Sim Pratique et Théorie des Couplages pour la sécurité de l'information et des communications

Nadia El Mrabet

LIASD
Université Paris VIII

Crypto'Puce 2013 Porquerolles
Jeudi 30 mai 2013

Courbes elliptiques et cryptographie

- La sécurité est basée sur la difficulté de calculer un logarithme discret dans un groupe
  - Dans $(G, +)$ un groupe, trouver n connaissant $P \in G$ et $[n]P = (P + P + \ldots + P)$ n fois.
- Les points d'une courbe elliptique forment un groupe pour l'addition.
- Il existe de nombreux protocoles utilisant les courbes elliptiques : échange/création clé, signature...

Couplages

Fonction bilinéaire et non dégénérée

$$e : G_1 \times G_2 \to G_T$$

G_1, G_2 et G_T étant des groupes cycliques d'ordre premier r.

Historique des couplages

Un objet mathématique

Le couplage de Weil [années 40]

- Objet mathématique construisant une fonction rationnelle dont les paramètres sont les diviseurs d'une courbe elliptique et le résultat est un élément d'un groupe de racine de l'unité dans un corps fixé.
- Le couplage de Tate-Lichtenbaum est un couplage "simplifié" une seule application de fonction rationnelle sur des diviseurs.

Equation de Miller [années 80]

Victor Miller décrit une relation de récurrence pour la fonction rationnelle et donc un algorithme pour la calculer explicitement.

- Première optimisation : le couplage peut être calculé directement sur les points d'une courbe elliptique plutôt que sur les diviseurs.

Historique des couplages

Un intérêt cryptanalytique

- La cryptographie repose aujourd'hui sur des problèmes difficiles à résoudre (factorisation ou logarithme discret).
- Le problème du logarithme discret se résoud différemment suivant les groupes considérés.
  - Uniquement (?) des algorithmes génériques sur courbes elliptiques.
  - Des algorithmes plus efficaces sur les corps finis.

Transfert du problème du logarithme discret

La bilinéarité des couplages permet de transférer le problème du logarithme discret depuis une courbe elliptique vers un corps fini :

$$e([n]P, Q) = e(P, Q)^n \quad (= e(P, [n]Q)) .$$

- Attaque MOV en 1993.
- Attaque Frey-Ruck en 1994.

Historique des couplages

Un intérêt cryptographique

- A. Shamir propose en 1984 un challenge : construire un protocole basée sur l'identité.
- Première proposition viable : le schéma de Boneh et Franklin en 2001 utilisant des couplages.
- Depuis, de nombreux protocoles basés sur l'identité tous (ou presque) à base de couplage,
- le fameux échange de clé tripartite à la Diffie Hellmann d'Antoine Joux,
- plus des schémas de signatures courtes, en groupe, anonyme...

Intérêt des courbes elliptiques

- signatures ou clés plus courtes
  - facteur 10 par rapport à RSA
- cryptographie basée sur l'identité
  - plus besoin de gérer une PKI
- propriétés supplémentaires
  - anonymat et authentification
  - confidentialité et partage
- peut on l'implémenter sur carte à puce ?

Résultats obtenus dans PACE

projet PACE (Pairing and Advances in Cryptology for E-cash)

projet ANR TELECOM 2007 (sur 2008-2012)

- implémentation d'un couplage
- implémentations effectuées par 4 partenaires différents
  - sur PC (langage C) : $<$ 10 ms (sécurité 128 bits)
  - sur PC (langage java) : $<$ 30 ms (sécurité 128 bits)
  - sur mobile (langage C) : $<$ 10 ms (sécurité 80 bits)
- dernières améliorations par Orange
  - implémentation sur un Samsung Galaxy S2
  - 60 ms (sécurité 128 bits)
- et sur cartes à puce ?

$\Rightarrow$ 750 ms sur un ST22 32-bit à 33MHz

Description du projet

Partenaires

Porteur du projet

Orange Labs (Caen).

Partenaires Grandes Entreprises

- Oberthur Technologies (Paris),
- ST-Ericsson (Le Mans),
- INVIA (Meyreuil) (TPE/PME).

Partenaires académiques

- ENS (Paris),
- Université de Bordeaux 1 (Bordeaux),
- Université de Caen Basse-Normandie (Caen),
- Université de Paris 8 (Paris),
- non financés : Univ de Rennes et ENS Lyon.

Description du projet

Financement INS 2012

SIMPATIC pour SIM and PAiring Theory for Information and Communications security

- Appel Ingenierie Numérique et Sécurité 2012, durée 36 mois.
- Labellisation par les pôles de compétitivité :
  - Transactions Electroniques Sécurisées.
  - Solutions Communicantes Sécurisées.
- Main d'oeuvres supplémentaires : recrutement prévu de post doctorant.

Description du projet

Division du projet

Tâche 1

- management du projet
- liens avec standardisation
- dissémination et exploitation des résultats

Tâches techniques

- 4 tâches différentes
- chacune gérée par 2 partenaires distincts

Description du projet

Division du projet

- Tâche 2 : Théorie et pratique des couplages.
- Tâche 3 : Implémentation des couplages.
- Tâche 4 : Cryptographie.
- Tâche 5 : Cas d'usage.

Tâche 2 : théorie et pratique des couplages

Univ de Caen et Paris 8

- choix des courbes et des paramètres
- étude de l'algorithme de calcul d'un couplage
- amélioration des algorithmes existants
- cas de la délégation du couplage
- aspects attaques physiques
- protection à prendre en compte au niveau algorithmique

Tâche 3 : implémentation des couplages

Invia et Oberthur

- architecture HW/SW
  - répartition des algorithmes
- implémentation
  - partie hardware
  - partie software
- validation et tests sur l'implémentation
- évaluation de la sécurité

Tâche 4 : cryptographie

ENS et Univ Bordeaux 1

- fournir les outils cryptographiques
- cryptographie à base de couplages
- recherche et spécifications
- implémentation des algorithmes sur la carte SIM
- certains protocoles seront implémentés pour les besoins des cas d'usage

Tâche 5 : cas d'usage

Orange et St Ericsson

e-ticket

- porteur : Oberthur Technologies
- système de e-ticket pour les transports avec protection de la vie privée
- suite de PACE, complément au projet LYRICS

stockage dans le cloud + cloud computing

- porteur : Orange Labs
- contrôle d'accès, recherche de document à l'aveugle, stockage aveugle, privacy (identité, localisation)

Montage d'un canal sécurisé entre SIM et TEE dans un mobile

- porteur : ST-Ericsson
- utilisation pour rentrer un mot de passe de façon sécurisée pour valider un paiement en ligne