Decentralized Multi-Authority ABE for DNFs from LWE

By Pratish Datta,

Joint work with Ilan Komargodski, Brent Waters

NTT Research, Hebrew University, UT Austin

EUROCRYPT 2021, October 17-21, 2021

Attribute-Based Encryption

[SW05,GPSW06,…]

- A secret key allows one to decrypt all ciphertext that satisfy

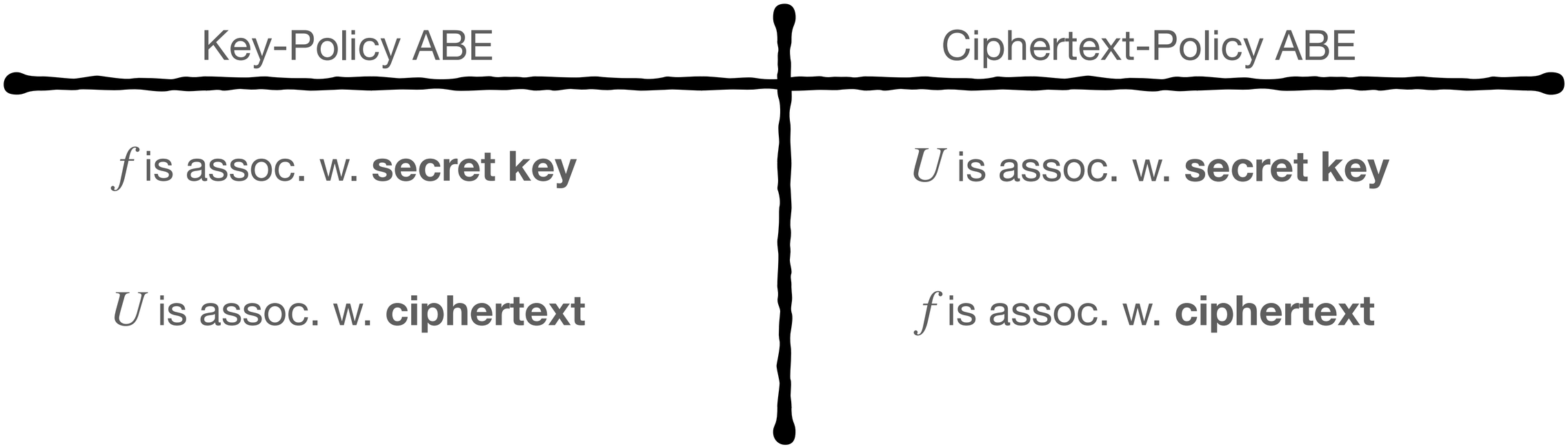
$$f(U) = \text{true}$$

Attribute-Based Encryption

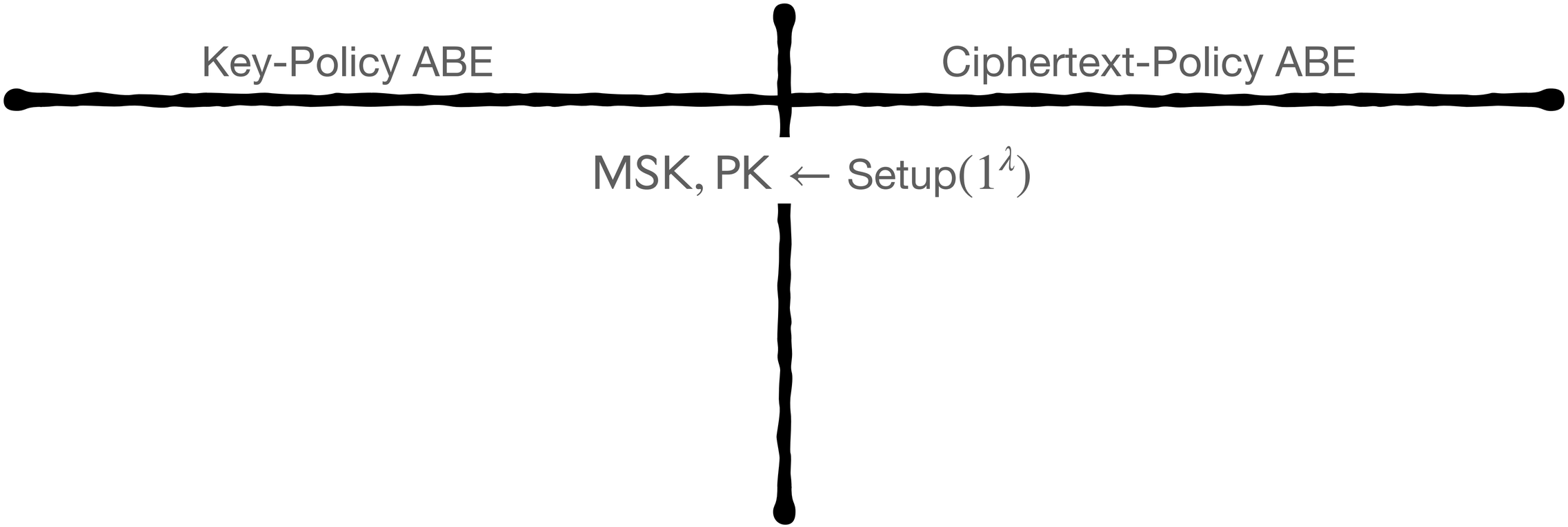
[SW05,GPSW06,…]

