Techniques Géneriques de Preuves de Sécurité

David Pointcheval

David.Pointcheval@ens.fr David.Pointcheval@info.unicaen.fr

GRECC
École Normale Supérieure

GREYC
Université de Caen

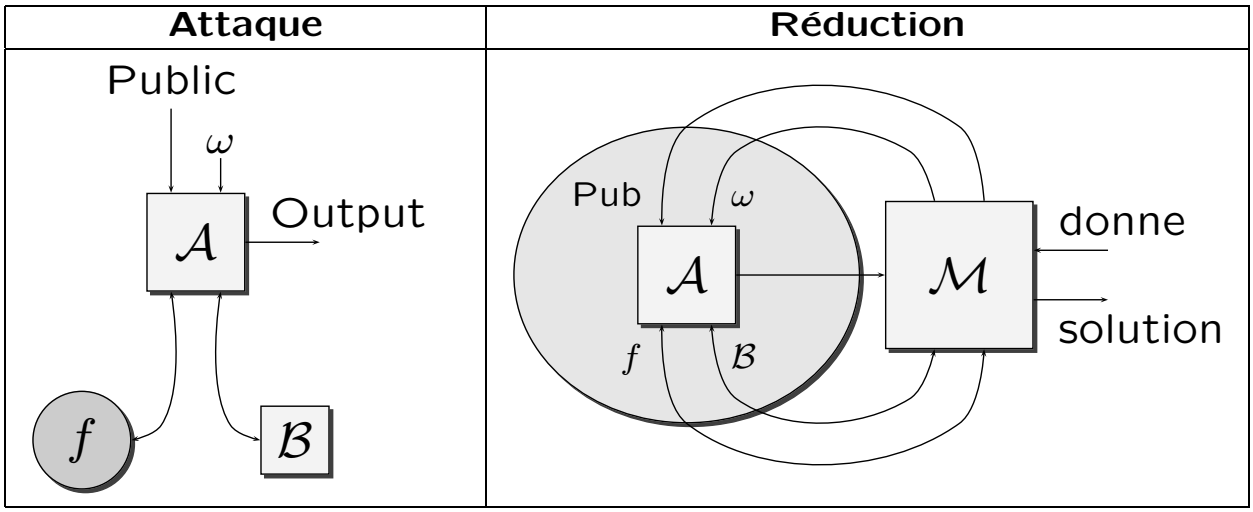
Plan

- Preuves de Sécurité
  - Preuves Formelles
  - Modélisation
- Signature Électronique
  - Définition – Exemple
  - Sécurité
  - Attaques sans message connu
  - Attaques à messages choisis adaptatives
  - Signature El Gamal
- Monnaie Électronique
- Signature en Blanc
  - Définition – Exemple
  - Sécurité – Attaques
  - Notion de « Témoins Indistinguables »
  - Résultat de Sécurité
- Conclusion

