

# 耐タンパディペンダブル VLSIシステムの開発・評価

*Tamper Resistance*

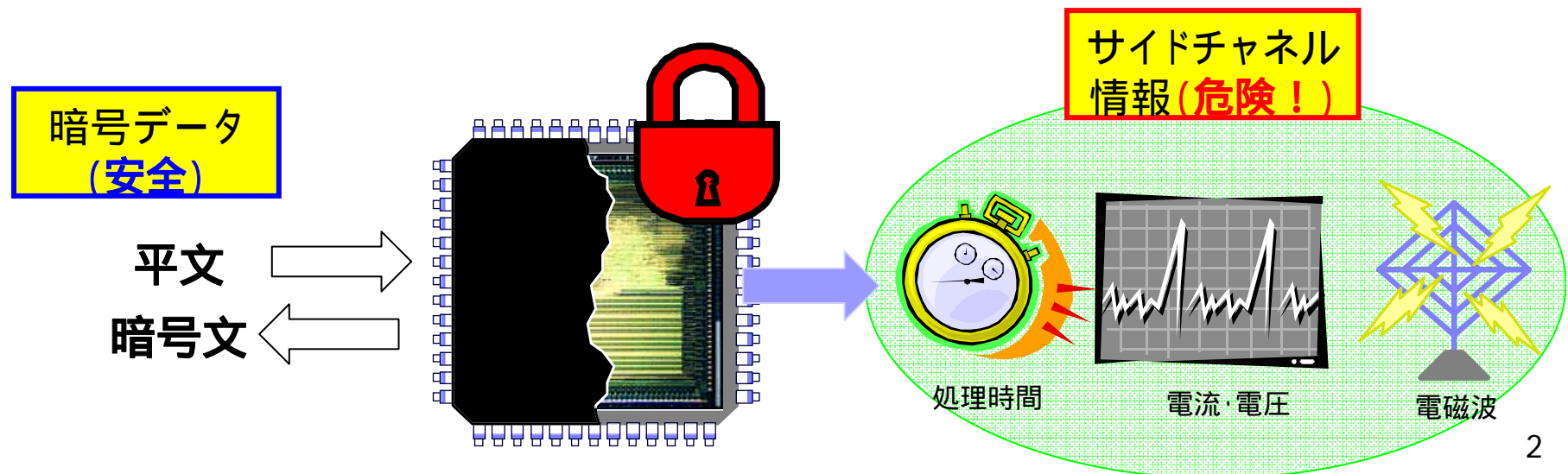
～ 人為的攻撃による内部機密情報の  
漏洩・複製を防止するVLSIの実現～

立命館大学・産総研・中央大学・名城大学

# 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

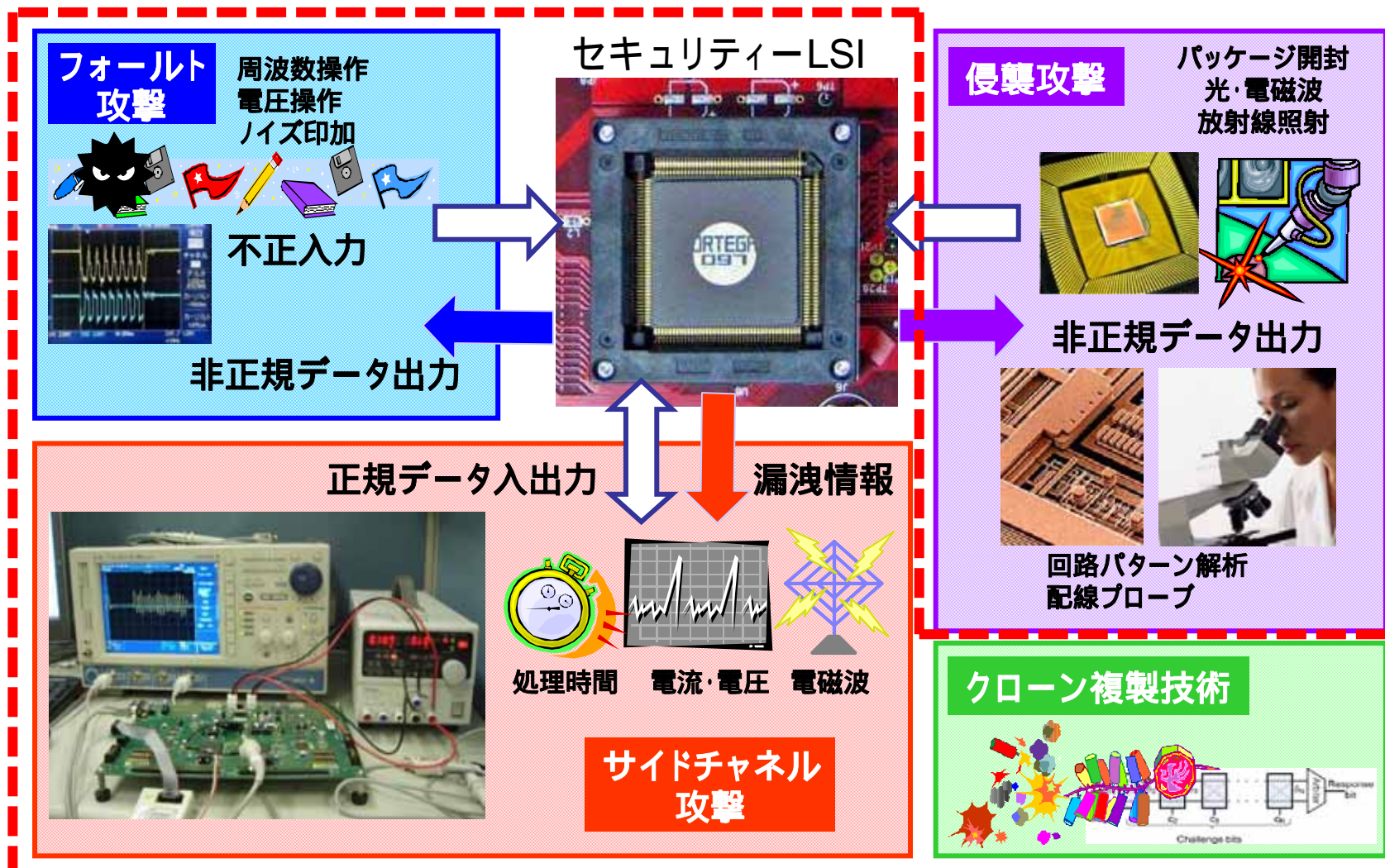


# 耐タンパディペンダブルLSIの要件

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

