Les Courbes Elliptiques pour la Sécurité des Appareils Mobiles

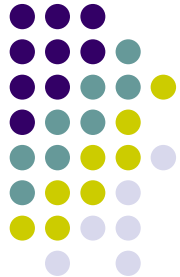
ACI Sécurité Informatique

LaBRI, Bordeaux, 23/11/05

LIENS – CNRS
École Normale Supérieure

TANC - INRIA
École Polytechnique

CESAM : objectifs



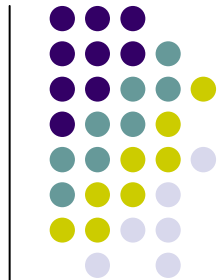
- Aspects théoriques et pratiques de la cryptographie en environnement contraint
- Protocoles utilisant les courbes elliptiques
- Sécurité concrète
  - Hypothèses algorithmiques réalistes
  - Attaquants réalistes
  - Réductions exactes (et non asymptotiques)

Échange de clé avec authentification à bas coût

Échange de clé

- Génération d'un secret commun par communication sur un canal non sûr
- Authentification lorsque chacun vérifie l'identité de son correspondant
  - Avec des moyens cryptographiques : chacun possède une biclé publique/privée
  - éventuellement par mot de passe : Encrypted Key Exchange

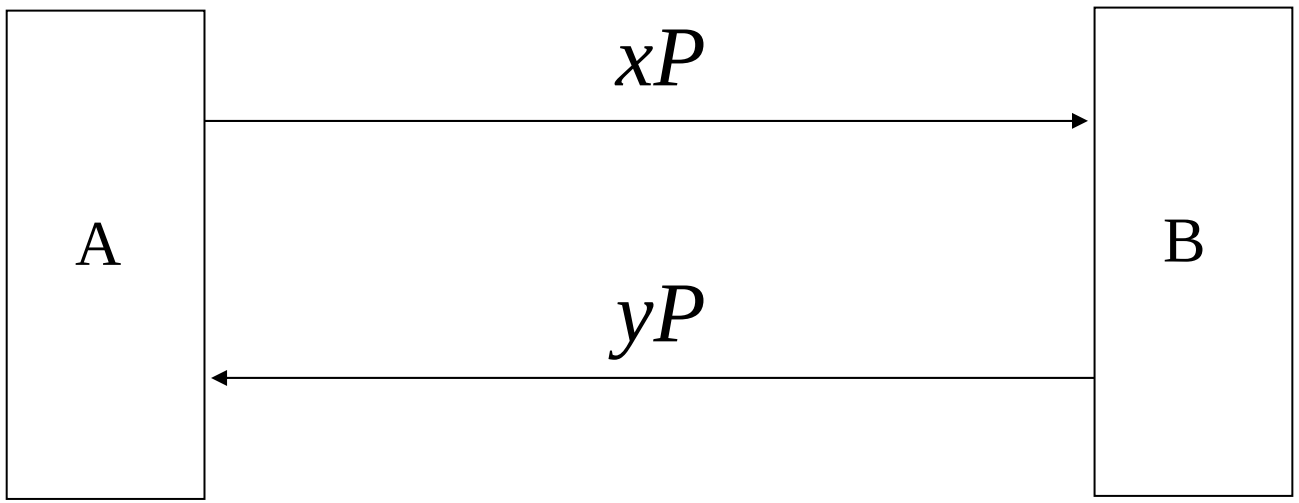
Le log discret



- La sécurité d'un protocole sur courbes elliptiques s'appuie en général sur la difficulté du **log discret** ou d'un problème connexe
- Courbe $\Rightarrow$ groupe $(G, +, P)$
  - Logarithme discret : étant donné h, trouver n t.q. $h = n.P$
  - Diffie-Hellman calculatoire : étant donnés xP, yP, calculer xyP
  - Diffie-Hellman décisionnel : étant donnés xP, yP, zP, décider si $z = xy$

Diffie-Hellman

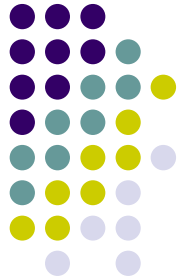
- Historiquement, le premier échange de clé (non authentifié) :



