Group Oriented Attribute-based Encryption Scheme from Lattices with Shamir's Secret Sharing scheme

Maharage Nisansala Sevwandi Perera[1],
Toru Nakamura[2], *Takashi Matsunaka*[1],
Hiroyuki Yokoyama[1], *and Kouichi Sakurai*[3]

1: Advanced Telecommunications Research Institute International (ATR), Kyoto, Japan
2: KDDI Research, Inc., Saitama, Japan
3: Kyushu University, Fukuoka, Japan

NSS 2023 – Canterbury, UK
15th Aug., 2023

Abstract

We construct Group Oriented (GO) Attribute-based Encryption (ABE) scheme (GO-ABE scheme) using the post-quantum cryptographic primitive lattices and employ Shamir's secret sharing scheme to satisfy GO-ABE requirements.

Abstract

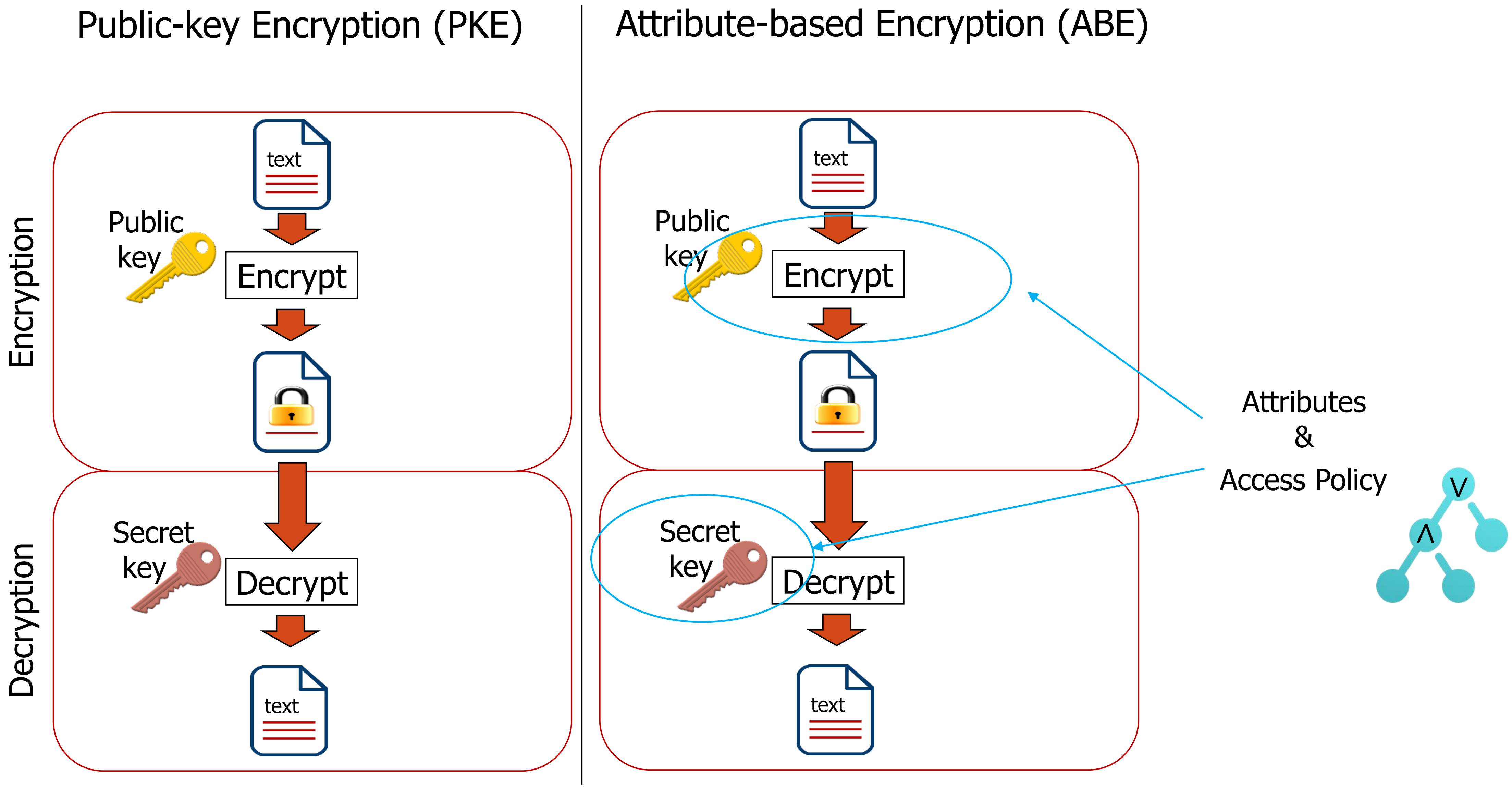
We construct Group Oriented (GO) Attribute-based Encryption (ABE) scheme (GO-ABE scheme) using the post-quantum cryptographic primitive lattices and employ Shamir's secret sharing scheme to satisfy GO-ABE requirements.

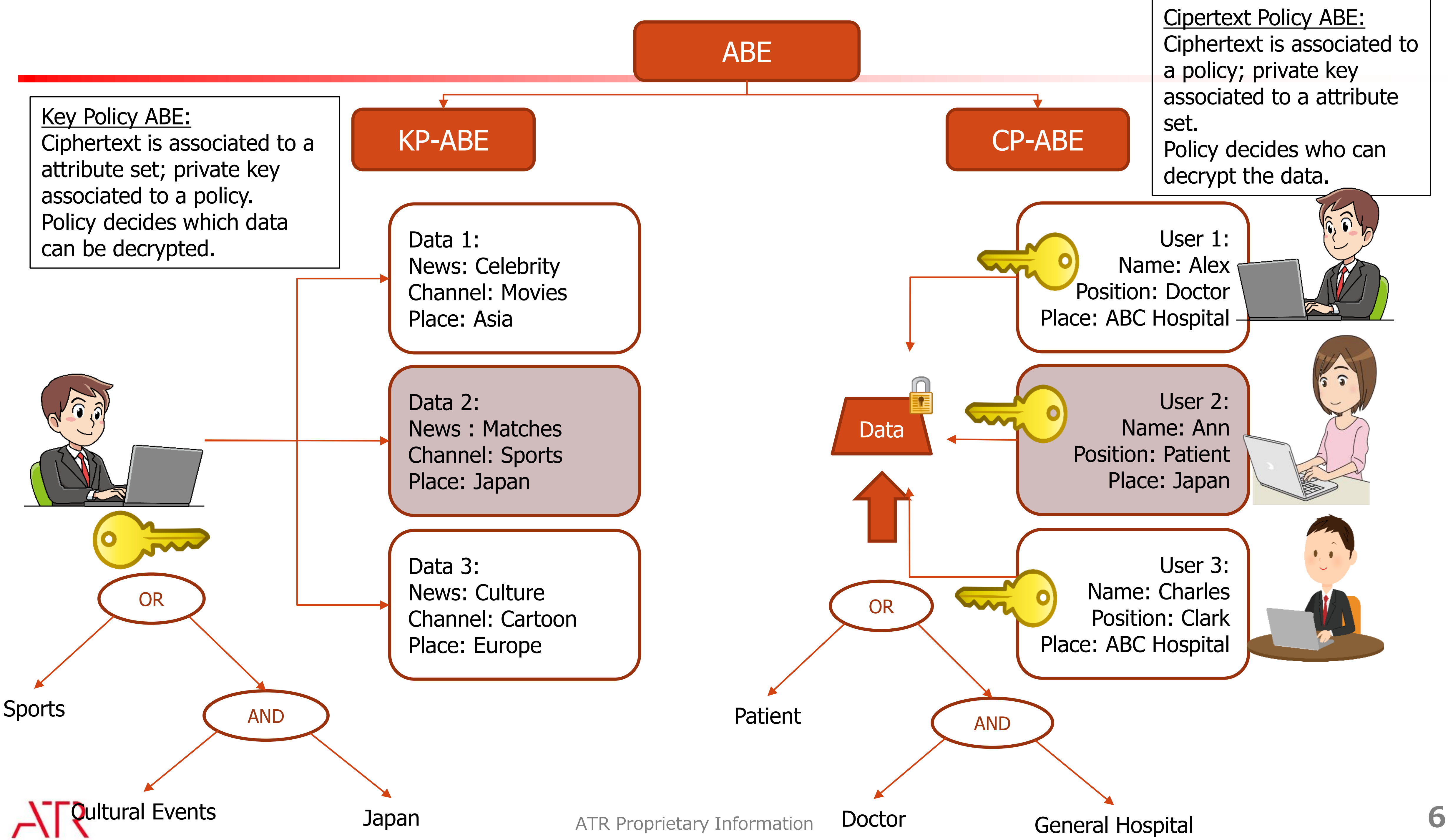
Content

- Group Oriented Attribute-based Encryption
  - Attribute-based Encryption (ABE) : KP-ABE and CP-ABE
  - GO-ABE Scheme
  - Requirement of GO-ABE
- Post-quantum construction of GO-ABE (our Goal)
  - Post-quantum primitive – Lattices
  - Need of Shamir’s Secret Sharing Scheme
  - Post- quantum (step by step) construction
  - Summary with Limitations

GROUP ORIENTED ATTRIBUTE BASED ENCRYPTION SCHEME

Attribute-based Encryption (ABE)

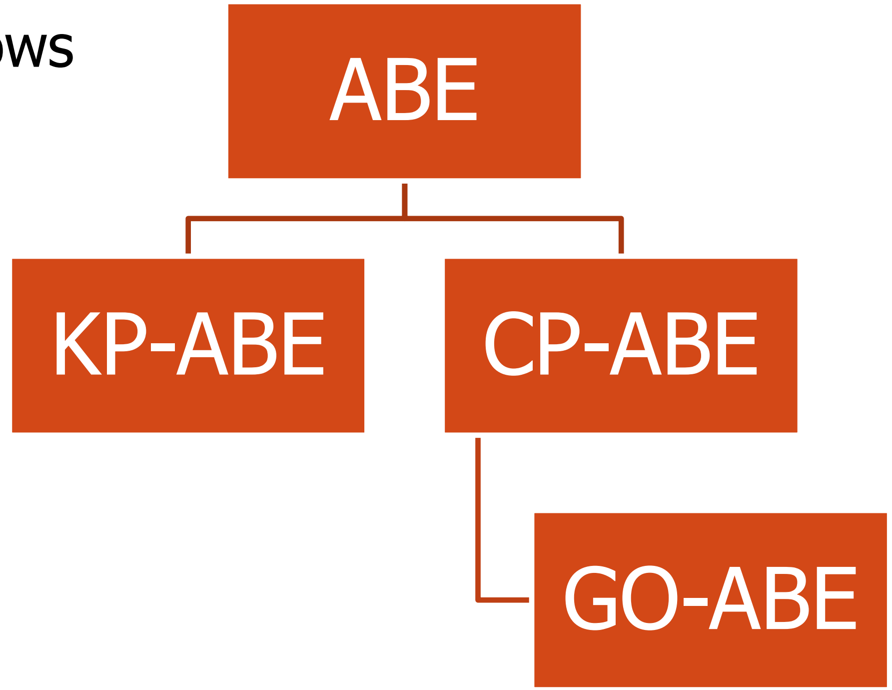



ABE
KP-ABE
CP-ABE
Key Policy ABE:
Ciphertext is associated to a attribute set; private key associated to a policy.
Policy decides which data can be decrypted.
Cipertext Policy ABE:
Ciphertext is associated to a policy; private key associated to a attribute set.
Policy decides who can decrypt the data.
Data 1:
News: Celebrity
Channel: Movies
Place: Asia
Data 2:
News : Matches
Channel: Sports
Place: Japan
Data 3:
News: Culture
Channel: Cartoon
Place: Europe
OR
Sports
AND
Cultural Events
Japan
User 1:
Name: Alex
Position: Doctor
Place: ABC Hospital
User 2:
Name: Ann
Position: Patient
Place: Japan
User 3:
Name: Charles
Position: Clark
Place: ABC Hospital
Data
OR
Patient
AND
Doctor
General Hospital

