Philips Usfa N.V. 3/5 – TH 11 – . . . / 3

CRYPTO

ONTWERP TECHNISCHE HANDLEIDING BREEDBAND CRYPTOFONIE APPARAAT UA 8301/00 (beproevingsmodel)

CRYPTOGRAFISCHE BESCHRIJVING

Inhoudsopgave van deel 3 van Ontwerp Technische Handleiding

Breedband Cryptofonie-apparaat UA 8301/00

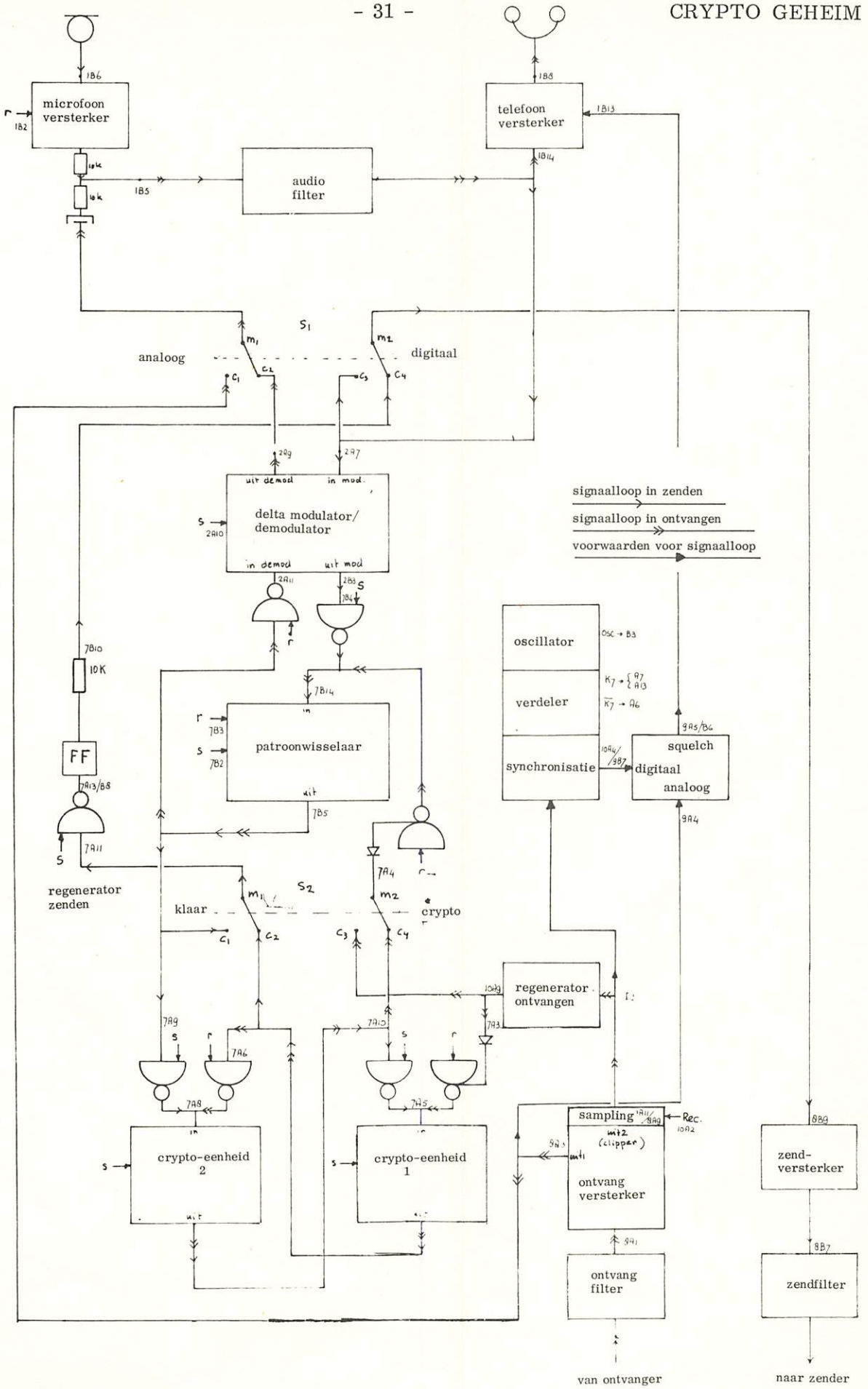
Cryptografische Beschrijving

Lijst van figuren

Gezien de inhoud van dit voorschrift rechtstreeks de vitale belangen van het Koninkrijk der Nederlanden raakt, is het verboden dit voorschrift over te dragen of van zijn inhoud kennis te geven aan onbevoegden.
Voorts moet ten aanzien van dit voorschrift de uiterste zorgvuldigheid in acht worden genomen, opdat noch het voorschrift zelf noch enig gegeven daaruit ter beschikking van onbevoegden komt. Het niet nakomen van de voren bedoelde verplichtingen levert een misdrijf op.

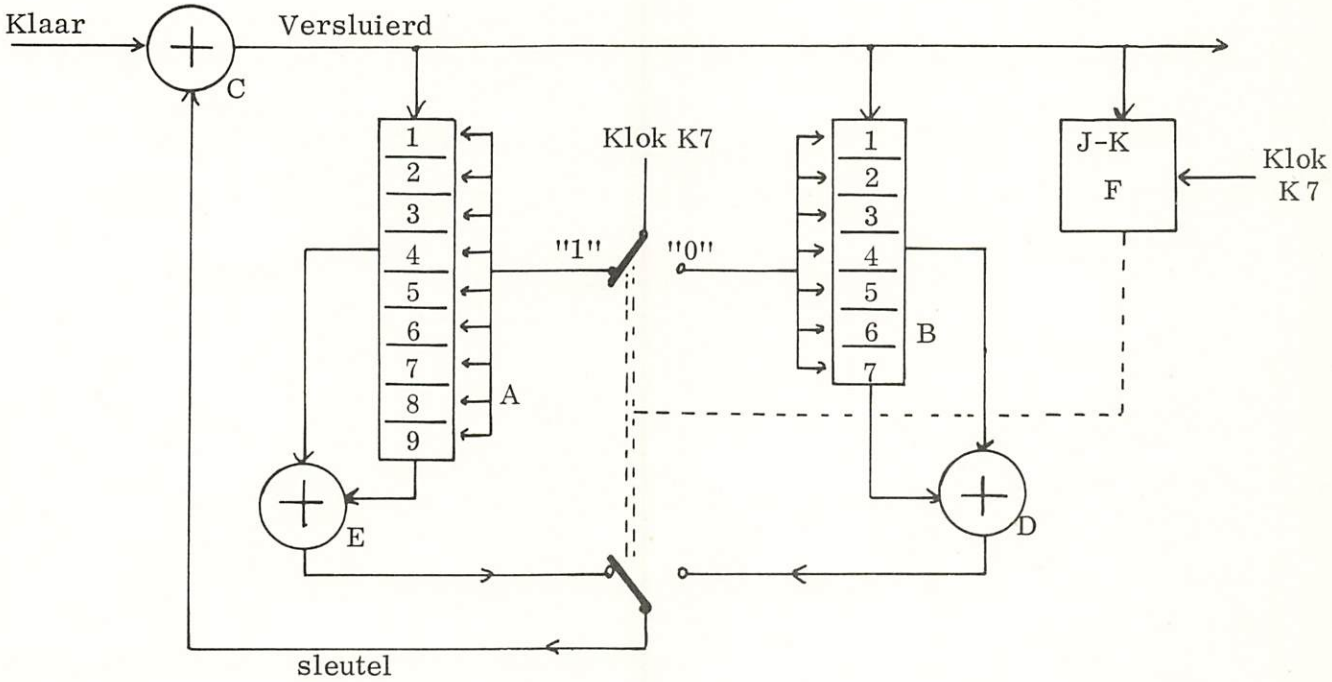
19. Overzicht Crypto gedeelte (zie figuur 29)

