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) ～暗号化方法～

田上正治† 石崎雅勝† 熊木武志† 幸野豊† 小出哲士† Hans. Juergen. Mattausch†
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，マルチメディアの分野において，MPEG4, H.264 など高品質な標準規格が次々と出現している．従来に比べ，短期間で規格が変更されていくため，これらの規格に対応していくにあたっては，プログラマブルでハイパフォーマンスな VLSI が必要となる．この要求を満たすアーキテクチャとして，現在，我々が開発している超並列 SIMD プロセッサ[1]がある．超並列 SIMD プロセッサは，大量のデータに対して同一の演算を行うことが多いマルチメディアアプリケーションに対して，従来のモバイル向けプロセッサに比べ，低消費電力で高速に処理できる[2].

本論文では，マルチメディア処理に用いたものと同様のアーキテクチャを用いて，代表的な暗号化アルゴリズムである AES を処理する方法を提案し，シミュレーションにより評価を行った．

2　超並列 SIMD プロセッサ

超並列 SIMD プロセッサは，主にモバイル情報機器に搭載する事を目的としており，動作周波数 200 MHz で消費電力 250 mW，処理性能が 40 GOPS であり，従来のモバイル向けプロセッサと比較して有効である[2]．図 1 に超並列 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，演算処理部の SIMD プロセッサコア，コア制御部のコントローラ，入出力部の TS (Time Space converter bus) ブリッジで構成されている．CPU から入力されるデータは，TS ブリッジによりビットパラレル・ワードシリアルからビットシリアル・ワードパラレルに変換され, SIMD プロセッサコア内の SRAM に格納される．格納されたデータは，2 ビット単位で PE (Processing Element) により演算される．エントリ毎に 2 ビット演算器と SRAM を密結合することで, 並列度が 2,048 と高い並列度でありながら, 小面積を実現している．

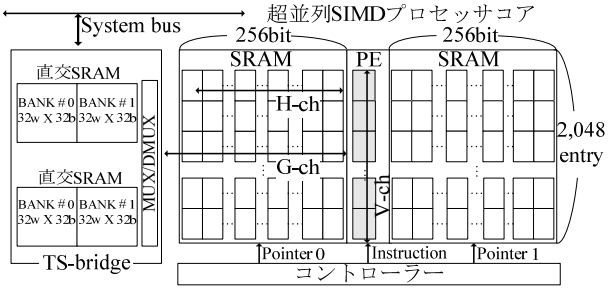

図 1　超並列 SIMD プロセッサ.

3　Advanced Encryption Standard (AES)

AES は，ブロックと呼ばれる 128 ビットのデータを 1 単位として暗号化/復号化を行うブロック暗号であり，128 ビットを 8 ビットずつに区切り，SubBytes（非線形変換処理），ShiftRows（シフト処理），MixColumns（行列演算処理）, AddRoundKey(XOR 演算処理) の 4 処理を繰り返し行う．

4　超並列 SIMD プロセッサによる AES 処理

超並列 SIMD プロセッサによる AES 処理は，1 ブロック 128 ビットを 1 エントリに格納し, 2,048 並列で暗号化を行う. AES の各処理結果を表 1 に示す[3].

表 1 から SIMD 処理が難しい SubBytes は，処理クロックサイクル数が大きく，SIMD 処理に適した他の処理は，クロックサイクル数が小さいことがわかる．また，SubBytes 処理は，全体の 94%のクロックサイクル数を占めており，SubBytes 処理のクロックサイクル数削減が，AES 処理の高速化の鍵となる．

表 1　超並列 SIMD プロセッサによる AES 処理.

Processing data	[bit]	262,144
Initialize and input data	[clock cycles]	8,225 (0.65 %)
SubBytes	[clock cycles]	190,090 (94.17 %)
ShiftRows	[clock cycles]	0 (0 %)
MixColumns	[clock cycles]	53,496 (4.23 %)
AddRoundKey	[clock cycles]	9,856 (0.78 %)
Output data	[clock cycles]	2,081 (0.16 %)
Total clock cycle	[clock cycles]	1,263,748
Throughput @ 200MHz	[Mbps]	41.49

5　CAM を有する超並列 SIMD プロセッサ

4 章より AES において SubBytes 処理がボトルネックになっていることがわかった．我々は，この問題を解決するために，図 2 に示すマルチメディア処理で用いた Content Adressable Memory (CAM) を入出力部の TS ブリッジに付加した超並列 SIMD プロセッサを使用する．パターンマッチング TS ブリッジの面積は，0.39 mm^2 となっており,TS ブリッジの約 22 %の面積増加で実現できる[2]．CAM とは，入力されたデータと CAM 内に格納されたデータの比較を行い，一致したデータが格納されているアドレスを出力するものである．そのため，SubBytes 変換のようなテーブル変換処理を行う際に，データとアドレスをテーブルの表に対応させて格納させておくことで，1 クロックで処理することが出来る．図 3 に

CAM を用いた SubBytes 処理の流れを示す.

