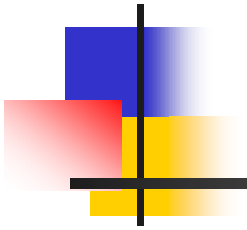
*平成21年12月19日公開ワークショップ資料*



# 耐タンパディペンダブル VLSIシステムの開発・評価

*Tamper Resistance*

## ～人為的攻撃による内部機密情報の漏洩・複製を防止するVLSIの実現～

立命館大学・産総研・中央大学・名城大学

# 発表内容

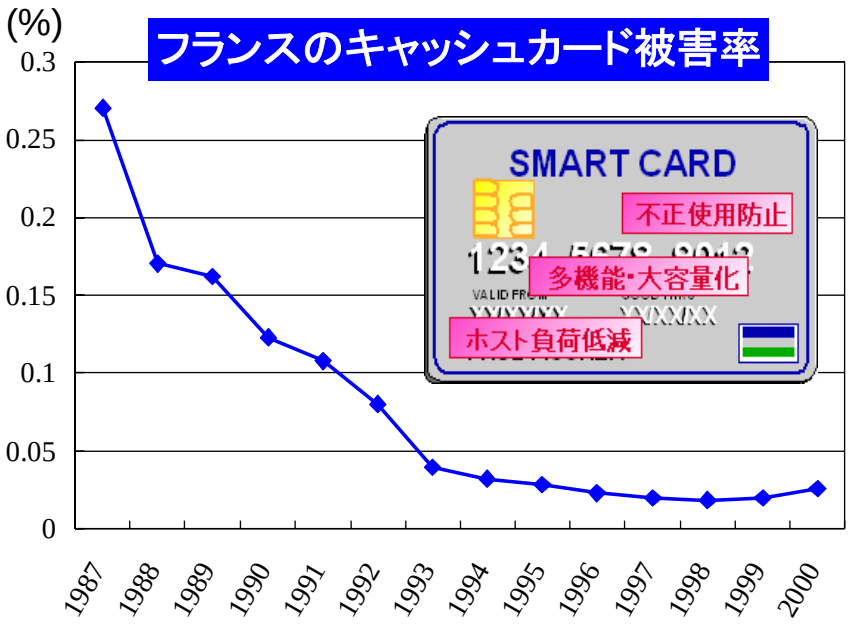
*Tamper Resistance*

- 暗号モジュールとディペンダビリティー
  - サイドチャネルアタック
- 耐タンパLSI設計プラットフォーム
  - DPA攻撃の原理
  - DPA攻撃対策回路（Domino-RSL方式）
- 耐タンパ性能評価プラットフォーム
  - 暗号モジュールの安全性評価制度
  - 攻撃評価ボードSASEBOプロジェクト
- 偽造LSIを識別するPUFを用いたセキュリティシステム

# 載機器

*Tamper Resistance*

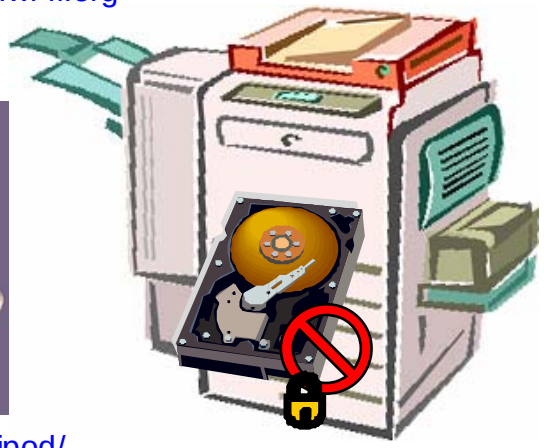
- ICカード・RFID・電子パスポート
- 暗号ネットワーク通信
- 音楽・映像メディアのコンテンツ保護
- ビジネス文書・FPGAの設計情報の保護