Valeur secrète commune

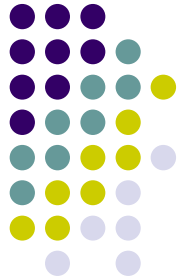
$$K = xyP = y(xP) = x(yP)$$

Échange de clé : authentification avec ressource de calcul externe



- Scénario : une ressource à bas coût embarque une clé privée
- Elle interagit avec un « calculateur » à qui elle délègue une partie des calculs nécessaires à une authentification
  - Téléphone/carte SIM (aujourd'hui authentification symétrique)
  - PC/carte à puce
- Le calculateur ne doit rien apprendre concernant la clé
  - Ou lui permettant de s'authentifier sans interagir avec la ressource d'authentification

Échange de clé : authentification avec ressource de calcul externe



- La ressource d'authentification fournit au calculateur des « coupons »
  - Ces coupons doivent être à usage unique
- Comment réaliser un protocole sûr dans ce modèle ?
- Une possibilité : la ressource d'authentification fait tout le travail
  - Aucun intérêt en termes de performance

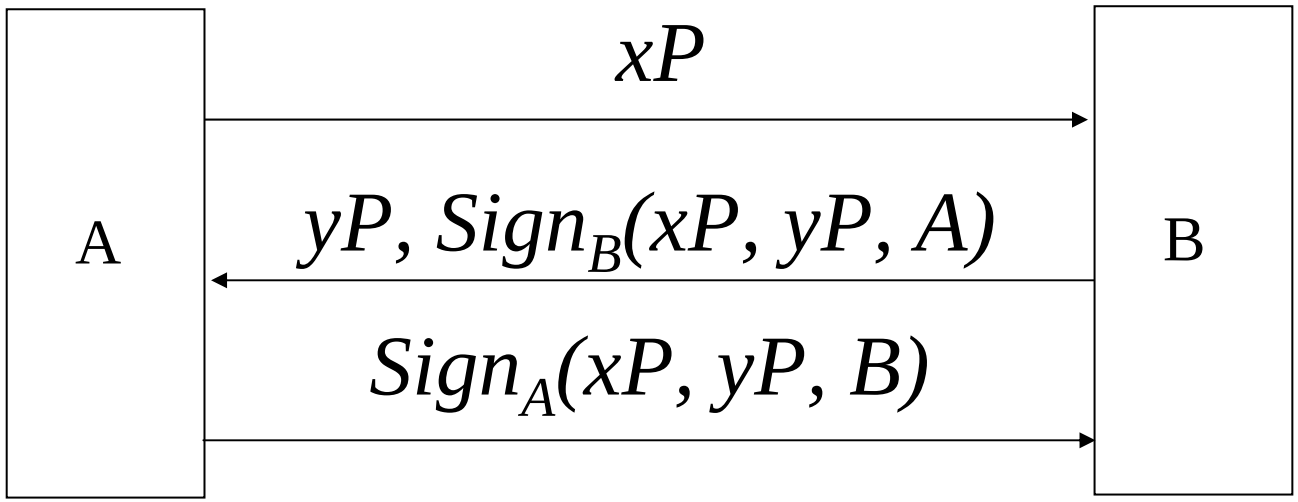
Échange de clé : authentification avec ressource de calcul externe

- Définition d'un modèle de sécurité pour l'échange de clé prenant en compte un calculateur malhonnête
- Deux objectifs de sécurité
  - Confidentialité du secret négocié (dans un cadre authentifié ou non)
  - Authentification mutuelle
- L'attaquant peut interagir avec les ressources d'authentification des utilisateurs

Ressource externe à bas coût

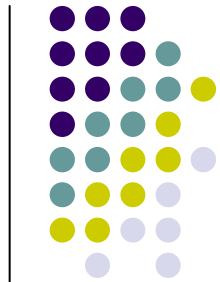
- Ne doit pas effectuer de calculs complexes
- Hachage, additions/multiplications modulaires
- Pas de multiplication scalaire $x \rightarrow xP$
  - sauf si précalcul possible

