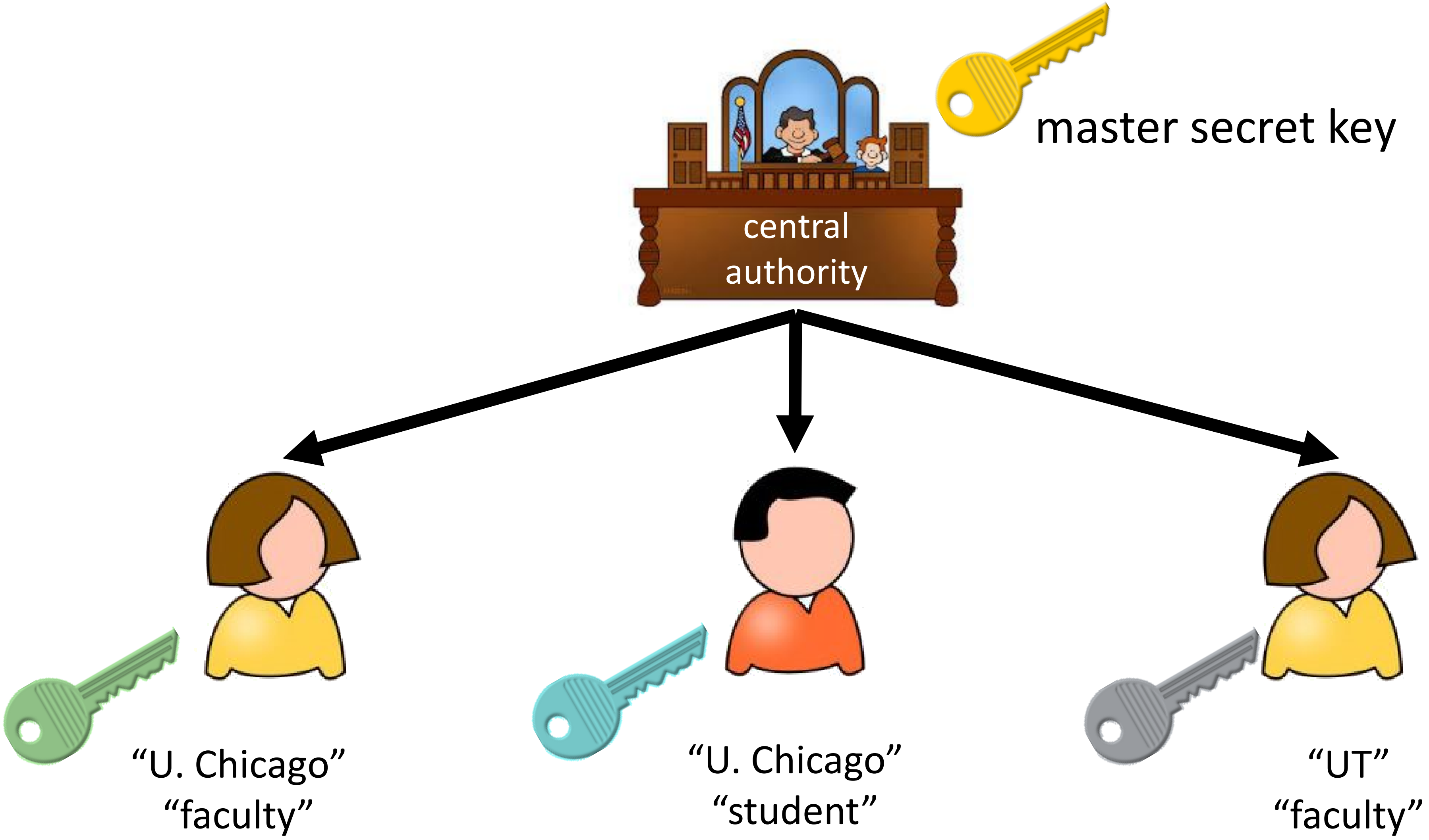
Multi-Authority ABE from Lattices without Random Oracles

Brent Waters, Hoeteck Wee, and David Wu

Attribute-Based Encryption (ABE)

[SW05, GPSW06]



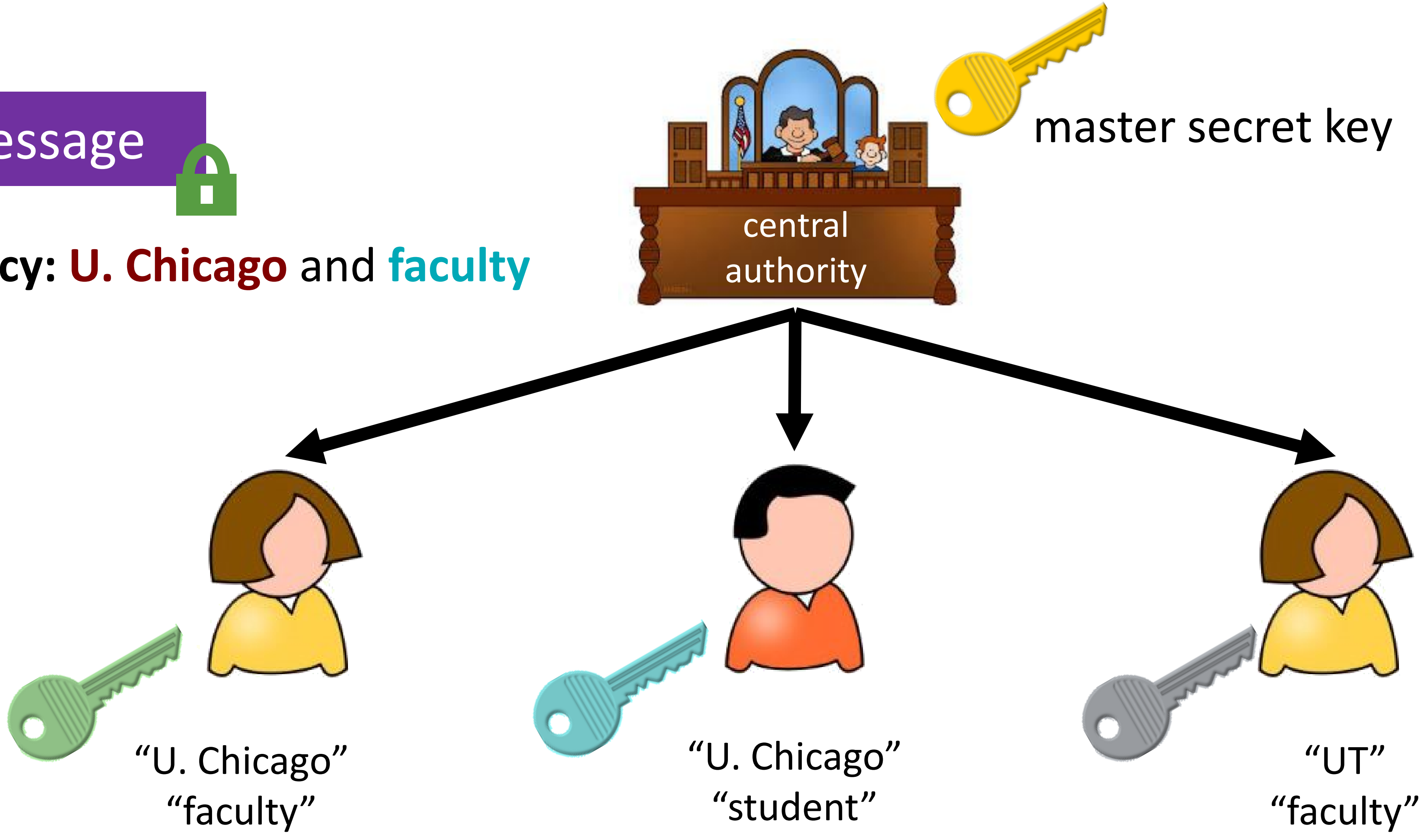
Secret keys associated with set of attributes

