東北大学

平成 26 年 9 月 24 日

報 道 機 関　各位

国立大学法人 東北大学大学院情報科学研究科
国立大学法人 神戸大学大学院システム情報学研究科

情報通信機器の安全性を高める攻撃検知センサの設計技術を確立

ー　近傍電磁界の乱れから攻撃の兆候を瞬時に検知できることを実証　ー

■ ポイント ■

・情報通信機器へのサイドチャネル攻撃を未然に防ぐ攻撃検知センサ回路（6 月にコンセプト・回路構造を公表）の設計技術を確立した
・上記技術を用いて製造したテスト LSI により,攻撃時に生じる微小な近傍電磁界の乱れから攻撃の兆候を瞬時（１マイクロ秒以内）に検知できることを実証した
・安価で効率的な設計・製造技術の確立により，今後 IC カードやスマートフォンをはじめとする様々な製品に同センサ技術が搭載され，安全性が飛躍的に高まることが期待される

■ 概　要 ■

東北大学大学院情報科学研究科本間 尚文准教授，林 優一准教授，青木 孝文教授と，神戸大学大学院システム情報学研究科三浦 典之特命助教，藤本大介研究員，永田 真教授らのグループが，暗号機能を実装した情報セキュリティ製品を，※１サイドチャネル攻撃と呼ばれる強力な攻撃から守る攻撃検知センサ回路（6 月にコンセプト・回路構造を公表）の設計技術を確立し，そのセンサ回路の有効性を示す実証実験に成功した。

近年，個人情報や金融情報といった大切な情報が IC（集積回路）カードをはじめとする情報通信機器を通してインターネット上でやりとりされることが一般的となっているが，そのような情報を守るため機器内部には暗号化処理を実行するソフトウェアやハードウェア（暗号モジュール）が搭載されている。一方，暗号モジュールの消費電力や電磁波などを利用して※２暗号の鍵を盗み出すサイドチャネル攻撃と呼ばれる攻撃が報告されており，同攻撃による現実的な脅威が指摘されている。暗号モジュールの普及が進む欧米では実際にサイドチャネル攻撃によるものとみられる被害も報告されている。特に，暗号モジュール動作中に放出される電磁波を観測・解析する電磁波解析攻撃は，非接触・非破壊な攻撃なため，サイドチャネル攻撃の中でも最も強力な攻撃の一つとされていた。近年では，従来の対策では原理的に防げない新たな電磁波解析攻撃が報告されており，有効な対策技術の開発が急務となっていた。

東北大学と神戸大学は，こうしたサイドチャネル攻撃を未然に防ぐ攻撃検知センサ回路の開発に世界で初めて成功した。開発した新技術では，暗号化処理を行う回路上もしくは内部に微小で安価なセンサーコイルを配置し，攻撃者が情報を奪おうと回路に探針を接近させると，そ

れにより生ずる電磁界の乱れをセンサーコイルが検出し，攻撃の気配を検知することができる。そうした電磁界の乱れは物理法則上必ず生じるため，将来にわたってこの種の攻撃に対する根本的な対策になり得ると期待される。今回は，従来技術を利用して同センサ回路を容易に製造可能であることを示すとともに，確立した技術を用いて製造したテスト回路により，上記のセンサ機能の有効性を実験により実証した。今後，開発した新技術により，IC カードやスマートフォンをはじめとする暗号機能を実装した情報セキュリティ製品全体の安全性向上に貢献することが期待される。なお，上記の新技術は，9 月 23 日から開催される暗号ハードウェアと組込みシステムに関して最もよく知られる国際会議（CHES）において発表された。本発表論文には，同会議から最優秀論文賞が授与されるなど，世界的な注目が集まっている。

