A FAIR E-TENDERING PROTOCOL

Vijayakrishnan Pasupathinathan, Josef Pieprzyk
ACAC, Department of Computing, Macquarie University, Sydney, Australia
krishnan@ics.mq.edu.au, josef@ics.mq.edu.au

Huaxiong Wang
Division of Mathematical Sciences, Nanyang Technological University, Singapore
HXWang@ntu.edu.sg

Keywords: e-tendering, e-procurement, fairness, anonymous token system.

Abstract: Fairness in electronic tendering is of utmost importance. Current proposals and implementations do not provide fairness and are vulnerable to collusion and favouritism. Dishonest participants, either the principal or tenderer can collude to alter or view competing tenders which would give the favoured tenderer a greater chance of winning the contract. This paper proposes an e-tendering system that is secure and fair to all participants. We employ the techniques of anonymous token system along with signed commitment approach to achieve a publicly verifiable fair e-tendering protocol. We also provide a analysis that confirms that our e-tendering protocol achieves the claimed security goals.

1 INTRODUCTION

Procurement is acquisition of works, supplies or services by public bodies, and tendering is considered one of the fairest means of awarding contracts to obtain such services. Electronic procurement has received considerable attention from governments (Public Works Canada, 2008; Inst. Info. Industry, 1998; NSW Government, 2008), because of obvious cost savings that are obtained by automating tendering and payment processes with electronic tools. Although this interest from government have led to development of various commercial and non-commercial e-tendering systems around the world, only parts of e-tendering process have been successfully deployed. In (Head, 2003), John Barnard refers to discrepancy in usage of e-tendering scheme. He observed that, although more than 75% of tenders are electronically advertised, less than 40% provide electronic documentation required by the tender process and less than 20% make electronic tender submissions.

This may in part be explained, by concerns regarding security, and availability of resources to help with e-tender submission and review. Many e-tendering security concerns are similar to other electronic commerce systems and they normally relate to inadequate guarantees for confidentiality, authentication and non-repudiation. But, the prime security issue, that has been the main obstacle in a wide adoption of e-tendering, is the lack of fairness of the e-tendering process. A secure e-tendering solution should support both fairness and transparency in order to guarantee tenderers to see progress of their submission processing. It is also important that when disputes arise, an e-tendering system should be able to provide a full history of the events leading up to contract award which can be publicly verified without compromising confidentiality or privacy.

RELATED WORK. Most studies related to e-procurement have mainly been in the field of electronic contracting and did not address security issues that are unique to e-tendering. The evident gap in the literature prompted Du *et al.* (Du et al., 2004b; Du et al., 2005) and Betts *et al.* (Betts et al., 2006) to define some of the security requirements for an e-tendering system and later to propose a submission protocol (Du et al., 2004a). Though, these studies addresses some important security requirements that new and existing e-tendering systems should satisfy, they do not address the issues concerning the fairness and transparency of the e-tendering process. An essential ingredient to provide fairness is anonymity of an e-tender submission, as anonymity guarantees that

all submitted tenders will be treated in the same unbiased way. Also, because of the legal status of awarded tenders, it is also essential for an e-tendering system to provide good auditing and public verification of tender award process that also meets evidentiary requirements in courts of law.

This paper addresses the issue of providing anonymity to an e-tender submission. We define fairness and provide the necessary constructs to achieve fairness in an e-tendering system. We also provide a complete set of security requirements and present an e-tendering system that satisfies those requirements.

ORGANISATION. Section 2 provides a overview of main components in an e-tendering system and defines its security requirements. In Section 3 we describe our proposal for a secure e-tendering system. We make a security analysis of our proposed system in Section 4, and finally conclude in Section 5.

2 BACKGROUND AND SECURITY REQUIREMENTS

Current e-tendering systems attempt to mirror the traditional tendering system. The main parties in an e-tendering system are the principal and the tenderers. The principal advertises tender requests and accepts submissions from tenderers. On receiving the submissions the principal performs tender evaluations and selects the winning tender. Many of the current e-tendering systems have been implemented on the assumption that tendering systems are similar to auction systems. In the next section we first highlight the main differences between an auction and tendering systems, we then provide an overview of a generic e-tendering system and the remaining of the section we summarise the main security goals that should be satisfied when designing an e-tendering system.

