Hideki Imai Ronald L. Rivest
Tsutomu Matsumoto (Eds.)

Advances in Cryptology – ASIACRYPT '91

International Conference on the
Theory and Application of Cryptology
Fujiyoshida, Japan, November 11-14, 1991
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 6980
Vincenz-Priessnitz-Straße 1
D-76131 Karlsruhe, Germany

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Hideki Imai
Tsutomu Matsumoto
Division of Electrical and Computer Engineering, Yokohama National University
156 Tokiwadai, Hodogaya, Yokohama 240, Japan

Ronald L. Rivest
Massachusetts Institute of Technology, Laboratory for Computer Science
Cambridge, Massachusetts 02139, USA

CR Subject Classification (1991): E.3-4, D.4.6, G.2.1, C.2.0, K.6.5

ISBN 3-540-57332-1 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57332-1 Springer-Verlag New York Berlin Heidelberg

Printed in Germany

Typesetting: Camera-ready by author
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

Preface

ASIACRYPT '91 was the first international conference on the theory and application of cryptology to be held in the Asian area. It was held at Fujiyoshida, Yamanashi, Japan, overlooking beautiful Mt. Fuji, from November 11 to November 14, 1991.

The conference was modelled after the very successful CRYPTO and EUROCRYPT series of conferences sponsored by the International Association for Cryptologic Research (IACR). The IACR and the Institute of Electronics, Information and Communication Engineers were sponsors for ASIACRYPT '91.

The program committee published a call for papers and received 100 extended abstracts for consideration. Three of them were not reviewed since they arrived too late. Each of the other abstracts was sent to all the program committee members and carefully evaluated by at least 10 referees. The committee accepted 39 papers for presentation. In addition, the program committee invited four papers for special presentation as "invited talks." Unfortunately, three of the accepted papers were withdrawn by the authors before the conference.

The conference attracted 188 participants from 17 countries around the world. The technical presentations were well attended and enthusiastically received. Following the CRYPTO tradition, an evening "rump session" was held. This session, chaired by Thomas Berson and Kenji Koyama, included short presentations of recent results. The non-technical portion of the conference included a sightseeing trip to the base of Mt. Fuji, a Japanese barbecue lunch (*robatayaki*), and a banquet with drummers and a magic show.

After the conference the authors produced the full papers, in some cases with slight improvements and corrections, for inclusion here. For ease of reference by those who attended the conference, the papers are placed in the same order and under the same headings as they appeared at the conference. Because of the interest expressed in the rump session presentations, we have included short papers contributed by the rump session speakers at the end of this proceedings. Of the 12 rump session presentations, the 6 abstracts included here have gone through a thorough, if expedited, refereeing process.

It is our pleasure to thank all those who contributed to make these proceedings possible: the authors, program committee, organizing committee, IACR officers and directors, and all the attendees.

Yokohama, Japan — Hideki Imai
Cambridge, U.S.A. — Ronald L. Rivest
Yokohama, Japan — Tsutomu Matsumoto
August 1993

ASIACRYPT'91

Program Committee:

Hideki Imai (Co-Chair, Yokohama National University, Japan)
Ronald L. Rivest (Co-Chair, Massachusetts Institute of Technology, U.S.A.)
Tsutomu Matsumoto (Vice Chair, Yokohama National University, Japan)
Thomas A. Berson (Anagram Laboratories, U.S.A.)
Chin-Chen Chang (National Chung Cheng University, R.O.C.)
Yvo G. Desmedt (University of Wisconsin – Milwaukee, U.S.A.)
Shimon Even (Technion, Israel)
Shafi Goldwasser (Massachusetts Institute of Technology, U.S.A.)
Ingemar Ingemarsson (Linköping University, Sweden)
Kenji Koyama (NTT Corporation, Japan)
James L. Massey (ETH Zürich, Switzerland)
Sang-Jae Moon (Kyung Pook National University, Korea)
Eiji Okamoto (NEC Corporation, Japan)
Keng-Cheng Zeng (Academia Sinica, P.R.O.C.)

Organizing Committee:

Shigeo Tsujii (Chair, Tokyo Institute of Technology)
Yoshihiro Iwadare (Vice Chair, Nagoya University)
Masao Kasahara (Vice Chair, Kyoto Institute of Technology)
Kenji Koyama (Local Arrangement Chair, NTT)
Ryota Akiyama (Fujitsu)
Hideki Imai (Yokohama National University)
Toshiya Itoh (Tokyo Institute of Technology)
Shin-ichi Kawamura (Toshiba)
Naohisa Komatsu (Waseda University)
Sadami Kurihara (NTT)
Kaoru Kurosawa (Tokyo Institute of Technology)
Tsutomu Matsumoto (Yokohama National University)
Hideo Nakano (Osaka University)
Koji Nakao (KDD)
Kazuo Ohta (NTT)
Tatsuaki Okamoto (NTT)
Ryoui Onda (SECOM)
Kazuo Takaragi (Hitachi)
Kazue Tanaka (NEC)
Atsuhiro Yamagishi (Mitsubishi)

Contents

THE TRANSITION FROM MECHANISMS TO ELECTRONIC COMPUTERS, 1940 TO 1950

Donald W. Davies, Independent Consultant
15 Hawkewood Road, Sunbury-on-Thames, Middlesex UK, TW16 6HL

Abstract

The peak of mechanical cryptography was reached in World War II, then electronics rapidly replaced these machines. A very remarkable technology then ended. Some of the best examples that I have found will be illustrated. The paper continues with some memories of building the first computer at NPL during 1947 to 1950.

The age of mechanisms

The difference engines and analytical engines designed by Charles Babbage would have been, if completed, one of the greatest achievements of the mechanical age. Computing devices remained mechanical (or electro-mechanical) for another 100 years. Today we are in the electronic age and it is interesting to look at the short period of transition from mechanisms to electronics, which began about 50 years ago. In this paper I shall consider only digital systems and my examples come from cryptography and my own memories of the first electonic computers.

