The Hagelin Cryptographers C-52 and CX-52

Bart Wessel

Keywords: Hagelin; Crypto AG; Cryptoteknik; C-52; CX-52

Abstract

While the C-52 and CX-52 devices enter the open market and are exhibited in museums, it is hard to the untrained eye tell the differences. There is a lot of confusion, and half-truths muddle the waters even further.

It turns out that there is only a limited number of standard configurations of C-52 and CX-52 machines. These 'models' are described in detail, to enable the reader to identify machines he/she comes across. All the configurable components are described to aid in the understanding of their differences and of the way the devices work.

The C-52 is usually cryptographically limited compared to the CX-52 – although an equally limited CX-52 is entirely possible! It all seems to come down to marketing and willingness of Hagelin to sell a certain cryptologic complexity to a particular customer – with the NSA looking over his shoulder.

The cryptologic quality of the various models is not explained here in mathematical detail. The author hopes to have presented a defining framework of configurable variables which can be built upon by a more crypto-analytical minded author.

Introduction

The Hagelin C-52 and CX-52 are deceivingly simple looking mechanical cryptographic machines that date from the early 1950's and are familiar to many cryptography enthusiasts, collectors and museums. Crypto AG, owned by Boris Hagelin[1], secretly created machines that differ in internal configuration without the customer being aware.

The C-52 and CX-52 devices seem, by virtue of their names, to date from 1952. Yet in August 1950 key features of the C(X)-52 where already in development and shared with AFSA (Armed Forces Security Agency, the forerunner of the NSA). In September Friedman[2] refers to the description of an apparently new Hagelin design with an internal AFSA note that starts "I think you'll find this rather interesting" [i].

A 1954 NSA report [ii] on preliminary studies on agency COMINT needs for large-scale analytic equipment mentions that:

> *Any CX-52 traffic that appears will tax our present facilities severely. It will require more complicated, faster programs; and most of the present special-purpose equipment will not be applicable.*

Widespread uncontrolled use of the CX-52 was clearly undesirable from the point of view of the NSA. In January 1955 there is talk of AFSA loaning a C-52 and a CX-52 from Hagelin, a little later some machines were ordered from the factory, indicating serious interest from AFSA in this development.

[1] **Boris Caesar Wilhelm Hagelin** (1892 –1983).

[2] **William Frederick Friedman** (1891 –1969) was a US Army cryptographer who ran the research division of the Army's Signal Intelligence Service (SIS) in the 1930s, and parts of its follow-on services into the 1950s (Wikipedia). He and Boris Hagelin became good personal friends.

The C-52 and CX-52 form a family of machines, there is no such thing as ‘the’ C-52 or ‘the’ CX-52.
A C-52 and a CX-52 can be internally configured to function identically, or two CX-52’s can be configured to perform wildly differently – and still both be labeled **Type CX-52, Series D**.

The name plate does not reflect the actual configuration of the machine as part of the companies’ explicit rouse to keep customers uninformed. Today, this leads to confusion among collectors and curators as seemingly identical machines behave very differently.

By comparing a multitude of machines, original factory brochures and spare part lists, this study aims to identify the internal configurations of C-52 and CX-52 machines. To distinguish between them, we use the term ‘models’. Some models are identified and described from documentation even when no actual machine of that configuration has been spotted yet.

It seems likely that specific configured behavior may have been destined for specific customers (countries) or groups of customers (regions/ideologies) and was fully intended so by Hagelin.

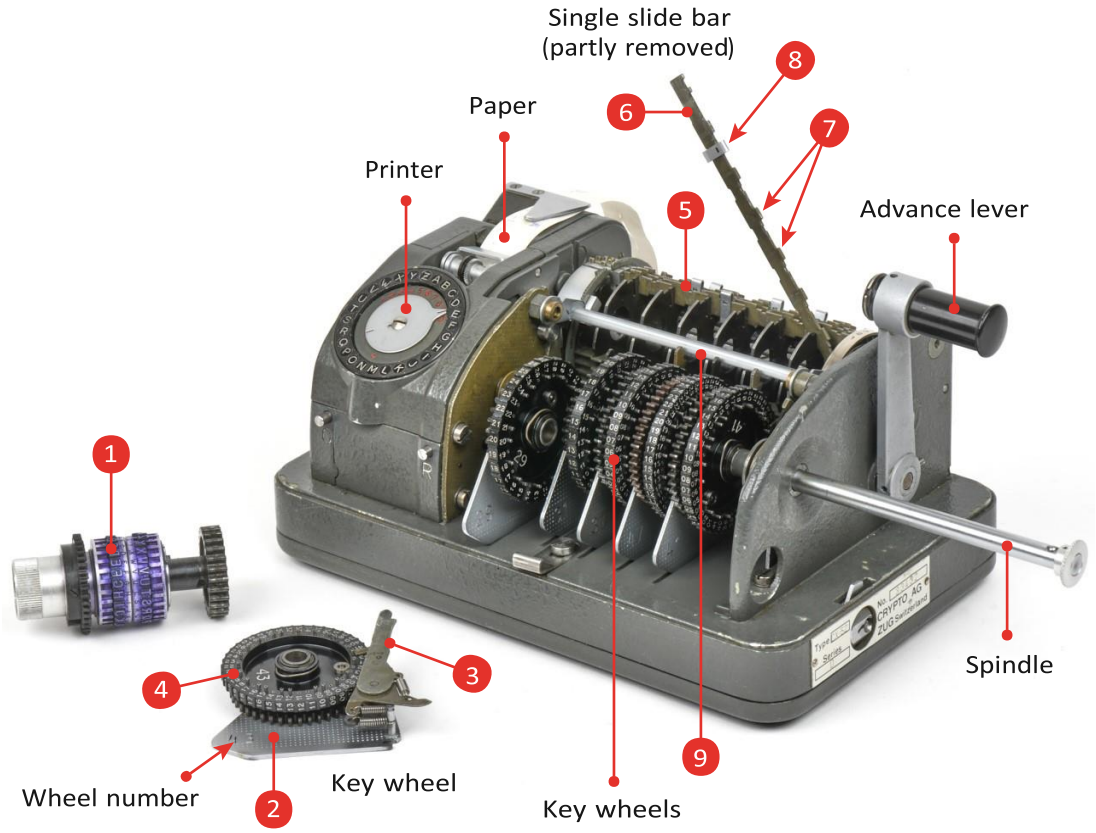
The C-52 and CX-52 share a lot of parts, most notably: the housings are identical. Many of the parts carry similar part numbers; *C-46750 Side cover cpl.* [iii] is identical and exchangeable with *CX-46750 Side cover, complete* [iv]. Where parts differ, the part numbers bear no relationship. Differences (mainly in the drum and the drive mechanism for the keywheels) are described in detail.

Terminology

Some of the terms and concepts are introduced immediately for reasons of clarity and consistency. Also three identifiers are introduced: types, series and models. It is important to understand the differences.

Terms

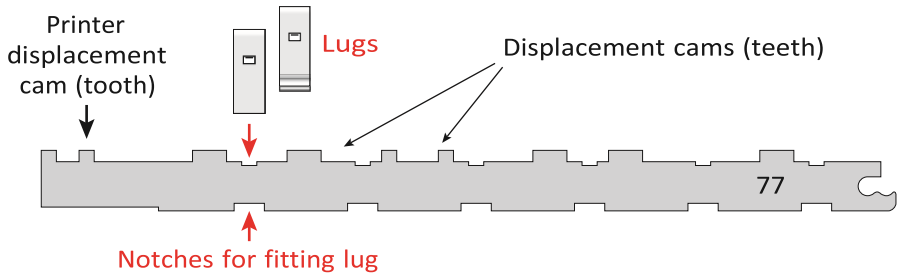
The terms in **Bold typeface** have been taken from the manual *Instructions for Operator* [v], the *Spare parts catalogue* [vi], *THE STORY OF THE HAGELIN CRYPTOS* [vii], or *Description of CRYPTOGRAPHERS "HAGELIN" TYPE CX-52* [viii]. In brackets are terms that may be familiar from descriptions of other makes of machines.



1. **Typewheel unit**, **alphabet unit, print wheels**, (print head). Contains primary typewheel and secondary typewheel. Rotation is referred to as **displacement** in **displacement steps**.
2. **Journal plate**. Forms a complete assembly together with the guide arm and the keywheel
3. **Guide arm** (sensing arm). Each keywheel has its own.
4. **Keywheel**, **key wheel**, **pin disk**¸ (cipherwheel, pin-wheel). Rotation is referred to as **advancement** to distinguish between movement of the alphabet unit and the keywheels. One speaks of the **arrangement** of pins on a pin disk.
5. **Bar drum**, **drum**, (cage). Holds the 32 slide bars.
6. **Bar**, **slide bar,** (sideways moveable bar). The word **displacement** is also used in connection with the slide bars. We call the default right-hand position the **undisplaced** and the left-hand position the **displaced** position. Depending on the cams on the bar we distinguish **Advance bars** and **Non-advance bars**.
7. **Cam**, **tooth**. Cams are used to displace the typewheel unit and advance the keywheels.
8. **Lug**, **bar lug**. Lugs are placed by the user as part of the key.
9. **Locking bar**, **top cradle**. Locks the guide arms in the CX-52 and limits their movement in the C-52.

Ciphering is used to avoid repetition of the expression ‘enciphering or deciphering’.

Slide bar specification



As an example, this fictional slide bar 77 is specified as follows:

	(left)					(right)		
print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
K	0	A	B	0	C	0	77	

- Cams, one for printwheel and six for keywheels:

```
K: displace print wheel when bar displaced.
A: advance this keywheel when bar displaced.
B: advance this keywheel when bar not displaced.
C: advance this keywheel.
0: do not advance this keywheel.
```

- Bar-id: specific number on the slide bar to identify it. This fictional bar (no slide bar has been identified that incorporates all the different cams) has number 77.
- Lugs: some bars cannot be lugged. If it cannot be lugged, this is indicated by ‘No’.

Slide bars and their cams are explained in extensive detail below.

C(X)-52Types, series and models

There are a number of publicly available documents on the C(X)-52. From these, the meaning of the type, series and model designators become clearer. These documents also give an idea of how the NSA viewed the machine at the time. This research however does not claim to be complete.

Types

The ‘type’ designator only distinguishes the machine from earlier ones like the C-446 and M-209. All C-52’s are labeled **Type C-52** and all CX-52’s are labeled **Type CX-52** on the serial number plate.

Series

‘Series’ refers to the designator (none, A, B, C and D are known so far) on the serial number plate like for example **Type CX-52, Series D**. In the *spare parts catalogue* [vi], the series A, B, C and D are mentioned (see for example pages 5, 15, 16).

Spare part catalogues suggest a strong link between the series designator and the serial number. At least minor manufacturing differences between the series exist. The series designator appears to indicate a state of mechanical evolution during the production life cycle of the C(X)-52.

