Signal and Information Processing Laboratory

Prof. Dr. G.S. Moschytz (Director) / Prof. Dr. J.L. Massey
Prof. Dr. F. Eggimann / Prof. Dr. A. Kälin / Dr. K. Heutschi

ANNUAL REPORT

1 9 9 6

Research Period 1996

Teaching Period 1995/96

Address:	Signal and Information Processing Laboratory ETH-Zentrum, Sternwartstr. 7, CH-8092 Zürich
Phone:	+41-1-632 2764
Fax:	+41-1-632 1208
Electronic mail:	sekr@isi.ee.ethz.ch
World Wide Web:	http://www.isi.ee.ethz.ch
Editor:	B. Röösli

Foreword

It is with great pleasure that we at the Signal and Information Processing Laboratory (ISI) reach out once again to our many friends to present our annual report on the events at ISI in the past year.

As will be apparent from reading the contents of the annual report, 1996 was a successful and active year with the usual turnover of doctoral students completing their thesis and leaving ISI, and young new teaching assistants coming aboard to fill the resulting vacant slots. Thomas Ernst completed his thesis on "Adaptive Detectors for Data Communications over Recursive Channels" and joined the Swiss Bank Corporation in Basel; Pius Estermann completed his thesis on "Adaptive Filters in the Frequency Domain: Analysis and Design Strategies" and started work at Siemens Schweiz AG in Zurich; Carlo Harpes completed his thesis on "Cryptanalysis of Iterated Block Ciphers" and returned to Luxembourg, where he is working at Weyderf in Fentage; Daniel Müller finished his thesis on "Hybrid Echocompensation with Applications in Digital Data Communications over Copper Wires" and accepted a position with Philips Semiconductors AG in Zurich, and Christian Waldvogel completed his thesis entitled "On the Nature of Authentication Protocols" and joined Eutelsat in Paris. As always, it was with mutual mixed feelings that these outstanding young researchers took their leave from ISI: on the one hand they were reluctant to leave what had become a close bond in research activities and friendship within ISI, and on the other they were eager to take on the challenge of applying their newly acquired expertise in an entirely different working environment.

Our freshly promoted PhDs were soon replaced at ISI by new assistants: Dani Lippuner and Thomas von Hoff, who had just graduated as ETH diplom engineers, and Madhu Reddy who joined us from the California State University at Long Beach, California, USA (and who, incidentally, is the son of our popular frequent guest and visiting professor, Dr. Hari Reddy). Another newcomer, dipl. El. Ing. Markus Erne, graduate of ETH, joined ISI as a research engineer after having spent nearly a decade in industry, during the last few years of which he ran his own company Scopein, which specializes in signal processing equipment for communications.

One very important activity of ISI is to host guests from academic and research institutes from all over the world. The last year was no exception; we had interesting visitors from the USA, UK, Israel, Spain and China. These contacts never fail to stimulate new ideas and, very often, result in ongoing joint research activities and formal projects. These visits, as well as most of our other activities, require support both financially and administratively. It is a pleasure, once again, to thank the EE department chairman and his staff, as well as the ETH administration, for providing this support generously and forthrightly at all times. Warmest thanks go also to all the members of ISI, whose constant cooperation, motivation and good will, in the final resort, are responsible for the fine accomplishments of our ISI.

Mai 1997

Prof. Dr. G.S. Moschytz Prof. Dr. J.L. Massey

Contents

1. Personnel

Institute Director and Professor for Communication Engineering (Network Theory and Signal Processing):

Prof. Dr. George S. Moschytz

Professor for Digital Systems Engineering (Coding and Information Theory):

Prof. Dr. James L. Massey

Professor for Information Technology:

Prof. Dr. Fritz Eggimann

Adjunct Lecturer:

Dr. K. Heutschi

Assistant Professsor (Signal Processing):

Prof. Dr. August Kälin

Secretaries:	**Mrs. Bernadette Röösli**		
	Mrs. Renate Agotai		
	Mrs. Heidi Schenkel		
Administr.Supervisor:	**Dr. Thomas Mittelholzer**		
Technical Supervisor	**Dr. Max Dünki**,		
Teaching Assistants:	**Martin Hänggi**	Dipl.El.Eng.	
	Felix Lustenberger	Dipl.El.Eng.	
	Dani Lippuner	Dipl.El.Eng.	since 1.4.96
	Thomas von Hoff	Dipl.El.Eng.	since 1.8.96
	Peter Wellig	Dipl.El.Eng.	
Research Assistants:	**Richard De Moliner**	Dipl.El.Eng.	
	Markus Erne	Dipl.El.Eng.	since 10.6.96
	Thomas Ernst	Dipl.El.Eng.	left on 30.9.96
	Pius Estermann	Dipl.El.Eng.	left on 31.12.96
	Markus Helfenstein	Dipl.El.Eng.	
	Marcel Joho	Dipl.El.Eng.	
	Beat Keusch	Dipl.El.Eng.	
	Gerhard Krämer	Master of Sci.	
	Xuejia Lai	Dr.	
	Drahoslav Lim	Master of Sci.	
	Urs Loher	Dipl.El.Eng.	
	Bahram Mirzai	Dipl. Phys.	
	Daniel Müller	Dipl.El.Eng.	left on 31.8.96
	Stefan Oberle	Dipl.El.Eng.	
	Andreas Poncet	Dipl.El.Eng.	
	Madhu Reddy	Master of Sci.	since 21.5.96

	Jossy Sayir	Dipl.El.Eng.	
	Hanspeter Schmid	Dipl.El.Eng.	
	Rolf Seiler	Dipl.El.Eng.	left on 31.10.96
	Rolf Steiner	Dipl.El.Eng.	
	Jürg Stettbacher	Dipl.El.Eng.	
	Felix Tarköy	Dr.	
	Sigi Wyrsch	Dipl.El.Eng	
Technical Staff:	**Francesco Amatore**		
	Petro Gavriilidi		
	Felix Frey	El.Eng.HTL	
	Thomas Schaerer		

Academic Guests: (see 6.1 for report of activities)

Prof. Ch. Toumazou	Imperial College, London, England	17.01. - 19.01.96
Prof. D. Graupe	Northwestern University, Evanston, USA	25.04 .- 05.05.96
Prof. L. Chua	University of California, Berkeley, USA	15.05. - 15.07.96
Prof. H. Reddy	California State University, Long Beach, USA	25.03. - 03.04.96 17.06. - 31.07.96 28.11. - 07.12.96
Prof. J. Katzenelson	Technion - Israel Institute of Technology, Haifa, Israel	03.07. - 18.07.96
Prof. A. Arbel	Technion - Israel Institute of Technology, Haifa, Israel	28.10. - 27.11.96
Prof. A. Carlosena	Universidad Publica de Navarra, Pamplona, Spanien	01.12. - 07.12.96
Prof. X. Lin	Beijing University of Posts & Telecommunications, Beijing, China	01.01.- 31.12.96
St. Ortman	Univ. of Notre Dame, Notre Dame, USA	20.05. - 27.07.96

2. Teaching

2.1 Lectures and Practica

Sem.	Instructors	Title	ETH-No.
5th	Prof. Moschytz Prof. Massey	Zeitdiskrete Systeme & stochastische Signale	35-405
6th	Prof. Moschytz Prof. Massey	Digitale Signalverarbeitung und Filterung	35-416
5/7th	Prof. Massey	Applied Digital Information Theory I	35-417
8th	Prof. Massey	Applied Digital Information Theory II	35-418
7th	Prof. Moschytz	Analoge Signalverarbeitung und Filterung	35-467
8th	Prof.Moschytz Prof.Eggimann	Adaptive Filter & neuronale Netzwerke	35-468
7th	Dr. Heutschi	Acoustics I	35-477
8th	Dr. Heutschi	Acoustics II	35-478
5/ 6th	Prof. Moschytz Prof. Massey et al.	Laboratory for "Fundamentals in Electrical Engineering"	35-095/6
	Prof. Moschytz Prof. Massey et al.	Colloquium on "Electronics and Communications	35-910
	Prof. Eggimann et al.	Colloquium on "Neuro-Informatics"	95-899 95-999
	Prof. Eggimann	Colloquium on "Material- und Werkstoffwissenschaften"	35-797
	Prof. Rathe	Acoustics Colloquium	35-950

2.2 Semester Projects and Diploma Theses

During the winter semester 1995/96 and summer semester 1996, 15 Semester Projects (27 candidates) and 9 Diploma Theses (13 candidates) were carried out.

Candidates	Title	Supervisor
Semester Projects WS 95/96 (7th Semester)		
Marius Portmann Marc Rennhard	Mehrkanaliges, adaptives Hörgerät	Joho
Alex Bänninger Jonas Fluri	Soundprocessing auf 32-bit DSP	Lustenberger Wyrsch
Matthias Giger Christoph Mäder	Geräuschunterdrückung bei Sprachsignalen	Oberle
Florian Albrecht Christian Rohner	Mehrdimensionale Spektrumschätzung von bewegten Schallquellen	Steiner
David Perels Olivier L. d'Epinay	Erkennung von akustischen Signalen	Mirzai
Mose Iadarola	High Rate Modulation/Coding Schemes	Mittelholzer
Johan Martensson Jonas Loefgren	Kodierung für den verrauschten Zwei-Benutzer-Addierkanal	Keusch
Semester Projects SS 96 (8th Semester)		
Marcel Bamert Patrick Häsler	Initialisierung von neuronalen Netzwerken	Mirzai
Robert Reutemann Michael Rüegg	Erkennung von akustischen Signalen	Mirzai
Daniel Gull Stefan Menzl	Digital generierte Schallfelder	Stettbacher
Matthias Fitzi Guido Steiner	Prädiktion von Börsenkursen mit neuronalen Netzen	Hänggi Bohli/Schweiz. Bankverein
Mauro Tibolla	Klirrfaktorreduktion bei Rundfunk-sendern mit neuronalen Netzen	Wellig Poncet
Ralph Tonezzer Pascal Vontobel	Untersuchung von Dynamik-kompressoren für Hörgeräte	Launer/Phonak Oberle, Wyrsch

Eric Suter	Schätzung des Spektrums von bewegten Schallquellen am Beispiel einer Lokomotive	Steiner
Catherine Lamy	Turbo-Coding for M-QAM	Mittelholzer
Benoist Guillard	Signal Sets	Lin

Diploma Theses WS 95/96

Armin Deiss Schmuel Holles	Automatische Selektion von Basisfunktionen für nichtlineare Prädiktion	Poncet Mirzai
Dominique Cachin Felix Egger	Adaptiver Kompensator für die aktive Schalldämpfung mit Gegenschall	Kälin Steinebrunner Sulzer/Innotec
Sandro Marcoli Thomas von Hoff	Akustische Rückkopplungskompen-sation bei Freihandtelefonen	Estermann
Guido Meyerhans	Concatenated Decoding	Costello
Daniel Lauk	Simulation mit ADSL	Muralt
Jens Hansson Elisabet Ivarsson	Source Modelling with Limited Memory	Sayir

