National Institute of
Advanced Industrial Science
and Technology
AIST

Research Center for
Information Security

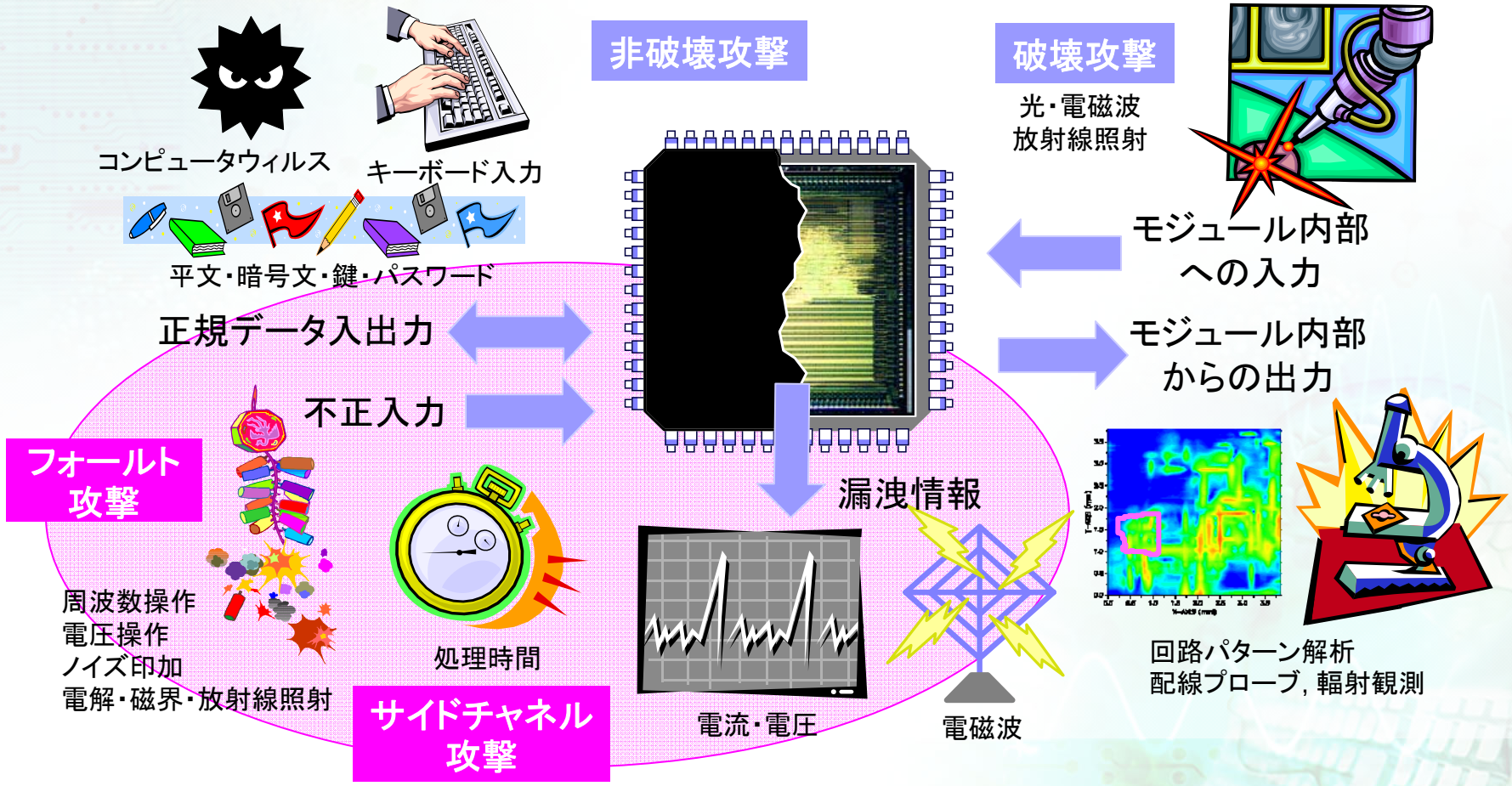
暗号モジュールの実装の安全性評価

(独)産業技術総合研究所
情報セキュリティ研究センター
佐藤　証

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

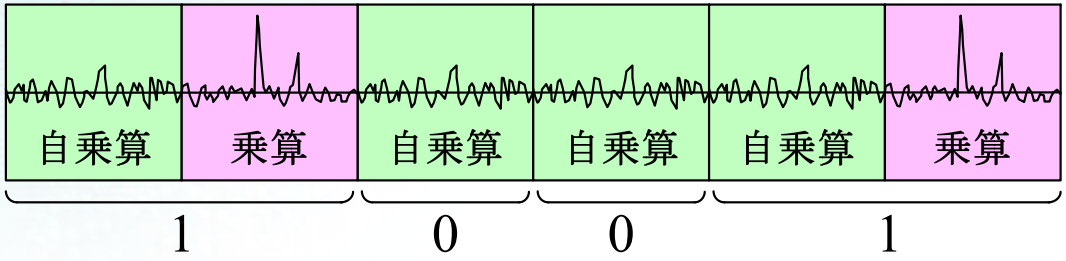