GO-ABE [Li et al. 2015]

- Group Oriented Attribute-based Encryption (GO-ABE) was introduced by Li et al. in NSS2015
- Group Oriented Attribute-based Encryption (GO-ABE) allows
  - **Users** from the **Same Group**

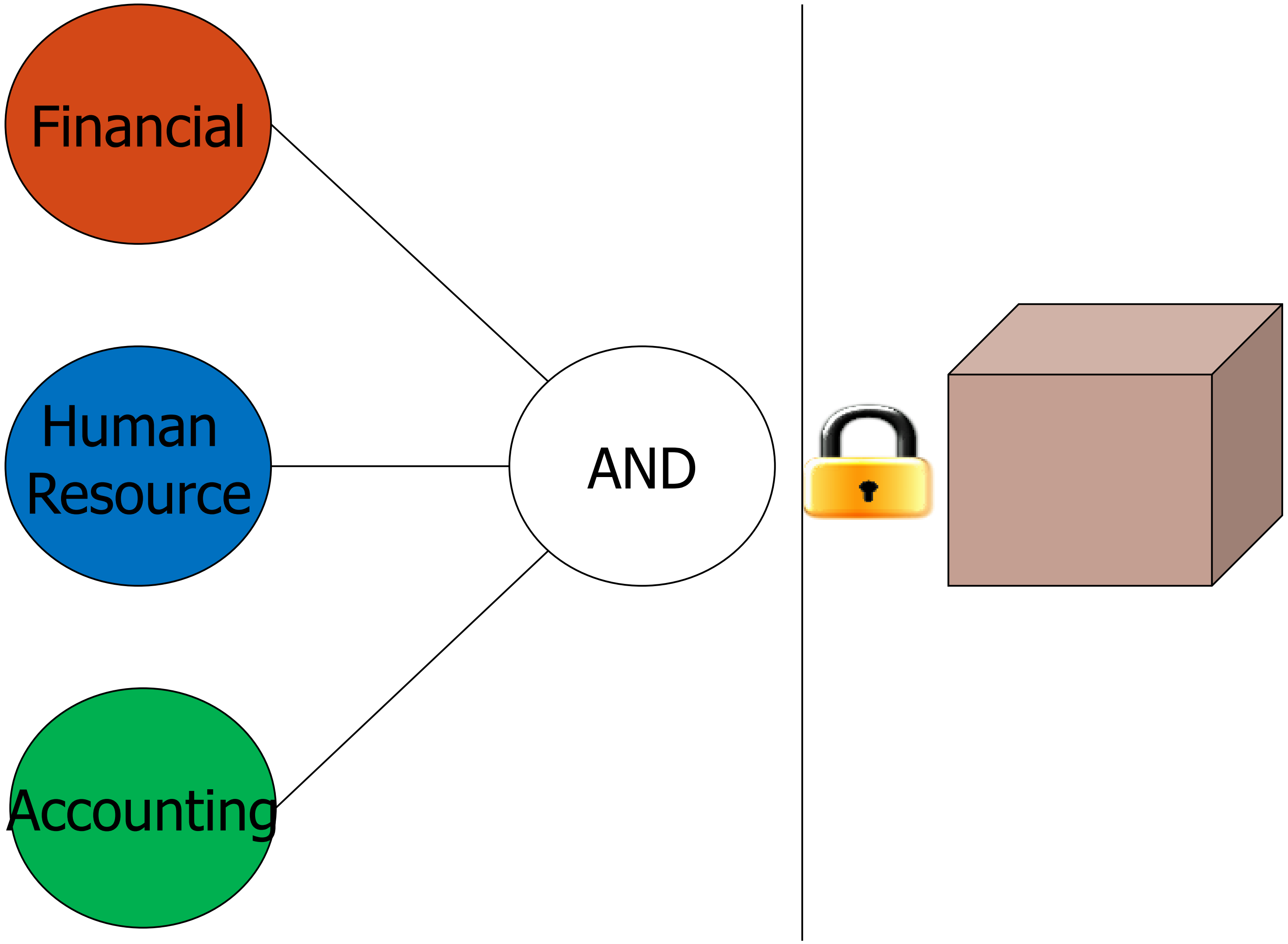
    to cooperate to decrypt a ciphertext
  - **Without revealing** their **secret keys**



"Users from the same group are able to cooperate with each other to decrypt a ciphertext encrypted under a set of attributes α such that a single user may not have enough attributes to match the attribute set α"

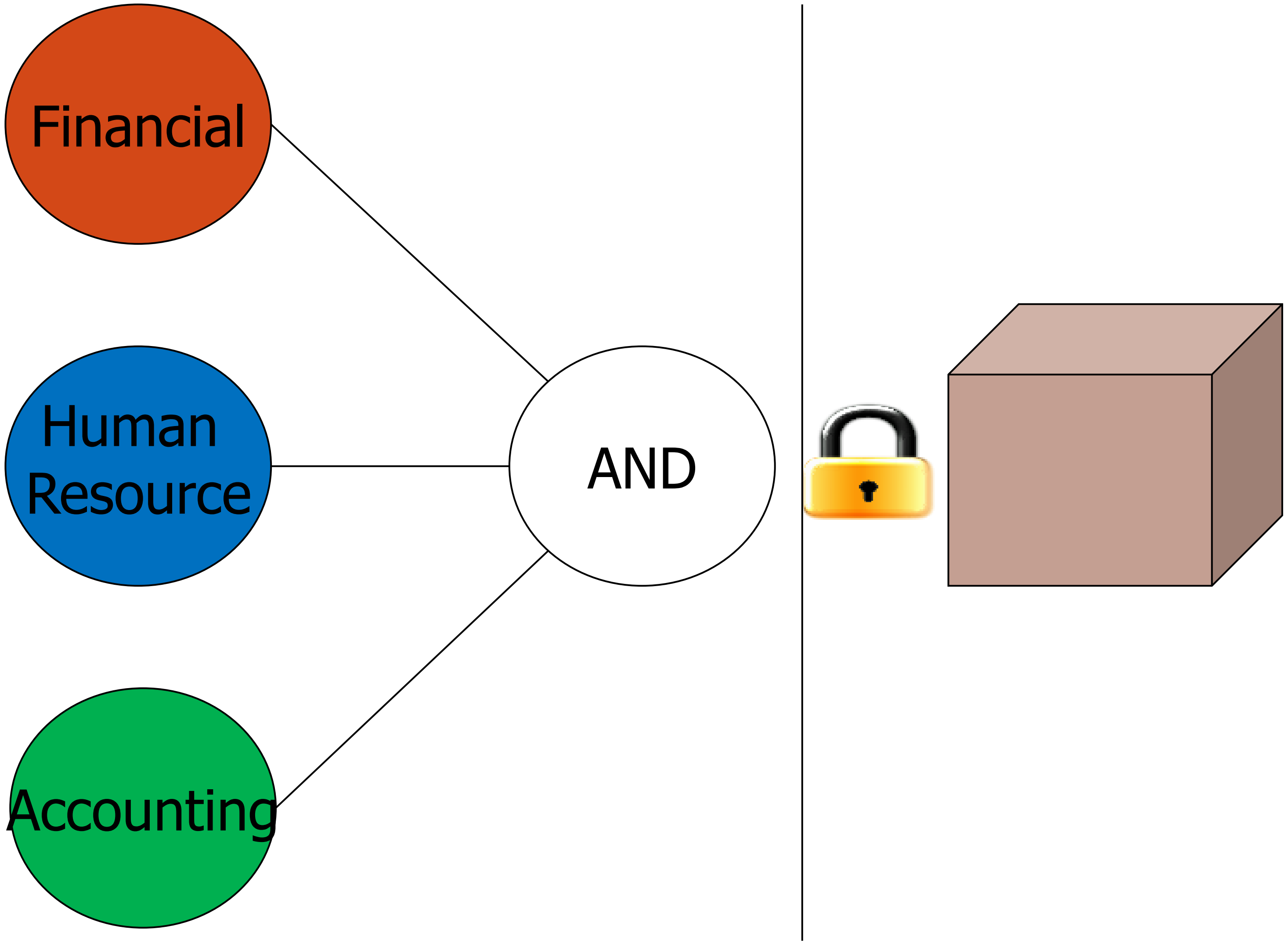
[Li et al. 2015].

Requirement of GO-ABE – Confidential Data Access



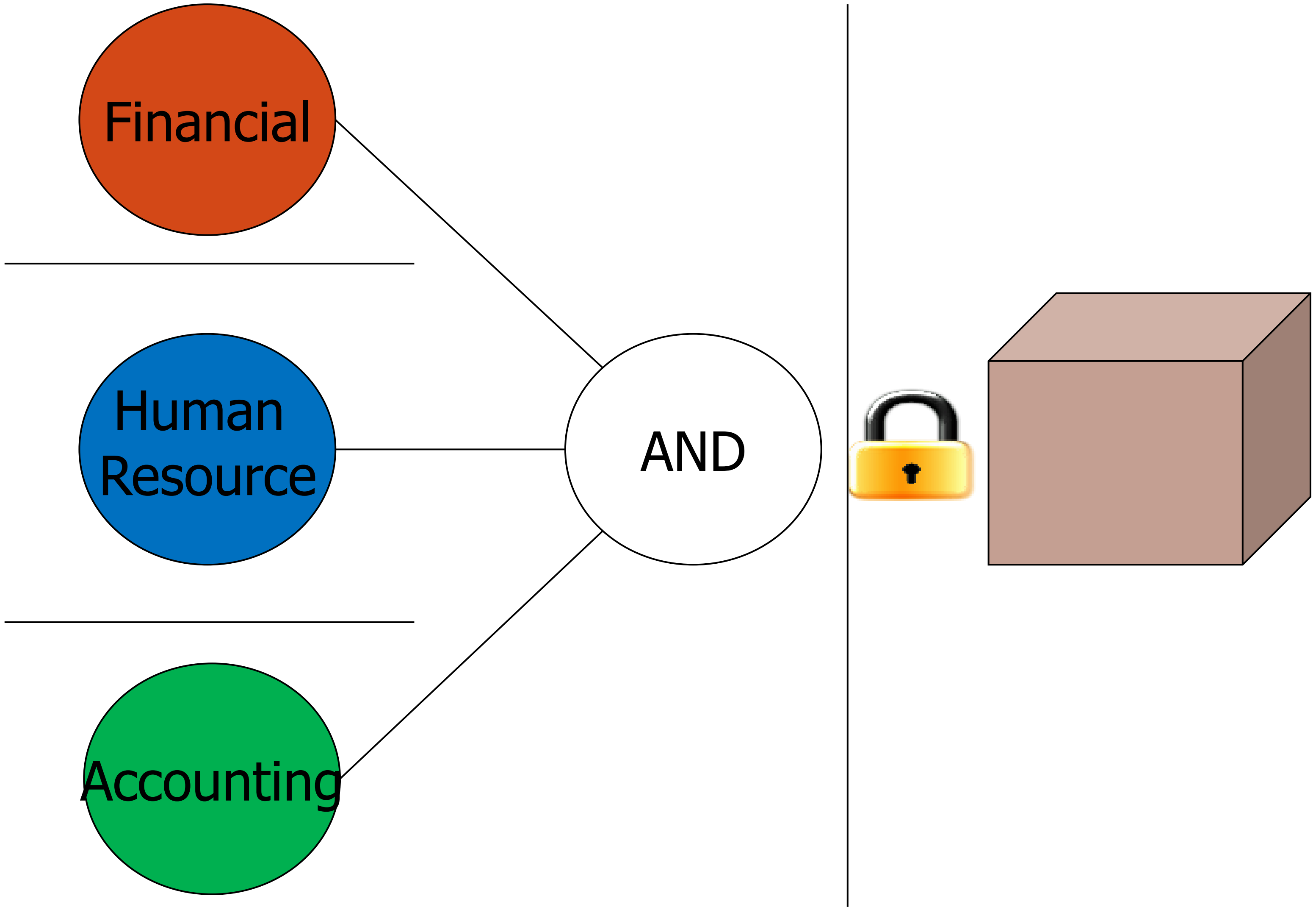
In a company structure, it is obvious requiring high level managers involvement from different departments to access company confidential data probably saved in the cloud.

