A Thesis for the Degree of Master of Science

Design of Unlinkable Transaction Protocol For Preserving Customer Privacy

Seok-kyu Kang

School of Engineering

Information and Communications University

2005

Design of Unlinkable Transaction Protocol For Preserving Customer Privacy

Design of Unlinkable Transaction Protocol For Preserving Customer Privacy

Advisor : Professor Kwangjo Kim

by

Seok-kyu Kang
School of Engineering
Information and Communications University

A thesis submitted to the faculty of Information and Communications University in partial fulfillment of the requirements for the degree of Master of Science in the School of Engineering

Daejeon, Korea
Dec. 23. 2004
Approved by

(signed)

Professor Kwangjo Kim
Major Advisor

Design of Unlinkable Transaction Protocol For Preserving Customer Privacy

Seok-kyu Kang

We certify that this work has passed the scholastic standards required by Information and Communications University as a thesis for the degree of Master of Science

Dec. 23. 2004

Approved:

Chairman of the Committee
Kwangjo Kim, Professor
School of Engineering

Committee Member
Jaechoon Cha, Assistant Professor
School of Engineering

Committee Member
So Ran Ine, Ph.D
NITZ Corporation

M.S. Seok-kyu Kang
20032003

Design of Unlinkable Transaction Protocol For Preserving Customer Privacy

School of Engineering, 2005, 38p.
Major Advisor : Prof. Kwangjo Kim.
Text in English

Abstract

Privacy is becoming a serious challenge in computerized environments, especially the Web where many companies constantly attempt to violate the privacy of users. Privacy infringements when companies gather customer information are more likely to occur if the customer lacks control over this process. In general, most of privacy-preserving systems use pseudonyms or employ the Trusted Third Party (TTP) that hides all user information from web servers. However, users may want or need to identify themselves over the net but still retain their activities and profile in private. On the contrary, it is necessary for internet companies to know the user preference for their marketing activities and auditing. It is obviously conflicting between the user privacy protecting and the company's requirements. In this thesis, we presented the system protocol that provides the customer's privacy and satisfies business requirements for the digital content transactions. In our approach, the customer reveals his/her identity information(such as bank account or credit card number) in exchange for a digital content while protecting the privacy. Moreover, the Internet company is also able to obtain customer's buying pattern or preferences but the customer's privacy is sufficiently protected by unlinkability between customer identity and profile information. The proposed system

is designed with Chaum's RSA blind signature scheme[13] and operated on the open network as well as anonymity networks.

Contents

List of Tables

List of Figures

List of Abbreviations

SP Service Provider

PS Payment Server

CA Certification Authority

TTP Trusted Third Party

PIM Personal Information Market

CRT Chinese Remainder Theorem

List of Notations

CI Content's sample Information

$PAYINFO$ user Payment Information containing identification, credit card number or account information etc.

P Content's Price Information

CID Individual CI's Identification

SID SP's Identification

$REFinQ$ user REFerence inQuiry

$REFanS$ user REFerence anSwer

$E(), D()$ Symmetric encryption/decryption algorithms

$Blind_x(K, M, r)$ Blinding function by entity X. It accepts a public key K, a message M and secret random number r, and generates a blinded output.

$Unblind_x(M, r)$ Unblinding function by entity X. It accepts a secret random number r and a message M, and generates a unblinded output.

N_x Nonce of entity X

M full Digital Content

K, K^{-1} public/secret key

Chapter 1
Introduction

Over the past year, as the number of Internet user has been tremendously getting increase, various business and technologies based on the Internet were developed. Above all, the e-commerce is the biggest market in these days but the concern of privacy protection is getting influential. For example, when a customer intends to purchase an item from the service provider on the Internet, his information, such as IP address, browsed items, date of visit and the number of page view, are stored in the company's server side. The service provider automatically collects customers' information to analyze and learn their purchasing patterns and inclination for the personalized advertisement and maintaining the customer relationship. However, the user who accesses sensitive web sites or wants to remain hidden on the network is dissatisfied with these kinds of personalized services. Moreover, it is possible that if companies deal illegally their customer information with other companies without any permissions or the customer information leak out of companies accidentally occurred, the privacy would be infringed and broken. We believe that the privacy protection features provide business advantages to the service provider. If two service providers sell the same digital contents with the same price while one of them provides privacy protection and the other does not, the former is definitely more attractive to customers. To provide useful privacy protection, many proposed protocols and applications have been introduced so far, but they are only useful for web surfing in which users have no desire or not required to be identified. Therefore, they are mostly

useful when users visit free web sites and download free digital contents. However, when customers wish to make online purchases using their credit card numbers or banking accounts, they need to provide some identifying or authenticating information. In such situations the issue of privacy is not user anonymity communication problem, but how to hide customers' shopping/surfing patterns as much as possible. In general, the explicit demands from customers and businesses regarding commerce based on the consumers's personal information are as follows. Customers want to be able to control their privacy perfectly while shopping over the network. The company needs reliable and various customer information and an access channel to analyze customers' purchasing pattern or dynamic market trends. This problem is essentially conflicting to the anonymity communications problem. The former is concerned with hiding user's surfing activities from the server but the user is required to reveal identification information to the server while latter is concerned with hiding user's identity but all the user's surfing activities are under the prey eyes of the server.

1.1 Our Contributions

In this thesis, we consider the protocol which prevents the service provider from finding out which customer have bought what kind of contents by the unlinkability between the payment and user-profile information. Besides, we do not employ any kind of anonymous payment system causing more computation complexities and overheads to the network, and our approach can be easily applied into the current implemented payment mechanisms. While customer's privacy is being protected, customers are required to reveal their identities to pay for desired contents and the service provider is able to get the necessary information for its marketing activities. To achieve described above, we design the RSA blind signature-based system architecture that protects the customer privacy for the digital content transaction.

1.2 Organization

The organization of this thesis is as follows: In Section 2, we present brief mathematical background, cryptographic primitives and previous works used in the thesis. In Section 3, we consider some requirements that the system should be provided and propose our scheme. In Section 4, we evaluate the security and performance of our scheme. Finally, we compare our scheme with other works in Section 5 and conclude in Section 6.

Chapter 2
Preliminaries

In this chapter, we introduce basic concepts which would be used in our proposed scheme and and previous works for preserving privacy over the network.

2.1 Mathematical Background

Chinese Remainder Theorem

Given are L *moduli* $m_1, m_2, ..., m_L$, each an integer bigger than 1 and relatively prime to all the others, so GCD(m_k, m_j)=1 whenever k≠j. Also given are L integers $y_1, y_2, ..., y_L$. We seek an integer solution x of the simultaneous congruences x $\equiv y_j$ **mod** m_j for j= 1,2,3,...,L. The *Chinese Remainder Theorem*(CRT) says just one solution x exists in the interval $0 \leq$ x $<$ M where M:= $m_1 \cdot m_2 \cdot ... \cdot m_L$.

This can be derived from the notion of an *Integer Inverse* **mod** m. If GCD(n,m)=1 then n has just one integer inverse u **mod** m that satisfies $u \cdot n \equiv 1$ **mod** m and $1 \leq u < m$. This follows from *Euler's theorem*: u $\equiv n^{\phi(m)-1}$ **mod** m where $\phi(m)$ is Euler's Phi function that counts the positive integers less than and relatively prime to m. Alternatively, u may be computed by the *Extended Euclidean GCD Algorithm* that obtains the Greatest Common Divisor of n and m by repeated remaining operations; this algorithm also exhibits integers u and w that satisfy GCD(n,m)= $u \cdot n + w \cdot m$ = (u-m)$\cdot n$ + (w+n)$\cdot m$=..., so that u can be chosen to lie in the interval 0

$\leq u < m$. If $u{\cdot}n + w{\cdot}m = \mathrm{GCD}(n,m){=}1$ then $1 = u{\cdot}n$ **mod** m and we may write $u{=}n^{-1}$ **mod** m. This integer inverse is unique because if $1{=}v{\cdot}n$ **mod** m too then $(v\text{-}u){\cdot}1{\equiv}(v\text{-}n){\cdot}n{\cdot}u{\equiv}(v{\cdot}n\text{-}u{\cdot}n){\cdot}u{\equiv}\ 0$ **mod** m.

