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 ２０ 日現在

機関番号：３４４１２
研究種目：基盤研究(C)（一般）
研究期間：2018～2021
課題番号：１８Ｋ０２９１７

研究課題名（和文）情報セキュリティ人材育成のための暗号技術学習支援eラーニングシステムの開発

研究課題名（英文）Development of e-learning system for human resource development in the information security field

研究代表者
村上　恭通（Murakami, Yasuyuki）

大阪電気通信大学・情報通信工学部・教授

研究者番号：５０３６８１７２

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究では(1)個々の暗号技術とその学習教材の開発、(2)暗号技術の組み合わせによる暗号プロトコルの構成に関する学習教材の開発、(3)上記(1),(2)を統合する教育用ユーザインタフェースおよび教材システム開発と評価、を行った。
(1)については、暗号プロトコルの安全性自動検証ツールProVerifにより、暗号学的ハッシュ関数・ブロックチェーン等の暗号技術の形式化を行った。(2)については、教育効果に配慮して穴埋め問題・デバッグ問題などを効果的に織り交ぜた教材を開発した。(3)については、開発したeラーニングシステムを学内に設置し、外部からインターネット経由で本システムを利用できる環境を整えた。

研究成果の学術的意義や社会的意義
本研究課題では、計算機援用による形式的暗号プロトコル安全性検証ツールを利用した暗号技術の基礎知識、利用方法を学習するCAI教材の開発を行った。形式的暗号プロトコル安全性検証ツールの利用により、既存の教材では実現しえない実際の暗号技術の動作や攻撃を、学習者が設定した暗号システム上でシミュレーションしてインタラクティブに学べる、より学習効果の高い教材を実現でき、本研究課題の成果は暗号技術の基礎知識を身に着けた情報セキュリティに強いICT技術者の育成に大きく貢献できると考えられる。

研究成果の概要（英文）：In this research, we studied the followings: (1) development of individual cryptographic techniques and learning materials of them, (2) development of learning materials on the composition of cryptographic protocols by combining cryptographic techniques, and (3) development and evaluation of the e-learning system that integrates the above (1) and (2). Regarding (1), we have formalized cryptographic technologies such as cryptographic hash functions and blockchains using ProVerif which is the cryptographic protocol security automatic verification tool. Regarding (2), we have developed teaching materials that effectively interweave fill-in-the-blank questions and debugging questions in consideration of educational effects. Regarding (3), we have developed e-learning server and publicized this system in order to be used from outside via the Internet.

研究分野：暗号と情報セキュリティ

キーワード：情報セキュリティ人材育成　暗号技術学習支援　eラーニングシステム　形式化　安全性自動検証　ProVerif　Moodle　Virtual Programing Lab

様式Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

我が国の情報セキュリティ向上は急務であるが、それを担う情報セキュリティ人材の不足が叫ばれている。情報セキュリティはウィルスやネットワーク不正侵入、情報漏洩の防御等の様々な分野での対策が必要であるが、暗号技術はそれらの対策を実現する基盤技術に位置づけられる。さらに暗号技術は、フィンテックや IoT 等の次代の産業を興すための要素技術としても期待されている。しかし、暗号の専門家以外のネットワーク技術者等の暗号技術を利用する立場の ICT 技術者には十分に暗号技術に関する知識が共有されているとは言い難い。例えば、インターネットの標準暗号プロトコルである SSL/TLS の実装において、POODLE、HeartBleed 等のセキュリティホールが相次いで発見されたが、これらのほとんどは実装した者が暗号技術を正しく理解していなかったことに起因する。暗号学の成り立ちが計算機科学、数学、通信工学等の様々な研究分野の境界領域上にあるために、暗号技術の技術文書が非常に難解なテクニカルタームを利用したり、学術的、あるいは技術的に厳格な書式を取ったりして難解に記載されていることが一因である。この問題に対し、一般の ICT 技術者への説明責任を果たしていないということが、暗号研究者の間でしばしば議論されるようになった。現状のような難解な表現を用いずに暗号研究者以外にも理解しやすく、かつ厳密性を失わずに正しく説明を行うためには何らかの革新的な表現方法を用いる必要があり、形式検証技術はその有力な表現方法の一つとして期待されている。

