Final

TCDG

VHDL & Verilog Synthesizable model of the Data Encryption Standard (DES)

DISTINCTIVE CHARACTERISTICS

- **High Performance**
  - 16 clock cycles for a complete DES encryption or decryption
  - Simple interface with a start/done handshake
  - No external logic necessary

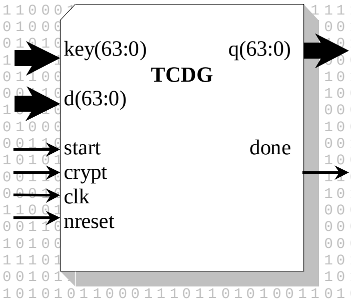
- **Compatibility**
  - Based on the FIPS PUB 44-2 specification
  - ANSI X3.92, ANSI X3.106
  - Suitable for triple DES implementations
  - Suitable for electronic code block (ECB), cipher block coding (CBC), cipher feedback (CFB) and output feedback (OFB) implementations

- **Description language & Synthesis caracteristics**
  - Available in VHDL and Verilog
  - Described for both synthesis and simulation
  - Fully Synchronous design
  - Low gate count
  - High clock speed
  - Test bench provided

- **Target Technology**
  - FPGA
  - ASIC
  - Gate Array
  - ....

- **Typical application**
  - Data files protection on any media (hard disk, CD-ROM, EEPROM,...)
  - Access authentification
  - Smart card applications
  - Internet & Intranet communication protection
  - Space telecommunication
  - Banking applications
  - Private informations protections

- **Complete product range**
  - See TETRAEDRE’s products portofolio for availability of low-power, full-scan products. As well as for C (C++) source files and Triple DES modules.



Version	: 1.0
Printing date	: 10/09/99

GENERAL DESCRIPTION

The Data Encryption Standard (DES) algorithm, adopted by the U.S. government in 1977, is a block cipher that transforms 64-bit data blocks under a 56-bit secret key, by means of permutation and substitution. It is officially described in FIPS PUB 46. The DES algorithm is used for many applications within the government and in the private sector.

In general, cryptography is used to protect data while it is being communicated between two points or while it is stored on a medium vulnerable to physical theft. Communication security provides protection to data by enciphering it at the transmitting point and deciphering it at the receiving point. File security proceeds protection to data by enciphering it when it is recorded on a storage medium and deciphering it when it is read back from the storage medium. In the first case, the key must be available at the transmitter and receiver simultaneously during communication. In the second case, the key must be maintained and accessible for the duration of the storage period.

Key

A key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm may be used for error detection if they are interpreted as parity bits. The TCDG modules doesn't use these bits at all. When these parity bit are used, they must be set to make the parity of each 8-bit byte of the key odd. The user must have the key that was used to encipher the data in order to decrypt it. Use of a different key causes the cipher that is produced for any given set of inputs to be different. The encryption algorithm specified for the DES is commonly known among those using the standard. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data.

Data input

The DES algorithm can crypt or decrypt any data (either text, numbers) expressed in 64 binary digits words. The input is processed in blocks. Therefore, this algorithm can be used to protect any kind of documents, like pictures, private data, bank account number, confidential documents, ...

Data output

Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, anyone who does have the key can decipher the cipher and obtain the original data.

Qualification

The cryptographic DES algorithm transforms a 64-bit binary value into a unique 64-bit binary value based on a 56-bit variable. If the complete 64-bit input is used and if the 56-bit variable is randomly chose, no technique other than trying all possible keys using known input and output for the DES will guarantee finding the chosen key. As these are over 70,000,000,000,000,000 (seventy quadrillion) possible keys of 56 bits, the feasibility of deriving a particular key in this way is extremely unlikely in typical threat environments. Moreover, if the key is changed frequently, the risk of this event is greatly diminished.

If improved security level are needed by your application, the Triple DES algorithm may be used. This algorithm, based on the DES uses three independents key (leading to 168-bit key) to cipher the data.

Products implemented the Triple DES algorithm are also available by Tetraedre.