Diploma Theses SS 96

Magnus Berggren	Coding for Higher Order Partial Response Channels Mittelholzer	Prof.Siegel
Felice Battiston	Bau eines Fuzzy-Reglers für Rastersensormikroskopie	Dr. Meier (Uni Basel)
Dieter-Michael Arnold	Turbo-Coding for Mobile Communications Mittelholzer	Perez

3. Research

3.1 Research Areas

The Institute for Signal and Information Processing engages in teaching and research in those aspects of communication engineering that deal with the processing of electrical signals and digital information. This includes:

Signal Processing

Analog and digital signal processing as applied to analog signals (e.g. speech or biological signals) and to digital signals (e.g. digitally transmitted data or coded speech signals). Current research topics include:

- Behavior of nonlinear dynamic systems
- Neural Networks and Cellular Neural Networks (CNNs) for Signal Processing (Speech, Acoustical Alarm Signals, Recognition of Handwriting)
- Switched-Capacitor (SC) and Switched Current (SI) Filters and Networks; Application to Mixed Mode Circuits for High-Speed Communication Systems
- CAS Tools for the Design and Layout of Analog, SC and SI Filters for the Realization of VLSI Technology
- Processing of Electromyograms (EMG's), EMG Modeling and Analysis
- Acoustical Signal Detection and Recognition
- Adaptive Filters and Systems for Communications
- Signal Processing Algorithms (e.g. Noise Suppression, Beam Forming, Adaptive Gain Control and Filters) for Hearing Aids
- Measurement of Sound Propagation in Open Spaces
- Sound Localization in Audiology

Information Theory

Information Theory as applied to problems in communications and data processing. Current research topics include:

- Codes over Rings and over Groups
- Spread-Spectrum Multiple-Access Techniques
- Coding for Spread-Spectrum Systems
- Design and Testing of Secret-Key Ciphers
- Complexity of Cryptographic Functions

3.2 Current Research Projects

Section 1: Signal Processing

Section Leader: Prof. Dr. G.S. Moschytz

Group 1: Analog and Digital Signal Processing

Group Leader: Prof. Dr. G.S. Moschytz

Design of Probabilistic Models for Estimation and Decision

A. Poncet, Tel. No. 632 3620; poncet@isi.ee.ethz.ch

The problem of designing a data-adaptive model for an application of system identification, signal prediction, or classification, is addressed in a unified probabilistic framework. The performance of a model is quantified by its generalization error (risk). According to the loss criterion used, the risk can be, e.g., the mean squared error, the mean relative entropy, or the misclassification rate. Since a model is trained with random data, the risk is a random variable. The probability distribution of this quantity was derived explicitly. This general result clarifies why (and how much) the performance of an adaptive model tends to degrade as soon as more parameters "than needed" are used. Furthermore, it suggests systematic solutions to the three main issues of model design.

First, a set of appropriate input variables (regressors) has to be selected. For this purpose, a method based on kernel density estimation was developed to infer Bayes risk from data. The second issue involves the choice of basis functions. It was shown how to select from a set of candidate basis functions the smallest subset needed to reach a given performance. The third issue consists in evaluating the performance of the designed model. This was solved using Bayesian inference: by combining the distribution mentioned above with the training data, one obtains the conditional distribution of the generalization error. The design methodology is illustrated by applications in noise reduction, time-series prediction, and pattern recognition.

In Collaboration with: Prof. M. Hasler, Swiss Federal Institute of Technology Lausanne.

Keywords: nonlinear signal processing, adaptive models, statistical inference

Design of Active CMOS Current-Mode Filters for the Video Frequency Range

H. P. Schmid, Tel. No. 632 3546; schmid@isi.ee.ethz.ch

Although most of today’s signal processing is done digitally, it is the analogue part of an IC which is difficult to build. One problem of analogue filters is their precision: switched capacitor and switched current filters can be very precise, but they are sampled data filters and therefore comparatively slow.

Time-continuous analogue filters are much faster, but they are normally less precise. The theoretical work done up to now (classification of current conveyor biquads, search for good biquad structures, sensitivity theory and optimization, investigations into conveyor realizations) has shown that there normally is a precision/speed tradeoff. The Sallen-Key biquadratic filters we wish to implement also show a quality-factor/precision tradeoff. However, the technique of on-chip tuning makes it possible to tune a filter during its operation and thus to eliminate most errors which come from process tolerances, temperature change and ageing.

With this technique, it seems possible to build a 10-20MHz 5th- or 7th-order elliptical lowpass filter using a standard 3V/1.2u CMOS process. To achieve this, we will first verify the function of our variable-gain current conveyor. It is the analogue part of an IC which is difficult to compare the performance of different variable MOSFET-resistors, discuss several tuning strategies used for voltage filters, find the maximum achievable precision and implement the tuning strategies in current-mode.

Keywords: current-mode amplifiers, current-mode filters, current conveyor, analogue integrated circuits, CMOS.

Design and Implementaion of Switched-Current Filters

M. Helfenstein, Tel. No. 632 3619; helfenst@isi.ee.ethz.ch

The specifications of many modern communication systems are making demands on the analog front end circuits that are pushing the limits of available technology. This is particularly true of baseband filters in various telecommunication systems in which requirements such as frequency range, power consumption, intermodulation distortion, and dynamic range may only be barely achievable with available design and production techniques. In an effort to compare the performance of two competing technologies, namely switched-capacitor (SC) and switched-current (SI) circuits, a switched-capacitor and a switched-current baseband filter meeting the specifications for a typical high performance communication system were designed, built, and measured.

The filters are sampled with clock frequencies up to 10MHz and the nominal center frequency fp is 500kHz with a pole-Q of 10. The focus of the investigation was on implementation issues, such as low voltage supply operation and PSRR. It is shown that in the SI case the design can be made independently of the modulation index, which results in superior circuit behavior for large input signals.

Although sampled-data filters may need a post-filter, the behavior in the frequency and voltage range under consideration is superior to that of continuous-time filters such as gm-C implementations. Among the sampled-data filters, the SC technique is superior when a large S/N-ratio and high accuracy of the filter is called for, whereas SI provides medium performance at lower cost. Nevertheless, in the SI case, it has been shown that a very good PSRR and a large modulation of the bias current can be achieved if gain-enhancement techniques designed for low saturation voltages are used. In combination with the bilinear integrator operating at double speed (i.e. the double sampling capability), a low transmission error in the integrator sections can be accomplished. Nevertheless, at low battery voltages, MOS device matching and clockfeedthrough remain a concern in SI designs.

Supported by: KTI

In Collaboration with: Philips (Faselec), Zurich

Keywords: switched-current filters, analog signal processing

Fast Algorithms for Adaptive Beamforming

Marcel Joho, Tel. No. 632 2771; joho@isi.ee.ethz.ch

Hearing-impaired people often complain about conventional hearing aids not only amplifying desired signals (targets, e.g. speaker in front) but also spatially distributed noise sources (jammers, e.g. engine noise, speakers from behind). It is usually difficult to separate targets from jammers with a single-microphone hearing aid because both are similar in nature.

Array signal processing provides a technique of discriminating between different sound sources (speaker in front, machine noise from aside) because of the different spatial locations. This allows to distinguish between the signals to be amplified and the ones to be attenuated (spatial filtering).

The Griffiths-Jim beamformer is a well-known structure for implementing spatial filters. It is used in this project to compare different adaptive algorithms in a hearing aid environment (LMS, RLS, frequency domain LMS). The main criteria are: jammer suppression, tracking ability and computational complexity.

Keywords: linear adaptive filters, array processing for hearing aids

Design and Applications of Robust Cellular Neural Networks

B. Mirzai, Tel. No. 632 7608; mirzai@isi.ee.ethz.ch

Cellular neural networks (CNNs) constitute a class of nonlinear, locally connected, dynamic systems which operate in parallel. This project is devoted to the following aspects: a) Analog implementations have necessitated a need for robust templates. In view of this, we investigate the performance of CNNs with regard to parameter variations and seek to design robust templates. For the class of applications requiring monotonic trajectories, we derived design rules based on which robust values can be chosen. In other cases, we had to explore the particular nature of the underlying dynamics to obtain robust templates. Connected component detection and shadowing are typical examples of this class which were considered successfully. We further developed learning algorithms that outperform the existing ones in the synthesis of templates. b) Issues concerning stable equilibria of symmetric and opposite sign templates are other subjects of interest, both in view of robustness and understanding of CNN dynamics. Here we classified all the possible equilibria of the opposite sign CNNs in the their simplest case and provided a comparison in the dynamics of symmetric CNNs with that of the opposite sign CNNs. c) Research concerning applications of CNNs to speech recognition has been conducted. Feature vectors are extracted in the time domain and transformed to 2-dimensional representations. A CNN is used in the process of feature extraction as an encoder to provide us with bipolar representations of utterances. This isolated word recognition system was applied to digit recognition using TI 46-Word data bank. The recognition rate for female utterances was 96.7% and for male utterances 99%.

Keywords: nonlinear circuit theory, cellular neural networks

A Mixed Analog/Digital Implementation of a Programmable Cellular Neural Network

Drahoslav Lím, Tel. No. 632 3616; drahoslav.lim@isi.ee.ethz.ch

A Cellular Neural Network (CNN) is a dynamic system based on parallel operation of simple units. In combination with digital logic, the system is referred to in the literature as the "CNN Universal Machine", which is capable of many types of processing tasks, including applications in several areas of signal and image processing (see the related project "Design and Applications of Robust CNNs"). The practicability and advantage of this approach depends on the network being implemented in hardware, rather than simulated by digital computer.

This project is concerned with developing techniques of implementing CNNs as integrated circuits, and with the design of CNN circuits programmable to a degree sufficient to be capable of a wide range of processing tasks. Such a system combines elements of analog continuous and sampled-data circuits, as well digital systems to a degree not found in conventional mixed analog/digital circuits. The analog part of such a CNN processor is essentially a gm-C circuit, and has little in common with with conventional Neural Networks. In particular, no "analog memory" is used for storing connection weights, and the weights are precomputed and stored as a low-resolution digital word. The circuits are be implementable in conventional (digital) CMOS processes.

Several small test chips have been designed and built to verify the function of the various component blocks. Based on the obtained results, a larger chip containing several CNN cells and digital logic is under development; several such chips connected together on a circuit board will comprise a CNN large enough to perform practical tasks. The designs incorporate several features new to CNN hardware: the ability to form a large network by connecting several smaller chips, template values chosen for CNN functionality rather than according to conventional binary weighting, and the ability to perform processing via so-called "spatially-variant template" programs.

