# Réputation et vie privée dans les réseaux dynamiques auto-organisés

Paul Lajoie-Mazenc

Université de Rennes 1, IRISA, équipe CIDRE

25 septembre 2015

Thèse dirigée par Emmanuelle Anceaume et co-encadrée par Valérie Viet Triem Tong, Gilles Guette et Thomas Sirvent


# Services en ligne

De nombreux services en ligne apparaissent :

- locations (Airbnb)
- covoiturage (Blablacar)
- conseils techniques (StackOverflow)
- commerce et services (Leboncoin)
- intermédiation (Mechanical Turk)

Les clients peuvent choisir des fournisseurs pour obtenir des services

Mais les clients ne savent pas s'ils peuvent faire confiance aux fournisseurs

- qualité du service
- délais de livraison

# Quel vendeur choisir ?


20€

Vendeur : toto35


15€

Vendeur : tagada42

Aucun indice que toto35 est meilleur que tagada42

# Mécanismes de réputation

Après une transaction, les clients peuvent témoigner

- témoignage positif : « le fournisseur s'est bien comporté » (7/10)
- témoignage négatif : « le fournisseur s'est mal comporté » (3/10)

À partir des témoignages, calcul d'un score de réputation (somme, moyenne)

Les réputations permettent aux clients d'effectuer un choix éclairé

# Mécanismes de réputation


20€

7/10

Vendeur : toto35

bar73 : 8/10
pierre84 : 7/10
julie90 : 9/10
alain2 : 5/10
marie78 : 7/10
sylvie65 : 7/10


15€

3,7/10

Vendeur : tagada42

baz4 : 4/10
jean37 : 5/10
anne45 : 2/10
michel20 : 7/10
foo87 : 1/10
alain42 : 3/10

Le service de toto35 coûte plus cher, mais est plus fiable

# Calcul de la réputation

La réputation calculée doit être proche du comportement du fournisseur

Les fournisseurs peuvent essayer :

- d'améliorer leur réputation
- de diminuer la réputation de leurs concurrents

Il faut garantir que le calcul de la réputation est robuste aux attaques

# Indéniabilité des témoignages


20€

8/10

Vendeur : toto35

marie72 : 7/10
jean39 : 9/10

Est-on sûr que toutes les transactions sont représentées ?

- Des clients n'ont pas pu témoigner de leur mécontentement
- D'autres n'ont pas voulu témoigner

Indéniabilité des témoignages

- Les clients peuvent toujours témoigner
- Les fournisseurs peuvent obtenir une preuve de leurs transactions

# Indéniabilité des témoignages


20€

5,3/10

Vendeur : toto35

marie72 : 7/10
jean39 : 9/10
julie50 : 3/10
michel97 : 2/10

Est-on sûr que toutes les transactions sont représentées ?

- Des clients n'ont pas pu témoigner de leur mécontentement
- D'autres n'ont pas voulu témoigner

## Indéniabilité des témoignages

- Les clients peuvent toujours témoigner
- Les fournisseurs peuvent obtenir une preuve de leurs transactions

# Indéniabilité des témoignages


20€

7,3/10

Vendeur : toto35

marie72 : 7/10
jean39 : 9/10
julie50 : 3/10
michel97 : 2/10
anne43 : 10/10
alain88 : 10/10
pierre44 : 10/10

Est-on sûr que toutes les transactions sont représentées ?

- Des clients n'ont pas pu témoigner de leur mécontentement
- D'autres n'ont pas voulu témoigner

## Indéniabilité des témoignages

- Les clients peuvent toujours témoigner
- Les fournisseurs peuvent obtenir une preuve de leurs transactions

# Indéniabilité des témoignages


20€

7,3/10

Vendeur : toto35

marie72 : 7/10
jean39 : 9/10
julie50 : 3/10
michel97 : 2/10
anne43 : 10/10
alain88 : 10/10
pierre44 : 10/10

Est-on sûr que toutes les transactions sont représentées ?

- Des clients n'ont pas pu témoigner de leur mécontentement
- D'autres n'ont pas voulu témoigner

## Indéniabilité des témoignages

- Les clients peuvent toujours témoigner
- Les fournisseurs peuvent obtenir une preuve de leurs transactions

# Inforgeabilité des témoignages


20€

6,8/10

Vendeur : toto35

foo55 : 9/10
pierre97 : 3/10
alain60 : 8/10
anne59 : 9/10
julie12 : 4/10
baz40 : 8/10

Les témoignages sont-ils légitimes ?

- ils ont effectivement été émis par les clients
- ils n'ont pas été modifiés

Inforgeabilité des témoignages

- Les témoignages sont légitimes
- Les témoignages et la réputation n'ont pas été modifiés

# Inforgeabilité des témoignages


20€

6,8/10

Vendeur : toto35

foo55 : 9/10
pierre97 : 3/10
alain60 : 8/10
anne59 : 9/10
julie12 : 4/10
baz40 : 8/10

Les témoignages sont-ils légitimes ?

- ils ont effectivement été émis par les clients
- ils n'ont pas été modifiés

Inforgeabilité des témoignages

- Les témoignages sont légitimes
- Les témoignages et la réputation n'ont pas été modifiés

# Inforgeabilité des témoignages


20€

5/10

Vendeur : toto35

pierre97 : 3/10

julie12 : 4/10

baz40 : 8/10

Les témoignages sont-ils légitimes ?

- ils ont effectivement été émis par les clients
- ils n'ont pas été modifiés

## Inforgeabilité des témoignages

- Les témoignages sont légitimes
- Les témoignages et la réputation n'ont pas été modifiés

# Inforgeabilité des témoignages


20€

3/10

Vendeur : toto35

pierre97 : 3/10

julie12 : 4/10

baz40 : 2/10

Les témoignages sont-ils légitimes ?

- ils ont effectivement été émis par les clients
- ils n'ont pas été modifiés

Inforgeabilité des témoignages

- Les témoignages sont légitimes
- Les témoignages et la réputation n'ont pas été modifiés

# Inforgeabilité des témoignages


20€

3/10

Vendeur : toto35

pierre97 : 3/10

julie12 : 4/10

baz40 : 2/10

Les témoignages sont-ils légitimes ?

- ils ont effectivement été émis par les clients
- ils n'ont pas été modifiés

## Inforgeabilité des témoignages

- Les témoignages sont légitimes
- Les témoignages et la réputation n'ont pas été modifiés

# Associabilité des témoignages


20€

6,7/10

Vendeur : toto35

sylvie58 : 8/10
marie19 : 1/10
sylvie58 : 10/10
pierre68 : 3/10
sylvie58 : 9/10
sylvie58 : 9/10

`sylvie58` a témoigné 4 fois !

Si on ne prend qu'un témoignage en compte, la réputation change drastiquement

## Associabilité des témoignages

- Savoir si deux témoignages émis sur le même fournisseur viennent du même client

# Associabilité des témoignages


20€

6,7/10

Vendeur : toto35

sylvie58 : 8/10
marie19 : 1/10
sylvie58 : 10/10
pierre68 : 3/10
sylvie58 : 9/10
sylvie58 : 9/10

`sylvie58` a témoigné 4 fois !

Si on ne prend qu'un témoignage en compte, la réputation change drastiquement

## Associabilité des témoignages

- Savoir si deux témoignages émis sur le même fournisseur viennent du même client

# Associabilité des témoignages


20€

4/10

Vendeur : toto35

sylvie58 : 8/10
marie19 : 1/10

pierre68 : 3/10

`sylvie58` a témoigné 4 fois !

Si on ne prend qu'un témoignage en compte, la réputation change drastiquement

## Associabilité des témoignages

- Savoir si deux témoignages émis sur le même fournisseur viennent du même client

# Associabilité des témoignages


20€

4/10

Vendeur : toto35

sylvie58 : 8/10
marie19 : 1/10

pierre68 : 3/10

`sylvie58` a témoigné 4 fois !

Si on ne prend qu'un témoignage en compte, la réputation change drastiquement

## Associabilité des témoignages

- Savoir si deux témoignages émis sur le même fournisseur viennent du même client

# Réputation et vie privée

Les mécanismes existants nécessitent des données personnelles :

- identifiants uniques, même s'ils sont décorrélés des identités
- transactions : services obtenus, dates, etc.
- témoignages

Elles permettent de reconstruire les profils des utilisateurs ou de discriminer

Quelles informations sont vraiment nécessaires ?
Quelles propriétés de vie privée sont attendues ?

