SAND 99-1081 C

A DES ASIC Suitable for Network Encryption at 10 Gbps and Beyond

D. Craig Wilcox, Lyndon G. Pierson, Perry J. Robertson, Edward L. Witzke
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185
{dcwilco, lgpiers, pjrober, elwitzk}@sandia.gov

Karl Gass
Utah State University
Albuquerque, NM 87111
kgass@sandia.gov

Abstract

The Sandia National Laboratories (SNL) Data Encryption Standard (DES) Application Specific Integrated Circuit (ASIC) is the fastest known implementation of the DES algorithm as defined in the Federal Information Processing Standards (FIPS) Publication 46-2. DES is used for protecting data by cryptographic means. The SNL DES ASIC, over 10 times faster than other currently available DES chips, is a high-speed, fully pipelined implementation offering encryption, decryption, unique key input, or algorithm bypassing on each clock cycle. Operating beyond 105 MHz on 64 bit words, this device is capable of data throughputs greater than 6.7 Billion bits per second (tester limited). Simulations predict proper operation up to 9.28 Billion bits per second. In low frequency, low data rate applications, the ASIC consumes less that one milliwatt of power. The device has features for passing control signals synchronized to throughput data. Three SNL DES ASICs may be easily cascaded to provide the much greater security of triple-key, triple-DES.

Keywords: Data Encryption Standard, DES, Triple DES, Encryption hardware, Low power encryption, Pipelined architectures

[1] Corresponding author

I. Introduction

Since 1977, the United States has had a Data Encryption Standard (DES). DES is a block cipher that operates on 64 bit blocks of data and uses a 56 bit key [2]. It is a Feistel-type cipher. Feistel Ciphers [5][7] operate on left and right halves of a block of bits, in multiple rounds. The block halves are exchanged (left for right) from their usual order after the last round. An important property of Feistel Ciphers is that the function *f*, employed by a Feistel Cipher to operate on a left or right half-block of data, need not be invertible to allow inversion of the Feistel Cipher. In DES, the function *f* can itself be considered a product cipher (or substitution-permutation cipher), since that function performs both substitutions (to introduce confusion) and permutations (to introduce diffusion).

Another important property of Feistel Ciphers is that due to their structure, decryption is performed using the same multiple round process as encryption, but using the subkeys (one required per round) in reverse order. By eliminating the need for two different algorithms (one for encryption and one for decryption), hardware implementation is simplified and real estate on a chip is conserved.

A survey of the available integrated circuit implementations of the DES showed only devices with throughputs below 0.5 Gbps, far below the encryption rates required to scale Asynchronous Transfer Mode (ATM) encryption beyond 10 Gbps (SONET OC-192c). The existing implementations appeared to implement the sixteen rounds of the DES algorithm by iterating data through the hardware of a single round 16 times, resulting in low throughputs and the inability to change key variables quickly. To achieve the high throughput and key agility required for high speed ATM cell encryption, a fully pipelined implementation of all 16 rounds of DES with the key variables pipelined along with the data stages was designed and studied.

II. Proof of Principle

In order to study pipelined (and non-pipelined) implementations of the DES, an Excel spreadsheet implementation of the DES key schedule and algorithm was developed. This spreadsheet implementation of DES enabled the designers to familiarize themselves with the algorithm, and to examine multiple options for hardware implementation of the key schedule. After verification of the proper operation of the spreadsheet, the well-tested descriptions of the permutations and "S-boxes" were "cut and pasted" into the hardware description language, minimizing the opportunity for transcription errors.

First, the permutations and S-boxes of a single round were implemented in ALTERA's AHDL; compiled and simulated for ALTERA's 7000, 8000, and 10k families of devices. The simulations indicated that these operations could be computed more swiftly in the 7000 series devices, but only a small portion of the required functionality could be fit into the smaller gate count devices. We found that only four of the sixteen rounds of the DES algorithm would fit into an ALTERA 10K100 device, necessitating four large Programmable Logic Devices (PLDs) to fully pipeline all sixteen rounds. The key was pipelined through each stage along with the data in order to provide full key agility (the ability to change keys on each and every clocked word transfer, if desired). This pipelining of key as well as data also increased greatly the number of I/O pins required to transfer the data between the devices comprising the pipeline.

The simulations of the circuitry in ALTERA 10K100-3 speed grade devices showed that the time required to compute and latch a single round was 50 ns. Once the synchronous pipeline was filled, 64 bits of output every 50 ns would yield approximately 1.3 Gbps throughput with a latency of 800 ns.