Supported by: Swiss National Science Foundation

Keywords: nonlinear circuit theory, cellular neural networks

Group 2: Adaptive Systems

Group Leader: Prof. Dr. A. Kälin

Compensation of Loudness Recruitment and Adaptive Feedback Cancellation in Hearing Aids

S.Wyrsch, Tel. No. 632 6589; wyrsch@isi.ee.ethz.ch

Hearing-impaired persons with loudness recruitment have a reduced range between threshold and discomfort. As a result the effective dynamic range of a hearing-impaired person is extremely compressed and varies with frequency.

In a preliminary project we used a limited set of bandpass filters in order to compensate for this loudness recruitment. The input signal in each band is weighted using an appropriate compression gain. Together with our frequency-domain feedback canceller and a sophisticated step size control we built a real-time system with the algorithm running on a DSP. This system shows excellent performance for recruitment compensation and feedback cancellation with no artefacts even while the overall gain is 20 dB above the critical gain (if no feedback is canceled).

The aim of the new project is a hearing aid which is based on a psychoacoustic model of the impaired listener. By considering resolution and invertability of this model we hope to obtain a new hearing aid which is computationally more efficient and suits the hearing-impaired better.

Supported by: KTI and Phonak AG

In Collaboration with: Phonak AG

Keywords: loudness recruitment, rigital hearing aid, feedback cancellation, multiband compression

Localization of Fast Moving Noise Sources

R. Steiner, Tel. No. 632 3620; steiner@isi.ee.ethz.ch

Nowadays the noise emission of moving objects such as cars, engines etc., is an important design criterion. What is needed to reduce noise emissions efficiently is the exact knowledge of each sound source on the object. In other words we are interested in the sound intensity field which is generated by the emitting object. For estimating this sound intensity field we measure in our project the sound pressure with a static microphone array consisting of 31 microphones.

Acoustical Holography allows to map the sound pressure on a specific plane (hologram plane) to the sound field (sound pressure or particle velocity) on any other plane. Two necessary conditions of conventional holography are (1) that the measured signals are stationary and (2) that the measurable area of the hologram plane is large enough to record the relevant part of the sound field. Since the microphone array in our application is static and consists of a few microphones only, both conditions are violated.

To tackle the nonstationarity of the sound sources the sound field is mapped from the stationary coordinate system into a moving coordinate system in which the sound field is stationary. In order to handle the rather restricted measurable part of the sound pressure on the hologram plane the sound field on any other plane is estimated in an optimal way incorporating a priori knowledge of the sound sources. The proposed new algorithm has recently been verified using real measurements on an engine type Ae 4/7.

Supported by: Sulzer Innotec, Winterthur

In Collaboration with: Sulzer Innotec, Winterthur

Keywords: wiener estimation, acoustical holography, moving noise sources

Noise Reduction with Hidden Markov Models

Stefan Oberle, Tel. No. 632 2771; oberle@isi.ee.ethz.ch

Enhancement of speech degraded by additive background noise plays an important role in communication systems such as mobile telephones and modern hearing aids. As opposed to noise reduction schemes which are based on a noise reference signal, we assume a scheme where only the noisy speech signal is available for processing (monophone noise reduction).
In this research project a noise reduction scheme is investigated that uses two separate hidden markov models (HMM) to describe the statistical properties of speech and noise. The speech HMM models the clean speech and is trained using typical speech sequences from different speakers; the training of the noise HMM is based on typical noise sequences. Given the separate HMM's for the clean speech and the noise, a composite model for the noisy speech can be obtained. For every frame of the noisy speech signal, the composite model gives an estimate of the power spectra of the clean speech and noise signal within that frame. Using these power spectra, a Wiener filter is computed and applied to the noisy signal.

Although the HMM-based approach yields reasonably well enhanced speech, voiced speech segments often sound rough or hoarse. In 1996, it was shown that this effect occurs because the noise between the harmonics of voiced segments is not removed by the Wiener Filter. An algorithm was proposed, which uses pitch period information, and which is based on least square (LS) estimation, to remove these noise components. Moreover, it was shown that the estimation involving low-energy states of the speech HMM is not reliable, and therefore a noise floor is inserted during low-energy speech segments instead of filtering the signal.

Keywords: noise reduction, speech enhancement, hidden markov models

Recognition of Environmental Sounds using Hidden Markov Models

Stefan Oberle, Tel. No. 632 2771; oberle@isi.ee.ethz.ch

Classification of environmental sounds has many applications in the field of signal processing. As an example, we consider in this project a tactile hearing aid which can facilitate the communication of the profoundly deaf with the hearing world. We use an approach called TIPS (Tactile Identification of Preclassified Signals) where an alarm signal is automatically assigned to one of a few predetermined classes. The classification result is then passed to the user by tactile stimulation. Other applications might be the automatic classification of background noise to adapt a hearing aid to a changing acoustical environment or the classification of environmental sounds in security and surveillance systems.

In this project a new recognition scheme for environmental sounds using Hidden Markov Models (HMM's) is investigated. A maximum likelihood classifier is used where the observation probability density function of each class is modelled by a four-state HMM. Training of model parameters is performed independently for each alarm class allowing an easy addition of new signal classes. The HMM-based recognition scheme shows a good recognition rate and very low computational costs making it well suited for a real-time implementation. In the

last report period, a demonstration system based on a single DSP-board has been successfully implemented and tested.

Keywords: classification, signal recognition, hidden markov models

Development and Implementation of a Hands-Free Phone System Based on a Partitioned Frequency-Domain Adaptive Echo Canceller

Thomas von Hoff, Tel. 632 3615; vonhoff@isi.ee.ethz.ch

Providing means for a comfortable unrestricted full-duplex hands-free conversation is of great interest for industry and still a current research topic. We applied a partitioned frequency-domain adaptive FIR filter based on the least-mean-square concept as an echo canceller to realize a robust hands-free phone which allows for a full-duplex operation. This echo canceller uses a partitioning of its filter-coefficients into segments which can be adapted individually in the frequency-domain. It is optimally designed in such a way that it approaches the tracking behavior of the recursive least-squares (RLS) algorithm. We combined our frequency-domain echo canceller with a new adaptive, step-size control in order to cope with varying far-end/local speaker situations. Its performance is demonstrated by means of real speech signals. Assuming a loudspeaker-room-microphone impulse response of approximately 3500 tabs (8 kHz sampling rate), an increase of the critical gain of 14 dB has been obtained (for each phone) by using an adaptive echo canceller with 1152 taps. Our concept uses an additional adaptive gain control in order to (i) equalize the time-varying level of the local-speaker signal (due to this movement in the room), (ii) to suppress local background noise in speech pauses, and (iii) to suppress the remaining residual echoes. Due to the used block processing technique, our realization is computationally very efficient and requires only one single processor (ADSP 21020) for each phone device.

Supported by: KwF and Alcatel STR AG, Zurich

Keywords: frequency-domain adaptive filters, block processing technique, feedback cancellation, hands-free phone system

Active Noise Control

Prof. A. Kälin, Tel. No. 632 2762; kaelin@isi.ee.ethz.ch

Conventional methods of suppressing acoustic noise using passive sound absorbers generally do not work well at low frequencies (below about 500 Hz). An approach to overcome this problem is to cancel the disturbing sound field with the help of a second interfering field, typically generated by coil loudspeakers. The generation and control of its input signals is the task which is usually associated with active noise control. Mostly, the acoustic system which describes the generation and transmission of the disturbing sound field is varying. This in turn asks for an adaptive controller. In general, the design of such a controller is still an open problem. The goal of this project is to find simple and efficient controllers for typical configurations by systematically using appropriate a-priori knowledge about the acoustic system and its excitation.

So far a simple adaptive feedforward controller which allows a periodic sound field to be canceled has been developed in cooperation with an industrial partner. In this report period we extended the investigation to stochastic sound fields. Based on an available estimation of the system, a fixed control filter (high-order FIR filter) is optimally designed and on-line adapted to the true system and to the true input process by means of a low-order FIR filter. Considering the loudness sensitivity of a human listener, an A-weighted performance criterion is used 1) in the design of the fixed control filter and 2) in adapting the additional low-order filter. The design has been verified by means of measurements on an experimental single channel system. A suppression level of more than 20dB(A) has been observed for a stochastic ventilation noise signal.

Supported by: Sulzer Innotec

In Collaboration with: Sulzer Innotec

Keywords: active noise control, frequency-domain adaptive filters, LMS algorithm

Group 3: Applied Acoustics

Group Leader: Prof. Dr. E.J. Rathe

Audiometry to Evaluate Binaural Hearing

Juerg M. Stettbacher, Tel. No. 632 2773; stettbac@isi.ee.ethz.ch

Hearing impaired persons suffer not only from their hearing loss but also from a decrease in the ability to locate sound sources. Today's audiometry possesses only rough tools to measure direction discrimination; and so far no scale or metric to judge a subject's directional hearing has been established.

This research project aims at a greater understanding of this complex field. Equipment as well as a measurement procedure and rules are called for. The equipment should be suitable for clinical use.

During a first step a comprehensive measuring device was developed and built. It consists of an array of loudspeakers an a multi DSP computer. Each loudspeaker is driven by one processor. The system can be accessed and used from a workstation or pc but is intended to work stand-alone later.

The device is now being used to generate three-dimensional, dynamic acoustical situations like moving sound sources for example. It is particularly interesting to compare different algorithms and signals with the (psychoacoustic) impression they create. Results from these experiments will imply rules for the clinical testing of the binaural hearing.

Supported by: Johann Jakob Rieter Stiftung, Winterthur.

In Collaboration with: ORL, Universitätsspital Zürich.

Keywords: binaural hearing, sound localization, audiology, audiometry, DSP.

Group 4: Information Technology

Group Leader: Prof. Dr. F. Eggimann

On-Line and Off-Line Handwritten Word Recognition

M. Reddy, Tel. No. 632 2766; reddy@isi.ee.ethz.ch

Systems for writer independent handwriting recognition have a wide variety of applications ranging, e.g., from automatic mail address recognition, to entering handwritten commands on computers. Whereas on-line recognition is based on trajectory data from a touch sensitive pad, off-line systems process scanned image data. The on-line system developed earlier was extended to the more difficult off-line case by using the same system design together with appropriate pre-processing methods.

The data is pre-processed in both cases by a normalization scheme which makes no irreversible segmentation decisions and processes complete words as units. Additional features are extracted and added to provide further information for the recognition. A time-delay neural network (TDNN) with local connections and shared weights estimates the a posteriori probabilities for characters. Using these probabilities, a hidden Markov model (HMM) segments the word into characters to optimize the word score with respect to a dictionary. The best systems were trained on 27000 words from 59 writers and used the 25000 word UNIX dictionary.