- A secret key allows one to decrypt all ciphertext that satisfy

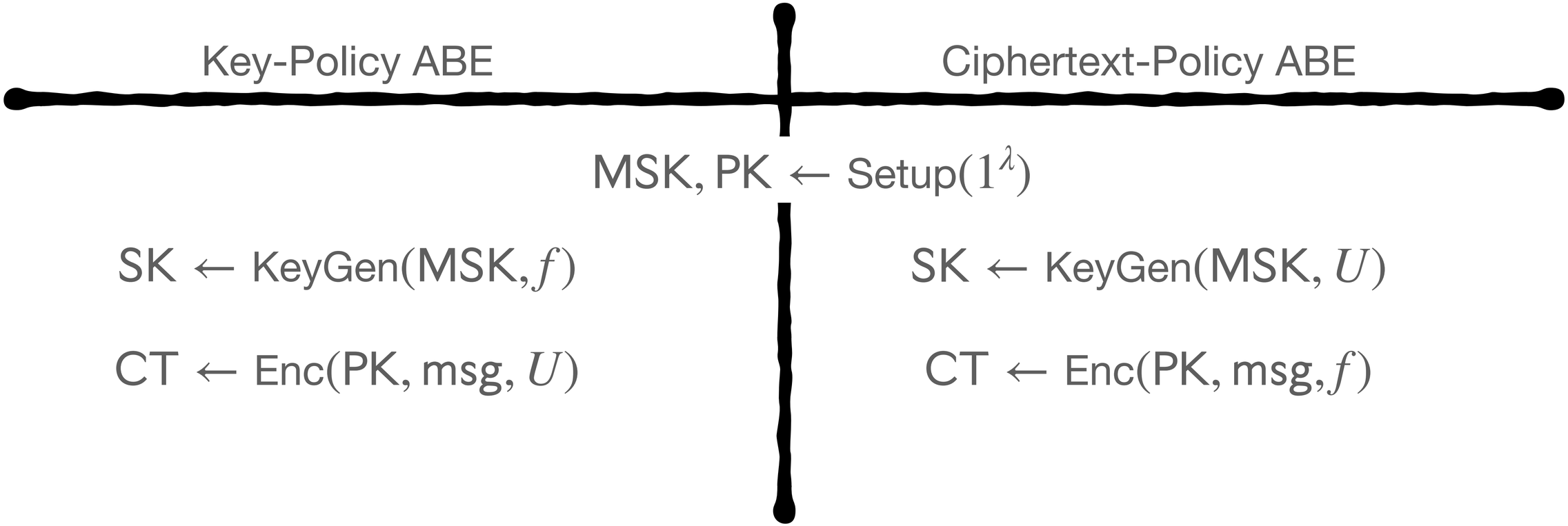
$$f(U) = \text{true}$$



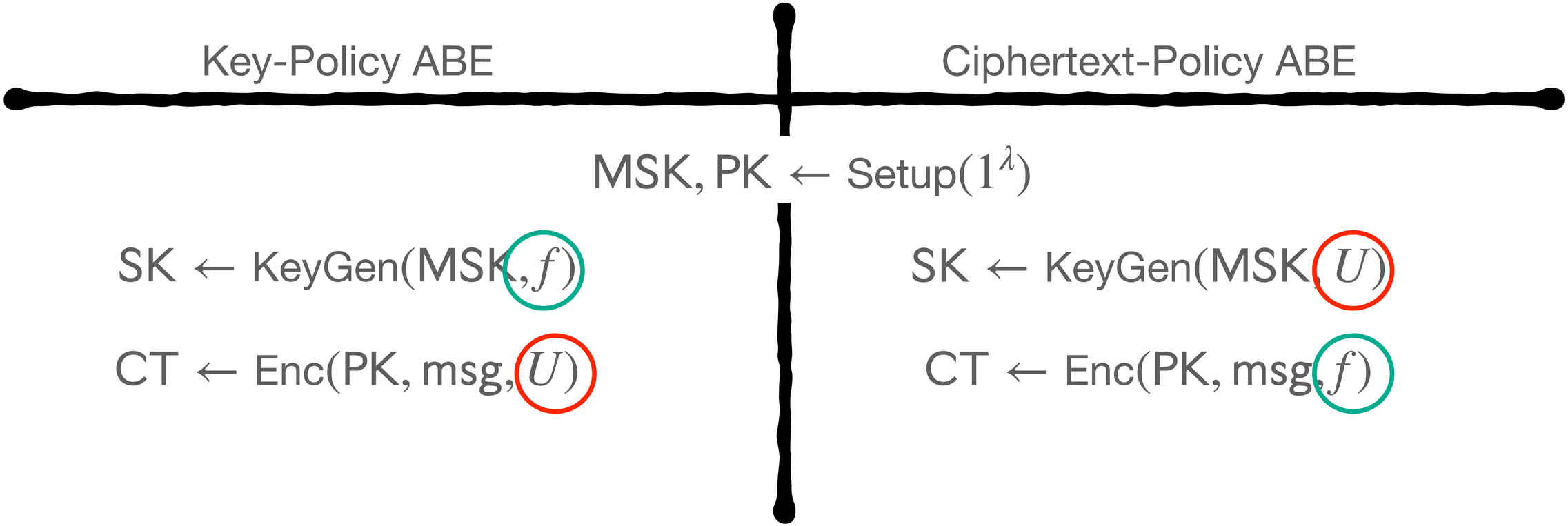
Attribute-Based Encryption



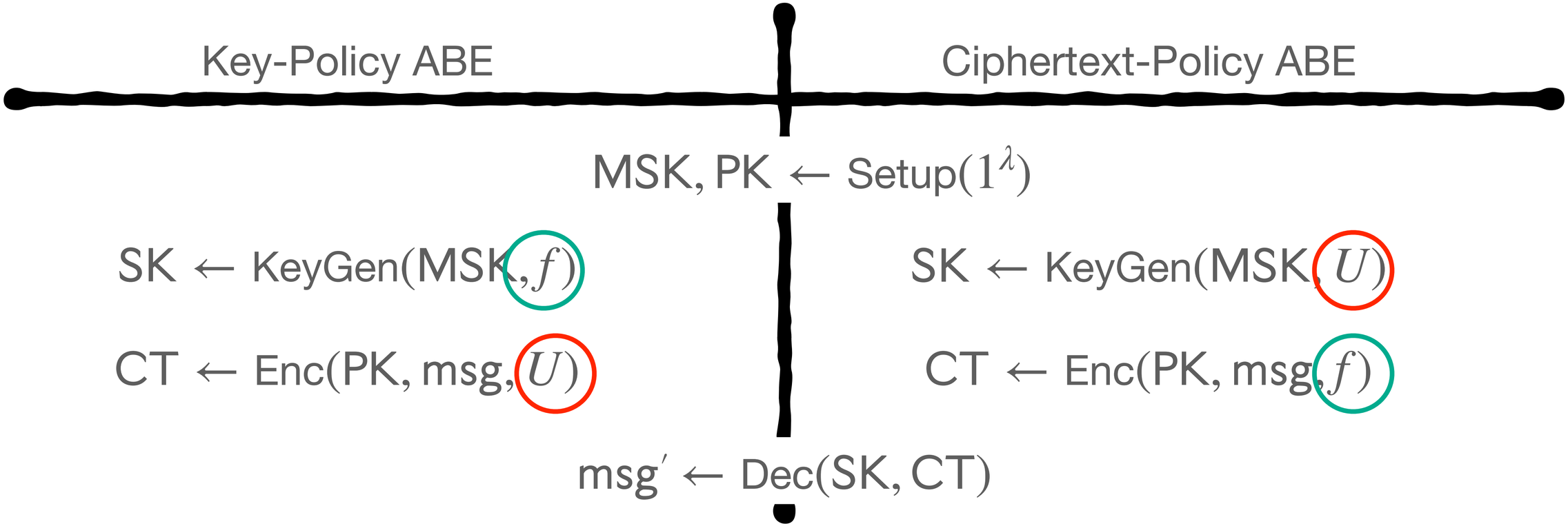
Attribute-Based Encryption



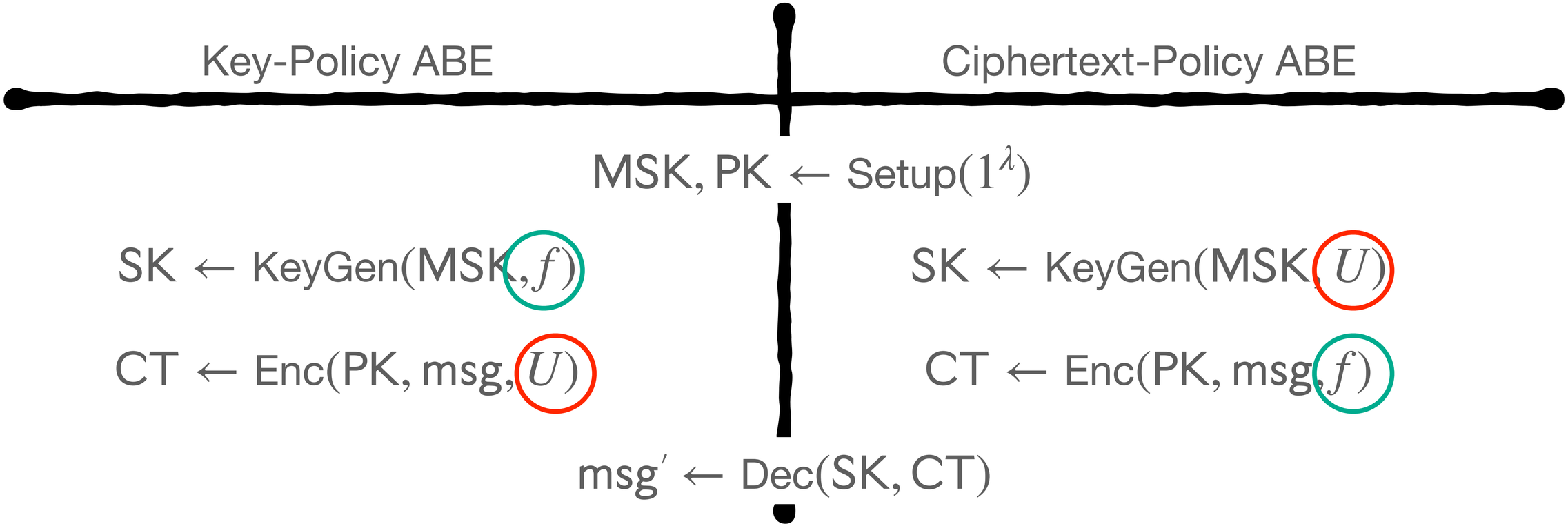
Attribute-Based Encryption



Attribute-Based Encryption



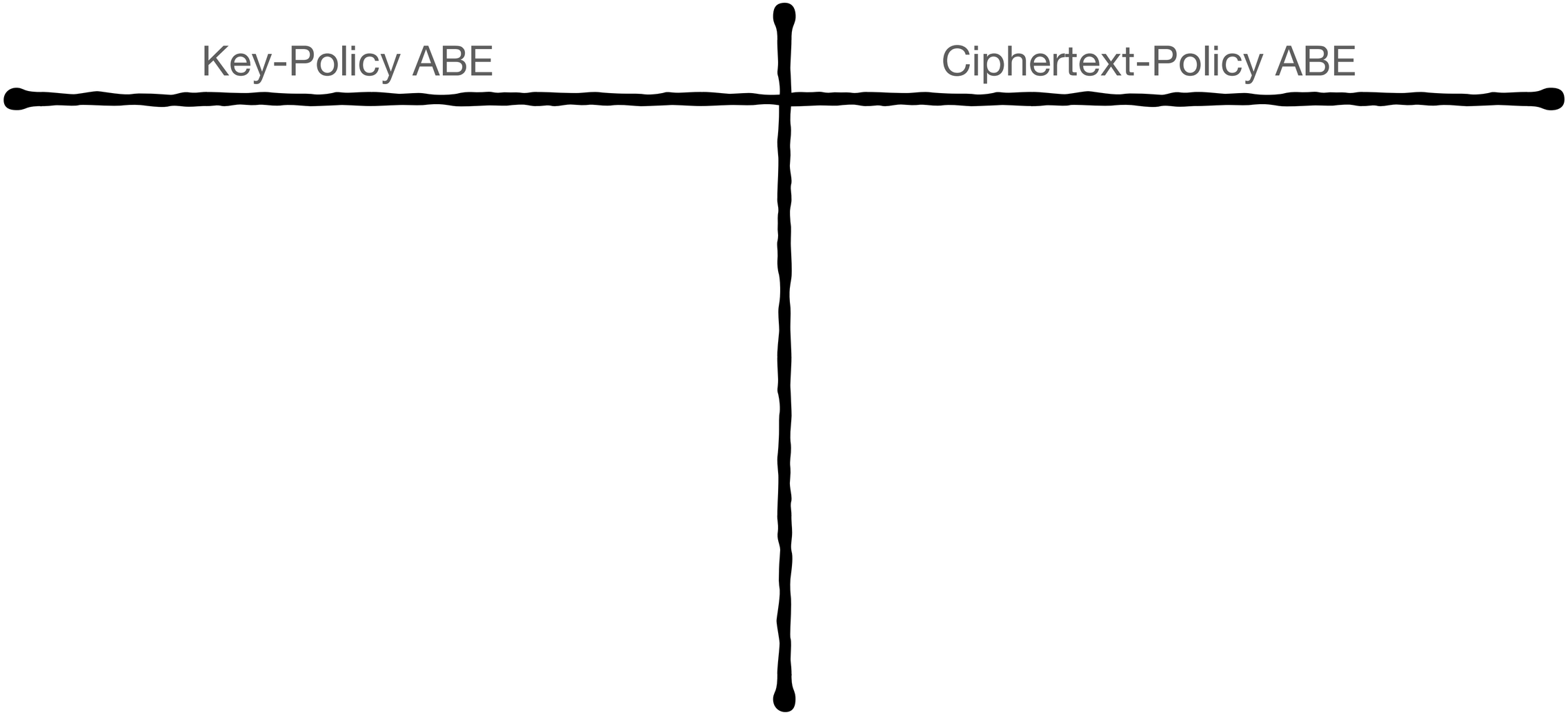
Attribute-Based Encryption



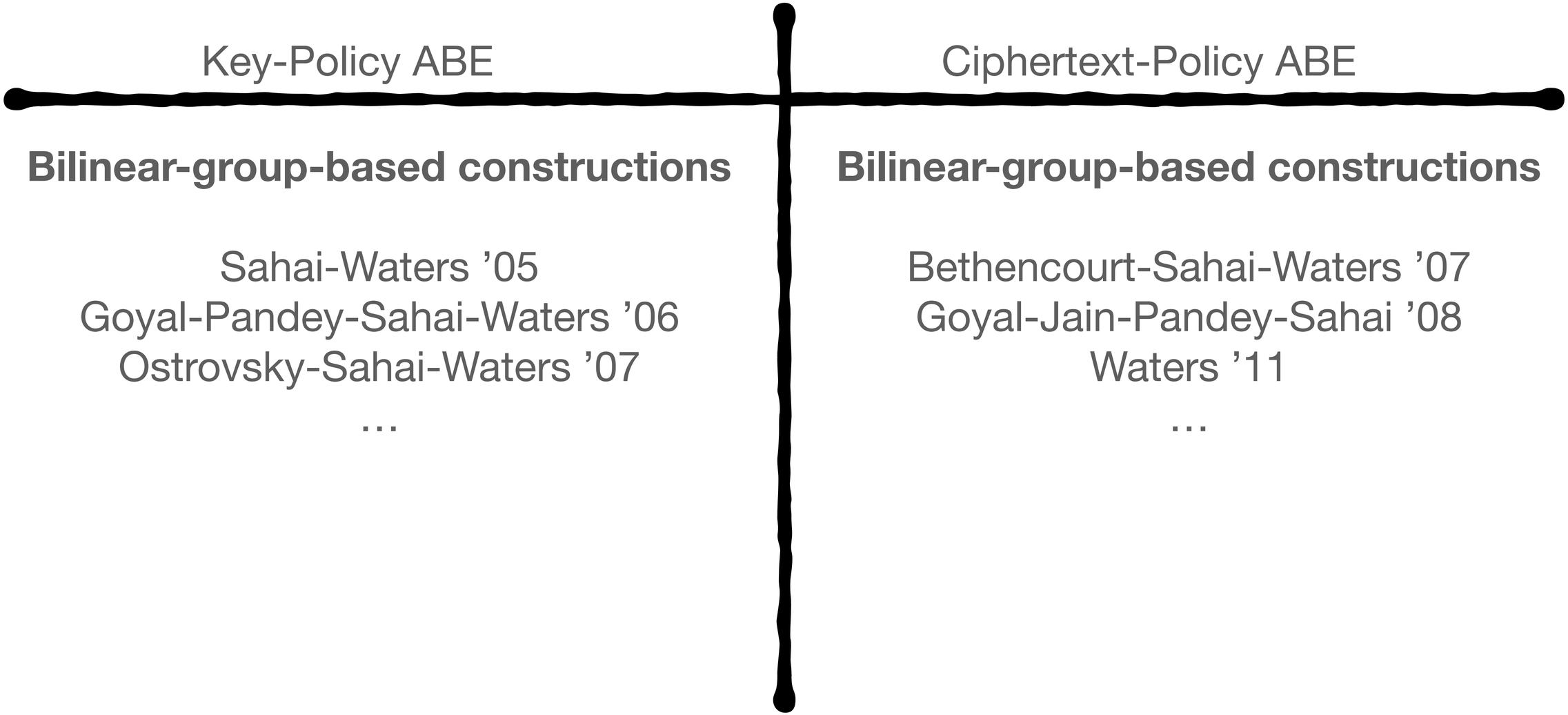
Correctness: If $f(U) =$ true then $\text{msg}' = \text{msg}$

Security: If $f(U) =$ false then msg is “hidden”

