HAGELIN-CRYPTOS
CRYPTO AG

No. 3542 B

C R M - 0 0 8

SHORT FORM DESCRIPTION

P.O. Box: 474 · CH-6301 Zug/Switzerland · Phone: 042-38 15 44 · Telex: 868 702 · Domicile: CH-6312 Steinhausen/Zug

CRM-008 CRYPTOCOM

SHORT FORM DESCRIPTION

1. GENERAL INFORMATION

The high security ciphering of speech transmitted over ordinary voice grade channels has been for a long time a serious problem because such channels (Telephone Lines and SSB-RF links) do not permit the transmission of digitalized voice information. Therefore, in the past, the only (unsatisfactory) alternative was the use of simple frequency Inverters or Rolling-Code Scrambler which however due to the nature of their information processing cannot give the required degree of security.

This important gap has now been closed by CRYPTO AG with the successful development of the CRYPTOCOM ® CRM-008 Voice Cipher Unit which uses completely new frequency- and time mixing techniques.

2. OUTLINE

The CRYPTOCOM CRM-008 is suitable for connection to any Voice Transmission Channel, in particular Telephone Lines according to CCITT recommendations and RF SSB Radio Channels provided these are in accordance with CCIR recommendations, for good voice quality.

The CRM-008 is a High Security Voice Cipher Equipment and not comparable to any type of Scrambler.

The CRM-008 is intended for voice communication systems, where, due to technical reasons, the fully digitally operating CRYPTOVOX ® CV-096 (CV-196) cannot be used. Long distance telephone channels, straight RF Radio Links on short-waves and other similar communication installations have a limited bandwidth and varying group time-delays, which exclude the transmission of high-speed digital information streams. Only information, which has similar characteristics as plain voice, can be transmitted.

As the CRM-008 produces a cipher information which exactly fits these requirements, its application lies in the field of large networks as:

- Telephone communication in world-wide diplomatic organization.
- Telephone communication in nation-wide government networks of all services, civil or defence.
- Radiotelephone communication in world-wide diplomatic organization.
- Fixed or mobile radiotelephone communication on nation-wide government networks of all services, civil or defence.
- All kind of world-wide telephone or radiotelephone communications for commercial or defence organizations.

3. PRINCIPLE

The CRM-008 is a highly-sophisticated voice ciphering equipment, built with the most modern microelectronic components. The plain text information is handled in seven distinctive steps. (See Fig. 1).

- In step one the voice frequency information flow is split into two frequency bands, A and B.
- In step two the information of these bands is digitized in highly adaptive analog-to-digital converters, similar to those used in the CRYPTOVOX ® CV-096 equipment.
- In step three the digital information stream is stored in buffer memories in digital form.
- In step four the stored information is subdivided in a number of equidistant time elements. (8 per channel)(Fig.2)
- In step five all the time elements of the two frequency bands are permutated by means of the information, supplied from the Key Generator. (See Fig. 3).
- In step six the multiplexed time elements are arranged into a continuous information stream in other buffer memories.

- In step seven the stored information is formed back into an acoustical signal in special digital-to-analog converters and routed to the output, via filters C and D.

At the receiving end the whole process is reversed and at the earphone the recovered, plain text is available, naturally with a certain delay due to the different intermediate store operations.

In semi-duplex operation however, this delay is not disturbing. The operator has only to keep in mind that, when he has said "over" and released the push-to-talk switch, he has to wait a short moment, until the answer from the other side is received.

4. CIPHER PROCEDURE

The CRM-008 is equipped with a 10 digit watertight push-button keyboard (Fig. 4). 32 digits, subdivided in 8 groups of four can be entered at any moment. Any group can be altered independently of the 7 other ones. The entered group number and its four figures are shown on an electronic display for verification. Whenever a group is entered by means of the push-button # into the memory, the display will be cleared. The Key memory is kept alive by means of an internal sealed Ni-Cad battery, such ensuring the storage of a once entered Key information for long shelf time (more than 1 month) independently of external power supply.

This Key information is stored in the Key Generator circuitry where no readout possibility exists.

