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　４ 年　 ６ 月 １３ 日現在

機関番号：３２６８９
研究種目：挑戦的研究（萌芽）
研究期間：2018～2021
課題番号：１８Ｋ１９７８７

研究課題名（和文）サイドチャネル攻撃耐タンパ性のためのプログラム検証・プログラム合成技術

研究課題名（英文）Program verification and program synthesis for side-channel attack resilience

研究代表者
寺内　多智弘（Terauchi, Tachio）

早稲田大学・理工学術院・教授

研究者番号：７０４４７１５０

交付決定額（研究期間全体）：（直接経費）　　4,800,000円

研究成果の概要（和文）：Bucketingというタイミング攻撃に対する防衛手段によって得られる安全性およびその限界についての研究を行い成果を得た。確率的adaptiveなである一般的なサイドチャネル攻撃に対する安全性を議論するためのゲーム理論に基づく枠組みを提案した。Spectre攻撃、ReDoS攻撃といった代表的なタイミング攻撃についての研究を行った。加えて、一階述語不動点論理による時相仕様検証、述語制約による関係的仕様の検証、循環証明による分離論理のための定理証明、必勝戦略合成による量化子を含む一階述語論理式の真偽性判定に関する研究など、関連する一般的なプログラム検証および定理証明についての研究も行った。

研究成果の学術的意義や社会的意義
Bucketingによるタイミング攻撃防衛手法の安全性について初めて形式的な保証を得ることや、確率的かつadaptiveなサイドチャネル攻撃に対する一般的な安全性の議論を可能とするゲーム理論に基づく枠組みを構築するなど、本研究はこれまでのプログラミング言語・形式検証によるセキュリティの研究を大きく飛躍させた。よって、本研究の成果は極めて高い学術的および社会的意義を持つと考える。

研究成果の概要（英文）：We have conducted a research on a formal analysis of a timing channel attack mitigation technique called "bucketing". We have obtained results on provable security guarantees achievable with the technique as well as its theoretical limits. We have proposed a game theoretic general framework for proving security of a system against probabilistic and adaptive side channel attacks. We have conducted research on Spectre attacks and ReDoS attacks which are popular timing attacks. Additionally, we have conducted research on more general program verification and automated deduction, including temporal property verification by first-order fixpoint logic solving, relational property verification by predicate constraint solving, type and effect systems for algebraic effects and handlers, and automated deduction for quantified formulas by game solving.

研究分野：コンピュータサイエンス

キーワード：サイドチャネル攻撃　耐タンパ性　プログラム検証　プログラム合成　情報セキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景
サイドチャネル攻撃とは、実行時間や消費電力など、プログラム動作中に観測できる「サイドチャネル情報」を利用して機密を盗み出す攻撃である。正規の入出力のみを観測する通常の攻撃と比べ痕跡を残しにくく、また、安価な環境で実現が可能であるなど、サイドチャネル攻撃は情報セキュリティへの深刻な脅威であるとされている。

一方、「プログラム検証」とは、プログラミング言語研究分野の主要テーマの一つであり、静的コード解析によりプログラム動作を理解する手法である。古くは、定数伝播などコンパイラ最適化のための単純な解析に留まるが、より近年では、ソフトウェアモデル検査など高精度な手法の研究が進み、複雑なプログラムの高精度な自動検証が現実的になるなど驚異的な進化を遂げている。また、仕様を満たすプログラムを（部分的に）自動生成する「プログラム合成」も、プログラム解析・検証の研究成果を応用することで近年著しく成長を遂げている。

応募者の先行研究も含め、サイドチャネル攻撃検出・防衛のためのプログラム検証・プログラム合成が研究されてきたが、対象として扱える攻撃・プログラム・防衛手段が限られるなどの問題があった。

２．研究の目的
本研究のねらいは、近年急速に発展したプログラム検証・合成などプログラミング言語研究の技術を、サイドチャネル攻撃のための耐タンパ技術へ応用することである。しかし、従来の検証・合成手法はサイドチャネルに関する情報を十分に考慮していない。実際、タイミング攻撃の検出のためのプログラム検証や差分電力解析攻撃に対する耐タンパ性のためのプログラム合成などサイドチャネル攻撃の検出・防衛を目的としたプログラム検証・合成も研究されているが簡易的なサイドチャネルのモデルを用いる場合が多く、現実の攻撃の対策には不十分である。そこで、本研究は、リゴラスなサイドチャネル攻撃耐タンパ性のためのプログラム検証・プログラム合成技術の確立を目指す。

