Abstract

This paper proposes a high efficiency data bus (DBUS) for Advanced Encryption Standard (AES) encrypted system-on-chips (SoCs). Using DBUS, the data sequence can be pre-selected for AES encryption/decryption, so that the state buffering and rescheduling overhead can be reduced. FPGA results show that the DBUS based design lowers the dynamic energy to 66.93%, and achieves up to 1.30 times higher valid throughput compared with the Advanced eXensible Interface (AXI) based implementation.