CoreDES v3.0

Handbook

Actel
POWER MATTERS

Actel Corporation, Mountain View, CA 94043

Printed in the United States of America

Part Number: 50200151-0

Release: March 2009

Trademarks

Table of Contents

Introduction

The CoreDES macro implements the Data Encryption Standard (DES), which provides a means of securing data. The DES algorithm is described in Federal Information Processing Standards (FIPS) Publication (PUB) 46-3. The algorithm takes as input 64 bits of plaintext data and 64 bits of a cipher key (only 56 of the 64 bits of the key are used in the calculations, as the least significant bit of each byte of the cipher key is used to provide odd-parity for the key bytes) and after 16 cycles, produces a 64-bit ciphered version of the original plaintext data as output.

During the 16 cycles or iterations of the algorithm, the data bits are subjected to permutation and addition functions, which consist of key schedules, calculated by rotations and permutations applied to the original 56-bit cipher key. Figure 1 illustrates the 16-iteration DES algorithm, as described in detail in FIPS PUB 46-3.

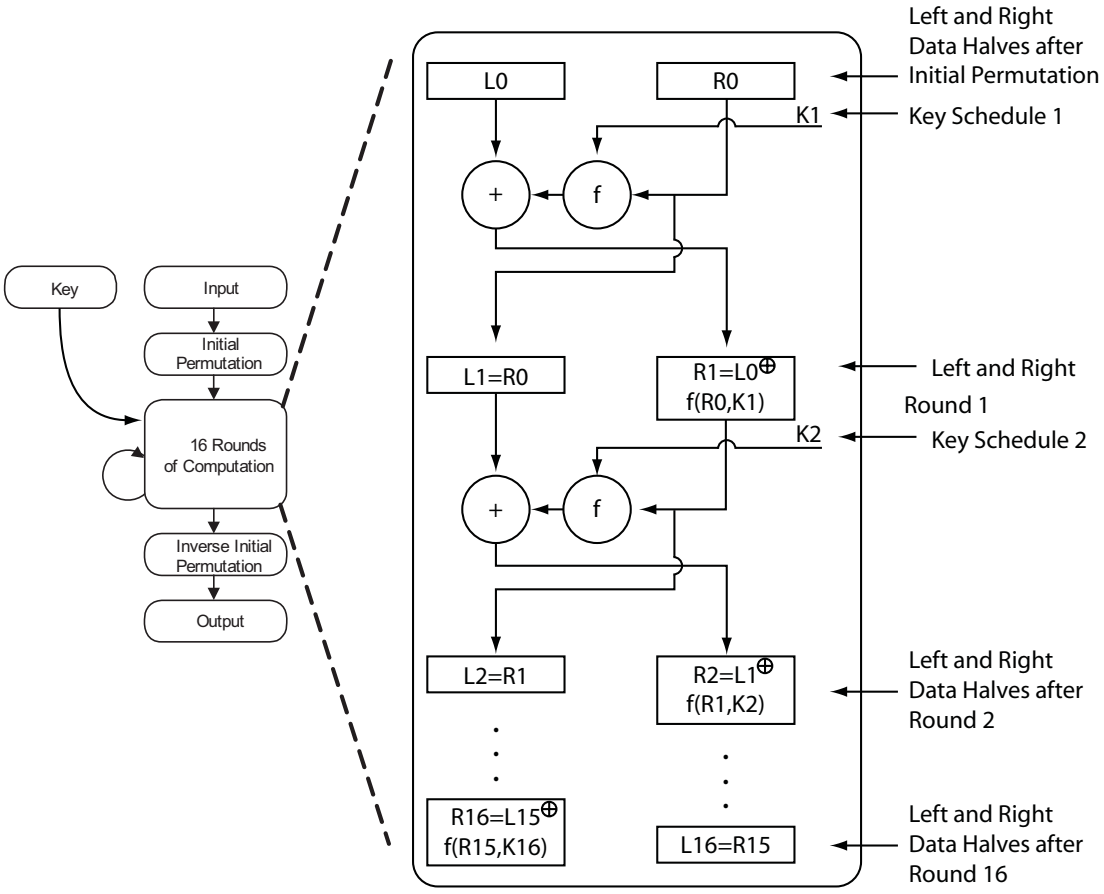

Figure 1 · DES Algorithm

Design Security

Figure 2 shows a typical system diagram. Note that the cipher key, which is the "secret" key, can be made up of FPGA logic cells, thereby preventing the possibility of design or data theft. Actel Flash-based devices (ProASIC3) employ FlashLock™ technology, and Actel antifuse-based devices (Axcelerator, SX-A, RT54SX-S) employ FuseLock™ technology, each of which provides a means to keep the cipher key and the rest of the logic secure. The output of the

