SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

ハイパースペクトルカメラによるカードベース暗号の安全性評価に向けた基礎的検討

Fundamental Study on Evaluating Security in Card-based Cryptography Using Hyperspectral Camera

嶌野　雅久 *　　宮原　大輝 * †　　崎山　一男 *
Masahisa Shimano　　Daiki Miyahara　　Kazuo Sakiyama

キーワード　物理暗号，カードベース暗号，ハイパースペクトルカメラ，物理仮定

あらまし

カードベース暗号とは，物理的なカード組を用いて秘密計算に代表される暗号機能を実現する手法である．カードベース暗号に関する主な研究は，新たなプロトコルの提案や，カード枚数と手順の効率化といった理論研究である．これらほぼ全ての理論研究では，カードの区別が付かないという物理的な仮定が前提となっている．本研究ではこの物理仮定の妥当性を物理的に検証することで，カードベース暗号の安全性を高めることを目的とする．特に本研究では，高性能化が進むカメラに注目し，カードベース暗号における物理仮定を視覚の観点から検証する．その基礎検討として，本稿では高性能カメラ（光を波長ごとに分光して撮影するハイパースペクトルカメラ）とインクを用いる強力な攻撃者を想定し，カードを見分けることができるか実験を行なった．

結果として，そのような攻撃者がカメラで撮影し画像を解析することで，インクの付着箇所を判別できることを確認した．また，本研究ではこのような強力な攻撃者が得ることのできる秘密情報を理論的に考察した．

図 1: インクを付着させたカード (画像右側中央付近)

* 電気通信大学, 東京都調布市調布ヶ丘 1 丁目 5-1, The University of Electro-Communications, 1-5-1, Chofugaoka, Chofu, Tokyo 182-8585, Japan
† 産業技術総合研究所, 東京都江東区青海 2-4-7, National Institute of Advanced Industrial Science and Technology (AIST), 2-4-7 Aomi, Koto, Tokyo 135-0064, Japan