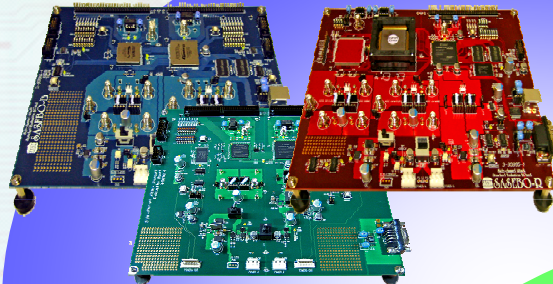


ハードウェアセキュリティ研究チームの活動概要

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
佐藤 証

ハードウェアセキュリティ研究チーム

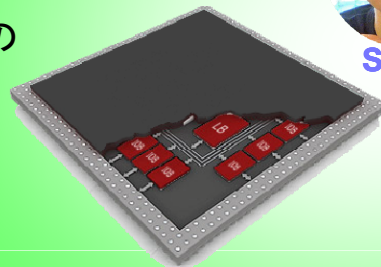
暗号モジュールの安全性評価



標準評価環境の整備



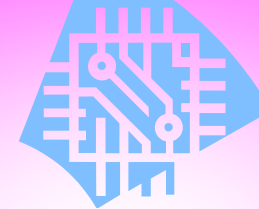
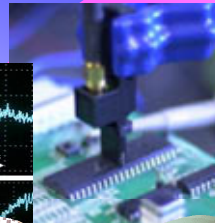
暗号モジュール評価制度への
貢献とガイドライン策定



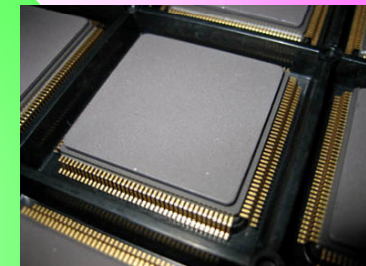
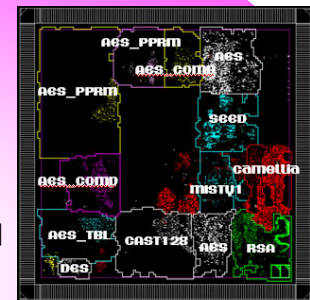
組み込みセキュリティ

