Systemizing Attribute-Based Encryption – In Search of Practical Decentralized ABE

Marloes Venema, Greg Alpár, Jaap-Henk Hoepman

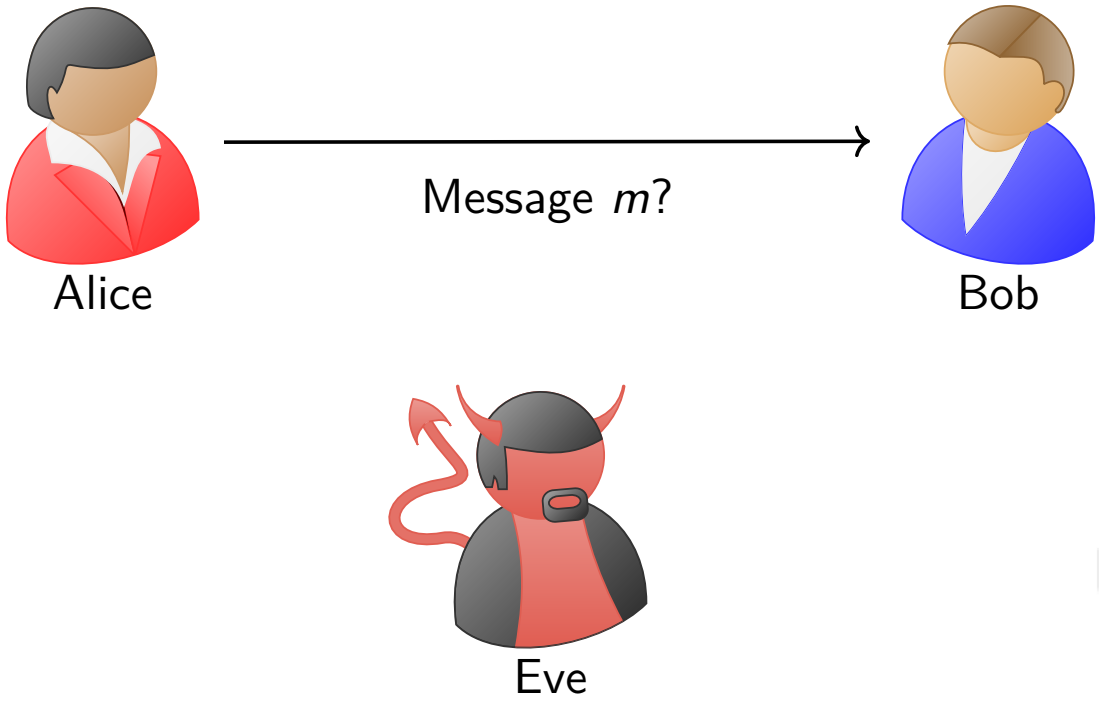
Radboud University, Nijmegen

OUrsi talk September 2020

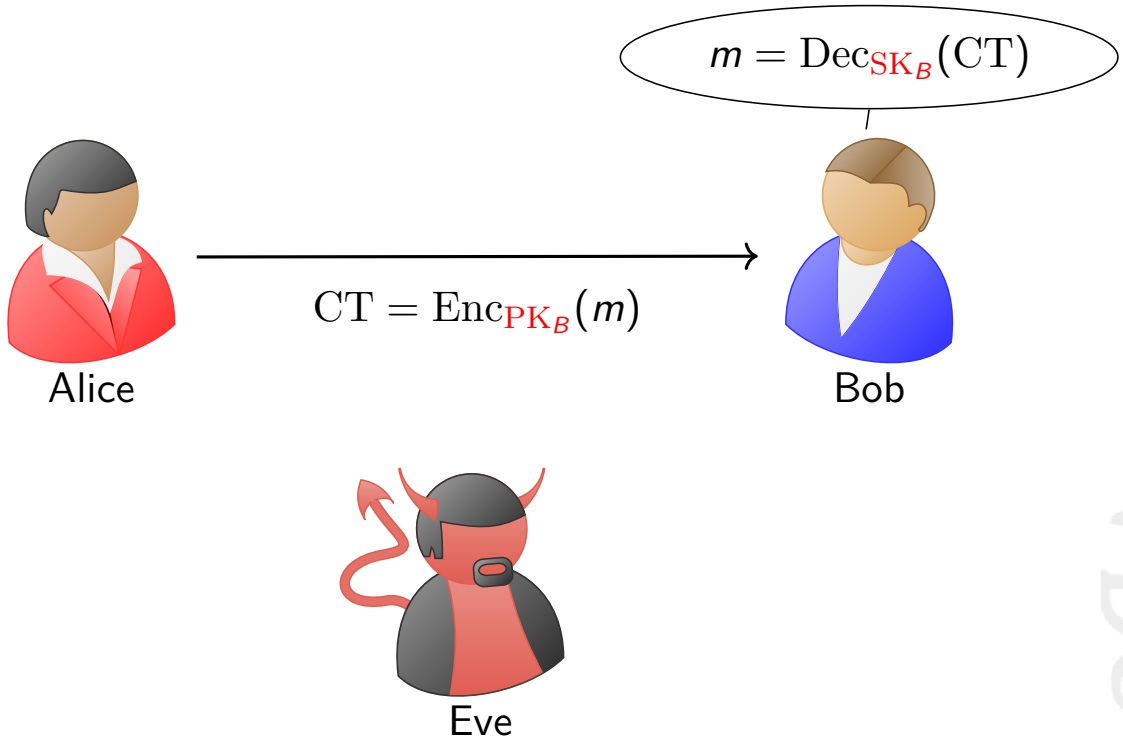
High-level overview

- Introduction to attribute-based encryption
- Motivation to ABE
- Use case: electronic health records
- Properties of ABE
- Open problems

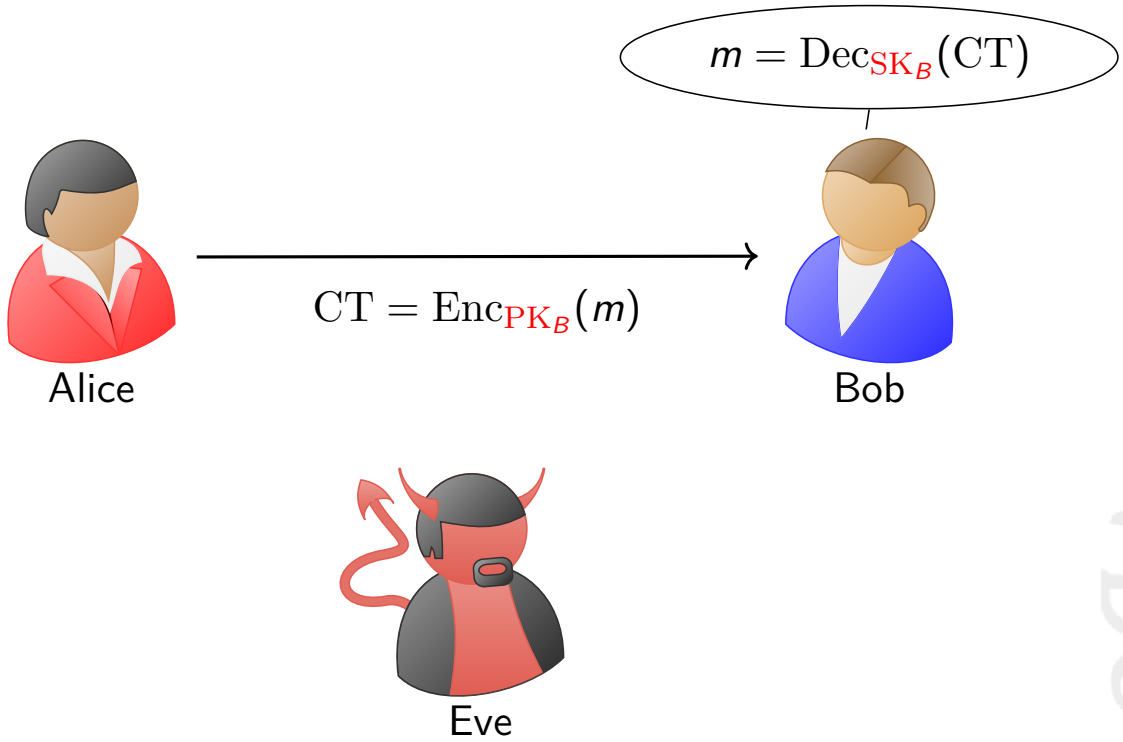
Traditional public-key encryption



Traditional public-key encryption



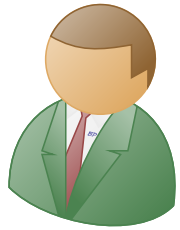
Traditional public-key encryption



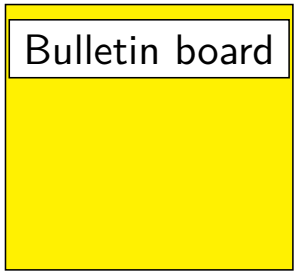
What if Alice wants to send encrypted messages to all people with a name starting with a B?