For certain "feedback" modes of operation, such as Cipher Block Chaining (CBC) [3], the output of the pipeline must be combined with the next input. This requires the pipeline to "run dry", with only one 64-bit data word traversing all the pipeline stages before the next word can be input to the pipeline. Therefore, the CBC mode throughput for the synchronous pipeline is 64 bits each 800 Ns, or 0.08 Gbps (one sixteenth of the full pipeline throughput). For this reason, an "asynchronous" version of the pipeline (with no latches between stages) was analyzed, in order to maximize the CBC mode throughput by minimizing the pipeline latency. Analysis of this "asynchronous" pipeline showed that the total latency could be reduced to 650 Ns, improving the potential CBC mode throughput to 64 bits per 650 Ns, or 0.098 Gbps. Clearly, CBC and other similar feedback modes of operation are difficult to scale to high speed operation.

For non-feedback modes of operation such as Electronic Codebook (ECB) [3] or Counter Mode [1], the full pipeline can be utilized. In order to achieve 10 Gbps throughput (SONET OC-192c), however, eight such 1.3Gbps pipelines would have to be operated in parallel. ATM cell order must be maintained, and cells of different Virtual Circuits (requiring different key variables) may be interleaved in the cell stream. The processing of more than one ATM cell in parallel therefore introduces great complexity into an encryptor. Since an ATM cell payload is 384 bits, evenly divisible into six 64 bit words, six is the practical limit for parallel operation of 64-bit encryption pipelines for ATM cell encryption. In order to achieve 10 Gbps encryption, the throughput of each of the six pipelines must be at least 1.7 Gbps, which is greater than the 1.3 Gbps predicted by the ALTERA 10K100-3 simulations.

The pipelined DES design was then implemented as a CMOS Application Specific Integrated Circuit in order to achieve the increased throughput required to implement ATM cell encryption at rates greater than 10 Gbps

III. SNL DES ASIC

The Sandia National Laboratories (SNL) DES Application Specific Integrated Circuit (ASIC) is the fastest known implementation of the DES algorithm as defined in FIPS Pub 46-2 [2]. The SNL DES ASIC, over 10 times faster than other currently available DES chips, is a high-speed, fully pipelined implementation providing encryption, decryption, unique key input, or algorithm bypassing on each clock cycle. In other words, for each clock cycle, data presented to the ASIC may be encrypted or decrypted using the key data presented to the ASIC at that cycle or the data may pass through the ASIC with no modification. Operating beyond 105 MHz on 64 bit words, this device is capable of data throughputs greater than 6.7 Gbps, while simulations show the chip capable of operating at up to 9.28 Gbps. In low frequency applications the device consumes less that one milliwatt of power. The device also has features for passing control signals synchronized to the data.

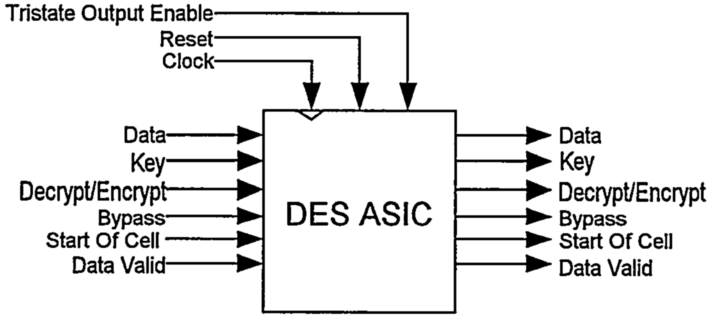

Figure 1. DES ASIC Block Diagram

The SNL DES ASIC was fabricated with static 0.6 micron CMOS technology. Its die size is 11.1 millimeters square, and contains 319 total pins (251 signals and 68 power/ground pins). All outputs are tristate CMOS drivers to facilitate common busses driven by several devices. This device accommodates the full input of plain text, 64 bits, and a complete DES key of 56 bits. Additionally, 120 synchronous output signals provide 64 bits of cipher text and the 56 bit key.

Three input only signals control electrical functions for logic clocking (CLK), logic reset (RST), and the tristate output enables (OE). The CLK signal provides synchronous operation and pipeline latching on the rising edge. Both RST and OE are asynchronous, active high signals.

Two synchronous signals, decrypt/encrypt (DEN) and bypass (BYP), determine the DES cryptographic functionality. On the rising edge of each CLK, the logic value presented to the DEN input selects whether input data will be decrypted (logic 1) or encrypted (logic 0). In a similar manner, BYP selects algorithm bypassing (logic 1) or not (logic 0) for each clock cycle. Both of these signals pipeline through the ASIC and exit the device synchronous with the key and data.

