ITU-T Kaleidoscope Conference
Innovations in NGN

A Self-Encryption Based Private Storage System over P2P Distributed File Sharing Infrastructure

Hiroki Endo
The University of Tokyo
endo@akg.t.u-tokyo.ac.jp

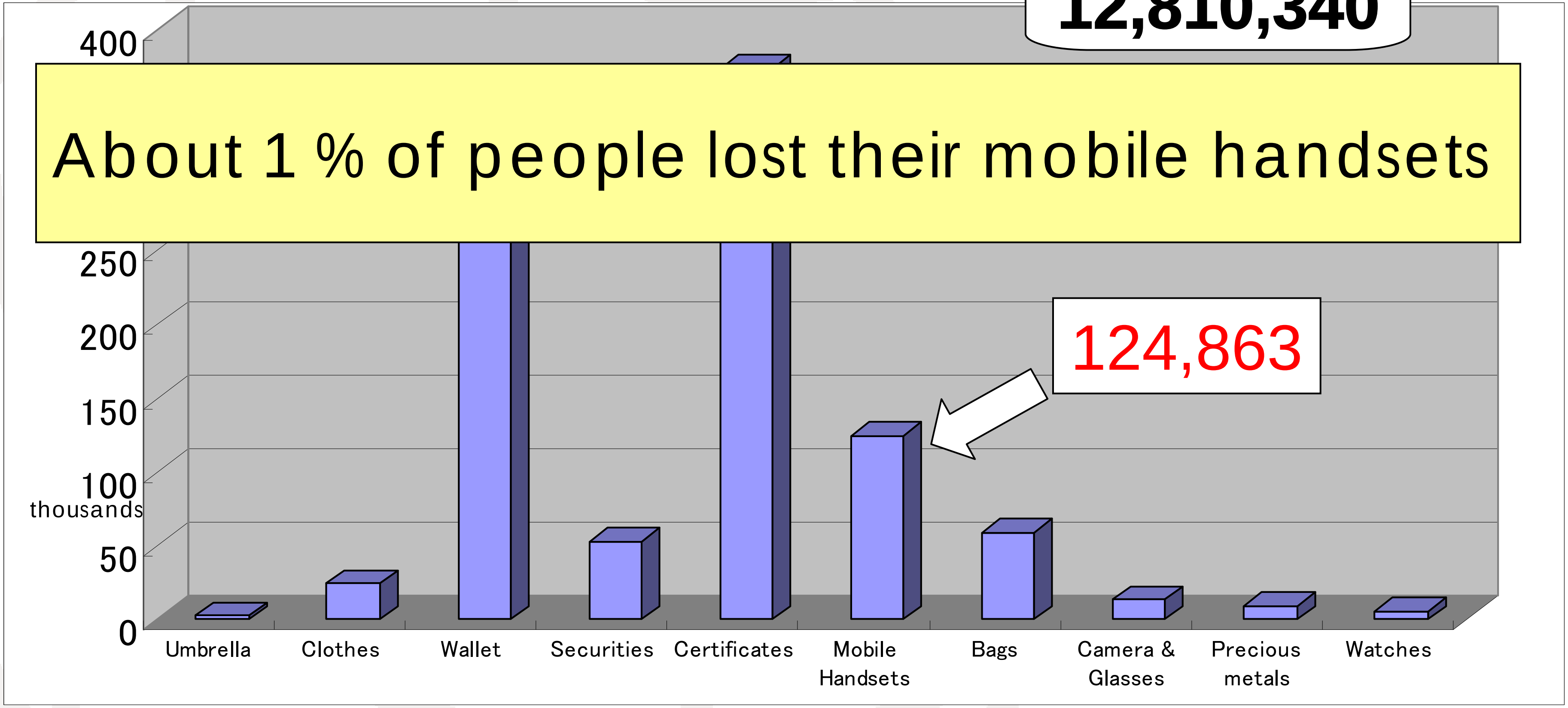
Geneva, 12-13 May 2008

Outline

- **Introduction**
  - **Security for the lost of the terminal**
- Proposal
  - Self-encryption scheme
  - Distributed Storage System by Self-encryption
- Problems
  1. Large cost for processing for encryption
  2. Large cost for Uploading data c_R
- Conclusion

Introduction

The number of the loss of articles(Tokyo, 2007)



12,810,340

About 1 % of people lost their mobile handsets

124,863

Tokyo Metropolitan Police Department
http://www.keishicho.metro.tokyo.jp/toukei/kaikei/kaikei.htm

Purpose

Mobile handsets are lost easily!

⇨ **Security for the case of loss**

- Encryption of all internal data of mobile handsets

For cases of the loss and theft

With Limited terminal resources

  - Computational resource
  - Communication resource

Outline

- Introduction
  - Security for the lost of the terminal
- **Proposal**
  - **Self-encryption scheme**
  - **Distributed Storage System by Self-encryption**
- Problems
  1. Large cost for processing for encryption
  2. Large cost for Uploading data c_R
- Conclusion