To derive the CRT, we have $M{:=}\ m_1, m_2, ..., m_L$ and set $M_j{:}\mathrm{M}/m_j$ and $W_j{:}M_j^{-1}$ **mod** m_j for each j= 1,2,...,L. Then x:=$(\sum_j {\cdot}y_j \cdot M_j \cdot W_j)$ **mod** M is the solution. This can be verified as follows: First, the sum's every term $y_j \cdot M_j \cdot W_j \equiv y_j$ **mod** m_j, but $y_j \cdot M_j \cdot W_j \equiv$ **mod** m_k for every $k \neq j$; therefore, $x \equiv y_j$ **mod** m_j. If also $v{\equiv}\ y_j$ **mod** m_j for every $j{=}1,2,...,\mathrm{L}$. Then $v - x \equiv 0$ **mod** m_j, where $v - x \equiv$ **mod** M, so either $v = x$ or only one of x and v lies in the interval $0 \leq \mathrm{x} < M$.

2.2 Digital Signature

A digital signature is an electronic signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been delivered is unchanged. The signature is formed by encrypting the entire message with the sender's private key or by encrypting a hash code of the message with the sender's private key. Thus the digital signature is able to provide authentication, non-repudiation and data integrity. Many applications for information security are adopting this technology to support desired security properties. We apply the signature scheme according to circumstances to satisfy the requirement of our proposed protocol. Especially, the blind signature scheme has been significantly employed in e-commerce area as well as in this thesis. We introduce blind signature in next section briefly.

2.3 Blind Signature

In a blind signature, the signer neither learn the messages they sign, nor the signatures the recipients obtain for their messages. A verifier who seeks a signature for a message m' from a signer with verifying key y prepares some related message m to the signer. The signer provides a response s back to the recipient, such that the recipient can derive a signature s' from y,a message m, m', s such that s' is valid for m' with respect to y. The resulting signature s' is called a 'blind signature', although it it not the signature that is blind, but the signer.

The first constructions of cryptographic blind signature were proposed by Chaum[13]. These early blind signature schemes were based on RSA signatures. The security of blind signature schemes is defined by a degree of unforgeability and a degree of blindness. Blindness is a property serving the privacy interests of honest recipients against cheating and collaborating signers and verifiers. The highest degree of unlinkability is unconditional unlinkability, where a dishonest signer and verifier, both with unconditional computing power, cannot distinguish (m, s) seen by the singer in the interaction with the honest recipient from the recipient's outputs (m', s'), which are seen by the verifier, even if the signer and the verifier collaborate.

Blind signatures have been employed extensively in cryptographic constructions of privacy oriented services such as untraceable electronic cash and anonymous voting schemes.

2.4 Anonymity Communication Channels

During the past years, several kinds of anonymity-preserving network systems have been proposed and these can be classified into multi-proxy based and single-proxy based system. The multi-proxy based anonymous systems, such as Crowds, Onion-routing and HORDES, employ a number of network

nodes between user and web server. In these systems, the user connection anonymity is protected by the cooperation of each node on the network. In the single-proxy based system, such as Anonymizer and LPWA, the connection anonymity is offered by the single proxy server; however, the user must trust this single proxy and all connection information are not anonymous to the proxy anymore. We will briefly explain functions and structures of these systems in this section.

2.4.1 Single-proxy based system

-Anonymizer[5][6] is one type of commercial available tools. It submits HTTP requests to the Internet on behalf of its users so that the only IP address revealed to the web server is that of the *Anonymizer*. The web server only sees the identity of Anonymizer server instead of seeing the user's true identity. However, users have to trust the *Anonymizer* and their own ISPs who can still observe their activities. Thus, the Anonymizer cannot guarantee its users perfect anonymity. One way in which anonymity can be viloated is the use of some streaming applications which go around the proxy by establishing their own direct net connections. Further, the technical standards underlying the Web are constantly in flux. That is, the changes to the HTML language can potentially create new routes around the Anonymizer's automatic link-rewriting mechanism.

-Lucent Personalized Web Assistant(LPWA)[1][4][15] is at a server that is remote from the user application like the Anonymizer. Hence it is subject to the same trust and vulnerability limitations. It enable users to browse web sites using aliases that are secure, consistent and pseudonymous. Each alias presents a different persona, such as user name, password and e-mail address to each web site. The personas for different web sites belong to the same user and they are independent and unrelated among them. To provide anonymous

personalized service for user, LPWA has three functional components: *Persona generator*, *Browsing proxy* and *E-mail forwarder*. The generated alias in the *Persona generator* would be used for a specific web site where a user wants to visit anonymously. The *E-mail forwarder* sends mail with alias e-mail address to the corresponding user. First of all, these aliases have to be satisfied the anonymity, consistency and uniqueness properties. To generate different aliases and meet those alias properties, LPWA employs the proxy using a collision-resistent hash function called *Janus function*. The alias is computed in this function which takes user-ID and secret phases as an input.

-JANUS[16][17][18] is a cryptographic engine that assists clients in establishing and maintaining secure and pseudonymous relationship with a server. JANUS is hiding the identity of recipients but not the identity of the senders. It employs a proxy, like an Anonymizer server, for the web browser's anonymity and encrypts the web server's URL with asymmetric encryption algorithm. The URL of web server is opened to the public as a form of encrypted. The sender requests the access to the server through the JANUS system with an encrypted URL:

$$http://janus.fernuni-hagen.de/janus_encrypted/encryptedURL$$

After the JANUS system decrypts the server's encrypted URL with its private key, then the user is able to access the desired web site via JANUS. In this case, the unlinkability between sender and receiver is provided. However, like an Anonymizer, the JANUS system knows all information and both participants in the interaction also have to trust the JANUS system. Moreover, the system only encrypted URLs but does not provide the confidentiality of data stream on the network.

2.4.2 Multi-proxy based system

-Onion Routing[3][4][9][15] provides anonymous connections using different layers of encryption. It is more robust than single-proxy systems for anonymous communication. In Onion Routing, a series of proxies communicating over encrypted channels cooperate to forward data to a responder. Data is wrapped in a series of encrypted layers that are peeled-off at a series of proxies(onion routers) along a path towards the responder.

It is assumed that each onion router knows the identities and public keys of each other onion router. The initiator, I, begins by choosing a route through the other onion routers to the responder R. For each onion router on the path, σ, the initiator constructs a layer of a connection setup packet consisting of the IP address of the next onion router, the encryption key seed information shared with the next onion router k, and the successor's layer. The innermost layer of the onion contains the identity of the responder and the data to be sent. Each layer is encrypted with the public key of the corresponding router, $K_{\sigma+}$. Each onion router pair uses a locally *unique anonymous connection identifer* so that subsequent communication does not require sending another onion.

$$I \rightarrow \sigma : aci,\ k,\ \{\sigma', k', \{\sigma'', k'', \{R, data\}_{K_{\sigma''+}}\}_{K_{\sigma'}}\}_{K_{\sigma+}}$$

As the packet is forwarded through the path of onion routers, the layers are peeled off. When the packet reaches the last onion router in the path, the data is forwarded directly to the responder. All requests from the initiator are sent along the same path of onion routers. Replies are sent to the last onion router on the path, which in turn forwards the data along the reverse path of onion routers towards the initiator. In implementation [14], Onion Routing is not typically deployed at every host. Instead, a number of dedicated onion routers are available for use, and an initiator must connect to one of these to contact the receiver. The first onion router thus knows all initiators it is servicing. Should an onion router be corrupted, all initiators that use that

router could be exposed.

