Accréditations Anonymes et Signatures Agrégeables

Orange Labs

Roch Lescuyer Sébastien Canard

Vendredi 7 avril 2011, Journées C2

Sommaire

- Introduction
- Intuition et Construction générique
- Construction à base de couplages
- Extensions et Conclusion

- Introduction
- Intuition et Construction générique
- Construction à base de couplages
- Extensions et Conclusion

Introduction

La Privacy

- La privacy : la protection de la vie privée des utilisateurs.
- Approche need-to-know : lorsque je m'authentifie, je ne fournis que le minimum d'information nécessaire.
- La cryptographie peut se mettre au service de la vie privée : signatures aveugles, signatures de groupes, accréditations anonymes, etc.

Introduction

Les Accréditations Anonymes

- De l'anglais anonymous credentials. Elles portent sur des attributs : "être étudiant", "habiter Paris", etc.
- Elles sont anonymes dans la mesure où on peut les utiliser sans révéler plus que la valeur des attributs.

Introduction

Les Accréditations Anonymes : Etat de l'Art

1. Le système de Brands ; à base de signature aveugles.

2. Les signatures Camenisch-Lysyanskaya ; à base de signatures de groupe.

Introduction

Les Accréditations Anonymes : Etat de l'Art

1. Le système de Brands ; à base de signature aveugles.