Het patroon van de digitale signalen uit de deltamodulator vertoont een zekere regelmaat, die versluierd wordt voordat de eigenlijke vercijfering begint. Het versluieren vindt plaats in de patroonwisselaar (eenheid 7) die volgens een vast ingestelde niet-lineaire terugkoppeling werkt. Hierdoor wordt het patroon ingrijpend gewijzigd, zodat bijvoorbeeld een lange serie "1" signalen niet als zodanig aan de volgende crypto-eenheden aangeboden wordt.
Bij zenden wordt het uitgangssignaal van de patroonwisselaar vervolgens door de crypto-eenheden 2 en 1 (in die volgorde) gevoerd, waarna het tenslotte door de zend-regenerator (via contact S2 - m1) aan de zendversterker wordt aangeboden. Bij ontvangen wordt het geregenereerde signaal door de crypto-eenheden 1 en 2 (in die volgorde) gevoerd, via schakelaar-contact S2 - m4 aan de patroonwisselaar aangeboden en tenslotte naar de ontvangstcircuits van de deltamodulator geleid.
De signaalloop voor zenden resp. ontvangen wordt geregeld door de voorwaarden "zenden" en "ontvangen", die al of niet de verschillende poorten open zetten.
De crypto-eenheden hebben ieder 10 duimwielen, waarop de dagsleutel wordt ingesteld. Ieder duimwiel bedient een groepje van 3 contacten, zodat er dus in totaal 2 (eenheden) x10 (duimwielen) x3 (contacten) = 60 contacten werkzaam kunnen zijn op de niet-lineaire terugkoppeling van de crypto-eenheden.
Het aantal mogelijke dagsleutels bedraagt dus 2^{60}.
In paragraaf 19 wordt de patroonwisselaar behandeld, paragraaf 20 is gewijd aan de crypto-eenheden en paragraaf 21 behandelt de uitlezing van de duimwielcontacten.
De crypto-eenheden zijn vanaf de voorkant van het cryptofonie-apparaat bereikbaar; de patroonwisselaar is een normale eenheid die verwijderd kan worden als de deksel van het apparaat verwijderd is.



