別紙１

論文の内容の要旨

論文題目	ハッシュ関数の設計理論
学位申請者	内藤　祐介

本論文では，ハッシュ関数を理想化したランダムオラクル(RO)からハッシュ関数への置き換えを保証するハッシュ関数のIndifferentiability From Random Oracle (IFRO)安全性に注目して、既存のハッシュ関数の救済と新しいハッシュ関数の設計を行った．

ランダムオラクル証明法(RO証明法)は暗号学的なハッシュ関数を用いた暗号システムの安全性を保証する最も重要な証明方法である．ハッシュ関数を部品とする暗号アルゴリズムをC（・）と書き，具体的なハッシュ関数H^PをCに組み込んだC(H^P)を暗号システムと呼ぶ．RO証明法を用いて暗号システムC(H^P)のG-安全性を証明するとき，まずハッシュ関数H^Pを理想化したランダムオラクル(RO)を用いる暗号システムC(RO)のG-安全性を証明する．一般には，ROをH^Pに置き換えたC(H^P)のG-安全性が保証されていない点がRO証明法の問題である．

ハッシュ関数H^Pは，入力長が任意長の関数で入出力長固定のプリミティブPと，Pを用いて任意長の入力を規定長の出力に変換する定義域拡張構造Hから構成される．H^PはHとPから構成されているので，入力に対して規定長のランダムな値を出力するROとは異なる動作をすることが，上記の問題の原因である．

Indiff. 理論 (Indifferentiability理論)は，Pを理想的化して，C(RO)のG-安全性からC(H^P)のG-安全性を保証する理論で，「関数H^PがIndifferentiable From RO（IFRO）（H^P:IFROと書く）ならば，シングルステージ（SS）という制約条件はあるものの，任意のSSの安全性Gsと任意のCに対し，C(RO)がGs-安全性ならばC(H^P)もGs-安全性となる(C(H^P)-Gs-C(RO)と書く)」ことを保証する．IFRO安全性は，Pの構造を理想化して H^PがROとみなせるための，Hの構造に関する安全性である．

IFRO安全の概念が提案されて以降，Sponge構造やChopMD構造など，多くのIFRO安全な定義域拡張構造が提案されている．特に，Sponge構造は次世代標準ハッシュ関数SHA-3として採用されることが決まっているおり，IFRO安全性は定義域拡張構造の標準的な安全性の概念となっている．

ところで，Merkle-Damgard（MD)構造はIndiff. 理論が提案される以前に設計されており，SHA-2ハッシュ関数族であるSHA-256とSHA-512の定義域拡張構造に採用されている．残念なことに，MD^PはIFROをみたさないことが知られている．すなわち，∃Gs，∃C s.t. $C(MD^P)$ NOT-Gs-C(RO)（C(RO)はGs-安全性を満たすが$C(MD^P)$はGs-安全性を満たさない）が知られている．

Indiff. 理論は，任意のSSの安全性をカバーするものの，任意のマルチステージ(MS)の安全性Gmをカバーしない．すなわち，∃Gm，∃H^P s.t. H^P:IFRO∧C(H^P) NOT-Gm-C(RO)が知られている．

実用面からは，ハッシュ関数は高速に計算できることが求められる．今後，SHA-3は多くの暗号システムで実装されるハッシュ関数であり，Sponge構造のハッシュ関数族の高速化はSHA-3を用いる暗号システムの高速化につながるため重要な研究テーマである．

また，ハッシュ関数の実装に関する要件として，ハッシュ関数のプログラムサイズや回路サイズが小さいことが好ましい．これらを小さくすることが可能な定義域拡張構造Hとして，ブロック暗号（例えば，AES）をプリミティブとする倍ブロック長定義域拡張構造がある．ブロック暗号とハッシュ関数を両方実装する場合，ブロック暗号を共通化して使うことができるなら，実装サイズを削減できると期待できる．既存研究では IFRO安全性より弱い安全性である衝突困難性を満たす構造Hは提案されているものの，IFRO安全をみたすHは提案されていない．

当然のことながら，ハッシュ関数を設計するために，既存の攻撃法の限界を見極めることは重要である．差分攻撃法は強力な攻撃法の1つであり，Message Modificationという攻撃技法が2004年にSHA-0とSHA-1に適用されて以降，ハッシュ関数の安全性解析が活発になった．この攻撃法の限界を見極めることは，ハッシュ関数を設計する立場からも重要である．

