立命館大学審査博士論文

LSI の低コスト化・設計資産保護を実現する

マスクプログラマブルデバイスの研究

(Study on Mask Programmable Devices for Low-Cost Fabrication and Intellectual Property Protection)

2015 年　3 月

March, 2015

立命館大学大学院理工学研究科

電子システム専攻博士課程後期課程

Doctoral Program in Advanced Electrical, Electronic and Computer System
Graduate School of Science and Engineering
Ritsumeikan University

堀　遼平

Ryohei　Hori

研究指導教員：藤野毅教授

Supervisor:　Professor　Takeshi Fujino

内容梗概

近年，大規模集積回路（LSI : Large Scale Integrated Circuit）の微細化・高集積化技術の進歩により，主要な機能を LSI 内にすべて組み込みことが可能になり，高機能かつ小面積なハードウェアの実現が可能になった．しかし，その一方で LSI 量産時に必要となるフォトマスクのマスクコストや設計費用といった初期開発コストの高騰が問題となっている．この問題によって，生涯生産数の少ない特定用途向け集積回路（ASIC：Application Speciific Integrated Circuit）の開発が困難になっており，フィールドプログラマブルゲートアレイ（FPGA : Field Programmable Gate Array）のような製造後に論理機能を書き換えられるデバイスを用いた開発が注目されるようになってきた．しかしながら FPGA はセルベース方式 ASIC と比較して単位面積あたりの論理機能，動作速度，消費電力などの性能面で劣っており，少量生産市場にある ASIC のすべての品種を置き換えるには至っていない．また，LSI 内の高価な設計資産（IP コア：Intellectual Property Cores）をリバースエンジニアリング（RE : Reverse Engineering）などの手段を用いて, 不正に模倣することも問題となっている. したがって, FPGA よりも高性能で ASIC よりも開発費が安価であるデバイスや RE 攻撃に耐性を持ったデバイスの開発が必須であるといえる．

本論文はこれらの問題点に対して，マスクプログラマブルデバイス（MPD：Mask Programmable Device）という設計・製造技術を用いた解決案について検討したものである．MPD とは LSI 積層構造の内，数層を変えるだけで論理機能を変更できる構造を有した LSI の総称であり．LSI の製造工程において，回路をウェハ（wafer）上に構成する際にはフォトマスクと呼ばれるガラス板が用いられる．このフォトマスクは LSI 積層構造の階層毎に用意され，最新プロセスの製造工程では 30～60 枚のフォトマスクが一つの LSI を実現するためのセット（マスクセット）となっている．MPD では使用されるマスクセットの大部分を共用化し 1~3 枚ほどのフォトマスクを変更するだけで全く別の論理回路を実現することが可能である．この技術を用いることで数層のビア層のみを変更して新しい論理回路を製造することや，拡散領域のみを変更することで配線層からは回路構造の特定ができない RE 耐性を持ったデバイスを実現することが可能になる．

本論文は 2 部構成となっており，1 部ではビア層のみを変更する MPD であるビアプログラマブル・ストラクチャード ASIC（VPSA：Via Programmable Structured ASIC）について第 2 章～第 8 章まで論じる．第 2 部では拡散領域のみを変更する MPD であるディフュージョンプログラマブルデバイス（DPD：Diffusion Programmable Device）について第 9 章から第 11 章まで論じる．

第 1 章では LSI の初期開発コストや RE の脅威について論じ, その対策方法として VPSA および DPD が有効であることを示す.

第 2 章では VPSA の背景を述べる．ストラクチャード ASIC の特徴について ASIC や FPGA のメリット・デメリットとの比較から明らかにし，ストラクチャード ASIC および VPSA の有効性や基本概念を述べる．

第 3 章では VPSA のアーキテクチャや論理構成方法を紹介し，具体的なアーキテクチャの例として LUT を用いた方式を紹介する．また LUT 型の問題点を新たに解決するために考案された排他的論理和（XOR：Exclusive-OR）論理ゲートをベースとして 13 種類の論理素子を再現することができる Via Programmable Device using Exclusive-or logic array（VPEX）について述べる．さらに，LUT 型および VPEX で使用されているロジックエレメント（LE : Logic Element）の特徴や工夫についてまとめる．

第 4 章では第 3 章で紹介した VPEX の問題点として第 2 ビア層がプログラムできないことのデメリットを考察する．この第 2 ビア層をプログラムを可能にし，LE を改良した新しいアーキテクチャ VPEX3 を提案する．プログラム可能なビア層を増やしたことで，既存提案の VPEX よりも小面積かつ再現論理の多い LE を実現した. またこの VPEX3 の性能を定量的に評価するために第 3 章で述べた他のアーキテクチャとの性能比較結果を示す.

第 5 章では他研究機関で提案された MPD との性能比較を行った．比較対象はビアコンフィギャラブルロジックブロック（VCLB : Via Configurable Logic Block）と呼ばれる方式で，VPEX のようにビアの座標変更によって数十種類の論理素子を再現する．また VPEX と同様の 180nm プロセスによって開発されているデバイスである．VCLB の性能評価は論文に掲載されており，VPEX3 においてもその論文と同等の方法を用いて性能評価を行い，面積・動作速度・消費電力の比較を行った.

第 6 章では VPEX3 のチップ試作のため開発した専用 CAD 環境について述べる．VPEX3 の配置配線はビア座標の有無のみによって実現されるため，通常のセルベース方式 ASIC とは大きく異なる．そのため VPEX3 によって大規模回路を実現するためには専用の開発環境を構築する必要がある. 本章ではアカデミック用に他の研究機関で開発されている配置最適化, 配線最適化プログラムを VPEX3 に適合できるように改良し，大規模回路においても配置配線を実現できる CAD システムを開発した結果を述べる.

第 7 章では VPEX3 の性能評価, および CAD の動作確認のために開発した 2 種類の試作チップとその性能評価結果について報告する. 本章では CAD によって大規模な論理回路が実現可能であること, ASIC や FPGA と比較したときの性能比較を示す.

第 8 章では 5 章，7 章の性能評価結果から得られた課題点を元にさらに改良を施した新アーキテクチャ VPEX4 について述べる. 配置配線後の評価より VPEX3 では配線リソース不足によって回路面積が大きくなってしまう問題点が明らかになった．これを改善するために LE の面積を大きくし，LE1 個あたりの配線リソースを増やすことで，配線成功率を向上させた．実際に大規模暗号回路である DES，AES を配置配線し，面積を比較することで，性能改善が実現されたことを示す.

第 9 章では第 2 部の背景として RE 攻撃の脅威について述べる．また既存の RE 対策手法として，ウェル（well）領域を利用した対策，拡散抵抗を利用した対策，アンチヒューズ（Antifuse）型 FPGA の RE 耐性についてそれぞれ述べる.

第 10 章では DPD を実現する基礎技術である DP-ROM について説明をする. また DP-ROM を用いた論理と配線のプログラム方法について，FPGA のアイランドスタイル（island style）構造を DP-ROM を用いて実現する方法について述べる.

第 11 章では DPD アーキテクチャを用いたチップについて，動作確認と耐性評価を行った実験結果について述べる．DPD を用いて構成したルックアップテーブル（LUT : Look-up Table）について，理論通りの動作をしていることを確認した．また光学顕微鏡や走査型電子顕微鏡（SEM : Scanning Electron Microscope）を用いた RE 耐性評価実験を行い，SEM の特定条件下では RE 攻撃が可能であるものの，光学顕微鏡では RE 攻撃が不可能であることを確認した.

第 12 章では本論文のまとめを述べ, 今回の論文では検証しきれなかった点や今後の展望について論じる.

目次

第１章　序論

１．１　背景

1940 年代に発明されたゲルマニウム（Ge）によって実現されたトランジスタ（transistor）は，その後の技術発展によってシリコン（Si）の基板表面で製造する技術（プレーナ技術）が開発され，同一基板上にまとめて複数のトランジスタを造りすことが可能になった．この技術がさらに発展し，複数のトランジスタを用いて回路を構成する集積回路（IC：Integrated Circuit）がトランジスタの誕生から 10 年後に登場した．これによってトランジスタを用いて論理演算器を作ることが可能になり，単純な論理素子から大規模集積回路（Large Scale Integrated circuit）を実現する設計技術へと発展していった．またトランジスタをより小さく，高密度に作りこむための微細加工技術も進歩していき，同一基板上に数十個程度の集積度であったトランジスタの IC チップは数千個から数万個へと飛躍的に集積度を上げていった．次第に数平方ミリメートル角の IC チップにすべて演算器が収まるようになり，膨大な信号を制御するための大規模な演算装置をトランジスタによって実現することが可能になった．こうして誕生したプロセッサ（Processor），デジタル信号処理プロセッサ（DSP：Digital Signal Processor），大容量メモリ（memory）よって，パソコンや携帯電話などの小型デバイスが実現した．今では技術の進歩によりゲート長がわずか数十 nm のトランジスタを数億個搭載した LSI を量産できるようになっており，タブレット型パソコンやスマートフォンなどの小型かつ高機能なデバイスが実現された．近年の技術進歩は主に製造プロセスの技術進歩によるところが大きい．トランジスタをより小さく製造することで限られた実装面積により高度なハードウェアやシステムを実現することができるからである．

しかし一方で，こうした最先端プロセス製造技術の利用にはいくつかの問題点・課題点が指摘されるようになってきた．その一つに初期開発費（NRE コスト：Non-Recurring Engineering Costs）の高騰がある．最新の製造技術を用いた LSI の開発では NRE コストだけで数億円単位の投資が必要となってきている．これは回路デザインの複雑化に伴う設計支援ツール（CAD：Computer Aided Design）や自動化支援ツール（EDA：Electronic Design Automation），それらを扱い設計する技術者の人件費の増加，設計資産（IP コア：Intellectual property Core）のライセンス費用などの設計費用（design cost）が大きな要因といわれているが，フォトマスク（photo mask）を造るためのマスクコスト（mask cost）の高騰などの製造費用（manufacturing cost）の増加も課題点の 1 つとなってきている[1]．NRE コストが膨大になったため携帯電話，デジカメ，情報家電，ゲーム機などの需要の多い大量生産市場でなければ最先端プロセスの製造技術を用いた LSI 開発が出来ない状態になってしまっている．

またこのような膨大な NRE コストをかけて製造された LSI が解析され，模倣されることも大きな問題となっている．模倣半導体の存在によって生涯生産数が予測値を下回ってしまえば LSI の NRE コストの回収が完了せず，利益がなくなってしまう．さらにこのリスクを意識することで新規 LSI を開発することが困難になるという悪循環が危惧される．一方，こうした模倣半導体の存在は生涯生産数の低下や粗悪品の混在を招くといった被害にとどまらず，悪意のある LSI を参入させることで，ハードウェアが実現していたセキュリティや信頼性を破壊することも危険視されている．

これらの問題を放置することは，最先端プロセスを用いた新しい LSI 開発の機会を損失させ，先端プ

ロセスを用いた半導体市場の成長を妨げるだけでなく，市場そのものが成り立たなくなる危険性を有している．先端プロセスを用いた低リスク開発手法の実現や，模倣半導体の対策が現在の半導体市場を成長させる上での課題といえる．

本論文はこれらの問題点に対して，マスクプログラマブルデバイス（MPD：Mask Programmable Device）という新しい設計・製造技術を用いた解決案について検討したものである．LSI の製造工程において，回路をウェハ（wafer）上に構成する際には最初の原板としてフォトマスクと呼ばれるガラス板に回路パターンを電子ビーム（EB：Electron Beam）で描画（drawing）する．そしてフォトマスク上のパターンをさらにウェハに光で一括転写（transfer）することでウェハ上にパターンを形成する．フォトマスクを変更しながら転写を繰り返すことで集積回路が構成される．このときフォトマスクは LSI 積層構造の階層毎に用意され，最新プロセスの製造工程では 30～60 枚のフォトマスクが一つの LSI を実現するためのセット（マスクセット）となっている．MPD ではこのマスクセットのうち 1~3 枚ほどを変更して全く別の LSI を造る試みである．本研究ではこの方式の実例・応用例に関して検討した．

１．１．１　初期開発コストの削減

高性能・多機能 LSI 実現の課題となっている初期開発コストの中でも，LSI 製造技術の進歩に追従する形で増加し続けているものがマスクコストと呼ばれるフォトマスクの製造費用である．フォトマスクに作られた回路パターンの寸法はウェハに転写する回路パターンの寸法と同等あるいは数倍程度の非常に小さなパターンが必要になる．そのためガラス板上に回路パターンを正確に形成する技術が必要である．これには高価な EB 描画装置が必要となり，フォトマスク 1 枚を製造するコストは製造プロセスの進歩とともに指数関数的に増大している．このマスクコストに関する問題に対してはフォトマスクの製造効率化や LSI の製造方法・工程の改善に関する多くの既存研究が報告されており[2]，こうした製造技術に関連する研究以外に，プログラマブルデバイス（programmable device）と呼ばれる LSI を用いたマスクコスト低減手法が提案されている[3-5].

プログラマブルデバイスの例としてフィールドプログラマブルゲートアレイ（FPGA：Field Programmable Gate Array）[3,4]と呼ばれるデバイスが存在する．この FPGA は製造後に論理回路の書き換えが可能なデバイスであり，所望の論理回路を開発する上で専用のフォトマスクを必要としない．したがって回路を実現するためにマスクコストを必要とせず，製造時に NRE コストの影響を受けない LSI である．そのため FPGA は製品開発の試作や生産数の少ない製品に広く用いられている[4]．FPGA はマスクコストによるコスト問題を解決したように思えるが，FPGA 上に実装された論理回路は従来の製造手法を用いて製造された特定用途向け集積回路（ASIC：Application Specific Integrated Circuit）に比べ，動作速度や消費電力などの性能面で劣っている[6,7]．そのためモバイル機器などの省電力性能が求められる用途では使用する事ができず，生涯生産数が少量生産となる ASIC の全ての品種を置き換えるには至っていない．また単位面積当たりの回路実装効率も悪く，IC チップのサイズ大きくなるためチップ単価（unit cost）が高い．そのため少量生産市場ではない大～中量生産市場の分野では ASIC を使用する方が安価となる．従って FPGA の採用には市場の需要や生涯生産数を見誤ることで不利益を被るリスクがある．

性能とコストのバランスを両立するためには FPGA とは異なる技術が必要である．そこで我々が注目した技術が MPD を用いたストラクチャード ASIC（Structured ASIC）[8]とよばれる製造手法である．

ストラクチャード ASIC は数枚の金属配線層用のフォトマスクを変更して異なる論理回路を作りこむ MPD であり，多数のフォトマスクを他の設計で再利用することによって NRE コストを低く抑えることができる．また金属配線接続によって直接的にゲート間を接続するため，論理回路の性能は FPGA よりも高く[9]，モバイル用途などでも十分に利用できる可能性がある．我々の研究室では 2008 年に Via Programmable device using EXclusive-or logic array（VPEX）[10]と呼ばれる独自のストラクチャード ASIC を提案した．VPEX は EB を用いたマスクレス（mask less）製造技術と組み合わせることで製造時のマスクコストを無くすことが可能である[10]．本論文ではこの VPEX を改良することで FPGA よりも高性能で NRE コストの少ない LSI の実現を検討した．初めて VPEX を用いた集積回路を試作チップを試作し，その性能評価を通して得られた課題点を考察することで新しいアーキテクチャ案を提案した．本論文ではシミュレーションや静的解析によってアーキテクチャを評価することで得られた高性能なストラクチャード ASIC 実現に向けた知見や考察について述べていく．

１．１．２　リバースエンジニアリング（Reverse Engineering）への耐性

LSI の内部構造を解析して回路図を再現し，同様の機能を持った LSI を模倣する工程や行為をリバースエンジニアリング（RE : Reverse Engineering）と呼ぶ[11-14]．こうした RE によって特定機能やハードウェアアルゴリズムの盗用や模倣半導体の製造などが問題となっている．これは市場への影響だけにとどまらず，近年では IC カードのようなハードウェアによって保障されていた情報セキュリティ（Information Security）保護機能の信頼性を失墜させることが危惧されている[12,13,15]．

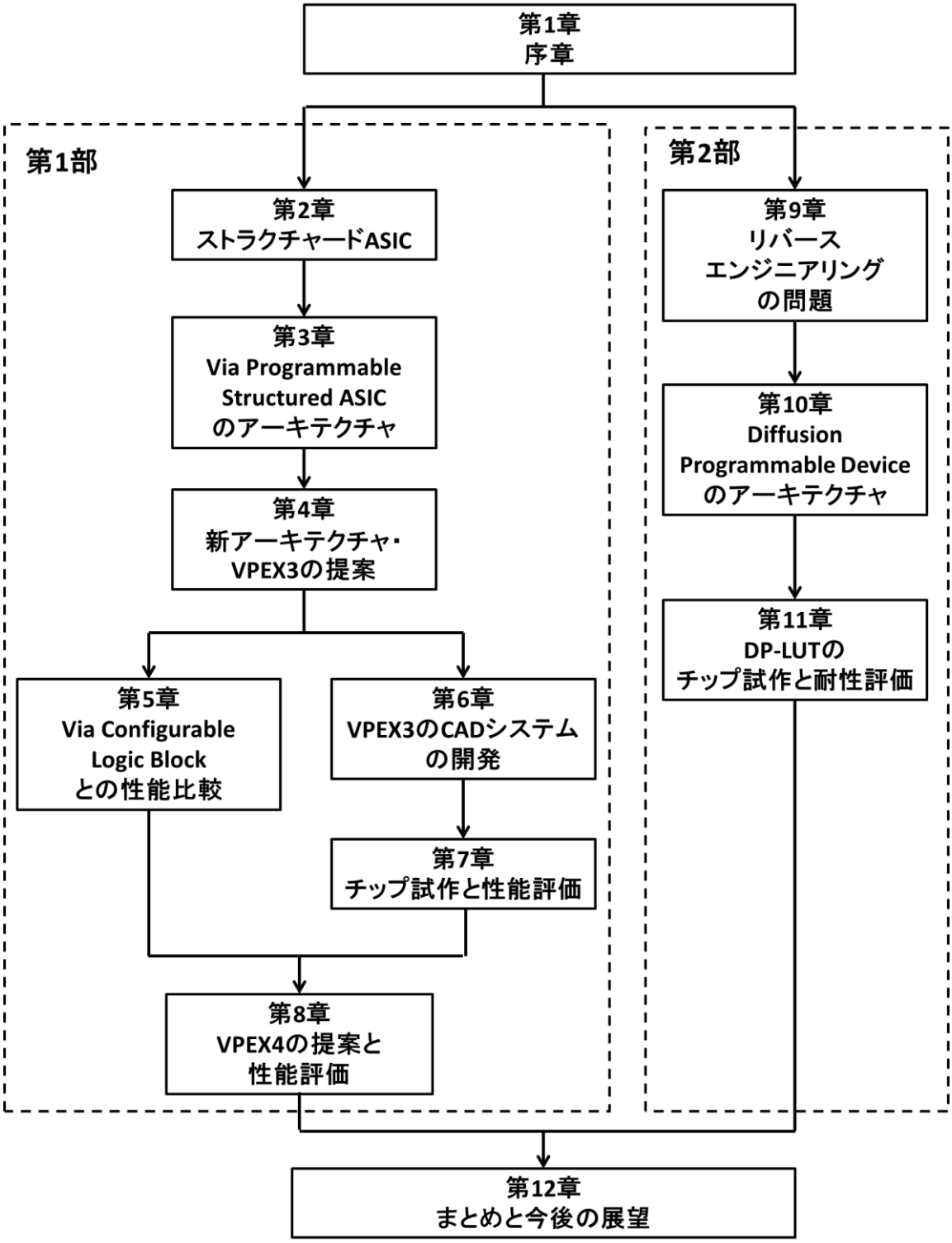
LSI 機能を特定する行為（攻撃）には「破壊攻撃」と「非破壊攻撃」の 2 種類存在し，RE は破壊攻撃に分類される．IC チップをパッケージング（packaging）している樹脂を取り除き，上層配線から順番にパターンを把握してゆく．金属配線層の除去にはエッチング（etching）装置やグラインディング（grinding）装置，撮影には光学顕微鏡（OPC : Optical Microscope）や電子顕微鏡（EM : Electron Microscope）など，LSI の製造工程や検査工程に用いられている装置によって実現される．したがってハードウェアの RE は上層から下層に向かって順に実行されるため，基板表面に近いほど解析コストが高くなる傾向にある．

この RE 問題に対応するためにディフュージョンプログラマブルデバイス（DPD : Diffusion Programmable Device）と呼ばれる MPD を考案した．このデバイスは LSI 上層よりも解析コストが高く，また解析自体も困難だといわれている拡散領域（Diffusion Region）に注入する(doping)不純物を N 型（donor），P 型（acceptor）から選択することで回路機能を変化させるものである．本提案は注入材料の変更や不純物注入量の調整などを含まないため，製造工程を変更する必要がない．そのため標準的な製造工程のまま回路を製造することが可能である．試作したチップの動作検証や実際にチップ構造を解析することで判明した DPD の RE 耐性について報告し，さらなる改良に向けた課題点について考察していく．

１．２　構成

本論文は層の一部を変更することで任意の LSI を実現するデバイス MPD の実例・応用例として，ストラクチャード ASIC と耐 RE デバイスの 2 つのデバイスについて論じたものである．本論文では第 1

部をストラクチャードASIC，第2部を耐REデバイスについて論じる論文構成としている．第2章ではストラクチャードASICの特徴や性能をASICやFPGAとの比較から明らかにし，ストラクチャードASICの一種であるビアプログラマブル・ストラクチャードASIC（VPSA：Via Programmable Structured ASIC）の長所・利点を説明していく．3章ではVPSAの基本構造に触れ，さらに今回の研究のために設計したロジックエレメント（LE：Logic Element）をいくつか紹介する．4章では既存LEの問題点を考察し，それらの改善を踏まえた新しいVPSAアーキテクチャ「VPEX3」について説明していく．後の5章ではVPEX3の性能評価と他のアーキテクチャとの比較を行う．続く6章ではVPEX3のチップ試作のため開発した専用CAD環境について述べ，7章に2種類の試作チップとその性能評価結果について報告する．8章では5章，7章の性能評価結果から得られた課題点を元にさらに改良を施した次世代VPEXアーキテクチャ「VPEX4」を紹介し，この性能評価結果を報告する．この8章でVPEXに関する議論を終え，続く9章ではリバースエンジニアリングの脅威と既存の対策手法について述べる．10章ではDPDの構造や論理素子，配線方法について説明し，11章では試作したチップを用いたDPDのRE耐性評価の結果について報告する．最後に本論文のまとめ，今回の論文では検討しきれなかった課題や今後の展望について論じる．


第1章
序章
第1部
第2章
ストラクチャードASIC
第3章
Via Programmable
Structured ASIC
のアーキテクチャ
第4章
新アーキテクチャ・
VPEX3の提案
第5章
Via Configurable
Logic Block
との性能比較
第6章
VPEX3のCADシステム
の開発
第7章
チップ試作と性能評価
第8章
VPEX4の提案と
性能評価
第2部
第9章
リバース
エンジニアリング
の問題
第10章
Diffusion
Programmable Device
のアーキテクチャ
第11章
DP-LUTの
チップ試作と耐性評価
第12章
まとめと今後の展望

第 1 章の参考文献

[1] 田邉功，竹花洋一，法元盛久，“フォトマスク 電子部品製造の基幹技術”，東京電機大学出版局，東京，4 月 2011.

[2] Artur Balasinki, “Multilayer and multiproduct masks: cost reduction methodology”, IEEE Transactions on Semiconductor Manufacturing, Vol.19, No.1, pp.121-129, Feb. 2006.

[3] Stephen D. Brown, Robert J. Francis, Jonathan Rose, and Zvonko G. Vranesic, “Field-Programmable Gate Arrays”, Springer Science & Business Media, June 1992.

[4] Stephen Trimberger, “Field-Programmable Gate Array Technology”, Springer Science & Business Media, Jan. 1994.

[5] 末吉敏則，天野英晴，“リコンフィギャラブルシステム”，（社）オーム社，東京， 8 月 2005 年.

[6] Ian.Kuon and Jonathan.Rose, “Measuring the gap between FPGAs and ASICs,” IEEE Trans. Computer-Aided Design, vol. 26, no. 2, pp. 203–215, Feb. 2007.

[7] Ian Kuon and Jonathan Rose, “Quantifying and Exploring the Gap Between FPGAs and ASICs”, Springer Science & Business Media, New York, Oct. 2009

[8] B. Zahiri, “Structured ASIC: opportunities and challenges,” in Proc. Int. Conf. Computer Design, Oct. 2003, pp. 404-409

[9] N. Shenoy, J. Kawa, and R. Camposano, “Design automation for mask programmable fabrics,” in Proc. Design Automation Conf., June 2004, pp. 192–197

[10] Akihiro Nakamura, Masahide Kawarazaki, Kouta Ishibashi, Masaya Yoshikawa, Takeshi Fujino, “Regular Fabric of Via programmable Logic Using Exclusive-or Array (VPEX) for EB direct Writing”, IEICE Trans. on Electron, Vol.E91-C, No.4, pp.509-516, April 2008.

[11] L. R. Avery, J. S. Crabbe, S. Al Sofi, H. Ahmed, J. R. A. Cleaver, and D. J. Weaver. “Reverse Engineering Complex Application-Specific Integrated Circuits (ASICs)”, Proceedings of Diminishing Manufacturing Sources and Material Shortages Conference (DMSMS 2002), March 2002.

[12] Nohl, K., Evans, D., Starbug, Plotz, H. “Reverse-Engineering a Cryptographic RFID Tag”, Proceedings of the 17th USENIX Security Symposium, 2008.

[13] Torrance, R., James, D. “The State-of-the-Art in IC Reverse Engineering”, Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol.5747, pp.363-381. Springer, Heidelberg (2009)

[14] Randy Torrance and Dick James, “The state-of-the-art in semiconductor reverse engineering”, In the Proc. of ACM/EDAC/IEEE, 48th Design Automation Conference (DAC), pp.333–338, June 2011.

[15] 情報処理推薦機構（IPA），“平成 11 年度 スマートカードの安全性に関する調査 調査報告書”，https://www.ipa.go.jp/security/enc/smartcard/sc.html，2 月 2000 年,

第２章　ストラクチャード ASIC

この章では本論文のキーワードの１つとなっているストラクチャード ASIC（Structured ASIC）について解説する. ストラクチャード ASIC は高騰した大規模集積回路（LSI：Large Scale Integrated circuit）の初期開発コストを抑えるために考案された設計手法の一つであり，セミカスタム（Semi-custom）LSI に分類される．本章ではまず現行の主要な LSI 開発手法の 2 種である特定用途向け集積回路（ASIC：Application Specific Integrated Circuit）とフィールドプログラマブルゲートアレイ（FPGA：Field Programmable Gate Array）について説明し，それぞれの特徴やメリット・デメリットを明らかにする．その上でストラクチャード ASIC の有効性について ASIC と FPGA と対比させて説明することで，本研究における課題の解決にストラクチャード ASIC が有効である根拠を示す.

２．１　ASIC（Application Specific Integrated Circuit）

ASIC とは特定使用用途に特化したハードウェア機構（論理回路・デジタル回路・アナログ回路）によって構成された LSI の一種である. 汎用的に作られた CPU やメモリを使用してハードウェアを作るのではなく，必要なシステムのみに機能を絞って１つの LSI を実現する手法であり，仕様に合わせた最適なハードウェア構造を選択できるため高い集積度と性能を実現する事が可能である.

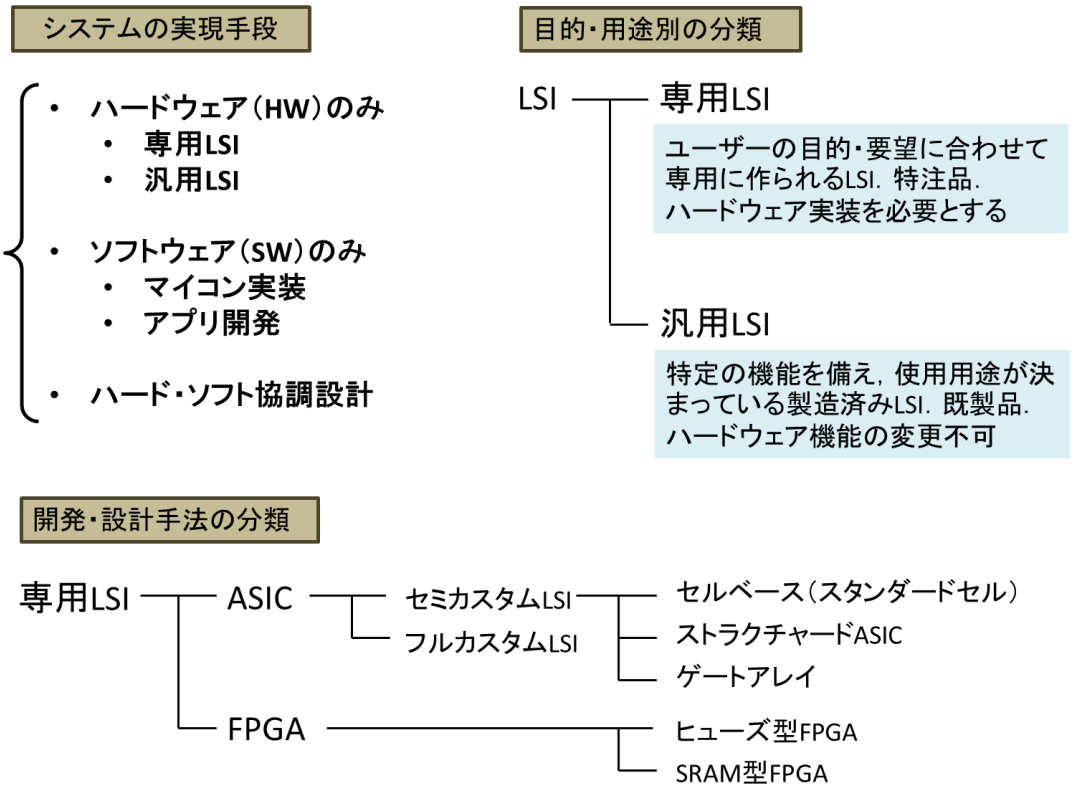


図２．１　ASIC と他の設計手法の分類

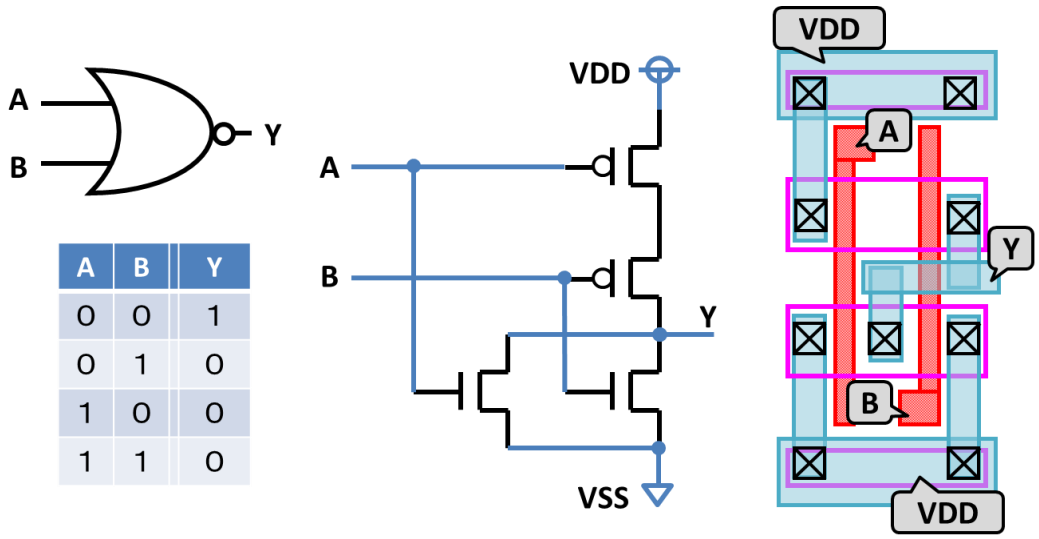
LSI には ASIC 以外にも図２．１で示すような分類名称が存在する[1]．ASIC はシステムをハードウェアのみで実現する手法の一つであり，要件に合わせて専用機能を設計する専用 LSI の一つである．また開発・設計手法の分類として ASIC を見た場合，製造時に回路を造りこむ開発手法全般を指し，FPGA のような製造後に論理回路を実装する手法との対比として用いられる．この ASIC は文献によっては特定ユーザ向け IC（USIC：User Specific Integrated Circuit）や特定顧客向け特定用途 IC（ASCP：Application specific customer product）という名称が使用される場合がある．また他の定義として，特定のシステム開発におけるハードウェア実装の総称として ASIC が用いられている場合もある．この場合ではマイコンへの組み込み実装やソフトウェア実装との対比として用いられる．

現在のデジタル開発ではセルベース方式と呼ばれる ASIC の分類の１つが主流である．

２．１．１　セルベース（cell base）方式

セルベース方式とは ASIC の分類の一つであるセミカスタム LSI のさらに小分類された方式の１つである．近年の LSI の大規模化に伴って，論理回路を手作業でレイアウトパターン（layout patter）に変換するフルカスタム（full-custom）LSI による設計は非常に困難なものになってきた．そこで論理接続情報からレイアウトパターンを自動的に作り出すデザインオートメーション（DA：Design Automation）技術が使われている．セルベース方式は DA を利用することで高性能な論理回路のレイアウトパターンを作り出す手法の１つである．この方式では，まずセル（logic cell）と呼ばれる論理構造と入出力座標を示したレイアウトパターンが定義される．セルにはスタンダードセル（standard cell）とマクロセル（macro cell）の２種類のセルが存在する．

スタンダードセルの例を図２．２に示す．スタンダードセルは論理回路を構成する上で標準的に使用される論理ゲート回路（Inverter：反転論理，AND：論理積演算，OR：論理和演算など）のレイアウトパターンが定義されたものである．図２．２は入力 NOR 回路（NOR2）の例を示している．



（a）ミル記号＆真理値表　　（b）スケマティック図　　（c）レイアウト図

図２．２　スタンダードセル（NOR2 の場合）

図２．３にスタンダードセルを用いた回路構成を示す．セルベース方式では論理合成（logic synthesis）の結果に応じて使用する基本論理ゲートをこのスタンダードセルの集合（セルライブラリ）の中から選択し，チップ上に配置し，相互接続を施すことでチップ全体のレイアウトパターンを作りこんでいく．またスタンダードセルとして存在しないメモリブロックやアナログ回路を予めマクロセルとして登録しておくことで，これらを混載した大規模なシステム構成の開発にも対応する事が可能である．こうして一度デザインされたデジタル回路のブロックを設計資産（IP コア：Intellectual Property Core）として登録しておき，別の設計で回路の一部として実装することも容易である．

スタンダードセル方式は最小論理単位から単位ブロック，全体へとボトムアップ方式で回路を作りこんでいく方式である．そのため回路設計の自由度が非常に広く，後述する FPGA と比較して高密度・高集積の LSI を実現することができる．

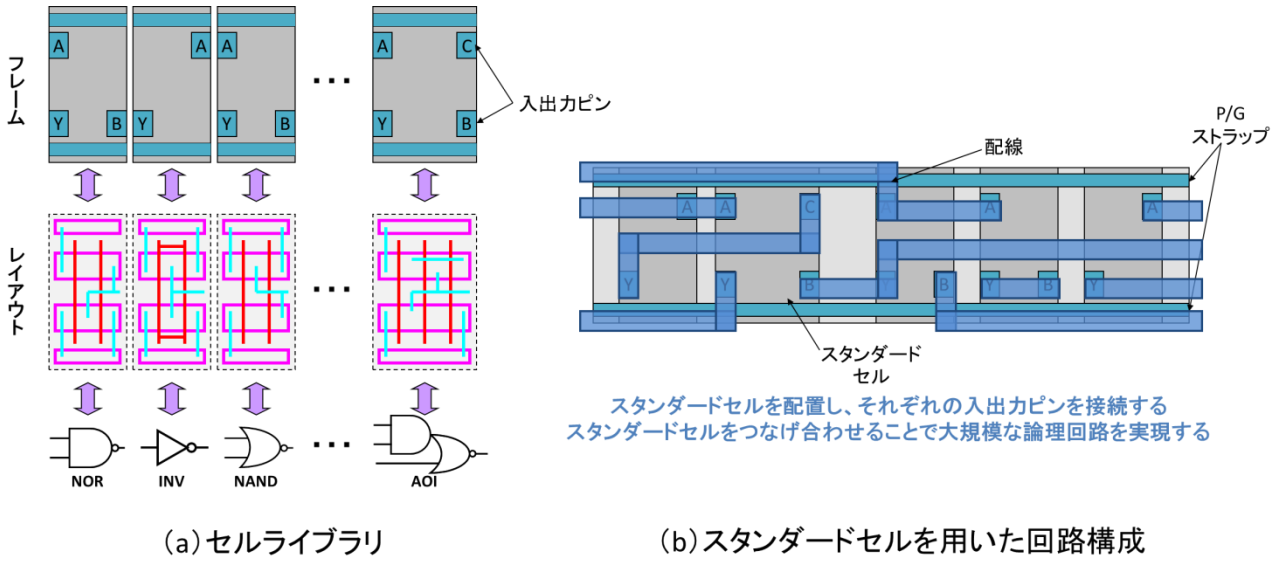


図２．３　セルライブラリとセルの配置・配線

２．１．２　ASIC の課題点

セルベース方式に限らず ASIC ではフォトリソグラフィ（photolithography）と呼ばれる製造技術を用いてシリコン（Si）基板上にレイアウトパターンが形成される．フォトリソグラフィにおけるパターン形成は「フォトマスク製造」と「紫外線露光」という工程を経て実現される．

まず前述した方法で設計された回路のレイアウトパターンをレチクル（reticle）と呼ばれる透明なガラス板（合成石英ガラス[2]）に描画（drawing）する．描画には電子線（EB：Electron Beam）露光装置と呼ばれるフォトリソグラフィ装置とは別の装置が利用される．図２．４にフォトマスク製造のパターン形成工程を簡略化したものを示す．作成したレイアウトパターンはフォトマスク上において遮光性材料のパターンとして形成される．また形成後は欠陥検査・修正工程を経て，保護膜（ペリクル）でマスク表面全体を覆うことで完成する．

通常の LSI は積層構造になっており，フォトマスクは各層毎に分けて製造される．１つの ASIC を作るためのフォトマスクの集合をマスクセット（mask set）と呼び，近年の ASIC では 30~60 枚ほどのフォトマスクがマスクセットに必要となる．フォトマスクに形成されたレイアウトパターンのことをマス

クパターンと呼び，遮光材料と反射防止膜の 2 層膜構造が一般的である[2]．これには遮光材料としてピュアクロム（Cr），反射防止膜として酸化クロム（Cr_2O_3）が用いられる[2]．

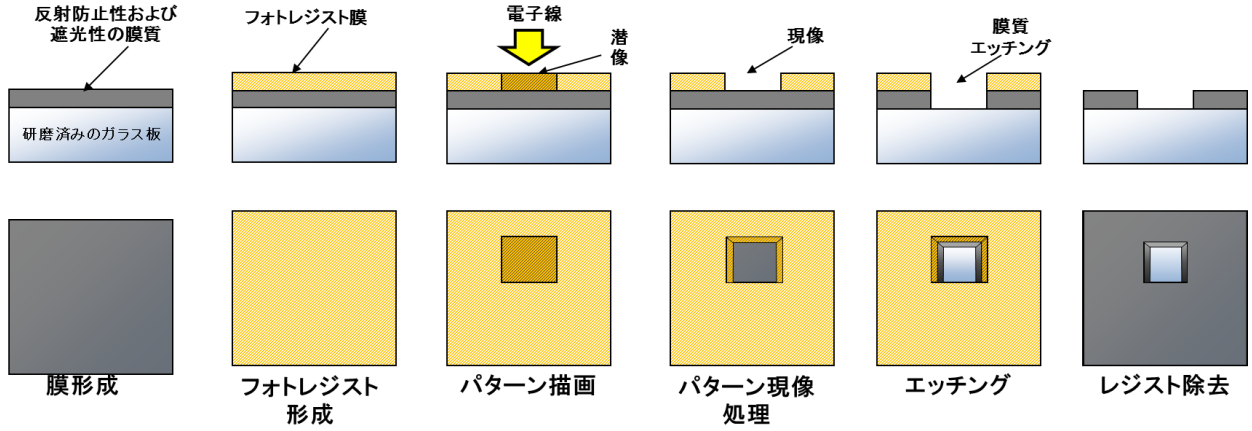


図２．４　フォトマスクの作成[2,3]

次に作成したマスクセットを用いてシリコン基板上に現像・露光する手法を図２.５に示す．フォトマスク製造時と同様，半導体基板上にレイアウトパターン（ゲート酸化膜，AL 膜，層間絶縁膜など）を形成する際はフォトレジストを介して加工する．大部分はフォトマスク製造工程と同様であるが，パターン転写（transfer）工程が大きく異なり，このフォトレジストの加工にはマスクパターンが加工されたフォトマスクと紫外線が利用される．IC の製造において電子線を用いない理由は生産効率（ウェハ１枚を加工する製造スループット）を向上させるためである．フォトマスクと違い IC そのものは短時間に大量に生産する必要がある．

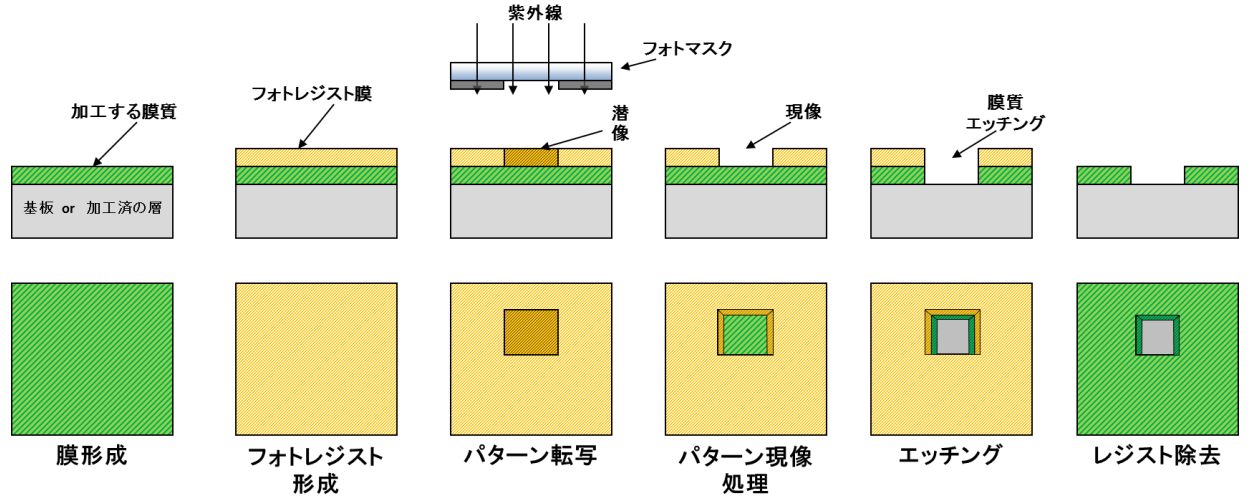


図２．５　フォトリソグラフィによる製造工程[2,3]

この方法以外にも膜形成を行わずにエッチング時に結晶成長させるものや，蒸着・塗布する場合もある[3]．いずれにしろ，LSI 製造において微細パターンを転写して加工するためのフォトマスクと露光技術は欠かすことが出来ない．

しかしこのフォトリソグラフィ製造技術を用いて最先端の ASIC を実現することが近年非常に難しくなってきている．図２．６はプロセス毎のマスクセット（mask set）あたりのマスク枚数の変移，図２．７はプロセス毎のマスクコスト(mask cost)の変移をそれぞれ表したものである．図で示すように１セットあたりのフォトマスク枚数はプロセスの微細技術向上とともに増化しており，それに伴ってフォトマスク費用が高価になっているのがわかる．またこれは多層化によるマスク枚数増加の影響だけではない．マスク製造装置に求められる性能がきわめて高度化したことによる製造装置開発費用の高騰や，フォトマスク １ 枚を仕上げるために要する時間の増大によって生産性が大きく低下したことなども影響している．チップ単価にはこのマスクコストの一部が上乗せされており，マスクコスト急騰の影響から現在の LSI チップ単価（unit cost）も数世代前と比較して非常に高価になっている．

この膨大なマスクコストに起因するチップ単価問題を緩和するための手段を５通り紹介する．

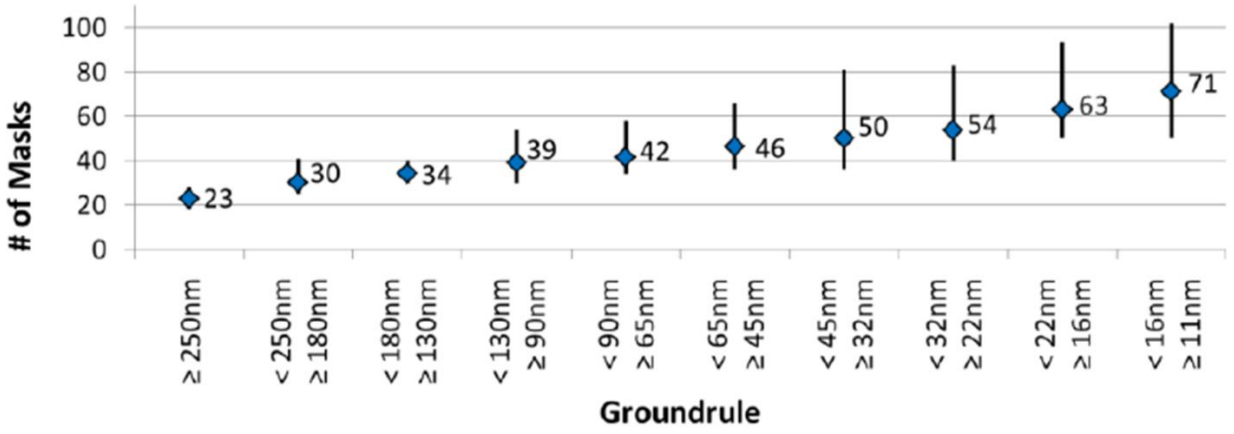
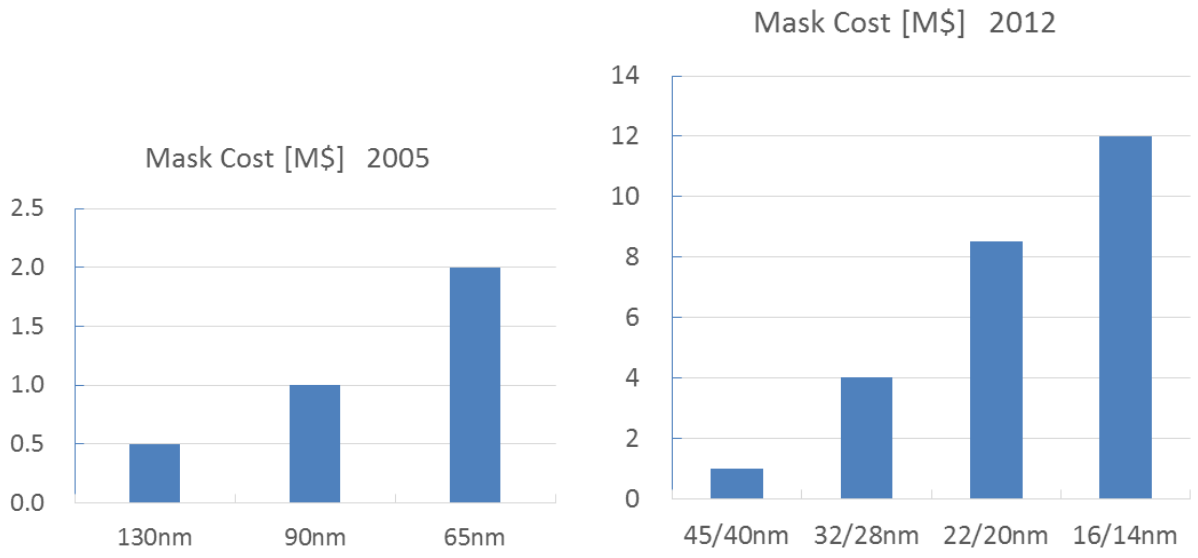


図２．６　プロセス枚のフォトマスク枚数[4]



（a）2005 年報告[5,6]　　（b）2012 年報告[7]

図２．７　製造プロセス毎のフォトマスク製造コストの遷移

（1）大量生産

1つは大量生産である．フォトマスクは 1 つの製品を生産するために繰り返し使用される．そのためチップ生産数に応じてチップ単価に影響するマスクコストが異なる．マスクコストをチップの価格に上乗せする場合，1 個当たりのコストはそのフォトマスクによって製造される生涯生産数に反比例する．したがって大量生産する場合であればチップ 1 枚あたりのマスクコストを低く抑えることができ，高価なマスクセットを用いた場合であってもチップコストを安価にする事ができる．当然ながらこの方法が利用できるケースは生産数分を売上に変えることのできる巨大な市場を有していることが前提である．この条件を満たせる市場は少なく現在ではゲーム，パソコン，デジカメ，スマートフォンなどのプロセッサや DSP，ネットワーク機器など ASIC というよりは特定用途向け汎用品（ASSP : Application Specific Standard Produce）に分類される分野しか残っていない．ほとんどの ASIC 市場は少量生産市場であるため，膨大な NRE コストを必要とする LSI 開発は経済的に困難である．

（2）混載マスク[2]

2つ目は混載マスクの利用である．フォトマスク 1 枚に形成するパターンは 1 デザイン 1 層が基本であるが，近年ではフォトマスク 1 枚の領域を分割し，複数のデザイン（プロジェクト）を混載させるマルチプロジェクトウェハ（MPW : Multi-Project Wafer）や複数の層を混載させるマルチレイヤーマスク（MLM : Multi-Layer Mask）が提案されている．共に設計毎のマスク枚数を削減する事が可能になりマスクコストの削減が期待できる．フォトマスクの半分以下の領域に 1 デザイン 1 層分のパターン形成を施すため，当然 LSI サイズはある程度小さい領域でなければならず，大規模デザインでは利用する事ができない．また MPW では異なるプロジェクト間で生産数や納期，チップサイズを統一する必要があり，そういった面でも利用可能プロジェクトが制限される．MLM においても時間毎に利用するフォトマスクの転写面積が小さくなることから生産性の低下が指摘されている．

（3）電子線（EB）直接描画製造法

3 つ目は EB 露光装置を用いたマスクレス加工技術の利用である．フォトマスク加工に用いるような EB 露光装置を用いて直接ウェハ上のレジストにパターンを描画する電子線直接描画製造法（EB 直描）などと呼ばれる手法が存在する．しかし電子線描画装置は生産時におけるスループットがフォトリソグラフィと比較して遅く，また電子線を用いるため稼働コストも極めて高価である．EB 直描では複雑なレイアウトを加工するために電子線描画装置を長時間専有する事になり，チップ生産コストが莫大になることが問題となっている．したがって，フォトリソグラフィの代替となるためには効率的なパターン描画・転写の実現など技術的進歩が今もなお求められている．

（4）成熟プロセスの利用

4つ目は数世代前の古い製造プロセスを再利用することである．先端プロセスにあえて乗り換えないことでマスクコストの削減を狙う方法である．実際に最新のプロセス技術を利用しても初期開発コストを回収できないため，多くの企業が数世代前のプロセス技術で LSI を製造している．

図 2.8 は SEMATEC が 2013 年までに調査した各 LSI 製造メーカが実際に運用している製造プロセスの実情を示したものである．2013 年でも 130nm 以前のプロセスが 7 割を超えており，利益（需要）

の見込める一部製品でしか，最新プロセスを利用することができない現状を示している．このデータは最新プロセスを利用した高性能な ASIC を効率よく製造できる手段が求められていることを表している．

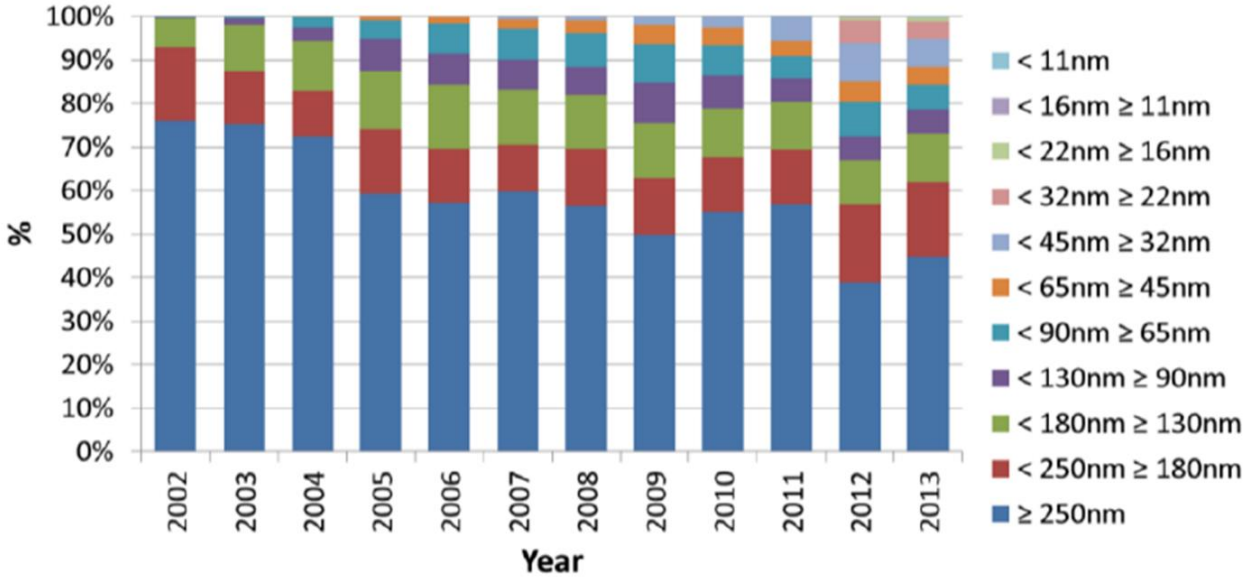


図２．８　ASIC 開発に利用されるプロセスの推移[4]

（５）FPGA

５つ目は FPGA の利用である．これは次節で説明する

※セマテック　【SEMATECH】

《 Semiconductor Manufacturing Technology 》米国半導体工業会（SIA）が中心となって 1987 年に発足した，官民共同による半導体製造技術研究組合．本部はニューヨーク州オールバニー．

２．２　FPGA（Field Programmable Gate Array）

FPGA とはプログラマブルデバイス（PLD：Programmable Logic Device）と呼ばれる ASIC とは異なる LSI 開発手法の一種である．FPGA はフォトマスクを用いて専用回路実装を行わない LSI であり，汎用品として製造された LSI に対して製造後に論理機能を変化させることが可能な専用回路の実装を行う. したがって ASIC で問題となっていたマスクコストが設計毎に発生しないという特徴を持っている．そのため少量生産を前提とした LSI の実現に適していない ASIC に取って代わり，多品種少量生産市場であり, 規格や仕様の変更が頻繁に起きる通信機器などを中心に FPGA が大きな市場を獲得している[8].

本節では PLD の持つ特徴を説明したうえで，FPGA の基本構造について説明する

２．２．１　FPGA の特徴

FPGA はチップ製造後に専用のツールキットを介して設計者が自由に論理仕様・演算機能を実装（configuration）でき，さまざまな論理回路機能の実装と変更を繰り返し行うことができる LSI の総称である. ASIC がシリコン上のトランジスタと金属配線を用いて論理回路を構成する技術であるのに対して，FPGA は電気信号の有無によって論理回路を実装することが可能な機構がトランジスタによって構築されている．製造直後の FPGA 上にはトランジスタ・金属配線は存在するが，これら自体は特定の論理回路の構造を有していない．製造後に専用の機器を通して配線の経路や電気信号の有無を変更することで所望の論理回路を実装する.

FPGA の最大の特徴はチップ製造に関わる NRE コストが発生しないことである．FPGA デバイス自身は実装される論理回路に依存して金属配線層などが変化することはない．そのため FPGA は多数のユーザに同一のチップを供給することが可能になり，1 種類のマスクセットで大量の FPGA を製造することが可能である．近年ではシステム要件が高度になり，開発の際にマイコン（Micro Controller）では目的の処理速度を達成できず，ASIC でもコストが要求を満たせない場合の選択肢として，研究・試作・データセンタ・航空宇宙開発などの少量多品種 LSI 開発を中心に需要を拡大している．また現代では最先端プロセスで開発された FPGA 市場が形成されており, 各社 FPGA ベンダー(vender)は高性能な FPGA を供給し続けることができる.

図２．９は ASIC と FPGA でそれぞれデジタル回路を開発した場合の総コストと生涯生産数の関係を表したグラフである. ASIC では主に原材料や装置稼働費の量産費用(RE コスト:Recurring engineering Costs＝running costs）以上に初期開発費用（NRE コスト：Non-recurring Engineering Costs＝initial costs）の占める割合が多く，また大半はマスクコストである．一方で FPGA はチップ単価，RE コストが高価であるものの，NRE コストは FPGA ベンダーが負担しているため，マスクコストは発生せず，少量生産分野では ASIC よりも安価に論理回路を実現することができる.

PLD デバイスが提案された当初はプログラマブルリードオンリーメモリ（PROM：Programmable Read Only Memory）やアンチフューズ（Antifuse）を用いて一度限り所望の論理回路を実装できるデバイスのみであったが，現在ではスタティックランダムアクセスメモリ（SRAM：Static Random Access Memory）などの書き換え可能な揮発性メモリ(volatile memory)とフラッシュメモリ（Flash memory）のような大容量の不揮発性メモリ(non-volatile memory)を組み合わせることで，何度でも論理回路情報を書き換えることが可能なデバイスに進化している.

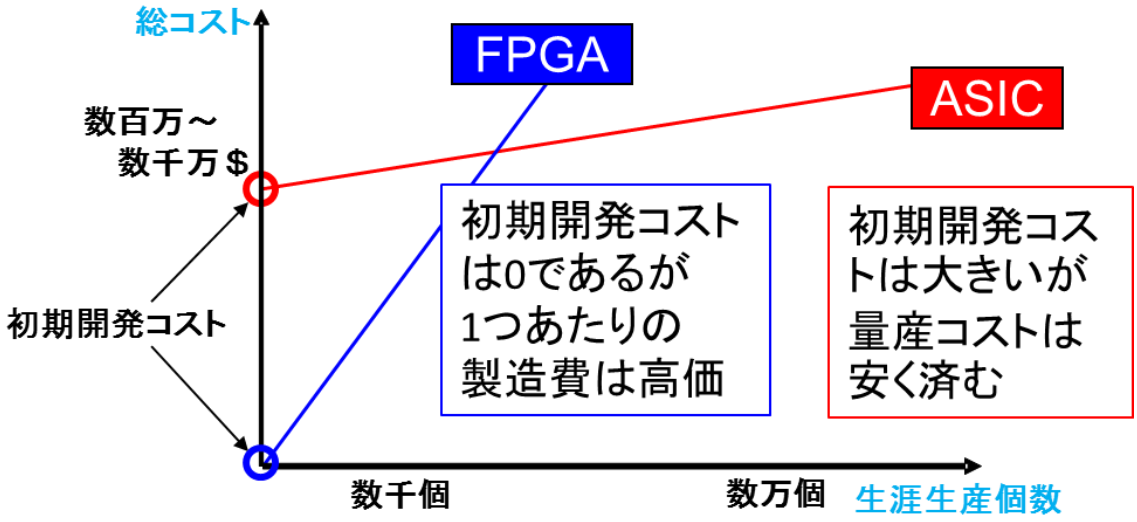


図２．９　ASIC と FPGA の生涯生産数と総コストの関係

２．２．２　FPGA の構造・性能

図　２．１０に FPGA の基本構造を示す. 一般的な FPGA はロジックエレメント（LE : Logic Element）と呼ばれる論理構成要素をアレイ状に並べ, LE の間にコネクションブロック（CB : Connection Block）とスイッチブロック（SB : Switch Block）を配置した構造をしている．設計・製造時点では LSI 内部に目的とする論理回路自体は実装されておらず，論理素子を相互接続することで論理回路を形成する仕組みになっている．したがって論理回路に機能上の問題が見つかり，やむをえず仕様を見直す場合においても，設計者やユーザの手元ですぐに修正することが可能である．このような特徴がフィールドプログラマブル（現場でプログラム可能）と呼ばれる所以となっている．

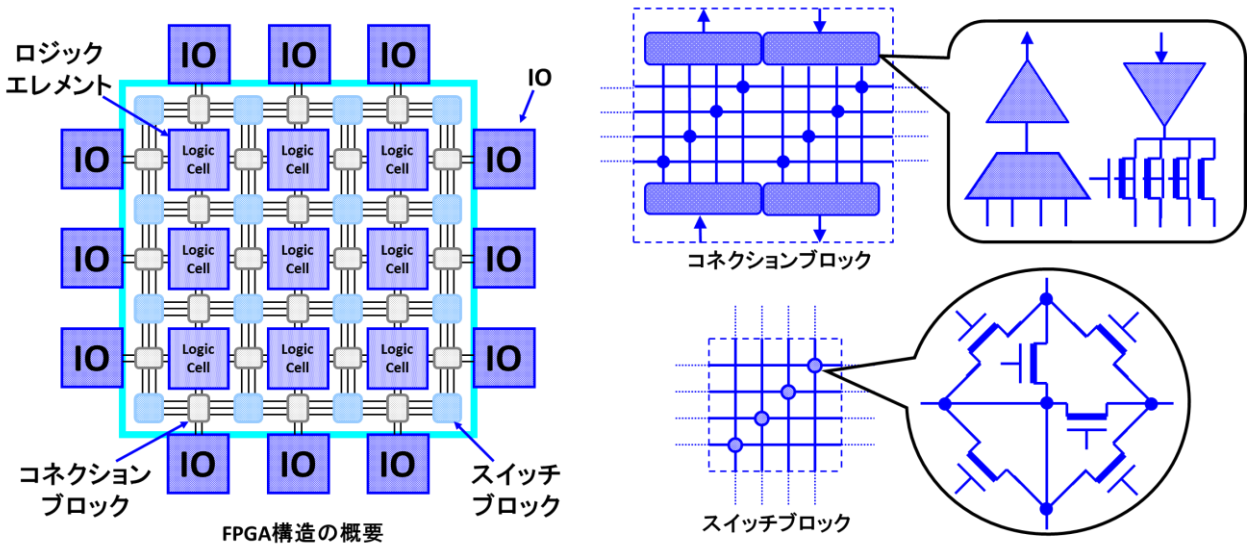


図２．１０　FPGA の基本構造[8]

FPGA は特定用途向けの論理回路をいつでも自由に実装することができ，また回路上のミスやバグを容易に修正することが可能である．その一方で LSI の大半をフィールドプログラマブルを実現するための機構（メモリやトランジスタスイッチ）に割くことになり，論理実装時の面積効率や消費電力の性能がセミカスタム LSI よりも大きく劣っているという問題がある[9,10]．図２．１１は同製造プロセス（90nm プロセス）における ASIC と FPGA の性能差を示したものである．

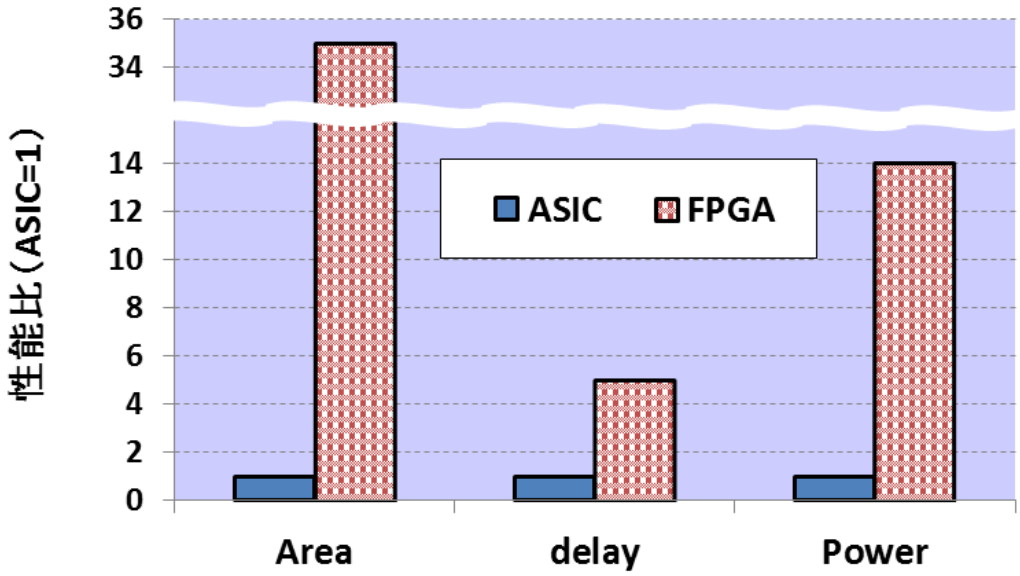


図２．１１　同製造プロセス帯における FPGA と ASIC の性能差[9,10]

図２．１１のように，同一プロセスにおいては ASIC の 35 倍もの面積と 14 倍もの電力を必要とする．そのためにモバイル機器や小型デバイスの適応が難しく，全ての少量生産分野の ASIC を置き換えるに至っていない．このように性能面・低電力化においては現在でも課題が存在している．

２．３　ストラクチャード ASIC

表２．１に ASIC と FPGA の特徴をまとめる．

表２．１　ASIC と FPGA の特徴と比較

	長所	短所
ASIC	高速動作 高集積 省電力 量産時のコストが低い	開発期間の長期化 製造後の変更・修正が困難 フォトマスクコストが高く，少中量生産に不向き
FPGA	開発期間が短い 製造後の論理変更可能 少量生産に対応	動作速度が低い 集積度が低い 高消費電力 チップ単価が高い

表２．１で示すように，ASIC と FPGA の双方では得意とする生涯生産個数や要求仕様（性能）が異なり，実装するハードウェアの用途によって製造手法を使い分ける必要がある．しかしながら少量多品種 LSI 製造において高性能な回路を安価に実現したい場合，ASIC，FPGA 両製造手法とも不向きであることがわかる．

このような現状に対して新しい LSI の設計・製造手法が提案されている．それがストラクチャード ASIC[11-13]と呼ばれる手法である．

２．３．１　ストラクチャード ASIC の特徴

ストラクチャード ASIC はあらかじめ構造が決定された（fixed）層を有する LSI 構造を利用してマスクコストを削減する設計・製造手法である．名前に ASIC があるように，製造工程自体は ASIC と同様フォトリソグラフィ技術が用いられる．

図２．１２にストラクチャード ASIC の基本構造を示す. ストラクチャード ASIC ではあらかじめ LSI 構造の大部分が定義済みのレイアウトパターンとして設計者（designer）に提供される．この提供される層の事をマスター層（master layer），欠落している層をカスタム層（custom layer）と呼ぶ．所望のカスタム層を作成することで１つのマスクセットが完成し，論理回路を製造することが可能になる．マスター層を作るためのフォトマスクをマスターマスク（master mask），カスタム層を作るためのマスクをカスタムマスク（custom mask）と呼ぶ．マスターマスクはこの設計・製造手法を利用するすべてのプロジェクト・デザインで共通なものを利用することができる．そしてマスターマスクは基本的に LSI 製造工場（ファブ）を持つベンダーから提供されるため，マスターマスクのマスクコストは NRE コストには含まれないことになる．このようにストラクチャード ASIC はカスタマイズ可能な領域を「層」という区切りで制限しておくことで，フォトリソグラフィ時に新たに必要となるフォトマスクの削減を実現している．マスクセットの一部のみを変更して LSI を設計するデバイスは Mask Programmable Device（MPD）と呼ばれ，ストラクチャード ASIC はこの MPD の一種である．カスタム層はスライス

層（slice layer）とも呼ばれ，図２．１３のように 2 種類の役割を持ったフォトマスクを活用して LSI を開発するためマスター・スライス（master-slice）方式とも呼ばれる．

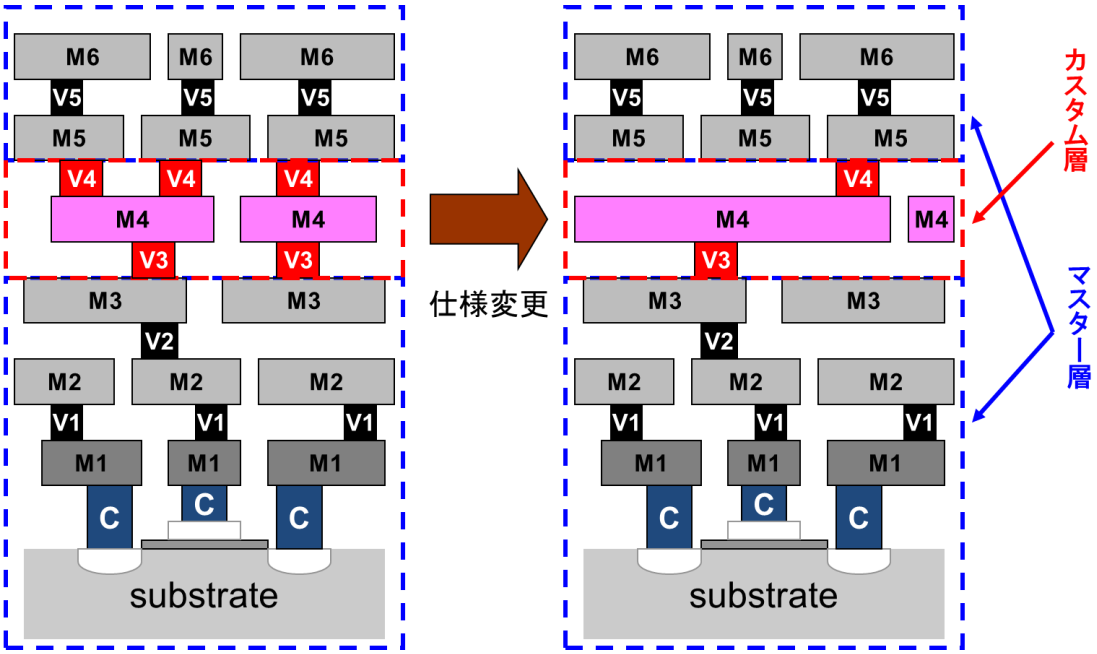


図２．１２　ストラクチャード ASIC の構造

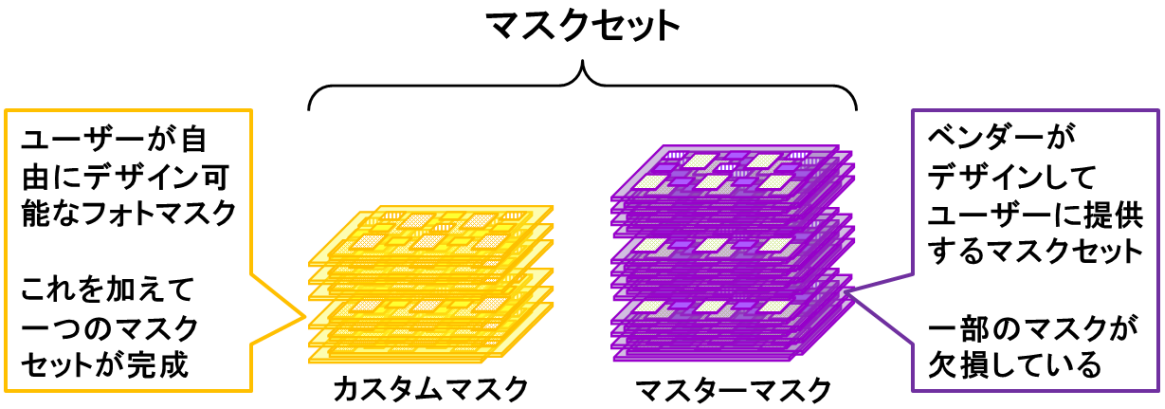


図２．１３　ストラクチャード ASIC におけるフォトマスクセットの分類

ストラクチャード ASIC は設計や製造に要する期間がセルベース方式よりも短く，NRE コストを下げることが可能である．このことから FPGA よりも高性能・高機能な小両～中量生産市場の LSI を実現する製造手段として期待されている．

表２．２は他研究機関や企業によって研究・開発が行われているストラクチャード ASIC を示している． HardCopy[14]は ALTERA 社の提供しているストラクチャード ASIC であり，同社が販売している FPGA デバイスの IO ピンやパッケージ規格と互換性を持っている．そのため FPGA でテストを行ったデバイスを HardCopy に置き換えることで性能向上や低消費電力化を簡単に実現する事ができる．また

開発チップの需要が上昇した際に HardCopy 化することでチップ量産時の単価を下げ，トータルのコストを削減するなどの市場に合わせた臨機応変な提供形態の変更を実現している．Nextreme[15]は eASIC 社のストラクチャード ASIC である．ビア層を 1 層変更することでカスタマイズができる VPSA（後述）の一種である．その他にも Triad Semiconductors 社の VCA[16]，BaySand 社の TeneX[17]，元智大学の研究している VCLB[8-10]など数多くのアーキテクチャが存在している．

表２．２　他ストラクチャード ASIC の種類

	HardCopy[14]	Nextreme[15]	VCA[16]	TeneX[17]	VCLB[18-20]
プロセス	28nm-180nm	28nm-90nm	180nm-350nm	28nm-90nm	180nm
研究機関	ALTERA	eASIC	Triad Semi.	BaySand	元智大学

２．３．２　ゲートアレイ方式との違い

マスター・スライス方式と呼ばれる製造手法には，ストラクチャード ASIC の他にゲートアレイ（GA：Gate Array）方式が存在する．GA はゲート酸化膜層や拡散層などをマスター層として作り置き，金属配線層をカスタマイズして論理回路を形成する．

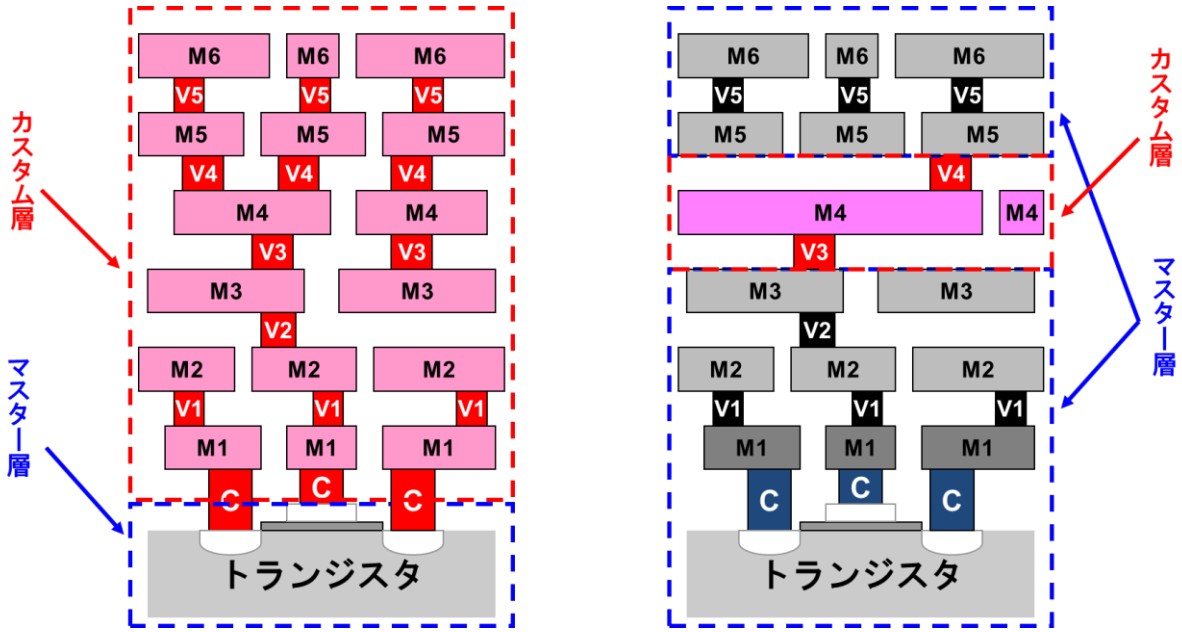


図２．１４　ゲートアレイ(左)とストラクチャード ASIC(右)の層構造の違い

両者にはセル（最小論理素子）の構成方法に違いがある．GA では金属配線層全体を自由に作り替えることが可能なため，ゲート素子を単純に整列させた Sea of Gate 構造が用いられる．必要な数のゲートを Sea of Gate から選び，相互接続することで 1 つのセルを形成する．ストラクチャード ASIC では下層の金属配線層を変更することはできないため，利用されやすいスタンダードセルなどをあらかじめ構築しておき，上層配線で使用の可否を決めるといった使われ方がされる．したがってカスタムマスクに使用される自動化支援（EDA：Electronic Design Automation）ツールが異なるなど開発環境に違いがある．

２．４．Via Programmable Structured ASIC

ビアプログラマブル・ストラクチャードASIC（VPSA：Via Programmable Structured ASIC）とはカスタム層を「ビア配線層」にのみに制限し，メタル配線層すべてを「マスター層」に含めたストラクチャードASICの事である[21-23]．ビア配線層はLSIの上層を構成する金属配線層領域の一部であり，メタル配線層の間に存在する．層の異なるメタル配線同士を短絡させる（接続する）ためのビア（Via）を形成する層であり，下層と上層の配線を接続する役割を担っている．VPSA ではすべてのメタル配線層をマスター層として作りこんでおき，ビアよって配線間を繋いでいくことのみで論理素子同士の接続を実現する．

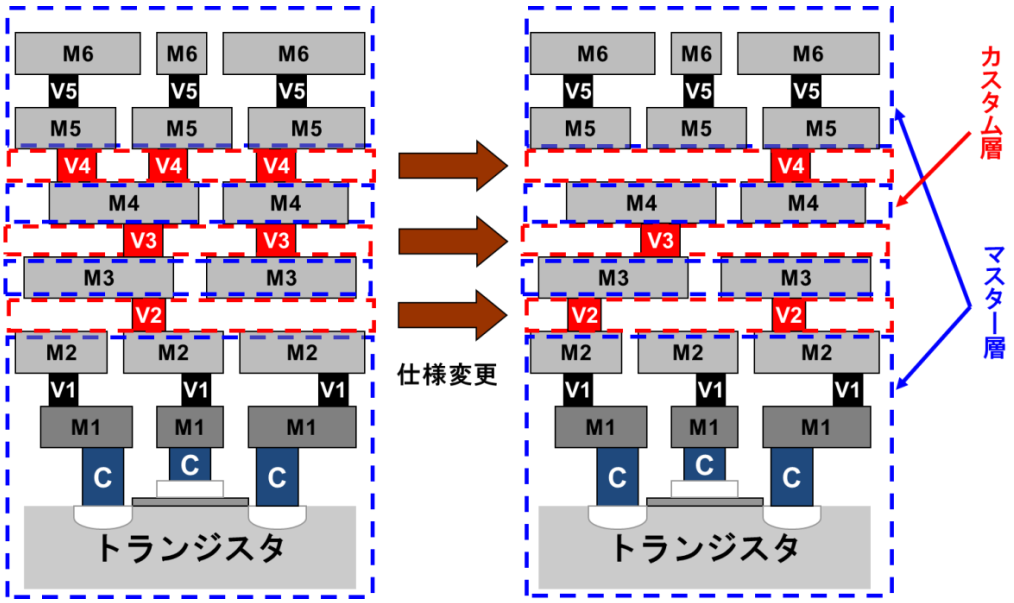


図２．１５　ビアによるストラクチャードASICのプログラマブル例

VPSA は研究機関や企業によってプログラマブル（programmable）の部分がコンフィギャラブル（configurable），アダプティブ（adoptive）などの名称になっている場合がある．また「ストラクチャードASIC」の部分もデバイス（device），ロジックアレイ（logic array），ゲートアレイ（gate array）などに変更された名称で語られることもある．本論文ではビアプログラマブル・ストラクチャードASICあるいはVPSAと呼称する

２．４．１　電子線直接描画製造法との親和性

EB直描では，従来のリソグラフィ技術と異なりフォトマスクを用いず直接レジストに電子回路のパターンを描画する．1度に描画できるレイアウト面積は非常に小さく，フォトリソグラフィと比較すると製造スループットが非常に遅い．しかし時間をかければマスクコストなしでLSIを仕上げることができるためマスクコストを安価に抑えたい生涯生産個数の少ないLSIや研究目的・試作のためのLSI開発などで用いられてきた．また近年では一定の範囲（キャラクタライズサイズ）を一度に EB 描画を打ち込むことの出来るキャラクタ・プロジェクション（character projection）[24-26]描画装置も開発されており，

これを使用すると大幅に描画スループットを向上させることが可能である．はじめに EB 直描技術の特徴をいくつか列挙する．

(a) 面積密度と寸法精度[27-29]

EB 直描におけるパターン描画の精度は描画対象の面積密度によって大きく変化する．面積密度とは描画対象のパターンとの疎密のことを示し，近接効果によって寸法精度に差が生じることが知られている[29]．したがって描画面積が大きくパターンの粗密の変化が大きい層では寸法精度を保つために工夫（近接効果補正）が必要となる．したがって，拡散領域のみならず，メタルやゲートなどの描画にも適していない．一方でビアなどの描画面積が小さいパターンを描画する場合においては寸法精度の劣化を抑えることが可能であることを示している．

(b) 露光時間

EB 直描では電子ビームの「電流密度」は「露光時間」に影響を及ぼす．レジストはある一定の電荷が与えられることで感光する．そのため「電流密度」を上げることで露光時間を短くすることができる．しかしながら電流密度を上げることは「ビームぼけ」という現象を引き起こし，寸法精度に悪い影響を与えてしまう．ビームぼけは総電流量に比例して大きくなるため，描画する面積密度が小さい場合に限ってのみ電流密度を大きくすることができる．したがってビア層のみ描画する VPSA であれば EB 直描の露光時間を短くすることが可能である．

(c) つなぎ合わせ精度

図に示すように，メタルパターンでは EB キャラクタサイズより大きいレイアウトパターンを多く持つため，EB キャラクタをつなぎ合わせないとパターンを作成することができない．この場合，正確につなぎ合わせを行わなければ，配線が断線してしまう可能性がある．一方でビアパターンはキャラクタサイズの境界面で描画するパターンを排除でき，メタルパターンのような断線を心配する必要がまったくない．

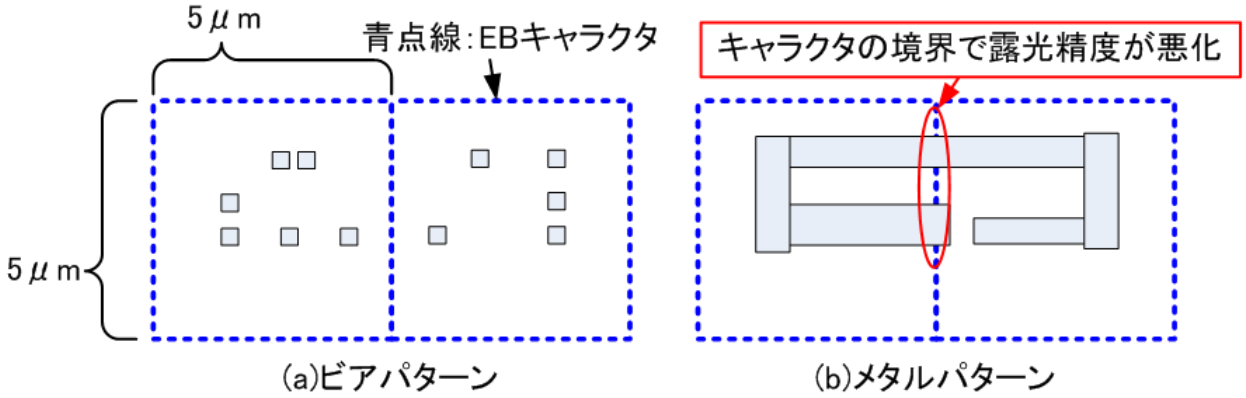


図２．１６　EB 直描の重ね合わせ精度

列挙した特徴をまとめると EB 直描はビア層の描画を高速に行うことが可能であることがわかる．これを利用するためカスタムマスクによる転写工程を EB 直描による描画工程に置き換えた VPSA について考察する．VPSA はストラクチャード ASIC の特徴を有し，少量生産品を製造する際に大きな経済効果を発揮する．しかし少ないながらもフォトマスクを製造する必要があり，初期開発にマスクコストを含む．ここで VPSA のビア層のパターン描画にのみ EB 直描技術を用いることで，わずかに存在したビアマスクのマスクコストを削減することが可能になる[30]．この VPSA と EB 直描の連携技術では描画時間の長くなる拡散層やメタル層は予め準備しておいたマスターマスクによるフォトリソグラフィで露光し，EB 直描装置でも高速に描画することが可能なビア層のみを EB 直描によって加工することでスループットの低下を抑えながらマスクレスリソグラフィ技術を実現することができる．

第 2 章の参考文献

[1] 吉本雅彦，“集積回路工学”，（社）オーム社，東京，9 月 2013 年.