Proposal

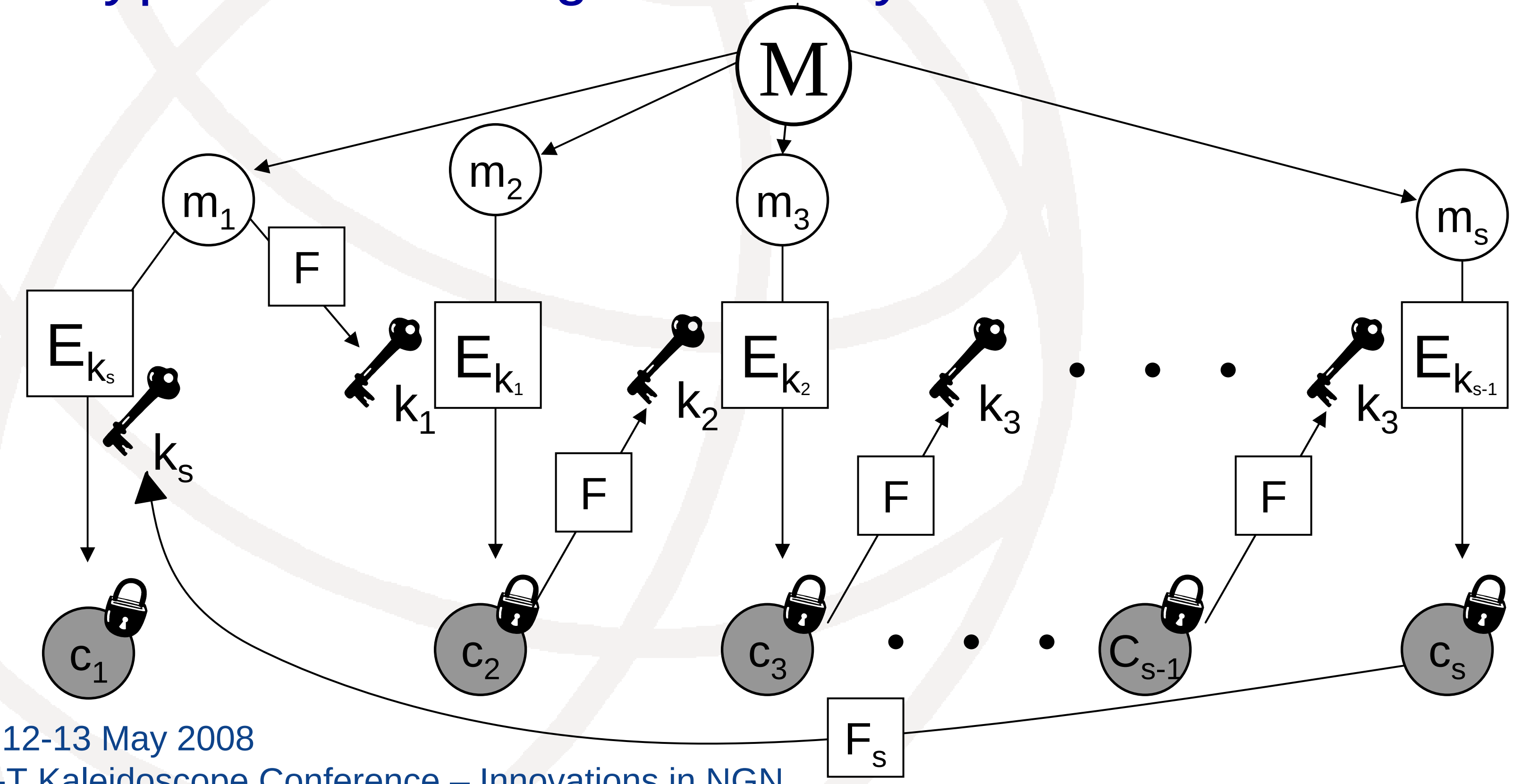
- Self-encryption scheme
  - The encryption key is generated from the information contained in the target file itself according to a certain algorithm
  - This scheme outputs some distributed data encrypted with generated keys
    - To decrypt the original file, all distributed data is required

