ASIC Cryptographical Processor based on DES.

Ingrid Verbauwhede[1] Frank Hoornaert[3] Joos Vandewalle[2] Hugo De Man[1,2]

IMEC v.z.w.[1] & ESAT, KULeuven[2] & Cryptech NV/SA[3]
Kapeldreef 75, B-3001 Heverlee, BELGIUM

Abstract

To date, many commercial applications in telecommunications, data transmission and data storage require a high level of cryptographical protection. The ASIC processor, presented here, can be programmed to execute a large set of cryptographical functions, not found in other cryptographical devices. Novel architectures for both data path and controller have been designed to realize this high degree of programmability, while still reaching a high throughput. The compact processor counts 18K transistors on 25 mm^2 in a 2.4 μm CMOS process and yet it reaches a throughput of 30 Mbit/s for every single-encryption mode. It is the fastest DES processor currently available.

1 Introduction.

Many cryptographical applications for commercial use, such as Electronic Funds Transfer, home banking, protection of medical data, etc. make use of the Data Encryption Standard (DES) algorithm, [1]. For high security, DES is used as a basic function based upon which cryptographical applications are built, [2]. Therefore, the cryptographical processor presented here incorporates a large set of cryptographical functions built around the DES algorithm. For instance, two Message Authentication Code (MAC) generating functions are shown on Fig. 1. One is based on single encryption, i.e. one DES computation is performed in the feedback loop, the other is based on triple encryption, i.e. a DES computation with a first key is followed by a DES-1 computation with a second key, followed by a DES computation, again with the first key.

The design of the cryptographical processor requires first a thorough investigation of the cryptographical requirements which are demanded from this type of processor. Secondly, to provide a processor which can be used as an application-specific co-processor, a high degree of programmability and a set of high level commands have to be incorporated. Thirdly, for an easy communication in several types of environments, a general, flexible IO interface has to be provided.

In section 2, the main features on all three levels, the cryptographical functions, the incorporation of the programmability, and the IO functions are summarized. This diversity imposes high requirements on both the data path and the controller architecture, which are presented in section 3. Next, in section 4 the implementation and test results are given. In section 5 some conclusions are made.

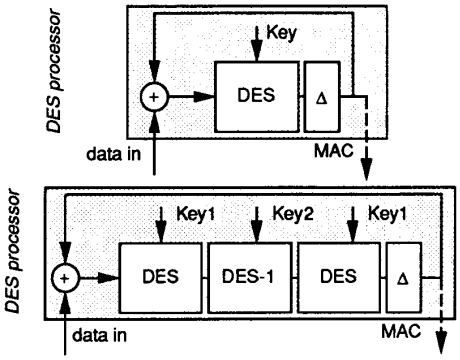

Figure 1: MAC generation combined with single or triple encryption.

2 Features.

The main features of the novel DES co-processor are summarized in Table 1. The NBS Data Encryption Standard (DES) is the basic kernel, [1]. However, to increase security, all *DES Modes of operation*, as specified in [3], have been implemented. For authentication purposes several MAC (Message Authentication Code) generating functions are provided, [4]. Also a Random Generation function (RGF) based on the OFB mode is provided. To enlarge the effective key length, the defacto standard for *triple* encryption with two different keys, as shown on Fig. 1 in combination with the MAC function, can be combined with each of the modes of operation and cryptographical functions. *Four* safe write-only key registers are provided to store up to four different keys. Next to the Input-Output registers in the IO interface, *four* internal data & initial vector registers allow the realization of all feedback modes. In general, the controllers and the logic are built with a cryptographical safe attitude in mind such that upon misuse of the device, by accident or on purpose, no sensitive data or keys are released.

