Core3DES

Product Summary

Intended Use

- Whenever Data Is Transmitted Across an Accessible Medium (wires, wireless, etc.)
- E-Commerce Transactions, Where Dedicated Encryption/ Decryption Hardware Can Ease the Load on Servers
- Personal Security Devices
- Bank Transactions, Where Financial Security Is Mandatory

Key Features

- Compliant with FIPS PUB 46-3
- TECB (TDEA Electronic Codebook) Implementation Per ANSI Standard X9.52
- Example Source Code Provided for TCBC, TCFB, and TOFB Modes
- 168-Bit Cipher Key (consisting of 56-bit cipher keys in 3 stages, with 24 additional parity bits)
- All Major Actel Device Families Supported
- Parity Checking Logic for Cipher Key
- Encryption and Decryption Possible with Same Core
- 48-Clock Cycle Operation to Encrypt or Decrypt 64 Bits of Data
- Pause/Resume Functionality to Continue Encryption or Decryption at Will
- Provides Data Security within a Secure Actel FPGA

Supported Families

- Fusion
- ProASIC3/E
- ProASIC$^{\underline{PLUS}®}$
- Axcelerator®
- RTAX-S
- SX-A
- RTSX-S

Core Deliverables

- Evaluation Version
  - Compiled RTL Simulation Model Fully Supported in the Actel Libero® Integrated Design Environment (IDE)
- Netlist Version
  - Structural Verilog and VHDL Netlists (with and without I/O pads) Compatible with the Actel Designer Software Place-and-Route Tool
  - Compiled RTL Simulation Model Fully Supported in the Actel Libero IDE
- RTL Version
  - Verilog or VHDL Core Source Code
  - Core Synthesis Scripts
- Actel-Developed Testbench (Verilog and VHDL)

Synthesis and Simulation Support

- Synthesis: Synplicity®, Synopsys (Design Compiler®/ FPGA Compiler™/ FPGA Express™), Exemplar™
- Simulation: OVI-compliant Verilog Simulators and Vital-Compliant VHDL Simulators

Core Verification

- Actel-Developed Simulation Testbench Verifies Core3DES Against Tests Listed in National Institute of Standards and Technology (NIST) Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*
- User Can Easily Modify Testbench Using Existing Format to Add More Tests Listed in NIST Special Publication 800-20 or Custom Tests

Contents

General Description

The Core3DES macro implements the Triple Data Encryption Standard (3DES or Triple DES), which provides a means of securing data. The Triple DES algorithm is described in the Federal Information Processing Standards (FIPS) Publication (PUB) 46-3, and is an extension of the DES (Data Encryption Standard) algorithm (Figure 1) and also described in FIPS PUB 46-3.

The Triple DES algorithm takes as inputs 64 bits of plaintext data and 192 bits of a cipher key, and after 48 cycles, produces a 64-bit ciphered version of the original plaintext data as output.[1] The entire 168-bit cipher key consists of three sub-keys, denoted as K1, K2, and K3, representing the left third (MSB), the middle third, and the right third (LSB) of the cipher key, respectively. During the 48 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 168-bit cipher key.

