Habilitation à Diriger des Recherches
de l'Université de Caen Basse-Normandie

la cryptographie au service de la protection de la vie privée

Sébastien Canard

Orange Labs

2 décembre 2009

quelques mots pour commencer

- ingénieur de recherche depuis 2003
- employé par le Groupe France Télécom
- domaine de recherche : cryptographie
- domaine application : protection de la vie privée dans les services
- montage, gestion et participation à des projets collaboratifs (PACE, SAVE, CRYPTO++, SPICE)
- encadrement de 3 thésards

quelques mots pour commencer

- ingénieur de recherche depuis 2003
- employé par le Groupe France Télécom
- domaine de recherche : cryptographie
- domaine application : protection de la vie privée dans les services
- montage, gestion et participation à des projets collaboratifs (PACE, SAVE, CRYPTO++, SPICE)
- encadrement de 3 thésards

- mais parlons plutôt d'Alice...

présentation d'Alice

- aujourd'hui, Alice est une étudiante
- elle a 21 ans
- elle a un frère de 16 ans
- elle possède un téléphone mobile
- elle aime bien les voyages et les vêtements
- elle possède un ordinateur avec une connection à Internet

journée n°1

- Alice utilise son téléphone mobile pour se connecter à un site web où elle peut poser des questions médicales
  - elle veut se renseigner sur une maladie particulière
  - comme elle est à l'Université, elle va utiliser son téléphone mobile
  - elle souhaite être anonyme pour ne pas révéler qu'elle s'intéresse à cette maladie
  - mais le site ne propose pas cette option sur mobile...

journée n°1

- Alice utilise son téléphone mobile pour se connecter à un site web où elle peut poser des questions médicales
  - elle veut se renseigner sur une maladie particulière
  - comme elle est à l'Université, elle va utiliser son téléphone mobile
  - elle souhaite être anonyme pour ne pas révéler qu'elle s'intéresse à cette maladie
  - mais le site ne propose pas cette option sur mobile...
- en rentrant à la maison, elle prépare la fête qu'elle va organiser avec ses amies
  - Alice va leur montrer les photos de son dernier voyage en Australie
  - elle ne veut pas que ses amies aient accès à d'autres contenus familiaux ou personnels
  - mais elle ne peut pas le gérer avec l'application proposée...

journée n°2

- Alice doit élire son réprésentant au Conseil d'Administration de l'Université
  - la participation étant très faible, il a été décidé cette année de faire du vote électronique
  - mais le système n'est pas suffisamment sécurisé
  - il y a une fraude et le résultat est compromis...

journée n°2

- Alice doit élire son réprésentant au Conseil d'Administration de l'Université
  - la participation étant très faible, il a été décidé cette année de faire du vote électronique
  - mais le système n'est pas suffisamment sécurisé
  - il y a une fraude et le résultat est compromis...
- après les cours, elle va rentrer chez elle pour surfer sur Internet
  - elle va tout d'abord sur le site web de la mairie de sa ville pour retirer un certificat de naissance
  - puis elle se connecte au site web de son opérateur téléphonique pour faire un achat en ligne
  - elle n'utilise qu'une seule fois son login et mot de passe pour se connecter aux deux services...

journée n°3

- après les cours, Alice veut s'acheter un pull dans un nouveau magasin
  - elle doit d'abord retirer des sous auprès de sa banque, via son téléphone mobile
  - dans le magasin, elle utilise son téléphone mobile pour payer son pull
  - ce dernier est équipé d'une étiquette RFID afin d'en assurer la traçabilité et de lutter contre la contrefaçon
  - tout lecteur d'étiquettes RFID est capable de lire l'identifiant unique de l'étiquette du pull acheté...

journée n°3

- après les cours, Alice veut s'acheter un pull dans un nouveau magasin
  - elle doit d'abord retirer des sous auprès de sa banque, via son téléphone mobile
  - dans le magasin, elle utilise son téléphone mobile pour payer son pull
  - ce dernier est équipé d'une étiquette RFID afin d'en assurer la traçabilité et de lutter contre la contrefaçon
  - tout lecteur d'étiquettes RFID est capable de lire l'identifiant unique de l'étiquette du pull acheté...
- elle va ensuite prêter des sous à son petit frère
  - ils utilisent tous les deux leurs téléphones mobiles pour cet échange
  - Alice utilise les pièces retirées initialement à sa banque
  - la banque est capable de tracer les pièces qu'elle a délivrées à Alice...

bilan sur les journées d'Alice

1. elle ne peut pas être anonyme quand elle utilise son téléphone mobile

bilan sur les journées d'Alice

1. elle ne peut pas être anonyme quand elle utilise son téléphone mobile
2. ses amies peuvent trouver des informations sur sa vie privée, alors qu'elle ne le souhaite pas forcément

bilan sur les journées d'Alice

1. elle ne peut pas être anonyme quand elle utilise son téléphone mobile
2. ses amies peuvent trouver des informations sur sa vie privée, alors qu'elle ne le souhaite pas forcément
3. le résultat du vote auquel elle a participé est erroné

bilan sur les journées d'Alice

1. elle ne peut pas être anonyme quand elle utilise son téléphone mobile
2. ses amies peuvent trouver des informations sur sa vie privée, alors qu'elle ne le souhaite pas forcément
3. le résultat du vote auquel elle a participé est erroné
4. la mairie et son opérateur peuvent croiser leurs bases

bilan sur les journées d'Alice

1. elle ne peut pas être anonyme quand elle utilise son téléphone mobile
2. ses amies peuvent trouver des informations sur sa vie privée, alors qu'elle ne le souhaite pas forcément
3. le résultat du vote auquel elle a participé est erroné
4. la mairie et son opérateur peuvent croiser leurs bases
5. à l'aide de l'étiquette RFID de son pull, n'importe qui est capable de tracer ses déplacements