Right **Low cost processing**

Wrong **Long encryption key**

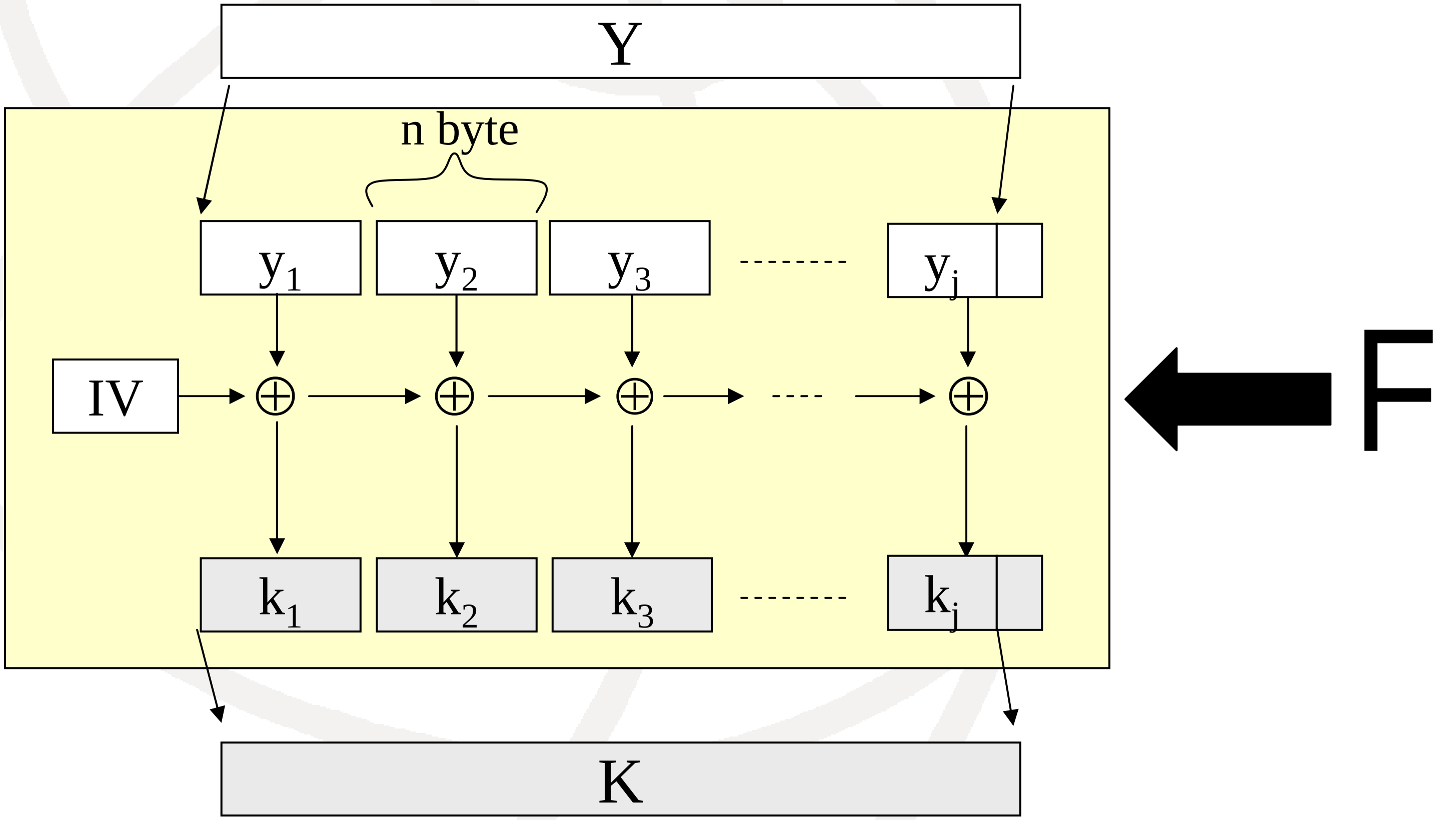
Self-encryption Scheme

- Sprit M into *s* pieces of data
- Generate *s* encryption keys from these data by Function F
- Encrypt *s* data using these keys



Key Generation Function

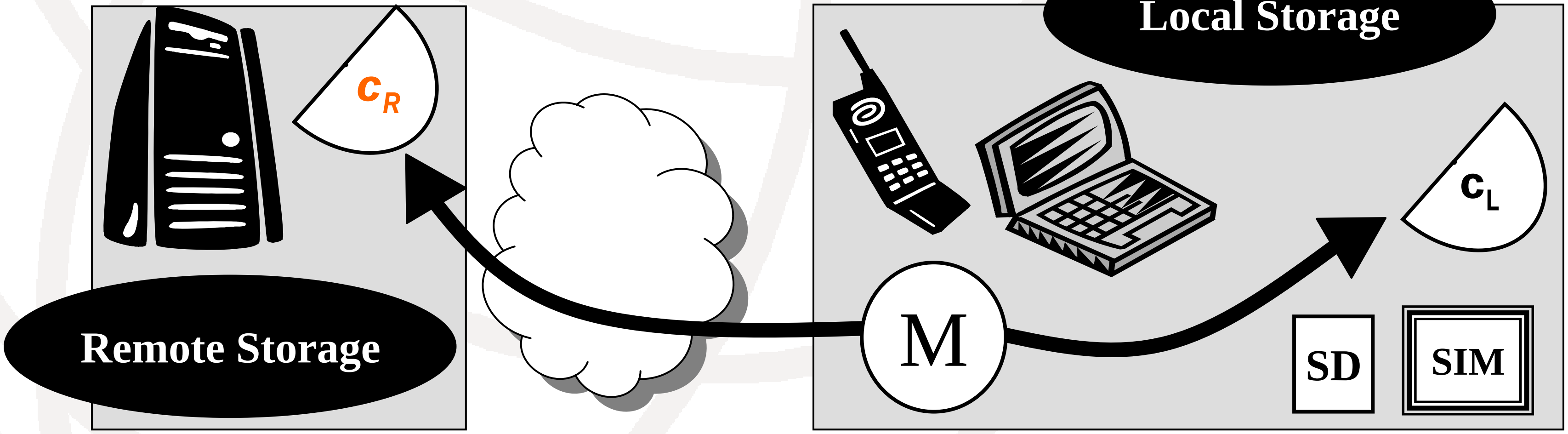
- Our proposed scrambling algorithm
- Generate key (K) from key source (Y)



⊕: exclusive OR, IV: initial value

Distributed Storage by Self-encryption scheme

- An encrypted part of file (c_R) is stored in *Remote storage*
- In cases of the loss and theft, the access to *Remote storage* is blocked
  - This system is effective even if the mobile handset is out of service!

