(What is meant by "placing the beam under the influence of an electric or magnetic field and directing it onto the screen" is merely that the electron gun is aimed at a target ~~is completed~~ by applying voltages to the members of two pairs of deflecting plates located within the tube; which plates act upon the beam.

Invention of an Electronic Cryptograph

1. The basic instrumentality ~~in~~ this invention is an ~~radial~~ electron gun ~~electron gun~~ of a type ~~quite~~ similar to that used in the cathode-ray tube of a modern oscillograph.

2. In the latter type of tube the electron stream is concentrated into a beam, which beam is placed under the influence of an electric (or magnetic) field and then directed onto a specially prepared screen located within the tube. This screen fluoresces at the point of impact of the electron beam and thus makes visible the trace of the beam by ~~at~~

3. ~~Let~~ the electron beam, instead of being aimed at ~~a~~ non-conducting target bearing or supporting a set of a fluorescent screen, be aimed at a ~~small~~ metal disks; ~~and~~ let each of these disks be connected to a terminal outside the tube; and let each of these terminals be in a separate electrical circuit outside the tube by means of a conductor passing through the glass wall of the tube. Then instead of producing a fluorescence on a screen the electron stream will produce ~~a~~ currents in the circuits in which the metal disks being bombarded by the area located ~~the disks struck by the electron beam is located~~ may then directly operate relays, or other electrically-responsive devices; or they may be amplified first and then used to control relays or other devices.

4. The aiming of the electron gun is usually accomplished by means of two pairs of deflecting plates upon which various amounts of current may be impressed, as the horizontal and the vertical deflecting plates, the electron beam can thus be made to describe various figures, simple or

complicated. If the impressed voltages impressed upon the deflecting plates are of a constant character (d.c.) then the stream of electrons may be directed against a specific

4. The cathode-ray tube of the ~~[illegible]~~ type just described has recently been invented by personnel of the International Business Machines Corporation and patents are pending on it. The tube itself forms no part of the present invention, which is concerned with circuits and arrangements for making combinations of such tubes serve cryptographic purposes. In other words, the object of the invention is to construct an ~~[illegible]~~ electronic cryptographic machine with as few moving parts as possible.

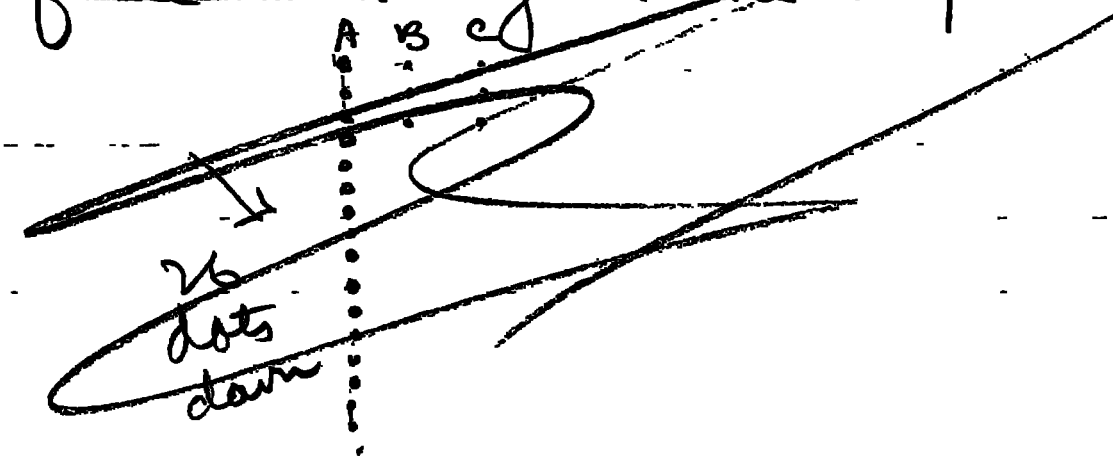
5. Suppose the conducting disks on the target be arranged upon the coordinate system, ~~[illegible]~~ in a square 26 x 26, or 676 disks in all. Each disk is connected to a terminal outside the tube. Now suppose that a series of 26 different voltages are available and can be impressed upon the vertical deflecting plates; these voltages then can be made to correspond to the letters of the plain text to be employed; suppose that another and similar series of 26 different

voltages are available and can be impressed upon the horizontal deflecting plates. These voltages then can be made to correspond to the letters of the ~~key~~ enciphering key. Encipherment by such a scheme will thus correspond to encipherment by means of cipher ~~the encipherment of~~ a quadricular Vigenère table, the cipher equivalent of a given plain-text letter depending upon the key letter employed in its encipherment.

