CAM を付加した超並列 SIMD プロセッサによる AES 処理高速化手法 (2) ～復号化方法～

石崎雅勝† 田上正治† 熊木武志† 小出哲士† マタウシュハンスユルゲン†
行天隆幸†† 野田英行†† 堂阪勝己†† 有本和民†† 齊藤和則††
† 広島大学 ナノデバイス・システム研究センター〒739-8527 東広島市鏡山 1-4-2
†† 株式会社 ルネサステクノロジ システムソリューション統括本部 〒664-0005 兵庫県伊丹市瑞原 4-1

1 はじめに

近年，デジタルカメラや携帯電話などの普及にともない，取り扱うデータ量が肥大化すると同時に新たな規格が次々と出現している．これらに対応するために我々は，超並列 Single Instruction Multiple Data (SIMD) プロセッサ[1] の開発を行ってきた．超並列 SIMD プロセッサは大量のデータに対し同様の演算を繰り返し処理するマルチメディアアプリケーションに特化させた構造となっている．また，逐次処理にも適用できるように Content Addressable Memory (CAM) を付加し，画像の標準規格である JPEG においては従来の Digital Signal Processor (DSP) と比較し，約 7.1 倍の処理性能が確認できている[2].

我々は超並列 SIMD プロセッサのプログラマブル性を活かすために，近年注目されている暗号化アルゴリズムへと適用することを検討した．本稿では CAM を付加した超並列 SIMD プロセッサによって National Institute of Standards and Technology (NIST) にて選定された暗号規格である Advanced Encryption Standard (AES) [3] を暗号化[3], 復号化する方法の提案を行い，シミュレーションによる評価を行った．その結果スループットは 81.92 Mbps となり，Pentium4 [5]と比較して，周波数あたりのスループットが約 11 倍という結果が得られた.

2 CAM を付加した超並列 SIMD プロセッサ

超並列 SIMD プロセッサは，モバイル機器向けに開発され，動作周波数 200 MHz において 250 mW と低消費電力ながら，40 GOPS という高い処理性能を実現している．更に CAM を付加することで，マルチメディアデータの処理に多いテーブル変換処理の高速化を図っている．図 1 に CAM を付加した超並列 SIMD プロセッサのブロック図を示す．超並列 SIMD プロセッサは，演算を行う超並列 SIMD プロセッサコア，制御を行うコントローラ，システムバスとのインタフェースを行う TS (time Space converter bus)ブリッジで構成される．システムバスから入力されたデータは TS ブリッジにより通常の 1 ワードごとの形からビットシリアル・ワードパラレルに変換され超並列 SIMD プロセッサコアに送信される．超並列 SIMD プロセッサコアでは 2,048 並列に各 Processing Element(PE) 内で 2 ビット単位に処理される．CAM を使用する場合は TS ブリッジ内の直交 SRAM にデータを格納することで，データをビットシリアル・ワードパラレルの状態から 1 ワード単位に変換し，一致検索を行う.

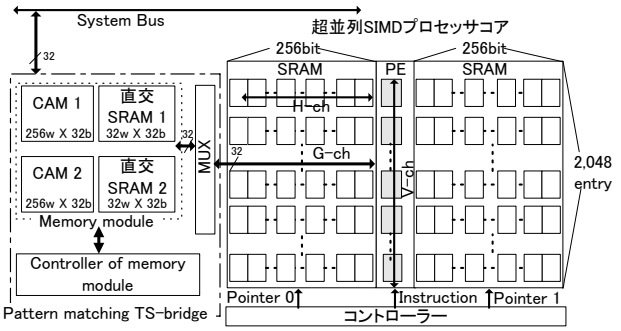

図 1 CAM を付加した超並列 SIMD プロセッサ

3 AES 復号化アルゴリズムの概要

AES では暗号化と逆の処理を行うことで復号化を実現する．ラウンドと呼ばれる処理単位を複数回繰り返し行い，各ラウンドは暗号化処理における Sub Bytes, Shift Row, Mix Column, Add Round Key の逆処理である Inv Sub Bytes, Inv Shift Row, Inv Mix Column, Inv Add Round Key から構成される.

Inv Sub Bytes 処理では暗号化時に用いたS-boxテーブルの逆のテーブルS^{-1}-boxテーブルを用いて 1 byte ごとに非線形変換を行う. Inv Shift Row 処理では 32bit内でシフトを行い, Inv Mix Column 処理では暗号化時に用いた行列の逆行列を掛けることで演算を行う. Inv Add Round Key 処理では暗号化時に用いられたラウンド鍵との排他的論理和演算を行う.

4 超並列 SIMD プロセッサによる AES 復号化

超並列 SIMD プロセッサによる AES 復号化では，2,048 エントリそれぞれに 1 つのブロック(128 bit) を格納し 2,048 並列で処理を行う．以下では各処理についてその詳細を述べる.

