Subterranean: A 600 Mbit/sec Cryptographic VLSI chip

L. Claesen[⋆‡], J. Daemen[‡], M. Genoe[⋆], G. Peeters[⋆]

[⋆]IMEC, Kapeldreef 75, B-3001 Leuven, Belgium
[‡]Kath. Univ. Leuven, ESAT Laboratory, Kardinaal Mercierlaan 94, B-3001 Leuven, Belgium

Abstract

In this paper the design of a high-speed cryptographic coprocessor is presented. This coprocessor is named Subterranean and can be used for both cryptographic pseudorandom sequence generation (Substream) and cryptographic hashing (Subhash). In Substream mode the chip can be used for stream encryption/decryption under control of a 256-bit key. A cryptographic resynchronization mechanism is provided for fast accessibility of encrypted data by legitimate parties.

Application fields include the real-time encryption of digital HDTV signals as well as high speed telecommunication and networking such as ATM. The chip has been fabricated within the INVOMEC / EUROCHIP educational VLSI Design Facilities in MIETEC 2.4μ CMOS technology. Measured samples are operating at encryption / decryption rates of 286 Mbits/sec and hashing rates of 572 Mbits/sec. The operation of the chip is demonstrated by a setup showing the real-time encryption and decryption of digitized PAL color composite video signals. The designed cryptographic module can be used as a stand-alone device or embedded as a mega-block in a larger chip.

Keywords: *Hardware Cryptography, Cryptographic Hash Functions, Pseudorandom Sequence Generators, Stream Ciphers.*

1 Introduction

Due to the increased possibilities for all kinds of communications among people by means of telephony, computers, broadcasting etc., the needs towards the protection and security of the information being stored or transmitted have also increased in demand. This is required to avoid unauthorized access to all kinds of information (data-bases, television programs, telecommunication etc...). This has led to several methods and algorithms that allow to protect such information. An overview of the field of cryptology is being presented in [1]

The Subterranean coprocessor chip has been designed according to the algorithms developed by Daemen e.a. [3]. The chip can be used as a cryptographic pseudorandom sequence generator (CPRG) *and* a cryptographic hash function (CHF), respectively called Substream and Subhash. Substream and Subhash are powerful primitives in the realization of computer security. A CPRG can be used for confidentiality of stored or transmitted data by stream encryption [1]. A CHF is an indispensable component of practical data integrity, authentication and digital signature schemes [1]. Moreover, the security of many cryptographic protocols depends on a CHF and unpredictable random bits that can be produced by a CPRG [1]. In the providing of security services, all bulk operations on large variable-length files, namely encryption and hashing, can be performed by the coprocessor.

Many of the cryptographic algorithms that have been developed are being used in software implementations on computers (e.g. to have protection of encoded passwords for users). For low complexity type of applications, such as the protection of information in files and databases this is probably the most economic solution. A number of applications however require such high throughputs for the encryption/decryption process that they cannot be executed on a normal general purpose microprocessor. These applications require dedicated ASIC implementations. A number of hardware implementations for cryptographic algorithms have been realized [6, 7, 8, 9, 10, 11]. These implementations allow for higher throughputs than if the algorithms would be executed in software on a general purpose processor. E.g. [6]: 14.2 Mbit/sec, [7]: 4.7 Mbit/sec, [8]: 20 Mbit/sec (1.5μm-CMOS), [9]: 30 Mbit/sec (2.4μm-CMOS at 24 MHz), [11]: 44.1 Mbit/sec (1.5μm-CMOS at 25 MHz). Some of these processors implement the DES [5] algorithm [9, 10]. All of these ASIC implementations are limited to medium throughput applications. High speed applications such as digital real-time video (e.g. pay television etc.) and telecommunication such as ATM require throughputs in excess of 155 Mbit/sec.

Appeared in *12th International Conference on Computer Design (ICCD 1993), VLSI in Computers and Processors*, R. Camposano, and A. Domic (eds.), IEEE Computer Society Press, pp. 610–613, 1993.

