Abstract

Security is becoming a de-facto requirement of System-on-Chips (SoC), leading up to a significant share of circuit design cost. In this article, we propose an advanced SBUS protocol (ASBUS), to improve the data feeding efficiency of the Advanced Encryption Standard (AES) encrypted circuits. As a case study, the direct memory access (DMA) combined with AES engine and memory controller are implemented as our design-under-test (DUT) using field-programmable gate arrays (FPGA). The results show that our presented ASBUS structure outperforms the AXI-based design for cipher tests. As an example, the 32-bit ASBUS design costs less in terms of hardware resources and achieves higher throughput (1.30 ×) than the 32-bit AXI implementation, and the dynamic energy consumed by the ASBUS cipher test is reduced to 71.27% compared with the AXI test.