修 士 論 文 の 和 文 要 旨

大学院　電気通信学　研究科　　博士前期課程　　情報通信工学　専攻		
氏　　名	佐々木　悠	学籍番号 0530018
論　文　題　目	How to Construct Sufficient Conditions for Hash Functions	

要　　旨

本研究は、2005年、Wangらによって提案されたハッシュ関数の衝突攻撃に関して、その手順の一部を自動化するためのアルゴリズムを提案する。衝突攻撃の手順は以下の通りである。

事前計算フェイズ

1．メッセージ差分（⊿M）を求める。
2．⊿Mがどのように伝播するかを定める差分パス（DP）を求める。
3．DPが実現されるための十分条件を求める。この条件をSufficient Condition(SC)と呼ぶ。
4．SCを高確率で満たすMessage Modification(MM)の手順を考える。

探索フェイズ

1．MMを適用しながら全てのSCを満たすメッセージMを探索する。
2．M'=(M+⊿M)を計算する。MとM'が衝突を起こす。

手順からわかる通り、SCを求めることは衝突攻撃において必須である。DPや⊿Mが変更された場合、SCを求め直す必要があるが、これまでの方式ではSCを手作業で求めており、時間がかかり過ぎて非効率であるという問題があった。また、衝突攻撃の計算量はSCの数に依存するので、できるだけ少ない個数のSCを生成することが重要であるが、これまでの方式ではSCを手計算で導出していたので、導出されたSCが部分的に無駄を含んでいるという問題があった。本研究では、⊿MとDPの一部を入力とし、SCを出力するアルゴリズムを提案する。このアルゴリズムにより、MD4, SHA-0, SHA-1のすべてのSCと、MD5の大部分のSCを求めることができる。実験として、MD5のWangらによって与えられた差分に対して提案するアルゴリズムを用いてSCを求めたところ、数秒以内にSCを生成することができた。また、生成されたSCの個数を、現在のMD5の衝突攻撃に対する最新の研究のものと比較したところ、我々のアルゴリズムで導出されたSCの個数は、従来のものより12個少ないことが判明し、アルゴリズムの有効性を示すことができた。