The first attempts at off-line recognition were done using on-line trajectories converted to off-line bitmaps. Now, the off-line system has been modified to also recognize scanned data.The results for the scanned data while not yet as good as those for the on-line data are quite encouraging. Using a database collected at the Institute, the scanned error rate for cursive script recognition was 42.6% while the on-line system had an error rate of 37.3% for the same data. Further work on the scanned recognition will hopefully lower this error rate.

In Collaboration with: Dr. Markus Schenkel, University of Sydney

Keywords: neural networks, handwriting recognition, hidden markov models, pen computing, cursive script recognition, off-line recognition

Section 2: Digital Information Theory

Section Leader: Prof. Dr. J.L. Massey

Error Control Scheme for Magic WAND (Wireless ATM Network Demonstrator)

B.Keusch, Tel. No. 632 5290; keusch@isi.ee.ethz.ch

Major research interest has recently been focused on Wireless ATM and interworking between ATM networks and mobile systems. The Magic WAND project (Wireless ATM Network Demonstrator) aims to develop and implement a wireless access system to an ATM network that will provide multi-media services with guaranteed Quality of Service (QoS) to the mobile users. The Medium Access Control (MAC) protocol, called the Mobile Access Scheme based on Contention and Reservation for ATM (MASCARA), will support traffic allocation according to the traffic contract of each ATM connection, mobility features, and an error control functionality.

The major design issues for an appropriate error control scheme are its robustness against variations in the channel quality, its flexibility (various service classes with different delay requirements), its complexity (high-speed environment), as well as high bandwidth efficiency. The error control functionality is embedded in the physical layer and the MAC layer: it is to be designed in combination with the channel-access algorithm and to be applied selectively for each type of ATM connection. A hybrid form of ARQ and forward error control (coded modulation) is proposed in which the required code rate is relatively high, resulting in a low decoding complexity and small processing delay, and the rate is selected according to the channel quality and the required quality of the service. A modified Go-Back-(At most-)N (GBAN-D) ARQ strategy was proposed that incorporates delay control features and a (cell-)discard mechanism. An improved version of this GBAN-D protocol and a selective-repeat strategy with delay control were investigated: these strategies require a buffer at the receiver.

Supported by: BBW

Keywords: ATM, error control, ARQ

Code-Time Division Multiple Access

U. Loher, Tel. No. 632 5194, G. Krämer, Tel. No. 632 5058; loher@isi.ee.ethz.ch

In recent years there has been a great increase in the demand for mobile radio communications and for services. Future mobile systems will support a variety of environments so that a single terminal can serve as a telephone, pager, fax, answering machine and digital diary. The goal of this joint project with the Swiss Telecom PTT was to design and to simulate the air interface of a future-generation access technique called "Code-Time Division Multiple Access" (CTDMA) and to implement efficient coding techniques for a CTDMA system. The practical aspects of implementability were also considered.

A possible receiver design and its performance on the link level in a single cell has been simulated and formed a basis for the investigation of system level performance parameters such as system capacity and spectral efficiency in a cellular environment. Various approaches for cell separation on the system level were proposed and methods for providing multiple and variable bit rates were suggested. In particular, the use of a "short" spreading sequence combined with a Walsh-Hadamard rate adapter proved useful for the latter issue. Indeed, we proposed a spreading sequence of length 13, which offers advantages not only in terms of multiple and variable bit rates but also in supporting wireless high-speed communications, e.g., 2 MBits/s.

Implementation aspects such as complexity and compatibility with GSM were also considered within this project. This project is now completed but CTDMA techniques are still being considered in European Standardization bodies such as ETSI.
Supported by: Swiss Telecom PTT

In Collaboration with: Swiss Telecom PTT

Keywords: multi-user communication, multiple access, spread spectrum

The Role of Feedback in Random-Accessing

U. Loher, Tel. No. 632 5194; loher@isi.ee.ethz.ch

It is rather surprising that, after almost fifty years since its birth as a science, information theory has only rarely been applied to communication systems that incorporate feedback. What is known about feedback in information theory is more qualitative than quantitative. For instance it is known that the existence of feedback from the base station in a mobile communications networks to the users increases the maximum stable throughput of random access systems and simplifies the communication protocols necessary for operation near this maximum. However, this maximum is not known to date for any kind of non-trivial feedback.

In this project we attack the problem of determing the maximum achievable throughput depending on the feedback and we focus on binary and ternary feedback. This allows one to identify precisely what information must be received by the base station from the users attempting to access it before the users can be granted access. In a cellular packet-radio system (and in many other forms of random accessing), this question is complicated by the fact that the packets that are used for gaining access to the base station also contain the information that is transmitted when the accessing is successful. It will be necessary to separate somehow the accessing information from the transmitted information. In this project we try to answer this essential question in an adequate information-theoretical treatment of random accessing. In a next step we will then exploit the insight obtained from the identification of the essential accessing information in order to develop improved protocols for random-accessing within a cellular packet-radio network.
Keywords: random accessing, collision resolution, multiple access protocols

Conditional Source Coding Using Competitive Lists

Jossy Sayir, Tel. No. 632 2767; sayir@isi.ee.ethz.ch

New universal source coding algorithms were devised that improved on the generalized recency ranking scheme method developed last year. While the new methods are still based on conditional self-organising lists, recency-ranking was replaced by the more performant competitive list. The latter was analyzed and an analytical derivation was given linking its output probability distribution to its input distribution.

The latest coding system developed surpasses the old system in terms of compression ratio, while reducing the memory requirement by several orders of magitude. This makes it the most memory-efficient coding algorithm available

today. It outperforms the state-of-the-art Ziv-Lempel algorithm, but its compression ratio is far below that of the memory-intensive PPM algorithm.

Keywords: universal source coding, data compression, context trees

Capacity and Coding for Multiple Access Channels with Feedback

G. Krämer, Tel. No. 632 5058; kraemer@isi.ee.ethz.ch

Feedback is an essential part of almost all communications systems. With feedback, simple coding techniques can transmit data reliably at the maximum possible rate, the channel capacity, for many practical channels. Feedback may even increase the capacity of channels with many users by allowing the users to coordinate their transmissions to combat disturbances and interference. In this project, the simplest of many-user channels, the two-user memoryless multiple access channel, is studied. In this scenario, there are two users who wish to transmit data reliably to a common receiver. The goal of this project is to determine the capacity of such channels and to specify simple coding techniques for achieving capacity. This should lead to a better understanding of the role of feedback in communications networks and in determining how best to utilize feedback for other many-user channels.

Keywords: multiple access channels, feedback, capacity, coding

Statistical Tests for Block Ciphers

Richard De Moliner, Tel. No. 632 2769; demoliner@isi.ee.ethz.ch

The aim of this project is to develop testing methods for deciding, when given a black box containing a block cipher, whether that cipher is secure or not. The goal is a theory of statistical testing that would be applicable to any block cipher. The testing should in principle detect any cryptographically significant weakness with high probability. In the past year, the main issues to be confronted by such a theory have been identified. Several statistical tests have been designed and/or considered and then applied to the ciphers DES, IDEA, SAFER, RC2 and RC5 (IDEA and SAFER were developed in our laboratory). Statistical dependencies between plaintext and ciphertext have been found for DES reduced to five rounds, for IDEA reduced to one round, for SAFER reduced to two rounds, for RC2 reduced to five rounds and for RC5 reduced to five rounds.

For computationally intensive testing, software has been written to support distributed computing of such testing by utilizing idle machines in a network and by utilizing the parallel computer MUSIC from the Electronics Laboratory.
Keywords: cryptography, cryptanalysis, statistical tests

Turbocoding for M-ary Quadrature-Amplitude Modulation

Dr. T. Mittelholzer, Tel. No 934 5614; mittelholzer@isi.ee.ethz.ch

The aim of this research is to develop a new transmission scheme that is able to accommodate the transmission of the high data rates of the next generation earth observation missions of the European Space Agency (ESA) using Synthetic Aperture Radar instruments. The main part of this research focuses on the design of a powerful, virtually optimal combination of a coding and decoding scheme using turbo-coding.

To attain the required high spectral bit rates in the range of 2 to 3 bit/sec/Hz, M-ary quadrature-amplitude modulation (QAM) schemes were proposed. For these standard modulation schemes, a novel multilevel coding architecture using turbo codes was developed, which results in reduced delay and reduced complexity compared to previously known multilevel turbo-coding schemes. Essentially optimal performance of the multilevel scheme with multistage decoding can be achieved if the rates of the component codes of the multilevel scheme are chosen according to information-theoretical criteria.

Supported by: European Space Agency,

Keywords: multilevel coding, turbo coding, rate design

3.3 Completed Research Projects

HARPES Carlo

Cryptanalysis of Iterated Block Ciphers

ETH-Diss. Nr. 11625 (Referee: Prof. Dr. J.L. Massey)

Matsui's linear cryptanalysis for iterated block ciphers is first generalized by replacing his linear expressions with I/O sums. For a single round, an I/O sum is the XOR of a balanced binary-valued function of the round input and a balanced binary-valued function of the round output. A last-round attack is described and conditions for it to be successful are given. A procedure for finding effective "homomorphic" I/O sums to be used in an attack is given. A cipher contrived to be secure against linear cryptanalysis but vulnerable to this generalization of linear cryptanalysis is given. It is argued that the ciphers IDEA and SAFER are secure against this generalization of linear cryptanalysis. Statistical evidence is provided for the hypotheses of fixed-key equivalence and of fixed-key randomization, on which the success of the attack relies.

A second generalization of linear cryptanalysis is obtained by replacing an I/O sum with the *m*-ary group difference of a function of the round input and a function of the round output. A corresponding attack on an iterative cipher is developed. Several different measures for the effectiveness of *m*-ary group differences are defined and analyzed.

The previous attacks are generalized to an attack called partitioning cryptanalysis. This attack exploits a weakness that can be described by an effective partition-pair, i.e., a partition of the plaintext set and a partition of the next-to-last-round output set such that, for every key, the next-to-last-round outputs are non-uniformly distributed over the blocks of the second partition when the plaintexts are chosen uniformly from a particular block of the first partition. The last-round attack by partitioning cryptanalysis is formalized and requirements for it to be successful are stated. The success probability is approximated and a procedure for finding effective partition-pairs is formulated. The usefulness of partitioning cryptanalys is demonstrated by applying it successfully to 6-rounds of the Data Encryption Standard (DES).