[2] 田邉功，竹花洋一，法元盛久，“フォトマスク 電子部品製造の基幹技術”，東京電機大学出版局，東京，4 月 2011.

[3] 岡崎信次，鈴木章義，上野巧，“はじめての半導体リソグラフィ技術”，（社）工業調査会，東京，6 月 2003.

[4] Matt Malloy, “2013 mask industry survey”, in Photomask Technology 2013, Proceedings of SPIE Vol.8880, 88800K, Sep. 2013

[5] Artur Balasinski, “Optimization of Sub-100-nm Designs for Mask Cost Reduction”, Journal of Microlithography, Microfabrication, and Microsystems, Vol.3, No.2, pp.322-331, Apr. 2004.

[6] Charles Weber, C. Neil Berglund and Patricia Gabella, “Mask Cost and Profitability in Photomask Manufacturing:An Empirical Analysis”, IEEE Transactions on, Semiconductor Manufacturing, Vol.19, No.4, pp.465-474, Nov. 2006.

[7] Shao Jun WEI, “Sustainability Challenging Fabless Beyond 20nm”, Global Semiconductor Alliance,
http://www.gsaglobal.org/events/2012/1107/docs/slft2012_wei.pdf, Nov. 2012

[8] 末吉敏則，天野英晴，“リコンフィギャラブルシステム”，（社）オーム社，東京， 8 月 2005 年.

[9] Ian.Kuon and Jonathan.Rose, “Measuring the gap between FPGAs and ASICs,” IEEE Trans. Computer-Aided Design, vol. 26, no. 2, pp. 203–215, Feb. 2007.

[10] Ian Kuon and Jonathan Rose, “Quantifying and Exploring the Gap Between FPGAs and ASICs”, Springer Science & Business Media, New York, Oct. 2009

[11] B. Zahiri, “Structured ASIC: opportunities and challenges,” in Proc. Int. Conf. Computer Design, Oct. 2003, pp. 404-409

[12] N. Shenoy, J. Kawa, and R. Camposano, “Design automation for mask programmable fabrics,” in Proc. Design Automation Conf., June 2004, pp. 192–197

[13] Kun-Cheng Wu, Yu-Wen Tsai, “Structured ASIC, evolution or revolution?”, Proceedings of the 2004 International Symposium on Physical Design (ISPD’04), pp.103-106, April 2004. http://eda.ee.ucla.edu/EE201A-04Spring/ASIC3.pdf

[14] Altera, “HardCopy Stratix ASIC Family Technical Information”,
http://www.altera.com/support/devices/structured_asics/hardcopystratix/dev-hardcopystx.html,

[15] eASIC, “eASIC Corporation - Low Cost FPGA & Low Power FPGA & Low NRE ASIC with High Speed Transceivers Solutions - 90nm Nextreme NEW ASICs, 45nm Nextreme-2 NEW ASICs, easicopy ASIC Migration, IP Cores, Low NRE”, http://www.easic.com/

[16] “Triad Semiconductor | The Mixed Signal ASIC Company”,
http://www.triadsemi.com/vca-technology/

[17] “BaySand Inc”,http://www.baysand.com/

[18] Mei-Chen Li, Hui-Hsiang Tung, Chien-Chung Lai, and Rung-Bin Lin, “Standard Cell Like

Via-Configurable Logic Block for Structured ASICs", in Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI '08), pp381-386, April 2008.

[19] Hui-Hsiang Tung, Yu-Chen Chen, Da-Wei Hsu, Shih-Jung Hsu, Chen Sin-Yu, and Rung-Bin Lin, "Via-configurable logic block architectures for standard cell like structured ASICs", Proceedings of the 2009 12th International Symposium on Integrated Circuits (ISIC'09), pp.17-20, Dec. 2009.

[20] Hui-Hsiang Tung, Rung-Bin Lin, Mei-Chen Li, and Tsung-Han Heish, "Standard Cell Like Via-Configurable Logic Blocks for Structured ASIC in an Industrial Design Flow", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol.20, No.12, pp.2184-2197, Dec. 2012.

[21] Chetan Patel, Anthony Cozzie, Herman Schmit, and Larry Pileggi, "An Architecture Exploration of Via Patterned Gate Arrays", Proceedings of the 2003 international symposium on Physical design (ISPD'03), pp.184-189, April 2003.

[22] Yajun Ran and Malgorzata Marek-Sadowska, "On Designing Via-Configurable Cell Blocks for Regular Fabrics", Proceedings of the 41st annual Design Automation Conference (DAC'04), pp.198-203, July 2004.

[23] Yajun Ran and Malgorzata Marek-Sadowska, "Designing a Via-Configurable Regular Fabric", Proceedings of the IEEE 2004 Custom Integrated Circuits Conference (CICC'04), pp.423-426, Oct. 2004.

[24] Hiroshi Yasuda, Kiichi Sakamoto, Akio Yamada and Ken-ichi Kawashima, "Electron Beam Block Exposure", Japanese Journal of Applied Physics, Vol.30, pp.3098-3102, July 1991.

[25] Y. Sakitani1 et al. , "Electron-beam cell-projection lithography system", Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures, Vol.10, No.6, pp.2759-2763, Nov. 1992.

[26] K.Hattori et al. ,"Electron-beam direct writing system EX-8D employing character projection exposure method", Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures, Vol.11, No.6, pp.2346-2351, Nov. 1993.

[27] Takeshi Fujino, Yoshihiko Kajiya, and Masaya Yoshikawa, "Character-Build Standard-Cell Layout Technique for High-Throughput Character-Projection EB lithography", Proc. of SPIE Photomask and Next-Generation Lithography Mask Technology XII, Vol.5853, pp.160-167, June 2005.

[28] Yoshihiko Kajiya, Akihiro Nakamura, Masaya Yoshikawa, and Takeshi Fujino, "Shot number estimation for EB direct writing for logic LSI utilizing character-build standard-cell layout technique", Proceedings in SPIE Photomask and Next-Generation Lithography Mask Technology XIII, Vol. 6283, pp.62832M.1-62832M.8, May 2006.

[29] 中村明博, 藤野毅, "EB 直描によるスタンダードセル一括露光での寸法精度の検討", 第 53 回応用物理学関係連合講演会, 3 月(2006)

[30] Akihiro Nakamura, Masahide Kawarazaki, Kouta Ishibashi, Masaya Yoshikawa, Takeshi Fujino, "Regular Fabric of Via programmable Logic Using Exclusive-or Array (VPEX) for EB

direct Writing", IEICE Trans. on Electron, Vol.E91-C, No.4, pp.509-516, April 2008.

第 3 章　Via Programmable Structured ASIC のアーキテクチャ

本章ではビアプログラマブル・ストラクチャード ASIC（VPSA：Via Programmable Structured ASIC）の詳細な構造や論理回路を実現方法について説明する．VPSA ではフィールドプログラマブルゲートアレイ（FPGA：Field Programmable Gate Array）と同様にロジックエレメント（LE：Logic Element）を組み合わせて論理回路を形成する．初めに VPSA で利用される LE の特徴や LE を用いた回路構成や配置配線構造について説明する．続いて VPSA において性能を左右する LE のアーキテクチャの実例を紹介していく．ここでは中村らによって 2008 年に開発された **V**ia **P**rogrammable Device using **XE**clusive-or logic array（VPEX）[1]についても紹介する．

３．１　VPSA のプログラマブル方式

VPSA を含むプログラマブルデバイス（PLD：Programmable Logic Device）には，カスタマイズ可能な階層や構造の範囲によってマスクコストや論理自由度が異なる．これをプログラマビリティ（programmability）と定義する．図３．１は特定用途向け集積回路（ASIC：Application Specific Integrated Circuit），マスクプログラマブルデバイス（MPD：Mask Programmable Device），FPGA の各プログラマビリティにおけるカスタマイズ方法と論理自由度のトレードオフ（trade off）を示したものである．

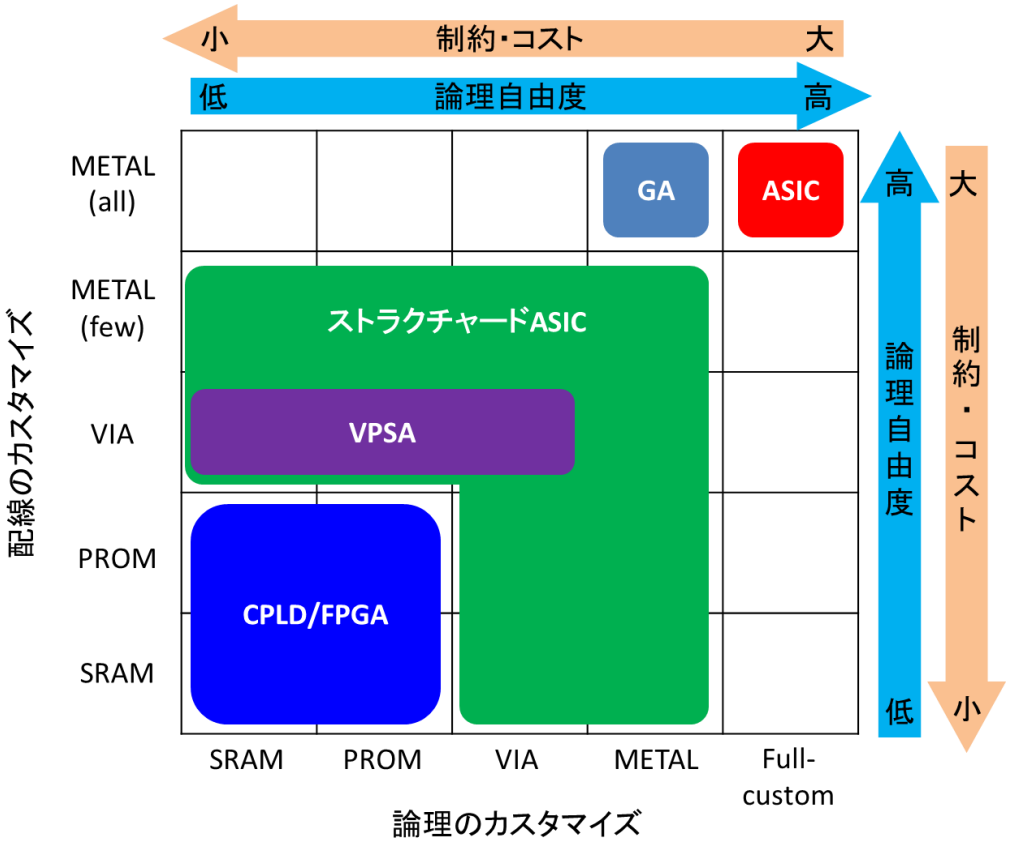


図３．１　デジタル回路のプログラマビリティによる分類

論理自由度は論理回路の性能を示しており，高いほうがより高性能・小面積・省電力な LSI を実現可能であるという事を示している．SRAM・PROM よりもビア層，ビア層のみよりもメタル層含むプログラマビリティの方がより理想に近い性能の論理回路を実現できるが，NRE コストが高価になる．VPSA には論理層のカスタマイズにビアを利用する「ビアプログラマブル方式」とメモリを用いる「メモリプログラマブル」方式の 2 種類が存在する．

この分類では VPSA は FPGA の次に自由度が低い．したがって回路性能は FPGA に近く，ASIC には及ばないものになることを示している．そのため VPSA によって設計された論理回路を ASIC の性能に近づけるためには，回路構成法や論理最適化，LE 構造など多くの工夫や技術を適用する必要がある

３．２　VPSA の基本構造

３．２．１　Logic Element

ロジックエレメント（LE：Logic Element）とは FPGA において論理回路を形成する最小論理要素である．セルベース方式の ASIC と FPGA の論理回路形成方法の違いを図３．２に示す．セルベース方式によって論理回路を形成する際，論理回路は最小論理単位の組み合わせで表現される．この最小論理単位は実際には予め定義された多種多様のスタンダードセルであり，これらを論理領域の任意の座標に配置し，相互接続していくことで論理回路を形成する．一方で FPGA の論理回路形成方法は ASIC とは少し異なる．論理最小単位を組み合わせることは FPGA においても同様であるが，FPGA においては LE が論理最小単位となるためサイズに違いがなく配置座標を変えることはできない．そのため特定座標の LE に任意の論理機能を持たせる論理機能変更を行い，論理機能を持たせた LE 同士を配線で繋げて組み合わせることで論理回路を実現する．

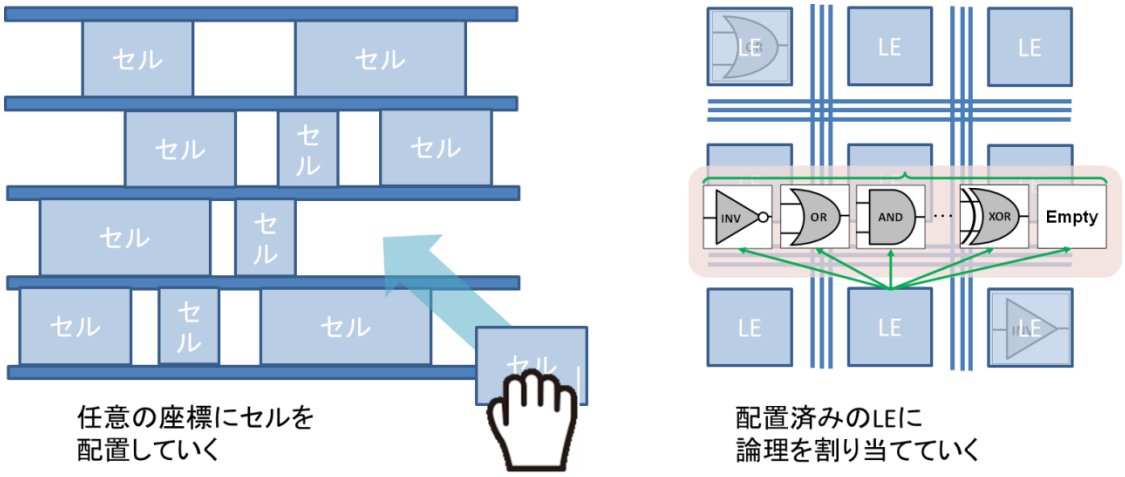


図３．２　スタンダードセル配置と LE の回路形成方法の違い

VPSA においても FPGA と同様，LE へ論理機能を持たせ，LE 間の相互接続を行うことで論理回路を形成する方法が用いられる．VPSA ではマスターマスクに論理が割り当てられていない LE の構造が形成される．この LE はトランジスタ層と一部の配線層によって形成されている．論理機能のカスタマイズはメモリあるいはカスタムマスク（ビアマスク）によって行われる．

３．２．２　Logic Element の配置構造

VPSA において LE を複数組み合わせるためにマスター層には LE を規則的に配置した構造が使用されている. この配置構造には様々なものが提案されている. 図３．３は FPGA のアイランドスタイル（island style）を VPSA で再現した構造である[2]. FPGA では SRAM とトランジスタによって再現されていたスイッチマトリクス（switch matrix）を 2 層のメタル配線を組み合わせることで実現する．これはビアによって経路を選択することが可能である．また LE と配線の接続にはクロスバースイッチ（crossbar switch）と呼ばれる交差する配線を利用することで実現される．これらは従来の FPGA に用いられているスイッチブロック（SB : switch block），コネクションブロック（CB : connection block）よりも小面積化が可能で，配線の占める割合を大きく削減することができる.

もう一つの方法は長方形の LE をタイル形状に隙間なく配置し，配線領域を形成しない構造である．概念図を図３．４に示す．この構造では下層部が LE のみで形成され，LE 間の配線はその上層部を使用して実現される．したがってアイランドスタイルよりも更に 2 次元的な論理密度に優れている．しかし金属配線層の層数が少ないプロセスでは LE を形成する領域の上層に配線を形成する階層を設けることは難しく，その場合はアイランドスタイルを用いられる．またアイランドスタイルの場合では FPGA 用の配置配線ツールを利用して開発を進めることが可能である.

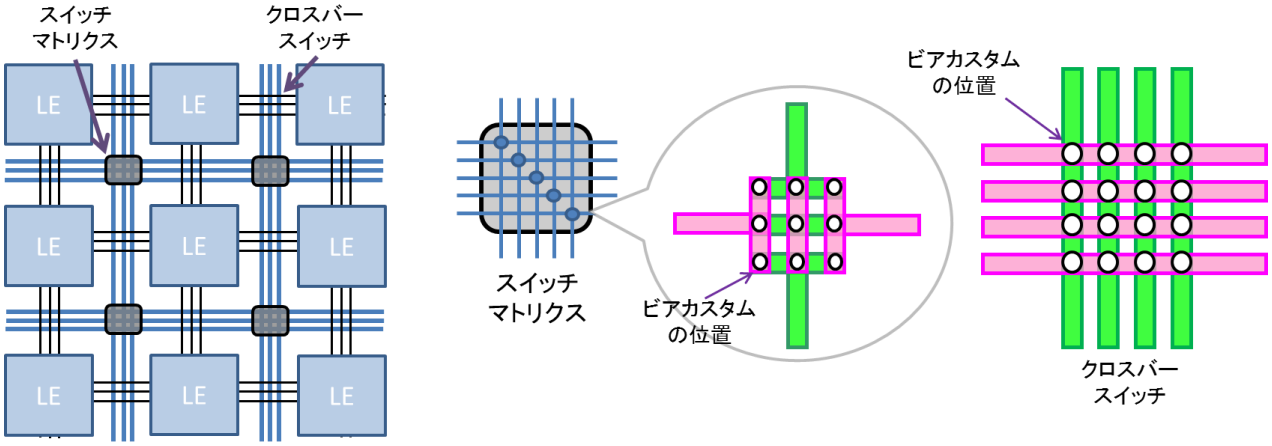


図３．３　VPSA のアイランドスタイル

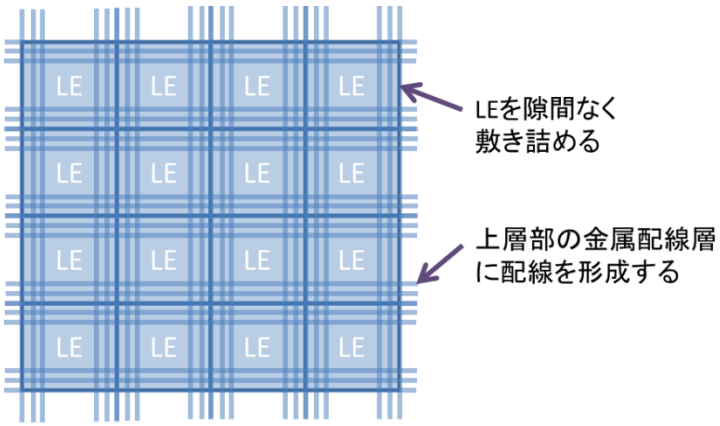


図３．４　タイル状配置構造と上層配線

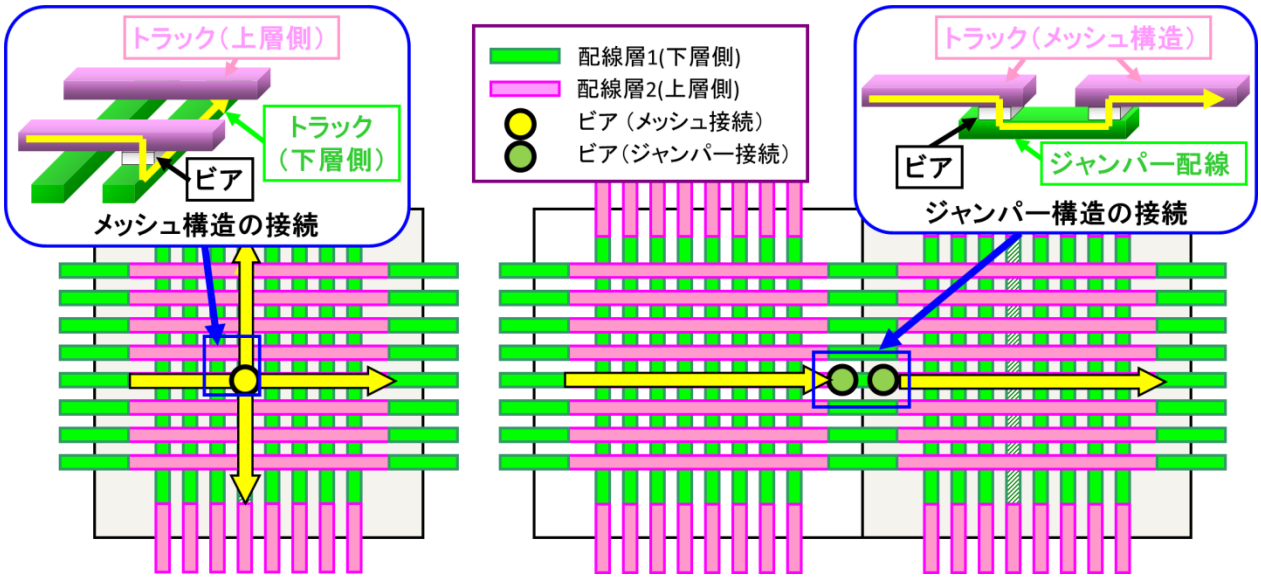
アイランドスタイルは金属配線が 3 層以下ならば使用されるが，今回は配線層 5 層プロセスを仮定しているためタイル状配置構造での検討を行っている．

３．２．３　Logic Element 間の配線構造

タイル状配置構造における上層配線の配線アーキテクチャの１つであるメッシュ・ジャンパー配線構造について説明する．図３．５にこの配線構造の概要および接続例を示す．この配線構造はメッシュ配線とジャンパー配線の二つの配線によって形成されている．

メッシュ配線とは図３．５（a）で示すような，２層のメタル配線で作られる配線トラックをメッシュ状に交差させた構造を示している．今回の図では上層の配線トラックの方向が垂直方向，下層の配線トラックの方向が水平方向の例を示している．図はメタル 2 層構造の例を示しているが，3 層目以降も同様に下層と交差する向きに配線トラックを設置することで多層のメッシュ構造を形成する事ができる．メッシュ配線は LE 上部の配線層によって配線トラックを複数個並べる事で構成されている．この配線トラックの長さや本数は LE サイズに依存しており，LE サイズが大きいほど１本あたりの長さと LE 面積あたりの本数が増大する．１つのメッシュ配線はかならず LE 境界で切断され，LE を跨ぐ形式でメッシュ配線が形成される事はない．２層間のビア配線層はカスタムマスク（custom mask）によって定義され，ビアで縦方向と横方向の２つのトラックを接続することで，水平方向に向いていた配線経路を垂直方向に分岐・転換させることができる．

次にジャンパー配線について説明する．ジャンパー配線は図３．５（b）に示すような LE の狭間に位置する小さな配線トラックを示している．ジャンパー配線は図のように異なるメッシュ配線の配線トラックの両端を繋ぐ位置に形成されており，カスタムマスクによってビアを定義する事で，二つの配線トラックを接続する事ができる．このように隣り合う LE 上の配線トラック同士をジャンパー配線とビアで接続していくことで複数の配線トラックを一つの配線に見立てることができる．これを繰り返すことで水平方向または垂直方向に任意の長さを有する配線を形成することができる．



（a）メッシュ配線の構造　　（b）ジャンパー配線の構造

図３．５　メッシュ・ジャンパー配線構造

メッシュ配線による方向転換とジャンパー配線による任意配線長の配線形成を繰り返すことで目的の LE 間を接続する 1 つの配線網を形成する．図３．６に実際にメッシュ・ジャンパー配線構造によって LE 間を接続した例を示す．この例では左下部に位置する LE（XOR）の出力ピンから右上部に位置する LE（AND） の入力ピンへの接続を表している．入出力ピンは下層のトラック上に現れるため，XOR の Y ピンと水平方向のメッシュ配線 1 本をビア A によって接続する．その後配線経路を水平方向に伸ばすため，隣り合う LE の水平方向に向いた配線トラックをジャンパー配線 BC によって接続する．次に垂直方向へ方向転換するために垂直方向の配線トラックとビア D でメッシュ接続する．これを繰り返すことで，AND の A ピンまで配線経路が形成され，XOR と AND の接続を実現している．

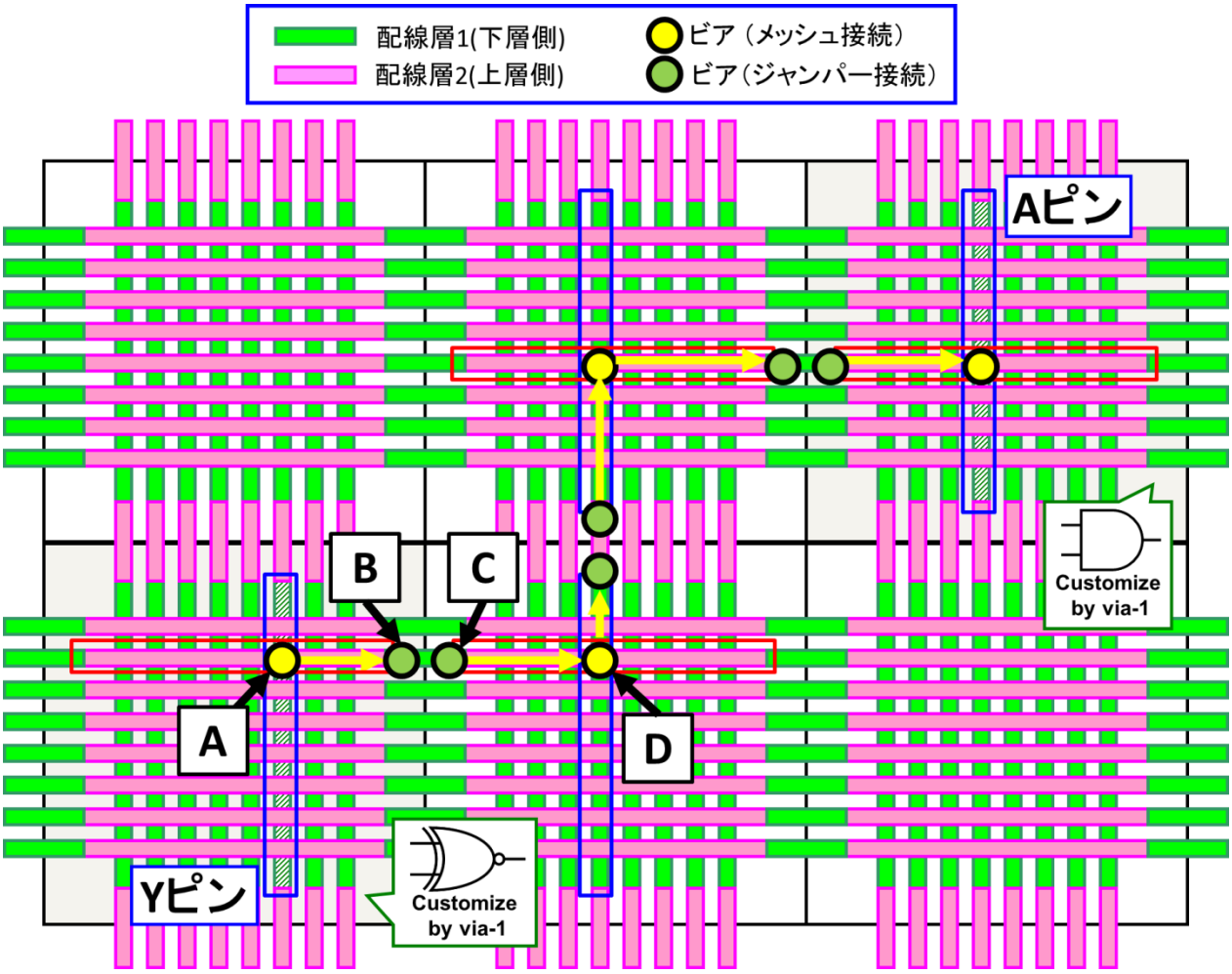


図３．６ メッシュ・ジャンパー配線構造での LE 間接続の例

３．２．４　LE Array Block の分割構造

VPSA のマスター層（master layer）では，LSI のコア領域に LE がタイル状に敷き詰められる．このとき図３．７（a）のようにコア領域に隙間なく LE を敷き詰める手法が最も面積効率に優れる．一方でこの巨大な LE タイルの中央部は，IO 近辺に構築される電源ネットワークやクロックネットワークとの距離が離れすぎており，IR ドロップやクロックのスキューが非常に大きくなることが予測できる．これは回路の性能を低下させるだけでなく，実装回路によっては動作速度低下や意図しない回路動作を引き起こす恐れも懸念される．したがって，回路動作の安定性を確保する上で全面タイル状配置構造は望ましくないといえる．

そこでタイル状配置構造を数個に分割してブロック化した LE Array Block（LAB）と呼ばれる数千～数万個の LE のまとまりを一つの単位として配置し，LAB 間に電源ネットワークやクロックネットワークを形成する構造を検討している．図３．７（b），（c）に構造例を示す．図では LAB を 4 分割した例と 16 分割した例を示している．回路中央に太い電源配線を配置することが可能になるため，IR ドロップの低減が期待できる．また LAB にはさらにクロックツリーが形成されており，それぞれの LAB のクロックツリーへはクロックソースから同一の配線長経路を経由して配線されているため，スキューを小さくすることも期待できる．

LAB 同士の配線は LE 間配線よりも多くの配線抵抗・寄生容量が付くため，論理回路は 1 つの LAB 内で完成させられることが望ましい．それが不可能な場合でも LAB 間を経由する配線をなるべく少なくするなどの工夫が必要である．したがって LAB サイズは細かく分割しすぎないサイズが望ましい．

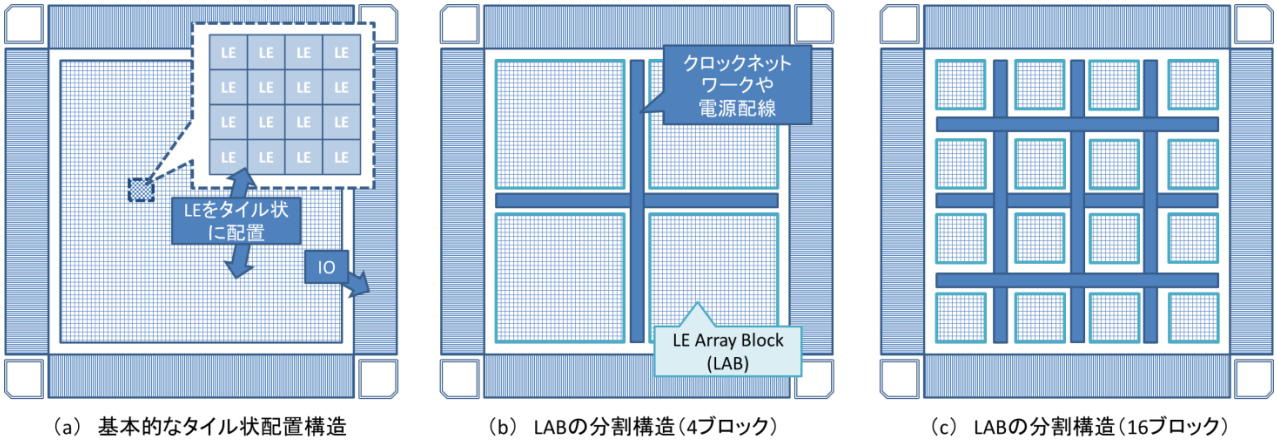


図３．７　LE Array Block 構造と分割例

我々は大規模な暗号回路を 1 個の LAB に構成できるサイズを想定し，横 100 個×縦 100 の合計 1 万 LE で構成された LAB を 1 ブロックとし，4 ブロック構造の LAB 分割構造を仮定してアーキテクチャの評価や最適化を行っている．VPSA におけるコア領域の LAB 分割構造の例として，4 ブロック時のレイアウトと LAB の内部構造を図３．８に示す．この例では格子状に電源ネットワークを構成し，クロックネットワークは右上部から右側面を経由し，中央に向かって各 LAB のクロックポートに接続される．LAB 内部は上部にクロックポートがあり，左右に配線が分かれ，それぞれの側部に形成されているクロックバッファアレイに接続される．クロックバッファアレイは受け取ったクロック信号を整形するバッ

ファセルが敷き詰められた領域で，各バッファの出力ポートから LE 配置領域上に構成された DFF のクロック入力にクロック信号が伝達される．

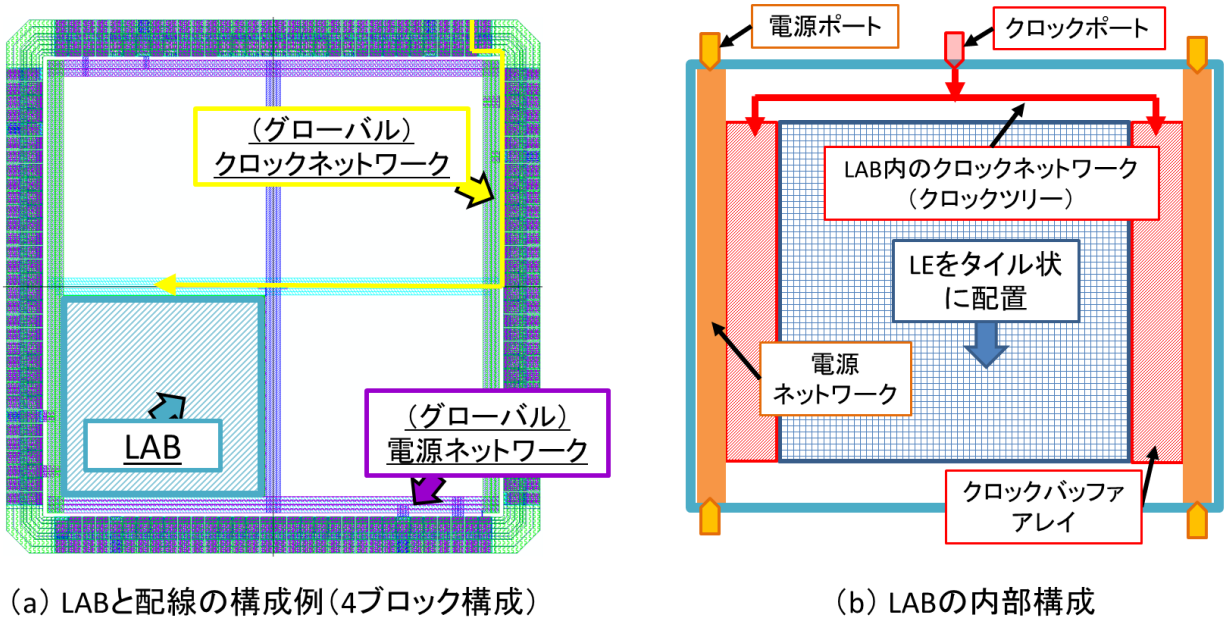


図３．８　LAB４分割構造と LAB 内部の構成例

３．３　Look-Up Table を用いた VPSA アーキテクチャ

本節では VPSA の LE アーキテクチャの例として，ルックアップテーブル（LUT : Look-Up Table）をベースとした LE について説明していく．はじめに LUT の基本的な仕組みを解説し，実際に 180nm プロセスルールで設計を行った 3 種類の LUT 型 LE について順次紹介していく

３．３．１　Look-Up Table について

デジタル回路における LUT とは，計算した値を ROM や RAM などのメモリセルにあらかじめ書き込んでおき，該当する入力パターンに応じて記憶しておいた値を出力する論理回路である．図３．９のようにマルチプレクサ（MUX : Multiplexer）MUX の入力信号側に RAM などの記憶素子を接続することで，セレクタ信号側（A,B,C 端子）の値に対応した RAM に格納された値を出力する．したがって，このとき入力に対応した任意の真理値表を RAM に記憶する事で，その真理値表のように振舞う論理回路を実現することができる．k 入力の LUT 回路を MUX を用いて表現したい場合，2^k から 1 信号選択する MUX と 2^k ビットの RAM を組み合わせることで実現できる．図３．９は「2^3 : 1 の MUX」と 2^3 個の RAM を用いて構成した 3 入力 LUT によって，3 入力 NAND 論理を再現した例を示している．入力信号（A，B，C）が（１，１，１）のときの出力信号を０，それ以外の入力信号パターンのときの出力信号を１とすることで 3 入力の NAND を実現している．

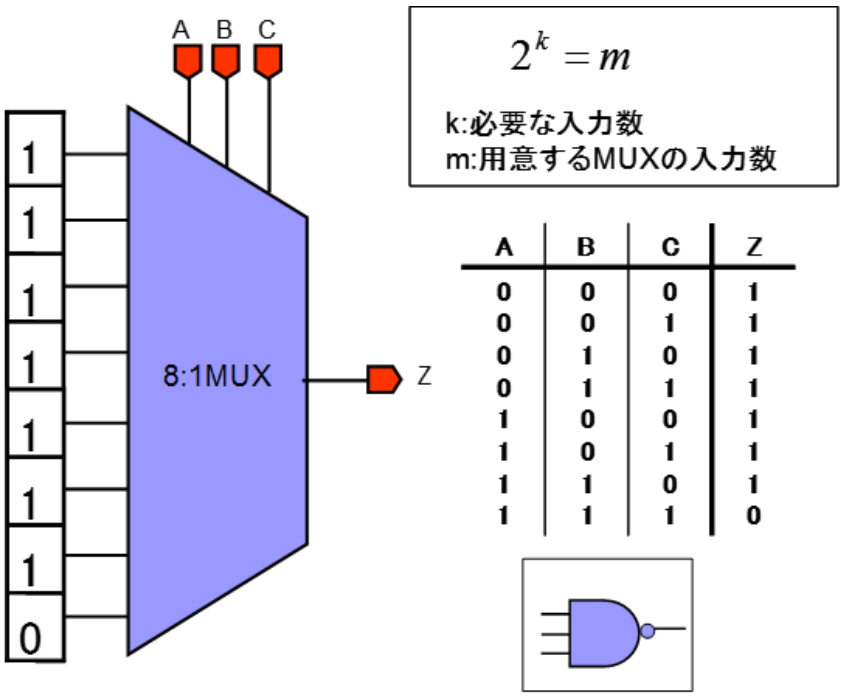


図３．９　3 入力 LUT の構造

３．３．２　Look-Up Table を用いた Logic Element

LUT を用いた LE について説明する. LUT 構造をベースとした VPSA の LE はメモリを利用する手法とビアマスクを利用する手法の 2 種類の実現方法が存在する.

（1）SRAM プログラム方式

LUT の構成に SRAM を利用した LE を図３．１０に示す．この構造では論理を決定する際にカスタムマスクを使用しない．したがって論理実装のためのマスクコストが発生しない LE の実現方法である．LE は LUT の他に D フリップフロップ（DFF : D Flip Flop）を内蔵している．通常の論理回路ではクロック同期回路を実現するために，組み合わせ回路の結果を記憶する DFF が多用される．LE 内に DFF を含めておく事で，任意の論理出力をそのまま出力するか，あるいは DFF に一旦格納し，次のクロックで出力するかを選択することが可能になる．この出力タイプの選択も MUX と SRAM によって実現される．これと同構成のものが実際に FPGA の LE としても用いられている．

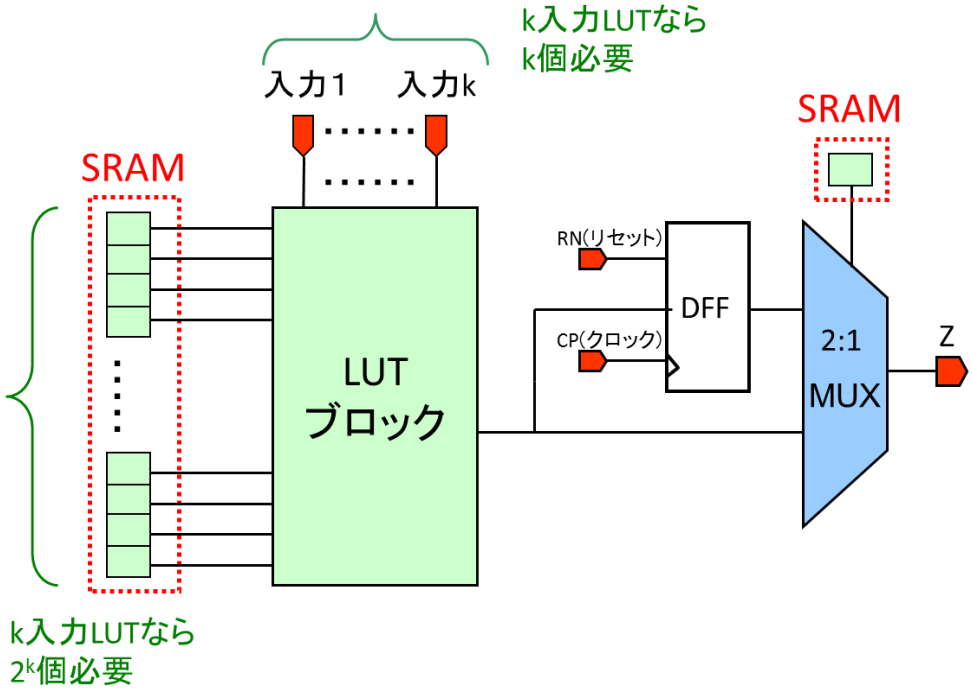


図３．１０　SRAM プログラム方式の構造

（2）ビアプログラム方式

SRAM を利用しない方式ではカスタムマスクを用いることで製造時に論理を定義する．SRAM プログラム方式ではメモリに論理 1，論理 0 を格納し，参照することで LUT 回路に論理関数を定義していた．このビアプログラム方式では電源配線と GND 配線のいずれかを MUX の入力端子に接続することで論理関数を定義する．この方法で LUT を形成する場合，内部に SRAM を利用しないため LE の面積が小さくなり，論理回路の面積をより小さくすることが可能になる．一方でカスタムマスクが必須であるため，マスクコストは前述の方式よりも増大する．図３．１１に構成例を示す．SRAM プログラム方式同様，同期回路を実現するための DFF を内蔵し，有無を切り替えられるようにした構造を有している．またこ

ちらの方式では MUX ではなくビアによって配線経路を変更することで DFF の有無を切り替える.

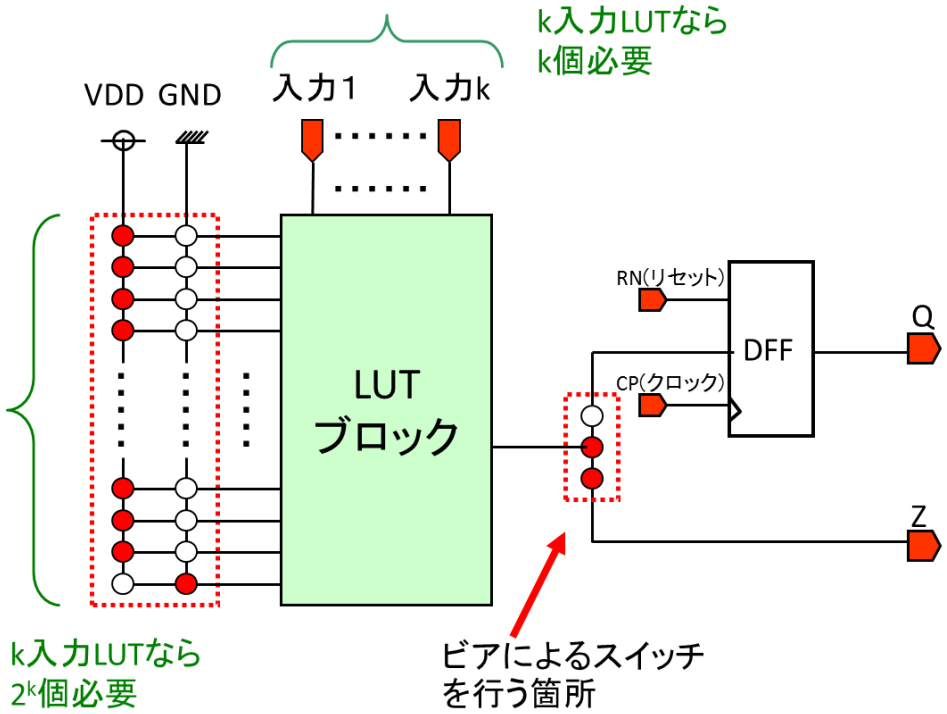


図３．１１　LE の各プログラマブル方式の例（LUT 型）

VPSA による設計・製造のソリューション事業を提供している eASIC Corporation の Nextreme[3]では，マスクコストをより低く抑えるために前者の SRAM プログラム方式を採用している．また元智大学の研究室ではビアプログラム方式で論理実装を行う LE[4]を開発し研究・評価を行っている.

３．３．３　Look-up Table 型 LE アーキテクチャの試作

東京大学 VDEC[6]より提供されているローム 180nm プロセスルールを用いて設計した 3 種類のビアプログラム方式の LUT 型 LE を紹介していく.

（１）　3 入力 LUT 型の LE（標準型）

図３．１２に 3 入力 LUT 型の LE の回路図を示す．3 入力の LUT は 8:1MUX から構成されており，セレクタ信号入力端子 S0，S1，S2 の 3 信号に与える論理値の組み合わせによって MUX の 8 つの入力端子に接続された論理値の内の 1 つが出力として選択される. この時の入力端子は電源配線 VDD または GND 配線のいずれか一方に接続されており，VDD が論理 1，GND が論理 0 を表している.

表３．１に 3 入力 LUT 型 LE の基本性能，図３．９に実際に設計した LE の回路図とレイアウト図を示す．図３．１３中のアルファベットの A~E は回路図（a）中のブロックとレイアウト（b）の対応個所を表したものである.

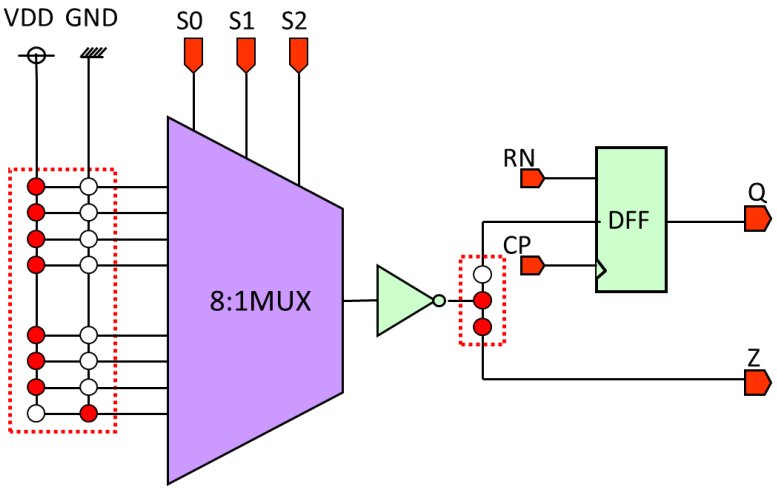
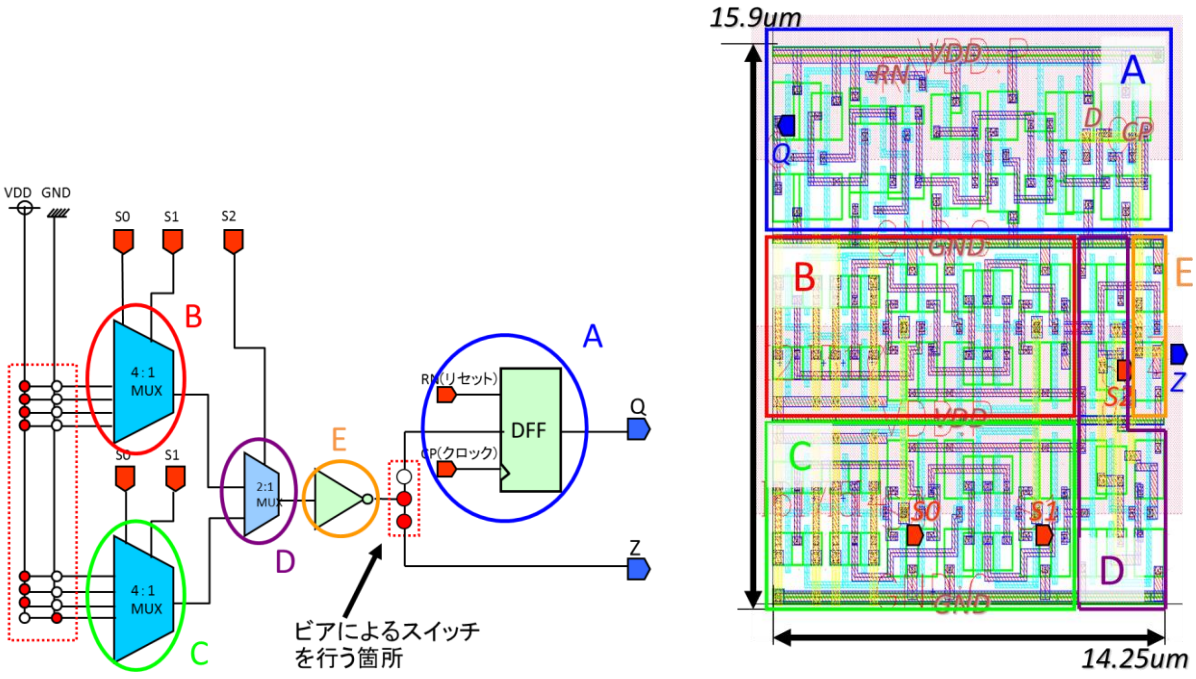


図３．１２　ビアプログラム方式３入力 LUT 型 LE

表３．１　３入力 LUT の概要

面積	226.6μm^2
縦長／横長	15.9μm／14.25μm
再現論理幅	2^8　論理＋DFF （全 3,2,1 入力論理）



（a）回路図　　（b）レイアウト図

図３．１３　３入力 LUT 型 LE の回路図

（２）　４入力 LUT 型の LE（マルチグレイン型）

４入力 LUT 型の LE について説明する．通常の４入力 LUT 型の LE は図３．１４のように１６：１ MUX によって構成される．セレクタ信号端子 S0，S1，S2，S3 に与えられた４つ入力論理の組み合わせによって MUX の 16 入力端子の内の１つのパスが選択される．これによって４入力１出力の任意の真理値表を表現する．

多入力 LUT を利用した LE の持つ長所として，LE 内部で規模の大きい論理ゲートを再現できることがあげられる．そのため少ない LE の組み合わせで所望の論理回路を形成することができ，LE 間を接続するための配線総数を少なくすることができる．そのため配線混雑度や動作速度性能が良くなるという利点をもつ．配線コストの高い FPGA では５～６入力 LUT などを用いた大きな LE が利用されている．

その一方で，２入力，３入力論理素子を多用する論理回路では，４入力 LUT で３入力論理や２入力論理を再現しなければならず, 小規模な LE を利用したときよりも回路面積の増大を招いてしまうことある．これは多入力 LUT の欠点としてしばしば挙げられる．この問題に対応するため，４入力 LUT を２つの３入力 LUT に分割することができる「マルチグレイン LUT 構造」を適用した．「マルチグレイン構造」は FPGA の LE でも用いられている構造であり，１つの LE で２つの小規模論理を再現することが可能なため，小規模論理が大部分を占める論理回路であっても面積効率を損なわないという利点を備えている．

表３．２に今回設計した４入力 LUT 型マルチグレイン LE の基本性能，図３．１５に回路図およびレイアウト図を示す．LUT 構造の切り替えは図３．１６のように，ビアの変更によって実現する．４入力 LUT モードのときは out1 が出力端子となり，３入力 LUT×２モードの時は out1，out2 の両端子が出力端子となる．また後段に DFF を接続することが可能なのは out1 端子側の LUT のみとなる．

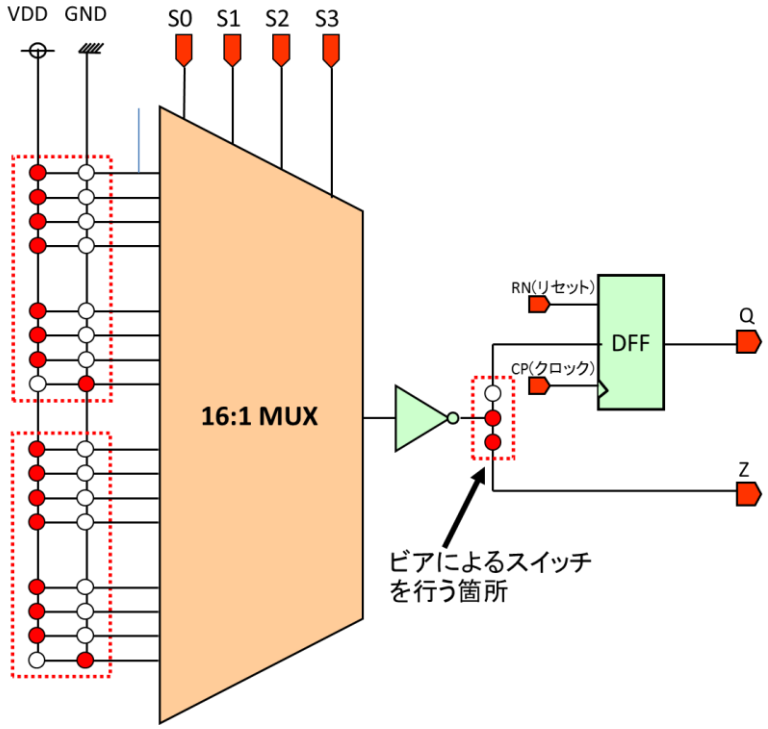
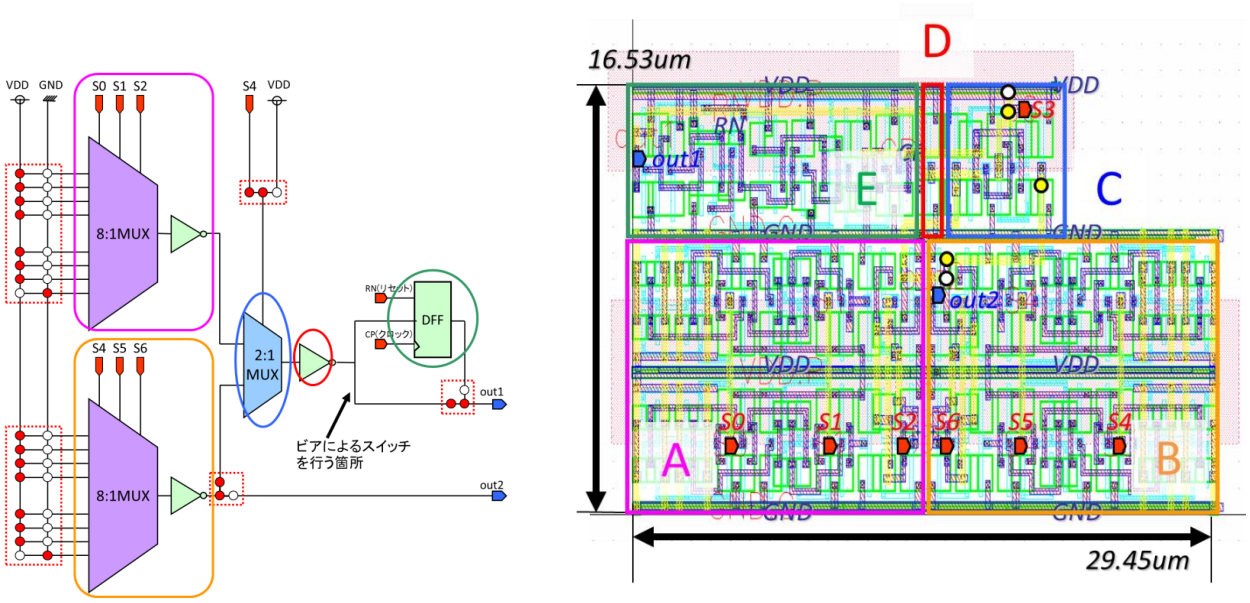


図３．１４　４入力 LUT 型 LE の回路図（通常版）

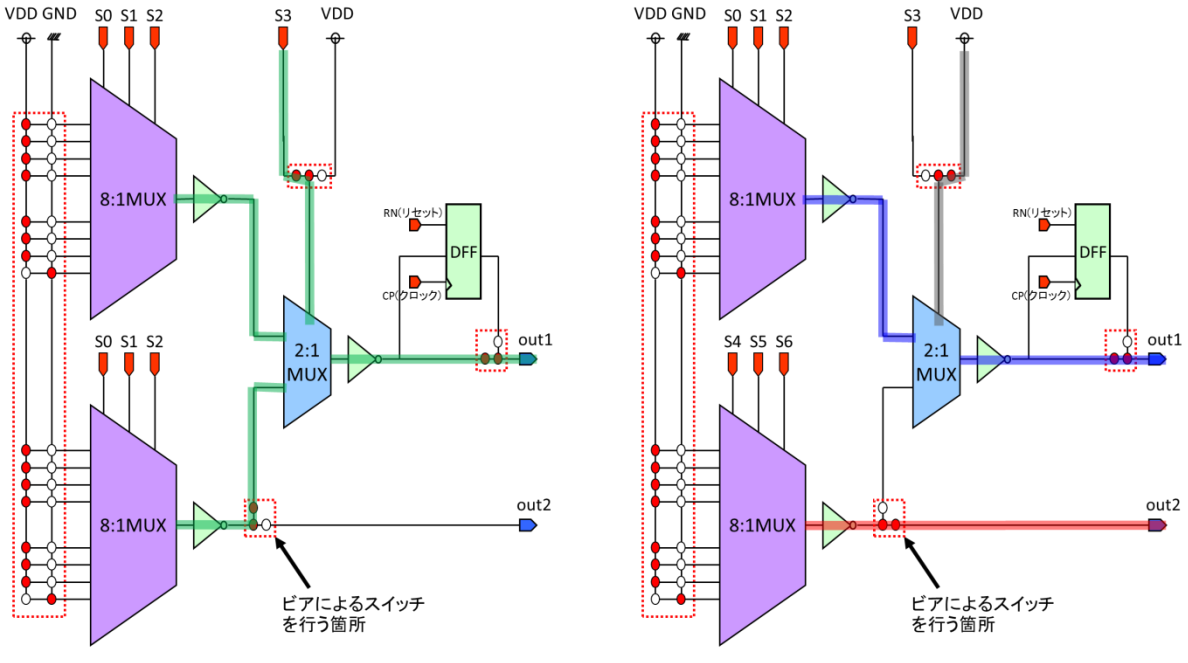
表３．２　４入力 LUT 型のマルチグレイン LE の基本性能

面積	226.6μm^2
縦長／横長	16.53μm／29.45μm
再現論理幅	2^{16} 論理＋DFF（全 4,3,2,1 入力論理） または 2^8 論理+2^8 論理＋DFF



（a）回路図　　（b）レイアウト図

図３．１５　４入力マルチグレイン LUT 型 LE の回路図



（a） 4入力LUTモード　　（b） 3入力LUT×2モード

図３．１６　入力数の切り替え

（３）2 入力 LUT 型の LE（DFF 可変型）

2 入力 LUT 型 LE を図３．１７に示す．この LE は 4 入力 1 出力 MUX と DFF によって構成することができる．しかし 2 入力 LUT のような小規模な LUT と DFF を組み合わせた場合，LE の大部分を DFF が占めることになる．これにより DFF を多用しない論理回路では回路面積の大部分が利用されない DFF の面積によって占められてしまう問題が存在する．表３．３は 2～4 入力 LUT 型 LE の各面積とその面積中に占められる DFF 面積の割合を示している．3～4 入力 LUT 型の場合では 1 割～3 割程度の領域が DFF によって占められている．その一方で 2 入力 LUT 型 LE においては，LE 面積の約 50%が DFF 面積によって占められている．

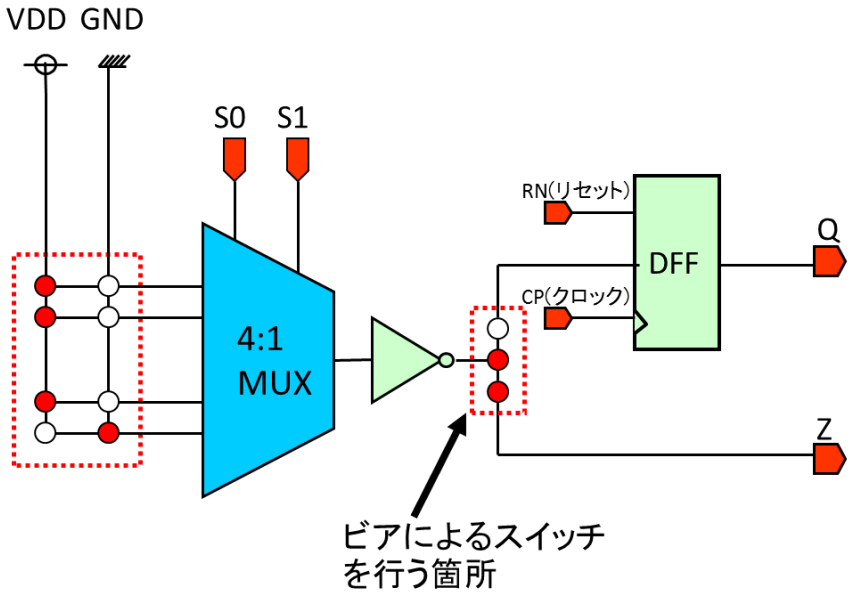


図３．１７　２入力 LUT 型 LE の回路図

表３．３　DFF の割合

	LE 面積	DFF の占める割合
2入力LUT	143.72μm^2	55.6%
3入力LUT	226.64μm^2	32.0%
4入力 LUT	486.81μm^2	16.7%

2 入力 LUT 型 LE における，この面積の課題を解決するために，従来の LUT 型 LE に改良を加えた新しい LE を開発した．これを「DFF 可変型」と呼称する．従来型との違いを図３．１８に示す．従来の LE の構造は LUT と DFF が組み合わさった「DFF 内蔵型」と呼ばれる構造であった．今回実現した DFF 可変型と呼ばれる構造はビアを指定座標に置くことで再現論理素子の一種として DFF を構成することが可能になっている．したがって LE 内部に DFF の領域が存在せず，そのため DFF 内蔵型よりも LE サイズを小さくすることが可能である．

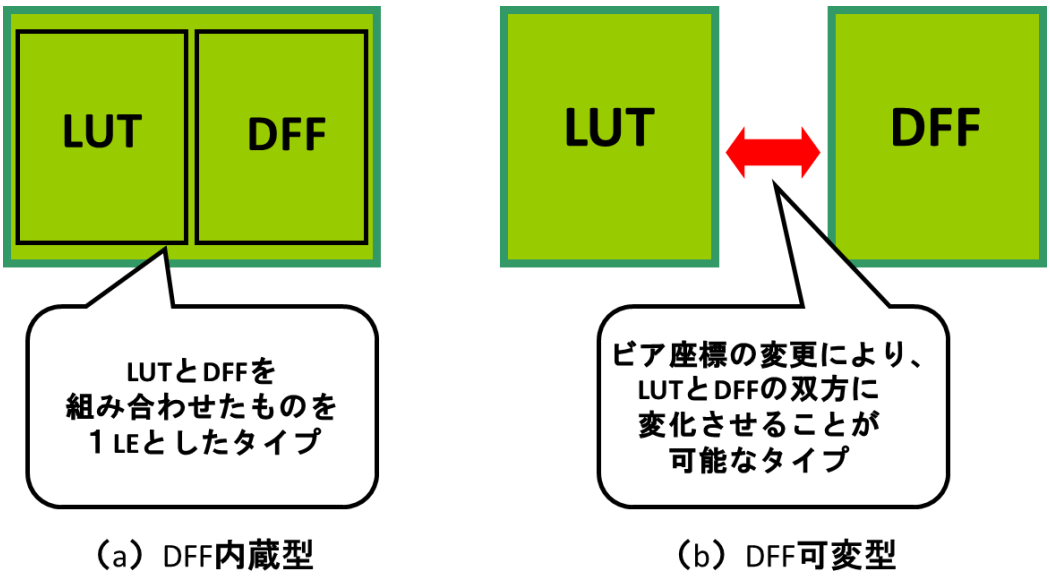


図３．１８　DFF のタイプに関して

通常，リセット付の DFF を構成するためには NAND 回路が２つ必要となる．しかし 2 入力 LUT を構成する４：１MUX はトランスミッションゲート（Transmission-Gate：TG）とインバータ（Inverter：INV）によって構成されるため，NAND 回路が存在せず，ビア座標の変更による配線切り替えだけでは LUT を DFF に組み替えることはできない．そこで図３．１９に示すような，NAND 回路に切り替えることが可能な INV と TG を導入した．

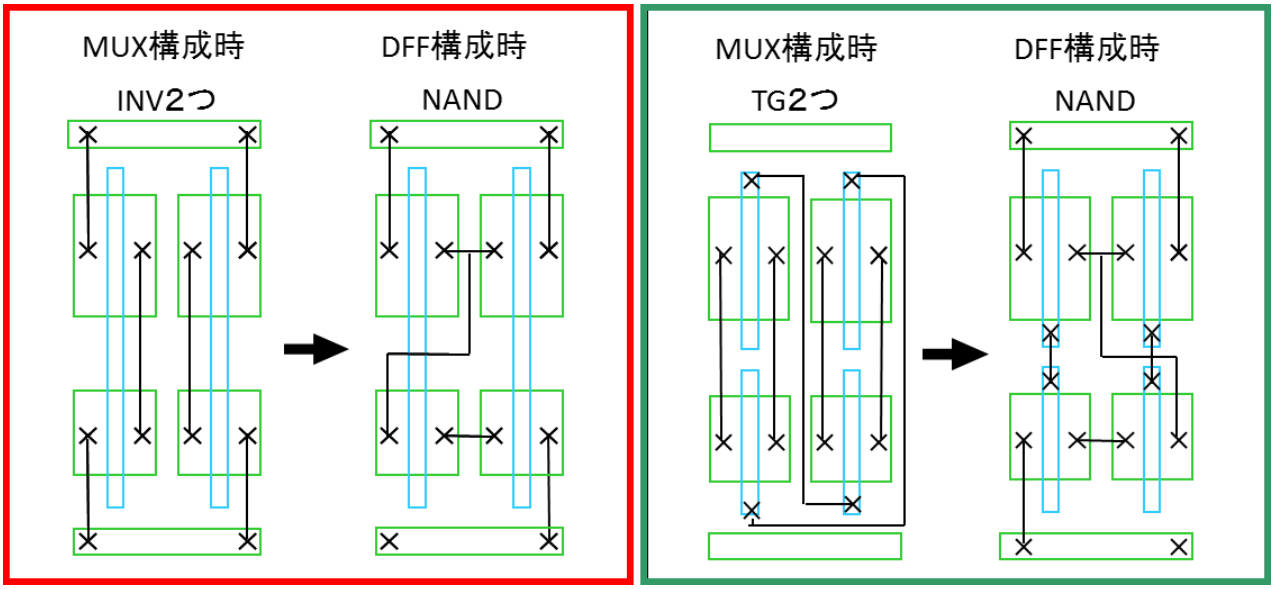


図３．１９　INV，TG を用いた NAND の構成

図３．２０に 2 入力 LUT 型 LE の LUT モードと DFF モードの回路図を示す．図３．２０（a）中の

線で囲まれた TG と INV は DFF の構成時に図３．２０（b）中の線で囲まれた NAND へと組み変わる．これによって MUX を構成する論理素子を用いて DFF を構成することが可能になる．

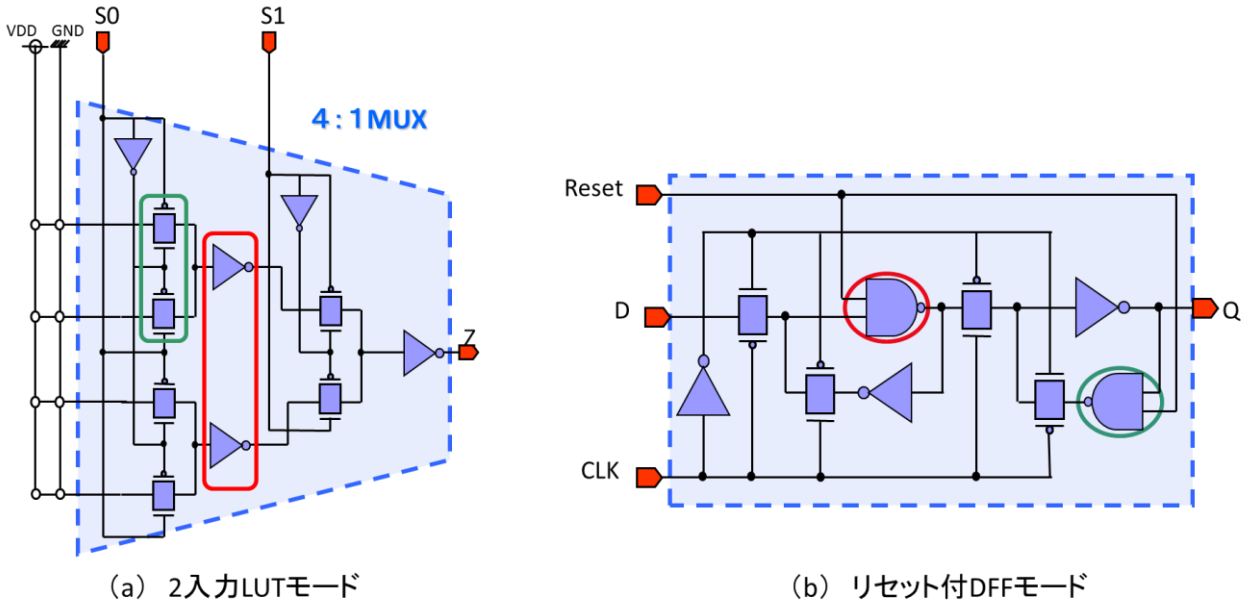


図３．２０　２入力 LUT と DFF の回路構成と共通項

この DFF 変形可能な 2 入力 LUT 型の LE のレイアウトを図３．２１に示す．トランジスタやメタル配線を形成するマスター層は構造が同一のものとなり，カスタムマスクを変更するだけで 2 入力 LUT と DFF の両方を再現できる．これにより必要に応じて順序回路に対応するときのみ DFF を再現することが可能となる．また必要に応じて LUT を DFF に変形するので，組み合わせ回路を実装した際に無駄な DFF 領域が一切存在しなくなる．

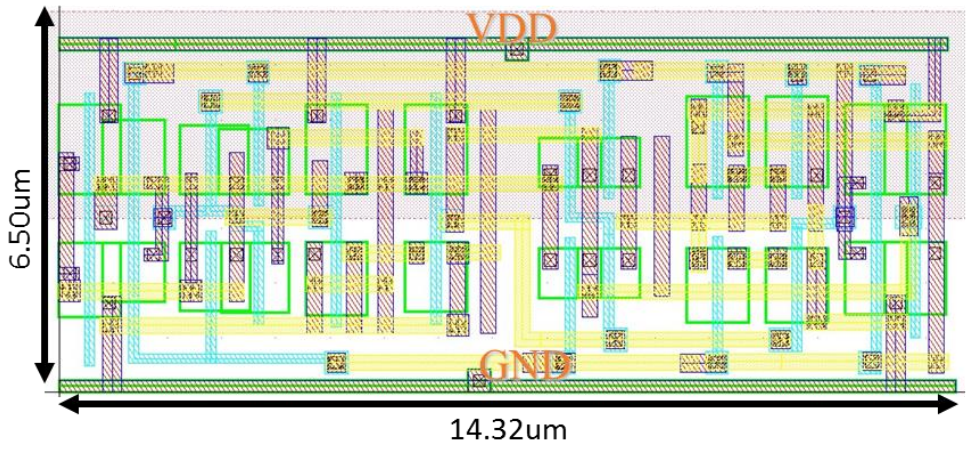


図３．２１　レイアウト図

３．４　VPEX2 アーキテクチャ

前章までは LUT を利用した LE を紹介してきた．これらの LUT ベースの LE はそれぞれ幅広い論理素子を再現することが可能であり，論理回路を形成する上で機能的な問題点はない．しかし消費電力や動作速度に問題点が存在する．

３．４．１　LUT ベース型 LE とスタンダードセル型 LE

（１）LE の入力負荷容量

LUT の入力端子は MUX のセレクタ信号端子である．このセレクタ入力端子は MUX 内部では TG と INV に接続されており，したがってこの入力端子からこれらのゲートをドライブする必要がある．3 入力 LUT の場合，図３．で示すように S0 端子が最も多くのトランジスタに接続されており，この端子が遷移すると，合計 18 個の MOS トランジスタのゲート容量に対して充放電を行うことになる．したがって，この端子の遷移頻度によっては，これが大きな動的消費電力となることが懸念される．