Preuve de Sécurité

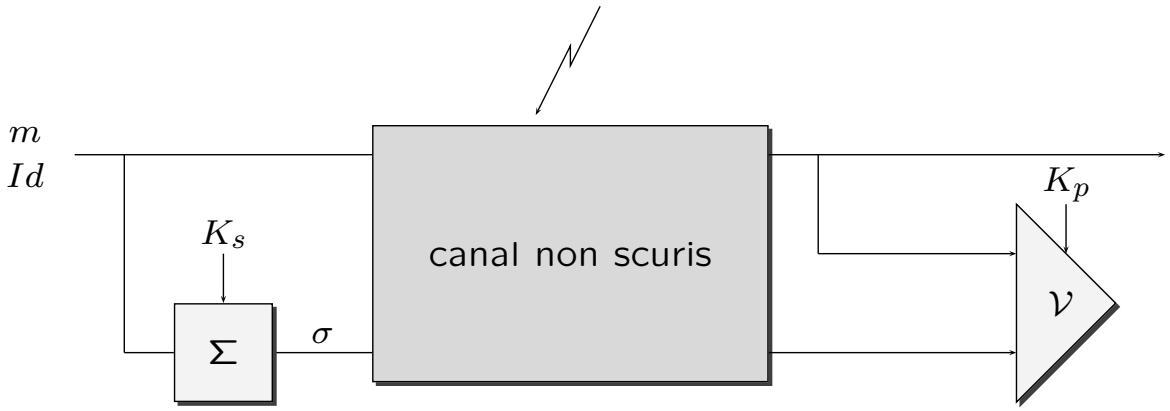
Le schéma S est sûr

- **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, PKP, SD, ...)



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

Signature Électronique



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

Signature de Schnorr

- public : p, q entiers premiers, $g, y \in (\mathbb{Z}/p\mathbb{Z})^\star$ d'ordre q
  secret : x tel que $y = g^{-x} \bmod p$

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

- $g^s y^e \stackrel{?}{=} r \bmod p$

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

Critères de Sécurité

Falsifications :

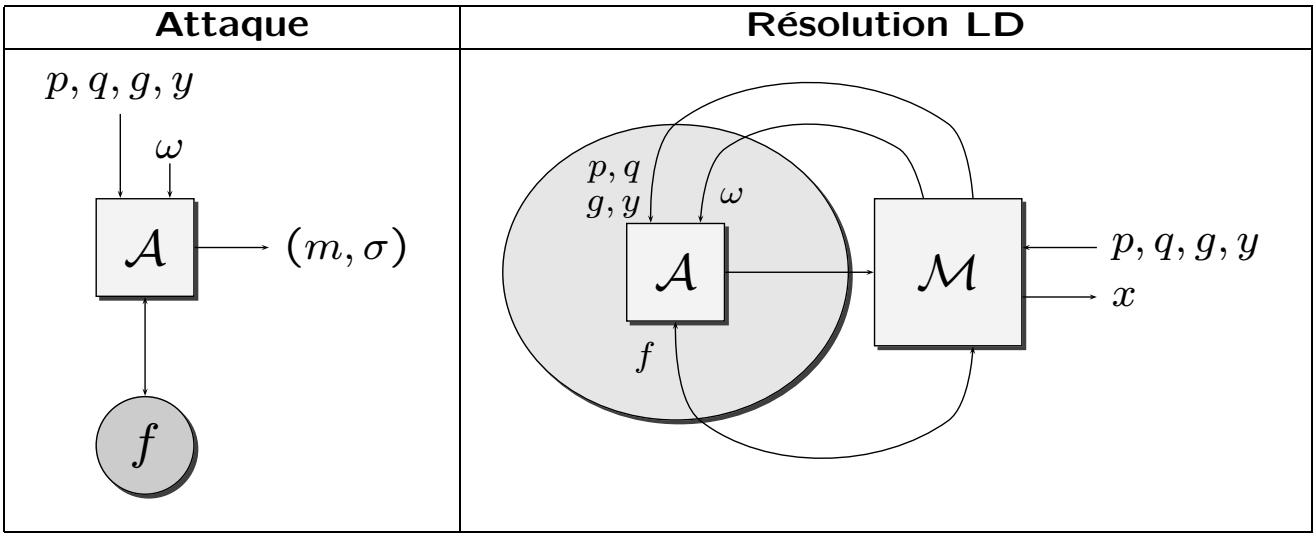
- cassage total
- falsification universelle
- falsification existentielle

Attaques :