暗号学において、形式検証技術は主に計算機援用による安全性検証に利用されている。形式的安全性検証では暗号に関する概念や定理の証明のライブラリ化、あるいは要素技術や安全性要件のモデル化を形式記述言語を用いて研究者が行い、計算機を用いて安全性を検証する。一度ライブラリ化、モデル化された技術要素は誰もが再利用可能であるので、安全性検証のみならず、暗号に関する専門知識を有しない ICT 技術者を対象とした、暗号技術のドキュメント化や CAI 教材としても利用することも可能となる。

研究代表者・村上は卒業研究指導において情報セキュリティ、特に暗号に関する指導をマンツーマンで行っているが、これを多人数向けの授業形式に適応することは困難であった。一方で研究分担者・岡崎、布田は暗号プロトコル安全性の形式検証システムの開発の一環として、検証システムの利用方法に関する CAI 教材作成を進めていた。村上は岡崎等の安全性検証システム利用教材が、ツールの利用のみならず暗号理論そのものの CAI 教材としても利用可能であると気づき、本研究の着想に至った。

海外を中心に既に暗号技術に関する様々な CAI 教材が公開されている。研究代表者の調べた限り先行研究は大別して既存の暗号理論の教科書そのまま解説したもの、具体的な暗号技術の方式を解説したものに大別される。前者は本研究で解決を目指す問題点をそのまま含んでおり、後者は要素技術の実装解説が目的であり、暗号の安全性の概念や攻撃モデル、暗号技術の正しい利用方法を解説する本研究の目的とは位置づけが異なる。

研究代表者は、素因数分解が困難となるように RSA 暗号の秘密鍵となる素数を生成する方法に関する研究、量子コンピュータに対抗し得る公開鍵暗号としてナップザック暗号の開発や組織間機密通信に適した暗号システムの提案等を行ってきた。オープンキャンパスや模擬授業用の暗号体験教材や moodle による暗号技術学習 Web 教材を開発した。研究分担者らは暗号の形式検証に従事しており、その一部として ProVerif を用いた暗号プロトコルの安全性検証システムの開発を行ってきている。また、Mizar を用いて楕円曲線暗号で利用される楕円曲線や、格子暗号で利用される Z 加群の格子、数論アルゴリズムの実行動作に関して、形式検証で必要となる形式化ライブラリを作成した。さらにこれらの形式化数学ライブラリを応用し、moodle 上で大学学部教育用の数学証明問題 CAI 教材の開発を行っている。

研究分担者・岡崎、布田が共同で行っている暗号プロトコル安全性の形式検証システムの開発にて、形式的定理証明検証システム Mizar および形式的暗号プロトコル安全性検証ツール ProVerif を用いて暗号技術に関する様々なライブラリやモデルの開発を既に行っている。本研究課題では上記の成果を教材化し、広く普及した LMS の一つである moodle のアドインとして開発する。岡崎等には既に Mizar を用いた数学教育システムの moodle アドイン開発を行った実績があり、本課題では暗号技術の教育を行うための教材のプレゼンテーション方法の探求が主な課題となる。一方で研究代表者・村上は学科講義においてアルゴリズム・プログラミングの初年次教育を行う際に、Scratch 等のビジュアルプログラミング言語や PAD 等のプログラム構造表記法を活用し、より教育効果の高い授業を行うノウハウを有している。そのため本研究課題では CAI 教材を開発する計算機及び、作成した教材を公開し、多人数授業で利用して実証実験を行う負荷に耐え得る moodle サーバを準備できれば本研究課題は実行することが可能である。

２．研究の目的

計算機援用による形式的暗号プロトコル安全性検証ツールを利用した暗号技術の基礎知識、利用方法を学習する CAI 教材の開発を行う。既存の教材や解説書のほとんどは上記の暗号機能