In this paper, a chip implementation of a cryptographic algorithm that is specifically dedicated towards high speed applications is presented. This chip called *Subterranean* has been implemented in a conservative technology of 2.4μm-CMOS technology and already demonstrates a throughput of 286 Mbit/sec at a clock rate of 18 MHz. Smaller technology and higher clock speeds will allow for even higher throughputs.

In this paper, first the algorithmic background of the subterranean algorithm will be explained in section 2, and afterwards in section 3 the implementation in a chip will be discussed as well as a demonstrator environment.

2 Functional Specification

Subterranean consists basically of a finite state machine with a state register, a key register, an updating function and some control logic.

The operation of the Coprocessor is given by the calculation of the next internal state A^{t+1}, key K^{t+1} and output Z^t from A^t, K^t and the input B^t. For both registers there are options, indicated by means of the control logic. For the internal state there are 3 options : *reset* (to the all-0 state), *hold* and *update*. For the key there are 2 options : *hold* and *load*. Every iteration a 16-bit value Z is presented at the output. We will now specify the updating, loading and output functions in detail.

The updating function $A^{t+1} = \mathrm{F_s}(A^t, K^t)$ can be considered as a 5-step transformation of the internal state A. In the following, all indices should be taken modulo 257, $\vee$ means OR and $\oplus$ means XOR.

Step 1 :	$a_i = a_i \oplus (a_{i+1} \vee \bar{a}_{i+2})$,	$0 \le i < 257$
Step 2 :	$a_0 = \bar{a}_0$	
Step 3 :	$a_i = a_i \oplus a_{i+3} \oplus a_{i+8}$,	$0 \le i < 257$
Step 4 :	$a_i = a_i \oplus k_{i-1}$,	$1 \le i < 257$
Step 5 :	$a_i = a_{12*i}$,	$0 \le i < 257$

Figure 1 clarifies how the five steps of $\mathrm{F_s}$ contribute to the calculation of one statebit. Step 1 is a nonlinear cellular automaton (CA) operation where each bitvalue a_i is updated according to the bitvalues in its neighborhood (in this step and step 3 periodic boundary conditions apply). Step 2 consists merely of complementing 1 bit to eliminate circular symmetry in case all statebits are 0. Step 3 is a linear CA operation. In step 4 the actual keybits are injected in A. Step 5 is a dispersing bit permutation. The length of A is 257 (a prime) to make step 1 and 3 invertible and to avoid circular symmetric patterns in A. The updating function is invertible with respect to the state. For a fixed key, every state has exactly one predecessor.

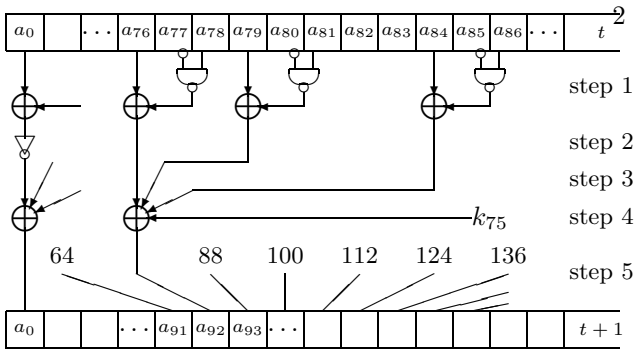

Figure 1: schematic overview of the calculation of one output bit using the $\mathrm{F_s}$ function.

In the key load option 32 bits are loaded into the keyregister in parallel. If a 32-bit word $B = b_0 b_1 \dots b_{31}$ is loaded at time t we have

$$k_i^{t+1} = b_i \quad \text{for } 0 \le i < 32 \qquad \text{and}$$
$$k_i^{t+1} = k_{i-32}^t \quad \text{for } 32 \le i < 256 \quad .$$

The 16 output bits $z_0 z_1 \dots z_{15}$ at time t are taken from the internal state A^t. The indices of the used statebits are given by

$$(11, 24, 37, 48, 60, 73, 84, 98, 117, 130, 143, 154, 168, 200, 235, 249) \ .$$

Every updating operation results in information *diffusion*: every bit of A^t depends on 9 bits of its predecessor state A^{t-1} and on 81 bits of A^{t-2}. After three iterations the dependence is complete, i.e. a statebit at time t depends on all bits of A^{t-3}. Alternatively a bit of A^t affects 9 bits of A^{t+1}, 81 bits of A^{t+2} and all bits of A^{t+3}.