bilan sur les journées d'Alice

1. elle ne peut pas être anonyme quand elle utilise son téléphone mobile
2. ses amies peuvent trouver des informations sur sa vie privée, alors qu'elle ne le souhaite pas forcément
3. le résultat du vote auquel elle a participé est erroné
4. la mairie et son opérateur peuvent croiser leurs bases
5. à l'aide de l'étiquette RFID de son pull, n'importe qui est capable de tracer ses déplacements
6. la banque et les marchands sont capables de tracer les dépenses/transferts d'Alice

bilan sur les journées d'Alice

1. elle ne peut pas être anonyme quand elle utilise son téléphone mobile
2. ses amies peuvent trouver des informations sur sa vie privée, alors qu'elle ne le souhaite pas forcément
3. le résultat du vote auquel elle a participé est erroné
4. la mairie et son opérateur peuvent croiser leurs bases
5. à l'aide de l'étiquette RFID de son pull, n'importe qui est capable de tracer ses déplacements
6. la banque et les marchands sont capables de tracer les dépenses/transferts d'Alice

$\Longrightarrow$ qu'est ce qu'Alice aurait dû utiliser ?

comment Alice peut-elle être anonyme avec son téléphone mobile ?

authentifications anonymes

- signatures aveugles
  - un utilisateur obtient une signature d'un signataire
  - le signataire ne connaît pas le message
  - il sera incapable de reconnaître a posteriori sa signature
- signatures de groupe
  - capacité de signer des messages au nom du groupe
  - signatures anonymes et intraçables
  - une autorité est capable de lever l'anonymat d'une signature
- signatures d'anneau
  - même principe que les signatures de groupe
  - pas de levé d'anonymat
  - pas d'autorité pour introduire les membres dans le groupe

problématique de l'efficacité

- ces signatures nécessitent de nombreux calculs
  - 11 exponentiations pour un exemple de signature de groupe
  - 43 pour un exemple de signature d'anneau avec 10 membres
- l'implémentation dans un dispositif limité est compromise
- deux solutions
  - faire des hypothèses supplémentaires (ex. inviolabilité du dispositif)

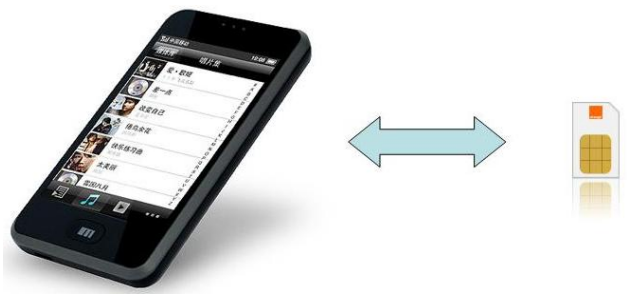
    [S.C., M. Girault, CARDIS 2002]

    [S.C., J. Traoré, CARDIS 2004]
  - se faire assister par une entité plus puissante...

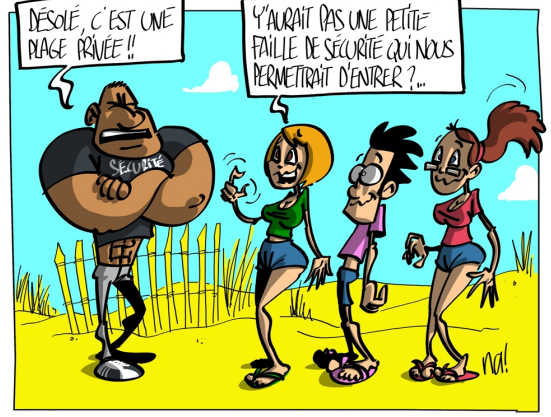
cryptographie anonyme assistée

[S.C., I. Coisel, en soumission]

- introduction d'un intermédiaire
  - grande puissance de calcul
  - se place entre le prouveur et le vérifieur (cas pratique)
  - délégation d'une partie des calculs du prouveur...
  - ... sans compromettre la sécurité
  - il possède éventuellement des connaissances supplémentaires propres au prouveur
- propriétés usuelles des schémas étudiés
  - consistance
  - validité
  - intraçabilité



sécurité *vs.* efficacité



- consistance assistée
  - confiance dans l'intermédiaire
- validité assistée
  - l'adversaire peut corrompre l'intermédiaire
  - il possède donc éventuellement des connaissances supplémentaires
- intraçabilité assistée
  - cas faible
    - l'intermédiaire est de confiance
    - équivalent à la propriété dans le cas non assistée
  - cas fort
    - l'adversaire n'est pas capable de reconnaître le prouveur, même en jouant le rôle de l'intermédiaire
- meilleur gain calculatoire

cas du schéma XSGS

- chaque membre possède (A,u,x) tel que $A^{u+\gamma} = g_1 h^x$
- signature non assistée
  - $T_1 = k^\alpha,\ T_2 = Ah^\alpha,\ T_3 = k^\beta,\ T_4 = Ag^\beta,\ z = u\alpha + x$
  - $\text{POK}\big(z,\alpha,\beta,u : T_1 = k^\alpha \wedge T_3 = k^\beta \wedge T_2/T_4 = h^\alpha/g^\beta \wedge e(T_2,g_2)^u e_{hw}^{-\alpha} e_{hg}^{-z} = e_{gg}/e(T_2,w)\big)(m)$
- signature assistée avec intraçabilité faible
  - l'intermédiaire peut avoir accès à (A,u)
  - $T_1 = k^\alpha,\ T_2 = Ah^\alpha,\ T_1 = k^\beta,\ T_4 = Ag^\beta,\ z = u\alpha + x$
  - $\text{SAPOK}\big(z,\alpha,\beta,u : T_1 = k^\alpha \wedge T_3 = k^\beta \wedge T_2/T_4 = h^\alpha/g^\beta \wedge e(T_2,g_2)^u e_{hw}^{-\alpha} e_{hg}^{-z} = e_{gg}/e(T_2,w)\big)(m)$

