

A Fair and Reliable e-Commerce Model In P2P NetWork

P2P 네트워크상의 공정하고 신뢰성있는
e-Commerce 모델

Advisor: Prof. Kyung Hyune Rhee



A thesis submitted in partial fulfillment of the requirements
for the degree of

Master of Engineering

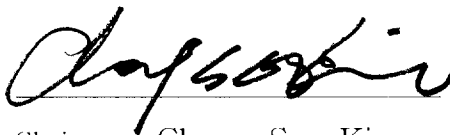
in Department of Information Security, The Graduate School,
Pukyong National University

February 2005

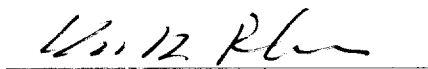
A Fair and Reliable e-Commerce Model
In P2P Network

A dissertation
by
Ji Won Jung

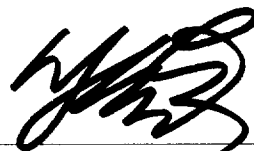
Approved by:



Chairman Chang-Soo Kim



Member Kyung Hyune Rhee



Member Sang Uk Shin

February 25, 2005

Contents

List of Figure	iii
Abstract	iv
Chapter I. Introduction	1
1.1. Background	1
1.2. Main Contributions and Organization of the Thesis	2
Chapter II. Preliminaries	4
2.1. Overview of P2P Network Model	4
2.2. P2P e-Commerce Service and Security Requirements	4
2.3. Cryptographic Tools	7
Chapter III. Fair and Reliable P2P e-Commerce Model	9
3.1. System Architecture and Components	9
3.2. Communication Model and Assumptions	12
3.3. Notations	14
3.4. Membership Enrollment	16
Chapter IV. Optimistic Fair Exchange Protocol with Distributed TTP	19
4.1. Main Protocol	20
4.2. Abort Protocol	23
4.3. Recovery Protocol	25
4.4. Analysis	27
Chapter V. Conclusion	33
References	35

Appendix	37
A. Fair exchange library structure diagram	37
B. Classes's detail relationship	38
C. Buyer peer's sequence diagram	39
D. Seller peer's sequence diagram	39
E. Buyer/Seller's simulation	40

List of Figure

Figure 1. Fair and Reliable P2P e-Commerce Model	9
--	---

P2P 네트워크상의 공정하고 신뢰성있는 e-commerce 모델

정 지 원

부 경 대 학 교 대 학 원 정 보 보 호 학 과

요 약

오늘날 Peer-to-Peer(P2P) 네트워크 패러다임(Paradigms)과 P2P 응용기술은 인터넷과 Mobile Ad-hoc Networks(MANETs)상의 새로운 서비스를 위한 기회를 제공하고 있다. 특히, 모바일 폰과 PDA같은 모바일 장치(Mobile device)는 이미 널리 보급되어 있으며, 이들 장치의 기능과 성능 또한 하루가 다르게 향상되고 있다. 이러한 기술의 급속한 발전으로 인해 모바일 장치들은 원하는 서비스를 요청하는 단계에서 다양한 서비스를 제공하는 능력을 가진 객체로 성장하게 되었으며 모바일 장치를 사용하여 객체들 사이에서 콘텐츠(contents)를 구매/판매하는 새로운 서비스가 P2P 네트워크에 등장하게 되었다. 또한, P2P 네트워크는 각 통신 객체 관리를 위한 어떤 중앙 서버 시스템에도 의존하지 않기 때문에, 본질적으로 확장적인 통신 모델 구현이 가능하므로 통신 객체들 사이에 효과적인 콘텐츠 분산 모델을 제공한다. 그러나 P2P 네트워크에서는 중앙 신뢰 서버의 부재와 객체 사이의 지속적인 연결을 보장하지 못하는 동적인 특성으로 인하여 e-commerce 거래를 위한 공정성(Fairness)과 신뢰성(Reliability)을 보장받기 힘들다.

본 논문에서는 P2P 네트워크에서 디지털 콘텐츠를 구매/판매하는 통신 객체들을 위한 공정하면서도 안전한 e-commerce 모델을 제안한다. 특히, 제안 모델에서는 중앙 서버 시스템인 단일 TTP(Trusted Third Party)에 의존한 기존의 공정한 교환 프로토콜과는 차별화된 분산된 통신 객체들의 협력에 기반하여, 분쟁상황이 발생했을시 분산된 통신 객체들이 협력적인 TTP의 역할을 수행하는 공정한 교환 프로토콜 설계에 초점을 맞춘다. 따라서, 제안 모델은 통신 객체의 관리를 위해 중앙 신뢰 서버에 의존하지 않으므로 P2P 환경에 적합한 모델로 간주되며 차세대 P2P e-commerce 모델의 하나의 본보기가 될 것이다.

Chapter I. Introduction

1.1 Background

Recently Peer-to-Peer (P2P) networking paradigms and its applications offer opportunities for new services over both Internet and Mobile Ad-hoc Networks (MANETs). Specially, mobile devices such as mobile phones and PDAs are already in widespread use, and functionality and performance of these devices are improving day by day. Due to the rapid growth of these technologies, mobile devices are expected to have capability to provide various services beyond the request of desired services. Hence, new services have appeared in P2P network, in which contents are bought and sold among entities by using mobile devices. Moreover, P2P network encourages an efficient contents distribution model among communication entities. Since each communication entity in P2P network does not depend on any central trusted authority for management, it is inherently scalable to implement communication models. Therefore, designing an e-commerce model in P2P network is a promising challenge which we have never met before in the Internet environment.

However, due to the lack of the central trusted authority, P2P network does not efficiently provide all the services required by e-commerce transaction such as reliability and fairness. In particular, guaranteeing *fairness* is a major challenge in an e-commerce model. That is, at the

end of exchange, it must be guaranteed that either each entity has received what it expects to receive or neither entity has received anything useful. Moreover, since the dynamic nature of P2P network implies that the consecutive connectivity between communication entities is not provided, it is more difficult to guarantee fairness for e-commerce transaction in P2P network.

1.2 Main Contributions and Organization of the Thesis

In this thesis we design a new e-commerce model to guarantee fairness and reliability in P2P network, in which communication entities can buy and sell digital contents by P2P contact. Especially, we focus on an optimistic fair exchange protocol based on collaboration with distributed communication entities distinguished from the traditional fair exchange protocol based on the central trusted authority. Moreover, the proposed protocol generally provides desirable property such as availability for P2P e-commerce model since we design the protocol by using threshold cryptography.

This thesis is concerned only with the mechanisms to make peer community fair and reliable. Hence we do not address the specification and the negotiation of peer community security policy.

This thesis is organized as follows. The next Chapter introduces the e-commerce services we have considered and identifies the security

requirements in those e-commerce services, and describes cryptographic tools to induce the motivation of the research. We outline our e-commerce model suitable for P2P network in Chapter 3. A new fair exchange protocol that provides fairness and reliability for the model is presented and analyzed in Chapter 4. Finally, we have conclusions in Chapter 5.

