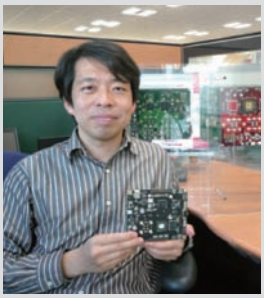
暗号モジュールの標準評価ボードを開発

ハードウエアのセキュリティ向上と国際標準規格策定に貢献



佐藤　証
さとう あかし

akashi.satoh@aist.go.jp

情報セキュリティ研究センター
ハードウェアセキュリティ
研究チーム
研究チーム長
（秋葉原事業所）

より安全で信頼性の高いハードウエアシステムの実現を目指し、情報セキュリティに関するアルゴリズムおよび、その高性能 VLSI 実装の研究を進めています。

関連情報：

● 共同研究者

片下 敏宏、坂根 広史（産総研）

● 参考文献

T. Katashita *et al.*: *Proc. ECCTD 2009*, 403-408, Aug.(2009).

● プレス発表

2007 年 12 月 17 日「暗号ハードウェアとして初めて JCMVP 認証を取得」

● この研究開発は、経済産業省の委託事業「暗号モジュールの実装攻撃の評価に関する調査研究」において行われました。

暗号の普及と実装の安全性評価

ユビキタス情報社会を支える基盤技術の一つとして、暗号技術の利用が拡大しています。暗号の安全性は、そのアルゴリズムを専門家が理論的に解析することで保たれてきました。しかし、暗号製品の普及につれて、実装上の弱点を突く攻撃方法が登場しています。その中でも特に、暗号モジュールの消費電力や電磁波などに漏洩する秘密情報を取得するサイドチャネル攻撃に対する評価と対策技術の開発が急がれています。私たちは安全性評価の国際標準規格策定への貢献と暗号製品の安全性向上を目的に、サイドチャネル攻撃研究用の標準評価ボードや解析ツールを開発し、その利用促進を図っています。

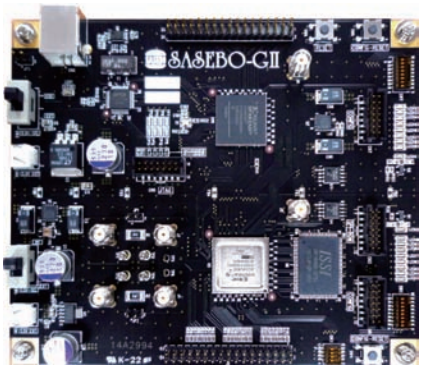
開発したSASEBO-GIIの特徴

安全で信頼性の高い情報システムの構築には、セキュリティを確保するほかに、故障や不具合なども迅速に対処できることが重要です。ハードウエアはソフトウエアのように簡単にはアップデートできず、一般的にはシステムを停止して修理を行う必要があります。そこで、回路を動作させながら機能の書き換えが可能なLSIであるFPGAの活用が有望視されています。

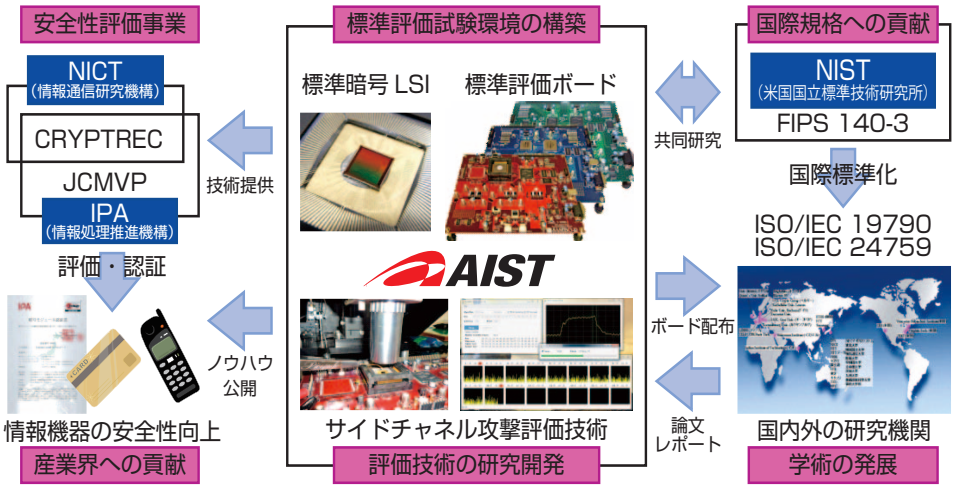
今回、開発したFPGAボードSASEBO-GIIは、これまでに比べて大幅な小型・高集積化を行い、サイドチャネル攻撃の解析精度に影響を与える電源ノイズの低減も実現しました。また、動作中に回路の一部を書き換えできる動的部分再構成機能もサポートしています。動的部分再構成技術の研究促進によって、正常な回路リソースによる故障の修復や、遠隔地にある装置のネットワーク経由による機能アップデート、そして必要な回路のオンデマンド実装による多機能化・小型・省電力化が実現され、ハードウエアシステムの信頼性と性能の大幅な向上が期待されます。

今後の展開

SASEBOボードを用いて、暗号モジュールに誤動作を誘発する故障利用解析攻撃や、LSIのパッケージを開封して内部を直接観察する侵襲攻撃など、より高度な攻撃と対策手法の研究を行っていきます。また、最先端の部分再構成技術を有する研究者・エンジニアの育成を目的に教育キットの開発も進めています。



新規開発の SASEBO－GII ボード



暗号モジュールの安全性評価技術の開発と国際標準規格策定への取り組み