Disclaimer: This document was part of the First European DSP Education and Research Conference. It may have been written by someone whose native language is not English. TI assumes no liability for the quality of writing and/or the accuracy of the information contained herein.

Developing Secure Communication Systems Using the TMS320C50 DSP

Authors: F. Sousa, P. Felix

ESIEE, Paris

September 1996
SPRA318

TEXAS INSTRUMENTS

IMPORTANT NOTICE

Texas Instruments (TI^{TM}) reserves the right to make changes to its products or to discontinue any semiconductor product or service without notice, and advises its customers to obtain the latest version of relevant information to verify, before placing orders, that the information being relied on is current.

TI warrants performance of its semiconductor products and related software to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are utilized to the extent TI deems necessary to support this warranty. Specific testing of all parameters of each device is not necessarily performed, except those mandated by government requirements.

Certain application using semiconductor products may involve potential risks of death, personal injury, or severe property or environmental damage ("Critical Applications").

TI SEMICONDUCTOR PRODUCTS ARE NOT DESIGNED, INTENDED, AUTHORIZED, OR WARRANTED TO BE SUITABLE FOR USE IN LIFE-SUPPORT APPLICATIONS, DEVICES OR SYSTEMS OR OTHER CRITICAL APPLICATIONS.

Inclusion of TI products in such applications is understood to be fully at the risk of the customer. Use of TI products in such applications requires the written approval of an appropriate TI officer. Questions concerning potential risk applications should be directed to TI through a local SC sales office.

In order to minimize risks associated with the customer's applications, adequate design and operating safeguards should be provided by the customer to minimize inherent or procedural hazards.

TI assumes no liability for applications assistance, customer product design, software performance, or infringement of patents or services described herein. Nor does TI warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right of TI covering or relating to any combination, machine, or process in which such semiconductor products or services might be or are used.

TRADEMARKS

CONTACT INFORMATION

US TMS320 HOTLINE	(281) 274-2320
US TMS320 FAX	(281) 274-2324
US TMS320 BBS	(281) 274-2323
US TMS320 email	dsph@ti.com

Contents

Figures

Tables

Developing Secure Communication Systems Using the TMS320C50 DSP

Abstract

This application report describes and characterizes secure communication systems over the Public Switched Telephone Network (PSTN). Global solutions are presented concerning the secure transmission of speech, data and facsimile group 3 signals. The areas covered by this work are source coding/decoding and ciphering/deciphering.

The Texas Instruments (TI^{TM}) TMS320C50 digital signal processor (DSP) facilitated the development of a low cost solution to a real-time problem. The TI DSP made it possible to implement simple and generic architectures while supporting complex computational models.

This document was part of the first European DSP Education and Research Conference that took place September 26 and 27, 1996 in Paris. For information on how TI encourages students from around the world to find innovative ways to use DSPs, see TI's World Wide Web site at www.ti.com.

Product Support on the World Wide Web

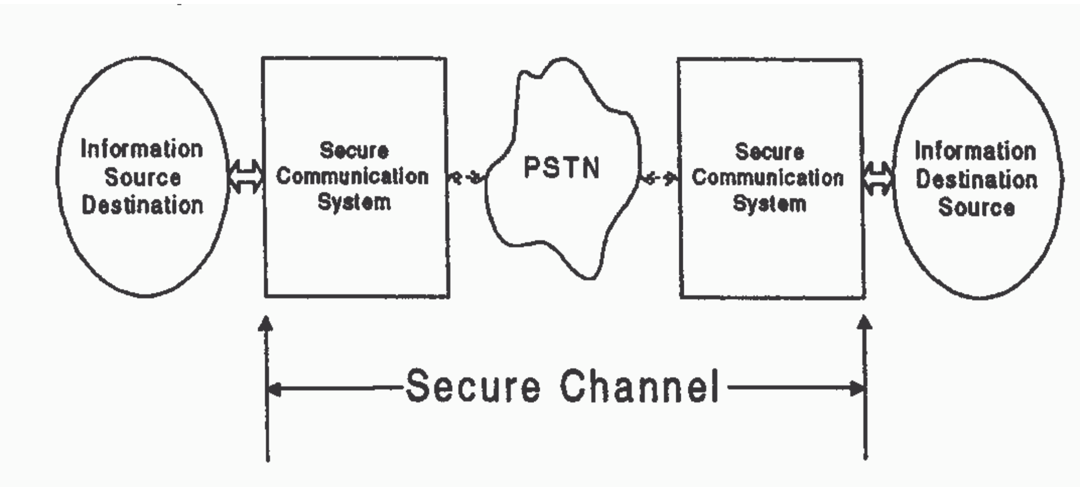
Our World Wide Web site at www.ti.com contains the most up to date product information, revisions, and additions. Users registering with TI&ME can build custom information pages and receive new product updates automatically via email.

