様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　５　月　１１　日現在

機関番号：　３２６８９
研究種目：　基盤研究(B)（一般）
研究期間：　2013～2015
課題番号：　２５２８００１７

研究課題名（和文）大域的超低エネルギー化を実現するLSI抽象モデルと上位下位統合化LSI設計技術

研究課題名（英文）Abstract LSI model and Its Associated Low-energy Integrated LSI Design Methodology

研究代表者
戸川　望（Togawa, Nozomu）

早稲田大学・理工学術院・教授

研究者番号：３０２９８１６１

交付決定額（研究期間全体）：（直接経費）　　14,000,000円

研究成果の概要（和文）：本研究では，LSI自動設計にて上位工程と下位工程の垣根を越えたエネルギー最適化を実現すべく，第一にLSI内部の三要素（レジスタ，制御回路，機能モジュール）に結合という概念を導入することで，LSI内部を単純化・抽象化することを提案，LSI抽象モデルを構築した．第二に提案したLSI抽象モデルのもと上位・下位工程を統合し超低エネルギー化を実現するLSI自動設計技術を構築，アルゴリズム体系化した．その結果，上位工程で極めて精度良く下位工程を予測・制御可能とし大域的な超低エネルギー化LSI自動設計を実現する．従来技術に比べ50%以上のエネルギー削減}を可能とするLSI自動設計技術を構築した．

研究成果の概要（英文）：In this research, we first propose an abstract LSI model, where functional units, registers and control units are packed into one functional block and hence interconnection delays can be ignored in it. Based on these functional blocks, we secondly propose a high-level synthesis algorithm which integrates behavioral synthesis and physical synthesis into a single synthesis flow. Experimental results demonstrate that our proposed synthesis algorithm successfully reduces the energy of a synthesized LSI chip by a maximum of 50%.

研究分野：　集積回路設計

キーワード：　高位合成　低エネルギー　低消費電力　LSI抽象モデル　統合化アルゴリズム

１．研究開始当初の背景

素子寸法の極限的な微細化により 1 つの LSI（大規模集積回路）の中に数億素子の集積を可能とした反面，1 つの LSI の消費電力は数百ワットにも達する．LSI の発熱は家庭用ホットプレートや原子炉に匹敵する場合もある．ユビキタス情報通信の中心的役割を担う LSI において消費エネルギーを劇的に削減することは喫緊の課題である．

一般に LSI 設計は数億個の素子を効率良く設計するため，上位工程（システムレベル等）と下位工程（トランジスタレベル等）に分離し別々に最適設計される．電力やエネルギー最適化の観点で見ると，抽象レベルが低い下位工程では見込み通りのエネルギー削減が得られるが電力やエネルギー削減は数%程度にとどまる．上位工程では 70¥%を越える大きなエネルギー削減を見込めるが下位工程が不確かな状態であり，見込み通りの電力やエネルギー削減効果が得られない．すなわち LSI の超低エネルギー化には上位・下位工程の融合・統一化による大域的最適化が必須である．

これに対し，上位工程と下位工程とを単に同一化する LSI 設計技術の研究は，これまで国内外でいくつか見られるが，これらは上位工程と下位工程を単純に単一化したため問題規模が実用レベルに到達しない，モジュール配置のみで配線を含まず配線遅延を正確に算出できない，といった問題点がある．上述した「下位レベルの LSI 抽象化」の構築には至っておらず，既存研究は従来の個別の上位工程および下位工程の自動化の範囲を越えるものではない}と言える．これら既存研究の本質的な問題点は，上位・下位の各 LSI 最適設計問題が組合せ問題として難しい問題（NP 困難問題）である一方で，単純にこれらを融合化し解法している点にある．申請者は超低エネルギー化を実現する上位・下位統合化には上位工程にとって必要十分な「下位工程の抽象化」とこれに基づく「LSI 抽象モデル」を確立すること，LSI 抽象モデルに基づく「低エネルギー指向統合化 LSI 設計アルゴリズムが強く求められると考える．

