廣瀬　勝一
福井大学工学研究科　准教授

暗号方式の構成とその効率の限界

ハッシュ関数は様々な暗号方式の構成に利用される重要な要素である。ハッシュ関数は任意長入力、固定長出力の関数である。ハッシュ関数に要求される性質として、原像計算困難性、第二原像計算困難性、衝突計算困難性が挙げられる。これらのうち、特に注目されるのが衝突計算困難性である。これは、ハッシュ関数の衝突、すなわち、同じ出力に対応する相異なる入力の組を得ることが困難であるという性質である。

一方、様々な暗号方式の安全性を保証する方法として、安全性を厳密に定義して、それが満たされることを数学的な証明により保証する手法が用いられる。そのような安全性証明では、ハッシュ関数はしばしば、理想的なランダム関数であると仮定されており、暗号におけるハッシュ関数の重要な利用法として、理想的なランダム関数の代替が挙げられる。

このような背景の下、本研究では、以下のハッシュ関数の構成法とその安全性および効率を検討した。

(1) 衝突計算困難性を満たすハッシュ関数
(2) 理想的なランダム関数の代替となるハッシュ関数

(1)に関しては、倍ブロック長ハッシュ関数と呼ばれる構成法に関して、ランダムオラクルモデルあるいは理想的暗号モデルと呼ばれる仮定の下で最適な安全性を有する、これまでで最も効率の良い構成法を提案した。

(2)に関しては、ランダムオラクルモデルの仮定の下でこれまでに提案されている構成法と同等の安全性を有しながら、最も効率の良い構成法を提案した。この構成法は(2)の意味での安全性を満たさない構成法にわずかな修正を施した方法であり、この効率はほぼ最適であると考えられる。また、この構成法によるハッシュ関数が衝突計算困難性を満たすことも容易に示すことができる。

研究成果

Some Plausible Constructions of Double-Block-Length Hash Functions
Lecture Notes in Computer Science pp210-225, 4047, 2006

How to Construct Double-Block-Length Hash Functions
The Second Cryptographic Hash Workshop, 2006

A Domain-Extension Scheme for Random Oracles
2007 年暗号と情報セキュリティシンポジウム予稿集 2007