Introduction

The growth of the communications market and the associated need for information integrity and secrecy encourages the development of secure communications systems. This work describes and characterizes the attributes of secure communication systems over the Public Switched Telephone Network (PSTN). This system supports speech, data (asynchronous serial format) and facsimile transmissions. The design criteria for these systems are:

- ❑ Communication privacy
- ❑ High quality synthetic voice
- ❑ Speaker identification
- ❑ Low coding/decoding delay
- ❑ Standard group 3 fax support
- ❑ Complexity constrained to an acceptable price

Figure 1. Secure Communication over PSTN


Information Source Destination
Secure Communication System
PSTN
Secure Communication System
Information Destination Source
Secure Channel

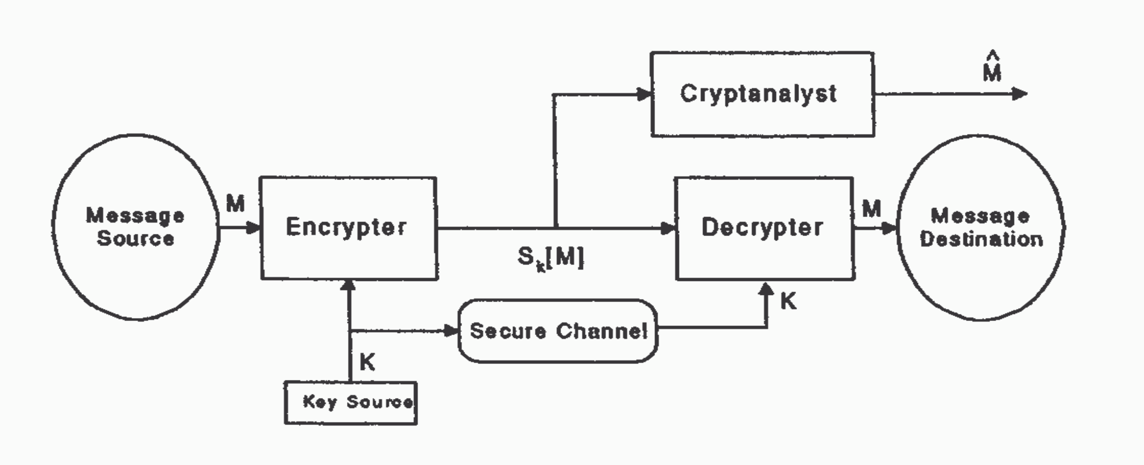
The use of programmable DSPs is spreading rapidly in telecommunications applications. The DSP is especially well suited for the implementation of source and channel coders. The 16-bit TI TMS320C50 DSP was chosen because of its low cost, low power consumption, and its ability to handle real-time events.

The goal of this work is to develop a secure communication system to be inserted between the information source and the non-secure channel PSTN, thereby providing a secure channel (see Figure 1).

Figure 2 shows the classical secure communication model.[1] The message M is encrypted (ciphered) by a transformation S_k obtained from the family of transformations S. The key K selects the appropriate transformation S_k.

The message M is obtained by application of the inverse transformation, M = S_k^{-j} (S_k[M]), at the destination. The crypt-analyst algorithm tries to estimate M from the knowledge of S_k[M], the family S, the universe of possible K and the universe of messages. The security of the system resides only in the secrecy of the key K.

Figure 2. Secure Communications Model



The main components of the developed systems, described in the following sections, are illustrated in Figure 3. They are

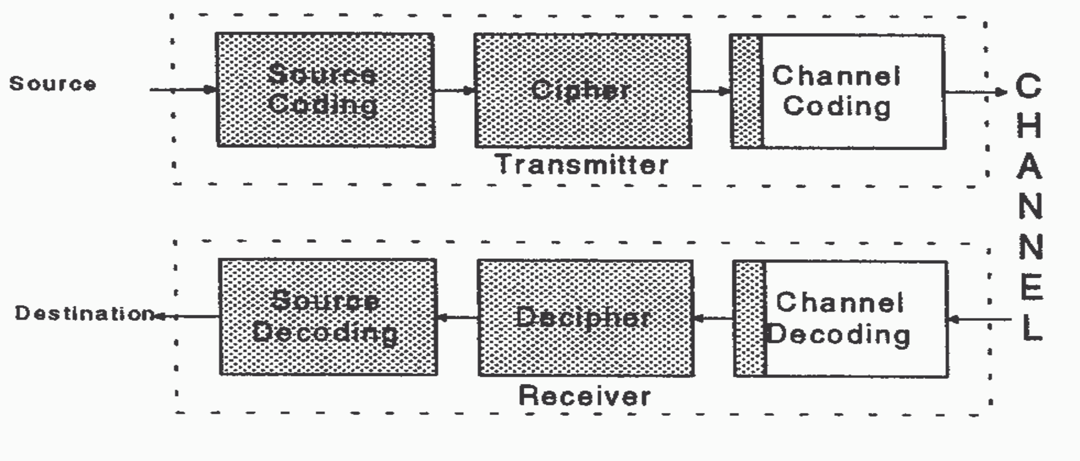
- ❑ Source coding and decoding
- ❑ Cipher and decipher
- ❑ Channel coding and decoding

