National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

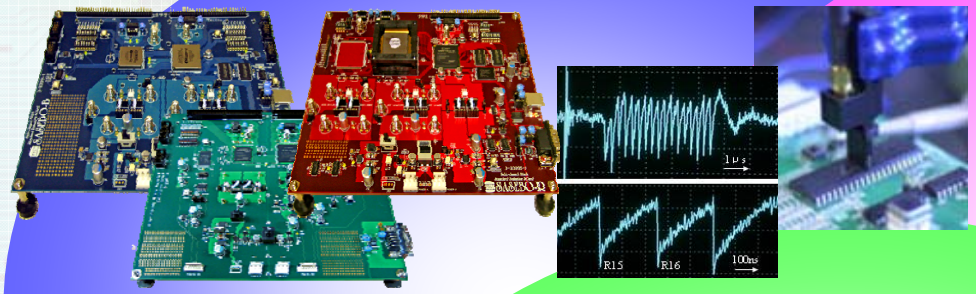
ハードウェアセキュリティ技術の動向

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

National Institute of Advanced Industrial Science and Technology
AIST

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

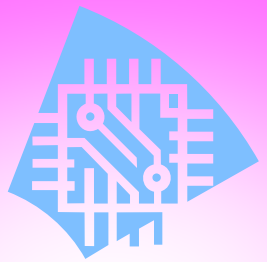


標準評価環境の整備

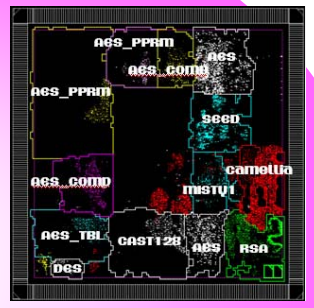
JCMVP

暗号モジュール評価制度への
貢献とガイドライン策定

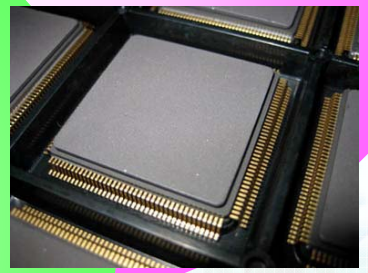
暗号回路の高性能実装技術



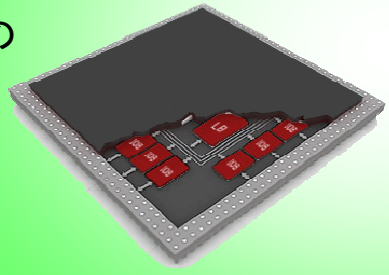
暗号回路IPマクロ



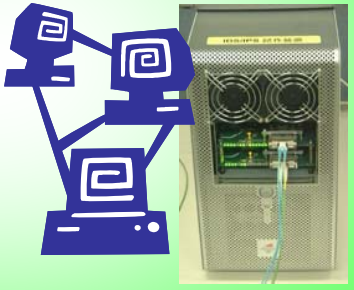
研究テーマ



ISO/IEC標準暗号LSI



組み込みセキュリティ



ネットワークセキュリティ

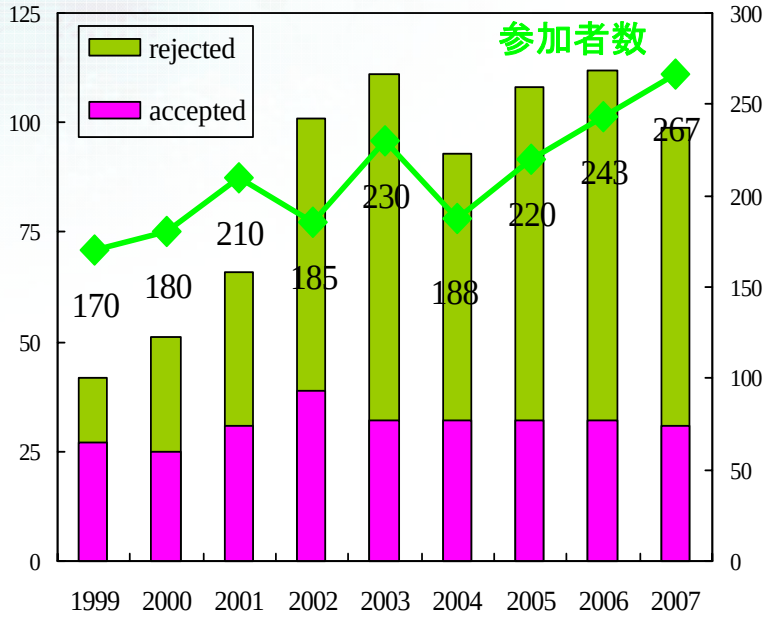
アプリケーション開発

National Institute of Advanced Industrial Science and Technology
AIST

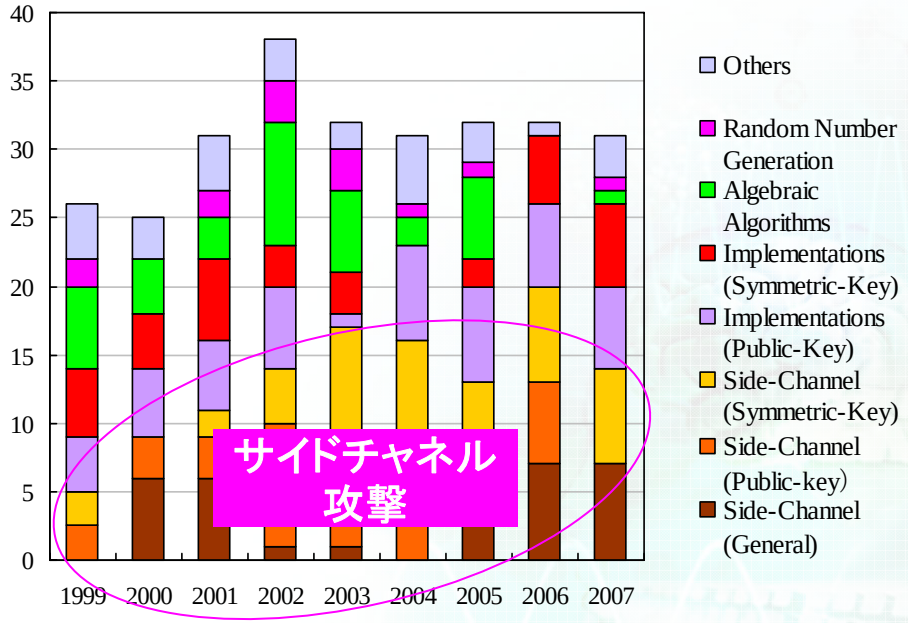
暗号モジュールの安全性に関する研究

- 暗号回路とシステムに関する最も権威のある学会CHES (Cryptographic Hardware and Embedded Systems) では，サイドチャネル攻撃の論文が半数を占めている
- 攻撃・対策アルゴリズムの論理的研究から，MPUやFPGAボード上の実装による物理的な実験がより重要となってきている