Protocoles candidats : Diffie-Hellman signé



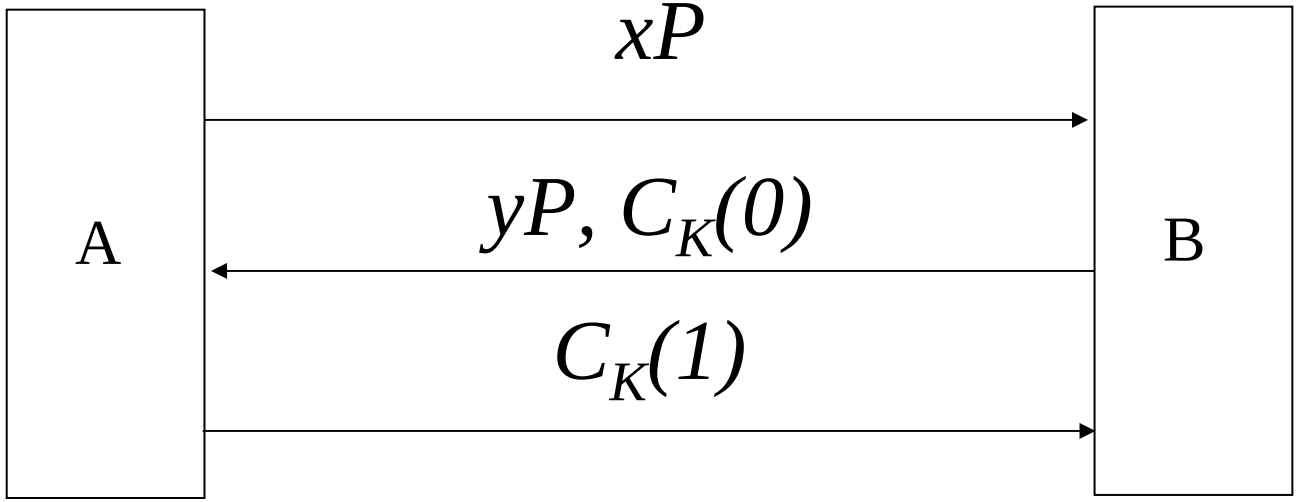
- La ressource d'authentification effectue alors des signatures
- Nécessite un algorithme de signature permettant le précalcul
  - Le coût doit tenir compte des vérifications de signatures

Protocoles candidats : MQV



- Algorithme d'échange de clé sur courbe elliptique
- Efficacité
  - Compacité du codage des points sur courbes
  - Pas de signatures
  - Très peu de multiplications scalaires par échange (2 par participant ; DH signé : 4)
- Standard de fait
  - « Standards for Efficient Cryptography Group»
  - Usage gouvernemental : licence NSA

Protocoles candidats : MQV



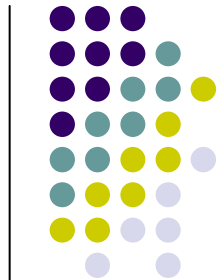
clé privée de A

- $K = (T(xP)\, s_a + x)(T(yP)\, s_b + y)\, P$
  $= (T(xP)\, s_a + x)\, (T(yP)\, P_B + yP)$
  $= \ldots$