   Technologie UProve de Microsoft

2. Les signatures Camenisch-Lysyanskaya ; à base de signatures de groupe.

   Technologie Idemix de IBM

Introduction

Protocoles

- Obtenir des accréditations

$$\mathcal{AC}.\textsc{Obtain} \leftrightarrow \mathcal{AC}.\textsc{Issue}$$

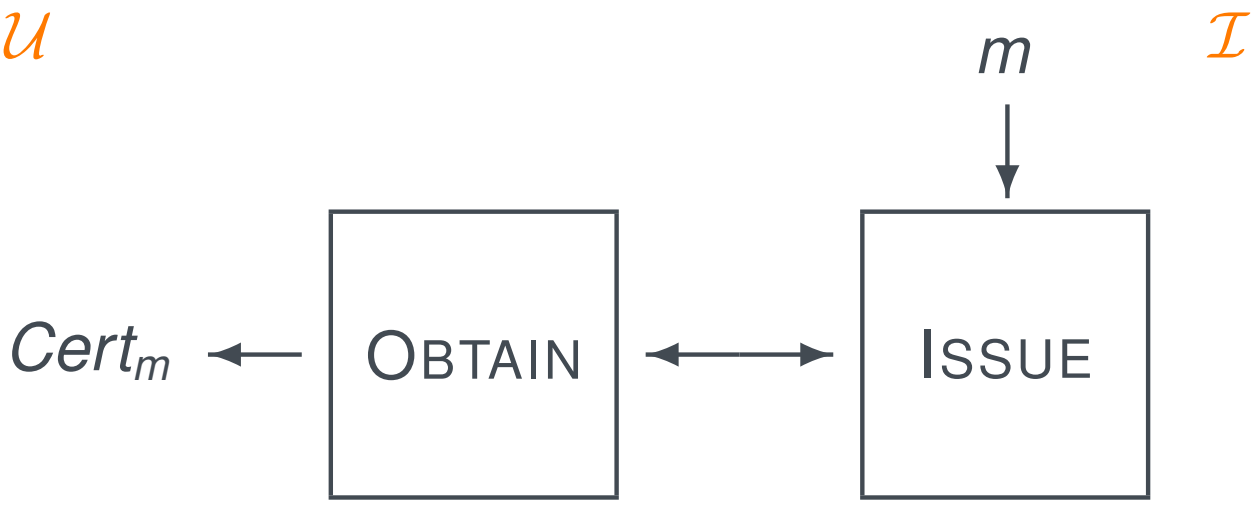
- Utiliser ses accréditations

$$\mathcal{AC}.\textsc{Show} \leftrightarrow \mathcal{AC}.\textsc{Verify}$$

Introduction

Protocoles

- Obtenir des accréditations



- Utiliser ses accréditations

$$\mathcal{AC}.\text{SHOW} \leftrightarrow \mathcal{AC}.\text{VERIFY}$$

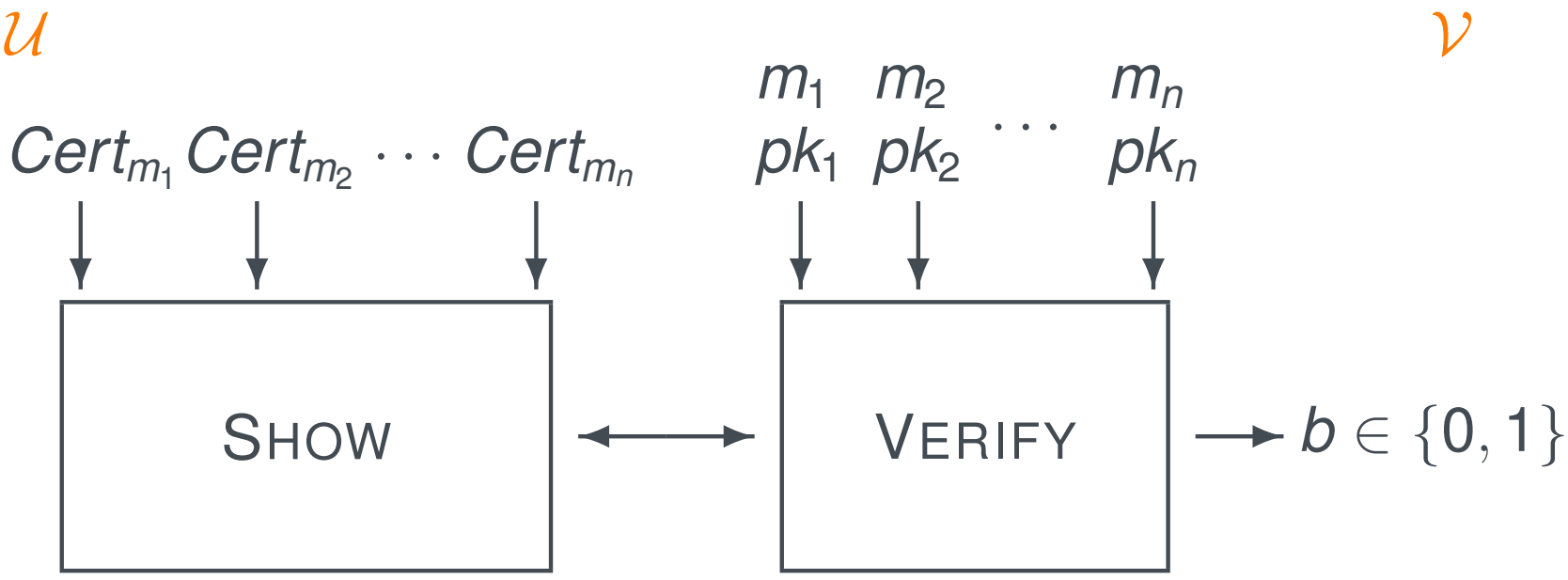
Introduction

Protocoles

- Obtenir des accréditations

$$\mathcal{AC}.\textsc{Obtain} \leftrightarrow \mathcal{AC}.\textsc{Issue}$$

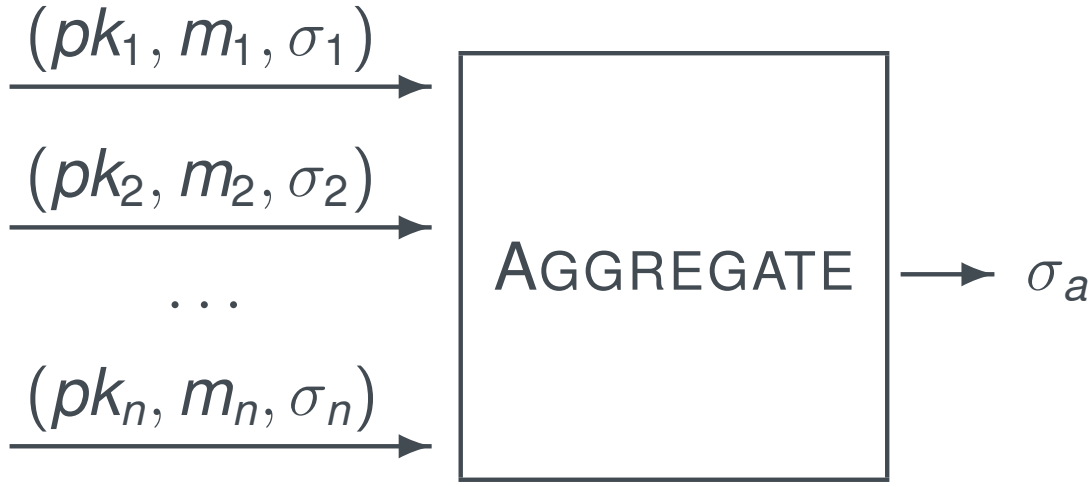
- Utiliser ses accréditations



Introduction

Les Signatures Agrégeables

- De l'anglais aggregate signatures. Agréger plusieurs signatures individuelles en une seule.



- Economies en stockage, en bande passante, etc.

Introduction

Idée

- Utiliser des signatures agrégeables à la place des certificats.

- Introduction
- Intuition et Construction générique
- Construction à base de couplages
- Extensions et Conclusion

Construction

