2003年9月19日
株式会社日立製作所

モバイル機器への搭載に最適なディジタル署名技術の開発に成功

株式会社日立製作所システム開発研究所（所長：小坂満隆）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の開発に成功しました。本技術により、モバイル機器において小メモリ・低消費電力で高速な署名処理を行なうことが可能です。

現在、携帯電話をはじめとして、多くの携帯電子端末（モバイル機器）が普及しつつあります。それら端末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を行ないます。個人レベルにおいても秘密情報の安全性に対するニーズが高まっている市場環境の中で、モバイル機器へディジタル署名を実装した場合、実行時間や電力消費量、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暴き出す攻撃手法が知られており、脅威となっております。そのため、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。実際に、ISOやCRYPTREC（＊1）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下に、その評価項目や評価基準制定のための検討を進める予定となっております。

昨今では、携帯電話などのモバイル機器には複数のアプリケーションが搭載されるのが一般的となってきています。既存方式による署名処理では、署名処理専用にリソースを割り当てる必要があったため、アプリケーションの追加や削除によりパフォーマンスの低下を招いていました。また、実装の安全性に対して配慮を行なった場合、速度低下やメモリ使用量・消費電力の増大といった事態が引き起こされました。そのため、モバイル機器に最適なディジタル署名技術の開発は重要な研究開発課題となっています。

このような背景から、当社システム開発研究所では、実装の安全性に配慮し、そのうえ小メモリ・低消費電力で高速なディジタル署名技術を開発しました。

本技術のポイントは次のとおりです。つまり、実際に暗号を生成する場合、単に、コンピュータ上で標準書通りのアルゴリズム（数式）を実行するだけでは不十分な場合が生じます。例えば、従来、高速優先処理を行なう場合、秘密鍵(例えば、110･･･101）のビットを一つ一つ取り出して、計算を実行していました。しかし、これでは、1を処理するときの電力消費量と0を処理するときの電力消費量が異なってしまい、電源パワー供給部に端子を当てて電力消費量パターンを計測することにより、秘密鍵が分かってしまいます（電力解析攻撃）。一方、安全優先処理として、関係のない計算を適宜入れることで電力消費量パターンを撹乱する方法が、従来、提案されていました。しかし、この方法では、逆に、従来の高速優先処理に比べて処理時間や消費電力が4倍ほ

どかかってしまい、IC カードやモバイル端末での利用はあまり好ましくありませんでした。そこで、本方式では、秘密鍵の表現を、従来の 0 と 1 の 2 進法に変えて、0 と 1 と-1 の 3 値を用いる方法に変えたうえで、毎回の電力消費パターンがうまく撹乱される方法を開発し適用しました。その結果、従来の安全優先処理と同じ安全性を実現しながらも、従来の高速優先処理に比べても処理時間や消費電力をほぼ同等に抑えることに成功しました。なお、この電力解析攻撃以外にも、処理時間を計測されることによるタイミング解析攻撃等、種々の実装攻撃に対しても本方式は有効に働きます。

新技術を用いると、署名処理を行なう際に、実装の安全性を確保でき、さら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ます。尚、本技術の一部アイデアは、2003 年 4 月に米国で行なわれた RSA カンファレンス（＊2）で wNAF（＊3）という方式名で発表し、好評を得ました。今回、モバイル機器実装時に占有されるメモリ量を最大 50%まで低減できるようにさらに改良し、有効性を大幅に向上させたものです。

今後は、本開発技術を、需要が高まると予想される楕円曲線暗号の種々の実装において採用していくことを検討しています。

尚、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）（＊4）との共同研究によるものです。

尚、本内容に関して、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る CHES2003 国際会議（Workshop on Cryptographic Hardware and Embedded Systems 2003）において、発表する予定です。

■用語解説

＊1　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。2003 年度より暗号モジュール委員会を設立する。

＊2　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。

＊3　wNAF　Width-w Non-Adjacent Form の略。楕円曲線暗号（＊5）の計算方法の一つ。

＊4　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る。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」を受賞した。

＊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 等でも推奨暗号として選定されている。

■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

このニュースリリースに掲載されている情報は、発表日現在の情報です。
発表日以降に変更される場合もありますので、あらかじめご了承ください。
