What can we do to help after a disaster?

- Approaches to share information securely -

Haruo Yokota

Tokyo Institute of Technology

Many Disasters Around Us

- Earthquakes
- Tsunamis
- Eruptions
- Deluges
- Storms
- …

Earthquakes in NZ

Kaikoura, New Zealand, Nov. 14, 2016
(Richter Magnitude Scale: 7.8)

Christchurch, New Zealand, Feb. 22, 2011
(Magnitude 6.3)

Jan. 24, 2017

Jan. 24, 2017

Earthquakes in Japan

Kansai Awaji, Japan, Jan 17, 1995 (Magnitude 6.9, 6,434 Deaths)

Kumamoto Japan
Apr. 16, 2016
(Magnitude 7.3)

Earthquake with Tsunami

Great East Japan Earthquake
March 11, 2011
- Magnitude: 9.1
- Deaths: 15,896
- Injured: 6,152
- Missing: 2,562

Nuclear Accident
in Fukushima Daiichi Nuclear Power Plant

- Electrical generators down
- Reactor cooling system stopped
- Active cores reached meltdown
- Hydrogen gas explosions
- Radioactive material released

Evacuation Facilities (Shelters, Refuges)

More than 450,000 people evacuated to more than 2,000 shelters in the case of Great East Japan Earthquake

Information is essential!

- To find safety of their families, relatives, friends, …
- To provide disaster medical support
- To distribute relief supplies appropriately

What can IT contribute?

- Cell phones tend to be useless
  - Network congestion
- SNS services were effective
- Google started “Crisis Response”
  - After 1 hour 45 minute later
  - Google Person Finder
    - “I’m looking for someone”
    - “I have information about someone”

Google person finder
a google.org project

English

Japan (in test mode)

How it works
Frequently asked questions
For responders
For developers

Google Person Finder helps people reconnect with friends and loved ones in the aftermath of natural and humanitarian disasters.

A crisis strikes and people get separated.

They let the world know they are looking for someone.

Individuals and organizations provide information.

People find information about their friends and family.

Responders

You can help people find each other in the aftermath of a disaster:

- Embed Google Person Finder in your site
- Download data from Google Person Finder
- Upload data into Google Person Finder

See how »

Developers

You can help continue to improve Google Person Finder:

- Learn about the PFIF data model
- Customize or improve Person Finder

Get started »

Google person finder
a google.org project

English

Japan

This repository is currently in test mode. While test mode is in effect, records that are over 24 hours old are deleted.

I'm looking for someone

I have information about someone

PLEASE NOTE: All data entered is available to the public and usable by anyone. Google does not review or verify the accuracy of this data. Learn more about Google Privacy Policy.

If you send information through "I'm looking for someone" box on Google Person Finder, the information will also be sent to J-anpi anpi jouhou matomete kensaku service ("J-anpi") operated by NTT Resonant Inc. If there is registered information responding to your query, you can see the registered information on J-anpi site. Your use of J-anpi is subject to J-anpi's terms of services. J-anpi is not service provided by Google.

Google person finder
a google.org project

English

Japan

This repository is currently in test mode. While test mode is in effect, records that are over 24 hours old are deleted.

Identify who you have information about

Identifying information

Name
What is this person's name?

Family name (required): foo
Given name (required): bar
Alternate family names:
Alternate given names:
Sex:
Age: Number or range (e.g. 20-30)

Home Address

Street name:
Street name only, no number
Neighborhood:
City:
Province or state:
Postal or zip code:
Home country:

Description

Describe how to identify this person.

Person Finder: Japan

Photo

If you have a photo of this person, upload it or enter its URL address.

URL:
Upload:

Profile Pages

Does this person have profile pages at other websites?

Select a website to add a profile page...

Expiry

When should this record disappear?
While test mode is in effect, records that are over 6 hours old are deleted regardless of the expiry date.

About 1 month (30 days) from now

Source of Record

Where did this information come from?

This is a new record.
This record is copied from another source.

Your name (required):
Your phone number:
Your e-mail address:
Subscribe to updates about this person:

Status of Person

Status

Status of this person:

Unspecified

Have you personally talked with this person AFTER the disaster? (required)

Yes
No

Last known location
Type an address or open the map below and indicate the location by clicking on the map.

Show Map Use current location

Message

Message (required)

https://www.google.org/...ource_url=&status=&style=&subscribe=&subscribe_email=&suppress_redirect=&target=&text=&ui=&utcnow=[2017/01/15 16:37:48]

Are they enough to help victims?