By means of the "Emergency Clear" button this information can however be erased.

The Key Generator produces, based on the 32 Key digits and by means of reinjected shift registers, quasi-random Key sequences which are used to control the permutation process.

Each time the push-to-talk switch is operated, a new Key sequence is selected. This sequence is controlling the time varying permutation blocks and selects every 320 ms one of 416'179'814'400 ~ 4.10^{11} possibilities. The receiving unit is automatically and continuously synchronized by means of a pilot-tone signal.

5. TRANSMISSION

In the center of the audio band (1600 Hz) a pilot tone is transmitted. This has three functions:

- Function one is to serve as center-frequency reference at the receiving end, where an AFC-system can compensate for frequency deviations as will mostly occur in RF-SSB systems up to ± 100 Hz. (A switch allows in addition to off-set the reference center frequency in five steps to - 300, -150, 0, + 150, + 300 Hz).

- Function two is to work as sync signal for the Key Generator at the receiving end. For this purpose the pilot-tone signal is frequency-modulated.

- Function three is to work as a reference level for the automatic AGC Circuit at the Receiver side.

In "Plain"-operation a "beep"-tone is automatically injected every 4 seconds into the system to warn both operators that they are operating in "Plain".

A receiving station will permanently monitor the pilot tone frequency of incoming Crypto messages, independently of the position of its Plain/Crypto switch. If the Basic Key setting is correct, always the deciphered plain text will be rendered at the output. If plain text is coming in, this also will be put straight-through. A LED indicator will show CRYPTO message reception.

Only the sending station decides whether Plain or Crypto mode is used. (In reality, however, both stations will immediately switch to Crypto, once the link is established, to ensure protection in both directions).

6. LAYOUT

Two models of the CRM-008 are available:

- CRM-008-001 is a field-type version for DC power input (10...30V) and 4 wire interface (Fig. 4a).

- CRM-008-007 is an office-type model with integral AC power supply unit and telephone adapter circuitry meeting international interface standards for 2 wire connections (Fig. 4b).

The basic construction of the processor as well as the front panel is identical at both models.

All functional groups are assembled on individual modules or printed circuit boards which are interlinked by plug-in connectors. This modular design gives a maximum of flexibility in view of servicing such equipment.

7. TECHNICAL SPECIFICATIONS

(OFFICE TYPE MODEL)		(FIELD TYPE MODEL)
	Power requirement	
220 (110) V 50...60 Hz 9 VA		10...30 V DC 7 W
	Local side (audio)	
2 wire, Z ≈ 600 Ω floating - 10 dBm...0 dBm level adjustable (AGC circuit covering 10 dB)		Input Mike: 2 wire Z ≧ 240 Ω - 50 dBm...-40 dBm adjustable ± 6 dBm Input Audio: Z ≧ 10 k Ω - 10 dBm...0 dBm adjustable Output Earphone: Z≈200 Ω adjustable -2,5 dBm
Output Level - mean value: -10 dBm (max. 0 dBm)		Output Audio: Z ≈ 600 Ω max 0 dBm (mean value -10 dBm) (all circuits with common ground)
	Line side (data)	
Input/Output 2 wire, Z ≈ 600 Ω floating Output: 0dBm level adjustable (pilot tone -10 dBm) Input: max 0 dBm level adjustable (AGC -10...-38 dBm)		DX out: Z ≈ 600 Ω (pilot tone -10 dBm) 0 dBm level adjustable DX in: Z ≧ 12 k Ω (AGC: max 0 dBm (pilot tone -10...-38 dBm) level adjustable

Synchronization:	Continuously by means of pilot tone 1600 ± 33 Hz
Startsync delay:	mean value : 2 sec max. 5.5 sec
Direction-change-over delay:	0,8 sec. (mean value)
Automatic Frequency Control:	± 100 Hz
Manually adjustable reference:	± 75 Hz ± 150 Hz
Key Setting:	Hermetically sealed push-button display with 8 digits + 2 functions 8 groups with 4 digits each: 10^{32} different settings. Each group can be changed individually.
Key Memory:	Non volatile RAM sustained by internal back-up Ni-Cad accumulator ensuring Key storage of more than 1 month. (20 hours operation will completely recharge battery).
Mode Switch:	Pos. 1 Static Frequency inversion Pos. 2 Frequency inversion in 40/80 ms intervals Pos. 3 Frequency inversion in n x 80 ms (n ≧ 1)

