Design and Verification of a Secure Electronic Auction Protocol

Srividhya Subramanian

Dept. of Computer and Information Science
The Ohio State University, Columbus, OH 43210-1277
Tel: (614) 292 5813, Fax: (614)-292-2911
E-mail: ssubrama@cis.ohio-state.edu

Abstract

Auctions are an important and common form of commerce today. A difficult aspect of auctions is that the bidder must be present at the site of the auction. This reduces the appeal of auction and restricts the number of people who would otherwise participate in it. An auction over an electronic network is, therefore, an attractive way of conducting business.

In this paper, I first present a protocol for electronic auctions between an anonymous customers and a merchant whose identity is public. Protocol interrruption by involved parties, passive and active attacks by an intruder, and corruption or loss of messages in the network do not cost the merchant or the customer more than some additional computation. Furthermore, under all circumstances, the transaction is either completed (the right amount of money is exchanged for the right goods) or aborted (there is no transfer of money or goods). In other words, the protocol ensures security, atomicity, and privacy in business transactions.

I next develop a logic based on the semantics of BAN-style [4] logic. Using this logic, I prove that the above properties are preserved in the presence of an intruder.

Keywords: Electronic commerce, auction, security, atomicity, privacy, anonymity, verification, validation.

1 Introduction

There is a plethora of information and products already available to us through the World Wide Web or through email. Some of these are electronic commodities such as electronic books, papers, reports, information, typesetting services, ownership titles, share certificates, software, etc. Others are non-electronic goods that are advertised, ordered and paid for electronically. According to a projection by *Business Week*, trade worth 1,650 billion dollars will be conducted over electronic networks by the year 2000.

This growing shift towards electronic marketing can be attributed to certain factors. Electronic transfer of goods and information is easy, fast, efficient, and inexpensive. In addition, electronically advertised goods are more widely available, and easier to search for. The convenience of being able to look up various products, compare prices and features, place orders and pay, all from one's desktop computer, further favors this shift towards electronic marketing.

Auctions are an important and common form of commerce today. In traditional auctions the bidder must be present at the site of the auction. This reduces the appeal of auction and restricts the number of people who would otherwise participate in it. An auction over an electronic network is, therefore, particularly attractive. However, electronic negotiation is very difficult to design [2], and hence, most existing electronic commerce protocols do not handle auctions. When they do, they allow only a very simplified version of auction with no more than one round of bidding [5].

Due to the popularity of electronic auctions, a number of electronic auction houses are already established on the web, such as, Onsale, FirstAuction, ZAuction, Dealdeal, and Ubid. However, these sites are not backed by a fully automated secure electronic negotiation engine.

Several properties have been identified as either required or desirable in protocols for transactions in electronic commerce [1, 11]. These properties are : (i)*Privacy*: No third party should be able to know details about the transaction (payment amount, product details, identity of parties that wish to remain anonymous, etc.) unless it has been part of the product advertisement available to all. (ii)*Anonymity*: Nobody (including the merchant involved in the transaction) should know the true identity of the customer involved. At the least, nobody should be able to trace all transactions made by a customer and create a profile of the customer. (iii)*Security*: Passive or active attacks by an intruder, abnormal termination of the protocol by involved parties, or corruption or loss of message in the network should not cost more than some additional computation to either party. (iv)*Atomicity*: Under all circumstances, the transaction must either go to completion (the right goods are exchanged for the right amount of money) or be aborted (there is no exchange of goods or money). (v)*Low*

Overhead: The cost for each transaction must be low enough to justify transactions involving a small amount of money.

In general, security and atomicity are required for an electronic commerce protocol to be viable. Breach of security or lack of atomicity can lead to loss of money, duplication of money, or transfer of money to a third party. This may have disastrous financial consequences for an individual or an organization, especially if the amount being transferred is large. It is, therefore, very important to ensure security and atomicity of transactions. Privacy, anonymity, and low overhead cost, on the other hand, are desirable features.

In this paper, I first propose a protocol for fully automated electronic auction between anonymous customers and a merchant whose identity is public. This protocol assures all the above mentioned properties: security, atomicity, anonymity, privacy, and low overhead cost. Next, I formally analyze the protocol in the presence of such an intruder to show that atomicity, security, privacy, and anonimity are ensured. I also argue that the protocol is secure in the presence of a more powerful intruder (than modeled in the logic), incurs nominal overhead charges, and can easily be extended to transactions involving non-electronic good.

The rest of the paper is organized as follows. Section 2 outlines the previous work in this area. Section 3 gives models for transaction execution and auction, and notations used in this paper. Section 4 outlines the logic I use for formal analysis of the protocol. Section 5 describes an auction protocol, formally analyzes the protocol for protocol correctness, and proves that the protocol ensures the properties enumerated above. I conclude in Section 6 with pointers to some directions for future research. Appendix A details proofs for the theorems in Section 4.

2 Previous Work

In this section, I briefly discuss some electronic auction protocols and methods of formal verification proposed in recent literature.

2.1 Protocols for Electronic Auctions

While there exist a number of auction sites on the internet, such as, Onsale (www.onsale.com), FirstAuction (www.firstauction.com), ZAuction (www.zauction.com), Dealdeal (www.dealdeal.com), and Ubid (www.ubid.com), that are fully/partially automated, few of them ensure some of the important properties such as security, privacy, anonymity, atomicity, etc. This is due to the inherent difficulties in automated price negotiation [2]. While electronic auctions are complex, they are also equally popular and desirable. Consequently, a lot of research has been done in the area of electronic auctions and particularly in electronic negotiations. Negotiation Support Systems (NSS) is a class of computer software systems geared specifically towards situations requiring negotiations. While these are powerful tools, they require near-constant human input and are far from being fully automated negotiation engines [2]. In [5] a secure and automated auction protocol has been proposed. However, this protocol allows only one round of bidding.

2.2 Methods for Formal Verification

Cryptographic protocols, if designed improperly, may have flaws that make them vulnerable to various security attacks. The use of formal methods to analyze the correctness of cryptographic protocols became prevalent with the development of the BAN logic in 1989 [4]. Since then several papers have been published reporting problems with the BAN logic [10, 12, 13] and several others proposing BAN-style logics that overcome many of these limitations [7, 14].

In analysis using BAN logic, a set of participant's final beliefs is generated from a set of initial assumptions and the protocol steps. If these beliefs satisfy the goal of the protocol, then the protocol is validated. Descendents of the BAN logic have introduced useful concepts such as correctness of the beliefs of the participants, order of the receipt of messages etc. However, the concept of an intruder is rarely included in the logic. Some tools such as model checkers and theorem provers are used to automate the proof process. Sometimes, these tools model an intruder [6]. However, such implementations are not based on formally verified models and their assumptions need to be checked for their correctness. Also, sometimes the tools make assumptions that, though correct in a general situation, may not be applicable to the specific domain of the problem being solved. In this paper, I extend the BAN logic to introduce an intruder who can eavesdrop, intercept messages, decrypt, and store the message components encrypted with keys available to the intruder. The extension of the logic to include attacks where the intruder can introduce fake messages, constructed from previously stored message components, and plain text components, is an interesting future exercise.

3 System Model

An auction involves a set of customers and a single merchant. The merchant must have a product that he is willing to sell for the highest price offered. A round of bidding consists of some customers sending the price they are willing to offer the merchant. The round of bidding is bounded by a cut-off time. At this time, the merchant collects all the offers and computes the highest offer. If no higher offer has been made since the previous round of bidding, the product is sold to the highest bidder and all other customers are notified about the sale. If a higher bid has been made, all customers are notified about this price and another round of bidding starts.

In electronic commerce transactions, these parties may be physically located anywhere. Each party has a computer connected to an electronic network. The parties communicate by sending messages to each other over the network. I assume the existence of some acceptable electronic form of payment such as a credit card number, an electronic coin withdrawn from a bank, or any other electronic entity that does not compromise the customer's privacy or anonymity. I also assume that there are third parties that issue pseudo-identities to the customers. Apart from facilitating anonymity, these third parties are expected to act as collection agencies if their customer does not pay for goods bought at an auction. Third parties have this extra role because, unlike in normal transactions, the customer cannot refuse to buy a product after making the highest bid in an auction. Since third parties are expected to act as collection agencies, they must know the customer's true identity. The customers must trust these third parties not to use a customer's identity or other information the customer reveals to the third party [8, 9].

Notation for Protocol Description

I will use the following notations to describe the protocols throughout the paper.

$\boldsymbol{A}$ stands for the customer, Alice, with public key $\boldsymbol{a}$ and private key $\frac{1}{\boldsymbol{a}}$.
$\boldsymbol{B}$ stands for the merchant, Bob, with public key $\boldsymbol{b}$ and private key $\frac{1}{\boldsymbol{b}}$.
$\boldsymbol{I}$ stands for the intruder, with public key $\boldsymbol{i}$ and private key $\frac{1}{\boldsymbol{i}}$.
$\boldsymbol{T}$ stands for the third party, Tom, with public key $\boldsymbol{t}$ and private key $\frac{1}{\boldsymbol{t}}$.
$\boldsymbol{e}$ and $\boldsymbol{E}$ are encryption keys with corresponding decryption keys $\frac{1}{\boldsymbol{e}}$ and $\frac{1}{\boldsymbol{E}}$

$\boldsymbol{X} \rightarrow \boldsymbol{Y}$: $[\boldsymbol{message}]^{\frac{1}{x}}$ stands for $\boldsymbol{X}$ sends "message" to $\boldsymbol{Y}$ signed with $\boldsymbol{X}$'s private key.

