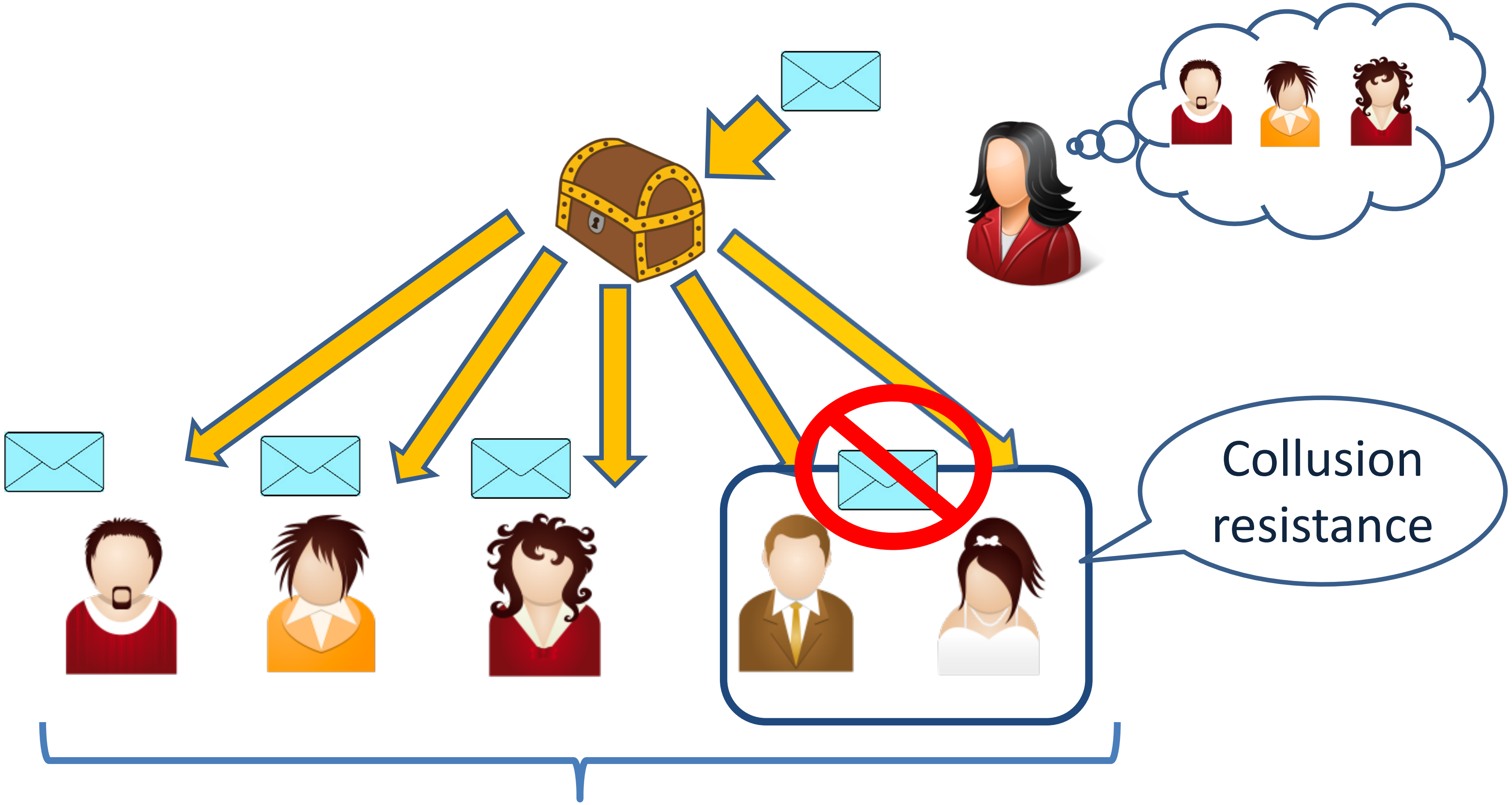
Optimal Broadcast Encryption from Pairings and LWE

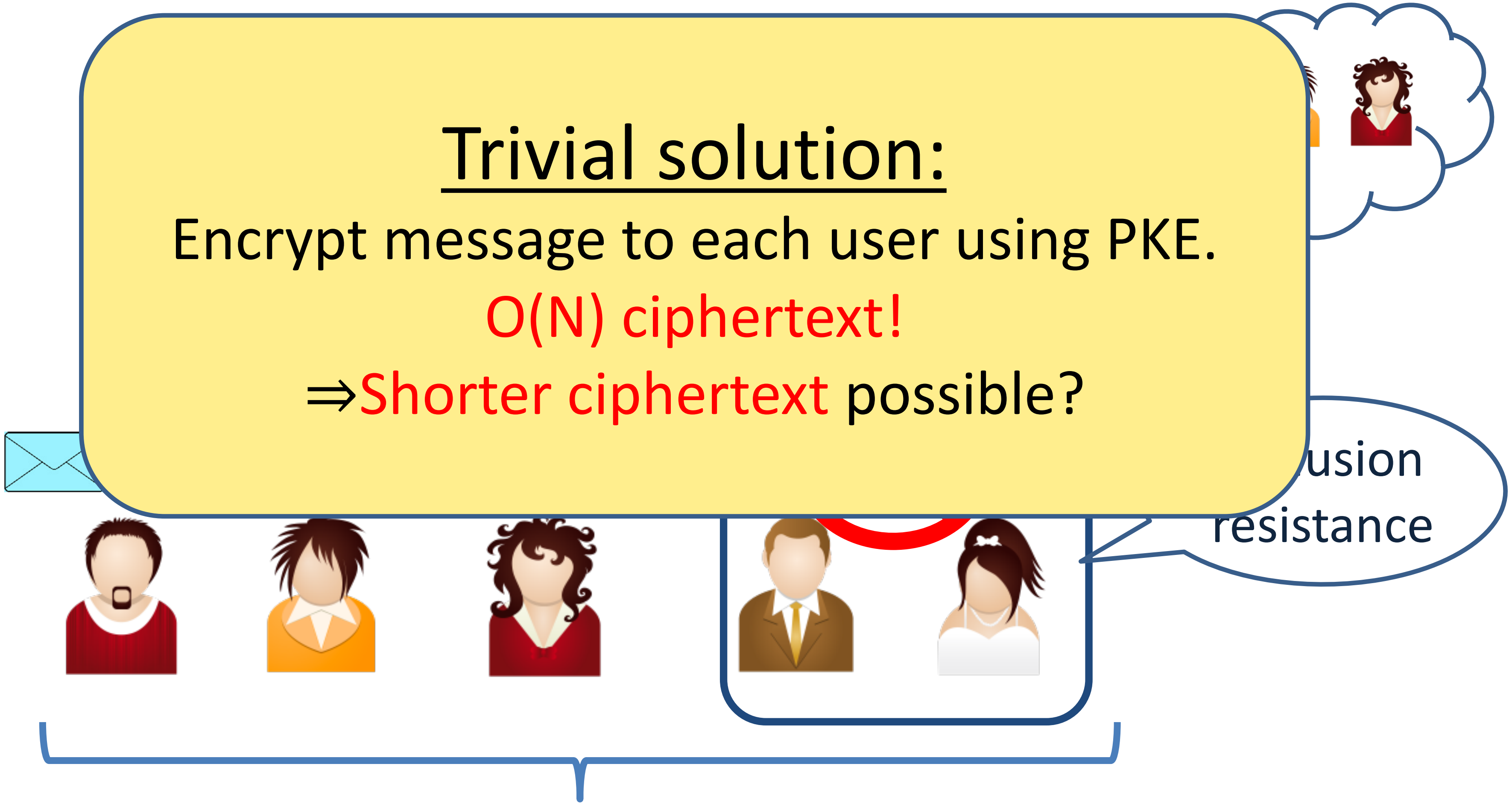
Shweta Agrawal (IIT Madras)
Shota Yamada (AIST)

Broadcast Encryption



All users in the system
(# of users = N)

Broadcast Encryption



Trivial solution:

Encrypt message to each user using PKE.

O(N) ciphertext!

⇒Shorter ciphertext possible?

All users in the system
(# of users = N)

Prior Work

	$\|\mathbf{mpk}\|$	$\|\mathbf{ct}\|$	$\|\mathbf{sk}\|$	**Assumption**
Trivial	$O(N)$	$O(N)$	$O(1)$	Plain PKE
[BGW05]	$O(N)$	$O(1)$	$O(1)$	Bilinear map
[BGW05]	$O(\sqrt{N})$	$O(\sqrt{N})$	$O(1)$	Bilinear map

Many follow-ups [GW09, DPP07, Del07, SF, AL10, HWL+16, BZ13] achieving other nice properties (adaptive security, identity based, CCA, anonymity etc.) but not improving PK size, even from iO!