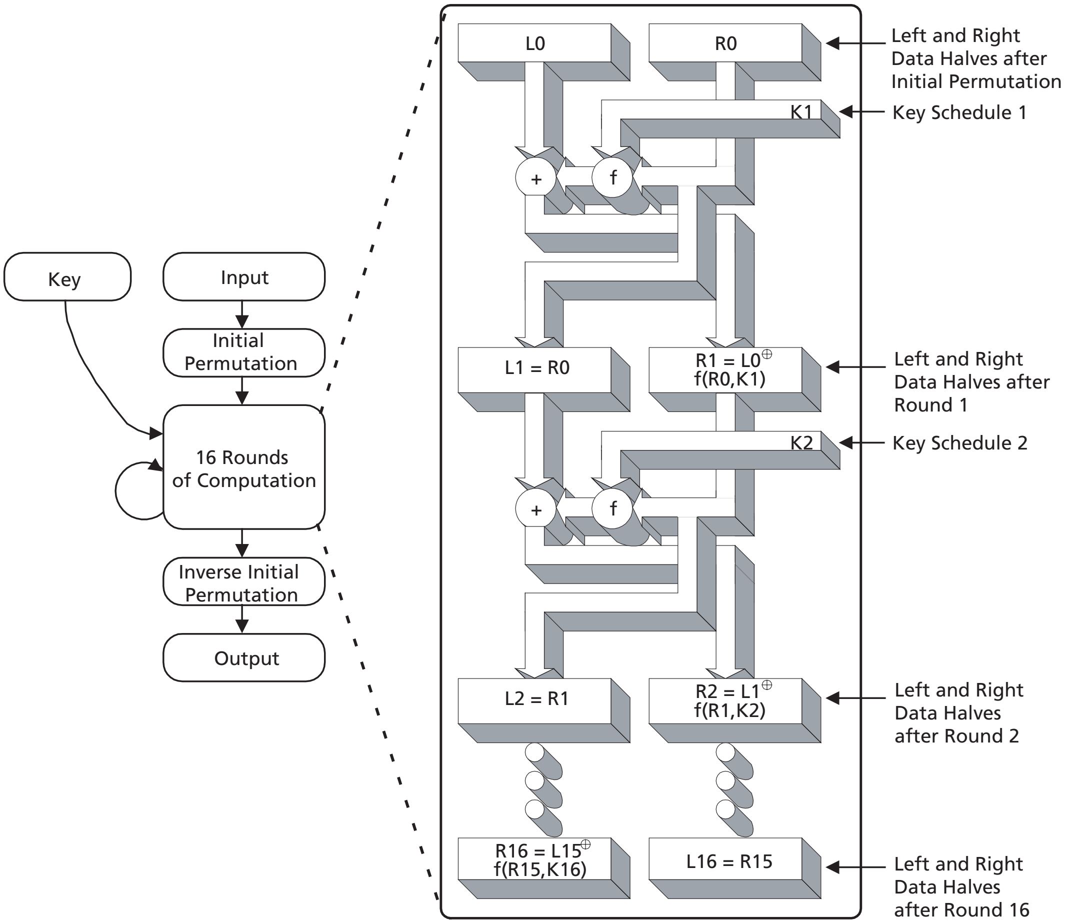

Key
Input
Initial Permutation
16 Rounds of Computation
Inverse Initial Permutation
Output
L0
R0
Left and Right Data Halves after Initial Permutation
K1
Key Schedule 1
+
f
L1 = R0
R1 = L0⊕ f(R0,K1)
Left and Right Data Halves after Round 1
K2
Key Schedule 2
+
f
L2 = R1
R2 = L1⊕ f(R1,K2)
Left and Right Data Halves after Round 2
R16 = L15⊕ f(R15,K16)
L16 = R15
Left and Right Data Halves after Round 16

Figure 1 • **DES Algorithm**

[1] *Only 168 of the 192 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.*

The Triple DES encryption algorithm is executed in the specific sequential order shown in Figure 2.

1. Encrypt using DES with cipher key K1 (left third of 168-bit cipher key).
2. Decrypt using DES with cipher key K2 (middle third of 168-bit cipher key).
3. Encrypt using DES with cipher key K3 (right third of 168-bit cipher key).

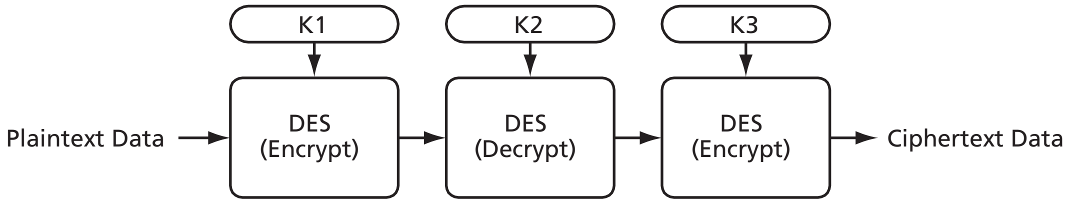


Figure 2 • **Triple DES Encryption Flow Diagram**

The Triple DES decryption algorithm is executed in the specific sequential order shown in Figure 3.

1. Decrypt using DES with cipher key K3 (right third of 168-bit cipher key).
2. Encrypt using DES with cipher key K2 (middle third of 168-bit cipher key).
3. Decrypt using DES with cipher key K1 (left third of 168-bit cipher key).

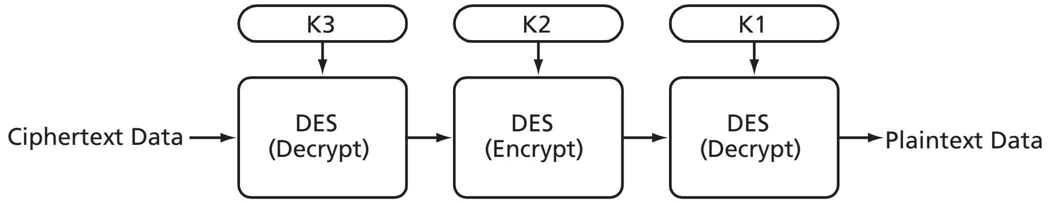


Figure 3 • **Triple DES Decryption Flow Diagram**

Since three sequential DES operations are required, the total compute time for Triple DES (encryption or decryption) is three times that for single DES or 16 x 3 = 48 clock cycles.

Core3DES consists of four main blocks (Figure 4).

1. Data schedule logic – computes the intermediate data values at each round of the Triple DES algorithm.
2. Iteration state machine logic – keeps track of which round of the Triple DES algorithm is currently in progress.
3. Key schedule logic – computes the intermediate keys at each round of the Triple DES algorithm.
4. Parity check logic – checks for odd-parity compliance of the 168 bits of cipher key and issues an error signal if parity is not correct.