２．研究の目的

研究代表者らはこれまで LSI 性能に焦点を当て，上位・下位工程の統合化に挑戦し，上述の「抽象モデル化」への答えとして一般化レジスタ・制御分散モデルを構築した．これはレジスタ・制御回路を細粒度化し，機能モジュール（加算・乗算などの計算機能を持つモジュール）と共に LSI 内部に一様に分散配置するで上位工程で，配線遅延を含む下位工程の一部を制御可能としたものである．これをもとにした高位合成技術は，既存技術に比較して 40%以上性能向上する LSI 自動設計を実現した．

ここまでの成果は LSI 性能向上面で目覚しいものだったが LSI エネルギーの飛躍的削減の観点から見ると次の問題点がある：

問題 1：LSI 内部の三要素（レジスタ-制御-機能モジュール）がチップ全体に一様に散在し，上位工程から見た下位工程の抽象化が不十分である．これらの間の「結び付き」に既存技術を覆す，大胆な抽象化が必要である．

問題 2：機能モジュールにまとまりがなく統一的なエネルギー制御が困難である．何らかの結び付きが必要である．

問題 1・問題 2 に共通する本質の問題点は，LSI 内部にレジスタ・制御回路・機能ジュールが自由に散在する点にあり，LSI エネルギーの飛躍的削減の観点から LSI 抽象モデルを深めるには，以下に示すような抽象概念として，LSI 内部の抽象化が必須であると考える．

まず問題 1 を解決するため，LSI 内部の三要素を『強/弱の 2 種類の物理的な結合』で抽象化することを提案する．まず強い結びつきとして，レジスタ-制御-機能モジュールを完全に一体とするもので実質的に配線遅延 0 で三要素を結合する．そして次に弱い結ぶびつきとして，一定の遅延以下で内部通信可能な要素を論理的に緩やかにまとめる．LSI 自動設計において，タイミング設計がクリティカルとなる箇所を「結びつき」によって実現することで，結果的に上位工程から極めて精度良く下位工程を制御可能となる．

次に問題 2 を解決するため，LSI 内部の強い結びつきによって構成される回路モジュールに対して，意味的な結びつきを提案する．LSI 自動設計において，これら複数の機能モジュールで緩やな集合体を形成し電源，クロック，周波数制御を基本単位に統一制御を実現する．これにより上位工程と下位工程の垣根を越えた大域的なエネルギー最適化を図る．

３．研究の方法

(1) 低エネルギー化 LSI 抽象モデルの構築

これまで研究代表者らが提案してきた LSI 抽象モデルは，ハドルと呼ばれる回路ブロック（これはハドルと呼ばれる）に機能モジュール，レジスタ，コントローラをパッキングしたものであり，これを利用することで回路ブロック内部の配線遅延の影響を隠蔽することに成功し，高性能な高位合成・物理合成統合アルゴリズムを構築したものであった．これに対して本研究では，動的複数電源電圧と配線遅延を高位合成に統合する新たなレジスタ分散型アーキテクチャとして AVHDR（Adaptive Voltages Huddle-based Distributed-Register アーキテクチャ）を構築した．AVHDR では演算器とクロック同期するレジスタ，コントローラに異なる電源レールを用意し，演算器の電圧を pMOS ヘッダスイッチにより制御する．ヘッダスイッチに

より演算器の動的な電源電圧の制御が可能となる．レジスタ，コントローラの電圧は固定とし，割り当てる電圧は高位合成中に決定する．ハドルによる抽象化で配線遅延，ゲート遅延の双方を考慮しハドルに電圧を割り当てることが可能である．

ハドルは AVFUs と FVUs から構成されるものとする:

Adaptive Voltage Functional Units (AVFUs)
ハドルに集められた演算器，レベルコンバータの集合．ハドル内で処理する演算に必要な演算器を必要数持つ．AVFU の演算器とレベルコンバータはそれぞれハドルとは独立した電源レールに接続し，pMOS ヘッダスイッチにより電圧を制御する．ヘッダスイッチのオーバヘッドを考慮し，pMOS ヘッダスイッチは演算器ごとに用意する．レベルコンバータは電圧の低いレジスタからデータを読み込む演算器に 2 つ，電圧の高いレジスタにデータを書き込む演算器 1 つ用意する．演算器が VddL で動作する場合に出力側のレベルコンバータが必要となり，VddH で動作する場合に入力側のレベルコンバータが必要となる．