CHESの論文投稿数と参加者の推移



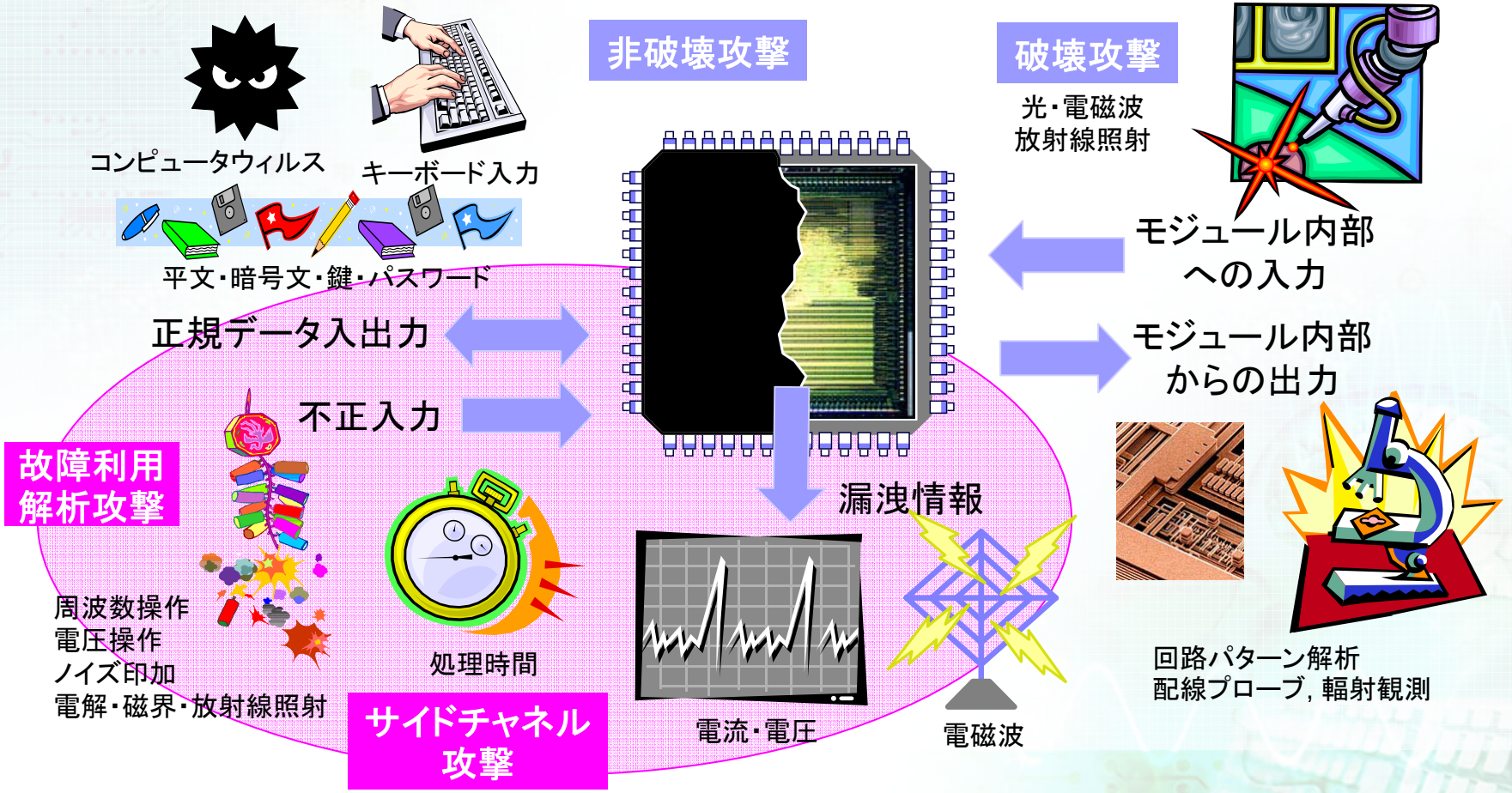
CHESの論文のカテゴリ



National Institute of Advanced Industrial Science and Technology
AIST

様々な物理解析攻撃法

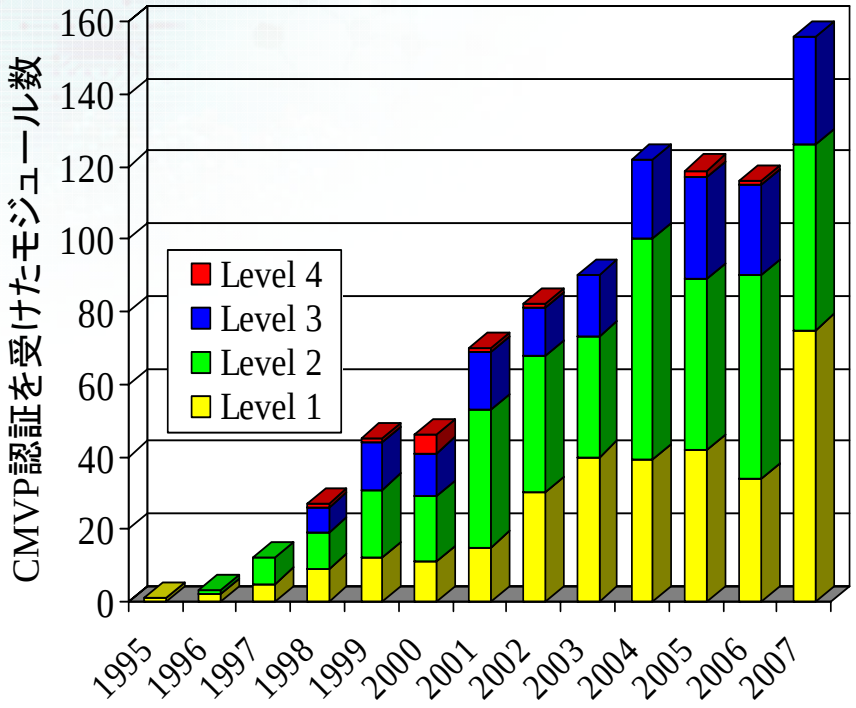
- モジュールへの様々な入出力の組み合わせによって解析を行う
- 論理的に安全な暗号アルゴリズムを用いていても実装の不備を突く物理解析攻撃に対する安全性は保障されない



National Institute of Advanced Industrial Science and Technology
AIST

FIPS 140-2 (ISO/IEC 19790)

- 米国連邦標準FIPS140-2 “暗号モジュールのセキュリティ要件”をベースに標準化されたISO/IEC 19790の国内評価制度JCMVPが始まっている
- 11のカテゴリ毎（ ISO/IEC 19790ではカテゴリ8は削除）に定められたセキュリティ要件に対して1~4のレベル評価が行われる
- 最新の研究であるサイドチャネル攻撃などを取り入れたFIPS140-3への改定作業も進んでいる



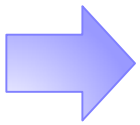
	セキュリティ要件	規定内容
1	暗号モジュール仕様	暗号モジュールの仕様と「FIPS 140-2」の適用範囲
2	暗号モジュールのポート･インタフェース	情報の入出力
3	役割，サービス，及び認証	ユーザーの役割や役割ごとに提供されるサービス，ユーザーの認証方法
4	有限状態モデル	状態遷移の記載
5	物理セキュリティ	表面処理やカバー等の物理的セキュリティ要件
6	動作環境	暗号モジュールの動作環境
7	暗号鍵管理	鍵生成，鍵の入出力等
8	電磁妨害／電磁両立性(EMI/EMC)	電磁波に対する要件
9	自己テスト	暗号モジュールの正しい動作を確認するテスト
10	設計保証	ガイドライン等
11	その他の攻撃の対処	「FIPS 140-2」で規定されていない攻撃への対処方法

