IoT 時代における機器認証を安全に実現するセキュリティ計算チップの開発（162308003）

Development of security chip that realizes device authentication safely in IoT era

研究代表者
野上保之　岡山大学
Yasuyuki Nogami　Okayama University

研究分担者
五百旗頭健吾†　籠谷裕人†　川西紀昭††
Kengo Iokibe†　Hiroto Kagotani†　Noriaki Kawanishi††
†岡山大学　††株式会社ゴフェルテック
†Okayama University　††GopherTec Inc.

研究期間　平成 28 年度～平成 30 年度

概要
IoT 時代においては、小型かつ計算リソースの限られたデバイスが、明示的な人の命令・操作を介すことなく、互いに認証し合いながら暗号化されたデータを通信する。そのデバイスの暗号計算中に、電界・磁界などの物理量を観測し、パスワードなど秘密情報を盗み取ろうとする攻撃（サイドチャネル攻撃）の脅威が指摘されている。本研究開発では、そのような暗号計算デバイス・機器認証処理を、具体的に楕円曲線暗号を用いた認証機能として設定し、そのサイドチャネル攻撃に対する安全性の評価手法を確立し、対策手法を開発する。

１．まえがき

IoT・AI 時代を迎えている。様々なデバイスが人間の手を介すことなく、AI やロボットが自律的に判断をして、ものを制御・駆動をする。このような社会において、悪意あるものによる操作の乗っ取りの脅威が指摘されている。IoT デバイスに対するセキュリティ技術の中で、とくにセンサなどデバイス・機器間での相互認証については、より高度な暗号技術が必要となる。具体的な問題点は、暗号計算の効率化と、サイドチャネル攻撃に対する安全性の確保である。ここでサイドチャネル攻撃とは、IC カードなどに搭載された暗号計算処理チップから、その暗号化や復号など計算処理中に発生する電磁ノイズなど物理的な情報を何らかの形で傍受し、そのノイズ情報からパスワードなど大切な秘密情報を抽出・解析しようと試みる極めて強力な解読攻撃である。サイドチャネル攻撃では、センサや制御ユニットに搭載されている暗号計算チップの暗号化・復号処理中に発生する電磁ノイズを傍受し、これを解析することによってパスワードなどを盗聴しようと試みる。この問題を本質的に解決するためには、暗号理論・数理、電磁ノイズなどの物理現象の精密な解析技術、その解析系・処理系を現実的かつ緻密に組み上げる技術が密に連携する研究開発が必要となる。

本研究開発では、岡山大学が保有する暗号実装技術およびサイドチャネル攻撃・対策技術と、岡山県内企業のゴフェルテック社が保有する高度な H/W 設計・開発技術を連携させ、「IoT 時代における機器認証を安全に実現するセキュリティ計算チップ」を開発する。具体的かつ緻密に実装・実験・評価するにあたり、サイドチャネル攻撃を回避するための楕円曲線暗号アルゴリズム（ソフト面での対策）と回路実装手法（ハード面での対策）を開発する。

２．研究開発内容及び成果

開発のコンセプトは、サイドチャネル情報としてパスワードなど秘密情報が漏えいする主たる要因が、暗号計算途上で発生する計算処理の不均一さであることに着目し、これを計算アルゴリズムおよび回路実装の両面から解消するものである。本研究開発では、以下のような研究内容（各フェーズ目標）を、それぞれ成果を得た。

フェーズ I（平成 28 年度）

既存の暗号計算 FPGA に対するサイドチャネル攻撃の安全性の評価：本研究開発のフェーズ I では、まず FPGA ボード上にこの楕円曲線暗号を SCA への耐性を簡便に評価できるよう細工をして搭載し、その SCA への安全性を評価する。

【成果】

SCA と FPGA 内部動作の関係を確認するための H/W の作成については、楕円曲線暗号を FPGA に実装した。暗号化アルゴリズムで使用される演算処理を分解して必要最小限な演算ブロックを設計し、それらをパイプライン構造として制御することで効率的かつ高速な暗号化処理を実現した。また、SCA に対する安全性の評価については、上記で試作した H/W に対するサイドチャネル攻撃について、AES 暗号回路を試作 H/W に実装し、安全性評価に必要なサイドチャネル波形を試作 H/W 上で取得できることを確認した。

フェーズ II（平成 29 年度）

SCA に対して安全な暗号計算アルゴリズムの開発とその安全性の評価：暗号計算中の電磁ノイズなどサイドチャネル情報から秘密情報が漏えいする原因の一つの側面は、その暗号計算アルゴリズム中の計算が、パスワードなど秘密情報に基づいた計算処理を行うことにある。これを回避するためのアルゴリズムサイドの対策（ソフト面での対策）として、この研究フェーズではアルゴリズム中の計算処理の均一化（バイナリデータに応じて行われる処理の均一化）を図る。

【成果】

暗号アルゴリズムの開発について、SW 的・アルゴリズム的な均一化として、広く知られるモンゴメリラダー法をベースとしながら、楕円曲線暗号における楕円加算・2 倍算の計算処理について、その均一的な計算処理を実現できる

