「ディペンダブル VLSI システムの基盤技術」
平成 21 年度採択研究代表者

H22 年度
実績報告

藤野　毅

立命館大学　理工学部・教授

耐タンパディペンダブル VLSI システムの開発・評価

§1. 研究実施の概要

(1) 耐タンパ性 LSI 設計プラットフォームの研究

立命館大学で提案する“ドミノ RSL ゲート”を用いた DES 暗号回路を，標準的な ASIC 設計フローに準拠した手順で設計し，ローム 180nmCMOS プロセスで実チップを試作した．試作したチップは，消費電力を利用したサイドチャネル攻撃（ハミングウエイト型，ハミングディスタンス型，電力相関係数（CPA）型）に対して耐タンパ性を有することを，耐タンパ性評価ボード SASEBO-R（改造）を用いて実験的に実証できた．

また，LSI の設計時点で耐タンパ性の評価を実行することのできる，高速耐タンパ電力解析シミュレータを試作した．このツールにより，AES 暗号回路の各種 S-Box 実装方式（テーブル法，PPRM 法，合成体　等）に依存して耐タンパ性の強度が異なることを高速にシミュレートすることができた．

(2) 耐タンパ性能評価プラットフォームの研究

23 種類の暗号回路を実装した暗号 LSI を，e-Shuttle 社の 65nmCMOS スタンダードセルライブラリにより製造し，120 個全ての LSI の正常動作を確認した．また電磁波解析攻撃実験を行うためのプラットフォームを構築し，市販及び試作磁界プローブによる比較実験を行い，試作プローブの高い性能が示された．

(3) 偽造 LSI を識別する PUF を用いたセキュリティーシステムの研究

標準的な PUF として提案されている，“セレクタチェイン型アービターPUF 回路”をローム 180nm プロセスを用いて試作し，発生される ID のユニーク性（異なるデバイスからは異なる ID が生成される特性）や再現性（電源電圧や測定温度によって ID が変動してしまう特性）の評価を行った．ID のユニーク性を向上させるために，セレクタチェインの到達時間差を ID 情報として利用する DTM(Delay Time Measurement) PUF を考案し，実チップ評価を行うことで，ユニーク性

が向上し理想的な PUF の特性が得られることを確認できた.

従来曖昧であった PUF の性能評価の指針として, 数学的に厳密に定義された Randomness, Steadiness, Correctness, Diffuseness, Uniqueness を導入し, SASEBO-GII の FPGA 上に実装した Arbiter PUF の性能評価を行った.

§2. 研究実施体制

(1)立命大グループ

①研究分担グループ長:藤野　毅 (立命館大学理工学部、教授)(研究代表者)

②研究項目

- 電力・電磁波を利用したサイドチャネル攻撃に対する対タンパ LSI 設計手法の研究
- 耐タンパ性 LSI マクロの回路設計
- PUF デバイス回路実装と特性評価およびモデル化

(2)産総研グループ

①研究分担グループ長:佐藤　証 (産業技術総合研究所、チーム長)(主たる共同研究者)

②研究項目

- サイドチャネル攻撃・フォールト攻撃用プラットフォーム開発
- 防御手法・解析手法の開発および有効性検証
- PUF の実装および測定
- PUF と暗号技術を融合したセキュリティシステムの構築

(3)中央大グループ

①研究分担グループ長:吉田　隆弘 (中央大学研究開発機構、専任研究員・機構助教)
(主たる共同研究者)

②研究項目

- サイドチャネル情報に基づく新攻撃手法に関する研究
- PUF の評価とプロトタイプの開発
- 暗号モジュールのフォールト攻撃に対する安全性評価
- フォールト攻撃の対策技術の開発・有効性評価

(4)名城大グループ

①研究分担グループ長:吉川　雅弥 (名城大学理工学部、准教授)(主たる共同研究者)

