Thèse de Doctorat
Université de Caen

Les Preuves de Connaissance et leurs Preuves de Sécurité

David Pointcheval

Travaux effectués au
Laboratoire d'Informatique
École Normale Supérieure

Plan

- Introduction
- Preuves de Sécurité
- Preuves de Connaissance
- Identification : PPP
  - Problème de base
  - Difficulté
  - Schéma
  - Performances
- Signature Électronique
  - Sécurité
  - Attaques
  - Résultat de sécurité
- Signature en Blanc
  - Sécurité
  - Attaques
  - Résultat de Sécurité
- Monnaie Électronique
- Conclusion

Introduction

La cryptographie a pour but de garantir

- la confidentialité des correspondances
  $\Longrightarrow$ chiffrement

- l'identité d'un correspondant
  $\Longrightarrow$ authentification, preuves d'identité

Et il existera toujours des fraudeurs pour tenter de

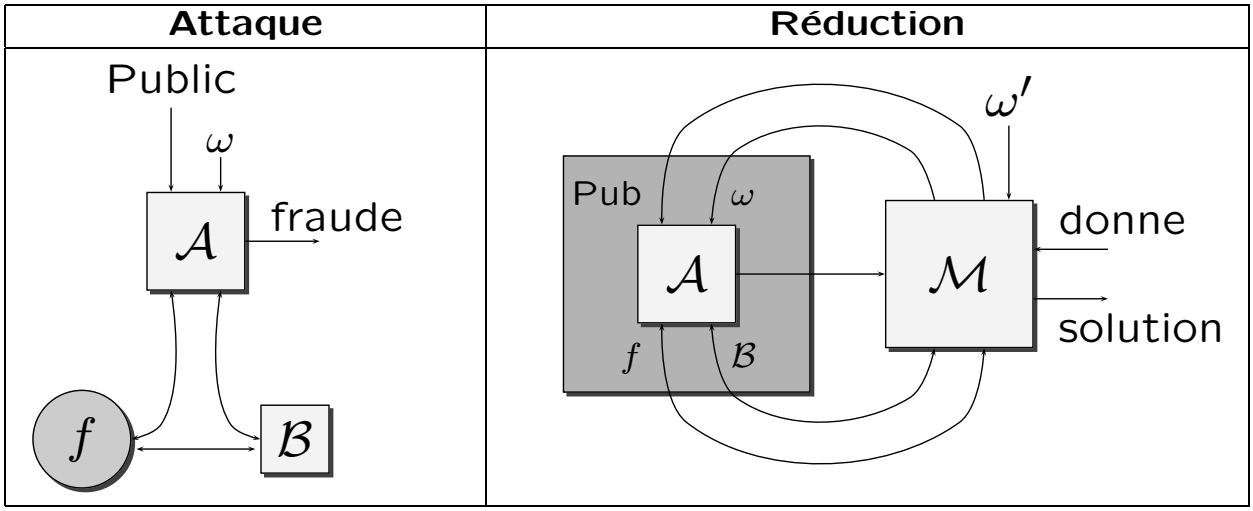
- violer la confidentialité
- falsifier une identité

Preuves de Sécurité

Le schéma S est sûr

- **Couramment :**
  on ne voit pas comment l'attaquer.

- **Preuve formelle :**
  un attaquant $\mathcal{A}$ permettrait la résolution efficace
  d'un problème P réputé très difficile.
  (factorisation, logarithme discret, RSA,
  PKP, SD, CLE, PPP, ...)



- *modèle de l'oracle aléatoire*
  fonction de hachage = fonction parfaitement aléatoire
- *théorie de la complexité*
  efficace = polynomial probabiliste

Preuves de Connaissance

En cryptographie, les preuves de connaissance
sont utilisées pour des **preuves d'identité**.

Alice publie une instance y d'un problème P,
dont elle **seule** connaît une solution x.

y est la clé publique d'Alice
x est la clé secrète d'Alice.

La preuve d'identité d'Alice consiste
à prouver qu'elle connaît une solution au problème P.

Identification

Alice prouve interactivement son identité,
en prouvant sa connaissance d'une solution au problème P.

