# Cell/B.E. における暗号処理の効率的なオフロード方式の提案と実装

杉浦 寛† 大釜 正裕† 羅 鏡栄† 齋藤 孝道††
†明治大学大学院 ††明治大学

## 1 はじめに

複数のプロセッサを一つのチップ上に搭載したマルチコアプロセッサが注目されている．その中でも，ヘテロジニアスマルチコアプロセッサは，OSなどの制御を受け持つ汎用系プロセッサと，画像処理や暗号処理に特化した演算系プロセッサを，それぞれ複数搭載している．そのため，汎用プロセッサで動作するアプリケーションがOpenSSLなどのツールキットを用いて暗号処理を実行する場合には，演算系プロセッサへ暗号処理をオフロードすることで，処理全体のパフォーマンス向上が期待できる．ここで，複数のアプリケーションが演算系プロセッサを利用する場合には，特定のプロセッサに処理が集中し，アプリケーション処理の遅延が発生する場合がある．そのため，演算系プロセッサの稼働状況を考慮してオフロード対象を決定することで，効率よく演算系プロセッサを利用することができる．

本論文では，ヘテロジニアスマルチコアプロセッサの一つであるCell Broadband Engine[1](以降，Cell/B.E.と呼ぶ)を用いて，OpenSSL[2]の暗号処理を高速化することを目的とし，複数のアプリケーションプロセスでの暗号処理を演算系プロセッサで実行するオフロード方式の提案と実装について示す．ただし，既存のOpenSSLは，Cell/B.E.の汎用系プロセッサでは動作できるが，演算系プロセッサには対応していない．そのため，提案方式では，演算系プロセッサを暗号処理専用のモジュールとして扱い，OpenSSL暗号処理の一部をオフロードするためのライブラリと，効率良く演算系プロセッサを利用するためのプロセススケジューラを実装する．これらの評価として，本論文で提案したシステムと，既存の汎用プロセッサでそれぞれパフォーマンス計測を行い，その結果について考察する．

## 2 Cell Broadband Engine

ここでは，開発環境として使用したPLAYSTATION3 (PS3)に搭載されているCell/B.E.について述べる．

Cell/B.E.は，汎用系プロセッサとしてPPEを1つ，演算系プロセッサとしてSPEを8つ搭載している．ただし，実質的にユーザが利用できるSPEは6つである．

PPEは，64bitのPowerPCアーキテクチャを基にしたプロセッサであり，既存のアプリケーションが動作できる．SPEは，プロセッサ本体であるSPUと，256Kbyteの専用メモリであるLS，外部とのデータのやりとりを行うためのインタフェースであるMFCを搭載している．SPEが直接アクセスできるのはLSだけであり，SPEが外部のメモリにアクセスする場合には，MFCを介したデータ転送機能であるDMA転送やメールボックスを用いる．

## 3 提案システム

ここでは，Cell/B.E.でOpenSSLの暗号処理をSPEにオフロードするシステムと，その実装について示す．

### 3.1 概要

本論文の提案システムでは，SPEを暗号処理モジュールとして扱い，OpenSSLからSPEを利用するためのライブラリ(以降，暗号処理オフロードライブラリと呼ぶ)と，暗号処理を実行するプロセス(以降，暗号処理プロセスと呼ぶ)の処理をSPEへ割り当てるためのスケジューラ(以降，プロセススケジューラと呼ぶ)を実装する．提案システムは，OpenSSLとSPE間の処理やSPEと暗号処理プロセスとの対応付け，暗号処理プロセスのスケジューリングを行う．また，暗号処理プロセスの制御のためのスケジューリングとして，FIFOを採用している．

### 3.2 実装

#### 3.2.1 暗号処理オフロードライブラリ

暗号処理オフロードライブラリは，PPE側で動作し，OpenSSLとSPE間の処理を行うモジュールと，SPE側で動作し，暗号処理を実行するモジュールで構成される．本提案システムで対応している暗号処理アルゴリズムは，AESのECBモード，CBCモード，CTRモードである．

以下に示す暗号処理オフロードライブラリの動作概要は，図1の各番号と対応している．ただし，説明の簡略化のため，SPEは1つのみ表記している．また，プロセススケジューラの動作については後述する．