The highlighted blocks are described in the following sections.

Source coding reduces the message redundancy. This process serves not only to reduce the bit rate of the source, making possible the digital transmission of speech in PSTN, it also increases the cipher efficiency.

The security component lies on the cipher/decipher modules. A cryptographic library was developed integrating private and public key algorithms. The integration of end user customized cryptographic algorithms is also possible.

Figure 3. Secure Communication System Structure



A standard module (Rockwell Socket-Modem) is used for channel coding over the PSTN. Modem functions are well suited for DSP-based implementation.[10]

Group 3 fax ciphering has a slightly different structure. These signals are already channel coded for the PSTN. Channel decoding is necessary after the source input. The receiver must reverse the coding sequence in order to retrieve the original input.

The following sections focus on the development and test criteria for these real-time systems.

This paper is organized as follows. The *Source Coding* section describes source coding schemes with special emphasis on speech compression algorithms. The *Security* section describes the security components (cipher/decipher). The *Hardware Architecture* section describes the hardware architecture of the implemented system. The *SPCS Software Architecture* section describes the computational model used in this solution.

Source Coding

Source coding removes redundant information. Different schemes were used depending on the type of source, i.e., data, Group-3 fax signals, and speech.

Data compression is performed by a universal source coder (based on Lempel-Zev algorithm – LZ77).[2]

Fax data was not encoded since it had previously been coded with the recommended Group 3 one-dimension coding scheme[3].

Two model based speech-compression algorithms have been developed. The Linear Predictive Coding (LPC) is used for transmission at 2.4 Kb/s were the Residual Excited Linear Predictive Coding (RELP) is used to transmit at 9.6 Kb/s. The RELP coder (RELP10) works if the link is established at the 9.6 Kb/s rate.

If the channel does not support 9.6Kb/s, the system commutes to the LPC coder (LPC10) thus preserving the communication integrity. The system performs echo cancellation since the speech interface is a standard 2-wire telephone. [4]

Informal subjective listening tests were used during development to improve the synthetic speech quality. A subjectively selected good version was used to compare with some well-known systems, namely SPENDEX and STUIL. The final version was selected based on Mean Opinion Scores (MOS) and paired comparisons tests (Portuguese words and sentences are used).[6] These tests have been carried out with non-specialized listeners. Both speech-compression algorithms are discussed in the following paragraphs.

LPC10 Coder

Table 1 summarizes the main characteristics of the LPC10 coder. Linear Predictive Coding is used to transmit at 2.4 Kb/s. [5] [6] [7] To improve quality, refinements have been introduced concerning quantization and interpolation of parameters, pitch estimation, and the synthesis of the excitation function.

Reflection coefficients are non-uniformly quantified according to the maximum entropy criterion. Coefficients statistics have been obtained by analysis of long time speech segments from several speakers (male and female) in different age groups.

To achieve smoother, more natural speech and avoid unwanted transients in the synthesized speech, model parameters are pitch interpolated synchronously between updates. Interpolation is performed only at the end of the pitch period when the overall energy in the filter is at a minimum.

Table 1. LPC10 Coder Characteristics

Sampling frequency	6510 Hz	
Speed	2400bps	
Frame period	28ms	
Bits per frame	56	
	parameters	53 (36)
	synchronization	3 (20)
Predictor order	10	(voiced)
	5	(unvoiced)
Pitch	AMDF modified median filter with 5 taps uniform quantization 50 to 350 Hz	
Gain	maximum entropy quantization	
Emphasis	$\alpha = 0.95$	
	$\beta = 0.74$	
LPC Analysis	asynchronous	
	hamming 42 ms window	
	28 ms shift	
Analysis method	autocorrelation	
Reflection coefficients	maximum entropy quantization	
Synthesis	pitch synchronization	
	parameters synchronization	
Excitation	achieved function with pitch dependence decimation	

Pitch extraction is based on the *Average Magnitude Difference Function* (AMDF). To minimize pitch determination errors, a post processing technique is used that combines a modified version of the automata proposed by Ross et al. and a median filter as a non-linear smoother. [8]

Selection of the excitation function has an important impact on synthetic speech quality. A random number generator is used for unvoiced sounds. For voiced sounds, the adopted excitation function (DOD) is interpolated and archived as a look up table.[9 6] Additionally, the look up table is later subjected to pitch dependent decimation.