cas du schéma XSGS

- chaque membre possède (A,u,x) tel que $A^{u+\gamma} = g_1 h^x$
- signature non assistée
  - $T_1 = k^\alpha,\ T_2 = Ah^\alpha,\ T_3 = k^\beta,\ T_4 = Ag^\beta,\ z = u\alpha + x$
  - $\textsc{Pok}\big(z,\alpha,\beta,u : T_1 = k^\alpha \wedge T_3 = k^\beta \wedge T_2/T_4 = h^\alpha/g^\beta \wedge e(T_2,g_2)^u e_{hw}^{-\alpha} e_{hg}^{-z} = e_{gg}/e(T_2,w)\big)(m)$
- signature assistée avec intraçabilité faible
  - l'intermédiaire peut avoir accès à (A,u)
  - $T_1 = k^\alpha,\ T_2 = Ah^\alpha,\ T_1 = k^\beta,\ T_4 = Ag^\beta,\ z = u\alpha + x$
  - $\textsc{SAPok}\big(z,\alpha,\beta,u : T_1 = k^\alpha \wedge T_3 = k^\beta \wedge T_2/T_4 = h^\alpha/g^\beta \wedge e(T_2,g_2)^u e_{hw}^{-\alpha} e_{hg}^{-z} = e_{gg}/e(T_2,w)\big)(m)$
- sécurité de la preuve de connaissance assistée

[S.C., I. Coisel, J. Traoré, ProvSec 2007]

cas du schéma XSGS

- chaque membre possède (A,u,x) tel que $A^{u+\gamma} = g_1 h^x$
- signature non assistée
  - $T_1 = k^\alpha,\ T_2 = Ah^\alpha,\ T_3 = k^\beta,\ T_4 = Ag^\beta,\ z = u\alpha + x$
  - $\textsc{Pok}\big(z,\alpha,\beta,u : T_1 = k^\alpha \wedge T_3 = k^\beta \wedge T_2/T_4 = h^\alpha/g^\beta \wedge e(T_2,g_2)^u e_{hw}^{-\alpha} e_{hg}^{-z} = e_{gg}/e(T_2,w)\big)(m)$
- signature assistée avec intraçabilité forte
  - l'intermédiaire ne doit pas avoir accès à (A,u)
  - $T_1 = k^\alpha,\ T_2 = Ah^\alpha,\ T_1 = k^\beta,\ T_4 = Ag^\beta,\ z = u\alpha + x$
  - $\textsc{SAPok}\big(z,\alpha,\beta,u : T_1 = k^\alpha \wedge T_3 = k^\beta \wedge T_2/T_4 = h^\alpha/g^\beta \wedge e(T_2,g_2)^u e_{hw}^{-\alpha} e_{hg}^{-z} = e_{gg}/e(T_2,w)\big)(m)$
- sécurité de la preuve de connaissance assistée

[S.C., I. Coisel, J. Traoré, ProvSec 2007]

bilan

Schéma	Version	Complexité
signature de groupe XSGS	standard	11 exponentiations et 1 couplage
	faible	1 exponentiation
	forte	11 exponentiations
signature d'anneau CGS	standard	$\nu^2 + 9\nu + 6$ exponentiations
	faible	9ν exponentiations
	forte	$\nu^2 + 9\nu + 6$ exponentiations
signature aveugle HT	standard	55 exponentiations et 3 couplages
	faible	2 exponentiations
	forte	10 exponentiations et 2 couplages

- son téléphone mobile est puissant mais peu sécurisé
- sa carte SIM est peu puissante mais très sécurisée
- Alice fait confiance à son mobile du point de vue l'anonymat

$\Longrightarrow$ Alice peut maintenant se servir de son mobile pour être anonyme

comment Alice peut-elle protéger et diffuser ses contenus numériques ?

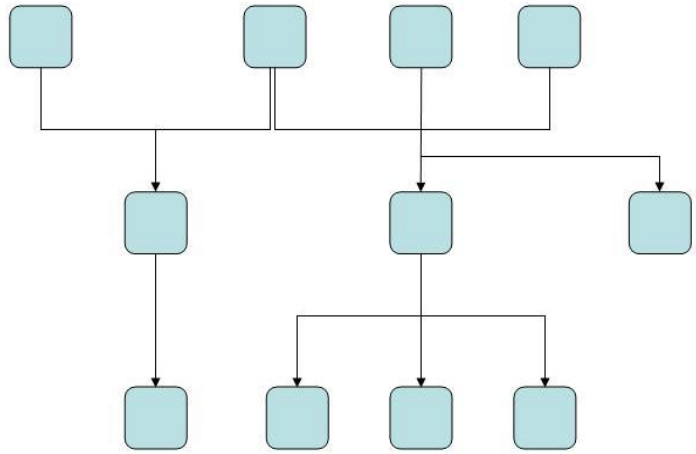
la protection des contenus

- protection des contenus dans un contexte de groupe
  - ici, la famille
  - chaque contenu va être chiffré avec une clé particulière
- membres (au sens large) d'une famille
  - les parents, les enfants, les amis
  - les personnes appartiennent à plusieurs catégories
    - famille (au sens strict) qui n'inclut pas les amis
    - adulte, ce qui inclut les amis, mais pas les enfants (contrôle parental)
- chacun possède des droits différents sur les contenus
  - chacun va posséder une clé de déchiffrement qui lui est propre
  - elle doit lui permettre de déchiffrer les contenus liés aux catégories auxquelles il appartient