本研究の領域



# 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

立命館・名城

- 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

産総研・中央

- 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

# 報告内容(立命・名城G)

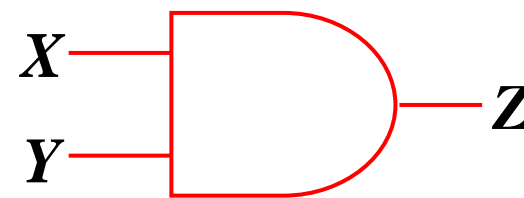
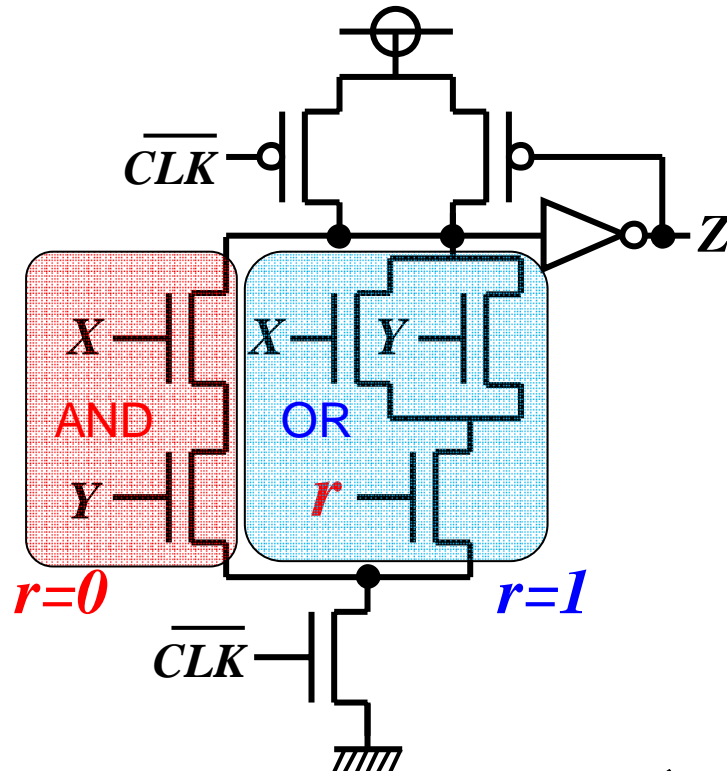
*Tamper Resistance*