CoreDES macro should be connected to registers or FIFOs, as it is only valid for one clock cycle, as shown in the sections "Encryption" and "Decryption".

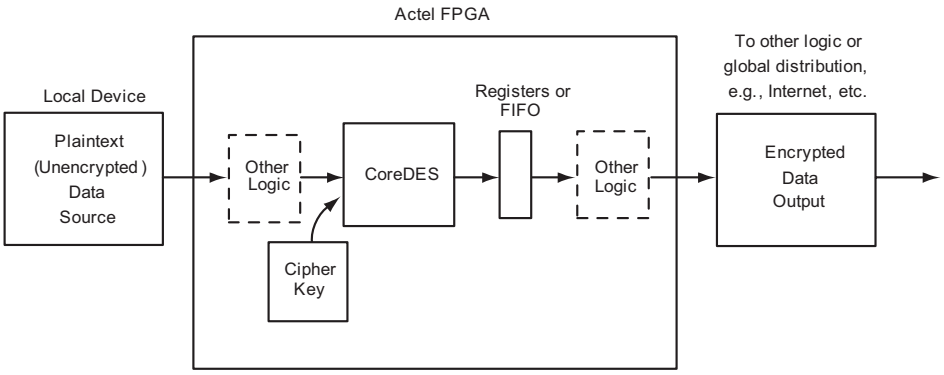

Figure 2 · Typical CoreDES System

Key Features

- 56-bit cipher key (with 8 additional parity bits)
- Parity Checking Logic for cipher key
- Encryption and decryption possible with same core
- 16-Clock cycle operation to encrypt or decrypt 64-bits of data
- Pause/Resume functionality to continue encryption or decryption at will
- Compliant with FIPS PUB 46-3
- ECB (Electronic Codebook) implementation per FIPS PUB 81
- Example source code provided for CBC, CFB and OFB Modes
- Provides data security within a secure Actel FPGA

Core Version

This handbook supports CoreDES version 3.0.

Supported Families

IGLOO® FPGAs
IGLOOe FPGAs
IGLOO PLUS FPGAs
Fusion FPGAs
ProASIC®3 FPGAs
ProASIC3E FPGAs
ProASIC3L FPGAs
Axcelerator® FPGAs
RTAX-S FPGAs
ProASIC PLUS® FPGAs

RTSX-S FPGAs
SX-A FPGAs

Device Utilization and Performance

The CoreDES macro has been implemented in the families listed in Table 1.

Table 1 · CoreDES Device Utilization and Performance

Family	Cells or Tiles			Utilization		Performance	Throughput
	Sequential	Combinatorial	Total	Device	Total		
IGLOO/e	132	1055	1187	AGL600V2/ AGLE600V2	9%	45MHz	180Mbps
IGLOO PLUS	132	1055	1187	AGLP125V2	38%	45MHz	180Mbps
Fusion	148	1123	1271	AFS600	10%	80MHz	320Mbps
ProASIC3/E/L	148	1123	1271	A3P600/ A3PE600/ A3P600L	10%	80MHz	320Mbps
Axcelerator	141	601	742	AX125	37%	125MHz	500Mbps
RTAX-S	141	601	742	RTAX1000S	4%	74MHz	296Mbps
ProASIC^{PLUS}	142	1328	1470	APA075	48%	50MHz	200Mbps
SX-A	141	628	769	A545SX	53%	100MHz	400Mbps
RTSX-S	141	628	769	RT54SX32S	27%	55MHz	220Mbps

Note: Data in this table achieved using typical synthesis and layout settings

Data throughput is computed by taking the bit width of the data (64 bits), dividing by the number of cycles (16), and multiplying by the clock rate (performance); the result is listed in Mbps (millions of bits per second).