Chapter II. Preliminaries

2.1 Overview of P2P Network Model

A P2P network is any network that does not rely on dedicated servers for communication, but instead mostly uses direct connections between peers. In general, a P2P network model can be classified as pure P2P model(e.g. Gnutella) and hybrid P2P model(e.g. Napster). A pure P2P model does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network. This model of network arrangement differs from the client-server model where communication is usually relayed by the server. As opposed to, a hybrid P2P model utilizes the server-client network structure. A central server maintains directories of contents stored on each node. Each time a client logs on or off the network, the directory is updated. In this model, all control and search messages are sent to the central server.

We allow for a pure P2P network model in order to design our e-commerce model in P2P network.

2.2 P2P e-Commerce Service and Security Requirement

P2P e-commerce service has the following features[3][10].

Services are provided by peers, but any peers may not necessarily

provide the services. Activities in commercial transactions of the services provided by peers are carried out by entities who play both roles of a buyer and a seller, and collaboration among the roles is necessary in commercial transactions. Roles will change dynamically according to the commercial transaction. For example, an entity who performs a buyer role in a commercial transaction might perform a seller role in another transaction.

Also, a peer does not always provide the reliable services since not all of the P2P services are offered by robust central servers. Services among peers are ad-hoc and temporal, and collaboration among peers in P2P commercial transaction is performed under ad-hoc and temporal connection. Consequently, these characteristics result in formidable challenge as far as providing fair and reliable e-commerce service.

The following security requirements are desirable in above P2P e-commerce service:

- Fairness

: No entity should be able to interrupt or corrupt the protocol to force an outcome to her advantage. The protocol should terminate with either each entity having obtained the desired information, or with neither one acquiring anything useful.

- Authentication

: A communication partner is certainly the target partner.

- Confidentiality

: The protocol should not need to disclose the message contents to any other entity excepting the communication entities.

- Non-Repudiation

: It is impossible for a single entity, after the execution of the protocol, to deny having participated in a part or the whole of the communication.

- Integrity

: In the middle of the protocol, an adversary cannot forge a message.

- Effectiveness

: If no messages are lost, both entities behave according to the protocol and do not abandon the exchange, then both entities receive the desired items.

- Timeliness

: It guarantees that both entities will achieve their desired items in the exchange within finite time.

Specially, *fairness* is the most considerable requirement in e-commerce

service. Therefore, it is crucial that a commercial transaction protocol guarantees fairness between communication entities in P2P e-commerce model.

2.3 Cryptographic Tools

2.3.1 Threshold Cryptography

A *threshold cryptography* distributes the ability to provide a cryptographic service such as signing or decryption. In a t out of n threshold scheme, any subset of greater than t peers (out of a total of n peers) can compute the desired functionality while any subset of less than or equal to t peers cannot. It offers better *availability* than non-threshold cryptography: even if some peers are unavailable, others can still perform the desired functionality. Threshold cryptography also provides better security since no single peer is entrusted to perform the desired functionality in its entirety. Consequently, it seems like an ideal choice to provide security services, such as secure, reliable and fair exchange in P2P network.

2.3.2 Fair Exchange Protocol

A *fair exchange protocol* ensures that, at the end of the exchange, either each party receives the item it expects or neither part receives any information about the other's item. The classical solution to the fair

exchange problem is based on the idea of *gradually* exchanging small parts of the items. Works in this approach generally rely on the unrealistic assumption that the two parties have equal computational power or require many rounds to execute properly.

The practical approach to resolve the problem is to use a trusted third party(TTP) as arbitrator. Specifically, this approach can be classified as *on-line* protocol and *optimistic* protocol according to the involvement of TTP[1][11][15]. On-line protocol requires the presence of the TTP as a delivery channel, intervening in each transaction. As the TTP is always involved in every transaction, this protocol considerably implies the communication and computation bottleneck. In optimistic protocol the TTP is not used during the transaction when the communication parties behave correctly, but is involved only in case of disputes with one of the parties. Since the TTP is mostly off-line, this protocol reduces the communication and computation overhead of the TTP.

Chapter III. Fair and Reliable P2P e-Commerce Model

3.1 System Architecture and Components

In this chapter we propose P2P e-commerce model, in which communication entities can buy and sell their products. Figure 1. shows the architecture of the proposed e-commerce model.

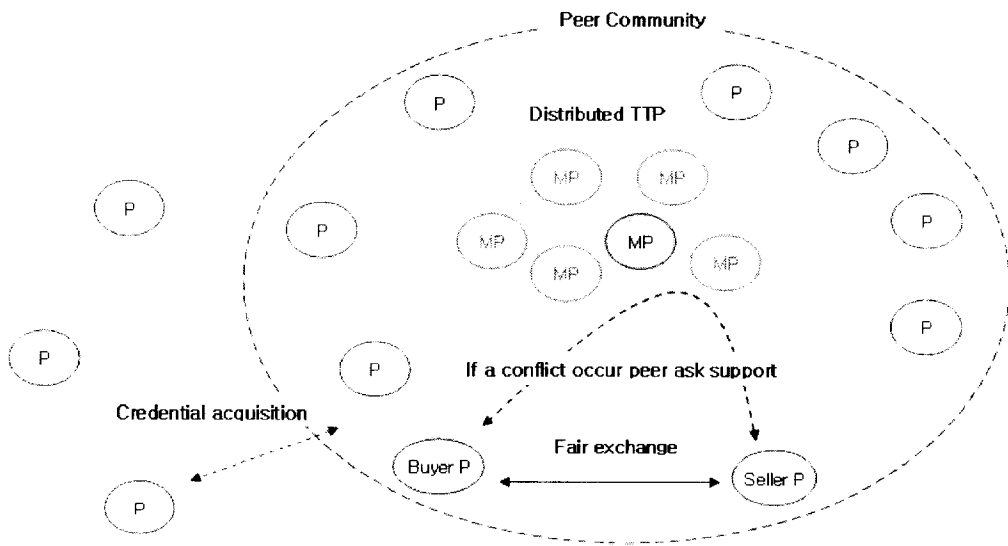


Figure 1. Fair and Reliable P2P e-Commerce Model

The proposed model is consists of peers who play both roles of a seller and buyer, and DTTP(Distributed TTP) which manages the service key of peer community. The description of system components is as follows:

- **Peer**

: An entity who plays either role of a seller or a buyer according to the demand that it desires.

- **DTTP(*Distributed TTP*)**

: DTTP is composed of a set of n special entities ($n \geq 3t+1$) which are called *master peers*(MP), each runs on a separate device in a network. Each master peer has the service secret key share ss_i of peer community and performs the threshold cryptographic operations for assuring fairness and reliability between commercial transaction entities in a peer community.

