Entrelacement des mécanismes d'identification et de respect de la vie privée pour la protection des contenus externalisés

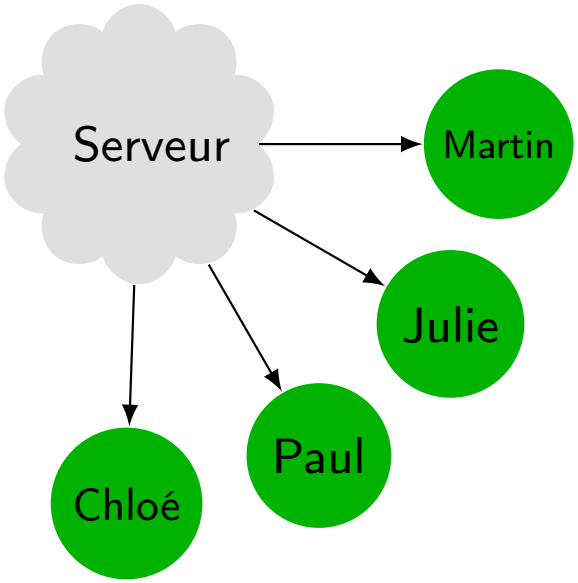
Julien Lolive
Encadré par Caroline Fontaine et Sébastien Gambs

Télécom-Bretagne Brest
Laboratoires Lab-STICC et IRISA
Équipes SFIIS et CIDRE

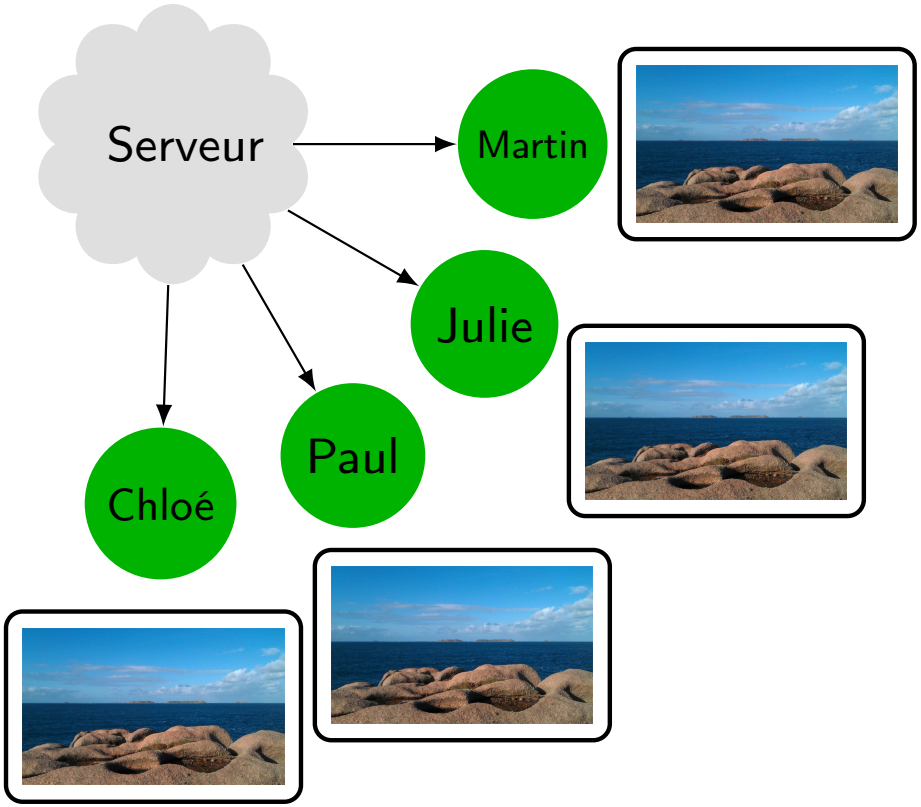
projet CominLabs POSEIDON

13 mai 2016

Contexte : comment prévenir les redistributions illégales ?

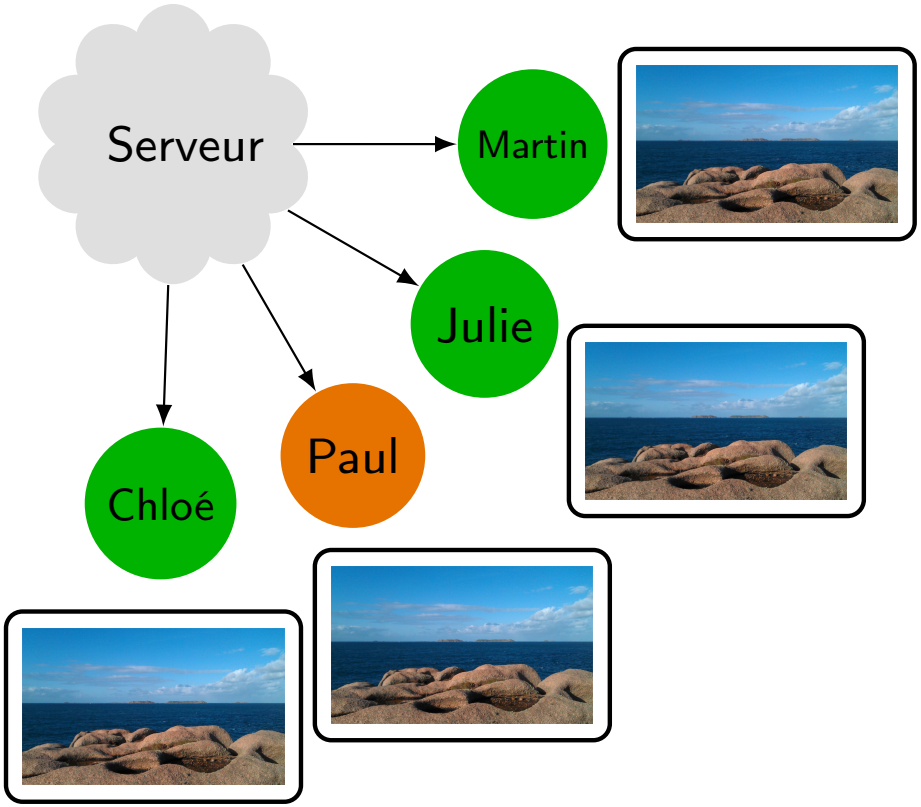


Contexte : comment prévenir les redistributions illégales ?



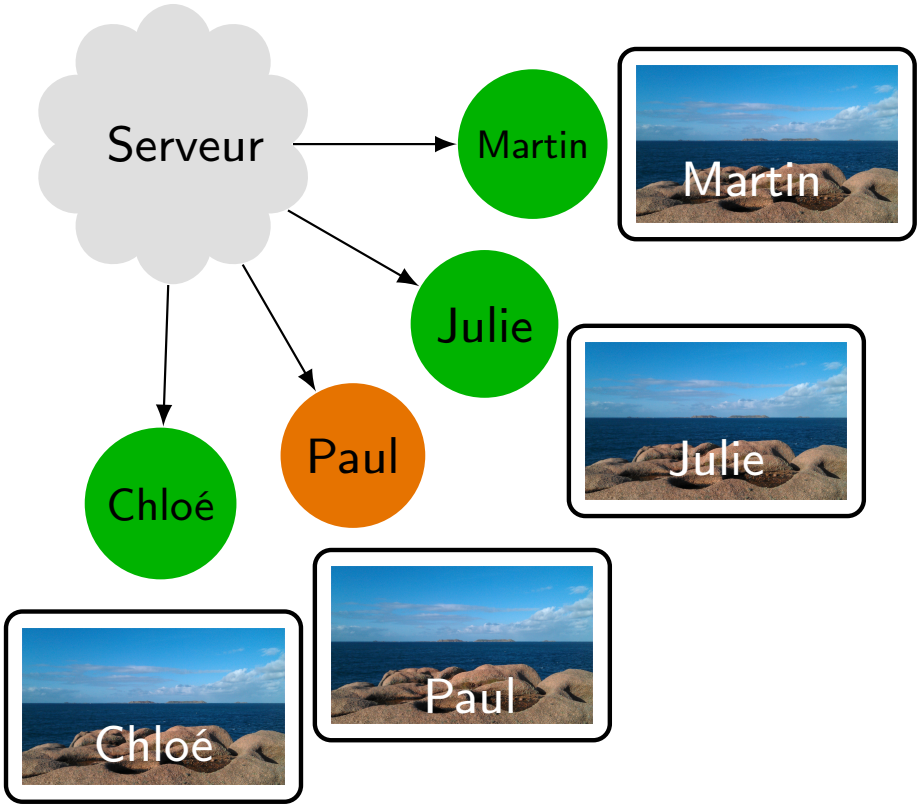
- Cryptographie ?

Contexte : comment prévenir les redistributions illégales ?



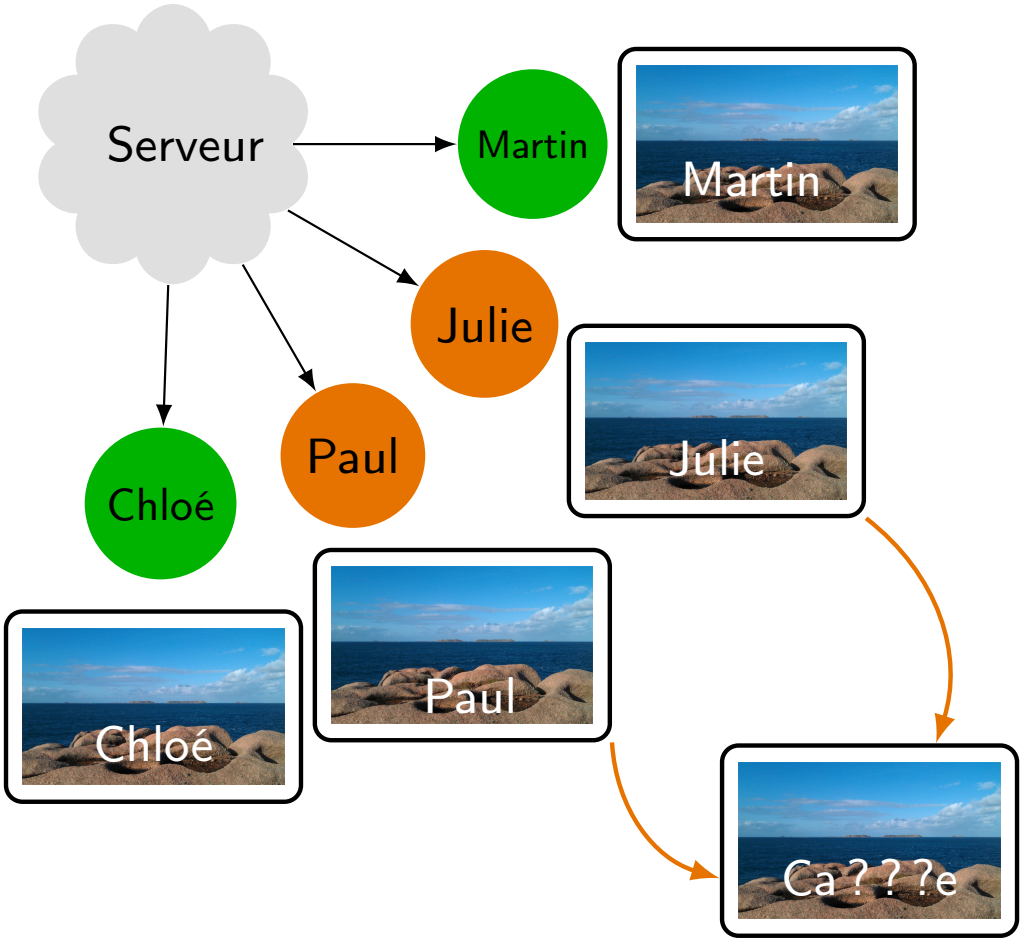
- Cryptographie insuffisante.

Contexte : comment prévenir les redistributions illégales ?



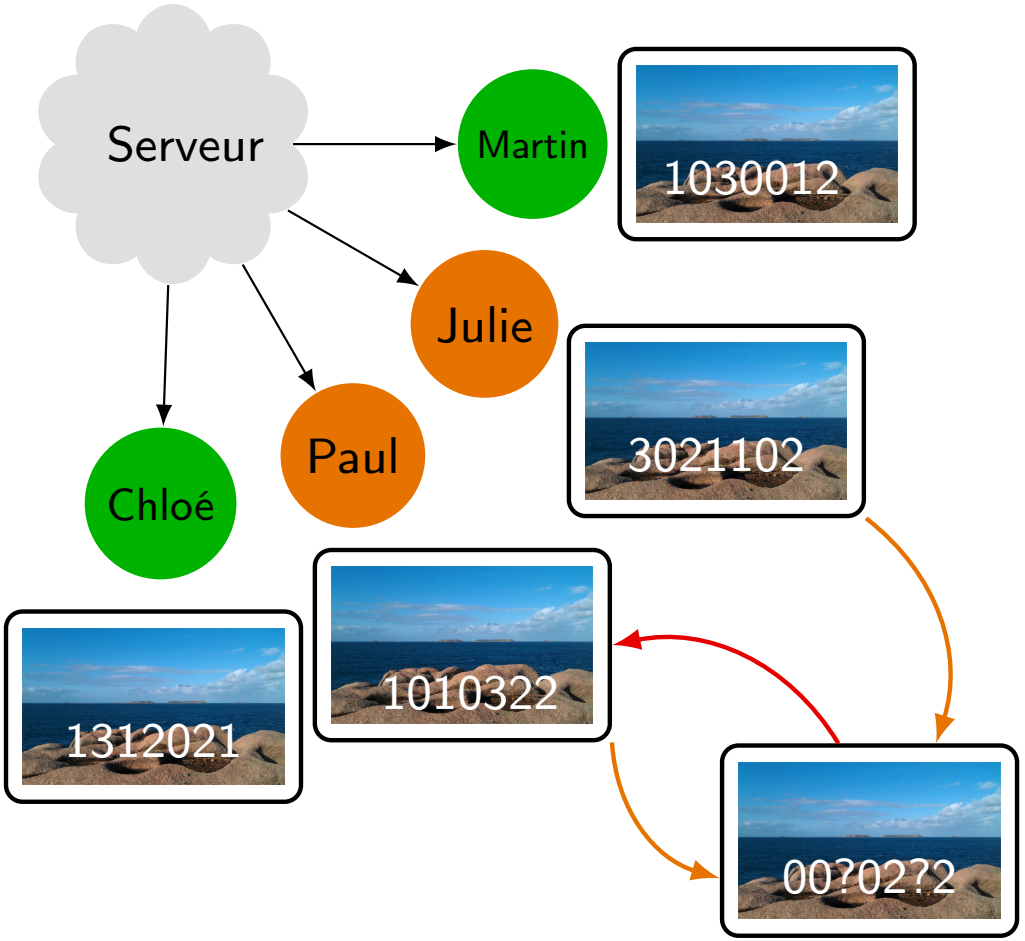
- Cryptographie insuffisante.
- Tatouage ?

Contexte : comment prévenir les redistributions illégales ?