troncature des bits de l'abscisse du point

clé publique de B

Protocoles candidats : ~~MQV~~

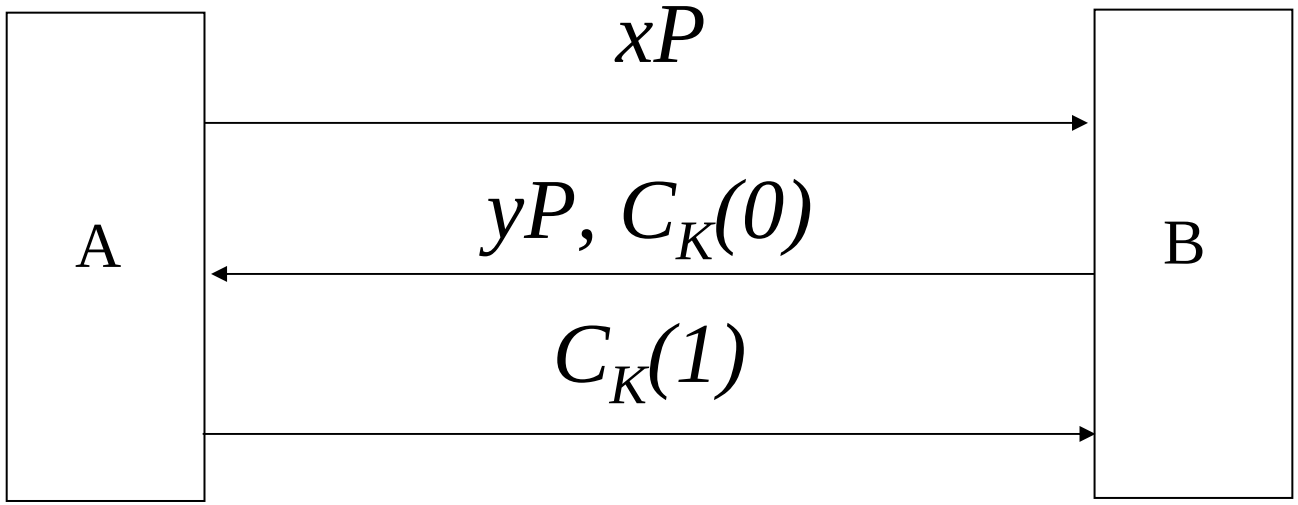


- $K = (T(xP)\, s_a + x)(T(yP)\, s_b + y)\, P$

- Coupons : $(x_iP,\ T(x_iP)\, s_a + x_i)$

- Ces coupons sont réutilisables

MQV′



- $K = (H(0, xP, yP, A, B)\ s_a + x)$
  $(H(1, xP, yP, A, B)\ s_b + y)\ P$

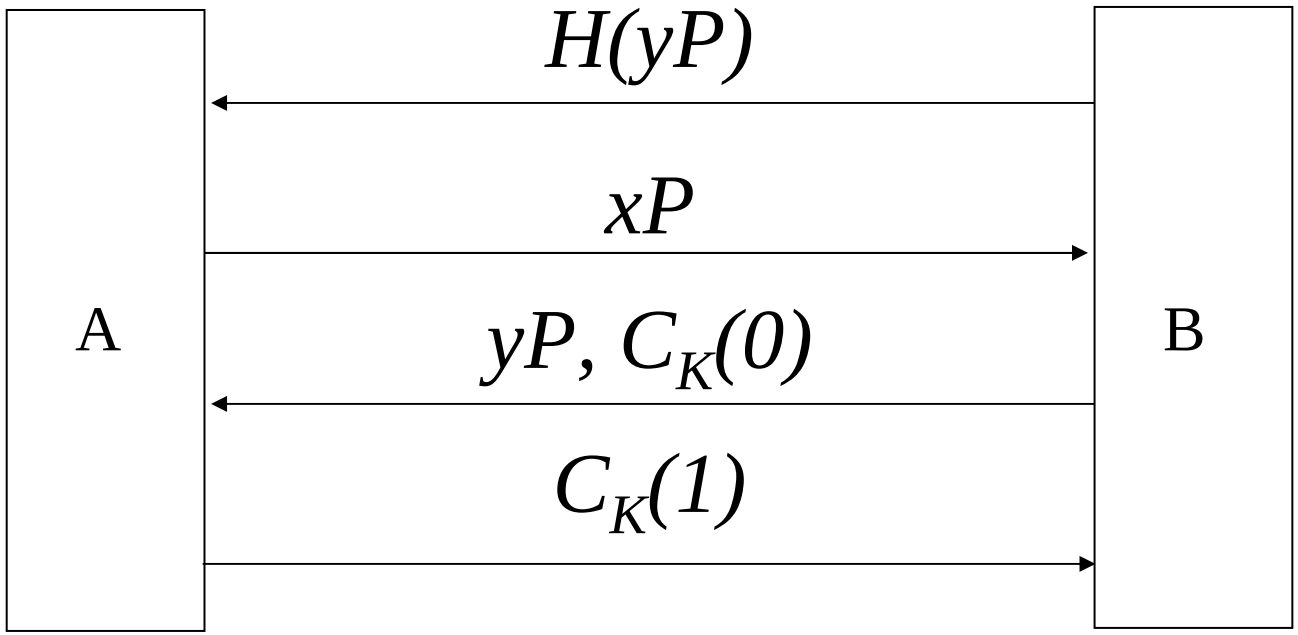
Coupons dans MQV'