- Assume full collusion resistance
- Hide poly (λ) factors

Prior Work

	$\lvert\mathbf{mpk}\rvert$	$\lvert\mathbf{ct}\rvert$	$\lvert\mathbf{sk}\rvert$	**Assumption**
Trivial	$O(N)$	$O(N)$	$O(1)$	Plain PKE
[BGW05]	$O(N)$	$O(1)$	$O(1)$	Bilinear map
[BGW05]	$O(\sqrt{N})$	$O(\sqrt{N})$	$O(1)$	Bilinear map
[BWZ14]	$O(1)$	$O(1)$	$O(1)$	log N-linear map

- Assume full collusion resistance
- Hide poly (λ) factors

Prior Work

	$\lvert\mathbf{mpk}\rvert$	$\lvert\mathbf{ct}\rvert$	$\lvert\mathbf{sk}\rvert$	**Assumption**
Trivial	$O(N)$	$O(N)$	$O(1)$	Plain PKE
[BGW05]	$O(N)$	$O(1)$	$O(1)$	Bilinear map
[BGW05]	$O(\sqrt{N})$	$O(\sqrt{N})$	$O(1)$	Bilinear map
[BWZ14]	$O(1)$	$O(1)$	$O(1)$	log N-linear map
AY20	$O(1)$	$O(1)$	$O(1)$	Bilinear map & LWE

Proof in generic group model

- Assume full collusion resistance
- Hide poly (λ) factors

Prior Work

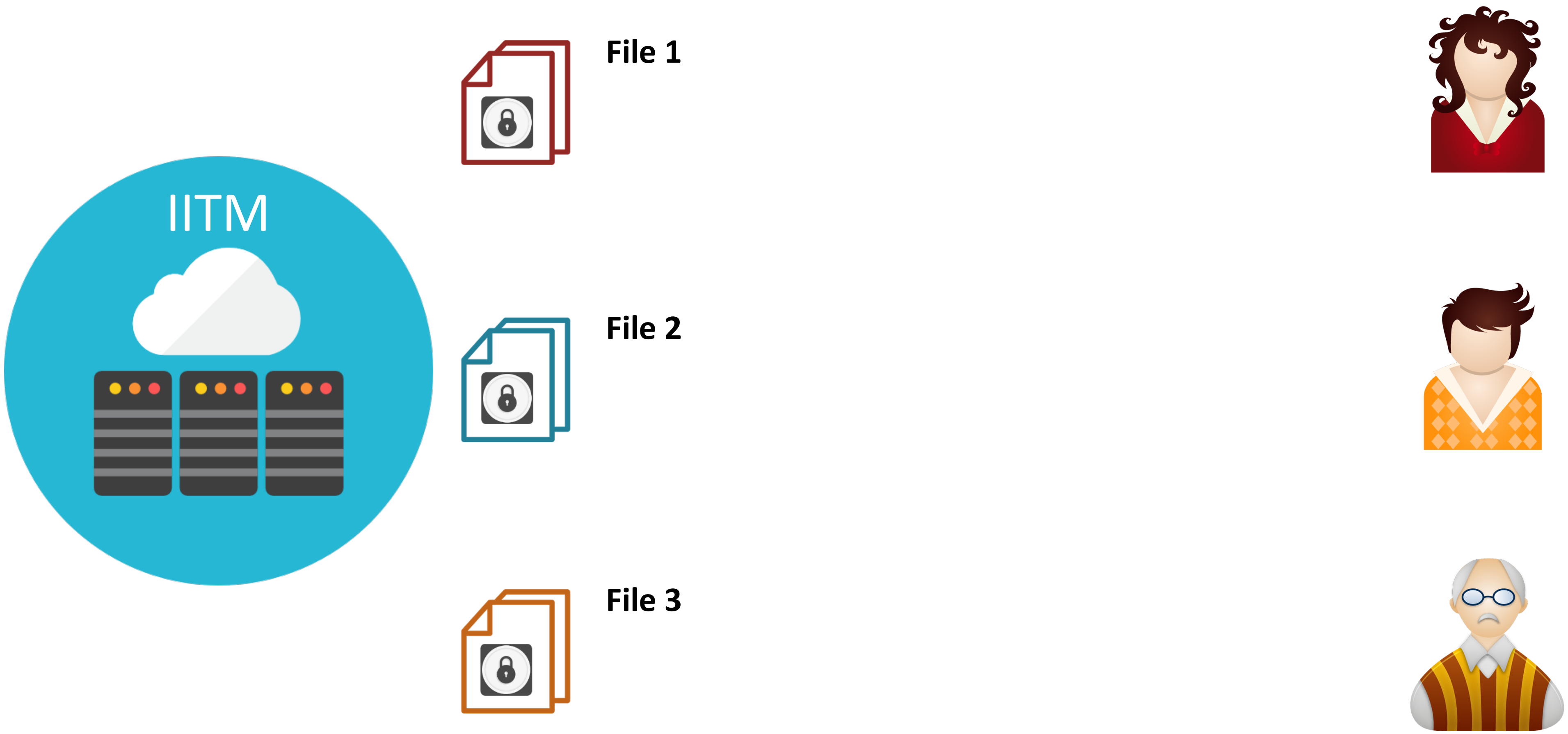
	$\lvert\mathbf{mpk}\rvert$	$\lvert\mathbf{ct}\rvert$	$\lvert\mathbf{sk}\rvert$	**Assumption**
Trivial	$O(N)$	$O(N)$	$O(1)$	Plain PKE
[BGW05]	$O(N)$	$O(1)$	$O(1)$	Bilinear map
[BGW05]	$O(\sqrt{N})$	$O(\sqrt{N})$	$O(1)$	Bilinear map
[BWZ14]	$O(1)$	$O(1)$	$O(1)$	log N-linear map
AY20	$O(1)$	$O(1)$	$O(1)$	Bilinear map & LWE
AWY20	$O(1)$	$O(1)$	$O(1)$	Bilinear map & LWE

Proof in standard model, from knowledge assumptions

- Assume full collusion resistance
- Hide poly (λ) factors

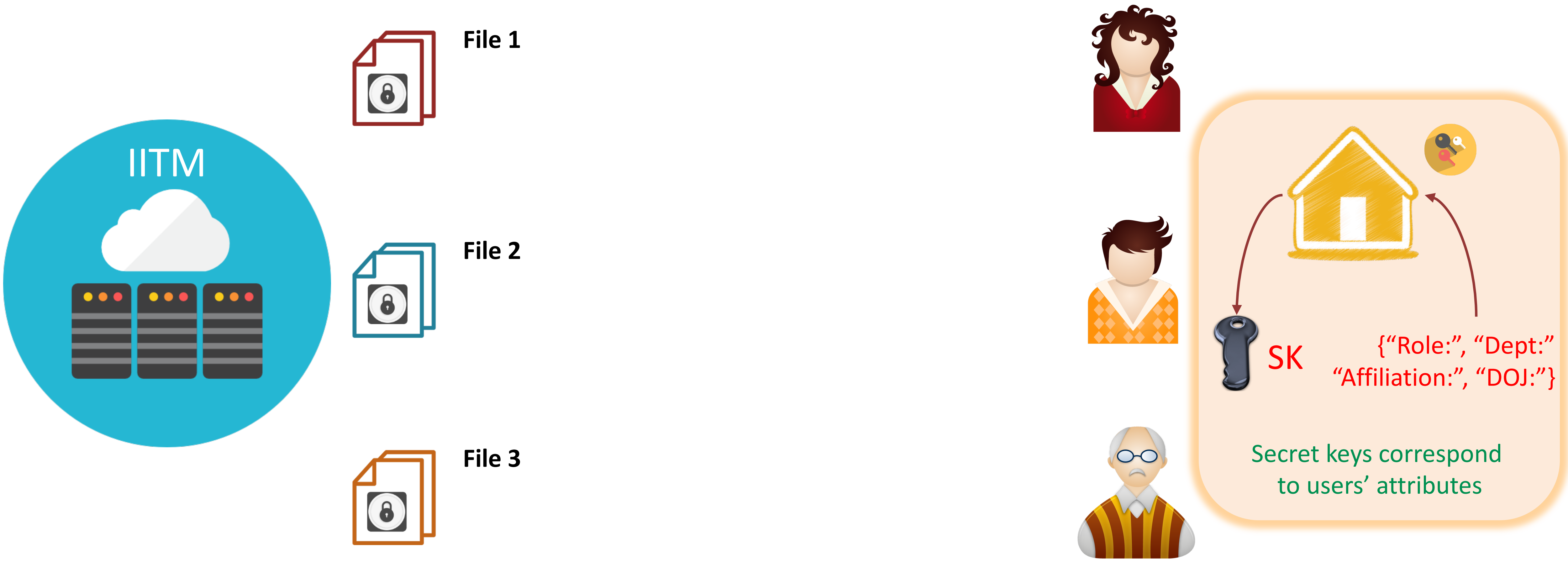
Via Connection to Attribute Based Encryption