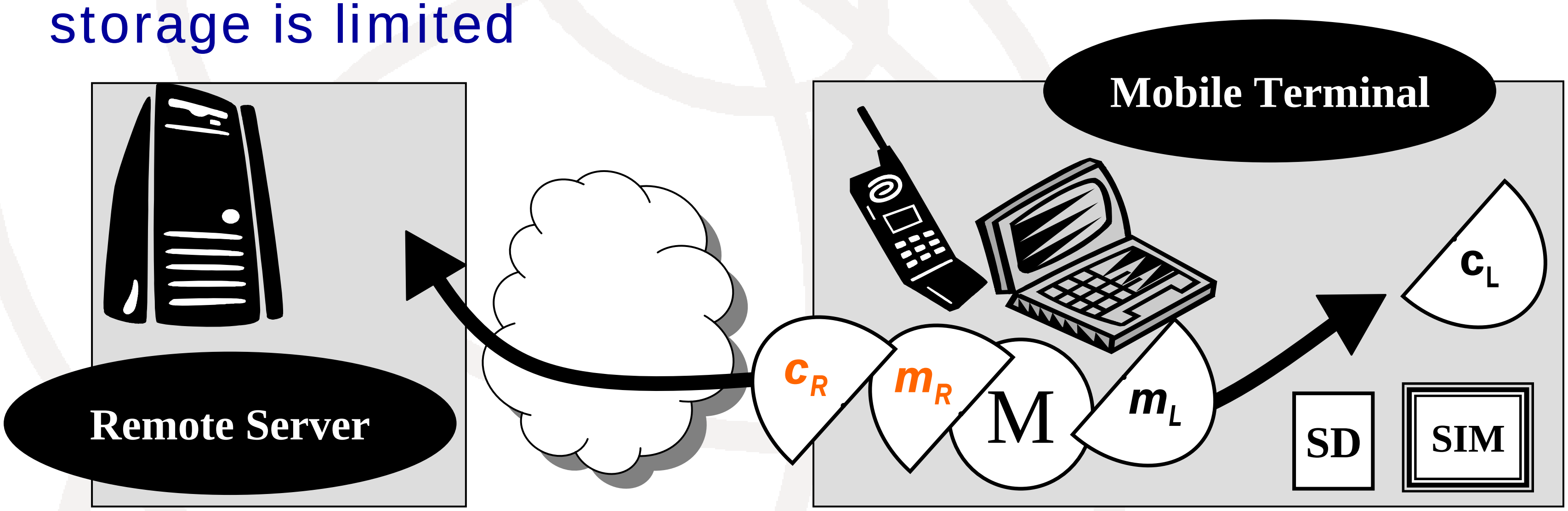


Outline

- Introduction
  - Security for the lost of the terminal
- Proposal
  - Self-encryption scheme
  - Distributed Storage System by Self-encryption
- **Problems**
  1. **Large cost for processing for encryption**
  2. **Large cost for Uploading data c_R**
- Conclusion

Problem Definitions

- An encrypted part of file (c_R) is stored in network storage
- In cases of the loss and theft, the access to Network storage is limited

