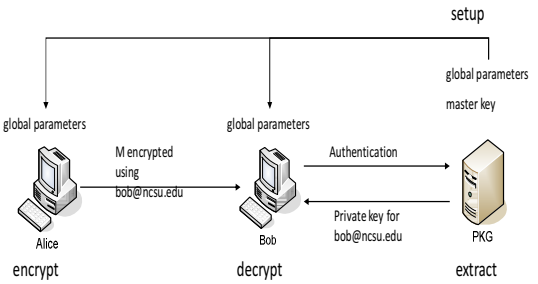

Fig 2 : Framework of ID-based encryption

Setup generates global system parameters and a master-key, Extract uses the master-key to generate the private key corresponding to an arbitrary public key string ID, Encrypt encrypts messages using the public key ID, Decrypt decrypts messages using the corresponding private key.

The security model for the encryption primitive is a combination of the models for encryption and digital signature. In the case of identity based encryption, the important security notions are semantically secured against an adaptive chosen cipher text attack, and existential unforgeability against a chosen message attack. The major difference is that instead of producing a valid message/signature pair, this must produce a valid encryption message.

Identity based cryptography was proposed by Shamir[1] in 1985. The problem that this author addressed was the need for multiple interactions between users using public key cryptography. Shamir's idea consists of using a readable representation of the identity as the public key, thereby eliminating the need for public key certificates.

The requirements for this type of scheme are the following:

- The KGC must be able to generate private keys efficiently from identities,using a given master key, which it keeps secret;
- Not knowing this master key, it must be infeasible for any party to obtain it, given an arbitrary number of key pairs and instances of the identity based algorithm execution; and,
- Not knowing this master key, it must also be infeasible to recover an agent's private key.

Public Parameters	$(G_1, G_2, G_T, e, H, P, P_{pub})$	Two cyclic groups of prime order q and a bilinear map between them $e:G_1xG_1 \rightarrow G_T$,such that DBDH problem is hard. Three hash functions H_1, H_2 and H_3 that take identity respresentations to G_1, arbitrary bit strings to Zq*, and element of G into the n-bit-long message space, respectively. A random generator P of G_1, and the KGC's public key $P_{Pub} \in G_1$.
KGC Master Key	s	The discrete logarithm of P_{Pub} to the base P, or Ppub = sP
Private Key Extraction	d_{ID}	Given a finite bit string representing the ID, the private key is $d_{ID} = sQ_{ID} = sH_1(ID)$
encryption	C=(U,V,c)	U = xP, with x random, r = $H2(U \| m)$, $V = xP_{Pub}+r*d_{IDA}$, $c=m \oplus H_3(e(P_{Pub}, Q_{IDB})^X)$
Deccryption	m	$M=c \oplus H_3(e(U, d_{IDB}))$, r = $H2(U \| m)$, If $e(V,P) = U(e(Q_{IDB}, P_{Pub})^r)e((U, P_{Pub})$ then m

Table 1 : Identity Based Enncryption Scheme

In the case of identity based encryption, the important security notions are semantical security against an adaptive chosen ciphertext attack, and existential unforgetability against a chosen message attack.

D. E-Tender System

E-Tendering comprises:

- Undertaking the tasks of advertising the requirement for goods or services, registering suppliers, and issuing and receiving tender documents via the internet[5]
- Automating the evaluation of responses to a tender.

Our e-tender model includes three kinds of entities—the tenderers (denoted as U_i,i=1~n), the tenderee (TE), and the trusted third party (TA). To clearly specify the adaptive property, we divide the process into six stages—the initial stage, the tender announcement and proposal submission stage, the qualification examination stage, the tender opening stage, the contract signing stage, and the arbitration stage.

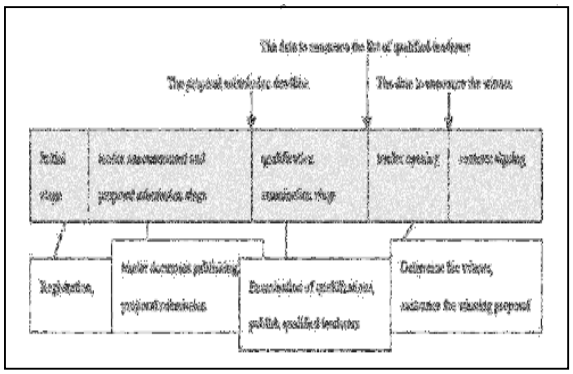

Fig 3 : Process of E-Tender System[5]

We derive the system by providing security from Identity Based encryption using bilinear pairings[3].

1). The Initialization Stage

Initially, the system sets up the parameters for all as tenderee(TE), tenderers(U_i) and trusted third party(TA) for providing both authentication and encryption. All the entities have their identities and private keys issued by Private key Generator(PKG)[3]. TE register their accounts at the PKG. The TE prepares the tender document doc that contains the specifications, the regulations, and the deadlines of the different stages. Then the TE submits the document doc to TA.

2). The tender announcement and proposal submission stage

After verifying the signature from TE, TA publishes the doc on its blackboard (BB) in an authenticated manner. Each interested U_i downloads the document, prepares his proposal m_i and his commitment C_i. Upon receiving the commitment C_i from U_i, the TA generates a signature on the commitment C_i concatenated with the current date as a receipt. U_i can download the receipt from the blackboard.

