Hardware Implementation of Triple-DES Encryption/ Decryption Algorithm

Fiolitakis Antonios*, Petrakis Nikolaos, Margaronis Panagiotis, Antonidakis Emmanouel

TEI of Crete, Department of Electronics
* E-mail: antonisf@chania.teicrete.gr

Abstract

This paper presents the design and the implementation of the Triple- Data Encryption Standard (DES) algorithm. A Hardware Triple-DES cryptographic algorithm has been implemented using a Field Programmable Gate Array (FPGA) chip.

In order to confirm the expected behavior of the Triple-DES circuitry, the implemented design was extensively simulated and analyzed. The Simulations were run under various clock frequencies.

The main objective of this paper is to provide the reader with a deep insight of the theory and design of a digital cryptographic circuit, which was implemented in a FPGA chip with the use of Very (High-Speed Integrated Circuit) Hardware Description Language (VHDL). A concise presentation of the cryptographic DES and Triple-DES Algorithms is given.

Keywords

Security, Communication, FPGA, VHDL

1 Introduction

Beyond any doubt, the need for secure storage or transfer of information is an inextricable part of human history. This need was initially created by the difference in social, political, military or even religious persuasions among people. Nowadays, the rapid evolution of communication systems offers, to a very large percentage of population, access to a huge amount of information and a variety of means to use in order to exchange personal data. Therefore, every single transmitted bit of information needs to be processed into an unrecognizable form in order to be secured. This encipherment of the data is necessary to take place in real time and for this procedure a variety of encryption algorithms have been developed.

This paper examines the full procedure of implementing an encryption algorithm using a high-level description language such as VHDL combined with the usage of FPGA technology.

The implementation of cryptographic algorithms on FPGAs can be reprogrammed on the same chip increasing the security through different versions of the same algorithm (DES and Triple-DES). The switching of wiring between algorithms on the FPGA chip can be easily achieved. Also, the features of the FPGA maximize the opportunity for on-chip parallelism. The DES and Triple-DES algorithms presented in this paper are used as an example for the implementation of cryptographic algorithms.
Finally, the completed designs after being tested, using the official test vectors for the implementations that the National Institute of Standards and Technology (NIST) [4] provides, were simulated in order to verify the expected defined outputs.

2 The Data Encryption Standard (DES) and Triple-DES Algorithms

Since the original development by an IBM team and the later on adaptation as a national standard in 1977 by NIST, the Data Encryption Standard (DES) has always been a basis for comparison for new encryption algorithms. Due to the constantly rising processor technology, DES is not an algorithm which is considered to be completely safe anymore. Despite this fact, it is still used in several applications such as IPSec protocols, ATM cell encryption, the secure socket layer (SSL) and in its Triple-DES form which was adopted in order to improve DES security in the X9.17 and the ISO 8732 standards [6-7].

In this section, we will describe in short the complete function of the DES algorithm as well as its variation called Triple-DES.

The operation of DES, as a symmetrical private key algorithm, is based on a single key of 64 bits which is used in order to perform both the encryption and decryption process. The data to be encrypted (plaintext) consists of 64 bits and after an initial permutation (IP) they are split into two equal halves $R_0$ and $L_0$ each of 32 bits of length. After 16 rounds of processing the final outputs $R_{16}$ and $L_{16}$ are inversed for the final permutation. This permutation is the inverse of the initial permutation. The complete function of the algorithm is shown in Figure 2-1.

![Complete DES Function](image)
1.1 The f Function and the Key Schedule

In this chapter, the f function will be analyzed and the key schedule will be explained in order to understand the complete procedure of the DES algorithm. As shown in Figure 2.2 the right half of the plaintext after being expanded from 32 bits to 48 bits is exclusively-ored with a certain round key. The result of this operation is led to the eight following substitution boxes which transform the 48-bit input to a 32-bit output. Finally, a simple permutation (P) is performed before the final output.

As mentioned before, on each round a certain key is applied. This key is produced by a specific procedure shown in Figure 2-3 and its characteristic is its two substitution permutations. When the initial 64-bit key is inserted, a permutation occurs (PC-1) in which every 8th bit of the key is used only for parity check and so its final size is reduced to 56-bits. Then, the key splits in two equal halves of 28-bits and each half is shifted (left, when we have an encryption progress or right, when decryption) zero, one or two bits depending on the number of round. After this operation a final permutation (PC-2) occurs.

Triple-DES is a minor variation of this standard. In fact, it contains three simple DES serial connected to each other in order to increase the length of the used key since two or three keys are applied depending on which mode of operation is used. Naturally, it is three times slower than the original form of DES but it is way more secure.
3 Implementation of Triple-DES

In this section, the implementation architecture of DES and Triple-DES will be analyzed. The complete design was implemented with the use of VHDL. The files of the components were run and tested on various clock frequencies. The maximum transfer rate achieved at 290 MB/sec (pipeline architecture).

Figure 3.1 represents the course that was followed for the digital implementation.

![Implementation Course Diagram]

Figure -4: Implementation Course

In order to implement the cryptographic algorithm, it was necessary to translate the mathematical expression of the specific algorithm to an equal expression on digital design. The following figures describe the complete process of the DES encryption algorithm which was separated to three parts. In the first part, an initial permutation of the plaintext and the permutation of the key occur (Figure 3-2). As shown in figure (Figure 3-3), the round function of DES is applied sixteen times before the final permutation IP⁻¹(Figure 3-4).
The complete Round function of DES is represented on Figure 3-5. This figure shows the architecture that was used in the present paper for the efficient implementation of the algorithm on a reconfigurable platform.
After programming, all the necessary VHDL files (Components) were connected to each other, as shown in the following Register Transfer Level (RTL) schematic diagram (Figure 3-6) in order to confirm the correct operation of the complete algorithm according to the official test vectors [4].

The Triple-DES algorithm was designed as three simple DES serial connected to each other. Instead of the first and third simple DES, the second performs the opposite operation using a different key. For instance, if the operation of Triple-DES is encryption, then the first and third simple DES perform encryption using key 1 while the second simple DES performs decryption using key 2. When Triple-DES operates in decryption mode, all the simple DES components work opposite respectively. The Triple-DES RTL architecture is illustrated in figure 3.7

Figure 3-8 illustrates the implemented components inside the chip. Additionally, the interconnections of the components are shown. The chip which was used for the Triple-DES implementation is mentioned below.

Xilinx, Device Family: Virtex- E, Chip XCV1600ebg560-8 C
Figure -11: Triple-DES Chip Implementation

Table 3-1 presents the chip’s implementation report.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Slices:</td>
<td>12635 out of 14039 90%</td>
<td></td>
</tr>
<tr>
<td>Number of Slice Flip Flops:</td>
<td>20505 out of 31104 65%</td>
<td></td>
</tr>
<tr>
<td>Number of 4 input LUTs:</td>
<td>15518 out of 31104 49%</td>
<td></td>
</tr>
<tr>
<td>Number of bonded IOBs:</td>
<td>243 out of 408 59%</td>
<td></td>
</tr>
<tr>
<td>Number of GCLKs:</td>
<td>1 out of 4 25%</td>
<td></td>
</tr>
<tr>
<td>Minimum period</td>
<td>6.564ns (Maximum Frequency: 152.346MHz)</td>
<td></td>
</tr>
</tbody>
</table>

Table -1: Implementation Summary

4 Conclusion

The present work introduces the worth point of a digital Triple-DES cryptographic algorithm implementation based on FPGA technology. This work can be used for high speed hardware circuitries where the need of privacy on communication is imperative.

5 References