Attribute based Encryption (ABE) [SW05, GPSW06]

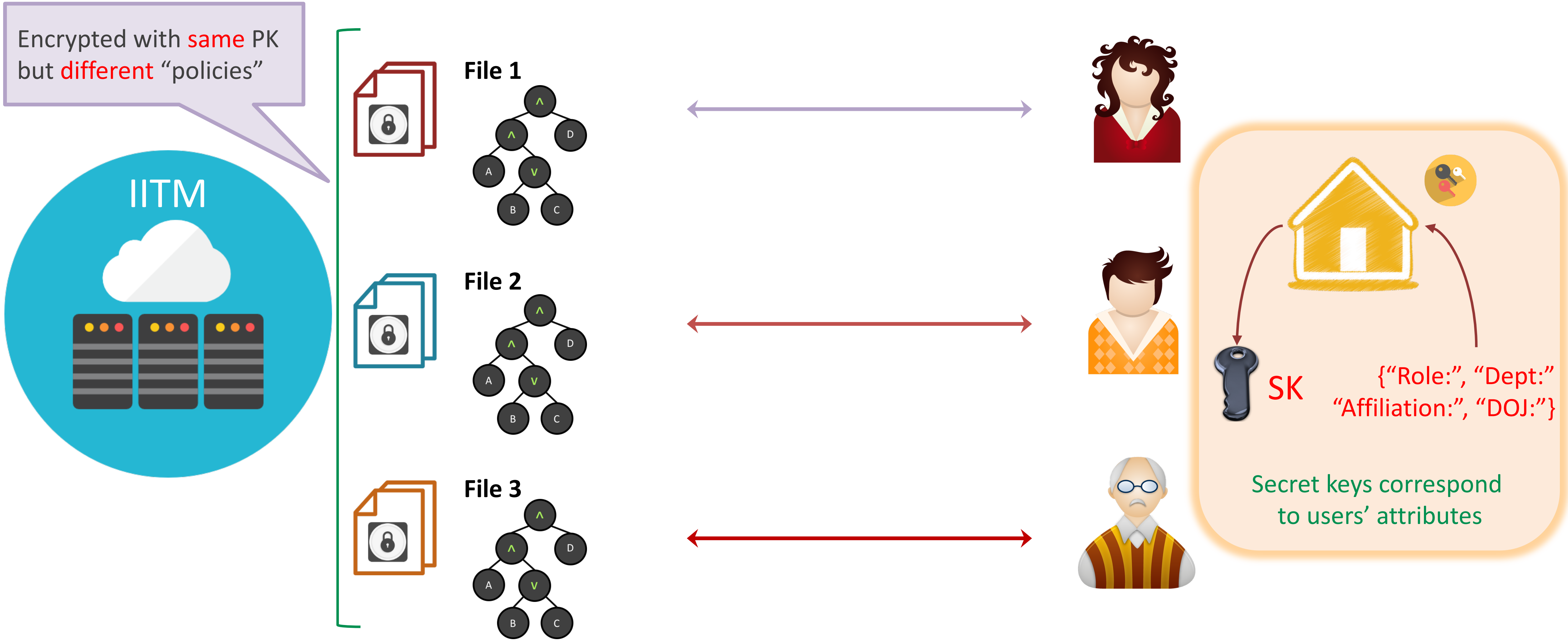


ABE Slides Credit: Monosij Maitra

Attribute based Encryption (ABE) [SW05, GPSW06]

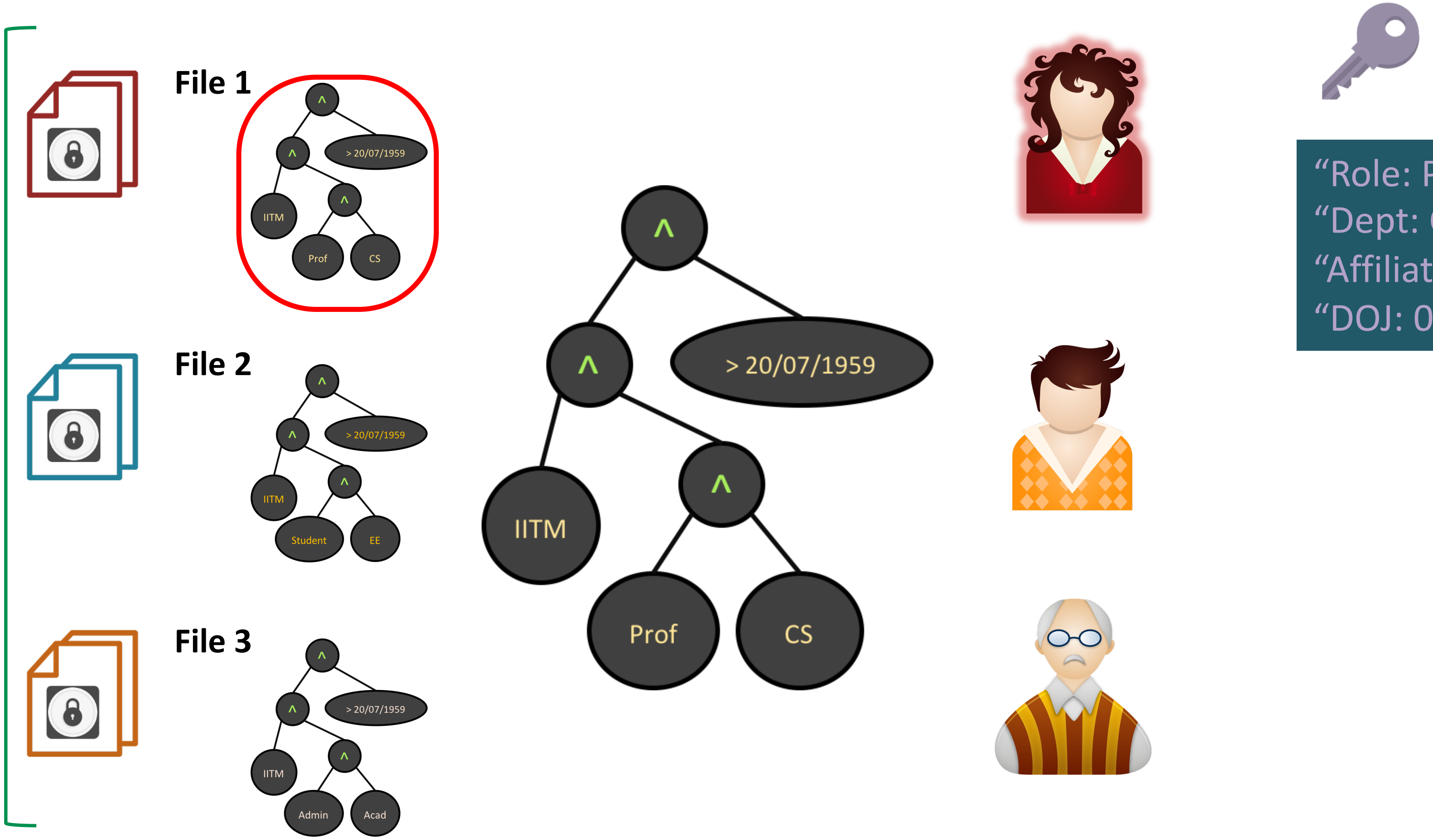


Attribute based Encryption (ABE) [SW05, GPSW06]



Attribute based Encryption (ABE) [SW05, GPSW06]

Encrypted with same PK but different "policies"