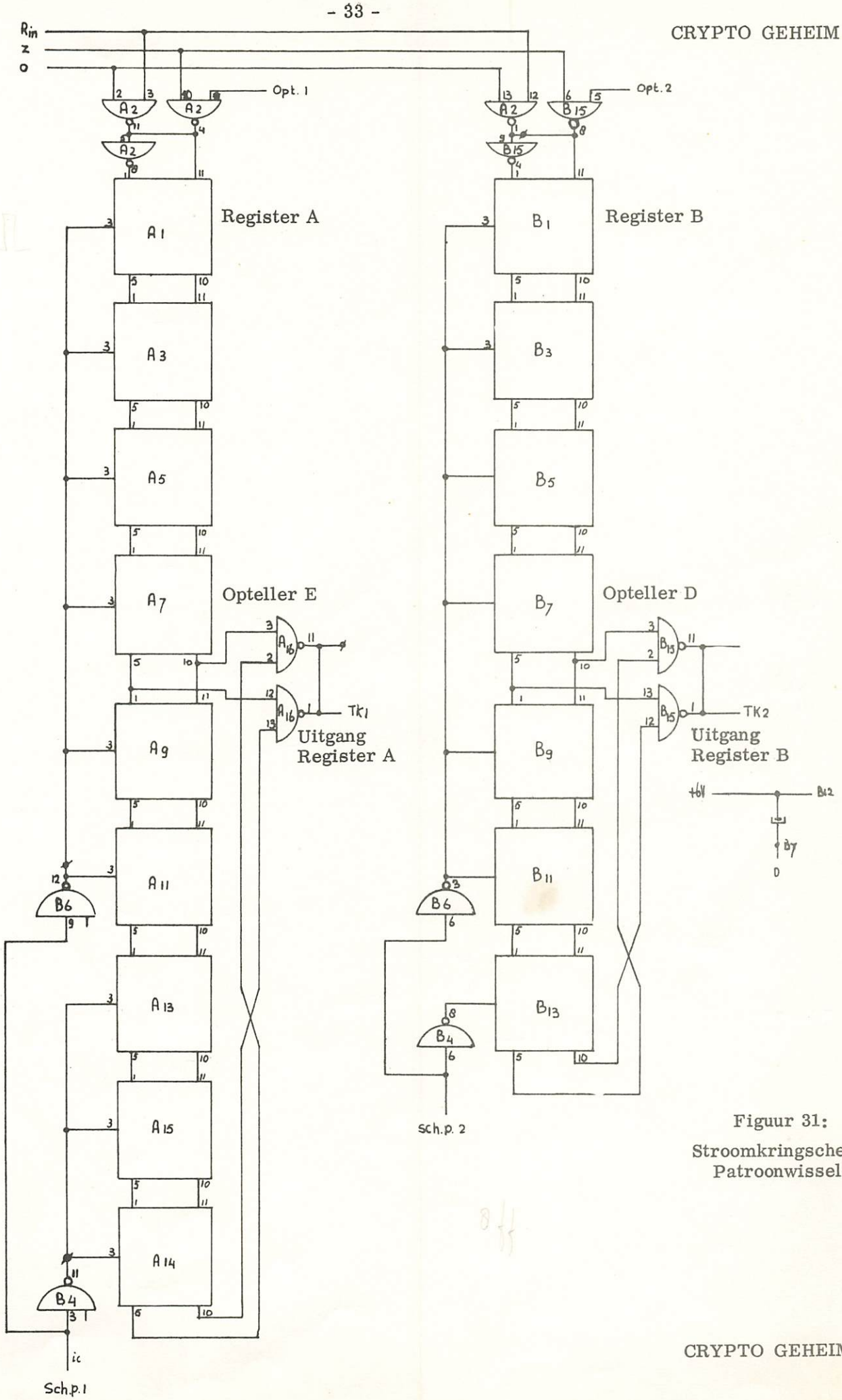
Figuur 29:
Overzicht Crypto-gedeelte

20. Patroonwisselaar (eenheid 7)

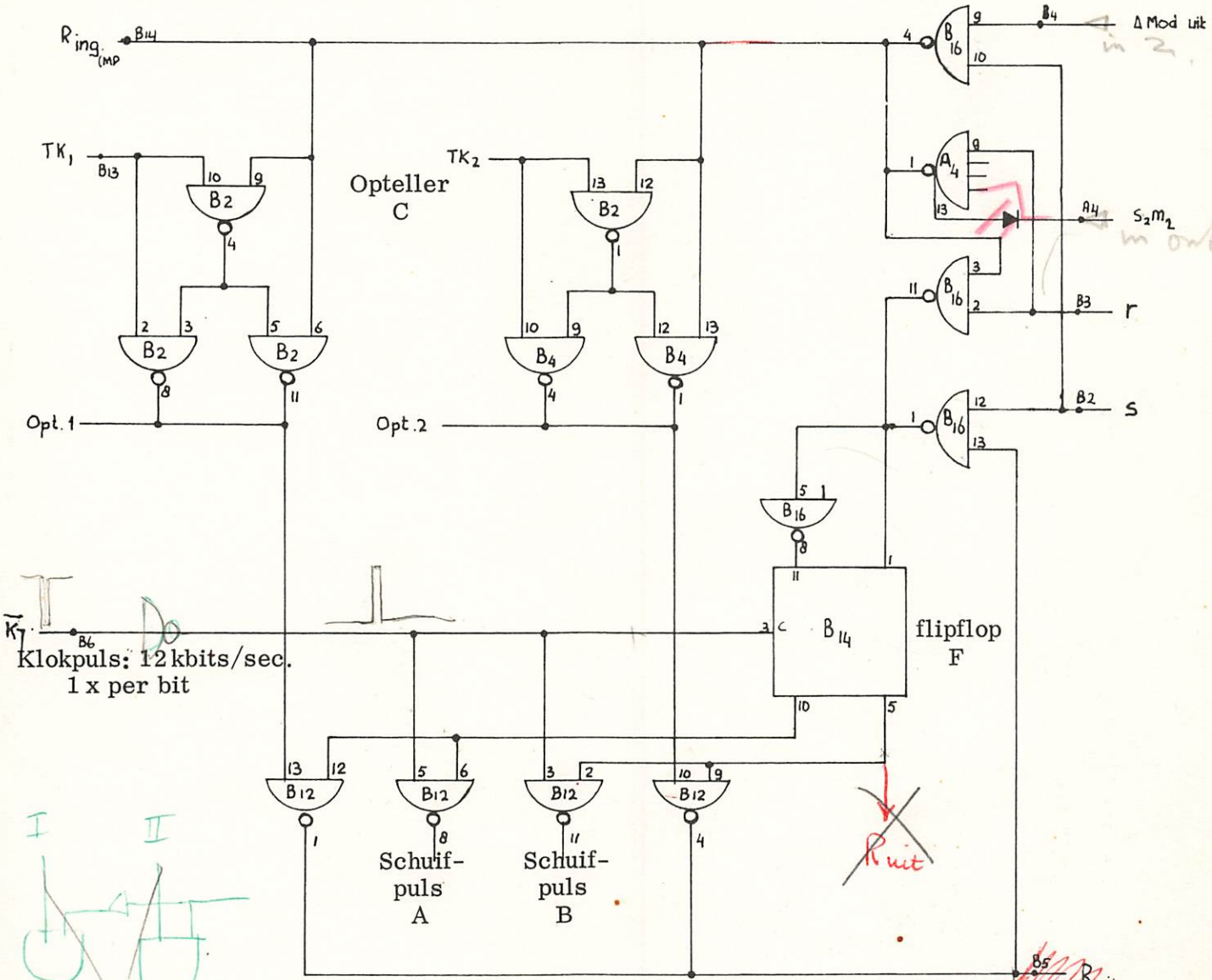


Figuur 30: Principe van de patroonwisselaar

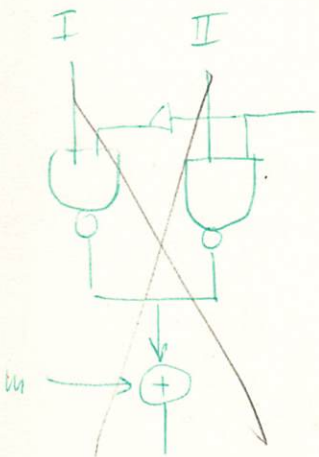
De patroonwisselaar bestaat uit een modulo-2 opteller C, twee schuifregisters A en B en een commando-flipflop F. Een sleutelbit wordt in C opgeteld bij een klare tekst bit, resulterende in een versluierd bit. Het sleutelbit zelf wordt van de versluierde tekst afgeleid, door middel van een niet lineaire terugkoppeling. De versluierde tekst uit C vormt het ingangssignaal voor de Registers A en B en ook voor flipflop F. Register A bezit 9 secties en de uitgang van de 9^e sectie wordt bij die van de 4^e sectie opgeteld in een modulo-2 opteller E.
Register B bezit 7 secties, en de uitgang van de 7^e sectie wordt bij die van de 4^e sectie opgeteld in een opteller D.
De schuifregisters worden in een onderling afwisselende wijze voortgestapt en uitgelezen; als register A wordt voortgestapt en uitgelezen, wordt B niet voortgestapt en uitgelezen.
De J-K ingangen van flipflop F zijn in faze en tegenfaze verbonden met de versluierde uitgang, waardoor deze flipflop op neergaande flanken van de klokpuls K7 het versluierde signaal gaat volgen. Als de uitgang = 1, wordt register A voortgestapt en uitgelezen, zoals hierboven in het schema is getekend.
De voorwaarden "zend" en "ontvangen" zorgen ervoor dat de patroonwisselaar steeds op de correcte wijze werkt: bij zenden komt het ingangssignaal uit de deltamodulator en gaat naar de crypto-eenheden; bij ontvangen is die volgorde omgekeerd.
De gelijkstroom flipflop die onderaan figuur 32 is getekend, is de regenerator die gebruikt wordt om een "schoon" digitaal signaal aan de zendversterker te leveren. De andere onderaan getekende poorten besturen de loop van de signalen voor zenden en ontvangen.
De stroomkringschema's voor de patroonwisselaar worden in de figuren 31 en 32 gegeven.

