# Renewal of Pre-shared Key for Secure Communication of Multiple Mobile Terminals through Broadcast Data Distribution Systems

Hirosato Tsuji[*,**], Takeshi Yoneda[**], Tadanori Mizuno[***] and Masakatsu Nishigaki[***]

[*]Graduate School of Science and Engineering, Shizuoka University, Japan
[**]Information Technology R&D Center, Mitsubishi Electric Corporation, Japan
[***]Graduate School of Science and Technology, Shizuoka University, Japan
Tsuji.Hirosato@bp.MitsubishiElectric.co.jp, Yoneda.Takeshi@ak.MitsubishiElectric.co.jp,
nisigaki@inf.shizuoka.ac.jp, mizuno@mizulab.net

***Abstract*** - To perform the secure communication of multiple mobile terminals (i.e. secure unicast communication or secure multicast communication), the encryption key should be shared among the terminals that join the communication. In such a case, if the same encryption key would be repeatly used, the key disclosure from the stolen terminal might cause the wire tapping and decryption of the encrypted communication. To minimize the risk of the disclosure, the renewal of pre-shared key must be operated. In this paper, we propose the renewal method of pre-shared key for secure communication of multiple mobile terminals. In this method, each terminal will renew its pre-shared key by one-way function (e.g. hash function) according to the instruction from the management server. We also apply the proposed method to the secure communication systems between multiple mobile terminals where the key renewal commands from the system management server to each mobile terminal is distributed through the broadcast data distribution systems.

***Keywords***: Secure Communication, Mobile Computing, Pre-shared Key Cryptography, Key Renewal, Broadcast Data Distribution Systems

## 1 INTRODUCTION

The evolution of mobile communication terminals and mobile networks enables the real-time communication using these devices. To protect against the unauthorized disclosure (i.e. wire tapping) of the communication between these terminals, the end-to-end encryption between mobiles is required. In addition, if the terminal is lost or stolen, the unauthorized use of such terminals, the decryption of encrypted communications using the stolen key from such terminals, the leakage of confidential information in such terminals should be also prevented. We've proposed the method of key/device management to realize the secure real-time communication in worldwide mobile environment [1]. In this method, the end-to-end encryption keys are frequently generated on the system management server and distributed to each terminal using one-way communication, such as the digital broadcast data distribution systems. In case of the loss or robbery of terminals, the encryption keys and the secret information will be erased and the terminal will be initialized by the remote control from the system management server. We've designed the protocol that realizes the management of encryption keys as well as the management of mobile terminals. As a result, we've confirmed that the sharing/updating encryption keys are achieved without any operation of the mobile terminal users. We've also confirmed that the lost/stolen terminal is excluded by the remote operation command of system management server and the cooperative action of the other terminals. In this paper, we propose the method renewal method of pre-shared key for secure communication of multiple mobile terminals. In this method, each terminal will renew its pre-shared key by one-way function (e.g. hash function) according to the instruction from the management server. We also apply the proposed pre-shared key renewal method to this system.

In section 2, we introduce the secure communication based on the pre-shared cryptography and threats to it. In section 3, we summarize the existing methods to protect against these threats. In section 4, we propose the method of the pre-shared key renewal. In section 5, we apply the proposed method to the secure real-time communication system. Finally, we conclude in section 6.

## 2 THREATS TO PRE-SHARED KEY CRYPTOGRAPHY

### 2.1 Secure Communication based on Pre-shared Cryptography

To perform the secure communication of multiple mobile terminals, the encryption key should be shared among the terminals that join the communication. The Figure 1 shows a method of sharing the encryption key based on the pre-shared key cryptography. In this method, the symmetric algorithm is used. Each mobile terminal has the same key shared in advance (i.e. pre-shared key) [2]. At the time of communication, each terminal derives the session key (i.e. encryption key) from its pre-shared key. Then the communication is encrypted by the derived encryption key [3].

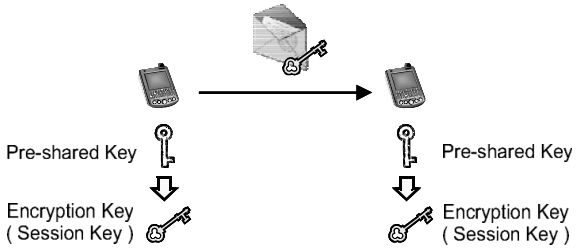


Figure 1: Secure Communication by Pre-shared Key

## 2.2 Threats from Key Disclosure

When a symmetric algorithm is used, the application of probable secure algorithms and the countermeasure against the attack on the implementation (e.g. side channel attack) are necessary [4][5][6]. They will protect against the unauthorized disclosure of the encrypted communication by the attack on the cryptographic algorithms. However, if the mobile terminal may be stolen and the encryption key can be extract from the terminal, the key disclosure might cause the following wire tapping.