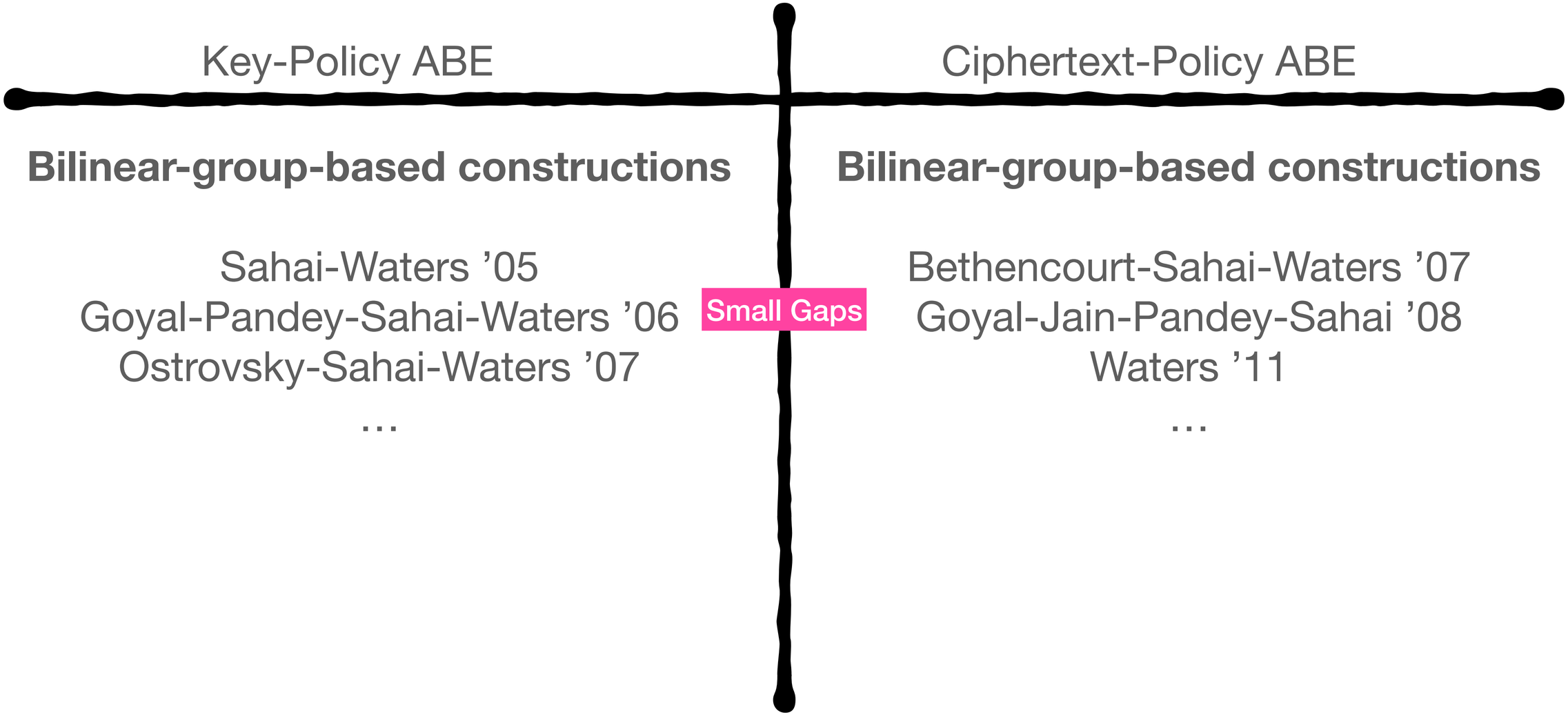
Attribute-Based Encryption



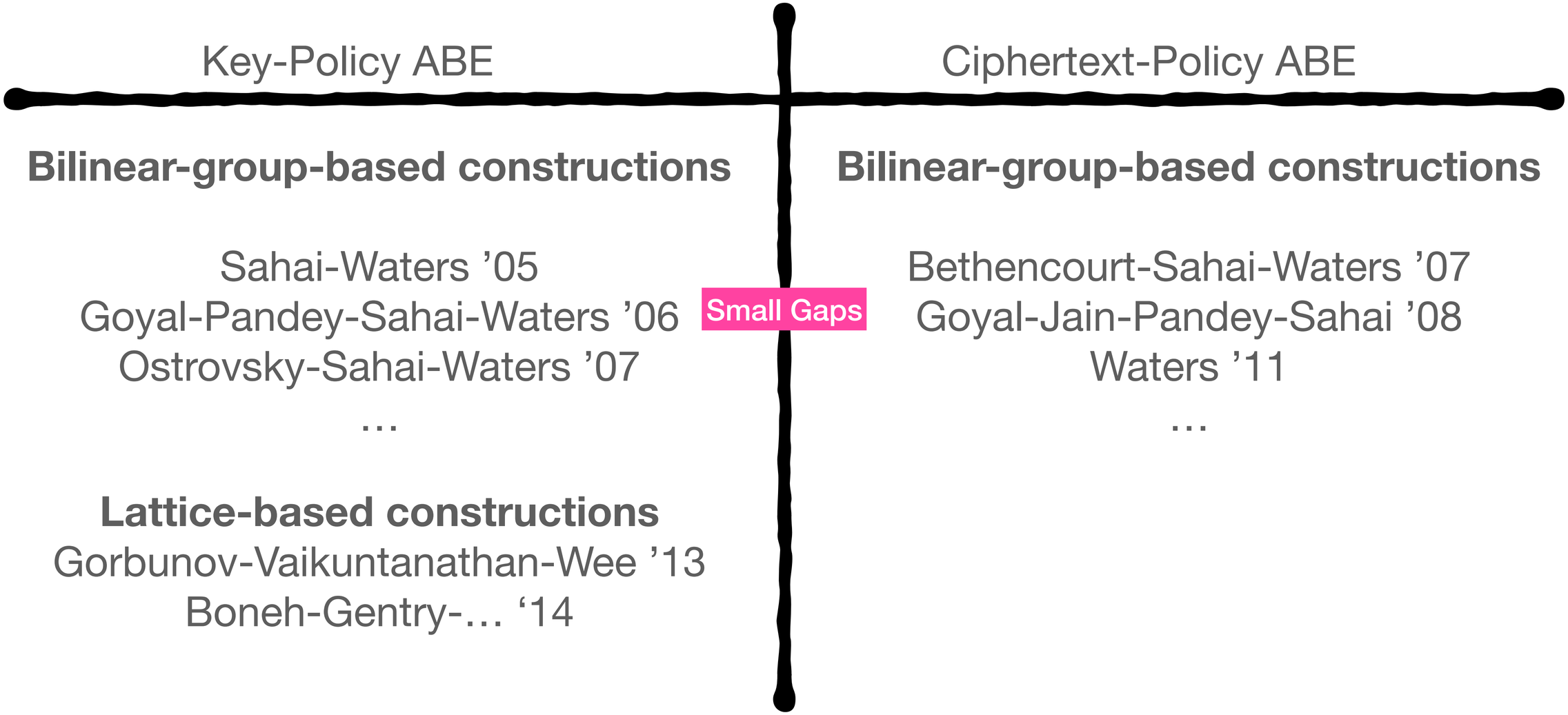
Attribute-Based Encryption



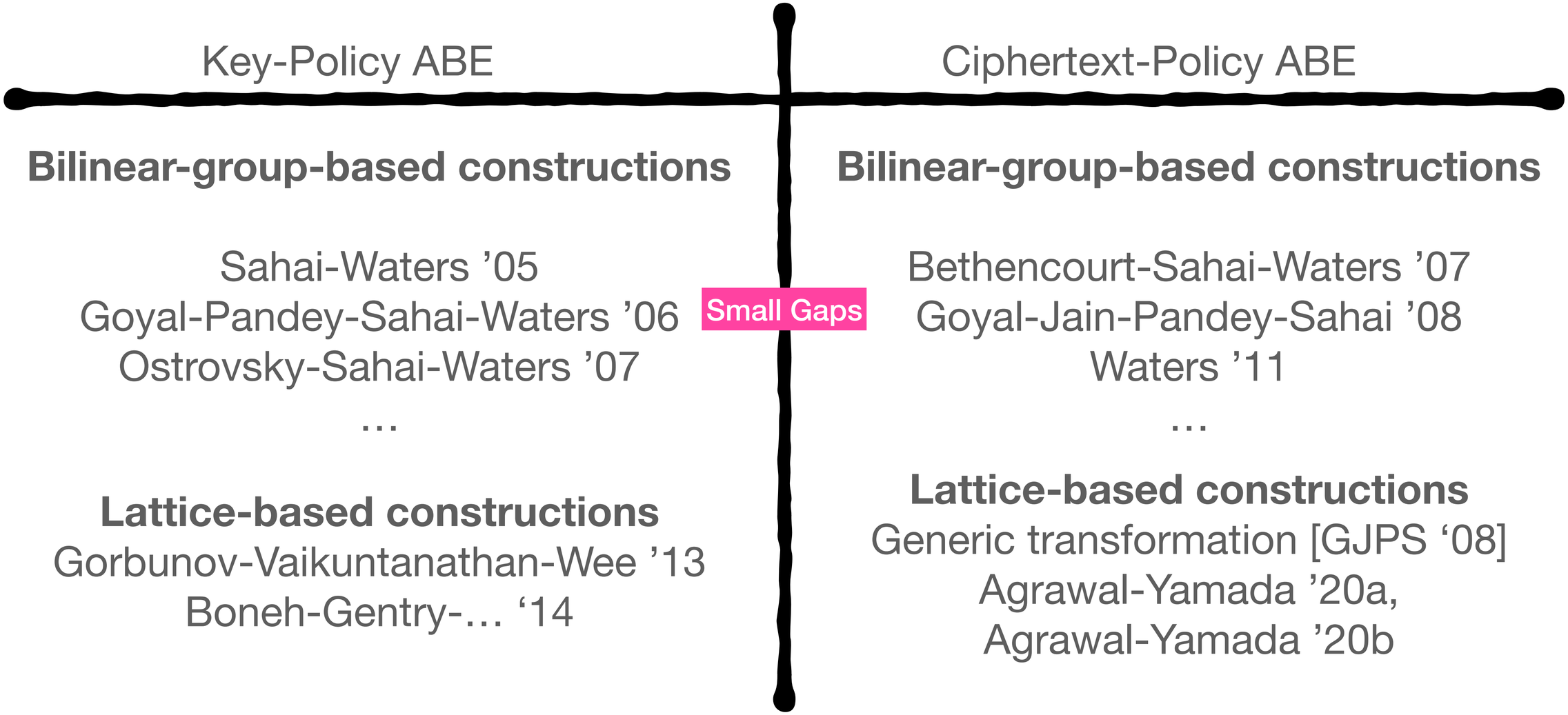
Attribute-Based Encryption



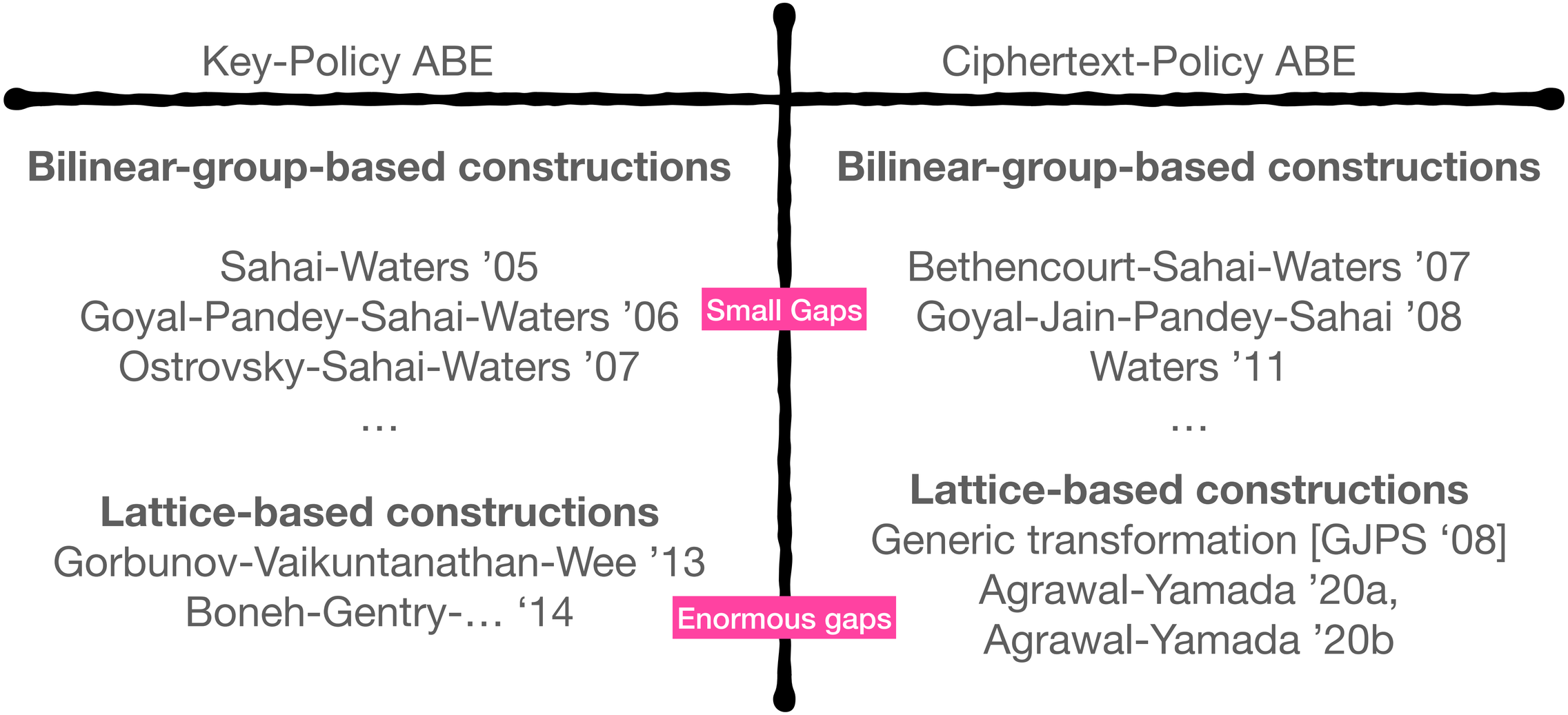
Attribute-Based Encryption



Attribute-Based Encryption



Attribute-Based Encryption



Multi-Authority ABE (MA-ABE)

- In ABE, *one central authority who verifies attributes and issues secret keys*

Multi-Authority ABE (MA-ABE)

- In ABE, *one central authority who verifies attributes and issues secret keys*
- In reality, multiple authorities are in charge of different attributes

Multi-Authority ABE (MA-ABE)

- In ABE, *one central authority who verifies attributes and issues secret keys*
- In reality, multiple authorities are in charge of different attributes
  - DMV for “holds a driving license”

Multi-Authority ABE (MA-ABE)

- In ABE, *one central authority who verifies attributes and issues secret keys*
- In reality, multiple authorities are in charge of different attributes
  - DMV for “holds a driving license”
  - University for “holds a Ph.D”

Multi-Authority ABE (MA-ABE)

- In ABE, *one central authority who verifies attributes and issues secret keys*
- In reality, multiple authorities are in charge of different attributes
  - DMV for “holds a driving license”
  - University for “holds a Ph.D”
  - Military for “veteran”