2.1 E-tendering vs. Auction Systems

Though tendering systems do share some of the properties of auction systems, there are some security considerations that are different. We also evaluate selected seal-bid auction protocols proposed in the literature as they enforce privacy of competitor bids.

There are a variety of auction systems such as *English, Vickery, Sealed-Bid, Dutch, Sealed-Double* etc. , and each system has distinctive goals and employ decision strategies depending on its own rules. In a traditional auction system the auctioneer sells the product to a bidder who has placed the highest bid value. Except for sealed-bid auction systems, the biding value generally are not confidential, on the contrary it is made public so as to receive the highest possible bid. This is fundamentally different to an e-tendering scheme where, the tender value should remain secret from other tenderer. In a traditional auction system the bid values are opened by the auctioneer before the auction closing time, whereas in a tendering system, it is important that the principal does not know any tender values before tender submission deadline. If this security consideration is not taken into account, the tendering system is vulnerable to collusion between the principal and its favourite tenderer.

A seal-bid auction system also shares some security properties that are applicable even to an e-tendering system. Particularly, in both an e-tendering system and a seal-bid auction system, there is a need to prevent other system participants accessing a tender (bid) submission. The authors in (Franklin and Reiter, 1996) presented a sealed-bid auction system based on threshold secret sharing of bidding price using verifiable signatures to provide non-repudiation. But their proposal does not protect the privacy of losers and losing bids. To preserve fairness in an e-tendering system it is essential that privacy of even losing tenderers are preserved. In (Cachin, 1999), Cachin proposed an auction system using homomorphic encryption with an hiding assumption and an oblivious third party. But this scheme cannot reveal the winning price but only identifies the winner, and thus is their system is vulnerable to bidder repudiation. In (Juels and Szydlo, 2003) Juels *et al.* proposed an auction system with proxy oblivious transfer. However, the scheme is not publicly verifiable, therefore such auction system when applied to e-tendering compromise the guarantees provided to tenderers. It is essential that transcripts generated in an e-tendering system are publicly verifiable without compromising the privacy of tender submissions or tenderers, as this provides confidence to all parties involved that an e-tendering process is being carried out in a fair and secure manner.

2.2 Security Requirements

Similar to other electronic commerce systems like e-payments, e-auctions etc. , an e-tendering is required to address generic security requirements like confidentiality, integrity, authentication and non-repudiation. As tendering is carried over insecure networks, the e-tendering system should provide communication security which protects information that is sent, between all participants. This is generally achieved by using a strong encryption. It is also essential that an e-tendering system provides strong storage security, as submissions are stored in

a database. Below we provide a definition for fairness that an e-tendering system should satisfy, but we refer the reader to the full version of paper (Pasupathinathan et-al., 2008) for a more detailed analysis on the security requirements in an e-tendering system.

Definition 2.1. *An e-tendering system is fair, if and only if:*

1. *It is impossible for a principal to obtain any information about a submitted tender before the tender submission deadline, or obtain the true identity of a tenderer without participation from either the tenderer or the registrar.*
2. *It is impossible for a corrupt participant to obtain (or issue) a valid tender, or prohibit a honest participant from obtaining a valid contract.*

3 PROTOCOL DESCRIPTION

Our e-tendering system consists of three phases: tenderer registration, tender submission and, wining tenderer trace. The aim of the system is, when a principal announces the winning tender, every participants (including the principal) is convinced that the tendering process was carried out in fair and transparent manner. In this section we first describe our protocol. For this purpose, we combine the techniques of *offline e-cash* (Frankel et al., 1996) by Frankel *et al.* and add *signed commitment* to tenders, using ideas from Pederson (Pedersen, 1991).

3.1 System Setting

The system consists of a principal $\mathcal{P}$, tenderer $\mathcal{T}_i$ (where the index i runs from $1,\ldots,n$) and a trusted third party called registrar $\mathcal{R}$. A suitable prime order subgroup, G of $\mathbb{Z}_p^*$, of order q is chosen, such that $p = 2q+1$ is a large prime and where the discrete logarithm problem is intractable. Suitable generators g, g_1 and g_2 are chosen such that $\log_g g_1$ is not known to any entity. A cryptographically strong hash function $\mathbf{H} : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ is chosen and the tuple $(p,q,g,g_1,\mathbf{H})$ is published.