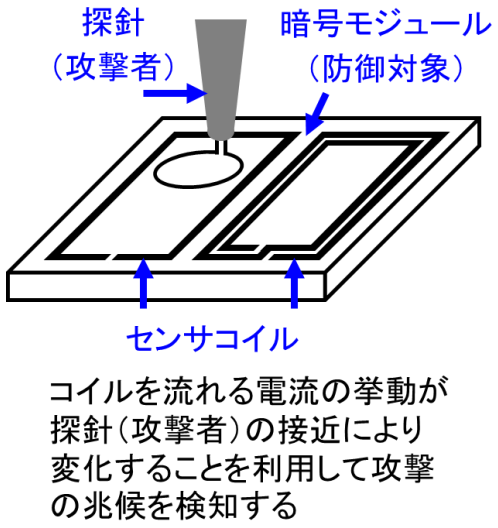

図１：開発したセンサの概観

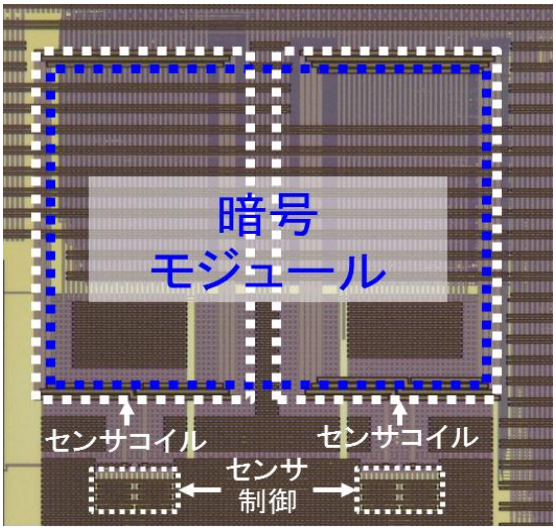

図２：製造したセンサ回路の概観

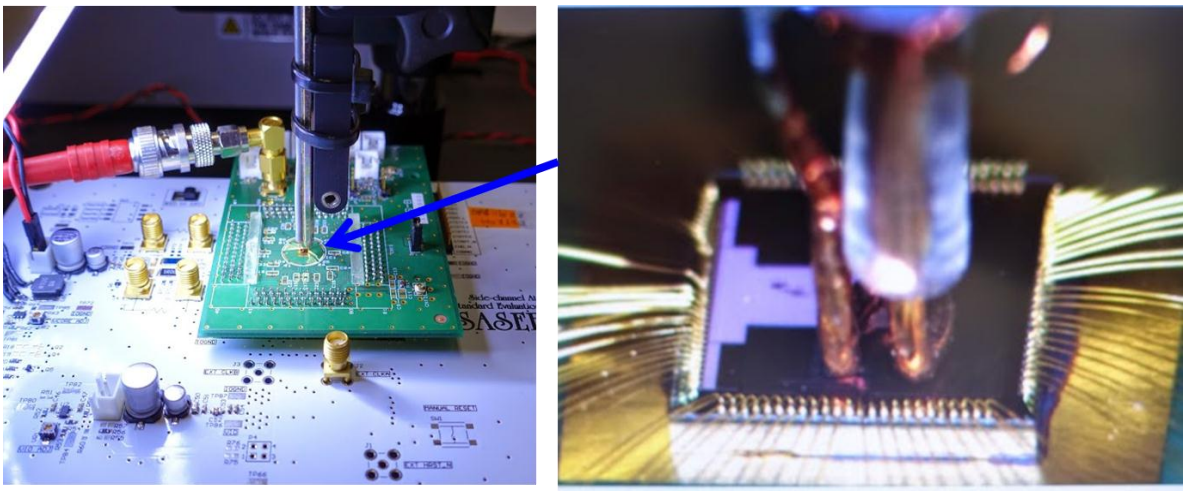

図３：センサによる攻撃検知実験の様子

■ 開発の社会的背景 ■

インターネットの急速な拡大と，スマート端末，IC カード，RFID タグ等の普及により，生活のあらゆる場面で大量のデータがやりとりされ，情報の漏洩や改ざんといったセキュリティ上の脅威が増している。暗号はそのような脅威へ対抗するために必須の基礎技術として民生品にも広く利用されている。しかし一方で，暗号処理を実行するソフトウェアやハードウェア※３（暗号モジュール）に対する実装攻撃の脅威が顕在化している。とりわけ動作時の消費電力や電磁波などに漏洩する内部処理情報を利用して秘密の鍵を盗み出すサイドチャネル攻撃は現実的な脅威となり得ることが専門家から指摘されている。