$\boldsymbol{X} \rightarrow \boldsymbol{Y}$: $[\boldsymbol{message}]^{y}$ stands for $\boldsymbol{X}$ sends "message" to $\boldsymbol{Y}$ secured with $\boldsymbol{Y}$'s public key.

4 The Logic for Formal Verification

In order to formally verify various properties of a protocol (e.g., security, atomicity, anonymity, privacy), one must develop a logic. The logic I use in this paper is based on a semantics of BAN logic [3, 4]. In this section, I will state the language (or syntax), the axioms, and the semantics of this logic. I will also develop some theorems that will be used later to analyze the protocol.

4.1 The Language

I distinguish between the following sorts: Principal, Key, Message, and Formula. Formula is subsort of Message. On Formula I have the traditional logical operators: $\wedge$, $\vee$, $\rightarrow$, and $\forall$. I also have the identity operator $=$. Furthermore, I have the following word operators:

- (*,*) : Message $\times$ Message $\longrightarrow$ Message
  (an associative, commutative, idempotent operator for message joining. Thus, if a message $\boldsymbol{Z}$ contains two message components $\boldsymbol{X}$ and $\boldsymbol{Y}$, $\boldsymbol{Z} = (\boldsymbol{X}, \boldsymbol{Y})$.)

- believes : Principal $\times$ Formula $\longrightarrow$ Formula

- once_said : Principal $\times$ Message $\longrightarrow$ Formula

- sees : Principal $\times$ Message $\longrightarrow$ Formula

- possesses : Principal $\times$ Key $\longrightarrow$ Formula

- public_key_of : Key $\times$ Principal $\longrightarrow$ Formula

- private_key_of : Key $\times$ Principal $\longrightarrow$ Formula

- $[*]^*$: Message $\times$ Key $\longrightarrow$ Formula
  (for encryption; intuitively, $[\boldsymbol{X}]^{\boldsymbol{k}}$ denotes $\boldsymbol{X}$ encrypted by $\boldsymbol{k}$)

- rightly_believes : Principal $\times$ Formula $\longrightarrow$ Formula
  Here, P rightly_believes $\varphi := (\boldsymbol{P}$ believes $\varphi)$ $\wedge\varphi$

The word operators have higher precedence than the traditional logical operators, e.g., $\boldsymbol{P}$ believes $\varphi \wedge \psi$ must be interpreted as $(\boldsymbol{P}$ believes $\varphi)$ $\wedge\psi$

4.2 Axiomatization

The axioms of my logic include the standard axioms of equational logic with modus ponens and the standard rule for universal quantification. Furthermore, I have:

1. **Rules of concatenation :** For message joining there are axioms of the forms:

$$\vdash (\boldsymbol{X}, (\boldsymbol{Y}, \boldsymbol{Z})) = ((\boldsymbol{X}, \boldsymbol{Y}), \boldsymbol{Z})$$
$$\vdash (\boldsymbol{X}, \boldsymbol{Y}) = (\boldsymbol{Y}, \boldsymbol{X})$$

2. **Rationality :** The rationality rule introduces a collection of axioms, one for each theorem of the logic:

$\vdash \varphi \rightarrow \boldsymbol{P}$ believes φ

3. **Believing Modus Ponens :** Modus Ponens under the believes operator:

$\vdash \boldsymbol{P}$ believes $(\varphi \rightarrow \psi) \rightarrow (\boldsymbol{P}$ believes $\varphi \rightarrow \boldsymbol{P}$ believes $\psi)$

4. **Saying parts of a joint message :** Uttering a joint message implies uttering each of its parts:

$\vdash \boldsymbol{P}$ once_said$(\boldsymbol{X}, \boldsymbol{Y}) \rightarrow \boldsymbol{P}$ once_said $\boldsymbol{X}$

5. **Saying contents of an encrypted message :** Uttering an encrypted message, signed by yourself, while you believe that the key is good, implies uttering the encrypted message:

$\vdash \boldsymbol{P}$ once_said $[\boldsymbol{X}]^{\boldsymbol{k}} \wedge \boldsymbol{k}$ private_key_of $\boldsymbol{P} \rightarrow \boldsymbol{P}$ once_said $\boldsymbol{X}$

6. **Seeing parts of a joint message :** Seeing parts of a joint message means seeing each part of the message separately as well:

$\vdash \boldsymbol{P}$ sees $(\boldsymbol{X},\boldsymbol{Y}) \rightarrow \boldsymbol{P}$ sees $\boldsymbol{X}$

7. **Possessing keys of a seen key statement :** If one sees a key statement, one possesses the key that it mentioned:

$\vdash \boldsymbol{P}$ sees $\boldsymbol{k} \rightarrow \boldsymbol{P}$ posseses $\boldsymbol{k}$

8. **Possessing believed keys :** One can only believe that a certain key is good if possessing the key:

$\vdash \boldsymbol{P}$ believes $\boldsymbol{k}$ public_key_of $\boldsymbol{Q} \rightarrow \boldsymbol{P}$ possesses $\boldsymbol{k}$
$\vdash \boldsymbol{P}$ believes $\boldsymbol{k}$ private_key_of $\boldsymbol{Q} \rightarrow \boldsymbol{P}$ possesses $\boldsymbol{k}$

9. **Decryption :** Seeing an encrypted message while having the key in possession, means seeing the message itself:

$\vdash P \text{ possesses } k \wedge P \text{ sees } [X]^k \rightarrow P \text{ sees } X$

10. **Seeing possessed keys:** If one possesses a key statement, one sees the key:

$\vdash P \text{ posseses } k \rightarrow P \text{ sees } k$

11. **Good key ensures utterer :** A collection of axioms that state that if a key is good, the only ones that use it for encryption are the owners, so if somewhere, someone sees a message that contains a part encrypted with that key, that part must have been said by the key owner who encrypted it:

$\vdash k \text{ private\_key\_of } P \wedge R \text{ sees } [X]^k \rightarrow P \text{ once\_said } X$

4.3 The model

The environment consists of a finite collection of *principals*. The local state of a principal P is defined as the tuple (B_P, O_P, S_P, K_P), with the following intuitive interpretation:

- $\mathcal{B}_P$, the set of formulas that P currently believes;
- $\mathcal{O}_P$, the set of (sub-)messages P once said;
- $\mathcal{S}_P$, the set of messages that P has seen so far;
- $\mathcal{K}_P$, the set of keys P posssesses.

Definition 1 *A global state is a mapping from principals to local states for each principal in the environment. The unqualified term "state" will, from now on, mean a global state.*

Definition 2 *The symbol $\models$ is defined as a relation between a state and a formula where $s \models \phi$ means that in state s formula ϕ holds.*

Definition 3 *The function $cts[*]$ takes a message and delivers a set of messages:*

$$\begin{array}{ll} cts[(X,Y)] & := \{(X,Y) \cup cts[X] \cup cts[Y]\} \\ cts[X^k] & := \{X^k \cup cts[X]\} \\ cts[X] & := X, \text{ otherwise} \end{array}$$

Intuitively $cts[*]$ gives all the components of a message that one could obtain if all decryption keys were available.

4.4 The Semantics

The semantics of the above logic is as follows:

$s \models True$;	
$s \models \phi \wedge \psi$	if $s \models \phi$ and $s \models \psi$;
$s \models (\phi, \psi)$	if $s \models \phi \wedge \psi$;
$s \models \phi \rightarrow \psi$	if $s \models \phi$ implies $s \models \psi$;
$s \models (\forall x : \phi)$	if $s \models \phi[x \leftarrow u]$ holds for all terms u of the appropriate kind not containing unbound variables;
$s \models P$ believes ψ	if $\phi \in \mathcal{B}_P$;
$s \models P$ believes X	if $X \in \mathcal{B}_P$;
$s \models P$ once_said X	if $X \in \mathcal{O}_P$;
$s \models P$ sees X	if $X \in \mathcal{S}_P$;
$s \models P$ Possesses k	if $k \in \mathcal{K}_P$;
$s \models k$ private_key_of P	if for all R, X, and Y such that $[X]^k \in cts[Y]$: $Y \in \mathcal{S}_R$ implies $X \in \mathcal{O}_P$;
$s \models k$ public_key_of P	if for all R : $[X]^k \in \mathcal{S}_R$ implies $X \in \mathcal{S}_P$;

It can be proved that the above logic is sound with respect to the given semantics [3].