The public key of the principal $\mathcal{P}$ is, $\mathtt{PK}_{\mathcal{P}} = g^{\mathtt{SK}_{\mathcal{P}}}$, where, $\mathtt{SK}_{\mathcal{P}}$ is the corresponding private key. The public keys of the registrar $\mathcal{R}$ is, $\mathtt{PK}_{\mathcal{R}} = g^{\mathtt{SK}_{\mathcal{R}}}$, $\mathtt{PK}^1_{\mathcal{R}} = g_1^{\mathtt{SK}_{\mathcal{R}}}$, and $\mathtt{PK}^2_{\mathcal{R}} = g_2^{\mathtt{SK}_{\mathcal{R}}}$ and public key of a tenderer $\mathcal{T}_i$ is, $\mathtt{PK}_{\mathcal{T}_i} = g^{\mathtt{SK}_{\mathcal{T}_i}}$. The tenderer also computes $z\prime = (\mathtt{PK}^1_{\mathcal{R}})^{\mathtt{SK}_{\mathcal{T}_i}} \cdot \mathtt{PK}^2_{\mathcal{R}}$

3.1.1 Notations

- $\in_R$, represents the action of choosing uniformly at random.
- $A \rightarrow B$, represents a message being send from entity A to entity B.
- A : represents operations performed by entity A.
- $\stackrel{?}{=}$ and $\stackrel{?}{\neq}$ are the testing operations for equality and non-equality, respectively.
- $\mathtt{SIGN}_k\langle M\rangle$ is the signature operation on message M using key k.

3.2 Registration

During the registration phase a tenderer $\mathcal{T}_i$ identifies himself/herself and presents the tuple $(\mathtt{PK}_{\mathcal{T}_i}, \mathtt{CERT}\langle\mathtt{PK}_{\mathcal{T}_i}\rangle)$ to the registrar and obtains a *restrictive blind signature* (Brands, 1993) on a *pseudonym*. The restrictive blind signature restrict the pseudonym to be of the form $I = (\mathtt{PK}_{\mathcal{T}_i} g_1)^s$. The value of I is formed by the tenderer and never revealed to the registrar. We can express this phase as, *"a tenderer $\mathcal{T}_i$ engages in the registration protocol with the registrar $\mathcal{R}$ using a random value s (known only to $\mathcal{T}_i$) to obtain a restrictive blind signature on the pseudonym I, signed using the registrar secret key $\mathtt{SK}_R$, but where the value of I is known only to $\mathcal{T}_i$"*. The following step are involved in the registration protocol:

1. $\mathcal{R}$: $w \in_R \mathbb{Z}_q$; $a' = g^w$; $b' = (\mathtt{PK}_{\mathcal{T}_i} g_2)^w$
2. $\mathcal{R} \rightarrow \mathcal{T}_i$: a', b'
3. $\mathcal{T}_i$: $s \in_R \mathbb{Z}_q$; $I = (\mathtt{PK}_{\mathcal{T}_i} g_2)^s$; $z = z'^s$;
   $x_1, x_2, u, v \in_R \mathbb{Z}_q$; $B_1 = g_1^{x_1}, B_2 = g_2^{x_2}$; $B = [B_1, B_2]$;
   $a = (a')^u, g^v$; $b = (b')^{su} I^v$; $c = \mathbf{H}(I, B, z, a, b)$;
   $c' = c/u$;
4. $\mathcal{T}_i \rightarrow \mathcal{R}$: c'
5. $\mathcal{R}$: $r' = c' \mathtt{SK}_R + w$
6. $\mathcal{R} \rightarrow \mathcal{T}_i$: r'
7. $\mathcal{T}_i$: $r = r'u + v \mod q$; $g^{r'} \stackrel{?}{=} \mathtt{PK}_{\mathcal{R}}^{c'} a'$;
   $(\mathtt{PK}_{\mathcal{T}_i} g_2)^{r'} \stackrel{?}{=} z'^{c'} b'$

The signature on value $(I,B) = (z,a,b,r)$ satisfies the relations $g^r = \mathtt{PK}_{\mathcal{R}}^{\mathbf{H}(I,B,z,a,b)} a$ and $I^r = z^{\mathbf{H}(I,B,z,a,b)} b$.