- Première solution : mot de passe = révélation de la solution
  un espion passif sur la ligne apprend le secret
  dans tous les cas, le vérifieur apprend le secret

- Deuxième solution : preuve à divulgation nulle de connaissance
  selon l'utilisation,
  - parallèle : un espion passif n'apprendra rien
  - séquentiel : même malhonnête, le vérifieur n'apprendra rien

Histoire

- 1985 – théorie des « preuves à divulgation nulle de connaissance »
  (Goldwasser – Micali – Rackoff)
- 1986 – Schéma de Fiat–Shamir (racine carrée modulaire)
  premier protocole d'identification
  « à divulgation nulle de connaissance »
- 1989 – Schéma de Schnorr (logarithme discret)
- 1989 – PKP (Shamir)
  premier protocole non basé sur la théorie des nombres
- 1993 – SD (Stern)
- 1994 – CLE (Stern)
- 1995 – PPP – le Problème des Perceptrons Permutés

Identification de Schnorr

Preuve de connaissance du logarithme discret de y en base g.

Alice		Bob
p et q premiers tels que $q\|(p-1)$		
g élément de $(\mathbb{Z}/p\mathbb{Z})^\star$ d'ordre $q \geq 2^t$		
clé secrète : $x \in (\mathbb{Z}/q\mathbb{Z})^\star$		
clé publique : $y = g^{-x} \bmod p$		
$k \in (\mathbb{Z}/q\mathbb{Z})^\star$		
$r = g^k \bmod p$	$\xrightarrow{r}$	
	$\xleftarrow{e}$	$e \in \mathbb{Z}/2^t\mathbb{Z}$
$s = k + ex \bmod q$	$\xrightarrow{s}$	
		$r \stackrel{?}{=} g^s y^e \bmod p$

Le Problème des Perceptrons Permutés

- Définition
  ε-matrice : matrice dont les composantes sont $+1$ ou -1.
  (idem pour ε-vecteur).

- Problème des Perceptrons
  Données : une ε-matrice A de taille $m \times n$.
  Trouver un ε-vecteur Y de taille n tel que $A \cdot Y \geq 0$.

- Problème des Perceptrons Permutés
  Données : une ε-matrice A de taille $m \times n$
  et un multi-ensemble S de m entiers positifs.
  Trouver un ε-vecteur Y de taille n tel que
  $\{\{(AY)_i | i = 1, \ldots m\}\} = S$ (ou $\exists \pi \ AY = S_\pi$).

Propriétés

- PP est $\mathcal{NP}$-complet
- Max-PP est Max-$\mathcal{SNP}$-dur
- PPP est $\mathcal{NP}$-complet

$\Longrightarrow$ complexité théorique : il existe des instances très difficiles.

Attaques pratiques : apparemment, peu d'instances faciles.

Pour une instance de taille 101×117
le temps moyen d'une attaque de PPP
est de plus de 1000 ans.

Temps d'attaque

taille	solutions	temps PP	temps PPP	
81×97	$5.1\ 10^8$	8 s	$1.4.10^9$ s	45 ans
101×117	$9.4\ 10^9$	12 s	$3.9.10^{10}$ s	1250 ans
121×137	$1.7\ 10^{11}$	25 s	$1.5.10^{12}$ s	47 mille ans
141×157	$2.7\ 10^{12}$	70 s	$6.6.10^{13}$ s	2 millions d'années
171×187	$1.7\ 10^{14}$	180 s	$1.0.10^{16}$ s	340 millions d'années
201×217	$8.7\ 10^{15}$	800 s	$2.4.10^{18}$ s	77 milliards d'années

Protocoles d'identification

Problème difficile
$\Longrightarrow$ protocole d'identification « à divulgation nulle de connaissance ».

Efficacité ?

