2007年1月22日
独立行政法人情報通信研究機構
株式会社日立製作所

RFIDタグにも搭載可能な演算処理量の少ないハッシュ関数を開発
小型電子機器の情報セキュリティ対策に最適な機器認証システムが実現可能に

独立行政法人情報通信研究機構(理事長:長尾 真／以下、NICT)と株式会社日立製作所(執行役社長:古川 一夫／以下、日立)は、このたび、通信データの暗号化や機器を認証するための演算手法として用いられているハッシュ関数*1をRFIDタグ*2などの小型機器にも搭載できる技術を開発しました。従来のハッシュ関数は、演算をするために多くのメモリ容量を必要とすることから、小型電子機器に利用することは困難でしたが、今回開発したハッシュ関数は、単一の演算処理を繰り返すアルゴリズムを用いるため、演算をするための回路規模を小さくすることができ、RFIDタグなどの小型機器にも利用することが可能になります。これにより、クレジットカードやRFIDタグなどによる認証分野などの幅広い分野でハッシュ関数を用いることができ、これらの分野で安全性を高めることが可能になります。

なお、本成果は、NICTから日立への委託研究「ICカード等における認証のための高度な暗号技術に関する研究開発」(2004～2006年度)によるものです。

ユビキタス情報社会では、多くの電子機器を用いてさまざまなサービスの提供を可能にするために、サービスの不正利用や情報漏洩などに対する情報セキュリティ対策が重要になっています。特に、利用者の機器を認証することはセキュリティを確保するために重要であり、その方法として、機器の固有情報からその要約値を偽造できない形で作成して、確認側の保有情報と比較する方法がとられています。この要約値を作成する演算手法がハッシュ関数ですが、従来のハッシュ関数では、演算をするために多くのメモリ容量を必要とするため、認証機能付きの回路を小型化することや低消費電力化することが難しく、RFIDタグなどの小型電子機器に用いることはできませんでした。

さらに、近年では、今まで一般的に使われてきたハッシュ関数において、機器を認証する際に同じ要約値になる可能性があることが報告され、安全に対する危険性が懸念されてきています。このような背景から、演算処理量が少なく、安全性の高いハッシュ関数の開発が課題となっていました。

そこで、NICTの委託研究として日立は、RFIDタグにも搭載することができる、小型化するための要素と高い安全性を併せ持つ新たなハッシュ関数を開発しました。本技術の特長は次のとおりです。

1.小型電子機器へ搭載可能なハッシュ関数

今回開発したハッシュ関数は、単一の演算処理を繰り返すアルゴリズムを用いるため、従来の約半分の8.2Kゲート相当の回路規模で実現できます。これまでに提案されたハッシュ関数の中では最軽量クラスであり、RFIDなどのユビキタス向け小型機器での利用に適しています。

2.衝突攻撃に対して安全なハッシュ関数

ハッシュ関数には、出力値が同じになることを発見することが困難であることが要求されます。これに対して、ある限られた試行回数で同一の出力値をもつ2つの入力メッセージを発見する攻撃を衝突攻撃と呼びます。今回、衝突攻撃に対する耐久性を指標化し、この指標化された数値を基に耐久性の高いハッシュ関数のアルゴリズムを開発しました。その結果、既存のハッシュ関数である MD5*3 や SHA-1*4 の攻撃に成功した最新の衝突攻撃に対しても十分な安全性を有しています。

なお、本技術は、1月23日から開催される「暗号と情報セキュリティシンポジウム」で発表する予定です。

*1 任意のメッセージ入力に対して固定長の出力値を生成する関数。出力値が同じになる入力の発見が困難であることが要求される。

*2 Radio Frequency Identification の略。ID情報を内蔵した小型の無線タグと、それを用いたID化技術の総称。

*3 Rivest が1992年に提案したインターネット標準のハッシュ関数アルゴリズム。

*4 米国商務省標準局(NIST: National Institute of Standards and Technology)が開発したハッシュ関数アルゴリズム。米国のみならず、インターネット、ISO等で標準化されている。

■照会先

株式会社日立製作所 システム開発研究所 企画室［担当:森］
〒215-0013 神奈川県川崎市麻生区王禅寺1099番地
電話 044-959-0325(直通)

以上