

## ★VLSI 設計技術研究会 (VLD)

専門委員長 戸川 望 副委員長 福田大輔  
幹事 小平行秀・桜井祐市 幹事補佐 池田一樹

## ★ハードウェアセキュリティ研究会 (HWS)

専門委員長 川村信一 副委員長 池田 誠・島崎靖久  
幹事 国井裕樹・小野貴継

日時 3月4日(水) 9:30~17:40  
5日(木) 9:30~17:15  
6日(金) 9:30~17:40  
7日(土) 10:30~14:15

会場 沖縄県青年会館(那覇市久米2-15-23, <http://www.okiseikan.or.jp/>)

議題 システムオンシリコンを支える設計技術, ハードウェアセキュリティ, 一般

### 4日午前 VLD-1:最適化手法

1. インデックス生成関数の行シフト分解における分解可能性判定法  
○常定京一郎・永山 忍・稲木雅人・若林真一(広島市大)
2. 集合対間配線における配線長さ削減を考慮した端子対間配線手法  
○和田邦彦・佐藤真平・高橋篤司(東工大)

### VLD-2:回路設計技術

3. EVBDDに基づく初等関数回路の設計検証 ○福原浩人・永山 忍・若林真一・稲木雅人(広島市大)
4. 複数プロセッサを用いた通信効率の良い行列ベクトル積演算の自動一般化手法 ○合田瑛洋・藤田昌宏(東大)
5. Via-Switch FPGAを対象とする算術演算アプリケーション回路の実装方式検討  
○今川隆司(立命館大)・劉 載勳(東工大)・橋本昌宜(阪大)・越智裕之(立命館大)

### 4日午後 VLD-3:低電力化技術

6. 2電源を用いた不揮発性フリップフロップの提案と評価 ○秋葉爽輔・宇佐美公良(芝浦工大)
7. 非同期式RTLモデルに対するラッチ挿入による動的電力最適化手法の検討 ○仙波翔吾・齋藤 寛(会津大)
8. LSIの最大消費電力を削減するスタック構造スタンダードセルライブラリ  
○今井祐貴(埼玉大)・西澤真一(福岡大)・伊藤和人(埼玉大)

### VLD-4:高信頼性設計(1)

9. フリップフロップの記憶保持特性とIDDQテストを組み合わせたプロセスばらつき推定  
○西澤真一(福岡大)・伊藤和人(埼玉大)
10. 製造後遅延調整における遅延調整素子のゲートサイジング手法 ○室井孝太・小平行秀(会津大)
11. 2グラフ制約表現による温度依存クロックス・キュー・スケジュール 金子峰雄(北陸先端大)

### VLD-5:リソグラフィ

12. ラグランジュ緩和法と境界Flippingによるプロセスばらつきを考慮したピクセルベースマスク最適化手法  
○東 梨奈・小平行秀(会津大)・松井知己・高橋篤司(東工大)・児玉親亮(キオクシア)
13. 機械学習を用いたリソグラフィホットスポット検出手法と評価に関して  
○高橋秀和・佐藤真平・高橋篤司(東工大)
14. リソグラフィホットスポット検出用既存訓練データの修正による訓練データの追加生成  
○片岡 岳・稲木雅人・永山 忍・若林真一(広島市大)
15. リソグラフィホットスポット検出のための画像スペクトルに基づく特徴量についての一検討  
○稲木雅人・片岡 岳・永山 忍・若林真一(広島市大)

### 5日午前 VLD-6:アルゴリズム

1. ドローンによる配送計画問題に対するモンテカルロ木探索手法 ○岩崎宏太・高島康裕(北九州市大)
2. HCP:History-based Congestion Prediction Algorithm for Network-on-Chip ○Zhenyu Hu・Michael Conrad Meyer(Waseda Univ.)・Xin Jiang(NITKIT)・Takahiro Watanabe(Waseda Univ.)

### VLD-7:高信頼性設計(2)

3. 電流兆候解析に基づくDCモーターのオンライン故障検知  
○大塚直樹(関西学院大)・神原弘之(京都高度技研)・石浦菜岐佐(関西学院大)
4. 誤差逆伝播を利用するメモリスタニユールネットワークの耐故障設計  
○石坂 守・新谷道広・井上美智子(奈良先端大)
5. 遅延故障に起因する回路寿命分布の確率的高速推定手法 ○富山葉月・増田 豊・石原 亨(名大)

### 5日午後 VLD-8:設計開発環境

6. プログラマブル SoC における Erlang からのハードウェア制御 ○若林秀和・石浦菜岐佐 (関西学院大)
7. Neural Programmer-Interpreters による実行形式の生成を目指した研究 ○津山雅彦・宮本龍介 (明大)
8. システムリソースを有効活用した H/W-S/W 協調設計支援手法 ○軽部文利・立見駿介・岡田尚也・山本 亮・小川吉大 (三菱電機)・ゴールドスミス アブラハム・クリネン リエン (MERL)

#### VLD-9: 記念講演

9. [記念講演] Small-Area and Low-Power FPGA-Based Multipliers using Approximate Elementary Modules  
○Yi Guo・Heming Sun・Shinji Kimura (Waseda Univ.)
10. [記念講演] A Tuning-Free Hardware Reservoir Based on MOSFET Crossbar Array for Practical Echo State Network Implementation  
○Yuki Kume・Song Bian・Takashi Sato (Kyoto Univ.)
11. [記念講演] ストレージ・クラス・メモリ (SCM) のデータ保持エラーとシステム性能のトレードオフを解決するマルチ SCM ストレージ向けデータ・エビクシオン自動調整システム  
○木下怜佳・松井千尋・鈴木敦也・福山将平・竹内 健 (中大)

