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 １５ 日現在

機関番号：１４４０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ１１８０９

研究課題名（和文）頑健なITS向けセキュア認証フレームワークに関する研究

研究課題名（英文）Research of a robust secure authentication framework for ITS

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）　　3,200,000円

研究成果の概要（和文）：本研究は、自動車における認証処理を行う車載CPUをITS向け専用の計算リソース環境を実現するために、次の3つの課題を設定した。認証処理を行う車載CPUとメモリが搭載された計算リソースを安定的に動作させる電力及び排熱・車載スペース等、車載により制約された条件において高速な認証プロトコルの確立、2. 車載CPUおよびデバイス間のI/Oバスを安定的に動作させるため、動作状況に応じてDC/DCコンバータを制御させることで直流電源の安定性を向上させる電源管理機構の確立、3.自動車専用ECUと、速度計や回転数計等の情報サービスを提供するデバイス間との通信秘匿性および安定性についての電気的特性の検証

研究成果の学術的意義や社会的意義
ITSにおける全プロトコルレイヤの情報を集約するレイヤ独立なシステムマネジメント機構と協調するセキュリティ要件の洗い出しを行なってきた結果、ITSアプリケーションにおけるセキュリティ機能・性能要件をSOAの視点から分析しなおすことが重要であり、本研究提案では、自動車に特化したシステム動作を司るマネジメント機構（電源管理など）およびメッセージング・セキュリティプロトコル（認証処理）を連携した機構の確立が重要であると判断して研究を進めた。特に、自動運転自動車そのもののアーキテクチャに関する研究は多いものの、内部処理における認証に着目した研究はあまり存在せず今後に重要な示唆を与えるものと思われる。

研究成果の概要（英文）：This research is in order to realize a computing resource environment dedicated to ITS for the onboard CPU that performs authentication processing in future vehicles following three themes. 1. Establishment of a high-speed authentication protocol under the restricted conditions imposed by the in-vehicle environment, such as power, heat dissipation, and on-board space, to ensure stable operation of the onboard CPU that performs authentication and the computing resources with its memory. 2. Establishment of a power management mechanism that improves the stability of the DC power supply by controlling the DC/DC converter according to the operating conditions in order to ensure stable operation of the I/O bus between the onboard CPU and devices in vehicles. 3. Verification of electrical characteristics regarding the confidentiality and stability of communication between the automotive-specific ECU and devices that provide information services such as speedometers and tachometers.

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　自動車　自動車セキュリティ　自動運転自動車

様　式　Ｃ－１９、Ｆ－１９－１（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し、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高度交通システムであり、特に国際標準化機構(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）の標準化が進められてきた。自動車においては、ISO/OSI 参照モデルを基盤とした 4 つの先進機構：(1)複数の通信デバイス同時制御、(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)を用いた車両移動に依存しない永続的なインターネット接続、(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が提供され、これらの機能が実現される。一方、ITS においては個々人のアクションや位置情報、自動車個体そのものを特定しうる ID 等プライバシ情報がやり取りされることが一般的であり、そのような機微性の高い情報を秘匿する技術は未だ不十分の段階にある。そのため ITS 向けセキュリティフレームワークの確立は喫緊の課題である。

自動車の安全上の観点から、車載 CPU は自動車制御以外に用いることができないよう ITS システムとはほぼ独立に構成されるような設計になっているが、上述したように今後の ITS 向けに適した頑健な認証プロトコルを確立するには、セキュリティ専用の計算リソースとメモリが確実に必須となる。さらに、機密性・可用性の面から見ても一般的な IT システムのような 2,3 年のライフタイムではなく、自動車そのものは SDGs の観点からも少なくみても 10 年以上は問題なく動作する必要もあることから、産業・制御システムまでとは言わずとも IT システムよりは比較して長い年数を耐えうる必要がある。すでに、産業・制御システムセキュリティ基準である IEC62443 が世界標準規格となり、OT 分野においては当該規格に準拠した電源装置が一般的に市場に投入されている。このような背景から、本研究提案者は、長年 ITS 世界における全プロトコルレイヤの情報を集約するレイヤ独立なシステムマネジメント機構と協調するセキュリティ要件の洗い出しを行なってきた結果、ITS アプリケーションにおけるセキュリティ機能・性能要件をサービス指向アーキテクチャ(SOA)の視点から分析しなおすことが重要であることがわかり、特に、自動車に特化したシステム動作を司るマネジメント機構（電源管理など）およびメッセージング・セキュリティプロトコル（認証処理）を連携した機構の確立が重要であると判断し、本研究提案の着想に至った。