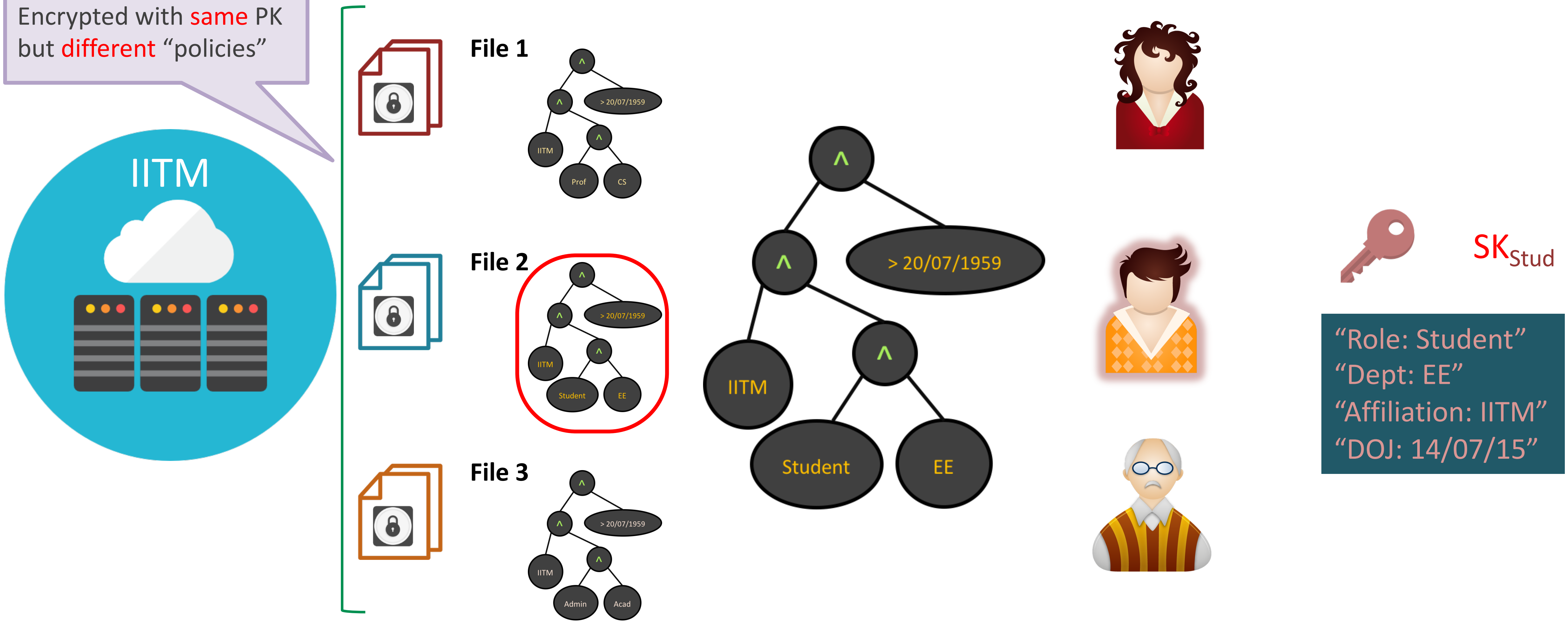


SK_{Prof}

"Role: Professor"
"Dept: CS"
"Affiliation: IITM"
"DOJ: 01/01/95"

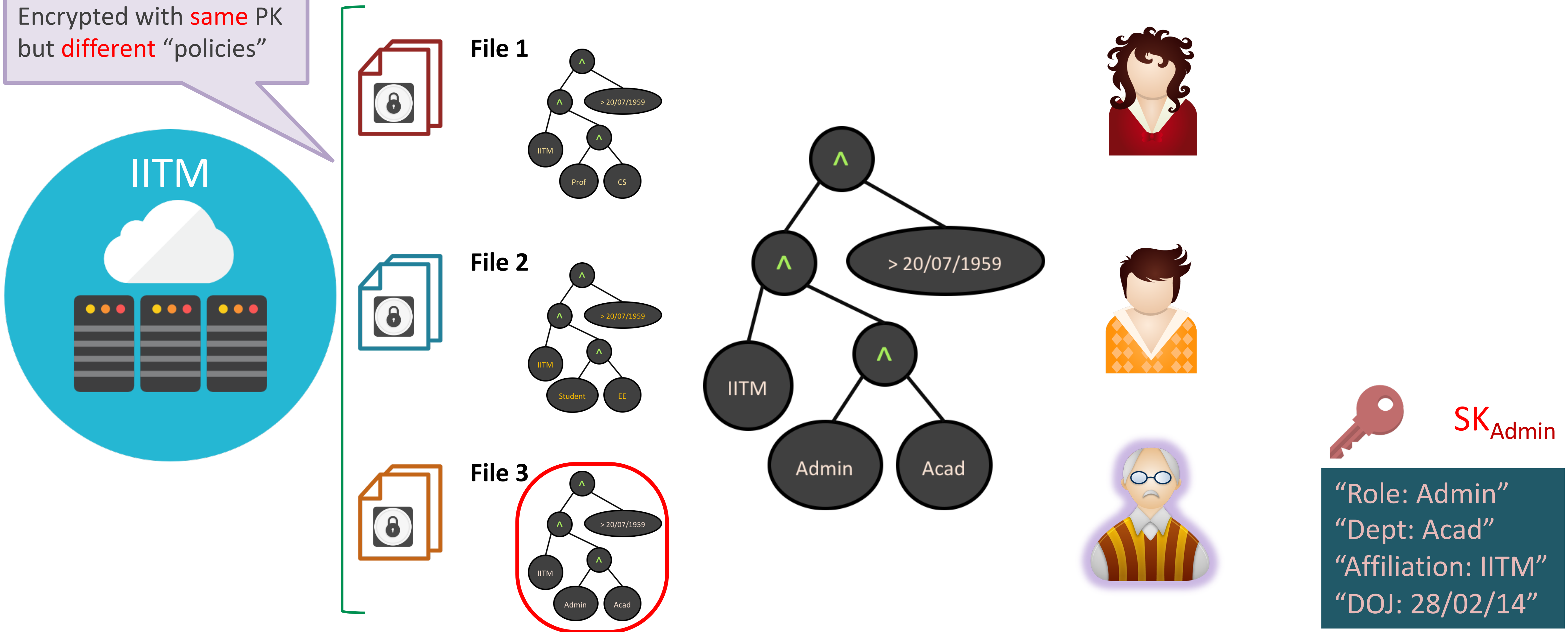
Attribute based Encryption (ABE) [SW05, GPSW06]

Encrypted with same PK but different “policies”

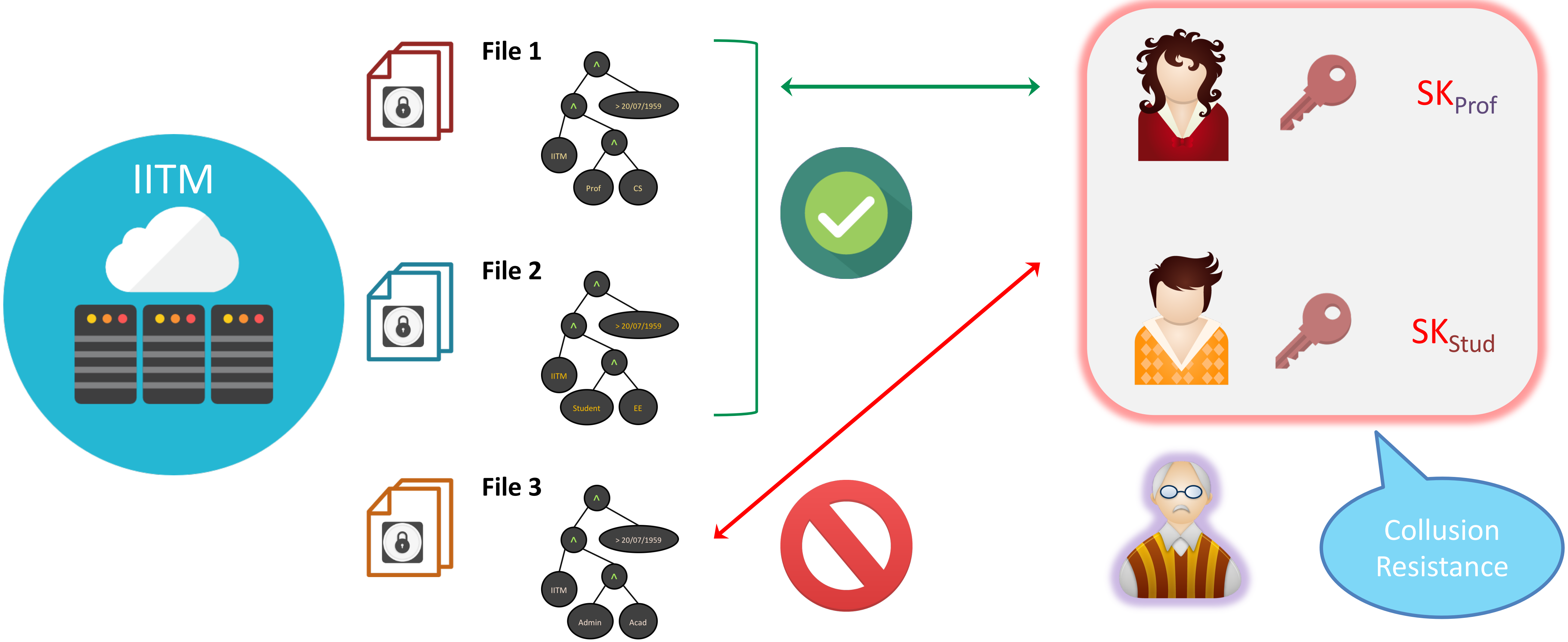


Attribute based Encryption (ABE) [SW05, GPSW06]