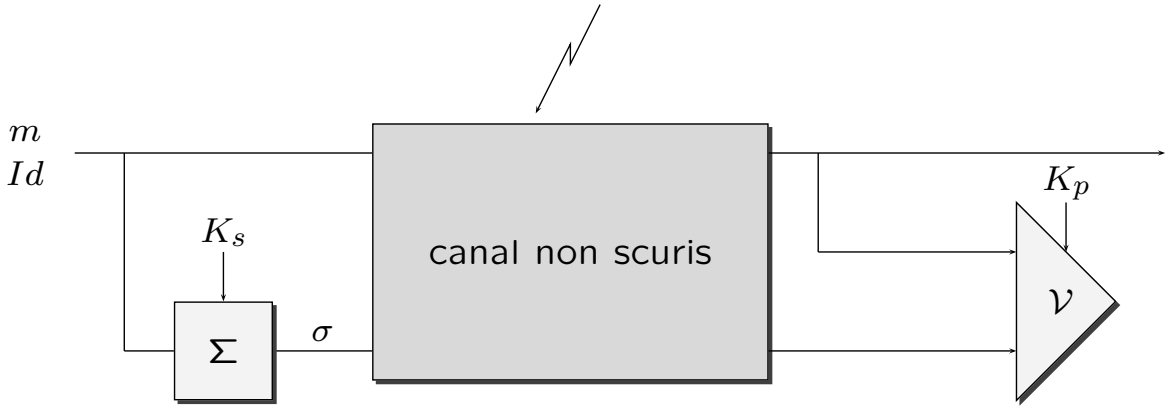
- protocole à 3 passes
  probabilité de fraude inférieure à 3/4 à chaque tour $\Longrightarrow$ 48 tours
- protocole à 5 passes
  probabilité de fraude inférieure à 2/3 à chaque tour $\Longrightarrow$ 35 tours

Tous deux à *divulgation nulle de connaissance*
$\Longrightarrow$ sûrs contre les attaques actives

Performances

	PKP	SD	CLE	PPP 3p	PPP 5p
matrice	16×34	256×512	24×24	101×117	
dans l'ensemble	$\mathbb{F}_{251}$	$\mathbb{F}_2$	$\mathbb{F}_{16}$	$\{-1,+1\}$	
complexité	2^{70}	2^{68}	2^{73}	2^{61}	
nombre de passes	5	3	5	3	5
nombre de tours	20	35	20	48	35
clé publique (bits)	272	256	80	149	
clé secrète (bits)	204	512	80	117	
transm./tour (bits)	741	954	824	896	1040
transm. (kOctets)	1.81	4.08	2.01	5.25	4.44

Signature Électronique



Seul le possesseur de K_s associée à K_p
est capable de fournir un certificat σ, du message m.

Ce certificat garantit l'identité de l'expéditeur
et l'intégrité du message.

Signature de Schnorr

- commun : p, q entiers premiers, $g \in (\mathbb{Z}/p\mathbb{Z})^\star$ d'ordre q
  clé secrète : $x \in (\mathbb{Z}/q\mathbb{Z})^\star$
  clé publique : $y = g^{-x} \bmod p$

- $r = g^k \bmod p$ où $k \in_R (\mathbb{Z}/q\mathbb{Z})^\star$
- $e = f(m, r)$
- $s = k + ex \bmod q$

- $g^s y^e \stackrel{?}{=} r \bmod p$ avec $e = f(m, r)$

$\sigma = (r, e, s)$ signature de m.

Sécurité des Signatures Électroniques

Falsifications :

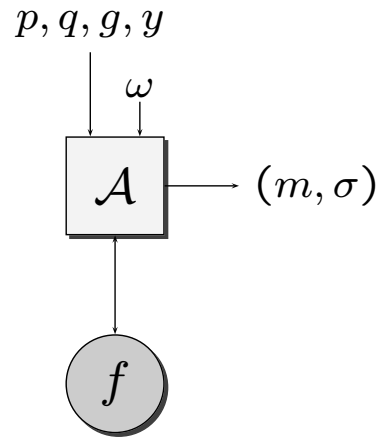
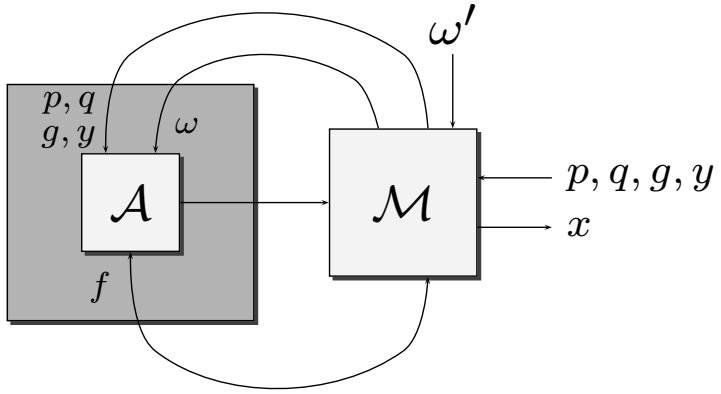
- cassage total
- falsification universelle
- falsification existentielle