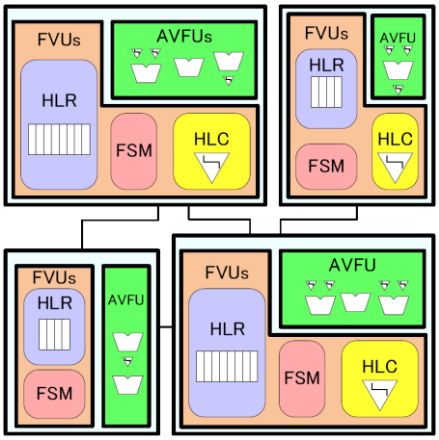

図 1: AVHDR による LSI 内部の抽象化

Fixed Voltage Units (FVUs)
ハドルに集められたレジスタ(HLR)，コントローラ(FSM)，レベルコンバータ(HLC)の集合．FVUs はクロック同期するため，1 つの電源レールと接続し動作中は一定の電圧が供給される．

Huddled Local Register (HLR)
各ハドル専用のローカルレジスタとマルチプレクサの集合．同一ハドルの AVFUs はハドル内の HLR のみにアクセスする．ハドル内は十分に近接しているため，配線遅延の影響を無視できる．

Finite State Machine (FSM)
各ハドル専用のコントローラ．同一ハドルの AVFU と HLR を制御する．AVFU の電圧も実行中に制御する．

Huddled Level Converter (HLC)
ハドルに集められたレベルコンバータの集合．HLR 間データ転送をする際，送信側の電圧が受信側の電圧より低い場合 HLC を用いる．

ハドルは図 1 のように構成される．同一ハドル内の AVFU でデータを処理する場合，ハドル内の HLR を使うことでデータ転送時間は無視できる．AVFU は FSM により動的に電源電圧が制御される．異なるハドルの HFU 同士でデータ通信する場合，HLR 間データ転送を行う．

(2) 低ネルギー化アルゴリズム

AVHDR はスケジューリング，バインディング結果でハドルの構成が決まり，ハドル間の通信の配線遅延が変化する．そのため，あらかじめスケジューリング，バインディング，フロアプランの回数を決定することは難しい．そこで本研究では，これらを反復改良するアルゴリズムを採用する．

アルゴリズム考案に向けて問題となるのが，AVHDR 特有の AVFUs の動的な電圧制御問題と FVUs の電圧制御問題の解法である．提案手法では，(A)動的複数電源電圧に対応したスケジューリング/FU バインディングと(B)ハドル電圧調整を実行する．(A)スケジューリング/FU バインディングにより AVFUs の動的な電圧制御問題を解決し，(B)スケジューリング/FU バインディングとハドル電圧調整を利用し，FVUs の電圧制御問題を解決する．

AVHDR を対象とする高位合成は以下の要素から構成される．

・初期ハドル合成
・スケジューリング/FU バインディング
・レジスタ/コントローラ合成
・ハドル電圧調整
・フロアプラン
・仮想面積見積もり
・フロアプラン指向ハドル合成

以上のうち，初期ハドル合成，フロアプラン，仮想面積見積もり，フロアプラン指向ハドル合成は，従来技術と同様の処理によって実現可能である．スケジューリング/FU バインディングはフロアプラン結果から配線遅延を見積もり，動的複数電源電圧，複数サイクルレジスタ間通信を考慮したスケジューリングおよび FU バインディングを行う．その際，AVFUs の動的な電圧制御を決定し，FVUs に割り当て可能な最も低い電圧を仮に割り当てる．レジスタ/コントローラ合成では，レジスタバインディングと従来のマルチプレクサ，レジスタの制御信号に加えて pMOS ヘッダスイッチの制御も行うコントローラを生成する．ハドル電圧調整ではレジスタ/コン