(1) 暗号処理プロセスが暗号処理オフロードライブラリを呼び出し，PPEモジュールへ制御が移る．
(2) SPEへプログラムをロードし，SPEを起動する．ただし，既にSPEが起動している場合は，この処理は行わない．
(3) プロセススケジューラを呼び出し，SPEを取得する．
(4) SPEモジュールへメールボックス機能を用いて暗号処理の実行を通知し，SPEモジュールへ制御が移る．
(5) SPEモジュールで，暗号処理に用いる平文，鍵などのデータをメインメモリからLSへDMA転送し，暗号処理を実行する．
(6) 暗号処理が終了すると，処理結果をLSからメインメモリへDMA転送する．そして，暗号処理オフロードライブラリへメールボックス機能を用いて暗号処理の終了を通知し，PPEモジュールへ制御が移る．
(7) プロセススケジューラを呼び出し，SPEを解放する．
(8) 全てのプロセスの処理が終わっている場合，SPEのプログラムを破棄し，SPEを終了する．
(9) 暗号処理プロセスに処理結果を返す．

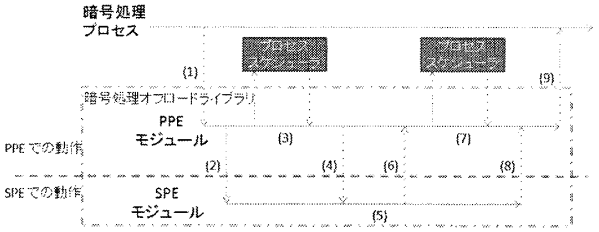


図1: 暗号処理オフロードライブラリの動作

#### 3.2.2 プロセススケジューラ

プロセススケジューラは，カーネルモジュールとして動作し，暗号処理プロセスからは，`ioctl`システムコールにより呼び出される．プロセススケジューラは，暗号処理オフロードライブラリから呼び出されると，`ioctl`システムコールの引数に従い，SPEの取得または解放を行い，その結果を返す．SPEの動作状態の管理には，SPEごとに構造体を用意し，それぞれにSPEを特定するための識別子であるSPE IDとSPEの動作状態を示す変数であるSPE動作フラグをメンバとして設定している．SPE動作フラグの値はWORKとIDLEの2種類があり，WORKはSPEが処理の実行中であることを，IDLEはSPEが処理を実行していないことを，そ

れぞれ表す．また，暗号処理プロセスのスケジューリングのために，プロセススケジューラ専用のリスト (以降，プロセスリストと呼ぶ) を用意する．プロセスリストには，全ての SPE の SPE 動作フラグが WORK の場合に，暗号処理プロセスのプロセス ID を登録する．プロセススケジューラは，このリストを基に，暗号処理プロセスの WAIT 状態または RUNNING 状態への遷移を行う．

### 3.3 提案システムの動作例

ここでは，プロセス A，B が提案システムを利用し，順に暗号処理を実行する場合を例に，提案システムの動作について示す．ただし，SPE は 1 つのみ動作しているものとする (図 2 参照)．また，以下の説明は図 2 の各番号と対応している．

(1) プロセス A がプロセススケジューラを呼び出す．プロセススケジューラは，SPE の動作フラグを WORK にし，SPE の SPE ID をプロセス A に返す．プロセス A は，SPE に暗号処理を実行させる．

(2) プロセス B がプロセススケジューラを呼び出す．プロセススケジューラは，全ての SPE が動作中のため，プロセス B のプロセス ID をプロセスリストに登録して，プロセス B を WAIT 状態へ遷移する．

(3) プロセス A は，SPE での処理が終了すると，プロセススケジューラを呼び出す．プロセススケジューラは，SPE の動作フラグを IDLE にする．さらに，プロセスリストの先頭に登録されているプロセス B をプロセスリストから削除し，RUNNING 状態へ遷移する．

(4) プロセス B がプロセススケジューラを再度呼び出す．プロセススケジューラは，動作フラグが IDLE となっている SPE の SPE ID をプロセス B に返す．プロセス B は，SPE に暗号処理を実行させる．

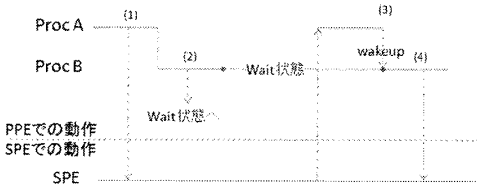


図 2: 提案システムの動作例

## 4 評価

### 4.1 評価環境

提案システムの評価を行うにあたり，Cell/B.E. 環境と，その比較対象として，Core2Duo 環境を用いて，OpenSSL の speed コマンドを実行した．Cell/B.E. 環境で使用した PS3 は，3.2GHz で動作する Cell/B.E. と 256MB の RAM を搭載したマシンであり，Fedora9 (Kernel2.6.25-14) と，Cell/B.E. に対応させるためのカーネルパッチ，Cell/B.E. 開発者向けのツールキットである CellSDK3.1[3] を使用した．評価に用いたコンパイラは，PPU 及び SPU をターゲットとした ppu-gcc4.1.1 及び spu-gcc4.1.1 である．Core2Duo 環境は，Core2Duo 3.16GHz と 3GB の RAM を搭載したマシンであり，Fedora9 (Kernel2.6.26.3) が動作している．また，OpenSSL のバージョンは，いずれの環境でも，0.9.8g である．