や規格の解説、すなわち暗号研究者や暗号技術者向けであり、それらを利用する ICT 技術者の大半を占めるネットワーク技術者や、暗号技術を利用したシステムやアプリケーション開発者等の暗号利用者を対象としたものは少ない。ICT 技術者にとっては個々の暗号技術(ハッシュ関数、公開鍵暗号、電子署名等)の実装方法や基礎理論は必要なく、それらを利用する目的(どのような攻撃を防ぐか)と利用する際の入力データの管理方針(どのようなデータを入力すると安全性を保てなくなるか)、どのように暗号技術を組み合わせれば目的の安全性を達成できるか等である。ICT 技術者がこのような暗号の利用方法を学ぶ際には、目的(データの秘匿、相手認証、改竄検知等やその組み合わせ)を実現するために暗号技術を用いたシステムやアプリケーションを実際に設計し、攻撃をシミュレーションすることが効果的であろう。形式的暗号プロトコル安全性検証ツールを適切に利用すれば、どのようなプロトコルを設計しても、もし攻撃が成功するのであれば具体的な攻撃手順を導出するため ICT 技術者にとって直観的に理解しやすい教材を作成できる。また、開発を行わず主に開発済の暗号システムの運用に従事する ICT 技術者にとっても、鍵や ID などの入力データが正しく管理されなければ攻撃が成功することもあるため、本研究では暗号システム運用のための教材作成も行う予定である。暗号プロトコル安全性検証ツールを用いて安全性検証を行うために高度な専門知識を要するが、ユーザインタフェースの工夫による可視化と、学習対象となる暗号技術を厳選し、学習者の理解度に応じて複雑な組み合わせのプロトコルを出題するスパイラル型コース設計を行うことにより、学習効果の高い暗号教材が実現できると考える。以下の図 1 に本研究課題で実現する CAI システムの概要を示す。

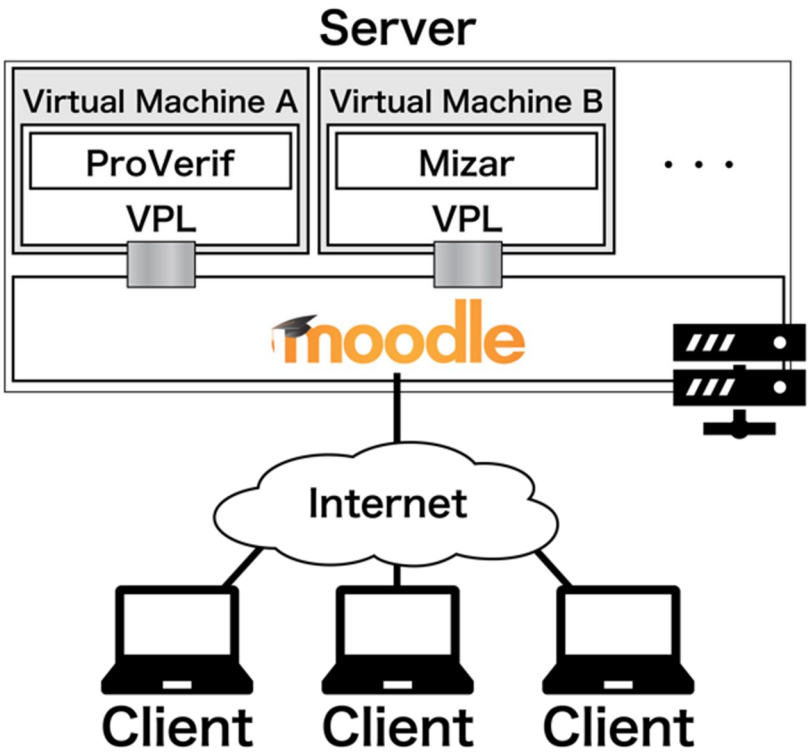

図 1. システム概要

本研究課題では、計算機援用による形式的暗号プロトコル安全性検証ツールを利用した暗号技術の基礎知識、利用方法を学習する CAI 教材の開発を行う。形式的暗号プロトコル安全性検証ツールの利用により、既存の教材では実現しえない実際の暗号技術の動作や攻撃を、学習者が設定した暗号システム上でシミュレーションしてインタラクティブに学べる、より学習効果の高い教材を実現でき、本研究課題の成果は暗号技術の基礎知識を身に着けた情報セキュリティに強い ICT 技術者の育成に大きく貢献できると考えられる。

3．研究の方法

本研究課題を遂行するために、(1)個々の暗号技術とその学習教材の開発、(2)暗号技術の組み合わせによる暗号プロトコルの構成に関する学習教材の開発、(3)上記(1),(2)を統合する教育用ユーザインタフェースおよび教材システム開発と評価、を行う。

(1) 個々の暗号技術とその学習教材の開発
研究代表者は暗号技術(公開鍵として安全な素数の設計・量子コンピュータに対抗し得る暗号・組織間通信に適した暗号)の研究開発を行っている。分担者等は暗号プロトコルモデル探索ツール ProVerif と形式的定理証明支援ツール Mizar を共用する安全性検証ツールの開発を行っている。このツールのために暗号技術についての諸定理やモデルが既に開発済であ