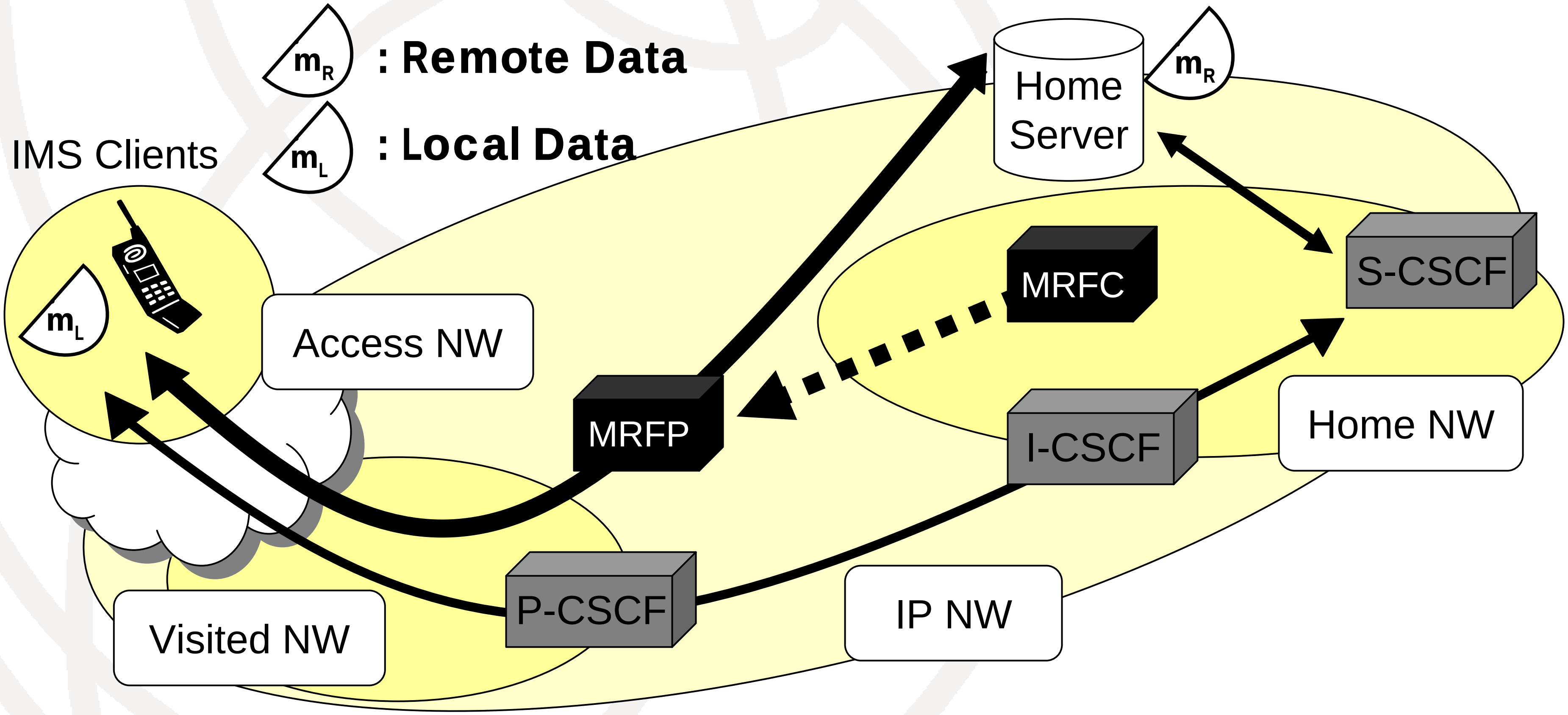


Problems

1. Large cost for processing for encryption m_L & m_R
2. Large cost for Uploading data c_R

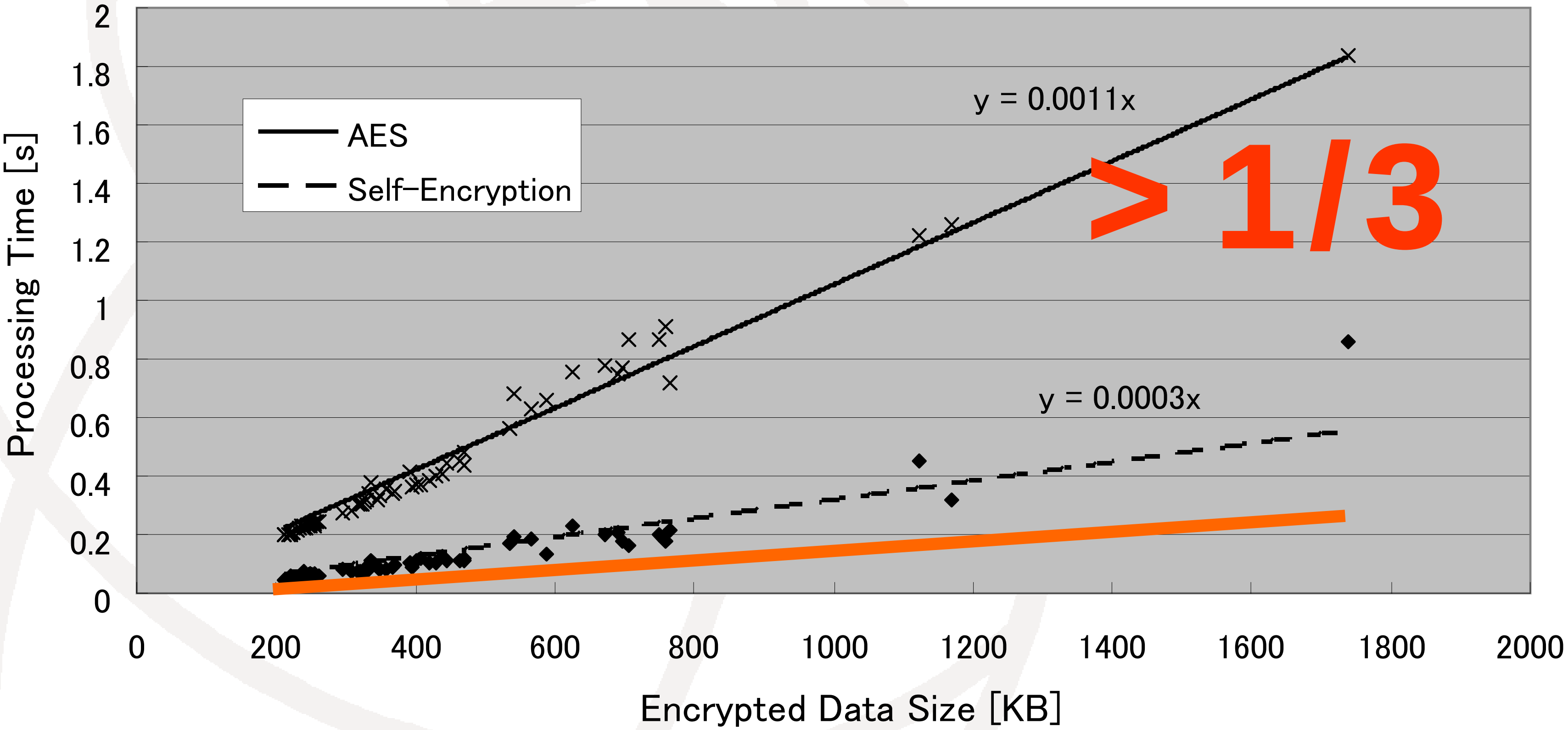
Target Environment

- Distributed Storage System Based on IMS framework
  - Communications are secure
  - Mobile terminals and Servers are authenticated