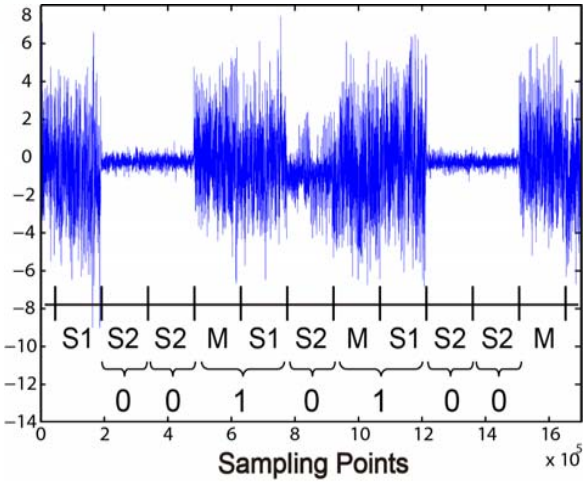
National Institute of Advanced Industrial Science and Technology
AIST

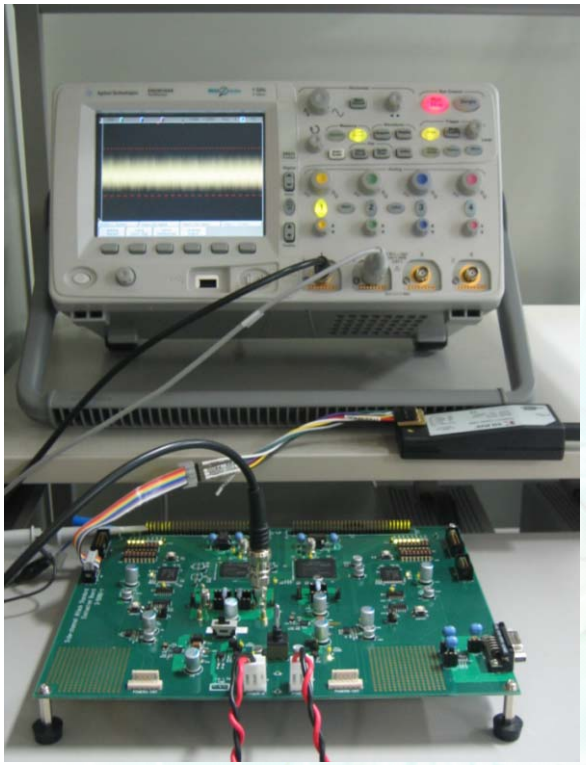
単純電力・電磁波解析

- 単純電力解析 (SPA : Simple Power Analysis)
- 単純電磁波解析 (SEMA : Simple Electromagnetic Analysis)
- データの違いにより特異なパターンを示す電力・電磁波から内部動作を解析