- $(xP, H(c, xP, yP, A, B)\, s_a + x)$, $c = 0$ ou 1
- Dépend du point aléatoire envoyé par le partenaire B $\Rightarrow$ non réutilisable
- Très proche d'un coupon pour produire une signature Schnorr
  - mais pas de vérification de signature
- Toujours possibilité de précalcul : (x, xP)
- La ressource d'authentification calcule
  $H(c, xP, yP, A, B)\, s_a + x \mod ord(G)$

Preuve de MQV’

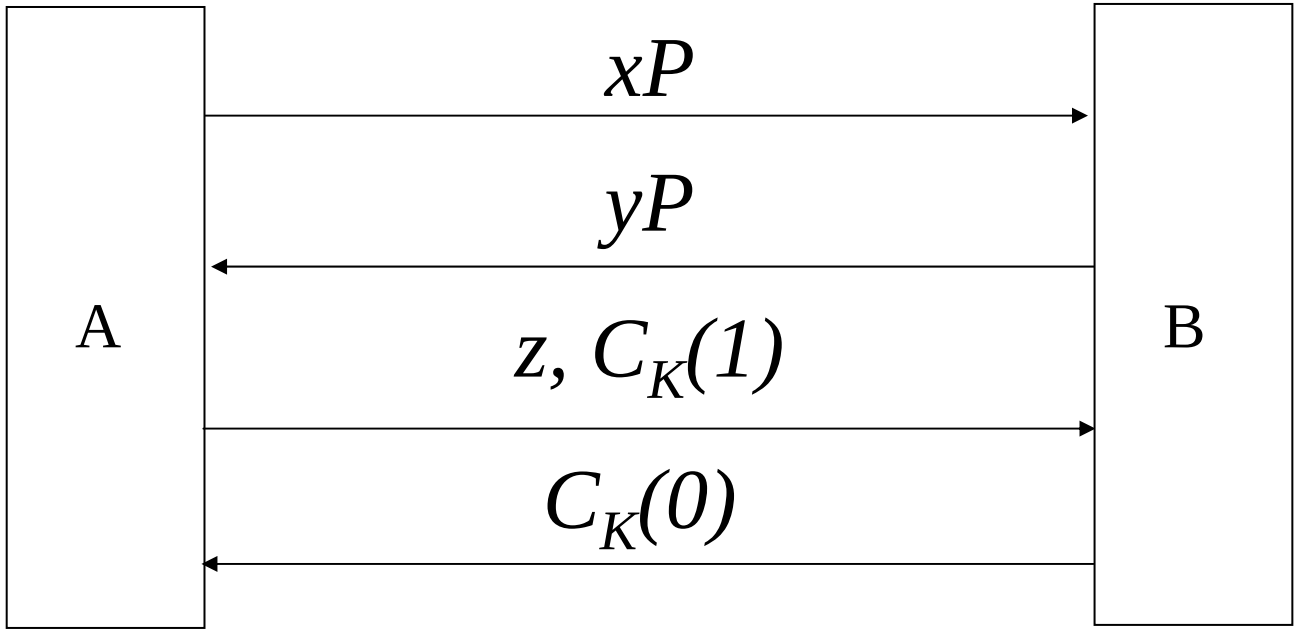
- Sous la forme précédente : semble difficile
- Ajout d’une passe préliminaire où B s’engage sur le point aléatoire qu’il envoie
- Preuve du protocole en 4 passes
  - confidentialité de la clé
  - authentification mutuelle des participants

MQV' 4 passes : version 1



- $K = (H(0, xP, yP, A, B)\ s_a + x)$
  $(H(1, xP, yP, A, B)\ s_b + y)\ P$

MQV' 4 passes : version 2



- $K = (H(0, \mathbf{z}, xP, yP, A, B)\ s_a + x)$
  $(H(1, xP, yP, A, B)\ s_b + y)\ P$