Attribute-Based Encryption (ABE)

[SW05, GPSW06]

message

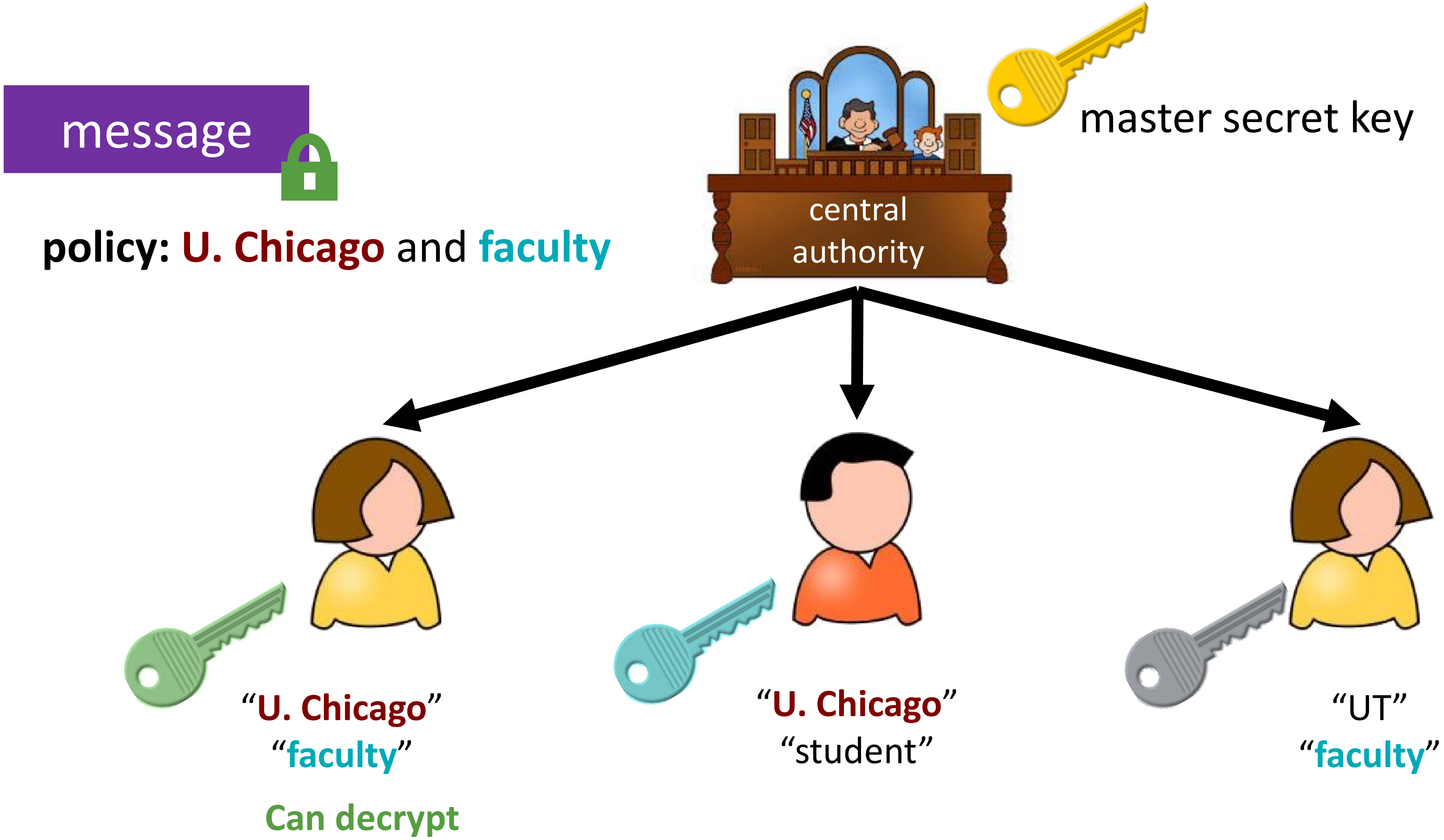
policy: U. Chicago and **faculty**



Secret keys associated with set of attributes

Attribute-Based Encryption (ABE)

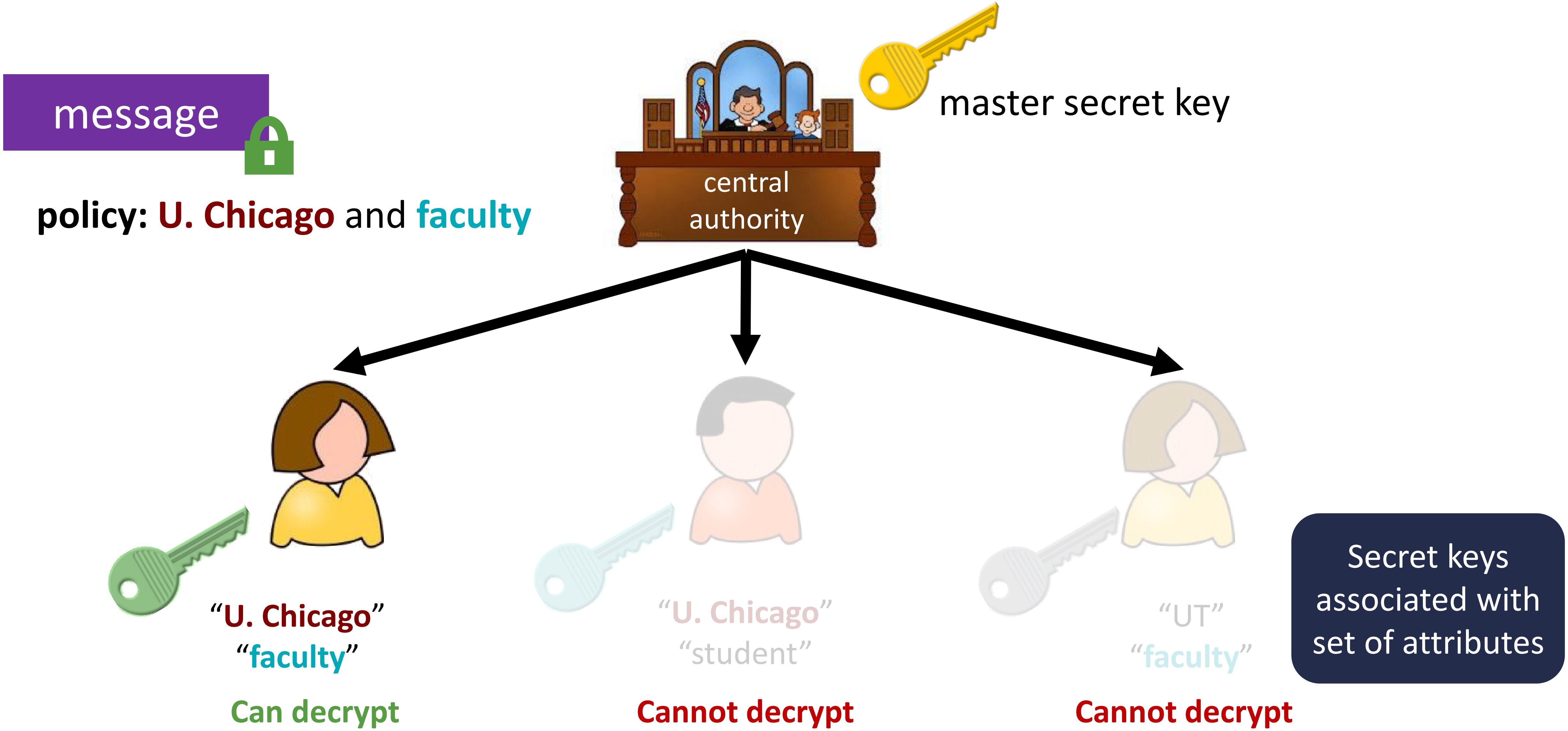
[SW05, GPSW06]