Problem *1*

- Cost for processing for encryption ***m_L*** & ***m_R***

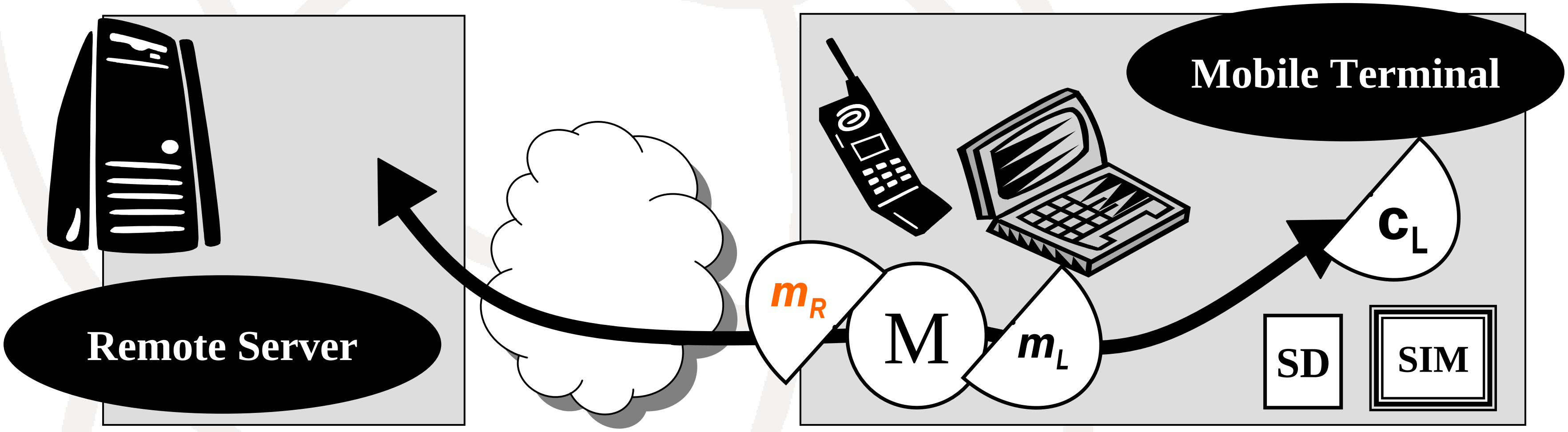


Experimental circumstance

Zaurus SL-C760, OS: Linux (OpenPDA),
CPU: Intel XScale(PXA255 400MHz), Work area: 64MB

Answer *1 (1/2)*

- Mobile terminal transmits remote data to the server in plaintext through secure pass
- The remote server encrypts the remote data stored in the network storage

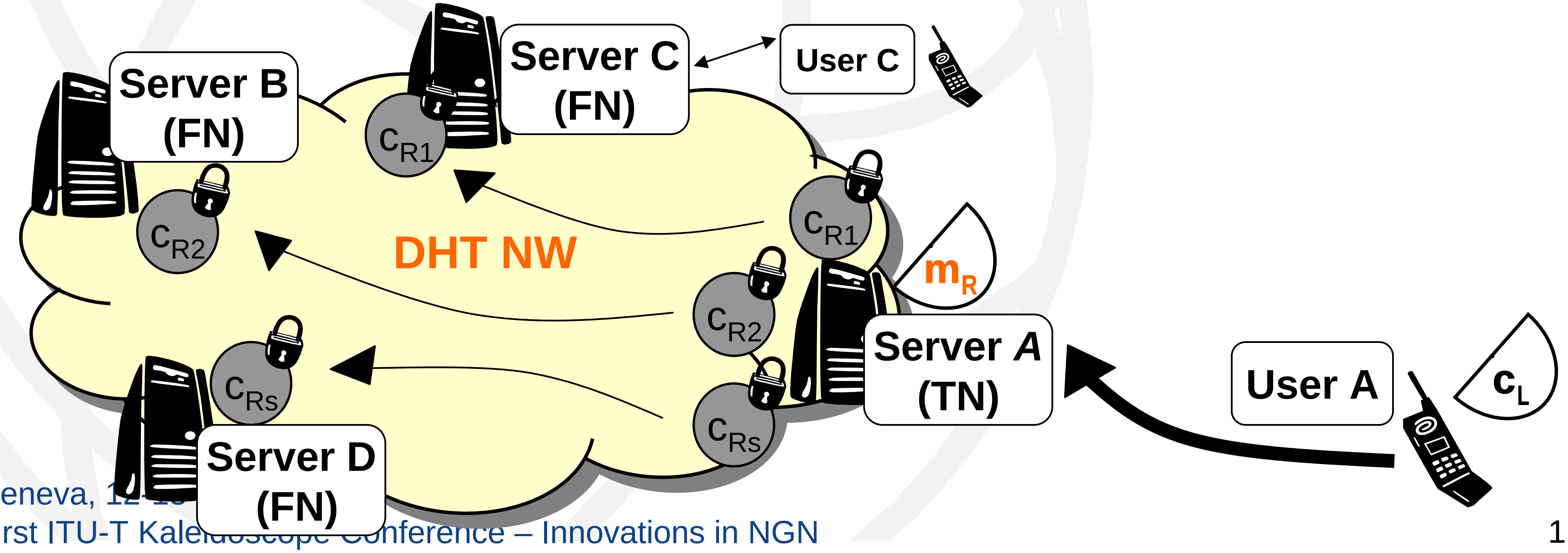


- However, if the server is attacked, m_R is leaked out

Distribute m_R against attacks!!