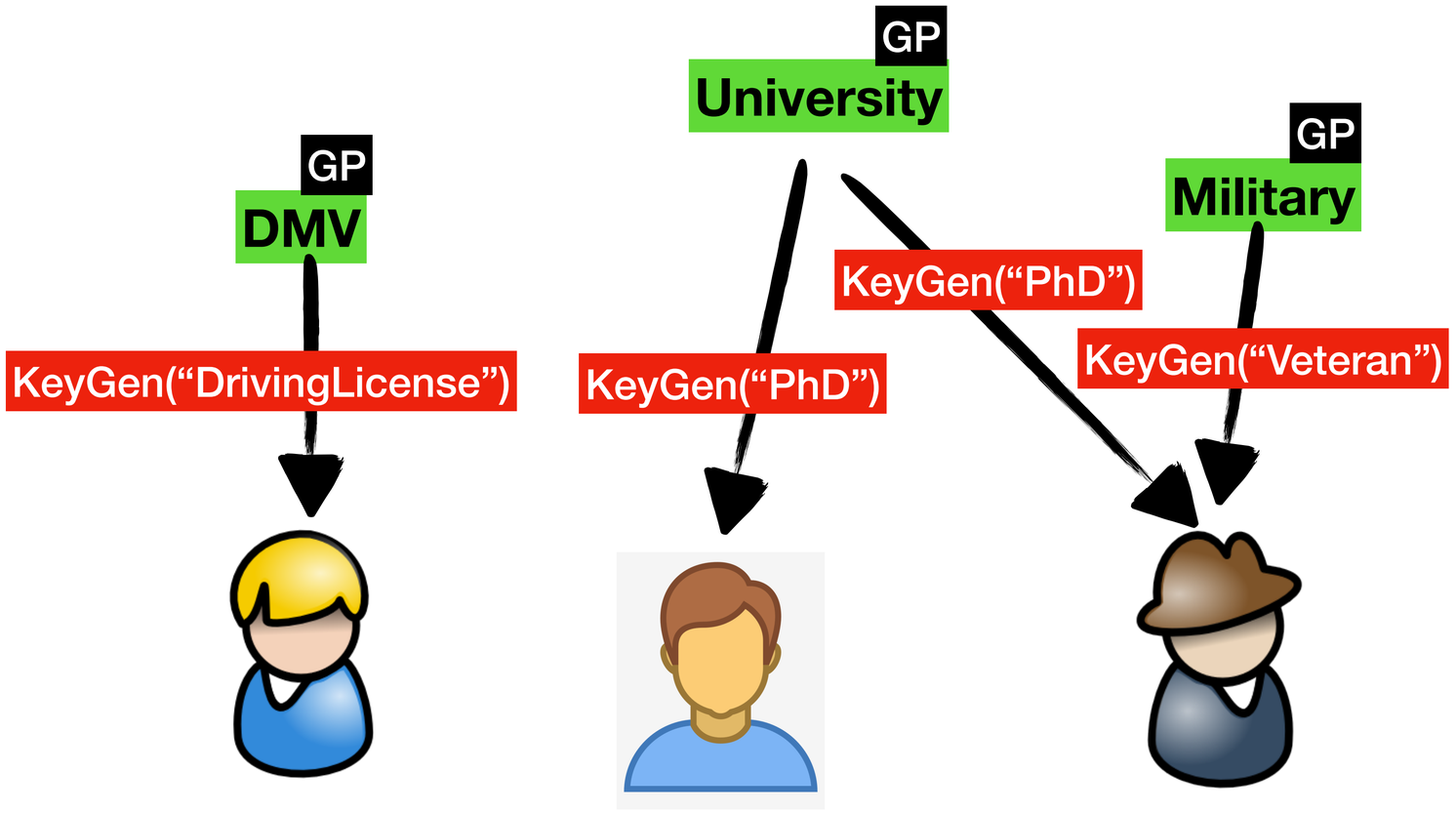
Multi-Authority ABE (MA-ABE)

- In ABE, *one central authority who verifies attributes and issues secret keys*
- In reality, multiple authorities are in charge of different attributes
  - DMV for “holds a driving license”
  - University for “holds a Ph.D”
  - Military for “veteran”
- “Multi-Authority” ABE
  - Chase ’07, …, Lewko-Waters ’11, Okamoto-Takashima ‘13, Rouselakis-Waters ‘15

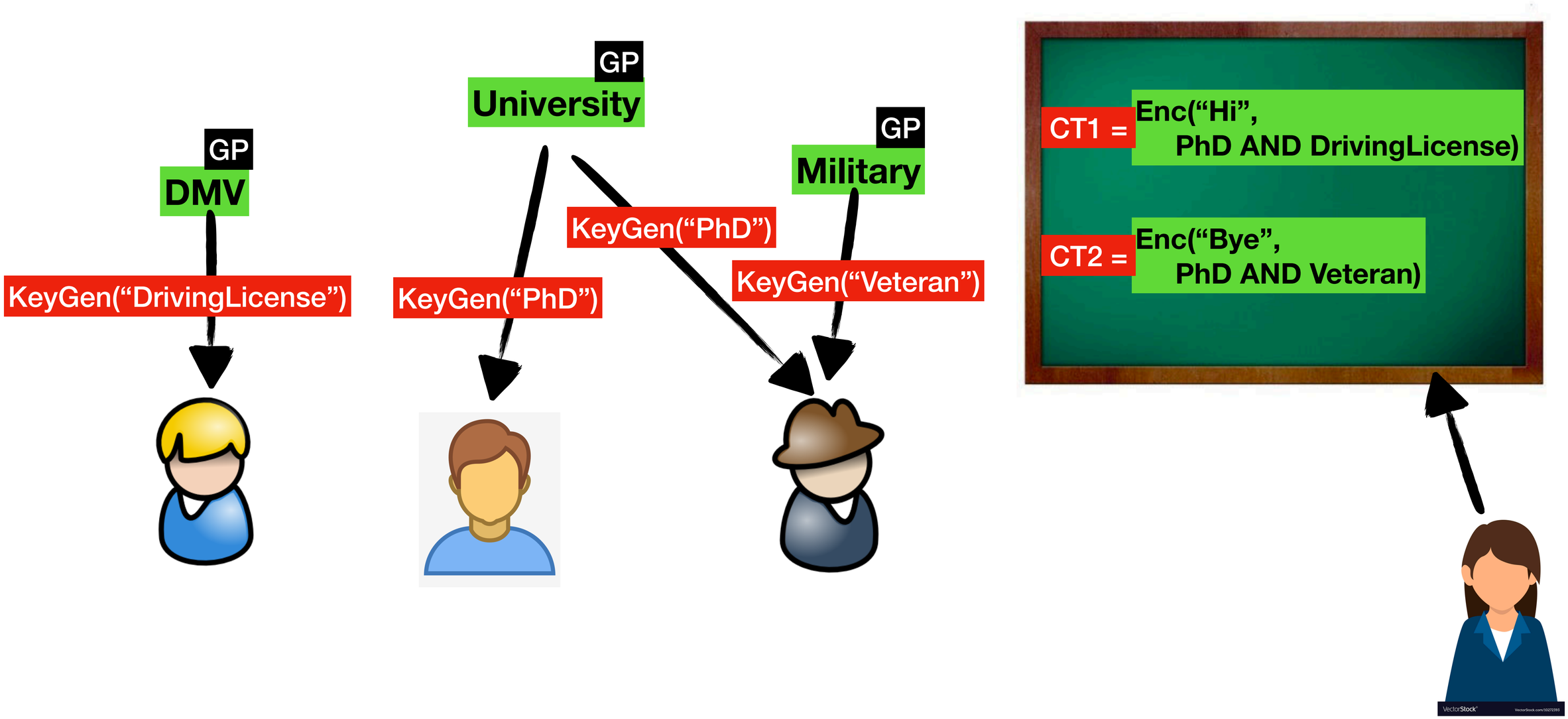
MA-ABE

- Anyone can become an authority
  - No coordination except global PublicParams
- Different authorities control different attributes
- No bound on # of authorities
- Each authority can issue secret keys to users possessing attributes under their control
  - without any interaction with other authorities

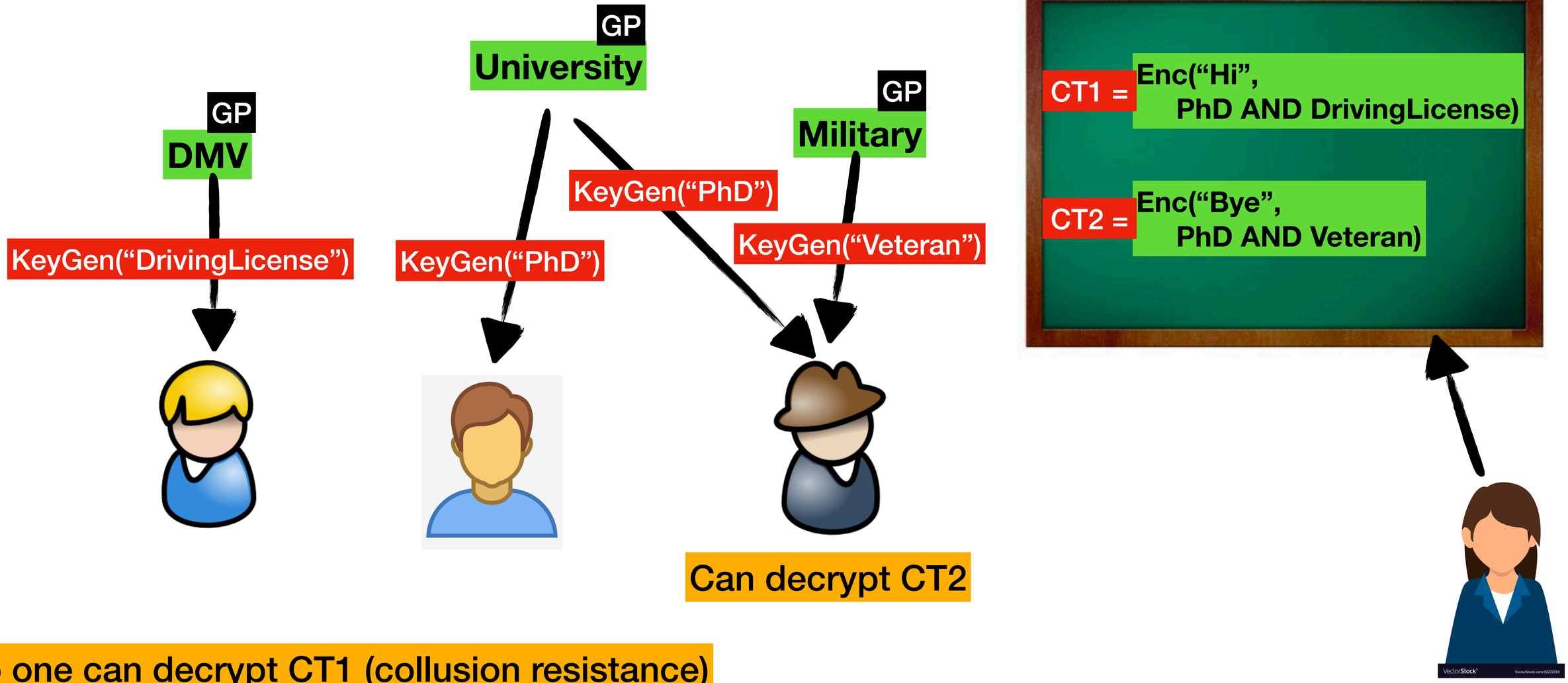
MA-ABE


GP
DMV
KeyGen(“DrivingLicense”)
GP
University
KeyGen(“PhD”)
KeyGen(“PhD”)
GP
Military
KeyGen(“Veteran”)

MA-ABE


GP
DMV
KeyGen(“DrivingLicense”)
GP
University
KeyGen(“PhD”)
KeyGen(“PhD”)
GP
Military
KeyGen(“Veteran”)
CT1 = Enc(“Hi”, PhD AND DrivingLicense)
CT2 = Enc(“Bye”, PhD AND Veteran)

MA-ABE



No one can decrypt CT1 (collusion resistance)

The GID Model

Chase ‘07

The GID Model

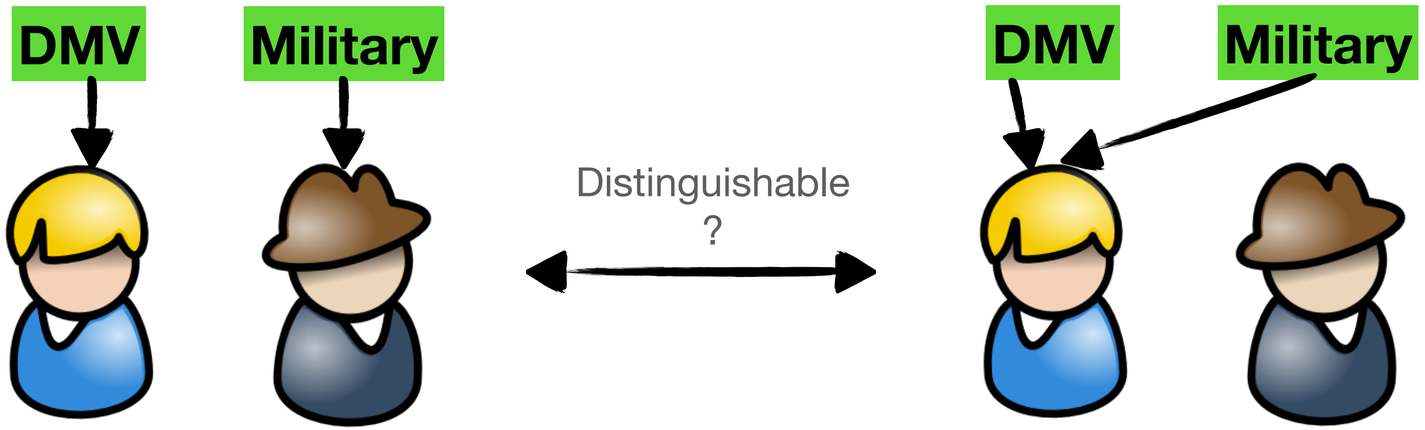
Chase ‘07

- How to uniquely identify a user?