To program these cryptographical functions, in to-

TH0367-3/91/0000/0292$01.00 © 1991 IEEE

tal *74* different *single* and *continuous* commands are defined. The single commands are basic instructions to perform single actions, for instance :

```
Load key in Key Register 3.
Execute DES on Data Register 1.
```

They allow the user to compose his own commands, e.g. to decrypt session keys, to compose keys by exoring several key parts or to define another type of multiple encryption. To avoid control and communication overhead during encryption sessions, 36 *continuous commands* are provided. These perform a continuous pipelined execution of a predefined sequence of basic instructions, for instance :

```
Do triple encryption in CBC mode.
```

This set of continuous commands consists mainly of all defined standards for modes of operation and MAC generation, each in combination with single or triple encryption. Because the amount of data that will be processed is unknown in advance, a continuous command remains active, once it is loaded. Only when a new command is asserted e.g. a NOP, the processor will stop.

To allow this processor being used in a large number of environments and applications, a flexible I/O interface has been incorporated, of which the main features are : an asynchronous interface, a micro processor bus, with a programmable width of 8, 16 or 32 bits, a DMA interface and programmable interrupt lines.

3 Architecture Design.

Key to the small silicon area and high performance, is a chip architecture carefully optimized by use of an optimized design strategy.

The DES processor consists of an internal synchronous processor with around it an I/O shell, as shown on Fig. 2. To cope with the complexity resulting from the large set of cryptographical demands, a high degree of modularity had to be applied during the design of the data path and the controller of the internal processor. This has resulted in four data path modules, shown on Fig. 2, each with a specific function. The first module is the DES module, which implements the actual DES algorithm. The second module contains four key registers and key logic. The third module consists of logic to configure all defined modes of operation and the fourth module contains the registers for data and initial vectors and the I/O logic to communicate with the I/O shell. To optimize the modularity and the pipelined operation of the modules, cryptographical algorithmic equivalences are applied, discussed in [5, 6], which do not change the behaviour of the algorithm but which still allow a compact realization.

To combine both, a high throughput of 30 Mbits/s and the high degree of programmability, a second main challenge was the design of the controller, which at the same time reaches this throughput and realizes the large set of high level commands. Therefore, a *hierarchically pipelined controller* has been designed, as

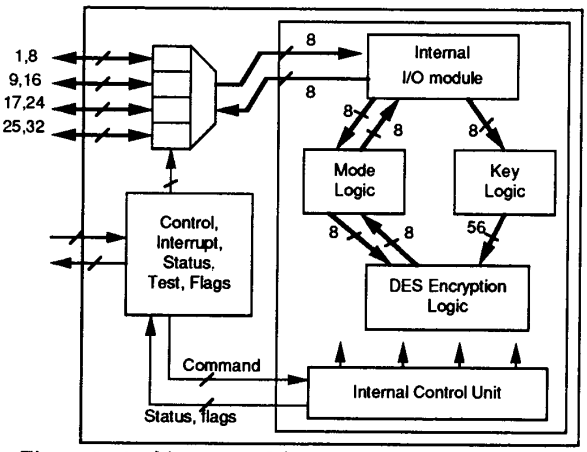

Figure 2: Architecture of the cryptographical DES processor.

shown on Fig. 3. Each of the data path modules has its local Finite State Machine (FSM) which contains from 2 up to 20 different sequences specific for the module. For instance, the local DES controller can execute the basic DES or DES-1 algorithm.

The global operation and *the pipelining of the modules* is organized by the master controller which starts and monitors the local controllers. It decodes the incoming commands and starts a high level program, which consists of instructions for the local controllers of the parallel operating modules. Based on the start pulse, the instruction from the master controller and the command bits, the local controllers decides on the local sequence to execute on its module. The length of the sequences of the local controllers is however not known to the master. For the local I/O controller it can even vary, depending on the data rate of the external data exchange. Therefore, a *handshake* communication between the controllers is implemented.

Important for a cryptographically safe operation is the correct filling and emptying of the pipeline, when starting and stopping a continuous pipelined command. Special attention has been paid to this, which adds extra constraints on the code for the FSM's.

This controller technique allows the pipelined and parallel operation of the data path and I/O modules. A global *pipelined* operation exists at the data level : the I/O input operation of the next data is performed in parallel with the encryption operation on the actual data and with the I/O output operation of the previous data. A smaller scale pipeline, e.g. by duplicating encryption hardware, has no sense because of the feedback loops defined by the modes of operation, as illustrated on Fig. 1 : the output of the previous encryption is needed to compute the input for the next.