National Institute of Advanced Industrial Science and Technology
AIST

FIPS 140-2からFIPS 140-3へ

- 2007年7月にFIPS 140-3のドラフトを公開
- セキュリティレベルは4段階から5段階に変更
- 有限状態モデルはライフサイクル保証の中で規定
- EMI/EMCの項は削除
- ソフトウェアセキュリティと非破壊の物理セキュリティ(サイドチャネル攻撃)の項を新設
- 暗号鍵管理は，暗号鍵を含むSecurity Sensitive Parameter管理に
- 設計保証は，設計からテスト・配送・運用等を含むライフサイクル保証に

FIPS 140-2	
1	暗号モジュール仕様
2	暗号モジュールのポート インタフェース
3	役割，サービス，及び認証
4	有限状態モデル
5	物理セキュリティ
6	動作環境
7	暗号鍵管理
8	電磁妨害／電磁両立性 (EMI/EMC)
9	自己テスト
10	設計保証
11	その他の攻撃の対処



FIPS 140-3	
1	暗号モジュール仕様
2	暗号モジュールのポート インタフェース
3	役割，サービス，及び認証
4	ソフトウェアセキュリティ
5	動作環境
6	物理セキュリティ
7	物理セキュリティ(非破壊)
8	Security Sensitive Parameter 管理
9	自己テスト
10	ライフサイクル保証
11	その他の攻撃への対処

National Institute of Advanced Industrial Science and Technology
AIST

FIPS 140-3のサイドチャネル攻撃

- 解析手法の単純さの度合いでレベル分けされているが詳細は未定
- 電磁波解析攻撃や故障利用解析攻撃は入っていない
- 各レベルに要求される試験自体が大きく変わる可能性がある

セキュリティレベル	タイミング解析攻撃	単純電力解析攻撃	差分電力解析攻撃
1, 2			
3	レベル3に要求される試験装置と試験手法	レベル3に要求される試験装置と試験手法	
4 (主要な攻撃への対策)	レベル4に要求される試験装置と試験手法	レベル4に要求される試験装置と試験手法	レベル4に要求される試験装置と試験手法
5 (全ての攻撃への対策)	レベル5に要求される試験装置と試験手法	レベル5に要求される試験装置と試験手法	レベル5に要求される試験装置と試験手法

National Institute of Advanced Industrial Science and Technology
AIST

FIPS 140-3のスケジュール

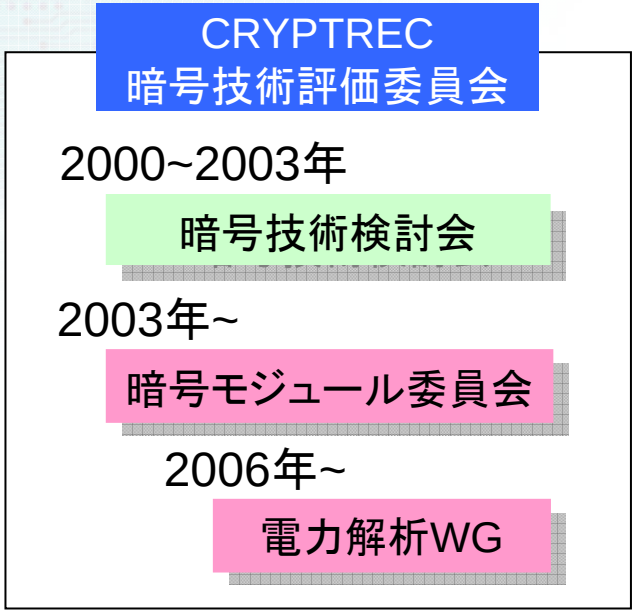
- 当初の計画の2006年11月FIPS140-3運用開始から大幅に遅れている

2004年9月15日	CMVP Symposium 2004でFIPS140-3改定の意向を表明
2005年1月12日	FIPS140-3への改定作業に入ることを正式発表
2005年2月28日	FIPS140-2に対するパブリックコメントの募集を開始
2005年9月26日	Physical Security Testing WorkshopをIPAと共同開催
2007年3月31日	FIPS140-3 1st Draftの内部レビューがNISTとCSEで終了
2007年7月13日	1st Draftを公開. 90日間のコメント募集期間を設定
2007年10月11日	コメント募集終了
2008年3月18日	Software Security Workshopを開催
2008年第2四半期	2nd Draftを公開. 90日間のコメント募集期間を設定
2008年第3四半期	コメント募集終了
2008年第4四半期	FIPS140-3の最終版公開
2008年第4四半期	米国商務省による承認
6ヶ月後	FIPS140-3の運用開始
6ヶ月後	FIPS140-2の運用終了

National Institute of Advanced Industrial Science and Technology
AIST

CRYPTREC委員会活動

- 2000年に経済産業省と総務省が電子政府で使用される暗号評価を目的とし，IPAとNICTの共同プロジェクトとしてCRYPTREC (Cryptography Research and Evaluation Committees)が発足
- 2003年に暗号モジュール委員会が発足
- 2006年に暗号モジュール委員会の下部に電力解析ワーキンググループが発足



電子政府推奨暗号リストと評価レポートを作成
暗号技術監視委員会へ継続

FIPS140-2のISO/IEC19790, 24759標準化への貢献
JCMVPや暗号モジュール評価基準策定への貢献

サイドチャネル攻撃の実験活動の効率化

CRYPTREC Cryptography Research and Evaluation Committees
IPA
NiCT

National Institute of Advanced Industrial Science and Technology
AIST

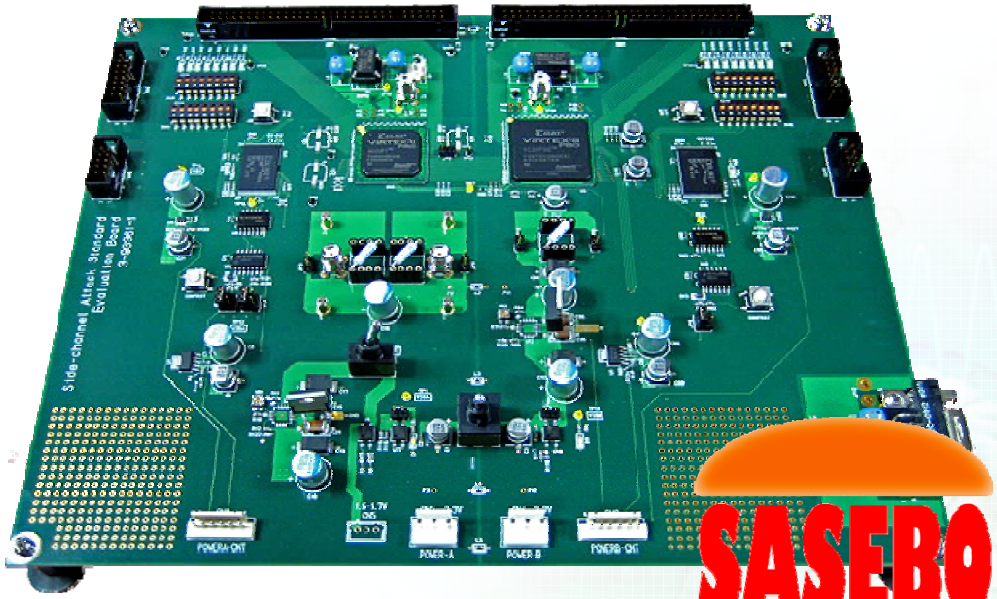
サイドチャネル攻撃用標準評価ボード

- 産業技術総合研究所と東北大学は平成18年度の経済産業省委託事業の中でサイドチャネル攻撃実験の標準評価用としてボードを開発
  - PowerPCプロセッサを搭載した2種類のXilinx社製FPGAを実装
  - FPGA上で実装評価可能な暗号回路ソースを公開