6. Means for impressing the various ~~different~~ voltages on the vertical deflecting plates (to correspond with the plain-text letters to be enciphered) are readily available. A potentiometer can be arranged to accomplish this function, so that, for example, when the key A is depressed on the keyboard, the electron beam comes under the influence of a ~~a voltage of such~~ potential of such ~~certain~~ voltage value as will cause the beam to be ~~in the electron beam~~ directed onto the 1st row of ~~the~~ disks on the target; when the key B is depressed, the beam is directed onto the 2d row, and so on. Thus the 26 voltages may be used to direct the beams at the 26 rows ~~of elements in a Vigenère square. The elements in the case~~ of conducting disks carried by the target inside the cathode ray tube. These then correspond to the 26 rows of letters in an ordinary quadricular cipher table. ~~These are three of the 26 rows of disks, corresponding to the 26 rows of letters in a Vigenère square.~~

(9)

7. Means for impressing the various voltages on the horizontal deflecting plates (to correspond with the successive key letters entering into the enciphering equations) are now to be discussed. It is obvious that if only one voltage were applied to the horizontal deflecting plates the result would be monoalphabetic encipherment. It follows, therefore, that for polyalphabetic encipherment means must be provided for successively varying the keying voltages impressed upon the horizontal deflecting plates, so that successive encipherments of even the same letter will yield different cipher equivalents, as the keying voltages change. This corresponds to selecting the various columns of a Vigenere square according as the key letter changes.



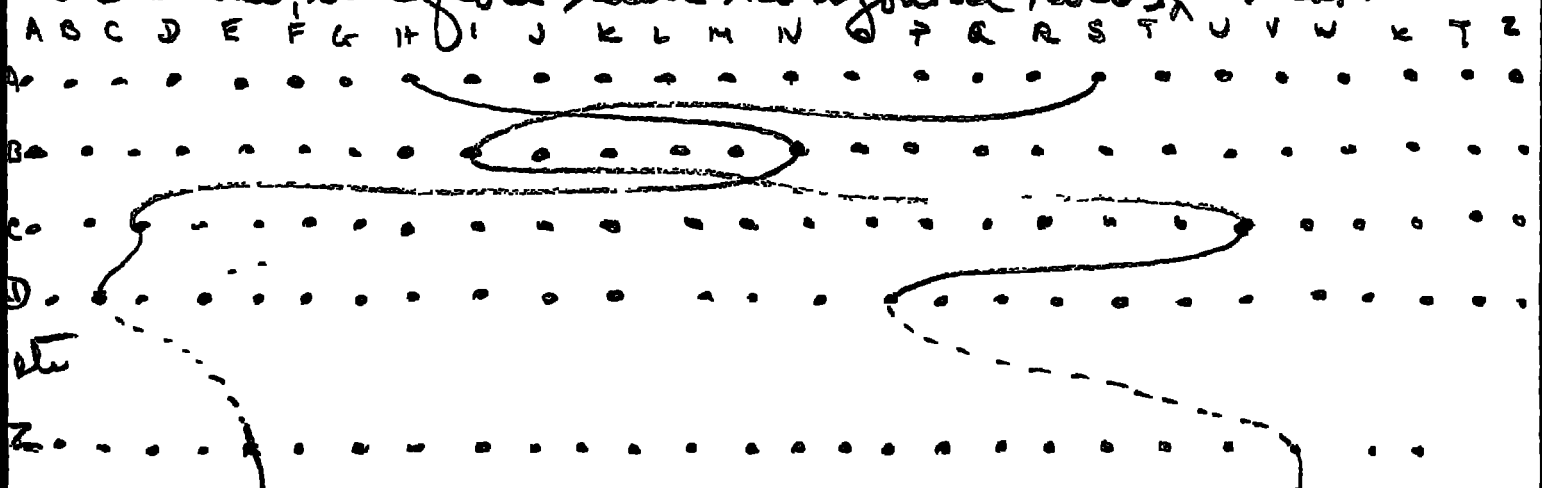
(J)

Thus these 26 voltages may direct the beam at the 26 columns of conducting disks carried by the target inside the cathode ray tube. These then correspond to the 26 columns of letters in the quadricular table. Thus, a coordinate system of finding cipher equivalents has been established and