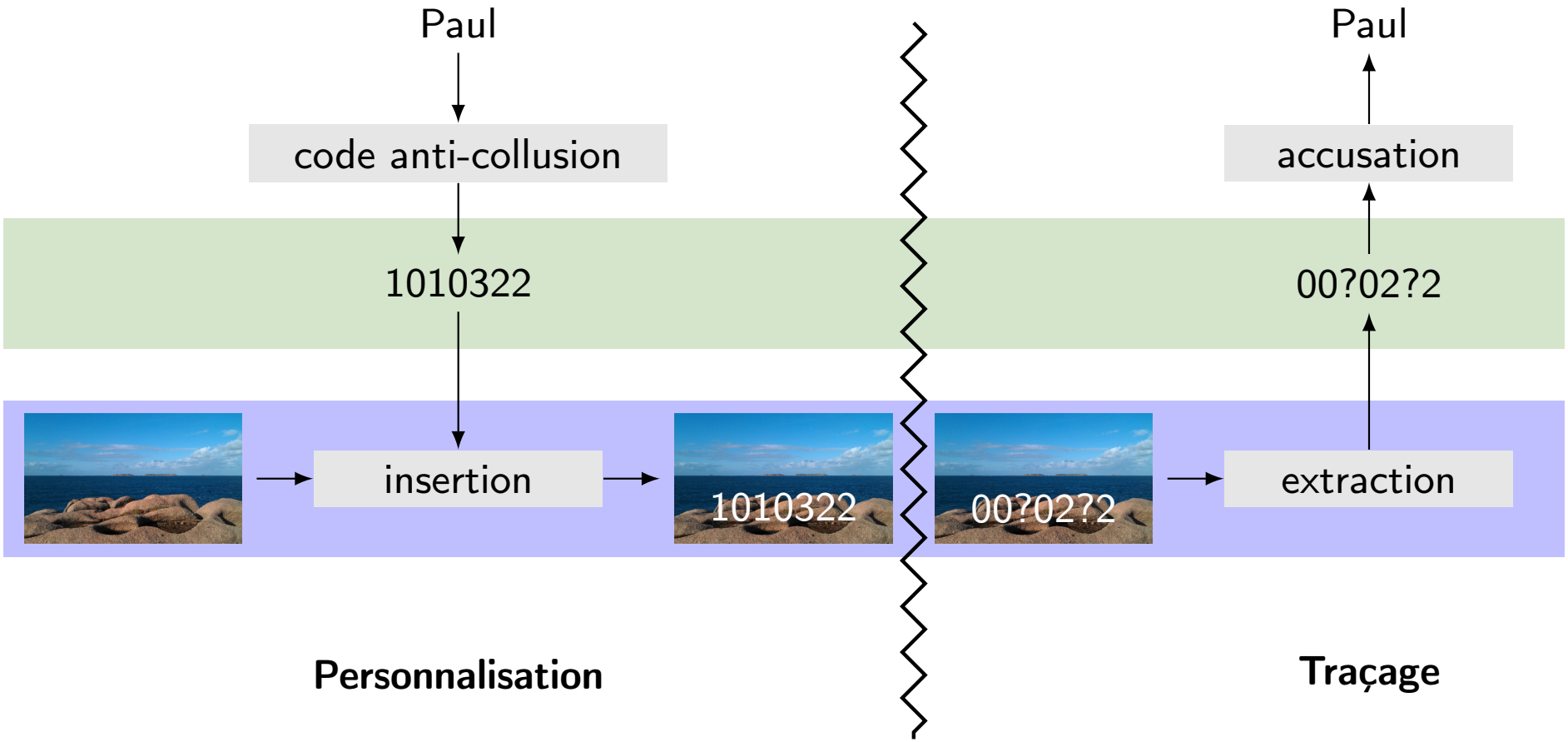
- Cryptographie insuffisante.
- Tatouage ? Oui, mais ...

Contexte : comment prévenir les redistributions illégales ?



- Cryptographie insuffisante.
- Tatouage ? Oui, mais ...
- ... il faut utiliser des codes anti-collusion avec une structure permettant le traçage.

Utilisation d'un code anti-collusion



Attaques et hypothèse de marquage


1 0 1 0 3 2 2 $\mathbf{X}_{\text{Paul}}$


3 0 2 1 1 0 2 $\mathbf{X}_{\text{Julie}}$


1 0 3 0 0 1 2 $\mathbf{X}_{\text{Martin}}$

Collusion (c acheteurs parmi n)


1 0 3 1 0 2 2 $\mathbf{Y}$

Copier/coller de blocs (*ex :* aléatoire, maj, etc.)


0 0 ? 0 2 ? 2 $\mathbf{Y}$

Fusion de blocs (*ex. :* moyenne pixel à pixel)

Boneh & Shaw : hypothèse de marquage $X_{j_1 i} = \ldots = X_{j_c i} = a \Rightarrow Y_i = a$.


? 0 1 2 ? 1 ? $\mathbf{Y}$

Traitement de signal individuel (*ex. :* compression)

Prévenir erreurs et effacements $\Rightarrow$ tatouage robuste.

Sommaire

Symétrique, asymétrique et anonyme

Symétrique[a] :

- Empreinte générée et insérée par le vendeur.
- Sortie : contenu marqué (acheteur), empreinte (vendeur).
- Le vendeur peut accuser un acheteur innocent !

Asymétrique[b] :

- Apporte la propriété d'*anti-framing* à l'acheteur.
- Protocole biparti pour générer l'empreinte.
- Sortie : contenu marqué (acheteur), halfword (vendeur).

a. **N.R. Wagner**, ***Fingerprinting***, **S&P**, **1983**.

b. **B. Pfitzmann, et M. Schunter**, ***Asymmetric fingerprinting***, **EUROCRYPT**, **1996**.

Symétrique, asymétrique et anonyme

Anonyme[a] = Asymétrique +

- Acheter anonymement un contenu.
- Lever l'anonymat s'il y a une redistribution illégale.
- Centre d'enregistrement (tierce partie de confiance) : connaît les identités de tous les acheteurs, mais pas les contenus obtenus.

a. B. Pfitzmann, et M. Waidner, *Anonymous fingerprinting*, EUROCRYPT, 1997.

Codes anti-collusion

- Permet de contrer des collusions.
- Taille du mot de code en fonction de c^a et de δ^b.

c	δ	Boneh et Shaw 95*	SKC 08+
2	1×10^{-10}	299 889	1894
10	1×10^{-10}	$4,78 \times 10^8$	47374
20	1×10^{-10}	$6,56 \times 10^9$	189496
30	1×10^{-10}	$4,16 \times 10^{10}$	426366

*** : Données empruntées à A. Charpentier. Thèse : "Identification de copies de documents multimédia grâce aux codes de Tardos".**

+ : Codes de Tardos améliorés par Škorić, Katzenbeisser et Celik.

c = taille maximale de la collusion tolérée par le système.

δ = probabilité maximale ($\delta << 1$) pour un innocent d'être faussement accusé.

Objectifs

Sécurité et protection de la vie privée

- Sécurité :
  - dissuader les acheteurs malveillants de redistribuer illégalement un contenu.
  - dissuader le vendeur malveillant de tricher durant le protocole.
- Protection de la vie privée : prévenir le profilage des acheteurs.

$\Rightarrow$ Défi principal : assurer la protection de la vie privée tout en conservant des propriétés de sécurité fortes.

Objectifs

Propriétés de Sécurité et de Protection de la vie privée

- Traçage de traîtres : le vendeur doit être capable de retrouver un traître avec une forte probabilité en cas de redistribution illégale.
- *Anti-framing* : un acheteur innocent ne peut pas être accusé par le vendeur malveillant.
- Anonymat révocable : l'identité de l'acheteur reste anonyme aussi longtemps qu'il est honnête.
- Non-chaînabilité des acheteurs : le vendeur ne peut pas savoir si deux transactions ont été effectuées par le même acheteur ou non.

Comparaison des propriétés atteintes

	Anti-framing	Traçage de traîtres	Analyse de sécurité formelle	Anonymat révocable	Non-chaînabilité des acheteurs	Compatible avec les codes de Tardos	Implem.
PS 96[a]	V	Oui	X	X	X	X	X
CFFC 11[b]	V	Oui	X	X	X	V	X
PS 97[c]	V	Oui	X	V	V	X	X
RDBPP 10[d]	V	Oui	V	V	V	X	V
AGC 10[e]	V	Non	X	V	V	X	X

a : B. Pfitzmann et M. Schunter, *Asymmetric fingerprinting*, EUROCRYPT, 1996.

b : A. Charpentier, C. Fontaine, T. Furon, et I. Cox, *An asymmetric fingerprinting scheme based on tardos codes*, IH, 2011.

c : B. Pfitzmann, M. Waidner, *Anonymous Fingerprinting*, EUROCRYPT, 1997.

d : A. Rial, M. Deng, T. Bianchi, A. Piva, et B. Preneel, *A provably secure anonymous buyer-seller watermarking protocol*, IEEE Transactions on Information Forensics and Security, 2010.

e : W. Abdul, P. Gaborit, et P. Carré, *Private anonymous fingerprinting for color images in the wavelet domain*, SPIE, 2010.

Sommaire

Entités du protocole

- Autorité de Certification (AC) : enregistre les acheteurs dans le système.
- Autorité d'Ouverture (AO) : lève l'anonymat des acheteurs accusés.
- Vendeur : fournisseur de contenus.
- Acheteur : acheteur de contenus.
- Autre composant : WORM (*Write Once Read Many*), utilisé pour l'intégrité.

Briques de constructions (1/5)

Code de Tardos[ab]

- Code de Tardos : probabiliste et efficace, amélioré par Škorić, Katzenbeisser et Celik, etc.
- Avantages : Optimal entre traçage de traîtres et longueur.
- Paramètres :
  - c = taille maximale de la collusion tolérée par le système.
  - δ = probabilité maximale ($\delta << 1$) pour un innocent d'être faussement accusé.
  - m = longueur des mots de codes.
  - Z = seuil d'accusation.
  - p = vecteur de probabilités de taille m.

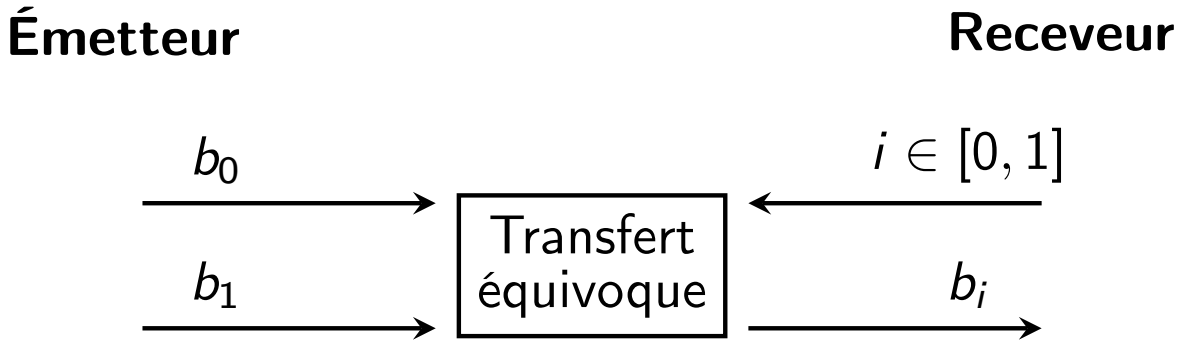
a : **G. Tardos, *Optimal probabilistic fingerprint codes*, Symposium on Theory of computing, 2003.**

b : **B. Škorić, S. Katzenbeisser, et M. Celik, *Symmetric tardos fingerprinting codes for arbitrary alphabet sizes*, Designs, Codes and Cryptography, 2008.**

Briques de constructions (2/5)

Transfert équivoque[a]

Un receveur récupère un élément parmi une liste de n éléments fournie par un émetteur sans que celui-ci ne sache quel élément est récupéré par le receveur et sans que ce dernier n'apprenne les autres éléments de la liste.

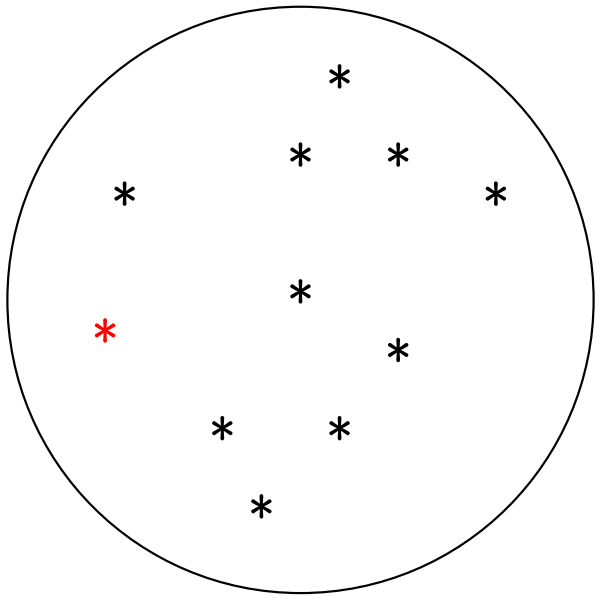


a : M. Naor, et B. Pinkas, ***Efficient oblivious transfer protocols***, Symposium on Discrete algorithms, 2001.

Briques de constructions (3/5)

Signature de groupe[a]

Apporte l'anonymat du signataire (cacher derrière le groupe, indistinguabilité, non-répudiation, resistance à la contrefaçon).



a : D. Chaum, et E. van Heyst, *Group Signatures*, EUROCRYPT, 1991.

Briques de constructions (4/5)

Canal de communication anonyme[a]

Empêche le receveur de retrouver la source du message (chemin de plusieurs nœuds et chiffrement en oignon, par exemple, TOR).

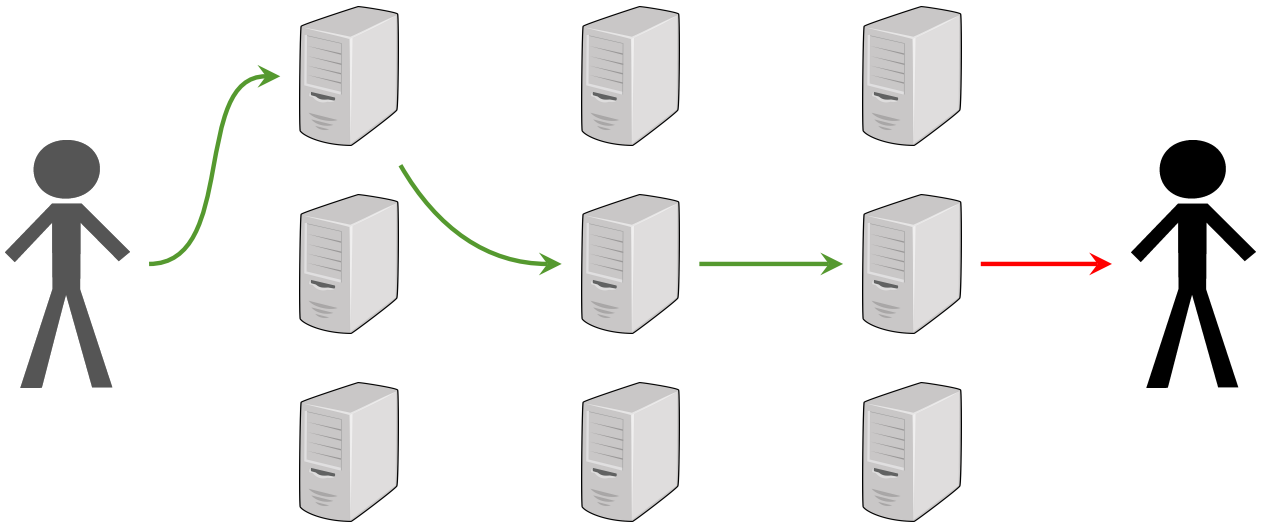


Figure: En vert, le message chiffré, en rouge le message en clair

a :R. Dingledine, N. Mathewson, et P. Syverson, *Tor : the second-generation onion router*, USENIX, 2004.