る。これらのうち ProVerif 等を用いて個々の暗号技術についての機能や対策できる攻撃などを暗号技術や攻撃者の動作をシミュレーションしながらインタラクティブに学ぶ moodle を用いた CAI 教材を開発する。

(2) 暗号技術の組み合わせによる暗号プロトコルの構成に関する学習教材の開発
実際に利用されている暗号システムは上記(1)の個々の暗号技術を組み合わせて構築された暗号プロトコルによって実現されている。たとえ安全な暗号技術を組み合わせたとしても、利用する乱数の設定ミスや、暗号化鍵など秘密情報の管理の不備によりプロトコル全体としては安全性が破られる場合がある。本課題ではユーザ認証、鍵共有、さらには SSL/TLS 等の実用的な応用プロトコルについて学習する CAI 教材を開発する。さらに暗号プロトコル設計法の教材も開発する。この際、Mizar で安全性要件の自動判定と ProVerif による攻撃シミュレーションを行うことでより学習者の安全性に関する学習効果を増進する。特に暗号プロトコル設計法の学習では、学習者が設計したプロトコルの評価を反転学習の手法により学習効果を高めることが出来るように教材を開発する。

(3) 教育用ユーザインタフェースおよび教材システム開発と評価
分担者等らは Mizar を CAI 教材内で実行させる moodle アドイン]を開発しており、この成果を流用することにより実際に ProVerif と Mizar を動作させながら暗号技術を学習できるような moodle を用いた CAI 教材を作成する。上記(1), (2)の成果をそれぞれ一単元とするコースとして教材を作成し、研究代表者等が担当する情報セキュリティに関連する講義において本教材システムを利用した教育を実践することで、本教材の教育効果を評価し、さらに改善を進める。

４．研究成果

本研究課題を遂行するために、(1)個々の暗号技術とその学習教材の開発、(2)暗号技術の組み合わせによる暗号プロトコルの構成に関する学習教材の開発、(3)上記(1),(2)を統合する教育用ユーザインタフェースおよび教材システム開発と評価、を行った。

2018 年度は、(1)については、暗号プロトコルの安全性自動検証ツールである ProVerif により基本的な暗号機能の形式化を行った。この成果の一部を利用して暗号プロトコルに関する教育を信州大学の学部 3 年生に対して行った成果を第 5 回実践的 IT 教育シンポジウム rePiT2019in 愛媛(ソフトウェア科学会、enPit2 共催)において発表した。本発表により、rePiT2019 の優秀教育実践賞を受賞した。(2)の暗号技術の組み合わせの教材の開発に着手した。(3)については、教育用ユーザインタフェースとしては､e ラーニングシステムとして定評のある Moodle を採用し、プログラミング教育用のプラグインである VirtualProgrammingLab(VPL)を組み込んだシステムを仮想マシン上に構築することで、教育支援システムのプロトタイプを開発した。更に、暗号プロトコルの安全性自動検証ツール ProVerif を開発した教育支援システムで利用可能となるように導入し、(1)で開発した ProVerif による教材を組み込んだ。更に、試作した計算機援用による暗号技術の基礎知識、利用方法を学習する演習授業を実施した。この成果を国内シンポジウム「第 41 回情報理論とその応用シンポジウム(SITA2018)」のポスターセッションおよび国際会議「InternetConference2018(IC2018)」のポスターセッションにて発表した。

2019 年度は、(1)については、形式化を 2018 年度の成果をもとに、暗号学的ハッシュ関数の構成法である MD 変換や、ブロック暗号の利用モードなどのより具体的な暗号技術の形式化を行った。 (2)の暗号技術の組み合わせの教材については、学生自身に一から記述させることは困難であるため、穴埋め問題、デバッグ問題などさまざまな出題方法の比較検討を行なった。(3)については、2018 年度に試作した e ラーニングシステムを本年度に購入した PC に複数の仮想マシンから構成されるサーバを構築し、共同研究者により外部からネットワーク経由でコンテンツの導入や開発ができる環境を整えることができた。更に、2018 年度に rePiT2019 で発表した成果をまとめたものを、日本ソフトウェア科学会「コンピュータソフトウェア」に「形式的安全性検証ツールを用いた暗号教育の実践とその e-Learning 教材化の課題について」として投稿し、掲載された。また、20 台の端末による同時接続を行い、動作することを確認した。さらに、開発した e ラーニングコンテンツを外部のクラウドサービスで提供する試みに着手したところである。本成果の元となった演習は現在も継続中である。今回のコロナ禍において、本システムは有効であると考えられるので、オンライン化の対応を前倒して推し進める準備をした。

