様式3

# 平成18年度　傾斜的研究費（特定）（全学分）（戦略分・公募分）研究報告書

研究テーマ区分　［①都市形成に関わる研究　②特徴ある教育プログラム開発をめざす研究］

| 研究課題名 | 情報セキュリティの数理とその都市における応用 | |
|---|---|---|
| 研究者または研究代表者名 | 所属部局名 | 職　位 |
| 中村　憲 | 都市教養学部・理工学系・数理科学 | 教　授 |
| 研究分担者名 | 部局名・所属研究機関名 | 職　位 |
| マーティン・ゲスト | 都市教養学部・理工学系・数理科学 | 教　授 |
| 福永　力 | 都市教養学部・理工学系・数理科学 | 教　授 |
| 村上　弘 | 都市教養学部・理工学系・数理科学 | 准教授 |
| 鈴木　登志雄 | 都市教養学部・理工学系・数理科学 | 准教授 |
| 内山　成憲 | 都市教養学部・理工学系・数理科学 | 准教授 |
| | | |
| | | |

## 研究実績の概要（600～800字で記入。図、グラフ等は記載しないこと。）

予算的制約から、情報セキュリティの数理、数理情報やデータの視覚化と共有のうち、情報セキュリティの数理を中心とした。各専門分野の結果を情報数理に統合し、その応用として新しい暗号系の提案や特許取得、試作品ソフト・ハード製作を目指した。具体的には(1)双線形写像を用いた楕円曲線暗号のパラメータ設定、(2)数体を用いた量子公開鍵暗号のパラメータ設定、(3)離散対数問題を高速に解く方式のFPGA実装、を行う事とした。

まず(1)に関しては、双線形写像計算、それに必要な多項式計算、それらを用いた有限素体上の有理点の群構造計算のＭＡＧＭＡプログラムにより、具体的な楕円曲線の双線形写像の値について、数値実験を繰返した。 それに基いて、ペアリングベース暗号に適した楕円曲線ＥＣを構成する、既知の方法を拡張したアルゴリズムを提案して、各種ペアリングベース暗号に使える新しい EC 族を生成する事に成功し、この特許を申請した。

次に(2)に関しては、有理数体と虚二次体の場合に、量子公開鍵暗号のパラメタ生成、暗号化、復号化を実行するプログラムを、中村研究室で開発中の数論システムＮＺＭＡＴＨに実装し実験した。 それにより量子計算機を使う部分以外で、鍵生成が低速である事を確認した。 そこで、鍵生成順序の変更を提案して実装し、高速化を実現した。 また、この暗号系の安全性はナップサック問題の密度や擬密度により保証されるが、従来方式によれば密度は十分高いが擬密度が低い事を調べ、これ迄の様に素数の法ではなく、合成数の法による暗号系を提案し、個々のナップサック問題は擬密度も低くできる事を示した。

最後に(3)に関しては、福永研究室で経験があるＦＰＧＡ実装をした。まずＢＳＧＳ法は値を大量に保存するため実用的ではない。そこで、単純に乗算を反復する方法を実装したが十分な効果は得られていない。今後ρ法などの値の保存が不要なものを実装してゆく。

様式3

研究発表 ［雑誌論文発表、図書、学会発表等］

| 著者（講演者） | 論文題目（発表題目） | 発表誌（発表大会名） | 年月 |
|---|---|---|---|
| C.A.ANTONIO,K.NAKAMULA, et al | Implementation of imaginary quadratic fields and elliptic or hyperelliptic curves over finite prime fields on the system NZMATH for number theory | Proc. 6th Symposium on Algebra and Computation AC2005, TMU | Nov. 2006. |
| K.NISHIMOTO and K.NAKAMULA | Computer experiment on key generation for the quantum public key cryptosystem over quadratic fields | Proc. 6th Symposium on Algebra and Computation AC2005, TMU | Apr. 2006. |
| NISHIMOTO, K.; NAKAMULA, K. | Computer experiment on key generation for the quantum public key cryptosystem over quadratic fields | 数論・組合せ論研究集会2006, 東北大学, 報告集, 59—70 | 2006.4 |
| 田中一之/鈴木登志雄他 | 「ゲーデルと20世紀の論理学(1)ゲーデルの20世紀」 | 東京大学出版（230ページ） | 2006 |
| ゲスト・マーティン | 「Harmonic maps and quantum cohomology」 | LMS Symposium on Methods of Integrable Systems in Geometry(Univ. of Durham) | 2006.8 |
| ゲスト・マーティン | 「Mirror Symmetry structures in differential geometry and complex geometry 」 | セミナー(名古屋大学) | 2006.7 |
| ゲスト・マーティン | 「Towards differential geometric mirror symmetry」 | 講話会（東北大学） | 2006.11 |
| ゲスト・マーティン | 「Pfaffin systems from harmonic maps」 | Ireland −Japan Workshop on Geometry and Dynamical Systems(慶應大学) | 2006.12 |
| ゲスト・マーティン | 「Introduction to homological geometry : Ⅰ in: Integrable System, Geometry, and Topology」 | AMS/IP Studies in Advanced Mathematics 36, 83—121 | 2006 |
| ゲスト・マーティン | 「Introduction to homological geometry : Ⅱ in: Integrable System, Geometry, and Topology」 | AMS/IP Studies in Advanced Mathematics 36, 123—150 | 2006 |
| H.Nomoto, Fukunaga, Chikara et al. | ″Installation and Test of the ATLAS Muon Endcap Trigger Chamber Electronics″, | Proceedings of 12th Workshop on Electronics for LHC and Future Experiments held at Valencia, Spain Sept 2006, pp.307-311, | 2007.1 |