**(1) Attempt to disclose past communication**
The attacker recorded the encrypted communication between terminals in advance. Then the attacker steals the one of the terminals and extracts the encryption key from it. Finally the attacker decrypts the pre-recorded communication by using the extract key.

**(2) Attempt to wiretap current/future communication**
If the terminals are used for the communication among the three or more terminals, the attacker steals one of the terminals. Then the attacker can wiretap the communication between the other terminals by using the stolen terminal. Or the attacker extracts the encryption key from the terminal in order to decrypt the communications.

The Figure 2 shows the threats to the secure communication based on the symmetric algorithm caused from the key disclosure.

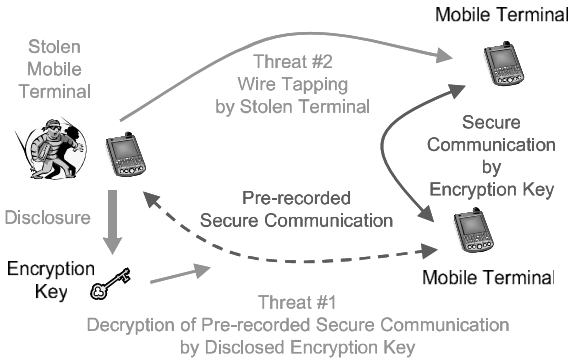


Figure 2: Threat caused from Key Disclosure

Therefore the frequent renewal of the encryption key is necessary in order to decrease the risk of the disclosure of past communications. The deletion of the encryption key in the stolen terminal should be also considered to protect against the wiretapping of the current and future communications by using such terminal.

# 3 EXISTING METHODS

## 3.1 Key Renewal Methods

There are several existing methods to renew the pre-shared key for secure communication between the mobile terminals.

**(1) Pre-sharing plenty number of keys**
The plenty number of pre-shared keys should be generated in advance. Then these keys had been pre-installed to each mobile terminal. The renewals of pre-shared key will be performed at the sufficient cycles.

**(2) Renewal Key Establishment without Servers** [2]
When the renewal of pre-shared key is required, the mobile terminals communicate each other to establish the new pre-shared keys. In general, the asymmetric algorithm is used such as RSA key transfer algorithm or Diffie-Hellman key agreement algorithm. The combination with the digital signature algorithm such as DSA signature algorithm or RSA signature algorithm is must be also performed.

**(3) Renewal Key Establishment with Servers** [7]
When the renewal of pre-shared key is required, the mobile terminals communicate to the trusted server to establish the new pre-shared keys. In general, the server acts as the key distribution center (KDC) and generates the new pre-shared keys and distributes them to each mobile terminals. The well-known implementation of KDC is the Kerberos server.

## 3.2 Terminal Management Methods

There are several existing methods to protect against the unauthorized use of the stolen mobile terminals.

**(1) User Authentication**
The mobile terminal can be protected from the unauthorized use by the user authentication functions. The authentication information may be PIN, password and the biometrics authentication information (e.g. fingerprint).

**(2) Tamper Resistant Terminal**
The extraction of keys from the mobile terminal can be protected, if the mobile terminal has the tamper resistant function. The keys will be automatically erased when the stolen mobile terminal would be illegally opened.

**(3) Remote Management from Server** [8]
The mobile terminals are managed by the management server. When the mobile terminal would be stolen, the remote operation command will be sent from the management server to the stolen terminal. Then the stolen terminal will be locked or initialized. In the latter case, the keys in the stolen terminal are erased.

# 4 PROPOSED METHOD

## 4.1 Design Policy

We propose the method of the pre-shared encryption key management for the secure communication of multiple mobile terminals. The design policies of our proposal are the followings.

**(1) Total Management by Administrator**
The management (i.e. renewal and deletion) of the pre-shared key should be performed according to the order of the system administrator. The users are not allowed to manage any pre-shared keys without the permission of the administrator.

**(2) No distribution of Renewal Key**
At the time of key renewal, the updated pre-shared key itself will not be distributed nor transferred via network.