Design Description

I/O Signals

The port signals for the CoreDES macro are defined in Table 1-1 and illustrated in Figure 1-1. CoreDES has 200 I/O signals (described in Table 1-1). All arrayed ports are labeled with indices that begin with the number 1 (most significant bit) and ascend up to the width of the arrayed port (least significant bit, which happens to be 64 for all arrayed ports in this core). The arrayed ports are labeled in this fashion to correspond with the nomenclature described in Federal Information Processing Standards Publication 46-3 (FIPS PUB 46-3).

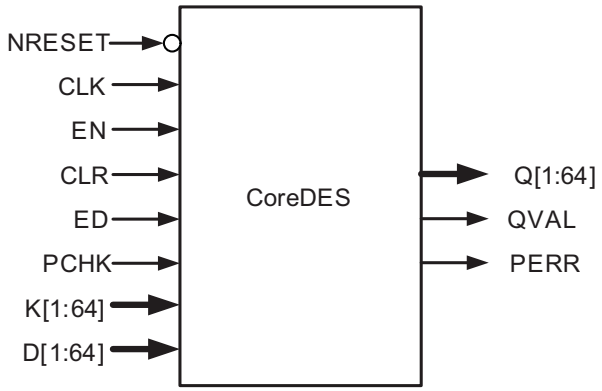

Figure 1-1 · CoreDES I/O Signal Diagram

Table 1-1 · CoreDES I/O Signals

Name	Type	Description
NRESET	Input	Active-low asynchronous reset
CLK	Input	System clock: reference clock for all internal design
EN	Input	Enable signal: set to '1' for normal continuous operation, set to '0' to pause
CLR	Input	Synchronous clear signal: set to '1' to clear logic at any time
ED	Input	Encryption/ Decryption: '1' to Encrypt, '0' to Decrypt
PCHK	Input	Parity check: set to '1' to enable parity checking of cipher key bits
K[1:64]	Input	Key: 64-bits (56 bits + 8 parity bits) cipher key input bus
D[1:64]	Input	Data In: 64-bits data input bus
Q[1:64]	Output	Data Out: 64-bits cipher test(for Encryption operation, plaintext for Decryption operation)
QVAL	Output	Q_Valid: '1' indicates that valid Encrypt/Decrypt data is available on Q_
PERR	Output	Parity Error: '1' indicates that a parity error has occurred on the K cipher key input bits

Parameters/Generics

CoreDES has a parameter (Verilog) and generic (VHDL), described in Table 1-2, for configuring the RTL code. A parameter and generic is an integer type. This parameter/generic is mapped to configuration options in the SmartDesign Configuration window.

Table 1-2 · CoreDES Configuration Parameter/Generic

Name	Values	Description
FAMILY	0 to 99	Must be set to match the supported FPGA family. IGLOO PLUS - 23 IGLOOe - 21 IGLOO - 20 Fusion - 17 ProASIC3L - 22 ProASIC3E - 16 ProASIC3 - 15 Axcelerator - 11 RTAX-S - 12 ProASICPLUS - 14 RTSX-S - 9 SX-A - 8

2 Functional Block Description

CoreDES consists of four main blocks (shown in Figure 2-1).

- Data schedule logic - computes the intermediate data values at each round of the DES algorithm.
- Iteration state machine logic - keeps track of which round of the DES algorithm is currently in progress.
- Key schedule logic - computes the intermediate keys at each round of the DES algorithm.
- Parity check logic - checks for odd-parity compliance of the 56 bits of cipher key and issues an error signal if parity is not correct.