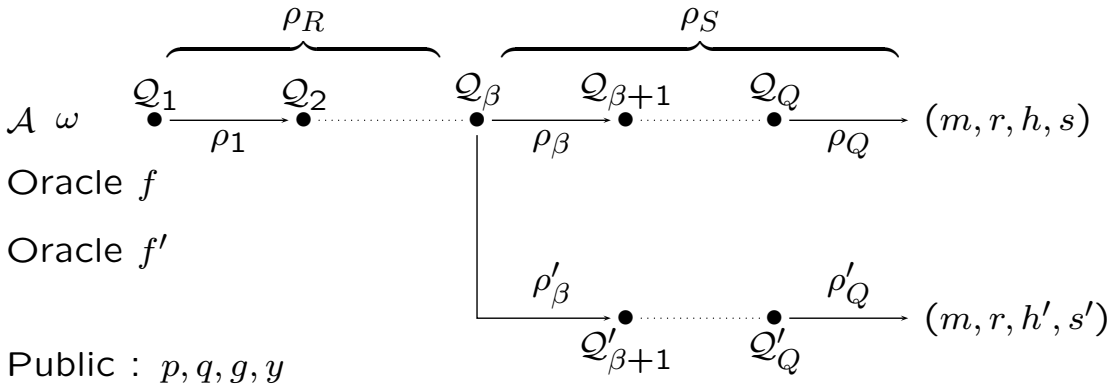
- attaque sans message connu
- attaque à messages connus
- attaque à messages choisis adaptative

Attaque sans message connu

Falsification existentielle
selon une attaque sans message connu



Lemme de « bifurcation »



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

Lemme de « bifurcation »(2)

Attaquant efficace : $\Pr_{\omega,f}[\text{attaque réussie}] \geq \varepsilon$.

Nécessairement, il existe β tel que

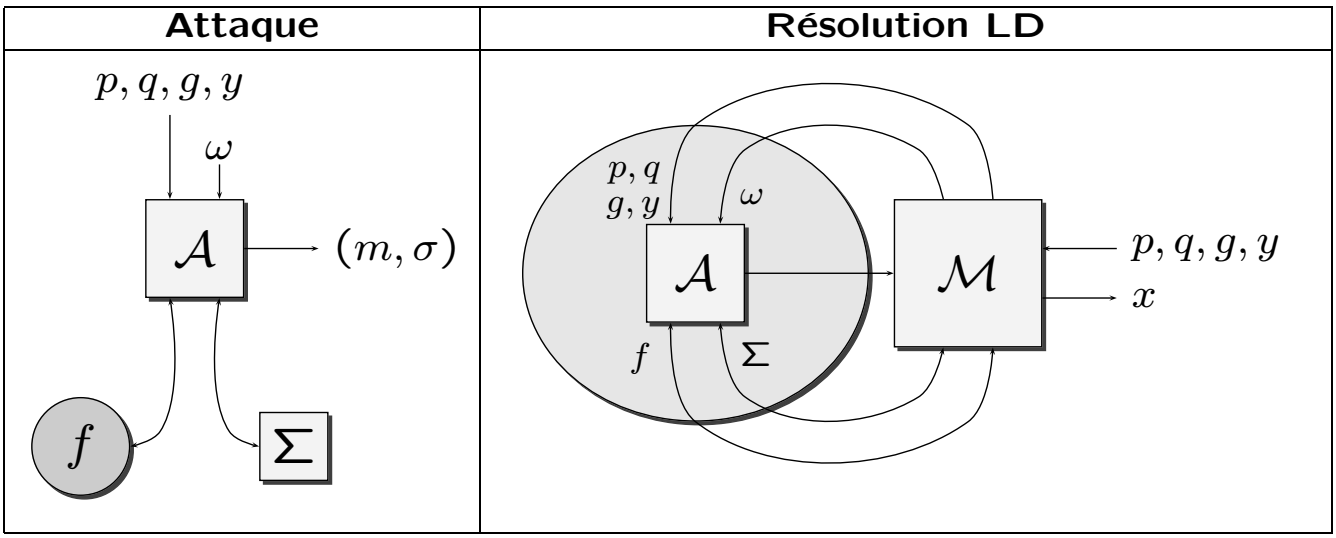
$\Pr_{\omega,f}[\text{attaque réussie et } \mathcal{Q}_\beta = (m, r)] \geq \varepsilon/Q$.

