岡山大学

PRESS RELEASE

平成２３年１０月２５日

科学技術振興機構 AStep シーズ顕在化ファンド

クラウドコンピューティング時代の認証技術を高度に実現する並列代数計算アルゴリズムの LSI 化

クラウドコンピューティング時代に入り、安全・安心な情報通信を支える情報セキュリティ技術に対する要求はますます高度化し、複雑になっています。それを支える暗号技術、そして暗号技術を実現する複雑な数学的計算は、スマートフォンに代表されるユビキタス端末上で快適に処理される必要があります。本研究グループでは、これを**高速かつ極めてコンパクトな回路規模で実現する暗号計算チップ**を開発しました。従来技術と比較して、**安全強度に対して数十倍のスケーラビリティを一つの計算チップで実現**するもので、様々なセキュリティ製品・システムで活用できます。

暗号の安全強度を 256 ビットから 5120 ビットまで、段階的に調整できる暗号計算処理チップを開発しました。

スマートフォンやクラウドコンピューティングといったキーワードで象徴される現代 ICT 社会では、ユーザや機器・端末を電子的に認証した上でサービスを行うことが当たり前になり、そのための電子認証技術は送受信される情報の安心・安全を確保するために必須のものとなっています。これを実現する公開鍵暗号技術に対する要求は年々高まっており、それを支える複雑な暗号計算は益々その高度化が望まれています（別紙：図１）。

これに対して本研究グループでは、256 ビットから 5120 ビットまで広範な安全強度の要求に対応できる暗号計算チップを、科学技術振興機構 AStep シーズ顕在化ファンドと東京エレクトロン デバイス（株）の協力により開発しました（別紙：図２）。これにより、これまでソフトウェアで処理してきた複雑な計算をより高速に処理することができ、益々大容量化する情報データに対する暗号化や認証の処理を、より高速に処理できるようになります。開発したチップは、暗号計算を高速に処理できる一方で、その回路規模は極めてコンパクトとなっており、様々なユビキタス端末への搭載が期待されます。

今後の展開として、更に研究開発を進め、暗号の安全の強度を無限大まで自由自在に調整できる計算チップの開発を試みる予定です。

＜お問い合わせ＞
岡山大学 工学部 電気通信系学科
野上 保之、籠谷 裕人
TEL/FAX：086-251-8127