Secret keys associated with set of attributes

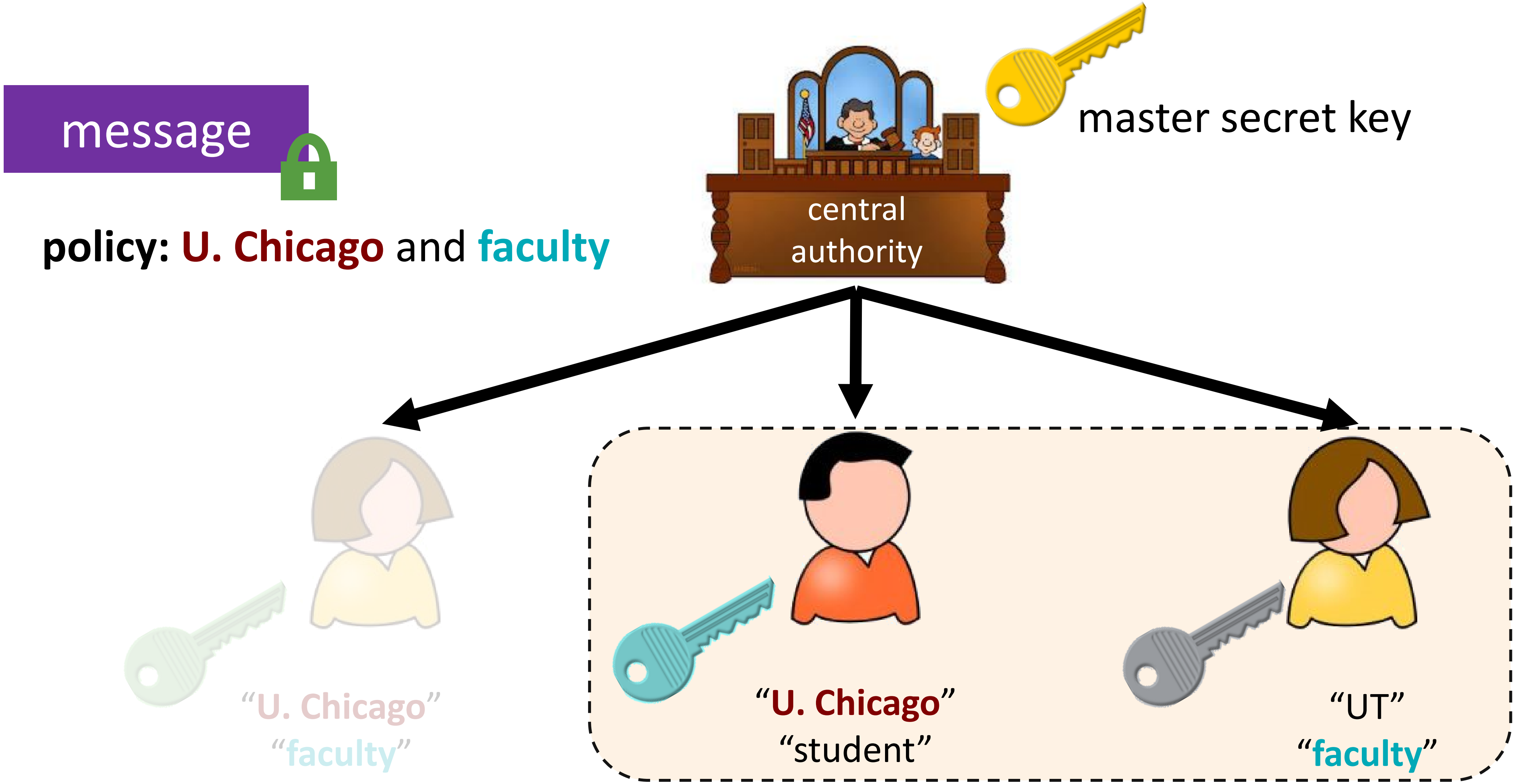
Attribute-Based Encryption (ABE)

[SW05, GPSW06]



Attribute-Based Encryption (ABE)

[SW05, GPSW06]



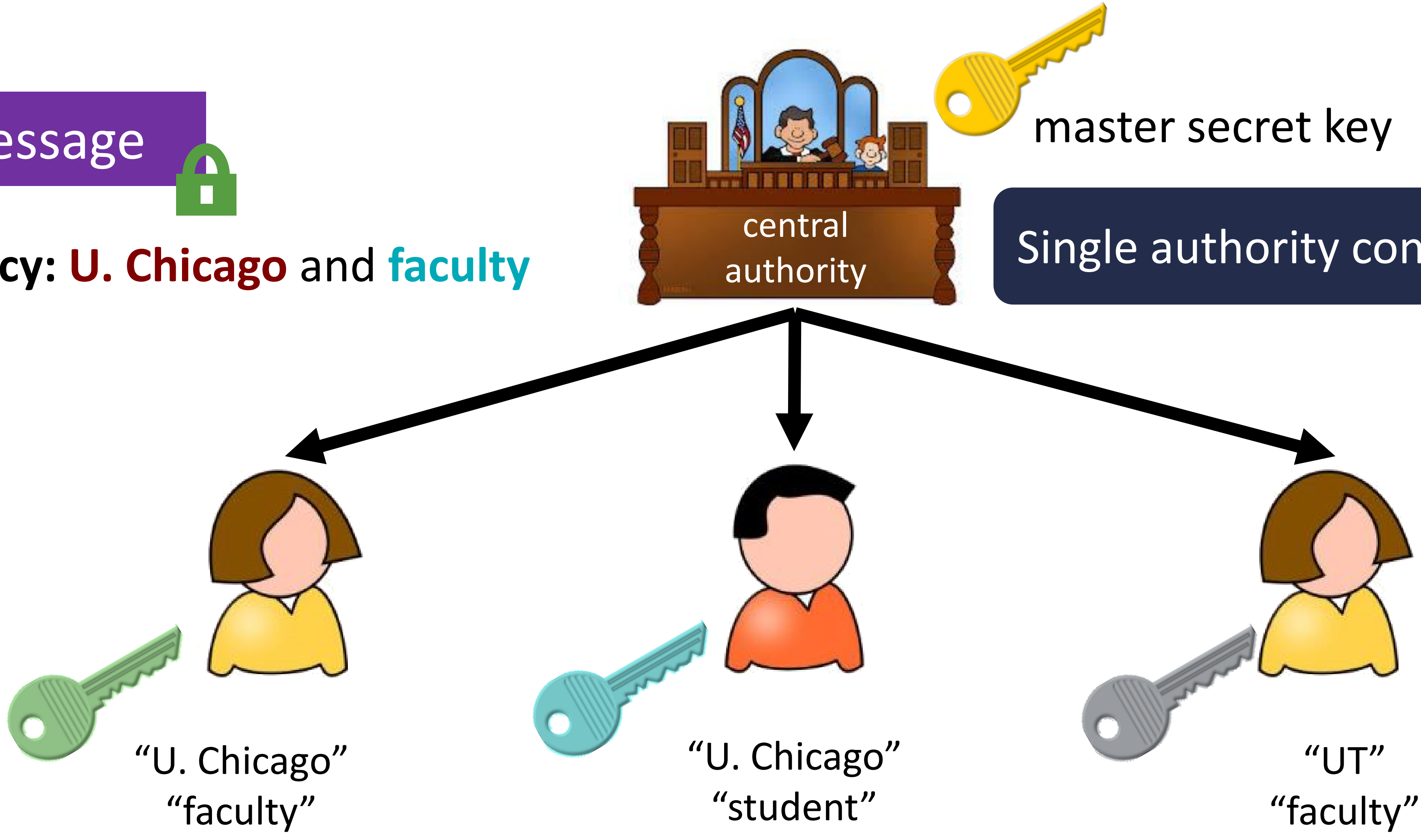
Users cannot collude to decrypt

Attribute-Based Encryption (ABE)