以上の背景を踏まえて，本論文ではハッシュ関数の利用法と設計論の確立を目標として，Indiff. 理論に関して次の5つの研究課題を設定して研究する．

1. シングルステージ(SS)の安全性に対するMerkle-Damgard 構造の救済．
2. マルチステージ（MS）の安全性に対するIFRO安全な定義域拡張Hの救済．
3. 構造Sponge族の高速化を狙いとした各種パラメータの選択法の確立．
4. 部品Pとしてブロック暗号を用いたIFRO安全性な定義域拡張Hの提案．
5. 攻撃技法 Message Modification の限界の探求．

【研究課題1について】
∃Gs，∃C s.t. $C(MD^P)$ NOT-Gs-C(RO)となることが知られているものの，重要なGsと実用的なC_0に対して，$C_0(MD^P)$ NOT-Gs-C_0(RO)となるとは限らない．また，MDの重要性から$C_0(MD^P)$がGs-安全性を満たすことが望ましい．

本研究では，IFRO安全性を弱めた安全性概念「Indifferentiable from Weakened RO（IFWRO）」を定義して，実用的なC_0としてRSA-FDH，RSA-OAEP，RSA-KEMに構造MDを用いたハッシュ関数を組み込んだ暗号システムが安全となることを証明した．本成果は広く使われている暗号システム$C_0(MD^P)$を救済するものである．

【研究課題2について】
$\exists Gm$, $\exists C$ s.t. $C(H^P)$ NOT-Gm-C(RO)となることが知られているものの，重要なGm^*と実用的なC_0に対して，$C_0(H^P)$ NOT-Gm^*-C_0(RO)となることは限らない．また，SpongeとChopMDの重要性から，$H^P \in$ {Sponge, ChopMD}，重要なGm^*，実用的なC_0に対して，$C_0(H^P)$ NOT-Gm^*-C_0(RO)となっていることが望ましい．
既存研究の成果として，Reset Indifferentiability (Reset Indiff.)理論はMSの安全性をカバーし，「ハッシュ関数H^PがReset Indifferentiable from RO (RIFRO) (H^P:RIFROと書く)ならば，$\forall Gm$, $\forall C$:C(H^P)-Gm-C(RO)となる」ことが示されているが，H∈{Sponge, ChopMD}はH^P:NOT RIFROなので実用性はない．

本研究では，RIFRO安全性を弱めた概念「Reset Indifferentiable from WRO (Weakened RO)」を定義して，IFRO安全で重要なH^PであるSponge構造とChopMD構造，重要なGm^*であるCDA安全性，C_0としてC_0(RO)でCDA安全となるように設計されたEwHとREwHに対して，C_0(H)がCDA安全性をみたすことを証明した．

CDA安全性は複数の攻撃者の結託を許す強力な攻撃を想定している．今後，攻撃技法が向上すると予想されるので，CDA安全性をみたすことが好ましい．現在，CDA安全性をもとに設計された暗号システムの適用先は研究段階であるが，今後，必須の安全性要件となる可能性を秘めている．

【研究課題3について】
Spongeは入力値を処理するAbsorbingステップと出力値を計算するSqueezingステップから構成される．Spongeでは，Absorbingステップの内部パラメータは最適な値が設定されているものの，Squeezingステップのパラメータを適切に選択すると高速化の余地が残されている．

本研究では，Sponge関数族としてパラメータを可変にしたMspongeとMSponge*を提案し，SpongeのIFRO安全性証明を見直した．IFRO安全性を厳密に証明することで，Squeezingステップの最適なパラメータを求めた．例えば，パスワードなど短いメッセージのハッシュ値を使用する状況でMspongeとMSponge*はSpongeと同じIFRO安全性を満たしつつ，1.5～2倍高速化できることを示した．SHA-3を仕様変更して最適なパラメータ値を選択することで，高速化が可能となる．

【研究課題4について】
本研究では，IFRO安全な倍ブロック長定義域拡張構造を提案する．提案方式は，既存方式とほぼ同等の速度と実装サイズを保証し，安全性は衝突困難性からIFRO安全性に向上した定義域拡張構造である．

【研究課題5について】
本研究では，既存のSHA-0に対する差分攻撃法を改良することで，SHA-0に対する差分攻撃法の限界点を見極める．本研究では，既存の差分攻撃法で用いられるMessage Modification技法を改良した，Submarine Modificationを提案する．次に，Submarine ModificationをSHA-0に適用し，SHA-0の衝突困難性は，既存結果で2^{39}回のSHA-0演算で破られていたが，本研究で2^{36}回のSHA-0演算で破れることを示す．
SHA-0は多くの暗号システムに組み込まれているSHA-1と非常に似た構造を持つので，本研究を足掛かりにSHA-1の差分攻撃計算量を改良できる可能性がある．本研究成果は，SHA-1の安全性を見極める重要な成果の1つである．

