研究課題別中間評価結果

1． 研究課題名： 耐タンパディペンダブル VLSI システムの開発・評価

2． 研究代表者： 藤野 毅（立命館大学 教授）

3． 研究概要

交通・流通系で急速に普及した非接触 IC カードなどに見られるように、LSI を利用した金銭情報や個人情報を保管するシステムが社会基盤として広く普及している。このような IC カード上の LSI（以降セキュリティ LSI と記す）に保管されている機密情報や個人情報が窃取される、あるいは LSI 複製によるカード偽造などが発生すると、大きな社会的混乱を引き起こす可能性があり、このような攻撃に対して、情報の防御システムを LSI 上で構成する研究が必要とされている。

セキュリティ LSI への主な物理的解析・攻撃手法としては、動作時の消費電力や電磁波などの漏えい情報を解析するサイドチャネル攻撃、LSI にスパイクノイズ等を印加して誤動作を誘起することで機密情報を窃取するフォールト攻撃、パッケージを開封し、内部を直接観測・改造する侵襲攻撃などが挙げられる。さらに、機密情報の窃取にとどまらず、回路パターンを解析複製した偽造 LSI の製造と悪用など、さまざまな脅威が存在する。耐タンパ性を指向したディペンダブル VLSI システム実現のためにはこれらの攻撃への対策が不可欠である。

本研究では、機密情報の観点でディペンダブルなセキュリティ LSI すなわち、上記 3 種の物理攻撃と偽造 LSI の製造に対する防御方法を備えた、耐タンパ LSI を実現するための技術開発を行い、以下3つの成果物を得ることを目標とする。

（1）耐タンパ性 LSI 設計プラットフォーム
（2）耐タンパ性能評価プラットフォーム
（3）偽造 LSI を識別する PUF を用いたセキュリティシステム

4． 中間評価結果

4－1. 研究の進捗状況及び研究成果の現状

（課題、目標の設定）

セキュリティシステムに用いる VLSI の耐タンパ性を高めることは、重要な社会的要請であり、本テーマは正面からその課題に対応している。本研究では、既知の攻撃手口への耐性を高めた回路の提案、回路設計・検証のツール、耐タンパ性評価ツール、PUF とその応用を研究している。耐タンパ性には定量的目標を掲げ、産学官の連携のもと研究を実施している。これまで日本では取り組みが手薄であったテーマであり、本研究には技術面でも、人材育成面でも貢献が期待される。耐タンパ性を高める努力と攻撃技術とは常にいたちごっことなり、目標は常に先に移動する。研究進捗に合わせて実用的な成果を出しつつも、課題や技術の新展開に備える取り組みが要求される。

（成果状況）

耐タンパ回路として当初取り上げた方式（「ドミノ RSL 回路」）は、試作・テストの結果電力解析によるサイドチャネル攻撃への脆弱性が明らかとなった。そこで 2 番目の回路方式（「2 線 RSL メモリ」）を試み、消費電力によるサイドチャネル攻撃への耐性を大幅に改善した。しかし、続いて漏洩電磁波によるサイドチャネル攻撃への耐性を調べたところ、この攻撃は加工寸法の微細化とともに効果的となることを見出し、第 2 の回路方式もこの攻撃には脆弱であることが判った。そこで回路方式にさらなる改良を加え耐性強化をはかった。設計段階で耐タンパ性を検証する CAD システムの開発も進め、電力解析につき多重解析による脆弱性評価手法を開発した。また、

VLSIの安全性（サイドチャネル攻撃耐性、PUFの攻撃耐性）評価につき国際標準化、電磁波解析の環境整備を行っている。

（外部との連携）

チームの一員である三菱電機が、産業用途の実適用に通じるよいチャネルとなるよう願っている。LSI 設計受託会社とも対話しているので、そのチャネルを通じて商業用途における実用化も進展するよう期待している。産総研は評価方法につきひろく外部と接触している。

4－2. 今後の研究に向けて

この 1 年、研究にスピードが出てきた感がある。研究の優位性を高め、他から世界的に認知されるように努力していただきたい。耐タンパ回路プラットフォームについては、試作して性能をテストするサイクルを回すのもよいが、むしろ豊富な回路アイデアをパイプライン化、複線化することが望ましい。有望な回路方式につき特許権利化を図られたい。攻撃法については組織的な検討が必要ではないか。PUF はすでに商用化している企業もある。研究の優位性、完成度を高め、実用化まで進めていただきたい。

他機関の開発成果と優位性、特に耐タンパ強度を比較する時、同じ尺度で比較ができることは基本前提になる。国際標準化に向けての努力に期待する。

4－3. 総合的評価

本テーマは継続推進が適当である。