SPECIFICATION AND IMPLEMENTATION OF A CRYPTO-COPROCESSOR FOR ISDN

Walter Sachs and Stefan Wolter

University of Applied Sciences Bremen
Laboratory for the Design of Integrated Circuits and Systems
Neustadtswall 30, D-28199 Bremen, GERMANY
Tel. +49-421 -5905-2402, Fax -2400, email: wolter@fbe.hs-bremen.de

ABSTRACT

At the University of Applied Sciences, Bremen, we have developed a Crypto-Chip for real-time enciphering connections in any ISDN-net in close cooperation with an ISDN-component manufacturer. The chip is called "TELECRYPT", has less than 40 pads and is especially designed for the requirements of the telecommunication industry.

Aside from the hardware implemention of the ciphering algorithm a new concept for the integration of a ciphering chip into telephones and telephone systems is proposed.

The underlying technology can also be used for ciphering other serial datastreams. With the development of TELECRYPT it will be possible for the first time to set up telephones and telephone systems with minimum effort with one security module.

1. INTRODUCTION

Because of the progress in digital signal analysis, computer-based and automated wiretapping technologies as well as illegal wiretapping- and espionage-attacks, there is a public demand for secure communication. Solutions for safe electronic document transfer are being developed and widely used. In contrast to this, the range of real-time data encipherment solutions (telephone, fax, video conferences) is not widely used at the moment. Although real-time ciphering systems are fully developed for the high-end telecommunication, there are no appropriate solutions for the low-cost area and the mass market. Existing solutions are mostly "black-box" solutions, will say a separate device which performs the encryption of the user data. For the area of speech encryption special proprietary and expensive telephones exist.

The main emphasis of this papers lies in the special new features of the chip and its integration in existing telecommunication solutions. TELECRYPT will be integrated directly into the serial datastream using a new interface technique. Once initialized, the chip works autonomously.

In existing ciphering concepts the advantages given by the serial format of the user data in almost all WAN are not used. Conventional encryption devices receive the serial datastream, convert it into a parallel one, forward it to a ciphering chip by parallel busses, read out the encrypted data and finally make a parallel-to-serial conversion of the user data.

In addition to the ciphering chip this technology needs a high hard- and software-overhead. The results are high costs and complex encryption devices.

Our idea was to design a ciphering chip especially for serial datastreams. As an example, this will be shown with the ISDN-net.

In the ISDN-net, user data (e.g. speech) and control data (e.g. charge information, calling party number) are transmitted separately in a logical view. The user data will be transmitted in so-called "B-channels" and the control data in the "D-channel". These datastreams will be multiplexed through one physical bus system.

Our first approach was to encipher the user data at the physical bus level. Our second approach was to design a scalable, small and cheap chip, because available chips are designed for high data rates [7][8][9]. Hence, they are expensive. Another postulation was that the chip interfaces and the ciphering algorithm must be exchangeable with minimum effort.

This paper is organized as follows. In Section 2 we discuss the interfaces of the TELECRYPT device and its programming. In Section 3 we then give an application example for the integration of TELECRYPT in existing telecommunication solutions. Finally, we summarize our major findings and outline our future work.

2. CHIP DESCRIPTION

The newly designed chip TELECRYPT is especially made for the encryption of two independent, bidirectional user data channels of an ISDN basic access. The serial data interface is designed on the basis of the serial IOM-2 interface from Siemens [6]. This is an open, free available standard for an ISDN Inter-IC-Bus.

2.1 CHIP FEATURES

In the following, the features of TELECRYPT are listed.

- 64 Bit block ciphering algorithm IDEA with 128 bit key length
- supports the standard encryption modes ECB, CBC, CFB (1, 7, 8, 16, 32, 64), OFB and 64-Bit MAC
- universal, parallel microprocessor interface, configurable as "Read / Write Strobe Mode" (compatible to Intel / Siemens) or "Datastrobe Mode" (compatible to Mo-

torola), each mode configurable for multiplexed or demultiplexed adress bus
- serial Interface: Standard IOM-2 bus
- bitstream mode: protocol-transparent insertion in the serial IOM-2 data stream, because of the integrated, full duplex serial interface
- continuous behaviour: allows continuous ciphering in bitstream mode without external processor intervention
- key memory: configurable up to 16 keys and associated initialization vectors, two of them selectable as session keys via key select register
- switching possibility on the fly between encryption and decryption mode, because of the stored expanded decryption subkeys
- detailed chip-status and -error reports, with automatic fall-back in a safe state in error case
- programmable interrupt requests
- modular oriented VHDL-code, which makes it easy to change the encryption engine, the interfaces or the number of stored keys

2.2 BLOCK DIAGRAM

The block diagram of the chip is shown in Figure 1.