Additionally we introduce *an adversary* who can easily steal or compromise all entities including master peers. Thus our adversary model includes active(or Byzantine) adversary who can compromise some bounded fraction of entities in the network. However, we assume that fewer than or equal to $1/3$ of the master peers are corrupted or malicious during the entire lifetime of the shared service secret key. This means that at least $2t+1$ master peers are *available* at any time.

For the sake of constituting our P2P e-commerce model, we assume that every peer who wants to participate in the beginning of peer community has already its own standard X.509 public key certificate[9] issued by a recognized Certificate Authority(CA).

In the initial phase, a peer(or peers) wants an e-commerce transaction of its contents constitutes peer community as a virtual market. The high-level description of initialization steps are as follows:

- step1.** To provide the fairness and reliability for e-commerce transaction, master peers are chosen at the constituting peer community. The master peers can be chosen by a peer community founder, or can be the participants at the beginning of peer community.
- step2.** Each master peer MP_i obtains her service secret key share ss_i and service public key from a centralized dealer or by collaborative computation among master peers. For example, the threshold scheme described in [4] provides share distribution by collaboration among master peers, while the threshold scheme presented in [14] supports share distribution by a trusted dealer.
- step3.** Each master peer publishes all identities of master peers and the service public key. After obtaining the identities of master peers and the service public key, an entity who wants to buy or sell its own digital contents performs an e-commerce transaction through peer community.

We assume that an entity who plays the role of seller broadcasts the information of its digital contents to all other entities of the peer community at any time.

Finally, common issues associated with peer community that we should consider are a peer community policy, an advertisement of digital contents and payment mechanisms. However, it remains beyond the scope of this work.

3.2 Communication Model and Assumptions

Generally, according to the definition of *Asokan et al.* in [1], a quality of communication channels can be classified as follows:

Definition 1. *A communication channel between two correctly behaving entities is **operational** if the messages inserted into it by the sender are received by the recipient within a known, constant time interval.*

Definition 2. *A communication channel between two correctly behaving entities is **reliable** if it is guaranteed to be always operational.*

An adversary will not be able to delay any message in a reliable channel.

Definition 3. *A communication channel between two correctly behaving entities is **resilient** if it is normally operational but an adversary can succeed in delaying messages by arbitrary, but finite amount of time.*

In other words, a message inserted into a resilient channel will eventually be delivered.

Definition 4. *A communication channel between two correctly behaving entities is **unreliable** if it has no assumptions about the communication channel between the two entities.*

In other words, a message inserted into a unreliable channel may be lost or modified.

Recent proposed fair exchange protocols[1][2][11][15] assume that communication channel between the entity and the TTP is resilient in order to resolve the dispute, because it is impossible to guarantee fairness between communication entities without at least resilient channel. However, the resilient channel assumption is not sufficient for our model since P2P network implies that no robust central servers are offered and consecutive connectivity is not provided between communication entities including master peers. Therefore, in order to elaborate our system for real P2P networking environment, we employ the idea used in Byzantine environment[6][13]. To implement resilient channel in P2P network, we use the following technique about communication channel between an entity and an available master peer.

- **Fair Communication**

- : A fair communication does not necessarily guarantee the delivery of all message to send, but if no parts of the network become permanently unavailable, given sufficient number of retransmissions,

every message is delivered eventually

Consequently, in our model we assume that communication channel between communication entities who carry out e-commerce transaction is *unreliable* by the nature of P2P network, and that communication channel between an entity and an available master peer is *resilient* by using fair communication. By consideration of the characteristics of P2P network, our qualitatively weaker communication model is reasonable and realistic. Finally we assume that the communication is carried over confidential and broadcast channels.

3.3 Notations

We use the following notations to describe our protocols:

- P_{new} : the identifier of a new peer.
- B, S : the identifiers of buyer and seller, respectively.
- MP_i : the identifier of i -th Master Peer, where $1 \leq i \leq n$.
- INF_X : the information of an entity X . (ex, name, e-mail address, etc)
- f : a flag indicating the purpose of a message.

- $item_X$: an item of an entity X .
- pay_X : a payment information of an entity X .
- $desc_{item_X}, desc_{pay_X}$: the description of the item and the payment of an entity X , respectively.
- t_X : the local timestamp value of an entity X .
- com_X : a randomly chosen commitment value by entity X .
- $DTTP$: a set of Master Peer's identifiers.

$$DTTP : \{ MP_i, \dots, MP_n \}$$

- PH : the protocol header, which contains relevant information such as the identities of the entities involved, the description of the desired item and payment.

$$PH : \{ B, S, DTTP, desc_{item_X}, desc_{pay_X} \}$$

- $H()$: a collision resistant one-way hash function.
- K : a randomly chosen session key for symmetric-key encryption function.
- $E_K()$: a symmetric-key encryption function under session key K .

- $C := E_K(item_X)$: the ciphertext of $item_X$ under session key K .
- $Sig_X()$: a signature function under X 's private key.
- $PE_X()$: an asymmetric-key encryption function under X 's public key.
- $PD_X()$: an asymmetric-key decryption function under X 's private key.
- $X \rightarrow Y : m$: message m is sent from an entity X to an entity Y .
- $X \rightarrow \forall Y_i : m$: message m is broadcasted from an entity X to each entity Y_i , where $1 \leq i \leq n$.
- $\forall X_i \rightarrow Y : m$: message m is sent from each entity X_i to an entity Y , where $1 \leq i \leq n$.

3.4 Membership Enrollment

Here, we describe the membership enrollment protocol used in our e-commerce model. A peer who wants to buy and sell digital contents on peer community needs to charter peer community.

The simplest way to enlist a new member in peer community is to enumerate all potential community members via a public Access Control

List(ACL). However, in a dynamic community, such as P2P network, it is difficult to enumerate all potential members. An alternative way is to appoint a central trusted authority to handle admission procedures. Having a single trusted authority, however, not only violates the characteristics of P2P network, but also introduces a single point of failure and limits scalability.

Therefore, our approach is to admit a new member by collaborative computation among special peers which are called master peers. The detailed steps are as follows:

step 1. A prospective peer who wants to perform e-commerce transaction generates its own public key $PK_{P_{new}}$ and a corresponding private key $SK_{P_{new}}$, and constitutes a membership credential request message to enroll in peer community. This request message contains the prospective peer's identity information, public key and timestamp value $t_{P_{new}}$. Then the prospective peer broadcasts the credential request message to all the master peers.

$$[E-1] P_{new} \rightarrow \forall MP_i : \text{Sig}_{P_{new}}(f_{EnrollReq}, INF_{P_{new}}, t_{P_{new}}, PK_{P_{new}})$$

step 2. Each master peer verifies the received [E-1]. Each MP_i want to approve enrollment of peer community for the prospective peer

and computes a partial signature $Sig_{ss_i}(f_{Enrolled}, INF_{P_{new}}, PK_{P_{new}})$ with its service secret share ss_i . Then these master peers send their confirmation of enrollment to the prospective peer.

$$[E-2] \quad \forall MP_i \rightarrow P_{new} : Sig_{MP_i}(Sig_{ss_i}(f_{Enrolled}, INF_{P_{new}}, PK_{P_{new}}))$$

step 3. To generate a valid membership credential, the prospective peer needs at least $t+1$ correct partial signature. Hence, the prospective peer chooses $t+1$ correct partial signature, and computes the membership credential $Sig_{DTP}(f_{Enrolled}, INF_{P_{new}}, PK_{P_{new}})$. This credential can be used to guarantee admission of peer community.

