早稲田大学大学院 理工学研究科

# 博士論文審査報告書

## 論　文　題　目

## A Study of Block Cipher Modes for Encryption and Authentication

## ブロック暗号モードによる暗号化と認証に関する研究

申　請　者

| 峯松 | 一彦 |
| --- | --- |
| Kazuhiko | Minematsu |

数理科学専攻　情報数学研究

2008 年　3 月

インターネットにおける商取引、電子政府など、近年の情報通信技術により可能となった高度な経済・社会活動において、個人情報などを守るための代表的セキュリティ技術である共通鍵暗号は必要不可欠の要素となっている。共通鍵暗号とは、秘密の情報（鍵）を共有する者同士が、他者による盗聴や改ざんに対して安全に通信を行うための技術を指す。その代表的な要素技術として、ブロック暗号がある。ブロック暗号 $E_K$ は、鍵 K によって番号付けされる固定長の置換の集合で定義される。置換の入出力長のことをブロック長と呼ぶ。

最初の実用的ブロック暗号 DES の登場以後、暗号設計・解析の理論が大きく発展し、短いブロック長であれば、効率的でかつ高い安全性を持つブロック暗号の構築が可能となってきた。一方、任意長のメッセージの暗号化や、通信中のメッセージの改ざんを防ぐメッセージ認証コード（Message Authentication Code, MAC）など、入出力空間や安全性要件が異なるアプリケーションごとに一から実用的暗号を作ることは大変な労力を伴うため、多くの現実のシステムでは、単一のブロック暗号をモジュールとして用いて、もとのブロック暗号とは異なる機能や入出力空間を持つ暗号処理を実現している。この技術はブロック暗号の暗号運用モード（以下ブロック暗号モード、もしくは単にモードと略す）と呼ばれる。

モードの安全性は用いるモジュールに依存するが、モジュールが満たすべき安全性の条件が明示的に示せること、すなわち、モードの安全性が用いるモジュールの安全性に帰着できることが、実用と理論双方の観点から望ましい。ここでのモジュールおよびモードの安全性とは、ある理想的に安全なシステムとの計算量的な判別困難性を指す。例えば、任意の長さのメッセージの暗号化が目的ならば、可変長の入力（平文）と出力（暗号文）を持ち、出力から入力を求める逆関数が存在するような疑似ランダム関数を安全な暗号とみなす。ここで、擬似ランダム関数とは、どのような適応的に平文を選択し暗号文を得る攻撃（選択平文攻撃）によっても、多項式時間で真のランダム関数（任意の入力について一様乱数を出力する関数）との判別が困難な暗号（関数）と定義される。別の例として，MAC が目的の場合は、出力は比較的短い固定長で、可変長入力を持つ疑似ランダム関数を安全な MAC とみなす。

本研究の目的は、個々のモジュールの安全性を仮定したもとで、所望の安全性が証明可能なモードを構築することである。従来の代表的モードでは、ブロック暗号 $E_K$ を n ビット入出力の疑似ランダム関数と仮定したもとで、$E_K$ のみをモジュールとして用い、任意の長さのメッセージの暗号化や MAC の要件を満たすモードを構築し、それが所望の疑似ランダム関数であることを証明することで安全性を保証していた。

本研究においては、まずモードの概念を拡張し、ブロック暗号を含めた複数種類のモジュールを用いることも可能とした。また安全性の帰着についても一般化し、個々のモジュールの安全性条件とモードの安全性条件とは必ずしも一致しなくてよいこととした。すなわち、本研究では複数種類のモジュールを許すため、各モジュールにはそれぞれの安全性（擬似ランダム関数以外の安全性基準でもよい）を仮定したもとで、所望の安全性を満たすことが証明可能なモードをそれら

のモジュールを用いて構築することを目的とする。本研究では、モードとその安全性の概念を上記のように拡張し、その理論面と実用面での有効性を、第3章と4章で、それぞれ異なるアプローチにより示している。

第3章では、主にMACの構成を目的としている。従来、Cipher Block Chaining (CBC)-MACに代表される、ブロック暗号のみを用いたMACのモードがある。一方、Almost Universal (AU)ハッシュ関数と呼ばれる、異なる入力ペアに対し出力が一致する確率の上界のみを保証する鍵付き関数とブロック暗号とを組み合わせたCater-Wegman (CW)-MACと呼ばれるモードがある。AUハッシュ関数は、代数的な構成方法が存在し、実装に応じた最適化によりかなり高速となることが知られている。しかし、最適化のため実装上の柔軟性が失われるなどの問題があった。そこで本研究では、ブロック暗号以外のある鍵付き置換と、ブロック暗号とを組み合わせた方式を提案している。この方式は、前者の置換が差分一様性という性質を持ち、ブロック暗号が疑似ランダム関数であるときに、モード内部でAUハッシュ関数を構成し、従来と同等の安全性をもつCW-MACを実現している。