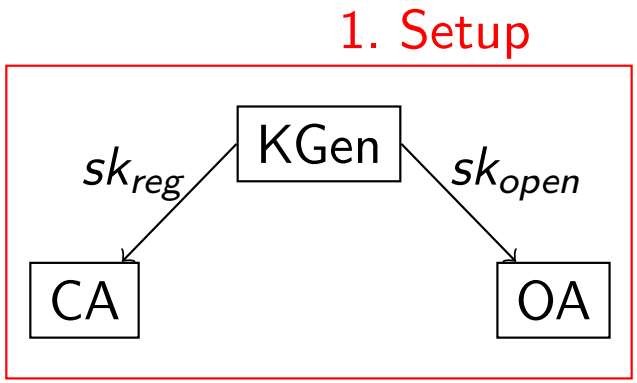
Briques de constructions (5/5)

Preuve non interactive sans divulgation (NIZK)[a]

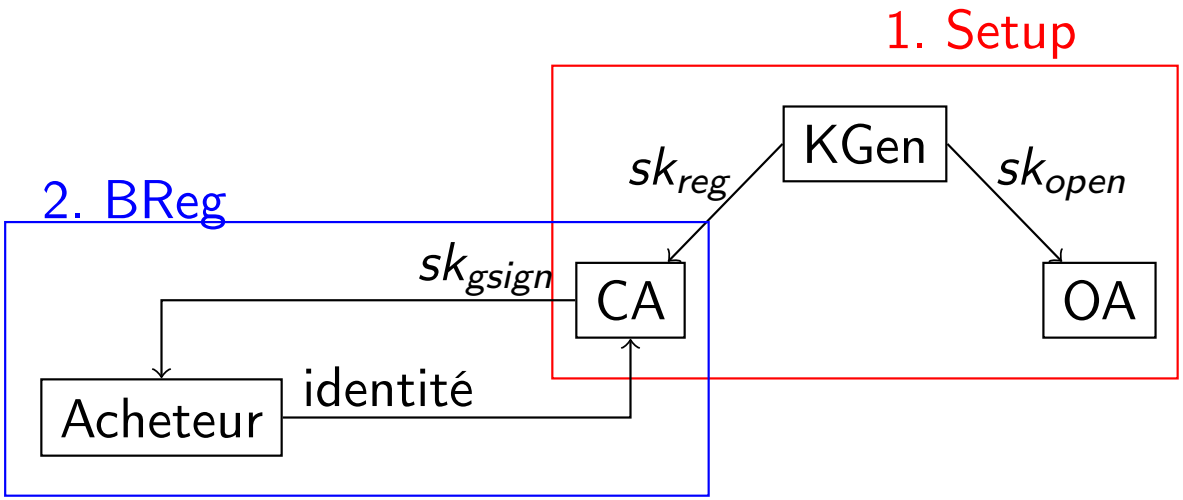
Permets à un prouveur de prouver qu'il connaît un secret auprès d'un vérifieur de telle sorte que le vérifieur n'apprend que la véracité du secret.

a :**J. Groth, R. Ostrovsky, et A. Sahai,** ***Perfect non-interactive zero knowledge for NP*****, EUROCRYPT, 2006.**

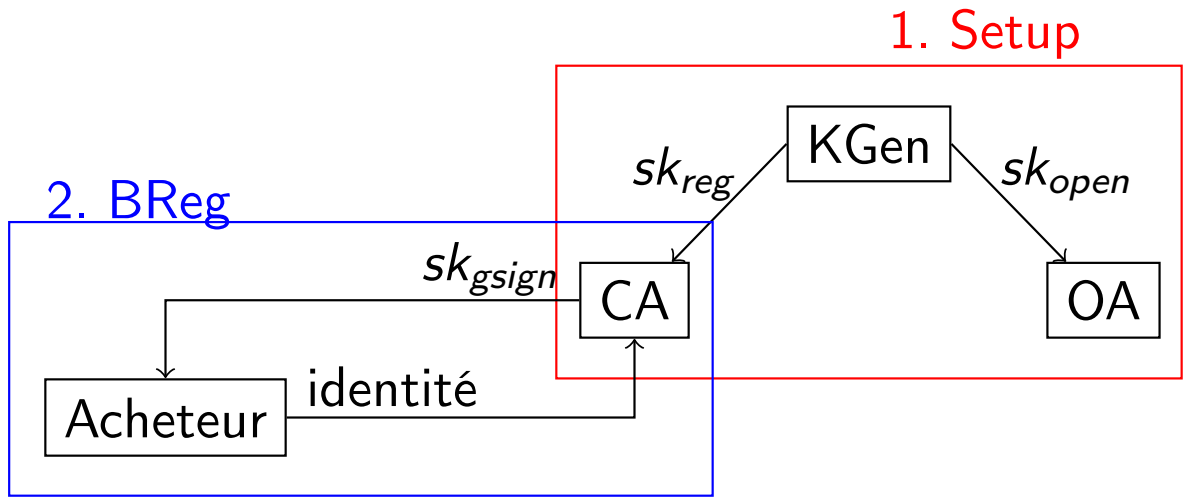
Initialisation (Setup) ; Enregistrement des acheteurs (BReg) ; et Préparation des contenus (IPrep)



Initialisation (Setup) ; Enregistrement des acheteurs (BReg) ; et Préparation des contenus (IPrep)



Initialisation (Setup) ; Enregistrement des acheteurs (BReg) ; et Préparation des contenus (IPrep)



Initialisation (Setup) ; Enregistrement des acheteurs (BReg) ; et Préparation des contenus (IPrep)

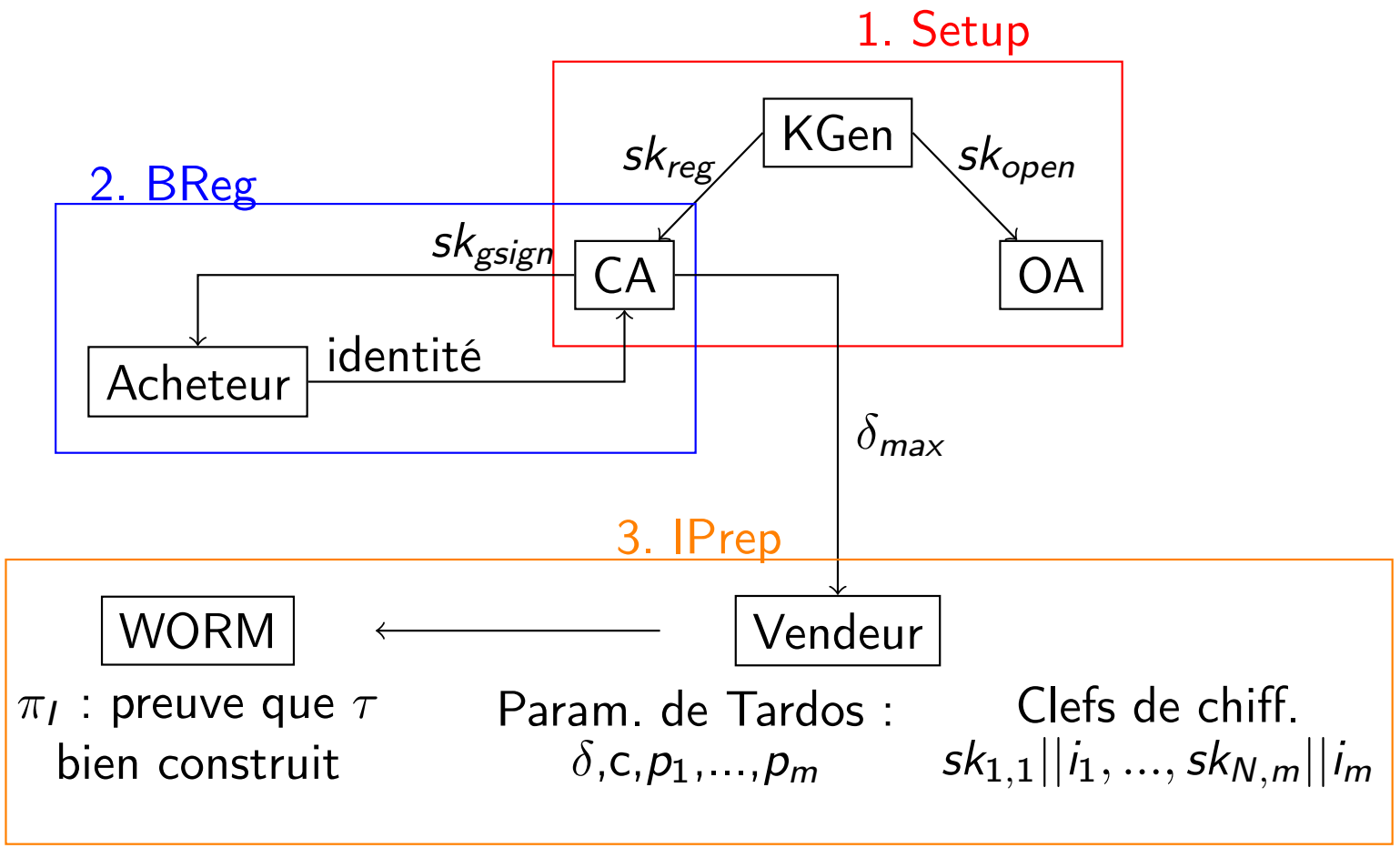


Illustration de la préparation des contenus

Illustration de la préparation des contenus

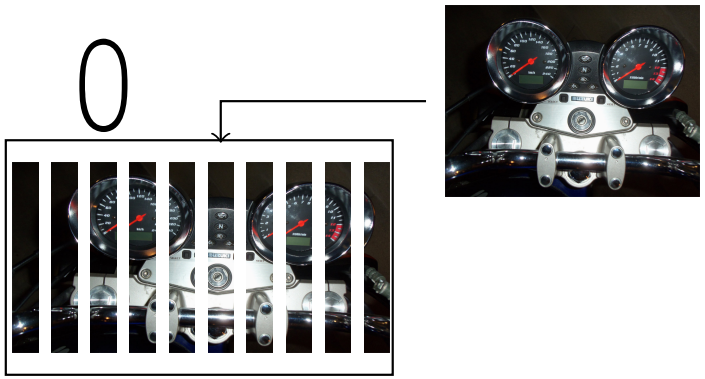


Illustration de la préparation des contenus

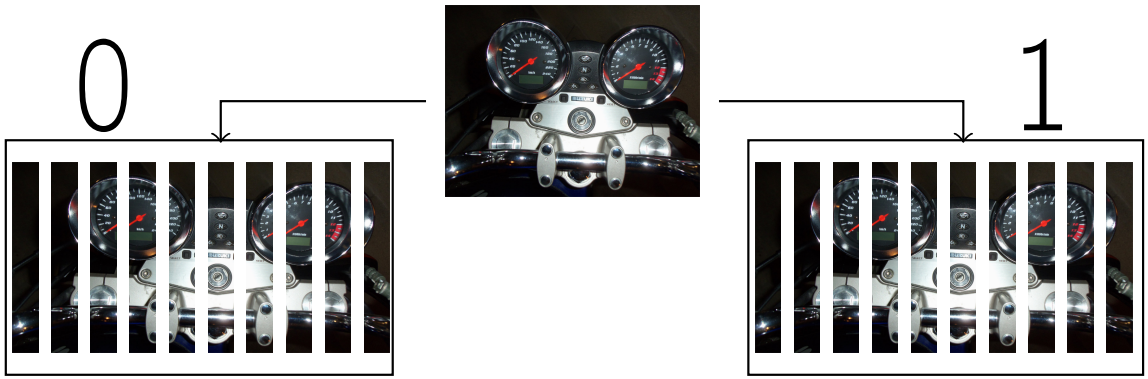
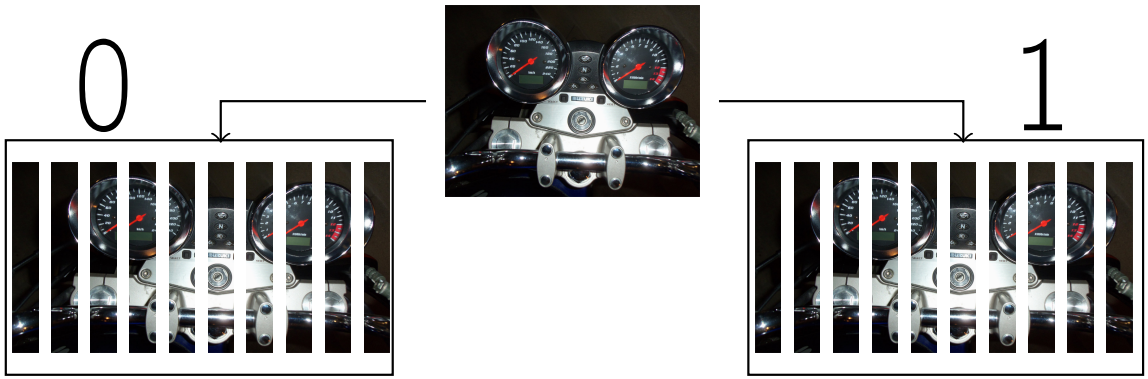
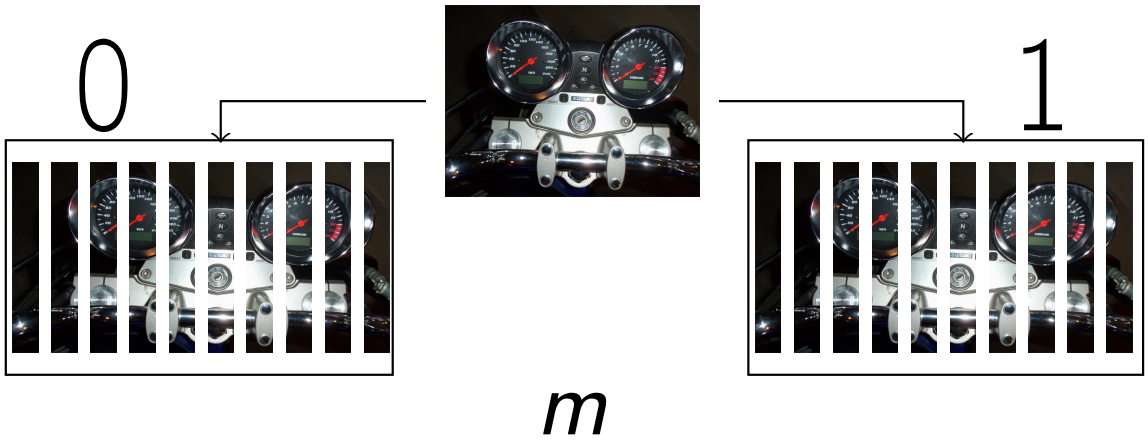


Illustration de la préparation des contenus



$$p = \boxed{0.9} \boxed{0.5} \boxed{\ldots} \boxed{\ldots} \boxed{\ldots} \boxed{0.1}$$