**(3) Deletion of Key in the stolen Terminal**
In case that the loss or robbery of mobile terminal might be happen, the keys in such terminal will be deleted to avoid the unauthorized disclosure of the secure communication.

## 4.2 System Architecture

The Figure 3 shows the basic system architecture of the proposed method. The components of the system are defined as the followings.

- **User Terminal**
  A terminal that perform the secure communication with other terminals using the pre-shared key.
- **Management Server**
  A server to manage the whole pre-shared key among user terminals.
- **Pre-shared Key**
  A key shared in advance among the user terminals. The pre-shared key consists of the following elements.

| Element | Meanings |
|---|---|
| Key ID | Specify the identifier of Key |
| Key | Encryption Key |
| Generation Number | Specify the current generation of key renewal |
| Validity Period | Specify the next key renewal date/time (optional element) |

- **Key Generation Renewal Command**
  A command sent from the management server to each user terminal in order to dictate the renewal of pre-shared key. The authentication value (e.g. the digital signature or the Message Authentication Code) is added to the command for the verification.
- **Pre-shared Key Renewal Mechanism**
  A kind of cryptographic mechanism implemented on both the management server and user terminals. The input is the current pre-shared key and the output is the next generation of pre-shared key.
- **Key Deletion Command**
  A command sent from the management server to the specific user terminal in order to delete the keys in the stolen terminal. The authentication value is added to the command for the verification.

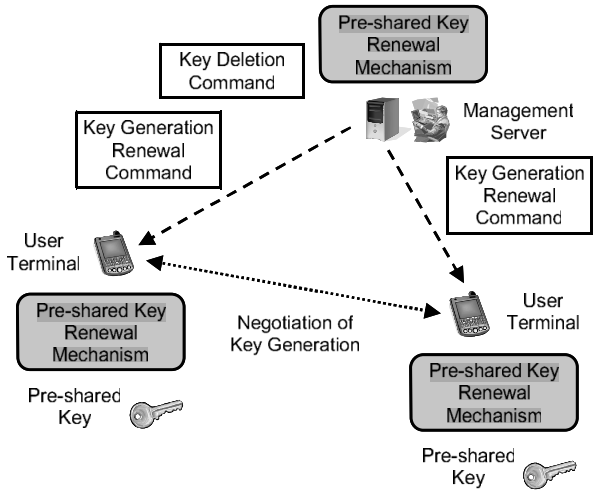


Figure 3: System Architecture of Proposed Method

## 4.3 Renewal of Pre-shared Key

The pre-shared key is renewed according to one of the following instructions.

**(1) Renewal by Key Renewal Command from Server**
The management server creates the key generation renewal command and issues it to the user terminals. The user terminal that receive the command will verify it and renew own pre-shared key.

**(2) Automatic Renewal by Key Validity Period**
The management server creates and issues the key generation renewal command with the key validity period. The user terminal will automatically renew its own pre-shared key when the key validity period would be expired.

**(3) Synchronized Renewal in case of Generation Gap**
The key generation renewal command from the management server may be lost. If it happens, the pre-shared key of the user terminal might not be renewed. When the key generation gap between the user terminals would be detected at the beginning of the secure communication, the user terminal will automatically renew the old pre-shared key for synchronization.

## 4.4 Renewal Mechanism Example

The pre-shared key renewal mechanism in both the management server and the user terminals can be implemented by using the probable secure one way functions (e.g. hush functions). The figure 4 shows the example of the implementation, where the current pre-shared key has been inputted and the next generation of pre-shared key will be outputted.


Figure 4: Pre-shared Key Renewal Mechanism

# 5 APPLICATIONS

## 5.1 Encryption Key Management through Broadcast Data Distribution Systems

We've proposed the secure real-time communication system where the pre-shared key for the end-to-end encryption between mobile terminals are generated by the system management server and are distributed through the broadcast data distribution systems in [1] (Figure 5). In this paper, we apply the proposed pre-shared key renewal method to this system.

