様式 C-19

科学研究費補助金研究成果報告書

平成　23 年　6 月 24 日現在

機関番号：34315
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号：20560340
研究課題名（和文）
電子ビーム直描による耐タンパ性を備えた個人認証用ビアプログラムデバイスの研究
研究課題名（英文）　Via programmable logic device with tamper resistance fabricated by EB direct writing technique applied for user authentication
研究代表者
藤野　毅　　（　FUJINO　TAKESHI　）
立命館大学・理工学部・教授
研究者番号：60367993

研究成果の概要（和文）：
本研究では，電子ビーム直描を用いて多品種少量生産システム LSI を低コストで設計・製造できる手法に関する研究を行った．具体的には，２～３層のビア工程を変更するだけで，任意のロジックを構成することが可能な,ビアプログラマブルASICアーキテクチャVPEXを考案し，標準的な ASIC との性能・コストの比較を行った．この結果，性能指標である面積・遅延積（AD 積）は，ASIC の約２倍であり，数万個以下の生涯生産個数の LSI では ASIC より低コストであることが明らかになった．

研究成果の概要（英文）：
We have studied the LSI fabrication method using EB direct writing, which is cost effective even in the small lifetime production volume. We have proposed the via programmable structured ASIC architecture “VPEX”, in which any logic can be programmed by changing only 2-3 via layers. The performance and the cost of VPEX architecture were evaluated compared to standard ASIC architecture. The product of Area and Delay, which is the performance indices, is twice that of ASIC, and the total cost is lower than that of ASIC in the case that the lifetime production volume is less than several ten thousands units.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,100,000	330,000	1,430,000
2009 年度	1,200,000	360,000	1,560,000
2010 年度	1,200,000	360,000	1,560,000
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：電気電子工学
科研費の分科・細目：電気電子工学、電子デバイス、電子機器
キーワード：①半導体超微細化②先端機能デバイス③電子ビーム描画④プログラマブルロジック⑤サイドチャネルアタック

１．研究開始当初の背景

半導体集積回路の微細化の進展によって大容量のメモリとマイクロプロセッサなどのロジック回路を含む電子システムを、１チップの大規模集積回路(LSI)上に実現することが可能になった．このような「システム LSI」は、小型低消費電力かつ高性能な電子情報システムの実現に必須の技術となっている．

しかしながら，最先端のシステム LSI は非常に多額の初期開発費用が必要になっている．特に回路転写（フォトリソグラフィー）用の

原版であるフォトマスク費用は１億円以上と高額となっており，この費用負担によって，多品種少量生産システムＬＳＩの開発が非常に困難となっている．
少量生産システムLSIの低コスト化を進める方法として，フォトマスクを使用しない電子ビームウエハ直接描画（EB 直描）技術が注目されているが，ウエハを処理する速度が低く，実用化に至っていない．

２．研究の目的
本研究では，多品種少量生産システム LSI を経済的に設計・製造できる手法に対する解決方法を研究する．具体的には，上述の EB 直描技術を用いて，EB 直描技術に最適化した LSI 設計技術を構築することにより，EB 直描技術によるウエハ処理速度を飛躍的に向上させることを研究の目的としている．

３．研究の方法
われわれの提案する，ビアプログラマブルロジック VPEX は，基本素子として２入力排他的論理和（EXOR）を用い，第１ビア層と第３ビア層によって回路論理を決定する等の基本アーキテクチャは固まった．本 VPEX 技術は，米国電気電子学会 IEEE が主催する，Custom Integrated Circuits Conference にて論文が採択され，2007 年 9 月に米国サンノゼで発表し，その新規性（EXOR ゲートを用いていること，EB 直描にレイアウト最適化していること）と有効性（EXOR ゲートを用いた基本論理素子が，面積が小さく，低消費電力かつ高速であること）は認められた．
上記の VPEX ビアプログラマブルロジック研究成果を，自動設計ツールの研究やデバイス試作を通じてさらに進展させていくとともに，本技術を個人認証デバイスに使用する際に必要となる暗号回路の耐タンパ性に関する研究・無線電力転送およびインターフェースに関する研究を行う．具体的には次の（１）～（４）の項目を検討する．