Requirement of GO-ABE – Confidential Data Access



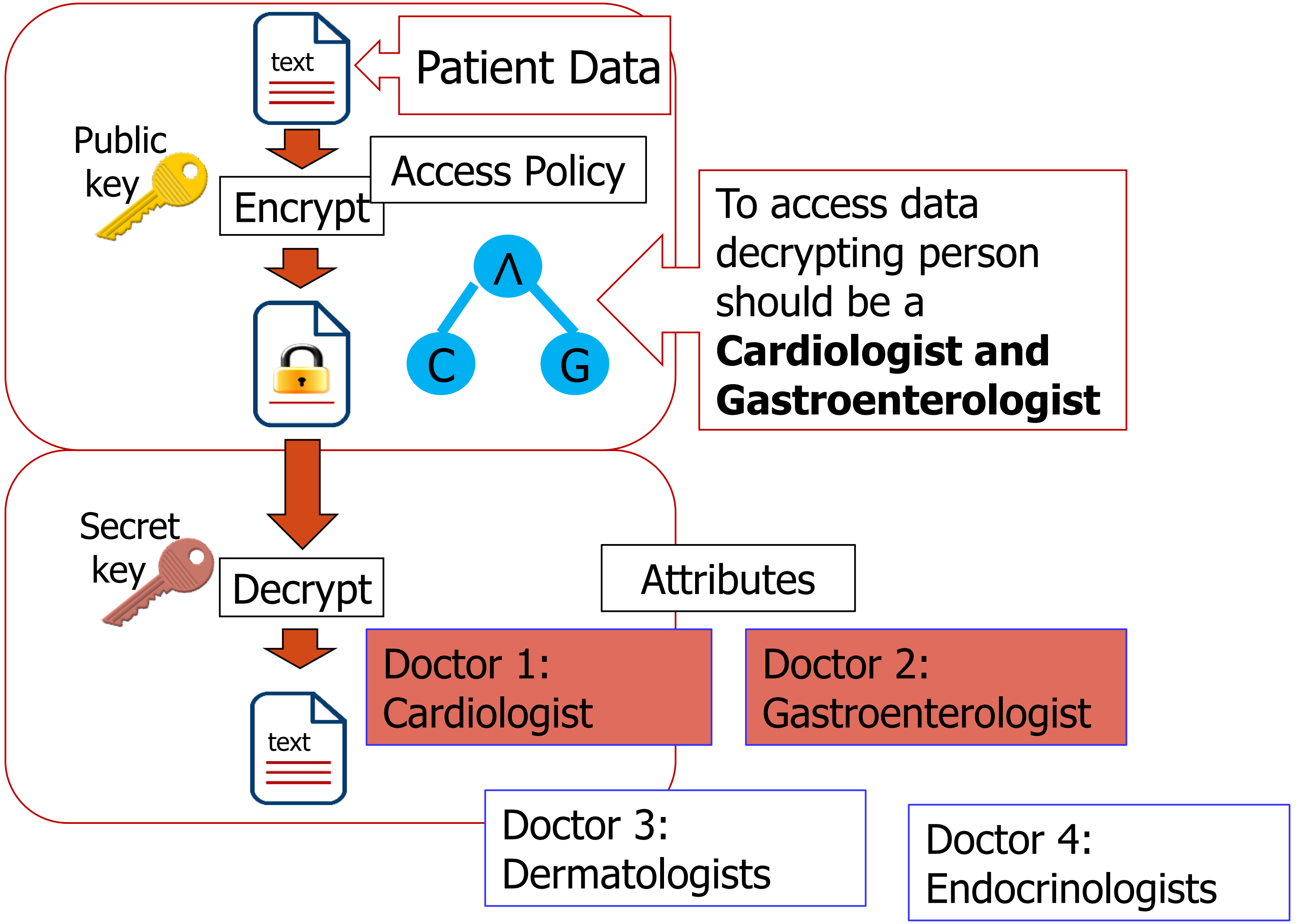
But CP-ABE allows a single party who possesses all the required attributes to access data. It is not practical because no manager may hold all the positions from different departments.

Requirement of GO-ABE – Confidential Data Access



Allow managers from all required departments to collaborate for accessing data – which is the real requirement of company structure

Requirement of GO-ABE – Access Patient Data [Li et al. 2015]



Doctor 1 (**Cardiologist**) and Doctor 2 (**Gastroenterologist**) collaborate

GO-ABE [Li et al. 2015]

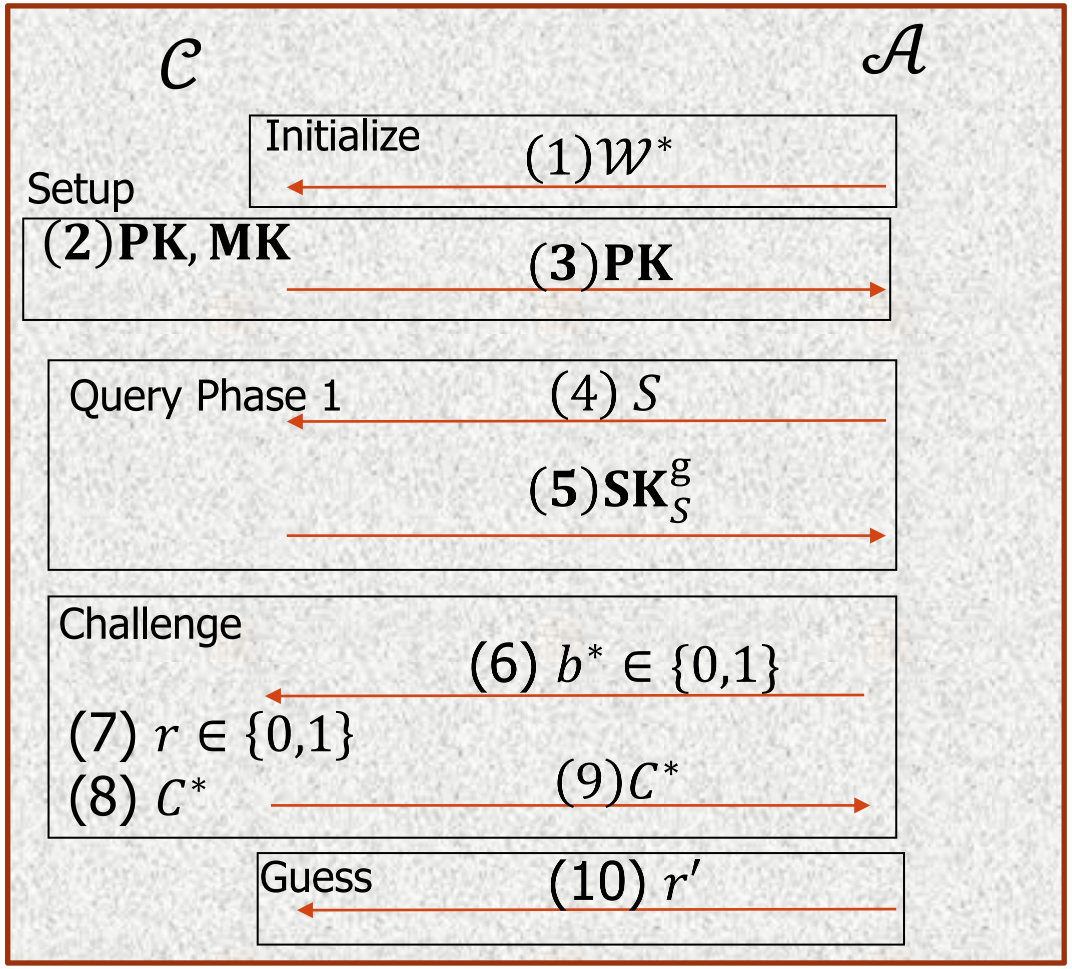
Algorithm	Input	Output
Setup	Security parameter λ	Public parameter **PK** Master secret key **MK**
Encryption	Public parameter **PK** Message M Access Policy $\mathcal{W}$	Ciphertext C
KeyGen	Public parameter **PK** Master secret key **MK** Group id g Attribute set S	Decryption Key $\mathbf{SK}_S^g$
Decryption	Ciphertext C Public parameter **PK** Group id g	Message M

Cooperating user attribute sets:
$U = S_1 \cup S_2 \cup \cdots \cup S_N$
Decrypt if $|\mathcal{W} \cap U| \geq t$,
t is the threshold value

- Satisfies the selective set model security

Selective Set-model Security

The adversary's goal is to determine which of the two messages is encrypted using the predefined attribute set $\mathcal{W}^*$.



$\mathcal{A}$ is an adversary against selective-set model anonymity.
$\mathcal{C}$ is a Challenger.
(1) $\mathcal{A}$ sends the challenging access structure $\mathcal{W}^*$.
(2) $\mathcal{C}$ creates PK and MK
(3) Gives PK to $\mathcal{A}$.
(4) $\mathcal{A}$ queries private keys for attribute set $S \neq \mathcal{W}^*$ and
(5) $\mathcal{C}$ replies with $\mathbf{SK}_\mathbf{S}^\mathbf{g}$ quering his own oracle.
(6) $\mathcal{A}$ sends the message $b^* \in \{0,1\}$.
(7) $\mathcal{C}$ selects a random $r \in \{0,1\}$.
(8) If $r = 0; c_1^*, c_2^*$ are honest values. Else selects randomly.
(9) $\mathcal{C}$ outputs $C^* = (\mathcal{W}^*, c_1^*, c_2^*)$
(10) $\mathcal{A}$ sends r'.
If $r' = r$ then $\mathcal{A}$ wins.

