Cryptographie RSA sur des polynômes (II)

A.Balan

13 septembre 2017

Résumé

Une cryptographie proche de RSA est définie pour des polynômes.

1 Définition

On définit un polynôme $N = PQ$ produit de deux polynômes irréductibles de $\mathbf{F}_q[X]$ (q est une puissance d'un nombre premier p) P,Q de degré a,b (voir [LN]). On considère $Z = \mathbf{F}_q[X]/(N)$.

2 Le théorème chinois

On a une application du théorème chinois (voir [M]) :

$$Z = \mathbf{F}_q[X]/(N) \cong \mathbf{F}_q[X]/(P) \times \mathbf{F}_q[X]/(Q)$$

Cela donne :

$$Card(Z) = q^{a+b}$$

le cardinal de Z,

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

le cardinal des inversibles de Z.

3 Alice, Bob et Oscar

Alice choisit P,Q et envoie N et i, un inversible de Z, à Bob. Bob multiplie son message m par i et envoie $i.m$ à Alice. Elle peut inverser i et décrypte im par $i^{-1}.i.m = m$. Oscar connait i et $i.m$ mais il ne peut trouver m car il ne connait pas l'inverse de i.

Références

[HPS] J.Hoffstein, J.Pipher, J.H.Silverman, "An Introduction to Mathematical Cryptography", Springer, 2000.

[LN] R.Lidl, H.Niederreiter, "Introduction to finite fields and their applications", Cambridge, 1994.

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

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