②研究項目

- プログラマブル LSI を指向した配線アーキテクチャと遅延モデルの開発と評価

・ 耐タンパ性を考慮するためのレイアウト制約の開発
・ 耐タンパドリブン CAD システムの構築

§3. 研究実施内容

(文中に番号がある場合は(4－1)に対応する)

(1) 耐タンパ性 LSI 設計プラットフォームの研究

立命館大Gで提案する耐タンパ暗号回路を実現するための，“ドミノ RSL ゲート”を用いた DES 暗号回路を設計し，ローム 180nmCMOS プロセスで実チップを試作した．試作に使用した設計 CAD フローは図1に示すとおりである．標準的な ASIC フローに対して，論理合成したネットリストの非線形回路部のみを，積和標準形の論理合成ツールで再論理合成する処理(左青破線枠)と，自動配置配線用のドミノRSL ゲートレイアウトライブラリを追加する処理を変更している．

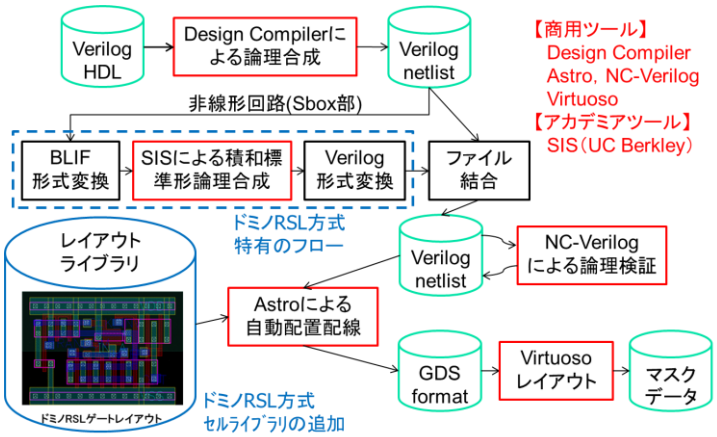
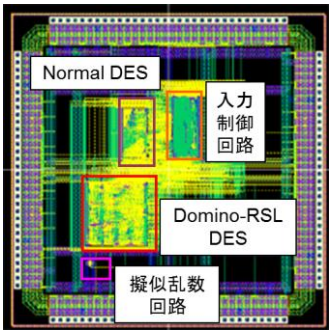


図１． ドミノ *RSL* 方式を用いて *DES* 暗号回路を作成するための設計フロー

試作したチップのレイアウトおよびチップ面積を図2に示す．比較のために，耐タンパ対策を行っていない DES 暗号回路(Normal DES)も同時に設計している．未対策経路に対して約 2.9 倍の面積ペナルティー(0.088mm²⇒0.254 mm²)が発生した．



	X(μm)	Y(μm)	面積(μm²)	Utilization(%)
Domino-RSL DES試作チップ	2022.48	2022.48	4090425	-
Domino-RSL DES(ECB)	499.64	508.56	254097	62.89
NORMAL DES(ECB)	220	400	88000	67.47
入力制御回路	220	500	110000	60.46
擬似乱数回路(9bitLFSR)	75.68	44.32	3354	59.38

図２． ドミノ *RSL* 回路を用いて構成した *DES* 暗号回路チップの概要

試作したドミノ RSL 回路を用いた DES 暗号回路のハミングディスタンス型の DPA 耐性評価結果を図3に示す．未対策回路では 8,000 波形の取得で，48bit のすべての正解暗号鍵を推定できたが，ドミノRSL 回路では4万波形を取得しても，全く正解鍵を特定することはできなかった．また，ハミングウエイト型，電力相関係数型に関しても同様の結果が得られており，

一般的な電力解析手法に対しては，十分な DPA 耐性が得られていることを確認できた [2].