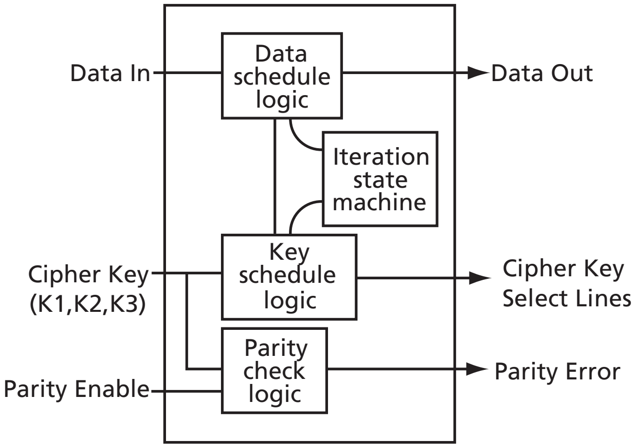


Figure 4 • **Core3DES Block Diagram**

Design Security

Figure 5 shows a typical system diagram. Note that the cipher key, which is the "secret" key, can be made up of FPGA logic cells, preventing the possibility of design or data theft. Actel Flash-based devices (ProASIC^{PLUS}) use FlashLock™ technology, and Actel antifuse-based devices (Axcelerator, SX-A, RTSX-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 Core3DES macro should be connected to registers or FIFOs, since it is only valid for one clock cycle, as shown by example in the "Encryption" section on page 7 and the "Decryption" section on page 8.

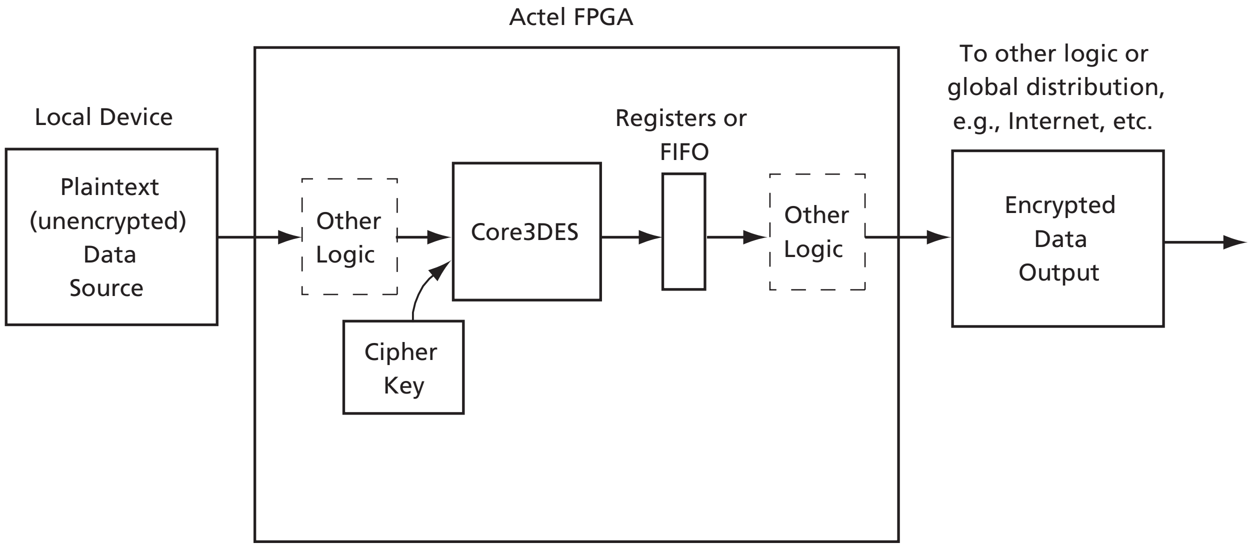


Figure 5 • **Typical Core3DES System**

Core3DES Device Requirements

The Core3DES macro has been implemented in several Actel device families. Table 1 lists a summary of the implementation data.

Table 1 • **Core3DES Device Utilization and Performance**

	Cells or Tiles			Utilization			
Family	**Sequential**	**Combinatorial**	**Total**	**Device**	**Total**	**Performance**	**Throughput**
Fusion	156	1257	1413	AFS600	11%	75 MHz	300 Mbps
ProASIC3/E	156	1257	1413	A3PE600-2	11%	75 MHz	300 Mbps
ProASIC^{PLUS}	150	1456	1606	APA075-STD	53%	50 MHz	66.7 Mbps
Axcelerator	152	620	772	AX125-3	39%	125 MHz	166.7 Mbps
RTAX-S	152	620	772	RTAX1000S-1	5%	81 MHz	108 Mbps
SX-A	152	640	792	A54SX16A-3	55%	100 MHz	133.3 Mbps
RTSX-S	152	640	792	RT54SX32S-2	28%	60 MHz	80 Mbps

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 (48), and multiplying by the clock rate (performance). The result is listed in Mbps (millions of bits per second).

Core3DES Verification

The comprehensive verification simulation testbench (included with the Netlist and RTL versions of the core) verifies the Core3DES macro against test cases listed in NIST Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*. The testbench applies several tests to the Core3DES macro, including: variable plaintext tests, variable cipher key tests, permutation operation tests, substitution table tests, and Monte Carlo tests. Using the supplied user testbench as a guide, the user can easily customize the verification of the core by adding or removing any of the tests listed in NIST Special Publication 800-20 or by adding any custom test cases.

I/O Signal Descriptions

The port signals for the Core3DES macro are defined in Table 2 and illustrated in Figure 6. Core3DES has 202 I/O signals that are described in Table 2. Most 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 is 64 for most of the 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). The only deviation from this nomenclature is the Key Select output bus, which descends from 1 down to 0.