Illustration de la préparation des contenus



N

$p =$

0.9	0.5	...	...	...	0.1

Illustration de la préparation des contenus

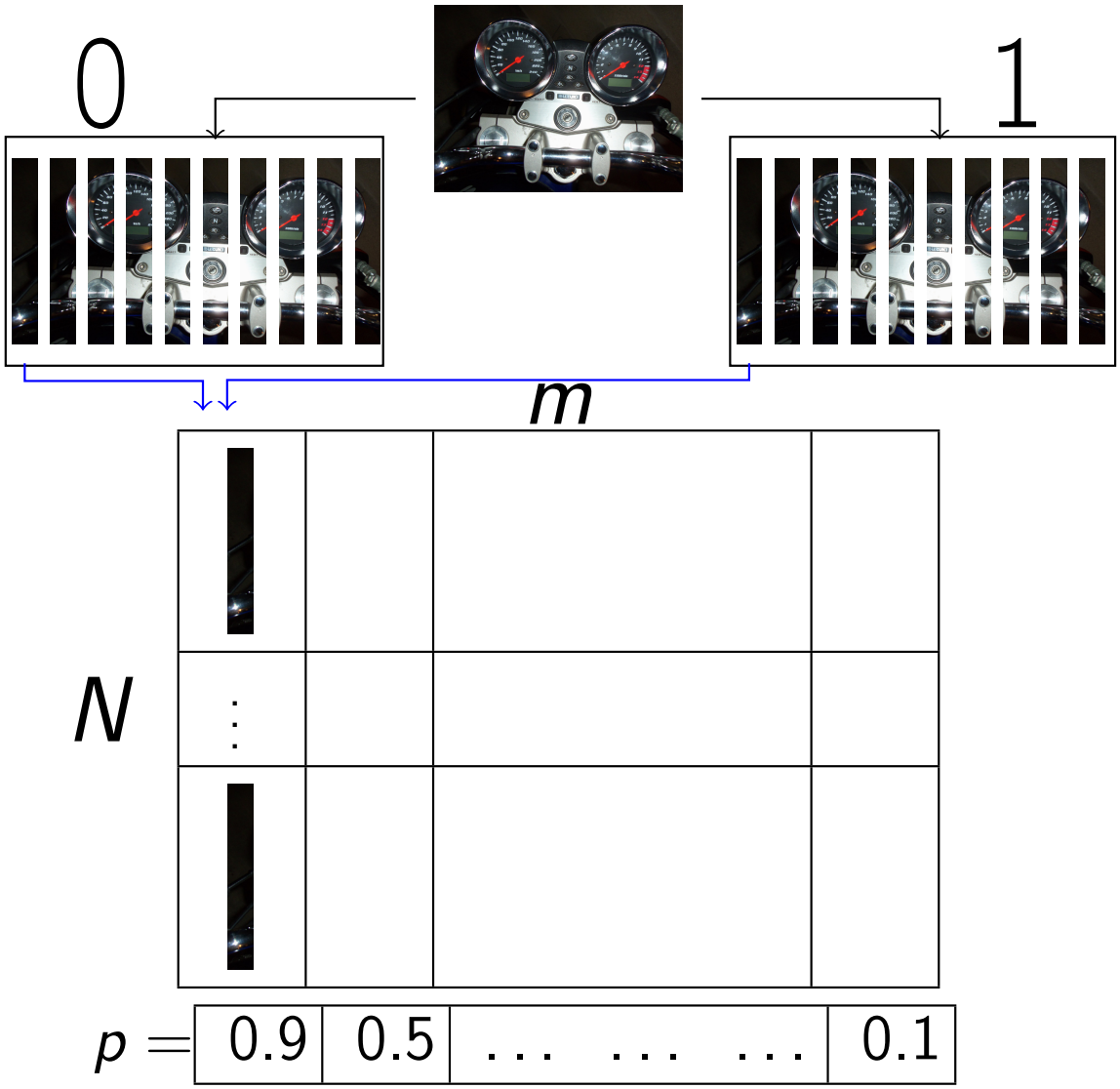


Illustration de la préparation des contenus

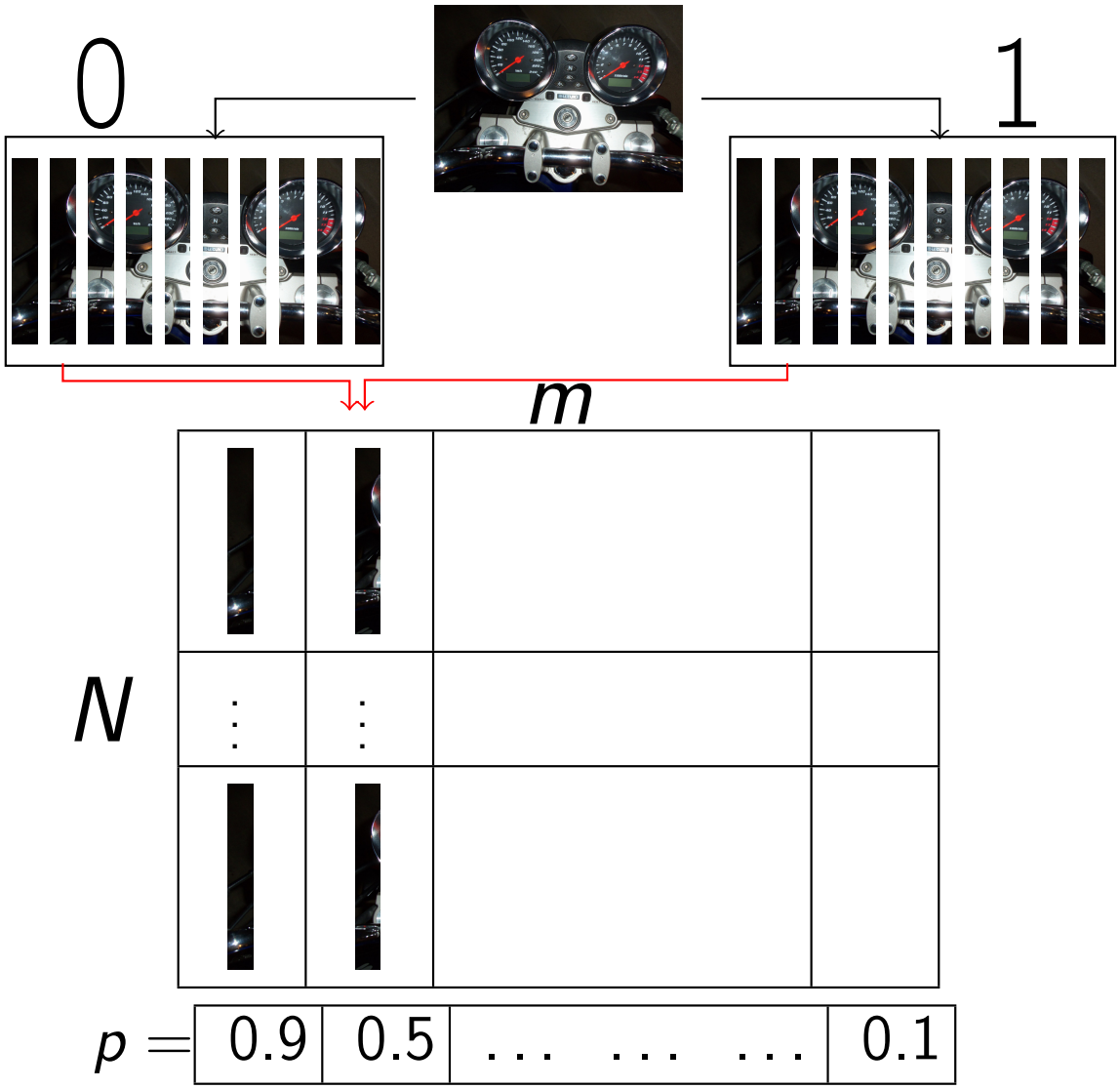


Illustration de la préparation des contenus

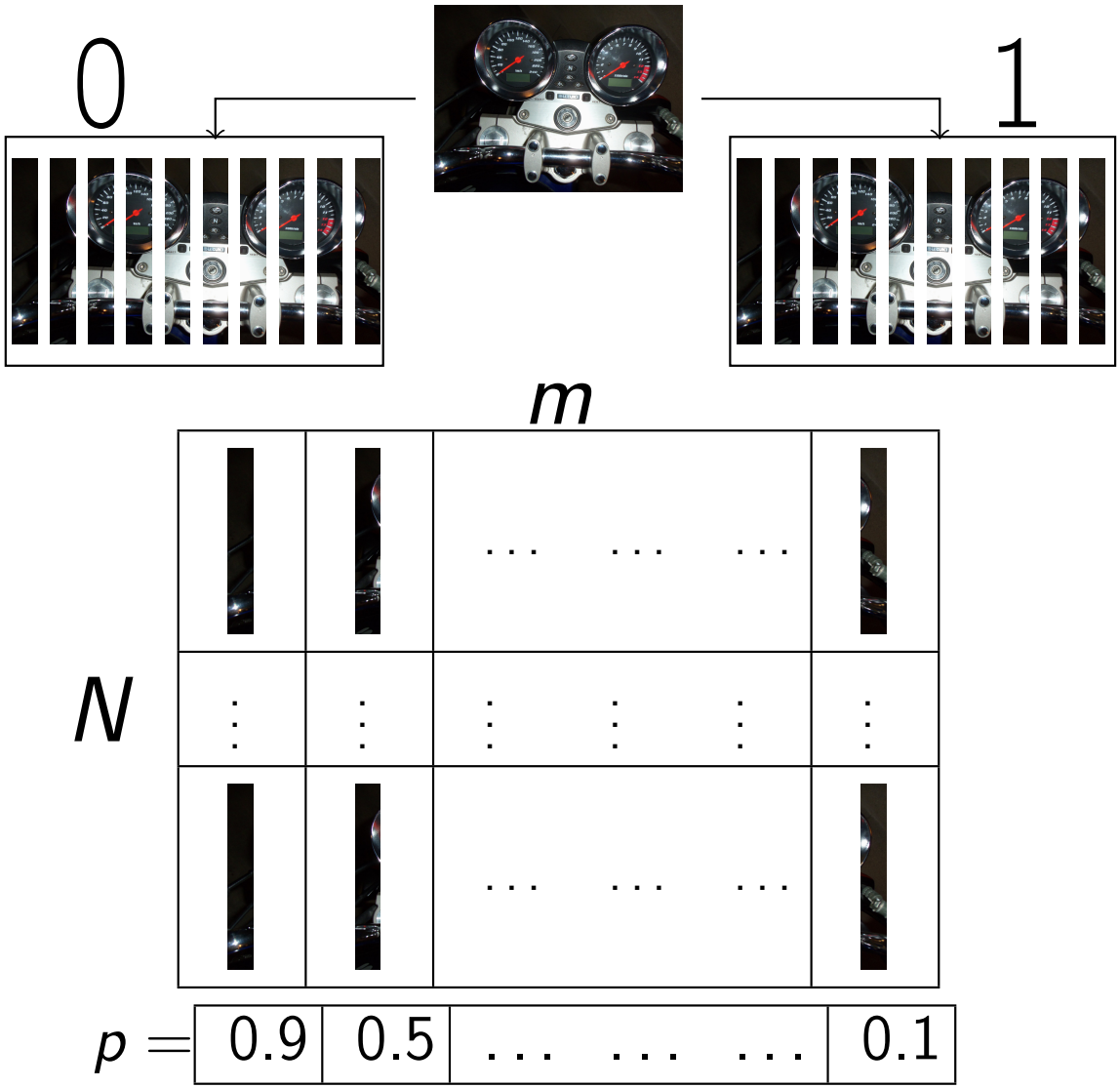


Illustration de la préparation des contenus

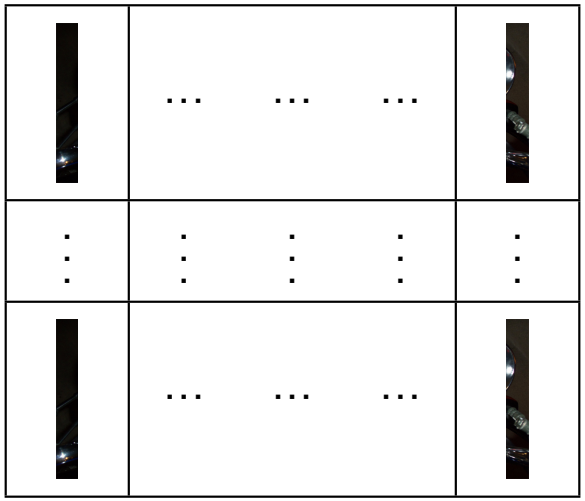
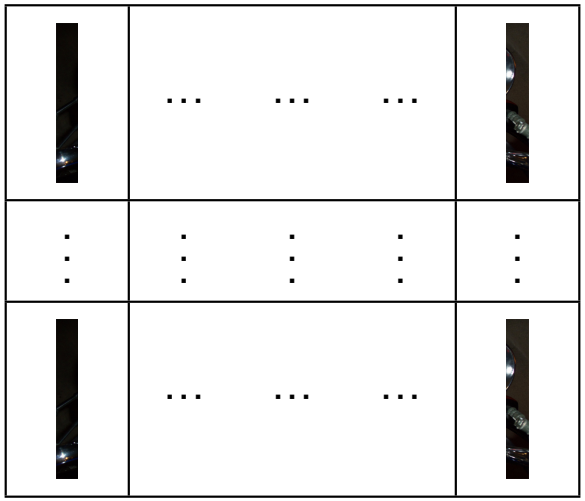
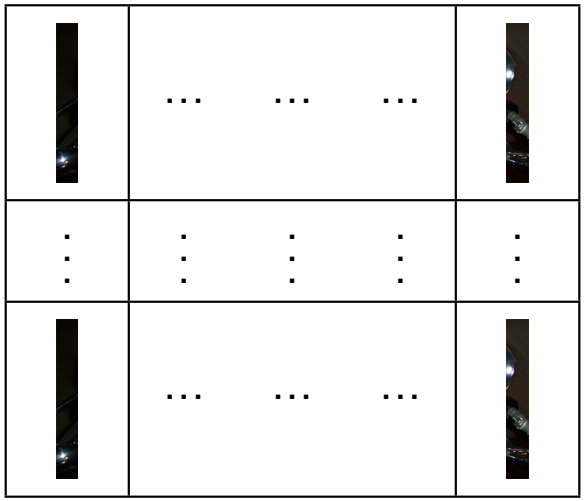


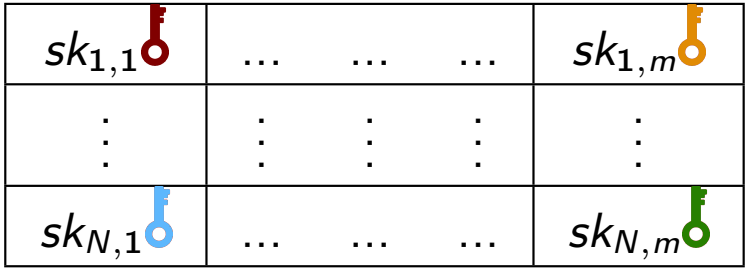
Illustration de la préparation des contenus