- We need to share information appropriately
  - Many classes of stakeholders
    - What kind of / how many medicines should be prepared
    - How many volunteers are required
    - …
  - Need to control privacy for each user class
    - Reflect the intentions of the owners of the information

Problem Breakdown

- Keep the information secure
  - Stored data should be encrypted
  - Searching for / calculating encrypted data
- Untrusted servers / administrators
  - Generate no plain text during processing
- Handling an unspecified number of classified users
  - If the members of a user class share a key
    - When a member leaves from the user class
      - The old key should be revoked and a new key distributed
    - This key redistribution is impractical for volunteers and friends
- Fine-grained Access Control
  - Treatment of privacy issues are proper to data owners

Granularity of Access Control

- Traditional relational databases
  - Relation (Table), Tuple (Row),Attribute (Column)
  - Not enough fine to reflect the intension of individual owner
  - Not suitable to indicate relationship between individuals

Name	Age	Gender	Stay at	email	Condition
Alice	38	female	gymnasium of school A	alic@a.com	null
Bob	60	male	hospital B	bob@b.edu	high blood pressure
Carol	29	female	gymnasium of school A	carol@c.org	pregnant
:	:	:	:	:	:

Tuple

Relation

Attribute

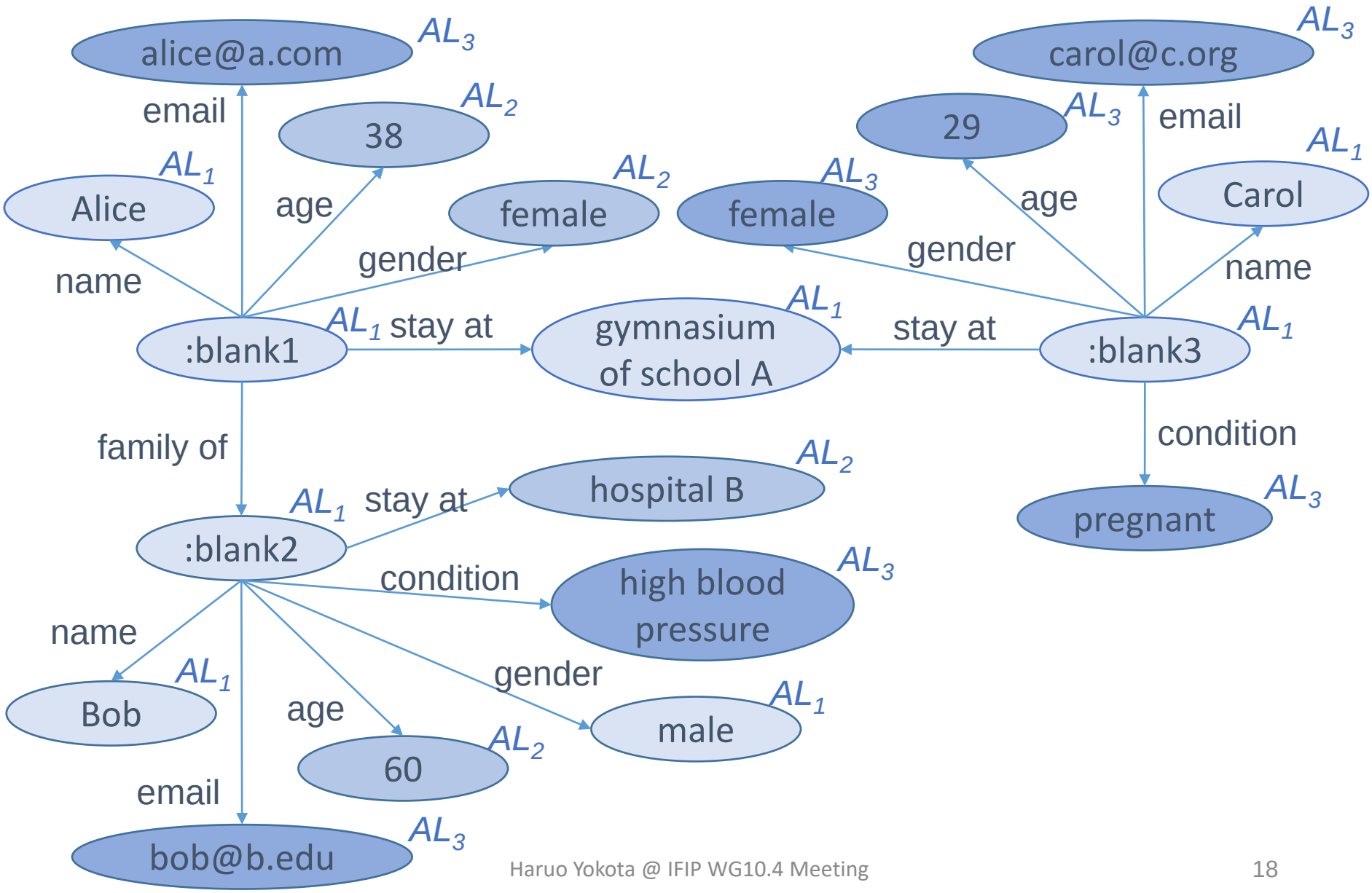
Approaches

- Represent information by graph structures
  - Such as RDF (Resource Description Framework)
  - To represent relationship between individuals
  - To enable fine grain access control
    - Encrypts each node corresponding to its access level
- Map a user class (UC) to an access level (AL)
  - Each user has a secret key and a public key (PKI)
  - Node is encrypted by a public key of access level
  - Re-encrypt data between
    - Those encrypted by user public key
    - Those encrypted by public key corresponding to access level for the user class