# Propriétés de vie privée

## Remarque sur l'associabilité des témoignages

Ne nécessite pas :

- de savoir qui est le client
- d'associer les témoignages émis sur différents fournisseurs

## Vie privée des clients

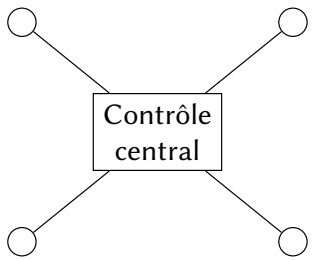
- Les interactions avec différents fournisseurs ne sont pas associables
- Au moment de la transaction, deux clients sont indistinguables

## Vie privée des fournisseurs

Au moment où un client note un fournisseur, deux fournisseurs de même réputation sont indistinguables

# Réseaux dynamiques auto-organisés

## Architecture centralisée



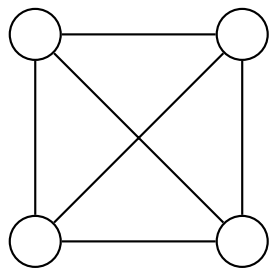

Avantages :

- Collecte des témoignages
- Calcul des réputations

Limites :

- Point unique de défaillance
  - ↪ sécurité, vie privée

## Architecture distribuée



Avantages :

- Gestion par les utilisateurs
- Tolère les comportements malveillants

Limites :

- Algorithmes plus complexes

# Mécanisme de réputation robuste préservant la vie privée

## Distribué

## Préservant la vie privée

- des clients
- des fournisseurs

## Permettant un calcul précis des réputations

- indéniabilité des témoignages
- inforgeabilité des témoignages et des scores de réputation
- associabilité des témoignages

# Travaux existants

| Mécanisme | Distribué | Vie privée | Indéniabilité | Inforgeabilité | Associabilité |
|---|---|---|---|---|---|
| [HBBS13] | ✔ | ✗ | ✔/✗ | ✔ | ✔ |
| [ACBM08] | ✗ | ✔ | ✗ | ✔ | ✗ |
| [BSS10] | ✔ | ✔ | ✗ | ✔ | ✔ |

Jusqu'à présent, aucun mécanisme n'est parvenu à combiner

- l'aspect distribué
- la vie privée des utilisateurs
- l'indéniabilité des témoignages

---

[HBBS13] : Hasan, Brunie, Bertino, Shang : *A Decentralized Privacy Preserving Reputation Protocol for the Malicious Adversarial Model*. IEEE Transactions on Information Forensics and Security, Vol. 8, 2013.

[ACBM08] : Androulaki, Choi, Bellovin, Malkin : *Reputation Systems for Anonymous Networks*. Privacy Enhancing Technologies, 2008.

[BSS10] : Bethencourt, Shi and Song : *Signatures of Reputation*. Financial Cryptography and Data Security, 2010.

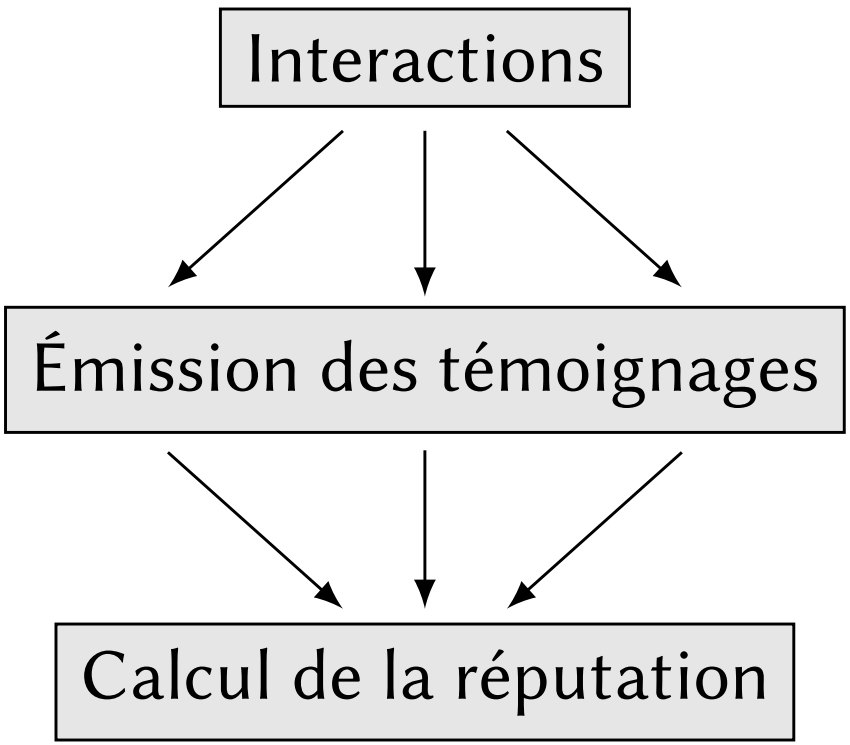
# Contributions de ma thèse

1. Formalisation des propriétés de sécurité et de vie privée
2. Premier mécanisme préservant la vie privée des clients
   - Atelier Protection de la Vie Privée (APVP), juin 2012
   - IEEE International Conference on Communications (IEEE ICC), juin 2013
3. Principes généraux permettant de garantir les propriétés définies
   - Poster à la conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SAR-SSI), septembre 2013
   - Journal IFIP : Privacy and Identity Management for Emerging Solutions and Technologies, juin 2013
4. Mécanisme de réputation
   - Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel), juin 2015
   - IEEE International Symposium on Network Computing and Applications (IEEE NCA), septembre 2015
5. Preuves de garantie des propriétés de sécurité et de vie privée
6. Analyse des performances
   - IFIP International Conference on Trust Management (IFIP TM), mai 2015

# Plan de la présentation

1. Formalisation des propriétés de sécurité et de vie privée
2. Premier mécanisme préservant la vie privée des clients
   - Atelier Protection de la Vie Privée (APVP), juin 2012
   - IEEE International Conference on Communications (IEEE ICC), juin 2013
3. Principes généraux permettant de garantir les propriétés définies
   - Poster à la conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SAR-SSI), septembre 2013
   - Journal IFIP : Privacy and Identity Management for Emerging Solutions and Technologies, juin 2013
4. Mécanisme de réputation
   - Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel), juin 2015
   - IEEE International Symposium on Network Computing and Applications (IEEE NCA), septembre 2015
5. Preuves de garantie des propriétés de sécurité et de vie privée
6. Analyse des performances
   - IFIP International Conference on Trust Management (IFIP TM), mai 2015

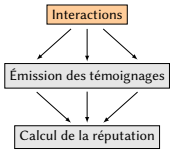
# Architecture d'un mécanisme de réputation




indéniabilité

associabilité

inforgeabilité




# Indéniabilité et vie privée

## Les clients

- ne doivent pas savoir avec qui ils interagissent
- mais doivent être capables de témoigner sur le bon fournisseur

## Les fournisseurs

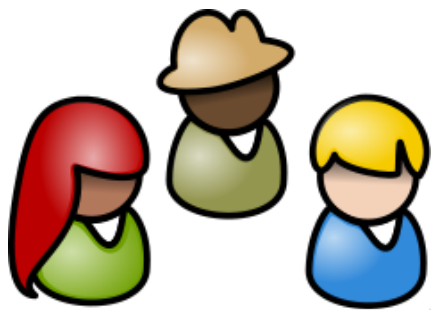
- ne doivent pas connaître leurs clients
- mais doivent être capables d'obtenir une preuve de leurs transactions

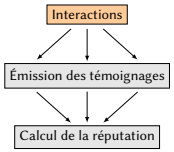
## Solution

Une tierce partie distribuée, choisie :

- aléatoirement
- parmi les fournisseurs (charge minimale)

les porteurs de part






# Porteurs de part

L'ensemble des porteurs de part doit permettre de construire le témoignage

Mais un porteur de part malveillant ne doit pas pouvoir

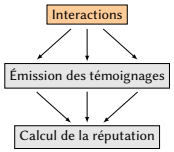
- permettre de construire un témoignage trop tôt (vie privée)
- empêcher de construire un témoignage (indéniabilité)

## Partage de secret

Un secret est divisé en $n$ parts, distribuées aux porteurs de part

- Avec moins de $t$ parts, aucune information sur le secret
- Avec $t$ parts, on peut le reconstruire