Next, low level fine tuning has been applied during the design of each data path module and each local controller. A pipelined single-encryption takes only *26*

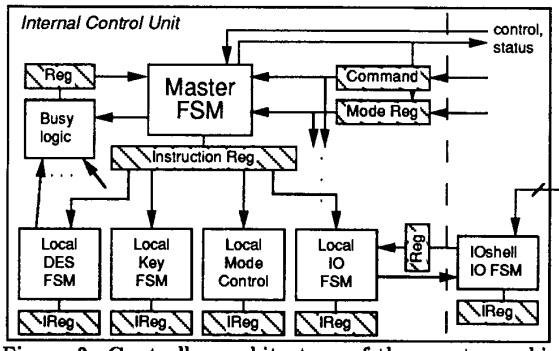

Figure 3: Controller architecture of the cryptographical DES processor.

clock cycles for each 8 bytes mode, providing the external I/O data rate, which depends on the speed of the busses and external circuitry to which the DES processor is communicating, is adequately fast. A pipelined triple encryption of every 8 bytes mode takes 66 clock cycles. Unique is also, that the throughput is independent of the mode of operation and does not decrease for the feedback modes, as a result of the carefully chosen level of pipelining.

4 Evaluation.

The processor data path consists of full custom bit sliced modules while the controller and the I/O shell are realized by means of PLA's and standard cells, as shown on Fig. 4. This has reduced the layout effort, while the area cost was kept small. The processor counts 18K transistors and measures 25 mm^2 in a 2.4 μm two level metal NWELL CMOS process. The area occupied by the DES kernel module itself takes about 20 % of the total area. The area occupied by the complete data path, i.e. the four basic data path modules is less than 50 %. It indicates the important contribution of control and I/O logic, which is often neglected when area estimations of ASIC's are made. Tests on the processed devices have indicated full functionality at a clock frequency of 12 MHz (crystal of 24 MHz), which corresponds to a throughput of *30 Mbits/s for every 8 bytes single-encryption mode* and a throughput of *12 Mbit/s for every 8 bytes triple-encryption mode.*

Aimed at the same application domain and widely used in practice are the Data Ciphering Processors Am9518, Am9568 and AmZ8068 from Advanced Micro Devices, [7]. Three single encryption modes of operation are provided : ECB, CBC and 1 byte CFB. The fastest version, the AmZ8068, reaches a maximal throughput of 14.2 Mbit/s. This maximal throughput is only reached in dual port mode, and requires a synchronous communication protocol, which imposes high constraints on the surrounding circuitry. The DEP (Digital Encryption Processor) of AT&T, [8], can be software programmed by the user to execute the four DES modes of operation, the speed for an 8 bytes mode is however only 4.7 Mbit/s.

5 Conclusions.

An ASIC cryptographical co-processor based on the DES algorithm has been designed and implemented. It combines a large set of cryptographical functions, not found in other cryptographical devices, with a high programmability and a flexible I/O interface. The main optimizations have been performed on the architectural level and a novel, modular and pipelined architecture for both data path and controller has been designed. Although implemented in a 2.4 μm CMOS process, the processor is very compact, 25 mm^2, and reaches a throughput of 30 Mbit/s for every single-encryption mode, as a result of the dedicated architectural optimizations. This is the fastest, programmable DES processor currently available.

Acknowledgements.

The authors wish to thank the members of the IMEC/VSDM division for the CAD support, the IMEC/INVOMEC division and MIETEC silicon foundry, and the Belgian national government for financial support.

References

[1] "Data Encryption Standard," FIPS, Federal Information Processing Standard, Pub no.46, National Bureau of Standards, January 1977.

[2] M.E. Smid, D.K. Branstad, "The Data Encryption Standard : Past and Future," *Proceedings of the IEEE, Special Section on Cryptology*, Vol. 76, No. 5, pp. 550-559, May 1988.