Table 2 • **Core3DES I/O Signal Descriptions**

Name	Type	Description
NRESET	Input	Active-low asynchronous reset
CLK	Input	System clock: reference clock for all internal Triple DES logic
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	Encrypt/Decrypt: '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 bit (56 bits + 8 parity bits) cipher key input bus (time-multiplexed K1,K2,K3 sub-keys)
D[1:64]	Input	Data in: 64 bit data input bus
Q[1:64]	Output	Data out: 64 bits of ciphertext (for Encrypt operation, plaintext for Decrypt operation)
QVAL	Output	Q Valid: '1' indicates that valid Encrypt/Decrypt data is available on Q [1:64]
KSEL[1:0]	Output	Key Select: Selection bits for cipher key sub-keys K1, K2, and K3. When 00: K1 needs to be presented on the K[1:64] input bus, when 01: K2 needs to be presented on the K[1:64] input bus, when 10: K3 needs to be presented on the K[1:64] input bus
PERR	Output	Parity Error: '1' indicates that a parity error has occurred on the K cipher key input bits

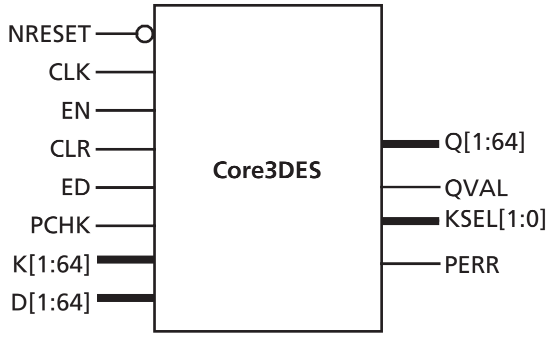


Figure 6 • **Core3DES I/O Signal Diagram**

Core3DES Operation

Cipher Key Selection

Since there is only one cipher key K[1:64] input port and the Triple DES algorithm requires three 64-bit cipher sub-keys (three 56-bit cipher sub-keys, less than 8 parity bits, per sub-key), the three cipher sub-keys will need to be presented in sequence on the same K[1:64] input port. The KSEL[1:0] output port will need to be decoded by the designer for use in external selection logic for each of the three 64-bit cipher sub-keys. Since the KSEL[1:0] output port may be connected to address lines of an external RAM or ROM device, there is an extra clock cycle of latency built into the Core3DES logic. In other words, when the KSEL[1:0] port changes value, the next cipher sub-key is not required immediately on the next rising edge of the clock, however; it will be required by the second rising edge of the clock. This is illustrated in the "Encryption" section on page 7 and the "Decryption" section on page 8.

Parity Checking

If parity checking is desired for the cipher key K[1:64] inputs, the PCHK input port should be held at logic '1.' The parity checking logic will determine whether or not an odd number of logic '1' values are present in each byte of the cipher sub-keys K1, K2, and K3. 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 sub-keys (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 7 illustrates a block diagram of the parity check logic.

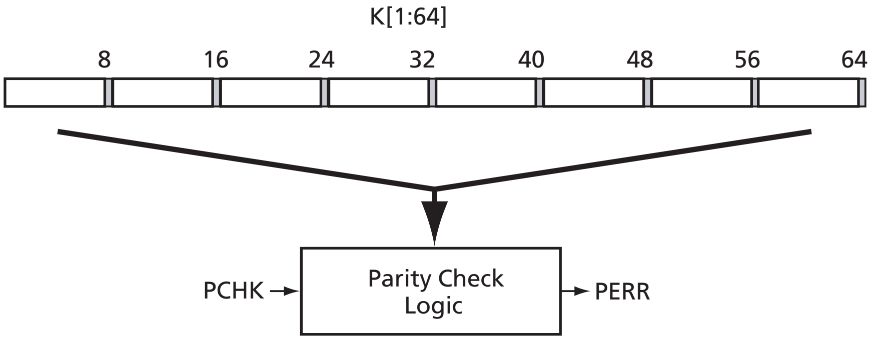


Figure 7 • **Key Parity Check**

Encryption

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

1. K[1:64] is set to the first of three cipher sub-keys ("ck1" in Figure 8) to encrypt the data.
2. D[1:64] is set to the plaintext data ("d1" in Figure 8) to be encrypted.
3. ED is set to logic '1'.
4. EN is set to logic '1'.

After 15 clock cycles of the EN input being held continuously at a logic '1' value, the KSEL[1:0] outputs will change from '00' to '01', indicating that the second of three cipher sub-keys (ck2 in Figure 8), will need to be presented on the K[1:64] inputs, which must be done by the rising clock edge of the start of clock cycle 17 (one complete clock cycle of slack is built into the Core3DES circuitry). After 31 clock cycles of the EN input being held at a logic '1', the KSEL[1:0] outputs will change from '01' to '10', indicating that the third of three cipher sub-keys (ck3 in Figure 8) will need to be presented on the K[1:64] inputs, which must be done by the rising clock edge of the start of clock cycle 33.

After 48 clock cycles of the EN input being held continuously at a logic '1' value, the QVAL signal will transition from logic '0' to logic '1' and remain valid for one clock cycle, indicating that valid ciphertext (encrypted) data (q1 in Figure 8) is available on the Q[1:64] outputs. Note that the encrypted data is only available during clock cycle 48, thus the user must register or latch the data on Q[1:64], using the QVAL signal as a qualifying register enable or latch enable.