トローラ合成により決定したハドルの構成から，最適な電圧を選択し FVUs に割り当てる．

提案手法は大まかに初期処理，反復処理，調整処理の 3 つの処理に分割される．初期処理では各要素を通してハドルの初期配置を行う．反復処理ではチップ内部の実面積を利用せず，仮想面積見積もりを行うことで高速，かつ効率的に解を見つける．フロアプラン指向ハドル合成において，スケジューリング/FU バインディングで決定したタイミングを満たす解を得たとき反復処理を終了する．調整処理では反復処理で決定したスケジューリング，バインディング結果を基に正確な面積見積もりを決定し，所属する演算器のないハドルは消去し，最終的なフロアプラン結果を得る．タイミングを満たすフロアプラン結果が得られた時点で提案手法は終了する．

(2-1) スケジューリング/FU バインディング

スケジューリング/FU バインディングの入力は，クロック周期制約，ステップ制約，動作を表すコントロールデータフローグラフ，演算器数，ハドルの構成，配置情報である．出力は演算ノードを実行するコントロールステップ・電圧・演算器，各コントロールステップにおける演算器の電圧，FVUs の電圧である．電圧を変更する対象ハドルは優先度により選択するものとする．

スケジューリング/FU バインディングは(i)初期フェーズ，(ii)電圧上昇フェーズ，(iii)電圧下降フェーズ，(iv)動的電圧処理，(v)FVU 電圧下降，(vi)ステップ演算器電圧設定の 6 つのフェーズで構成される．初期フェーズは前回の反復時の配置，電圧を変更せずにスケジューリング/FU バインディングを行う．電圧上昇フェーズは初期フェーズの結果がステップ制約を満たさない場合実行され，ステップ制約を満たすようハドルごとに電圧を上げる．電圧下降フェーズはステップ制約を満たす範囲で消費エネルギーが最小となるようハドルごとに電圧を下げる．動的電圧処理はステップ制約を満たす範囲で消費エネルギーが最小となるよう，動的複数電源電圧により演算と AVFUs の電圧を下げる．FVU 電圧下降は FVUs の電圧を下げるものである．ステップ電圧設定は，各ステップで各演算器の電圧を決定するものである．

(2-2) レジスタ/コントローラ合成

レジスタ/コントローラ合成はスケジューリング/FU バインディング結果からハドルのレジスタ，コントローラの構成を決定する．特に，コントローラの構成はパワースイッチを制御する信号を考慮する必要がある．なおパワースイッチ制御信号は一意に決定することができる．

(2-3) ハドル電圧調節

ハドル電圧調整は全体の消費エネルギーを最小にする FVUs の電圧を決定する．レジスタ/コントローラ合成後，異なる電圧のハドル間通信に必要な HLC 以外のハドルの構成は決定する．FVUs の電圧が決定すれば必要な HLC 数は決定し，全体のエネルギーを見積もることが可能である．

ハドル電圧調整はスケジューリング/FU バインディング結果にもとづき最適な FVUs の電圧を決定する．そのため，遅延のオーバヘッドによるスケジューリング/FU バインディング結果への影響がないようにする．そのため，FVUs の電圧をスケジューリング/FU バインディングで決定した電圧より上げることは可能だが，下げることはできない．スケジューリング/FU バインディングで可能な限り FVUs の電圧を下げているため，電圧を上げる操作のみで効率よく最適な FVUs の電圧を探索できる．

４．研究成果

提案・構築した抽象 LSI モデルのもと，低エネルギー化アルゴリズムを C++言語を用いて計算機上に実装した．計算機実験環境は，CPU が AMD Quad-Core Opteron 2360 SE 2:5 GHz ×2，メモリ容量が 16GB である．対象アプリケーションとして DCT（ノード数 48），EWF3（ノード数 102），7 次 FIR フィルタ(ノード数 75）を用いた．各演算器は 16 ビット幅とし，クロック周期を 1.5 ns とする．電圧は 0.8V，1.0V，1.2V の 3 通りとした．