$\Longrightarrow$ représentation par un graphe

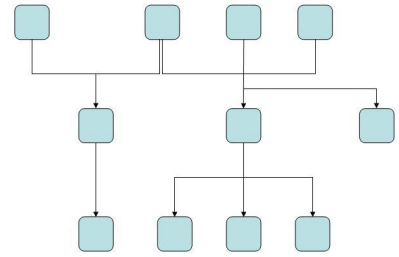
problématique de gestion des clés

- chaque membre appartient à un nœud du graphe
- chaque nœud est lié à une clé de déchiffrement
- un nœud doit avoir accès à toutes les clés des nœuds en dessous
- un nœud ne doit pas avoir accès aux clés des nœuds au dessus
- graphe orienté acyclique avec plusieurs racines
- exemple :



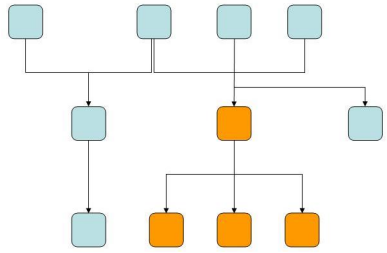
$\Longrightarrow$ comment gérer les clés dans ce graphe ?

une solution



[S.C., A. Jambert, Indocrypt 2008]

une solution

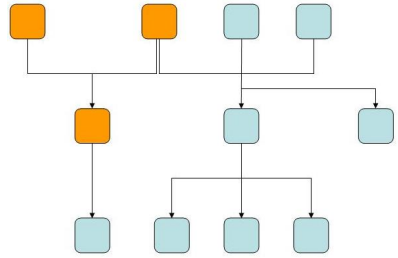


[S.C., A. Jambert, Indocrypt 2008]

- cas un père

$$k_{fils} = \mathrm{HMAC}(k_{pere} \| C \| c_{pere})$$

une solution



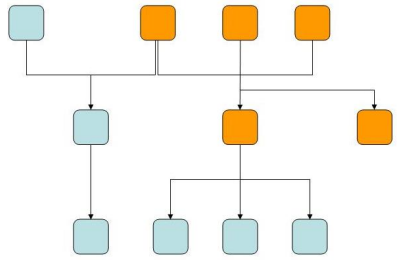
[S.C., A. Jambert, Indocrypt 2008]

- cas un père

$$k_{fils} = \mathrm{HMAC}(k_{pere} \| C \| c_{pere})$$

- cas plusieurs pères et un fils
  - utilisation d'un système de gestion de clés dans un groupe non hiérarchique
  - généralisation du Diffie-Hellman à plusieurs acteurs

une solution

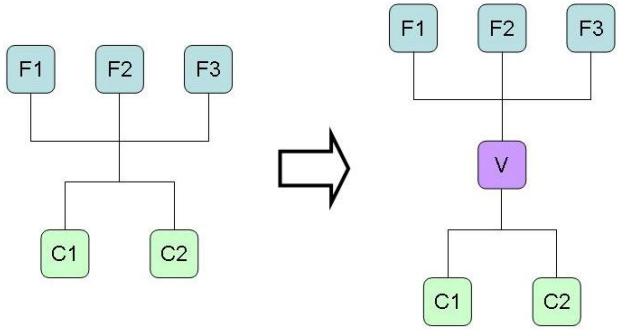


[S.C., A. Jambert, Indocrypt 2008]

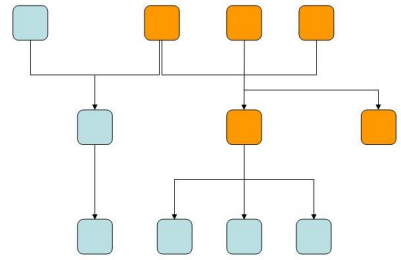
- cas un père

$$k_{fils} = \mathrm{HMAC}(k_{pere} \| C \| c_{pere})$$

- cas plusieurs pères et un fils
  - utilisation d'un système de gestion de clés dans un groupe non hiérarchique
  - généralisation du Diffie-Hellman à plusieurs acteurs
- cas plusieurs pères et plusieurs fils



une solution

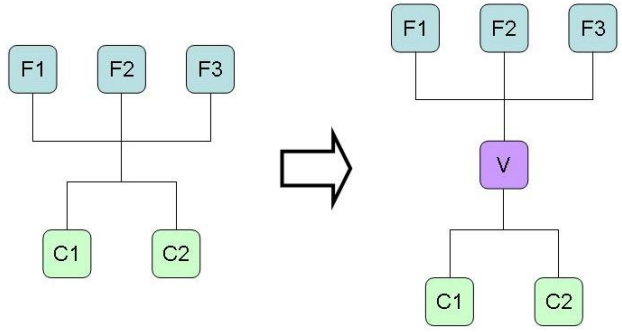


[S.C., A. Jambert, Indocrypt 2008]

- cas un père

$$k_{fils} = \mathrm{HMAC}(k_{pere} \| C \| c_{pere})$$

- cas plusieurs pères et un fils
  - utilisation d'un système de gestion de clés dans un groupe non hiérarchique
  - généralisation du Diffie-Hellman à plusieurs acteurs
- cas plusieurs pères et plusieurs fils



$\Longrightarrow$ Alice peut maintenant protéger ses contenus en toute souplesse

quel système de vote électronique aurait dû utiliser l'Université ?

le vote électronique

- propriétés de sécurité
  - vérification universelle du vote
  - secret du vote
  - démocratie
  - pas de résultat partiel
  - sans reçu
- grandes familles de constructions cryptographiques
  - chiffrement homomorphique [SAVE, non publié]
  - réseau de mélangeurs universellement vérifiable
  - signatures avec anonymat

focus sur les signatures avec anonymat

- signatures de groupe
  - pas adaptées (intraçabilité, révocation d'anonymat)
  - il faut utiliser les signatures de liste
    [S.C., B. Schoenmakers, M. Stam, J. Traoré, Journal DAM]
  - utilisation d'une carte à puce, sous l'hypothèse d'inviolabilité
    [S.C., H. Sibert, FEE 2006]
- signatures aveugles
  - le votant chiffre son choix
  - le votant obtient une signature aveugle de ce chiffré
  - le votant envoie son bulletin dans l'urne
  - problématique de l'anonymat lors de l'envoi

$\Longrightarrow$ utilisation d'un réseau de mélangeurs
(non universellement vérifiable)

vote et signatures aveugles

- système de vote Votopia (utilisé par l'Université d'Alice)

  $\Longrightarrow$ le premier mélangeur peut tricher

  - si $n < N$
    - remplace des bulletins aléatoires par des bulletins non envoyés
  - si $n = N$
    - demande à des complices d'envoyer des faux bulletins
    - remplace des bulletins aléatoires par les bulletins de ses complices
- le premier mélangeur doit prouver qu'il a bien fait son travail
  - mais le permier et second mélangeurs peuvent tricher ensemble
  - le second mélangeur doit aussi être universellement vérifiable...