The GID Model

Chase ‘07

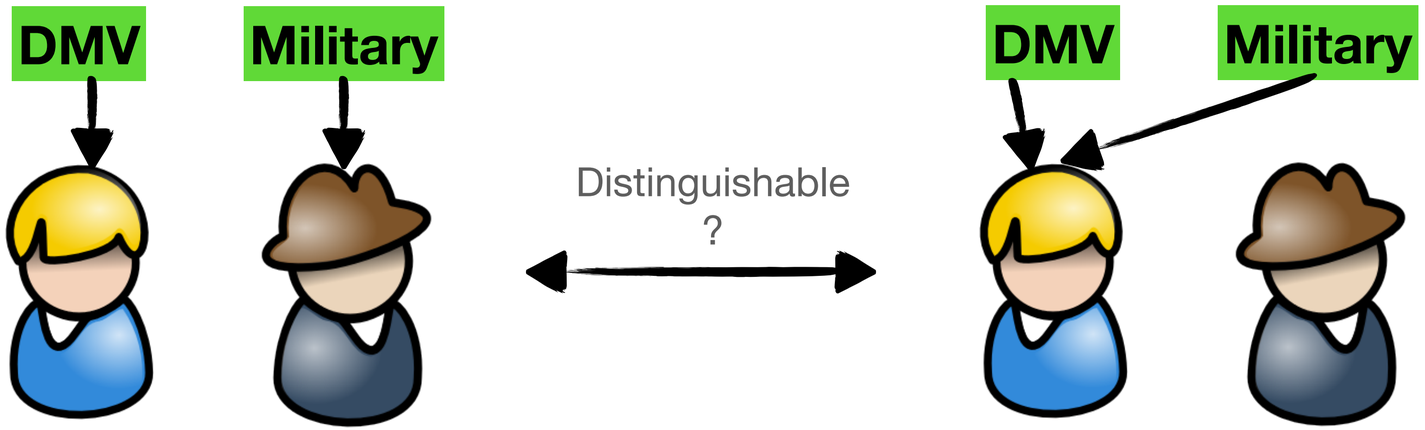
- How to uniquely identify a user?



The GID Model

Chase ‘07

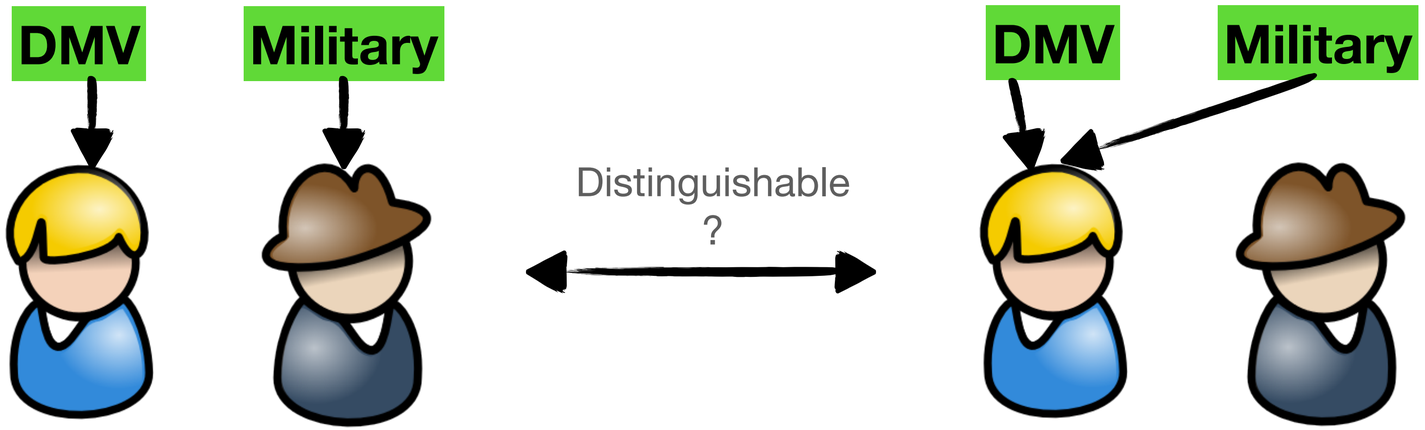
- How to uniquely identify a user?
- Associate a unique global *verifiable* identifier (GID)



The GID Model

Chase ‘07

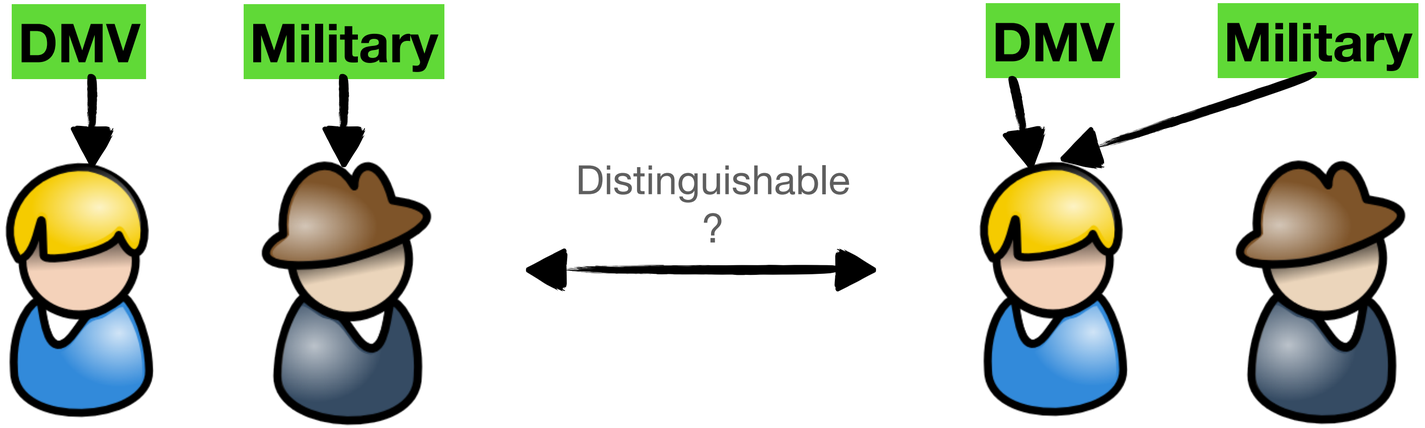
- How to uniquely identify a user?
- Associate a unique global *verifiable* identifier (GID)
- The global identity of a user remains fixed for the entire lifetime of the system



The GID Model

Chase ‘07

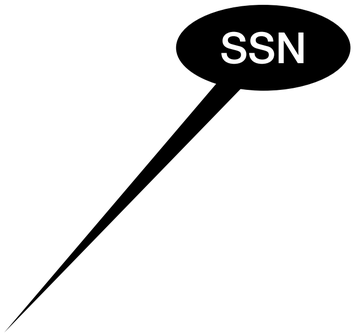
- How to uniquely identify a user?
- Associate a unique global *verifiable* identifier (GID)
- The global identity of a user remains fixed for the entire lifetime of the system
- Users have no freedom to choose their global identities

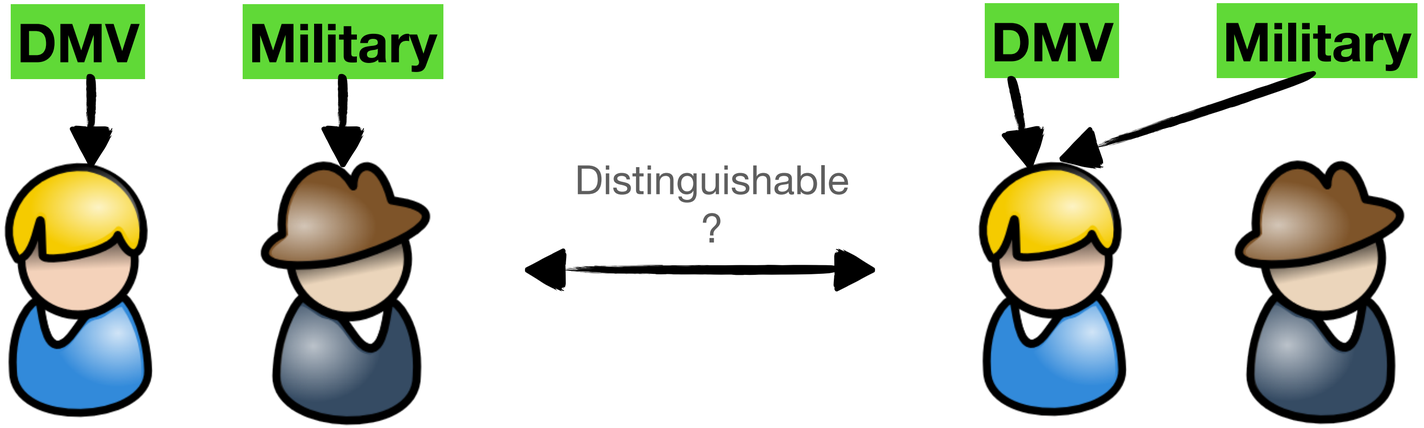


The GID Model

Chase ‘07

- How to uniquely identify a user?
- Associate a unique global *verifiable* identifier (GID)
- The global identity of a user remains fixed for the entire lifetime of the system
- Users have no freedom to choose their global identities





MA-ABE Syntax

(Assume one attribute per authority)

$$\mathsf{GP} \leftarrow \mathsf{GlobalSetup}(1^{\lambda})$$

MA-ABE Syntax

(Assume one attribute per authority)

$$\mathsf{GP} \leftarrow \mathsf{GlobalSetup}(1^\lambda)$$

$$\mathsf{PK}_u, \mathsf{MSK}_u \leftarrow \mathsf{AuthSetup}(\mathsf{GP}, u) \qquad \mathsf{SK}_{\mathsf{GID},u} \leftarrow \mathsf{KeyGen}(\mathsf{MSK}_u, \mathsf{GID})$$

MA-ABE Syntax

(Assume one attribute per authority)

$$\mathsf{GP} \leftarrow \mathsf{GlobalSetup}(1^\lambda)$$

$$\mathsf{PK}_u, \mathsf{MSK}_u \leftarrow \mathsf{AuthSetup}(\mathsf{GP}, u) \qquad \mathsf{SK}_{\mathsf{GID},u} \leftarrow \mathsf{KeyGen}(\mathsf{MSK}_u, \mathsf{GID})$$

$$\mathsf{CT} \leftarrow \mathsf{Enc}(\{\mathsf{PK}_u\}_{u \in f}, \mathsf{msg}, f)$$

MA-ABE Syntax

(Assume one attribute per authority)

$$\mathsf{GP} \leftarrow \mathsf{GlobalSetup}(1^\lambda)$$

$$\mathsf{PK}_u, \mathsf{MSK}_u \leftarrow \mathsf{AuthSetup}(\mathsf{GP}, u) \qquad \mathsf{SK}_{\mathsf{GID},u} \leftarrow \mathsf{KeyGen}(\mathsf{MSK}_u, \mathsf{GID})$$

$$\mathsf{CT} \leftarrow \mathsf{Enc}(\{\mathsf{PK}_u\}_{u \in f}, \mathsf{msg}, f)$$

$$\mathsf{msg}' \leftarrow \mathsf{Dec}(\{\mathsf{SK}_{\mathsf{GID},u}\}_{u \in U}, \mathsf{CT})$$

(All with same GID)

MA-ABE Syntax

(Assume one attribute per authority)

$$\mathsf{GP} \leftarrow \mathsf{GlobalSetup}(1^\lambda)$$

$$\mathsf{PK}_u, \mathsf{MSK}_u \leftarrow \mathsf{AuthSetup}(\mathsf{GP}, u) \qquad \mathsf{SK}_{\mathsf{GID},u} \leftarrow \mathsf{KeyGen}(\mathsf{MSK}_u, \mathsf{GID})$$

$$\mathsf{CT} \leftarrow \mathsf{Enc}(\{\mathsf{PK}_u\}_{u \in f}, \mathsf{msg}, f)$$

$$\mathsf{msg}' \leftarrow \mathsf{Dec}(\{\mathsf{SK}_{\mathsf{GID},u}\}_{u \in U}, \mathsf{CT})$$

(All with same GID)

Correctness: If $f(U) = \text{true}$ then $\mathsf{msg}' = \mathsf{msg}$

Security: If $f(U) = \text{false}$ then msg is "hidden"
(Collusion among users and some corrupt authorities is allowed)

MA-ABE (Main) Known Constructions

& Our Main Result

Schemes	Supported Policy Class	Assumption	Attribute per Authority	Security
Lewko-Waters ‘11	NC1	Subgroup decision (composite order)	Bounded	Adaptive
Okamoto-Takashima ‘13	NC1	DLIN (prime order)	Bounded	Adaptive
Rouselakis-Waters ‘15	NC1	q-type (prime order)	Unbounded	Static

(All schemes are in GID model and are proven secure in the random oracle model)

MA-ABE (Main) Known Constructions

& Our Main Result

Schemes	Supported Policy Class	Assumption	Attribute per Authority	Security
Lewko-Waters ‘11	NC1	Subgroup decision (composite order)	Bounded	Adaptive
Okamoto-Takashima ‘13	NC1	DLIN (prime order)	Bounded	Adaptive
Rouselakis-Waters ‘15	NC1	q-type (prime order)	Unbounded	Static
This Work	DNF	LWE	Bounded	Static

(All schemes are in GID model and are proven secure in the random oracle model)

Our Main Theorem

There exist an MA-ABE scheme in the GID model for access policies captured by DNF formulas that is statically secure against an arbitrary collusion of parties in the random oracle model and assuming the LWE assumption.

