研究成果最適展開支援プログラム（A-STEP）　FS ステージ（シーズ顕在化）
事後評価報告書

プロジェクトリーダー（企業責任者）：東京エレクトロンデバイス（株）
研究責任者：岡山大学　野上 保之
研究開発課題名：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

１．研究開発の目的

ネット上などで用いられている従来の認証技術は、用いるパスワードがユーザ個人の情報と表裏一体であり、いつでもどこからでも個人情報が漏洩しうる。ここに個人情報を介すことなく認証を行うグループ署名と呼ぶ革新的な匿名認証技術が提案された。これには楕円ペアリングという代数計算が必要であり、本開発では、到来するクラウドコンピューティング時代における安全・安心かつ快適な認証技術の実現に向け、これに必要となる計算アルゴリズムおよびその並列計算処理チップの開発を行う。これは世界初の試みであり、ユビキタス機器に要求される省電力かつ高速な処理を実現し、高度 ICT 社会を根底から支える技術として重要な役割を果たすものである。

２．研究開発の概要

①成果

ユビキタス・クラウドコンピューティング時代における高度な認証技術に必要となる代数計算を、効率よく、高速に計算処理できることはもとより、様々なアプリケーションにも適用できるよう高度なスケーラビリティをもって実現するベクトル乗算アルゴリズム（CVMA）を FPGA 上に実装する。そのために、１）CVMA の計算コストの足枷となっていた整数パラメータを低減する手法､およびそれに伴う CVMA の改良が必要となる｡加えて、２）これを FPGA 上で実現するために、多倍長計算部をコンパクトに実装し、それを上手にリソースシェアリングしながら効率よく使用する回路で構成する必要がある。これらを解決し、コンパクトな回路規模で、次世代の暗号技術に対しても十分に安全であり高速に処理できる暗号計算チップを開発した。今回の研究開発による実験データに基づき、事前計算する整数データテーブルのサイズがより小さければ、さらなるコンパクト化、効率化が期待できることが分かった。そして、それを実現するアルゴリズムを開発し、具体的な結果として、次元数の 3 乗のオーダーから、2 乗のオーダーにまでデータ圧縮できることが判明している。そこで更なる展開として、これによる改良手法を FPGA へ搭載した場合の性能向上について、実装評価したい。

②今後の展開

二つの展開を考えている。一つは、今回の研究開発用ボード SASEBO-GII と共に、得られた主たる成果である CVMA のアルゴリズムを、広く研究開発用として公開し、活用してもらうことである。もう一つは、新たに他の事業の支援を受けながら研究開発を継続し、より具体的に上階層の暗号応用技術・製品に向けてカスタマイズや改良などしてゆくことである。

３．総合所見

目標通りの成果が得られた。
シーズである「ベクトル乗算アルゴリズム CVMA」の FPGA を用いたハードウエア化を達成し、高効率化を図る工夫もされ、その成果が認められる。
数値アルゴリズムとハード向けアルゴリズムにそれぞれ強みのある学と産が協力して相乗的な成果が得られた。
研究成果を広く公開するのみならず、より高度に発展させるために、さらなる研究の展開が望まれる。