研究成果展開事業　研究成果最適展開支援プログラム
本格研究開発ステージ　ハイリスク挑戦タイプ　事後評価報告書

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
プロジェクトリーダー 所属機関	:	東京エレクトロンデバイス(株)
研究責任者	:	野上保之 (岡山大学)

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ー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、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

暗号強度を自在に調整(具体的には 256ビットから 5120ビット強度)でき、かつ計算処理時間が実時間内(具体的には 5120 ビット強度の際にも 1 秒以内)で快適に処理できる楕円暗号およびペアリング暗号計算処理を、FPGA 回路実装によりコンパクトに機能実装することである。

これまでの研究で下層より「計算チップ・電磁波解析」、「多倍長整数演算」、「離散数学・四則演算」、「楕円曲線暗号」、「ペアリング暗号」、「匿名認証技術」、「認証応用技術」で構成されているレイヤ構造で、「離散数学・四則演算」レイヤまでの原理的な実装を完了している。今回の研究ではさらに実用的な回路を達成するため下記を到達点とする。

①ペアリング暗号のレイヤまで実装する。

②また前回未達であった「並列処理」を取り入れながらより高速な回路構成を研究し実装する。

CVMA　(Cyclic Vector Multiplication Algorithm)のハードウェア-による LSI 化へのプロジェクトと言う事で、3 年間の研究を実施してきた。さらに実用化へ向けての楕円加算、スカラー倍算、楕円ペアリング暗号のアルゴリズムまでを FPGA に実装して実用的な回路規模と演算スピードを達成できた。また、本研究を通して新たな研究テーマも発生して、さらに研究を進めていくこととなる。

一方、暗号化の商品化については、CVMA での知名度が有っても、各研究機関、企業においてそれぞれが独自の方法を研究しているため、本方式の普及には技術的な側面以外の壁を感じている。

このような技術に関しては、実用製品に採用されて普及が進む事は明白であるため、事業化に向けては研究用途や教育用途以外の企業へ向けても採用されるようなライセンス形態を考えて普及を進めていくことが必要と感じている。

研究開発目標	達成度
① CVMA のための事前計算テーブル計算機能の FPGA 上への実装	① 事前計算テーブルの計算機能を FPGA のロジックとして実装した。作成したテーブルを円滑に利用できるようにテーブルデータサイズは 36Kb ブロック RAM1 つ、18Kb ブロック RAM3 つの FPGA リソースで実現している。
② 楕円加算・スカラー倍算・楕円ペアリング暗号の改良アルゴリズムの FPGA 搭載	② 次元数 m=1～20 のスケーラビリティを持たせた状態で楕円加算・スカラー倍算・楕円ペアリング演算機能を FPGA に実装、機能確認を行った。
③ ハードウェア実装の最適化を施し速度向上を実現	③ プリミティブ演算器の最適化ではなく、逆元計算のアルゴリズムの最適化により最終的な楕円加算・スカラー倍算・楕円ペアリングの演算速度の向上を実現している。 演算速度性能としては、楕円スカラー倍算では m=1(256bit 暗号強度)の時では 10[ミリ秒]、m=20(5120bit 暗号強度)の時では 374[ミリ秒]で実現しており、楕円ペアリング演算については m=18(4608bit 暗号強度)の時で 309[ミリ秒]程度で実現できている。
④ ハードウェア的な情報の漏洩が無いか（サイドチャネル攻撃という）への耐性を検証	④ RSA 暗号で明確に識別できる場合に対して、CVMA においては波形からは暗号計算処理との相関が見られない耐性を持つ傾向が観測できている。

②今後の展開

本 ASTEP にて実装した暗号計算装置は、昨今の IoT 技術に積極的に活用が可能である。具体的には、スマートメータを始め、様々な機器がインターネットに接続されようとしており、そこでは個人情報の保護はもとより、厳密な相互の機器認証のもとデータの送受信がなされなければならない。そのための高度な公開鍵暗号技術としてペアリング暗号が活用されようとしている場面において、本開発の成果として得られた実装および実装手法が活用できる。特に、IoT 端末としての活用を考えたとき、いまもっとも注意すべきとされている事柄が、サイドチャネル攻撃に対する耐性である。本開発では、その最後の方において検討に着手したものの、必ずしも厳密なサイドチャネル攻撃に対する安全性評価が行えていない。さらには、これを回避するための追加的な工夫も必要になることが考えられる。これを具体的に実験し、検討し、そして安全な設計法としての尺度や評価法を世界標準として確立しようとするプロジェクトとして、上記の研究開発を進めることを予定している。この過程を経て、厳格に安全な実装手法として本 ASTEP の成果を社会に還元できるよう進めている。

3. 総合所見

概ね目標を達成し、次の研究開発フェーズに進むための成果が得られており、今後の取り組み次第ではイノベーション創出の可能性がある。

暗号アルゴリズムを FPGA 実装し、ハードウェアコストと性能のトレードオフを検討してフィードバックし、当初の目標を達成を達成した。しかし、社会ニーズと技術シーズとのギャップが埋められておらず、現状では、

本技術のユーザ適用とそれによる社会的イノベーションの道筋が見えていない。国際学会への発表と標準化活動、キラーアプリの明確化等を通して、イノベーションへの道筋の具体化を期待する。