研究課題別事後評価結果

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．　研究代表者名及び主たる共同研究者名：

研究代表者

藤野　毅（立命館大学理工学部　教授）

主たる共同研究者

堀　洋平（(独)産業技術総合研究所　主任研究員）

鈴木　大輔（三菱電機株式会社　情報技術総合研究所　情報セキュリティ技術部　主席研究員）

吉川　雅弥（名城大学理工学部　教授）

3．　事後評価結果

○評点

A+　期待を超える十分な成果が得られている

○総合評価コメント

3－1．研究の達成状況及び得られた研究成果

（課題、目標の設定）

システムのセキュリティ、耐タンパ性を確保することは安全・安心への社会的に重要な要請である。本テーマでは既知の攻撃方法に対し耐性を高めた回路、攻撃への脆弱性評価（設計時、実装後）技術、正当性認定に使用する PUF と、重要な、具体的課題を挙げて取り組んでいる。国費での研究として適切なテーマである。

それぞれの研究項目に定量的な目標を掲げており、妥当な目標設定となっている。また、悪意の攻撃技術や攻撃対象は時間とともに進歩するため、セキュリティの研究課題は、ムービング・ターゲットとなる。それに対応する意味でも、本チームは柔軟に対応している。

（成果状況）

LSI の攻撃手法、脆弱性評価、ならびに攻撃耐性を強化する回路技術、設計時に耐性を評価する技術、PUF 技術などについて、実践的で多角的な研究から、たくさんの重要な知見が得られている。まず、模擬攻撃/攻撃耐性評価システム（評価 LSI、評価ボード、フォールト導入/フォールト解析技術含む）、タンパ耐性設計評価技術などが各グループの連携のもと実施され優れた研究プラットフォームを形成しつつある。

共通鍵暗号（AES）用耐タンパ回路方式として当初取り上げたドミノRS回路は実験の結果判明したその脆弱性から断念し、新しく MDR-ROM を用いた耐タンパ暗号回路と PUF との統合アーキテクチャを提案し、SASEBO ボードを用いて耐タンパ性が高いことを示すことができた。PUF 技術について他機関発案の方式改良に加え独自考案の方式をいくつか実装した。PUF を固有 ID として認証鍵の複製を防止する技術は車載用としてデモした。Glitch PUF については商用装置実装への見通しを得た。

暗号化回路、評価方法、PUF につき、それぞれ顕著に研究が進み、新しい展望が得られている。ET2014 の会場でも、車載システムへの攻撃が起こりうること、暗号化により耐性が強化できることをわかりやすくデモしていたが、来場者から大きな反響があった。大手車載システムメーカとの連携が始まったとのことであり喜ばしい。

３－２. 研究成果の科学技術や社会へのインパクト、戦略目標への貢献

この分野の日本の技術水準は、高度の情報活動が行われる諸外国（米、中、英、ロ）に比較して、攻撃の研究、防御の研究とも一般には遅れている。本研究は、そうした状況を挽回する上で大きな効果を挙げ、世界水準に近づけた。産総研の SASEBO は公開されている評価技術として国際的に高く評価されており、本研究においてもさらにその技術水準を向上させることができた。

本研究の成果を車載システム適用、産業制御用システム等に適用することにより、産業競争力を増すことができる。日本が競争力を持つハードウエァ中心の製品競争力を、重要な ICT であるセキュリティ技術によって強化する道筋であり、社会・経済・生活における安心安全からみた科学技術イノベーションに貢献すると考える。さらに、本技術の基盤は基礎数学にあることを考えると、基礎から応用をつなぐこうした分野において適切なプロジェクトを立てて人材を育成することが重要である。

セキュリティシステムは必ず悪意の攻撃の対象になる。したがって、基礎研究として攻撃の研究、暗号化や攻撃耐性強化回路技術、攻撃耐性評価システムなどの研究は、絶えず進歩している。本研究テーマを通じて、我が国のセキュリティ技術研究拠点（チーム）が大きく強化されたわけであるが、JST としても今後ともこの種のテーマへの研究支援を発展継続していただきたい。

３－３. 総合的評価

一部研究成果が実装されており、評価技術に関して一部は世界水準、回路技術に関しても世界競争水準に近づいている。