- 耐タンパLSI設計プラットフォーム成果
  - DPA攻撃対策回路(Domino-RSL方式)
  - F P G Aを用いたDPA耐性の検証(DES回路)
  - Domino-RSL方式チップ試作(Simplified DES回路)
- PUF回路設計成果
  - アービターPUF回路
  - ゲート長ばらつきを用いたPUFのシミュレーション
  - アービターPUFのチップ試作
- 今後の課題と対応
  - 耐タンパ性検証ツール
  - Domino-RSL方式のDEMA評価・非接触ICカード試作
  - 産業界への貢献とヒアリング

# DPA攻撃対策回路: Domino-RSL方式

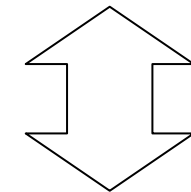
*Tamper Resistance*

- 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

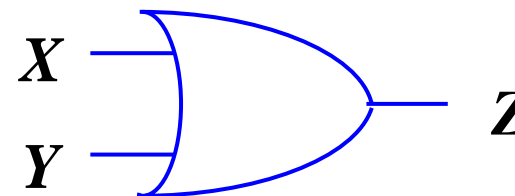


$r=0$

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*

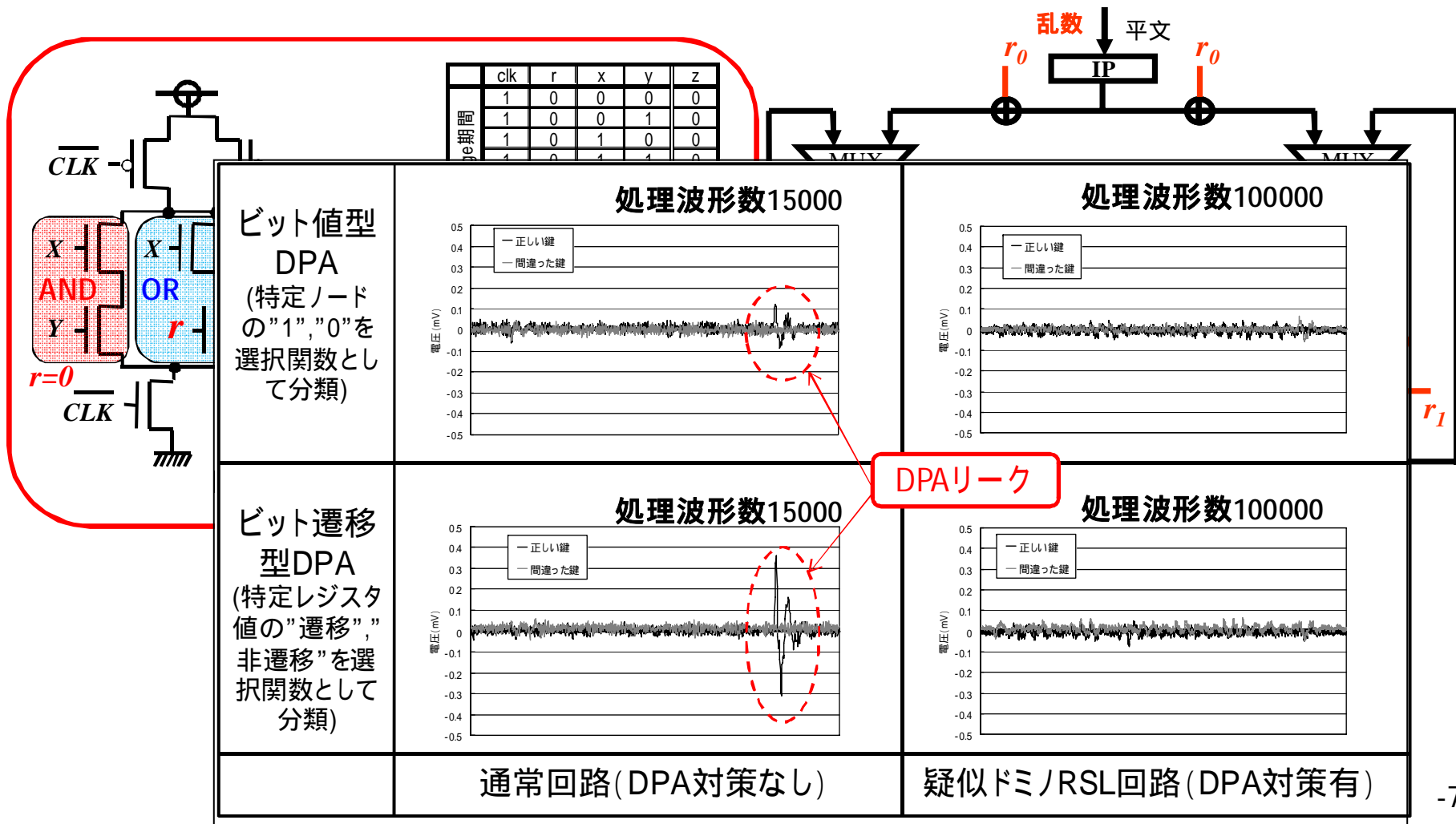
\* DPA耐性の確認されている三菱電機考案RSLゲートと原理は同じ。  
非同期enable信号が不要で、ゲート面積が小さい特長がある。