-Crowds[2][3][15][19] is a network infrastructure with multiple nodes and based on the idea that people can be anonymous when they blend into a crowd. It is similar in operation to Onion Routing, however, the path through cooperating proxies is chosen randomly, on a hop-by-hop basis, as the initial request is forward through the crowd. Once a path out of the crowd is chosen, it is used for all anonymous communication from the initiator to any responder within 24-hour period.

Crowds begins with an initialization protocol. When complete, the initiator knows a private, symmetric key between itself and every *jondo*, the local program running Crowds. To send data, the initiator constructs and forwards a packet containing a random path id, p, the IP address of the responder, and the data are all encrypted with the key K_{Ij}, shared with the randomly chosen next *jondo*, j.

$$I \rightarrow j : \{R,\ p, data\}_{K_{Ij}}$$

Each crowd member receiving a packet with a new path id then randomly decides based on a probability of forwarding, $0.5 \leq P_f < 1$, whether to forward it on to the responder or to another randomly chosen *jondo*. Eventually, a *jondo* will decide to forward the packet to the responder based on P_f.

$$j' \rightarrow R : p'', data$$

Once the responder receives the packet, it returns a reply packet along the reverse path of the request. Subsequent packets between the initiator and responder always follow the same path. This use of static paths is necessary because if a number of *jondos* collaborate to discover the identity of an initiator. The initiator must be on each path, and therefore shows up more often than any other *jondo*. To limit the number of paths available to collaborators, Crowds only changes paths at a set period, typically every 24 hours. The use of static paths can lead to a slightly different problem. If new members that join immediately create a path, they can be easily identified

as new members have already established paths. A new member should wait until the next commit to form a path out of the crowd, and every initiator must flush and recreate al existing connections through the crowd.

While the identities of the crowds members are public knowledge, responders, and other crowds members never learn which particular crowd member is the initiator, as it is not easy to determine if the a successor on a path is sending its own message or forwarding one of another member. In this case, each member of the crowd gains anonymity at the cost of bandwidth in forwarding others communications.

-HORDES[7][15] employs multiple proxies similar to those used in the Crowds to anonymously route packets, but it uses the multicasting network to reply response. It provides only sender anonymity but not the receiver anonymity. In forwarding message step, the initiator sends his/her messages to the responder through randomly selected *jondos* and the message send from the initiator, in addition, has the multicast group address of the HORDES network to receive a responder's data. After a number of hops through the HORDE member, the last *jondo* forwards the message to the responder. It is prefaced with the random number, *id*, to identify it to the receiver for easy recognition from the multicast group. In HORDES, the forward and reverse paths are not always the same. Because of this property, the traceback attack would be difficult. For example, an active traceback attack along the forward path can be occurred against a HORDES session, but only while the session is active. It is more difficult that the packet does not follow the same path through the network. A passive attack would be also difficult because of the dynamic path in HORDES. That is, the path is re-established every session in this system. Against the malicious participants' collaborations the HORDES provides the same sender anonymity compared with the Crowds and Onion Routing, but the collaboration is possible only at the forward path but not the reverse path. However, the reply in HORDES can be eavesdropped by

any multicast receivers, and because the reply comes without being processed by some proxies, the timing attack is possible.

2.5 Related works

Recently, there have been several proposal on the privacy-preserving systems for transactions on the Internet. In this section, we discuss some previous works related with our system and suggest their weakness.

In [8], Bao and Deng concerned about the anoymous transaction and commensurate with the general problem of the Private Information Retrieval(PIR). Particulary authors introduced the system that allows a customer to disclose his/her identity information to the web site in exchange for a digital item, but prevents the web site from learning which specific item a customer intends to obtain. In this idea, the potential customer is able to pay for his desired content on the Internet but also his purchasing information is hidden from the web site. Therefore, it is difficult to get the necessary sales information for service provider's business activities. To do this, the merchant(the web site is equivalent to the merchant) generates the secure package including item information, encrypted item and encrypted encryption key. The customer downloads this secure package with free of charge through the Internet. So to get an encryption key for item decryption, the user must obtain the key from the transaction server which is independent entity in the system architecture. Of course, the static number of downloaded item can be gathered at the service provider but such numbers cannot precisely reflect the number of sold copies of each digital item. In the real world, the sales information is very important to run business and the royalty payment.

Gritzalis,Moulinos and Kostis[4] introduced the system based on the informediaries. The informediary(I/M) is a business entity surpporting the development of anonymous busines models and its basic role is to accumulate user information, and deals products and services on behalf of them. In other

words, the informediaries provide the user information that is not enough to identify each user to suppliers and maximize the value of customers profile while they prevent suppliers or commercial web servers from collecting user profile. Therefore, the use of I/M enable customers to increase their bargain capability without revealing personal data and, at the same time, enables vendors to promote products and service without violating customers' privacy.

In the work[12] by Enzman, Kunz and Schneider, the proposed system prevents the vendor(or supplier) from linking the user information which is gathered while searching with identifying information. In order to do this, the system requires asymmetric algorithm for data encryption by using public key of the vendor. If the user wants to buy some products or services, the user generates agents which contain the desired product information, and sends it to the base station which is in the middle of communication between a user and vendors. That is, all agents from the user are send to the destined vendor via the base station. The base station dispatches these agents and plays a role of proxy. Thus, the vendor cannot gather users' IP addresses and cookies for linking the received order.

In [4][12], these approaches generate the pseudonyms for customers and employ the TTP between the customer and the service provider. The service provider is able to get the necessary information related with its customers, but the customer must trust the TTP.

In [11], Otsuka and Onozawa proposed the system that applied the idea of personal information market. It supports that businesses obtain the reliable customer information and also access customer itself while customers are able to control their privacy. The Personal Information Market(PIM) is a framework for personal information sharing and people trade their own preferences with others. That is, the business entity buys the information from customers while customers control the use of their personal information. The PIM consists of four entities: Sender who provides his/her information, Receiver who

collects and uses user information and provides services or products, Broker who intermediates between Sender and Receiver, and Deliverer who delivers the service from Receiver to Sender. In PIM, Sender has the description file which contains the user identifier(*e.g.,* address, phone number etc.) which is traceable and the payload(*e.g.,* gender, age, purchasing history etc.) which is untraceable information. The payload information involves the set of categorized behavioral data and the user keeps his/her personal information in the description file. The Receiver who plays role of business entity or other comsumer is able to get the Sender's payload information but not the identifying information. The Broker and Deliverer are only able to get the identifier information but not payload. If the Broker, Deliverer and Receiver conspired together, the Sender's anonymity cannot be protected. Moreover, this system still employs TTP consisting of the Broker and Deliverer.

Chapter 3
Proposed Scheme

We consider new privacy preserving system for digital content transactions. In our proposed scheme, we use the blind signature and anonymity communication channels for providing unlinkable transactions.