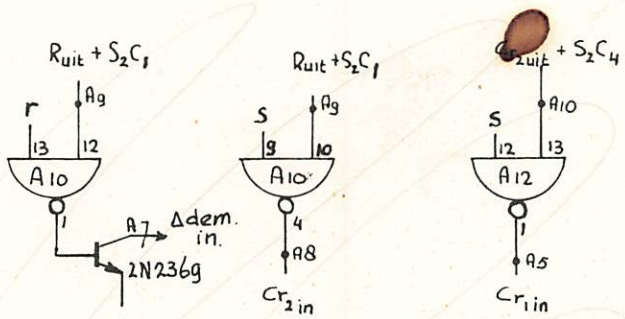


Figuur 31:
Stroomkringschema I
Patroonwisselaar

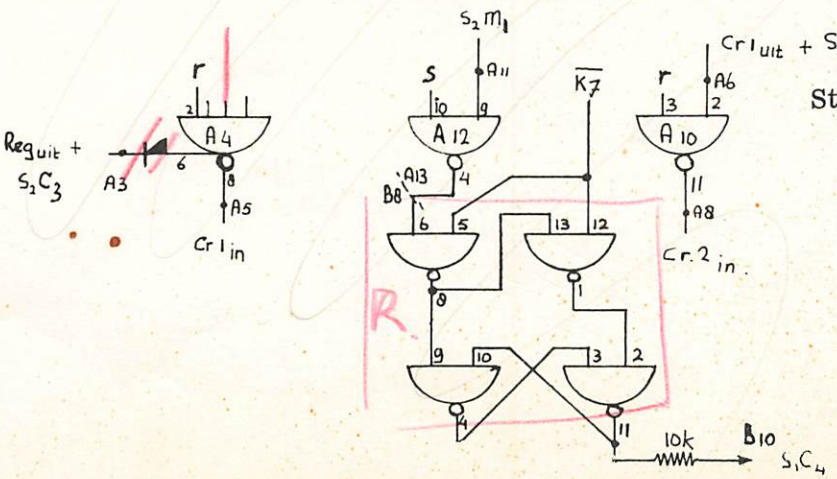


Klokpuls: 12 kbits/sec.
1 x per bit





Regenerator voor zenden



Figuur 32:
Stroomkringschema II
Patroonwisselaar

20. Crypto-eenheden

In figuur 33 is het principe van de crypto-eenheid weergegeven.
In de modulo-2 opteller Q wordt een sleutelbit opgeteld bij een klare tekst bit, resulterende in de crypto tekst. Het sleutelbit wordt afgeleid van de crypto-tekst door middel van een schuifregister A, twee selectie-netwerken Y en Z, die door de dagsleutel bepaald worden, en een transformatie-netwerk.

Het schuifregister A heeft zes schuifsecties en stapt regelmatig op de klokpulsen. Het ingangssignaal wordt gevormd door de crypto-tekst. Het register is verbonden aan twee selectie-netwerken Y en Z, die ieder voor zich 16 verschillende standen kunnen aannemen onder invloed van 4 voorwaarden (4/16 netwerken). De werking van de selectie-netwerken wordt bepaald door de dagsleutel; een en ander wordt behandeld in paragraaf 21. Selectie-netwerk Z is verbonden met de uitgangen van de secties nr. 1, 3, 4 en 5 van schuifregister A; het uitgangssignaal van netwerk Z wordt in modulo-2 opteller C opgeteld bij de uitgang van de 6^e sectie van schuifregister A. Het resultaat van de optelling in C wordt bit U 2 genoemd.
Selectienetwerk Y is verbonden met de uitgangen van de secties nr. 1, 2, 4 en 6 van schuifregister A; het uitgangssignaal van netwerk Y wordt in modulo-2 opteller E opgeteld bij het ingangssignaal van schuifregister A.
Het uitgangssignaal van modulo-2 opteller E wordt bit U 1 genoemd.

Het transformatie-netwerk bestaat uit twee regelmatig stappende 3-sectie schuif-registers J en M, waarvan de uitgang naar hun eigen ingang teruggekoppeld wordt in een onderling afhankelijke en afwisselende wijze. De terugkoppeling wordt bepaald door bit U 1, dat de poorten F en G open of dicht zet; als U 1 = 0, is poort F gesloten en poort G geopend. Als bit U 1 daarentegen = 1, is poort F open en poort G gesloten.
Bit U 2 gaat naar opteller H en vormt dan het ingangssignaal voor schuifregister J of indirect het ingangssignaal voor poort L voor schuifregister M. De beide schuifregisters J en M hebben ieder een modulo-2 opteller die K resp. N genoemd wordt; K is verbonden met de secties 7 en 9 van register J en N is verbonden met de secties 11 en 12 van register M. Of de uitgangen van tellers K of N teruggekoppeld worden naar de ingangen van schuifregisters, hangt af van bit U 1, dat de poorten F of G open zet. Als poort F open is, wordt de ingang van schuifregister J gevormd door de optelling van bit U 2 en de uitgang van teller K; als poort G open is wordt de ingang van register M gevormd door bit U 2, opgeteld in L met de uitgang van terugkoppel-opteller N.

In modulo-2 opteller P worden de uitgangen van de optellers K en N opgeteld en het resultaat van deze optelling wordt als sleutelbit aangeboden aan opteller Q waardoor de crypto tekst ontstaat.

In de figuren 34 en 35 worden de stroomkringschema's voor de crypto eenheid gegeven; de poorten die op figuur 34 boven de optellers E en C getekend zijn dienen voor het uitlezen van de selectie-netwerken, evenals de schakelingen die links onderaan figuur 35 getekend zijn.