OFFICE TYPE MODEL		FIELD TYPE MODEL
	Dimensions	
255 mm (10")		W: 240 mm (9 1/2")
340 mm (13 1/2")		D: 375 mm (14 5/8")
140 mm (5 1/2")		H: 80 mm (3 1/8")
	Weight	
7,1 kg (14 1/2 lbs)		5,7 kg (11 lbs)
	MIL Tests:	
	Storage temp.	810.501.I/502.I (-30° C...+71° C)
	Temp. shock	810.503.I (-30° C...+71° C)
	Humidity	810.507.I/II
	Service-shock	810.516 1 V
	Modules-shock	810.516 1 I
	Operational Limits	
	Storage	-40°C...+80°C
	Operation	-25°C...+55°C
	Performance of specs	0°C...+55°C

HAGELIN-CRYPTOS
CRYPTO AG

8. AUXILIARIES

To match the CRM-008-007 (office-type model) two specially adapted table telephone sets are available. Both are equipped with a push-to-talk switch at the handset and a push-button at the main unit enabling the selection of Plain or Crypto mode operation.

- ATF-110 (without dial) is used in addition to the already existing telephone set of the station (either with manually operated or automatic exchange office). Operation of the set via CRM-008 is shown by turn-flag indicator. Recommended in all cases where the "official" set is supplied by the telephone company.

- ATF-114 with incorporated dialing disc. will be used as normal as well as "special" telephone set. It is recommended at places where the telephone company does not supply the set i.e. where it is to be acquired by the subscriber. The station has a handset with push-to talk switch, a turn-flag indicator showing CRM-008 operation, a Plain/Crypto push button with LED indicator and the usual button for PABX-internal back calls.

According to requirements, the field type model (CRM-008-001) can be completed with the following auxiliary devices to simplify its connection:

- ATF-109 Telephone adapter for Field-or Civil Telephone Systems, still making use of the field type handset.

- ATF-108 Telephone adapter for Civil (or other central-battery) telephone systems using specially adapted table telephone sets

- ATF-110 or ATF-114 (see above)

- ARA-100 Radio adapter (Normally wired in the factory according to interface conditions of the customers radio set).

9. CONCLUSIONS

The CRM-008 is actually the only commercially available voice cipher equipment which gives real cipher protection for use over telephone channels as well as RF SBB wireless links.