３．研究の方法
応募者のプログラム検証によるタイミング攻撃検出方法やプログラム解析と制約解消による差分電力解析等の攻撃に対する防衛コードを自動生成等の先行研究などで得られた知見を基に研究を行う。一般的に、プログラム検証・合成においては、実機上でのプログラム動作を直接対象とするのは現実的ではないため、「プログラム意味論」という動作を数理論理的に簡潔に定式化したモデルを考える。意味論は目的に必要な情報のみ定式化すればよいため、通常はサイドチャネル情報は十分に考慮されない。そこで、本研究は、まず目的となるサイドチャネルの対策に十分な情報を含む意味論を構築する。また、述語抽象・CEGAR など、近年のプログラム検証・
合成に用いられる基礎技術をサイドチャネル情報を扱う意味論に対応する形へ拡張する。そして、拡張された基礎技術を用い、サイドチャネル攻撃に関するプログラム検証・合成の手法を確立する。

４．研究成果
サイドチャネル攻撃の検出・防衛のためのプログラム検証・プログラム合成について研究を行った。特に形式理論に裏付けられた証明可能な安全性の保証を得られる方法について研究を行い成果を得た。より具体的には、以下の研究成果を得た。

- タイミング攻撃の基礎理論に関する研究を行った。具体的には、どのようなプログラムおよび攻撃者に対して bucketing によるタイミング攻撃に対する防衛手法が有効であるのか調査することを目指し、bucketing により安全性の保証を得るための必要条件および十分条件に関する成果を得た。これら、必要条件・十分条件は解析対象システムの正規チャネルとサイドチャネルの安全性を分離して議論することを可能とする枠組みであり、また、過去の観測に依存した動作を行える強力な adaptive な攻撃者を考慮している。この研究の成果はまとめた論文はセキュリティに関する国際会議 The 8th International Conference on Principles of Security and Trust (POST 2019)に採録された。

- 確率的かつ adaptive な攻撃者に対する安全性を議論するためのゲーム理論に基づく枠組みについて研究を行った。具体的には、n-round r-confidence ゲームという新たなゲームを提案し、このゲームが確率的かつ adaptive な攻撃に対する安全性を正確に表現することを証明した。この研究の成果をまとめた論文はセキュリティに関する国際会議 The 32nd IEEE Computer Security Foundations Symposium (CSF 2019)に採録された。

- Bucketing によるタイミング攻撃防衛の研究の拡張を行った。具体的には、POST 2019 で提案した条件を強化することにより、より多くのプログラムに対して、より強い安全性の保証が可能となった。また、本手法の枠組みで得られる保証の理論的限界についての結果も得た。成果をまとめた論文はセキュリティに関する国際論文誌 Journal of Computer Security に採録された。

- これまでのサイドチャネル攻撃に関する基礎的研究で得られた知見を元に、タイミング攻撃を用いた代表的な攻撃手段である Spectre 攻撃および Regular expression Denial of Service (ReDoS) 攻撃に関する研究を行った。Spectre 攻撃に関しては、近年 speculative non-interference, weak speculative noninterference, speculative constant-time-security など多数の形式的定義が提案されており、それぞれの利点・問題点を明らかにする研究を行った。また、静的コード解析による Spectre 攻撃脆弱性の検出についても研究を行った。ReDoS 攻撃に関しては、後方参照・先読み後読みなどの機能で拡張された拡張正規表現の ReDoS 脆弱性を修正する手法について研究を行った。

- 加えて、一階述語不動点論理による時相仕様検証、述語制約による関係的仕様の検証、循環証明による分離論理のための定理証明、必勝戦略合成による量化子を含む一階述語論理式の真偽性判定に関する研究、代数的エフェクト・ハンドラを含むプログラムのための時相仕様検証、述語制約解消による関係的仕様の検証など、関連するより一般的なプログラム検証および定理証明についての研究も行った。

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　6件／うち国際共著　5件／うちオープンアクセス　4件）

１．著者名 Hiroshi Unno, Tachio Terauchi, Eric Koskinen	４．巻 12759
２．論文標題 Constraint-Based Relational Verification	５．発行年 2021年
３．雑誌名 In Proceedings of the 33rd International Conference on Computer-Aided Verification (CAV 2021)	６．最初と最後の頁 742～766
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-81685-8_35	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 Terauchi Tachio, Antonopoulos Timos	４．巻 28
２．論文標題 Bucketing and information flow analysis for provable timing attack mitigation	５．発行年 2020年
３．雑誌名 Journal of Computer Security	６．最初と最後の頁 607～634
掲載論文のDOI（デジタルオブジェクト識別子） 10.3233/JCS-191356	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 該当する