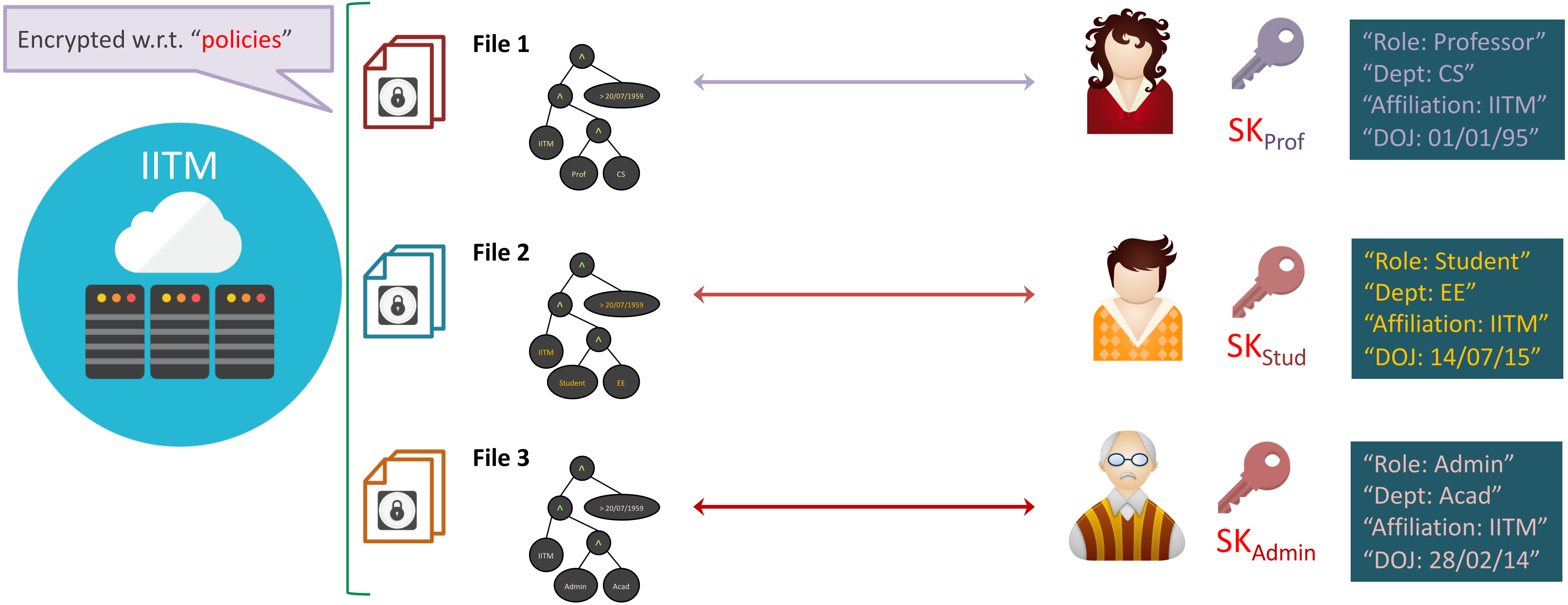
Encrypted with same PK but different "policies"



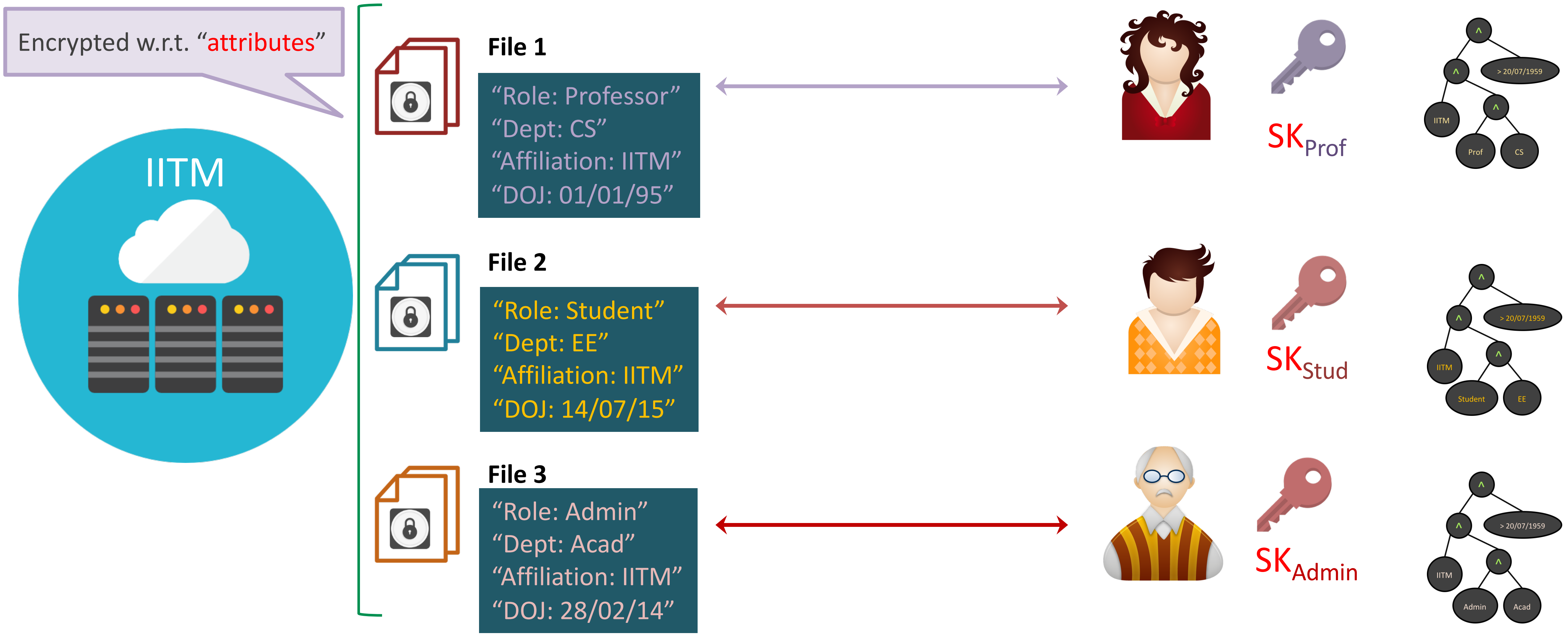
Attribute based Encryption (ABE) [SW05, GPSW06]