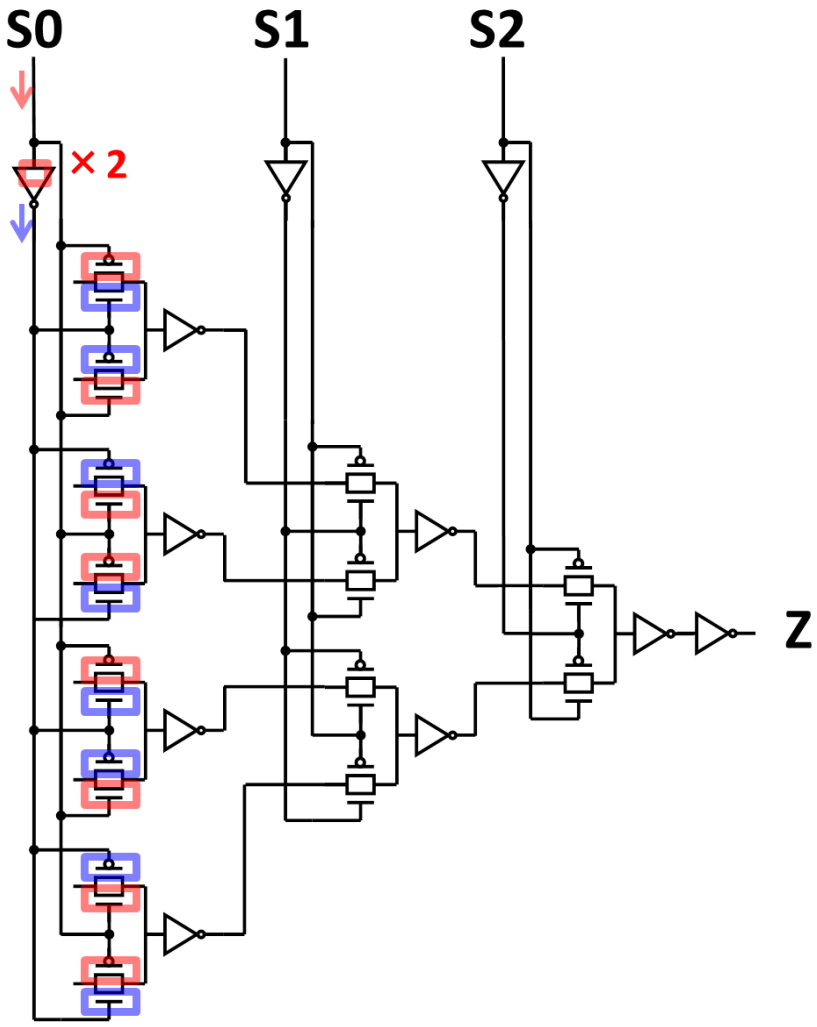


図３．２２　LUT の入力負荷容量

（２）LUT の動作速度

LUT で構成した論理回路はスタンダードセルよりも経由する論理ゲート数が多くなる．例えば 3 入力 NAND 回路を例に考える．図３．２３は 3 入力 NAND 論理ゲート素子をスタンダードセルと LUT の 2 通りで再現したとき，出力が論理 1 から論理 0 に遷移するときの信号伝搬のクリティカルパスを示したものである，スタンダードセルの場合では NAND ゲート素子内部 NMOS トランジスタを 3 つ経由して出力がドライブされる．したがって遅延は最悪でも 3 ゲート分ということになる．一方 LUT の場合では 4 個の INV 回路と 3 個の TG を経由する必要がある．加えて，S1 の入力端子側にはさらに INV をドライブして MOS を制御しており，多くのゲートを経由して出力信号の遷移が行われる．このため LUT で小規模な論理回路を形成するとスタンダードセルの同等論理ゲートと比較して遅延が大きくなってしまう問題がある．

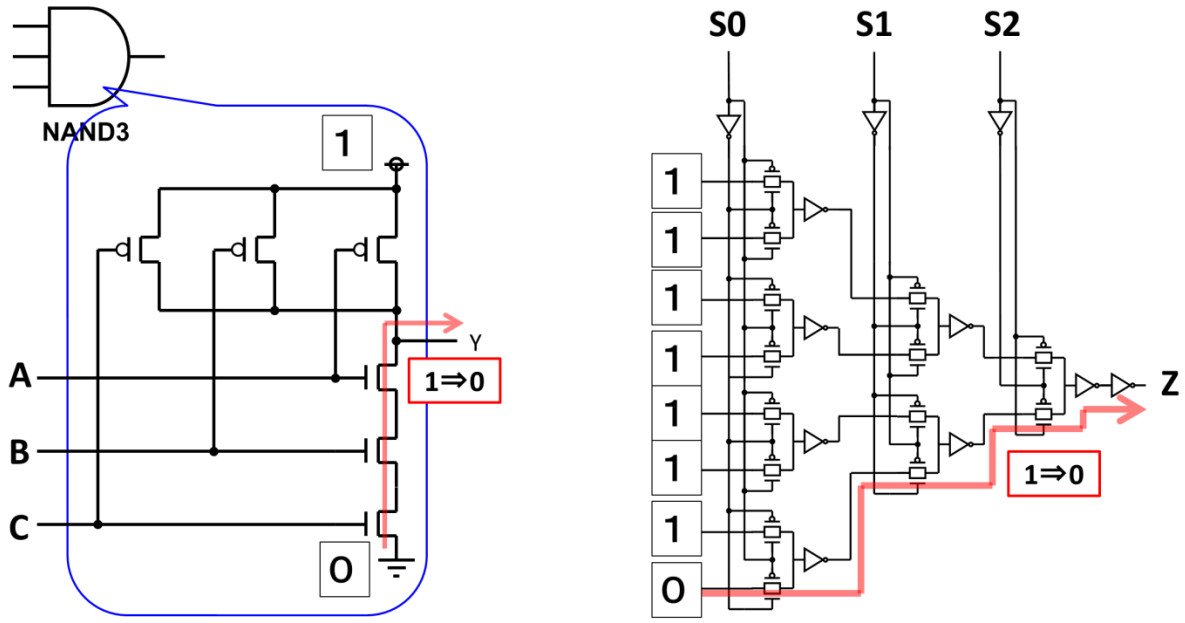


図３．２３　3 入力 AND 回路の再現

これら（1）（2）の問題より，動作速度および消費電力における性能面では LUT を利用するよりも，スタンダードセルやそれらの組み合わせが有効であることが分かる．したがって，高性能な VPSA を実現する手法の一つとして，LUT ではなくスタンダードセルの組み合わせから LE を構成し，数種類の論理ゲート素子の再現を検討する事が考えられる．

そこで 2008 年に中村らによって XOR 論理ゲートと INV 論理ゲートをベースとして，他の十数種類の論理ゲートを再現することが可能な VPEX アーキテクチャが[1]検討された．さらに 2010 年には西本らによって順序回路の実現に最適化するために LE に改良が施され，「VPEX2 アーキテクチャ」[6-7]となった．本節ではこの VPEX2 アーキテクチャの LE について説明する．

３．４．２　LE アーキテクチャ

ここでは VPEX2 の LE について説明する．VPEX2 の LE は複合型 Exclusive-OR（XOR）ゲートと Inverter（INV）ゲートを組み合わせた構造になっている．表３．４に LE の基本性能としてサイズや再現可能な基本論理の数を示す．また図 ３．２４に LE のレイアウト図ならびに論理回路図を示す．

表３．４　VPEX2 アーキテクチャ LE の基本性能

面積	88μm²
縦長／横長	8.8μm／10μm
再現論理幅	13 論理

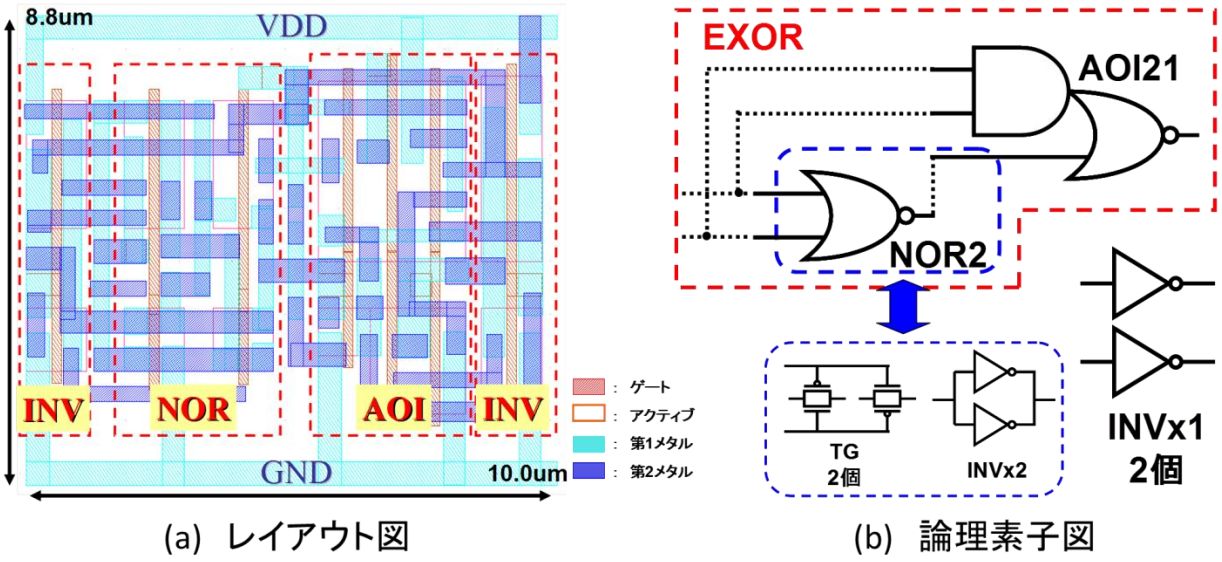


図３．２４　LE の構造

LE で採用した複合ゲート型 XOR ゲートは, AOI ゲートと NOR ゲートから構成されている. また, NOR ゲートは拡散領域を共用しない「セパレート構造」になっており，図３．２４（b）に示すように 2 倍サイズの INV ゲートあるいは 2 個分のトランスミッションゲート（TG）として利用することが可能である．XOR ゲート以外の論理を演算するためには，AOI ゲート，NOR ゲートおよび INV ゲート間の接続を，第 1 ビア層を用いて変更する．これによって計 13 種類の論理が実現可能となる．VPEX2 アーキテクチャは 88μm² の領域内ですべて 2 の入力 1 出力論理に加え，3 種類の 3 入力論理を再現できることが特徴である．

実際に論理を構成した場合の LE のレイアウト図・回路図を図３．２５に示す．今回は例として，AND 機能を再現する．図（a）中の丸枠の内，内部が塗りつぶされている位置にビア 1 を配置することで INV や AOI のセルを接続し，AND 論理を形成している．また図（b）の INV や OR セルのように論理の再現に使用しないゲート素子の入力端子はビアで GND に配線することで無効化させる．

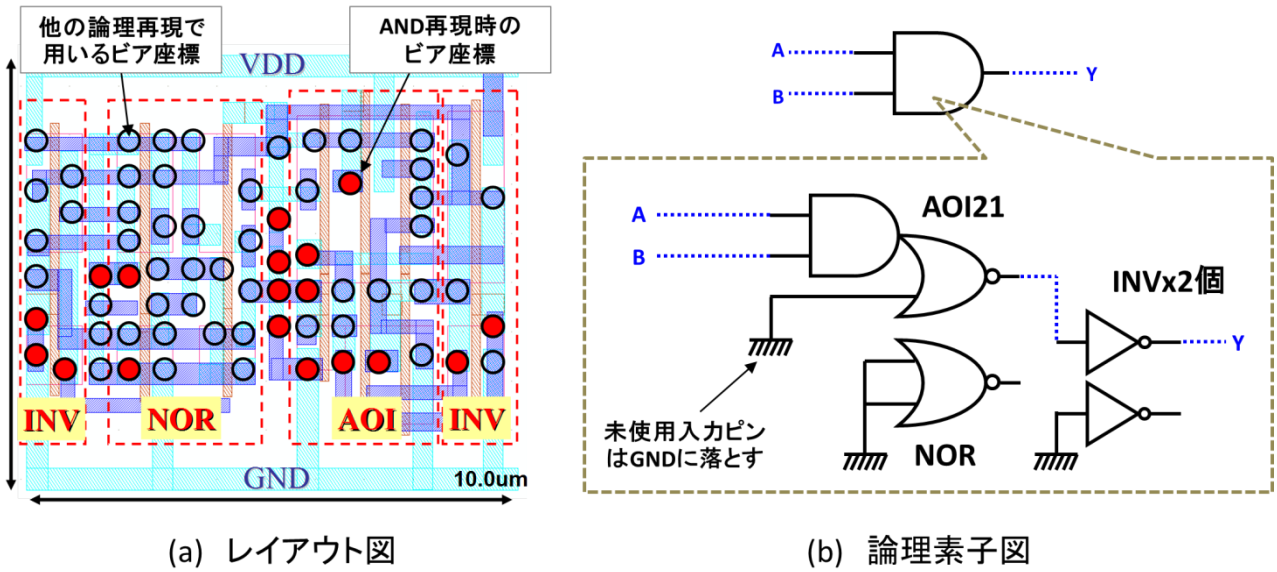


図３．２５　カスタムレイヤ（ビア）による AND 論理ゲート素子の再現

同様にして，特定の位置のビアを打つことにより，13 種類の論理をそれぞれ実現することができる．VPEX の LE を用いた 13 論理の回路図を図 ３．２６に示す．図に示すように，１入力１出力論理の INV, BUF, ２入力１出力論理のすべての論理（NAND, NOR, AND, OR, bubble AND, bubble OR, EXOR, EXNOR），３入力１出力論理の AOI ゲート，および 2 入力マルチプレクサ MUX, MUXI の合計 13 種類の論理回路を形成することができる．

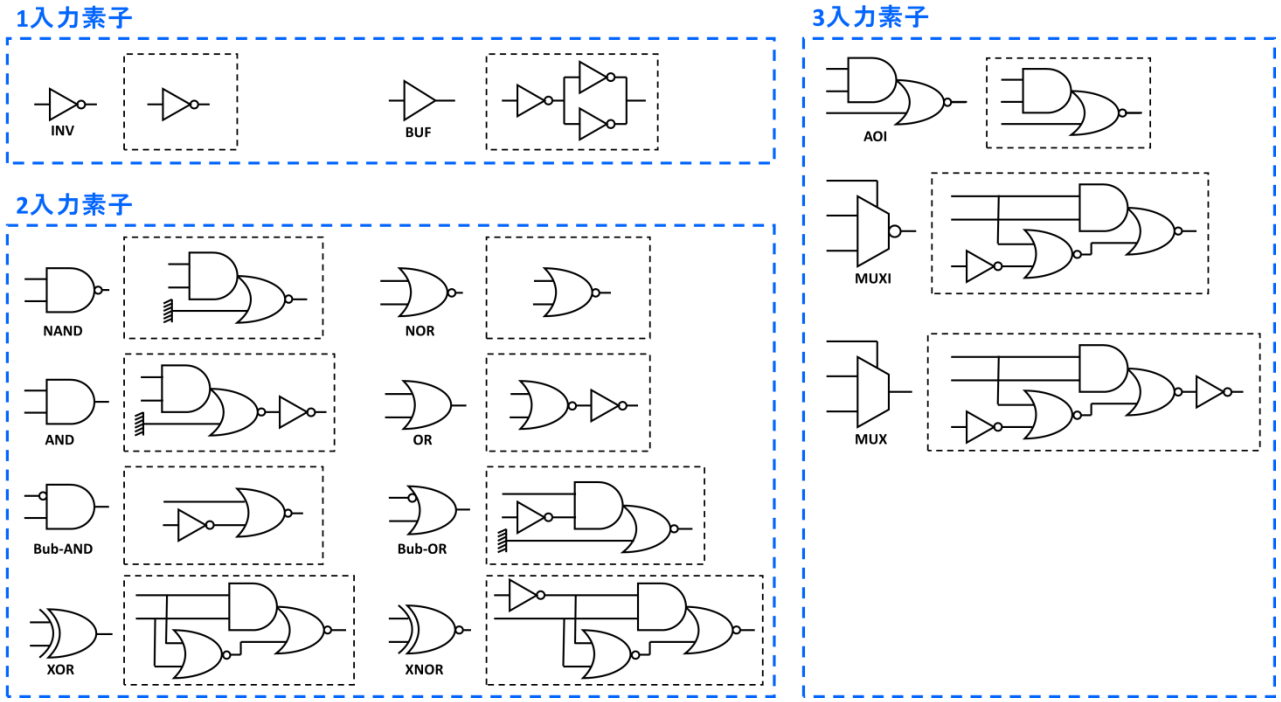


図３．２６　VPEX2 で構成可能な論理素子

また VPEX は NOR ゲートの拡散領域を切ることで作成可能な２つの TG を利用することによって，2 個の LE を組み合わせて DFF を構成することができる．図３．２７に DFF を再現した際のそれぞれの LE の回路図を示す. また実際に構成した場合のレイアウト図とビア座標および使用した配線リソースを図３．２８に示す．前節で紹介した DFF 可変 2LUT 型 LE と同様に，必要な DFF だけを構成できるので，無駄な DFF が発生しない.

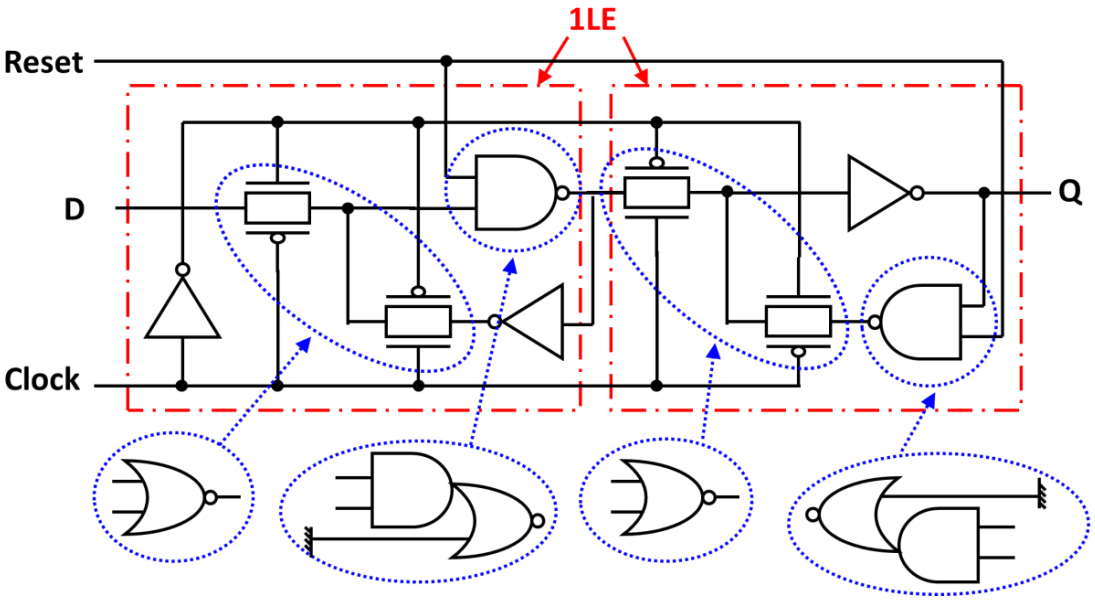


図３．２７　VPEX2 における DFF 構成時の回路図

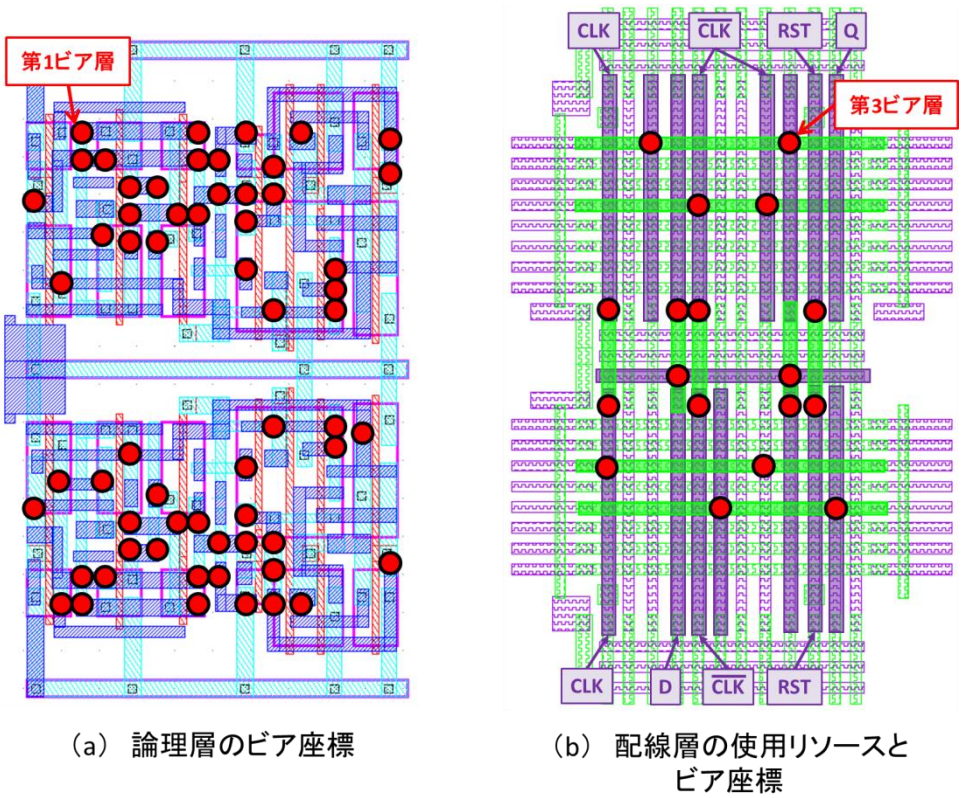


図３．２８　VPEX2 における DFF 構成時のビア・リソース詳細

３．５　各 LE のまとめ

最後に本章で紹介した LE アーキテクチャを表にまとめる．最も面積の大きい LE アーキテクチャは 4 入力 LUT であり，VPEX2 が最も LE の面積が小さい．また 4 入力 LUT は 1 つの LE 内で 2 つの 3 入力論理を再現することが可能で，論理合成後の総 LE 数が非常に少なくなることが期待できる．一方で 2 入力 LUT は再現可能論理数が最も少なく，さらに 1 LE を使用して DFF を構成するため，総 LE は最も多くなると予測できる．これらの詳細な素子数・面積の性能評価および性能比較は 4 章で述べる．

表３．５　各 VPSA の LE アーキテクチャのまとめ

	3 入力 LUT 標準型	**4 入力 LUT マルチグレイン型**	**2 入力 LUT DFF 可変型**	**VPEX2**
面積	226.6μm²	484.6μm²	93.1μm²	88.0μm²
再可能現 論理数	3 入力論理	4 入力論理 or 3 入力論理×2	2 入力論理	2 入力論理 ＋AOI, MUX, MUXI
DFF タイプ	内蔵型	内蔵型	可変 （LE 1 個使用）	可変 （LE2 個使用）
ベースタイプ	LUT	LUT	LUT	スタンダードセル

第 3 章の参考文献

[1] Akihiro Nakamura, Masahide Kawarazaki, Kouta Ishibashi, Masaya Yoshikawa, Takeshi Fujino, “Regular Fabric of Via programmable Logic Using Exclusive-or Array (VPEX) for EB direct Writing”, IEICE Trans. on Electron, Vol.E91-C, No.4, pp.509-516, April 2008.

[2] Chetan Patel, Anthony Cozzie, Herman Schmit, and Larry Pileggi, “An Architecture Exploration of Via Patterned Gate Arrays”, Proceedings of the 2003 international symposium on Physical design (ISPD’03), pp.184-189, April 2003.

[3] eASIC, “eASIC Corporation - Low Cost FPGA & Low Power FPGA & Low NRE ASIC with High Speed Transceivers Solutions - 90nm Nextreme NEW ASICs, 45nm Nextreme-2 NEW ASICs, easicopy ASIC Migration, IP Cores, Low NRE”, http://www.easic.com/

[4] Hui-Hsiang Tung, Yu-Chen Chen, Da-Wei Hsu, Shih-Jung Hsu, Chen Sin-Yu, and Rung-Bin Lin, “Via-configurable logic block architectures for standard cell like structured ASICs”, Proceedings of the 2009 12th International Symposium on Integrated Circuits (ISIC’09), pp.17-20, Dec. 2009.

[5] VDEC, “VLSI Design and Education Center Homepage”, http://www.vdec.u-tokyo.ac.jp/

[6] 西本智弘，川原崎正英，長谷川英司，寺川知宏，藤野毅，“ビアプログラマブルデバイス VPEX のロジックエレメント改良による面積削減と高性能化”，電子情報通信学会，ICD2008-122，pp.101-106，2008 年

[7] T.Fujino, T.Nishimoto, Y.Kokusho, M.Yoshikawa, G.Lemieux, “Via-programmable Logic Array VPEX2 with Configurable DFF using 2 Logic Elements”, The 12th International Symposium on Integrated Circuits (ISIC’09), pp.21-24, (2009)

第４章　新アーキテクチャ・VPEX3 の提案

本章では前章で紹介した VPEX2 をベースに改良を加えた新たな VPSA アーキテクチャ「VPEX3」について述べる．VPEX2 の LE は約 88μm² の面積を有していた．この LE のサイズはスタンダードセルと比較して非常に大きく，そのため VPEX2 を用いて構成された論理回路は ASIC と比べて回路規模が大きくなることが懸念される．この面積の性能差を縮めるために，LE の抜本的な改良について検討を行った．面積効率を向上させるための手法としては LE の構成を見直し再現可能論理数を増加させることや，レイアウトを最適化し，不要な領域を取り除くことで LE 面積を縮小させる手法が考えられる．これらについての考察を述べる．

また本章では従来構造の見直しとして，カスタム層 2 層構造の課題点について考察し，VPSA において面積効率の良い LE を実現する手段としてカスタム層 3 層構造を用いた LE についても検討を行った．

最初に VPEX2 アーキテクチャで採用しているカスタム層 2 層構造についての問題点についてまとめる．次いで VPEX3 に向けて検討していった改良項目について説明し，各問題点を解消する改良案や方針を提示していく．そしてそれらを組み合わせて実現した VPEX3 アーキテクチャの LE や再現可能論理などを説明していく．最後に 3 章で紹介した既存アーキテクチャとの性能比較を示すことで，VPEX3 アーキテクチャの優位性・特徴を明らかにする．

４．１　VPEX2 の構造における問題点

図４．１に VPEX2 アーキテクチャの階層構造を表した断面図を示す．

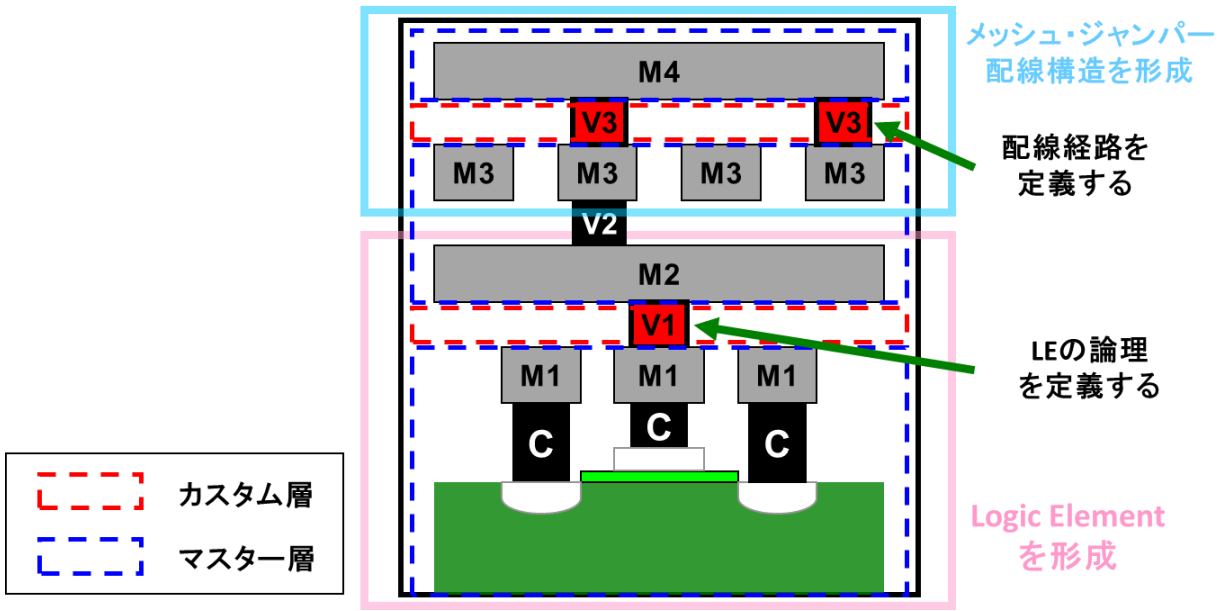


図４．１　VPEX2 の階層構造

VPEX2 アーキテクチャは配線 4 層以上のプロセスでの実装を想定しており，第 1 ビア層および第 3 ビア層をカスタム層とした VPSA アーキテクチャである[1-2]．したがって，第 2 ビア層および第 4 以降のビア層はカスタマイズ不可のマスター層となっている．また VPEX2 アーキテクチャの階層は下層と上層の 2 つの領域に分断する事ができ，第 2 メタル配線層以下の領域では LE を形成し，第 2 ビア配線層以上の階層（図では第 4 メタル層まで）ではメッシュ・ジャンパー配線構造を形成している．したがって LE の論理実装には第 1 ビア層，配線の形成には第 3 ビア層が用いられる構造になっている．

ここで第 2 メタル配線層と第 3 メタル配線層の間にある第 2 ビア配線層がマスター層として固定されているため，LE の領域において，いくつかの第 2 メタル配線は第 2 ビアに接続され，そのままメッシュ配線構造を形成する第 3 メタル層の配線トラックと自動的に接続される構造になっている．この構造は LE の配線効率と LE 面積の両方の面でデメリットを生んでいる．

まず LE の配線効率の問題点について説明する．VPEX2 では垂直方向へ配線経路を伸ばすためには第 3 メタル層のメッシュ配線用トラックと第 4 メタル層のジャンパー配線用トラックが使用される．しかし同時にこの第 3 メタル層のメッシュ配線トラックは LE の入出力ピンとしても使用される．したがって図３．２に示すような配線経路とは無関係な入出力ピンが配線経路上に出現してしまう問題が生じる事がある．

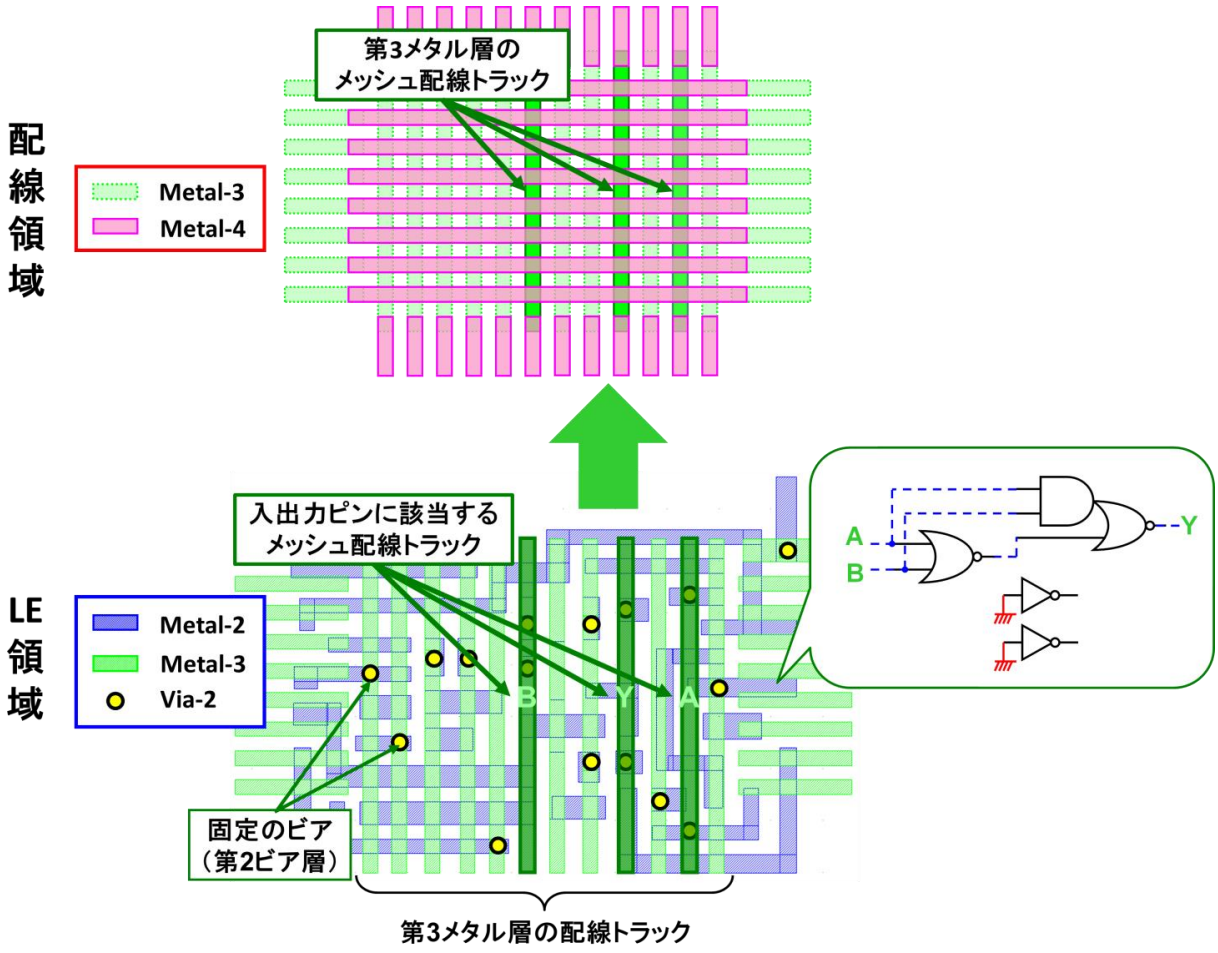


図４．２　VPEX２の LE の入出力ピンの自動割り当て

このように入出力ピンが自動的に割り当てられ，その配線トラックが使用できないことで，理想的な配線経路を形成できない問題が引き起こされる．VPEX2 では配線経路に割り当てる配線トラックと入出力ピンの出現する配線トラックの位置が重なってしまった場合，配線経路の方を変更しなければならない．図 4．3は A トラックから C トラック間を配線する場合において，LE の入出力ピンに割り当てられている B の配線トラックが配線経路の障害となるケースを示している．A の配線トラックから C の配線トラックまでを接続する場合，通常であれば A と C の間になる B の配線トラックを利用することが最も配線効率のよい配線経路となる．しかし今回のケースでは B の配線トラックが入出力ピンに割り当てられるため．最適な配線経路をとることが出来ない．そのため，図のように迂回経路を通って接続しなければならない．

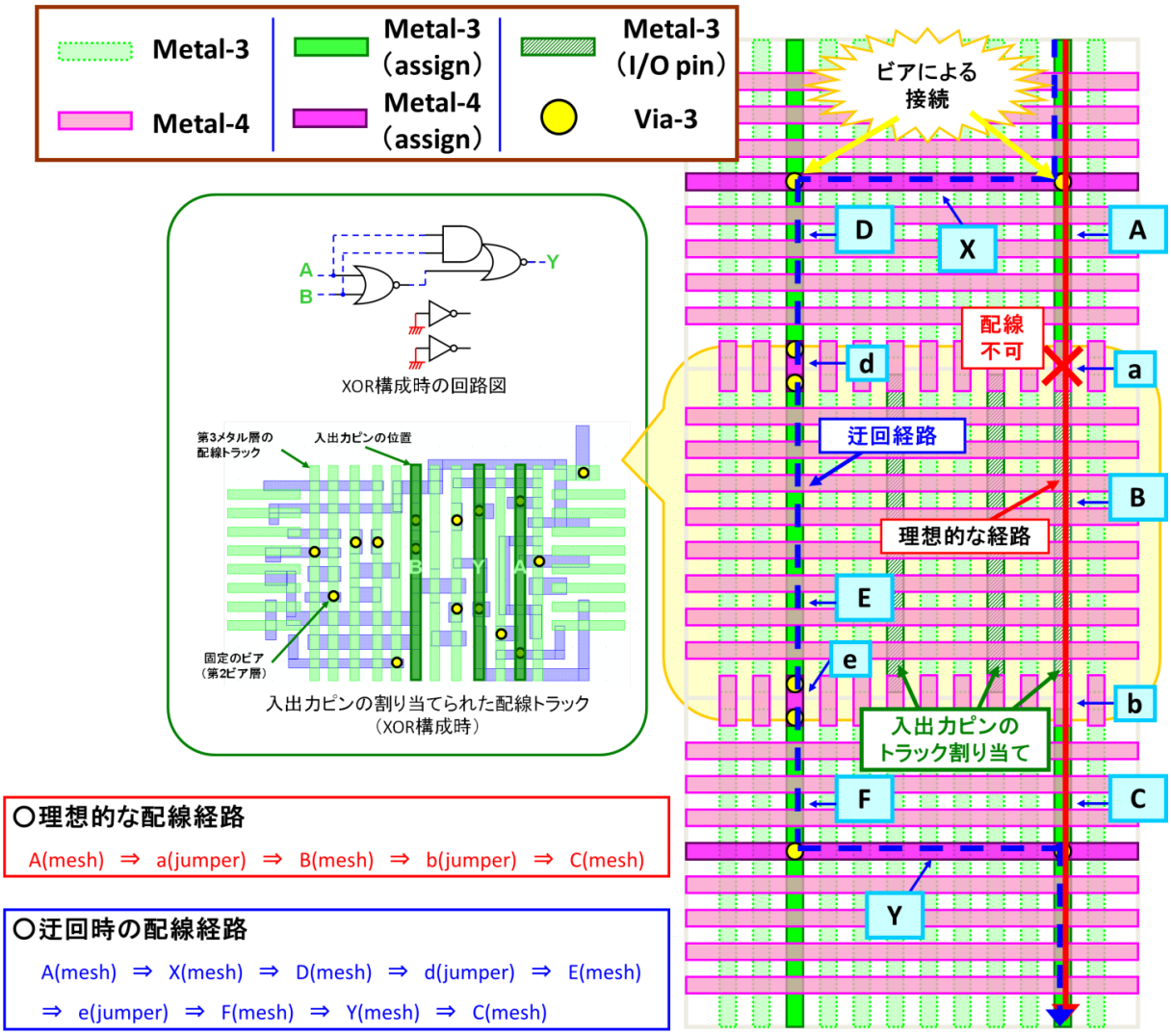


図４．３　IO ピントラックによる迂回配線の発生と配線混雑度の増加

VPEX2 アーキテクチャのメッシュ配線構造において，この迂回経路の形成が大きな問題となる[3]．図の破線は接続のできない領域を迂回して配線したときの例を示したものである．入出力ピン用のトラックの直前で配線経路を変更している． 図の例では迂回配線を形成するためだけに水平方向のメッシュ配

線トラックを 2 本，垂直方向のメッシュ配線トラックを 2 本の計 4 本の配線リソースを理想配線時よりも多く消費している．加えて，VPEX2 アーキテクチャでは LE の入出力ピンに割り当てられるトラックは再現する論理毎に異なる．したがって，今回示した迂回配線を必要とする領域が配線経路上の多くで形成されることになり，結果としてリソース損失が多く引き起こされる．結果として面積マージンを大きく見積もらなければ配線処理を成功させることが難しくなっている．

また第 2 ビア層がマスター層になっていることで引き起こされる 2 つ目の問題点として，第 2 メタル層の配線が複雑化し，LE の面積を小さくすることができない問題が上げられる．図 4．4 は VPEX2 の LE の第 2 配線層の形状を示したものである．LE 内を接続するための配線（a）と，入出力ピンとして第 3 メタル層に接続されるための配線（b）の 2 種類の配線が混載されている．2 種類の配線が混載している構造によって，第 2 メタル層の配線構造は非常に複雑になっている．そのため下層のトランジスタよりも大きな面積を必要するようになっていた．この LE 面積を削減するためにためには，まずこの第 2 メタル層の構造を最適化する必要がある．

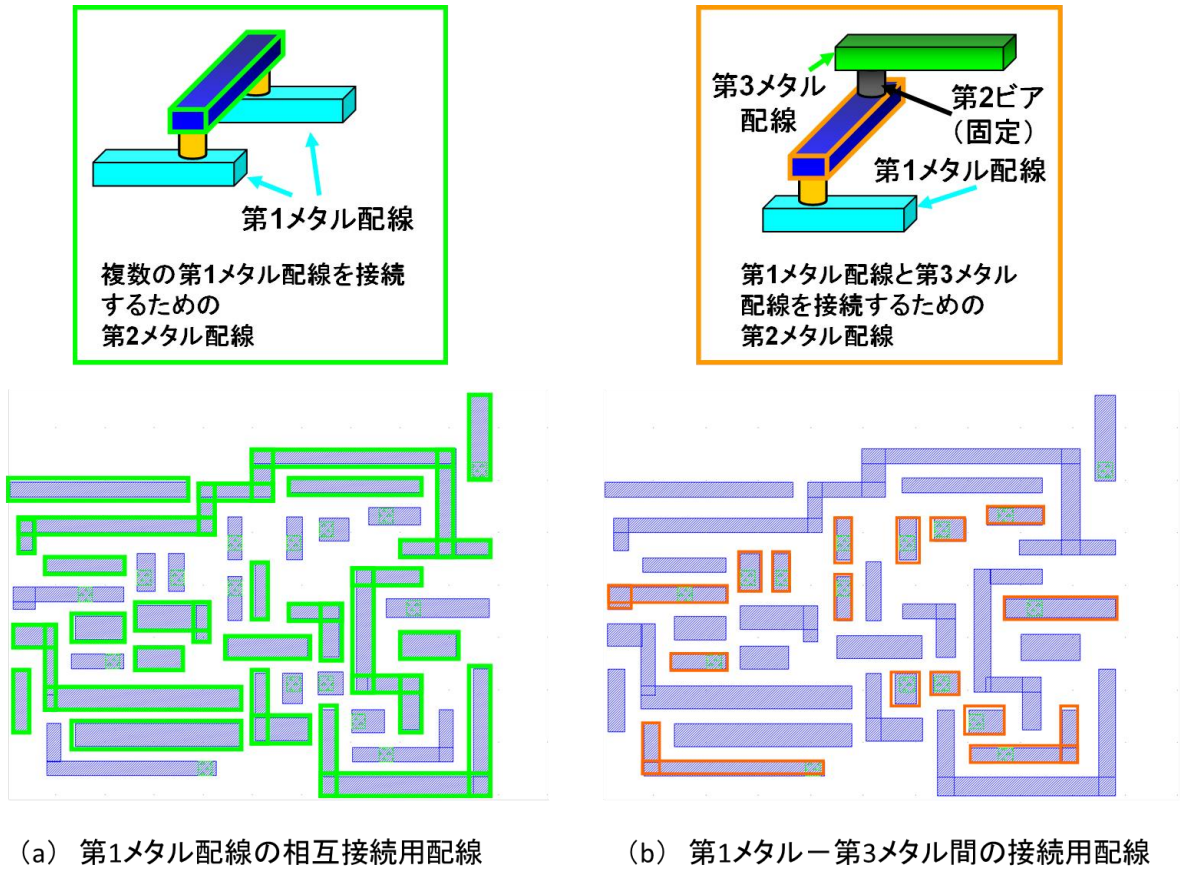


図 4．4　VPEX2 の LE の第 2 配線層パターンと役割

4．2　カスタム層 3 層構造の検討

VPEX2 の第 2 ビア層固定によって引き起こされている迂回経路問題を解決する手法として，図 4．6 で示すようにカスタム層を 1 層増やす事が考えられる．VPEX2 アーキテクチャでは第 1 ビア層と第 3 ビ

ア層の 2 つのビア層をカスタム層として利用していた．しかしカスタム層が 2 層の場合では，LE 内のトランジスタ同士を接続する配線と入出力ピンとして配線層に割り当てる際に用いる配線の 2 つの役割を持った配線を混載させる必要があり，LE の回路面積が悪化させていた．そこでカスタム層を 2 層から 3 層に増やし，この 2 つの役割を第 2 ビアによって切り替えるカスタム層 3 層構造について検討する

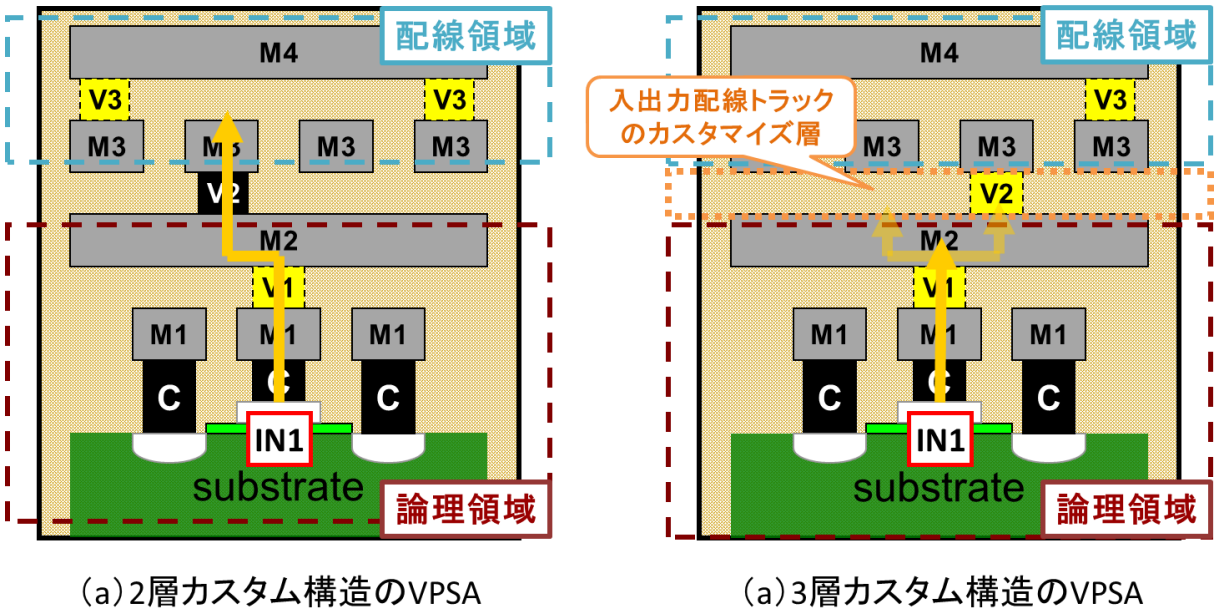


図４．６　論理領域・配線領域の領域分離構造

第 2 メタル配線層の入出力ピンと配線領域を分断しておき，ビアによるカスタム接続でピンと配線を繋ぐ，入出力配線トラックの「ビアカスタマイズ」について説明する．従来の VPEX2 アーキテクチャでは論理領域の入出力ピンは LE の再現論理ゲートが決定した段階で第 3 メタル層の配線トラックに自動的に割り当てられていた．

これに対して，入出力配線トラックを第 2 ビアによって決定するビアカスタマイズでは構成した論理ゲートに依存せず，自由な位置に入出力配線トラックを設定することができる．これを実現する方法が図４．７に示す第 2 メタルと第 3 メタルのメッシュ構造化である．メッシュ構造では任意の論理ゲートを再現したときに第 2 メタルの配線トラックのいずれかに入出力ピンが割り当てられる．この第 2 メタル配線は上部の配線層からは分離されており，任意の第 3 メタル配線トラックは第 2 ビアの座標を決定するときにはじめて入出力ピンが割り当てられる．そのため配線領域上で配線経路が決定した後に配線トラックと入出力を繋ぐ事が可能であり，入出力ピンが理想的な配線経路の構築を妨げることがなくなる．結果として，迂回配線の削減と配線混雑度の低減を期待することができる．

その例を図４．８に示す． 配線混雑度の増加は LE 内部の論理が決定した際に入出力ピンが配線領域上の配線トラックに定義され，それが配線経路の障害となっていたために引き起こされていた．ビアカスタマイズを用いることで入力配線トラックを任意の位置に設定することが可能になるため，理想配線経路を維持することが可能になる．

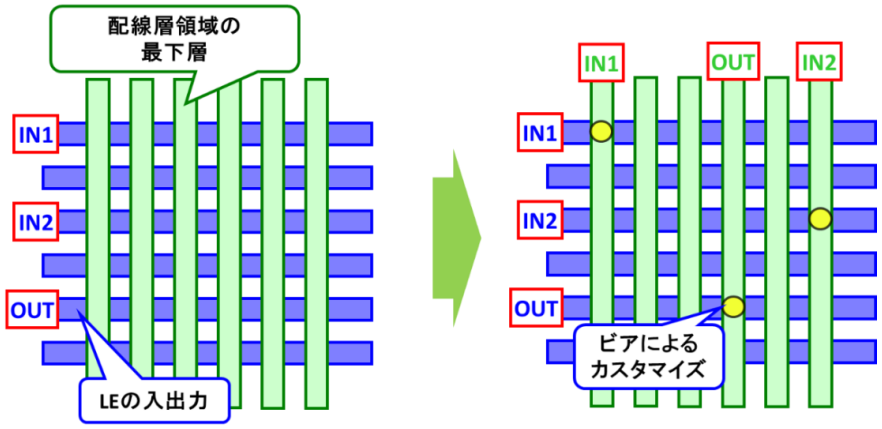


図４．７　入出力配線トラックのビアカスタマイズ

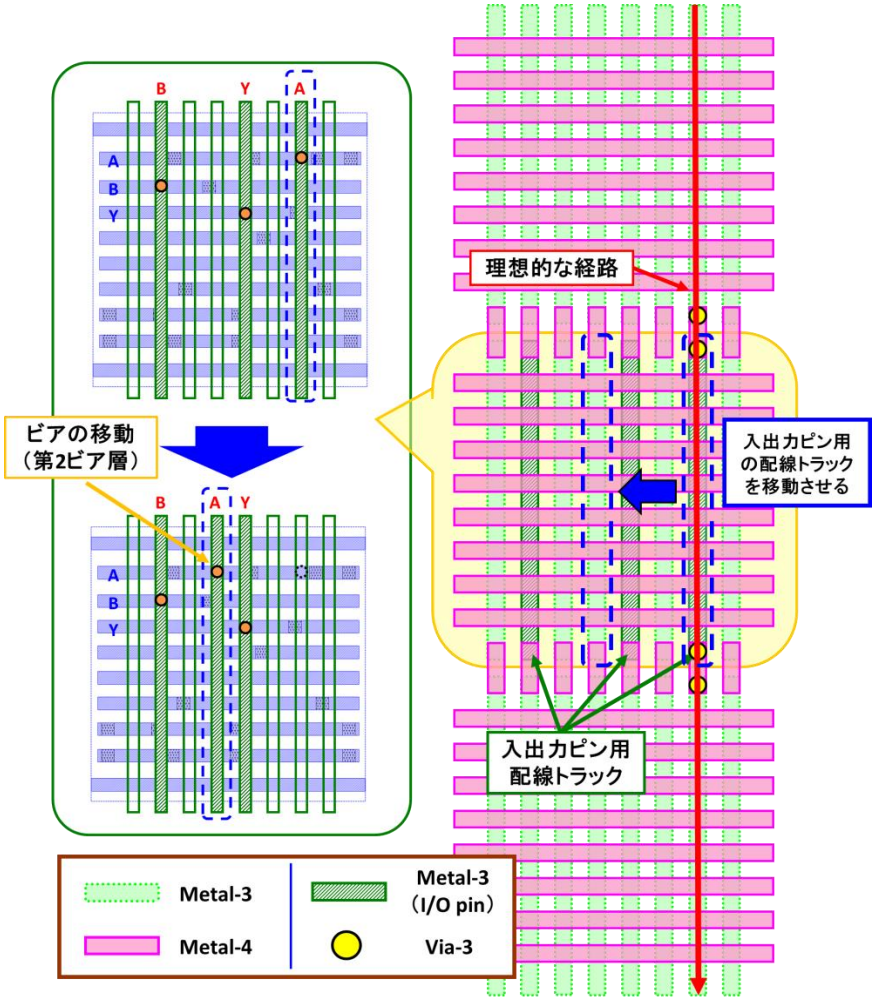


図４．８　第２ビア層による配線領域上の IO ピントラック座標の移動

４．３　LE の問題点に対する改善案検討

論理回路実装時の面積を改善するポイントは LE の再現可能な論理ゲートの種類を増やすことである．再現可能な論理ゲートの数が増すことで, 従来では複数の LE を使用して構成していた小規模な回路を 1 つの LE，あるいはより少ない LE 数で再現できるようになる．これによって回路を構成する論理素子の総数が減り，面積が削減される．他の試みとして LE を構成する論理ゲート素子を見直すことも考えられる．また VPEX2 の LE では INV，AOI，NOR の 3 つのゲート素子がベースとなっているが，この組み合わせを変えることで再現論理な論理ゲートの種類が拡張することも期待できる．

ここでは再現論理の増やすための LE レベル，LE を構成する論理ゲート素子レベルの改良案について紹介していく

① LE の再現論理の増加

VPEX2 アーキテクチャの LE が再現できる 3 入力の論理ゲートは AOI，MUX，MUXI の 3 種類である．しかしこれは十分な数の再現論理を網羅しているとはいえない．実際 ASIC の論理合成用ライブラリには，3 入力の AND，OR 素子など他にも多くの種類の 3 入力論理が登録されており，回路面積を縮小するのに役立てられている．したがって VPEX アーキテクチャでも LE で再現可能な 3 入力素子を増やすことで，面積の縮小に繋がると考えられる．

図４．９に VPEX2 の LE 構成においても再現可能な 3 入力素子の例を示す. 図のように AOI と INV を接続することで「AO」を，全ての素子を組み合わせることで 3 入力 AND を再現することができる．

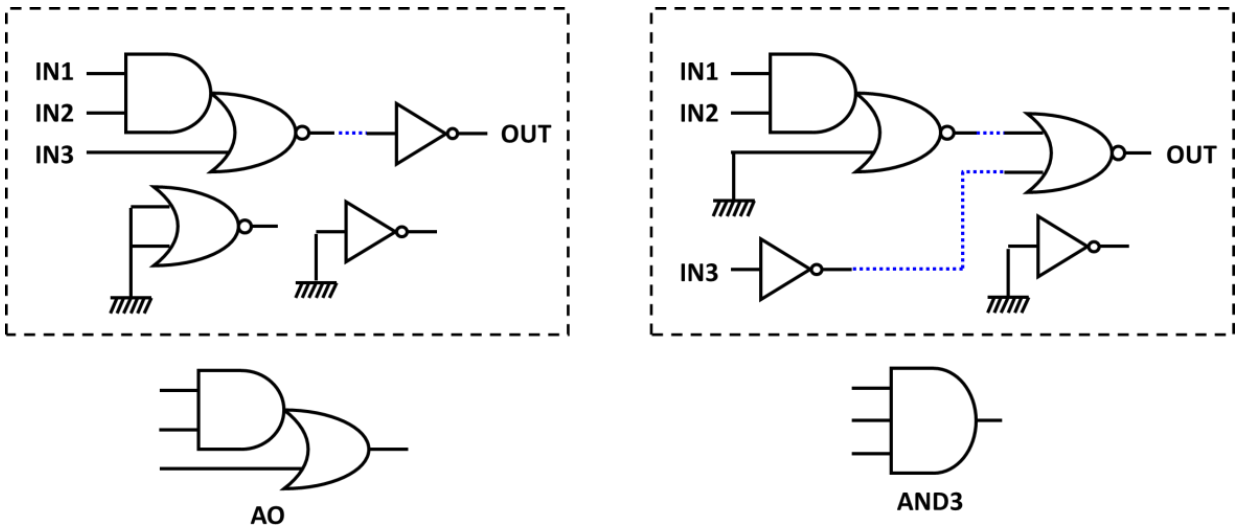


図４．９　VPEX2 アーキテクチャの LE で追加可能な再現論理素子の例

② Flexible-AOI

ビアのカスタマイズによって AOI 以外の基本論理ゲートに変化させることが可能な Flexible-AOI を提案する．図４．１０に AOI，OAI，NAND，INV-X2，TG(トランスミッションゲート)＋Clocked-INV の５つの素子を再現したときの例を示す．レイアウト図の黒線で繋がっている部分はそのまま変更せず,

青点線の接続を切り替えることで，同一のトランジスタ構造から様々な論理素子を再現することが可能である．

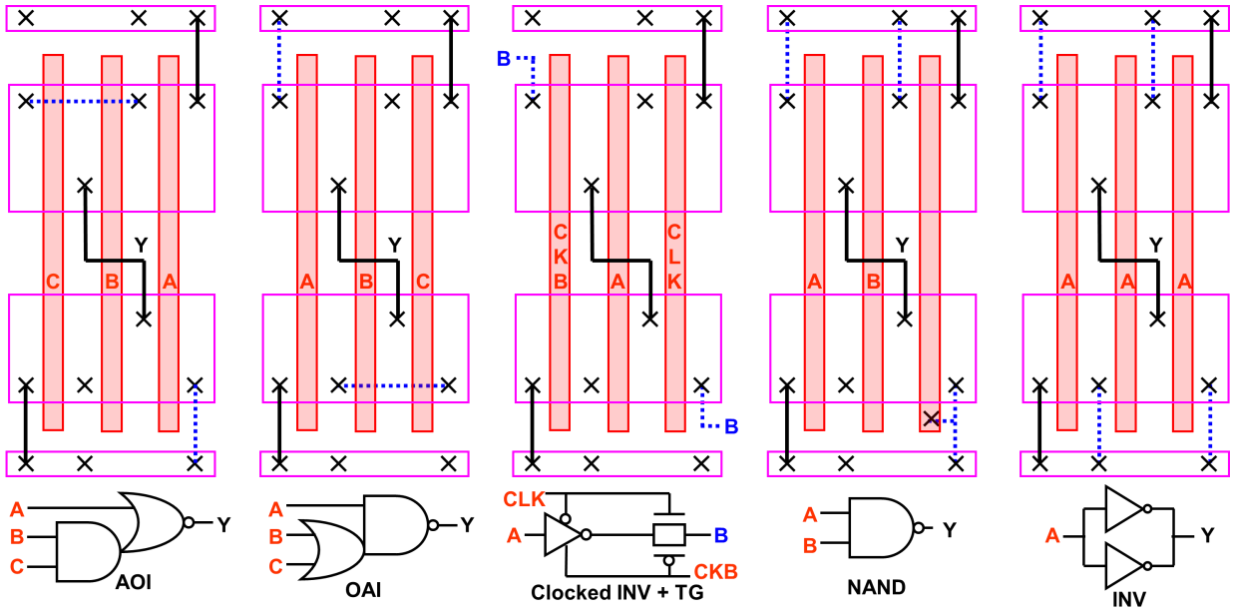


図４．１０　Flexible-AOI で再現可能な論理

Flexible-AOI によって再現された AOI ゲートは標準セルの AOI ゲートと使用する CMOS ゲートの数などは同じである．そのため Flexible-AOI は標準セルの AOI 論理素子と同等の面積でレイアウトを再現することが可能である．したがって，この Flexible-AOI を採用することで面積を増大させることなく OAI や Clocked-INV などの VPEX2 アーキテクチャでは再現不可能な論理ゲートを再現する事が期待できる．

③　NOR ゲートの通常構造化

VPEX2 アーキテクチャの LE を構成する NOR ゲートではトランジスタの S-D 接続あるいは D-D 接続の拡散領域を分割し，メタルとビアによって接続する「セパレート構造」を採用していた．セパレートにした部分は通常切り離しておき，第 1 ビア層のカスタマイズによって用途を変更する事が可能であった．これを利用することで図４．１１に示すように 2 入力 NOR 論理ゲート素子をトランスミッションゲートやバッファの出力段などに変化させ，DFF 再現や遅延改善用の BUF 再現などを行っていた．

しかし Flexible-AOI を通常の AOI の代わりに用いる場合，セパレート構造の NOR ゲートを利用しなくとも DFF や BUF の再現を行うことが可能になる．そこで NOR ゲートをセパレート構造から S-D や D-D を共有する通常構造に変更した．セパレート構造は 2 つの CMOS ゲートを分離する必要があったため，図４．１２のようにわずかなスペースシングやビア抵抗の増加が引き起こされていた．通常構造に戻したことで，これらが改善されることが期待できる．

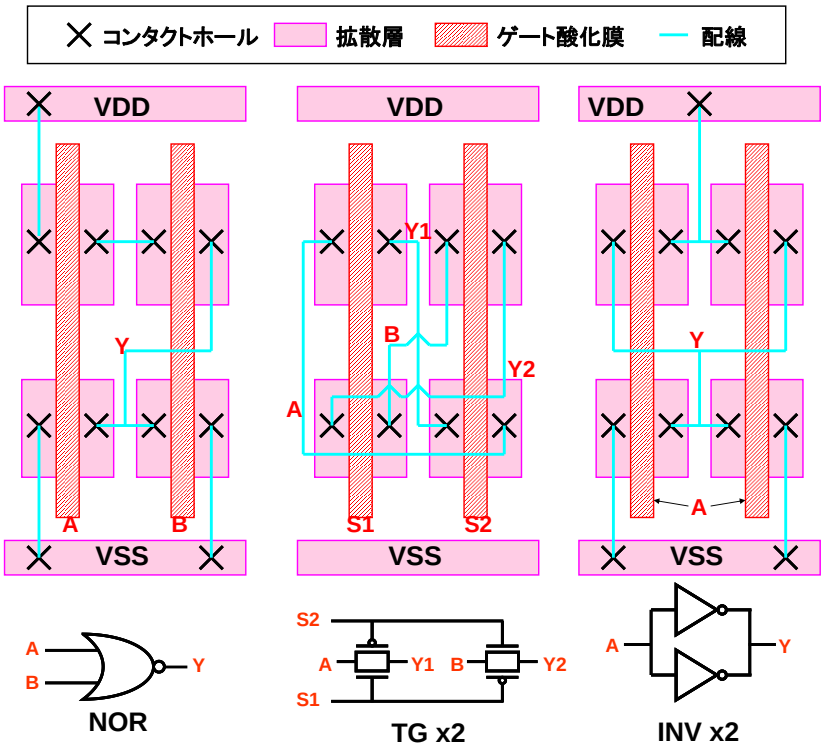


図４．１１　VPEX2 で使用されたセパレート構造の NOR ゲート

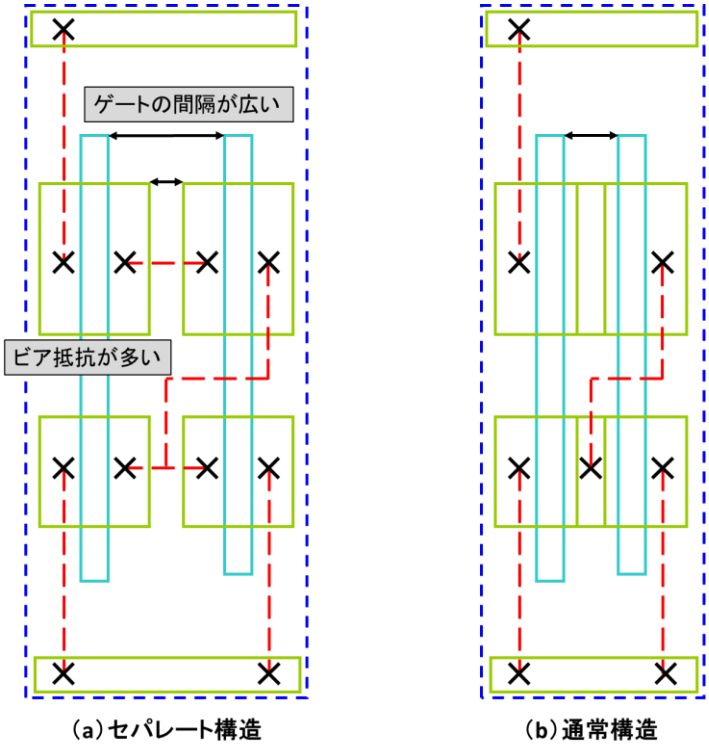


図４．１２　スタンダード構造とセパレート構造の面積比較

４．４　VPEX3 アーキテクチャの提案

以上の改善案を踏まえ，新しい VPEX アーキテクチャとして VPEX3 を本節で提案する．この VPEX3 はカスタム層 3 層構造を持つ VPSA アーキテクチャとして開発されている．まず初めに VPEX3 アーキテクチャの LE 構造について紹介する．VPEX3 アーキテクチャの LE は図４．１３が示すように縦 6μm，横 6μm，大きさで構成されており，LE 面積は 36μm² である．表４．２は VPEX3 アーキテクチャの LE の性能を VPEX2 と比較したものである．この LE サイズは VPEX2 アーキテクチャのおよそ 41%のサイズであり，59%の面積削減が行われている．また基本論理として新たに 9 種類の論理が再現可能であり，再現可能論理数でも VPEX2 を上回っている．

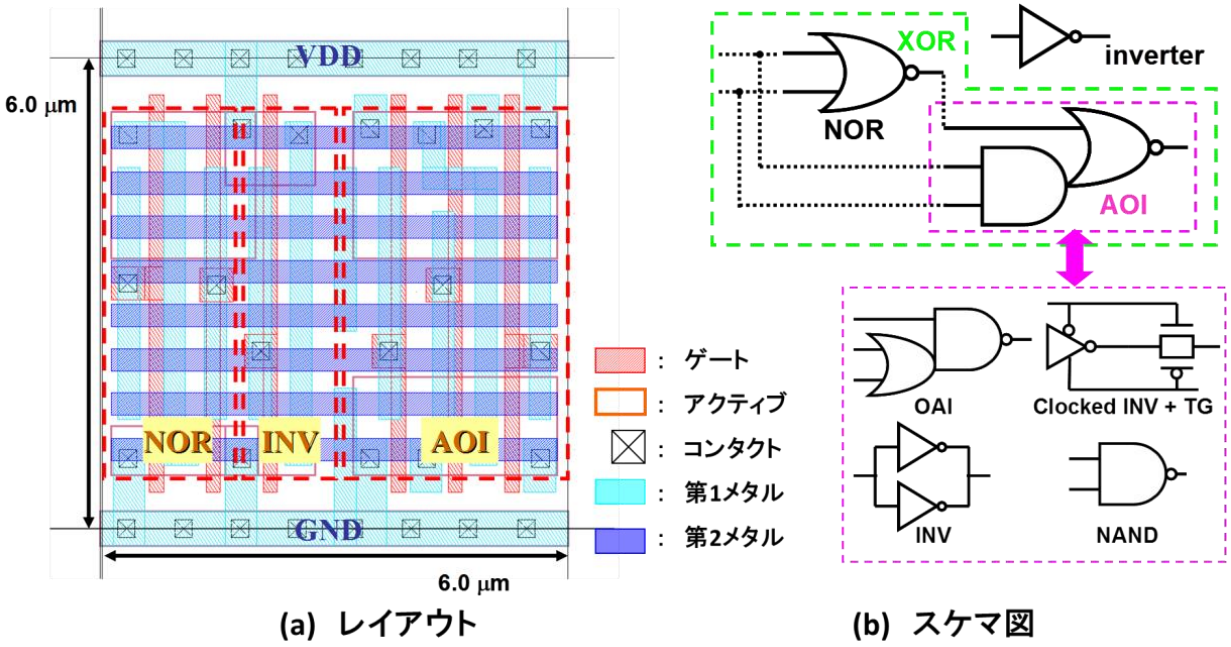


図４．１３ VPEX3 アーキテクチャの LE 構造

表４．２ VPEX2 との LE の基本性能比較

	VPEX2	VPEX3
面積	88.0μm²	36.0μm²
再可能現 論理数	2 入力論理 ＋AOI，MUX，MUXI	2 入力論理 ＋3 入力論理（12 種類）
DFF タイプ	可変 （LE2 個使用）	可変 （LE2 個使用）
ベースタイプ	スタンダードセル	スタンダードセル

VPEX3 アーキテクチャの基本構造は VPEX2 アーキテクチャと同様であり，LE をアレイ状に配置し，各 LE を配線領域で相互接続することで複雑な論理回路を実現する．また LE の構成も従来どおり，AOI

ゲートと NOR ゲートからなる XOR ゲートと INV ゲートの組み合わせによって構成されている.図４．１３に VPEX3 の LE の論理素子構成およびレイアウト図を示す．Rohm0.18μm プロセスルールでの設計を想定しており，LE を構成する要素素子間の隙間をなくし，可能な限り縮小したレイアウト構造をしている.

次に旧アーキテクチャと新アーキテクチャの差異および構造上の工夫について述べる．VPEX3 アーキテクチャの LE の様々な工夫によって 36μm² という面積を実現している．以下に LE の特徴を VPEX2 アーキテクチャの LE と対比させることで説明していく.

① 第 2 メタル層のメッシュトラック化と第 2 ビア層のプログラマブル化

VPEX3 アーキテクチャでは前節で紹介した「カスタム層 3 層構造」を採用している．論理領域の最上層である第 2 メタル層を水平に引き，配線領域の最下層である第 3 メタル層と直交する構造になっている(図４．１４中央)．また LE の各素子を第 1 ビア層で接続するために，第 1 メタル層で構成される全てのピンを第 2 メタル層と直行するメッシュ形状によって構成している（図 4.14左)．したがって VPEX3 アーキテクチャの LE はすべての階層がメッシュ状に重なった構造になっている.

VPEX3 は第 2 ビア層を含む，ビア 3 層がカスタム層になる．VPEX3 では用意しなければならないカスタムマスクが VPEX2 より多くなるため，初期開発コストの増化が懸念される．しかし VPEX3 では VPEX2 同様に「EB 直描技術」を利用してビア層を製造した場合には，カスタムマスクのマスクコストは 0 にすることができ，初期開発コストは VPEX2，VPEX3 ともに変わらない.