National Institute of Advanced Industrial Science and Technology
AIST

TOHOKU UNIVERSITY

METI
Ministry of Economy, Trade and Industry



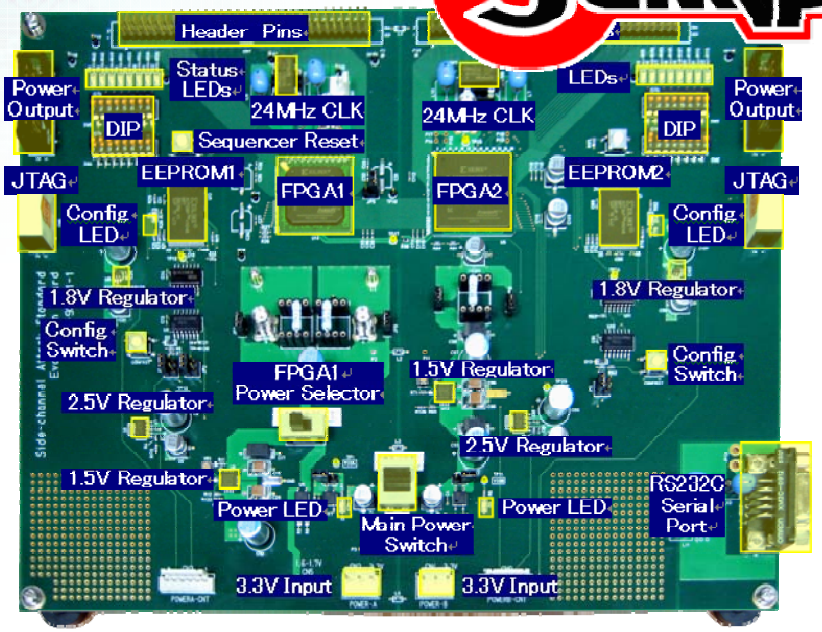
Side-channel Attack Standard Evaluation BOard

National Institute of Advanced Industrial Science and Technology
AIST

JCMVP認証を取得

- SASEBO上にAES回路を実装し，暗号ハードウェアモジュールとして始めてJCMVP認証を取得
- JCVMP制度普及に向けて，暗号ハードウェアのソースコードやボード回路図等の技術情報等を全てWeb公開

Japan Cryptographic Module Validation Program ®



IPA

JCMVP VALIDATED

暗号モジュール認証書

暗号モジュール試験及び認証制度に基づき、下記のとおり認証する。

平成 [illegible] 日
独立行政法人 [illegible]
理事長 [illegible]

認証番号 F0003

日本語名： SASEBO-AES暗号FPGAボード

英語名：

暗号モジュールバージョン： SASEBO-AES-G1.1
ハードウェアバージョン： P/N 3-93961-1
ファームウェアバージョン： 1.1 （ファームウェア名称： SASEBO-FPGA1）
1.0 （ファームウェア名称： SASEBO-FPGA2）
物理形態： マルチチップ組込型

適合規格： JCMVP暗号モジュールセキュリティ要件 平成18年10月16日
試験要件： JCMVP暗号モジュール試験要件 平成18年10月16日
JCMVP暗号アルゴリズム試験要件 平成18年10月16日
申請者： 東北大学・産業技術総合研究所 暗号ハードウェア開発プロジェクト
所在地： 仙台市青葉区片平二丁目1番1号
特記事項： なし

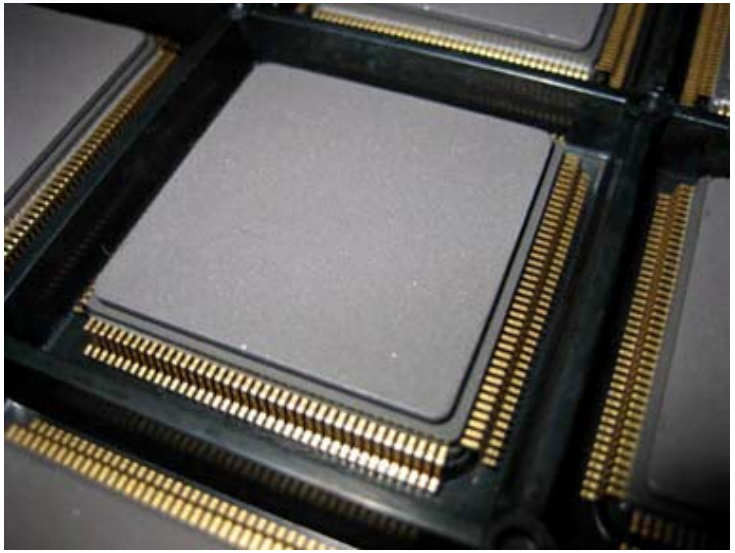
注意事項：本暗号モジュール認証書で識別される暗号モジュールは、「暗号モジュール試験及び認証制度」で承認された試験機関による、暗号モジュール試験要件に基づく暗号モジュール試験結果が、適合していることを示す。本暗号モジュール認証書は、暗号モジュール試験を受けた構成及び動作環境に関して、暗号モジュールの特定のバージョンのみに適用される。暗号モジュール試験は「暗号モジュール試験及び認証制度」の規定に従って実施され、暗号モジュール試験報告書の試験機関による結論は、暗号モジュール試験に用いた提供物件にのみ対応している。この暗号モジュール認証書は独立行政法人 情報処理推進機構による暗号モジュール製品等の保証書ではない。また、独立行政法人 情報処理推進機構は、明示、黙示を問わず、本暗号モジュールを用いた暗号モジュール製品等に関していかなる保証も行わない。なお、本認証書を、不正にしようした場合、並びに誤解を招くような方法で広告又は説明等に使用した場合には、暗号モジュール認証の取消を行うことがある。

National Institute of Advanced Industrial Science and Technology
AIST

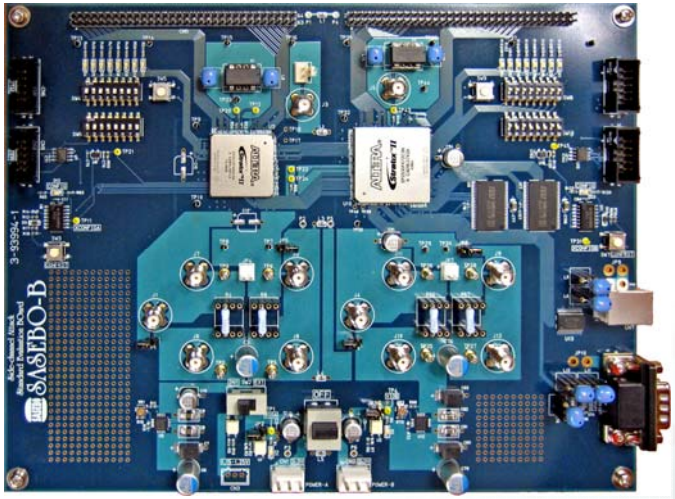
標準暗号を実装したLSIを開発

- 平成19年度に全てのISO/IEC標準ブロック暗号とRSA暗号を実装した評価用LSIおよびボードを開発
  - 128bit暗号：AES，Camellia
  - 64bit暗号：DES，MISTY1，SEED，CAST128
- XILINX社に加えてALTERA社のFPGAを用いたボードも開発

