様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 ２１ 日現在

機関番号：１４３０１
研究種目：基盤研究(B)（一般）
研究期間：2019～2023
課題番号：１９Ｈ０４０８４

研究課題名（和文）IoT システムのための形式検証手法の深化

研究課題名（英文）Enhancement of Formal Verification for IoT Systems

研究代表者
末永　幸平（Suenaga, Kohei）

京都大学・情報学研究科・准教授

研究者番号：７０６３３６９２

交付決定額（研究期間全体）：（直接経費）　　13,100,000円

研究成果の概要（和文）：IoT システムの数学的なモデルであるハイブリッドシステムのための形式検証手法を主眼において研究した．主な研究成果としては (1) ハイブリッドシステム検証のための PDR モデル検査アルゴリズムの拡張，(2) 束論を用いた PDR の本質の解明が得られた．この他にも，IoT システムに関わるソフトウェアの主要な実装言語であるポインタを含む命令型言語のための型理論に基づく検証手法や，ブラックボックスを含むシステムを効率的にテストする手法，機微情報を含むデータを暗号文のままでモニタリング可能とする秘匿モニタリング手法等の成果が得られた．

研究成果の学術的意義や社会的意義
この研究課題では，IoTシステムの安全性を確保するための新しい形式検証手法について扱った．特に，ソフトウェアと物理的プロセスが融合したハイブリッドシステムの安全性を保証するために，PDR (Property-Directed Reachability) と呼ばれるモデル検査手法を拡張した．この技術により，IoTデバイスが互いに安全に連携し，データを交換できるようになる．この成果は，社会全体のIoT技術の信頼性と効率を向上させ，高度なデジタル化社会の発展に大きく貢献する成果である．

研究成果の概要（英文）：This research project mainly focused on formal verification methods for hybrid systems, which are mathematical models of IoT systems. The main research results include (1) extension of the PDR model checking algorithm for verifying hybrid systems, and (2) elucidation of the essence of PDR using lattice theory. In addition, the following results were obtained: type-based verification for imperative languages equipped with pointers, methods for efficiently testing systems with black boxes, and methods for oblivious monitoring that allow monitoring of data containing sensitive information while it remains encrypted.

研究分野：形式検証

キーワード：ハイブリッドシステム　モデル検査　プログラム検証　形式検証　ブラックボックス検査　モニタリング　PDR

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

モノのインターネット（IoT; Internet of Things）は，センサーやアクチュエータを備えソフトウェアによって制御された物理デバイスが相互に接続しデータのやり取りを行う大規模ネットワークである．IoT の社会基盤化は国際的な潮流となっており，米国においては IoT 技術の高度化を目指すコンソーシアム IIC が立ち上げられ，ドイツにおいては第 4 次産業革命の社会実装を目指す Industrie 4.0 戦略が進展し，また日本においても第 5 期科学技術基本計画においてサイバー空間とフィジカル空間を融合させた社会 Society 5.0 が我が国の目指すべき未来社会の姿として提唱されている．この国際的潮流において，IoT システムの IoT の安全性保証が，学術的にも産業的にも重要性な研究課題となっている．

IoT システムの安全性検証の手段として，IoT システムの数学的なモデルであるハイブリッドシステム（ソフトウェアによる離散時間遷移と物理システムによる連続時間遷移が両方現れるシステム）の形式検証の研究が，研究代表者の末永らによるものを含め，多くなされている．形式検証とは，システムの安全性を数理的手法に基づいて証明する手法であり，ソフトウェアにおいてはすでに実用に供されるようになってきている．

ハイブリッドシステムの形式検証は概ね以下の通りに進む．形式検証において，検証器 V はシステムのモデル M と仕様 P を受け取る．モデル M は Simulink やハイブリッドオートマトン等のモデリング言語で記述され，仕様 P は論理式で記述されることが多い．検証器 V は，M が常に P を満たし続けるかどうかを M を実際に動作させることなく判定する．V は，もし P を満たし続けるのであればその証明を，P を満たさない状態に至りうるならばその動作履歴を生成する．