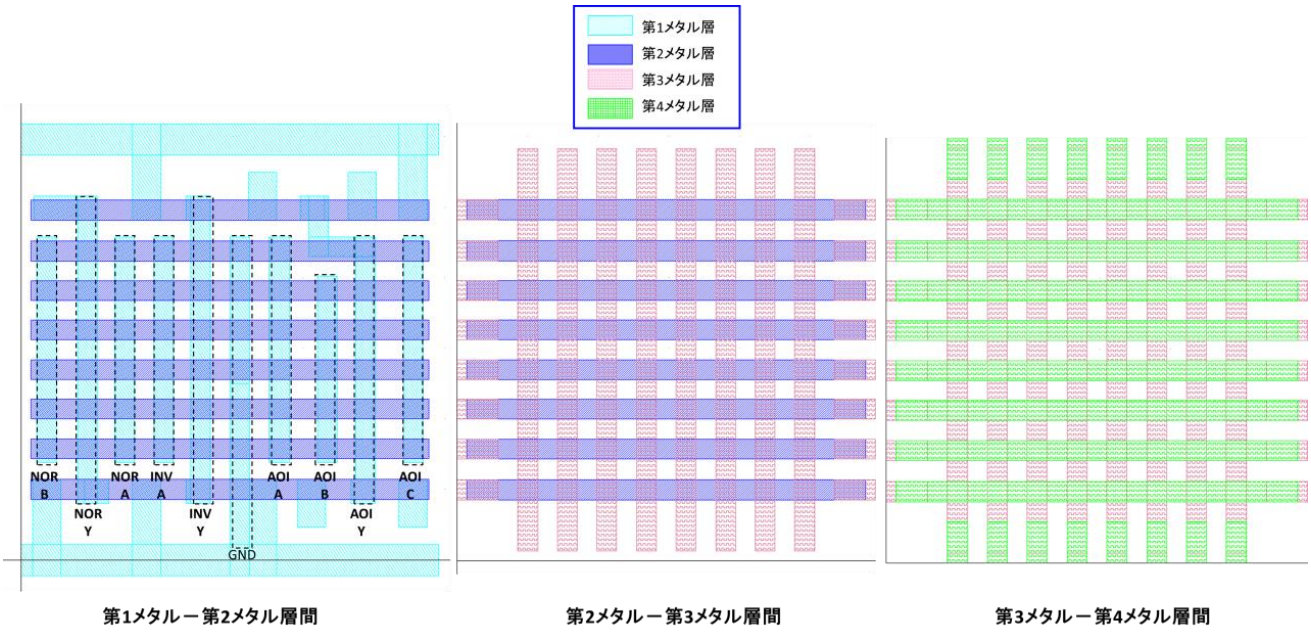


図４．１４ 各階層の構造図

② インバータを 1 つ削除

図４．15 に VPEX2 の LE と VPEX3 の LE のスティック図を示す．VPEX2 では 2 つのインバータ

素子（INV）を LE の両端の領域にそれぞれ設置されたレイアウトになっていた．VPEX2 では第 2 メタル層および第 1 メタル層の配線構造が複雑であったため，最左端と再右端の素子同士をビアプログラマブルによって接続する事が困難であり，左側の INV は NOR 論理ゲート素子との接続に，右側に置かれた INV は AOI 論理ゲート素子との接続に使用されていた．VPEX3 ではこれを廃止し，1 つ INV を LE の真ん中に据える構造に改造した. VPEX3 アーキテクチャでは第 1 メタルー第 2 メタル層間をメッシュ上にすることで離れた素子同士を繋ぐ事が容易になったため，この構造が 3 つの論理ゲートをそれぞれつなぐことが可能になり，この構造であっても VPEX2 で構成可能であった 13 種類の論理ゲートを実現できている．

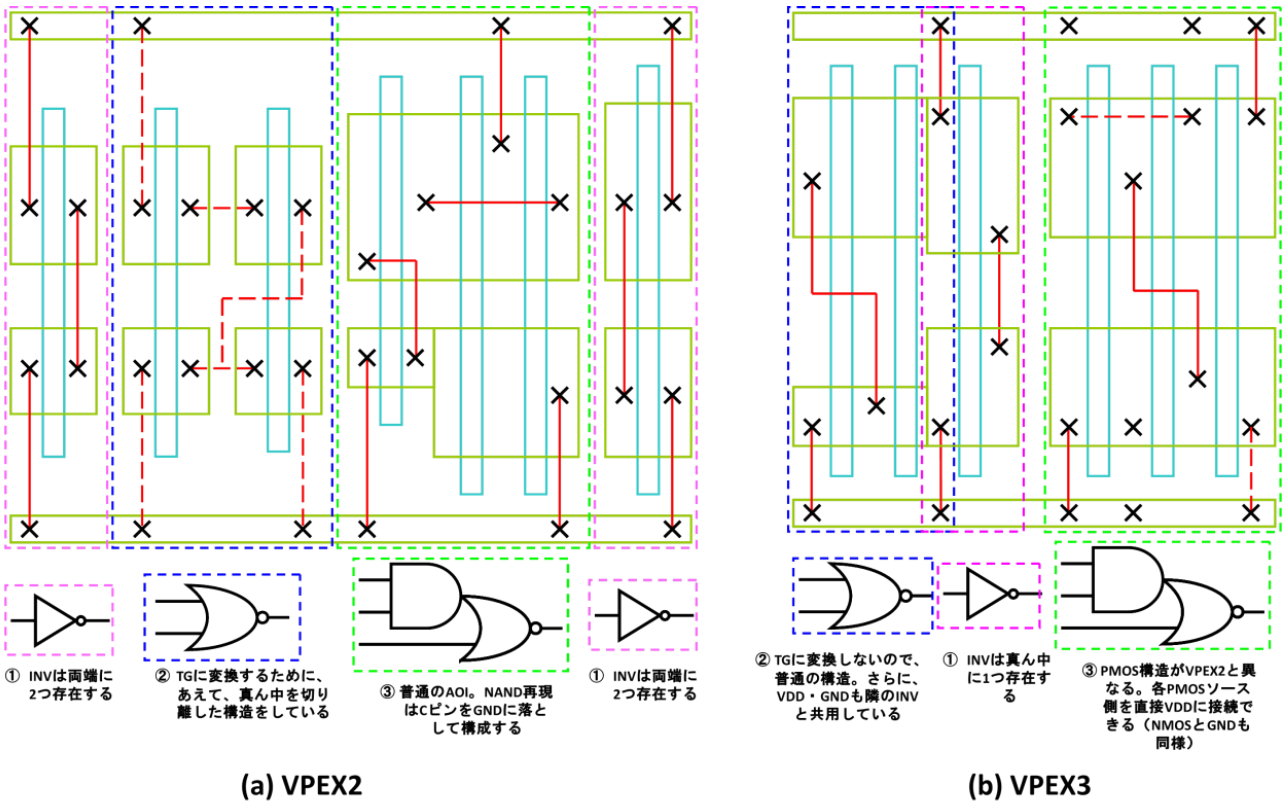


図４．１５　VPEX 毎の LE 構造の違い

① ゲート幅 W の削減

VPEX2 の LE に使用されている「AOI」「NOR」「INV」の 3 素子に関して，実際に LE 内部に実装されている基本論理素子のゲート幅と VDEC より提供されているスタンダードセルに使用されている同名の論理素子のゲート幅を比較すると，VPEX2 アーキテクチャの LE を構成する 3 つの素子のゲート幅は標準セルよりも非常に大きく設計されている．論理セルの設計方針には 2 通りあり，ゲート幅を大きくすることで動作速度を向上させる方法とゲート幅を小さくすることで面積を削減する方法を選択できる．VPEX2 ではセル速度を向上させるため構成に用いた論理ゲート素子に高いドライブ能力を持たせる設計になっていた．

VPEX3 アーキテクチャでは面積の削減を第 1 目標として設計するため，このゲート幅を最適化することで LE 面積の削減か可能である．そこで VEPX3 アーキテクチャの LE を構成する各論理ゲートのゲ

ート幅を VPEX2 のものより小さく設計した．

実際にゲート幅に関しては表４．３にまとめた．VPEX2 アーキテクチャでは PMOS の最大ゲート幅は 3400nm，NMOS の最大ゲート幅は 2000nm であったのに対して，VPEX3 アーキテクチャでは PMOS の最大ゲート幅 2400nm，NMOS の最大ゲート幅は 1200nm と大幅に削減している．

これによって形成する論理回路のセル速度の低下が懸念されるが，VPEX3 ではバッファセルを用いることでクリティカルパスの動作速度を改善することが可能であると考えている．

表４．３　ゲート幅の縮小

		スタンダードセル	VPEX2	VPEX3
AOI	P	620nm	2400nm	2100nm
	N	610nm	1200nm	1200nm
NOR	P	620nm	3400nm	2400nm
	N	610nm	2000nm	1200nm
NOT (Inverter)	P	620nm	2400nm	2100nm
	N	610nm	1200nm	600nm

④　Flexible-AOI ゲートの採用

VPEX3 アーキテクチャでは XOR を構成する AOI ゲートに前節で紹介した Flexible-AOI を使用している．この Flexible-AOI の採用により OA，OAI を再現したり，2 つの LE を組み合わせて記憶素子を再現したりすることが可能になった．

⑤　ノーマル NOR ゲートの採用

VPEX3 では NOR をセパレート構造にすることによって TG や INV にカスタマイズし，DFF や BUF ゲートを再現可能にしていた．この役割を Flexible-AOI ゲートが担うことが可能になったため，スタンダードセル同様の拡散領域を共有した構造に変更した．

４．４．１　再現可能な論理ゲート

VPEX3 では VPEX2 で再現可能であった 13 種類の論理素子に加えて，新たに 9 個の論理素子を再現可能にしている．図 ４．．１６に VPEX3 の LE が再現可能な論理ゲートを示す．図中で「New」となっている素子群が VPEX3 から新たに再現可能となった論理ゲートである．

これらはいずれも標準セルライブラリにも登録されている素子であり，論理合成時の素子削減が期待できる．

また図４．１７，１８に 2 つの LE を用いて構成した DFF の構成図を示す．VPEX3 では AOI 部を Clocked INV＋TG の構造にカスタマイズすることで DFF を再現する．この構成を用いることにより，VPEX2 よりも INV が１個少ない LE での DFF 構成を実現している．

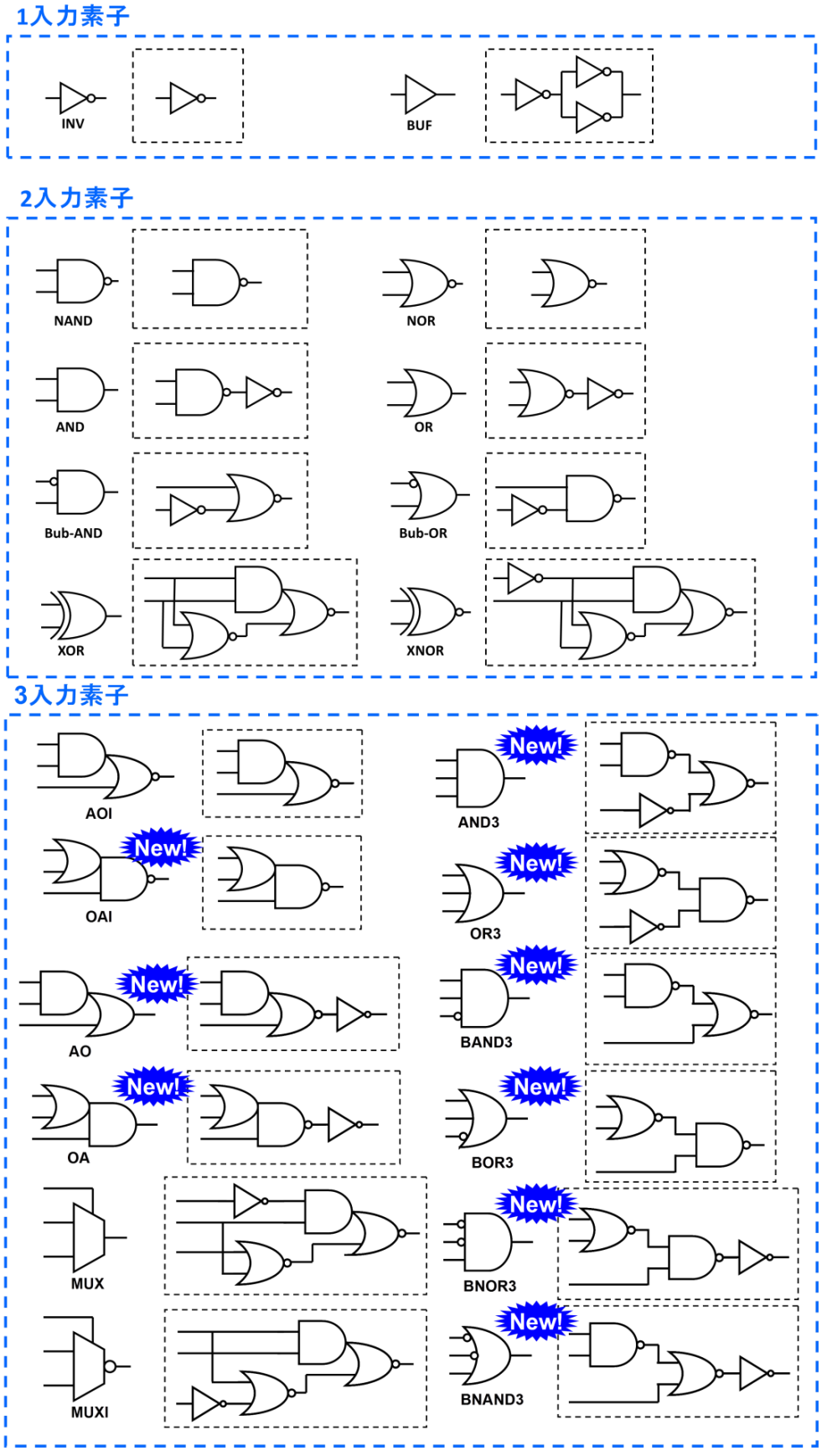


図４．１６　VPEX3 の LE で再現可能な論理ゲート一覧

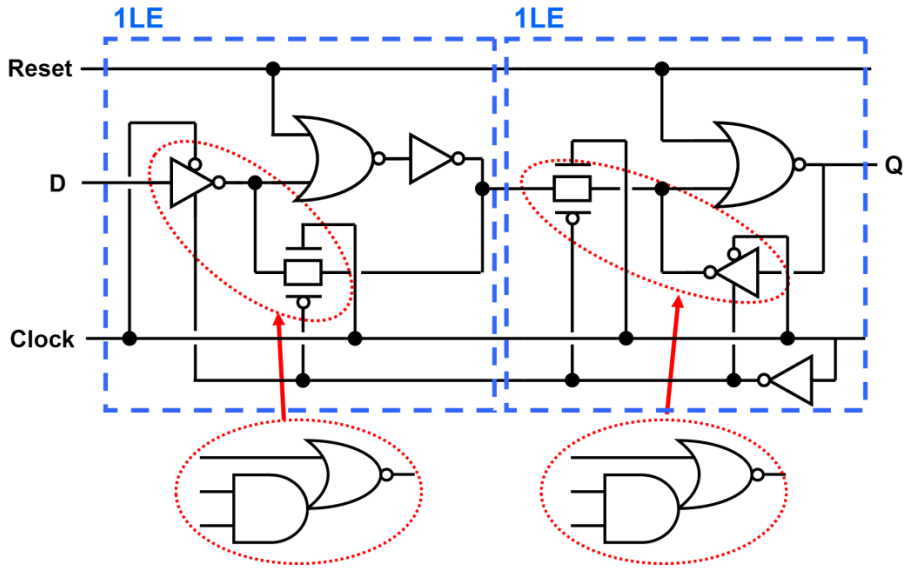
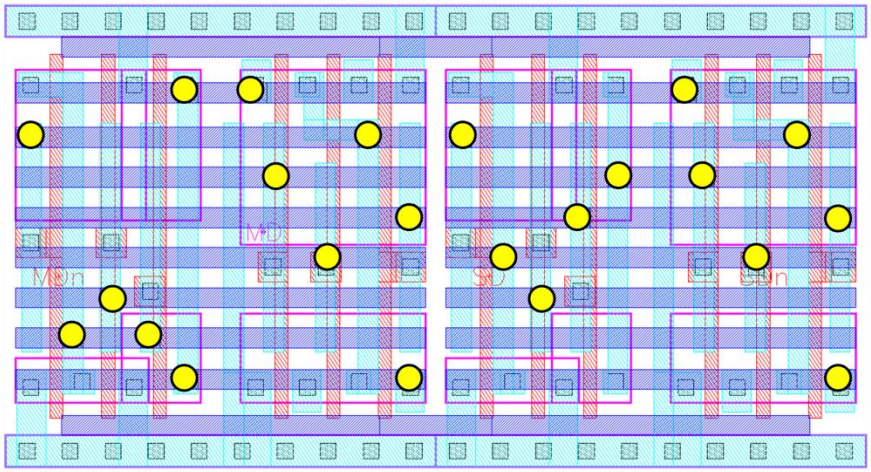
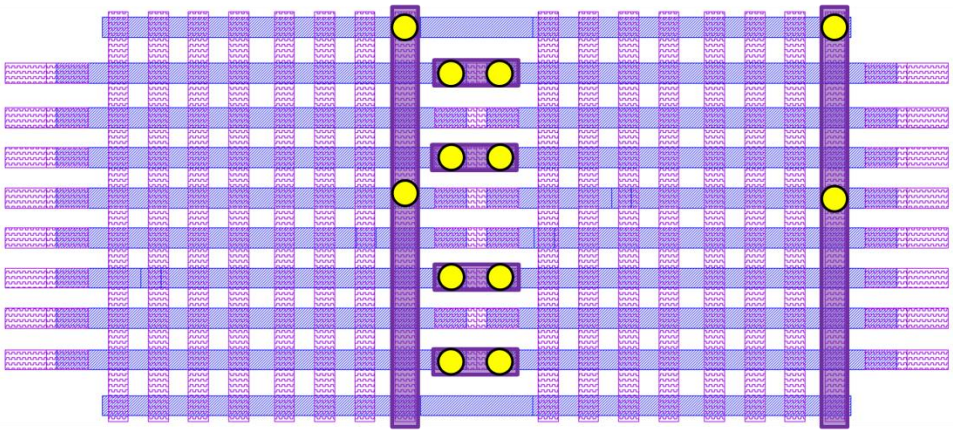


図４．１７　VPEX3 アーキテクチャの DFF 構造



（a） DFF再現時の第1ビアの座標



（b） DFF再現時に使用する配線リソースと第2ビアの座標

図４．１８　DFF のレイアウト構造

４．５　ベンチマーク回路を用いた性能評価

本節ではこれまで紹介した VPSA アーキテクチャ（2~4 入力 LUT，VPEX2，VPEX3）の回路実装面積の性能評価と性能比較を行う．

４．５．１　LE アーキテクチャのまとめ

3 章にて紹介した各 LE と VPEX3 の LE の特徴を表４．４にまとめる．LE 単体の面積では VPEX3 が最も小さく，4 入力 LUT が最も大きい．その逆に再現論理数では 4 入力 LUT が一番多くなる．

表４．４　各 LUT 型 LE の概要と面積

名称	入力数	DFF アーキテクチャ	LE 面積[μm²]
2-LUT	2 入力	可変型	93.1
3-LUT	3 入力	内蔵型	226.6
4-LUT	4 入力	内蔵型	484.6
VPEX2	2-3 入力	可変型※	88.0
VPEX3	2-3 入力	可変型※	36.0

※2 つの LE で 1 つの DFF を再現する

４．５．２　ベンチマーク回路

本実験で用いたベンチマーク回路を表４．５に示す．これらの回路を用いた性能評価によって LE アーキテクチャ間の性能差を明らかにする．本性能評価では ISCAS’85[4]および ISCAS’89[5]ベンチマーク回路から，8 つの論理回路を用いた．

また，東京大学 VDEC より提供されている Rohm180nm プロセスルールのスタンダードセルライブラリ「京大セル」を用いた場合の論理合成結果について表４．６に示す．論理合成時の制約条件は面積最小化のみで速度制約は与えていない．後の性能評価では各 VPSA アーキテクチャの論理回路実装後の面積性能をこの面積値を基準値とした相対値で示す．

表４．５　ベンチマーク回路のスペック

回路名	組み合わせ／順序	IO 数	DFF 数
c2670	組み合わせ回路	221	なし
c3540	組み合わせ回路	72	なし
c5315	組み合わせ回路	301	なし
c6288	組み合わせ回路	64	なし
s1494	順序回路	24	6
s5378	順序回路	86	176
s9234	順序回路	22	145
s13207	順序回路	216	627

表４．６　ASIC の論理合成結果

回路名	動作速度[us]	論理素子数[個]	面積[μm²]
c2670	8.89	289	5331.917
c3540	17.63	420	7289.856
c5315	10.87	689	12908.85
c6288	59.26	1646	26662.81
s1494	8.14	594	10428.36
s5378	9.03	1116	25675.78
s9234	9.73	912	22569.52
s13207	9.76	2004	67344.08

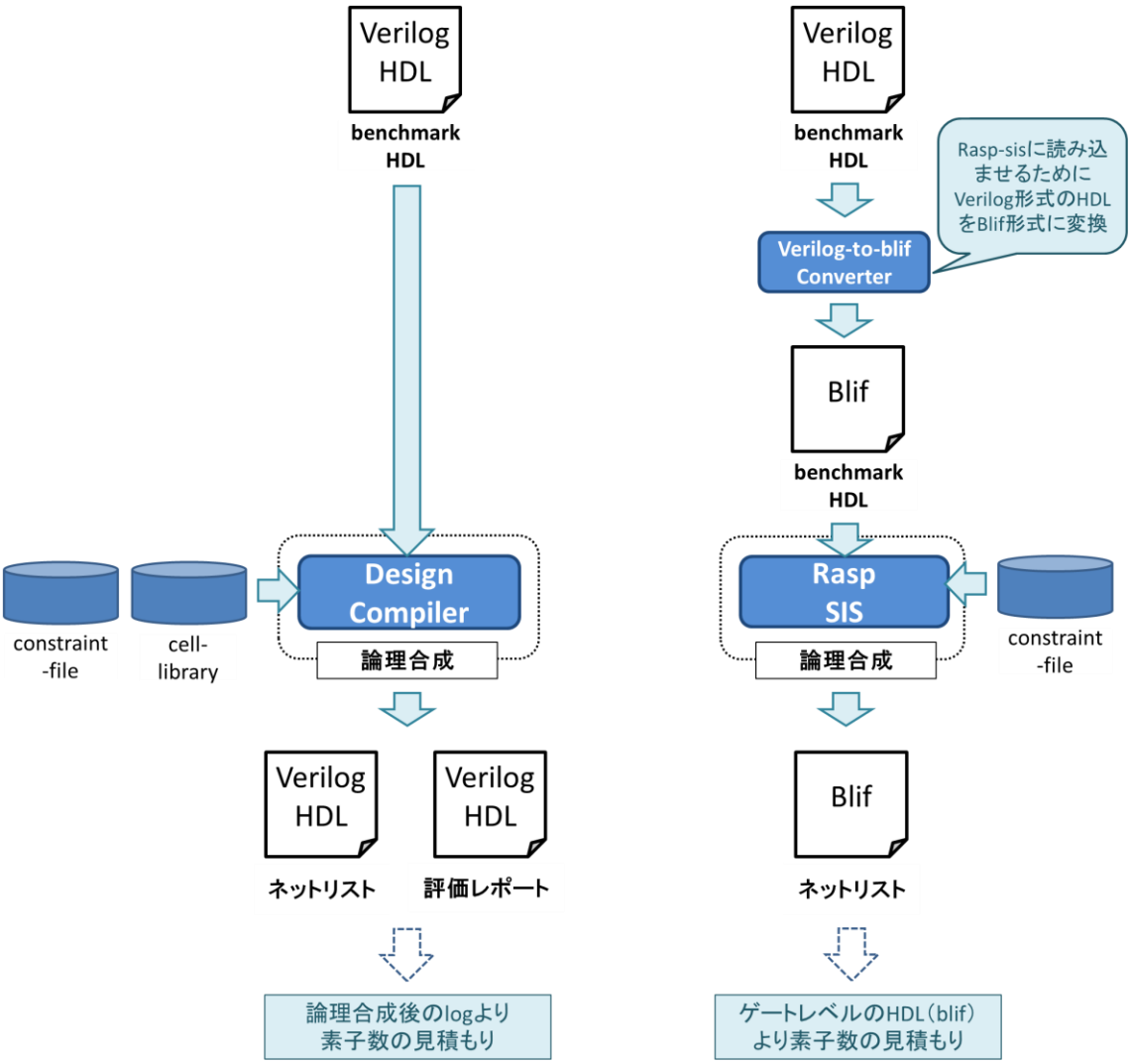
４．５．３　性能評価フロー

各 VPSA アーキテクチャにおける性能評価方法について説明する．本性能評価では論理合成後のネットリストを分析することで素子数や面積を割り出した．図４．１９にフローの詳細を示す．アーキテクチャによって利用した論理合成ツールが異なり，VPEX2 および VPEX3 では Synopsys 社の論理合成ツール DesignCompiler，各 LUT では Rasp-sis[6]を利用した．

ベンチマーク回路は Verilog-HDL によって記述されており，そのままでは rasp-sis によって論理合成を行うことができない．そこで rasps-sis の入力ファイル形式である「blif」というフォーマットに変換する．blif は論理回路を真理値表で記述する形式をした HDL であり，今回用いたベンチマーク回路を一旦単純なゲートレベルの Verilog HDL に変換し，さらにゲート論理と対応した真理値表テーブルに機械的に変換することで blif フォーマットのベンチマーク回路を作成した．この変換プログラムは C 言語を用いて自作した．

また DesignCompiler には専用のセルライブラリが必要となる．そこで VPEX3 および VPEX2 の論理合成用ライブラリは，提供された MOS の SPICE モデルと寄生抵抗・寄生容量パラメータを用いて再現論理ゲート素子すべての回路図を作成し，HSPICE のシミュレーション結果より動作速度および消費電力のモデル化を行った．この動作速度-消費電力モデルは Non-Linear Delay Model（NLDM），Non-Linear Power Model（NLPM）と呼ばれるテーブル参照式モデルを採用した．シミュレーションに用いた回路図を作成する際には MenterGraphic 社の回路検証・寄生パラメータ抽出用 CAD ツール「Calibre」によって寄生容量・寄生抵抗の抽出を行っている．なお今回の性能評価では rasp-sis に動作速度と消費電力を見積もる手段が存在しなかったため，論理合成時の回路面積の比較結果のみを報告する．

また図４．１５の各フローでは面積最小制約のみを与え，速度制約を与えない条件での論理合成を行った．これは Rasp-sis では面積最小制約を与える事は可能であったが，動作速度モデルが存在せず，DesignCompiler と同精度の速度見積もりを行うことが出来ためである．



（a） VPEXシリーズの素子数見積もり手法　　（b） 各LUT型の素子数見積もり手法

図４．１９　アーキテクチャ毎の性能評価フロー

４．５．４　素子数比較

VPSA 毎のベンチマーク回路合成時の必要論理素子数を比較する．表４．８に各 LE アーキテクチャで８種類のベンチマーク回路を再現するために使用した論理素子数をまとめた．表には２入力論理素子から４入力論理素子までを入力数毎に分けて示しているが，１入力素子（インバータ，バッファ）は２入力論理素子の項に含まれている．また DFF の数は割愛している．

さらに ASIC の素子数を基準値１としたときのベンチマーク回路毎の素子数比を図４．２０に示す．

表４．８　回路構成に必要な素子数

	2-LUT	3-LUT		4-LUT		
	2 入力素子	2 入力素子	3 入力素子	2 入力素子	3 入力素子	4 入力素子
c2670	468	111	284	102	54	116
c3540	624	68	354	52	118	177
c5315	1141	201	629	168	298	225
c6288	2245	195	1036	214	272	627
s1494	746	70	417	26	86	212
s5378	1413	229	684	226	286	272
s9234	1024	191	384	110	246	253
s13207	2544	638	872	448	442	668

	VPEX2		VPEX3	
	2 入力素子	3 入力素子	2 入力素子	3 入力素子
c2670	291	69	234	102
c3540	375	129	205	216
c5315	564	259	401	322
c6288	1196	438	855	603
s1494	744	18	378	203
s5378	1448	59	727	434
s9234	856	112	611	260
s13207	2128	230	1320	646

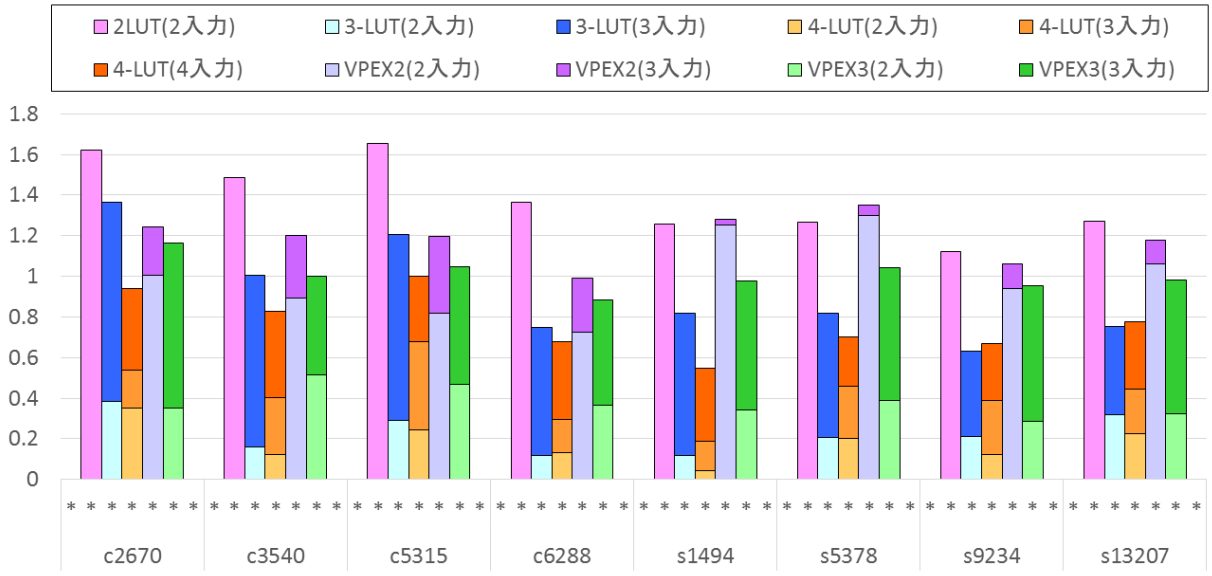


図４．２０　素子数の比較

（スタンダードセル ASIC 時の素子数を１とした際の素子数比）

素子数を比較すると，3 入力 LUT 型および 4 入力 LUT 型の VPSA アーキテクチャがより少ない論理素子数で各論理回路を実現できていることが分かる．これは 3，4 入力 LUT 型の方が再現できる論理の幅（3 入力論理，4 入力論理）がほかの 2 つのアーキテクチャよりも遥かに広いためと考えることができる．実際にこれらのアーキテクチャは 2 入力論理の使用率が少なく，3 入力以上の論理が多く使用されている．同様にして VPEX3 でも 3 入力論理が多く使用され，結果として 3 番目に素子数が少なくなっている．

一方で VPEX3 と VPEX2 を比較すると，すべてのベンチマーク回路で VPEX3 の素子数の方が少ない事がわかる．これは VPEX2 が再現可能な 3 入力論理が MUX,MUXI,AOI の 3 種類であったのに対して，VPEX3 では AND3，OR3，OAI，AO，OA などスタンダードセルにおいても良く利用される主要な 3 入力論理を 5 種類多く再現できるようにしたことが影響していると考えられる．特に s1494 と s5378 では VPEX2 と比較して素子数が約 35%削減されており，これらの結果から VPEX3 で拡張した 3 入力論理が素子数を減らす上で有効であったことを示しているといえる．

４．５．５　面積比較

素子数より各ベンチマーク回路の面積見積もりを行った．各 VPSA アーキテクチャの LE 面積および DFF 面積については表４．９に示した方法に則って面積の見積もりを行った．今回の評価では内蔵型 DFF アーキテクチャの場合は論理再現に用いた LE 内にある DFF を利用しているとして面積評価にカウントしていない．一方で可変型 DFF アーキテクチャの場合では DFF の面積を回路面積に含めて評価を行った．また 4 入力 LUT ではマルチグレイン構造を採用しているため 3 入力以下の論理素子を再現するときの面積は通常の半分の面積になるとしている．

表４．９　VPSA アーキテクチャごとの単位面積

名称	DFF アーキテクチャ	論理再現時の面積 [μm²]	DFF 再現の面積 [μm²]
2-LUT	可変型	93.1	93.1
3-LUT	内蔵型	226.6	0
4-LUT	内蔵型	484.6 (242.3)	0
VPEX2	可変型※	88.0	176.0
VPEX3	可変型※	36.0	72.0

面積性能の比較結果を表４．１０，図４．２１に示す．図４．２１は横軸を各ベンチマーク回路を示しており，左の棒グラフから順に 2 入力 LUT，3 入力 LUT，4 入力 LUT，VPEX2，VPEX3 を表している．また縦軸は ASIC の面積を 1 とした時の面積比を表している．

表４．１０　各アーキテクチャにおける面積性能

(a) 論理構成後の面積

面積	2-LUT	3-LUT	4-LUT	VPEX2	VPEX3
c2670	43570.8	89507.0	94012.4	31680.0	12096.0
c3540	58094.4	95625.2	126965.2	44352.0	15156.0
c5315	106227.1	188078.0	221946.8	72424.0	26028.0
c6288	209009.5	278944.6	421602.0	143792.0	52488.0
s1494	70011.2	110354.2	129872.8	68112.0	21348.0
s5378	147935.9	206885.8	255868.8	163592.0	54468.0
s9234	108833.9	130295.0	208862.6	110704.0	41796.0
s13207	295220.1	342166.0	539359.8	317856.0	115920.0

(b) スタンダードセル ASIC における面積を 1 とした際の比

面積	2-LUT	3-LUT	4-LUT	VPEX2	VPEX3
c2670	8.17	16.79	17.63	5.94	2.27
c3540	7.97	13.12	17.42	6.08	2.08
c5315	8.23	14.57	17.19	5.61	2.02
c6288	7.84	10.46	15.81	5.39	1.97
s1494	6.71	10.58	12.45	6.53	2.05
s5378	5.76	8.06	9.97	6.37	2.12
s9234	4.82	5.77	9.25	4.91	1.85
s13207	4.38	5.08	8.01	4.72	1.72

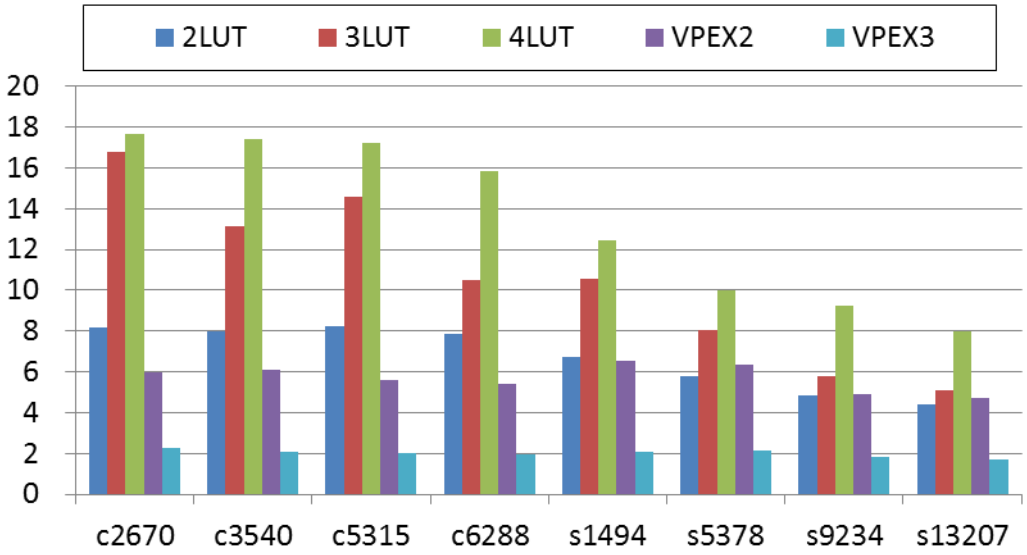


図４．２１　VPSA アーキテクチャ毎の面積比の比較
（スタンダードセル ASIC 時の面積を１とした際の面積比）

性能評価結果をみると，2 入力 LUT 型の最小面積が ASIC の約 4.4 倍，3 入力 LUT 型が約 5.0 倍，4 入力 LUT 型が約 8.0 倍，VPEX2 が約 4.7 倍であるのに対して，VPEX3 の最小面積は 1.7 倍となった．よって評価結果から VPEX3 アーキテクチャが LE アレイ構造を持つビアプログラマブルアーキテクチャ群の中でも，非常に小面積化が可能な優れたアーキテクチャである事が分かる．

また，それぞれの実装における面積の平均値に注目すると，VPEX2 が ASIC の約 5.6 倍．2 入力 LUT 型が 6.7 倍，3 入力 LUT 型では約 10．5 倍，4 入力 LUT 型では ASIC の約 13.5 倍であるのに対して．VPEX3 では平均して約 2.0 倍という結果が得られた．よってすべての回路で VPEX3 が優れており，また VPEX3 アーキテクチャを用いて構成した場合では他の LE と比較して 1/5～1/3 の面積で実装可能という結果になった．したがって VPEX3 アーキテクチャは回路面積を大幅に削減することに成功したといえる．

第 4 章の参考文献

[1] 西本智弘，川原崎正英，長谷川英司，寺川知宏，藤野毅，“ビアプログラマブルデバイス VPEX のロジックエレメント改良による面積削減と高性能化”，電子情報通信学会，ICD2008-122，pp.101-106，2008 年.

[2] T.Fujino, T.Nishimoto, Y.Kokusho, M.Yoshikawa, G.Lemieux, “Via-programmable Logic Array VPEX2 with Configurable DFF using 2 Logic Elements”, The 12th International Symposium on Integrated Circuits (ISIC’09), pp.21-24, (2009)

[3] 山田翔太，國生雄一，西本智広，吉田直之，堀遼平，松本直樹，北森達也，吉川雅弥，藤野毅，“ビアプログラマブルデバイス VPEX のロジックアレイブロックと配線アーキテクチャの検討” 電子情報通信学会技術研究報告 VLD2009-107, pp.49-54, 3 月 2010 年.

[4] F.Brglez, H.Fujiwara, "A neutral netlist of 10 combinational benchmark circuits and a target translator in FORTRAN", Proc. of the IEEE International Symposium on Circuits and Systems (ISCAS), Special Session on ATPG and Fault Simulation, pp.695-698, June 1985.

[5] F.Brglez, D.Bryan, K.Kozminski, "Combinational profiles of sequential benchmark circuits", Proc. of of the IEEE International Symposium on Circuits and Systems (ISCAS), Vol.3, pp.1929-1934, May 1989.

[6] "RASP - LUT Based FPGA Technology Mapping Package", http://cadlab.cs.ucla.edu/software release/rasp/htdocs/

第 5 章　Via Configurable Logic Block との性能比較

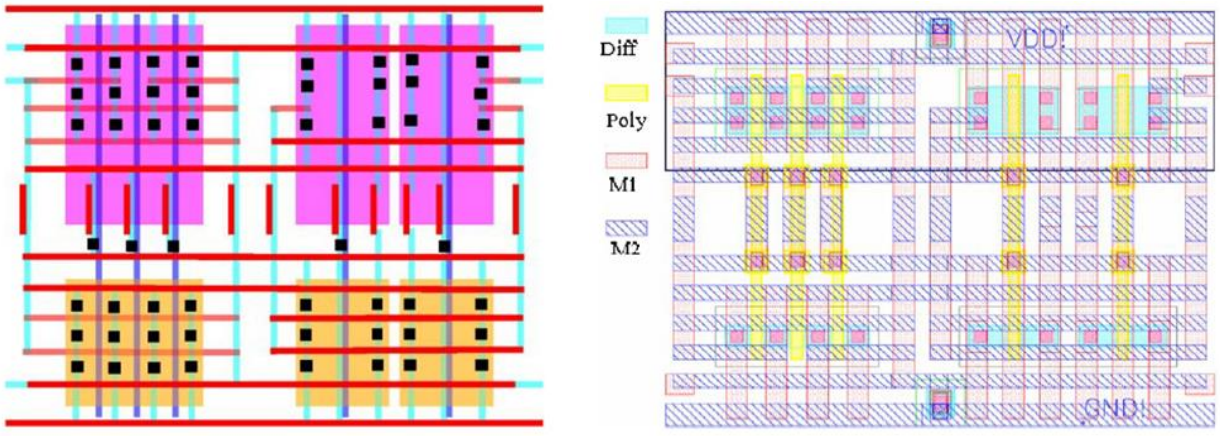
本章では VPEX3 アーキテクチャの性能を客観的に評価するために他の研究機関で提案されているマスクプログラマブルデバイス（MPD：Mask Programmable Device）との比較を行った．比較対象は VPEX3 の開発に用いた Rohm180nm プロセスルール[1]と同じゲート長（180nm）プロセスで開発されていた，台湾の元智大学で研究開発が進められている Via Configurable Logic Block（VCLB）[2-4]を選択した．本章では VCLB のアーキテクチャを説明および評価方法を説明し，面積・動作速度・消費電力に関する比較結果を示す．

５．１　Via Configurable Logic Block の概要

VCLB は TSMC[5]180nm プロセスによって設計されている MPD である．VCLB は VPEX と同様にロジックエレメント（LE：Logic Element）をアレイ状に配置した構造によって構成されており，論理の変更は第 1 ビア層のカスタマイズによって実現されている．図５．１（a）に VCLB のスティック図，図５．１（b）にレイアウト図を示す．論理はビアのカスタマイズによって実現されているが，その一方で論理ゲート間の結線は，スタンダードセルやゲートアレイのように金属配線層をフルカスタマイズして接続する構成になっている．

VCLB の LE の面積は 78μm² となっており，VPEX3 の 2 倍のサイズである．またゲート幅は PMOS 側が 3.665μm，NMOS 側が 2.255μm であり，VPEX3 の 1.5～3.6 倍の大きさを有している．構成可能な素子は出力駆動能力の異なるセルを含めて 105 種類存在し，さらに複数の LE を利用することで 73 種類の論理ゲートを再現することができる．

参考論文[2]ではいろいろな制約条件による ASIC との比較結果が報告されている



（a）VCLB の LE スティック　　（b）VCLB の LE レイアウト図

図５．１　VCLB の LE 構造[2]

(Hui-Hsiang Tung,“Via-configurable Logic Block Architectures for Standard Cell like Structured ASICs”　p, 383 より引用)

５．２　ベンチマーク回路

本章での比較では VCLB の評価で使用されていた ITC'99 ベンチマーク回路[6]から 5 種類の回路をベンチマーク用回路として用いた．回路の機能を表５．２に示す．表に示すように，ITC'99 ベンチマーク回路では b14，b15 が基本回路となっており，b17～b19 は b14,b15 を複数組み合わせた回路となっている．

表５．１　ITC'99 ベンチマーク回路機能

回路名	機能	b14	b15
b14	Viper processor	1	0
b15	80386 processor	0	1
b17	Three copies of b15	0	3
b18	Two copies of b14 and two of b17	2	6
b19	Two copies of b18 and two of b17	4	18

５．３　性能評価と比較

初めに評価方法について説明する．本評価では複数の制約条件によって論理合成を行い，その結果得られたゲートレベル論理回路に対して静的解析を行い，面積，動作速度，消費電力をそれぞれ測定した．まず動作速度制約を課さず，面積制約のみを与えた最小面積条件による論理合成を行う．この結果得られた回路は最も面積が小さい回路となるが，動作速度は最適化されていない．これを「Base1.0」と呼ぶことにする．次に Base1.0 の動作速度解析結果に注目する．このときの動作速度に対して，表５．２に示すような動作速度制約を各回路に与え，論理合成を実行する．表５．２に示した制約条件では下に行くほど速度制約が厳しくなっていく．したがって表５．２の上にあるほど低速で面積の小さい回路が合成され，下にあるほど高速で回路規模の大きい回路が合成される．

表５．２　名称と制約条件

制約条件名	面積制約	動作速度制約
Base1.0	最小サイズ	なし
Base0.8	最小サイズ	Base1.0 時の動作速度を 0.8 倍した値
Base0.5	最小サイズ	Base1.0 時の動作速度を 0.5 倍した値
Base0.2	最小サイズ	Base1.0 時の動作速度を 0.2 倍した値
Base0.1	最小サイズ	Base1.0 時の動作速度を 0.1 倍した値

５．３．１　各性能評価結果

VPEX3 と VCLB の各制約条件における性能評価結果を報告する．なお，VCLB の評価結果は参考論文[2]に報告されている結果である．次にこれらの各評価結果を ASIC の評価結果を 1.0 とした時の比で表す．面積性能の評価結果を表５．３，表５．４，図５．２，動作速度の性能評価結果を表５．５，表５．６，図５．３，消費電力の評価結果を表５．７，表５．８，図５．４にそれぞれ示す．

表５．３　面積性能（×1000[um2]）

		b14	b15	b17	b18	b19
ASIC	Base1.0	121.4	104.0	309.3	933.6	1804.4
VPEX3	Base1.0	240.3	195.0	601.8	1874.1	3594.2
	Base0.8	244.2	198.4	610.4	1884.7	3609.5
	Base0.5	282.6	204.9	634.2	2020.2	3892.7
	Base0.2	456.6	278.7	807.8	2370.9	4446.0
	Base0.1	427.0	283.9	832.7	2340.0	4447.7
VCLB [2]	Base1.0	274.0	434.0	1237.0	3236.0	6336.0
	Base0.8	499.0	492.0	1467.0	4077.0	8104.0
	Base0.5	679.0	493.0	1488.0	4341.0	8655.0
	Base0.2	1044.0	596.0	2102.0	5801.0	11210.0
	Base0.1	951.0	762.0	2189.0	6089.0	11905.0

表５．４　面積性能比（ASIC の結果を１としたとき）

		b14	b15	b17	b18	b19
ASIC	Base1.0	1.00	1.00	1.00	1.00	1.00
VPEX3	Base1.0	1.98	1.87	1.95	2.01	1.99
	Base0.8	2.01	1.91	1.97	2.02	2.00
	Base0.5	2.33	1.97	2.05	2.16	2.16
	Base0.2	3.76	2.68	2.61	2.54	2.46
	Base0.1	3.52	2.73	2.69	2.51	2.46
VCLB	Base1.0	2.26	4.17	4.00	3.47	3.51
	Base0.8	4.11	4.73	4.74	4.37	4.49
	Base0.5	5.59	4.74	4.81	4.65	4.80
	Base0.2	8.60	5.73	6.80	6.21	6.21
	Base0.1	7.83	7.33	7.08	6.52	6.60

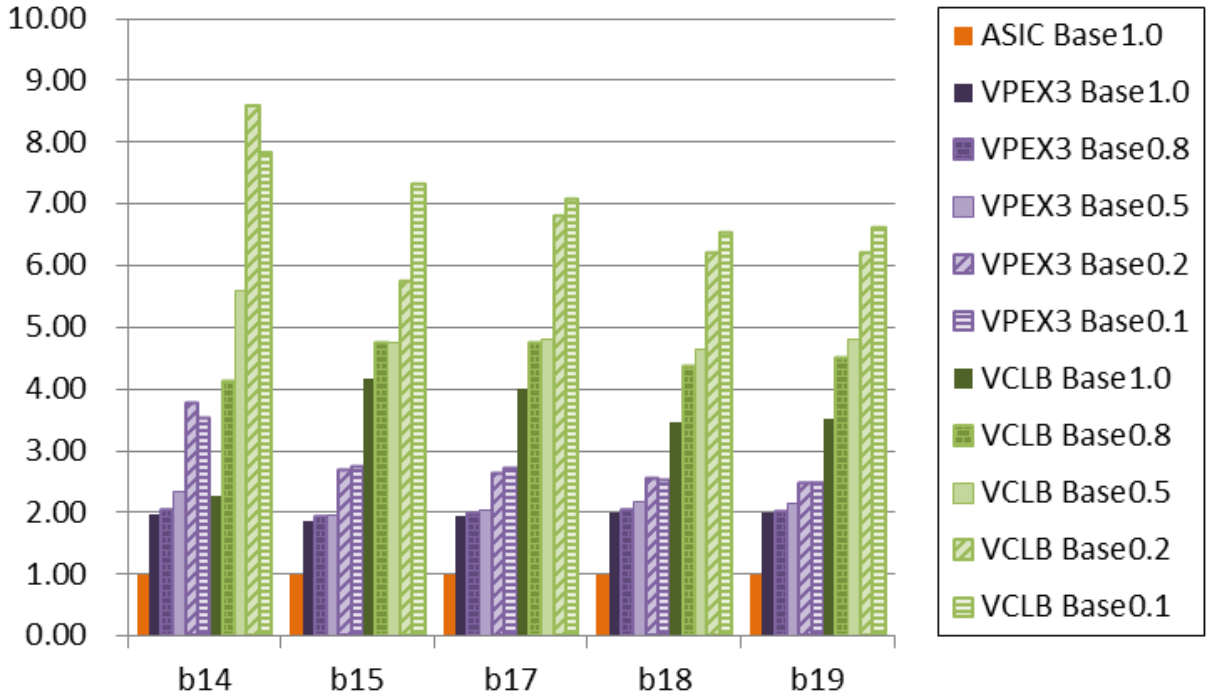


図５．２　面積性能比（ASIC の結果を１としたとき）

表５．５　動作速度性能（単位は[ns]）

		b14	b15	b17	b18	b19
ASIC	Base1.0	29.4	16.2	15.6	29.2	28.9
VPEX3	Base1.0	49.9	31.7	31.7	48.2	48.3
	Base0.8	39.5	24.9	24.8	38.1	38.1
	Base0.5	24.4	15.3	15.3	28.2	26.6
	Base0.2	12.4	8.1	8.3	26.9	26.1
	Base0.1	13.1	8.0	8.1	26.7	25.8
VCLB [2]	Base1.0	21.6	66.9	44.7	53.7	55.4
	Base0.8	13.6	20.7	21.0	29.2	31.4
	Base0.5	10.5	19.2	17.7	28.1	28.2
	Base0.2	11.6	13.2	17.0	36.7	22.1
	Base0.1	12.4	14.4	16.2	37.6	29.4

表５．６　動作速度性能比（ASIC の結果を１としたとき）

		b14	b15	b17	b18	b19
ASIC	Base1.0	1.00	1.00	1.00	1.00	1.00
VPEX3	Base1.0	1.70	1.95	2.03	1.65	1.67
	Base0.8	1.34	1.54	1.59	1.30	1.32
	Base0.5	0.83	0.94	0.98	0.96	0.92
	Base0.2	0.42	0.50	0.53	0.92	0.90
	Base0.1	0.45	0.49	0.52	0.91	0.89
VCLB	Base1.0	0.73	4.13	2.86	1.84	1.92
	Base0.8	0.46	1.28	1.35	1.00	1.09
	Base0.5	0.36	1.18	1.13	0.96	0.98
	Base0.2	0.39	0.81	1.09	1.26	0.77
	Base0.1	0.42	0.89	1.04	1.29	1.02

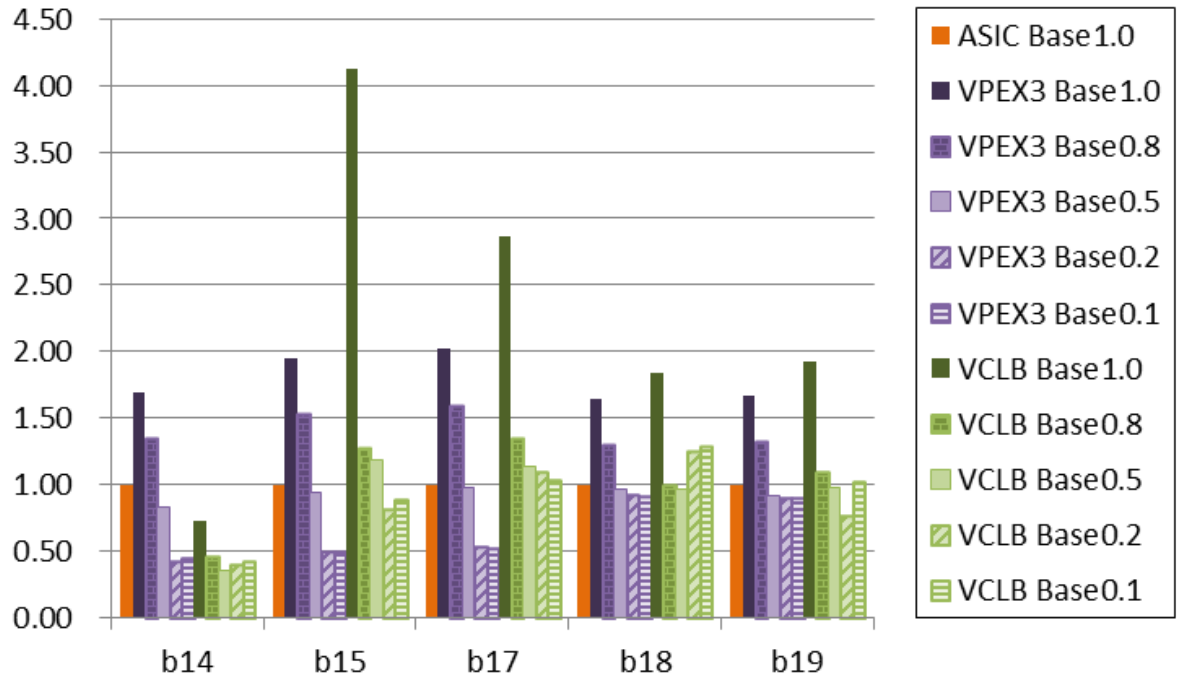


図５．３　動作速度性能比（ASIC の結果を１としたとき）

表５．７　消費電力性能（単位は[mW]，動作速度 100MHz，トグルレート 20%）

		b14	b15	b17	b18	b19
ASIC	Base1.0	11.4	4.7	13.7	31.3	60.5
VPEX3	Base1.0	27.9	8.8	23.1	51.3	99.4
	Base0.8	27.9	8.9	23.1	51.5	99.6
	Base0.5	28.5	8.8	22.8	51.6	100
	Base0.2	33.2	9.9	24.4	51.7	99.9
	Base0.1	32.2	9.8	24.6	51.8	99.9
VCLB [2]	Base1.0	4.8	8.3	25.1	65.8	128.1
	Base0.8	7.3	9	28.2	78.1	157.6
	Base0.5	10	8.9	28.5	80.9	161.5
	Base0.2	15.2	10.2	35.7	96.9	188.5
	Base0.1	13.8	11.7	35.1	96.7	193

表５．８　消費電力性能比（ASIC の結果を１としたとき）

		b14	b15	b17	b18	b19
ASIC	Base1.0	1.00	1.00	1.00	1.00	1.00
VPEX3	Base1.0	2.45	1.87	1.69	1.64	1.64
	Base0.8	2.45	1.87	1.69	1.65	1.65
	Base0.5	2.50	1.85	1.66	1.65	1.65
	Base0.2	2.91	2.09	1.78	1.65	1.65
	Base0.1	2.82	2.07	1.80	1.65	1.65
VCLB	Base1.0	0.42	1.76	1.83	2.10	2.12
	Base0.8	0.64	1.90	2.06	2.50	2.60
	Base0.5	0.88	1.88	2.08	2.58	2.67
	Base0.2	1.33	2.16	2.61	3.10	3.12
	Base0.1	1.21	2.47	2.56	3.09	3.19

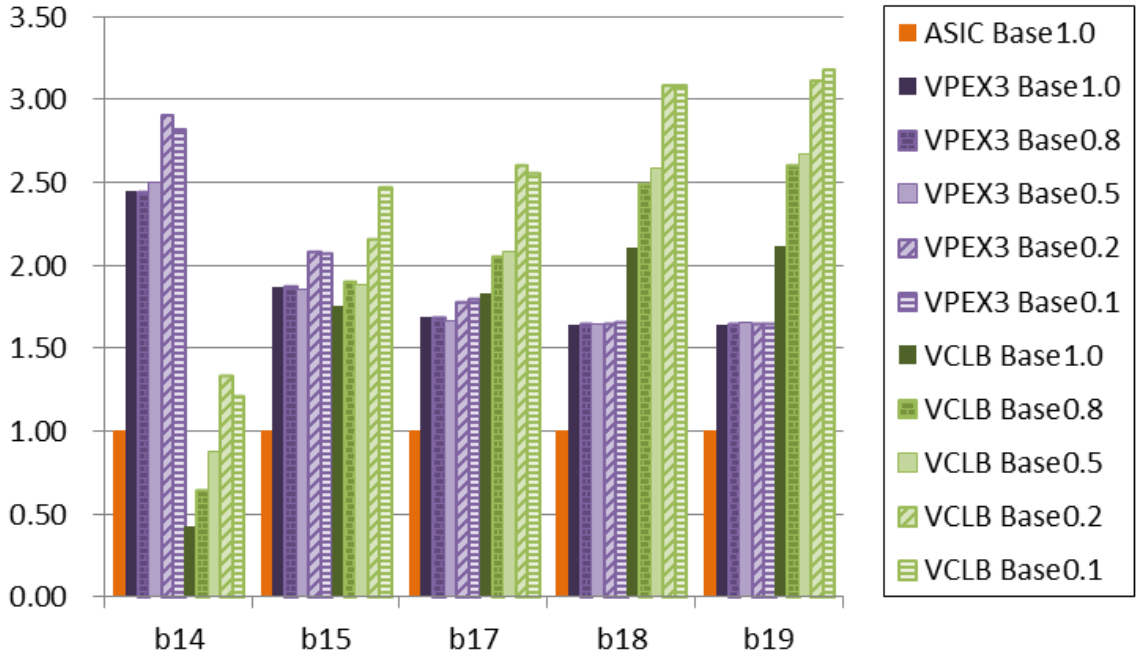


図５．４　消費電力性能比（ASIC の結果を１としたとき）

まず面積性能比に注目する．VCLB は ASIC の 2.2～8.6 倍，平均値で見ると 5.3 倍になっているのに対して，VPEX3 では 1.9～3.7 倍，平均値が 2.33 倍であることが分かる．このことから VPEX3 の方が面積性能に優れた回路を作成できることを示しており，VPEX3 の方が VCLB よりも小面積回路の開発に向いている．

一方で動作速度を比較すると VPEX3 は ASIC の 0.4～2.0 倍であるのに対して，VCLB では 0.4～4.1 と広い範囲に分布していることが分かる．平均すると VPEX3 は 1.09，VCLB は 1.21 となり，VPEX3 はわずかに VCLB よりも動作速度性能に優れていることが分かった．

一方消費電力は b14 とその他の回路で異なる結果が得られた．まず b14 回路について考察する．b14 回路の消費電力比較では VCLB の消費電力は最小面積時では ASIC の 1/2 未満になっており，非常に小さいものとなっている．VPEX3 においても b14 回路の消費電力は ASIC の 2.4～2.9 倍と他のベンチマーク回路と比較しても，非常に大きいものになっている．したがって，b14 回路には VCLB では低消費電力，VPEX3 では高消費電力となる回路構造となっていることが分かる．一方で b14 以外のベンチマーク回路では ASIC に対して VPEX3 が 1.6~2.0 倍，VCLB が 1.8～3.2 倍となっており，b14 を除く他の 4 つの回路の消費電力の平均値は VPEX3 が 1.74 倍，VCLB が 2.42 倍となっており VPEX3 の方がより多くのベンチマーク回路で低消費電力な回路を実現できることが分かった．

５．３．２　動作速度・面積分布評価

ここでは動作速度と回路面積の両方の性能分布について考察する．図５．５はベンチマーク回路に対して表５．４，表５．６に示した５つの制約条件における面積性能比と動作速度性能比の分布を示したものである．　また VCLB におけるベンチマーク回路 b14 の結果だけが他の回路と比べて，速度性能が非常に良いため，その分布を破線で囲んで示している．

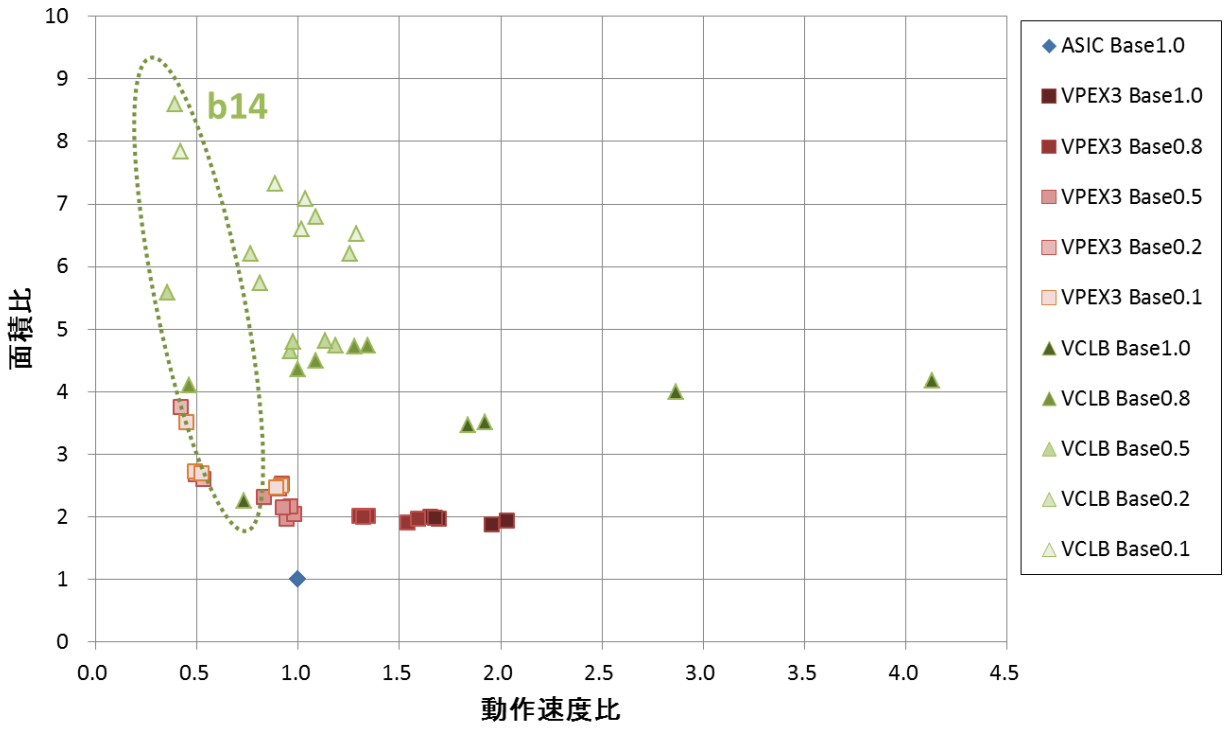


図５．５　動作速度比と面積比のプロット（ASIC を１としたとき）

図の分布は X 軸 Y 軸ともに 0 に近ければ近いほど性能が高い．VPEX3 によって合成された回路面積性能は ASIC の約 2～4 倍の範囲に分布している．また動作速度は約 0.5～2.0 倍の範囲に分布している．

一方で VCLB の面積性能は ASIC の約 3～9 倍に分布しており，動作速度は約 0.5～4 倍に分布している．ここで b14 に対する結果だけは，あらゆる制約条件下においても速度性能が ASIC や VPEX3 よりも良いという結果が得られた．

VPEX3 の分布をまとめると，b14 以外のベンチマーク回路においては ASIC と VCLB の中間に分布しており，一方で b14 回路においては VCLB の方が速度性能面において VPEX3 よりも高速な回路が実現されているという結果が得られた．

したがって，b14 がベンチマーク回路の中では回路規模が小さいことを考慮すると，大規模な論理回路では VPEX3 アーキテクチャは VCLB よりも回路面積・動作速度ともに優れた論理回路を実現できることを示している．

５．３．３　動作速度・消費電力分布評価

ここでは動作速度と消費電力の性能分布について考察する．図５．６はベンチマーク回路に対して表５．４，表５．６に示した５つの制約条件における動作速度性能比と消費電力性能比の分布を示したものである． また前節の結果同様，VCLB におけるベンチマーク回路 b14 の結果だけが他の回路と比べて性能が非常に良いため，その分布を破線で示している．また VPEX3 の b14 の消費電力性能が突出して悪いため，この分布も破線で囲んで示している．

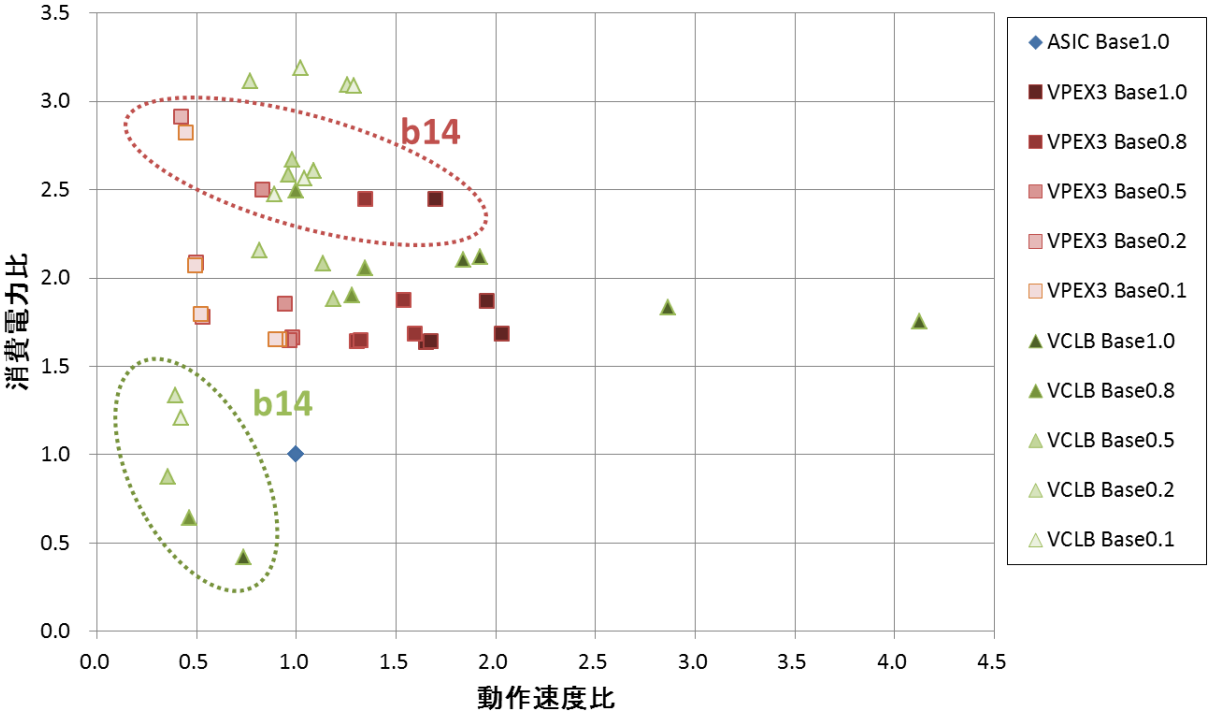


図５．６　動作速度比と消費電力比のプロット（ASIC を１としたとき）

まず b14 の回路について考察する．b14 において VPEX3 の消費電力は約 2.5~3.0 倍となった．その一方で VCLB の消費電力は約 0.5~1.5 倍の範囲に分布している．また動作速度に関しても VPEX4 は 0.5~2.0 であるのに対して，VCLB は 0.5~1.0 倍の，より狭く高速な範囲に分布している．よって b14 の場合においては VCLB の方が速度・消費電力に優れた論理回路が実現できる．

次に b14 以外の回路について考察する．VPEX3 によって合成された消費電力性能は ASIC の約 1.5～2.0 倍の範囲に，動作速度は 0.5~2.0 の範囲に分布している．一方で VCLB の消費電力性能は ASIC の約 1.5～3.5 倍の広範囲に分布しており，動作速度は約 0.5～5 倍の範囲に分布している．したがって，b14 以外の回路では VPEX4 による高性能な回路を実現できている．

したがって，面積速度分布の結果と同様に b14 以外の比較的大規模な回路では VPEX3 の方が高速・省電力の回路がより実現しやすいことが分かった．

５．３．４　まとめ

本章では新しく提案した VPEX3 と元智大学が提案した VCLB の性能比較を行った．その結果より回路面積・動作速度では VPEX3 のほうが優れているという結果が得られたが，消費電力では回路構成によっては VCLB の方が VPEX3 よりも低消費電力の優れた論理回路を実現していることがわかった．

一方で，消費電力の比較は配置後の面積や実際の配線長による配線容量を含めた評価でなければ正当に比較することが難しいため，今回の結果から一概にどちらのアーキテクチャが優れているかという議論をすることは難しい．このような実配線を考慮した消費電力の議論は第 7 章で行う．

第 5 章の参考文献

[1] VDEC, “VLSI Design and Education Center Homepage”, http://www.vdec.u-tokyo.ac.jp/

[2] Mei-Chen Li, Hui-Hsiang Tung, Chien-Chung Lai, and Rung-Bin Lin, “Standard Cell Like Via-Configurable Logic Block for Structured ASICs”, in Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI '08), pp381-386, April 2008.

[3] Hui-Hsiang Tung, Yu-Chen Chen, Da-Wei Hsu, Shih-Jung Hsu, Chen Sin-Yu, and Rung-Bin Lin, “Via-configurable logic block architectures for standard cell like structured ASICs”, Proceedings of the 2009 12th International Symposium on Integrated Circuits (ISIC’09), pp.17-20, Dec. 2009.

[4] Hui-Hsiang Tung, Rung-Bin Lin, Mei-Chen Li, and Tsung-Han Heish, “Standard Cell Like Via-Configurable Logic Blocks for Structured ASIC in an Industrial Design Flow”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol.20, No.12, pp.2184-2197, Dec. 2012.

[5] TSMC, “Taiwan Semiconductor Manufacturing Company Limited”, http://www.tsmc.com/english/default.htm

[6] Scott Davidson, “ITC'99 Benchmark Homepage”, http://www.cerc.utexas.edu/itc99-benchmarks/bench.html

第 6 章　VPEX3 の CAD システムの開発

本章では VPEX3 における配置配線工程と専用の設計支援（CAD : Computer-aided design）システムの開発について説明する．セルベース方式の ASIC のような論理ゲートとその相互配線を利用して論理回路を形成するセミカスタム（semi-custom）LSI の場合，限られたリソース(配置可能な領域の広さ，あるいは配線の長さや本数)で効率の良い配置配線を実現するためにコンピュータ（Computer）によるセルの配置位置や配線経路の最適化を行うことが必要不可欠である.そしてこれは Mask Programmable Device （MPD）でも同様である.

しかしながら，VPEX3 ではセル（＝LE） がタイル状に整列して配置される必要があるため，従来のセルベース方式 ASIC 用の CAD システムを利用して配置最適化を完了させることができない. また配線処理においてもメタル配線層が固定されており，ビアの有無のみで配線経路を形成するものであるため，ASIC 用の CAD システムのみで配線経路最適化を完了させる事は不可能である．FPGA 用の CAD システムとして VPR[1]と呼ばれる配置配線最適化ツールが存在するが，これはアイランドスタイル用の配置配線最適化ツールであるため，VPEX3 で検討しているメッシュ・ジャンパー配線構造に利用することが難しい．また他の VPSA アーキテクチャにおいても，各研究機関はオープンソースなどの容易に利用できる形態によって，これらのアーキテクチャに則った CAD システムを提供しておらず，MPD の開発に利用することができる CAD システムは存在していない．したがって VPEX3 で大規模な論理回路を設計し，レイアウトを自動生成する環境を構築する必要がある.

そこで，本研究では「LE アレイ状配置」「メッシュ・ジャンパー配線」に対して最適化を行い，配置配線結果をビア座標として出力することが出来る VPEX3 専用の CAD システムの開発研究を行った.

６．１ 設計フローチャート

図６．１に VPEX を用いてデジタル LSI を設計する際に必要となるフローを示す．このフローでは設計済みのハードウェア記述言語（HDL : ）で設計されたレジスタ転送レベル（RTL : Register ransfer level）で記述された論理回路が最初に与えられるものとして構成されている．ネットリストは論理合成用の設計自動化（EDA : Electronic Design Automation）ツールである米シノプシス（Synopsys）社の Design Compiler[2]を使用して作成されることを想定している．論理合成フローは前章の性能評価フローと同様の流れで実行される．したがって本章での説明は割愛する．論理合成までのフローは基本的にセルベース ASIC と同様の設計環境を用いて実行することができる.

次に配置最適化および配線最適化を実行する．本フローでは開発を行った配置・配線プログラムによって「フロアプラン処理」「配置処理」「配線処理」「レイアウトデータ変換」が順次実行される．各フローを経て， VPEX3 のカスタム層である第 1～3 ビア層の座標情報が決定され，GDSII 形式（GDSII stream format）[3]のファイルとして出力される．この GDSII 形式のデータをマスター層にあたる LAB のレイアウトと合わせることで，目的の論理回路を VPEX3 によって形成したレイアウトが完成する.

次に開発した CAD における各工程について詳細に述べる.

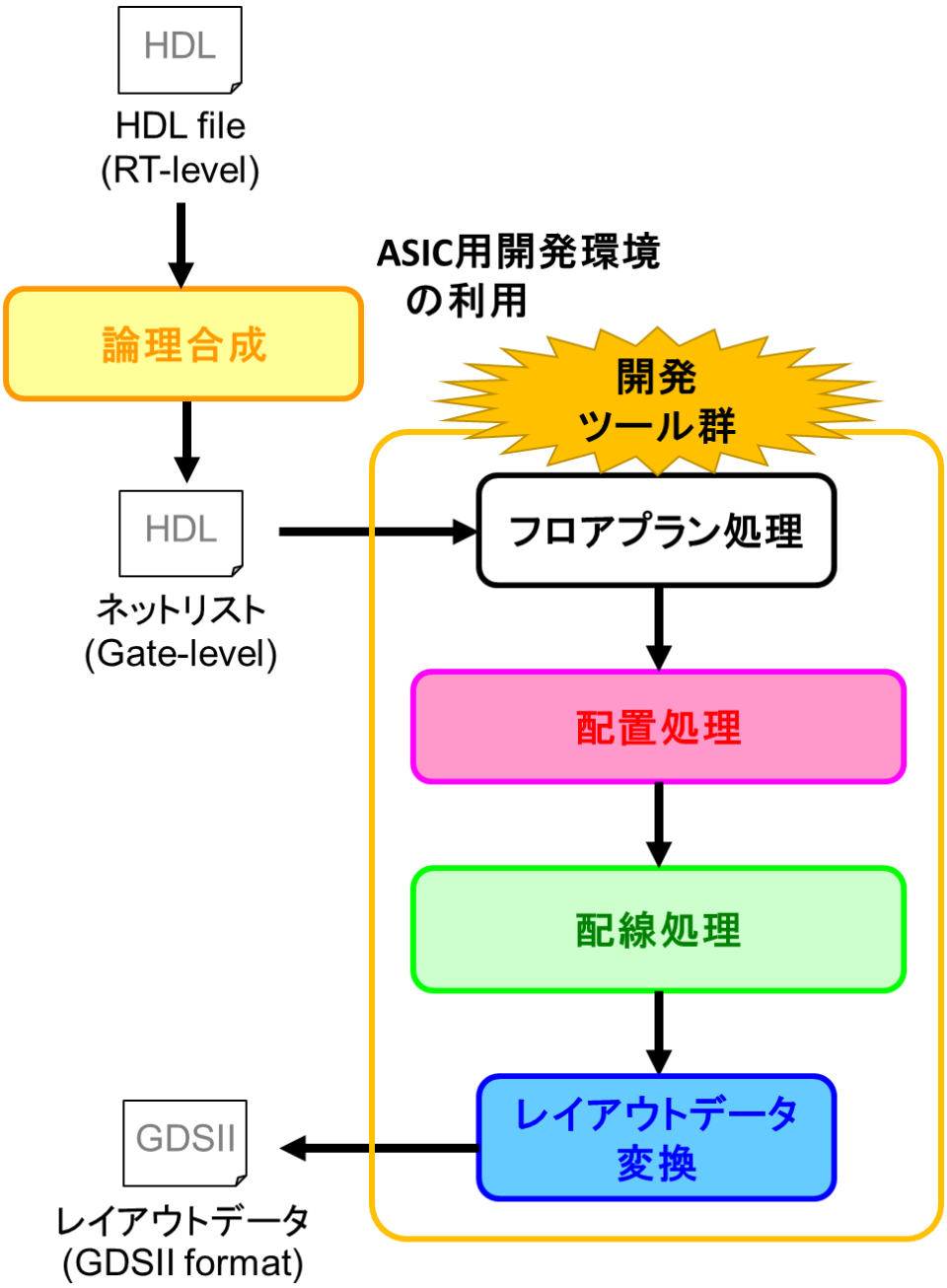


図６．１　設計のフローチャート

６．２　開発ツール群の詳細説明

開発した CAD システムは図６．１に示すように 4 つの工程に細分化される．1 つはフロアプラン工程（FloorPlanning），2 つ目は配置工程（Placement），3 つ目は配線工程（Routing），4 つ目がレイアウトデータ変換工程である．なおスタンダードセル ASIC には配置工程と配線工程の間にクロックツリー合成（CTS：clock-tree-synthesis）が入るが，VPEX3 アーキテクチャでは FPGA 同様に組み込みのクロックツリー領域を設けているので、この工程は存在しない．各工程を順番に解説する．

６．２．１　フロアプラン工程

フロアプラン工程は後の配置工程に用いる配置領域の定義や入出力の座標定義を決定するための工程である. この工程では図６．２に示すようにネットリスト(Net list)と呼ばれるゲートレベル(gate level)の HDL のほかに「配置範囲制約ファイル」「入出力座標定義ファイル」を作成する必要がある.

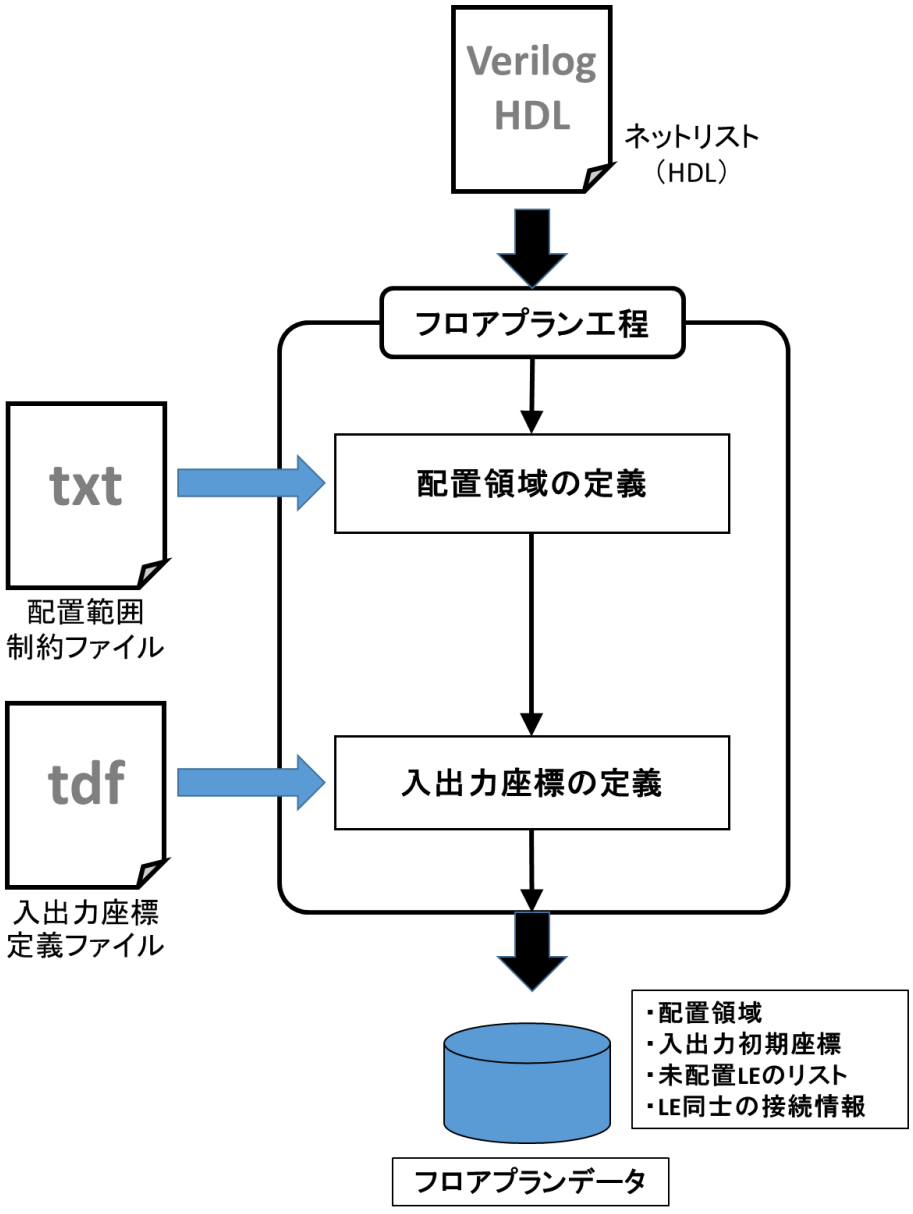


図６．２　フロアプラン工程の詳細フロー

配置領域は図６．３に示すような長方形を想定しており，ユーザーが「縦方向の LE 数」「横方向の LE 数」を「配置範囲制約ファイル」に定義する．このときの縦方向の個数と横方向の個数の積が配置領域の「最大 LE 配置数」となる．ここではネットリストに記載されている総セル数（LE 数）よりも最大 LE 配置数が大きくなるように配置領域を設定する必要がある.