The possibility to insert into a cipher a backdoor, i.e., a hidden weakness, for partitioning cryptanalysis is considered. Substitution boxes that act a linear-block transducers are defined and used to build ciphers that are easily breakable by partitioning cryptanalysis but are secure against both linear and differential cryptanalysis. A general construction of such S-boxes is given and their properties are discussed. Some techniques for finding the backdoor in an S-box are presented, and they suggest that it is impossible to hide the existence of an effective partition pair in an invertible S-box with only a small number of inputs and outputs.

Keywords: Block cipher, cryptanalysis, linear cryptanalysis, partitioning cryptanalysis, differential cryptanalysis, piling-up lemma, backdoor, trapdoor, IDEA, SAFER, DES.

ERNST Thomas

Adaptive Detektoren für die Datenübertragung über rekursive Kanäle

ETH-Diss. Nr. 11860 (Referee: Prof. Dr. A. Kälin)

In this thesis, adaptive detectors for the transmission of digital data over recursive channels are analyzed and compared to classical adaptive detectors for nonrecursive channels.

In general, classical adaptive detectors are based on the assumption of a nonrecursive channel model. For channels with a long impulse response, such a model is inappropriate with respect to the computational complexity required for data detection and channel estimation. In many practical cases, however, the channel can be modeled recursively with only few parameters, i.e. only few poles and zeroes. This property can be exploited in the detector.

Following the description of the transmission system under consideration, the optimal adaptive detector is introduced and some widely used classical suboptimal detectors for nonrecursive channels are discussed: the linear equalizer, the decision-feedback equalizer, and the decision-feedback sequence detector.

It is shown what with a simple extension these detectors can also be applied to recursive channels. This extension consists of two part: a linear prefilter designed to compensate for the channel poles and a noise feedback loop which equalizes the noise coloring caused by the prefilter. In this was, the detector has to take into account only the channel zeroes. A novel analytical comparison proves that such a detector for recursive channels will have exactly the same symbol error probability as a classical detector, provided that both detectors are based on the same number of states.

As a result of the correlation introduced by the prefilter, the use of the conventional least-mean-square (LMS) algorithm is not recommended for the adaptation of the extended detectors. The closely related LMS/Newton algorithm turns out to be more appropriate for that purpose due to its capability to decorelate the input signal. It is demonstrated that the matrix-vector multiplication contained in this algorithm can be avoided if an a-priori knowledge of the channel poles is available. In many cases this leads to a heavily simplified update of the coefficients in the numerator. Because less parameters have to be adapted, a considerable increase in adaptation speed compared to the classical detectors can be attained - most often at a reduced computational complexity.

By using a sequence detector in place of a symbol detector, a significant decrease in symbol error probability is obtained for recursive as well as for nonrecursive channels. However, the price that has to be paid for this performance gain is a delay in the availability of the final data decisions. As a further consequence, the adaptation process will suffer from this delay, too. For a general adaptation environment based on the LMS or the LMS/Newton algorithm the impact of such a delay on the stability of the adaptation is analyzed for the first time. Expressions are derived which allow to easily determine the critical adaptation step size and the steady-state excess mean-squared error.

The obtained results are verified and illustrated by means of two practically relevant reference channels.

ESTERMANN Pius

Adaptive Filters in the Frequency Domain: Analysis and Design

ETH Diss. Nr.11981 (Referee: Prof. Dr. A. Kälin)

The subject of this thesis is the analysis of a frequency-domain LMS (Least Mean square) algorithm that partitions the filter coefficients into segments, the so-called PFLMS (Partitioned Frequency-Domain LMS) algorithm. Compared to the conventional time-domain LMS algorithm, the PFLMS algorithm is computationally more efficient and less sensitive to correlated input signals. It is very promising, especially for acoustic real-time applications where a large number of coefficients have to be adapted, such as echo suppression for hands-free phones or active noise control.

The thesis starts by describing the frequency-domain filtering on which the PFLMS algorithm is based on as a multirate system. Using such a description, two filtering variants (the overlap-add and the overlap-save method) directly follow. The discrete Fourier transform (DFT) and its inverse are applied as analysis and synthesis filter bank. The efficient implementation of these two transforms by fast Fourier transforms (FFT) is the reason for the mentioned computational efficiency of frequency-domain filters. Furthermore, the DFT has the property that it decorrelates the input signal to some degree of approximation depending on the DFT length. In contrast to the optimum signal-dependent Karhunen-Loeve transformation, the DFT is not signal dependent.

To demonstrate the power of the PFLMS algorithm, we compare its tracking behavior, i.e., the ability to track changes of an unknown system, with the tracking behavior of the optimum BRLS (Block Recursive-Least-Squares) algorithm. We show that for typical acoustic applications, such as echo suppression or active noise control, the PFLMS algorithm attains the optimum tracking behavior of the BRLS algorithm if the DFT length is selected sufficiently large.

In a simplified theoretical analysis of the PFLMS algorithm we assume a perfect decorrelation of the input signal by the DFT. By applying the so-called independence theory we are able to describe the transient behavior of the mean parameter error and the excess MSE (Mean Squared Error) as simple first order difference equations. To investigate the influence of segment-dependent step sizes, the analysis has been extended. Assuming small step sizes, we write the excess MSE as a sum of decoupled first-order difference equations. We show that the final excess MSE is proportional to the sum of the step sizes. Finally, an exact theoretical analysis takes the correlation of the input signal after the DFT into consideration. Applying again the mentioned independence theory, we again obtain a weighted sum of first-order difference equations. We are able to show qualitatively that the PFLMS algorithm attains the optimum convergence rate if the MSE contributions of the slow eigen oscillations have initial conditions that lie below the given final excess MSE.

The realization of a hands-free phone with an echo compensator based on an optimally designed PFLMS algorithm concludes this thesis. It incorporates a new adaptive segment-dependent step-size control that adapts to the different time-varying system modes. For an echo impulse response with 3500 coefficients, we obtain an increase in the critical gain of more than 14dB.

Keywords: DFT, block processing, partitioned frequency-domain LMS algorithm, optimum tracking behavior, block RLS algorithm, analysis of the convergence rate, hands-free phone.

WALDVOGEL Christian

On the Nature of Authentication Protocols

ETH-Diss. Nr. 11941 (Referee: Prof. Dr. J.L. Massey)

A framework for the study of authentication protocols is proposed. This framework is intended to serve as a tool for investigating the security of authentication protocols in a unified manner and can be applied to a wide variety of authentication protocols. An authentication protocol is de- fined as a protocol in the course of whose execution by two distinct users, one being the "prover" and the other the "verifier", the verifier acquires a "valid" message, one or more component of which is determined by the prover and the remaining ones (if any) by the verifier. The acquired message is said to be "valid" if it belongs to some specified set of messages.

This set of valid messages constitutes one of the two essential parameters specifying an authentication protocol.Upon acquiring the message andverifying its validity, the verifier concludes that the message is "authentic". The "authenticity" of the acquired message refers both to its "sender" and to the "manner" according to which it was formulated by the prover and the verifier.

This protocol-specific "authenticity" is expressed in terms of a "predicate", which constitutes the other essential parameter of an authentication protocol.

An "attack" against an authentication protocol is defined as a second protocol involving at least two users, one being the "enemy" and another the "victim", in the course of whose execution the victim proceeds in precisely the same way as if he or she were executing the authentication protocol as a verifier with some purported prover, and thus acquires a message and verifies its validity.

The aim of the enemy is to "force" the victim into making an erroneous conclusion of authenticity, i.e., to force the victim into concluding that the acquired message is authentic when in fact it is not. The execution of an attack is "successful" if the victim makes an erroneous conclusion with respect to the authenticity of the acquired message, and is "unsuccessful" otherwise. An attack is then defined as "benign" if the pro-bability of a successful execution is negligibly small, and as "malignant" otherwise. The "feasibility" of an attack, i.e., whether it is practicable to execute the protocol specifying the attack, is also treated. Moreover, an authentication proto- col is defined as "insecure" against a particular attack if that attack is both malignant and feasible, and as "secure" otherwise.

Several authentication protocols are studied in order to illustrate the proposed framework. The very simple "password protocol" is considered first. Both "explicit and implicit digital signature protocols" based on secret-key cryptographic primitives (e.g., on a block cipher or on a message authentication code (MAC) and on public-key cryptographic primitives (e.g, on the Rivest-Shamir-Adleman (RSA) trapdoor one-way function, on the El Gamal public-key signature scheme or its variants, the scheme suggested by Agnew, Mullin and Vanstone and the Digital Signature Standard (DSS) are also considered.

The pros and cons of an "identity-based versus a certificate-based explicit signatureprotocol" are discussed. As examples, an identity-based protocol proposed by Shamir in~1984 and a simplified version of the certificate-based

ISO~9594-8 standard are described. It is shown that time can be easily integrated into the proposed framework by introducing a "timestamp-based explicit signature protocol." Two types of interactive authentication protocols are considered, namely "challenge-response protocols" and "commitment-challenge-response protocols."

MUELLER Daniel

Hybrid Echo Cancellation with Application in Digital Data Transmission on Copper Wires

ETH-Diss. Nr. 11957 (Referee: Prof. Dr. A. Kälin)

This thesis investigates several aspects of echo cancellation in the field of fast digital data transmission on copper wires.

Two of the major problems in realizing*"high bit-rate digital subscriber line"* (HDSL) modems are the complexity of the echo canceler and the high dynamic range of the A/D converter. In this thesis, possible solutions to these problems are suggested and investigated. Measurements of echo impulse responses on real test lines serve as a starting point of this work.

In contrast to conventional FIR echo cancelers, a combination of FIR and IIR filters is proposed. By introducing "a priori" knowledge about the relevant test loop environment in the IIR part, the total number of weights to be adapted can be reduced significantly. This leads to a reduction of hardware cost and, if an appropriate filter structure is used for the IIR part, to a faster adaptation. It is shown that orthonormal lattice filters have this property. A synthesis method is presented. Methods of distributed arithmetic are used to realize the lattice filter and its adaptation algorithm. Noise considerations are used to compute the relevant word lengths. This bit-serial based processing scheme is then compared to alternative realizations.

The transmit path of an HDSL modem needs a highly linear D/A converter. A memory based compensation filter (MBCF) is used to reduce these linearity requirements. Realizing the FIR part of the echo canceler as an MBCF allows for a partial compensation of the D/A nonlinearities. The remaining error power is calculated. The different convergence behavior, compared to a true FIR filter, is further analyzed.

One of the most critical design parameters in designing HDSL modems is the resolution of the A/D converter. Analog precancellation is a method to reduce this resolution. It needs an additional D/A converter. It is proposed to compensate its nonlinearities using a simple MBCF. A major contribution of this thesis is a detailed analysis of the joint convergence behavior of this MBCF together with the echo canceler. It is shown that a joint adaptation cannot meet the speed requirements of the specified start-up phase. Thus, a calibration phase is necessary. Measurements with a prototype built at Siemens Schweiz AG confirm the analysis results of the analysis.

