様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　６月１０日現在

機関番号：32682
研究種目：若手研究(B)
研究期間：2010 年度～2012 年度
課題番号：２２７００００８６
研究課題名（和文）
暗号モジュールを持つマルチコアＣＰＵでの暗号処理の効率的なオフロードに関する研究
研究課題名（英文）An proposition of an efficient offloading method for multi-core CPU with cryptographic modules
研究代表者
齋藤　孝道（SAITO TAKAMICHI）
明治大学・理工学部・准教授
研究者番号：９０３０７７０２

研究成果の概要（和文）：
当該研究では,専用のハードウェア暗号処理モジュールをもつマルチコア CPU において,暗号処理を暗号モジュールにオフロード（処理の委託）することを試み，成功した．また，その高速化にも成功した．
研究成果の概要（英文）：
In this reserch, we propose and implement to off-load a part of cryptographic process of CPU into cryptographic modules efficiently. We also and evaluate it.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,400,000	420,000	1,820,000
2011 年度	1,200,000	360,000	1,560,000
2012 年度	500,000	150,000	650,000
年度			
年度			
総　計	3,100,000	830,000	4,030,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：ネットワークセキュリティ技術

１．研究開始当初の背景

高度情報化社会において，セキュリティ技術が重要視されている．セキュリティ技術の中の暗号通信が様々なシーンで利用されるになってきた．

２．研究の目的

しかしながら，暗号通信は，その処理のコストが高いので，効率を考慮した方式が必要である．そこで，本研究では，マルチコア CPU において，効率的なオフロードを実現する技術の開発を目的とする．

３．研究の方法

いくつかのマルチコア CPU において，暗号処理基盤システムを構築し，その上で，カーネルモジュールとしてオフロード技術を開発した．

４．研究成果

当初，想定していた CPU、インテル社製 IXP425 だけではなく，ソニー・コンピュータエンタテインメント(SCE)、ソニー、IBM、東芝によって開発された CELL/B.E.といったヘテロジニアスな CPU でもオフロードを実装し，効率化に成功した．
以下の図 8～9 は，インテル社製 IXP425 において提案した暗号処理のオフロード処理方式の実行結果を，既存方式と比較したものである．

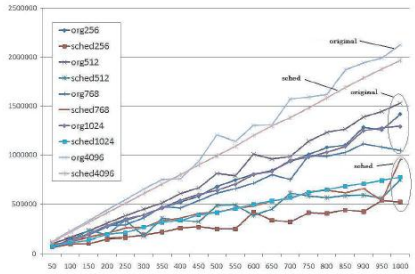

図 8　OCF と sched の比較（3DES）：プロセス数 4
Fig. 8　Comparison between OCF and sched: 4 processes, 3DES.

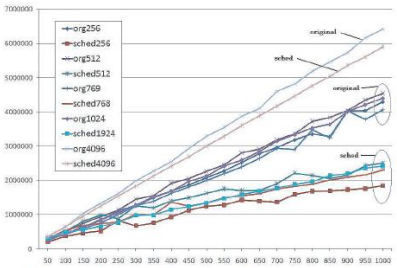

図 9　OCF と sched の比較（3DES）：プロセス数 12
Fig. 9　Comparison between OCF and sched: 12 processes, 3DES.

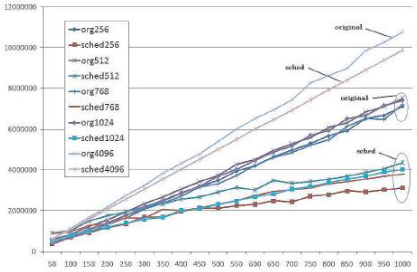

図 10　OCF と sched の比較（3DES）：プロセス数 20
Fig. 10　Comparison between OCF and sched: 20 processes, 3DES.

同時に，実行するプロセス数を 4 つとしたものを図 8 とし，実行するプロセス数を 12 つとしたものを図 9 とし，実行するプロセス数を 20 つとしたものを図 10 とした．いずれにおいても，提案方式が既存方式より高速に処理できることがわかる．

また，図 11 より，提案システムでは，オフロード実行時，既存方式より，汎用 CPU に負荷を掛けていないことが分かる．

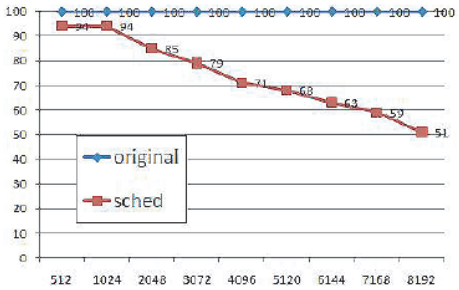

図 11　CPU 使用率の比較（3DES）
Fig. 11　Comparison of CPU load: 3DES.

