2023 年 01 月 12 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
中山 泰一

令和 4 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 Ronaldo Enrique Serrano Peña

論文題目 Research on Hardware Primitives for Root-of-Trust in Secure Systems
（セキュアシステムにおけるルートオブトラストのためのハードウェアの基本要素に関する研究）

日時 2023 年 1 月 19 日（木）午後 13 時 30 分～

場所 電気通信大学 西 2 号館 Ｂ１０１ 号室

論文概要：

本論文では、安全なシステムの RoT で使用されるプリミティブ群を提案する。特定用途向け集積回路（ASIC）およびフィールド プログラマブル ゲート アレイ（FPGA）の周波数崩壊に基づいて TRNG を実装するための新しいプリミティブ群が提案され、物理現象から抽出されたエントロピーが改善される。さらに、プロセス、電圧、および温度（PVT）の変動に対する耐性を提供し、健全なエントロピー ソースを保証する。さらに、新しい統合 NVRAM-TRNG-PUF は、標準 CMOS テクノロジのシングル フローティング ポリ（SFP）を用い、センス アンプの準安定性を実施する。 NVRAM の SFG を使用して TRNG 応答を調整し、メタスタビリティに基づく TRNG で提示される低エントロピー抽出を軽減する。また、OTP-PUF メモリは、アンチヒューズ ビット セルを使用して、標準的な CMOS テクノロジでマスクを追加することなく提供できる。最後に、TLS 1.3 と互換性のある ChaCha20-Poly AEAD ハードウェア構造が提示され、ハードウェア効率の点で AES に基づく暗号とは異なるソリューションが提供される。さらに、新しい AEAD 構造は、ラッチを用いた FPGA 実装で生じるミスマッチを利用する PUF と統合され、AEAD 実装でのワンタイム キー生成に新しい機能を提供する。

本論文で提案した新しいセキュア プリミティブは、それぞれのアプリケーションの品質を向上させるために実装した。

連絡先：範 公可（phamck@uec.ac.jp）

2023 年 01 月 12 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
中山 泰一

令和 4 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 Le Anh-Tien

論文題目 Research of RISC-V Out-of-order Processor Cache-Based Side-Channel attacks
-Systematic Analysis, Security Models, and Countermeasures-
（RISC-V アウト・オブ・オーダープロセッサのキャッシュに基づくサイドチャネル攻撃に関する研究 -体系的な分析、セキュリティ モデル、および対策-）

日時 2023 年 1 月 20 日（金）午前 10 時 00 分～

場所 電気通信大学 西 2 号館 Ｂ１０１ 号室

論文概要：

本研究では一連の実質的なテストを実施し、Spectre に対する RISC-V プロセッサの脆弱性を証明し、サイドチャネル攻撃を防止するための方法を提案する。
まず、RISC-V プロセッサを用いて Spectre などのキャッシュ サイドチャネル攻撃をリアルタイムで検出するシステムを提案する。キャッシュ サイドチャネルは通常、劇的に変更されたキャッシュ消費パターンを生成するため、提案した多層パーセプトロン ネットワークは、シミュレーション モデルでのパフォーマンスへの影響を最小限に抑えながら、95% を超える精度で攻撃イベントを検出する可能となった。
また、RISC-V アウト・オブ・オーダー プロセッサ アーキテクチャには、投機的実行後のキャッシュからのメモリ リークを回避するために、提案する安全なミス ステータス保持レジスタを含むようにした。実験結果によると、提案したアーキテクチャは、適度なパフォーマンス オーバーヘッドとハードウェア リソースの使用をトレードオフしながら、Spectre 攻撃をよりよく保護することが可能となった。

連絡先：範 公可（phamck@uec.ac.jp）