For the C-52, recognizable mechanical changes in development are:

Series	Serial number	Slide bar retaining ring	Lock type	typewheel/Index wheel
Series B onwards		Shift lock		
Series A & B			Cross key	
	< 25.000		Cross key	
Series C onward			Flat key	
Series A & B & C				Conical gear
	< 25.000			Conical gear
Series D onwards				Straight gear

For the CX-52, recognizable mechanical changes in development are:

Series	Serial number	Slide bar retaining ring	Lock type	typewheel/index wheel
Series A		Push-pin		
	< 21.999	Push-pin		
Series B onwards		Shift lock		
Series A & B			Cross key	
	21.101 … 21.999		Cross key	
Series C & D onwards			Flat key	
Series A & B & C				Conical gear
	21.101 … 21.999			Conical gear
Series D onwards				Straight gear

Notes:

- The slide bar retaining ring can be rotated after unlocking it. In early versions, this is done by pushing down a small locking pin. With later versions, the pin is to be shifted.
- The cross key lock is familiar from the C-446 and BC-543 machines. This type of lock was later replaced by one with a common flat key.
- The connection between the operating knob and the index pointer is made by means of interlocking gears. The shape and number of teeth in these gears changed starting with Series D.

Models

Machines with identical type and series designators on the serial number plate may however behave very differently. This phenomenon has added greatly to the confusion in understanding how 'the CX-52' actually works.

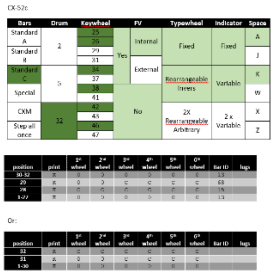
The 'model' designator is used to distinguish between internally different CX-52's and C-52's. A model can be understood to be a C(X)-52 with a specific set of configuration options, implying a specific cryptographic behavior and strength. The model is not indicated anywhere on the machine and only for the CX-52M is its model name publicly identified in the 1960's manuals. Friedman and Hagelin used it as a secret designator, but confusingly called it 'secret type', too easily confused with the 'type' as labeled on the serial number plate.

As models, **CX-52a**, **CX-52b**, **CX-52c, CX-52M** (**CXM-52**, **CX-52-M**) and **CX-52RT** (**CX/RT**, **RT/CX**) have been identified.

For the C-52 the **C-52[c2]**, **C-52[d]** and **C-52Y** models are identified, the latter never went into production. Square brackets indicate model names created by de author in lieu of official documentation.

The full range of C(X)-52 machines is by no means clear. No documents from the manufacturer defining all the different models and configurations have yet been made public. There are publications however that touch upon the subject.

Model sheets



Bars	Drum	Keywheel	FV	Typewheel	Indicator	Space
Standard A	2	25	Yes	Internal	Fixed	Fixed	A
Standard A		29				J
Standard A		31		External		
Standard A	3	33		Rearrangeable	Variable	K
Special		37		Dress		W
CKM		38	No	2X Rearrangeable Arbitrary	2 x Variable	X
Step all once	32	41				Z
		43				
		45				
		47				

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
01-32	R	0	0	C	C	C	C	69	
29	R	0	0	C	C	C	C	69	
29	R	0	0	C	C	C	C	69	
1-27	R	0	0	C	C	C	C	69	

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
32	R	C	C	C	C	C	C		
31	R	0	0	C	C	C	C		
1-30	R	0	0	C	C	C	C		

To be able to quickly identify the properties of a machine, model sheets are used by the author as shown in the example. Appendix A shows model sheets for the main models identified. All of the properties shown are explained in the following chapters.

How the machine works

It is imperative to have a basic knowledge of how the machine works to understand the effect of each configurable part on the cryptographic process. C(X)-52 machines are configurable in that some features may or may not be present and that some parts may be exchanged for similar but functionally different parts.

The cryptographic heart of the machine consists of a drum with 32 slide bars, six rotatable keywheels with pins, and the typewheel unit with two print wheels. There is a drive mechanism and an input character selection mechanism, both hand operated. See also for example [ix].

Although essential for the function of the machine as a whole, some mechanisms like the printer, counter, primary letter indicator, paper tape cutting and transport system are not described in detail here because they do not affect the cryptographic process itself. They are identical in all machines.

We assume a fully set-up device. Any configuration and key-setting procedures are assumed to be taken care of which includes setting of the pins on the keywheels, the setup of lugs on the slide bars and resetting the counter. This description is purely to describe how the different parts of the machine operate on each other so that the effect of variations can be understood later on.

The encryption process is a Beaufort cipher, which is a polyalphabetic substitution cipher similar to Vigenère but with the second alphabet reversed. The primary (left-hand) print wheel contains the normal alphabet, the secondary print wheel the reversed alphabet. For each new input letter, a mechanical pseudorandom generator (PRG) dictates the amount of displacement. The PRG is made up of the keywheels with pins, the guide arms, and the slide bars with lugs in the drum.

The ciphering and deciphering processes are cryptographically identical. They only differ in that ciphering adds spaces to group the output and deciphering translates a dedicated ‘space character’ to an actual space in the output. For this reason, only the ciphering process is described.

Global description of operation

For the operator, a ciphering cycle consists of:

1. On the left-hand side of the machine, turn the operating knob of the typewheel unit to select the letter that is to be ciphered on the alphabet ring at the front of the machine.
2. Operate the handle on the right-hand side of the machine and let it return. The handle remains locked until a new input letter is selected.

These steps are repeated until the message is completely ciphered.

During a ciphering cycle, the following happens:

- At the start of each cycle the clear text letter is printed on the left hand side of the paper by the left-hand print wheel of the typewheel unit.
- While the drum makes one full rotation, lugs on the 32 slide bars are exposed to six guide arms, each corresponding to one of the six keywheels. Depending on the pins on the keywheels, some guide arms will be activated, some remain inactive. Interaction between active guide arms and lugs on the bars will displace some slide bars to the left where they act as teeth on a gear wheel to rotate the typewheel unit, thus constituting the transformation of the input letter. The effective number of teeth varies for each new cipher cycle.
- Additionally, slide bars can have cams that can advance keywheels, so that the next cycle starts with a different keywheel setting and thus another set of six active and inactive pins.

- At the end of the cycle, the encrypted character is printed on the right hand side of the paper by the right hand print wheel, the tape is advanced and cut into two strips.

Indicating ring and typewheel unit

The indicator is directly linked to the primary (left hand) printwheel so that the user can choose a letter. The two printwheels contain alphabets running in the opposite directions. This is what makes enciphering and deciphering identical processes. Both print wheels are normally rotationally fixed with respect to each other, more on this later.

Keywheels, pins, guide arms

The number of displacement steps of the typewheel unit during a cycle is dictated by the combination of active pins on the keywheels and lugs on the slide bars.

Keywheels have a number of pins that are set active (protrude to the right) as part of the key. Each keywheel has a guide arm that interacts with the pins. The guide arm probes the keywheel for a pin at a fixed position in the machine. When it senses an active pin, the guide arm is displaced towards the rear of the machine and is considered active.

When the keywheel advances, the guide arm becomes successively activated or not, depending on the pin pattern of the keywheel. Thus the six keywheels present a pattern of six adjacent guide arms that are active or inactive, depending on the six pin patterns. With each advancement of one or more keywheels, the pattern of adjacent guide arms is established anew.

Drum, slide bars, lugs, cams

The drum contains 32 slide bars. Each slide bar has six positions where lugs can be placed, corresponding to the six keywheels. Lug placement is part of the key. When an active guide arm meets a lug on a slide bar during the ciphering cycle, that bar is displaced to the left and displaces the typewheel unit one step.

Each slide bar can only be displaced once during every cycle, even if it has multiple lugs. Multiple lugs will however increase the chance that it will become displaced. To confuse things, some slide bars cannot carry lugs and thus will never be displaced.

On the m-209 and similar older machines, all wheels advance one step at the end of each cycle. What makes the C(X)-52 stand out is that advancement of the keywheels is now controlled by additional cams (or ‘teeth’) on the slide bars. Slide bars that contain such cams are called **advance bars**. Different types of these cams on the slide bars allow for configurable irregular advancement of the keywheels.

As a result, subsequent ciphering cycles will not only result in a different number of typewheel displacement steps and thus in a different encryption, but may also induce irregular advancement of the keywheels.

CX-52 left-hand keywheel advancement

It is suggested online ([x] for example, but not exclusively) that the first or left-hand keywheel is always advanced during the cipher cycle. This is not necessarily true. There is no fixed mechanism in the C(X)-52 machines to cause this effect.

However, particular models have one bar with an ‘always advance’ cam for the first keywheel, which forces the left-hand keywheel to advance once during every cipher cycle. It is important to note this is a configurable property and not an inextricable C(X)-52 design feature.

CX-52 guide arms latching

We initially anticipated that the guide arms – commanded by pins in the pinwheels – would be able to change from active to inactive (or vice versa) during the cipher cycle when keywheels advance. This would constitute a major part of the cryptologic because the order of advance bars in the drum would become of importance. However, there is evidence to the contrary: none of the investigated CX machines mechanically allows for it and it is contradicted in at least one official document [xi]:

> *The position of the guide arm, determined by the keywheel pins at the beginning of each operation, must remain the same until its completion, even while the keywheels are displaced, and the guidearms must not prevent the keywheels from being displaced.*

In actual fact, at the start of the cipher cycle in the CX-52 the guide arms are selected by the active pins on the six pin wheels. Next, still at the beginning of the cipher cycle, they are latched into place by the locking bar (sometimes referred to as top cradle) for the duration of the cycle. It is important to note that during the cipher cycle keywheels may rotate such that some pin wheels rotate into an active or inactive position but the guide arms stay latched and their new selection is only effectuated at the start of the next cipher cycle.

As a result, the order of the advance bars in the bar drum (as far as their effect on the advancement of the wheels is concerned) is of no cryptographic importance.

C-52 guide arms, top cradle and keywheel advancement

The C-52 uses a different advance mechanism for the keywheels which would allow for changes in the active guide arm pattern during the cycle, but it is prevented in all investigated machines.

The top cradle does not lock the guide arms during the cipher cycle. It limits their movement, but only to within both extremes of their function. This means that the guide arms – driven by the pins in the pinwheels – would be able to change from active or inactive (or vice versa) during the cipher cycle when keywheels advance during the cycle. Not only would this complicate the cryptologic, it would also mean that the order of the advance bars in the drum would become of importance.

However, by special design of the supporting disks in the drum, keywheel advancement is blocked for all of the slide bars except the last two. Then, by using (in the last two positions) two unluggable advance bars that have unconditional advance cams, the order of the advance bars becomes unimportant and the advancement of the keywheels becomes regular.