Two more signals, start-of-cell (SOC) and data valid (VAL) enter and exit the device synchronous with data and key information. These are merely data bits that may provide any user-defined information to travel with input text and key. These signals are typically used to indicate the start of an ATM cell and which words in the pipeline contain valid data.

ASICs from two wafer lots were shown to operate beyond the maximum frequency (105 MHz) of Sandia's IC Test systems. For 64-bit words, this equates to 6.7 Gb/s. This operational frequency was tested over a voltage range of 4.5 to 5.5 Volts and a temperature range of –55 to 125 degrees C.

Design

After implementing the DES algorithm in the set of four PLDs, the design was translated into VHDL and synthesized into the Compass library of standard cells. The device (figure 2) was fabricated in Sandia's MDL (Microelectronics Development Laboratory). Two wafer lots were successfully fabricated.

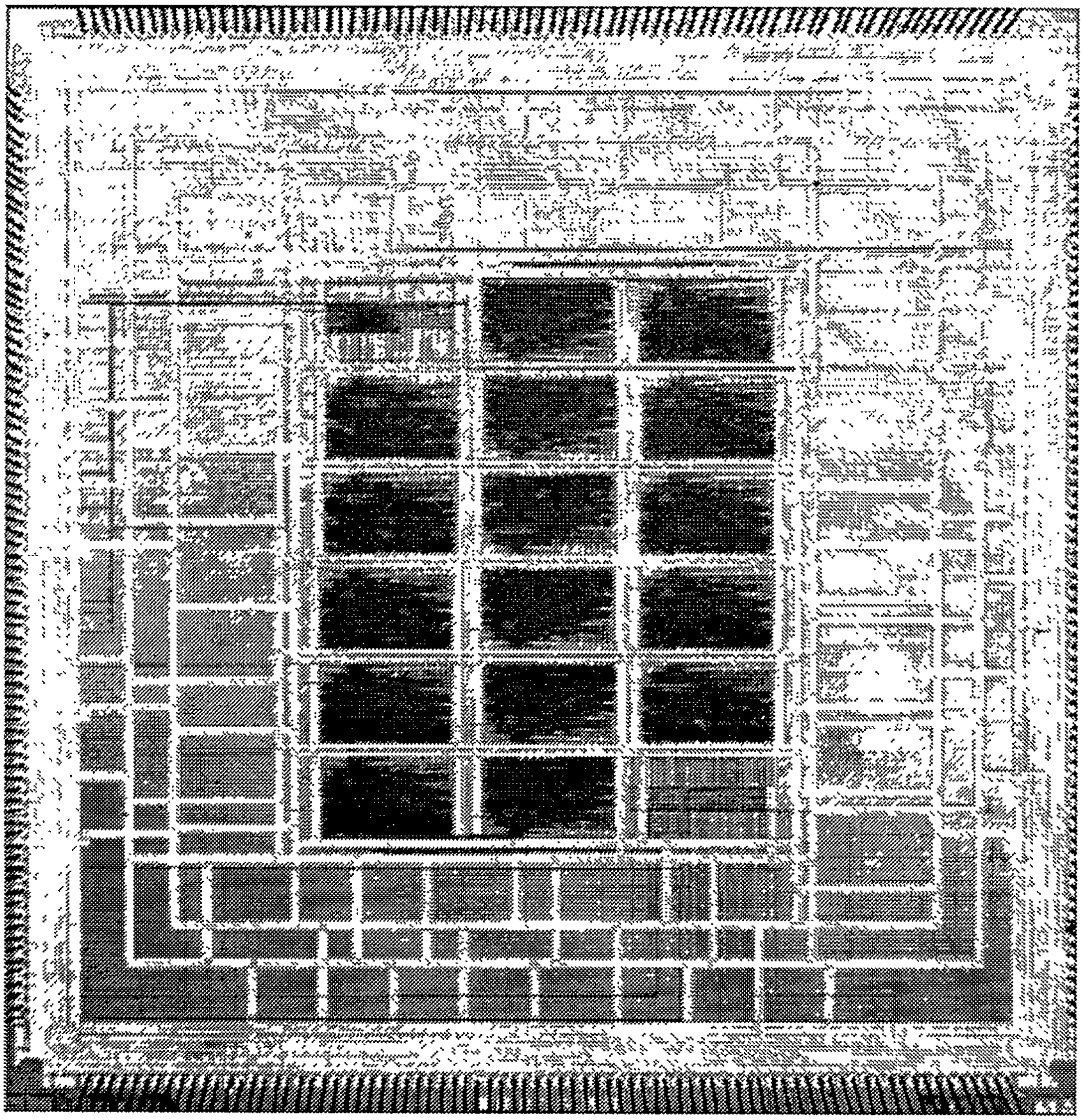

Figure 2. DES ASIC Die (11.1 x 11.1 mm).