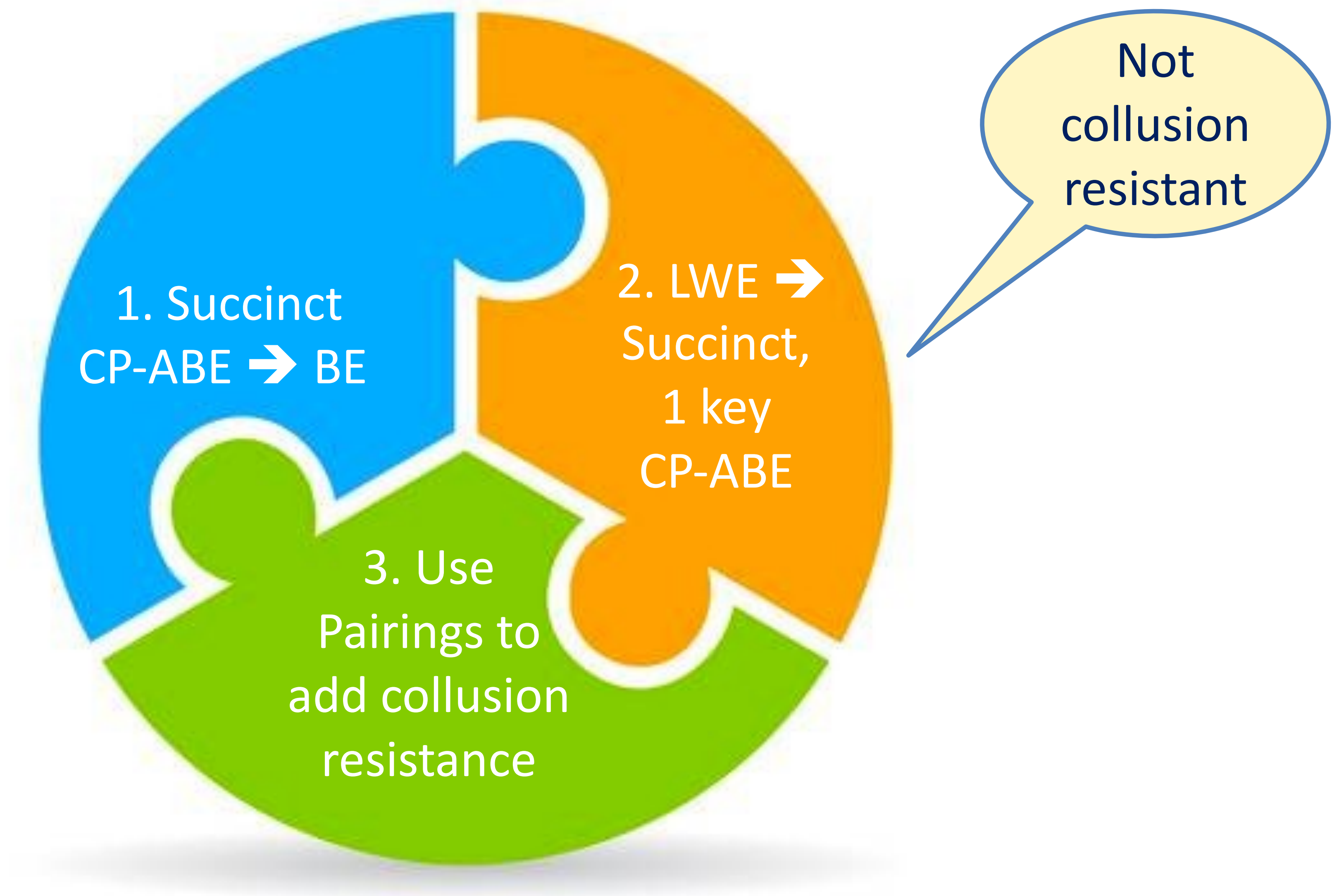
Ciphertext-Policy ABE



Key-Policy ABE



BE via ABE: Solution Steps



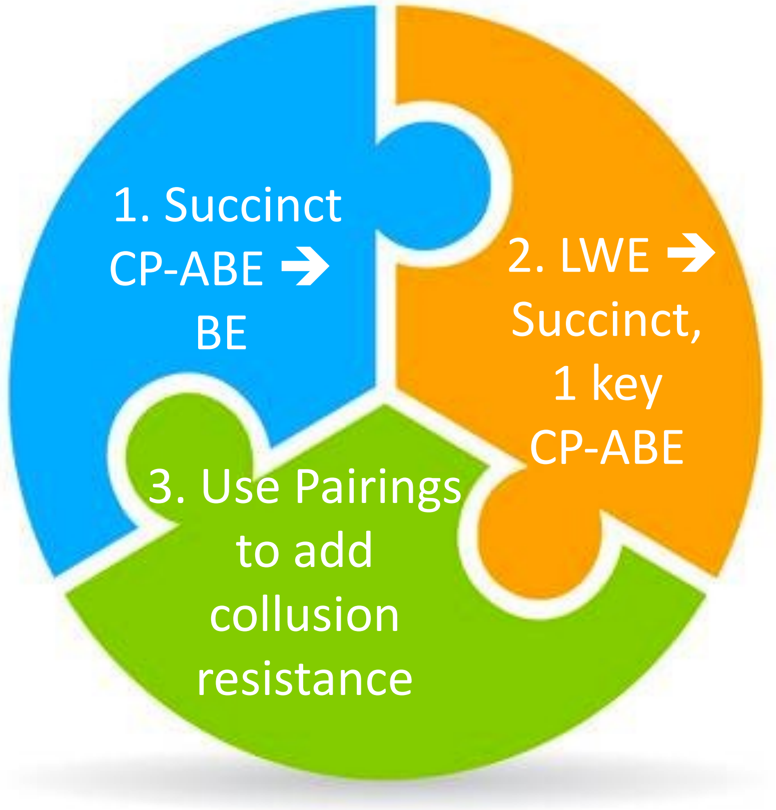
Perspective

- Steps 1 and 2 independently observed by Brakerski-Vaikuntanathan, Yamada, Boneh-Kim, A, (others?) several years ago

- Main hurdle: Step 3, adding collusion resistance

- Using pairings to achieve step 3 is main technical contribution of our work

- Inspired by recent constructions of $i\mathcal{O}$ that combine LWE and pairings [A19, AJLMS19,..]



Step 1: BE as CP-ABE for NC_1

- SK attribute = $j \in [N]$ where j = user index
- CT policy = $F_S(\cdot)$ where $S \subseteq [N]$, recipients

$$F_S(j) = \begin{cases} 1 & \text{if } j \in S \\ 0 & \text{if } j \notin S \end{cases}$$

$j \in \{0,1\}^{\log N}$ $\qquad S = \{s_1, s_2, \dots, s_{|S|}\}$

$$\downarrow$$

$$j \stackrel{?}{=} s_1 \quad j \stackrel{?}{=} s_2 \quad \cdots \quad j \stackrel{?}{=} s_{|S|}$$

$$\downarrow$$

0/1

Step 1: BE as CP-ABE for NC_1

F_S has

- Short input $(\approx O(\log N))$
- Shallow depth $(\approx O(\log N))$
- But, wide width $(\approx O(N))$

$j \in \{0,1\}^{\log N}$

$j \stackrel{?}{=} s_1 \quad j \stackrel{?}{=} s_2 \quad \cdots \quad j \stackrel{?}{=} s_{|S|}$

0/1

CP-ABE with <u>width-independent (succinct) parameters</u>
is enough for optimal BE!

Step 2: Designing CP-ABE from LWE

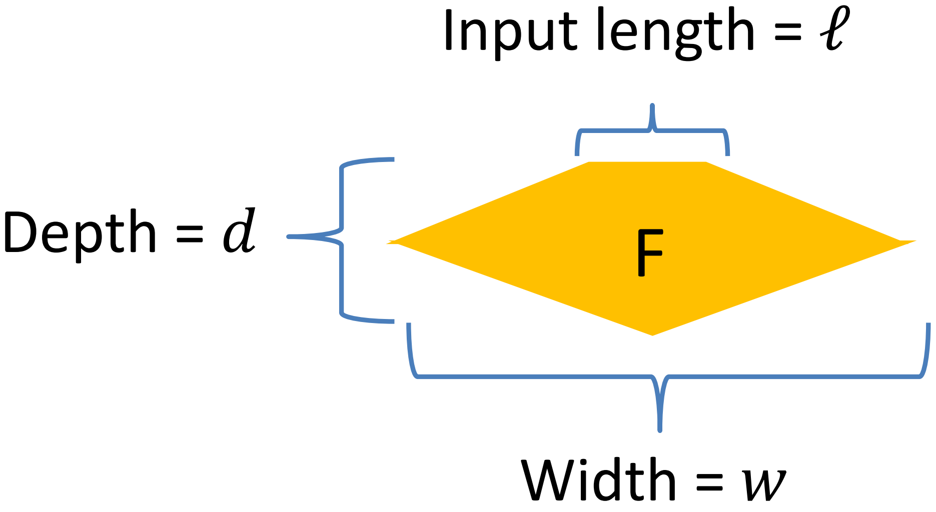
- CP-ABE from LWE is itself a central open question (even without width ind.).

- ABE from LWE: KP-ABE for P [GVW13], and can be width-independent [BGG+14]

$$|\mathrm{mpk}| = \mathrm{poly}(\lambda, \ell, d)$$

$$|\mathrm{ct}_{\boldsymbol{x}}| = \mathrm{poly}(\lambda, \ell, d)$$

$$|\mathrm{sk}_{\boldsymbol{F}}| = \mathrm{poly}(\lambda, d)$$



Convert BGG+ KP-ABE into CP-ABE?