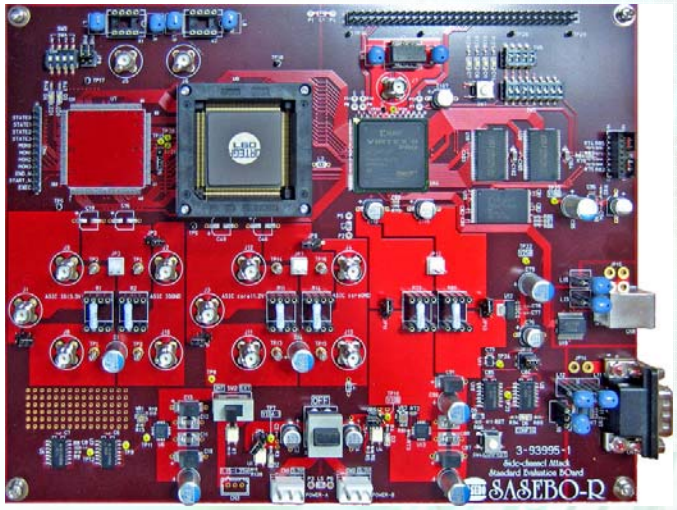
標準暗号LSI



ALTERAボード



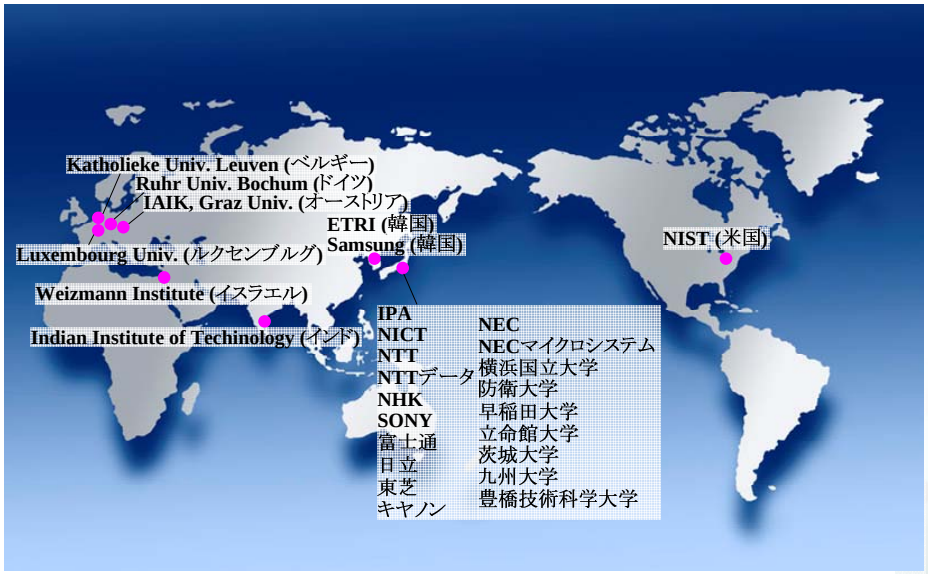
暗号LSIボード



National Institute of Advanced Industrial Science and Technology
AIST

プロジェクト概要

- 各研究機関は独自の実験環境を用いているため第三者評価が困難
- 暗号は機密性の高い技術が用いられるため情報の公開が限られる
- 標準評価ボードによる実験を通じて得られた技術とノウハウを暗号製品の設計指針として公開
- サイドチャネル攻撃を含む新たな試験基準を策定



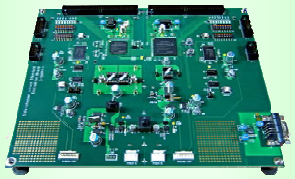
製品の安全性向上

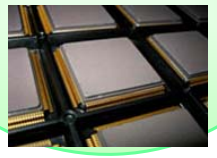
暗号製品の設計指針

技術情報公開

本事業の研究開発

暗号回路開発と実験環境整備

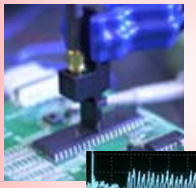


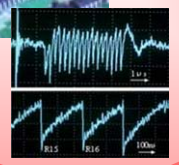


標準化機関と協力

国際標準への貢献

新たな試験基準策定のための実験

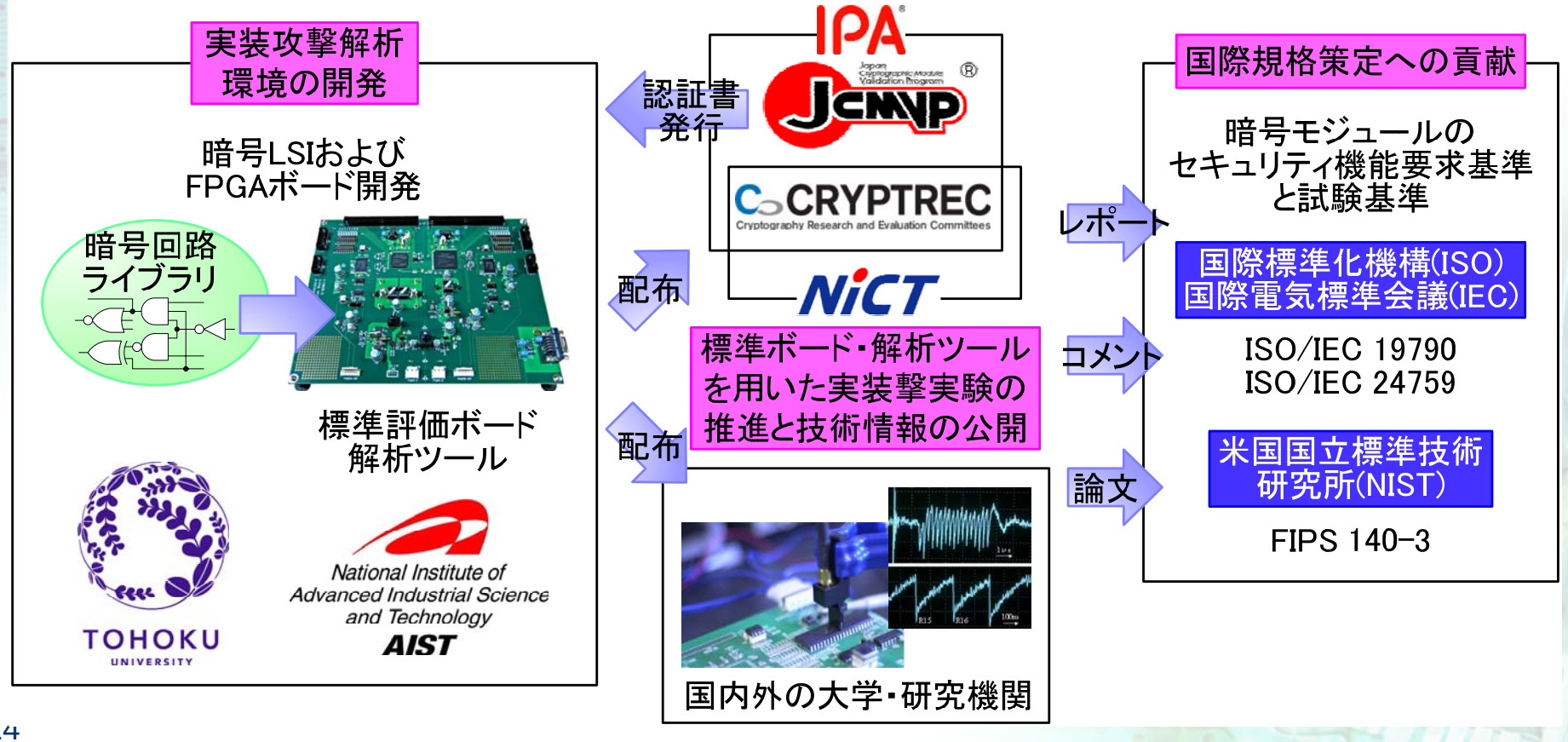




National Institute of Advanced Industrial Science and Technology
AIST

プロジェクト概要

- 開発したFPGAボード，LSIボード，暗号回路ライブラリを国内外の研究機関に配布し統一された評価実験環境を構築する
- NISTとの協力関係を密にし，FIPS 140-3の標準化およびISO/IEC 19790の改定作業に大きく貢献する



