WP115 (v1.0) March 9, 2000

Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs

Author: Amit Dhir

Summary

Today's connected society requires secure data encryption devices to preserve data privacy and authentication in critical applications. Of the several data encryption types, Data Encryption Standard (DES) and its variant Triple-DES (TDES) have emerged to be the most commonly used in varying applications. The Spartan™-II devices with their extensive features and cost effectiveness compete effectively against ASICs and ASSPs. Through the value proposition of the DES/TDES IP in a Spartan-II FPGA, the programmable ASSP message is further confirmed. There is an immense value in integrating critical IP solutions like Discrete Cosine Transform/Inverse DCT (DCT/IDCT) and DES within a Xilinx FPGA to enhance performance and security in communication applications. A FPGA-based DES/TDES solution provides the necessary scalability and flexibility to handle all these applications and allows for tracking of new standards.

Introduction

Data encryption is used pervasively in today's connected society. The two most basic facets of modern day data encryption are data privacy and authentication. As modern society becomes more connected, and more information becomes available there is a need for safeguards which bring data integrity and data secrecy. In addition, authenticating the source of information gives the recipient, with complete certainty that the information came from the original source and that it has not been altered from its original state. Both, the needs for information privacy and data authentication has motivated cryptography.

- C*ryptosystem* or *cipher system* - A method of disguising messages so that only certain people can see through the disguise.
- *Cryptography* - The art of creating and using cryptosystems.
- *Cryptanalysis* - The art of breaking cryptosystems, and seeing through the disguise even when you are not supposed to be able to.
- *Cryptology* - The study of both cryptography and cryptanalysis.
- *Plaintext* - The original message
- *Ciphertext* - The disguised message
- *Encryption* - A fundamental security mechanism in which the ordinary data (plaintext) are transformed by the encryption process into ciphertext.
- *Decryption* - A procedure to convert ciphertext back into plaintext.

Encryption techniques are used to safeguard information while it is stored within a network node or while it is in transit across communications media between nodes. A cryptosystem is usually a whole collection of algorithms. The algorithms are labeled; and the labels are called *keys*. The people who are supposed to be able to see through the disguise are called recipients. Other people are enemies, opponents, interlopers, eavesdroppers, or third parties.

As an example, for a plaintext message being sent, if every A is replaced with a D, every B is replaced with an E, and so on through the alphabet, only someone who knows the "shift by 3" rule can decipher the messages. Hence a "shift by n'' encryption technique can be performed for several different values of n. Therefore, n is the key here.

With the expansion of applications requiring data encryption, the number of different encrypting methods have also increased. Each method has its strengths and weaknesses. Some of the encryption methods are RSA (Rivest-Shamir-Adleman), Data Encryption Standard (DES), Diffie-Hellman, Secure Hashing Algorithm (SHA), Blowfish, RC4/RC5, Elliptic Curves, ElGamal, LUC (Lucas Sequence) and so on.

This white paper discusses DES and its variant Triple-DES (TDES). The Spartan-II family, combined with a vast soft IP (Intellectual Property) portfolio is the first programmable logic solution to effectively penetrate the ASSP (Application Specific Standard Products) marketplace. The DES and TDES solutions presented from Xentec, when ported on a Spartan-II device are good examples highlighting the concept of a programmable ASSP. Xentec is a member of the Xilinx AllianceCORE™ program and has a wealth of IP cores in other applications.

Xentec, Inc., founded in 1995, provides solutions for the design and development of analog/digital ASICs and FPGAs. The FPGA and ASIC solutions developed by Xentec are being used in multimedia, telecommunications, and cryptoprocessor designs. The company has over 50 analog and digital projects to its credit, ranging from developing test programs to full turnkey IC designs. Xentec provides cores in Xilinx-specific formats as well as in RTL HDL to suit customers' needs. Xentec also offers comprehensive design services and support. For more information regarding Xentec and their IP portfolio for Xilinx products please visit http://www.xilinx.com/products/logicore/alliance/xentec/xentecinc.htm.

The X_DES Cryptoprocessor and X_3DES Triple DES Cryptoprocessor cores are developed, sold, and supported by Xentec. The Spartan-II devices which implement these cores support the X9.52 standard and are NIST (National Institute of Standards and Technology) certified. These cores are available immediately for use in Spartan-II FPGAs and can be purchased directly from Xentec. The X_DES application note can be obtained from http://www.xilinx.com/products/logicore/alliance/xentec/xdes.pdf. The X_3DES application note can be obtained from http://www.xilinx.com/products/logicore/alliance/xentec/x3des.pdf.

Data Encryption Standard

The DES is based on the work of IBM Corporation, and was adopted as the American National Standard (ANSI) X3.92-1981/R1987. The DES algorithm was adopted by the U.S. government in 1977, as the federal standard for the encryption of commercial and sensitive-yet-unclassified government computer data and is defined in *FIPS 46* (1977). (FIPS are Federal Information Processing Standards published by NIST).

A "block cipher" refers to a cipher that encrypts a block of data all at once, and then goes on to the next block. The DES, which is a block cipher, is the most widely known encryption algorithm. In block encryption algorithms, the plaintext is divided into blocks of fixed length which are then enciphered using the secret key. The DES is the algorithm in which a 64-bit block of plaintext is transformed (encrypted/enciphered) into a 64-bit ciphertext under the control of a 56-bit internal key, by means of permutation and substitution.