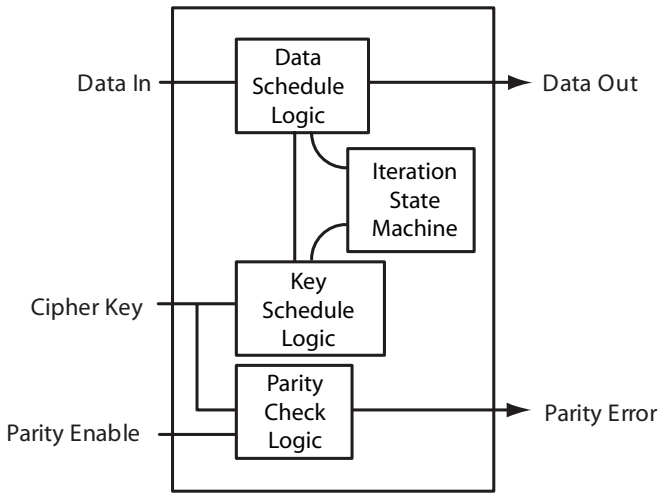

Figure 2-1 · DES Algorithm Block Diagram

CoreDES Operation

Parity Checking

If you want to use parity checking with the cipher key K[1:64] inputs, the PCHK input must be held at logic '1'. The parity checking logic determines whether or not an odd number of logic '1' values are present in each byte of the cipher key. This function can be disabled at any time by setting the PCHK input to logic '0'. Note that if parity checking is disabled by setting the PCHK input to logic '0,' the least significant bits of each byte of the cipher key (K[8], K[16], K[24], K[32], K[40], K[48], K[56], and K[64]) can each be statically connected to either a logic '1' or logic '0' value, since they are the parity bits and will not be used (Figure 3-1).

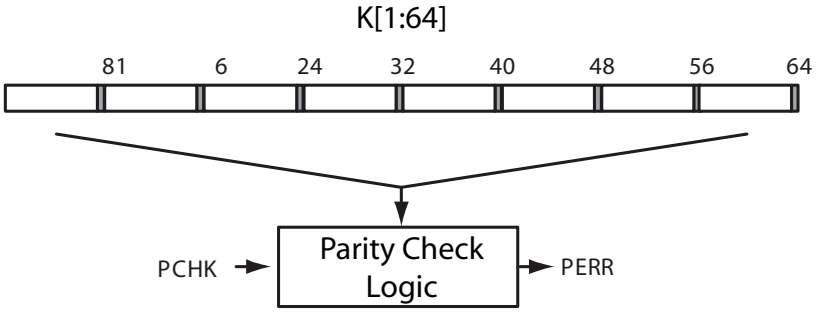

Figure 3-1 · Key Parity Check

Encryption

To begin the process of encrypting data, the following inputs are set:

1. K[1:64] is set to the cipher key (ck1 in Figure 3-2) to encrypt the data.
2. D[1:64] is set to the plaintext data (d1 in Figure 3-2) to be encrypted.
3. ED is set to logic '1'.
4. EN is set to logic '1'.

After 16 clock cycles of the EN input being held continuously at a logic '1' value, the QVAL signal transitions from logic '0' to logic '1' and remains valid for one clock cycle, indicating that valid ciphered (encrypted) data (shown as q1 in Figure 3-2) is available on the Q[1:64] outputs.

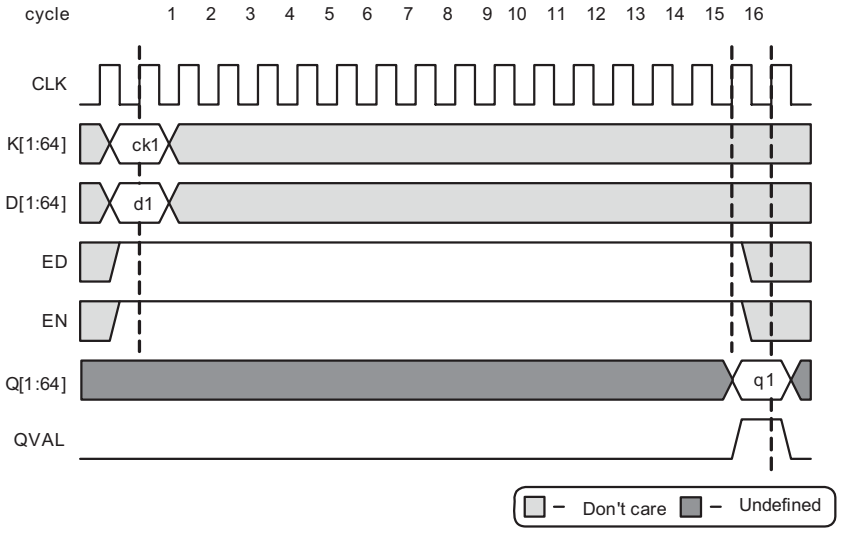

Figure 3-2 · Example Encryption Sequence

Decryption

To begin the process of decrypting data, set the following inputs :