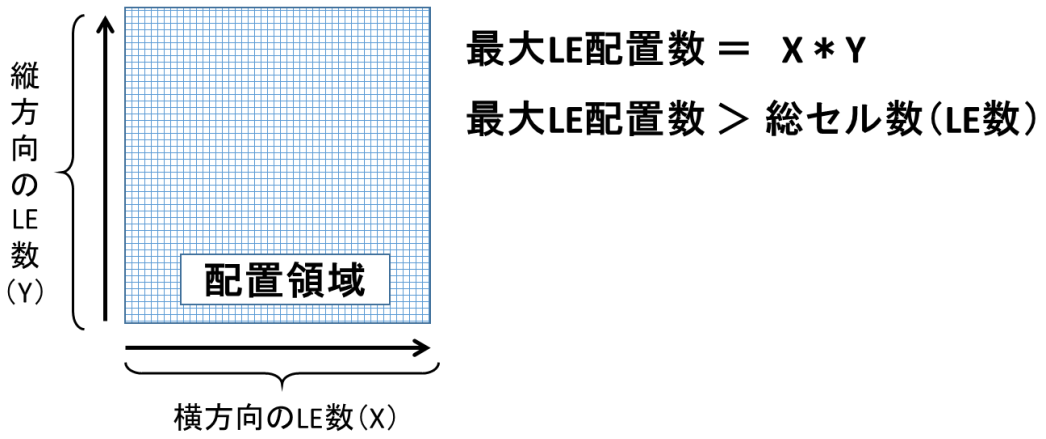
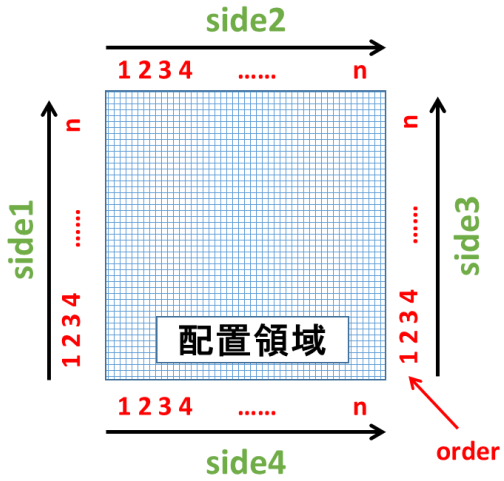


図６．３　配置領域の定義と制約

また入出力の初期位置などもこの工程で決定する．本開発 CAD システムでは入出力ポートの初期位置は ASIC の配置配線ツールにも使用されている TDF 形式のファイルを作成し，それを反映させる．TDF 形式では-side によって配置領域の四方を，-pin_name によって入出力の名称を，-order によって相対的な座標をそれぞれ指定し，任意の位置に各入出力を配置する．この時の座標は図６．４のような形式になっている．




```
set_pin_physical_constraints -side 1 -pin_name {“clk”}  –order 1
set_pin_physical_constraints -side 1 -pin_name {“IN1”}  –order 2
set_pin_physical_constraints -side 1 -pin_name {“IN2”}  –order 4
set_pin_physical_constraints -side 2 -pin_name {“OUT1”} –order 1
set_pin_physical_constraints -side 2 -pin_name {“OUT2”} –order 3
                              .
                              .
                              .
```

図６．４　入出力座標ファイルの中身（TDF 形式）

６．２．２　配置処理

配置処理ではセルをフロアプラン工程で定義した配置領域に割り当てていく工程である．今回開発した専用 CAD 環境における配置処理の処理フローを図６．５に示す．専用 CAD システムの配置処理は「配置最適化」「正規化」「LE ピン座標割り当て」の 3 フェイズによって構成されている．

「配置最適化」ではランダムにセルを配置するのではなく，後の配線工程で効率のよい配線経路を形成できるように LE 間の接続情報から最適な座標を決定する．また最適化後の配置結果はタイル状の配置形状ではない．そこで配置結果を VPEX3 の配置アーキテクチャのように整列させる「正規化」が行われる．この 2 つの工程を経てタイル状に並べられた LE の配置領域の中で，セルが実際に割り当てられる座標が決定される．最後に後の配線工程にデータを引き渡すため，LE 上の入出力ピンの座標を割り出す「LE ピン座標割り当て」が実行される．

各処理の詳細について説明する．

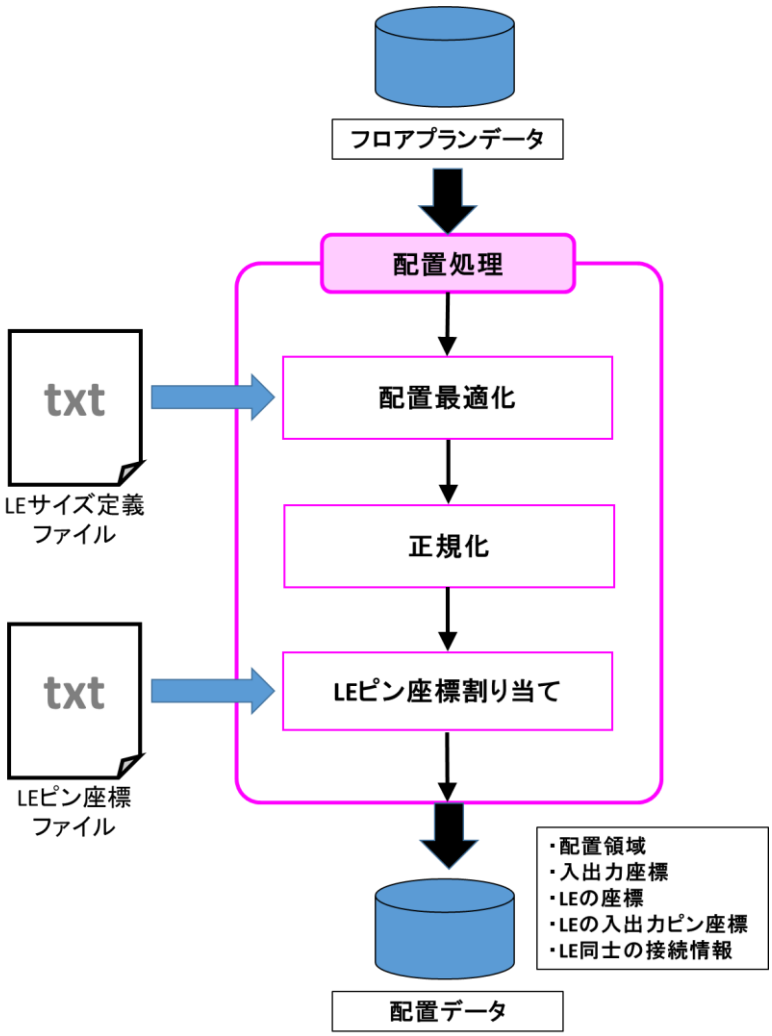


図６．５　配置フロー

（1）配置最適化

配置最適化ではフロアプランニングで設定を行った「配置領域」上の最適な位置にセルを割り当てる．これはアルゴリズムによって実行される．このような配置アルゴリズムを 1 から作りこむことは難しく，非常に時間のかかる作業であるため，今回開発した CAD システムでは ASIC 用の自動配置ツールとして公開されている Capo[4,5]を利用している．Capo はミシガン大学の研究室で開発された自動配置ツールであり，最適化には Min-Cut アルゴリズム[4,5,6]を用いている．また後の配線工程における配線成功率を向上させるため，素子を置かない空白スペースを集中させずに配置するアルゴリズム[4]も有している．Capo は ASIC 用の配置配線ツールではあるため，このソフトウェア単体では VPEX3 の配置工程を完了させることはできないが、配線のしやすい最適なセル座標を見積もる目的では十分に活用できると考え，今回の配置最適化に利用している．

Min-Cut のアルゴリズムは図 6． 6 に示すような手順によってカットラインを横切るセル間の総配線数が少なくなる配置結果を導くアルゴリズムである．まず配置領域を分割し，各セルを均等に割り振る．セルの割り振りでは分割線を横切る配線をプラス 1 と横切らない配線の個数をマイナス 1 としてカウントし，合計数値が最も大きいセル同士を交換する．これを任意回数繰り返し，最終的に最も合計利得の小さくなった（カットラインを横切る総配線数が少なくなった）配置結果を採用する．セルの交換を任意回数行った後は領域をさらに分割し，新たなカットラインに対して同様にセル交換を実行していく．この動作を繰り返すことで各セルの配置座標を決定する．

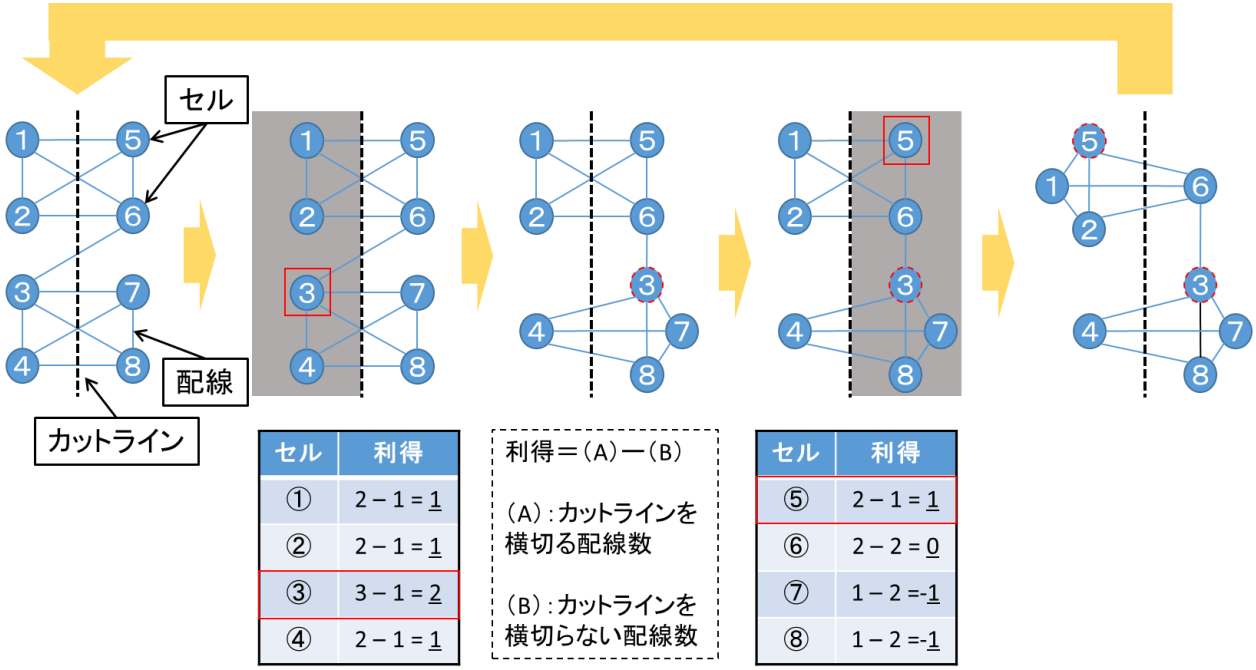


図 6． 6　MinCut アルゴリズム[6]

Capo の入力ファイルは独自の形式を採用しており，Verilog-HDL 形式のネットリストをそのまま与えることができない．そこでフロアプランによって形成した「配置領域」「セルサイズ」「配線情報」「初期配置」の 4 つデータを対応フォーマットにコンバートする必要がある．配置最適化ではこの入力ファイル生成器を作成した．図 6． 7 に配置最適化における処理フローを示す．この処理工程では「ファイル

生成器」によって Capo の入力ファイルを生成し，Capo による最適化を実行する．その結果を「ファイル解析器」で解析することよってセルの最適な配置結果を得る．

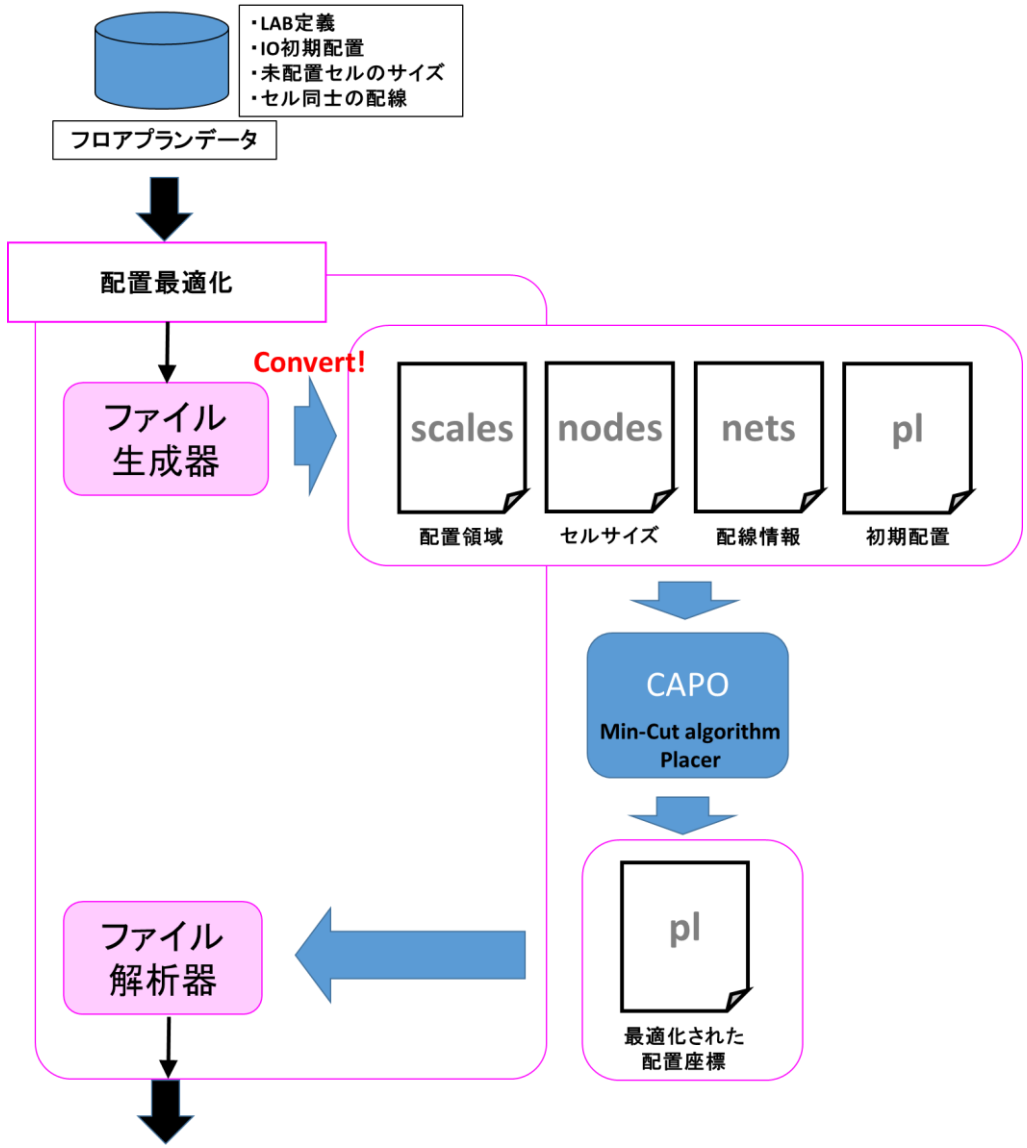


図６．７　配置フロー

（2）正規化（Legalize）

VPEX3 は LE がタイル模様のように並べられているため，図６．８（a）のような格子状グリッドの中に LE が揃えられるような配置結果となる．しかし ASIC 用の配置ツールを使用して配置処理を行った場合，その配置結果は図６．８（b）のように格子状グリッドを跨ぐようにセルが置かれた状態になる．

正規化では図６．８（c）のように，複数の LE と重なってしまったセルを移動させ，座標を修正することで各セルと LE が重なる様に整列させる．正規化のアルゴリズムは様々な手法があるが，本システムではセルの左方側の一番近い LE に合わせこむようにセルを左側に移動させる左詰めアルゴリズムを採用している．

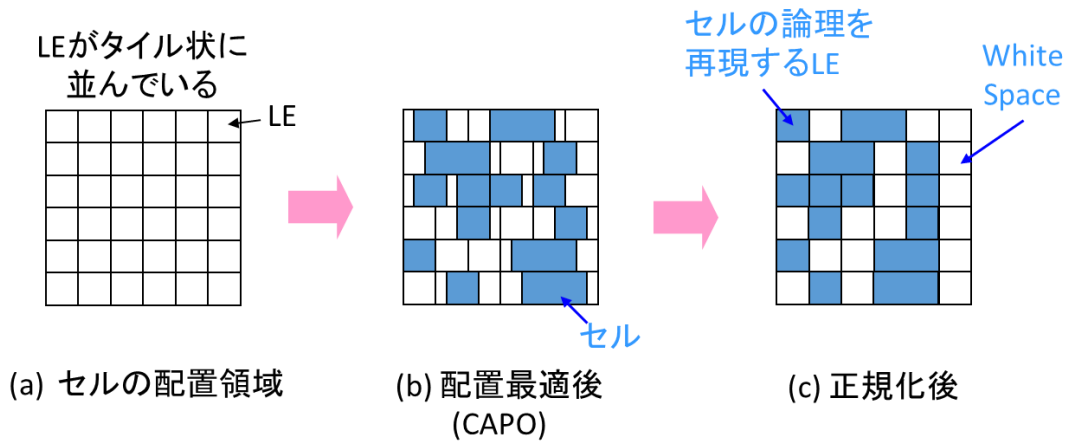


図６．８　配置結果の正規化

（３）LE ピン座標割り当て

セルの論理を割り当てる LE の座標が明らかになった後に，配線トラックへのピン割り当て処理を実行する．この工程は図６．９に示すように各 LE の座標と割り当て論理毎の入出力ピン定義より決定される．この工程では「LE ピンの座標ファイル」が使用される．このファイルにはセル毎の入出力ピンの配線トラック番号やオフセット座標が定義される．この工程を終えることで，接続すべき入出力トラックの座標が明確になる．配置処理は以上で完了する．

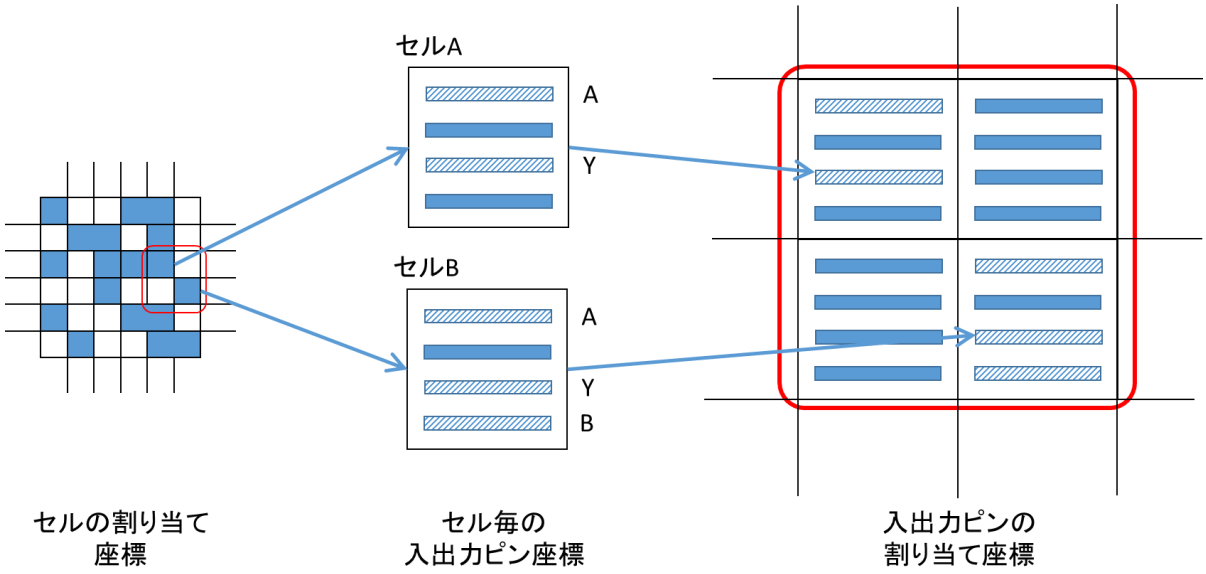


図６．９　LE の入出力ピンの割り当て

６．２．３　配線処理

配線処理ではネットリストに記された各入出力ピン同士の接続情報と，配置処理によって得られた LE の入出力ピンの座標を用いて，メッシュ・ジャンパー配線構造上に最適な経路を形成する．今回開発した CAD システムでは図６．１０に示す３つの工程を経て，目的の配線経路およびそれを実現するためのビア座標を形成する．各工程は配線経路を決定する「経路最適化」．各配線をメッシュトラックに割り当てる「トラック割り当て配線」．トラックへの割り当て情報からビアを割り当てる座標を抽出する「ビア割り当て」によって構成される．それぞれの詳細について説明していく．

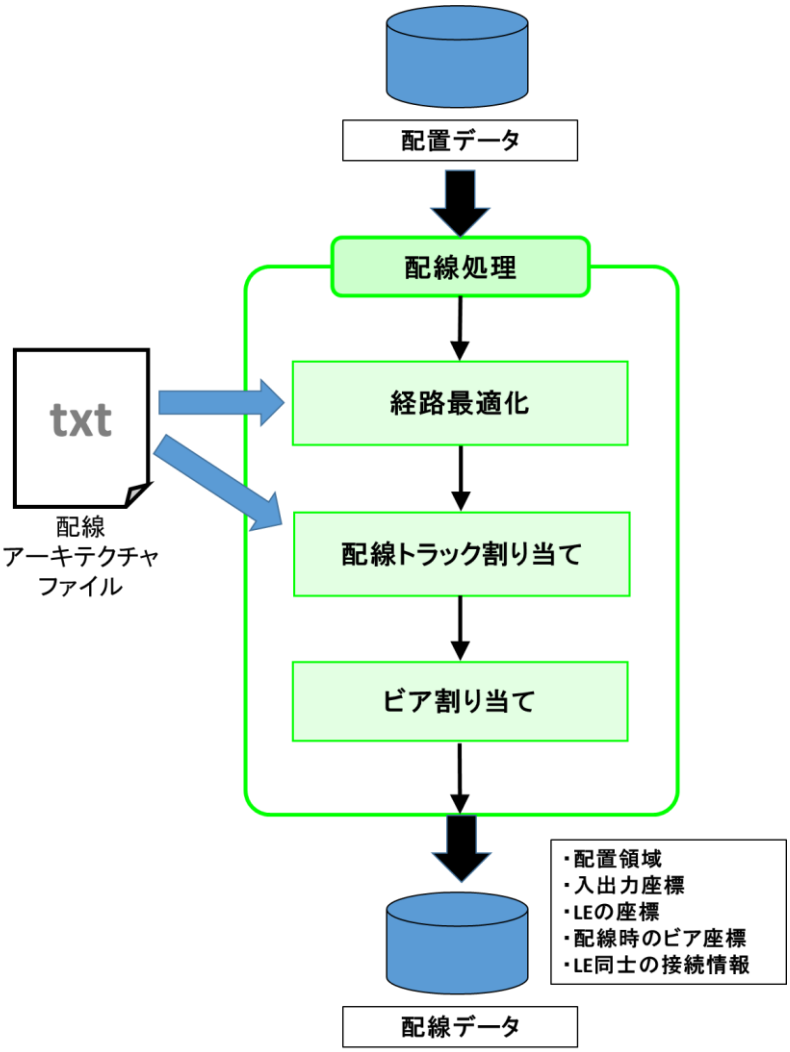


図６．１０　配線処理フロー

（１）経路最適化

経路最適化では，配置領域の分割とブロック座標の定義を行う．まず初めに図６．１１（a）に示すように配置領域を小さなブロックに分割し，各入出力ピンの属するブロックを決定する．その後，図６．１１（b）に示すように LE ピンを分割したブロックの座標情報に変換する．この座標情報をブロック座標と呼称する．これによって各配線の接続先となるブロック座標が定義される．

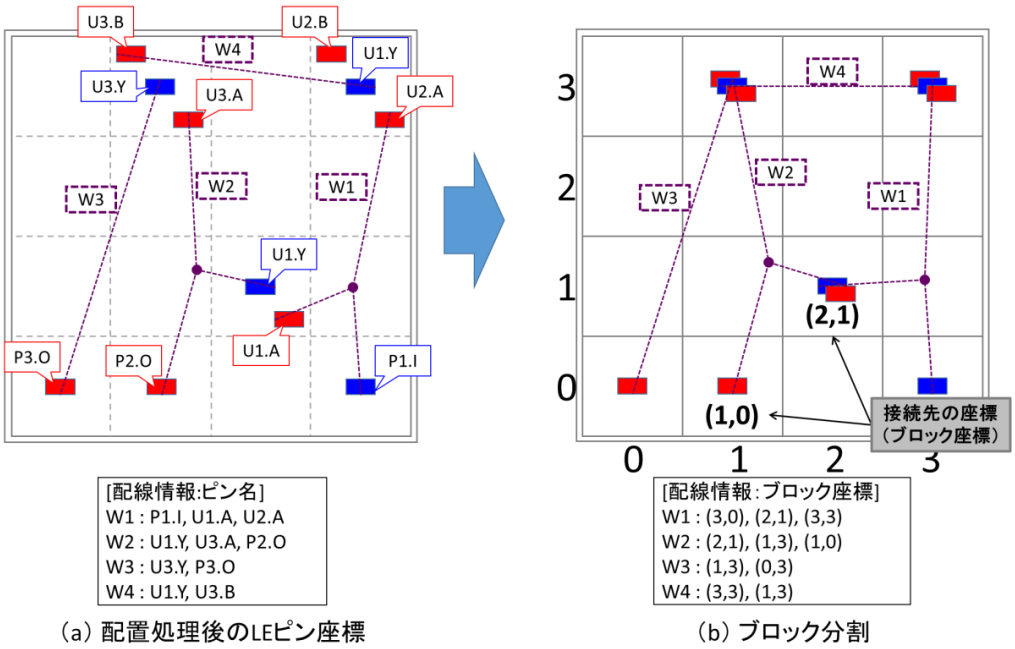


図６．１１　ブロック分割と配線するブロック座標の定義

次に各配線のブロック座標から，それらを接続するための最適な配線経路を定義する．この配線経路は必ずＸ軸方向またはＹ軸方向にのみ直線状に定義することが可能で，斜めに方向に配線することはできない．また配線経路は互いのブロック以外に，間にあるいくつかのブロックを経由して形成されている．したがって，（0,0）座標から（2,2）座標に向かって配線経路を形成する場合，図６．１２のように（2,0）あるいは（0,2）を経由し，方向転換されることで配線経路が形成される．

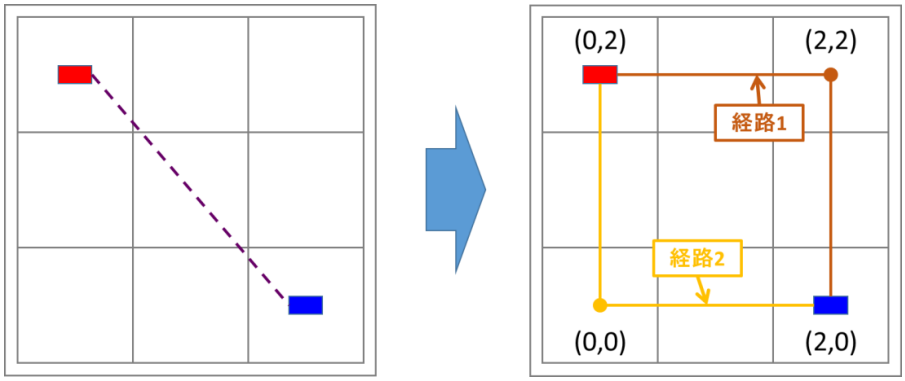


図６．１２　配線経路の形成

このような２つのブロック座標を繋ぐために方向転換を１度しか行わない配線は特に「Ｌ字型配線経路」と呼ばれ，すべてのブロック座標をＬ字型配線経路によって数珠つなぎにすることで形成した配線経路のことを直線最小全域木（RMST : Rectilinear Minimal Spanning Tree）と呼ぶ．図６．１３（a）にブロック座標（ノード）が５つある配線における RMST を示す．この例では１ブロックの配線長を１としたときの総配線長が 12，Ｌ次型配線が５つ存在する．したがってこの配線を再現する場合に，12×１ブロック分の総配線長の配線と５個のビア接続が必要となる．今回与えられた５つのブロック座標を

繋ぐ経路パターンの中で，図６．１３（a）の RMST は最小の総配線長をもつ経路パターンではない．最小の総配線長となる経路パターンの一つは図６．１３（b）に示したような形状が該当する．このような配線を直線最小スタイナー木（RSMT : Rectilinear Steiner minimal tree）と呼ぶ．経路最適化ではまず RSMT を作成することが良い配線経路を導くうえで重要となる．しかしながら，すべての配線に対して RSMT を求めることは難しく，ノードが 10 を超える場合などでは RMST によって経路の形成が行われる．

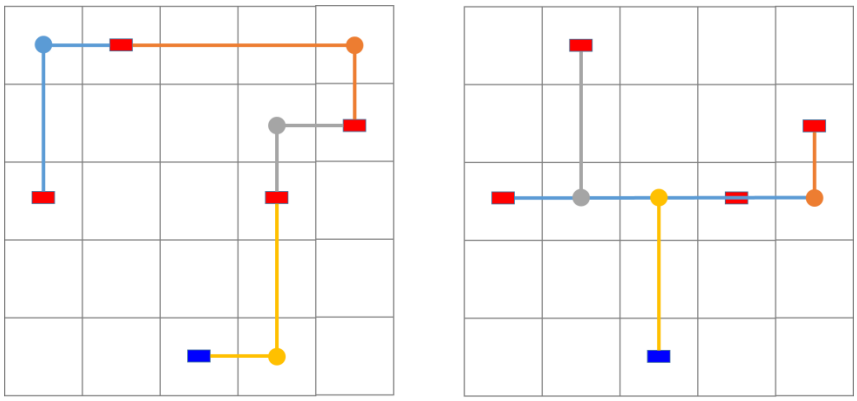


図６．１３　配線の接続先ブロック座標が 5 つの場合の経路パターンの例

次に一つのブロックを経由する配線数が配線アーキテクチャファイルより与えられた「最大トラック数」を超えないように配線経路を修正していく．図６．１４に例を示す．(a) に注目する．この例では最大配線トラック数の制約が４であるにも関わらず，ブロックを横切る配線が５本になっている個所が 2 か所存在する．配線経路の修正ではこの 5 本の配線のうち一つを選択し，最大トラック数を超過した配線経路を通らない新しい配線経路を形成する．修正例を図６．１３（b）に示す．この修正を繰り返すことで，トラック数の制約を満たす２次元的な配線経路が形成される．これが最適化された配線経路となる．

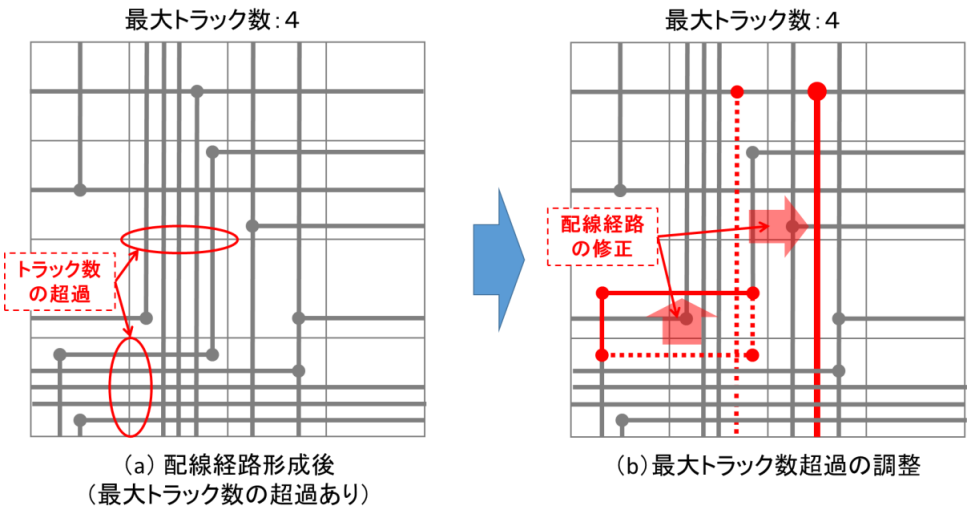


図６．１４　配線経路の修正

この経路最適化には既に様々なアルゴリズムが提案されており[7-16]，また配置最適化アルゴリズム同様に経路最適化アルゴリズムを 0 から開発・実装することは非常に困難である．そこで本 CAD システムでは配線経路の形成に，オープンソースの配線ツール Fairly Good Router（FGR）[7-10]を使用した．

FGR は 2007 年に行われた ISPD のグローバルルーティングコンテスト[17]において 2D（平面）構造のグローバル配線最適化部門で最も高い評価を得たソフトウェアである．この 2D 構造配線は 2 層の配線層において片方の層を垂直方向用，もう片方を水平方向用と仮定して配線する形である．VPEX3 に用いられているメッシュ・ジャンパー配線構造は水平/垂直 2 方向に 1 層ずつの配線構造であるため，これは 2D 構造配線にあたる．したがって FGR は VPEX3 の配線経路最適化に用いるグローバルルーティングとして非常に適したアルゴリズムを備えていると考え，今回選定した．

FGR は Labyrinth[13]と呼ばれるフォーマットを入力とし，BoxRouter[11]と呼ばれるフォーマットで出力される．したがって配置情報から Labyrinth 形式の入力ファイルを出力するプログラムと BoxRouter 形式のファイルから配線経路を解析するプログラムが必要である．

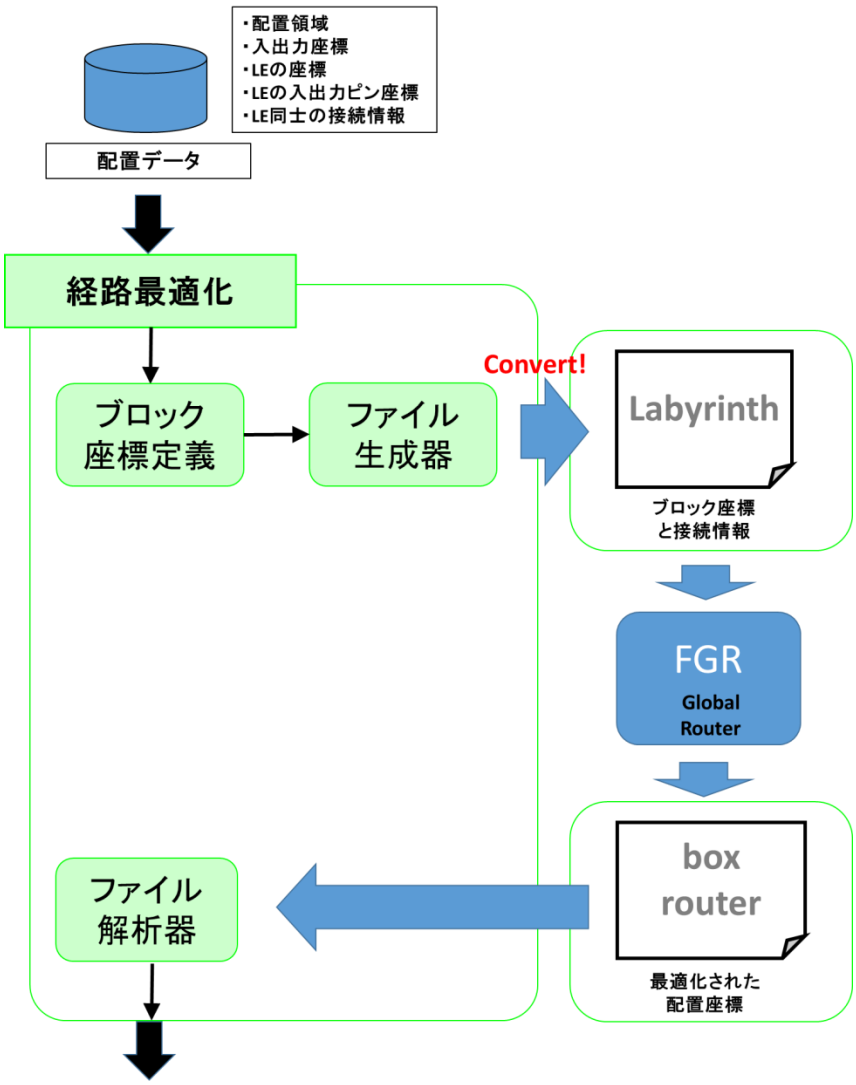


図６．１５　ファイル変換工程

（２）トラック割り当て処理

経路最適化によって各配線の経路が決定した後は配線トラックへの割り当て処理を行う．このトラック割り当て処理では，まず初めに図６．１６に示すように配線経路を水平方向と垂直方向に分解する．分解された経路は線分となり，この線分は図のように始点と終点をもつ１次元の線分となる．これでトラック割り当ての前処理が完了する．

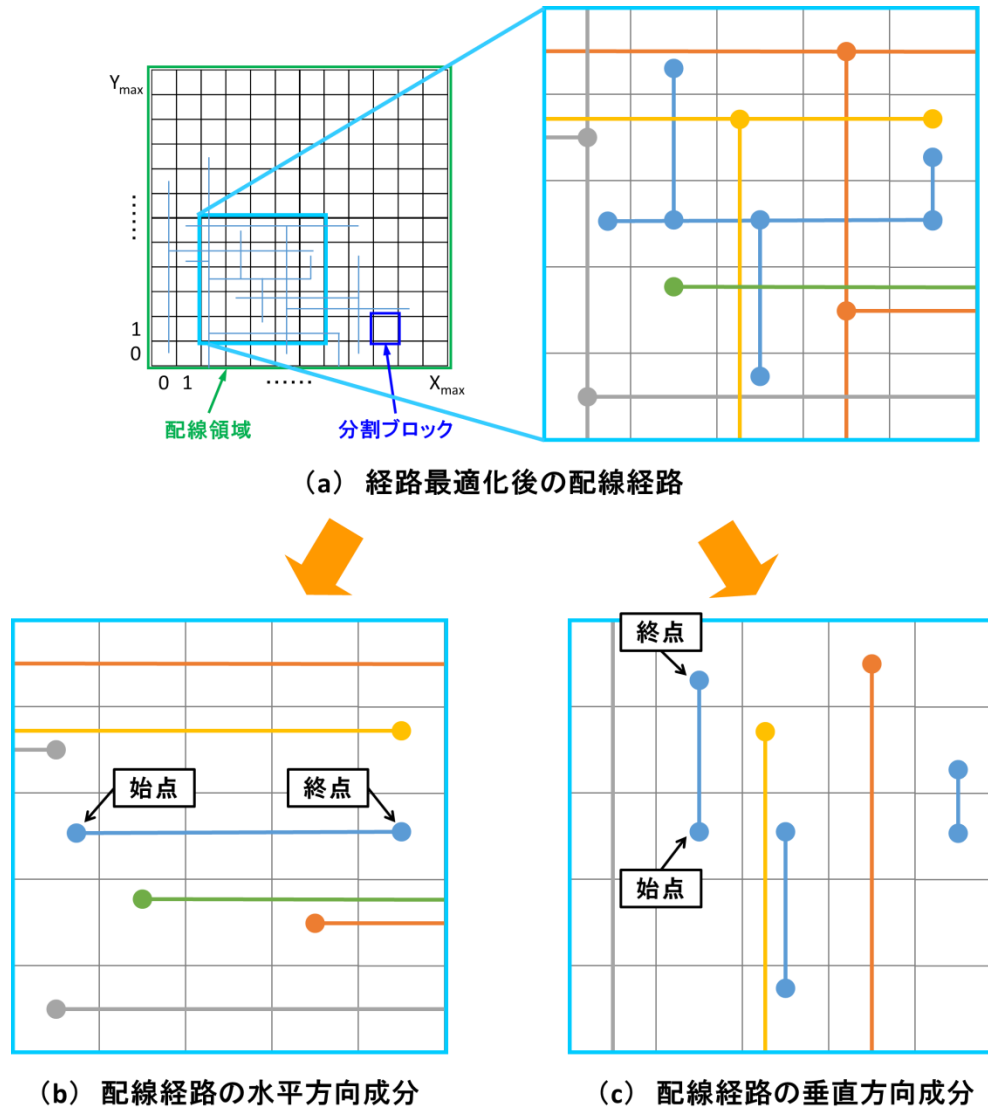


図６．１６　配線経路の分割と始点・終点の抽出

次に線分をメッシュ・ジャンパー配線のトラックに割り当てていく．この処理は２つのフェイズより構成される．第１の走査探索フェイズでは，ブロック座標（0，0）からブロック座標（X_{max}，Y_{max}）まで「線分の始点」を探す．線分の始点を見つけた場合に第２のフェイズであり「割り当て可能トラック」の探索フェイズに入る．割り当て可能トラックの探索では始点から終点までの配線トラックの「未割り当て/割り当て済」情報を参照する．そして１列目のトラックに配線の割り当てが可能であるかどうか．始点座標から終点座標までの全ての１列目トラックを調査する．途中で割り当て済みのトラックが発見

された場合には 2 列目の調査に移行する．これを割り当てが可能な N 列目トラック群を発見できるまでに探索を続ける．図６．１７の例では 3 列目のトラック群が配線の割り当てが可能なことを発見している．配線トラックをすべて調べ，すべての列に対して配線割り当てが実行できない場合は配線失敗となる．

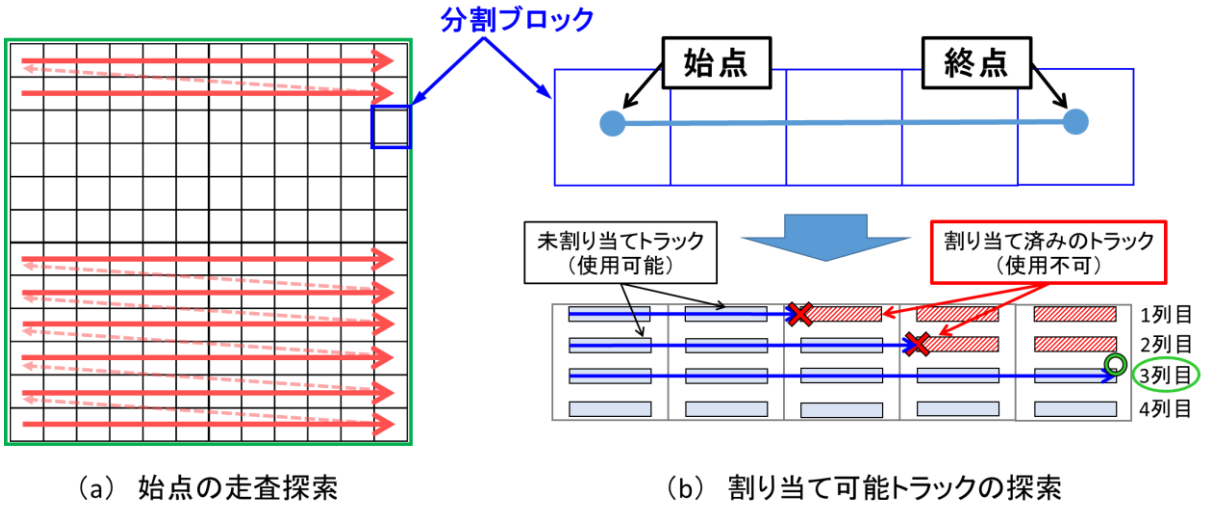


図６．１７　各配線のトラック割り当ての工程

このようにして，水平方向の割り当てが完了した後は，同様にして垂直方向の割り当てを開始する．両方向のトラック割り当てが完了し，失敗した線分が１つも存在しない場合に配線割り当て処理が成功となる．成功した場合は次のビア座標割り当て処理に移行する．

（３）ビア座標割り当て処理

ビア座標割り当てでは，各ビア（VPEX3 では第 2，3 ビア層）の座標を配線結果より抽出する．この処理で抽出するビア座標は LE 上でメッシュ配線トラックを接続するメッシュ接続ポイントと，異なる LE 間を跨ぐためのジャンパー接続ポイントの 2 種類のビアの有無を分析し，各接続ポイントをビアの物理座標に変換する．図６．１８（c）はトラック割り当て後の結果（a）（b）からメッシュ接続とジャンパー接続のポイントを分析した結果を示している．また各ビアの座標は「ビア座標変換用定義ファイル」を参照して算出される．この定義ファイルには LE 上の各ポイントに対応するビア座標が定義されている．したがって，対象としている LE の座標と定義ファイルに定義されたポイントの対応するビア座標からビアの座標が判明する．

ビア座標の割り当ては図６．１８（d）のように LE 単位で行なわれる．最初に座標(0,0)の LE に対してビア座標割り当てを行い，次に座標(1,0)，座標(2,0)，・・・，座標(Xmax,0)と X 軸方向を処理していく．その後は座標(1,1)の LE から座標(Xmax,1)の LE まで X 軸方向を順次処理していく．これを（Xmax,Ymax）までの全ての LE に対して実行する．

この工程により，配線網を形成するために必要となるビアの座標の位置が判明する．メッシュ・ジャンパー配線の接続が完了した後に LE の入出力ピンと配線トラックの接続を行う．図６．１９に示す

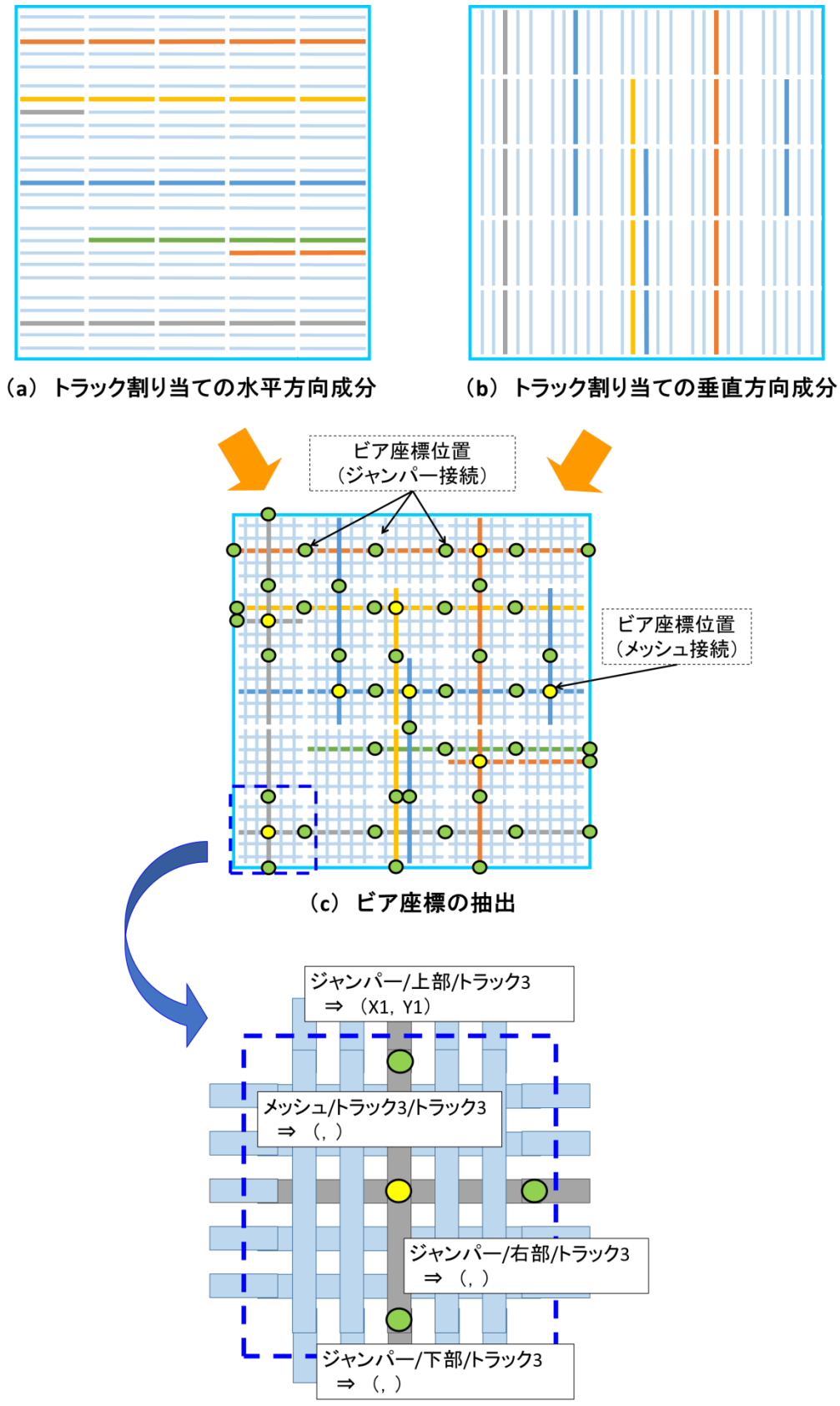


図６．１８　トラックの割り当て情報を用いたビア座標割り当て処理

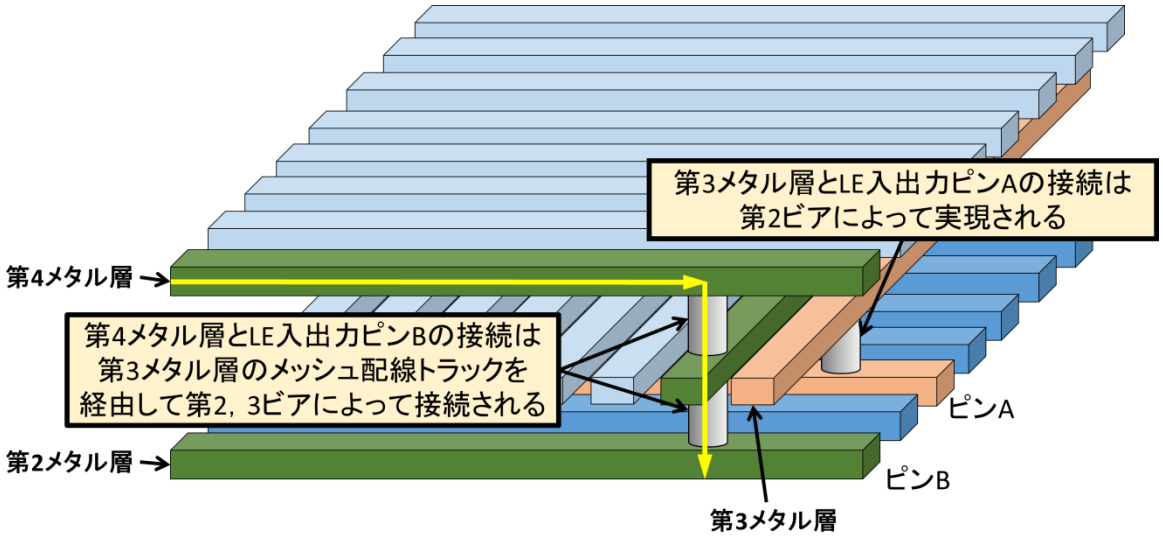


図６．１９　LE の入出力ピンとの接続

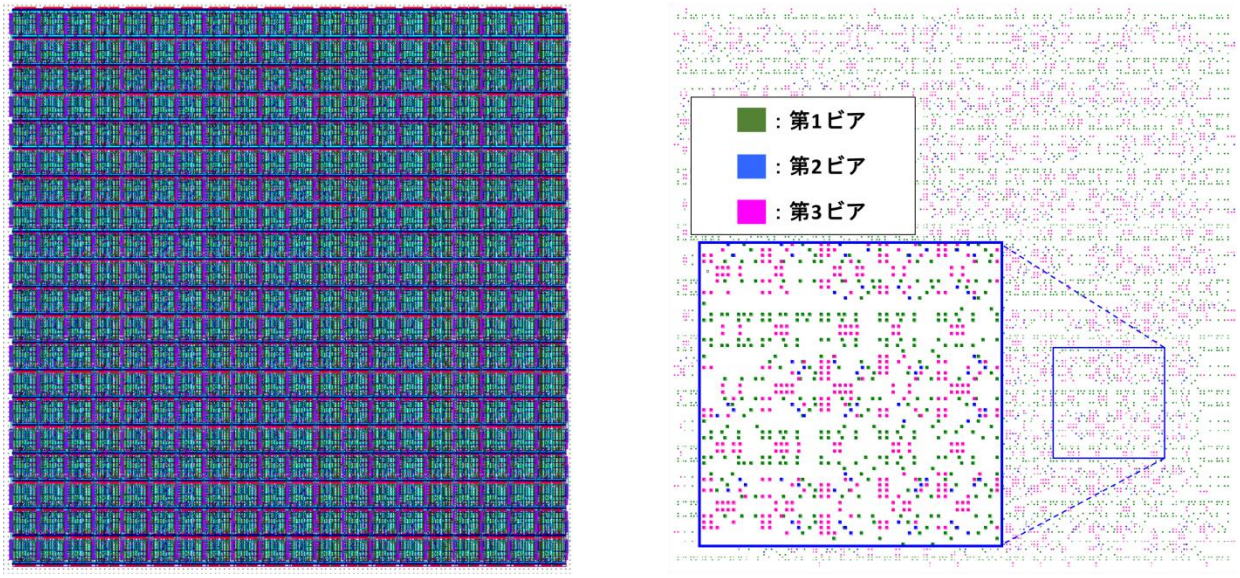
第 3 メタルに形成した配線を LE の入出力ピンとつなぐ場合は，第 2－第 3 メタル層間にある第 2 ビア層によって短絡させることで接続が完了する．一方で第 4 メタル層に形成した配線を LE の入出力につなぐ場合に関しては第 3 メタル層を経由する必要がある．したがって，このとき第 3 メタル層の配線トラックがすべて使用されている場合は，トラックが割り当て処理となる．

問題なくすべての配線と入出力を接続した後では，先ほどと同様にビア座標定義ファイルを参照しながら各ビアの座標を定義していく．以上で配線処理が完了する

６．２．４　レイアウトデータ変換工程

配線と入出力の接続が失敗なく終了し，全てのビア割り当てが完了したあとは，その結果を GDSII 形式のファイルに出力する．GDSII 形式とはレイアウトデータの保存用に利用されているバイナリフォーマットである．オブジェクトの｛タイプ，レイヤ番号，座標，サイズ，向き｝などをバイト単位で表現する．今回開発した GDSII 形式出力プログラムではビアオブジェクト層番号，形状などを Boundary 型のデータ構造で表現し，ビアの配置座標はオブジェクトを配置する SREF 型で表現する．以上の工程を経て第 1～3 層までのビアレイアウトパターンを作成する．

最後に CAD システムを用いてレイアウトを実際に作成した結果を示す．CAD システムを使用して VPEX3 に対応した LAB とビア座標を図６．２０に示す．回路は 8bit×8bit 乗算器を用いた．図（a）は VPEX3 の LAB を示しており，400 個の LE を縦 20 横 20 にアレイ状配置したものである．図（b）は第 1 ビア，第 2 ビア，第 3 ビアのみを表示した結果になっており，400 個の LE 上の所望の位置に論理ゲート素子を再現し，それぞれをビアのみで配線した．



（a） 配置エリアのレイアウト（LAB）　　（b） CADシステムが生成した各ビア座標

図６．２０　8bit×8bit 乗算器の CAD を用いたレイアウト生成の例

第 6 章の参考文献

[1] Vaughn Betz, “VPR and T-VPack: Versatile Packing, Placement and Routing for FPGAs”, http://www.eecg.toronto.edu/~vaughn/vpr/vpr.html

[3] Synopsys, “Synopsys.com”, http://www.synopsys.com/home.aspx

[2] Steven M. Rubin, “Computer Aids for VLSI Design”, http://www.rulabinsky.com/cavd/text/chapc.html, 1994

[4] Saurabh Adya, Andrew Caldwell, Andrew B. Kahng, Igor Markov, and Jarrod Roy, “Capo: a large-scale fixed-die Floorplacer”, http://vlsicad.eecs.umich.edu/BK/PDtools/Capo/, Oct. 2005

[5] J. A. Roy, S. N. Adya, D. A. Papa and I. L. Markov, ``Min-cut Floorplacement'', IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 25 No. 7, Page 1313-1326, July 2006

[6] 末吉敏則，天野英晴，“リコンフィギャラブルシステム”，（社）オーム社，東京， 8 月 2005 年.

[7] Jarrod A. Roy and Igor L. Markov, “FGR - A Fairly Good Router”, http://vlsicad.eecs.umich.edu/BK/FGR/, April 2104

[8] Jarrod A. Roy and Igor L. Markov, “High-performance Routing at the Nanometer Scale”, in Proc. International Conference on Computer-Aided Design (ICCAD’07), pp.496-502, Nov. 2007.

[9] Jin Hu, Jarrod A. Roy, and Igor L. Markov, “Completing high-quality global routes”, Proceedings of the 19th international symposium on Physical design (ISPD’10), pp. 35-41, March 2010.

[10] Moffitt, M.D , “MaizeRouter: Engineering an effective global router”, Asia and South Pacific Design Automation Conference (ASPDAC ‘08), pp.226-231, March 2008.

[11] Minsik Cho, Kun Yuan, Katrina Lu and David Z. Pan, “BoxRouter”, http://www.cerc.utexas.edu/utda/download/BoxRouter.htm, Nov. 2007.

[12] Minsik Cho and David Z. Pan, “BoxRouter: A New Global Router Based on Box Expansion and Progressive ILP”, Proc. Design Automation Conference (DAC), July 2006.

[13] Ryan Kastner, “Labyrinth: A Global Router and Routing Development Tool”, http://kastner.ucsd.edu/ryan/labyrinth-a-global-router-and-routing-development-tool/, Dec. 2014

[14] Ryan Kastner, Elaheh Bozorgzadeh and Majid Sarrafzadeh, “Pattern Routing: Use and Theory for Increasing Predictability and Avoiding Coupling“, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, July 2002

[15] Chris Chu, “FLUTE: Fast Lookup Table Based Technique for RSMT Construction and Wirelength Estimation”, http://home.eng.iastate.edu/~cnchu/flute.html, Feb. 2011.

[16] Chris Chu, “FLUTE: Fast Lookup Table Based Wirelength Estimation Technique”, In Proc. International Conference on Computer Aided Design, pp.696-701, 2004.

[17] ISPD 2007 Global Routing Contest, “ISPD 2007 Global Routing Contest Announcements”, http://archive.sigda.org/ispd2007/contest.html, Feb. 2013.

第７章　チップ試作と性能評価

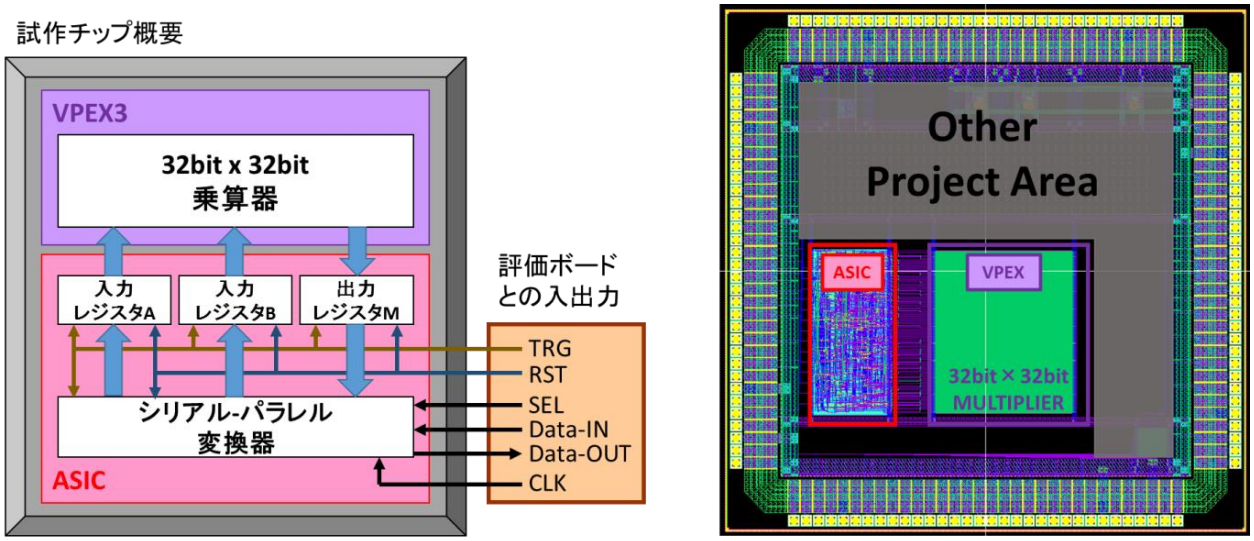
本章では開発した CAD システムを利用して試作した VPEX3 の評価用チップについて報告する．試作した回路は 2 種類あり，組み合わせ回路と順序回路をそれぞれ 1 つずつ開発した．2 種類の試作チップは共に東京大学 VDEC[1]より提供されている，Rohm180nm プロセスによって設計と製造を行った．このチップ試作では VPEX3 の動作確認, CAD システムの有効性の確認, および性能評価を目的としており，それぞれのチップ試作から得られた知見について考察していく．

７．１　組み合わせ回路―乗算器

ここでは VPEX3 を用いて実現した乗算器回路に関して報告する. 本試作回路には組み合わせ回路として 32bit×32bit 乗算器を選択した．この回路は I/O ポートが合計で 128bit になる大規模な回路である．性能評価のために VPEX を用いた試作チップの開発は以前より行われてきたが[2-4]，手動配置・手動配線による小規模な回路であり，専用の CAD システムを利用した大規模回路の試作はこれが初めての試みとなる．本回路試作の目的は CAD による大規模回路の実現が可能であることを証明することである．

７．１．１　仕様

図７．１に本試作チップの構造図および完成レイアウトを示す．今回開発した回路は順序回路を必要とする部分はすべてセルベース方式によって実装し, 組み合わせ回路部分のみを VPEX で実装している．



（a）内部構造　　（b）完成レイアウト

図７．１　回路構造

試作回路の詳細を説明していく. 回路を動作させるための入出力ポートは Data-IN, Data-OUT, CLK, TRG, SEL, RST の 6 ポート存在する. 評価ボードから入力データを転送する際はデータ入力ポート Data-IN から 1bit ずつデータを転送する. この時の同期用の信号はクロック入力ポート CLK に与えられる. 与えられたデータを用いて乗算演算を実行する際は TRG ポートにパルスを 2 度入力する. 1 度目の入力でデータが入力レジスタ A,B に書き込まれ, 乗算演算が開始される. 2 度目のパルスで乗算演算の結果を出力レジスタ M に格納する. データを確認する際はクロック入力ポート CLK にクロックパルスを与えることでデータ出力ポート Data-OUT から 1bit ずつデータが出力される. シリアルパラレル変換器はデータ転送の際は SEL に 0 を与えることでシリアルデータの受信と転送を行い, SEL に 1 を与えることでデータレジスタ M の値をセットする.

① 乗算器

乗算器は 2 つの入力を二つ受け取り, 乗算演算を実行し, 結果を出力する回路である. 図 7. 2 に 4bit 乗算器の仕組みを示す. 2 進数の乗算演算の場合, 積の最大 bit 数は入力 bit 数の合計となるため, 今回の 32bit×32bit 乗算器の場合, 出力の bit 幅は 64bit の出力となる. したがって, 入力と出力の合計 bit 幅は 128bit となる. この bit 幅を単純に入出力ポートに割り当てる場合, 128 ポートの IO が必要となるが, 試作チップに用いる IO は最大 80 ポートであるため, 128 ポートを割り当てる事ができない. そのため, 今回はシリアル-パラレル変換機を利用して, 入力および出力を外部から転送している

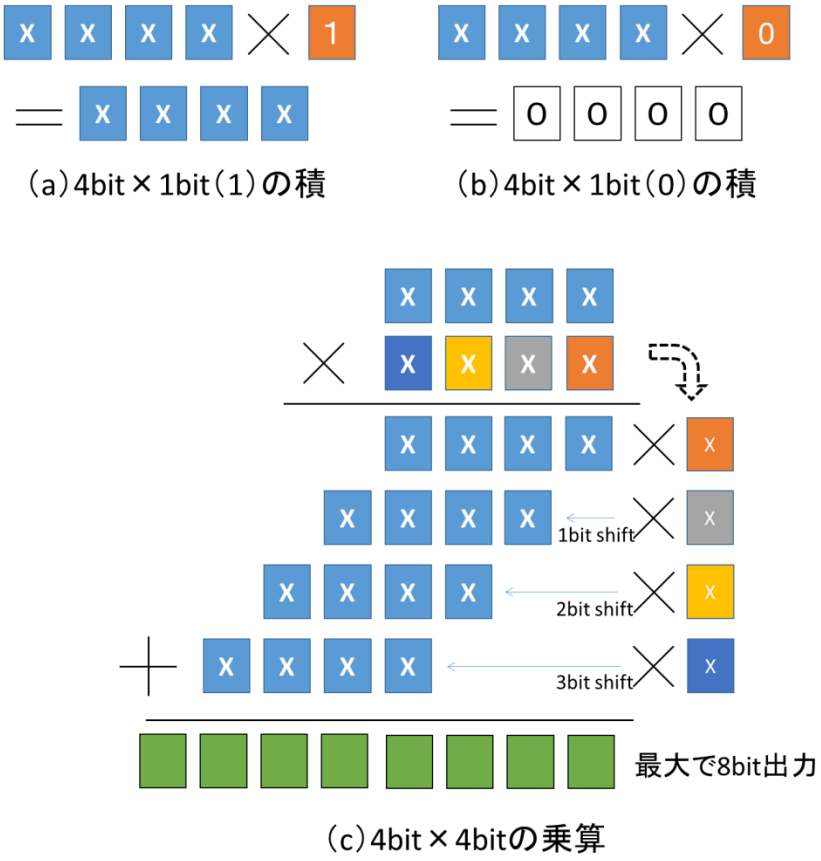


図 7. 2　2 進数乗算器の構造

② シリアル-パラレル変換器

シリアルパラレル変換器は 1bit の入力を N 回受け取り，N-bit 幅のデータへと変換する回路である．図７．３にこの概念を示す．通常の N-bit のデータを送信する場合，受信間との間に N 個のパラレルポートが必要となるが，ピン数の制限によりこれを設けることが難しい場合がある．こういった場合では N 個のデータを 1bit ずつ N 回に分けて送信することで目的が達せられる．これを実現する回路がパラレル-シリアル変換器およびシリアル-パラレル変換器である．この回路はシフトレジスタによって実現する事ができる． 設計したシリアル-パラレル変換回路を図７．４に示す．図で示している回路は 4bit のデータに対応したものであり，実際にはこれを 64bit に拡張したものを２つ使用した．

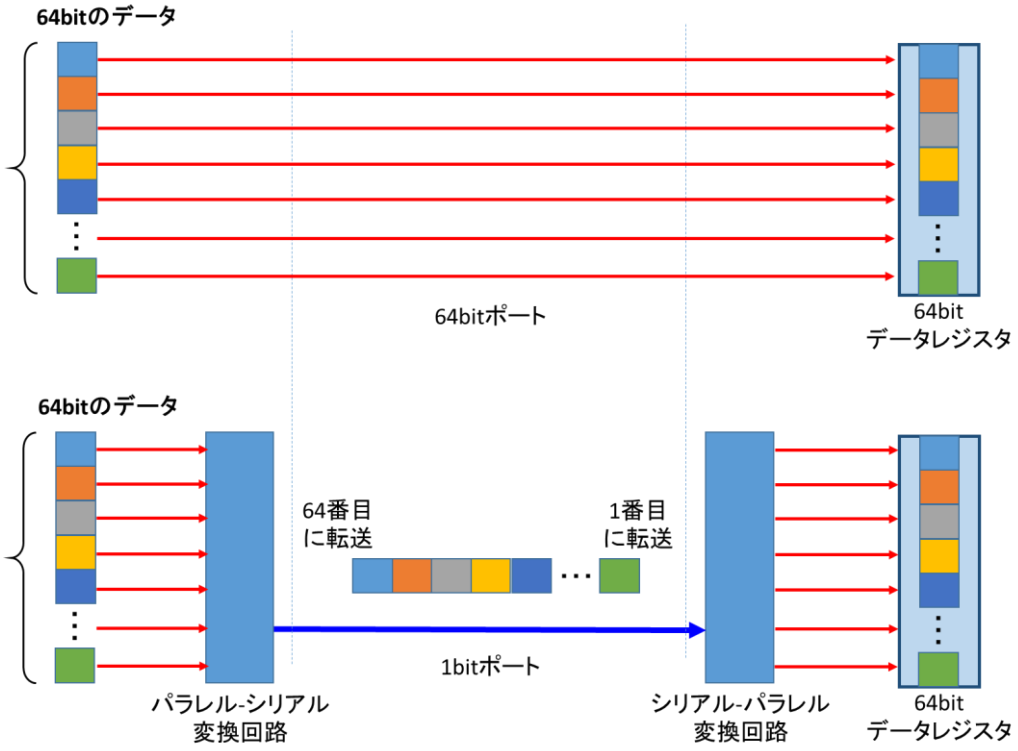


図７． 3　シリアル-パラレル変換機を利用した転送（64bit データの例）

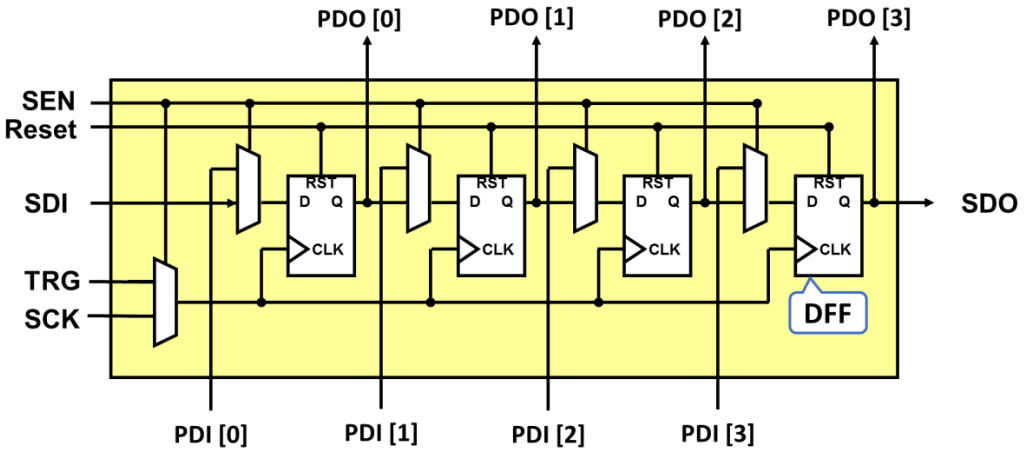


図７． 4　4bit シリアル-パラレル変換回路

設計した乗算器とシリアル-パラレル変換器の縦横長，面積，利用率（Utilization ※）を表７．１に示す．今回の回路は空白領域を広く含んでいる．また動作速度制約には乗算器とシリアル-パラレル変換器で異なる値を設定した．

表７．１　試作回路の仕様

	VPEX	ASIC
回路	乗算器	シリアル-パラレル変換器
横長 / 縦長 [μm]	704.04 / 781.56	406.54 / 800.00
面積 [μm²]	550249.5	325232.0
Utilization [%]	36.62	28.99
動作速度制約[MHz]	10	100

７．１．２　性能評価

VPEX3 によって実現した乗算器の面積と速度の性能に関して報告する．試作チップの設計段階では動作周波数制約を 4 通りに変化させた場合の論理合成を行った．この時の各性能を ASIC のもの比較した結果を表７．２に示す．

表７．２　面積・動作速度の性能評価

	ASIC	VPEX			
制約条件	100MHz	100MHz	33MHz	30MHz	10MHz
面積	95774.5	354096	361008	211068	188568
動作速度	12.68	28.47	28.45	33.30	36.16

論理合成時の結果では，ASIC と比較して動作速度は 2.2~2.8 倍，面積は 2.0～3.7 倍という結果になった．また動作速度は 28～36ns であり，この制約条件を十分に満たす条件として，試作では動作周波数制約が 10MHz の時の論理回路を使用している．

※　Utilization

実回路の面積に対して，論理回路を形成するために必要となるスタンダードセルの合計面積の割合を示したもの．この数値が高いほど，スタンダードセル間の空白領域の割合が小さく，論理密度が高いことを示している．例えば Utilization が 50%の場合は回路面積の半分が空白領域，Utilization が 25%の場合は 3/4 が空白領域であることを示している．セルベース ASIC の場合は 70～80%が標準的な数値である．

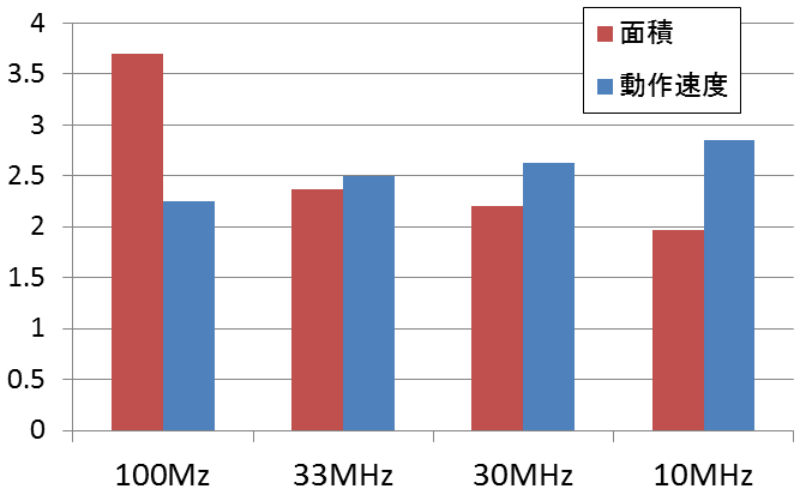


図７．５　面積・動作速度の性能比較

次に 10MHz 時の論理合成結果を用いて配置配線を行ったときの LAB サイズ毎のトラック割当失敗数および配線使用率の平均値を算出した．LAB サイズは論理合成から得られたセル数に対して Utilization が 80%，60%，40%，20%のとなる配置領域を定義した．このときの配置領域に形成される LE 数と配線時に使用可能な総トラック数を表に示す．この評価では 4 通りの LAB サイズ毎に 10 回の配置配線処理を試行し，トラック割当失敗数と配線利用率を記録した．

表７．３　各 Utilization における LE 数とトラック数

Utilization	20%	40%	60%	80%
配置領域の LE 数	26244	13225	8836	6561
総トラック数	419904	211600	141376	104976

表７．４　配線トラック割当失敗数

Utilization	20%	40%	60%	80%
Trial1	0	0	14	86
Trail2	0	0	17	92
Trail3	0	1	14	48
Trial4	0	3	7	118
Trial5	0	3	13	97
Trial6	0	1	19	45
Trial7	0	2	17	93
Trial8	0	1	23	63
Trial9	0	1	16	98
Trial10	0	0	27	106
平均	0	1.2	16.7	84.6

表７．５　各 Utilization における配線トラックの利用率

Utilization	20%	40%	60%	80%
Trial1	127693	102004	92486	84776
Trial2	125867	103144	91621	85290
Trial3	128050	106035	92132	82733
Trial4	125924	101199	92644	84874
Trial5	126346	101832	92287	84881
Trial6	125853	103166	92218	82377
Trial7	127573	102924	91574	84069
Trial8	128808	101050	93315	83243
Trial9	125226	101763	92223	84099
Trial10	125789	103965	91914	84687
平均	126712.9	102708.2	92241.4	84102.9
割合	30.18%	48.54%	65.25%	80.12%

トラック割り当て失敗数を見ると，60%では割当処理が成功することは無く，40%以降でようやくトラック割当時の失敗頻度が少なくなる．Utilization40%では配線トラックの利用数は約 10000 本，総トラック数からの割合は 48.5%となっている．チップ試作ではこの結果を考慮して Utilization を 30%ほどに設定して配置配線を実行した．配置配線では図７．６に示すように，LAB の左側のみに入出力ポートを割り当てた初期配置で配置配線を行った．これは ASIC 領域との結合を簡単に行うためである．

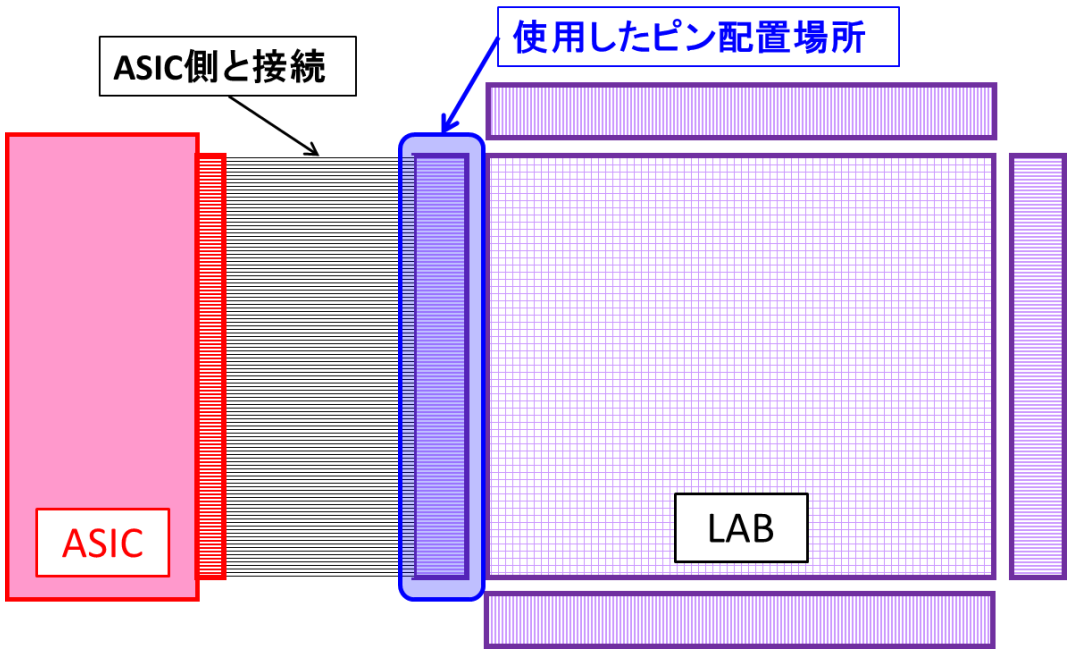


図７．６　ピン座標の制約

７．１．３　動作確認

完成した試作チップを評価ボードに取り付け，入力に対する出力を確認した． 今回の動作検証には三菱電機マイコン機器ソフトウェア株式会社の MU-300-EM[4]を使用した．この評価用ボードは評価対象 LSI に対して入力テストパターンを用いた機能テストが可能であり，また各テストパターン生成における出力パターンを保存する機能が備わっている．この機能を利用して動作確認を行った．実際の検証環境を図７．７に示す

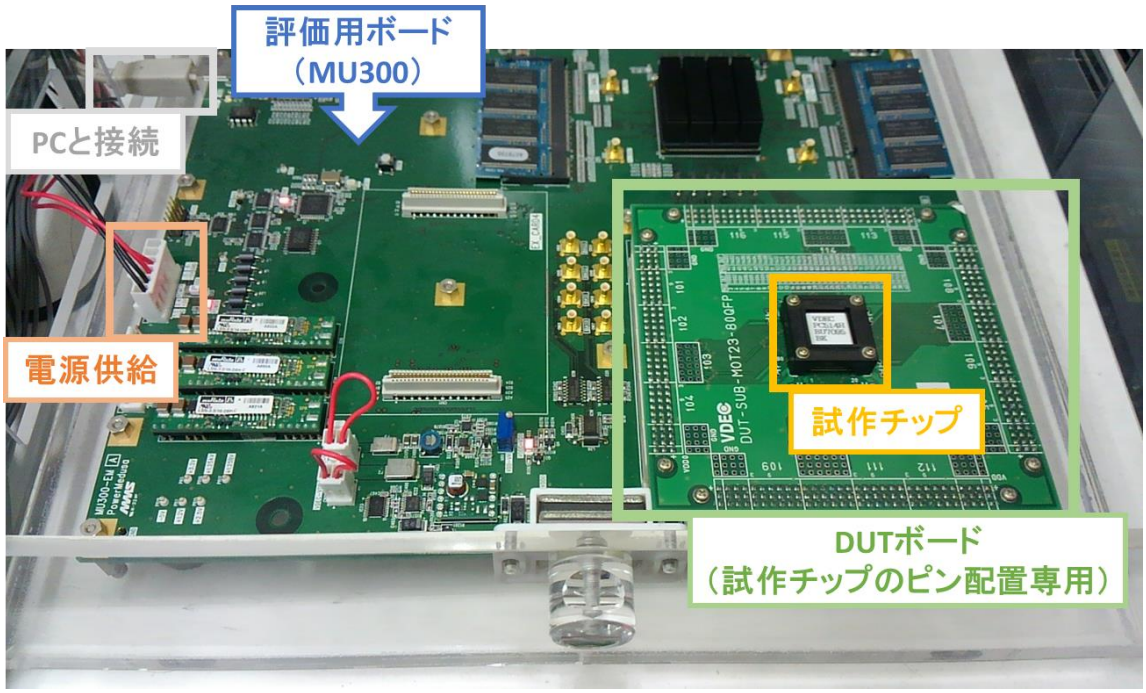


図７．７　評価環境

動作確認では複数の入力テストパターンに対する出力パターン結果を取得し，その値が乗算演算で得られる値と等しいことを確認した．表７．６に入力テストパターンに対する出力テストパターン結果を一部抜粋して示している．

したがって，設計した 32bit×32bit 乗算器は正しく動作している事が確認できた．これにより CAD および VPEX3 アーキテクチャによって, 組み合わせ回路の設計および実装が実現できていることを確認した．

表７．６　検証した試作チップにおける入力パターンと出力結果

入力 A	入力 B	出力 M
0000’0001	0000’0001	0000’0000’0000’0001
1111’1111	1111’1111	0123’4567’8765’4321
FFFF’FFFF	FFFF’FFFF	FFFF’FFFE’0000’0001

７．２　順序回路—DES 暗号回路

ここでは VPEX3 を用いて実現した DES 暗号回路に関して報告する．DES 暗号回路は内部に DFF のような記憶素子を持つ順序回路である．前節の試作結果より，VPEX3 を用いて開発した組み合わせ回路が正しく動作できており，VPEX3 用の CAD システムを用いた開発が可能であることが分かった．そこで順序回路の実チップ動作検証を試みるため DES 暗号回路の開発を行った．また本試作では実チップの消費電力評価を行うことも目的の１つに設定している．

７．２．１　回路仕様

図７．８は今回試作した DES 暗号回路の概要図を示している．回路は評価用ボード用のインターフェース部と暗号回路部に分かれている．インターフェース部は図中の各レジスタへデータ転送するための回路である．今回の試作では評価用ボードとデータの送受信を行うインターフェース回路部も VPEX3 の LAB 上に構成している．評価用ボードはインターフェース回路の接続は 1bit 幅の CLK, RST, Write, Read，Busy，Trig 信号と，16bit の Addr，Din，Dout 信号によって構成されている．

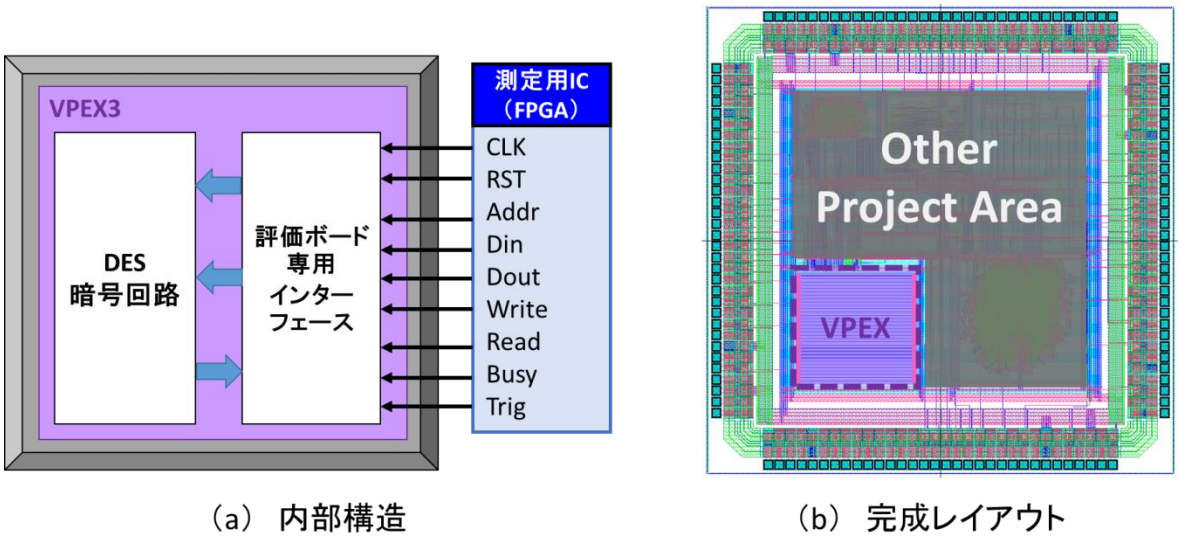


図７．８　回路構造

①　DES 暗号回路[6,7]

DES 暗号化回路は 56 ビットの鍵を使った共通鍵暗号回路である．アルゴリズムとしては 16 回の共通処理があるため，この 1 回分をハードウェアとして実装し，これを 16 回動作させることで平文を暗号化する．今回の試作では東北大学にて公開されている DES 暗号回路の IP コア[8]を利用した．

図７．９に DES の暗号化処理を示す．初めに平文 64bit を 32bit に分割し，下位 32bit（1bit 目～32bit 目：R0）を Feistel 関数と呼ばれる非線形関数に渡され，鍵との XOR 演算やテーブル参照変換，並べ替えなどの処理が行われる．非線形関数の出力値は切り離されていた上位 32bit（33bit 目～64bit 目：L0）と XOR 演算が行われ，これが第 1 ラウンド目の処理における下位 32bit 出力（R1）となる．また R0 は第 1 ラウンド目の処理における上位 32bit 出力（L1）となる．この R1,L1 が第 2 ラウンド目の処理の入

力 64bit となり，再び同様の処理が実行される．この処理が 16 回繰り返されることで平文が暗号文に変換される．この平文を元に戻すためには，暗号処理に用いたものと同じ暗号鍵を用いる必要がある．

DES 暗号回路自体は鍵長の短さなどから現在では安全でない暗号回路であり[9]，近年ハードウェアとして開発される機会は少なくなっているが，今回はあくまで VPEX3 による順序回路の実装検証が目的であるため，試作回路として選択した．

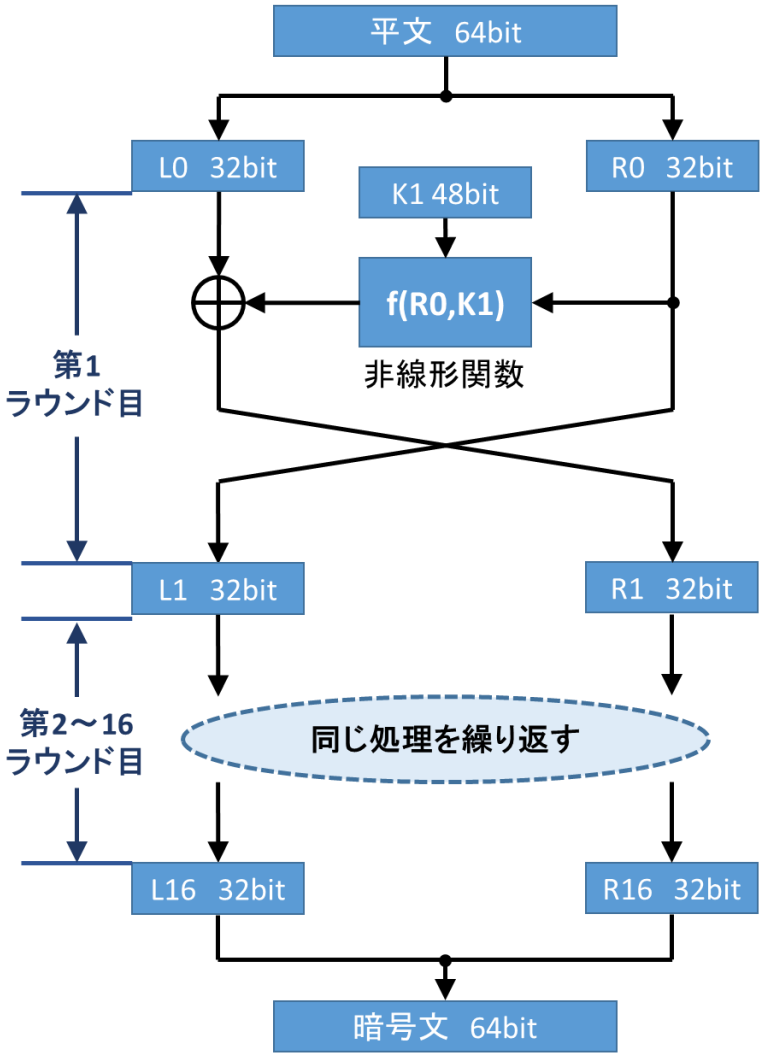


図 7．9　DES 暗号化回路のアルゴリズム

② 評価ボード専用インターフェース

本試作チップの動作検証には産業技術総合研究所（産総研）の開発した「SASEBO-RII」評価ボード[10]を用いた．この評価用ボードは暗号回路のサイドチャネルアタック解析および耐性評価用のボードとして開発されたものである．チップと電源回路の間に 1Ω の抵抗素子が繋いであり，抵抗素子の両端の電位差を測定するための接続口が設けられている．そのため動作時に回路に流れる電流の評価を行う事が可能である．また暗号回路の動作テストを行うためのアプリケーションや FPGA に書き込む評価回路がインターネットより入手可能であるため[10]機能テストを容易に行う事ができる．

この評価用ボードは独自のインターフェースを有しており，暗号回路の機能テストを行うためには専用インターフェース回路をチップ内に実装しておく必要がある．インターフェース回路の構造を図７．１０に示す．この回路は暗号回路側に 390，外部の制御回路側に 50 の I/O ポートを有する回路である．

制御回路側の lbus_a ポートから与えられた制御信号を解釈して，入力信号の受信，暗号回路を初期化や動作，暗号処理結果の送信などを行う． 内部に約 400 個のレジスタを有しており，このインターフェース回路自身も大規模な順序回路である．

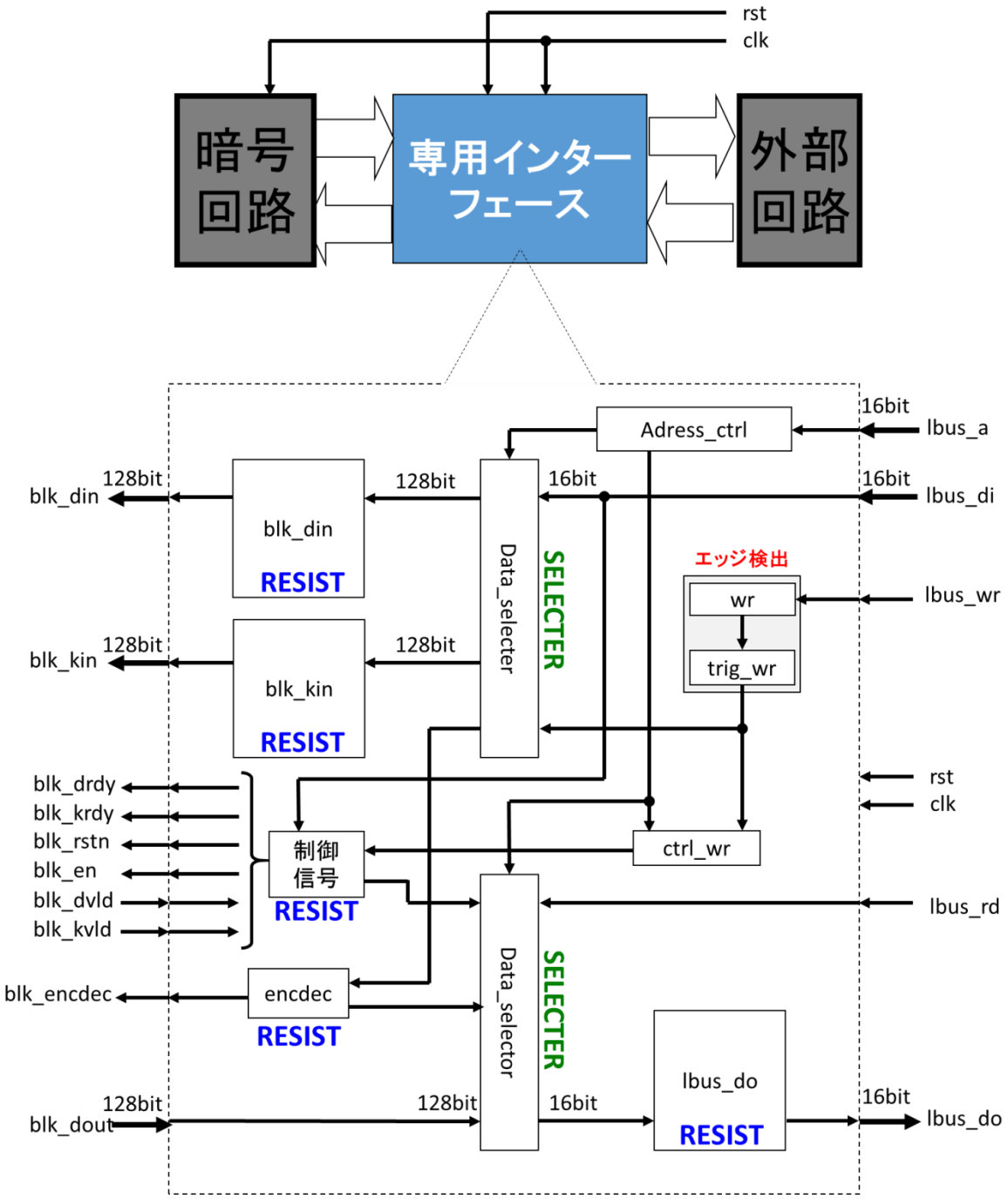


図７．１０　SASEBO-RII 専用インターフェース回路

表７．７に今回開発した回路の性能をまとめた．DES 暗号回路とインターフェース回路の複合回路として設計しており，前節の乗算器同様に Utilization が低く，回路面積の 68%以上が空論理の LE によって構成されている．

表７．７　試作回路の仕様

	VPEX
回路	DES 暗号回路＋ 評価ボード用専用インターフェース
横長 / 縦長 [μm]	653.8 / 615.1
面積 [μm²]	402152.4
Utilization [%]	31.5
動作速度制約[MHz]	4

７．２．２　性能評価

VPEX3 上に実装した暗号回路，およびインターフェース回路の面積，動作速度に関して報告する．本回路は動作速度制約条件を 3MHz として設計を行った．これは，評価用ボードのアプリケーションおよび FPGA 内の生成するクロックが 3MHz 動作を想定しており，その条件に合わせるためである．表７．８に試作回路の論理合成時の面積，動作億度，消費電力を示す．

表７．８　試作回路の性能（論理合成時）

面積	動作速度	消費電力
113400 μm²	11.89 ns	0.1429 mW

この回路に対して配置配線処理を行ったときの LAB サイズ毎の割当失敗トラック数および配線トラック使用率の平均値を算出した．LAB サイズは論理合成から得られた面積に対して Utilization が 80%，60%，40%，30%，20%のとなる 5 通りの配置領域を定義した．このときの配置領域に形成される LE 数と配線時に使用可能な総配線トラック数を表７．９に示す．この評価では 5 通りの LAB サイズ毎に 10 回の配置配線処理を試行し，割り当て失敗トラック数と配線トラック利用数を記録した．割り当て失敗トラック数を表７．１０，配線トラック利用数を表７．１１に示す．

表７．９　各 Utilization における LE 数とトラック数

Utilization	20%	30%	40%	60%	80%
配置領域の LE 数	15625	10609	7921	5329	3969
総トラック数	250000	169744	126736	85264	63504

表７．１０　各 Utilization における割り当て失敗トラック数

Utilization	20%	30%	40%	60%	80%
Trial1	0	12	25	484	918
Trial2	0	2	2	239	879
Trial3	0	8	52	245	1088
Trial4	0	8	73	198	923
Trial5	0	45	29	167	861
Trial6	0	0	12	547	759
Trial7	0	13	40	69	877
Trial8	0	10	37	208	1319
Trial9	0	0	19	278	675
Trial10	0	13	4	296	898
平均	0	11.1	29.3	273.1	919.7

表７．１１　各 Utilization における配線トラックの利用数

Utilization	20%	30%	40%	60%	80%
Trial1	78563	68548	64761	56534	51354
Trial2	79569	71030	63331	57044	51251
Trial3	80517	71558	64715	56069	51569
Trial4	81516	68500	64592	55745	51143
Trial5	79356	70294	64558	55985	51397
Trial6	79720	71431	64487	57939	51105
Trial7	78538	70953	64810	54207	51378
Trial8	78463	69199	64550	55142	52896
Trial9	78584	69036	63229	55564	50149
Trial10	80646	71383	64130	56872	51525
平均	79547.2	70193.2	64316.3	56110.1	51376.7
割合	31.82%	41.35%	50.75%	65.81%	80.90%

配線失敗トラック数をみると，40%以上の Utilization では配線処理が成功することがなく，30%まで下げる必要があることが分かった．これは前節の乗算器の配線成功時の Utilization よりもさらに悪くなっており，また乗算器の方が今回の回路よりも面積の大きな論理回路であったことを考慮すると，組み合わせ回路よりも DFF を含む順序回路の方が配線成功率および Utilization が悪化することが考えられる．

これらの結果から, チップ試作時の配置領域の LE 数は縦 100 個×横 100 個の 10000LE を想定した領域上に実装を行った.

