System integration of QKD and post-quantum signatures for a distributed storage system with long-term security

(1) **Confidentiality**
No information leak on the data in transit and at rest.

(2) **Integrity**
The data existed at time $t_0$ and has not been changed since.
### Requirements for long-term security system

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Meaning</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i) Confidentiality</td>
<td>The data should be accessible only to authorized parties.</td>
<td>- <strong>Information theoretically secure storage and communication</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Secure <strong>access control</strong></td>
</tr>
<tr>
<td>(ii) Integrity</td>
<td>The data should remain unaltered.</td>
<td>Signature and authentication with <strong>prolongable validity</strong></td>
</tr>
<tr>
<td>(iii) Availability</td>
<td>The data should be available whenever required.</td>
<td><strong>Redundant</strong> data backup</td>
</tr>
<tr>
<td>(iv) Functionality</td>
<td>The data can be processed without decryption.</td>
<td>(Fully) <strong>homomorphic</strong> encryption</td>
</tr>
</tbody>
</table>

So far, partial solutions have been developed and used, i.e., long-term confidentiality only, or long-term integrity only. However, no comprehensive solution has been demonstrated yet.
Long-term integrity, authenticity, and confidentiality protection system  
“LINCOS”

proposed and demonstrated by TU Darmstadt and NICT,  
Basic components for LINCOS

1. **Information theoretic** confidentiality of storage
2. **Computational but prolongable** integrity
3. Availability (redundant data backup)
4. Functionality (Multi-party secret computing)

(1) Secret sharing

Original data → Share 1 → Share 2 → Share 3 → Share 4

(2) QKD + OTP

(3) Time-stamp chains of signature

1. **Information theoretic** confidentiality of data link
Proof of concept demonstration of LINCOS


Integrity protection
- Evidence service
- Timestamp authority

Next talk by Matthias Geihs (TUDA)
- Basic principle
- New results

Data owner
- Original data

Time-stamp chain of signature

Secret sharing system
Key supply ~ 40 kb/s

Max link distance ~ 90km

Tokyo QKD Network

Share 1
Share 2
Share 3
Share 4

Key
Key
Key

Secret sharing system

Max link distance ~ 90km

Tokyo QKD Network

Key supply ~ 40 kb/s
Healthcare LINCOS

e.g. Genome data
Medical records
- Authentication and access control of healthcare workers
- End point security for medical information devices
Healthcare PKI (H-PKI)

PKI Certificate

- Name,
- Address
- Age,
- Male/Female

- User authentication
- Integrity protection

H-PKI Certificate

- Name,
- Address
- Age,
- Male/Female

- Healthcare Role

- Medical Doctor
- Pharmacist
- Medical Technologist
- Radiological Technologist
- Registered Nurse
- Public Health Nurse
- Physical Therapist
- Occupational Therapist
- ....

- Access control based on national qualification certificate in healthcare

Healthcare Post-Quantum-PKI (H-PQ-PKI)

See talk by Atsushi Yamada (ISARA) in the subsequent session
Testbed of H-LINCOS
- PQ-VPN (~800km range)
- QKD (~90km range)

Kochi Health Science Center

Osaka

Nagoya

Koganei

Medical records

1st Gen: PQ-VPN

2nd Gen: QKD

Tokyo QKD Network
Diagram of H-LINCOS testbed

Kochi Health Science Center

Kochi U Tech

NICT

Root CA

Certificates

Client devices

Gateway server

Layer-2 private channel

Layer-3 private channel

Secret sharing network

- Authentication
- Access control
- Access right management

Data owner server

Controller

Gateway server

Certificates

Client devices

Client devices

Client devices

Client devices

Client devices

Kochi U Tech

Kochi Health Science Center

NICT

Certificates

Certificates

Certificates

Layer-3 private channel

Osaka

Otemachi

Nagoya

Koganei
Experiment

- Use PQ TLS
to secure communications between client device and gateway server
  • For key establishment:
    \textbf{NewHope} (Lattice) or \textbf{SIDH} (Isogeny)
  • For end entity to sign packets:
    \textbf{Dilithium} (Lattice), \textbf{q-TESLA} (Lattice), \textbf{Rainbow} (Multivariate)

- Use PQ PKI
  • For CAs to sign certificates:
    \textbf{LMS} or \textbf{XMSS} (hash-based)

- Objectives:
  • Feasibility study of PQ Crypto algorithms,
    especially \textbf{client authentication of TLS}
  • PKI migration to PQ Crypto algorithms
    to be presented by A. Yamada (ISARA) in the subsequent session
<table>
<thead>
<tr>
<th>Root certificate</th>
<th>Key exchange</th>
<th>Signature</th>
<th>Encryption</th>
<th>Message authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMS</td>
<td>NewHope</td>
<td>Dilithium</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIDH</td>
<td></td>
<td>Dilithium</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XMSS</td>
<td>NewHope</td>
<td>Dilithium</td>
<td>AES 256 (GCM)</td>
<td>SHA 384</td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIDH</td>
<td></td>
<td>Dilithium</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Client authentication was successfully operated with all of the above PQ-TLS cipher suites.
### Preliminary results (in the ISARA Lab)

