20 mars 2026

Breaking Anonymity in Attribute-Based Access Control Encryption

Baptiste Bazin

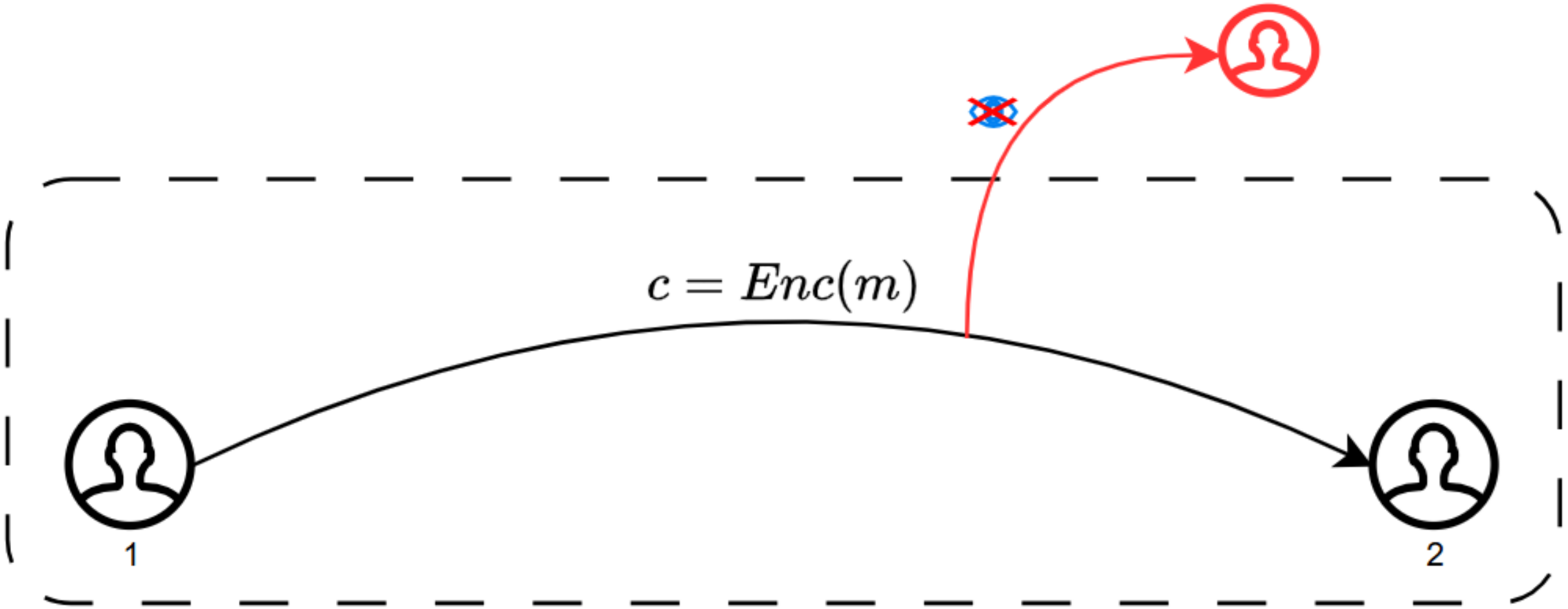
Contrôle d’accès

- Définir qui peut accéder à quoi
- Contrôler l’accès aux données, c’est préserver :
  - la confidentialité
  - l’intégrité
  - la disponibilité