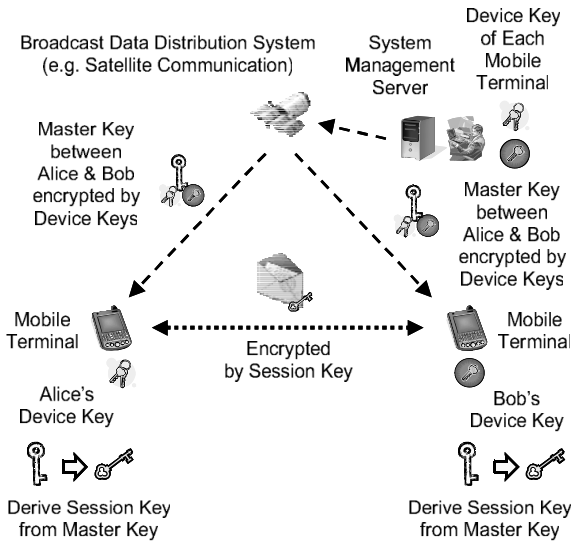


Figure 5: End-to-End Encryption Key Management through Broadcast Data Distribution Systems

This secure real-time communication system consists of the following entities/elements.

- **Mobile Terminal**
  A terminal that performs the secure real-time communication of voices and movies. To protect against the unauthorized disclosure, the end-to-end encryption is operated.
- **System Management Server**
  A trusted server that generates and distributes the pre-shared keys used for the secure communication between mobile terminals. It also orders the renewal of pre-shared keys among the mobile terminals and the deletion of keys in the stolen mobile terminal.
- **Broadcast Data Distribution System**
  A network used for the one-way communication from the system management server to each mobile terminal, such as the broadcast data distribution service using the satellite communication.

The following three types of keys are used in this system.

- **Device Key**
  A pre-shared key between each mobile terminal and the system management server. A device key is used to encrypt the commands that are sent from the system management server to each terminal. It is also used to archive integrity of the commands.
- **Master Key**
  A pre-shared key between mobile terminals that perform secure communication. An initial master key is generated in the system management server and distributed to each mobile terminal via a key distribution command.
- **Session Key**
  An encryption key between mobile terminals that perform secure communication. A session key is derived from the master key shared in advance.

## 5.2 Pre-sharing Device Key

The device keys must be shared between the system management server and each mobile terminal before the operation of the secure communication system would be started. The system management server generates the device keys for each mobile terminal. Then each device key was pre-distributed to the corresponding terminals securely. The figure 6 shows the pre-sharing device key between the system management server and the mobile terminals.

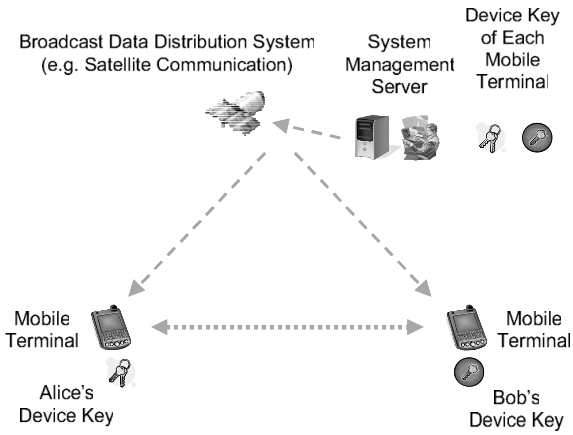


Figure 6: Pre-sharing Device Key

## 5.3 Distribution of Master Key

The system management server generates the master keys which are used for the secure communication between mobile terminals. Then the master keys are encrypted by the pre-shared device keys where the only legal terminal can decrypt the encrypted master key. Then system management server distributes the encrypted master keys via the broadcast data distribution systems to the whole mobile terminals. For example, the system management server generates the master key between Alice and Bob. The server generates the key-encryption key and encrypts the master key by the key-encryption key. The both encryptions of the key-encryption key by Alice's device key and Bob's device key are added to the master key. That is, the master key can

be only decrypted by either Alice's device key or Bob's device key. The master key for Alice and Bob is distributed through the satellite broadcast data distribution system. All mobile terminals including Carol's receive the encrypted master key, but only Alice's and Bobs' can be decrypt it. The figure 7 shows the generation and distribution of master keys.