<table>
<thead>
<tr>
<th>Root certificate</th>
<th>Key exchange</th>
<th>Signature</th>
<th>Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LMS</strong></td>
<td>NewHope</td>
<td>Dilithum</td>
<td>87.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td>70.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td>179.2</td>
</tr>
<tr>
<td></td>
<td>SIDH</td>
<td>Dilithum</td>
<td>242.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td>237.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td>302.5</td>
</tr>
<tr>
<td><strong>XMSS</strong></td>
<td>NewHope</td>
<td>Dilithum</td>
<td>61.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td>65.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td>170.4</td>
</tr>
<tr>
<td></td>
<td>SIDH</td>
<td>Dilithum</td>
<td>232.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td>236.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td>348.4</td>
</tr>
</tbody>
</table>

- NewHope is faster than SIDH.
- Rainbow is slower than the others.
## Preliminary results (in the NICT Lab)

<table>
<thead>
<tr>
<th>Root certificate</th>
<th>Key exchange</th>
<th>Signature</th>
<th>Time (ms)</th>
<th>Processing times at NICT are 10 times longer than those at ISARA.</th>
<th>NewHope is a bit slower than SIDH.</th>
<th>Rainbow is slower than the others.</th>
<th>The difference between LMS and XMSS is larger in the NICT Lab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMS</td>
<td>NewHope</td>
<td>Dilithum</td>
<td>785.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td>672.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td>3091.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIDH</td>
<td>Dilithum</td>
<td>741.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td>626.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td>3358.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XMSS</td>
<td>NewHope</td>
<td>Dilithum</td>
<td>192.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td>310.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td>4124.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIDH</td>
<td>Dilithum</td>
<td>129.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>q-TESLA</td>
<td>172.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rainbow</td>
<td>3160.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Host machine**

**Client**

- PQ-PKI certificate store
  - Certificate for healthcare worker
  - Root certificate
  - PQ-TLS
    - PQ-signature
    - PQ-key exchange

**Gateway server**

- PQ-PKI certificate store
  - Certificate for gateway server
  - Root certificate
  - PQ-TLS
    - PQ-signature
    - PQ-key exchange

**Client authentication**

---

<table>
<thead>
<tr>
<th>Host machine</th>
<th>ISARA</th>
<th>NICT</th>
</tr>
</thead>
<tbody>
<tr>
<td>MacBook</td>
<td></td>
<td>NEC Notebook</td>
</tr>
<tr>
<td>i7-4770HQ</td>
<td>i5-6200U</td>
<td></td>
</tr>
<tr>
<td>4 cores @ 2.2 GHz</td>
<td>2 cores @ 2.3 GHz, 2.4 GHz</td>
<td></td>
</tr>
<tr>
<td>RAM 16 GB</td>
<td>8 GB</td>
<td></td>
</tr>
<tr>
<td>macOS 10.13.6 High Sierra</td>
<td>Windows 10</td>
<td></td>
</tr>
<tr>
<td>Ubuntu 16.04 Server mode</td>
<td>Ubuntu 16.04 Desktop mode</td>
<td></td>
</tr>
</tbody>
</table>

**CPU Intel(R) Core(TM)**

- 4 cores @ 2.2 GHz
- 2 cores @ 2.3 GHz, 2.4 GHz

**RAM**

- 16 GB
- 8 GB

**OS**

- MacOS 10.13.6 High Sierra
- Windows 10

**Guest machine**

- Ubuntu 16.04 Server mode
- Ubuntu 16.04 Desktop mode

---

100 ms ~ 300 ms

100 ms ~ 4,000 ms
Summary

H-LINCOS

- Confidentiality protection by secret sharing and AES/QKD.
- Integrity protection by timestamp chains of signature with prolongable validity.

Operating in the field testbed with sample medical records

- Authentication and access control by PQ-TLS and PQ-PKI.

12 cipher suites have been implemented and successfully operated in the Lab.

Challenges

- Install PQ-TLS and PQ-PKI in the field testbed.
- Put the whole system to reliability test in various conditions.
- Study smooth migration to PQ infrastructures.
- Extend to multiple data owners and realize cross referencing.
Final goal

PQ Crypto system
- Signature
- Authentication
- Access control
- Key exchange

Electronic health record management system
- Secret sharing
- Multi-party computing

- 1st gen: PQ-VPN
- 2nd gen: QKD

R&D, Pharmacy, Precision medicine, ... Healthcare
Acknowledgement

The Cabinet Office, Government of Japan

Deutsche Forschungsgemeinschaft
Collaborative Research Centre 1119

Cooperation with

- Kochi Health Science Center
- Kochi University of Technology
- NEC
- NTT Communications
- Panasonics
- ZenmuTech
- Rocketworks
- SBS Information Systems