従来技術（GDR と RDR アーキテクチャ；レジスタ分散型アーキテクチャを利用した LSI 設計技術の一つ）と提案技術との比較結果を図 2 に示す．図 2 では GDR における消費エネルギーを 1.0 に正規化している．構築した LSI 抽象モデル AVHDR とこれに基づく低エネルギー化アルゴリズムによって，消費エネルギーを最大 63.0% ，平均 50.8%削減していることが確認できる．

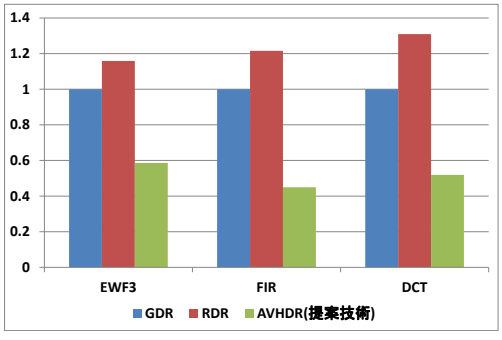

図 2 エネルギー評価結果

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２件）

[1]［査読有］ Masashi Tawada, Shinji

Kimura, Masao Yanagisawa, and Nozomu Togawa, ECC-based bit-write reduction code generation for non-volatile memory, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E98-A, no. 12, pp.2494-2504 2015, Dec. 2015, DOI: 10.1587/transfun.E98.A.2494.

[2] [査読有] Mika Fujishiro, Masao Yanagisawa, and Nozomu Togawa, Scan-based attack against trivium stream cipher using scan signatures, IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, vol. E97-A, no. 7, pp. 1444-1451, 2014, DOI: 10.1587/transfun.E97.A.1444.

〔学会発表〕(計３０件)

[1] 藤原晃一, 川村一志, 柳澤政生, 戸川望, クリティカルパス最適化フロアプラン指向 FPGA 高位合成手法のアプリケーション適用評価, 電子情報通信学会総合大会, 2016 年 3 月 15 日～2016 年 3 月 18 日, 福岡県福岡市.

[2] [査読有] Koki Igawa, Youhua Shi, Masao Yanagisawa, and Nozomu Togawa, A delay variation and floorplan aware high-level synthesis algorithm with body biasing, IEEE International Symposium on Quality Electronic Design (ISQED), 2016 年 3 月 15 日～2016 年 3 月 16 日, Santa Clara, USA.

[3] 藤原晃一, 川村一志, 柳澤政生, 戸川望, フロアプラン指向高位合成を用いたレジスタ分散型アーキテクチャ回路の FPGA 実装, 電子情報通信学会 VLSI 設計技術研究会, 2016 年 2 月 29 日～2016 年 3 月 2 日, 沖縄県那覇市.

[4] 吉田慎之介, 史又華, 柳澤政生, 戸川望, タイミングエラー耐性を持つ AES 暗号回路の設計, 電子情報通信学会 VLSI 設計技術研究会, 2016 年 2 月 29 日～2016 年 3 月 2 日, 沖縄県那覇市.

[5] 多和田雅師, 木村晋二, 柳澤政生, 戸川望, 冗長符号化を用いたマルチレベルセル不揮発性メモリ書き込み量削減, 電子情報通信学会 VLSI 設計技術研究会, 2016 年 1 月 19 日～2016 年 1 月 22 日, 神奈川県横浜市.

[6] 井川昂輝, 柳澤政生, 戸川望, 動的遅延ばらつきに対する適応性を考慮したフロアプラン指向高位合成手法の検討, 電子情報通信学会 VLSI 設計技術研究会, 2016 年 1 月 19 日～2016 年 1 月 22 日, 神奈川県 横浜市.

[7] 藤原晃一, 川村一志, 柳澤政生, 戸川望, 配線遅延とクロックスキューを利用したフロアプラン指向 FPGA 高位合成手法, 電子情報通信学会 VLSI 設計技術研究会, 2015 年 12 月 1 日～2015 年 12 月 3 日, 長崎県長崎市.