RELP10 Coder

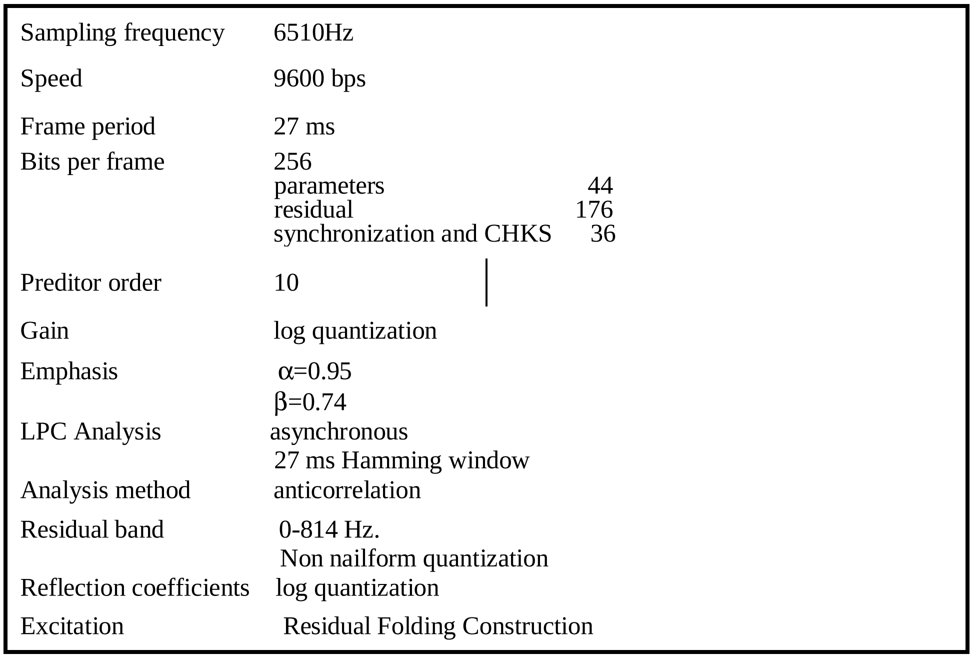
The Residual Excited Linear Predictive Coding algorithm is used to transmit at 9.6 Kb/s.[5] [6] [7] This transmission rate is a result of a commitment between the source coder-decoder complexity, the channel coder/decoder complexity, and the transmission error effects on the synthetic speech quality. In fact, the speech coder actually works at 8 Kb/s. The other bits in the frame are used for synchronization.

The RELP coder is a hybrid, communication-quality speech coder that combines LPC spectral modeling with transmission of some aspects of the residual error signal. This approach provides a major contribution to the naturalness of the synthetic speech, since the residual signal carries the highest perceptual content. The absence of voicing and pitch estimators significantly simplifies the analyzer and avoids the serious consequences of pitch and voicing errors in LPC synthesis.

Only the 0 - 814 Hz baseband of the residual error signal is transmitted. The receiver interpolates the residual baseband back to the original signal by spectral folding.

The RELP10 coder provides good signal quality with a moderate rate of transmission (9.6 Kb/s). Table 2 summarizes the characteristics of the RELP10.[7]

Table 2. RELP10 Coder Characteristics



Sampling frequency	6510Hz	
Speed	9600 bps	
Frame period	27 ms	
Bits per frame	256	
	parameters	44
	residual	176
	synchronization and CHKS	36
Preditor order	10	
Gain	log quantization	

Emphasis	α=0.95
	β=0.74	

LPC Analysis	asynchronous 27 ms Hamming window	
Analysis method	anticorrelation	
Residual band	0-814 Hz. Non nailform quantization	
Reflection coefficients	log quantization	
Excitation	Residual Folding Construction	

Table 3 lists the processor utilization and the memory requirements for the RELP10 coder software running on a TMS320C50 at 40 MHz. The processor requirement value reflects execution from zero-wait-state external SRAM (Program segment) and use of processor internal RAM (Data segment). Both memory segments can be mapped on the internal RAM.