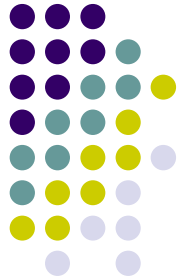
Extraction d’aléa sur courbes elliptiques : corps premier et extension quadratique

Dérivation de clé et extraction d'aléa

- Diffie-Hellman produit un « secret maître » de la forme g^{xy}, avec g^x et g^y publics, dans un groupe G
- Sous l'hypothèse "Decisional Diffie Hellman", la distribution de (g^x, g^y, g^{xy}) est indistinguable de la distribution uniforme (g^x, g^y, g^z) dans G^3

$\Rightarrow$ Diffie-Hellman produit un « secret maître » aléatoire uniforme dans G

Dérivation de clé et extraction d'aléa

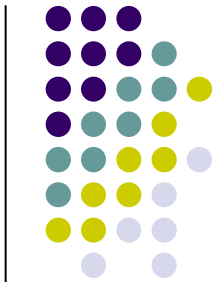


- Clé pour usage symétrique $\Rightarrow$ élément aléatoire uniforme dans un intervalle $[0, 2^s]$
  - Uniformité nécessaire dans les preuves de sécurité des modes symétriques
- Pb de la dérivation de clé : passer d'un élément aléatoire dans G à une chaîne de bits aléatoire
- 1ère solution : « Twist-AUgmented Key Exchange »

Courbe elliptique sur une extension quadratique

- Courbe elliptique C sur un corps $K = F_p[\alpha]$, α de degré 2
- Eléments de C = points $P=(x,y) \in K^2$
- Chaque coordonnée dans K est un couple d'éléments de F_p
- $x = x_0 + \alpha\, x_1$
- $P \in C \rightarrow x_0$ est-il « à peu près uniforme » dans [0, p] ?

Courbe elliptique sur une extension quadratique



- H: $P=(x_0 + \alpha\, x_1 , y_0 + \alpha\, y_1) \in C \rightarrow x_0$
- Si $x_0 \neq 0$,

  $$\mathbf{|H^{-1}(x_0) - (p+1)| \leq 20\ \sqrt{p} + 14}$$

- Hasse : $|\#C-(p^2+1)| \leq 2p$
- On obtient bien une distribution quasi-uniforme dans [0, p-1]

Courbe elliptique sur un corps premier

- Courbe C sur $K = F_p$
- Peut-on extraire k bits de l'abscisse d'un point uniformément choisi sur C ?
- $H : P=(x, y) \rightarrow [x]_k$
- Pour $0 \leq x_0 \leq 2^k-1$,

  $$\mathbf{|H^{-1}(x_0) - \#C/2^k| \leq 3 \sqrt{p} \log(p)}$$

- Pour $2^k << \sqrt{p}$, on obtient une distribution quasi-uniforme

Applications des couplages en chiffrement

Couplages :

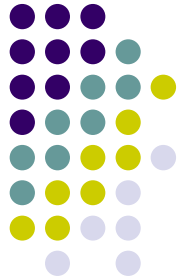
- e : G x G $\rightarrow$ H une « application bilinéaire admissible », i. e.
  - bilinéaire
  - non-dégénérée
  - calculable efficacement

  Exemples : couplage de Tate/Weil sur les courbes elliptiques

Couplages :

- Nouveaux problèmes algorithmiques
- Permet de construire des protocoles cryptographiques avec de nouvelles propriétés
  - Diffusion de données chiffrées avec traçage de traîtres p.ex. pour télévision à péage
- Idée pour le chiffrement (en cours) :
  - Délégation de déchiffrement
  - Transchiffrement

Délégation de déchiffrement



- Le destinataire d'un message chiffré permet à une tierce personne de déchiffrer *certains* messages (origine, période de temps...)

Transchiffrement

- Un utilisateur transforme un chiffré qui lui est destiné en un chiffré pour quelqu'un d'autre
  - plus efficace que déchiffrement/chiffrement
  - Éventuellement sans la clé de déchiffrement