Signatures agrégeables indexées

- On veut limiter les possibilités d'agrégation.
- On ne peut agréger des signatures que si elles ont été générées sur le même index.

$$\sigma \leftarrow \mathcal{AG}.\textsc{Sign}(sk, m)$$

$$\sigma_a \leftarrow \mathcal{AG}.\textsc{Aggregate}(\{pk_n, m_n, \sigma_n\}_n)$$

$$\{0,1\} \ni b \leftarrow \mathcal{AG}.\textsc{Verify}(\{pk_n, m_n\}_n, \sigma_a)$$

Construction

Signatures agrégeables indexées

- On veut limiter les possibilités d'agrégation.
- On ne peut agréger des signatures que si elles ont été générées sur le même index.

$$\sigma \leftarrow \mathcal{AG}.\textsc{Sign}(sk, x, m)$$

$$\sigma_a \leftarrow \mathcal{AG}.\textsc{Aggregate}(x, \{pk_n, m_n, \sigma_n\}_n)$$

$$\{0,1\} \ni b \leftarrow \mathcal{AG}.\textsc{Verify}(x, \{pk_n, m_n\}_n, \sigma_a)$$

Construction

Construction générique

- Génération des clefs
  - (opk, osk) : clefs du schéma de signature agrégeable
  - (upk, usk) : toute paire de clefs telle que $\{usk\} = \{x\}$
- Obtenir une accréditation

$$cred = \sigma \leftarrow \mathcal{AG}.\textsc{Sign}(osk, x, m)$$

- Utilisation des accréditations

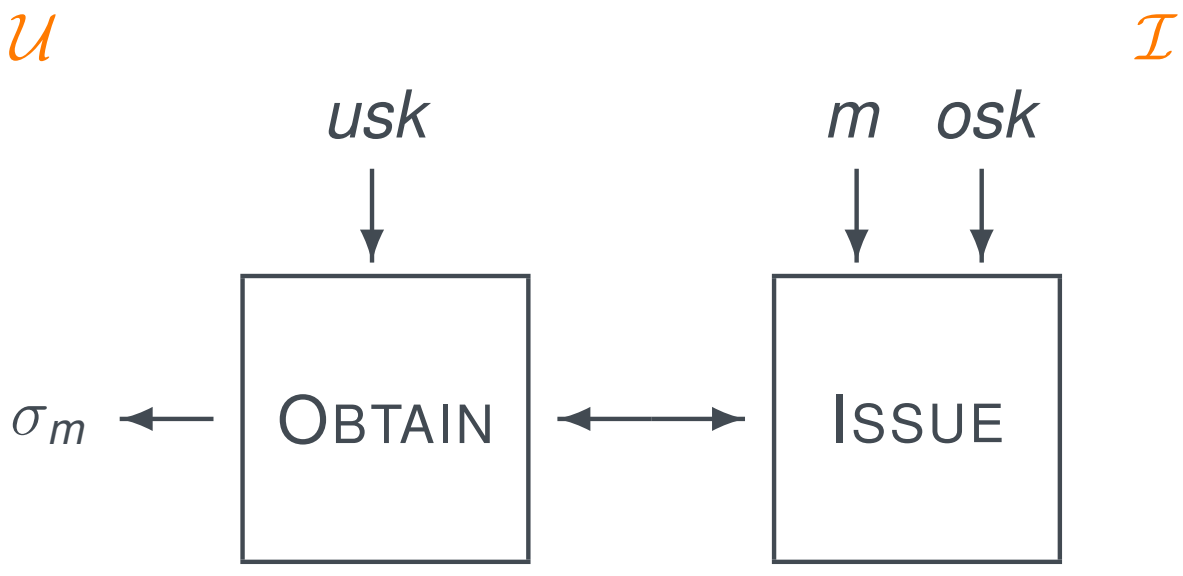
$$\sigma_a \leftarrow \mathcal{AG}.\textsc{Aggregate}(x, \{opk_n, m_n, \sigma_n\}_n)$$