Table 3. Full Duplex REPL10 Coder Requirements

Processor (% usage)	**Data Memory (words)**	**Program Memory (words)**
70	1.3K	13K

Security

The cipher and decipher modules of the communication system displayed in Figure 3 are based on a cryptographic software library. The use of software, when compared with the use of specialized hardware, makes the system more versatile and easier to adaptate to different end users. The design goals of the cryptographic library are:

- ❑ Characterization and implementation of the basic elements of cryptographic algorithms: pseudo-random generators, one-way functions, permutation functions, extended-precision modular arithmetic, etc.
- ❑ Implementation of standard and proprietary cryptographic algorithms and protocols

During the communication session, conventional secret-key algorithms such as the Data Encryption Standard (DES) are used.[10] The private keys for these algorithms are obtained in the initiation phase of each session, using public-key techniques. The characteristics of the communication systems make it impossible to have static session keys in each machine for all the possible interlocutors.

The accepted key management protocol is based on the use of certificates.[11] A certification authority generates public and private keys, as well as certificates, for each member of the network. A certificate establishes a reliable relation between a user identity and his public key. The certificate is composed of the key, a timestamp and the user name. This set is ciphered with the public key of the certification authority, making the reading of the certificate possible. The key pair and the certificates are delivered to each user on a secure media, usually a chipcard.

On a session initiation, the users exchange their certificates, obtaining each others public key. It is followed by the exchange of the keys for the secret-key algorithm, ciphered by the public key. The keys of the secret-key algorithm (e.g., DES) are different for each session since they are generated randomly.

Most of the known public-key algorithms involve extended-precision modular arithmetic, which leads to time-consuming operations. Therefore, a special emphasis was given to the optimization and adaptation of this family of operations to the TI DSP architecture. An analysis of the optimization methods available was performed, and a hybrid technique using the Chinese remainder theorem, Montgomery's reduction algorithm and a convolution sum based multiplication algorithm was implemented for the modular exponentiation computation.[12] [13]

Table 4 shows the profiling results of the multiplication, addition, Montgomery's reduction algorithm (REDC), convolution sum based multiplication (CONVSM) and squaring (CONVSS). The results were obtained on a TM5320C50 EVM running at 40 MHz.

Table 4. Number of Cycles and Execution Times of Each Algorithm for Different Modulus Lengths

Algorithm **Number of bits**	**Number of cycles**	**Time (µs)**
512		
Addition	212	10.6
Multiplication	6598	329.9
CONVSM	3948	197.4
CONVSS	3056	152.8
REDC	7232	361.6
1024		
Addition	340	17.0
Multiplication	25382	1269.1
CONVSM	11193	559.7
CONVSS	7569	378.5
REDC	26432	1321.6

Details and more results with the RSA system implementation are available.[13] [14]

Hardware Architecture

Two hardware architectures were developed to sustain the proposed systems:

- ❑ Cryptographic card, capable of performing fast cryptographic and signal processing operations, for use in a PC open system
- ❑ Embedded systems for secure digital speech and data communications

The kernel of the prototype versions is based on the TMS320C50 DSP Starter's Kit (DSK5), which includes the DSP and a COMBO (A/D and D/A converters and filters), and offers the following advantages:[15]

- ❑ Reduction in board complexity, decreasing the probability of logical errors and inadequate physical layout, which results in a shorter design time
- ❑ In-circuit debugging capabilities using the DSK5D debugger

The presence of the data, address and control buses on the expansion connectors of the DSK5 makes it possible to design a prototype board satisfying the system memory and I/O requirements. The DSP and the COMBO remain on the kit. The design of the final version (industrial version), without the DSK5, remains a trivial task if the prototype is properly tuned.