It has been mathematically proven that block ciphers are completely secure. The DES block cipher is highly random, nonlinear, and produces ciphertext which functionally depends on every bit of the plaintext and the key. At least five rounds of DES are required to guarantee such dependence. In this sense, a product cipher should act as a "mixing" function which combines the plaintext, key, and ciphertext in a complex nonlinear fashion. The DES has more than 72 quadrillion (72×10^{15}) possible encryption keys that can be used. For each given message, the key is chosen at random, from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. The process can run in several modes and involves 16 rounds or operations. The DES algorithm is widely used and is still considered reasonably dependable but a more secure variant, which applies DES three times with different keys in succession called Triple-DES (TDES). The Xilinx Spartan-II FPGAs and Xentec soft IP present a solution for both DES and TDES.

The DES cryptographic algorithm converts plaintext to ciphertext using the 56-bit key in the encryption process. The same algorithm is reused with the same key to convert ciphertext back to plaintext, in the decryption process. The key is given in a 64-bit word, of which eight are parity bits, at locations 8, 16, 24,…, 64. The algorithm consists of 16 "rounds" of operations that mix the data and key together in a prescribed manner using the fundamental operations of permutation and substitution. The goal is to completely scramble the data and key so that every bit of the ciphertext depends on every bit of the data plus every bit of the key.

Authorized users of encrypted computer data must have the key that was used to encrypt the data in order to decrypt it. The unique key chosen for use in a particular application makes the results of encrypting data using the algorithm unique. Using a different key causes different results. The cryptographic security of the data depends on the security provided for the key used to encrypt and decrypt the data. FIPS 171 (Key Management Using ANSI X9.17) provides approved methods for managing the keys used by the DES.

There are four official DES operating modes (provided in FIPS 81) to encrypt or decrypt data: ECB (Electronic Codebook), CBC (Cipher Block Chaining), OFB (Output Feedback) and CFB (Cipher Feedback).

The security provided by a cryptographic system depends on the mathematical soundness of the algorithm, length of the keys, key management, mode of operation, and implementation.

The DES was originally developed to protect unclassified computer data in federal computer systems against a number of (passive and active) attacks in communications and computer systems. It was assumed that a knowledgeable person might seek to compromise the security system by employing resources commensurate with the value of the protected information. Agencies determining that cryptographic protection is needed based on an analysis of risks and threats can use the DES for applications such as electronic funds transfer, privacy protection of personal information, personal authentication, password protection, and access control.

The DES has been evaluated by several organizations and has been proven mathematically secure. Some individuals have analyzed the DES algorithm and have concluded that the algorithm would not be secure if a particular change were made (e.g., if fewer "rounds" were used). Modifications of this sort are not in accordance with the standard and, therefore, may provide significantly less security. NIST believes that DES provides adequate security for its intended unclassified applications. The algorithm is also widely used by the private sector. NIST will continue to evaluate the security provided by the DES. The standard provides increasing, qualitative levels of security and covers module design and documentation, interfaces, authorized roles and services, physical security, software security, operating system security, key management, and other issues.

The users of DES (including federal organizations) may generate their own cryptographic keys. DES keys must be properly generated and managed to assure a high level of protection to computer data. The key management process for DES (or even other cryptosystems) includes the generation, distribution, storage (and protection), maintenance of access control, and destruction of the cryptographic keys used in the encryption and decryption processes. The encryption keys are used to "lock" and "unlock" the secure data traffic, with the sender of data using the key to encrypt the data, and the recipient using the same key to restore the data to its original form. In a network with 100 nodes the number of keys required could reach over 4,900; and in a network with 500 nodes the number could total over 124,000.

Technical Overview (Fundamental Theory) of the DES Algorithm

The DES is a block cipher. It is in a high grade, similar to ordinary simple substitution ciphers except that there are blocks of symbols instead of single symbols. Simple substitution is to replace an input symbol with another symbol. A block cipher works in the same way, except that the symbols are grouped in blocks, and substitution takes place over this large composite symbol space. (See Figure 1.)

Let **m** be a block of bits of plaintext, **k** the key for encipherment and **c** the resulting block of bits of ciphertext. The enciphering function **f** is dependent on key **k** and plaintext **m**, such that **c** = **f**(**k**,**m**). Also **m** is uniquely recoverable from **c** with an inverse deciphering function dependent on the key **k** and ciphertext **c**, such that **m** = $\mathbf{f}^{-1}$(**k**,**c**).

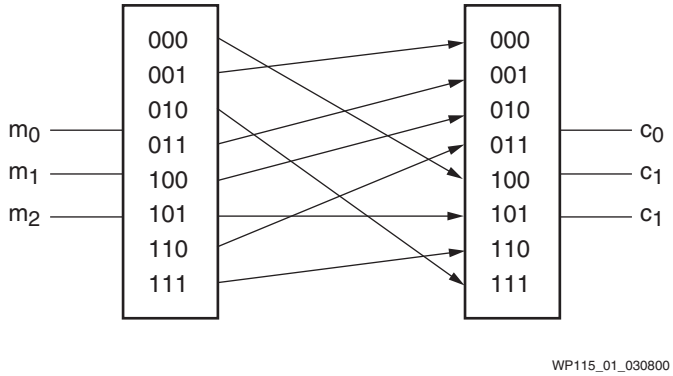

Figure 1: **Block Cipher System**

A simple example clarifies the definition of the block cipher system. Suppose that size(**m**) = size(**c**) = **n** bits. The key **k** is a vector that determines the permutation.