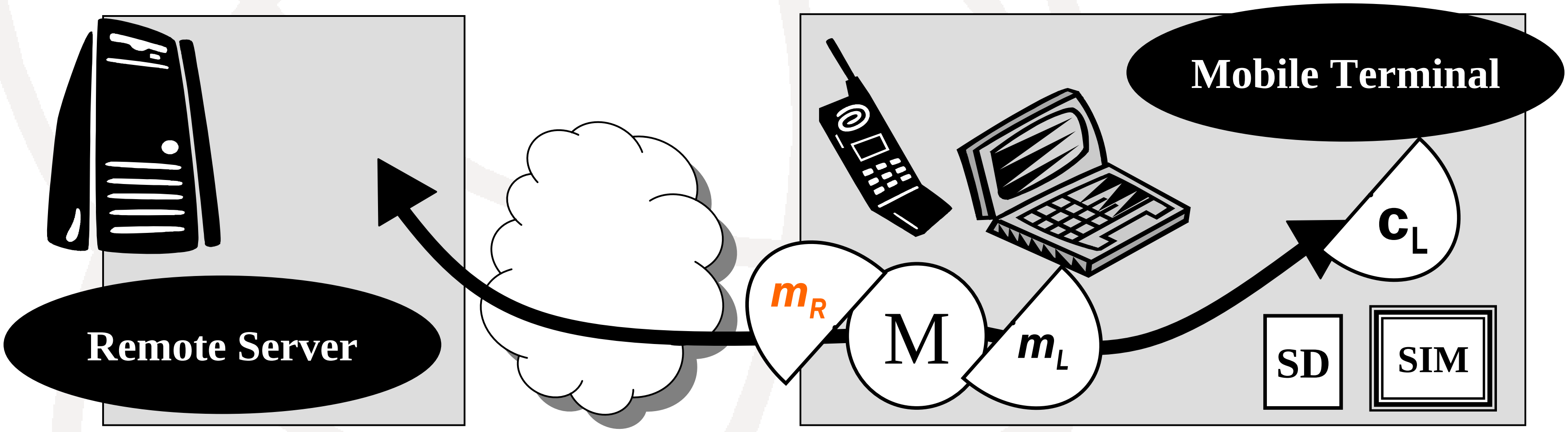
Answer *1 (2/2) against server attacks*

- P2P Overlay Network Storage
  - Compose network storage of remote servers managed by each user by P2P overlay NW (DHT).
  - Encrypt ***m_R*** into *s* pieces of decryption data (c_{R1}, c_{R2},…,c_{Rs}) in his own server (Server *A: Trusted Node[TN]*)
  - *s* pieces of decryption data are uploaded into Foreign Nodes **owned by other users** (*Foreign Node[FN]*)



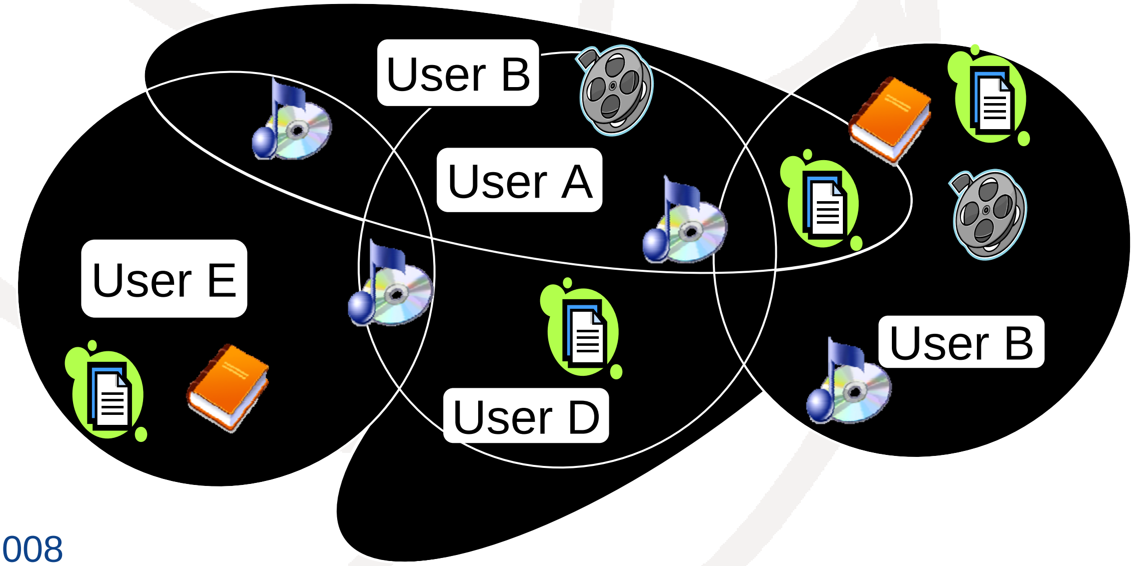
Problem 2

- To Reduce cost for Uploading remote data m_R



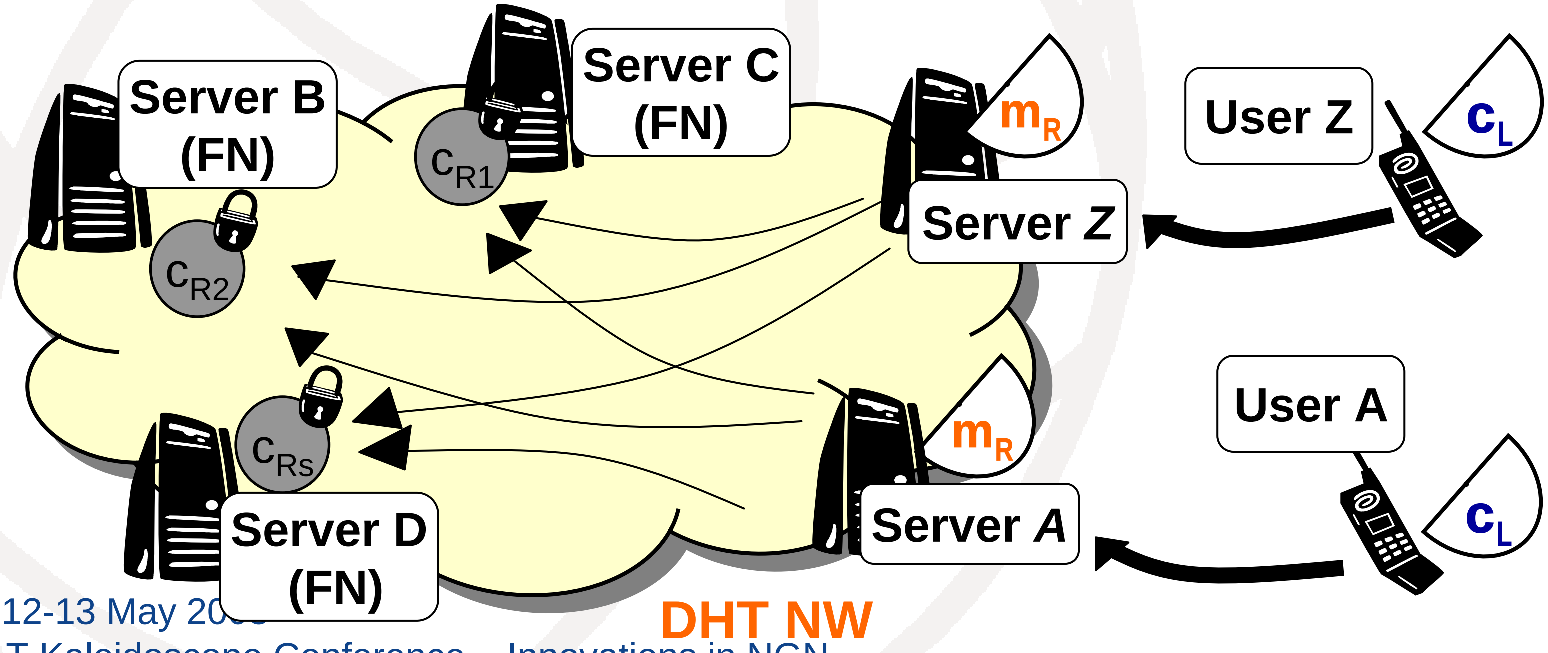
Answer 2 (1/3)