3.3 Submission

The submission consists of two sub phases. Phase one involves the tenderer making a commitment to

participate in the tendering process. After the submission deadline has elapsed, phase two begins, during which the tenderer reveals his/her commitment, thus revealing his/her tender details.

Phase One: During this phase the tender identifies himself/herself to the principal and commits on the tender details. $\mathcal{T}_i$ engages in the protocol to convince the principal about the correctness of the pseudonym I. If this phase is successful, then the protocol transcript will contain $I_1 = g_1^{u_1 s}$ and $I_2 = g_2^s$, such that $I = I_1 I_2$. $\mathcal{T}_i$ also creates a hash value m of its tender documents (**M**), and commits this value (m). We shall express this phase as, "*a tenderer $\mathcal{T}_i$ engages in phase one of the submission protocol with the principal $\mathcal{P}$, using $\mathcal{R}-certified$ (I), secret values ($s, \mathtt{SK}_{\mathcal{T}_i}$), and the tender details* **M**, *to generate proof transcripts, which contains the encryption of $\mathcal{T}_i$'s identity under public key of the registrar $\mathtt{PK}_R^2$, and a signed commitment on* **M** *using the secret keys of the tenderer*". The following are the steps involved in phase one of submission protocol:

1. $\mathcal{T}_i : I_1 = g_1^{u_1 s}$; $I_2 = g_2^s$; $m \in_R \mathbb{Z}_q$;
   $D_1 = \mathtt{PK}_{\mathcal{T}_i} g^{\mathtt{PK}_R^2 m}$; $D_2 = g_2^m$;
2. $\mathcal{T}_i \rightarrow \mathcal{P} : I_1, I_2, I, B, (z,a,b,r), D_1, D_2$
3. $\mathcal{P} : I \stackrel{?}{=} I_1 I_2$; $I \stackrel{?}{\neq} 1$; $\mathtt{SIGN}_{\mathtt{PK}_R}\langle (I,B)\rangle \stackrel{?}{=} (z,a,b,r)$;
   $d = \mathbf{H}(I_1, B_1, I_2, B_2, \mathtt{PK}_{\mathcal{P}}, date/time)$;
   $s_0, s_1, s_2 \in_R \mathbb{Z}_q$
   $D = D_1^{s_0} g_2^{s_1} D_2^{s_2}$; $f = (\mathtt{PK}_{\mathcal{R}}^2)^{s_0} g_2^{s_2}$
4. $\mathcal{P} \rightarrow \mathcal{T}_i : d, f, D$
5. $\mathcal{T}_i : V = \mathbf{H}(D^s / f^{ms})$; $r_1 = d(u_1 s) + x_1$; $r_2 = ds + x_2$;
   $m = \mathbf{H}(\mathbf{M}), \alpha, \gamma_1, \gamma_2 \in_R \mathbb{Z}_q^*$;
   $S = g^m g_1^\alpha \mod p$; $T = g^{\gamma_1} g_1^{\gamma_2} \mod p$
   $c = \mathbf{H}(I_1, I_2, S, T)$;
   $s_1 = \gamma_1 - c u_1 s \mod q$; $s_2 = \gamma_2 - cs \mod q$;
   $t_1 = s - mc \mod q$; $t_2 = s - \alpha c \mod q$
6. $\mathcal{T}_i \rightarrow \mathcal{P} : r_1, r_2, S, t_1, t_2, c, V$
7. $\mathcal{P} : V \stackrel{?}{=} \mathbf{H}(I_1^{s_0} I_2^{s_1})$; $g_1^{r_1} \stackrel{?}{=} I_1^d B_1$; $g_2^{r_2} \stackrel{?}{=} I_2^d B_2$;
   $c \stackrel{?}{=} \mathbf{H}(I_1, I_2, S, (SI_1 I_2)^c g^{t_1} g^{t_2} \mod p)$
8. $\mathcal{P} \rightarrow \mathcal{T}_i : \mathtt{SIGN}_{\mathtt{SK}_P}\langle S, t_1, t_2, c, I_1, I_2, g, g_1\rangle$

Phase Two: This phase begins after the submission deadline has passed. The principal contacts the tenderer and request them to provide their tenders corresponding to their commitment in phase one. We shall express this phase as, "*the tenderer $\mathcal{T}_i$ engages in phase two of the submission protocol with the principal $\mathcal{P}$, by revealing the tender details and α, to obtain a proof of tender submission acceptance, signed using the secret key of the principal ($\mathtt{SK}_{\mathcal{P}}$)*".