Attaques :

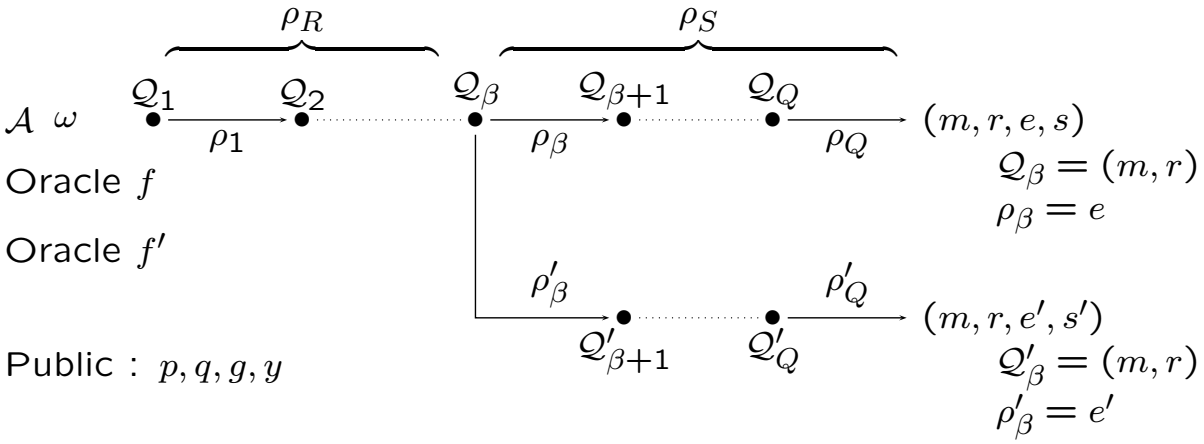
- attaque sans message connu
- attaque à messages connus
- attaque à messages choisis adaptative

Attaque sans message connu

Falsification existentielle
selon une attaque *sans message connu*

Attaque	**Résolution Logarithme Discret**
	

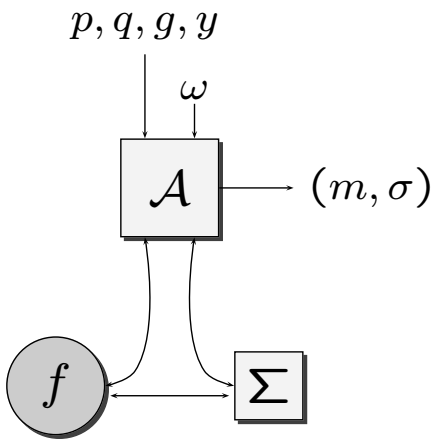
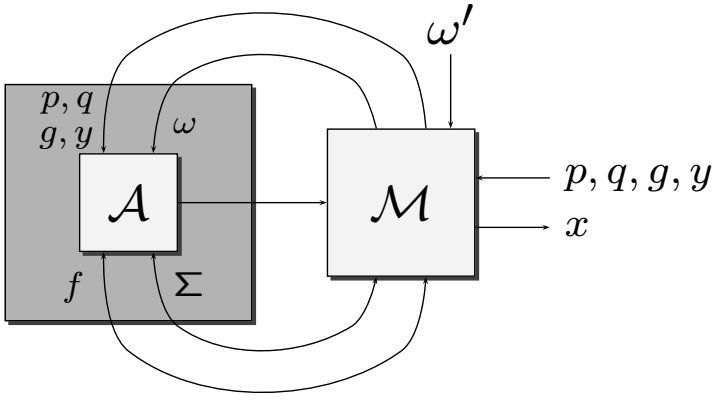
Lemme de « bifurcation »



Signature valide : $r = g^s y^e \bmod p$ avec $e = f(m, r)$.
(m, r, e, s) et (m, r, e', s') valides : $g^s y^e = r = g^{s'} y^{e'} \bmod p$
$\Longrightarrow$ $\boldsymbol{x = -\log_g y \bmod q}$.