Attribute-based encryption

Bob

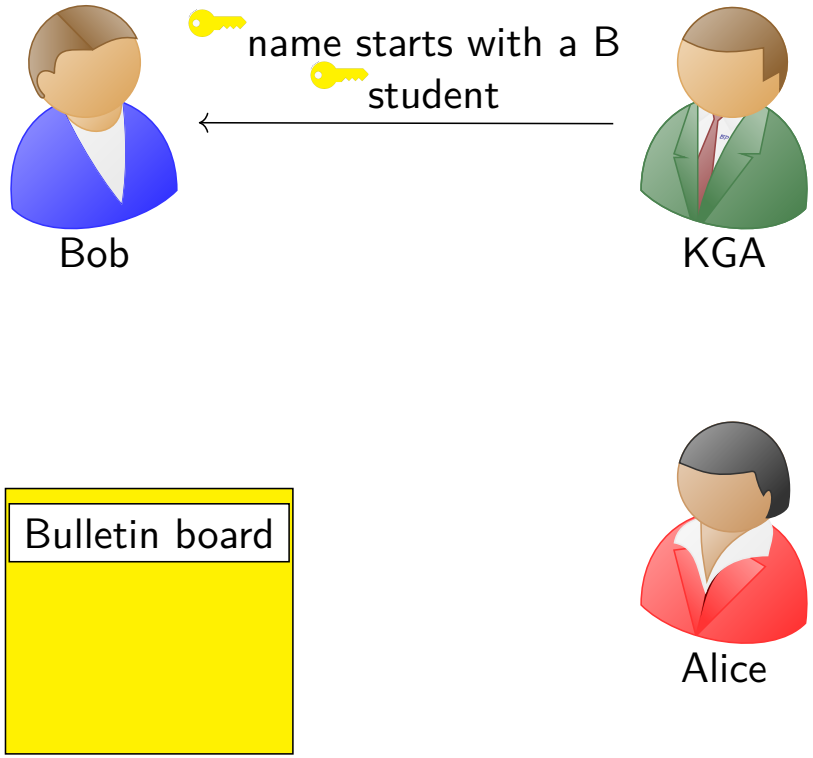


KGA

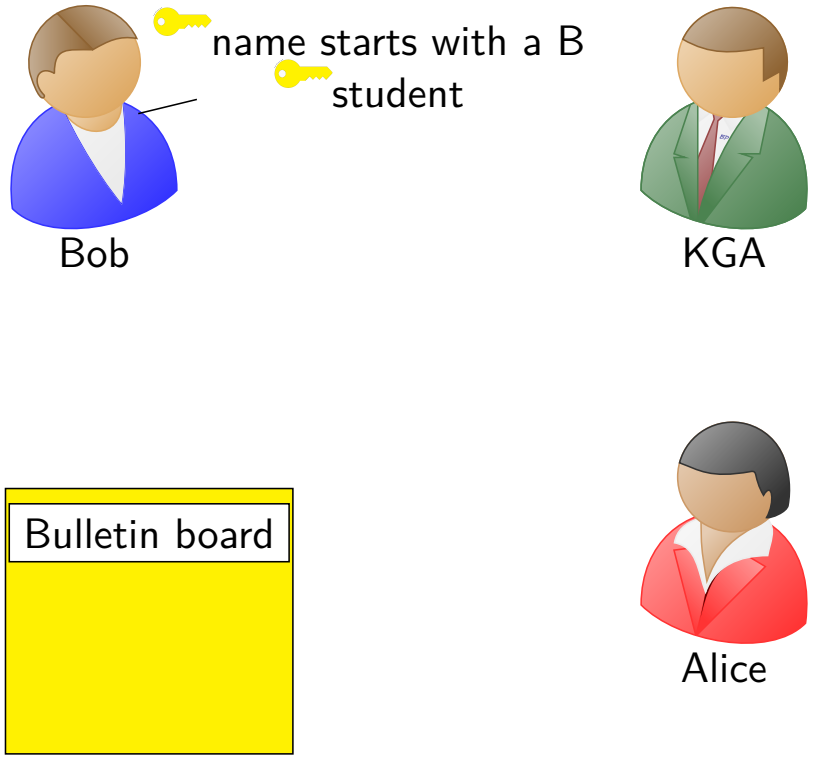


Alice

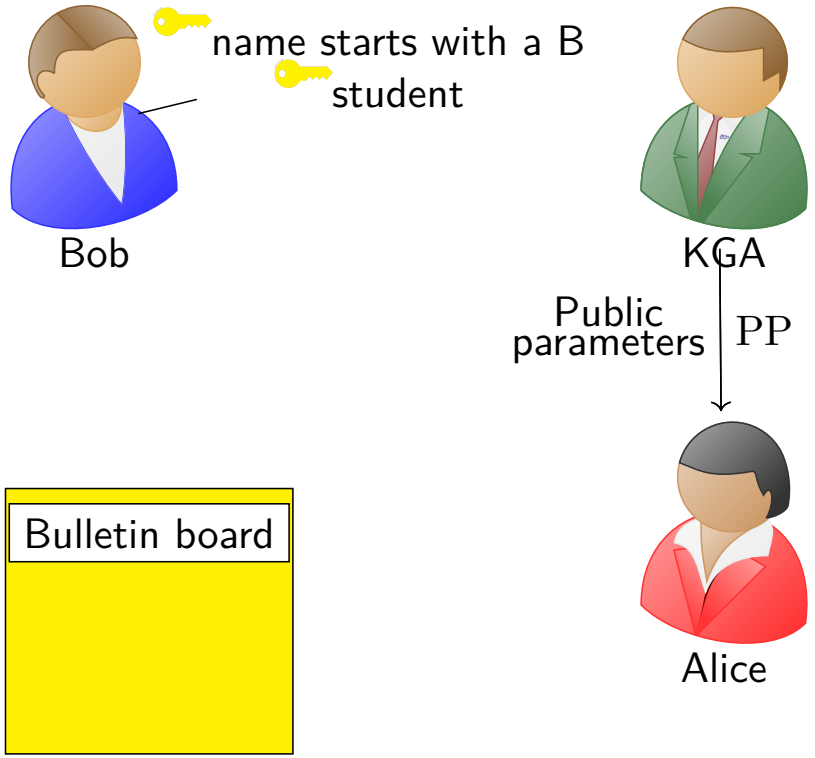
Attribute-based encryption



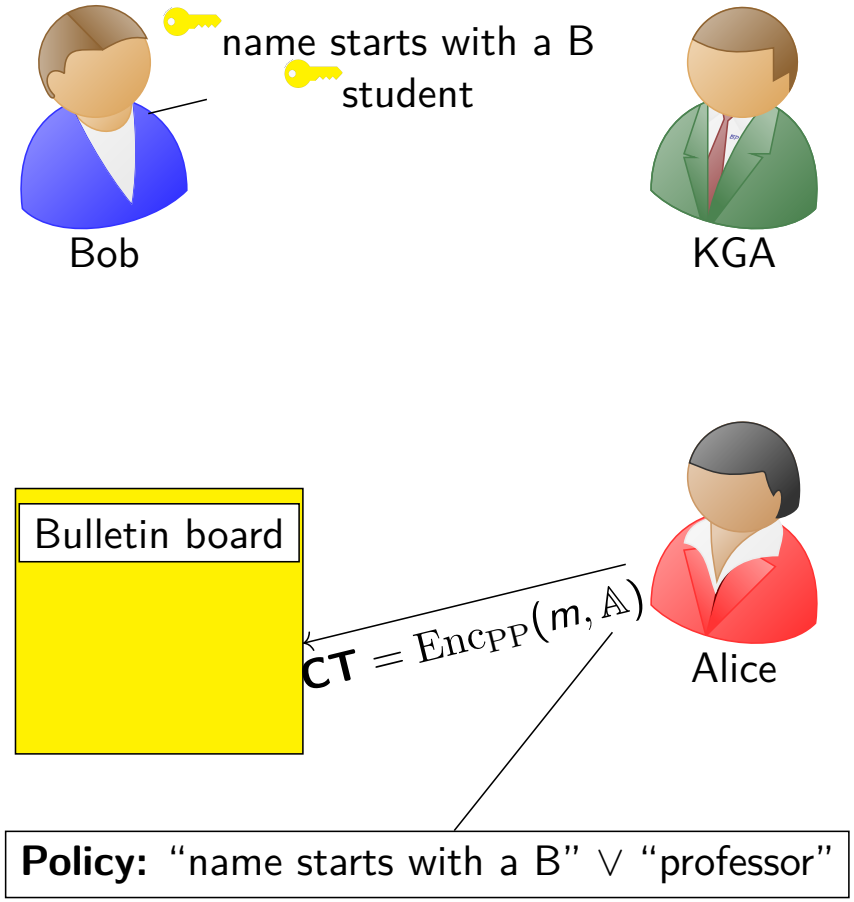
Attribute-based encryption



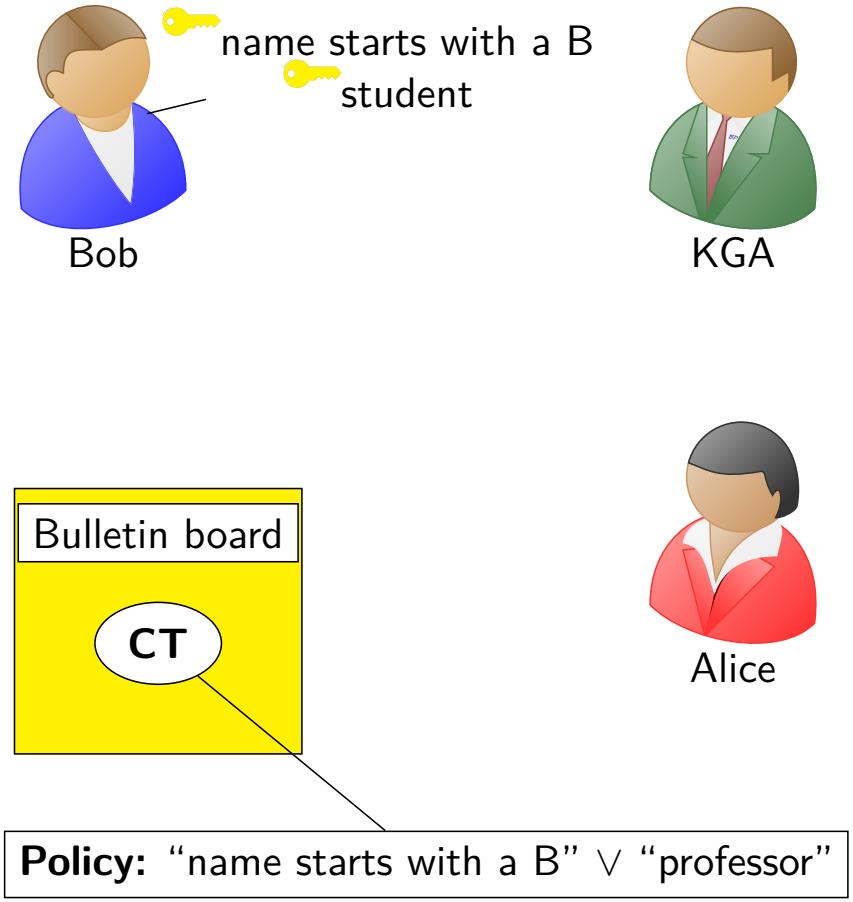
Attribute-based encryption



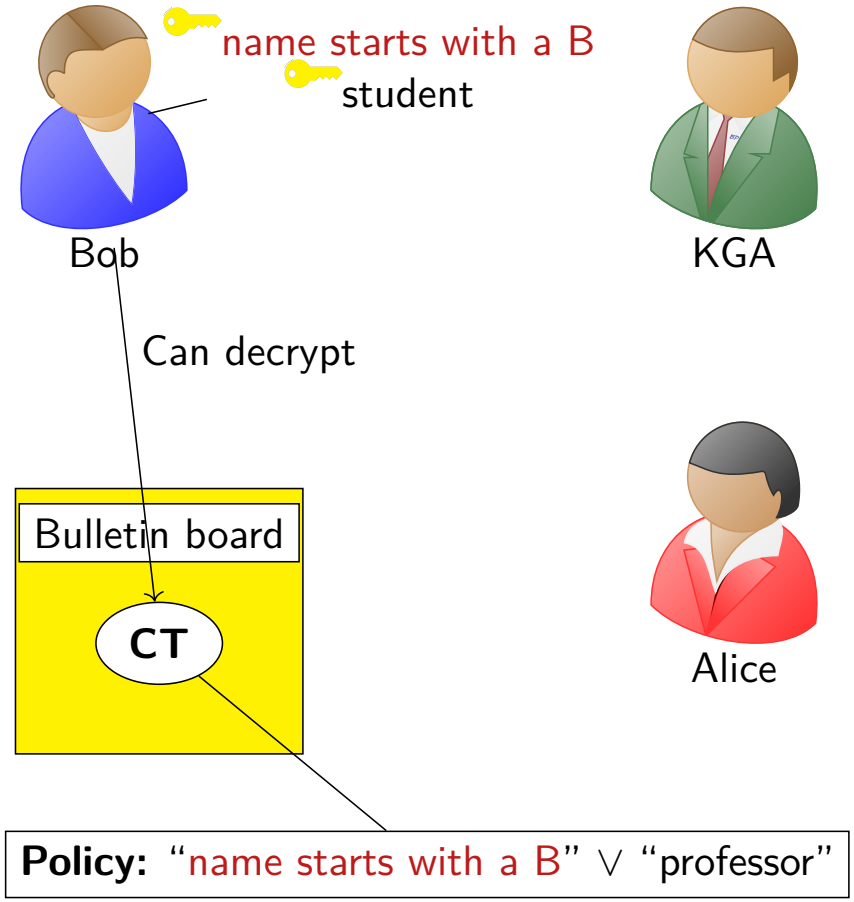
Attribute-based encryption



Attribute-based encryption



Attribute-based encryption



Attribute-based encryption

- Introduced by Sahai and Waters in 2005
- Associates key-pairs with attributes rather than with individual users

Attribute-based encryption

- Introduced by Sahai and Waters in 2005
- Associates key-pairs with attributes rather than with individual users
- More flexible than traditional PKE
- Encrypting user (Alice) can determine which decrypting users (e.g. Bob, Bart) can decrypt based on their attributes, including roles or other features
- Alice doesn't even need to know Bob

Attribute-based encryption

- Introduced by Sahai and Waters in 2005
- Associates key-pairs with attributes rather than with individual users
- More flexible than traditional PKE
- Encrypting user (Alice) can determine which decrypting users (e.g. Bob, Bart) can decrypt based on their attributes, including roles or other features
- Alice doesn't even need to know Bob
- Potentially a nice cryptographic tool for implementing e.g. access control

Definition

Generally, any ABE scheme has four algorithms:

- **Setup:** executed by the key generation authority to generate master public and secret keys

Definition

Generally, any ABE scheme has four algorithms:

- **Setup:** executed by the key generation authority to generate master public and secret keys
- **KeyGen:** key generation algorithm, executed by KGA; creates secret keys for each user with some set of attributes

Definition

Generally, any ABE scheme has four algorithms:

- **Setup:** executed by the key generation authority to generate master public and secret keys
- **KeyGen:** key generation algorithm, executed by KGA; creates secret keys for each user with some set of attributes
- **Encrypt:** encrypts a message under a chosen access policy