Experiments with C-52 wheels in a CX-52 machine show that changes in the active and inactive guide arm pattern during the cipher cycle are possible, but not reliable. It is surmised that this functionality has been traded for reliability.

Model overview

Appendix A presents model sheets for every model identified.

Standard models CX-52a, CX-52b and CX-52c

Friedman visited Hagelin in February 1955 to propose a deal whereby Hagelin would refrain from supplying the cryptographically stronger CX-52 to countries that might be considered unfriendly by the NSA. The CX-52 would simply not be mentioned and a cryptographically weaker C-52 would be offered instead. Even for friendly and for NATO countries variations in cryptographic strength remain possible by supplying different models of the CX-52.

The official report of Friedman's visit to Hagelin mentions discussions on some of the cryptographic characteristics of the C-52 and CX-52. The report was kept secret, but in 2014 three different censored versions [xii] were declassified by the NSA. As censoring is not identical in all three versions, combined they bring out more information into the public realm than was probably intended.

In this report, in paragraph II. 1. d. (2), 'Class 2 machines' are mentioned with the following models with the 'secret designators' (which we refer to as models):

1. CX-52a (& 4. CX-52ak)
2. CX-52b (& 5. CX-52bk)
3. CX-52c (& 6. CX-52ck)
7. CX-52/10
8. CX-52/30
9. CX-52/RT

The models 4, 5, and 6 carry the 'k' designator to indicate the Hüttenhain (also 'Komplementär' or 'Complimentary') feature, which is not discussed here.
The RT is the Random Tape or One Time Tape (OTT) machine. It is a very strong concept but is not a prime part of this research into the CX-52 proper. The /10 and /30 machines are modified for ciphering numbers or non-roman alphabets, which bears no major implications on the cryptologic way in which the CX-52 works. Thus, they fall outside the scope of this report.

The CX-52a, CX-52b and CX-52c models in this list (note the lower case a, b & c) refer to the use of Standard type A, Standard type B and Standard type C slide bar sets. To a great extent, these standard sets of slide bars define the models **CX-52a**, **CX-52b**, and **CX-52c**.

Model CX-52a

This machine uses the Standard A slide bars, which produce irregular angular advancement of the keywheels, each wheel advancing 0, 1, 2, 3, 4 or 5 steps per cycle. The keywheels are 29, 31, 37, 41, 43 and 47.

Model CX-52b

This machine uses the Standard B slide bars, which produce fixed angular advancement of the keywheels: all wheels advancing the same number of steps per cycle but the number varies between 1 and 32 per cycle. The keywheels are 29, 31, 37, 41, 42 and 47.

Model CX-52c

This machine uses the Standard C slide bars, which makes it compatible with the older types of machines like the C-446, the M-209 or a special type of C-52. Mandatory keywheels are 25, 26, 46, 42, 38 and 34, in that order.

Model CX-52M (also: CXM-52, CX-52-M)

The CX-52M is a later development with five specific advance bars with a prescribed lugging pattern that the user is not allowed to alter. Initially, these bars were also used for displacing the typewheel unit, but this was found to be confusing and later five advance bars were used that could be lugged but not displace the typewheel, leaving 27 that could. Six 47-position keywheels are mandatory.

Model C-52[c2]

The Crypto AG document *No. 3011-c, THE CRYPTOGRAPH TYPE C-52 Specifications* [xiii] mentions: '*Standard "C2" drum bars for correspondence between C-52 and C-4 or similar machines*'.

By using the Standard C slide bars, this machine is compatible with the older types of machines like the C-446, the M-209 or the CX-52c. As such, it would need the keywheel set 25-26-34-38-42-46, the ones over 30 are stepped twice in each cycle, effectively halving their period.

However, it can also use keywheels with more steps than the ones in the M-209 and it can be provided with 32 slide bars which is five more than the M-209.

Model C-52[d]

The same document also mentions: '*Standard "D" for organizations using C-52 cipher machines*'.

The Standard D slide bar set is assumed to have just one advance bar that advances all keywheels one step. This should not be used with 6 identical keywheels.

Model C-52Y

Friedman's REPORT OF VISIT [xii] in II. 1. e. (1) onwards mentions a C-52Y:

> *e. (1) However, there is a new C-52 machine which is of interest, and which Hagelin Junior mentioned with much enthusiasm. This model we agreed to call the C-52Y.*
>
> *(2) In the C-52Y, the print wheel may be advanced according to combinations of one to 4 different amounts, and each of the key wheels may also be advanced according to combinations of one to 4 different amounts. Perhaps the best way to explain what this model will do is first to mention what the M-209 or the C-446, or the ordinary C-52 does. In each of these models, if there are say 4 lugs presented to a key wheel and the latter is in "active" position, the print wheel advances 4 steps; but in the C-52Y this same condition can bring about 4 kinds or amounts of stepping of the print wheel: 0, 1, 3, or 4 steps can be made, depending upon the particular slide bar and lug arrangements in the cage. Or, if 7 lugs are presented to a key wheel (and the latter is in "active" position), the print wheel can advance 0, 3, 4, or 7 steps by one arrangement; or 0, 2, 5, 7 steps by a second arrangement; or 0, 1, 6, 7 steps by a third arrangement (the total amount is the sum of the 4 parts). So much for the advance of the print wheel.*
>
> *…*
>
> *This type of action, which was conceived only recently (December 1954), can be brought about in the C-52 merely by placing standard B slide bars in the cage in a certain sequence and with a certain kind of lug assembly.*

How this exactly was to work is yet unclear from this description. However, Hagelin apparently never got it to work reliably. In 1958, Friedman reports[xiv]:

> 9 e Two final and important notes:
> (1) Mr. *Hagelin told me during this conference that, because of technical difficulties, he was giving up the CY-type motion and machine; the firm was going to use [CENSORED] machine models*

Model RT-CX or One Time Tape (OTT)

Any C(X)-52 can easily be adapted to use punched One Time Tape (OTT) instead of the six keywheels with pin disks. A user swappable *RT*-CX mechanism is available to this end. By default [xv], bar lugs are set to the pattern 1-2-4-8-11 to allow for 26 displacements steps.

Note that the sixth bar position is reserved for advancing the paper tape. Sometimes a dedicated non-luggable, non-displacable advancement bar is used with an always advancing (C-) cam in position six and no K-tooth.

In RT machines the relative position of the typewheels is fixed.

With this machine the whole cryptographic strength is in the randomness of the tape. It is not further studied in greater detail in this report.

CX-52 configuration options in detail

The CX-52 is a highly configurable machine. The list of configuration options that affect cryptographic strength include[3]:

- Slide bars.
- Keywheels.
- Indicating ring and typewheel unit.
- F-V feature.

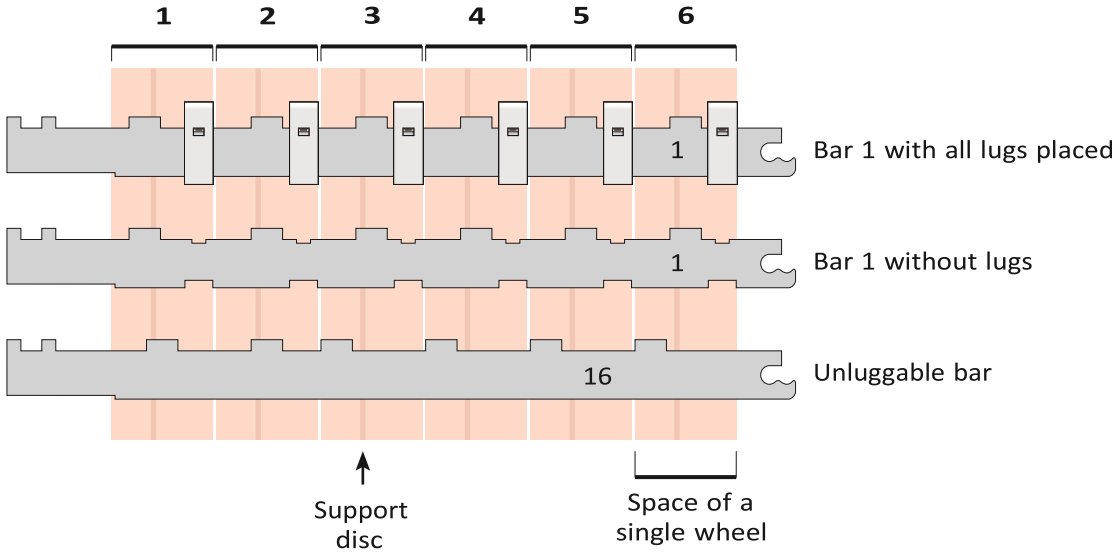
By combining configuration options in different ways, CX-52's with highly different behavior are created. In this way, cryptographic strength can be influenced to a high degree.

The slide bars, the typewheel unit and the indicating ring can be exchanged by the operator or a technician. The keywheels are normally exchanged by the operator. The F-V feature would typically be installed by the factory and never removed.

It is assumed that not all customers were made aware of all available options.

Slide bars

The 32 replaceable bars in the bar drum play an important part in the cryptographic configuration of a C(X)-52. They differ mainly in the way their cams control the advancement of the keywheels. There is a limited number of standard slide bars sets, but individual bars could be ordered from the factory.



It can be derived from the *spare parts catalogue* [vi] that there were 78 different bars available (page 11 or 12, part number CX-46663-1…78) at that point in time. The last digits of the part number identify the bar. In later machines numbers reaching up into 157 have been identified (see appendix B which also contains a handy way to identify the cams on a slide bar you may want to inspect yourself).
Usually (but not always) the ID is stamped into the bar, usually (but not always) slightly to the right of where a lug in position 5 would be. The ID can often be viewed without removing the bar from the bar drum. Sometimes ID's are stamped upside down, more to the left or at the back. However, bars without ID do also exist.

[3] The color of the pin disks for example is not considered of major cryptographic importance. Other such options include: number of characters (normally 26, but 30 and 10 are available), internal or external F-V switching and choice of the 'space'-character.

The bars can normally be easily removed and repositioned by hand. According to [x] this is not always true:

> *There are different versions of the C-52 and CX-52. Some have fixed advance bars spread all over the drum instead of the normal first 5 bars. On some machine versions the advance bars are detachable and their order can be changed.*

In most inspected machines all slide bars were detachable, but in some CX-52-M's the five advance bars at the end of the drum cannot be removed easily.

Furthermore, the order of the bars has no impact on the cryptographic strength (see paragraph *CX-52 guide arms latching*).

Typewheel displacement

The cam on the slide bar responsible for displacing the typewheel is called the K-tooth on the left-hand side. Most of the bars identified displace the typewheel one step if a bar is displaced by an active pin/guide arm/lug combination, in the old M-209/C-446 tradition. However, there are two other types of bars.

