【ネットワークLSIシステム（藤野）研究室】
～IoT（Internet of Things）&AIセキュリティ～

RITSUMEIKAN NTSOC LAB.

○研究室の基礎データ

所在地・連絡先	研究室スタッフ
ローム記念館３F南側（RO301　藤野個研室，並びでエレベータに向かって第１～第４研究室） Webページ http://www.ritsumei.ac.jp/se/re/fujinolab/ 電話（教授室）077-561-5150（内線 8391） 教員（藤野）mail: fujino@se.ritsumei.ac.jp	【教授】藤野　毅（たけし） 【客員研究教員】白畑　正芳【秘書】松田　詩織 【学生】博士後期課程　２名（１名は社会人学生） 博士前期課程：１１名　学部生：９名

○研究テーマの概要

図１に示すように，サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会，すなわち Society 5.0 を実現することがこれからの社会の目標となっています．（内閣府 HP より）

当研究室では，特にフィジカル空間に配置される IoT 機器を安心して使用するために，下記のようなセキュリティ＆深層学習技術（AI 技術と記載します）を研究することを目標としています．

(1) 各種センサで正しいデータを取得する
(2) 搭載されるエッジ AI で正しい判断を行う
(3) IoT 機器が搭載される機器の知的財産を守る
(4) 収集されるデータのプライバシーを守る

上記の目標を搭載するためには，様々な暗号関連技術の導入が必要です．特にフィジカル空間では攻撃者が IoT 機器に直接触れて悪意ある攻撃を行うことができるので，ハードウェア自身にもさまざまな対策（ハードウェアセキュリティ技術）を行うことが必要です．

図１．Society 5.0 で目指している社会
https://www8.cao.go.jp/cstp/society5_0/index.html

○研究テーマ解説

＊サイドチャネル攻撃･フォルト攻撃

暗号技術は，情報の秘匿だけでなく，通信相手が正しい相手であること，データが改ざんされてないことを保証するために必須の技術ですが（秘密にすべき）暗号鍵を攻撃者に入手されないようにすることが不可欠です．図２に示すように暗号回路に入力する平文，暗号文を解析しても，攻撃者は現実的な時間では暗号鍵を取得できません．しかしながら，暗号回路が動作しているときの消費電力や漏洩電磁波を用いる（サイドチャネル攻撃），または，電源電圧や異常クロックなどの外乱を入力する（フォルト攻撃）ことで暗号鍵を取得する技術があります．研究室では AI 技術を適用してより高度なサイドチャネル攻撃を実現できる手法の研究を行っています．

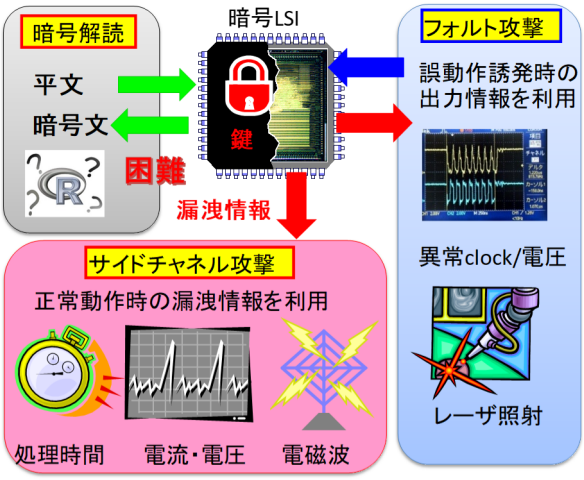

図２．暗号鍵を取得する各種攻撃

＊複製不可能デバイス PUF（Physical Unclonable Function）

図３に示すように LSI の個々のデバイスの製造ばらつきを使用して，デバイスの指紋となる固有の識別番号（ID）を生成する技術を PUF と呼びます．PUF の ID を使用することで，機器固有の複製不可能な暗号鍵を生成することができるため，従来の不揮発性メモリにあとから暗号鍵を書き込む方式と比較して，安価で高いセキュリティを実現できます．最近では大倉研究室と共同でイメージセンサを用いた PUF 技術の研究を行っています．

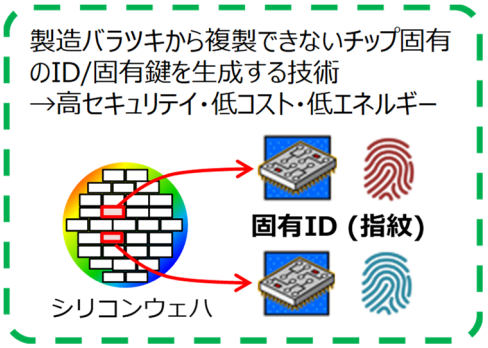

図３．PUF 技術

＊AI をだます攻撃（Adversarial Examples 等）

AI 技術は，予測や判断の過程がブラックボックス化されているため，(1)判断の根拠がわからない，(2)人間には考えられないような誤動作を引き起こす場合がある，ことが問題点となっています．特に画像認識システムにおいて，人間にはほとんど感じられないような微小なノイズを画像に付加することで AI に誤判断を引き起こすという「Adversarial Examples（AE）攻撃」が話題になっています．本攻撃を用いて，図４のように交通標識にステッカーを貼ることで，自動運転車向けのエッジ AI を誤動作させ事故を誘発できる可能性が学会で示されました． AE の生成をするためには，AI 処理の内部パラメータが必要なのですが，そのパラメータを，サイドチャネル攻撃を用いて取得する研究や，AI 処理の内部パラメータを使わずに AE を作成する研究などを行っています．

