Système de réputation non-monotone préservant la vie privée

Paul Lajoie-Mazenc Emmanuelle Anceaume Gilles Guette Thomas Sirvent
Valérie Viet Triem Tong

IRISA/IRMAR, équipe CIDRE, Rennes

2014

Contexte

Des utilisateurs interagissent sans se connaître (clients et fournisseurs de service)

Problème

Toute transaction comporte un risque :
« Vais-je recevoir l'objet acheté, et dans quel état ? »

Mécanisme de réputation

Après chaque transaction, le client témoigne sur le fournisseur
Permet de calculer un score de réputation pour chaque fournisseur

Plus un fournisseur se comporte bien, plus sa réputation est élevée

Contexte

Des utilisateurs interagissent sans se connaître (clients et fournisseurs de service)

Problème

Toute transaction comporte un risque :
« Vais-je recevoir l'objet acheté, et dans quel état ? »

Mécanisme de réputation

Après chaque transaction, le client témoigne sur le fournisseur
Permet de calculer un score de réputation pour chaque fournisseur

Plus un fournisseur se comporte bien, plus sa réputation est élevée

Contexte

Des utilisateurs interagissent sans se connaître (clients et fournisseurs de service)

Problème

Toute transaction comporte un risque :
« Vais-je recevoir l'objet acheté, et dans quel état ? »

Mécanisme de réputation

Après chaque transaction, le client témoigne sur le fournisseur
Permet de calculer un score de réputation pour chaque fournisseur

Plus un fournisseur se comporte bien, plus sa réputation est élevée

Vie privée dans les mécanismes de réputation

Dans un système sans anonymat, les clients hésitent à témoigner :

- mise en danger de leur vie privée
- peur des représailles

L'identifiant d'un fournisseur peut impacter les témoignages reçus

Compromis réputation/vie privée

Une réputation parfaite et un anonymat total semblent incompatibles

Clients parfaitement anonymes

Attaques par bourrage d'urne :
un seul client vote de nombreuses fois pour un fournisseur

Détecter les témoignages multiples pour améliorer la robustesse des mécanismes de réputation

Compromis réputation/vie privée

Une réputation parfaite et un anonymat total semblent incompatibles

Clients parfaitement anonymes

Attaques par bourrage d'urne :
un seul client vote de nombreuses fois pour un fournisseur

Détecter les témoignages multiples pour améliorer la robustesse des mécanismes de réputation

Signatures de réputation [Bethencourt *et al.*, 2010]

Mécanisme de réputation distribué

Fournisseurs dévoilent uniquement leur réputation

Réputation : nombre de clients différents ayant témoigné sur le fournisseur

Les témoignages d'un même client sur un même fournisseur sont associables

Problèmes

- Efficacité : preuve de réputation $\approx$ 500ko par témoignage reçu
- Pas de témoignages négatifs

Signatures de réputation [Bethencourt *et al.*, 2010]

Mécanisme de réputation distribué

Fournisseurs dévoilent uniquement leur réputation

Réputation : nombre de clients différents ayant témoigné sur le fournisseur

Les témoignages d'un même client sur un même fournisseur sont associables

Problèmes

- Efficacité : preuve de réputation $\approx$ 500ko par témoignage reçu
- Pas de témoignages négatifs

Pourquoi faut-il des témoignages négatifs ?

Cas des agents dormants

Un fournisseur entre dans le système
Il se comporte honnêtement jusqu'à ce que sa réputation soit bonne
À partir de là, il devient malhonnête

Sans témoignages négatifs, on ne peut pas détecter cette attaque

Objectifs

Nous souhaitons construire un système de réputation :

- Distribué
- Préservant la vie privée
- Témoignages positifs et négatifs
- Efficace

Plan

1. Propriétés assurées
2. Briques utilisées
3. Notre système de réputation anonyme
4. Performances

Vie privée

Fournisseurs Pendant une interaction, deux fournisseurs de même réputation sont indistinguables

Clients Les interactions avec des fournisseurs différents ne sont pas associables

Émission des témoignages

Non-forgeabilité Il est impossible de forger un témoignage

Non-déniabilité Le fournisseur ne peut empêcher le client de témoigner sur l'interaction
Même si le client ne témoigne pas sur le fournisseur, ce fournisseur peut recevoir un témoignage par défaut

Le témoignage par défaut améliore la réputation du fournisseur

Calcul de la réputation

Non-forgeabilité Il est impossible de forger un score de réputation

Associabilité Deux témoignages d'un même client sur un même fournisseur sont détectés

Signataires accrédités

On ne peut faire confiance aux fournisseurs pour calculer leur réputation

↪ Tierce partie de confiance calculant et signant les réputations

Nous distribuons cette autorité parmi des signataires accrédités

Signataires accrédités

On ne peut faire confiance aux fournisseurs pour calculer leur réputation

↪ Tierce partie de confiance calculant et signant les réputations

Nous distribuons cette autorité parmi des signataires accrédités

Porteurs de part

Comment assurer la non-déniabilité ?