At this stage, even though anyone gets to know whether there is any encrypted proposal C_i already submitted, she/he (except the TA) cannot identify who submitted the proposal and has no access to the proposal contents. The concealment of the tenderer's identity and the proposal contents at this stage is very important. After the submission deadline, the TA rejects any submission.

3). The qualification examination stage

At this stage, the TA verifies whether each submitted commitment C_i is valid as follows.

1. whether the U_i is valid Tenderer
2. C_i is a valid commitment
3. Check m is the proposal
4. Checks whether Ui satisfies the qualification regulations if there are regulations specified in the document.

Public verifiability to the list along with concealment of the proposal contents at this stage is very important. If the number of qualified proposals does not reach or exceed the threshold value, the proposal content is still kept secret from the public and the TE such that every U_i can still resubmit her/his proposal for the next tender process.

4). The tender opening stage

If the number of qualified proposals reaches or exceeds the threshold value, then the TA forwards the qualified proposals to the TE securely (for example, through a SSL channel). Only until this stage can the TE see the contents of the proposals. Then the TE evaluates these proposals and determines the winner according to the regulations. The TE forwards the results and his signature to the TA, and the TA publishes the winning proposal in an authenticated manner.[5]

Now the public can verify the validity of the winning proposal. If all the verifications turn out positive, the proposal is valid. A competitor Uj can compare her/his proposal m_j with the winning proposal m_i and asks the TA for arbitration if she/he does not agree with the result.

5). The contract signing stage

If no dispute happens within the specified time limit, then the winning tenderer U_i and TE can sign the contract.

6). The arbitration stage

Within the specified time limit, U_j can ask TA for arbitration by submitting the decrypted proposal if he does not agree with the result. The TA can verify the validity of the proposal by going through the verification procedure at the tender opening stage.

E. Security analysis

The security of the proposed system is analyzed as follows.

Authentication :

The authenticity of the tenderee's doc and TA's published data can be assured by verifying the corresponding signatures. The authenticity of the decrypted proposal can be verified through the verification equations. Therefore, the authenticity can be assured because the underlying scheme is secure.

Integrity, non-repudiation :

The integrity and the non-repudiation property of the tender document doc, the qualified list, and the proposal m_i are assured due to the corresponding signatures and the commitment

Privacy protection and Adaptive verifiability :

At the tender announcement and proposal submission stage, no one except the TA can decrypt and verify the commitment. At the qualification examination stage, the TA publishes the list of qualified proposals. Later every one can verify whether Ui has indeed submitted some proposal by checking the equation. However even though any one can verify the commitment the TA knows nothing about the content of the proposal at this stage.

Finally, at the tender opening stage, the winning proposal is published, such that everyone can verify the validity of the proposal contents by checking the corresponding verification equations. The adaptiveness property is achieved.

IV. RESULTS AND DISCUSSION

Secure e-tendering system facilitates the complete tendering process from the advertising of the requirement through to the placing of the contract. This includes the exchange of all relevant documents in electronic format with secured cryptographic techniques. From a tenderee's perspective e-tendering is a means of electronically notifying, inviting, vetting and selecting tenderers to tender for products or services. For tenderers, e-tendering can be defined as the electronic submission of competitive bids for the provision of products or services. Security concern is carried out in the entire procedure by the application using concept of Identity based encryption from Bilinear Pairings.

V. CONCLUSION

In this paper, we have offered the first secure e-tender system that supports privacy protection and adaptive verifiability. This adaptiveness property is important to fair competition during a tender process. It is very efficient that only one message interaction is required for each tenderer and both the computation overhead and communication overhead is very low. System is assumed to run under the condition that all tendering parties (tenderee and tenderers) are dishonest players. Our informal and formal security analysis shows that the system meets the security goals under well known collusion scenarios. Because security is a process not a product, our approach will have broad industry application for developing secure electronic business processes in areas other than e-tendering.

REFERENCES

[1] Dan Boneh, Matthew Frankliny "Identity-Based Encryption from the Weil PairingDan," Appears in SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.

[2] John Malone-Lee, "Identity Based Signcryption," *University of Bristol*, Department of Computer Science, Bristol, UK.

[3] Xiuxia Tian Yong, "ID-Based Encryption with Keyword Search Scheme from Bilinear Pairings," School of Computer and Information Engineering Shanghai University of Electric Power .

[4] Mengbo Hou and Qiuliang "Two-Party Authenticated Key Agreement Protocol from Certificateless Public Key Encryption Scheme," School of Computer Science and Technology Shandong University Jinan, 250101, China.

[5] Mohammadi, S. Jahanshahi, "A Secure E-Tendering system" IT group, Faculty of industrial engineering K.N.Toosi University of technology Tehran, Iran.

[6] Ian Blake, Kumar Murty and Guangwu Xu, "ARefinements of Miller's Algorithm for Computing Weil/Tate Pairing" University of Toronto.

[7] Luther Martin "Identity-Based Encryption : A closer look " ISSA A Global Voice of Information Security ISSA Journal September 2005.

◈◈◈