No typewheel displacement bars

Some bars never advance the typewheel. To this end the tooth to displace the keywheel is simply absent. According to [x] these bars are used to prevent confusion in setting up the lug pattern:

> *The special wheel movement bars in the early CX-52 setup are also used for enciphering. When using the movement bars also for enciphering the lugs, one must follow the rules as explained above, but also be sure to create a good stepping cycle for the wheels. Therefore, due to complications in preparation of acceptable lug patterns, later CX-52 models use the special movement bars exclusively for the stepping of the pin wheels and no longer had a thoot [sic] at their left side to advance the print wheel.*

If the K-tooth is absent, it is marked in the table as '-'.

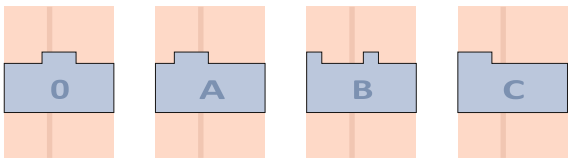
Inverse typewheel displacement bars

This type of bar carries only one tooth on the left side, positioned in the middle of the normal two teeth. This single tooth only displaces the typewheel when the bar is *not* displaced by an active pin/guide arm/lug combination. In the table this tooth is marked '$\overline{\mathrm{K}}$'.

This type of bar has so far only been found in one CX-52 RT. It can be used to personalize machines, so that various groups of users within a client's organization cannot read each other's messages, even if they have access to the same key.

Keywheel advancement

Bars can differ in the effect they have on advancing the keywheels during the cipher cycle. Note that there are six keywheels. This means that to fully define one bar, its effect on each of the six keywheels has to be defined.



For each of the six keywheels, a bar can have a **cam**, or **tooth**, that advances that specific keywheel. Cams come in four different forms, each with a different effect. Cams are defined by their width and position on the bar:

0 Do not advance.
This is standard behavior for bars that match the familiar ones in the M-209 and like machines. Such cams never advance a keywheel.

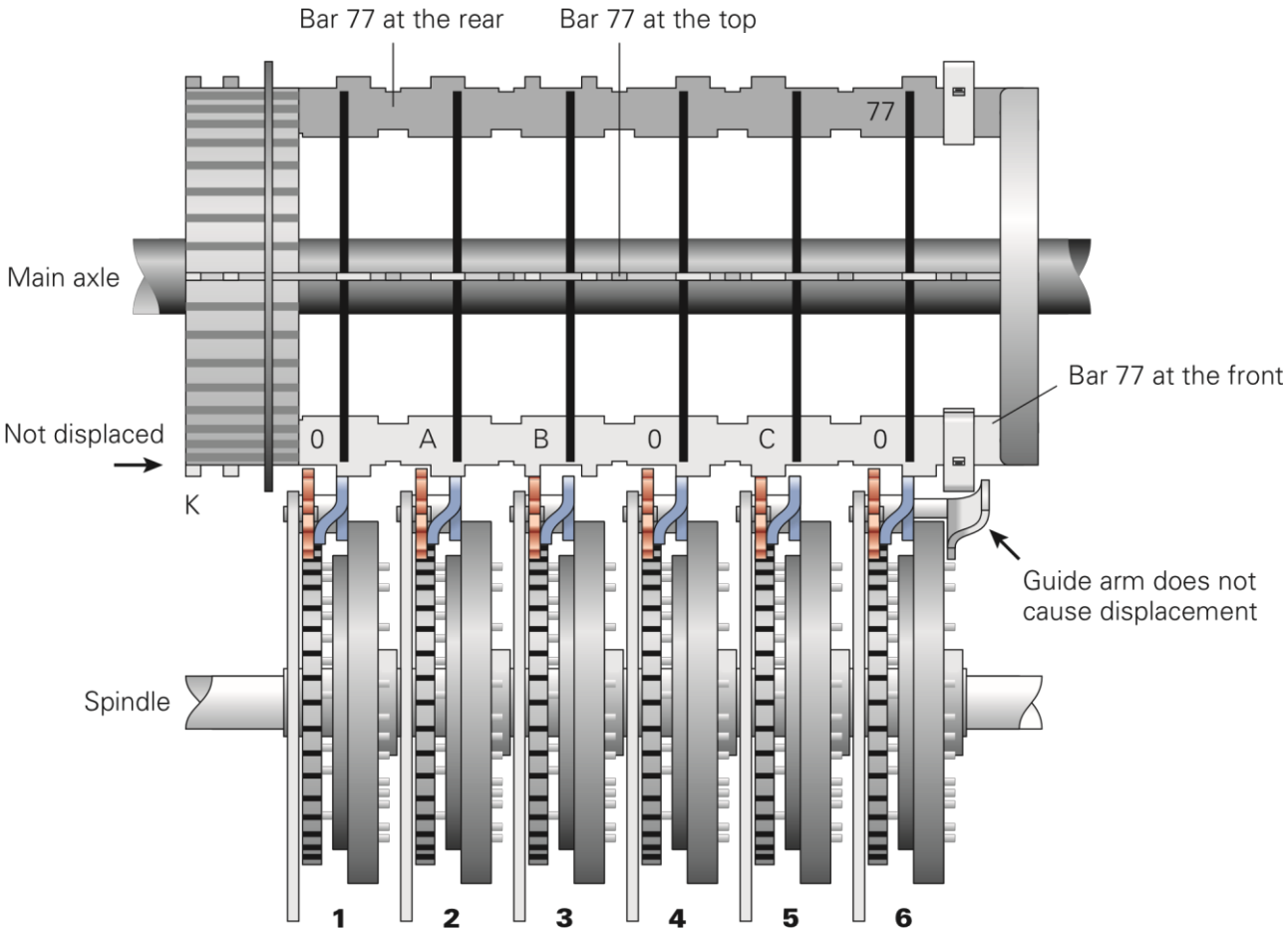
A Advance if displaced.
Only if the bar is displaced by means of an active pin/guide arm/lug combination, this cam operates a gear on the keywheel and advances it.

B Advance if not displaced.
This cam only advances the corresponding keywheel if the bar is not displaced.

C Always advance.
This cam advances a keywheel regardless of whether the bar is displaced or not.

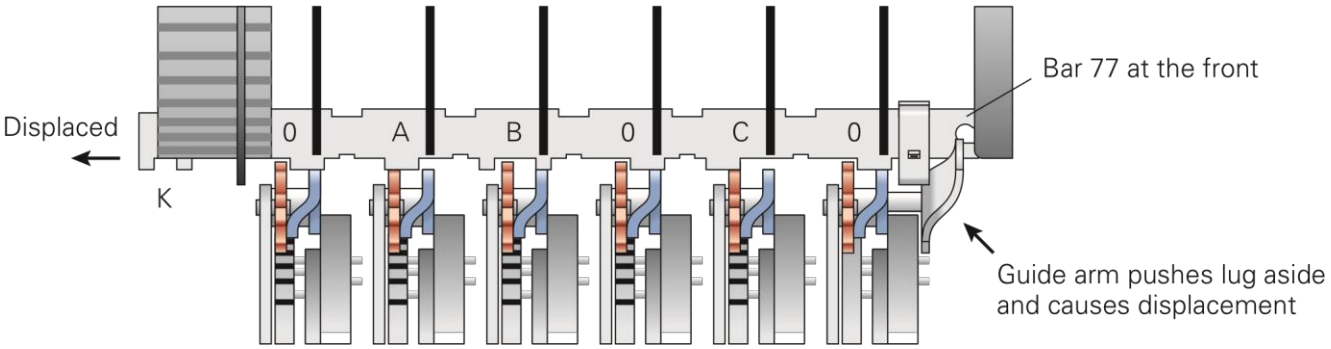
Bars that have advancement cams (type A, B or C) are called **advance bars**. A particular machine can for example have two advancement bars, and thirty **non-advance bars**.

Note that when a cam on a bar does not advance a keywheel it locks advancement of that keywheel by blocking its locking pawl of which the position coincides with the support disc (the darker brown vertical line in the above image). The 0 cam always blocks the locking pawl. The B cam in effect consists of two smaller teeth, the left-hand cam to advance a keywheel and the right-hand cam to block it – only one is effective in each state of the slide bar.



This shows the already introduced fictive slide bar 77 (defined such that it contains all four cams 0, A, B and C – which is not known to exist in real life) and the way it interacts with the six keywheels when the slide bar is not displaced. Only the rightmost guide arm is shown here for clarity.

When a cam interacts with a red gear, that keywheel is advanced (B). Otherwise it prevents the blue locking pawl from moving (0, A & C). In this example, keywheels 3 & 5 will advance.



When the bar is displaced by an active guide arm the effects of cams A and B changes, whereas the effect of cams 0 and C remains the same even though they have moved to the left. In this example, keywheels 2 & 5 will advance.

Displaceable (luggable) /non-displaceable bars

Most bars have six positions where a lug can be placed. A lug makes them displace to the left-hand side if engaged by an active guide arm. Some bars however cannot carry lugs. This implies that they cannot be displaced and thus never displace the typewheel.

C-52 non-displaceable bars

Some non-luggable as in 'cannot be lugged' or non-displaceable bars were identified in a C-52 and a CX-52 RT. Note that non-displaceable slide bar number 18 (K000000) appears identical to slide bar number 13 (K000000). The difference lies in the fact that the former never displaces the print wheel, whereas any lug on the latter might.

Standard A, B and C bars

Friedman's *REPORT OF VISIT* [xii] mentions 'Standard A slide bars' and 'Standard B slide bars'. In the *Description of CRYPTOGRAPHERS "HAGELIN" TYPE CX-52* [viii] 'three different sets of bars' are offered 'as a standard':

REPORT OF VISIT	Description of CRYPTOGRAPHERS "HAGELIN" TYPE CX-52
II. 1. D. (2) (a.) CX-52a: The model with Standard A slide bars (for the cage), which produce irregular or varying angular displacements of the key wheels, each wheel advancing 0, 1, 2, 3, 4, or 5 steps per operation	With standard A, each of the keywheels will be advanced a varying number of steps, from 1 [sic] to 5, the program being determined by placing the lugs.
II. 1. D. (2) (b) CX-52b: The model with Standard B slide bars (for the cage), which produce regular or fixed angular displacements of' the key wheels, all wheels advancing the same number of steps but the number may be any one from 1 to 32	With standard B, the keywheels will always be advanced together, the same number of steps, varying between 1 and 32. The following relation exists between the advancement of the keywheels and the displacement of the alphabetwheel assembly: if the alphabetwheel assembly is displaced n steps, the keywheels will be advanced 32-n steps.
II. 1. D. (2) (c) CX-52c: The model which is compatible with the old	Standard C. … This standard is only used, when machines type CX-52 shall correspond with

types of C machines, the M-209, the C-446, or a certain version of the C-52 machines	machines of earlier types, such as the C-446 or the M-209.