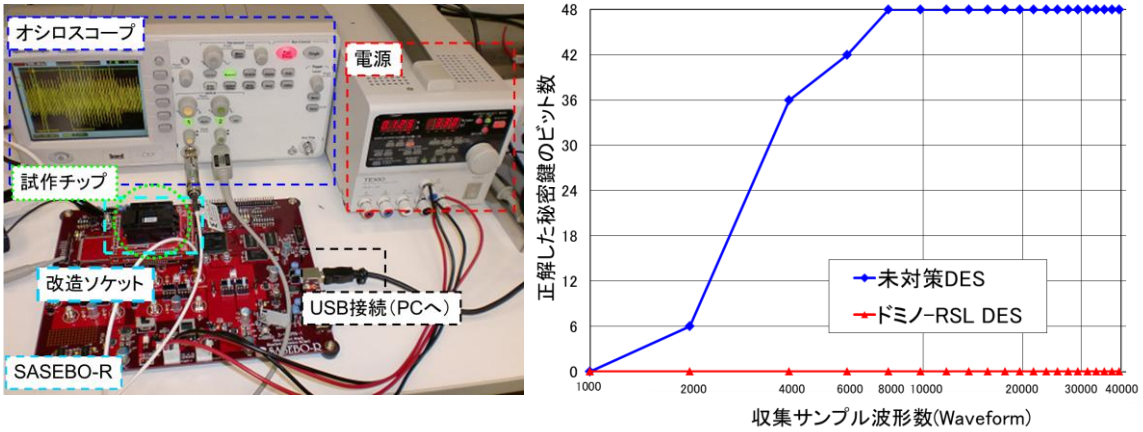


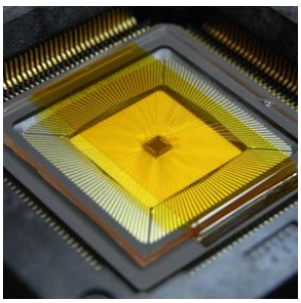
図３．ドミノ RSL 回路を用いた DES 暗号回路のハミングディスタンス型 DPA 耐性評価

今後は，試作した DES 暗号回路チップを用いて，①高度なサイドチャネル攻撃に対する耐性の検証，②電磁波を用いたサイドチャネル攻撃に対する検証，③故障利用解析攻撃を用いたサイドチャネル攻撃に対する検証，を順次進めていく [5),7)].

また，現在主流となっている AES 暗号回路の LSI 実装方式に関しては，ASIC デザインフローに対して，より変更点が少なく，面積ペナルティーも少ないメモリを用いた方式を設計中であり，H23 年度中には試作評価結果できる予定である．

(2) 耐タンパ性能評価プラットフォームの研究

65nm e-shuttle ライブラリを用いて開発した LSI(図4)の動作確認を行い，AES 回路の動作波形を既開発の 130nm, 90nm TSMC ライブラリと比較し(図5)，製造プロセスの進歩がサイドチャネル攻撃に与える影響の解析や，計測手法改良のための実験環境を充実させた [1)]．また，LSI が発生する電磁波を利用したサイドチャネル攻撃の実験環境を構成し(図6)，市販の磁界プローブ（NEC 製 CP-2S）の他に，サイドチャネル攻撃に特化したオリジナルのプローブ（K-1,K-5,M10）を3種作成し，CEMA (Correlation ElectroMagnetic Analysis) を実施した．5,000 波形による攻撃の結果，図7に示したようにオリジナルのプローブは市販プローブと比較して，少ない波形数で高い精度で鍵の推定に成功した．



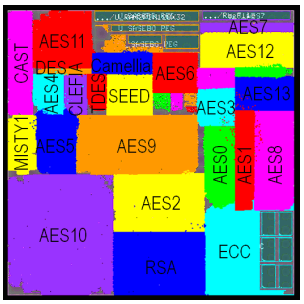


図4　暗号 LSI の外観(左)とマクロ配置(右)

