2004 年 8 月 23 日
株式会社日立製作所

楕円曲線暗号の高速化･省メモリ化を実現する計算手法の開発に成功
モバイル機器への搭載を可能に

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、このたび、安全性の高い楕円曲線暗号[*1)]の高速化を実現する新しい効率的な計算方法を開発し、携帯電話などのモバイル機器への搭載への道を拓きました。本手法は通常の楕円曲線暗号だけでなく、メールアドレスを直接暗号化鍵として用いることのできる ID ベース暗号などにおいても、省メモリ･低消費電力で高速な暗号･署名処理を行なうことが可能となります。

ユビキタス社会において、ますますニーズが高まるモバイル情報端末機器では、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います。情報セキュリティの確保には通常暗号技術が用いられますが、小型軽量で低消費電力が要求されるモバイル情報端末機器においては、効率的な暗号技術実装を行なう必要があります。種々の暗号の中で楕円曲線暗号は、短いビット長で高い安全性を達成できるため、モバイル情報端末機器への実装に向いています。しかし、これを実際にモバイル情報端末機器に搭載する場合には、限られたメモリ使用量で高速暗号計算をする技術の開発が必要でした。

このような背景から、日立では、楕円曲線暗号の高速化技術として MOF (Mutual Opposite Form、相互交代形式)[*2)]を開発しました。MOF 技術の特長は以下の通りです。

(1) 符号化バイナリ表現による高速化：
従来の 0 と 1 のみを用いるバイナリ表現から、0,1,-1 の 3 値を用いる符号付バイナリ表現を採用しました。これによって、計算機が行なう演算を効率化し、楕円曲線暗号の高速化を実現できます。

(2) 楕円曲線暗号向け符号化バイナリ計算：
現在の符号化バイナリ表現を用いた計算は最下位ビットから変換しますが、新たに最上位ビットから変換する計算手法を開発しました。これによって、アルゴリズムの特性から最上ビットから変換する必要がある楕円曲線暗号の符号化バイナリ表現による計算を世界ではじめて実現しました。

最上位ビットから変換する手法は、計算機科学分野において長年の間、未解決問題として知られているもので、今回この問題を解決したことは学術的な意味合いからも大きな影響を与えるものです。開発した MOF 技術を用いることにより、高速な楕円暗号処理を行なうことが可能となります。これによって、限られたメモリ容量のモバイル情報端末機器においても、安全性の高い楕円曲線暗号を搭載する道を拓きました。

なお、本開発技術の一部はドイツのダルムシュタット工科大(学長：ヨハン・ヴェルネル)*3)との共同研究によるものです。また、本内容に関して、2004年8月15日から19日までの5日間の日程で、米国サンタバーバラで開催されるCRYPTO2004国際会議において、発表する予定です。

■用語解説

*1）楕円曲線暗号：

楕円曲線上の演算規則を利用した新しい公開鍵暗号技術。暗号強度を確保しつつ、短い鍵長で高速にデータを暗号化できるため、次世代公開鍵暗号として注目されています。ECDSA（Elliptic Curve Digital Signature Algorithm）は、楕円曲線暗号による電子署名のアルゴリズムであり、ISO等でも推奨暗号として選定されています。

*2）MOF技術：

MOF表現とは符号付バイナリ列の一種で、0値ビットを除くと符号が反転しているものです。バイナリ列からMOF表現への変換は、バイナリ列を2倍しビットごとに元のバイナリ列を引くことにより得ることができます。またMOF表現を左から順に $1\dot{1}\rightarrow 01$, $\dot{1}1\rightarrow 0\dot{1}$ と変換することにより変換MOF表現となります。ただし、$\dot{1}$は-1を示しています。変換MOF表現は非0ビットの数が最小となります。楕円曲線暗号では非0ビットは楕円基本演算を行なうことに相当するため、変換MOF表現を用いることにより楕円基本演算の回数を削減でき、暗号処理を高速化することができます。

例：

10進 2393 =	[バイナリ列]	101101101111	(a)
	[2倍化]	1011011011110	(b)=(a)×2
	[MOF表現]	$1\dot{1}10\dot{1}10\dot{1}1000\dot{1}$	(c)=(b)-(a) ビットごとの引き算
	[変換MOF表現]	$01100\dot{1}00\dot{1}000\dot{1}$	(d) $1\dot{1}\rightarrow 01$, $\dot{1}1\rightarrow 0\dot{1}$
	($\dot{1}$ = -1)		

(a)では非0ビットの数は9個ですが、(d)では5個に削減されています。

*3）ダルムシュタット工科大：

ドイツ最大規模の総合技術大学の一つとして知られています。1826年創立。ドイツ高等教育機構より、ドイツ242大学の中から「best practice price 2001」を受賞しました。

■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