（１）VPEX グローバルアーキテクチャの研究
VPEX の基本ロジックエレメントアーキテクチャをベースとして，基本素子間の配線手法などのグローバルアーキテクチャを改良し，より小面積で高速なアーキテクチャの研究を行う．

（２）ビアプログラマブルロジック用自動設計ツールの研究
上記のロジックエレメントに対して，実際に所望の回路を実装する上で，それぞれの素子に回路を割り当てていくための自動設計ツールの研究を行う．

（３）VPEX デバイス試作と動作検証
新しく提案した LSI アーキテクチャが有効であることを示すためには，やはり実デバイス（LSI）による動作の実証が必要となる．現在，ローム 0.18μmCMOS のデザインルールを用いてレイアウト設計に着手しており，小規模な回路を搭載した実証 LSI チップを，東京大学大規模集積システム設計教育研究センター（VDEC）を通して試作依頼する予定である．試作 LSI の製造完了は来年度となり，チップの評価および評価結果をフィードバックしたより大規模なチップを再試作・評価を実施していく．

（４）暗号回路の耐タンパ性に関する研究
暗号回路を実装した個人認証用デバイスでは，図２に示すように，暗号処理を実行している際の消費電力を解析することによりその暗号処理に使用している暗号鍵を推定するという「電力差分攻撃（DPA）によるサイドチャネルアタック」が問題となっている．当研究室でも，DPA に対する耐タンパ性を備えた回路の基礎検討を開始しており，「ドミノ型 RSL(Random Switching Logic)回路」を新しく考案した．今後， VPEX 技術にドミノ型 RSL の技術を取り込んだ VPEX の耐タンパ性技術に関して研究を行う．

４．研究成果
（１）VPEX グローバルアーキテクチャの研究

<2008 年度>
・VPEX の改良型アーキテクチャ VPEX2 の検討を行い，ディジタル回路の構成に必須な D-FF の面積を半減するロジックエレメントを採用することで，平均チップ面積を 20%削減できることを示した．

<2009 年度>
・VPEX の改良型アーキテクチャ VPEX2 では，レイアウトの最適化およびロジックエレメント構成素子の追加により，目的とする回路を構成したときのチップ面積の削減および演算性能の向上を実現した．本 VPEX2 アーキテクチャのロジックエレメント構造を特許出願するとともに，査読付き国際会議で発表した．

<2010 年度>
・VPEX の新改良型アーキテクチャ VPEX3 のアーキテクチャを考案した．ロジックエレメント構成素子の削減とレイアウトの抜本的見直し，およびプログラムレイアウトしてビア３層を使用することにより，目的とする回路を構成したときのチップ面積が昨年度の VPEX と比較して約1/3に削減できることが明らかになった．本新アーキテクチャは英文論文誌に投稿・査読中である．

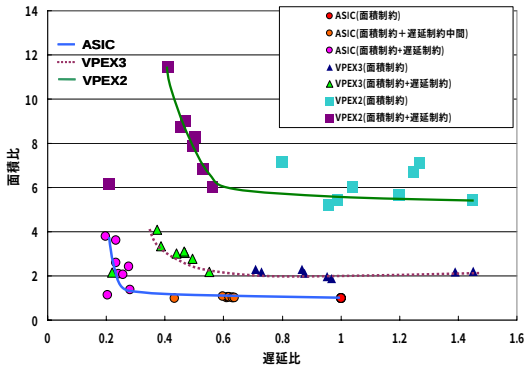

図１．新 VPEX3 アーキテクチャの評価結果

（２）ビアプログラマブルロジック用自動設計ツールの研究

<2008 年度>
・VPEX を使ったチップ作成のための設計自動化ツールの検討を行い，ロジックエレメントへの自動配置およびロジックエレメント間の配線を行う自動設計ツールのプロトタイプを完成させた．

<2009 年度>
・VPEX2 に対応した設計自動化ツール（HDL 記述よりレイアウトを自動生成するための自動配置配線ツール）を作成した．本ツールを使用して，VPEX2 の配線アーキテクチャの検討を行った．

