A Thesis for the Degree of Master of Science

Location Authentication in Ubiquitous Computing Environment

Kyusuk Han

School of Engineering

Information and Communications University

2004

Location Authentication in Ubiquitous Computing Environment

Location Authentication in Ubiquitous Computing Environment

Advisor : Professor Kwangjo Kim

by

Kyusuk Han
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
Jun. 8. 2004
Approved by

(signed)

Professor Kwangjo Kim
Major Advisor

Location Authentication in Ubiquitous Computing Environment

Kyusuk Han

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

Jun. 7. 2004

Approved:

Chairman of the Committee
Kwangjo Kim, Professor
School of Engineering

Committee Member
Myungchul Kim, Associate Professor
School of Engineering

Committee Member
So Ran Ine, Ph.D
NITZ Corporation

M.S. Kyusuk Han
2001814

Location Authentication in Ubiquitous Computing Environment

School of Engineering, 2004, 41p.
Major Advisor : Prof. Kwangjo Kim.
Text in English

Abstract

In the ubiquitous computing, user's availability will be maximized with the wireless network. Users get the proper service anytime, anywhere without any restriction of time and location. Without user's concerns, user's contexts are sensed by the network to provide the proper service.

However, the increasing of user's availability also will occur the increasing of security risks. Sensing user's context cause privacy issues. Also, forgery of contexts is also problem.

Forgery on location information is critical risk of context based service. There are several researches on location authentication. Denning [11] proposed Differential GPS based location authentication method, while Sastry [12] proposed location authentication method using the time difference from the velocity of radio frequency and sonic. Nakanishi [13] adopted RFID for location information. And, Kindberg [14] showed general model using constrained channel with Wi-Fi, Bluetooth, and etc. But these works are only focused on authentication of location information, there is no consideration of privacy of user. Moreover, they require specific device for protocol.

We generalize the risks in the location based service model, and define security requirements in this paper. We also introduce new model of privacy preserving location authentication method which can be adopted in universal. Based on the model, we propose several protocol using asymmetric/symmetric key encryption and one-time key or timestamp.

Finally, we discuss DRM in ubiquitous computing environments with location authentication.

Contents

List of Tables

List of Figures

List of Abbreviations

LA Location Authentication

TA Trusted Authority

$\mathcal{AOLAP}$ Asymmetric encryption with One-time key based LA Protocol

$\mathcal{ATLAP}$ Asymmetric encryption with Timestamp based LA Protocol

$\mathcal{SOLAP}$ Symmetric encryption with One-time key based LA Protocol

$\mathcal{STLAP}$ Symmetric encryption with Timestamp based LA Protocol

List of Notations

C Client, Prover

$E_K(m)$ message m encrypted with symmetric key K

$D_K(m)$ message m decrypted with symmetric key K

$h(m)$ hashed message m

L_C location information of C

OP Operator, TA

SP Service Provider, SP, Verifier

K a shared key

TS timestamp shared between C and OP

SK a private key

PK a public key

Chapter 1
Introduction

1.1 Location authentication

In the ubiquitous computing environment, users are possibly connected in wireless network, and user will move dynamically anywhere maintaining network connection. Ubiquitous computing is the method of enhancing computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user.

The concept of the pervasive computing environment is based on the idea that future communications systems will allow mobile and fixed devices access to a wide range of services over a diversity of mobile inter-working, or collaborating networks. The devices available to the user will form a Mobile Ad hoc network (MANET) and may or may not be available with anyone, any organizations, any time, anywhere, any networks and any devices (A6). According to [1], the ubiquitous computing devices "encompasses a user perspective of multiple devices (both local and remote) accessing multiple services via multiple networks, all of which can be changing dynamically".

Many researches about ubiquitous environment like Oxygen project of MIT [2], Portolano project of Washington University [3], Aura project of CMU [4] are studied. These works focused on how to keep users away from complicated computer controlling. Daedalus project of Berkeley University [5] focused on wide overlay network which connecting buildings, cities, even nations. In these pervasive computing environments users expect to access resources and services anytime and anywhere. Users only care about service they get, not the computing itself in pervasive computing environment. For the availability, those researches focus on context awareness. With sensing user's situation, the proper service can be provided.

But, risks on security are increasing in the ubiquitous computing environment. It is well known that User's context sensing can occur the privacy problem. There are many studies on the privacy problem [6, 7, 8, 9, 10] But also, the forgery on location information is important risk in the ubiquitous environment. Forgery on location information is critical risk of context based service. When user's contexts are forged, the service may provide in proper service.

1.2 Our Contributions

Several location authentication methods were studied. Those studies focus on the authentication of user for service provider. Denning [11] proposed Differential GPS based location authentication method, while Sastry [12] proposed location authentication method using the time difference from the velocity of radio frequency and sonic. Nakanishi [13] adopted RFID for location information. And, Kindberg [14] showed general model using constrained channel with Wi-Fi, Bluetooth, and etc. But these works are only focused on authentication of location information, there is no consideration of privacy of user.

We generalize the risks in the location based service model, and define security requirements in this paper. We also introduce new model of location authentication method which can be adopted in universal. Based on the model, we propose several protocol using asymmetric/symmetric key encryption and one-time key or timestamp. Also, we show the application model of location authentication.

1.3 Outline of the Thesis

The remainder of the thesis is organized as follows: In Chapter 2, we describe risks on location based services in the aspect of security at first and describe several previous works. In Chapter 3 we introduce our model and propose several schemes. In Chapter 4 we analyze the security of our protocols. In Chapter 5 we show the DRM model of location authentication.

Chapter 2
Risks on Location Based Services

2.1 Location Based Service Model

Location is the context most related in ubiquitous computing environments. Several examples follow.

2.1.1 Taxi Calling Service

Divyan proposed taxi calling service scenario in [15]. In the scenario, a user wants to catch a taxi. The user request to a taxi center that his position. The center find the nearest taxi from the user. When the center finds the proper taxi, the taxi get the user's location information and arrive at the user's location.

2.1.2 Content Distribution

K. Han proposed digital content distribution scenario in [16]. In the scenario, a user wants to buy a music from online store. The store ask the user where he located currently. The user send his location information to the store. The store transfer to the user i f the condition holds. (In real, each country has the different rule about contents. For example, Japanese music was prohibited in Korea until recent years.)