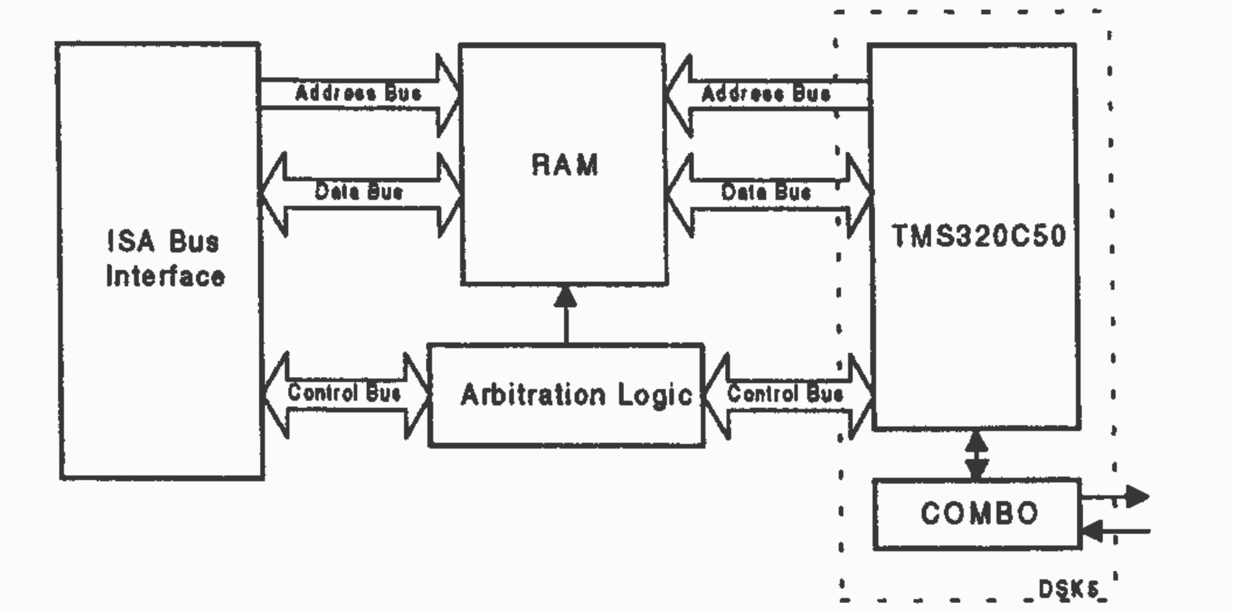
The cryptographic card was designed to enable the use of the time-consuming algorithms, such as the RSA, on applications with real-time requirements, running on a PC platform. The first version of the Secure Facsimile Communication System (SFCS) was implemented over a PC platform and this card is used to perform RSA cipher and decipher operations as well as line tone-signaling detection. The channel encoding and decoding task are accomplished using two commercial ISA bus Modem-Faxcards.

The card's design criteria were:

- ❑ Low complexity
- ❑ Fast processing capabilities
- ❑ Fast communication interface with the host

It consists of a TM5320C50, 64 Kbytes of Single Access Random Access Memory (SARAM), arbitration logic, and an ISA bus interface.

Figure 4. ISA Card Hardware Architecture



The SARAM is mapped on both the data and the program space of the DSP as well as in the memory space of the PC. The mutual exclusion in the access to the SARAM is controlled by the arbitration logic, using the HOLD/ and HOLDA/ signals of the DSP. This feature enables shared memory communication between host and DSP as well as dynamic program loading. This allows the transmission of data between host and the card to use all the ISA bandwidth, minimizing the communication overhead. This makes the distribution of the processing viable. The low cost and specially fitted architecture of the DSP makes it the best choice for the card kernel.[16]

The prototype board with the DSK5 allows simultaneous debugging of the PC and DSP programs, reducing the development phase for the interface software.

The embedded system was designed to provide the hardware base of the Secure Personal Communication System (SPCS) supporting the implementation of the LPC10 and RELP10 vocoders.

This architecture was designed to be:

❑ Simple to minimize cost

❑ Easy to update as a result of the vocoder’s refinement and/or integration of other vocoders in response to speech coding evolution

❑ Provide secure data communication

- ❑ Provide a friendly human interface

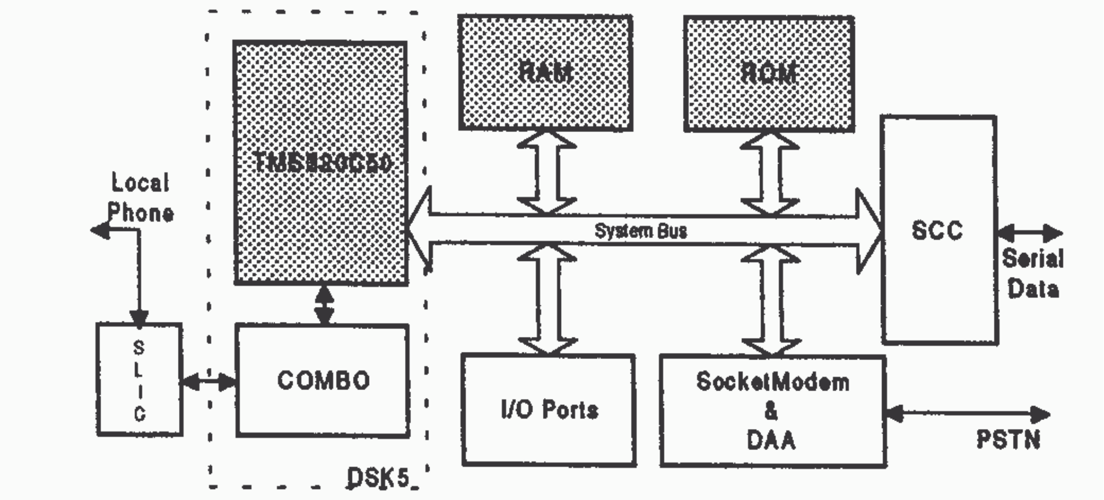
The system is constituted by a main kernel (highlighted area in Figure 5) consisting of:

- ❑ TMS320C50
- ❑ RAM
- ❑ ROM

The system also includes these peripherals:

- ❑ COMBO chip
- ❑ I/O ports (4x4 keyboard, LCD, Smart-card, etc.)
- ❑ Serial Communication Controller (SCC)
- ❑ Socket-Modem and Data Access Arrangement (DAA)
- ❑ Subscriber Line Interface Circuit (SLIC)

Figure 5. SPCS Hardware Architecture



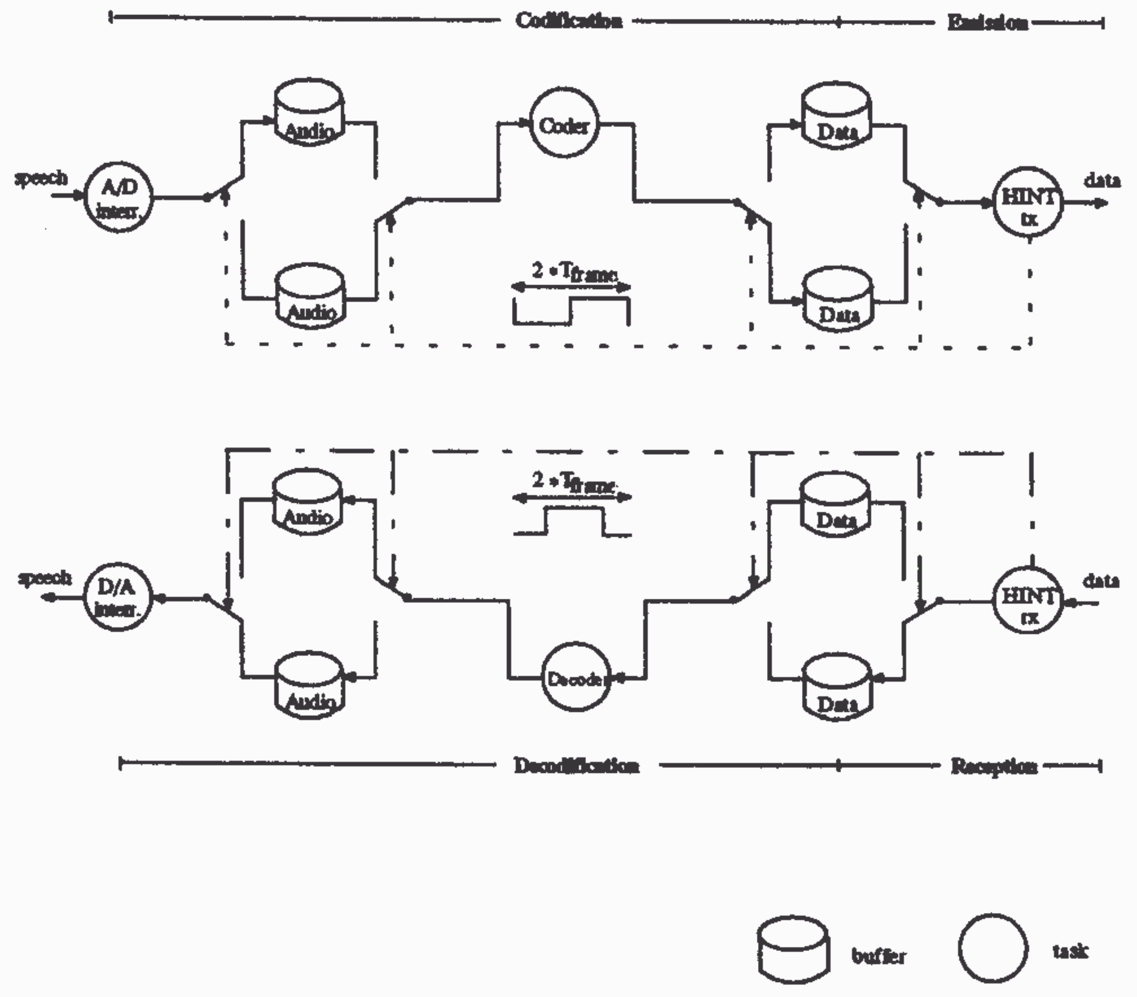
To support facsimile group 3 ciphering, this system is designed to incorporate an extra Socket-Modem. Fax machines with a digital interface are linked to the serial port.

The prototype version is also built using the TMS320C50 DSP Starter's Kit.