Electronics can be pretty, but what you see is only distantly related to its function. At the peak of the mechanical age, the function of mechanisms was very clear; they could be seen working at human speeds. This led their designers and constructors to emphasize their function with shapes of striking beauty and with surface finishes that were often much more elaborate than strictly required. Not only steam engines and pumps had this quality - it can be seen in Babbage's designs and in his test assemblies.

It has often been assumed that Babbage did not complete his machines because the technology of the time was inadequate. The recently completed difference engine No.2 at the London Science Museum shows that Babbage's machines do work, when they are built with the materials and precision available to Babbage. The design needed

several corrections and some counterbalancing springs. The very complex running carry mechanism works perfectly and spectacularly, and wheels that are not being stepped are firmly held. The only concerns of its designers and operators at the Science Museum are with lubrication and with wear. The part of the machine which impressed the printing plates has not yet been built and urgently needs sponsorship.

Calculating mechanisms often have repeated units such as counter wheels and registers but they cannot be organised simply by linking together large numbers of very simple devices in the way that gates and storage cell are used. The best that can be done is illustrated by Babbage's notation for mechanisms and his suggestions for some general-purpose mechanical principles. Conrad Zuse once described to me a mechanical binary store array with which he had proposed to make a mechanical 'minicomputer'. But these were exceptions and usually a digital mechanism is designed as a whole rather than assembled from identical subunits. In this respect, the precursors of the gates and cells of electronics were electro-mechanical systems such as telephone exchanges which used relays and rotary switches as subunits, and appeared briefly in cryptography.

To illustrate this period of transition I will first describe two cryptographic mechanisms used by Germany in WWII, then some of my own experience with the first electronic computers.

On-line ciphers of World War II

The Enigma machine is very well known. This was operated off-line, producing a written ciphertext which was then manually transmitted. In the Defence Museum in Oslo there are printer attachments for enigma machines, remote displays and a large commutator called 'Enigma-Uhr' which could be wired to the plugboard to give hourly changes of key. Fortunately for the Allies, this last device came into use very late. By upsetting the involution property of the plugboard, the Enigma-Uhr would have given a major problem to the cryptanalysts.

There were two on-line machines in wide use by the German forces.

One was known as SZ40 or SZ42, where SZ stands for Schluessel Zusatz

meaning cipher attachment. As its name implies, it operated 'in-line' in a teleprinter circuit and did not have its own keyboard or printer. The maker was Lorenz. It was installed with a teleprinter and radio equipment in a vehicle designed for the warfare of rapid movement or 'blitzkrieg' planned by Germany. This machine was used at the level of high command, making its messages very valuable to the allies.

The second on-line machine was the T52, essentially a standard teleprinter working together with a built-in cipher unit. This was made by Siemens and Halske. For most of the war it was used with transmission by cable, but at a late stage it enciphered radio messages and the Allied cryptographers began to take an interest in it.

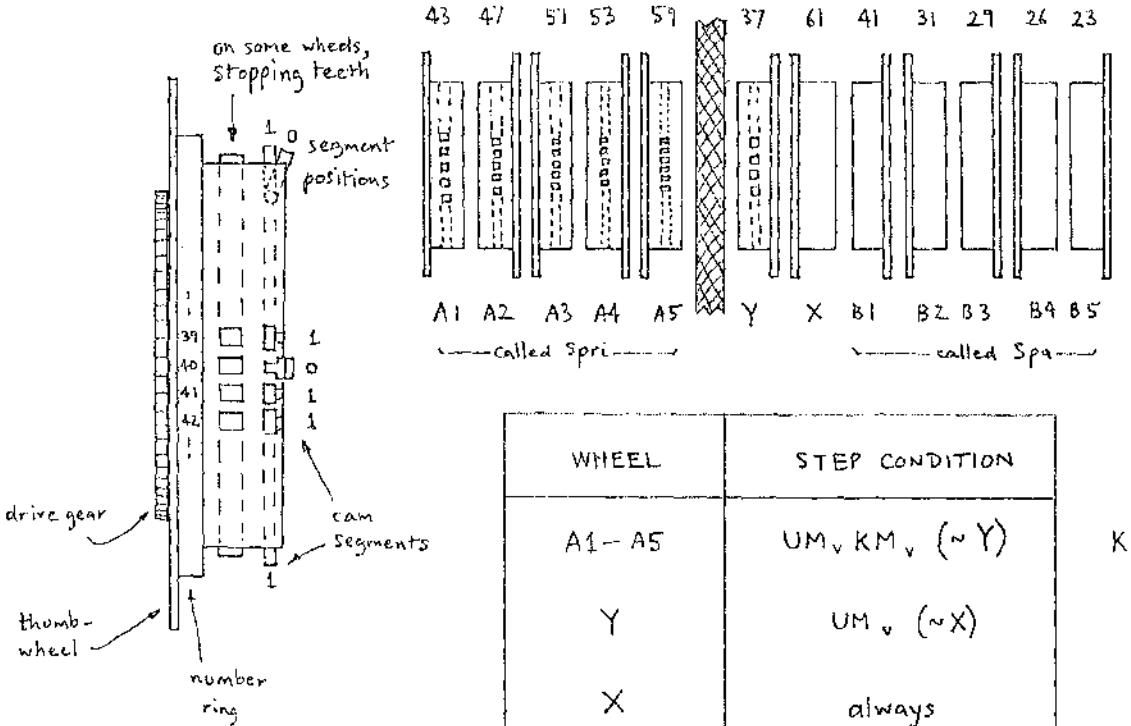
Eric Huttenhain, who developed cryptanalytic machines for the cipher bureau of the OKW told me that his group made a comparison of the security level of these two machine, but he would not tell me the outcome. In the event, the SZ was put in the most sensitive place. I believe the T52 as eventually developed was stronger.

The T52 was very bulky and heavy, compared with the SZ. The SZ needed a teleprinter but this was a separate unit, easier to instal in a vehicle. Perhaps these considerations led to the decision that SZ should be in the mobile system.