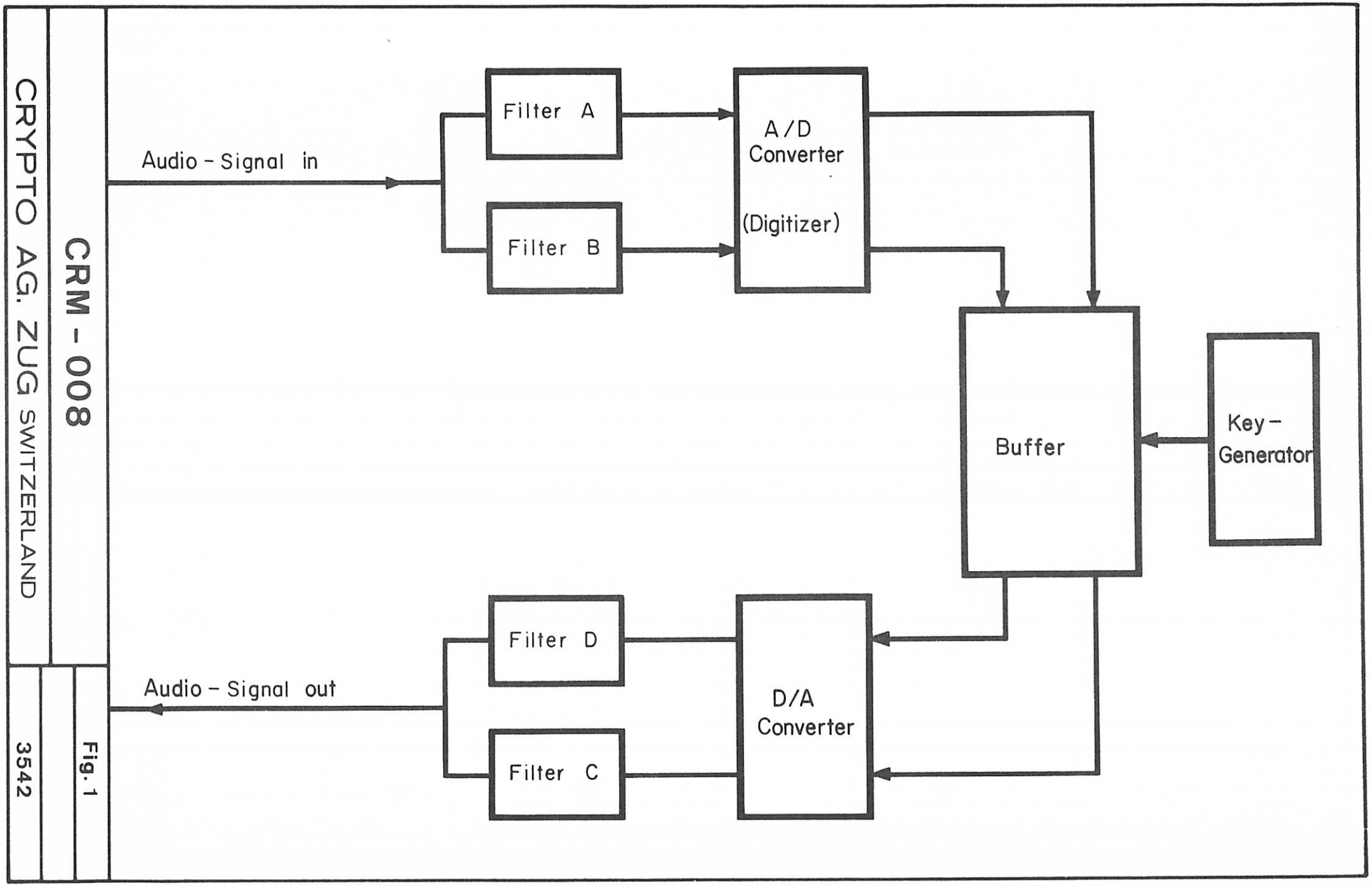
The CRYPTOCOM equipment is the result of research made during about 8 years by CRYPTO AG, based on experiences obtained with the fully digitally operating CRYPTOVOX ® (CV-096) unit.

As explained above, the CRM-008 can by no means be compared to actually available cheap voice scramblers, which are just good enough to avoid eavesdropping from an avid newspaper-man, but give by no way the high security needed in top-level communications.

In all cases, where, due to limited band-width or other technical reasons the CV-096 cannot be used, the CRM-008 is the only alternate solution to solve the problem.

The CRYPTOCOM ® processes the information in a way not realized up-to-date on a commercial basis. The information-package which are permutated internally are neutral regarding frequency and time as they are represented by a given pattern of Bits. It is therefore not possible, as this can be done with time-splitting or frequency-splitting scramblers, to attempt a decryption by correlation processes. The interfaces between two packages have no relation to each other because, what is sent to the line, are completely synthetically produced sound pieces. Here lays the main advantage of the CRM-008. The totally $8! \cdot 8! \cdot 2^8 \sim 4 \cdot 10^{11}$ permutations are controlled hereby by the quasi-random Key-Generator which at the receiver station is automatically synchronized to ensure correct deciphering.

