自己紹介

岩田　哲
名古屋大学大学院工学研究科
計算理工学専攻

専門分野

- 暗号理論
- 共通鍵暗号系
  - ブロック暗号利用モード
  - メッセージ認証コード
  - 証明可能安全性
- NIST SP 800-38B CMAC (Cipher-based MAC) の設計者の一人

最近の研究

- 暗号化モードCENCの設計 (FSE 2006)
  - バースデーバウンドを超える安全性
  - CTRモードと同等の計算効率