The Lorenz Schluessel Zusatz

This machine fits well into our theme because the cipher unit was almost completely mechanical. It is a mechanism of great elegance. Though the principle is simple, designing it mechanically was difficult. I have not, at the time of writing, had enough time with a working model to understand the mechanism completely. Two exist, at the Oslo museum and the DeutschesMuseum in Munich.

From the many photographs I have obtained it is clear that the SZ went through many changes and improvements. This also appears in the official history, which mentions changes in the cipher called 'Fish'. But I have been unable to match the various clues and produce a coherent account of its varieties. We can guess that SZ40 and SZ42 were introduced in 1940 and 1942, but the significant changes were later.



WHEEL	STEP CONDITION
A1 – A5	$UM_v\, KM_v\, (\sim Y)$
Y	$UM_v\, (\sim X)$
X	always
B1 – B5	always

$KM = A1 \oplus B2 \oplus ?$

Figure 1: Cipher Wheels

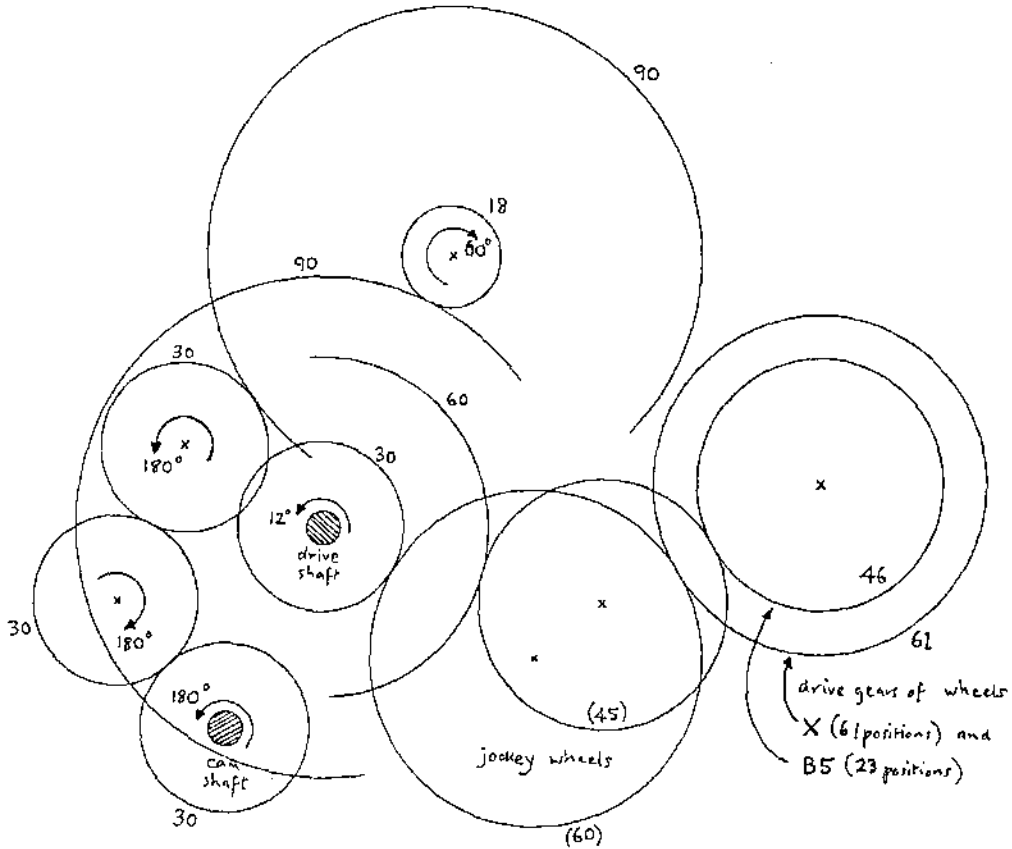
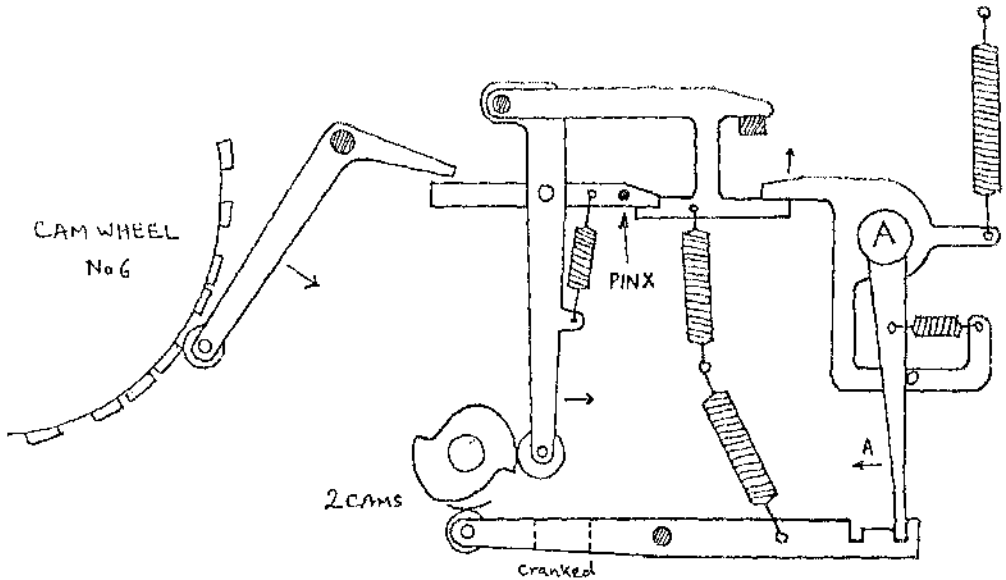


Figure 2: Gear Train



PINX lifted by UM or KM
removes stops on 1-5

raised tooth on # 6
applies stops on 1-5

Figure 3

The outer case of the machine contained both the mechanical cipher unit and electromechanical devices to convert from the start/stop 5 unit telegraph signal to 5 parallel signals and back from the parallel channels to the serial signal.