This implementation is a fully design. It takes eighteen clock cycles to completely process data through the pipeline causing the appropriately decrypted, encrypted, or bypassed data to appear on the ASIC outputs. Additionally, all key and control input signals pass through the pipeline and exit the ASIC synchronized to the ciphertext outputs.

The SNL DES ASIC is the only known fully pipelined implementation of all 16 rounds of the DES algorithm. Pipelining increased the device throughput by dividing the algorithm into equally sized blocks and latching information at the block boundaries. This gives signals just enough time to process through each block between clock cycles, thereby maximizing the operational frequency.

Pipelining the algorithm allows a high degree of key and function agility for this device. Here, agility means that the SNL DES ASIC processes inputs differently on each clock cycle. As an example, the device may encrypt data with one key on one clock cycle, decrypt new input data with a different key on the very next clock cycle, bypass the algorithm (pass the data unencrypted) on the following clock, then encrypt data with yet another independent key on the fourth clock cycle. The control signals used to select these various modes of operation are presented at the output, passing through the device synchronized to the input data and the input key information. All inputs and outputs (control, key, and data) enter and exit the part synchronously. The authors know of no other single-chip implementation with all these features.

Features

This DES ASIC is unique in its ability to encrypt or decrypt with a new key, or pass information unprocessed, on each and every clock cycle. This enables the separate encryption of many virtual channels within a high speed communication system. In addition, it enables cryptosystems to be built with fewer components and lower cost. Also, as stated previously, no other encryption chip outputs the key corresponding to each data word in every clock cycle.

This per-cycle input and output of all variables facilitates cascading the devices for increased encryption strength, and paralleling the devices for even higher throughput. Another unique feature of this device is its ability to pass two user-defined control bits in synchronism with the data being encrypted, decrypted, or bypassed. This capability is indispensable for the design of ATM data encryptors, which must identify the Start of Cell boundaries and for systems that must flag data as “valid” or “not valid” in the encryption/decryption pipeline .

Design Enhancements

Since the initial ASICs were fabricated, several enhancements have been identified. These enhancements would increase throughput, aid in cascading devices, and ease the use at the board level. Projected enhancements include use of improved design tools, improved synthesis options, low-voltage high-speed I/O buffers, improved pin-outs, greater parallelism, and processing in higher-speed technologies.

Several design techniques could improve the design of the existing SNL DES ASIC. For example, recent synthesis developments would allow the DES ASIC to be redesigned with additional pipeline stages. A greater number of pipeline stages with improved timing, would increase the operational frequency and boost the throughput beyond 10 Gb/s.

To enhance the high-frequency operation at the circuit-board level, higher performance input-output buffers would reduce switching noise. The present design uses CMOS level (0 – 5 V) interfaces. Future designs would incorporate these low voltage, low power I/O buffers. Bringing out the clock phased with the output data, would facilitate higher speeds and greater performance by enabling source synchronous clocking. Also, optionally inverting the encrypt/decrypt output would better facilitate encrypt-decrypt-encrypt triple DES (described below).

A redesign into Gallium Arsenide (GaAs) technology should yield a factor of 3 to 4 improvement in speed of the ASIC. This would produce expected throughputs of 30-40 Gbps.

To achieve higher total throughput, multiple SNL DES ASICs can operate in parallel, with each ASIC processing a 64 bit block of the data stream. Figure 3 contains an example of multiple devices, performing DES operations on two blocks of data in parallel.

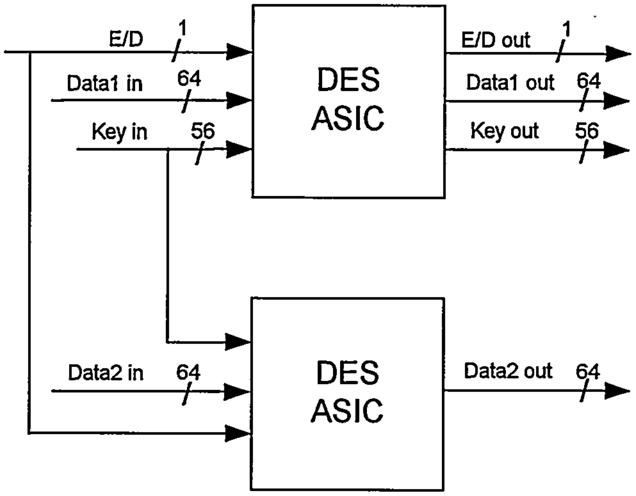

Figure 3. Parallel DES ASIC Implementation.