フランス銀行カード協会調べ

www.wi-fi.org

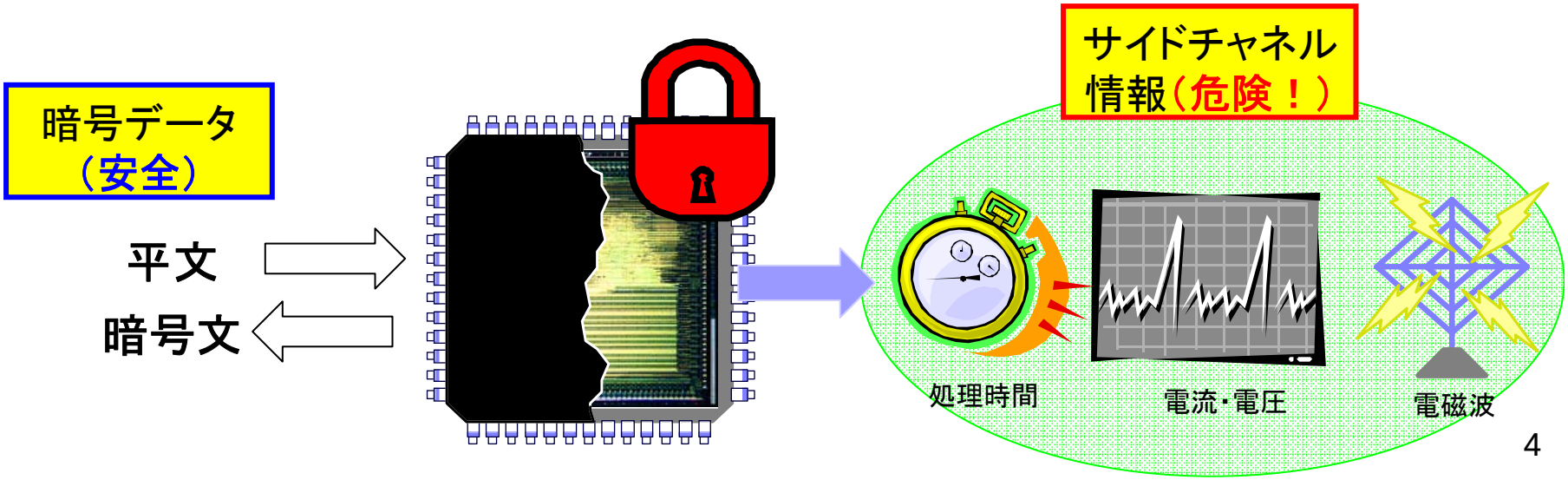
http://www.apple.com/ipod/



# 暗号処理回路とサイドチャネル情報

*Tamper Resistance*

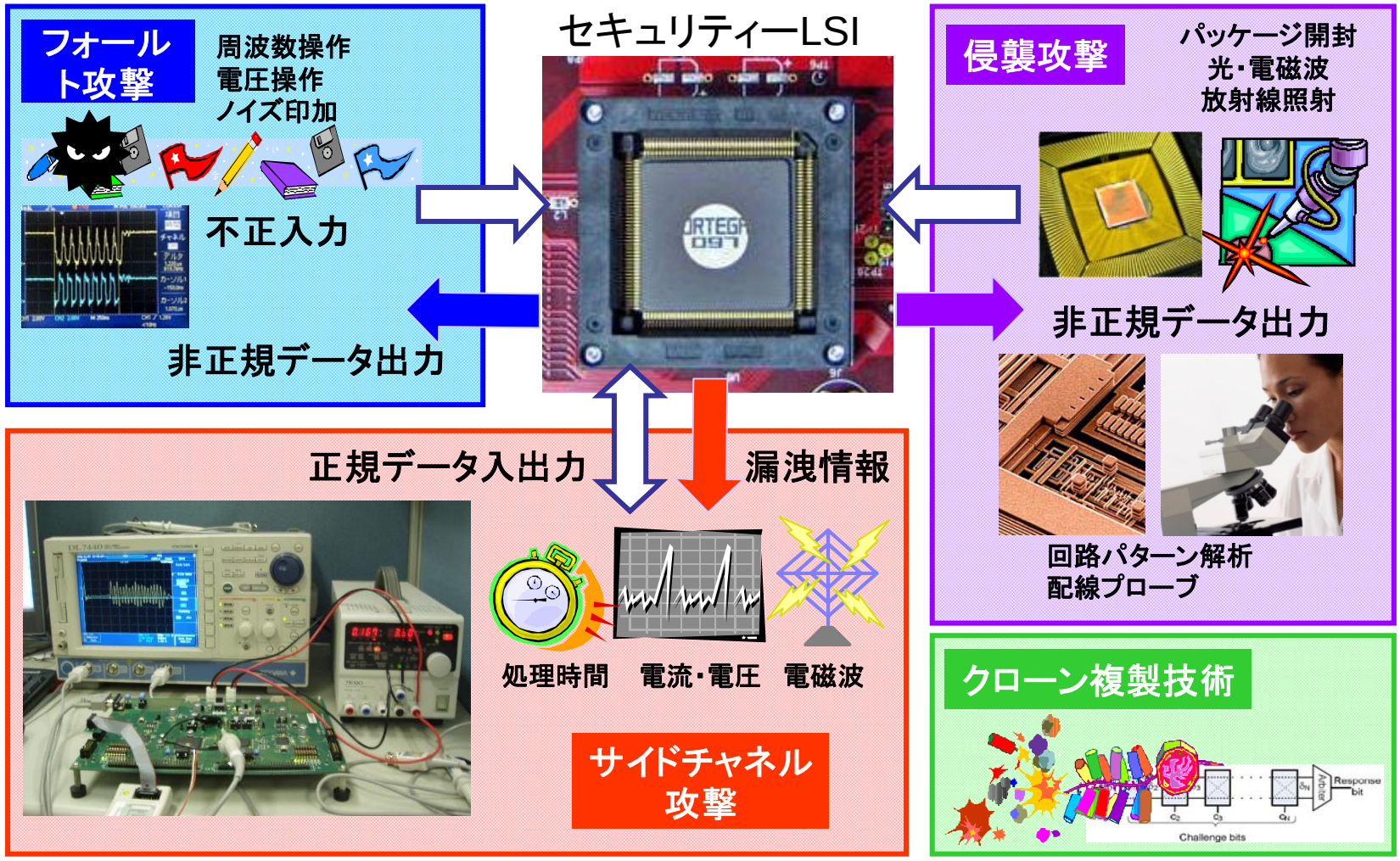
- 暗号鍵が機密情報を守る
- 標準暗号　3DES，AES
  ⇒　暗号アルゴリズムは公開
  ⇒　多くの研究者によって数学的な安全性は保証
- 暗号回路動作時のサイドチャネル情報
  - サイドチャネル情報＝処理時間．消費電力，電磁波
  - サイドチャネル情報から暗号鍵を推定



# 耐タンパディペンダブルLSIの要件

*Tamper Resistance*

- 下記のような物理攻撃・複製技術に対して耐性のあるセキュリティーLSI



# 本研究の目標

*Tamper Resistance*

- 3種の物理攻撃と偽造LSIの製造に対する防御方法を備えた，耐タンパLSIを実現し以下3つの成果物を得る．

（1）耐タンパ性LSI設計プラットフォーム

- 物理攻撃に対する，耐タンパ性を有するLSIの設計指針
- LSIを容易かつ低コストで設計・製造するための設計プラットフォームを提供．

（2）耐タンパ性能評価プラットフォーム

- セキュリティLSIの耐タンパ性能を評価する指針
- 攻撃実験用のLSIボードを開発し，評価試験環境を構築

（3）偽造LSIを識別するPUFを用いたセキュリティシステム

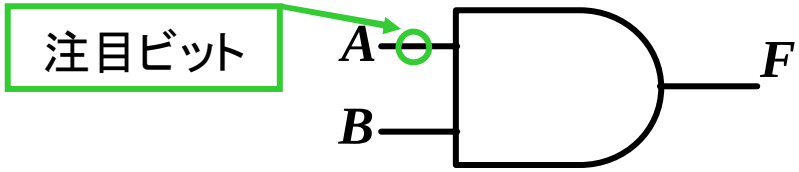
- LSIに固有の物理特性の差異を識別するPUF（Physically Unclonable Function）の回路設計・開発
- PUFと暗号技術を融合した新しいセキュリティシステムの提案

# 電力利用サイドチャネル攻撃の原理

*Tamper Resistance*

- 単純な2入力ANDゲートの場合

A1⇒A2，B1⇒B2，の遷移は$2^4$＝16通り




A1=0のときの遷移確率　2/8

1/4回電力増加

消費電力に差が出る

A1=1のときの遷移確率　4/8

1/2回電力増加

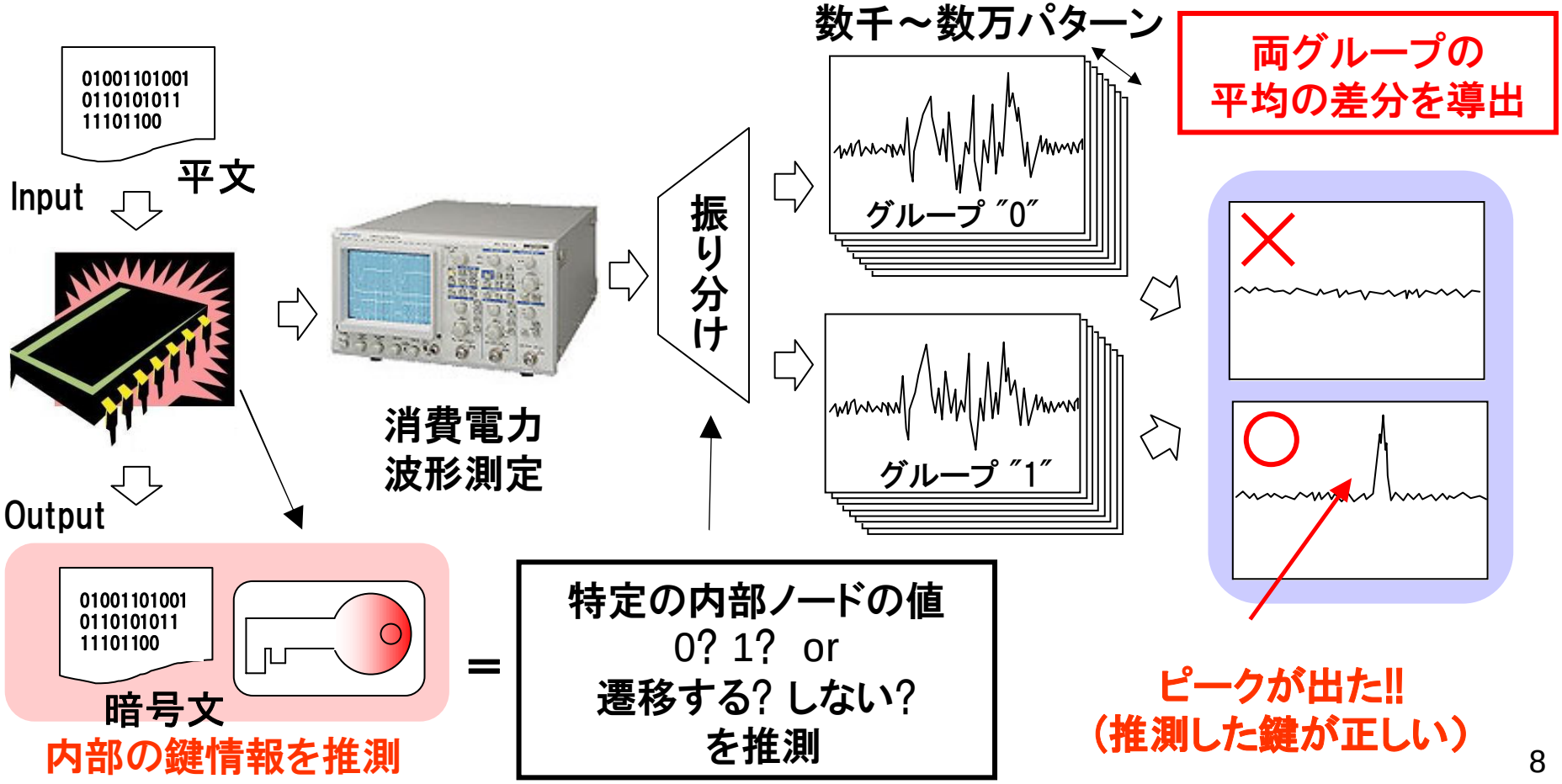
注目ビットの値を推定し，注目ビットが1の場合と0の場合の消費電力に差が生じれば推定値は正しい