Export control and restrictions

In the United States of America, cryptographic devices and technical data regarding them are subject to U.S. Federal Government export controls (Code of Federal Regulations). Some export of cryptographic modules implementing this standard and technical data regarding them must comply with these regulations and be licensed by the U.S. Department of State or by the Bureau of Export Administration of the U.S. Department of Commerce.

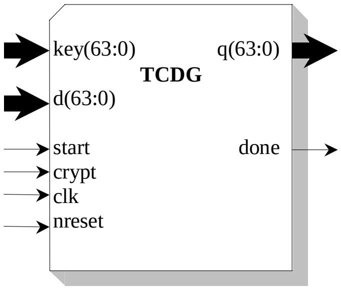
This product is not suitable for life support equipment.

Patents

Cryptographic devices implementing this standard may be covered by U.S. and foreign patents issued to the International Business Machines Corporation. However, IBM has granted nonexclusive, royalty-free licenses under the patents to make, use and sell apparatus which complies with this standard.

The VHDL and Verilog modules, TCDG products, are protected by copyrights and belong to Tetraedre Sarl, Switzerland. These modules can be used only by signing a license agreement with Tetraedre Sarl.

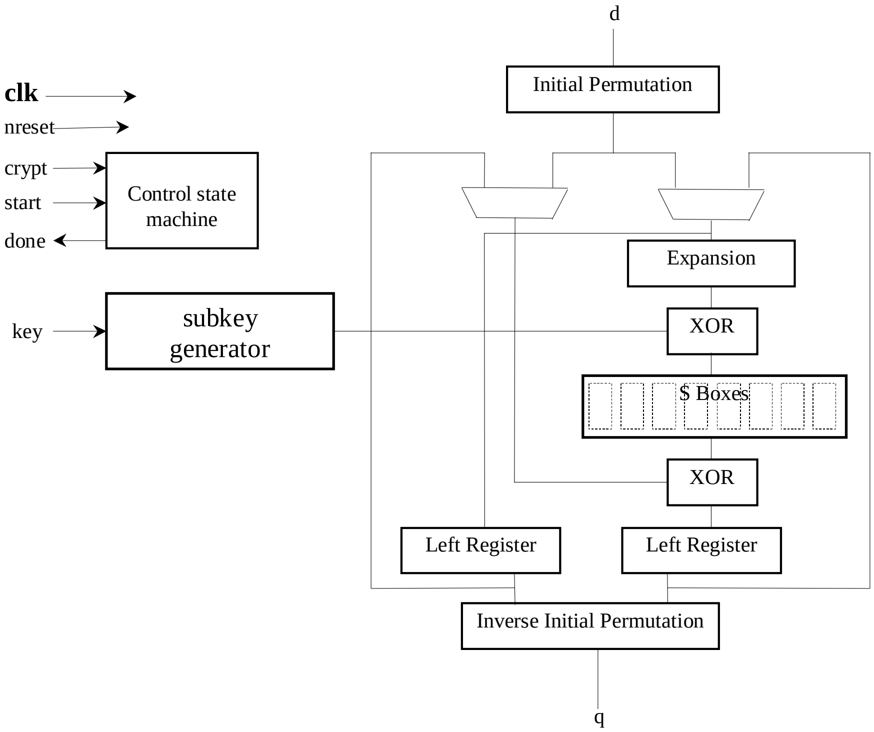
LOGIC SYMBOL



PIN CONFIGURATION

key(63:0)	key input
d(63:0)	data input
q(63:0)	result output
start	conversion start
crypt	crypt/decrypt mode selection
done	conversion done flag
clk	clock input
nreset	asynchronous reset

Block diagram



OPERATING MODES

The TCDG module is a very easy to use component. The data to be encrypted or decrypted is applied to the **d** input, the appropriate operation mode is selected by setting **crypt** in the right state. Then, to start the conversion, the **start** signal is asserted. Once the conversion is finished, the **done** signal is asserted. The result can be read on the **q** output pin.
The word "conversion" is used hereafter to indicate either an encryption or a decryption. The choice of the operation is selected by the crypt pin, as explained below.

Since the design is completely synchronous, no clock signals are generated and no gated clock are used inside this component. So the interface between the DES module and your application is very easy to implement.

