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　２ 年　 ６ 月 １１ 日現在

機関番号：１４４０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１９２

研究課題名（和文）高セキュリティを考慮したITS向けセキュア認証プロトコルに関する研究

研究課題名（英文）Study of a high secure authentication protocol for the intelligent transportation system

研究代表者
猪俣　敦夫（Inomata, Atsuo）

大阪大学・情報セキュリティ本部・教授

研究者番号：９０５０５８６９

交付決定額（研究期間全体）：（直接経費）　　2,500,000円

研究成果の概要（和文）：ITSは、車両、道路、路側の建造物、および交通利用者をネットワーク接続することにより新たな付加価値提供を行うシステムである。今や自動運転の技術が進化し、自動車そのものが移動手段のみならず情報を提供するパブリッシャーでもあり、今後無人運転での販売サービスや移動手段の代替になる時もそう遠くはない。しかしながら、安全性を最優先にしなければならない自動車においては、その制御と情報との間のリアルタイムな応答性は極めて重要であり、かつセキュリティは重要な課題である。本研究では、自動車のような制約された環境において可能な限りで秘匿性が高く、応答性に優れた認証技術の確立が最大目標である。

研究成果の学術的意義や社会的意義
安全性を最優先にしなければならない自動車の世界においては、制御と情報との間のリアルタイムな応答性は極めて重要であり、かつセキュリティは重要な課題である。今や自動車は外部と通信を行うことが一般的になりつつあるが、自動車は非常に膨大な数の制御デバイス等が連携して動作しており、より高速な認証が必要である。特に安全性を最優先にしなければならないデバイスやモジュール間通信においてセキュリティを意識することは最重要かつ喫緊の課題である。そこで本研究においては、自動車等の計算能力や動作環境が非常に制約された中において、応答性を確保しつつ軽量化された安全な認証処理を実現するための要素技術の確立を目指した。

研究成果の概要（英文）：ITS is a system enables to provide added values to vehicle users (driver, passenger and pedestrian). The values include an enhancing road safe, optimizing traffic management (clearing traffic jam, save and secure path of emergency car) by connecting vehicle, road, roadside and its construction and all users on untrusted network. In this world, the vehicles are also the publisher that provide some of many service to users in order to realize safe communication. In this research, i focus on this security mechanism that enable to establish more safe authentication mechanism and more real time response on vehicle control.

研究分野：情報セキュリティ

キーワード：ITS　ペアリング　暗号　モバイルセキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

ITS(Intelligent Transportation System)は、車両、道路、路側の建造物、および交通利用者をネットワーク接続することにより、交通安全の向上、交通管理の最適化（渋滞解消、緊急車両の経路確保等）、利用者（運転者、同乗者、および歩行者）への付加価値提供を行うシステムであり、国際標準化機構(ISO)、欧州電気通信標準化機構(ETSI)、および各国の研究機関が産学が連携してITS通信基盤（ITSコミュニケーションアーキテクチャ）の標準化を推進し、ISO/OSI参照モデルを基盤とする4つの先進的機構：

(1)複数の通信デバイスの同時制御

(2)車々間アドホックネットワーク(VANET)

(3)ネットワークモビリティ(NEMO)を用いた車両の移動に依存しない永続的なインターネット接続の提供

(4)地理位置を基準とした通信機構

を具備し「サービス」と呼ばれる基本機能の連携によって実現される。このようにITS技術の進化に伴い、世界的にも自動運転時代の入り口に入りつつある中、2020年国内でも自動車が創り出すモバイルシティの実現に向けた取り組みが進められ始めた。この世界では、自動車そのものが移動手段のみならず情報を提供するパブリッシャーでもあり、今後無人運転での販売サービスや移動手段の代替になる時もそう遠くはないことが感じ取られる。しかしながら、安全性を最優先にしなければならない自動車においては、その制御と情報との間のリアルタイムな応答性は極めて重要であり、かつセキュリティは重要な課題である。例えばICカードにおいては約50msec程度の許容で認証の運用がなされており自動車においてもそれ以上の応答性が求められている。しかし、自動車は膨大な数の制御装置が連携して動作しており、さらにより高速な認証速度が必要であり、特に安全性を最優先にしたセキュリティを意識することは今や最重要かつ喫緊の課題である。

２．研究の目的

現在のほとんどの自動車に搭載されている OBD2 インタフェースは、自動車のメンテナンス用として利用されてきた経緯があるが、最近では容易に接続するためのデバイスが多数登場しており、ユーザーも容易に利用することが可能となった。しかしながら、自動車メーカーはこのインタフェースをユーザのために提供していないことから、不正な目的で利用するためのデバイスが多数存在し、しかも非常に安価に売られているという問題がある。このため自動車を構成する全てのデバイスにおいては安全性を保証することが第一であり、その通信の秘匿性を保証すること、そして制御に負荷をかけることなく高速に処理させることが重要な課題であり、本研究課題を目的として設定した。