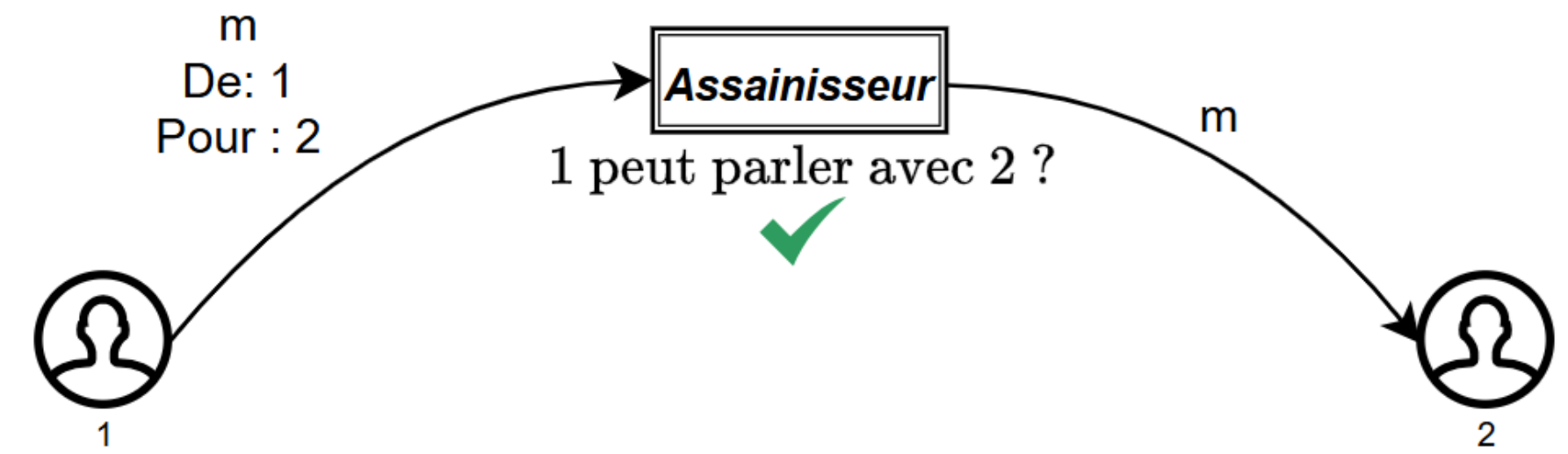
Contrôle d’accès

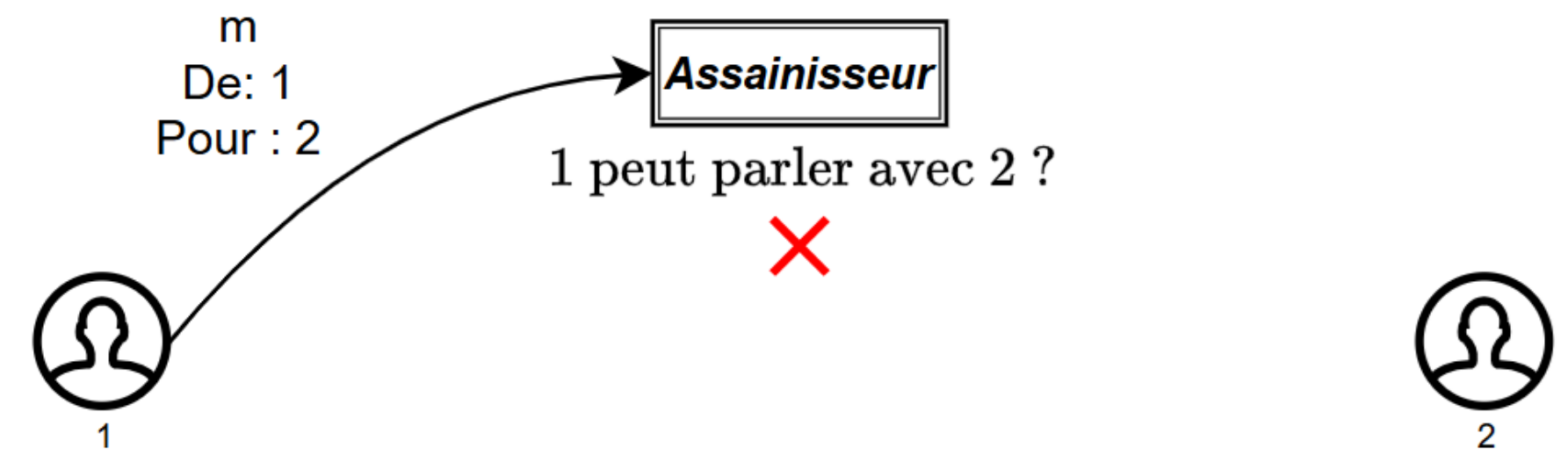
- Qui définit la politique d’accès ?
  - Discrétionnaire (DAC)
  - Obligatoire (MAC)
- Comment la politique d’accès est exprimée ?
  - Utilisateurs
  - Rôles (RBAC)
  - Attributs (ABAC)

