IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

共通鍵暗号をベースとした
ハッシュ関数安全性評価手法の調査
概要報告書

2008 年 5 月

独立行政法人　情報処理推進機構

共通鍵暗号をベースとしたハッシュ関数安全性評価手法の調査
概要報告書

1. 目的

本調査は NIST の公募への提案が想定されるハッシュ関数を対象とし、共通鍵暗号をベースとしたハッシュ関数が満たすべき安全性要件を明確化すること、これらの要件が暗号学的あるいは数学的に何を根拠に達成されているかを調査すること、共通鍵暗号をベースとした新しいハッシュ関数の安全性とそれを評価する手法の枠組みに関する知見を得ることを目的とする。

2. 作業内容と手法概要

文献調査、ヒアリング調査、学会参加による調査、内容分析等の手法により、次の(1) から(4) を行った。

(1) ハッシュ関数 MAME の安全性評価手法の調査
(2) 証明可能なハッシュ関数の安全性証明手法の調査
(3) 実装効率性を重視した新しいハッシュ関数の安全性評価手法の調査
(4) 共通鍵暗号をベースとしたハッシュ関数の安全性評価ツール仕様の検討

3. 調査結果

2.(1) については、MAME の安全性を担うブロック暗号部の調査、検討を行い、AES 会議以降に提案されてきた重要な安全性評価手法を纏めることにより、MAME のへの適用が可能と考えられる安全性評価手法や脅威を洗い出し、将来の MAME の安全性評価のための指針とした。

2.(2) については、ハッシュ関数の安全性評価を行うための基礎をなす安全性評価のためのモデルに関する動向を整理した上で、既存のハッシュ関数について、標準として利用されているもの、また、近年新しく提案されたものを中心としての比較を行なった。調査と検討により、設計方法や安全性評価のためのモデル等に関し、抜本的な見直しが行われていることを把握し、ハッシュ関数の定義域拡大の構成方法や証明方法に関する技術や、本研究分野の方向性や課題に関する知見を得た。

2.(3) については、近年盛んに研究がなされてきた、衝突耐性に対する攻撃を重点的に扱った。既存のハッシュ関数を、定義域拡大+圧縮関数型と PANAMA 型の 2 つに分け、それぞれにおいて、具体的なアルゴリズムに対する攻撃例を調査、検討した。定義域拡大＋圧縮関数型では、ラウンド削減された Tiger 及びフルラウンドの FORK-256 に対する衝突攻撃を扱った。簡約版 Tiger に対しては、中間一致によるメッセージ更新の手法を用いて差分解析で攻撃されることを見た。攻撃は、16 ラウンドの Tiger に対して、2^{44} 回の圧縮関数呼び出しで行われるものである。新たなハッシュ関数の設計の際には、この手法に対

する耐性も考える必要があることが分かった。FORK-256 に対しては、メッセージの拡散の不十分さに起因して、フルラウンドの関数が破られることを見た。攻撃計算量は、$2^{112.9}$ 回の圧縮関数呼び出しである。FORK-256 の圧縮関数は、4 並列で処理を進めるという実装効率上の利点があるが、逆にこの点が安全性上の弱点となり、攻撃を可能にしたと言える。その他のアルゴリズムとして、MD4, MD5, SHA-1, SHA-256, HAVAL 等の調査、検討を行った。PANAMA 型としては、PANAMA 及び Grindahl を扱った。特に、Grindahl の衝突耐性に対する切り詰め差分攻撃に関して詳しく調査、検討した。攻撃は、全バイトに差分のある状態ペアを 2112 組だけ生成する計算量で行われる。Grindahl は Rijndael の構成要素を用いて構成されており、MixColumns 及び ShiftRows の効用により、わずかな差分が数ラウンドのうちに全バイトに広がるという性質を持つ。しかし、攻撃では、この性質を逆手にとり、全バイトに差分がある状態を出発点にしている。設計者は、差分のあるバイトが常に少ないような差分パスは存在しないことは確かめていたが、攻撃手法のパスはこのようなパスには含まれない。このことは、設計時には一般的な攻撃法のみならず、多様な攻撃法をできる限り想定する必要があることを、示している。

2.(4) については、特に、ハッシュ関数の構成ブロック暗号部の差分攻撃耐性を評価するための方法論を纏めた。