| A1 | B1 | A2 | B2 | F1 | F2 | |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | |
| 0 | 0 | 0 | 1 | 0 | 0 | |
| 0 | 0 | 1 | 0 | 0 | 0 | |
| 0 | 0 | 1 | 1 | 0 | 1 | 遷 |
| 0 | 1 | 0 | 0 | 0 | 0 | |
| 0 | 1 | 0 | 1 | 0 | 0 | |
| 0 | 1 | 1 | 0 | 0 | 0 | |
| 0 | 1 | 1 | 1 | 0 | 1 | 遷 |
| 1 | 0 | 0 | 0 | 0 | 0 | |
| 1 | 0 | 0 | 1 | 0 | 0 | |
| 1 | 0 | 1 | 0 | 0 | 0 | |
| 1 | 0 | 1 | 1 | 0 | 1 | 遷 |
| 1 | 1 | 0 | 0 | 1 | 0 | 遷 |
| 1 | 1 | 0 | 1 | 1 | 0 | 遷 |
| 1 | 1 | 1 | 0 | 1 | 0 | 遷 |
| 1 | 1 | 1 | 1 | 1 | 1 | |

# 差分電力解析(Differential Power Analysis)攻撃



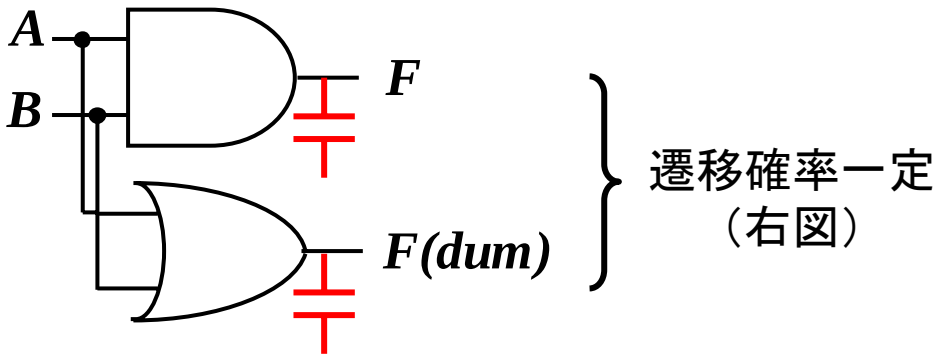
- 1999年にKocherらによって提案された差分電力解析(DPA)攻撃により，未対策回路では，実際に共通鍵暗号回路の鍵は容易に窃取可能



# DPA対策回路例：2線式ロジック



- AND回路の横にダミーのORゲートを配置
  ⇒ LSIゲート出力の遷移確率50%



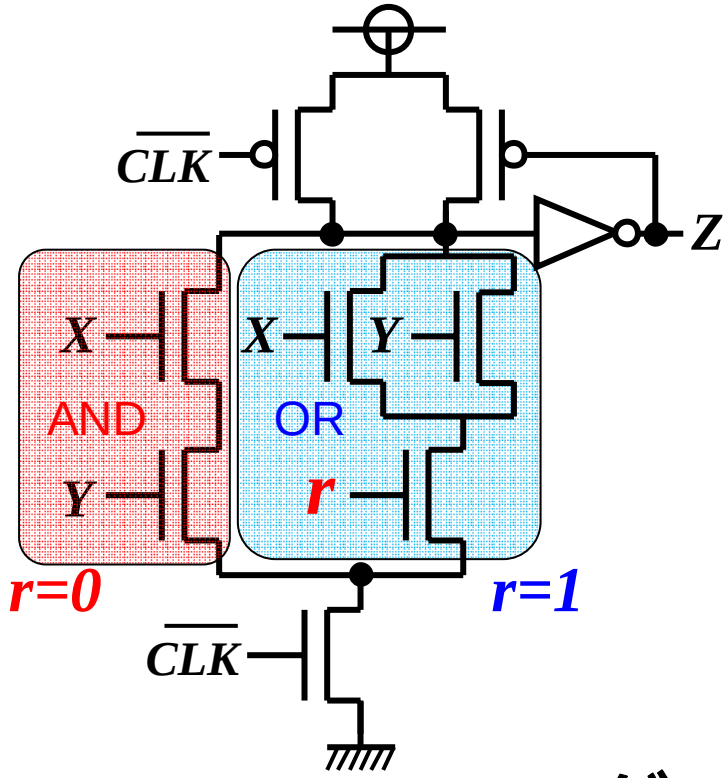

- 問題点
  - 遷移確率は一定になったが、***F***と***F(dum)***の負荷容量を一定にしないと消費電力が一定にならない
    ⇒LSI実装時の大きな制約

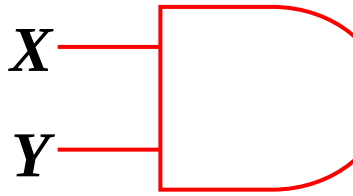
| | | | | AND | | OR | |
|---|---|---|---|---|---|---|---|
| A1 | B1 | A2 | B2 | F1 | F2 | F1 | F2 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

# DPA対策回路：RSL(Random Switching Logic)方式

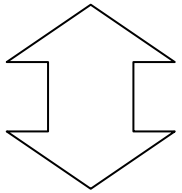
*Tamper Resistance*

- 乱数rでAND/ORが切り替わるRSL方式ゲート
  どんな入力値に対しても消費電力が均一になる



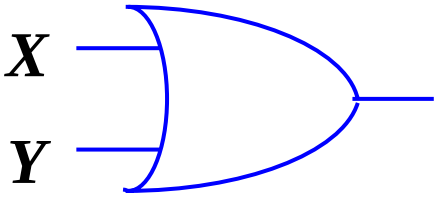




r=0



2線式ロジックと
同じ原理で
消費電力一定
(出力容量均一)

r=1



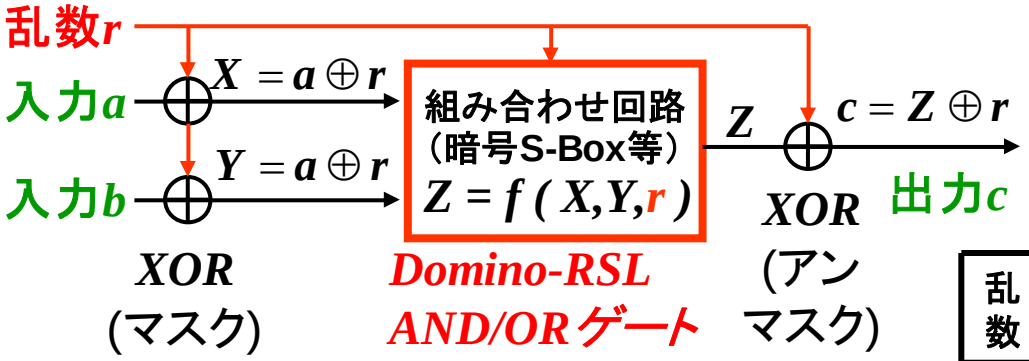

***Domino-RSL　AND/ORゲート***

＊DPA耐性の確認されている三菱電機考案RSLゲートと原理は同じ.
非同期enable信号が不要で，ゲート面積が小さい特長がある.