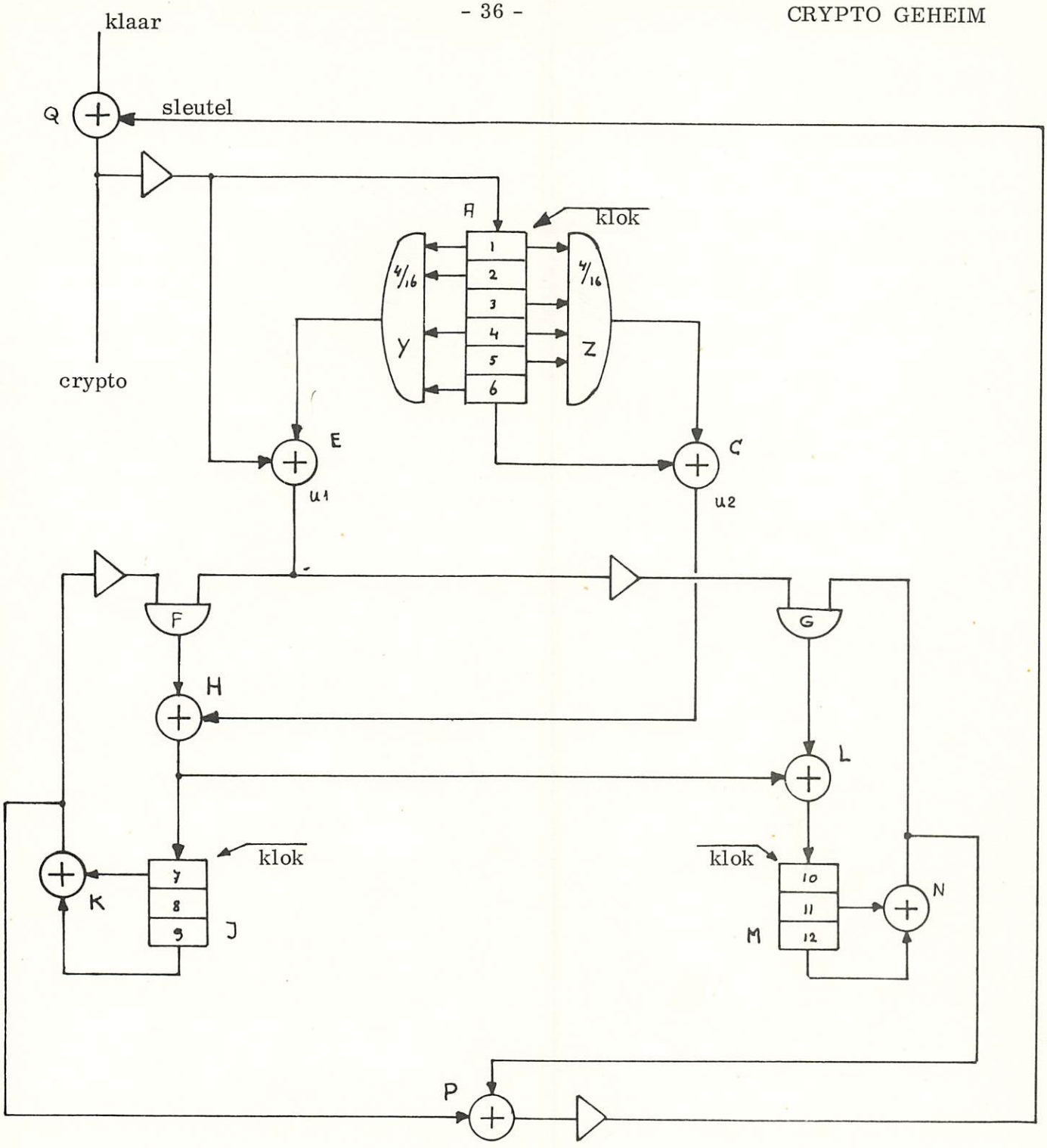


Fig. 33:
Principe van crypto-eenheid