$$x^{11001_{(2)}} = (((x^2 \times x)^2)^2)^2 \times x$$





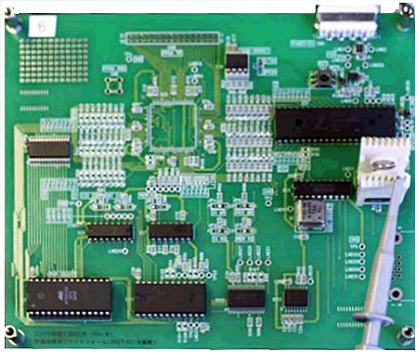


SASEBO上のHW実験

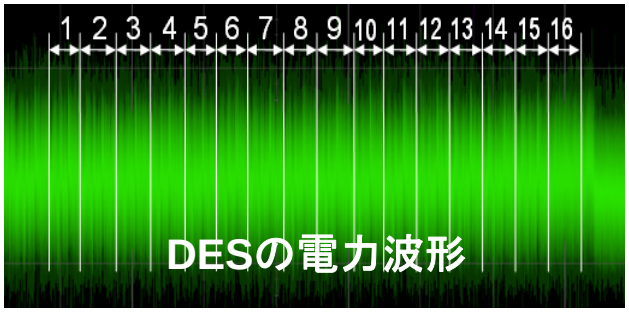
National Institute of Advanced Industrial Science and Technology
AIST

差分電力・電磁波解析

- 差分電力解析 (DPA : Differential Power Analysis)
- 差分電磁波力解析 (DEMA : Differential ElectroMagnetic Analysis)
  - 共通鍵暗号で鍵に依存する処理の電力・電磁波形は微弱で1波形では観測できない
  - 数千～数万波形を集め，推定した鍵情報を基に複数グループに分類
  - 鍵の推定が正しければ，波形を平均することで鍵情報が増幅されるピークが出る