Figure 1 shows the 12 cipher wheels, which had relatively prime numbers of teeth, namely 23, 26, 29, 31, 41, 61, 37, 59, 53, 51, 47, 43 reading from the right. Functionally there were two sets of 5 wheels (coresponding to the 5 channels) at each end and special wheels of 61 and 37 teeth in the middle.

A very distinctive feature of the SZ is that the binary output of each wheel can be set by moving to one side or another individual hinged teeth. We can imagine that setting these patterns would be tedious and error prone, so it would not be done frequently.

The cipher priniple was simply to add the output of one A wheel and one B wheel, modulo 2 to each channel. If every wheel moved one step between characters, this is a conventional Vernam cipher and rather weak. Clearly some extra principle is needed. This is the intermittent stopping of all the A wheels.

To drive the wheels at their various rates there is an ingenious set of gears and jockey wheel of diferent sizes shown in Figure 2. Wheels which might need to stop are driven through a slipping mechanism inside the wheel. On the edge of these wheels are square teeth which can be engaged by a latch to stop them for one or more character times. Incidentally, Babbage deplored the use of slipping like this and insisted that all movements were positively driven. His machines could possibly jam but would never make errors by bouncing or overshooting. I wonder if the SZ had any such problems.

In the simplest form the SZ worked in this way: The X wheel always moved. Its output controlled the stopping of wheel Y. The output of the Y wheel controlled the stopping of all the A wheels together. The later developments controlled the stopping of the A wheels also by outputs from individual A and B wheels.

Figure 3 shows part of the mechanism which uses the output of the Y wheel to lift an interposer and either turn shaft A or not, powered by