1. $\mathcal{T}_i \rightarrow \mathcal{P} : \mathbf{M}, \alpha$
2. $\mathcal{P} : m = \mathbf{H}(\mathbf{M})$
   $S = g^m g_1^\alpha$; $s_1 = t_1 + \alpha c \mod q$; $s_2 = t_2 + mc \mod q$;
   $c \stackrel{?}{=} \mathbf{H}(I_1, I_2, S, (I_1 I_2)^c g^{s_1} g_1^{s_2} \mod p)$
3. $\mathcal{P} \rightarrow \mathcal{T}_i : \mathtt{SIGN}_{\mathtt{SK}_{\mathcal{P}}}\langle S, s_1, s_2, c, I_1, I_2\rangle$

When all tenders have been received, the principal begins tender evaluation procedure and announces the winning tender. Note that the anonymity of the winning tenderer *need not* be revoked, but generally in government procurement the identity is made public. To do so, the principal contacts the registrar and perform the trace protocol.

3.4 Trace

The trace protocol is invoked when the principal has announced the winning tender and would like to trace the real identity of the winning tenderer ($\mathtt{PK}_{\mathcal{T}_i}$) that corresponds to the pseudonym I. The trace protocol may also be invoked in case of disputes (such as, no communication from the winning tenderer after announcement of results). We shall express this phase as, "*a principal $\mathcal{P}$ or any judicial authority engages in a trace protocol with $\mathcal{R}$ to obtain the identity $\mathtt{PK}_{\mathcal{T}_i}$ using $R-certified(I)$, and proofs obtained during the submission protocol*".

1. $\mathcal{P} \rightarrow \mathcal{R} : I, B, (z,a,b,r), I_1, I_2, r_1, r_2,$
   S, t_1, t_2, D_1, D_2
2. $\mathcal{R} : I \stackrel{?}{=} I_1 I_2$; $I \stackrel{?}{\neq} 1$;
   $\mathtt{SIGN}_{\mathtt{PK}_R}\langle (I,B)\rangle \stackrel{?}{=} (z,a,b,r)$;
   $d' = \mathbf{H}(I_1, B_1, I_2, B_2, \mathtt{PK}_{\mathcal{P}}, date/time)$;
   $g_1^{r_1} \stackrel{?}{=} I_1^{d'} B_1$; $g_2^{r_2} \stackrel{?}{=} I_2^{d'} B_2$;
   $\mathtt{PK}_{\mathcal{T}_i} = D_1 / D_2^{\mathtt{SK}_{\mathcal{R}}}$
3. $\mathcal{R} \rightarrow \mathcal{P} : \mathtt{SIGN}_{\mathcal{R}}\langle \mathtt{PK}_{\mathcal{T}_i}\rangle$

REMARK: Two cases of disputes can occur in the e-tendering system, (A) the winning tenderer does not respond to a principal's announcement, (B) the winning tender is denied the contract. In the former case, the principal contacts the registrar and runs the trace protocol to obtain the true identity of the winning tenderer and, in the later case, the tenderer needs to contact $\mathcal{R}$ or a judicial authority by producing the signed proof obtained at the end of phase two of the submission protocol and identifies himself/herself using the pseudonym I_1, and proves that the winning tender belongs to him/her.

4 SECURITY ANALYSIS

Theorem 4.1. (Fairness) *The e-tendering system describe in Section 3 is fair.*

In order to prove our proposed system is fair, we have to prove mainly two things (*cf.* Definition 2.1), (A) a principal is unable to obtain any information regarding the tender before tender opening time (tender hiding) or tenderer's details until the principal has made a decision on the tender (anonymity), and (B) a corrupt participant does not gain any advantage. We make use of the following theorems.