アプリケーション開発

暗号回路の高性能実装技術



暗号回路IPマクロ



ISO/IEC標準暗号LSI



Sakane



Katashita



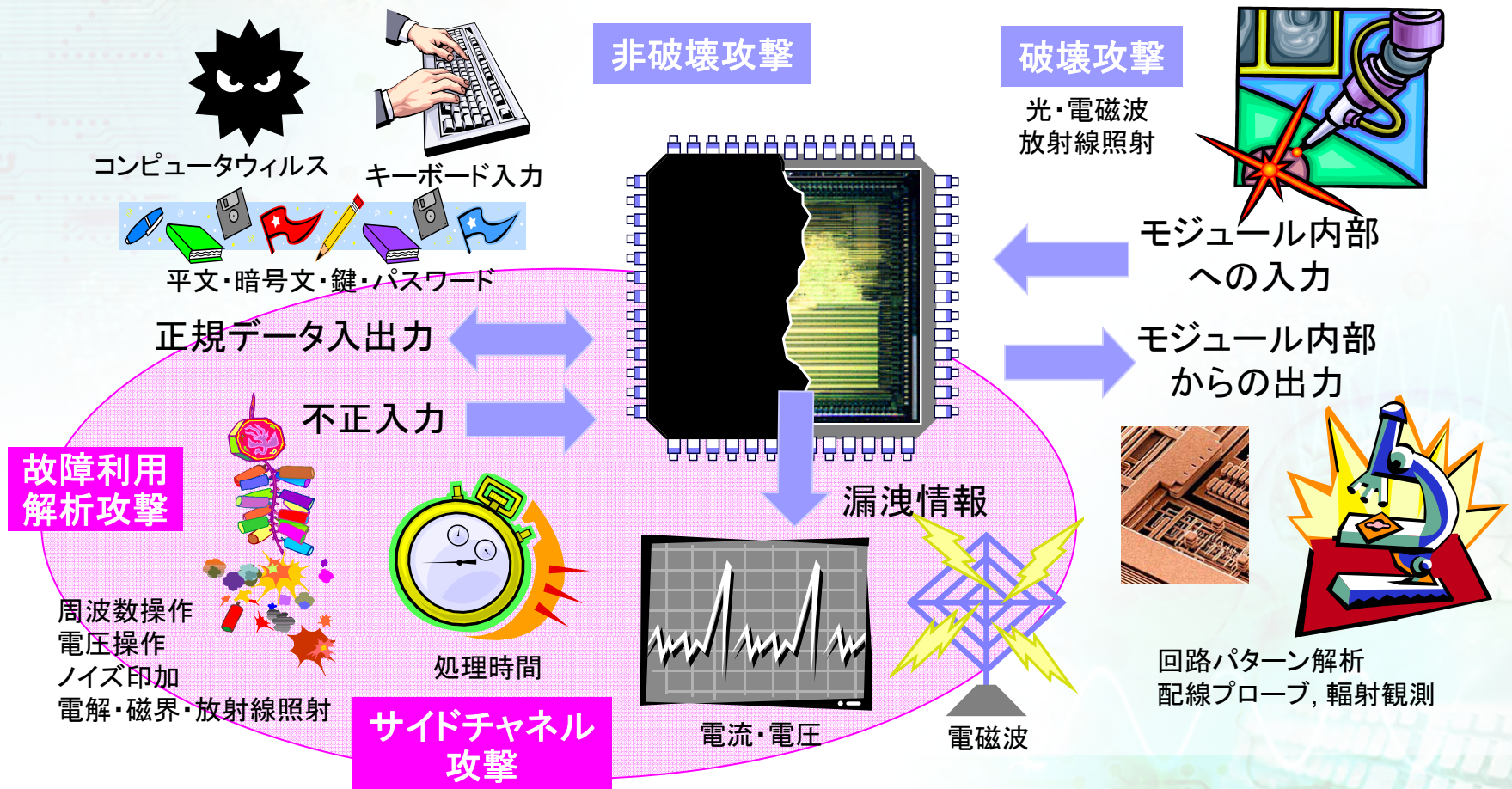
Satoh



ネットワークセキュリティ

様々な物理解析攻撃法

- モジュールへの様々な入出力の組み合わせによって解析を行う
- 論理的に安全な暗号アルゴリズムを用いても実装の不備を突く物理解析攻撃に対する安全性は保障されない



プロジェクト概要

- ・ サイドチャネル攻撃評価ボードと暗号回路を開発し標準評価実験環境を構築
- ・ NISTとの協力関係を密にし, FIPS 140-3標準化・ISO/IEC 19790改定に貢献