Dans notre cas, on prend $t = \lceil n/3 \rceil$

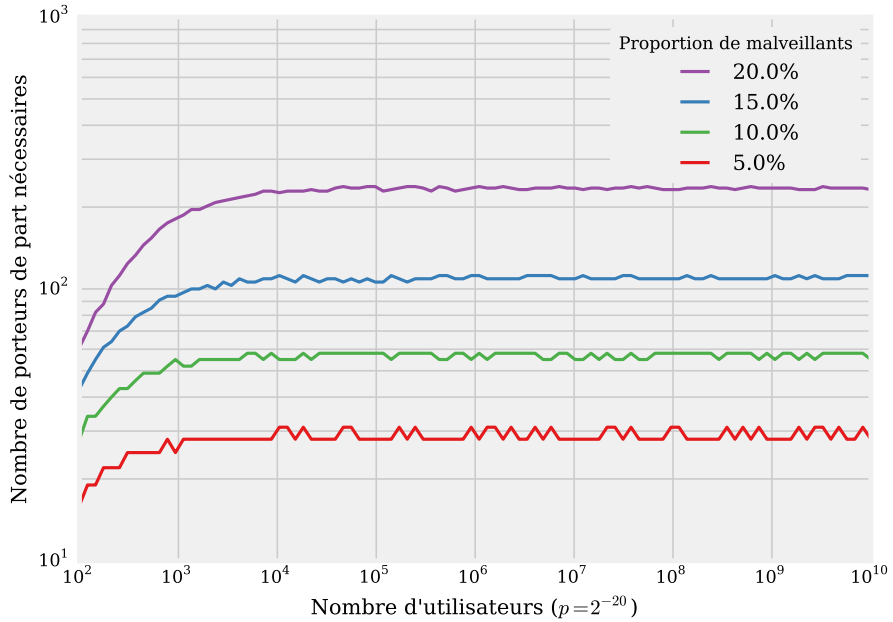


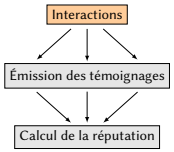

# Choisir les porteurs de part

## Nombre nécessaire

Dépend des paramètres :

- Nombre d'utilisateurs
- Nombre de malveillants
- Probabilité de collusion réussie



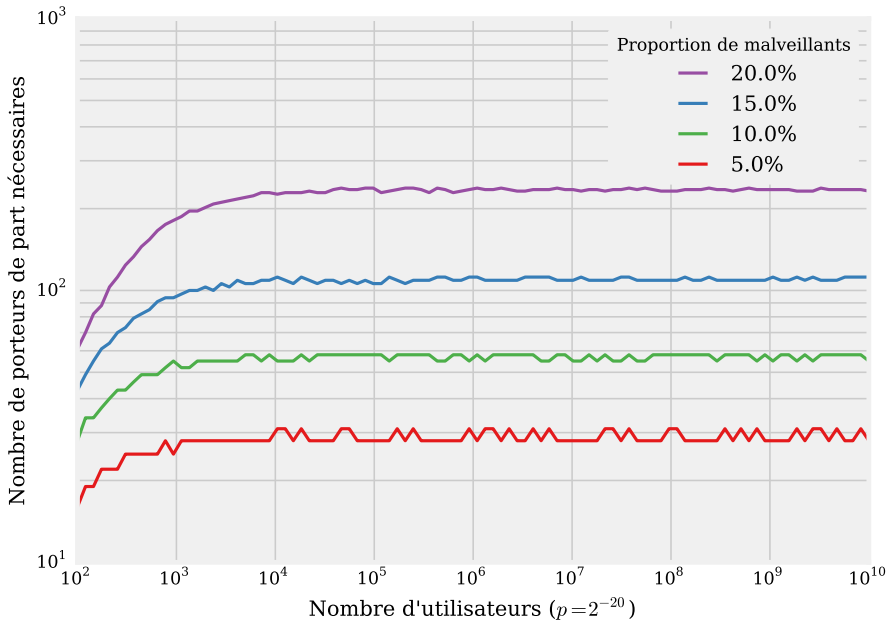



# Choisir les porteurs de part

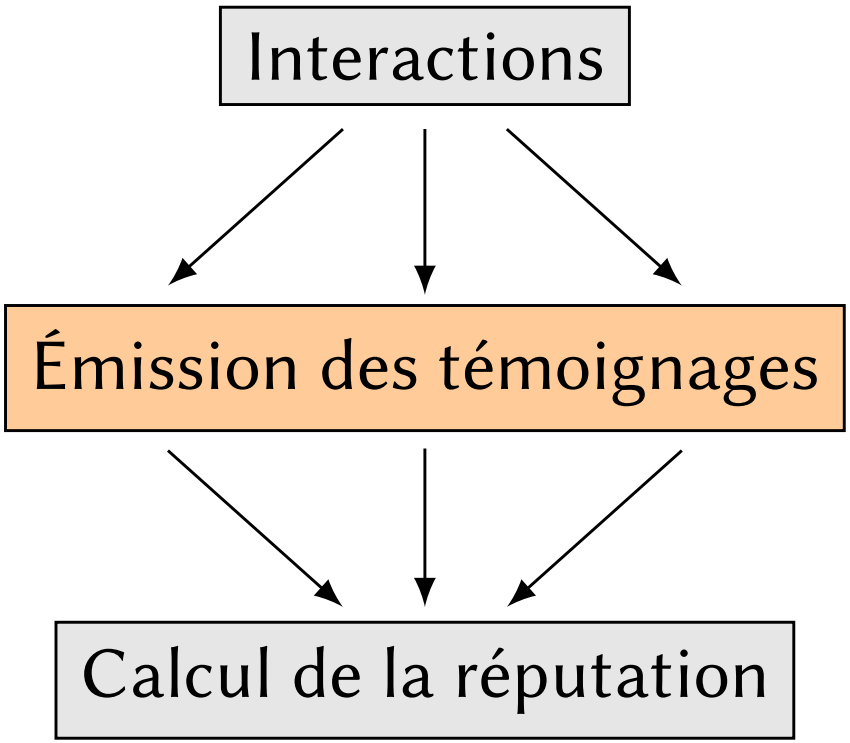
## Nombre nécessaire

Dépend des paramètres :

- Nombre d'utilisateurs
  100 millions
- Nombre de malveillants
  5 millions
- Probabilité de collusion réussie $1/1\,000\,000$



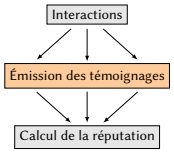

En pratique, $n = 28$ suffit




indéniabilité

associabilité

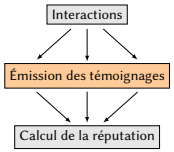
inforgeabilité




# Témoignages

Un témoignage comporte :

- la note du client (optionelle)
- une preuve de transaction
  - client masqué, légitime et consentant
  - fournisseur légitime et consentant
  - indicateur pour l'associabilité : l'invariant



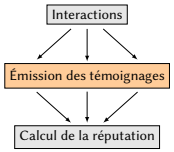

# Invariant

## Objectif

- Associer les témoignages émis sur un même fournisseur
- Sans savoir qui est le client
- Sans associer les témoignages émis sur différents fournisseurs

Calcul d'un invariant :

$$\text{inv} = \text{Inv}(\text{Id}_{\text{FS}}, \text{id}_{\text{Cl}})$$




# Calcul de l'invariant

## Mise en place

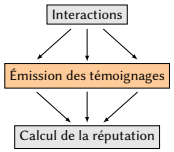
$\mathbb{G}$ un groupe multiplicatif
$G, Y \in \mathbb{G}$, des paramètres du système
$\mathrm{Id_{FS}} \in \mathbb{G}$, l'identifiant du fournisseur, aléatoire
$\mathrm{id_{Cl}} \in \mathbb{Z}$, l'identifiant du client, aléatoire

$$\mathrm{Inv}(\mathrm{Id_{FS}}, \mathrm{id_{Cl}}) = \mathrm{Id_{FS}}^{\mathrm{id_{Cl}}}$$

Pour un couple $(\mathrm{Id_{FS}}, \mathrm{id_{Cl}})$, les invariants sont identiques

DL Connaissant inv, il est difficile de retrouver $\mathrm{id_{Cl}}$

DDH Connaissant $\mathrm{Id_{FS_1}}$, $\mathrm{Id_{FS_2}}$, $\mathrm{inv_1}$, $\mathrm{inv_2}$, il est difficile de savoir si $\mathrm{Cl_1} = \mathrm{Cl_2}$




# Invariant et vie privée

## Problème

Pour calculer $\mathrm{Inv}(\mathrm{Id_{FS}}, \mathrm{id_{CI}})$, il faut connaître $\mathrm{Id_{FS}}$ et $\mathrm{id_{CI}}$

