BP's Sturgeon, The FISH That Laid No Eggs

Frode Weierud*

CERN, Div. SL, CH-1211 Geneva 23, Switzerland

1 Introduction

The German armed forces employed three different types of teleprinter cipher machines during the Second World War, the Lorenz machines SZ40 and SZ42 also called Tunny by Bletchley Park (BP), the Siemens & Halske *Schlüsselfernschreibmaschine* (SFM) T52, and the one-time-tape machine T43, also manufactured by Siemens. The Lorenz machines, which existed in three different models, SZ40, SZ42a, and SZ42b, are well known as the machines that were broken at BP with the aid of Colossus. The Siemens T52 existed in four functionally distinct models, T52a/b, T52c and T52ca — which was a modified version of the T52c machine, T52d, and T52e, all going under the BP code name of Sturgeon, while the Siemens T43 probably was the unbreakable machine that BP called Thrasher. The T43 machine came into use relatively late in the war and appears to have been used only on a few selected circuits.

This paper will explain in detail the events that led to BP breaking the Sturgeon machines. In 1964, the Swedish Under-Secretary of State Erik Boheman first revealed that Sweden had broken the German Geheimschreiber (T52) during the Second World War. [7] In 1967, David Kahn gave further details about this achievement. [25] However, it was only in 1984, when Hinsley et al. published part one of the third volume of *"British Intelligence in the Second World War,"* that it was officially acknowledged that BP also had experienced some success against the Siemens T52. [22] Previously, many authors had confused the T52 with the Lorenz SZ40/42 machines and had erroneously linked the Siemens T52 to Colossus. Since 1982, Donald Davies has published detailed information about the electrical and mechanical construction of the machines. [10–12] And Wolfgang Mache has through his contacts and interviews with former Geheimschreiber operators and technicians presented the evolutionary history of the Siemens T52 machines. [30–32] Apart from Sir Harry Hinsley's and Professor Tutte's [39] references to BP's attack against the T52 there had not been any detailed account of this part of BP's history before an earlier, shorter version of this paper was published in 2000. [43]

To make the presentation more easily accessible to the non-mathematically oriented readers it has been split into two parts. Part I is devoid of any difficult mathematical details yet it explains the basic functionality of the

* This article represents the views of the author but not necessarily those of his employer or any other third party.

Sturgeon machines. This will allow the reader to follow BP in its quest to conquer and master this rather elusive species of the "FISH" family. Part II, on the other hand, looks in detail at the cryptanalytical problems that confronted the codebreakers at BP. Here the machines' cryptographic principles will be expressed mathematically. However, the mathematical concepts are relatively simple and I would like to encourage the readers to try to grapple with the few equations there are. Many readers will find the intellectual challenge rewarding.

The first section of Part I gives a short overview of the German teleprinter cipher machines and their use, followed by a short section explaining how and when BP first encountered the Sturgeon traffic. The third section explains the cryptographic principle used by the Siemens T52 machines. Here the "Pentagon" is introduced and an explanation is given of how important this device was for BP's attack against the first T52 model it encountered. The next section gives, for the first time, a short overview of some of the special Q-codes that were used by the German operators. It then continues the historical presentation of BP's attack on the T52 and its struggle to keep abreast with the German cryptographers' continuous changes to the machines. The following section reveals that BP broke the T52d, a machine with irregular code wheel movement. This was indeed a major achievement. The sixth section shows how incorrect use of the machines further eroded their security. This section also contains new information about T52 machines that had different code wheels from those used on the standard machines. The next section explains what knowledge BP gained from the captured machines, while section eight shows how the Germans reacted to the news that the SFM T52 was insecure.

Three new sections have been added to this version of the Sturgeon history. The first gives an overview of the German Air Force (*Luftwaffe*) FISH links that were known to BP. The next section proves that BP knew about the Swedish codebreaking success against the SFM T52 well before it attacked the machine for the first time. The final section in Part I gives a few snapshots of Sturgeon's post-war history with the aim of preparing the ground for a future, more complete, historical account. Part II, entitled The Cryptanalytical Problem, gives new and detailed cryptanalytical information about the structure of the T52 key generators and how this information was used to attack the machines. A constructed example of how to perform an attack on T52 messages in depth[1] concludes this section.

[1] Two or more cipher texts or messages are said to be in depth when the texts have been aligned such that the entire texts or parts thereof have been enciphered by the same key, which can occur when a cipher machine or system is used incorrectly, or due to the use of poorly constructed keys, or where a key is reused.

2 The Machines and Their Use

All the German teleprinter cipher machines were on-line machines. This means that when an operator types his plain text message on the transmitting machine, A, the same plain text appears immediately on the receiving machine, B. Neither of the operators ever sees the cipher text. The Lorenz machines were from their inception designed to be suitable for use on high frequency radio circuits operating in the 3 to 30 MHz bands. Radio signals in this frequency range are affected by both slow and fast fading, Doppler shift and multipath propagation which can easily play havoc with the digital teleprinter signals. All these machines used the standard teleprinter speed of that time, 50 Baud, which results in an element time of 20 ms. They were

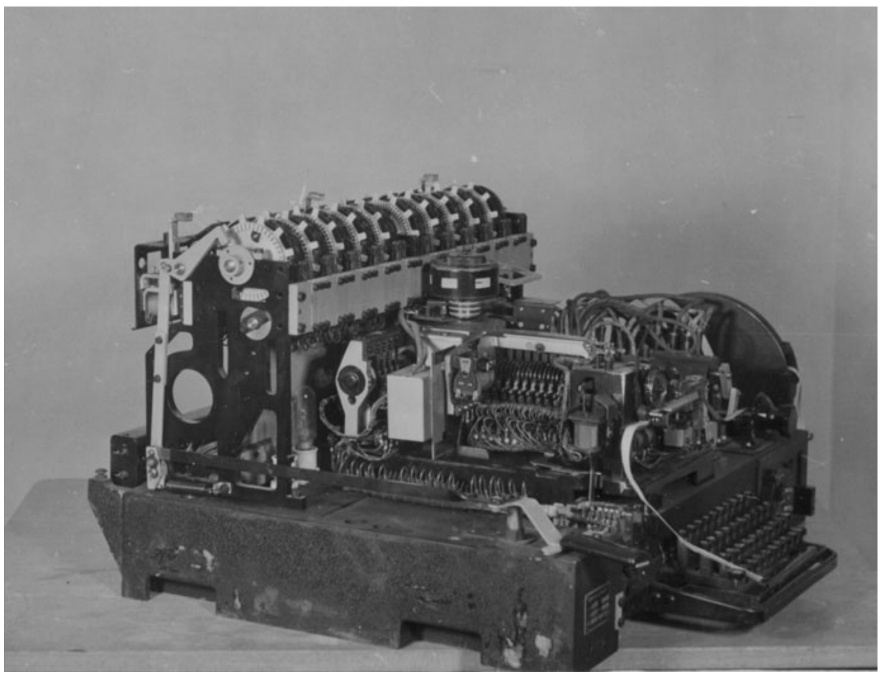

Figure1. Sideways view of the SFM T52d without its protective cover.

asynchronous machines using a start and stop pulse for each transmitted character. The SZ40/42 machines had a better receiver design than the T52 and were therefore more successful in reconstituting severely distorted teleprinter pulses. Towards the end of the war Lorenz worked on the development of an improved machine, the SZ42c, which applied the cryptographic process directly to the radio signal itself. [4] It was used in conjunction with a continuously operating, synchronous teleprinter which maintained its speed with the help of a crystal controlled oscillator. The SZ42c was an advanced design and the German engineers were clearly leading in this area.

It may therefore seem that technical reasons led to the Lorenz machines being used on radio teleprinter circuits. However, the author believes that logistics are more likely to have been the reason. The Lorenz SZ40/42 machines were a German Army development, while from an early stage the T52 machines were adopted by the Air Force and the Navy. The T52 machines were only allowed to remain on board naval ships while they were in harbour. It is evident that they would mainly be connected to the well developed telegraph line network which covered the most of German occupied territory. This was also the situation for the machines used by the German Air Force. On the other hand, a large part of the German Army tended to be continually on the move and it was relatively seldom that they could connect their machines to the fixed telegraph network.

With time the T52 machines also appeared on radio circuits. Initially they were used on radio relay connections using frequencies in the VHF and UHF range, while later they would also appear on circuits in the HF (3–30 MHz) area. The teleprinter signals were frequency modulated on radio carriers using multiple audio sub-band carriers. To increase the quality of the signal at reception the same signal was transmitted on two or more radio channels (frequency diversity) and on the receiving side they used two or more horizontally spaced antennas (space diversity). The Germans called their radio teleprinter equipment Sägefisch. [29] The name is apparently derived from the shape of the signal that could be observed at the output of the receiving detectors. At the end of the war a total of nine different *Sägefisch* models were planned, in use, or under construction. The two manufacturers involved were Telefunken and Siemens & Halske. *Sägefisch* I, II, IV and V were made by Telefunken while WTK I and II (*Wechselstrom-Telegraphie über Kurzwellen* — voice-frequency telegraphy over short wave) was made by Siemens. However, there was some co-operation between the two firms and EFFK I (*Einheits-Funkfernschreibgerät für Kurzwellen* — Standard radio teleprinter equipment for short wave) was a joint development by the two firms. *Sägefisch* II, a Siemens development, was never brought into service and *Sägefisch* V and WTK II only reached the prototype stage. The last *Sägefisch* equipment, EFFK II, was still under development when the war ended and only the receiver part had been through factory tests. In addition to the sets with frequency shift keying, equipment using phase shift keying (*Wechselstrom-Telegraphie mit Phasenumtastung* — WTP) was under development at *Allgemeine Elektrizitäts-Gesellschaft* (AEG).

3 The First Encounter

BP first observed Siemens T52 traffic in the summer and autumn of 1942. Most of the traffic passed on a radio link between Sicily and Libya, which BP called the "Sturgeon" link. [1] In the same period there was also another link from the Aegean to Sicily that BP called "Mackerel". The operators on these links were in the habit of sending a large number of cipher text messages using the same machine settings. When using the machine, they sent a short cipher text, followed by some operator chat in clear text. They then transmitted in clear the signal "UM UM" (*Umschalten* — switch over) and the cipher text continued but with the machine set to its initial setting. These interruptions and operator exchanges were frequent and the cipher texts in depth continued to accumulate. The depths allowed the BP cryptanalyst Michael Crum, an Oxford research mathematician, to analyse the machine in detail and he soon discovered that the machine had 10 code wheels whose patterns appeared to be fixed. [44] At least that was his assumption based on the intercepts during September and October and the first two days of November. After that, the Sturgeon link and its traffic came to an end. In the period before September the interception was too bad to allow any of the traffic to be read.

4 The Cryptographic Principle

The analysis of the intercepts showed that the Sturgeon machine was using two operations, a modulo two addition, which is the same as the Boolean logic operation exclusive-or (XOR), and a permutation of the resulting five teleprinter code elements. Modulo two addition or the exclusive-or operation is really nothing more than a simple inversion. A plain text element will change from 0 to 1 or from 1 to 0 if the key element is 1, while if the key is 0 it will remain unchanged. This can be seen from the XOR truth table in Fig. 2 where Σ_i represents the XOR key element, P_i the plain text element and C'_i the resulting cipher text element. We use C' to indicate that it is an intermediate result and that the real cipher text character, C, will appear only after the permutation has taken place.

Σ_i	P_i	C'_i
0	0	0
0	1	1
1	0	1
1	1	0

Figure2. XOR truth table.

The permutation is a pure reordering of the teleprinter elements or bits, which is the modern name for binary digits. The permutation 12345 is the identity permutation giving the normal order of the elements, while 52413 shows that bit 1 now is in element position 4, bit 2 does not move, 3 goes to position 5, 4 goes to 3 and bit 5 ends up in position 1. This is the permutation shown in the diagram on Fig. 4.

The cryptographic algorithm, transforming a plain text character P into its cipher text character C, consists of first applying the XOR operation to each of the five teleprinter elements of the plain text character and finally permuting or rearranging the order of the five resulting bits. The two cryptographic operations, modulo two addition and permutation, are controlled by two continuously changing key values. At BP the modulo two key was called the *subtractor* and represented by the symbol Σ, while the permutation key was called the *permutor*, and represented by Π.

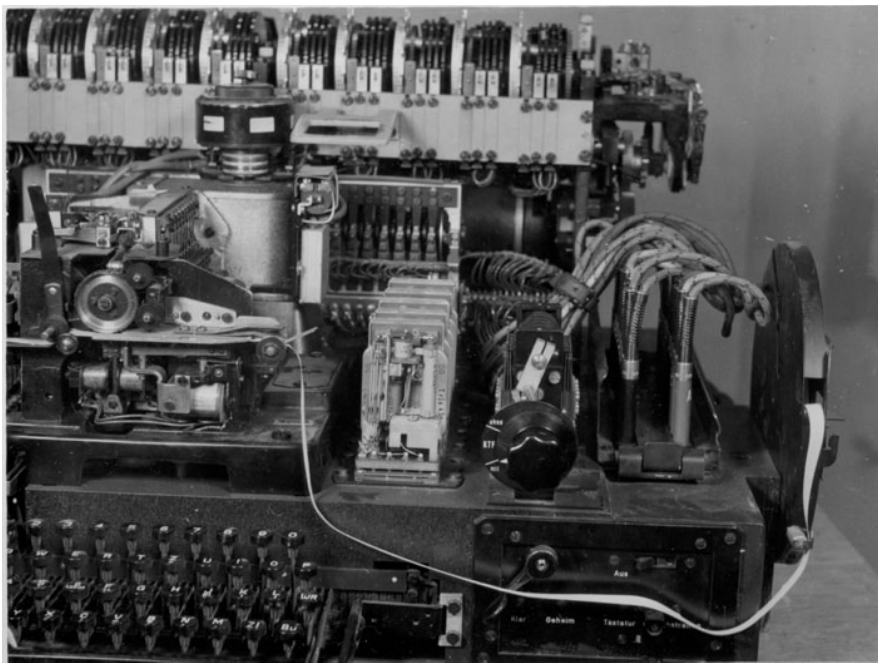

Figure3. Closeup view of the T52d code wheels and inner plug connections.

The two keys, Σ and Π, are each generated by five code wheels. The five Σ-wheels and the five Π-wheels could be chosen freely from the machine's ten code wheels. In the T52a/b and T52d machines this selection was done by plugging cables into the respective subtractor and permutor sockets, as we will see shortly. While in the T52c and T52e the selection was done by a switch and relay assembly. The T52 code wheels are similar in functionality to the wheels used in the Tunny machines, Lorenz SZ40 and SZ42. However, they were constructed differently. While the Tunny wheels had metal cams that could be set in an active or an inactive position, i.e. the wheel patterns could be changed at will, the T52 wheels were moulded in Bakelite. Each code wheel carried its own fixed code pattern.

On reception, the cryptographic algorithm consists of first applying the inverse permutation to the cipher text elements before performing the modulo two addition. The inverse permutation is the permutation that will return the bit order 52413 to the order we started with, the identity permutation 12345. We easily see that the reordering we need to turn 52413 into 12345 is 42531, which is the inverse permutation.