2020 年度は、対面での演習を前提とする実証実験を計画していたが、コロナ禍により実施できなくなった。また、発表を予定していた学会が中止になったため、発表することができなかった。

2021 年度は、(1)については、形式化を 2019 年度～2020 年度の成果をもとに、カメレオンハッシュ関数、修正可能なブロックチェーンなどのより具体的な暗号技術の形式化を行った。(2)の暗号技術の組み合わせの教材については、学生の教育効果を考慮して、穴埋め問題、デバッグ問題などさまざまな出題方法を比較、検討中である。(3)については、2018 年度～2019 年度に外

部サービスを用いて構築した e ラーニングシステムを大阪電気通信大学内に設置したサーバに導入し、外部からインターネット経由で本システムを利用できる環境を整えた。この成果は第 8 回実践的 IT 教育シンポジウム rePiT2022(ソフトウェア科学会主催)において発表した。

コロナ禍により、共同研究者間での対面での開発が叶わない、２年間弱対面授業を実施することができない等の理由により、残念ながら当初予定していたところまでの評価を行うことはできなかった。しかしながら、最終年度には、ほぼ当初予定していた通りの内容の学習支援環境を開発することができた。また、コロナ禍前までの対面授業による評価結果により、コンテンツや提案方式が教育上有効であることが評価され、実践的 IT 教育シンポジウム rePiT2019 にて優秀教育実践賞を受賞することができた。今後は、開発したシステムについて、学習効果を評価し、さらにコンテンツを充実させること、使いやすさを改善していくこと、等が課題である。

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　0件／うちオープンアクセス　1件）

１．著者名 Takehiko Mieno, Togo Yoshimura, Hiroyuki Okazaki, Yuichi Futa, Kenichi Arai	４．巻 2020
２．論文標題 Formal Verification of Merkle-Damgard Construction in ProVerif	５．発行年 2020年
３．雑誌名 The International Symposium on Information Theory and Its Applications(ISITA2020)	６．最初と最後の頁 pp.602-606
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.65.E03-2	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 岡崎 裕之，紫村 彰吾，宮本 樹，渡邊 樹，布田 裕一，村上 恭通	４．巻 37(1)
２．論文標題 形式的安全性検証ツールを用いた暗号教育の実践とそのe-Learning教材化の課題について	５．発行年 2020年
３．雑誌名 日本ソフトウェア科学会論文誌コンピュータソフトウェア	６．最初と最後の頁 99-113
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.37.1_99	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 境 隆一，村上 恭通	４．巻 54
２．論文標題 剰余変換の法を秘匿する公開鍵暗号への攻撃	５．発行年 2019年
３．雑誌名 大阪電気通信大学 研 究論集(自然科学編)	６．最初と最後の頁 27-41
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 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 村上 恭通，境 隆一	４．巻 19
２．論文標題 公開鍵暗号の安全性評価に関する研究	５．発行年 2019年
３．雑誌名 大阪電気通信大学 MERI Activity Report 2018	６．最初と最後の頁 145-152
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 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 境 隆一, 村上 恭通	４．巻 19
２．論文標題 多変数公開鍵暗号のグレブナー基底攻撃に対する安全性評価	５．発行年 2019年
３．雑誌名 大阪 電気通信大学 MERI Activity Report 2018	６．最初と最後の頁 153-158
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 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 境 隆一, 村上 恭通	４．巻 19
２．論文標題 公開鍵暗号の安全性評価およびその基礎的技術開発	５．発行年 2019年
３．雑誌名 大阪 電気通信大学 MERI Activity Report 2018	６．最初と最後の頁 162-167
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 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 －

〔学会発表〕　計15件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 杉山 航平, 荒井 研一,岡崎 裕之,布田 裕一,三重野 武彦
２．発表標題 ProVerifを用いたPolicy-based Chameleon Hashによる修正可能なブロックチェーンの形式化
３．学会等名 日本応用数理学会 2021年度 年会
４．発表年 2021年