- There is large number of common files shared among the users such as music tracks, movie videos and novels .
  - Every file are encrypted into same c_R
- Sharing common c_R with other users
  - If c_R exists in the network storage, uploading c_R is omitted, the processing cost will be reduced



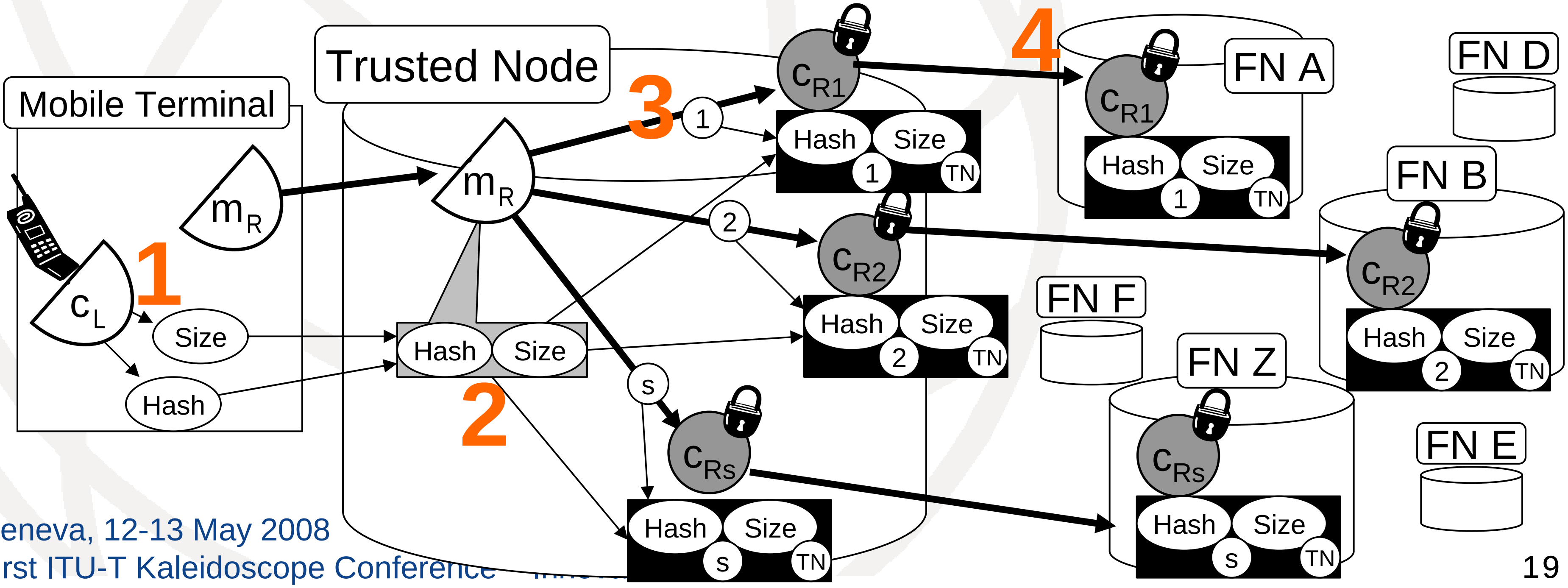
Answer 2 (2/3)

- P2P Overlay Network Storage
  - The trusted node decides which servers in a P2P network manages each distributed data according DHT ID
  - DHT ID is derived from only $\mathbf{c_L}$



Ans. *2 (3/3)* - The method for deriving DHT IDs

1. Mobile Terminal names m_R “Hash:Size” derived from C_L.
2. TN receives the name and derives DHT IDs consisting of the name of m_R, the distributing number and the ID of the trusted node
3. If the data does not exist on DHT network storage, TN receives m_R and encrypts It and divide it s items (C_{R1} to C_{Rs})
4. TN stores these *s* items to the corresponding nodes.



For the Standardization

- Require the following protocols
  - Authentication of mobile terminals and servers
    - Mobile terminals are authenticated by IP Multimedia Services Identity Module (ISIM)
    - Servers are authenticated by Public Key Infrastructure (PKI)
  - The algorithms in self-encryption scheme and protocols for communication
  - The method for deriving DHT IDs

Conclusion

- A Self-encryption based private storage system over p2p distributed file sharing Infrastructure
  - Protect all internal data for cases of loss of the terminal
  - Reduce costs for encryption processing in mobile terminal
  - Reduce costs for upload processing by letting users share common remote data.
- P2P Overlay Network Storage
  - Protect servers against attacks.

Thank you for your attention!