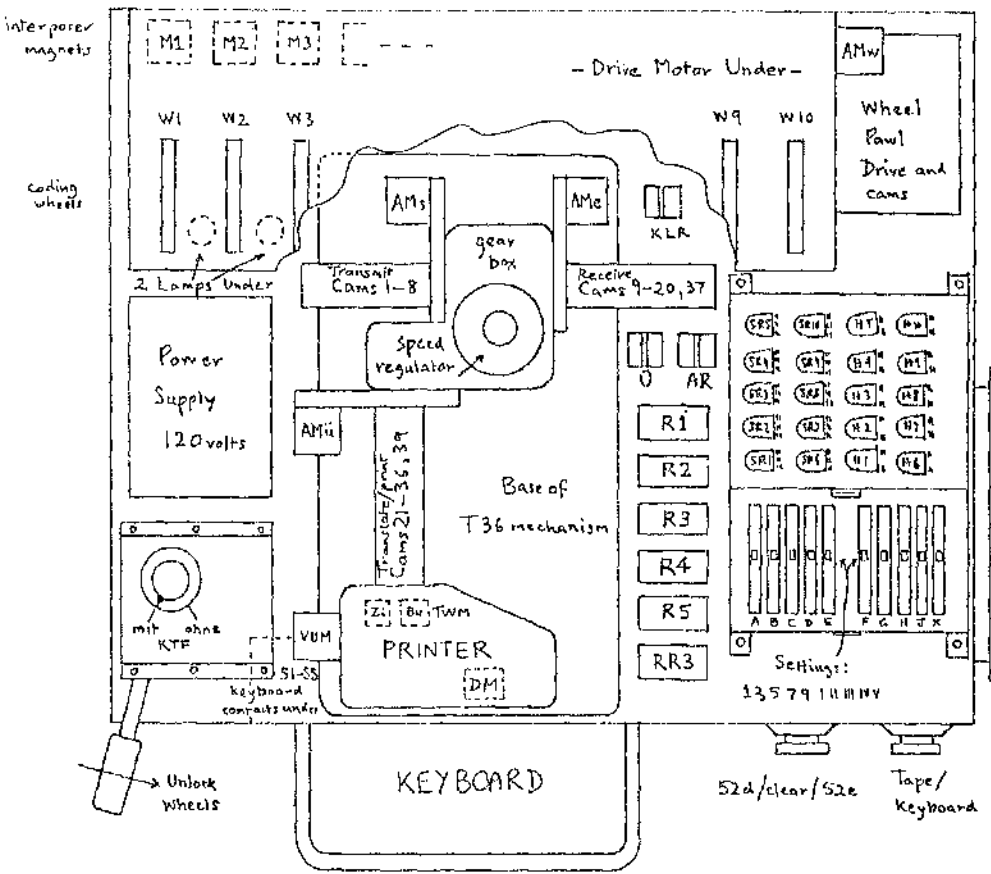


Figure 4: Plan View of the T52e

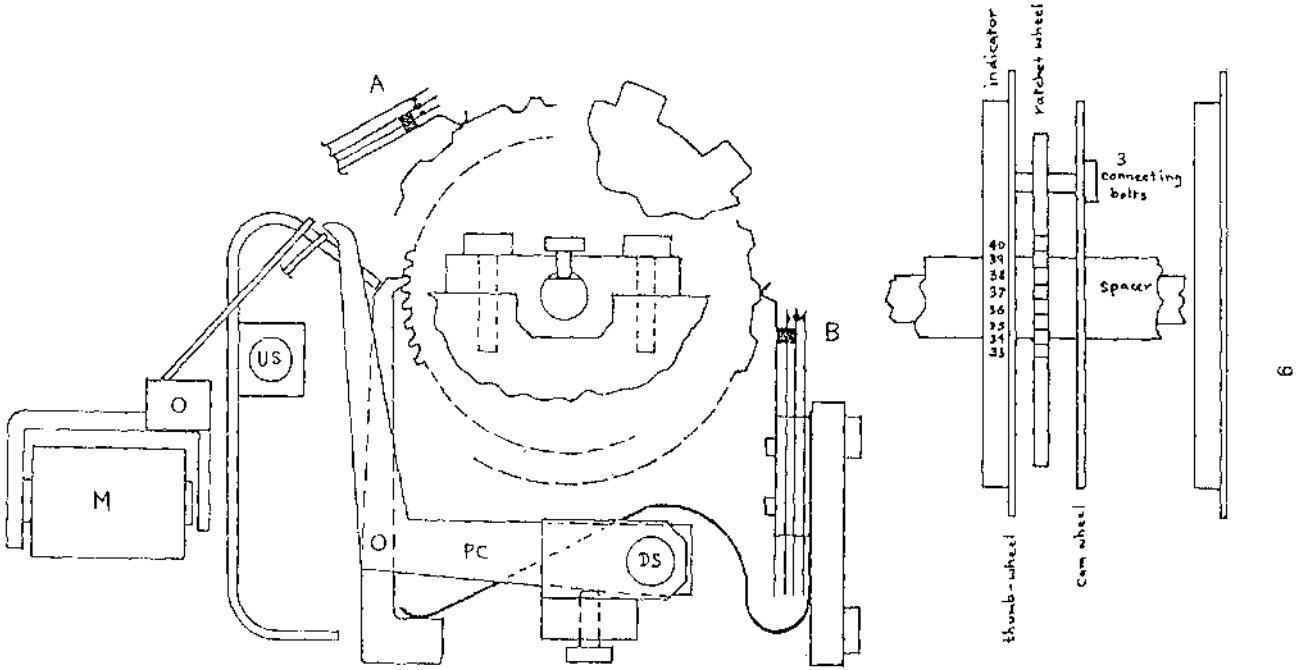


Figure 5: Interposer Machanism, Cam-wheels and Contacts

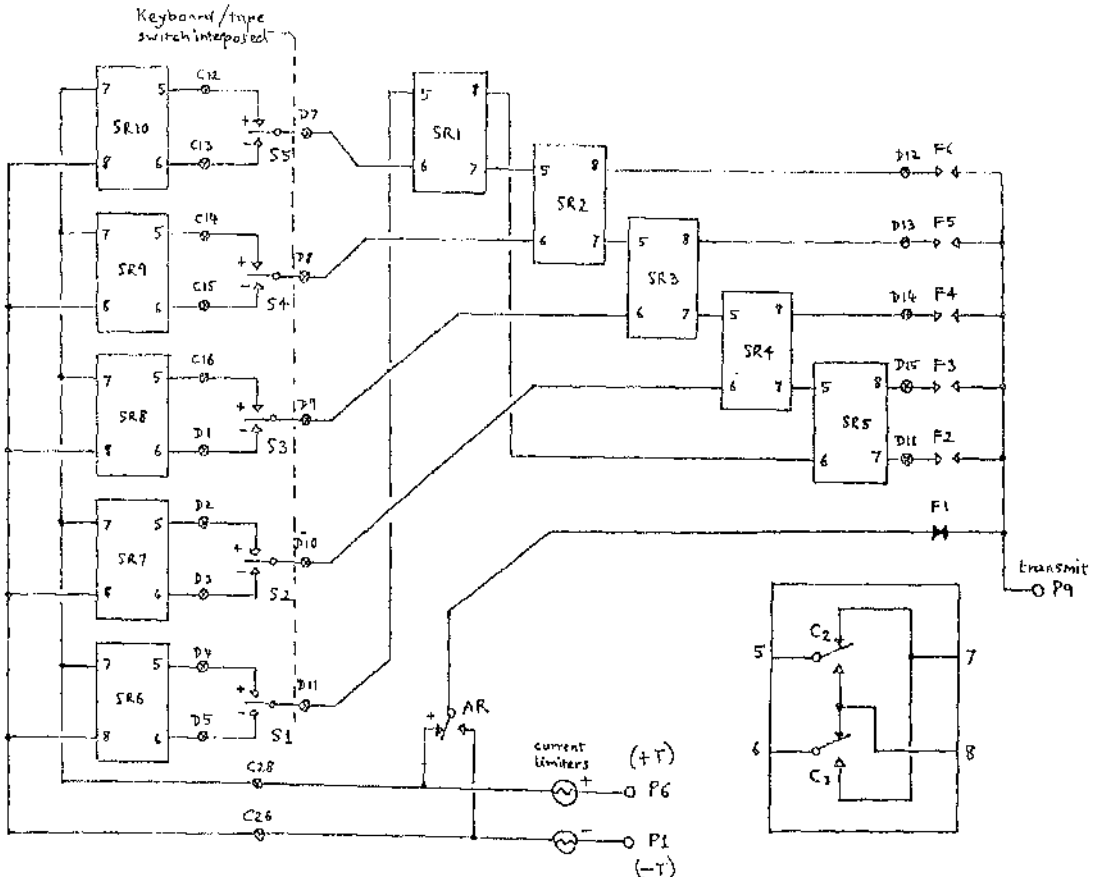


Figure 6: Encipher-Transmit

a cam. The output of A is locked by another cam. Shaft A drives the mechanisms on each of the A wheels which stop their movement.

The Siemens and Halske T52

The very large baseplate of the T52 holds the mechanism of a T36 teleprinter, with it's keyboard, tape reader and printer, together with all the cipher equipment. Figure 4 is a plan view. The largest addition is a set of 10 cipher wheels at the back. The other main additions in the figure are 20 relays and 10 rotary switches on which the basic key is entered.

There were five models labelled a to e and the one I shall describe is model e. The machines were sometimes modified in the field without changing their label, but I have been able to get a detailed picture of each model. Models a and b were logically identical, b having improved electrical filters, supposedly to reduce radio interference. Models c and d introduced the important feature of intermittent wheel motion. A model f was under development but was not made and no information about it has been found.

The 10 wheels have relatively prime numbers of teeth, respectively 47, 53, 59, 61, 64, 65, 67, 69, 71 and 73. The cam profiles were fixed for the whole time the T52 was used, as far as I know. A change of wheel is possible with simple tools but readjustment of contacts could have been a problem. In some models modified for use in Norway, wheels have been assembled in different orientations and there are very few original machines in existence.

Figure 5 shows how a wheel is driven by a ratchet and how magnet M stops the drive. Each has two sets of contact springs. One is used in the cipher transformation, the other drives the wheel stopping logic.