$$\mathbf{k} = \{\mathbf{k_1}, \mathbf{k_2}, \ldots\ldots, \mathbf{k_n}\}.\ \text{Assume now that } \mathbf{n} = 3, \text{ and } \mathbf{k_E} = \{4,0,7,1,2,5,3,6\}_8$$

The system would then look like Figure 1. There is now a 3-bit input and a 3-bit output. The key serves as a reference table for substitution. For example, if m = 001_2, look at the key and find that 001_2 is replaced by 000_2 and that is the output. The decryption is no different from the encryption except that the encryption key must be reversed. The key for decryption would then look like $\mathbf{k}_D = \{1,3,4,6,0,5,7,2\}_8$.

In the example described above blocks of three bits are used. In general there exists a theoretical possibility to describe all block cipher systems in this way. But this would be an impossible task to practice. Imagine that size(**m**) = size(**c**) = 6 bits; this would imply that we require a 296-bit key. The goal is to design block cipher systems with the ability to encipher large blocks of bits, with a small key, which is however sufficiently large to resist an exhaustive search.

The DES algorithm (explained in FIPS 46) contains three types of operation: permutation, substitution and bitwise-XOR (⊕). All exchanges with blocks and shifts on blocks may also be regarded as permutations. The permutations included in the standard work are used in three different ways:

- First, there is plain permutation, where all the bits are used exactly once. The output block has the same size as the input block.
- Permuted choice is when the block size is reduced by only choosing some bits of the input block.
- Finally the expansion permutation, where some input bits are copied more than one time to different ouput locations. The resulting block in this kind of permutation is larger than the input block.

These are all shown in Figure 2.

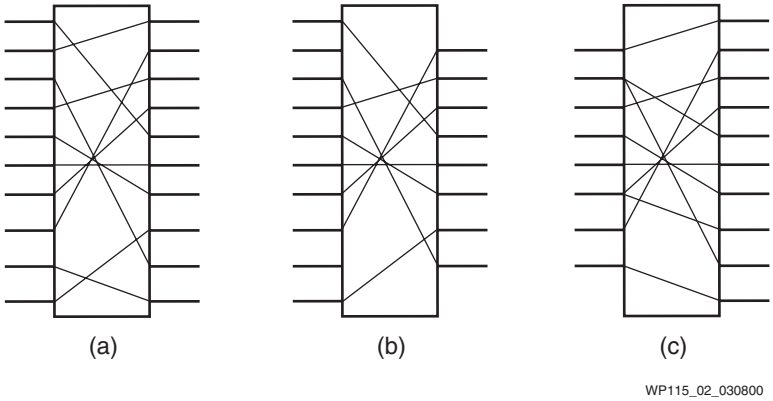

Figure 2: **a) Plain Permutation; (b) Permuted choice; (c) Expansion permutation**

The DES algorithm works with 64-bit blocks, as seen in Figure 3. The input block is first subject to a plain permutation, which in the standard is called the initial permutation and denoted IP. See Table 1 for the result of the IP. All the permutation tables show the output block, and for each position, the number indicates the position in the input block to be copied.

Table 1: **Initial Permutation (IP)** *(courtesy: THE DES)*

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

The permuted block is split into two equally sized blocks (L_0, R_0), which become the input for the first round. The round manipulates these two blocks and the output becomes two new blocks (L_1, R_1).

$$L_1 = R_0$$

$$R_1 = L_0 \oplus f(R_0, K_1)$$

The subkey K_1 is chosen by a key scheduling algorithm, which generates subkeys from a 56-bit long key. The DES contains 16 rounds and each round can be described as:

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$$

Except in the last round, where the swap at the end of the round is skipped.

$$R_{16} = R_{15}$$

$$L_{16} = L_{15} \oplus f(R_{15}, K_{16})$$

The two blocks are finally subject to a final permutation, denoted FP, which is, in fact, the inverse of the Initial Permutation. The result of the FP is shown in Table 2.

Table 2: **Final Permutation (FP) (Courtesy: THE DES)**

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

The decryption of the algorithm does not differ from the encryption. The very same algorithm is used, with the only difference being that we use the subkeys in reverse order. The outline of the DES cipher system is shown in Figure 3.

