2006年3月16日

日立の公開鍵暗号「HIME(R)[ハイムアール]」がISO国際標準規格に採用

株式会社日立製作所(執行役社長：庄山 悦彦／以下、日立)が提案していた、高い安全性があり、省電力性に優れた暗号技術(1)である公開鍵暗号「HIME(R)(読み方：ハイムアール)」が、このたび、ISO(国際標準化機構)/IEC(国際電気標準会議)18033「暗号アルゴリズム」標準化プロジェクト(2)での投票の結果、ISO 国際標準規格に採用されました。すでに国際標準規格に採用されている共通鍵暗号ストリーム方式(3)の「MUGI(4)」、「MULTI-S01(5)」とあわせて、日立からは、一つの企業からとしては世界最多の3方式が、暗号技術の国際標準規格に採用されたことになります。

ユビキタス情報社会の進展に伴い、パソコンや携帯電話などの情報機器を用いた商取引やデータの送受信、各種申請などを行う機会が増えています。しかしながら、通信中の情報漏えい、第三者による成りすまし、権限のない者による情報アクセスや情報改ざんなどの問題があり、情報を安全にやり取りするには、情報の機密性や正確性の維持、アクセス者の本人証明を行うことが必要となります。すでに、個人情報保護法の施行や、企業の内部統制強化に向けた日本版SOX法の検討など、情報漏えい防止や情報の信頼性向上に向けた法制度の整備も進められています。このような社会の要請に対応するため、通信中やパソコン等に蓄積されたデータの盗み見や改ざんを防止し、機密性と証拠性を確実に保全できる暗号技術が開発されていますが、より強固な安全性を確保するため、比較的大きなサーバやパソコンだけでなく手軽に持ち運べるような情報機器にも、使用可能な省電力かつ高速な暗号技術が求められてきました。

日立は、1988年にマルチメディア向け高速暗号技術として共通鍵暗号「MULTI2」を開発し、1994年に「MULTI2」が郵政省電波審議会において日本におけるデジタル衛星放送用標準暗号として採用されるなど、暗号技術分野における経験と実績を有しています。その後開発した共通鍵暗号ストリーム方式「MUGI」、「MULTI-S01」も2003年4月に電子政府推奨暗号に指定され、2005年7月には、ISO/IEC 18033 Part 4 にて、国際標準規格に採用されています。今回、「HIME(R)」が ISO 国際標準規格に採用されたことから、日立からは、一つの企業からとしては世界最多の3方式が、暗号技術の国際標準規格に採用されたことになります。

高い安全性と省電力性・高速性を併せ持つ公開鍵暗号「HIME(R)」の特長は次の通りです。

(1) 安全性証明可能な暗号方式：
「HIME(R)」は、公開鍵暗号の安全性理論において最強とされる安全性レベルを有しています。このため、非常に強力な攻撃者であっても、暗号文から元データの一切の部分情報を引き出すことが困難です。また、標準化活動などを通じて多くの安全性評価・検証結果が得られており、安全性証明の正しさも客観的に保証されています。

(2) 省電力性・高速性：
「HIME(R)」の暗号化は、メッセージに対し、OAEP 法(6)と呼ばれるパディング(7)を施し、その後、平方剰余算(8)を一回行うだけで実施されます。これらの操作は極めて簡潔で高速性に優れています。
また剰余乗算における法(合成数)(9)の形を工夫し、復号化の高速処理も達成しました。RSA暗号に比べ、同じ鍵長の場合、暗号化で約10倍、復号化で2～3倍の高速処理性能を発揮します。処理性能向上は消費電力を抑えることに直結し、ユビキタス端末でも動作可能です。

ユビキタス情報社会では、機器の扱うデータサイズは大きくなる一方で、機器の小型化、省電力化が重要な技術課題となっていますが、日立ストリーム暗号「MUGI™」や「MULTI-S01」はこれら課題

を解決し、ユビキタス向け小型端末間でも大切なデータを安全に送信することを可能にしました。今回、国際標準規格に採用された「HIME(R)」についても、高速かつ省電力での処理が可能であることから、このような小型機器でも「MUGI(TM)」や「MULTI-S01」とのハイブリッド型で利用可能です。

日立ではこれらの省電力暗号系を駆使してユビキタス情報社会の安全性を提供する技術を研究し、その技術を日立および日立グループの各種製品に展開していきます。

日立暗号「HIME(R)」、「MUGI(TM)」、「MULTI-S01」の仕様や性能評価結果などの詳細情報は下記ホームページで公開しています。
http://www.sdl.hitachi.co.jp/crypto/index-j.html