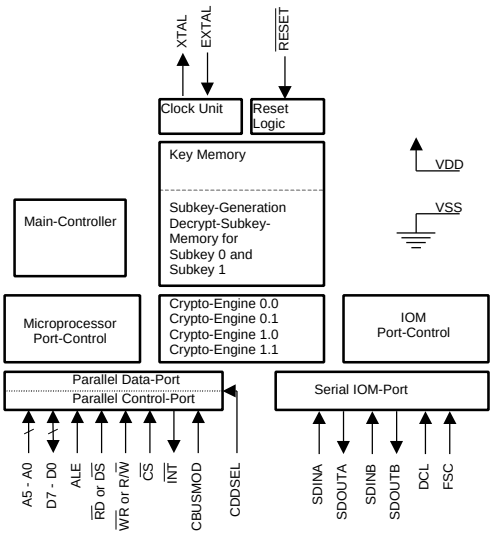

Figure 1: Block diagram of TELECRYPT

One main feature of the chip are the two independent data paths:

- *Dataport Mode*: the data goes completely through the parallel Data Port (D-Port), which is multiplexed with the configuration Port (C-Port)

- *Bitstream Mode*: the data goes completely through the IOM-Port

There is no internal data path between the two interfaces, because of security reasons.

The chip has three interfaces:

- one parallel data interface for ciphering the parallel-bus-based data, e.g. decryption of a master key.
- one parallel control interface for configuring the chip and key loading.
- one serial data interface for ciphering the serial data, which must be conform to the IOM-2 standard.

The two parallel interfaces are multiplexed by one physical 8-bit interface. The selection will be made by the signal "CDSEL".

Thanks to the serial data interface it is possible to implement the chip in existing serial data streams. Details are given in Section 3.

Furthermore, the chip has a scalable key memory up to 16 keys, extensive chip surveillance features and a mathematical unit for computing the encryption and decryption subkeys from the given IDEA-key.

The chip is made for real-time ciphering of two independent ISDN B-channels. Each of these channels is bidirectional ("talk and listen"). Through each of these channels it is possible to make a independent call. The conclusion for the key management is that for each B-channel an own key must be available. In consequence of the transfer of the user data in 8-bit blocks through the ISDN-net, the claimed real-time capability and the 64-bit block ciphering algorithm used, the ciphering must be performed in a feedback operating mode (CFB 8)[4]. Therefore, each data direction needs its own feedback register. This leads to the following structure inside the ciphering engine, as shown in Figure 2.

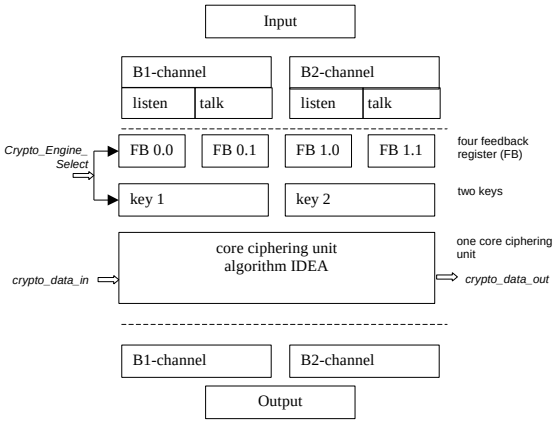

Figure 2: Physical structure of the ciphering engine

2.3 IDEA-ALGORITHM

Xuejia Lai and James Massey started with the development of this algorithm in the eighties. One reason was the increased computation power, through which a brute force attack on the widely used Data Encryption Standard (DES) Algorithm was thinkable, because it has only a key length of 56 bit. The new algorithm of Lai and Massey was published under the name "PES" (Proposed Encryption Standard). When the differential crypto analysis by Biham and Shamir showed weak elements in the PES, Lai and Massey redesigned this algorithm with the help of So Murphy in 1991. The new name was now "IPES" (Improved Proposed En-

cryption Standard). 1992 this algorithm was renamed in "IDEA" (International Data Encryption Algorithm) [5].

The IDEA-algorithm is a symmetrical block-ciphering algorithm with a data-block width of 64 bit and a key length of 128 bit [1]. It is known as one of the safest algorithms in the world. The German Telekom is using this algorithm for all its security products [2]. The algorithm consists, like most modern algorithms, of one round, which will be repeated several times. The structure of one round is shown in Figure 3.