# RSL方式による演算



- 組み合わせ論理回路をDomino-RSL回路で構成し、その前後でマスク/アンマスク処理を実施することで正常演算可能




正論理 $A \cdot B = C$

$\overline{A} + \overline{B} = \overline{C}$ 負論理

| 乱数 | マスク処理前 | | 演算処理 | | | アンマスク処理後 |
|---|---|---|---|---|---|---|
| r | a | b | X | Y | Z | c |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 1 | 0 | 1 | 0 | 0 |
| | 1 | 0 | 1 | 0 | 0 | 0 |
| | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| | 0 | 1 | 1 | 0 | 1 | 0 |
| | 1 | 0 | 0 | 1 | 1 | 0 |
| | 1 | 1 | 0 | 0 | 0 | 1 |

AND演算

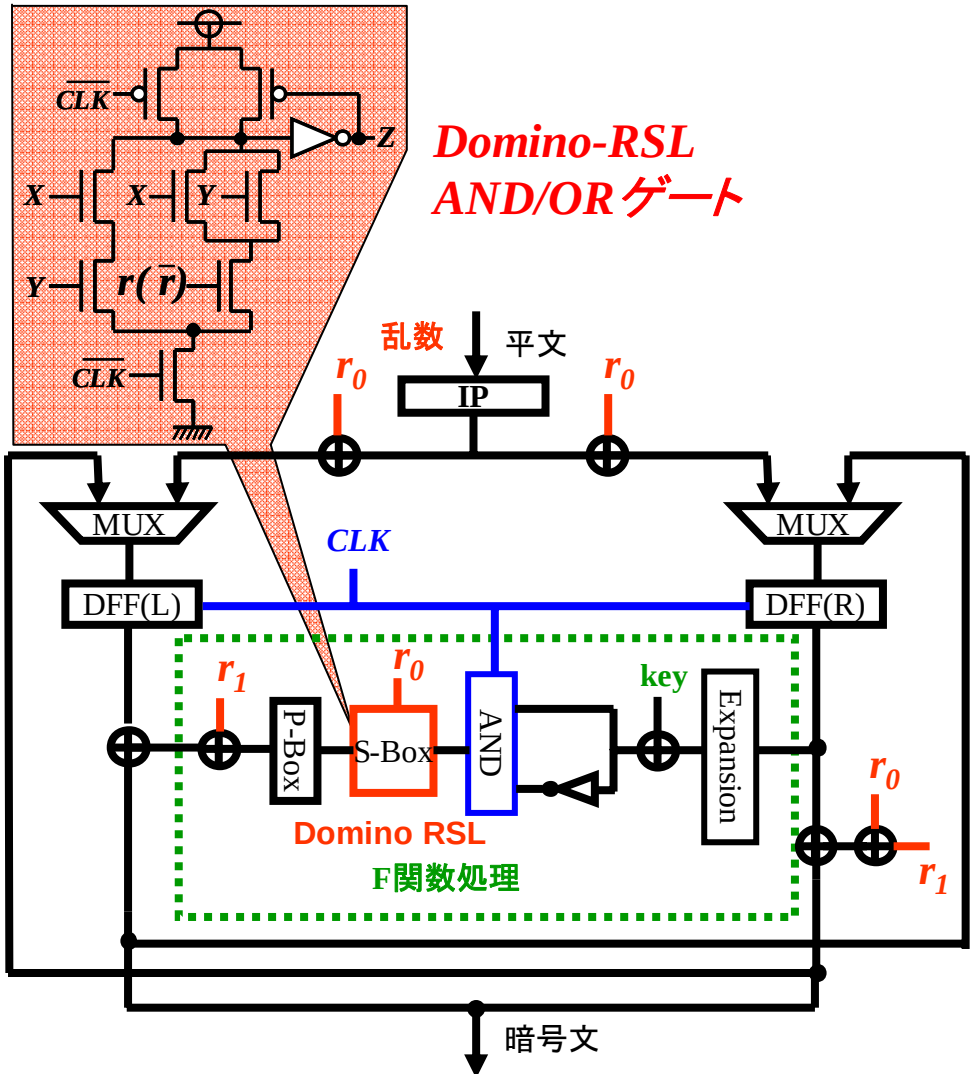
OR演算

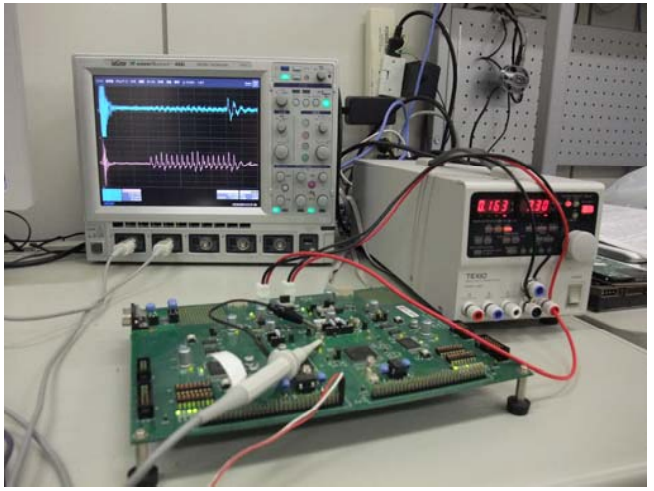
同一論理

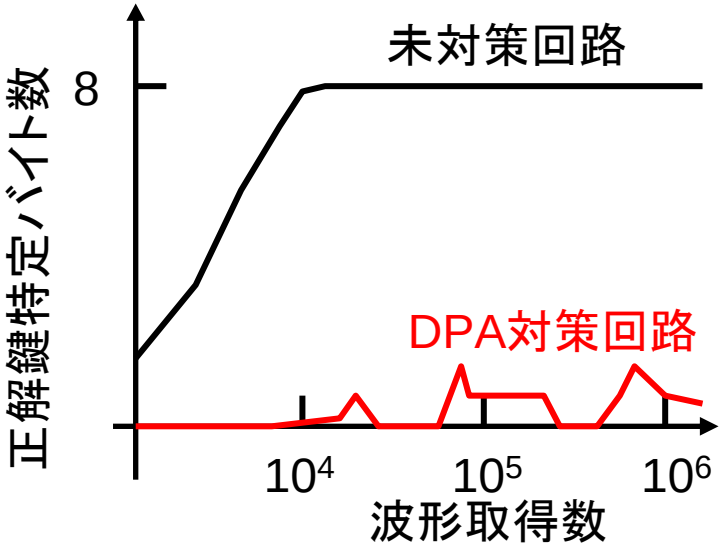
# 消費電力サイドチャネル攻撃耐性目標

*Tamper Resistance*

- Domino-RSLゲート使用暗号回路では約100万波形収集をおこなっても暗号鍵特定不可能を確認する