Chapter IV. Optimistic Fair Exchange Protocol with Distributed TTP

In this chapter we present *an optimistic fair exchange protocol with distributed TTP*, which is used for guaranteeing the fairness and reliability in P2P e-commerce model. In contrast to previously proposed fair exchange protocols [1][2][11][15] that are required the central trusted authority for providing fairness and reliability, our protocol does not require any central trusted authorities since it guarantees the fairness and reliability through collaboration with distributed community entities. Therefore, the proposed protocol is very suitable for P2P e-commerce model.

The proposed protocol is composed of three sub-protocols: *the main protocol*, *the abort protocol*, and *the recovery protocol*. The main protocol consists of messages exchanged directly between buyer and seller. In case of problematic happening during this main protocol, two possibilities are offered to the entities. Either buyer executes the abort protocol in order to cancel the exchange, or buyer(or seller) launches the recovery protocol to complete the exchange.

4.1 Main Protocol

We assume that a buyer has already obtained the description of the desired item and all entities agree on the DTTP to be possibly invoked in case of conflict. When a buyer wishes to receive the desired item from a seller against a payment of the item, the buyer can launch the main protocol. The detailed steps are as follows:

step 1. A buyer who wants to perform e-commerce transaction constitutes the protocol header PH . The buyer also selects a commitment value com_B and timestamp value t_B , then computes $H(pay_B)$, $H(com_B)$, $PE_{DTTP}(pay_B)$. The buyer configures a purchasing message including all above parameters and signs the purchasing message, then sends it to the seller as [M-1].

$$[M-1] \ B \rightarrow S ; \text{Sig}_B(PH, H(pay_B), H(com_B), t_B, PE_{DTTP}(pay_B))$$

step 2. The seller who receives [M-1] checks whether the signature of purchasing message is valid. If the check is invalid, the seller *quits* the exchange. Otherwise the seller constitutes the protocol header \overline{PH} , then chooses a random session key K and

computes $C, H(item_S, K), PE_{DTP}(K)$. The seller forms a selling message and signs the selling message, then sends it to the buyer as [M-2].

$$[M-2] \ S \rightarrow B ; \text{Sig}_S(\overline{PH}, H(item_S, K), C, PE_{DTP}(K))$$

step 3. After having checked the validity of the received message in step 2, the buyer sends pay_B, com_B together with the buyer's signature on those information to the seller as [M-3]. If the validity of [M-2] is not satisfied, or the buyer gives up receiving the [M-2] message, then the buyer runs *the abort protocol*.

$$[M-3] \ B \rightarrow S ; \text{Sig}_B(pay_B, com_B)$$

step 4. The seller checks the validity of [M-3]. If the check is valid, the seller obtains the desired payment information pay_B . The seller sends the session key K to the buyer together with its signature. If any problem occurs in the above process, the seller may *quit* the protocol.

$$[M-4] \ S \rightarrow B ; \text{Sig}_S(K)$$

step 5. After receiving the [M-4] message from the seller, the buyer verifies the signature and obtains the desired item by using the session key K . If the validity of the received message is invalid or the buyer gives up finishing the protocol, then launches *the recovery protocol*.

Remark 1.

- The protocol headers are constituted of both entities PH and \overline{PH} , they contain not only the identities of the involving entities but also the description of the desired item and payment, respectively. Hence, each protocol header has to be checked, by both entities, to confirm the correctness of information relevant to the protocol.
- The use of the commitment com_B , in steps 1 and 3, prevents a malicious seller from launching the recovery protocol without sending the second message to a buyer. Unless receiving commitment com_B , the DTTP does not run the recovery protocol to resolve the conflict.
- Timestamp t_B is used to identify the execution of buyer requests. Timestamps for buyer's requests are totally ordered by the time such that later requests have larger timestamps than earlier ones,

e.g., the timestamp could be the value of the buyer's local clock when the request is issued.

4.2 Abort Protocol

If the seller does not send the second message of the main protocol, the buyer can collaborate with the DTTP in order to abort the protocol. The detailed step is as follows:

step 1. The buyer broadcasts an abort request to all the master peers.

$$[A-1] \quad B \rightarrow \forall MP_i : \text{Sig}_B(f_{\text{AbortReq}}, t_B, [M-1])$$

step 2. Each master peer verifies the received [A-1]. If [A-1] is correct, each master peer computes a partial signature $\text{Sig}_{ss_i}(f_{\text{Aborted}}, t_B, [M-1])$ with its service secret share ss_i . Then all master peers send their abort confirmation to the buyer.

$$[A-2] \quad \forall MP_i \rightarrow B : \text{Sig}_{MP_i}(\text{Sig}_{ss_i}(f_{\text{Aborted}}, t_B, [M-1]))$$

step 3. To generate a valid signature of DTTP, the buyer needs at least $t+1$ correct partial signatures. Hence, the buyer chooses $t+1$ correct partial signatures, and computes an abort token

$Sig_{DTTP}(f_{Aborted}, t_B, [M-1])$. This abort token can be used to guarantee the fairness in case of potential dispute.

Remark 2.

- By using the fair communication, the buyer periodically repeats step 1 until it receives sufficient $[A-2]$ messages as the response to its abort request. In fact, the buyer can try to compute the abort token as soon as it has received $t+1$ partial signatures from master peers. So, the buyer has to wait for more partial signatures only if some partial signatures it received are incorrect.
- Our protocol has been designed by considering the threshold RSA scheme because the threshold scheme based on discrete logarithms may require an agreement upon random number to generate partial signature. Furthermore, the threshold RSA scheme can be applicable to threshold decryption.
- Since the validation of partial signature depends on the underlying threshold scheme, the buyer can check the validation of partial signature by means of applying the threshold RSA schemes that provide the *robustness*[8][14] to our protocol.