Attaque à messages choisis adaptative

Falsification existentielle
selon une attaque *à messages choisis adaptative*

Attaque	**Résolution Logarithme Discret**
	

Simulation

L'attaquant doit avoir l'« impression »de communiquer
avec un véritable signeur « Σ »qui connaît la clé secrète x.

Si $\mathcal{M}$ connaît x, cette réduction n'a plus aucun intérêt :
$\mathcal{M}$ doit simuler Σ sans connaître x.

- $\Sigma : m \longrightarrow (r, e, s)$
- Simulation : m
  - e aléatoire (comme retourné par f)
  - s aléatoire (comme apparemment retourné par Σ)
  - $r = g^s y^e \bmod p$ (comme apparemment retourné par Σ)

Résultat de Sécurité

Si une machine de Turing polynomiale probabiliste $\mathcal{A}$
est capable d'effectuer *une falsification existentielle*,
selon une attaque *à messages choisis adaptative*,
en temps T, avec probabilité $\varepsilon \geq 1/P$,
après Q appels à l'oracle aléatoire et R appels au signeur,

si de plus $\varepsilon \geq 16(R+1)(R+Q) \cdot 2^{-k}$,
où k est la taille des sorties de l'oracle aléatoire,

alors il existe une machine capable de résoudre
le problème du logarithme discret dans les sous-groupes premiers
en temps $T' \leq 2QT/\varepsilon$, avec probabilité $\varepsilon' \geq 1/30$.

Généralisation

- Cette preuve est générique :

  elle s'applique à tout schéma de signature
  dérivé d'un protocole d'identification
  « à divulgation nulle de connaissance »
  (face à un vérifieur honnête).

  En effet, « divulgation nulle de connaissance »$\Longleftrightarrow$ simulation.

- Application à El Gamal.

Monnaie Électronique

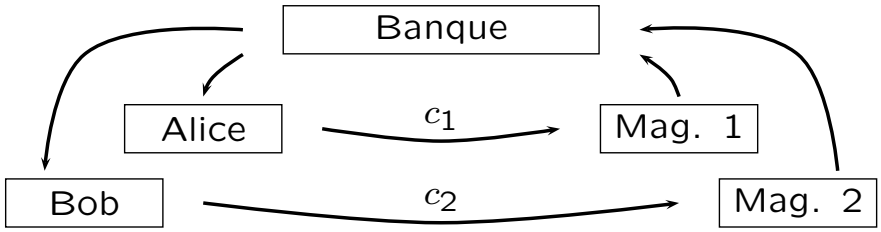
- **Dans la vie réelle :**
  une pièce de monnaie est un morceau de métal
  produit et certifié par la banque (ou une autorité).

  Deux pièces sont parfaitement indistinguables

- **Dans le monde informatique :**
  une pièce est un nombre aléatoire
  produit et certifié par la banque

  Les distributions de probabilité de deux pièces doivent être indistinguables, même pour la banque.

Parcours d'une Pièce



Si la banque peut reconnaître la pièce qu'elle a donnée à Alice,
elle sait qu'Alice a acheté quelque chose dans le Magasin 1.

$\Longrightarrow$ **Traçage d'une pièce.**

Anonymat

respect de la vie privée $\Longrightarrow$ anonymat
traçage impossible $\Longrightarrow$ signatures en blanc

Signature en Blanc

une autorité aide un utilisateur
à obtenir une signature valide

le message et la signature
doivent rester inconnus pour l'autorité

Une pièce électronique est un nombre certifié par la banque
de telle manière que la banque ne connaisse
ni ce nombre ni le certificat qu'elle fournit.