２．研究の目的

ハイブリッドシステムの形式検証手法を代表者のこれまでの成果を踏まえて研究する．具体的には，仕様主導可達性解析のハイブリッドシステムへの導入をメインとして研究を行う．ハイブリッドシステム検証の研究においては，モデル M が到達しうる状態の集合（到達可能集合）を近似し，その近似された集合が仕様 P に含まれていることを検証する手法が主流である．この手法では到達可能集合を近似するコストがボトルネックとなっており，大規模ハイブリッドシステムにスケールさせるための障害となっている．この問題を解決するために，ソフトウェア検証の分野で研究され一定の成功を収めている仕様主導可達性（Property-Directed Reachability; PDR）の手法をハイブリッドシステムに適用する．PDR は到達可能集合の計算において，モデル M のみではなく検証すべき仕様 P も考慮する手法である．他の検証手法と比較した PDR の特徴は主に二点あり，(1) M のみから到達可能集合の近似を求める場合と違い，P によって近似の精密さをコントロールできる点に特徴があり，P が検証の容易な性質であれば近似を求める計算が短時間で済むことが多く，(2) PDR は他の検証手法と同様に近似を求めるために必要な制約の解消のために外部ソルバへの問い合わせを行うが，他の検証手法が複雑な問い合わせを少数発行することで近似を一度に求めようとするモノリシックなアルゴリズムであるのに比べ，PDR は軽量な問い合わせを多数発行することで徐々に近似を求めようとするインクリメンタルなアルゴリズムとして設計されている．

また，これに加えて，IoT システムにおけるモニタリングや（プロプライエタリな部品を含んだり機械学習で実装されている等の理由で）ブラックボックスを含む IoT システムを効率よくテストするための手法の研究を行う．

3. 研究の方法

すでに確立している形式検証手法研究の方法論を取る．一般的に形式検証手法の研究においては，(1) モデル（今回はハイブリッドシステム）の動作を状態遷移システムとして数学的に定義し，(2) 検証アルゴリズムをモデル M を受け取って M の安全性を判定するアルゴズムとして定義し，(3) そのアルゴリズムの健全性（検証によって「安全」という結果が得られたときに M に危険な動作が存在し得ないこと）を証明する．本研究においてもこの手法を取ることで，最終的な検証器の信頼性を高めることを目指し，その健全性の証明を完了させる．

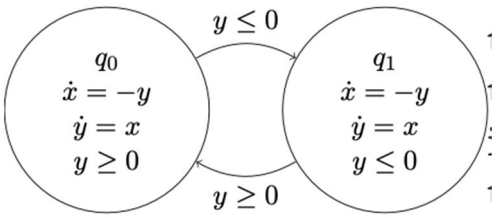
４．研究成果

以下に得られた主な成果の概要を述べる．

モデル検査手法 PDR のハイブリッドシステムへの適用と理論的基盤：PDR (Property-Directed Reachability) はシステムの安全性を検証するためのモデル検査手法の一種であり，状態遷移シ

ステムの帰納的不変条件とよばれる，1 ステップの遷移で不変であり，かつシステムの安全性を保証できる程度に強力な条件を発見するための手法である．テンプレートを用いる手法や抽象解釈を用いる手法に比べて，初期状態から i ステップの遷移で到達可能な状態集合の over-approximation であるフレーム R_i の列であるフレーム列 $R_0, R_1, \cdots, R_N$ を保持し，計算の途中で発見された反例の解析を通じてこのフレーム列を精緻化したり延長したりしつつ帰納的不変条件に収束させようとする点に特徴がある．PDR はソフトウェアのモデル検査において近年広く用いられるようになっており，大規模なシステムへの応用も多くなされている．