# FPGAを用いたDPA耐性の検証 (DES回路)

*Tamper Resistance*

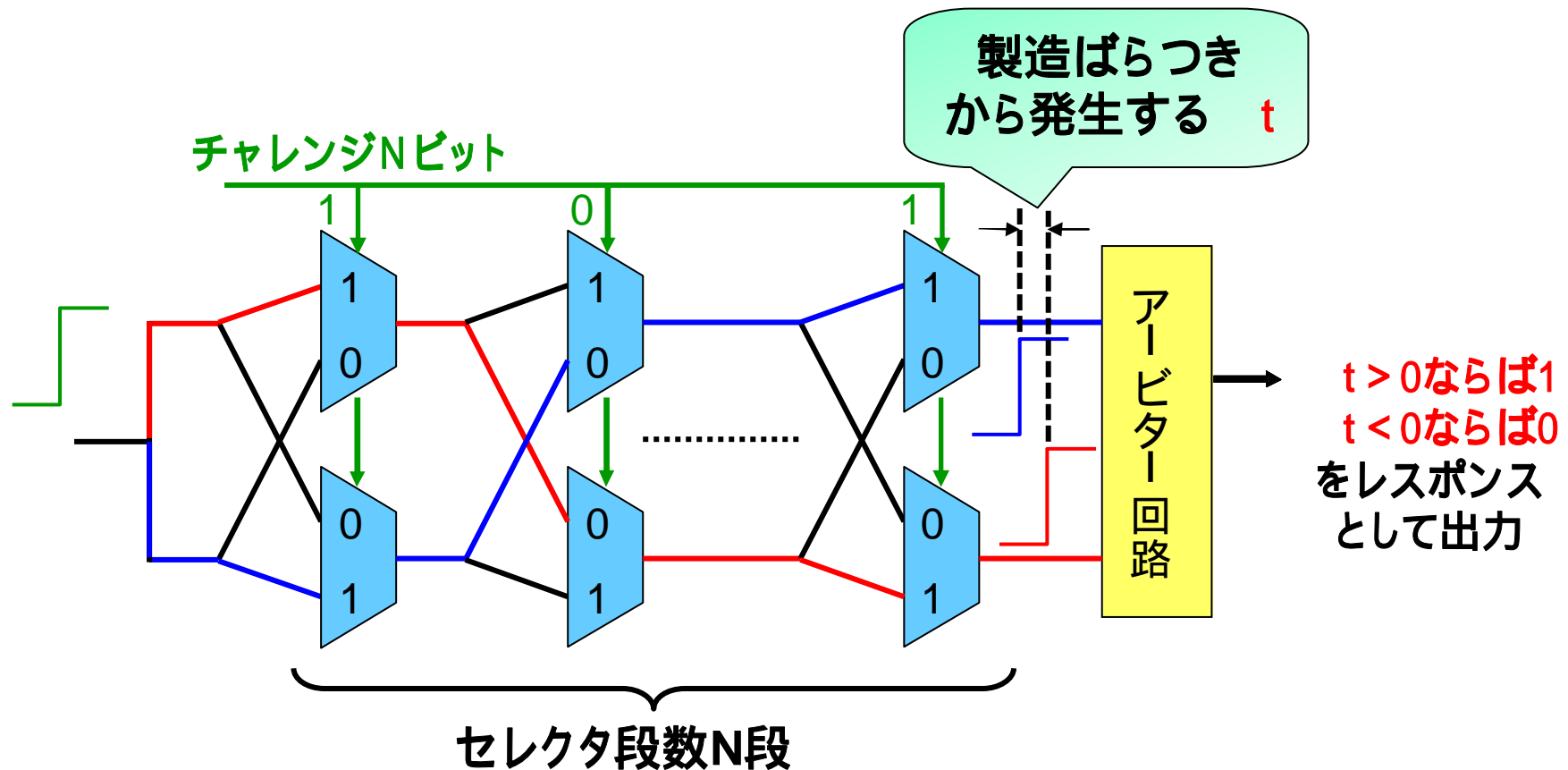
- DES暗号回路で、疑似“ドミノRSL回路”を実装し、DPA耐性検証を確認した (SCIS2010発表)