Lemme de séparation :
il existe Ω tel que

- $\Pr_{\omega,\rho_R}[(\omega, \rho_R) \in \Omega] \geq \varepsilon/2Q$
- Pour tout $(\omega, \rho_R) \in \Omega$
  $\Pr_{\rho_S}[\text{attaque réussie et } \mathcal{Q}_\beta = (m, r)] \geq \varepsilon/2Q$

Attaque à messages choisis adaptative

Falsification existentielle
selon une attaque à messages choisis adaptative



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.

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

Résultat de Sécurité

Si une machine de Turing $\mathcal{A}$ 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 « zero-knowledge »
face à un vérifieur honnête.

En effet, « zero-knowledge »$\Longleftrightarrow$ simulation.

Signature El Gamal

- public : p entier premier, $g, y \in (\mathbb{Z}/p\mathbb{Z})^\star$ générateurs de $(\mathbb{Z}/p\mathbb{Z})^\star$
  secret : x tel que $y = g^x \bmod p$
- $r = g^k \bmod p$ où $k \in_R \left(\mathbb{Z}/(p-1)\mathbb{Z}\right)^\star$
- $s = (m - xr)/k \bmod (p-1)$
- $g^m \stackrel{?}{=} y^r r^s \bmod p$

Falsification existentielle :

- $e, v \in_R \left(\mathbb{Z}/(p-1)\mathbb{Z}\right)^\star$
- $r = g^e y^v$
- $s = -r/v \bmod (p-1)$
- (r, s) signature valide de $m = es \bmod (p-1)$

Signature El Gamal Modifiée

- public : p entier premier, $g, y \in (\mathbb{Z}/p\mathbb{Z})^\star$ générateurs de $(\mathbb{Z}/p\mathbb{Z})^\star$
  secret : x tel que $y = g^x \bmod p$
- $r = g^k \bmod p$ où $k \in_R \left(\mathbb{Z}/(p-1)\mathbb{Z}\right)^\star$
- $h = f(m, r)$
- $s = (h - xr)/k \bmod (p-1)$
- $g^h \stackrel{?}{=} y^r r^s \bmod p$ où $h = f(m, r)$

Une falsification existentielle
selon une attaque à messages choisis adaptative
du schéma de El Gamal modifié
est équivalente au problème du logarithme discret.

Monnaie Électronique

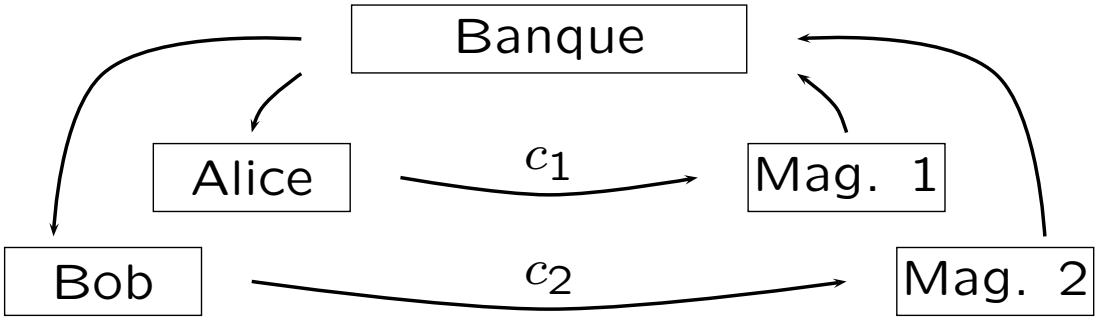
- **Dans la vie réelle :**
  une pièce de monnaie est un morceau de métal
  produit et certifié par la banque (ou une authorité).

