Cryptographie RSA sur des polynômes

A.Balan

4 septembre 2017

Résumé

Une cryptographie proche de RSA est définie pour des polyômes.

1 Définition

On définit un nombre $n = pq$ produit de deux nombres premiers et on considère $Z = (\mathbf{Z}/n\mathbf{Z})[X]/(X^a - 1)$ avec a un nombre premier (on quotiente par l'idéal principal).

2 Le théorème chinois

Par le théorème chinois [M], on a :

$$\mathbf{Z}/n\mathbf{Z} \cong (\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$$

Et donc :

$$Z = (\mathbf{Z}/n\mathbf{Z})[X]/(X^a - 1) \cong (\mathbf{Z}/p\mathbf{Z})[X]/(X^a - 1) \times (\mathbf{Z}/q\mathbf{Z})[X]/(X^a - 1)$$

De ce fait, on a pour les inversibles Z^* de Z :

$$Z^* = [(\mathbf{Z}/p\mathbf{Z})[X]/(X^a - 1)]^* \times [(\mathbf{Z}/q\mathbf{Z})[X]/(X^a - 1)]^*$$

3 RSA pour les polynômes

On choisit donc $n = pq$ et a et on choisit un inversible i de Z dont l'inverse se calcule sachant le cardinal de Z^*.

4 Le cardinal de Z^*

Le cardinal est donné, sachant le cardinal de $[(\mathbf{Z}/p\mathbf{Z})[X]/(X^a - 1)]^*$ qui est $p^a - 1$. On a donc :

$$Card(Z^*) = (p^a - 1)(q^a - 1)$$

5 Alice et Bob

Alice envoit p,q,a à Bob ; elle choisit un inversible i de Z qu'elle envoit aussi à Bob. Bob multiplie son message par i. Alice peut décoder car elle peut inverser i.

Références

[M] P.Meunier, "Arithmétique modulaire et cryptologie", éd. Cépaduès, 2010.

[S] I.Shparlinski, "Number Theoretic Methods in Cryptography", Birkäuser, 1999.