A potentiometer can also be arranged to accomplish this function, so that, for example, when the letter A is the key letter, the electron beam is directed onto the 1st column of disks on the target; when B is the key letter, the beam is directed onto the 2d column, and so on. ~~That is~~ It is essential by regulating the voltages impressed upon both the horizontal and the vertical deflecting plates, to correspond with plain-text / key letter relationships, encipherment corresponding to ~~key~~ the usual quadricular cipher table method can be accomplished instantaneously by means of the tube described. ~~But thus far no means for changing the successive key letters has been devised. This will not be done~~ simple, preferably electronic means are incorporated to change the key letter with each encipherment, according to some aperiodic sequence, then a fairly secure method will have been established for cryptographic purposes. It is to be understood, of course, that the 676 disks are connected to but 26 different final terminals, so that only 26 different resultant effects are obtained from the aiming of the electron gun at the target. This obviously corresponds to the final effects of a quadricular table, which are reduced to but 26 different effects.

with REF ID: A67404 conductor and then to one terminal outside the tube.

8. The reduction to 26 different effects may be accomplished entirely within the tube itself, by joining 26 disks, one from each horizontal row. Thus:



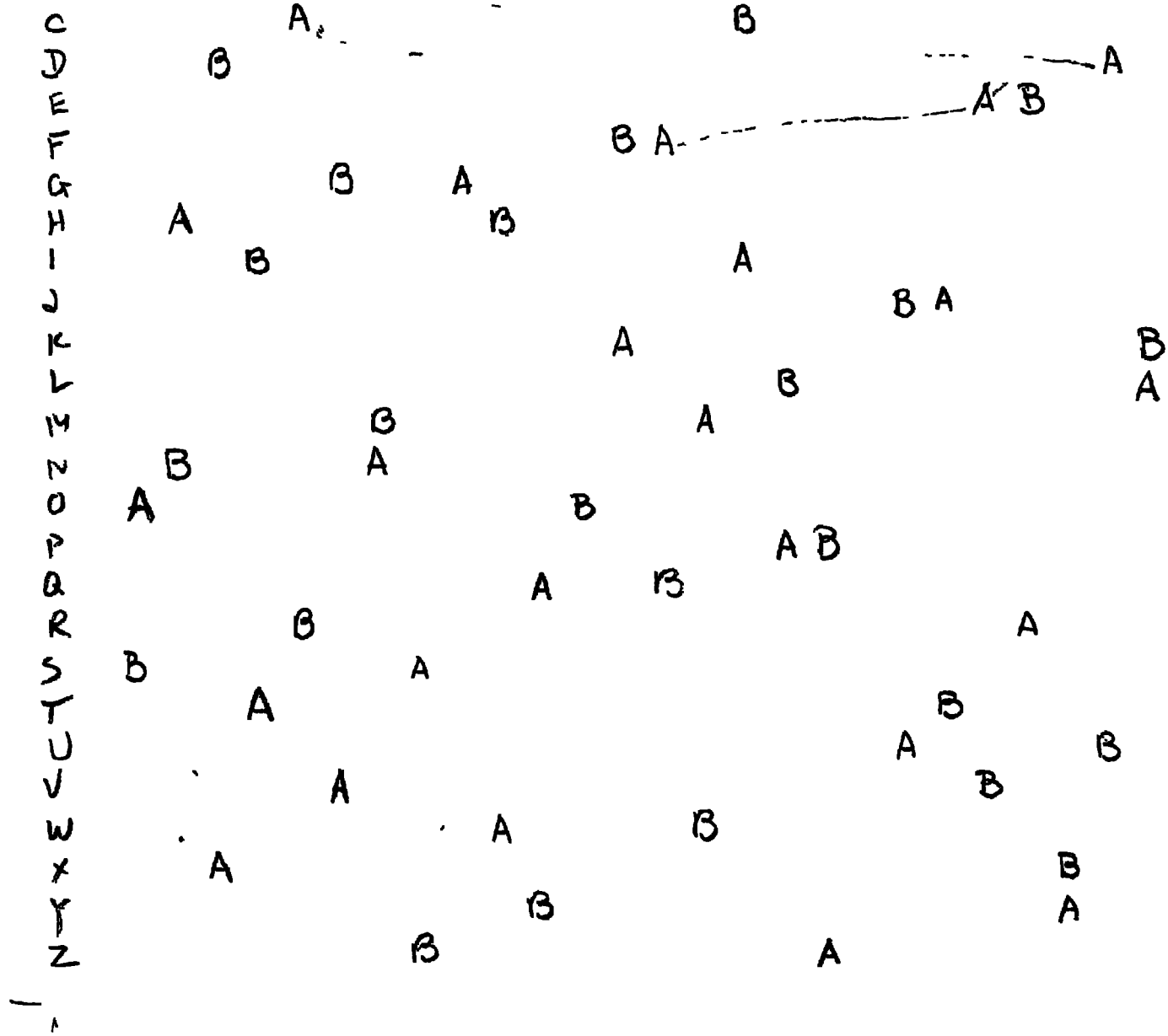
J I L V A K C Z U H S W G M R B T X F N D Q P Y O E

