



令和 4 年 4 月 13 日

報道機関 各位

東北大学 電気通信研究所

ハードウェアに挿入された不正な機能を高速かつ 漏れなく検知する技術を開発

【発表のポイント】

- 半導体集積回路（IC）チップの設計データに挿入された不正な機能（ハードウェアトロイ）を高速かつ漏れなく検知する新技術を開発。
- 数学的な等価性判定の技法を駆使することで、これまで困難だった大規模で複雑な IC 設計データにも適用可能。
- 特にセキュリティ向けハードウェア・システム製品の信頼性・安全性向上に貢献。

【概要】

近年、インターネットに接続する身近な機器が設計・製造段階で改ざんされ、システム使用開始後に不正な振る舞いを起こす「ハードウェアトロイ Hardware Trojan: HT)」の脅威が指摘されています。東北大学電気通信研究所は、半導体集積回路(IC)チップの設計データに含まれる HT を高速かつ漏れなく検知する新技術を開発しました。今回開発した技術では、設計仕様と設計データの等価性をグレブナー基底と呼ばれる数学的な表現を用いて検証することで、機能改変を伴うあらゆる HT の検知が可能です。また、これまで難しかった大規模で複雑な回路データにも適用できます。さらには、秘密情報保護やプライバシー保護に必要な暗号回路等のセキュリティ向け IC の HT 検知に効果を発揮することも実証しました。今回開発した技術は、IC チップおよびそれを搭載した製品の信頼性・安全性向上に大きく貢献することが期待されます。

この成果は、米国電気電子学会 (IEEE) の主要国際学術誌 IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems の 2022 年 3 月号に掲載されました。

【問い合わせ先】

東北大学 電気通信研究所

担当: 教授 本間尚文, 助教 上野嶺

電話: 022-217-5506

E-mail: contact.ecsislab@grp.tohoku.ac.jp



【開発の社会的背景】

モノのインターネット (Internet of Things: IoT) に代表される様々なデバイスがインターネットを介して接続される社会の到来に伴って、ネットワークに接続する身近な機器が設計・製造段階で改ざんされ、システム運用開始後に不正な振る舞いを起こす「ハードウェアトロイ (Hardware Trojan: HT)」が挿入される危険性が指摘されています。例えば、暗号回路等のセキュリティ向け回路に HT が挿入されると機密情報の漏洩に繋がる恐れがあります。また、人工知能の IC チップに HT が挿入されると、それを利用するシステムにおいては大変な脅威となります。一方、今日の半導体集積回路 (Integrated Circuit: IC) チップおよびそれを搭載したハードウェア・システムの開発では、IC 設計支援ツールを提供するツールベンダや、様々な IP (Intellectual Property) コア*を提供する IP ベンダ、設計された回路の配置配線情報に合わせて製造を行うファウンドリ、IC と電子部品をプリント基板上に実装する電子システム実装メーカーなど様々な企業が国を越えて関わるのが一般的です。以上の背景から、こうした設計・製造プロセスにおいて、秘密裏に HT が IC 内部に挿入されていないことをいかに保証するかが世界的な課題となっています。

【開発の経緯】

東北大学 電気通信研究所 環境調和型セキュア情報システム研究室(本間尚文教授, 上野嶺助教, 伊東燦日本学術振興会特別研究員)の研究グループは、今後 IoT に進展に伴い社会基盤の一部として需要がますます高まると予想される IC チップを安心・安全に利活用するためのシステム設計とその検証技術の確立を目指し、IC チップの設計時に HT を完全に検知・排除する技術の研究開発を行ってきました。

【発見・開発した内容】

今回開発した HT 検知技術は、IC チップの設計データの機能（入出力関係）が、設計仕様通りに過不足なく正しいことを数学的に検証する技術です。本技術を用いることで、微小な HT であっても 1 ビットでも設計仕様と異なれば漏れなく検知することができます。

