Introduction

of Funabiki Laboratory

November 1, 2006

Nobuo Funabiki

Okayama University, Japan
Members

- **Professor**
  - Nobuo Funabiki
- **Associate Professor**
  - Toru Nakanishi
- **D2**
  - Jun Kawashima, Megumi Isogai
- **D1**
  - Tamer Farag, Walaa Hassan, Yukikazu Murakami
- **M2**
  - Yousuke Shinohara, Noriaki Nagao, Youhei Nomura, Yoshinori Nagata, Naoto Hamada
- **M1**
  - Hideaki Kato, Koji Tanigawa, Shota Baba, Shun Higashine, Kouhei Miki, Aki Mouri
- **B4**
  - Yuta Hira, Hiroki Obayashi, Tomoya Shoji, Yuriko Nitta, Hiroyasu Kasai, Genya Okada, Takuya Nakayama
- **Research Student**
  - Han Yue, Yousuke Isshiki, Bai Ping An
Research Topics (1)

• **Educational Technology**
  - English class arrangement support system, **ECASOU**
  - Education activity support system, **NOBASU**
  - Laboratory activity support system, **NOBASU@LAB**

• **Optimization Algorithms**
  - Parameter fitting algorithm for IC/LSI power-ground linear circuit model, **LECSS**
  - Adviser assignment algorithm for undergraduate final projects

• **Security Engineering**
  - Improved group signature protocol
  - Electric money & auction protocol using group signature
  - Electric voting protocol
  - Anonymous user authentication for mobile communication networks
Research Topics (2)

• **Network Engineering**
  - Optimal design for wireless infrastructure mesh network
  - Routing algorithm for application-level multicast communications
  - Topology design for WDM optical networks
  - Channel assignment for WDM optical networks

• **Image Media Engineering**
  - Digital picture-card show system
Educational Technology
English Class Arrangement Support system of University: **ECASOU**

**Outline**

**System Manager:**
- Registration
- Class information

**English Teachers:**
- Desired time/subject for teaching
- Execute assignment program

**Server Program**
- JSP
- Apache+Tomcat
NetwOrk Based Assistant System for University education: NOBASU

- Students
- Teachers
- Class documents, scores
- Questions, report submission
- Messages
- Reports, questions
- Class documents, scores
- INTERNET

Client

- Mobile phone
- Browser

Server

- Linux
- HTML
- JSP/Servlet
- SQL
- Apache (WEB server)
- Tomcat (application server)
- MySQL (database)

Distributed System Laboratory 7
Optimization Algorithms
Parameter Fitting Algorithm for IC/LSI
Power-ground Linear Circuit Model
(LECCSS)

IC/LSI power-ground linear circuit model (LECCS-model)

$|Z_i|$: impedance between power & ground.

Algorithm:
Finds proper values for $L_i$, $C_i$, $R_i$ from $|Z_i|$
Security Engineering
Secure File System for Memory Cards on Linux: **SAS**

- Secure file system for memory cards of PDA on Linux
  - SHARP Zaurus SL-C860 (OpenPDA : Linux kernel-2.4.18)
  - Memory-cards of PDA can be easily lost as they are used outside and detachable.

- **Features of SAS (Storage Add-on Security)**
  1. No update of OS (Linux) when SAS is installed.
  2. Adoption of AES as fast, powerful encryption algorithm
  3. Encryption of meta-data (file information) — conventional file system cannot detect files.
  4. Possibility of applying different security policy to every file.

SAS is the first file system with the four features.
Group Signature

• **Features of Group signature**
  - Formal members of the group can make signatures.
  - Other members or verifiers cannot identify owners of signatures.
  - Only manager of signatures can identify them.

• **Application to credit card system**
  - Manager=Card company (Visa, Master, …) , Verifier=Store owner, Member=Card user
Optimal Design for Wireless Infrastructure Mesh Network

- **WDS (Wireless Distribution System):**
  - wireless connections between multiple access points (APs).
  - can expand wireless LANs with low cost
  - may increase interference and decrease bandwidth.

- **Optimal design of WDS**
  - Locations of APs.
  - Routing and scheduling of communications between APs.
  - Selections of associated APs for hosts.
Application-Level Multicast Communications

- **Application-level multicast (ALM) communications**
  - hosts replicate packets to deliver multiple destinations.
  - routing can be made on host level instead of routers.

- **Research issues**
  - optimal routing (multicast tree) algorithm to minimize delay and host loads.
  - design and implementation of the system, and experiments in class in our department.
Image Media Engineering
Panoramic Image Generation Algorithm from Multiple Cameras

Input images (Images A, B)

Rough calibration (Image B → B')
rotation around y-axis + scaling + shifting

\[
\begin{bmatrix}
x' \\
y'
\end{bmatrix} = \begin{bmatrix} r_1 - r_2 \\ -\tan \alpha \cdot (x - \frac{W}{2}) - r_2 \\
\end{bmatrix} \begin{bmatrix} x - \frac{W}{2} \\
y - \frac{W}{2}
\end{bmatrix} + \begin{bmatrix} \Delta x \\
\Delta y
\end{bmatrix}
\]

Detailed calibration (Image B' → B'')
rotation around z-axis + scaling + shifting + gray-scale adjustment

\[
\begin{bmatrix}
x' \\
y'
\end{bmatrix} = \begin{bmatrix} k_x & 0 \\
0 & k_y
\end{bmatrix} \begin{bmatrix} \cos \beta & \sin \beta \\
-\sin \beta & \cos \beta
\end{bmatrix} \begin{bmatrix} x - x_0 \\
y - y_0
\end{bmatrix} + \begin{bmatrix} x_0 \\
y_0
\end{bmatrix} + \begin{bmatrix} \Delta x \\
\Delta y
\end{bmatrix}
\]

\[
f_{\theta''}(x, y) = K \cdot f_{\theta'}(x, y)
\]

Synthesizing (Image A + Image B'')
License Plate Recognition Algorithm

- **input gray-scale image**
  - Chinese & Japanese
  - Cross-count method
  - Numbers
  - Template-matching method

- **binary image**
  - Symbol recognition
  - V = (7, 6, 8, 4), (4, 2, 1, 1)

- **extract character regions**
  - identify character regions for recognition
Tooth Contour Extraction Algorithm

input image → binary image → reshaping → edge extraction → separation

image for template-matching

tooth contour model = four ¼ ecliptic curves
Publications in 2004-2005
Journals with Referees


Domestic Conference
Proceedings with no Referees


Distributed System Laboratory  23
Books

• 持田敏之, 舗曳信生 編著, "情報セキュリティ対策の要点 - 実務と理論 -", コロナ社, 2005 (Japanese).