2.1.3 Company's Critical Information Access Control

A company want to keep the critical marketing information in secret. Even employees of the company cannot access that information, also low-level managers. To keep the secret perfectly, the information can be accessed only in the company building. When the manager want to access that information, the manager send his/her location information to server. Even the legitimate user cannot access from outside of building.

Figure 2.1: Location based service model

2.2 Risks on Location Based Service

Most of all, service provider has to be able to verify user's location. *(Authentication)*. As cases above, users will inform their location to service provider, and some of users will forge their location to cheat their real status. *(Unforgeability)* Also, it is possible to think that any adversary forge user's location. *(Unforgeability)* When the user succeed to be authenticated by service provider with the location, the user probably try to re-use accepted parameter. *(Unreusable)*

Adversaries can try to track user's moving by catching user's location. *(Privacy)* And User want to reveal only sufficient location information to service provider. *(Privacy)*

Of course, the message transmitting to service provider can be eavesdropped by the adversary. *(Confidentiality)*

We analyzed security requirements as following section.

2.3 Security Requirements

We define security requirements for the risks as following.

1. *Authentication* of location : Service provider can verify user's location.

2. *Privacy* of user from Attacker : Attacker cannot know user's location.

3. *Privacy* of user from Service provider : Service provider only knows sufficient location information of user.

4. *Confidentiality* of message : Attacker cannot know the message.

5. *Un-forgeability* of location from Attacker : Attacker cannot forge user's location

6. *Un-forgeability* of location from User : User cannot forge user's location

2.4 Related Works

2.4.1 Location Sensing

In this section, we briefly describe several location sensing technologies, Trangulation, GPS, and Circket.

Trangulation

Location is established by overlaying the existing cellular network with equipment that measures aspects of the interaction between the network and the mobile device. One method in this category relies upon Time of Arrival (TOA) where the time it takes the signal to travel from the mobile device to an upgraded base station is measured and sometimes augmented with Angle of Arrival (AOA) information. A second method in this category involves the use of Trangulation between multiple base stations to compute a fix on the transmitting device. The main cost of network based location methods is the additional equipment required for base stations - between $9,000 \mathit{and} 30$,000 per cell. The cost of the upgrade is offset by two factors. First, network-based solutions work with existing cellular phones and would not require carriers to institute a mandatory upgrade policy for their subscriber base. Second, by not requiring upgrade, the carrier mitigates the risk that a subscriber will choose to change providers in search of a better service package.

GPS

The frontrunner in this category are phones equipped with Global Positioning System receiver technology embedded within the mobile unit itself. Since the required network hardware infrastructure upgrades are a fraction of the cost (10 to 25 percent) of that required by network based solutions, the initial cost to the carrier is lower. However, in order to take advantage of this type of location solution, it will be necessary for the consumer to receive a new phone, thereby exposing the carrier to the risk of losing the subscriber. Also, GPS traditionally suffers from long initial startup times of 45 to 60 seconds when the receiver has been inactive and needs to locate the necessary satellites to determine its initial position. The use of GPS, a satellite technology, is more susceptible to problems associated with line of site issues and loss of signal strength, most notably inside of buildings and "urban canyons".

Qualcomm announced the purchase of SnapTrack for $1 billion dollars thereby providing a high profile endorsement of the ability to embed GPS functionality into existing cellular phone designs. Second, the US government turned off Selective Availability (SA), the intentional degradation of the GPS signal to introduce inaccuracies in the computed location, several years earlier than expected thereby increasing the accuracy of location to within several meters. Finally, the GPS technology as developed by SnapTrack had made technical gains that addressed both the time to compute position and signal loss issues such that locations could be computed within 5-10 seconds for the initial fix even while inside of a building.

Cricket Indoor Location System [17], [18]

Location information in outdoor environments may be obtained by GPS. But in indoor environments, using GPS is usually unavailable. Cricket is location-aware application for inside building. Cricket uses a combination of RF and ultrasound technologies to provide a location-support service to users and applications. Beacons are spread through the building, publishing information on an RF signal operating in the 418MHz AM band. Listeners attached to devices and mobiles listen for RF signals, and upon receipt of the first few bits, listen for the corresponding ultrasonic pulse. When this pulse arrives, they obtain a distance estimate for the corresponding beacon. The listeners run maximum-likelihood estimators to correlate RF and ultrasound samples and to pick the best one. Cricket Compass [19] provides position (x,y,z coordinate) information and orientation (the direction at which the device is pointing) information. Cricket uses active beacons and passive listeners, which has two significant benefits. First, it is not a tracking system where a centralized controller or database receives transmissions from users and devices and tracks them. Second, it scales well as the number of devices increases; a system with active transmitters attached to devices wouldn't scale particularly well with the density of instrumented devices. Third, its decentralized architecture makes it easy to deploy. This does not mean it is hard to manage; a centralized front-end allows easy management and control. Cricket can estimate position to a few centimeters of accuracy and angles to within 3-5 degrees of the true value. It can determine which space a device is in by detecting boundaries to within about 2 feet. These combined capabilities are better than other available location systems that we know of.

2.4.2 Location Authentication Method

GPS Based Authentication [11]

Main idea is generation of 'Location Signature' using Location Signature Sensor (LSS) from GPS. They adopted differential GPS (DGPS) technique [21] for sharing the same location information between prover and verifier. Since both prover and verifier share prover's location information, forgery by prover or any attacker is impossible. But, for adopting this method, high cost in system design is most problem. Also, it is difficult to use in indoor environment.

Time-Bound Based Authentication [12]

Main idea is speed of sound and light. Physical distance can be measured by elapsed time of signal. When the elapsed time from prover to verifier is within the maximum allowed time, prover is authenticated. They proposed 'ECHO' protocol for this concept in [12]. It is lightweight protocol and available in both indoor and outdoor authentication. But physical state severally affect on the success of operation. Basic 'ECHO' protocol is following.

1. $p \longrightarrow^{radio} v \ : \ l$
2. $v \longrightarrow^{radio} p \ : \ N$
3. $p \longrightarrow^{sound} v : \ N$. v accepts iff $l \in R$ and elapsed time $time \leq d(v,l) \cdot (c^{(} - 1) + s^{-1}$

v denotes verifier, l denotes location, and N denotes nonce. s denotes speed of sound, $331m/s$, and c denotes speed of light, $3 \times 10^8 m/s$.