[SW05, GPSW06]

message

policy: U. Chicago and **faculty**

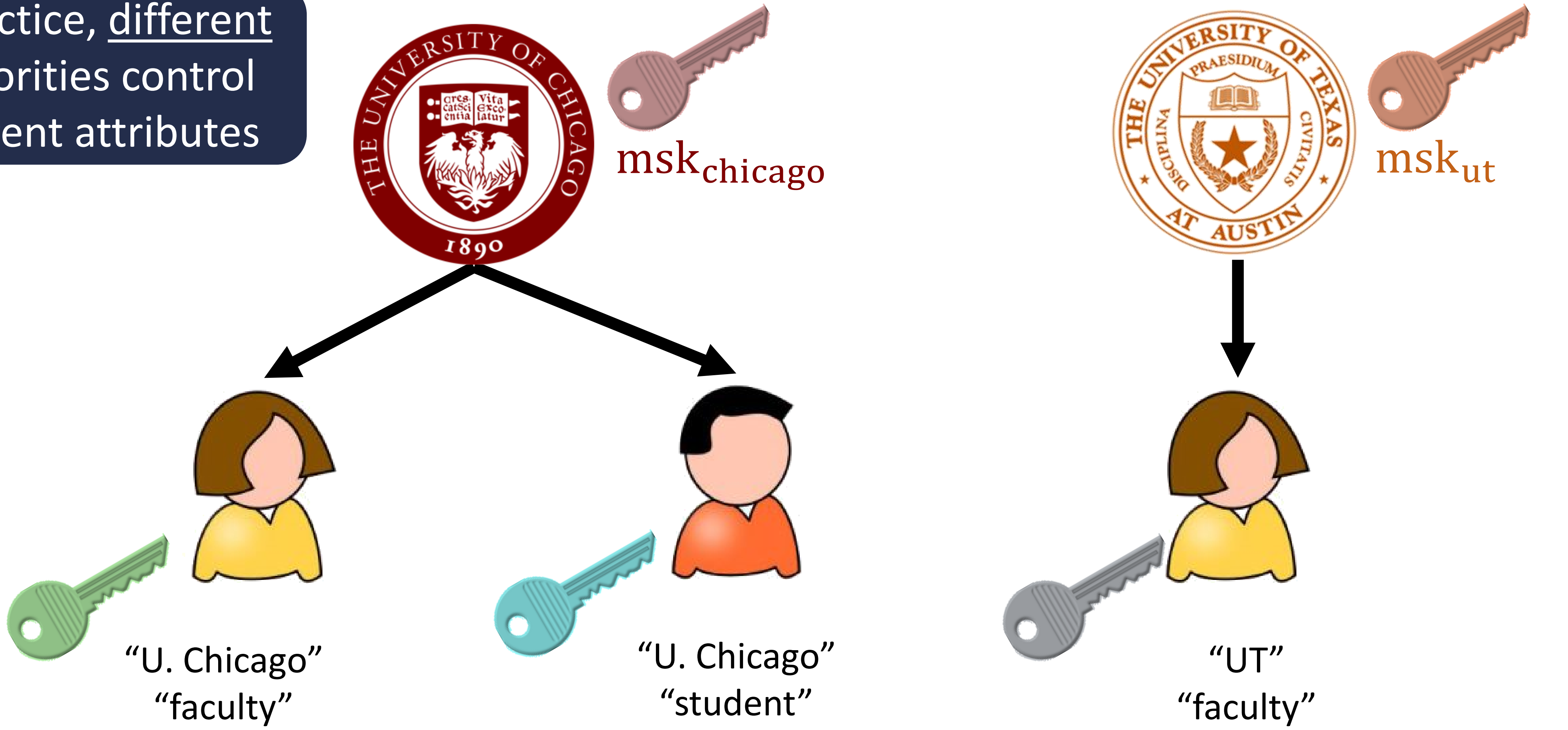


Single authority controls *all* attributes

Multi-Authority ABE

[Cha07, CC09, LW11]

In practice, different authorities control different attributes



Multi-Authority ABE

[Cha07, CC09, LW11]

In practice, <u>different</u> authorities control different attributes

$\text{msk}_{\text{chicago}}$

$\text{mpk}_{\text{chicago}}$

"faculty"
"student"
"visitor"

Each authority publishes a public key along with the set of attributes it controls

msk_{ut}

mpk_{ut}

"faculty"
"student"

Multi-authority ABE: *anyone* can become an authority

Multi-Authority ABE

[Cha07, CC09, LW11]

In practice, <u>different</u> authorities control different attributes

no interaction between authorities

$\mathsf{msk}_{\mathsf{chicago}}$

$\mathsf{mpk}_{\mathsf{chicago}}$

"faculty"
"student"
"visitor"

Each authority publishes a public key along with the set of attributes it controls

$\mathsf{msk}_{\mathsf{ut}}$

$\mathsf{mpk}_{\mathsf{ut}}$

"faculty"
"student"

Multi-authority ABE: *anyone* can become an authority

Multi-Authority ABE

[Cha07, CC09, LW11]

In practice, different authorities control different attributes

no interaction between authorities

$\mathrm{msk}_{\mathrm{chicago}}$

$\mathrm{mpk}_{\mathrm{chicago}}$

"faculty"
"student"
"visitor"

Each authority publishes a public key along with the set of attributes it controls

$\mathrm{msk}_{\mathrm{ut}}$

$\mathrm{mpk}_{\mathrm{ut}}$

"faculty"
"student"

message

policy: visitor (U Chicago) and student (UT)

policy is a function on attributes from one or more authorities

Multi-authority ABE: *anyone* can become an authority

Multi-Authority ABE

[Cha07, CC09, LW11]

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

Multi-Authority ABE

[Cha07, CC09, LW11]

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

[DKW21a]: Multi-authority ABE for conjunctions from LWE

Multi-Authority ABE

[Cha07, CC09, LW11]

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

[DKW21a]: Multi-authority ABE for conjunctions from LWE

All of these constructions are in the **random oracle model**

Multi-Authority ABE

[Cha07, CC09, LW11]

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

[DKW21a]: Multi-authority ABE for conjunctions from LWE

All of these constructions are in the **random oracle model**

Can we construct multi-authority ABE without random oracles?

Multi-Authority ABE

[Cha07, CC09, LW11]

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

[DKW21a]: Multi-authority ABE for conjunctions from LWE

All of these constructions are in the **random oracle model**

Can we construct multi-authority ABE without random oracles?