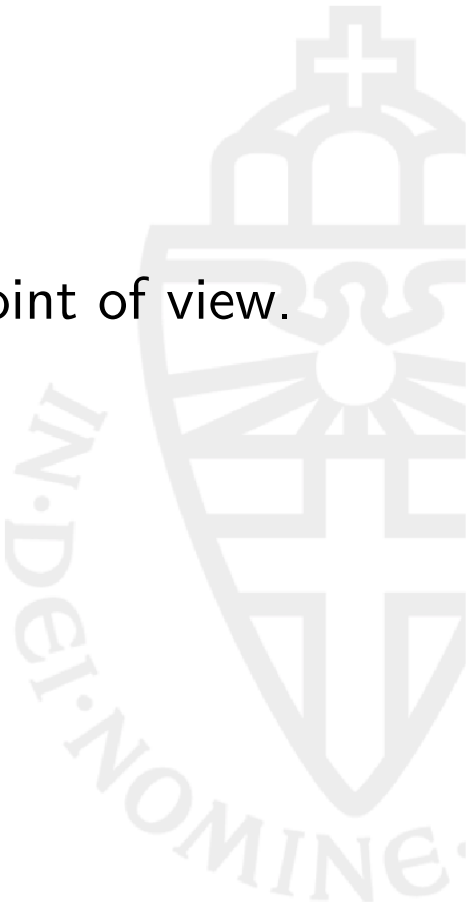
Definition

Generally, any ABE scheme has four algorithms:

- **Setup:** executed by the key generation authority to generate master public and secret keys
- **KeyGen:** key generation algorithm, executed by KGA; creates secret keys for each user with some set of attributes
- **Encrypt:** encrypts a message under a chosen access policy
- **Decrypt:** ciphertext is decrypted if the set associated with the secret key satisfies the access policy

(My) motivation

ABE is interesting from both a theoretical and practical point of view.



(My) motivation

ABE is interesting from both a theoretical and practical point of view.

Theoretical aspects:

- Pairings
- Secret sharing
- Security proofs
- Linear algebra
- And more

(My) motivation

ABE is interesting from both a theoretical and practical point of view.

Theoretical aspects:

- Pairings
- Secret sharing
- Security proofs
- Linear algebra
- And more

$\Rightarrow$

These aspects make ABE

- computationally more expensive than e.g. traditional PKE
- and more difficult to securely design

(My) motivation

ABE is interesting from both a theoretical and practical point of view.

Theoretical aspects:

- Pairings
- Secret sharing
- Security proofs
- Linear algebra
- And more

$\Rightarrow$

These aspects make ABE

- computationally more expensive than e.g. traditional PKE
- and more difficult to securely design

Practical motivation therefore needs to be very strong!

Use case: electronic health records

- Electronic health record (EHR) systems may benefit from the decentralized access control that ABE provides
- While EHRs simplify the sharing of health records across organizations, they also increase the risk of privacy infringements

Use case: electronic health records

- Electronic health record (EHR) systems may benefit from the decentralized access control that ABE provides
- While EHRs simplify the sharing of health records across organizations, they also increase the risk of privacy infringements
- Many privacy-enhancing technologies (PETs) have been proposed to address these privacy concerns
- Most of these include a form of access control on the data by using encryption

Use case: electronic health records

- Electronic health record (EHR) systems may benefit from the decentralized access control that ABE provides
- While EHRs simplify the sharing of health records across organizations, they also increase the risk of privacy infringements
- Many privacy-enhancing technologies (PETs) have been proposed to address these privacy concerns
- Most of these include a form of access control on the data by using encryption
- Keys are often held by the same entity that stores the data, and effectively enforces access control
- This entity needs to be trusted and needs to be online when access is requested
- These approaches are difficult to decentralize

Use case: electronic health records (cont.)

- Suppose Alice wants to share her medical data with her doctor and an employee at her insurance company
- She could specify an access policy, e.g. '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'

Use case: electronic health records (cont.)

- Suppose Alice wants to share her medical data with her doctor and an employee at her insurance company
- She could specify an access policy, e.g. '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'
- Assume that the hospital server stores the data and enforces access control to these data
- A VGZ actuary can request access by contacting the hospital server

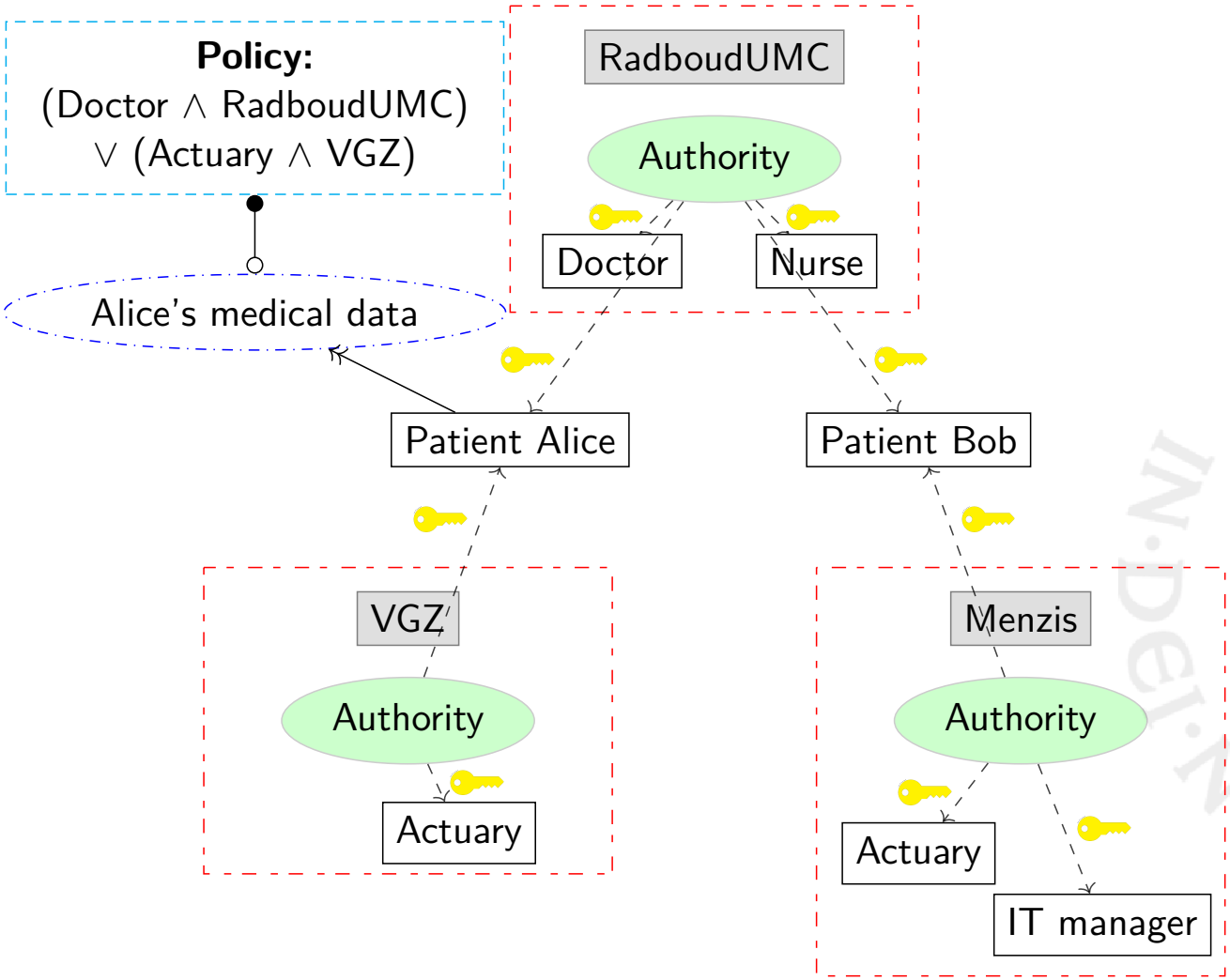
Use case: electronic health records (cont.)

- Suppose Alice wants to share her medical data with her doctor and an employee at her insurance company
- She could specify an access policy, e.g. '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'
- Assume that the hospital server stores the data and enforces access control to these data
- A VGZ actuary can request access by contacting the hospital server
- The server then checks whether the requesting user is authorized with respect to the policy
- and ideally only needs to contact some authority at VGZ to verify that the user is an actuary at VGZ

Use case: electronic health records (cont.)