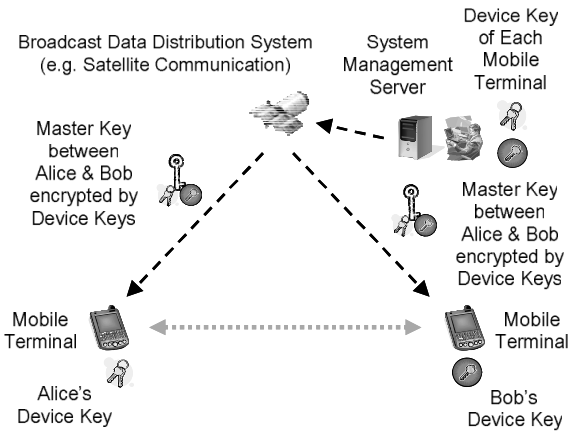


Figure 7: Generation and Distribution of Master Key

## 5.4 Generation of Session Key

At the time of secure communication, each mobile terminal derives the session key from the pre-shared master key. Then their communication is encrypted by the session key. The figure 8 shows the generation of session key and secure communication with it. The session key should be re-derived from the same master key when it would be used to encrypt/decrypt the specific number of times.

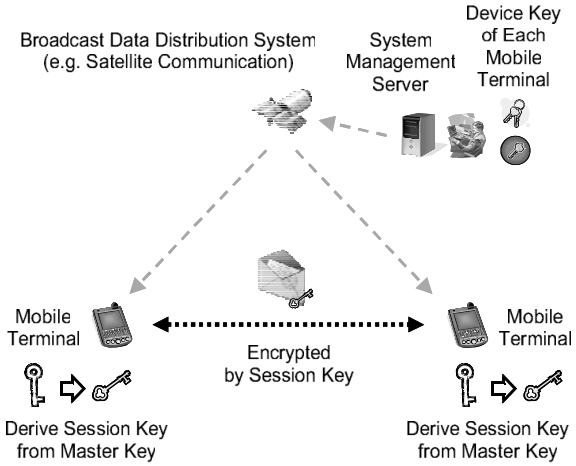


Figure 8: Generation of Session Key

## 5.5 Renewal of Device Key

The device keys are used for the one-way secure communication from the system management server to each mobile terminal. Therefore the keys should be renewed at the sufficient intervals. The renewal of device keys are operated according to the instructions described in section 4.3. The figure 9 shows the renewal of device keys by sending the device key renewal command from the system management server to each mobile terminal.

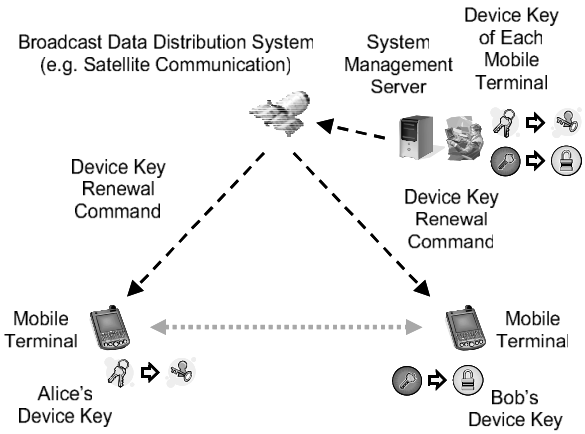


Figure 9: Renewal of Device Key

The mobile terminals will also renew the device keys when the validity of the current device key would be expired or when the generation gap of the device keys would be detected.

## 5.6 Renewal of Master Key

The master keys are used to derive the session keys (encryption keys) between mobile terminals. The master key should be renewed at the sufficient intervals. In some cases, the master keys must be renewed at every time when the new secure session would be established between the same pair of mobile terminals. Thus the renewal of master keys are operated according to the instructions described in section 4.3. The figure 10 shows the renewal of master keys by sending the master key renewal command from the system management server to each mobile terminal.

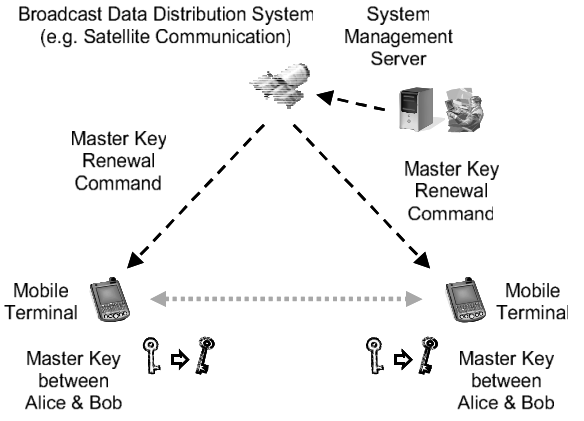


Figure 10: Renewal of Master Key (1)

The mobile terminals will also renew the master keys when the validity of the current master key would be expired or when the generation gap of the master keys would be detected. The figure 11 shows another renewal of master keys by the detection of generation gap between the mobile terminals.