Calcul en trois temps :

1. le fournisseur masque son identifiant avec un aléa (DDH)

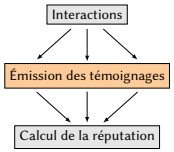
$$\mathrm{pre\_inv} = \mathrm{Pre\_inv}(\mathrm{Id_{FS}}, r) = \left(G^r,\ \mathrm{Id_{FS}} \cdot Y^r\right)$$

2. le client injecte son identifiant

$$\begin{aligned}\mathrm{masked\_inv} &= \mathrm{Mask}\left(\mathrm{pre\_inv}, \mathrm{id_{CI}}, s\right)\\ &= \left(G^s \cdot Y^{\mathrm{id_{CI}}},\ \mathrm{pre\_inv}_1{}^s \cdot \mathrm{pre\_inv}_2{}^{\mathrm{id_{CI}}}\right)\\ &= \left(G^s \cdot Y^{\mathrm{id_{CI}}},\ \mathrm{Id_{FS}}{}^{\mathrm{id_{CI}}} \cdot (G^s \cdot Y^{\mathrm{id_{CI}}})^r\right)\end{aligned}$$

3. le fournisseur obtient l'invariant

$$\mathrm{masked\_inv}_1{}^{-r} \cdot \mathrm{masked\_inv}_2 = \mathrm{Id_{FS}}{}^{\mathrm{id_{CI}}}$$




# Prouver le calcul de l'invariant

## Rappel

$$\text{pre\_inv} = \left(G^r,\ \mathrm{Id}_{\mathrm{FS}} \cdot Y^r\right)$$

$$\text{masked\_inv} = \left(G^s \cdot Y^{\mathrm{id}_{\mathrm{CI}}},\ \text{pre\_inv}_1{}^s \cdot \text{pre\_inv}_2{}^{\mathrm{id}_{\mathrm{CI}}}\right)$$

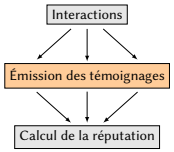
Le client doit être sûr qu'il ne calcule pas autre chose que masked_inv
Mais le fournisseur ne doit pas révéler $\mathrm{Id}_{\mathrm{FS}}$ ou $r$

## Solution

Preuves de connaissance à divulgation nulle de connaissance (NIZK) [GS08]

- Fournisseur : « pre_inv = $(G^r, \mathrm{Id}_{\mathrm{FS}} \cdot Y^r)$ »
- Client : « masked_inv = $\left(G^s \cdot Y^{\mathrm{id}_{\mathrm{CI}}},\ \text{pre\_inv}_1{}^s \cdot \text{pre\_inv}_2{}^{\mathrm{id}_{\mathrm{CI}}}\right)$ »

[GS08] Groth, Sahai : *Efficient Non-Interactive Proof Systems for Bilinear Groups*. Eurocrypt, 2008.




# Prouver le calcul de l'invariant

## Rappel

$$\text{pre\_inv} = \left(G^{r},\ \mathrm{Id}_{\mathrm{FS}} \cdot Y^{r}\right)$$

$$\text{masked\_inv} = \left(G^{s} \cdot Y^{\mathrm{id}_{\mathrm{CI}}},\ \text{pre\_inv}_1{}^{s} \cdot \text{pre\_inv}_2{}^{\mathrm{id}_{\mathrm{CI}}}\right)$$

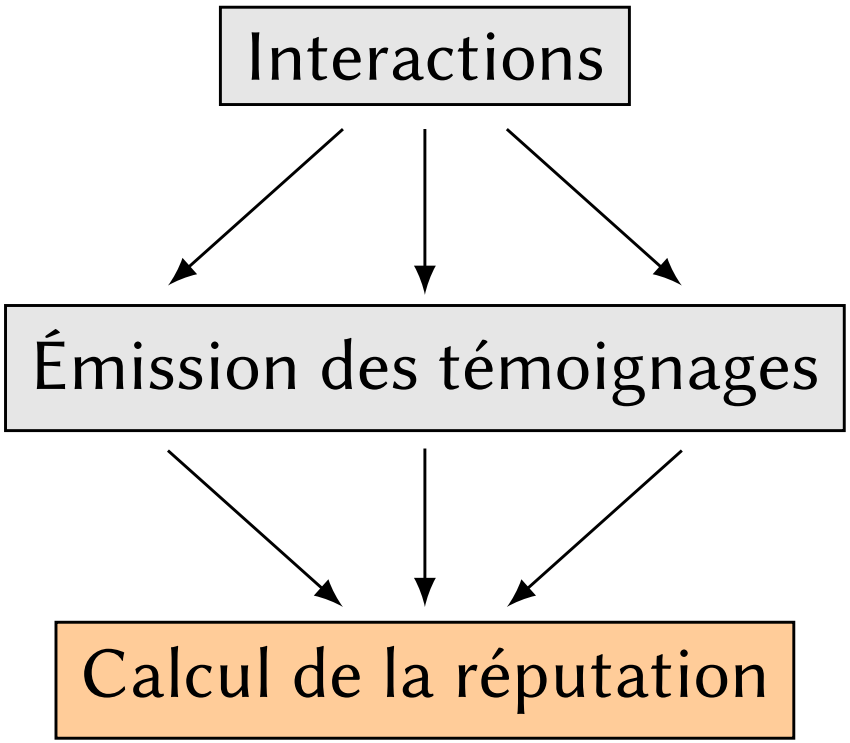
Le client doit être sûr qu'il ne calcule pas autre chose que masked_inv
Mais le fournisseur ne doit pas révéler $\mathrm{Id}_{\mathrm{FS}}$ ou $r$

## Solution

Preuves de connaissance à divulgation nulle de connaissance (NIZK) [GS08]

- Fournisseur : « pre_inv = $(G^{\blacksquare}, \blacksquare \cdot Y^{\blacksquare})$ »
- Client : « masked_inv = $\left(G^{\blacksquare} \cdot Y^{\blacksquare}, \text{pre\_inv}_1{}^{\blacksquare} \cdot \text{pre\_inv}_2{}^{\blacksquare}\right)$ »

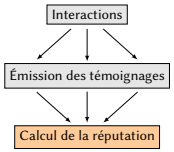
[GS08] Groth, Sahai : *Efficient Non-Interactive Proof Systems for Bilinear Groups*. Eurocrypt, 2008.




indéniabilité

associabilité

inforgeabilité




# Gestion des scores de réputation

On ne peut pas faire confiance aux fournisseurs

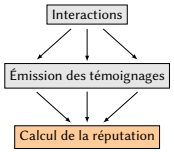
- oubli « accidentel » des témoignages négatifs

## Solution

Utiliser une tierce partie distribuée pour

- stocker les témoignages
- garantir le calcul des scores de réputation

les signataires accrédités




# Signataires accrédités

Ils n'ont pas besoin d'être présents pendant les interactions

À intervalles réguliers, ils

- collectent les nouveaux témoignages
- calculent les réputations
- signent les réputations pour les fournisseurs

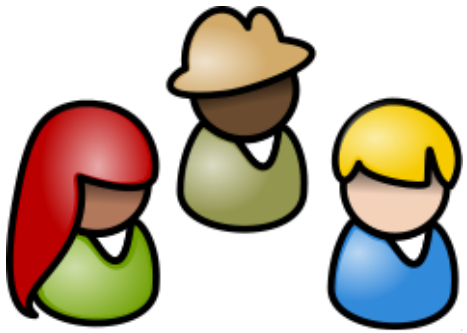
Si deux fournisseurs étaient gérés par deux tierces parties différentes :

↪ On peut les distinguer !

