修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　情報システム学研究科　　情報ﾈｯﾄﾜｰｸｼｽﾃﾑ学専攻　博士前期課程		
氏　　名	二本松　智	学籍番号	0852023
論 文 題 目	SHARK 暗号の Diffusion layer を応用した新たな暗号作成		

要　旨

暗号は文章やデータの機密性を守るため、昔から広く使われており、現在ではコンピュータを利用した暗号がメインであるが、暗号に脆弱性が見つかれば解読されてしまい、結果的に暗号の意味をなさないものになってしまう。そのため現在の暗号はアルゴリズムが公開され、かつ既存の解読法に耐性を持つことが必須となっている。ブロック暗号とは、平文を決まった長さ毎に分割し、鍵を利用して暗号化・復号化する暗号である。ブロック暗号には、暗号化・復号化の過程により Feistel 構造と SPN 構造に分けられ、また暗号毎に一長一短がある。

本研究では、構造や安全性を中心とした既存のブロック暗号の利点と欠点、特に現在広く使われている暗号 AES の鍵スケジューリングや拡大転置の問題点を指摘し、暗号 SHARK の拡散(Diffusion layer)を改良して作成した可変ブロック暗号について述べている。可変ブロック暗号とは、鍵の長さを自由に決めることができ、鍵の長さ毎に平文を分割し、暗号化・復号化する SPN 構造のブロック暗号である。Diffusion layer は行列計算であり、それを任意の大きさに対応させるため、暗号化・復号化毎に作成する必要があり、鍵が長ければ 3 次関数的に時間がかかるが、鍵の長さは理論的に上限なく任意の長さに決めることができ、また鍵の長さ毎に別々のアルゴリズムを作成する必要はないメリットがある。また安全性に関して、暗号解読の主流とされる差分解読法・線形解読法への耐性を持つ条件に影響する、置換(S-box)と Diffusion layer の関係から可変ブロック暗号の安全性が証明でき、鍵の長さに比例して安全性が高まるだけでなく、無意味に過剰な計算を排除した暗号となった。結果的に暗号 AES や SHARK より堅牢であり、同じ平文と鍵の長さを持つ暗号の中で最も安全性が高い暗号となっている。この安全性の条件から、現実的かつ理想的な暗号の条件について考察している。可変ブロック暗号は C 言語で作成したため、そのプログラムも載せている。