２．研究の目的

本研究の目的は、ITS システムが確立されたことを前提にした社会インフラに対して適切なセキュリティ機能の洗い出しを行うとともに、定性的のみならず定量的な評価結果を得ることから、実機を用いた実証実験を行うことでその可能性を示すことにある。世界中すべての国々がコロナ禍を経て大きな社会変容が起きたことは記憶に新しい、例えば交通インフラにおいてはタクシーやバスなどの自動運転車両が社会インフラとしてより現実化し、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して交通安全の向上や交通管理の最適化などの検討が急速に進み、都市部のみならず限界集落などでの実証が開始された。このように自動運転技術に関する研究開発は進む一方、個々人や位置情報、自動車個体そのものを特定しうる ID 等のプライバ

シ情報に関する検討はあまり進んでおらず、ITS 世界では比較してプライバシなど機微性の高い情報を秘匿する必要があると思われているが、技術面においては未だ不十分な段階にある。そこで研究提案者は、これまで楕円曲線上の点の集合をベースとした演算としてペアリング暗号として知られる小標数の有限体を定義体に持つ超特異曲線上のηT ペアリングをベースとした ITS 向けに最適化した認証プロトコルを設計してきた。特に、自動車の安全性を最優先とするために認証処理を行う車載 CPU を ITS 向け専用の計算リソースとして提供する必要があることを明らかにする必要があると考え、以下の課題を設定した。

1．認証処理を行う車載 CPU とメモリが搭載された計算リソースを安定的に動作させる電力及び排熱・車載スペース等、車載により制約された条件において高速な認証プロトコルの確立

2．車載 CPU およびデバイス間の I/O バスを安定的に動作させるため、動作状況に応じて DC/DC コンバータを制御させることで直流電源の安定性を向上させる電源管理機構の確立

3.自動車専用 ECU と、速度計や回転数計等の情報サービスを提供するデバイス間との通信秘匿性(中間者攻撃対策等)および安定性(リアルタイム応答性)についての電気的特性の検証

３．研究の方法

本研究は、ITS 世界における認証の仕組みを確立することを想定しておりその主たる環境として自動車を想定するが、自動車のように計算機を動作させる環境が厳しく制約されている状況で、高速に暗号処理を実現するための機能を検討する手段として、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向けに軽量化したアルゴリズムを確立し、実機環境への実装・評価を行うといった流れをとることとした。

1．ITS 認証プロトコル最適化・実装評価

大きな自己同型群を持つ等の優位性から超楕円曲線をもとに進めていくが、まず 192bit, 256bit 安全なペアリングを考慮した曲線選択を行った上で Tate および Weil ペアリングベースで構成するが、その分解問題として優れた数体ふるい法(NFS)に対して優位とされている TNFS をベースとした最適化および実装の改良を行う。

2．電源管理機構設計・実装評価

車載電源は蓄電池であり定格電圧は直流 13.8V（大型車は 24V）である。これは、内燃機関や燃調制御のための車載 ECU および電装系装置を適切に動作させるのに消費される一方、エンジン動作により回生されることで充電され安定的な電源が供給される仕組みがとられている。今回、認証処理においては一時的な計算負荷により大きな電流が流れる可能性もあることから安定化 DC/DC コンバータによる電源制御を実現させることとする。

3．情報サービスデバイスへの電気的特性監視と評価

ITS デバイスから通信が行われる際に認証処理が時にバースト的に発生することも考えられるため、CAN バス間を流れる信号の電圧を動作タイミングとともに観測し、制御遅延や影響等を検証する。