本研究課題で対象とする IoT システムに PDR を適用するにあたっては，以下の２つの問題があった．



(1) 既存の PDR は離散的な状態遷移システムに対して定義されている．一方，IoT システムはセンサやアクチュエータの動作に連続時間遷移を含むハイブリッドシステムであるため，既存の PDR をそのまま使用することができなかった．具体的には，このようなシステムは左図のような，各状態に微分方程式が記述されたハイブリッドオートマトンとよばれる状態機械で表現できるが，このような状態機械に対して適用することのできる PDR は研究されていなかった．

(2) PDR は扱うシステムやアルゴリズムに応じて様々な変種が別個に提案されており，かつそれぞれの手法を統一的に扱う方法が知られていなかった．そのため，さまざまなアルゴリズムの変種を試す場合に，一からアルゴリズムの設計を繰り返す必要があり，かつアルゴリズムの本質が見えにくいという問題があった．

この問題を解決するために，本研究課題ではハイブリッドシステムへの応用を見据えた PDR の本質を明らかにするための研究を行った．主に以下の２つの成果が上がった．

$$
\begin{array}{ll}
\textsc{Initialize} & \rightsquigarrow \emptyset \mid\mid \langle R_0 := \mathcal{F}_{\mathcal{H}}(\lambda q.\mathit{false}); R_{rem} := \lambda q.\mathit{true}; N := 0\rangle \\
& \quad \textbf{if } \forall q \in Q.\models R_0(q) \implies \varphi_P \\
\textsc{Valid} & M \mid\mid A \rightsquigarrow \textbf{Valid} \\
& \quad \textbf{if } \exists i < N. \forall q \in Q.\models R_i(q) \implies R_{i-1}(q) \\
\textsc{Unfold} & M \mid\mid A \rightsquigarrow \emptyset \mid\mid A[R_{N+1} := \lambda q.\mathit{true}; R_{rem} := \lambda q.\mathit{true}; N := N+1] \\
& \quad \textbf{if } \forall q \in Q.\models R_{rem}(q) \implies \varphi_P \\
\textsc{Induction} & M \mid\mid A \rightsquigarrow \emptyset \mid\mid A[R_j := \lambda q.R_j(q) \wedge R(q)]_{j=1}^{i+1} \\
& \quad \textbf{if } \forall q \in Q.\models \mathcal{F}_{\mathcal{H}}(\lambda q.R_i(q) \wedge R(q))(q) \implies R(q) \\
\textsc{Decide} & \langle \sigma_2, q_2, i+1\rangle\ M \mid\mid A \rightsquigarrow \langle \sigma_1, q_1, i\rangle\ \langle \sigma_2, q_2, i+1\rangle\ M \mid\mid A \\
& \quad \textbf{if } \langle q_1, \varphi, \varphi_c, q_2\rangle \in \delta \textbf{ and } \sigma_1, \sigma_2' \models R_i(q_1) \wedge \langle F(q_1) \mid \mathit{inv}(q_1)\rangle(\varphi \wedge \varphi_c) \\
\textsc{Model} & \langle \sigma, q_0, 0\rangle\ M \mid\mid A \rightsquigarrow \textbf{Model}\ \langle \sigma, q_0, 0\rangle\ M \\
\textsc{Conflict} & \langle \sigma', q', i+1\rangle\ M \mid\mid A \rightsquigarrow \emptyset \mid\mid A[R_j := \lambda q.R_j(q) \wedge R(q)]_{j=1}^{i+1} \\
& \quad \textbf{if } \models R(q') \implies \neg\sigma' \textbf{ and } \forall q \in Q.\models \mathcal{F}_{\mathcal{H}}(R_i)(q) \implies R(q) \\
\textsc{PropagateCont} & M \mid\mid A \rightsquigarrow M \mid\mid A[R_{rem} := \lambda q.R_{rem}(q) \wedge R(q)] \\
& \quad \textbf{if } \forall q \in Q.\models R_N(q) \vee \mathcal{F}_C(R_N)(q) \implies R(q) \\
\textsc{CandidateCont} & \emptyset \mid\mid A \rightsquigarrow \langle \sigma, q, \mathit{rem}\rangle \mid\mid A \\
& \quad \textbf{if } \sigma \models R_{rem}(q) \wedge \neg\varphi_P \\
\textsc{DecideCont} & \langle \sigma_2, q, \mathit{rem}\rangle \mid\mid A \rightsquigarrow \langle \sigma_1, q, N\rangle\ \langle \sigma_2, q, \mathit{rem}\rangle \mid\mid A \\
& \quad \textbf{if } \sigma_1, \sigma_2' \models R_N(q) \wedge \langle F(q) \mid \mathit{inv}(q)\rangle(\boldsymbol{x} = \boldsymbol{x}') \\
\textsc{ConflictCont} & \langle \sigma', q', \mathit{rem}\rangle \mid\mid A \rightsquigarrow \emptyset \mid\mid A[R_{rem} := \lambda q.R_{rem}(q) \wedge R(q)] \\
& \quad \textbf{if } R(q') \implies \neg\sigma', \textbf{and} \models R_N(q') \vee \mathcal{F}_C(R_N)(q') \implies R(q')
\end{array}
$$