4.3 Recovery Protocol

If the seller does not send his final message of the main protocol, the buyer can launch the recovery protocol by means of collaborating with the DTTP, in order to complete the exchange. The detailed steps are as follows:

step 1. The buyer broadcasts the received $[M-1], [M-2]$ and her commitment com_B along with her signature to all the master peers.

$$[R-1] \quad B \rightarrow \forall MP_i : [M-1], [M-2], Sig_B(f_{RecoverReq}, t_B, com_B)$$

step 2. Each master peer checks all the validity of received $[R-1]$. If the check is valid, each master peer performs the following:

- To complete the exchange for the buyer, each master peer generates a partial decryption $PD_{ss_i}(PE_{DTTP}(K))$ of the session key with its service secret share ss_i . Then all master peers send their recovery information to the buyer.

$$[R-2-B] \quad \forall MP_i \rightarrow B : Sig_{MP_i}(f_{Recovered}, t_B, PD_{ss_i}(PE_{DTTP}(K)))$$

- Also, each master peer computes partial decryption $PD_{ss_i}(PE_{DTTP}(pay_B))$ of the payment information with its

service secret share ss_i . Then all master peers send corresponding information to the seller.

$$[R-2-S] \quad \forall MP_i \rightarrow S : [M-1], [M-2],$$

$$Sig_{MP_i}(f_{Recovered}, t_B, PD_{ss_i}(PE_{DTP}(pay_B)), com_B)$$

step 3. Finally, Each buyer and seller perform the following, respectively.

- To generate the session key K , the buyer chooses $t+1$ correct partial decryptions, and computes the session key K . Therefore, the buyer can obtain the desired item by using session key K .
- The seller selects $t+1$ correct partial decryptions, then obtains the desired payment with respect to his item. Then the seller sends $Sig_S(f_{Recovered}, t_B, PD_{ss_i}(PE_{DTP}(pay_B)))$ as acknowledgment of [R-2-S] to all master peers corresponding to the received message.

Remark 3.

- Since the recovery protocol is performed as the abort protocol by using fair communication, the buyer periodically repeats step 1 until it receives sufficient [R-2-B] messages. Also, each master peer who intervenes in the recovery protocol periodically resends their recovery information to the seller until it receives the

acknowledgment of [R-2-S] from the seller.

- Since the seller does not engage in recovery protocol with the DTTP in main protocol, basically the seller need not launch the recovery protocol for assuring fairness. However, the seller is able to recognize the activity of recovery caused by receiving [R-2-S] message when the buyer runs the recovery protocol. Thus, if the seller does not receive sufficient information to generate the desired payment information in desired amount of time, the seller can launch the recovery protocol together with commitment com_B , [M-1], [M-2] within [R-2-S] in order to assure his fairness.

4.4 Analysis

In this section we give an analysis of our protocol, checking the requirements described in Section 2, and then we discuss additional desirable property provided by our protocol. Our claim is as follows:

Claim. *The optimistic fair exchange protocol with distributed TTP above is a fair exchange protocol which provides fairness, timeliness, effectiveness, authentication, confidentiality, integrity, and non-repudiation.*

Sketch. Clearly our protocol provides authentication, non-repudiation, and

integrity through the signature of each communication entity on the messages exchanged and the hash values of $H(\text{pay}_B)$ and $H(\text{item}_S, K)$ in [M-1] and [M-2], respectively. Furthermore, these hash values can be used for potential dispute resolution.

Regarding to confidentiality, it is sufficient to prove that: any master peer which belongs to the DTTP can not open $PE_{DTTP}(\text{pay}_B)$ or $PE_{DTTP}(K)$ while intervening in the exchange. Since any master peer has not entire service secret key, but has service secret key share ss_i through the threshold scheme, it is possible for any master peer to open $PE_{DTTP}(\text{pay}_B)$ or $PE_{DTTP}(K)$ if and only if it must conspire with at least t other master peers.

It is obvious that both entities obtain the expected items, if the main protocol is executed without errors. Therefore, our protocol provides effectiveness.

Before we discuss fairness and timeliness of our protocol, we start with considering the quality of communication channel among participants. In previously presented fair exchange protocols, to prove both fairness and timeliness, the protocols must assume that communication channel between the entity and the TTP is at least resilient. Furthermore, a single TTP is used to guarantee the fairness of the protocol in its entirety. However, communication channel among all the entities is *really unreliable* and *no robust central servers* are offered in P2P network. To overcome the characteristic of P2P network, we applied fair

communication technique to communication channel between the entity and the DTTP. In order that communication channel between the entity and the DTTP is proved eventually resilient by using fair communication, it is sufficient to prove that: an entity who wants to contact the DTTP should eventually receive enough information from any available subset of DTTP needed and stop retransmitting its own requests. Although fair communication can be applied to communication channel between the entity and the TTP, it is difficult to guarantee the fairness of protocol if a single TTP is used. Because a single TTP should become bottleneck and vulnerable to malicious attacks such as denial of service. Furthermore, the existing of robust central servers violates the nature of P2P network. However, our protocol is based on collaboration with distributed communication entities for guaranteeing the fairness by using the threshold cryptography. This feature inherently implies that any single entity is not wholly entrusted to guarantee the desired fairness. Since we have assumed that the entire DTTP contains at least $2t+1$ (out of a total of n peers) *available* master peers at any time, due to availability of DTTP, all entities are able to eventually contact at least $2t+1$ master peers belonging to the DTTP. Thus, the entire DTTP can always provide resilient communication channel by using fair communication technique. This communication model makes our protocol very reasonable and realistic in P2P network such as ad-hoc and temporal.

Now we can prove the fairness and timeliness of our protocol with

above communication model.

Regarding on timeliness, we consider three situations:

- The main protocol ends up successfully without any time-out.
- The buyer aborts the protocol and receives the abort confirmation signed by the DTTP within a time elapse which may be arbitrarily long, yet finite amount of time.
- The buyer(or if necessary, the seller) has the ability to launch the recovery protocol to complete the exchange and eventually receive the desired item in a finite period of time.

Therefore, our protocol provides timeliness.

Finally, we show the fairness of our protocol for both the seller and the buyer, and start with the fairness of seller.

- In main protocol the seller does not basically need to engage in both the abort protocol and the recovery protocol for assuring fairness since the seller sends the session key to the buyer after receiving the desired payment information.
- Also, if the buyer starts the recovery protocol to complete the exchange, the seller can recognize the activity of the recovery. In

this case the seller may receive sufficient information to generate the desired payment information from the DTTP, otherwise he can launch the recovery protocol to complete the exchange.

For the fairness of buyer, we analyze the following cases in which the buyer does not obtain the desired item $item_S$.

- If the seller stops the main protocol after receiving the [M-3] message, the buyer can perform the recovery protocol with collaborating the DTTP in order to compute the session key K . All information sent by the DTTP to the buyer may be eventually arrived in our communication model.
- If the seller does not send the [M-2] message to the buyer, the buyer can start the abort protocol through collaborating with the DTTP in order to obtain the abort token which can be used in case of potential conflict.
- Also, we note that the seller can not perform the recovery protocol without the commitment com_B as discussed in Remark 1. The seller can launch the recovery protocol to complete the exchange if and only if the buyer has previously launched the recovery protocol. So, in this case it will never happen that the seller gains pay_B

while the buyer does not receive $item_S$.

Therefore, our protocol provides fairness.