National Institute of Advanced Industrial Science and Technology
AIST

自動評価ツールの開発

- AESとRSAの代表的な攻撃だけでも非常に多くの手法が提案されている
- 第三者機関が公平かつ効率的に評価を行うためには自動化ツールが不可欠

● AESへの実装攻撃
<< Simple Power Analysis >>
--- General Topic ---
R. Mayer, et al., “Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards,” CHES 2000.
S. Mangard, “A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion,” ICISC 2002.
G. Bertoni, et al.,“AES Power Attack Based on Induced Cache Miss and Countermeasure,” ITCC 2005.
--- Collision Attack ---
K. Schramm, et al.,“A New Class of Collision Attacks and its Application to DES,” FSE 2003.
K. Schramm, et al.,“A Collision-Attack on AES Combining Side Channel and Differential-Attack,” CHES 2004.
H. Ledig, et al., “Enhancing Collision Attacks,” CHES 2004.
<< Differential Power Analysis >>
--- General Topic ---
P. Kocher, et al.,“Introduction to Differential Power Analysis and Related Attacks,” http://www.cryptography.com/dpa/technical/index.
P. Kocher, et al.,“Diffrential Power Analysis,” Crypto ’99
T. S. Messerges, et al.,“Investigations of Power Analysis Attacks on Smartcards” USENIX Workshop on Smartcard Technology 1999.
J. S. Coron, et al.,“Statistics and Secret Leakage,” FC 2000.
M. L. Akker, et al.,“Power Analysis, What is Now Possible,” Asiacrypt 2000.
R. Bevan, et al.,“Ways to Enhance Differential Power Analysis,” ICISC 2002.
D. Agrawal, et al.,“Multi-Channel Attacks,” CHES 2003.
E. Brier, et al.,“Correlation Power Analysis with a Leakage Model,” CHES 2004.
T. -H. Le, et al.,“A proposition for Correlation Power Analysis enhancement,” CHES 2006.
J. Jaffe,“A First-Order DPA Attack against AES in Counter Mode with Unknown Initial Counter,” CHES 2007.
--- Electromagnetic Analysis ---
J. -J. Quisquater, et al.,“ElectroMagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards,” E-smart 2001.
K. Grandolfi, et al.,“Electromagnetic Analysis: Concrete Results,” CHES 2001.
S. Agrawal, et al.,“The EM Side Channel(s),” CHES 2002.
H. Li, T. Markettos, et al.,“Security Evaluation against Electromagnetic Analysis at Design Time,” CHES 2005.
--- Second Order ---
T. S. Messarges,“Using Second-Order Power Analysis to Attack DPA Resistant Software,” CHES 2000.
J. Dj. Golic, et al.,“Multiplicative Masking and Power Analysis of AES,” CHES 2002.
I. Waddle, et al.,“Towards Efficient Second-Order Power Analysis,” CHES 2004.
M. Joye, et al.,“On Second-Order Differential Power Analysis,” CHES 2005.
D. Suzuki, et al.,“DPA Leakage Models for CMOS Logic Circuits,” CHES 2005.
S. Mangard, et al.,“Side-Channel Leakage of Masked CMOS Gates,” CT-RSA 2005.
S. Mangard, et al.,“Successfully Attacking Masked AES Hardware Implementations,” CHES 2005.
E. Oswald, et al.,“Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers,” CT-RSA 2006.
S. Mangard, et al.,“Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations,” CHES 2006.
--- Higher Order ---
S. Chari, C. Jutla, J. Rao, and P. Rohatgi, “Towards Sound Approaches to Counteract Power-Analysis Attacks,” Crypto ’99.
K. Schramm and C. Paar, “Higher Order Masking of the AES,” CT-RSA 2006.
J. Coron, E. Prouff, and M. Rivain, “Side Channel Cryptanalysis of a Higher Order Masking Scheme,” CHES 2007.