Pinout description

key(63:0) This 64-bit wide bus represents the key of the DES encryption or decryption. The key input must remain stable during the complete conversion. The key must not change until the result has been stored since the output depends directly on the key value.

d(63:0) This 64-bits input represents the data which must be encrypted or decrypted. The data is sampled in internal registers at **clk**'s rising edge at the conversion's start.

q(63:0) This 64-bits output represents the result of the calculation. This signal can be sampled by your application at **clk**'s rising edge, when **done** is asserted (high). The result appears on the output line simultaneously with the **done** signal.

start This signal indicates to the internal state machine to start a conversion. The conversion starts at **clk**'s rising edge after **start** has changed from 0 to 1. The **start** signal is internally synchronized with the clock.

crypt This signal indicates if the data at the input must be encrypted (crypt=1) or decrypted (crypt=0). This signal is sampled in an internal register at **clk**'s rising edge when the conversion starts.

done This output indicates (at 1) when the result has been calculated. This signal remains at one as long as no START signal is asserted.

clk Clock signal.

nreset This signal is an asynchronous reset signal (low active).

Conversion timing diagram

The figure 1 shows the timing diagram of a conversion. Since the data (*d*) and crypt inputs are sampled at the start of the conversion, the can change after the start. The key input is not sampled inside the component so modifying the key will change the result, even after the conversion ended.
The **start** signal starts the conversion. **done** is asserted 15 clock cycles after start has been negated. The result remains stable as long as no START occurs and as long as the input remains stable.

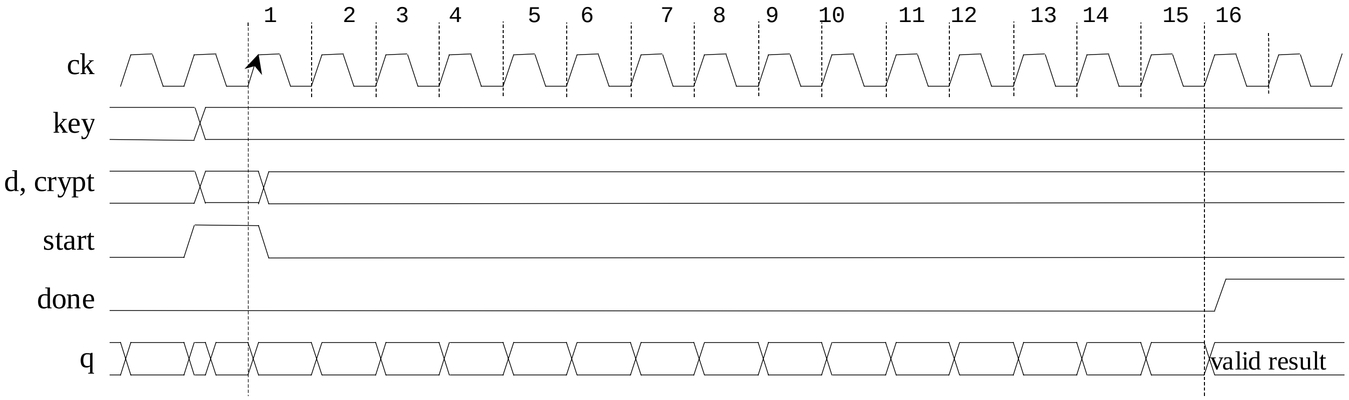


Figure 1. Conversion timing

Alternative modes of using the DES

Four different modes for using the algorithm have been described in several standard (for example FIPS PUB 81). The four modes are called the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode and the Output Feedback (OFB) mode.

ECB is a direct application of DES algorithm to encrypt and decrypt data.

CBC is an enhanced mode of ECB which chains together blocks of cipher text.

CFB uses previously generated cipher text as input to the DES to generate pseudorandom outputs which are combined with the plaintext to produce cipher, thereby chaining together the resulting cipher.

OFB is identical to CFB except that the previous output of the DES is used as input in OFB while the previous cipher is used as input in CFB. OFB does not chain the cipher.

SIMULATION INFORMATION

The DES module, TCDG, is delivered with a HDL testbench (either VHDL or Verilog). This testbench is composed of several hundreds encryption and decryption calculations. The test vectors define the input parameters (d, key, crypt) and also the expected output of the block. The value generated by the DES module is compared with the expected value. If they don't match, the "erreur" signal is asserted (high) and an error message is displayed on the simulator's standard output[see note 1]. The "erreur" signal is negated at the beginning of the simulation and remains low as long as no error is detected.