1. K[1:64] is set to the cipher key (ck1 in Figure 7) to decrypt the data.
2. D[1:64] is set to the ciphertext data (d1 in Figure 7) to be decrypted.
3. ED is set to logic '0'.
4. EN is set to logic '1'.

After 16 clock cycles of the EN input being held continuously at a logic '1' value, the QVAL signal transitions from logic '0' to logic '1' and remains valid for one clock cycle, indicating that valid plaintext (unencrypted data shown as q1 in Figure 3-3) is available on the Q[1:64] outputs.

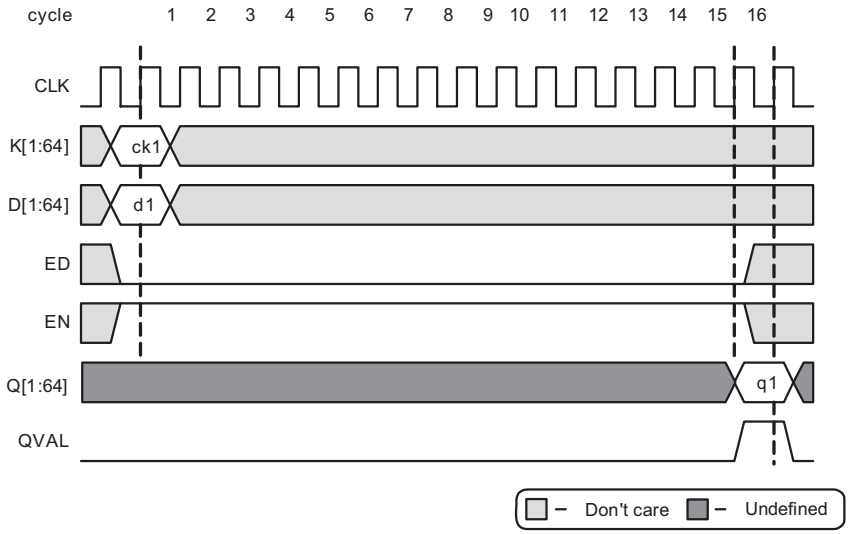

Figure 3-3 · Example Decryption Sequence

Pause/Resume

For normal operation, the EN input is held at a logic '1' value. The core can be paused by holding the EN input at a logic '0' value, indefinitely, as shown in Figure 3-4. To resume operation, the EN input should be brought back to a logic '1' value. This functionality applies to either encryption or decryption. Note that the ED input must remain at logic '1' throughout an entire encryption cycle, or at logic '0' throughout an entire decryption cycle; otherwise, unpredictable results on the Q[1:64] outputs will occur.

The pause/resume functionality is provided as an aid to you. One possible use for the pause functionality is the case where many blocks of data are encrypted one after another, for which the EN input can be held statically at a logic '1' value, the data input changing every 16 clock cycles to encrypt the next block. After all blocks of data are encrypted, the user would then need to hold the EN input at a logic '0' value, since if it is left at logic '1', data continues to be encrypted forever. When ready for the next blocks of data, you can then resume the encryption process by holding the EN input at a logic '1' value.

Another possible use is if you have an elastic buffer (FIFO) connected to the Q[1:64] outputs. If the FIFO is filling up with encrypted data faster than the encrypted data is being read out of the FIFO, you may want to pause the CoreDES macro by setting the EN input to a logic '0' when the full or almost-full flag logic from the FIFO is active. When the

FIFO full or almost-full flag logic clears, the CoreDES macro can then resume operation by again setting the EN input to a logic '1' value.