# アービターPUF回路

*Tamper Resistance*

- チップ製造時のトランジスタのゲート遅延のばらつきを用いて複製不可能な固有IDを生成

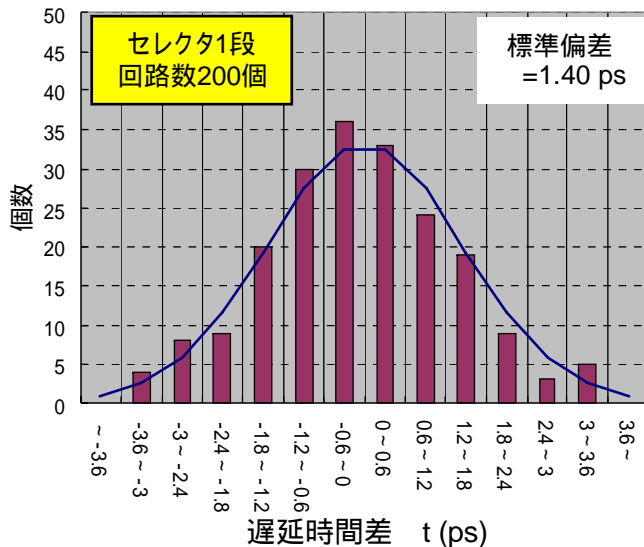
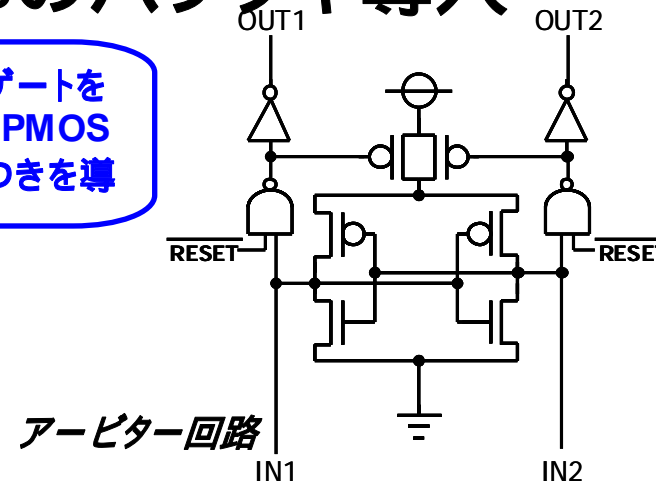
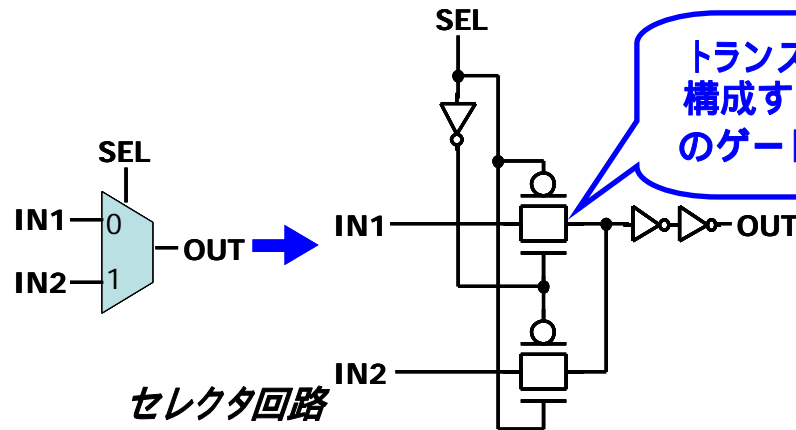