The cryptographic strength of all cryptographic algorithms is ultimately based on the presence of strong *confusion*. This term was introduced by C. Shannon [2] to denote a qualitative aspect of information propagation. Strong confusion corresponds to involved and complicated dependencies, weak confusion to simple dependencies. A detailed treatment of the confusion of Subterranean with respect to known cryptanalytic methods can be found in [3].

We would like to stress that no absolute proof of security can be given for any practical cryptographic algorithm. The only way for a cryptographic algorithm to gain credibility is aging in the absense of cryptanalytic attacks that refute the cryptographic claims made, despite serious effort of the cryptologic community. The formal cryptographic claims made for the Subterranean functions can be found in [3] .

Appeared in *12th International Conference on Computer Design (ICCD 1993), VLSI in Computers and Processors*, R. Camposano, and A. Domic (eds.), IEEE Computer Society Press, pp. 610–613, 1993.

2.1 Substream

In Substream mode the Cryptographic Coprocessor is initialized by fixing the *Initial State* and the *Key*. This takes 16 input words (of 32 bits) and 16 clockcycles. This can be expressed in a *sequence diagram*:

Clockcycle	State	Key Load	Output
t = 0	0*(reset)*	I_t*(load)*	
t = 1...,7	–*(hold)*	I_t	
t = 8	F_s	K_{t-8}	
t = 9...,15	–	K_{t-8}	

Here K is the secret key and I the Initialization constant that can be used for resynchronization. After initialization 16 random bits $r_0 r_1 \dots r_{15}$ are presented at the output per iteration and the key is not changed:

Clockcycle	State	Key Load	Output
t ≥ 16	F_s	–*(hold)*	$R^t = Z^t$

Informally, the cryptographic claim can be formulated as follows: Substream cannot be distinguished from a binary symmetric source by an adversary not in possession of the key.

2.2 Subhash

The system is initialized by resetting the internal state and making sure that the keyregister contains only 0-bits. The (padded) message is loaded into the keyregister 32 bits at a time while the finite state machine is iterated. After loading all message words 24 more iterations are performed. During these iterations all-0 words are loaded into the keyregister. The Hash Result is given by the words Z output during the last 16 iterations.

Suppose we want to calculate the hash result H_S of a b-bit message using Subhash. Here b may be any integer. Before hashing, the message has to be padded so that its length is a multiple of 32.

Padding of the message
The message is extended with a number p of 0-bits so that its length in bits is a multiple of 32 and $0 \leq p < 32$. Subsequently the message is extended with a 32-bit word representing the value $2^{32} - 1 - p$, most significant bit first. The resulting message can be written as $M_0 M_1 \dots M_{N-1}$, i.e. the concatenation of N (32-bit) words M_i.

The hashing process

Figure 2: Chip layout of the Subterranean Cryptographic Chip.

Clockcycle	State	Key Load	Output
t = −7..., −1	–	*(load)* 0	
t = 0	0	M_t	
t = 1..., N−1	F_s	M_t	
t = N..., N+7	F_s	0	
t = N+8..., N+23	F_s	0	$H_{t-(N+8)}$

The **Hash Result** is defined by $H_0 H_1 \dots H_{15}$.

Subhash is claimed to be collision-free: it should be computationally infeasible to come up with two messages that hash to the same result.

3 Chip Realization

3.1 Overall Functionality

The design has been realized in such a way as to fit in a 40 pin package. This required multiplexing information from different sources as well as bidirectional busses.

In Substream mode a parallel input of 16 bit words as well as a simultaneous parallel output of 16 bit words is provided at the speed of the overall clock.