4.5 Proving properties of the protocol

Definition 4 *The logic translation of an action a, $\mathcal{T}(a)$ is defined as:*

$$
\begin{array}{lcl}
\mathcal{T}(P \rightarrow Q : X) & := & (P \textit{ once\_said } X \wedge Q \textit{ sees } X \wedge I \textit{ sees } X) \\
 & & \textit{(here, } I \textit{ refers to the intruder)} \\
\mathcal{T}(\emptyset) & := & \emptyset \\
\mathcal{T}(P_1; P_2) & := & \mathcal{T}(P_1) \cup \mathcal{T}(P_2)
\end{array}
$$

Intuitively, $\mathcal{T}(P)$ is the minimal set of predicates required to compute the transition from a state to a new state on execution of a. The new state is given by the set of predicates:

$\{X : \{\mathcal{A} \cup \mathcal{T}(a) \vdash X\}$

Definition 5 *For a collection of predicates $\mathcal{A}$ and a protocol step $a = P \rightarrow Q : X$, the predicate "$\mathcal{A}$ allows a" is defined recursively with respect to the structure of message X:*

$$
\begin{array}{ll}
\mathcal{A} \textit{ allows } P \rightarrow Q : X^k,\, k \in \mathcal{K}_P & := \textit{for some } S\textit{: } \mathcal{A} \textit{ allows } P \rightarrow S : X \\
\mathcal{A} \textit{ allows } P \rightarrow Q : X^k,\, k \notin \mathcal{K}_P & := \mathcal{A} \vdash P \textit{ sees } X^k \\
\mathcal{A} \textit{ allows } P \rightarrow Q : (X, Y) & := \mathcal{A} \textit{ allows } P \rightarrow Q : X \textit{ and } \mathcal{A} \textit{ allows } P \rightarrow Q : Y \\
\mathcal{A} \textit{ allows } P \rightarrow Q : \phi & := \mathcal{A} \vdash P \textit{ believes } \phi \\
\mathcal{A} \textit{ allows } P \rightarrow Q : X & := \textit{True} \textit{ (all other cases)}
\end{array}
$$

Intuitively, $\mathcal{A}$ *allows* a means that action a is a valid action in any state where $\mathcal{A}$ holds. Any action where the message sent is built from plaintext, seen message components and known keys is an allowed action.

Definition 6 *Positive formulas are the least set such that:*

ϕ	*is positive if* $\vdash \phi$*;*
k private_key_of P	*is positive;*
k public_key_of P	*is positive;*
P believes ϕ	*is positive if* ϕ *is positive;*
P sees X	*is positive;*
P once_said X	*is positive;*
$\phi \wedge \psi$	*is positive if* ϕ *is positive and* ψ *is positive;*
$\phi \vee \psi$	*is positive if* ϕ *is positive or* ψ *is positive;*
$(\forall x : \phi)$	*is positive if* $\phi[x \leftarrow u]$ *is positive for all terms* u *of the appropriate kind not containing unbound variables.*
A finite set of formulas $\mathcal{F}$	*is positive if the logical AND of all the formulas in* $\mathcal{F}$ *is positive.*

Intuitively, a *positive formula* is a formula such that if it is $\boldsymbol{True}$ in a state, it remains $\boldsymbol{True}$ after execution of any *allowed* action in that state. Note that formulas where a principal sees or once_said are always positive.

Definition 7 *A specification of a protocol is given by two sets of formulas,* $\mathcal{A}$ *(the assumptions) and* $\mathcal{C}$ *(the conclusions). Protocol* P *satisfies such a specification (notation:* $\{\mathcal{A}\}P\{\mathcal{C}\}$*) when "*$\mathcal{A}$ *holds initially" guarantees that "*$\mathcal{C}$ *holds finally", i.e., after executing* P*.*

Definition 8 *The rectify operation* $\mathcal{R}[*]$ *maps formulas to formulas. In particular, it maps formulas of the form "*P believes ϕ*" to "*P rightly_believes ϕ*". It is defined as follows:*

$\mathcal{R}[P \text{ believes } Q]$	$:= P \text{ rightly\_believes } \phi$
$\mathcal{R}[\phi \wedge \psi]$	$:= \mathcal{R}[\phi] \wedge \mathcal{R}[\psi]$
$\mathcal{R}[\phi \vee \psi]$	$:= \mathcal{R}[\phi] \vee \mathcal{R}[\psi]$
$\mathcal{R}[\phi \rightarrow \psi]$	$:= \mathcal{R}[\phi] \rightarrow \mathcal{R}[\psi]$
$\mathcal{R}[\forall x : \phi]$	$:= (\forall x : \mathcal{R}[\phi])$
$\mathcal{R}[\phi]$	$:= \phi$, *other cases*

The *rectify* operation is important in being able to express statements such as Theorem 1 below.

Theorem 1 *If* $\mathcal{A} \cup \mathcal{T}(P)$ *is positive,* $\mathcal{A}$ *allows* P*, and* $\mathcal{A} \cup \mathcal{T}(P) \vdash C$*, then* $\{\mathcal{R}[\mathcal{A}]\}\ P\ \{\mathcal{R}[\mathcal{C}]\}$*. For a proof, see [3].*

Corollary 1 *If* $\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_{n-1})$ *is positive,* $\mathcal{A}$ *allows* $(P_1;P_2;\ldots;P_{n-1})$*,* $\mathcal{T}(P_n)$ *is positive,* $\mathcal{A} \cup \mathcal{T}(P_1) \cup \mathcal{T}(P_2) \cup \cdots \cup \mathcal{T}(P_{n-1})$ *allows* P_n*, and* $\mathcal{A} \cup \mathcal{T}(P_1) \cup \mathcal{T}(P_2) \cup \cdots \cup \mathcal{T}(P_{n-1}) \vdash C$*, then* $\{\mathcal{R}[\mathcal{A}]\}\ P\ \{\mathcal{R}[\mathcal{C}]\}$*. For a proof, see Appendix A.1.*

Theorem 2 *If* $\mathcal{A} \vdash Y \notin \mathcal{S}_R$, $a = P \to Q : X$, $Y \notin cts[X]$, *and* $\{\mathcal{A}\}a\{\mathcal{C}\}$, *then* $\mathcal{C} \vdash Y \notin \mathcal{S}_R$.
For a proof, see Appendix A.2.

Intuitively, R cannot see a previously unseen message if it is not part of the message(s) transmitted in the system. Here we assume that no decryption keys have been sent as part of the message.

Corollary 2 *If* $\mathcal{A} \vdash k \notin \mathcal{K}_R$, $a = P \to Q : X$, $k \notin cts[X]$, *and* $\{\mathcal{A}\}a\{\mathcal{C}\}$, *then* $\mathcal{C} \vdash k \notin \mathcal{K}_R$.
For a proof, see Appendix A.3.

Intuitively, R cannot aquire a key not sent as a part of the message(s) transmitted in the system. Here again we assume that the message in question contains no decryption keys.

Theorem 3 *If* $\mathcal{A} \vdash Y \notin \mathcal{S}_R$, $a = P \to Q : X^k$, $\mathcal{A} \vdash \frac{1}{k} \notin \mathcal{K}_R$, $Y \neq X^k$, *and* $\{\mathcal{A}\}a\{\mathcal{C}\}$, *then* $\mathcal{C} \vdash Y \notin \mathcal{S}_R$.
For a proof, see Appendix A.4.

Intuitively, R cannot see a previously unseen message if the message(s) transmitted in the system cannot be decrypted by R.

5 A Secure and Atomic Protocol for Electonic Auction Transactions

In this section, I describe a secure and atomic protocol for electronic auction. Using the logic developed in Section 4, I formally show that the protocol is atomic, private, anonymous, and secure in the presence of an intruder who can eavesdrop and intercept messages. I illustrate in Section 5.4 that the protocol is also secure in the presence of an intruder who can introduce fake messages (created from heard components, plain text, and known keys) into the system. I also show that the protocol incurs nominal overhead charges and can easily be adapted for electronic commerce transactions involving non-electronic goods.

5.1 The Auction Protocol

An auction involves a merchant, say Bob, and many customers. An auction can be broken into three stages. In the first stage, Bob advertises his product. In the second stage, the customers bid for the product until no customer wishes to make a higher bid. The highest bidder, say Alice, and the merchant, Bob, now exchange the product and the payment. The important feature of an auction is that once Alice makes the highest bid for a product she must buy it. This aspect of auctions makes it extremely difficult to ensure customer anonymity. How can the customer be forced to honor her bid if her identity is to be kept a secret?

The protocol I present is based on public key cryptography and uses trusted third parties to ensure anonymity.

5.2 The Protocol

Figure 1 illustrates the auction protocol with respect ot the highest bidder, Alice. There may, however, be any number of customers involved until the product is sold to Alice.

$$(1a)\quad B \rightarrow everybody\ :\ [\,product\ description,\ list\ of\ recognized\ third\ parties\,]^{\frac{1}{b}}$$

$$(1b)\quad B \rightarrow everybody\ :\ [\,product\ identifier,\ product^{E}]^{\frac{1}{b}}$$

$$(2a)\quad A \rightarrow B\ :\ [\,message\ (1a),\ a,\ third\ party\ t,\ payment^{e},\ [\,price\,]^{\frac{1}{a}}\,]^{b}$$

$$(2b)\quad B \rightarrow A\ :\ [\,[\,payment^{e}\,]^{\frac{1}{b}},\ [\,price\,]^{\frac{1}{a}}\,]^{a}$$

$$(3)\quad B \rightarrow everybody\ :\ [\,product\ description,\ maximum\ price\ offered\,]^{\frac{1}{b}}$$

$$(4)\quad B \rightarrow everybody\ :\ [\,product\ description,\ sold\ for\ price\,]^{\frac{1}{b}}$$

$$(5)\quad A \rightarrow B\ :\ [\,[\,product\ description,\ sold\ for\ price\,]^{\frac{1}{b}},\ [\,\tfrac{1}{e}\,]^{\frac{1}{a}}\,]^{b}$$

$$(6)\quad B \rightarrow A\ :\ [\,[\,\tfrac{1}{e}\,]^{\frac{1}{a}},\ [\,\tfrac{1}{E}\,]^{\frac{1}{b}}\,]^{a}$$

Figure 1: Auction Protocol between the merchant, Bob, and a representative customer, Alice.

