高位合成処理システム CCAP を用いた AES 暗号処理の高速化

神原弘之、梅原直人、中谷嵩之、石浦菜岐佐、冨山宏之

我々は C Compatible Architecture Prototyper (CCAP) 高位合成処理系を開発している。CCAP は、ANSI C で記述された組込みソフトウェアについて、プロセッサによる解釈実行より高速であり、かつ回路規模がコンパクトな専用ハードウェアを、もとのプログラムを変更することなく生成することを目指している。CCAP では、生成された専用ハードウェアとプロセッサへの主記憶へのアクセスを制御する CCAP 専用の調停回路を用意している。これにより、生成された専用ハードウェアは、ハードウェア設計者の助力がなくともプロセッサと一体化されてもとのソフトウェアと同じように実行結果を得ることができる。本稿では、この CCAP を用いたシステム設計手法を AES 暗号処理の高速化に適用した結果について報告する。

Speed Improvement of AES Encryption using hardware accelerators synthesized by C Compatible Architecture Prototyper (CCPA)

Hiroyuki Kanbara, Naoto Umehara, Takayuki Nakatani, Nagisa Ishiura, and Hiroyuki Tomiyama

The authors are developing a high-level synthesizer called C Compatible Architecture Prototyper (CCAP). CCAP compiles ANSI C program which is a part of embedded software generates an application specific hardware accelarator in HDL. Synthesized accelarator executes faster than a cpu and accesses to main memory like a cpu. CCAP offers an arbiter circuit which makes it possible for the synthesized accelarator and a cpu to access main memory in parallel. In this paper we report the speed improvement of AES Encryption using CCAP.