GO-ABE [Li et al. 2015]

- Group Oriented Attribute-based Encryption (GO-ABE) allows
  - **Users** from the **Same Group**

    to cooperate to decrypt a ciphertext
  - **Without revealing** their **secret keys**

Users from the same group are able to cooperate with each other to decrypt a ciphertext encrypted under a set of attributes α such that a single user may not have enough attributes to match the attribute set α [Li et al. 2015].

Li et al.'s proposal is constructed using bilinear mappings.
Not quantum safe

Our Goal

- Provide a quantum safe construction for the GO-ABE scheme

  - What are the supporting primitives / building blocks in our proposal
    - Lattice-based cryptography
    - Shamir's secret sharing scheme

GO-ABE SCHEME FROM LATTICES

Lattice-based Cryptography

- Is quantum safe because computational problems like Approximate Shortest Independent Vector Problem ($SIVP_\lambda$) not broken (yet).
- We use Learning with error (LWE) and Small Integer Solution (SIS).
- LWE asked to distinguish LWE samples from truly random samples
- SIS asked to find small non-zero vector x, such that $A.x = 0 \; mod \; q$ and $\|x\|_\infty \leq \beta$

LWE: Learning With Errors

$$\begin{pmatrix} A \end{pmatrix} \begin{pmatrix} x \end{pmatrix} + \begin{pmatrix} e \end{pmatrix} = \begin{pmatrix} z \end{pmatrix}$$

For given (A,z), find (x, e)

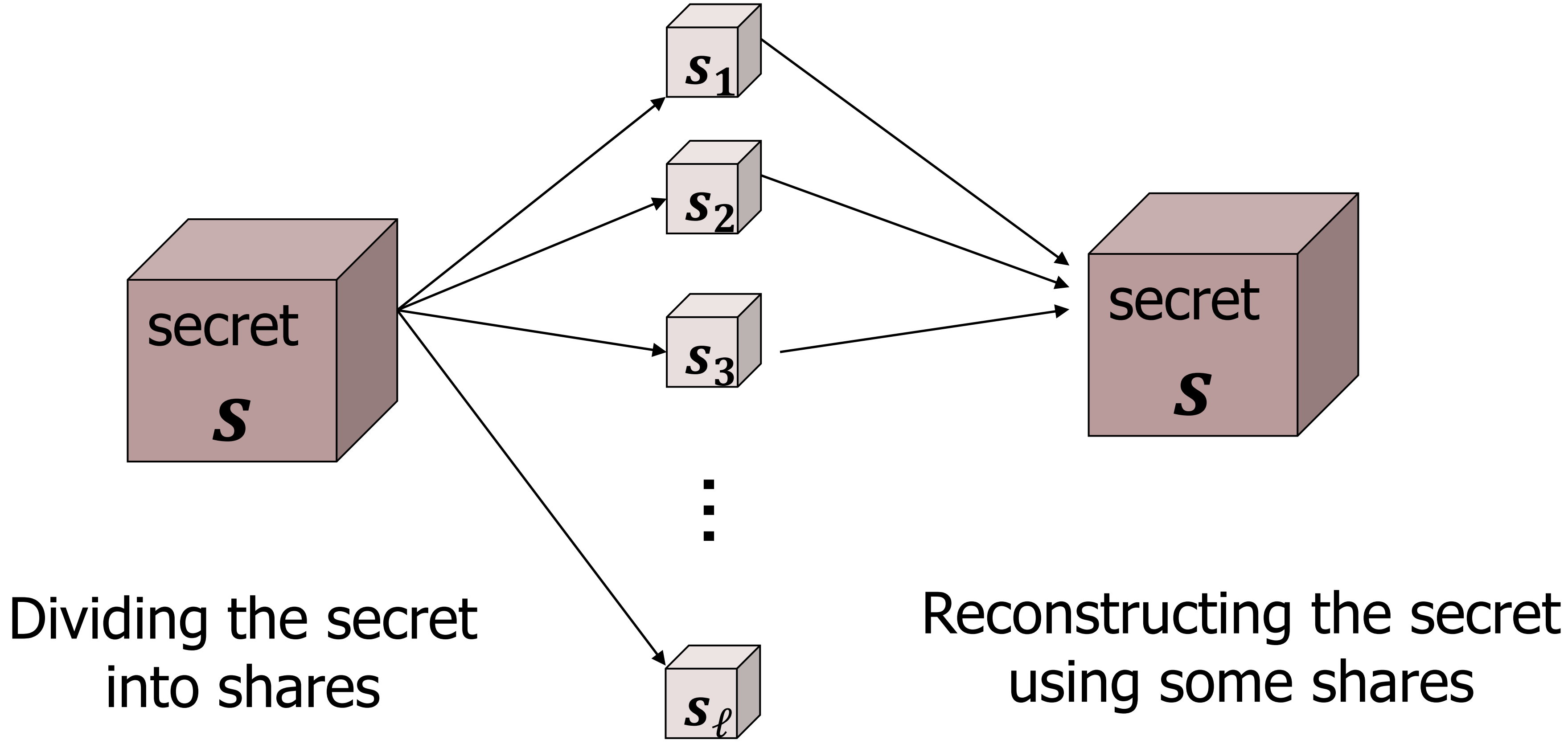
SIS: Short Integer Solution

$$\begin{pmatrix} A \end{pmatrix} \begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix} \quad \text{mod q}$$

For given (A), find non-zero vector(x)

Shamir's Secret Sharing (SSS) scheme

- A secret s is split in to ℓ shares; at least k shares should be combined to reconstruct the secret s



Why we use Shamir's Secret Sharing (SSS) scheme

GO-ABE Requirement:

Users should be from the same group
Users should keep their attribute secret keys secure

Why we use Shamir's Secret Sharing (SSS) scheme

GO-ABE Requirement:

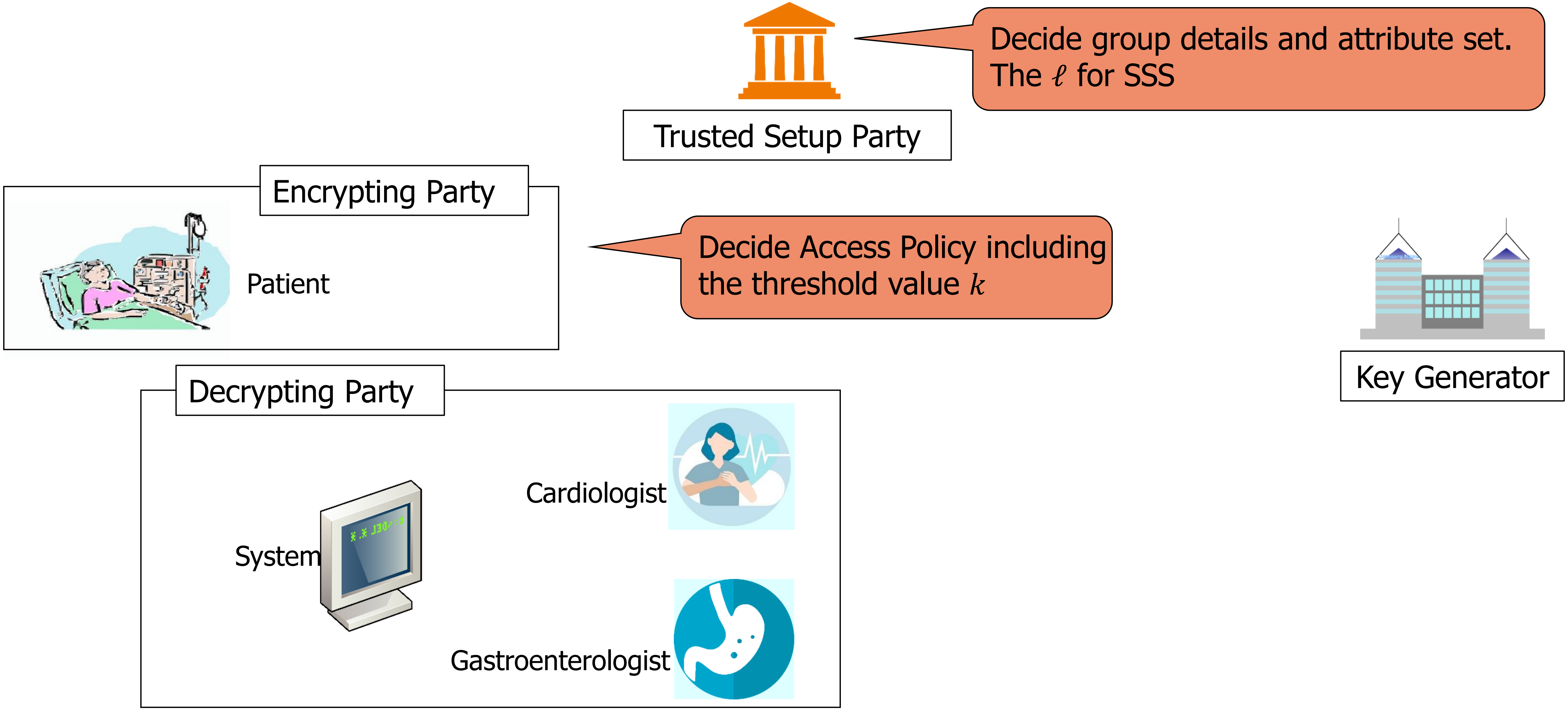
Users should be from the same group
Users should keep their attribute secret keys secure

SSS allows J shares of ℓ shares to construct the origin.
In our construction,

Public key $\mathrm{u} = (u_1, u_2, \dots, u_n)$
Share u among ℓ shares, such that j-th share vector $\hat{u}_j = \left(\hat{u}_{j,1}, \dots, \hat{u}_{j,n}\right)$
The fractional Lagrangian coefficient L_j is calculated such that, $u = \sum_{j \in J} L_j$, where $J \subset [\ell]$

❖Our proposal does not use SSS to reconstruct a secret; use for proving the users are from the same group.
❖Shares are used to generate secret keys of individual users.