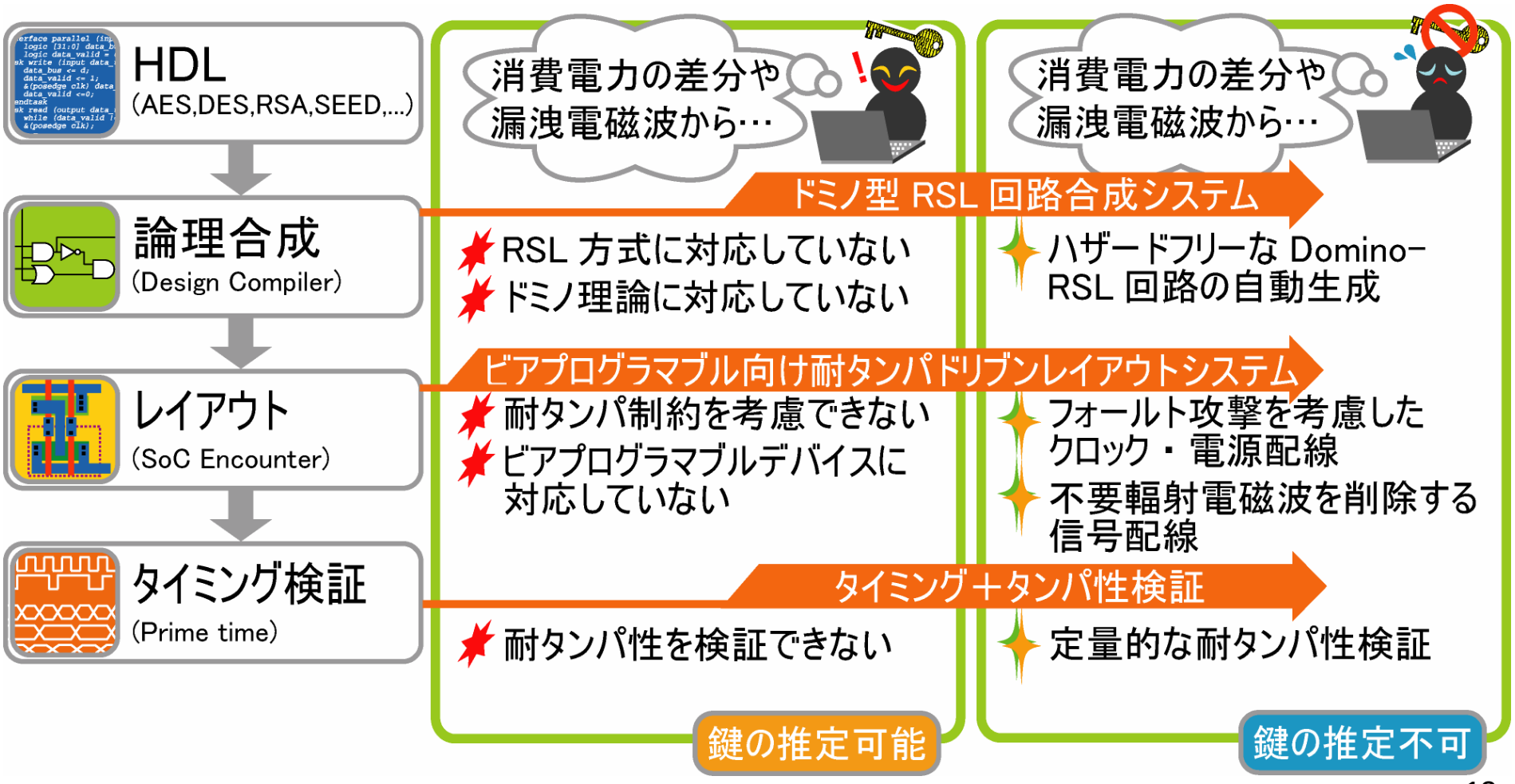





# Domino-RSLを用いたLSI設計環境

*Tamper Resistance*

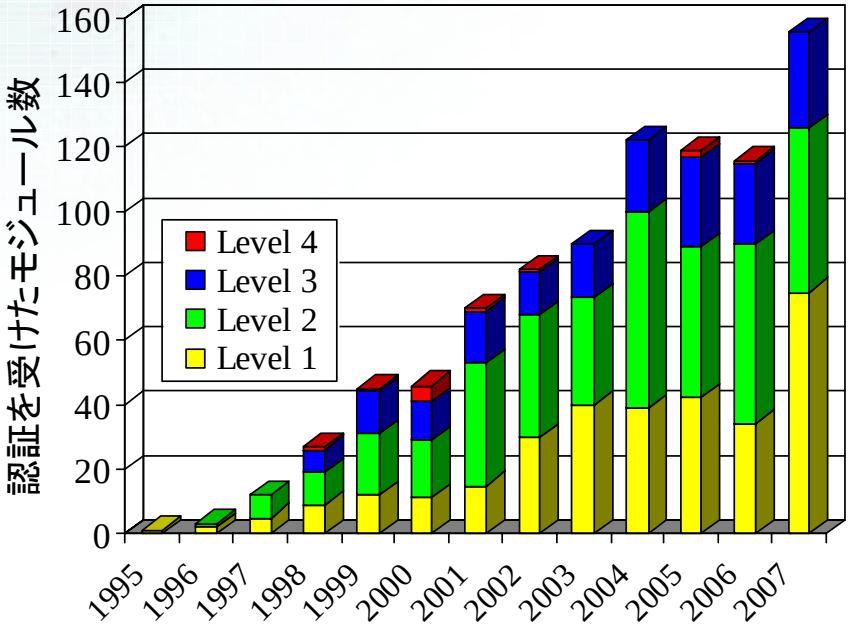
- HDL記述からレイアウト合成までの自動設計ツールと検証ツールフローを確立する



National Institute of Advanced Industrial Science and Technology
AIST

# 暗号モジュールの認証：FIPS 140–2

- 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

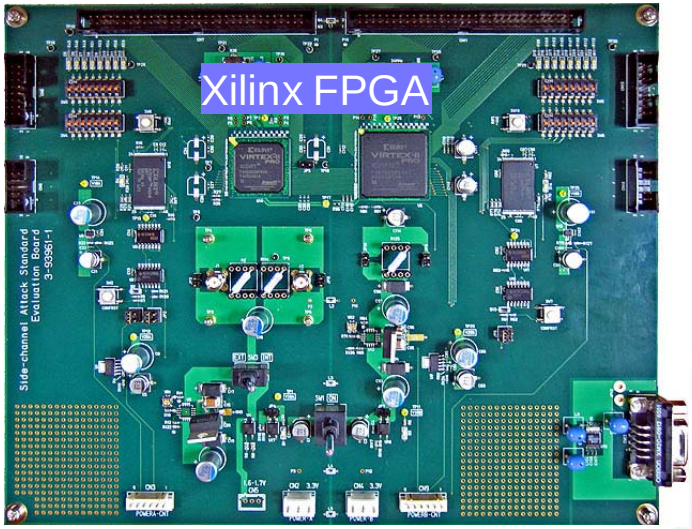



| | セキュリティ要件 | 規定内容 |
|---|---|---|
| 1 | 暗号モジュール仕様 | 暗号モジュールの仕様と「FIPS 140-2」の適用範囲 |
| 2 | 暗号モジュールのポート･インタフェース | 情報の入出力 |
| 3 | 役割，サービス，及び認証 | ユーザーの役割や役割ごとに提供されるサービス，ユーザーの認証方法 |
| 4 | 有限状態モデル | 状態遷移の記載 |
| 5 | 物理セキュリティ | 表面処理やカバー等の物理的セキュリティ要件 |
| 6 | 動作環境 | 暗号モジュールの動作環境 |
| 7 | 暗号鍵管理 | 鍵生成，鍵の入出力等 |
| 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

