Manaba 提出

２０１４年度　中央大学特定課題研究費　－研究報告書－

所属	理工学部	身分	教授
氏名	藤中　晋輝		
NAME	Fujinaka Shinki		

１．研究課題

（和文）情報セキュリティとヒューマン処理に関する研究

（英文）Studies on Information Security and Human Information Processsing

２．研究期間

２年

３．研究の概要（背景・目的・研究計画・内容および成果　和文 600 字程度、英文 50word 程度）

（和文）

情報セキュリティ技術の中で、暗号理論の安全性保証が極めて重要である。特に、安全性が極めて高い楕円暗号とその一般化となる超楕円暗号に対して、最近 GHS 攻撃という強力な攻撃が提案され、その攻撃に対する楕円・超楕円暗号の解析が、数学的に難解のため、難航極めている。そこで、本研究は、楕円・超楕円暗号の GHS 攻撃に対する弱い曲線に対して完全分類を求め、安全性解析を行うことを目的としている。

研究成果として、奇標数素数次拡大体上の楕円曲線に対して、また、種数 2 の超楕円曲線については、完全分類を得たため、楕円・超楕円暗号の安全性確保に大きく貢献した。特に 2,3,5,7 の素数次数拡大体上では、ほとんどの曲線が、GHS 攻撃をうけるという衝撃な結果を得た。この事実は、標準化されている楕円暗号系の設計や運用に大きな影響を及ぼす可能性がある。

また、ネットワークセキュリティにおいては、SQL 攻撃、XSS 攻撃、バファオバーフロー攻撃などに関して、機械学習の手法も応用して、特徴量の抽出による攻撃の検知法を開発している。

一方、マルチメディア情報処理について、人間の感性と生理特性に基づく数理モデルの構築と、それを応用した基本アルゴリズムの開発を行った。色彩情報グループは、健常者と同様な色彩感覚を色弱者に与える色弱補正法を開発し、その成果は、Journal of Optical Society of America, IEEE Transactions on Image Processing にて発表している。また、色彩工学においては、現在広く使われている ICC プロファイル方式よりも、高速で簡便なプロファイルと補正 3DLUT を構築する方法を提案し、国際会議 AIC2015 に発表した。

（英文）

This research is on theory of elliptic and hyperelliptic cryptosystems, in particular the security analysis of GHS attack.

We shown a complete classification of weak curves against the attack.

The other topic is on human media information processing, which including color vision modeling and color weak compensation.

３．研究成果について（研究期間終了後２年以内・予定のものを含めて記入）

Rika Mochizuki, Takanori Kojima, Reiner Lenz and Jinhui Chao
"Color-weak compensation using local affine isometry based on discrimination threshold matching"
Journal of the Optical Society of America A, Optica, Image Science and Vision
Vol. 32, No. 11,