Useful Structure: Decomposability of BGG+14

Decomposability:
$\mathrm{BGG+.Enc}(x, msg)$ can be divided into the following 2 steps:

1. First generate encodings

$$\left\{\begin{matrix} \mathbf{c}_{1,0} & \cdots & \mathbf{c}_{i,0} & \cdots & \mathbf{c}_{\ell,0} \\ \mathbf{c}_{1,1} & \cdots & \mathbf{c}_{i,1} & \cdots & \mathbf{c}_{\ell,1} \end{matrix}\right\}$$

Can be generated without knowing x

Where ℓ = length of x

2. To generate a ciphertext for attribute $x \in \{0,1\}^{\ell}$, output

$$\mathrm{BGG+.ct}_x = \{\mathbf{c}_{i,x_i}\}_{i\in[\ell]}$$

CP-ABE First Attempt: Combining [SS10] and [BGG+14]

$$\text{mpk} = \left\{ \begin{matrix} \boxed{PK_{1,0}} \\ \boxed{PK_{1,1}} \end{matrix} \quad \cdots \quad \begin{matrix} \boxed{PK_{i,0}} \\ \boxed{PK_{i,1}} \end{matrix} \quad \cdots \quad \begin{matrix} \boxed{PK_{\ell,0}} \\ \boxed{PK_{\ell,1}} \end{matrix} \right\}$$

$\text{msk} =$ corresponding secret keys $\{SK_{i,b}\}_{i,b}$

Encryption for F

Sample fresh KP-ABE BGG+, compute $\text{BGG+.}\,\text{sk}_F$, BGG+ CT for all possible x

$$\text{ct}_F = \left\{ \boxed{\begin{matrix} \mathbf{c}_{1,0} \\ \mathbf{c}_{1,1} \end{matrix}} \quad \cdots \quad \begin{matrix} \mathbf{c}_{i,0} \\ \mathbf{c}_{i,1} \end{matrix} \quad \cdots \quad \begin{matrix} \mathbf{c}_{\ell,0} \\ \mathbf{c}_{\ell,1} \end{matrix} \quad \begin{matrix} \text{BGG+.}\,\text{sk}_F \\ \text{BGG+.}\,\text{mpk} \end{matrix} \right\}$$

Learning both values at any index breaks security via linear attack

First Attempt: Combining [SS10] and [BGG+14]

$\mathrm{mpk} =$

Collusion of only 2 users breaks security:

E.g., 00000000 and 11111111

$\mathrm{msk} =$

Encryption for F:

Generate $\mathrm{BGG+.mpk}$, $\mathrm{BGG+.msk}$, $\mathrm{BGG+.sk}_F$, and

$$\mathrm{ct}_F = \left\{ \begin{matrix} \mathrm{Enc}_{PK_{1,0}}(\mathbf{c}_{1,0}) & \cdots & \mathrm{Enc}_{PK_{i,0}}(\mathbf{c}_{i,0}) & \cdots & \mathrm{Enc}_{PK_{\ell,0}}(\mathbf{c}_{\ell,0}) & \mathrm{BGG+.sk}_F \\ \mathrm{Enc}_{PK_{1,1}}(\mathbf{c}_{1,1}) & & \mathrm{Enc}_{PK_{i,1}}(\mathbf{c}_{i,1}) & & \mathrm{Enc}_{PK_{\ell,1}}(\mathbf{c}_{\ell,1}) & \mathrm{BGG+.mpk} \end{matrix} \right\}$$

KeyGen for x:

$$\mathrm{sk}_x = \left\{ SK_{1,x_1} \quad \cdots \quad SK_{i,x_i} \quad \cdots \quad SK_{\ell,x_\ell} \right\}$$

Decryption:

Recover $\mathrm{BGG+.ct}_x = \{\mathbf{c}_{i,x_i}\}_{i\in[\ell],b\in\{0,1\}}$ and use $\mathrm{BGG+.sk}_F$ to retrieve msg

Step 3: Add collusion resistance

Use Pairings in place of PKE to encrypt each LWE encoding

PAIRINGS & LWE

Pairings.

$$e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

$$e\left(g_1^a, g_2^b\right) = e(g_1, g_2)^{ab}$$

Idea: Can we provide all pairs $\left\{ \mathbf{c}_{i,b} \right\}_{i,b}$ in the exponent?

Bracket Notation.

$g_1^a \leftrightarrow [a]_1$

$g_2^b \leftrightarrow [b]_2$

$g_T^c \leftrightarrow [c]_T$

Q1: How to prevent collusion attacks?

- Standard trick in pairings: randomize keys for user u with fresh randomness $\boldsymbol{\delta_u}$

- Set up scheme so that decryptor recovers

User specific randomness

$$\left\{ \boxed{\left[\boldsymbol{\delta_u} \mathbf{c}_{i,x_i} \right]_T} \right\}_i$$

- Cannot combine $\boldsymbol{\delta_{u'}} \mathbf{c}_{1,1}$ and $\boldsymbol{\delta_u} \mathbf{c}_{1,0}$

Q2: How to select exactly one of two encodings

Introduce position-wise randomness & use pairing
to cancel one of two random terms per column

$$\mathrm{mpk} = \left\{ \begin{matrix} [w_{1,0}]_1 & \cdots & [w_{i,0}]_1 & \cdots & [w_{\ell,0}]_1 \\ [w_{1,1}]_1 & & [w_{i,1}]_1 & & [w_{\ell,1}]_1 \end{matrix} \right\}$$

$$\mathrm{ct}_F = \left\{ \begin{matrix} [w_{1,0}\mathbf{c}_{1,0}]_1 & \cdots & [w_{i,0}\mathbf{c}_{i,0}]_1 & \cdots & [w_{\ell,0}\mathbf{c}_{\ell,0}]_1 & \text{Other terms} \\ [w_{1,1}\mathbf{c}_{1,1}]_1 & & [w_{i,1}\mathbf{c}_{i,1}]_1 & & [w_{\ell,1}\mathbf{c}_{\ell,1}]_1 & \end{matrix} \right\}$$

$$\mathrm{sk}_x = \left\{ [\delta/w_{1,x_1}]_2 \ \cdots \ [\delta/w_{i,x_i}]_2 \ \cdots \ [\delta/w_{\ell,x_\ell}]_2 \quad [\delta]_T \right\}$$

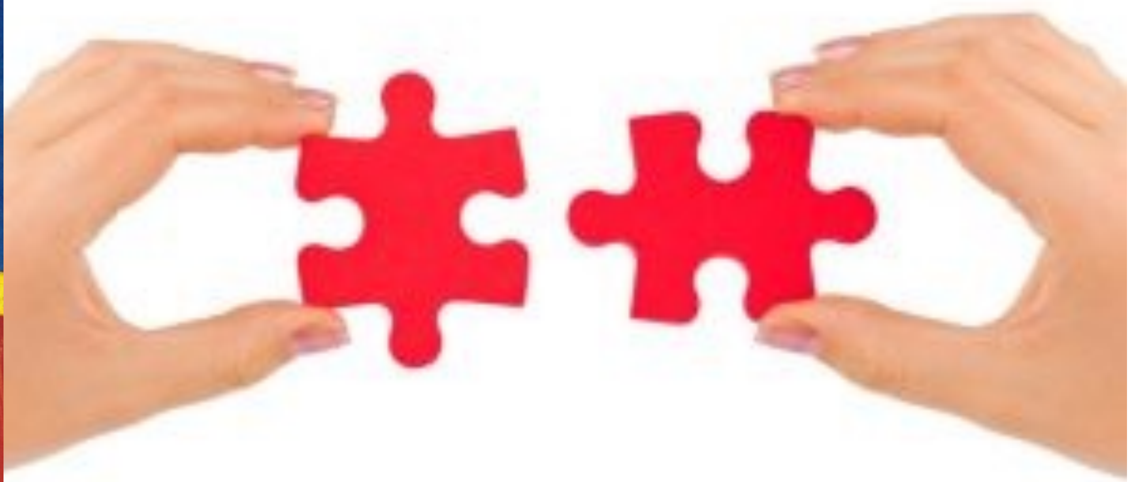
Can recover $[\delta\mathbf{c}_{i,x_i}]_T = e\left([w_{i,x_i}\mathbf{c}_{i,x_i}]_1, [\delta/w_{i,x_i}]_2\right)$

So Far…

- Randomize with user specific scalar in the exponent – standard trick for collusion resistance
- Select one out of two encodings – quadratic operation, can be done inside pairings.
- But testing whether input $x \in S$ is in NC_1. Moreover, x is encoded using LWE (BGG+14) and placed in exponent!

Pairings can compute only quadratic polynomials.
Why should this be possible?

The Happy Coincidence



- The structure of BGG+14 algorithm to compute NC_1 circuit on LWE encodings is linear.
- Compatible with pairings!

Q3: How to check set membership in exponent?

Structure of Decryption Algorithm in BGG+14:

– Can compute a linear function L_F such that

$$L_F\left(\{\mathbf{c}_{i,x_i}\}_{i\in[\ell]}\right) = m\left\lceil\frac{q}{2}\right\rceil + noise$$

In the exponent:

Assume that $m \in \{0,1\}$

$$L_F\left(\boxed{\{\,[\delta\mathbf{c}_{i,x_i}]_T}\}_{i\in[\ell]}\right) = \boxed{\left[\delta\left(m\left\lceil\frac{q}{2}\right\rceil + noise\right)\right]_T}$$

– Remove the noise to retrieve message $m \in \{0,1\}$

In the exponent:

$\delta\left(m\left\lceil\frac{q}{2}\right\rceil + noise\right)$ is exponentially large.