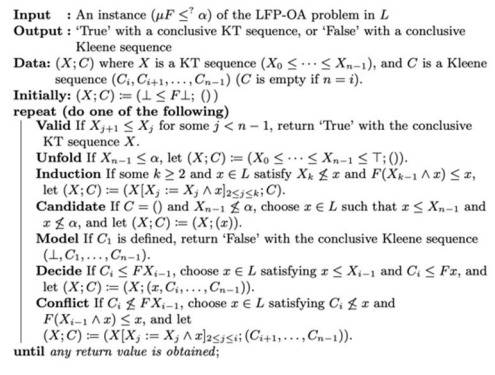
Hybrid PDR: ハイブリッドシステム検証のための PDR の拡張 [VMCAI'20]： 連続時間遷移を含むシステムのための PDR の拡張を行った．具体的には [Hoder et al. SAT'12] において提案された Generic PDR (GPDR) と呼ばれる PDR の形式化に対し，離散時間遷移と連続時間遷移が交互に現れるようなシステムのための拡張を行った．これにより，ハイブリッドオートマトンで表現される遷移を扱うことが可能となった．

提案した HybridPDR を上図に示す．拡張前の PDR と異なるのは，主に以下の二点である．

(1) 拡張前の PDR においては，フレーム列 $R_0, R_1, \cdots, R_N$ を扱うアルゴリズムとして手法が定義されていた．一方拡張後の手法では，フレーム列の末尾に，R_N から一回の連続時間遷移で到達できる状態集合の over-approximation を表す特別なフレーム R_{rem} を設けた．そのうえで，フレーム R_i は初期状態から「離散遷移を一回行ってから有限時間の連続時間遷移を経る」という遷移を i 回行って到達可能な集合の over-approximation と意味づけた．これにより，ハイブリッドオートマトンによって引き起こされる状態遷移が PDR において捉えられるようになった．

(2) GPDR におけるフレーム列の操作において，離散時間遷移と連続時間遷移が両方捉えられるように各種定義を拡張した．これにより，前記 1 の特徴と併せて，ハイブリッドオートマトンのための PDR が定義できることになった．

提案手法の正しさの証明を行った上で，この手法に基づいたソフトウェアを実装し，実験を行った．実装したソフトウェアは https://github.com/ksuenaga/HybridPDR にて公開している．