Cryptographie classique



Contrôler l'émetteur : Assainisseur



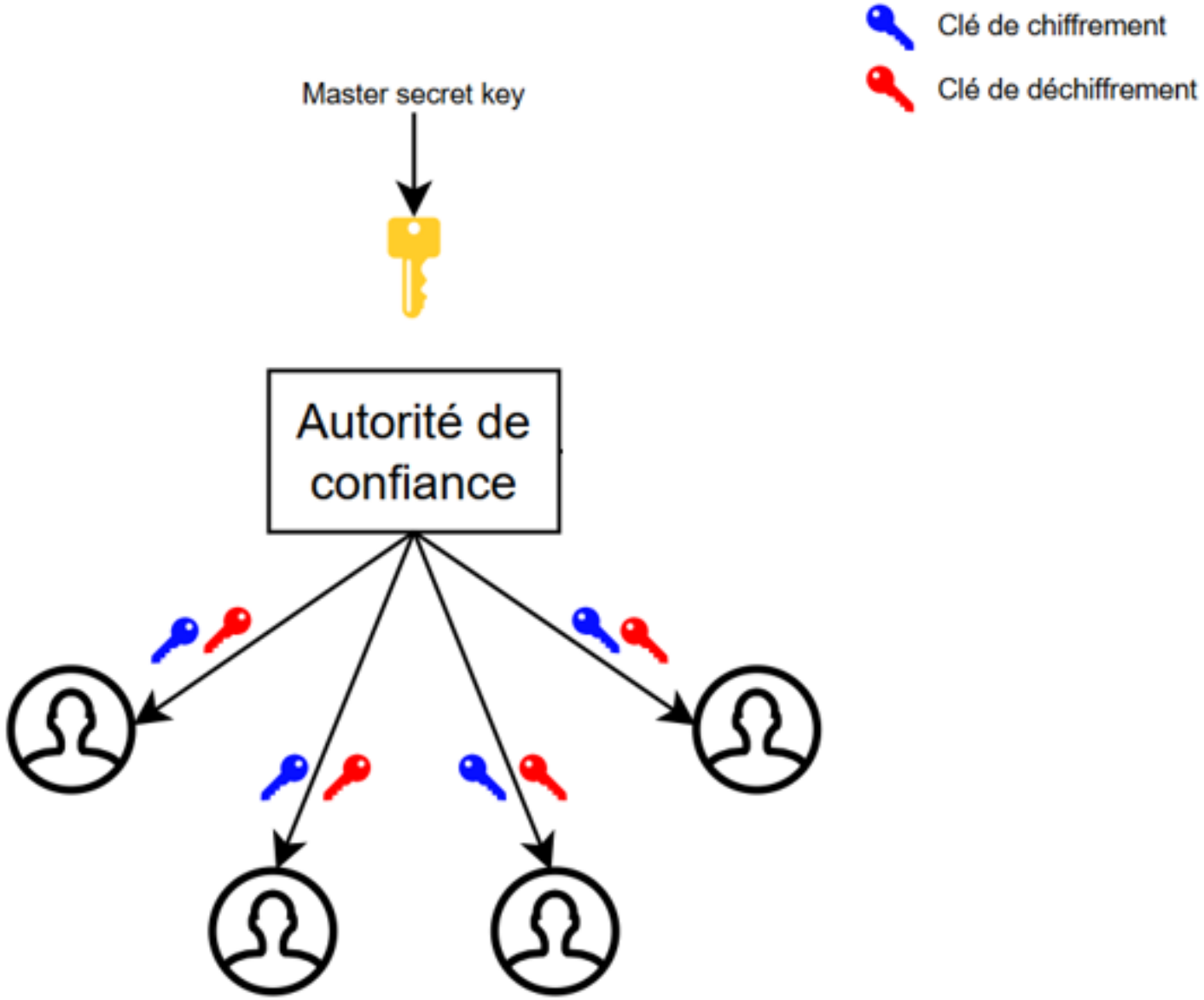


Access Control Encryption (ACE)