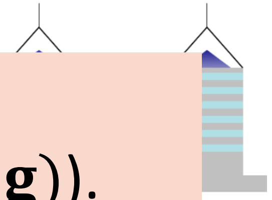
Our Proposal: GO-ABE scheme construction from Lattices



Our Proposal: GO-ABE scheme construction from Lattices

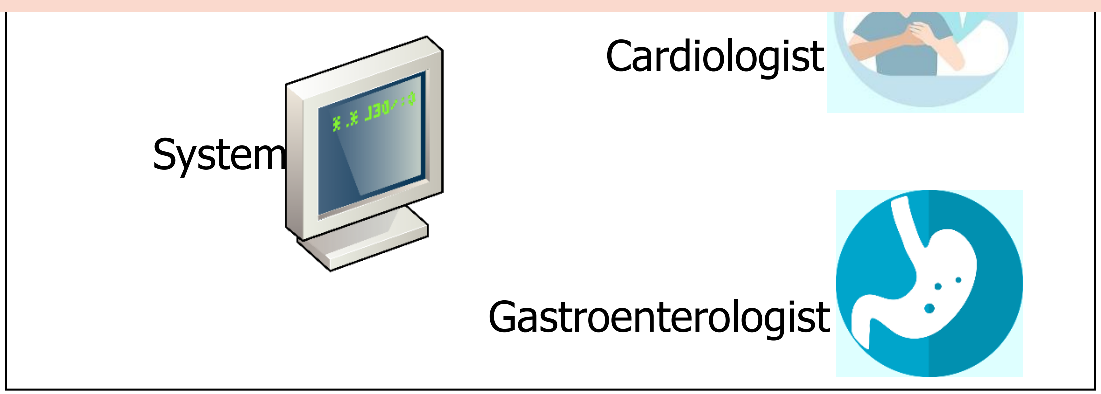
Trusted Setup Party

Encrypting Party



ator

Let
each group has an id g and has unique group public key ($\mathbf{GPK} = (\mathbf{G}, \mathbf{G}_0, \mathbf{G}_1, \mathbf{g})$).
and a secret key ($\mathbf{GSK} = \mathbf{T}$) selected from $(\mathbf{G}, \mathbf{T_G}) \leftarrow$ TrapGen(n, m, q) and
$\mathbf{G}_0, \mathbf{G}_1 \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{g} \in \mathbb{Z}_q^n$ randomly.



Our Proposal: GO-ABE scheme construction from Lattices

Setup(λ)→ $\left(\textbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right), \textbf{MK} = \{\mathbf{T}\}_{i\in[\ell]}\right)$

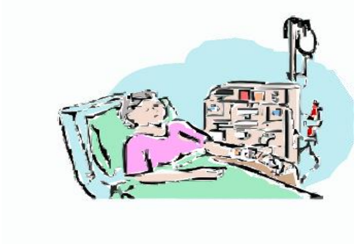
1. For all attribute $i \in \mathbb{A}$:

$$\mathbf{A}_{i=1}^{\ell}, \mathbf{T}_{i=1}^{\ell} \leftarrow \mathrm{TrapGen}(n, m, q)$$

2. Select vector $\mathbf{u} \in \mathbb{Z}_q^n$

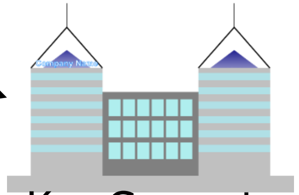
Trusted Setup Party

$\textbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$



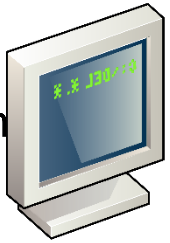
$\textbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$

$\textbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$
$\textbf{MK} = \{\mathbf{T}\}_{i\in[\ell]}$



Key Generator

System



Our Proposal: GO-ABE scheme construction from Lattices

Encrypt($\mathbf{PK}$, $M, \mathcal{W}$)→ $(C = c_1, c_2)$

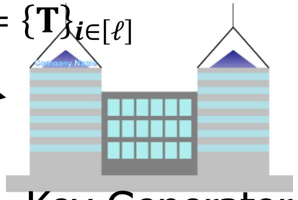
1. Let $\mathrm{D} \stackrel{\text{def}}{=} (\ell!)^2$
2. Select $\mathbf{s} \in \mathbb{Z}_q^n$, for $i \in [w]$: $\mathbf{e}_i \in \mathbb{Z}_q^m$, and $e \in \mathbb{Z}_q$
3. $c_1 = \mathbf{A}_i^T \mathbf{s} + D\mathbf{e}_i$ for $i \in [w]$,
   $c_2 = \mathbf{u}^T s + De + M\lfloor q/2 \rceil$

Trusted Setup Party

Setup(λ)→ $\left(\mathbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right), \mathbf{MK} = \{\mathbf{T}\}_{i\in[\ell]}\right)$

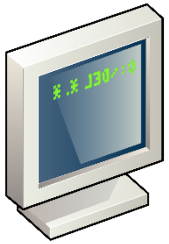
1. For all attribute $i \in \mathbb{A}$:
   $\mathbf{A}_{i=1}^{\ell}, \mathbf{T}_{i=1}^{\ell} \leftarrow \mathrm{TrapGen}(n, m, q)$
2. Select vector $u \in \mathbb{Z}_q^n$

$\mathbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$
$\mathbf{MK} = \{\mathbf{T}\}_{i\in[\ell]}$



Key Generator

$\mathbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$



$\mathbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$

Our Proposal: GO-ABE scheme construction from Lattices

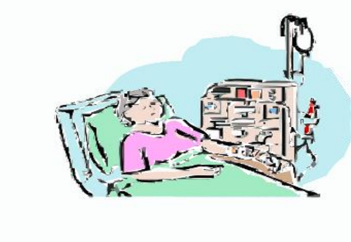
Encrypt(**PK** , $M, \mathcal{W}$)→ $(C = c_1, c_2)$

1. Let $\mathrm{D} \stackrel{\text{def}}{=} (\ell!)^2$
2. Select $\mathbf{s} \in \mathbb{Z}_q^n$, for $i \in [w]$: $\mathbf{e}_i \in \mathbb{Z}_q^m$, and $e \in \mathbb{Z}_q$
3. $c_1 = \mathbf{A}_i^T \mathbf{s} + D\mathbf{e}_i$ for $i \in [w]$,
   $c_2 = \mathbf{u}^T s + De + M\lfloor q/2 \rfloor$

Trusted Setup Party

Setup(λ)→ $\left(\textbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right), \textbf{MK} = \{\mathbf{T}\}_{i\in[\ell]}\right)$

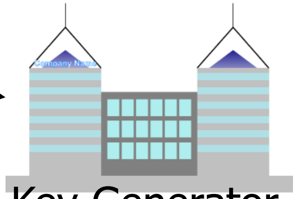
1. For all attribute $i \in \mathbb{A}$:
   $\mathbf{A}_{i=1}^{\ell}, \mathbf{T}_{i=1}^{\ell} \leftarrow \mathrm{TrapGen}(n, m, q)$
2. Select vector $u \in \mathbb{Z}_q^n$



PK $= \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$

PK $= \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$

PK $= \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$
MK $= \{\mathbf{T}\}_{i\in[\ell]}$

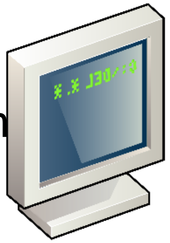


Key Generator

KeyGen(**PK** , **MK**, $\mathbf{g}$, S)→ $\left(\mathbf{SK}_S^{\mathbf{g}} = \left(\left(\boldsymbol{x}_1^d, \ldots, \boldsymbol{x}_s^d\right), \boldsymbol{d}\right)\right)$

1. For a group: $\mathbf{G}, \mathbf{T_G} \leftarrow \mathrm{TrapGen}(n, m, q)$
   $\mathbf{G_0}, \mathbf{G_1} \in \mathbb{Z}_q^{m\times n}$, $\mathbf{g} \in \mathbb{Z}_q^n$
   Set **GPK** $= (\mathbf{G}, \mathbf{G_0}, \mathbf{G_1}, \mathbf{g})$, **GSK** $= \mathbf{T_G}$
2. User id $d \in \mathbb{N}$
3. Use SSS on $\mathbf{u}$, such that $\mathbf{u} = \sum_{j\in J} L_j \cdot \hat{\mathbf{u}}_j$
4. For $i \in S$:
   $\mathbf{v}_i \leftarrow \mathrm{SamplePre}(\mathbf{A}_\mathrm{i}, \mathbf{T}_\mathrm{i}, \hat{\mathbf{u}}_i - \mathrm{g}, \sigma)$; $\mathbf{A}_\mathrm{i} \cdot \mathbf{v}_i = \hat{\mathbf{u}}_i - \mathbf{g}$
5. Compute $\mathbf{G}_d = [\mathbf{G}|\mathbf{G}_0 + d\mathbf{G}_1]$ and
   $\mathbf{T}_d \leftarrow \mathbf{ExtBasis}(\mathbf{T}_G, \mathbf{G}_d)$
6. For $i \in S$: $\boldsymbol{x}_i^d \leftarrow \mathrm{SamplePre}(\mathbf{G}_d, \mathbf{T}_d, \mathbf{v}_i, \sigma)$; $\mathbf{G} \cdot \boldsymbol{x}_i^d = \mathbf{v}_i$

$\mathbf{SK}_{S=Cardi}^{\mathbf{g}}$



System

$\mathbf{SK}_{S=Gas}^{\mathbf{g}}$

Our Proposal: GO-ABE scheme construction from Lattices

Encrypt(**PK** , $M, \mathcal{W}$)→ $(C = c_1, c_2)$

1. Let D $\stackrel{\text{def}}{=} (\ell!)^2$
2. Select $\mathbf{s} \in \mathbb{Z}_q^n$, for $i \in [w]$: $\mathbf{e}_i \in \mathbb{Z}_q^m$, and $e \in \mathbb{Z}_q$
3. $c_1 = \mathbf{A}_i^T \mathbf{s} + D\mathbf{e}_i$ for $i \in [w]$,
   $c_2 = \mathbf{u}^T s + De + M\lfloor q/2 \rfloor$

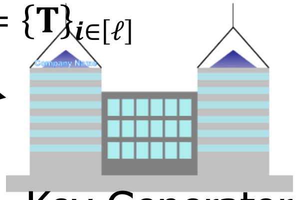
Trusted Setup Party

Setup(λ)→ $\left(\mathbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right), \mathbf{MK} = \{\mathbf{T}\}_{i\in[\ell]}\right)$

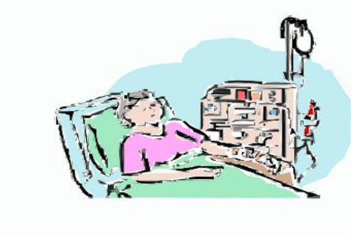
1. For all attribute $i \in \mathbb{A}$:
   $\mathbf{A}_{i=1}^{\ell}, \mathbf{T}_{i=1}^{\ell} \leftarrow \mathsf{TrapGen}(n, m, q)$
2. Select vector $u \in \mathbb{Z}_q^n$

PK $= \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$

MK $= \{\mathbf{T}\}_{i\in[\ell]}$



Key Generator

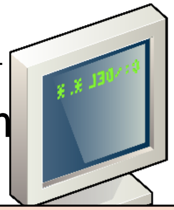


PK $= \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$

PK $= \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right)$

Decrypt(**PK** , C, $\mathbf{g}$)→ M

M

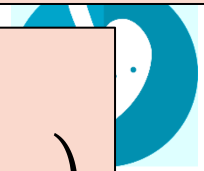


System

$\mathbf{y}_C$

$\mathbf{y}_G$

$\mathbf{SK}_{S=Cardi}^{\mathbf{g}}$



$\mathbf{SK}_{S=Gas}^{\mathbf{g}}$

KeyGen(**PK** , **MK**, $\mathbf{g}$, S)→ $(\mathbf{SK}_S^{\mathbf{g}} = ((\boldsymbol{x}_1^d, \ldots, \boldsymbol{x}_S^d), \boldsymbol{d}))$