# ゲート長ばらつきを用いたPUFのシミュレーション

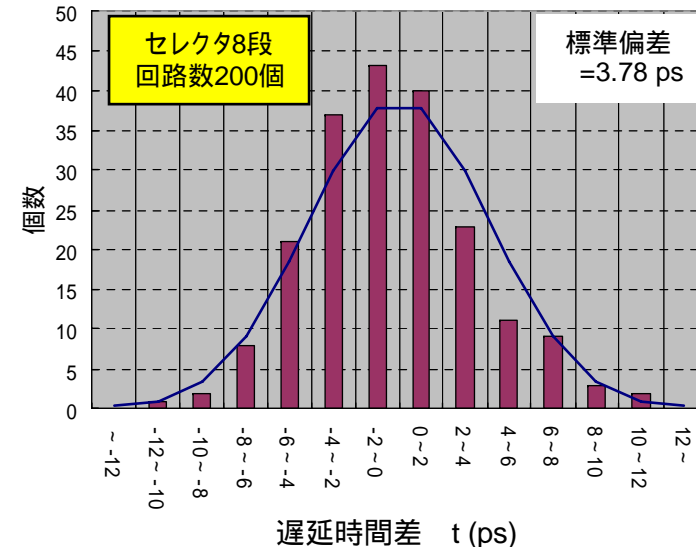
*Tamper Resistance*

- セレクタを構成しているトランスミッションゲートのトランジスタゲート長に3%のバラツキを導入



2 2倍

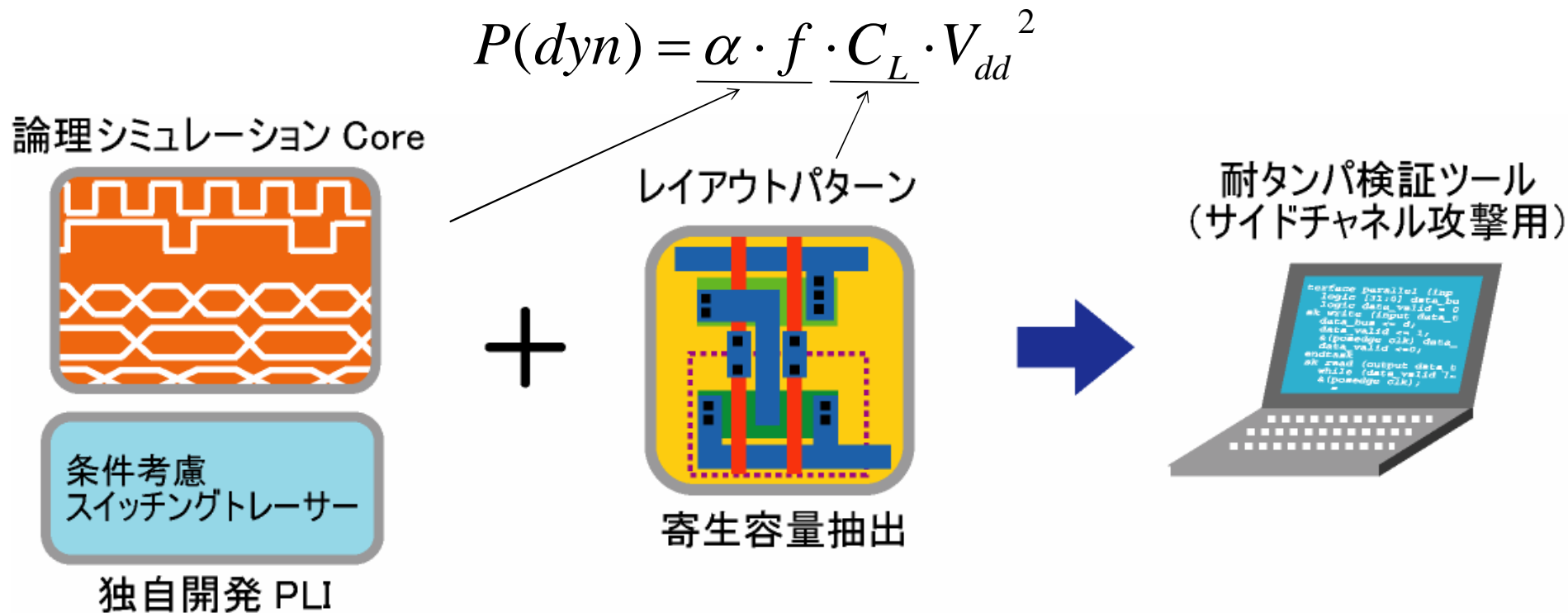
セレクタ段数Nに  
対して  
遅延時間差 tの  
分布の標準偏差  
は約  $\sqrt{N}$  倍



# DPA耐性検証ツール(1)

*Tamper Resistance*

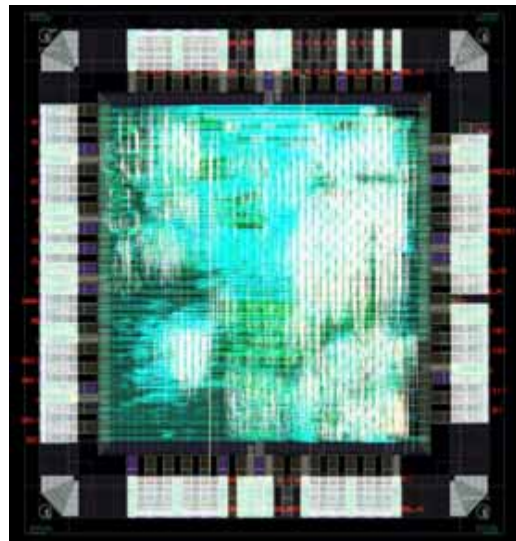
- LSI設計データから回路ノードの寄生容量や、遷移確率・遷移タイミングを抽出し、DPA耐性を検証できるCADツールを開発する。