#### VLD-10: 近似・ストカスティック計算

12. Approximate Floating Point Multiplier based on Shifting Addition Using Carry Signal from Second-Highest-Bit  
○Jie Li・Yi Guo・Shinji Kimura (Waseda Univ.)
13. 直近計算結果に基づく Approximate Computing を用いた画像のエッジ検出手法の提案と有効性評価  
○尾地 肇・宇佐美公良 (芝浦工大)
14. 乱数化関数を用いた乱数生成回路を共有するストカスティック数生成器 ○多和田雅師・戸川 望 (早大)

#### 6日午前 VLD-11: イジングマシン

1. イジングマシンを用いたアミューズメントパークの経路最適化手法  
○武笠陽介・若泉朋弥・田中 宗・戸川 望 (早大)
2. イジング計算機による 3次元直方体パッキング問題の解法  
○金丸 翔・寺田晃太郎・川村一志・田中 宗 (早大)・富田憲範 (富士通研)・戸川 望 (早大)

#### VLD-12: 応用事例

3. Isolation Forest による異常検知の効率化に関する検討  
○池田 翼・永山 忍・若林真一・稲木雅人 (広島市大)
4. 選択的な低処理遅延データ圧縮による高バンド幅相互結合網  
○丹羽直也 (慶大)・平澤将一・鯉渕道紘 (NII)・天野英晴 (慶大)
5. ハードウェアアクセラレータ内蔵仮想化対応トラフィック監視システムの開発  
○池田奈美子・右近祐太・大輝晶子・吉田周平・新田高庸 (NTT)

#### 6日午後 HWS-1

6. 順序回路の値取込みに発生する不均一な頻度分布を持つ誤りを用いた故障利用解析に関する基礎検討  
○岡本拓実・藤本大介 (奈良先端大)・崎山一男・李 陽 (電通大)・林 優一 (奈良先端大)
7. 無線通信 IC に対するサイドチャネル攻撃の基礎検討 ○一ノ瀬竜矢・坂本純一・松本 勉 (横浜国大)
8. Fp256 楕円曲線暗号の高速化に向けた設計空間探索 ○池田健人・池田 誠 (東大)

#### VLD-13: テスト・暗号化・ハードウェアトロイ

9. パーシャル MAX-SAT を用いた抵抗性オープン故障に対するテスト生成法 ○山崎紘史・石山悠太・松田竜馬・細川利典 (日大)・吉村正義 (京都産大)・新井雅之 (日大)・四柳浩之・橋爪正樹 (徳島大)
10. アフィン変換を用いた論理暗号化手法の評価 松永裕介 (九大)
11. トリガ回路の性質にもとづく特徴量を利用したニューラルネットワークによるハードウェアトロイ識別  
○井上智貴・長谷川健人・戸川 望 (早大)

#### VLD-14: ニューラルネットワーク実装

12. ゼロビットスキップ機能付きビットシリアル内積回路を用いた畳み込み演算の高速化に関する一検討  
○磯部 宙・富岡洋一 (会津大)
13. 制御機器における Deep Neural Network の FPGA 向け回路アーキテクチャの検討  
○山本 亮・岩河秀知・小川吉大 (三菱電機)
14. MOSFET クロスバアレイを用いる Echo State Network の精度評価  
○久米祐貴・辺 松・名倉健太・佐藤高史 (京大)
15. ニューラルネットワークの集積ナノフォトニクス実装に適した回路構造探索  
○服部直樹・増田 豊・石原 亨 (名大)・塩見 準 (京大)・新家昭彦・納富雅也 (NTT)

#### 7日午前 HWS-2

1. Non-IID PUF のエントロピー低下要因とエントロピー見積もり手法(1)  
○汐崎 充 (立命館大)・堀 洋平 (産総研)・大倉俊介・白畑正芳・藤野 毅 (立命館大)
2. Non-IID PUF のエントロピー低下要因とエントロピー見積もり手法(2)

○汐崎 充 (立命館大)・堀 洋平 (産総研)・大倉俊介・白畑正芳・藤野 毅 (立命館大)

3. 車線検出機能に対する色調改変攻撃 ○宮園史規・吉田直樹・松本 勉 (横浜国大)

7日午後 HWS-3

4. 誘導インパルス型の瞬時自己破壊回路を利用した検知後対処に基づく物理攻撃対策

○多田 捷・松田航平・永田 真 (神戸大)・崎山一男 (電通大)・三浦典之 (神戸大)

5. IC チップレベル電源雑音シミュレーションによる暗号モジュールのサイドチャンネル漏洩評価

○安田一樹・門田和樹・月岡暉裕・三浦典之・永田 真 (神戸大)・カシーク スリニバサン・シャン ワン・ラン  
リン・イン シェン リー・ノーマン チャン (アンシス)

6. 暗号回路における基板電流検出型レーザー故障注入攻撃対策の軽量設計法

○山下憂記・松田航平・永田 真・三浦典之 (神戸大)

☆VLD 研究会

**【問合せ先】**

小平行秀 (会津大)

E-mail : kohira@u-aizu.ac.jp

◎VLD 研究会ホームページも御覧下さい.

<http://www.ieice.org/~vld/>

☆HWS 研究会

**【問合せ先】**

三浦典之 (神戸大)・国井裕樹 (セコム)

E-mail : hws-sec@mail.ieice.org