<2010 年度>
・VPEX3 に対応した設計自動化フロー（HDL 記述よりレイアウトを自動生成するための自動配置配線ツール）を構築した．カナダの University of British Columbia との研究交流により，アメリカの大学が開発した自動配置ツール Capo と概略配線ツール FGR を VPEX3 の設計フローに取り込むことが可能になり，VPEX3 アーキテクチャの性能評価を正確に行うことができるようになった．

（３）VPEX デバイス試作と動作検証

<2008 年度>
・VPEX 技術(VPEX1)を使用して，ローム 0.18μmCMOS のデザインルールを用いてレイアウト作成を行い，チップ試作をおこなった．試作したチップは，FPGA ボードを用いて正常動作・電気的特性の評価を行った結果，基本論理素子の正常動作を確認した．

<2009 年度>
VPEX2 アーキテクチャを用い，ローム社 0.18μmCMOS プロセス上で配線遅延評価テストチップの設計を行った．通常の ASIC と比較した場合の配線遅延比較および，VPEX2 で採用している長距離配線用 BW(Bridge Wire)配線の効果を検討した．

<2010 年度>
ビアプログラマブルロジックにおいては，配線経路中のビア個数の増大に伴う抵抗の増加，配線経路上以外の余分な冗長配線上の寄生容量によって，ASIC と比較して，配線における信号遅延が増加する．この影響を定量的に評価するために，ローム社 0.18μmCMOS プロセス上で配線遅延評価テストチップのリングオシレータにより評価を行った．その結果と，上記 CAD ツールを用いて作製したチップレイアウトから，ビアプログラマブルロジックの配線遅延の定量的評価を行い，通常の ASIC に対して，約 1.5 倍の仮想配線容量を持つことを明らかにした．

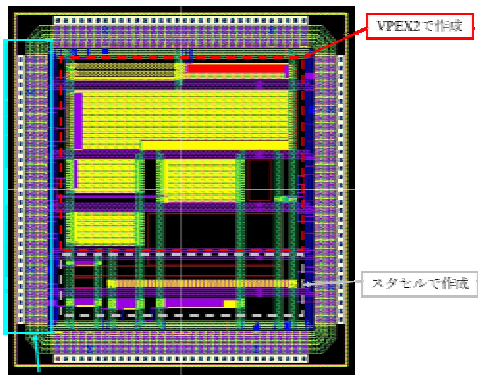

図２．ﾋﾞｱﾌﾟﾛｸﾞﾗﾏﾌﾞﾙ配線評価ﾃｽﾄﾁｯﾌﾟ

（４）暗号回路の耐タンパ性に関する研究

<2008 年度>
・VPEX 技術の応用アプリケーションとして，暗号処理回路を検討しているが，暗号処理を実行している際の消費電力を解析することによりその暗号処理に使用している暗号鍵を推定するという「電力差分攻撃（DPA）によるサイドチャネルアタック」対策が問題となっている．われわれの提案する「ドミノ型 RSL(Random Switching Logic)回路」回路がサイドチャネルアタックに耐性があることをシミュレーションにより確認した．

<2009 年度>
・VPEX 技術の応用アプリケーションとして，暗号処理回路を検討しているが，暗号処理を実行している際の消費電力を解析することによりその暗号処理に使用している暗号鍵を推定するという「電力差分攻撃（DPA）によるサイドチャネルアタック」対策が問題となっている．本サイドチャネル攻撃に対する耐性すなわち「耐タンパ性」に対して検討を行い，われわれの考案した「ドミノ RSL 回路」を用いることにより耐タンパ性が実現できることを FPGA 評価ボード上で検証した．