We categorized the customer's information into the payment information and user-profile information. The payment information that includes the credit card number or banking account which is usually used to authorize the customer for the payment when he/she purchases any desired digital content, and the payment information is only revealed to a payment entity. (In this thesis, the payment information of customer is equivalent to identity.) The user-profile information contains the user-untraceable data, such as customer's age, gender or habit, and is used in the service provider to obtain necessary information for its business activities.

3.1 Overall Architecture

Our proposed system consists of three components: Customer, Service Provider (SP) and Payment Server (PS). The customer purchases digital contents from SP on the Internet, and has to pay for desired contents validly by revealing their information required in the payment process. SP provides digital contents to the customer and this participant should have user-profile information for its marketing activities. However, SP is not permitted to get customers' identities,thus, it has to be difficult for SPs to trace a customer who bought

a certain digital item. PS is an entity performing the payment process for the customer. In the real world, PS could be a credit-card company, a bank or payment gateway. In our approach, PS cannot know about the customer's purchasing information, such as what the customer bought or which content he/she expects to buy. Simply, PS only deals with the payment information received from a customer and there is no way for PS to know which customer intends to purchase what kinds of contents. PS does not reject SP's request to transfer money after finishing the transaction of the customer.

In addition, our approach uses the multi-proxy based anonymity network system, as we mentioned above, between the customer and SP. we assume that it is vulnerable to eavesdropping but robust against the traffic analysis attack. For more deep understanding, we describe some properties that the multi-proxy based anonymity network we employed should provide.

• Avoiding the information centralization

Because of the multi-proxy based anonymity network, the customer does not need to trust a single proxy for maintaining anonymity, and since requests of the customer are destined for the web server through multiple proxies, it is more effective for providing connection anonymity. Moreover, it must be difficult to recognize who have initiated the request even if some of proxies are colluded.

• Recovery the packet loss while transferring contents

While SP and the customer are communicating together, the anonymity system must guarantee the content delivery without the loss. If the content is lost on the anonymity network, the system can provide the recovery method.

• User overhead should be low as much as possible

To design the effective and practical system, the anonymity network does not cause much overhead for the network performance and efficiency.

We also assume that the customer may cheat SP. For example, a wicked customer may download contents without paying fairy or with paying less than the content price. Finally, the Third Trusted Party(TTP) does not need to be involved in our system. In other words, all participants do not trust each other and the customer information is dispersed and decentralized over the system entities.

3.2 Requirement of Our System

3.2.1 System Requirements

We consider that the protocol is operated under the Public-key certification infrastructure. Every participated entities have their own public key from the Certificate Authority(CA). Since RSA algorithm is already, generally implemented and used in Internet browsers such as MS Internet Explorer and Netscape, our proposed system can be easily adapted in current existing network systems. Moreover, other various web sites are also applying RSA algorithm for security thus these technological trends are one of the reason why we adopted RSA-based blind signature. As we described in previous section, the customer uses the anonymity network to be hide his information, such as IP addresses, cookies, in the browsing step, because if the anonymity network does not used in the browsing step, SP is able to know who have accessed and analyze the accessing patterns from staying time in its site.

- *Decentralization of customer information*
  The user identities and his profile information should be managed in PS and SP repeatedly. If the single system component manages and stores all information about customers, the information exposure could be more fatal than it could be at the system that disperses its customer information over participated components. Besides, customers are required to trust a single system component for being anonymous.

Thus, our proposed system should scatter and decentralize customer information.

- *Providing customer identities for the payment*
  For applying the current payment technology and designing the system more practically, the protocol should not use the anonymous payment system. Consequently, to pay for desired digital contents, the customer needs to open his payment information but not any information related with desired contents.

- *Controlling the profile information exposure*
  The customer should provide his profile information selectively. That is, the customer needs to determine his preferences to be revealed to control his privacy from SP, and our proposed system needs to ensure that the providing user preferences must depend on the customer's willingness.

- *Unlinkability between customer identities and their profiles*
  Any entities except the customer itself cannot link the customer identifying information to his profile information. Even if SP and PS collude and share their information mutually, it must be difficult to find any relation between identities and profiles.

3.3 Protocol

In this section we describe our proposed system protocol, and how the unlinkability of customers' identities and their transactions are provided. Overall protocol is consist of three phases: Setup, Purchasing and Delivery. We will use the following notations to describe the protocol.

3.3.1 Setup phase

Setting up Parameters SP and PS individually set up the system wide RSA parameters as follows:

1. Pick a 1024-bit RSA module $n = pq$ with primes $p = 2p'+1$ and $q = 2q'+1$ where p' and q' are also primes.
2. Choose a random 120-bit number d_p and let $d_q = d_q+2$.
3. Compute the RSA secret exponent d by the Chinese Remainder Theorem(CRT) such that $d = d_p \textbf{ mod } 2p'$ and $d = d_q \textbf{mod } 2q'$.
4. Compute the RSA public exponent e such that $ed = 1 \textbf{ mod } 2p'q'$.

The public key (e,n) is made public and the private key d is distributed securely. We define the public/secret key for SP as K_{sp} and K_{sp}^{-1} respectively. Similarly, the public/secert key for PS are defined as K_{ps} and K_{ps}^{-1}.

CI Creation. Before a transaction with customers, SP creates the content's sample information (CI). That can be a movie trailer, a part of music file or any kind of attractable information. Note that SP creates many CIs that introduce the same digital content, thus, each CI has its own identifier (CID) to be used when SP sends a full content to the customer at the delivery phase. After SP creates CI with CID, SP stores CID into the database.

REFinQ Creation SP also creates the $REFinQ$ which is a questionnaire of kind and required for SP to understand customers' preferences. To do this, SP makes questions asking the user-untraceable information, for example, it may ask about age, gender, favorites, motive of buying and so on. It means that customers can specify what information should be disclosed to whom, when it should be disclosed, and for what purpose, and that they

are guaranteed the information will be treated so. Furthermore, SP can analyze unspecified individual customer's preference without knowing his/her identifier for business.

Step.1 SP carries out the following: generate the signature for its own ID (*SID*) and price of i*th* digital content's P_i with a private key. After that, generate the bundle $[CI_i, \{SID, P_i\}_{K_{sp}^{-1}}, REFinQ]$.
Any potential customers can download this bundle without charge via an anonymous communication network. This bundle is only one-time downloaded in order to avoid the content re-delivery.

Step.2 After downloading the bundle, SP stores CID_i into the database because even though the digital content is not purchased yet, those information about stored *CID*s could be a good statistical data for analyzing and auditing digital contents.

3.3.2 Purchasing Phase

Step.3 The potential customer who downloaded a bundle and decided to purchase makes out the *REFinQ* and we call it as *REFanS* after answering. To answer *REFinQ* is not a mandatory in our system and this step totally depends on the customer's intention. In other words, the customer does not need to make a *REFanS* or he can select any questions he just wants to answer.