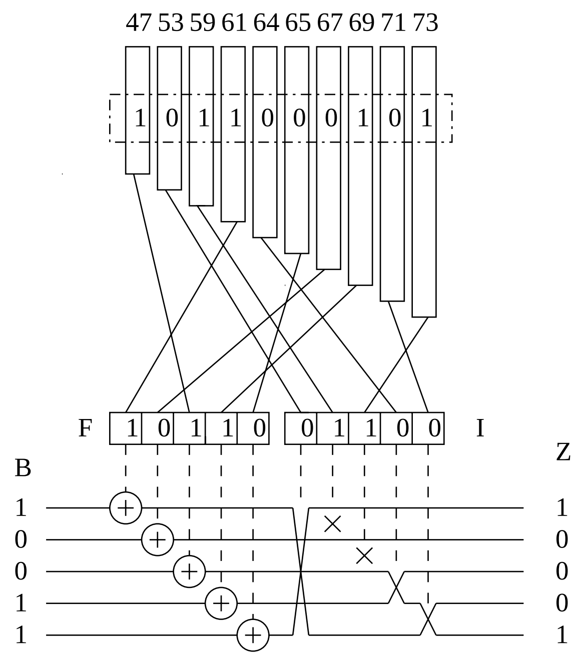

Figure4. SFM T52's functional diagram.

A schematic diagram of the basic operations of all the T52 machines is given in Fig. 4, while photos of the T52d machine are shown in Fig. 1 and Fig. 3. The ten rectangles of varying heights symbolize the ten code wheels whose circumference carried the bit patterns of different lengths. The wheels were Bakelite disks with protrusions which were sensed by one or more electrical contacts. A more modern analogy for the code wheels is shift register sequences of different lengths. In Fig. 4 the length of the code wheel sequences is written above each of the ten wheels. The code wheels were labelled A to K from right to left, omitting I. These wheel identities are used later in Fig. 6 which gives a description of the wheel stopping logic for the T52d machine.

Below the wheels, the plug connections that make up the main inner key are shown connecting each of the ten wheels to the various elements of the XOR and transposition circuits. The figure is an accurate representation of the functioning of the T52a/b and T52d machines. In these two models each code wheel consisted of four identical cams, each fitted with a changeover contact which was used in either the XOR circuits or the transposition circuits of the transmitter and receiver part of the machine. Fig. 3 shows the ten code wheels, each consisting of four cams, and the plug connections for selecting the code wheels used in the XOR and transposition circuits. The plugs connected to the code wheel contacts were labelled with the corresponding wheel identities A to K, each wheel being equipped with two plugs, one red and the other black. The corresponding sockets in the transposition circuit, ten in total, were labelled from 1 to 10. Sockets 1 and 2, 3 and 4, etc. were paired together but we will see later that any of the two plugs of a given wheel can be plugged into any of the transposition sockets. Further, the red/black order had no electrical significance and the two plugs could be swapped. The ten sockets in the XOR circuit were labelled with Roman numerals from I to V in pairs, where each socket in a pair carried an additional a or b label, e.g. sockets Ia and Ib. For the XOR circuit the plug order had to be strictly adhered to and the two plugs of a given wheel had to be plugged to the sockets with the same Roman numeral pair, e.g. red K would plug to IIa and black K to IIb. If the plugs of a given wheel were connected to two different Roman socket pairs a short circuit of the ± 60 volt signalling supply would be the result.

The T52c/ca and T52e machines modified this relatively complex circuit by using relays with multiple contact sets for the functions in the XOR and transposition circuits. These so-called SR relays were controlled via a logic circuit driven by the cam contacts on four different code wheels. On these machines the code wheels had one single cam on each wheel; the other three cams became superfluous and were therefore removed. The relays SR1–SR5 were used in the permutation circuit, while SR6–SR10 made up the substitution circuit. The machines also did away with the flexible transposition circuit of the T52a/b and d models which allowed full freedom in the configuration of the circuit as will be explained in Part II. The T52c/ca and T52e machines used a standard configuration of the transposition units which were wired permanently in place.

Instead of changing wheel order by plugging, these machines used ten switches, one for each wheel, which could be set to one of ten positions labelled $1, 3, 5, 7, 9, \mathrm{I}, \mathrm{II}, \mathrm{II}, \mathrm{IV}$, and V. The plugs and sockets of the T52a/b and T52d machines were completely removed. The previous pairing of plugs and sockets which were designated by 1–2 and IIa–IIb etc., were now simply represented by respectively 1 and II. The ten outputs from the wheel order selection circuit carried the same labels as the switch positions. Here the outputs from the wheel order selection unit are called 'output channels', such as to distinguish them from the outputs of the code wheels which are the inputs to the selection unit. These output channels would then enter the wheel combination logic and control the SR relays as shown in Fig. 5. The code wheel output channels are labelled $1, 3, 5, 7, 9$ and $\mathrm{I}, \mathrm{II}, \mathrm{III}, \mathrm{IV}, \mathrm{V}$. A cross in the row for one of the SR relays means that the control of the relay depends on the marked output channels, e.g. the function for the SR4 relay is given by the modulo two sum of the output channels $7, 9, \mathrm{I}$ and IV. Any of the

Relays		Wheel Output Channels									
		1	3	5	7	9	I	II	III	IV	V
Permutor	SR1	X	X				X		X		
	SR2		X	X				X		X	
	SR3			X	X				X		X
	SR4				X	X	X			X	
	SR5	X				X		X			X
Subtractor	SR6			X	X			X		X	
	SR7		X	X					X		X
	SR8	X	X					X			X
	SR9	X				X	X		X		
	SR10				X	X	X			X	

Figure5. Wheel combination logic for T52c.

ten wheels could be connected to any of the ten output channels going to the wheel combination logic with the only restriction that a given output channel could only be selected once. For example, if wheel A was selected to use the output channel labelled II, then this output channel could not be selected by any of the other wheels. If this rule was not obeyed a short circuit of the ± 60V supply would occur. Furthermore, the labels had lost their previous meaning of Arabic numerals belonging to the transposition circuit and the Roman numerals belonging to the XOR circuit. The three machines, T52c, T52ca and T52e, controlled each of the SR relays via a wheel combination logic which consisted of the modulo two sum of four different output channels. The wheel combination logic for the T52c has previously been published by Donald Davies in his paper on the T52 machines [11] and is reproduced here in Fig. 5. The wheel combination logic was different on each of the three machines. The logic for the T52e machine has also been published by Donald Davies in his paper on the T52e machine, [10] while the logic for the T52ca machine will be presented in Part II. The information in Fig. 5 has also been compared with information from the archives of the Swedish signal intelligence organization, FRA,[2] and found to be correct.

The T52c and T52ca machines introduced yet another complexity, the message key unit. This unit, which consisted of 15 transposition units and

[2] FRA, Försvarets Radioanstalt. See [6, 9, 40].

which will be introduced later, was connected between the code wheel cam contacts and the wheel order selection circuit. Its function was to further permute the order of the wheels before their contacts were selected in the wheel order selection circuit which was the main inner key. As explained later, a new setting of the message key unit was selected for each new message. This meant that even if the main inner key remained the same the wheels would still have a different function for each new message.

The T52d and e models also had irregular movement of the code wheels, a so-called stop-and-go movement. The movement of each wheel was controlled by contacts on two of the other wheels. These two machines also had a switchable autokey[3] element where the third bit of each plain text character would control the movement of the wheels in addition to the control given by the wheels themselves.

Here is how the machine works in an example as shown in Fig. 4. First, a plain text character, B say, will be represented by its Baudot code equivalent 10011 or $\times\bullet\bullet\times\times$[4] as given in the Baudot alphabet in Fig. 11. The plain text character B is then added bitwise modulo two to the subtractor character, F say, and the result routed through the transposition circuit, which is controlled by the permutor character, I say. The resulting cipher text character is Z. The two key characters, F and I, are determined from the code wheel setting and the inner key configuration once the plain text character B enters the machine. In addition, the figure shows that an element of the transposition circuit, the transposition unit, is active when the controlling bit is 0 or, as BP said, a dot.

The analysis of the T52 key generator showed that the ten code wheels were combined in fours. They named this circuit the "Pentagon" after the shape of the graph that resulted when combining the different logic relationships given by this circuit. A more detailed explanation of the Pentagon is given in Part II.

The Pentagon was cryptographically a weak device. Only four different subtractors could be associated with a given permutation. Furthermore, the subtractor character was always even, i.e. the five code impulses always summed to zero. [1] Therefore the plain text character was even whenever the cipher text character was even, and odd whenever the cipher text character was odd. For the cryptanalyst this was similar to the Enigma's peculiarity that no letter can encipher to itself, and it was of great help in reading depths and placing cribs.

The first Sturgeon message to be read was at a depth of 40, an almost incredible depth, which clearly shows that the German operators had no idea of the detailed functioning of the machine and that they must have disobeyed

[3] Autokey or autoclave is where a part of the key is generated from the plain text or the cipher text.

[4] BP used the terms cross and dot to describe the Baudot code elements mark and space, logical 1 and 0.

orders or been wrongly instructed. Eventually, with the detailed knowledge of the limitations imposed by the Pentagon device, depths of four or five, i.e. four or five messages enciphered with identical machine settings, could be read fairly easily. The 10 code wheels were set once a day and this initial setting remained in force during the whole day. However, the machine was equipped with a small crank which allowed the operator to bring the machine back to its initial code wheel settings easily.

This was the main reason for the large number of messages in depth. With this knowledge, it was possible to read messages at depths of two or three as soon as the daily wheel settings had been recovered. When they could make a guess at a crib of about six letters even single messages could be broken with the help of the Pentagon limitations.

The different messages were sent using different wheel orders. There was some form of message key device that changed the connections between the code wheels and the Pentagon. However, as the machine was brought back to its initial position, the binary streams from each of the wheels were always the same. Five letters were given as a message key, and these always came from the reduced alphabet: P S T U W X Y Z. A letter could appear more than once in the group of five — once the indicator WWWWW was even observed. BP noticed that when two indicators agreed in n positions, then usually but not always, $2n$ of the wheels had the same function in the Pentagon. However, this rule did not apply to indicators sent on different days. The indicator system of this machine was never broken cryptanalytically.

Comparing the above description with what is known about the different Siemens T52 models it is evident that BP was confronted with the T52c machine. [10–12, 30–32] This machine had a code wheel combination logic like the one described for the Pentagon. It also had a message key unit with five levers that could be set in eight different positions indicated by the letters P S T U W X Y Z. Like the T52a/b, the c model also had the small crank that allowed the code wheels to be brought back to an index position. This was a conceptual error in this model as the main reason for this wheel resetting mechanism was to allow the operator to set the message key easily on the wheels. The T52a/b machines were not equipped with a message key unit like the T52c and therefore the message key was set directly on five of the code wheels. The 10 wheels were therefore brought back to the initial position and the five wheels selected as message key wheels would be set to their new position. It is debatable whether even this limited wheel resetting on the T52a/b was a good idea. However, it is evident that the complete wheel resetting used on the T52c machines was a blunder of some magnitude.

The Sturgeon and Mackerel links came to an end with the second battle of El Alamein which started at the end of October 1942. One other signal transmitted on a T52c machine was intercepted later in November. It was believed to have come from the Caucasus. It consisted of the usual messages in depth and was successfully attacked. The messages dealt with the situation on the Russian front. That was the last appearance of traffic from a T52c machine.

5 The German Use Of Q-Codes

In the first six months of 1943 other teleprinter links appeared which also used "UM UM". Some of the links were known to use the Tunny machine and from this moment it was often difficult to distinguish between links using the two machines. Both types of link gave only a QEP number for the indicator. The only exception to this rule was a link named Salmon where some groups of letters were sent, apparently as indicators.

QEP was a special German code added to the international set of abbreviations for radio operators, the so-called Q-codes, which are still in use. The code groups QRA to QUZ are meant for use by all radio services, while the groups QAA to QNZ are reserved for the aeronautical service and QOA to QQZ for the maritime service. However, many of the more obscure codes were given new meanings by the German operators. Many of the German codes dealt with the use of teleprinters and cipher machines. QEH meant *Handbetrib* — send by hand, while QES stood for *'Komme mit Sender'* — will use the tape transmitter. QEX meant *'Geben Sie Kaufenschleife'* — send a test tape, while QFL stood for *Fliegerangriff* — air raid. [19]

The codes referring to cipher machine use were QDL — QEP is set up, QDO — GKDOS (*Geheime Kommandosache* — Top Secret) traffic, QEO — officers key, QEP — cipher key specification, QGS — *G-Zusatz* (Tunny machine), QSN — former term for QEP, QSS — cipher transmission, QTQ — additional "limitation" in use and QZZ — daily key setting. In addition QEK was used to indicate which cipher machine to use. QEK alone meant SFM T52a/b, while QEKC stood for SFM T52c and QEKZ meant the Lorenz SZ40, Tunny. It is not known by this author which terms were used for the T52d and T52e machines, however, it is possible they would have used the codes QEKD and QEKE. The form of the QEP numbers and letters would depend on which cipher machine was used and the QEP details were given in the cipher instructions for each type of machine. As the cipher instructions changed so would also the format of the QEP setting change.

The Salomon indicators were quite different from the normal Sturgeon indicator groups. Messages on Salmon, which linked Königsberg and Mariupol, were intercepted from 11 January to 6 February 1943. The machine was of a much simpler construction than the Pentagon machine and there was no combination of the wheels. Five of the wheels made up the subtractor key while the other five wheels constituted the permutor key. The messages consisted mainly of operator chat.

Even though the new machine was simpler than the Pentagon machine (T52c), it was more difficult to break. The absence of the Pentagon meant that the parity of the cipher letter was no longer the same as the parity of the corresponding plain text letter. And instead of having only 60 different alphabets this new machine had 960. From this description it is evident that the machine must have been the T52a/b.

In May 1943, a new link, codenamed Sardine by BP, started to operate between Sicily and Sardinia. This link was never broken. Later in the year, two operator log books were captured which contained references to the intercepted traffic on the Sardine link. Time, numbers and priority codes corresponded to those of the intercepted traffic. Also the same type of *Luftwaffe* addresses that had earlier been used on Sturgeon appeared on this link.

A new link codenamed Halibut by BP appeared in July 1943. The link, which operated between Königsberg and Munich,[5] ceased to operate in August but reappeared in a changed form in 1944. In its first period, from July to August, a few depths of four and one of five were found. One depth of four from August was read and was found to have been enciphered in the same way as the depths that had earlier appeared on Salmon (T52a/b). Like the Salmon messages it consisted of operator chat. However, the July depth of five resisted all attempts to break it. It only succumbed a year later, in June 1944, to a sustained attack. It then turned out that it was enciphered on a new machine, the T52d.

6 A Historic Achievement

This break constituted the first break of the T52d machine, a machine similar in construction to the T52a/b but with irregular, stop-and-go, code wheel movements. The Halibut message did not use the autokey element, *Klartextfunktion*, of this machine but in June 1944 other Sturgeon links were suspected of using this machine with the autokey function. The break was nevertheless an outstanding achievement. The T52d was completely broken from reading a depth of five for a part of the message, while for the remainder it was only a depth of four. [18] From BP's subsequent analysis of the machine a depth of four appeared to be the absolute minimum. How was it possible to break such a complicated machine from only one message in depth of four and five? One answer is that BP was not confronted with a completely new machine. It was mainly the stop-and-go code wheel movements which differentiated this machine from the T52a/b. The code wheels themselves had the same patterns as on the T52a/b and T52c machines. It would turn out later that almost all the machines in the T52 series used the same code wheel patterns. The patterns were fixed and no changes were ever made to them. This constituted a very serious weakness of these machines.

[5] A list of FISH links in one of the Fried reports gives the link as operating between Memel and Königsberg. [16] However, as the distance between Memel (Klaipeda) and Königsberg is only 120 km, mainly over water, the use of an HF link does not sound right.

However, this is not the whole story. There did exist machines with different code wheels.