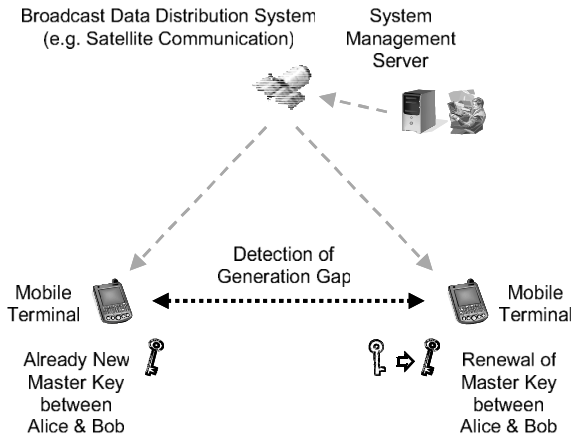


Figure 11: Renewal of Master Key (2)

The renewal of master keys may be achieved by the re-distribution of new master keys from the system management server. If the distribution of renewal key (see 3.1) may be acceptable, the new master keys might be distributed by the same procedure as mentioned in section 5.3.

### 5.7 Deletion of Keys

If the mobile terminal might be stolen, the user would report that to the system administrator. The administrator will operate the system management server in order to create the key deletion command and send it to the stolen terminal. The terminal that receives the command will delete the all cryptographic keys inside. In some cases, the initialization of the mobile terminal (the deletion of everything inside the terminal) may be performed by sending the terminal initialization command instead. The figure 12 shows the deletion of keys in the stolen terminal.

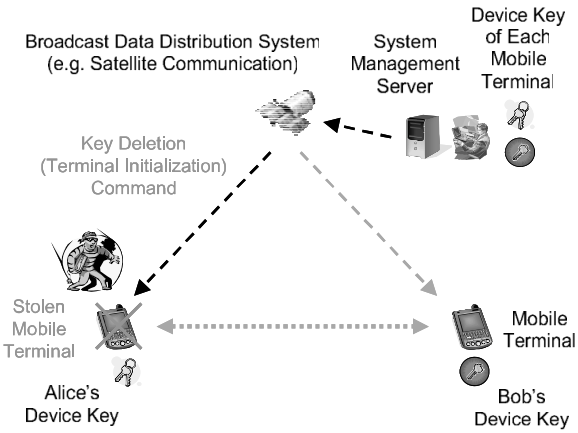


Figure 12: Deletion of Keys in stolen Terminal

## 6 CONCLUSION

In this paper, we propose the renewal method of the pre-shared key for the secure communication of multiple mobile terminals. We also apply the proposed method to the secure real-time communication systems where the management operations from the system management server to the mobile terminals are distributed through the broadcast data distribution systems. The prototype of this system is being implemented, but not completed yet [9]. We will extend our implementation to support the proposed method and evaluate its effectiveness.

## REFERENCES

[1] H.Tsuji, T.Yoneda, T.Mizuno and M.Nishigaki, Realization of Secure Real-time Communication for Worldwide Mobile Environment by Frequent Key Renewal Method through Broadcast Data Distribution Systems, IPSJ Journal Vol.50 No.9 (2009).

[2] RFC 3830, MIKEY: Multimedia Internet KEYing (2004).

[3] RFC 3711, The Secure Real-time Transport Protocol (SRTP) (2004).

[4] P.Kocher, Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS and Other Systems, CRYPTO'96 (1996).

[5] P.Kocher, J.Jaffe, B.Jun, Differential Power Analysis, CRYPTO'99 (1999).

[6] Y.Tsunoo, E.Tsujihara, K.Minematsu, H.Miyauchi, Cryptoanalysis of Block Ciphers Implemented on Computers with Cache, ISITA2002 (2002).

[7] B.C.Neuman, T.Ts'o: Kerberos: An Authentication Service for Computer Networks, IEEE Communications Magazine, Vol.32, No.9 (1994)

[8] Open Mobile Alliance: OMA Device Management Protocol, Approved Version 1.2.1 - 17 Jun 2008 (2008).

[9] H.Tsuji and T.Yoneda, Secure Mobile Phone System, Mitsubishi Electric Technical Report, Vol.82 No.5 (2008)

[10] H.Tsuji and T.Yoneda, Renewal of Pre-shared Key among Multiple Mobile Terminals, The 2009 Symposium on Cryptography and Information Security (SCIS 2009), 3D4-3 (2009).