Step.4 The customer generates his payment information(*PAYINFO*) to pay for desired content. The *PAYINFO*, in this protocol, is a credit card number, banking account, or any other information to be used for the payment process. We consider that the *PAYINFO* can be used as user identification and is only opened to the PS. To get a PS's blind signature, the customer creates a

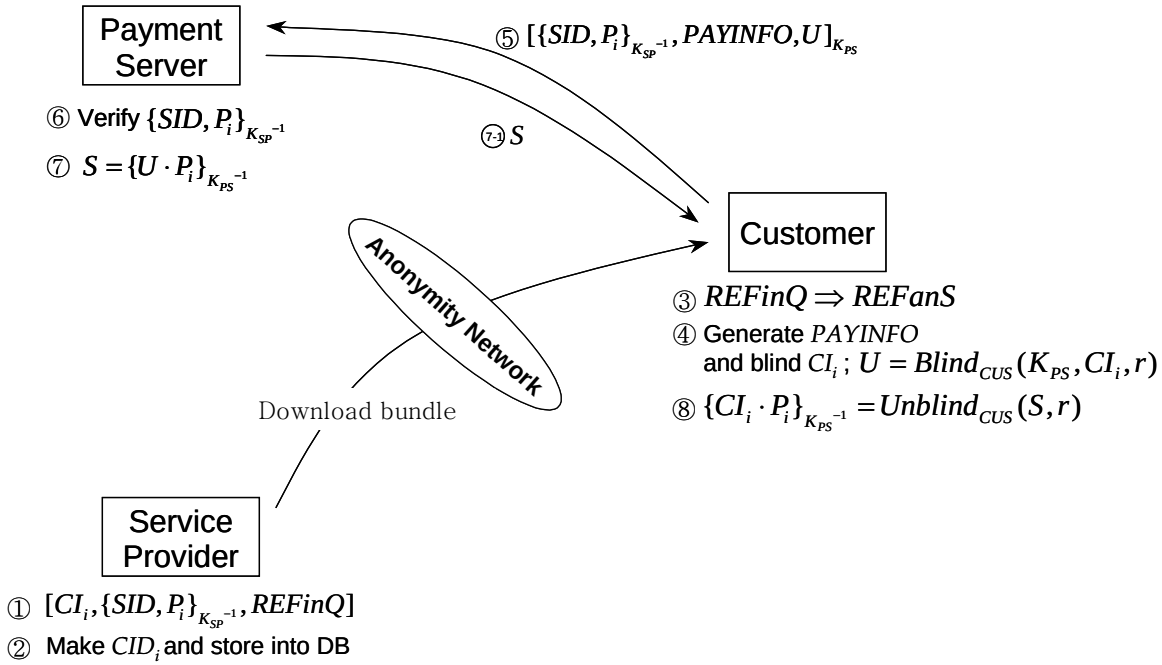

Figure 3.1: Setup and Purchasing Phases

random secret integer r, and computes U=$Blind_{CUS}(K_{PS}, CI_i, r)$ with the public key of PS. The value U is the blinded CI and the customer sends it to PS for obtaining its signature.

Step.5 The customer encrypts a set of $\{SID, P_i\}_{K_{SP}^{-1}}$, $PAYINFO$ and U with the public key of PS, and sends it to PS.

Step.6 The PS verifies $\{SID, P_i\}_{K_{sp}^{-1}}$ whether it is generated in SP. If it is valid, the PS starts to process the customer's payment request with $PAYINFO$ and P_i.

Step.7 If the payment process is successfully processed, PS computes where P_i is the content's price just processed in **Step.6** and generates the signature

S=$\{U \cdot P_i\}_{K_{PS}^{-1}}$

Step.7-1 PS send S to the customer.

Step.8 At this step, the customer receives the value S. So, PS's signature, S, justifies whether the customer paid properly without revealing what the customer intends to buy. To unblind the value S, the customer computes $\{CI_i \cdot P_i\}_{K_{PS}^{-1}}$= $Unblind_{CUS}(S,\, r)$

3.3.3 Delivery Phase

When SP delivers the digital contents to the customer, an anonymity network is employed between them. An anonymity network to be employed in our system is used to provide the connection anonymity for the customer. Thus, the customer would be anonymous from SP while he purchases the digital contents. As we described, we use the concept of multi-proxy bases system to avoid that the single proxy determines the customer's identity.

Step.9 In this step, the customer demands SP to send the full digital content (M) by sending an encrypted data $[\{CI_i \cdot P_i\}_{K_{PS}^{-1}}, CI_i, REFanS, N_{CUS}]_{K_{SP}}$ where N_{CUS} is a nonce generated by the customer.

Step.10 SP verifies $\{CI_i \cdot P_i\}_{K_{PS}^{-1}}$ and compares P_i with $P_i' = CI_i^{-1}(CI_i \cdot P_i)$ to validate whether the customer paid accurate price for his desired content, and check the state of CID_i from the database to avoid the double delivery of digital content. Since the state of CID_i is automatically changed when the matching digital content is purchased or downloaded, we can easily obstruct the double use of $\{CI_i \cdot P_i\}_{K_{PS}^{-1}}$

Step.11 After doing all confirmation, SP encrypts the full digital content (M) with N_{CUS} which is from the customer. That is, $Z_i = E(M_i, N_{CUS})$

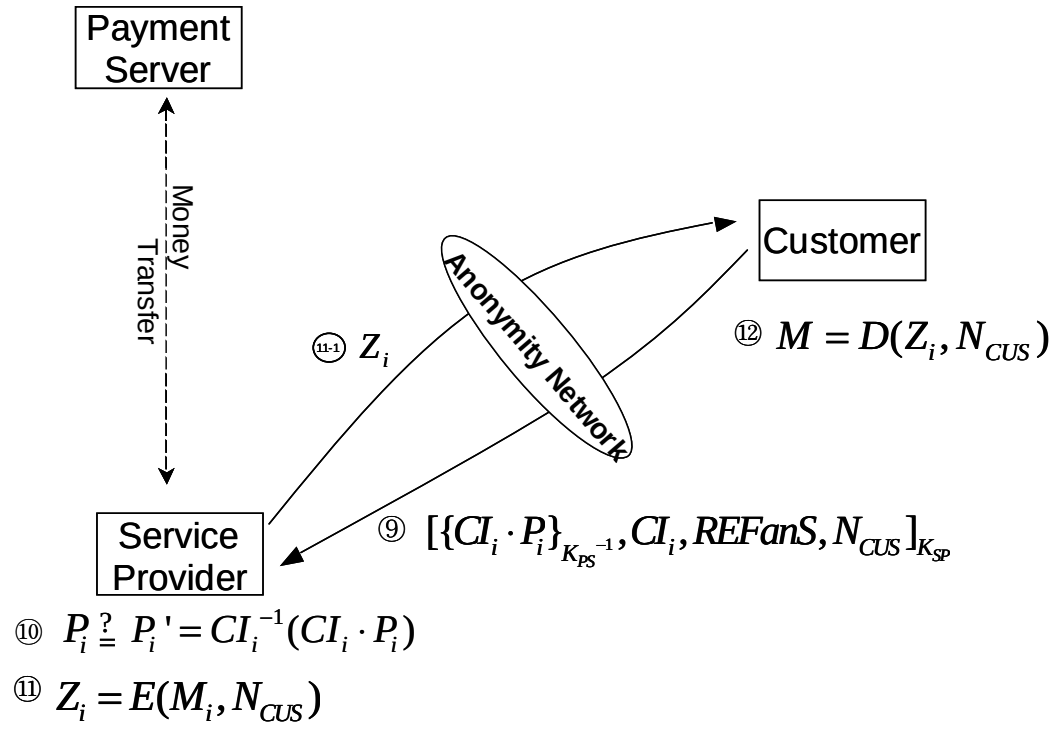

Figure 3.2: Delivery Phases

Step.11-1 SP sends encrypted full digital content Z_i through the anonymous communication channel. When finishing the content delivery, the service provider changes the state of CID_i to purchased condition in the database.

Step.12 If the customer receives the encrypted full digital content, Z_i, he computes $M = D(Z_i, N_{CUS})$ to get his purchased digital content.