1. For a group:
   $\mathbf{G}, \mathbf{T_G} \leftarrow \mathsf{TrapGen}(n, m, q)$

GSK $= \mathbf{T_G}$

3. Use SSS on $\mathbf{u}$, such that $\mathbf{u} = \sum_{j\in J} L_j \cdot \hat{\mathbf{u}}_j$
4. For $i \in S$:
   $\mathbf{v}_i \leftarrow \mathsf{SamplePre}(\mathbf{A}_i, \mathbf{T}_i, \hat{\mathbf{u}}_i - g, \sigma)$; $\mathbf{A}_i \cdot \mathbf{v}_i = \hat{\mathbf{u}}_i - \mathbf{g}$
5. Compute $\mathbf{G}_d = [\mathbf{G}|\mathbf{G}_0 + d\mathbf{G}_1]$ and
   $\mathbf{T}_d \leftarrow \mathbf{ExtBasis}(\mathbf{T}_G, \mathbf{G}_d)$
6. For $i \in S$: $\boldsymbol{x}_i^d \leftarrow \mathsf{SamplePre}(\mathbf{G}_d, \mathbf{T}_d, \mathbf{v}_i, \sigma)$; $\mathbf{G} \cdot \boldsymbol{x}_i^d = \mathbf{v}_i$

Compute $\mathbf{G}_d = [\mathbf{G}|\mathbf{G}_0 + d\mathbf{G}_1]$
publishes $\mathbf{y}_i = (\mathbf{G}_d \cdot \boldsymbol{x}_i)$

Calculate L_i; $\sum_{i\in[k]} L_i \mathbf{A}_i \mathbf{y}_i = \mathbf{u} \bmod q$

Compute $r \leftarrow c_2 - \left((k \times \mathbf{g})^T + \sum_{i\in[k]} L_i \mathbf{y}_i^{\mathbf{T}} \boldsymbol{c}_1\right)$

If $|r| < \frac{q}{4}$,output 0, else 1 as the message M

ation

Our Proposal: GO-ABE scheme construction from Lattices

Encrypt($\mathbf{PK}, M, \mathcal{W}$)→ ($C = c_1, c_2$)

1. Let $\mathrm{D} \overset{\text{def}}{=} (\ell!)^2$
2. Select $\mathbf{s} \in \mathbb{Z}_q^n$, for $i \in [w]$: $\mathbf{e}_i \in \mathbb{Z}_q^m$, and $e \in \mathbb{Z}_q$
3. $c_1 = \mathbf{A}_i^T \mathbf{s} + D\mathbf{e}_i$ for $i \in [w]$,
   $c_2 = \mathbf{u}^T s + De + M\lfloor q/2 \rfloor$

Trusted Setup Party

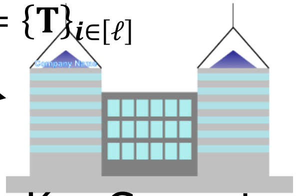
Setup(λ)→ $\left(\mathbf{PK} = \left(\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u}\right), \mathbf{MK} = \{\mathbf{T}\}_{i\in[\ell]}\right)$

1. For all attribute $i \in \mathbb{A}$:
   $\mathbf{A}_{i=1}^{\ell}, \mathbf{T}_{i=1}^{\ell} \leftarrow \mathrm{TrapGen}(n, m, q)$
2. Select vector $u \in \mathbb{Z}_q^n$

$\mathbf{PK} = (\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u})$

$\mathbf{PK} = (\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u})$

$\mathbf{PK} = (\{\mathbf{A}\}_{i\in[\ell]}, \mathbf{u})$
$\mathbf{MK} = \{\mathbf{T}\}_{i\in[\ell]}$



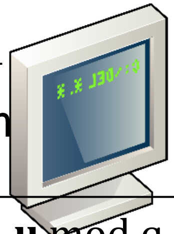
Key Generator

KeyGen($\mathbf{PK}, \mathbf{MK}, \mathbf{g}, S$)→ $\left(\mathbf{SK}_S^{\mathrm{g}} = \left(\left(\boldsymbol{x}_1^d, \ldots, \boldsymbol{x}_S^d\right), \boldsymbol{d}\right)\right)$

1. For a group:
   $\mathbf{G}, \mathbf{T_G} \leftarrow \mathrm{TrapGen}(n, m, q)$
   $\mathbf{G_0}, \mathbf{G_1} \in \mathbb{Z}_q^{m\times n}$, $\mathrm{g} \in \mathbb{Z}_q^n$
   Set **GPK** = $(\mathbf{G}, \mathbf{G_0}, \mathbf{G_1}, \boldsymbol{g})$, **GSK** $= \mathbf{T_G}$
2. User id $d \in \mathbb{N}$
3. Use SSS on $\mathbf{u}$, such that $\mathbf{u} = \sum_{j\in J} L_j \cdot \hat{\mathbf{u}}_j$
4. For $i \in S$:
   $\mathbf{v}_i \leftarrow \mathrm{SamplePre}(\mathbf{A}_\mathrm{i}, \mathbf{T}_\mathrm{i}, \hat{\mathbf{u}}_i - \mathrm{g}, \sigma)$; $\mathbf{A}_\mathrm{i} \cdot \mathbf{v}_i = \hat{\mathbf{u}}_i - \mathbf{g}$
5. Compute $\mathbf{G}_d = [\mathbf{G}|\mathbf{G}_0 + d\mathbf{G}_1]$ and
   $\mathbf{T}_d \leftarrow \mathbf{ExtBasis}(\mathbf{T}_G, \mathbf{G}_d)$
6. For $i \in S$: $\boldsymbol{x}_i^d \leftarrow \mathrm{SamplePre}(\mathbf{G}_d, \mathbf{T}_d, \mathbf{v}_i, \sigma)$; $\mathbf{G} \cdot \boldsymbol{x}_i^d = \mathbf{v}_i$

Decrypt($\mathbf{PK}, C, \mathbf{g}$)→ M

M



System

$\mathbf{y}_C$

$\mathbf{SK}_{S=Cardi}^{\mathrm{g}}$

$\mathbf{y}_G$

$\mathbf{SK}_{S=Gas}^{\mathrm{g}}$

Calculate L_i; $\sum_{i\in[k]} L_i \mathbf{A}_i\, \mathbf{y}_\mathrm{i} = \mathbf{u} \bmod \mathrm{q}$
Compute $r \leftarrow c_2 - \left((k \times \mathbf{g})^T + \sum_{i\in[k]} L_i \mathbf{y}_i^{\mathbf{T}} \boldsymbol{c}_1\right)$
If $|r| < \frac{q}{4}$, output 0, else 1 as the message M

Compute $\mathbf{G}_d = [\mathbf{G}|\mathbf{G}_0 + d\mathbf{G}_1]$
publishes $\mathbf{y}_i = (\mathbf{G}_d \cdot \boldsymbol{x}_i)$

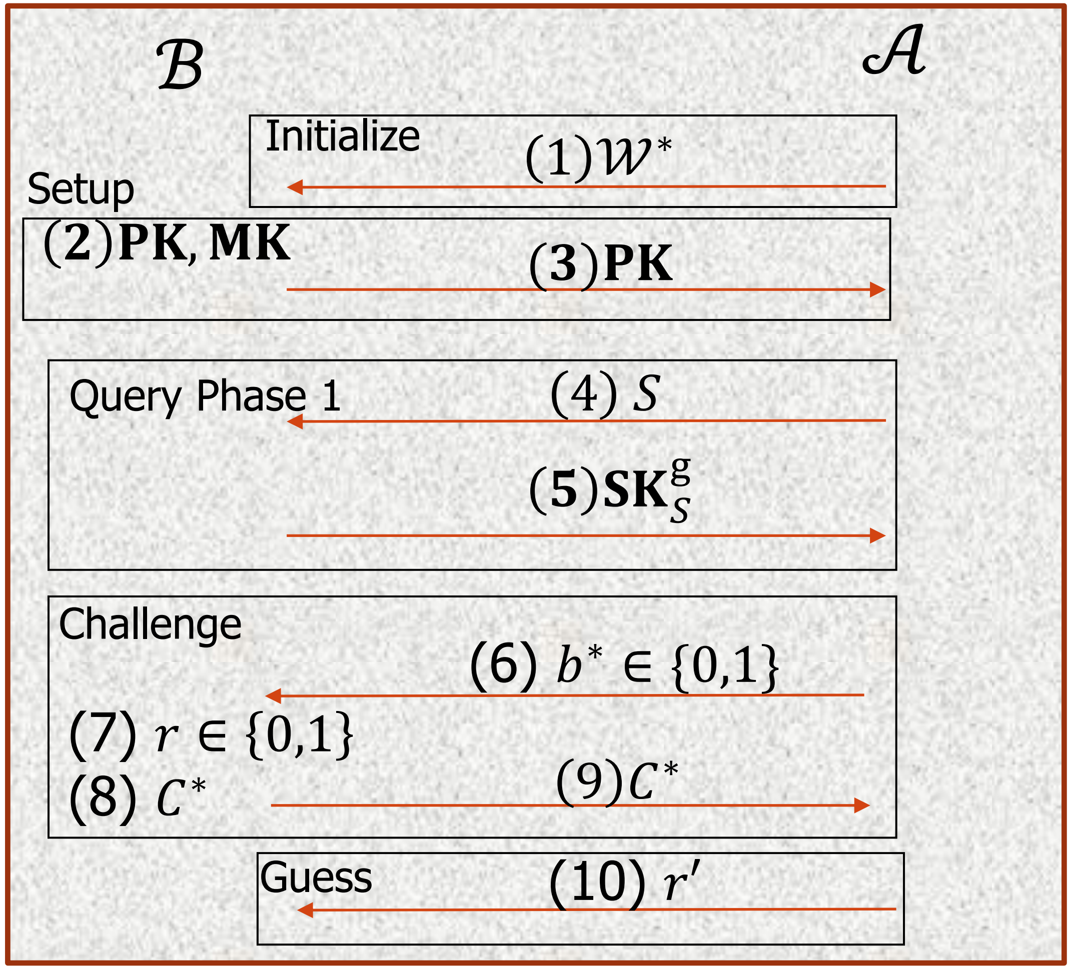
Security Proof

- Based on the hardness of Decision-LWE problem we proved that Lattice-based construction of GO-ABE scheme provides ciphertext privacy in the Selective-Set model.
- Selective-Set model: The adversary declares the attribute set $\mathcal{W}$ that he wishes to be challenged upon.

Theorem 1. *If there is an adversary $\mathcal{A}$ with advantage > 0 against the selective-set model for the GO-ABE scheme, then there exists a PPT algorithm $\mathcal{B}$ that can solve the decision-LWE problem.*

Selective Set-model Security

Proof. The simulator $\mathcal{B}$ uses the adversary $\mathcal{A}$ to distinguish LWE oracle $\mathcal{O}$. First $\mathcal{B}$ queries the LWE oracle $\mathcal{O}$ for $(\ell m + 1)$ times and obtain LWE samples $(a_k, b_k) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $k \in \{0,1,2, \ldots, m\}$. Then $\mathcal{B}$ proceeds as below.



