Les Courbes Elliptiques pour la Sécurité des Appareils Mobiles

LIENS – CNRS

Ecole normale supérieure

TANC – INRIA

Ecole polytechnique

ACI Sécurité Informatique

IRISA – Rennes

11 – 12 Décembre 2003

La cryptographie

Les objectifs essentiels :

- Confidentialité
  - Données inintelligibles pour toute tierce personne
  - Chiffrement
- Identité – Authenticité
  - Lien fort entre individu et message/action
  - Signature / MAC
- Intégrité
  - Données non altérées
  - Signature / Hachage

Environnements

Des secrets sont nécessaires

- pour déchiffrer
- pour signer / s'authentifier

car seules certaines personnes sont habilitées

⇒ *Stockage sécurisé*

Des calculs sont à effectuer

⇒ *Puissance de calcul*

Des données sont à transmettre

Clés communes

Cryptographie symétrique / conventionnelle :
les interlocuteurs ont un secret commun

- un « grand » secret
  - « grand » = 128 bits – pas de recherche exhaustive
  - chiffrement – authentification
  - pas de « non-répudiation »
- un « petit » secret : password/passphrase
  - « petit » = 4 chiffres...
  - mise en accord de clé de session authentifiée
  - puis chiffrement/authentification

secret key

password-based

Clés publique/privée

Cryptographie asymétrique :
chacun a son secret propre *clé privée* lié à une information publique *clé publique* associée à son identité

- certificat : un tiers de confiance garantit l'association *clé publique – identité*
  ⇒ Infrastructures de Clés Publiques
- cryptographie basée sur l'identité :
  clé publique = identité

public key

identity-based

Fonctions à sens unique

A part pour la cryptographie à clé secrète, des fonctions à sens-unique (à trappe) sont nécessaires :

- Problèmes algorithmiques difficiles
- Factorisation / RSA
- Logarithme discret / problème Diffie-Hellman

⇒ Coût calculatoire important

Logarithme discret

- Soit **G** = ($<g>$, $\times$) un groupe fini cyclique
- Pour tout $y \in$ **G**, on définit

$$\mathrm{Log}_g(y) = \min\{x \geq 0 \mid y = g^x\}$$

- Fonction à sens-unique
  - $x \rightarrow y = g^x$ facile (cubique)
  - $y = g^x \rightarrow x$ difficile (au moins super-polynomial)
- Fonction à trappe : Problème Diffie-Hellman
  - à partir de $A=g^a$ et $B=g^b$ calculer DH(A,B) = $C=g^{ab}$
  - facile avec la connaissance de a

Groupes et cryptographie

- De nombreux protocoles sont définis sur LD/DH
  - Chiffrement : El Gamal
  - Signature : El Gamal – Schnorr – DSA
  - Mise en accord de clé : Diffie-Hellman
- Groupes classiques
  - **G** = $\mathbf{Z}_p^*$ ou est inclus algos sous-exponentiels
  - **G** est une coube elliptique algos exponentiels

$\Rightarrow$ ECDSA variante de DSA sur courbes elliptiques

Migration : problème de sécurité potentiel

Estimations de complexité

Pour la factorisation

Lenstra-Verheul 2000

Module (bits)	Mips-Year (en $\log_2$)	Opérations (en $\log_2$)	ECC (bits)	Clé secrète (bits)
512	13	58	111	60
1024	35	80	135	72
2048	66	111	166	88
4096	104	149	207	110

Valables pour RSA

Bornes inférieures pour le logarithme discret dans $\mathbf{Z}_p^*$

Problèmes concrets

- Cryptographie à clé secrète
  - efficace, mais peu flexible
- Cryptographie à clé publique
  - plus flexible, mais plus coûteuse
    - RSA/LD(p) : grands nombres
    - PKI : difficile à mettre en place
    - Chiffrement peu efficace (vs. chiffrement symétrique)

Peu adapté aux appareils « mobiles »

- faible puissance de calcul
- faible stockage – débit de transmission
- faible autonomie

Solutions envisagées

- Efficacité
  - Cryptographie hybride (asymétrique + symétrique)
  - Protocoles « off-line/on-line »
  - Protocoles « unbalanced » (client - serveur)
- Gestion des clés
  - Mots de passe
    - aucun secret à stocker : l'utilisateur s'en charge
  - Cryptographie basée sur l'identité
    - pas de PKI : clé publique = identité
- Taille des objets
  - Courbes elliptiques

Obstacles à franchir

- Courbes elliptiques
  - génération des clés
  - calcul des couplages de Weil et de Tate
  - migration : représentation des objets
    prouver la sécurité
- Mots de passe
  - résister aux « *attaques par dictionnaire* »
- Nouveaux protocoles : *sécurité prouvée*
  - hybrides
  - « unbalanced », « off-line/on-line »
  - basés sur l'identité