The break itself was a manual operation, but assisted by a large number of catalogues which showed the possible alphabets that resulted from an assumption of a plain-cipher text pair of characters. BP did not develop a machine to assist in deciphering. All the operations were done by hand so that even developing the subtractor and permutor keys from a given wheel order and setting was a very slow and tedious process. BP also tried to use masks and inverse probability calculations, but it is not known if this was successful. As will be shown later, the permutation circuit only produced 30 out of the 120 possible permutations. Thirty-two permutations should have been possible with the five double changeover contacts used for the permutation function, but / and Z produced identical permutations, as did T and E.[6]

Wheel		Controlled by
ID	Length	
K	47	E crosses, D dots[a]
J	53	K crosses, A dots
H	59	K dots, J crosses
G	61	J dots, H dots
F	64	H crosses, G crosses
E	65	G dots, F crosses
D	67	F dots, E dots
C	69	F dots, E dots
B	71	F dots, E dots
A	73	F dots, E dots

[a] Dot and cross are BP parlance for 0 and 1, space and mark.

Figure6. Wheel stopping logic for T52d.

The break was a success, but it also showed the difficulty this machine presented cryptanalytically. BP launched a substantial research effort to understand the T52d machine fully and to explore possible cryptanalytical attacks against it. BP realised that solutions through depths could not be relied upon in the future because of the increasing use of the autokey function. Another problem that presented itself was how to differentiate between this traffic and ordinary FISH traffic generated by the Lorenz SZ40/42 machines. BP hoped to find statistical techniques that would allow it to identify the traffic.

[6] BP replaced the six teleprinter control characters *carriage return*, *line feed*, *letter* and *figure shift*, *space*, and *null* with the special characters *3,4,8,+,9,* and */*. See the teleprinter alphabet in Fig. 11 and Appendix A of [40].

It is not known how long the July 1943 message was but it is nevertheless an extraordinary feat to have fully deduced the "motor wheel" logic of the T52d. In contrast with the Lorenz SZ40/42, the T52d did not have separate "motor wheels." Instead, each "motor" was formed by the modulo two addition of two other wheels, sometimes with inverted logic for one or both of the wheels. The "motor" or wheel stopping patterns were read from a different part of the code wheels than those used for the subtractor and permutor keys. And of course the movement of these wheels was again controlled by others. Four of the wheels, with the lengths 73, 71, 69 and 67, were controlled in parallel by two of the other wheels. This was presumably done to ensure a periodicity of at least $73 \cdot 71 \cdot 69 \cdot 67 = 23\,961\,009$. The wheel stopping logic as derived cryptanalytically by BP is given in Fig. 6. [17] The figure shows how the movement of a given wheel depends on two other wheels, e.g. the K wheel, which is the leftmost wheel in the machine and with a sequence length of 47, will not move if there is a cross (1) on the E wheel and a dot (0) on the D wheel. The other wheels have similar relationships to two other wheels.

The deciphered messages referred to experiments with a machine the operators called T52d, which gave BP the final proof that it had broken a new Sturgeon model. Later two captured T52d machines were found to contain the same logic as had been derived cryptanalytically from the Halibut message.

7 Insecure Use and New Wheels

In September 1943, the link named Conger appeared between Athens and Berlin. Hundreds of messages were sent and all were in depth so there was no great difficulty in reading them. However, their intelligence value was nil. The messages contained only operator chat.

Conger contained references to the T52b, a machine that had previously been captured in Tunisia. By correlating the recovered code wheel sequences with those of the actual machine it was found that the initial position corresponded to that of all wheels set to one. The wheels were used in the order of their periods, while the operation of the machine corresponded to what had earlier been observed on Salmon, and in the August Halibut messages. In November, similar Conger messages in depth were sent; this time the wheels were all set to two.

The description of the Conger usage is frankly amazing and shows a complete disregard for applying secure keying instructions for the machines. It would seem that the machines were used by operators who had never read the instructions and who had not been issued with operational keys for these machines. One also gets the very strong impression that the majority of these links were not operational links, but reserve channels kept open mainly with operator chat and test messages. However, their usage was cryptographically damaging to the machines.

Both Conger and Halibut reappeared early in 1944 in a slightly changed form. The new Halibut messages were all short, while earlier they had often been very long. Conger, on the other hand, often contained long messages. Depths, in this case messages with the same QEP number, of up to four occurred. However, the messages had no repeats, which strongly indicated that the autokey function was being used. This hypothesis was further supported by the intercept logs which contained phrases like "*Mit KTF*" and "*Ohne KTF*" where KTF was the abbreviation for "*Klar Text Funktion*". BP did find one depth of two without the autokey function, but a depth of two was considered to be unbreakable.

Shortly afterwards it was decided to cease the interception of links using the Sturgeon machines as it was considered to be unprofitable. In the autumn of 1944 many Tunny links, which also used an autokey element, ceased to use this function and Enigma messages were found ordering the Sturgeon operators to stop using autokey on the T52d and T52e machines. During the same period, one day's traffic on Conger was intercepted. It was found to be in depth of two and without the autokey function. However, there are no further indications that a lot of effort was invested in the Sturgeon machines and their traffic.

As mentioned above there existed machines which had different code wheels from those used on the standard T52 machines. The Swedish cryptanalysts detected altogether three other machines that were different from the machines used on the main German Air Force (*Luftwaffe*) and Navy circuits. The normal code wheels were called the B-wheels by the Swedes.[7] In August 1940 the Swedes broke a T52a/b machine which used different code wheels and which they named the D-wheels. This machine was in use for a relatively short period and the traffic consisted of personal messages to military personnel in Norway. The last message was intercepted and broken on 11 February 1941. In April 1941 they broke into a T52a/b machine with a new set of wheels which they called SB1. The machine was used for diplomatic traffic. In June 1943 the machine was changed to a SFM T52ca but it kept the SB1-wheels. And finally in January 1943 they discovered yet another T52a/b with different code wheels. These wheels they named the E-wheels and the machine was used for transmitting police traffic. The machine was only observed once over a period of a few days.

Therefore Wolfgang Mache's earlier reports of German teleprinter technicians who changed SFM T52 wheels seems to be correct. However, neither Swedish nor Allied documents support his claim that the T52 wheels were changed every six month. [32] The B-wheel patterns that were first used on the T52a/b machines in 1940 were still in use on the T52e machine at the end of the war. From the Swedish observations of machines with different code wheels it is very tempting to draw the conclusion that the reason for the change was to protect the traffic on these circuits from other legitimate

[7] Some of the information about the different code wheels has been provided by Bengt Beckman (private communications). Further details are from Lars Carlbom. [9]

T52 users. Hence the change of code wheels was not made to increase the security of the T52 machines.

8 The Captures

The first Sturgeon machine to be captured was a T52b which was found in Tunisia. It was discovered that the code wheels on this machine moved regularly and that they did not combine. It was therefore evident to BP that it was not the Pentagon machine (the first Sturgeon type of machine to be intercepted and broken).

Later a full technical description of a machine which combined the functions of the T52a/b and T52c was captured on Elba. It appeared from this description that the T52c machine was related to the Pentagon machine as it combined the code wheels in fours. However, the number of alphabets was found to be 256 instead of 60 as for the Pentagon machine. It will be shown later that this T52c machine was the modified version, T52ca. The T52a/b mode showed that the machine could have been used for the Salmon, August Halibut messages and the early Conger traffic.

The Elba description also showed that the T52c machine was equipped with a wheel permuting mechanism corresponding to the message key unit described earlier. It was found that the unit consisted of five levers each of which controlled three switches out of a set of 15. Each switch interchanged two wheels in its active position and left their order unaffected in the inactive position. A switch was active or inactive depending on the position of the controlling lever, but the correlation of active switch position and lever position was different for the three switches controlled by a given lever. This circuit has been described in Donald Davies' paper on the T52 machines. [11]

In addition, it was found that all the machines were equipped with a set of switches or plugs which constituted the main inner key setting. The switches or plugs selected which of the ten code wheels controlled a given function in the cryptographic process. After the capture of the Elba description, an actual machine of this type was captured at Naples. This was clearly a T52c machine, but the message key unit with the five levers had been removed. It was noted that the machine was very similar to the first captured T52b machine; the T52b also had room for a message key unit although none was actually fitted. Yet another machine was captured at Naples. On this machine the original type number, T52b, had been altered to T52d. This machine was equipped with the wheel stopping logic and had a switch to enable or disable the autokey function KTF. Without KTF the code wheels had the same movement as the one derived cryptanalytically from the July Halibut message. When the KTF was active, the wheel movement logic became more symmetrical and the third impulse of the clear text governed part of the logic. Two of the wheels were controlled by a plain text cross (1), while two others were controlled by a dot (0). This logic has also been described in detail by Donald Davies. [10–12]

Later yet another T52d machine was captured, which had been altered from a T52a. Comparing this machine with the T52b, it became obvious that the two models must have been very similar. It is known from German sources that the only real difference between the two machines was that the T52b was fitted with extra filters to reduce interference to radio installations. [31, 34]

Together with the T52c machine description captured at Elba, allied forces also captured two key book pages, one for the T52d, and one for the T52a/b and T52c machine. One side of each page gave the table for 3 June 1944, while on the other side was the table for 4 June. Each table consisted of 25 rows labelled with the letters from A to Z, omitting J. A similar table for the T52d/e machine is reproduced in Appendix A. The message key QEP FF OO PP AA ZZ VV CC MM HH UU corresponded to setting the leftmost code wheel to 19, as can be found in column 1, row F. The wheel to its right is set to 11 as given in column 2, row O etc. The complete code wheel setting for this message key was: 19 11 56 31 59 33 13 46 02 25.

The corresponding table for the T52c machine is reproduced in Appendix B. The same method of indicating the code wheel setting applies to this table, but in addition the lever settings for the message key unit are in the first five columns. The same QEP message as above would give the code wheel settings: 47 23 09 27 34 45 26 09 02 48 here, with the message key levers at: p t p s x. The use of these tables and the method of disguising the code wheel settings that were transmitted as QEP numbers or letters changed several times throughout the war, but the tables themselves largely retained their original structure and layout. The main instructions for the use of teleprinter cipher machines, *Wehrmacht Schlüsselfernschreibvorschrift (SFV)* [14], indicate there were three basic key tables in use, *Fernschreibgrundschlüssel* (main inner key), *Fernschreibwalzenschlüssel* (code wheel key), and *Fernschreibspruchschlüssel* (message key). An example of the *Fernschreibgrundschlüssel* for the T52d is reproduced in Appendix C.

9 German Security Alarms

References to the Sturgeon machines were frequent in both Tunny and Enigma traffic. In 1942 the decodes referred only to the T52a/b and T52c machines. The *Wehrmacht SFV* as referred to above was issued on 1 December 1942 and also refers only to the T52a/b, T52c and SZ40 type of cipher machines. It is therefore very likely that these were the only machines available in 1942. BP also appears to have captured a copy of the *Wehrmacht* instructions some time before November 1944.

On 17 October 1942 a message[8] from C.S.O.[9] *Luftflotte 2* to *Fliegerführer Afrika* mentioned that T52c had inadequate security. It gave orders that

[8] Message on the *Luftwaffe's* Red (the main Air Force) key, 121-2-3, 17/10, 6610. The author has so far not been able to trace any of these messages.

[9] C.S.O. = Chief Signal Officer.

"Secret" and "Secret Commands Only" (probably a translation of *Geheime Kommandosache* — Top Secret) are to be enciphered on Enigma before being sent over *Sägefisch* (Sawfish) links.

This message passed between stations served by the Sturgeon link using the T52c machine. Nevertheless, seemingly important messages continued to pass over this link without being previously enciphered on the Enigma. However, many Enigma messages also passed over this link before it ceased operation on 2 November 1942.

This message doubting the security of the T52c stands in contrast with the *Wehrmacht SFV* which contains a clear instruction not to use the T52a/b over radio and radio relay connections (*Richtstrahlverbindungen*). The T52c was the only machine authorized for use over radio and radio relay links. However, we have seen that the *Luftwaffe* for some reason did not obey these instructions and that they used the T52b machine for practice messages on the Salmon, Halibut and Conger links. This shows that *Luftwaffe* cipher officers must have been unaware of the close links and similarities between the different T52 models and that they did not see the danger these practice transmissions were to the other machines.

In February 1943, decodes show that the Germans suddenly had discovered that something was seriously wrong with their *Sägefisch* machines. A message from Madrid to Paris[10] said that the T52 was very badly compromised and that enemy decipherment was possible. "Secret" and "Top Secret" messages were no longer to be sent over the T52.

On 18 February 1943, a new set of instructions for using the T52 machines was issued:[11]

1. The indicator systems in use with the T52a/b and c are cancelled.
2. Henceforth the ten wheel settings are to be given instead and sent on a specific emergency key.
3. A new method of indicating the settings of the five message key levers is to be used.
4. The device for setting back all the wheels to the so-called zero position is to be removed.

Point four of these new instructions shows that the Germans had finally discovered the faulty operator practice of sending many messages on the same key due to the facility for doing so offered by the T52 wheel resetting mechanism. Apparently they also suspected some weakness in the use of the message key procedure and therefore introduced new, temporary measures. They would later abandon the use of QEP numbers and use the QEP structure with ten bigrams that has been described in the previous section. It is not clear why this was considered a better procedure but it is possible it

[10] Message on the *Abwehr* link Madrid–Paris, RSS 6713/2/43.
[11] Message on the Army's Bullfinch II (Italy) key, 1735/18/2/43.

offered more flexibility in choosing message keys than the previous method using QEP numbers.

On 19 February, yet another message[12] gave further instructions:

1. T52a/b is not to be used for "Secret" and "Top Secret" messages, except when other means are not available.
2. If teleprinter links are used there must be previous encipherment on Enigma.
3. After the changes to the T52c, and after a change in the indicator system, "Secret" and "Top Secret" messages may again be forwarded without previous encipherment on Enigma.

In March two messages[13] said that traffic on the *Aptierte*[14] (adapted) T52c no longer needed to be first enciphered on the Enigma. From then on there were references to the T52ca, which probably stands for T52c *Aptierte*. Then finally on 14 June 1943 there was a message[15] to the Naval Communications Officer in Sulina and other addressees that said: "On the completion of the adaptation to SFM T52c, the designation T52ca will no longer be used. The designation T52c only is to be used from now on." The changes made to the T52c concerned the wheel combining logic which BP had found to be of such great help when breaking the Pentagon machine. This indicates that the Germans must have made a detailed analysis of the machine and found this part of the logic to be particularly weak.

The German security evaluations and analysis of their own cipher machines have not yet been fully declassified and released. It is therefore not yet possible to give a detailed picture of what the Germans knew and suspected with respect to the security of their crypto systems. However, it is known that Dr. Erich Hüttenhain, the chief of the cryptanalytic research section of OKW/Chi (*Oberkommando der Wehrmacht/Chiffrierabteilung*), examined the T52a/b machine in 1939. [5] He found that this machine had an extraordinarily low degree of security and could be broken with about hundred letters of cipher text without a crib.[16]

One hundred letters of cipher text seems an extremely low figure. It does not correlate well with the amount the Swedish codebreakers used to break this machine. Unfortunately TICOM[17] report I–31 has not yet been declassified. It is therefore impossible to tell if this figure is an error or if it refers to the length needed for an attack under some special conditions. Another

[12] Message on the Army's Merlin (Southern Europe) key, 19/2/43.
[13] Message on the *Luftwaffe's* Red key, Nos. 322/4 and 387/7 of 6 March 1943.
[14] *Aptierte*, as given in the BP reports, is not a German word. It is possible it is a typing error for *Adaptierte* which does mean adapted.
[15] Naval message 14/6/43, 77, Mediterranean.
[16] TICOM Report I–31: "Detailed Interrogation of Dr. Hüttenhain, formerly head of research section of OKW/Chi, 18–21 June 1945."
[17] TICOM — Target Intelligence Committee.

TICOM report, based on a paper written jointly by Dr. Fricke[18] and Dr. Hüttenhain, shows that the T52a/b could be broken given an enciphered text of 1000 letters. [15] This seems a much more realistic figure. For this attack to succeed an a priori knowledge of the code wheel patterns was necessary. To also derive the code wheel patterns they estimated they would need about 2000–3000 letters of cipher text. If they had access to several messages in depth, each of 2000–3000 letters, the solution would be greatly simplified.