情報機器の安全性向上



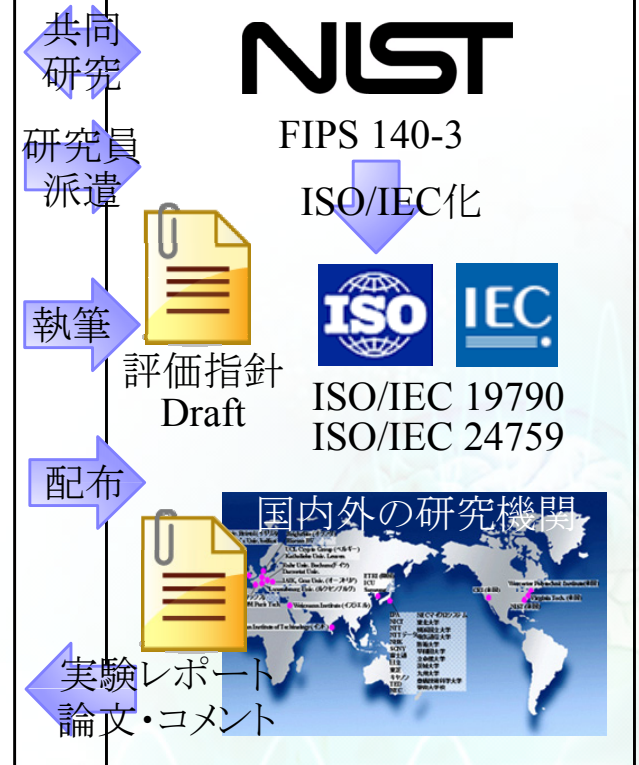
技術
提供

ノウハウ
公開

標準評価試験環境の構築

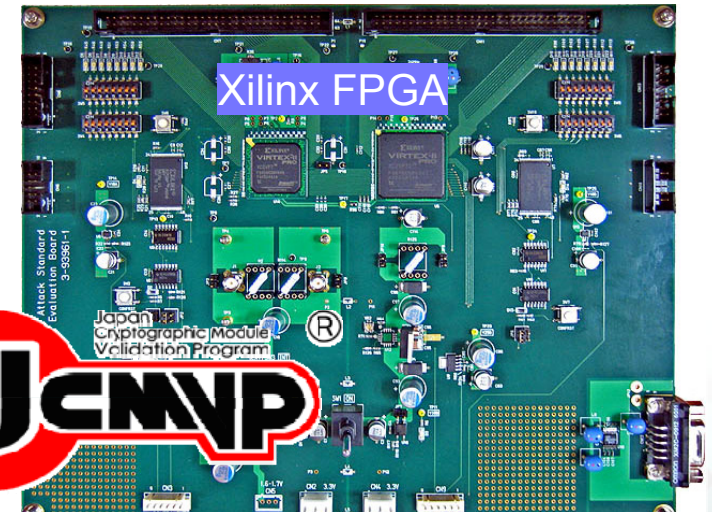
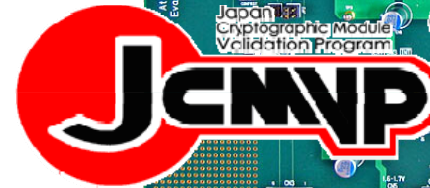


国際規格策定への貢献



サイドチャネル攻撃標準評価ボード SASEBO

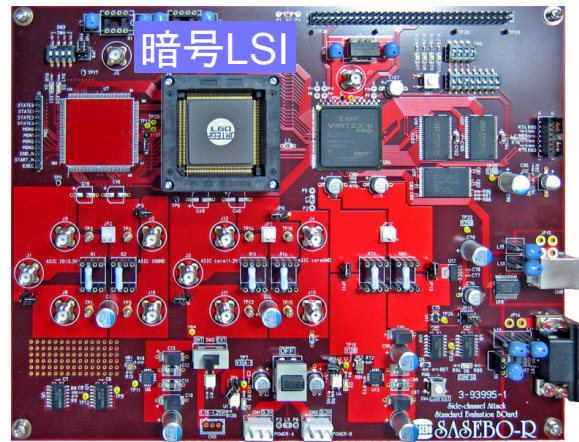
- 4種類のボードを開発
 - SASEBO: Xilinx FPGA (18年度)
 - SASEBO-B: ALTERA FPGA (19年度)
 - SASEBO-R: 暗号LSI (19年度)
 - SASEBO-G: Xilinx FPGA (20年度)
- SASEBOにAESを実装したSASEBO-AESは暗号ハードウェアモジュールとして初のJCMVP認証を取得



Side-channel Attack Standard Evaluation Board



SASEBO-B



SASEBO-R



SASEBO-G

佐世保市を抜いてGoogle検索第3位



Research Center for
Information Security (RCIS)

[Japanese](#) | [English](#)



Side-channel Attack Standard Evaluation Board (SASEBO)

▶ [RCIS Top](#)

▶ [News](#)

▶ [About RCIS](#)

▶ [Research](#)

▶ [Members](#)

▶ [Job Offers](#)

▶ [Events](#)

▶ [Contact](#)

[AIST](#) > [RCIS](#) > Side-channel Attack Standard Evaluation Board (SASEBO)

What's NEW

2008.10.1	SASEBO Quick Start Guide is released
2008.10.1	SASEBO-G Specifictaion is added
2008.6.28	SASEBO page is relaunched.