Input : An instance $(\mu F \leq^{?} \alpha)$ of the LFP-OA problem in L
Output : 'True' with a conclusive KT sequence, or 'False' with a conclusive Kleene sequence
Data: $(X; C)$ where X is a KT sequence $(X_0 \leq \cdots \leq X_{n-1})$, and C is a Kleene sequence $(C_i, C_{i+1}, \ldots, C_{n-1})$ (C is empty if $n = i$).
Initially: $(X; C) \coloneqq (\bot \leq F\bot;\ ())$
repeat (do one of the following)
- **Valid** If $X_{j+1} \leq X_j$ for some $j < n-1$, return 'True' with the conclusive KT sequence X.
- **Unfold** If $X_{n-1} \leq \alpha$, let $(X; C) \coloneqq (X_0 \leq \cdots \leq X_{n-1} \leq \top; ())$.
- **Induction** If some $k \geq 2$ and $x \in L$ satisfy $X_k \not\leq x$ and $F(X_{k-1} \wedge x) \leq x$, let $(X; C) \coloneqq (X[X_j \coloneqq X_j \wedge x]_{2 \leq j \leq k}; C)$.
- **Candidate** If $C = ()$ and $X_{n-1} \not\leq \alpha$, choose $x \in L$ such that $x \leq X_{n-1}$ and $x \not\leq \alpha$, and let $(X; C) \coloneqq (X; (x))$.
- **Model** If C_1 is defined, return 'False' with the conclusive Kleene sequence $(\bot, C_1, \ldots, C_{n-1})$.
- **Decide** If $C_i \leq FX_{i-1}$, choose $x \in L$ satisfying $x \leq X_{i-1}$ and $C_i \leq Fx$, and let $(X; C) \coloneqq (X; (x, C_i, \ldots, C_{n-1}))$.
- **Conflict** If $C_i \not\leq FX_{i-1}$, choose $x \in L$ satisfying $C_i \not\leq x$ and $F(X_{i-1} \wedge x) \leq x$, and let $(X; C) \coloneqq (X[X_j \coloneqq X_j \wedge x]_{2 \leq j \leq i}; (C_{i+1}, \ldots, C_{n-1}))$.

until *any return value is obtained*;

束論を用いた PDR の本質の解明 [CAV'22]：これまでの PDR に関する研究ではフレームの意味論を状態の集合や論理式等の具体的な表現で与えて形式化することがほとんどであった．このような方法では，例えば確率的なシステムについて PDR を拡張する場合などに新たな表現が必要になる等，拡張性に問題がある．また，PDR を具体的なフレーム表現で定式化することにより，PDR のどの特徴がフレームの特定のデータ表現に固有の特徴で，どの部分が PDR の本質であるかについての見通しが悪くなるという難点がある．

この問題に対し，フレームの意味を様々なアプリケーションにおける PDR の適用を包摂する一般的な数学的構造である束（ある条件を満たす半順序集合）の元で与えることで PDR の抽象的な定式化を与えた．また，様々な PDR の変種がこの束による定式化のインスタンスとして得られることを示し，実験で有効性を示した．