１．著者名 Timos Antonopoulos, Tachio Terauchi	４．巻 CSF 2019
２．論文標題 Games for Security Under Adaptive Adversaries	５．発行年 2019年
３．雑誌名 In Proceedings of the 32nd IEEE Computer Security Foundations Symposium (CSF 2019)	６．最初と最後の頁 216～229
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CSF.2019.00022	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 該当する

１．著者名 Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, Hiroshi Unno	４．巻 37
２．論文標題 Failure of Cut-Elimination in Cyclic Proofs of Separation Logic	５．発行年 2020年
３．雑誌名 コンピュータ ソフトウェア	６．最初と最後の頁 1_39～1_52
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.37.1_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 Tachio Terauchi, Timos Antonopoulos	4．巻 11426
2．論文標題 A Formal Analysis of Timing Channel Security via Bucketing	5．発行年 2019年
3．雑誌名 Proceedings of the 8th International Conference on Principles of Security and Trust (POST 2019), Lecture Notes in Computer Science 11426, Springer	6．最初と最後の頁 29〜50
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-17138-4_2	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 Yoji Nanjo, Hiroshi Unno, Eric Koskinen, Tachio Terauchi	4．巻 LICS 2018
2．論文標題 A Fixpoint Logic and Dependent Effects for Temporal Property Verification	5．発行年 2018年
3．雑誌名 Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2018), ACM	6．最初と最後の頁 759〜768
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3209108.3209204	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

〔学会発表〕　計10件（うち招待講演　4件／うち国際学会　7件）

1．発表者名 川俣楓河、寺内多智弘
2．発表標題 代数的エフェクトハンドラを持つ言語のためのトレースエフェクト
3．学会等名 ソフトウェア科学会 第24回プログラミングおよびプログラミング言語ワークショップ (PPL 2022)
4．発表年 2022年

1．発表者名 Nariyoshi Chida, Tachio Terauchi
2．発表標題 Repairing DoS Vulnerability of Real-World Regexes
3．学会等名 ソフトウェア科学会 第24回プログラミングおよびプログラミング言語ワークショップ (PPL 2022)
4．発表年 2022年

１．発表者名
Tachio Terauchi

２．発表標題
Constraint-based Relational Verification

３．学会等名
Workshop on Hyperproperties: Advances in Theory and Practice (HYPER 2021)（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
Yoji Nanjo, Hiroshi Unno, Eric Koskinen, Tachio Terauchi

２．発表標題
A Fixpoint Logic and Dependent Effects for Temporal Property Verification

３．学会等名
Dagstuhl Seminar 19371: Deduction Beyond Satisfiability（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Souta Yamauchi, Tachio Terauchi

２．発表標題
Inferring Simple Strategies for Efficient Quantified SMT Solving

３．学会等名
17th Asian Symposium on Programming Languages and Systems (APLAS 2019)（国際学会）

４．発表年
2019年

１．発表者名
Takashi Nishikawa, Yuki Satake, Yoji Nanjo, Hiroshi Unno, Naoki Kobayashi, Tachio Terauchi, Eric Koskinen

２．発表標題
Solving First-Order Fixpoint Logic for Program Verification

３．学会等名
Third Workshop on Mathematical Logic and its Applications (MLA 2019)（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Koji Nakazawa, Daisuke Kimura, Tachio Terauchi, Hiroshi Unno, Kenji Saotome

２．発表標題
On Cut-Elimination Theorem in Cyclic-Proof Systems

３．学会等名
Third Workshop on Mathematical Logic and its Applications (MLA 2019)（国際学会）

４．発表年
2019年

１．発表者名
Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, Hiroshi Unno

２．発表標題
Failure of Cut-Elimination in Cyclic Proofs of Separation Logic

３．学会等名
日本ソフトウェア科学会 第21回プログラミングおよびプログラミング言語ワークショップ（PPL2019）

４．発表年
2019年

１．発表者名
Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, Hiroshi Unno

２．発表標題
On Cut-elimination in Cyclic Proof Systems

３．学会等名
The 4th Workshop on New Ideas and Emerging Results in Programming Languages and Systems (NIER 2018)（国際学会）

４．発表年
2019年

１．発表者名
Tachio Terauchi

２．発表標題
Information Flow Security and its Applications to Side Channel Attack Resilience

３．学会等名
The 4th Franco-Japanese Workshop on Cybersecurity（招待講演）（国際学会）

４．発表年
2018年

〔図書〕　計0件

〔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

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