In Step 1, Bob advertises for the product by broadcasting the product description and a list of third parties that he trusts. He also broadcasts the product encrypted with key E. Both messages have the product identifier (may be a part of the product description) to prevent mix-ups with messages regarding sales of other products. Bob signs both messages so that customers can verify that they are from him.

In Step 2, Alice (and other interested customers) responds to the advertisement with a reference to the advertisement, her pseudo-identity (i.e., Alice's public key and name of the third party that issued the public key), price offered, payment encrypted with key e and the signed value of the price offered. Bob can look up the third party's directory to check that Alice's public key is indeed issued by the third party involved. Furthermore, he can verify the message is from Alice by decrypting the signed value of the price offered. Since the message is secured with Bob's public key, only Bob can read it. Bob also acknowledges the receipt of the bid.

Once the time allotted for a round of bidding is over, Bob broadcasts the maximum price offered. This constitutes Step 3. The message is signed by Bob so that the customers can verify that it is from him. Bob can hike the maximum price announced in Step 3. This is an accepted practice in auctioneering. Most auctions have their agents among the bidders. These agents artificially hike the maximum bid, goading other bidders to offer more. This method may also be used to resolve ties between bidders. Step 2 and 3 are repeated till no higher price is offered.

When the no higher bid is made, the product is advertised to be sold for the highest price quoted (Step 4). This announcement is again signed by Bob so that it can be verified that he sent it.

In Step 5, the highest bidder, Alice, responds with the decryption key for her payment. (If she does not respond, Bob approaches the third party with her bid and collects the payment.) Alice encloses the old notice for reference and a signed copy of the decryption key so that Bob can verify that the message is from her.

In Step 6, Bob acknowledges the payment and sends the signed product encryption ke

5.3 Formal Analysis of the Protocol

I now formally analyze the protocol in the presence of an intruder using the logic presented in Section 4.

5.3.1 Initial State

The state of the system at the start of the protocol is given below:

$\mathcal{O}_A = \emptyset$; $\mathcal{O}_B = \emptyset$; $\mathcal{O}_I = \emptyset$;

$\mathcal{S}_A = \emptyset$; $\mathcal{S}_B = \emptyset$; $\mathcal{S}_I = \emptyset$;

$\mathcal{B}_A = \{\phi : \vdash \phi\} \cup \{\ b \ \textsf{public\_key\_of} \ B,\ i \ \textsf{public\_key\_of} \ I,\ a \ \textsf{public\_key\_of} \ A,\ \frac{1}{a} \ \textsf{private\_key\_of} \ a\}$;

$\mathcal{B}_B = \{\phi : \vdash \phi\} \cup \{\ b \ \textsf{public\_key\_of} \ B,\ i \ \textsf{public\_key\_of} \ I,\ \frac{1}{b} \ \textsf{private\_key\_of} \ B\}$;

$\mathcal{B}_I = \{\phi : \vdash \phi\} \cup \{\ b \ \textsf{public\_key\_of} \ B,\ i \ \textsf{public\_key\_of} \ I,\ \frac{1}{i} \ \textsf{private\_key\_of} \ I\}$;

$\mathcal{K}_A = \{\frac{1}{a}, a, b, i\}$;

$\mathcal{K}_B = \{\frac{1}{b}, b, i\}$;

$\mathcal{K}_I = \{\frac{1}{i}, b, i\}$;

5.3.2 Properties

The properties I want to verify are security, anonymity, privacy, and atomicity. These translate logically into:

Security:	$\frac{1}{a} \notin \mathcal{S}_I \wedge \frac{1}{b} \notin \mathcal{S}_I \wedge payment \notin \mathcal{S}_I \wedge product \notin \mathcal{S}_I$ (the intruder must not find out the private keys of the parties involved or get the payment or the product being transacted)
Anonymity, Privacy:	$a \notin \mathcal{S}_I$ (the intruder must also not find out the public key (i.e., psuedonym) that the customer is using for the transaction)
Atomicity:	$(product \in \mathcal{S}_A \wedge payment \in \mathcal{S}_B) \vee$ $(product \notin \mathcal{S}_A \wedge payment \notin \mathcal{S}_B) \vee$ $(product^E \in \mathcal{S}_A \wedge [\,product\ description,\ price\,]^{\frac{1}{a}} \in \mathcal{S}_B \wedge$ $[\,payment^e,\ [\,product\ description,\ price\,]^{\frac{1}{a}}\,]^{\frac{1}{b}} \in \mathcal{S}_A \wedge$ $[\,product\ description,\ sold\ for\ price\,] \in \mathcal{S}_A)$ (the product and payment should have been exchanged or neither the product nor the payment exchanged or the customer must have proof that the encrypted product and the encrypted payment have been exchanged)

5.3.3 Verification

Let $\mathcal{A}$ be the set of assumptions or the initial state I start with (where all the beliefs of principals are true), P the protocol, and $\mathcal{C}$ the properties I want to prove. Since the protocol may be interrupted by either the customer or the merchant failing to send the next message, I must show that $\mathcal{C}$ holds after *every step* of the protocol. That is, if P_n is step n of the protocol, then I must show $\{\mathcal{R}[\mathcal{A}]\}$ $P_1;P_2;\ldots;P_n$ $\{\mathcal{R}[\mathcal{C}]\}$ for every step in the protocol.

Step 1a: $B \rightarrow everybody\ :\ [\,product\ description,\ list\ of\ recognized\ third\ parties\,]^{\frac{1}{b}}$

$$\begin{aligned}\mathcal{T}(P_{1a}) = \quad & B \text{ once\_said } [\,product\ description,\ list\ of\ recognized\ third\ parties\,]^{\frac{1}{b}} \wedge \\ & A \text{ sees } [\,product\ description,\ list\ of\ recognized\ third\ parties\,]^{\frac{1}{b}} \wedge \\ & B \text{ sees } [\,product\ description,\ list\ of\ recognized\ third\ parties\,]^{\frac{1}{b}} \wedge \\ & I \text{ sees } [\,product\ description,\ list\ of\ recognized\ third\ parties\,]^{\frac{1}{b}}\end{aligned}$$

(Since the only principals involved are A, B, and I, $everybody$ is treated as A, B, and I.)

From Definition 6,

$$\mathcal{A} \text{ is } \textit{positive} \tag{1}$$

$$\mathcal{T}(P_{1a}) \text{ is } \textit{positive} \tag{2}$$

From (1) and (2),

$$\mathcal{A} \cup \mathcal{T}(P_{1a}) \text{ is } \textit{positive} \tag{3}$$

From Definition 5,

$$\mathcal{A} \textit{ allows } P_{1a} \tag{4}$$

We know that,

$$\begin{aligned}\mathcal{A} \vdash\ & \tfrac{1}{a} \notin \mathcal{S}_I \wedge \tfrac{1}{b} \notin \mathcal{S}_I \wedge payment \notin \mathcal{S}_I \wedge product \notin \mathcal{S}_I \wedge a \notin \mathcal{S}_I \wedge \\ & product \notin \mathcal{S}_A \wedge payment \notin \mathcal{S}_B\end{aligned} \tag{5}$$

$\frac{1}{a} \notin cts[product\ description,\ list\ of\ recognized\ third\ parties]^{\frac{1}{b}} \wedge$
$\frac{1}{b} \notin cts[product\ description,\ list\ of\ recognized\ third\ parties]^{\frac{1}{b}} \wedge$
$payment \notin cts[product\ description,\ list\ of\ recognized\ third\ parties]^{\frac{1}{b}} \wedge$
$product \notin cts[product\ description,\ list\ of\ recognized\ third\ parties]^{\frac{1}{b}} \wedge$
$a \notin cts[product\ description,\ list\ of\ recognized\ third\ parties]^{\frac{1}{b}}$ (6)

From Theorem 2, (5) and (6) above,

$\mathcal{A} \cup \mathcal{T}(P_{1a}) \vdash \frac{1}{a} \notin \mathcal{S}_I \wedge \frac{1}{b} \notin \mathcal{S}_I \wedge payment \notin \mathcal{S}_I \wedge product \notin \mathcal{S}_I$ (security) (7)

$\mathcal{A} \cup \mathcal{T}(P_{1a}) \vdash a \notin \mathcal{S}_I$ (anonymity, privacy) (8)

$\mathcal{A} \cup \mathcal{T}(P_{1a}) \vdash product \notin \mathcal{S}_A \wedge payment \notin \mathcal{S}_B$ (atomicity) (9)

From (7), (8), and (9),

$\mathcal{A} \cup \mathcal{T}(P_{1a}) \vdash \mathcal{C}$ (10)

From Theorem 1, (1), (2), (4), (10), and the fact that all initial beliefs of all principals are valid,

$\{\mathcal{R}[\mathcal{A}]\}\ P_{1a}\ \{\mathcal{R}[\mathcal{C}]\}$ (11)

Step 1b: $B \rightarrow everybody\ :\ [product\ identifier,\ product^E]^{\frac{1}{b}}$

$$\begin{aligned} \mathcal{T}(P_{1b}) = \quad & B \text{ once\_said } [product\ identifier,\ product^E]^{\frac{1}{b}} \wedge \\ & A \text{ sees } [product\ identifier,\ product^E]^{\frac{1}{b}} \wedge \\ & B \text{ sees } [product\ identifier,\ product^E]^{\frac{1}{b}} \wedge \\ & I \text{ sees } [product\ identifier,\ product^E]^{\frac{1}{b}} \end{aligned}$$

(Since the only principals involved are A, B, and I, $everybody$ is treated as A, B, and I.)