- Ivan Damgård, Helene Haagh, Claudio Orlandi
- Introduit un assainisseur pour contrôler l'émetteur
- Toutes les communications passent par lui
- Supposé honnête mais curieux
- Avantages :
  - Plus d'authentification
  - L'assainisseur ne connaît que le chiffré

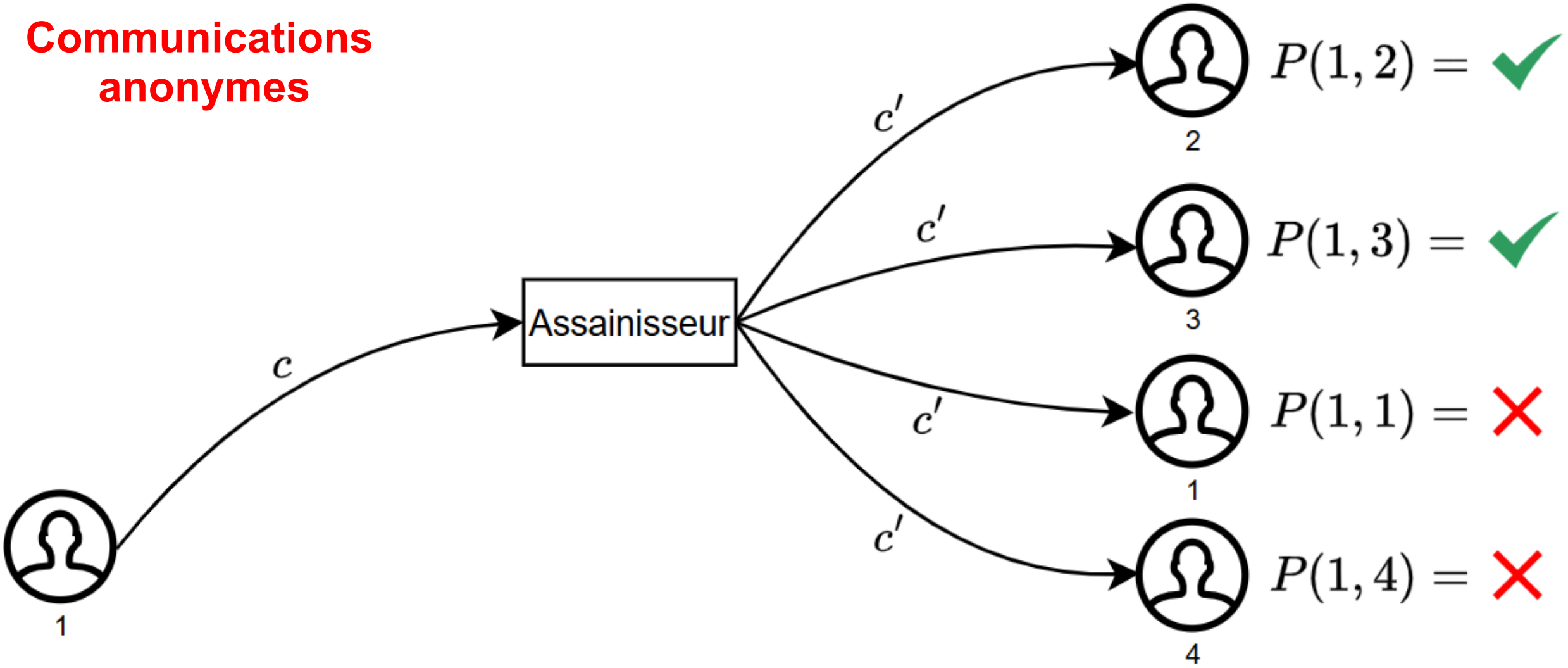
[Damgard *et al.*, 2016] *Access Control Encryption: Enforcing Information Flow with Cryptography*

Access Control Encryption (ACE)



Access Control Encryption (ACE)

Communications anonymes



Attribute-Based Encryption

Espace des attributs : $\mathbb{U} = \{U_1, \ldots, U_n\}$

A

$\{U_1, U_2, U_5\}$

B

$\{U_3\}$

C

$\{U_1, U_2, U_3, U_4\}$

L'utilisateur A associé à $\{U_1, U_2, U_5\}$
L'utilisateur B associé à $\{U_3\}$
L'utilisateur C associé à $\{U_1, U_2, U_3, U_4\}$