Figure 2.2: Time Based Location Authentication

Via Constrained Channel [14]

The basic idea is from devices has their constrained channel like Transport Layer Security (TLS) [20]. Using Bluetooth, Wi-Fi, if the authenticator has direct access to a physically constrained (e.g. range-bounded) channel, it is trivial to implement location authentication. For example, Bluetooth transceiver located at location L, within the range of transceiver, the principal can employ a challenge-response protocol.

If the authenticator does not have direct access to a physically constrained communication channel, the authenticator us a trusted channel proxy to be connected with the constrained channel.

Figure 2.3 shows the system model for location authentication via constrained channel.

Figure 2.3: Location Authentication via Constrained channel

LEXP : Location Information Exchange Protocol [13]

Protection of user's anonymity and validation of location information. Four principals are in the model, a detector, a client, a service provider, and a resolver. The detector is a detection entity, connected to an RFID-reader. The resolver is the entity which manages a mapping table between clients' RFID and IP address. Clients send their address to the resolver every time the address has changed. (Address notification). When detectors detect an RFID inside their sensing area, they request the resolver to resolve the client's address that corresponds to the RFID (Address resolution), and send a notification to the address that a ticket is available. Then the client can obtain the ticket, which is a presence evidence at the detector's sensing area. (Ticket publication) When clients are requested a ticket by a service provider, they decide whether they consume the ticket based on user's intention or a formulated policy. After service providers obtain a ticket, they request the detector, which published the ticket, to verify it. (Ticket verification)

Figure 2.4: $\mathcal{LEXP}$

2.4.3 Summary

The model of Time-bound based authentication method [12] and Authentication method via constrained channel [14] is that only a prover has his location information initially, and a verifier verifies prover using specific method like time. For that, they have to be synchronized physically, and when the communication is disconnected, it fails. Since they rely on the time variance, their methods are only be able to be used in short distance where the a little distance changing occurs big difference. And, in practical, they require large number of host (verifiers) to cover wide range for general use.

The model of LEXP [13] and GPS based authentication [11] is that prover and verifier share prover's location information. LEXP adopted RFID which is actively studied currently. Actually the service provider who wants to verify user's location doesn't have the exact location information of user, but the range of RFID is to small, it can be considered that service provider knows user's location. GPS based method used differential GPS which there two kinds of GPS receiver, one is static receiver and the other is roving receiver. When satellite transmit signal of prover's position, both prover and verifier receive the same information. From this, verifier can check if prover is valid. But those method are device specific methods that LEXP relies on RFID and GPS based method relies on Location Signature Sensor (LSS) which is built for that specific purpose.

Chapter 3

The Proposed Scheme

3.1 Model

In the model, there are three entities, a client C, a service Provider SP, and a trusted operator OP. C want to prove his location to SP, while SP wants to verify C's location information.

We discuss about sharing location information of client with operator here.

In our model, we do not consider receiving location information from location sensors like the satellite (In case of GPS), the station (In case of Trangulation) and the beacon (In case of Cricket).

In the aspect of security, attack on receiving the location information is meaningless. While location sensors like satellite broadcast signals, C and OP passively receive the message. In this case, attacker can not even know whether C and OP received the information from location sensors or not.

Figure 3.1 shows an example that a satellite broadcast signals to the large number of clients. While the satellite send the signals, some clients receive the signals, but the other clients do not receive the signals. It is like the Television broadcasting station broadcasts TV programs.

Fault resistance from inaccuracy of satellite signals or radio signals is out of focus.

Now, we introduce a basic location authentication protocol which only considers authentication of C's location.

Figure 3.1: Clients receives location from satellite

$\mathcal{BLAP}$: **Basic Location Authentication Protocol** Assume C and OP share key k_1, and OP and SP share key k_2.

1. C and OP share C's location information L_C with *LocationSensor* like DGPS [21] or Cricket [17, 18, 19].
2. OP sends $MAC_{K_1}(L), MAC_{K_2}(L_C, MAC_{K_1}(L_C))$ to U.
3. C checks $MAC_{K_2}(L_C, MAC_{K_1}(L_C))$ with $MAC_{K_1}(L_C)$ and L. If C assure that $MAC_{K_1}(L_C)$ is not forged, C continues operation.
4. C sends $MAC_{K_1}(L_C), L_C$ to SP.
5. SP check the validity of $MAC_{K_1}(L_C)$ with L_C and K_1.

Figure 3.2: Basic Location Authentication Protocol

a

U can check that $MAC_{K_1}(L)$ from OP is not forged, since U can verify $MAC_{K_2}(L, MAC_{K_1}(L)$ with $MAC_{K_1}(L), L$ and K_2. Also, SP can verify $MAC_{K_1}(L)$ with K_1. So, the requirement of $unforgeability$ from attacker holds. Since, U doesn't know K_1, U cannot forge L.

Initial key distribution to $clients, SPandOP$ follows the concept of *'resurrecting duckling'* [22]. When we assume the channel is secure and authenticated, the $confidentiality$ of message holds, but still naive.

$\mathcal{BLAP}$ still have the risk of $reuse$ of L_C by C. We will show two kinds method protecting from reuse of L_C and propose more concrete protocol with holding all security requirements later.

3.1.1 Protecting Reuse of Location Information

Key Replacement

OP and SP share K_1 for generating $MAC_{K_1}(L_C)$. When $Client$ sends L_{Client} and $MAC_{K_1}(L_C)$ to SP, OP and SP replace K_1 to new key, ${K_1}'$. Next time, ${K_1}'$ is used to generate $MAC_{{K_1}'}({L_C}')$. ${L_C}'$ is new location information of C.

An example of replacing share key K_1 between OP and SP is using PKI.

When SP request OP to change K_1, OP generates the new key $K_1^{'}$ and encrypts the key with SP's public key PK_SP. OP sends $E_{SK_SP}(K_1^{'})$ to SP, and SP decrypts it with SP's private key SK_SP.

Timestamp

When C sends C's location information L_C to L_C, SP request Timestamp TS about L_C. SP checks TS for verification of validity of L_C.

3.2 Proposed Protocol

We propose four protocols holding security requirements we analyzed; $\mathcal{AOLAP}$, $\mathcal{ATLAP}$, $\mathcal{SOLAP}$, and $\mathcal{STLAP}$.