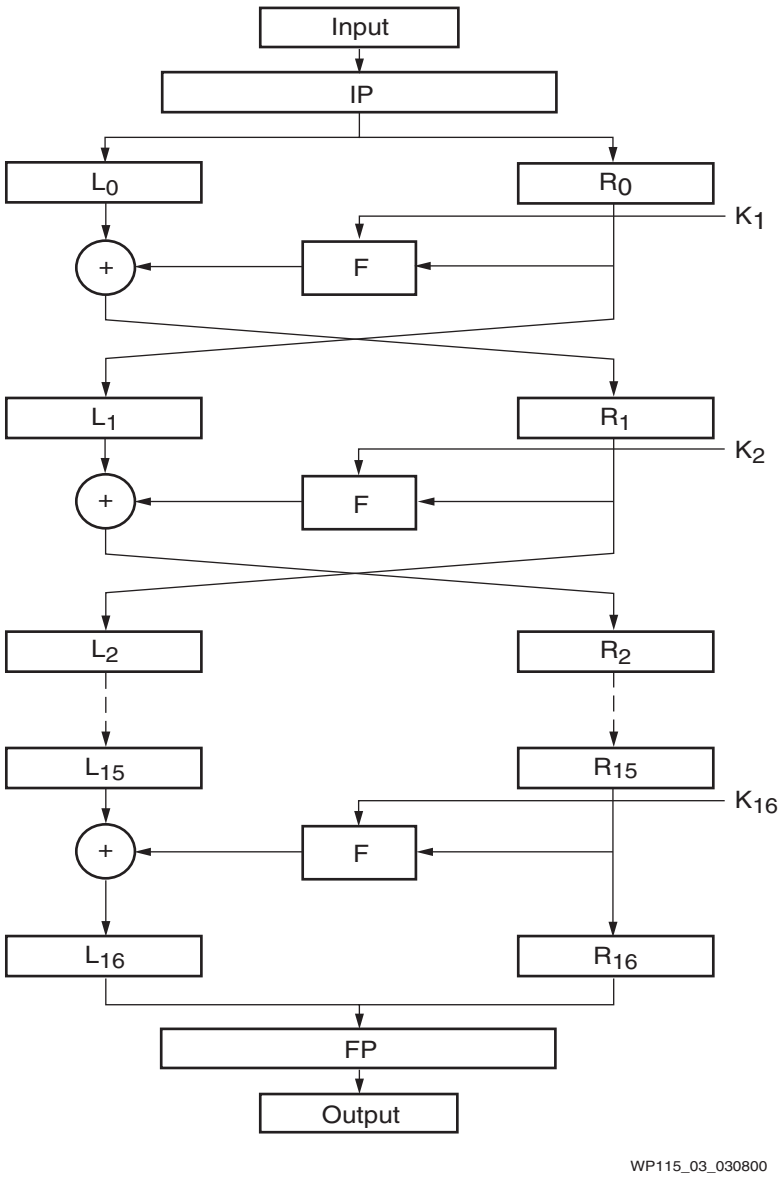

Figure 3: **Outline of the DES Cipher System** *(courtesy: THE DES)*

Triple-DES

The DES algorithm is popular and in wide use today because it is still reasonably secure and fast. There is no feasible way to break DES, however because DES is only a 64-bit (eight characters) block cipher, an exhaustive search of 2^{55} steps on average, can retrieve the key used in the encryption. For this reason, it is a common practice to protect critical data using something more powerful than DES.

A much more secure version of DES called Triple-DES (TDES), which is essentially equivalent to using DES three times on plaintext with three different keys. It is considered much safer than the plain DES and like DES, TDES is a block cipher operating on 64-bit data blocks. There are several forms, each of which use the DES cipher three times. Some forms of TDES use two 56-bit keys, while others use three. TDES can however work with one, two or three 56-bit keys. With one key TDES = DES. The TDES can be implemented using three DES blocks in serial with some combination logic or using three DES blocks in parallel. The parallel implementation improves performance and reduces gate count.

Using standard DES encryption, TDES encrypts data three times and uses a different key for at least one of the three passes. The DES "modes of operation" may also be used with triple-DES. This 192-bit (24 characters) cipher uses three separate 64-bit keys and encrypts data using the DES algorithm three times. While anything less than that can be considered reasonably secure only the 192 bit (24 characters) encryption can provide true security. One variation that takes a single 192 bit (24 characters) key and then: encrypts data using first 64 bits (eight characters), decrypts same data using second 64 bits (eight characters), and encrypts same data using the last 64 bits (eight characters).

For some time, it has been a common practice to protect and transport a key for DES encryption with triple-DES. This means that the plaintext is, in effect, encrypted three times. A number of modes of TDES have been proposed:

- DES-EEE3: Three DES encryptions with three different keys.
- DES-EDE3: Three DES operations in the sequence encrypt-decrypt-encrypt with three different keys.
- DES-EEE2 and DES-EDE2: Same as the previous formats except that the first and third operations use the same key.

Encryption can be further intensified with longer keys. Keys are usually 56 bits or 128 bits, with 56 bits generally considered the smallest size for sufficient protection. For multinational organizations, this is a problem because the U.S. State Department requires that exportable encryption technology use keys no longer than 40 bits. TDES has not been broken and hence its security has not been compromised.

Applications of DES/TDES

The DES and TDES devices are used by the federal department and other government agencies for cryptographic protection of classified information. The federal government standardizes DES and specifies interoperability and security-related requirements for using encryption at the Physical Layer of the ISO Open Systems Interconnection (OSI) Reference Model in telecommunications systems conveying digital information. In addition to preserving confidentiality, cryptography can be used for:

- Authentication: the receiver of the message can ascertain its origin
- Integrity: the receiver can verify if the message was modified during the transmission
- Non-repudiation: the sender cannot deny that she sent the message

The DES and TDES cores are very compact cores. Encryption cores are typically implemented with data and key buses connected to other modules internal to the FPGA. Data encryption (and particularly DES) is primarily applied in:

- Electronic financial transactions: Automatic Teller Machines (devices limited to the issuance of cash or travelers checks, acceptance of deposits, or account balance reporting)
- Secure data communications, paving the road for e-commerce
- Secure video surveillance systems
- Encrypted data storage and proprietary software protection
- Access control: Software or hardware which protects passwords or Personal Identification Numbers (PINs) against unauthorized access.