The 10 binary wheel outputs go first to the rotary switches on which the main key has been set, which permute them. Then they go to the relays which perform a linear (mod 2) tranformation on the 10 bits. 5 of the bits are added modulo 2 to the telegraph code, then the other 5 bits determine a permutation of the 5 elements of the code, as shown in figure 6. The machine has separate relay logic for encipherment and decipherment. When transmitting in cipher it simultaneously receives, deciphers and prints the character, giving a check on the operation of some (but not all) of the equipment.

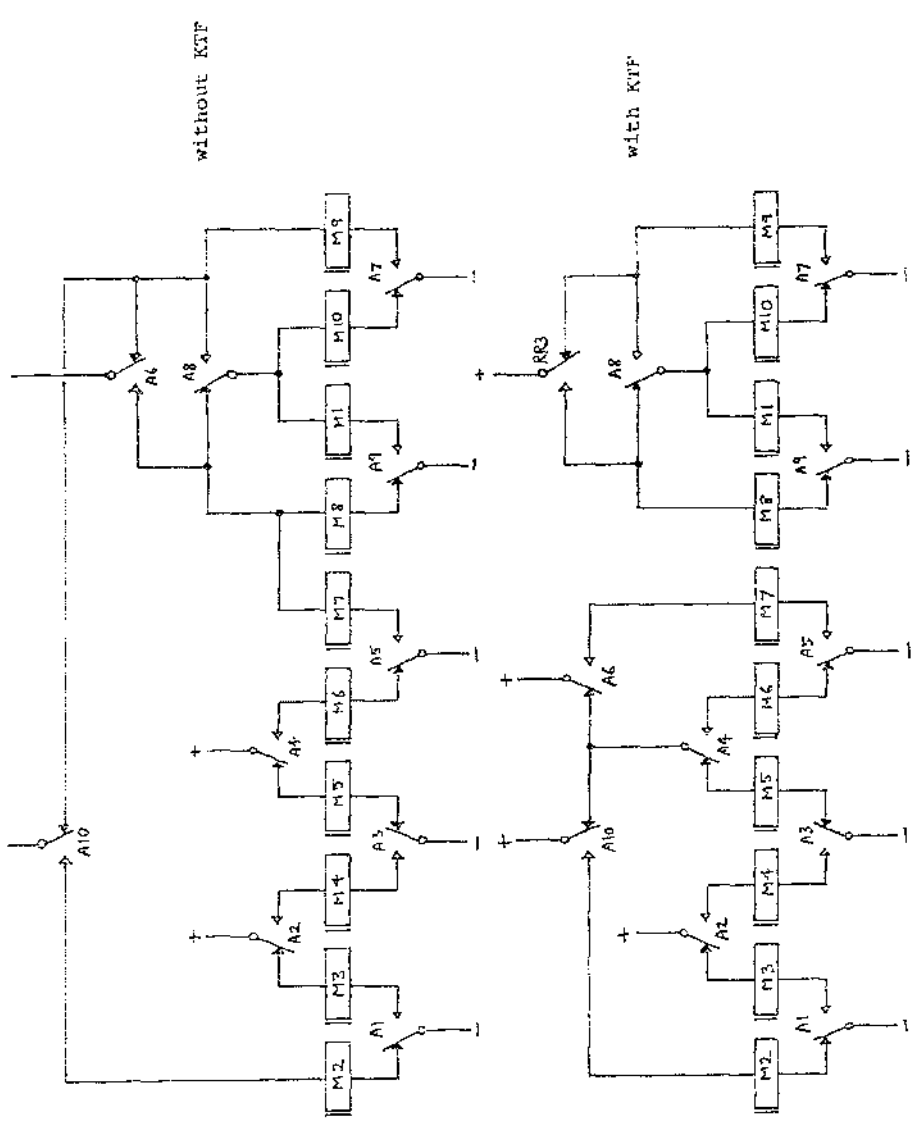


Figure 7: Schematic of Interposer Logic

Perhaps the most interesting feature is the wheel stopping logic, one version of which is shown in Figure 7. The wheels have a total of 8.9 x 10^{17} states. A random state transition table would give a cycle length of the order of 9.5 x 10^{8} and it would be interesting to know what cycle lengths were actually obtained.

The main key was set by a plugboard in earlier models. Both the plugboard and the later rotary switches were in a locked box and were probably changed infrequently. The 'message key' was probably the initial wheel settings, but the method of transmitting them is unknown. Models a, b and c had an elaborate mechanism for returning all wheels to a chosen setting, perhaps for sending the message key.

Model c had an additional unit with 10 levers on which a 'message key' could be set. These performed yet another permutation on the outputs of the 10 wheels.

The last of their line?

The early history of the SZ is unknown but the T52 can be traced back to a patent in 1930. US patent 1,912,983 is closer to the eventual T52. It was developed as a commercial venture and I was told that one version was supplied to Hungary in 1932. Another person said the first deliveries of the T52 were in 1934. Bombing stopped production in Berlin in 1944 but a small facility in Kladov near Berlin tried to continue for a while until the Russian army arrived in May 1955.

On-line cipher machines for teleprinter messages had to encipher a 5-bit code in about 150 ms. Electro-mechanical technology of the 1930-1940 period implied a stream cipher driven by contacts from cams on wheels, or the use of uniselectors. My experience suggests that uniselectors would be difficult to maintain, the T52 would be reliable with skilled maintenance and the mainly mechanical SZ would work best in practice in military conditions.

I have no information about other on-line cipher machines of the WWII period. The two I have described represent, I believe, the most advanced level of on-line cryptography before electronics took over. In particular, the T52 suggests some interesting theoretical problems.

The first electronic computers

I joined a small team at the UK National Physical Laboratory (NPL) under the leadership of Alan Turing in 1947. By that time the logical design of ACE had reached version 7c, but nothing of significance had been built.

There were three pioneering computer projects in UK, the others were at Cambridge University and Manchester University. I shall speak only about my own experience.

For months our design team continued to refine the design, testing the order code by programming excercises and the logical design by stepwise tabulation of the states of triggers etc. This was extremely tedious and frustrating. Only a short time after I joined, Turing left the project but I did have one discussion with him about his 'computable numbers' paper. Rather it was an argument because I wanted to correct all the many errors in the formal part of the paper and Turing felt this was a waste of time.