3.2.1 $\mathcal{AOLAP}$: Asymmetric Encryption and One-time key Based Location Authentication Protocol

We propose the improved protocol using PKI. In the protocol, shared key K_1 is shared between OP and SP. When the operation is finished, K_1 is revoked and replaced to new key.
Assume a user C has private key SK_C, shares keys K_2 with OP and K_3 with SP. OP shares K_1 with SP and K_2 with U. SP has K_1, K_2 and a private key SK_SP. ID_C means the client c's identity.

1. C and OP share C's location information L_C with $LocationSensor$.

2. OP sends $E_{PK_C}(MAC_{K_1}(ID_C|L_C), MAC_{K_2}(L_C, MAC_{K_1}(ID_C|L_C)))$ to C.

3. C decrypt $E_{PK_C}(MAC_{K_1}(L_C), MAC_{K_2}(L_C, MAC_{K_1}(L_C)))$ with his/her private key SK_C, and checks $MAC_{K_2}(L_C, MAC_{K_1}(L_C))$ with $MAC_{K_1}(L_C)$ and L_C. If C assure that $MAC_{K_1}(L_C)$ is not forged, C continue operation.

4. C sends $ID_C, E_{PK_{SP}}(MAC_{K_1}(L_C), L_C)$ to SP.

5. SP check the validity of $MAC_{K_1}(L_C)$ with L_C and K_1.

6. OP and SP replace key K_1 to the new key.

Figure 3.3 shows operations of $\mathcal{AOLAP}$.

Figure 3.3: Proposed Protocol 1: $\mathcal{AOLAP}$

3.2.2 $\mathcal{ATLAP}$: Asymmetric Encryption and Timestamp Based Location Authentication Protocol

In this section, we propose location authentication protocol using timestamp TS. In this protocol, OP and SP do not need to replace the key K_1 after operation.

Assume C and OP share key K_2, and OP and SP share key K_1.

1. C and OP share C's location information L_C and timestamp TS.

2. OP sends $E_{PK_C}(MAC_{K_1}(L_C|TS), MAC_{K_2}(MAC_{K_1}(ID_C|L_C|TS)|L_C|TS))$ to C.

3. C decrypts $E_{PK_C}(MAC_{K_1}(ID_C|L_C|TS), MAC_{K_2}(MAC_{K_1}(ID_C|L_C|TS)|L_C|TS))$ with his/her private key SK_C, and checks $MAC_{K_2}(MAC_{K_1}(ID_C|L_C|TS)|L_C|TS)$ with C's ID ID_C, $MAC_{K_1}(ID_C|L_C|TS)$, L_C, and TS. If C assures that $MAC_{K_1}(ID_C|L_C|TS)$ is not forged, C continue operation.

4. C sends ID_C, $E_{PK_SP}(MAC_{K_1}(ID_C|L_C|TS), MAC_{K_2}(L_C|TS)L_C, TS)$ to SP.

5. SP check the validity of $MAC_{K_1}(ID_C|L_C|TS)$ with ID_C, L_C, TS and K_1.

Figure 3.4 shows operations of $\mathcal{ATLAP}$.

3.2.3 $\mathcal{SOLAP}$: Symmetric Encryption and One-time Key Based Location Authentication Protocol

In this section, we show the protocol based on symmetric key encryption. Assume C and OP share a key k_2, OP and SP share a key K_1, and C and SP share a key K_3.ID_C denotes C's ID, L_C denotes C's location.

1. C and OP share C's location information L_C

2. OP sends $E_{K_2}(MAC_{K_1}(ID_C|L_C), h(L_C|MAC_{K_1}(ID_C|L_C))$ to C.

3. C decrypts $E_{K_2}(MAC_{K_1}(ID_C|L_C), h(L_C|MAC_{K_1}(ID_C|L_C))$ with K_2. C checks $h(L_C|MAC_{K_1}(ID_C|L_C))$ with L_C and $MAC_{K_1}(ID_C|L_C)$. If C assure that $MAC_{K_1}(ID_C|L_C)$ is not forged, C continue operation.

4. C sends ID_C,$E_{K_3}(MAC_{K_1}(ID_C|L_C), L_C)$ to SP.

Figure 3.4: Proposed Protocol 2: $\mathcal{ATLAP}$

5. SP check the validity of $MAC_{K_1}(ID_C|L_C)$ with ID_C, L_C and K_1.

6. OP and SP replace key K_1 to the new key.

3.2.4 $\mathcal{STLAP}$: Symmetric Encryption and Timestamp Based Location Authentication Protocol

In this section, we propose the protocol using symmetric key encryption and timestamp. Assume C and OP share key k_2, OP and SP share key k_1, and C and SP share key K_3. ID_C denotes ID of C, L_C denotes location of C. TS denotes timestamp.

1. C and OP share L_C and TS.

Figure 3.5: Proposed Protocol 3: $\mathcal{SOLAP}$

2. OP sends $E_{K_2}(MAC_{K_1}(ID_C|L_C|TS), h(MAC_{K_1}(ID_C|L_C)|L_C|TS))$ to C.

3. C checks $h(MAC_{K_1}(ID_C|L_C|TS)|L_C|TS))$ with $MAC_{K_1}(ID_C|L_C|TS)$, L_C and TS. If C assure that $MAC_{K_1}(ID_C|L_C|TS)$ is not forged, C continue operation.

4. C sends $ID_C, E_{K_3}(MAC_{K_1}(ID_C|L_C|TS), L_C, TS)$ to SP.

5. SP check the validity of $MAC_{K_1}(ID_C|L_C|TS)$ with ID_C, L_C, TS and K_1.

Figure 3.6 shows operations of protocol.

Figure 3.6: Proposed Protocol 4: $\mathcal{STLAP}$

Chapter 4
Security Analysis

4.1 Security Analysis

4.1.1 Unforgeability by Attacker

When the client C sends the encrypted message, attacker has no key. Also, with the property of hash function, Success probability of forgery by attacker is $1over2^n$ for the total message length n.

4.1.2 Unforgeability by User

Though client C generate C's fake location ${L_C}^{'}$, C cannot forge $MAC_{K_1}({L_C}^{'})$ without key K_1. Success probability of forgery by C is $1over2^{n'}$ for the MAC of location length n'.