## Anonymat des fournisseurs

Les signataires accrédités gèrent les réputations de tous les fournisseurs

# Deux tierces parties



## Signataires accrédités

- Uniques
- Présents à intervalles réguliers
- Garantissent toutes les réputations

## Porteurs de part

- Présents pendant les interactions
- Garantissent l'émission d'un témoignage

Avoir une seule tierce partie est irréaliste

# Outils utilisés

Deux tierces parties :

- Les signataires accrédités, pour la gestion des réputations
- Les porteurs de part, pour l'indéniabilité des témoignages

Des outils cryptographiques :

- partage de secret, pour la vie privée des utilisateurs
- invariant, pour l'associabilité des témoignages
- système de preuve de connaissance à divulgation nulle de connaissance

# Plan

# Mise en place

On considère un client et un fournisseur

## Client

- Identifiant
- Paire de clés de signature
- Certificat sur l'identifiant

## Fournisseur

- Identifiant
- Paire de clés de signature
- Certificat sur l'identifiant
- Signatures sur la réputation : (identifiant, réputation, date)

# Mise en place

On considère un client et un fournisseur

## Client

- Identifiant
- Paire de clés de signature
- Certificat sur l'identifiant

## Fournisseur

- Identifiant
- Paire de clés de signature
- Certificat sur l'identifiant
- Signatures sur la réputation : (identifiant, réputation, date)

# Mise en place

On considère un client et un fournisseur

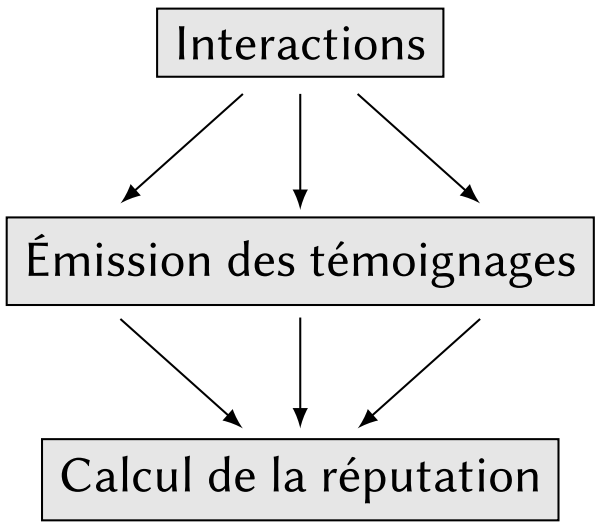
## Client

- Identifiant
- Paire de clés de signature
- Certificat sur l'identifiant

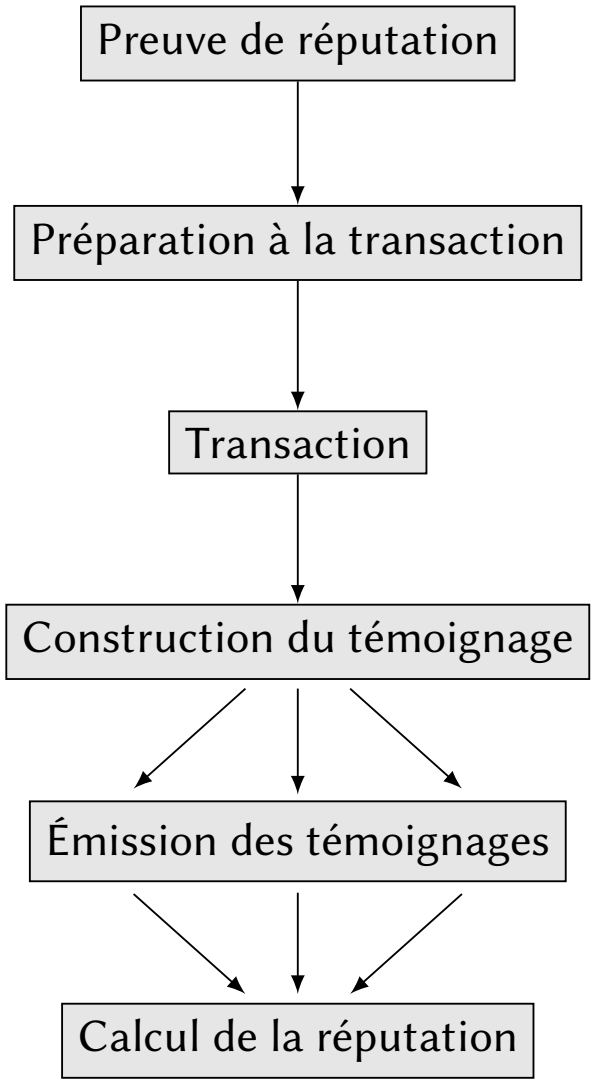
## Fournisseur

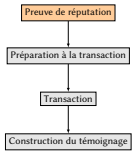
- Identifiant
- Paire de clés de signature
- Certificat sur l'identifiant
- Signatures sur la réputation : (identifiant, réputation, date)

# Déroulement d'une interaction



# Déroulement d'une interaction






# Preuve de réputation

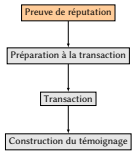
Fournisseurs

Client

rep = 8,4

rep = 9

rep = 7,5




# Preuve de réputation

Fournisseurs

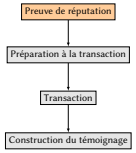
Client

rep = 8,4

« Prouve-moi ta réputation »

rep = 9

rep = 7,5




# Preuve de réputation

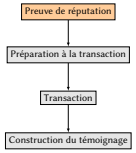
Fournisseurs

Client

rep

rep = 9

$\blacksquare : \mathrm{Verify}(\sigma_{\mathrm{rep}}, \langle \mathrm{Id}_{\mathrm{FS}}, \mathrm{rep}, \mathrm{date} \rangle, \mathrm{vk}_{\mathrm{SA}})$




# Preuve de réputation

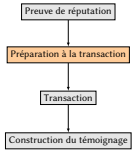
Fournisseurs

Client

rep

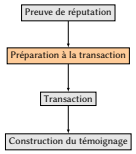
rep = 9

[redacted] : Verify([redacted], ⟨[redacted], rep, date⟩, $vk_{SA}$)

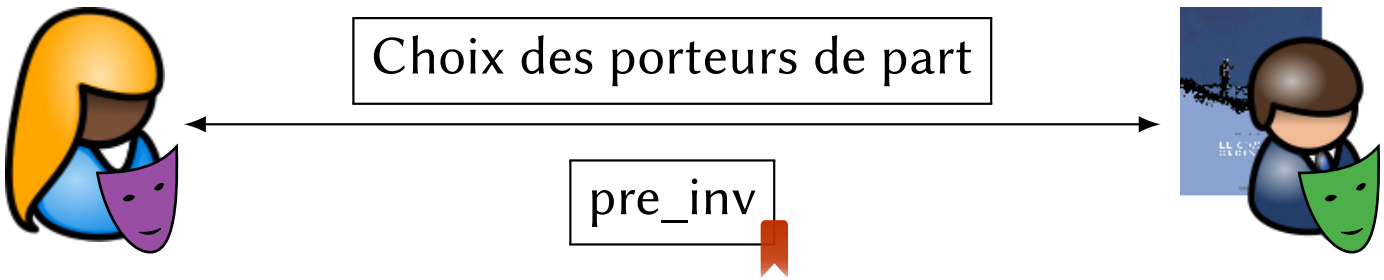



# Préparation à la transaction

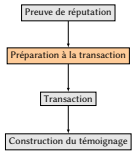
« Même si tout va mal, tu pourras construire le témoignage »