In this sketch A_p exemplified by H_k, ~~[illegible]~~ B_p by N_k, ~~[illegible]~~ C_p by C_k, D_p by B_k, and Z_p by E_k all yield A_c. A_p by S_k, B_p by I_k, C_c by W_k, D_p by O_k, Z_p by $X_k = Y_c$.

9. If this is the case, then once a tube has been wired up, no changes are possible so far as concerns the exact cipher equivalent obtained for each specific encipherment. But if the 676 individual disks were connected to 676 individual terminals outside the tube, then the cipher results could be changed at will, by suitable ~~[illegible]~~ patchboard arrangements.

10. By arranging the wirings for reciprocity, the same tube can be employed for encipherment and decipherment. An illustration follows.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	O	H	X	T	C	V	N	S	G	W	Q	A	K	F	M	I	P	Z	B	U	J	E	R	T	D	L
B	S	N	D	I	R	G	M	Z	B	H	Y	O	F	Q	W	C	L	P	A	J	T	V	E	X	U	K

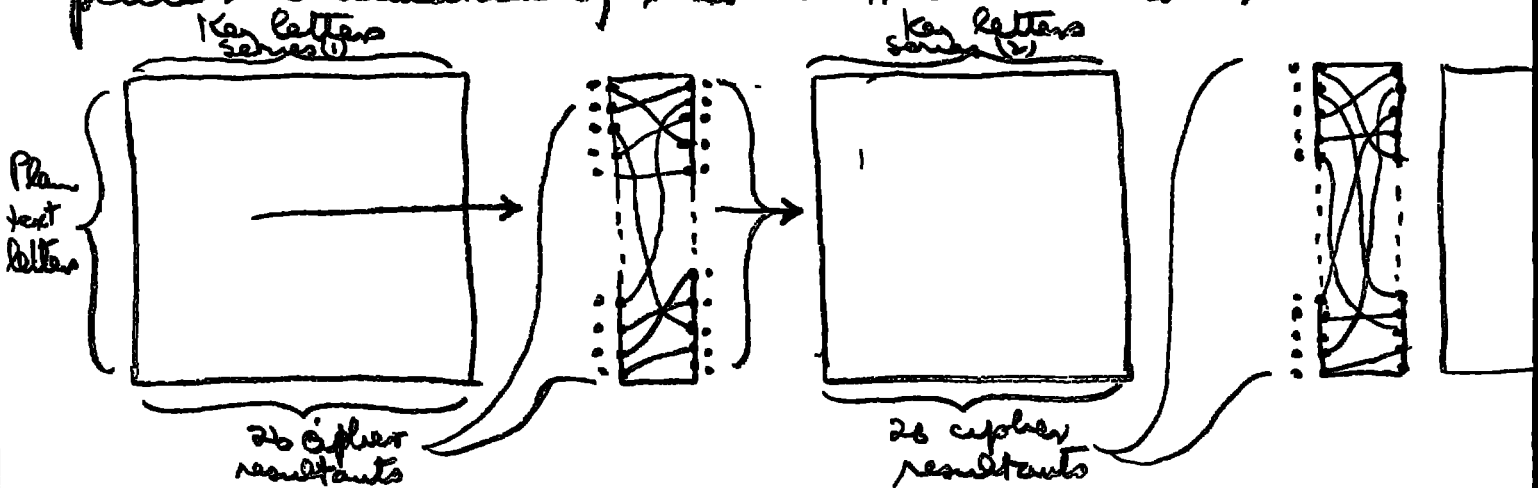


$\begin{cases} A_p(A_{p_2}) = O \\ O(A_k) = A \end{cases}$

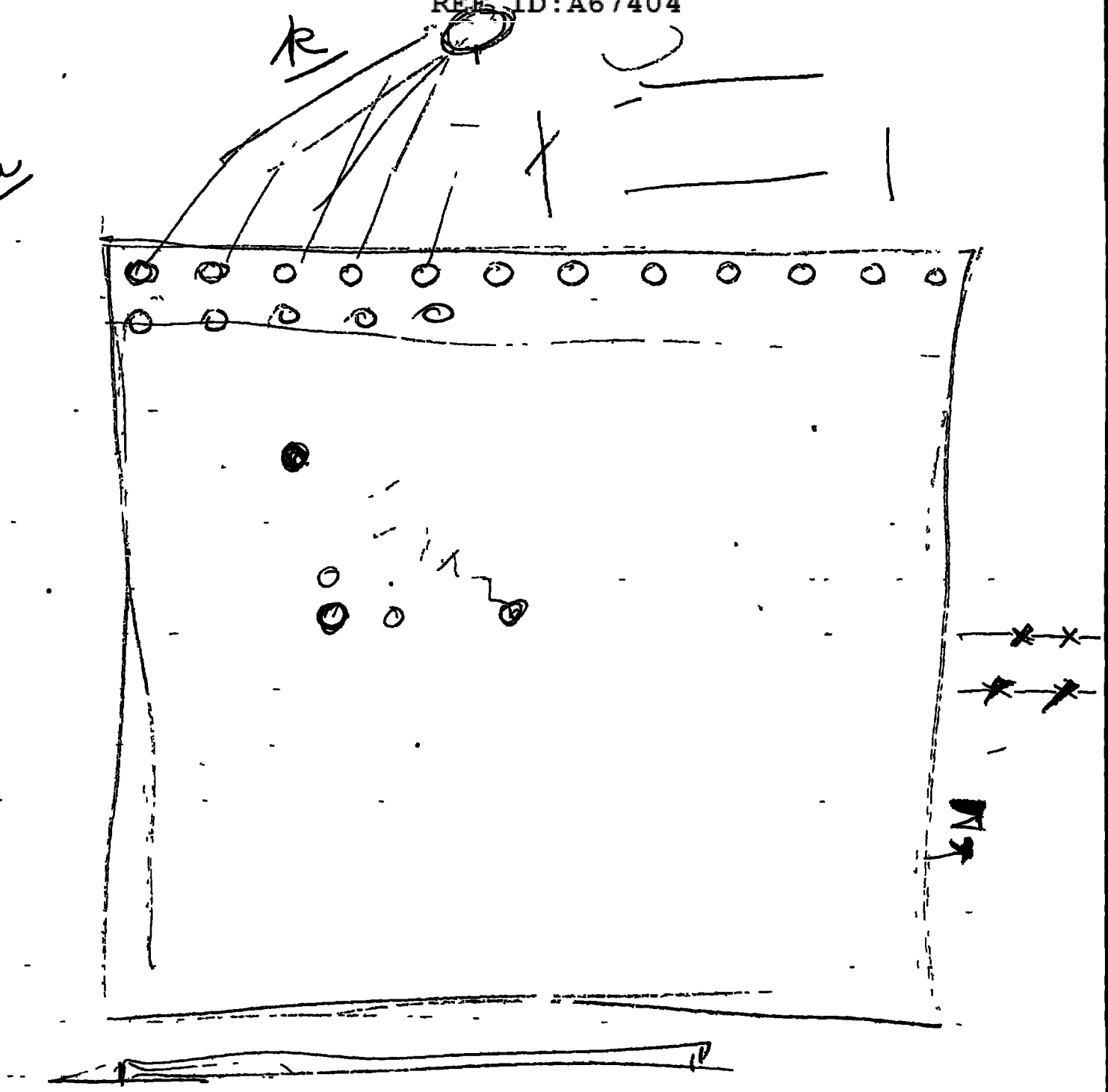
$\begin{cases} B_p(L_k) = O \\ O(L_p) = B \end{cases}$

$\begin{cases} A_p(B_k) = H_c \\ H_p(B_k) = A_c \end{cases}$

11. The 26 different resultants coming out of one tube may be led to a second tube via a connection changer plate. Schematically this is shown below:



12. By continuing this arrangement a "cascade effect" may be obtained, analagous to that obtained by juxtaposing rotatable cipher commutators.



26