Chapter 4
Analysis of the Protocol

In our protocol, since the customer blinds his desired CI, and the PS merely generates a signature for blinded *CI*, PS cannot learn which content the customer intends to purchase. Even though PS has customers' identity information from *PAYINFO*, it does not provide enough information to infer or track the customers' buying pattern because the *CI* is blinded by the customer's secret random number r using *RSA* blind signature scheme. SP has the customers' profile information from the *REFanS* received from customers at the purchasing phase. Each *REFanS* contains the individual customer's preference such as his age, gender, date of purchasing, his favorites and so on, but these preference information do not say about any customer identifying information.

Additionally, all communication of SP and the customer is achieved on the anonymity network so that SP cannot trace the specific customer's identity. SP just delivers contents to the customer through the anonymity network after authorizing whether the customer paid or not.

In another consideration, our proposed system enables the customer to pay for separated desired contents with different *PI*s at the same time because PS processes the payment process according to individual *PI*s received from the customer without regard to *CI*. For example, assume that if the customer has several bundles, $[CI_1,\ \{SID, P_1\}_{K_{sp}^{-1}},\ REFinQ]$, $[CI_2,\ \{SID, P_2\}_{K_{sp}^{-1}},\ REFinQ]$...$[CI_n,\ \{SID, P_n\}_{K_{sp}^{-1}},\ REFinQ]$ and wants to purchase all of them, he sends U_1=$Blind_{CUS}(K_{PS},\ CI_1,\ \mathrm{r})$, U_2=$Blind_{CUS}(K_{PS},$

CI_2, r)...U_n=$Blind_{CUS}(K_{PS}, CI_n, \text{r})$ and $\{SID, P_1\}_{K_{SP}^{-1}}$, $\{SID, P_2\}_{K_{SP}^{-1}}$...$\{SID, P_n\}_{K_{SP}^{-1}}$ to PS. PS verifies every single $\{SID, P_i\}_{K_{SP}^{-1}}$ and computes $S_1 = \{U_1 \cdot P_1\}_{K_{PS}^{-1}}$, S_2=$\{U_2 \cdot P_2\}_{K_{PS}^{-1}}$,...$S_n$=$\{U_n \cdot P_n\}_{K_{PS}^{-1}}$. In theses transactions, PS that may contract with another SPs has to recognize each *SID* for different *PI* in order to transfer money to the right SP.

4.1 Performance Analysis

The most heavy computational burden to PS is the verifying operation $\{CI_i \cdot P_i\}_{K_{PS}^{-1}}$ in step 10. The operation $\{SID, P_i\}_{K_{sp}^{-1}}$ is also expensive, but it is conducted only once for each digital content M, while verifying operation is performed per transaction. Hence we want to reduce the cost of $\{CI_i \cdot P_i\}_{K_{PS}^{-1}}$ as much as possible. This is the reason why we choose the secret key K_{PS}^{-1} through applying the CRT. Since d_p and d_q for generating secret keys are small 120-bit numbers, the computation is much cheaper than an direct 1024-bit RSA algorithm.

Since the secret key is chosen in a special way, the most expensive computation for the customer is $Blind_{CUS}(K_{PS}$, CI,r). But this step can be done in advance as a pre-computation, i.e., the selection of r and the computation of blinding function can be carried out as soon as the customer's machine is power on or during the machine idle time. The task for the customer's machine to do after unblinding of S is getting random nonce N and decrypting $M = D(Z_i, N_{CUS})$. They are very cheap operations.

4.2 Security Analysis

The problem of speeding up RSA encryption algorithm has been studied in cryptography for many years. It has been noticed that choosing small secret exponent d could be dangerous[20][22]. So far the best way is to choose small d_p and d_q. The meet-in-the-middle attack with Fast Fourier Transform tech-

nique provides an algorithm of complexity $\mathcal{O}(\sqrt{d_p}(\log_2 \sqrt{d_p})^2)$ to factorize n[21]. Therefore, a 120-bit d_p can provide a security level higher than 2^{72}, which is not much lower than the cost of the best factorization of 1024-bit n.

4.2.1 Information Disclosure

One possible attack is that the collusion of SP and PS by sharing their information: customer identities and profiles. In our proposed protocol, if two participants share their information mutually, they cannot link customers' identities to their profile information together since the PS does not know CI that the customer paid for unless knowing the customer's secret number r. Also, SP does not know who have bought its digital content, and there is no way to find any relevance between them.

4.2.2 Dispute Resolution

SP requests PS to transfer money after transactions. It is also possible that the money transfer between the PS and SP can be occurred every fixed time period. Since the PS has SIDs, the sale charge can be transferred to the right SP.

Our approach provides protection against unfair activities by either SP or the customer. Possible disputations and cheatings are addressed in this section. All cases require the authority as a mediator. In addition, if required, the customer can reveal his identity. At the end of the transaction, even if the customer paid for his desired content to PS, it is possible that SP refuses to deliver a full content. In this case, the customer shows his S to the mediator for proving that he already paid P_i for CI_i to PS. If it is valid, the customer prevails.

Another possible fraud is that the customer who downloaded a number of bundles and accumulated multiple $\{SID, P\}_{K_{sp}^{-1}}$ can cheat SP by replacing $\{SID, P_{i-1}\}_{K_{sp}^{-1}}$ associated with a high cost item with another $\{SID, P_i\}_{K_{sp}^{-1}}$

associated with a low cost item. Because PS receives the $\{SID, P_i\}_{K_{sp}^{-1}}$ and blinded CI of P_{i-1}, the malicious customer can pay lower cost and request CI of P_{i-1} to SP by showing the signature $\{CI_{i-1} \cdot P_i\}_{K_{PS}^{-1}}$ of PS. However, SP computes $P_i' = CI_{i-1}^{-1}(CI_{i-1} \cdot P_i)$ and compares with P_{i-1} corresponding with CI_{i-1} at the delivery phase, and if P_i' and P_{i-1} are not the same, SP easily becomes aware of the customer's cheating.

4.2.3 How Common Threats are dealt with

Blind signature and content delivery exploit public and symmetric key cryptography. These technologies are deployed to defend against most threats.

1. *Monitoring of communication lines.* Avoided by using Public Key Cryptography.

2. *Shared key stealing.* Avoided by using public key encryption.

3. *Unauthorized modification of information in transit.* Avoided by using public key encryption during all communication steps between two entities

4. *Forged Network Addresses and Masquerade*: We distinguish two cases of forging:

   - An unscrupulous user pretends to be a self-signed S - This is avoided by issuing certificates by authority as a mediator.
   - An unscrupulous user pretends to be a trusted party - Avoided by using certificate-hashing mechanisms.

5. *Unauthorized access*: Avoided through the use of a sound access control policy.

Table 4.1: Services and candidate technologies and standards

Service	Candidate technologies
Registration	WWW, SSL, Secure e-mail(PGP, S/MIME)
Cryptographic services	RSA Cryptokit, Microsoft CryptoAPI
Certificate management	X.509, SPKI
Anonymity Communication	Onion-routing, Crowds
Database management	Medium-class or high-end DBMS supporting SQL
Delivery	S/MIME, PGP

6. *Private key stealing and Private key compromise*: Avoided by using strong encryption and by storing cryptographic tokens in removable media.

Chapter 5
Comparison

In this section, there is a comparison table of previous systems described in the preliminaries section. In this table,the customer privacy issues are itemized into 4 factors: Privacy control, Technical traceability, Sales audit and Unlinkability of transactions.

Privacy control means that how much customers can manage or control identity information themselves. The proposed system in [8] requires customers to disclose their identities for the payment operation to the transaction server. That is, the customer provide his/her identities even though their surfing activities are hidden. In [4] and [11], the disclosure of customer profile information is depended on the system proxy which has a capability to build customers' identity information. The system in [12] using agents has also high privacy control has high privacy control. The customer himself generates agents and sets the attributes that will be disclosed to web servers. In our proposed system, the customer is free to answer questions in *RefinQ*. In other word, the customer control the degree of the profile disclosure by himself. Thus, the customer of our system has high privacy control.