(and without strong tools like extractable witness encryption or indistinguishability obfuscation)

This Work

[Cha07, CC09, LW11]

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

[DKW21a]: Multi-authority ABE for conjunctions from LWE

All of these constructions are in the **random oracle model**

This work: instantiate the random oracle in [DKW21a] with a **concrete** hash function and argue security using the **evasive LWE** assumption

This Work

[Cha07, CC09, LW11]

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

[DKW21a]: Multi-authority ABE for conjunctions from LWE

All of these constructions are in the **random oracle model**

Hash function is not "random-looking:"

$$H(x_1 x_2 \cdots x_n) \coloneqq \left(\prod_{i \in [n]} \boldsymbol{D}_{x_i}\right) \boldsymbol{e}_1$$

where $\boldsymbol{D}_0, \boldsymbol{D}_1$ are public low-norm matrices and $\boldsymbol{e}_1$ is first basis vector

This work: instantiate the random oracle in [DKW21a] with a **concrete** hash function and argue security using the **evasive LWE** assumption

This Work

[Cha07, CC09, LW11]

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

[DKW21a]: Multi-authority ABE for conjunctions from LWE

All of these constructions are in the **random oracle model**

Hash function is not "random-looking:"

$$H(x_1 x_2 \cdots x_n) \coloneqq \left(\prod_{i \in [n]} \boldsymbol{D}_{x_i}\right) \boldsymbol{e}_1$$

where $\boldsymbol{D}_0, \boldsymbol{D}_1$ are public low-norm matrices and $\boldsymbol{e}_1$ is first basis vector

This work: instantiate the random oracle in [DKW21a] with a **concrete** hash function and argue security using the **evasive LWE** assumption

Evasive LWE is not a standard assumption, but provides useful evidence for soundness of the approach

This Work

[Cha07, CC09, LW11]

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

[DKW21a]: Multi-authority ABE for conjunctions from LWE

All of these constructions are in the **random oracle model**

Hash function is <u>not</u> "random-looking:"

$$H(x_1 x_2 \cdots x_n) := \left(\prod_{i \in [n]} \boldsymbol{D}_{x_i}\right) \boldsymbol{e}_1$$

where $\boldsymbol{D}_0, \boldsymbol{D}_1$ are public low-norm matrices and $\boldsymbol{e}_1$ is first basis vector

This work: instantiate the random oracle in [DKW21a] with a **concrete** hash function and argue security using the **evasive LWE** assumption

Open question: prove security from *standard* LWE

Why Random Oracles?

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

[DKW21a]: Multi-authority ABE for conjunctions from LWE

All of these constructions are in the **random oracle model**

Can we construct multi-authority ABE without random oracles?

(and without strong tools like extractable witness encryption or indistinguishability obfuscation)

policy: visitor (U Chicago) and student (UT)

student (UT)

visitor (U. Chicago)

- Different users should <u>not</u> be able to combine their keys to decrypt

Why Random Oracles?

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

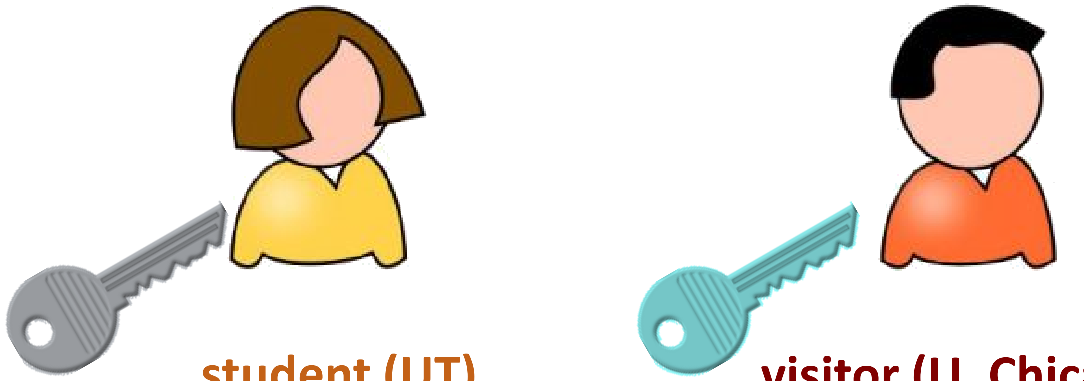
[DKW21a]: Multi-authority ABE for conjunctions from LWE

All of these constructions are in the **random oracle model**

Can we construct multi-authority ABE without random oracles?

(and without strong tools like extractable witness encryption or indistinguishability obfuscation)

Single-authority setting: generate all of the attribute keys for a user using common randomness to prevent mixing and matching across users



student (UT) **visitor (U. Chicago)**

- Different users should <u>not</u> be able to combine their keys to decrypt

Why Random Oracles?

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

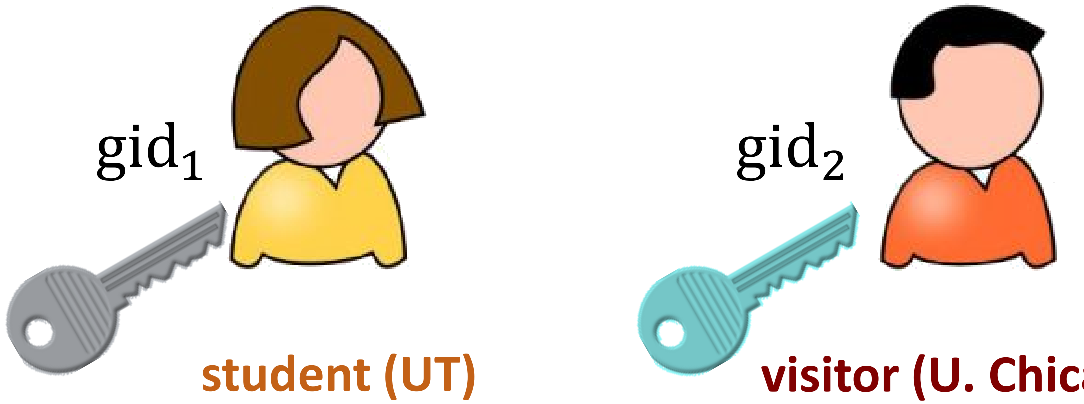
[DKW21a]: Multi-authority ABE for conjunctions from LWE

All of these constructions are in the **random oracle model**

Can we construct multi-authority ABE without random oracles?

(and without strong tools like extractable witness encryption or indistinguishability obfuscation)

policy: visitor (U Chicago) and student (UT)



- Different users should <u>not</u> be able to combine their keys to decrypt
- Keys for a single user are generated using *correlated* randomness (derived by hashing *unique* user identifier: $r \leftarrow H(\mathrm{gid})$)

Why Random Oracles?

[LW11, RW15, DKW21b]: Multi-authority ABE for NC^1 from bilinear maps

[DKW21a]: Multi-authority ABE for conjunctions from LWE

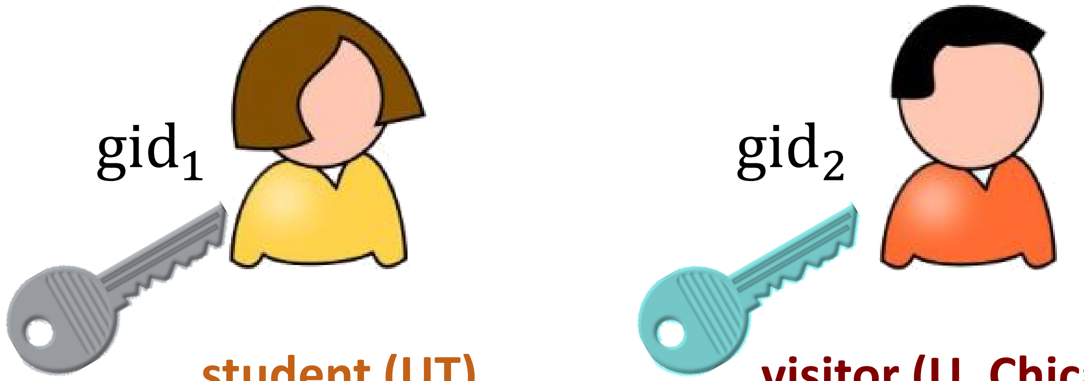
All of these constructions are in the **random oracle model**

Can we construct multi-authority ABE without random oracles?