Le client ne sait pas à qui attribuer son témoignage

↪ le fournisseur doit engager son identifiant

Pour chaque interaction, le client et le fournisseur choisissent une tierce partie de confiance distribuée : les porteurs de part

Ils sont en charge du bon déroulement de l'interaction

Porteurs de part

Comment assurer la non-déniabilité ?

Le client ne sait pas à qui attribuer son témoignage

↪ le fournisseur doit engager son identifiant

Pour chaque interaction, le client et le fournisseur choisissent une tierce partie de confiance distribuée : les porteurs de part

Ils sont en charge du bon déroulement de l'interaction

Partage de secret

Principe

Un secret est divisé en n parts
Moins de t parts ne donne aucune information sur le secret
À partir de t parts, on peut reconstruire le secret

Dans notre cas

Parts distribuées aux porteurs de part
Garantit la non-déniabilité :

- le client peut savoir à quel fournisseur destiner son témoignage
- le fournisseur peut récupérer un témoignage par défaut

Partage de secret

Principe

Un secret est divisé en n parts
Moins de t parts ne donne aucune information sur le secret
À partir de t parts, on peut reconstruire le secret

Dans notre cas

Parts distribuées aux porteurs de part
Garantit la non-déniabilité :

- le client peut savoir à quel fournisseur destiner son témoignage
- le fournisseur peut récupérer un témoignage par défaut

Associabilité des témoignages

Nous voulons :

- détecter deux témoignages du même client sur le même fournisseur
- sans pouvoir associer les clients de fournisseurs différents

À chaque interaction est associée un invariant, représentant le couple (Client, Fournisseur)

Associabilité des témoignages

Nous voulons :

- détecter deux témoignages du même client sur le même fournisseur
- sans pouvoir associer les clients de fournisseurs différents

À chaque interaction est associée un invariant, représentant le couple (Client, Fournisseur)

Calcul d'un invariant

Fournisseur : $\mathsf{Id}_{\mathsf{FS}} \in \mathbb{G}$

Client : $\mathsf{id}_{\mathsf{Cl}} \in \mathbb{Z}_p$

$$\mathsf{inv} = \mathsf{Id}_{\mathsf{FS}}{}^{\mathsf{id}_{\mathsf{Cl}}}$$

garantit les propriétés voulues

Pour préserver la vie privée des utilisateurs, en trois étapes :

1. Le fournisseur masque son identifiant, et l'envoie au client (pré-invariant)
2. Le client injecte son identifiant dans le pré-invariant (invariant masqué)
3. Le fournisseur déchiffre l'invariant masqué, et obtient l'invariant

Calcul d'un invariant

Fournisseur : $\mathsf{Id}_{\mathsf{FS}} \in \mathbb{G}$

Client : $\mathsf{id}_{\mathsf{Cl}} \in \mathbb{Z}_p$

$$\mathsf{inv} = \mathsf{Id}_{\mathsf{FS}}{}^{\mathsf{id}_{\mathsf{Cl}}}$$

garantit les propriétés voulues

Pour préserver la vie privée des utilisateurs, en trois étapes :

1. Le fournisseur masque son identifiant, et l'envoie au client (pré-invariant)
2. Le client injecte son identifiant dans le pré-invariant (invariant masqué)
3. Le fournisseur déchiffre l'invariant masqué, et obtient l'invariant

Calcul d'un invariant

Fournisseur : $\mathsf{Id}_{\mathsf{FS}} \in \mathbb{G}$

Client : $\mathsf{id}_{\mathsf{Cl}} \in \mathbb{Z}_p$

$$\mathsf{inv} = \mathsf{Id}_{\mathsf{FS}}{}^{\mathsf{id}_{\mathsf{Cl}}}$$

garantit les propriétés voulues

Pour préserver la vie privée des utilisateurs, en trois étapes :