図４． Adversarial Examples 攻撃

〇研究環境と研究設備

藤野研究室では，2009 年より，科学技術振興機構（JST）の戦略的創造研究推進事業（CREST）でハードウェアセキュリティに関する研究を本格的に開始し，その後新エネルギー・産業技術総合開発機構（NEDO）の PUF の研究を実施し，現在も JST の未来社会創造事業で AI のハードウェアセキュリティの研究を行っており，常に産業界と交流しながら研究を進めています．研究設備としても，ディープラーニング用計算機，各種計測機器，FPGA が搭載された実験ボードなどがそろっています．今後これらの機器を活用した，さまざまな新しい研究の提案も歓迎します．

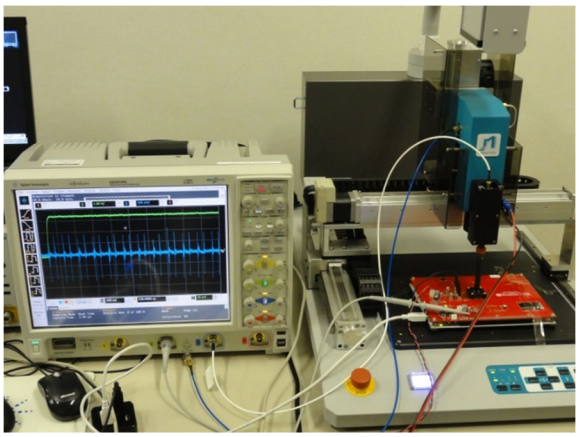

図５． サイドチャネル攻撃評価環境

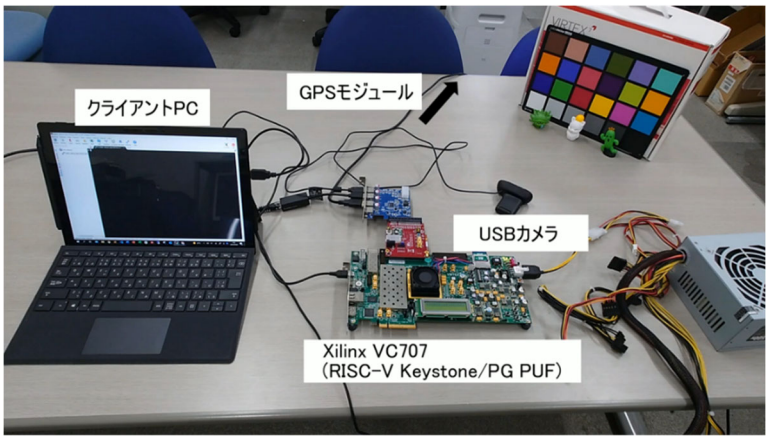

図６．RISC-V（オープンコア CPU）を使った PUF デモシステム

〇応用演習・卒業研究の進め方・大学院での研究

応用演習では，機械学習や深層学習を用いた画像処理を，Python を用いてプログラミング演習します．応用演習終了後の２月中旬以降，週１回，英文書（暗号技術に関する入門書）を一年間かけて輪講するとともに，５月頃から大学院生から，AI をだますプログラミングやサイドチャネル攻撃などの実践的な実習を開始します．院進学希望学生は，４回生の４月に仮研究テーマを選択して，院生と一緒に研究を開始します．７月の上旬に発表会を行い，夏休み前後に卒研での研究テーマを最終決定して本格的に卒業研究を開始します．

大学院に関してですが，研究および技術開発職に就きたいのであれば進学を勧めます．修士課程で，学会発表や企業との共同研究の打ち合わせに参加することで，企業で実際に求められている技術スキルの内容やレベルを実際に感じて，自分の能力をどのような企業のどんな分野で活用したいのかが分かってくると思います．

〇さいごに

政府の「AI 戦略」では，25 万人の学生を「AI 人材」として教育するという目標が立てられており，もはや理工系特に情報を名の付く学生には「AI」は必須の技術として学んでおく必要があるでしょう．さらに，当研究室の学生には，もう一つ「セキュリティ」の技術をしっかり学んでほしいと思っています．

ただし，電子情報技術分野で長く活躍できる人材となるためには，学生時代に知識や技術力を修得するだけでなく，新しい技術に対する好奇心を育て常に新しい技術にチャレンジする能力，さらに，高いコミュニケーション能力とプレゼンテーション能力も必要です．このような意欲を持つ学生を歓迎します．