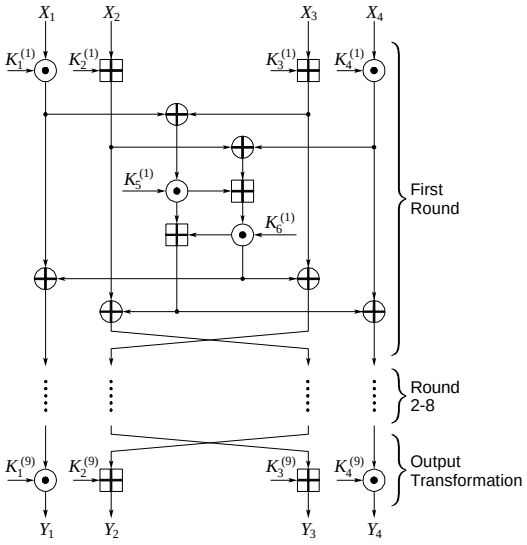

Figure 3: Structure of one IDEA-round, $K_x^{(y)}$ is subkey x of round y

The 64-bit data block is separated in four 16-bit sub-blocks X_1, X_2, X_3 and X_4. These sub-blocks will be combined with six 16-bit subkeys, which will be generated with help of a certain key schedule from the 128-bit IDEA-Key for each round. A dominant design concept in IDEA is mixing operations from three different algebraic groups, in detail:

- ⊕ Bitwise XOR of two 16-bit sub-blocks.
- ⊞ Addition modulo 2^{16} of two 16-bit sub-blocks.
- ⊙ Multiplication modulo (2^{16}+1), whereas an operand with the value zero will be replaced by 2^{16} [5].

Each round has as an output of four 16-bit blocks and they are the input for the next round. After the eighth round the output will be combined with four subkeys in the output transformation. The four result sub-blocks Y_1, Y_2, Y_3 and Y_4 will be concatenated to one 64-bit output block.

2.4 SERIAL IOM-2 INTERFACE

The IOM-2 bus standard is a serial Inter-IC-Bus, especially designed for the ISDN area. Since it has different operation modes, here we only take a closer look at the "linecard mode". The bus consists of four signals: Data Upstream (DU), Data Downstream (DD), Data Clock (DCL) and Frame Synchronization Clock (FSC). In the "linecard mode", the bus is capable of transmitting eight IOM-subframes. In Figure 4 it is shown, how the eight subframes will be transmitted. The bottom part of this figure shows in detail the structure of one subframe. It consists of two ISDN-B-Channels, named B1 and B2, each eight bit wide, one monitor channel for transmitting internal control data between ICs (eight bit wide) plus the two handshake bits MR and MX. Each subframe transmits two bit of the ISDN-D-channel and a four bit C/I channel (it carries real-time status information between the ICs in an application). The IOM-DCL-signal is used to clock data to and off the bus, it operates at twice the data rate. The IOM-FSC-signal is an 8-kHz clock. The rising edge signals a new IOM-frame.

The ISDN-net, the control data ("D-channel") and the user data ("B-channel") are separated. This makes it possible to process each channel independently. For the ciphering application, only the B-channel data is of interest. The control data needs not to be encrypted, because it routes the data stream through the public ISDN-net [3]. Our approach was to encrypt only the first 16 bit of each IOM-subframe, which holds the B-channel user data. The control data will be bypassed by the ciphering unit. This is graphicly shown in Figure 5.

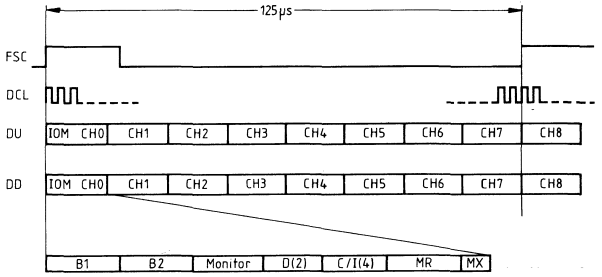

Figure 4: IOM-Linecard Mode [6]

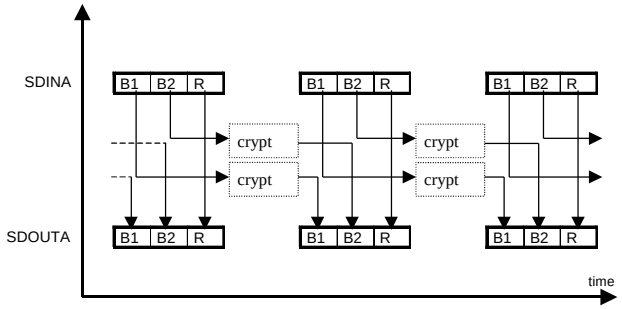

Figure 5: IOM-subframe rebuilding, only one direction shown. B1 and B2 are the ISDN-B-channel data signals, internal IOM-data (e.g. monitor channel) is marked as "R"

2.5 TELECRYPT INITIALIZATION AND PROGRAMMING

The chip is designed for autonomous data ciphering. This means that after the initialization and the input of the keys the chip starts ciphering by itself. There is no need anymore for a processor overhead after initialization. The chip detects start and end of a B-channel datablock and automatically starts the integrated ciphering unit.