The different new concepts for HDSL echo cancelation proposed in this work have a potential to reduce hardware cost significantly. Which of these ideas should

be implemented depends, among others, on integration technology and can only be decided by considering a concrete realization.

Keywords: DSL, echo cancellation, adaptive filters, nonlinear filters, memory based compensation schemes, lattice filters, distributed arithmetic

3.4 Completed Dissertations

HARPES Carlo — Cryptanalysis of Iterated Block Ciphers

ETH Diss. Nr. 11625
Referee: Prof. Dr. J.L. Massey
Co-referee: Prof. U. Maurer

ERNST Thomas — Adaptive Detectors for the Data Transmission over Recursive Channels

ETH Diss. Nr. 11860
Referee: Prof. Dr. A. Kälin
Co-referee: Dr. E. Eleftheriou, IBM

WALDVOGEL Christian — On the Nature of Authentication Protocols

ETH Diss. Nr. Nr. 11941
Referee: Prof. Dr. J.L. Massey
Co-referee: Prof. Refik Molva

MUELLER Daniel — Hybrid Echo Cancellation with Application in Data Transmission on Copper Wires

ETH Diss. Nr. 11957
Referee: Prof. Dr. A. Kälin
Co-referees: Prof. Dr. G.S. Moschytz
Dr. G. Cherubini, IBM

ESTERMANN Pius — Adaptive Filter im Frequenzbereich: Analyse und Entwurfsstrategie

ETH-Diss. Nr. 11981
Referee: Prof. Dr. A. Kälin
Co-referee: Prof. Dr.-Ing. E.Hänsler, TU Darmstadt

3.5 Internal Report

9601	R. Seiler M. Schenkel F. Eggimann	Off-line Cursive Handwriting Recognition compared with On-line Recognition

4. Congresses, Meetings and Committees

4.1 Congress Organization

Prof. Moschytz

Member of the Scientific Committee for EUSIPCO, Brussels.

International Zurich Seminar on Digital Communications: Steering Committee (as Chairman of the IEEE Switzerland Chapter on Digital Communications).

Member of ESTA (European Scientific and Technical Assembly, Brussels).

Member of Board of Governors, IEEE Circuits and Systems Society.

Organization of 1st ETHZ-EPFL Summer school on Linear, Nonlinear, and Adaptive Circuits, Systems and Signal Processing together with Prof. M. Hasler, CIRC EPFL and Prof. L.O.Chua, UC Berkeley.

Member of Board of Governors, IEEE Circuits and Systems Society.

Prof. Kälin

Organization of 1st ETHZ-EPFL summer school on Linear, Nonlinear, and Adaptive Circuits, Systems and Signal Processing, entitled "Introduction to Linear and Nonlinear Adaptive Signal Processing", together with Prof. M. Hasler, CIRC EPFL and Prof. L.O.Chua, UC Berkeley.

Prof. Massey

Organizing Committee, 1996 Isaac Newton Institute on Cryptography Cambridge, England.

Int. Advisory Committee, IEEE ISSSTA'96, Mainz, Germany.

Organizing Committee, 1996 Information Theory Workshop, Haifa, Israel.

Advisory Board, MMT'96, Paris, France.

Program Committee, Fast Software Encryption, 1997 4th Int. Workshop, Haifa, Israel.

Program Committee, 1997 IEEE Int. Symp. on Information Theory, Ulm, German.

Program Committee, CRYPTO'97, Santa Barbary, USA.

Advisory Board, SSC 97, Lausanne, Switzerland.

Prof. Rathe

Chairman, Organizing Committee for the Congress DAGA 1998 in Zurich.

4.2 Participation in Congresses and Meetings

Group: Analog and Digital Signal Processing

Moschytz George S.	Research Stays with AT&T Bell Labs, Middletown, NJ., USA, 14.2.-13.3.96 and 11.8.-19.9.96.
Moschytz George S. Mirzai Bahram Helfenstein Markus Lím Drahoslav	ISCAS'96, Atlanta, USA, 12.-15.5.96
Moschytz George S. Hänggi Martin Lím Drahoslav Mirzai Bahram	CNNA-96, Sevilla, Spain, 24.-26.6.96.
Moschytz George S.	ICECS'96, Rhodos, 13.-16.10.96
Moschytz George S.	Technion - Israel Institute of Technology, Haifa, Israel, 21.-23.10.96
Poncet Andreas	NICROSP'96, Venice, Italy, 19.-24.8.96.
Helfenstein Markus	European Workshop on Multirate Digital Signal Processing and Applications, Hamburg, 20.-21.5.96.
Helfenstein Markus	Low Power Suite, Zurich, 30.10.96.

Group: Adaptive Systems

Kälin August	Fourth International Congress on Sound and Vibration, St. Petersburg, Russia, 24.-27.6.96.
Kälin August Poncet Andreas	ETHZ-EPFL Summer School on Linear and Nonlinear AdaptiveSignal Processing, Zurich, 15.- 19.7.96.
Estermann Pius Kälin August	EUSIPCO-96, Triest, Italy, 9.-13.9.1996.

Group: Digital Information Theory

Reddy Madhu Recognition Schenkel Markus	13th International Conference on Pattern Vienna, Austria, 25.-29.8.96.
Reddy Madhu Schenkel Markus	Fifth International Workshop on Frontiers in Handwriting Recognition, Colchester, England, 31.8.-5.9.96.
Reddy Madhu	Berne Technology Forum 1996, Berne, 17.10.96.

Group: Applied Acoustics

Rathe Eric J.	Computer Graphics, Zurich, 1.2.96.
Rathe Eric J.	DAGA Congress, Bonn, 26.-28.2.96.
Rathe Eric J. Stettbacher Jürg	EUROPEAN-FORUM ACUSTICUM, Antwerp, 1.-4.4.96.
Rathe Eric J.	GISWISS-Meeting, Morges, 16.-17.4.96.
Rathe Eric J.	Annual Acoustical Standards Meeting, Zurich, 23.4.96.
Rathe Eric J.	Swiss Acoustical Society Regional Meeting, Vevey, 14.6.96.
Rathe Eric J.	Motorway Inauguration, Schaffhausen, 15.8.96.
Rathe Eric J. Stettbacher Jürg	Swiss Acoustical Society Annual Meeting, Lucerne, 7.-8.11.96.
Stettbacher Jürg	DSP Germany, Munich, 1.-2.10.96.

Group: Digital Information Theory

Massey James L.	University of Erlangen, Germany, 31.1.96.
Massey James L.	1996 Int. Zurich Seminar on Digital Communications, Zurich, Switzerland, 19.-23.2.96.
Massey James L.	Isaac Newton Inst. for Mathematical Sciences, Univ. of Cambridge, and Royal Holloway, Univ. of London, UK, 12.2.-16.2.96 and 21.2.-8.3.96.
Massey James L. Mittelholzer Th.	Math. Forschungsinstitut Oberwolfach, Germany, 18.2.-21.2.96.
Massey James L.	Centennial Symposium, Future Trends in Electrical Engineering: Education, Research, and Technology, Univ. of Notre Dame, USA, 26.3.96.
Massey James L.	Univ. of Michigan, Ann Arbor, USA, 2.4.96.
Massey James L.	EUROCRYPT'96, Zaragoza, Spain,12.-16.5.96.
Massey James L.	MMT'96, ENST, Paris, France, 20.-22.5.96.
Massey James L.	22nd Marconi Int. Fellowship, London, UK, 3.-7.6.96.
Massey James L.	ETT Editors' Meeting, Milano, Italy, 17.6.96.

Massey James L Sayir Jossy	1996 IEEE Information Theory Workshop, Haifa, Israel, 9.-13.96.
Massey James L.	UBC/EPFL Workshop on Multimedia Networking, Lausanne, Switzerland,11.-12.7.96.
Massey James L.	1st ETHZ-EPFL Summer School on Linear, Nonlinear, and Adaptive Circuits, Systems, and Signal Proc., Zurich, Switzerland, 15.-19.7.96.
Massey James L	Security in Communication Networks, Amalfi, Italy, 16.-17.9.96.
Massey James L. Loher Urs	ISSSTA'96, Mainz, Germany, 22.-25.9.96.
Massey James L.	INRIA, Rocquencourt, France, 8.-10.10.96.
Massey James L.	Swiss Computer Science Conference, Zurich, Switzerland, 22.-23.10.96.
Massey James L.	EPFL - SSC Seminar, Lausanne, Switzerland, 7.11.96.
Massey James L.	ICCS'96 and ISPACS'96, Singapore, 25.-19.11.96.
Massey James L. Krämer Gerhard Loher Urs Sayir Jossy	Winter School on Coding and Info. Th., Mölle, Sweden, 15.-18.12.96.
Keusch Beat	LESIT Final Convention, Berne Switzerland, 16.1.96.
Keusch Beat	ACTS Magic WAND Meeting, Ulm, Germany, 22.-24.1.96.
Keusch Beat	ACTS Magic WAND Meeting, Zurich, Switzerland, 26.-28.2.96.
Keusch Beat	ACTS Magic WAND Meeting, Leiden, The Netherlands, 17.-19.4.96.
Keusch Beat	ACTS Magic WAND Meeting, Athens, Greece, 21.-24.5.96.
Keusch Beat	ACTS Magic WAND Meeting, Lancaster, UK, 3.-5.7.96.
Keusch Beat	Wireless ATM Workshop, Espoo, Finland, 2.-3.9.96.
Keusch Beat	ACTS Magic WAND Meeting, Helsinki, Finland, 4.-5.9.96.
Keusch Beat	ETH Magic WAND Meeting, Zürich, Switzerland, 19.9.96.

Keusch Beat	ACTS Magic WAND Meeting, Nice, France, 14.-16.10.96.
Keusch Beat	ACTS Magic WAND Meeting, Zürich, Switzerland, 16.-18.12.96.
Krämer Gerhard Loher Urs	ACTS FRAMES A10 Meeting, Paris, France, 9.-10.1.96.
Krämer Gerhard	ACTS FRAMES A10 Meeting, Munich, Germany, 2.2.96.
Krämer Gerhard	ACTS FRAMES CT-SYS Meeting, Göteborg, Sweden, 12.-13.3.96.
Krämer Gerhard	ACTS FRAMES A10 Meeting, Kaiserslautern, Germany, 18.-19.4.96.
Krämer Gerhard	GLOBECOM'96, London, England,19.-22.11.96.
Loher Urs	COST-231, Belfort, France, 24.-26.1.96.
Loher Urs	ETSI, Nice, France, 16.12.96
Mittelholzer Thomas	Lund University, Lund Sweden, 20.3.96.
Mittelholzer Thomas	ATS in Cryptography, Engelberg, Switzerland, 10.-12.9.96.
Mittelholzer Thomas Sayir Jossy	Int. Seminar on Coding Theory and Combinatorics, Thahkadzor, Armenia, 6.-11.10.96.