### 4.2 評価項目

提案システムの性能評価として，表 1 に示す項目それぞれについて，計測を行った．

提案システムと Mars では Cell/B.E. での SPE を用いた場合の性能評価を，PPE と Core2Duo では汎用プロセッサでの性能評価を，それぞれ目的としている．また，Mars[4] とは，既存のマルチコア環境で演算系プロセッサを効率よく利用するための API 群である．Mars と共に OpenSSL と Mars を組み合わせたパフォーマンス評価のためのライブラリがリリースされており，これを提案システムと同じ環境下で実行する．これらの項目について，プロセス数が 1 つの場合と 6 つの場合で計測を行った．また，計測に用いた暗号処理アルゴリズムは，AES の ECB モードであり，実行時には，プログラム実行の実時間を計測した．

表 1: 評価項目一覧

| 名称 | 詳細 |
|---|---|
| 提案システム | Cell/B.E. 環境で提案システムを用いて計測 |
| Mars | Cell/B.E. 環境で Mars を用いて計測 |
| PPE | Cell/B.E. 環境で PPE のみを用いて計測 |
| Core2Duo | Core2Duo 環境で計測 |

以下，プロセス数が 1 つの場合と 6 つの場合での計測結果を表 2，表 3 それぞれに示す．表に示すデータサイズとは，一度に暗号処理を行うデータサイズを指し，評価項目は，表 1 の名称に対応している．ここで，プロセス数が 6 つの場合は，提案システムと MARS では 6 つの SPE で同時に演算し，Core2Duo では，2 つのプロセスで同時に演算が可能である．

表 2: プロセス数 1 つの場合のスループット

| データサイズ (byte) | 16 | 64 | 256 | 1024 | 8192 |
|---|---|---|---|---|---|
| 提案システム (Mbps) | 4.67 | 18.75 | 74.14 | 283.22 | 499.38 |
| Mars (Mbps) | 8.25 | 12.76 | 51.22 | 106.14 | 274.68 |
| PPE (Mbps) | 306.5 | 356.5 | 373.4 | 380.46 | 385.13 |
| Core2Duo (Mbps) | 1091.2 | 1197.6 | 1230.9 | 1240.8 | 1233.4 |

表 3: プロセス数 6 つの場合のスループット

| データサイズ (byte) | 16 | 64 | 256 | 1024 | 8192 |
|---|---|---|---|---|---|
| 提案システム (Mbps) | 12.5 | 49.67 | 95.14 | 350.52 | 2646.4 |
| Mars (Mbps) | 7.26 | 28.72 | 116.92 | 431.92 | 1313.6 |
| PPE (Mbps) | 306.5 | 356.5 | 373.4 | 380.46 | 385.13 |
| Core2Duo (Mbps) | 2175.4 | 2396.5 | 2451.5 | 2456.2 | 2497.7 |

計測結果より，一度に暗号処理を行うデータサイズが 8192byte，プロセス数が 6 つの場合の提案システムでのスループットが最も高くなった．また，PPE，Core2Duo では，データサイズによるスループットの変化はほとんど見られなかったが，提案システム，Mars では，データサイズが大きくなるにつれ，スループットが向上した．これは，データサイズが小さい場合は，暗号処理のオフロードにより生じるデータ転送などのオーバーヘッドが暗号処理の処理時間よりも大きくなるためだと考えられる．

## 5 まとめと今後の課題

本論文では，Cell/B.E. で OpenSSL の暗号処理を SPE にオフロードするためのシステムを提案した．また，提案システムについて実装を行い，そのパフォーマンスを計測した．これにより，標準的な並列化ライブラリである MARS と比べても，比較的高速な演算ができることが，示せた．

今後として，様々な暗号処理アルゴリズムへの拡張や，より効果的なスケジューラの実装などの課題がある．

### 参考文献

[1] http://cell.scei.co.jp/index_j.html

[2] http://www.openssl.org/

[3] http://www.bsc.es/projects/deepcomputing/ linuxoncell/

[4] http://ftp.uk.linux.org/pub/linux/Sony-PS3/mars/latest/mars-docs-1.1.4/html/