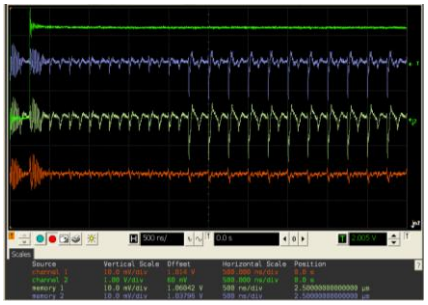


図5　AES 処理時の電圧変動波形の比較（上から 65nm,130nm,90nm）

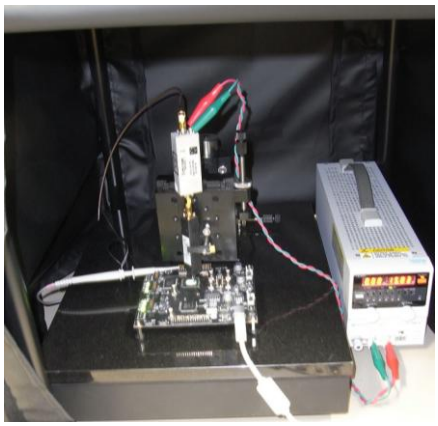


図6　電磁界測定環境

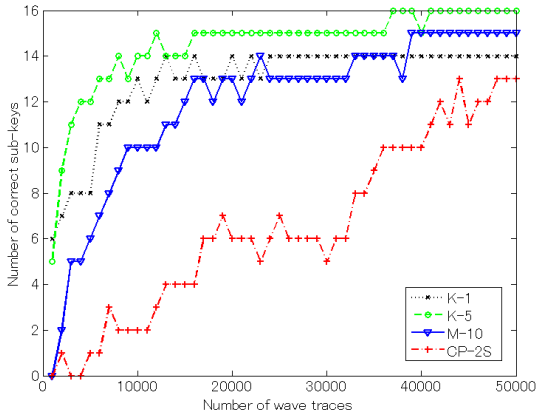


図7　4種類の磁界プローブを用いたCEMAの結果

(3) 偽造LSIを識別するPUFを用いたセキュリティシステムの研究

PUFはチップ製造時のランダムなばらつきを抽出して固体固有のIDを生成する回路であり，今回，多段接続セレクタチェイン型Arbiter　PUFを対象にアーキテクチャの検討，問題点の抽出，およびPUFの性能評価手法の開発を行った[6]．

立命館大Gでは実チップを用いて評価をおこなった．従来型のArbiter PUFの試作を行い，デバイス間のユニーク性を示す指標（異なるデバイス間でのIDのハミングディスタンス）の分散が理想値より非常に大きくなることを実験的に確認した．これは，アービターPUF 方式の原理的な問題であり，レスポンスIDの出現確率に偏りがあるためである．上記問題点を解決する提案として，図8に示す，遅延時間差検出(DTM: Delay Time Measurement)型アービターPUF の提案を行った．通常のアービターでは，2つの等価な経路間でどちらの経路が早く信号を伝搬したかによって出力を決定しているが，本DTM方式PUFでは，経路の時間差を測定し，その大きさによってレスポンスを0,1に決定する点が特徴である．