通常、IC の機能をテストする場合、様々な入力を与えて仕様通りに出力されるかを確認します。しかし、回路規模が大きくなり、仮に100 桁の入力パターンがあった場合、すべてを入力して確認することは現実的ではありません。そこで、いくつかの入力パターンにしぼってテストが行われます。しかし、HT が挿入される場合、極めて稀な入力パターン時にのみ動き出すよう設計される可能性が高く、従来のテストでは HT に対する安全性を十分に保証できませんでした。これに対して、今回の技術は、設計仕様と回路構造(IC データ)をそれぞれグレブナー基底**と呼ばれる数式による表現に変換し、その等価性判定により HT が含まれないことを数学的に保証します。これにより、全ての入力パターンを入力・検証したのと同じ保証を与えることができます。

図1は開発した技術の概要です。特に、この数学的表現(グレブナー基底)による等価性判定を高速に行う手法を新たに考案することで、大規模で実用的な IC 設計データであっても適用できるようになりました。また、今回の技術では、もし HT(やバグ)が含まれる場合、その動作条件まで特定できます。この度、暗号技術が搭載されたセキュリティ向け IC チップ設計に同技術が有効であり、これまで難しかった複雑なセキュリティ向け IC 設計データの HT 検知に適用できることを世界で初めて明らかにしました(図 2)。

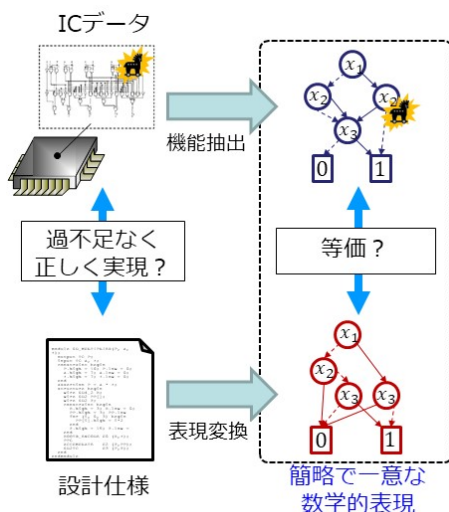


図 1：開発した技術の概要：設計仕様と IC データの機能をそれぞれ数学的に表現して等価性を判定。

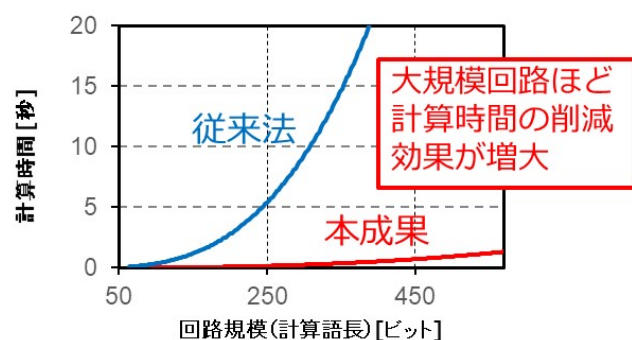


図 2：開発した技術の性能（暗号処理回路への適用例）。大規模な回路ほど計算時間の削減効果が増大。

なお、本成果は、米国電気電子学会 (IEEE) の主要な国際学術誌「IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems」の 2022 年 3 月号に掲載されました。

【今後の予定】

今回開発した技術は、IC チップ設計の上流にあたる機能設計の工程で HT やバグが一切含まれていないことを数学的に完全に保証する技術です。今後は、より大規模かつ多様な IC への適用および IC を搭載する製品の設計から製造・組立までの一貫した HT 排除を達成する技術の実現に向けて、更なる研究開発をすすめます。今後のスマート社会の恩恵を安心・安全に享受するためには IC チップ内に挿入される HT の脅威を排除・抑止する技術の確立が不可欠であり、その発展に本研究を通して貢献することを目指しています。

【発表論文】

著者: Akira Ito, Rei Ueno, and Naofumi Homma

論文タイトル: Efficient Formal Verification of Galois-Field Arithmetic Circuits Using ZDD Representation of Boolean Polynomials

発表論文誌: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

発行年月: 2022 年 3 月号

【用語解説】

*IP (Intellectual Property) コア: 半導体集積回路を設計・構成するための部分回路情報。特定の機能単位で提供されることが多い。大規模な回路の場合、あらかじめ設計された IP コアを組み合わせる設計が多い。

**グレブナー基底: 複数の多項式で一つの多項式を簡約 (割り算) する際に、その割り算の順序に依らず最終的に一意の数式が得られるような多項式の集合。コンピュータによる連立方程式の求解に利用される。