Signature de Schnorr en Blanc

Banque		Alice
commun : p, q, g		
clé secrète : $x \in (\mathbb{Z}/q\mathbb{Z})^\star$		
clé publique : $y = g^{-x} \bmod p$		
$k \in (\mathbb{Z}/q\mathbb{Z})^\star$		
$r = g^k \bmod p$	$\xrightarrow{r}$	
		$\alpha, \beta \in \mathbb{Z}/q\mathbb{Z}$
		$\rho = r g^\alpha y^\beta \bmod p$
		$\varepsilon = f(m, \rho)$
	$\xleftarrow{e}$	$e = \varepsilon - \beta \bmod q$
$s = k + ex \bmod q$	$\xrightarrow{s}$	
		$g^s y^e \stackrel{?}{=} r \bmod p$
		$\sigma = s + \alpha \bmod q$

Alors $g^\sigma y^\varepsilon = \rho \bmod p$.

$(\rho, \varepsilon, \sigma)$ est une signature valide d'un message m inconnus de la Banque.

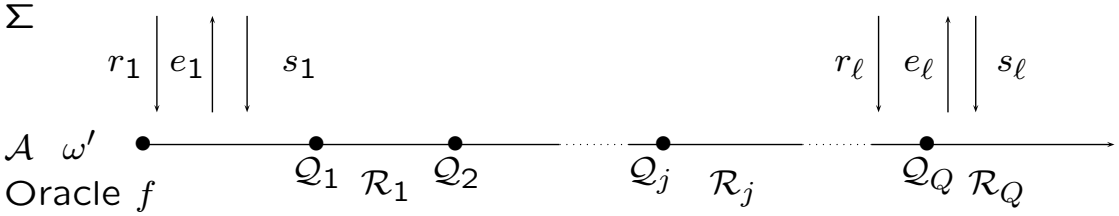
Propriétés de Sécurité

- $(\ell, \ell+1)$-**falsification** :
  après ℓ interactions avec la Banque
  l'attaquant est capable de forger
  $\ell + 1$ couples message–signature valides.

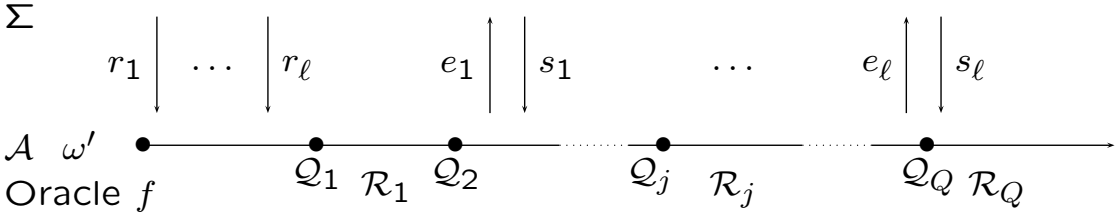
- **falsification supplémentaire** :
  une $(\ell, \ell+1)$-falsification
  pour un entier ℓ.

Attaques

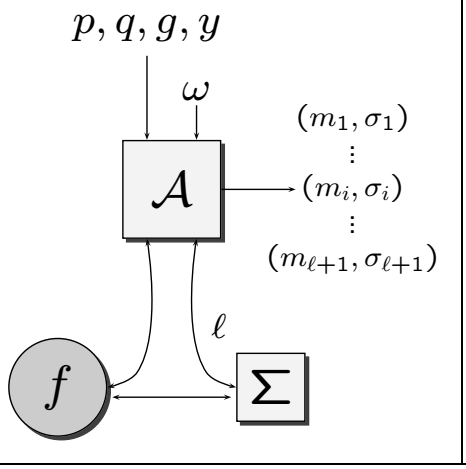
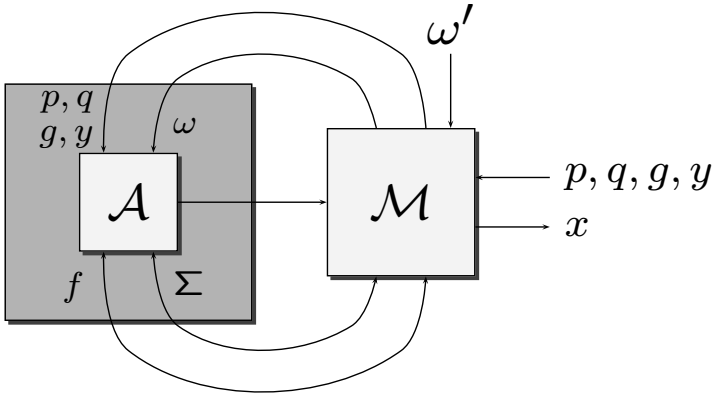
- **attaque séquentielle** : l'attaquant fait signer une pièce à la fois.



