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２６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)　　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 |
|---|---|---|---|
| 90505869 | イノマタ　アツオ<br>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

近年、自動車の高度IT化が進むとともに自動車そのものが計算機リソースを持ち、情報を収集するだけでなく自ら情報を発信するデバイスそのものにもなっている。本研究では、この高度道路交通システム(Intelligent Transportation System:ITS)に注目し、安全性の高いITSアプリケーション向けセキュリティプロトコルの実現を目指すことが最終目標である。特に、自動車から発信される情報として、自動車の位置情報や車内CANでの通信情報等、それ自体において機微的な取り扱いも含まれるようなプライバシー情報も保護することが狙いである。特に、本研究では、通信のやり取りを行う暗号化アルゴリズムとして署名長の短くかつ安全性が高いとされるアルゴリズムを実装し、実機を用いて実証する手段をとる。具体的には、楕円曲線上の体で定義されるペアリング演算に着目し、通常m計算処理負荷が高くなるとされるモジュールを、車載されることを想定したGPUプロセッサが提供する命令セットにカスタマイズし、暗号処理における整数演算処理等の最適化を目指す。最終的には、本学が保有する自動車に搭載し、実車を用いて処理の負荷について検討を行う予定である。

10.キーワード

| | | | |
|---|---|---|---|
| (1) ITS | (2) 多項式計算 | (3) 楕円曲線 | (4) ペアリング暗号 |
| (5) GPGPU | (6) | (7) | (8) |

11.現在までの達成度

(区分)(2)おおむね順調に進展している。

(理由)

平成26年度では、多項式計算部分の並列化を目指し、実装を進めた。特に、GPUプロセッサ上で稼動させるために、通常の多倍長演算のAPIの利用ではなく、GPUに特化した算術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った。今回得られた結果がある程度、可能性を示すデータであったため国際会議へ投稿したところ採録されたことから、ある程度この方針で問題がないと考えている。

12.今後の研究の推進方策　等

(今後の推進方策)

今回、一般的なGPUプロセッサに搭載されている命令セットのみで実装をすすめたが、処理性能の限界もある程度見えてきたという問題も得られた。このため、最新のGPUプロセッサで提供されているComput Capability 2.0の命令セットで設計をしなおし、特にワード長変更での処理の最適化および高速化を狙うこととする。これをくみ上げた後、車載用ボックスを設計、実装する予定である。

(次年度使用額が生じた理由と使用計画)

(理由)

当初、初年度に購入予定であったGPUプロセッサに最新の命令セットが搭載されたデバイスが販売されなかったため、購入を見合わせた。および研究成果を実装したプロトタイプをフランスでの実証実験に向けた調整を進めていたが、無線周波数等の問題が発生し、プロトタイプデバイスそのものの見直しが必要になったため。

(使用計画)

今年度に発売される最新のGPUプロセッサの購入に充当する予定である。さらに、実証した成果を論文に整理し、国際会議への投稿を目指す。

13.研究発表（平成26年度の研究成果）

〔雑誌論文〕 計( 0 )件　うち査読付論文 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 |
|---|---|---|---|---|
| | | | | |

| 掲載論文のDOI（デジタルオブジェクト識別子） |
|---|
| |

〔学会発表〕 計( 1 )件　うち招待講演 計( 0 )件

| 発表者名 | 発表標題 【発表確定】 | |
|---|---|---|
| Naohiro Washio, Satoshi Matsuura, Masatoshi Kakiuchi, Atsuo Inomata, Kazutoshi Fujikawa | A Vehicle Clustering Algorithm for Information Propagation by Inter-Vehicle Communications | |
| **学会等名** | **発表年月日** | **発表場所** |
| Proc. of 12th IEEE Workshop on Managing Ubiquitous Communications and Services part of PerCom 2015 | 2015年03月22日～2015年03月27日 | USA, St. Louis |

〔図書〕 計( 0 )件

| 著者名 | 出版社 |
|---|---|
| | |

| 書名 | 発行年 | 総ページ数 |
|---|---|---|
| | | |

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<br>出願年月日 | 国内･外国の別 |
|---|---|---|---|---|---|
| | | | | | |

15.備考

| |
|---|
| |

（注）･印刷に当たっては、A4判（縦長）･両面印刷すること。