In Subhash mode a parallel input of 32 bit words is provided a the speed of the overall clock.

The 256 bit keywords can be entered in 8 consecutive pieces of 32 bits in parallel.

A tree like clock distribution network has been designed in order to have an equal balancing of the clocks among all of the registers in the circuit.

3.2 MPC Service

The algorithm of Subterranean has been implemented in an integrated circuit. This has been done in the scope of the IMEC/INVOMEC multi project chip service. IMEC/INVOMEC is the division of

Appeared in *12th International Conference on Computer Design (ICCD 1993), VLSI in Computers and Processors*, R. Camposano, and A. Domic (eds.), IEEE Computer Society Press, pp. 610–613, 1993.

IMEC that is organizing the education, CAD support and MPC service towards educational institutions. IMEC/INVOMEC is also one of the five major organizers of the European wide EUROCHIP initiative, which provides these services to over 300 institutes (universities and polytechnics all over Europe).

The implementation technology has been the 2.4μm CMOS standard cell technology of MIETEC. The layout of the chip is shown in figure 2. The active area is 5.00mm x 7.01mm ($35mm^2$). The area including bonding pads is 6.00mm x 7.85mm ($47mm^2$). The correct operation of this chip has been measured up to a clock period of 56 nsec on a Tektronix LV-500 tester. This is a clock frequency of 17.8MHz and corresponds to an encryption/decryption throughput in CPRG mode of 286 Mbit/sec. In CHF Subhash mode this corresponds to 572 Mbit/sec.

3.3 Testability Considerations

In the first version of the design, careful considerations were taken from the start in order to make the chip testable. This was achieved by making all of the registers scan-testable. It turned out however that for many chip implementations of cryptographic algorithms it is undesirable to realize the registers with the keys as scan registers as they can be read out in test mode. In cases that one would include the scan chains in the additional test modes of a boundary scan according to JTAG, this would facilitate very much the readout of key registers.

Therefore the scanable registers in the key and state registers have been removed for additional security. In the current implementation the keys are *write-only*. This means that there is no direct access possible to the key- or state information via the external pins of the chip.

This of course had its consequences for the testability. Due to the cryptographic aspects of confusion and diffusion as explained above, it is such that the influence of stuck-at faults propagates very fast over all bits in the state register and consequently manifest their effect at the output of the chip. A number of test sequences, that exploit this aspect of confusion and diffusion, have been determined (with a maximum length of 43 iteration cycles). By means of fault-simulation it has been shown that these test sequences allow for a 100% testability of all stuck-at faults at the inputs and outputs of the standard cells.

4 System Demonstration

The feasibility of the chip has been demonstrated in a system setup for real-time video encryption/decryption. This is illustrated in figure 3. This application could be representative for an environment of pay television in case the television programs would be broadcasted in digital form, as is planned for high definition TV. This application could allow that the broadcaster uses different passwords for different programs, and a subscriber could pay for only these programs that he/she is interested in. Even when one would be in the possession of the Subterranean chip, with all of its internal details, it would be impossible to get access to the information in an unauthorized way without having access to the password.

Figure 3: Demonstration system for real-time video encryption/decryption.

In the demonstration system, a composite color video signal (PAL) is captured by a video camera, and converted in digital form by an A/D converter. This results in a digital signal at 115 Mbit/sec. This digital signal is encrypted on a first board hosting the Subterranean chip into an encrypted digital signal, which could than be broadcasted to all subscribers. At the other end a receiver board with the Subterranean chip is used to decrypt the digital information at a speed of 115 Mbit/sec. Hereafter the information can be converted by means of a D/A-convertor in analog form so that it can be shown on a color monitor.

In the demonstration setup, the passwords are entered for the encryption and decryption board via PC's interfaced to resp. the encryption and decryption boards. This demonstrator is operational and pictorally illustrates the concepts of cryptography and the practical applicability of the Subterranean algorithm. The chip and the algorithm itself however has the potential to be applied for much higher throughput applications as well.

5 Conclusions and Future Work

Current work concentrates on the further optimization of the circuit designs to improve on the speed.