$$PK\{\langle \alpha, \beta \rangle : \mathcal{AG}.\textsc{Verify}(\beta, \{opk_n, m_n\}_n, \alpha) = 1\}$$

Construction

Construction générique

- Obtenir une accréditation

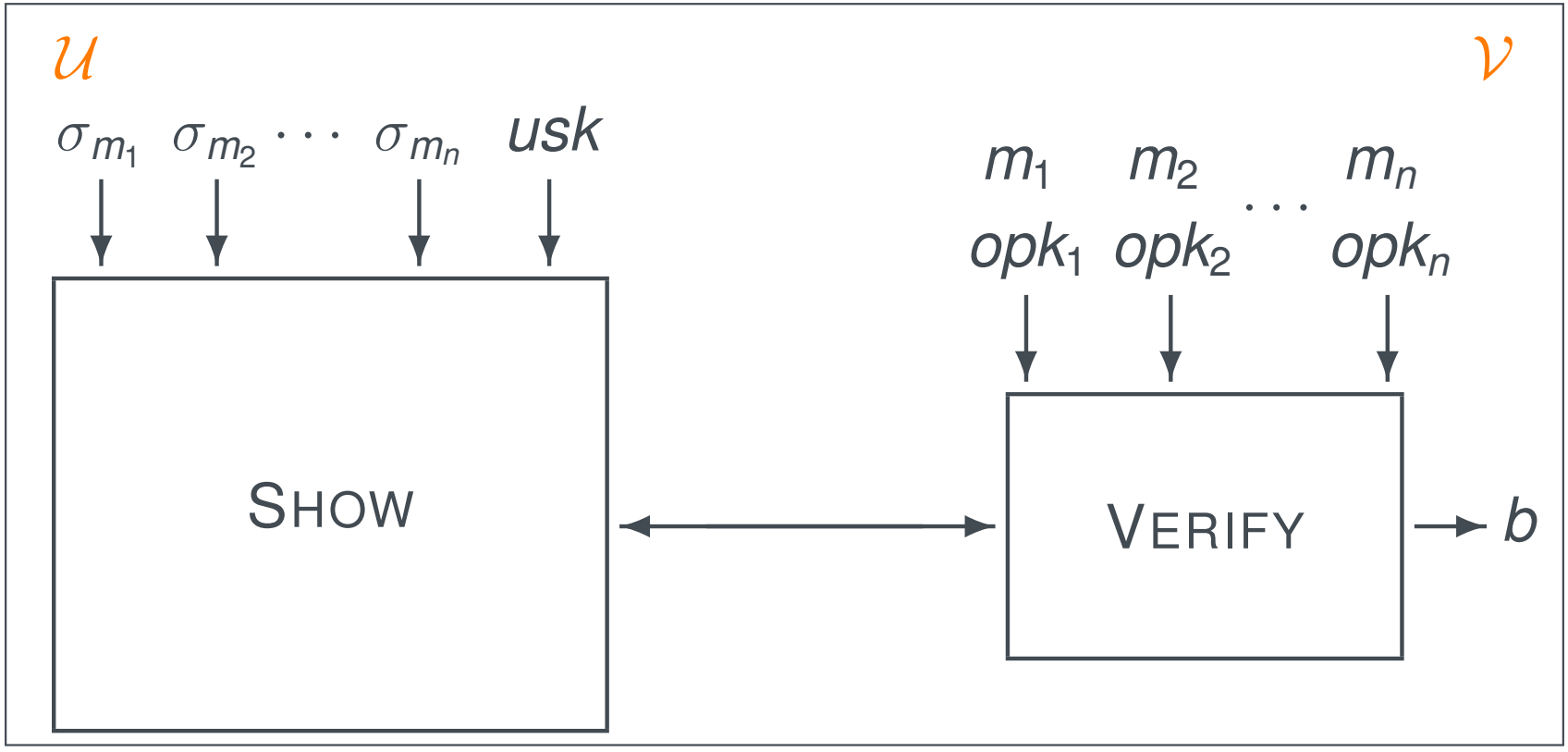