From this, it can be concluded that the Standard A, B and C bar sets match models CX-52a, CX-52b and CX-52c (see *Standard* ***models CX-52a,*** *CX-52b* ***and*** **CX-52c** below). Of course, there is more to these models than just the bars in the drum, for instance: the keywheels.

The Standard bar specifications are given in *Description of CRYPTOGRAPHERS…* (pages 33 – 34) as:

Standard A slide bars

		(left)					(right)
		1st	2nd	3rd	4th	5th	6th
position	print	wheel	wheel	wheel	wheel	wheel	wheel
31-32	K	0	0	0	0	0	0
30	K	0	0	0	0	0	B
26-29	K	0	0	0	0	0	A
25	K	0	0	0	0	B	0
11-24	K	0	0	0	0	A	0
20	K	0	0	0	B	0	0
16-19	K	0	0	0	A	0	0
15	K	0	0	B	0	0	0
11-14	K	0	0	A	0	0	0
10	K	0	B	0	0	0	0
6-9	K	0	A	0	0	0	0
5	K	B	0	0	0	0	0
1-4	K	A	0	0	0	0	0

Position: there are 32 numbered positions in the drum. Here positions 1-4 carry identical bars, position 5 carries a unique one, 6-9 are identical again, etc. The order of the bars in the tables spatially reflects the order of the bars in the drum, i.e. bar 2 will be above bar 1 etc., with bar 32 at the top and last to be processed.

Standard B slide bars

		1st	2nd	3rd	4th	5th	6th
position	print	wheel	wheel	wheel	wheel	wheel	wheel
32	K	C	C	C	C	C	C
1-31	K	B	B	B	B	B	B

Standard C slide bars

		1st	2nd	3rd	4th	5th	6th
position	print	wheel	wheel	wheel	wheel	wheel	wheel
32	K	C	C	C	C	C	C
31	K	0	0	C	C	C	C
1-30	K	0	0	0	0	0	0

In *Spare Parts Catalogue* [xvi] a handwritten variation on Standard C set is inserted:

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Lugs
32	K	0	0	C	C	C	C	
31	K	C	C	C	C	C	C	
28-30	K	0	0	0	0	0	0	No
1-27	K	0	0	0	0	0	0	

An interesting variation spotted (CX-52 No 11810) is:

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel
32	K	C	0	0	0	0	C
31	K	0	0	0	0	C	C
30	K	0	0	0	C	C	0
29	K	0	0	C	C	0	0
28	K	0	C	C	0	0	0
1-27	K	0	0	0	0	0	0

This is functionally similar to the previous two schemes for 'Standard C', but all five advance bars now each advance only two keywheels at the time. This creates a smoother mechanical action.

In theory, an additional four advancement patterns can be created by a customer with such a machine from the original C pattern 112222: 111122, 111111, 112112, and 112211 by removing slide bars from the drum.

CX-52-M bars

In *Usage of Hagelin cryptographer CX-52* [xvii] the bars for the CX-52-M are defined as:

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel
32	–	0	0	0	0	0	A
31	–	0	0	0	0	A	0
30	–	0	0	0	A	0	0
29	–	0	0	A	0	0	0
28	–	C	A	0	0	0	0
1-27	K	0	0	0	0	0	0

The prescribed lugging pattern for these bars is:

position		1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel
32		X	X	X	X	X	–
31		X	X	X	X	–	–
30		X	X	X	–	–	–
29		X	X	–	–	–	–
28		X	–	–	–	–	–

The CRYPTO AG document *Usage of the Hagelin cryptographer CX-52* [xviii] dated 1962 describes the movement scheme as:

"The stepping of the keywheels functions as follows:

1. Key wheel one steps one step for each operation.
2. Key wheel two steps one step whenever there is an active pin on key wheel one.
3. Key wheel three steps one step whenever there is an active pin on either key wheels one or two.
4. Key wheel four steps one step whenever there is an active pin on either key wheels one, two or three.
5. Key wheel five steps one step whenever there is an active pin on either key wheels one, two, three or four.
6. Key wheel six steps one step whenever there is an active pin on either key wheels one, two, three, four or five.

The result of this is that, although their progression is irregular, from any initial alignment the six keywheels will step through every possible offset before coming back to the initial setting. This is a cycle of over 10,000,000,000 steps."

This CRYPTO AG document uses the 'M model' (referring to the secret type M) to explain proper CX-52 use and states: '*Many of the remarks are equally applicable to the older models of the machine CX-52*'. This suggests that the CX-52-M configuration was introduced later, as a viable model on its own.

According to Hagelin, the CXM machine is a compromise between the other two (C and CX) machines [xxiv]. Of the period, he writes:

> *All six wheels having the same number of divisions, the length of the period will be n^6, or with six wheels with 47 divisions a length of about 10^{10}.*

Note that this description of the type CXM does not specify the F-V feature nor the typewheel unit.

Note that the five advance bars do not displace the typewheel unit:

> *In an early version of the CX-52-M ciphering machine the first five bars contributed to both the key and the stepping of the keywheels. This complicated greatly the preparation of acceptable lugging patterns. There are also theoretical advantages to a complete independence of the key from the stepping. Consequently on later models of this machine the effect of these five bars has been limited to the [advancement] of the keywheels.*

Note also that the five advance bars are confusingly mentioned as *the first five bars* where illustrations clearly identify them as bars 28-32. *First* might refer to the specification in a table, but they are *last* in the cipher cycle.

CX-52, Irish bars

A CX-52 that stems from Eire looks like a modified CX-52c with one advance bar removed and 6 new advance bars scattered across the drum. These bars numbered 2, 4, 35, 56, 60 & 64 are made of a remarkably brighter metal:

position	print	(left) 1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	(right) 6th wheel	bar ID	lugs
29	K	0	0	0	0	A	A	64	
28	K	0	0	C	C	C	C	16	no
20	K	0	0	A	A	0	0	60	
11	K	A	A	0	0	0	0	56	
10	K	0	B	0	0	0	0	4	
6	K	B	0	0	0	0	0	2	
3	K	0	0	B	B	B	B	35	
all others	K	0	0	0	0	0	0	13	

How its cryptographic strength relates to that of the standard types will be the subject of a follow up study.

Special bars, user defined

The factory could deliver special bar configurations on demand. Whether this was always advertised to the customer is not known.

List of identified bars

The table in Appendix B lists identified bars to date.

Keywheels

There is not one standard keywheel configuration for the CX-52. There are twelve different keywheels available with 25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46 & 47 pins on the disks. A choice of six replaceable keywheels is used in the CX-52.

In practice, three different wheel sets are typically used:

- Set of six identical 47 pin keywheels – this would give to the largest key space for the start setting of the keywheels, but not necessarily the largest key period. Mandatory for the CX-52M, but can also be used on its own. In a CX-52M they are additionally labeled A to F for easy reference.
- The set 25-26-34-38-42-46 offers backward compatibility with M-209-like devices and the C-52[c] but can also be used on its own. For M-209 compatibility, the wheel order 26-25-46-42-38-34 is set up and the first two wheels (26-25) are advanced just once at the end of the cycle. The remaining keywheels are advanced twice, effectively halving their lengths to 23-21-19-17. Care must be taken to properly pin those four keywheels, as half of their positions will not be used.
- The complimentary set 29-31-37-41-43-47.

Except for the M-209 emulation setup where specific keywheels have a mandatory order, keywheels and their order in the machine can be changed at will to quickly establish a different key.

Indicating ring and typewheel unit

The indicator is internally linked to the primary (left hand) print wheel by means of gears.

The typewheel unit contains the two print wheels. These are available with either fixed letters and typeface or with rearrangeable letters and typeface. With the fixed letters, the alphabets run in opposite directions. With the rearrangeable kind, either inverse or arbitrary alphabets can be used. In the latter case, two typewheel units and indicating rings are necessary for enciphering respectively deciphering.

The relative positions of the print wheels can often easily be changed by pulling out the operating knob of the typewheel unit– the actual setting is part of the key.

In machines without the F-V feature, sometimes typewheel units are found with a fixed relative position of the print wheels, often in the A=A position.
In some machines an extra Bakelite ring is used to prevent accidental repositioning during use - to deliberately reposition the printwheels, the typewheel assembly must be removed from the machine before the Bakelite ring can be removed.

Different letters and typeface are available. Normally the typewheels have 26 positions, but special sets of 30 are also available. In that case, a matching indicating ring has to be used.

A special ring with a pin is used to mark the ‘space character’, this is the character that is to be inserted into the plain text stream instead of a space. When decoding, the pin prevents the character from being printed, thus creating a space.

F-V feature

The Fixed-Variable feature utilizes the ability of the printwheels to be offset with respect to each other. When this feature is installed and activated, the relative position of the printwheels is changed by an amount equal to the secondary print wheel’s displacement in each ciphering cycle.

It works by disconnecting the printwheels as soon as the clear text letter is printed. While the drum rotates and the secondary print wheel is displaced, the primary print wheels remains fixed. At the end of the cycle, the print wheels are connected again and the secondary letter is printed.

When installed, the control knob can either be visible and operable from outside or hidden behind the left cover, in which case it is completely invisible from the outside. In this case, the left cover has to be removed to activate or deactivate it.

No CX-52M has been identified with the F-V feature installed and it is not mentioned in the corresponding manual.

C-52 configuration options in detail

Mechanically, the C-52 is almost identical to the CX-52. The differences are in the keywheel advancement mechanism and the slightly altered drum, as explained below. In general, the version of the C-52 as delivered to non-NATO friendly customers has a regular keywheel advance pattern (either step-all-wheels-at-once or the M-209 compatible stepping) and few options to modify it.

It is assumed that the C-52's possibilities were toned down after the gentlemen's agreement between Hagelin and the NSA and that not all options were offered to all customers.

Configuration options

In general, most of the configuration options of the CX-52 were also available for the C-52 but additionally there seem to be different versions of the drum:

- Choice of slide bars.
- Drum.
- Choice of keywheels.
- Choice of indicating ring/typewheel unit.
- F-V feature.

Slide bars

CX-52 and C-52 slide bars are identical. However, the choice of advance bars is limited because the drum allows for only a few advance slide bars (see *Drum* below). The AFSA order [xx] does not define the slide bars for the C-52.

The inspected C-52's so far all contain five unluggable slide bars at positions 28-32, only one or two of which (per machine) are advance bars, and always with unconditional advance cams, i.e. 0 and C.

Standard C2 and D bars

The Crypto AG document *THE CRYPTOGRAPH TYPE C-52 Specifications* [xiii] mentions two options for the type of slide bars: '*Standard "D" for organizations using C-52 cipher machines, or Standard "C2" for correspondence between C-52 and C-4 or similar machines.*' As C2 is described to be functionally compatible to the M-209, it is assumed to refer to a set of Standard C bars which uses only two advance bars.