[8] 川村一志, 柳澤政生, 戸川望, タイミングエラー予測回路によるデータ依存最適化回路設計とその FPGA 評価, 電子情報通信学会 VLSI 設計技術研究会, 2015 年 12 月 1 日～2015 年 12 月 3 日, 長崎県長崎市.

[9] 多和田雅師, 木村晋二, 柳澤政生, 戸川望, 回路面積を考慮した不揮発性メモリ書き込み削減符号生成手法, 電子情報通信学会 VLSI 設計技術研究会, 2015 年 12 月 1 日～2015 年 12 月 3 日, 長崎県長崎市.

[10] [査読有] Koichi Fujiwara, Kazushi Kawamura, Masao Yanagisawa, and Nozomu Togawa, Clock skew estimate modeling for FPGA high-level synthesis and its application, IEEE 11th International Conference on ASIC, 2015 年 10 月 27 日～2015 年 10 月 30 日, Chengdu, China.

[11] 古城辰朗, 多和田雅師, 柳澤政生, 戸川望, 不揮発メモリを対象とした最大ハミング距離と最小ハミング距離を制約した符号による書き込み手法のエネルギー評価, 電子情報通信学会 VLSI 設計技術研究会, 2014 年 11 月 26 日～2014 年 11 月 28 日, 大分県別府市.

[12] 多和田雅師, 木村晋二, 柳澤政生, 戸川望, 不揮発メモリの書き込み削減手法のための小面積なエンコーダ/デコーダ回路構成, 電子情報通信学会 VLSI 設計技術研究会, 2014 年 11 月 26 日～2014 年 11 月 28 日, 大分県別府市.

[13] 吉田慎之介, 史又華, 柳澤政生, 戸川望, 回路面積を考慮した Suspicious Timing Error Prediction 回路の挿入位置決定手法の改良と評価, 電子情報通信学会 VLSI 設計技術研究会, 2014 年 11 月 26 日～2014 年 11 月 28 日, 大分県別府市.

[14] 川村一志, 阿部晋矢, 史又華, 柳澤政生, 戸川望, タイミングエラー予測回路による再構成可能デバイス上でのデータ依存最適化回路設計, 電子情報通信学会 VLSI 設計技術研究会, 2014 年 11 月 26 日～2014 年 11 月 28 日, 大分県別府市.

[15] [査読有] 吉田慎之介, 史又華, 柳澤政生, 戸川望, Suspicious Timing Error Prediction を用いた回路全体の遅延ばらつきに対するロバスト設計, 情報処理学会 DA シンポジウム 2014, 2014 年 8 月 28 日～2014 年 8 月 29 日, 岐阜県下呂市.