(and without strong tools like extractable witness encryption or indistinguishability obfuscation)

message

policy: visitor (U Chicago) and student (UT)



student (UT) **visitor (U. Chicago)**

Security proof needs to model H as a random oracle

- Different users should not be able to combine their keys to decrypt
- Keys for a single user are generated using *correlated* randomness (derived by hashing *unique* user identifier: $r \leftarrow H(\mathrm{gid})$)

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

For simplicity, assume each authority has one attribute

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

For simplicity, assume each authority has one attribute

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

$\boldsymbol{A}_3, \boldsymbol{B}_3, \boldsymbol{p}_3$

Public key for each authority/attribute consist of (random) matrices $\boldsymbol{A}_i, \boldsymbol{B}_i$ and vector $\boldsymbol{p}_i$ (over $\mathbb{Z}_q$)

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

For simplicity, assume each authority has one attribute

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$
td_1

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$
td_2

$\boldsymbol{A}_3, \boldsymbol{B}_3, \boldsymbol{p}_3$
td_3

Public key for each authority/attribute consist of (random) matrices $\boldsymbol{A}_i, \boldsymbol{B}_i$ and vector $\boldsymbol{p}_i$ (over $\mathbb{Z}_q$)

Secret key for each authority/attribute is trapdoor td_i for $\boldsymbol{A}_i$

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

For simplicity, assume each authority has one attribute

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

td_1

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

td_2

$\boldsymbol{A}_3, \boldsymbol{B}_3, \boldsymbol{p}_3$

td_3

Public key for each authority/attribute consist of (random) matrices $\boldsymbol{A}_i, \boldsymbol{B}_i$ and vector $\boldsymbol{p}_i$ (over $\mathbb{Z}_q$)

Secret key for each authority/attribute is trapdoor td_i for $\boldsymbol{A}_i$

Trapdoor for $\boldsymbol{A}_i$ can be used to sample **short** solution $\boldsymbol{x}$ where $\boldsymbol{A_i x} = \boldsymbol{y}$

We denote this by writing $\boldsymbol{x} \leftarrow \boldsymbol{A}_i^{-1}(\boldsymbol{y})$

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

For simplicity, assume each authority has one attribute

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

td_1

$\boldsymbol{r} \leftarrow H(\mathrm{gid})$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

td_2

$\boldsymbol{A}_3, \boldsymbol{B}_3, \boldsymbol{p}_3$

td_3

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

For simplicity, assume each authority has one attribute

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

td_1

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

td_2

$\boldsymbol{A}_3, \boldsymbol{B}_3, \boldsymbol{p}_3$

td_3

$\boldsymbol{r} \leftarrow H(\mathrm{gid})$

$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1 \boldsymbol{r})$

Invariant: $\boldsymbol{A}_i \boldsymbol{k}_i = \boldsymbol{p}_i + \boldsymbol{B}_i \boldsymbol{r}$

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

For simplicity, assume each authority has one attribute

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

td_1

$\boldsymbol{r} \leftarrow H(\mathrm{gid})$

$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r})$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

td_2

$\boldsymbol{r} \leftarrow H(\mathrm{gid})$

$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r})$

$\boldsymbol{A}_3, \boldsymbol{B}_3, \boldsymbol{p}_3$

td_3

$\boldsymbol{r}$ is the **common randomness** that ties the keys for a particular user together

Invariant: $\boldsymbol{A}_i\boldsymbol{k}_i = \boldsymbol{p}_i + \boldsymbol{B}_i\boldsymbol{r}$

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

For simplicity, assume each authority has one attribute

Encrypt to these attributes

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

td_1

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

td_2

$\boldsymbol{A}_3, \boldsymbol{B}_3, \boldsymbol{p}_3$

td_3

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

squiggly underline denotes noise

$$\utilde{\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}} = \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \mathrm{error}$$

For simplicity, assume each authority has one attribute

Encrypt to these attributes

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

td_1

$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1}$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

td_2

$\utilde{\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2}$

$\boldsymbol{A}_3, \boldsymbol{B}_3, \boldsymbol{p}_3$

td_3

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

For simplicity, assume each authority has one attribute

squiggly underline denotes noise

$$\utilde{\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}} = \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \text{error}$$

Encrypt to these attributes

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

td_1

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

td_2

$\boldsymbol{A}_3, \boldsymbol{B}_3, \boldsymbol{p}_3$

td_3

$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1}$

$\utilde{\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2}$

$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2}$

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

For simplicity, assume each authority has one attribute

squiggly underline denotes noise

$$\utilde{\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}} = \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \text{error}$$

Encrypt to these attributes

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

td_1

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

td_2

$\boldsymbol{A}_3, \boldsymbol{B}_3, \boldsymbol{p}_3$

td_3

$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1}$

$\utilde{\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2}$

$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2}$

$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil}$

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

squiggly underline denotes noise

$$\utilde{\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}} = \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \mathrm{error}$$

For simplicity, assume each authority has one attribute

Encrypt to these attributes

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

td_1

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

td_2

$$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1}$$

$$\utilde{\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2}$$

$$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2} \qquad \utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil}$$

Decryption:

$\boldsymbol{r} \leftarrow H(\mathrm{gid})$

$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r})$

$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r})$

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

squiggly underline denotes noise

$$\utilde{\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}} = \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \text{error}$$

For simplicity, assume each authority has one attribute

Encrypt to these attributes

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

td_1

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

td_2

$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1}$

$\utilde{\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2}$

$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2}$ $\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil}$

Decryption:

$$\utilde{\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1}\boldsymbol{k}_1 \approx \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1\boldsymbol{r} + \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1$$

$$\utilde{\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2}\boldsymbol{k}_2 \approx \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2\boldsymbol{r} + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2$$

$\boldsymbol{r} \leftarrow H(\mathrm{gid})$

$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r})$

$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r})$

Construction Overview

Starting point: ABE for conjunctions from LWE [DKW21a]

squiggly underline denotes noise

$$\mathbf{s}^{\mathrm{T}}\mathbf{A} = \mathbf{s}^{\mathrm{T}}\mathbf{A} + \text{error}$$

For simplicity, assume each authority has one attribute

Encrypt to these attributes

$\mathbf{A}_1, \mathbf{B}_1, \mathbf{p}_1$

td_1

$\mathbf{A}_2, \mathbf{B}_2, \mathbf{p}_2$

td_2

$\mathbf{s}_1^{\mathrm{T}}\mathbf{A}_1$

$\mathbf{s}_2^{\mathrm{T}}\mathbf{A}_2$

$\mathbf{s}_1^{\mathrm{T}}\mathbf{B}_1 + \mathbf{s}_2^{\mathrm{T}}\mathbf{B}_2$ $\quad$ $\mathbf{s}_1^{\mathrm{T}}\mathbf{p}_1 + \mathbf{s}_2^{\mathrm{T}}\mathbf{p}_2 + \mu \cdot \lfloor q/2 \rceil$

$$(\mathbf{s}_1^{\mathrm{T}}\mathbf{B}_1 + \mathbf{s}_2^{\mathrm{T}}\mathbf{B}_2)\mathbf{r} + \mathbf{s}_1^{\mathrm{T}}\mathbf{p}_1 + \mathbf{s}_2^{\mathrm{T}}\mathbf{p}_2 + \mu \cdot \lfloor q/2 \rceil$$

$\mathbf{r} \leftarrow H(\mathrm{gid})$

$\mathbf{k}_1 \leftarrow \mathbf{A}_1^{-1}(\mathbf{p}_1 + \mathbf{B}_1\mathbf{r})$

$\mathbf{k}_2 \leftarrow \mathbf{A}_2^{-1}(\mathbf{p}_2 + \mathbf{B}_2\mathbf{r})$

Decryption:

$$\mathbf{s}_1^{\mathrm{T}}\mathbf{A}_1\mathbf{k}_1 \approx \mathbf{s}_1^{\mathrm{T}}\mathbf{B}_1\mathbf{r} + \mathbf{s}_1^{\mathrm{T}}\mathbf{p}_1$$

$$\mathbf{s}_2^{\mathrm{T}}\mathbf{A}_2\mathbf{k}_2 \approx \mathbf{s}_2^{\mathrm{T}}\mathbf{B}_2\mathbf{r} + \mathbf{s}_2^{\mathrm{T}}\mathbf{p}_2$$