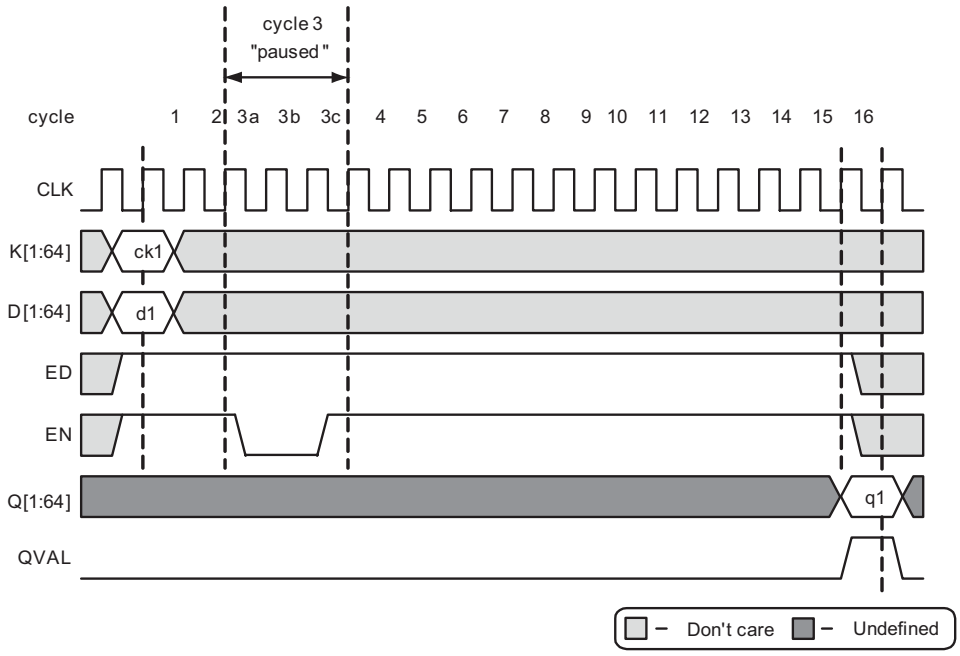

Figure 3-4 · Example Encryption Pause/Resume Sequence

Clear/Abort

At any point in the process of encrypting or decrypting data, you can abort the current operation by setting the CLR input to logic '1'. This clears all current calculations with the key schedule and data schedule logic. You can then immediately begin to use a different cipher key and data input on the very next cycle, as shown in Figure 3-5.

The clear/abort functionality is useful when you want to change the cipher key, possibly in the middle of an encryption or decryption sequence. You are able to immediately halt the current operation simply by holding the CLR input at a logic '1' value for at least one clock cycle, and commence immediately on the following clock cycle with a new cipher key

and/or new data. If the CoreDES macro is integrated into a system containing a processor, the processor may want to abort the encryption or decryption operation for some specific event (e.g., low or failing power condition).

