2005年1月28日
株式会社日立製作所

日立ストリーム暗号方式が国際標準へ
大容量データの高速暗号化を容易に

日立製作所システム開発研究所(所長:小坂満隆／以下、日立)は、高速ストリーム暗号[1)]MUGI(TM)[2)]と暗号運用モードMULTI-S01[3)]を独自開発し、国際標準化機構ISOに標準化を提案していましたが、このたび、これら2方式ともにISOでの技術的審査が終了し、ストリーム暗号としては初のISO標準となることが確定しました。

ユビキタス情報社会の伸展に伴い、データ通信装置やハードディスク装置が急速に小型化される一方で、それらが扱うデータサイズは飛躍的に大きくなっています。こうした大規模なデータの処理形態は、Web上などのコンテンツ等で使用されるオンデマンド処理から、バーチャルオフィスやテレビ会議システムを実現するリアルタイム処理へと発展しつつあり、画像処理や信号処理の速度、質、量の向上が求められています。同時に、情報ネットワークで支えられる社会においては、取り扱う情報のセキュリティ確保が重要な技術課題となっており、その解決策として暗号技術が用いられています。その中の代表的な技術であるストリーム暗号は、ランダムなデータストリームを発生する擬似乱数生成器を使って暗号化を行う方式で、ブロック暗号[4)]と比べて小規模での実装が可能であり小型機器への搭載が容易なこと、ビット単位処理が容易であることなどのメリットがあり、携帯電話やBluetooth(TM)などの無線通信区間暗号として採用されています。しかし、ストリーム暗号の工業会における標準化体制は十分ではなく、世界中の暗号研究者の評価にも耐える安全かつ高性能なストリーム暗号の実現が望まれていました。

このような背景から、日立では、ストリーム暗号の改良技術としてMUGI(TM)とその暗号運用モードであるMULTI-S01を開発するとともに標準化への提案をしてきました。その結果、2003年4月に電子政府推奨暗号に認定され、このたび、ISO標準に認定されることが確定しました。本方式の特長は以下の通りです。

(1) 実績ある暗号技術採用による安全性確保:

MUGIの開発においては、実績あるAES[5)]の安全性評価結果に着目し、国内の暗号方式としては初めてAESの部分関数を使うなど安全性の施策を施しました。国内標準化活動を通じて多くの安全性評価結果が得られ、高い安全性を持つことが示されました。

(2) サイズ-処理速度トレードオフによる劇的な処理速度の高速化:

MUGI(TM)は、ブロック暗号に比較して、よりサイズの大きな内部状態(乱数表)をもつことで、計算スループットを劇的に向上することに成功しました。Intel(R)社製Pentium(R) 4プロセッサでは、実質暗号処理がギガビットレートを達成します。また、カスタムLSIの場合、0.18ナノメートルのプロセスで、毎秒10ギガビット超のスループットを達成します。

(3) 証明可能な改ざん検知手法の開発:

従来のストリーム暗号では、擬似乱数生成機能によって生成された乱数をメッセージに単に排他的論理和で加算するという暗号運用モードを適用することで暗号文を生成していました。この方式はデータ秘匿性が保証されます。しかし、この方式では、例えば、通信途中の暗号文の 1 箇所を変化させると復号文の同じ箇所も変化し、かつ変化したことは検知されませんでした。この問題に対し、MULTI-S01 では、加算と乗算を併用したシンプルな工夫を施すことにより、暗号学的な誤り検出機能をも実現できることを発見しました。これにより、データ秘匿とデータ改ざん検知が安全に行われることが保証されたストリーム暗号を提供することが可能になりました。

MUGI(TM)の設計にあたっては基本的な安全性に関する部分部品は AES の部品を用いましたが、MUGI 全体における広域的な攪拌では従来の設計にとらわれない新規の構造から検討しました。これらの安全性評価には、2001 年より開始したルーベン大学[6]との共同研究の結果を踏まえています。これにより、近年のプロセッサ上で可能な限り効率的かつ効果的にデータを攪拌することに成功し、安全性の高い高速なストリーム暗号を一般的に実用化できる道を拓きました。

本技術は、株式会社日立国際電気が 2005 年に同社の映像監視用システムに組み込んで製品化する予定です。また、今後、日立製作所、および、日立グループの製品・サービス群に展開していきます。

なお、本内容に関して、2005 年 1 月 25 日から 28 日までの 4 日間の日程で、神戸で開催される「暗号と情報セキュリティシンポジウム SCIS2005」で発表しました。また、2005 年 3 月 21 日から 24 日までの 4 日間の日程で、大阪府で開催される「電子情報通信学会総合大会」において、発表する予定です。

■用語解説

1）ストリーム暗号:

ランダムなデータストリームを発生する擬似乱数生成器を使って暗号化を行う方式をストリーム暗号といいます。ブロック暗号と比べて小規模での実装が可能であること、ビット単位処理が容易であること、などのメリットがあり、携帯電話や Bluetooth(TM)などの無線通信区間暗号としてストリーム暗号が採用されている。暗号処理効率の面から見れば、一般にストリーム暗号はブロック暗号よりも優れており、これからの高度情報網社会での利用増が期待される。ISO では初めてのストリーム暗号標準 ISO18033-4 の最終案 FDIS(Final Draft International Standard)に、日本の MUGI(TM)と MULTI-S01、および、スウェーデンの SNOW 2.0 が入り、実質的に標準化が確定しました。

2)）MUGI(TM):

大容量のデータを暗号化･復号化するにあたり高速処理が可能な暗号方式です。MUGI(TM)を用いることによって、64 ビットプロセッサや 32 ビットプロセッサ、ならびに専用 LSI による処理で、本来の安全性の高さに加え大容量の処理が軽負荷･低コストで実現できるようになりました。例えば、映像データ DVD 1 枚分(4.7GB)をパソコン（Intel(R)社製 Pentium(R) 4 2 GHz プロセッサ）

のソフトで暗号化あるいは復号化する場合、処理に要する時間(ディスクアクセス時間を除く)は約 36 秒です。また、専用チップを用いる場合は、小規模回路(46K ゲート)で約 3 秒と、高速な暗号処理を達成しました。

3)MULTI-S01:

従来のストリーム暗号がデータ秘匿機能しかなかったのを、データ改ざん検知機能をも併せて持つようにした暗号運用モードで、オプションとして MUGI(TM)などの擬似乱数生成機能と組み合わせて用いることができます。これにより、電子取引データなど、1 ビットでも違えては困るデータを通信したり蓄積する場合に、データを不当に改ざんされたとしても瞬時に検出することを可能にしました。

4)ブロック暗号:

暗号処理などの安全性のよりどころとなる部品関数の名前。具体的には、鍵入力(通常 128 ビット程度)をパラメータとしながら、固定長(通常 128 ビットなど)の入力を鍵に依存しながらランダムな出力となるよう変換するもの。入出力のペアから鍵入力が逆算されない、などの暗号強度に関する性質がいくつかあります。

5)AES(Advanced Encryption Standard):

米国次世代暗号標準。2001 年 11 月に NIST(National Institute of Standards and Technology, 商務省技術標準局)が、FIPS(Federal Information Processing Standards, 商務省連邦情報処理規格)に FIPS PUB. 197 として登録したブロック暗号。ブロック長 128 ビットで、鍵長は 3 種類の鍵長、128, 192, 256 ビットが利用可能です。

6)ルーベン大学:

ベルギー最大の大学(学生数 29,000 人)。1425 年創立。ルーベン大学の暗号研究グループ(代表プレネール教授)は現在の米国暗号標準 AES を開発したことで有名です。

■本件に関する照会先

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

以上