Because the data outputs of the SNL DES ASIC are tri-stated, there are several ways the ASICs can be used in parallel. The data outputs from both ASICs can be connected to a single output bus in a time-multiplexed fashion and the two DES ASICs can be operated using opposite clock phases to double the data throughput to greater than 13 Gbps. If both ASICs are driven off the same clock edge, the two 64 bit wide data outputs can also be combined into a single 128 bit wide output to achieve the 13 Gbps throughput..

For encryption of Asynchronous Transfer Mode (ATM) communication sessions where six SNL DES ASICs could operate in parallel on 64 bit blocks to encrypt a 384 bit payload, 40 Gbs (OC-768) rates could be achieved. The authors would expect six parallel DES ASICs made using a GaAs process to support encryption at 160 Gbps and beyond.

Power consumption

Being a fully static CMOS device, the power usage is proportional to operating frequency. At 105 MHz, the SNL DES ASIC consumes 6.5 Watts of power. While designed to dissipate the heat generated in high-bandwidth applications, the SNL DES ASIC can be operated at much lower data clock rates, consuming very little power, thus enabling many low speed, extremely low power applications

MHz Vdd	0.01	1	105
3.0	510 µW	54 mW	*
3.3	*	66 mW	*
5.0	*	165 mW	6.5 W

* untested

Table 1. Power Consumption of SNL DES ASIC.

In the 1200 to 640,000 bits per second range, the DES ASIC consumes only microwatts of power. The SNL DES ASIC operating at 10 KHz (640,000 bits per second, or ten 64 Kbps voice channels) only consumes 510 microwatts. Iterating around the ASIC to triple encrypt a single 64 Kbps voice channel, the SNL DES ASIC would need to operate at about 3 KHz, requiring well less than half of a milliwatt of power. Triple encrypting lower data rate channels (1200-28800 bps) requires even less power, enabling operation from a small battery or solar panel.

Package Development

The SNL DES ASIC has been packaged into three different packages including a 360 pin PGA, a 503-pin PGA and a 352 pin BGA. The original 360-pin package was used in initial testing of the DES ASIC performance. It was in this package that the DES chip was shown to operate at over 105 MHz. Sandia had earlier developed a 1.1 million gate PLD board that used 11 Altera 10K100 devices. This board was used in the development of the DES ASIC pipeline design, housing the four 10K100 devices. It was determined that the SNL DES ASIC could be used with the original PLD11 board, being substituted for a single 10K100 device, if a 503-pin equivalent package were available. Sandia designed an FR4 board onto which the DES ASIC was wire bonded and 503 pins could be inserted. The chip-on-board package had to be designed to dissipate up to 5 watts produced by the DES ASIC. This is accomplished by attaching the DES die directly onto a gold plated copper insert that is attached to the FR4 board using a tin-lead solder preform. Pictures of a representative cross section and this package are shown in figures 4 and 5.

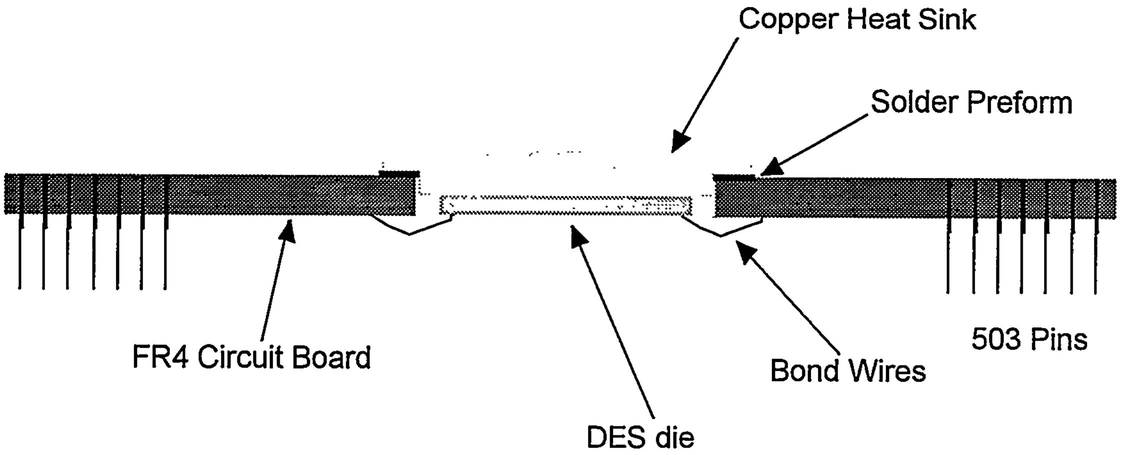

Figure 4. Cross Section of the 503-Pin Package.