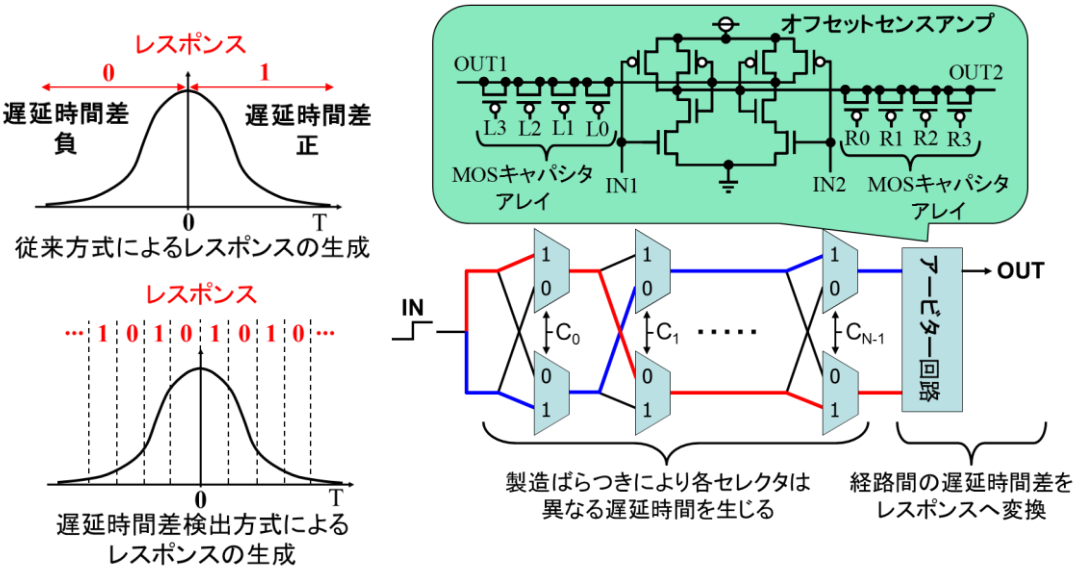


図8．遅延時間差検出(DTM)型アービターPUFの原理と回路

図9に，新しく提案した DTM 方式 PUF の試作チップとユニーク性の評価結果を示す．8 段のアービターPUF において，遅延時間差を 16 分割して 1,0 の割り当てを行うと，ほぼ理想的なハミングディスタンス分布が得られ，ユニーク性の向上が確認できた．

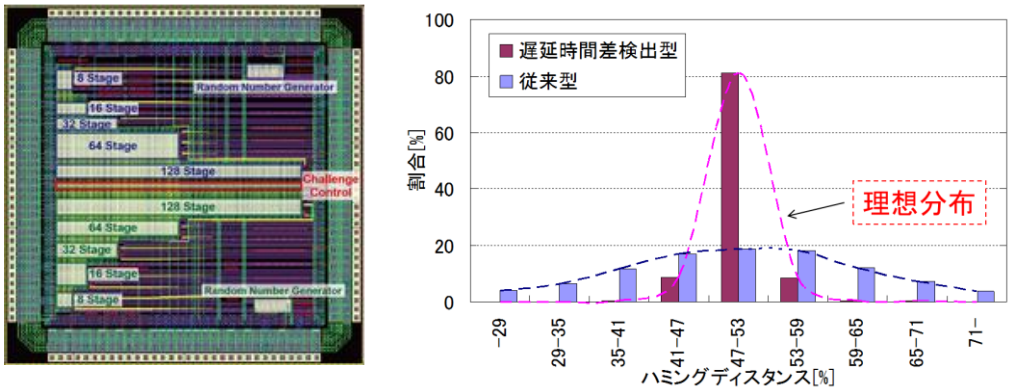


図 9． DTM 方式アービターPUF の試作チップとユニーク性評価結果

産総研グループでは FPGA ボードを用いた検討を行い，45 枚の SASEBO-GII 上の Xilinx Virtex-5 に Arbiter PUF を実装した [4]．この結果から，PUF の性能を表1に示す Randomness, Steadiness, Correctness, Diffuseness, Uniqueness の 5 項目により数学的に厳密な定義を与え，定量的評価を行った．