This study could have resulted in the *Wehrmacht SFV* instruction prohibiting the use of the T52a/b on any form of radio channel. However, it is perhaps more likely the discovery by the Germans on 17 June 1942 of the Swedish success in breaking this machine led to the restriction. [40] OKW/Chi suggested changes in the machine, including ways of producing non-uniform code wheel stepping but for engineering reasons Siemens refused to accept these changes. Instead a new machine, the T52c, was produced which overcame some of the more obvious weaknesses of the earlier model. The T52c was studied by the Army cryptanalyst, Doering, from OKH/Gen d Na (*Oberkommando des Heeres/General der Nachrichten Aufklärung*) in 1942. He showed that it could be broken on a text of 1 000 letters. This study was apparently assisted by cryptanalytical machinery in use by OKW/Chi, but it is not known how involved Dr. Hüttenhain and his people were in the actual study and its recommendations. The investigations resulted in the design and production of the T52d. The security analysis of the T52d was continued, mainly by Doering, and early in 1943 he showed that this machine was also insecure. This resulted in the production of the T52e. However, it was known that both the T52d and T52e machines were open to attacks through messages in depth and that at a depth of ten messages could be read without a crib.

However, the cries of alarm from the German cryptographers were not heard, or at least not acted on, by the German Army and Air Force. In the summer of 1942 the totally insecure model T52a/b was still in use and the equally insecure T52c was being distributed. The Army's position was that the teleprinter traffic went over land lines and could not be intercepted, hence there were no need to worry about inadequate security. Evidence of tapping of the teleprinter lines that appeared in Paris in 1942 and 1943 gave the Army a serious jolt and the Army's signal authorities were forced to reconsider their views on teleprinter cipher security. However, it was too late and the newly developed T52e was only slowly being introduced at the end of 1944. The first reference to the T52d machine appeared in the decodes in October 1943.[19] Subsequently, there were frequent references to all three models, T52 a/b, c, and d. From September 1944 onwards, there were also references to the newly

[18] Sonderführer Dr. Fricke was the leader of OKW/Chi's Referat (Department) IIb that was responsible for the development of German code and cipher systems and the production of cipher keys.

[19] Message on the *Luftwaffe's* Red key, 279/0, 4/10/43.

developed machine T52e. Traffic from this machine was never observed or at least identified as such by any of the allied cryptanalytical services and the machine remained unknown to them until the end of the war.

10 FISH Links

Given the rather poor intelligence content of the Sturgeon messages we are left with the question: Did BP capture and break it all? This is still very much an open question but there are some indications that perhaps many of the more important links were never broken. We have already underlined that BP had big difficulties in differentiating between the Tunny (SZ42) and the Sturgeon traffic, but generally they were able to identify whether a link belonged to the German Army, the Air Force or the Navy. On 21 January 1944 SIXTA, BP's traffic analysis section, compiled a list of Non-Morse call signs and frequencies that had been observed in the period 1 November 1943 to 10 January 1944. [36] The list consists of two parts, the first dealing with the regular Germany Army Tunny links while the second part, which is shown in Fig. 7, lists the German Air Force links.

Link Name	Stations	Number of Frequencies
Anchovy	Königsberg – Paris	Not available
Bass	Königsberg – Salonika	Total: 6
Carp	Not indicated	Total: 13
Conger	Berlin – Athens	Berlin: 17, Athens: 7
Goldfish	Oslo – Kemi	Oslo: 4, Kemi: 5
Gudgeon	Salonika – N.E. Italy	Total: 16
Pilchard	Berlin – Lemberg (?)	Berlin: 3, Lemberg: 5
Barbel	Belgrade (?) – Athens (?)	Total: 7

Figure7. Early German Air Force links.

On 20 January 1944, Captain John N. Seaman from the US Signal Corps compiled a list of FISH links with the amount of traffic for the month of January and the beginning of Feburary. An extract of this list with the traffic figures for the German Air Force links is given in Fig. 8. [36] A link was considered potentially breakable if the messages were longer than a given minimum length. The value for Carp was 2500 characters.

In September 1944, the German Air Force circuits were further refined and the links set out in Fig. 9, were better defined. The picture is complicated by the fact that some of these links might have used the German Army machine Tunny (SZ42) for their communications. It is known that Carp (Königsberg – Italy) was using the SZ42 and had been broken until it started to use the

Link Name	Station	Traffic in 1944		Potentially breakable
		January	Feb. 7–13	
Anchovy	Paris	9	18	0
	Königsberg	114	30	0
Carp	Königsberg	1572	274	0
	Italy	1282	69	1
Goldfish	Oslo	96	13	0
	Kemi	114	30	0
Gudgeon	Italy	493	—	—
	Salonika	253	—	—
Barbel	Berlin	14	6	0

Figure8. German Air Force traffic.

Link Name	Stations	Remarks
Anchovy	Biesental – L.FL. 3	Biesental: 30km N. of Berlin, Luftflotte 3 (*"Wehrwolf"*)
Barbel 1	Belgrade – Athens	Belgrade: Pancevo (*"Konsul"*)
Barbel 2	Berlin – Belgrade	Belgrade: *Lw. Kdo. Suedost*
Barbel 4	Berlin – Athens	
Barbel 5	Berlin – Oslo	Oslo: *Luftflotte 5*
Bass	Königsberg – Belgrade	
Carp	Königsberg – Italy	Italy: *Luftflotte 2*
Char	Biesental – Riga	Riga: *Luftflotte 1* (*"Standarte 4"*)
Dab	Biesental – Wiesbaden	Wiesbaden: *Fliegerkorps X*
Goldfish	Oslo – Kemi	Oslo: *Eskimo 1, L.FL. 5* Kemi: *Eskimo 4, L.FL. 5*
Gudgeon	Belgrade – Italy	Italy: *Luftflotte 2*
Hake 1	Treuenbrietzen – Poznan	Treuenbrietzen: 60 km SW of Berlin
Hake 2	Treuenbrietzen – Bucharest	
Stingray	Hannover – Nürnberg	Not known if Army or Air Force

Figure9. German Air Force links in September 1944.

P5 limitation.[20] It is possible that the other Königsberg link, Bass operated by the same *Sägefischtrupp 8* — also called "Robinson 6", was also using the Tunny machine. However, it is known that several of the other links used the Siemens T52 or T43 machines. In August 1945, the British Air Disarmament Wing No. 8801 was operating in Norway and one of its tasks was to dismantle

[20] The P5 limitation was BP's name for adding the 5th plain text element to the Tunny key stream similar to what was done by the T52's autokey function

the *Luftwaffe's Sägefisch* stations. [35] In all the disarmament teams visited at least three such radio stations. Their location and equipment are shown in Fig. 10.

Name	Location	Links	Cipher machines
Skedsmo	Oslo	Oslo – Trondheim Oslo – Bardufoss Oslo – Flensburg	SFM T43: 4 SFM T52d: 3
Tuftan	Trondheim	Trondheim – Oslo Trondheim – Bardufoss	SFM T52d: 2
Bardufoss	North Norway	Bardufoss – Oslo	SFM T43: 2 SFM D1: 2

Figure10. Norwegian *Sägefisch* stations.

The equipment SFM D1 found at Bardufoss station is completely unknown but it is quite possible that it was an SFM T52d which somehow has been wrongly identified or listed by the men in Air Disarmament Wing 8801. The station at Oslo, Skedsmo, maintained the link with Kemi in Finland. The equipment list shows that these links used only the SFM T52d and the one-time-tape machine T43. However, it is impossible to know if the equipment situation at the end of the war really reflected the situation in 1944. The one-time-tape machine, SFM T43, was progressively introduced towards the end of the war. Unfortunately we do not know what proportion of the traffic was sent over this machine. Some of the Air Force links clearly were operational links and must have carried operational traffic. However, with the limited information we possess about the traffic and the possible use of the unbreakable T43 machine, we cannot draw any firm conclusions. It nevertheless appears that BP took the right decision when deciding to abandon the Sturgeon traffic and allocate its cryptanalytical resources to other more promising targets.

11 Indiscretions Among Friends

When BP first detected and subsequently broke into the Sturgeon traffic did it know of the Swedish success against the SFM T52? This question has been raised several times but has never been given a satisfactory answer. That Swedish Intelligence had a source of unprecedented reliability and which had access to the highest level of military and diplomatic intelligence became clear to BP and British Intelligence already in 1941.

When Captain Henry M. Denham took up his post as the naval attaché at the British embassy in Stockholm in June 1940 he quickly set out to become friends with important Swedish military and intelligence personnel. One of these high level officers was Colonel Carl Björnstjerna, the chief of Foreign Intelligence at the Swedish General Staff. They met frequently and Captain Denham regularly obtained important information from Colonel Björnstjerna about naval developments in the Baltic and the North Sea. However, Captain Denham also had regular contact with several of his fellow attaché colleagues from other countries. One of these officers was the Norwegian military attaché, Colonel Ragnvald Alfred Roscher Lund, who came to Stockholm in March 1941. Colonel Roscher Lund was Norway's chief intelligence officer who in 1935 started courses in cryptography and then created Norway's first signal intelligence and cipher office. Very early on he made contact with the Swedish cryptanalysts, who were already quite advanced in this special field. He quickly became a close friend of one of Sweden's most famous cryptanalysts, Yves Gyldén. Roscher Lund, who made frequent trips to Sweden before the war, was well known in Swedish military circles and was held in high esteem by those who met him.

Roscher Lund's connections with Swedish military officers seem to have paid off during the Bismarck affair. He was alerted to the sighting of the battleship by his friend Captain Ternberg, who was the Chief of Staff to the head of the Swedish Intelligence Service. Roscher Lund immediately informed Captain Denham who again would alert the British Admiralty. This incident does not seem to have originated in information from the German Geheimschreiber traffic, but other intelligence clearly came from this most precious source. It is not clear if BP had irrefutable evidence that the intelligence Captain Denham obtained from his Swedish sources came from German teleprinter traffic passing over Swedish telegraph lines. However, British Intelligence apparently knew or strongly suspected that the information came from codebreaking. In his book about his years in Sweden during the war Captain Denham mentions several times that the intelligence must have come from codebreaking. [13]

However, in 1942, British Intelligence seems to have known the source of the Swedish Intelligence. As Sir Harry Hinsley explains: "On 18 June, however, it received from the Naval Attaché Stockholm an account of how the Germans planned to attack the next Arctic convoy with U-boats, air forces and two groups of surface ships." [21] In a footnote Hinsley explains the provenance of this information. "This was the first information obtained from a source subsequently graded A2 by the Admiralty (Enigma was graded A1) via the Naval Attaché in Stockholm. He had succeeded at this point in obtaining via the Deputy Chief of the Swedish Combined Intelligence Staff decrypts of German operational orders passing from Berlin to the German naval commands in Norway by land line, presumably in the FISH cypher."[21]

Somehow the source of the Swedish Intelligence would appear to have been revealed. It has been claimed that Colonel Björnstjerna never revealed

[21] Hinsley et al. gives C. Morgan's "NID History 1939–1942" — ADM 223/64, as the source for this information.

the true source of his information and this is probably correct. However, Colonel Roscher Lund was informed about the deciphering of the German teleprinter messages passing over Swedish land lines. Colonel Roscher Lund rapidly became an important source of information to the British and when he was ordered to travel to London to organise the Norwegian intelligence office there it was immediate consternation in British circles. On 10 September 1941 Winston Churchill sent a letter to the Norwegian prime minister, Johan Nygaardsvold, and asking him to reconsider his decision to move Roscher Lund from Stockholm. Churchill wrote: "This officer has been of great service to the British Intelligence organization in Sweden, and his presence there is of special value to His Majesty' Government, and to the Allied Cause as a whole... I sincerely hope that your Excellency and your colleagues may feel able to reverse the decision which has been taken. It is a matter to which I attach great importance." [41]

However, Nygaardsvold maintained his decision to transfer Roscher Lund to London. He arrived in London on 12 October 1941 and took office in the Norwegian exile government's headquarters in Kingston House, Knightsbridge. Within a month Colonel Roscher Lund asked a Captain Howard if he could help him with resolving questions the Norwegians had about the security of their Hagelin machines. They had heard rumours, originating from British sources, that the cipher machine was unsafe and was being read. At the insistence of Captain Howard, one of the British cryptanalysts from Major John Tiltman's section in Elmer's School at Bletchley Park went to London on 14 November and met Roscher Lund for lunch at the Royal Automobile Club. After lunch the unknown cryptanalyst accompanied Roscher Lund to Kingston House where he was introduced to the Commercial Counsellor Johan G. Ræder and Erling Quande who was the chief of the cipher office in London. The BP man was shown the Hagelin machines being used by the Norwegian exile government and again the questions about cipher security were discussed. During these more detailed discussions Colonel Roscher Lund, who perhaps wanted to show the cryptanalyst that he was talking to fellow cipher experts, gave an overview of his and his colleague's experiences in this field. The explanations he gave included details about his contacts with the Swedish and Finnish cipher bureaux. He estimated the personnel in the Swedish Cryptographic Bureau to be about 150 and designated Yves Gyldén as head of the this office.[22] He described Gyldén as Europe's greatest cryptanalyst but finally confined his greatness to Scandinavia. In his report the BP cryptanalyst says: "The Swedish Bureau had had considerable success in their attacks on French cyphers and which he [Roscher Lund] put at 95%, Italian military 85%, and fair progress on the German cyphers. Lund said the Germans were sending masses of messages to their troops in the north

[22] In 1941 the real chief of the Crypto Department of the Swedish Defense Staff was Commander Torgil Thorén, who had taken over as chief from Eskil Gester in the autumn of 1940. Yves Gyldén was the leader of the French section.

of Norway by teleprinter and that the telephone manufacturing firm L. M. Ericsson had built a machine which decyphered these messages which dealt mainly with personnel and administration." [2]

This is a most explicit reference to the Swedish success in breaking the German Geheimschreiber (T52) machines and it even correctly names the manufacturer of the deciphering machines. From what Colonel Roscher Lund said and from the knowledge that he was on very friendly terms with Yves Gyldén it is most likely that this most secret information came from him. Swedish cryptanalytical security probably did not suffer any harm, however it clearly illustrates the danger of "loose" talk, even among friends. He also spoke in great detail about the Finnish cryptanalyst Reino Hallamaa and his success in breaking Russian codes and ciphers. Colonel Roscher Lund was obviously trying to bargain some of his cryptographic secrets in exchange for obtaining help from the British in securing Norwegian communications.

At least Roscher Lund succeeded in impressing his guest about his sincerity. The BP cryptanalyst concluded his report with the following words: "Major Lund gave me the impression of being most anxious to help the British Government, and having regard to the rumours referred to his concern about the security of the Hagelin machine was quite genuine. I would therefore like to suggest that the appropriate steps be taken to put Major Lund's mind at rest on this matter." If Colonel Roscher Lund got the information he wanted is not known. What he did get was an OBE for his services to British Intelligence.

12 Sturgeon, A Modern Phoenix

The Siemens T52 machine was not the only cipher machine that rose from the ashes of the the Third Reich after the end of the war. The Enigma in its many variations was used by several countries for many, many years. Most of the countries belonged to the western powers like Norway where the Enigma was used by the Security Police (*Overvåkingstjenesten*) until the 1960's. [20] But the Enigma was also used by at least one of the Warsaw Pact countries, the new enemy. Perhaps the most prominent example is the Enigma machine which was used by the East German State Police, the notorious Stasi. It is not known when the East Germans started to use the Enigma or for how long it was in use, but a US Armed Forces Security Agency document describing the deciphering process is dated 22 May 1952.[23] [28] This seems to fit well with the report that some US Navy Bombes, the Enigma codebreaking machines, were taken out of storage and put back into service.[24]

[23] The document titled "Deciphering on the M8" and marked Top Secret Suede is itself undated. However, it is written on the ASA Form 781-C10S with the date 6 Jul 1951. In the margin it carries the handwritten note: "Used for deciphering E. German Police Enigma on the tape-printing Sigaba. Not applicable to other machines being used as ?. 22-May 1952. MKS"

[24] Private communication.

