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

Hiroyuki KANBARA, Takayuki NAKATANI, Naoto UMEHARA, Nagisa ISHIURA, 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 and generates an application specific hardware accelerator in HDL. Synthesized accelerator has an ability to read/write main memory and executes calculation faster than embedded processor. CCAP offers an arbiter circuit which makes it possible for the synthesized accelerator and a processor to access main memory in parallel. In this paper we report the speed improvement of AES Encryption using design methodology of CCAP synthesizer.