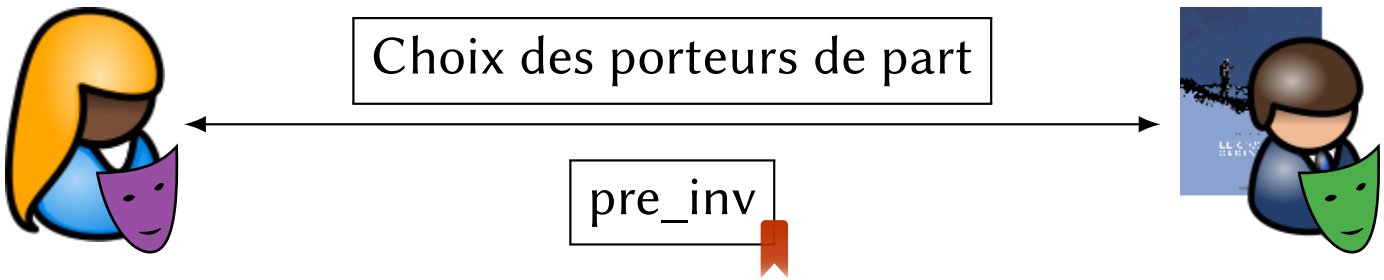

# Préparation à la transaction



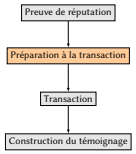

$$\text{pre\_inv} = \text{Pre\_inv}(\text{Id}_{\text{FS}}, r)$$



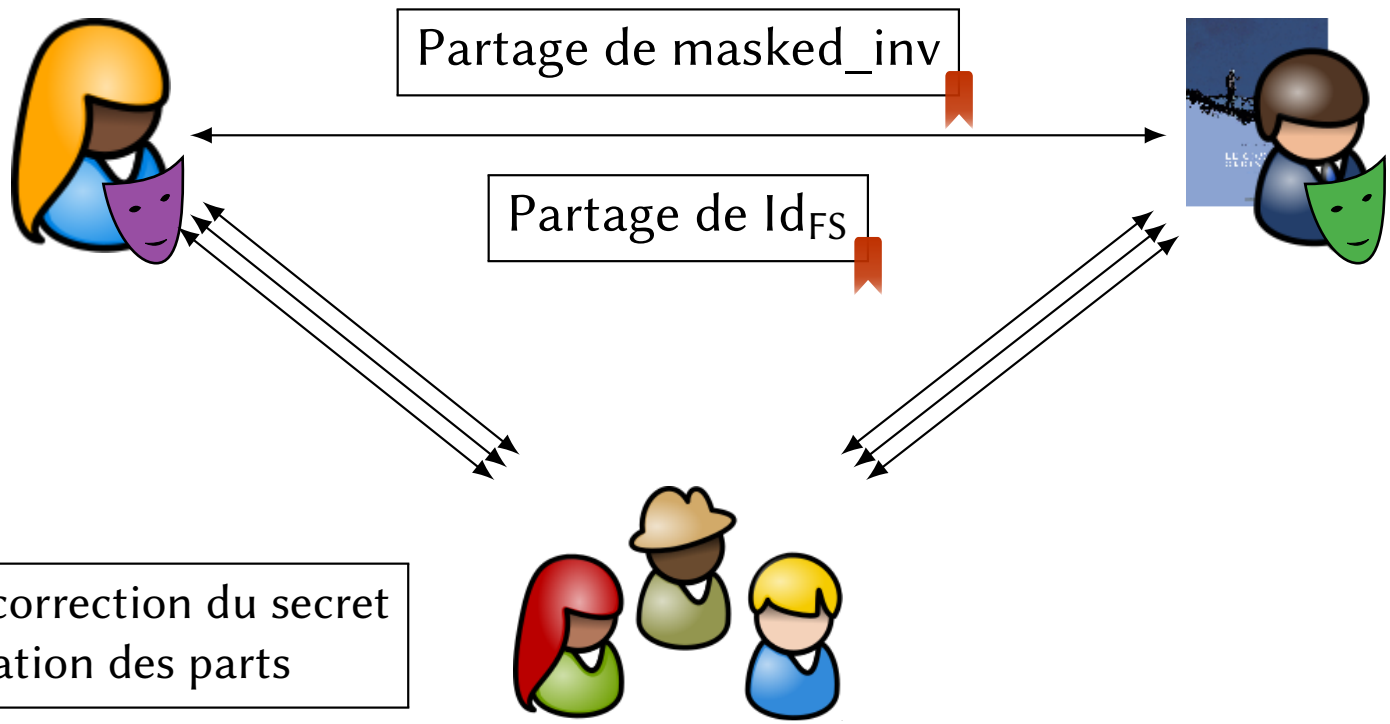

# Préparation à la transaction

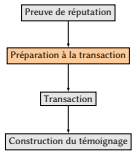



: pre_inv = Pre_inv([redacted],[redacted])

