

3DES/DES Core

Tallika's 3DES/DES core is a silicon proven, flexible and scalable solution built by experts with years of experience in building security solutions for commercial as well as government applications in Networking, Storage and Consumer market segments.

Features:

- ◆ Fully compliant with NIST FIPS PUB 46-3, CBC/ECB modes in NIST PUB 81
- ◆ 56-bit DES and 168-bit Triple-DES implementations
- ◆ Supports both encryption and decryption
- ◆ User configurable for number of ciphers per cycle to suite design requirements
- ◆ Provides ability to pre-load Initialization Vector (IV)
- ◆ Single channel provides 4 Gbps throughput for DES and 1.33 Gbps throughput for TDES in @250 MHz in 0.13u
- ◆ Suitable for insertion in pipelined designs
- ◆ Provides ability to pass cleartext and upto 16 bits of control information through the DES pipeline
- ◆ No dead cycles for key loading or mode switching
- ◆ Suitable for Electronic Codebook (ECB), Cipher Block Chaining (CBC), CFB and OFB implementations

Deliverables:

- ◆ Verilog RTL
- ◆ Testbench
- ◆ Primetime and DC scripts

TALLIKA CORPORATION

2222 S. Dobson Rd, Suite 1103
Mesa, AZ 85202

Phone: 480 422 5410

www.tallika.com

Email: sales@tallika.com

Product Brief