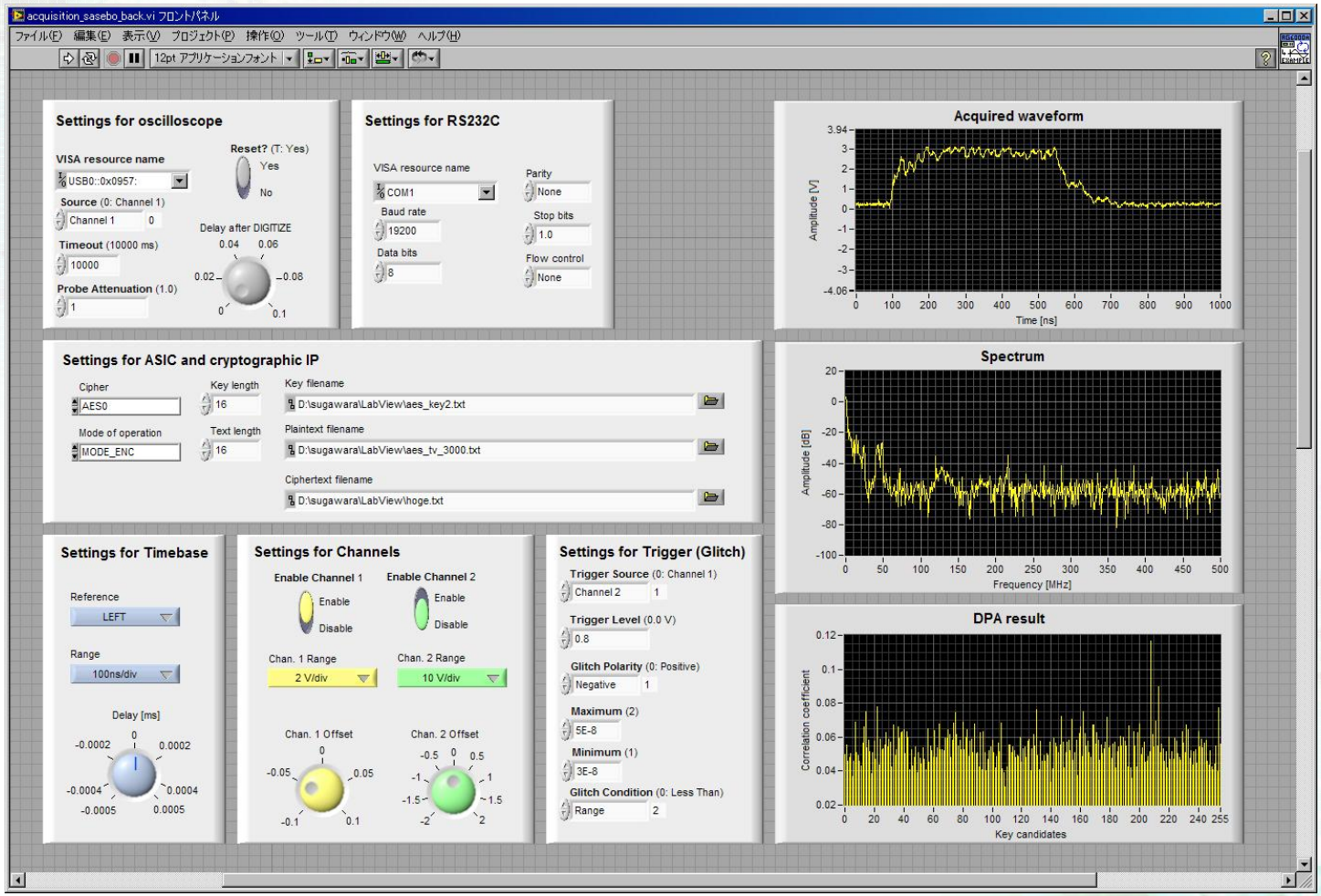
<< Template Attack >>
E. Biham, et al.,“Power Analysis of the Key Scheduling of the AES Candidates,” The Second Advanced Encryption Standard Candidate Conference.
P. N. Fahn, “IPA: A New Class of Power Attacks,” CHES 1999.
S. Chari, et al.,“Template Attacks,” CHES 2002.
C. Rechberger, et al.,“Practical Template Attacks,” WISA 2004.
D. Agrawal, et al.,“Templates as Master Keys,” CHES 2005.
E. Peeters, et al.,“Improved Higher-Order Side-Channel Attacks with FPGA Experiments,” CHES 2005.
W. Schindler, et al.,“A Stochastic Model for Differential Side Channel Cryptanalysis,” CHES 2005.
C. Archambeau, et al.,“Template Attacks in Principal Subspaces,” CHES 2006.
B. Gierlichs, et al.,“Templates vs. Stochastic Methods,” CHES 2006.
E. Oswald, et al.,“Template Attacks on Masking – Resistance is Futile,” CT-RSA 2007.
K. Lemke-Rust, et al.,“Gaussian Mixture Models for Higher-Order Side Channel Analysis,” CHES 2007.
<< Experiments >>
C. Clavier, et al.,“Differential Power Analysis in the Presence of Hardware Countermeasure,” CHES 2000.
F. -X. Stadaert, et al.,“Power Analysis of an FPGA Implementation of Rijndael: Is Pipelining a DPA Countermeasure?,” CHES 2004.
C. Gebotys, et al.,“M Analysis of Rijndael and ECC on a Wireless Java-based PDA,” CHES 2005.
S. B. Ǿrs, et al.,“Power-analysis attack on an ASIC AES implementation,” ITCC 2004.
<< Enhancing Method >>
N. Homma, et al.,“High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching,” CHES 2006.
S. Skorobogatov,“Optically Enhanced Position-Locked Power Analysis,” CHES 2006.

● RSAへの実装攻撃
<< Timing Attack >>
P. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,” Crypto ’96.
W. Schindler, “A Timing Attack against RSA with the Chinese Remainder Theorem,” CHES 2000.
C. D. Walter, et al.,“Distinguishing Exponent Digits by Observing Modular Subtractions,” CT-RSA 2001.
W. Schindler, “Combined Timing and Power Attack,” PKC 2002.
<< Simple Power Analysis >>
P. Kocher, et al.,“Introduction to Differential Power Analysis and Related Attacks,” http://www.cryptography.com/dpa/technical/index.
C. D. Walter, “Sliding Windows Succumbs to Big Mac Attack,” CHES 2001.
R. Novak, “SPA-based Adaptive Chosen-ciphertext Attack on RSA Implementation,” PKC 2002.
V. Klima, et al.,“Further Results and Considerations on Side Channel Attacks on RSA,” CHES 2002.
P. A. Fouque, et al.,“Attacking Unbalanced RSA-CRT Using SPA,” CHES 2003.
P. A. Fouque, et al.,“The Doubling Attack – Why Upwards Is Better Than Downwards,” CHES 2003.
S. M. Yen, et al.,“Power Analysis by Exploiting Chosen Message and Internal Collisions – Vulnerability of Checking Mechanism for RSA-Decryption,” Mycrypt 2005.
P. A. Fouque, et al.,“Power Attack on Small RSA Public Exponent,” CHES 2006.
<<Differential Power Analysis>>
P. Kocher, et al.,“Differential Power Analysis,” Crypto ’99.
T. S. Messerges,et al.,“Power Analysis Attacks of Modular Exponentiation in Smartcards,” CHES 1999.
J. S. Coron, “Resistance against differential power analysis for elliptic curve cryptosystems,” CHES 1999.
B. D. Boer,et al.,“A DPA Attack against the Modular Reduction within a CRT Implementation of RSA,” CHES 2002.
F. Amiel,et al.,“Power Analysis for Secret Recovering and Reverse Engineering of Public Key Algorithms,” SAC 2007.

National Institute of Advanced Industrial Science and Technology
AIST

自動評価ツールの開発

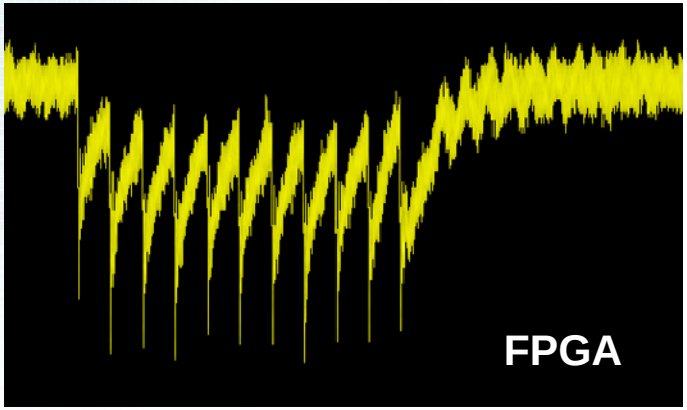
- LabVIEW+MATLABでSASEBOに実装したAESを自動解析するプロトタイプを作成
- 拡張性と速度性能の向上を目指してC言語ベースにより開発中

