電気通信大学　Ⅱ類 セキュリティ情報学プログラム ／ 大学院 情報学専攻

李研究室　暗号を、物理の世界から守る。

崎山・李・宮原 研究室

ハードウェアセキュリティ　サイドチャネル攻撃　故障注入攻撃　耐量子暗号（PQC）　ロジックロッキング　AI × セキュリティ

数学的に安全な暗号も、「動かす機器」から秘密が漏れる

スマートフォン、ICカード、自動車、IoT機器。暗号はすべて、小さなチップの上で計算されています。

計算中のチップは電力を使い、電磁波を出し、ときには誤動作します。こうした物理現象を手がかりにすると、数学的には解けないはずの**秘密鍵が盗まれてしまう**ことがあります。

攻撃して理解し、防御して証明する
物理攻撃を自分たちの手で再現し、防ぐ技術をつくる研究室です



サイドチャネル攻撃　「漏れ」を観測する
消費電力や電磁波の波形を観測して、秘密鍵を推定する

故障注入攻撃　わざと誤らせる
電圧などで計算をわざと誤らせ、誤りから鍵を推定する

回路の改ざん・盗用　中身に手を加える
ハードウェアトロイの混入や、設計の不正コピー

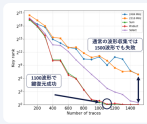
いま、学生が取り組んでいる研究

学年は2026年度

量子コンピュータ時代の暗号を守る　耐量子暗号（PQC）の安全な実装

修士2年　室本 悠生

無線チップから漏れる電波で鍵を読む



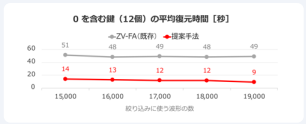
通常の測定
1500波形でも失敗
2周波数の同時測定
1100波形で成功

無線チップでは、暗号計算の情報が通信の電波に混ざって漏れます。2つの周波数を同時に測定し解析。

少ない波形数で鍵の復元に成功

修士1年　蔵谷 陸

電子署名 ML-DSA の鍵復元を高速化

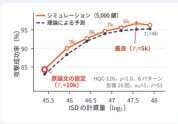


波形から鍵を推定する既存手法に、値が0の鍵を見落とす弱点を発見。0を優先して探す方法に改良。

鍵の復元 約50秒 → 約9〜14秒

学部4年　YAN XIN

攻撃の成功率を理論で予測する



シミュレーション
約5分
理論モデル
数秒

暗号 HQC への攻撃がどこまで成功するかを、シミュレーションなしで計算できる理論モデルを構築。

予測の誤差は最大 約2ポイント

WANG

計算の「誤り」を見逃さない乗算



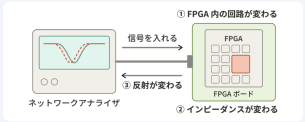
暗号で繰り返し使う「乗算」が攻撃で誤っても検出できる仕組みを研究。開発ボードで検証します。

目標：安全性と処理性能の両立

チップと回路そのものを守る

学部4年　疋出 真翔

電気の「反射」でチップの改ざんを見抜く



チップの電源に信号を入れ、返ってくる反射の変化から、回路が改ざんされていないかを調べます。

AES回路の有無を3帯域で検出

修士2年　LI ENZE

回路にかけた「鍵」は故障攻撃に耐えるか



正しい鍵がないと動かない回路で盗用を防ぐ「ロジックロッキング」。故障注入に対する影響を評価。

進行中：復元率への影響を比較

AI時代の新しいリスク

学部4年　山本 怜奈

声でコードを書く時代の落とし穴



話した言葉
「退会」
AIの補正後
「再開」

AIに話しかけてコードを書かせる開発で、日本語の誤認識とAIの自動整形が招くバグの危険を検証。

正反対の処理に変わる例を確認

体験してみよう

実機不要・ブラウザだけ

物理攻撃をブラウザで体験

攻撃のしくみを学べる
ミニ実験を4種類公開中

李研究室の案内ページへ

研究室を探している学部3・4年生へ

こんな人を歓迎

- 新しい技術を進んで学びたい人
- 実機や実験データに粘り強く向き合える人
- コツコツ手を動かす時間をつくれる人
- AI時代の自分の専門性を考えたい人
- ソフト・ハード・AIの得意を活かしたい人

身につく力

- 論文から情報を集め、整理する力
- 課題を見つけ、わかりやすく伝える力
- 相手の視点に立って議論・発表する力
- AI・装置・時間・人脈を活かす力
- 成果を論文・発表・デモにまとめる力

研究の進め方

- テーマは興味・得意・進路を相談して決定
- 週1回の全体ゼミ（オンライン）と個別ゼミ
- 崎山研・宮原研と共同運営、合同ゼミも
- 国内外の学会で発表するチャンス
- 2026年は修士1年が国際会議で発表

李 陽　准教授　LI Yang

電気通信大学 大学院情報理工学研究科。同大学で博士後期課程を修了後2018年より現職。

東3号館（総合研究棟）828室
Liyang AT uec.ac.jp
https://sakiyama-lab.jp/

見学・配属の相談

- メールでお気軽に（Zoom面談も可）
- オープンキャンパスでは東3号館818室で研究デモ

研究室HP