５．主な発表論文等

〔雑誌論文〕　計13件（うち査読付論文　11件／うち国際共著　6件／うちオープンアクセス　11件）

１．著者名 Shijubo Junya、Waga Masaki、Suenaga Kohei	４．巻 12974
２．論文標題 Efficient Black-Box Checking via Model Checking with Strengthened Specifications	５．発行年 2021年
３．雑誌名 Lecture Notes in Computer Science book series	６．最初と最後の頁 100～120
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-88494-9_6	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kawamoto Yusuke、Sato Tetsuya、Suenaga Kohei	４．巻 N/A
２．論文標題 Formalizing Statistical Beliefs in Hypothesis Testing Using Program Logic	５．発行年 2021年
３．雑誌名 Proceedings of the 18th International Conference on Principles of Knowledge Representation and Reasoning(KR)	６．最初と最後の頁 411～421
掲載論文のDOI（デジタルオブジェクト識別子） 10.24963/kr.2021/39	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Nishida Yuki、Saito Hiromasa、Chen Ran、Kawata Akira、Furuse Jun、Suenaga Kohei、Igarashi Atsushi	４．巻 12652
２．論文標題 Helmholtz: A Verifier for Tezos Smart Contracts Based on Refinement Types	５．発行年 2021年
３．雑誌名 Lecture Notes in Computer Science book series	６．最初と最後の頁 262～280
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-72013-1_14	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Kori Mayuko、Urabe Natsuki、Katsumata Shin-ya、Suenaga Kohei、Hasuo Ichiro	４．巻 13371
２．論文標題 The Lattice-Theoretic Essence of Property Directed Reachability Analysis	５．発行年 2022年
３．雑誌名 Lecture Notes in Computer Science book series	６．最初と最後の頁 235～256
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-13185-1_12	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Banno Ryotaro、Matsuoka Kotaro、Matsumoto Naoki、Bian Song、Waga Masaki、Suenaga Kohei	4．巻 13371
2．論文標題 Oblivious Online Monitoring for?Safety LTL Specification via?Fully Homomorphic Encryption	5．発行年 2022年
3．雑誌名 Lecture Notes in Computer Science book series	6．最初と最後の頁 447～468
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-13185-1_22	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Nishida Yuki、Saito Hiromasa、Chen Ran、Kawata Akira、Furuse Jun、Suenaga Kohei、Igarashi Atsushi	4．巻 40
2．論文標題 Helmholtz: A Verifier for Tezos Smart Contracts Based on Refinement Types	5．発行年 2022年
3．雑誌名 New Generation Computing	6．最初と最後の頁 507～540
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-022-00167-1	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Nishida Yuki、Saito Hiromasa、Chen Ran、Kawata Akira、Furuse Jun、Suenaga Kohei、Igarashi Atsushi	4．巻 12652
2．論文標題 Helmholtz: A Verifier for Tezos Smart Contracts Based on Refinement Types	5．発行年 2021年
3．雑誌名 ETAPS 2021	6．最初と最後の頁 262～280
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-72013-1_14	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Ichiro Hasuo, Yuichiro Oyabu, Clovis Eberhart, Kohei Suenaga, Kenta Cho 0002,	4．巻 -
2．論文標題 Control-Data Separation and Logical Condition Propagation for Efficient Inference on Probabilistic Programs	5．発行年 2021年
3．雑誌名 arXiv	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Hatakeyama Yuhki、Sakuma Hiroki、Konishi Yoshinori、Suenaga Kohei	4．巻 12624
2．論文標題 Visualizing Color-Wise Saliency of Black-Box Image Classification Models	5．発行年 2021年
3．雑誌名 ACCV 2020	6．最初と最後の頁 189～205
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-69535-4_12	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Toman John、Siqi Ren、Suenaga Kohei、Igarashi Atsushi、Kobayashi Naoki	4．巻 12075
2．論文標題 ConSORT: Context- and Flow-Sensitive Ownership Refinement Types for Imperative Programs	5．発行年 2020年
3．雑誌名 ESOP 2020	6．最初と最後の頁 684～714
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-44914-8_25	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Suenaga Kohei、Ishizawa Takuya	4．巻 11990
2．論文標題 Generalized Property-Directed Reachability for Hybrid Systems	5．発行年 2020年
3．雑誌名 VMCAI 2020	6．最初と最後の頁 293～313
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-39322-9_14	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Gu Yu、Tsukada Takeshi、Unno Hiroshi	4．巻 7
2．論文標題 Optimal CHC Solving via Termination Proofs	5．発行年 2023年
3．雑誌名 Proceedings of the ACM on Programming Languages	6．最初と最後の頁 604～631
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3571214	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Gu Yu、Tsukada Takeshi、Unno Hiroshi	4．巻 7
2．論文標題 Optimal CHC Solving via Termination Proofs	5．発行年 2023年
3．雑誌名 Proceedings of the ACM on Programming Languages	6．最初と最後の頁 604～631
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3571214	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計13件（うち招待講演　0件／うち国際学会　5件）

1．発表者名 伴野 良太郎 ， 松岡 航太郎 ， 松本 直樹 ， Bian Song ， 和賀 正樹 ， 末永 幸平
2．発表標題 完全準同型暗号を用いた秘匿LTLオンラインモニタリング
3．学会等名 コンピュータセキュリティシンポジウム 2021 (CSS 2021)
4．発表年 2021年