However, the Sturgeon machine created a lot more interest among its prospective users than the Enigma. The Siemens T52 was a much more complete and modern design and in addition it could be directly connected to modern telecommunication lines. Probably the first country to consider the machine for use was Britain. In September 1945 the Royal Air Force had already started service trials with the machine. Their aim was expressed in the following way: [3]

> In accordance with the Minutes of a Meeting to discuss the policy regarding radio teleprinting in the Royal Air Force, held at Air Ministry, Whitehall, on Friday 7th September, 1945, it is desired to determine the suitability of the *G. Schreiber*[25] as a cypher machine or as a scrambler device associated with either landline or radio circuits. Arrangements are to be made to carry out service trials of this machine on a similar basis to those conducted for the GP 28.

The cipher machine GP 28, which had been delivered to the Royal Air Force from the Telecommunication Research Establishment at Malvern, had already undergone service trials in June and July 1945 and the final report was submitted to the Air Ministry in August. The *G. Schreiber* trials started in early October and were completed in November. The final verdict was:

> Tests on the *G. Schreiber* equipment were completed during the month and reports rendered to Air Ministry. It was decided at Air Ministry that the equipment should not be brought into use on RAF radio circuits.

Unfortunately the detailed test reports have not been found and it is not known if the negative outcome was due to cryptographic security considerations or simply because it was unsuited for its intednded service.

However, other countries were a lot more receptive to Sturgeon's charms. In 1946, the Norwegian Cipher Office under the leadership of Captain Nils Stordahl started to test and modify the T52d and T52e machines which were left behind in Norway. [37] About 50 machines were modified, a number of which were used to encipher the teleprinter communications between the Security Police's headquarters in Oslo and their regional outstations. The total number of machines may have been as high as 70. This is the number of *G. Schreibers* that the Air Disarmament Wing No. 8801 had prepared for transfer to England. However, in a meeting between Royal Air Force officers and Norwegian Post Office personnel, which took place in Oslo on 8 September 1945, it was agreed to leave all or at least a major part of the

[25] The *G. Schreiber* is not clearly identified as the SFM T52. The possibility therefore exists that they confused the term *G. Schreiber* to mean the Lorenz SZ42. However, as this machine was less secure than the SFM T52d it is very unlikely it would have been adopted for service trials.

Geheimschreibers with the Norwegians. [35] Other SFM T52 machines were used by the Norwegian Intelligence Service (*Etterretningstjenesten*) for their internal communications and a few machines were given to Sweden to protect the intelligence link which existed between Oslo and Stockholm.

Wolfgang Mache mentions that about 380 SFM T52 machines survived at the end of the war, the greatest number being in Germany. The majority of the machines were collected at the Post Office central store in Elmshorn, formerly the communication equipment arsenal of the German Navy, where there were about 280 SFM T52 machines and a few SFM T43. The machines were meant to have been destroyed or demilitarised but apparently they were only dismantled. [32] From 1948 onwards the electromechanical firm Willi Reichert[26] in Trier started to rebuild SFM T52d and T52e machines from a large stock of T52 parts. Possibly these are the dismantled parts from the Post Office's Elmshorn store. In the period 1949–1953[27] Willi Reichert delivered more than 235 T52 machines to the French Foreign Office and other French military organisations. [32] The French undoubtedly were the largest user of SFM T52 machines after the war.

The Dutch Navy also found the SFM T52 to be an attractive machine and used a number of them in the 1950's. It is not known where the Dutch Navy used their SFM T52 machines but possibly on links between land stations in The Netherlands and perhaps on links to their stations in Indonesia.

The East Germans also showed an interest in the SFM T52. In April 1951 the East German State Police, Stasi, already had an extensive teleprinter network consisting of six main centres servicing a total of 48 stations. The equipment consisted mainly of teleprinters, hand perforators, and tape transmitters and receivers from Siemens, Lorenz and Olivetti. However, as far as we know they did not use any on-line ciphering equipment. Instead they enciphered all their teleprinter messages by hand using a manual cipher called TAPIR. [33] Letters, numbers, signs and all the special teleprinter characters were first encoded using a five by ten encoding rectangle. The resulting numbers were set out in groups of five which were superenciphered by adding five-digit numbers from an additive book that was valid for a given teleprinter link. This must have been a long and tedious procedure and it very much negated the advantages of using teleprinter communications.

In July 1951 a United States Intelligence report on "Communications in the Soviet Zone of Germany" described the interest the East Germans showed in the T52 machines. [26] A former Siemens employee, who during the war had assembled the SFM T52 machines and who remained with Siemens in East Berlin until 1947, subsequently entered the communication service of

[26] The name of the firm was Willi Reichert, *Elektronik und Electromechanik*, Trier, Petrisberg. Later it was called Willi Reichert, *Werkstätten für Radio- und Fernmeldetechnik*, Trier, Güterstrasse 1.

[27] Some electrical drawings for the SFM T52d and which carry the name of Willi Reichert's firm are marked with the dates 22 Feb. 1957, 3 Sept. 1959 and 29 Sept. 1959. This seems to indicate a continued interest in the machine.

the *Volkspolizei* (People's Police). Before his defection to West Berlin, he was approached by German communist officials regarding his opinion on the feasibility of manufacturing the T52e machines at the former Siemens plant in Chemnitz. The idea apparently was to buy a model of the SFM T52e in the Western Zone and an engineer was given such a task. How successful he was in procuring a machine and if any machines were ever built is not known. Generally speaking, we do not know too many details about the post-war history of the Sturgeon machines. Hopefully the relevant documents will be released in the not too distant future which should allow us to complete the history of the SFM T52 machines.

13 Conclusion

Not only did Bletchley Park intercept traffic enciphered on the Siemens SFM T52, but it also broke all the different models that it discovered. However, it was clear from the very beginning that the T52 was a very difficult machine to break. It probably would have remained unbroken had it not been for the German security blunders in using the machines. The blame should not be put entirely on the German teleprinter operators. The Siemens designers of the machine are equally responsible for not listening to the advice of the German cryptographic experts. The Siemens engineers appear to have been more focused on the engineering problems than on the cryptographic security of the machine. The T52a/b and the original T52c machines were basically machines with limited security. The T52c is an extraordinary example of how not to go about designing cryptographic algorithms. The wheel combining logic, which clearly was meant to strengthen the machine, had exactly the opposite effect — it eased the task of breaking the machine.

On the other hand, the T52d was a relatively well-designed machine. If this machine been the first to see service and the teleprinter operators had been properly instructed in using the machine, it is highly unlikely that it would have been broken. Another weakness of all of these machines is the fixed code wheel patterns. It is understandable that the designers thought that with the complexity of the machine it would not be necessary to vary the code wheel patterns. However, variable code wheel patterns would have strengthened the machines considerably. Due to the transposition circuit, cribs would not have led to the recovery of the key stream and even complete plain text of thousands of characters would not have resulted in recovered code wheel patterns.

Sir Harry Hinsley's statement, [22–24] that BP decided to concentrate its non-Morse interception, cryptanalytical, and decryption resources on the Army's Tunny traffic because of a need to husband resources and the need for good intelligence on the German Army, is undoubtedly correct. However, these were probably not the only reasons why BP abandoned its efforts against the Sturgeon machines. The cryptanalytical difficulties BP faced in attacking these machines, the small number of exploitable Sturgeon links, and the very limited intelligence that could be derived from the traffic must have played important roles in the outcome of BP's decision to concentrate on the Tunny traffic.

The significant post-war interest that was shown in these machines is an indication that the SFM T52 continued to be of concern to the American and British cryptanalytical organisations. It is known that both the American and British agencies had a considerable interest in French codes and ciphers. The fact that the French adopted a slightly modified version of the SFM T52 for one of their cipher systems leads to a suspicion that post-war attacks could have taken place. However, whether these new members of the Sturgeon family laid any of their golden eggs is still an open question.

14 Acknowledgements

The author should like to thank Bengt Beckman who, through his friendship over the last seven years, has been a constant inspiration for my research into the history of the Siemens SFM T52 machines. His help with obtaining material about the Swedish cryptanalysts and their success against these machines has been crucial to this work. As usual, Ralph Erskine has been very helpful with suggestions and improvements, not to forget his help with proof reading and archive material. David Alvarez has given generous support and supplied several documents. Torbjörn Andersson, Jürg Drobick, Philip Marks, Jon Paul and Wolfgang Mache have very generously helped me with documentation. Special thanks go to Captain Jon Ulvensøen and The Armed Forces Museum (Forvarsmuseet) in Oslo for supplying many German documents and for giving me access to their collection of cipher machines. I should also like to thank the late Donald Davies for answering my questions about the T52c wheel combining logic and generally for his help over a great many years. Furthermore, I am very grateful to Geoff Sullivan who has helped me with the simulations of the permutation circuit, and whose computer simulation of the complete cipher machine in all its versions and models has been of the utmost importance to this research. And finally, I should like to thank Professor Friedrich L. Bauer for finding an error in a previous version of this paper.

Part II

15 The Cryptanalytical Problems

On 29 July 1944 Captain Walter J. Fried, the US Army Signal Security Agency's (SSA)[28] liaison at BP, sent his report No. 68, [18] which he devoted

[28] The agency went through a number of changes in both name and organization during the period 1939–1945. It was named Signal Intelligence Service, Signal

entirely to the Sturgeon problem, to the SSA headquarters at Arlington Hall. He started the report with the following assessment: "The problem of solving current traffic seems completely hopeless. The only feasible method of solving messages enciphered on the T52d machine seems to be through depths. Sometimes the "motor" action is switched off and this gives rise to several possible techniques of solution.[29] For the most part, however, the problems which seem capable of solution are comparatively trivial. The fundamental difficulty of the general problem arises from the fact that that a crib does not yield key."

To give a better feeling for the fundamental cryptanalytical problems I will attempt to give an overview of what is involved in breaking the T52 machines, and how certain features of the machine hampered this task, while other features made it easier for the cryptanalyst. The basic algorithm of the machine has already been explained. To recapitulate, a five element teleprinter plain text character P will first be added modulo two to a five element *subtractor* character Σ and then permuted under the control of another five element *permutor* character Π resulting in the cipher text character C.

The cryptographic algorithm, transforming a plain text character P into its cipher text character C, can be expressed mathematically by

$$C = \Pi(P \oplus \Sigma) \tag{1}$$

where $\oplus$ signifies modulo two addition. The plain text character is first added to the subtractor modulo two and the permutor then permutes the result. On reception the inverse permutation takes place before the addition of the subtractor, which gives

$$P = C\Pi^{-1} \oplus \Sigma \tag{2}$$

A simple way of representing the relationship between the four elements P, C, Σ and Π is through a $32 \times 32 \times 32$ cube. One of the elements P, C or Σ can be placed in the cube and the other three elements along the three axes. Π cannot be placed inside the cube as it is not uniquely defined by P, C and Σ. The cube can then be cut by planes along any of the axes and it will then be represented by 32 squares slices each of the size $32 \times 32 \times 1$. The choice of the representation will entirely depend on the problem to be solved. It is now easily seen that a plain text character from the 32 element teleprinter alphabet will be transformed into a cipher text character through $32 \cdot 32 = 1024$ cipher alphabets. However, this theoretical limit was seldom achieved

Security Division, Signal Security Service, Signal Security Branch, etc. before it was redesignated Signal Security Agency on 1 July 1943, later to be changed to Army Security Agency on 15 September 1945.

[29] The author's studies of the T52d and e models have not revealed any possibility of switching off the "motor" or wheel stopping function on these machines. It is more likely the observed absence of wheel stopping was due to the use of the T52a/b machine.

in practice. If we analyse the basic permutation circuit used in the T52c and T52e machines we will find that / and Z produce identical permutations, as do T and E. This means that, instead of producing 32 permutations, the circuit only generate 30 unique permutations. Therefore these machines only have $32 \cdot 30 = 960$ cipher alphabets. However, this was only achieved in the T52e. In the T52c and T52ca machines the wheel combination logic reduced the number of cipher alphabets even further.

Before we use the cipher squares in our analysis it is useful to introduce the concept of Baudot classes. The class of a Baudot character is defined as the number of crosses (or 1's) that it contains. It is clear that we have six classes labelled from 0 to 5 inclusive. There are various ways of arranging these classes but the method used here is the one used at BP, and is shown in Fig. 11. The Baudot classes are indicated in the top row with the letter shift alphabet used by BP in the row below. The Baudot control characters have been given the special BP values as previously indicated in footnote 6 on page 14. Below the alphabet are the five bits of each character's Baudot code value indicated by dots and crosses. The bottom row shows the corresponding figure shift characters.

	0	1					2										3										4					5
	/	E	4	9	3	T	A	S	D	Z	I	R	L	N	H	O	U	J	W	F	Y	B	C	P	G	M	K	Q	+	X	V	8
1	•	×	•	•	•	•	×	×	×	×	•	•	•	•	•	•	×	×	×	×	×	×	•	•	•	•	×	×	×	×	•	×
2	•	•	×	•	•	•	×	•	•	•	×	×	×	•	•	•	×	×	×	•	•	•	×	×	×	•	×	×	×	•	×	×
3	•	•	•	×	•	•	•	×	•	•	×	•	•	×	×	•	×	•	•	×	×	•	×	×	•	×	×	×	•	×	×	×
4	•	•	•	•	×	•	•	•	×	•	•	×	•	×	•	×	•	×	•	×	•	×	×	•	×	×	×	•	×	×	×	×
5	•	•	•	•	•	×	•	•	•	×	•	•	×	•	×	×	•	•	×	•	×	×	•	×	×	×	•	×	×	×	×	×
[a]	#	3	#	#	#	5	-	’	#	+	8	4	)	,	*	9	7	#	2	*	6	?	:	0	*	.	(	1	#	/	=	#

[a] In the figure shift row control characters and other special functions are marked with #, while the national special characters are marked with *.

Figure11. International Telegraph Alphabet No. 2 in class order

As previously mentioned an analysis of the T52c key generator showed that the ten code wheels were combined in fours. The circuit combining the wheels were called the "Pentagon". Previously, the author had not been able to find any documentary information about the Pentagon, however, largely inspired by Professor William Tutte's beautiful little book on graph theory, [38] he thought he had found the answer. The BP Pentagon has come to light very recently in a wartime document. BP's Cryptographic Dictionary, originally written in 1944 but recently republished in electronic format by Tony Sale, shows a picture of the Pentagon and gives an explanation of its construction. [45]

The graph in Fig. 12 is constructed from the wheel combining logic in Fig. 5. In the graph in Fig. 12 the SR relays are represented by the vertices

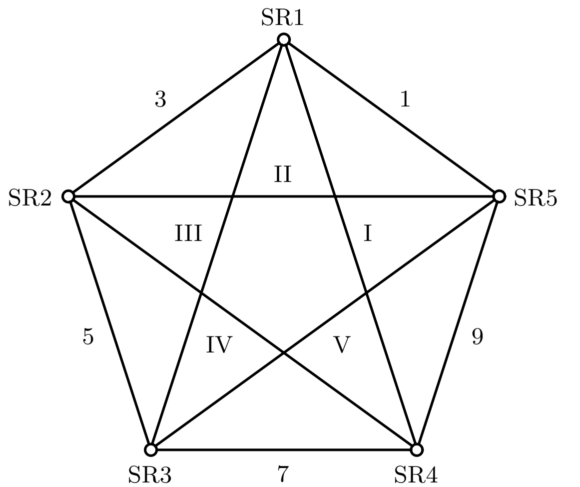

Figure12. The Pentagon

and the controlling wheel output channels by the edges which join in a given vertex. The graph quickly reveals the relationship between the different SR relays; it shows the topology of the circuit clearly. The symmetry of the graph is such that it very probably corresponds to what BP called the Pentagon.

