Proposition de recherche doctorale

Potentiel des attaques d'ordre élevé, notamment électromagnétiques.

Mots clés :

- **Directeur de thèse** : JEAN-LUC DANGER
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire Traitement et Communication de l'Information
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Toute implémentation cryptographique fuit de l'information via divers canaux auxilliaires (Consommation de puissance, émissions électromagnétiques ...). Certaines fuites sont facilement exploitables, et permettent à un attaquant potentiel d'extraire des informations a priori secrètes. L'objet de la thèse est d'étudier les attaques par canaux auxilliaires, dîtes d'ordre élevé, et de les comparer à des attaques d'ordre simple afin de déterminer quelle quantité d'information elle sont capables d'extraire.