■用語解説

1) 暗号技術

暗号技術は一般に、共通鍵暗号技術と公開鍵暗号技術に分類される。共通鍵暗号技術は、特殊な「鍵」を使用してデータを暗号化するが、暗号化に使用する鍵と復号化に使用する鍵が同じであることから、データの送受信者の双方が、何らかの手段で安全に鍵を共有する必要がある。この鍵共有問題を解決したのが公開鍵暗号技術である。

公開鍵暗号技術は、暗号化に必要な鍵(暗号化鍵)と暗号化されたデータの復元に使用する鍵(復号化鍵)が異なっており、データの受信者が復号化鍵を秘密にしておけば、暗号化鍵を公開しても安全性を確保できる暗号方式である。受信者は、自分の暗号化鍵をインターネット上に公開し、送信者はその鍵を使用して送信データを暗号化し、受信者は自分の復号化鍵により復号する。しかし、暗号化および復号化に使用する鍵が異なることから、公開鍵暗号方式はその暗号・復号化プロセスが複雑であり、共通鍵暗号方式に比べるとやや処理速度が遅いという問題があり、大容量のデータの暗号化は共通鍵暗号で行い、その暗号化鍵(＝復号化鍵)を公開鍵暗号で暗号化して送信する、ハイブリッド型で用いるのが一般的である。

2) ISO/IEC 18033「暗号アルゴリズム」国際標準化プロジェクト

国際標準の規格書は、Part 1:「総論」、Part 2:「公開鍵暗号」、Part 3:「ブロック暗号」、Part 4:「ストリーム暗号」の4部からなる。1999年に活動を開始、公募により集まった種々の暗号アルゴリズムを専門家で構成される委員会で審議し、2005年3月1日 にPart 1、2005年7月15日にPart 3と4 が発行された。Part 2は2006年2月に最終投票が終了し、2006年内に発行される予定となっている。

3) 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である。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採用されている。暗号処理効率の面から見れば、一般に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ている。

4) 「MUGI(TM)」

大容量のデータを暗号化・復号化の高速処理が可能な暗号方式。「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る。例えば、映像データ DVD1 枚分(4.7GB)をパソコン（Intel(R)社製Pentium(R) 4.2GHz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秒である。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ている。

5)「MULTI-S01」
従来のストリーム暗号がデータ秘匿機能だけであったのを、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る。これにより、電子取引データなど、1 ビットでも間違うことのできないデータの通信や蓄積を行う場合に、データを不当に改ざんされた場合も瞬時に検出することが可能。

6) OAEP 法
OAEP 法は、公開鍵暗号の安全性強度を向上させるためのデータ処理方法のことであり、実際には、メッセージを入力して、パディング(7)を施し、その後、平方剰余算(8)を一回行うだけで実施される。これらの操作は極めて簡潔で高速性と安全性に優れている。

7) パディング
メッセージが入力されたとき、別のデータをそのメッセージにくっつける処理のこと。

8) 平方剰余算
整数 n に対し、整数 x の 2 乗 x^2を、n で割ったときの余りを「$x^2 \bmod n$」と書く。このような演算を平方剰余算といい、このときの n を法という。

9) 剰余乗算における法(合成数)
整数 n に対し、整数 x、y の乗算 x・y を、n で割ったときの余りを「x・y mod n」と書く。このような演算を剰余乗算といい、このときの n を法という。特に、RSA や HIME(R)の計算では、n は合成数、つまり、複数個の素数の積が用いられる。

■他社商標等
Bluetooth(TM)は、アメリカ合衆国における Bluetooth-SIG Inc.の商標または登録商標です。
Intel(R)および Pentium(R)は、アメリカ合衆国ならびにその他の国におけるインテル コーポレーションまたはその子会社の商標または登録商標です。
RSA は、RSA Security Inc.の登録商標です。
MUGI(TM)は、日本における株式会社日立製作所の登録商標です。

■略語
ISO : **I**nternational **O**rganization for **S**tandardization
HIME(R) : **Hi**gh Performance **M**odular-squaring-based public-key **E**ncryption (**R**evised Version)
MULTI-S01 : **MULTI**media encryption algorithm, **S**tream cipher No.**01**
MUGI : **Mu**lti **Gi**ga cipher

■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：森］
〒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