Our Main Theorem

DNF = OR of ANDs

$$(x \wedge y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (\neg x \wedge y \wedge \neg z)$$

There exist an MA-ABE scheme in the GID model for access policies captured by DNF formulas that is statically secure against an arbitrary collusion of parties in the random oracle model and assuming the LWE assumption.

Our Main Theorem

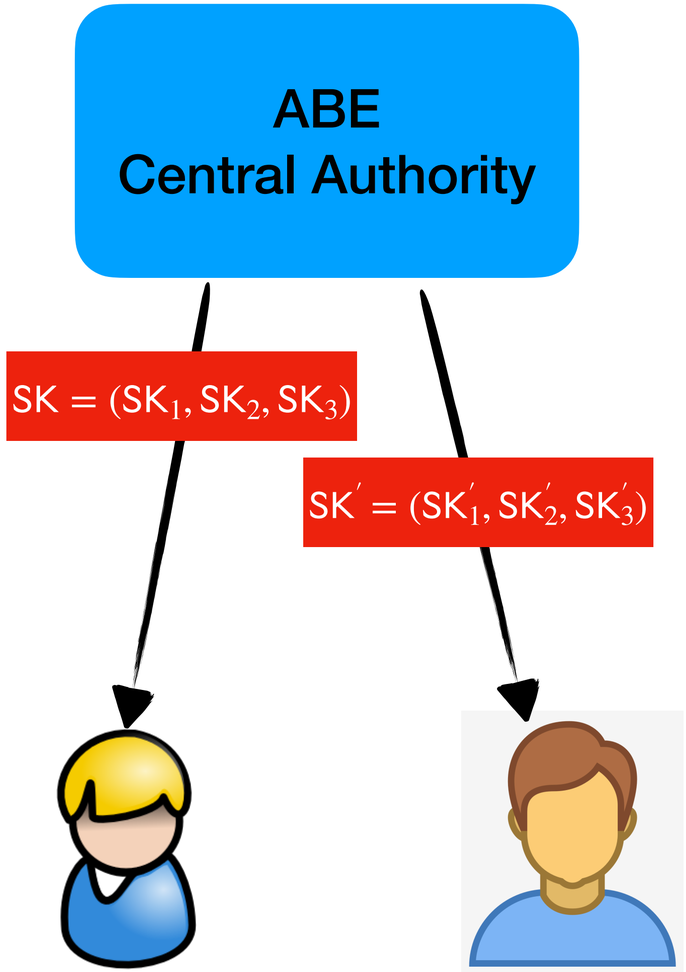
DNF = OR of ANDs

$$(x \wedge y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (\neg x \wedge y \wedge \neg z)$$

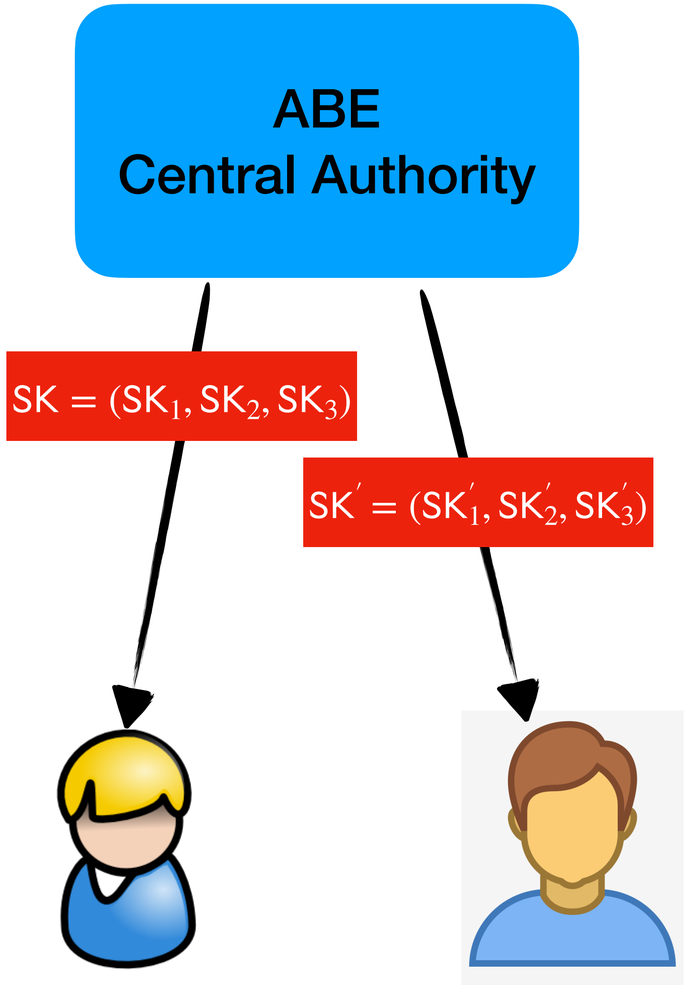
There exist an MA-ABE scheme in the GID model for access policies captured by DNF formulas that is statically secure against an arbitrary collusion of parties in the random oracle model and assuming the LWE assumption.

sub-exp. modulus-to-noise ratio

Challenges



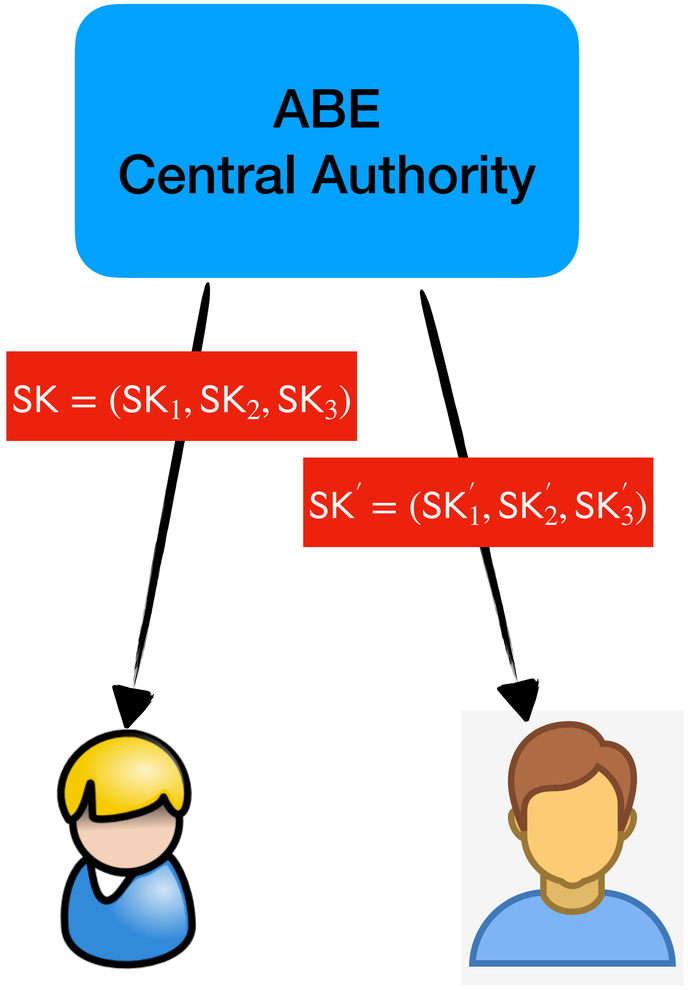
Challenges



Collusion resistance is obtained by using fresh randomness for every SK specific to the user

The components of SK (and SK') are compatible within themselves, but incompatible across sets

Challenges



Collusion resistance is obtained by using fresh randomness for every SK specific to the user

The components of SK (and SK′) are compatible within themselves, but incompatible across sets

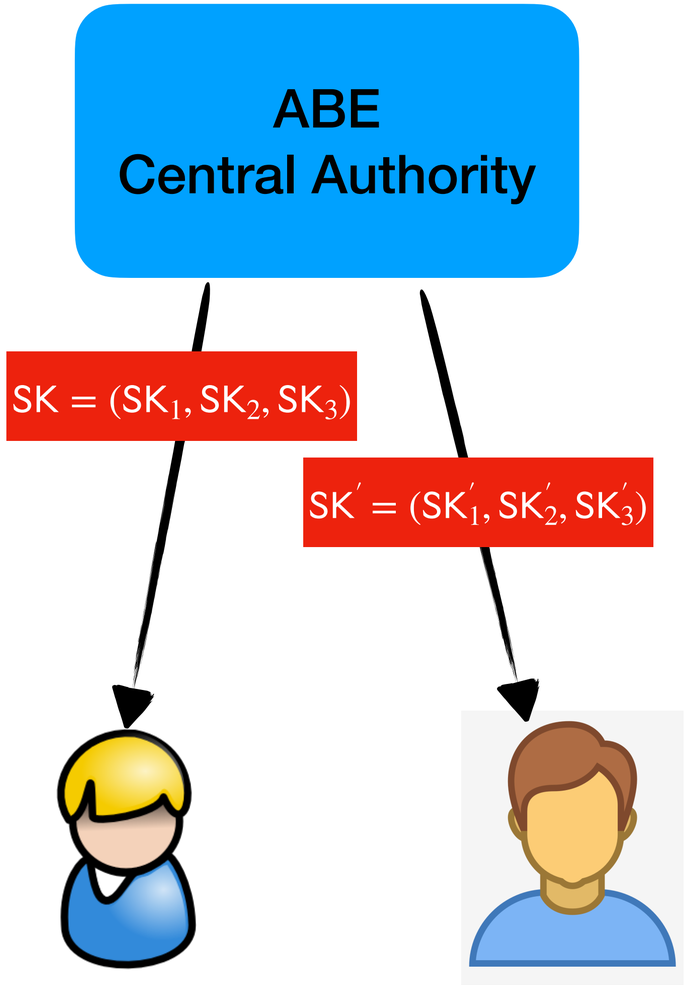
MA challenge 1

The randomness used to tie together different key components for a specific user is obtained from $H(\mathrm{GID})$

Randomness is essentially public

Existing LWE-based CP-ABE schemes fail to satisfy public randomness

Challenges



Collusion resistance is obtained by using fresh randomness for every SK specific to the user

The components of SK (and SK′) are compatible within themselves, but incompatible across sets

MA challenge 1

The randomness used to tie together different key components for a specific user is obtained from $H(\text{GID})$

Randomness is essentially public

Existing LWE-based CP-ABE schemes fail to satisfy public randomness

MA challenge 2

Should support arbitrary authorities joining on the fly

Keys should be “piecewise”. Master PK and user SK should consist of components specific to attributes

Existing LWE-based CP-ABE schemes fail to satisfy modular keys

(Non-Monotone) Linear Secret Sharing Schemes (LSSS)

[Shamir,KW93…]

- A secret sharing scheme where sharing & reconstruction are linear functions

(Non-Monotone) Linear Secret Sharing Schemes (LSSS)

[Shamir,KW93…]

- A secret sharing scheme where sharing & reconstruction are linear functions
- Equivalent to *span programs* (M, ρ)

(Non-Monotone) Linear Secret Sharing Schemes (LSSS)

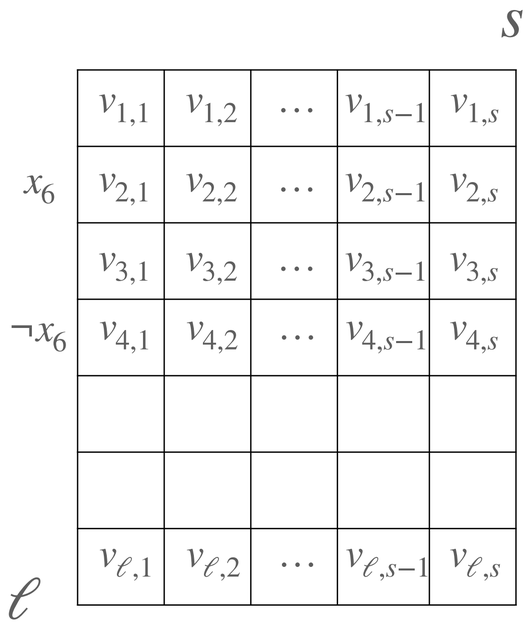
[Shamir,KW93…]

- A secret sharing scheme where sharing & reconstruction are linear functions
- Equivalent to *span programs* (M, ρ)

$$M \in \mathbb{Z}_q^{\ell \times s}$$

$$\rho : [\ell] \mapsto \text{parties} \cup \neg\text{parties}$$

Monotone / non-monotone



Additional Properties of LSSS Used in This Work

- **Small reconstruction coefficients:** Reconstruction of the secret can be done by small coefficients, i.e., coming from $\{0,1\}$.
- **Linear independence for unauthorized rows:** Any unauthorized set of rows of the share generating matrix are linearly independent.