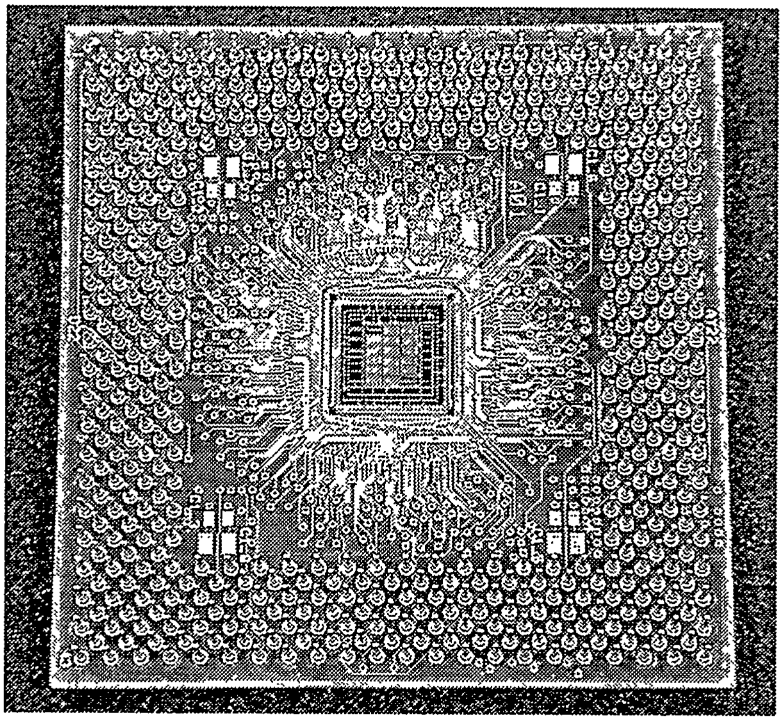

Figure 5. Picture of the 503-Pin FR4 Board Package.

The design of this package enables a heat sink and integrated fan to be attached to the back of the copper insert to enable the package to dissipate over 6 watts. The FR4 printed wiring board uses 3 mil copper traces and spaces with 5 mil vias. This design also allowed the board to be used to connect the existing bus signal assignments from the PLD11 board to the appropriate key and text signals on the SNL DES ASIC. Two versions of the package were designed and fabricated. Each has a different wiring schematic designed to fit into a different socket on the PLD11 board. SNL DES ASICs in the 503 pin package were demonstrated at the Super Computing 98 Conference in Orlando, November 1998.

The SNL DES ASIC has also been packaged in a 35 x 35 mm, 352-pin ball grid array (BGA) package. This is an open tool commercial package available from Abpac Inc. (of Phoenix , Arizona, U.S.A.). The package was chosen not only for its capability to dissipate over 5 watts and smaller size, but also its low cost. Abpac's automated manufacturing capability enabled a reduction of over 20 times in packaging costs. This package is being used in the design of a triple key, triple DES encryption module.

Applications

Although mainly used as an encryption engine for single DES or triple DES cryptosystems, the SNL DES ASIC has other uses such as a data randomizer. Some encryption algorithms need to hide or obscure relationships between bits or bytes of data prior to encryption. Using the SNL DES ASIC on the front end as a randomizer introduces no significant delay to the host cryptosystem. In a similar vein, this device can be used as a pseudo random number generator as part of a larger cryptosystem.

In a counter mode or filter generator cryptosystem (shown in figure 6), a linear recurring sequence (LRS) generator produces a sequence, which is fed to a non-linear function. The purpose of the non-linear function (in this case, an SNL DES ASIC) is to mask the linearity properties of the LRS. The output of the DES ASIC is then combined with the data, through an Exclusive-OR operation.

