受賞者氏名	尾花　賢	
所属	情報科学部コンピュータ科学科	
受賞年月日	2025 年 6 月	
国内・国外	国外	
授与機関等名称	NASA Formal Method Symposium	
受賞名	Honorable Mention	
受賞(研究)内容詳細	ロケットと基地局間、あるいは人工衛星同士の通信では、商業的価値の高い情報や飛行の安全性に関わる制御コマンドがやり取りされるため、通信の秘匿化や偽造・改ざんを防止する暗号技術が不可欠です。法政大学、インターステラテクノロジズ、情報通信研究機構（NICT）の 3 者は、産官学連携の共同研究を通じて宇宙機向け暗号通信技術の開発に取り組みました。日本で初めて宇宙空間に到達した民間ロケット「MOMO」に本技術を搭載し、共同研究が終了した 2025 年度までにその有効性を実証してきました。 本研究で開発した暗号技術の特長は、「情報理論的安全性」を保証する点にあります。情報理論的安全性とは、攻撃者が無限の計算リソースを持っている状況であっても解読や偽造・改ざんができないことを保証する、理論上最高峰の安全性です。この安全性の実現には膨大な量の鍵（送受信者間で共有する秘密情報）が必要となるため実用化には高い障壁がありましたが、ロケットや人工衛星のように通信のライフタイム（運用期間）が比較的短い機器であれば実際に利用可能であることを示した点も大きな成果です。 今回受賞対象となった研究は、情報理論的安全性を保証する暗号技術をハードウェア化する際、設計通りに動作するかを検証する手法に関するものです。情報理論的安全性を備えた暗号技術では、「有限体」と呼ばれる複雑な代数構造の上での乗算を利用します。特に回路規模をコンパクトに抑えるための乗算処理は構造が極めて複雑であり、ハードウェアが正しく動作しているかを検証することが非常に困難でした。そのため従来の研究では、8 ビット程度の非常に小さな有限体でしか検証が行われていませんでした。 これに対し本研究では、従来のスケールを大幅に上回る「128 ビット」の有限体上における乗算回路の正当性検証に成功しました。本来、これほど大きなサイズの乗算回路を全数検査するには 2^{256} 通りの入力を調べる必要があります。これは 1 秒間に 1 京（10^{16}）通りの検査を行っても約 37 恒河沙（ごうがしゃ）年（37×10^{52} 年）を要する途方もない作業です。しかし本研究では、複雑な乗算回路の正当性検証をより単純な構造の回路検証へと帰着させる手法を開発し、さらに論理学ベースの検証手法を応用することで、完全な検証をわずか 17 時間で実現しました。今回開発した手法は、情報理論的安全性を有する暗号のハードウェア検証にとどまらず、IC カードなどに用いられる「楕円曲線暗号」や、スマートフォンの無線通信に用いられる「誤り訂正符号（通信途中で生じるデータの誤りを訂正する技術）」など、幅広い技術におけるハードウェア検証手法としての応用が期待されています。	