ブロック暗号アルゴリズム実装性能評価

中嶋純子*
松井　充**

Performance Evaluation of Block Encryption Algorithms on Core2

Junko Nakajima, Mitsuru Matsui

要　旨

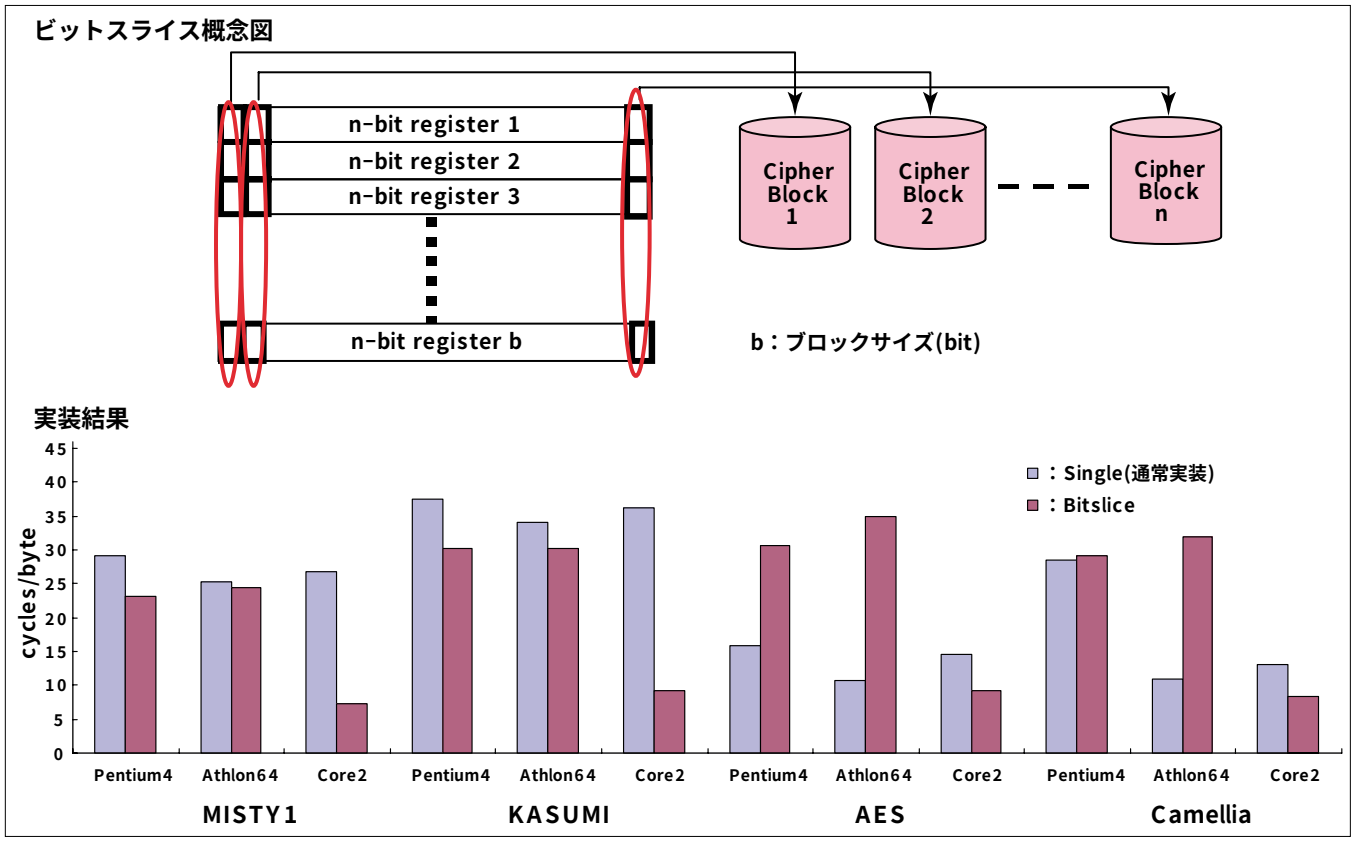
ブロック暗号のソフトウェアによる高速化手法である“ビットスライス実装”を，Intel(注1)の新しいプロセッサCore 2 (注1)に適用した結果について述べる。ビットスライス実装はこれまでRISC(Reduced Instruction Set Computer)プロセッサ上で特に有効性が実証されてきた一方で，PC(x86)プロセッサ上では次に示す理由によってあまり利用されることがなかった。

(1) PCプロセッサはレジスタ数が少ないため，ビットスライス実装ではメモリアクセスの頻度が高くなり，これが速度のボトルネックになる。

(2) ビットスライス実装は特殊なデータフォーマットを利用するので，既存の実装とデータの互換性を保持するためには，暗号化／復号処理の前後にフォーマット変換処理を必要とする。

本稿ではCore 2 プロセッサで大幅に強化されたSIMD(Single Instruction Multiple Data)整数命令を用いて(1)(2)の課題がともに克服できることを明らかにする。またこの結果KASUMIが通常の実装の４倍高速化できること，AES(Advanced Encryption Standard)でも既存の結果よりも高速な実装がビットスライスで実現できることを示す。ビットスライス実装は，その潜在的な高速性のみならず，今後暗号化モードとして主流になるとみられるCTR(CounTeR)モードなどで使用可能であることに加えて，キャッシュ攻撃のようなサイドチャネル攻撃に対して安全であるという有効な長所も備えているため，今後実用面でもますます重要になると考えられる。

(注１)　Intel，Coreは，Intel Corp.の登録商標及び商標である。



ブロック暗号アルゴリズム実装性能評価

ビットスライス実装の基本的概念を上図に示す。ビットスライス実装ではn-bit長のCPU(Central Processing Unit)レジスタを用いて，nブロック分のデータを並列に処理する。このとき，ソフトウェア１命令が，n個のハードウェアロジックゲートに相当する演算となる。また上記グラフはブロック暗号アルゴリズム(MISTY1，KASUMI，AES，Camellia)を各種プロセッサ上で実装した結果を示す。ビットスライス実装をCore2に適用した結果，KASUMIが通常の実装の4倍高速化でき，AESでも従来よりも高速な実装を実現した。

*情報技術総合研究所　**同研究所(情報理工博)