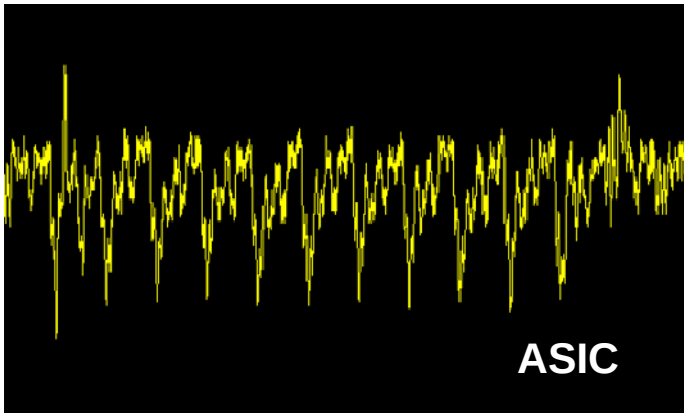


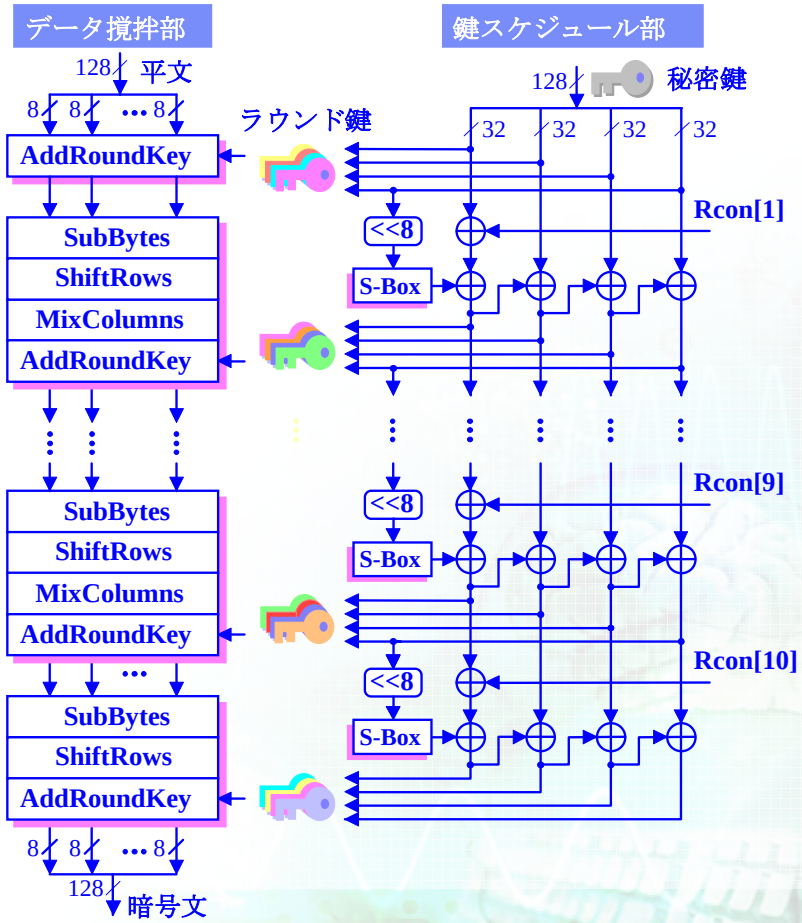
National Institute of Advanced Industrial Science and Technology
AIST

AES への電力解析攻撃

- ブロック暗号AESの10ラウンド処理がFPGAとASICの双方で目視可能だが，秘密鍵の導出には数千～数万波形の統計処理する必要があり，実装法によって有効な解析手法が異なる





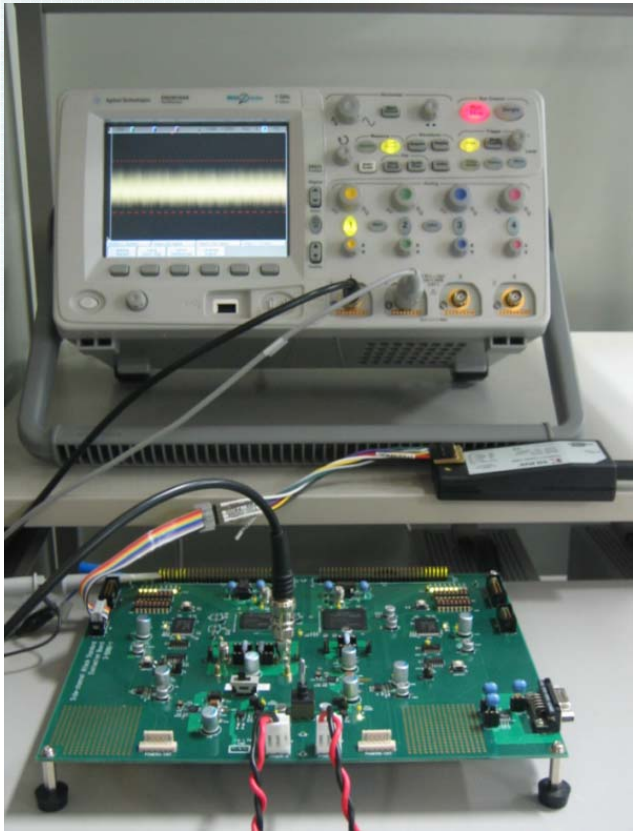


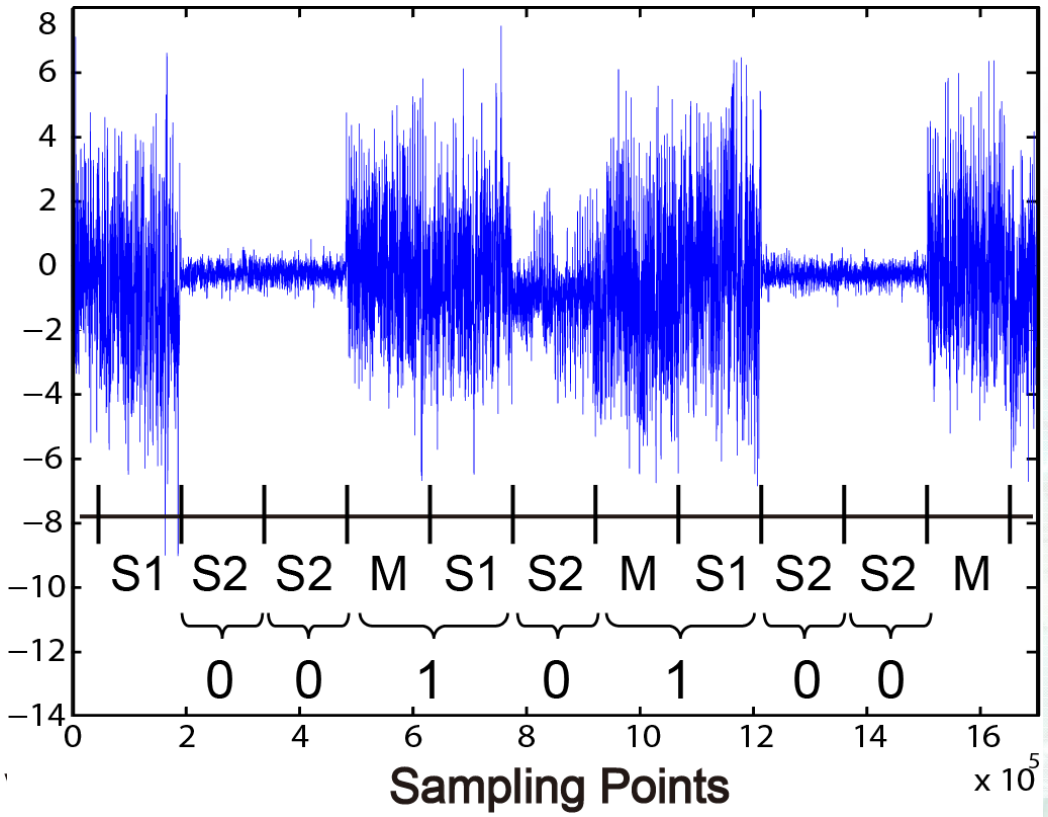
National Institute of Advanced Industrial Science and Technology
AIST

RSA暗号回路の電力解析攻撃

- 秘密鍵dのビットパターンに応じて乗算と自乗算を繰り返すRSA暗号では，実装によっては秘密鍵を電力波形から直接読み取ることが可能
- 特殊な入力データや波形処理を行う手法を開発

$$M=C^d \bmod n$$





National Institute of Advanced Industrial Science and Technology
AIST

2007年研究開発スケジュール