<2010 年度>
2009 年度 9 月より，JST/CREST の「ディペンダブル VLSI システムの基盤技術」において，「耐タンパディペンダブルＶＬＳＩシステムの開発・評価」のテーマで研究代表者として採択された．したがって 2010 年度以降の耐タンパ性に関する研究成果に関しては，その多くを JST/CREST の成果とみなせるため，省略する．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 11 件）
① 著書名：北森達也、堀遼平、上岡泰輔、吉川雅弥、藤野毅、論文標題：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、雑誌名：電子情報通信学会技術研究報告書、査読：無、巻：VLD2010-147、発行年：2011、ページ：183-188
② 著書名：上岡泰輔、北森達也、堀遼平、吉川雅弥、藤野毅、論文標題：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、雑誌名：電子情報通信学会技術研究報告書、査読：無、巻：VLD2010-146、発行年：2011、ページ：177-182
③ 著書名：岩井克彦、小島憲司、汐崎充、浅川俊介、藤野毅、論文標題：Domino-RSL 方式を用いた DPA 耐性を持つ DES 暗号回路の設計試作と安全性評価、雑誌名：電子情報通信学会技術研究報告書、査読：無、巻：VLD2010-126、発行年：2011、ページ：57-62
④ 著書名：堀遼平、北森達也、上岡泰輔、吉川雅弥、藤野毅、論文標題：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、雑誌名：電子情報通信学会技術研究報告書、査読：無、巻：ICD2010-91、発行年：2010、ページ：49－62
⑤ 著書名：西本智広、北森達也、國生雄一、山田翔太、藤野毅、吉川雅弥、論文標題：ビアプログラマブルデバイス VPEX の配線遅延評価、雑誌名：電子情報通信学会技術研究報告書、査読：無、巻：VLD2009-109、発行年：2010、ページ：61-66
⑥ 著書名：堀遼平、國生雄一、西本智広、山田翔太、吉田直之、藤野毅、吉川雅弥、論文標題：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、雑誌名：電子情報通信学会技術研究報告書、査読：無、巻：VLD2009-108、発行年：2010、ページ：55-60
⑦ 著書名：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、藤野毅、吉川雅弥、論文標題：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、雑誌名：電子情報通信学会技術研究報告書、査読：無、巻：VLD2009-107、発行年：2010、ページ：45-54
⑧ 著書名：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、論文標題：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、雑誌名：電子情報通信学会技術研究報告書、査読：無、巻：VLD2008－139、発行年：2009、ページ：77－82
⑨ 著書名：國生雄一、川原崎正英、石橋宏太、西本智広、北村一真、吉川雅弥、藤野毅、論文標題：ビアプログラマブルロジックデバイスVPEXにおける自動配置ツールの開発と性能評価、雑誌名：電子情報通信学会技術研究報告書、査読：無、巻：ICD2008-123、発行年：2008、ページ：107-112
⑩ 著書名：西本智広、 川原崎正英、 長谷川英司、 寺川知宏、 藤野毅、論文標題：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、雑誌名：電子情報通信学会技術研究報告書、査読：無、巻：ICD2008-122、発行年：2008、ページ:101-106
⑪ 著書名：A.Nakamura, M.Kawaharazaki, M.Yoshikawa, T.Fujino,論文標題：Regular Fabric of Via Programmable Logic Device using EXclusive-or Array (VPEX) for EB Direct Writing、雑誌名：IEICE TRANS. ELECTRON、査読：有、巻：Vol.E91-CNo.4、発行年：2008、ページ：509-516

〔学会発表〕（計 13 件）
① 発表者名：上岡泰輔、北森達也、堀遼平、吉川雅弥、藤野毅、発表標題：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、学会名：電子情報通信学会 VLSI 設計技術研究会、発表年月日：2011 年 3 月 3 日、発表場所：沖縄県男女共同参画センター「てぃるる」那覇市（沖縄県）
② 発表者名：北森達也、堀遼平、上岡泰輔、吉川雅弥、藤野毅、発表標題：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、学会名：電子情報通信学会 VLSI 設計技術研究会、発表年月日：2011 年 3 月 3 日、発表場所：沖縄県男女共同参画センター「てぃるる」那覇市（沖縄県）
③ 発表者名：堀遼平、北森達也、上岡泰輔、

吉川雅弥、藤野毅、発表標題：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、学会名：電子情報通信学会集積回路研究会、発表年月日：2010年11月29日、発表場所：九州大学　福岡市（福岡県）