Subtract to obtain
$\mu \cdot \lfloor q/2 \rceil + \text{noise}$

Security Analysis

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

challenge ciphertext

$\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2$

$\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$

Security Analysis

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

challenge ciphertext

$$\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1 \qquad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2$$

$$\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2 \qquad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$$

Strategy: Argue ciphertext is pseudorandom (by LWE) if none of the keys satisfy the policy

Security Analysis

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

challenge ciphertext

$$\boldsymbol{s}_1^{\mathrm{T}} \boldsymbol{A}_1 \qquad \boldsymbol{s}_1^{\mathrm{T}} \boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}} \boldsymbol{B}_2$$

$$\boldsymbol{s}_2^{\mathrm{T}} \boldsymbol{A}_2 \qquad \boldsymbol{s}_1^{\mathrm{T}} \boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}} \boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$$

Strategy: Argue ciphertext is pseudorandom (by LWE) if <u>none</u> of the keys satisfy the policy

Challenge: Need to simulate keys $\boldsymbol{k}_1$ and $\boldsymbol{k}_2$ *without* trapdoors for $\boldsymbol{A}_1$ or $\boldsymbol{A}_2$

secret key

$$\boldsymbol{r}_1 \leftarrow H(\mathrm{gid}_1)$$
$$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1 \boldsymbol{r}_1)$$

$$\boldsymbol{r}_2 \leftarrow H(\mathrm{gid}_2)$$
$$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2 \boldsymbol{r}_2)$$

Security Analysis

public keys

A_1, B_1, p_1

A_2, B_2, p_2

challenge ciphertext

$s_1^{\mathrm{T}} A_1 \quad s_1^{\mathrm{T}} B_1 + s_2^{\mathrm{T}} B_2$

$s_2^{\mathrm{T}} A_2 \quad s_1^{\mathrm{T}} p_1 + s_2^{\mathrm{T}} p_2 + \mu \cdot \lfloor q/2 \rceil$

Strategy: Argue ciphertext is pseudorandom (by LWE) if <u>none</u> of the keys satisfy the policy

Challenge: Need to simulate keys k_1 and k_2 *without* trapdoors for A_1 or A_2

secret key

$r_1 \leftarrow H(\mathrm{gid}_1)$
$k_1 \leftarrow A_1^{-1}(p_1 + B_1 r_1)$

$r_2 \leftarrow H(\mathrm{gid}_2)$
$k_2 \leftarrow A_2^{-1}(p_2 + B_2 r_2)$

Previously [DKW21a]: model H as a random oracle and rely on "lattice trapdoor sampling" lemma

- **This work:** We describe a modular approach that allows us to use LWE with a **polynomial** modulus-to-noise ratio (as opposed to a **sub-exponential** modulus-to-noise ratio)

[see paper for details]

Security Analysis

public keys

A_1, B_1, p_1

A_2, B_2, p_2

challenge ciphertext

$s_1^{\mathrm{T}} A_1 \qquad s_1^{\mathrm{T}} B_1 + s_2^{\mathrm{T}} B_2$

$s_2^{\mathrm{T}} A_2 \qquad s_1^{\mathrm{T}} p_1 + s_2^{\mathrm{T}} p_2 + \mu \cdot \lfloor q/2 \rceil$

Strategy: Argue ciphertext is pseudorandom (by LWE) if <u>none</u> of the keys satisfy the policy

Challenge: Need to simulate keys k_1 and k_2 *without* trapdoors for A_1 or A_2

secret key

$r_1 \leftarrow H(\mathrm{gid}_1)$
$k_1 \leftarrow A_1^{-1}(p_1 + B_1 r_1)$

$r_2 \leftarrow H(\mathrm{gid}_2)$
$k_2 \leftarrow A_2^{-1}(p_2 + B_2 r_2)$

Evasive LWE [Wee22, Tsa22]:

if $\left([A \mid P], s^{\mathrm{T}}[A \mid P]\right) \approx ([A \mid P], u)$

Security Analysis

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

challenge ciphertext

$\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2$

$\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$

Strategy: Argue ciphertext is pseudorandom (by LWE) if <u>none</u> of the keys satisfy the policy

Challenge: Need to simulate keys $\boldsymbol{k}_1$ and $\boldsymbol{k}_2$ *without* trapdoors for $\boldsymbol{A}_1$ or $\boldsymbol{A}_2$

secret key

$\boldsymbol{r}_1 \leftarrow H(\mathrm{gid}_1)$

$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r}_1)$

$\boldsymbol{r}_2 \leftarrow H(\mathrm{gid}_2)$

$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r}_2)$

Evasive LWE [Wee22, Tsa22]:

if $\left([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{s}^{\mathrm{T}}[\boldsymbol{A} \mid \boldsymbol{P}]\right) \approx \left([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{u}\right)$

then $\left([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}, \boldsymbol{A}^{-1}(\boldsymbol{P})\right) \approx \left([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{u}, \boldsymbol{A}^{-1}(\boldsymbol{P})\right)$

Security Analysis

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

challenge ciphertext

$\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2$

$\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$

Strategy: Argue ciphertext is pseudorandom (by LWE) if none of the keys satisfy the policy

Challenge: Need to simulate keys $\boldsymbol{k}_1$ and $\boldsymbol{k}_2$ *without* trapdoors for $\boldsymbol{A}_1$ or $\boldsymbol{A}_2$

secret key

$\boldsymbol{r}_1 \leftarrow H(\mathrm{gid}_1)$

$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r}_1)$

$\boldsymbol{r}_2 \leftarrow H(\mathrm{gid}_2)$

$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r}_2)$

Evasive LWE [Wee22, Tsa22]:

if $\left([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{s}^{\mathrm{T}}[\boldsymbol{A} \mid \boldsymbol{P}]\right) \approx ([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{u})$

then $\left([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}, \boldsymbol{A}^{-1}(\boldsymbol{P})\right) \approx \left([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{u}, \boldsymbol{A}^{-1}(\boldsymbol{P})\right)$

Security Analysis

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

challenge ciphertext

$\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2$

$\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$

Strategy: Argue ciphertext is pseudorandom (by LWE) if <u>none</u> of the keys satisfy the policy

Challenge: Need to simulate keys $\boldsymbol{k}_1$ and $\boldsymbol{k}_2$ *without* trapdoors for $\boldsymbol{A}_1$ or $\boldsymbol{A}_2$

secret key

$\boldsymbol{r}_1 \leftarrow H(\mathrm{gid}_1)$

$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r}_1)$

$\boldsymbol{r}_2 \leftarrow H(\mathrm{gid}_2)$

$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r}_2)$

Evasive LWE [Wee22, Tsa22]:

if $\left([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{s}^{\mathrm{T}}[\boldsymbol{A} \mid \boldsymbol{P}]\right) \approx ([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{u})$

then $\left([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}, \boldsymbol{A}^{-1}(\boldsymbol{P})\right) \approx \left([\boldsymbol{A} \mid \boldsymbol{P}], \boldsymbol{u}, \boldsymbol{A}^{-1}(\boldsymbol{P})\right)$

Show: $\boldsymbol{s}_1^{\mathrm{T}}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r}_1)$ is pseudorandom when $\boldsymbol{r}_1 \leftarrow H(\mathrm{gid}_1)$

Security Analysis

public keys

A_1, B_1, p_1

A_2, B_2, p_2

challenge ciphertext

$s_1^{\mathrm{T}} A_1 \quad s_1^{\mathrm{T}} B_1 + s_2^{\mathrm{T}} B_2$

$s_2^{\mathrm{T}} A_2 \quad s_1^{\mathrm{T}} p_1 + s_2^{\mathrm{T}} p_2 + \mu \cdot \lfloor q/2 \rceil$

Strategy: Argue ciphertext is pseudorandom (by LWE) if none of the keys satisfy the policy

Challenge: Need to simulate keys k_1 and k_2 *without* trapdoors for A_1 or A_2

secret key

$r_1 \leftarrow H(\mathrm{gid}_1)$

$k_1 \leftarrow A_1^{-1}(p_1 + B_1 r_1)$

$r_2 \leftarrow H(\mathrm{gid}_2)$

$k_2 \leftarrow A_2^{-1}(p_2 + B_2 r_2)$

Evasive LWE [Wee22, Tsa22]:

if $\left([A \mid P], s^{\mathrm{T}}[A \mid P]\right) \approx ([A \mid P], u)$

then $\left([A \mid P], s^{\mathrm{T}} A, A^{-1}(P)\right) \approx \left([A \mid P], u, A^{-1}(P)\right)$

Show: $s_1^{\mathrm{T}}(p_1 + B_1 r_1)$ is pseudorandom when $r_1 \leftarrow H(\mathrm{gid}_1)$

How to design the hash function H?