From (3),

$\mathcal{A} \cup \mathcal{T}(P_{1a})$ is *positive* (12)

From Definition 6,

$\mathcal{T}(P_{1b})$ is *positive* (13)

From Definition 5,

$\mathcal{A}$ *allows* P_{1a} (14)

$\mathcal{A} \cup \mathcal{T}(P_{1a})$ *allows* P_{1b} (15)

We know that,

$\mathcal{A} \cup \mathcal{T}(P_{1a}) \vdash \frac{1}{a} \notin \mathcal{S}_I \wedge \frac{1}{b} \notin \mathcal{S}_I \wedge payment \notin \mathcal{S}_I \wedge product \notin \mathcal{S}_I \wedge a \notin \mathcal{S}_I \wedge$
$\quad product \notin \mathcal{S}_A \wedge payment \notin \mathcal{S}_B$ (16)

$\frac{1}{a} \notin cts[product\ identifier,\ product^E]^{\frac{1}{b}} \wedge$
$\frac{1}{b} \notin cts[product\ identifier,\ product^E]^{\frac{1}{b}} \wedge$
$payment \notin cts[product\ identifier,\ product^E]^{\frac{1}{b}} \wedge$
$a \notin cts[product\ identifier,\ product^E]^{\frac{1}{b}}$ (17)

We know from $\boldsymbol{\mathcal{T}(P_{1a}; P_{1b})}$ and Theorem 2,

$\boldsymbol{E \notin S_I \wedge E \notin S_A}$

From Theorem 3, Theorem 2, (16) and (17) above,

$$\mathcal{A} \cup \mathcal{T}(P_{1a}; P_{1b}) \vdash \frac{1}{a} \notin \mathcal{S}_I \wedge \frac{1}{b} \notin \mathcal{S}_I \wedge payment \notin \mathcal{S}_I \wedge product \notin \mathcal{S}_I \text{ (security)} \tag{18}$$

Let $P_{1a}; P_{1b}$ be P_1

$$\mathcal{A} \cup \mathcal{T}(P_1) \vdash a \notin \mathcal{S}_I \text{ (anonymity, privacy)} \tag{19}$$

$$\mathcal{A} \cup \mathcal{T}(P_1) \vdash product \notin \mathcal{S}_A \wedge payment \notin \mathcal{S}_B \text{ (atomicity)} \tag{20}$$

From (18), (19), and (20),

$$\mathcal{A} \cup \mathcal{T}(P_1) \vdash \mathcal{C} \tag{21}$$

From Corollary 1, (12), (13), (14), (15), (21), and the fact that

all initial beliefs of all principals are valid,

$$\{\mathcal{R}[\mathcal{A}]\}\ P_1\ \{\mathcal{R}[\mathcal{C}]\} \tag{22}$$

Step 2a: $A \rightarrow B\ :\ [\,a,\ third\ party\ t,\ price,\ payment^e,\ [\,product\ descriptio,\ price\,]^{\frac{1}{a}}\,]^b$

$$\begin{aligned}\mathcal{T}(P_{2a}) = \quad & A \text{ once\_said } [\,a,\ t,\ price,\ payment^e,\ [\,product\ descriptio,\ price\,]^{\frac{1}{a}}\,]^b \wedge \\ & A \text{ sees } [\,a,\ t,\ price,\ payment^e,\ [\,product\ descriptio,\ price\,]^{\frac{1}{a}}\,]^b \wedge \\ & B \text{ sees } [\,a,\ t,\ price,\ payment^e,\ [\,product\ descriptio,\ price\,]^{\frac{1}{a}}\,]^b \wedge \\ & I \text{ sees } [\,a,\ t,\ price,\ payment^e,\ [\,product\ descriptio,\ price\,]^{\frac{1}{a}}\,]^b\end{aligned}$$

From (12) and (13) and Definition 6,

$$\mathcal{A} \cup \mathcal{T}(P_1) \text{ is } \textit{positive} \tag{23}$$

From (14) and (15),

$$\mathcal{A}\ \textit{allows}\ (P_1) \tag{24}$$

From Definition 6,

$$\mathcal{T}(P_{2a}) \text{ is } \textit{positive.} \tag{25}$$

From $\mathcal{T}(P_{1a})$ above, A sees $product\ description$.

Hence, from Definition 5,

$$\mathcal{A} \cup \mathcal{T}(P_1)\ \textit{allows}\ A \rightarrow B\ :\ [\,product\ description\,]. \tag{26}$$

From (26) and Definition 5,

$\mathcal{A} \cup \mathcal{T}(P_1)\ \textit{allows}\ A \rightarrow B\ :\ [\,a,\ t,\ price,\ payment^e,\ [\,product\ description,\ price\,]^{\frac{1}{a}}\,]^b$

(27)

That is,

$$\mathcal{A} \cup \mathcal{T}(P_1)\ \textit{allows}\ P_{2a} \tag{28}$$

We know that,

$$\mathcal{A} \vdash \frac{1}{b} \notin \mathcal{K}_I \tag{29}$$

$$\frac{1}{b} \notin cts[P_1] \tag{30}$$

From Theorem 2, (29) and (30) above,

$$\mathcal{A} \cup \mathcal{T}(P_1) \vdash \frac{1}{b} \notin \mathcal{K}_I \tag{31}$$

From Theorem 3, (7), (8), (9), and (31) we can conclude,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_{2a}) \vdash \frac{1}{a} \notin \mathcal{S}_I \wedge \frac{1}{b} \notin \mathcal{S}_I \wedge payment \notin \mathcal{S}_I \wedge product \notin \mathcal{S}_I \text{ (security)} \tag{32}$$

$$\mathcal{A} \cup \mathcal{T}(P_1) \vdash a \notin \mathcal{S}_I \text{ (anonymity, privacy)} \tag{33}$$

$$\mathcal{A} \cup \mathcal{T}(P_1;P_{2a}) \vdash product \notin \mathcal{S}_A \wedge payment \notin \mathcal{S}_B \text{ (atomicity)} \tag{34}$$

From (32), (33), and (34) we can conclude that,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_{2a}) \vdash \mathcal{C} \tag{35}$$

From Theorem 1, (23), (24), (25), (28), and (35) we can conclude that,

$$\{\mathcal{R}[\mathcal{A}]\}\ P_1;P_{2a}\ \{\mathcal{R}[\mathcal{C}]\} \tag{36}$$

Note: The statements about $\mathcal{A} \cup \mathcal{T}(P_1)$ are also true about $\mathcal{A} \cup \mathcal{T}(P_1;P_2;P_3)$ as we will see below. Hence, we can reproduce this proof for the situation where P_{2a} is not part of the first bid.

Step 2b: $B \rightarrow A\ :\ [\,[\,payment^e\,]^{\frac{1}{b}},\ [\,product\ description,\ price\,]^{\frac{1}{a}}\,]^a$

$$\begin{aligned}\mathcal{T}(P_{2b}) = \quad & B \text{ once\_said } [\,[\,payment^e\,]^{\frac{1}{b}},\ [\,product\ description,\ price\,]^{\frac{1}{a}}\,]^a \wedge \\ & A \text{ sees } [\,[\,payment^e\,]^{\frac{1}{b}},\ [\,product\ description,\ price\,]^{\frac{1}{a}}\,]^a \wedge \\ & B \text{ sees } [\,[\,payment^e\,]^{\frac{1}{b}},\ [\,product\ description,\ price\,]^{\frac{1}{a}}\,]^a \wedge \\ & I \text{ sees } [\,[\,payment^e\,]^{\frac{1}{b}},\ [\,product\ description,\ price\,]^{\frac{1}{a}}\,]^a\end{aligned}$$

From (23), (25) and Definition 6,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_{2a}) \textit{ positive} \tag{37}$$

From (24) and (28) and Definition 5,

$$\mathcal{A} \textit{ allows } (P_1;P_{2a}) \tag{38}$$

From Definition 6,

$$\mathcal{T}(P_{2b}) \text{ is } \textit{positive.} \tag{39}$$

From $\mathcal{T}(P_{2a})$ above and Axiom 6 and Axiom 9, B sees $[\,product\ description,\ price\,]^{\frac{1}{a}}$ (40)

From Definition 5 and (40),

$$\mathcal{A} \cup \mathcal{T}(P_1;P_{2a}) \textit{ allows } B \rightarrow A\ :\ [\,[\,payment^e\,]^{\frac{1}{b}},\ [\,[\,product\ description,\ price\,]^{\frac{1}{a}}\,]^{\frac{1}{b}}\,]^a$$

That is,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_{2a}) \textit{ allows } P_{2b} \tag{41}$$

We know that,

$$\frac{1}{a} \notin cts[P_1;P_{2a}] \tag{42}$$

$$\mathcal{A} \vdash \tfrac{1}{a} \notin \mathcal{S}_I \tag{43}$$

From Theorem 2, Axiom 10, and (42),

$$\mathcal{A} \cup \mathcal{T}(P_1;P_{2a}) \vdash \tfrac{1}{a} \notin \mathcal{K}_I \tag{44}$$

From Theorem 3, ((44), 32), (32), and (34) ,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_{2a};P_{2b}) \vdash \tfrac{1}{a} \notin \mathcal{S}_I \wedge \tfrac{1}{b} \notin \mathcal{S}_I \wedge payment \notin \mathcal{S}_I \wedge product \notin \mathcal{S}_I \wedge a \notin \mathcal{S}_I \tag{45}$$

