2004 年 6 月 11 日
株式会社日立製作所

公開鍵暗号を搭載したモバイル機器の高速･高セキュリティ実装技術を開発
計算時間や電力消費量、漏洩電磁波などによる秘密情報の特定を防御

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、公開鍵暗号基盤＊1)などで広く利用されているRSA暗号＊2)を、モバイル機器やICカードなどに搭載し利用した場合に、脅威となるサイドチャネル攻撃に強い実装手法を開発しました。本技術により、携帯電子端末やICカードにおける暗号･署名処理を安全かつ高速に行なうことが可能です。

現在普及が進んでいる、携帯電話をはじめとするモバイル機器へ、公開鍵暗号を実装した場合、計算時間や電力消費量、漏洩電磁波などにより、秘密情報を特定するサイドチャネル攻撃と呼ばれる攻撃手法が知られており、情報セキュリティの新たな脅威となっています。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*3)。

一方、公開鍵暗号の代表的な暗号である RSA 暗号では、その高速化手法として、中国人剰余定理と呼ばれる数学理論を用いる手法があります。これは、暗号演算を複数の処理に分解して計算を行ない、それらの結果を結合して最終結果とする計算方法で、通常の計算方法と比べて数倍の高速化を達成できることが知られています。しかしながら、部分演算結果を結合するステップにおいて、実装安全性を担保することが難しいという課題がありました。そのため、公開鍵暗号を携帯情報端末に実装する上で、実装安全性と高速性の両立が、重要な研究開発課題となっていました。

このような背景から、今回、日立は中国人剰余定理を用いて高速化を行なう場合においても、サイドチャネル攻撃に対して安全となる実装方法を開発しました。暗号文を復号化する場合の、本技術のポイントは以下の通りです。

(1) 暗号文のランダム化（暗号文 C→ランダム化暗号文 C'）
暗号文をランダム化した暗号文に変換します。この変換はランダムデータにより暗号文をマスクすることにより達成されます。これによりサイドチャネル攻撃を実行不可能とします。ただし、最終ステップでのランダム化解除を容易とするために、ランダムデータ自身も暗号化して用います。

(2) 高速手法による復号化（ランダム化暗号文 C'→ランダム化復号文 M'）
ランダム化した暗号文を、中国人剰余定理を利用した高速復号化手法を用いて復号化します。復号化結果はランダム化された復号文となります。

(3) ランダム化の解除（ランダム化復号文 M'→復号文 M）
ランダム化復号文のランダム化を解除します。このランダム化の解除は、最初のランダム化変換方式を効果的に行なっているため、高速に行なうことができます。ランダム化の解除により、安全かつ高速に復号文を得ることができます。

本方式を用いることにより、中国人剰余定理を利用した高速処理とサイドチャネル攻撃の安全性を両立することが可能となります。今後、日立は本開発技術を、RSA 暗号の実装に採用することを進めていく予定です。

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）*4)との共同研究によるものです。

■用語説明

*1) 公開鍵暗号基盤:
公開鍵暗号とは、暗号化を行なう公開鍵と、復号化を行なう秘密鍵の 2 種類の鍵を用いる暗号方式。公開鍵暗号を利用することにより、ディジタル署名を実現できる。公開鍵暗号基盤は公開鍵暗号技術を利用したネットワーク上のセキュリティ技術基盤において、特に電子証明書を発行・配布するシステムで、ネットワーク上での通信相手の真正性を保証し、安全な通信のために用いられている。

*2) RSA 暗号:
公開鍵暗号方式の一つ。開発者 3 名の頭文字を取って RSA 暗号と命名された。

*3) 実装方法の安全性:
ISO においても、暗号アルゴリズムの「実装安全性」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る。

*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ひとつで 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。

■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