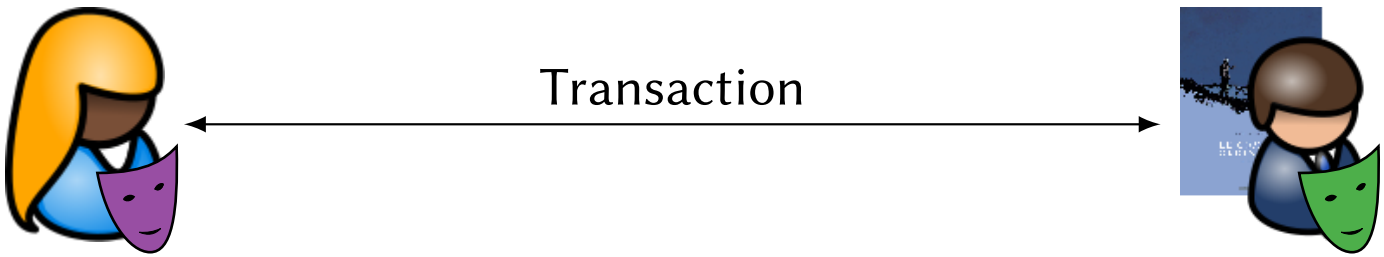


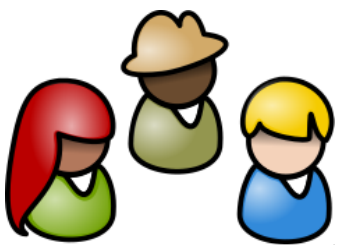

# Préparation à la transaction

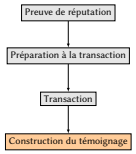





# Préparation à la transaction

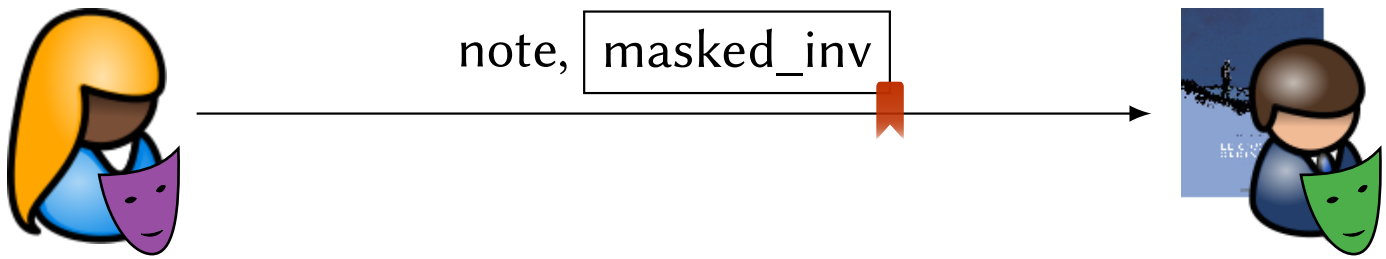


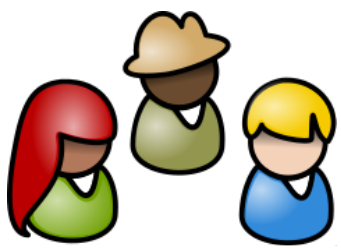


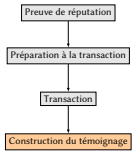

# Construction du témoignage

## Si le client et le fournisseur sont honnêtes



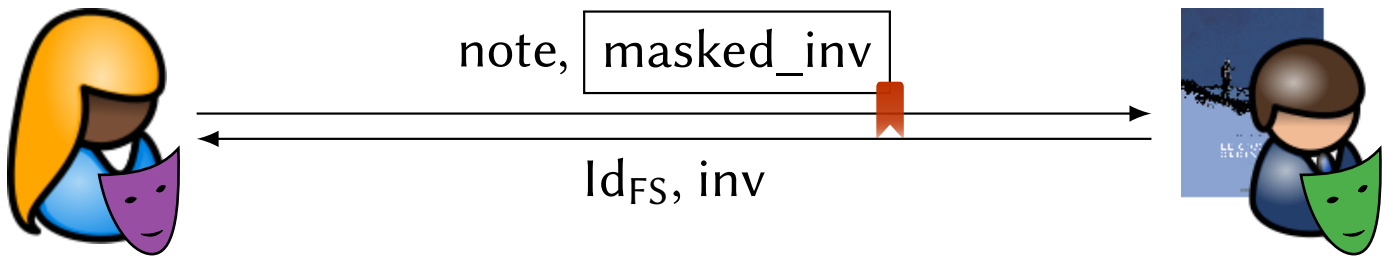

: masked_inv = $\text{Mask}(\text{pre\_inv}, \text{id}_{\text{Cl}}, s)$



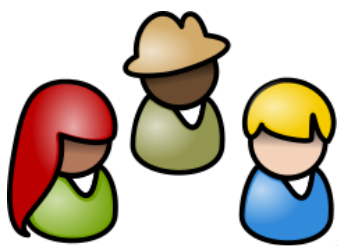


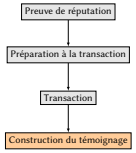

# Construction du témoignage

## Si le client et le fournisseur sont honnêtes



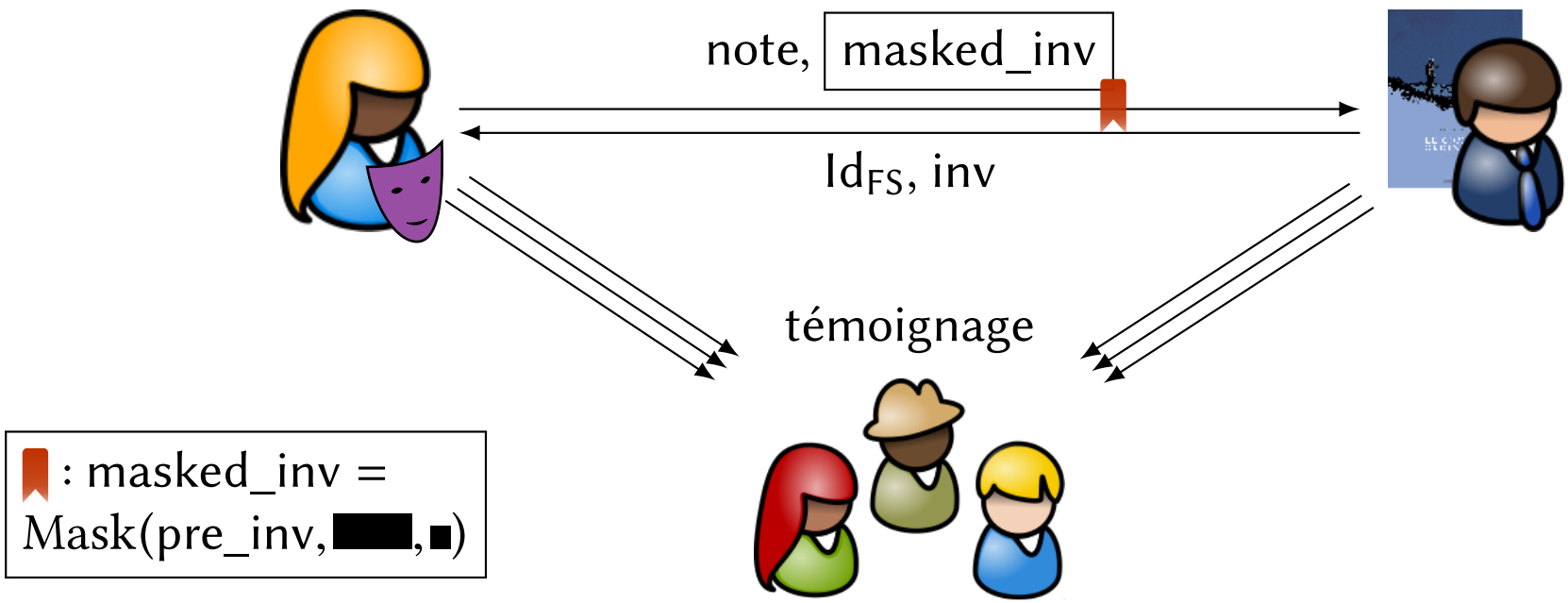

: masked_inv = Mask(pre_inv, [redacted], [redacted])

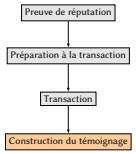





# Construction du témoignage

## Si le client et le fournisseur sont honnêtes

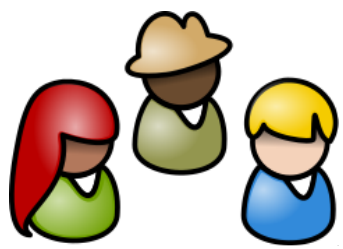




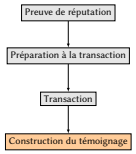

# Construction du témoignage

## Si le client est malveillant

Reconstruction de masked_inv
et construction du témoignage



: reconstruction du secret

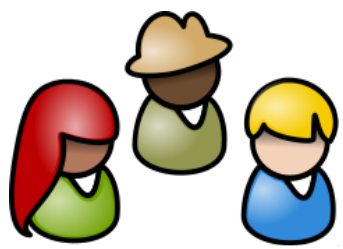


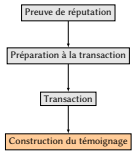

# Construction du témoignage

## Si le fournisseur est malveillant

Reconstruction de $Id_{FS}$ et construction du témoignage

: reconstruction du secret, $inv = Inv(Id_{FS}, id_{Cl})$



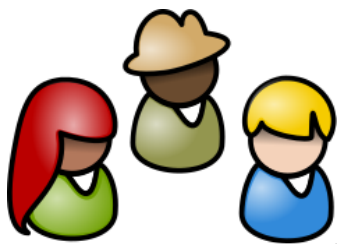


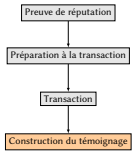

# Construction du témoignage

## Si le fournisseur est malveillant

Reconstruction de $Id_{FS}$ et construction du témoignage

: reconstruction du secret,
inv = Inv($Id_{FS}$, [redacted])



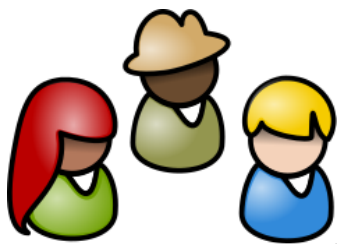


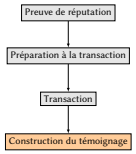

# Construction du témoignage

## Si le fournisseur est malveillant

Reconstruction de $Id_{FS}$ et construction du témoignage

: reconstruction du secret,
inv = Inv($Id_{FS}$, [redacted])






# Construction du témoignage

témoignage

Preuves des identifiants,
du calcul de inv,
du choix de la note

# Plan

# Paramètres

Tailles des éléments et temps de calcul [AKL+11] :

- Sur un processeur haut de gamme de 2010

10 signataires accrédités

28 porteurs de part par interaction

[AKL+11] Aranha, Karabina, Longa, Gebotys and López : *Faster Explicit Formulas for Computing Pairings over Ordinary Curves*. Eurocrypt, 2011.

# Taille des messages échangés

## Rappel

Signatures de réputation [BSS10] : $n \cdot 500$ Kio pour la preuve de réputation

## Notre mécanisme

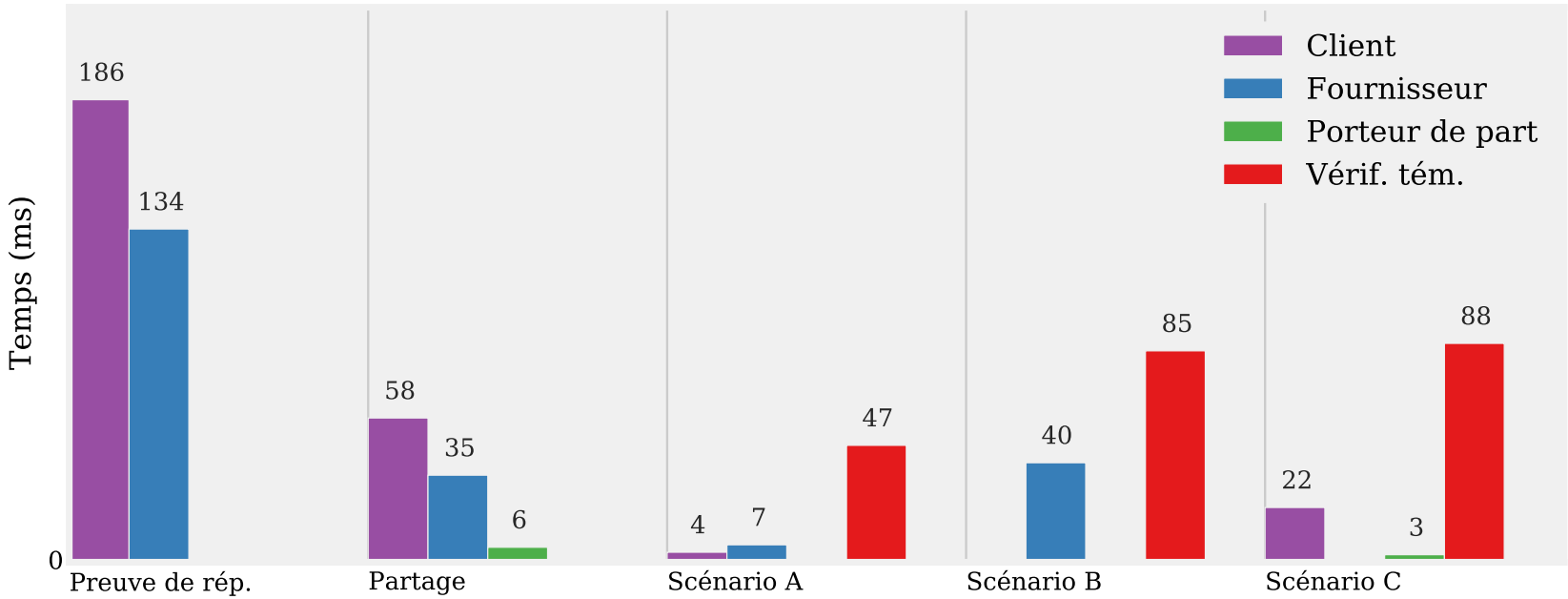
- Preuve de réputation : 50 Kio
- Interaction complète : 150–300 Kio
- Témoignage : 10–20 Kio

---

[BSS10] Bethencourt, Shi and Song : *Signatures of Reputation*. Financial Cryptography and Data Security, 2010.