4.1.3 Unreusability by User

Client C keeps L_C and $MAC_{K_1}(ID_C|L_C)$ for a long time, and try to use later. But, when C keeps L_C and $MAC_{K_1}(ID_C|L_C)$, SP can revoke K_1 after a time period.(*One-time key*) Or SP can check the timestamp TS. (*Timestamp*)

4.1.4 Privacy against Attacker

Attacker cannot know C's location L_C without the key. The success probability of attacker relies on the strength of encryption schemes.

4.1.5 Privacy against Verifier

Until C send location information L_C to service provider (Verifier) SP, SP has no information of C's location L_C. In practical application, L_C can be described as following figure 4.1.

In above example, Location information has five fields;nation, state, city,

Figure 4.1: Fields of Location information

street, building number. When SP require the information of **level 1**, C sends only information of nation to SP. If SP requires **level 4**, C sends all fields except building number.

In [16], the scenario of digital content distribution requires only the information of C's current 'nation'.

4.1.6 Against Relay attack

If C sends L_C to other user C', SP can check L_C from C' is invalid. Since $MAC_{K_1}(ID_C|L_C)$ is infeasible by C without key K_1. Computational infeasibility of hash function is well known property. The success probability of C' cheating SP is $1 over 2^n$ for the message length n.

4.2 Functional Analysis

4.2.1 Universality

As we discussed in chapter 3, OP and C share L_C using GPS, Trangulation, or Beacon. When SP authenticate C, C sends L_C as a message. So, we can generalize as transmitting a message with encryption.

4.2.2 Covered Range

Unlike previous works, C directly sends SP L_C. and the distance between C and SP has not important. So, there is no limits of range that SP can authenticate C in our design.

4.3 Comparison

4.3.1 Comparison among Proposed Protocols

$\mathcal{AOLAP}$ and $\mathcal{ATLAP}$ are based on asymmetric key encryption method, while $\mathcal{SOLAP}$ and $\mathcal{STLAP}$ are based on symmetric key encryption method.

Also, $\mathcal{AOLAP}$ and $\mathcal{SOLAP}$ are based on one-time key method, while $\mathcal{ATLAP}$ and $\mathcal{STLAP}$ are based on timestamp.

Table 4.1 shows the comparison among proposed protocols.

	AOLAP	ATLAP	SOLAP	STLAP
Encryption	Asymmetric	Asymmetric	Symmetric	Symmetric
Location validity	One-time key	Timestamp	One-time key	Timestamp

Table 4.1: Comparison of protocols

4.3.2 Comparison with Previous Protocols

We compare our design to other protocols. O denotes that the protocol holds the requirement in the row, X denotes that it doesn't. Table 4.2 shows the comparison with protocols. Time-bounded location authentication method

	Time-based	LEXP	GPS-based	Constrained Channels	Our Protocols
Authentication of Location	O	O	O	O	O
Unforgeability	O	O	O	O	O
Privacy against attacker	X	O	O	O	O
Privacy against SP	X	X	X	X	O
Unreusability	O	O	O	O	O
Relay attack	O	O	X	O	O
Universality	X	X	O	X	O
Covered range	Near	A few meters	Devices Specific	3,000km	No limit

Table 4.2: Comparison of protocols

[12] requires connectionless synchronization, and fails with disturbance of communication. Sound is disturbed by temperature, air pressure, and so

on. Location signature sensor method [11] requires specific devices for authentication. Compare to our protocol, for sensing location information, the efficiency is same, but generating location signature make additional overhead and devices. LEXP [13] doesn't need synchronization with verifier, but their availability is limited to RFID. Constrained channel method is just general model.

4.3.3 Computational Evaluation

In this section, we show implementation results of proposed protocols. For MAC, we used hmac and MD5 with key size 64 bit. The output size of MD5 and hmac is 128 bits. For asymmetric encryption, we used RSA. RSA key size is 1024 bits. For symmetric encryption, we used 3DES with 112 bits key size. The tested system environment is Pentium 4 2.0 GHz PC with Windows 2000. Used cryptographic library is Crypto++ 4.2. The length of client ID ID_C is 32 bits, and the length of timestamp TS is 32 bits. The length of location L_C is 160 bits. The results in the tables are average of 10 times operated results. We omitted computation of TS and key replacement. The number in the table is second.

For $\mathcal{BLAP}$, computation time was negligible. Computing $MAC_{K_2}(L_C, MAC_{K_1}(L_C))$, $MAC_{K_1}(L_C)$ was very short.

Table 4.3 shows the computation time of $\mathcal{AOLAP}$. Public key size of PK is fixed to 1024 bits. Let $A1 = MAC_{K_1}\ (ID_C|L_C)$. For $E_{PK_SP}(A1, MAC_{K_2}(L_C), L_C)$, $A1$ is considered as strings. Computation results shows the time 0.015   0.017 for encryption and decryption. Since the message size is very small, even $E_{PK_SP}(A1, MAC_{K_2}(L_C), L_C)$'s length is larger, it doesn't show any significant difference. We skip the computation of replacing share key K_1 between OP and SP.

Table 4.4 shows the computation time of $\mathcal{ATLAP}$. Let $A2 = MAC_{K_1}(ID_C|L_C|TS)$. For $E_{PK_SP}(A2, MAC_{K_2}(L_C|TS), L_C, TS)$, $A2$ is considered as strings.

	$E_{PK_C}(A1, MAC_{K_2}(A1\|L_C))$	$E_{PK_SP}(A1, MAC_{K_2}(L_C), L_C)$
Encryption	0.016	0.017
Decryption	0.015	0.016

Table 4.3: Implementation results of $\mathcal{AOLAP}$

We omit computation of TS. We consider TS as 30 bytes string here. Compare to $\mathcal{AOLAP}$, the computation time of $\mathcal{ATLAP}$ is almost same. Since the length of timestamp TS is not significant in shorter included message, as we assumed the length of TS as 30 bytes in $\mathcal{ATLAP}$. If TS is short, the computation time difference was not significantly shown.

	$E_{PK_C}(A2, MAC_{K_2}(A2\|L_C\|TS))$	$E_{PK_{SP}}(A2, MAC_{K_2}(L_C, TS), L_C, TS)$
Encryption	0.016	0.016
Decryption	0.015	0.015

Table 4.4: Implementation results of $\mathcal{ATLAP}$

Table 4.5 shows the computation time of $\mathcal{SOLAP}$. Let $A = MAC_{K_1}(ID_C|L_C)$. For $E_{K_3}(A, L_C)$, MAC_{K_1} $(ID_C|L_C)$ is considered as strings. Since it uses symmetric encryption, it is faster than asymmetric encryption method. The tested result was 10 times computed 3DES. One time computation take less than 0.001 s.