# 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 (Japan Cryptographic Hardware Module Validation Program)認証を取得




Side-channel Attack Standard Evaluation BOard


SASEBO-B

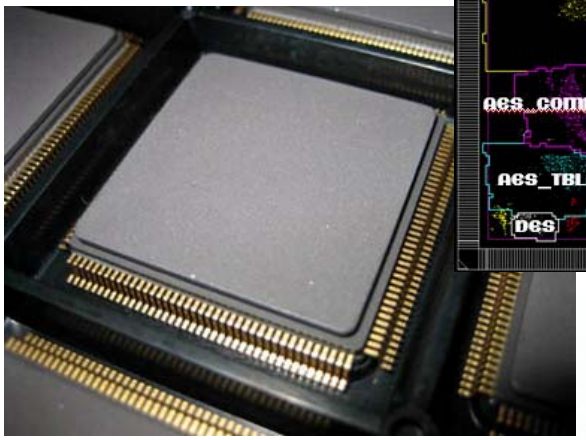

SASEBO-R

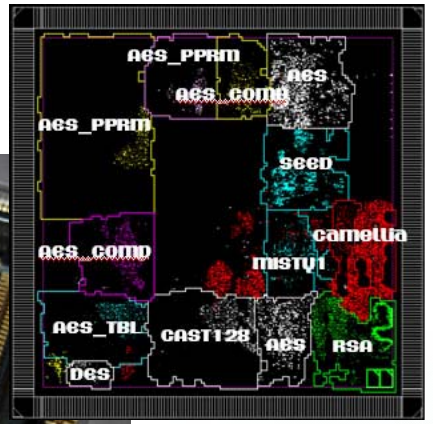

SASEBO-G

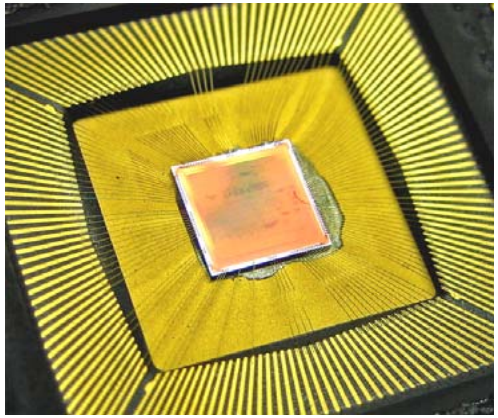
National Institute of Advanced Industrial Science and Technology
AIST

# タンパ性評価用標準暗号LSI

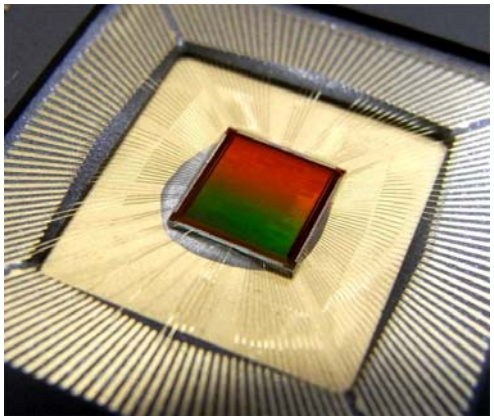
- 平成19年度に全てのISO/IEC標準ブロック暗号とRSA暗号を実装した130nm CMOSによる評価用LSIを開発
  - 128bit暗号：AES，Camellia
  - 64bit暗号：DES，MISTY1，SEED，CAST128
- 平成20年度は各種DPA対策を施したAES回路(横浜国立大学提供)や楕円曲線暗号(電気通信大学提供)を実装した130nmと90nmの2種類のLSIを開発



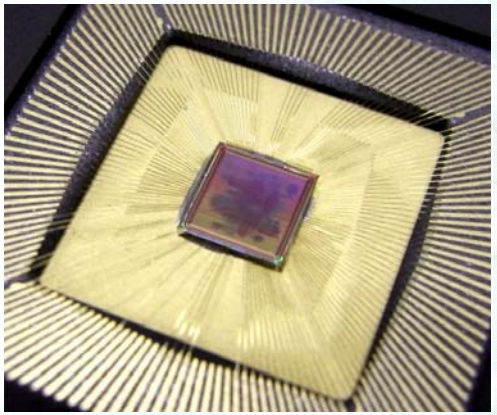


標準暗号LSI (130nm)



DPA対策版LSI (130nm)

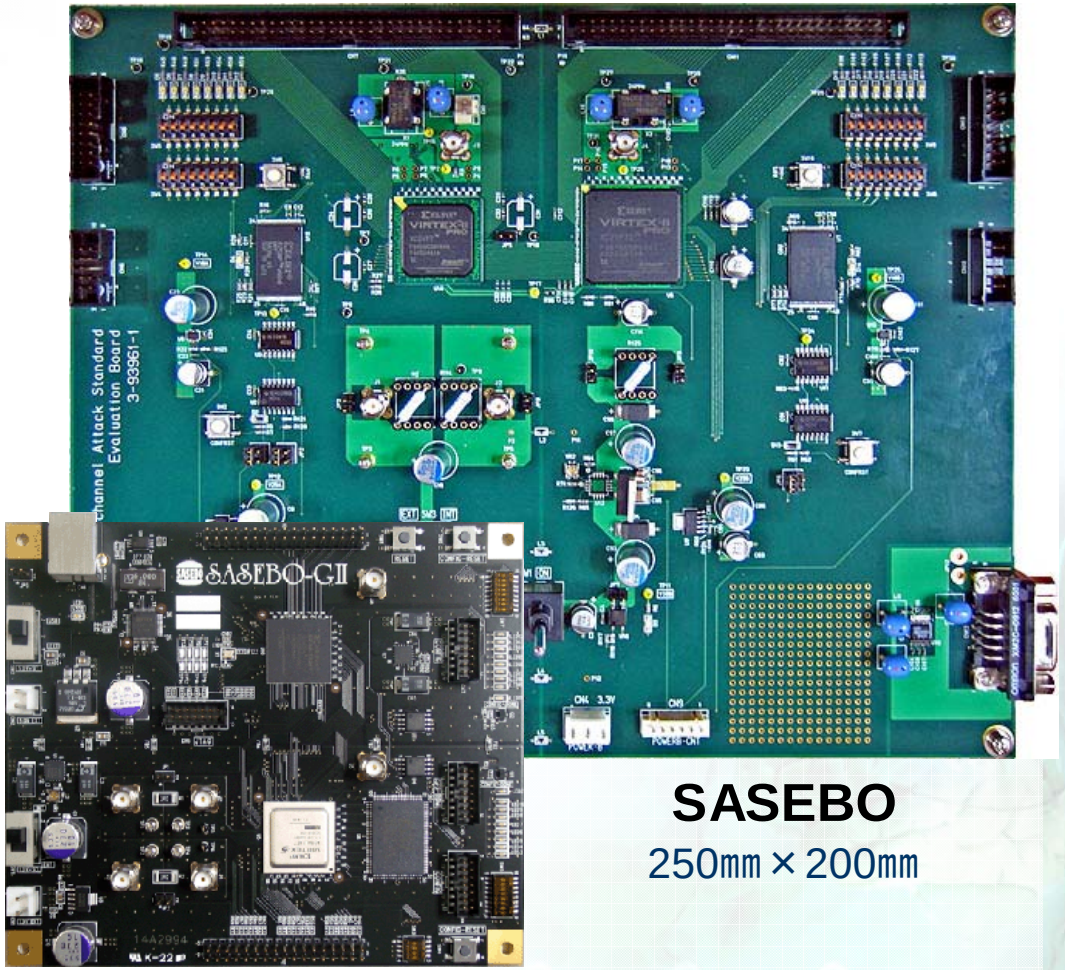


DPA対策版LSI (90nm)

National Institute of Advanced Industrial Science and Technology
AIST

# 普及版タンパ性評価FPGAボード SASEBO-GII

- 小型・高性能ボードSASEBO-GIIを用いた研究とビジネス
  - 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
  - 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，東京エレクトロンデバイスから商用として2009/1月に販売
    - ロジック容量は4~7倍
    - ボードサイズが1/3
    - 電源・クロック系のノイズ低減
    - 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