    $\Longrightarrow$ on a besoin d'un réseau de mélangeur universellement vérifiable

    $\Longrightarrow$ plus besoin de la signature aveugle
- utilisation d'un schéma de signature aveugle à anonymat révocable

  [S.C., M. Gaud, J. Traoré, Financial Cryptography 2006]

anonymat révocable

[S.C., M. Gaud, J. Traoré, Financial Cryptography 2006]

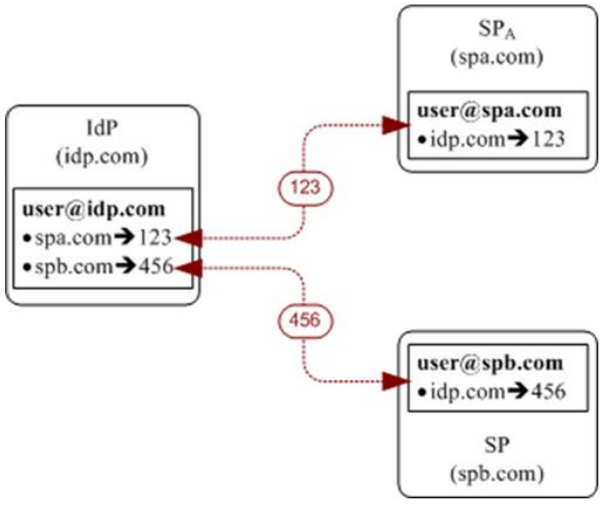
- obtient le message et la signature à partir du protocole initial
  - tout bulletin non envoyé est mis sur liste de révocation
  - les bulletins rajoutés par le premier mélangeurs seront refusés
- obtient l'identité de l'utilisateur après divulgation du message et de la signature
  - révocation de l'anonymat des faux bulletins après passage par le réseau de mélangeurs
  - si un problème, le réseau de mélangeurs doit prouver sa bonne foi

$\Longrightarrow$ Alice peut maintenant voter en toute tranquilité

quelle technologie Alice doit-elle utiliser pour ne pas que la mairie et son opérateur puissent croiser leurs bases de données ?

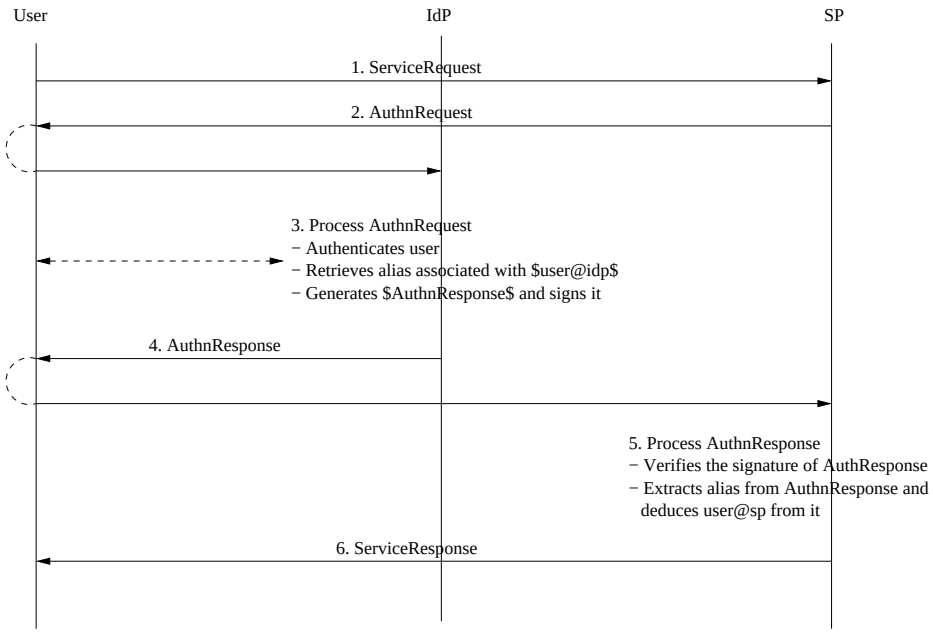
fédération d'identité

- Alice veut accéder à plusieurs services
  - a priori, elle doit s'authentifier à chaque fois
  - mais elle a fédéré ses identités
    $\Longrightarrow$ une seule authentification nécessaire
- rôle de la mairie (IdP)
  - authentifier Alice
  - certifier à l'opérateur (SP) qu'elle a authentifié Alice
- utilisation d'un alias pour référencer Alice chez le SP
- qu'est ce qu'un alias ?
  - valeur pseudo-aléaoire
  - signé par l'IdP
  - généré par le SP ou l'IdP
  - pas de correspondance avec Alice
  - différent d'un SP à un autre



authentification jetable (SSO)