- **attaque parallèle** : l'attaquant effectue des interactions avec le signeur comme il le souhaite.



Preuve Formelle de Sécurité

Attaque	Résolution LD
	

Cette fois-ci, il n'est plus possible de simuler Σ sans clé secrète

$\Longrightarrow$ **protocoles à témoins indistinguables.**

Témoins Indistinguables

- plusieurs clés secrètes sont associées à une même clé publique
- les distributions des rubans de communication sont indistinguables quelle que soit la clé secrète utilisée par le signeur
- deux clés secrètes distinctes associées à une même clé publique fournissent la solution d'un problème difficile.

Exemple : le problème du bi-logarithme discret

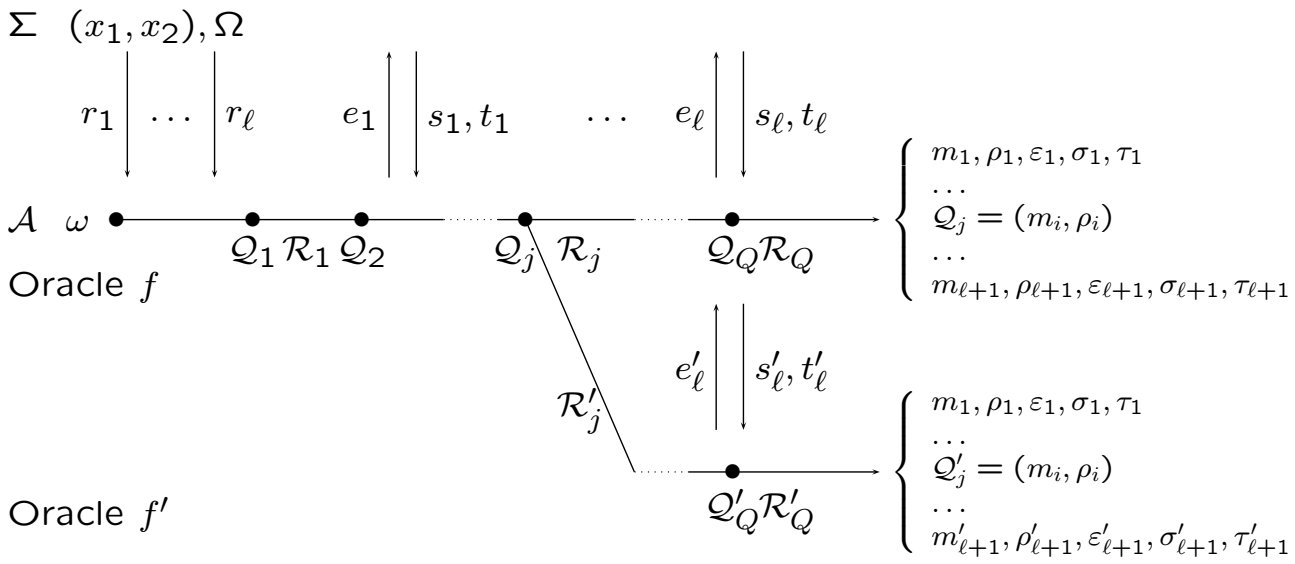
$$y = g^{-x_1} h^{-x_2} = g^{-x'_1} h^{-x'_2} \bmod p$$
$$\text{avec } x_1 \neq x'_1 \bmod q$$
$$\Longrightarrow \quad h = g^{-(x_1 - x'_1)/(x_2 - x'_2)} \bmod p.$$

