様式 C-19

科学研究費補助金研究成果報告書

平成２２年　６月１８日現在

研究種目：若手研究（Ｂ）
研究期間：2007～2009
課題番号：１９７００７０
研究課題名（和文）　組込みシステム用暗号ミドルウェア開発に関する研究

研究課題名（英文）　An Effective Off-Loading of Cryptographical Operations and its Evaluation

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）：
昨今の CPU アーキテクチャの多様化の中で，コア内に暗号処理を専ら行うモジュール（以降，暗号モジュールと呼ぶ）を持つプロセッサがいくつか登場した．この種のプロセッサでは，暗号処理以外の処理は汎用モジュールで行い，処理速度の要求される暗号処理は暗号モジュールで行うことにより，プロセッサ全体で処理速度の向上を狙っている．しかしながら，既存のソフトウエアの多くは，この種のプロセッサ向けに設計されておらず，一般的に，暗号モジュールを活用するためにはソフトウエアを改修するなどの処置が必要となる．
本研究では，コアの中に暗号モジュールを一つ持つプロセッサにおいて，暗号ライブラリの処理の一部を透過的に暗号モジュールへオフロードし暗号処理を行う仕組みを提案し，その実装と評価を行い，効果があることを確認した．

研究成果の概要（英文）：
Recently, as there are many types of CPUs in a market, we have some CPUs which have cryptographical modules. In the type of CPUs, a cryptographical module can be used to off-load a part of cryptographical operation. However, since an established cryptographic library such as cryptographic library can not be applied to it, we need a solution for it. In this research, we implemented a scheduler in a cryptographic middleware to solve it, and evaluated its off-loading performance.
We also confirm that our work is effective.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,000,000	0	1,000,000
２００８年度	1,300,000	390,000	1,690,000
２００９年度	900,000	270,000	1,170,000
年度			
総　計	3,200,000	660,000	3,860,000

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：セキュリティ，暗号技術，組込み技術

１．研究開始当初の背景

ユビキタスネットワーク社会の到来に向け，様々な組込み機器がネットワークに接続されつつある．組み込み機器の中でも，特に，通信速度の向上や処理能力向上のため，IP パケットの高速処理を実現するネットワークプロセッサ（以降，NP と呼ぶ）が注目されている．更に，組み込み機器の通信セキュリティの確保のため，IPSec や SSL（Secure Socket Layer)といった暗号処理を伴うシステムが増え，高い（暗号）処理能力が求められている．これに対処するため，専用のハードウェア暗号処理モジュールをもつ NP（以降，暗号モジュールを持つ NP を適宜 CNP 呼ぶ）が開発されてきている．

一般的に，組込み機器に使用される CPU や OS は，製品によりさまざまであり，使用される暗号アルゴリズムやその利用形態も多種多様である．その一方で，暗号処理用 API（以降，暗号 API と呼ぶ）を独自に実装することは，非常にリスクが高く，非専門家による実装はタブー視されている．暗号 API は，一般的に広く利用され，実装の確実性が検証されているものを利用すべきである，とされている．

現状では，CNP 上で，暗号処理を伴う開発を行う際，各ベンダが用意したドライバを利用し，アプリケーションから直接利用するケースが多いが，今後，より複雑かつ高機能な暗号処理システムの構築の際には，高機能かつ実績のある既存の暗号 API を利用する必要性が高まることが予想される．

２．研究の目的

上述のとおり，CNP における暗号処理を伴う開発環境の状況を鑑みて，当該研究では，様々な CNP 用のミドルウェアの開発を目的とする．ここで，想定する（暗号）ミドルウェアとは，単なるドライバや透過的なインターフェースとしての役割りだけではなく，汎用計算処理能力，メモリ（容量やアクセス速度）や電力など，様々な制約がある CNP という計算機リソースにおいて，暗号処理の高速化のために，最適なリソースマネージメント機能を擁するものである．

