2008 年 9 月 22 日
株式会社日立製作所

世界で初めて、CPUを搭載しないメモリチップ単体で電子署名を実現

メモリカードや電子チケット、カートリッジなどの偽造・改ざん防止が可能に

株式会社日立製作所(執行役社長：古川一夫／以下、日立)は、このたび、世界で初めて、メモリチップ単体に高いセキュリティで真贋を認証する「電子署名」機能を組み込む技術を開発しました。本技術は、メモリチップ本体において、電子署名を生成するための CPU(演算機能)を用いずに認証を行うことができるため、低コストにて既存メモリデバイスのセキュリティを高めることが可能です。具体的には、デジタルカメラ、携帯ゲーム機器のメモリカード、電子機器のカートリッジ、入場券や商品券の電子チケットなど、様々なメモリデバイスに適用することで、偽造・改ざん防止を実現します。

物品や文書が本物であることを証明する場合に ID、印鑑、署名が用いられるように、ソフトウェアや電子文書の真正性の証明には、「電子署名」が用いられます。電子署名には、作成者の認証とともに、内容が改ざんされない仕組みも必要であるため、通常は、CPU によって所定の演算処理、例えば、数百桁にも及ぶ数値を何百回も繰返し掛け合わせる複雑な演算を実施します。そのため、CPU を持たない従来のメモリデバイス(メモリカード、電子チケットなど)では、電子署名の機能を組み込まずに、シリアル番号などによる識別*1 を用いた真正性の確認が一般的です。また、メモリデバイスに電子署名の機能を付加するために CPU を新たに組み込むことは、メモリデバイスのコスト上昇にもつながることとなります。しかしながら、デジタルカメラや携帯ゲーム機器のメモリカードなど、着脱可能なメモリデバイスが急速に普及し、市場が拡大するなか、メモリデバイスの模造品対策が課題となっていました。

このような背景のもと、日立は CPU を搭載しないメモリチップで、電子署名が実現できる技術を世界で初めて開発しました。今回開発した技術は、署名生成に必要となるデータをあらかじめ暗号化してメモリチップに記録し、同データを適切に組み合わせることで電子署名を生成します。本技術により、高度な演算を必要とする従来の署名方式とは異なり、メモリチップ単体での電子署名の実現が可能です。

日立は、今回、本技術を CHAP*2 方式に用いることで、低コストにて、高いセキュリティが必要とされる用途への認証の適用を可能としました。デジタルカメラ、携帯ゲーム機器のメモリカード、認証トークン、電子機器のカートリッジなどの真贋判定、さらには、入場券や商品券の電子チケットなどの偽造・改ざん防止が可能です。

*1 識別とは、対象物の真贋を判定する作業のことです。一般には、シリアル番号やパスワードなど特定の情報により判定します。シリアル番号やパスワードなどが不正取得された場合は真贋の判定ができなくなります。
*2 CHAP とは、認証方式の一つで、Challenge Handshake Authentication Protocol の省略形です。認証者はチャレンジコードを被認証者に送付し、被認証者はチャレンジコードに対して電子署名を行い、認証者へ返送します。

なお、本技術の一部は、ドイツのダルムシュタット工科大学（学長：ハンス　ユルゲン　プレーメル）との共同研究によるものです。また、本技術の詳細については、2008 年 9 月 23 日から 25 日に韓国の済州島で開催される WISA 2008 国際会議(International Workshop on Information Security Applications)、および 2008 年 10 月 17 日から 19 日に米国のシンシナティで開催される PQCrypto 2008 国際会議（International Workshop on Post-Quantum Cryptography）において発表する予定です。

■開発技術の詳細

⑴ 複製品に対する安全性

装置に着脱されるメモリデバイスが正規のものであることを確かめるために、装置からメモリデバイスにランダムな数値列(チャレンジコード)を送付します。メモリデバイスは、送られてきたチャレンジコードに対して電子署名をして装置側に返送します。メモリデバイスには、あらかじめ暗号化された情報が記録されており、その情報を組み合わせて電子署名を生成します。装置側は、返送された電子署名が正しい場合にのみ、メモリデバイスが正規であると判断します(CHAP 方式)。したがって、複製品では正しい電子署名を生成できないため、認証に成功しません。

⑵ 認証情報の不正取得への対応

第三者が正規品のチャレンジコードに対応した電子署名を不正に取得し、複製品のメモリデバイスに利用した場合においても、確実に検出できます。装置からメモリデバイスに送付されるチャレンジコードは、毎回、ランダムに選択されます。そのため正しい電子署名も毎回異なることとなり、不正取得した電子署名では認証に成功しません。したがって、シリアル番号を用いた識別よりも高い安全性を実現できます。

■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：塚越］
〒215-0013 神奈川県川崎市麻生区王禅寺 1099 番地
電話 044-959-0325（直通）

以　上