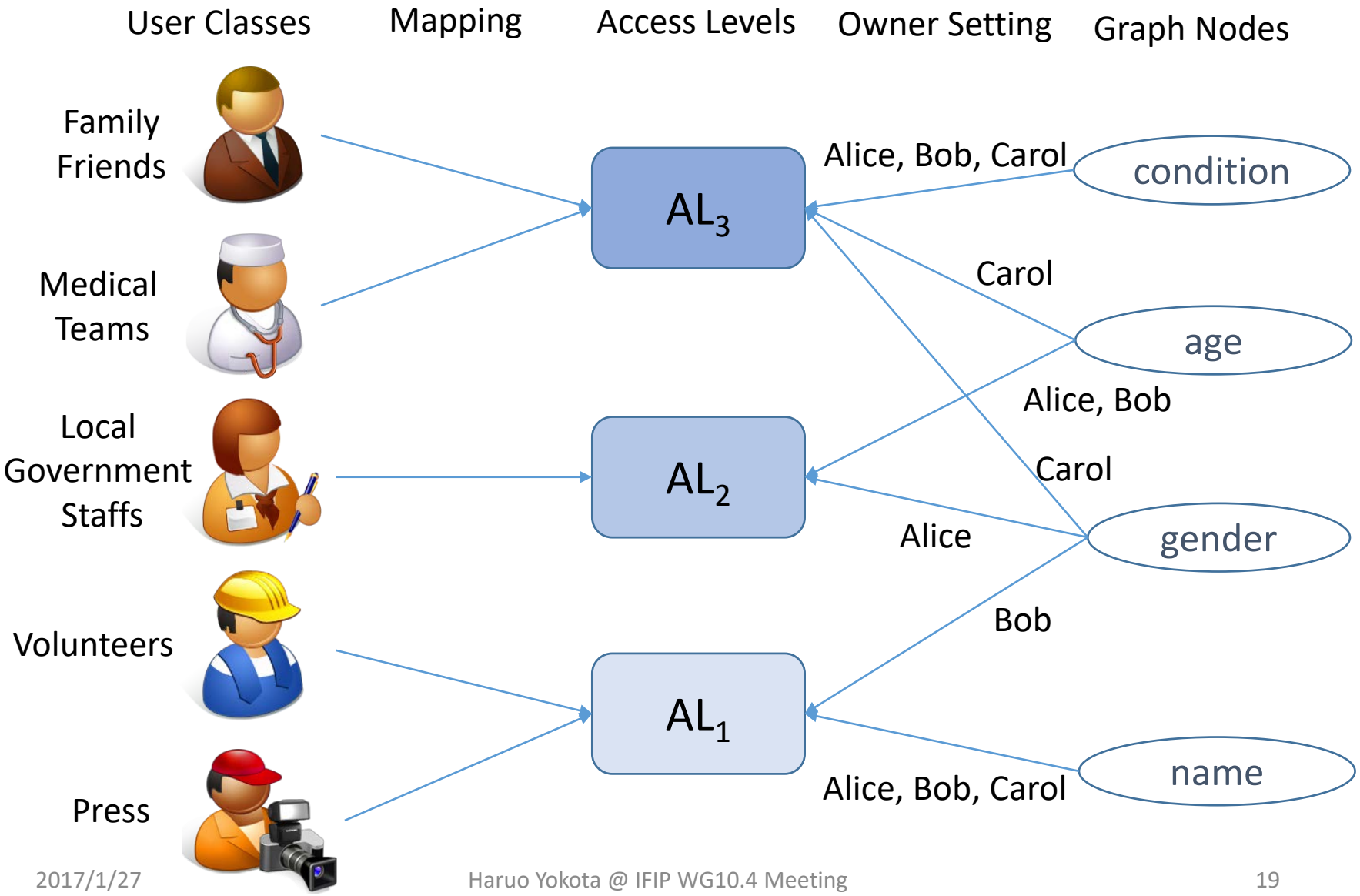
RDF Data Model

- Triple: <Subject, Predicate, Object>
  - Subject indicates a resource (an entity)
  - Predicate represents a property of the entity
  - Object is a value of the property in form of a resource or literal
- A set of triples builds a directed graph
  - Subject and Object are nodes respectively
  - Predicate is a labeled directed edge from the subject to the object

An RDF Graph Example



Example of Mapping UCs to ALs



No Plain Text in Servers

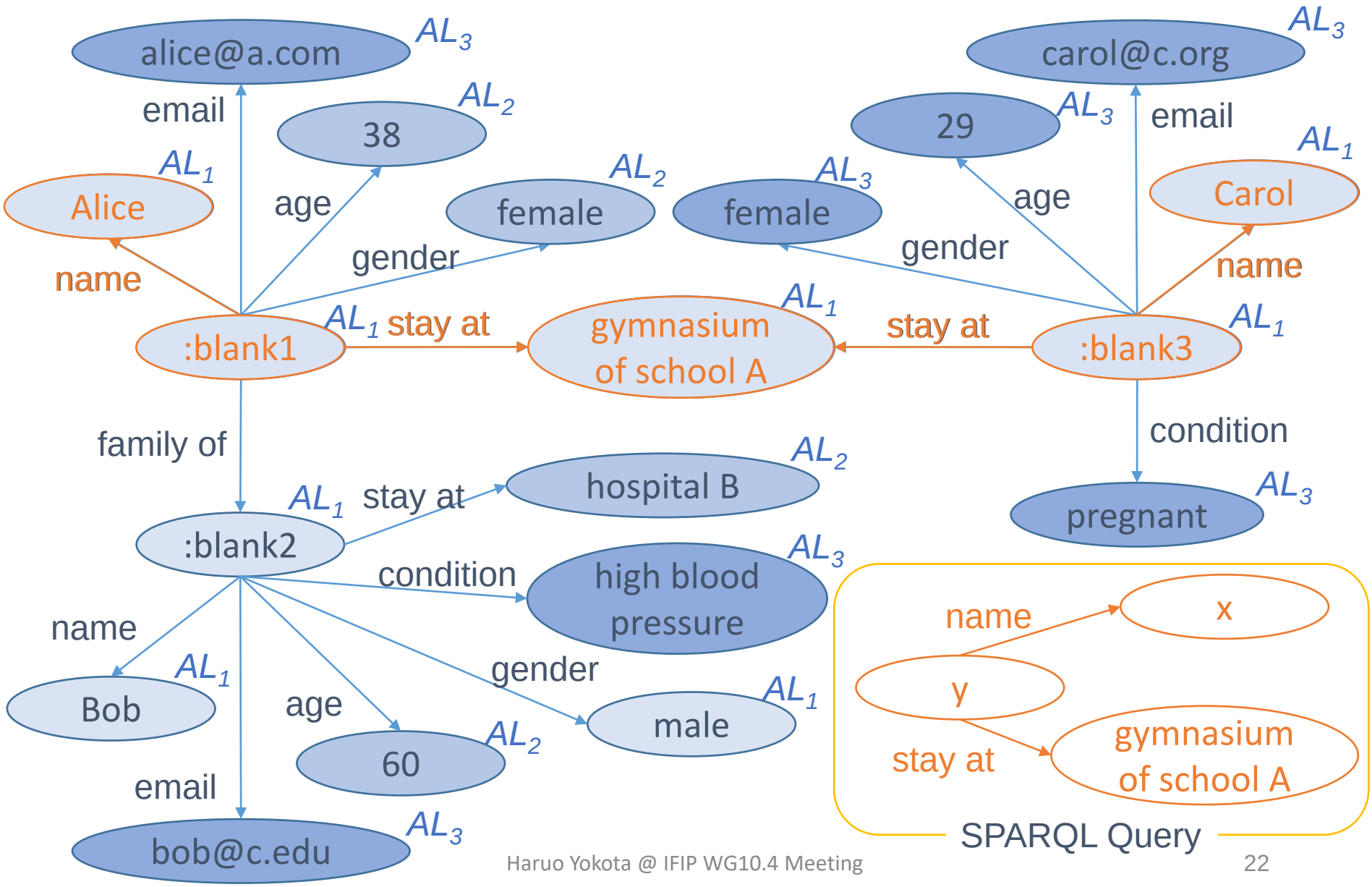
- Proxy re-encryption
  - rencrypt(chiper(X, PK_{ui}),$REK_{ui,alj}$) → cipher(X, PK_{alj})
    - From cipher data encrypted by public key of the user (PK_{ui})
    - To cipher data encrypted by public key of the correspond access level (PK_{alj})
  - All Keys including the re-encryption keys ($REK_{ui,alj}$) are managed in a certificate authority
- Searchable encryption
  - Pattern match with deterministic encryption
  - X = Y → cipher(X, K) = cipher(Y, K)
- Homomorphic encryption
  - Calculation on Encrypted Data
  - f(X, Y) = Z → f(cipher(X, K), cipher(Y, K)) = cipher(Z, K)