- si les identités sont fédérées, le SSO est possible
- permet à Alice de ne s'authentifier qu'une seule fois
- l'IdP retrouve l'alias correspondant à alice@idp et le SP
- le SP n'a pas besoin d'authentifier Alice
  - il extrait l'alias de la requête
  - et l'utilise pour retrouve l'identité d'Alice



identité et protection de la vie privée

- premier niveau de protection de la vie privée
- problème avec le système actuel
  - IdP et SP peuvent corréler leurs bases
  - IdP a toute l'information pour corréler les identités d'Alice
- est ce un problème ?
  - corrélation désirée dans certains cas (*Circle Of Trust*)
  - exemple de *COT* : administratif, bancaire, loisir, etc.
  - mais pas entre *COT*
- introduction de la fédération d'identité "côté client"

[S.C., E. Malville, J. Traoré, ACM DIM]

identité et protection de la vie privée

- la fédération d'identité est identique à celle de l'Alliance Liberty
- l'IdP doit signer l'alias de fédération
  - sans le connaître
  - sans être capable de reconnaître sa signature a posteriori
  - tout en authentifiant l'utilisateur

    $\Longrightarrow$ nous avons besoin d'une signature aveugle
- structure d'une réponse d'authentification
  - contient l'alias de fédération d'Alice
  - contient des données (identifiant de requête, date, etc.) permettant de tracer la requête
  - contient des données générales telles que les balises SAML ou l'identité du SP
  - toutes ces données sont signées par l'IdP

une nouvelle signature aveugle

- masquer ou ne pas masquer ?
  - l'alias doit être masqué
  - les données de "traçage" doivent aussi être masquées
  - les données générales NE doivent PAS être masquées

  $\Longrightarrow$ nous avons besoin d'une signature partiellement aveugle
- intéressons nous à l'alias
  - il doit être le même à chaque authentification jetable
  - l'IdP doit vérifier que c'est le même
  - nous devons introduire un nouveau type de signature aveugle

$\Longrightarrow$ la signature partiellement aveugle invariable

[S.C., E. Malville, J. Traoré, Journal IIS]

$\Longrightarrow$ Alice utilise facilement et en toute sécurité la fédération d'identité

comment faire en sorte que le pull d'Alice ne permette pas de tracer ses mouvements ?

systèmes RFID

- les étiquettes RFID doivent remplacer les codes à barres
  - identifiant unique EPC
  - embarquer de la sécurité
  - moins l'étiquette est chère, moins elle est puissante
  - nécessité d'adapter les algorithmes cryptographiques
- outils cryptographiques disponibles
  - aucune multiplication modulaire (ex. de GPS)
  - quelques algorithmes à clé secrète (XOR, AES, PRESENT, etc.)
- authentification et identification d'une étiquette RFID
  - une étiquette valide doit toujours être acceptée par le lecteur
  - une étiquette non valide doit être refusée par le lecteur
  - notion de protection de la vie privée...
    - authentification et identification par un lecteur autorisé
    - anonymat et intraçabilité pour les autres

[S.C., I. Coisel, M. Girault, en soumission]

constructions à base de clé secrète

- l'étiquette et le lecteur autorisé partagent une même clé secrète
- anonymat des étiquettes
  - le lecteur autorisé ne sait pas a priori à quelle étiquette il a affaire
  - recherche exhaustive sur l'ensemble des étiquettes valides
- intraçabilité des étiquettes
  - les systèmes actuels nécessitent une mise à jour de la clé partagée
- attaques possibles
  - suffisamment désynchroniser l'étiquette et le lecteur
    $\Longrightarrow$ une étiquette valide peut être refusée
  - envoyer une valeur aléatoire au lecteur
    $\Longrightarrow$ le lecteur ne va jamais trouver d'étiquette correspondante

$\Longrightarrow$ il faut une modélisation supplémentaire dans ce cas

[S.C., I. Coisel, RFIDSec 2008]

un construction à base de clé publique

[S.C., I. Coisel, M. Girault, en soumission]

Etiquette RFID		Lecteur
		$a \in_R \{0,1\}^k$
$b \in_R \{0,1\}^k$	$\xleftarrow{\quad a \quad}$	
$T_0 = f(\mathsf{sk}[\mathsf{ID}], a \Vert b)$		
$T_1 = (T_0 \Vert \mathsf{k}[\mathsf{ID}] \Vert b) \oplus \mathcal{H}(y^w)$		
$T_2 = g^w$	$\xrightarrow{\quad T_1, T_2 \quad}$	$T_0 \Vert \mathsf{k}[\mathsf{ID}] \Vert b = T_1 \oplus \mathcal{H}(T_2^x)$
		Vérifie T_0

- implémentation pratique
  - utilisation des coupons pour $\mathcal{H}(y^w)$ et T_2
  - utilisation de PRESENT en mode CBC pour la fonction f

    $\Longrightarrow$ taille $\approx$ 1200 portes équivalentes, exécution $\approx$ 100 ms
- autre possibilité : utiliser un algorithme de chiffrement à clé publique

[S.C., I. Coisel, J. Etrog, WLC 2010]

$\Longrightarrow$ le pull ne révèle plus rien aux lecteurs extérieurs

quel système utiliser pour ne pas que la banque et les marchands tracent les dépenses/transerts de pièces d'Alice ?

monnaie électronique

- émulation électronique de la monnaie traditionnelle
  - Alice peut retirer des sous à sa banque (porte-monnaie)
  - Alice peut dépenser des sous auprès des marchands
  - Alice peut transférer des sous dans un autre porte-monnaie
  - anonymat et intraçabilité d'Alice dans ses dépenses/transferts
- qu'est ce qu'on entend par anonymat et intraçabilité ?
  - vis-à-vis des marchands
  - vis-à-vis de la banque
  - mais pas en cas de fraude
    - cas de la double-dépense
    - autres cas (monnaie équitable)

concept de pièce électronique

- qu'est ce qu'une pièce de monnaie électronique ?
  - un numéro de série
  - une validation (signature) de ce numéro de série par la banque
- qu'est ce que la dépense d'une pièce ?
  - preuve qu'on utilise une pièce validée par la banque
  - preuve de connaissance d'une signature de la banque
  - ne pas révéler son identité