Additional Properties of LSSS Used in This Work

- **Small reconstruction coefficients:** Reconstruction of the secret can be done by small coefficients, i.e., coming from $\{0,1\}$.
- **Linear independence for unauthorized rows:** Any unauthorized set of rows of the share generating matrix are linearly independent.

Theorem:
There exists such a **non-monotone** LSSS* for LOGSPACE
(implicit in GVW13)

Additional Properties of LSSS Used in This Work

- **Small reconstruction coefficients:** Reconstruction of the secret can be done by small coefficients, i.e., coming from $\{0,1\}$.
- **Linear independence for unauthorized rows:** Any unauthorized set of rows of the share generating matrix are linearly independent.

Theorem:
There exists such a **non-monotone** LSSS* for LOGSPACE
(implicit in GVW13)

A different construction for NC1 in the paper

Width of LSSS ≈ policy size

Additional Properties of LSSS Used in This Work

- **Small reconstruction coefficients:** Reconstruction of the secret can be done by small coefficients, i.e., coming from $\{0,1\}$.
- **Linear independence for unauthorized rows:** Any unauthorized set of rows of the share generating matrix are linearly independent.

Agrawal et al. ’20, Lewko-Waters ‘11

Theorem: There exists such a monotone LSSS* for DNFs

Theorem:
There exists such a non-monotone LSSS* for LOGSPACE (implicit in GVW13)

A different construction for NC1 in the paper

Width of LSSS ≈ policy size

Additional Properties of LSSS Used in This Work

- **Small reconstruction coefficients:** Reconstruction of the secret can be done by small coefficients, i.e., coming from $\{0,1\}$.
- **Linear independence for unauthorized rows:** Any unauthorized set of rows of the share generating matrix are linearly independent.

Agrawal et al. ’20, Lewko-Waters ‘11

Theorem: There exists such a monotone LSSS* for DNFs

Theorem:
There exists such a non-monotone LSSS* for LOGSPACE (implicit in GVW13)

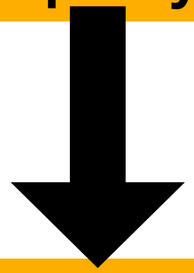
A different construction for NC1 in the paper

Open: such a monotone LSSS for NC1?

Width of LSSS ≈ policy size

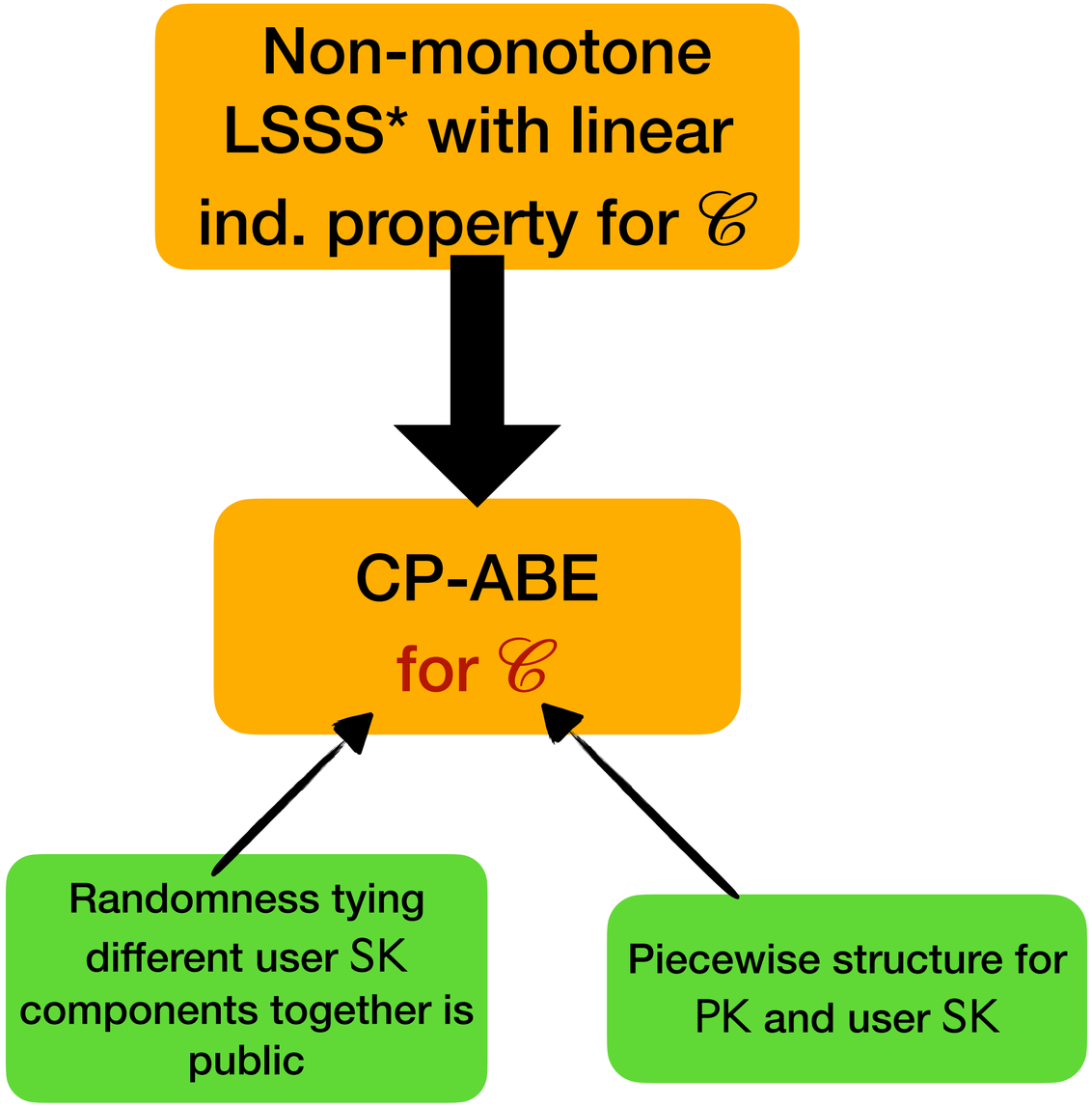
The Recipe

Non-monotone LSSS* with linear ind. property for $\mathscr{C}$

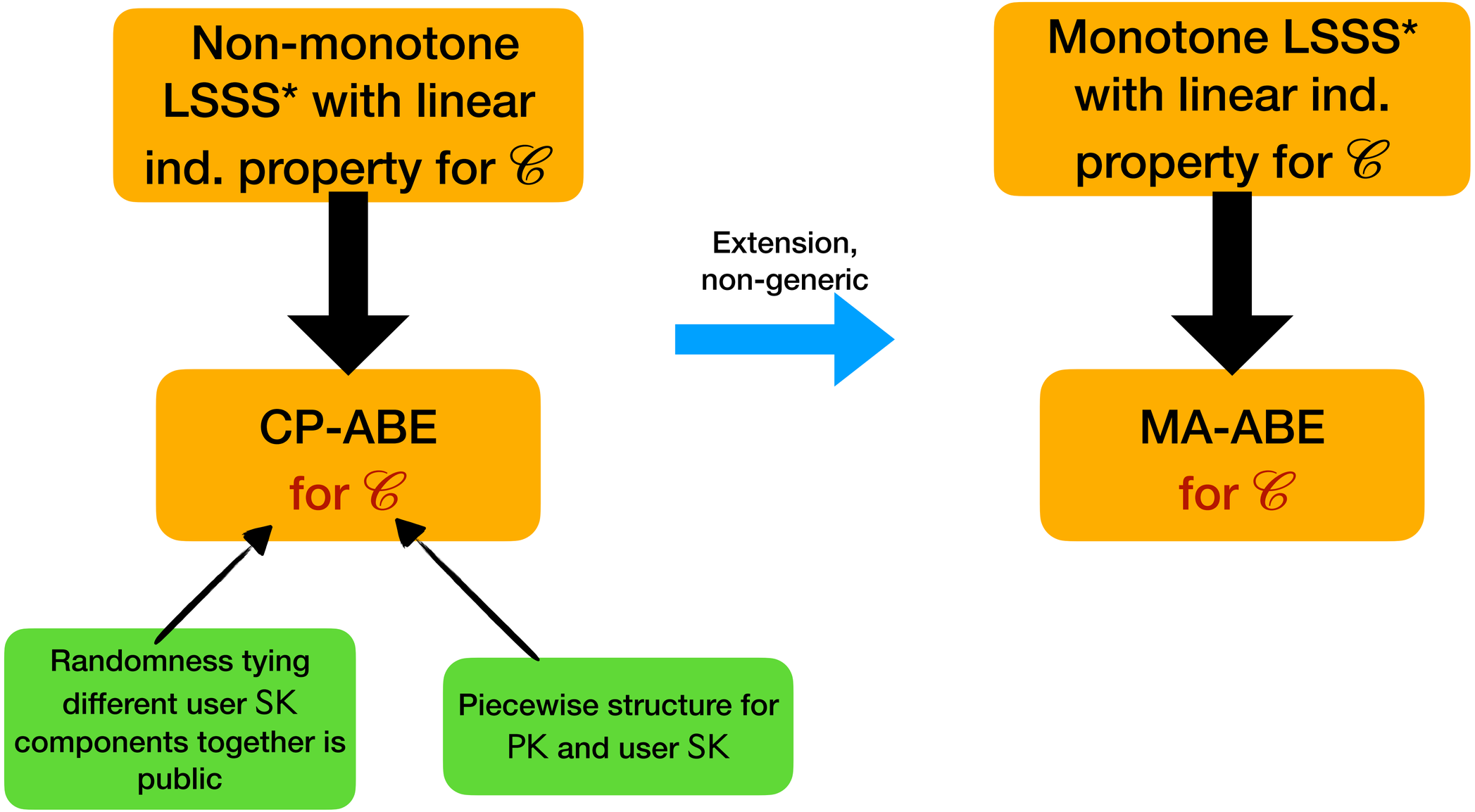


CP-ABE for $\mathscr{C}$

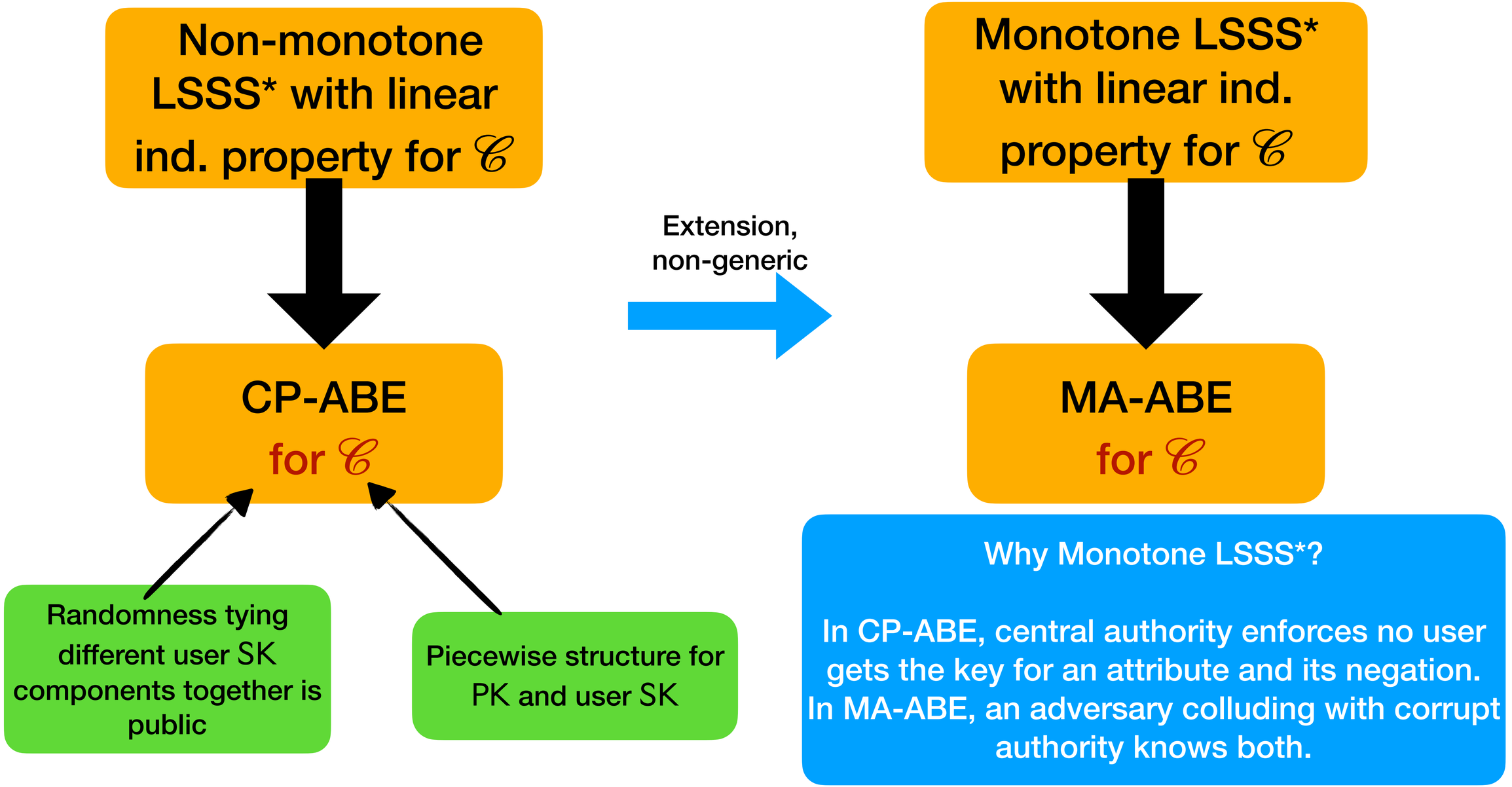
The Recipe


Non-monotone LSSS* with linear ind. property for $\mathscr{C}$
CP-ABE for $\mathscr{C}$
Randomness tying different user SK components together is public
Piecewise structure for PK and user SK