７．２．３　クロックツリー

CAD を用いて完成した試作チップの配置領域に対して，クロックツリーを加えたブロックのレイアウトを図７．１１（a）に示す．またクロックツリーを構成するバッファや配線の位置を図７．１１（b）に示す．クロックツリーは LAB の上部と側部に存在し，クロックソースを受取る専用の外部入出力ポートは上部中央に存在する．またこのクロックツリーは３段のバッファセルを経由する構造になっている．初めに上部中央で初段バッファを経由して左右に出力信号が伸びる．その後上部コーナーに位置する二つ目のバッファを経由して側面に敷き詰められたバッファアレイに接続される．バッファアレイは縦に並べられた LE の行数と同じ数のバッファセルが組み込まれており，このバッファがクロックツリーの最終段バッファとなる．LE 配置領域内の側面から中央に向かって構成されているクロックローカルラインにバッファが接続される．クロックパルスがクロックローカルラインを経由して配置領域内のすべての DFF のクロック入力端子に接続される．こうして各 DFF はクロックパルスに同期して，動作することが可能になる．

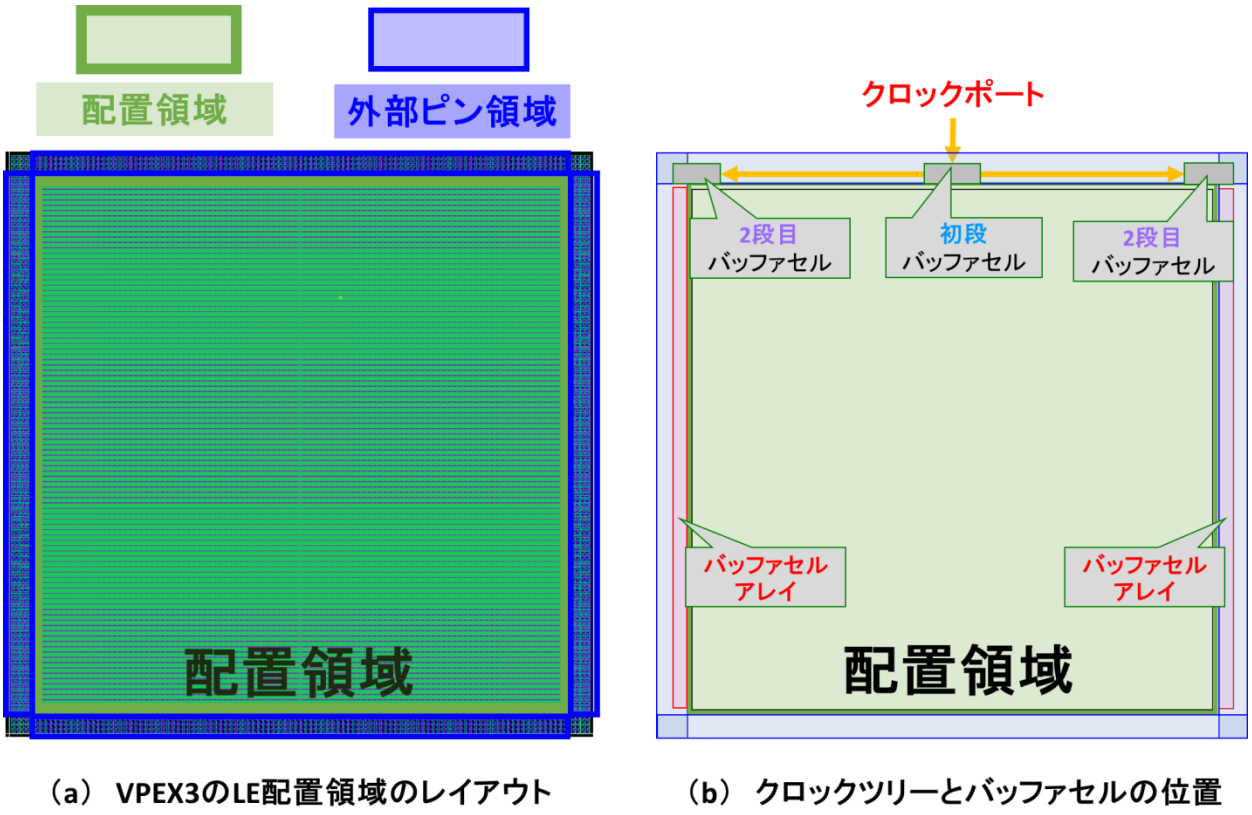


図７．１１　配置領域とクロックツリー

７．３　実チップを用いた ASIC，FPGA との消費電力性能比較

本節では DES 暗号回路をベンチマーク回路としてスタンダードセル ASIC による実装，FPGA による実装，VPEX による実装の 3 種類の実装における実機評価を行い，それぞれの実装間での消費電力性能比較を行った結果に関して報告する．

初めに評価環境の説明を行う．評価には実際に試作した LSI を評価用ボードに取り付け，VDD の電位差をオシロスコープを用いて測定することで電力の見積もりを行った．スタンダードセル ASIC および VPEX は「SASEBO-RII」という評価用ボードを利用し測定した．FPGA への実装では同じく「Zuiho」と呼ばれる評価用ボードを使用した．Zuiho のボード上には Xilinx 社製 FPGA「Spartan3A」が実装されており，この FPGA 回路を実装し，VDD ポートに流れる電流をオシロスコープで測定した．各評価用ボードと測定機器の接続例をそれぞれ図７．１２と図７．１３に示す．

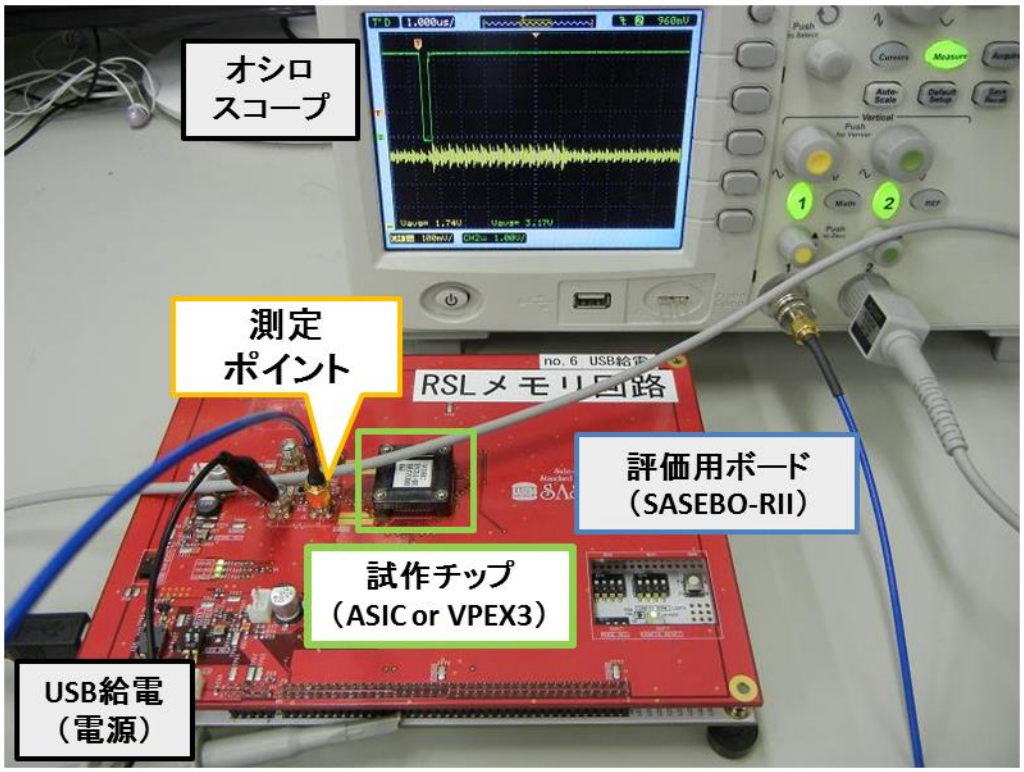


図７．１２　評価ボード SASEBO-RII[10]と評価環境

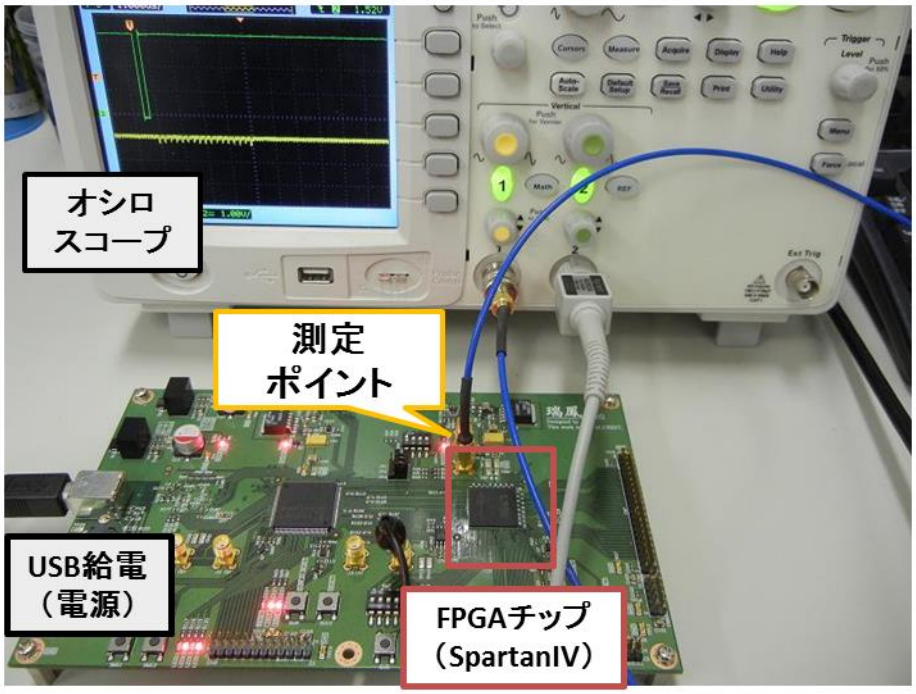


図７．１３　評価ボード Zuiho[10]と評価環境

次に評価方法について説明する．評価用ボードの電源は USB で供給され，そこから電源回路がチップに流すための電源電圧を生成する．電源回路と評価チップとの間の配線（電源配線）には図７．１６に示すような 1Ω のシャント抵抗が直列につながっており，さらにシャント抵抗の両端には 2 つの 50Ω 抵抗が並列につながっている．電源配線を流れる電流の測定ではシャント抵抗の両端の電圧を並列につながった 50Ω 抵抗素子を介して測定する．このときのシャント抵抗の電位差から，DES 暗号回路に流れる電流が判明し，電流と電圧から消費電力が判明する

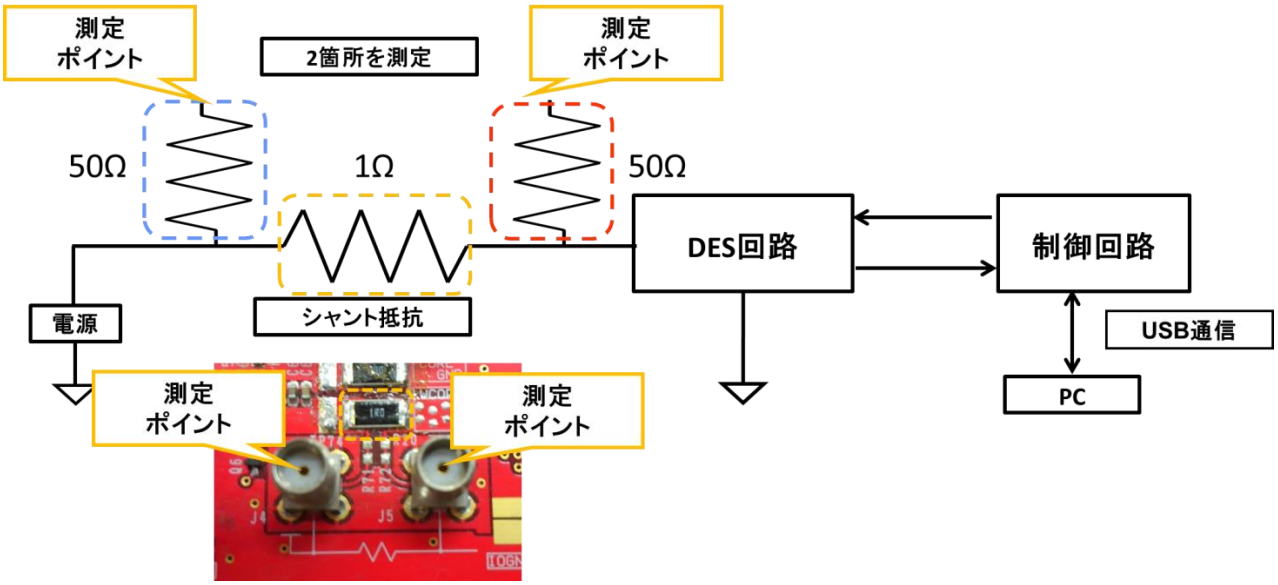


図７．１４　測定ポイント

今回の測定ではASICおよびVPEXの評価に用いた評価用ボードとFPGAボードでは測定条件が異なっている．評価用ボードごとの測定条件の違いを表７．１２にまとめる．

表７．１２　各評価用ボード，試作チップの仕様

	測定アーキテクチャ	製造プロセス	電源電圧値	動作周波数
SASEBO-RII	VPEX3	180nm	1.8V	3MHz
	セルベース ASIC	180nm	1.8V	3MHz
Zuiho	FPGA	90nm	1.2V	4MHz

表７．１３に測定条件を示す．評価は 2 種類の状態を測定した．状態 1 では暗号処理を行っている通常動作時の測定結果．状態 2 では入出力遷移およびクロック信号を停止させたときの静的な消費電力の評価を行った．ここでシャント抵抗を流れる電流はチップを流れる電流と，チップに近い側の 50Ω抵抗を流れる電流の合計を測定していることになる．

表７．１３　測定時の状態

	電源の供給	クロック供給	入力パターン	リセット信号
状態１ (動作時)	あり	あり	ランダム	OFF
状態２ (待機時)	あり	なし	遷移なし	ON

ここで「状態１」の電流値から「状態 2」の電流値を引いた値がチップの動的電流．状態 2 の電流からチップ側の 50Ω抵抗に流れる電流を引いた値がチップの静的電流となる．この電流値を表７．１４に示す．VPEX3 および ASIC における静的電流の測定値が 0A となっているが，これは測定に用いたオシロスコープおよびプローブでは 1Ω抵抗間の電位差が小さすぎたため正確に測定することができなかったことを示している．

表７．１４　実測した消費電流の平均値

	動的電流(mA)	静的電流(mA)
VPEX(180nm)	1.6571	0.0000
ASIC(180nm)	0.5506	0.0000
FPGA(90nm)	1.6689	15.7714

さらにこの結果を元に 3MHz 動作時の消費電力を表７．１５および図７．１５に示す．このとき ASIC と VPEX3 の動作速度はともに 3MHz であるが，FPGA の消費電力は 4MHz で測定を行っているため，測定値に 3/4 倍の補正をかけた結果となっている．

表７．１５　各設計方式における平均消費電力

	動的電力(mW)	静的電力(mW)
VPEX(180nm)	2.9829	0.0000
ASIC(180nm)	0.9911	0.0000
FPGA(90nm)	1.5020	18.9257

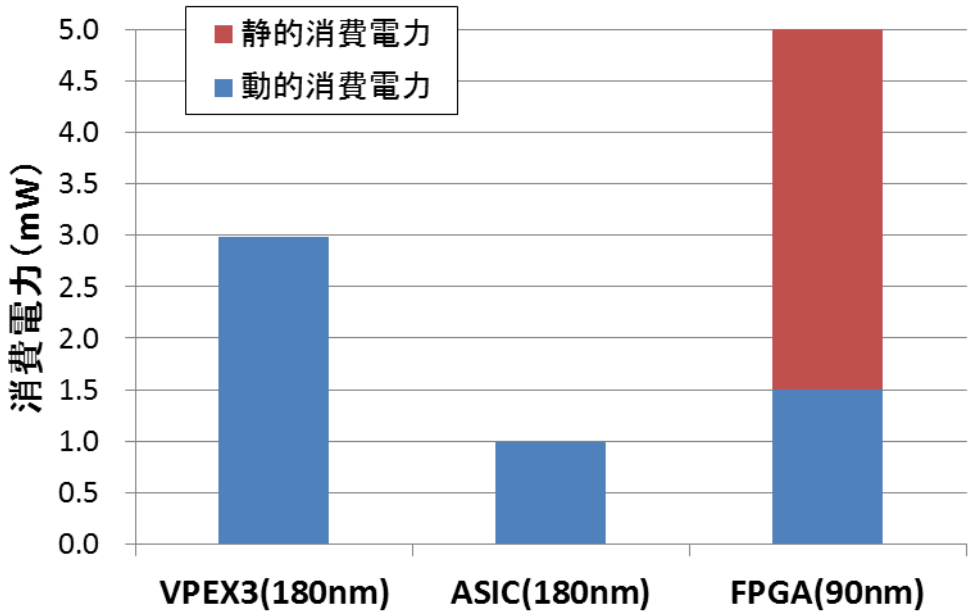


図７．１５　各製造方式における DES 暗号回路の平均消費電力

VPEX3 と ASIC を比較すると，ともにリーク電流の低い 180nm プロセスであるため静的消費電力は観測できないほど低電流であり，実チップでは電力差を観測することはできない．一方で動的消費電力を比較すると 3 倍の電力差が確認された．したがって ASIC と VPEX3 では消費電力性能に約 3 倍の差が存在するということになる．

VPEX3 と FPGA を比較すると，FPGA は 90nm プロセスであり電源電圧も 1.2V と VPEX3 よりも低い．そのため動的消費電力を比較すると，FPGA の消費電力は VPEX3 の約 1/2 ほど低くなっている．一方で待機時の静的消費電力は FPGA の方が明らかに大きい．動作周波数が遅いデバイスにおいては 180nm プロセスで設計された VPEX3 の方が低消費電力なハードウェアを実現できるが，常に高速動作が求められるシステムにおいては FPGA よりも消費電力が大きくなることが懸念される．

次に FPGA との比較において，プロセスおよび電源電圧の違いを考慮した比較を示す．今回入手できた FPGA が 90nm, 電源電圧 1.2V であったため, 同一のゲート長プロセスで製造された VPEX3 と FPGA の比較を行うことはできなかった．ここでは 90nm/1.2V の評価結果を用いて 180nm/1.8V 時の消費電力の推定を行い，動的消費電力の比較を行う．今回のゲート長のサイズ比は 1/2 である．トランジスタのスケーリング則[11]より，ゲート長 L が 1/2 倍になれば，ゲート幅 W およびゲート酸化膜厚 tox も 1/2 倍となる．また電源電圧は 2/3 倍となっている．CMOS 回路の動的消費電力は式（A）で表される．

$$P_{dyn} = f C_L V_{dd}^2 \quad \cdots\cdots \quad (A)$$

ここで出力負荷容量 C_L が次段のゲート容量 Cg と仮定すると式（B）のようになる．

$$C_L \approx Cg = \frac{LW}{t_{ox}} \quad \cdots\cdots \quad (B)$$

よってゲート長が 1/2 にスケーリングされることで C_L は 1/2 倍，動的消費電力 P_{dyn} は 2/9 になると考えられる．FPGA の動的消費電力にこれを考慮し，同プロセスと仮定したときの動的消費電力差を改めて表７．１５および図７．１６に示す．

表７．１４　各設計方式における平均消費電力

	動的電力(mW)
VPEX(180nm)	2.9829
ASIC(180nm)	0.9911
FPGA(90nm)	6.7594

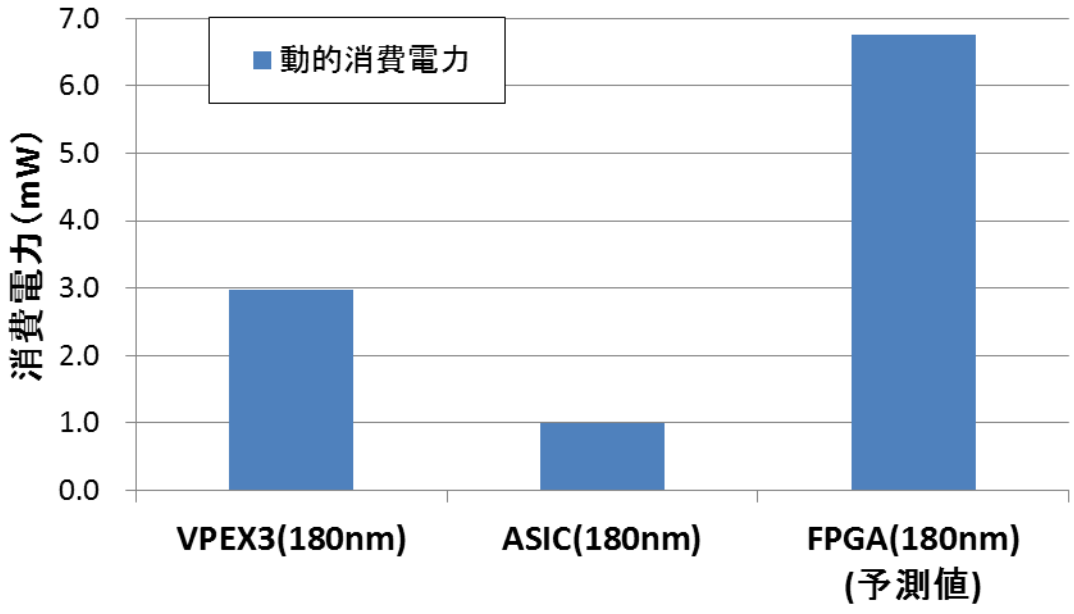


図７．１６　同プロセス条件における DES 暗号回路の平均動的消費電力
（スケーリング則を適用）

図表より，動的消費電力は VPEX3 の方が FPGA よりも約 56%小さい消費電力になると予測される．よって，同一プロセスにおける動的消費電力性能では FPGA よりも VPEX3 の方が省電力化を実現でき

ることが期待される．

総合的に比較すると，VPEX3 によって実装した DES 暗号回路の動的消費電力は ASIC 実装と比較して約 3 倍，FPGA と比較して約 1/2 倍という結果となった．これより VPEX3 が ASIC と FPGA の中間の動的消費電力性能を有していることが分かった．また待機時の静的消費電力では ASIC 同様今回の測定方法では観測できないほど小さく，FPGA と比較して非常に小さくなることが判明した．

これらの評価結果から VPEX3 はモバイル用途に対して FPGA よりも優れた選択肢であると考察できる．一方で VPEX3 を用いてモバイル用途の低消費電力デジタル回路を設計するためには，ASIC と比較して動的消費電力が大きいことが課題であるといえる．この議論については次章で行う．

7 章の参考文献

[1] VDEC, "VLSI Design and Education Center Homepage", http://www.vdec.u-tokyo.ac.jp/

[2] Akihiro Nakamura, Masahide Kawarazaki, Kouta Ishibashi, Masaya Yoshikawa, Takeshi Fujino, “Regular Fabric of Via programmable Logic Using Exclusive-or Array (VPEX) for EB direct Writing”, IEICE Trans. on Electron, Vol.E91-C, No.4, pp.509-516, April 2008.

[3] 川原崎 正英，西本 智広，國生 雄一，北村 一真，山田 翔太，吉川 雅弥，藤野 毅，“ビアプログラマブルデバイス VPEX のチップ評価と DES 暗号回路実装の検討”, 電子情報通信学会技術研究報告, VLD2009-108（478），pp77-82，3 月 2009 年

[4] 西本 智広, 北森 達也, 國生 雄一, 山田 翔太, 吉川 雅弥, 藤野 毅，“ビアプログラマブルデバイス VPEX の配線遅延評価”，電子情報通信学会技術研究報告，VLD2010-109， pp.61-66. 3 月 2010 年

[5] 三菱電機マイコン危機ソフトウェア株式会社, “大容量 FPGA ボード:MU300-EM PowerMedusa”, http://www.mms.co.jp/powermedusa/products/em.html

[6] Biham Eli, and Shamir Adi, “Differential Cryptanalysis of DES-like Cryptosystems”, Journal of Cryptology, Vol.4, No.1, pp.3–72, Jan. 1991.

[7] William Mehuron, and Raymond G. Kammer, “FIPS 46-3: The official document describing the DES standard”, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, Oct. 1999

[8] Aoki Laboratory, Tohoku University, “Cryptographic Hardware Project in Aoki Lab., Tohoku Univ.”, http://www.aoki.ecei.tohoku.ac.jp/crypto/

[9] “DES Challenge III Broken in Record 22 Hours, https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html, Jan. 1999.

[10] “Evaluation Environment for Side-channel Attacks”, http://www.risec.aist.go.jp/project/sasebo/，6 月 2014 年

[11] Dennard, R. H., Gaensslen F. H., Rideout V. L., Bassous, E., LeBlanc A. R., “Design of ion-implanted MOSFET's with very small physical dimensions”, IEEE Journal of Solid-State Circuits, Vol.9 , No. 5, pp.256-268, Oct. 1974.

第 8 章　VPEX4 の提案と性能評価

本章では VPEX3 を改良した新しい VPSA アーキテクチャとその LE 構造について説明する．前章の性能評価より VPEX3 には性能面でまだ多くの課題点が残されていることが明らかになった．そこでこれらの課題点の原因を解明し，その改良方法について考察した．初めに VPEX3 での問題点・課題点を整理する．次にそれらの解決方式について考察していく．最後にすべての解決案を盛り込んだ新しい VPSA アーキテクチャ「VPEX4」を提案し，その構想や改良点の詳細を説明する．

８．１　VPEX3 の性能における問題点

本節では VPEX3 の LE の問題点について考察していく．VPEX3 は VPEX2 の論理合成の結果をもとに問題点を考察し，改良を行った．その後 CAD や実チップ試作などのより詳細な性能評価環境が整ったことで，配置配線や消費電力に関する新たな問題点が明らかになった．VPEX3 のアーキテクチャにおける主な問題点を 2 つ指摘する．

（1）実装面積・Utilization

VPEX3 のアーキテクチャに対応した専用の CAD システムを開発したことで，論理合成の結果から得られる理論上の面積ではなく，実際に配置配線処理が成功した場合における Utilization を考慮した実面積を算出することが可能になった．図８．１に 7 章で紹介した VPEX3 の DES 暗号回路の面積を示す．比較対象としてスタンダードセル方式で設計した DES 暗号回路の ASIC を用いた．ASIC は VPEX3 と同様，動作速度制約は 3MHz，論理合成および配置配線では共に最小面積になるように面積制約をかけている．また ASIC の配置配線時の資源利用率（Utilization）の制約は 70%とした．

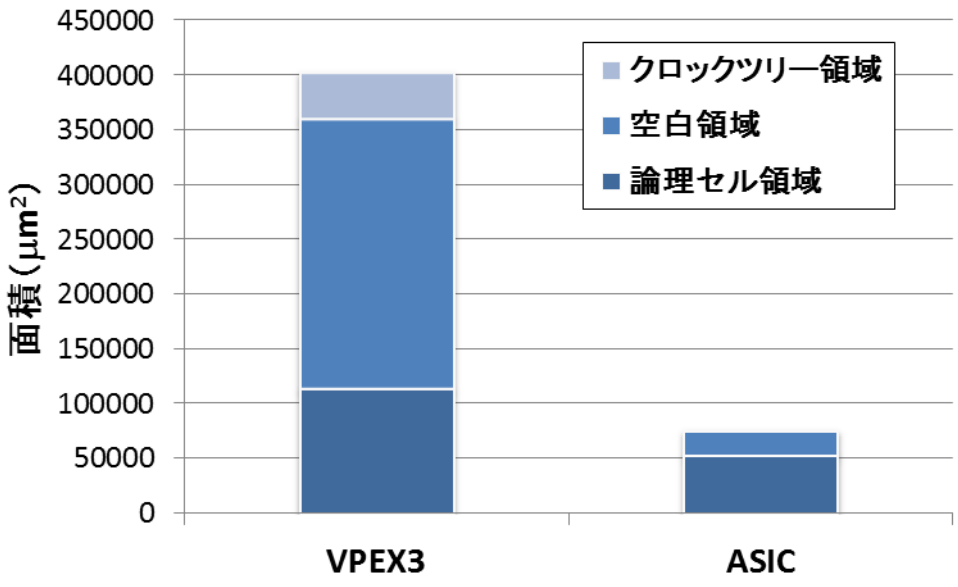


図８．１　ベンチマーク回路の実面積比（ASIC を 1 とした時）

図８．１の結果が示すように，論理合成後の理想的な面積を比較すると VPEX3 による実装では ASIC による実装の約 2.14 倍であり，これは他の VPSA アーキテクチャ方式と比較して面積性能に優れた結果であった．しかしながら配置配線の結果を含めると，この面積の差は約 4.76 倍に膨れ上がる．これは配線リソースを増やすためだけに，特定の論理機能を持たない空論理セルを大量に配置しなければ配置配線処理が成功しないためである．すなわち Utilization が非常に低くなってしまう． セルベース ASIC の場合では Utilization は 70~90%が平均的な水準であり，大部分の領域が論理セルによって埋められるデザインが標準的な回路ブロックの形となる．一方で VPEX3 アーキテクチャによる実装では配線リソースの不足により，この Utilization が 50%に満たないという結果になる．そのため，実面積における ASIC と VPEX3 の性能比較結果では差が非常に大きいものになる．

ISCAS'89 ベンチマーク回路[1]を用いて配置配線処理が成功したとき Utilization の見積もりを行った．その見積もりでは配置領域の Utilization を 20%から徐々に上げていき，トラック割り当て処理が完了しなくなった時の Utilization を示したものである．結果を図８． ２に示す．

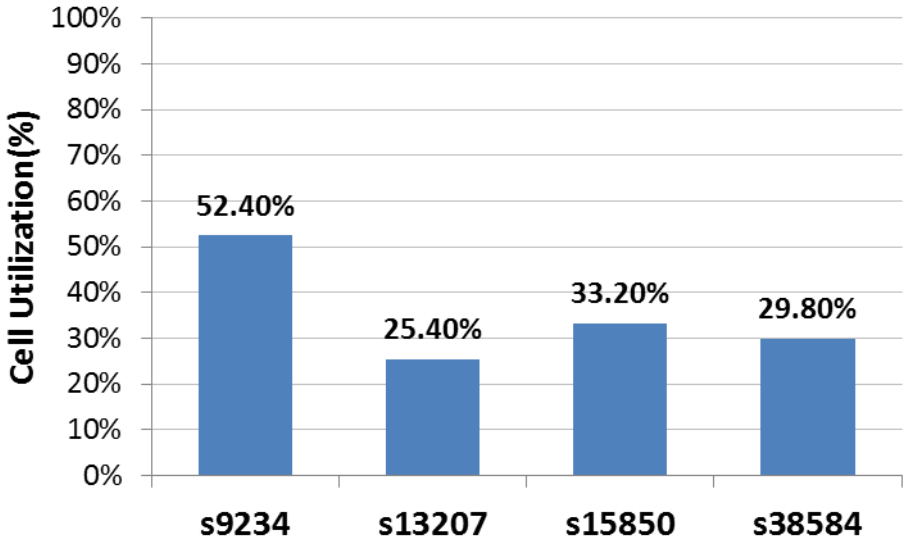


図８． ２　ベンチマーク回路毎の Utilization

図８． ２のように，VPEX3 によって各回路を実装した場合，Utilization は回路規模の小さい s9234 でも約 52%，大規模の s38584 では 30%を下回るような，大部分が空論理セルで占められる構造になってしまうことが確認できた．VPEX3 アーキテクチャは LE のサイズが小さい上にいくつかの 3 入力論理ゲート素子を再現できるため，理論上は面積効率に優れる LE だと考えられていた．しかし実際は LE1 個当たりの配線リソースが少なく，さらにその少ないリソースを入出力ピンに割く必要があるため，配線リソースを確保することが非常に難しいアーキテクチャとなってしまっている． このため VPEX3 アーキテクチャにおいては LE1 個当たりの配線リソースが不足しており，LE サイズの見積もりが必要だと考察することができる．

加えて，VPEX3 の DFF を再現することも，Utilization を低下させる原因になっている．図８． ３は DFF を再現する際にジャンパー配線のリソースを消費していることを図示したものである．VPEX3 アーキテクチャの LE において，DFF のような 2 つの LE を用いて 1 つのセルを再現する場合，2 つの LE

を接続する必要がある．しかし現状この 2 個の LE の接続には配線リソースを消費するほかに実現する方法がなく，これは DFF においても例外ではない．DFF では常に固定座標のジャンパー配線を使用するため，DFF を横切って水平方向に配線を伸ばすためには，図示した個所とは違うトラックを使用しなければならない．

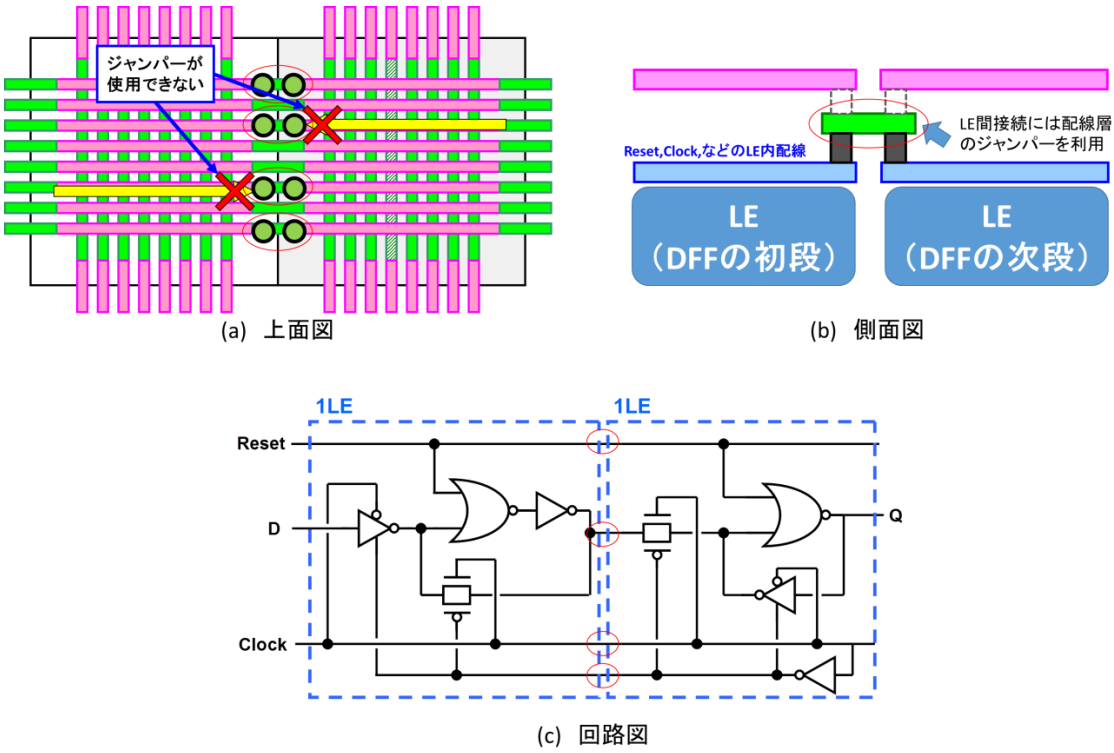


図８．３　DFF による配線トラックリソースの減少

したがって DFF 上の配線リソースは配線経路以外の目的で使用される個所が生まれる．これが配線経路最適化において多くの迂回配線を発生させる原因となる．迂回配線は理想経路を通る場合よりも多くの配線リソースを消費する．このような LE 間配線以外に使用される配線リソースが結果として順序回路の CU を低下させる原因だと考えられる．

（２）クロックツリーの消費電力

次に実機チップの再評価を行った．7 章の実チップ評価では回路を動作させた場合（状態 1）と動作をさせない場合（状態 2）の 2 状態の電流を測定したが，ここではクロックツリーのみを動作させた状態１’を新たに設定し，表８．１に示すような 3 つの状態の測定を評価した．

表８．１　測定時の状態

	電源の供給	クロック供給	入力パターン	リセット信号
状態 1	あり	あり	ランダム	OFF
状態 1’	あり	あり	遷移なし	ON
状態 2	あり	なし	遷移なし	ON

各状態で得られた電流から実装した回路の「実回路部」と「クロックツリー部」を見積もる．新たに測定を行った状態 1’は実回路部の入力遷移がなく，DFF には常にリセット信号が与えられているため「実回路部」が動作せず，クロックツリー部のみが動作することになる．したがって，各状態で得られた電流より，各部で消費している電流を見積もりことが可能である．これを表８．２に示す．

表８．２　クロックツリー部の消費電流見積もり式

		消費電流見積もり方法
動的消費電流	実回路部	電流（状態 1）―電流（状態 1’）
	クロックツリー部	電流（状態 1’）―電流（状態 2）

これら結果から見積もりを行った実回路部およびクロックツリー部の消費電力を表８．３，図８．４に示す．動作周波数や電源電圧は 7 章のチップ測定と同様の条件である．

表８．３　消費電力[mW]

	実回路部	クロックツリー部
VPEX3	0.998	1.985
ASIC	0.436	0.555

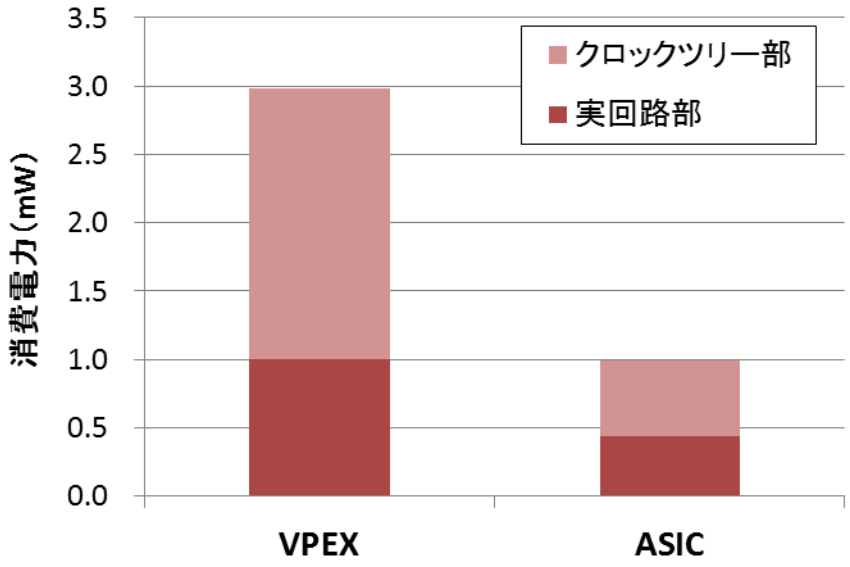


図８．４　DES 暗号化回路の消費電力

測定結果から，VPEX3 のクロックツリーの充放電動作によって消費されている電力が全体の消費電力の 2/3 以上を占めていることが判明した．また ASIC のクロックツリー部と比較すると同じ動作周波数において約 4 倍の電力を消費していることも読み取れる．したがって VPEX3 は ASIC よりもクロックツリー部の占める消費電力が支配的であることが分かる．

VPEX3 アーキテクチャでは，順序回路を実現するために LE 配置領域の周囲の領域にマスターマスク

によってクロックツリーが組み込まれる．この組み込まれたクロックツリーはセミカスタム IC 設計のものとは異なり，デザインする回路毎に 1 から CTS 設計をし直す必要がなく，あらゆる回路デザインにおいて共通の構造として用いられる．その一方で，組み込みクロックツリーはデザインによってバッファサイズや配線網を変化させることができない．DFF の配置状態に依存せず，すべて DFF のクロックピンとクロックツリー内のバッファとの接続する必要がある．これを実現するために，VPEX3 の組み込みクロックツリーはLAB全体に張り巡らせた非常に長い配線と大量のクロックバッファによって構成されている．組み込みクロックツリーの構造を図８．４に示す．図中の数値はスタンダードセルのインバータセルを１とした時の，バッファ内インバータセルのサイズ（ドライブ能力）を表している．

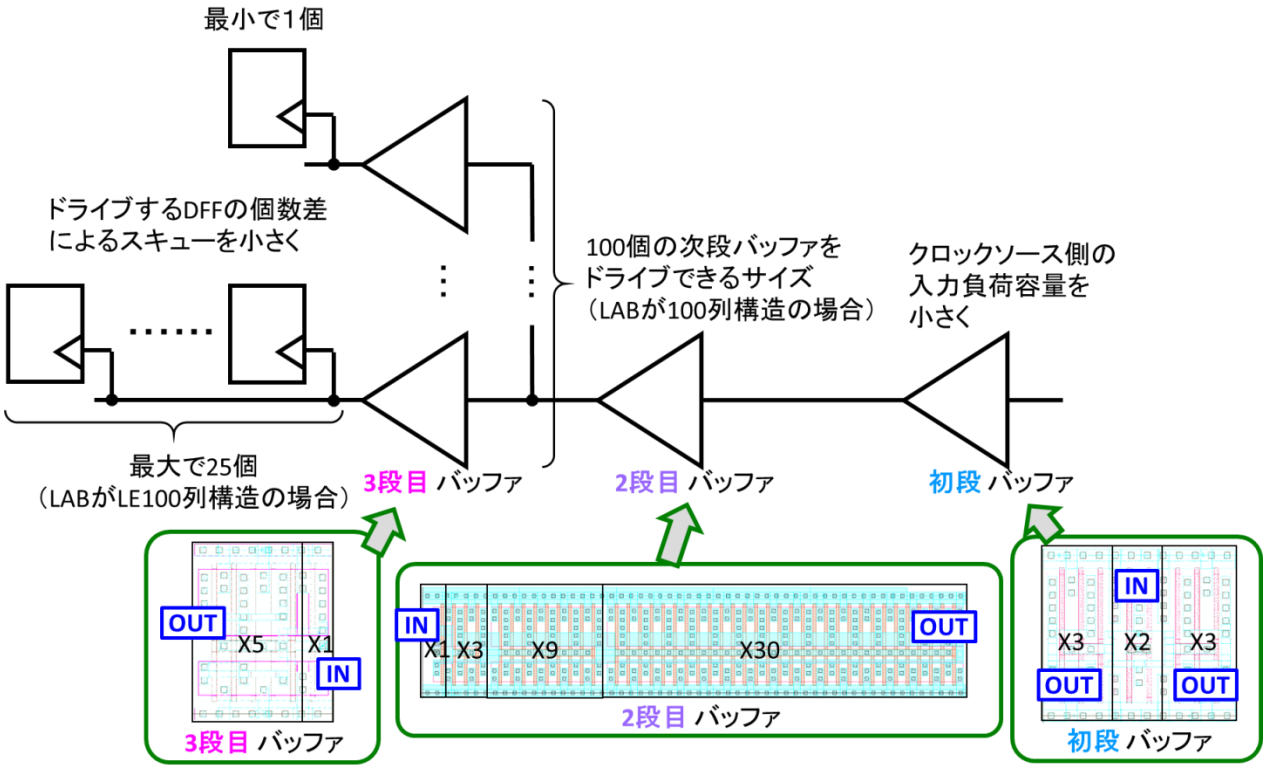


図８．５　組み込みクロックツリーの構成（LE の行列が 100×100）の場合

組み込みクロックツリーに用いているバッファは「初段バッファ」「二段目バッファ」「三段目バッファ」の 3 段階で構成されており，初段のバッファは 2 つの 2 段目バッファをドライブし，2 段目のバッファは 100 個の 3 段目バッファをドライブしている．3 段目のバッファは 1 個当たり LE 配置領域内の DFF を 0 個～25 個ドライブする．VPEX3 のクロックツリーがこのような 3 段構造になっている理由はクロックツリーのそれぞれの経路におけるの「最大遅延」と「最小遅延」の差（クロックスキュー）を小さく抑えるためである．実際に配線の寄生容量見積もりを行い，最悪条件（温度 85 度，電源電圧 1.62V，PMOS，NMOS のトランジスタモデルを共に Slow モデル使用）時のクロックスキューをシミュレーションにより調査したところ，スキューは約 0.495ns になるという結果が得られている．これは 100MHz 動作時の周期に対して 2%以下に抑えられており，十分に実用に足ると考えられるスキュー差である．

順序回路の動作中において，クロックツリーは常に動作しているため，他の回路の動作や入出力の遷移に関わらず，常に充放電を繰り返している．したがって，VPEX3 の組み込みクロックツリーはクロッ

クパルスが与えられ続けられている間，非常に大きな消費電力を発生させていることが懸念される．

図８．６は VPEX3 の組み込みクロックツリーをモデル化し，SPICE シミュレーションによって消費電力の見積もりを行った結果である．クロックの周波数は 3MHz 動作とし，GND に流れる電流から消費電力の見積もりを行った．グラフの縦軸はクロックツリー動作時の平均消費電力，横軸はクロックツリーに接続された DFF の個数を示している．またバッファごとに電流を測定している．このときの LE 配置領域のサイズは 10000 個の LE を縦に 100 個，横に 100 個並べた場合を想定している．クロックツリーモデルのシミュレーションでは Cadence 社の SPICE シミュレータ「Spectre」を用いた．

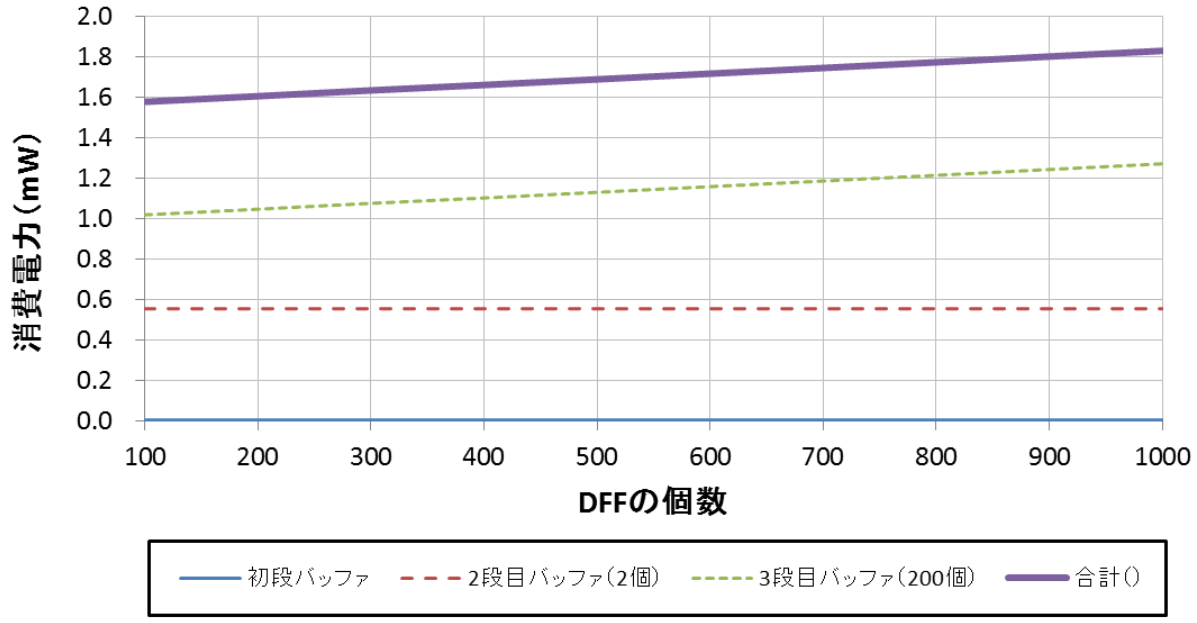


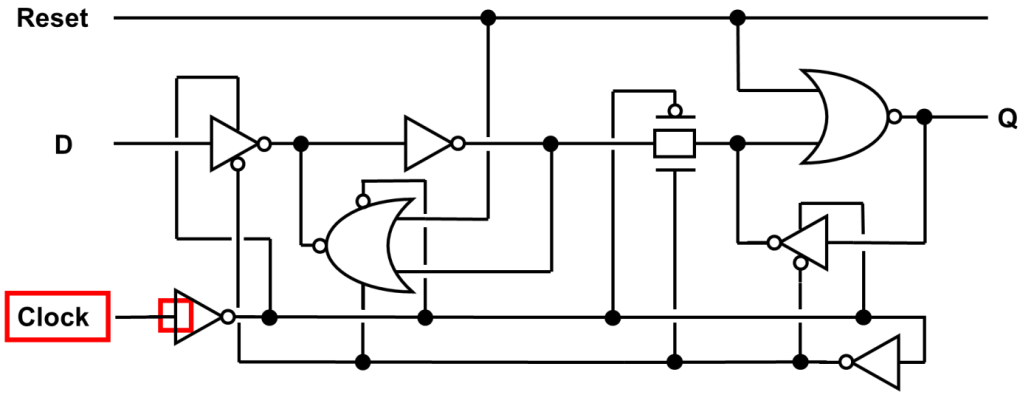
図８．６　DFF 数とクロックツリーの消費電力（クロック周波数 3MHz）

結果より，組み込みクロックツリーの合計値では 100 個の DFF が接続されたときに約 1.58mW の消費電力となった．この内，クロックツリー内部で消費電力の大きいバッファは 3 段目バッファ（200 個）の合計値が支配的であることが分かる．

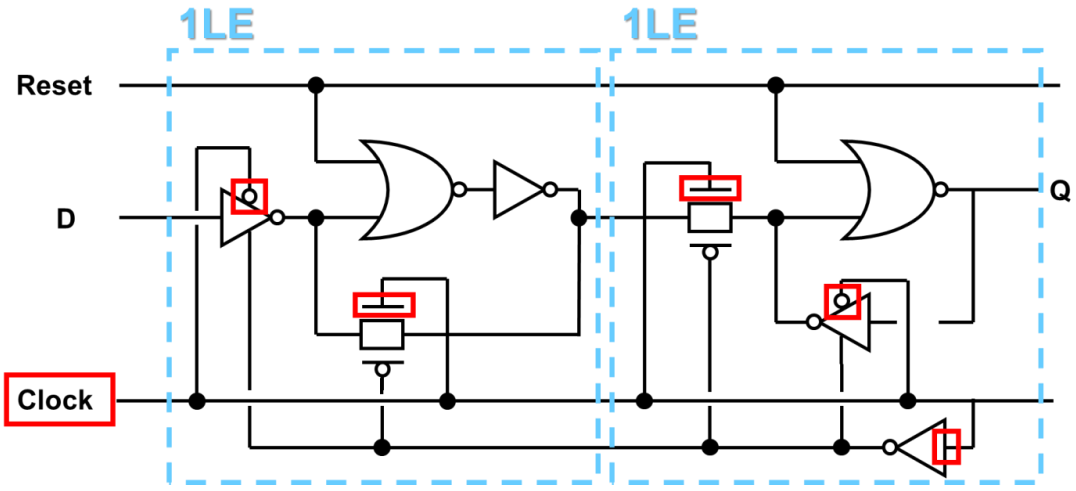
図８．８にスタンダードセルに用いられる DFF と VPEX3 アーキテクチャで用いられる DFF のクロックピンの入力容量を示す．通常の DFF の内部構造はインバータを介してクロックパルスを反転させ，逆位相のクロックパルスを生成する．その後もう一度インバータを経由することで入力時と同位相のクロックパルスを再び生成している．一方で VPEX3 アーキテクチャの DFF では入力されたクロックパルスをそのまま TG やクロックドインバータの入力として与えている．LE 内のインバータの数が足りないためにスタンダードセルと同一の構成を再現できないからである．しかし，このように外部から供給されるクロックパルスを直接利用する構造では，クロック入力端子に接続されるトランジスタの数がインバータ 1 個分だけでなくクロックインバータや TG のゲート端子も含むことになり，入力負荷容量が激増する．実際に VPEX3 のものとスタンダードセルのものを比較すると 10 倍もの負荷容量差が存在することが確認されている．これがクロックバッファのサイズを大きくしなければならない要因になってしまっている．

表　DFF の入力負荷容量

スタンダードセルの DFF	2.38fF
VPEX3 の DFF	28.91fF



（a）スタンダードセルの DFF



（b）VPEX3 の DFF

図８．８　DFF の負荷容量の比較

８．２　性能の改善案検討

本節では，前節にて考察を行った VPEX3 アーキテクチャの課題点・問題点に対する改善案・新構造案について考察する．

８．２．１　Utilization の向上案

ここでは配線処理の成功率が低いために引き起こされる Utilization 低下の対策について述べる．Utilization の主な原因は配線リソースの不足と，配線経路以外に配線リソースを使用しなければならない DFF の存在である．この問題を解決するための改良案を以降に述べる．

（1）LE 面積拡大による配線リソースの最適化

Utilization の問題を解決する単純な手法として，LE1 個あたりの配線リソースを増大させる手法が存在する．図で示すようにメッシュ・ジャンパー配線は LE の真上の領域に形成される．そのため LE1 個あたりに構成できる配線リソースは LE の面積に深く依存している．したがって，LE の面積を今よりも拡大することで配線トラックを増大させ，配線リソースを増やすことが可能になる

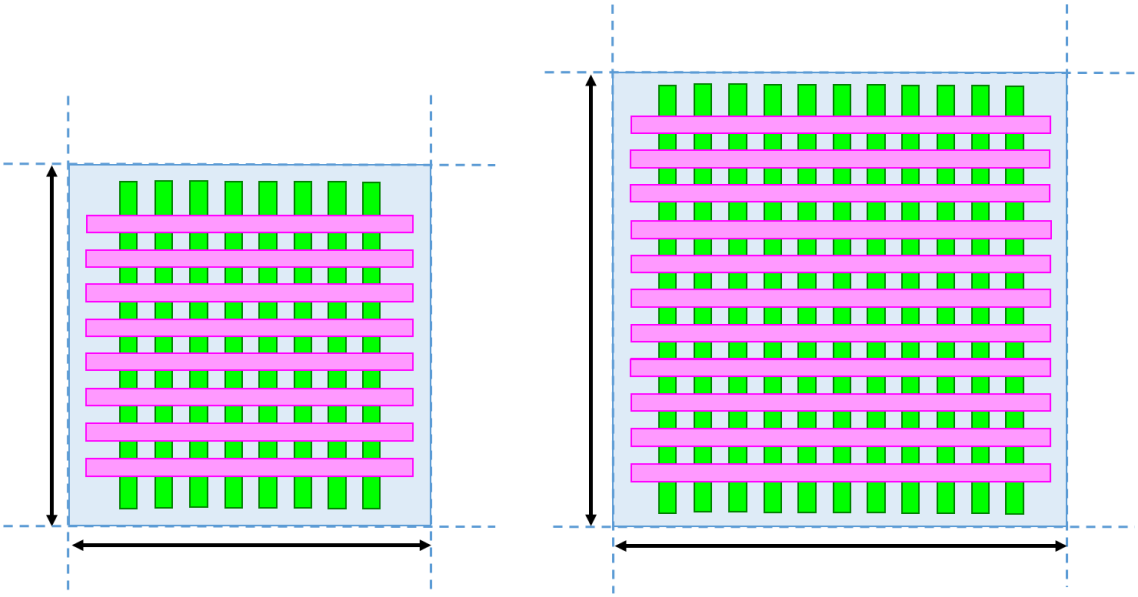


図８．９　LE 面積と配線リソース

VPEX2 から VPEX3 へ LE を改造した際は LE の面積を小さくすることに腐心した．しかしこれはメッシュ．ジャンパー配線による配線経路構築に必要となる配線リソースが LE 個当たり 8 本であっても十分であるという仮定によるものであった．

しかし CAD システムを開発し，実際に配線処理プログラムによる配線成功率の見積もりを行った結果，これが必ずしも正しくないことが分かった．そこでメッシュ・ジャンパー配線構造に用いる配線トラック数の見直し，および LE サイズの最適化を検討した． LE の面積と Utilization はトレードオフの関係にある．LE の面積を大きくすれば，より少ない LE 数で配線処理を完了させることが可能になるが，同時に LE 数当たりの回路面積も大きくなる．表８．４および図８．１０にベンチマーク回路に対して，１

LE あたりの配線リソースを縦横 8 本（VPEX3 アーキテクチャのリソース数），10 本，12 本，14 本と増やした場合の Utilization を示す．

表８．４　配線リソース/LE 毎の Utilization [%]

	8 本 (VPEX3)	10 本	12 本	14 本
s9234	52.40	97.20	97.20	97.20
s13207	25.40	65.30	95.30	95.30
s15850	33.20	71.30	95.00	95.00
s38584	29.80	74.10	96.00	96.00

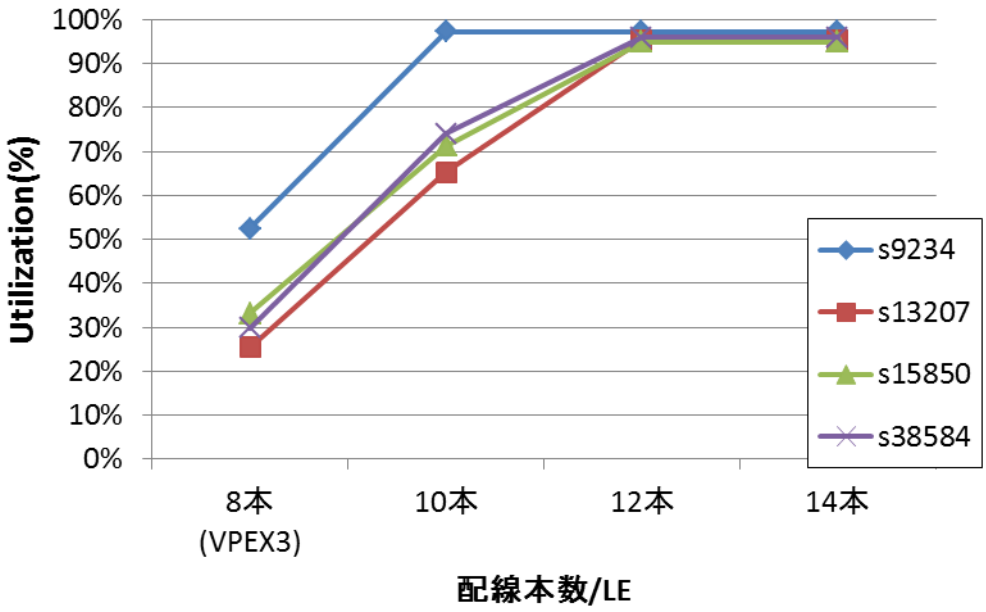


図８．１０　配線リソース/LE 毎の Utilization

図表より，LE1 個当たりの配線リソースが多いほど配線処理最適化に必要となる空論理セルの数が少なくなり，Utilization が向上していることが分かる．したがって 1 LE の配線リソースを増やすことが配線混雑度を緩和し，配線成功時の Utilization を改善できることが分かる．

次に配線リソース数毎の LE 面積の見積もりと，配線成功時の実面積の計算を行った．この実験では LE 1 つあたりの縦横長を配線トラック数に応じて定義した．まず配線トラック 8 本時の LE の一辺の長さを VPEX3 の縦横長である 6.0um と仮定した．この数値を基準にリソース数 1 本当たり縦横長が 0.56um 増加すると定義して各 LE のサイズの見積もりを行った．各配線リソースにおける LE1 つあたりの面積を表８．５に示す．

表８．５　配線リソース実現に必要な縦横長の見積もり

配線本数	縦横長[μm]	LE の面積[μm²]
8 本	6.0	36.00
10 本	7.12	50.69
12 本	8.24	67.90
14 本	9.36	87.61

最後に配線リソース毎の面積見積もり結果を示す．面積見積もりは配線成功時の配置領域に並べた LE の総数と表８．５で定義した LE 面積によって求めた．結果を表８．６に示す．また表８．６の結果を元に，LE 一個あたりの配線本数が８本のときの面積を１として，全体の結果を比で表したものを図８．１１に示す．

表８．６　配線リソース毎のベンチマーク回路面積の見積もり(μm²)

	s9234	s13207	s15850	s38584
8 本	14406.0	86400.0	72600.0	405600.0
10 本	9434.9	40950.0	40950.0	198198.0
12 本	10886.4	32289.6	35490.0	176610.0
14 本	12389.8	36748.6	40391.0	200999.0

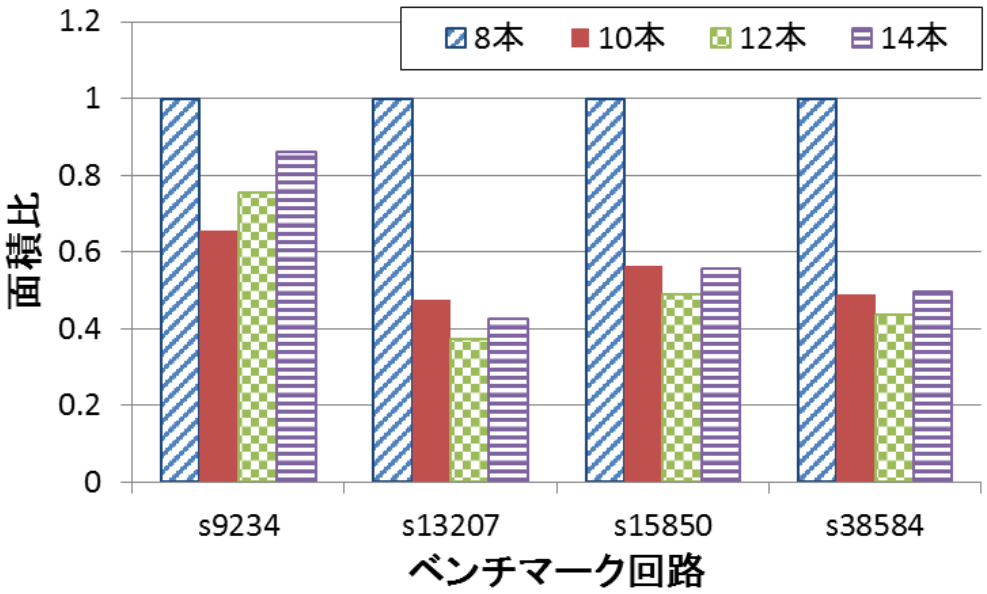


図８．１１　配線リソース毎のベンチマーク回路面積比（8 本の面積を１とした場合）

この配線リソース毎の面積見積もり結果には興味深い点がある．まず LE の配線トラックは従来の 8 本と比較して，それ以上のサイズの方が全体の面積が小さくなる．これは 1 LE あたりの配線リソースは

10 本構成以上が望ましく，8 本構成では実装面積が非常に効率の悪い方式であったことを示している．さらに 10 本，12 本，14 本の比較を行うと大規模な回路では 12 本，小規模な回路では 10 本が最も効率が良くなることが分かる．

この結果より，必要 LE 数が多くなる大規模回路を実装する際は，従来の 1 LE あたり配線リソース数 8 本構造よりも 10 本，あるいは 12 本構造の方が最適解であることがわかる．

（2） 2 LE 間の接続方法の改良

VPEX3 の LE は DFF を構成するときにジャンパー配線を使用する．そのため DFF の置かれた LE 上に配線を形成する際の配線の本数に制約がかかる．これはジャンパー配線を使用せずに隣接する LE 同士を接続する特殊配線を設けることで解決することが可能である．LE を形成する配線層を利用した構造および接続例を図８． １２に示す．

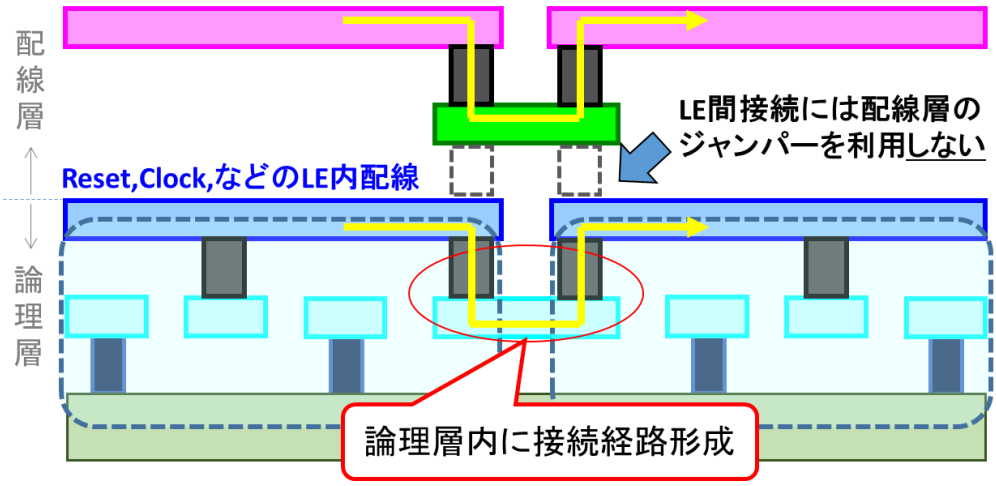


図８． １２　DFF 構成時の LE 間の配線経路

８． ２． ２　クロックネットワークの消費電力削減案

ここではクロックネットワークの膨大な消費電力を緩和する方法について考察する．クロックネットワークの低電力化は構成するクロックバッファの数を少なくすることで実現することが可能である．しかし現在のクロックバッファのバランスを崩すことはクロックスキューの増大を招き，結果として回路実現の自由度を低下させることになる．ここではクロックスキューを保ったまま消費電力を削減する方法について考えていく．

（1）DFF のゲート容量削減

スタンダードセルの DFF と同様，セル内でインバータを 2 段介したクロック信号をクロックドインバータやトランスミッションゲートの CLK 端子に接続することで，クロック入力端子の入力負荷容量を削減することが可能である．この構想の例を図８． １３に示す．この構造により，最終段バッファの充放電電力の削減が期待できる．

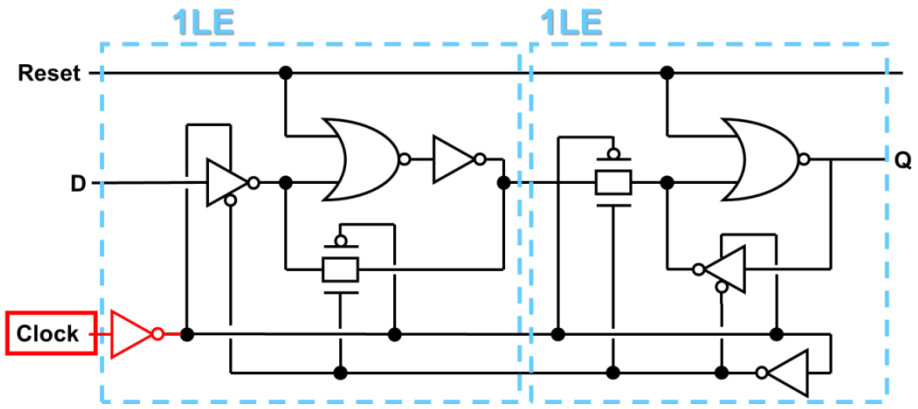
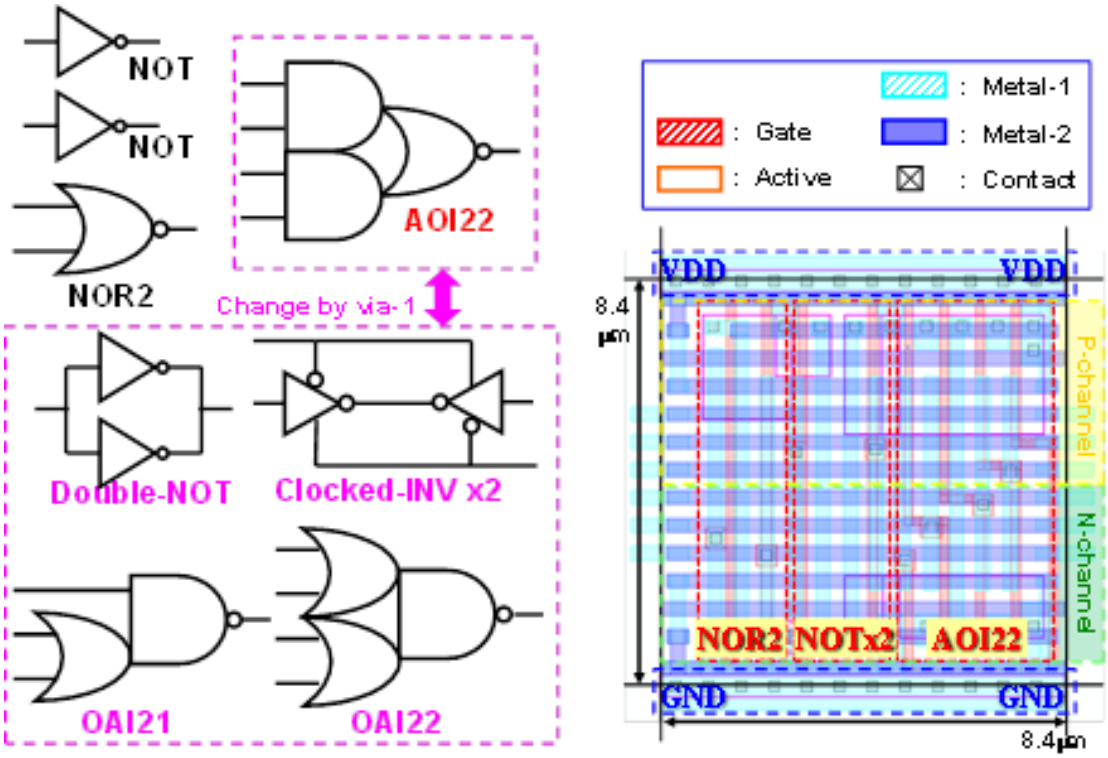


図８．１３　インバータを追加した LE における DFF の再現

これは LE を構成する INV を１つから２つに増やすことで容易に実現することが可能である．VPEX3 の LE には INV をさらにもう一つ追加できるだけのスペースが余っていないため，これを実際に実現するため LE を改造しなければならない．