BP's Cryptographic Dictionary confirms that the BP Pentagon and the graph in Fig. 12 are indeed the same. Only the labelling of the diagonals and the vertices differ. In the BP Pentagon the vertices are numbered from 1 to 5 in a clockwise manner, while the sides and diagonals are labelled by the lower case letters a–j. However, BP's research had shown that not only could the logic equations for the permutor relays, SR1–SR5, be formed from the Pentagon but also the subtractor equations. What BP discovered was

Combined Relays	Wheel Output Channels									
	1	3	5	7	9	I	II	III	IV	V
SR2 ⊕ SR7							X	X	X	X
SR1 ⊕ SR8						X	X	X		X
SR3 ⊕ SR6							X	X	X	X
SR5 ⊕ SR9						X	X	X		X

Figure13. Reduction of Pentagon terms.

that the wheel combining logic was governed by seven linearly independent equations. The first five equations are those of the permutor relays, SR1–SR5, which are given by our pentagon in Fig. 12, while the subtractor relays are governed by the two last equations. How is this possible? First of all, from

Permutor \ Subtractor	/	E	4	9	3	T	A	S	D	Z	I	R	L	N	H	O	U	J	W	F	Y	B	C	P	G	M	K	Q	+	X	V	8
/	⋆						⋆							⋆													⋆					
E																																
4																																
9																																
3																																
T																																
A								⋆	⋆		⋆	⋆																				
S								⋆	⋆		⋆	⋆																				
D															⋆	⋆												⋆	⋆			
Z	⋆						⋆							⋆													⋆					
I	⋆						⋆							⋆													⋆					
R										⋆			⋆																	⋆	⋆	
L								⋆	⋆		⋆	⋆																				
N										⋆			⋆																	⋆	⋆	
H								⋆	⋆		⋆	⋆																				
O															⋆	⋆												⋆	⋆			
U																																
J																																
W																																
F																																
Y																																
B																																
C																																
P																																
G																																
M																																
K															⋆	⋆												⋆	⋆			
Q	⋆						⋆							⋆													⋆					
+										⋆			⋆																	⋆	⋆	
X										⋆			⋆																	⋆	⋆	
V															⋆	⋆												⋆	⋆			
8																																

Figure14. Alphabet distribution for T52c.

Fig. 5 we see that the equation for SR10 is the same as SR4. Furthermore, we also notice that SR6 depends on the same 1–9 output channels as SR3, SR7 the same channels as SR2, SR8 the same as SR1 and finally SR9 uses those of SR5. This means that these equations are not linearly independent and by adding them together modulo two we will get new relationships which still are based on only four output channel terms. This is shown in Fig. 13. The symbol $\oplus$ is used to describe the modulo two addition (XOR). We see that SR2 $\oplus$ SR7 and SR3 $\oplus$ SR6 are both described by the same output channel terms, while SR1 $\oplus$ SR8 is the same as SR5 $\oplus$ SR9. Hence, the control of the remaining subtractor relays can be described by only two logical expressions which each comprises four out of the five diagonals in the pentagon in Fig. 12. The Pentagon clearly illustrates the inspiration and depth of thought that governed the cryptanalytical work at Bletchley Park.

Using computer simulations, the T52c's wheel combination logic has been analysed: a plot of the 32×32 permutor/subtractor square is given in Fig. 14.

The alphabets along the permutor and subtractor axes are in the Baudot class order: an asterisk indicates the existence of an alphabet. We see that there are no alphabets in the odd classes 1, 3 and 5. All the alphabets are clustered in the even classes 0, 2 and 4. This is a confirmation of BP's finding that the parity of the subtractor character was always even. We further see that there are $16 \cdot 4 = 64$ alphabets which, with our knowledge of the reduced permutor alphabet, gives a total number of 60 cipher alphabets. As the parity of the characters T and E is odd, the doublet T–E is not possible. Only the doublet /–Z exists, hence we get $15 \cdot 4 = 60$ cipher alphabets. We also see that for each permutor character there are only four possible subtractor characters as mentioned by BP. The plot clearly shows that this machine was extremely insecure.

Relays		Wheel Output Channels									
		1	3	5	7	9	I	II	III	IV	V
Permutor	SR1				X	X	X			X	
	SR2	X	X	X	X						
	SR3				X		X	X			X
	SR4	X				X		X		X	
	SR5	X				X			X		X
Subtractor	SR6	X	X					X			X
	SR7						X	X	X	X	
	SR8		X	X		X				X	
	SR9			X	X		X		X		
	SR10		X	X					X		X

Figure15. Wheel combination logic for T52ca.

The wheel combining logic of the modified T52ca machine has been reconstructed using data from the FRA archives. The truth table is given in Fig. 15 while the corresponding permutor/subtractor plot is in Fig. 18. In the plot in Fig. 18 the alphabets are in the binary order, not the Baudot class order, since such a representation shows more clearly the inherent structure of the wheel combining logic. As we can see, the alphabets are well spread out and are no longer exclusively of even parity. However, the linear structure is there and changing one single entry in the truth table will drastically change both the structure and number of possible alphabets. Each permutor character is associated with eight subtractor characters, which is twice as many as for the T52c logic. However, if we plot the permutor/subtractor square in Baudot class order, we find that when a permutor character is even, the alphabets have an even subtractor character, and when the permutor character is odd, so is the subtractor. This information can still be exploited by the cryptanalyst. The permutor characters, which form the doublets T–E and /–Z, each have a different set of subtractor characters. Due to the non-overlapping subtractor characters, the T52ca doublets will not reduce the alphabet size like in the T52c. Hence, the T52ca has a total of $32 \cdot 8 = 256$ unique cipher alphabets.

The T52a/b and T52d machines use the same layout of the transposition[30] circuit as the T52c and T52e, but instead of using relays for the transposition units, these machines directly use the cam contacts on each coding wheel. What distinguishes the a/b and d models from the others is that the transposition units, which consisted of double changeover contacts, were not wired permanently into the transposition circuit. Each of the five contact sets was equipped with two plug connections which were then plugged into the transposition circuit. Figure 16 shows the layout of the transposition circuit

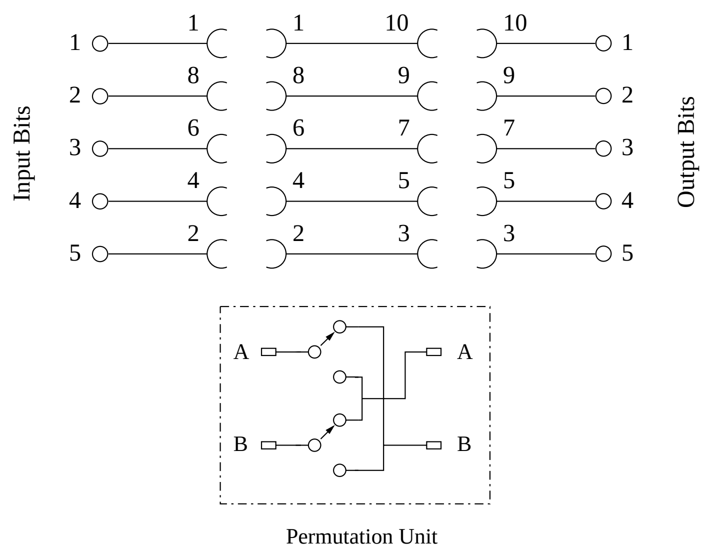

Figure16. SFM T52's transposition circuit.

together with the circuit of a single transposition unit. The figure shows that there are two possible contact points in each Baudot bit or element branch.

The connection 1–3 means that either the A or B plug of a transposition unit will connect to the socket marked with 1's, while the other plug will go to the socket marked with 3's. If A goes to socket one, the left part of the A plug will plug into the left-hand side of socket one, while the right part of the A plug goes to the right-hand side of the socket. In this particular case, bit one will end up in position five when the transposition unit is inactive, while in the active position bit one will leave on the branch connected to socket

[30] The terms transposition circuit and transposition unit reflect the cryptographic usage; mathematically speaking the circuit performs a permutation.

ten. Its final position will depend on the connection that is made from socket ten.

There are $9 \cdot 7 \cdot 5 \cdot 3 \cdot 1 = 945$ different ways that the five contact sets can be inserted into the transposition circuit. Computer simulations show that each of these 945 connection variants results in unique permutation sets. However, the majority of the permutation sets, a total of 561, are degenerate in the sense that each set contains only from 1 to 16 unique permutations.

	Number of Unique Permutations in a Set												
Bits Stuck	1	2	4	5	6	10	12	14	16	27	30	32	Total
1 bit			60				30	180	30				300
2 bits				20	60								80
3 bits		20											20
5 bits	1												1
None						40	120			24	240	120	544
Total	1	20	60	20	60	40	150	180	30	24	240	120	945

Figure17. Permutation distribution for T52d.

The set with only one single permutation is a special case — it contains the identity permutation, hence no transposition takes place. There are further variants on this where one, two or three of the Baudot character pulses will not be permuted. There are in total 300 cases where one pulse remains in place, 80 cases where two pulses are fixed and 20 instances where three pulses are unaffected. All of these cases belong to the set of the degenerate permutations. Figure 17 gives an overview of the distribution of the different permutation sets. The figure shows that among the remaining 384 permutation sets, 24 sets have 27 unique permutations, 240 sets have 30 permutations and 120 sets contain all the 32 permutations. Figure 17 shows that of the degenerate sets only the sets with 10 and 12 unique permutations also have normal permutations, in the sense that none of the bits remain in place. All the other degenerate sets have one or more bits that are not affected by the permutations.

Looking at the *Wehrmacht* SFM T52d Key table reproduced in Appendix C, it can be shown that all the connections in this table belong to the two groups with 30 and 32 unique permutations. This means that in reality only 360 permutation sets were used by the German cryptographers during the period this key list was in use. It also means that there may be more than 960 cipher alphabets — there can be as many as 1024. It seems that the Germans were aware of the fact that not all of the permutations could be used for cryptographic purposes. Dr. Fricke and Dr. Hüttenhain refer to what they call non-permissible transposition pyramids. [15] The forbidden connections

		Subtractor																															
		/	E	4	A	9	S	I	U	3	D	R	J	N	F	C	K	T	Z	L	W	H	Y	P	Q	O	B	G	+	M	X	V	8
Permutor	/	⋆						⋆			⋆						⋆		⋆						⋆	⋆						⋆	
	E		⋆						⋆	⋆						⋆		⋆						⋆			⋆						⋆
	4			⋆		⋆							⋆		⋆						⋆		⋆					⋆		⋆			
	A				⋆		⋆					⋆		⋆						⋆		⋆							⋆		⋆		
	9			⋆		⋆							⋆		⋆						⋆		⋆					⋆		⋆			
	S				⋆		⋆					⋆		⋆						⋆		⋆							⋆		⋆		
	I	⋆						⋆			⋆						⋆		⋆						⋆	⋆						⋆	
	U		⋆						⋆	⋆						⋆		⋆						⋆			⋆						⋆
	3		⋆						⋆	⋆						⋆		⋆						⋆			⋆						⋆
	D	⋆						⋆			⋆						⋆		⋆						⋆	⋆						⋆	
	R				⋆		⋆					⋆		⋆						⋆		⋆							⋆		⋆		
	J			⋆		⋆							⋆		⋆						⋆		⋆					⋆		⋆			
	N				⋆		⋆					⋆		⋆						⋆		⋆							⋆		⋆		
	F			⋆		⋆							⋆		⋆						⋆		⋆					⋆		⋆			
	C		⋆						⋆	⋆						⋆		⋆						⋆			⋆						⋆
	K	⋆						⋆			⋆						⋆		⋆						⋆	⋆						⋆	
	T			⋆		⋆							⋆		⋆						⋆		⋆					⋆		⋆			
	Z				⋆		⋆					⋆		⋆						⋆		⋆							⋆		⋆		
	L	⋆						⋆			⋆						⋆		⋆						⋆	⋆						⋆	
	W		⋆						⋆	⋆						⋆		⋆						⋆			⋆						⋆
	H	⋆						⋆			⋆						⋆		⋆						⋆	⋆						⋆	
	Y		⋆						⋆	⋆						⋆		⋆						⋆			⋆						⋆
	P			⋆		⋆							⋆		⋆						⋆		⋆					⋆		⋆			
	Q				⋆		⋆					⋆		⋆						⋆		⋆							⋆		⋆		
	O				⋆		⋆					⋆		⋆						⋆		⋆							⋆		⋆		
	B			⋆		⋆							⋆		⋆						⋆		⋆					⋆		⋆			
	G		⋆						⋆	⋆						⋆		⋆						⋆			⋆						⋆
	+	⋆						⋆			⋆						⋆		⋆						⋆	⋆						⋆	
	M		⋆						⋆	⋆						⋆		⋆						⋆			⋆						⋆
	X	⋆						⋆			⋆						⋆		⋆						⋆	⋆						⋆	
	V				⋆		⋆					⋆		⋆						⋆		⋆							⋆		⋆		
	8			⋆		⋆							⋆		⋆						⋆		⋆					⋆		⋆			

Figure18. Alphabet distribution for T52ca.

were 1–10, 2–3, 4–5, 6–7, or 8–9, because as they say: "these connections are not effective".

When the Swedish cryptanalyst Lars Carlbom analysed the transposition circuit, he found four main permutation families, of which two could be divided further into three sub-groups. One of these families, he said, consisted of connections where one of the transposition units was inactive or disconnected. It is not possible to disconnect a transposition unit and still expect the machine to function, but Lars Carlbom did not know this as he had never seen a T52 machine. He based his analysis entirely on cryptanalytical evidence. In practice, what happened was that an input impulse exited the transposition circuit at the same level as it entered; hence no Baudot element permutation was taking place. The identity permutation referred to earlier is caused by such a set of connections: 1–10, 2–3, 4–5, 6–7 and 8–9, which leave all the bits in their original positions. If one or more of these special connections are combined with other more random connections, the other cases of one or more bits stuck will occur.

