

Address of Government (Arlington Hall Station)
 Station Where Inventors (4000 Lee Blvd.)
 are Located (Arlington, Virginia)

To The Chief Signal Officer:

I/~~we~~ believe myself/ourselves to be sole inventor/~~s~~ of an
 (sole or joint)
authenticating device,

and request that you investigate its military value, patentability, and inventorship. In support of this request the following information is submitted:

At the time I/~~we~~ conceived the invention, my/~~our~~ employment was Director of Com. Research, SSA. I/~~we~~ originally conceived the idea in Sept. 1943 and communicated it to: Major Leo Rosen 22 October 1943 (date)
 (names) (date)

The first written and dated records are 8 June 1944, first detailed description and drawing.

It was first actually tried not tried with the result that
 (date)

Its uses are for authenticating messages, particularly banking messages involving the transfer of money.
 Others associated with me/~~us~~ in this development or having knowledge concerning it are:
Major Leo Rosen, Sgt. Henry B. Stauffer.

Attached are 4 sheets, each initialed and dated by me/~~us~~ and two disinterested witnesses, giving a detailed description of the invention, a ~~brief history of its development~~ and a clear statement of what is believed to be new.

I/~~we~~ agree to abide by the decision of the Patent Board or of the Chief Signal Officer and will promptly execute all papers required of me/~~us~~ by these authorities including an assignment of the invention to the Government if it is decided by the Patent Board and confirmed by the Chief Signal Officer, that the application should be kept secret.

Signature _____	Signature <u>William J. Fredeman</u>
Rank, position or employment _____	Rank, position or employment <u>Dir. of Com. Research, SSA.</u>
Legal residence _____	Legal residence <u>8952 Military Road, Washington 15, D. C.</u>
Present home P. O. address _____	Present home P. O. address <u>Same</u>
Date of signature _____	Date of signature <u>12 June 1944</u>
Witnesses: _____ Date _____	Witnesses: <u>Mark Choad</u> Date <u>12 June 1944</u>
	<u>4921 Bedford St. Arlington, Va.</u>

A.R. 850-50 outline the procedure to be followed in submitting inventions to the Chief Signal Officer. If the invention relates to Signal Corps equipment this form together with a full description of the invention should be forwarded directly to the Chief Signal Officer. If the invention relates to equipment of another arm of service, the invention should be submitted directly to that arm or service.

Most descriptions of inventions received by the Signal Corps from inventions are too brief, vague and indefinite for the purpose of preparing patent applications. The Chief Signal Officer insists on very complete and clear descriptions.

~~CONFIDENTIAL~~

This invention is an authenticating device and, particularly, is a device by means of which the bona fides of certain types of messages can be readily proved.

It is customary in certain fields of commerce, as for instance banking, to transmit cable and radio communications in code or cipher, rather than in clear text. This is economical, and serves in some measure to protect the interests of customers and of the commercial institutions themselves. According to the following description, this invention is to be used by banking and other financial institutions, but it will be obvious that it is applicable as well to other types of businesses, and has military applications as well.

In the drawings:

Figure 1 is a diagram of one of the mixing or "scrambling" elements used in the invention.

Figure 2 is a diagrammatic representation of the authenticating device of this invention.

The invention comprises a group of ten mixing elements in the nature of cryptographic rotors. One such rotor is shown in Figure 1, where it may be seen to consist of a body member 10, formed of Bakelite or some other insulating material, and a group of ten contacts 11-20, inclusive. A second group of contacts 21-30, appear on the opposite face of the body member.

The contacts 11-20 will normally serve as input contacts and the other set will normally serve as output contacts. Connections between the several input contacts and the output contacts are made at random or according to some predetermined complicated rule. The result is, of course, that an input

~~CONFIDENTIAL~~

signal representing one condition is converted to an output signal representing something entirely different.

Referring to Figure 2, the invention may be seen to include a shaft 35, supported at its two ends in members 38 and 39. The members 38, 39 may be of any form desired. Their only functions are to support the shaft 35, and to carry stationary electrical contacts, 41-50, on the one hand, and 51-60, on the other.

Mounted on the shaft 35 are ten cryptographic rotors 71-80, such as that illustrated in Figure 1, and earlier described. The rotors are all essentially similar, but their internal wiring normally will be different. The rotors bear on their peripheries indicia of one type or another, the type depending, to some extent at least, on the material to be handled by the authenticator. In Figure 2, rotors 71 and 72 and 74-80 bear ordinary Arabic numerals arranged in normal order from 0 to 9. Rotor 73 carries symbols representing the money of various countries. The rotors are, in addition, identified by number, as 81, or otherwise, so that they can be readily arranged in any desired order.

At the left end of the device of Figure 2, is a rotary switch 90 adapted for manual operation, and this switch is in circuit with a battery 91 or other source of current. There are six make contacts 92-97 on switch 90, and, if desired, a neutral or non-make position 98. The six make contacts are adapted for variable connections to the ten contacts 41-50, inclusive, by means of plugs and jacks, as 99', 99".