	$E_{K_2}(A, h(A\|L_C))$	$E_{K_3}(A, L_C)$
Encryption	0.016	0.016
Decryption	0.015	0.016

Table 4.5: Implementation results of $\mathcal{SOLAP}$

Table 4.6 shows the computation time of $\mathcal{STLAP}$. Let $A = MAC_{K_1}(ID_C|$

$L_C|TS)$. For $E_{K_3}(A, L_C|TS)$, $MAC_{K_1}(ID_C|L_C|TS)$ is considered as strings. The difference from $\mathcal{SOLAP}$ is the message length is longer with addition of TS. But it doesn't show any significant effect on the computation.

	$E_{K_2}(A, h(A\|L_C\|TS))$	$E_{K_3}(A, L_C, TS)$
Encryption	0.017	0.017
Decryption	0.016	0.017

Table 4.6: Implementation results of $\mathcal{STLAP}$

While computation time of $ATLAP$ and $STLAP$ are bigger than $AOLAP$ and $SOLAP$. Actually, the message size may be reduced for practical use. We enlarged the message sizes intentionally for significant comparison. We show the comparison in the table 4.7. The table 4.7 shows the computation time in each step. We omit the computation in step 1 and step 6, since it is the same procedure in step 1 and step 6 requires only communication between OP and SP. The unit is second.

Protocol	$\mathcal{BLAP}$	$\mathcal{AOLAP}$	$\mathcal{ATLAP}$	$\mathcal{SOLAP}$	$\mathcal{STLAP}$
Step 2	N/A	0.016	0.016	0.0016	0.0017
Step 3	N/A	0.015	0.015	0.0015	0.0016
Step 4	N/A	0.017	0.016	0.0016	0.0017
Step 5	N/A	0.016	0.016	0.0016	0.0017

Table 4.7: Implementation results of $\mathcal{STLAP}$

Since those implementation is done by the PC, the time will take longer in handheld devices. But, the result shows that the computation cost is not high. For the further works, we need to apply optimized encryption methods. Light weight algorithms may reduce computation times.

Chapter 5

On the Design of Secure DRM in Ubiquitous Environment

5.1 Overview

In this chapter, we shows how our protocol is applicable to user access control for digital right management (DRM) based on location authentication in ubiquitous computing environment.

When the user once registers to the content provider, he purchases wants to access the digital contents, he can purchase the permission for contents without any complicated procedure. The property of ubiquitous computing, 'any time, any where' makes protecting the right of distribution of digital contents more difficult.

Many researches on DRM are focused on the relation between a contents distributor and a user, a contents creator and a distributor, and so on. Early research on DRM is from IMPRIMATUR project [23] in 1995 (end in 1998), which studied the design of generic business model, watermarking, and so on. Their model is early business model of MPEG-21 [24]. [25] project in 1998 (end in 2000) formalized basic architecture of DRM. Their work is continued in MPEG-21. MPEG-21 proposes general DRM framework. AAP (American Association of Publishers) and CNRI (Corporation for National Research Initiatives) proposed DOI (Digital Object Identifier) [26]. From 1999, AAP proposed ONIX (Online Information eXchange) [27] which is based on INDECS and focusing distribution of e-book contents. They focus on the protection of illegal use of content from invalid user. They concerns about payment, that only payed customer can use the digital content.

In the ubiquitous computing environment, it is important to concern about the right of content distribution. In real world, Local music distributors have the right of distribution in their location, while other distributors, even the content owner cannot distribute the music. For example, when a japanese distributor has the license of a korean music album, only he can sell that album in japan, and the right of distribution is protected by law. In case of digital contents, it is difficult to protect the right of distribution, since digital contents are distributed via the network. Current client-server model can protect the right from the registration of user. When a user register to a distributor, the user submits his detailed information of address, age, and so on. When the user purchase a content, the content distributer authenticate the user and send the license of the content to user. Figure 5.1 shows how a user contact a content distributer in client-server environment.

Figure 5.1: Communication in client-server environment

But, it is more difficult in the ubiquitous computing environment, since users do not directly contact the content distributer by themselves. Users delegate their role of contacting to agent [28, 29]. Users just request the content to the agent, and the agent search the content distributer. The agent contact the content distributer and get the license for the user. Details of the agent is out of focus in this thesis.

Figure 5.2: Communication in ubiquitous computing environment

Figure 5.2 shows how user contact content distributer via agent in ubiquitous computing environment. In this case, it is important to know the user's location, since only the content distributer in the same location with the user currently can distribute the license of the content.

Here, we show the scenarios of content distribution in ubiquitous computing environments and also propose the protocol of content distribution in the following section.

5.1.1 Scenarios

Assume Alice wants to get the service. She requests the agent the service.

Purchasing - self use Alice purchase contents for himself. She request and then agent check content distributer and her location. Agent checks her location and location of content provider. After that agent proceed purchasing for Alice. In the figure 5.3, (1) shows the purchasing procedure.

Transferring license Alice transfer license of content to Bob. She requests to transfer his license of the content to Bob. Agent checks Alice and Bob's location. If both are in the same location, proceed transferring the license to Bob and revoke Alice's license. In the figure 5.3, in case of (2), Alice can transfer the license to Bob, but in case of (3), it is not allowed.

Purchasing - for others Alice purchase contents for Bob. Alice requests for Bob. Agent checks Bob's location and find the content provider in the same location. Agent proceeds purchasing, this is receiving payment from Alice, and transfer Bob the license. In the figure 5.3, (4) shows the purchasing procedure between the different regions.

Figure 5.3: DRM scenarios in the ubicomp

5.2 Proposed Protocol

We show content distribution model based on location. General procedures like purchasing after checking user's location are assumed to be followed by existing DRM standards [24]. We denote *Purchasing* for the process of purchasing in existing DRM.

Assume there are **user 1**, **user 2**, **agent**, and **content distributer**. **agent** denotes the mobile agents who are delegated by users and control the the access in the ubiquitous network. More details are in [28, 29].

