Discipline(s) : Infomatique et télécommunications

# EUCLIDEAN LATTICES FOR CRYPTOGRAPHY

| | |
|---|---|
| **Nature** | UE |

## RESPONSABLES

Christophe Ritzenthaler

## OBJECTIFS

Cette UE est commune avec le master de cryptographie de l'UFR de mathématiques.

## CONTENU

Définitions et propriétés élémentaires (Gram-Schmidt, Minkowski) puis les bornes théoriques sur les vecteurs courts
LLL : Algorithme de proprification, algorithme global, analyse de la complexité
Application de LLL à RSA, RSA OAEP
SVP/CVP, réseau dual, smoothing parameter, gaussiennes discrètes
Complexité des problèmes sur les réseaux
Problèmes SIS et LWE et réductions pires-cas moyens-cas
Construction de signature reposant sur SIS
Construction de chiffrement à clé publique reposant sur LWE
Si le temps le permet, Réseaux idéaux et applications

## APPARTIENT À

Master 2 informatique parcours Science Informatique

Mise à jour le 17 juillet 2017

## CONTACT(S)

Département Informatique et télécommunications
École normale supérieure de RennesCampus de Ker LannAvenue Robert Schuman
35170 BRUZ
Tél. : 02 99 05 52 43
E-mail
Site Internet