  Deux pièces sont parfaitement indistinguables

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

  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 quelquechose 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
public : p, q, g, y		
secret : $y = g^{-x} \bmod p$		
$k \in (\mathbb{Z}/q\mathbb{Z})^\star$		
$r = g^k \bmod p$	$\xrightarrow{r}$	
		$\alpha, \beta \in \mathbb{Z}/q\mathbb{Z}$
		$r' = rg^\alpha y^\beta \bmod p$
		$e' = H(m, r')$
	$\xleftarrow{e}$	$e = e' - \beta \bmod q$
$s = k + ex \bmod q$	$\xrightarrow{s}$	
		$g^s y^e \stackrel{?}{=} r \bmod p$
		$s' = s + \alpha \bmod q$

Alors $g^{s'} y^{e'} = r' \bmod p$.
(r', s') est une signature inconnue d'un message inconnu m.

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.

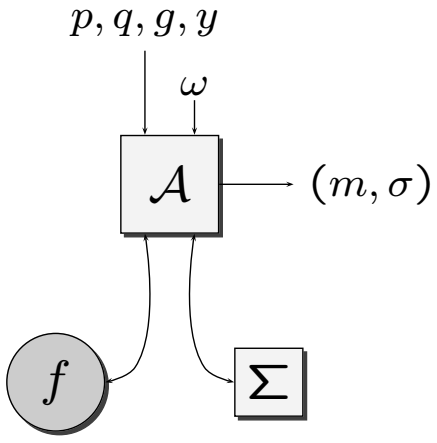
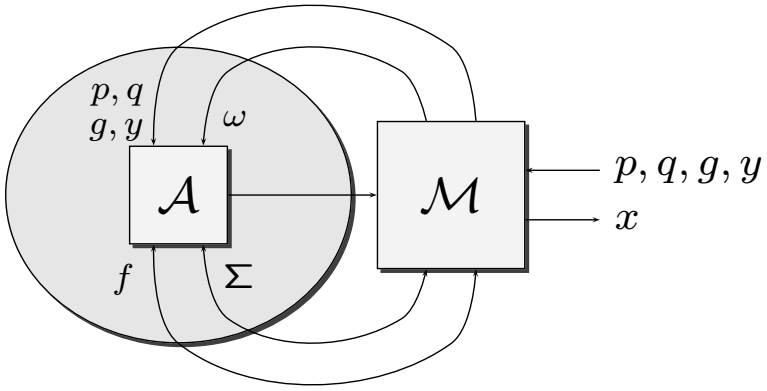
- **falsification supplémentaire** :
  une $(\ell, \ell + 1)$-falsification
  pour un entier ℓ.

Attaques

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

- **attaque parallèle** :
  l'attaquant effectue des interactions
  avec le signeur quand il le souhaite.
  Il peut notamment initialiser une nouvelle interaction
  avant que les précédentes ne soient achevées.