[3] "DES modes of operation," FIPS, Federal Information Processing Standard, Pub no.81, National Bureau of Standards, December 1980.

[4] "American National Standard for Financial Institution Message Authentication," ANSI X9.9 - 1982.

[5] M. Davio, Y. Desmedt, J. Goubert, F. Hoornaert, and J.-J. Quisquater, "Efficient hardware and software implementations of the DES," *Advances in Cryptology, Proceedings CRYPTO-84*, August 84.

[6] I. Verbauwhede, F. Hoornaert, J. Vandewalle, H. De Man, "Security and Performance Optimization of a new DES Data Encryption Chip," *IEEE Journal of Solid-State Circuits*, Vol. 23, No. 3, pp. 647-656, June 1988.

[7] "Data Ciphering Processors Am9518, Am9568, AmZ8068," System Timing Controller Technical Manual, Advanced Micro Devices, Inc., 1985.

[8] R.C. Fairfield, A. Matusevich, J. Plany, "An LSI Digital Encryption Processor (DEP)," *IEEE Communications Magazine*, Vol. 23, No. 7, pp. 30-41, July 1985.

Functions	DES algorithm, DES & DES-1, [1], single or triple encryption & decryption
Modes of operation	ECB, CBC, CFB (1 or 8 byte), OFB (1 or 8 byte), [3] Message Authentication Code, [4], Random Generation Function
Registers	4 write-only key registers of 56 bits 4 internal data & initial vector registers of 64 bits
IO interface	2 data input, 1 data output register of 32 bits programmable bus width : 8, 16 or 32 bits DMA and micro-processor interface
Technology	2.4 μm double level metal N-well CMOS
size	5.2 mm $\times$ 4.8 mm (centre scribe to centre scribe)
# transistors	$\approx$ 18000
max. crystal freq.	24 MHz* (from -50 °C to +125 °C at 4.5 V) (equals 12 MHz internal clock freq.)
max. operation speed	30 Mbit/s (all Modes, 8 bytes, single enc., 12 MHz clock) 12 Mbit/s (all Modes, 8 bytes, triple enc., 12 MHz clock) 3.6 Mbit/s (all Modes, 1 byte, single enc., 12 MHz clock) 1.5 Mbit/s (all Modes, 1 byte, triple enc., 12 MHz clock)
Power supply	5 V (4.5V, 5.5V)
Power consumption	125 mW stand-by, 250 mW operation, typical at 25 °C , 5V
Package type	48 pins DIP, 68 pins PLCC

* Measured Characteristics, but functional correctness is guaranteed to 16 MHz crystal frequency by Cryptech NV/SA.

Table 1: Characteristics of the ASIC DES co-processor.

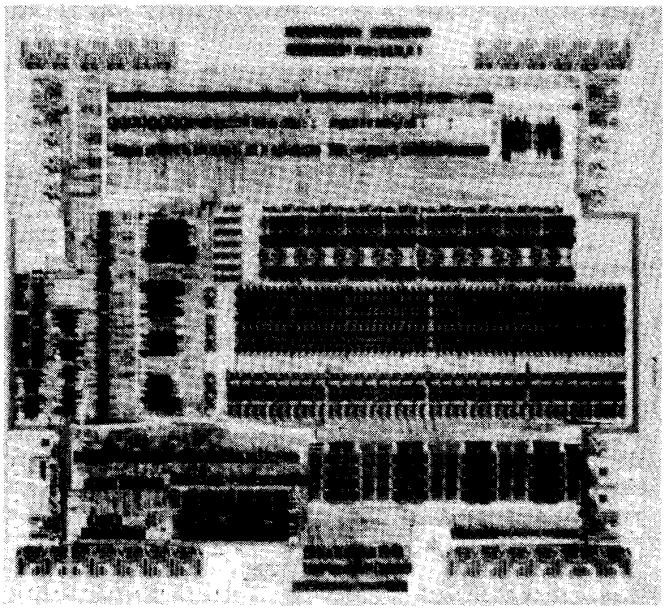

Figure 4: Chip photograph of the DES device.