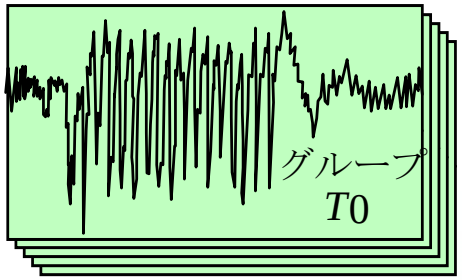


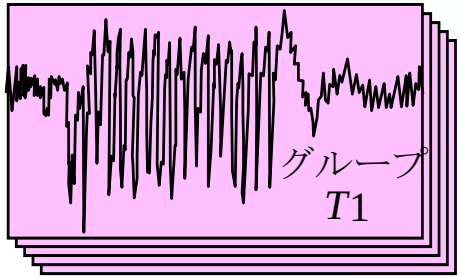
INSTAC-8上のSW実験



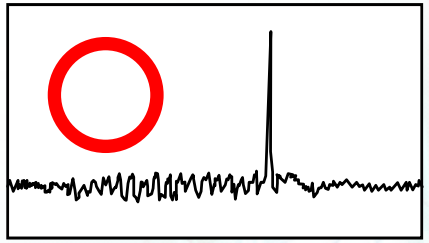
数千～数万
波形取得

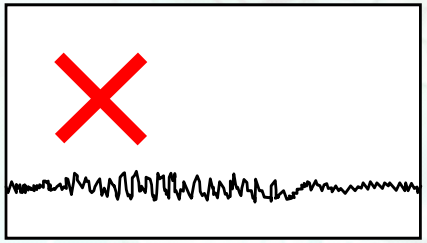
鍵を推定して分類





推定が正しければ
ピークが出る

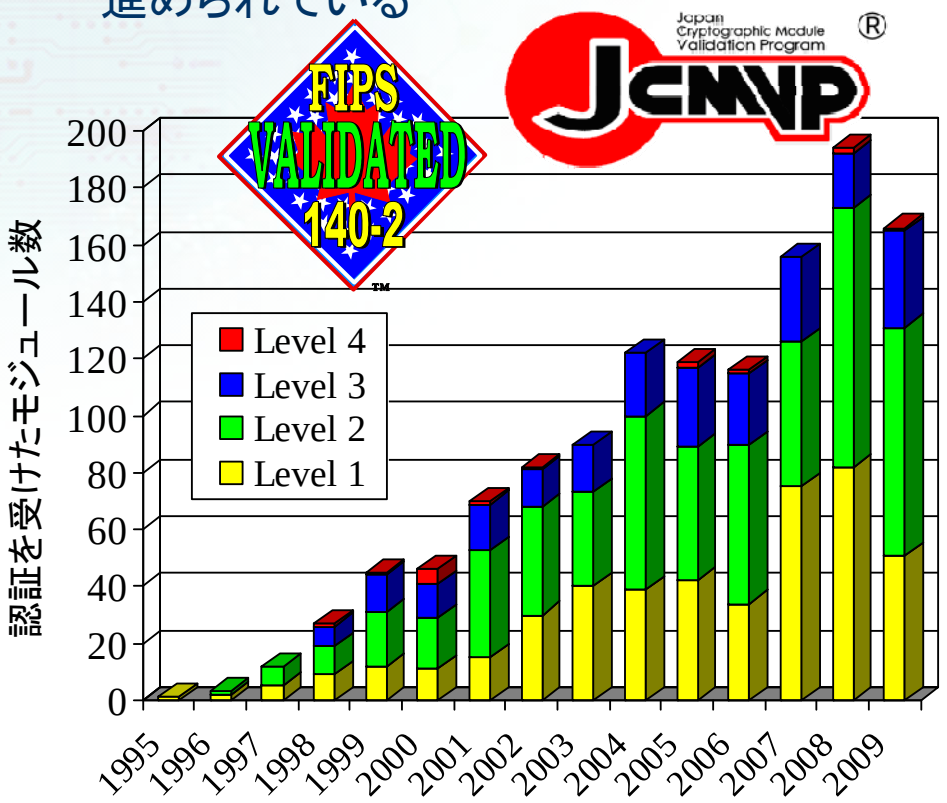




National Institute of Advanced Industrial Science and Technology
AIST

暗号モジュールのセキュリティ要件

- 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の国内評価試験制度JCMVPがIPAで運用されている
- 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
- サイドチャネル攻撃を取り込んだFIPS140およびISO/IEC 19790への改定作業が進められている



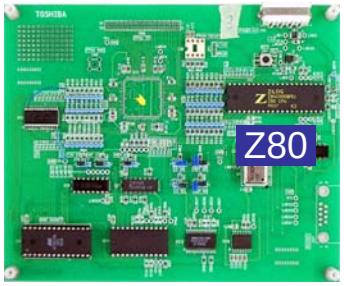
	セキュリティ要件	規定内容
1	暗号モジュール仕様	暗号モジュールの仕様と「FIPS 140-2」の適用範囲
2	暗号モジュールのポート･インタフェース	情報の入出力
3	役割，サービス，及び認証	ユーザーの役割や役割ごとに提供されるサービス，ユーザーの認証方法
4	有限状態モデル	状態遷移の記載
5	物理セキュリティ	表面処理やカバー等の物理的セキュリティ要件
6	動作環境	暗号モジュールの動作環境
7	暗号鍵管理	鍵生成，鍵の入出力等
8	電磁妨害／電磁両立性(EMI/EMC)	電磁波に対する要件
9	自己テスト	暗号モジュールの正しい動作を確認するテスト
10	設計保証	ガイドライン等
11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

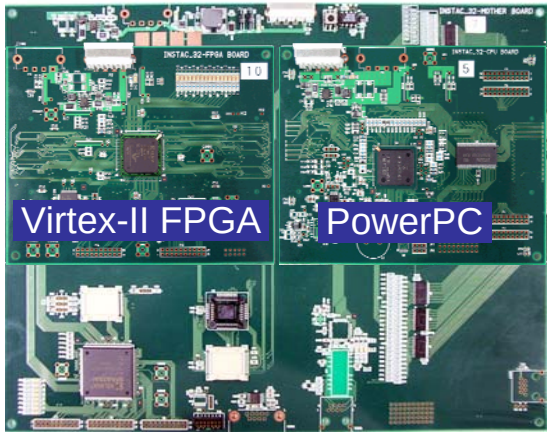
標準評価プラットフォームの開発

- 各研究機関が独自の環境で実験を行っていたため，第三者による検証・追試ができず，標準評価指針の策定が困難であった
- 標準評価プラットフォームを開発し企業・大学の研究機関へ配布
  - 日本規格協会情報技術標準化研究センター (INSTAC)
    - INSTAC-8/-32
  - 産総研
    - SASEBO-R/-B/-G/GII