３．研究の方法

自動車などの計算能力や動作環境の制約された中で、高速に暗号処理を実現するための機能を検討する。その手段として、楕円曲線上の数の集合で定義される体から構成されるペアリング演算に着目し、一般的に計算処理負荷が大きくなるとされるモジュール部分を車載むけに軽量化したアルゴリズムを確立する。さらにその有効性を評価するために実機実装し、実証実験を行う。結果として、セキュリティ・プライバシ保護を目的とした内容として成果をまとめ、国内研究会および国際会議に論文投稿を目指す。

４．研究成果

平成 29 年度は、主に楕円曲線上のペアリング演算を自動車むけに最適化を行い、主に実機を想定した実装を行った。OBD2 に接続可能なデバイスの調査も合わせて行い、実際に入手して実験を実施し評価を得た。ただし、実験を実施するにあたり、自動車を利用する点、また違法な無線電波が出力されていないかを確認することが重要であり、その点は法的側面についても検討を行いながら進めた。実機実装においては、計算処理負荷が大きくなるとされるモジュール部分を車載向けに軽量化したコードを実装した。結果として、セキュリティ・プライバ シ保護を目的とした内容として成果をまとめ、国内研究会および国際会議に論文投稿し、採択された。平成 30 年度は、計算量の軽減を目指した実装を継続的に行い、nvdia 製の GeForce(GPU グラフィックボード)上で評価検証を行った結果、動作までは確認が出来た。一方、動作が安定せずその原因追求も並行して行っているが、命令セットの問題と考えており、他の GPU グラフィックボードでも検証するなど問題点の洗い出しを行った。最終年度となる平成 31（令和元）年度は、自動車のような安全性が最優先されるような電源環境を含めて厳しい動作環境等の制約条件の中で、高速に認証処理(暗号計算)を実現を目指した。その具体的な手段として、計算処理負荷が大きくなるモジュール群を車載向けに軽量化した専用のアルゴリズムを確立し、その有効性を評価を進めた。さらに、攻撃モデルを想定し、車載計算機と情報端末とのやり取りで扱われるデータに対するいくつかの攻撃を仮定し、それを防御しつつ安定かつ高速に認証できるのかという観点にて評価を実施した研究成果を取りまとめ、 国際会議に論文投稿した。

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Takaaki Sugiu、Atsuo Inomata	４．巻 978-1-4503-6178-1
２．論文標題 Dark Web Content Analysis and Visualization	５．発行年 2019年
３．雑誌名 ACM international workshop on security and privacy analytics	６．最初と最後の頁 53,59
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3309182.3309189	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 Yuki Nakazawa, Ryoichi Sasaki, Atsuo Inomata	４．巻 ISSN:2305-001
２．論文標題 Survey and analysis of regional characteristics of unmanaged stray IoT devices	５．発行年 2018年
３．雑誌名 International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(3), The Society of Digital Information and Wireless Communications (SDIWC)	６．最初と最後の頁 200, 208
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4件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 Ryota Kawakami, Atsuo Inomata, Naoto Yanai, Toru Fujiwara
２．発表標題 Wireless Access Point Spoofing by Unmanned Aerial Vehicles (UAVs)
３．学会等名 The Network and Distributed System Security Symposium (NDSS) 2020（国際学会）
４．発表年 2020年

１．発表者名 Jiaxing Zhou, Yoshio Kakizaki, Miyuki Hirose, Atsuo Inomata
２．発表標題 Evaluation to Classify Ransomware Variants based on Correlations between API
３．学会等名 6th International Conference on Information Systems Security and Privacy (ICISSP2020)（国際学会）
４．発表年 2020年

１．発表者名 Yuki Fujita, Atsuo Inomata, Hiroki Kashiwazaki
２．発表標題 Implementation and Evaluation of a Multi-Factor Web Authentication System with Individual Number Card and WebUSB
３．学会等名 20th Asia-Pacific Network Operations and Management Symposium (APNOMS2019)（国際学会）
４．発表年 2019年

１．発表者名 Tomoya Kitagawa, Ismail Arai, Masatoshi Kakiuchi, Atsuo Inomata, Kazutoshi Fujikawa
２．発表標題 Fingerprinting of ECUs using difference of delay time on Controller Area Networks
３．学会等名 ISCIS CyberSecurity Workshop (ISCIS2018)
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