The chip monitors itself; in case of an error or in case of writing in the wrong parameters upon initializisation, it will put itself in a safe state.

TELECRYPT can be programmed for performing the following features (among other things):

- Cipher-Mode / Transparent-Mode (for plain text connections), adjustable for each ISDN-B-channel separately
- Switch-off of one or both B-channels with output of a free definable idle-pattern
- Power-down behaviour of the integrated IOM-interface

3. APPLICATION EXAMPLE

An application example of the chip is given in Figure 6.

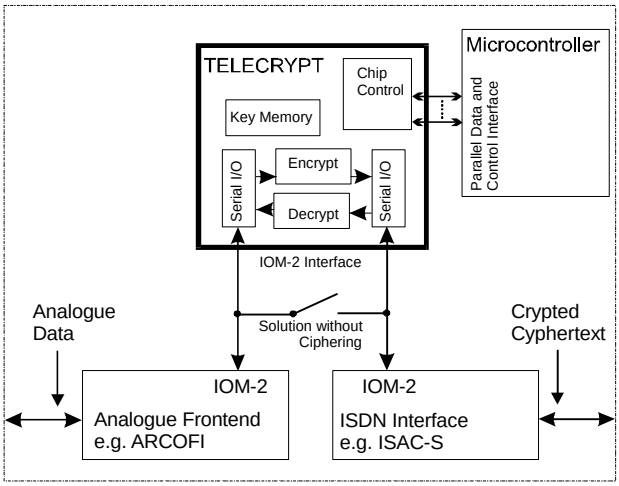

Figure 6: Application example for TELECRYPT

The chip is inserted in an ISDN-telephone or a telephone exchange unit. It is not necessary to redesign the hardware or the software, because the chip is simply added in an existing design by cutting the IOM-2 bus and inserting the chip. In Figure 6, the switch marks the same ISDN-solution without ciphering unit. The configuration of the chip and the key loading can be performed by the existing microcontroller by simply adding a new software task.

4. SUMMARY

With the solution proposed here it would be possible for the first time to design cheap and easy ciphering techniques for the digital telecommunication market. The VHDL-code of this chip is modular. So it was possible to design a chip derivative named TELECRYPT-S with minimum effort. This chip derivative is only capable of ciphering one ISDN-B-channel and has no parallel data port. Results of our prototype synthesis are given in Table 1.

Chip	**equivalent gate count**	**fits into listed FPGA**
TELECRYPT (two B-Channels, parallel dataport)	83.839	XILINX VIRTEX XCV 600
TELECRYPT-S (one B-channel, no parallel dataport)	40.561	XILINX VIRTEX XCV 300

Table 1: Chip synthesis results

Tests have been carried out successfully with an HP-ASIC-Tester.

In the future we plan the concept of this chip to be the basis for the implementation of other interface systems as well as carrier for other cryptographic algorithms.

5. REFERENCES

[1] Brueggemann T., and Buerk H. *The Encryption Algorithm IDEA.* ASCOM, Solothurn

[2] German Telekom AG. *Press release* of Feb. 14., 1997.

[3] Kambach, A. *ISDN*. Huethig Verlag, Heidelberg; 1998

[4] International Organisation for Standardization. *Information Processing; International Standard / ISO 8372.*Genf, 1987

[5] Lai X., *On the Design and Security of Block Ciphers*. Dissertation, ETH Zuerich, No. 9752, 1992

[6] Siemens AG. *ICs for Communications. IOM-2 Interface Reference Guide.* Siemens, Muenchen, 03.91

[7] Wolter S., et al. *VLSI Architecture for the Data Encryption Algorithm IDEA with advanced on-line Built-In Self-Test.* 5th International Conference on Signal Processing Applications & Technology, Oct. 1994, Dallas, Conference Proceedings

[8] Wolter S., Matz H., Schubert A., and Laur R. *On the VLSI Implementation of the International Data Encryption Algorithm IDEA.* IEEE International Symposium on Circuits and Systems, April 1995, Seattle, Conference Proceedings

[9] Zimmermann R., Curiger A., Bonnenberg H., Kaeslin H., Felber N., and Fichtner W. *A 177 Mb/s VLSI Implementation of the International Data Encryption Algorithm.* IEEE Journal of Solid-State Circuits, Vol. 29, No. 3, March 1994