１．発表者名 田中 健士朗, 布田 裕一, 岡崎 裕之, 鈴木 彦文
２．発表標題 ブロックチェーン技術を用いたDNSキャッシュポイズニング検知方式の評価
３．学会等名 電子情報通信学会 ICSS研究会
４．発表年 2022年

１．発表者名
大町 隆人，岡崎 裕之，布田 裕一，村上 恭通

２．発表標題
情報セキュリティ人材育成のための形式的安全性検証ツール学習用eラーニング環境の構築

３．学会等名
第8回実践的IT教育シンポジ ウムrePiT2022

４．発表年
2022年

１．発表者名
徳山 凌， 布田 裕一 ，鈴木 彦文，岡崎 裕之

２．発表標題
SDNを用いたDDoS攻撃に対する防御機構構築

３．学会等名
2022年暗号と情報セキュリティシンポジウム SCIS2022

４．発表年
2022年

１．発表者名
原田 雄基．布田 裕一 ，岡崎 裕之

２．発表標題
SVM による工場ネットワークにおける偽装通信の検知手法のリアルタイム性の検証

３．学会等名
2022年暗号と情報セキュリティシンポジウム SCIS2022

４．発表年
2022年

１．発表者名
五十嵐 孝洋，布田 裕一

２．発表標題
ブロックチェーンとフォグノードを用いたIoT機器の認証・認可

３．学会等名
ICSS

４．発表年
2020年

１．発表者名
吉村 東悟,荒井 研一,岡崎 裕之,布田 裕一,三重野 武彦

２．発表標題
ProVerifを用いたMD変換の形式化

３．学会等名
日本応用数理学会 2020年度 年会

４．発表年
2020年

１．発表者名
吉村 東悟,荒井 研一,岡崎 裕之,布田 裕一,三重野 武彦

２．発表標題
ProVerifを用いたスポンジ構造の形式化

３．学会等名
2021年暗号と情報セキュリティシンポジウム（SCIS2021）

４．発表年
2020年

１．発表者名
岡崎 裕之，紫村 彰吾，宮本 樹，渡邊 樹，布田 裕一，村上 恭通

２．発表標題
形式的安全性検証ツールを用いた暗号教育の実践とそのe-Learning教材化の課題について

３．学会等名
第5回 実践的IT教育シンポジウム rePiT2019

４．発表年
2019年

１．発表者名
Togo Yoshimura, Kenichi Arai, Hiroyuki Okazaki, Yuichi Futa

２．発表標題
Formalization of Security Requirements and Attack Models for Cryptographic Hash Functions in ProVerif

３．学会等名
The 2019 International Conference on Security and Management (SAM'19)（国際学会）

４．発表年
2019年

１．発表者名
岡崎 裕之，布田 裕一，師玉 康成

２．発表標題
Mizarによる離散確率分布の統計的識別不能性の形式化

３．学会等名
日本応用数理学会 2019年度 年会 予稿集

４．発表年
2019年

１．発表者名
磯貝 百恵，岡崎 裕之，荒井 研一，布田 裕一，三重野 武彦

２．発表標題
モデル検査器ProVerifによるDES暗号の形式化

３．学会等名
2020年電子情報通信学会総合大会

４．発表年
2020年

１．発表者名
渡邊 樹，宮本 樹，紫村彰吾，岡崎裕之，布田裕一，村上 恭通

２．発表標題
Moodle を用いた Proverifの e ラーニングシステム

３．学会等名
第41回 情報理論とその応用シンポジウム（SITA2018）

４．発表年
2018年

１．発表者名
紫村 彰吾，岡崎 裕之，宮本 樹，渡邊 樹，布田 裕一，村上 恭通

２．発表標題
形式的安全性検証ツールを用いた暗号教育の実践とその e-Learning 教材化の課題について

３．学会等名
第5回 実践的IT教育シンポジウム（rePiT2019）

４．発表年
2019年

１．発表者名 Tatsuki Miyamoto, Shogo Shimura, Tatsuki Watanabe, Hiroyuki Okazaki, Yuichi Futa, Yasuyuki Murakami
２．発表標題 e-Learning System for Cryptography on Moodle
３．学会等名 Internet Conference 2018 (IC2018)（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
研究分担者	岡崎　裕之 (Okazaki Hiroyuki) (50432167)	信州大学・学術研究院工学系・准教授 (13601)	
研究分担者	布田　裕一 (Futa Yuichi) (50706223)	東京工科大学・コンピュータサイエンス学部・教授 (32692)	

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