■ 研究の経緯 ■

東北大学と神戸大学では，JST（科学技術振興機構）の戦略的国際共同研究プログラムなどを通して，IC カードに代表される暗号機能を持つ製品の安全性向上を目的として，2010 年より共同で研究開発に取り組んできた。2014 年 6 月には，集積回路技術に関する世界的な国際会議 VLSI シンポジウムにおいて，当該センサ回路のコンセプトと基本回路構成について報告し，同シンポジウムの注目論文として同シンポジウムから広報されていた。なお，今回は，科学研究費補助金「暗号ＶＬＳＩの電磁波セキュリティを確保するサイドチャネル攻撃センサの構成法と実証」（研究代表：神戸大学　永田真）の研究開発の一環として行われた。

■ 研究の内容 ■

今回確立した設計技術では，手設計部分を排除し，従来の LSI 設計ツールのみを用いる。これにより，多様な暗号モジュールの構成に応じて当該センサ回路を容易かつ安価に集積できるようになった。また，従来の対策技術では，暗号モジュールの演算性能を大幅に低下させることが課題であったが，当該センサ回路では性能のオーバーヘッドを数%程度に抑えることに成功している。さらに，今回開発したセンサは，暗号モジュールに限らず，探針による攻撃にさらされる可能性のある製品すべてに適用可能である。今回製造したテストモジュールでは，国際標準暗号アルゴリズムである※４AES の回路とともに，センサ回路を集積した。実験により，従来の対策では防ぐことが難しい電磁波解析攻撃を瞬時に検知・無効化できることを実証した。また，センサ搭載による全体の速度低下は高々0.2%程度と非常に小さいことを確認した。

■ 今後の予定 ■

センサ回路の性能向上を図る。特に，現在暗号モジュールの近傍に限られるセンシング範囲（0.1㎜）を延伸するための改良を行っていく。また，実用化に向けて，多様な攻撃を想定し，実証実験を引き続き実施していく。将来的には，当該センサ回路技術を通して，IC カードやスマートフォンをはじめとする様々な製品の安全性向上に貢献することを目指している。

■ 本件問い合わせ先 ■

国立大学法人 東北大学　大学院　情報科学研究科
准教授　本間　尚文　　〒980-8579　宮城県仙台市青葉区荒巻字青葉 6-6-05
TEL：022-795-7169　FAX：022-263-9308
E-mail：homma@aoki.ecei.tohoku.ac.jp

国立大学法人 神戸大学　大学院　システム情報学研究科
特命助教　三浦　典之　　〒657-8501　兵庫県神戸市灘区六甲台町 1-1
TEL：078-803-6221　FAX：078-803-6221
E-mail：miura@cs.kobe-u.ac.jp

【用語の説明】

※１サイドチャネル攻撃

暗号アルゴリズムを実行するハードウェアもしくはソフトウェア（暗号モジュール）が動作中に消費する電力や放射する電磁波は，処理内容に応じた独特の波形として観測される。このような正規のデータ入出力パスでない副次的なパス“サイドチャネル”に漏洩している内部動作の情報から秘密情報を盗み出す攻撃法。

※２暗号の鍵

暗号はデータを第三者の盗聴などから守るために，ある規則によって入力文（平文）を暗号文に変換したり，元のデータに逆変換するアルゴリズムである。しかし，その規則が常に同じでは誰にでも同じ変換ができてしまうため，データを守ることができない。そこで，変換規則を変えるために，利用者毎に異なる鍵と呼ばれる秘密のパラメータが用いられる。

※３暗号モジュールの実装攻撃

標準規格に採用されている暗号のアルゴリズムは一般に，公開の場において専門家による安全性評価に合格したものであり，理論的な解析によって解読することは現実問題としてできない。しかし，ソフトウェアやハードウェアによって暗号モジュールとして実装されたときに，その実装方式の弱点を突いて暗号の鍵を盗み出すのが実装攻撃である。暗号モジュールを破壊する攻撃と，サイドチャネル攻撃のように破壊を伴わない攻撃に大きく分けられる。

※４AES

Advanced Encryption Standard。2001 年に米国国立標準技術研究所が連邦標準（FIPS PUB 197）として制定した暗号アルゴリズムで，2005 年に国際標準規格（ISO/IEC18033-3）として採用された。世界で最も広く利用されている暗号アルゴリズムの一つ。