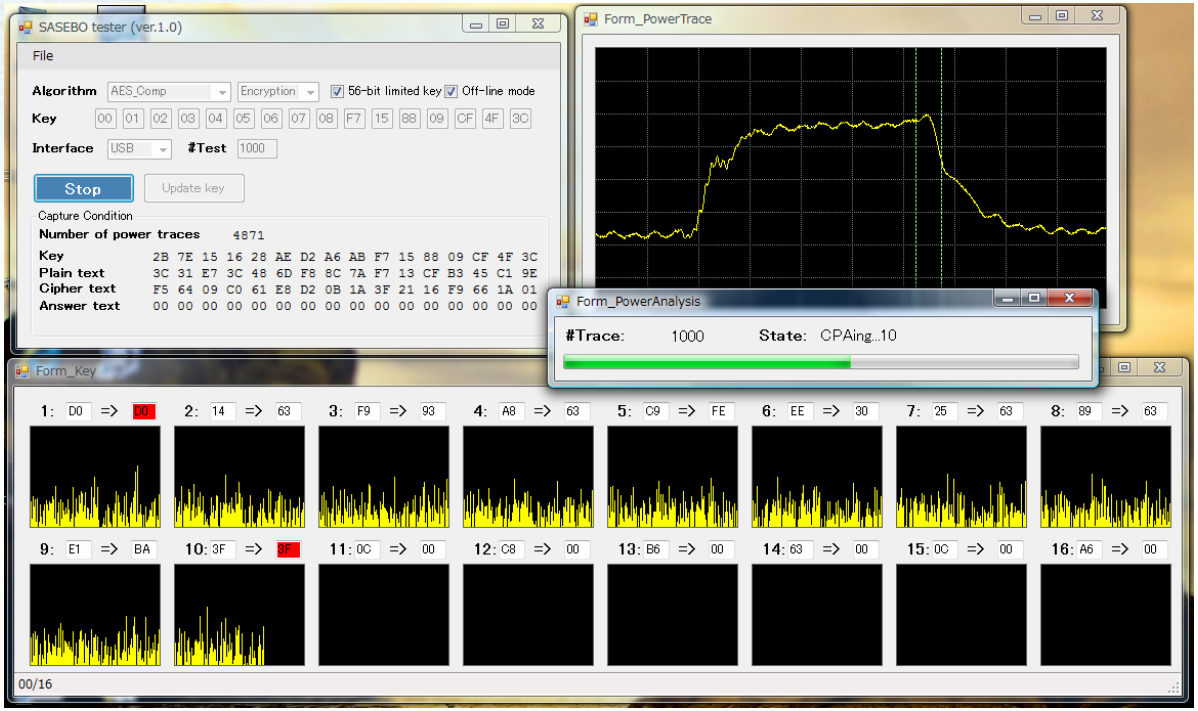


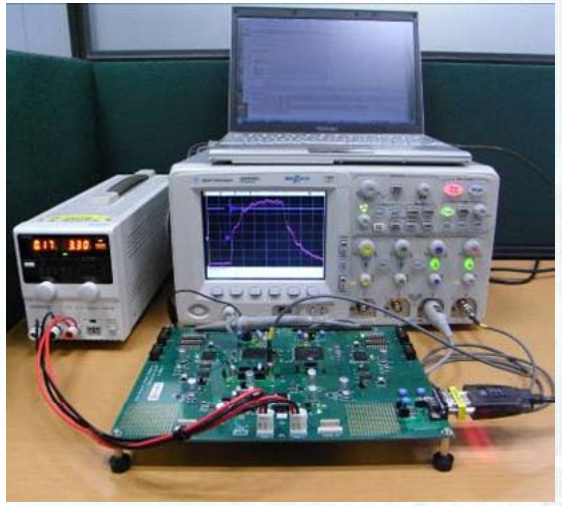

**SASEBO**
250㎜×200㎜

**SASEBO-GII**
140㎜×120㎜

# 耐タンパ性測定環境・解析ツールの開発

- 試験機関で統一された安全性評価を行うために，測定環境の統一化を図り，様々な評価（攻撃）手法をガイドラインとして定めるとともに，それを実装した自動評価ツールのプロトタイプを開発
- 同じツールを用いても，解析結果は測定環境や試験者のスキルに大きく依存するので，SASEBOに暗号回路を実装し，それを解析するテストにより試験機関のレベルをそろえる
- 試験環境ツールのサポート体制の強化のため，国内外のボードメーカーやICカード評価ツールメーカーと協力

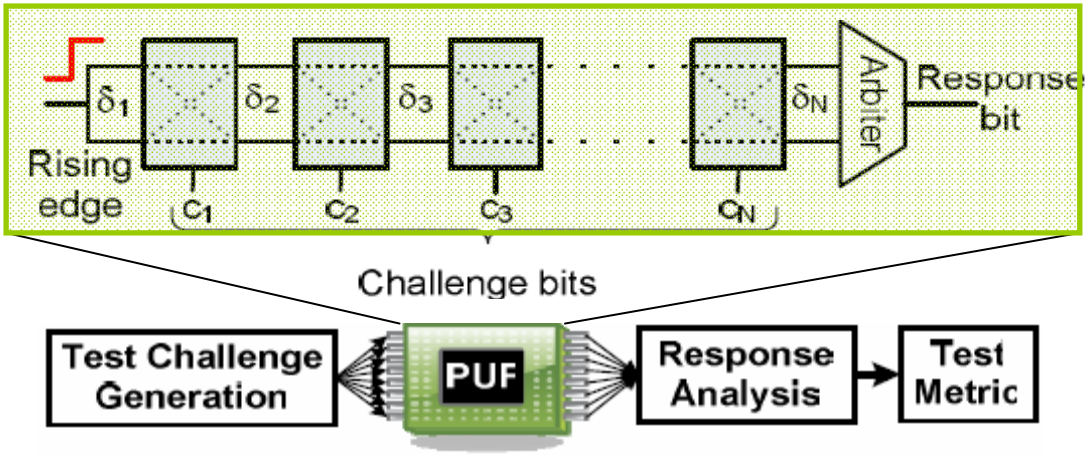


# PUF（Physically Unclonable Function）とは？

*Tamper Resistance*

- 人工物メトリックスによる真贋判定：人の指紋のように紙の模様・磁気体の磁力ムラなど人工物の偶然にできるパターンを活用
- LSIにおいてもトランジスタや配線の製造時のばらつきを利用し，ハードウェアの個体を判別する技術PUF（Physically Unclonable Function ）の研究が開始.
- LSIのパターンが丸ごと不正にコピーされても，本物と偽物の区別が可能であることからICカードの偽造対策等に有望.