Signature d'Okamoto–Schnorr en Blanc

Banque		Alice
commun : p, q, g, h		
clé secrète : $x_1, x_2 \in (\mathbb{Z}/q\mathbb{Z})^\star$		
clé publique : $y = g^{-x_1} h^{-x_2} \bmod p$		
$k_1, k_2 \in (\mathbb{Z}/q\mathbb{Z})^\star$		
$r = g^{k_1} h^{k_2} \bmod p$	$\xrightarrow{\quad r \quad}$	
		$\alpha, \beta, \gamma \in \mathbb{Z}/q\mathbb{Z}$
		$\rho = r g^\alpha h^\beta y^\gamma \bmod p$
		$\varepsilon = f(m, \rho)$
	$\xleftarrow{\quad e \quad}$	$e = \varepsilon - \gamma \bmod q$
$s = k_1 + e x_1 \bmod q$		
$t = k_2 + e x_2 \bmod q$	$\xrightarrow{\quad s, t \quad}$	
		$g^s h^t y^e \stackrel{?}{=} r \bmod p$
		$\sigma = s + \alpha \bmod q$
		$\tau = t + \beta \bmod q$

$(m, \rho, \varepsilon, \sigma, \tau)$ tel que $\rho = g^\sigma h^\tau y^\varepsilon \bmod p$ avec $\varepsilon = f(m, \rho)$.

Lemme de « bifurcation »



Lemme de « bifurcation »(2)

Avec probabilité non négligeable,
il existe i tel que $\mathcal{Q}_j = \mathcal{Q}'_j = (m_i, \rho_i)$ alors

$$g^{\sigma_i} h^{\tau_i} y^{\varepsilon_i} = \rho_i = g^{\sigma'_i} h^{\tau'_i} y^{\varepsilon'_i} \bmod p.$$

avec $\varepsilon_i \neq \varepsilon'_i \bmod q$.

$$\left.\begin{array}{l} x'_1 = (\sigma'_i - \sigma_i)/(\varepsilon'_i - \varepsilon_i) \bmod q \\ x'_2 = (\tau'_i - \tau_i)/(\varepsilon'_i - \varepsilon_i) \bmod q \end{array}\right\} \quad y = g^{-x'_1} h^{-x'_2} \bmod p.$$

Puisque les rubans de communication suivent une distribution
indépendante de la clé secrète utilisée par la Banque,
avec grande probabilité, $x_1 \neq x'_1 \bmod q$
$\Longrightarrow \mathbf{log_g\, h}$.

Résultat de Sécurité

Si une machine de Turing polynomiale probabiliste $\mathcal{A}$
est capable d'effectuer une *falsification supplémentaire*,
selon une *attaque parallèle*,
en temps T, avec probabilité $\varepsilon \geq 1/P$,
après Q appels à l'oracle aléatoire et ℓ appels à l'autorité,

si de plus, $\varepsilon \geq 4Q^{\ell+1}/q$,

alors il existe une machine capable de résoudre
le problème du logarithme discret dans les sous-groupes premiers
en temps $T' \leq 33Q\ell T/\varepsilon$ et avec probabilité $\varepsilon' \geq 1/72\ell^2$.

Monnaie Électronique

Il est possible d'utiliser ces signatures en blanc prouvées sûres
pour produire un schéma de monnaie électronique « off-line »
avec des preuves formelles de sécurité :

- les dépenses sont parfaitement anonymes
- un fraudeur par « double dépense »sera démasqué
- la Banque a le contrôle de la quantité d'argent en circulation :
  après ℓ interactions avec la Banque,
  un utilisateur ne peut détenir plus de ℓ pièces
- les utilisateurs ont des garanties :
  la Banque ne peut faire accuser un de ses clients
  de fraude par « double dépense »

Conclusion

- *Identification*
  Protocoles dont une fraude selon une attaque active
  est équivalente au Problème des Perceptrons Permutés
- *Signatures Électroniques*
  Une falsification existentielle selon
  une attaque à messages choisis adaptative est
  équivalente au LD (ou FACT, RSA, PKP, SD, CLE, PPP,...)
- *Signatures en Blanc*
  Une falsification supplémentaire selon
  une attaque parallèle est
  équivalente au LD (ou FACT, RSA)
- *Monnaie électronique*
  Premier schéma, avec preuves formelles,
  équivalent au LD