From $\mathcal{T}(P_1; P_2)$, Axiom 6, and Axiom 9 we know that,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_{2a};P_{2b}) \vdash E \notin \mathcal{S}_A \wedge e \notin \mathcal{S}_B \tag{46}$$

From (45) and (46), $\mathcal{A} \cup \mathcal{T}(P_1;P_{2a};P_{2b}) \vdash \mathcal{C}$ (47)

From (37), (38), (39),(41), (47), and Theorem 1, we can conclude that,

$$\{\mathcal{R}[\mathcal{A}]\}\ P_1;P_{2a};P_{2b}\ \{\mathcal{R}[\mathcal{C}]\} \tag{48}$$

Step 3: $B \rightarrow everybody\ :\ [product\ description,\ sold\ for\ price]^{\frac{1}{b}}$

$$\begin{aligned}\mathcal{T}(P_3) = \quad & B \text{ once\_said } [product\ description,\ sold\ for\ price]^{\frac{1}{b}} \wedge \\ & A \text{ sees } [product\ description,\ sold\ for\ price]^{\frac{1}{b}} \wedge \\ & B \text{ sees } [product\ description,\ sold\ for\ price]^{\frac{1}{b}} \wedge \\ & I \text{ sees } [product\ description,\ sold\ for\ price]^{\frac{1}{b}}\end{aligned}$$

From (37), (39) and Definition 6,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_2)\ \textit{positive} \tag{49}$$

From (38), (41) and Definition 5,

$$\mathcal{A}\ \textit{allows}\ (P_1;P_2) \tag{50}$$

From Definition 6,

$\mathcal{T}(P_3)$ is *positive.* (51)

From Definition 5

$$\mathcal{A} \cup \mathcal{T}(P_1;P_2)\ \textit{allows}\ P_3 \tag{52}$$

We know that,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_2) \vdash \tfrac{1}{a} \notin \mathcal{S}_I \wedge \tfrac{1}{b} \notin \mathcal{S}_I \wedge payment \notin \mathcal{S}_I \wedge product \notin \mathcal{S}_I \wedge a \notin \mathcal{S}_I \wedge$$
$$E \notin \mathcal{S}_A \wedge e \notin \mathcal{S}_B \tag{53}$$

From (53), $\mathcal{A} \cup \mathcal{T}(P_1;P_2;P_3) \vdash \mathcal{C}$ (54)

From (49), (50), (51),(52), (54), and Theorem 1, we can conclude that,

$$\{\mathcal{R}[\mathcal{A}]\}\ P_1;P_{2a};P_3\ \{\mathcal{R}[\mathcal{C}]\} \tag{55}$$

Step 4: $A \rightarrow B\ :\ [product\ description,\ sold\ for\ price]^{\frac{1}{b}}$

$$\begin{aligned}\mathcal{T}(\boldsymbol{P_4}) = \quad & \boldsymbol{A}\ \textsf{once\_said}\ [\,\boldsymbol{product\ description,\ sold\ for\ price}\,]^{\frac{1}{b}} \wedge \\ & \boldsymbol{A}\ \textsf{sees}\ [\,\boldsymbol{product\ description,\ sold\ for\ price}\,]^{\frac{1}{b}} \wedge \\ & \boldsymbol{B}\ \textsf{sees}\ [\,\boldsymbol{product\ description,\ sold\ for\ price}\,]^{\frac{1}{b}} \wedge \\ & \boldsymbol{I}\ \textsf{sees}\ [\,\boldsymbol{product\ description,\ sold\ for\ price}\,]^{\frac{1}{b}}\end{aligned}$$

From (37), (39) and Definition 6,

$\mathcal{A} \cup \mathcal{T}(\boldsymbol{P_1};\boldsymbol{P_2})$ *positive* (56)

From (38), (41) and Definition 5,

$\mathcal{A}$ *allows* $(\boldsymbol{P_1};\boldsymbol{P_2})$ (57)

From Definition 6,

$\mathcal{T}(\boldsymbol{P_4})$ is *positive.* (58)

From Definition 5

$\mathcal{A} \cup \mathcal{T}(\boldsymbol{P_1};\boldsymbol{P_2})$ *allows* $\boldsymbol{P_4}$ (59)

We know that,

$\mathcal{A} \cup \mathcal{T}(\boldsymbol{P_1};\boldsymbol{P_2}) \vdash \frac{1}{a} \notin \mathcal{S}_I \wedge \frac{1}{b} \notin \mathcal{S}_I \wedge \boldsymbol{payment} \notin \mathcal{S}_I \wedge \boldsymbol{product} \notin \mathcal{S}_I \wedge \boldsymbol{a} \notin \mathcal{S}_I \wedge$

$\boldsymbol{E} \notin \mathcal{S}_A \wedge \boldsymbol{e} \notin \mathcal{S}_B$ (60)

From (60) and Theorem 2, $\mathcal{A} \cup \mathcal{T}(\boldsymbol{P_1};\boldsymbol{P_2};\boldsymbol{P_4}) \vdash \mathcal{C}$ (61)

From (56), (57), (58),(59), (61), and Theorem 1, we can conclude that,

$\{\mathcal{R}[\mathcal{A}]\}\ \boldsymbol{P_1};\boldsymbol{P_2};\boldsymbol{P_4}\ \{\mathcal{R}[\mathcal{C}]\}$ (62)

Note: Step 4 follows Step 2. Multiple cycles of Step 3 followed by Step 2 may have occured - but all the statements we make about $\mathcal{A} \cup \mathcal{T}(\boldsymbol{P_1};\boldsymbol{P_2})$ are also true about $\mathcal{A} \cup \mathcal{T}(\boldsymbol{P_1};\boldsymbol{P_2};\boldsymbol{P_3};\boldsymbol{P_2})$. Hence the proof can be reproduced for goods not sold at the first bid.

Step 5: $\boldsymbol{A} \rightarrow \boldsymbol{B}\ :\ [\,[\,\boldsymbol{product\ description,\ sold\ for\ price}\,]^{\frac{1}{b}},\ [\,\frac{1}{e}\,]^{\frac{1}{a}}\,]$

$$\begin{aligned}\mathcal{T}(\boldsymbol{P_5}) = \quad & \boldsymbol{A}\ \textsf{once\_said}\ [\,[\,\boldsymbol{product\ description,\ sold\ for\ price}\,]^{\frac{1}{b}},\ [\,\tfrac{1}{e}\,]^{\frac{1}{a}}\,] \wedge \\ & \boldsymbol{A}\ \textsf{sees}\ [\,[\,\boldsymbol{product\ description,\ sold\ for\ price}\,]^{\frac{1}{b}},\ [\,\tfrac{1}{e}\,]^{\frac{1}{a}}\,] \wedge \\ & \boldsymbol{B}\ \textsf{sees}\ [\,[\,\boldsymbol{product\ description,\ sold\ for\ price}\,]^{\frac{1}{b}},\ [\,\tfrac{1}{e}\,]^{\frac{1}{a}}\,] \wedge \\ & \boldsymbol{I}\ \textsf{sees}\ [\,[\,\boldsymbol{product\ description,\ sold\ for\ price}\,]^{\frac{1}{b}},\ [\,\tfrac{1}{e}\,]^{\frac{1}{a}}\,]\end{aligned}$$

From (56), (58) and Definition 6,

$\mathcal{A} \cup \mathcal{T}(\boldsymbol{P_1};\boldsymbol{P_2};\boldsymbol{P_4})$ *positive* (63)

From (57), (59) and Definition 5,

$\mathcal{A}$ *allows* $(\boldsymbol{P_1};\boldsymbol{P_2};\boldsymbol{P_4})$ (64)

From Definition 6,

$\mathcal{T}(\boldsymbol{P_5})$ is *positive.* (65)

From Definition 5

$$\mathcal{A} \cup \mathcal{T}(P_1;P_2;P_4) \ \textit{allows}\ P_5 \tag{66}$$

We know that,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_2;P_4) \vdash \frac{1}{a} \notin \mathcal{S}_I \wedge \frac{1}{b} \notin \mathcal{S}_I \wedge payment \notin \mathcal{S}_I \wedge product \notin \mathcal{S}_I \wedge a \notin \mathcal{S}_I \tag{67}$$

We know from $\mathcal{T}(P_1;P_2;P_4)$,

$product^E \in \mathcal{S}_A \wedge$

$[\,product\ description,\ price\,]^{\frac{1}{a}} \in \mathcal{S}_B \wedge$

$[\,payment^e\ [\,product\ description,\ price\,]^{\frac{1}{a}}\,]^{\frac{1}{b}} \in \mathcal{S}_A \wedge$

$[\,product\ description,\ sold\ for\ price\,] \in \mathcal{S}_A$

From (67), (69) and Theorem 3, $\mathcal{A} \cup \mathcal{T}(P_1;P_2;P_4;P_5) \vdash \mathcal{C}$ (68)

From (63), (64), (65),(66), (68), and Theorem 1, we can conclude that,

$$\{\mathcal{R}[\mathcal{A}]\}\ P_1;P_2;P_4;P_5\ \{\mathcal{R}[\mathcal{C}]\} \tag{69}$$

Note: Step 4 follows Step 2. Multiple cycles of Step 3 followed by Step 2 may have occured - but all the statements we make about $\mathcal{A} \cup \mathcal{T}(P_1;P_2;P_4)$ are also true about $\mathcal{A} \cup \mathcal{T}(P_1;P_2;P_3;P_2;P_4)$. Hence the proof can be reproduced for goods not sold at the first bid.