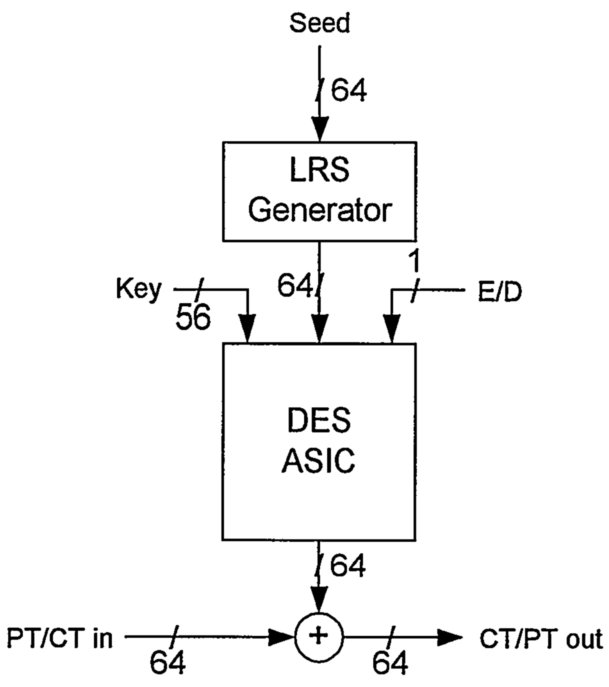

Figure 6. Encryption/Decryption for Counter Mode.

This device can be used to keep encryption/decryption keys synchronized with the data in cascaded triple DES implementations (described below). At the highest data rates, programmable logic devices (PLDs) may not be able to keep pace with the SNL DES ASIC for passing keys with the data. Consequently, SNL DES ASICs operating in bypass mode may be used to pass keys to subsequent encryption chips in step with the data.

Triple DES

Triple DES employs the Data Encryption Standard algorithm in a way sometimes referred to as encrypt-decrypt-encrypt (E-D-E) mode. E-D-E mode using two keys, was proposed by W. Tuchman and summarized by Schneier in [7]. The incoming plaintext is encrypted with the first key, decrypted with the second key, and then encrypted again with the first key. On the other end, the received ciphertext is decrypted with the first key, encrypted with the second key, and again decrypted with the first key to produce plaintext. If the two keys are set alike, it has the effect of single encryption with one key, thereby preserving backward compatibility. While advances have been made in cracking single DES cryptosystems [4], data protected by the SNL DES ASICs using two key, triple DES have a good degree of cryptographic robustness.

Two key, triple DES schemes (with 56 bit keys) can be cryptanalyzed using a *chosen plaintext* attack with about 2^{56} operations and 2^{56} words of memory [6]. (In terms of work, this is on par with two key, double DES, which is susceptible to a *known plaintext* attack with 2^{56} operations and 2^{56} words of memory [6].) Although in theory this is a weakness, Merkle and Hellman [6] state that in practice it is very difficult to mount a chosen plaintext attack against a DES cryptosystem. This makes two key, triple DES significantly stronger than two key, double DES, because an attack would now require 2^{112} operations (and no memory).

Triple DES can also be performed with three independent keys, using a separate key for each of the encryption and decryption operations. Triple DES with three independent keys gives a slightly higher level of protection, but is susceptible to a meet-in-the-middle attack requiring about 2^{112} operations and 2^{56} words of memory [7]. Again, with regards to compatibility, keys one and three could be set to the same value, to interoperate with Tuchman's two key, triple DES, or all three keys could be set alike to interoperate with single DES.

The SNL DES ASIC supports triple DES in several unique ways. For highest throughput speeds, multiple SNL DES ASICS can be cascaded to implement the encrypt-decrypt-encrypt mode. In situations where top performance is not needed, but board real estate, cost, or power consumption are constrained, a single SNL DES ASIC may perform triple DES in an iterative manner.

Because keys and control information march in lock step with the data, a string of three SNL DES ASICs can be cascaded. This would be accomplished by connecting the output data, key out, and control information output pins of one ASIC to the input data, key in, and control information input pins on the next ASIC. To perform E-D-E triple DES, an inverter must be placed on the path of the encrypt/decrypt signal between ASICs. This way, the middle ASIC will always perform the opposite operation (encrypt or decrypt) from the first and last ASICs in the string. PLDs, or SNL DES ASICs set to bypass mode, can be used to provide the proper (18 clock tick) delay, so that the keys for the second and third encryption/decryption operations will arrive in synchronization with the appropriate data. An example of this, using two keys is shown in figure 7.