- **Step1.** 超並列 SIMD プロセッサから SRAM0 に SubBytes 処理前のデータを出力する.
- **Step2.** 直交 SRAM0 でデータの流れをビットシリアル・ワードパラレルからビットパラレル・ワードシリアルに変換する.
- **Step3.** 直交 SRAM0 から SubBytes 変換のために CAM0 及び CAM1 にデータを出力する.
- **Step4.** CAM0 及び CAM1 で SubBytes 変換を行う.
- **Step5.** CAM0 及び CAM1 は，変換されたデータ，すなわち一致アドレスを直交 SRAM1 に出力する.
- **Step6.** 直交 SRAM1 は，変換されたデータをビットシリアル・ワードパラレルで超並列 SIMD プロセッサに返信する.

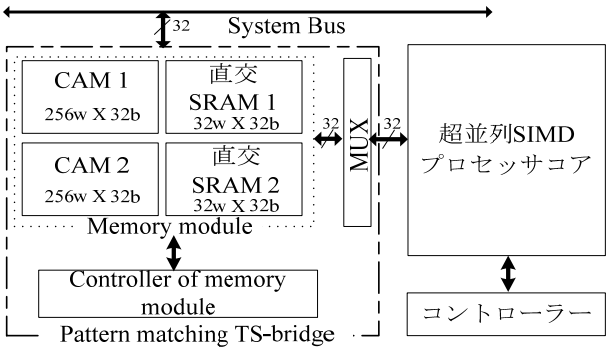

図 2　CAM を付加した超並列 SIMD プロセッサ.

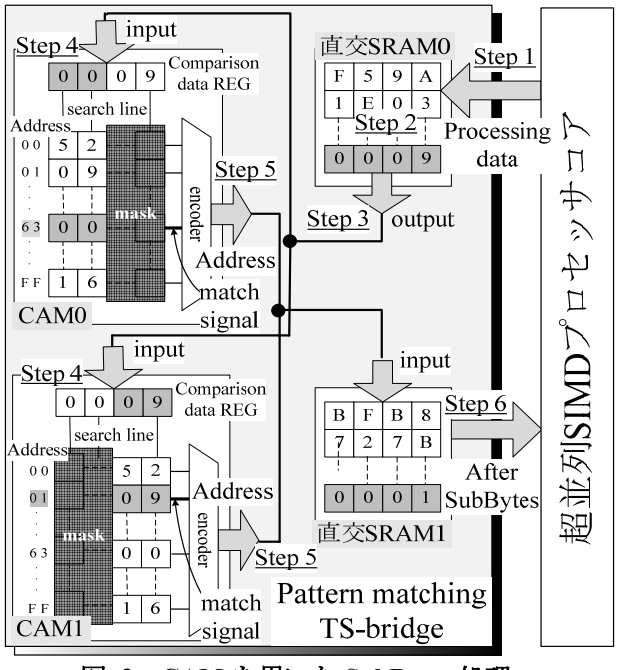

図 3　CAM を用いた SubBytes 処理.

6　シミュレーションによる性能評価

超並列 SIMD プロセッサの機能シミュレータを用いて，鍵長 128 ビットの AES 暗号化のスループットを導出した．表 2 に CAM 有り及び CAM 無し[3]の超並列 SIMD プロセッサによる AES 処理結果を示す．CAM を用いることで，SubBytes 処理が約 70 % 削減でき，スループットが約 3 倍，単位面積当たりのスループットも約 2.4 倍の結果となった．また，表 3 に Pentium-pro と, DSP との比較結果を示す [4]. CAM を付加することで，スループットが向上し，有効性が示された.

表 2　CAM の有無による AES 処理結果の比較.

Platform		CAM無し	CAM有り
Processing data	[bit]	262,144	262,144
Initialize and input data	[clock cycles]	8,225	8,225
SubBytes	[clock cycles]	1,190,090	353,360
ShiftRows	[clock cycles]	0	0
MixColumns	[clock cycles]	53,496	53,496
AddRoundKey	[clock cycles]	9,856	9,856
Output data	[clock cycles]	2,081	2,081
Total clock cycle	[clock cycles]	1,263,748	427,018
Throughput @ 200 MHz	[Mbps]	41.49	122.78
Throughput/area	[Mbps/mm^2]	13.38	34.79

表 3　AES 処理性能比較.

Platform	Frequency [MHz]	Throughput [Mbps]
超並列SIMDプロセッサ [3]	200	41.5
CAMを付加した超並列SIMDプロセッサ	200	122.8
Pentium-Pro [4]	200	70.5
DSP (TMS320C6201) [4]	200	112.3

7　まとめ

本研究では，メディア処理専用 LSI である超並列 SIMD プロセッサによる AES 処理アルゴリズムの高速化の提案と評価を行った．マルチメディア処理で用いた CAM を用いることにより，AES 処理のスループットが約 123 Mbps となり，Pentium-pro と比べて約 1.7 倍，DSP と比較して約 1.1 倍となった．これらにより, CAM を付加した超並列 SIMD プロセッサの有効性が示された.

謝辞

本研究は, 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 40GOPS 250mW 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, pp. 39-44，2006.

[3] 田上正治，他“超並列 SIMD プロセッサによる暗号化(AES)処理の一手法”，Proceedings of the 2007 IEICE General Conference, C-12-9, pp88.

[4] T. Wollinger et al., “How well are high-end DSPs suited for the AES algorithms?,” Proceedings of 3rd AES conference, New York, pages 94-105, April 2000.