SPCS Software Architecture

To support the structured design of the SPCS, a computational model was developed, as shown in Figure 6.

Figure 6. Computational Model: Synchronization and Communication



This computational model has two main background processes (Coder and Decoder) and several foreground tasks associated with hardware interrupts. Foreground tasks virtualize an input/output block system. The transmitter works this way: in the codification process one block of speech samples (Audio buffer) is transformed into one encrypted data frame while the emission sends another data frame (Data buffer). The data frame includes synchronization and error control information.

The receiver (reception and the de-codification) works inversely. Communication between tasks uses common memory with simple synchronization mechanisms. The foreground tasks are associated with A/D and D/A hardware interrupts and to modem interrupts (HENT). The processor is shared via external interrupt processing. Coder and Decoder processes run asynchronously in background.

In data communication mode, the speech coder task is replaced by the universal source coder. The interrupts from the A/D and D/A are replaced by the *SCC* interrupt.

Summary

In this paper global solutions covering aspects of source coding/decoding, ciphering/deciphering have been described. The systems herein proposed have some particular features: both are based on a commercially available DSP chip and are capable of ciphering data, fax and speech.

The developed architecture provides compatibility by supporting other standard source coders and ciphers model implementations, namely the NSA-developed Government Standard LPC-1O algorithm.[9]

To cope with real-time and low cost implementation on a DSP, simple and generic architectures and a computational model have been developed. The characteristics of these architectures allow software upgradability and integration of end user customized cryptographic algorithms. The techniques developed in this work can also be applied to another type of channel, such as radio.[7]

Acknowledgements

The authors acknowledge the support provided by the Centro de Calculo do Insuituto Superior de Engenharia de Lisboa (CCISEL).

References

[1] W. Diffie, M. Hellman, “New Directions in Cryptography”, *JEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 644-645, November 1976.

[2] D. Coulinbo, F. Sousa, I. Milano, P. Sampaio, “Compression of Programs for Download via Packet Switch Data Networks, Using a DSP Based Lempel Ziv Algorithm Implementation”, *Proceedings of The International Conference on Signal Processing Applications & Technology* – ICSPAT96, Boston, 1996.

[3] ITU-T Standardization of Group 3 Facsimile Apparatus for Document Transmission, ITU-T Recommendation T,4.ITU, 1994.

[4] P. Marques, F. Sousa, “TMS320C50 Echo Canceller Based on Low Resolution Time delay Estimation”, *Proceedings of The First European DSP Education and Research Conference*, Paris, 1996.

[5] J. Markel and A. Gray Jr., *Linear Prediction of Speech*, Springer-Veriag Berlin Heildelberg New York, 1976.

[6] P. Papamichalis. *Practical Approaches to Speech Coding*, Pretince Hall. Inc.,Englewood Cliffs, New Jersey, 1987.

[7] F. Sousa, “DSP Based Secure Systems for Digital Speech Communication over PSTN and via Radio”, Proceedings of The International Conference on Signal Processing Applications & Technology – ICSPAT94, Dallas, Vol. II. pp. 1405-1410, 1994.

[8] M. Ros, H. Shaffer, A. Cohen, R. Freudberg, H. Manley. “Average magnitude difference function pitch extractor”, *IEEE Transactions on Acoustics, Speech, and Signal Processing*, Vol. ASSP 22, pp. 353-362, October 1974.

[9] Documentation of the Government Standard LPC-10 Algorithm, USA.

[10] P. Papamichalis, J. Reimer. “Implementation of the Data Encryption Standard Using TMS32010”, in *Digital Signal Processing Applications with the TMS320 Family*, Vol. 1, Texas Instruments, pp. 455-465, 1986.

[11] J. Nechvatal, “Public Key Cryptography”, in *Contemporary Cryptology*, edited by G. Simmons, IEEE Press Piscataway, pp. 190-195, 1992.

[12] F. Sousa, P. Felix, “The Computation of Extended-Modular Exponentization on a DSP Architecture”. *Proceedings of The International Conference on Signal Processing Applications & Technology* ~ ICSPAT96, Boston, 1996.

[13] P. Montgomery, “Modular multiplication without trial division”, *Mathematics of Computation*, Vol. 44, pp. 519-521, 1985.

[14] R. Rivest, A. Shamir, and A. Adleman, “A method for obtaining digital signatures and public key cryptosystems”, *Commun*, ACM. Vol. 21, No. 2 pp. 120-126, 1978.

[15] *TMS320C5x DSP Starter Kit User’s Guide*, Texas Instruments, 1994.

[16] TI, *TMS320C5x User’s Guide – Digital Signal Processor Products.* Texas Instruments, 1993.