Step 1 **User 1** request **'Purchase'** for **'User 1'**, **'Purchase'** for **'User 2'**, or **'Transfer'** to **'User 2'**. **Agent** checks **user 1**'s location and find the region of the location.

Step 2 From **step 1**, if the request is for **'user 2'**, **agent** checks **user 2**'s location and find the region of the location.

Step 3 From **step 2**, if the request is **'Transfer'**, **agent** checks if the region of **user 1** and that of **user 2** is same. Then **agent** let **user 1** transfer the license to **user 2**. If they are different, **agent** rejects the request.

Step 4 From **step 2**, if the request is **'Purchase'**, **agent** finds **content distributer** in the same region with **user 2**, and proceed *'Purchasing'*.

Step 5 From **step 1**, if the request is for **'user 1'**, **agent** finds **content distributer** in the same region with **user 1**, and proceed *'Purchasing'*.

Figure 5.4 shows, the structures in proposed design. Each number in the figure denote steps in the proposed protocol. We assume **Location DB** in the design, which stores regional information of the location. When users request authenticate their location, the agent checks regions for those location. In the figure, for example, Seoul, Daejeon, and Incheon are in the region 1, while Tokyo is in the region 2. Comparing the regions from requests, the agent can decide permissions.

Figure 5.4: Procedures in Design

With checking the location information of user, our protocol protects the content distribution over different location. Also, our protocol allows content distribution in the same location, purchasing and transferring contents.

5.2.1 Summary

We showed a new DRM model in ubiquitous computing environment. We extended current DRM models whose researches were focused on the secure transaction among the different entities like content creator, content distributor, user(customer), and so on. We added the new concept of locality which protects local distributor's right on digital contents. We believe that our location based access control model will solve the region problem of digital content distribution.

Chapter 6
Conclusion

In this thesis, we showed why location authentication in ubiquitous computing environments is important and showed several important studies focus on location authentication. And then, we analyzed security requirements in location authentication.

We proved that it is impossible for a verifier to authenticate a prover's location without knowing some information of prover's location when there are only two entities, prover and verifier. Also, we argued that prover's privacy about location against verifier is important. To achieve the authentication of location and the privacy or prover, we introduced a trusted entity, $Operater$. We introduced our framework and introduced several protocols based on that framework. Finally, we proved that our design meets all security requirements we analyzed.

Significant difference from previous studies is that we do not require any synchronized communication between the prover and the verifier. Between two, the location information is transferred as typical message. Therefore, our design does not rely on any specific devices like LSS [11], signaling [12] and RFID [13].

We believe that authentication of context information is critical issue in ubiquitous computing environments and our model is most applicable solution for this issue.

유비쿼터스 환경에서의 위치 정보에 대한 인증 기법

한규석

유비쿼터스 환경에서 사용자의 가용성은 무선 네트워크를 통해 최대화된다. 사용자는 언제 어디서나 시간과 공간에 제약을 받지 않고 적절한 서비스를 얻게 된다. 사용자는 컴퓨팅 자체에 신경을 쓰지 않으며, 사용자의 환경 정보에 기초한 적절한 서비스를 제공받게 된다.

그러나, 사용자의 편의성 증대에 대해 보안 위협도 역시 증가한다. 사용자의 환경 정보의 인식은 사용자의 프라이버시 문제를 야기한다. 사용자의 프라이버시 문제 외에, 사용자의 환경 정보의 변조를 통한 부적절한 서비스 제공의 위협 역시 발생한다.

사용자의 위치 정보 인증 문제는 환경 정보 기반 서비스에서 가장 중요한 문제이다. 위치 정보 인증에 대한 여러 연구가 진행되어 왔다. Denning [11]은 Differential GPS 기반의 위치 정보 인증 기법을 제안했다. Sastry [?]은 음파와 전파 속도를 기반으로 도달 거리에 따른 시간을 통한 기법을 제안했다. Nakanishi [13]는 RFID를 통한 위치 정보 인증 기법을 제안했으며, Kindberg [14]은 Wi-Fi, Bluetooth, IrDA 등의 하드웨어 접속 방법을 통한 집중 채널을 사용한 일반 모델을 제시했다. 그러나 이러한 방식은 위치 정보 인증에 대해서만 고려하고 있으며, 사용자의 프라이버시 보호에 대한 고려는 취약하다. 게다가, 이러한 방식들은 특정한 하드웨어 설비를 요구하며, 일반적인 모델로 적용하기에는 부적합하다.

본 논문에서는 먼저 이러한 위치 정보 기반 서비스 모델에 대한 설명과, 이에 대한 보안 취약점 및 요구 사항을 분석한 후, 기존 연구의 취약점을 소개한다. 그 후, 우리의 모델을 소개한 후, 대칭키 기반, 공개키 기반 암호 기법, 일회용 키 및 Timestamp를 사용한 몇가지 프로토콜을 제안하며, 이에 대한 보안 분석을 하며, 이런 위치 정보 인증을 응용하는 디지털 컨텐츠 유

통 관리 시나리오를 소개한다.

References

1. M. Weiser, "The Computer for the Twenty-First Century", in Scientific American, Sep. 1991, pp. 94-104
2. Project Oxygen, MIT, http://oxygen.lcs.mit.edu
3. Project Portolano, Washington University, http://portolano.cs. washington.edu/
4. Project Aura, CMU, http://www-2.cs.cmu.edu/ aura/
5. Project Daedalus, Berkeley University, http://daedalus.cs.berkeley.edu/
6. J. Al-Muhtadi, A. Ranganathan, R. Campbell, M. D. Mickunas, "A Flexible, Privacy-Preserving Authentication Framework for Ubiquitous Computing Environments", Proc. of the 22nd ICDCSW'02, 2002
7. J. Al-Muhtadi, R. Campbell, A. Kapadia, M.D. Mickunas, and S. Yi, "Routing through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments,", Proc. of ICDCS'02
8. J. Al-Muhtadi, R. Campbell, A. Kapadia, M. D. Mickunas, and S. Yi, "Routing through The Mist: Design and Implementation, ", UIUC Technical Report UIUCDCS-R-2002-2267
9. P. G. McLean, "A secure pervasive environment", Australasian Information Security Workshop 2003
10. A. Novobilski, "Pervasive/Invasive Computing; Two sides of the location-enabled coin", March 11, 2002

11. D. E. Denning and P. F. Macdoran, “Location-Based Authentication: Grounding Cyberspace for Better Security”, Computer Fraud & Security, Feb, 1996

12. N. Sastry, U. Shankar, D. Wagner, “Secure Verification of Location Claims”, WiSE’03, Sep 19, 2003, San Diego, California, USA, ACM 1-58113-769-9/03/0009

13. K. Nakanishi, J. Nakazawa, “LEXP: Preserving User Privacy and Certifying the Location Information”, H. Tokuda, Security workshop of Ubicomp 2003

14. T. Kindberg and K. Zhang, “Context Authentication Using Constrained Channels”, HPL-2001-84, Hewlett-Packard, Apr 2, 2001

15. K. M. Divyan, and *et al.*, “A Secure and Privacy Enhanced Location-based service transaction protocol in ubiquitous computing environment”, SCIS04, vol. 1/2, pp.931 936, Jan. 27 30, 2004, Sendai, Japan.