As shown in Figure 8, continuous encryption is possible. For example, the second 64-bit plaintext data word (d2 in Figure 8) can be immediately encrypted by presenting d2 on the D[1:64] inputs by the rising clock edge of clock cycle 49 and by presenting the cipher sub-keys ck1, ck2, and ck3 in the sequence described earlier in this section.

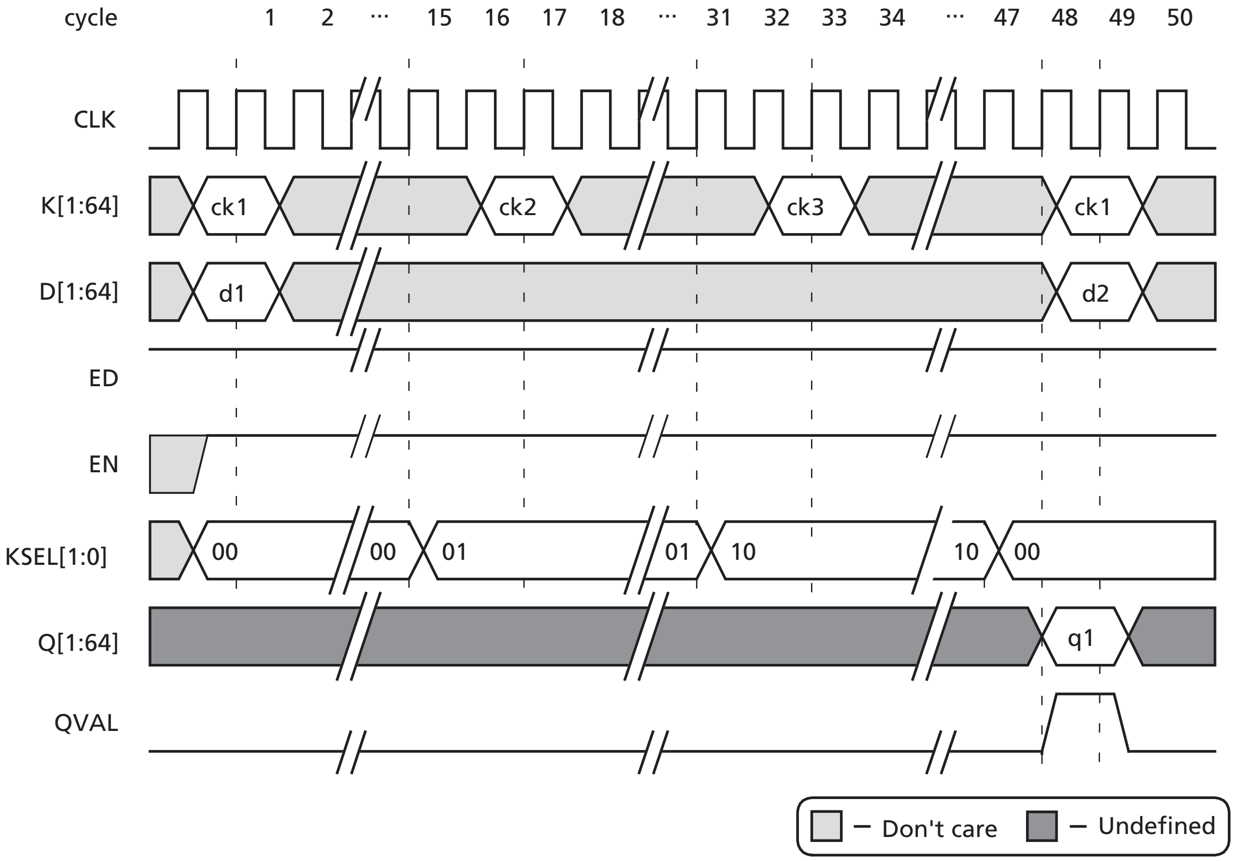


Figure 8 • **Example Encryption Sequence**

Decryption

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

1. K[1:64] is set to the third of three cipher sub-keys ("ck3" in Figure 9) to encrypt the data.
2. D[1:64] is set to the ciphertext data ("d1" in Figure 9) to be decrypted.
3. ED is set to logic '0'.
4. EN is set to logic '1'.

After 15 clock cycles of the EN input being held continuously at a logic '1' value, the KSEL[1:0] outputs will change from '10' to '01', indicating that the second of three cipher sub-keys (ck2 in Figure 9) will need to be presented on the K[1:64] inputs, which must be done by the rising clock edge of the start of clock cycle 17 (one complete clock cycle of slack is built into the Core3DES circuitry). After 31 clock cycles of the EN input being held at a logic '1', the KSEL[1:0] outputs will change from '01' to '00', indicating that the first of three cipher sub-keys (ck1 in Figure 9) will need to be presented on the K[1:64] inputs, which must be done by the rising clock edge of the start of clock cycle 33. Note that for decryption, the order in which the three cipher sub-keys are required differs from the encryption process (described in the previous section); cipher sub-key three is required first, cipher sub-key two is next, and cipher sub-key one is last.