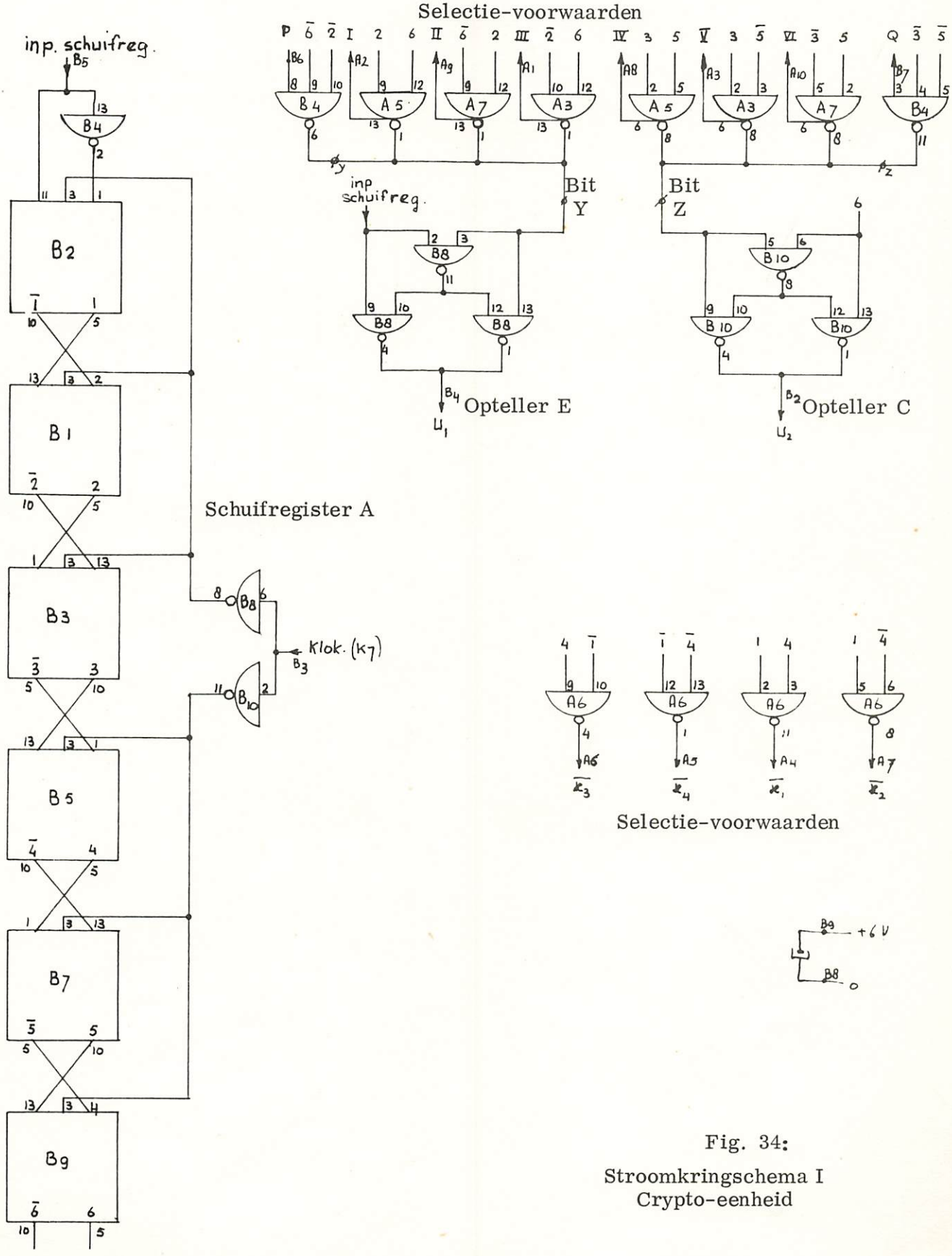
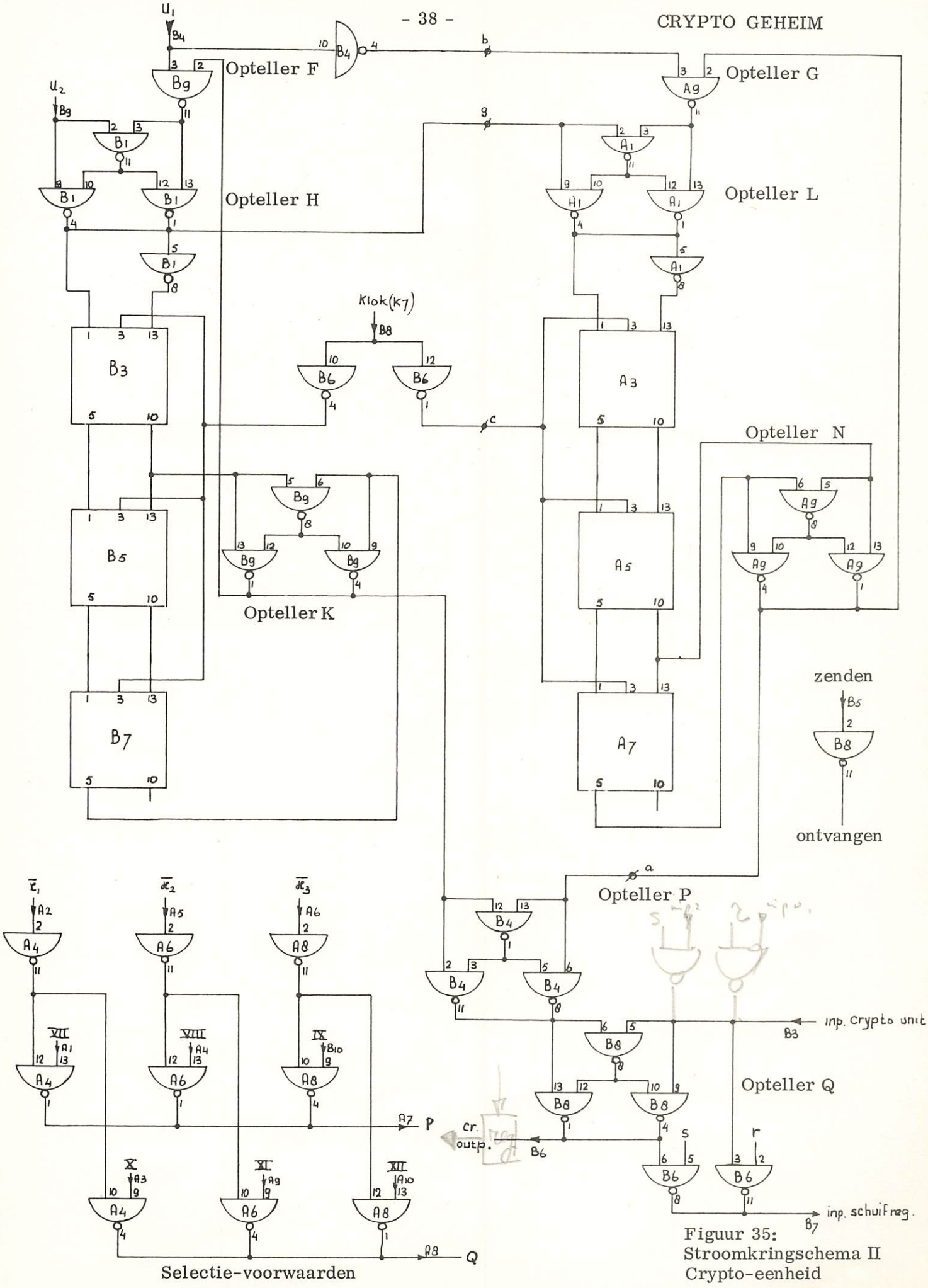