Project Overview

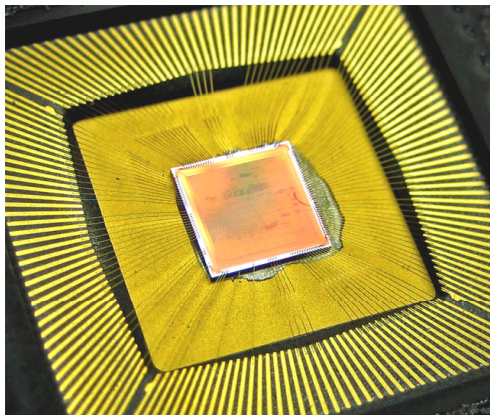
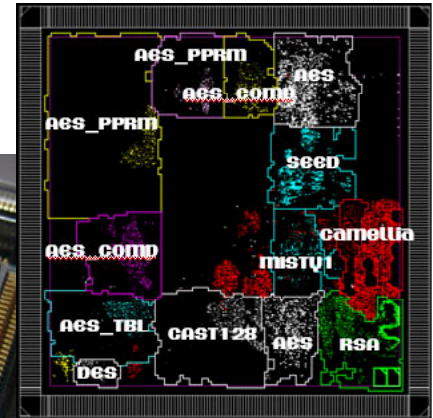
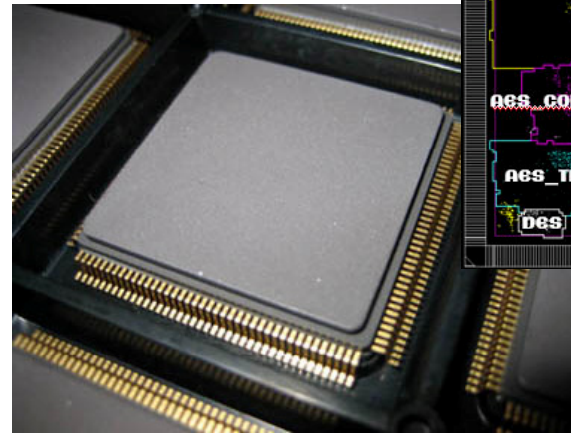
With the rapid expansion of broadband networks and the spread of information appliances, IC cards, and radio frequency identification (RFID) tags, etc., large amounts of data are transferred in every phase of daily life. At the same time, security threats such as leakages and falsification of information are on the rise. Cryptography is widely used even in consumer products as a fundamental countermeasure against such threats. However, it is difficult for users to determine whether or not a cryptographic algorithm is implemented properly; it is not unusual for security flaws to be discovered in products advertised as perfectly secure.

[FIPS 140-2](#), issued by the National Institute of Standards and Technology ([NIST](#)) and [ISO/IEC 19790](#) and [24759](#) represent security evaluation standards specifying the requirements that should be satisfied by cryptographic modules. The Japan Cryptographic Validation Program ([JCMVP](#)®), which is compliant with the above standards, is also operated in Japan by [IPA](#)®. However, these standards do not cover side-channel attacks, which represent a new type of physical attack using secret information leaking from side channels instead of the designated I/O channels of the cryptographic module, in the form of

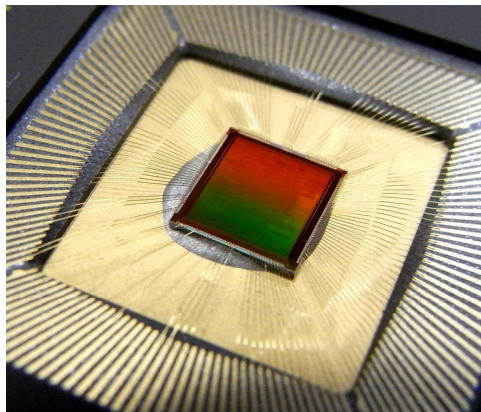


標準暗号LSI

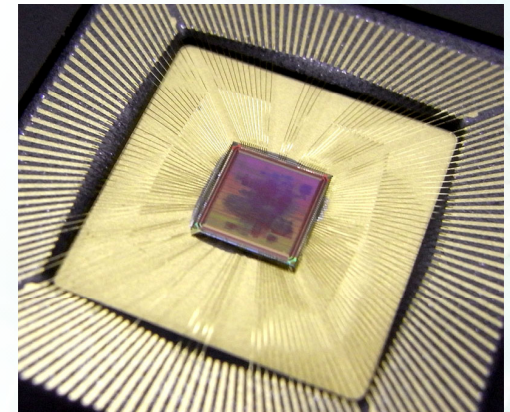
- 平成19年度に全てのISO/IEC標準ブロック暗号とRSA暗号を実装した130nm CMOSによる評価用LSIを開発
 - 128bit暗号: AES, Camellia
 - 64bit暗号: DES, MISTY1, SEED, CAST128
- 平成20年度は各種DPA対策を施したAES回路(横浜国立大学提供)や楕円曲線暗号(電気通信大学提供)を実装した130nmと90nmの2種類のLSIを開発



標準暗号LSI (130nm)