$\sigma_m = \mathcal{AG}.\text{SIGN}(osk, usk, m)$

Construction

Construction générique

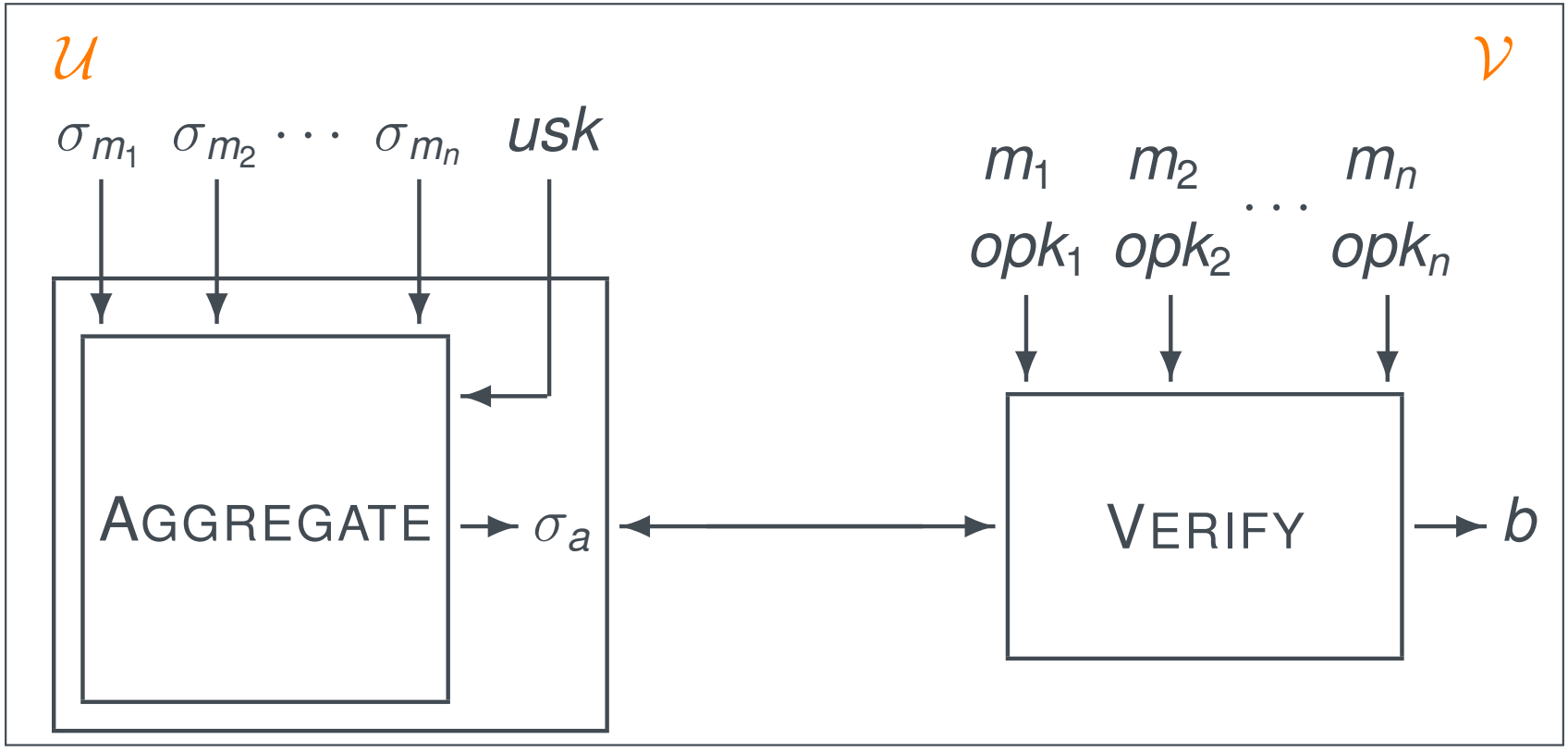
- Utilisation des accréditations



Construction

Construction générique

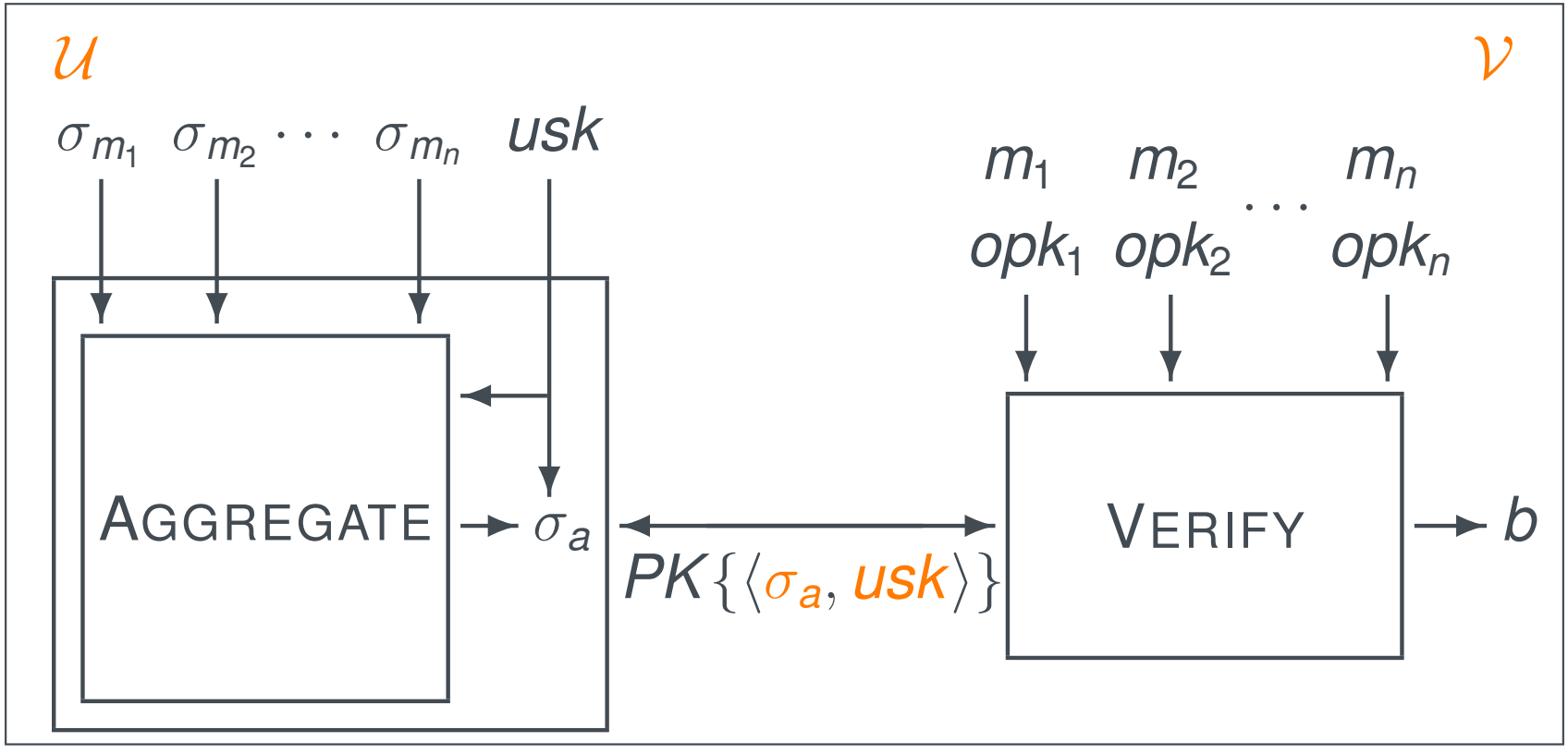
- Utilisation des accréditations



Construction

Construction générique

- Utilisation des accréditations



- Introduction
- Intuition et Construction générique
- Construction à base de couplages
- Extensions et Conclusion