1．発表者名 小野 雄登 ， 西田 雄気 ， 古瀬 淳 ， 末永 幸平 ， 五十嵐 淳
2．発表標題 スマートコントラクト検証器Helmholtzのためのエラー原因提示手法
3．学会等名 日本ソフトウェア科学会 第39回大会
4．発表年 2022年

1．発表者名 服部 佑哉 ， 西田 雄気 ， 古瀬 淳 ， 末永 幸平 ， 五十嵐 淳
2．発表標題 SCameleer: スマートコントラクト記述言語SCamlのための自動検証器
3．学会等名 日本ソフトウェア科学会 第39回大会
4．発表年 2022年

１．発表者名
Mayuko Kori, Natsuki Urabe, Shin-ya Katsumata, Kohei Suenaga, Ichiro Hasuo

２．発表標題
The Lattice-Theoretic Essence of Property Directed Reachability Analysis

３．学会等名
CAV 2022（国際学会）

４．発表年
2022年

１．発表者名
Ryotaro Banno, Kotaro Matsuoka, Naoki Matsumoto, Song Bian, Masaki Waga, Kohei Suenaga

２．発表標題
Oblivious Online Monitoring for Safety LTL Specification via Fully Homomorphic Encryption

３．学会等名
CAV 2022（国際学会）

４．発表年
2022年

１．発表者名
Junya Shijubo, Masaki Waga, Kohei Suenaga

２．発表標題
Efficient Black-Box Checking via Model Checking with Strengthened Specifications

３．学会等名
RV 2021（国際学会）

４．発表年
2021年

１．発表者名
Yusuke Kawamoto, Tetsuya Sato, Kohei Suenaga

２．発表標題
Formalizing Statistical Beliefs in Hypothesis Testing Using Program Logic.

３．学会等名
KR 2021（国際学会）

４．発表年
2021年

１．発表者名
Yuki Nishida, Hiromasa Saito, Ran Chen, Akira Kawata, Jun Furuse, Kohei Suenaga, Atsushi Igarashi

２．発表標題
Helmholtz: A Verifier for Tezos Smart Contracts Based on Refinement Types.

３．学会等名
TACAS 2021（国際学会）

４．発表年
2021年

１．発表者名
畠山雄気，佐久間宏樹，小西嘉典，末永幸平

２．発表標題
ブラックボックス画像分類モデルの否定的判断根拠と色情報根拠の可視化

３．学会等名
MIRU 2020

４．発表年
2020年

１．発表者名
伴野良太郎，佐藤聡太，古瀬淳，末永幸平，五十嵐淳

２．発表標題
暗号通貨向けストレージシステムにおけるデータ永続化処理の形式検証

３．学会等名
PPL 2021

４．発表年
2021年

１．発表者名
四十坊純也，和賀正樹，末永幸平

２．発表標題
物理情報システムに対するブラックボックス検査の構文的仕様強化による最適化

３．学会等名
PPL 2021

４．発表年
2021年

１．発表者名 佐藤 聡太，古瀬 淳，末永 幸平，五十嵐 淳
２．発表標題 F*を用いたMerkle Patricia Treeライブラリの形式検証
３．学会等名 PPL 2020
４．発表年 2020年

１．発表者名 齋藤 大聖，西田 雄気，五十嵐 淳，末永 幸平
２．発表標題 スマートコントラクトのための Effectively Callback-Free 性の型に基づく静的検証
３．学会等名 PPL 2020
４．発表年 2020年

〔図書〕　計1件

１．著者名 徳山 豪、小林 直樹	４．発行年 2022年
２．出版社 朝倉書店	５．総ページ数 800
３．書名 理論計算機科学事典（8.3節「型に基づくプログラム検証」）	

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	五十嵐　淳 (Igarashi Atsushi) (40323456)	京都大学・情報学研究科・教授 (14301)	

６．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	海野　広志 (Unno Hiroshi) (80569575)	筑波大学・システム情報系・准教授 (12102)	
研究分担者	池渕　未来 (Ikebuchi Mirai) (70961796)	京都大学・情報学研究科・助教 (14301)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関