以下の図 8 は，CELL/B.E.において提案した暗号処理のオフロード処理方式の実行結果を示したものである．また，既存方式と比較したものが，表 5 となる．

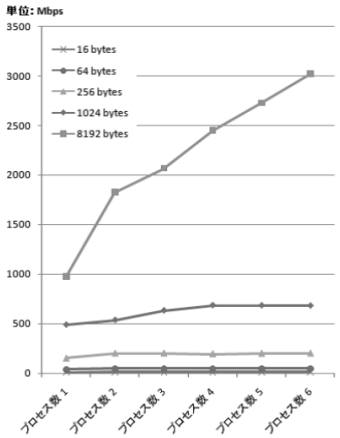

図 8　プロセス数を変化させた場合の提案システムのスループット
Fig. 8　Throughput of the proposed system when the number of processes

8192 バイト単位で暗号化した場合，プロセス数に応じて，処理速度が向上していることが分かる．

表 5　AES-CBC モード，プロセス数 6 つの場合のスループット
Table 5　Throughput of six processes, AES-CBC

データサイズ (bytes)	16	64	256	1024	8192
提案システム (Mbps)	12.62	50.06	197.45	655.75	2282.47
Mars (Mbps)	8.17	33.0	130.87	848.43	1761.78
PPE (Mbps)	231.3	273.81	285.13	286.92	294.2
Core2Duo (Mbps)	1757.1	2411.5	2660.5	2667.4	2799.0

また，表５より，既存方式より，提案システムは高速に処理ができることが分かる．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

齋藤孝道，大釜正裕，羅 鏡栄，杉浦 寛
IXP425 における暗号処理の効率的なオフロード方式の実装と評価，情報処理学会 論文誌，Vol.51 No.9 (2010)，pp.1530-1541.

齋藤孝道，杉浦 寛，「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」，情報処理学会 論文誌，Vol.53，No.2 (2012)，pp.815-824.

Takamichi Saito，Kiyomi Sekiguchi，and Ryosuke Hatsugai，
Authentication Binding between SSL/TLS and HTTP，
IEICE TRANSACTIONS on Information and Systems Vol.E95-D,No.3，pp 786-796.

〔学会発表〕（計　15 件）

金子洋平，天野桂輔，齋藤孝道，Android 端末における暗号モジュールの利用と評価，2013 年暗号と情報セキュリティシンポジウム概要集，pp105-110，2013.

後藤浩行，齋藤孝道，Web 行動追跡のためのハードウェア特徴点の抽出，2013 年暗号と情報セキュリティシンポジウム概要集，pp72-77，2013.

塚本耕司,後藤浩行，齋藤孝道，JavaScript ベンチマークを用いた CPU 推定手法の提案と実装，情報処理学会全国大会予稿集，2013.

桐生直輝,後藤浩行，齋藤孝道，CPU 拡張命令の対応の有無による CPU アーキテクチャの推測，情報処理学会全国大会予稿集，2013.

金子洋平,天野桂輔，齋藤孝道，Android 端末における 暗号モジュールの利用と評価，情報処理学会全国大会予稿集，2013.

上原崇史,川口謙太郎，齋藤孝道，イントラネット環境構築システムの提案と実装，情報処理学会全国大会予稿集，2013.

小川梨恵,天野桂輔，齋藤孝道，SSL/TLS 処理のパフォーマンス解析について，情報処理学会全国大会予稿集，2013.

鈴木舞音,天野桂輔，齋藤孝道，SEAndroid におけるアクセス制御の可視化，情報処理学会全国大会予稿集，2013.

磯侑斗,今野真希,武佑香，齋藤孝道，SAML による属性情報の選択的提示の可能なシングルサインオンシステムの提案と実装，情報処理学会全国大会予稿集，2013.

大丸雅人,今野真希,武佑香，齋藤孝道，OpenID による属性情報の選択的提示の可能なシングルサインオンシステムの提案と実装，情報処理学会全国大会予稿集，2013.

村上智祐，笠原竜大，齋藤孝道，2011，
UltraSPARC T2 における暗号処理のオフローディング方式の実装と評価，
第 73 回情報処理学会全国大会公演論文集
3-533，3-534

天野桂輔，渥美裕太，笠原竜大，村上智祐，齋藤孝道，2011，
IXP425 における暗号処理をオフロードする Web サーバのパフォーマンス計測，
第 73 回情報処理学会全国大会公演論文集
3-531，3-532

川口謙太郎，森皓生，齋藤孝道，2011，
仮想化リモートデスクトップ環境 VCL に関するパフォーマンスの測定，
第 73 回情報処理学会全国大会公演論文集
3-405，3-406

後藤浩行, 武佑香, 鳥居悟, 齋藤孝道, 2011, OAuth におけるトークンを用いた権限管理方式の提案と実装,
第 73 回情報処理学会全国大会公演論文集
3-517, 3-518

武佑香, 後藤浩行, 鳥居悟, 齋藤孝道, 2011, Shibboleth を用いた Web アプリケーションのアクセス制御の実現,
第 73 回情報処理学会全国大会公演論文集
3-515, 3-516

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
なし

６．研究組織
(1)研究代表者
齋藤　孝道（Saito Takamichi）
明治大学・理工学部・准教授
研究者番号：９０３０７７０２

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：