The DES and TDES functionality is usually integrated within embedded systems. Xilinx presents several IP solutions which integrate with the DES/TDES IP. The DCT/IDCT (discrete cosine transform/inverse DCT) solutions (also provided by Xentec) are applied in DVDs (JPEG), cable TV, DBS systems, HDTV, graphics, Ultrasound/MRI systems, digital VCRs, set-top boxes, digital cameras, etc. These applications also require the DES algorithm for data encryption, thus presenting a smart system-on-a-chip solution. The combination of the DCT/IDCT and DES cores from Xentec ported on a Xilinx FPGA shortens time to market (TTM), and also makes Xilinx a one stop shop for data encryption for various applicatons like real-time video, secure camera systems, etc.

The Virtex™ series FPGAs are well suited for high-performance applications due to the high clock speeds, large gate densities and system-level features. The X_DES core runs at an effective bit rate of about 500 Mbits/sec in a Xilinx Virtex-E device. The small DES and TDES cores allow for easy integration with other Xilinx IP solutions to build large complex systems in the Virtex series FPGAs. These include internet, intranet, and extranet networks facilitating secure business-to-business transactions, satellite digital cinema, secure satellite broadcast, secure video surveillance and space imaging systems.

The DES and TDES cores developed specifically for Spartan-II devices offer a low-cost solutions that designers can use in combination with other Xilinx IP solutions to develop consumer appliances. Some of these consumer applications include e-commerce security enabled PCs and cable modems, set-top boxes, home networking, wireless LAN and Bluetooth wireless systems, and financial transactions such as prepaid smart cards and personal banking systems.

DES is used in gateways to ensure privacy of user data. It is portable terminals, POS (point-of-sale) equipment in wireless communication products. The DES algorithm also provides secure digital voice encryption in hand-held communication devices such as land mobile radio and dispatch control consoles.

Data encryption through DES and Triple-DES is prevalent in Fax machines. This allows secure data transfer over phone lines and prevents active interception of one's faxes at the receiver end, which is prevented by password entry by the user for fax retrieval.

Networking applications use DES and Triple-DES to provide network protection through data privacy, data integrity, access control and authentication. Message and file security, user authentication, secure remote system logon, and multilevel system access require data encryption, and DES and Triple-DES algorithms are the most prevalent.

Virtual Private Networks (VPN)

There is a need for control and access between different entities in a company's business environment, to provide secure communication between remote offices, business partners, customers, and travelling and telecommuting employees. Transmitting messages over the existing Internet backbone poses risks. VPNs were introduced to tackle exactly these issues to provide a company owned and managed network architecture. These networks provide

scalable and comprehensive solutions by utilizing existing Internet backbone with additional hardware and software solutions. Strong data encryption is necessary to extend security and control features for which DES and Triple-DES are the most commonly used. This provides secure network traffic through data privacy, data integrity, access control and authenticating entities by providing a gateway to each point of access into the business.

DES/TDES Applications in ATM Networks

(courtesy: SECANT Network Technologies/ Celotek Corporation):

TDES and DES algorithms have been used for cell payload encryption. Key management in perimeter security systems that provide privacy through high-speed cryptography for information traversing between private and public ATM (Asynchronous Transfer Mode) networks. The cryptographic units heighten security interfaces between a secure LAN and a public network. As data crosses this interface, the system encrypts each ATM cell's payload without affecting the header. Encrypted cells pass through the public network infrastructure and are decrypted upon arriving at the destination LAN. The benefit is that the user can conduct business as usual within the LAN and can encrypt the data as it enters the non-secure public network or non-secure area of a LAN. The system provides privacy and access control guarantees when using public ATM networks.

Data security in e-Commerce applications is required to have secure website, conduct financial transactions over the Internet, authentication of users to Intranets and Extranets, secure messaging (including X.400/EDI) and secure storage of digital signature keys for signature generation and verification for digital documents.

Smartcard Solutions

(courtesy: Cylink Corporation)

Smartcard solutions are used in wireless communication, loyalty systems, banking Pay TV and government ID. These are used to provide strong authentication in e-business. These solutions are used with standard non-secured PCs. Consumers, vendors and financial institutions need to know that the transactions, documents and identities are authentic. DES and Triple-DES algorithms are the most used encryption methods in data security for the Smartcard solutions.

Spartan-II FPGA and DES/TDES Soft-IP Solution

The Spartan-II family with its unique features, density, an extensive synthesizable IP (Intellectual Property) portfolio and the cost structure competes effectively against ASSPs. Spartan-II IP cores are available through the AllianceCORE program, which is a cooperative effort between Xilinx and independent third-party core developers. It is designed to produce a broad selection of industry-standard solutions dedicated for use in Xilinx FPGAs. A programmable logic version of a core must have value over an ASIC/ASSP version of the same function. It must be cost effective and make sense for use in a programmable device in a production system. Consequently, Xilinx does not promote generic, synthesizable cores as AllianceCORE products. Instead, they are generally provided as black boxes. This guarantees that the implementation is optimized for density while still meeting performance, preserving the time-to-market value of programmable logic. Allowing quick implementation of unique logic on the same device provides flexibility. Partners may provide cores customized to meet specific design needs. Source code versions of the cores are often available from the partners at additional cost for those who need ultimate flexibility.

