審査の結果の要旨

論文提出者氏名　　李 善英

本論文は「Design and Evaluation of Cryptographic Hash Functions (暗号学的ハッシュ関数の構成と評価に関する研究)」と題し，ユーザやメッセージの正当性を認証する認証コード(MAC)・ディジタル署名などの認証技術の基本的要素であり，その安全性・効率性と密接な関係にあるハッシュ関数について，その二つのクラスであるユニバーサルハッシュ関数と衝突困難ハッシュ関数の双方の新しい構成法を提案・評価したものである．特に，安全性の証明が困難であるMDx族ハッシュ関数の連鎖の特徴を評価する方法を提案し，MD5の連鎖特徴の評価を行っている．これにより，MD5以外のMDx族ハッシュ関数における連鎖の特徴を考察することができること，さらに差分攻撃に耐性を持つためのモデルが考えられることを示している．論文の構成は「序論」を含めて6章からなり，英文で書かれている．

第一章は「序論」であり，本研究の背景を明らかにした上で，研究の動機と目的について言及し，研究の位置づけについて整理している．

第2章は「暗号学的ハッシュ関数」と題し，ハッシュ関数の定義，応用，ハッシュ関数の構成に必要である要素，基本理論を概括し，ハッシュ関数の設計理念を明確にしている．特に安全性の証明の面でハッシュ関数をユニバーサルハッシュ関数と衝突困難ハッシュ関数の2つのクラスに分けて考察している．

第3章は「安全性を証明可能なハッシュ関数の構成」と題し，その安全性が衝突確率で証明できるユニバーサルハッシュ関数について述べている．ユニバーサルハッシュ関数の問題点はハッシュ値の計算に時間がかかることである．そのため，実用的なユニバサールハッシュ関数のためには演算を高速で行う必要がある．本論文では，現実的に使用可能で安全なユニバーサルハッシュ関数として，最も効率がよいとされているSquare Hashに基づいたハッシュ関数 SNH(Square and Non-linear Hash)を構成し，その安全性を衝突確率で評価している．提案ハッシュ関数SNHは，Square Hashに比べ計算量が多少多いが，現在のコンピューターの構造を用いるとほぼ同じ実行時間でハッシュ値の計算が可能である．また，提案ハッシュ関数はSquare Hashに対し衝突確率が3分の1となり，安全性が高いことを証明している．

第4章は「多重パタンーを用いるMD5の新しい連鎖」と題し，MD5ににおける差分攻撃を想定した時の連鎖の特徴を考察し，差分攻撃に対し，さらに良い連鎖が存在することを述べている．最も幅広く使われている衝突困難ハッシュ関数であるMD4に基づいたMDx族ハッシュ関数は，簡単な演算の繰り返しでハッシュ値を計算する．しかし，試行錯誤的方法によって構成されるた

め，その理論的な安全性の評価が困難であった．本章では，MDx族ハッシュ関数の連鎖を考察するため，ハッシュ関数の演算を排他的論理和として近似するモデルを提案し，MD5の圧縮関数の評価を行っている．さらに，MDx族ハッシュ関数の安全性を高める方法として多重連鎖を用いた方式を提案し，評価している．多重連鎖を用いる方式は圧縮関数で使われる変数の順番だけを変えるため，余分のメモリも作業も必要としない．

第5章は「マルコフモデルに基づいたハッシュ関数」と題し，安全なハッシュ関数をマルコフモデルに基づいて記述している．また，ハッシュ関数における攻撃として差分攻撃を想定して，その攻撃に耐性を持たせる方法として入力の差分を拡散する方法を提案し，その安全性について述べている．入力の差分はマルコフ連鎖に基づいて生成される新しいメッセージにより拡散され，圧縮関数により差分が減少しても，次の段階で原入力の差分を保つ新しい入力を用いるため，最後まで入力の差分を出力に残すことができることを証明し，差分攻撃に対し，耐性のあるハッシュ関数設計の指針を与えている．

最後に第6章は「結論」で，本研究の総括を行い，併せて将来のハッシュ関数の展望などについて述べている．

以上これを要するに，本論文は，暗号学的ハッシュ関数の構成と評価に関する理論をまとめたものであり，これらのハッシュ関数に関する研究はハッシュ関数の構成や評価の基盤となるとともに，暗号の応用分野，特に認証の効率性・安全性の向上に貢献するところが少なくない．

よって本論文は博士（工学）の学位請求論文として合格と認められる．