1. Le fournisseur masque son identifiant, et l'envoie au client (pré-invariant)
2. Le client injecte son identifiant dans le pré-invariant (invariant masqué)
3. Le fournisseur déchiffre l'invariant masqué, et obtient l'invariant

Calcul d'un invariant

Fournisseur : $\mathsf{Id}_{\mathsf{FS}} \in \mathbb{G}$

Client : $\mathsf{id}_{\mathsf{Cl}} \in \mathbb{Z}_p$

$$\mathsf{inv} = \mathsf{Id}_{\mathsf{FS}}{}^{\mathsf{id}_{\mathsf{Cl}}}$$

garantit les propriétés voulues

Pour préserver la vie privée des utilisateurs, en trois étapes :

1. Le fournisseur masque son identifiant, et l'envoie au client (pré-invariant)
2. Le client injecte son identifiant dans le pré-invariant (invariant masqué)
3. Le fournisseur déchiffre l'invariant masqué, et obtient l'invariant

Preuves de connaissance

« Je connais x vérifiant l'équation E » sans dévoiler x

Système de preuve de Groth et Sahai (2008) :

- permet de prouver des équations algébriques dans un groupe bilinéaire
- de manière efficace

Dans notre cas

Prouver les calculs sans dévoiler d'éléments identifiants

Par exemple, prouver chaque étape du calcul de l'invariant

Preuves de connaissance

« Je connais x vérifiant l'équation E » sans dévoiler x

Système de preuve de Groth et Sahai (2008) :

- permet de prouver des équations algébriques dans un groupe bilinéaire
- de manière efficace

Dans notre cas

Prouver les calculs sans dévoiler d'éléments identifiants

Par exemple, prouver chaque étape du calcul de l'invariant

Signatures proxy anonymes

Proposé par Fuchsbauer et Pointcheval (2008)

Principe

Les utilisateurs peuvent signer des messages

- En prouvant qu'ils sont enregistrés
- Sans dévoiler leur clé de vérification

Comment construire un tel schéma ?

- Schéma de signature structure-preserving (Abe *et al.*, 2010)
- Système de Groth-Sahai pour masquer les éléments identifiants

Signatures proxy anonymes

Proposé par Fuchsbauer et Pointcheval (2008)

Principe

Les utilisateurs peuvent signer des messages

- En prouvant qu'ils sont enregistrés
- Sans dévoiler leur clé de vérification

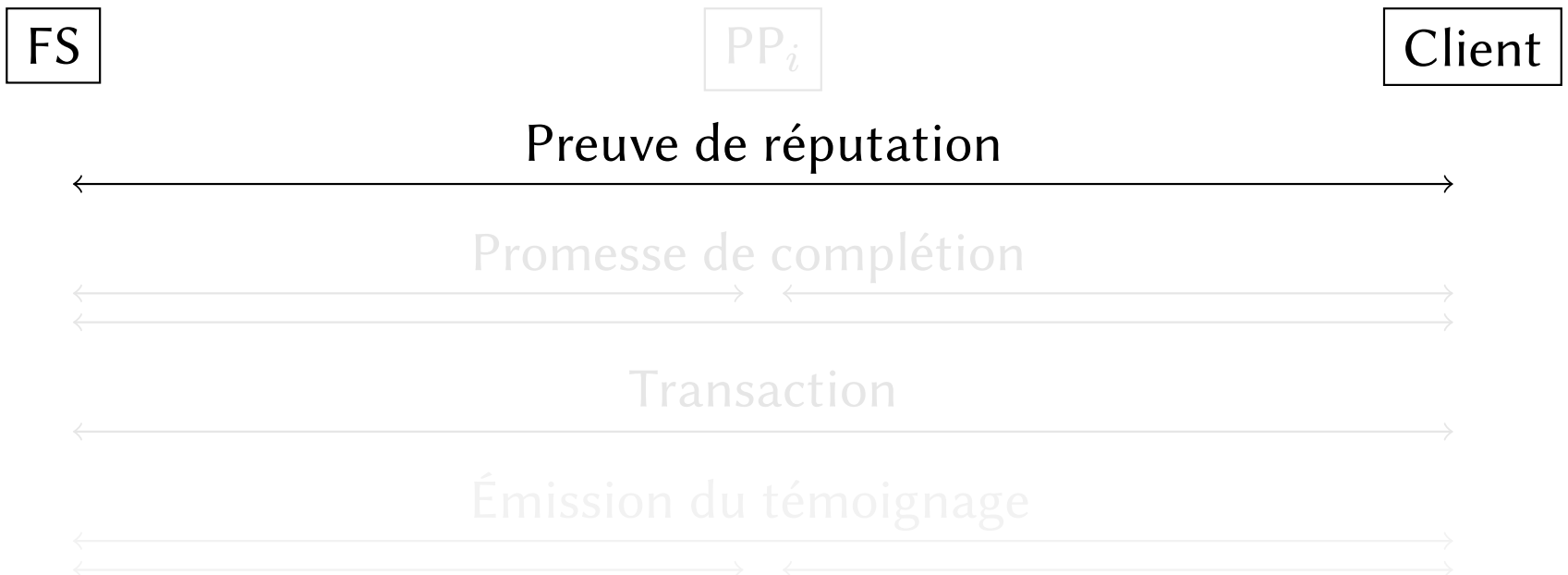
Comment construire un tel schéma ?