Encl. Fig. 1-4
GGF
OSt/ma

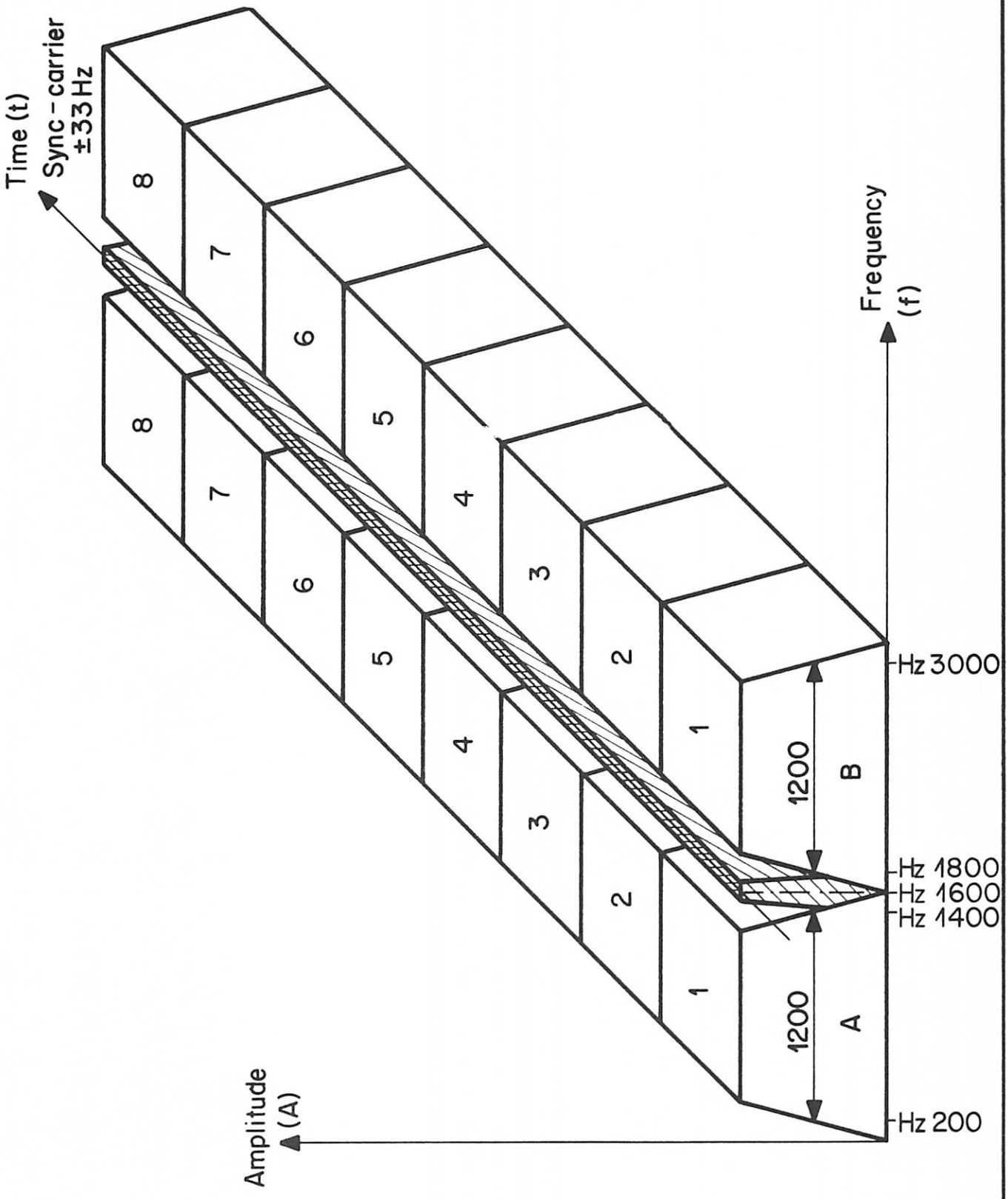


CRYPTO AG. ZUG SWITZERLAND

CRM - 008

3542

Fig. 1



CRM - 008	Fig. 2
CRYPTO AG. ZUG SWITZERLAND	3542

CRM - 008	Fig. 3
CRYPTO AG. ZUG SWITZERLAND	3542

a

b

CRM - 008	Fig. 4
CRYPTO AG. ZUG SWITZERLAND	3542