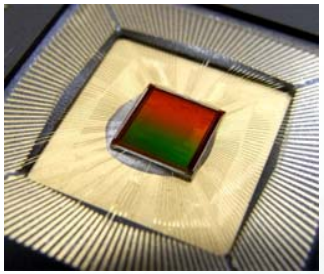
2003 INSTAC-8



2004 INSTAC-32



2007~ SASEBO-R/-B/-G/-GII



SASEBO

National Institute of Advanced Industrial Science and Technology
AIST

国際標準規格への貢献

- 日本発の評価プラットフォームが標準化作業や学術研究に広く利用されている
- 産総研，IPA，NICT，NIST，企業，大学が協力して研究を進めている

情報機器の安全性向上

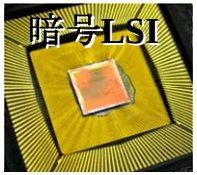
NiCT
CRYPTREC
Cryptography Research and Evaluation Committees
Japan Cryptographic Module Validation Program
JCMVP
IPA

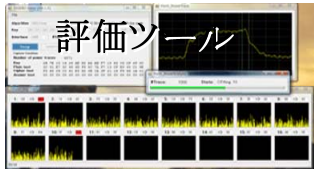
技術提供

評価・認証

ノウハウ公開

標準評価試験環境の構築

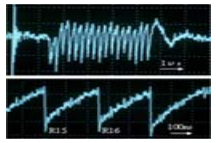




標準評価ボード

National Institute of Advanced Industrial Science and Technology
AIST

TOHOKU UNIVERSITY



評価技術研究開発

国際規格策定への貢献

共同研究

研究員派遣

執筆

配布

実験レポート
論文・コメント

NIST
FIPS 140-3

ISO/IEC化

ISO
IEC

評価指針
Draft

ISO/IEC 19790
ISO/IEC 24759

National Institute of Advanced Industrial Science and Technology
AIST

評価手法をどうすべきか？

暗号モジュールの物理攻撃に対する安全性評価手法

- ソフトウェアもプロセッサというハードウェアの上で評価されるため ハードウェアモジュールとしての評価が必要

暗号アルゴリズムの評価手法

- 理論的安全性
- ソフトウェア性能 （速度・コードサイズ）
- ハードウェア性能（速度・回路規模・消費電力）
- 物理攻撃に対する安全性

National Institute of Advanced Industrial Science and Technology
AIST

暗号モジュールの評価手法

- 2007年7月にNISTから出されたFIPS 140-3の1stドラフトでは5つのセキュリティレベルが設定され，Level 3~5がサイドチャネル評価の対象となっていた
  - 2009年12月の2ndドラフトでは4つのレベルに変更
- 測定の容易さでレベル分けしているが，サイドチャネル攻撃耐性とは関係がない
  - Level 3：タイミング攻撃
  - Level 4：Level 3 + 電力解析攻撃
  - Level 5：Level 4 + 電磁波解析攻撃
- CRYPTREC/INSTACは解析手法の違いによる分類を提案したが，解析ツールがサポートしていれば手間はまったくかからない
  - Level 3：タイミング攻撃，単純電力・電磁波解析攻撃
  - Level 4：Level 3 + 差分電力・電磁波解析攻撃，フォールト攻撃
  - Level 5：Level 4よりも高度な解析手法

