2004年8月6日
株式会社日立製作所

モバイル機器向け省メモリ・低消費電力のディジタル署名技術を確立
電力消費量や電磁波などからの情報漏洩に対する実装の安全性を証明

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、携帯電話などのモバイル機器に組込み可能で、既存の署名技術より安全性が高い、次世代ディジタル署名技術を確立しました。本技術は、実行時間や電力消費量、漏洩電磁波等の情報を利用して、モバイル機器内部に格納されている、秘密情報を調べる攻撃から回避する機能を備えた、省メモリ・低消費電力で高速なディジタル署名の実装技術です。

現在、急速に普及、利用が拡大している、携帯電話をはじめとするモバイル機器では、通信相手の真正性を確認するために、ディジタル署名などを利用した認証処理が行なわれています。しかし、これに対して、実行時間や電力消費量、漏洩電磁波などの物理情報を利用して、モバイル機器内部に格納されている秘密情報を調べる攻撃手法が脅威となっています。そこで、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[*1)]。しかし、アルゴリズムと実装の安全性を同時に兼ね備えた暗号技術をモバイル機器に搭載する場合には、ソフトウエアや実装に新たな負荷が加わるために、速度低下やメモリ使用量・消費電力の増大が生じることが実用上の課題となっていました。

このような背景から、日立では実装の安全性に配慮し、省メモリ・低消費電力で高速なディジタル署名実装技術 wNAF[*2)] を開発してきました。日立の wNAF 技術の特長は、署名処理を行なう際に、実装の安全性を確保するとともに、アプリケーションの状態に応じて処理速度や使用メモリなどを常に最適な状態にカスタマイズできる点です。しかし、このような特長を用いて、今後、wNAF 技術をモバイル機器へ適用するためには、理論的な安全性を明らかにし、最適条件の指標を得る手段を確立する必要がありました。

今回、この wNAF 技術をモバイル機器に実装した場合の安全性について理論的な検証を行なった結果、以下の成果が得られました。

(1)表現選択を行なう部分に焦点をあて、変換後の表現の分布に関して統計的な解析を行ないました。その結果、ある種のケースでは分布の偏りが存在することが判明しましたが、計算手法を若干修正することで偏りがなくなることを示しました。

(2)最適状態選択のための指標を確立し、最適なパラメータ設定を容易に行なうことができます。また、モバイル機器実装時における安全性について理論的な検証を行ない、最適状態選択のための指標を確立しました。これにより、本技術の導入がさらに容易となります。

本成果は、物理情報からモバイル機器の秘密情報を調べる攻撃を回避する機能を備えた、省メモリ・低消費電力で高速なディジタル署名の実装技術の実現に道を拓くものです。

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、本内容は、2004年7月13日から15日までの3日間の日程で

オーストラリアのシドニーで開催された ACISP2004 国際会議(Australasian Conference on Information Security and Privacy)において、発表されました。

■用語説明

＊1) 実装の安全性：
ISO や CRYPTREC[*4] においても、今後は暗号アルゴリズムの「実装の安全性」の評価が重要であるとの認識のもと、その評価項目や評価基準制定のための検討を進めています。

＊2) wNAF：
Width-w Non-Adjacent Form の略。楕円曲線暗号[*5] の計算方法のひとつで、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、必要に応じて最適な表現を選択するというものです。2003 年 4 月に米国で行なわれた RSA カンファレンス[*6]、及び 2003 年 9 月にドイツで行なわれた CHES 国際会議[*7] で発表しています。

＊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 年創立で、ドイツ高等教育機構より、ドイツ 242 大学の中から“best practice prize 2001”を受賞しました。

＊4) 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で、2003 年度に暗号モジュール委員会を設立し、実装安全性の評価基準選定等を進めています。

＊5) 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、CRYPTREC 等でも推奨暗号として選定されています。

＊6) 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 万人以上です。

＊7) CHES 国際会議(Workshop on Cryptographic Hardware and Embedded Systems 2003)：
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国際会議で、暗号実装技術に関する権威ある国際会議です。

■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