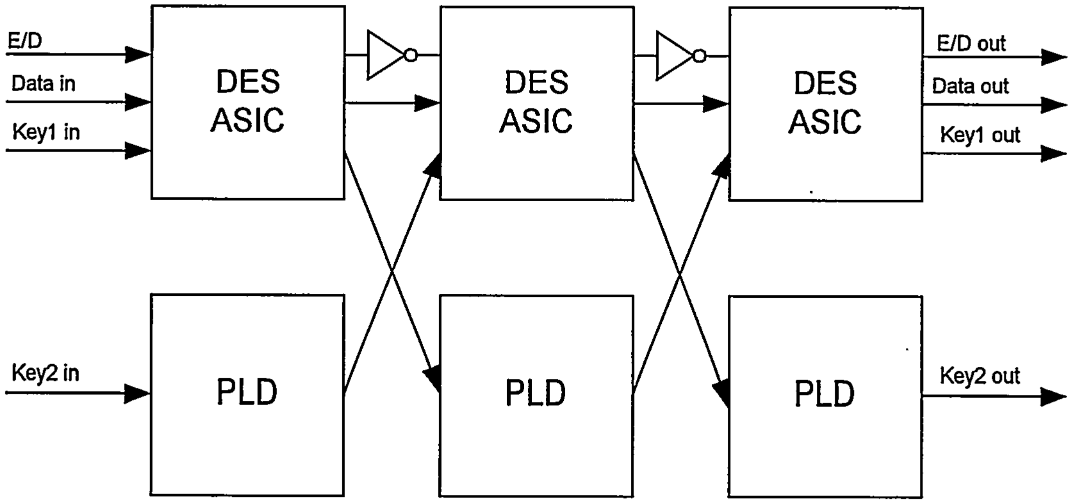

Figure 7. Cascaded, Multiple ASIC, Two Key, Triple DES Implementation.

By applying appropriate glue logic, the SNL DES ASIC can be used to perform E-D-E triple DES in an iterative manner by looping the data, key, and control information around the ASIC, processing the data three times. The glue logic will need to contain a two bit wide, 18 stage delay to count (in synchronization with the data, key, and control information) the number of times a given block of data has been processed. Logic will also be needed to invert the encrypt/decrypt bit between passes through the SNL DES ASIC. An example of this is shown in figure 8.

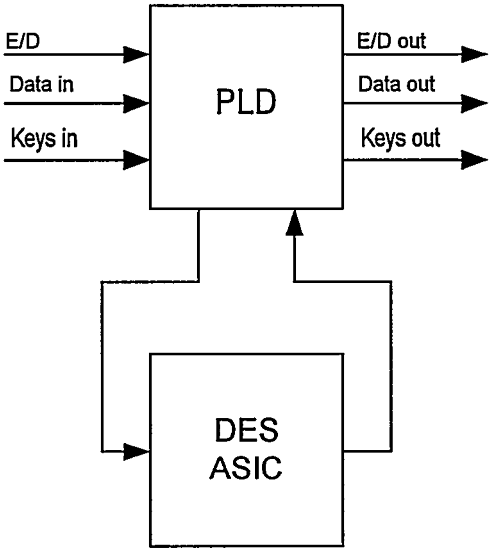

Figure 8. Iterative, Single ASIC, Triple DES Implementation.

IV. Summary

For this project, the authors explored how a representative "heavyweight," unclassified encryption algorithm could be optimized and pipelined. This project has yielded a device that could be used in building encryption research prototypes. The project was successful, producing not only a research vehicle, but the fastest known ASIC implementation of DES.

The SNL DES ASIC can support two- or three-key triple DES using a multiple cascaded ASIC configuration at rates of 6.7 Gbps and beyond. It can also support very low power triple DES, iteratively, in a single ASIC configuration.

Acknowledgements

The work described in this paper was performed by Sandia National Laboratories (a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company) under contract number DE-AC04-94AL85000 to the United States Department of Energy. The authors would like to Hans Rodriques de Miranda, formerly of RE/SPEC, for his contribution to this work.

Bibliography

1. The ATM Forum Technical Committee, ATM Security Specification Version 1.0, Straw Ballot, STR-SECURITY-01.00, The ATM Forum, Mountain View, CA, December 1997.
2. Data Encryption Standard (FIPS PUB 46-2), Federal Information Processing Standards Publication 46-2, National Bureau of Standards, Washington, D.C., December 30, 1993.
3. DES Modes of Operation (FIPS PUB 81), Federal Information Processing Standards Publication 81, National Bureau of Standards, Washington, D.C., December 2, 1980.
4. http://www.eff.org/descracker, January 1999.
5. Menezes, Alfred J., et al., Handbook of Applied Cryptography, CRC Press, Boca Raton, FL, 1997.
6. Merkle, Ralph C., and Martin E. Hellman, "On the Security of Multiple Encryption," Communications of the ACM, Vol. 24, No. 7, p. 465-467, July 1981.
7. Schneier, Bruce, Applied Cryptography, 2nd edition, John Wiley & Sons, New York, 1996.