Finally, our protocol provides additional interesting property that a seller does not basically need to engage in both abort protocol and recovery protocol in order to guarantee its fairness. Therefore, a seller does not need to maintain state information regarding to the transaction in main protocol. This feature makes our protocol more practical in e-commerce environments in which the seller involvement is preferable to the buyer involvement in e-commerce transactions.

Chapter V. Conclusion

Recently by reason of the rapid growth of decentralized technologies, Peer-to-Peer (P2P) networking paradigms and its applications offer opportunities for new services over both Internet and Mobile Ad-hoc Networks (MANETs). Specially, P2P network encourages an efficient contents distribution model among communication entities. Since each communication entity in P2P network does not depend on any central trusted authority, it is inherently scalable to implement communication models. Therefore, a design of an e-commerce model in P2P network is a promising challenge which we have never met before in the Internet environment.

However, P2P network does not provide the central trusted server for managing communication entities and does not guarantee the consecutive connectivity between communication entities. Consequently, these characteristics of P2P network result in formidable challenge as far as providing fair and reliable e-commerce services.

In this thesis we have presented a fair and secure e-commerce model suitable for P2P network, in which communication entities can buy and sell digital contents by P2P contact. In particular, we have proposed and analyzed a new optimistic fair exchange protocol with distributed TTP which is used to guarantee the fairness and reliability for presented P2P e commerce model.

Compared with the traditional fair exchange protocol based on the

central trusted authority, our protocol does not require any central trusted authority. Consequently, our protocol is attractive in P2P networking environment which does not naturally depend upon any central trusted authority for managing communication entities. Therefore, we believe that the proposed e-commerce model will be useful for evolving the next generation e-commerce in P2P network.

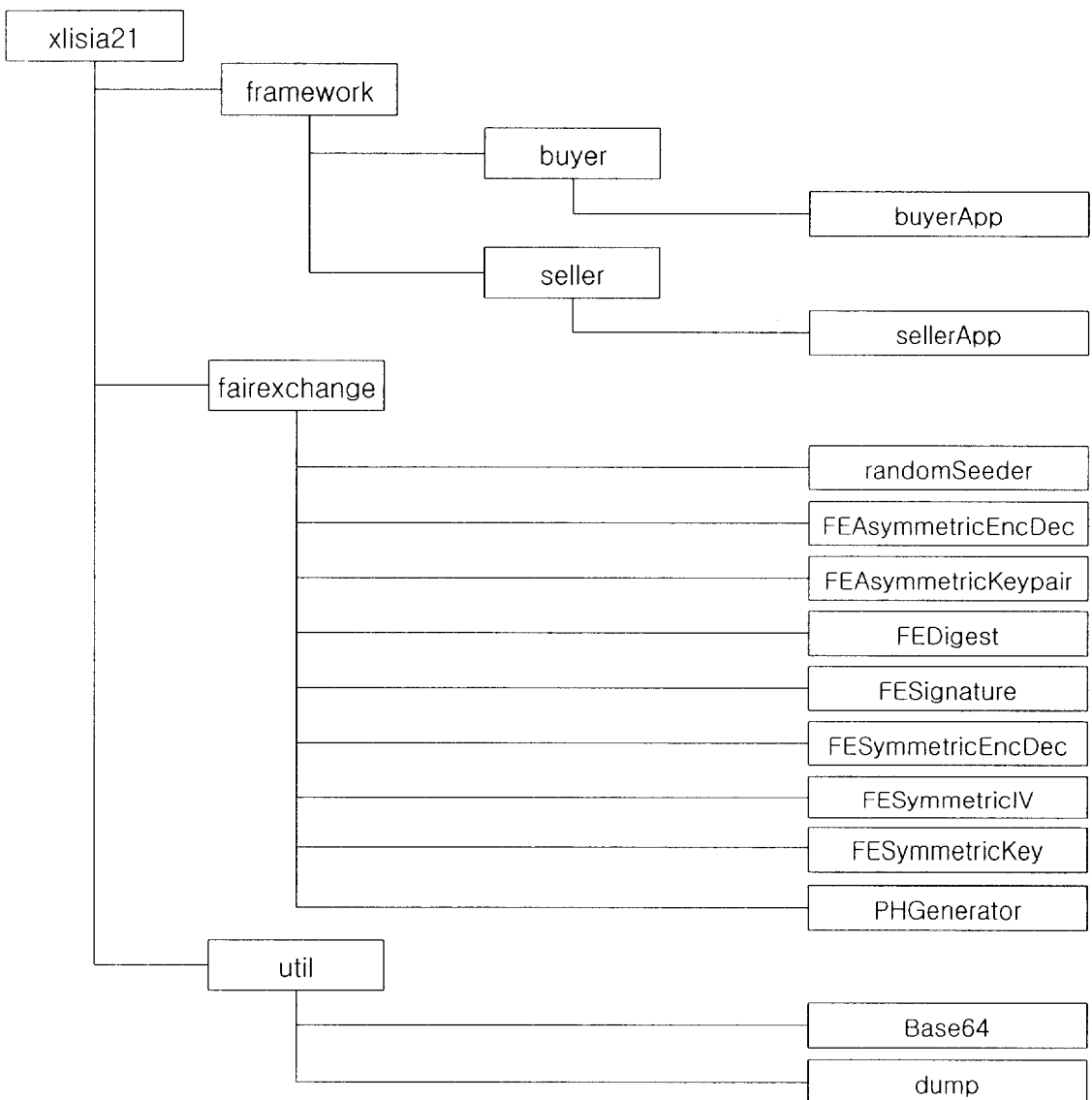
References

- [1] N. Asokan, V. Shoup, and M. Waidner, "*Asynchronous protocols for optimistic fair exchange*", in Proceeding of the IEEE Symposium on Research in Security and Privacy, May 1998.
- [2] N. Asokan, V. Shoup, and M. Waidner, "*Optimistic fair exchange of digital signatures*", In Proc. Eurocrypt'98, LNCS 1403, pp. 591–606, 1998.
- [3] P. Antoniadis, C. Courcoubeits, "*Market models for P2P content distribution*", In Proc. AP2PC'02, 2002.
- [4] D. Boneh, M. Franklin, "*Efficient generation of shared RSA keys*", in Proceedings Crypto'97, pp.425–439, 1997.
- [5] G.T. Byrd, F. Gong, C. Sargor and T.J. Smith, "*Yalta: A Secure Collaborative Space for Dynamic Coalitions*", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, June 2001.
- [6] M. Castro and B. Liskov, "*Practical Byzantine fault tolerance*", in Proc. the 3rd USENIX OSDI'99, pp.173–186, 1999.
- [7] P. Fouque, J. Stern, "*Fully Distributed Threshold RSA under Standard Assumptions*", In Proc. ASIACRYPT 2001, pp. 310–330, 2001.
- [8] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "*Robust and efficient sharing of RSA functions*", In Proc. Crypto'96, LNCS 1109, pp.157–172, 1996.