    $\Longrightarrow$ ne révéler ni le numéro de série, ni la signature de la banque
- la monnaie électronique efficace nécessite
  - des procédures rapide
  - la manipulation de données de petite taille

efficacité du retrait

- système *compact e-cash*
  - basé sur les schémas de signature de groupe
  - retrait efficace de 2^L pièces
  - porte-monnaie compact
- principe
  - utilisation d'un compteur incrémenté $j \in [1,J]$ à chaque dépense
  - nécessité d'une preuve qu'un secret appartient à un intervalle

    [S.C., I. Coisel, A. Jambert, J. Traoré, en soumission]

    [S.C., C. Dulong, non publié]
- amélioration possible

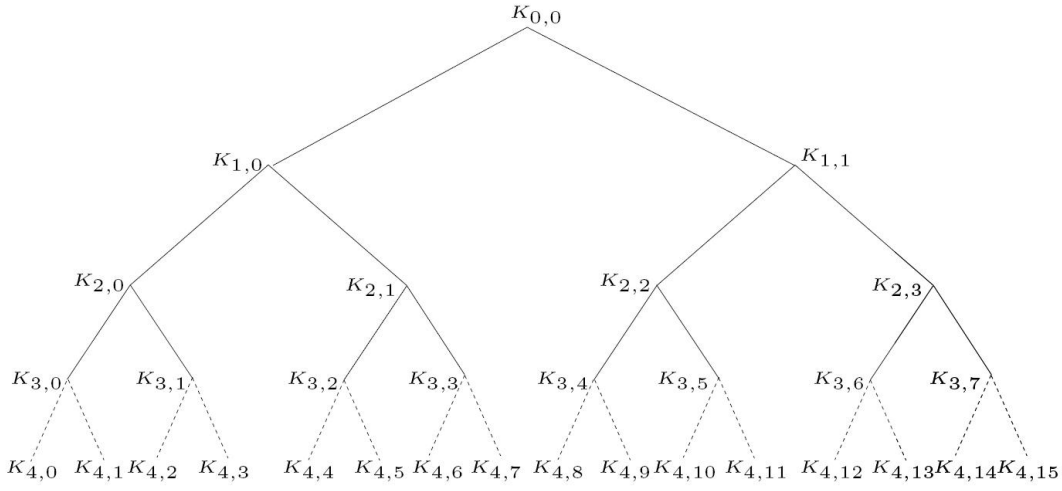
  [S.C., A. Gouget, E. Hufschmitt, ACNS 2006]
  - retrait efficace d'un nombre quelconque J de pièces
  - gestion des pièces de valeurs différentes

efficacité de la dépense

- basé sur *compact e-cash*
  - calcul et taille des données toujours proportionnels en le nombre de pièces ℓ dépensées
- nouvelle vision des choses [PACE, ISC 2009]
  - dépense ultra compacte, en $\mathcal{O}(\log \ell)$
  - utilisation du *batch RSA* en version aveugle
  - permet de décomposer une signature RSA sur plusieurs messages en une unique signature sur plusieurs sous-messages
- utilisation de la monnaie divisible...

monnaie divisible

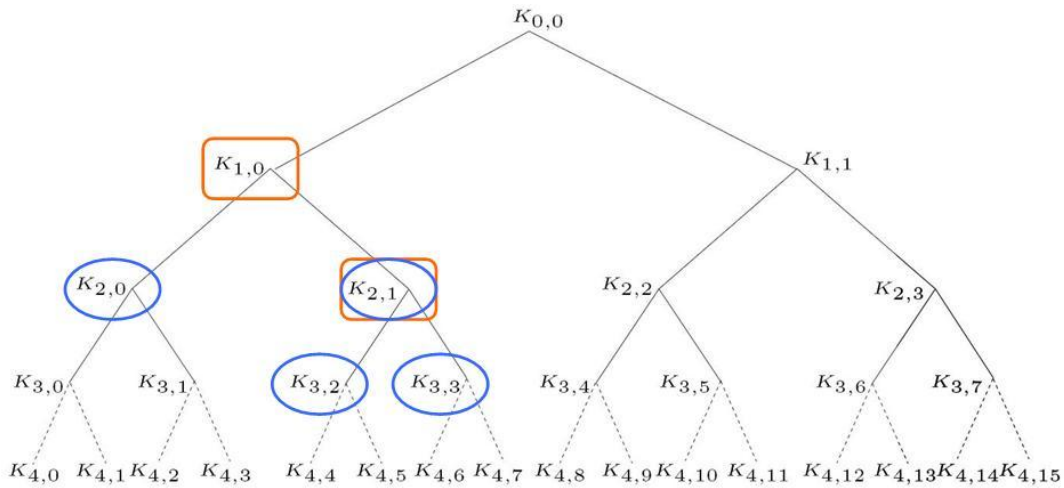
- retrait d'une grosse pièce de monnaie
- possibilité de diviser cette pièce en petites pièces, en fonction des dépenses
- problématiques d'anonymat
  - infaisable de savoir si deux dépenses proviennent de la même pièce retirée
  - infaisable de savoir quelle partie de la pièce est dépensée



anonymat fort

[S.C., A. Gouget, Eurocrypt 2007]

- premier système avec toutes les propriétés d'anonymat énoncées
- construction générique pour la dépense d'un nœud
  - numéro de série = clé des deux nœuds fils
  - tag de sécurité = chiffrement de l'identité du dépenseur à l'aide de la clé du nœud dépensé
- première tentative de réalisation pratique par Au-Susilo-Mu
  - très grande efficacité
  - mais seulement non-falsification statistique



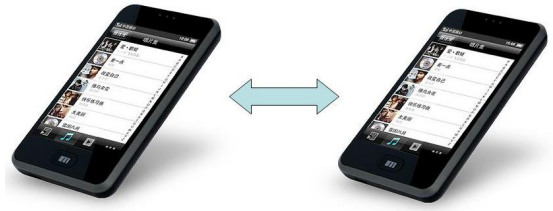
anonymat fort et efficacité

[S.C., A. Gouget, Financial Cryptography 2010]