ここでモジュールに対して仮定した差分一様性という条件は擬似ランダム性よりも遙かに弱い条件であり、通常のブロック暗号を簡略化しても達成されることが期待される。これは、差分一様性が、差分攻撃（特定の平文対の差分値における暗号文対の差分値の偏りを利用する暗号解析手法）に対する安全性指標であり、この攻撃法からのブロック暗号の安全性を保証するため、標準のブロック暗号のサブルーチンに必ず含まれている性質と考えられる。具体的には、米国標準暗号(Advanced Encryption Standard, AES)は、段関数と呼ばれる比較的単純な鍵付き置換を、異なる鍵について10回繰り返すことで構成されているが、4回の繰り返しでも十分な差分一様性を持つことが知られている。この事実を利用し、AESで提案方式を実装した場合、AESによるCBC-MACよりも約2.5倍高速な方法となる。提案方式は、AES実装の一部を利用し、有限体の積などの代数的演算を要しないため、ハード・ソフトを問わず、従来のAESそのものを用いたモードよりも高速である。さらに、計算量的な仮定としてモジュールとして用いたブロック暗号AESの擬似ランダム性のみ仮定することで、従来法と同等の理論的安全性を持つ。これらの利点を併せ持つ方式は今まで存在せず、実用上極めて重要な成果であり、高く評価できる。

第4章では、nビットブロック長のブロック暗号を用いて、任意の大きい（整数$m>1$についてmnビットの）ブロック長のブロック暗号を構成することを目的とする。モードの安全性の基準としては、擬似ランダム置換もしくは強擬似ランダム置換である。前者は暗号文から平文を求める逆関数が存在する擬似ランダム関数であり、後者はさらにその逆関数も疑似ランダム置換となることを求める。

従来のモードは、モジュールとして用いるブロック暗号が疑似ランダム関数・置換もしくは強疑似ランダム置換であるという条件のもとで安全性を証明していた。これに対して本研究では、モジュールとして疑似ランダム関数・置換より弱い暗号である、弱擬似ランダム関数を用いる点に新規性がある。弱擬似ランダム関数とは、ランダムに平文を生成する既知平文攻撃によって真のランダム関数と

判別困難な鍵付き関数のことである。

本研究の目的は、モードのモジュールとして弱擬似ランダム関数と、それより強い関数（疑似ランダム関数・置換や強疑似ランダム置換）を用い、強い関数の最小限の使用のもと、モード全体の安全性を従来と同等に保つことである。弱い暗号ほど高速に動作する、という自然な仮定のもと、このアプローチは従来法より高速な方式となることが期待できる。結果的に、mn ビットブロック（強）疑似ランダム置換の構成において、モジュールである n ビットブロック（強）擬似ランダム置換を m によらず常に 1 回と、n ビットブロック弱擬似ランダム関数を m-1 回用いるモードを提案している。これは、従来が n ビットブロック擬似ランダム置換もしくは強疑似ランダム置換を少なくとも m 回必要としていたのに比べると、理論的に大幅な効率化を達成している。これらの成果は極めて理論的なものであるが、本研究はこれらの理論的成果の現実的な応用として、ハードディスクなどのストレージの暗号化に対する具体的なモードの提案も行っている。弱疑似ランダム関数を積極的に用いて、より強い関数の使用回数を最小限にするというアプローチは、従来 W. Aiello らによる研究しか存在せず、またのその安全性証明などに不完全な点が多かった。4 章の成果は弱い関数と強い関数を組み合わせるというアプローチを初めて包括的かつ理論的に扱い、有用性を示したものであり、理論的に興味深い、極めて重要な成果である。

また本研究のその他の理論的特長として、3 章と 4 章の提案方式の安全性証明において、U. Maurer により提案された条件付き確率分布を用いたアプローチを用いていることが挙げられる。一般にモードの安全性証明は、2 者（攻撃者と暗号）の相互作用により定義される複雑な確率論的問題となり、従来極めて複雑なゲーム理論的アプローチがとられてきた。しかし本研究は一貫して Maurer の枠組みを用いることで、直感的に明確でかつ精密な証明を示している。Maurer の枠組みは比較的新しく、実際の適用事例は少ないが、本研究はその枠組みの本質をとらえ、問題に応じて様々に一般化することで有効性を実証している点が非常に興味深い。

以上を総括すると、本論文はブロック暗号モードの概念と安全性基準を拡張し、その拡張に基づいた理論的なモード構成方法を示している。同時に、従来法より少ない計算量を達成しつつ、従来と同等の理論的安全性を保証する実用的な方式を提案し、理論上のみならず実用上の見地からも重要な成果を示している。よって本論文は博士（理学）の学位論文として価値のある論文と認める。

2008 年 3 月

| | | | |
|---|---|---|---|
| 審査員（主査） | 早稲田大学教授 | 博士（工学）早稲田大学 | 松嶋 敏泰 |
| | 早稲田大学教授 | 工学博士（早稲田大学） | 大石 進一 |
| | 早稲田大学教授 | 工学博士（大阪大学） | 平澤 茂一 |