Initialize: $\mathcal{A}$ announces to $\mathcal{W}^*$ to $\mathcal{B}$

Setup: $\mathcal{B}$ selects LWE challenges $\{(a_0, b_0), (a_i^1, b_i^1), (a_i^2, b_i^2), \ldots (a_i^m, b_i^m)\}_{i \in [\ell]}$ for public matrices $\widehat{\mathbf{A}_i}$ and a_0 as $\mathbf{u}$

Phase 1: $\mathcal{B}$ answers each private key query by selecting parameters from LWE

Challenge: When $\mathcal{A}$ sends $b^* \in \{0,1\}$, $\mathcal{B}$ uses $\mathcal{W}^*$ and sets $c_1 = \left(Db_i^1, Db_i^2, \ldots, Db_i^m\right)$ for $i \in [\ell]$
$c_2 = Da_0 + M_b\lfloor q/2 \rfloor$ if he wishes to generate C^*. That is $r = 0$. Otherwise he randomly selects values.

Guess: $\mathcal{A}$ outputs b' If

Summary

- We present the Lattice based construction of GO-ABE scheme
- We employed Shamir's Secret Sharing Scheme to satisfy GO-ABE requirements
- **Limitations**:

  1. Efficiency is less in decryption because need to collect users' shares; however, this is reasonable fulfilling practical applications like access company confidential data

  ----

  2. Only AND-gets on multivalued attributes are considered; not complex access policies
  3. There is no tracing mechanism to track cooperated users
  4. The cooperating situation is not controlled
  5. Issues may occur due to the use of SSS:

     Ex: If any structural change happens like introducing new attributes, need recreate all the keys

Thank you for Listening

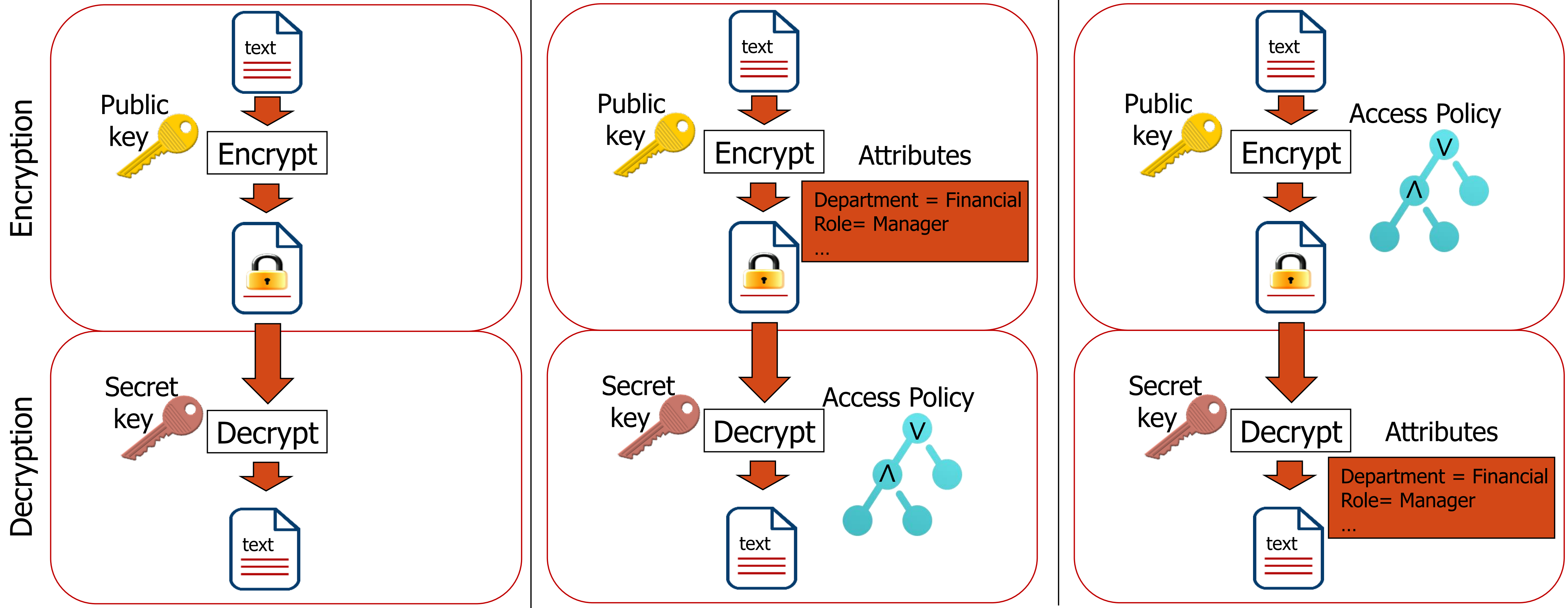
perera.nisansala@atr.jp

Attribute-based Encryption (ABE)

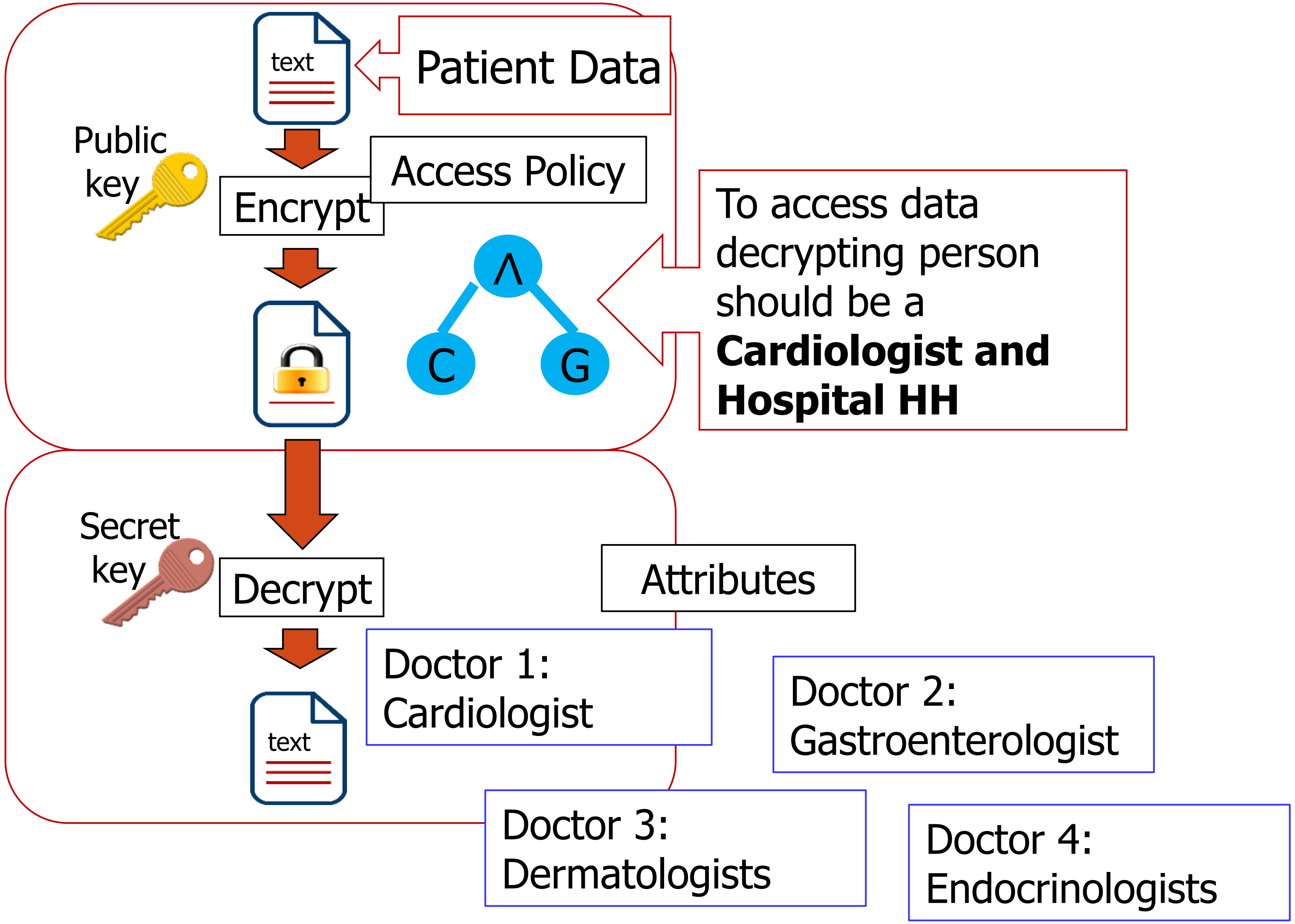
Public-key Encryption (PKE)
公開鍵暗号

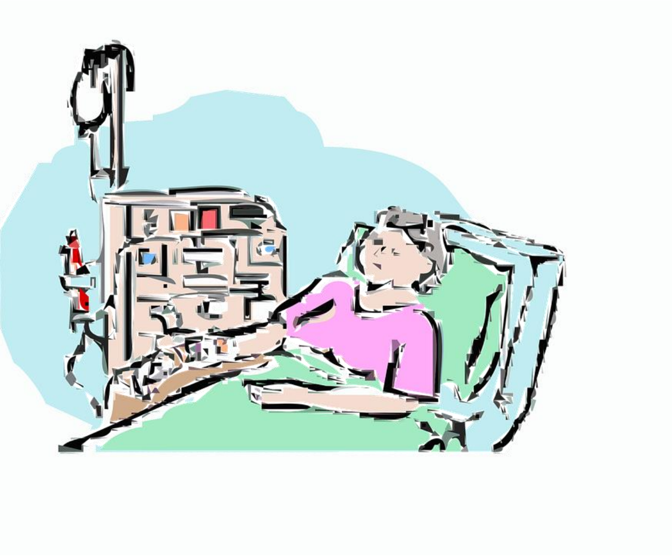
Key-Policy Attribute-based Encryption (KP-ABE)

Ciphertext-Policy Attribute-based Encryption (CP-ABE)