④ 発表者名：M.Yoshikawa、Y.Kokusyo、T.Fujino、発表標題：Placement Tool Dedicated for a Via-programmable Logic Device VPEX、学会名：Proc. of 23rd International Conference on Computer Applications in Industry and Engineering、発表年月日：2010年11月8日、発表場所：ラスベガス　アメリカ

⑤ 発表者名：Kenji Kojima、Kazuki Okuyama、Katsuhiro Iwai、Mitsuru Shiozaki、Masaya Yoshikawa、Takeshi Fujino、発表標題：LSI Implementation Method of DES Cryptographic Circuit utilizing Domino-RSL Gate Resistant to DPA Attack、学会名：The 16th Workshop on Synthesis And System Integration of Mixed Information technologies、発表年月日：2010年10月18日、発表場所：台北市（台湾）

⑥ 発表者名：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、藤野毅、吉川雅弥、発表標題：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、学会名：電子情報通信学会VLSI設計技術研究会、発表年月日：2010年3月3日、発表場所：沖縄県男女共同参画センター「てぃるる」 那覇市（沖縄県）

⑦ 発表者名：西本智広、北森達也、國生雄一、山田翔太、藤野毅、吉川雅弥、発表標題：ビアプログラマブルデバイスVPEXの配線遅延評価、学会名：電子情報通信学会VLSI設計技術研究会、発表年月日：2010年3月3日、発表場所：沖縄県男女共同参画センター「てぃるる」那覇市（沖縄県）

⑧ 発表者名：堀遼平、國生雄一、西本智広、山田翔太、吉田直之、藤野毅、吉川雅弥、発表標題：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、学会名：電子情報通信学会VLSI設計技術研究会、発表年月日：2010年3月3日、発表場所：沖縄県男女共同参画センター「てぃるる」 那覇市（沖縄県）

⑨ 発表者名：Takeshi Fujino、Tomohiro Nishimoto、Yuichi Kokusyo、Masaya Yoshikawa、Guy Lemieux、発表標題：Via-programmable Logic Array VPEX2 with Configurable DFF using 2 Logic Elements、学会名：The 12th International Symposium on Integrated Circuits, B1.2、発表年月日：2009年12月14日-16日、発表場所：シンガポール（シンガポール）

⑩ 発表者名：Kazuma Kitamura、Syouta Yamada、Masahide Kawarasaki、Yuuichi Kokusyou、Usman Ahmed、Guy Lemieux、Masaya Yoshikawa、Takeshi Fujino、発表標題：Interconnect Utilization of the VPEX Via-Programmable Structured ASIC、学会名：The 15th Workshop on Synthesis And System Integration of Mixed Information technologies、発表年月日：2009年3月9日、発表場所：沖縄パシフィックホテル　那覇市（沖縄県）

⑪ 発表者名：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、発表標題：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、学会名：電子情報通信学会 VLSI 設計技術研究会、発表年月日：2009年3月、発表場所：沖縄県男女共同参画センター「てぃるる」那覇市（沖縄県）

⑫ 発表者名：西本智広、川原崎正英、長谷川英司、寺川知宏、藤野毅、発表標題：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、学会名：電子情報通信学会集積回路研究会、発表年月日：2008 年 12 月 11 日、発表場所：東京工業大学（東京都）

⑬ 発表者名：國生雄一、川原崎正英、石橋宏太、西本智広、北村一真、吉川雅弥、藤野毅、発表標題：ビアプログラマブルロジックデバイス VPEX における自動配置ツールの開発と性能評価、学会名：電子情報通信学会集積回路研究会、発表年月日：2008年12月11日、発表場所：東京工業大学（東京都）

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計１件）

名称：半導体装置およびその製造方法
発明者：藤野　毅
権利者：立命館大学
種類：特許
番号：特願2009-134429
出願年月日：2009年6月3日
国内外の別：国内

○取得状況（計０件）

〔その他〕

ホームページ等
http://www.ritsumei.ac.jp/se/re/fujinolab/

６．研究組織
(1)研究代表者
藤野　毅（ FUJINO TAKESHI ）
立命館大学・理工学部・教授
研究者番号：60367993
(2)研究分担者　なし
(3)連携研究者　なし