IoT向け耐タンパー技術の研究

研究者プロフィール

・工学部　情報基盤工学科　教授　神永　正博
・解析学、情報セキュリティ
・作用素論、暗号理論
・日本数学会、電子情報通信学会、IEEE、国際暗号学会
・東京電機大学情報科学科助手、日立製作所中央研究所を経て
現職。著書に『現代暗号入門』『「超」入門微分積分』
講談社ブルーバックス、『Pythonで学ぶ暗号理論』コロナ社等多数

研究内容

研究分野は複数あるが、ここでは暗号理論について述べる。主にICカードなどのデバイスに実装された暗号に対するサイドチャネル攻撃とその対策技術の研究を行っている。関連して、乱数発生装置とそのモデリングの研究や、量子コンピュータでも破れないブロック暗号の研究も行っている。ここ数年は、格子を利用したフェイステル型ブロック暗号や、ハッシュ関数やランダム格子の性質を研究している。

関連キーワード

暗号、ICカード（スマートフォンSIMカード）、耐タンパー技術、IoT

地域・産学官連携の可能性、事業化のイメージ 他

研究者への連絡先

産学連携推進センター
E-mail　srcenter@mail.tohoku-gakuin.ac.jp
電話　022-354-8122