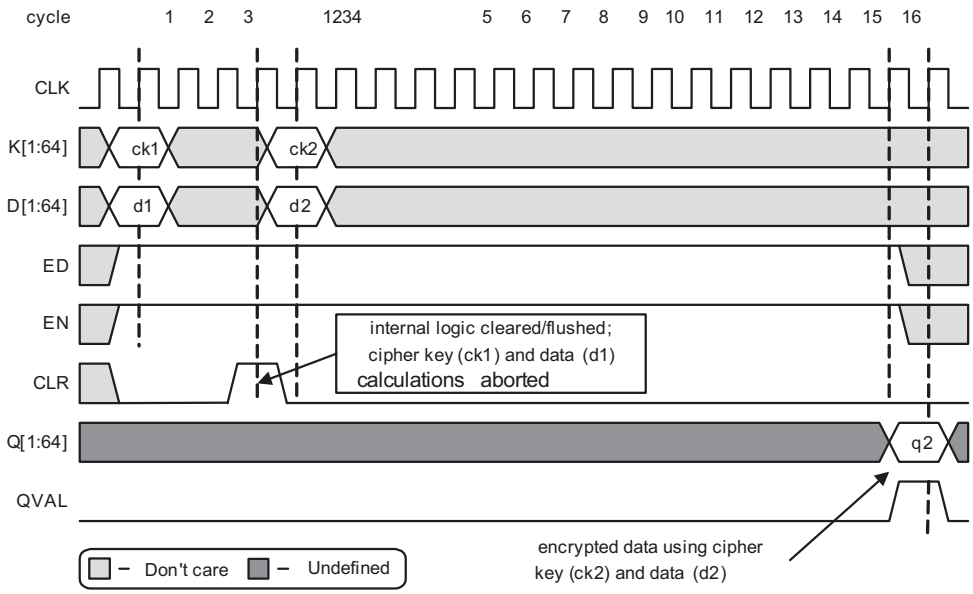

Figure 3-5 · Example Encryption Abort Sequence

Modes of Operation

CoreDES is implemented using the ECB (Electronic Codebook) mode of operation, per FIPS PUB 81.

Depending upon the application, other modes of operation for DES may be desirable. For this reason, Actel provides example VHDL and Verilog source code for the CBC (Cipher Block Chaining), CFB (Cipher Feedback), and OFB (Output Feedback) modes. For detailed information on specific modes of operation, refer to FIPS PUB 81.

4

Tool Flows and Testbench Operation

CoreDES is licensed in two ways. Depending on your license tool flow, functionality may be limited.

Obfuscated

Complete RTL code is provided for the core, allowing the core to be instantiated with SmartDesign. Simulation, Synthesis, and Layout can be performed within Libero IDE. The RTL code for the core is obfuscated and the some of the testbench source files are not provided; they are precompiled into the compiled simulation library instead.

RTL

Complete RTL source code is provided for the core and testbenches.

SmartDesign

CoreDES is preinstalled in the SmartDesign IP Deployment design environment. The core can be configured using the configuration GUI within SmartDesign, as shown in Figure 4-1. For information on using SmartDesign to instantiate and generate cores, refer to the Using DirectCores in the Libero IDE Online Help.

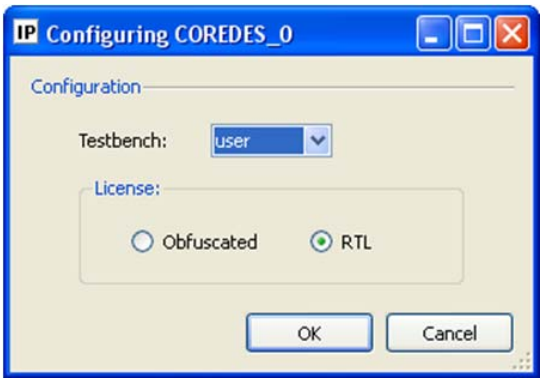

Figure 4-1 · CoreDES Configuration Window in SmartDesign

Simulation Flows

To run simulation, select the user testbench flow in SmartDesign through the CoreDES configuration GUI. From the Generate pane, select Save & Generate. When SmartDesign generates the Libero IDE project, it will install the user testbench files.

To run the user testbench, set the design root to the CoreDES instantiation in the Libero IDE File Manager and click the Simulation icon in the Libero IDE Design Flow window. This will invoke Model*Sim*® and automatically run the simulation.

Synthesis in Libero IDE

To run synthesis on the core with the parameter/generic set in SmartDesign, set the design root appropriately and click the Synthesis icon in Libero IDE Project Flow window. The Synthesis window appears, displaying the Synplicity® project. If using Verilog, set Synplicity to use the Verilog 2001 standard. Run Synplicity.

Place-and-Route in Libero IDE

After running Synthesis, click the Layout icon in Libero IDE to invoke Designer. CoreDES requires no special place and-route settings.

5 Testbench Operation

An example user testbench is included with the obfuscated and RTL releases of CoreDES. The obfuscated and RTL releases provide the precompiled Model*Sim* format, as well as the source code for the user testbench to ease the process of integrating and verifying the CoreDES macro into a design. The user testbench includes a simple example design that serves as a reference for users that want to implement their own designs.

The source code for each user testbench includes example support routines to aid the user in testing the CoreDES macro. Refer to the comments in the user testbench source code for details on the support routines (tasks for Verilog testbenches, functions and procedures for VHDL testbenches.) Using the supplied testbench as a guide, you can easily customize the verification of the core by adding or removing any of the tests listed in NIST Special Publication 800-17 or by adding any custom test cases.