4.3 Service Activities and Society Memberships

Prof. Moschytz

Member of the Swiss Section of the IEEE

Chairman of the IEEE Switzerland Chapter on Digital Communication Systems

Member of the Editorial Board of the "International Journal of Circuit Theory and Applications" (Publ. John Wiley & Sons, Chichester, GB)

Member of the European Editorial Board of the journal: "Journal of Circuits, Systems and Computers," Scientific Publ. Co., Singapore, New Jersey, London, Hongkong

Member of the Editorial Board of the International Journal "Analog Integrated Circuits and Signal Processing", Kluwer Academic Publishers, Norwell MA, USA

Member of the international Editorial Board of the newly appearing "Annales des télécommunications", Issy-les-Moulineaux, France

Swiss Committee of URSI, Member and Deputy of Commission C

Präsident des AGEN-Rates (Arbeitsgemeinschaft für elektr. Nachrichtentechnik) der Stiftung Hasler-Werke, Berne

Fellow of the IEEE, New York

Member, Swiss Electrical Engineering Society

Member, Swiss Academy of Engineering Sciences

Member of ESTA (European Science and Technology Assembly)

Member of the Board of Governors; IEEE Circuits and Systems Society

Chairman Selection Committee IEEE Van Valkenburg Award

External Ph.D. Examiner, Swiss Federal Institute of Technology, Lausanne

Prof. Kälin

External Ph.D. Examiner, Swiss Federal Institute of Technology, Lausanne

Prof. Massey

Co-Editor, Book Series: Communications and Control Engineering, Springer-Verlag

Member, Advisory Board, Lecture Notes in Control and Information Sciences, Springer-Verlag

Member, Editorial Board, European Transactions on Telecommunication.

Member, Editorial Board, Journal of Information and Optimization Sciences

Member, Editorial Board, Journal of Cryptology

Member, Editorial Board, AAECC Journal of Applicable Algebra in Engineering, Communication and Computing

Fellow of the IEEE New York

Member, Swiss Academy of Engineering Sciences

Member, Swiss Electrical Engineering Society

Member, IEEE Education Medal Committee

Member, Board of Governors, IEEE Information Theory Society

Member, U.S. National Academy of Engineering

Member, European Academy of Arts and Sciences

Member, International Asociation for Cryptologic Research

Honorary Member of the Hungarian Academy of Sciences

Member, Selection Committee of the Marconi Award

Member, Scientific Advisory Board, THESEUS Institute for Advanced Studies in Communications Strategy, Sophia Antipolis, France

Member, ComSoc Awards Board for 1996-98

Member, Board of Electors, Chair in Communications, Univ. of Cambridge, UK

Member, Election Committee, Professorships in Communications, EPFL

Member, Election Committee, Professorship in Computer-Vision, ETHZ

External Ph. D. Examiner, INRIA, Rocquencourt

Prof. Rathe

Member, Federal Oberschätzungskommission

Consultant, Organization for Economic Cooperation and Development, (OECD) Paris

Member, Eidg. Kommission für Lärmgrenzwerte im Rahmen des Umweltschutzgesetzes

Fellow of the Acoustical Society of America

Honorary President, Swiss Acoustical Society (SGA)

Member, Audio Engineering Society

Member, Société Française d'Acoustique

Member, Swiss Electrical Engineering Society

Member, Swiss Society of Engineers and Architects (SIA)

Member, Swiss Society of Consulting Engineers (ASIC)

Honorary President, Swiss Acoustical Society (SGA)

4.4 Presentations by Institute Members

Groups: Analog and Digital Signal Processing and Information Technology

Poncet Andreas	"On the Design of Nonlinear Learning Systems by Statistical Inference", Institut Dalle Molle d'Intelligence Artificielle Perceptive, IDIAP Martigny, 16.6.96.
Poncet Andreas	"Nonlinear Adaptive Signal Processing", ETHZ-EPFL Summer School on Linear and Nonlinear Adaptive Signal Processing, Zurich, 17.7.96.
Poncet Andreas	"Selecting Inputs and Measuring Nonlinearity in System Identification", NICROSP'96, Venice, 21.8.96.
Poncet Andreas	"Asymptotic Probability Density of the Generalization Error", NICROSP'96, Venice, 22.8.96.
Poncet Andreas	"Design of Models for Signals and Systems", Sulzer Innotec, Winterthur, 19.12.96.
Mirzai Bahram	"On the Robustness of CNNs and a Design Approach for Robust Templates", ISCAS'96, Atlanta, USA, 11.5.96.
Mirzai Bahram	"Robust CNN Templates: Theory and Simulations", CNNA'96, Sevilla, Spain, 26.6.96.
Helfenstein Markus	"Design Techniques for HDTV SI Decimators", European Workshop on Multirate Digital Signal Processing and Applications, Hamburg, 21.5.96.
Lím Drahoslav	"Cellular Neural Networks in Signal Processing", Swiss Nat. Science Foundation, SP Informatics Programme Closing Conference, EPFL Lausanne, 20.3.96.
Lím Drahoslav	"Robust CNN Templates: Theory and Simulations", CNN'96, Seville, Spain, 26.6.96.

Group: Adaptive Systems

Kälin August	“An Adaptive Feedforward A-Weight-Optimized Controller for the Active Reduction of Stochastic Sound“, ICSE’96, St. Petersburg, Russia, 24.-27.6.96
Kälin August	“Partitioned Frequency-Domain Adaptive FIR Filters, Linear Adaptive IIR Filters“, 1st ETHZ-EPFL Summer School on Linear, Nonlinear, and Adaptive Circuits, Systems and Signal Processing, Zurich, 15.-19.7.96.
Wyrsch Sigi	“Untersuchung von Dynamikkompressoren für Hörgeräte“, Phonak AG, Stäfa, 12.7.96.

Group: Applied Acoustics

Stettbacher Jürg	“Audiometry to Evaluate Binaural Hearing“, Forum Acousticum, Convention of the European Acoustics Association EAA, Antwerp, Belgium, 1.-4.4.96.
Stettbacher Jürg	“Digital generierte, bewegte virtuelle Schallquellen“, DSP Munich, Germany, 1.-2.10.96.

Group: Digital Information Theory

Massey James L.	"Coding for Multiple-Access Channels", Electrical Engr. Seminar, Univ. Erlangen, Germany, 31.1.96.
Massey James L.	"Linear Complexity of Sequences with Arbitrary Period and a Generalized Discrete Fourier Transform", Math. Seminar, Royal Holloway, Univ. of London, UK, 6.3.96.
Massey James L.	"Can Electrical Engineering Education Survive another Century?", Guest Speaker, Electrical Engr. Centennial Symposium, Univ. of Notre Dame, USA, 26.3.96.
Massey James L.	"Shannon and His Tricks", Univ. of Michigan, Ann Arbor, USA, 2.4.96.
Massey James L.	"The Difficulty with Difficulty", IACR Distinguished Lecture, EUROCRYPT'96, Zaragoza, Spain, 12.-16.5.96.
Massey James L.	"Watch the Received Chip!", Featured Talk, Workshop on Multicaccess, Mobility and Teletraffic for Personal Communications, Paris, France, 20.-22.5.96.
Massey James L.	"The Difficulty with Difficulty", IEEE Information Theory Workshop, Haifa, Israel, 9.-13.6.96.

Massey James L.	"Multimedia Networking - A Hacker's Paradise?", EPFL-UCB Workshop on Multimedia Networking, Lausanne, Switzerland, 11.-12.7.96.
Massey James L.	"Some Remarks on Triple DES", Invited Talk, Security in Communication Networks, Amalfi, Italy, 16.-17.9.96.
Massey James L.	"Is the Choice of Spreading Sequences Important?", IEEE 4th Int. Symposium on Spread Spectrum Techniques & Applications, Mainz, Germany, 22.-25.9.96.
Massey James L.	"Coding Theory: From Algebra to Algorithms", Invited Talk, Swiss Computer Science Conference, ETH Zurich, Switzerland, 22.-23.10.96.
Massey James L.	"Stream Ciphers from Block Ciphers: Pitfalls and Cures", EPFL - SSC Seminar, Lausanne, Switzerland, 7.11.96.
Massey James L.	"From Bits to Bytes in Batches", Keynote Address, ICCS'96 and ISPACS'96 Singapore, 25.-29.11.96.
Massey James L.	"A Fourier Transform of Length Np^m over fields of Characteristic p, with Applications to Coding and Cryptography", Invited Talk, Winter School on Coding and Information Theory, Mölle, Sweden, 15.-18.12.96.
Keusch Beat	"High-Speed Adaptive Coded Modulation for Wireless ATM", ACTS Magic WAND Meeting, Leiden, The Netherlands, 18.4.96.
Keusch Beat	"Error Control Concepts and Automatic Repeat Request Schemes with Discard Mechanism for Magic WAND", ETH Magic WAND Meeting, 19.9.96.
Krämer Gerhard	"A Comparison of Demodulation Techniques for Code Time Division Multiple Access", Globecom '96, London, England, 19.11.96.
Krämer Gerhard	"Feedback Strategies Suggested by Horstein's Strategy", Winter School on Coding and Info. Th., Mölle, Sweden, 17.12.96.
Loher Urs	"Code Time Division Multiple Access: CDMA and TDMA - A Marriage Made in Heaven", ETSI, Nice, France, 16.12.96.
Loher Urs	"Can Mixing of Enabled Sets Increase the Throughput of Collision-Resolution Algorithms?", Winter School on Coding and Info. Th., Mölle, Sweden, 17.12.96.
Mittelholzer Th.	"Fast Maximum-Likelihood Decoding of Group Codes from Finite Reflection Groups", Math. Research Inst, Oberwolfach, Germany, 18.- 24.2.96.

Mittelholzer Th.	"Minimality Tests for Encoding Matrices Using Canonical Trellises", Invited Talk, Lund University, Lund, Sweden, 20.3.96.
Mittelholer Th.	"Minimal-Trellis Decoding Versus Permutation Decoding of Permutation Modulation Codes", Int. Seminar on Coding Th.and Comb., Thahkadzor, Armenia, 6.-11.10.96.
Sayir Jossy	"Conditional Recency-Ranking for Source Coding", 1996 Info.Th. Workshop, Haifa, Israel, 9.-13.6.96.
Sayir Jossy	"Ordering Memoryless Source Alphabets Using Competitive Lists", Int. Seminar on Coding Th. and Combinatorics, Tsahkadzor, Armenia, 6.-11.10.96.
Sayir Jossy	"A Method for Source Coding Using Conditional Competitive Lists", Winter School on Coding and Info. Th., Mölle, Sweden, 15.-18.12.96.