- Suppose Alice wants to share her medical data with her doctor and an employee at her insurance company
- She could specify an access policy, e.g. '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'
- Assume that the hospital server stores the data and enforces access control to these data
- A VGZ actuary can request access by contacting the hospital server
- The server then checks whether the requesting user is authorized with respect to the policy
- and ideally only needs to contact some authority at VGZ to verify that the user is an actuary at VGZ
- Traditionally, to handle an access request, both entities need to be online

EHRs and ABE


Policy:
(Doctor ∧ RadboudUMC)
∨ (Actuary ∧ VGZ)
Alice's medical data
RadboudUMC
Authority
Doctor
Nurse
Patient Alice
Patient Bob
VGZ
Authority
Actuary
Menzis
Authority
Actuary
IT manager

EHRs and ABE (cont.)

- Using ABE would provide some interesting benefits in this setting
- The data does not need to be stored by the hospital server, but can be stored externally

EHRs and ABE (cont.)

- Using ABE would provide some interesting benefits in this setting
- The data does not need to be stored by the hospital server, but can be stored externally
- Access control can be simultaneously enforced by RadboudUMC **and** VGZ by using decentralized ABE
- Alice can encrypt the data by using attributes managed by the RadboudUMC and VGZ authorities

EHRs and ABE (cont.)

- Using ABE would provide some interesting benefits in this setting
- The data does not need to be stored by the hospital server, but can be stored externally
- Access control can be simultaneously enforced by RadboudUMC **and** VGZ by using decentralized ABE
- Alice can encrypt the data by using attributes managed by the RadboudUMC and VGZ authorities
- Once they have received keys for their attributes, VGZ actuaries can independently decrypt the ciphertext (and therefore access the data)
- They don't need to interact with the VGZ authority for each access request
- Furthermore, they don't need to interact with the RadboudUMC authority at all

Practical motivation: privacy-friendly access control

- ABE cryptographically implements a fine-grained access control on data
- Data can be securely stored by an entity that is not trusted to access the data by using ABE

Practical motivation: privacy-friendly access control

- ABE cryptographically implements a fine-grained access control on data
- Data can be securely stored by an entity that is not trusted to access the data by using ABE
- Instead, access control can be enforced by an external trusted third party (i.e. the key generation authority)
- Main advantage of ABE over other cryptographic primitives: trusted party does not need to be online for each access request

Practical motivation: privacy-friendly access control

- ABE cryptographically implements a fine-grained access control on data
- Data can be securely stored by an entity that is not trusted to access the data by using ABE
- Instead, access control can be enforced by an external trusted third party (i.e. the key generation authority)
- Main advantage of ABE over other cryptographic primitives: trusted party does not need to be online for each access request
- As such, users are much less dependent on the availability of this party
- Additionally, some variants of ABE can implement decentralized access control (like in the example)
- This makes ABE especially attractive compared to other solutions

Practical ABE

- There are various variants of ABE with many different properties
- Not all of them are practical

Practical ABE

- There are various variants of ABE with many different properties
- Not all of them are practical
- As already mentioned, some variants are decentralized (while most employ a single key generation authority)
- Sometimes, the amount of attributes that can be used is bounded after the setup

Practical ABE

- There are various variants of ABE with many different properties
- Not all of them are practical
- As already mentioned, some variants are decentralized (while most employ a single key generation authority)
- Sometimes, the amount of attributes that can be used is bounded after the setup
- The policies can be enforced on the keys, rather than the ciphertexts
- The expressivity of the access policies can be rather limited

Practical ABE

- There are various variants of ABE with many different properties
- Not all of them are practical
- As already mentioned, some variants are decentralized (while most employ a single key generation authority)
- Sometimes, the amount of attributes that can be used is bounded after the setup
- The policies can be enforced on the keys, rather than the ciphertexts
- The expressivity of the access policies can be rather limited
- There are various levels of security (e.g. which model and complexity assumption are used in the proof, whether random oracles are required, etc.)
- And much more (i.e. at least 19 properties in total)

Practical ABE

- There are various variants of ABE with many different properties
- Not all of them are practical
- As already mentioned, some variants are decentralized (while most employ a single key generation authority)
- Sometimes, the amount of attributes that can be used is bounded after the setup
- The policies can be enforced on the keys, rather than the ciphertexts
- The expressivity of the access policies can be rather limited
- There are various levels of security (e.g. which model and complexity assumption are used in the proof, whether random oracles are required, etc.)
- And much more (i.e. at least 19 properties in total)

Collusion resistance

- In (all variants of) ABE, users are not allowed to collude
- If two or more users cannot individually decrypt a ciphertext, then together they shouldn't be able to do this either

Collusion resistance

- In (all variants of) ABE, users are not allowed to collude
- If two or more users cannot individually decrypt a ciphertext, then together they shouldn't be able to do this either
- For instance, consider the policy in our example: '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'

Collusion resistance

- In (all variants of) ABE, users are not allowed to collude
- If two or more users cannot individually decrypt a ciphertext, then together they shouldn't be able to do this either
- For instance, consider the policy in our example: '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'
- Then some Menzis actuary should not be able to decrypt a ciphertext encrypted under this policy

Collusion resistance

- In (all variants of) ABE, users are not allowed to collude
- If two or more users cannot individually decrypt a ciphertext, then together they shouldn't be able to do this either
- For instance, consider the policy in our example: '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'
- Then some Menzis actuary should not be able to decrypt a ciphertext encrypted under this policy
- Neither does a VGZ IT manager

Collusion resistance

- In (all variants of) ABE, users are not allowed to collude
- If two or more users cannot individually decrypt a ciphertext, then together they shouldn't be able to do this either
- For instance, consider the policy in our example: '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'
- Then some Menzis actuary should not be able to decrypt a ciphertext encrypted under this policy
- Neither does a VGZ IT manager
- So, together, they shouldn't be able to decrypt it either (even though together they have the attributes 'actuary' and 'VGZ', which satisfies the policy)

Collusion resistance (cont.)

- In traditional PKE such as ElGamal there's no concept of collusion $\rightarrow$ attacker only has access to ciphertexts
- In ABE, attacker has access to ciphertexts, but also possibly some (unauthorized) keys, e.g. can the keys be combined to decrypt more ciphertexts?

Collusion resistance (cont.)

- In traditional PKE such as ElGamal there's no concept of collusion $\rightarrow$ attacker only has access to ciphertexts
- In ABE, attacker has access to ciphertexts, but also possibly some (unauthorized) keys, e.g. can the keys be combined to decrypt more ciphertexts?
- $\rightarrow$ we need security assumptions for the ciphertexts **and** secret keys
- To this end, both are represented by group elements, but then we can't perform ElGamal-like decryption

Collusion resistance (cont.)

- In traditional PKE such as ElGamal there's no concept of collusion $\rightarrow$ attacker only has access to ciphertexts
- In ABE, attacker has access to ciphertexts, but also possibly some (unauthorized) keys, e.g. can the keys be combined to decrypt more ciphertexts?
- $\rightarrow$ we need security assumptions for the ciphertexts **and** secret keys
- To this end, both are represented by group elements, but then we can't perform ElGamal-like decryption
- Decryption uses a pairing operation

Pairings

- Let $\mathbb{G}, \mathbb{H}, \mathbb{G}_T$ be three groups of prime order p, where $g \in \mathbb{G}, h \in \mathbb{H}$ are generator
- A pairing is a mapping $e : \mathbb{G} \times \mathbb{H} \rightarrow \mathbb{G}_T$ such that
  - For all $a, b \in \mathbb{Z}_p$ holds that $\boxed{e(g^a, h^b) = e(g, h)^{ab}}$ and
  - $e(g, h) \neq 1_{\mathbb{G}_T}$