# Calculs cryptographiques

## Temps théoriques




**Scénario A** Client et fournisseur honnêtes

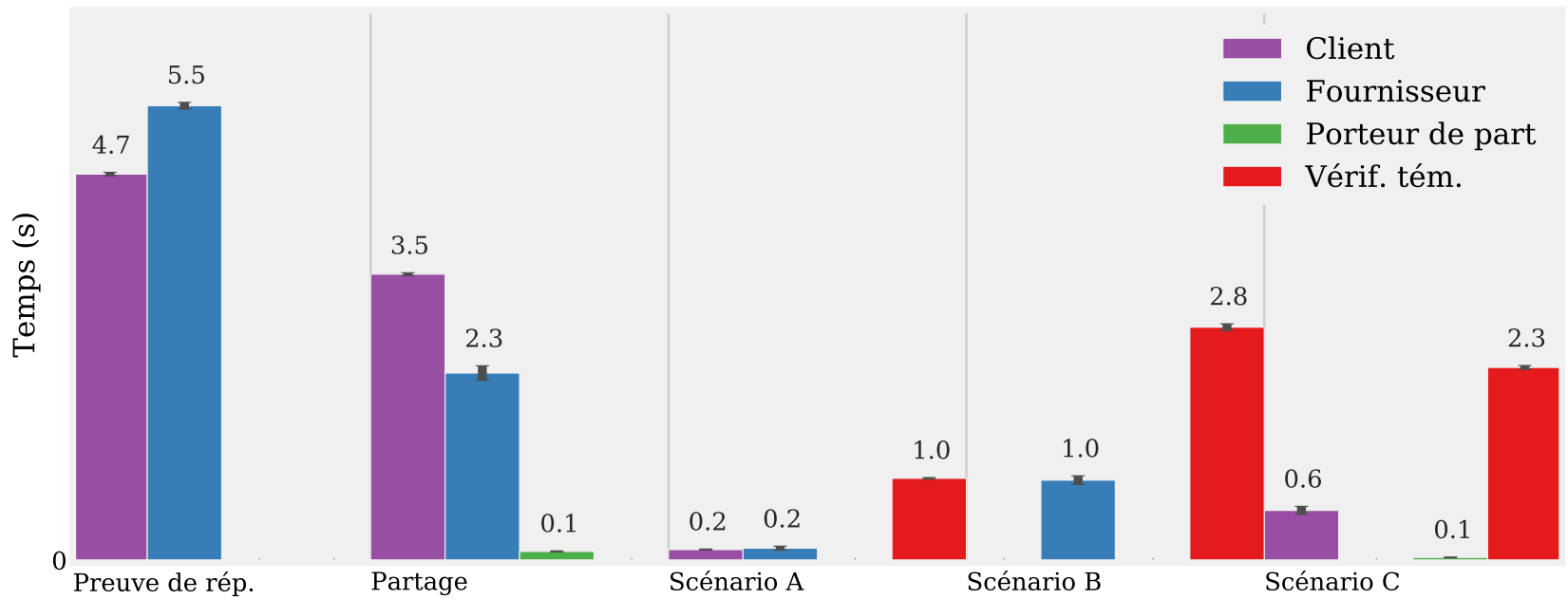
**Scénario B** Client malveillant

**Scénario C** Fournisseur malveillant

# Calculs cryptographiques

## Temps pratiques

Implémentation utilisant le framework Charm [AGM+13], avec David Lanoë
Sur un Dell Latitude E6430 avec un Core i7-3720 QM à 2,6 GHz




Sur un Raspberry Pi : $\times$ 30

[AGM+13] Akinyele, Garman, Miers, Pagano, Rushanan, Green et Rubin : *Charm : a framework for rapidly prototyping cryptosystems*. Journal of Cryptographic Engineering, Vol. 3, 2013.

# Plan

# Résumé

Pendant cette présentation, nous avons analysé

- les éléments nécessaires au calcul de la réputation
- les besoins en données personnelles des mécanismes de réputation

Nous avons tiré parti des outils existants et proposé l'invariant pour construire un mécanisme de réputation robuste préservant la vie privée

| Mécanisme | Distribué | Vie privée | Indéniabilité | Inforgeabilité | Associabilité |
|---|---|---|---|---|---|
| [HBBS13] | ✔ | ✗ | ✔/✗ | ✔ | ✔ |
| [ACBM08] | ✗ | ✔ | ✗ | ✔ | ✗ |
| [BSS10] | ✔ | ✔ | ✗ | ✔ | ✔ |
| Ma thèse | ✔ | ✔ | ✔ | ✔ | ✔ |

# Travaux futurs

Trois axes principaux :

## Implémentation

Améliorer l'implémentation Python pour être plus proche des temps théoriques

## Choix des signataires accrédités

Ils ont une charge lourde

↪ les choisir parmi les plus actifs ?

Et en cas de collusion entre ces fournisseurs ?
Réduire leur charge pour permettre à plus de fournisseurs d'en faire partie ?

## Vie privée des fournisseurs

Comment faire pour que les fournisseurs ne révèlent pas leur identifiant ?
Dans ce cas, comment garantir l'indéniabilité des témoignages ?

# Dissémination des travaux

## Projets et séminaires

- Projet ANR AMORES : « *Architecture for MObiquitous REsilient Systems* », 2011–2015
- Séminaire du département Large-échelle de l'IRISA, janvier 2013, Rennes
- Journées Codage et Cryptographie, mars 2014, Les Sept Laux
- Séminaire Cryptologie & Sécurité du GREYC, octobre 2014, Caen

# Dissémination des travaux

## Publications


Paul Lajoie-Mazenc. “Système de réputation préservant la vie privée”.
Dans : *Atelier Protection de la Vie Privée (APVP)*. Groix, France, 06/2012.


Emmanuelle Anceaume, Gilles Guette, Paul Lajoie-Mazenc, Nicolas Prigent et Valérie Viet Triem Tong.
“A Privacy Preserving Distributed Reputation Mechanism”.
Dans : *IEEE International Conference on Communications (IEEE ICC)*. Budapest, Hungary, 06/2013, p. 1951–1956.


Emmanuelle Anceaume, Gilles Guette, Paul Lajoie-Mazenc, Thomas Sirvent et Valérie Viet Triem Tong.
“Signatures de réputation anonymes”.
Dans : *Sécurité des Architectures Réseau et des Systèmes d’Information (SARSSI)*. Poster. Mont-de-Marsan, France, 09/2013.


Emmanuelle Anceaume, Gilles Guette, Paul Lajoie-Mazenc, Thomas Sirvent et Valérie Viet Triem Tong.
“Extending Signatures of Reputation”.
Dans : *Privacy and Identity Management for Emerging Services and Technologies*. T. 421. IFIP Advances in Information and Communication Technology. Nijmegen, The Netherlands, 2014, p. 165–176.


Paul Lajoie-Mazenc, Emmanuelle Anceaume, Gilles Guette, Thomas Sirvent et Valérie Viet Triem Tong.
“Privacy-Preserving Reputation Mechanism : A Usable Solution Handling Negative Ratings”.
Dans : *IFIP WG 11.1 International Conference on Trust Management*. Hamburg, Germany, 05/2015.


Paul Lajoie-Mazenc, Emmanuelle Anceaume, Gilles Guette, Thomas Sirvent et Valérie Viet Triem Tong.
“Mécanisme de réputation distribué préservant la vie privée avec témoignages négatifs”.
Dans : *Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel)*. Beaune, France, 06/2015.


Emmanuelle Anceaume, Yann Busnel, Paul Lajoie-Mazenc et Géraldine Texier.
“Reputation for Inter-Domain QoS Routing”.
Dans : *IEEE International Symposium on Network Computing and Applications (IEEE NCA)*. Cambridge, Massachusetts, USA, 09/2015.

Merci de votre attention !