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

平成　２９　年　　８　月　１９　日現在

機関番号：　３２６５７
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１５６

研究課題名（和文）軽量なITSアプリケーション向けセキュリティ機構に関する研究

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）

東京電機大学・未来科学部・教授

研究者番号：９０５０５８６９

交付決定額（研究期間全体）：（直接経費）　　2,300,000円

研究成果の概要（和文）：本研究では、ITS上でより強度な安全性を提供するための暗号ミドルウェアの確立を目指し田母野である。具体的には、自動車のような計算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注目し、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する。さらにその有効性を評価するに実機に実装し評価をし、今後の自動車システム全般に対してセキュリティ・プライバシ保護の１要素として導入されることを目指した研究である。

研究成果の概要（英文）：In this study, I focused on ITS (Intelligent Transporting System) and then established a cryptography middleware in order to provide more powerful and safe authentication mechanism on ITS. First, I studied some kind of functions that are realized the cryptography computation faster in the constrained environment such car system. So I applied the pairing computation based on the number theory on elliptic curve into this ITS authentication mechanism and then optimized its computation flow. Furthermore, I implemented and executed an experimentation in order to evaluate the effectiveness of this proposed model. Finally, I summarized this research and then submitted this result to an international conference and a journal paper.

研究分野：　情報セキュリティ

キーワード：　ITS　楕円曲線　ペアリング演算

１．研究開始当初の背景

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、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。近年、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。しかしながら、このモデルは安全性についての言及が未だ不十分である。

また、2016年度は世界的なUBERの普及に合わせて、自動運転元年と言われるぐらいに国内でも非常に注目される年となった。自動運転は、いずれもドライバーに運転責任がある「レベル２」にとどまり、ドライバーは自動運転時にも安全運転に配慮する義務を負う。また「レベル３」ではアクセル、ブレーキ、ハンドルの全ての操作が自動で行われ、事故時の運転責任は原則としてシステム側が負うことになる。基本的にはドライバーが運転操作に関わる必要はなくなるが、システム異常など緊急時に操作する義務が生じるため、ドライバーの責任がなくなるわけではない。自動運転の例をとって見ても、自動車そのものが発信する情報の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と言える。

２．研究の目的

本研究では、高度道路交通システム(ITS)に対するセキュリティ機能要件の洗い出しを行い、より安全性の高い、かつ効率の良い新しいITS向けセキュリティプロトコルの確立を目指している。前研究においては、フランス国立情報学自動制御研究所(**INRIA**)と進めてきたITSコミュニケーションアーキテクチャ上で動作する通信メカニズムに適したセキュリティ機構として、本研究においても以下に示す2要件を設定した。

1. 車両、歩行者、観測者が混在する環境におけるプライバシ保護

通信性能への影響を抑制させた形で、通常の通信にダミー通信を加えた形でPseudonym IDをベースとした匿名手法を提案、実装し、シミュレーションによる評価を実施した。しかし、車両の移動に関わる情報等を考慮した場合、処理において比較的高性能な計算能力が必須となり、現状の認証手段をそのまま適用するだけでは（車載を想定した）計算機に大きな負荷を与える可能性があることが判明した。

2. **軽量なITS向けセキュア認証プロトコル**の確立

楕円曲線上の数体をベースとしたペアリング暗号の実装経験が豊富であり、FPGA上で最速の実装を成功させた成果を有している。ここでペアリングとは、楕円曲線上の点の集合、或いは超楕円曲線のJacobian上の群構造を保つ双線形写像である。前研究においては、最も高速なペアリングとして知られてい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、GPU プロセッサ上で動作可能な**高速なITS向けセキュリティプロトコル**の設計と実装を行い、評価を得た。

３．研究の方法

はじめに、ITS独自とも言えるレイヤ独立なシステムマネジメント機構の上で、それと

協調するサービスディスカバリにおけるセキュリティ機能要件の整理を行う。特に、ITSにおいてセキュリティ機能に渡される情報には、アクセス技術、ネットワークおよびトランスポート、各ファシリティ、アプリケーション、全てのレイヤからの情報が含まれる。このように複数レイヤから渡されるデータの暗号化・認証処理を独立して効率よく実行する必要がある。しかしながら、車載計算機の動作条件の制約等から、可能な限りやり取りされる鍵長サイズおよび署名長、暗号処理計算、等の処理負荷の軽減が求められる。そこで、主として有限体上の多倍長モジュラ算術等のGPUを用いた並列計算に取り組み、CUDAライブラリとして実装を行う。近年、GPUプロセッサの開発環境である**CUDA**の整備が進み、かつ安価なGPUプロセッサも多数登場している。本研究提案のターゲットであるITSアプリケーションにおいては、処理効率の面からメインプロセッサ上で処理をさせず、GPUプロセッサ上で処理させることで効率化を図るという方針で研究を進めてきた。