Attribute-Based Encryption

$$\mathbb{S} = (U_1 \text{ ET } U_2) \text{ OU } U_4$$

Chiffré c associé à $\mathbb{S}$

A

$\{U_1, U_2, U_5\}$

B

$\{U_3\}$

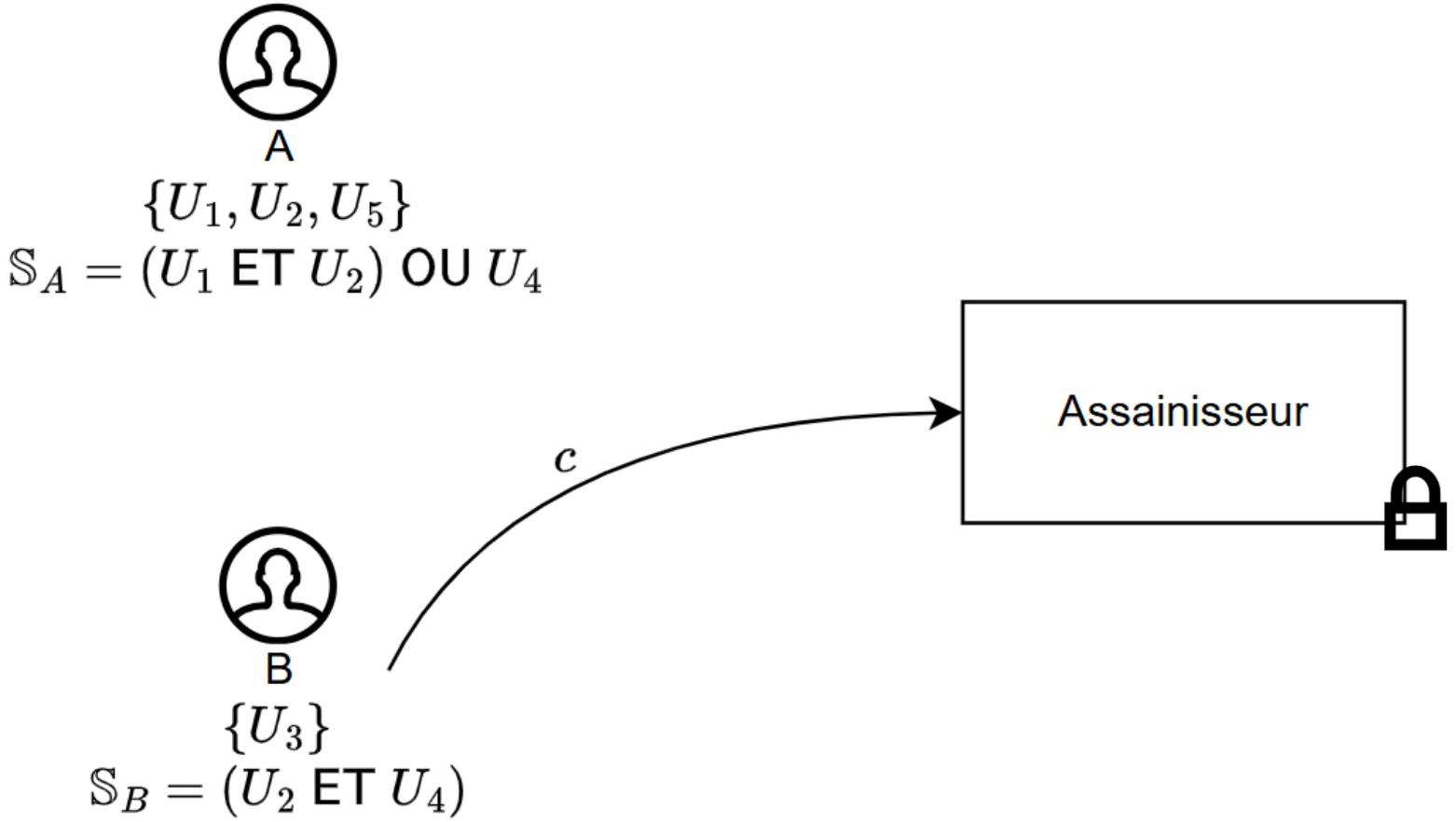
C

$\{U_1, U_2, U_3, U_4\}$

A et C peuvent déchiffrer c, B ne peut pas

Contrôler l'émetteur : imposer $\mathbb{S}$

Distinguer deux émetteurs différents



Comme c est associé à $\mathbb{S}_B$, et que $\mathbb{S}_A \neq \mathbb{S}_B$,
l'assainisseur sait que le message ne provient pas de A