$sk_{1,1}$	...	...	$sk_{1,m}$
⋮	⋮	⋮	⋮
$sk_{N,1}$	...	...	$sk_{N,m}$

Illustration de la préparation des contenus





$N \times m$ WORM=

Illustration de la préparation des contenus

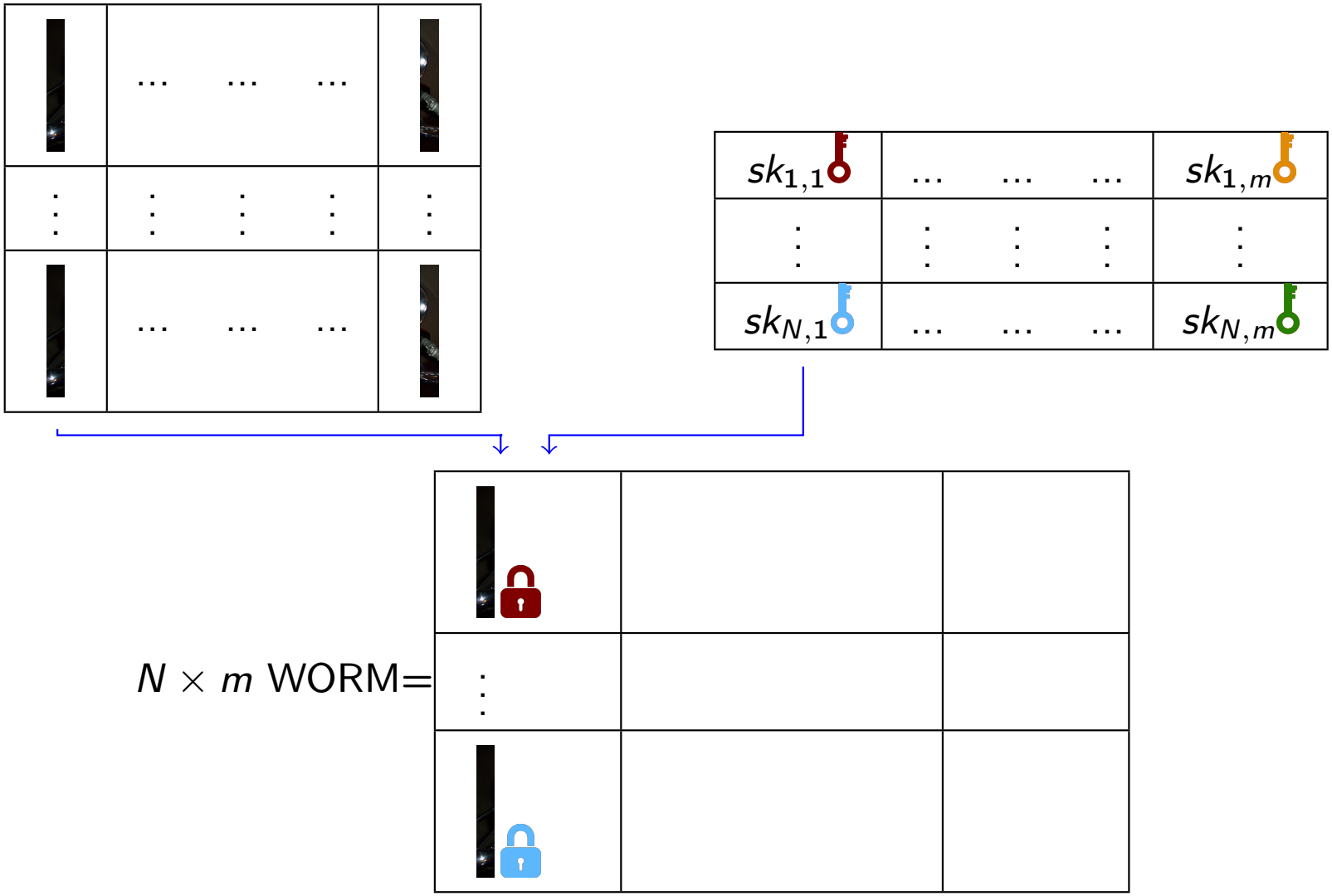
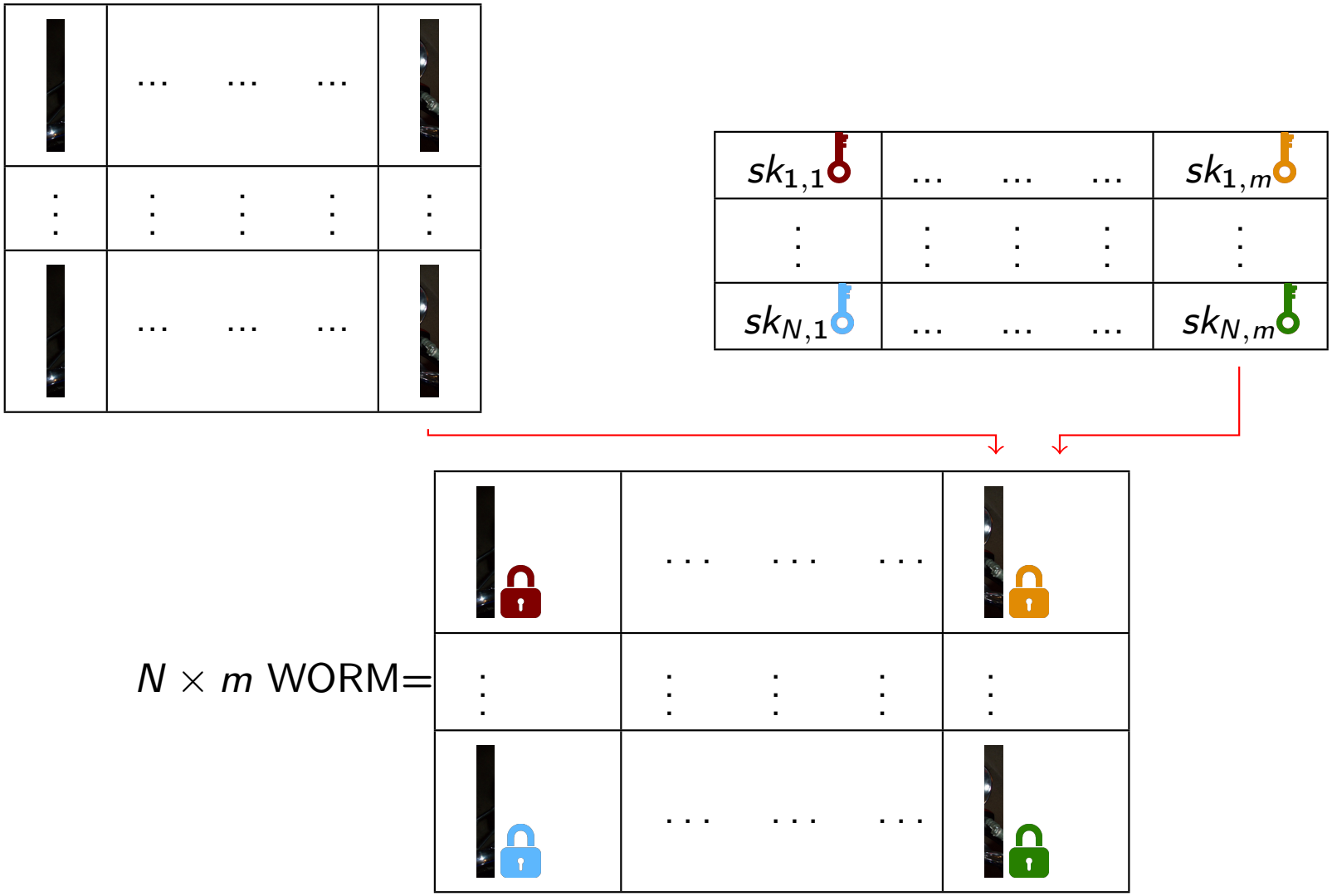
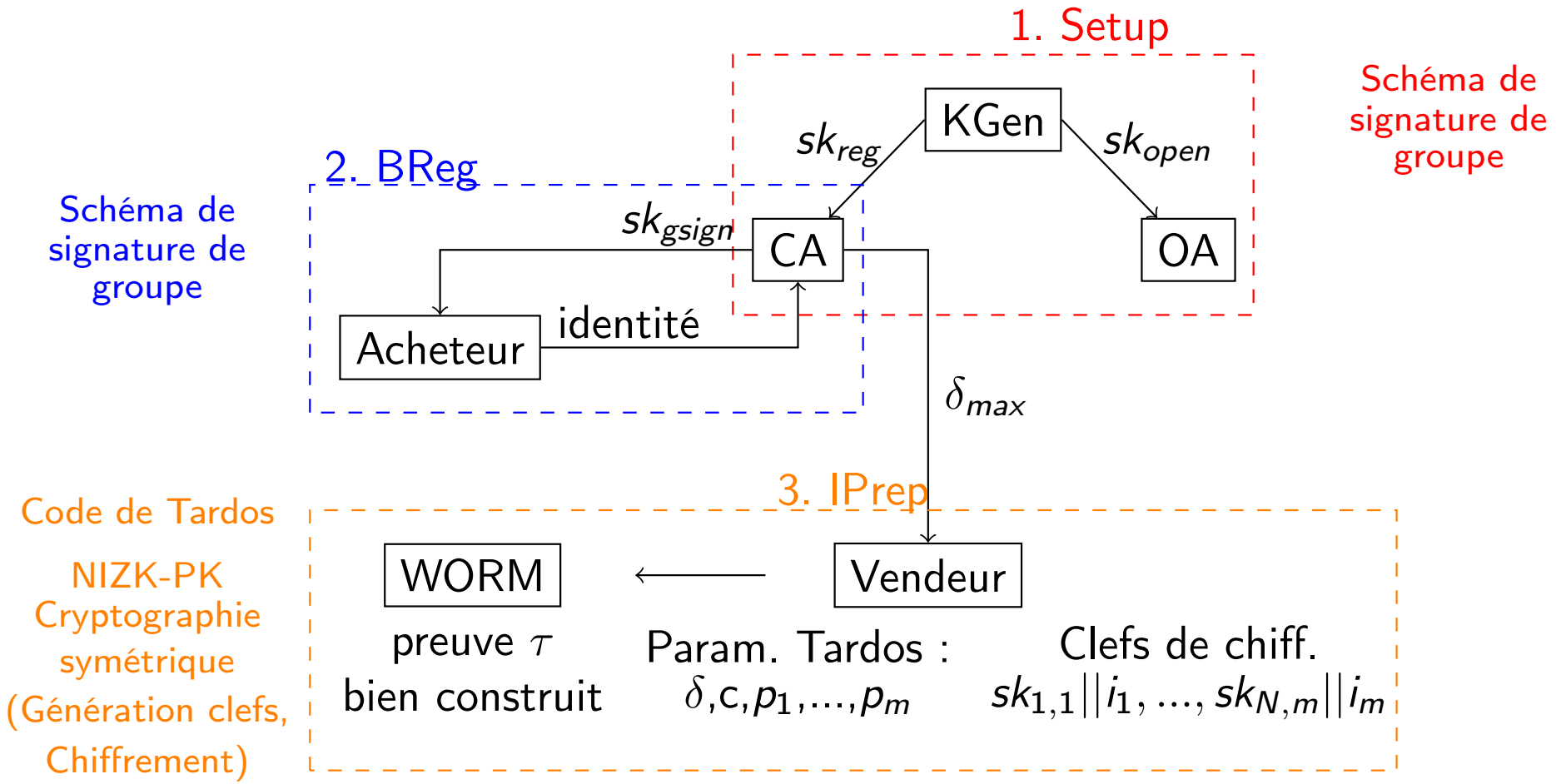


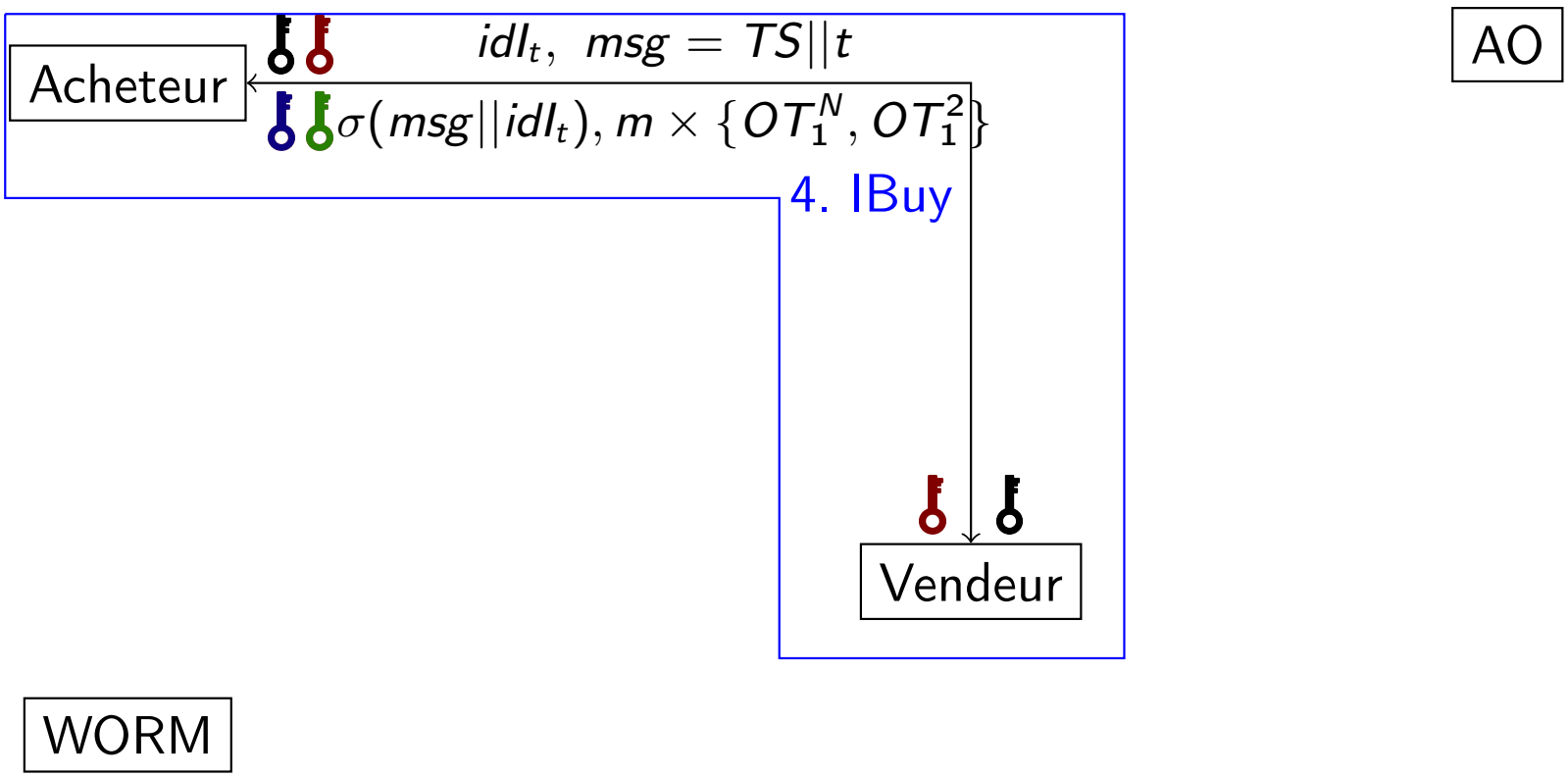
Illustration de la préparation des contenus



Initialisation (Setup) ; Enregistrement des acheteurs (BReg) ; et Préparation des contenus (IPrep)



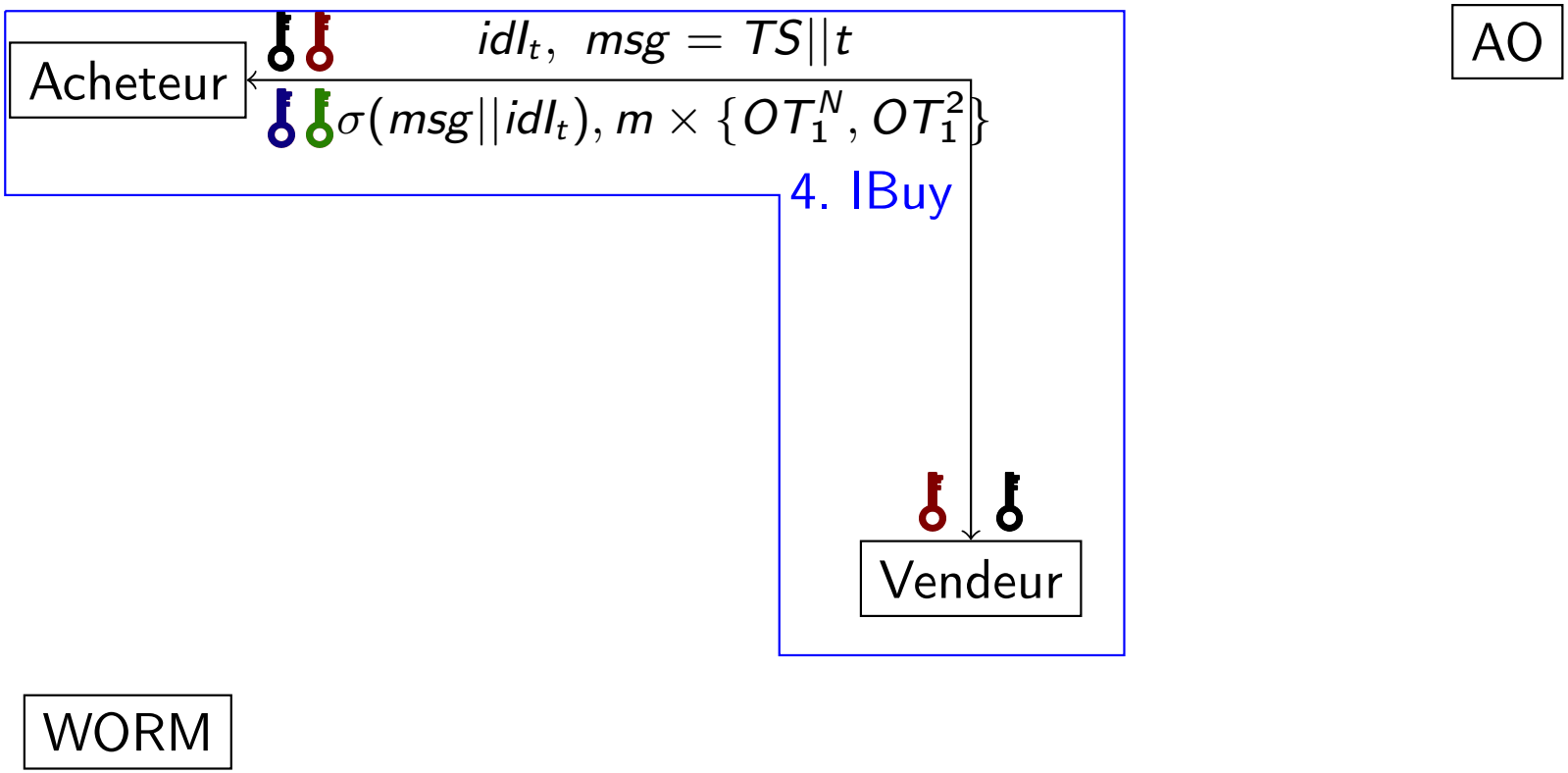
Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)



Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)

NIZK-PK, Transfert Équivoque

Canal anonyme, Signature de groupe



Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)

Acheteur

5. IRecover

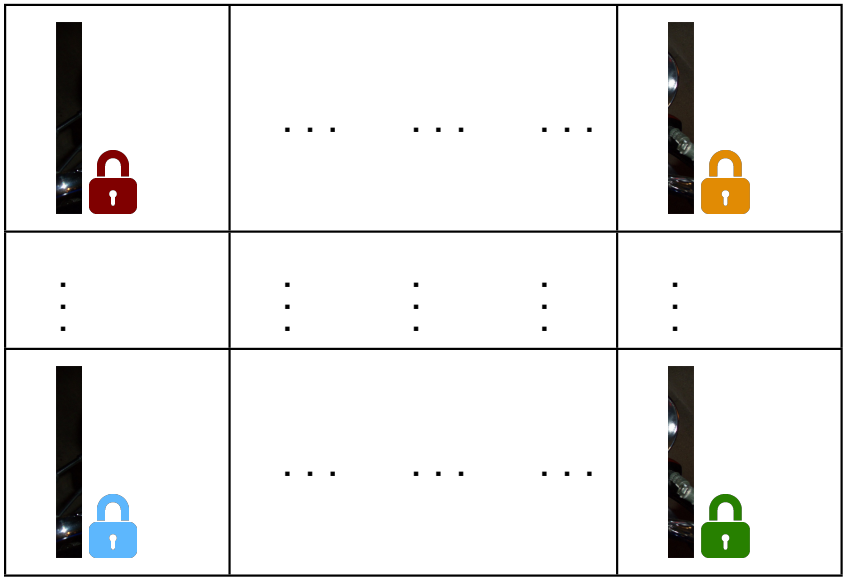

WORM

AO

Vendeur

Illustration de la récupération d'un contenu

WORM



Acheteur

i_1	...	...	...	i_m

Illustration de la récupération d'un contenu

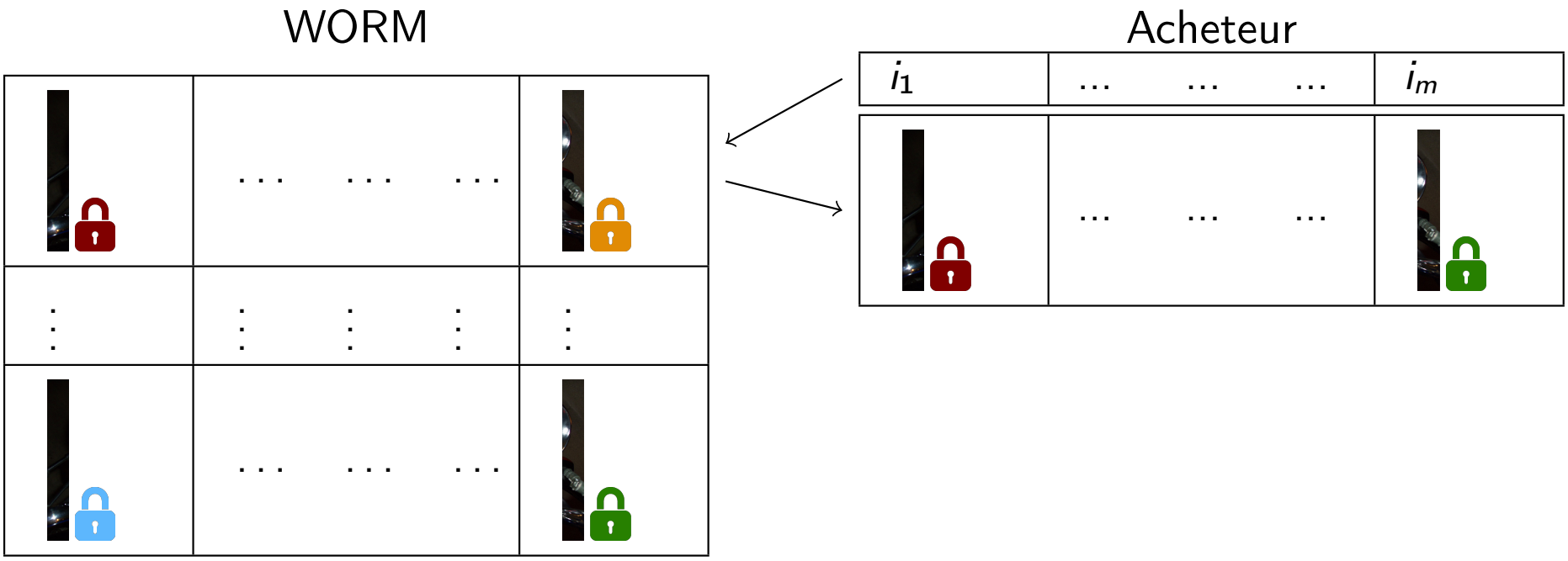


Illustration de la récupération d'un contenu

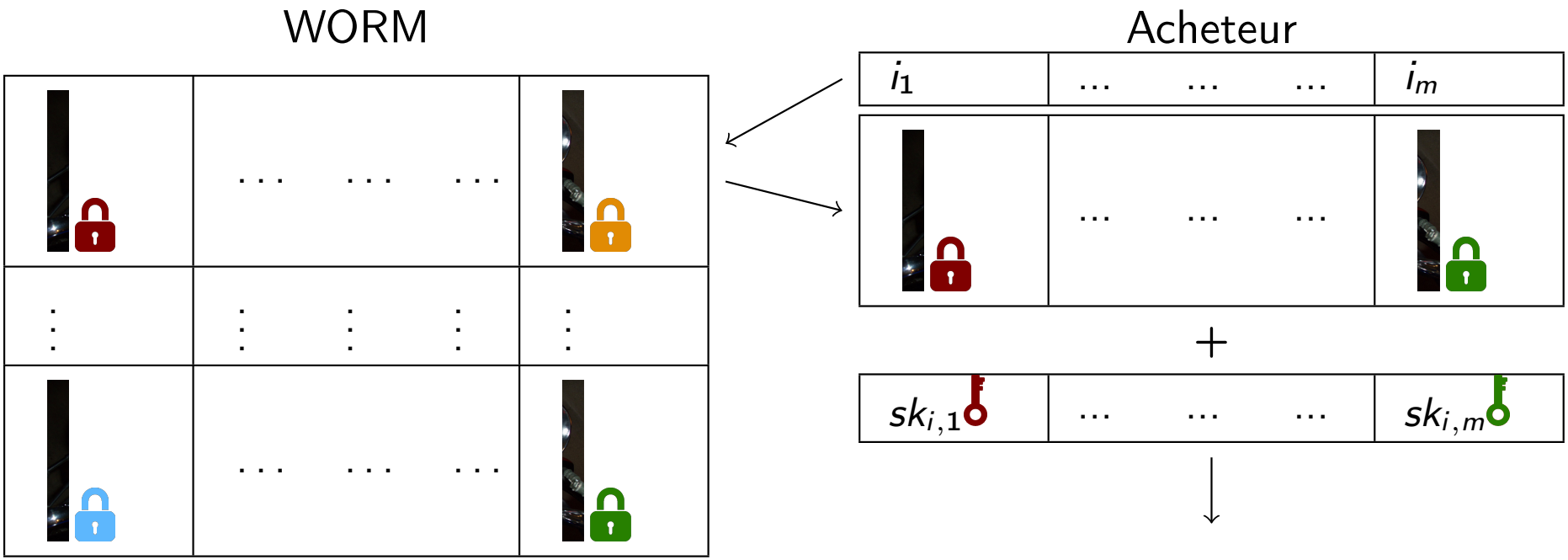


Illustration de la récupération d'un contenu

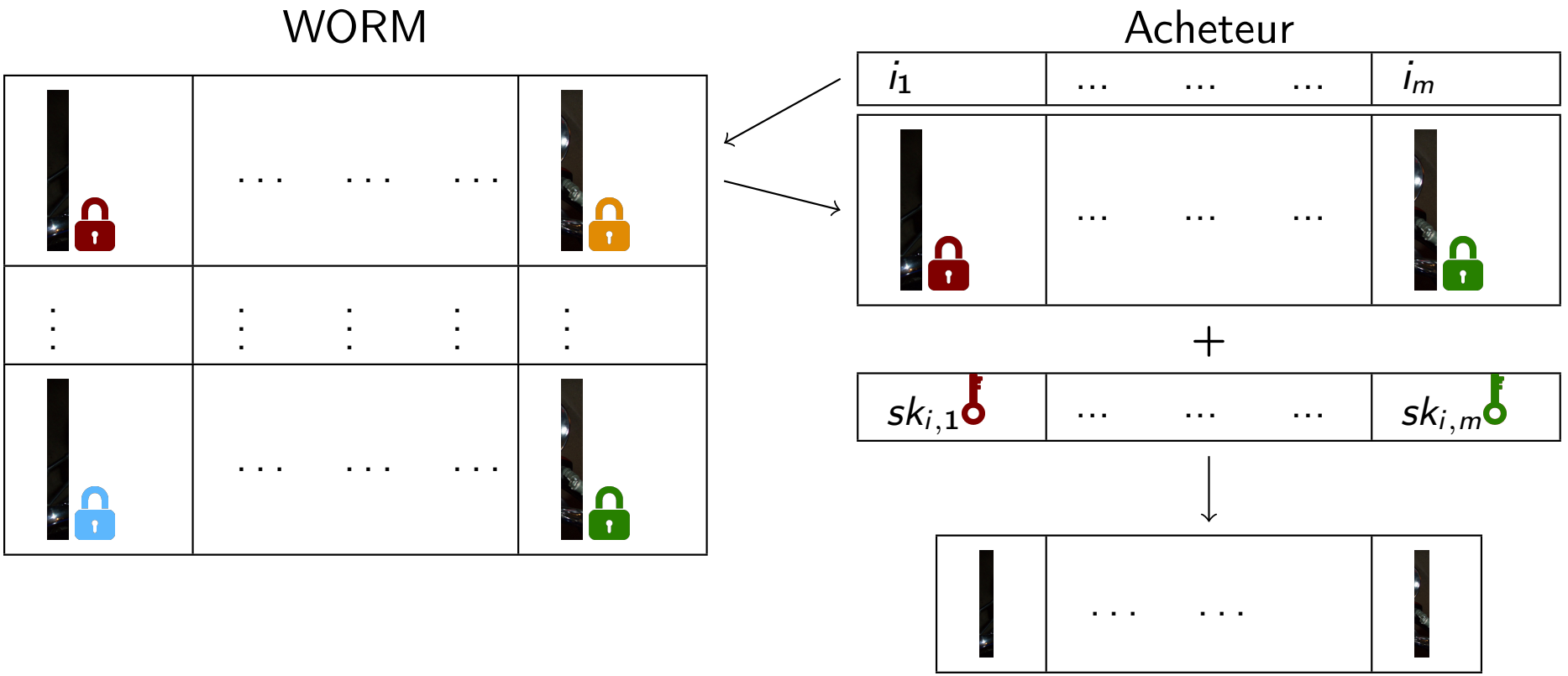
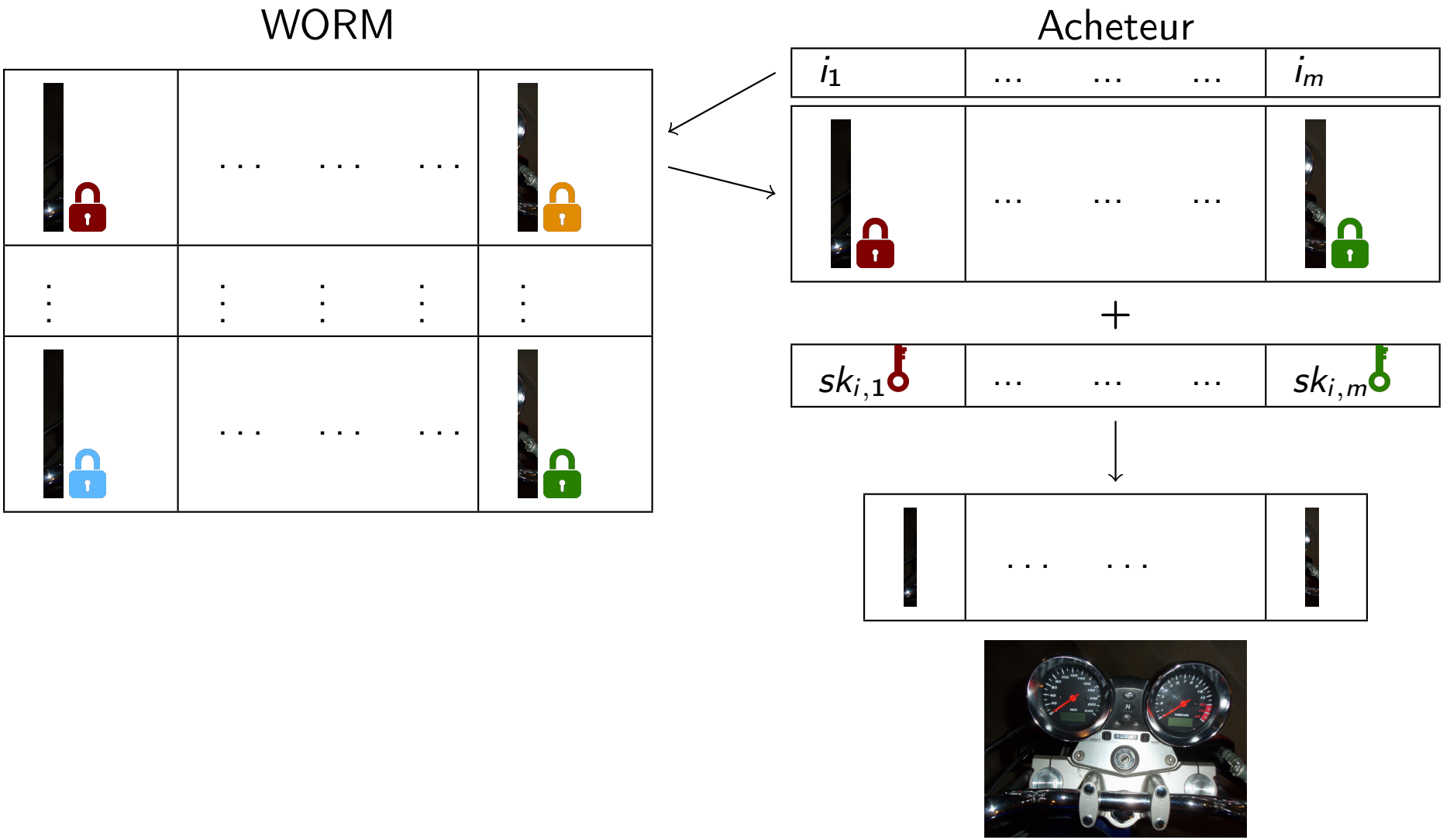
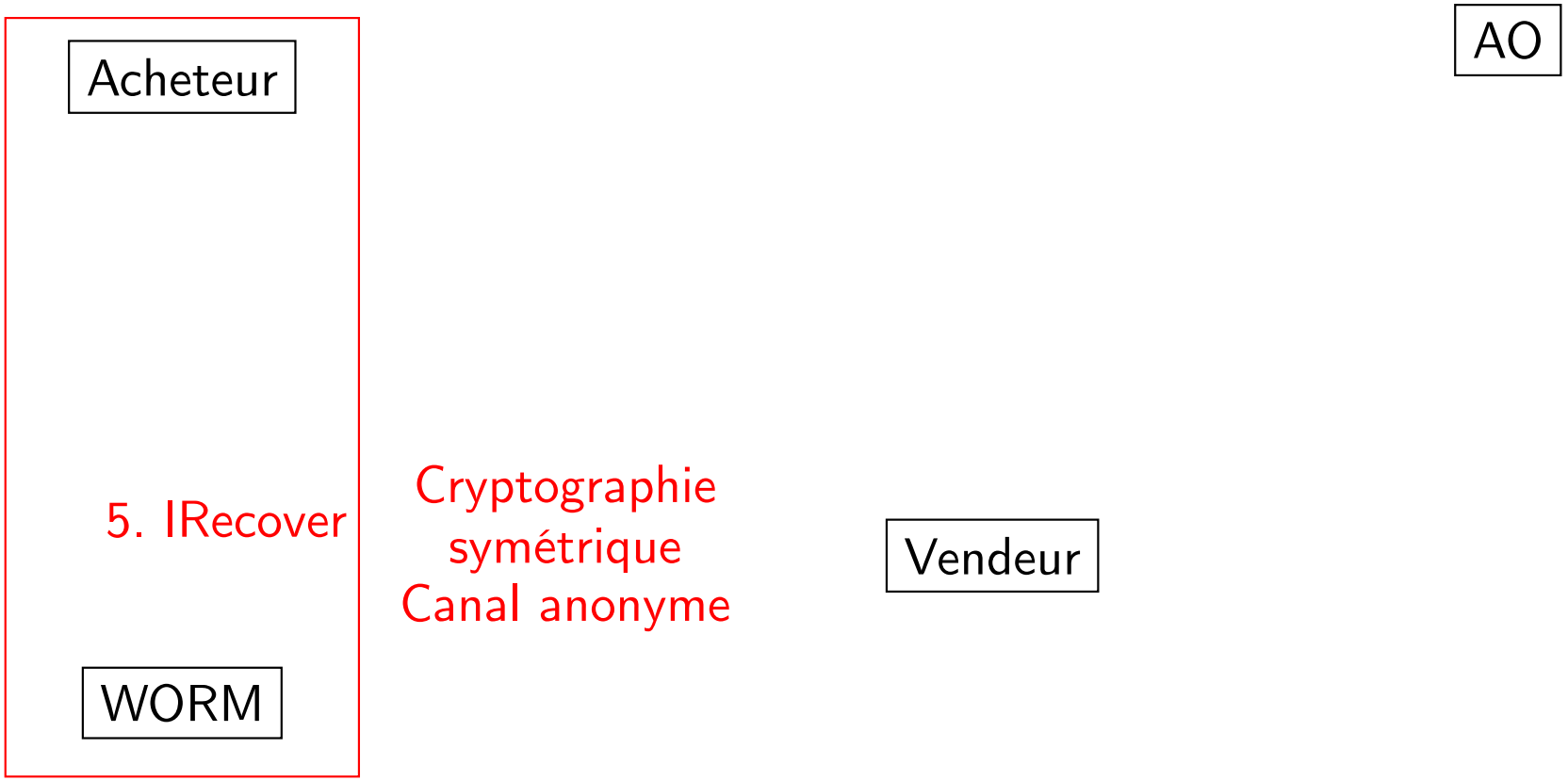