８．３　VPEX4 アーキテクチャの提案

上記の改善点を組み入れた新しい VPEX アーキテクチャを提案する．このアーキテクチャを VPEX4 と呼称する．初めに VPEX4 の LE 構造について紹介する．図８，１５に LE の回路図，レイアウト図を，表８．８に VPEX3 との LE 基本性能の比較を示す．LE のサイズは VPEX3 と比較すると縦横ともに長くなっており，縦 8.4μm，横 8.4μm である．LE の面積同士を比較すると VPEX3 の 36μm²に対して VPEX4 の LE 面積は 70.56μm² となっており，約 2 倍の大きさになっている．また VPEX4 の LE の再現可能な論理ゲート素子は表に示すように 8 種類増えて 30 種類になっている．次に VPEX4 アーキテクチャにおける主な変更点・改良点を順に示す．



（a）回路図　　（b）スケマティック図

図８．１５　VPEX4 アーキテクチャの LE 構造

表８．８　VPEX3 との LE の基本性能比較

	VPEX3	VPEX4
面積	36.0μm²	70.56μm²
再可能現論理数	2 入力論理 ＋3 入力論理（12 種類）	2 入力論理 ＋3 入力論理（14 種類） ＋4 入力素子（4 種類）
DFF タイプ	可変 （LE2 個使用）	可変 （LE2 個使用）

（1）　配線リソースの拡大

VPEX4 の LE1 個当たりの配線リソースは水平／垂直方向各 1 層ずつに 12 本構造となっており，VPEX3 の各 8 本構造よりも 4 本ずつ増えている．配線構造に関しては VPEX3 アーキテクチャ同様メッシュ・ジャンパー構造を採用しており，配線アーキテクチャの大きな変更点はない．前節の配線リソース毎の面積比較において，8 本の LE よりも 12 本の LE の方がより小面積での実装が可能であることを示した．したがって配置配線を考慮した場合，VPEX4 アーキテクチャは VPEX3 アーキテクチャよりも面積性能に優れた回路の実現が期待できる．

（2）インバータ素子（INV）の追加

LE のサイズが大きくなったことで新たに素子を追加する領域が LE 内部にできた．そこで VPEX4 の LE では，VPEX3 を構成する 3 つ論理素子（AOI，NOR，INV）に加え，さらに INV を一つ追加した．これにより 2 つのことが可能になった．

1 つは 3 入力 AND，および 3 入力 OR 論理ゲートの再現である．従来のアーキテクチャでは 3 入力 NAND と 3 入力 NOR は再現することができたが，インバータが 1 つ足りず，LE1 つで AND と OR の論理ゲートを再現することができていなかった．VPEX4 では INV 素子の増加により図８．１６のような接続によって，これらのセルが再現可能になった．3 入力 AND，OR ともにスタンダードセルライブラリ利用時の論理合成において利用率が高いセルであるため，VPEX4 では更なる素子数・面積の削減が期待される．

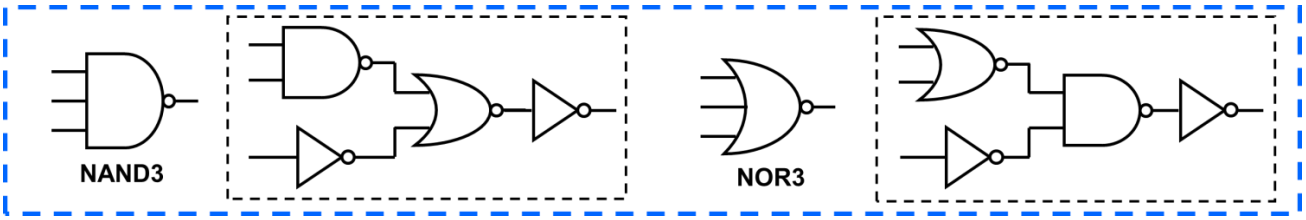


図８．１６　新しい回路構成案

2 つ目は DFF 構成の改良が可能になったことである．これは後述の DFF 構成の項目で説明する

（3）新しい Flexible-AOI の実現

従来の Flexible-AOI は 3 入力 AOI をベースとしたものであった．これに改良を加えて，4 入力 AOI をベースに OAI やクロックドインバータを構成することができる新たな Flexible-AOI を開発した．LE が 4 入力素子を再現できるようになれば，3 入力までしか再現できない LE よりも論理合成時の論理素子数の削減が期待できる．この 4 入力 Flexible-AOI の構造および切り替え可能な論理セルを図８．１７に示す. Flexible-AOI では SOP セルの他にアウトプットピンが共通のクロックドインバータ 2 つを再現することができる．このセルを利用することで，従来通り DFF を再現することができる．

また新 Flexible-AOI を利用して VPEX4 から新たに再現可能になった論理ゲート素子を図８．１８に示す. Flexible-AOI と INV を組み合わせることで 4 種類の 4 入力論理素子を再現することが可能になる．

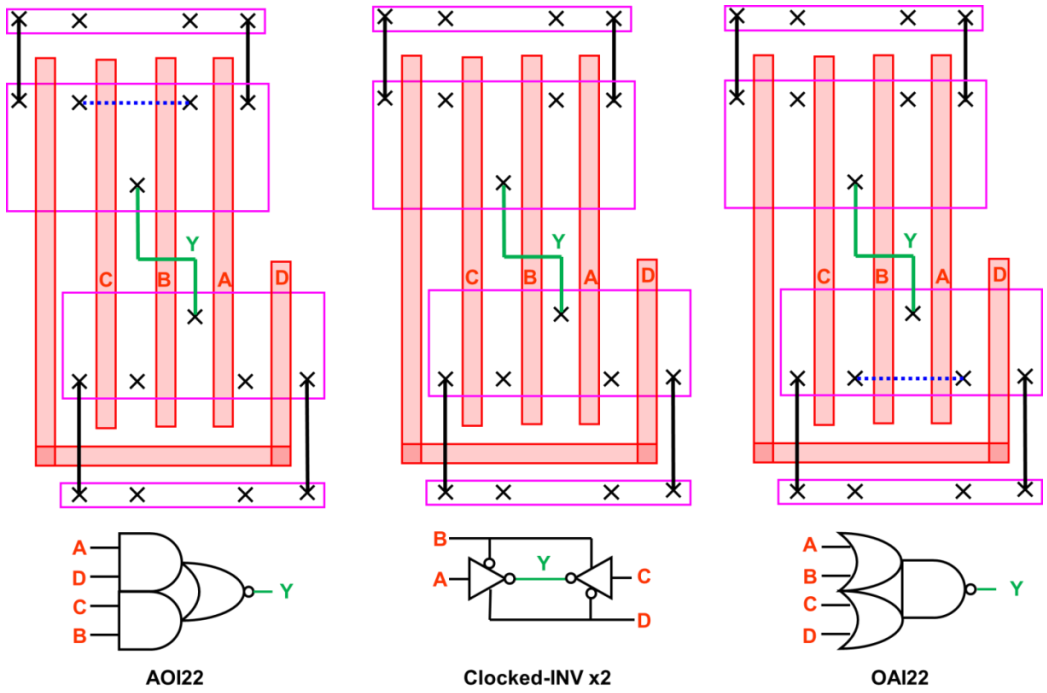


図８．１７　新たな Flexible-AOI 構造

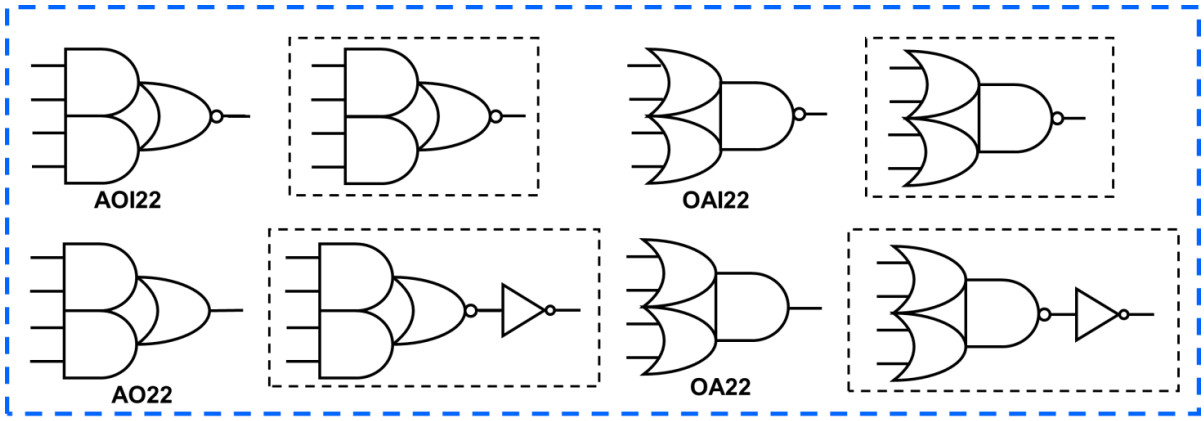


図８．１８　再現可能な 4 入力論理ゲート素子

（4）DFF の実現手法の変更

VPEX3 アーキテクチャの DFF は入力負荷容量が非常に大きいため，サイズの大きいバッファセルをクロックツリーの最終段に設ける必要があった．これはクロックツリーの動的消費電力が大きくなる原因になっていた．VPEX4 アーキテクチャでは INV 素子を 2 つに増やしたことで，入力端子を直接クロックドインバータやトランスミッションゲートに接続しない構造を形成することが可能になっている．そのため入力容量を大幅に削減することが可能になる．

図８．１９に新しい DFF を示す．また追加した INV の入力端子を DFF 構成時の入力端子とした場合の入力負荷容量の比較を表８．９に示す．VPEX3 と VPEX4 の DFF 構成時の入力負荷容量を比較すると，およそ 1/3 に削減されている．これによってクロックツリーが DFF の入出力端子を充放電する際に発生する消費電力の削減が期待できる．

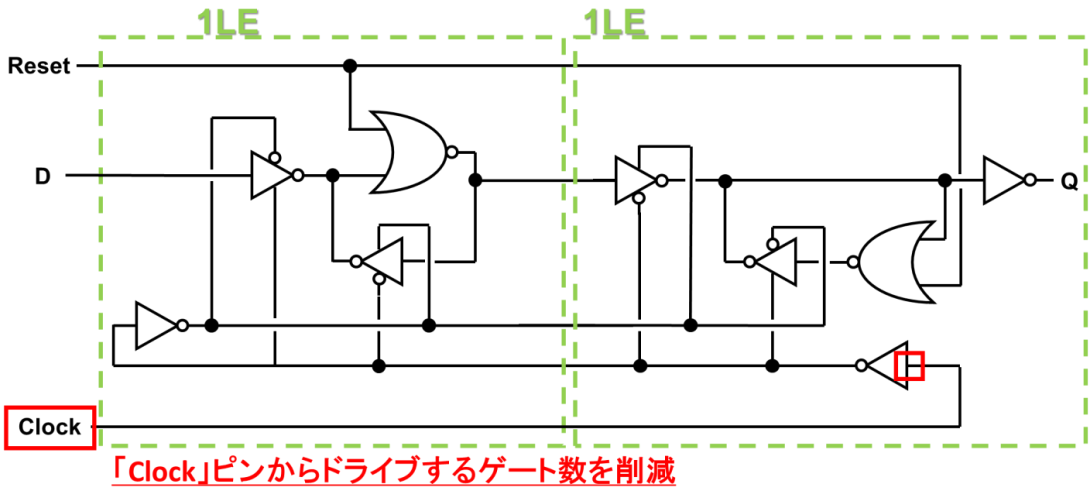


図８．１９　VPEX4 アーキテクチャにおける DFF の構成

表８．９　DFF クロック端子の入力負荷容量の違い

VPEX3	VPEX4
28.91fF	**11.65fF**

（５）DFF 再現時の２LE 間接続方法の改善

従来の DFF 再現時の LE 間接続には第 3 層のジャンパー配線を利用していいた．これによって DFF 上を水平方向へ跨ぐためのジャンパー配線のリソースが少なくなっており，Utilization の低下を招いていた．今回はこの２つの LE 間の接続を図８．２０に示すよう第１ビア層と第１メタル層によって実現できるようにした．これによって DFF 構成時に配線リソースを消費することがなくなり，配線成功率の改善が期待できる．

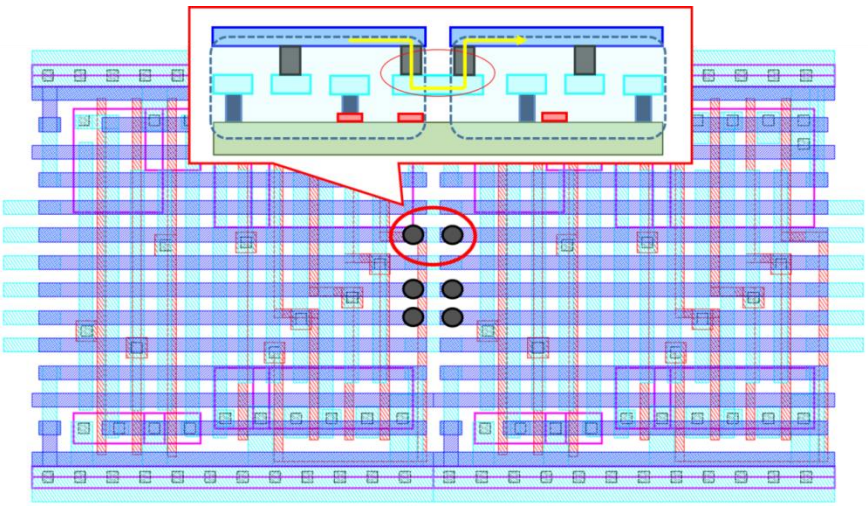


図８．２０　LE の第１メタル層の構造

（６）LAB 内のクロックラインの変更

図８．２１に VPEX3 と VPEX4 のクロック配線とクロックピンの接続方法の違いを示す．クロックツリーを経由したクロックパルスは LE 内部に張り巡らせている「ローカルクロックライン」と呼ばれる配線から供給されていた．VPEX3 において，この配線をクロックピンに接続する場合は一度第 3 メタル層のメッシュ配線を経由しなければならなかった．これはクロックと DFF の接続に配線容量やビア抵抗を発生させる原因となり，また垂直方向の配線リソースを 1 つ消費するため．配線成功率低下の要因となっていた．VPEX4 ではローカルクロックラインを LE の内側に僅かに移動させた．これによってクロック入力端子の入力ピンにあたる第 1 メタル層とローカルクロックラインが直行する構造を実現することができた．したがって，メッシュトラックを経由せずとも DFF のクロック端子とクロックツリーを接続することが可能になっている．

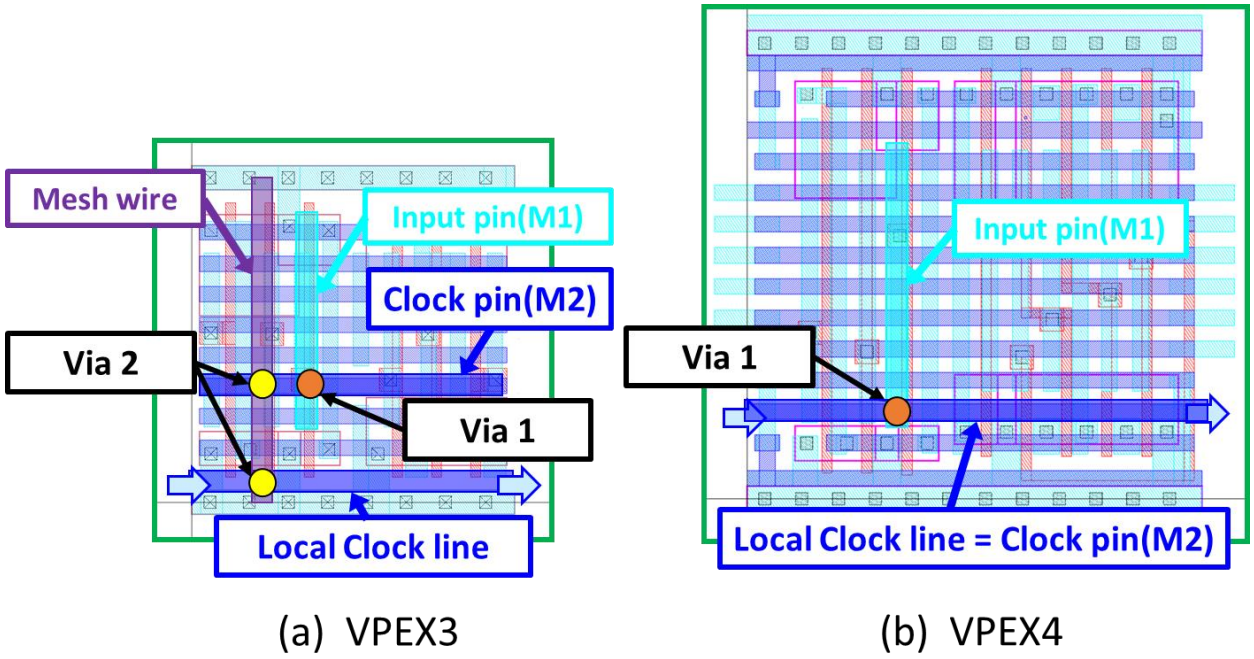


図８．２１　配線リソースを消費しない LE 間接続方法案

８．４　VPEX4 アーキテクチャの面積・消費電力評価

本節では VPEX4 アーキテクチャの性能評価を行う. この性能評価では VPEX3 用に開発を行った CAD システムに改良を加え，VPEX4 アーキテクチャの配置配線処理を可能にしたものを利用した．性能評価には 2 つの暗号回路を用いた．この性能評価では論理回路の評価とクロックツリーの消費電力評価をそれぞれ行った．

８．４．１　クロックツリーの消費電力

VPEX3 および VPEX4 におけるクロックツリーの配線容量，配線抵抗の見積もりを行い，クロックツリーの消費電力測定モデルを作成した．このモデルを使用し，Cadence 社の SPICE シミュレータである Spectre を用いて消費電力の測定を行った．結果を図８．２２に示す．

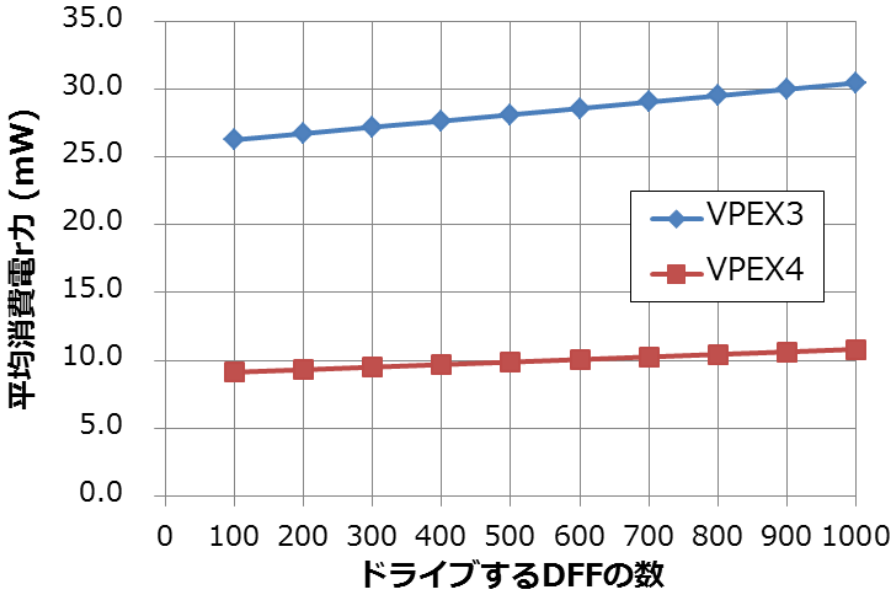


図８．２２　クロックツリーの消費電力

図８．２２の結果は動作速度 50MH z 時の消費電力を示している．図より VPEX3 ではクロックツリーの消費電力が 25～30mW であるのに対して，VPEX4 では約 10mW の消費電力に抑えられている．またドライブする DFF の個数による消費電力増加の傾きも VPEX4 のクロックツリーの方が小さい．したがって DFF の負荷容量を小さくすることでクロックネットワークの低消費電力化を実現することができたといえる．

８．４．２　暗号回路の性能評価

VPEX３および VPEX4 のアーキテクチャ毎の回路面積および消費電力の比較結果について述べる．性能評価用のベンチマーク回路として DES 暗号回路と AES 暗号回路の 2 つの回路を利用した，回路実装には ASIC，VPEX3，VPEX4 の３通りの方法を用いた．面積の比較結果を表８．１０，図８．２３に示す．

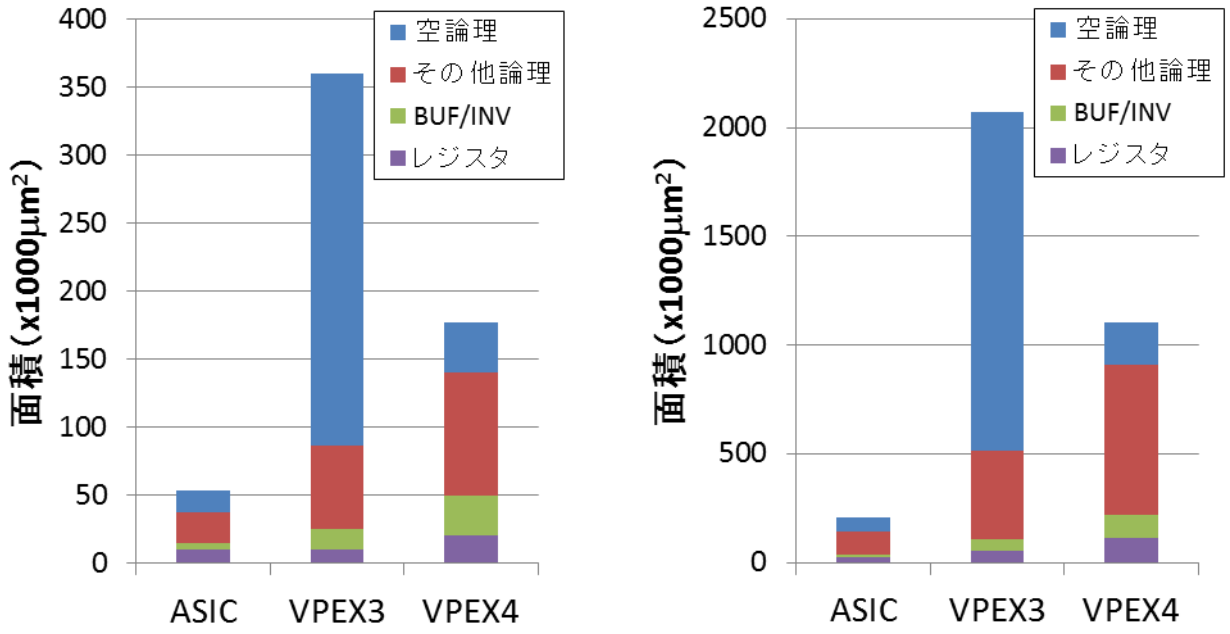
表８．１０　面積の性能評価結果（μm²）

（a）DES 暗号回路

	ASIC	VPEX3	VPEX4
空論理	15856.1	274248.0	36409.0
その他論理	22495.3	60768.0	90528.5
BUF/INV	5019.03	14904.0	29705.8
レジスタ	9483.3	10080.0	19756.8
合計	52853.8	360000.0	176400.0

（b）AES 暗号回路

	ASIC	VPEX3	VPEX4
空論理	61668.9	1560276.0	195098.4
その他論理	109051.1	405936.0	688171.7
BUF/INV	7951.1	50076.0	106898.4
レジスタ	26891.8	57312.0	112331.5
合計	205562.9	2073600.0	1102500.0



（a）DES 暗号回路　　（b）AES 暗号回路

図８．２３　面積の性能比較

今回の測定では，動作速度の制約条件はすべて 50MHz として実験をおこなった．また ASIC の配置配線時の Utilization は 70%として配置配線を実行した．VPEX3 と VPEX4 に関しては，配置配線が成功した中で最も面積の小さいくなった結果を性能評価に使用した．

結果を比較すると，DES 暗号回路，AES 暗号回路とも VPEX4 の方が VPEX3 よりも面積性能に優れた結果が得られた．DES 暗号面積においては VPEX3 実装時の面積は ASIC の約 6.8 倍であったのに対して，VPEX4 の実装では約 3.3 倍まで小さくなった．また AES 暗号回路においては VPEX3 実装時の面積が約 10.1 倍であったのに対して，VPEX4 の実装では約 5.4 倍まで小さくなった．よって VPEX4 は VPEX3 の約 1/2 倍の面積で同等の回路が実現できることが確認された．

次に消費電力の比較を行った．この比較では回路部を Synopsys 社の静的解析ツール PrimeTimePX を用いて解析し，クロックツリーの消費電力を Cadence 社の SPICE シミュレータ Spectre を用いて解析

を行った．結果を表８．１１，図８．２４に示す．なお ASIC 実装時のクロックツリーの消費電力見積もりが困難であったため，クロックツリーに関しては VPEX3 と VPEX4 の消費電力の結果のみをのせる．

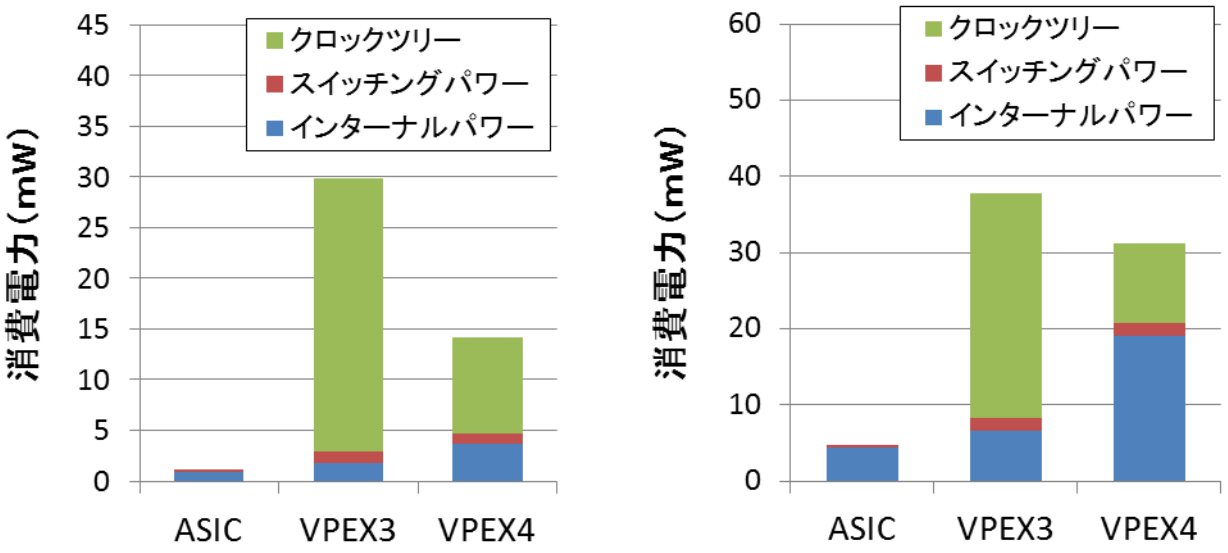
表８．１０　消費電力の性能評価結果（mW）

（a）DES 暗号回路

	ASIC	VPEX3	VPEX4
インターナルパワー	0.94	1.79	3.66
スイッチングパワー	0.26	1.10	1.08
クロックツリー	N/A	26.93	9.39
合計	1.20	29.81	14.13

（b）AES 暗号回路

	ASIC	VPEX3	VPEX4
インターナルパワー	4.36	6.63	19.14
スイッチングパワー	0.39	1.62	1.59
クロックツリー	N/A	29.54	10.45
合計	4.75	37.79	31.17



（a）DES 暗号回路　　（b）AES 暗号回路

図８．２４　消費電力の性能比較

まずクロックツリー以外の回路の消費電力を比較すると，DES 暗号回路において VPEX3 実装時は ASIC の約 2.4 倍であるのに対して，VPEX4 実装時は約 3.9 倍となった．また AES 暗号回路において，VPEX3 実装時は ASIC の約 1.7 倍，VPEX4 実装時は 4.4 倍となった．この結果より LE の消費する電力は VPEX4 の方が 2 倍以上大きいことが分かった．

次にクロックツリーの消費電力を合わせて比較を行うと，DES 暗号回路においては， VPEX4 の消費電力が VPEX3 の約 47%，AES 暗号回路においては VPEX4 の消費電力は VPEX3 の約 82%となり，低消費電力化を実現していることが分かった．

以上の面積，消費電力の性能評価結果より，VPEX4 は VPEX3 よりも性能面で優れたアーキテクチャを実現していることが分かった.

第 8 章の参考文献

[1] F.Brglez, D.Bryan, K.Kozminski, "Combinational profiles of sequential benchmark circuits", Proc. of of the IEEE International Symposium on Circuits and Systems (ISCAS), Vol.3, pp.1929-1934, May 1989.

第９章　リバースエンジニアリングの問題

リバースエンジニアリング（RE : Reverse engineering）とは，広義的には，機械の分解や製品の動作観察，ソフトウェア動作の解析などによって製品の構造を分析し，そこから製造方法や動作原理，設計図，ソースコードなどを調査・復元する行為・工程である．大規模集積回路（LSI : Large Scale Integrated Circuit）においては図９．１に示すように顕微鏡を用いて半導体や金属配線構造を観察し，各層の形状や材料から回路図や製造設備・製造工程を分析する行為を指す[1-4].

LSI においては効率的に開発を進めるために，一度開発した設計モジュールや他人が設計した設計モジュールを利用する．このような完成された機能モジュールを設計資産（IP コア : Intellectual Property Core）とよび，近年では論理演算やアルゴリズムを工夫したり，製造プロセスに合わせて最適化した様々な IP コアが使用されている．この IP コアを社外から購入して自社製品の開発に組み込むことは，近年の設計において珍しいことではない．そのため高付加価値を持った IP コアを開発する事を目的とした企業やプロジェクトが存在する．IP コアの構造やデザインの盗用および模倣半導体の存在はその IP コアを用いた LSI の製品寿命や信頼性の維持に大きく関わるとともに，IP コアの開発を専門とした企業にとって自社製品のブランドを守るための重要な問題である．したがって LSI や IP コアを RE 攻撃から保護するための耐 RE 技術の開発・研究によって LSI の模造を防ぐことは，現在の半導体市場において重要な課題の一つといえる．

本章では集積回路の RE 攻撃によって引き起こされる様々な問題・脅威やそれに対抗するための既存技術に関して議論する．

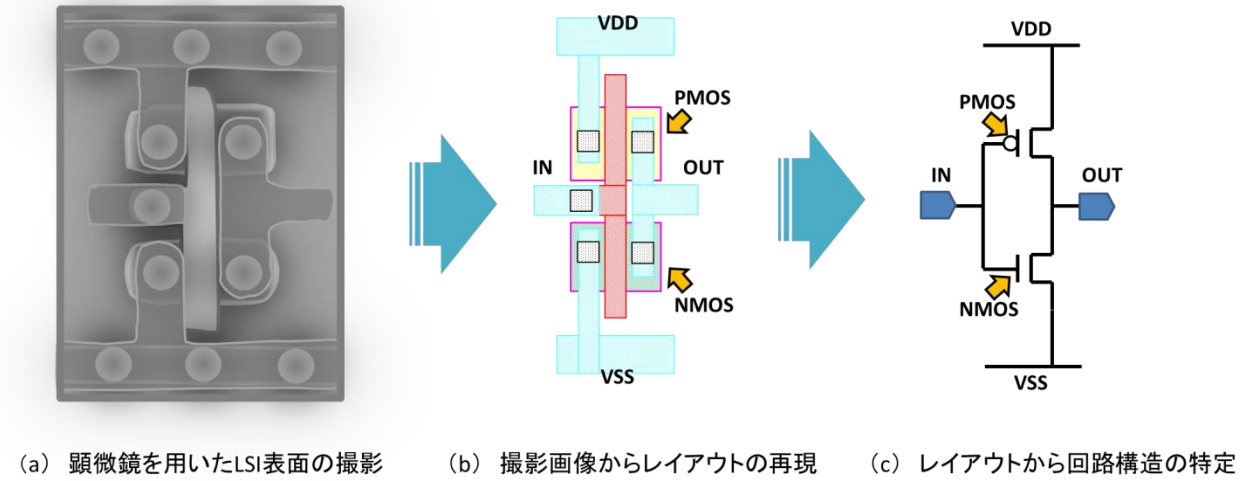


図９．１　リバースエンジニアリング攻撃の例

９．１　リバースエンジニアリング攻撃による脅威

ここではRE攻撃によって引き起こされる問題について議論する．RE攻撃を行う攻撃者の目的は2つの場合が考えられる．一つは回路構造の模倣のためである．回路構造を解析することで，回路内に存在する知的財産や技術あるいは製造に用いた材料や製造手法を解析することが目的である．現在では半導体製造を専門に行うファンダリの存在によって，半導体製造工場を持たないファブレス企業や機関が増えてきた．その為回路の設計図を手に入れることができれば，誰でも模倣LSIを製造することができるようになっている．

もう一つはLSI内部の回路が担っているセキュリティ機構を破るためである[5-7]．例えば，暗号回路の鍵を特定する攻撃を行うためにレイアウト情報・回路構造が必要になることがあり，そのためにリバースエンジニアリング技術が悪用されることがある．

９．１．１　模倣半導体の法的保護

RE攻撃によってトランジスタの位置や繋がり，材料などを解析し，そのデザイン・レイアウトをそっくりそのまま丸写しする行為をクローニングと呼ぶ．クローニングは解析を用いて得られた回路情報を製造用のレイアウトに変換する手法で，既存のLSIと同一の機能・性能を再現することができる．これによる被害は同等機能を持った模倣半導体によって製品シェアが奪われてしまうことである．

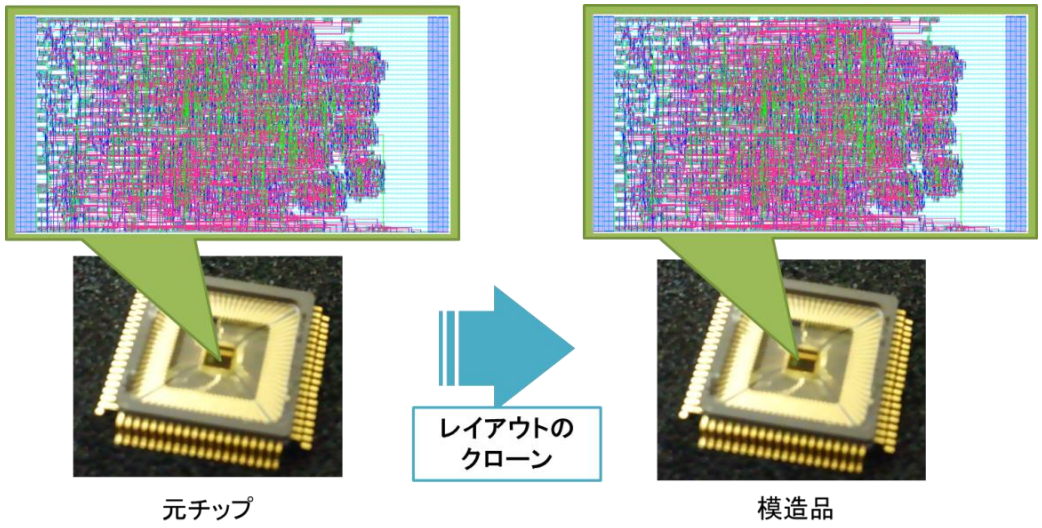


図９．２　クローニングの例

クローニングによる問題は短期的に見た上記の問題の他に，長期的に見た場合の市場モデルの破壊による半導体業界の衰退の危惧が存在する．クローニングは解析手段と製造設備さえ有していれば，LSI設計技術をもった人材やIPコアがなくともチップを複製することが可能である．これはLSI設計に携わる業界全体の成長意欲を著しく割く行為である．LSI 開発には研究開発や初期投資費用といった大きなリスクがある．これらの莫大な初期開発費を製品の価格に分散させることで回収するというモデルが現在のLSI市場の開発・販売のモデル形態であり，先端プロセスのLSI開発はこのモデルの上で成り立っ

ている．そのため莫大な開発費をより多くの製品に分散する大量生産が主流である．しかしここに模造品が混在することで，LSI の製品寿命予測や初期開発コストの回収が困難になる．そのため LSI 開発のリスクがさらに増すという事態が引き起こされる．リスクの高い市場の中では，新しい LSI を設計する技術者や組織がますます少なくなり，LSI 設計技術の成長が停滞することになる．また現在においてはファブレスの存在によって製造設備を持たずとも LSI 製造が行えるようになった．これによって製造設備を有する組織に属さなくても LSI を製造できるようになった．これは模倣半導体が誰にでも造れるようになったことを意味しており，より多様な RE 攻撃から LSI を守る必要がある．

日本においてはクローニングによる製品のデットコピーは「半導体集積回路の回路配置に関する法律（半導体集積回路配置保護法　※)」によって保護されており，実行すれば刑罰の対象となる．国内のクローニング被害は法によって保護されることで蔓延するような事態には陥っていない．しかし国外においては法律によって完全に保護されていない地域もあり，グローバル市場においては現在でもしばしば問題となっている．

※　半導体集積回路の回路配置に関する法律

法令番号 昭和 60 年法律第 43 号

一定の条件を満たす回路配置を「回路配置利用権」によって保護することを定めた日本の法律．回路配置利用権の存続期間は登録日から 10 年間．半導体集積回路の回路素子や金属配線の配置・配線パターンを保護し，適正利用を図ることで，半導体集積回路の開発を促進・経済発展に寄与することを目的としている．

９．１．２　ハードウェアアーキテクチャ模倣の脅威

クローニングと似た問題として，アーキテクチャの模倣がある．リバースエンジニアリングによって解析した LSI の各トランジスタ，抵抗素子，負荷容量素子，ダイオード，さらにはそれらの繋がり方等をレイアウトではなく回路設計情報に変換し，自動化支援（EDA：Electronic Design Automation）ツールによって異なるレイアウトの半導体製品を製造する．この行為によって，同等の機能を有した LSI をクローニングではない方法によって製造することが可能である．現状，このようなハードウェアアーキテクチャを模倣する RE 攻撃から LSI を保護する法律は存在しない[8]．EDA ツールが普及・発展のしていなかった時代ではレイアウト作成に設計時間の大部分が費やされていたが，これらのツールの進歩によりレイアウト工程は大幅に効率化された．その結果，同じ機能を有する異なるレイアウトパターンの半導体製品の製造が以前とは比べられないほど容易に作ることができるようになってしまった．このような行為はクローニングにおける短期的・長期的な問題点と同様の被害を半導体市場にもたらす危険性がある．

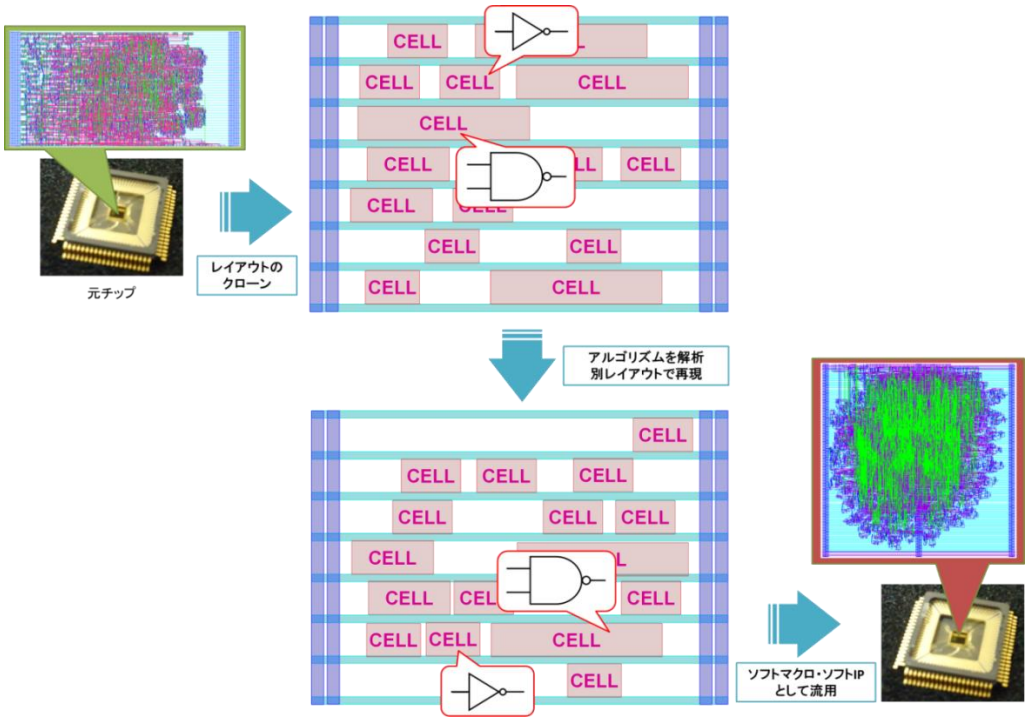


図９．３　アルゴリズムやアーキテクチャの模倣

９．１．３　回路構造解析による機密情報漏洩の幇助

LSI の用途は産業機器やコンピュータに留まらず，現在では非常に多様化している．その用途の一つとして通信の暗号化がある．通信は認証や秘密情報の交換において第 3 者に内容を傍受されない仕組みが必要であり，この暗号通信用の LSI は秘密鍵を用いて情報の暗号化と復号化を高速に行うデバイスである．さらに近年では LSI 内部に暗号鍵を保管しており．IC カードに記憶された膨大なデータ自身に対して暗号化を施して保存しておくことで，不正な手法を用いたデータ解読を防いでいる[5,6]．このような情報保護を成立させるためには，LSI 内部の保管された暗号鍵は決して知られることがないように厳重に保護する必要がある．

一般的な暗号アルゴリズムは，そのアルゴリズムが分かったとしても秘密鍵や共通鍵のような情報を知らなければ暗号文を解読できないような仕組みになっており，これによって鍵を持たない対象に対する機密性を実現している．しかし暗号アルゴリズムからではなく，そのアルゴリズムが動作する際に発生する電磁波などの 2 次情報を解析することで鍵を摂取するサイドチャネルアタック（SCA：Side Cannel Attack）[9,10]や，あえて誤動作を引き起こした時の出力信号から鍵を推測するフォールトアタック（FA：Fault Analysis Attack）[11]など，ハードウェアの副次的な情報による機密情報漏えいが近年深刻な問題となっている．さらにこれらの攻撃はハードウェアアーキテクチャや回路構造を理解していることでより効率的に行うことが可能であり，ここにリバースエンジニアリングが用いられることが指摘されている[6]．リバースエンジニアリングは SCA や FA のような直接的な攻撃ではないものの，それらの脅威をさらに引き上げるために用いられる攻撃の一つであり，情報漏えい保護の観点からリバースエンジニアリングに耐性のあるデバイスの開発が望まれている．

９．２　リバースエンジニアリングによる回路解析の手順

９．２．１　LSI のリバースエンジニアリング工程[4]

LSI の構造解析は「断面図解析」「ディレイヤリング」「パターン解析」「回路復元」の順に実行される．本節ではこれらの解析法について説明する．

（１）断面図解析

LSI のリバースエンジニアリングを行う基本的な方法の一つとして，研磨やエッチング装置を用いた層除去によって LSI の各層を露出させ，その配線パターンやスルーホール位置を特定する方法がある．この手法では LSI のパッケージを破壊し，LSI 積層を上層から順に構造解析を実行していく．

その最初の手順として，まず配線層の階層数や厚み，エッチングに用いる化学材料を特定するために LSI の断面構造に対して構造解析を行う．この解析によってメタル層やポリシリコン層の層数や材料を把握し，次の工程に必要な情報を集めていく

（２）ディレイヤリング（Delayering）

次に最上位層から順に配線層や絶縁層の剥ぎ取りと撮影を基板まで繰り返す行うディレイヤリングを行う．ディレイヤリングでは研磨，エッチング装置によって各層の全面を露出させ，光学顕微鏡や電子顕微鏡を用いてその階層の構造を画像として取得する．１回の撮影で LSI 表面全域をすべて保存することはできないため，撮影領域を分割し，それぞれを撮影することで１層分の画像が得られる．

（３）パターン解析

顕微鏡から得られた画像の明暗・コントラストなどから配線に用いられた金属パターンやスルーホールの形状や座標を特定し，各階層間の接続を明らかにする．この工程によって下層のトランジスタの接続情報が明らかになる．

（４）回路復元

特定したトランジスタと結線情報を基に回路図を作成する．これによって解析元チップの回路情報の解析が完了する．

９．２．２　自動化支援ツールによる RE 攻撃の効率化

セルベース方式によって開発された ASIC はスタンダードセルの組み合わせによって構成されている．このときスタンダードセルは論理毎にそれぞれ異なる金属配線パターンを有している．この特性を利用して，金属層解析から得られたパターンから下層のスタンダードセルを推測することで，解析効率を簡易化する手法がある[4]．図９．４のように，あらかじめスタンダードセルの金属パターンを抽出しておき RE 攻撃の用のライブラリとして登録する．そのライブラリと専用のパターン解析ツールを用いて，下層のコンタクト層やポリシリコン層を解析せずともスタンダードセルを推測することが可能である．

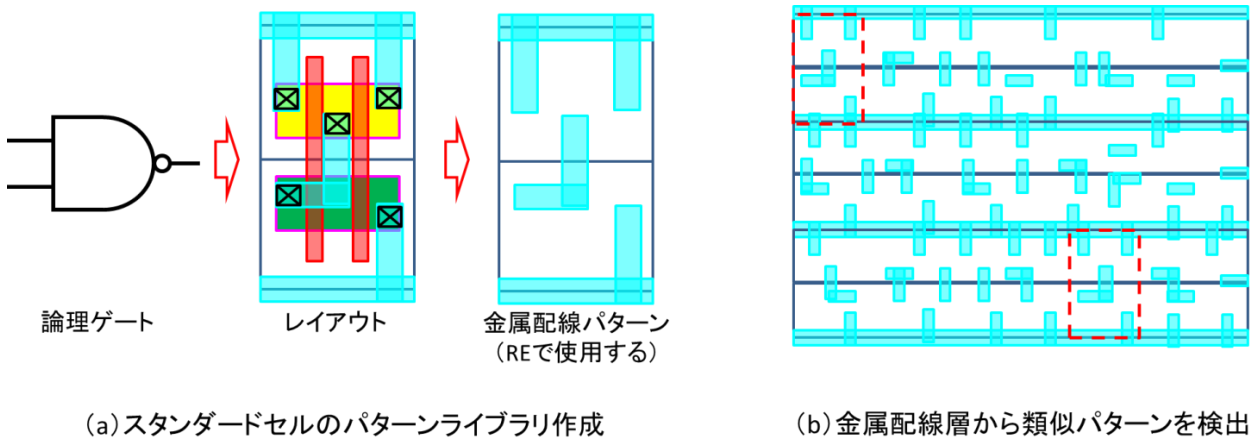


図９．４　下層配線からスタンダードセルを推測する

９．３　対策手法

RE 攻撃は対策のされていないセルベース方式によって開発された ASIC に対しては金属配線層のパターンのみを用いて，効率的に解析する手法が提案されている．その一方で，メタル層よりも下層（拡散層・ウェル層）を光学顕微鏡により特定することは困難であるため，解析コストは非常に高いものになる．したがって配線層よりも下の層に通常のスタンダードセルでは用いられない機構を設けることで，RE 攻撃に要するコストを高騰させる対策が存在する．攻撃者は経済的なメリットのために RE 攻撃を行うため，解析に必要となるコストを上げることが RE 耐性を高めることに直結する．本節では RE 耐性を向上させる既存提案手法をいくつか紹介する．

初めに解析が困難になるように金属配線の解析だけでは回路の構造を把握できないようにして ASIC を設計する耐 RE 設計について２つ報告する．次に ASIC ではなくプログラマブルデバイスの一種である FPGA を用いた RE 対策デバイスについて報告する．

９．３．１　Well ドープを利用した耐 RE 設計

通常の MOS トランジスタは N-well 上に P 型半導体，P-well 上に N 型半導体を形成する．半導体のプロセスでは well 層と同タイプの拡散領域を形成してしまうと，well 層と拡散層が導通してしまう．しかしこれを逆に利用することでゲート電圧によらず常に導通したデバイスを形成することが可能になる[12]．図９．５（b）にポリシリコンゲートの真下に拡散層と同型の well を形成し，ゲートの電圧によらず常に導通するように改変されたトランジスタを示す．

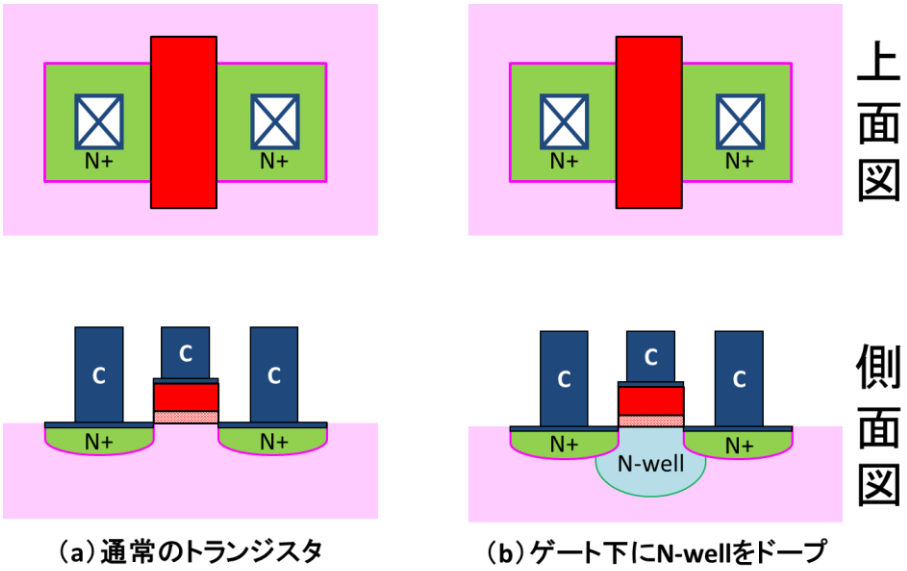


図９．５　N-well ドープによる偽 MOS トランジスタの再現

この構造はゲート層までをリバースエンジニアリングした時点では，図（a）に示した通常のトランジスタと判別かつかない．しかし図（b）はゲート電圧によらず，常に導通している．したがって，この構造を用いてスタンダードセルを偽装し，LSI 内に混載させることで金属配線パターンからの解析を不可能にする．したがって RE 攻撃時のコストを金属配線解析レベルから Well 解析レベルまで引き上げることになる．

この手法の特徴として，回路のほんの一部分にこの構造を入れておくだけで，非常に高い RE 耐性を回路に持たせることができる点があげられる．攻撃者にこの構造が入っていることを認識させることで，すべてのトランジスタに対して Well レベルの解析を強制することが可能になり，解析コストを大きく向上させることが可能になる．

９．３．２　拡散抵抗を利用した耐 RE 設計

現在の MOS トランジスタ製造プロセスでは拡散層の上部にはシリサイド（Silicide）と呼ばれる物質に覆われている．シリサイドとはゲートや拡散層上に形成される金属とシリコンの化合物の名称であり，ゲートおよび拡散層の抵抗を下げるために用いられる．通常の拡散領域の抵抗率が $10^{-5}\Omega \cdot m$ であるのに対して，シリサイド化された場合は $10^{-6}\Omega \cdot m$ と格段に小さくなる．したがって，シリサイド化された拡散領域とされていない拡散領域とでは抵抗に大きな違いがある．この特性を利用し，あえて拡散抵

抗を設けないことでシリコン基板上に抵抗器を形成することが広く知られている．これを拡散抵抗という．拡散抵抗は N+型あるいは P+型によって形成される．

図（a）は N+拡散を用いて作られた拡散抵抗である．この時左右の領域は拡散抵抗を介して導通している．ここで図（b）のようにシリサイドが形成されていない拡散層のドープ材料を変更し，P+拡散に変更する．すると拡散領域が分断され，左右のシリサイドが形成された領域が互いに非導通状態になる．通常拡散領域の N+/P+型を製造後に判別することは非常に困難であることが知られている．したがって，図に示した構造はリバースエンジニアリング時には同一の構造であると判別される．しかし実際は左右の領域が導通している場合と非導通の場合の 2 通りの状態が考えられる．これを利用して，図（a）を接続関係のあるトランジスタ間に，図（b）を非接続関係のあるトランジスタ間に用いることで，回路の接続情報を混乱させ，RE 攻撃によって容易に回路構造を解析・推測させない LSI を形成することが可能である．

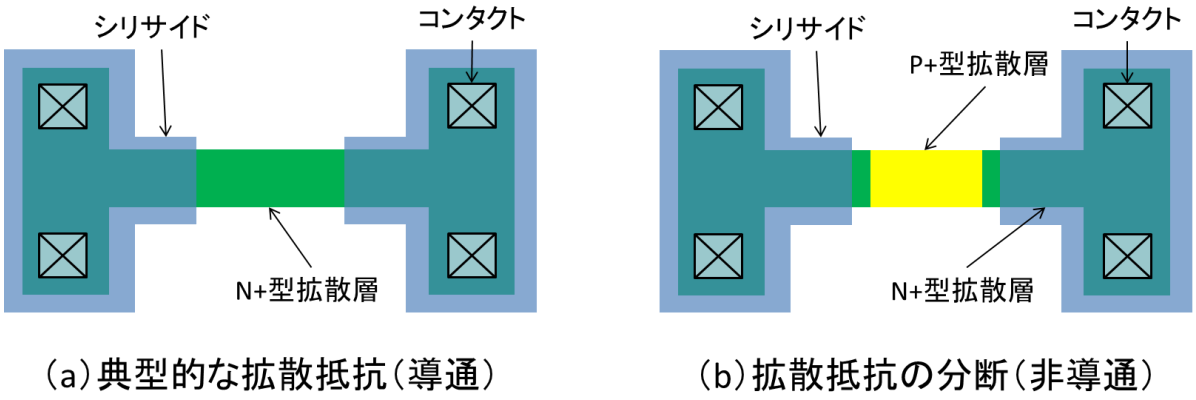


図９．６　拡散抵抗を利用したドープ材料の N+/P+による導通・非導通制御

９．３．３　不揮発性 FPGA デバイスの利用

フィールドプログラマブルゲートアレイ（FPGA : Field Programmable Gate Array）のようなメモリを使用して配線経路を決定するデバイスは，RE 攻撃によって実装された回路構造を特定することはできない．

SRAM 型 FPGA などの揮発性メモリを用いた FPGA は起動の後にコンフィギュレーションメモリから回路構成用のビットストリームをロードすることで自動的に論理回路を形成することが可能である．しかしながら，このときコンフィギュレーションメモリと SRAM メモリインターフェースとの間に流れるビットストリームを盗聴することで回路構成情報をコピーすることや，誤情報を混入させることで構成回路の信頼性を低下させるなどの悪意ある攻撃を受ける危険性が指摘されている[14].

そのため，回路情報をデバイス内の不揮発性メモリに保存しているアンチフューズ型 FPGA やフラッシュメモリ型 FPGA 用いた耐リバースエンジニアリングデバイスが提案されている[14]．これらのデバイスは金属配線層やポリシリコン層に違いがない．それゆえ高い RE 耐性を有しているといわれている[14].

第 9 章の参考文献

[1] L. R. Avery, J. S. Crabbe, S. Al Sofi, H. Ahmed, J. R. A. Cleaver, and D. J. Weaver. “Reverse Engineering Complex Application-Specific Integrated Circuits (ASICs)”, Proceedings of Diminishing Manufacturing Sources and Material Shortages Conference (DMSMS 2002), March 2002.

[2] Nohl, K., Evans, D., Starbug, Plotz, H. “Reverse-Engineering a Cryptographic RFID Tag”, Proceedings of the 17th USENIX Security Symposium, 2008.

[3] Torrance, R., James, D. “The State-of-the-Art in IC Reverse Engineering”, Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol.5747, pp.363-381. Springer, Heidelberg (2009)

[4] Randy Torrance and Dick James, “The state-of-the-art in semiconductor reverse engineering”, In the Proc. of ACM/EDAC/IEEE, 48th Design Automation Conference (DAC), pp.333–338, June 2011.

[5] 情報処理推薦機構（IPA），“平成 11 年度 スマートカードの安全性に関する調査 調査報告書”，https://www.ipa.go.jp/security/enc/smartcard/sc.html，2 月 2000 年,

[6] 電子商取引安全技術研究組合，“「システム LSI チップのセキュリティ評価」に関する調査研究報告書”，http://www.meti.go.jp/policy/netsecurity/docs/cc/lsi.pdf，3 月 2003 年

[7] 中田量子，“ハードウェア脆弱性評価技術の最新動向”，
http://www.ipa.go.jp/security/event/2013/ist-expo/documents/preso14.pdf，5 月 2013 年

[8] 東京理科大学大学院，“集積回路の設計資産（IP）の法的保護”，
http://most.tus.ac.jp/mip/column/detail.php?i=490，7 月 2011 年

[9] K. Gandolfi, C. Mourtel, F. Olivier, "Electromagnetic analysis: concrete results", CHES2001, pp.251-261, 13-16 May 2001.

[10] Paul Kocher, Joshua Jaffe, Benjamin Jun, “Differential Power Analysis”, Advances in Cryptology — CRYPTO’ 99, LNCS, Vol.1666, pp 388-397, Dec. 1999.

[11] D. Boneh, R. A. DeMillo, R. J. Lipton, “A New Breed of Crypto Attack on Tamperproof Tokens Cracks Even the Strongest RSA Code”, 25 Sep 1996.

[12] エイチアールエル ラボラトリーズ，エルエルシー，“ウェル注入を用いた集積回路の改変”，特表 2006-510225，3 月 2006 年

[13] エイチアールエル ラボラトリーズ，エルエルシー，“リバースエンジニアリングを防ぐための導電性チャネル擬似ブロック処理方法及びその回路”，特開 2010-118688，5 月 2010 年.

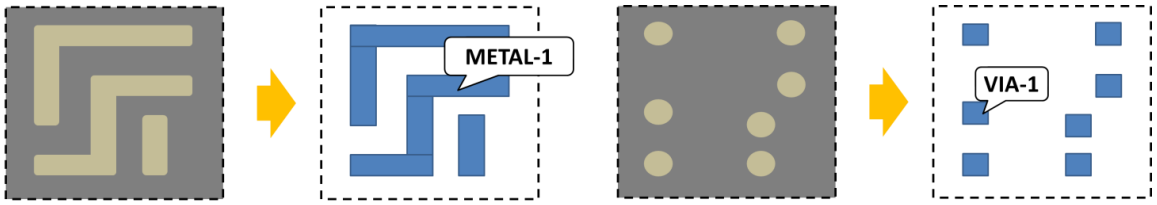
[14] Mohammad Tehranipoor, Cliff Wang, “Introduction to Hardware Security and Trust”, Springer, New York, Sep. 2011

第 10 章　DPD アーキテクチャ

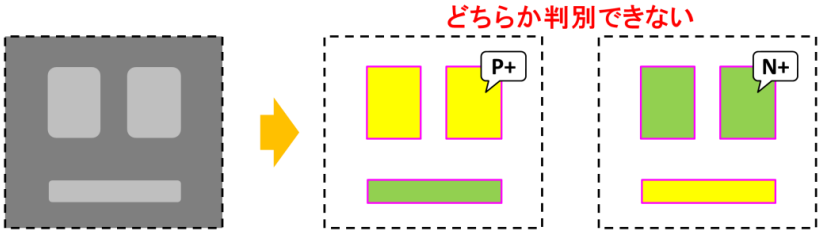
ここではリバースエンジニアリング（RE：Reverse Engineering）耐性を有するデバイスとして開発したディフュージョンプログラマブルデバイス（DPD：Diffusion Programmable Device）の詳細について報告する．DPD アーキテクチャは拡散層をカスタマイズすることで任意の論理回路を生成するロジックエレメント（LE：Logic Element）を用いたマスクプログラマブルデバイス（MPD：Mask Programmable Device）である．この DPD は Diffusion Programmable ROM（DP-ROM）とルックアップテーブル（LUT：Look-up Table）によって形成される．本章では DPD の構造や RE 耐性を持つ根拠などを論じる

１０．１　拡散層の RE 耐性

図１０．１の（a）や（b）のように，パターン転写とエッチングによって形成された金属配線層はリバースエンジニアリングによってパターン形状を容易に特定されてしまう．しかし拡散層においては拡散領域の大きさや形状を特定することは可能であっても，図１０．１（c）のように，その拡散領域に注入したイオンの種類，すなわち N+/P+型の判別を行うことは容易ではないとされている．したがって，形状を変化させず，拡散領域の型だけを切り替えることで論理機能を変更できるデバイスは高い耐タンパ性を有する．



（a） メタル配線層のリバースエンジニアリング　　（b） ビア配線層のリバースエンジニアリング



（c） 拡散層のリバースエンジニアリング

図１０．１　拡散層のリバースエンジニアリング耐性

１０．２　DP-ROM

図１０．２に N+型と P+型の切り替えによる導通の有無を示す．MOSFET ではウェル層や基板そのものを特定の電圧に印加させる場合，同型の拡散層を形成して電圧を与える．これによって N 側を高電圧，

P 側を低電圧に保ち N+/P+拡散領域と n-well/p-sub 領域を分離している．ここで n-well/p-sub 層と同型の拡散層を形成することで，逆に基板やウェルに印加された電圧を取り出すことが可能になる．図１０．２に拡散領域の型と形成する n-well/p-sub 領域の違いによって，電流の導通・非導通が変化することを示す．これによって p-sub 上の P＋拡散領域からは VDD 電圧，n-well 上の N+拡散領域からは VSS 電圧を得ることができる．これを利用して ROM を造ることができる．

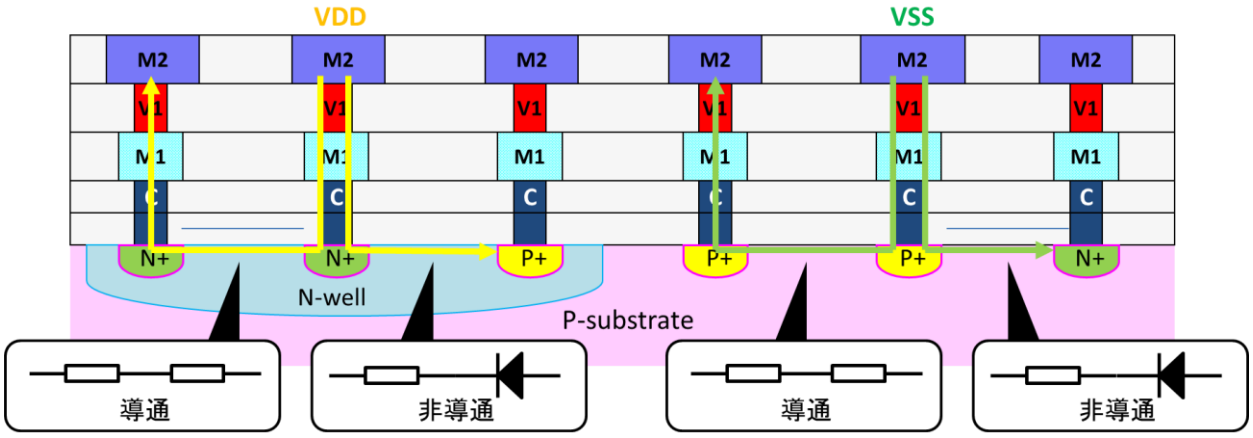


図１０．２　拡散層の型の違いによる導通・非導通の違い

図１０．３に拡散層にドープした型の違いによって実現した ROM の例を示す．図中の破線で囲われた拡散層がプログラム領域であり，製造時にドープする M+/P+を変えることで任意の 1bit を再現し，OUT 端子からその値を取り出すことができる．図（a）の例では論理１の場合を示している．この場合２つのプログラム領域を両方とも N+型にドープする．すると P-sub 上の N+拡散と P-sub は逆バイアスによってフローティング状態になる．一方で n-well 上の N+拡散は n-well と接続関係にあり，また n-well を VDD に固定していることから n-well を介して VDD と接続されている．したがって OUT 端子は VDD に保持され，出力論理は１となる．（b）では同様にして VSS に固定された p-sub と P+拡散が接続され，n-well 上の P+拡散がフローティング状態にあるため OUT 端子は VSS に保持され，出力論理は 0 となる．

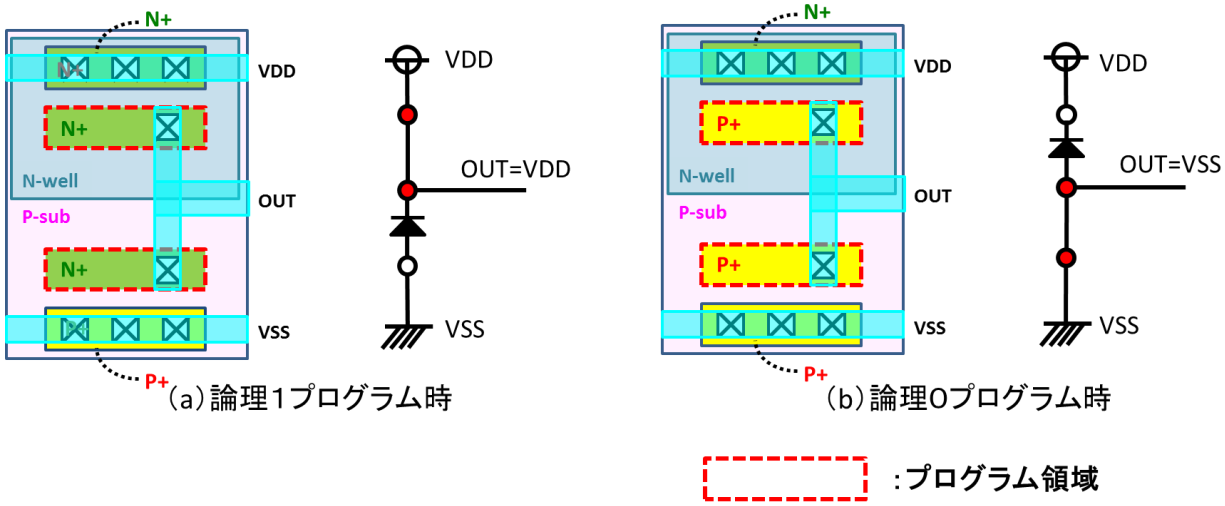


図１０．３　DP-ROM の構造図

このように金属配線層や拡散層などの形状を一切変えずに，ドープする N+/P+型を変更するだけで OUT 端子の出力を任意に変更することが可能になる．このようにして拡散領域のみをプログラムして ROM を実現できることから，このデバイスを Diffusion Programmable ROM （DP-ROM）と呼称している．この性質を利用することで様々な素子を再現することができる．

１０．３　リバースエンジニアリング耐性を持ったデバイス

本節では DP-ROM を用いて実現したプログラマブルデバイス，DPD を説明する．DPD は論理を構成する際と，配線を構成する際に DP-ROM を利用する．

１０．３．１　論理のリバースエンジニアリング対策案

DP-ROM とトランスミッションゲート（TG : Transmission Gate）を用いたマルチプレクサ（MUX : multiplexer）を組み合わせることで LUT を再現することが可能である．この回路は 2 つの入力の組み合わせにおける出力パターンを DP-ROM で定義することで，任意の 2 入力論理素子を再現する．DP-ROM を用いて実現した LUT（DP-LUT）の回路図を図１０．４に，実際に作成したレイアウトを図１０．５に示す．また，DP-ROM を定義して再現した１入力，２入力論理素子の例を図１０．６に示す．

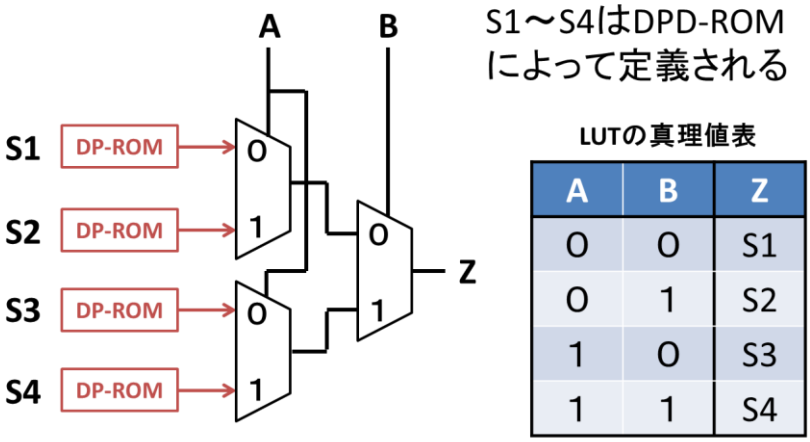


図１０．４　DP-LUT の構造

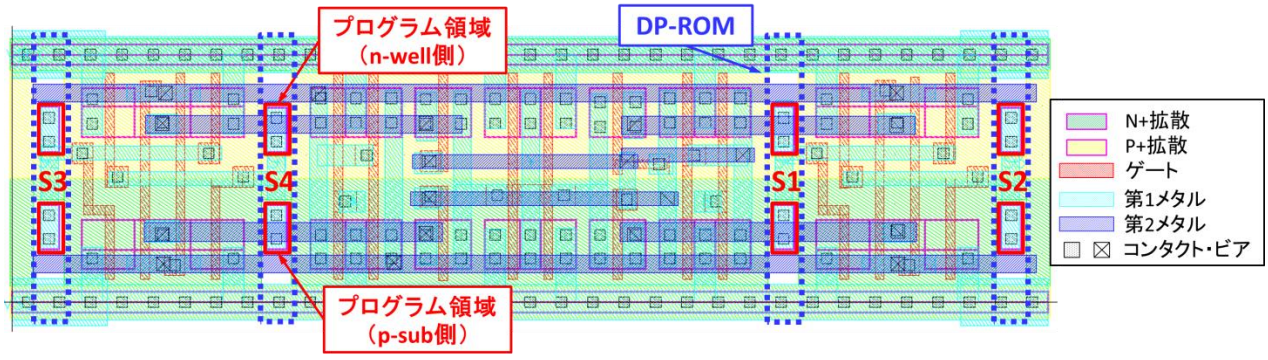


図１０．５　DP-LUT のレイアウト

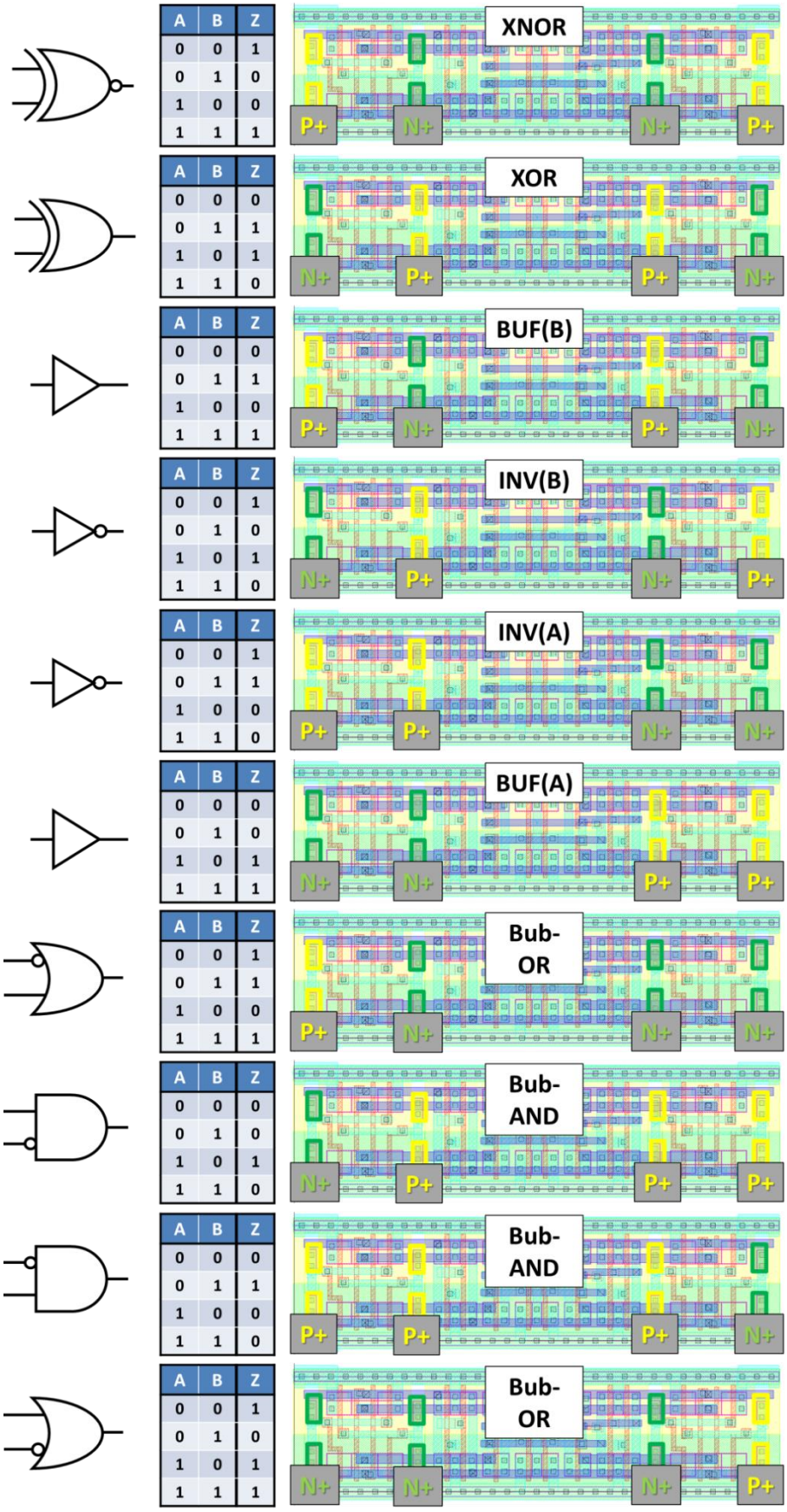


図１０．６　DP-LUT における 2 入力論理素子の再現例

図１０．６以外にも AND，NAND，OR，NOR 素子などのすべての 2 入力論理素子を再現することができる．

この DP-LUT のみを用いて構成した論理回路は金属配線層のパターンから論理素子間の接続が判明したとしてもその論理素子（LUT）の持つ論理機能は隠ぺいされている．そのため論理回路の構造を推測することが極めて困難になる．図１０．６の例に挙げた回路はすべてこの拡散領域の N+ / P+が異なるだけで，全階層のパターン形状が同一である．

また図１０．７に示すように，DP-ROM をマルチプレクサの入力端子ではなく信号選択端子と接続することで，2 つの配線経路のうちどちらか一方を常に導通させる配線セレクタ（selector）を再現することが可能になる．この配線セレクタを用いることで DP-LUT と DFF を組み合わせた FPGA のなどに用いられている Logic Element を構成することが可能になる．この回路の構成例を図１０．８に示す．

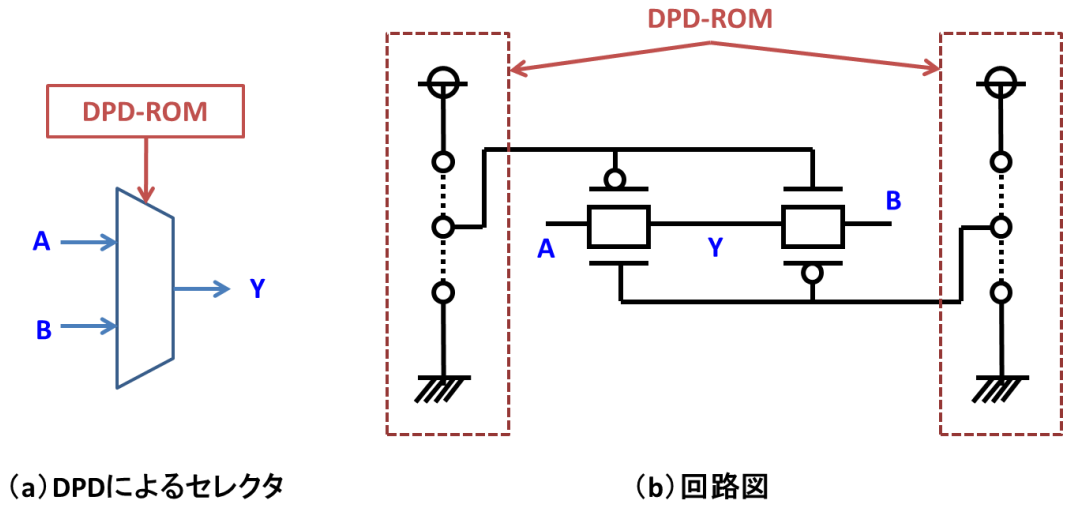


図１０．７　DP-ROM を用いたセレクタ素子

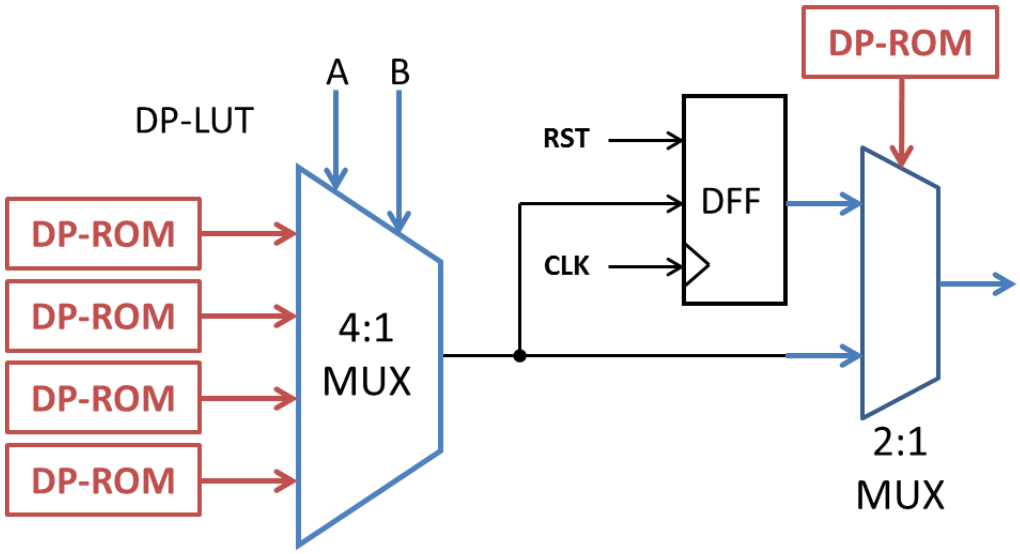
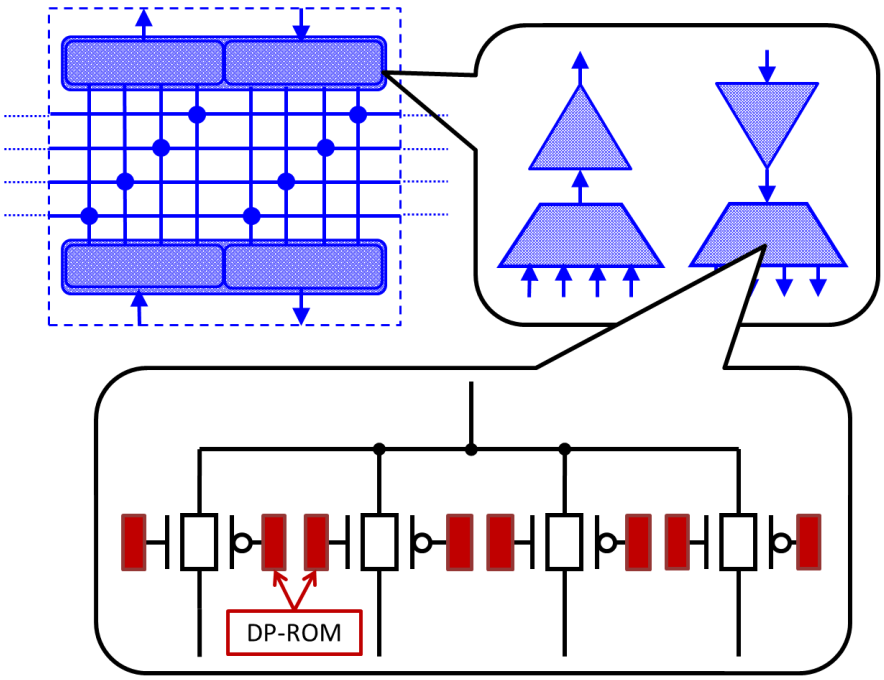


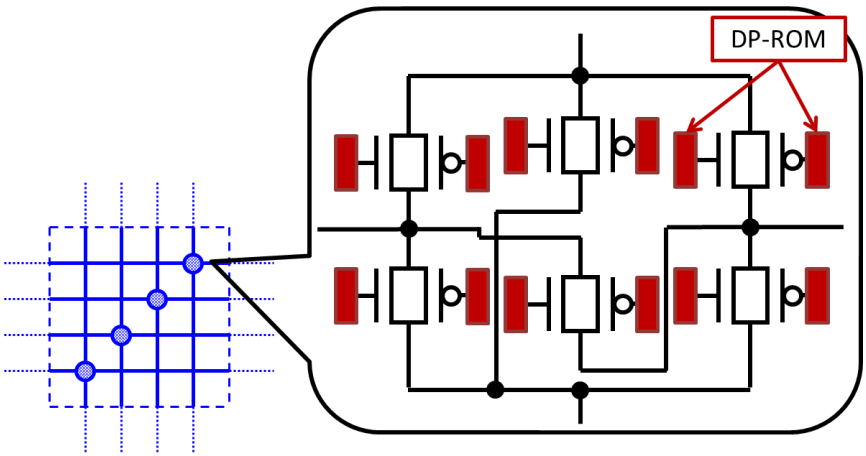
図１０．８　DP-LUT，DFF，セレクタを組み合わせた Logic Element

１０．３．２　配線のリバースエンジニアリング対策案

回路構造の解析をより困難にするためには LUT や LE の RE 対策だけでなく，素子間の接続を偽装することも効果的である．前述した DP-ROM のセレクタを利用して，FPGA のスイッチブロック（SB：Switch Block）[1]やコネクションブロック（CB：Connection Block）[1]を作成することができる．下記に DP-ROM を用いた SB と CB の構成例を示す．CB はセレクタの他にデコーダ（decoder）が必要になる．デコーダの構成はマルチプレクサに用いた構成をそのまま用いることで，構成することが可能になる．



（a） コネクションブロック



（b） スイッチブロック

図１０．９　DP-ROM を用いた配線アーキテクチャ

第 10 章の参考文献

[1] 末吉敏則，天野英晴，“リコンフィギャラブルシステム”，（社）オーム社，東京， 8 月 2005 年.