During the year when BP struggled with the July Halibut message enciphered on the T52d it developed and tried out various methods of attack. Several of them were of a statistical nature and were based on knowledge gained through the use of statistical techniques against the Lorenz SZ40/42 machines. The statistical methods BP developed only applied to the "motorless" machines and would not work on machines with wheel stopping. The T52 code wheels had an almost even distribution of dots and crosses with a slight preponderance of crosses. This meant that the modulo two addition was nearly random. However, this was not the case for the permutations,

			C															
			/ 8	E V	4 X	9 +	3 Q	T K	A M	S G	D P	Z C	I B	R Y	L F	N W	H J	O U
	/	8	32															
	E	V		9	9	2	4	8										
	4	X		8	8	16	0	0										
	9	+		4	4	8	16	0										
	3	Q		2	2	4	8	16										
	T	K		9	9	2	4	8										
	A	M							8	6	1	2	6	1	2	2	4	0
Φ	S	G							4	2	6	1	2	6	1	4	2	4
	D	P							2	1	2	6	1	2	6	0	4	8
	Z	C							4	2	4	8	2	4	8	0	0	0
	I	B							0	8	4	0	8	4	0	8	0	0
	R	Y							0	4	2	4	4	2	4	4	8	0
	L	F							8	6	1	2	6	1	2	2	4	0
	N	W							0	0	4	2	0	4	2	8	4	8
	H	J							4	2	6	1	2	6	1	4	2	4
	O	U							2	1	2	6	1	2	6	0	4	8

Figure19. SFM T52's dibit distribution.

since certain impulses were more likely to go to some positions than others. Therefore the statistical techniques were based on developing statistics for certain impulse combinations of the "pseudo plain text" character, Φ, and their probability of ending up in certain positions in the cipher text character. Here the "pseudo plain text" is the real plain text transformed by the subtractor key.

$$\Phi = P \oplus \Sigma \tag{3}$$

The method applies to both single impulses or to pairs, dibits, but plain text characteristics are more pronounced when using a pair of impulses. For a

0	1					2										3										4					5
/	E	4	9	3	T	A	S	D	Z	I	R	L	N	H	O	U	J	W	F	Y	B	C	P	G	M	K	Q	+	X	V	8
A	4	E	U	J	W	/	I	R	L	S	D	Z	K	Q	+	9	3	T	C	P	G	F	Y	B	8	N	H	O	V	X	M
B	O	+	X	Z	D	G	M	T	3	8	W	J	Y	F	E	V	L	R	H	N	/	Q	K	A	S	P	C	4	9	U	I
C	K	N	R	I	V	F	J	U	8	3	9	M	4	G	P	D	S	X	A	+	Q	/	O	H	L	E	B	Y	W	T	Z
D	3	J	F	E	B	R	N	/	O	K	A	+	S	X	Z	C	4	G	9	M	T	U	8	W	Y	I	V	L	H	Q	P
E	/	A	S	D	Z	4	9	3	T	U	J	W	F	Y	B	I	R	L	N	H	O	K	Q	+	X	C	P	G	M	8	V
F	N	K	D	S	X	C	3	9	M	J	U	8	E	B	Y	R	I	V	/	O	H	A	+	Q	Z	4	G	P	T	W	L
G	+	O	V	L	R	B	8	W	J	M	T	3	P	C	4	X	Z	D	Q	K	A	H	N	/	I	Y	F	E	U	9	S
H	Y	P	T	M	9	Q	Z	X	S	L	V	I	O	/	N	W	8	U	B	E	F	G	4	C	3	+	A	K	D	R	J
I	U	9	4	C	P	S	A	K	Q	/	N	H	R	L	V	E	F	Y	J	W	8	3	T	M	G	D	Z	X	+	O	B
J	R	D	K	A	+	3	C	4	G	F	E	B	U	8	W	N	/	O	I	V	L	S	X	Z	Q	9	M	T	P	Y	H
K	C	F	J	U	8	N	R	I	V	D	S	X	A	+	Q	3	9	M	4	G	P	E	B	Y	W	/	O	H	L	Z	T
L	W	T	P	G	4	Z	Q	+	A	H	O	/	V	I	R	Y	B	E	8	U	J	M	9	3	C	X	S	D	K	N	F
M	X	V	O	H	N	8	B	Y	F	G	P	C	T	3	9	+	Q	K	Z	D	S	L	R	I	/	W	J	U	E	4	A
N	F	C	3	9	M	K	D	S	X	R	I	V	/	O	H	J	U	8	E	B	Y	4	G	P	T	A	+	Q	Z	L	W
O	B	G	M	T	3	+	X	Z	D	V	L	R	H	N	/	8	W	J	Y	F	E	P	C	4	9	Q	K	A	S	I	U
P	Q	H	L	V	I	Y	W	8	U	T	M	9	G	4	C	Z	X	S	+	A	K	O	/	N	R	B	E	F	J	3	D
Q	P	Y	W	8	U	H	L	V	I	Z	X	S	+	A	K	T	M	9	G	4	C	B	E	F	J	O	/	N	R	D	3
R	J	3	C	4	G	D	K	A	+	N	/	O	I	V	L	F	E	B	U	8	W	9	M	T	P	S	X	Z	Q	H	Y
S	9	U	E	F	Y	I	/	N	H	A	K	Q	D	Z	X	4	C	P	3	T	M	J	W	8	B	R	L	V	O	+	G
T	Z	L	H	O	/	W	Y	B	E	P	G	4	M	9	3	Q	+	A	X	S	D	V	I	R	N	8	U	J	F	C	K
U	I	S	A	K	Q	9	4	C	P	E	F	Y	J	W	8	/	N	H	R	L	V	D	Z	X	+	3	T	M	G	B	O
V	8	M	G	P	C	X	+	Q	K	O	H	N	L	R	I	B	Y	F	W	J	U	T	3	9	4	Z	D	S	A	/	E
W	L	Z	Q	+	A	T	P	G	4	Y	B	E	8	U	J	H	O	/	V	I	R	X	S	D	K	M	9	3	C	F	N
X	M	8	B	Y	F	V	O	H	N	+	Q	K	Z	D	S	G	P	C	T	3	9	W	J	U	E	L	R	I	/	A	4
Y	H	Q	Z	X	S	P	T	M	9	W	8	U	B	E	F	L	V	I	O	/	N	+	A	K	D	G	4	C	3	J	R
Z	T	W	Y	B	E	L	H	O	/	Q	+	A	X	S	D	P	G	4	M	9	3	8	U	J	F	V	I	R	N	K	C
3	D	R	N	/	O	J	F	E	B	C	4	G	9	M	T	K	A	+	S	X	Z	I	V	L	H	U	8	W	Y	P	Q
4	A	/	I	R	L	E	U	J	W	9	3	T	C	P	G	S	D	Z	K	Q	+	N	H	O	V	F	Y	B	8	M	X
8	V	X	+	Q	K	M	G	P	C	B	Y	F	W	J	U	O	H	N	L	R	I	Z	D	S	A	T	3	9	4	E	/
9	S	I	/	N	H	U	E	F	Y	4	C	P	3	T	M	A	K	Q	D	Z	X	R	L	V	O	J	W	8	B	G	+
+	G	B	8	W	J	O	V	L	R	X	Z	D	Q	K	A	M	T	3	P	C	4	Y	F	E	U	H	N	/	I	S	9
/	E	4	9	3	T	A	S	D	Z	I	R	L	N	H	O	U	J	W	F	Y	B	C	P	G	M	K	Q	+	X	V	8

Figure20. Baudot XOR square in class order

given permutation it was possible to enumerate how often dibits of a given "pseudo plain text" character, Φ, and its inverse would be associated with dibits in different cipher text characters, C. This is shown in Fig. 19 where the permutation is generated by the transposition circuit used on the T52c and e models, and which used the connections: 1–2, 3–4, 5–6, 7–8 and 9–10.

The alphabets in the figure have only a length of 16, as the normal 32 element Baudot alphabet has been folded in half, with each position in the alphabet occupying a given Baudot character and its inverse, e.g. E and V, which have the Baudot vectors $\times\bullet\bullet\bullet\bullet$ and $\bullet\times\times\times\times$. The characters /–8 (which are all dots and all crosses) can only go to one place under all the 32 different permutation, while in all the other cases there are varying distributions. The characters belonging to classes 1 and 4 have single cross/dot distributions, while the characters in classes 2 and 3 have double cross/dot distributions. This is the reason for the clustering of the distributions in the two squares of size 5 and 10.

But on the T52a/b and d models the permutations were not fixed, but variable depending on the connections of the transposition units. Therefore the permutation probabilities, and hence the statistics, depended on the given permutation set which, of course, was unknown until the machine was broken. So the statistical techniques available in 1944 were nothing more than tools for getting a better knowledge about the cryptanalytical problem. They were not of much use in attacking the machines.

It appears that messages in depth were the only viable attack on these machines in 1944. Describing a full blown attack on a real example is far too involved a process, but looking at a very small constructed example with a depth of two and a known crib will give a feeling for the problem. As mentioned earlier, the attacks in depths were helped by the use of tables and catalogues. One such table is the Baudot XOR or modulo two square. However, the table becomes a lot more useful when one of the alphabets is arranged in class order. This is illustrated in Fig. 20, where the plain text alphabet is in its normal order along the left hand column and the key alphabet is arranged in class order along the top row. The intersection of a plain text character and a key character will give the resulting cipher text character. However, due to the properties of modulo two addition any of the two alphabets, the one in normal order or the one in class order, can be used for any of the three elements plain, cipher or key characters.

To see what is actually taking place and how one might attack two messages in depth it is helpful to return to the principal encipherment equation (1)

$$\Pi(P \oplus \Sigma) = C$$

It is easily shown that permutation is distributive under modulo two addition

$$\Pi(X \oplus Y) = \Pi X \oplus \Pi Y \tag{4}$$

If we apply (4) to (1) we get

$$\Pi P \oplus \Pi\Sigma = C \tag{5}$$

In other words, the cipher character can also be obtained by first applying the permutation on the plain text character and the subtractor before combining these two transposed elements by modulo two addition. In the case of two messages P and Q enciphered in depth by the subtractor key Σ and the permutor key Π we can write the following

$$\Pi P \oplus \Pi\Sigma = C \tag{6}$$

$$\Pi Q \oplus \Pi\Sigma = D \tag{7}$$

Combining (6) and (7) by modulo two addition eliminates the $\Pi\Sigma$ term and gives at the basic equation for messages in depth

$$\Pi(P \oplus Q) = C \oplus D \tag{8}$$

Equation 8 shows that if either P or Q is known the value of the other cannot be automatically determined, as with pure Vernam [42] encipherment where there is only a subtractor function and no permutor function. In reality there might be as many as ten possible solution for P or Q depending on the Baudot class in which the operation took place. If the operation takes place in class 0 or 5, P and Q are uniquely determined, while in class 1 and 4 there are five possibilities and in class 2 and 3 there are ten possible solutions.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	P	G	I	+	L	X	G	L	T	N	E	3	Y	O	X	P	J	3	B	V
2	Y	N	+	8	4	I	P	P	9	E	B	D	K	W	E	8	E	I	4	H
n	2	3	4	1	1	4	2	1	2	3	2	1	3	3	3	2	2	3	4	2

Figure21. Two messages in depth.

One opening for attack is the fact that the permutation only reorders the Baudot code elements: it does not change the elements themselves. Therefore if $C \oplus D$ contains m crosses and n dots, it must also be the same for $P \oplus Q$. So if we know or can make a guess at P we will have a limited number, from 1 to 10, of choices for Q. This is the basis for an attack on messages in depths enciphered on the Siemens T52.

The two messages in Fig. 21 have been enciphered with the same key on a computer simulation of the T52d machine.[31] They are enciphered without the KTF and the main inner key, *Fernschreibgrundschlüssel*, is 6–8, 1–2, 5–7, III, 4–10, IV, II, I, 3–9, V, which is the key for day one in the *Norwegen Nr. 7* key table in Appendix C. The message key, *Fernschreibspruchschlüssel*, is the same as given on page 18, QEP FF OO PP AA ZZ VV CC MM HH UU. The second message is suspected to start with "three" or "four", since message numbers in the region of three to four hundred are expected.

The class numbers appearing in the last row are found by forming the modulo two sum of the two cipher text characters and looking up in which class the resulting character belongs. Taking the first two cipher text characters P and Y and combining them modulo two results in A. This result is found by using a simple Baudot XOR square or using the class XOR square in Fig. 20. Looking up P in the vertical left hand alphabet and Y in the horizontal class alphabet, we find A at their intersection. Looking in the top row class alphabet, we find that A belongs to class 2. The class information can also be found from the Baudot class alphabet in Fig. 11. Another, perhaps even faster, method is to look up one of the cipher text characters, say P,

[31] The T52 computer simulation is available on the Cipher Simulation Group's (CSG) Web servers which are accessible through the author's Cryptology Web page at URL: http://frode.home.cern.ch/frode/crypto/

in the left hand vertical alphabet and then searching down the row to find the other cipher text character, Y. Doing so we find Y situated in one of the columns for class 2.

Trying the word “three” with a space, here represented by 9, as a crib for the beginning of the second message gives the following possible solutions for the characters of the beginning of the first message, as shown in Fig. 22. The possible solutions for each character are given in the generatrices[32] which have been obtained from the class XOR table. Looking up the first clear text letter of the crib, T, in the left hand vertical alphabet the corresponding generatrix is found further along the row in the columns for the Baudot class 2. The generatrix characters are: WYBEPG4M93 which have been entered in alphabetical order to ease the search for a possible plain text word.

	1	2	3	4	5	6
n	2	3	4	1	1	4
2	T	H	R	E	E	9
	B	B	H	A	**A**	B
	E	C	Q	D	D	**G**
	G	**E**	**S**	**S**	S	J
	M	F	X	Z	Z	W
1	P	G	Z	/	/	8
	W	U				
	Y	W				
	3	3				
	4	4				
	9	8				

Figure22. Trying the crib “three” in message no. 2.

The most prominent plain text word is the beginning of the word “MESSAGe”. We can now try to extend the plain text in the second message by using the expected “E9” (E and a space) as a further crib in the first message. This is shown in Fig. 23a.

Since the beginning of the first message is suspected to contain a message number the continuation is expected to be another number. Of the numbers from one to ten the only possible solutions are “THree” or “FIve”. “ThREE” and 9 do not give any promising plain text in message number one but “fiVE” and 9 give “ONE” as shown in Fig. 23b. This is even a unique solution as none of the other characters needed for the other numbers are present in the first generatrix. The rest of the solution is left as an exercise for the reader. However, solutions are not always as straightforward as here: often it will

32 Generatrix, plural generatrices, is a decipherment or encipherment out of a set of decipherments or encipherments of the same text under a given hypothesis or cryptographic principle.

	7	8
n	2	1
1	E	9
	B	<u>H</u>
	<u>F</u>	<u>I</u>
	J	N
	<u>T</u>	S
2	U	/
	W	
	Y	
	3	
	4	
	9	

(a)

	9	10	11
n	2	3	2
2	V	E	9
	H	H	C
	I	I	**E**
	K	K	F
	L	L	M
1	N	**N**	P
	O	O	T
	Q	Q	U
	R	R	Y
	X	X	3
	+	+	4

(b)

Figure23. Continuing the cribs in messages no. 1 and no. 2.

not be possible to carry on with only two messages in depth. Very often the messages contained numbers or abbreviations which made it extremely difficult, if not impossible, to extend the messages with only a depth of two or three.

It is one thing to break a number of messages in depth. However, the aim is to break the machine, so as to be able to recover the key streams and hence to break all other messages for the rest of the key period. For this purpose it is necessary to be able to uniquely determine the permutation Π for each encryption step. It can be shown that at least a depth of four is necessary, but that it is generally not sufficient. With a depth of four one has only a 20 % probability of finding a unique permutation. With a depth of seven or eight the probabilities are such that a workable key extraction can take place. As the code wheel patterns are fixed, it is possible to determine from the extracted key streams which code wheel is used where and for what purpose. From this information it is then possible to recover the plug connections and starting positions of the machine.