With the availability of the Spartan-II family, the DES and TDES solution can be implemented using a single Spartan-II device and the IP provided by Xentec.

Xentec, Inc.

The *X_DES Cryptoprocessor core* (Figure 4) from Xentec supports Spartan-II devices . The solution has the following features:

- Fully compliant (conforms to FIPS 46-3 and ANSI x9.52) 56-bit DES implementation
- Both encryption and decryption is supported
- Encryption and decryption performed in 16 clock cycles
- No dead cycles for key loading or mode switching
- Suitable for triple DES implementations
- Suitable for ECB, CBC, CFB and OFB implementations
- Sustained bit rate is four times the clock speed
- High clock speed and low gate count achieved
- Fully synchronous design
- Fully functional and synthesizable VHDL or Verilog soft-core is available
- Test benches provided

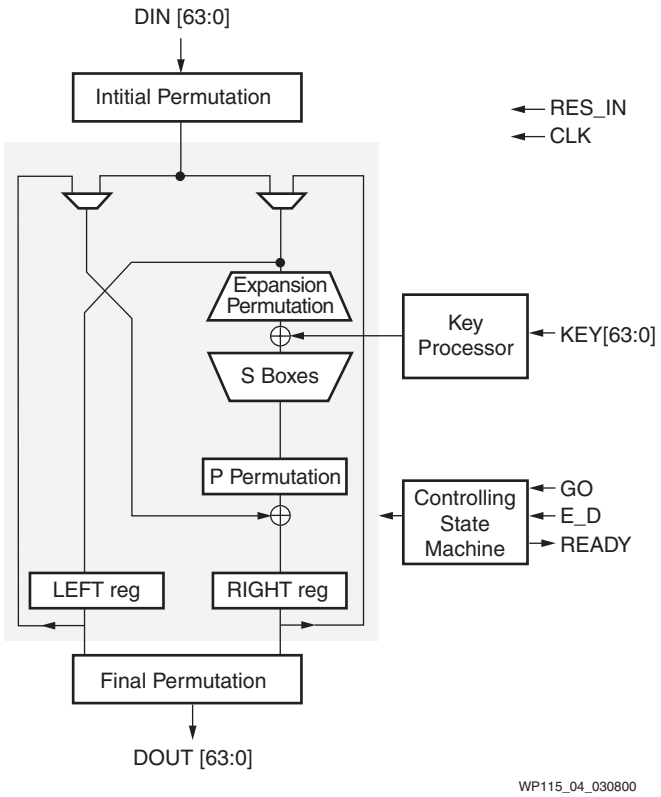

Figure 4: **X_DES Cryptoprocessor Block Diagram** *(courtesy: Xentec, Inc.)*

The X_DES core is a fully compliant hardware implementation of the DES encryption algorithm, suitable for a variety of applications. The DES algorithm is the result of a joint effort between IBM and the NSA and was adopted as a federal standard in November 1974.

The Xentec *X_3DES Triple-DES Cryptoprocessor* (Figure 5) supports the Spartan-II FPGA family . The features are:

- Implemented according to the X9.52 standard
- Implementation based on NIST certified DES core
- Two independent keys supported
- Both encryption and decryption supported
- Encryption and decryption latency is 48 clock cycles and throughput is 16 clock cycles
- No dead cycles for key loading or mode switching
- Fully synchronous design
- Available as a fully functional and synthesizable VHDL or Verilog soft-core
- Test benches provided
- Xilinx netlist available

