Etude détaillé:
Les schémas de chiffrement basés sur les courbes Edwards

Mouhamadou Lamine Ndiongue
Mamadou Sall
El Hadji Mamadou Dia

UFR Sciences Appliquées et Technologies
Universite Gaston Berger de Saint Loius
Master II Cryptologie,Codage et Application (CCA)

Juillet 2022

Étude détaillée

1. Cryptosystéme KMOV basé sur les courbes Edwards
   - Principe
   - Concept
   - Fonctionnement

2. Edwards-curve Digital Signature Algorithm (EdDSA)
   - Principe
   - Concept
   - Fonctionnement
   - Avantage

Cryptosystéme KMOV basé sur les courbes Edwards

Principe

- Le principe de ce genre d'algorithme ne repose que sur la difficulté de factoriser de grands nombres et sont similaires à RSA et au schéma de Rabin.

- Ce schéma de chiffrement utilise seulement une coordonnée d'un point sur une courbe edward pour représenter les messages

Cryptosystéme KMOV basé sur les courbes Edwards

Concept

- Une clé publique **Kpub** $= (e, n)$ pour chiffrer.
- Une clé privée **Kpriv** $= (k)$ pour déchiffrer avec

$$ke \equiv p^{r-1} * (p+1)q^{s-1} * (q+1)$$

.

- Le chiffrement se fait en calculant $C = (x_C, y_C) = e(x_M, y_M)$ avec la courbe Edward Tordu $E_{-d,d,n}$ avec l'équation $-d * x^2 + y^2 \equiv 1 + d * x^2 * y^2 (\text{mod n})$
- Le déchiffrement se fait en calculant $M = (x_M, y_M) = k(x_C, y_C)$ avec la courbe Edward Tordu $E_{-d,d,n}$ avec l'équation $-d * x^2 + y^2 \equiv 1 + d * x^2 * y^2 (\text{mod n})$
- Propriété : La connaissance de **Kpub** ne permet pas de déduire **Kpriv**.
- **DKeypriv (EKpub (Message)) = Message**.

- Cependant, à l'inverse du chiffrement symétrique où le nombre de clés est le problème majeur, ici, seules n paires sont nécessaires.
- Alors, chaque utilisateur possède une paire (Kpub, Kpriv) et tous les transferts de message ont lieu avec ces clés.
- Chaque utilisateur conserve sa clé secrète (privée) sans jamais la divulguer. Seule la clé publique devra être distribuée.

Edwards-curve Digital Signature Algorithm (EdDSA)

Principe

- EdDSA est un algorithme de signature à clé publique similaire à EcDSA.

- Le principe de EdDSA est un schéma de signature déterministe car il utilise un processus déterministe pour générer le scalaire secret r (appelé clé de session) nécessaire pour signer un message M.

Edwards-curve Digital Signature Algorithm (EdDSA)

Concept

- Une clé privée **Kpriv** $= a$ pour signer avec $a = 2^{b-2} + \sum_{3 \leqslant i \leqslant b-3} 2^i h_i$
- Une clé publique **Kpub** $= A$ pour vérifier une signature.
- A est calculé à partir du point de base $B \neq 0, 1$ d'ordre l et $a = 2^{b-2} + \sum_{3 \leqslant i \leqslant b-3} 2^i h_i$ tel que $A = a * B$
- La signature est (R, s) avec $R = r * B$ et $s = (r + a * h) modl$.

Edwards-curve Digital Signature Algorithm (EdDSA)

Fonctionnement

- Nous devons d'abord choisir l'algorithme à utiliser pour créer et utiliser notre signature EdDSA(Ed25519 et Ed448).

- Une fois que nous avons choisi notre courbe, nous commençons la génération du clé publique et Clé privée.

- La signature avec EdDSA est assez simple mais efficace et sûre. Le processus consiste à prendre les informations que l'on souhaite signer et à en créer un hachage. Ce hachage garantit que la clé aléatoire pour générer la clé publique est complètement différente à tout moment. Cette clé aléatoire est ensuite appliquée à la formulation de la courbe elliptique qui produit la signature du document.

Edwards-curve Digital Signature Algorithm (EdDSA)

Avantage

- EdDSA offre un haut niveau de rapidité, d'optimisation et de sécurité dans une seule application.
- Les signatures EdDSA sont complètement déterministes. Cela signifie que les signatures auront toujours les mêmes propriétés et valeurs à tout moment.
- Le système offre une résistance aux attaques par canal latéral. Il s'agit d'une mesure de sécurité qui empêche les signatures d'être brisées par ce type d'attaque par force brute.
- Les formules sont valables pour tous les points de la courbe, sans exception. Cela évite à EdDSA de procéder à une validation de points coûteuse sur des titres publics non approuvés.

Edwards-curve Digital Signature Algorithm (EdDSA)

Avantage

- EdDSA fournit également une résistance aux collisions, ce qui signifie que les collisions de fonction de hachage ne cassent pas ce système (ne s'applique qu'à PureEdDSA).
- Les signatures et clés générées par EdDSA sont de petite taille.