Communication bidirectionnelle

Hypothèse de travail :

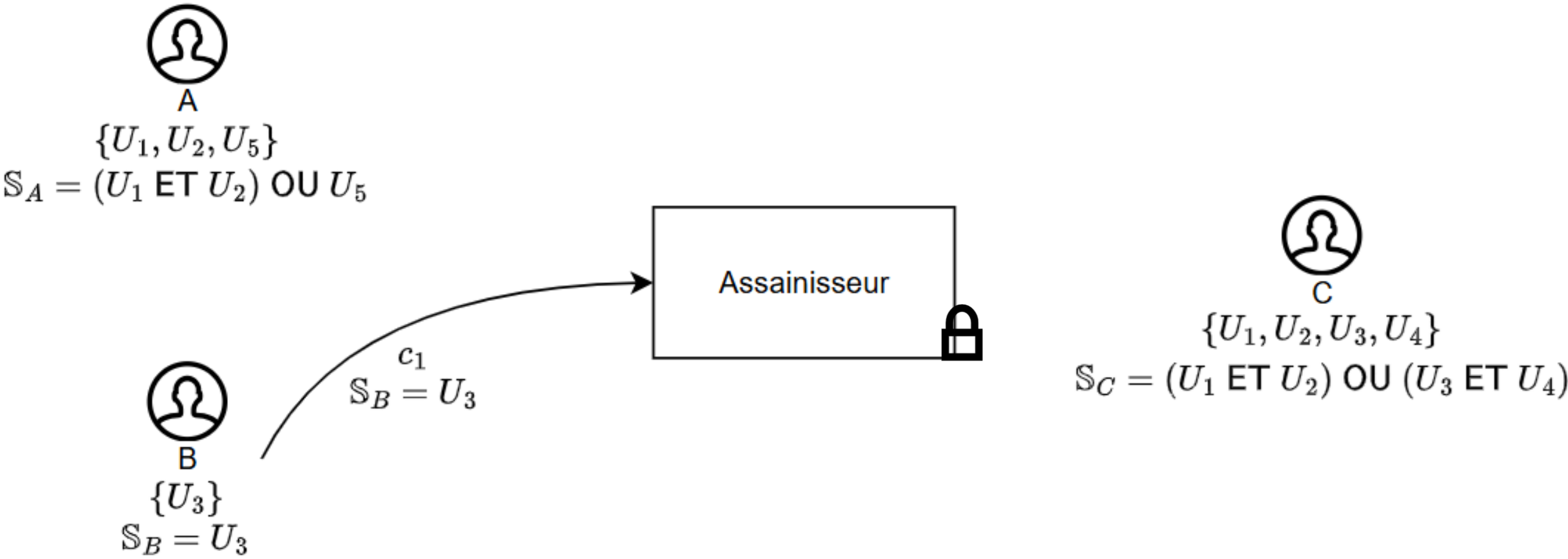
$$A \text{ peut communiquer à } \mathbb{S}_A = (U_1 \text{ ET } U_2) \text{ OU } U_5$$