Theorem 4.2. (Hiding) *Given the tuple (S,T,t_1,t_2) it is infeasible to determine the value of m. Thereby, the e-tendering system hides the value of m.*

Proof. (Sketch) The commitment scheme belongs to a class of three-pass, honest verifier zero knowledge protocol. The protocol transcripts can be simulated by calculating $T = (SI_1I_2)^c g^{t_1} g^{t_2}$ after choosing S,c,t_1,t_2. As the protocol is zero-knowledge the value of m is hidden from the principal (verifier) until the tender submission time has elapsed. □

Theorem 4.3. (Binding) *If the value of the tuples (S,T,c,t_1,t_2) cannot be altered, then the e-tendering system possesses the properties required for binding to the value of m.*

This theorem follows trivially from the theorem presented by Pedersen (Pedersen, 1991) (Theorem 3.1), which proves that the commitment scheme reveals no information about the value of m and such a commitment scheme can later be opened by revealing the value of m and α.

Theorem 4.4. *If the discrete logarithm problem is hard, a corrupt tenderer who does not know the private keys of a honest tenderer can convince about the commitment to the principal with a probability of $1/2^{|q|}$, where $|q|$ is bit size of q.*

Proof. (Sketch) The proof follows from (Viswanathan et al., 2000), a corrupt tenderer can cheat the principal by guessing the challenge correctly in advance and can form the correct commitment transcript (From Theorem 4.2). If $|q| = log_2 q$, then the number of legal challenges will be of the form $2^{|q|}$. When the principal chooses the challenges at random, the probability that a corrupt tenderer will correctly guess the challenge is $1/2^{|q|}$. □

Theorem 4.5. *If El-Gamal encryption is secure, and the discrete logarithm problem is intractable then, the e-tendering system preserves tenderer anonymity.*

Proof. The proof is by contradiction. Let us assume that the principal can trace the user, *i.e.* given the view of submission protocol, with non-negligible probability η it can compute the true identity of the tenderer. Let us also assume that the principal has access to a polynomial time algorithm $\mathcal{A}$, which on input (g,y), produces an output x such that, $x = log_g\ y$. For the principal (who is the attacker on the protocol) to obtain $\mathtt{PK}_{\mathcal{T}_i}$, has two options. (A) The principal obtains the secret key $\mathtt{SK}_R$ of the registrar, using the algorithm $\mathcal{A}$ with inputs $(g_2, \mathtt{PK}_R^2)$ and therefore can calculate the value of D_1 and D_2, thus can obtain the public key $\mathtt{PK}_{\mathcal{T}_i}$ as in step 2 of the tracing protocol. (B) The principal uses the algorithm $\mathcal{A}$ to solve for the values $(g,I_1),(g,I_2)$ and obtains the value of u_1 and therefore can calculate $\mathtt{PK}_{\mathcal{T}_i}$. Both of these options depend on the existence of a polynomial time algorithm $\mathcal{A}$ that can solve the discrete logarithm problem, which from our assumption, is hard. Therefore, there exists no such algorithm $\mathcal{A}$ which a principal has access to, that can solve the discrete logarithm problem, and thus our e-tendering system preserves tenderer anonymity. □

REMARK 1: The confidentiality of the tender documents is provided by the hiding property, until the tender submission closing time. Since, with an overwhelming probability, only the tenderer can open the commitment values correctly, the scheme provides tenderer-controlled confidentiality. Our current proposal does not address database security as it is outside the scope of this paper, but standard security techniques should be employed to protect the contents of databases used.

REMARK 2: Non-repudiation is provided by the hiding property and tender binding is provided by the *non-transferability property* of the *e-cash scheme* which is dependent on the tenderer. To transfer credentials of a corresponding tender to another entity, the tenderer would need to reveal his/her secret key and the value of s. Thus a sealed tender is bound to the real identity of the tenderer.

5 CONCLUSION

Electronic procurement has seen tremendous growth in recent years and thus, there is a need for a secure and fair system to award contracts. E-tendering has the potential to deliver such as system in a convenient and transparent manner, and also provide confidence to participants and creates a high degree of trust in the process.