Technical Traceability means the possibility of tracking customers through the technical factors, such as IP addresses and cookies. The [8] and [11] have low possibility because they plays as a role of filter in between the user and the web server, so these traceable factors could be removed. In our system, each transaction between the SP and customer is occurred through the anonymity communication channel. Therefore, all technical traceability are filtered out

Table 5.1: Comparison among Customer Privacy Preserving Systems

		Proposed System	[8]	[4]	[11]	[12]
Privacy Control		O	X	X	X	X
Technical Traceability	cookies	X	O	O	△	O
	IP address	X	△	O	X	O
User Authentication		password-based	¬	IP address, signature	password-based	¬
Sale Audit		O	X	O	O	O
IDs - Profiles Unlinkability		Yes	Yes	No	No	No
Credential Integrity		signature	MAC	Signed Hash	MAC	Signed Hash

O: available , X: Not available , △: Partially available , ¬: Not applied

during the transmitting on the channel.

In *Authentication*, the proposed scheme uses a nonce generated by the customer to provide protection against replay attacks. However, S must be included in order to prevent a malicious customer from replaying a stolen $\{CI_i \cdot P_i\}_{K_{PS}^{-1}}$ with a new nonce N, potentially increasing the customer's workload.

Sales Audit is that whether service provider are able to know the sales figure, (*e.g.,* a number of sold items, what kind of group person have bought and so on) or not. The system [8] does not provide sales figure information to the service provider. Merely, the static number of downloaded items are gathered and these numbers are not helpful in real world and unpractical. In other systems [11], [4] and [12], their proxies provide sales information to the service provider instead of the customer. In our system, the *REFanS* generated by customers are provided to the SP through the anonymity channel and the number of sold item can be easily recognized at the delivery phase, hence the SP can get the enough sales information without interfering customer

identities.

User Information is classified with Payment information and User-profile information in our proposed scheme. That is, most previous works manage all user information at the single trusted proxy between customers and service providers. However, our proposed system lets these information are stored at different entities. For example, payment information including customer identity only goes to PS, and user-profile only goes to SP. So, these architecture helps decrease the risk of information exposure.

Unlinkability between transactions is one of important properties in our proposed system. The [4], [11] and [12] don't provide unlinkable transaction. The systems preserving customer privacy control all information on their customer as a TTP. Therefore, it is possible to expose customer identities if they are conspired together. However, although our proposed system request customers to reveal their identities like these systems, the unlinkability between user identities and purchasing history are provided by applying the RSA blind signature scheme. Especially, we modified this scheme by signing blinded content's CI with its price information at the PS. Even if the customer information is not revealed to SP and PS but also they are colluded together, due to the unlinkable transaction property, finding the relevance between occurred transactions and user profiles would be difficult.

Chapter 6
Conclusion

Throughout this thesis, we have studied on privacy preserving unlinkable protocol for digital content transactions. For the concrete design, we reviewed previous related works and pointed out their problems. And then we have suggested the improved protocol with *RSA* blind signature scheme.

Many kinds of customer privacy-preserving systems use pseudonyms or TTP that hides all customer information from service providers, but our proposed protocol, in this thesis, uses a current implemented payment architecture instead of an anonymous payment system. In addition, customer privacy is to protected without TTP. The customer only sends PS his/her payment information as an identity in order to pay for desired content and SP performs the verification based on *RSA* blind signature scheme whether the customer paid validly. Since the communication between SP and the customer is achieved on anonymity network, SP cannot learn and track a content that the customer intended to purchase.

Moreover, even if SP and PS may collude together and share their customer information mutually, two entities cannot find out customer's purchasing record due to the difficulty for linking customer identity to profile information.

It is commonly recognized that one of the most important issues for e-commerce of digital contents is content protection and management. This is on-going effort in a number of industrial initiatives. However, additional efforts are required to study detailed integration issues with specific content

protection and management systems. Therefore, it is necessary to study how to seamlessly integrate our system with a digital content protection system.

고객 프라이버시를 위한 비연결성 거래프로토콜의 설계

강석규

프라이버시 보호 문제는 지금과 같이 통신 기술이 발전할수록 중요한 이슈로 받아들여 지고 있다. 특히 사용자에게 있어서 인터넷 기업은 잠재적으로 자신의 프라이버시를 침해할 수 있는 존재로 여겨지고 있다. 즉, 인터넷 기업이 자신들의 고객 정보를 수집하고 분석하면서 프라이버시 침해가 발생할 수 있는데, 이러한 상황은 고객이 직접 정보제공 기능을 갖고 있지 못한 상황에선 더욱 빈번하게 발생 할 수 있다. 일반적으로 대부분의 사용자 프라이버시 제공 시스템은 의사아이디를 제공하거나 웹 서버로부터 사용자에 대한 모든 정보를 숨기기 위하여 신뢰기관(TTP)를 사용하여 왔다. 하지만 현실세계에 있어서 사용자가 인터넷을 통해 물건을 구매하고자 할 경우엔, 지불을 위해 반드시 자신의 신분정보를 제공하여야 하며, 동시에 자신의 구매내역, 검색내역 등을 숨기고 싶어한다. 이와 반대로, 인터넷 기업, 즉 판매자 입장에서는 최소한 고객 개개인의 신분정보를 얻을 수 없더라도, 자신들의 비즈니스 활동 및 고객의 구매 패턴 분석 등을 위하여 고객 선호도(preference)등을 알고 싶어한다. 이러한 요구 사항들은 명백하게 대립되는 요소이기 때문에 모두 만족시키기 상당히 어렵다. 본 논문에서는 고객의 프라이버시 보호를 보호 할 수 있을 뿐만 아니라, 판매자에게도 비즈니스 활동에 필요한 정보를 제공할 수 있는 시스템 프로토콜을 설계하였다. 우리가 제안하는 시스템에서는, 고객의 정보를 고객신분정보(Identity Information)과 고객 구매패턴, 선호도를 포함하는 프로파일(Profile information)으로 나누었다. 고객은 지불을 하기 위해 자신의 신분정보를 지불담당 개체(payment server)에 제공하고, 판매자는 비즈니스에 필요한 정보를 제공받을 수 있다. 일련의 이러한 것들은 Chaum이 제안한 익명서명 기법을 응용하여 이루어 지며, 지불담당 개체와 판매자간의 공

모가 발생하여 고객 신분정보와 고객 프로파일 정보를 공유하게 되더라도 두 정보간에 아무런 관련성을 찾을 수 없기 때문에 결과적으로 전자거래에서의 고객 프라이버시는 보호 받을 수 있게 된다.

마지막으로 본 논문에서는 제안된 프로토콜의 안전성 및 성능을 분석하였고, 지금까지 제안된 고객 프라이버시 제공 시스템들과 비교를 해 보았다.

References

1. D.Kristol, E.Gabber, P.Gibbons, Y.Matis and A.Mayer, "Design and Implementation of the Lucent Personalized Web Assistant(LPWA)", http://www.math.tau.ac.il/ matias/lpwa.html

2. M.Reiter and A.Rubin, "Anonymous Web Transactions with Crowds", Communication of the ACM, Volume 42, Issue 2, pp. 32-48, February,1999.

3. S.Fischer, "Privacy-Enhancing Technologies", 5th International Conference on Applications of Natural Language to Information Systems, LNCS, Springer-Verlag, pp. 107-165, 2001.