４．研究成果

平成 2 年度は、楕円曲線上のペアリング演算を自動車向け最適化を行い、主に車載する計算機を想定した実装を行った。計算機としては 2 種類用意し、通常の Intel Core i3 搭載のものと Raspberry Pi3B を利用して検証行った。また、UART から自動車側 OBD2 インタフェースに接続可能なデバイスの調査も行い、接続実験を行った。ただし、実証実験を実施するにあたり、一般道路走行可能な自動車を利用する点、また法律で許可されていない無線電波が出力されていな

いかを法的側面についても慎重に調査しながら進めた。令和 3 年度は、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。さらに処理過程におけるニューラルネットワークへの展開など、セキュリティ・プライバシ保護の応用技術として成果をまとめ、研究会および国際会議への論文投稿を行った。令和４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、動作までは確認出来たが、車載上で動作が安定せずその原因追求も並行して実施した。確固たる原因の特定が出来なかったが、おそらく使用した命令セットの負荷により想定以上の電力消費が必要となり、車載上の DC-DC インバータではリソース不足ではないかと考え、当初から想定していた DC-DC コンバータを用いた安定化回路を設計し、実装を行った。さらに、より詳細な原因特定のために他の GPU グラフィックボードを借用し、検証するなど問題点の洗い出しを行った。最終年度となる令和5 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で高速に認証処理の実現を目指した。その手段として、計算処理負荷が大きくなるモジュール群を車載向けにアルゴリズムを軽量化し、評価を得た。実際に脅威シナリオとして、DDoS 攻撃のような CAN 内にバースト的にトラヒックを発生するなどして車載計算機と情報端末とのやり取りがどのようになるかをオシロスコープからも電気的特性から観測を行った。結果としてプロトコルスタックでの ICMP を無視させる処理を施したところ、ほぼ問題がないことが示された。さらに車載器からクラウドへ接続を行い、認証処理を外部に委譲させる手段についても検討を進め、結果これらの成果を取りまとめ、オープンアクセスの論文誌に投稿した。結論からいうと、自動車の直流電源をインバータで交流化すると電圧変動が激しいことから認証処理のための環境には特に電源環境が重要であり、動作環境および設置条件について詳細に洗い出す必要がある。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　0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 Teerakanok Songpon、Uehara Tetsutaro、Inomata Atsuo	４．巻 2021
２．論文標題 Migrating to Zero Trust Architecture: Reviews and Challenges	５．発行年 2021年
３．雑誌名 Security and Communication Networks	６．最初と最後の頁 1～10
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2021/9947347	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 －

１．著者名 Teerakanok Songpon、Uehara Tetsutaro、Inomata Atsuo	４．巻 2021
２．論文標題 Migrating to Zero Trust Architecture: Reviews and Challenges	５．発行年 2021年
３．雑誌名 Security and Communication Networks	６．最初と最後の頁 1～10
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2021/9947347	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 －

１．著者名 Yamakawa Daiki、Okimoto Takashi、Teerakanok Songpon、Inomata Atsuo、Uehara Tetsutaro	４．巻 2021
２．論文標題 Enhancing Digital Certificate Usability in Long Lifespan IoT Devices by Utilizing Private CA	５．発行年 2021年
３．雑誌名 Security and Communication Networks	６．最初と最後の頁 1～14
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2021/6610863	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3件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 Kazuki Nomoto, Mitsuaki Akiyama, Masashi Eto, Atsuo Inomata, Tatsuya Mori
２．発表標題 Can the Exposure Notification Framework Expose Personal Information
３．学会等名 Proc. of The Network and Distributed System Security Symposium (NDSS) 2021（国際学会）
４．発表年 2021年

１．発表者名 Hoang Nguyen, Songpon Teerakanok, Atsuo Inomata, Tetsutaro Uehara
２．発表標題 The Proposal of Double Agent Architecture using Actor-critic Algorithm for Penetration Testing
３．学会等名 Proceedings of the 7th International Conference on Information Systems Security and Privacy（国際学会）
４．発表年 2021年

１．発表者名 Hai Nguyen, Songpon Teerakanok, Atsuo Inomata, Tetsutaro Uehara
２．発表標題 The Comparison of Word Embedding Techniques in RNNs for Vulnerability Detection
３．学会等名 Proceedings of the 7th International Conference on Information Systems Security and Privacy（国際学会）
４．発表年 2021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