2009年1月21日
株式会社日立製作所

安全で高速な次世代ハッシュ関数を開発

スポンジ型構成法を適用し標準ハッシュ関数SHA-1が持つ安全性の弱点を解決

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、ベルギーのルーヴァン・カトリック大学と共同で、情報の安全性を確保する暗号技術の土台となる、安全で高速な次世代ハッシュ関数[*1]を開発しました。今回開発したハッシュ関数は、「スポンジ型構成法」と呼ばれる、全データを一括して安全な圧縮処理を行う方式を適用することで、現在標準となっているハッシュ関数「SHA-1[*2]」より安全性を高めながら、パソコンや携帯電話、ICカードなどの様々な製品やシステムにおいて高速処理が可能です。

急速に進展する情報化社会において、ネットワークを介して送受信される金融情報や機密情報などの様々な重要情報を保護するために、高度な暗号技術が重要な役割を果たしています。中でもハッシュ関数は暗号技術の土台となるもので、デジタル情報を圧縮して特徴値[*3]を抽出する関数です。この特徴値はデータの指紋とも呼ばれており、異なるデータから抽出された特徴値が一致する可能性はきわめて低く、情報がわずかでも変わると、変換される数値が大きく異なります。これにより、ハッシュ関数は、意図的な特徴値の操作が困難なことから、データの破損を検出するために用いられるほか、悪意ある第三者によるデータの改ざんを検出するためにも用いられています。

現在、最も普及が進んでいるハッシュ関数は160ビット長の特徴値を出力するSHA-1と呼ばれる関数です。しかし、2005年に、最新の暗号解析技術によって、ある種のデータについては特徴値が一致するようなデータを見つけやすい、という脆弱性が発見され、期待される安全性を確保できないことが明らかになりました。2004年以降、米国商務省国立標準技術研究所（以下、NIST[*4]）は、256ビット長の特徴値を出力するSHA-2[*5]への移行を推奨していましたが、これと並行して、2007年11月に、新たな標準ハッシュ関数を選定するコンペティション[*6]（以下、SHA-3コンペ）を開始しました。

このような背景から、今回、日立はルーヴァン・カトリック大学と共同で、日立が持つストリーム暗号の研究開発で培った技術と、ルーヴァン・カトリック大学が持つ安全性評価技術とを融合した、安全で高い処理性能を持つ次世代ハッシュ関数を開発しました。

■開発技術の詳細

⑴ 安全性の高い「スポンジ型構成法」

これまでの多くのハッシュ関数は、一定サイズのデータブロック毎に安全な圧縮処理を行うという設計思想に基づいて設計されていました。これに対し今回開発したハッシュ関数は、全データを一括して安全な圧縮処理を行う「スポンジ型構成法」を適用し、レジスタの効率的な利用により、データ全体を効果的に攪拌[*7]し、従来型に比べて高い安全性を実現しました。

⑵ 高処理性能の実現

ハッシュ関数は大量のデータを処理する用途も多く、処理に時間がかかると実用化の障壁となります。そこで、新方式では、単一の基本関数を複数個並列に配置する構造にし、並列処理実装を可能にしました。これにより、ソフトウェアによる高速処理ができ、パソコンや携帯電話、IC カードなど様々な製品やシステムで高い処理性能を出すことが可能になりました。

以上の技術により開発したハッシュ関数について、256 ビットの特徴値を生成するアルゴリズムと、512 ビットの特徴値を生成するアルゴリズムを試作し性能を評価した結果、前者は 32 ビット CPU 上で 13.9 cycles／byte、64 ビット CPU 上で 13.2 cycles／byte、後者は 32 ビット CPU 上で 25.5 cycles／byte、64 ビット CPU 上で 23.2 cycles／byte の処理性能が得られ、両 CPU 上で高速な処理性能を出すことができました。特に、32 ビット CPU 上での結果は、SHA-3 コンペでの評価基準の一つであるハッシュ関数 SHA-2 と比べても、約 20 パーセント高速となるものです。

2008 年 10 月、日立とルーヴァン・カトリック大学は共同で、今回開発したハッシュ関数を SHA-3 コンペに応募[*8] し、全 64 ハッシュ関数の中から今回開発した関数を含む 51 のハッシュ関数が候補として認定されました。今後は、安全性や性能等の様々な面から候補の比較が行われ、2012 年に NIST により次世代ハッシュ関数 SHA-3 が選定される予定です。

なお、このハッシュ関数の技術詳細は、2009 年 1 月 20 日から滋賀県の大津市で開催されている「2009 年 暗号と情報セキュリティシンポジウム」で発表しました。

*1 ハッシュ関数：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等の安全性基準を満たすことが要求される。
*2 SHA-1：Secure Hash Algorithm-1 の略。米国連邦標準規格 FIPS(Federal Information Processing Standard)180-2 に掲載され、NIST が開発した、160 ビット長の特徴値を出力するハッシュ関数。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。
*3 特徴値：ハッシュ関数の出力する固定長のビット列で、入力データにより一意に定まるランダムな値である。
*4 NIST：National Institute of Standards and Technology の略。米国の商務省下の国立標準技術研究所で政府向けの標準暗号を制定する。
*5 SHA-2：Secure Hash Algorithm-2 の略。FIPS180-2 に掲載され、NIST が開発した、224 ビット、256 ビット、384 ビット、512 ビット長の特徴値を出力するハッシュ関数。高速性に長けているが、SHA-1 の構造を踏襲して設計されているため、安全性については不明な点が多いとの指摘がある。SHA-3(Secure Hash Algorithm-3)は、SHA-2 に続く標準のハッシュ関数になる予定である。
*6 コンペティション：NIST が主催する次世代のハッシュ関数を選定するプロジェクトで、正式には「Cryptographic Hash Algorithm Competition」。選ばれたハッシュ関数は 2012 年に SHA-3 として FIPS に掲載され、全世界で利用されることになる。
*7 攪拌：関数に入力されたデータをランダムなデータへと変換すること。
*8 日立では、この他に、独立行政法人情報通信研究機構（理事長：宮原 秀夫）からの委託研究「次世代ハッシュ関数の研究開発」において、国立大学法人福井大学、国立大学法人神戸大学と共同で別方式を開発し、SHA-3 コンペの候補として認定されている。

■お問い合わせ先

株式会社日立製作所　システム開発研究所　企画室　[担当：塚越]
〒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

このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL 等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性もありますので、あらかじめご了承ください。