Illustration de la récupération d'un contenu



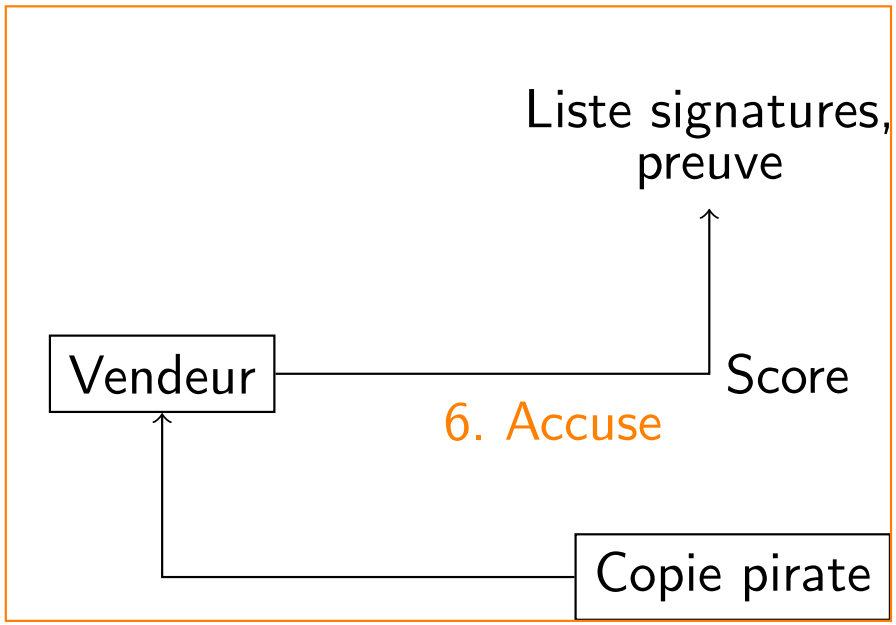
Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)



Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)

Acheteur

AO

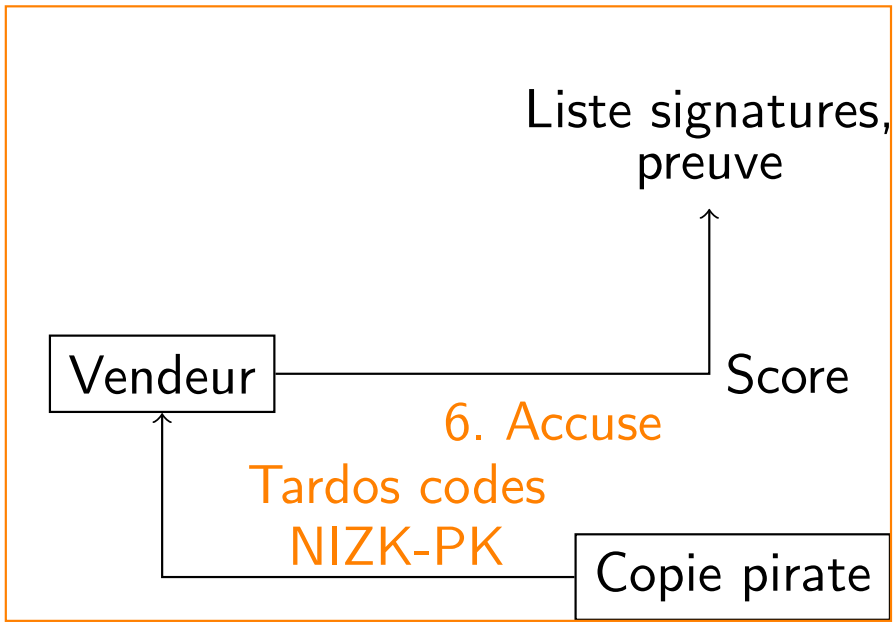


WORM

Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)

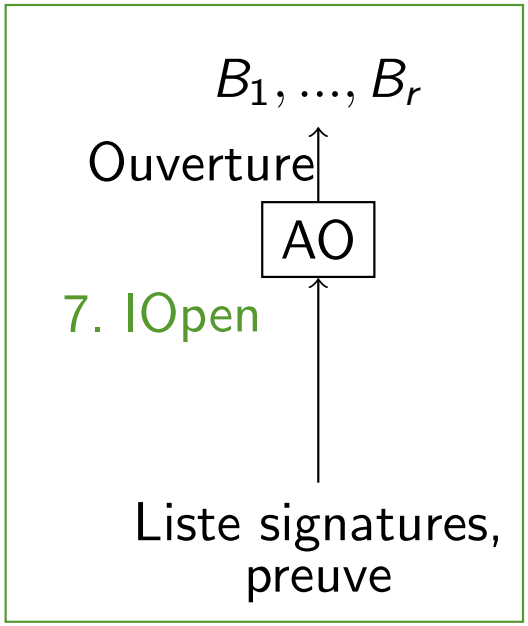
Acheteur

AO



WORM

Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)



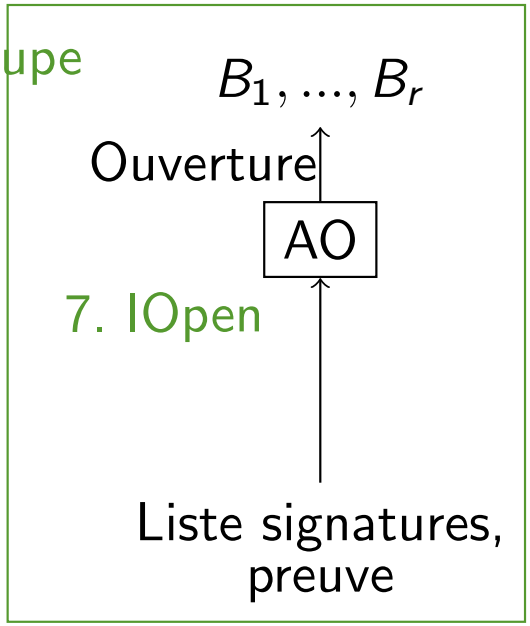
Acheteur

Vendeur

WORM

Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)

Signature de groupe
NIZK-PK
Tardos code

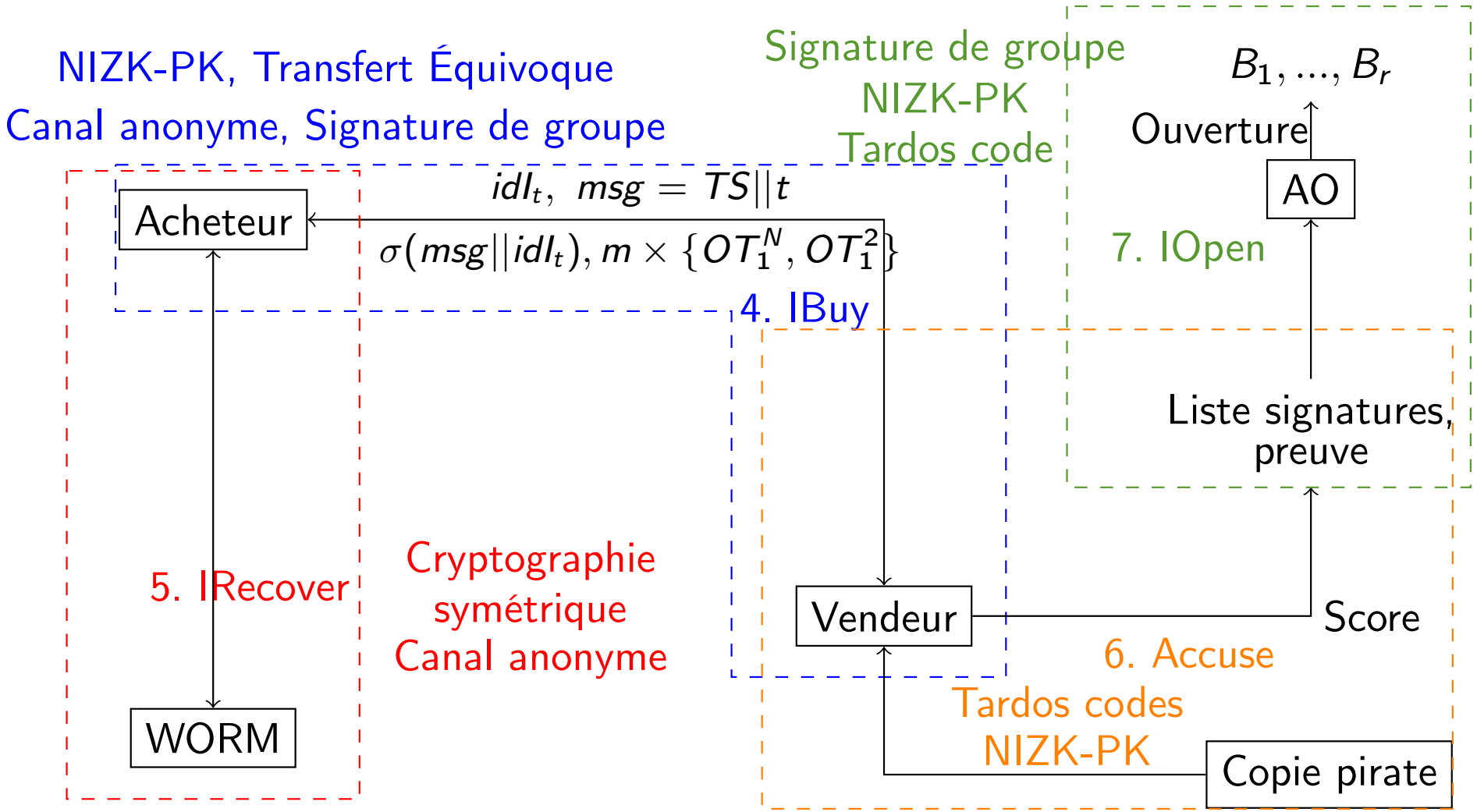


Acheteur

Vendeur

WORM

Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)



Sécurité et de protection de la vie privée

- Traçage de traître : assuré par les codes anti-collusion de Tardos (mot de code unique, identification d'acheteur malveillant, résistance aux collusions).
- *Anti-framing* : protocole asymétrique, utilisation de signature de groupe (infalsifiable, non-répudiation).
- Anonymat révocable et Non-chaînabilité des acheteurs : canal de communication anonyme et signature de groupe (anonyme, non-chaînable).

Propriétés de sécurité et de protection de vie privée formalisées.

Comparaison des propriétés atteintes

	Anti-framing	Traçage de traîtres	Analyse de sécurité formelle	Anonymat révocable	Non-chaînabilité des acheteurs	Compatible avec les codes de Tardos	Implem.
PS 96[a]	V	Oui	X	X	X	X	X
CFFC 11[b]	V	Oui	X	X	X	V	X
PS 97[c]	V	Oui	X	V	V	X	X
RDBPP 10[d]	V	Oui	V	V	V	X	V
AGC 10[e]	V	Non	X	V	V	X	X
PIMENTO	V	Oui	V	V	V	V	P

a : **B. Pfitzmann et M. Schunter**, ***Asymmetric fingerprinting***, **EUROCRYPT, 1996.**

b : **A. Charpentier, C. Fontaine, T. Furon, et I. Cox**, ***An asymmetric fingerprinting scheme based on tardos codes***, **IH, 2011.**

c : **B. Pfitzmann, M. Waidner**, ***Anonymous Fingerprinting***, **EUROCRYPT, 1997.**

d : **A. Rial, M. Deng, T. Bianchi, A. Piva, et B. Preneel**, ***A provably secure anonymous buyer-seller watermarking protocol***, **IEEE Transactions on Information Forensics and Security, 2010.**

e : **W. Abdul, P. Gaborit, et P. Carré**, ***Private anonymous fingerprinting for color images in the wavelet domain***, **SPIE, 2010.**

Implémentation

Implémentation du protocole

- Préparation des contenus (librairie Bouncycastle, notre code : libre, Broken Arrow : libre, mais langage C).
- Initialisation et enregistrement (code de David Schönfeld : libre).
- Achat (notre code : libre, transfert équivoque : code de Lior Malka non libre, NIZK-PK : pas d'implémentation, projet TOR : libre).
- Accusation (notre code :libre).
- Récupération du contenu (notre code : libre).

Performances

Phase	TE (ET)
Initialisation GS	1,57 (0,814)
Enregistrement	0,20 (0,139)
Sign	m $\times 0,43$ (0,034)
m $\times OT_1^2$	m $\times 0,005$ (0,022)
m $\times OT_1^N$	m $\times 0,02$ (0,009)

Table: Temps d'exécution (TE) et écart type (ET) pour différentes phases de PIMENTO (en secondes).