Appeared in *12th International Conference on Computer Design (ICCD 1993), VLSI in Computers and Processors*, R. Camposano, and A. Domic (eds.), IEEE Computer Society Press, pp. 610–613, 1993.

Retargeting the design to a technology with smaller line widths will already increase the speed, as well as reorganizations in the logic.

The demonstration setup mentioned above will be used as a driving vehicle for the development and practical application of formal design and verification methods that are being developed in the CHARME ESPRIT Basic Research Action[14]. The demonstration environment is a heterogenous mixture of different design paradigms and implementation technologies. At the same time it combines hardware and software aspects. A manual exercise has been conducted already to formally prove the correctness of the cryptographic chip with respect to its higher level behavior by means of the *SFG-Tracing* verification methodology [12]. This methodology has currently successfully been applied already for the automatic verification of high level synthesis results [13].

Acknowledgements

The authors wish to acknowledge the help of many colleagues who have contributed in the succesful realization of this project: C. Das, B. Demey, R. Govaerts, D. Lambrichts, G. Vanderwegen, J. Vandewalle, M. Van Eylen, A. Vanhelmont, G. Vanwijnsberghe and P. Wambacq.

References

[1] *Contemporary Cryptology*, Gustavus J. Simmons Ed. IEEE Press, New York.

[2] C.E. Shannon, "Communication theory of secrecy systems", *Bell Syst. Tech. Journal*, Vol. 28, pp. 656–715, 1949.

[3] J. Daemen, R. Govaerts and J. Vandewalle, " A Hardware Design Model for Cryptographic Algorithms", *Computer Security–Esorics '92*, pp.. 419–434. LNCS, vol. 648, Springer-Verlag, Berlin 1992.

[4] Special issue on cryptography, *Proc. IEEE*, Vol. 76, No. 5, May 1988.

[5] M.E. Smid, D.K. Barnstad, "The Data Encryption Standard: Past and Future", *Proc. IEEE*, Vol. 76, No.5, pp. 550-559, May 1988.

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

[7] R.C. Fairfield, e.a., "An LSI Digital Encryption Processor (DEP)", *IEEE Comm. Mag.*, Vol. 23, No. 7, pp. 30-41, July 1985.

[8] H.M. Deppermann, e.a., "SICURE - A Crypto Chip for Rapid Encipherment", *Proc. EURO-ASIC'91*, pp. 68-73, May 1991.

[9] I. Verbauwhede, e.a., "Security and Performance Optimization of a new DES Data Encryption Chip",*IEEE JSSC*, Vol. 23, No.3, pp. 647-656, June 1988.

[10] I. Verbauwhede, e.a., "ASIC Cryptographic Processor based on DES", *Proc. EURO-ASIC'91*, pp. 292-295.

[11] H. Bonnenberg, e.a., "VLSI Implementation of a New Block Cipher", *Proc. ICCD'91*, pp. 510-513.

[12] L.Claesen, M. Genoe, e.a. "SFG-Tracing: a Methodology for the Automatic Verification of MOS Transistor Level Implementations from High Level Behavioral Specifications", *Proc. ACM-SIGDA Int. Workshop on Formal Methods in VLSI Design*, Miami, January 9-11, 1991.

[13] M. Genoe, L. Claesen, e.a. "Illustration of the *SFG-Tracing* multi-level behavioral verification methodology, by the correctness proof of a high to low level synthesis application in CATHEDRAL-II", *Proc. ICCD-91*, Cambridge, October 14-16, 1991, pp. 338-341.

[14] L. Claesen, D. Borrione, H. Eveking, G. Milne, J.L. Paillet, P. Prinetto, "Turning the Formal Verification of VLSI Hardware into Reality", *Proc. ESPRIT Conf. 1991*, North-Holland, Brussels, November 1991, pp. 857-873.

Appeared in *12th International Conference on Computer Design (ICCD 1993), VLSI in Computers and Processors*, R. Camposano, and A. Domic (eds.), IEEE Computer Society Press, pp. 610–613, 1993.