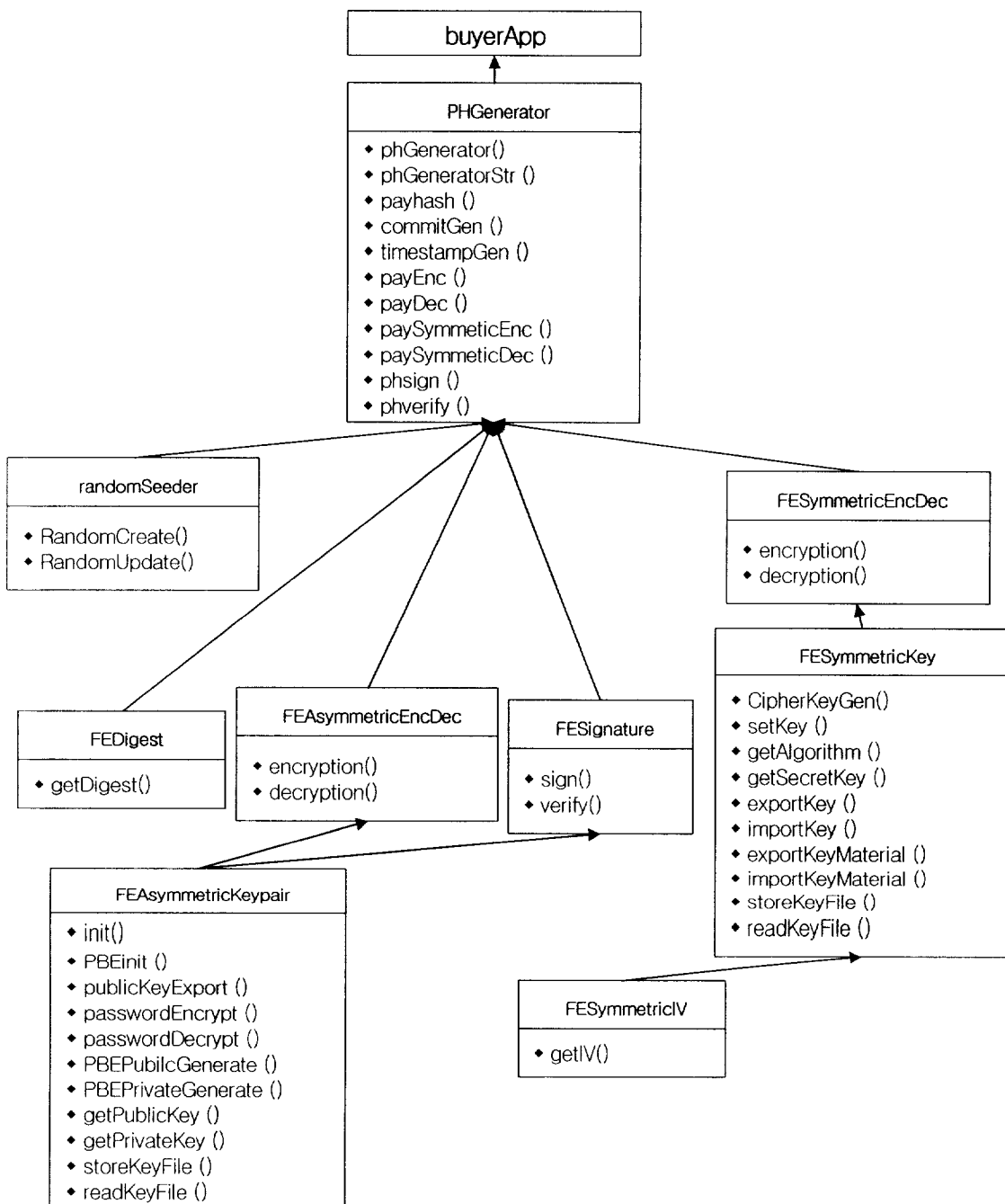
- [9] R. Housley, W. Ford, W. Polk, D. Solo, "*Internet X.509 Public key infrastructure certificate and CRL profile*", RFC 2459. January 1999.
- [10] T. Iwao, Y. Wada, S. Yamasaki, M. Shiouchi, M. Okada, M. Amamiya, "*A Framework for the Next Generation of E-Commerce by Peer-to-Peer Contact*", IEEE WET ICE 2001.
- [11] O. Markowitch and S. Saeednia, "*Optimistic Fair Exchange with Transparent Signature Recovery*", In Proc. Financial Cryptography 2001, LNCS 2339, pp. 339–350, 2002.
- [12] Alfred J. Menezes, Paul C. van Oorshot, Scoot A. Vanstone "*Handbook of Applied Cryptography*", 1997, CRC Press
- [13] Tal Rabin, "*A Simplified Approach to Threshold and Proactive RSA*", In H. Krawczyk, editor, Advances in Cryptology-CRYPTO'98, LNCS 1462, pp. 89–104, 1998.
- [14] Victor Shoup, "*Practical threshold signatures*", In Proc. Eurocrypt 2000, LNCS 1807, pp.207–220, 2000.
- [15] Holger Vogt, "*Asynchronous Optimistic Fair Exchange Based on Revocable Items*", In Proc, Financial Cryptography 2003, LNCS 2851, pp. 193–207, October 2003.
- [16] Lidong Zhou, Zygmunt J. Haas, "*Securing Ad Hoc Networks*", IEEE Network Magazine, 13(6), 1999.

Appendix

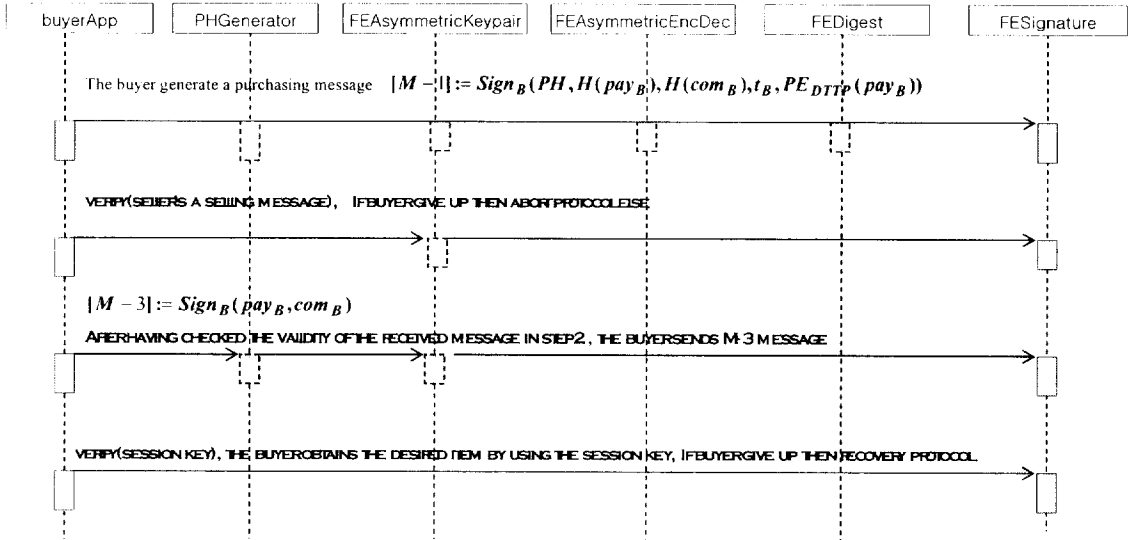
A. Fair exchange library structure diagram



