財団法人セコム科学技術振興財団助成研究
（平成 22 年度～平成 25 年度）

LSI テスト設計技術に起因する IC カードの脆弱性の解明と対策手法の構築

平成 27 年 9 月

早稲田大学理工学術院・教授
戸川 望

全体要旨

本研究では，LSI テスト設計技術の 1 つスキャンパス設計に注目し，これを悪用することで IC カード内部に含まれる暗号回路－主に銀行用 IC カードで利用される公開鍵暗号回路，主に交通機関で利用される共通鍵暗号回路の双方－に含まれる「秘密鍵」を解読できることを実証する．

まず FPGA プロトタイプシステム上で AES 暗号回路をスキャン脆弱性の実証する.加えて，公開鍵暗号方式の 1 つとして RSA 暗号回路（Rivest-Sharmir-Adelman 暗号回路）を取り上げ，これについても LSI テスト設計技術に起因するスキャン脆弱性があることを解明し，FPGA プロトタイプシステム上で RSA 暗号回路のスキャン脆弱性を実証する．つまり第一のゴールとして，FPGA プロトタイプシステム上において，共通鍵暗号回路ならびに公開鍵暗号回路の双方について，LSI テスト設計技術に起因するスキャン脆弱性が存在することを実証する．

続いてここまでの実証結果を踏まえ，まず共通鍵暗号方式の実 IC チップを試作し，実 IC チップ上で LSI テスト設計技術に起因するスキャン脆弱性があることを解明する．さらにこの結果を用いて共通鍵暗号方式の IC チップに対し，これを理論上，防御するしくみを考案し，防御手法の有効性を FPGA プロトタイプシステム上で実証する．つまり第二のゴールとして，実 IC チップ上の共通鍵暗号回路について，LSI テスト設計技術に起因するスキャン脆弱性が存在することを実証すること，ならびに，これを理論上，防御する手法を考案する．

さらに，公開鍵暗号方式の実 IC チップを試作し，実 IC チップ上で LSI テスト設計技術に起因するスキャン脆弱性があることを解明する．この結果を用いて公開鍵暗号方式の IC チップに対し，これを理論上，防御するしくみを考案し，防御手法の有効性を FPGA プロトタイプシステム上で実証する．つまり第三のゴールとして，実 IC チップ上の公開鍵暗号回路について，LSI テスト設計技術に起因するスキャン脆弱性が存在することを実証すること，ならびに，これを理論上，防御する手法を考案する．

最後に，ここまでの実証結果を踏まえ，防御対策を施した共通鍵暗号方式ならびに公開鍵暗号方式の実 IC チップを試作し，実 IC チップ上で LSI テスト設計技術に起因するスキャン脆弱性が解消されることを実証する．つまり第四のゴールとして，これらの目的を達成し，実 IC チップ上で共通鍵暗号回路ならびに公開鍵暗号回路について，LSI テスト設計技術に起因するスキャン脆弱性が解消されることを実証する．

研究期間を通した技術開発の結果，IC カードに内在する LSI テスト設計技術に起因する IC カードのスキャン脆弱性が防御できることを目指す．