Plateforme de test : Intel i7-2600QM cadencé à 2.40GHz par coeur (un coeur utilisé), 4Go de mémoire vive et Mac OSX Yosemite 64bits.

Sommaire

PIMENTO+ :

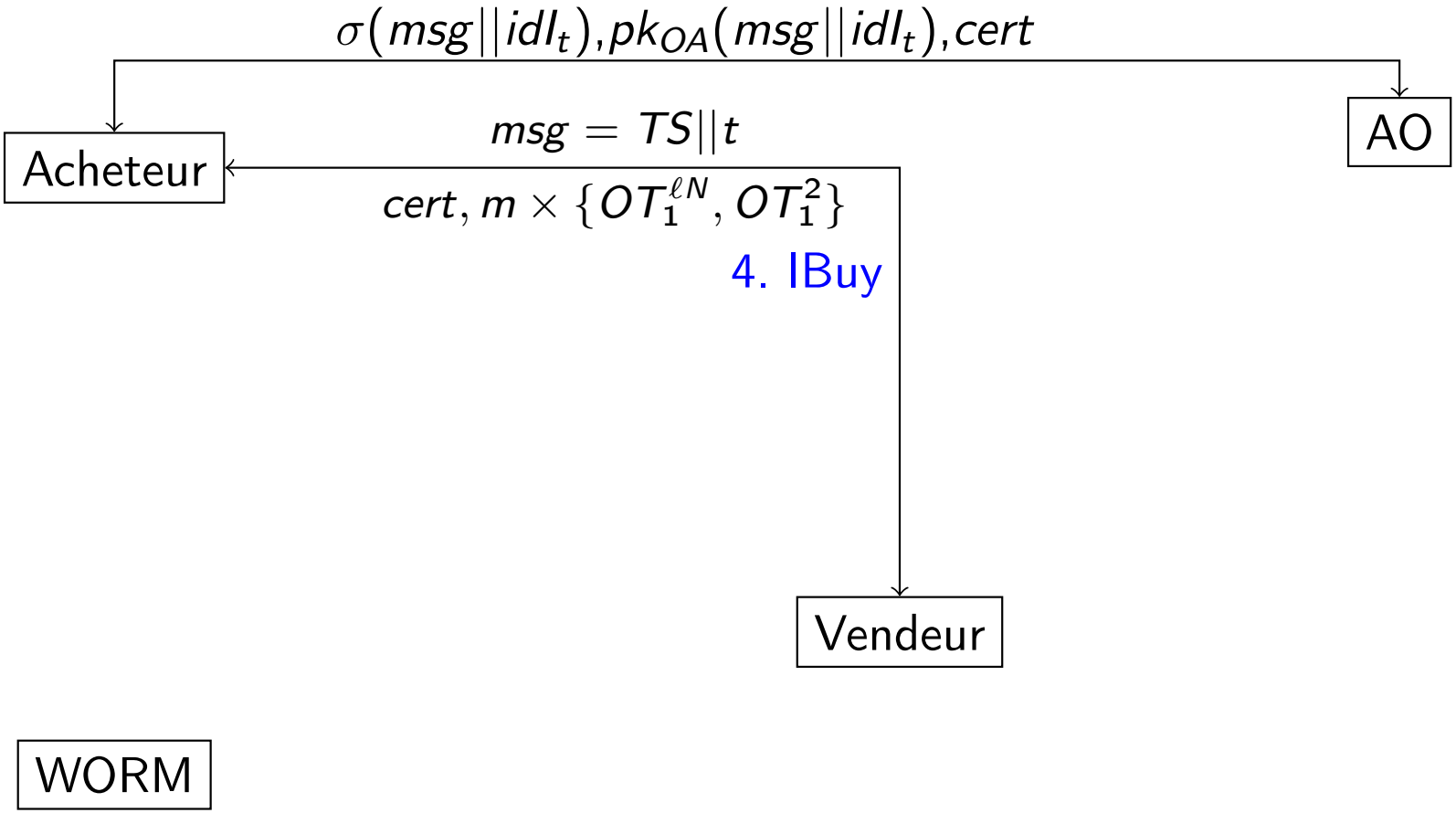
Propriété de protection de la vie privée supplémentaire et différences

- Non-chaînabilité des contenus : le vendeur n'apprend pas quels contenus sont vendus.
- Seulement AGC 10[a], RBP 11[b] et nous avons considéré la propriété de non-chaînabilité des contenus.
- Différences avec PIMENTO :
  - Signature de groupe, certificat.
  - Entrées de l'OT_1^N et de l'OT_1^2.
  - Accusation.

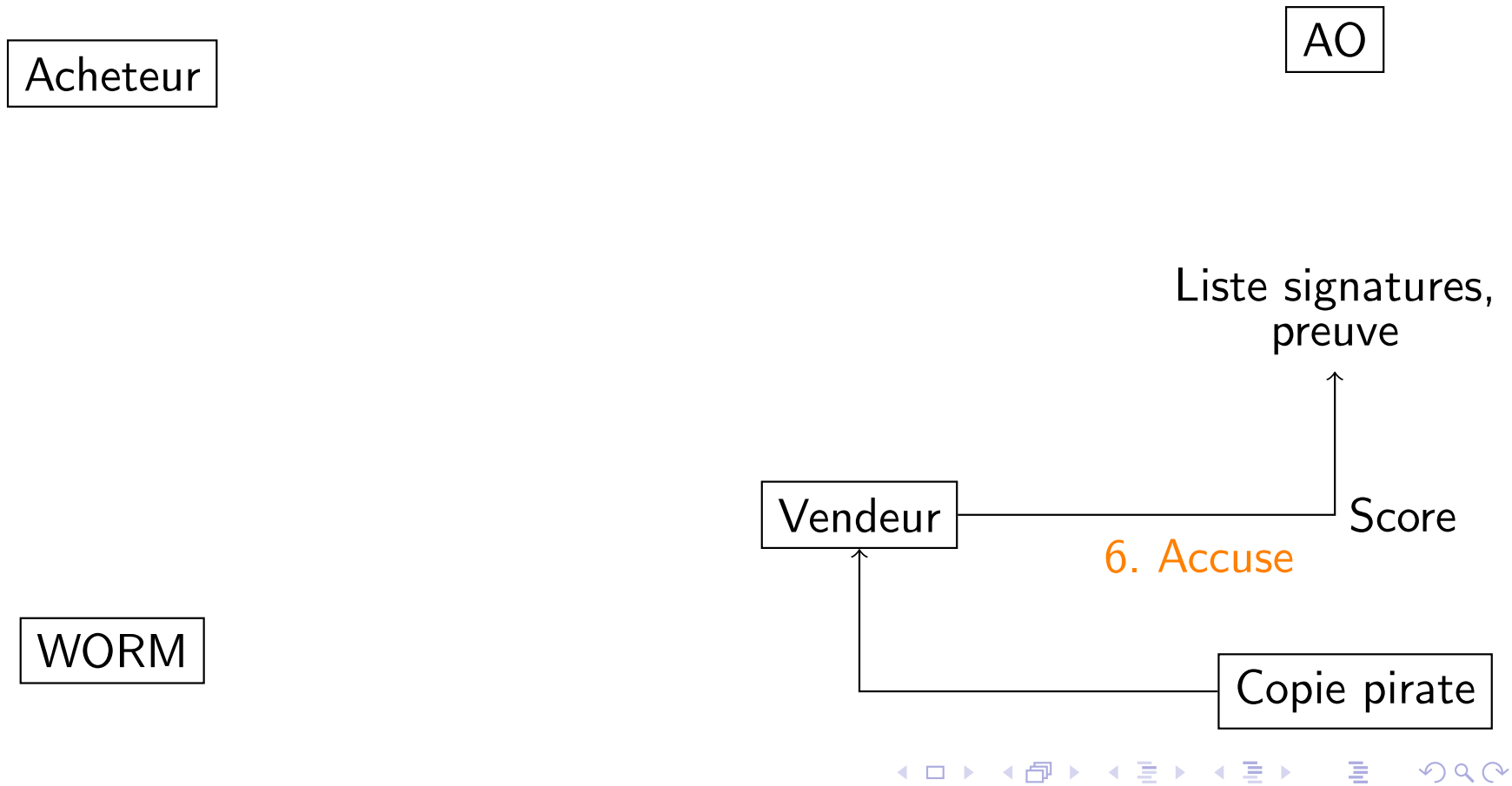
a : **W. Abdul, P. Gaborit, et P. Carré, *Private anonymous fingerprinting for color images in the wavelet domain*, SPIE 2010.**

b : **A. Rial, J. Balasch, et B. Preneel, *A Privacy-Preserving Buyer Seller Watermarking Protocol Based on Priced Oblivious Transfer*, IEEE Transactions on Information Forensics and Security 2011.**

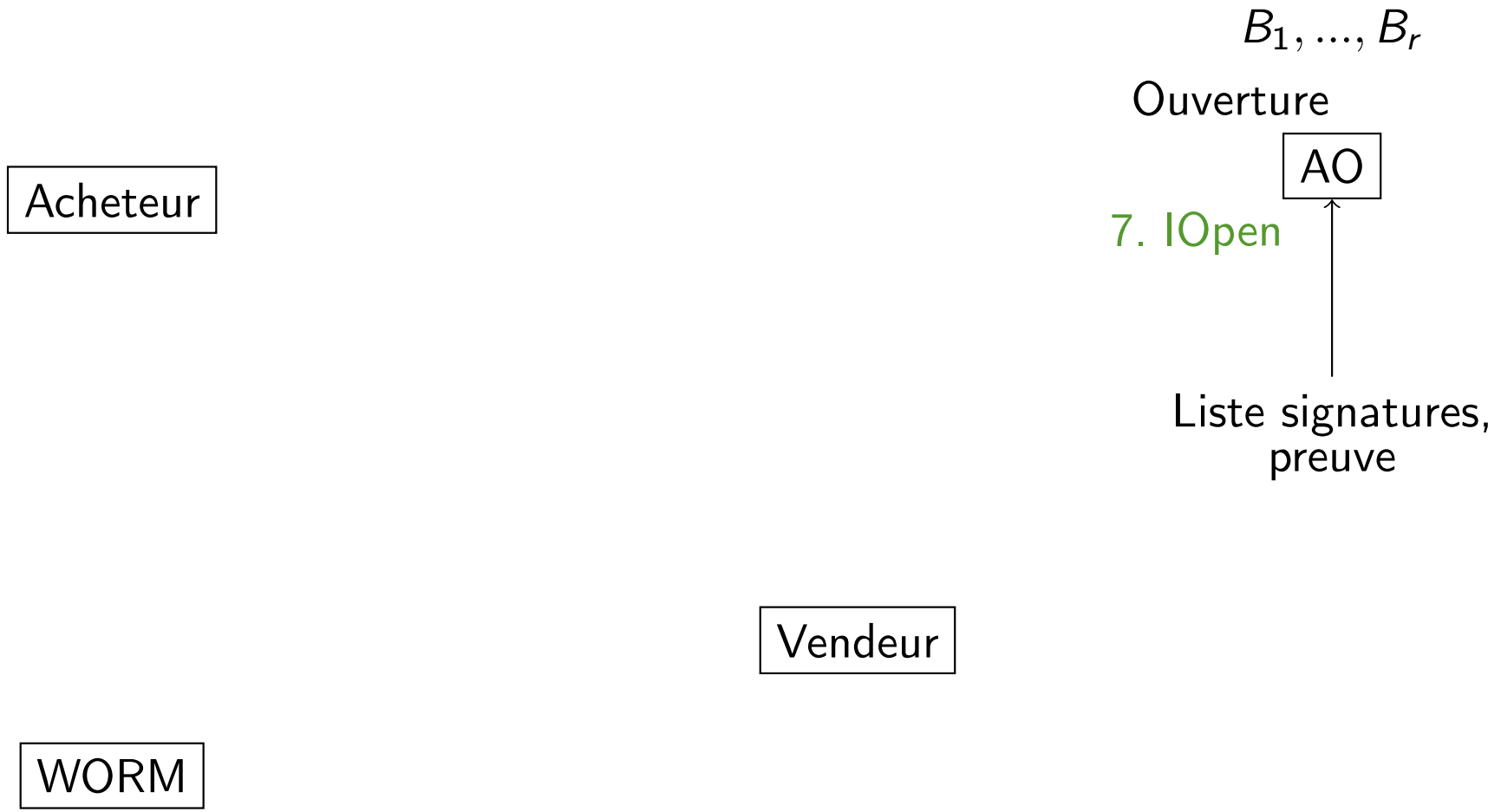
Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)



Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)



Transaction (IBuy) ; Récupération (IRecover) ; Accusation (Accuse) ; et Ouverture (IOpen)



Comparaison des propriétés atteintes

	Anti-framing	Traçage de traîtres	Analyse de sécurité formelle	Anonymat révocable	Non-chaîn. des acheteurs	Non-chaîn. des contenus	Compatible avec les codes de Tardos	Imp.
RBP 11[a]	V	Oui	V	X	X	V	X	V
AGC 10[a]	V	Non	X	V	V	V	X	X
PIMENTO+	V	Oui	V	V	V	V	V	P

a : **A. Rial, J. Balasch, et B. Preneel, *A Privacy-Preserving Buyer Seller Watermarking Protocol Based on Priced Oblivious Transfer*, IEEE Transactions on Information Forensics and Security 2011.**

b : **W. Abdul, P. Gaborit, et P. Carré, *Private anonymous fingerprinting for color images in the wavelet domain*, SPIE, 2010.**

Performance $OT_1^{\ell N}$

ℓN	TE (ET)
20	0,026 (0,009)
200	0,19 (0,005)
400	0,38 (0,008)
600	0,56 (0,011)
800	0,74 (0,011)
1000	0,93 (0,017)

Table: Temps d'exécution (TE) et écart type (ET) pour la phase de transfert équivoque (en secondes).

Plateforme de test : Intel i7-2600QM cadencé à 2.40GHz par coeur (un coeur utilisé), 4Go de mémoire vive et Mac OSX Yosemite 64bits.

Pinocchio...

... un deuxième protocole préservant la vie privée et traçant les traîtres

- Atteins les mêmes propriétés que PIMENTO.
- Conçu pour être plus performant en terme de coût de calcul que PIMENTO.
- Discussion pour un brevet.

Sommaire

Conclusion

- Conception des deux premiers protocoles de personnalisation de contenus préservant la vie privée assurant en même temps :
  - *Anti-framing*.
  - Traçage de traître.
  - Anonymat révocable.
  - Non-chaînabilité des acheteurs.
  - Non-chaînabilité des contenus (PIMENTO+).
  - Compatibilité avec les codes de Tardos.
- Proposition d'un modèle de sécurité.
- Définition du modèle d'adversaire.
- Formalisation des propriétés.
- Preuves que ces protocoles atteignent les propriétés définies.
- Implémentation.

Perspectives futures

PIMENTO

- Diffuser l'implémentation de PIMENTO ? Problème : certains blocs de construction sont non-libre.
- Intégrer un système de recommandation de contenus et un système de réputation préservant la vie privée pour avoir un protocole « complet »type VoD.

Base de données (BDD)

- Personnaliser une BDD assainie avant sa distribution (traçage de traîtres, protection de la vie privée).
- Intégrer l'idée de personnalisation de contenus de BDD dans un protocole tel que PIMENTO pour assurer les propriétés d'*anti-framing*, anonymat révocable, non-chaînabilité.

Valorisations

Internationales

- LATINCRYPT 2014 - *Third International Conference on Cryptology*, Septembre 2014, Flórianopolis.
- Révision de la version journal pour TISSEC (*Transactions on Information and System Security*).

Conférences nationales, séminaires

- JC2S 2013, JC2 2014 et APVP 2014.
- Présentation au séminaire Crypto à l'ENSICAEN et Combinatoire et Algorithmes à l'Université de Rouen.

Pinocchio

- Discussion pour un brevet.
- Publication.

Merci de votre attention
Questions ?

julien.lolive@telecom-bretagne.eu