- utilisation d'un accumulateur
  - accumulation des nœuds d'un même niveau
  - accumulation de tous les nœuds ensemble (sauf la racine)
- retrait
  - signature de tous les accumulateurs par la banque
  - rajout d'un secret de liaison et de la clé secrète utilisateur
- efficacité de la dépense
  - prouver que le nœud dépensé est bien dans deux accumulateurs
  - prouver que les deux accumulateurs sont bien signés

  $\Longrightarrow$ la complexité en temps et espace est sous-linéaire

la monnaie transférable



- une pièce reçue peut à nouveau être dépensée
- peu d'attention reçue
  - meilleurs systèmes nécessitent le retrait d'une pièce vide
  - Chaum et Pedersen ont montré qu'une pièce transférée grossit nécessairement
- mais...
  - les capacités de stockage sont de plus en plus importantes
  - ce grossissement peut être rendu minime
- difficulté : chaque dépenseur doit insérer son identité et prouver la validité de sa dépense

construction efficace

[S.C., A. Gouget, J. Traoré, Financial Cryptography 2008]

- premier schéma efficace de monnaie transférable
- plus besoin de préalablement interagir avec la banque
- principe
  - le numéro de série est tout le temps le même
  - le tag de sécurité dépend
    - du numéro de série
    - d'une valeur pseudo-aléatoire utilisée lors de la dépense précédente
    - de la clé secrète du dépenseur
    - de l'historique de la pièce

anonymat des pièces transférables

[S.C., A. Gouget, ACNS 2008]

- anonymat faible
  - infaisable de faire le lien entre un retrait et une dépense
- anonymat fort
  - infaisable de savoir si deux dépenses proviennent du même utilisateur
- anonymat complet
  - infaisable de reconnaître une pièce que l'on a déjà vu
  - proposition d'une construction générique
- anonymat parfait
  - infaisable de savoir une pièce reçu a déjà été en notre possession
  - propriété inatteignable si $\mathcal{A}$ est tout puissant (Chaum-Pedersen)
  - propriété inatteignable si l'adversaire est la banque
  - construction générique dans les autres cas

$\Longrightarrow$ Alice peut dépenser/transférer efficacement ses pièces tout en protégeant sa vie privée

conclusion

- Alice sait maintenant comment protéger sa vie privée
  - quand elle utilise son téléphone mobile
  - avec ses contenus numériques
  - quand elle vote
  - quand elle se connecte à ses sites favoris
  - lorsqu'elle s'habille
  - dans ses dépenses

conclusion

- Alice sait maintenant comment protéger sa vie privée
  - quand elle utilise son téléphone mobile
  - avec ses contenus numériques
  - quand elle vote
  - quand elle se connecte à ses sites favoris
  - lorsqu'elle s'habille
  - dans ses dépenses
- on aurait aussi pu aborder
  - la facturation anonyme du paiement d'Alice chez son opérateur...
    [S.C., A. Jambert, en soumission]
  - ...et l'utilisation des signatures "déléguées"
    [S.C., F. Laguillaumie, M. Milhau, ACNS 2008]
    [S.C., A. Jambert, CT-RSA 2010]
  - la santé
    [F. Boudet, S.C., S. Guilloteau, non publié]

perspectives... Quelques exemples

- cryptographie assistée
  - faire des *benchmark* précis pour des cas pratiques
  - prendre en compte les échanges entre le prouveur et l'intermédiaire
  - modélisation et constructions sans faire confiance à l'intermédiaire

perspectives... Quelques exemples

- cryptographie assistée
  - faire des *benchmark* précis pour des cas pratiques
  - prendre en compte les échanges entre le prouveur et l'intermédiaire
  - modélisation et constructions sans faire confiance à l'intermédiaire
- problématique d'attestation anonyme
  - étude des briques de base
  - révocation des droits d'attestation

perspectives... Quelques exemples

- cryptographie assistée
  - faire des *benchmark* précis pour des cas pratiques
  - prendre en compte les échanges entre le prouveur et l'intermédiaire
  - modélisation et constructions sans faire confiance à l'intermédiaire
- problématique d'attestation anonyme
  - étude des briques de base
  - révocation des droits d'attestation
- preuves de connaissance
  - utiliser les preuves de sécurité pour construire des systèmes

perspectives... Quelques exemples

- cryptographie assistée
  - faire des *benchmark* précis pour des cas pratiques
  - prendre en compte les échanges entre le prouveur et l'intermédiaire
  - modélisation et constructions sans faire confiance à l'intermédiaire
- problématique d'attestation anonyme
  - étude des briques de base
  - révocation des droits d'attestation
- preuves de connaissance
  - utiliser les preuves de sécurité pour construire des systèmes
- les systèmes RFID
  - trouver un chiffrement à clé secrète où l'aléa du chiffrement n'est pas nécessaire (ni retrouvable) par le lecteur qui déchiffre

perspectives... Quelques exemples

- cryptographie assistée
  - faire des *benchmark* précis pour des cas pratiques
  - prendre en compte les échanges entre le prouveur et l'intermédiaire
  - modélisation et constructions sans faire confiance à l'intermédiaire
- problématique d'attestation anonyme
  - étude des briques de base
  - révocation des droits d'attestation
- preuves de connaissance
  - utiliser les preuves de sécurité pour construire des systèmes
- les systèmes RFID
  - trouver un chiffrement à clé secrète où l'aléa du chiffrement n'est pas nécessaire (ni retrouvable) par le lecteur qui déchiffre
- monnaie électronique
  - utiliser la puissance des preuves Groth-Sahai, tout en améliorant leur efficacité
  - trouver d'autres principes pour le transfert de pièces

merci