16. K. Han, and *et al.*, “On the design of secure DRM in ubiquitous environment”, KIISC Youngnam branch workshop, Feb. 20, 2004. Kyungil univ., Kyungsan.

17. N. B. Priyantha, A. Chakraborty, H. Balakrishnan, “The Cricket Location-Support system”, Proc. of 6th ACM MOBICOM, Boston, MA, Aug 2000

18. H. Balakrishnan, R. Baliga, D. Curtis, M. Goraczko, A. Miu, N. B. Priyantha, A. Smith, K. Steele, S. Teller, K. Wang, “Lessons from Developing and DEploying the Cricket Indoor Location System”, Nov 2003, Preprint

19. N. B. Priyantha, A. Miu, H. Balakrishnan, S. Teller, "The Cricket Compass for Context-Aware Mobile Applications", Proc. of 7th ACM MOBICOM, Rome, Italy, Jul 2001

20. T. Dierks and C. Allen, "Transport Layer Security", RFC2246, www.ietf.org, 1999

21. "Differential GPS", GPS Tutor, http://www.mercat.com/QUEST/DGPS.htm

22. F. Stajano, and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks", Security Protocols, 7th International Workshop Proceedings, LNCS, 1999

23. Project IMPRIMATUR. The Project is finished in 1998, and its work is being carried forward by Imprimatur Services Ltd. All publications are available here. http://www.imprimatur.net

24. ISO/IEC JTC1/SC29/WG11/N5231

25. An international initiative of rights owners creating metadata standards for e-commerce, http://www.indecs.org/

26. William Y. Arms, "Digital Object Identifiers (DOIs) and Clifford Lynch's five questions on identifiers". ARL Newsletter, October 1997.

27. Now supported by EDItEUR, http://www.editeur.org/

28. Lampson, B., Abadi, M., Burrows, M. and Wobber, E., "Authentication in distributed systems: Theory and practice", ACM Transactions on Computer Systems, 10(4):265-310, 1992

29. Q. He, *et al.*, "A practical study on security of agent-based ubiquitous computing", AAMAS 2002, LNAI 2631, pp.194-208,2003

Acknowledgements

First and foremost I would like to thank my academic advisor Prof. Kwangjo Kim 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 are due to Prof. Myung Chul Kim and Dr. So Ran Ine for their generosity and serving in my thesis committee.

I would also like to thank Dr. Chan Yeop Yeun for discussion and advise of thesis. This thesis is the result from our discussion during his visiting ICU.

Also, I would like to thank all members of cryptology and information security laboratory: Zeen Kim, Jungkyu Yang, Hyunrok Lee, Seokkyu Kang, Jaemin Park, Sang Sin Lee, Vo Duc Lim and Dang Ngyen Duc from Vietnam, Ren Kui and Wang Ping from China, and Divyan from India, for giving me lots of interests and good advices during the course of my study. I also thank Jeongmi Choi for helpful support as a staff member.

In addition, I would like to thank the graduates: Myungsun Kim, Jongseong Kim, Wooseok Ham, Hyungki Choi, and Jungyeon Lee for their everlasting guidance in life and study of ICU and I want to present my sincere gratitude to Sangbae Park of HCI lab., Jihyun Lee of GTA lab and Juhyung Lee of LIT lab.

My biggest gratitude goes to my parents for their endless concerns and devotional affection. I cannot forget their trust and encouragement on me. And, my two brothers and doggy soondoong, thank you. God bless my family to be happy forever.

Curriculum Vitae

Name : Kyusuk Han

Date of Birth : Jan. 23. 1978

Sex : Male

Nationality : Korean

Education

1996.3–2001.2	Mechanical Engineering Hongik University (B.A.)
2001.6–2004.6	Cryptology and Information Security, Engineering Information and Communications University (M.S.)

Career

2003.7–	Graduate Research Assistant Ubiquitous System Security Technology: Protecting Digital Contents from Illegal Use NITZ Co.
2004.3–	Gifted Students Teaching Assistant Education Program for gifted students Education Research Center for the Gifted in IT School of Engineering, ICU

2002.2–2003.2	Graduate Research Assistant A Middleware Architecture for Virtual Community Service Electronics and Telecommunications Research Institute(ETRI)
2004.4–	Graduate Research Assistant A Group-Aware Middleware Infrastructure for Active Surroundings Electronics and Telecommunications Research Institute(ETRI)
2001.6–2004.2	Graduate Research Assistant Cultivation of Top Level IT Security Manpower The Ministry of Information and Communications(MIC)

Academic Experience

2001.6–	KIISC (Korea Institute of Information Security and Cryptology) student member

Publications

(1) 2004.4	Songwon Lee, Kyusuk Han, Seokkyu Kang, Kwangjo Kim, and So Ran Ine, "Threshold Password- Authenticated Key Retrieval Protocol Using Bilinear Pairings", Accepted by 1st European PKI Workshop, Samos island, Greece, June 25-26, 2004.

(2) 2004.2 Kyusuk Han, Songwon Lee, Kwangjo Kim, and So Ran Ine, "On the design of secure DRM in ubiquitous environment", KIISC Youngnam Branch Workshop 2004, Kyungil Univ., Kyungsan, Feb 2, 2004.

(3) 2003.2 Kyusuk Han, Fangguo Zhang, Jongseong Kim and Kwangjo Kim, "A Secure Testment Revealing Protocol", SCIS2003, vol 1/2 pp 399 404, Itaya, Japan, Jan.26 29, 2003.