Pairings

- Let $\mathbb{G}, \mathbb{H}, \mathbb{G}_T$ be three groups of prime order p, where $g \in \mathbb{G}, h \in \mathbb{H}$ are generator
- A pairing is a mapping $e : \mathbb{G} \times \mathbb{H} \rightarrow \mathbb{G}_T$ such that
  - For all $a, b \in \mathbb{Z}_p$ holds that $\boxed{e(g^a, h^b) = e(g, h)^{ab}}$ and
  - $e(g, h) \neq 1_{\mathbb{G}_T}$
- Basically, we perform an ElGamal-like 'exponentiation' (e.g. $(g^a)^b$) but with pairings
- There exist various groups and pairings with varying levels of efficiency

Pairings

- Let $\mathbb{G}, \mathbb{H}, \mathbb{G}_T$ be three groups of prime order p, where $g \in \mathbb{G}, h \in \mathbb{H}$ are generator
- A pairing is a mapping $e : \mathbb{G} \times \mathbb{H} \rightarrow \mathbb{G}_T$ such that
  - For all $a, b \in \mathbb{Z}_p$ holds that $\boxed{e(g^a, h^b) = e(g, h)^{ab}}$ and
  - $e(g, h) \neq 1_{\mathbb{G}_T}$
- Basically, we perform an ElGamal-like 'exponentiation' (e.g. $(g^a)^b$) but with pairings
- There exist various groups and pairings with varying levels of efficiency
- Generally, exponentiations in $\mathbb{G}$ are cheaper than those in $\mathbb{H}$ and $\mathbb{G}_T$
- and exponentiations are cheaper than pairing operations

Pairings

- Let $\mathbb{G}, \mathbb{H}, \mathbb{G}_T$ be three groups of prime order p, where $g \in \mathbb{G}, h \in \mathbb{H}$ are generator
- A pairing is a mapping $e : \mathbb{G} \times \mathbb{H} \rightarrow \mathbb{G}_T$ such that
  - For all $a, b \in \mathbb{Z}_p$ holds that $\boxed{e(g^a, h^b) = e(g, h)^{ab}}$ and
  - $e(g, h) \neq 1_{\mathbb{G}_T}$
- Basically, we perform an ElGamal-like 'exponentiation' (e.g. $(g^a)^b$) but with pairings
- There exist various groups and pairings with varying levels of efficiency
- Generally, exponentiations in $\mathbb{G}$ are cheaper than those in $\mathbb{H}$ and $\mathbb{G}_T$
- and exponentiations are cheaper than pairing operations
- As such, efficiency of a scheme is determined by the groups in which the key and ciphertext components live
- Remarkably, little to no research has been done in an accurate efficiency analysis of ABE. Most works treat efficiency very naively

Multi-authority ABE

- ABE requires a key generation authority (KGA) to generate the secret keys
- This entity can decrypt every ciphertext and needs to be trusted

Multi-authority ABE

- ABE requires a key generation authority (KGA) to generate the secret keys
- This entity can decrypt every ciphertext and needs to be trusted
- Multi-authority (MA) ABE mitigates this issue by employing multiple KGAs
- Each KGA can securely manage its own (unique) set of attributes

Multi-authority ABE

- ABE requires a key generation authority (KGA) to generate the secret keys
- This entity can decrypt every ciphertext and needs to be trusted
- Multi-authority (MA) ABE mitigates this issue by employing multiple KGAs
- Each KGA can securely manage its own (unique) set of attributes
- MA-ABE requires security against corruption
- That is, even if some authorities are corrupt, the scheme still provides security with respect to the honest authorities

Multi-authority ABE

- ABE requires a key generation authority (KGA) to generate the secret keys
- This entity can decrypt every ciphertext and needs to be trusted
- Multi-authority (MA) ABE mitigates this issue by employing multiple KGAs
- Each KGA can securely manage its own (unique) set of attributes
- MA-ABE requires security against corruption
- That is, even if some authorities are corrupt, the scheme still provides security with respect to the honest authorities
- As such, authorities do not need to trust one another
- We have identified that there exist two types of MA-ABE: distributed and decentralized

Decentralized ABE

- Consider again the electronic health record example with the policy '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'
- During an access request, the authority ideally only needs to check with the *relevant* authorities whether the requesting user satisfies it

Decentralized ABE

- Consider again the electronic health record example with the policy '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'
- During an access request, the authority ideally only needs to check with the *relevant* authorities whether the requesting user satisfies it
- So, after the server has confirmed the user is a VGZ actuary, it does not need to check with the hospital whether the user is a doctor
- In some MA-ABE, a user with attributes 'actuary' and 'VGZ' can decrypt the ciphertext without requiring keys from the RadboudUMC's KGA

Decentralized ABE

- Consider again the electronic health record example with the policy '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'
- During an access request, the authority ideally only needs to check with the *relevant* authorities whether the requesting user satisfies it
- So, after the server has confirmed the user is a VGZ actuary, it does not need to check with the hospital whether the user is a doctor
- In some MA-ABE, a user with attributes 'actuary' and 'VGZ' can decrypt the ciphertext without requiring keys from the RadboudUMC's KGA
- We call MA-ABE schemes that satisfy that property *decentralized*
- However, not all MA-ABE schemes have this property

Decentralized ABE

- Consider again the electronic health record example with the policy '(doctor $\wedge$ RadboudUMC) $\vee$ (actuary $\wedge$ VGZ)'
- During an access request, the authority ideally only needs to check with the *relevant* authorities whether the requesting user satisfies it
- So, after the server has confirmed the user is a VGZ actuary, it does not need to check with the hospital whether the user is a doctor
- In some MA-ABE, a user with attributes 'actuary' and 'VGZ' can decrypt the ciphertext without requiring keys from the RadboudUMC's KGA
- We call MA-ABE schemes that satisfy that property *decentralized*
- However, not all MA-ABE schemes have this property
- Rather, they need keys from all authorities, regardless of whether they have attributes managed by that authority
- We call these schemes *distributed*