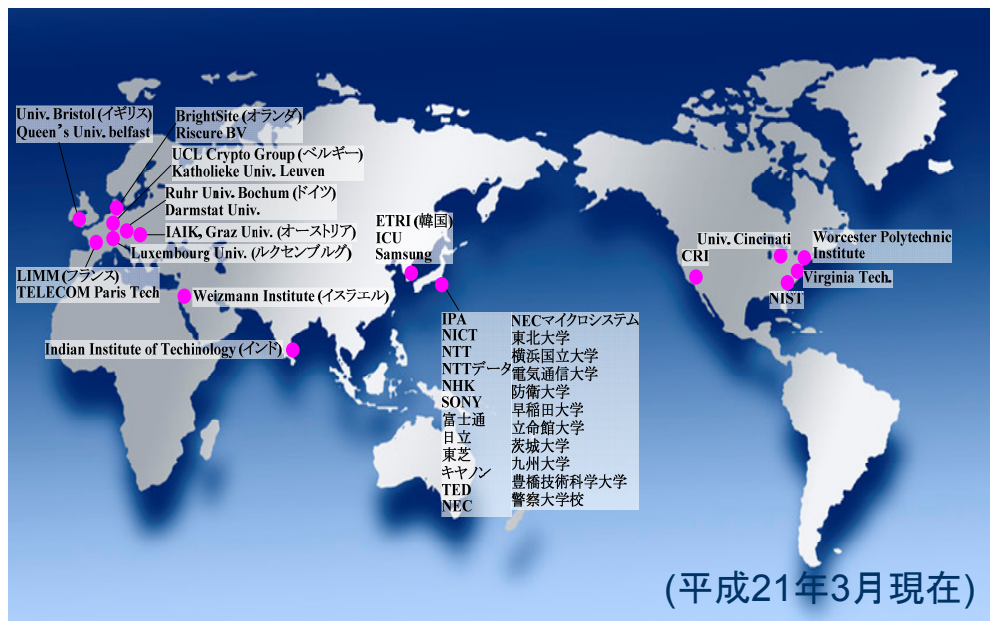
DPA対策版LSI (130nm)



DPA対策版LSI (90nm)

学術研究活動への貢献

- 暗号実装の研究で実績のある国内27機関、海外25機関に配布
- 英文誌・国際会議19件、和文紙・国内研究会50件の関連発表
- 暗号ハードウェアに関する最も権威のある国際会議CHES2008のスポンサーを務め、10周年記念のパネル討論のパネリストとして参加
- CHES2010のスポンサー
- CHES2006の横浜に続きCHES2011の東京誘致を計画



CHES Home

PROGRAM

ACCEPTED PAPERS



Workshop on Cryptographic Hardware and Embedded Systems 2008 (CHES 2008)

Washington, DC, USA

Sunday August 10th - Wednesday 13th, 2008

Co-located with [5th Workshop on Fault Diagnosis and Tolerance in Cryptography](#) - FDTCT 2008, Sunday August 10th.

Participants of CHES may also be interested in attending the [Cryptography Research Introduction to Side Channel Analysis - SPA, DPA and Timing Attacks Workshop](#), Thursday, August 14th.