- Schéma de signature structure-preserving (Abe *et al.*, 2010)
- Système de Groth-Sahai pour masquer les éléments identifiants

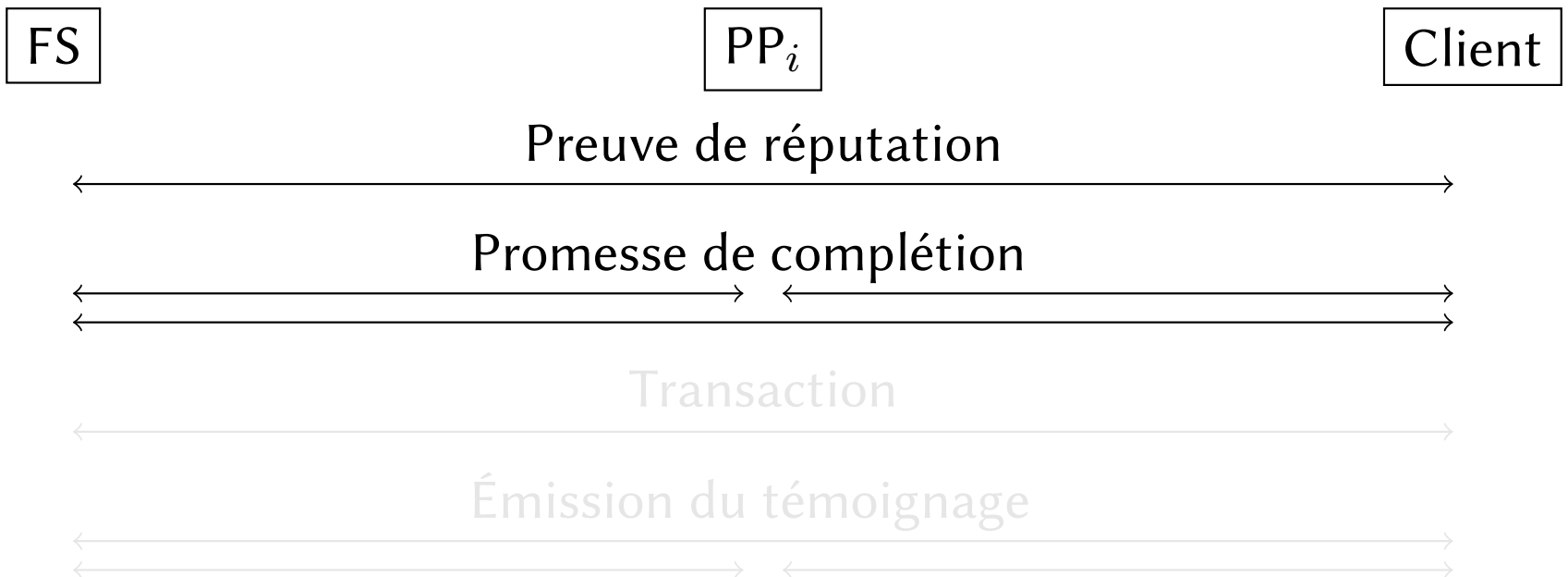
Résumé des briques

- Signataires accrédités, signant les réputations
- Porteurs de part, garantissant le bon déroulement des interactions
- Partage de secret, combinant non-déniabilité et vie privée
- Invariant, associant les témoignages
- Preuves Groth-Sahai, garantissant les calculs effectués
- Signatures proxy anonymes