ように工夫を行った。また、SCA と FPGA 内部動作の関係を確認するための H/W の作成として、乗算器の削減を行った FPGA 回路を元に SCA の耐性を高める二つの試みを図に示す FPGA に実装した。一つ目は、使用する鍵が 0 と 1 の時での処理の統一化である。一般的には鍵によって異なる処理が行われるが、算出値を得るまでの計算順序を工夫することにより、最終的な算出値の取込以外の部分を共通化することが出来た。SCA に対する安全性の評価と問題点の検討として、FPGA 実装された楕円曲線暗号のサイドチャネル攻撃耐性評価について検討を行った。まず、昨年度の予備検討で構築したサイドチャネル波形取得環境を使用し、楕円曲線暗号回路より漏洩する波形の観測を試みた。その結果、近傍磁界プローブにより暗号処理と同期したサイドチャネルを取得した。一方、受動及び差動電圧プローブではそのような波形は取得できず、暗号処理内容と関係のある振幅変化を確認できなかった。次に、受動プローブや差動プローブより高精度なパワーレールプローブによりサイドチャネル波形を観測した。暗号処理に起因する電圧変動を確認でき、パワーレールプローブによりサイドチャネル波形を高精度に測定できている。

フェーズ II（平成 30 年度）

暗号計算の H/W 実装における SCA への対策技術の開発と安全性の評価 : 本フェーズでは、意図的なデータ改ざんの可能性を探ることに加え、それに対抗する物理的な均一化手法を開発する。そして、実際に効果を示すかを検証するための解析システムを作成し、実際に SCA に対する安全性の評価を実施する。

【成果】

選択暗号文攻撃という攻撃の脅威について検討した。その攻撃に用いることができる選択暗号文について、2 つの成果を得ることに成功している。まず、このような IoT デバイス向けに持ちられる楕円曲線は、Curve25519 と呼ばれる極めて実装効率の良いものであり、これは様々な標準化機関で推奨されてるものである。その楕円曲線暗号に対して、本研究では 2 つの選択暗号文攻撃の脅威を示すことができた。一つ目は、位数 4（4 回で巡回する）を用いた攻撃であり、その短い巡回性およびその計算途中で現れるゼロ乗算を分析する SCA 攻撃になる。もう一つは、位数 8（8 回で巡回する）を用いた攻撃であり、位数 4 と比べるとさらに難しい SCA 攻撃になるが、現代では AI の悪用も考えられ、極めて現実的な選択暗号文攻撃となってしまった。

その対策試作機の設計・製作については、汎用品として設計されている H/W を使用しており、もとよりノイズの測定や FPGA の設計においてサイドチャネル攻撃対策研究用として使い易いものではなかった。そこで、機能をコンパクトに収め、研究開発用として評価を行い易い H/W を設計・製作した。具体的には、楕円曲線暗号では、計算式を分配則により式展開することで、暗号鍵の違いによって発生するノイズの差異が少ない方法を実現した（岡山大学）。具体的な FPGA 実装については、連携企業であるゴフェルテックの方で実施した。そして、この対策効果を確認するため、対策を施した FPGA と対策を施さない FPGA を共に開発して効果を確認した結果、スケジュール最適化と重畳による対策が極めて強力な対策であることを確認でき、十分な SCA 攻撃対策を実現できていることが分かった。

図：開発に用いた FPGA ボード

３．今後の研究開発成果の展開及び波及効果創出への取組

まず本研究では、対策の開発に Intel 社製の FPGA を使用したが、Xilinx 社製の FPGA でも同様の効果があるのかを検証することで対策の汎用性を確認した。H/W による差異が発生し易い AES 暗号に対する対策を、Xilinx 社製 FPGA を搭載した H/W に実装し、Intel 社製と同様の効果があることを確認した。これにより、開発した対策が汎用的に使用可能であることが確認できた。また SCA に対する脆弱性の啓発と教育支援という観点で、製作した H/W を用いて SCA の脅威と対策の重要性を簡単に体感できる環境を整えた。ICT 人材育成・社会人教育に向けたより簡易（安価）にサイドチャネル攻撃の脅威を理解できる環境を構築し、人材育成はもとより、安全・安心な製品を開発するため実験ツールとしても活用してもらいたい。

４．むすび

本研究の成果は、安全・安心なセキュリティチップを、マイコンや FPGA といった情報通信の末端のデバイスから確実なものとするための研究開発であり、昨今とくに重要となるサイバーフィジカルセキュリティの「信頼の創出」を担えるものである。本成果および本成果物（FPGA ボード）を広く社会に活用いただけるよう、還元・社会啓蒙したいと考えている。

【誌上発表リスト】

[1] Md. Al-amin Khandaker, Yasuyuki Nogami, “An Improvement of Scalar Multiplication by Skew Frobenius Map with Multi-Scalar Multiplication for KSS Curve”, IEICE Trans., vol. E100-A, no. 9, pp. 1838-1845, Sept. 2017.

[2] Y. Nanjo, Md. Al-Amin Khandaker, M. Shirase, T. Kusaka, and Y. Nogami, ” Efficient Ate-Based Pairing over the Attractive Classes of BN Curves,” The 19th World Conference on Information Security Applications (WISA2018), 2018.

[3] 堀之内信輔、五百旗頭健吾、籠谷裕人、渡辺哲史、豊田啓孝、”クロックグリッチ掃引による AES 回路の故障利用攻撃耐性判定法” 2017 年暗号と情報セキュリティシンポジウム（那覇）、(2017 年 1 月 25 日)

【本研究開発課題を掲載したウェブページ】

http://isec.ec.okayama-u.ac.jp/scope-regional-ict-promotion-2016-2018-jp/