How do we manage this? (Next slide)

Q4: How to compute circuit for membership check in exponent?

- Let decryptor learn

$$\boxed{\left[\delta\left(m\left\lceil\frac{q}{2}\right\rceil + noise\right)\right]_T} \text{ and } \boxed{[\delta]_T}$$

- If $noise$ is polynomially small, one can learn m by brute force search:
  - Check all possible $m \in \{0,1\}, noise \in [-\text{poly}, \text{poly}]$
- How do we have polynomially small noise?
  - Use asymmetric noise growth in ciphertext evaluation [BV15,GV15]
  - Limits the circuit class to be NC_1, but suffices for BE

Bilinear Generic Group Model

- Security is proven in the bilinear generic group model (GGM).
- Intuition about bilinear GGM:
  – The only thing an adversary can do with group elements is to take pairings, take linear combinations, and test if equals zero.
  – If it doesn't equal zero, adversary learns nothing about the encoded value.

$$e(\square, \square) = \square$$
$$e(\square, \square) = \square$$
$$e(\square, \square) = \square$$

$$\square^{a} \, \square^{b} \, \square^{c} = 0?$$

Security Proof (1)

What can the adversary see?

The challenge ciphertext

$$\mathrm{ct}_F = \left\{ \begin{array}{ccccccc} \boxed{[w_{1,0}\mathbf{c}_{1,0}]_1} & \cdots & \boxed{[w_{i,0}\mathbf{c}_{i,0}]_1} & \cdots & \boxed{[w_{\ell,0}\mathbf{c}_{\ell,0}]_1} & \mathrm{BGG+.mpk} \\ \boxed{[w_{1,1}\mathbf{c}_{1,1}]_1} & & \boxed{[w_{i,1}\mathbf{c}_{i,1}]_1} & & \boxed{[w_{\ell,1}\mathbf{c}_{\ell,1}]_1} & \mathrm{BGG+.sk}_F \end{array} \right\}$$

The secret keys

$$\mathrm{sk}_{x^{(j)}} = \left\{ \boxed{\left[\delta^{(j)}/w_{1,x_1^{(j)}}\right]_2} \cdots \boxed{\left[\delta^{(j)}/w_{i,x_i^{(j)}}\right]_2} \cdots \boxed{\left[\delta^{(j)}/w_{\ell,x_\ell^{(j)}}\right]_2} \boxed{[\delta^{(j)}]_T} \right\}$$

where $j \in [Q]$, $Q =$ # of key queries, $F\left(x^{(j)}\right) = 0$

What can the adversary do?

To take pairings between above components to obtain:

$\boxed{\left[(\delta^{(j)} w_{i,b}/w_{i',b'})\mathbf{c}_{i,b}\right]_T}$ where $(i,b) \neq (i',b')$ $\qquad$ $\boxed{\left[\delta^{(j)}\mathbf{c}_{i,x_i^{(j)}}\right]_T}$

and take linear combination among the terms.

Security Proof (2)

What can the adversary do?

To take linear combination among the following terms

$$\underbrace{\boxed{\left[(\delta^{(j)} w_{i,b}/w_{i',b'})\mathbf{c}_{i,b}\right]_T}}_{\text{(A)}} \quad \text{where } (i,b) \neq (i',b') \qquad \underbrace{\boxed{\left[\delta^{(j)}\mathbf{c}_{i,x_i^{(j)}}\right]_T}}_{\text{(B)}}$$

given $\mathrm{BGG+.sk}_F, \mathrm{BGG+.mpk}$

Claim 1

If the adversary puts a term of form (A) into the linear combination, the result is not 0 with overwhelming probability.

(Proof intuition) The term $\delta^{(j)} w_{i,b}/w_{i',b'}$ appears only when pairing

$$\boxed{\left[w_{i,1}\mathbf{c}_{i,1}\right]_1} \quad \text{and} \quad \boxed{\left[\delta^{(j)}/w_{i',b'}\right]_2}$$

Other terms are multiplied by $\delta^{(j)} w_{i,b}/w_{i',b'}$ with different (i,j,b,b').
Different monomials cannot cancel each other by linear combination.

Security Proof (3)

<u>What can the adversary do?</u>

To take linear combination among the following terms

$\cancel{\underbrace{\boxed{\left[(\delta^{(j)} w_{i,b}/w_{i',b'})\mathbf{c}_{i,b}\right]_T}}_{\text{(A)}}}$ ~~where~~ $\cancel{(i,b) \neq (i',b')}$ $\qquad \underbrace{\boxed{\left[\delta^{(j)}\mathbf{c}_{i,x_i^{(j)}}\right]_T}}_{\text{(B)}}$

given $\mathrm{BGG+.sk}_F$, $\mathrm{BGG+.mpk}$

> **<u>Claim 2</u>**
>
> If the adversary puts terms from (B) with different $\delta^{(j)}$ into the linear combination, the result is not 0 with overwhelming probability.

(Proof intuition) Different monomials cannot cancel each other by linear combination.

Recall that $\delta^{(j)}$ is user specific randomness.

- ➢ Collusion of different users is not useful.
- ➢ We can focus on single-key setting.

Security Proof (4)

What can the adversary do?

To take linear combination among the following terms

$$\underbrace{\boxed{\cancel{\left[(\delta^{(j)} w_{i,b}/w_{i',b'})\mathbf{c}_{i,b}\right]_T}}}_{(A)} \quad \cancel{\text{where } (i,b) \neq (i',b')} \qquad \underbrace{\boxed{\left[\delta^{\cancel{(j)}} \mathbf{c}_{i,x_i^{\cancel{(j)}}}\right]_T}}_{(B)}$$

given $\mathrm{BGG+.sk}_F$, $\mathrm{BGG+.mpk}$

From single key and single ciphertext security of BGG+:

$$(\ \mathrm{BGG+.sk}_F,\ \mathrm{BGG+.mpk},\quad \{\ \boxed{\left[\delta \mathbf{c}_{i,x_i}\right]_T}\ \}_i\ )$$

$$\approx_c (\ \mathrm{BGG+.sk}_F,\ \mathrm{BGG+.mpk},\ \boxed{[\mathrm{random}]_T}\ )$$

Security Proof (4)

<u>What can the adversary do?</u>

To take linear combination among the following terms

$$\underbrace{\cancel{\boxed{\left[(\delta^{(j)} w_{i,b}/w_{i',b'})\mathbf{c}_{i,b}\right]_T}}}_{\text{(A)}} \quad \cancel{\text{where } (i,b) \neq (i',b')} \qquad \underbrace{\boxed{\left[\delta^{\cancel{(j)}}\mathbf{c}_{i,x_i^{\cancel{(j)}}}\right]_T}}_{\text{(B)}}$$

given $\mathrm{BGG+.sk}_F$, $\mathrm{BGG+.mpk}$

From single key and single ciphertext security of BGG+:

$$(\ \mathrm{BGG+.sk}_F,\ \mathrm{BGG+.mpk},\quad \{\boxed{[\delta\mathbf{c}_{i,x_i}]_T}\}_i\ )$$

$$\approx_c (\ \mathrm{BGG+.sk}_F,\ \mathrm{BGG+.mpk},\ \boxed{[\text{random}]_T}\ )$$

No information about message revealed!

Follow-Up Work [AWY20]

- BE with optimal parameters (|mpk|=O(1), |ct|=O(1), |sk|=O(1)) from bilinear map and LWE in the standard model.

- Selective security of the scheme is shown from a variant of the "KOALA assumption [BW19]" on bilinear groups.
  - A knowledge type assumption

If ∃  distinguishes $g^{\mathbf{Vr}}$ from random $g^{\mathbf{w}}$,

then ∃  that outputs a vector $\mathbf{x}$ such that $\mathbf{xV} = \mathbf{0}$.

Follow-Up Work [AWY20]

- The KOALA assumption says that if an adversary distinguishes group elements whose exponents are on some Hyperplane from random group elements, then there exists another adversary that outputs a vector that is orthogonal to the Hyperplane.

- Intuitively says that the only way to distinguish group elements is to find an orthogonal vector to the hyperplane.

Summary

- Constructed CP-ABE for NC_1 circuits with compact parameters from LWE and bilinear GGM.
- Implies first Optimal BE without multilinear maps.
- Implies Identity Based BE with similar efficiency.
- Many Open Questions: Standard Model? New Applications? Support P (with proof)? From LWE?

Thank You

Images Credit:
Hans Hoffman