2005 年 7 月 4 日

専用演算器が不要な小型マイコン向け暗号実装技術を開発
電子署名で用いる楕円曲線暗号のＩＣカードやＵＳＢメモリへの実装を容易に

株式会社日立製作所システム開発研究所（所長：前田章、以下：日立）は、このたび、モバイル機器や IC カードなどで利用されている小型マイコン上で、暗号専用演算器なしで動作する次世代公開鍵暗号技術を開発しました。本技術は、電子署名法で指定されている楕円曲線暗号[*1)]のうちでも“コブリッツ曲線”と呼ばれる種類の楕円曲線を用い、日立が独自開発した安全性の高い実装技術である wNAF[*2)]を、コブリッツ曲線に対応させたものです。同じく電子署名法で指定されている RSA 暗号と比べて、暗号専用演算器なしで速度低下なく同等以上の安全性を実現します。

本技術によって、普及型廉価チップを用いた高強度（住民基本台帳用 IC カード並）認証を実用速度で行うことが可能となり、最近、クレジットカードなどで頻発している磁気カード偽造対策として IC カードへの置き換えや、ネット犯罪対策としてパソコンに差し込んでネット認証を行う USB 認証チップなどに用いることができます。

日立では、本技術を、近い将来のユビキタス情報社会において大きな脅威となり得る IC カードのスキミング行為にも一定の耐性があり、低コストで実現可能なデジタル署名技術と位置付け、今後、本成果を小型マイコン向けの暗号ライブラリ、ないしは暗号チップとして提供することを計画しています。

ユビキタス情報社会では、携帯端末や設備機器など身の回りの機器が情報処理能力を備え、相互に情報を通信します。これらの機器において、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、特に、端末や設備機器などの“実行時間や電力消費量、漏洩電磁波”等物理情報を利用して、機器内部に格納されている秘密情報を調べる攻撃手法である実装攻撃に対する対策が求められています。そのため、近年、暗号技術を適用する際に、アルゴリズムレベルでの安全性だけでなく、暗号技術の実装方法の安全性が重要であるとの認識が高まっています。

一般に、コンピュータが暗号処理を実行する際には、秘密情報に応じて処理を振り分けるという特徴があります。例えば秘密情報のあるビットの値が 0 の場合には 0 に対応する処理を行い、1 の場合には 1 に対応する別の処理を行う、そしてそれらの処理を繰り返すことにより暗号処理を行っています。実装攻撃は、そういった暗号処理を、計算時間や電力消費量、電磁波などを計測することにより推測し、それにより秘密情報を特定します。秘密情報のビットの値が 0 であれば 0 に対応する処理が実行され、その処理に対応する電力消費波形が観測されます。1 であればそれとは異なる電力消費波形が観測されます。したがって、電力消費波形を形状により分類することにより、対応する秘密情報を特定できます。

日立では、実装攻撃を回避する暗号実装技術として、wNAF（Width-w Non-Adjacent Form）という楕円曲線暗号の計算手法を開発し、2003 年 4 月に米国で行なわれた RSA カンファレンス[*3)]及び 2003 年 9 月にドイツで行なわれた CHES 国際会議[*4)]で発表しています。wNAF では、秘密情報のビットの値によらず、秘密情報の表現形式の変換を行って、常に一定の処理を行うことにより、実装攻撃を回避します。通常、秘密情報は 0、1 の 2 値を用いて表されますが、これを、－1 も用いる表現に変換します。その後、適当な幅のブロックに区切り(例えば 3 ビットごと)、それらのブロックの表現を 00…0x (ただし x は非 0 値)といった形式に変換します。これにより、どんな秘密情報に対しても、00…0x という固定されたパターンが繰り返されることになり、常に一定の処理を行うことが可能となりますが、より高い安全性を確保するためには、暗号用の専用演算器が必要です。

しかし、IC カードのように、より低コストでの製造・運用が求められるアプリケーションにおいて、暗号用の専用演算器を準備することは、コスト的な観点から見て非常に難しいことから、日立では wNAF の基本コンセプト

を生かしながら、専用演算器を必要としない手法の開発を進めてきており、今回、あらたな暗号実装技術を開発したものです。

今回開発した技術の特長は、以下の通りです。

(1) 楕円曲線暗号（コブリッツ曲線）を利用：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、小型マイコンへの実装に向いています。その中でもコブリッツ曲線と呼ばれる楕円曲線を用いることにより、さらなる高速暗号計算を達成できます。
(2) τ倍算の利用：コブリッツ曲線ではτ倍算と呼ばれる特殊な演算が利用可能です。τ倍算の計算は、対象データをローテートすることにより達成できるため、専用演算器を必要としません。
(3) 耐タンパwNAF法を拡張：実装の安全性を備えた実装技術wNAFを、コブリッツ曲線へと拡張することに成功し、これにより実装の安全性を達成しました。

なお、本内容に関しては、2005年7月4日から6日までの3日間の日程でオーストラリアのブリズベンで開催されるACISP2005 国際会議(Australasian Conference on Information Security and Privacy)において、発表する予定です。

■用語説明

＊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る。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、CRYPTREC（総務省および経済産業省が行なった、電子政府における調達のための暗号評価プロジェクト）等でも推奨暗号として選定されている。

＊2 wNAF：
Width-w Non-Adjacent Form の略。楕円曲線暗号の計算方法の一つ。wNAF 法の基本アイデアは、秘密鍵の表現を従来の0と1の2値によるものから、0,1,-1の3値を用いた表現へと変換し、この表現をもとにしてブロック毎に00…0x (ただしxは非0値)という固定されたパターンから成る表現へと変換するというもの。2003年4月に米国で行なわれたRSAカンファレンスで発表。

＊3 RSA カンファレンス：
2003年4月13日から5日間の日程で、米国サンフランシスコで開催された国際会議。セキュリティ関連の国際会議のうち、最も大きいものの一つであり、参加者は1万人以上。

＊4 CHES国際会議：
2003年9月7日から4日間の日程でドイツのケルンで開催された暗号実装技術に関する国際会議

■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