氏名	廣瀬勝一（ひろせしょういち）
学位(専攻分野)	博士（工学）
学位記番号	論工博第3004号
学位授与の日付	平成7年5月23日
学位授与の要件	学位規則第4条第2項該当
学位論文題目	Boolean Functions Related to Cryptography and Their Complexity （暗号に関連するブール関数とその複雑さ）
論文調査委員	（主査） 教授 池田克夫　教授 矢島脩三　教授 吉田　進

論文内容の要旨

本論文は，暗号に関連するブール関数の性質と計算の複雑さについて論じたもので，全5章で構成されている。

第1章は暗号に関する研究動向について述べるとともに，問題点を挙げ，従来の関連研究に対する本論文の位置付けを明確にしている。

第2章では秘密鍵暗号システムの設計および解析における重要な概念である非線形ブール関数の性質について論じている。従来より，ブロック暗号，ストリーム暗号等の秘密鍵暗号システムに対して，それぞれに適した非線形性の尺度が幾つか提案されているが，本章ではその内の伝達基準と雪崩基準について論じ，

(1) n変数ブール関数が$(n-1)$次の伝達基準を満たすための必要十分条件，

(2) n変数ブール関数が$\{0, 1\}^n - \{(0, \cdots, 0)\}$の線形独立な要素を除くすべての要素について伝達基準を満たすならば，そのすべてあるいは1個を除くすべての要素は伝達基準を満たすこと，

(3) 同じくその内の1個または3個の要素を除いたすべての要素が伝達基準を満足するn変数ブール関数の構成法，

(4) n変数ブール関数が$(n-2)$次の伝達基準を満たすための必要十分条件，

(5) 伝達基準と雪崩基準の関係について述べている。

第3章では伝達基準を満たすブール関数の複雑さについて論じている。多くの秘密鍵暗号方式に対して適用可能な強力な暗号解読方式は線形性を利用している。このことから，秘密鍵暗号方式の構成要素として，より多数の入力および出力を持つ非線形ブール関数が必要になる。本章では，

(1) 伝達基準を満たすブール関数のユネイト性について論じ，1次の伝達基準を満たすブール関数は高々2個の変数についてユネイトであることと，2次の伝達基準を満たすブール関数はどの変数についてもユネイトでないことを示すとともに，1次の伝達基準を満たし，かつ，2個の変数についてユネイトであるブール関数の存在とその構成法を与え，

(2) Maioranaの方法によって構成される n 変数完全非線形ブール関数を計算する組合せ回路に必要な否定素子の個数の最適な下界 $\lfloor \log n \rfloor - 1$ を示し,

(3) 1次の伝達基準を満たす n 変数ブール関数の式量の下界が $n^2/4-1$ であることを示し,

(4) 各出力関数がMaioranaの方法によって構成される n 入力 $n/2$ 出力完全非線形ブール関数を計算するVLSI回路の面積時間自乗複雑さの下界が $\Omega(n^2)$ であることを示し,

(5) Nybergの方法によって構成される n 入力 $n/2$ 出力完全非線形ブール関数の出力関数の中に,それを表現する変数順序つき二分決定グラフの節点数が n の指数関数に比例するような関数の存在することを示している。

第4章では秘密分散共有方式における秘密復元のために実用上重要なスライスブール関数と斉次ブール関数の回路計算複雑さについて論じている。本章では,

(1) 第 k スライスの単調回路素子数複雑さの下界が $\Omega({}_nC_k/\log_n C_k)$ であり,かつ,第 $u(>k)$ スライスの単調回路素子数複雑さの上界が $O(n\log n)$ なる k 斉次ブール関数の存在することを示し,

(2) 回路素子数複雑さと単調回路素子数複雑さとがほぼ等しい斉次ブール関数の集合を与えている。

第5章は結論で,本論文の成果をまとめている。

論文審査の結果の要旨

本論文では,情報システムのセキュリティの要である暗号に関して重要な働きをするブール関数の性質および複雑さについて論じたもので,主な成果は次の通りである。

1．秘密鍵暗号システムの設計および解析において重要な非線形ブール関数の性質に関し,伝達基準と雪崩基準について論じ,各種の場合について,n 変数ブール関数が要求された伝達基準を満たすための条件や雪崩基準との関係を求めた。

2．秘密鍵暗号方式の構成要素として,より多数の入力および出力を持つ非線形ブール関数が必要になることから,伝達基準を満たすブール関数の複雑さについて論じ,そのような関数のユネイト性やVLSI回路モデル上での計算量の下限などを示した。

3．鍵管理の方法の一つである秘密分散共有方式にとって重要なスライスブール関数と斉次ブール関数の回路計算複雑さについて論じ,回路素子数複雑さと単調回路素子数複雑さとがほぼ等しくなるような斉次ブール関数の集合を与えた。

以上要するに本論文は,暗号に関連するブール関数の性質および複雑さについて論じたもので,学術上,実際上寄与するところが少なくない。よって,本論文は博士（工学）の学位論文として価値あるものと認める。また,平成7年4月17日,論文内容とそれに関連した事項について試問を行った結果,合格と認めた。