Construction

Environnement de calcul

- Environnement bilinéaire (e, G_1, G_2, G_T, p)
  - G_1, G_2, G_T groupes d'ordre premier p
  - $e : G_1 \times G_2 \rightarrow G_T$ bilinéaire non dégénérée

Construction

Environnement de calcul

- Environnement bilinéaire (e, G_1, G_2, G_T, p)
  - G_1, G_2, G_T groupes d'ordre premier p
  - $e : G_1 \times G_2 \rightarrow G_T$ bilinéaire non dégénérée
- Clefs

$$\begin{cases} opk & : \Gamma = (g_1{}^{\gamma}, g_2{}^{\gamma}) \in G_1 \times G_2 \\ osk & : \gamma \in \mathbb{Z}_p \end{cases}$$

$$\begin{cases} upk & : X = (g_1{}^{x}, g_2{}^{x}) \in G_1 \times G_2 \\ usk & : x \in \mathbb{Z}_p \end{cases}$$

Construction
Certificat

- Certificat BGLS (EUROCRYPT 2003)

$$\sigma = \left(\mathcal{H}(m)\right)^{\gamma}$$

Valide sous $\Gamma = {g_2}^{\gamma}$ si, et seulement si,

$$e(\sigma, g_2) = e(\mathcal{H}(m), \Gamma)$$

Construction
Certificat

- Certificat BGLS (EUROCRYPT 2003)

$$\sigma = \left(u^x \mathcal{H}(\Gamma \| m)\right)^\gamma$$

Valide sous $\Gamma = {g_2}^\gamma$ si, et seulement si,

$$e(\sigma, g_2) = e(u, \Gamma)^x e(\mathcal{H}(\Gamma \| m), \Gamma)$$

Construction

Obtention d'une Accréditation

- $C \leftarrow u^x g_1{}^s$
- $\pi \leftarrow PK\{\langle \alpha, \rho \rangle : X = g_1{}^\alpha \wedge C = u^\alpha g_1{}^\rho\}$

$\xrightarrow{C\ ,\ \pi}$

- $A \leftarrow \left(C \cdot \mathcal{H}(g_1{}^\gamma \| g_2{}^\gamma \| m)\right)^\gamma$

$\xleftarrow{A}$

- $\sigma \leftarrow A \cdot \Gamma_1{}^{-s}$

Construction

Utilisation d'une Liste d'Accréditations

- Agrégation

$$\sigma_a \leftarrow \prod_{n=1}^{N} \sigma_n$$

- Chiffrement ElGamal

$$r \overset{\$}{\leftarrow} \mathbb{Z}_p^* \; ; \; (T_1, T_2) \leftarrow ({g_1}^r, {\sigma_a}^{1/x} \cdot u^r)$$

- Preuve de connaissance sur (x, r, xr)

$$PK\Big\{\langle \beta, \rho, \delta \rangle : \quad T_1 = {g_1}^{\rho} \quad \wedge \quad {T_1}^{\beta} = {g_1}^{\delta} \quad \wedge$$

$$e(T_2, g_2)^{\beta} e(u, g_2)^{-\delta} = e(u, \prod_{n=1}^{N} \Gamma_n)^{\beta} \prod_{n=1}^{N} e(\mathcal{H}(\Gamma_n \| m_n), \Gamma_n)\Big\}$$

Construction

Sécurité

- Correction. Toute accréditation correctement délivrée sera utilisable.
- Non Forgeabilité. Impossible de prouver qu'on possède des accréditations si les organisations ne les ont pas délivrées.
- Anonymat. Les utilisateurs ne sont pas tracés dans leurs actes.

- Introduction
- Intuition et Construction générique
- Construction à base de couplages
- Extensions et Conclusion

Extensions

- Découper les messages en sous-messages et cacher certains attributs.
- Manager d'ouverture.
- Anonymat CCA.
- Impossibilité : prouver des valeurs sur des attributs cachés.

Extensions

Construction dans le modèle standard ?

- [LOASW'06] : remplacer BGLS'03 par Waters'05 et Fiat-Shamir'86 par Groth-Sahai'08.
- Mais : agrégation séquentielle.
- Piste : signature agrégeables synchronisées ? AGH'10

Conclusion

- Utiliser les signatures agrégeables pour faire des accréditations anonymes.
- Transporter les avantages des signatures agrégeables sur les certificats.

merci

orange™