There is evidence that when the project was officially approved, the possible future use of computers for cryptanalysis was in the mind of at least one member of the committee. Also the wartime experience in making Colossus may have led to the decision that the Post Office Research Station at Dollis Hill should build the machine. I should explain that the telephone network was part of the Post Office; Martlesham is the successor of Dollis Hill, where the Collossi had been built. Two of that team became our engineers. But the arrangement did not work well, hence our frustration. In the long run our design transferred to Dollis Hill became a computer which worked well in a defence establishment, but we cut ourselves loose from this scheme and built ACE ourselves.

Getting it started at NPL met further snags and it was only when finally the mathematicians and electronics engineers finally all moved into one large room and made a single team that construction really began. We lost years in this muddle.

One of our strokes of luck was that Harry Huskey, from the ENIAC team, joined us for a year. He started a project to build a 'test assembly'

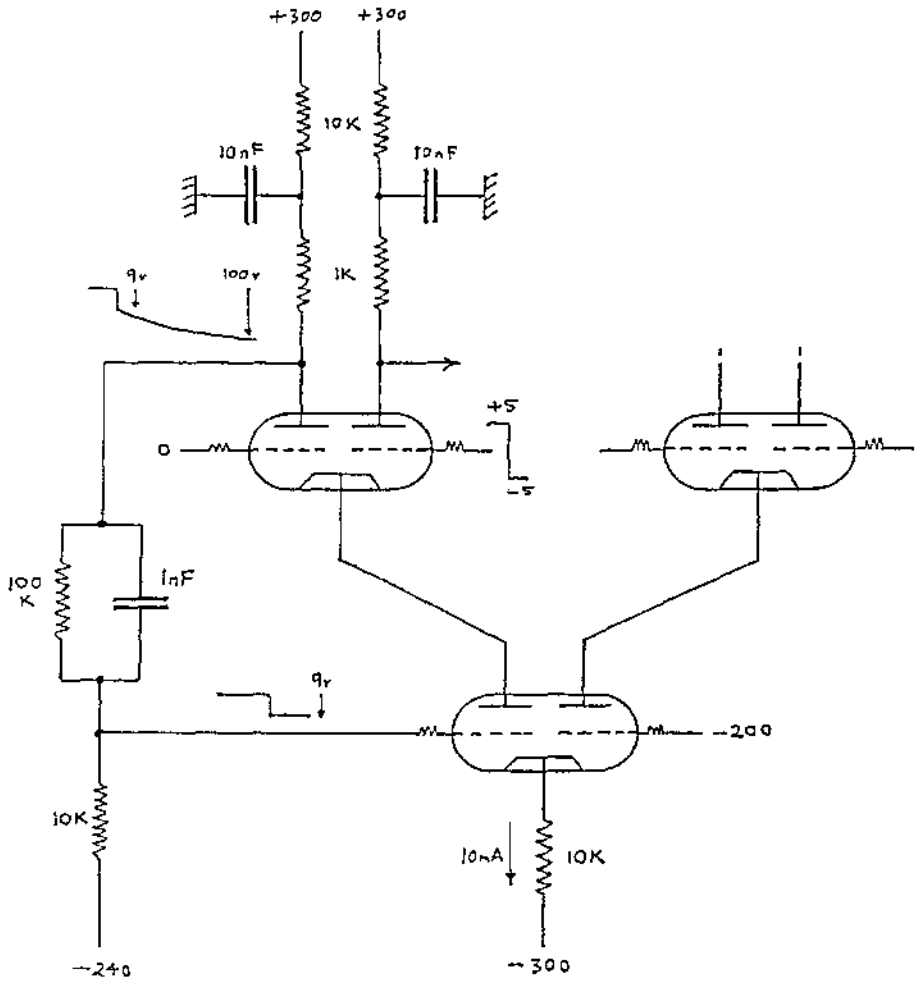


Figure 8: Current-Steering (long-tailed pair) due to Blumlein

which later, under the name 'Pilot ACE' was adopted as the main objective. It became the English Electric 'Deuce' and in the US used the design for the Bendix G15, which was an early commercial success. Huskey had one in his garage in Berkley when I visited him and this must be the first personal computer, though it was rather large and hot. Now this machine is on display in the Smithsonian Museum in Washington DC.

Engineering

ACE had only about 1000 thermionic tubes(valves in UK jargon) so I think it was the first RISC machine. Its memory (we called it the store) was about 8 mercury delay lines (long tanks) each holding 32 numbers of 32 bits, together with a small number of short mercury delay lines (short tanks). I later made a basic redesign of the long tanks, folding in half by two reflections and making the crystals fully adjustable.

The clock rate was 1 MHz, considered fast for valves but actually conservative with the circuit design we employed. The later full scale ACE ran easily at 1.5 MHz. Our circuit design came from the work of Blumlein at EMI, who developed the UK's prewar television equipment and wartime radar losing his life while testing radar in an aircraft.

The basic circuit is shown in Figure 8. It fed a constant current into the common cathode of two triodes and diverted to one or other anode. This is precisely the analogue of current steering or emitter coupled logic. We stacked these two high and with the necessary current defining resistors it meant voltages from -300v to +300v. Since all testing was done under power, we learnt to think before touching. I still work on live 240v circuits without fear, though with caution.

Then we needed couplings for the 10v signals from a top anode to a lower grid. Blumlein had a perfect answer which is shown in Figure 8, but it would take too long to analyse this circuit and its tolerancing here. Two engineers from EMI joined us with this technology. Without them we would have floundered. We also had to learn a good discipline for the timing of signals and that is another story.