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

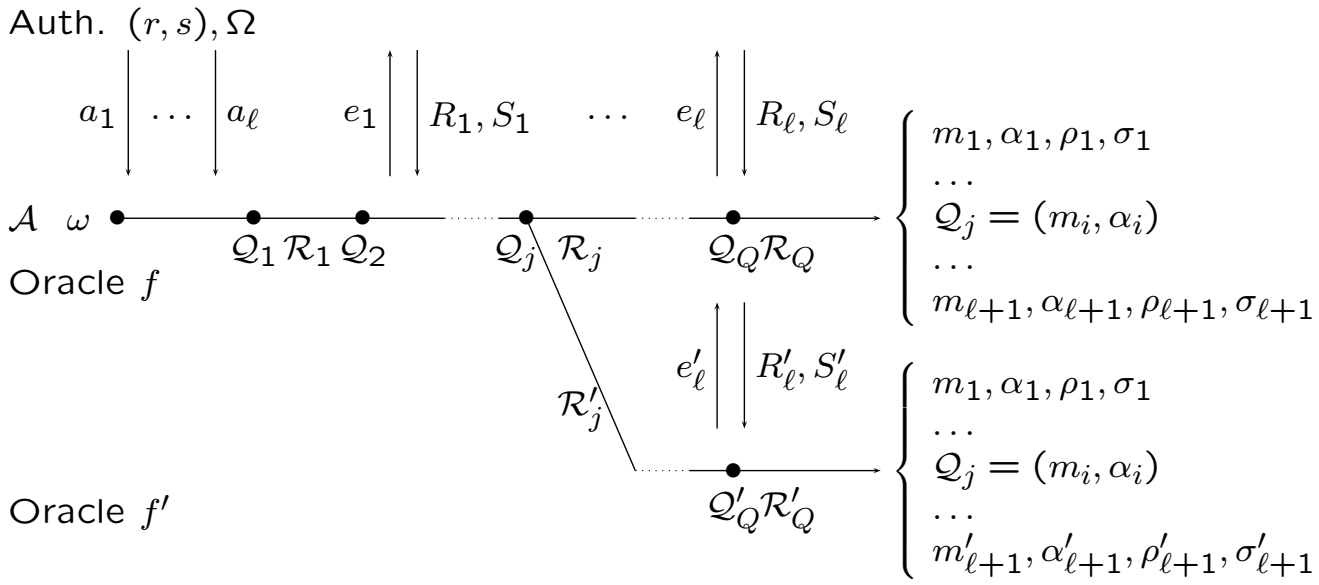
$$y = g^r h^s = g^{r'} h^{s'} \bmod p$$
$$\text{avec } r \neq r' \bmod q$$
$$\Longrightarrow h = g^{-(r-r')/(s-s')} \bmod p.$$

Signature d'Okamoto–Schnorr en Blanc

Banque		Alice
public : p, q, g, h, y secret : $y = g^{-r} h^{-s} \bmod p$ $t, u \in (\mathbb{Z}/q\mathbb{Z})^\star$ $a = g^t h^u \bmod p$	$\xrightarrow{a}$	
		$\beta, \gamma, \delta \in \mathbb{Z}/q\mathbb{Z}$ $\alpha = a g^\beta h^\gamma y^\delta \bmod p$ $\varepsilon = H(m, \alpha)$
	$\xleftarrow{e}$	$e = \varepsilon - \delta \bmod q$
$R = t + er \bmod q$ $S = u + es \bmod q$	$\xrightarrow{R, S}$	
		$g^R h^S y^e \stackrel{?}{=} a \bmod p$ $\rho = R + \beta \bmod q$ $\sigma = S + \gamma \bmod q$

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

Lemme de « bifurcation »



Lemme de « bifurcation »(2)

- On lance $\mathcal{A}$ avec (r, s), Ω, ω et f aléatoires
- On relance $\mathcal{A}$ avec les mêmes (r, s), Ω, ω
  mais l'oracle aléatoire f' qui diffère de f à la j^{e}réponse.

Avec probabilité non négligible,
il existe un indice i tel que $\mathcal{Q}_j = \mathcal{Q}'_j = (m_i, \alpha_i)$
alors

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

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

En posant $r' = (\rho'_i - \rho_i)/(\varepsilon'_i - \varepsilon_i) \bmod q$
et $s' = (\sigma'_i - \sigma_i)/(\varepsilon'_i - \varepsilon_i) \bmod q$,

$$y = g^{-r'} h^{-s'} \bmod p.$$

Lemme de « bifurcation »(3)

Puisque les rubans de communication
suivent une distribution indépendante
de la clé secrète utilisée par la Banque,
avec grande probabilité, $r \neq r'$ mod q

$$\Longrightarrow \log_g h.$$

Résultat de Sécurité

Si une machine de Turing $\mathcal{A}$ 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 $\varepsilon' \geq 1/72\ell^2$.

Conclusion

Lemmes de « bifurcation » :

- *Signatures Électroniques*
  Falsification existentielle impossible
  selon des attaques à messages choisis adaptatives

- *Signatures en Blanc*
  Falsification supplémentaire impossible
  selon des attaques parallèles