論 文 の 内 容 の 要 旨

情報システムが社会へ浸透し，シンクライアントやクラウドサービスのように，ネットワークを介してサーバへ接続するリモートコンピューティング環境が注目されるようになってきた．この環境では，サーバにはあらゆる端末のデータを一括保管するため，ストレージの容量は膨大となる．暗号化によるデータ防護は，情報漏洩に対するセキュリティ対策の基本手段であるため，膨大なデータを高速に暗号化する必要性が生じてきている．一方，暗号アルゴリズムの処理の効率性は，コンピュータ内のプロセッサの影響を受ける．プロセッサのアーキテクチャは，2000 年頃まではシングルコアで設計されてきた．しかし，消費電力に起因する発熱の問題から，そのアーキテクチャ設計は 2002 年以降，主にマルチコアやメニ―コアに移行しており，今後はこのような並列プロセッサにおける暗号の設計及び実装評価が重要になると考えられる．特に現在では，マルチコア CPU だけでなく，専用ハードウェア並みの演算能力を持った Graphics Processing Unit（GPU）や Intel Xeon Phi が，暗号処理を効率化できる並列プロセッサとして注目されてきている．

しかし，並列プロセッサに対する暗号の設計及び実装評価は，上記のような様々な種類のプロセッサを対象としなければならず，その負担は大きい．その上，現在使用されている暗号は多種多様である．そのため，本研究では，並列プロセッサ向けの暗号設計用ツールがあれば，暗号設計の負担を軽減できる．そこで本研究では，暗号アルゴリズムを選択して実行可能な並列プロセッサとして注目されている GPU 向けに，大容量データの処理に適するブロック暗号を効率的に設計するためのフレームワーク(Performance Prediction Framework: PPF) を開発することを目的とした．PPF には，ブロック暗号の逐次処理コードの GPU 実装性能を，設計段階で予測できるという特徴を持たせる．また本研究では，並列プロセッサに共通したプラットフォームである OpenCL を採用した．このことにより PPF は，GPU ベンダに依存したフレームワークにならず，将来的にはマルチコア CPU や Intel Xeon Phi への拡張も可能となる．

第 2 章では，OpenCL プラットフォームの仕様とそれに準拠した並列プロセッサ及び GPU について述べる．この章で述べた GPU アーキテクチャの特徴は，第 6 章で述べる PPF の設計に反映される．

第 3 章では，PPF の設計及び実装評価で用いるブロック暗号のアルゴリズムについて述べる．PPF は，公開鍵暗号等での利用も視野に入れて設計しているが，本研究での PPF の評価はブロック暗号に対してのみ行う．

本研究で提案する PPF では，これから並列プロセッサ向けに暗号アルゴリズムを設計しようとする設計者が容易に利用できるように，設計の簡単化を目指す．そこで，第 4 章では，AES を題材として，複数のブロック暗号に共通した GPU への実装方針を導出する．この実装方針は，第 6 章で述べる PPF の設計の簡単化に反映される．

第 5 章では，第 4 章で導出した実装方針を用いて，ブロック暗号の代表的な構造である

SPN 構造，Feistel 構造，SPN と Feistel のハイブリッド構造の暗号アルゴリズムを実装し，異なる世代のアーキテクチャで開発された NVIDIA Geforce GTX 580 と GeforceGTX 280 という 2 種の GPU での処理速度を測定する．具体的な暗号アルゴリズムには，SPN 構造に AES, Feistel 構造に Camellia, SPN と Feistel のハイブリッド構造に SC2000 をそれぞれ選択した．この値は，第 6 章で必要となる GPU を用いた暗号処理性能の実測値となる．なお，Camellia と SC2000 はそれぞれ AES と異なる構造をとるブロック暗号であるため，この測定結果から，併せて第 4 章で導出した実装方針の有効性も確認できる．

第 6 章では，PPF の開発と評価について述べる．PPF の評価では，第 5 章で測定した完成版のブロック暗号に加え，ブロック暗号の設計段階の実装性能を予測し，暗号設計者の作業量を軽減できることを示す．第 5 章と同じ種類のブロック暗号と GPU を対象として PPF の評価を行ったところ，これらの暗号化処理時間を測定した結果は，PPF から見積もられる結果と概ね一致した. また, 仕様書を基にシミュレートした設計段階の Camellia に対しても，GPU 実装による暗号化処理時間を予測できることを確認し，効果的な開発を補助できることを確認できた．本研究で実施した PPF の評価は，Fermi 及び GT200 アーキテクチャの NVIDIA GPU のみで評価した．今後は，Kepler アーキテクチャの NVIDIA GPU に加え，AMD 社の GPU や Intel Iris Graphics 等のモバイル型 GPU にも評価を行う必要がある．また，マルチコア CPU や Intel Xeon Phi などの並列プロセッサに対しても評価を行い，PPF の適用可能範囲を拡張していく必要がある．本研究では，暗号アルゴリズムとして，共通鍵暗号を対象としたが，公開鍵暗号等も実利用されている．今後は，このような暗号にも PPF を対応させていく必要がある．