After 48 clock cycles of the EN input being held continuously at a logic '1' value, the QVAL signal will transition from logic '0' to logic '1' and remain valid for one clock cycle, indicating that valid plaintext (un-encrypted data, shown as q1 in Figure 9) is available on the Q[1:64] outputs. Note that the decrypted plaintext data is only available during clock cycle 48, thus the user must register or latch the data on Q[1:64] using the QVAL signal as a qualifying register enable or latch enable.

As shown in Figure 9, continuous decryption is possible. For example, the second 64-bit ciphertext data word (d2 in Figure 9) can be immediately decrypted by presenting d2 on the D[1:64] inputs by the rising clock edge of clock cycle 49 and by presenting the cipher sub-keys ck3, ck2, and ck1 in the sequence described earlier in this section.

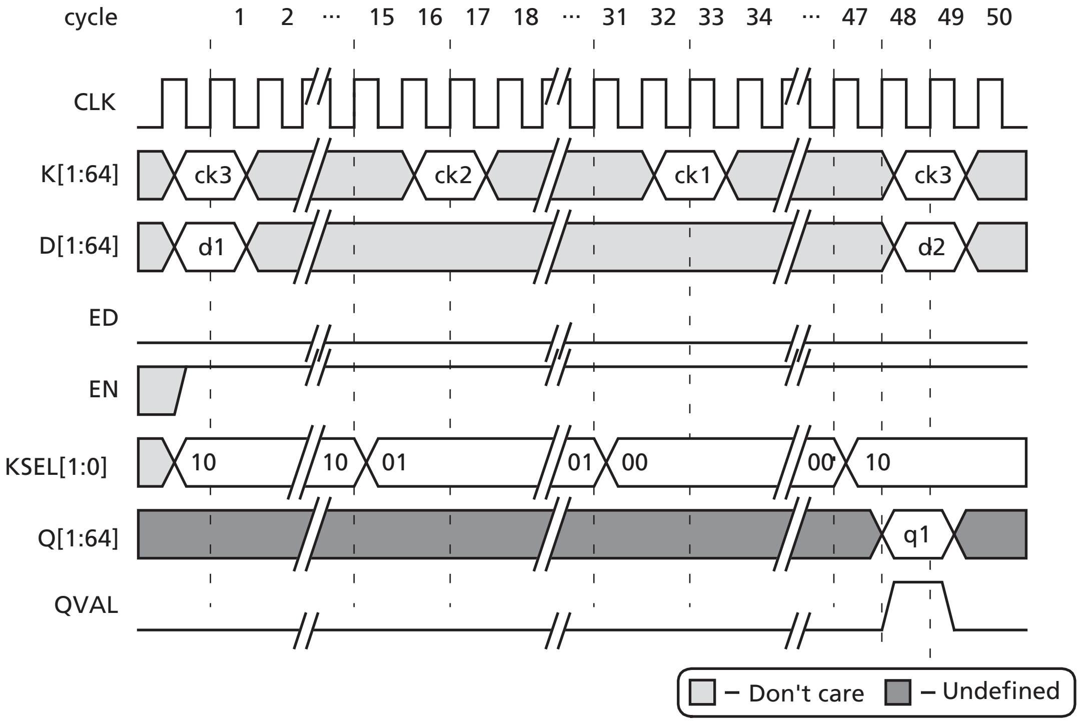


Figure 9 • **Example Decryption Sequence**

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 by the example in Figure 10 where cycle 3 of an encryption operation is paused. 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 the user. One possible use for the pause functionality is a case where many blocks of data are encrypted one after another. The EN input would be held statically at a logic '1' value, and the data input needs to change every 48 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 a logic '1', data will continue to be encrypted ad infinitum. When ready for the next blocks of data, the user can then resume the encryption process by holding the EN input at a logic '1' value. Another possible use may be if the user has 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, the user may wish to pause the Core3DES 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 Core3DES macro can then resume operation by again setting the EN input to a logic '1' value.