Step 6: $A \rightarrow B\ :\ [\,[\,product\ description,\ sold\ for\ price\,]^{\frac{1}{b}},\ [\,\frac{1}{e}\,]^{\frac{1}{a}}\,]$

$$\begin{aligned}\mathcal{T}(P_6) = \quad & A \text{ once\_said } [\,[\,product\ description,\ sold\ for\ price\,]^{\frac{1}{b}},\ [\,\tfrac{1}{e}\,]^{\frac{1}{a}}\,] \wedge \\ & A \text{ sees } [\,[\,product\ description,\ sold\ for\ price\,]^{\frac{1}{b}},\ [\,\tfrac{1}{e}\,]^{\frac{1}{a}}\,] \wedge \\ & B \text{ sees } [\,[\,product\ description,\ sold\ for\ price\,]^{\frac{1}{b}},\ [\,\tfrac{1}{e}\,]^{\frac{1}{a}}\,] \wedge \\ & I \text{ sees } [\,[\,product\ description,\ sold\ for\ price\,]^{\frac{1}{b}},\ [\,\tfrac{1}{e}\,]^{\frac{1}{a}}\,]\end{aligned}$$

From (63), (65) and Definition 6,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_2;P_4;P_5)\ \textit{positive} \tag{70}$$

From (64), (66) and Definition 5,

$$\mathcal{A}\ \textit{allows}\ (P_1;P_2;P_4;P_5) \tag{71}$$

From Definition 6,

$\mathcal{T}(P_6)$ is *positive.* (72)

From Definition 5

$$\mathcal{A} \cup \mathcal{T}(P_1;P_2;P_4;P_5)\ \textit{allows}\ P_6 \tag{73}$$

We know that,

$$\mathcal{A} \cup \mathcal{T}(P_1;P_2;P_4;P_5) \vdash \frac{1}{a} \notin \mathcal{S}_I \wedge \frac{1}{b} \notin \mathcal{S}_I \wedge payment \notin \mathcal{S}_I \wedge product \notin \mathcal{S}_I \wedge a \notin \mathcal{S}_I \tag{74}$$

We know from $\mathcal{T}(P_1;P_2;P_4;P_5)$,

$product^E \in \mathcal{S}_A \wedge payment^e \in \mathcal{S}_B \wedge$

$E \in \mathcal{S}_A \wedge e \in \mathcal{S}_B$

Hence,

$$\boldsymbol{product} \in \boldsymbol{\mathcal{S}_A} \wedge \boldsymbol{payment} \in \boldsymbol{\mathcal{S}_B} \tag{75}$$

From (74), (75) and Theorem 3, $\boldsymbol{\mathcal{A}} \cup \boldsymbol{\mathcal{T}}(\boldsymbol{P_1};\boldsymbol{P_2};\boldsymbol{P_4};\boldsymbol{P_5};\boldsymbol{P_6}) \vdash \boldsymbol{\mathcal{C}}$ (76)

From (70), (71), (72),(73), (76), and Theorem 1, we can conclude that,

$$\{\boldsymbol{\mathcal{R}}[\boldsymbol{\mathcal{A}}]\}\ \boldsymbol{P_1};\boldsymbol{P_2};\boldsymbol{P_4};\boldsymbol{P_5};\boldsymbol{P_6}\ \{\boldsymbol{\mathcal{R}}[\boldsymbol{\mathcal{C}}]\} \tag{77}$$

Note: Step 4 follows Step 2. Multiple cycles of Step 3 followed by Step 2 may have occured - but all the statements we make about $\boldsymbol{\mathcal{A}}\cup\boldsymbol{\mathcal{T}}(\boldsymbol{P_1};\boldsymbol{P_2};\boldsymbol{P_4};\boldsymbol{P_5})$ are also true about $\boldsymbol{\mathcal{A}}\cup\boldsymbol{\mathcal{T}}(\boldsymbol{P_1};\boldsymbol{P_2};\ \boldsymbol{P_3};\ \boldsymbol{P_2};\boldsymbol{P_4};\boldsymbol{P_5})$. Hence the proof can be reproduced for goods not sold at the first bid.

5.4 Intelligent Replay Attacks, Cost, and Non-Electronic Goods

In the formal analysis, I did not prove security in the case of intelligent replay attacks. Intelligent replay attacks are attacks where the intruder may also introduce fake messages built from message components the intruder has seen and plain text components. I also did not discuss transactions involving non electronic goods. Next, I discuss these issues briefly.

5.4.1 Intelligent Replay Attacks

Since atleast one component of all messages is signed with the sender's private key, an intruder cannot forge that component. An intruder can try constructing a message with that component replaced from an old message. Again, all messages except for the messages in Step 1a, Step 1b, Step 3, and Step 4, are secured with the intended recepient's public key. Thus, from Theorem 3, we can conclude that the intruder cannot see the signed components except in Step 1a, Step 1b, Step 3, and Step 4. The only attack possible is a plain replay attack where the intruder replays a whole message from an earlier transaction.

Let us first assume that the intruder replays the message in Step 1a and Step 1b from Bob. Alice responds with an encrypted payment. Bob, even if he receives this payment will respond with a note saying he is not selling the product anymore. The intruder cannot acknowledge the payment, since he cannot read and parse Alice's message. The transaction will simply abort. Let us now assume that the intruder responds to an advertisement by Bob, with an old response from Alice. If the response is from an auction for another product, the product description will not match (in the rare case that the same product comes up for auction again the product description can be deliberately changed by adding a nonce). If the response is from a previous bid for the same product, the bid cannot be higher than the highest bid and cannot change the winner of the auction. Since Alice has not sent a new bid, she will ignore Bob's acknowledgement even if she receives it. The intruder cannot acknowledge

Alice's true bid with an old acknowledgement either. As the highest bid must increase after every round, this Step 4 cannot be replayed either. Step 5 is sent only once for a certain product description and cannot also be replayed. Thus, the intruder cannot cause a transaction to occur, or tamper an ongoing transaction between Bob and Alice, by just replaying old messages.

5.4.2 Non-Electronic Goods

With some minor modifications, the protocol can be extended to non-electronic goods. Step 1b is skipped. Then in the Step 6, instead of sending an encryption key for the product, Bob acknowledges receipt of the payment encryption key and sends the product via some other medium (e.g. certified post).

6 Conclusion

In this paper, I presented a secure, atomic protocol for electronic auction transaction execution. I also developed a logic based on the BAN logic that models an intruder who can eavesdrop, intercept, decrypt, and store components of messages encrypted with keys available to the intruder. I formally proved atomicity, security, anonymity, and privacy in the presence of such an intruder. I also showed that our protocol is secure in the presence of intelligent replay attacks where intruders may introduce fake messages composed of previously stored message components, plain text components, and known keys. Furthermore, I showed that our protocol incurs nominal charges and can easily be extended to transactions involving non-electronic goods.

Future areas of interest include extending the logic developed to model a more powerful intruder, extension of the auction protocol to buyers auctions where sellers send bids for the lowest price to the buyer, and extention of the auction protocol to handle multiple identical goods.

References

[1] R. Anderson. Why Cryptosystems Fail. In *Communications of ACM*, volume 37, 1994.

[2] C. Beam, A. Segev, and J. G. Shanthikumar. Electronic Negotiation through Internet-based Auctions. In *CITM working paper 96-WP-1016, Haas School, Berkeley*, 1996.

[3] A. Bleeker and L. Meertens. A Semantics for BAN Logic. In *DIMACS Workshop on Design and Formal Verification of Security Protocols*, 1997.

[4] M. Burrows, M. Abadi, and R. Needham. A Logic of Authentication. In *ACM Transactions on Computer Systems*, 1990.

[5] M. Franklin and M. Reiter. The Design and Implementation of a Secure Auction Service. In *Proceedings of IEEE Symposium on Security and Privacy*, 1995.

[6] F. Germeau and G. Leduc. Model-based Design and Verification of Security Protocols using LOTOS. In *DIMACS Workshop on Design and Formal Verification of Security Protocols*, 1997.

[7] L. Gong, R. Needham, and R. Yahalom. Reasoning about Beliefs in Cryptographic Protocols. In *Proceedings of IEEE Symposium on Research in Security and Privacy*, 1990.

[8] S. Ketchpel. Transaction Protection for Information Buyers and Sellers. In *DAGS95: Electronic Publishing and the Information Superhighway*, 1995. Available at http://robotics.stanford.edu/users/ketchpel/dags4.html.

[9] S. P. Ketchpel and H. Garcia-Molina. Making Trust Explicit in Distributed Commerce Transactions. In *Proceedings of the 16th ICDCS*, 1996.

[10] C. Meadows. Analyzing the Needham-Schroeder Public Key Protocol: A Comparison of Two Approaches. In *Proceedings of ESORICS*, 1996.

[11] B. C. Neuman and G. Medvinsky. Requirements for Network Payment: The NetCheque Perspective. In *Proceedings of IEEE COMPCON'95*, 1995.

[12] E. Snekkenes. Exploring the BAN Approach to Protocol Analysis. In *Proceedings of IEEE Symposium on Research in Security and Privacy*, 1991.

[13] P. Syverson. Adding Time to a Logic of Authentication. In *Proceedings of First ACM Conference on Computer and Communications Security*, 1993.

[14] P. Syverson and P. van Oorschot. On Unifying some Cryptographic Protocol Logics. In *Proceedings of IEEE Symposium on Research in Security and Privacy*, 1994.