Fig. 34:
Stroomkringschema I
Crypto-eenheid



Figuur 35:
Stroomkringschema II
Crypto-eenheid

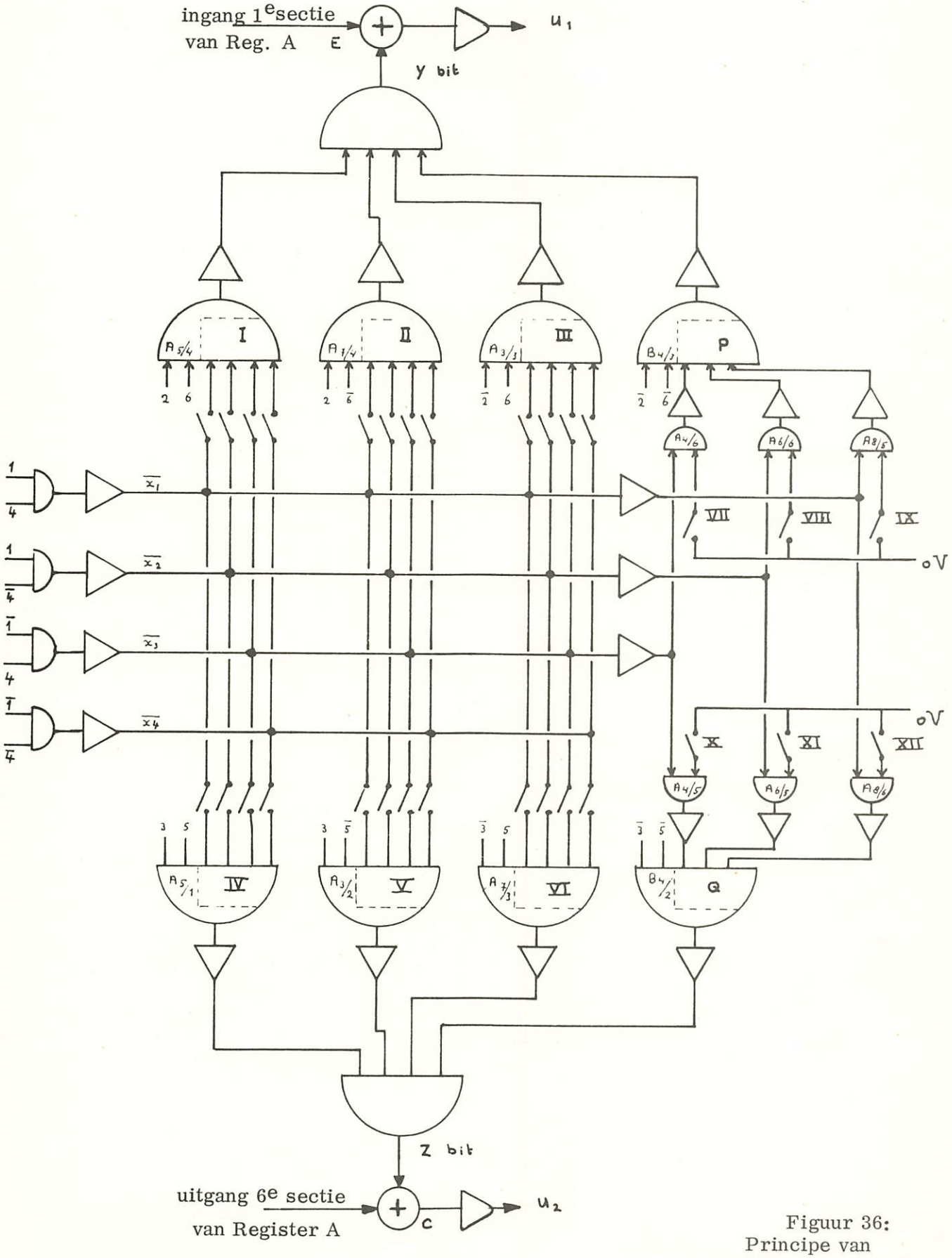
22. Selectie-netwerken, sleutelinstelling

Figuur 36 geeft het principe van de selectie-netwerken weer.
De selectie-netwerken Y en Z worden bestuurd door het schuifregister A.
Beide netwerken zijn verbonden aan de uitgangen van de eerste en vierde secties van schuifregister A; de gecombineerde uitgangen van deze secties wijzen één uit de vier $\overline{x1}$ .... $\overline{x4}$ lijnen aan, waardoor de weg vrijgemaakt wordt om een van de schakelaars I t/m VI, P of Q aan te wijzen.
Selectie-netwerk Y wordt bestuurd door de uitgangen van de secties 2 en 6, terwijl netwerk Z bestuurd wordt door de secties 3 en 5.
Indien bijvoorbeeld het schuifregister A de volgende inhoud heeft:

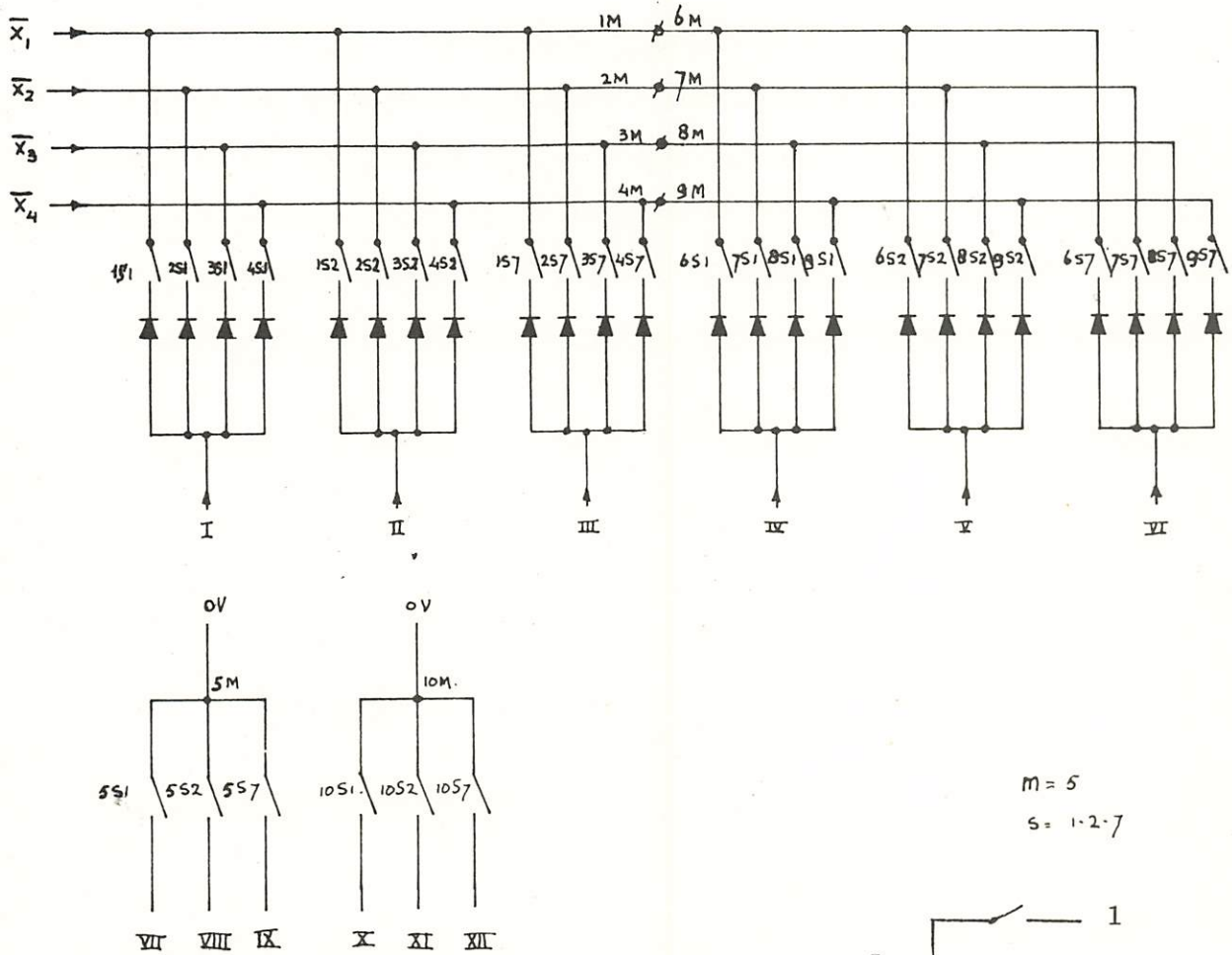
sectie	1	2	3	4	5	6
inhoud	1	1	0	0	1	0

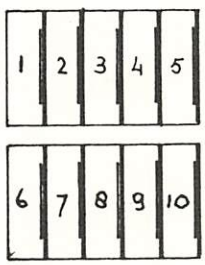
, hetgeen volgens het principe-schema gelezen moet worden als $\overline{1}$ $\overline{2}$ 3 4 $\overline{5}$ 6, dan zal $\overline{1}$ en 4 tezamen de lijn $\overline{x3}$ = "1" aanwijzen en zal $\overline{2}$ en 6 tezamen de poort A 3/3 vrijmaken voor schakelaar III en zal 3 en $\overline{5}$ tezamen de poort A 3/2 vrijmaken voor schakelaar V.
Indien nu vanwege de sleutelinstelling het betrokken gedeelte van schakelaar III gesloten is, zal poort A 3/3 een Y bit = "0" afleveren; als de schakelaar open is, wordt het Y bit = "1". Dit hangt af van de positie van het duimwiel, in dit geval contact nr. 7 van duimwiel 3 (zie figuur 37).
Op dezelfde wijze zal de stand van duimwiel V (= duimwiel 8 op figuur 37) bepalen of poort A 3/2, vrijgegeven door lijn $\overline{x3}$, een Z-bit "1" of "0" zal afgeven.
De uitlezing van de toestanden $\overline{2}$ en $\overline{6}$ (poort B 4/3, schakelaar P) en $\overline{3}$ en $\overline{5}$ (poort B 4/2, schakelaar Q) is anders uitgevoerd: de polariteit van de x-draden is hier omgedraaid en de instelling van de duimwielen 5 en 10 bepaalt rechtstreeks of de poorten A 4/6 ... A 8/5 resp. A 4/5 ... A 8/6 een constant 0-potentiaal zullen ontvangen of niet.
Voor de combinaties ($\overline{1}, \overline{4}, \overline{3}$ en $\overline{5}$) of ($\overline{1}, \overline{4}, \overline{2}$ en $\overline{6}$) worden geen poorten vrijgegeven.
In die gevallen is de uitgang van de netwerken = een vaste "1".
De daadwerkelijke Y- en Z-bits, die geproduceerd worden voor de verschillende instellingen van de duimwielen, zijn vermeld op de lijsten van de figuren 38 en 39.
In figuur 37 wordt de bedrading van de duimwielen weergegeven.

-.-.-.-.-.-.-.-.-.-.-.-.-.-.-



Figuur 36:
Principe van
Selectie-netwerk





Positie	Contacten		
0	0	0	0
1	1	0	0
2	0	1	0
3	1	1	0
4	0	0	1
5	1	0	1
6	0	1	1
7	1	1	1

Figuur 37:
Stroomkringschema
Duimwielen

Position of shiftregister A		Output selection matrix Y				
Pos. no.	Output of sections 1 2 4 6	If thumbwheel 1 is in pos. no. 0 1 2 3 4 5 6 7	If thumbwheel 2 is in pos.no. 0 1 2 3 4 5 6 7	If thumbwheel 3 is in pos.no. 0 1 2 3 4 5 6 7	If thumbwheel 4 is in pos.no. 0 1 2 3 4 5 6 7	If thumbwheel 5 is in pos.no. 0 1 2 3 4 5 6 7
0	0 0 0 0	1 0 1 0 1 0 1 0				
1	1 0 0 0			1 0 1 0 1 0 1 0		
2	0 1 0 0	1 1 1 1 0 0 0 0				
3	1 1 0 0			1 1 1 1 0 0 0 0		
4	0 0 1 0		1 0 1 0 1 0 1 0		↓	
5	1 0 1 0	→			1 0 1 0 1 0 1 0	
6	0 1 1 0		1 1 1 1 0 0 0 0		↓	
7	1 1 1 0	→			1 1 1 1 0 0 0 0	
8	0 0 0 1	1 1 0 0 1 1 0 0				
9	1 0 0 1			1 1 0 0 1 1 0 0		
10	0 1 0 1					0 1 0 1 0 1 0 1
11	1 1 0 1					0 0 0 0 1 1 1 1
12	0 0 1 1		1 1 0 0 1 1 0 0		↓	
13	1 0 1 1	→			1 1 0 0 1 1 0 0	
14	0 1 1 1					0 0 1 1 0 0 1 1
15	1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1

Output of the matrix is:
If the key setting happens to be: all thumbwheels in position "4", the output Y from the matrix will be in the position ... of shift Register:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
1 1 0 0 1 1 0 0 1 1 0 1 1 1 0 1 , as indicated by arrows for positions 5, 7 and 13.

Figuur 38:
Output van selectie-netwerk Y

CRYPTO GEHEIM

Position of shiftregister A		Output selection matrix Z				
Pos. no.	Output of sections 1 3 4 5	If thumbwheel 6 is in pos.no. 0 1 2 3 4 5 6 7	If thumbwheel 7 is in pos.no. 0 1 2 3 4 5 6 7	If thumbwheel 8 is in pos.no. 0 1 2 3 4 5 6 7	If thumbwheel 9 is in pos.no. 0 1 2 3 4 5 6 7	If thumbwheel 10 is in pos.no. 0 1 2 3 4 5 6 7
0	0 0 0 0	1 0 1 0 1 0 1 0				
1	1 0 0 0			1 0 1 0 1 0 1 0		
2	0 1 0 0	1 1 1 1 0 0 0 0				
3	1 1 0 0			1 1 1 1 0 0 0 0		
4	0 0 1 0		1 0 1 0 1 0 1 0			
5	1 0 1 0				1 0 1 0 1 0 1 0	
6	0 1 1 0		1 1 1 1 0 0 0 0			
7	1 1 1 0				1 1 1 1 0 0 0 0	
8	0 0 0 1	1 1 0 0 1 1 0 0				
9	1 0 0 1			1 1 0 0 1 1 0 0		
10	0 1 0 1					0 1 0 1 0 1 0 1
11	1 1 0 1					0 0 0 0 1 1 1 1
12	0 0 1 1		1 1 0 0 1 1 0 0			
13	1 0 1 1				1 1 0 0 1 1 0 0	
14	0 1 1 1					0 0 1 1 0 0 1 1
15	1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1

Figuur 39:
Output van selectie-netwerk Z