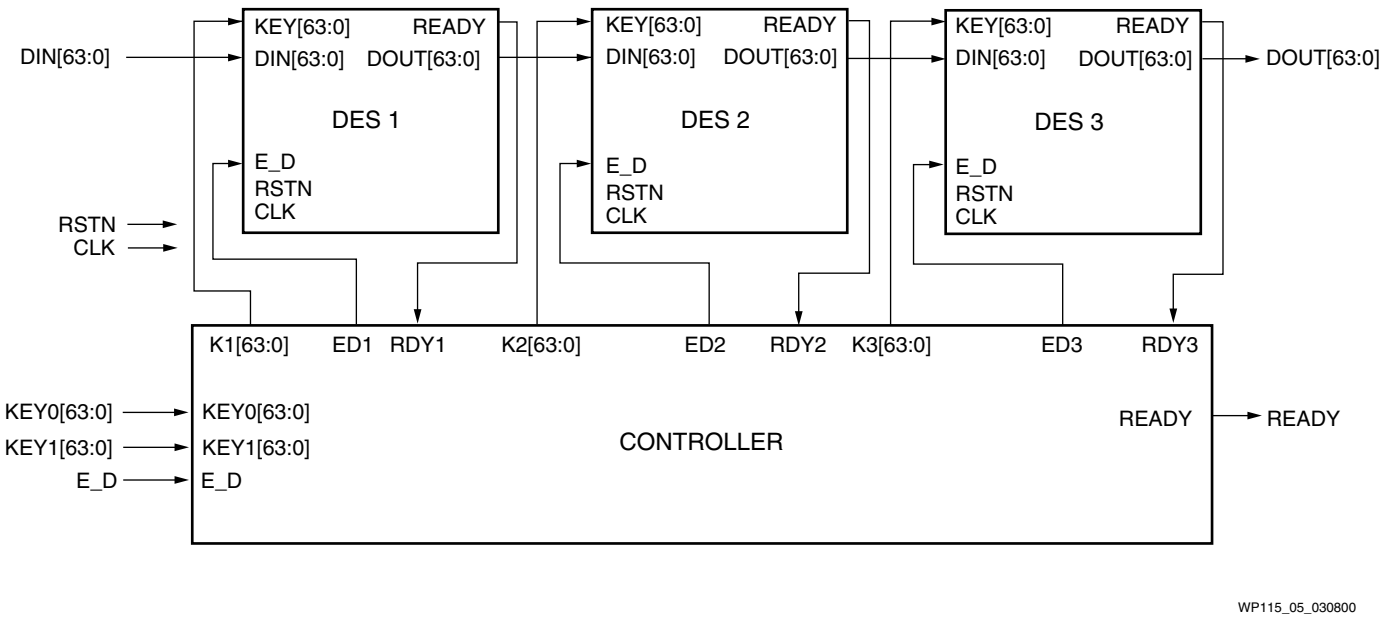

Figure 5: **The Triple-DES Implementation** *(courtesy: Xentec, Inc.)*

This core is a full implementation of the TDES encryption algorithm. Both encryption and decryption are supported. The TDES algorithm was proposed by IBM Corporation when it became clear that the security of the DES had been compromised by advances in computer technology. Compared to the DES algorithm, the TDES provides a significantly higher level of security. Each TDES encryption/decryption operation (as specified in ANSI X9.52) is a compound operation of the DES encryption and decryption operations. The X_3DES triple DES core supports the most popular ECB mode, while providing customization for other modes as well. The TDES algorithm coincides with the DES algorithm, providing backward compatibility.

Advantage of the Spartan-II FPGA and DES/Triple-DES Soft-IP Solution

Programmable Logic Devices (PLDs) have always been viewed as being expensive, slower, and less feature rich than comparable ASICs. This limited their success in penetrating the ASSP market. Bringing programmability and its traditional benefits to a design solution is always an expensive proposition and PLDs have traditionally lost the battle to the cost-optimized custom solution or ASIC. The use of innovative process technologies has leveled this playing field. This approach has allowed PLDs to significantly reduce die sizes, and therefore

lower the cost of the overall solution. This rapid transition in process technology has allowed PLD vendors to service the needs of today's ASSP designers. The Spartan-II FPGAs offer more than 100,000 system gates at under $10, hence making them the most cost-effective PLD solution ever offered. They address low cost and fast time-to-market, but more importantly integrate powerful new system-level features that provide an attractive solution for today's system level designer. The associated features include SelectI/O™, Block SelectRAM™, Distributed RAM, DLL (delay-locked loop) circuits, clock speeds up to 200 MHz, and aggressive power management.

The extensive features position the Spartan-II family as a low-cost, high-performance ***programmable ASSP*** alternative and expand the time-to-market advantage that PLDs traditionally offer. There are some significant advantages in using the DES/TDES soft-IP in a Spartan-II device.

Performance

FIPS 46 allows implementation of the cryptographic algorithm in software, firmware, hardware, or any combination thereof to enable more flexible, cost-effective implementations. However, a hardware implementation runs inherently faster (even by an order of magnitude) than a software implementation. The bit data rate is four times the clock rate, i.e., 100 MHz = 400 Mbps. The hardware implementation of the DES and TDES IP ported on a Spartan-II device uses 272 CLBs and provides performance upwards of 100 MHz. Most real-world consumer applications such as real-time video require only DES (and not TDES) due to performance degradation, because of extra computation.

The Xilinx Spartan-II FPGA hardware can speed the factorization of large numbers, by setting up four memory banks that are accessed simultaneously, and hence offering parallel computing. This approach increases execution speeds in repetitive calculations, required for sieving.

NIST approved

The DES soft IP for Spartan-II FPGAs is NIST approved and meets all government standards. The TDES standard is still in the process of being approved by NIST, and is a standard that all ASSPs are required to meet.

Value addition of a reconfigurable fabric

The Spartan-II family accommodates specification changes that can be easily adopted, in post volume production as part of the solution. Conflicting specifications and lack of a clear direction create the need for programmable ASSP solutions. The reprogrammable FPGA fabric permits the use of DES and TDES as needed, and allows ability to include any specification changes made by the government later. It would be nearly impossible and cost-prohibitive for an ASSP vendor to cater to all the various specifications. However, at the same time betting on the success of one single product may preclude them from being successful in the marketplace. These conditions create many opportunities for the Spartan-II family—the industry's first programmable ASSP. Because of the high profit margins involved with these products, designers can easily continue using programmable ASSPs in volume production.

The programmable fabric can also encode and decode with larger and better transformation blocks. The key can be changed within the fabric in quick intervals. Additionally if a key is ever broken, the Xilinx solution can be reconfigured instantly. Use of reconfigurable devices lets the algorithms be changed or swapped entirely, which has become a requirement in some multi-algorithmic cryptographic systems (such as Secure Socket Layer). Hence, AES hardware can be designed now, even before the standard is established.