The goal of any electronic system trying to achieve what has been traditionally carried out in the brick-and-motor world should be, not only to replicate the requirements of the traditional system but, to improve the system to provide better services. We have proposed an e-tendering system that achieves such a goal. E-tendering systems previously proposed do not adequately address the need for fairness. Our proposal provides a publicly verifiable fair e-tendering system that not only meets all the security requirement of the traditional tendering system, but offers new services such as anonymity and, tendering hiding and binding.

REFERENCES

Angelov, S. and Grefen, P. (2001). B2b eContract handling - a survey of projects, papers and standards. Technical report, University of Twente, The Netherlands.

Betts, M., Black, P., Christensen, S., Dawson, E., Du, R., Duncan, W., Foo, E., and González Nieto, J. (2006). Towards secure and legal e-tendering. In *Special Issue e-Commerce in Construction*, volume 11, pages 89–102. ITcon.

Boulmakoul, A. and Sall, M. (2002). Integrated contract management. In *9th Workshop of HP OpenView University Association Online Conference*.

Brands, S. A. (1993). Untraceable off-line cash in walltes with observers. In *Advances in Cryptology - Crypto'93*, volume 773, pages 302–318. Springer-Verlag.

Cachin, C. (1999). Efficient private bidding and autions with an oblivious third party. *ACM Conference on Computer and Communications Security'99*, pages 120–127.

Du, R., Foo, E., , González Nieto, J., and Boyd, C. (2005). Designing secure e-tendering systems. In *TrustBus'2005*, Lecture Notes in Computer Science, pages 70–79.

Du, R., Foo, E., Boyd, C., and Firzgerald, B. (2004a). Secure communication protocol for preserving e-tendering integrity. In *Fifth Aisa-Pacific Industrial Engineering and Management Systems Conference (APIEMS'2004)*, volume 14, pages 16.1–16.15. Asia-Pacific Industrial Engineering and Management Society.

Du, R., Foo, E., Boyd, C., and Fitzgerald, B. (2004b). Defining security services for electronic tendering. In *The Australasian Information Security Workshop (ASIW2004)*, volume 32 of *Conferences in Research and Practice in Information Technology*, pages 43–52. Australian Computer Society.

Frankel, Y., Tsiounis, Y., and Yung, M. (1996). Indirect discourse proofs: Achieving efficient fair off-line e-cash. In Kim, K., editor, *Advances in Cryptology - ASIACRYPT'96*, number 1163, Berlin. Springer-Verlag.

Franklin, M. and Reiter, M. (1996). The design and implementation of a secure auction service. *IEEE Transactions on Software Engineering*, 22(5):302–312.

Head, B. (2003). Love me e-tender. http://www.theage.com.au/articles/2003/08/18/1061059763517.html.

Insititute for Information Industry (1998). *Report for The Planning of Electric System of Government Procurement*. Public Contruction Commission (Taiwan R. O. C.).

Juels, A. and Szdlo, M. (2003). A two-server, sealed-bid auction protocol. *Financial Cryptography'03*, page 72.

Liao, T. S., Wang, M. T., and Tserng, H. P. (2002). A framework of electronic tendering for government procuremnet: a lesson learned in taiwan. *Automation in Construction*, (11):731–742.

Pasupathinathan, V.,Pieprzyk, J., and Wang, H. (2008). A Fair E-tendering System. http://www.cprotocol.com.

New South Wales Government Australia (2008). NSW government electroic procurement implementation strategy. http://www.cpsc.nsw.gov.au/e-procurement/framework.htm.

Pedersen, T. (1991). Non-interactive and information theoretic secure verifiable secret sharing. In Feigenbaum, J., editor, *Advances in Cryptology - CRYPTO'91*, Lecture Notes in Computer Science. Springer-Verlag.

Public Works and Government Services Canada (2008). MERX: Canada's electronic tendering service. http://www.merx.com/.

Viswanathan, K., Boyd, C., and Dawson, E. (2000). A three phased scheme for seal bid auction system design. In Dawson, E., Clark, A., and Boyd, C., editors, *ACISP'2000*, volume 1841 of *Lecture Notes in Computer Science*, pages 412–426. Springer-Verlag.