Existing work

Scheme	Based on	KP/CP	Expr.	LU	Bounded	RFI	Prime	Type	CS-CT	CP-D	Model	CCA*	Assump.	ROM	MA-ABE	On/off	Revoc.	A-H	Out. dec.	Trace.
SW05 [98] I	-	KP	T	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	$\checkmark_V$	Static	✗	✗	✗	✗	✗	✗	✗
SW05 [98] II	-	KP	T	✓	LU	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
GPSW06 [52] I	[98] I	KP	MSP	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	$\checkmark_V$	Static	✗	✗	✗	✗	✗	✗	✗
GPSW06 [52] II	[98] II	KP	MSP	✓	LU	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
Cha07 [27] I	[98] I	KP	MA-T	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	$\checkmark_V$	Static	✗	◑	✗	✗	✗	✗	✗
Cha07 [27] II	[52] II	KP	MA-MSP	✓	LU	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	Static	✗	◑	✗	✗	✗	✗	✗
BSW07 [18]	[52] II	CP	MSP	✓	LU	✓	✓	I	✗	✗	◑	$\checkmark_{D,V}$	GGM	✗	✗	✗	✗	✗	✗	✗
CN07 [37]	[52] I	KP*	AND	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	✓	Static	✗	✗	✗	✗	✗	✗	✗
OSW07 [87]	[52] II	KP	NMSP	✓	LU	✗	✓	I	✗	✗	◑	$\checkmark_V$	Static	✗	✗	✗	✗	✗	✗	✗
NYO08 [82] I	[37] I	KP*	AND	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	$\checkmark_V$	Static	✗	✗	✗	✗	✓	✗	✗
NYO08 [82] II	[18]	CP	AND	✗	$\|\mathcal{U}\|$	✓	✓	II	✗	✗	◑	$\checkmark_{D,V}$	GGM	✗	✗	✗	✗	✓	✗	✗
CC09 [28]	[27]	KP	MA-T	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	$\checkmark_V$	$q(\|\mathcal{A}\|)$	✗	◑	✗	✗	✗	✗	✗
YWRL10 [115]	[37] I	KP*	AND	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	✓	Static	✗	✗	✗	✓	✗	✗	✗
HLR10 [56]	-	CP	T	✗	$\|\mathcal{U}\|$	✓	✓	I	✓	✓	◑	✗	$q(\|\mathcal{U}\|)$	✗	✗	✗	✗	✗	✗	✗
LOSTW10 [66]	[110]	CP	MSP	✓	LU,OU	✗	✗	I	✗	✗	●	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
OT10 [84]	[66]	KP,CP	NMSP	✓	OU,$\|\mathcal{A}\|$	✓	✓	III	✗	✗	●	✓	Static	✗	✗	✗	✗	✗	✗	✗
Wat11 [111] I	[66]	CP	MSP	✓	LU	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✗	✗	✗	✗	✗
Wat11 [111] II	[66]	CP	MSP	✓	LU,OU	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	$q(\mathrm{AND})$	✗	✗	✗	✗	✗	✗	✗
Wat11 [111] III	[66]	CP	MSP	✓	LU,OU	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
LHCC+11 [72]	[28, 82]	KP*	AND	✗	$\|\mathcal{U}\|$	✗	✓	II	✗	✗	◑	$\checkmark_V$	$q(\|\mathcal{A}\|)$	✗	◑	✗	✗	✓	✗	✓
LW11 [68] I	[66]	CP	MSP	✗	$\|\mathcal{U}\|$,OU	✗	✗	I	✗	✗	●	✗	Static	✓	●	✗	✗	✗	✗	✗
LW11 [67] II	[66]	CP	MSP	✗	$\|\mathcal{U}\|$,OU	✗	✓	I	✗	✗	◑	✗	GGM	✓	●	✗	✗	✗	✗	✗
LW11b [69]	[66]	KP	MSP	✓	-	✗	✗	I	✗	✗	◑	$\checkmark_{D,V}$	Static	✗	✗	✓	✗	✗	✗	✗
GHW11 [54] I	[111]	CP	MSP	✓	LU	✓	✓	I	✗	✓	◑	RCCA	$q(\|\mathcal{A}\|)$	✓	✗	✗	✗	✗	✓	✗
GHW11 [54] II	[52]	KP	MSP	✓	LU	✓	✓	I	✗	✓	◑	RCCA	Static	✓	✗	✗	✗	✗	✓	✗
LCHWY11 [75]	[66]	CP	MSP	✗	$\|\mathcal{U}\|$	✗	✗	I	✗	✗	●	$\checkmark_{D,V}$	Static	✗	◑	✗	✗	✗	✗	✗
LW12 [70]	[66]	CP	MSP	✓	LU	✗	✗	I	✗	✗	●	$\checkmark_{D,V}$	$q(\mathrm{AND})$	✗	✗	✗	✗	✗	✗	✗
SSW12 [97]	[66]	KP,CP	MSP	✓	LU,OU	✗	✗	I	✗	✗	●	✗	Static	✗	✗	✗	✓	✗	✗	✗
OT12 [85]	[84]	KP,CP	NMSP	✓	-	✓	✓	III	✗	✗	●	$\checkmark_V$	Static	✗	✗	✓	✗	✗	✗	✗
HW13 [58]	[52] II	KP	MSP	✗	$\|\mathcal{U}\|$	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	$q(\|\mathcal{U}\|)$	✗	✗	✗	✗	✗	✗	✗
CCLZ+13 [30]	[49]	KP	T	✓	LU	✓	✗	I	✓	✓	●	✗	Static	✗	✗	✗	✗	✗	✗	✗
OT13 [86]	[84]	KP,CP	NMSP	✓	$\|\mathcal{U}\|$,$\|\mathcal{A}\|$	✓	✓	III	✗	✗	●	$\checkmark_{D,V}$	Static	✓	●	✓	✗	✗	✗	✗
LCLJ+13 [71]	[98]	KP	T	✓	LU	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	Static	✗	✗	✗	✓	✗	✓	✗
RW13 [95]	[69]	KP,CP	MSP	✓	-	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✓	✗	✗	✗	✗
LCW13 [76]	[48, 70]	CP	MSP	✓	LU	✗	✗	I	✗	✗	●	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✗	✗	✗	✗	✓
HW14 [59]	[95]	KP,CP	MSP	✓	-	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✓	✗	✗	✗	✗
NCDWL14 [83]	[95]	CP	MSP	✓	-	✓	✓	I	✗	✗	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✓	✗	✗	✗	✓
KL15 [64]	[66]	KP	MSP	✗	$\log\|\mathcal{U}\|$	✗	✗	I	✗	✗	●	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
RW15 [96]	[68]	CP	MSP	✓	LU	✗	✓	I	✗	✗	◑	✗	$q(\|\mathcal{A}\|)$	✓	●	✗	✗	✗	✗	✗
LW15 [77]	[76, 95]	CP	MSP	✓	-	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✓	✓	✗	✗	✗	✓
ZGTC+16 [116] I	[33, 105]	KP	MSP	✗	$\|\mathcal{U}\|$	✓	✓	III	✓	✓	◕	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
ZGTC+16 [116] II	[33, 105]	KP	MSP	✓	$\|\mathcal{S}\|$	✓	✓	III	✓	✓	◕	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
AHMTY16 [14]	[10, 69]	KP	MSP	✓	-	✗	✗	III	✓	✓	●	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✗	✗	✗	✗	✗
CDLQ16 [40]	[95]	CP	MSP	✓	-	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✓	✓	✗	✓	✗
MST17 [78] I	[58]	CP	DNF	✓	LU,OU	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✗	✗	✗	✗	✗
AC17 [5]	[31]	KP,CP	MSP	✓	LU,OU	✓	✓	III	✗	✓	●	$\checkmark_{D,V}$	Static	✓	✗	✗	✗	✗	✗	✗
CGKW18 [32]	[10, 95]	KP,CP	MSP	✓	OU	✗	✓	III	✗	✗	●	$\checkmark_{D,V}$	Static	✗	✗	✓	✗	✗	✗	✗
LYZL18 [74]	[20, 111]	CP	MSP	✓	LU,OU	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	$q(\mathrm{AND})$	✗	✗	✗	✓	✗	✗	✗
MJ18 [79]	[31]	CP	T	✗	$\|\mathcal{U}\|$	✗	✓	III	✗	✓	●	✗	Static	✓	◑	✗	✗	✓	✗	✗
KW19 [65] I,II	[70]	KP,CP	BF	✗	$\|\mathcal{U}\|$	✗	✓	III	✗	✗	●	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
KW19 [65] III	[69]	KP	BF	✓	-	✗	✓	III	✗	✗	●	$\checkmark_{D,V}$	Static	✗	✗	✓	✗	✗	✗	✗
TKN20 [106]	[5, 65]	KP,CP	NM-BF	✓	LU	✗	✓	III	✗	✓	●	$\checkmark_{D,V}$	Static	✓	✗	✗	✗	✗	✗	✗