The Standard D set is not explained in detail. It is assumed to have just one advance bar that advances all keywheels one step. This should not be used with 6 identical keywheels.

Drum

Three C-52 different drums are identified for the C-52: with either 32, 5 or 2 positions available for advance bars. The 32-position version is implied in the AFSA order, but has not yet been seen. The 5-position version is mentioned in a manual, but has not yet been seen either. The 2-position version is the only one actually encountered so far. It is expected that most will be of the latter version, because the C-52 seems mostly to have been marketed as a dimmed down version of Crypto AG's C(X)-52 machines.

32 available positions for advance bars

The AFSA order of 1954 does not mention the drum when converting a C-52 to a CX-52, suggesting they are the identical. This in turn would suggest that there were 32 positions available in the drum for placement of advance bars. The Standard "A" drum bars mentioned are for the CX-52, this set contains 30 advance bars, making good use of the 32 available positions.

Also, the CRYPTO AG document *No. 3011-c, THE CRYPTOGRAPH TYPE C-52 Specifications* [xiii] explicitly states: '*all bars are easily interchangeable*, suggesting that there are no limitations to do so.

5 available positions for advance bars

The Crypto AG document *D-036 The <<Hagelin Cryptographer>>, Type C-52* [xix] states on page 1: '*There are 27 bars for the displacement of the typewheel and 5 bars for the stepping of the keywheels*'. This suggests a drum with only five positions available for advance bars.

2 available positions for advance bars

On inspection of several C-52's and referring to the spare parts catalog it was found that the supporting disks within the drum are shaped differently from the ones in the CX machines. By having a slightly larger diameter across most of their circumference, they block advancement of the keywheels during most of the cipher cycle. Only at two slide bar positions (31 and 32) the supporting disks have the same diameter as used in the CX-52 to allow for advancement of the keywheels. In all other positions the advance mechanisms of the keywheels are blocked and a displaced advance bar at such a position would lock the drum in mid-cycle.

In these machines, the advance bars in positions 31 and 32 cannot be lugged, meaning that their order is of no importance and that keywheel advancement is regular.

It is not unlikely that some early C-52's have drums which would allow for a different number of positions for advance bars, this is still an area of active research.

Keywheels

The keywheels of the C-52 differ from those in the CX-52 in the way their advance mechanism works and they are not exchangeable between the machines.

An indication of early differences between the two machines can be deducted from an order placed for C-52's by the Army Forces Security Agency (AFSA) in December 1954 [xx]. In 2014 the NSA released documents pertaining that order which reveal that a C-52 can be converted to a CX-52 by replacing:

1. The 'guide arms'; one on each keywheel.
2. The 'feed arm', one on each keywheel.
3. The 'Top commanding lever', one per machine.
4. The 'Button commanding cradle', one per machine.
5. Using the standard "A" drum bars, one set of 32 per machine.

From the above list, 1 and 2 refer to the difference in the way the keywheels are driven. Points 3 and 4 highlight the difference in function of the locking bar.

Choice of keywheels

A choice of six replaceable keywheels is used in the C-52. Common knowledge seems to suggest that the C-52 is typically equipped with six identical keywheels of 47 positions. Although such a machine is spotted, this choice of keywheels is not mandatory.

The AFSA order of 1954 [xx] mentions a choice of keywheels: it usually comes with one of two mixed sets, but all twelve available wheels with 25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46 & 47 pins can be used.

- The set 25, 26, 34, 38, 42, 46 is for backward compatibility with M-209-like devices. This demands the Standard C2 slide bars.
- The complimentary set 29, 31, 37, 41, 43, 47.

Both sets can also be used with the Standard D slide bars. Using six 47 pin keywheels should not be used together with the Standard D slide bars set.

Indicating ring and typewheel unit

According to the AFSA order of 1954 [xx] the indicating ring/typewheel unit is available with either fixed letters and typeface or with rearrangeable letters and typeface. All indicating rings and typewheels available for the CX-52 should work in the C-52 as well.

No C-52 has been identified with rearrangeable type wheels nor is it mentioned in the manual [xix]. Most likely it was not offered anymore to customers later in time.

One C-52 had a print wheel in which any one character can be chosen as 'space character'.

F-V feature

The F-V feature is mentioned in the AFSA order of 1954 [xx] as 'accessible without raising the lid', however it is not mentioned in the C-52 Spare parts catalogue [iii]. As the CX and C casings are identical, it would be mechanically feasible.

No C-52 has been identified with the F-V feature installed nor is it mentioned in the manual [xix]. Most likely it was not offered anymore to customers later in time.

Tidbits

Individuals

It is likely that apart from the standard models mentioned above special configurations may have been delivered with possibly increased cryptographic strength. Special configurations with limited cryptographic strength are a real possibility too.

But it is also good practice to provide customers with customized machines. In this case the goal is not to increase the cryptographic strength, but to provide minor variations to prevent direct compatibility between different customers or different departments of one customer.

To this end, some of the following methods can be used:

- Print wheels locked in different relative positions: A=A is common, but A=C was also spotted (seen in a C-52).
- Replacing a few slide bars with ones that advance the keywheels differently (see Irish CX-52).
- Using the inverted K cam (seen in an RT).

Rearrangeable letters

In 1951 the French demonstrated [xxi] to AFSA a patented modification of the M-209-B that corresponds to the C(X)-52's typewheel unit with rearrangeable letters. It is unclear whether Hagelin invented this separately.

CX-52H

A 1953 report from a subcommittee of the UK/US Communications conference [xxii] mentions the CX-52H:

> *CX-52 and CX-52H*
> *The U.K. and U.S. require further study as a matter of urgency but there seems little doubt that it will give a very high degree of security if properly used.*

It is unclear whether this refers to an as yet unidentified model or to the Hüttenhain feature as mentioned before. The released documents contains no further details on the machine, but lists many other contemporary crypto systems.

DDR

On the 16th of May 1978, a package was inspected sent from Krypto-AG in Switzerland to the Ethiopian embassy in the DDR. Apparently they ordered a "schreibende Chiffriermaschine", either a C-52 or CX-52 [xxiii].

C-52 with 30 characters

A C-52 for the Arabian market (30 characters) was found to contain only 27 bars able to displace the typewheel. Of the five remaining bars, only one was an advancing bar (advancing all keywheels a step) so two could easily have been used to make up for the missing two to displace the typewheel. It is yet unclear whether this was simply a default bar configuration for use with a 26 character typewheel, the default bar configuration for use with any typewheel or that the mismatch was deliberately undercutting the cryptographic optimum.

Mathematical conditions for key material

Hagelin himself originally wrote *Die Geschichte der HAGELIN*-CRYPTOS in German [xxiv]. On page 57 of the English translation he writes with respect to the CX machines:

> *The CX machine with irregular movement of the pinwheels brings the advantage that non-linear movement sequences can be obtained. If certain mathematical conditions are met in the compilation of the material for the keys, then the periods occurring will be sufficiently long.*

What these mathematical conditions exactly entail is probably published in a document we have not yet unearthed.

Long key periods or irregular keywheel movement

In *Der Geschichte der HAGELIN CRYPTOS*[xxiv], on page 32 Hagelin writes:

> *Before going into the details of the various improvements, it is important to emphasize that the requirements of our customers led in two opposite directions. One group required long key periods, while the other wanted a movement of the pin-wheels that was as irregular as possible. It required great mathematical competence to compile keys which would assure that sufficiently long periods were obtained. In order to satisfy our customer we also developed hybrid systems where usually one pin-wheel stepped regularly and the others irregularly.*

Long key periods are achieved for example with the C-52[d] with six wheels that are coprime and all advance once every cycle. A movement of pin wheels that are as irregular as possible could be the CX-52a or CX-52b: the CX-52a has irregular angular advancement of the keywheels, each wheel advancing 0, 1, 2, 3, 4 or 5 steps per cycle. The CX-52b has fixed angular advancement of the keywheels: all wheels advancing the same number of steps per cycle but the number varies between 1 and 32 per cycle. The CX-52M is an example of a 'hybrid system' where the first keywheel steps advances cycle and the other five keywheel advance irregularly.

Prices

The January 1955 pricelist [xxv] lists the standard model for US$ 590. Extra key-wheels are $ 29 each (twelve available), a single pin disk is $ 9.30. Normal, standard A or B drum bars are $ 1 each; specials costs $ 2.20 (each, for 20 pieces) but prices go down to $1 each when 500 identical bars are purchased.

An extra fixed indicating ring and typeface ring set cost $56 and $85 for a rearrangeable one. For an extra $29 the standard model comes with the rearrangeable indicating ring and typeface rings instead of the fixed version.

Acknowledgements

Paul Reuvers and Marc Simons Cryptomuseum.com for the suggestion to ‘once and for all explain this properly’, their never ending support, making machines available for close inspection and supplying both documentation and coffee in abundance. Extra kudos to Paul for supplying his exquisite drawings and proofreading.

Klaus Kopacz for exciting, stimulating and informative on- and offline chat sessions and for documentation. We cannot drink coffee together often enough.

Gerry Sulger-Buel for kindly allowing me access to a great deal of Hagelin brochures so they can be brought into the public domain.

Dirk Rijmenants and Jean-François Bouchaudy for their support and getting me going on this research.

Ralph Simpson, Niall McLaughlin, Bob Welsh, Jan Staller for the long distance inspection of their machines and lots and lots of photos.

Mark Blair for documenting the cleanup and repair of his CX-52 in his online TECH JOURNAL (I studied those pictures with a caliper in hand) and Marc Sachs for supplying a copy of the CX-52M manual to the community.

Historische Collectie Verbindingsdienst for making available another Hagelin brochure.

National Cryptologic Museum for taking the time to provide digital copies of Hagelin brochures.

Some collectors not mentioned here for various reasons: thank you so much for your help and the collective fun of researching.

About the author

Bart A. Wessel (1958) has an engineering degree in Technical Physics (1984). After relatively brief orientating stints in Electro-Optical Research, Software Engineering (UNIX, C, Modula II) and User Interface Design and Testing he spent most of his career designing and developing computer training courses for the Dutch, English, French and German market for SPC Training and its successors. Currently most of his time involves his family, studying Enigma, Nema, Fialka, & Hagelin machines and volunteering in WWII and Crypto museums.

