課題別事後評価結果

【課題名】

Security evaluation of physically attacked cryptoprocessors in embedded systems（SPACES）

（邦題：組込み暗号処理システムの統合安全性評価プラットフォームの開発）

【研究代表者】

日：Naofumi Homma (Tohoku University)

仏：Jean-Luc Danger (Telecom ParisTech)

【評価】

正規の入出力チャネル以外から漏洩する情報への物理攻撃（サイドチャネル攻撃）に対する脆弱性を製品開発の過程で評価する高精度シミュレーションとプロトタイプによる実地的な評価を組み合わせた統一的な安全性評価プラットフォームが構築され、当初の目的は十分に達成された。成果発表も十分になされた。また、１件の国際特許の出願が予定されている。

プロジェクトは、研究ブロックごとに区切りそれらを相互に連携させる手法で運営された。非常に優れたスキームであり、国際共同研究プロジェクトのマネジメントの一つのモデルとして賞賛に値する。適宜プロジェクト内ワークショップを開催し、十分な研究交流があった。さらに、本プロジェクトが運営した国際ベンチマーキングコンテスト（DPA Contest version4）は 20 種もの攻撃が提案され有効であった。

また、本成果を契機に米国電気電子学会(IEEE)環境電磁工学ソサイエティにおいて、電磁情報セキュリティに関する新たな技術小委員会が設立された点も興味深く注目に値する。

本プロジェクト成果の産業応用は SASEBO-W によって一定程度達成されているが、本分野の重要性からみて、一層の普及を急ぐべきである。DPA で標準の評価ボードに採用されるなど SASEBO-W の認知度は高まっていること、シミュレーションソフトはオープンソース化が予定されていることから、本プロジェクトの更なる展開が期待される。具体的な産業応用例としては、特定の機器向けにカスタマイズしたサイドチャネル攻撃検出シミュレーションソフトを構築するサービスへ発展する可能性がある。産業応用に向けては ISO、IEC などの国際標準への働きかけ、デファクトスタンダードと成るような戦略が必要であり、さらに工業所有権の獲得が鍵となる。

本プロジェクトで形成された協力体制を基に、今後日仏あるいは日 EU 間でセキュリティチップ向けの新たな検査、分析、保証サービスのスキームやシステムの構築に取り組むことを期待する。