SPARQL Query Language for RDF

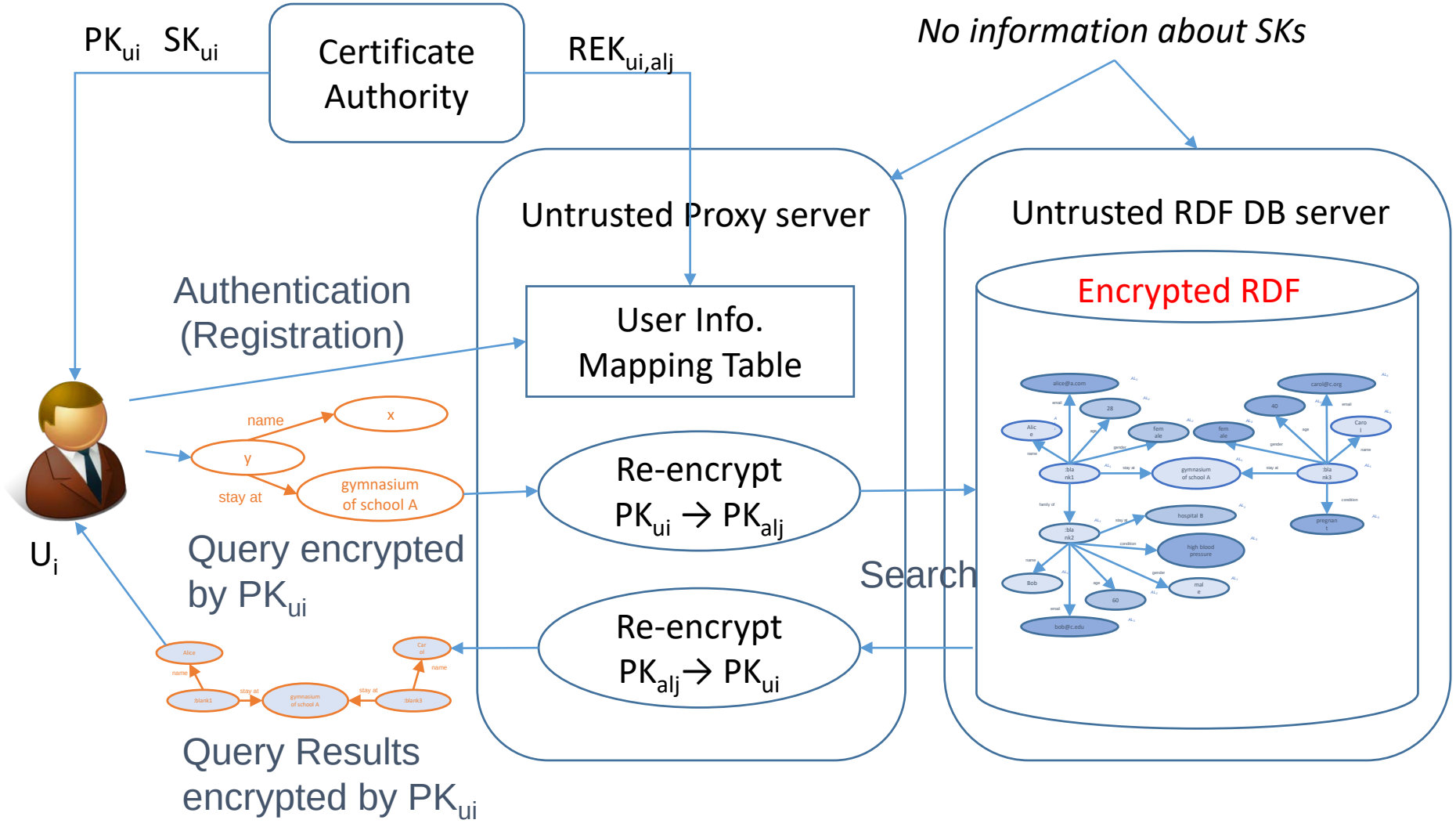
- Recursive definition (W3C)
  - SPARQL Protocol and RDF Query Language
- Pattern match for <S, P, O>
- Example
  - To derive name of victims staying in the gymnasium of school A

```
SELECT ?x
WHERE {?y  name ?x
           ?y  stay_at  gymnasium_of_school_A
}
```