At the end of the simulation, a message is displayed indicating if the complete test failed or if it succeed [see note 1]. This message has a severity of type "error" if the test failed and a severity of type "note" if it succeeded. Don't forget to enable the display of these type of message for a proper simulation.

The DES component and all its sub-blocks are described in a single file: TCDG.V or TCDG.VHD. The testbench is completely described in the TCDG_BENCH.V or TCDG_BENCH.VHD file. This file must be compiled AFTER the other file since it has the highest level of hierarchy.
The figure 2 shows this hierarchy.

Compilation and Simulation script

The following commands are for Mentor ModelSim Tools™

Library creation:

```
vlib work
```

Compilation:

```
vcom -work work -explicit tcdg.vhd
```

Compilation of the test bench:

```
vcom -work work -explicit tcdg_bench.vhd
```

Simulation:

```
vsim -lib work tcdg_bench
```

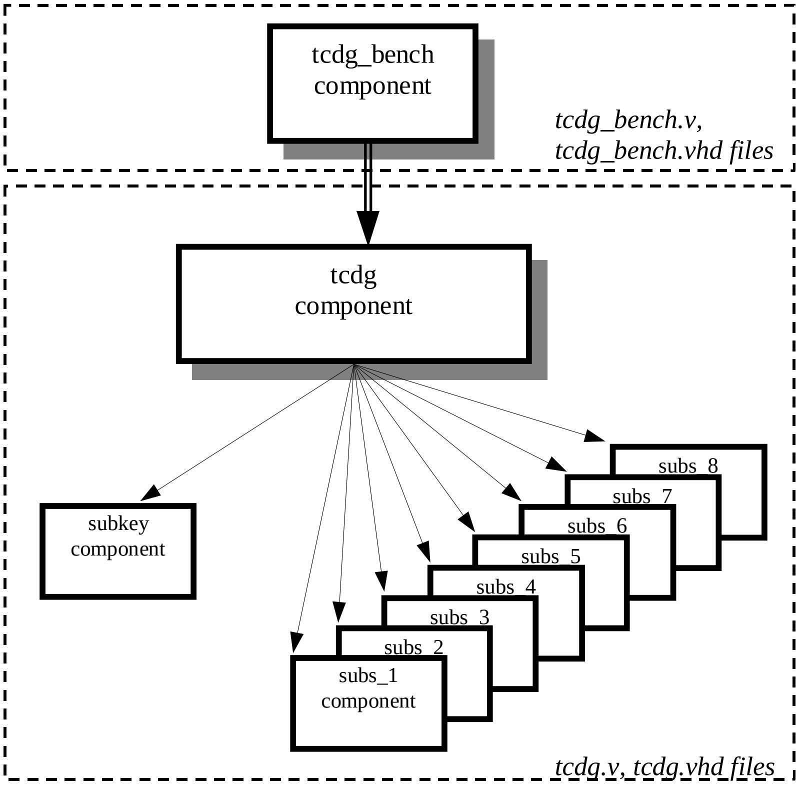


Figure 2. HDL files and design hierachy

[1] This feature is only available for the VHDL description. For the Verilog model, the value of the "erreur" signal must be tested at the end of the simulation.

Validation

The TCDG module is validated using test vectors. These vectors are composed of input parameters and an expected result. This expected result is automatically compared with the result of the TCDG operation.

The data input and expected results for these testbenches are taken from the following sources:

- The ANSI X3.106 specification
- The ANSI X9.52 specification
- Some vectors have been calculated using shareware using the DES algorithm.
- Some vectors have been calculated with the C++ description of the DES function.

In addition, the different permutation tables and the S-Box are formally compared with the one in the ANSI specification.