Existing work

Scheme	Based on	KP/CP	Expr.	LU	Bounded	RFI	Prime	Type	CS-CT	CP-D	Model	CCA*	Assump.	ROM	MA-ABE	On/off	Revoc.	A-H	Out. dec.	Trace.
SW05 [98] I	-	KP	T	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	$\checkmark_V$	Static	✗	✗	✗	✗	✗	✗	✗
SW05 [98] II	-	KP	T	✓	LU	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
GPSW06 [52] I	[98] I	KP	MSP	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	$\checkmark_V$	Static	✗	✗	✗	✗	✗	✗	✗
GPSW06 [52] II	[98] II	KP	MSP	✓	LU	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
Cha07 [27] I	[98] I	KP	MA-T	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	$\checkmark_V$	Static	✗	◑	✗	✗	✗	✗	✗
Cha07 [27] II	[52] II	KP	MA-MSP	✓	LU	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	Static	✗	◑	✗	✗	✗	✗	✗
BSW07 [18]	[52] II	CP	MSP	✓	LU	✓	✓	I	✗	✗	◑	$\checkmark_{D,V}$	GGM	✗	✗	✗	✗	✗	✗	✗
CN07 [37]	[52] I	KP*	AND	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	✓	Static	✗	✗	✗	✗	✗	✗	✗
OSW07 [87]	[52] II	KP	NMSP	✓	LU	✗	✓	I	✗	✗	◑	$\checkmark_V$	Static	✗	✗	✗	✗	✗	✗	✗
NYO08 [82] I	[37] I	KP*	AND	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	$\checkmark_V$	Static	✗	✗	✗	✗	✓	✗	✗
NYO08 [82] II	[18]	CP	AND	✗	$\|\mathcal{U}\|$	✓	✓	II	✗	✗	◑	$\checkmark_{D,V}$	GGM	✗	✗	✗	✗	✓	✗	✗
CC09 [28]	[27]	KP	MA-T	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	$\checkmark_V$	$q(\|\mathcal{A}\|)$	✗	◑	✗	✗	✗	✗	✗
YWRL10 [115]	[37] I	KP*	AND	✗	$\|\mathcal{U}\|$	✓	✓	I	✗	✗	◑	✓	Static	✗	✗	✗	✓	✗	✗	✗
HLR10 [56]	-	CP	T	✗	$\|\mathcal{U}\|$	✓	✓	I	✓	✓	◑	✗	$q(\|\mathcal{U}\|)$	✗	✗	✗	✗	✗	✗	✗
LOSTW10 [66]	[110]	CP	MSP	✓	LU,OU	✗	✗	I	✗	✗	●	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
OT10 [84]	[66]	KP,CP	NMSP	✓	OU,$\|\mathcal{A}\|$	✓	✓	III	✗	✗	●	✓	Static	✗	✗	✗	✗	✗	✗	✗
Wat11 [111] I	[66]	CP	MSP	✓	LU	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✗	✗	✗	✗	✗
Wat11 [111] II	[66]	CP	MSP	✓	LU,OU	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	q(AND)	✗	✗	✗	✗	✗	✗	✗
Wat11 [111] III	[66]	CP	MSP	✓	LU,OU	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
LHCC+11 [72]	[28, 82]	KP*	AND	✗	$\|\mathcal{U}\|$	✗	✓	II	✗	✗	◑	$\checkmark_V$	$q(\|\mathcal{A}\|)$	✗	◑	✗	✗	✓	✗	✓
LW11 [68] I	[66]	CP	MSP	✗	$\|\mathcal{U}\|$,OU	✗	✗	I	✗	✗	●	✗	Static	✓	●	✗	✗	✗	✗	✗
LW11 [67] II	[66]	CP	MSP	✗	$\|\mathcal{U}\|$,OU	✗	✓	I	✗	✗	◑	✗	GGM	✓	●	✗	✗	✗	✗	✗
LW11b [69]	[66]	KP	MSP	✓	-	✗	✗	I	✗	✗	◑	$\checkmark_{D,V}$	Static	✗	✗	✓	✗	✗	✗	✗
GHW11 [54] I	[111]	CP	MSP	✓	LU	✓	✓	I	✗	✓	◑	RCCA	$q(\|\mathcal{A}\|)$	✓	✗	✗	✗	✗	✓	✗
GHW11 [54] II	[52]	KP	MSP	✓	LU	✓	✓	I	✗	✓	◑	RCCA	Static	✓	✗	✗	✗	✗	✓	✗
LCHWY11 [75]	[66]	CP	MSP	✗	$\|\mathcal{U}\|$	✗	✗	I	✗	✗	●	$\checkmark_{D,V}$	Static	✗	◑	✗	✗	✗	✗	✗
LW12 [70]	[66]	CP	MSP	✓	LU	✗	✗	I	✗	✗	●	$\checkmark_{D,V}$	q(AND)	✗	✗	✗	✗	✗	✗	✗
SSW12 [97]	[66]	KP,CP	MSP	✓	LU,OU	✗	✗	I	✗	✗	●	✗	Static	✗	✗	✗	✓	✗	✗	✗
OT12 [85]	[84]	KP,CP	NMSP	✓	-	✓	✓	III	✗	✗	●	$\checkmark_V$	Static	✗	✗	✓	✗	✗	✗	✗
HW13 [58]	[52] II	KP	MSP	✗	$\|\mathcal{U}\|$	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	$q(\|\mathcal{U}\|)$	✗	✗	✗	✗	✗	✗	✗
CCLZ+13 [30]	[49]	KP	T	✓	LU	✓	✗	I	✓	✓	●	✗	Static	✗	✗	✗	✗	✗	✗	✗
OT13 [86]	[84]	KP,CP	NMSP	✓	$\|\mathcal{U}\|$,$\|\mathcal{A}\|$	✓	✓	III	✗	✗	●	$\checkmark_{D,V}$	Static	✓	●	✓	✗	✗	✗	✗
LCLJ+13 [71]	[98]	KP	T	✓	LU	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	Static	✗	✗	✗	✓	✗	✓	✗
RW13 [95]	[69]	KP,CP	MSP	✓	-	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✓	✗	✗	✗	✗
LCW13 [76]	[48, 70]	CP	MSP	✓	LU	✗	✗	I	✗	✗	●	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✗	✗	✗	✗	✓
HW14 [59]	[95]	KP,CP	MSP	✓	-	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✓	✗	✗	✗	✗
NCDWL14 [83]	[95]	CP	MSP	✓	-	✓	✓	I	✗	✗	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✓	✗	✗	✗	✓
KL15 [64]	[66]	KP	MSP	✗	$\log\|\mathcal{U}\|$	✗	✗	I	✗	✗	●	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
RW15 [96]	[68]	CP	MSP	✓	LU	✗	✓	I	✗	✗	◑	✗	$q(\|\mathcal{A}\|)$	✓	●	✗	✗	✗	✗	✗
LW15 [77]	[76, 95]	CP	MSP	✓	-	✗	✓	I	✗	✗	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✓	✓	✗	✗	✗	✓
ZGTC+16 [116] I	[33, 105]	KP	MSP	✗	$\|\mathcal{U}\|$	✓	✓	III	✓	✓	◕	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
ZGTC+16 [116] II	[33, 105]	KP	MSP	✓	$\|\mathcal{S}\|$	✓	✓	III	✓	✓	◕	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
AHMTY16 [14]	[10, 69]	KP	MSP	✓	-	✗	✗	III	✓	✓	●	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✗	✗	✗	✗	✗
CDLQ16 [40]	[95]	CP	MSP	✓	-	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✓	✓	✗	✓	✗
MST17 [78] I	[58]	CP	DNF	✓	LU,OU	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	$q(\|\mathcal{A}\|)$	✗	✗	✗	✗	✗	✗	✗
AC17 [5]	[31]	KP,CP	MSP	✓	LU,OU	✓	✓	III	✗	✓	●	$\checkmark_{D,V}$	Static	✓	✗	✗	✗	✗	✗	✗
CGKW18 [32]	[10, 95]	KP,CP	MSP	✓	OU	✗	✓	III	✗	✗	●	$\checkmark_{D,V}$	Static	✗	✗	✓	✗	✗	✗	✗
LYZL18 [74]	[20, 111]	CP	MSP	✓	LU,OU	✗	✓	I	✗	✓	◑	$\checkmark_{D,V}$	q(AND)	✗	✗	✗	✓	✗	✗	✗
MJ18 [79]	[31]	CP	T	✗	$\|\mathcal{U}\|$	✗	✓	III	✗	✓	●	✗	Static	✓	◑	✗	✗	✓	✗	✗
KW19 [65] I,II	[70]	KP,CP	BF	✗	$\|\mathcal{U}\|$	✗	✓	III	✗	✗	●	$\checkmark_{D,V}$	Static	✗	✗	✗	✗	✗	✗	✗
KW19 [65] III	[69]	KP	BF	✓	-	✗	✓	III	✗	✗	●	$\checkmark_{D,V}$	Static	✗	✗	✓	✗	✗	✗	✗
TKN20 [106]	[5, 65]	KP,CP	NM-BF	✓	LU	✗	✓	III	✗	✓	●	$\checkmark_{D,V}$	Static	✓	✗	✗	✗	✗	✗	✗

Open problems

- In conclusion, there is still some work to make it truly practical
- We have identified several open problems that help ABE become more practical

Open problems

- In conclusion, there is still some work to make it truly practical
- We have identified several open problems that help ABE become more practical
- One covers the briefly mentioned issue with more accurately analyzing efficiency of ABE schemes
- Others cover e.g. the design of more efficient and privacy-friendly decentralized ABE

Open problems

- In conclusion, there is still some work to make it truly practical
- We have identified several open problems that help ABE become more practical
- One covers the briefly mentioned issue with more accurately analyzing efficiency of ABE schemes
- Others cover e.g. the design of more efficient and privacy-friendly decentralized ABE
- If we solve these, ABE can truly practically implement a privacy-friendly fine-grained access control in multiple-domain settings

Thank you for your attention!