Security Analysis

Show: $\underset{\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim}{\boldsymbol{s}_1^{\mathrm{T}}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r}_1)}$ is pseudorandom when $\boldsymbol{r}_1 \leftarrow H(\mathrm{gid}_1)$

(and given some additional components that depend on $\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1$ and $\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1$)

Main idea: for an input $x \in \{0,1\}^{\ell}$, define $H(x) = \left(\prod_{i\in[\ell]} \boldsymbol{D}_{x_i}\right)\boldsymbol{e}_1$

where $\boldsymbol{D}_0, \boldsymbol{D}_1$ are public short matrices and $\boldsymbol{e}_1$ is the first basis vector

subset product of short matrices

Security Analysis

Show: $\underset{\sim\sim\sim}{\boldsymbol{s}_1^{\mathrm{T}}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r}_1)}$ is pseudorandom when $\boldsymbol{r}_1 \leftarrow H(\mathrm{gid}_1)$

(and given some additional components that depend on $\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1$ and $\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1$)

Main idea: for an input $x \in \{0,1\}^\ell$, define $H(x) = \left(\prod_{i\in[\ell]} \boldsymbol{D}_{x_i}\right)\boldsymbol{e}_1$

where $\boldsymbol{D}_0, \boldsymbol{D}_1$ are public short matrices and $\boldsymbol{e}_1$ is the first basis vector

subset product of short matrices

[BLMR13]: $F_{\boldsymbol{D}_0,\boldsymbol{D}_1}(\boldsymbol{s}, x) \coloneqq \boldsymbol{s}^{\mathrm{T}} \prod_{i\in[\ell]} \boldsymbol{D}_{x_i}$ is a pseudorandom function

Security Analysis

Show: $\underset{\sim\sim\sim}{\boldsymbol{s}_1^{\mathrm{T}}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r}_1)}$ is pseudorandom when $\boldsymbol{r}_1 \leftarrow H(\mathrm{gid}_1)$

(and given some additional components that depend on $\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1$ and $\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1$)

Main idea: for an input $x \in \{0,1\}^{\ell}$, define $H(x) = \left(\prod_{i\in[\ell]} \boldsymbol{D}_{x_i}\right)\boldsymbol{e}_1$
where $\boldsymbol{D}_0, \boldsymbol{D}_1$ are public short matrices and $\boldsymbol{e}_1$ is the first basis vector

subset product of short matrices

[BLMR13]: $F_{\boldsymbol{D}_0,\boldsymbol{D}_1}(\boldsymbol{s}, x) \coloneqq \boldsymbol{s}^{\mathrm{T}} \prod_{i\in[\ell]} \boldsymbol{D}_{x_i}$ is a pseudorandom function

Evasive LWE precondition (essentially) follows via [BLMR13]

see paper for full details

Summary

public keys

A_1, B_1, p_1

A_2, B_2, p_2

ciphertext

$s_1^{\mathrm{T}} A_1 \quad s_1^{\mathrm{T}} B_1 + s_2^{\mathrm{T}} B_2$

$s_2^{\mathrm{T}} A_2 \quad s_1^{\mathrm{T}} p_1 + s_2^{\mathrm{T}} p_2 + \mu \cdot \lfloor q/2 \rceil$

secret key

$r \leftarrow H(\mathrm{gid})$

$k_1 \leftarrow A_1^{-1}(p_1 + B_1 r)$

$k_2 \leftarrow A_2^{-1}(p_2 + B_2 r)$

Multi-authority ABE for conjunctions based on [DKW21a] is secure assuming either

- LWE (with polynomial modulus-to-noise ratio) if H is modeled as a random oracle; or

Summary

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

ciphertext

$\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2$

$\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$

secret key

$\boldsymbol{r} \leftarrow H(\mathrm{gid})$

$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r})$

$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r})$

Multi-authority ABE for conjunctions based on [DKW21a] is secure assuming either

- LWE (with polynomial modulus-to-noise ratio) if H is modeled as a random oracle; or
- evasive LWE if H is a subset-product of short matrices

Summary

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

ciphertext

$\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2$

$\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$

secret key

$\boldsymbol{r} \leftarrow H(\mathrm{gid})$

$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r})$

$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r})$

Multi-authority ABE for conjunctions based on [DKW21a] is secure assuming either

- LWE (with polynomial modulus-to-noise ratio) if H is modeled as a random oracle; or
- evasive LWE if H is a subset-product of short matrices

Not a “random looking” function!

Summary

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

ciphertext

$\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2$

$\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$

secret key

$\boldsymbol{r} \leftarrow H(\mathrm{gid})$

$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r})$

$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r})$

Multi-authority ABE for conjunctions based on [DKW21a] is secure assuming either

- LWE (with polynomial modulus-to-noise ratio) if H is modeled as a random oracle; or
- evasive LWE if H is a subset-product of short matrices

Open problems:

- Multi-authority ABE from *plain* LWE

Summary

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

ciphertext

$\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2$

$\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$

secret key

$\boldsymbol{r} \leftarrow H(\mathrm{gid})$

$\boldsymbol{k_1} \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r})$

$\boldsymbol{k_2} \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r})$

Multi-authority ABE for conjunctions based on [DKW21a] is secure assuming either

- LWE (with polynomial modulus-to-noise ratio) if H is modeled as a random oracle; or
- evasive LWE if H is a subset-product of short matrices

Open problems:

- Multi-authority ABE from *plain* LWE
- Lattice-based multi-authority ABE beyond conjunctions

Summary

public keys

$\boldsymbol{A}_1, \boldsymbol{B}_1, \boldsymbol{p}_1$

$\boldsymbol{A}_2, \boldsymbol{B}_2, \boldsymbol{p}_2$

ciphertext

$$\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{A}_1 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{B}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{B}_2$$

$$\boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{A}_2 \quad \boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{p}_1 + \boldsymbol{s}_2^{\mathrm{T}}\boldsymbol{p}_2 + \mu \cdot \lfloor q/2 \rceil$$

secret key

$$\boldsymbol{r} \leftarrow H(\mathrm{gid})$$

$$\boldsymbol{k}_1 \leftarrow \boldsymbol{A}_1^{-1}(\boldsymbol{p}_1 + \boldsymbol{B}_1\boldsymbol{r})$$

$$\boldsymbol{k}_2 \leftarrow \boldsymbol{A}_2^{-1}(\boldsymbol{p}_2 + \boldsymbol{B}_2\boldsymbol{r})$$

Multi-authority ABE for conjunctions based on [DKW21a] is secure assuming either

- LWE (with polynomial modulus-to-noise ratio) if H is modeled as a random oracle; or
- evasive LWE if H is a subset-product of short matrices

Open problems:

- Multi-authority ABE from *plain* LWE
- Lattice-based multi-authority ABE beyond conjunctions

`https://eprint.iacr.org/2022/1194`

Thank you!