例えば，対象とする CNP は，専用のハードウェア暗号処理モジュールを一つしか搭載していないものや複数搭載しているものあるというように，様々ある．また，汎用 NP の場合，外部にハードウェア暗号処理モジュールを用意するケースや独自にソフトウェアによるエミュレータを利用するケースも想定される．よって，暗号 API を適用するターゲット CNP に応じて，そのハードウェア的な差異を吸収する必要がある．更に，それら専用のハードウェア暗号処理モジュールを，適切に利用できない場合，暗号処理がシステム全体の中で，致命的なボトルネックになりかねない．例えば，あるプロセスがデータを暗号化する際，暗号化する平文が数百バイトにわたるとき，そのプロセスだけで（一つしかない）ハードウェア暗号処理モジュールを占有していると，他のプロセスが暗号処理を行うことができなくなる．複数個のハードウェア暗号処理モジュールが有る場合には，適切にモジュールを利用するように処理を割振るべきである（図 1 参照）．また，NP の外に暗号モジュールがある場合は，バス転送のオーバーヘッドとの兼ね合いで，適切なサイズのみの転送を行うべきである．これらからも明らかなように，（暗号）ミドルウェアは，環境に応じて最適なリソースマネージメント機能を必要とする．

３．研究の方法

OSS のミドルウェアをベースに，実機を用いてシステムを実装する（図 1 参照）．

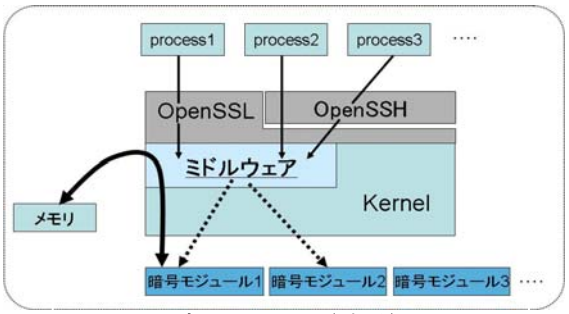

図 1　NP 内における（暗号）ミドルウェアの役割り

４．研究成果

目標とする暗号ミドルウェアを実装し，効率的にオフロードすることに成功した．

図 2，3 および 4 において，AES を用いた実験結果をしめす．同時に起動しているアプリケーションプロセスが 4，12，20 個のケースで，暗号化回数が約 200 回を超えるあたりから，今回作成したシステム（図中では sched と表記）の処理速度が，オリジナルシステム（図中では OCF と表記）優位が顕著化しており，本研究が有効であるとの結果を得られた．

