様　式　Ｆ－７－１

科学研究費助成事業（学術研究助成基金助成金）実施状況報告書（研究実施状況報告書）（平成２７年度）

1．機関番号　1 4 6 0 3

2．研究機関名　奈良先端科学技術大学院大学

3．研究種目名　基盤研究(C)（一般）

4．補助事業期間　平成２６年度～平成２８年度

5．課題番号　2 6 3 3 0 1 5 6

6．研究課題名　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

7．研究代表者

研究者番号	研究代表者名	所属部局名	職名
9 0 5 0 5 8 6 9	イノマタ　アツオ 猪俣　敦夫	総合情報基盤センター	准教授

8．研究分担者

研究者番号	研究分担者名	所属研究機関名・部局名	職名

9．研究実績の概要

2015年に入り自動車の自動運転システムが現実化しつつあるように、自動車そのものがITデバイスとして情報を受け取るだけではなく発信もするような計算機の1つになりつつある。自動車の走行軌跡などはカーナビなどでは一般的になりつつあるが、そのような走行軌跡をオンラインで活用することは、各ユーザーのプライバシーなどの問題からまだ一般的に普及するような段階には至っていない。しかしながら、自動車そのものが位置情報などを自律的に発信できるようになれば、渋滞や事故などから回避できる可能性が高くなると考えられる。そのようなシステムの確立を目指したものがITS(Intelligent Transporting System)である。本研究ではそのITSに対して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提供を狙っており、特に自動車のような計算機環境が制約された中で高速に暗号処理を実現するための機能の確立を目指している。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向けに軽量化したアルゴリズムを確立し、実システムに実装することで評価を狙ったものである。本年度は、特に実機を想定した安全性として192bit安全をベースとした曲線選択を行い、Twisted Ate Pairingの高速アルゴリズムを実現することに成功した。その成果は、国際会議に論文として投稿し、採択がなされている。

（注）・印刷に当たっては、Ａ４判（縦長）・両面印刷すること。

10.キーワード

(1) ITS	(2) 楕円曲線	(3) ペアリング暗号	(4) 曲線選択
(5)	(6)	(7)	(8)

11.現在までの進捗状況

(区分)(2)おおむね順調に進展している。

(理由)

平成27年度は、特に実機を想定した安全性として192bit安全をベースとした曲線選択を行った。具体的には、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することに成功した。その成果は、国際会議に論文として投稿し、採択がなされている。なお、安全性証明については今年度においては示すことができなかったため、社会実装の観点から安全性証明は重要な要素になるため、これについては早急に実施する予定である。

12.今後の研究の推進方策　等

(今後の推進方策)

最終年度は、提案手法の有効性の確認が主である。確立したアルゴリズムの検証としてフランスでの実証実験を目指す。特に、フランスでの軽量な実行環境とされる有名なアーキテクチャ(Kalray MPPA-256)上での評価を行い、最終的に本研究の成果の取りまとめを行う予定である。

(次年度使用額が生じた理由と使用計画)

(理由)

(使用計画)

(課題番号： 26330156)

(注)・印刷に当たっては、Ａ４判（縦長）・両面印刷すること。

13.研究発表（平成27年度の研究成果）

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

著者名	論文標題

雑誌名	査読の有無	巻	発行年	最初と最後の頁	国際共著

掲載論文のDOI（デジタルオブジェクト識別子）

オープンアクセス

〔学会発表〕 計（1）件／うち招待講演 計（0）件／うち国際学会 計（1）件

発表者名	発表標題
Masahiro Ishii, Atsuo Inomata, Kazutoshi Fujikawa	A Construction of a Twisted Ate Pairing on a Family of Kawazoe-Takahashi Curves at 192-bit Security Level and Its Cost Estimate

学会等名	発表年月日	発表場所
2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)（国際学会）	2016年02月19日～2016年02月22日	Barcelo Aran Mantegnaホテル、ローマ市、イタリア

〔図書〕 計（1）件

著者名	出版社
猪俣敦夫	共立出版

書名	発行年	総ページ数
サイバーセキュリティ入門	2016	231

14.研究成果による産業財産権の出願・取得状況

〔出願〕 計（0）件

産業財産権の名称	発明者	権利者	産業財産権の種類、番号	出願年月日	国内・外国の別

〔取得〕 計(0)件

産業財産権の名称	発明者	権利者	産業財産権の種類、番号	取得年月日 出願年月日	国内･外国の別

15.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

国際研究集会名	開催年月日	開催場所

16.本研究に関連して実施した国際共同研究の実施状況

(1)国際共同研究: ー

17.備考