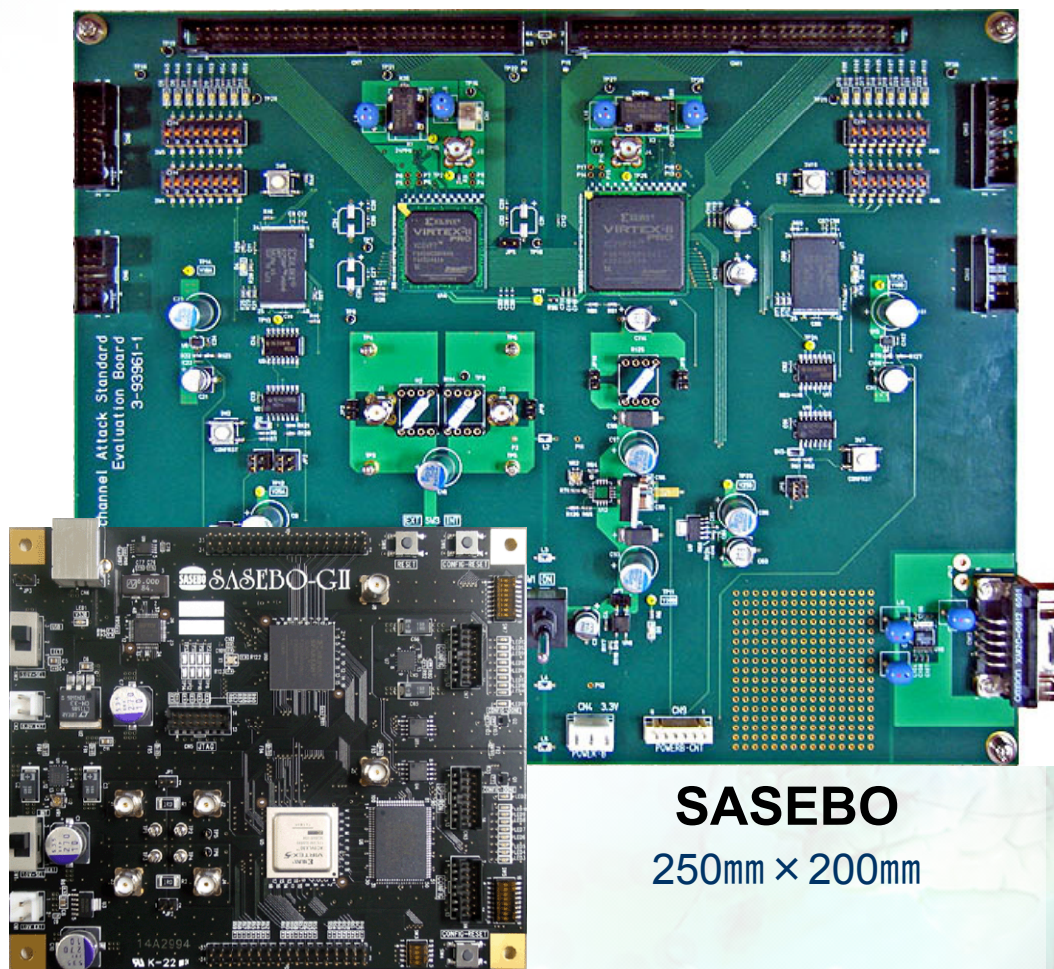
GOLD SPONSOR



SPONSORS

小型・高性能FPGAボードSASEBO-GII

- SASEBO-GのFPGA Virtex-IIのロジック容量では, DPA対策を施した回路に対して不足してきた
- SASEBOを利用したいというリクエストが多く寄せられるが, 実績のある研究機関にのみ配布
- 最新のVirtex-5 LX30/50を用い, これまでの実験・研究で得たノウハウを集約したSASEBO-GIIを開発し, 東京エレクトロデバイスから商用として販売を予定
 - ロジック容量は4~7倍
 - ボードサイズが1/3
 - 電源やクロック系のノイズを低減
 - USB経由で4種類のコンフィグレーションモードをサポート



SASEBO
250mm × 200mm

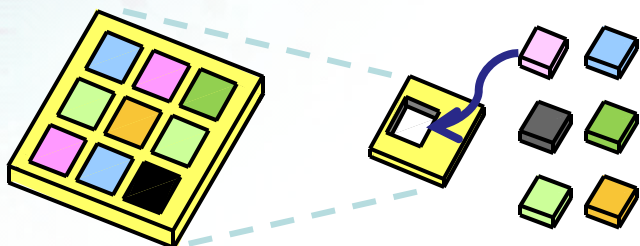
SASEBO-GII
140mm × 120mm

再構成可能ハードウェアの応用

- FPGAにより小型, 省電力, フレキシブルな暗号システムが実現できる
- これまで固定されたハードウェアモジュールに対する多くの研究がなされてきた
- SASEBO-GIIは動的部分再構成機能を有しており, 様々な動的セキュリティシステムの実験が可能である.

小型実装

Modules can be time-multiplexed



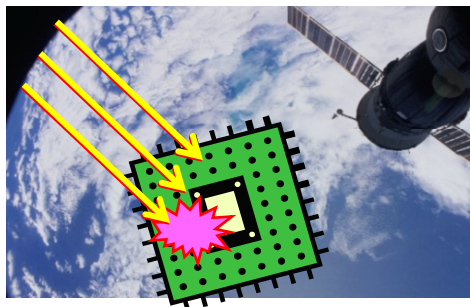
省電力・高速

H/W is superior to S/W



耐故障性

Damaged module can be replaced



動的再構成

Required function can be downloaded



商用ICカード評価ツール

- FIPS140-3でSCA評価が義務付けられるのはシングル暗号モジュールで、主な対象はICカード。
- 商用ICカード評価ツールは3社が販売しており、全ツールにSASEBOが組込まれている。
 - Cryptography Research Inc.(米国): DPA Workstation
 - BrightSight (オランダ) : Sideways
 - Riscure (オランダ) : Inspector
- RCISの評価手法を組み込み、標準評価ツールとして試験期間での利用を検討中



bright sight[®]