The Recipe


Non-monotone LSSS* with linear ind. property for $\mathscr{C}$
CP-ABE for $\mathscr{C}$
Randomness tying different user SK components together is public
Piecewise structure for PK and user SK
Extension, non-generic
Monotone LSSS* with linear ind. property for $\mathscr{C}$
MA-ABE for $\mathscr{C}$

The Recipe


Non-monotone LSSS* with linear ind. property for $\mathscr{C}$
CP-ABE for $\mathscr{C}$
Randomness tying different user SK components together is public
Piecewise structure for PK and user SK
Extension, non-generic
Monotone LSSS* with linear ind. property for $\mathscr{C}$
MA-ABE for $\mathscr{C}$
Why Monotone LSSS*?
In CP-ABE, central authority enforces no user gets the key for an attribute and its negation.
In MA-ABE, an adversary colluding with corrupt authority knows both.

The CP-ABE Scheme

Setup$(1^\lambda, \mathbb{U})$**:**

For each attribute $u \in \mathbb{U}$, sample

- $\mathbf{A}_u \leftarrow \mathbb{Z}_q^{n \times m}$ together with a trapdoor $\mathbf{A}_u^{-1}$
- $\mathbf{H}_u \leftarrow \mathbb{Z}_q^{n \times m}$

Sample $\mathbf{y} \leftarrow \mathbb{Z}_q^n$

Output:

$$\text{PK} = (\mathbf{y}, \{\mathbf{A}_u\}, \{\mathbf{H}_u\}), \quad \text{MSK} = \{\text{PK}, \mathbf{A}_u^{-1}\}$$

The CP-ABE Scheme

KeyGen(MSK, U**):** // U is a set of attributes

Sample $\hat{\mathbf{t}} \leftarrow \text{noise}^{m-1}$ and set $\mathbf{t} = (1, \hat{\mathbf{t}})$

For each attribute u, sample $\mathbf{k}_u \leftarrow \mathbf{A}_u^{-1}(\mathbf{H}_u \cdot \mathbf{t}^\top)$

Output:

$$\text{SK}_U = (\{\mathbf{k}_u\}, \mathbf{t})$$

$$\text{PK} = (\mathbf{y}, \{\mathbf{A}_u\}, \{\mathbf{H}_u\})$$

$$\text{MSK} = \{\mathbf{A}_u^{-1}\}$$

The CP-ABE Scheme

KeyGen(MSK, U**):** // U is a set of attributes

Sample $\hat{\mathbf{t}} \leftarrow \text{noise}^{m-1}$ and set $\mathbf{t} = (1, \hat{\mathbf{t}})$

For each attribute u, sample $\mathbf{k}_u \leftarrow \mathbf{A}_u^{-1}(\mathbf{H}_u \cdot \mathbf{t}^\top)$

Output:

$$\text{SK}_U = (\{\mathbf{k}_u\}, \mathbf{t})$$

$$\text{PK} = (\mathbf{y}, \{\mathbf{A}_u\}, \{\mathbf{H}_u\})$$

$$\text{MSK} = \{\mathbf{A}_u^{-1}\}$$

$\mathbf{t}$ is the (public) randomness that ties together different key components

The CP-ABE Scheme

KeyGen(MSK, U**):** // U is a set of attributes

Sample $\hat{\mathbf{t}} \leftarrow \text{noise}^{m-1}$ and set $\mathbf{t} = (1, \hat{\mathbf{t}})$

For each attribute u, sample $\mathbf{k}_u \leftarrow \mathbf{A}_u^{-1}(\mathbf{H}_u \cdot \mathbf{t}^\top)$

Output:

$$\text{SK}_U = (\{\mathbf{k}_u\}, \mathbf{t})$$

$$\text{PK} = (\mathbf{y}, \{\mathbf{A}_u\}, \{\mathbf{H}_u\})$$

$$\text{MSK} = \{\mathbf{A}_u^{-1}\}$$

Public nature of randomness is important for MA-ABE

$\mathbf{t}$ is the (public) randomness that ties together different key components

The CP-ABE Scheme

Enc(PK, **msg** $\in \{0,1\}, (M, \rho)$**):**

// $M = \begin{bmatrix} M_1 \\ M_2 \\ \cdots \\ M_\ell \end{bmatrix} \in \mathbb{Z}_q^{\ell \times s}$

Sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{v}_2, \ldots, \mathbf{v}_s \leftarrow \mathbb{Z}_q^m$

Compute:

$$\mathbf{c}_i = \mathbf{s}\mathbf{A}_{\rho(i)} + \text{noise}_i$$

$$\hat{\mathbf{c}}_i = M_i \cdot \begin{bmatrix} \mathbf{s}\mathbf{y}^\top & 0 & \ldots & 0 \\ & \mathbf{v}_2 & & \\ & \mathbf{v}_3 & & \\ & \cdots & & \\ & \mathbf{v}_s & & \end{bmatrix} - \mathbf{s}\mathbf{H}_{\rho(i)} + \hat{\text{noise}}_i$$

Output:

$$\text{CT} = (\{\mathbf{c}_i\}_{i\in[\ell]}, \{\hat{\mathbf{c}}_i\}_{i\in[\ell]}, C = \text{MSB}(\mathbf{s}\mathbf{y}^\top) \oplus \text{msg})$$

$$\text{PK} = (\mathbf{y}, \{\mathbf{A}_u\}, \{\mathbf{H}_u\})$$

$$\text{MSK} = \{\mathbf{A}_u^{-1}\}$$

$$\text{SK}_U = (\{\mathbf{k}_u\}, \mathbf{t})$$

The CP-ABE Scheme

Dec($\mathsf{SK}_U, \mathsf{CT}$**):**

If U does not satisfy (M, ρ), output $\perp$
Else do the following:

I — Indices of rows of M corresponding to available attributes

$\{w_i\}_{i \in I} \in \{0,1\}$ — Reconstruction coefficients

Compute:

$$K' = \sum_{i \in I} w_i (\mathbf{c}_i \mathbf{k}_{\rho(i)}^\top + \hat{\mathbf{c}}_i \mathbf{t}^\top)$$

Output:

$$\mathsf{msg}' = C \oplus \mathsf{MSB}(K')$$

$$\mathsf{PK} = (\mathbf{y}, \{\mathbf{A}_u\}, \{\mathbf{H}_u\})$$

$$\mathsf{MSK} = \{\mathbf{A}_u^{-1}\}$$

$$\mathsf{SK}_U = (\{\mathbf{k}_u\}, \mathbf{t})$$

$$\mathsf{CT} = (\{\mathbf{c}_i\}_{i \in [\ell]}, \{\hat{\mathbf{c}}_i\}_{i \in [\ell]}, C = \mathsf{MSB}(\mathbf{s}\mathbf{y}^\top) \oplus \mathsf{msg})$$

Correctness

(Ignoring small noise-like terms)

$$K' = \sum_{i \in I} w_i (\mathbf{c}_i \mathbf{k}_{\rho(i)}^\top + \hat{\mathbf{c}}_i \mathbf{t}^\top)$$

$$\text{msg}' = C \oplus \text{MSB}(K')$$

$$\mathbf{c}_i \mathbf{k}_{\rho(i)}^\top + \hat{\mathbf{c}}_i \mathbf{t}^\top = \mathbf{s}\mathbf{A}_{\rho(i)} \mathbf{k}_{\rho(i)}^\top + M_i \cdot \begin{bmatrix} \mathbf{s}\mathbf{y}^\top & 0 & \dots & 0 \\ & \mathbf{v}_2 & & \\ & \mathbf{v}_3 & & \\ & \dots & & \\ & \mathbf{v}_s & & \end{bmatrix} \mathbf{t}^\top - \mathbf{s}\mathbf{H}_{\rho(i)} \mathbf{t}^\top$$

Correctness

(Ignoring small noise-like terms)

$$K' = \sum_{i \in I} w_i (\mathbf{c}_i \mathbf{k}_{\rho(i)}^\top + \hat{\mathbf{c}}_i \mathbf{t}^\top)$$

$$\text{msg}' = C \oplus \text{MSB}(K')$$

$$\mathbf{c}_i \mathbf{k}_{\rho(i)}^\top + \hat{\mathbf{c}}_i \mathbf{t}^\top = \mathbf{s}\mathbf{A}_{\rho(i)} \mathbf{k}_{\rho(i)}^\top + M_i \cdot \begin{bmatrix} \mathbf{s}\mathbf{y}^\top & 0 & \dots & 0 \\ & \mathbf{v}_2 & & \\ & \mathbf{v}_3 & & \\ & \dots & & \\ & \mathbf{v}_s & & \end{bmatrix} \mathbf{t}^\top - \mathbf{s}\mathbf{H}_{\rho(i)} \mathbf{t}^\top$$

Recall $\mathbf{A}_{\rho(i)} \mathbf{k}_{\rho(i)}^\top = \mathbf{H}_{\rho(i)} \mathbf{t}^\top$

Correctness

(Ignoring small noise-like terms)

$$K' = \sum_{i \in I} w_i (\mathbf{c}_i \mathbf{k}_{\rho(i)}^\top + \hat{\mathbf{c}}_i \mathbf{t}^\top)$$

$$\text{msg}' = C \oplus \text{MSB}(K')$$

$$\mathbf{c}_i \mathbf{k}_{\rho(i)}^\top + \hat{\mathbf{c}}_i \mathbf{t}^\top = \mathbf{s}\mathbf{A}_{\rho(i)} \mathbf{k}_{\rho(i)}^\top + M_i \cdot \begin{bmatrix} \mathbf{s}\mathbf{y}^\top & 0 & \dots & 0 \\ & \mathbf{v}_2 & & \\ & \mathbf{v}_3 & & \\ & \dots & & \\ & \mathbf{v}_s & & \end{bmatrix} \mathbf{t}^\top - \mathbf{s}\mathbf{H}_{\rho(i)} \mathbf{t}^\top$$

Recall $\mathbf{A}_{\rho(i)} \mathbf{k}_{\rho(i)}^\top = \mathbf{H}_{\rho(i)} \mathbf{t}^\top$

Correctness

(Ignoring small noise-like terms)

$$K' = \sum_{i \in I} w_i (\mathbf{c}_i \mathbf{k}_{\rho(i)}^\top + \hat{\mathbf{c}}_i \mathbf{t}^\top)$$

$$\text{msg}' = C \oplus \text{MSB}(K')$$

$$\mathbf{c}_i \mathbf{k}_{\rho(i)}^\top + \hat{\mathbf{c}}_i \mathbf{t}^\top = \mathbf{s}\mathbf{A}_{\rho(i)} \mathbf{k}_{\rho(i)}^\top + M_i \cdot \begin{bmatrix} \mathbf{s}\mathbf{y}^\top & 0 & \dots & 0 \\ & \mathbf{v}_2 & & \\ & \mathbf{v}_3 & & \\ & \dots & & \\ & \mathbf{v}_s & & \end{bmatrix} \mathbf{t}^\top - \mathbf{s}\mathbf{H}_{\rho(i)} \mathbf{t}^\top$$

Recall $\mathbf{A}_{\rho(i)} \mathbf{k}_{\rho(i)}^\top = \mathbf{H}_{\rho(i)} \mathbf{t}^\top$

Reconstruction gives $\mathbf{s}\mathbf{y}^\top$

Conclusion

- The first MA-ABE for a non-trivial class of access policies from LWE
- A direct LWE-based approach for CP-ABE

Conclusion

- The first MA-ABE for a non-trivial class of access policies from LWE
- A direct LWE-based approach for CP-ABE

Open problems:

- More expressive policies than DNFs
- Better security (we only get static)
- Better parameters (even for CP-ABE)
- Unbounded number of attributes per authority (we only get bounded)

Conclusion

Thank you!

- The first MA-ABE for a non-trivial class of access policies from LWE
- A direct LWE-based approach for CP-ABE

Open problems:

- More expressive policies than DNFs
- Better security (we only get static)
- Better parameters (even for CP-ABE)
- Unbounded number of attributes per authority (we only get bounded)