4. D.Gritzalis, K.Moulinos and K.Kostis, "A Privacy-Enhancing e-Business Model Based on Infomediaries", Mathematical Methods, Models, and Architectures for Network Security: International Workshop MMM-ACNS, Vol.2052, pp. 72-83, 2001.

5. Seo, I.S, "Anonymity in Web", http://security.kaist.ac.kr/?report

6. Anonymizer.com, http://www.anonymizer.com

7. C.Shields and B.Levine, " Protocol for Anonymous Communication Over the Internet", In Proc. of the 7th Conference on Computer and Communications Security, pp. 33-42, 2000.

8. Feng Bao and Robert Deng, "rivacy Protection for Transactions of Digital Goods", The Third International Conference on Information and Communications Security, LNCS, Springer-Verlag, pp. 202-213, 2001.

9. M.Reed, P.Syverson and D.Goldschlag, "Anonymous Connections and Onion Routing", IEEE Journal on Selected Areas in Communications, Vol.16, pp. 482-494, 1998.

10. D.Goldschlag, M.Reed and P.Syverson, "Onion Routing for Anonymous and Private Internet Connections", Communications of the ACM Vol. 42, Issue 2, pp. 39-41, February, 1999.

11. T.Otsuka and A.Onozawa, "Personal Information Market: Toward a Secure and Efficient Trade of Privacy",the First International Conference on Human.Society@Internet, LNCS, Springer-Verlag, pp. 151-163, 2001.

12. M.Enzmann, T.Kunz and M.Schneider, "Privacy Protection through Unlinkability of Customer Activities in Business Process Using Mobile Agents", the Third Electronic Commerce and Web Technologies, LNCS, Springer-Verlag, pp. 314-323, 2002.

13. D. Chaum, "Blind signatures for untraceable payments" Advances in Cryptology-CRYPTO'82, LNCS, Springer-Verlag, pp. 199-203, 1982.

14. http://www.freedom.net/info/freedompapers/index.html, November, 1999.

15. J.Argyrakis, S.Gritzalis and C.Kioulafas, "Privacy Enhancing Technologies: A Review", The eGovernment Conference, LNCS, Spinger-Verlag, pp. 282-287, 2003.

16. Park, Y.H. and Lee,K.H, "Privacy Protection and Anonymity Services for the WWW", The journal of Korea Multimedia Society, Volume 3, Issue 2, pp. 518-521, November, 2000.

17. I.Goldberg and D.Wagner, "TAZ Servers and the Rewebber Network: Enabling Anonymous Publishing on the World Wide Web", Peer-reviewed Journal on the Internet, vol.3, 1998.

18. E.Gabber, P.Gibbon and D.Kristol, "On secure and pseudonymous clients-relationships with multiple servers", ACM Transactions on Information and System Security (TISSEC) Volume 2 ,Issue 4, pp. 390-415, 1999.

19. I.Goldberg, "Privacy-Enhancing Technologies for the Internet, II : Five Years Later", Workshop on Privacy Enhancing Technologies, LNCS, Springer-Verlag, pp. 1-12, 2003.

20. D.Boneh and G.Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$", Advances in Cryptology, Eurocrypt'99, Springer-Verlag, pp. 1-11, 1999.

21. P.Q.Nguyen, "Private Communication", International Conference on the Theory and Application of Cryptographic Techniques, LNCS, Springer-Verlag, pp. 53-70, 2000.

22. M.Wiener, "Cryptanalysis of short RSA secret exponents", IEEE transactions on Information Theory, Vol.36, pp. 553-558, 1990.

Acknowledgements

First, I would like to express my sincere gratitude to Prof. Kwangjo Kim, my academic advisor, for his constant direction and support. He always has shown his consistent affection and encouragement for me to carry out my research and life in ICU. Special thanks also goes to Prof. Jaechoon Cha and Ph.D So Ran Ine for their generosity and agreeing to serve as committee members of my thesis.

I also would like to thanks to all members of cryptology and information security laboratory: Jeongkyu Yang, Kyusuk Han, Hyunlok Lee, Zeen Kim, Jaemin Park, Sangshin Lee and Sungchul Hur, Vo Duc Liem and Dang Nguyen Duc from Vietnam, Ping Wang from China, for giving me lots of interests and good advices during the course of my study.

In addition, I appreciate to the graduates, Jaehyrk Park, Sungjun Min, ByeongKon Kim, Songwon Lee, Sang-won Lee, Hwasun Chang, Chul-Joon Choi and Joong Man Kin for their everlasting guidance in life and study of ICU.

Most of all, I should mention my father and mother for their endless concerns and devotional affection. I cannot forget their trust and encouragement on me. My sister, brother-in-law and my brother studying in Australia also have given me warmhearted concerns. I pray my lovely nephew and niece to be an admirable person and I hope God bless my family and to be happy.

Finally, I will always remember the life of ICU. It filled up my poor knowledge and made me a grown-up person.

Curriculum Vitae

Name : Seok-kyu Kang

Date of Birth : Jan. 16. 1977

Sex : Male

Nationality : Korean

Education

1995.3–2003.2	Information Systems ChungAng University (B.A.)
2003.2–2005.2	Cryptology and Information Security, Engineering Information and Communications University (M.S.)

Career

2004.4–	Graduate Research Assistant Research on User Authentication and Privacy for Ubiquitous Environment Digital Media Laboratory in ICU
2004.3–	Graduate Research Assistant Research on the Security for Special Digital Signature National Security Research Institute(NSRI)

2004.6–2004.8 Apprentice Researcher
Information Technology Laboratories. Secure System Group,
SONY, Japan

2003.12–2004.4 Graduate Research Assistant
Ubiquitous System Security Technique
Next Information Technology Zone(NITZ)

2003.8–2003.12 Graduate Research Assistant
Research on Link Security Algorithm and Standardization
Electronics and Telecommunication Research Institute(ETRI)

2003.2–2004.2 Graduate Research Assitant
Cultivation of Top Level IT Security Manpower
The Ministry of Information and Communications(MIC)

Publications

(1) 2005.1 Seok-kyu Kang, Tomoyuki Asano, and Kwangjo Kim, A Protocol of Unlinkable Transaction for Preserving Customer Privacy, *submitted to The 2005 Symposium on Cryptography and Information Security*, Kobe, Japan.

(2) 2005.1 Ping Wang, Seok-kyu Kang, and Kwangjo Kim, Tamper Resistant Software Through Dynamic Integrity Checking, *submitted to The 2005 Symposium on Cryptography and Information Security*, Kobe, Japan

(3) 2004.10 강석규, 토모유키 아사노, 김광조, Unlinkability between Customer Profile and ID for Preserving Privacy in Digital Content Transactions, 2004년도 한국정보보호학회 충청지부학술대회, pp. 69-82, 공주대학교, 한국

(4) 2004.8 강석규, 김광조, 디지털 컨텐츠 거래에서의 사용자 익명성 보장기법, 2004년도 한국정보보호학회 하계학술대회, Vol.14, No.1, pp. 615-618, 경동대학교, 속초

(5) 2004.6 Songwon Lee, Kyusuk Han, Seok-kyu Kang, Kwangjo Kim and So Ran Ine, Threshold Password-Based Authentication Using Bilinear Pairings, *European PKI*, Samos island, Greece, 2004

(6) 2003.11 Jaehyrk Park, Seok-kyu Kang and Kwangjo Kim, Group Mutual Exclusion based Secure Distributed Protocol, *The 1st Computer Security Symposium 2003*, Kokura, Japan