（ 続紙 １ ）

京都大学	博士（情報学）	氏名	岩崎　淳
論文題目	Study on permutation polynomials over a ring of modulo 2^w and their applications to cryptography		

（論文内容の要旨）

本論文では、2冪剰余環上置換多項式を用いた既存暗号の解析・改良を行うとともに、将来的な暗号技術開発の基礎となる、2冪剰余環上置換多項式が最大周期を持つ必要十分条件を、初めて明らかにするなどの理論的な解析を行っている。

第一章は、序章であり、暗号学の歴史的な背景とIoT(Internet of Things)等の近い将来への応用において要求される暗号の課題を挙げ、暗号における2冪剰余環上置換多項式の研究の重要性を説いている。

第二章は、2冪剰余環上置換多項式を用いた鍵交換法の安全性評価を行い、その安全性に関して、一定の限界があることを明らかにした。具体的には、既に2冪剰余環上置換多項式になることが証明されている奇数次Chebyshev多項式を用いたDiffie-Hellman型の鍵交換法についての安全性の評価を行った。安全性の評価を行う上で、2冪剰余環上Chebyshev多項式が2冪剰余環上でもつ軌道の周期性と、次数の周期性を、完全に明らかにしたことが安全性評価の鍵となった。この提案されていた鍵交換法を多項式時間で解読するアルゴリズムを開発することで、Chebyshev多項式を用いた鍵交換法は安全ではないことを証明し、また、結果を更に一般化し、一定の条件を満たす一般の2冪剰余環上置換多項式を用いて同様の鍵交換法を構成しても、多項式時間で解読可能であることを示した。

第三章は、2冪剰余環上置換多項式を用いたストリーム暗号(共通鍵暗号の一種)の改良とその暗号に関する攻撃に対する耐性の評価を行った。具体的には、Vector Stream Cipher(VSC)に関する改良とその評価である。VSCは、高速性・軽量性で優れていたものの、いくつかの理論攻撃が成立することが知られていた。本論文では、VSCに改良を加え、安全性を向上させたVSC2.0とVSC2.1を提案した。改良後の暗号は、ランダム性評価で良好な結果を与えるとともに、線形マスクを用いた識別攻撃に対する証明可能な安全性を有することを示した。

第四章は、2冪剰余環上置換多項式の最大周期を持つ(一本の軌道が2冪剰余環をくまなく巡る)必要十分条件を明らかにした。ストリーム暗号・乱数生成の分野では、一般に、用いられる写像の周期は長いほうが良い。2冪剰余環上置換多項式が最大周期となる必要十分条件は、多項式の次数が低い場合を除き、知られていなかった。ここでは、その必要十分条件を初めて理論的に導出した。

第五章は、最大周期を持つ2冪剰余環上置換多項式を組み合わせる方法を考察した。最大周期を持つ2冪剰余環上置換多項式は、単体ではあまりに単純すぎ、そのままストリーム暗号・乱数生成に用いることはできない。そこで、最大周期となる多項式を複数組み合わせ、より複雑な挙動をさせることが考えられる。ここでは、組み合わせることによって最大周期性が保存するような組み合わせ方を提案した。また、組み合わせることでさらに周期を伸ばす方法も提示した。

第六章は結論で、本文で得られた成果を要約している。

注)論文内容の要旨と論文審査の結果の要旨は１頁を３８字×３６行で作成し、合わせて、３，０００字を標準とすること。
論文内容の要旨を英語で記入する場合は、４００～１，１００wordsで作成し
審査結果の要旨は日本語５００～２，０００字程度で作成すること。

（続紙 ２ ）

（論文審査の結果の要旨）

サイバーセキュリティの要となる暗号において、暗号攻撃に対する安全性と、暗号化速度の高速性という相異なる2つの特性を、同時に追及するのは、重要ではあるが困難な課題である。暗号の安全性を追及すれば、暗号化の速度が低下し、暗号化の速度の高速性を追及すれば、安全性が低下する、というトレードオフがあるからである。

本論文では、2冪剰余環上置換多項式という処理速度の高速性が保証される基本変換を用いた様々な暗号化方式に関して、いくつかの暗号攻撃に関する耐性を解析し、更に、暗号を構成する基本変換要求条件である長周期性を保証する様な、2冪剰余環上置換多項式の基本的な性質を明らかにすることで、将来、暗号に利用可能な2冪剰余環上置換多項式の条件を解明している。ここで、2冪剰余環上置換多項式であるとは，2冪剰余環上で全単射となる多項式のことである。2の冪乗を法とする剰余演算はデジタルコンピュータ上では上位ビットの切り捨てという操作と等価となることから、実質的に処理コストが無視できるため、非常に高速に計算可能となるのである。これらの性質から、2冪剰余環上置換多項式は、軽量かつ高速という要求条件を満足し得る暗号を構成するための、基本変換の一つと考えられる。その一方で、2冪剰余環上置換多項式は、2001年の２冪剰余環上で置換多項式となる必要十分条件の導出(Rivest)等の少数の例外を除いて、これまでほとんど理論的な研究がされておらず、RC6等、暗号への応用例もあるにはあるが、非常に少なかった。

本研究は、2冪剰余環上置換多項式を用いた暗号に関する解析を行い、幾つかの問題を解決した。まず第一に、2005年に提案されていた2冪剰余環上置換多項式である奇数次Chebyshev多項式に基づく高速鍵交換法について解析を行い、これは最終的に安全でないことを理論的に証明した。これは、奇数次Chebyshev多項式の軌道及び次数の周期性を完全に解明したことにより得られたものである。更に、より一般の2冪剰余環上置換多項式に基づく鍵交換法に拡張しても、同鍵交換法は、安全ではないことを理論的に証明した。この結果は、2冪剰余環上置換多項式の鍵交換法への適応する場合、高速性と安全性とは両立しないという一定の限界があることを理論的に示すものである。更に、本研究は、一般の次数の2冪剰余環上置換多項式が2^wの最大周期を持つ必要十分条件を導出した。最大周期性は、軌道の完全均一性（エルゴード性）を与えるものであり、理論及び暗号への応用上、重要である。2次の2冪剰余環上置換多項式については、最大周期を持つ必要十分条件は、1969年に、Coveyouによって与えられていたが、本研究は、それを一般の次数にまで拡張し、48年ぶりの理論的成果と評価できる。また、2次の2冪剰余環上置換多項式に基づくストリーム暗号VSCを改良し、線形マスクを用いた識別攻撃に対する証明可能な安全性を有することを示した。これらの結果は、2冪剰余環上置換多項式のストリーム暗号・乱数生成の分野での一定の有用性を示唆するものである。

以上、本研究は、2冪剰余環上置換多項式の最長周期を持つ必要十分条件を導出するなどの長年の懸案だった問題を解決し、とりわけ周期性を解明し、更に、鍵交換法やストリーム暗号に関する解析や改良を与えるなど、学術上意義深い結果を与えている。

よって、本論文は博士（情報学）の学位論文として価値あるものと認める。また、平成29年2月27日、論文内容とそれに関連した口頭試問を行った結果、合格と認めた。

注)論文審査の結果の要旨の結句には、学位論文の審査についての認定を明記すること。更に、試問の結果の要旨（例えば「平成　年　月　日論文内容とそれに関連した口頭試問を行った結果合格と認めた。」）を付け加えること。

Webでの即日公開を希望しない場合は、以下に公開可能とする日付を記入すること。

要旨公開可能日：　　年　　月　　日以降