

---

# Engagements flous non linéaires basés sur les codes de Kerdock

Patrick Lacharme\*<sup>1</sup>

<sup>1</sup>ENSICAEN, Greyc, Caen – Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen – France

## Résumé

Les schémas d'engagement flou (fuzzy commitment) sont utilisés pour protéger les données biométriques. Ils sont basés sur des codes correcteurs linéaires, ce qui les rend vulnérables à des attaques par indistinguabilité. Dans cet exposé, on étudiera comment utiliser des codes non linéaires pour se protéger contre ces attaques, en se focalisant en particulier sur le cas des codes de Kerdock.

---

\*Intervenant