Table of Contents

Endnotes

[i] REF ID:A72380, Extract from letter dated 24 Aug. 1950 from Hagelin, declassiefied 07-08-2015.
[ii] REF ID A56966, TOP SECRET FROTH, Report of Special Study Group on FARMER-NOMAD, 15 nov 1954, declassified 2014-06-16.
[iii] Spare parts catalogue C-52 (No 20 501 etc), No 063697, Crypto AG. Zug, L-063, courtesy of Gerhard Sulger-Buel.
[iv] SPARE PARTS CATALOGUE for Hagelin Ciphering Machine Type CX – 52, Crypto AG, Nr unknown, May 1956, MARID, courtesy of cryptomuseum.com .
[v] http://www.cryptomuseum.com/crypto/hagelin/cx52/files/cx52_manual.pdf , retrieved 2018-10-13.
[vi] http://www.cryptomuseum.com/crypto/hagelin/cx52/files/cx52_spares.pdf , L-061, retrieved 2018-10-13.
[vii] Boris C. W. Hagelin & David Kahn (1994) THE STORY OF THE HAGELIN CRYPTOS, Cryptologia, 18:3, 204-242, DOI: 10.1080/0161-119491882865
[viii] Description of CRYPTOGRAPHERS "HAGELIN" TYPE CX-52, Crypto AG. ZUG, August 1956, MARID, courtesy of cryptomuseum.com.
[ix] H. Paul Greenough (1999) CRYPTANALYSIS OF THE HAGELIN C-52 AND SIMILAR MACHINES A KNOWN PLAINTEXT ATTACK, Cryptologia, 23:2, 139-156.
[x] http://users.telenet.be/d.rijmenants/en/c52tech.htm, retrieved 2018-10-13.
[xi] Description of CRYPTOGRAPHERS "HAGELIN" TYPE CX-52, Crypto AG Zug, No 3027, page 26: '54 – Guide-arm assembly', courtesy of Historische collective verbindingsdienst, March 2019.
[xii] REF ID's A2436243, A60616 and A2436259
[xiii] THE CRYPTOGRAPH TYPE C-52 Specification, Crypto AG Zug, No. 3011-c, part of binder No. 3337, courtesy of the National Cryptologic Museum
[xiv] REF ID A60669, MEMORANDUM FOR THE RECORD, page 27, 10 January 1958
[xv] RT/CX One Time Tape Auxiliary device, No. 3093 A, Crypto AG. Zug, courtesy of cryptomuseum.com.
[xvi] SPARE PARTS CATALOGUE for Hagelin Ciphering Machine Type CX – 52, Crypto AG, Nr unknown, May 1956, MARID, courtesy of cryptomuseum.com.
[xvii] Usage of Hagelin cryptographer CX-52, Crypto AG. Zug, courtesy of cryptomuseum.com.
[xviii] Usage of the Hagelin cryptographer CX-52, Crypto AG Zug, No. 7001 e, courtesy of Gerhard Sulger-Buel.
[xix] The <<Hagelin Cryptographer>>, Type C-52, Crypto AG, D-036, courtesy of Gerhard Sulger-Buel.
[xx] REF ID A63909, A63700, A63867, A67370, A63645, A67364, A63351, A67363, and A72371 [xxv]: AFSA order for C-52 and CX-52 Cypher machines and a price list, early 1955, Approved for Release by NSA on 06-19-2014.
[xxi] REF ID:A58828, REPORT ON VISIT TO FRENCH "SECTION DU CHIFFRE", declassified.
[xxii] REF ID:A522923 (Final Draft and A522921 (Report (Final)), UK/US COMMUNICATIONS SECURITY CONFERENCE 1953, REPORT OF THE SECURITY SUB-COMMITTEE to the EXECUTIVE COMMITTEE, 6th November 1953, declassified by NSA 05-27-2014.
[xxiii] http://scz.bplaced.net/zco.html , "Chiffriergerät der Äthiopischen Botschaft, Belegjahr 1978", BStU, MfS, HA II Nr. 033174, retrieved 2019-01-19.
[xxiv] Die Geschichte der HAGELIN-CRYPTOS, B. Hagelin, CRYPTO AG, nr. 1E 720. An official English translation exists as *The Story of the HAGELIN-CRYPTOS*. Finally, there is an edited version available as an article in Cryptologia: *THE STORY OF THE HAGELIN CRYPTOS*, by David Kahn.
[xxv] PRICELIST for Cryptographers Type CX-52, Crypto AG, No. 3803, https://ftp.nohats.ca/nsa-friedman/41782999082206.pdf page 32, retrieved 2019-04-10.

Model sheets shows the configuration of the identified models by means of two tables:

- A colored table of configurable options. Its format is designed to illustrate the configuration at a glance.
- A black and white table detailing the cams on the slide bars and their positions in the drum. This table is similar to what is explained in detail in the chapter on *Slide Bars*. If different slide bar configurations were identified, these are listed separately.
  Apart from the M model, lugging is not prescribed and thus not mentioned.

This is an example model sheet for the CX-52c:

CX-52c

<table>
<tr><th>Bars</th><th>Drum</th><th>Keywheel</th><th colspan="2">FV</th><th>Typewheel</th><th>Indicator</th><th>Space</th></tr>
<tr><td>Standard A</td><td rowspan="2">2</td><td>25</td><td rowspan="3">Yes</td><td rowspan="2">Internal</td><td rowspan="2">Fixed</td><td rowspan="2">Fixed</td><td>A</td></tr>
<tr><td>Standard B</td><td>26</td><td>J</td></tr>
<tr><td>Standard C</td><td rowspan="2">5</td><td>29</td><td rowspan="2">External</td><td rowspan="2">Rearrangeable Invers</td><td rowspan="2">Variable</td><td>K</td></tr>
<tr><td>Special</td><td>31</td><td>W</td></tr>
<tr><td>CXM</td><td rowspan="2">32</td><td>34</td><td rowspan="3">No</td><td rowspan="3">2X Rearrangeable Arbitrary</td><td rowspan="3">2 x Variable</td><td>X</td></tr>
<tr><td>Step all once</td><td>37</td><td>Z</td></tr>
<tr><td></td><td></td><td>38</td><td></td></tr>
<tr><td></td><td></td><td>41</td><td></td></tr>
<tr><td></td><td></td><td>42</td><td></td></tr>
<tr><td></td><td></td><td>43</td><td></td></tr>
<tr><td></td><td></td><td>46</td><td></td></tr>
<tr><td></td><td></td><td>47</td><td></td></tr>
</table>

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
30-32	K	0	0	0	0	0	0	13	
29	K	0	0	C	C	C	C	68	
28	K	C	C	C	C	C	C	15	
1-27	K	0	0	0	0	0	0	13	

Or:

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
32	K	C	C	C	C	C	C		
31	K	0	0	C	C	C	C		
1-30	K	0	0	0	0	0	0		

The colored table shows which set of slide bars is used, the number of advance bars that the drum allows for (always 32 for CX models), the key wheels used, the availability of the FV feature, the typewheel/indicator configuration and which character is the designated ‘space’ character. All models have a unique color. Dark colored fields are deemed essential for a specific model, while lighter shades are used to signify variations that have been encountered. One could argue that these could identify as sub models, but that distinction is not made in this report.

Multiple black and white tables show when the same keywheel advancement is achieved by different advance slide bars, or by a different position of identical advance bars in the drum.

No CX-52b was spotted in the field, so only the characterizing configuration options deduced from literature are colored.

The CX-52Eire is included as an illustration of a custom machine, even though it is not technically a model.

Bart Wessel

CX-52a

Bars	Drum	Keywheel	FV		Typewheel	Indicator	Space
Standard A	2	25	Yes	Internal	Fixed	Fixed	A
		26					
Standard B		29					J
		31		External			
Standard C	5	34			Rearrangeable Invers	Variable	K
		37					
Special		38	No				W
		41					
CXM	32	42			2X Rearrangeable Arbitrary	2 x Variable	X
		43					
Step all once		46					Z
		47					

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID
31-32	K	0	0	0	0	0	0	13
30	K	0	0	0	0	0	B	12
26-29	K	0	0	0	0	0	A	11
25	K	0	0	0	0	B	0	10
21-24	K	0	0	0	0	A	0	9
20	K	0	0	0	B	0	0	8
16-19	K	0	0	0	A	0	0	7
15	K	0	0	B	0	0	0	6
11-14	K	0	0	A	0	0	0	5
10	K	0	B	0	0	0	0	4
6-9	K	0	A	0	0	0	0	3
5	K	B	0	0	0	0	0	2
1-4	K	A	0	0	0	0	0	1

CX-52b

Bars	Drum	Keywheel	FV		Typewheel	Indicator	Space
Standard A	2	25	Yes	Internal	Fixed	Fixed	A
		26					
Standard B		29					J
		31		External			
Standard C	5	34			Rearrangeable Invers	Variable	K
		37					
Special		38	No				W
		41					
CXM	32	42			2X Rearrangeable Arbitrary	2 x Variable	X
		43					
Step all once		46					Z
		47					

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID
32	K	C	C	C	C	C	C	{15}
1-31	K	B	B	B	B	B	B	{14}

{..} educated guess

CX-52c

Bars	Drum	Keywheel	FV		Typewheel	Indicator	Space
Standard A	2	25	Yes	Internal	Fixed	Fixed	A
		26					
Standard B		29					J
		31		External			
Standard C	5	34			Rearrangeable Invers	Variable	K
		37					
Special		38	No				W
		41					
CXM	32	42			2X Rearrangeable Arbitrary	2 x Variable	X
		43					
Step all once		46					Z
		47					

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
30-32	K	0	0	0	0	0	0	13	
29	K	0	0	C	C	C	C	68	
28	K	C	C	C	C	C	C	15	
1-27	K	0	0	0	0	0	0	13	

Or:

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
32	K	C	C	C	C	C	C		
31	K	0	0	C	C	C	C		
1-30	K	0	0	0	0	0	0		

A handwritten note defines Standard C set as:

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
32	K	0	0	C	C	C	C		
31	K	C	C	C	C	C	C		
28-30	K	0	0	0	0	0	0		no
1-27	K	0	0	0	0	0	0		

Other slide bar variations also exist:

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
32	K	C	0	0	0	0	C		
31	K	0	0	0	0	C	C		
30	K	0	0	0	C	C	0		
29	K	0	0	C	C	0	0		
28	K	0	C	C	0	0	0		
1-27	K	0	0	0	0	0	0		

CX-52Eire

Bars	Drum	Keywheel	FV		Typewheel	Indicator	Space
Standard A	2	25	Yes	Internal	Fixed *)	Fixed	A
		26					
Standard B		29					J
		31		External			
Standard C	5	34			Rearrangeable Invers	Variable	K
		37					
Special		38	No				W
		41					
CXM	32	42			2X Rearrangeable Arbitrary	2 x Variable	X
		43					
Step all once		46					Z
		47					

*) locked in A=A position

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
30-32	K	0	0	0	0	0	0	13	
29	K	0	0	0	0	A	A	64	
28	K	0	0	C	C	C	C	16	no
21-27	K	0	0	0	0	0	0	13	
20	K	0	0	A	A	0	0	60	
12-19	K	0	0	0	0	0	0	13	
11	K	A	A	0	0	0	0	56	
10	K	0	B	0	0	0	0	4	
7-9	K	0	0	0	0	0	0	13	
6	K	B	0	0	0	0	0	2	
4-5	K	0	0	0	0	0	0	13	
3	K	0	0	B	B	B	B	35	
1-2	K	0	0	0	0	0	0	13	