Graph Match by SPARQL



Access Flow


PK_ui SK_ui
Certificate Authority
REK_ui,alj
No information about SKs
Untrusted Proxy server
Untrusted RDF DB server
Authentication (Registration)
User Info. Mapping Table
Encrypted RDF
name
x
y
stay at
gymnasium of school A
Re-encrypt PK_ui → PK_alj
Search
Re-encrypt PK_alj → PK_ui
U_i
Query encrypted by PK_ui
Query Results encrypted by PK_ui

Security

- The queries and search results for them can only be read by U_i who has the secret key SK_{ui}
  - Because they are encrypted by PK_{ui}
- Untrusted administrators of the DB or proxy server cannot read the contents of DB, queries, or results
  - There is no information about the secret keys in servers
- Even leaked contents of the DB can be read nobody
  - No SK_{alj} is available
  - Re-encryption keys only generate cypher text that can be decrypted by authorized users
- The authorization relies on the certificate authority

Benchmark

- To evaluate approaches in environments reflecting situations of actual disasters
- Tools for generating RDF data sets
  - Use the actual location and size of the evacuation facilities
    - Published in the Web pages by Ministry of Land, Infrastructure, Transportation and Tourism, Japan
  - Place victims whose age and gender are based on the population statistics of Japan to the evacuation facilities
  - The size of benchmark is variable by changing the number of the evacuation facilities with the distance from the center of the disaster
- Prepare SPARQL queries considering situations for helping victims
  - such as to count the victims requiring medicines

Open Issues

- Sophisticated schemes
  - Can encrypt/decrypt/re-encrypt in reasonable time
    - Searchable encryption
    - Proxy re-encryption
    - Homomorphic encryption
- Appropriate class assignment to each user
  - Assuming PKI like authentication with a certificate authority
  - Some classes may rely on user declaration, e.g. friends
- User friendly setting of the intended access level for each element by owner
  - Especially for untrained people in evacuation facilities

Other Related Issus

- Fragile IT infrastructure after the disaster
  - Power supply, server, and network environment
- Approaches
  - Distributed and redundant data placement
    - Need to consider comprehensive access level control
  - Adaptive network path selection
    - Using the information based on SNS

Related works

- Encrypted Relational Database Systems
  - CryptDB [Popa et al. SOSP'11, CACM2012]
  - MONOMI [Tu et al. PVLDB'13]
  - SDB [He et al. PVLDB'15]
  - ENKI [Hang et al. SIGMOD'15]
  - DBMask [Sarfraz et al. CODASPY'15]
- Fine-granularity encryption for RDF (Semantic Web) [Kong et al. CIS2009, Kim et al. ICUIMC2010, Rachapalli et al. ACMT2014, …]
- Hierarchical access control [Yang et al. CompSec2004, Chen et al. AMC2005, Chung et al. InfoSci2008, ..]
- (Distribute) Proxy re-encryption [Blaze et al. ICTACT 1998, Ateniese et al. TISS2006, Canetti et al. CCS2007, …]

Summary

- We have been suffered many disasters
- Information is essential to help victims of disasters
- Fine-grained access control on the information with providing privacy and security is required
- Approaches of mapping a user class to an access level for a graph based RDF data without handling plain text in servers are required
- There are still many issues to be solved

Questions ?