別紙 2

論文審査の結果の要旨

学位申請者氏名　内藤　祐介

審査委員主査　太田　和夫

委員　西野　哲朗

委員　崎山　一男

委員　吉浦　裕

委員　※安藤　清

本論文では，ハッシュ関数を理想化したランダムオラクル(RO)からハッシュ関数への置き換えを保証するハッシュ関数のIndifferentiability From Random Oracle (IFRO)安全性に注目して、既存のハッシュ関数の救済と新しいハッシュ関数の設計を行った．

第1章では，本論文の背景の背景として，ハッシュ関数Hを暗号アルゴリズムCに組み込んだ暗号システムC(H)の安全性をC(RO)で証明するRandom Oracle (RO)証明法があることを述べた．そして，C(H)がC(RO)と同じ安全性を持つための必要十分条件としてHがIFRO安全性を満たすことを述べた．次に，IFRO安全性に関する課題として，下記の5つの課題があることを述べ，課題に対する本論文の成果を述べた．

1. シングルステージ(SS)の安全性に対するMerkle-Damgard 構造の救済．
2. マルチステージ (MS) の安全性に対するIFRO安全な定義域拡張Hの救済．
3. 構造Sponge族の高速化を狙いとした各種パラメータの選択法の確立．
4. 部品Pとしてブロック暗号を用いたIFRO安全性な定義域拡張Hの提案．
5. 攻撃技法 Message Modification の限界の探求．

第2章では，本論文で扱うIFRO安全性と既存研究についてまとめた．特に，本論文で取り組む研究課題について詳しく述べた．

第3章では，MD (Merkle-Damgard)構造を救済する方法として，ROを弱めた安全性概念「Indifferentiable From Weakened RO (IFWRO)」を定義し，実用的なC_0としてRSA-FDH, RSA-OAEP, RSA-KEMに構造MDを組み込んだ暗号システムが安全となることを証明した．本成果は現在広く使われている暗号システム$C_0(MD^P)$を救済することに成功した．

第4章では，MSの安全性において，C_0(RO)の安全性からIFRO安全なハッシュ関数Hを用いたC_0(H)の安全性を保証するReset Indifferentiable From RO安全性を弱めた概念「Reset Indifferentiable From WRO (RIFWRO)」を定義して，HとしてSponge構造とChopMD構造，重要なMSの安全性であるCDA安全性，C_0としてEwHとREwHに対して，C_0(H)のCDA安全性を証明した．

CDA安全性は複数の攻撃者の結託を許す強力な攻撃を想定しているので，今後，攻撃技法の向上の対策として，CDA安全性をみたすことが好ましい．現在，CDA安全性をもとに設計された暗号システムの適用先は研究段階であるが，今後，必須の安全性要件となる可能性を秘めている．

第5章では，次世代米国標準ハッシュ関数SHA-3に採用されているSponge関数族として，IFRO安全性を保ちつつ高速化可能なMSponge構造とMSponge*構造のパラメータ選択法を提案した．この結果はSHA-3の仕様に影響を与える可能性がある．

第6章では，ブロック暗号の暗号化関数を部品として用い，さらにIFRO安全性を満たすハッシュ関数の構造を提案した．この構造により，暗号化とハッシュ関数両方実装する環境において，ブロック暗号の暗号化関数をハッシュ関数の部品として使うことができるため，プログラムサイズや回路サイズの削減に寄与する．

第7章では，ハッシュ関数に対する強力な攻撃法である差分攻撃法に注目し，差分攻撃法で用いられる手法であるMessage Modificationを拡張したSubmarine Modificationを提案した．そして，Submarine ModificationをSHA-0に適用し，衝突困難性を破る計算量を2^{39}から2^{36}に改良することに成功した．

以上のように3章では，IFRO安全性ではカバーできないMD構造をIFWROを用いて救済した．4章では，IFRO安全性がカバーしていないMSの安全性に対して，IFRO安全な構造HをRIFWROを用いて救済した．5章では，次世代標準ハッシュ関数SHA-3の構造に採用されているSponge構造をベースにMSpongeとMSponge*を提案して，IFRO安全性を保ちつつ高速化可能なことを示した．そして，6章では，ブロック暗号の暗号化関数を用いることでプログラムサイズや回路サイズを削減できるIFRO安全な構造を提案した．最後に，7章では差分攻撃法の改良手法を提案した．

このように，本論文は既存構造の救済，実装コストを考慮に入れた新しい構造の提案，そして，強力な攻撃法の改良とハッシュ関数の研究に幅広く貢献した結果を与えており，本論文は博士（工学）の学位請求論文として十分な価値を有するものと認める．