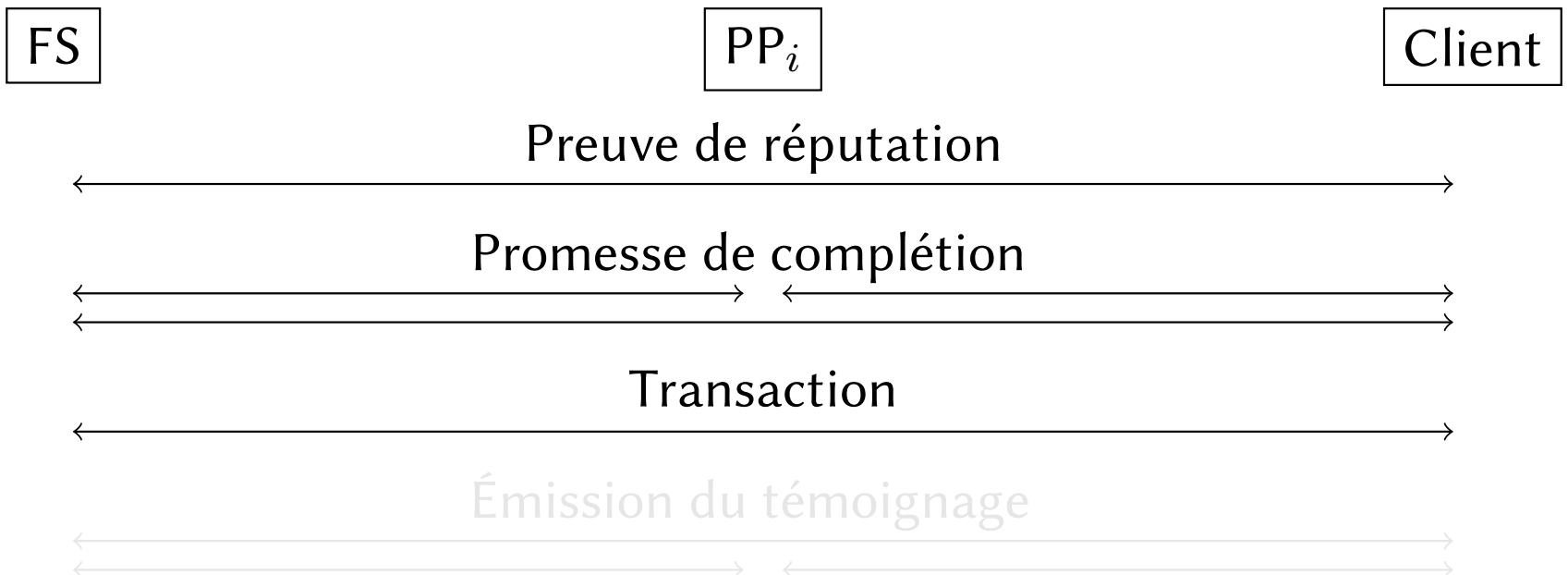
Protocole d'interaction



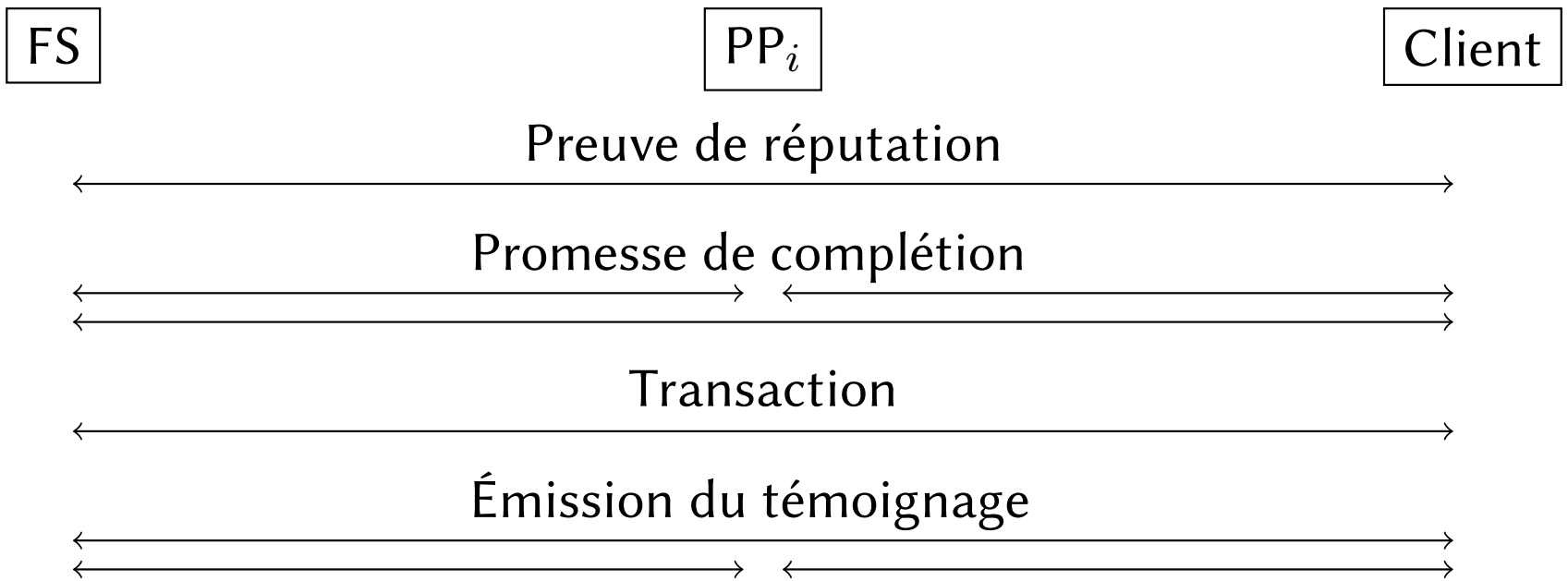
Protocole d'interaction



Protocole d'interaction



Protocole d'interaction



Preuve de réputation

Le fournisseur prouve

- qu'il est enregistré dans le système (signature proxy anonyme)
- que sa réputation est valide
  - sans dévoiler son identifiant ou les signatures sur sa réputation

(signataires accrédités, preuves Groth-Sahai)

Promesse de complétion

1. Le client et le fournisseur choisissent les porteurs de part
2.a Le fournisseur partage son identifiant aux porteurs de part
2.b Le client partage l'invariant masqué

(partage de secret)

Les partages sont prouvés (preuves Groth-Sahai)

Une fois que les partages ont été vérifiés, la transaction a lieu

Émission du témoignage

Trois cas possibles :

1. Tout se passe bien
2. Le fournisseur refuse de dévoiler son identifiant
3. Le client refuse de dévoiler l'invariant masqué

Si le fournisseur est malhonnête

Les porteurs de part permettent au client de reconstruire l'identifiant du fournisseur

Si le client est malhonnête

Les porteurs de part permettent au fournisseur de reconstruire l'invariant

Émission du témoignage

Trois cas possibles :

1. Tout se passe bien
2. Le fournisseur refuse de dévoiler son identifiant
3. Le client refuse de dévoiler l'invariant masqué