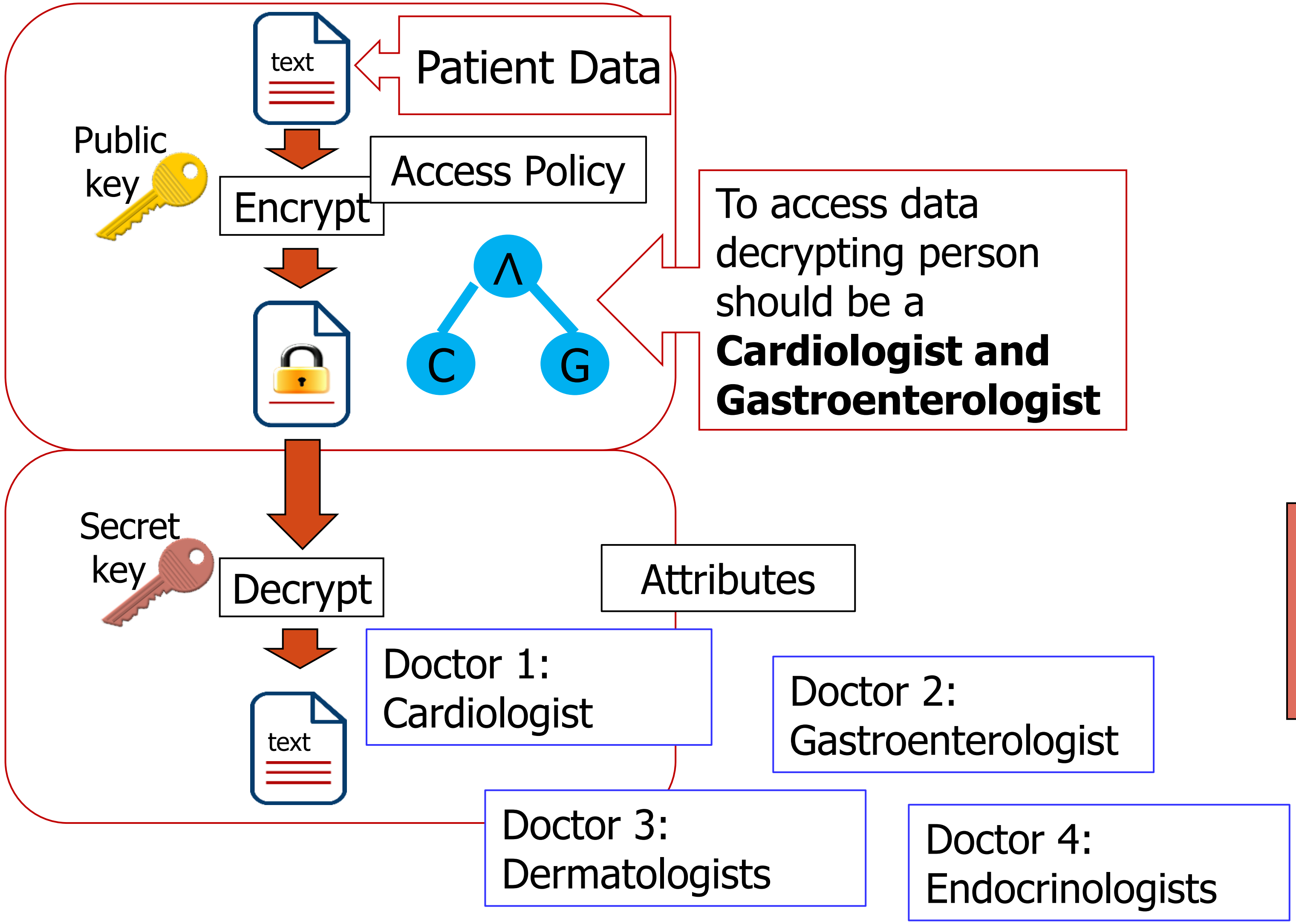


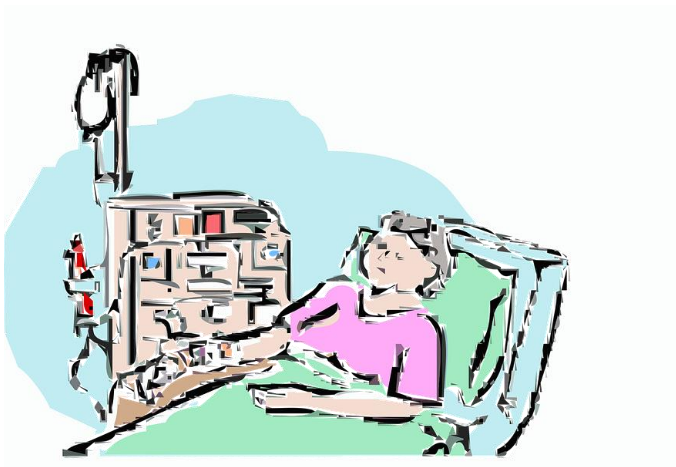
CP-ABE Application – Patient Health Record System??





Necessity of GO-ABE [Li et al. 2015]

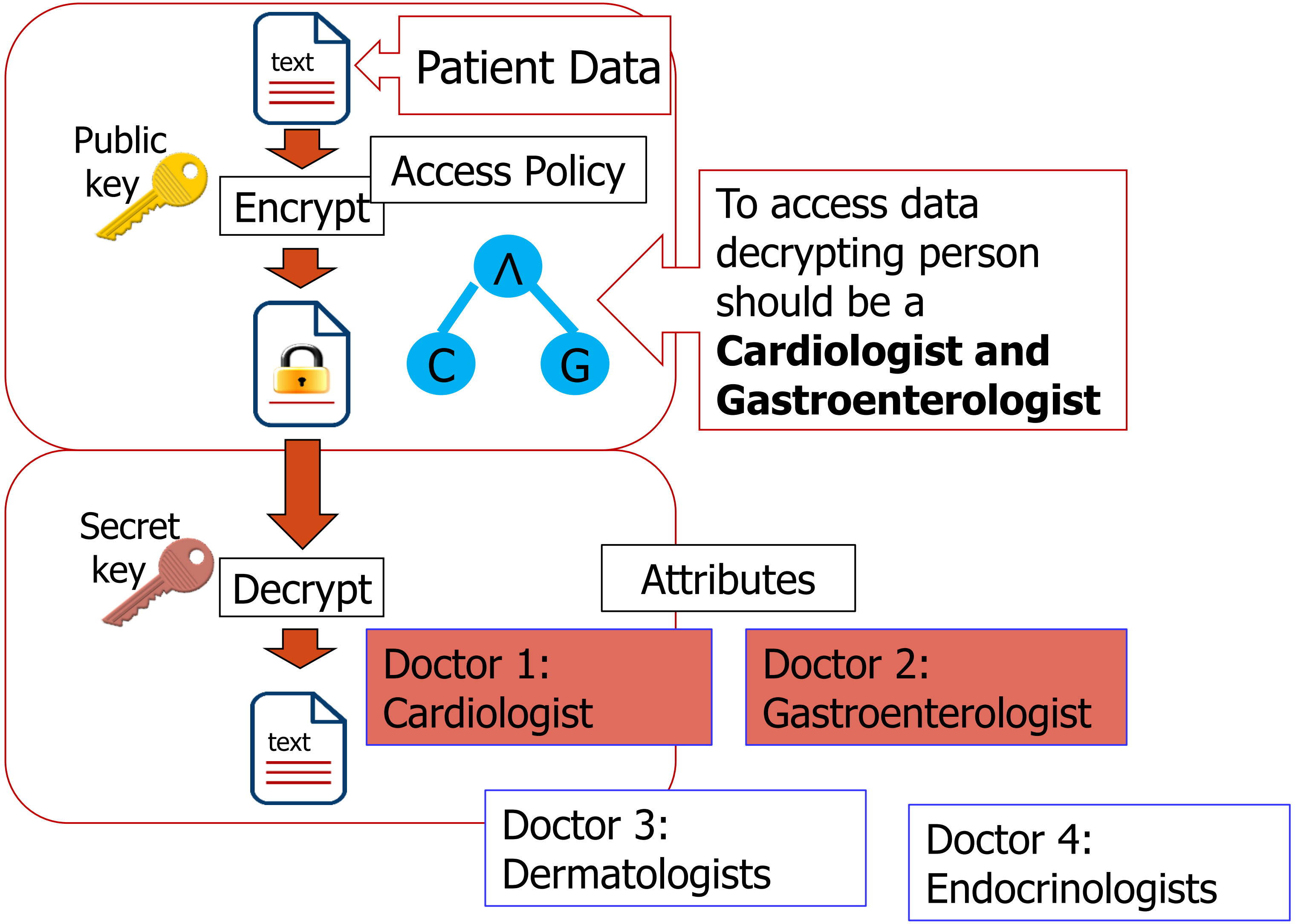




Since any doctor cannot satisfy the Access Policy Patient's life is in danger

Li, Mengting, et al. "GO-ABE: group-oriented attribute-based encryption." *International Conference on Network and System Security*. Springer, Cham, 2015.

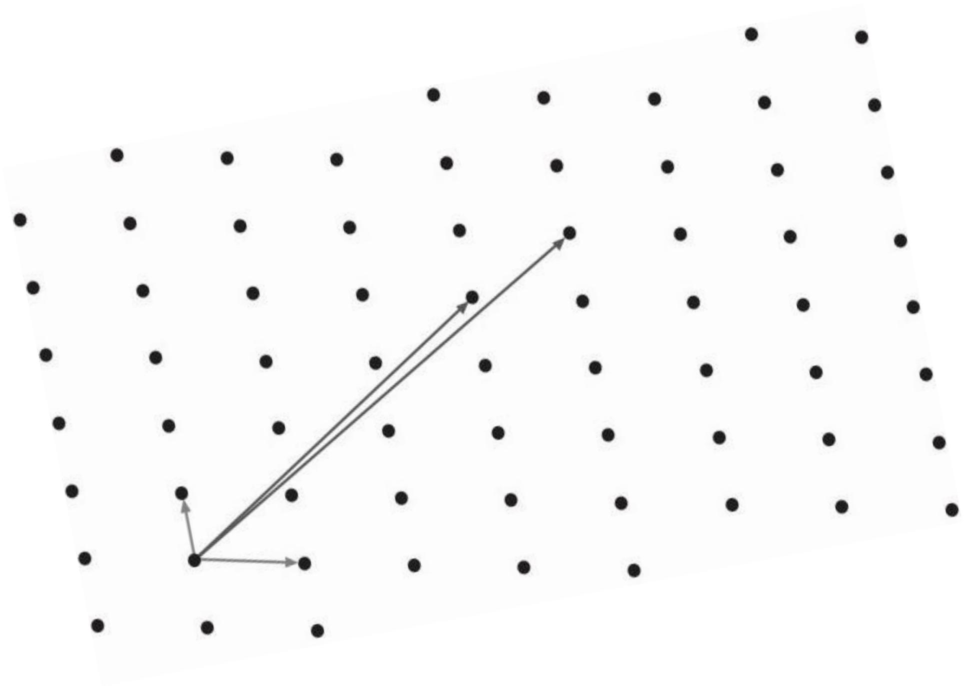
Necessity of GO-ABE [Li et al. 2015]

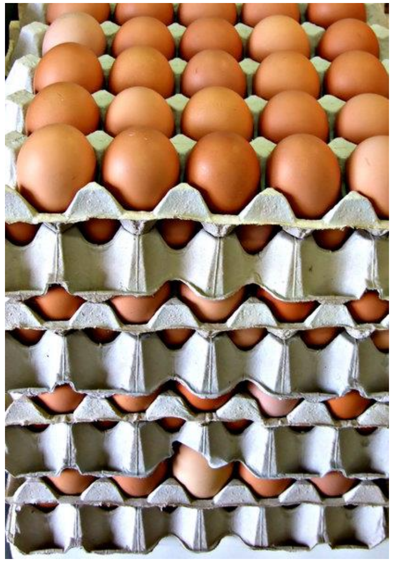


Doctor 1 (**Cardiologist**) and Doctor 2 (**Gastroenterologist**) collaborate

- Even though both numerator and denominator in Li can be bounded as a fraction of integers, when presenting Author Proof 6 M. N. S. Perera et al. as an element in Zq the value Li is arbitrarily large. The idea of clearing the denominators prevents the large-value problem of Li. Let D := (!)2 be a sufficiently large constant, such that DLi ∈ Z for all i. Multiplying noise vectors of the encryption function with D we get, Cid = IBE.Enc(id, b ∈ {0, 1})=(AT 1,id1 s+De1,..., AT ,id s+De, uT s+De +bq/2). Thus, it is sufficient to bind the below for the correctness of the IBE scheme by q/4. Dei − k i∈S DLixT i ei Since DLi is an integer bounded by D2, it is enough to select noise vectors bounded by q/4D with overwhelming probability.

Lattices





Set of points in a n-dimension space, arrange on a periodical manner

ATR