$$\Rightarrow$$

$$A \text{ possède les attributs } \{U_1, U_2, U_5\}$$

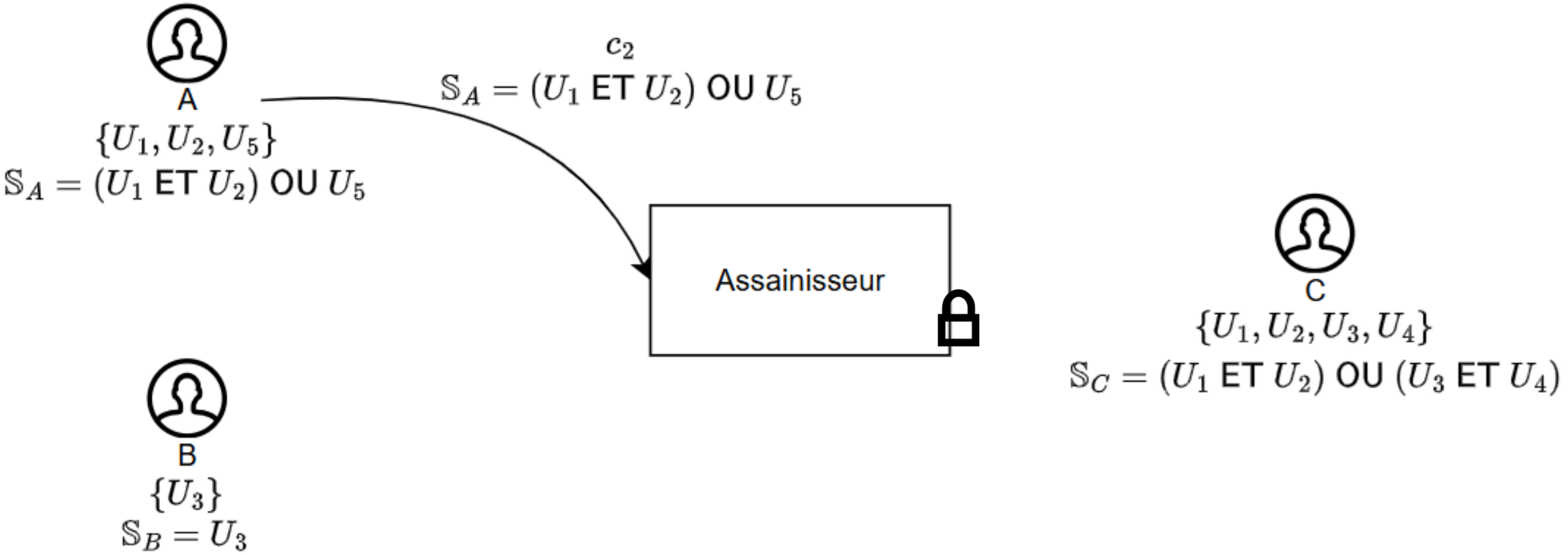
[Han *et al.*, 2019] *Fine-grained information flow control using attributes*
[Cui *et al.*, 2022] *A Practical and Efficient Bidirectional Access Control Scheme for Cloud-Edge Data Sharing*

Retrouver le trafic interne



L'assainisseur sait que : B possède l'attribut U_3

Retrouver le trafic interne



L'assainisseur sait que : A possède les attributs $\{U_1, U_2, U_5\}$
B possède l'attribut U_3

Retrouver le trafic interne

A

$\{U_1, U_2, U_5\}$

$\mathbb{S}_A = (U_1 \text{ ET } U_2) \text{ OU } U_5$

c_3

$\mathbb{S}_C = (U_1 \text{ ET } U_2) \text{ OU } (U_3 \text{ ET } U_4)$

Assainisseur

C

$\{U_1, U_2, U_3, U_4\}$

$\mathbb{S}_C = (U_1 \text{ ET } U_2) \text{ OU } (U_3 \text{ ET } U_4)$

B

$\{U_3\}$

$\mathbb{S}_B = U_3$

L'assainisseur sait que :

A possède les attributs $\{U_1, U_2, U_5\}$

B possède l'attribut U_3

C possède les attributs $\{U_1, U_2, U_3, U_4\}$

Identifier un émetteur sans la structure d'accès

- L'autorité de confiance introduit un aléa dans la clé de chiffrement.
- Cet aléa se retrouve dans chaque chiffré produit par cet utilisateur.
- En l'isolant (par des moyens algébriques), on peut déduire si deux chiffrés différents proviennent du même émetteur.

Exemple

- La clé de chiffrement contient g^r
- Il existe une fonction f tel que $f(c) = \mu^r$
- $f(c) = f(c') \Rightarrow c$ et c' proviennent du même émetteur

- Merci d’avoir écouté !

- Des questions ?