PRESS RELEASE

兵庫県教育記者クラブ加盟各社御中

２０１４．６．１２

神　戸　大　学

東　北　大　学

ICカードの覗き見を検知するセンサを開発

神戸大学大学院システム情報学研究科の三浦 典之特命助教、永田真教授らと東北大学大学院情報科学研究科の林 優一准教授、 本間 尚文准教授、青木孝文教授の共同研究グループは、ICカードに保存されている重要な情報の覗き見を検知するセンサを開発。6月13日（現地時間）ハワイで開かれている半導体分野で世界的に知られる国際会議「VLSIシンポジウム」で発表します。この論文は会議のハイライト論文に取り上げられ、プレスリリースにも紹介されています。

http://www.vlsisymposium.org/wp-content/uploads/2013/06/2014-VLSI-Symposia-Tip-Sheet-Japanese-Apr17_2014_fin1.pdf

内容についての取材、問い合わせを勘案して、この論文についての報道解禁は新聞を6月14日組朝刊、放送・WEBを15日午前4時に設定させていただきます。

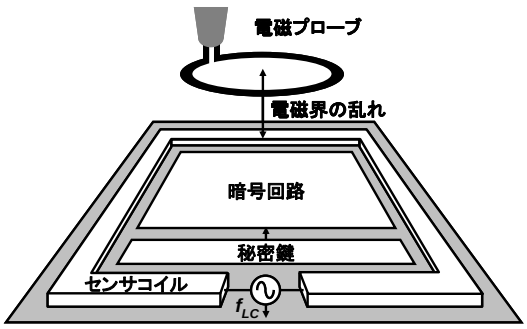

図１ 提案する電磁波攻撃センサの概念図

近年の高度情報化社会においては、取り扱いに注意すべきセンシティブな情報(例えば個人、医療、口座、社内、国家機密あるいは防衛に関わる情報)があまねく電子化されて、コンピュータすなわち集積回路(IC)チップによって保存・管理されている。また電子マネーやネットショッピング、IC付きATMカードやクレジットカードが広く普及しており、我々の身近な生活の中においても、高い秘匿強度が要求されるデジタルセキュリティICの需要が高まっている。電子データを安心・安全に取り扱うためには、電子データを暗号化してICの内部で保存・管理すればよい。近年、IC内部で利用されている暗号処理方式は、高度に実装された数学的な暗号化アルゴリズムによってソフトウェア的には極めて堅牢に保護されている。しかし、いったんICとしてハードウェアに落とし込むと、暗号処理時に電源を流れる電流や電源から放射される電磁波を覗き見ることによって、暗号化に必要な秘密鍵等の致命的な情報漏洩の脅威にさらされる。このような非正規経路(サイドチャネル)の情報から内部状態を解析する攻撃はサイドチャネル攻撃と呼ばれ、90年代後半からサイバーセキュリティに対する大きな脅威とされてきた。このようなサイドチャネル攻撃に対する対抗手段として、多くの回路技術が提案されてきており、電源電流や放射電磁波をICを封入したパッケージ外部から解析する攻撃に対しては対処が可能となってきている。しかし、一方で近年では、サイドチャネル攻撃の手法が

高度化しており、パッケージを開封してICチップの表面に電磁プローブを近接させて内部からの放射電磁波を盗聴する近接電磁解析攻撃が2013年に報告され、これまで提案された全ての対策技術が無効化され、極めて深刻な脅威となっている。

