



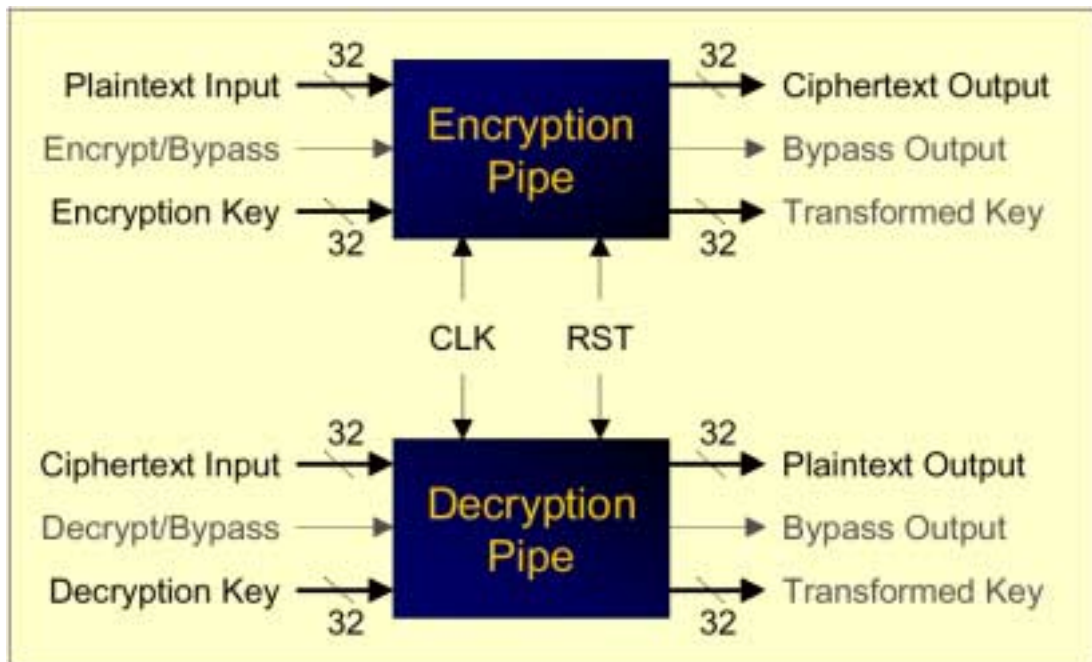
Summary

D'Crypt's AES core is a high-performance pipelined implementation of the AES (Rijndael) encryption algorithm. Optimized for PLD architectures, the core achieves in excess of 2.5Gbit/s encryption and decryption throughput on 128-bit block-sizes when implemented on Altera APEX 20KE or equivalent devices. It employs a 128-bit key and features zero key-setup latency on both encryption and decryption. With key-agility and selective bypass control, D'Crypt's AES core is the ideal building block for high-performance packet-smart routers and switches.

Features

- >2.5Gbit/s throughput for fiber-speed encryption
- Key-agility on both encryption & decryption allows keys to be switched without stalling the core
- Simple streaming architecture obviates the need for elaborate control logic outside the core
- Bypass control allows data flow-through for selective encryption
- Simple 32-bit data and key ports reduce logic required to interface to high-speed standards

Block Diagram



For more information, please contact:

D'Crypt Pte Ltd. 20 Ayer Rajah Crescent, #08-08 Technopreneur Centre, Singapore 139964.
Phone: +65 773 9016, Fax: +65 873 0796, Email: ipcore@d-crypt.com, Web Site: www.d-crypt.com