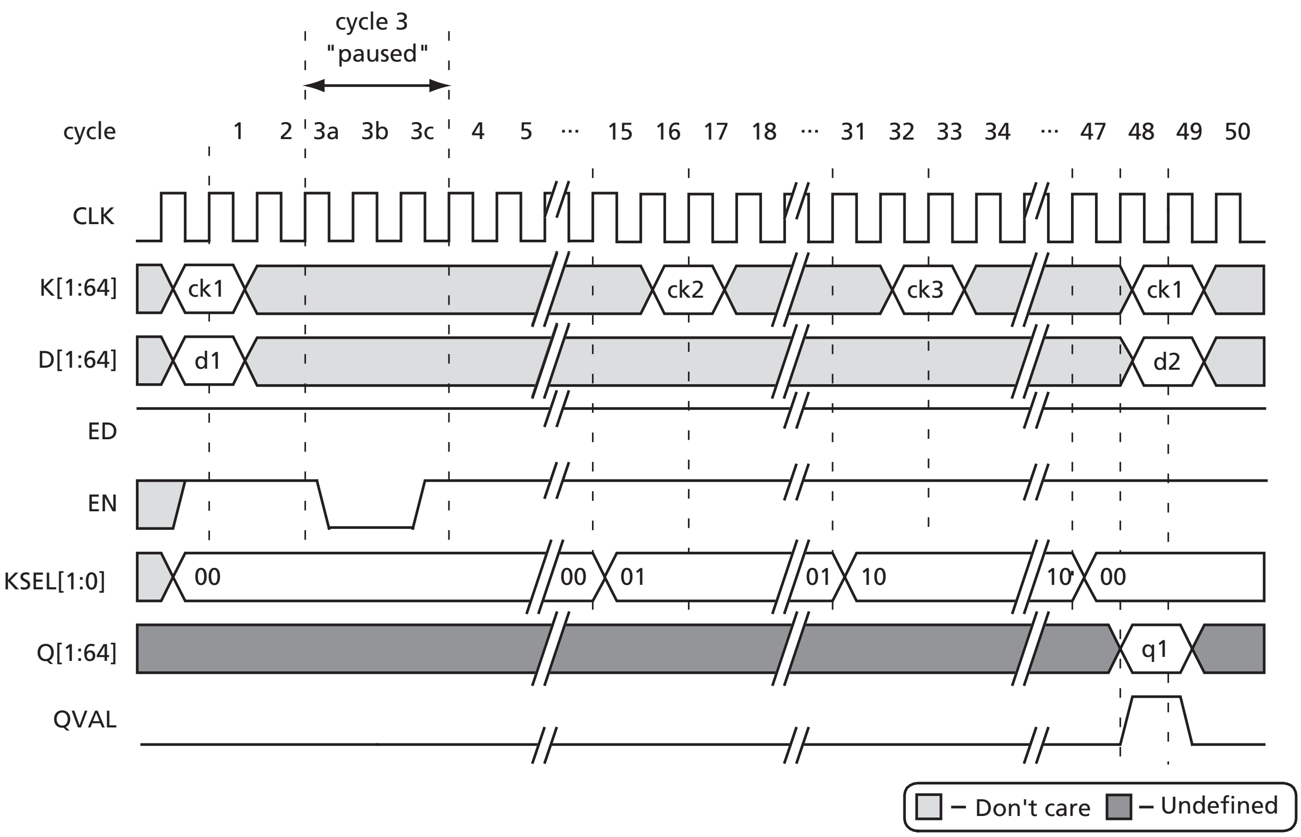
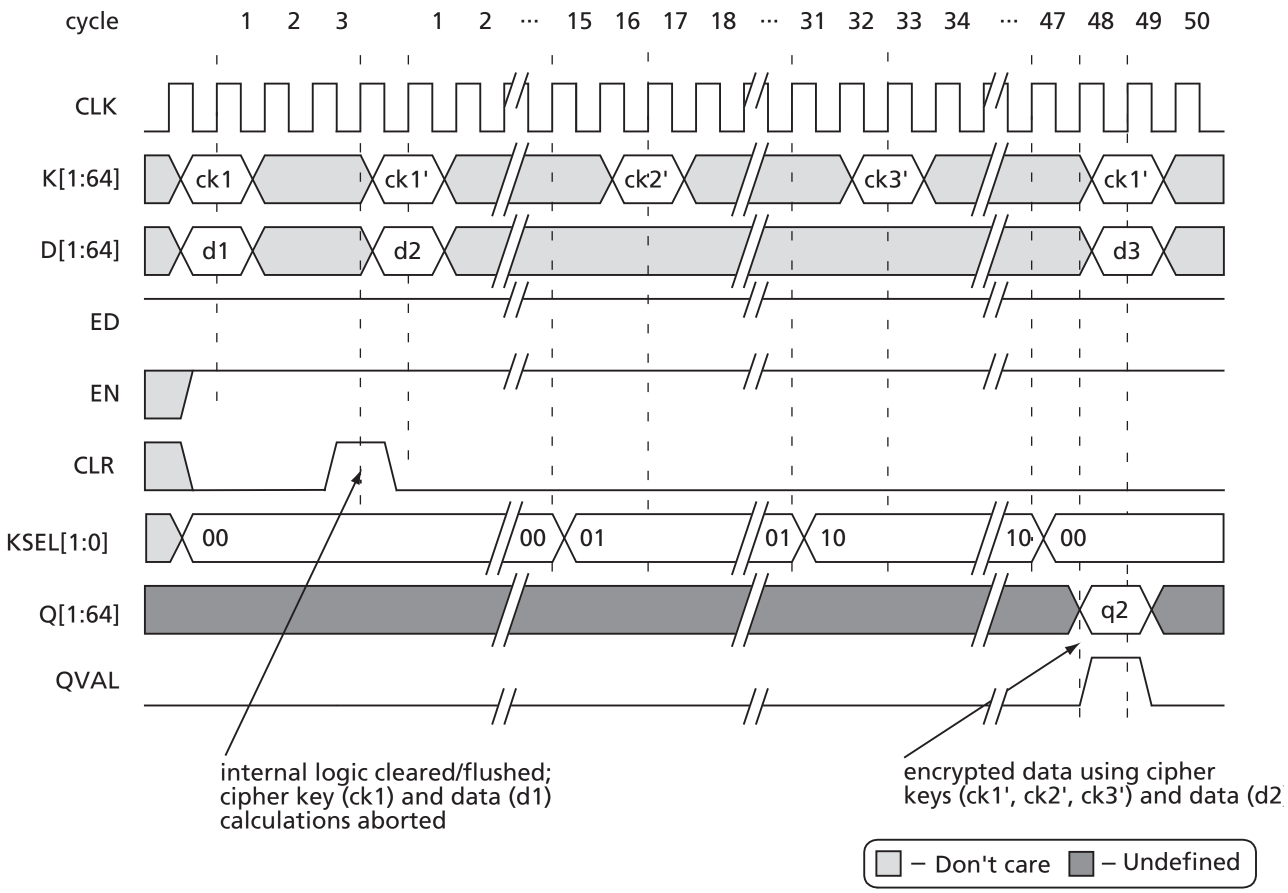


