平成 8年度入学 大学院博士後期課程 システム情報工学専攻 生体数理情報学講座

氏　名　**松 川 公 一**（Koichi MATSUKAWA）

論文題目　セル・オートマトンを用いた共通鍵暗号アルゴリズムの設計

英訳題目　The Design of a New Secret-key Block Cipher Algorithm UsingCellular Automata

- **Abstract**

We propose a new secret-key block cipher algorithm called MKC1 (Matsukawa-Kobayashi Cipher NO. 1). This cipher is a Feistel type block cipher that has variable block length and key length and number of rounds. Characteristics of this algorithm is to form Multitudinous structure by choosing cryptographic function. As cryptographic function, Cellular Automata which can insure the number of enormous structure has been adopted. And some power functions in Galois Field which have resistance against differential cryptanalysis and linear cryptanalysis have been adopted. By these, the proposed block cipher is resistant against brute force attack and shortcut attack. Moreover, we clarify that the rules within 1-dimension 2-states 3-neighbors'CA whose intensity is relatively higher are almost equivalent to class 3 of Wolfram' classification. A C language implementation of MKC1 is some times faster than that of DES ona 200 MHz Pentium. We confirm industrial availability of this cipher whichwe implement on the automatic passenger gate system using contactless IC card.This thesis consists of ten chapters. In chapter 1, we introduce the background, the purpose, and the outline of this thesis. In chapter 2 we summarize block cipher algorithm. In chapter 3 we summarize cryptanalysis. In chapter 4 we explain Cellular Automata and value intensity of CA as cryptographic function. In chapter 5 we explain a way of composition of Multitudinous structure. In chapter 6 we develop substitution tables by power functions in Galois Field. In chapter 7 we describe the specification of MKC1. In chapter 8 we evaluate the security of MKC1 against brute force attacks and short-cut attacks . In chapter 9 we compare a transactional speed of MKC1 with DES, and we implement MKC1 on the automatic passenger gate system using contactless IC card. Chapter 10 concludes this thesis.

（和訳要旨）

近年、コンピュータ技術の発達により、商取り引きの分野でもネットワーク化とICカード化の2大潮流にのって電子化が進展中である。ここにおいて安全かつ円滑な活動をささえるものが社会基盤としての情報セキュリティであり、その中核技術

が暗号である。

暗号方式は共通鍵暗号と公開鍵暗号に大別できる。本研究の対象である共通鍵暗号においては、特に、近年の研究において解読法の進展にめざましいものがある。一つには、計算機能力の飛躍的向上により全数探索法に要する時間が短縮されてきており、これに対抗するため鍵長の増大が必要となってきている。他方、差分解読法、線形解読法、高階差分解読法、補間攻撃等の解析的解読法の発表・進展により、解読の危険性が増している。これらの点から、アルゴリズム側の強度が相対的に低下してきており、現在、より高い強度を持つ暗号アルゴリズムがせつに求められている。

次に、暗号アルゴリズムの用途面からながめてみると、非接触ICカードなどのように8ビットコアという低いCPU能力でかつ短時間処理を求められる用途があるため、軽く高速な暗号アルゴリズムの品揃えが求められている。

そこで本論文では、暗号化関数を選択することにより多数の構造を構成可能として高強度化をはかり、ビット処理は一部にとどめ大部分をバイト処理とすることにより高速化をはかった新しい共通鍵ブロック暗号アルゴリズムMKC1（Matsukawa-Kobayashi Cipher NO. 1）を提案している。

MKC1は、全数探索法に対しては、アルゴリズム構造を規定するビット数を共通鍵ビット数の増加分とみなせば、従来の共通鍵よりもビット数を実効的に増大することができ、高強度化をはかっている。

解析的解読法に対しては、攻撃側が使用する暗号アルゴリズムの近似表現、代数表現等の記述を不可能にするか、又はいちじるしく困難にするか、または表現導出時間を増大させるかのいずれかを施す必要があり、今回採用した関数を選択する構造が有効である。関数を選択する構造とは、暗号化関数を多数用意しておき選択組み合わせすることによって多種類の構造を構成可能とするものであり、攻撃側にとっては、攻撃対象のアルゴリズム構造が一意に定まらないため、解析的解読法の適用に非常な困難をきたす。

万が一、アルゴリズム構造が特定されたとしても、多種類の構造を選択使用できる利点を生かし、一つのアルゴリズム構造での暗号化・復号化回数を、解析的解読法が必要とする平文・暗号文組数未満にとどめて、順次、アルゴリズム構造を更新してゆけば解読はさらに困難となる。これを極限まで進めれば、一回の暗号化・復号化の都度アルゴリズム構造を使い捨てにすることができる。

この、関数を選択する構造のもとで、暗号化関数としてセル・オートマトンを採用し、そのルール数が多くとれる特長を生かした。その他の暗号化関数として、差分解読法／線形解読法に対する安全性の指標である最大差分確率／最大線形確率が最小となることが知られている有限体上のべき乗関数も使用した。

本論文は10章から構成される。第1章は研究の背景、目的、論文概要である。第2章では暗号アルゴリズムを概観している。第3章では暗号解読法を概観している。第4章はセル・オートマトンの概論を述べたのちに、暗号化関数としてのセルオートマトンの強度を評価し、使用可能なルールを選択するとともに、1次元2状態3近傍セルオートマトンの全256ルールのうち暗号関数として相対的に強度の高

いルールは、ウォルフラムの分類でクラス3にほぼ相当することを述べている。第5章では関数を選択する構造の構成法を説明している。第6章では有限体上のべき乗関数による変換テーブルを示す。第7章では、MKC1の仕様を記述している。第8章では、MKC1の安全性を暗号解読法毎に検討している。第9章では計算機実験によりDESとMKC1を比較し、MKC1はDESより数倍の処理速度をもつことを示す。さらに、MKC1を非接触ICカードを用いる自動改札システムへ実装した結果、工業的有用性が得られたことを示す。最後に第10章にて結論とする。