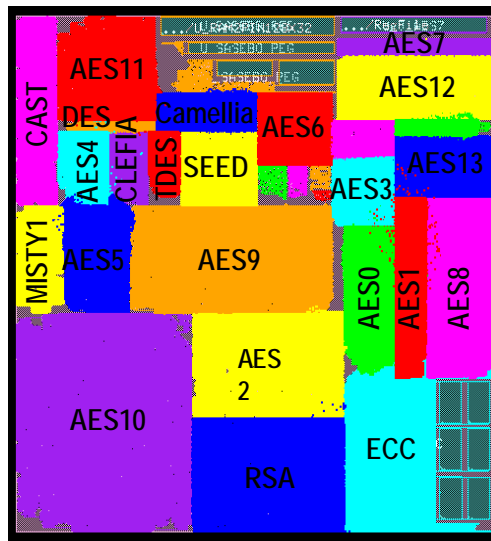
スイッチング確率と寄生容量を用いた耐タンパ性検証ツール

# 耐タンパ性能評価用標準暗号LSIの開発

- ISO/IEC 15033-3標準ブロック暗号や公開鍵暗号等23種類の暗号マクロを搭載したLSIをeシャトル 65nmを用いて設計
- 2010年9月上旬納品の後にはサイドチャネル攻撃・フォルト攻撃実験の予定
- 搭載マクロ(東北大・横浜国立大・電通大の協力)
  - ブロック暗号: AES(4種類のS-box, 6種類の対策, 等14種類) Camellia, SEED, MISTY1, CAST128, DES, Triple-DES, CLEFIA(次期電子政府推奨暗号候補)
  - 公開鍵暗号: RSA, ECC