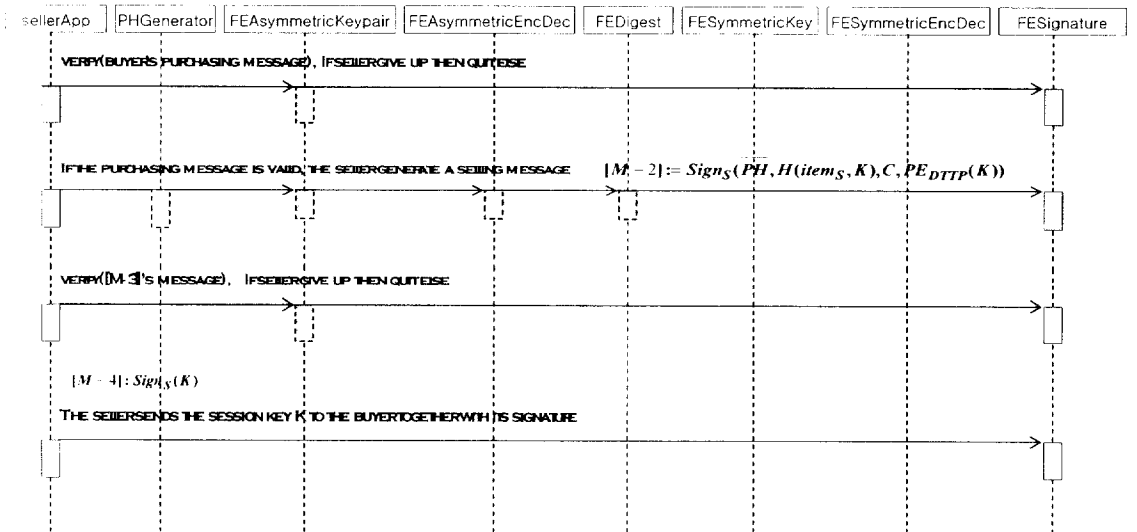
B. Classes's detail relationship



C. Buyer peer's sequence diagram



D. Seller peer's sequence diagram



E. Buyer/Seller's simulation

UI-42 File Exchange Protocol Library (Buyer/Seller)

Main Protocol

Alert Protocol

Recovery Protocol

Buyer ID

Seller ID

DT (PID)

buyeid

sellereid

dpotid

Descripton

DescriptPay

MP3

1000 지불

PlayItem Select

Key Select

buyerpaymt

InfoSelect

buyerprivkey

KeySelect

Gen

Enc

Dec

Sign

Verify

Reset

Source file name

Sign file name

source bt

sign bt

Send

Display

EVDhcAZjBAs5VkbQZFac5CNULicC8gweQUDg68FpviC80k

LISIA

Close

UI-42 File Exchange Protocol Library (Buyer/Seller)

Main Protocol

Alert Protocol

Recovery Protocol

Buyer ID

Seller ID

DT (PID)

buyeid

sellereid

dpotid

Descripton

DescriptPay

MP3

1000 지불

PlayItem Select

Key Select

MP3 mid

InfoSelect

buyerpubkey

KeySelect

Gen

Enc

Dec

Sign

Verify

Reset

Source file name

Sign file name

source bt

sign bt

Send

Display

전자지불 검증에 성공!!!!!!

LISIA

Close

감사의 글

연구실을 들어온지 2년이 넘는군요. 처음 연구실에 들어올때는 2년이 참 길게 느껴져서 이거 저거 다해보자고 굳게 다짐했는데, 감사의 글을 쓰고 있는 오늘 지난 2년을 돌아보면 열심히 한 저보다는 언제나 이 핑계 저 핑계로 게으름을 피운 제 모습이 먼저 떠오릅니다. 이런 저를 격려해주시고 바른 길로 방향을 잡아주신 교수님과 선·후배들이 있어서 지난 2년을 잘 보낸 것 같습니다.

먼저 저의 지도교수님으로 많은 조언과 격려를 아끼지 않으셨던 이경현 교수님께 깊은 감사를 드립니다.

그리고 많은 지도를 해주신 김창수 교수님, 정연호 교수님, 조경연 교수님, 조성진 교수님, 정목동 교수님, 최명구 교수님, 연구실 선배에서 교수님이 되신 신상욱 교수님께도 감사드립니다. 또한 지금은 고인이 되신 고 박지환교수님께도 감사드립니다.

2년동안 동고동락하며 보낸 정보보호 및 인터넷 응용 연구실원들에게도 감사드립니다. 2년동안 언제나 연구실의 든든한 버팀목이었던 준석선배, 연구실의 안주인으로 늘 편안히 대해주시던 정화선배, 수정선배, 연구실의 굶은일엔 언제나 앞장서며 술선수범하는 종필선배, 옆집 오빠같지만 범접하기 어려운 영호선배께 감사드립니다. 그리고 올해 2학기때부터 한 가족이 됐지만 이제는 연구실 분위기를 자지우지하며 늘 웃음꽃을 피우게하는 재귀선배, 해란선배, 소진선배께도 감사드립니다. 이번에 같이 졸업하게된 동기 미선이, 직장과 학교를 오가면 열심히 공부하시는 춘길씨, 주현씨, 연구실의 귀엽고 착한 학부생들 민현이, 광규, 봉기, 희숙이, 종찬이에게도 감사의 마음을 전합니다. 그리고 연구실을 졸업해서 다들 사회인으로 생활하게시는 신원 선배, 현호선배, 희현선배, 지철 선배, 명진선배, 성렬선배, 영경이, 화경이에게도 감사의 마음을 전합니다.

항상 내 옆에서 힘이 되었던 나의 친구들 현미, 은주, 경희, 현정이, 희진이, 미애, 선욱이, 옥현이, 경훈이 오빠, 도현이 오빠, 우승이에게 감사의 마음을 전합니다. 보안팀으로 같이 일했던 반응호 팀장님, 수경언니와 희정언니에게 감사의 마음을 전합니다.

오늘의 제가 있기까지 항상 옆에서 믿고 힘이 되어주신 아버지, 어머니께 진심으로 머리숙여 감사드립니다. 우리 집의 막내지만 언제나 속정이 깊은 현석이, 열심히 회사생활하는 정화, 미래 선생님이 될 혜영이에게도 감사의 마음을 전합니다.

마지막으로 항상 옆에서 많은 조언과 격려를 아끼지 않아준 사랑하는 철이선배에게도 감사의 마음을 전합니다.