Figure 10 • **Example Encryption Pause/Resume Sequence**

Clear/Abort

At any point in the process of encrypting or decrypting data, the user can abort the current operation by setting the CLR input to logic '1'. This will clear all current calculations with the key schedule and data schedule logic. The user can then immediately begin to use a different cipher key and data input on the very next cycle, as shown in Figure 11.

The clear/abort functionality is provided as another aid to the user. An example of its use occurs when the user wants to change the cipher key, possibly in the middle of an encryption or decryption sequence. Immediately, the user can stop the current operation simply by holding the CLR input at a logic '1' value for at least one clock cycle and immediately commence on the following clock cycle with a new cipher key and/or new data. If the Core3DES macro is integrated into a system containing a processor, the processor may wish to abort the encryption or decryption operation for some specific event (e.g., low or failing power condition).



internal logic cleared/flushed; cipher key (ck1) and data (d1) calculations aborted

encrypted data using cipher keys (ck1', ck2', ck3') and data (d2

Figure 11 • **Example Encryption Abort Sequence**

Modes of Operation

Core3DES is implemented using the TECB (TDEA Electronic Codebook) mode of operation, per ANSI Standard X9.52. Depending upon the application, other modes of operation for Triple DES may be desirable. For this reason, Actel provides example VHDL and Verilog source code for the TCBC (TDEA Cipher Block Chaining), TCFB (TDEA Cipher Feedback), and TOFB (TDEA Output Feedback) modes. For detailed information on specific modes of operation, refer to ANSI Standard X9.52.

Ordering Information

Order Core3DES through your local Actel sales representative. Use the following number convention when ordering: Core3DES-XX, where XX is listed in Table 3.

Table 3 • **Ordering Codes**

XX	**Description**
EV	Evaluation Version
SN	Netlist for single-use on Actel devices
AN	Netlist for unlimited use on Actel devices
SR	RTL for single-use on Actel devices
AR	RTL for unlimited use on Actel devices
UR	RTL for unlimited use and not restricted to Actel devices

Export Restrictions

Core3DES is subject to export controls and is licensable under the U.S. Department of Commerce's Export Administration Regulations, the U.S. Department of State's International Traffic in Arms Regulations, or other laws, government regulations or restrictions. Actel is in the process of obtaining additional permissions to ship Core3DES to a wider audience. The licensee will not import, export, reexport, divert, transfer or disclose Core3DES without complying strictly with the export control laws and all legal requirements in the relevant jurisdictions, including, without limitation, obtaining the prior approval of the U.S. Department of Commerce or the U.S. Department of State, as applicable.

List of Changes

The following table lists critical changes that were made in the current version of the document.

Previous version	Changes in current version (v5.0)	Page
v4.0	The "Supported Families" section was updated to include Fusion.	1
	Table 1 was updated to include Fusion data.	4
v3.0	The "Supported Families" section was updated to include ProASIC3/E.	1
	Table 1 was updated to include ProASIC3/E data.	4
v2.0	Figure 6 • Core3DES I/O Signal Diagram was updated.	5

Datasheet Categories

In order to provide the latest information to designers, some datasheets are published before data has been fully characterized. Datasheets are designated as "Product Brief," "Advanced," "Production," and "Datasheet Supplement." The definitions of these categories are as follows:

Product Brief

The product brief is a summarized version of a datasheet (advanced or production) containing general product information. This brief gives an overview of specific device and family information.

Advanced

This datasheet version contains initial estimated information based on simulation, other products, devices, or speed grades. This information can be used as estimates, but not for production.

Unmarked (production)

This datasheet version contains information that is considered to be final.

Datasheet Supplement

The datasheet supplement gives specific device information for a derivative family that differs from the general family datasheet. The supplement is to be used in conjunction with the datasheet to obtain more detailed information and for specifications that do not differ between the two families.

www.actel.com

Actel Corporation

2061 Stierlin Court
Mountain View, CA
94043-4655 USA

Phone 650.318.4200
Fax 650.318.4600

Actel Europe Ltd.

Dunlop House, Riverside Way
Camberley, Surrey GU15 3YL
United Kingdom

Phone +44 (0) 1276 401 450
Fax +44 (0) 1276 401 490

Actel Japan
www.jp.actel.com

EXOS Ebisu Bldg. 4F
1-24-14 Ebisu Shibuya-ku
Tokyo 150 Japan

Phone +81.03.3445.7671
Fax +81.03.3445.7668

Actel Hong Kong
www.actel.com.cn

Suite 2114, Two Pacific Place
88 Queensway, Admiralty
Hong Kong

Phone +852 2185 6460
Fax +852 2185 6488