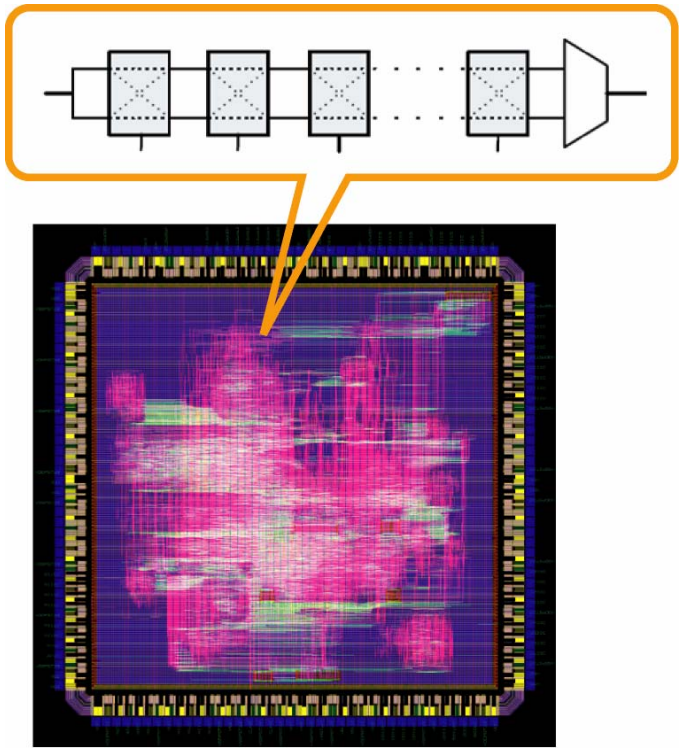

セレクタチェインによる信号遅延を利用したPUF回路

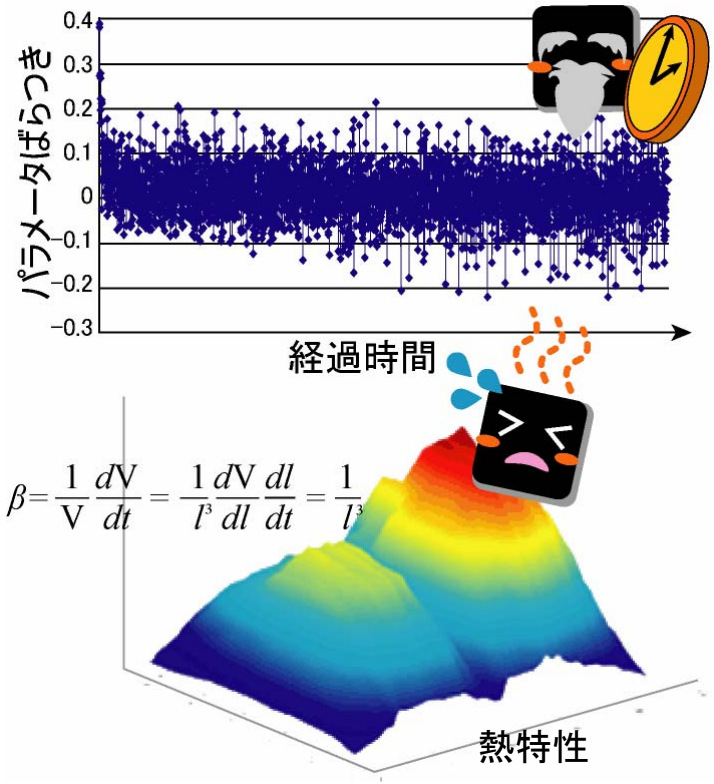
（引用）M.Majzoobi et. al. : International Test Conference 08, Paper31.3

# PUFデバイス回路設計と特性評価の定式化

*Tamper Resistance*

- 様々なTEGについて各種物理的特性を測定し，熱の影響や経時変化を考慮した特性ばらつきにモデル化・定式化を行う（シミュレーションとTEG試作）
- セレクタチェインをベースとするフィードフォワードループ追加等様々な回路を実装し，物理特性パラメータの測定・評価を行う（FPGA検証）

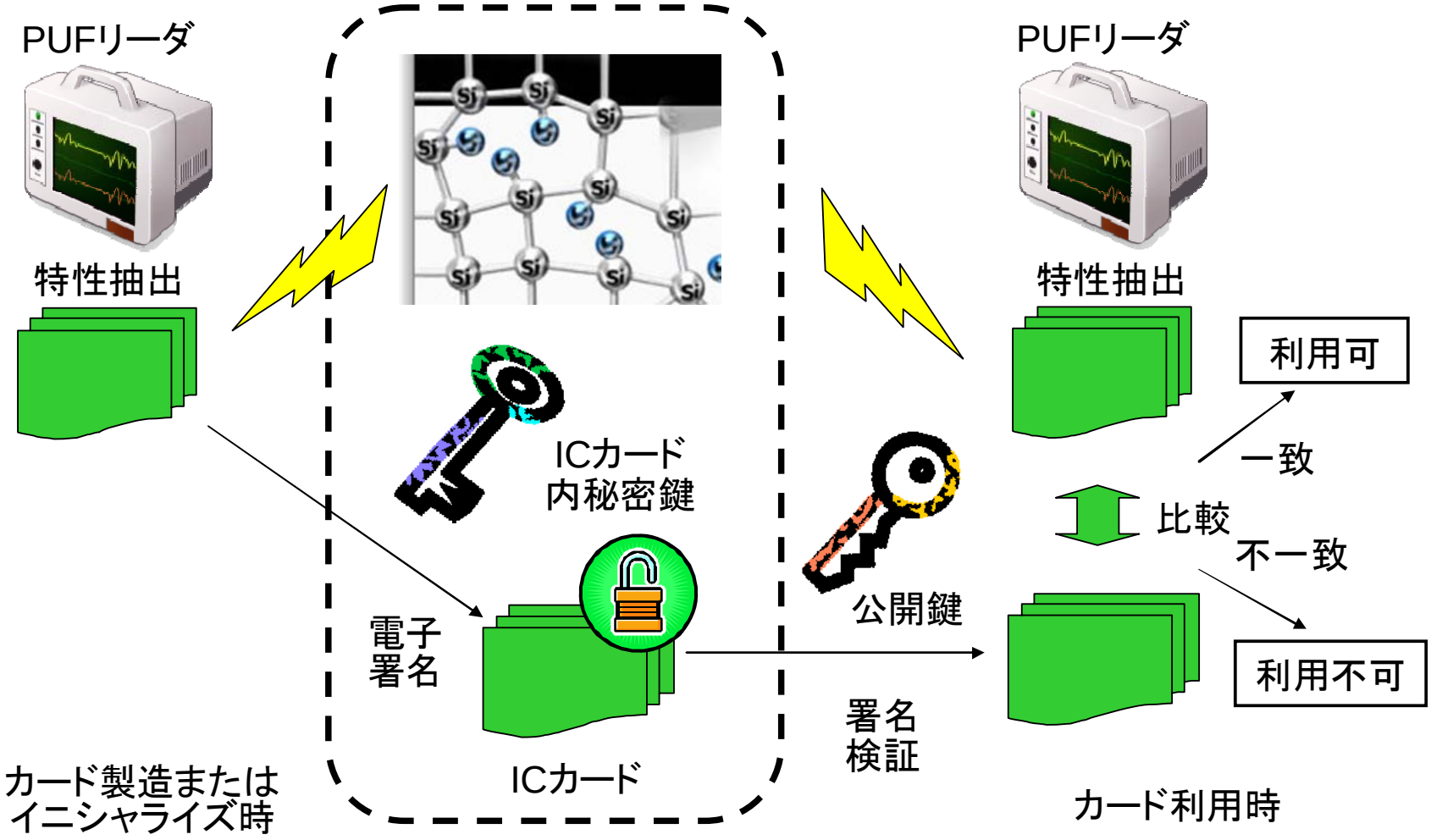




# PUFと暗号技術を融合した偽造防止システム

*Tamper Resistance*

- ICカード等の実システムにおいてPUFを利用するため，暗号技術と融合した利用方式の提案と評価を行う



# 研究役割分担体制

*Tamper Resistance*

| | 専門分野 | 耐タンパ性LSI設計ﾌﾟﾗｯﾄﾌｫｰﾑ | 耐タンパ性性能評価ﾌﾟﾗｯﾄﾌｫｰﾑ | PUFﾃﾞﾊﾞｲｽ使用ｾｷｭﾘﾃｨｽｼﾃﾑ |
|---|---|---|---|---|
| 立命大 | プログラマブルLSI設計と回路設計 | 耐タンパプログラマブルLSIマクロ設計 | ｻｲﾄﾞﾁｬﾈﾙ攻撃実験評価 | PUFデバイスの回路実装 |
| 産総研 | LSI論理設計と各種攻撃評価システム | | 各種評価ボード設計と評価 | PUFﾃﾞﾊﾞｲｽ設計とPUF利用ｾｷｭﾘﾃｨｰｼｽﾃﾑ構築 |
| 中央大 | 暗号アルゴリズムとLSI論理設計 | フォールト攻撃対策検討 | ｻｲﾄﾞﾁｬﾈﾙ攻撃/フォールト攻撃実験評価 | |
| 名城大 | プログラマブルLSI設計CAD構築 | 耐タンパLSIマクロ設計CAD構築 | | |