SYNTHESIS INFORMATION

Architecture

The DES has nine sub-blocks: "subkey" and "subs_1" to "subs_8". All the sub-blocks are completely combinatorial. The DES component and all its sub-blocks are grouped in the same file. The synthesis can be made directly on the top module by loading the TCDG.V or TCDG.VHD file. The subkey module is solely composed of multiplexers. Thus flattening this component will not modify drastically the result in term of area or speed.
The subs (S-Box permutation) are mainly look-up tables. Due to the specificity of the DES algorithm (pseudo-random permutations), the S-Box cannot be very well optimized.

The internal architecture of the DES is mainly composed of multiplexers, XOR gated and the substitution boxes. The control logic is very simple .

The easiest way to synthesize this component is to define a clock, set the correct input and output constraints regarding your design's constraints and to optimize the block (see "synthesis script" below)

The DES specification uses only a 56-bit key, but for most applications, a 64-bit key is provided. The 8 unused bits are often treated as parity control bit.
In this HDL description, the key input is 64-bit wide therefrom 8 inputs are unused. These unused inputs will be notified by the synthesizer.

Synthesis

The following commands provide you an example of constraints to synthesize the TCDG module with your Synthesizer.

synthesis script (for Synplicity™ Tools):

```
define_clock clk -freq 30.0

define_input_delay {k[63:0]}    -1000
define_input_delay {d[63:0]}    10
define_input_delay start        7
define_input_delay crypt        5
define_input_delay nreset       -1000

define_output_delay done        15
define_output_delay {q[63:0]}   5
```

synthesis result on FPGA Actel A54SX32-1:

Estimated frequency:	31 MHz
IO number:	187
Sequential cells:	163*
Combinatorial cells:	886

*The number of sequential cells given by the synthesizer is bigger here than the number of necessary flip-flops because of fan-out constraints. (Results given by Synplicity™ Tools).

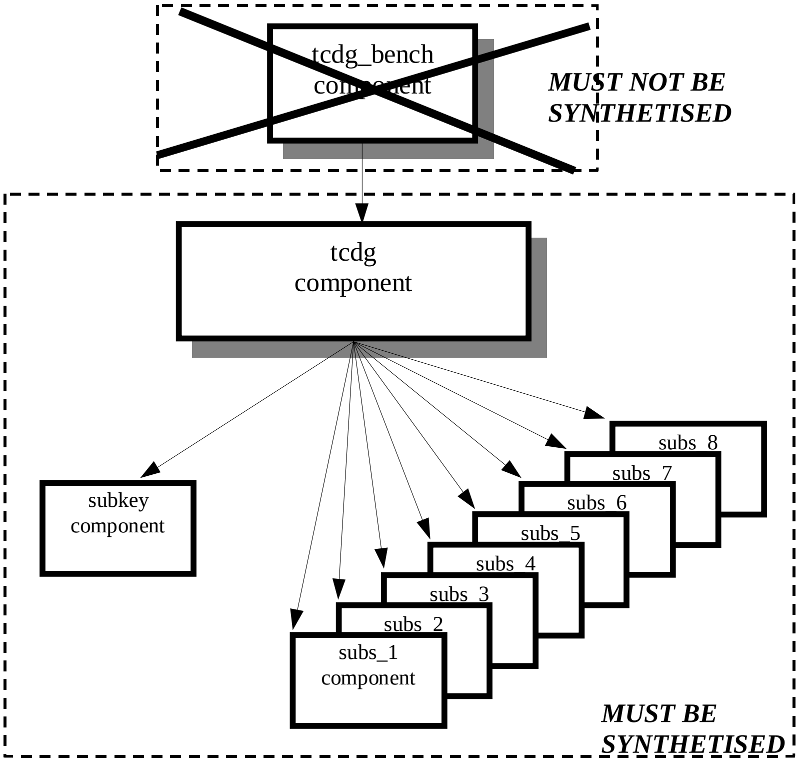


Figure 3. Design hierachy and synthesis

ORDERING INFORMATION

Worldwide Sales Offices

Tetraedre Sarl
Chenes 19
2072 Saint-Blaise
Switzerland

e-mail:	sales@tetraedre.com
web:	www.tetraedre.com
phone:	+41 79 402 25 39
fax:	+41 86 079 402 25 39

Device Number

TCDG VHDL VHDL description of the DES, including functional test bench.

TCDG Verilog Verilog description of the DES, including functional test bench.