Most stand-alone ASSPs never behave as expected, due to reasons ranging from bugs in the silicon, system integration issues, software drivers, or even user errors. Irrespective of the cause, verifying and identifying device problems can be very difficult with ASSPs, but a lot easier with programmable ASSPs. Having been built on the fabric of a proven FPGA technology and having silicon that is pre-verified and guaranteed to perform, potential problems in the Spartan-II family are narrowed down to a software-only issue. Xilinx provides powerful

tools that improve the transparency of the final solution. With the help of HDL simulators, test benches, and run-time debugging tools like ChipScope designers can easily identify the problem. Because a programmable ASSP is inherently reprogrammable, fixing the problem is also simple. This is a tremendous value-add feature that a stand-alone ASSP cannot offer. It is much simpler to integrate a DES/TDES device that is reprogrammable, than an ASSP which performs its specific task.

Solutions Approach

Using the Spartan-II family in conjunction with appropriate IP cores allows the designer to choose the right feature set and optimize the programmable ASSP, to achieve the best possible results. Designers can also integrate their value proposition within the same piece of silicon, to allow product customization and reduce costs. This flexibility comes at a significantly lower cost when compared to the fixed ASSP solution, due to the inherent low cost of the Spartan-II family. Being integrated in consumer applications like e-commerce security-enabled PCs, cable modems, set-top boxes, home networking, wireless LAN and Bluetooth wireless systems, and in financial transactions such as prepaid smart cards and personal banking systems, highlights the value proposition of Spartan-II FPGAs.

IRL: Internet Reconfiguration Logic

Through the Xilinx Online (IRL) program, a programmable ASSP, such as the Spartan-II family, allows a designer to gain market share by bringing them to market sooner than a stand-alone ASSP. Spartan-II FPGAs are based on SRAM technology and are customized by loading configuration data into internal memory cells and therefore it is very easy to re-program them an unlimited number of times. Updating the functionality of the FPGA only requires that the designer include a mechanism for updating the configuration bitstream. Remotely updating software with any new enhancements and bug fixes, increases the life of the DES/TDES device within any equipment. Designing systems that do remote upgrades can also provide new revenue opportunities. After the initial product is released, new hardware features can be developed, sold and distributed inexpensively to existing customers in much the same way as new versions of software can be distributed today. In addition, a standard "off-the-shelf" application can be developed so that the features can be swapped in and out depending on what the end-user purchases or needs. The designer can hence take advantage of the fact that the solution now allows them to upgrade their hardware and stay in the market-place longer, thus maximizing profitability.

These significant features like high performance, being NIST approved, value proposition against ASSPs by accommodation of specification changes (through reconfigurable logic), reduced TTM, improved testing and verification, field upgradability (IRL) and cost effectiveness show the advantage presented by Spartan-II devices. This positions the Spartan-II FPGAs to better than other programmable logic and ASSP solutions, making the Spartan-II family a clear winner in not only the data encryption market, but in other ASSP niche areas also.

The Spartan-II family is unaffected by the hurdles that an ASSP vendor needs to overcome and offers a cost-effective programmable ASSP solution; its inherent advantages extend the reach of the Spartan family to new levels and creates new opportunities for PLDs in the ASSP market.

The dynamics in the ASIC/ASSP marketplace are opening up new opportunities for PLDs and is allowing them to compete against ASSPs. Due to its extensive features and cost effectiveness, the Spartan-II solution has all the unique ingredients that enable Xilinx to succeed against traditional ASSPs. The underlying programmable nature to the solution further bolsters the value of a programmable ASSP. An end customer can choose to use the DES/TDES solution as sold by Xilinx or choose to augment or change the solution to best suit their needs. This is a testimonial to the tremendous potential that PLD vendors have for addressing the ASSP marketplace.

Conclusions

Data encryption devices are deployed within a vast number of different critical data communication applications. DES and Triple-DES are the most common of encryption methods. The Spartan-II devices with their extensive features and cost effectiveness compete effectively against ASICs and ASSPs. Through the value proposition of the DES/TDES IP in a Spartan-II FPGA, the programmable ASSP message is further confirmed. These solutions enhance performance and security within communication applications. A FPGA-based DES/TDES solution provides the necessary scalability and flexibility to handle all these applications and allows for tracking of new standards. This positions the Spartan-II family uniquely in being able to compete with ASSPs.

References

"The Spartan-II Family – The Complete Package", Krishna Rangasayee

Xentec, Inc.

"The DES, An Extensive Documentation and Evaluation", Mikael J. Simovits

NIST, *"Computer Security Resource Clearinghouse"*; http://csrc.nist.gov

Export and Usage Restrictions

Concerned that the encryption algorithm could be used by unfriendly governments, the U.S. government has prevented export of encryption software. Since there is some concern that the encryption algorithm will remain relatively unbreakable, NIST has indicated DES may not be recertified as a standard and submissions for its replacement are being accepted. The next standard will be known as the Advanced Encryption Standard (AES). Specific cryptographic implementations under jurisdiction of the Department of Commerce, Bureau of Export Administration, U.S. Department of Commerce, are responsible for granting export licenses for cryptographic products (including DES).

The National Security Agency (NSA) of the U.S. Department of Defense (DoD) develops requirements for telecommunications and automated information systems with functions that:

- Involve intelligence activities,
- Involve cryptologic activities related to national security,
- Involve the direct command and control of military forces,
- Involve equipment which is an integral part of a weapon or weapon systems, or
- Is critical to the direct fulfillment of a military or intelligence mission

Encryption commodities, software, and technology are subject to US Government Export restrictions. **The user is advised to check current government policies on the export of these commodities, software, and technology**.

Revision History

The following table shows the revision history for this document.

Date	Version	Revision
03/09/00	1.0	Initial Xilinx release.