Cryptographie sur le cercle

A.Balan

12 septembre 2017

Résumé

Une cryptographie est définie pour le cercle en tant que groupe commutatif.

1 Définition

On considère le cercle dans le corps fini à q éléments:

$$S_q^1 = S^1(\mathbf{F}_q) = \{(x,y) \in \mathbf{F}_q^2; x^2 + y^2 = 1\}$$

La multiplication est commutative et associative, ce qui rend au cercle une structure de groupe :

$$(x,y) \times (x',y') = (xx' - yy', xy' + x'y)$$

2 Le cardinal du cercle

Le cardinal du cercle s'obtient en faisant un paramétrage du cercle par des droites passant par (1,0). On obtient ainsi :

$$Crad(S_q^1) = Card(S^1(\mathbf{F}_q)) = q + 1$$

si -1 n'est pas un carré de $\mathbf{F}_q$.

$$Card(S_q^1) = Card(S^1(\mathbf{F}_q)) = q - 1$$

si -1 est un carré de $\mathbf{F}_q$.

3 Cryptographie RSA et ElGamal

On produit un cryptosystème RSA sur le groupe S^1 :

$$S_n^1 = S^1(\mathbf{Z}/n\mathbf{Z}) \cong S^1(\mathbf{F}_p) \times S^1(\mathbf{F}_q)$$

$n = pq$.

$$Card(S_n^1) = Card(S_p^1).Card(S_q^1)$$

Et aussi ElGamal sur le cercle en tant que groupe fini.

Références

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

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

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