A Proofs

A.1 Proof of Corollary 1

Theorem 1 states,

If $\mathcal{A} \cup \mathcal{T}(P)$ is positive, $\mathcal{A}$ *allows* P, and $\mathcal{A} \cup \mathcal{T}(P) \vdash C$, then $\{\mathcal{R}[\mathcal{A}]\}\ P\ \{\mathcal{R}[\mathcal{C}]\}$

Hence, for each step P_n :

If $\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_n)$ is positive, $\mathcal{A}$ *allows* $(P_1;P_2;\ldots;P_n)$, and $\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_n) \vdash C$, then $\{\mathcal{R}[\mathcal{A}]\}\ P\ \{\mathcal{R}[\mathcal{C}]\}$ (78)

From Definition 4 and (78) we get,

If $\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_{n-1}) \cup \mathcal{T}(P_n)$ is positive, $\mathcal{A}$ *allows* $(P_1;P_2;\ldots;P_n)$, and $\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_{n-1}) \cup \mathcal{T}(P_n) \vdash C$, then, $\{\mathcal{R}[\mathcal{A}]\}\ P\ \{\mathcal{R}[\mathcal{C}]\}$ (79)

From Definition 5 and (79) we get,

If $\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_{n-1}) \cup \mathcal{T}(P_n)$ is positive, $\mathcal{A}$ *allows* $(P_1;P_2;\ldots;P_{n-1})$, $\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_{n-1})$ allows P_n, and $\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_{n-1}) \cup \mathcal{T}(P_n) \vdash C$, then, $\{\mathcal{R}[\mathcal{A}]\}\ P\ \{\mathcal{R}[\mathcal{C}]\}$ (80)

From Definition 6 and (80 we get,

If $\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_{n-1})$ is positive,

$\mathcal{T}(P_n)$ is positive,

$\mathcal{A}$ *allows* $(P_1;P_2;\ldots;P_{n-1})$,

$\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_{n-1})$ allows P_n, and

$\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_{n-1}) \cup \mathcal{T}(P_n) \vdash C$, then,

$\{\mathcal{R}[\mathcal{A}]\}\ P\ \{\mathcal{R}[\mathcal{C}]\}$ (81)

From Definition 4 and (81) we get,

If $\mathcal{A} \cup \mathcal{T}(P_1;P_2;\ldots;P_{n-1})$ is positive,

$\mathcal{T}(P_n)$ is positive,

$\mathcal{A}$ *allows*$(P_1;P_2;\ldots;P_{n-1})$,

$\mathcal{A} \cup \mathcal{T}(P_1) \cup \mathcal{T}(P_2) \cup \cdots \cup \mathcal{T}(P_{n-1})$ allows P_n, and

$\mathcal{A} \cup \mathcal{T}(P_1) \cup \mathcal{T}(P_2) \cup \cdots \cup \mathcal{T}(P_{n-1}) \vdash C$, then

$\{\mathcal{R}[\mathcal{A}]\}\ P\ \{\mathcal{R}[\mathcal{C}]\}$ (82)

∎

A.2 Proof of Theorem 2

$\mathcal{A} \cup \mathcal{T}(a) \vdash k \notin \mathcal{S}_P$

$\equiv \mathcal{A} \cup \mathcal{T}(a) \nvdash P \text{ sees } k \wedge$

Let, $\mathcal{A} \cup \mathcal{T}(a) \vdash P \textsf{ sees } k$

Since the only rule of inference is Modus Ponens,

$\exists z : (\mathcal{A} \cup \mathcal{T}(a) \vdash z \rightarrow P \textsf{ sees } Y) \wedge (\mathcal{A} \cup \mathcal{T}(a) \vdash z)$

We can extend this arguement to proof of $z \rightarrow P \textsf{ sees } Y$ and further till we find a suitable expression $z \ni$

$z \in \{\mathcal{A} \cup \mathcal{T}(a)\} \wedge z$ is of the form $(z_1 \rightarrow (z_2 \rightarrow (\ldots (z_n \rightarrow P \textsf{ sees } Y) \ldots)))$

The only candidates for z are Axiom 6 and Axiom 9. Hence,

$\exists X : ((P \textsf{ sees } X) \in \{\mathcal{A} \cup \mathcal{T}(a)\}) \wedge Y \in cts[X]$

We know that if,

$\exists X : ((P \textsf{ sees } X) \in \mathcal{A}) \wedge Y \in cts[X]) \Rightarrow P \textsf{ sees } Y$, then

$\mathcal{A} \vdash P \textsf{ sees } Y$

Since the implication is not true, $\exists X : ((P \textsf{ sees } X) \in \mathcal{T}(a)) \wedge Y \in cts[X]$

We know from Definition 4,

$(P \textsf{ sees } X) \in \mathcal{T}(a))$ only if X is the message transmitted in action a

But we also know that, $Y \notin cts[X]$ where X is the message transmitted in action a

Proof by contradiction. ■

A.3 Proof of Corollary 2

We know that, $\mathcal{A} \not\vdash P \textsf{ possesses } k$

Using Axiom 7, $\mathcal{A} \not\vdash P \textsf{ sees } k$

We know $k \notin cts[X]$, where X is the message transmitted during action a

From Theorem 2,

$\mathcal{A} \cup \mathcal{T}(a) \not\vdash P \textsf{ sees } k$

Using Axiom 10,

$\mathcal{A} \cup \mathcal{T}(a) \not\vdash P \textsf{ possesses } k$

■

A.4 Proof of Theorem 3

$\mathcal{A} \cup \mathcal{T}(a) \vdash Y \notin \mathcal{S}_P$

$\equiv \mathcal{A} \cup \mathcal{T}(a) \not\vdash P \textsf{ sees } Y \wedge$

Let, $\mathcal{A} \cup \mathcal{T}(a) \vdash P \textsf{ sees } Y$

Since the only rule of inference is Modus Ponens,

$\exists z : (\mathcal{A} \cup \mathcal{T}(a) \vdash z \rightarrow P \textsf{ sees } Y) \wedge (\mathcal{A} \cup \mathcal{T}(a) \vdash z)$

We can extend this arguement to proof of $\boldsymbol{z} \rightarrow \boldsymbol{P}$ sees $\boldsymbol{Y}$ and further till we find a suitable expression $\boldsymbol{y} \ni$

$\boldsymbol{y} \in \{\mathcal{A} \cup \mathcal{T}(\boldsymbol{a})\} \wedge \boldsymbol{y}$ is of the form $(\boldsymbol{z_1} \rightarrow (\boldsymbol{z_2} \rightarrow (\ldots(\boldsymbol{z_n} \rightarrow \boldsymbol{P} \text{ sees } \boldsymbol{Y})\ldots)))$

The only candidates for $\boldsymbol{y}$ are Axiom 6 and Axiom 9. Hence,

$\exists \boldsymbol{X} : ((\boldsymbol{P} \text{ sees } \boldsymbol{X}) \in \{\mathcal{A} \cup \mathcal{T}(\boldsymbol{a})\}) \wedge \boldsymbol{Y} \in \boldsymbol{octs}[\boldsymbol{P}, \boldsymbol{X}]$

Here $\boldsymbol{octs}[\boldsymbol{X}]$ is defined as

$\boldsymbol{octs}[\boldsymbol{P}, (\boldsymbol{M}, \boldsymbol{N})] := \boldsymbol{cts}[[(\boldsymbol{M}, \boldsymbol{N})]$

$\boldsymbol{octs}[\boldsymbol{P}, \boldsymbol{M}^{\boldsymbol{k}}] :=$ if $\boldsymbol{P}$ possesses $\boldsymbol{k}$ then $\boldsymbol{M}^{\boldsymbol{k}} \cup \boldsymbol{cts}[\boldsymbol{M}^{\boldsymbol{k}}]$ else $\boldsymbol{M}^{\boldsymbol{k}}$

$\boldsymbol{octs}[\boldsymbol{P}, \boldsymbol{M}] := \boldsymbol{cts}[\boldsymbol{M}]$, otherwise

We know that if,

$(\exists \boldsymbol{X} : ((\boldsymbol{P} \text{ sees } \boldsymbol{X}) \in \mathcal{A}) \wedge \boldsymbol{Y} \in \boldsymbol{cts}[\boldsymbol{X}]) \Rightarrow \boldsymbol{P} \text{ sees } \boldsymbol{Y}$, then

$\mathcal{A} \vdash \boldsymbol{P} \text{ sees } \boldsymbol{Y}$

Since the implication is not true, $\exists \boldsymbol{X} : ((\boldsymbol{P} \text{ sees } \boldsymbol{X}) \in \mathcal{T}(\boldsymbol{a})) \wedge \boldsymbol{Y} \in \boldsymbol{cts}[\boldsymbol{X}]$

We know from Definition 4,

$(\boldsymbol{P} \text{ sees } \boldsymbol{X}) \in \mathcal{T}(\boldsymbol{a}))$ only if $\boldsymbol{X}$ is the message transmitted in action $\boldsymbol{a}$

We know that, $\boldsymbol{octs}[\boldsymbol{P}, \boldsymbol{X}] = \boldsymbol{X}$ where $\boldsymbol{X}$ is the message transmitted in action $\boldsymbol{a}$

Hence, $\boldsymbol{Y} \notin \boldsymbol{octs}[\boldsymbol{P}, \boldsymbol{X}]$

Proof by contradiction. ■