今回、神戸大学と東北大学の研究グループは、この近接電磁解析攻撃をセキュリティIC側で検出するセンサを開発した(図1)。これまで電磁解析攻撃は、非侵襲(非破壊)のサイドチャネル攻撃とされており、従来はICからの電磁放射を抑制する対策が基本であった。今回の方式は、セキュリティICが攻撃そのものを検出する世界初のリアクティブな攻撃対策であり、攻撃検知さえできれば暗号処理を停止したり、暗号ICに偽の動作をさせる等によって情報漏洩を回避できる。センサの原理は、IC内部にコイル形状のアンテナをそなえ、攻撃のためのプローブの接近によって生じる電磁界の乱れを検出するものである。また、検出回路そのものはいたってシンプルで、コイルアンテナを備えた発振器を搭載し、プローブ攻撃による電磁界の乱れを発振周波数の変動として検知する。発振周波数の変化は、極めて小面積のカウンタで検出でき、コイルアンテナ以外の回路は全てデジタル回路で処理できるため、センサを追加搭載することの面積や消費電力ペナルティは、数%に抑えることができる。今回、さらにセキュリティ強度を高めるために、複数(今回は2つ)のコイル発振器を搭載する方式を考案した。1つのコイル発振器だけの方式(図2上図)では、プローブ攻撃による周波数変動を検出するために、チップ上に別途、周波数基準を搭載する必要がある。しかしながら、セキュリティICを動作させる外部入力のクロック信号は、周波数基準としてもともとチップ上に存在しているが、攻撃者によって周波数を自由に変化させることが可能なので、今回のセンサのための周波数基準には使用できない。また、IC内部で周波数基準を発生する回路も選択肢として考えられるが、精度の高い周波数基準発生回路は、大きな面積と消費電力のアナログ回路が必要となり、暗号ICの面積や電力が2倍以上になってしまう。そこで、複数のコイル発振器を搭載し、互いを周波数基準ととらえて、攻撃による周波数変動をコイル発振器間の相対的な周波数差として検出する(図2下図)。外部入力クロック信号もアナログの周波数基準発生回路も不要とした。このことにより、攻撃耐性を向上し、かつ面積・電力のペナルティの少ないセンサを実現できた。

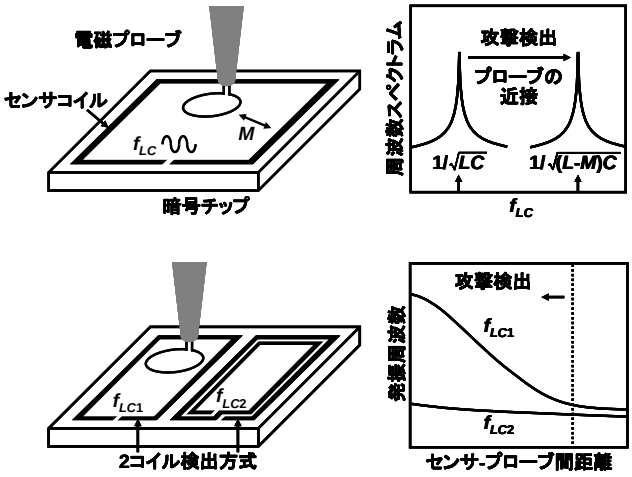

図 2 提案センサの検出動作原理

今回考案したセンサを実測により評価した。ICカードの分野で広く利用されている米国標準のAdvanced Encryption Standard (AES)暗号処理回路とセンサを搭載したデジタルセキュリティICを製造し、攻撃検知が可能となることを実証した。今回の研究成果は、権威ある集積回路の国際会議Symposium on VLSI Circuits 2014 (6/9-13にハワイにて開催)で発表予定である(発表番号はC16.4にて日本時間6/14午前4時20分より講演予定)。本研究は、科学研究費補助金によるものである。

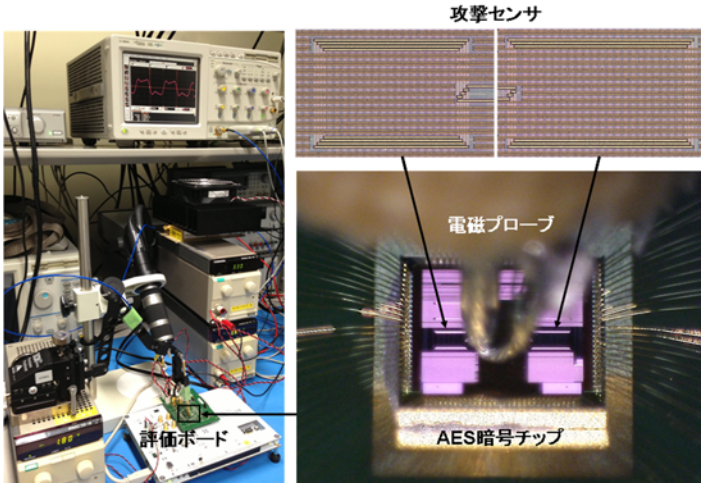

図 3 センサを搭載暗号チップと評価環境

三浦 典之[1], 藤本 大介[1], 田中 大智[1], 林 優一[2],
本間 尚文[2], 青木 孝文[2], 永田 真[1]
[1]神戸大学, [2]東北大学

本件の問い合わせは、神戸大学は永田教授のメールアドレスnagata@kobe-u.ac.jp
東北大学は本間准教授のメールアドレスhomma＠aoki.ecei.tohoku.ac.jp

以上、宜しくお願いします。