Bart Wessel

CX-52French

Bars	Drum	Keywheel	FV		Typewheel	Indicator	Space
Standard A	2	25	Yes	Internal	Fixed	Fixed	A
		26					
Standard B		29					J
		31		External			
Standard C	5	34			Rearrangeable Invers	Variable	K
		37					
Special		38	No				W
		41					
CXM	32	42			2X Rearrangeable Arbitrary	2 x Variable	X
		43					
Step all once		46					Z
		47					

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
28-32	K	0	0	0	0	0	0	13	
27	K	B	B	B	B	B	B	14	
25-26	K	0	0	0	0	0	0	13	
24	K	B	B	B	B	B	B	14	
22-23	K	0	0	0	0	0	0	13	
21	K	A	A	A	A	A	A	54	
19-20	K	0	0	0	0	0	0	13	
18	K	A	A	A	A	A	A	54	
16-17	K	0	0	0	0	0	0	13	
15	K	C	C	C	C	C	C	15	
1-14	K	0	0	0	0	0	0	13	

CX-52-M

Bars	Drum	Keywheel	FV		Typewheel	Indicator	Space
Standard A	2	25	Yes	Internal	Fixed	Fixed	A
		26					
Standard B		29					J
		31		External			
Standard C	5	34			Rearrangeable Invers	Variable	K
		37					
Special		38	No				W
		41					
CXM	32	42			2X Rearrangeable Arbitrary	2 x Variable	X
		43					
Step all once		46					Z
		47 (6)					

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
32	K	0	0	0	0	0	A		
31	K	0	0	0	0	A	0		
30	K	0	0	0	A	0	0		
29	K	0	0	A	0	0	0		
28	K	C	A	0	0	0	0	57	
1-27	K	0	0	0	0	0	0		

Late version:

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
32	-	0	0	0	0	0	A	111	
31	-	0	0	0	0	A	0	109	
30	-	0	0	0	A	0	0	107	
29	-	0	0	A	0	0	0	105	
28	-	C	A	0	0	0	0	157	
1-27	K	0	0	0	0	0	0	13	

Nonprinting slide bars 157, 105, 107, 109 & 111 cannot be removed

The prescribed lugging pattern for the advance bars is:

position		1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel
32		X	X	X	X	X	-
31		X	X	X	X	-	-
30		X	X	X	-	-	-
29		X	X	-	-	-	-
28		X	-	-	-	-	-

C-52[c2]

Bars	Drum	Keywheel	FV		Typewheel	Indicator	Space
Standard A	2	25	Yes	Internal	Fixed	Fixed	A
		26					
Standard B		29					J
		31		External			
Standard C2?	5	34			Rearrangeable Invers	Variable	K
		37					
Special		38	No				W
		41					
CXM	32	42			2X Rearrangeable Arbitrary	2 x Variable	X
		43					
Step all once		46					Z
		47					

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
32	K	C	C	C	C	C	C		no
31	K	0	0	C	C	C	C		no
28-30	K	0	0	0	0	0	0		no
1-27	K	0	0	0	0	0	0		

Or:

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
32	K	0	0	C	C	C	C	16	no
31	K	C	C	C	C	C	C	17	no
1-30	K	0	0	0	0	0	0	13	

C-52[d]

Bars	Drum	Keywheel	FV		Typewheel	Indicator	Space
Standard A	2	25	Yes	Internal	Fixed	Fixed	A
		26					
Standard B		29					J
		31		External			
Standard C	5	34			Rearrangeable Invers	Variable	K
		37					
Special		38	No				W
		41					
CXM	32	42			2X Rearrangeable Arbitrary	2 x Variable	X
		43					
Step all once		46					Z
		47					

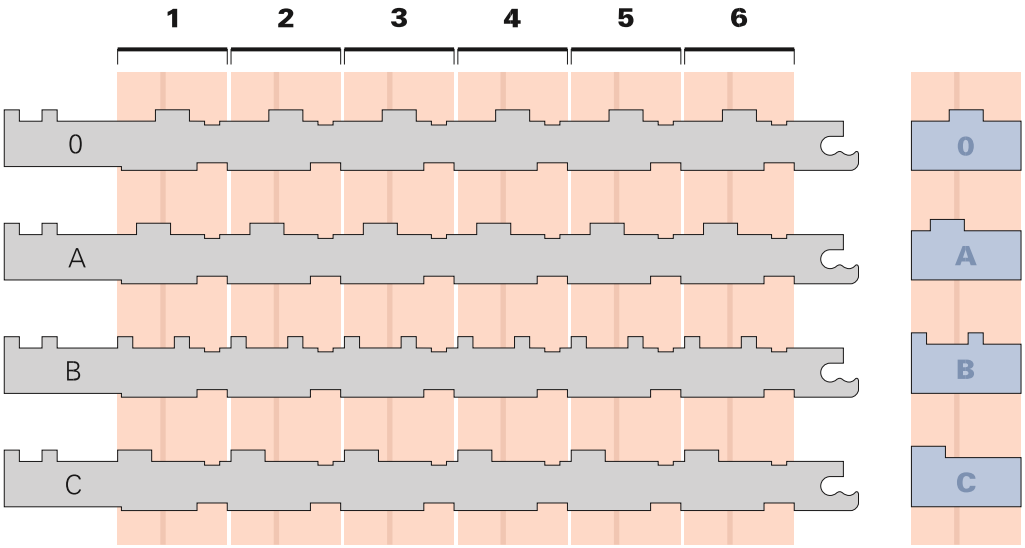
position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
32	K	0	0	0	0	0	0	18	no
31	K	C	C	C	C	C	C	17	no
28-30	K	0	0	0	0	0	0	18	no
1-27	K	0	0	0	0	0	0	13	

List of identified C(X)-52 slide bars

print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs	Model
K	A	0	0	0	0	0	1		CX-52a
K	B	0	0	0	0	0	2		CX-52a,Eire
K	0	A	0	0	0	0	3		CX-52a
K	0	B	0	0	0	0	4		CX-52a,Eire
K	0	0	A	0	0	0	5		CX-52a
K	0	0	B	0	0	0	6		CX-52a
K	0	0	0	A	0	0	7		CX-52a
K	0	0	0	B	0	0	8		CX-52a
K	0	0	0	0	A	0	9		CX-52a
K	0	0	0	0	B	0	10		CX-52a
K	0	0	0	0	0	A	11		CX-52a
K	0	0	0	0	0	B	12		CX-52a
K	0	0	0	0	0	0	13		CX-52a,c,M,Eire, French CX-RT C-52
K	B	B	B	B	B	B	14		CX-52{b},French
K	C	C	C	C	C	C	15		CX-52b,c, French
K	0	0	C	C	C	C	16	no	CX-52Eire C-52[c2]
K	C	C	C	C	C	C	17	no	C-52[c2]
K	0	0	0	0	0	0	18	no	C-52 CX-RT
K	0	0	0	0	0	C	33		CX-RT
K	0	0	B	B	B	B	35		CX-52Eire
K	A	A	À	A	A	A	54		CX-52French
K	A	A	0	0	0	0	56		CX-52Eire
K	C	A	0	0	0	0	57		KK collection
K	0	0	A	A	0	0	60		CX-52Eire
K	0	0	0	0	A	A	64		CX-52Eire
K	0	0	C	C	C	C	68		CX-52c
K	0	0	0	0	0	0	[A]	no	C-52
K	0	0	0	0	0	0	[B]		C-52
–	0	0	0	0	0	A	[C]		CX-RT
*)	0	0	0	0	0	C	[D]	no	CX-RT
K	0	0	0	0	0	A	[E]		CX-RT
K	B	B	B	B	B	B	(F)		CX-52b
K	C	0	0	0	0	C	[G1]		CX-52
K	0	0	0	0	C	C	[G2]		CX-52
K	0	0	0	C	C	0	[G3]		CX-52
K	0	0	C	C	0	0	[G4]		CX-52
K	0	C	C	0	0	0	[G5]		CX-52
K	0	0	0	0	0	0	[G6]		CX-52
$\overline{K}$	0	0	0	0	0	0	[H]		CX-RT
K	A	0	0	0	0	0	72	no	CX-RT
-	0	0	A	0	0	0	105	no	CX-52M
-	0	0	0	A	0	0	107	no	CX-52M
-	0	0	0	0	A	0	109	no	CX-52M
-	0	0	0	0	0	A	111	no	CX-52M
-	C	A	0	0	0	0	157	no	CX-52M

*) Overlaps [C]&[C]neighbors
K: displace typewheel when bar displaced, $\overline{K}$ when bar not displaced
0: never advance this keywheel
A: advance this keywheel when bar displaced
B: advance this keywheel when bar not displaced
C: always advance this keywheel
[A…] brackets indicate this bar carries no ID, mentioned here for reference purposes
(F)is part of Standard B slide bars set
{b} educated guess

For easy reference, the following image provides four real sized slide bars with six identical cams each. Simply put your bar on the image to see which of the 0, A, B or C cams it has:



You may want to laminate this page as the bars usually leave some smudges on the paper.

C(X)-52 spec sheet for fill-in purposes

type	seris	serial No	make	owner	used in	secret type
C-52 CX-52 CX-RT	- A B C D		Cryptoteknik CRYPTO AG			CX-52a CX-52b CX-52c CX-RT C-52[c2] C-52[d]

Bars	Drum	Keywheel	FV		Typewheel	Indicator	Space
Standard A	2	25	Yes	Internal	Fixed	Fixed	A
		26					
Standard B		29					J
		31		External			
Standard C	5	34			Rearrangeable Invers	Variable	K
		37					
Special		38	No				W
		41					
	32	42			2X Rearrangeable Arbitrary	2 x Variable	X
		43					
CXM		46					Z
		47					

position	print	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel	Bar ID	lugs
example	K-$\overline{\text{K}}$	A	B	C	0	0	0	22	no
32									
31									
30									
29									
28									
27									
26									
25									
24									
23									
22									
21									
20									
19									
18									
17									
16									
15									
14									
13									
12									
11									
10									
9									
8									
7									
6									
5									
4									
3									
2									
1									

Bart Wessel

Keying when found (might not be official)

lug position	1st wheel	2nd wheel	3rd wheel	4th wheel	5th wheel	6th wheel
32						
31						
30						
29						
28						
27						
26						
25						
24						
23						
22						
21						
20						
19						
18						
17						
16						
15						
14						
13						
12						
11						
10						
9						
8						
7						
6						
5						
4						
3						
2						
1						

pin	1	2	3	4	5	6
01						
02						
03						
04						
05						
06						
07						
08						
09						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						