[16] [査読有] 古城辰朗, 多和田雅師, 柳澤政生, 戸川望, 最大ハミング距離と最小ハミング距離を制約した符号による

不揮発メモリの書き込み手法，電子情報通信学会第 27 回回路とシステムワークショップ，2014 年 8 月 4 日～2014 年 8 月 5 日，兵庫県淡路市.
[17][査読有] 吉田慎之介，史又華，柳澤政生，戸川望，回路面積を考慮した Suspicious Timing Error Prediction 回路の挿入位置決定手法，電子情報通信学会第 27 回回路とシステムワークショップ，2014 年 8 月 4 日～2014 年 8 月 5 日，兵庫県淡路市.
[18][招待講演] Kazushi Kawamura and Nozomu Togawa, Floorplan-driven architecture and high-level synthesis for hot-spot temperature optimization, The 29th International Technical Conference on Circuit/Systems Computers and Communications (ITC-CSCC 2014), Phuket, Thailand, 2014年7月1日～2014年7月4日, 2014.
[19][査読有] Mika Fujishiro, Masao Yanagisawa, and Nozomu Togawa, Scan-based attack on the LED block cipher using scan signatures, 2014 IEEE International Symposium on Circuits and Systems (ISCAS 2014), 2014 年 6 月 1 日～2014 年 6 月 5 日, Melbourne, Australia.
[20][査読有] Yuta Atobe, Youhua Shi, Masao Yanagisawa and Nozomu Togawa, Secure scan design with dynamically configuravle connection, 2013 IEEE 19th Pacific Rim International Symposium on Dependable Computing, 2013 年 12 月 4 日～2013 年 12 月 4 日, Vancouver, Canada.
[21]川村一志，柳澤政生，戸川望，信頼性と時間オーバーヘッド間のトレードオフを考慮した面積制約にもとづく RDR アーキテクチャ向けフォールトセキュア高位合成手法，電子情報通信学会 VLSI 設計技術研究会，2013 年 11 月 27 日～2013 年 11 月 29 日，鹿児島県鹿児島市.
[22]五十嵐博昭，史又華，柳澤政生，戸川望，チェックポイント観測によるタイミングエラー予測手法，電子情報通信学会 VLSI 設計技術研究会，2013 年 11 月 27 日～2013 年 11 月 29 日，鹿児島県鹿児島市.
[23][査読有] 藤代美佳，柳澤政生，戸川望，ストリーム暗号 Trivium に対するスキャンチェインの構造に依存しないスキャンベース攻撃手法，電子情報通信学会第 26 回回路とシステムワークショップ，2013 年 7 月 29 日～2013 年 7 月 30 日，兵庫県淡路市.
[24][査読有] 跡部悠太，史又華，柳澤政生，戸川望，ランダムオーダースキャンによるセキュアスキャン設計，電子情報通信学会第 26 回回路とシステムワークショップ，2013 年 7 月 29 日～2013 年 7 月 30 日，兵庫県淡路市.
[25][査読有] 川村一志，柳澤政生，戸川望，RDR アーキテクチャを対象とした時間・面積制約にもとづくフォールトセキュア高位合成手法，電子情報通信学会第 26 回回路とシステムワークショップ，2013 年 7 月 29 日～2013 年 7 月 30 日，兵庫県淡路市.
[26][招待講演] 戸川望，スキャンシグネチャを利用したブロック暗号に対するスキャンベース攻撃，電子情報通信学会第 26 回回路とシステムワークショップ，2013 年 7 月 29 日～2013 年 7 月 30 日，兵庫県淡路市.
[27][査読有] Kazushi Kawamura, Sho Tanaka, Masao Yanagisawa, and Nozomu Togawa, A partial redundant fault-secure high-level synthesis algorithm for RDR architectures, 2013 IEEE International Symposium on Circuits and Systems (ISCAS 2013), 2013 年 5 月 19 日～2013 年 5 月 23 日, Beijing, China.
[28][査読有] Hiroaki Igarashi, Youhua Shi, Masao Yanagisawa, and Nozomu Togawa, Concurrent faulty clock detection for crypto circuits against clock glitch based DFA, 2013 IEEE International Symposium on Circuits and Systems (ISCAS 2013), 2013 年 5 月 19 日～2013 年 5 月 23 日, Beijing, China.
[29]藤代美佳，柳澤政生，戸川望，スキャンシグネチャを用いたストリーム暗号 Trivium へのスキャンベース攻撃手法，電子情報通信学会 VLSI 設計技術研究会，2013 年 5 月 16 日，福岡県北九州市.
[30]川村一志，柳澤政生，戸川望，RDR アーキテクチャを対象とした時間及び面積オーバーヘッドのないフォールトセキュア高位合成手法，電子情報通信学会 VLSI 設計技術研究会，2013 年 5 月 16 日，福岡県北九州市.

〔その他〕
ホームページ
[1] http://www.togawa.cs.waseda.ac.jp/research/high_synthesis/high.html

６．研究組織
(1)研究代表者
戸川 望 (TOGAWA, Nozomu)
早稲田大学・理工学術院・教授
研究者番号：30298161

(2)研究分担者
木村 晋二 (KIMURA, Shinji)
早稲田大学・理工学術院・教授
研究者番号： 20183303