WISG 18

WORKSHOP INTERDISCIPLINAIRE SUR LA SÉCURITÉ GLOBALE

16 ET 17 OCTOBRE 2018

ESPACE OUEST LYONNAIS - LYON

AGENCE NATIONALE DE LA RECHERCHE ANR

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATION

DGA

SGDSN

Olivier BLAZY

Maître de Conférences
Université de Limoges / Xlim

IDFIX: ID-based cryptography For Identity and eXchange

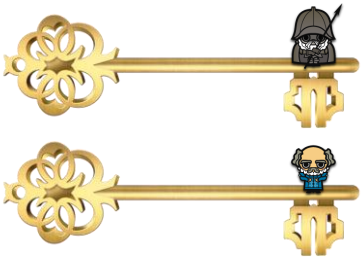
- Projet JCJC de 4 ans démarré en Octobre 2016

- Porté par l'université de Limoges
- Des collaborations avec l'ENS et Paris 2

- Financement de thèse, décharge, missions

Problématique usuelle : Gestion des clés publiques

Problématique usuelle : Gestion des clés publiques



Problématique usuelle : Gestion des clés publiques

Problématique usuelle : Gestion des clés publiques

Solution évoquée en 1984 : ID-Based Cryptography

- Remplacer la clé publique par une chaine sans entropie
  - On peut utiliser un numéro de téléphone pour chiffrer !

- 17 ans avant la première instanciation
- Encore 4 ans avant la première dans le modèle standard
- Puis 8 ans avant une construction « tight »

- Peu d'applications pratiques existantes

Identity Based Encryption (5 algorithmes)

- Setup(k) : Génère les paramètres du système
  - Explique quel type de cryptographie va être utilisée, pour quel niveau de sécurité
- KeyGen(param) : Génère les clés maitres (mpk,msk)
  - Mpk est publique, seule l'autorité garde msk
- UKeyGen(msk,id) : Permet à U de récupérer sa clé secrète
  - Usk[id] peut ne pas être déterministe, l'autorité peut toujours la regénérer
- Encrypt(M,mpk,id) : Chiffre M en C pour une cible id
  - Le chiffré peut ne pas fuiter à qui il est destiné
- Decrypt(C,usk[id]) : Déchiffre C avec la clé secrète, retrouve M

Identity Based Encryption (1-2 notions de sécurité)

- IND-ID-CPA : Etant donné un accès à usk[id] pour id dans I, C et M_0, M_1, un adversaire ne peut pas savoir si C est un chiffré de M_0 ou de M_1, si id^* n'est pas dans I.
  - Peut-être renforcé en PCA, CCA
- Anon-ID-CPA : Etant donné un accès à usk[id] pour id dans I, C, M et Id_0, Id_1 un adversaire ne peut pas savoir si C est un chiffré de M pour Id_0 ou Id_1, si elles ne sont dans I.

Projet IDFIX :

- Améliorer les modèles
  - Contrecarrer le poids de l'autorité
- Proposer de nouveaux chiffrements IBE
  - L'ordinateur quantique se fait menaçant
- Trouver de nouvelles applications
  - Supprimer la confiance dans les autorités intermédiaires de stockage
  - Mais éviter les attaques par les gestionnaires d'identité

Projet IDFIX : Solution PostQuantique

- IBE basé sur la cryptographie à base de codes
  - Solution Post-Quantique
  - S'inscrit dans une logique de transformation de Naor inversée

Projet IDFIX : De nouvelles applications

- Signal : Communication chiffrée sécurisée
  - Gestion des clés publiques par l'autorité centrale (Open Whisper Systems)
  - Les clés publiques sont tagguées par une identité (téléphone)

- Notre solution :
  - Remplacer les clés publiques par de l'IBE
  - Permettre un processus de healing pour empêcher des attaques par l'autorité

Projet IDFIX : De nouvelles applications

- Non-Interactive Key Exchange
  - Date du papier fondateur de Diffie Hellman de 1976
  - Demande des serveurs de clés publiques de confiance
  - NIKE -> IBE existe déjà

- Notre solution :
  - Proposer une construction de NIKE à partir d'IBE (Suppression d'un tiers de confiance)
  - Fonctionne sous plusieurs hypothèses
  - -> Nouvelle caractérisation possible pour les IBE

Projet IDFIX : De nouvelles applications

- ID-based Signature à vérifieur désigné par une identité
  - Authentifie un message pour une autre personne
  - Non cessible

- Notre solution :
  - Plus efficace que les existantes (4 éléments de groupe)
  - Meilleur modèle de sécurité, meilleure hypothèse sous-jacente
  - Construction générique donc transposable au post quantique

Projet IDFIX : De nouvelles applications

- IBE Anonyme Traçable
  - Une autorité supplémentaire qui détecte si un chiffré est pour un utilisateur précis
  - Elle ne peut pas lire les messages
  - Applicable dans l'IoT pour faire du routing
  - Peut filtrer des nœuds/utilisateurs corrompus défectueux

- Notre solution :
  - Transformation semi-générique (ne marche que sur les courbes elliptiques)
  - N'amoindrit pas la sécurité de l'IBE
  - Ne change pas les chiffrés (donc retro compatible)

Projet IDFIX : Perspectives

- Oblivious Transfer optimisé
  - Technologie pour récupérer une ligne dans une base de données de façon *oblivieuse*
  - Première étape lors de la gestation du projet
    - Coût amorti optimal
    - Possibilité d'améliorer le modèle de sécurité

- Une alternative sécurisée aux PIR utilisés en pratique

Projet IDFIX : Perspectives

- Instanciations Pratiques
  - Proposition de prototypes exploitables
  - Diffusion à une communauté plus large pour une adoption générale

    - Code disponible sur le site du projet sous License LGPL V2.1

IDFIX

Merci, des questions ?