4.5 Organization of Lectures, Seminars, and Colloquia

Collquium Speakers for the Colloquium “Electronics and Communications“ were:

Invited by Prof. Moschytz:

07.02.96	**Prof. Y. Z. Zeevi,** Technion - Israel Institue of Technology, Haifa, Israel “Biologically-Based Localized Techniques of Linear and Processing Images“.
18.01.96	**Prof. Ch. Toumazou,** Imperial College London “Towards a New Generation of Analogue IC Design Architectures“.
22.04. - 25.04.96	**Prof. D. Graupe,** Northwestern University, Evanston, USA Short course on “Wavelets for Signal Processing“.
21.05.- 12.06.96	**Prof. L. Chua,** University of California, Berkeley, USA Course on “Cellular Neural Networks: Foundations and Primer“.
08.07.96	**Prof. J. Katzenelson,** Technion - Israel Institute of Technology, Haifa, Israel “A Network Charge-oriented MOS Transistor Model“.
18.07. - 19.07.96	**Prof. B. Widrow,** Stanford University, Stanford, USA “Adaptive Inverse Control“, “Various Aspects of Quantization Noise“.
19.07.96	**Prof. M. Hasler,** CIRC EPFL, Lausanne “Synchronization of Chaotic Systems and Applications“.
19.07.96	**Prof. L. Chua,** University of California, Berkeley, USA “Exploiting Chaos, Nonlinear dynamics, and Adaptive Control for Information Technology“.
10.10.96	**J. Barreiro da Silva,** Instituto Superior Technico, IST, Portugal.
05.11.- 12.11.96	**Prof. A. Arbel,** Technion - Israel Institute of Technology, Haifa, “A Guide to the Analysis and Design of Feedback Stabilized Analog Circuits“.
05.12.96	**Prof. A. Carlosena,** Universidad Publica de Navarra, Pamplona, Spain “Analog Universal Active Device: Theory, Design and Applications“.
16.12.96	**Prof. P.P. Vaidyanathan,** California Institute of Technology, Pasadena, “Optimal Orthonormal Subband Coders“.

Invited by Prof. Massey:

08.01.96 **Prof. Dr. Ch. Schlegel**, University of Texas at San Antonio, USA:
"Projection Receivers: A Class of Linear Multiple-User Receivers for Coded CDMA Systems".

15.03.96 **Dr. V. Sidorenko**, Inst. for Info. Trans. Problems, Russian Academy of Sciences, Moscow, Russia:
"On Minimal Trellises of Linear Codes".

Invited by Prof. Rathe

17.01.96 **Mr. R. Johnson,** Artec Consultants, New York
“Acoustic Concepts for the Concert Hall in Lucerne“.

31.01.96 **PD Dr. M. Sigrist,** Quantenelektronik ETH, Zurich
“Grundlagen und Anwendungen der Photoakustik“.

24.04.96 **Dr. H. Bloemhof,** Rieter Automotive Systems AG, Brüttisellen
“Aktuelle Verfahren zur Berechnung der Akustik in Automobilen“.

29.05.96 **Dr. M. Heckl,** Keele University, England
“Kurvenquietschen bei Eisenbahnen“.

19.06.96 **Prof. Dr. M. Ochmann,** Techn. Fachhochschule, Berlin
“Abstrahlung und Streuung von Schall: Vom Würfel zum Propeller“.

13.11.96 **Dr.-Ing. Ch. Maschke,** Inst. Techn. Akustik, TU Berlin
“Die Auswirkungen von nächtlichem Verkehrslärm auf Schlaf und Gesundheit“.

18.12.96 **Dipl. Ing. B. Barsikow,** Ingenieurbüro akustik-data, Berlin
“Schallquellenlokalisation an Eisenbahnfahrzeugen mittels Arraytechnik“.

5. Publications

Group: Analog and Digital Signal Processing

Poncet Andreas Moschytz George S.	"Selecting Inputs and Measuring Nonlinearity in System Identification", Neural Networks for Identificaiton, Control, Robotics, and Signal/Image Processing", pp. 2-10, IEEE Computer Society, 1996.
Poncet Andreas	"Asymptotic Probability Density of the Generalization Error", Neural Networks for Identification, Control, Robotics and Signal/Image Processing", pp. 66-74, IEEE Computer Society, 1996.
Mirzai Bahram Moschytz George S.	"Upper Bounds for Robustness of CNN Templates and a Design Approach for Robust Templates", Proceedings of ISCAS'96, Atlanta, Vol. 3, pp. 284-287..
Mirzai Bahram Lím Drahoslav Moschytz George S.	"Robust CNN Templates: Theory and Simulations", Proceedings of CNNA'96, Sevilla, pp. 393-398.
Helfenstein Markus José E. Franca Moschytz George S.	"Design Techniques for HDTV Swiched-Current Decimators", Proceedings IEEE Int. Symposium on Circuits and Systems, Atlanta, USA, pp. 195-198, May 1996.
Helfenstein Markus José E. Franca Moschytz George S.	"Design techniques for HDTV SI Decimators", Proceedings Europen Workshop on Multirate Digital Signal Processing and Applications, Hamburg, Session: Image and Video Coding II, March 1996.
Schaerer Thomas	"Spezielle Spannungsversorgung fuer empfindliche und rauscharme Mess- und Audioschaltungen", MEGALINK Nr. 6, pp. 2, April 1996.

Group: Adaptive Systems

Kälin August Cachin D. Egger F.	"An Adaptive Feedforward A-Weight-Optimized Controller for the Active Reduction of Stochastic Sound, Proceedings ICSE'96, St. Petersburg, Russia, 1996, pp. 1005-1012.
Estermann Pius Kälin August	"A Hands-Free Phone System Based on a Partitioned Frequency-Domain Adaptive Echo Canceler", Proceedings EUSIPCO'96, Triest, Italy, pp. 1131-1134.

Group: Applied Acoustics

Stettbacher Jürg	"Audiometry to Evaluate Binaural Hearing", Acta Acustica, Vol. 82, Suppl. 1, p. S217, Jan./Feb. 96.

Group: Digital Information Theory

Massey James L.	"Causal Interpretations of Random Variables" (in Russian), Problemy Peredachi Informatsii, Vol. 32, No. 1, pp. 131-136, January-March, 1996.
Ganz Jürg	"Binary Representations of Finite Fields and Their Application to Complexity Theory", Finite Fields & their Appl., Vol 2, pp. 348-368, 1996.
Massey James L. Serconek S.	"Linear Complexity of Periodic Sequences:A General Theory", in Advances in Cryptology - CRYPTO'96 (Ed. N. Koblitz), Lecture Notes in Computer Science No. 1109. New York: Springer, 1996 pp 358-371.
Hiltgen Alain P. Paterson Kenneth G. Brandestini M.	"Single-Track Gray Codes", IEEE Trans. Info.Th., Vol. IT-42, pp.1555-1561, Sept.1996.
Loeliger Hans-A. Mittelholzer Thomas	"Convolutional Codes over Groups", IEEE Trans. in Info. Th.,Vol.41, No. 6, p. 1660-1686, Nov. 1996.
Mittelholzer Thomas Lahtonen J.	"Group Codes Generated by Finite Reflection Groups", IEEE Trans, in Info. Th.,Vol.42,No. 2, pp. 519-528, March 1996.
Mittelholzer Thomas	"Minimal-Trellis Decoding Versus Permutation Decoding of Permutation Modulation Codes", Proc.Int.Seminar on Coding Theory and Combinatorics, Thahkadzor, Armenia, Oct. 6-11, 1996.
Ruprecht Jürg Loher Urs Krämer Gerhard	"Performance, Service Provision and Implementation Issues of Cellular Code Time Division Multiple Acdess", Proc. ISSSTA'96, Mainz. Germany, pp. 344-350.
Krämer Gerhard Loher Urs Ruprecht Jürg Jung Pierre	"A Comparison of Demodulation Techniques for Code Time Division Multiple Access", Proc. Glocecom'96, London, England, pp. 525-529.

6. Guests, Visitors

6.1 Activities of Academic Guests at the Institute

Guests of Prof. Moschytz:

Prof. Ch. Toumazou,
Information Engineering Section, Dept. of Electrical Engineering, Imperial College, London, England
worked together with Prof. Moschytz and held a lecture "Towards a New Generation of Analogue IC Design Architectures". 17.01. - 19.01.96

Prof. D. Graupe,
Northwestern University, Evanston, USA
held short course on "Wavelets for Signal Processing". 25.04. - 05.05.96

Prof. L. Chua,
University of California, Berkeley, USA
Course on "Cellular Neural Networks;
Foundations and Primer" and interacted with various
ISI researchers in the field of non-linear networks and CNN's. 15.05. - 15.07.96

Prof. H. Reddy,
California State University, Long Beach, USA
worked togehter with Prof. Moschytz in the field of 25.03. - 03.04.96
analog and digital signal processing and held various 17.06. - 31.07.96
colloquia on the application of the Delta Transformation 28.11. - 07.12.96
for CNNs.

Prof. J. Katzenelson,
Technion - Israel Institute of Technology, Haifa, Israel
worked together with Prof. Moschytz and held 2 lectures on
"A Network Charge-oriented MOS Transistor Model" and on
"Integrated Circuits and parallel Processing". 03.07. - 18.07.96

Prof. A. Arbel,
Technion - Israel Institute of Technology, Haifa, Israel
worked together with various ISI researchers on current-mode analog circuits for high frequency applications and gave a series of lectures on "A Guide to the Analysis and Design of Feedback Stabilized Analog Circuits". 28.10. - 27.11.96

Prof. A. Carlosena,
Universidad Publica de Navarra, Pamplona, Spanien
worked together with analog circuit group; gave a

colloquium on “Analog Universal Active Device: Theory, Design and Applications“. 01.12. - 07.12.96

Guests of Prof. Massey:

Prof. X. Lin, Beijing University of Posts & Telecommunications, Beijing, China
worked with Dr. Mittelholzer on the improvement of TURBO decoding methods, with Prof. Massey on the cryptanalysis of the Perigee cipher, and with Mr. Keusch on multiple-access systems for mobile communications. 01.01. - 31.12.96

St. Ortman,
Univ. of Notre Dame, Notre Dame, USA
worked, as an undergraduate research trainee, with Mr. Sayir on data compression techniques, programming several algorithms in C and testing their performance. 20.05. - 27.07.96

7. Honors and Awards

Moschytz George S. Recipient of the 1996 Society Education Award, IEEE Circuits and Systems Society.