評価レベル	FIPS 140-3 1st ドラフト	CRYPTREC コメント
Level 3	TA	TA, SPA, SEMA
Level 4	TA, SPA, DPA	TA, SPA, DPA, SEMA, DEMA, FI
Level 5	TA, SPA, DPA, SEMA, DEMA	TA, SPA, DPA, SEMA, DEMA, FI

産総研と東北大は攻撃のコストに基づくレベル分けを提案

National Institute of Advanced Industrial Science and Technology
AIST

攻撃コストに基づく評価

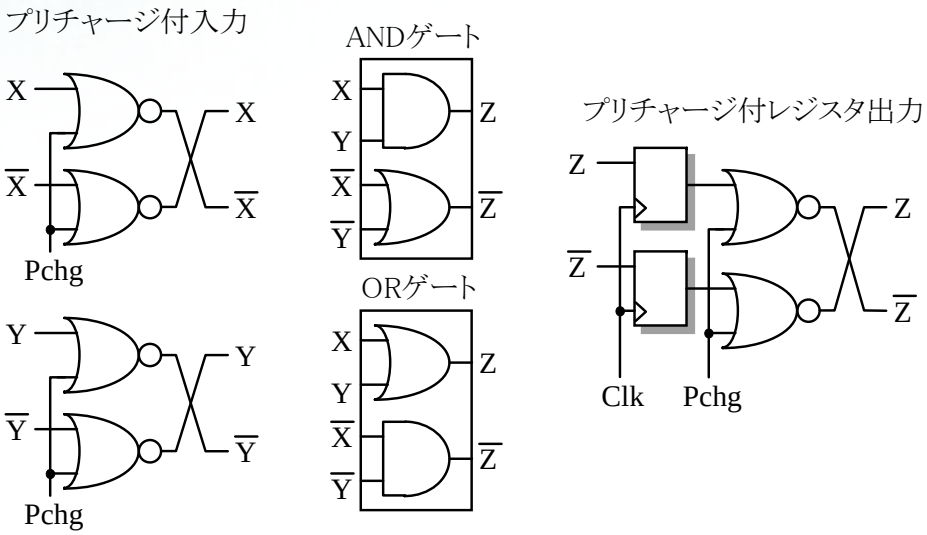
- 攻撃者にとって解析の時間や労力とそれによって得られる利益が重要
- 試験機関もビジネスとして評価を行うため，評価（＝攻撃）にかけたコストによってレベル分けをすべきである
- 試験機関は攻撃者よりも極めて有利な立場にある
  - 暗号モジュールの設計情報にアクセスできる
  - 暗号モジュールに様々な物理的アクセスができる
  - 試験者は正解の鍵を知っているため，正しい鍵と誤った鍵を設定した解析結果に差が出るかを調べればよい
  - 攻撃者は多数の鍵候補に対する解析を行う必要があり，かつ高い相関値を示した鍵が正解である保証もない
  - 試験者は鍵の一部の情報（ビット）が漏えいしていることが明らかになった場合，全ての情報の漏えいを確認する必要ななく，その場で不適合とすることができる
  - 攻撃者は全ての鍵ビットを導出できなければ意味がない
- 試験機関にとって，暗号モジュールの測定環境のセットアップが最もコストを要するため，ベンダー自身による実機試験の評価レポートを要求し，その試験環境を利用
  - Level 3 : 評価レポートによるドキュメントチェック
  - Level 4 : 評価レポート＋試験機関での実機評価

National Institute of Advanced Industrial Science and Technology
AIST

暗号アルゴリズムの評価手法

- ハードウェア性能（速度・回路規模・消費電力）
  - 既存の“標準”アルゴリズムに対するアドバンテージを示す必要がある
  - 一つの実装に対する速度・回路規模評価だけでなく，バリエーションも重要
  - 実機プラットフォームではなく論理合成の評価レポートでもよいのではないか？
- 物理攻撃に対する安全性
  - 多くの対策はAESやRSAに対して実装されているが，実装形態に大きく依存する
  - アルゴリズム評価と対物理攻撃耐性は分けるべきではないのか？

2線ロジックによる電力の平均化



乱数による電力のランダム化