6 Ordering Information

Order CoreDES through your local Actel sales representative. Use the following number convention when ordering: CoreDES-XX, where XX is listed in Table 6-1.

Table 6-1 · Ordering Codes

XX	Description
OM	RTL for Obfuscated RTL: multiple-use license
RM	RTL for RTL source: multiple-use license

Note: CoreDES -OM is included with Libero IDE license

A

Product Support

Actel backs its products with various support services including Customer Service, a Customer Technical Support Center, a web site, an FTP site, electronic mail, and worldwide sales offices. This appendix contains information about contacting Actel and using these support services.

Customer Service

Contact Customer Service for non-technical product support, such as product pricing, product upgrades, update information, order status, and authorization.

From Northeast and North Central U.S.A., call **650.318.4480**
From Southeast and Southwest U.S.A., call **650. 318.4480**
From South Central U.S.A., call **650.318.4434**
From Northwest U.S.A., call **650.318.4434**
From Canada, call **650.318.4480**
From Europe, call **650.318.4252** or **+44 (0) 1276 401 500**
From Japan, call **650.318.4743**
From the rest of the world, call **650.318.4743**
Fax, from anywhere in the world **650.318.8044**

Actel Customer Technical Support Center

Actel staffs its Customer Technical Support Center with highly skilled engineers who can help answer your hardware, software, and design questions. The Customer Technical Support Center spends a great deal of time creating application notes and answers to FAQs. So, before you contact us, please visit our online resources. It is very likely we have already answered your questions.

Actel Technical Support

Visit the Actel Customer Support website (www.actel.com/custsup/search.html) for more information and support. Many answers available on the searchable web resource include diagrams, illustrations, and links to other resources on the Actel web site.

Website

You can browse a variety of technical and non-technical information on Actel's home page, at www.actel.com.

Contacting the Customer Technical Support Center

Highly skilled engineers staff the Technical Support Center from 7:00 A.M. to 6:00 P.M., Pacific Time, Monday through Friday. Several ways of contacting the Center follow:

Email

You can communicate your technical questions to our email address and receive answers back by email, fax, or phone. Also, if you have design problems, you can email your design files to receive assistance. We constantly monitor the email account throughout the day. When sending your request to us, please be sure to include your full name, company name, and your contact information for efficient processing of your request.

The technical support email address is tech@actel.com.

Phone

Our Technical Support Center answers all calls. The center retrieves information, such as your name, company name, phone number and your question, and then issues a case number. The Center then forwards the information to a queue where the first available application engineer receives the data and returns your call. The phone hours are from 7:00 A.M. to 6:00 P.M., Pacific Time, Monday through Friday. The Technical Support numbers are:

650.318.4460
800.262.1060

Customers needing assistance outside the US time zones can either contact technical support via email (tech@actel.com) or contact a local sales office. Sales office listings can be found at www.actel.com/contact/offices/index.html.

Actel is the leader in low-power and mixed-signal FPGAs and offers the most comprehensive portfolio of system and power management solutions. Power Matters. Learn more at www.actel.com.

Actel Corporation *• 2061 Stierlin Court • Mountain View, CA 94043 • USA*
Phone 650.318.4200 • Fax 650.318.4600 • Customer Service: 650.318.1010 • Customer Applications Center: 800.262.1060

Actel Europe Ltd*. • River Court, Meadows Business Park • Station Approach, Blackwater • Camberley Surrey GU17 9AB • United Kingdom*
Phone +44 (0) 1276 609 300 • Fax +44 (0) 1276 607 540

Actel Japan *• EXOS Ebisu Building 4F • 1-24-14 Ebisu Shibuya-ku • Tokyo 150 • Japan*
Phone +81.03.3445.7671 • Fax +81.03.3445.7668 • http://jp.actel.com

Actel Hong Kong *• Room 2107, China Resources Building • 26 Harbour Road • Wanchai • Hong Kong*
Phone +852 2185 6460 • Fax +852 2185 6488 • www.actel.com.cn

50200151-0/03.09