(i) Inv Sub Bytes : この処理ではインタフェースモジュール内のCAMを用いる．暗号化時にはCAMの一致検索機能を利用し，S-Box前のデータを一致検索しアドレスを変換後データとしたが，復号化時はS^{-1}-Box前のデータをアドレスとして入力し，CAMからデータを出力する．このように処理することで，CAM内部のデータ入れ替えを全く行わずにS-Box, S^{-1}-Box 処理が可能である[4]. 図２にインタフェースモジュールによるInv Sub Bytes 処理の概要を示す.

a) 超並列SIMDプロセッサコアから直交SRAM0 に Inv Sub Bytes 処理前のデータを送信する.

b) 直交 SRAM 内のデータをビットシリアル・ワードパラレルからビットパラレル・ワードシリ

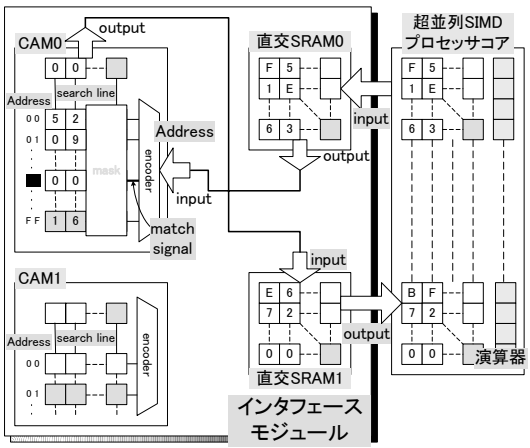

図２　インタフェースモジュールによる
Inv Sub Bytes 処理

アルに変更し読み出す.

c) CAM0 のアドレス信号に入力することで Inv Sub Bytes 後のデータを読み出す.

d) 直交 SRAM1 に出力されたデータを格納する.

e) 直交 SRAM1 から超並列 SIMD プロセッサにデータを返信する.

以上の工程をパイプラインで処理する．インタフェースモジュールに CAM を付加しているため，逐次演算が苦手な SIMD プロセッサでも高速にテーブル変換処理が可能である．また，専用の追加ハードウェアを全く必要とせずに暗号化・復号化が可能である.

(ii) Inv Shift Row：1 ブロックが 1 エントリに格納されているため，Inv Mix Column 時の格納位置を Inv Shift Row 後の位置にすることでクロックをかけずに処理が可能である.

(iii) Inv Mix Column：Inv Mix Column 処理に用いる行列は

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0D & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix}$$

と表せる．ここで c は処理後のデータ， d は

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} + \begin{bmatrix} 08 & 08 & 08 & 08 \\ 08 & 08 & 08 & 08 \\ 08 & 08 & 08 & 08 \\ 08 & 08 & 08 & 08 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} + \begin{bmatrix} 04 & 00 & 04 & 00 \\ 00 & 04 & 00 & 04 \\ 04 & 00 & 04 & 00 \\ 00 & 04 & 00 & 04 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix}$$

処理前のデータを示す．この行列は

と変形でき，超並列 SIMD プロセッサ上で高速に処理できるシフトにより構成されている．Inv Mix Column 前のデータ d を 1bit シフトすることで"d×02"の演算が可能である．次に"d×02"を 1bit シフトすることで"d×04"とする．さらに"d×04"を 1bit シフトすることで"d×08"のデータを生成する．これらのデータを行列に従って排他的論理和をとることで処理を行う.

(iv) Inv Add Round Key 処理：ラウンド鍵を各 PE にブロードキャストし 2,048 並列で処理を行う.

表１　AES 復号化結果

処理データ量	[bit]	262,144
動作周波数	[MHz]	200
合計クロックサイクル数	[clock cycles]	639,994
スループット	[Mbps]	81.92
単位面積当たりのスループット	[Mbps/mm^2]	21.56

表２　AES 復号化性能比較

	CAMを付加した超並列SIMDプロセッサ	Pentium4[5]
動作周波数 [MHz]	200	2400
暗号化スループット [Mbps]	122.78	106.79
復号化スループット [Mbps]	81.92	89.38
動作周波数当たりの暗号化スループット [bps/Hz]	0.614	0.044
動作周波数当たりの復号化スループット [bps/Hz]	0.410	0.037

5　シミュレーションによる性能評価

４章で述べた処理方法を, 超並列SIMDプロセッサの機能シミュレータを用いて性能を評価した．超並列SIMDプロセッサではAESのデータ 128 bitを 2,048 並列に処理を行うため, 処理するデータ量を 262,144 bit としている．表１に復号化処理結果を示す．動作周波数 200 MHzでのスループットは 81.92 Mbps となった．また単位面積あたりのスループットは 21.56 Mbps/mm^{2}となった．表２に性能比較結果を示す．復号化スループットは動作周波数 2.4 GHz の Pentium4[5]と比較しても遜色のない値である．また, 周波数当たりのスループットに換算すると, 約 11 倍となり，CAMを付加した超並列SIMDプロセッサの有効性が示された.

6　まとめ

CAM を付加した超並列 SIMD プロセッサによる AES 復号化処理高速化手法について述べた．マルチメディア用に開発された超並列 SIMD プロセッサを用いて CAM 内のデータの入れ替え無しに暗号化, 復号化を実現可能であり, 復号化スループット 81.92 Mbps と高速に実現できることがわかった.

謝辞

本研究の一部は, 文部科学省 先端融合領域イノベーション創出拠点の形成『半導体・バイオ融合集積化技術の構築プロジェクト』により行われた.

参考文献

[1] M. Nakajima et al.,“A 40 GOPS 250 mW massively parallel processor based on matrix architecture”, ISSCC Dig. Tech. Papers, Paper, pp. 410-411, 2006.

[2] 幸野豊, 他“CAM による高速パターンマッチング機能を有する超並列 SIMD プロセッサ”, 信学技報, IcD2006-116, pp. 39-44, Oct. 2006.

[3] 田上, 他“CAM を付加した超並列 SIMD プロセッサによる AES 処理高速化手法(1),”本大会予稿

[4] Hua Li, "A New CAM Based S/S-1-Box Look-up Table in AES", ISCAS, pp. 4634-4636, 2005.

[5] VIA Technologies Inc., VIA PadLock Hardware Security Suite. http://www.via.com.tw/en/initiatives/padlock/hardware.jsp.