ACE PILOT MODEL 1949 to 1956

List of Sources and Destinations

Number	Source	Destination
0	Input 32 bits	Control
1 to 10	Long Delay Lines 32 words each	
11	TS11 1 word	TS11
12	DS12 2 words	DS12
13	DS14 DIV 2	Add to DS14
14	DS14 Long Acc	DS14
15	TS15	TS15
16	TS16 Short Acc	TS16
17	NOT TS26	ADD to TS16
18	TS26 DIV 2	SUBTRACT from TS16
19	TS26 times 2	MULTIPLY
20	TS20	TS20
21	TS26 AND TS27	Set TCA
22	TS26 XOR TS27	spare
23	P17	TCB
24	P32	Jump if negative
25	P1	Jump if non zero
26,27	TS26, TS27	TS26, TS27
28	ZERO	OUTPUT 32 bits
29	ONES	Buzzer
30	TIL (card control)	Start Punch
31	spare	Start Reader

In 1954 DL9 handled magnetic drum transfers which were controlled by two destinations

Figure 9

Programming

The order code had 2 store addresses for data and one short address for the next instruction. Each operation took data from a source and moved it to a destination. The source or destination value defined also the type of operation, for example some addresses belonged to the accumulator or multiplier or to tanks which precessed at each use (for sequential access). Figure 9 shows a list of the sources and destinations.

The really novel feature was that operations could transfer up to 32 words in sequence (the first vector operations) and whan an operation ended the next instrucion could be loaded at once, if it was in the right place in a tank. These things could make the machine very fast, for its time, but to exploit them was a difficult problem for the programmer. It has been called 'optimum programming' but it is simply making the best of an awkward kind of memory with long latency.

Programming had two stages. First we wrote the program then we laid the instructions carefully in the store. This second phase was like solving a puzzle. For important subroutines, days might be spent trying to reduce the length of a loop to get it into one less circuit of a long tank (one less major cycle, or one millisecond.)

Input and output

Our input and output was on 80 column punched cards, but not usually in the standard way. We usually put one binary word on each row of the card, 12 to a card. Since this could in principle reduce a card to 'lace' there was no certainty that the card machine could handle it, but they always did. We found that chads could be pushed back into a card and were very firm. This was useful to correct minor errors in programs, which we punched ourselves in binary. I still remember the number up to 31, least significant bit first. The convention arose because the unit bit had to go first through an adder and appeared first on the monitor screen. We were quite shaken when we found the rest of the world put the msb first.

Our card machines read at 200 cards per minute and punched at 100, making them much faster than the paper tapes others were using, especially if each held 384 bits. With our small store we had to

operate on big matrices, so we used cards as intermediate memory until our drum came along. The operators became skilled at loading blocks of cards in the right sequence and avoiding jams.

The drums were novel. Like the Manchester team we were able to synchronize the drum rotation accurately to the clock. We chose one revolution in 9 major cycles, precisely 9216 microseconds, making 6510.4 rpm. The drum surface must not be more than about 1 microsecond late or early. We also had moving heads driven by moving coil linear motors, after trying several other drive principles which would make an interestng story themselves. Mechanisms have not disappeared, of course, they tend to get simpler but faster.

What was it like?

I have been asked about our motivation. NPL had a Division specializing in numerical mathemetics and its members, myself included, had struggled for years with heavy calculations that demanded man years (more accurately woman years) of a human computer's time. In this Mathematics Division were some acknowledged experts on numerical analysis. In some ways this was more highly developed for human computers than it is today because we could use judgement about how to approach a singularity or when to use an alternative iterative step. We were fully ready to exploit the machine when it worked and we ran one of the world's first computer services, early customers being aircraft designers with their new flutter problems.

At the start we all saw clearly the potential of the vast increase of computing speed and there was plenty of discussion of big numerical problems, such as weather forecasting. I do not remember our group talking about applications in commerce until much later.

My main impression was of isolation from the rest of the world. To describe properly what we were doing would have needed a long lecture about numerical work, programs, instructions, electronics and input and output. We could talk to the teams in Cambridge and Manchester (we met often in Cambridge) and to friends in the US but for the rest we tended to remain silent. Colleagues in analogue computing looked at our work and thought we were crazy.

In one sense we were crazy. Experience showed that our collections of

more than 1000 valves would never all work together. The completely accurate working of everything seemed too much to hope for. The first trials seemed to confirm the gloomy view. The simplest possible program ran for a second before it failed. Next day it ran for 10 seconds after an improvement in timing, for example. There was often enough an improvement to keep us motivated, but all thoughts of the complex programs written in the pre-building stage were forgotten.

When the tolerancing in signal level and timing had been got right we were at the mercy of valves. Heater failures were not such a problem and stability of characteristics was made unimportant by Blumlein's genius but their were other plagues. Our double triodes had grids close to the cathode. They could become 'tap happy', causing momentary faults when they had the slightest movement. The faults, I should explain, never gave wrong results but would drop out of the program. We found (or thought so) that small particles of cathode material were lodging between cathode and grid. These valves should be replaced, so we sometimes ran a test program and tapped all the valves one by one. We felt this was not good engineering but it worked

Years later I visited IBM's first computer producion line, I think it was the 650 magnetic drum machine. At the final stage of testing, blue suited IBM engineers were tapping all the valves with a carefully designed special hammer. I felt vindicated. We had been engineers after all.

The progress from just working to becoming an important service to industry was very gradual, with many backward slides. Always the best test program was the latest really complex application. The mature machine could always sail through the programs devised by engineers. Jim Wikinson, our genius of linear algebra would say 'It's a poor machine that won't run its test programs.'

I ran the first program that used a subroutine, just a ray tracing program with a square root. Seeing happen what we had thought about four years earlier was exciting. The reality of programming (more important, of problem solution) was very different from the early dream. Later I did the first simulation of traffic, both road traffic and men receiving warnings and exiting a coal mine. But others took over the programming art. Unfortunately the nice trick of optimum programming was not very compatible with languages. Turing had been the first to conceive a machine as having a language and being able to

interpret another language, but his creation, the logic design of ACE and its Pilot ACE paradoxically did not shine in this environment. Still, our small team made a contribution to Algol (and later to ADA) and went on to many achievements.

My interests moved to data communications, then to security and processors, once the centre of our thoughts, became something you can buy at the corner shop.