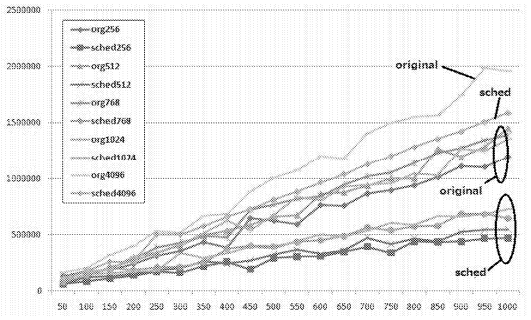

図２　同時に起動しているアプリケーションプロセスが 4 個

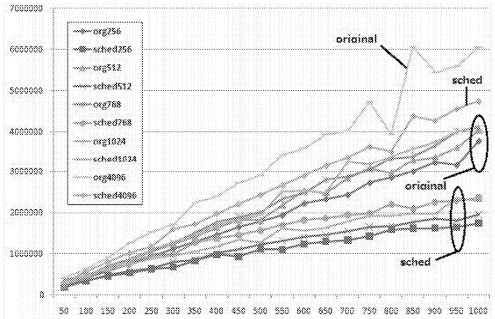

図３　同時に起動しているアプリケーションプロセスが 8 個

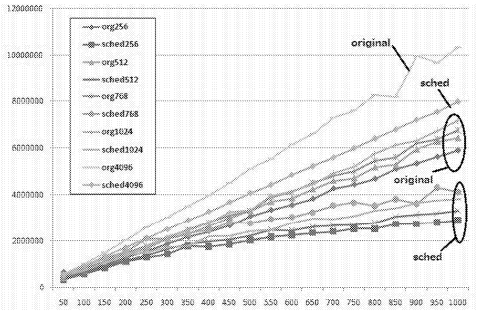

図４　同時に起動しているアプリケーションプロセスが 12 個

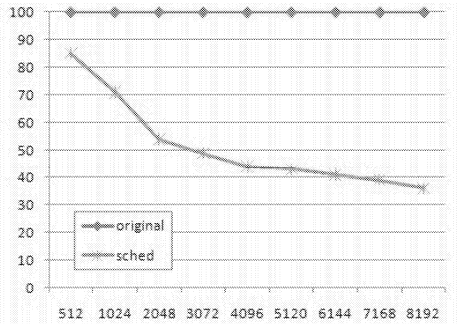

図５　CPU 利用率

また，オリジナルシステムと今回作成したシステムの２つのシステムにおいて，CPU 使用率を計測した結果を，図５ に示す．これは，今回作成したシステムにおいて，オフロードが有効である有意な結果である．

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１件）
①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　２０１０年掲載決定

〔学会発表〕（計１０件）
①杉浦 寛，大釜正裕，羅 鏡栄，齋藤孝道，CELL/B.E. での効率的な暗号モジュールの実装と評価，暗号と情報セキュリティシンポジウム概要集 p268，2010 年 1 月 22 日，サンポート高松．

②羅 鏡栄，杉浦 寛，大釜正裕，齋藤孝道，UltraSPARC T2 における暗号モジュールの利用と評価，暗号と情報セキュリティシンポジウム概要集 p267，2010 年 1 月 22 日，サンポート高松．

③杉浦 寛，大釜正裕，羅 鏡栄，齋藤孝道 CELL/B.E. での効率的な暗号モジュールの実装と評価，第 72 回情報処理学会全国大会公演論文集(3)pp647-648，2010 年 3 月 8 日，東京大学．

④羅 鏡栄，杉浦 寛，大釜正裕，齋藤孝道 UltraSPARC T2 における暗号モジュールの利用と評価，第 72 回情報処理学会全国大会公演論文集（1）pp143-144，2010 年 3 月 8 日，東京大学．

⑤村上智祐，笠原竜大，杉浦 寛，大釜正裕，羅 鏡栄，齋藤孝道，GPGPU での暗号アルゴリズムの実装と評価，第 72 回情報処理学会全国大会公演論文集（1）pp57-58，2010 年 3 月 8 日，東京大学．

⑥杉浦，齋藤，大釜，羅，関口，Cell/B.E. での AES 処理のオフロードの実装と評価，組込みシステムシンポジウム 2008(ESS2008)予稿集，2008 年 10 月 29 日，国立オリンピック記念青少年総合センター．

⑦羅 鏡栄，大釜 正裕，杉浦 寛，関口 聖美，齋藤 孝道，MPC8272 における暗号モジュ

ールの利用と評価，マルチメディア通信と分散処理ワークショップ論文集，2008 年 12 月 10 日，山口県萩市.

⑧大釜 正裕，杉浦 寛，羅 鏡栄，関口 聖美，黒羽 秀一，齋藤 孝道，IXP425 上での暗号ミドルウェア OCF のスケジューラの実装と評価，マルチメディア通信と分散処理ワークショップ論文集，2008 年 12 月 10 日，山口県萩市.

⑨杉浦 寛，大釜 正裕，羅 鏡栄，齋藤 孝道，Cell/B.E.での OpenSSL 暗号処理のオフロードの実装と評価，マルチメディア通信と分散処理ワークショップ論文集，2008 年 12 月 10 日，山口県萩市.

⑩黒羽 秀一，齋藤 孝道，IXP425 における XScale 利用時の暗号モジュールへの影響，組込みシステムシンポジウム予稿集，2007 年 10 月 18 日，独立行政法人科学技術振興機構 日本科学未来館

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