PRESS RELEASE

岡山大学
OKAYAMA UNIVERSITY

平成２８年２月１９日

暗号強度を自在に変えられる暗号計算処理チップを開発

岡山大学大学院自然科学研究科（工）の野上保之准教授の研究グループは、暗号の安全強度を自在に変えられる世界初の暗号計算処理チップを開発しました。高速処理・コンパクト・高機能・安全強度の高度なスケーラビリティを同時に行える同チップは、これまで一つの計算チップではできなかった、ユーザ・機器認証を実現する楕円曲線暗号から、暗号文のままでデータ検索ができる楕円ペアリング暗号まで実現します。

本研究成果により、これまでソフトウェアで処理してきた複雑な暗号計算をより高速に処理することができ、情報の重要度や端末性能にも柔軟に対応（高度にスケーラブル）できます。また、同チップの回路規模は極めてコンパクトで、さまざまなユビキタス端末・IoT デバイスへの搭載が期待されます。

＜業　績＞

野上准教授の研究グループは、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処理チップを開発しました。また、同チップは、従来のユーザ・機器認証のみならず、より複雑かつ高度化した暗号技術にも対応します。このように、ハードウェアの変更を必要とせず暗号の強度を自在に変えることができる高度な暗号計算処理チップは他に例がありません。

＜背　景＞

クラウドコンピューティング時代において、暗号を代表とする情報セキュリティ技術は、必要不可欠なものとなっており、その機能的な要求も年々複雑化・高度化しています。これに加えて IoT 技術が急速に展開しており、これを支える小型デバイスに対しても、複雑な暗号計算を処理できる機能の実装が求められています。

スマートフォン・クラウドコンピューティング・IoT（Internet of Things）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・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となっています。さらにそれは、自動運転や遠隔手術など、もはや人間の手や判断を介すことなく、コンピュータやロボットが自律的に考え、動作する時代に突入しようとしています。加えて、その節々に繋がれているデバイスは、必ずしもスーパーコンピュータのような高性能なものではなく、計算リソースの限られた小型デバイスです。ここに、悪意あるユーザによる操作データ改ざんや、雑音などで誤りが混入した操作信号が入ってしまったら何が起こるでしょうか。ときにそれが、人の命を脅かすものになってしまうことが容易に想像されます。そのようなことが無いように、以前にも増して情報セキュリティ技術に対する要求が高まっており、その複雑かつ高度化した機能をリ

ソースの限られた小型デバイスで実現する必要があります。

＜見込まれる成果＞

本研究により、これまでソフトウェアで処理してきた複雑な暗号計算をより高速に処理することができ、情報の重要度や端末性能にも柔軟に対応（高度にスケーラブル）できます。また、同チップの回路規模は極めてコンパクトで、さまざまなユビキタス端末・IoT デバイスへの搭載が期待されます。

本研究は、科学技術振興機構 研究成果展開事業 研究成果展開支援プログラム（A-STEP)の支援を受け、東京エレクトロンデバイス株式会社と共同開発しました（別紙）。

＜語句説明＞

[1]スケーラビリティ

さまざまなパラメータ設定にハードウェア的な変更を加えることなく対応でき、加えてその性質は暗号強度（情報の安全性）を自在に調整できる機能にも使えます。

＜お問い合わせ＞
岡山大学大学院自然科学研究科（工）
岡山大学セキュリティ研究グループ
准教授　野上 保之
（電話・FAX）086-251-8127