表 1 PUF の性能の定義

性能指標	性能	定義
Randomness (H_n)	出力の 0/1 のバランス	$p_n = \frac{1}{K \cdot T \cdot L} \sum_{k=1}^{K} \sum_{t=1}^{T} \sum_{l=1}^{L} b_{n,k,t,l}$ $H_n = -\log_2 \max(p_n, 1-p_n)$
Steadiness (S_n)	ID のチップ内での再現性	$S_{n,k,l} = 1 + \log_2 \max(p_{n,k,l}, 1-p_{n,k,l})$ $S_n = \frac{1}{K \cdot L} \sum_{k=1}^{K} \sum_{l=1}^{L} S_{n,k,l}$ $= 1 + \frac{1}{K \cdot L} \sum_{k=1}^{K} \sum_{l=1}^{L} \log_2 \max(p_{n,k,l}, 1-p_{n,k,l})$
Correctness (C_n)	出力された ID の正しさ	$C_{n,k,l} = 1 - \frac{\sum_{t=1}^{T} (b_{n,k,l} \oplus b_{n,k,t,l})}{T/2}$ $C_n = \frac{1}{K \cdot L} \sum_{k=1}^{K} \sum_{l=1}^{L} C_{n,k,l}$ $= 1 - \frac{2}{K \cdot T \cdot L} \sum_{k=1}^{K} \sum_{t=1}^{T} \sum_{l=1}^{L} (b_{n,k,l} \oplus b_{n,k,t,l})$
Diffuseness (D_n)	同一チップ内で，異なるチャレンジに対して異なる ID が出る性質	$D_n = \frac{1}{L} \sum_{l=1}^{L} \frac{d_{n,l}}{(K/2)^2} = \frac{4}{L \cdot K^2} \sum_{l=1}^{L} \sum_{i=1}^{K-1}$
Uniqueness (U_n)	異なるチップ間で，同一のチャンレンジに対して異なる ID が出る性質	$U_n = \frac{4}{K \cdot L \cdot N} \sum_{k=1}^{K} \sum_{l=1}^{L} \sum_{j=1, j \neq n}^{N} (b_{n,k,l} \oplus b_{j,k,l}).$

§4. 成果発表等

（4－1） 原著論文発表

●論文詳細情報

[1] Akashi Satoh, Toshihiro Katashita, and Hirofumi Sakane, “Secure Implementation of Cryptogpraphic Modules -Development of Standard Evaluation Environment for Side Channel Attacks-,” Synthesiology - English edition, vol. 3, no. 1, pp. 86-95, July 2010. (DOI なし)

[2] Kenji Kojima, Kazuki Okuyama, Katsuhiro Iwai, Mitsuru Shiozaki, Masaya Yoshikawa, and Takeshi Fujino, “LSI Implementation Method of DES Cryptographic Circuit utilizing Domino-RSL Gate Resistant to DPA Attack,” SASIMI Digest of Technical Papers, October 2010.(DOI なし)

[3] M.Yoshikawa, Y.Kokusyo, and T.Fujino, “Placement Tool Dedicated for a Via-programmable Logic Device VPEX”, Proc. of 23rd International Conference on Computer Applications in Industry and Engineering, pp.21-25, November, 2010.(DOI なし)

[4] Yohei Hori, Takahiro Yoshida, Toshihiro Katashita and Akashi Satoh, “Quantitative and Statistic Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs”, International Conference on ReConFigurable Computing and FPGAs (ReConFig2010), pp.298-303, December, 2010. (DOI なし)

[5] Anh-Tuan Hoang, Masaya Yoshikawa, and Takeshi Fujino, “AES Side Channel Attack Using Final to First Rounds Hamming Distance”, NCSP 2011 Technical Papers, March 2011. (DOI なし)

[6] Mitsuru Shiozaki, Teruri Fukushima, Kota Furuhashi, Takahiko Murayama, and Takeshi Fujino, “Evaluation of Uniqueness and Environmental Stability of IC Identification Generated by Arbiter-PUF,” NCSP 2011 Technical Papers, March 2011. (DOI なし)

[7] Masaya Yoshikawa and Toshiya Asai, "High-Level Simulation for Side Channel Attacks", Proc. of The International MultiConference of Engineers and Computer Scientists, Vol.2, pp.1565-1568, March 2011. (DOI なし)

(4－2)知財出願

① 平成22年度特許出願件数(国内 0 件)

② CREST 研究期間累積件数(国内 1 件)