2022 年 1 月 5 日

学位論文公聴会のお知らせ

電気通信大学大学院情報理工学研究科情報・ネットワーク工学専攻専攻長
肖鳳超

令和 3 年度(3 月期)学位論文公聴会を下記の通り開催します。多数の皆様のご来聴をお待ちいたします。

記

論文申請者 Ba-Anh Dao

論文題目 Research on hardware-based hiding countermeasures against Power Analysis Attacks
（電力解析攻撃に対するハードウェアベースの隠蔽対策に関する研究）

日時 2022 年 1 月 28 日（金）午前 10 時～

場所 電気通信大学 西 5 号館 109 号室（対面）

論文概要：

近年、電力解析攻撃は、暗号デバイスのセキュリティに対する深刻な脅威として浮上している。これらの攻撃は、対応する暗号アルゴリズムの理論的弱点の分析に焦点を合わせるのではなく、物理的な実装によって引き起こされる意図しないデバイス内の情報のリークを利用する、サイドチャネル攻撃の一種に分類される。ここでいう意図しないリークとは、暗号デバイスが機密性の高い中間値を処理する際の、電力消費または電磁放射である。このリーク情報を解析することで、攻撃者は対応する暗号アルゴリズムの秘密鍵を取得する。

電力解析攻撃には多くの対策が提案されているが、マスキング対策と隠蔽対策の 2 つのグループに分類できる。マスキング対策は、暗号処理中の中間値を予測されないようにランダムにマスクする。一方、隠蔽対策は、中間値のリーク情報を低減するため、暗号デバイスの消費電力特性を変更する。マスキング対策は多くの場合、暗号処理が複雑となり、計算量が大幅に増加するため、スループット低下や実装コストの増加を引き起こす。さらに、ディープラーニングを利用した最先端の電力解析攻撃では、使用されているマスクに関する情報がなくてもマスキング対策を破れる可能性が示されている。

一方、隠蔽対策は暗号アルゴリズムの変更が不要ないため、一つのデバイスに複数のアルゴリズムを実装する際に、すべてに同様に適用することができる。また、マスキング対策よりもディープラーニングベースの電力解析攻撃への耐性が高いことも実験的に証明されている。概して、隠蔽対策はマスキング対策と比較して、ハードウェアコストや速度性能等のパフォーマンスに優れているが、実装のオーバーヘッドは依然として少なくない。

本論文は、電力解析攻撃への耐性が大きく実装が容易、かつ汎用性を有した二つの新しいハードウェアベースの隠蔽対策を提案している。第一の対策は、デバイス速度と消費電力の動的制御に広く用いられる SOTB（Silicon On Thin Buried Oxide）製造技術のバックゲートバイアス技術を利用するる。これにより特殊な回路を付加することなく、消費電力をランダム化することができる。第二の対策は、暗号デバイスの動作周波数を動的に変更するランダム動的周波数スケーリングである。提案手法を施した暗号デバイスを FPGA と ASIC で実装し、電力解析攻撃実験を行った。その結果により、提案手法は、隠蔽対策よりも少ないハードウェアリソースで、高い耐性を有することが示された。

提案対策適用する場合としない場合で、FPGA と ASIC の両方に実装された実際の暗号化デバイスに対して電力解析攻撃による評価を行った。最先端の Vector Leakage Assessment（TVLA リークテスト）、Correlation Power Analysis（CPA）攻撃や Deep Learning-based サイドチャネル攻撃（DL-SCA）による実験結果から、提案対策は特にハードウェアリソースの使用率の点で、他の隠蔽対策よりも優れていることが明らかとなった。

審査委員： 範 公可（主査）、石橋 孝一郎、佐藤 証、崎山 一男、菅原 健

2022 年 1 月 5 日

学位論文公聴会のお知らせ

電気通信大学大学院情報理工学研究科情報・ネットワーク工学専攻専攻長
肖鳳超

令和 3 年度(3 月期)学位論文公聴会を下記の通り開催します。多数の皆様のご来聴をお待ちいたします。

記

論文申請者 Trong-Thuc Hoang

論文題目 Trusted Execution Environment with Silicon Level Root-of-Trust based on RISC-V Computer System
（RISC-V コンピュータシステムに基づくシリコンレベルの信頼ルートを有する信頼できる実行環境）

日時　　2022 年 1 月 28 日（金）午後 13 時 30 分～

場所　　電気通信大学　西 5 号館 109 号室（対面）

論文概要：

信頼できる実行環境 Trusted Execution Environment（TEE）は、認証されていないプログラム等の実行を防ぐための安全な環境を提供することを目的としている。 TEE の強度は、一連のハッシュ、署名、および検証によって作成された信頼の鎖 Chain-of-Trust（CoT）に依存する。 CoT の開始点は、Root-of-Trust（RoT）と呼ばれる。今日、RISC-V のオープンソースの命令セットアーキテクチャ Instruction Set Architecture（ISA）は、セキュリティの目的でコンピュータシステムを再検討する機会を提供している。 RISC-V を使用することでシリコンレベルまで前述のような安全なハードウェア RoT を作成できる。この RoT において、理論的には、ルートキーをハッキングすることは、チップ製造プロセスに干渉することを意味する。

本論文の目的は、安全なハードウェア RoT を備えた RISC-V ベースの TEE コンピュータシステムを提案する。提案した SoC は Linux で起動可能であり、TEE の構築に必要な複数のハードウェア暗号化アクセラレータが含まれている。本 SoC の目標は、代替ハードウェアを使用して TEE を完全に起動し、ブートローダーソフトウェアから暗号化機能を保護することでである。提案アーキテクチャは、Linux 対応プロセッサと 32 ビットの隠し MCU を組み合わせた複数の種類のプロセッサからなるヘテロジニアス・システム・アーキテクチャである。 32 ビット MCU は TEE 側から分離され、ルートキーなどの機密データ、および Zero Stage Boot Loader（ZSBL）やキー生成プログラムなどの機密動作を処理する。分離されたサブシステム内に RoT が実装されているため、起動後に TEE 側から RoT にアクセスすることはできなくなる。さらに、MCU がブートシーケンスを実行するため、キーの生成は柔軟なアルゴリズムを使用するため、任意のセキュリティスキームに合わせた更新が可能となる。

本論文は、安全性の高いコンピュータシステムを提案することだけでなく、将来使用するためのフレームワークにも注目する。提案フレームワークは使いやすく、長期的に将来の脅威に適応するための柔軟性を有している。 RISC-V アーキテクチャの柔軟性により、ユーザーはセキュリティ機能をオンまたはオフにできるため、コストとセキュリティの懸念のバランスをとることが可能となる。また、フレームワークをオープンソースプロジェクトとして維持することにより、本提案は、今後コンピュータセキュリティ開発者にとって強力な開発ツールになると期待できる。

審査委員： 範　公可 (主査)、石橋　孝一郎、佐藤　証、崎山 一男、菅原　健