

✧ **5月31日（木）**

✧ **午後5時00分開始**

✧ **情報科学研究科棟 2F 大講義室**

話題：暗号実装技術の最前線

～暗号モジュールへのサイドチャネル攻撃とその防御～

話題提供者： 本間 尚文 准教授

（情報基礎科学専攻 計算科学講座 計算機構論分野）

暗号は安心・安全な情報化社会を構築する上で欠かすことのできない基盤技術です。近年、暗号アルゴリズムを実装したソフトウェアやハードウェア（暗号モジュール）は、ICカードやスマートフォンなど身の回りの電子機器にも広く搭載されています。

一方で、暗号モジュールの実装上の脆弱性から秘密情報を奪う実装攻撃の危険性が指摘されています。特に、暗号モジュールの動作中に生じる消費電力や放射電磁波といった本来の入出力以外の情報（サイドチャネル情報）を観察することで秘密情報を奪うサイドチャネル攻撃は、比較的安価な装置で実行できるだけでなく、攻撃の痕跡も残さないことから、現実的な脅威であると言われています。

本談話会では、サイドチャネル攻撃とその対策について説明し、暗号実装研究の最新動向を紹介します。

第46回 情報科学談話会