発表概要

SIMD並列表引き参照命令向けコンパイラ最適化

黒田 和宏[1,a)]　安仁屋 宗石[2]　鈴木 貢[3]

2012年1月24日発表

規格化されて以来，AESは世界的に最も一般的な暗号化アルゴリズムの1つである．しかしAESに対するIntel SSE等のメディア処理向けSIMD拡張命令セットを用いた高速化には限界がある．高速化の障害となっているのは，ガロア体GF(2^8)で満たされた256エントリのバイトデータ表S-boxを用いたSubBytes変換である．従来のSIMD命令セットには，SubBytesのような変換向けの並列な表引き命令が備わっていない．我々は，SIMD表引き命令の追加を提案し，FPGAを用いてMIPS命令セットアーキテクチャに実装したが，この命令を対象としたコンパイラ最適化は将来の課題として残された．そこで本発表では，COINSコンパイラインフラストラクチャを用いた実装方法を示し，最適化の手法を紹介する．

Compiler Optimization for SIMD Parallel Table Lookup Instructions

Kazuhiro Kuroda[1,a)]　Souseki Aniya[2]　Mitsugu Suzuki[3]

Presented: January 24, 2012

The AES has become one of the world's most popular encryption algorithms, since it had been adopted as a standard. But it has a limitation on fast processing with SIMD extended instruction sets for media processing such as Intel SSE and so on. The bottleneck on the processing is SubBytes transformation with S-box that is a 256 entries of byte data table making up a Galois field GF(2^8); conventional SIMD instruction sets do not include parallel table lookup instructions for such transformation. While we proposed to add SIMD table lookup instruction and accompanying instructions, and implemented them on MIPS ISA with FPGA, compiler optimization targeting to this instruction was left to be a future work. Then, we present a method for the optimization, and show an implementation using COINS compiler infrastructure.

[1] 島根大学大学院総合理工学研究科数理・情報システム学専攻
Major of Mathematics and Computer Science, Interdisciplinary Graduate School of Science and Engineering, Shimane University, Matsue, Shimane 690–8504, Japan
[2] 広島市立大学大学院情報科学研究科情報工学専攻
Major of Computer and Network Engineering, Graduate School of Information Sciences, Hiroshima City University, Hiroshima 731–3194, Japan
[3] 島根大学総合理工学部数理・情報システム学科
Department of Mathematics and Computer Science, Interdisciplinary Faculty of Science and Engineering, Shimane University, Matsue, Shimane 690–8504, Japan
[a)] s109309@matsu.shimane-u.ac.jp