Si le fournisseur est malhonnête

Les porteurs de part permettent au client de reconstruire l'identifiant du fournisseur

Si le client est malhonnête

Les porteurs de part permettent au fournisseur de reconstruire l'invariant

Émission du témoignage

Trois cas possibles :

1. Tout se passe bien
2. Le fournisseur refuse de dévoiler son identifiant
3. Le client refuse de dévoiler l'invariant masqué

Si le fournisseur est malhonnête

Les porteurs de part permettent au client de reconstruire l'identifiant du fournisseur

Si le client est malhonnête

Les porteurs de part permettent au fournisseur de reconstruire l'invariant

Performances

Temps et tailles donnés par Aranha *et al.* (EuroCrypt'11) sur des courbes de Barreto-Naehrig.

TABLE : Temps de calcul (ms) et taille des messages (ko) approchés

Phase	Temps de calcul (ms)				Tailles (ko)
	Client	Fournisseur	Porteurs	Signataires	
Préparation	200	100	30	0	50
Émission, 1.	10	10	0	40	10
Émission, 2.	N/A	160	10	200	60
Émission, 3.	80	N/A	30	140	40

Conclusion

Nous avons proposé un système de réputation :

- Distribué
- Préservant la vie privée des utilisateurs
- Témoignages positifs et négatifs
- Efficace

Axes de travaux futur :

- Pour l'instant, l'anonymat des fournisseurs est temporaire
- Anonymat permanent et témoignages négatifs sont-ils compatibles ?

Merci de votre attention !

Questions ?