標準暗号LSI



暗号マクロ配置図

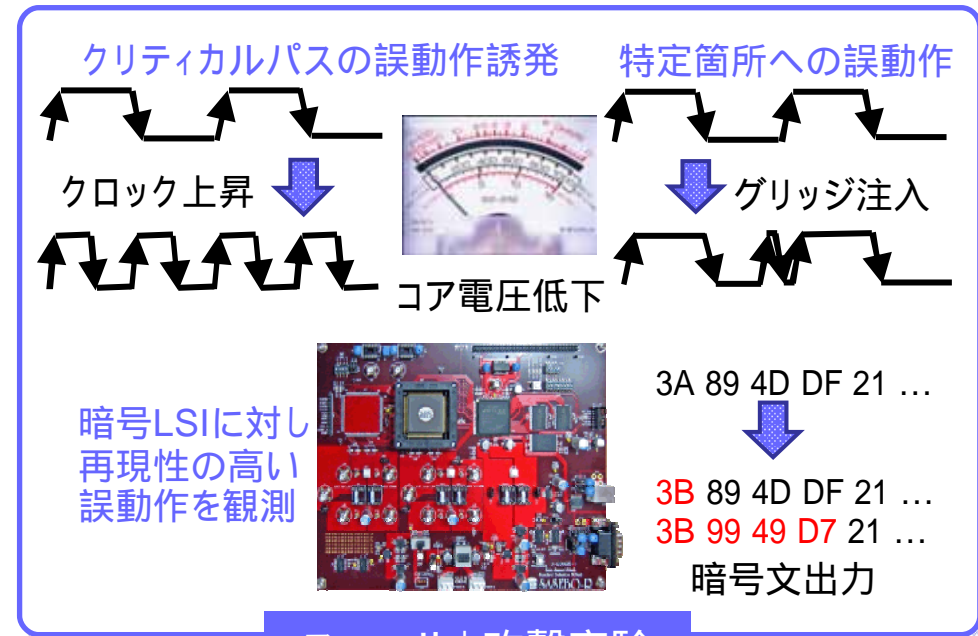
ライブラリ	富士通e-shuttle CS202(LVt)
プロセス	65nm CMOS
置配線層	メタル12層
ダイサイズ	2.1mm x 2.1mm
パッケージ	セラミックQFP 160pin
セル面積	1,404,242 $\mu\text{m}^2$
ゲート数	731,376 2-NAND gates
セル使用率	77.72 %
動作周波数	35.1 MHz

# サイドチャネル攻撃・フォールト攻撃

- 電力・電磁波解析攻撃のための計測環境を構築
  - 複数のオシロスコープへの対応
  - 各種磁界プローブによる評価実験
  - 暗号回路制御および電力・電磁波測定ソフトウェアの開発
- クロック制御とコア電圧低下の組み合わせにより、暗号LSIで再現性の高いエラーの誘発に成功
  - FPGAは電圧低下により動作が停止、クロック制御による誤動作のさらなる検討が必要
  - エラーデータを用いた秘密鍵導出の論理的解析手法の研究が重要



サイドチャネル実験環境構築



フォールト攻撃実験

# PUFの性能評価基礎実験

- FPGA上にArbiter PUFを構築し性能を評価
  - 同一デバイス内での ID の再現性
  - 異なるデバイス間での ID の差異性
  - 128 bit ID の 0/1 の偏り
- デバイス間で出力に差異があり, 識別子として利用可能
- エントロピーが小さく, 出力bit数を長くする必要あり
- 誤り訂正符号と組み合わせることでエラーの低減