第１１章　DP-LUT のチップ試作と検証

本章では DP-LUT の動作確認のために試作した評価用チップについて述べる．試作したチップには 3 種類の異なる論理が実装された DP-LUT と論理 1 論理 0 にそれぞれプログラムした DP-ROM が搭載されている．

初めに試作チップのレイアウトや実装された回路の詳細について説明し，試作されたチップに対する動作検証結果について報告する．次に走査型電子顕微鏡（SEM：Scanning Electron Microscope）を用いてリバースエンジニアリング（RE：Reverse Engineering）を行った結果に関して報告する．

１１．１　DP-LUT のチップ試作と動作検証

DP-LUT の動作検証と RE 耐性評価のために，チップを試作した．本試作チップは東京大学 VDEC[1] から提供されている Rohm180mm プロセスルールによって設計，製造がおこなわれている．図１１．１に試作チップの全体図，図１１．２に拡大図と配置の詳細を示す．

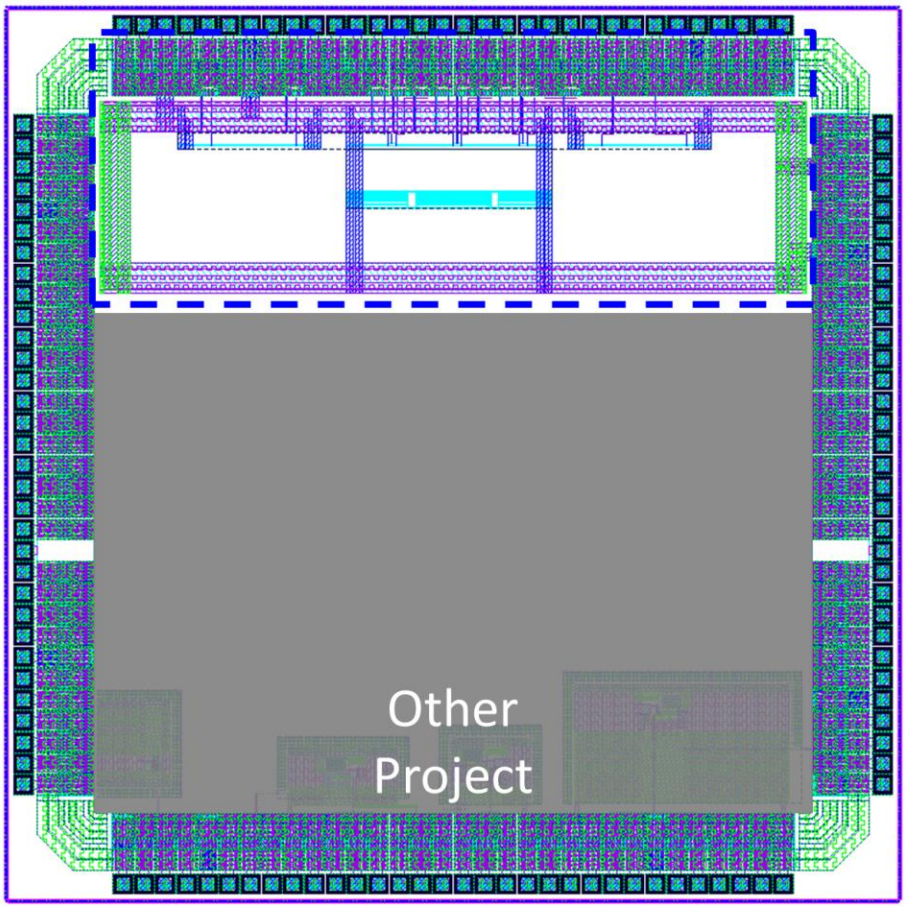


図１１．１　DP-LUT 試作チップのレイアウト図（全体図）

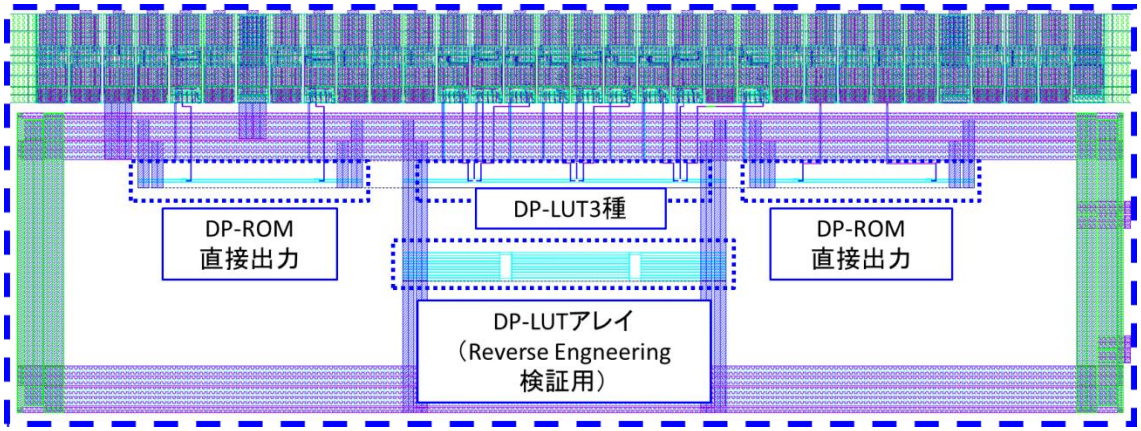


図１１．２　DPD 実装領域の拡大図

１１．１．１　DP-ROM の実装と検証

本チップには前章で紹介した DP-ROM を単体で実装し，チップの出力端子と接続を行っている．この出力電圧を測定することで，DP-ROM が期待通りに動作することを確認した．図１１．３はチップに実装した DP-ROM 領域のレイアウトを拡大表示したものである．図内の DP-ROM の部分がプログラム領域で，今回の試作では論理１，論理 2 にプログラムした素子を 2 つずつ配置している．

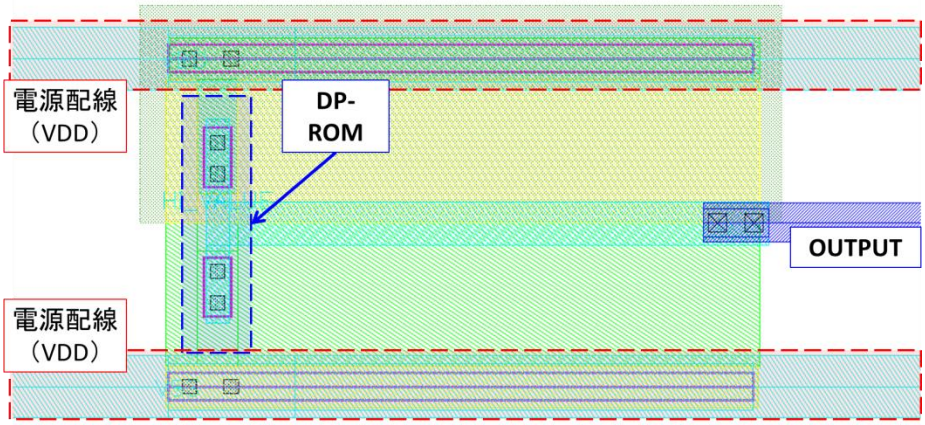


図１１．３　チップ上の DPD-ROM のレイアウト図

オシロスコープを用いて出力電圧を測定した結果について報告する．測定では専用の DUT ボードにチップを装着し，ボードの出力端子にプローブを当て，出力波形を観測した．測定時の波形を画像保存したものを図１１．４に示す．

DP-ROM はコア電圧をそのまま外部に伝える出力端子に接続されている．したがって出力電圧は論理１の場合はコア電圧の最大値である 1.8V，論理 0 の場合は 0V となる．オシロスコープを用いて測定した結果を観測すると，論理値を１としてプログラムした DP-ROM は 1.8V が出力されている．また論理値 0 にプログラムした DP-ROM は 0V が出力されている．よって Diffusion 領域にプログラムした通りの，期待した結果が得られていることが分かる．

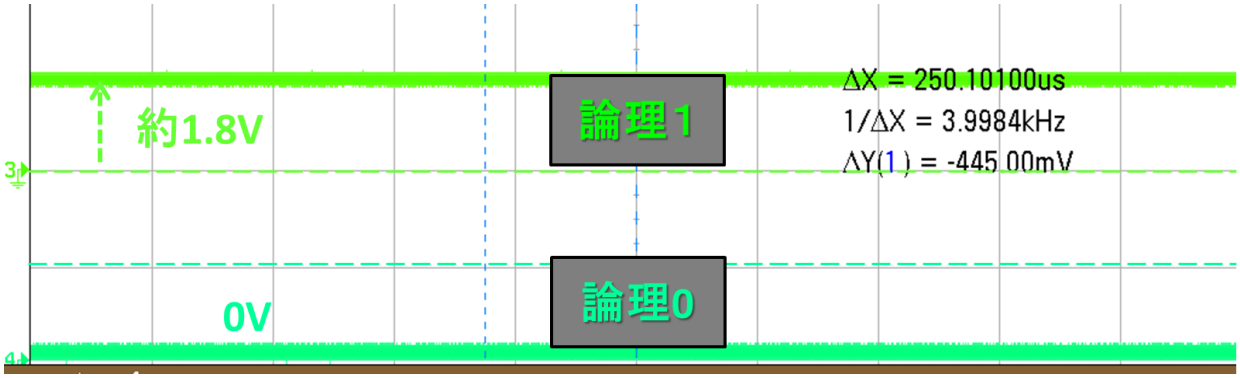


図１１．４　実チップの測定結果（DP-ROM）

１１．１．２　DP-LUT の実装

本試作チップの DP-LUT 実装領域の拡大図を図１１．５に示す．チップには Bub-OR，Bub-AND，XNOR の 3 種類の論理をプログラムした DP-LUT を搭載している．各入出力はチップの I/O ポートに接続されており，外部から DP-LUT に対して信号を与えることが可能である．各 LUT に接続された各 DP-ROM は製造時に図１１．６に示すようにプログラムが施されており，図中の真理値表に沿って動作することが期待される．

次に DPD-LUT の実測定を行った．チップの動作検証では 2 つの入力端子 A,B のうち A 端子にはファンクションジェネレータから振幅 3.3V の方形波を入力し，B 端子には定電圧源から 0V または 3.3V を入力した．このとき出力端子 Y にプローブを接続することで，それぞれ入力に対する出力電圧の波形が得られる．

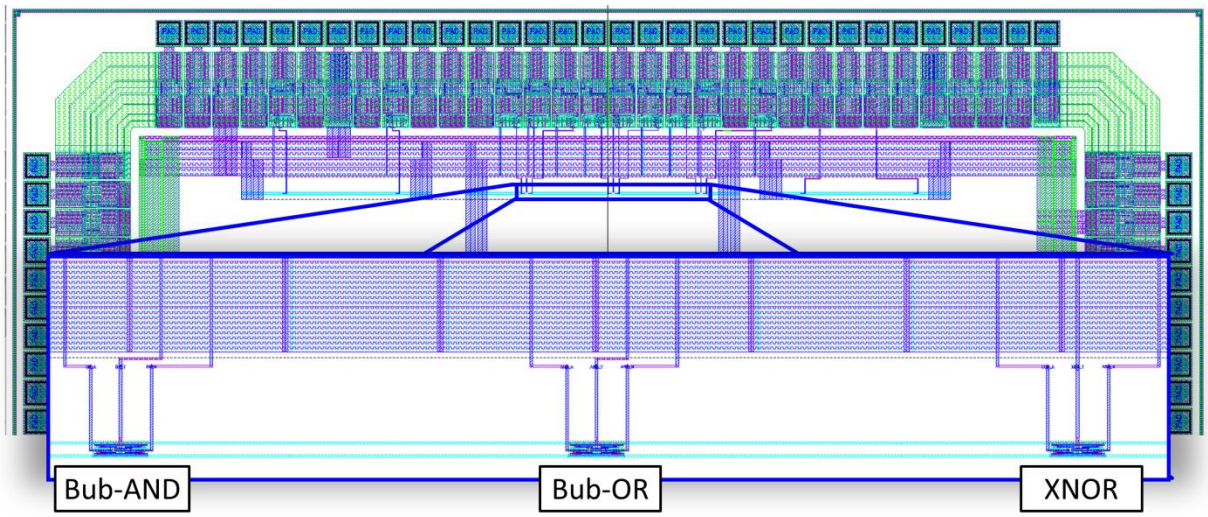
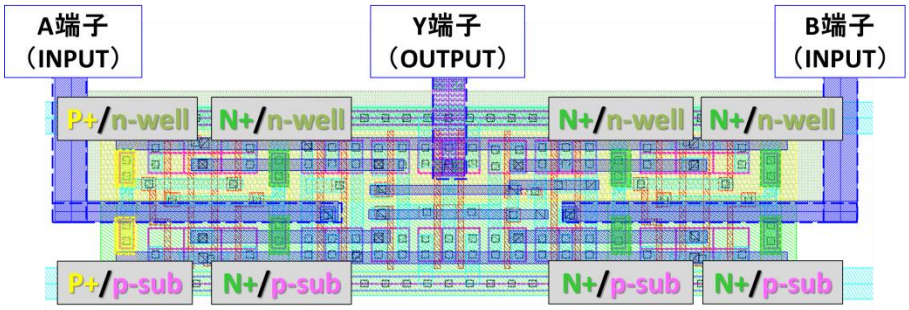
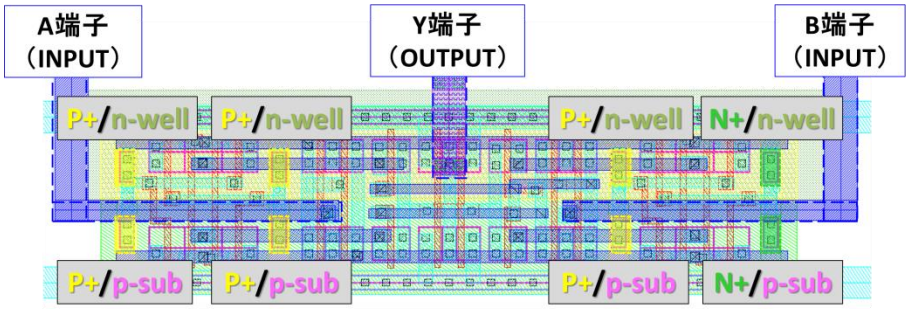


図１１．５　DP-LUT の実装領域（拡大図）



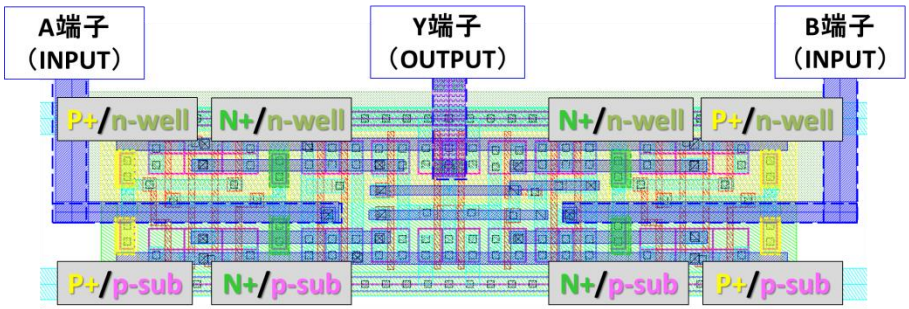
A	B	Y
0	0	0
1	0	1
0	1	0
1	1	0

（a） Bub-AND



A	B	Y
0	0	1
1	0	1
0	1	0
1	1	1

（b） Bub-OR



A	B	Y
0	0	1
1	0	0
0	1	0
1	1	1

（c） XNOR

図１１．６　各 DP-LUT のレイアウト図とプログラム状態

図１１．７―９に各 DPD-LUT の出力電圧をプローブとオシロスコープを用いて測定した結果を示す．図１１．７が Bub-AND，図１１．８が Bub-OR，図１１．９が XNOR を再現したときの DP-LUT の入出力波形をそれぞれ示している．

図１１．７の出力波形に注目する．DP-LUT の出力波形は A が 3.3V，B が 0V の時に 3.3V を出力し，それ以外の入力の組み合わせでは 0V を出力している．これは図１１．６で示していた Bub-AND の動作と同様の結果を示している．したがって，この DP-LUT は意図通りに動作しており，Diffusion 領域のドープタイプの N+/P+のプログラムによって目的の論理セルを実現している．同様にして図１１．８，図１１．９の出力波形も図１１．６の真理値表と同様の結果になっている．したがって Diffusion 領域のドープ材料の変更のみで任意の 2 入力論理回路を実現するデバイスを目的通り実現することに成功したといえる．

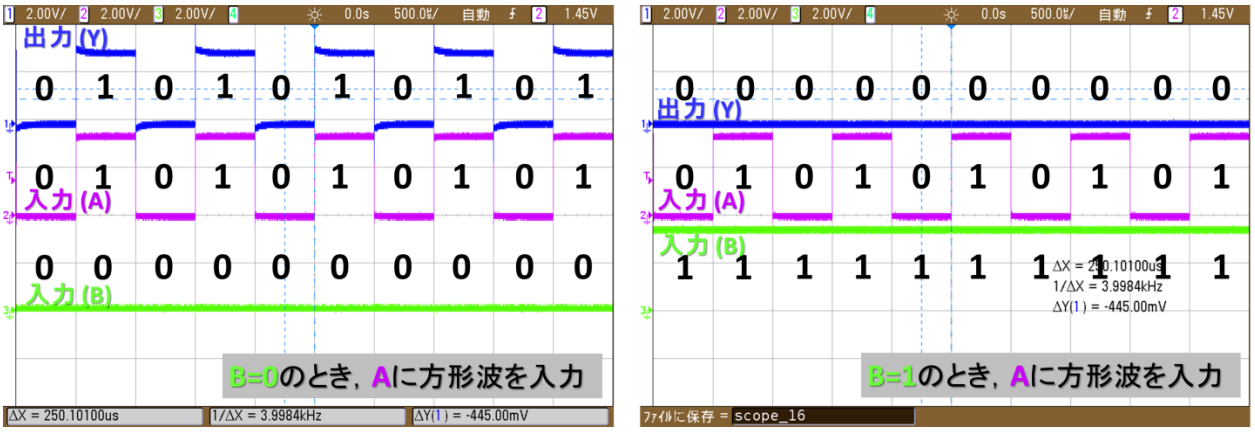


図１１．７　Bub-AND を再現した DP-LUT の入出力測定

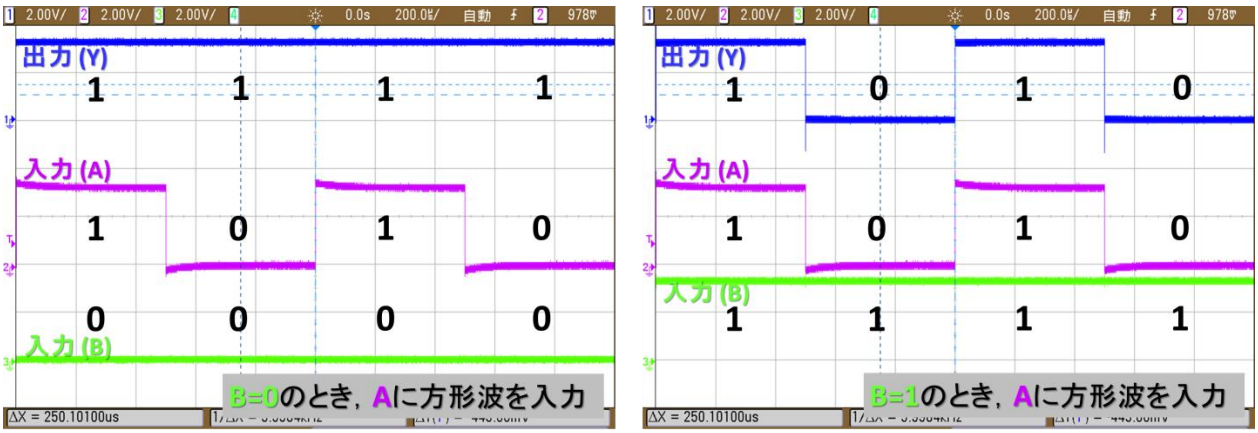


図１１．８　Bub-OR を再現した DP-LUT の入出力測定

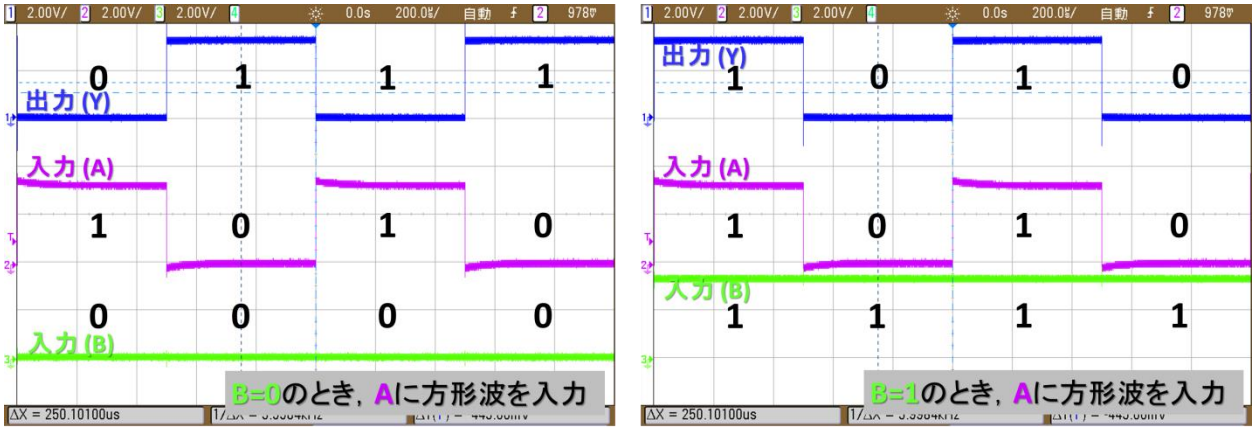


図１１．９　XNOR 再現時の DP-LUT の入出力測定

１１．２　リバースエンジニアリング耐性の評価

本節では試作チップ上に実装した DP-LUT のアレイ領域に対してエッチングを行い，顕微鏡を用いて DP-LUT の解析を行った．解析では光学顕微鏡の他に走査型電子顕微鏡（SEM：Scanning Electron Microscope）として日立ハイテクノロジーズ社製の S-5200 SEM, 集束イオンビーム加工観察装置（FIB：Focused ion beam）として日立ハイテクノロジーズ社製の FB-2100 FIB を利用した．

１１．２．１　SEM／FIB の動作原理

SEM および FIB の撮像原理について説明する．SEM は細く絞った電子線を試料表面に照射し，その際に発生・放出される信号を検出することで試料の構造を観察する電子顕微鏡の一種である[2]．電子線の軸を少しずつずらしながら照射することで試料の表面を網羅的に走査して像を得ることから走査型電子顕微鏡と呼ばれる．検出信号として 2 次電子が用いられ，電子線の照射座標と 2 次電子の総量を処理することで画像を表示し，像を視認することが可能になる．またこのような 2 次電子から得られた試料の像を 2 次電子像という．2 次電子像は検出した 2 次電子の電荷量によってコントラスト（明暗）が異なり，これは試料表面の凹凸や材質，照査する電子線のエネルギーによって異なる．電子の波長は光よりも短いため，光学顕微鏡では観察できない微細な形状も表示することができる．

図１１．１０に電子線照射装置と二次電子検出器によって構成された SEM の構造を示す．電子銃より照射した電子は 2 種類のレンズによって試料表面の一点に収束される．収束させた電子を受けた試料表面からは 2 次電子が放出され，それを 2 次電子検出器によって信号としてとらえ，画像化する仕組みである．

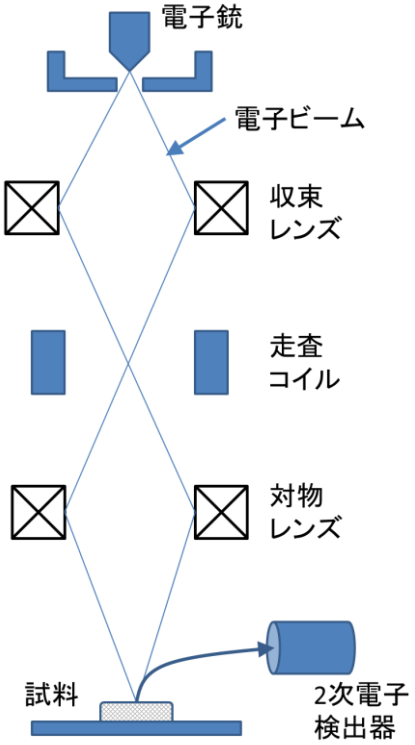


図１１．１０　SEM の構造

FIB では入射粒子として電子ではなく，イオンを収束させて照射し，放出された二次電子を検出して二次電子像を表示する．

１１．２．２　リバースエンジニアリングによる回路の構造解析

対象チップに対して，顕微鏡を用いたリバースエンジニアリングを実行した．図１１．１１にリバースエンジニアリング耐性評価のために試作した DPD-LUT のアレイブロックを示す．このアレイブロックは行列 10×10 の DPD-LUT をタイル状に敷き詰めた構造になっており，上段から順にそれぞれ 10 種類の異なる論理回路を再現している．図１１．１１中にある番号は表１１．２に対応しており，DP-LUT のプログラム領域 S1～S4 が N+/P+によってプログラムされている．表中の数値が 1 の場合は N+が，0 の場合は P+が n-well/p-sub 上にドープされている．また行毎には同一の論理回路にプログラムされた DP-LUT が並んでいる．

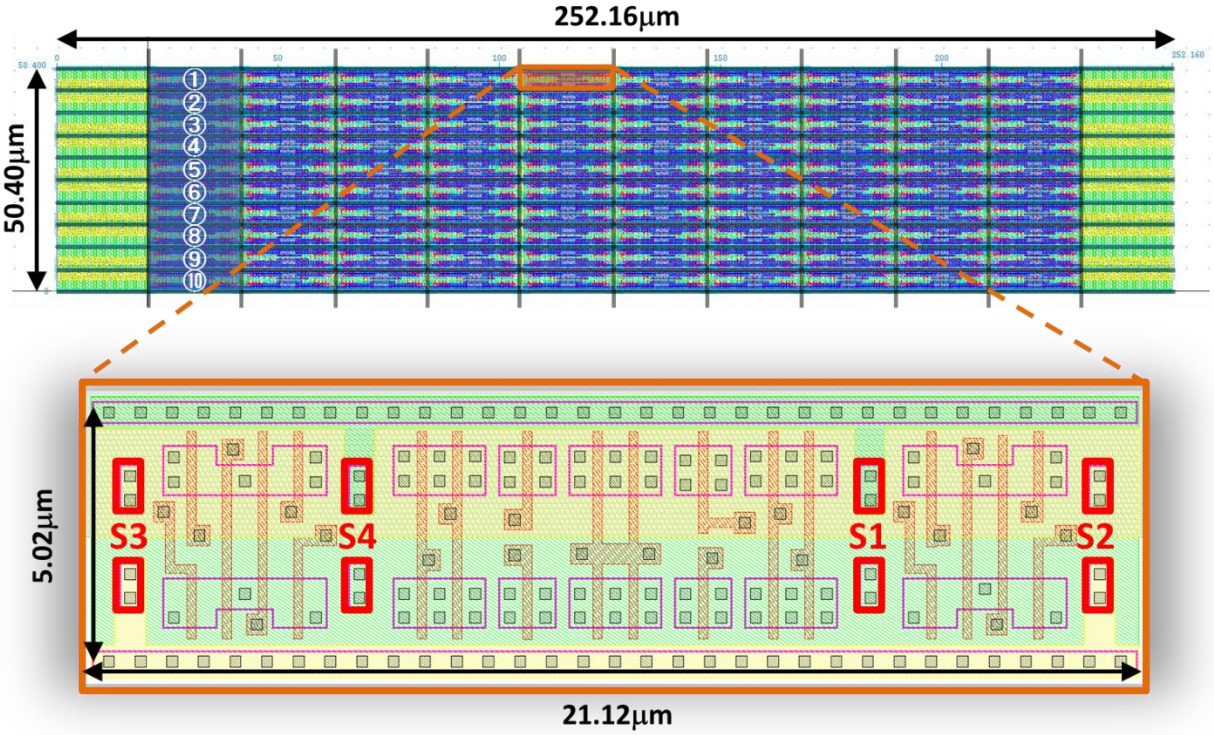


図１１．１１　DP- LUT のアレイブロックと拡大図

表１１．２　各 DPD-LUT にプログラムされた論理

	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩
S1	1	0	0	1	1	0	1	0	0	1
S2	0	1	1	0	1	0	1	0	1	0
S3	0	1	0	1	0	1	0	1	0	1
S4	1	0	1	0	0	1	1	0	0	1

DP-LUT は第 2 メタル層までの金属配線層が使用されている．リバースエンジニアリング耐性を評価する際は下層の拡散領域のタイプを解析するために図１１．１２に示すように拡散領域と直接接続されているコンタクトが観察できるまでメタル・ビア配線を除去し，コンタクト層表面を露出させた．

図１１．１３にコンタクト表面を露出させた DP-LUT のアレイブロックのチップ撮影画像を示す．この撮影画像は実チップ表面をエッチングし，光学顕微鏡を用いて撮影した画像である．

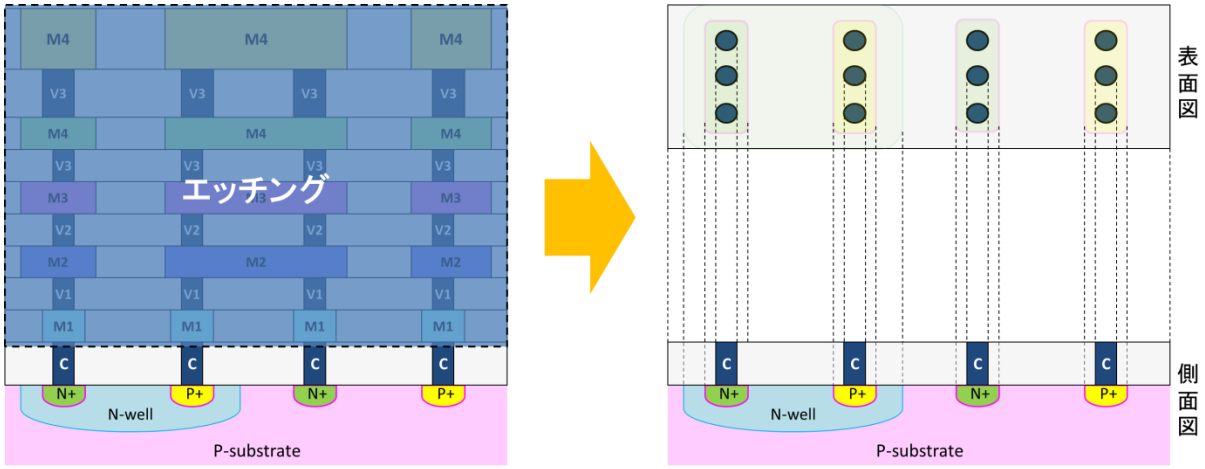


図１１．１２　メタル・ビア層のエッチングとコンタクト層の露出

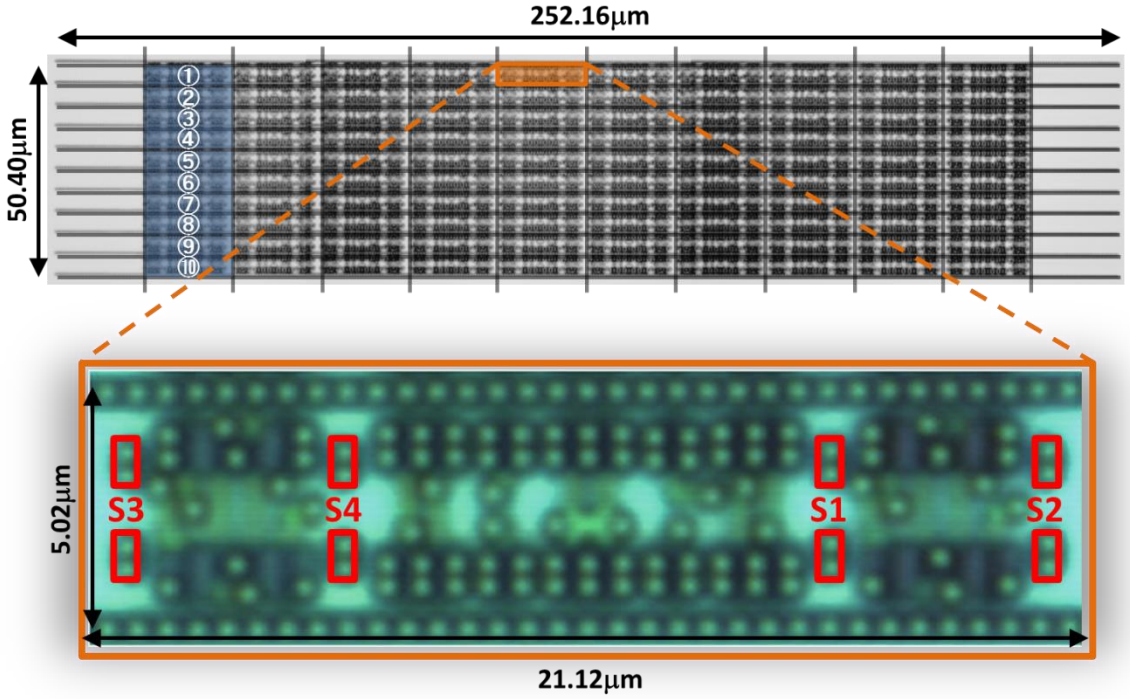
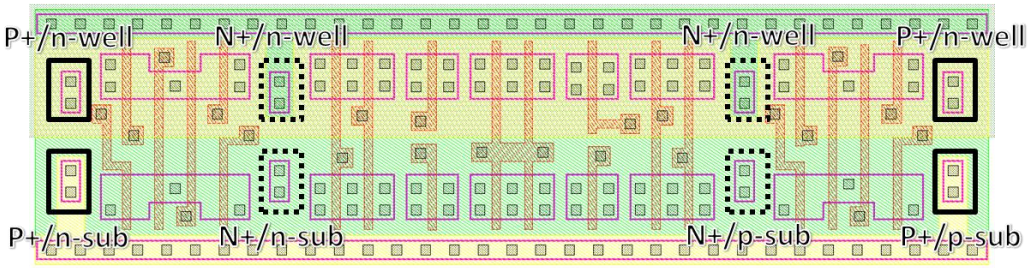
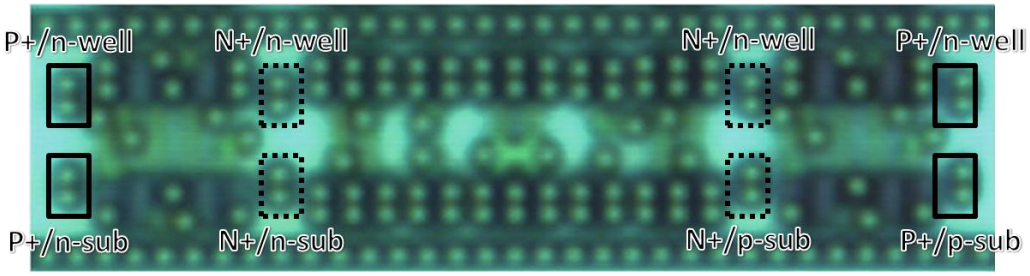


図１１．１３　光学顕微鏡を用いて撮影したアレイブロックのコンタクト層表面

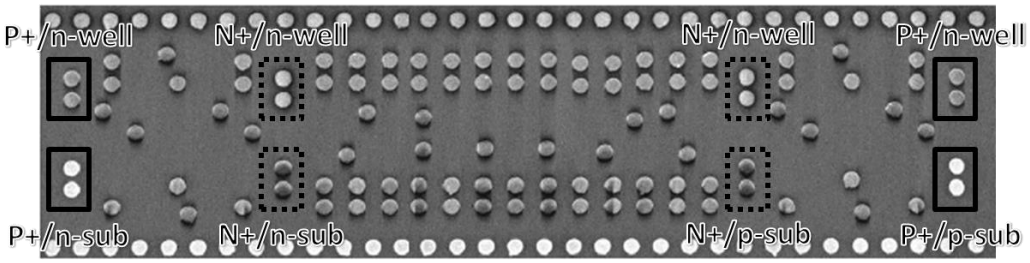
図１１．１３のアレイブロックの内，最上部に配置された DP-LUT①に注目する．この DP-LUT①は XNOR がプログラムされており，図１１．１４（a）のように左側から順に P+，N+，N+，P+がドープされている．この回路に対して光学顕微鏡，SEM，FIB の 3 つの顕微鏡を用いてチップ表面の撮像を行った結果を図１１．１４（b）（c）（d）に示す．図１１．１４の（b），（c），（d）中の実線の領域は P+ドープ，破線の領域は N+ドープされたコンタクトの位置を示している．



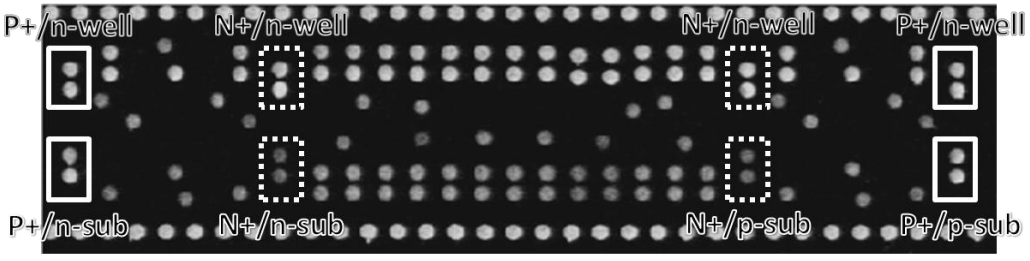
（a） レイアウト図面



（b） チップ撮影像 （光学顕微鏡：100倍）



（c） 2次電子像 （SEM：8000倍，加速電圧0.7kV）



（d） 2次電子像 （FIB：12000倍，加速電圧40kV）

図１１．１４　DPD-LUT（XNOR 再現時）の光学顕微鏡/SEM/FIB による撮像結果

まず光学顕微鏡における解析結果について述べる．図１１．１４(b)ではチップ内の DP-LUT を 100 倍に拡大した画像を示している．光学顕微鏡においてコンタクトおよび拡散領域を観察すると，すべてのコンタクトの像に変化はなく，拡散領域の N+/P+の違いを識別できないことが分かる．したがって光学顕微鏡を用いて DPD-LUT のリバースエンジニアリングを行うことは不可能といえる．これは従来のメタル配線層からスタンダードセルを解析する手法が使用できないことを意味しており，セルベース ASIC によって開発された LSI よりも高い耐タンパ性を有していると考えることができる．

次に SEM による二次電子像の解析結果に注目する．図１１．１４（c）では 8000 倍に拡大した 2 次電子像を示している．2 次電子像は試料表面の凹凸の他に，電位差によってコントラストが変化する．このコントラストは電位が高い場合に 2 次電子検出器の検出効率が低下して暗くなり，逆に電位が低い場合に明るくなる．この帯電している電位差によって生じる 2 次電子像の明暗の差は「電位コントラスト（Voltage Contrast : VC)」と呼ばれる．さらに VC は入射電子の一部が試料表面に残ることによっても生じるため，表面に帯電する電子と基板に吸収される電子の違いによっても発生する．これを Passive Voltage Contrast（PVC）と呼ぶ．図中の 2 次電子像の明暗は，この PVC を反映した結果を示していると考察できる．N+/P+拡散領域に接続されたコンタクトの明暗に注目する．コンタクトの PVC は下層の接続先にある拡散領域の P＋/N+の違い，および拡散領域が形成された n-well/p-sub の違いによって，明らかに明暗がはっきりと異なっていることが観察できる．図１１．１５に基板上に形成された拡散領域およびウェル領域の構成によって発生している PN 接合ダイオードや抵抗の違いを示す. 図のように N+/P+拡散領域と n-well/p-sub の組み合わせによって，それぞれ異なる PN 接合ダイオード・抵抗が付加される．その為，基板間との抵抗値に差が生まれ，PVC によって 2 次電子像に反映されることになる．その結果，コントラストの違いからそのコンタクトに接続された P+/N+を推測することが可能になる．図１１．１５の接合条件より予測される電圧の高低とコントラストの明暗の差を表１１．３にまとめる．

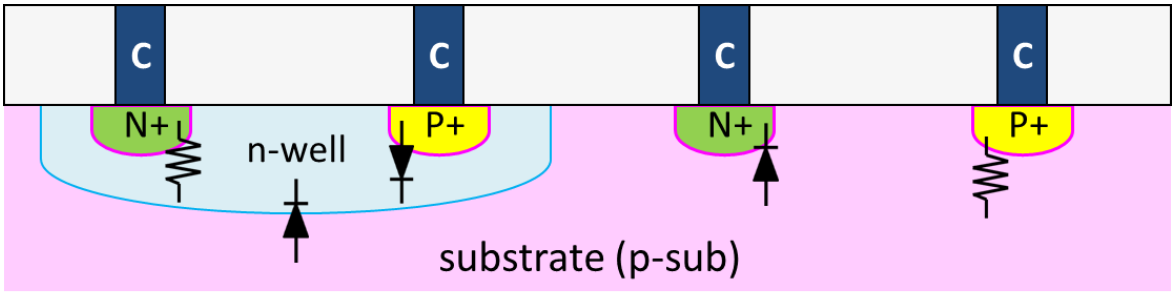


図１１．１５　N+/P+領域および n-well/p-sub 領域の組み合わせによる接合ダイオード・抵抗の違い

表１１．３　N+/P+領域および n-well/p-sub 領域における表面電位・コントラストの違い

	diffusion-type	well/sub-type	表面電位	コントラスト
N+/n-well	n	n	中（低）※	2
P+/n-well	p	n	中（高）※	3
N+/p-sub	n	p	高	4（最も暗い）
P+/p-sub	p	p	低	1（最も明るい）

PN 接合ダイオードのビルトイン電圧分 P+/n-well の方が高電位になる

表面電位を予測すると，P+/p-sub が接地された基板と直接接続されているため，最も 2 次電子の発生が大きくなる．そのため 2 次電子像が最も明るく（白く）なると考えられる．一方で N+/p-sub は小さな拡散領域が基板から独立しており，吸収電流が小さいため最も高電圧に帯電する．そのため低エネルギーの 2 次電子は放出されず，最も暗く（黒く）なると考えられる．n-well 上に P+/N+拡散領域は双方ともウェル領域と接続されており，well に吸収される電荷量は等しい．しかし P+/n-well は PN 接合ダイオードを構成しているためビルトイン電圧分の電位差が生じる．そのため抵抗接続の N+/n-well よりも P+/n-well の方が高電位になる．よって P+/n-well の 2 次電子像は N+/n-well よりもわずかに暗くなると考えられる．

表１１．４に図１１．１４（c）中の 2 次電子画像のコントラストを分析した結果を示す．実際の二次電子像において，予想したコントラスト順位と同様の明暗が得られた．これは DP-LUT の構造を知っている場合，プログラムされた 2 入力論理を判別できるということを示している．したがって，SEM を用いたリバースエンジニアリングを試みた場合，DP-LUT のレイアウトを把握しているリバースエンジニアは容易に DP-LUT の論理を特定することが可能になる．これは SEM による RE 攻撃に対しては完全な RE 耐性を有していないことを表している．

表１１．４　実際のコントラスト

	diffusion-type	well/sub-type	二次電子像	コントラスト
N+/n-well	n	n		2
P+/n-well	p	n		3
N+/p-sub	n	p		4
P+/p-sub	p	p		1

同様に実装したすべての DP-LUT に対して SEM の 2 次電子像による N+/P+の解析を試みた結果を図に示す．DP-LUT①と同様に，N+/P+と n-well/p-sub の組み合わせによってコントラストに明らかな差が観測され，これを用いて論理プログラム時に N+/P+のどちらを用いたものか判別することが可能である．

最後に FIB による二次電子像の解析結果に注目する．図１１．１４（c）は 12000 倍に拡大した 2 次電子像である．FIB の 2 次電子像についても SEM のものと同様にコントラストに違いがみられる．しかし，こちらは N+/p-well のみが暗くなり，ほかの組み合わせではコントラスト比に明らかな差はみられなかった．よって p-sub 上にドープした N+/P+を判別することで，論理の 1/0 を解析することが可能になる．一方で n-well 上にドープした場合では判別ができず，RE 耐性を有していると考えることができる．

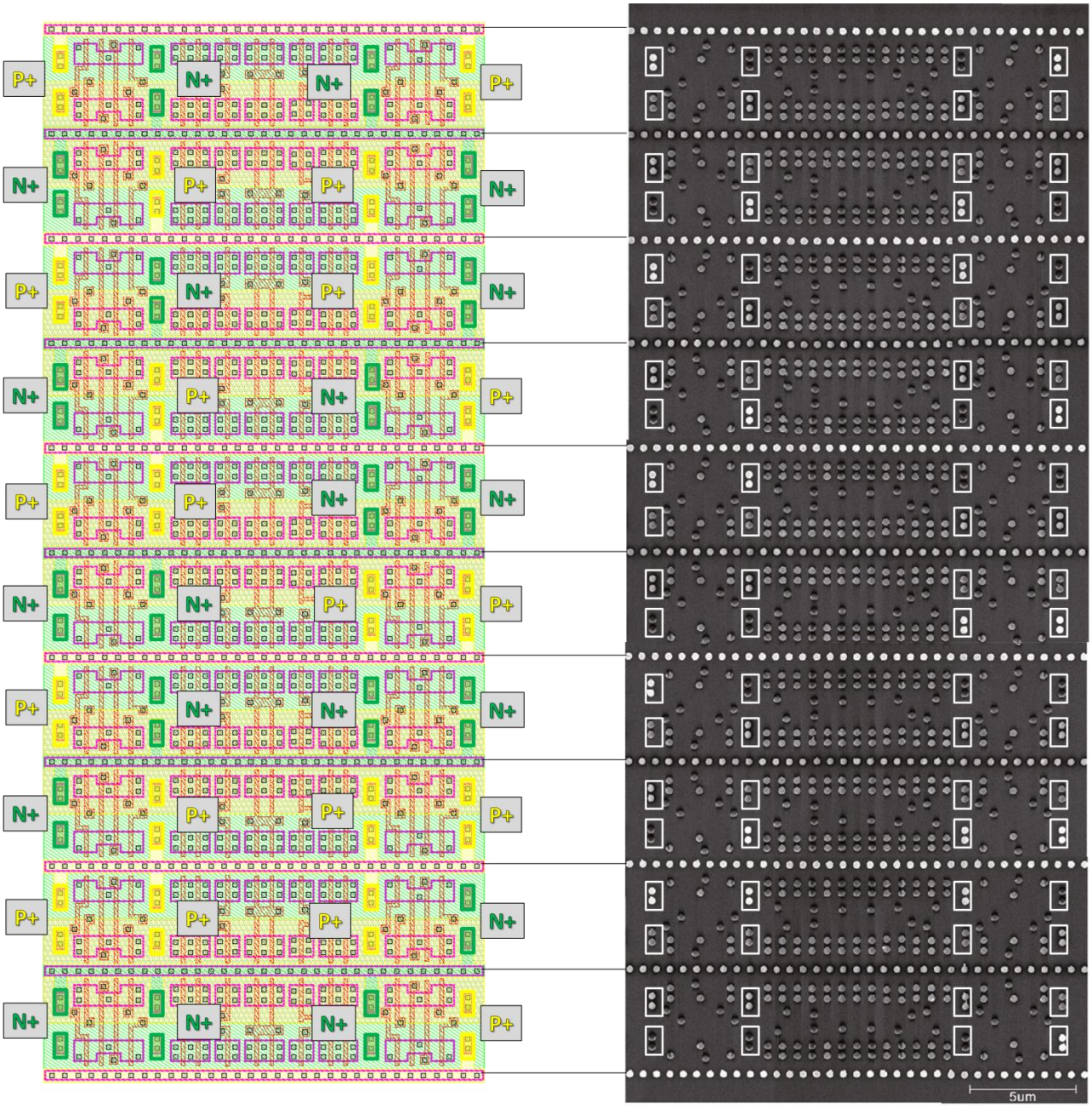
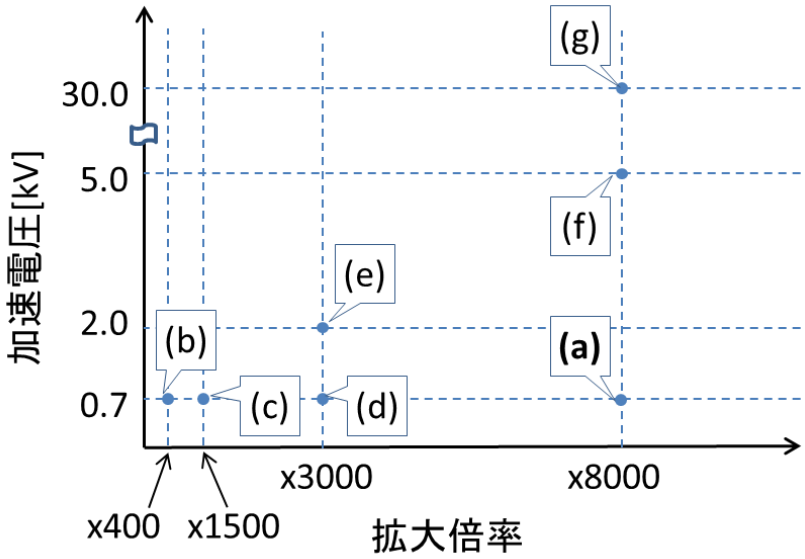


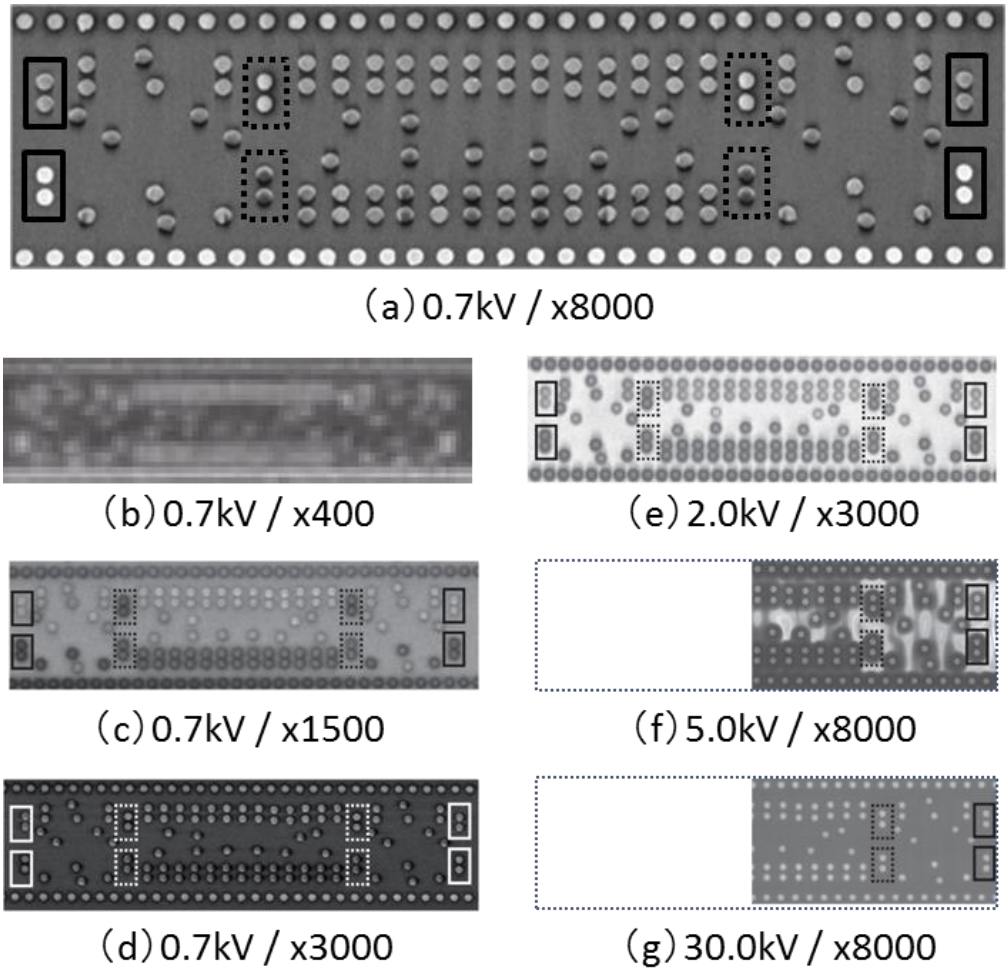
図１１．１６　SEM の 2 次電子像における DPD-LUT の再現論理とコントラストの違い

１１．２．３　リバースエンジニアリング耐性の考察

SEM を用いた解析によって DP-ROM の論理タイプを判別することが可能であることが明らかになった．これは DP-LUT を用いた論理回路でも，配線層をすべて除去し，SEM を使用するとリバースエンジニアリングが可能であるということを示している．次に SEM の仮想電圧や拡大倍率の設定を変更したときの 2 次電子像を図に示す．図１１．１４（c）に示した設定は図１１．７（1）（a）に該当し，この設定であれば N+/P+の判別を 2 次電子像から行うことができた．しかし異なる設定の場合ではコントラストの明暗に差がなく，N+/P+の判別を行うことが不可能であることが分かる．



（1）SEM の加速電圧，拡大倍率の設定



（2）各設定における二次電子画像

図１１．１８　SEM の加速電圧/拡大倍率毎の 2 次電子像の違い

また SEM の 1 回の撮影によって回路全体の 2 次電子像が得られるわけではない．このことから，リバースエンジニアリングを行う者は高価な SEM の設定を調整しながら，配置されたすべての DP-LUT を解析しなければならない．したがってそのコストは非常に甚大なものになると考えられる．

このことから，DP-LUT を用いた論理回路は光学顕微鏡を用いた配線から回路構造を解析する従来の手法ではリバースエンジニアリングを行うことができず，結果として，SEM や FIB などの高価な解析装置を何度も用いらなければならず，リバースエンジニアリングに要するコストを格段に高くすることに成功している．したがって，拡散領域の N+/P+を変更する回路設計技術 DPD は一定のリバースエンジニアリング耐性を持たせることに成功したといえる．

第 11 章の参考文献

[1] VDEC, "VLSI Design and Education Center Homepage",
http://www.vdec.u-tokyo.ac.jp/
[2] 日本電子株式会社, “走査電子顕微鏡 基本用語集”,
http://www.jeol.co.jp/words/semterms/

第 12 章　まとめと今後の展望

１２．１　まとめ

本論文では LSI の初期開発コスト高騰問題とリバースエンジニアリング（RE：Reverse Engineering）による設計資産（IP：Intellectual Property）窃取と模造半導体の脅威について取り上げた．それぞれの課題に対して，マスクプログラマブルデバイス（MPD：Mask Programmable Device）を用いた新たな LSI 設計手法を提案した．

特定用途向け IC（ASIC：Application Specific Integrated Circuit）の初期開発コストを削減するために，ビアマスクのみを変更して論理回路を設計するビアプログラマブル・ストラクチャード ASIC（VPSA：Via Programmable Structured ASIC)と呼ばれる低マスクコスト設計製造手法に注目した．（第 2 章）

より実装効率･性能のよいVPSA を実現するために, 2008 年に著者が所属する研究室提案されたVPSA アーキテクチャの一つである Via Programmable Device using EXclusive-or logic array（VPEX）を含め, 従来 FPGA において使用されてきた LUT 型アーキテクチャを MPD 化したデバイスの検討の検討を行った．（第 3 章）

さらに，検討結果をもとに VPEX を改良した VPEX3 を新たに提案し，ベンチマーク回路を用いた性能評価により他の MPD を含めて VPEX3 の性能評価を行った．論理合成後の面積見積もりでは，他のアーキテクチャが ASIC の約 5.6～13.5 倍の実装面積であったのに対し，VPEX3 の実装面積は ASIC の約 2 倍であり，面積性能の大きく改善できたことを示した．（第 4 章）

また客観的な性能比較を行うために他の研究機関（元智大学）で開発されている MPD アーキテクチャ Via Configurable Logic Block との比較を行った．この比較ではベンチマーク回路に対して複数の制約条件を与え，それぞれの面積，動作速度，消費電力の見積もりを行った．VCLB の面積，動作速度，消費電力の各性能がそれぞれ ASIC の 5.30 倍，1.21 倍，2.42 倍であるのに対し，VPEX3 では 2.33 倍，1.09 倍，1.74 倍と，VPEX3 の方がより多くのベンチマーク回路・制約条件において性能の良い実装を実現できることを確認した．（第 5 章）

VPEX3 を用いて大規模回路を実現するために専用の CAD システムを構築した．（第 6 章）

専用の CAD システムを用いて大規模な乗算器や DES 暗号回路の自動設計・チップ試作を達成した．また DES 暗号回路の実機測定を行い，ASIC，FPGA で試作・実装した同一の回路との消費電力性能評価を実施した. この比較より, VPEX3 と ASIC の消費電力差が約 3 倍となることを確認した. また FPGA の動的消費電力結果にスケーリング側を適用し, VPEX3 と比較を行ったことで FPGA の 1/2 倍の動的消費電力を実現できていることを確認した．（第 7 章）

またこれらのチップを測定することで VPEX3 の新たな問題点として Utilization とクロックツリーの消費電力が判明した．この２つの問題を解決するために LE を大きくすることで配線リソースを増やし，また DFF の構成を変更することでクロックツリーの消費電力を削減した新しい VPSA アーキテクチャ VPEX4 を提案した．この VPEX4 を評価するために暗号回路をベンチマーク回路とした面積，消費電力の評価を行った．実装面積を考慮した比較において，VPEX4 は VPEX3 の約 1/2 倍の面積になることを

確認した．また消費電力では 18～53%の低消費電力化を実現した．（第 8 章）

またリバースエンジニアリングによる IP の模倣，および回路解析によるセキュリティ対策のために拡散領域をプログラマブル層とした Diffusion Programmable Device（DPD）を提案した．DPD は金属配線から論理素子の特定を防ぐことで RE コストを高騰させる RE 対策手法を用いたデバイスで，実験によって光学顕微鏡による素子の特定が不可能であることを示した．またより高額な解析手法である走査型顕微鏡（SEM）を用いた解析では，受動的電位コントラスト（PVC：Passive Voltage Contrast）によって特定が可能であるが，加速電圧や拡大倍率などの設定によっては PVC が観測できないため，解析コストが非常に高額になる．これより提案した DPD は高いリバースエンジニアリング耐性を有していると結論が得られた．（第 9～11 章）

１２．２　今後の展望

本論文では，１２．１に示したように，LSI の初期開発コスト削減としては VPEX，リバースエンジニアリング対策としては DPD という 2 種類の MPD を研究し，どちらも優れた提案であることを示してきた．しかしながら，実用化を目指した今後の展望として考えると，更なる改良点が残されている．以下，LSI の初期開発コストを解決するための VPEX に対しては（1）～（4），リバースエンジニアリング対策 DPD に関しては（5）を今後の検討課題としてまとめておく．

（1）VPEX 専用 CAD システムの自動配線処理の高精度化

VPEX3 および VPEX4 の配置配線では配線経路最適化アルゴリズムを実施し，トラック割り当てを行った結果，割り当てが失敗した場合に，再配線や経路の修正を実行する工程が存在しない．そのため配線経路最適化プログラムの最適化した配線経路の結果が配線成功率に強く依存している．したがって，配線失敗時にトラック割り当て処理の中で迂回配線による配線を試行する処理を加えることで，配線成功率が向上する可能性がある．

また，今回作成した CAD システムは自動配置配線後に動作速度のタイミングが制約条件を違反しないように，クリティカルパスやタイミング猶予の厳しいパスを優先して配線するタイミングドリブン機構が備わっていない．したがって，この最適化を CAD システムに取り入れることで，タイミングを考慮した回路が実現できると考えられる．

（2）クロック供給に関連する消費電力の削減

順序回路を VPEX4 アーキテクチャで設計すると，スタンダードセルを用いた ASIC と比べて，クロックに供給に依存する消費電力が非常に大きいという問題点がある．これは DFF を再現する際に受け取ったクロックパルスより内部で論理を反転させた逆位相のクロックと，さらに反転させた正位相のクロックを 2 つ生成しているため，DFF 内部の充放電電力が大きくなってしまったことが原因である．

よって現在の消費電力をさらに削減するためには，LE のレイアウトを工夫して，DFF 内部のクロック経路のゲート容量と配線容量を小さくする必要がある．これにより，従来 FPGA で適用が困難であっ

たモバイル機器や低エネルギーデバイスへの VPEX 利用の可能性がさらに拡大すると考えられる．

（3）マスクプログラム方式のアナログ回路の検討

VPEX3 はディジタル回路をカスタムマスク（ビアマスク）の変更のみで実現するデバイスである．最近では，ＩＯＴ（Internet of Things）という言葉があるようにインターネットに接続可能なセンサーデバイスを生活空間に多数配置するような取り組みが始まっている．このようなデバイスでは，ディジタル回路以外にアナログ回路が必要とされる．したがって，MPD をこのようなデバイスに適用していくためにはアナログ回路もビアマスクでプログラムできる必要がある．著者が所属する研究室においても，センサー向けのアナログ回路の構成の変更をビアプログラムで行う VPA（Via Programmable Analog）アーキテクチャの検討を行っている．

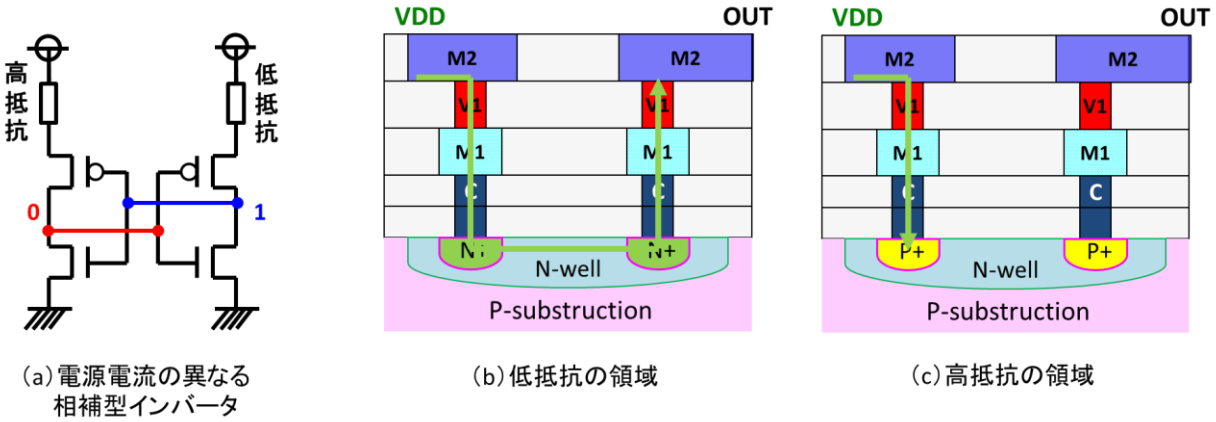
（4）VPEX アーキテクチャの先端プロセスへの適用

本論文ではすべてメタル配線数が 5 層の Rohm180nm プロセスを使用して評価・試作を行っている．現在の先端プロセス（22nm，16nm）では配線層の数が 10 層以上になることも多い．本論文で提案した VPEX は LE 間を接続するルーティング層として第 3，第 4 層メタルを使用したが，先端プロセスでは，その層数は増加すると考えられる．したがって VPEX を最先端プロセスで利用するためには，また多層配線に合わせた配線アーキテクチャの提案など，プロセスの進歩に合わせた，新たな検討が必要である．

（5）DPD 方式に対する SEM によるリバースエンジニアリングへの対策

耐リバースエンジニアリングデバイスとして開発した DP-LUT は光学顕微鏡においては拡散領域の N+/P+を特定することは不可能であった．その一方では SEM を用いた 2 次電子像の検出によって N+/P+拡散層の特定を上層のコンタクト層で行うことができる．SEM は導入や撮影が非常に高額であるため．SEM を保有していない機関にたいして RE 耐性を実現しているといえる．その一方で，現在では RE を目的とし，SEM を用いた構造解析を請け負う企業が存在する．これらの機関を利用されることで，SEM を有していない組織にも DP-LUT を用いた設計資産の詳細を特定されてしまう恐れがある．したがって，SEM を用いたとしても論理情報や配線経路の特定が不可能，あるいはより困難な撮影条件を強制するようなデバイスを検討する必要がある．

より RE 攻撃に耐性のある DPD の構成例を図１２．１に示す．この例では n-well 上 N+/P+の特定が P-sub 上の N+/P+よりも困難であることに注目し，n-well 上のみの N+/P+プログラムのみで ROM を実現した例である．この例では相補型のインバータの電源電圧の抵抗を操作して，起動時に出力される論理１と論理０を制御した構成である．このときの抵抗値を図（b）（c）に示した DPD で制御する．



(a)電源電流の異なる相補型インバータ　(b)低抵抗の領域　(c)高抵抗の領域

図１２．１　電源電圧の抵抗操作による ROM

謝辞

本論文をまとめるにあたり、終始暖かい激励とご指導、ご鞭撻を頂いた立命館大学理工学部電子情報学科教授・藤野毅教授に心より感謝申し上げます．藤野教授には学部生の研究室仮配属時より 6 年と半年間の長期間にわたり，研究に対する姿勢や考え方をご指導いただきました．また，3 年数か月前に突然の進学希望を願い出た私を快く引き受けてくださり，充足した研究環境を提供していただきました．本論文の成果は教授の木目細やかな指導と心遣いによって達成できたものだと感じております．自身の未熟さより大変なご迷惑をおかけいたしましたが，見捨てずご指導いただいたこと誠に感謝しております．本当にありがとうございました．

ビアプログラマブルデバイスに関する打ち合わせや論文執筆などで多くの御助言・ご指導を頂きました名城大学理工学部情報工学科教授・吉川雅弥教授に深く感謝致します．耐リバースエンジニアリング対策技術に関するご助言・ご指導を頂きお世話になりました汐崎充博士に深く感謝致します．チップ開発環境の立ち上げ，およびチップ試作作業でお世話になりました浅川俊介技術補助員に感謝いたします．

SEM によるリバースエンジニアリング耐性評価を行うにあたり，実験の実施にご協力をいただきました三菱電機株式会社情報技術総合研究所・菅原健博士に感謝いたします

研究だけでなく多岐にわたりご指導を賜りました．立命館大学理工学部電子情報工学科講師・熊木武志博士にはに深く感謝致します．論文添削などで，他分野にもかかわらずお世話いただきました久保田貴也研究員に感謝いたします．CMOS アナログ回路の勉強会やご指導，論文執筆にあたりお世話になりました大阪産業大学工学部電子情報通信工学科教授・熊本敏夫教授に感謝いたします．

プログラマブルデバイス研究の実験実施にあたり、評価用ライブラリの作成および実機測定を担当してくれた立命館大学理工学部電子情報学科藤野研究室卒業生の上岡泰輔君，VCLB との性能比較を丁寧にまとめてくれた卒業生の大谷拓君，評価用ライブラリを用いた消費電力の比較を行ってくれた在校生の人見達郎君，VPEX4 の性能評価を担当してくれた在校生の上口翔大君，ビアプログラマブル設計技術を共に研究した卒業生の中澤亮君，上田佳祐君．他、研究室の皆さんの熱心な協力を得たことを記すとともに心より感謝申しあげます．

最後に，急遽進学を決め，自身の思う道を進む私をあたたかく応援し，支援してくださった両親に心から深い感謝の意を表します．

研究業績目録

１．学会誌採択論文

[1] Ryohei Hori, Tatsuya Kitamori, Taisuke Ueoka, Masaya Yoshikawa, Takeshi Fujino,"Improved Via-Programmable Structured ASIC VPEX3 and its Evaluation", IEICE Trans. on Fundamentals of Electronics, Communications and Computer, Vol.E95-A, No.9, pp.1518-1528, Sep. 2012.

[2] Ryohei Hori, Taisuke Ueoka, Taku Otani, Masaya Yoshikawa, Takeshi Fujino,"Via Programmable Structured ASIC Architecture “VPEX3” and CAD Design System", IEICE Trans. on Fundamentals of Electronics, Communications and Computer, Vol.E95-A, No.12, pp.2182-2190, Dec. 2012.

[3] Taku Otani, Shota Ueguchi, Ryohei Hori, Masaya Yoshikawa, Takeshi Fujino, “Via-Programmable Structured ASIC "VPEX3S" for High-Speed Application,” Journal of Signal Processing, Special Issue on Papers Awarded the Student Paper Award at NCSP'14, Vol. 18 No.4, pp. 161-164, July 2014.

[4] Takeshi Sugawara, Daisuke Suzuki, Ryoichi Fujii, Shigeaki Tawa, Ryohei Hori, Mitsuru Shiozaki, and Takeshi Fujino, “Reversing Stealthy Dopant Level Circuits,” Workshop on Cryptographic Hardware and Embedded Systems (CHES), LNCS8731, pp112-126, Sep. 2014.

２．研究会等発表論文（査読付き）

[1] Ryohei Hori, Masaya Yoshikawa, Takeshi Fujino,"The Development of CAD System for Via Programmable Structured ASIC VPEX3", The 17th Workshop on Synthesis And System Integration of Mixed Information Technologies (SASIMI 2013), pp.470-475, March 2012.

[2] Ryohei Hori , Kazuho Nakagawa, Toshiya Honda, Takeshi Kumaki, Takeshi Fujino, “Low Power Sensor System Using Smart Analog under Normally Off Operation” 2013 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP’13), pp.644-647, March 2013

[3] Ryohei Hori, Taisuke Ueoka, Taku Otani, Masaya Yoshikawa, Takeshi Fujino, “The implementation of DES circuit on via-programmable structured ASIC architecture VPEX3,” 2013 International Symposium on VLSI Design, Automation, and Test (VLSI-DAT), April 2013

[4] Taku Otani, Ryohei Hori, Masaya Yoshikawa, and Takeshi Fujino, “Improved Via-Programmable Structured ASIC VPEX3S and Its Evaluation,” 2014 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP’14), pp.97-100, March 2014

[5] Tatsuro Hitomi, Toshiya Honda, Ryohei Hori, Takeshi Kumaki, Takeshi Fujino, “Hardware Controller of camera sensor node using IR array sensor and CMOS image sensor for ultra-low-power operation,” 2014 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP’14), pp.749-752, March 2014.

[6] 堀遼平，上口翔大，吉川雅弥，藤野毅，“ビアプログラマブルアーキテクチャ VPEX4 の提案と性能評価”，第 13 回情報科学技術フォーラム講演論文集 第 1 分冊，pp.1-6， Sep. 2014.

３．その他研究会発表

[1] 堀遼平，国生雄一，西本智広，山田翔太，吉田直之，松本直樹，藤野毅，吉川雅弥，“ビアプログラマブルデバイスに最適な基本論理ゲートアーキテクチャの検討”，電子情報通信学会技術研究報告，Vol.109, No.462 , VLD2009-108, pp.55-60, March 2010.

[2] 山田翔太，國生雄一，西本智広，吉田直之，堀遼平，松本直樹，北森達也，吉川雅弥，藤野毅，“ビアプログラマブルデバイス VPEX のロジックアレイブロックと配線アーキテクチャの検討” 電子情報通信学会技術研究報告, Vol.109, No.462 , VLD2009-107, pp.49-54, March 2010.

[3] 堀遼平，北森達也，上岡泰輔，吉川雅弥，藤野毅， “ビアプログラマブルストラクチャード ASIC・VPEX の新アーキテクチャ提案と性能評価” 電子情報通信学会技術研究報告, Vol.110, No.315, ICD2010-91, pp.49-54, Nov. 2010.

[4] 上岡泰輔, 北森達也, 堀遼平, 吉川雅弥, 藤野毅, “ビアプログラマブル ASIC アーキテクチャ VPEX3 の面積と遅延評価” 電子情報通信学会技術研究報告, Vol.110, No.432, VLD2010-146, pp.177-182, March 2011.

[5] 北森達也，堀遼平，上岡泰輔，吉川雅弥，藤野毅，“ビアプログラマブルデバイス VPEX における配線リソースと配線遅延の評価”，電子情報通信学会技術研究報告, Vol.110, No.432, VLD2010-147, pp.183-188, March 2011.

[6] 上岡泰輔，堀遼平，北森達也，吉川雅弥，藤野毅，“ビアプログラマブルロジック VPEX のソフトエラー率の検討”，電子情報通信学会技術研究報告, Vol.111, No.352, ICD2011-119, pp.93-98, Dec. 2011.

[7] 中澤亮，堀遼平，上田佳祐，汐崎充，藤田智弘，藤野毅，“ビアプログラマブルアナログ(VPA)の提案と基本素子構造の検討”，電子情報通信学会技術研究報告, Vol.111, No.352, ICD2011-120, pp.99-103, Dec. 2011.

[8] 大谷拓，堀遼平，北森達也，上岡泰輔，吉川雅弥，藤野毅，“ビアプログラマブル ASIC アーキテクチャ VPEX の消費電力評価と面積･遅延性能評価”, 電子情報通信学会技術研究報告, Vol.111, No.450, VLD2011-121, pp.7-12, March 2012.

[9] 大谷拓，堀遼平，上岡泰輔，吉川雅弥，藤野毅，“ビアプログラマブルロジック VPEX の配置配線ツールを用いた性能評価”，電子情報通信学会技術研究報告, Vol.112, No.320, VLD2012-90, pp.177-182, Nov. 2012.

[10] 上田佳祐，中澤亮，堀遼平，汐崎充，藤田智弘，藤野毅, “ビアプログラマブルアナログ回路 VPA の提案とチップ設計”，LSI とシステムのワークショップ 2012, May 2012.

[11] 上田佳祐，中澤亮，堀遼平，汐崎充，藤田智弘，藤野毅，“ビアプログラマブルアナログ回路 VPA のチップ設計と特性評価”，電子情報通信学会技術研究報告, Vol.112, No.324, ICD2012-85, pp.49-54, Nov. 2012.

[12] 中川和歩，堀遼平，熊木武志，木股雅章，藤野毅，“センサノード低消費電力化のためのノーマリーオフ動作検証環境の構築と評価”，電子情報通信学会技術研究報告, Vol.112, No.481, CPSY2012-87, pp.211-216, March 2013.

[13] 人見達郎，堀遼平，上岡 泰輔，吉川雅弥，藤野毅，“ビアプログラマブルストラクチャード ASIC アーキテクチャ VPEX の DES 暗号回路における消費電力性能評価”，LSI とシステムのワークショップ 2013, May 2013.

[14] 上田佳祐，堀遼平，汐崎充，熊本敏夫，藤田智弘，藤野毅，“ビアプログラマブルアナログ(VPA)回路設計とプログラマブルアナログ回路との性能比較”，電子情報通信学会技術研究報告, Vol.113, No.323, ICD2013-87, pp.13-18, Nov. 2013.

[15] 大谷拓，堀遼平，吉川雅弥，藤野毅，“ビアプログラマブルアーキテクチャ VPEX3S～ 動作速度を改善するための基本論理素子の改良 ～”，電子情報通信学会技術研究報告, Vol.113, No.320, VLD2013-70, pp.75-80, Nov. 2013.

[16] 堀遼平，大谷拓，人見達郎，上口翔大．吉川雅弥，藤野毅，“ビアプログラマブルアーキテクチャ VPEX4 (1) ～ 配線混雑度改善と低消費電力性能向上のための基本論理素子の改良 ～”，電子情報通信学会技術研究報告, Vol.113, No.320, VLD2013-71, pp.81-86, Nov. 2013.

[17] 上口翔大，堀遼平，大谷拓，吉川雅弥，藤野毅，“ビアプログラマブルアーキテクチャ VPEX4 のベンチマーク回路を用いた性能評価”電子情報通信学会技術研究報告, Vol.113, No.320, VLD2013-72, pp.87-92, Nov. 2013.

[18] Mitsuru Shiozaki, Ryohei. Hori, and Takeshi Fujino, “Diffusion Programmable Device: The Device to Prevent Reverse Engineering”, IACR Cryptology ePrint Archive 2014/109, 2014.