４．研究成果

平成２６年度は、多項式計算部分の並列化を目指し、実装を進めた。特に GPU プロセッサ上で稼働させるために通常の多倍長演算の API を利用するのではなく、GPU に特化した処理が行えるような基礎演算モジュールの設計を進め、CUDA ライブラリ上に実装を行なった。

平成２７年度は、ITS が搭載されうる実機を想定した安全性を考慮し、192bit 安全をベースとした曲線選択を行った。実際には、Kawazoe-Takahashi 曲線をベースとした Twisted Ate Pairing の高速アルゴリズムを実現し、その成果を国際会議論文としてまとめ、投稿を行った。

最終年度となる平成２８年度は、ITS システム搭載可能な実機を想定した環境に適用するための設計、実装を行った。最終的に研究全体を考察し直し、国際会議およびジャーナル論文誌への投稿を行い、採録された。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　2　件）

1. Masahiro Ishii, Atsuo Inomata, Kazutoshi Fujikawa, "A Weil Pairing on a Family of Genus 2 Hyperelliptic Curves with Efficiently Computable Automorphisms", IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences Special Section on Cryptography and Information Security, Vol.E100-A, No.1, pp.62--72, 2017.

2. Naohiro Washio, Satoshi Matsuura, Masatoshi Kakiuchi, Atsuo Inomata, Kazutoshi Fujikawa. "A Vehicle Clustering Algorithm for Information Propagation by Inter-Vehicle Communications", Proc. of 12th IEEE Workshop on Managing Ubiquitous Communications and Services part of PerCom 2015, No.18, Multicon Lecture Notes,pp.35--40, multicon verlag Schoneiche bei Berlin, 2015.

〔学会発表〕（計　6　件）

1.Ryota Jinnai, Atsuo Inomata, Ismail Arai, Kazutoshi Fujikawa, "Proposal of Hardware Device Model for IoT Endpoint Security and Its Implementation", 15th IEEE International Conference on Pervasive Computing and Communications (PerCom2017), No.DEMO-D14, 2017.

2.古川智也，猪俣敦夫，新井イスマイル，藤川和利, "通信データの特徴を用いた Ring-LWE 問題に基づく鍵交換プロトコルの通信削減方法の検討", コンピュータセキュリティシンポジウム（CSS）2016 論文集, 2016.

3.石井将大, 猪俣敦夫, 藤川和利, "種数 2 の Kawazoe-Takahashi 曲線族上の optimal ペアリングの構成とそのコスト評価", コンピュータセキュリティシンポジウム (CSS) 2015 論文集, pp.258--265, 2015.

4.辻井高浩, 猪俣敦夫, 垣内正年, 油谷曉, 藤川 和利, "非常時における車載型衛星インターネット通信システムの実装と評価", 情報処理学会インターネットと運用技術研究会

予稿
集,Vol.2015-03-IA-IPSJ-IOT-SITE,No.IOT-9,
2015.
5.鷲尾直大, 松浦知史, 垣内正年, 猪俣敦夫,
藤川和利, "車車間通信を用いた情報伝播のた
めの車両クラスタリング手法", 電子情報通
信学会インターネットアーキテクチャ研究
会予稿集,Vol.2014-IA,No.12-7, 2014.
6.Mehnaz Seraj, Atsuo Inomata, Kazutoshi
Fujikawa, "A context aware routing metric for
reliable route discovery in MANET using fuzzy
logic", 電子情報通信学会 ITS 研究会予集,
Vol.2014-12-WBS-ITS,No.ITS-23, 2014.

〔図書〕（計　1　件）
1．猪俣敦夫，共立出版，サイバーセキュリティ入門，2016．

〔産業財産権〕

○出願状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
猪俣　敦夫（INOMATA, Atsuo）
東京電機大学・未来科学部・教授
研究者番号：90505869