References

1. Unknown Author: Sturgeon Type Ciphers (Research Section, November 1944). Addendum to Captain Walter J. Fried's report No. 116 of 17 Nov. 1944. Henceforth called Fried reports. National Archives and Records Administration (NARA) RG 457 NSA Historical Collection Box 880 Nr. 2612
2. Unknown Author: Memo to The Head of the G.C. & C.S. (15th November 1941). Public Record Office (PRO), Kew, HW 14/22. Source: Ralph Erskine (RE)
3. Abrook, R. H.: Headquarters No. 26 Group. Air Staff Memorandum. Task No. 817. Appendix X. PRO, Kew, AIR 25/563
4. Army Security Agency: European Axis Signal Intelligence in World War II: Vol. 2 – Notes on German High Level Cryptography and Cryptanalysis, (1 May

1946). A TICOM Publication released under the US Freedom of Information Act (FOIA). Source: David Alvarez (DA)
5. Army Security Agency: European Axis Signal Intelligence in World War II: Vol. 3 – The Signal Intelligence Agency of the Supreme Command, Armed Forces, (1 May 1946). A TICOM Publication released under the FOIA. Source: DA
6. Beckman, Bengt: *Svenska kryptobedrifter (Swedish Crypto Achievements)*. In Swedish. Stockholm: Albert Bonniers Förlag (1996)
7. Boheman, Erik: *På Vakt. Kabinettssekreterare under andra världskriget (On Duty. Under-Secretary of State During the Second World War)*. In Swedish. Stockholm (1964)
8. Campaigne, Howard: Report on British Attack on "FISH". NARA RG 457 NSA Hist. Col. Box 579 Nr. 1407 (1945)
9. Carlbom, Lars: Tyska Teletypechiffer (German teleprinter cipher). In Swedish. Försvarets Radioanstalt (FRA), Stockholm, (31 January 1944). Source: Torbjörn Andersson
10. Davies, Donald W.: The Siemens and Halske T52e Cipher Machine. Cryptologia **6(4)** October (1982) 289–308
11. Davies, Donald W.: The Early Models of the Siemens and Halske T52 Cipher Machine. Cryptologia **7(3)** July (1983) 235–253
12. Davies, Donald W.: New Information on the History of the Siemens and Halske T52 Cipher Machine. Cryptologia **18(2)** April (1994) 141–146
13. Denham, Henry: *Inside the Nazi Ring. A Naval Attaché in Sweden 1940-1945*. London (1984) 82–99
14. Deutsche Wehrmacht: Schlüsselfernschreibvorschrift (SFV). H.Dv. g 422, L.Dv. g 704/3b, M.Dv. Nr. 924a Geheim, 1 Dezember 1942
15. Fricke, Dr. and Hüttenhain, Dr. Erich: OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cipher Teleprinter Machines. TICOM Report I-45. Released under FOIA request. Source: RE
16. Fried, Walter J.: FISH Notes. Fried Report No. 43 of 27 May 1944. NARA RG 457 NSA Hist. Col. Box 880 Nr. 2612
17. Fried, Walter J.: FISH Notes. Fried Report No. 46 of 12 June 1944. NARA RG 457 NSA Hist. Col. Box 880 Nr. 2612
18. Fried, Walter J.: FISH Notes (Sturgeon). Fried Report No. 68 of 29 July 1944. NARA RG 457 NSA Hist. Col. Box 880 Nr. 2612
19. Fried, Walter J.: Fish Notes (Non Morse Army Q Code). Fried Report No. 122 of 29 November 1944. NARA RG 457 NSA Hist. Col. Box 880 Nr. 2612
20. Haarstad, Gunnar: *I Hemmelig Tjeneste (In Secret Service)*. In Norwegian. Oslo: Aschehoug (1988) p. 70
21. Hinsley, F.H. et al.: *British Intelligence in the Second World War*. London: HMSO Vol. **2** (1981) p. 213
22. Hinsley, F.H.: Geheimschreiber (Fish). In F.H. Hinsley et al. *British Intelligence in the Second World War*. London: HMSO Vol. **3** Part 1 Appendix 2 (1984) 477–482
23. Hinsley, F.H.: Cracking the Ciphers. Electronics & Power IEE July (1987) 453–455
24. Hinsley, F.H.: An Introduction to Fish. In F.H. Hinsley and Alan Stripp (eds.), *Codebreakers, The Inside Story of Bletchley Park*. Oxford: Oxford University Press (1993) 141–148
25. Kahn, David: *The Codebreakers*. New York: Macmillan (1967)

26. Kimbrell, G. T.: Communications in the Soviet Zone of Germany. 18 July 1951. Index as “Three German Language Radio Communication Reports”. NARA RG 457 NSA Hist. Col. Box 1112 Nr. 3457
27. Levin, Dr. J.: Band-Transposition Systems. Technical Paper, Signal Security Agency, Cryptanalytic Branch, Washington, June 1944 NARA RG 457 NSA Hist. Col. Box 1029 Nr. 3304
28. Lewis, Arthur: Deciphering on the M8. Part of the file “The Setting Rotor”. NARA RG 457 NSA Hist. Col. Box 950 Nr. 2805
29. Maas, F.J: Der Stand der Funkfernschreibtechnik in Deutschland bis 1944 (The state of radio teleprinter techniques in Germany until 1944). Manuscript (15 February 1946). Source: Wolfgang Mache
30. Mache, Wolfgang: Geheimschreiber. Cryptologia **10(4)** October (1986) 230–242
31. Mache, Wolfgang: The Siemens Cipher Teletype in the History of Telecommunications. Cryptologia **13(2)** April (1989) 97–117
32. Mache, Wolfgang: Der Siemens-Geheimschreiber — ein Beitrag zur Geschichte der Telekommunikation 1992: 60 Jahre Schlüsselfernschreibmaschine. In German. Archiv für deutsche Postgeschichte Heft **2** (1992) 85–94
33. Ministerium für Staatssicherheit (MfS): "Schlüssel für den Fernschreibverkehr (Encryption for teleprinter traffic)", MfS, Abteilung Nachrichtenwesen, Berlin 21.10.50. Geheime Verslußsache (Secret). Source: Jürg Drobick.
34. Oberkommando der Kriegsmarine: Die Siemens-Schlüsselfernschreibmaschine SFM T52d (T typ 52 d). M.Dv. Nr. 35IV, D.(Luft) T.g.Kdos. 9105d. Geheime Kommandosache, Berlin März 1944
35. Royal Air Force: No. 8801 Air Disarmament Wing, Operations Record Book. PRO, Kew, AIR 26/508 (1945)
36. Seaman, John N., Albert M. Small et al.: FISH Notes. NARA RG 457 NSA Hist. Col. Box 1009 Nr. 3179
37. Selmer, Ernst S.: The Norwegian Modification of the Siemens and Halske T52e Cipher Machines. Cryptologia **18(2)** April (1994) 147–149
38. Tutte, William T.: *Graph Theory As I Have Known It.* Oxford Lecture Series in Mathematics and Its Applications Vol. **11** Oxford: Oxford University Press (1998)
39. Tutte, William T.: FISH and I. In David Joyner (ed.), *Coding Theory and Cryptology: From Enigma and Geheimschreiber to Quantum Theory.* New York: Springer Verlag (2000)
40. Ulfving, Lars and Weierud, Frode: The Geheimschreiber Secret: Arne Beurling and the Success of Swedish Signals Intelligence. In David Joyner (ed.), *Coding Theory and Cryptology: From Enigma and Geheimschreiber to Quantum Theory.* New York: Springer Verlag (2000)
41. Ulstein, Ragnar: *Etterretningstjenesten i Norge 1940–45 (Intelligence Service in Norway 1940–45).* In Norwegian. Oslo: Cappelen Bind 2 (Vol 2) (1990). Note 3 to chapter 9, p. 361
42. Vernam, Gilbert S.: Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications. Transactions A. I. E. E. Vol. **XLV** Feb. (1926) 295–301
43. Weierud, Frode: Sturgeon, The FISH BP Never Really Caught. In David Joyner (ed.), *Coding Theory and Cryptology: From Enigma and Geheimschreiber to Quantum Theory.* New York: Springer Verlag (2000)

44. Wylie, Shaun: Breaking Tunny and the Birth of Colossus. In Michael Smith and Ralph Erskine (eds.), *Action This Day: Bletchley Park from the breaking of the Enigma Code to the birth of the modern computer*. London: Bantam (2001) 317–341
45. Wyllie, James: The 1944 Bletchley Park Cryptographic Dictionary. NARA RG 457 NSA Hist. Col. Box 1413 Nr. 4559. Republished by Tony Sale on his Web page Codes and Ciphers at: http://www.codesandciphers.org.uk

16 Appendix A

M. Fschr. Spr. Schl.

Geheim! SFM T 52 d/e Prüfnr. 104

Norwegen Nr. 4

1. Tag ab 0900 Uhr DGZ

	1	2	3	4	5	6	7	8	9	10	
A	*18*	*20*	*38*	*31*	*54*	47	67	54	70	17	A
B	*05*	*30*	*22*	*60*	*63*	29	35	42	55	04	B
C	*37*	*28*	*58*	*36*	*03*	46	13	47	20	67	C
D	*46*	*27*	*42*	*32*	*10*	07	64	41	08	15	D
É	*23*	*13*	*30*	*29*	*24*	56	20	31	39	32	E
F	*19*	*45*	*57*	*07*	*55*	61	27	58	68	72	F
G	*42*	*22*	*19*	*26*	*08*	11	53	29	16	58	G
H	*35*	*08*	*28*	*55*	*58*	22	19	68	02	19	H
İ	*29*	*49*	*17*	*47*	*36*	30	61	08	40	65	İ
K	*02*	*19*	*48*	*43*	*42*	20	24	14	31	47	K
L	*33*	*51*	*25*	*10*	*32*	05	52	28	18	22	L
M	*38*	*06*	*35*	*05*	*60*	17	04	46	64	11	M
N	*43*	*01*	*09*	*27*	*35*	44	66	12	59	30	N
O	*47*	*11*	*37*	*59*	*64*	25	22	56	71	14	O
P	*14*	*07*	*56*	*49*	*13*	19	44	38	27	07	P
Q	*44*	*25*	*11*	*21*	*48*	28	51	17	35	29	Q
R	*17*	*12*	*15*	*40*	*34*	12	57	05	48	57	R
S	*15*	*26*	*52*	*46*	*62*	45	26	37	44	62	S
T	*39*	*21*	*18*	*14*	*01*	38	11	50	56	21	T
U	*03*	*52*	*23*	*53*	*26*	14	49	69	61	25	U
V	*36*	*24*	*54*	*16*	*37*	33	23	59	34	52	V
W	*16*	*50*	*44*	*24*	*53*	43	18	21	53	50	W
X	*40*	*48*	*41*	*33*	*51*	65	45	34	46	12	X
Y	*34*	*37*	*20*	*39*	*18*	23	33	63	36	73	Y
Z	*10*	*53*	*34*	*45*	*59*	02	48	16	54	37	Z
	1	2	3	4	5	6	7	8	9	10	

Figure24. T52d *Spruchschlüssel* — message key.

17 Appendix B

Geheim! **Lw.-RV-Fs. Spr. Schl.** **Prüfnr.**

RV 51 **T 52 c**

1. Monatstag ab 0900 Uhr DGZ

	1	2	3	4	5	6	7	8	9	10	
A	11 z	19 x	49 u	27 s	59 p	61	19	42	10	17	A
B	26 y	29 w	50 t	08 p	07 z	08	24	63	14	62	B
C	05 x	10 t	39 s	56 z	22 y	04	26	12	52	65	C
D	36 u	09 s	13 z	12 x	17 w	32	30	11	17	06	D
E	09 s	17 z	25 x	13 u	15 t	47	45	41	34	11	E
F	47 p	14 y	38 w	14 t	03 s	12	19	03	15	66	F
G	12 w	16 t	56 p	09 y	42 u	30	27	02	58	57	G
H	08 t	32 p	17 y	23 w	46 x	65	09	44	02	64	H
I	42 p	19 s	27 t	13 u	58 w	08	67	40	52	20	I
K	34 x	28 y	26 z	21 p	10 s	11	45	61	57	50	K
L	29 t	20 u	43 w	32 x	52 y	23	09	60	49	11	L
M	27 z	27 p	33 s	41 t	15 u	52	11	09	12	59	M
N	28 w	09 x	34 y	59 z	47 p	40	53	66	39	24	N
O	45 s	23 t	14 u	44 w	19 x	48	57	67	32	48	O
P	35 y	43 z	09 p	53 s	10 t	52	49	30	43	31	P
Q	03 u	35 w	52 x	02 y	08 z	26	34	10	23	28	Q
R	46 p	14 s	06 t	32 u	18 w	62	15	66	24	17	R
S	16 z	38 y	32 x	30 s	12 p	12	35	50	20	15	S
T	14 w	04 t	27 p	29 x	45 z	20	32	04	47	40	T
U	19 s	27 u	28 z	21 w	39 t	31	38	57	66	48	U
V	45 x	05 w	09 u	03 z	46 y	45	14	19	05	03	V
W	44 t	34 p	20 s	56 y	05 u	38	62	62	34	16	W
X	33 p	03 x	10 t	59 u	24 w	15	24	37	39	10	X
Y	30 u	45 t	55 z	02 x	21 p	52	30	18	21	12	Y
Z	14 y	22 z	09 w	28 s	34 x	39	02	13	16	61	Z
	1	2	3	4	5	6	7	8	9	10	

Figure25. T52c *Spruchschlüssel* — message key.

18 Appendix C

NORD NR. 3

Geheime Kommandosache! [redacted] Nr. 00114

Norwegen Nr. 7

Wehrmacht-Fernschreibgrundschlüssel für die SFM T 52 d

(W.Fschr.Grd.Schl.)

Wechsel täglich um 0900 Uhr DGZ.

Nach Ablauf der Gültigkeit tageweise abschneiden und vorschriftsmäßig vernichten!

Monatstag	Einstellungen									
	A	B	C	D	E	F	G	H	I	K
31.	V	IV	3—8	III	1—6	4—10	I	2—5	II	7—9
30.	7—9	II	V	1—3	III	4—10	2—6	5—8	I	IV
29.	6—9	3—7	I	5—10	V	2—4	1—8	III	II	IV
28.	6—10	I	2—5	V	3—8	II	III	1—4	7—9	IV
27.	IV	4—8	II	1—9	V	III	6—10	I	3—5	2—7
26.	2—9	I	6—8	1—3	II	4—7	V	IV	5—10	III
25.	6—8	3—7	I	9—10	2—5	V	IV	1—4	III	II
24.	8—10	V	4—6	I	III	3—9	2—5	II	1—7	IV
23.	I	III	3—6	8—10	II	1—5	IV	7—9	V	2—4
22.	V	2—8	6—9	I	3—10	IV	1—5	4—7	II	III
21.	3—5	IV	II	1—6	III	2—10	I	V	7—9	4—8
20.	V	5—6	IV	7—10	I	1—3	4—9	III	2—8	II
19.	9—10	IV	7—8	V	3—5	1—4	I	2—6	III	II
18.	3—10	V	II	7—8	I	2—4	IV	1—9	III	5—6
17.	4—6	1—2	IV	II	5—9	III	3—7	I	8—10	V
16.	II	III	2—6	I	5—10	7—8	IV	1—3	4—9	V
15.	I	6—10	III	2—4	V	1—8	5—9	IV	II	3—7
14.	3—8	III	2—7	V	1—4	I	IV	5—6	II	9—10
13.	1—7	II	3—8	4—6	IV	5—9	I	2—10	III	V
12.	II	1—3	V	2—9	I	4—6	7—8	IV	5—10	III
11.	III	5—10	IV	4—8	2—7	I	V	1—6	3—9	II
10.	2—8	III	6—10	5—7	II	V	3—4	IV	I	1—9
9.	1—2	5—8	III	I	4—6	7—10	IV	V	3—9	II
8.	6—8	IV	2—10	III	5—7	V	1—4	II	I	3—9
7.	V	9—10	IV	1—3	5—8	I	II	4—6	2—7	III
6.	IV	II	1—9	2—10	III	4—8	I	3—7	V	5—6
5.	1—3	III	I	IV	4—7	V	6—8	II	2—5	9—10
4.	IV	4—8	1—5	II	6—9	3—10	V	I	2—7	III
~~3.~~	~~2—8~~	~~IV~~	~~I~~	~~9—10~~	~~II~~	~~1—6~~	~~4—7~~	~~V~~	~~III~~	~~3—5~~
~~2.~~	~~V~~	~~9—10~~	~~I~~	~~4—8~~	~~IV~~	~~1—6~~	~~III~~	~~3—5~~	~~II~~	~~2—7~~
~~1.~~	~~6—8~~	~~1—2~~	~~5—7~~	~~III~~	~~4—10~~	~~IV~~	~~II~~	~~I~~	~~3—9~~	~~V~~

Figure26. T52d *Grundschlüssel* — main inner key.

Subject Index