~~CONFIDENTIAL~~

At the other end of the rotor system, ten output leads may be seen, and, associated with each, an electric lamp, as 101-110, inclusive, these lamps being likewise in the circuit of battery 91. Adjacent the lamps is a strip 111, bearing ten numerals randomly arranged. This strip is slidably mounted in a holder 112, so that it may be removed therefrom and replaced by another strip.

In the preferred embodiment of the invention, means are provided for stepping one or more of the rotors 71-80 each time a signal is fed through the system. In Figure 2, such means are represented by block 120. After positioning rotary switch 90, switch 121, which may be in the nature of a simple pushbutton, is closed. When it is reopened, rotor 71 is advanced one step. The other rotors are stepped under the control of rotor 71 in any of several well-known manners.

Assuming switch 121 to be closed, it will be apparent that an electrical current from battery 91 will traverse a path through the rotor system depending, in the first instance, on the input contact utilized, and, secondly, upon the internal wiring of the several rotors, the order in which the rotors are arranged on shaft 35, and the relative rotatory positions of the rotors. Under one set of conditions, for example, a signal introduced at the contact 2 on the leftmost rotor of Figure 2 may find its way through the rotor maze to energize lamp 110. A change in any one of the conditions mentioned just above, may cause the signal to illuminate lamp 101. The number on the strip 111, adjacent the energized lamp, will depend upon the arrangement of the numerals on the strip.

One method of using the invention, by bank or other financial organization, will now be described. A United States bank, wishing to make a deposit in a London bank, would compose the basic text of its cablegram according to the standard private code in use. It would then take the device of this invention and, in conformity with a prearranged plan, insert a particular strip 111 in the holder 112 and arrange the rotors in proper order. The contacts 92-97 inclusive, would next be plugged into predetermined input connections in member 38. The rotors would then be individually adjusted so that, for example, (reading the second row of indicia on the rotors), the first two indicate the serial number of the message (35, in Figure 2), rotor 73 indicates United States dollars, and rotors 74-80, the amount of the deposit (\$9,756,125, in the illustration).

The operator would then move switch arm 90 to contact 92, for example, and under these circumstances it may be assumed that the lamp 102, adjacent numeral 7 on strip 111, will be lighted. Arm 90 would then be moved to contact 93, and lamp 101 adjacent numeral 5 would be energized. Upon movement of arm 90 to contact 94, lamp 107, adjacent numeral 9, would be energized. The operator would take these three numerals in the order in which they occurred, namely, 7-5-9, and encode them by means of his standard code, thereby obtaining group such as ROXIP. This group, located in a prearranged position in the message, would then be transmitted as an authenticator.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

The bank receiving the cablegram would, after decoding, set up its machine just as the machine was set up by the transmitting bank, arranging the rotors in accordance with the amount of the deposit, the serial number of the message, etc. The operator would next move the switch arm 90 of his device to the three contacts 92-93-94 in order. Unless he derived the number represented in his codebook by the group ROXIP, he would know that either the message was not authentic or that some error had been made.

Of course the device will not furnish a different code group for each possible condition of the rotors and other variable elements. Considering the seven rotors 104-110 alone, it will be apparent that ten million different combinations can be set up, whereas using the ten lamps, 101-110, inclusive, in combinations of three, only 720 different test groups can be obtained. A greater number of groups can, of course, be achieved if it is desired to use longer test groups, but in ordinary business usage the three-numeral group has been found to be satisfactory.

Further, it will be obvious that either more or fewer rotors may be used, without altering the principles of the invention. The number decided upon will depend upon many factors.

The above description is in specific terms. It should be understood, however, that the invention is not limited to the exact structure shown and described, and, therefore, for the true scope of the invention, reference should be had to the appended claims.

I claim:

~~CONFIDENTIAL~~

1. In a device of the character described, a source of current, a series of multiple-contact switches adapted to provide a plurality of variable paths for electrical signals, the said series having a plurality of contacts at each end thereof, another switch for selecting a contact at one end of said series, and a signaling device associated with each of the contacts at the other end of said series.

2. In a device of the character described, a source of current, a series of multiple-contact switches adapted to provide a plurality of variable paths for electrical signals, the said series having a plurality of contacts at each end thereof, another switch for selecting a contact at one end of said series, a signaling device associated with each of contacts at the other end of said series, and means for varying the significance of the energization of a signaling device.

3. In a device of the character described, a source of current, a series of multiple-contact switches adapted to provide a plurality of variable paths for electrical signals, the said series having a plurality of contacts at each end thereof, another switch adapted to make successive circuits between said sources of current and a predetermined number of selected contacts at one end of said series, and a signaling device associated with each of the contacts at the other end of said series.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

4. In a device of the character described, a source of current, a series of multiple-contact switches adapted to provide a plurality of variable paths for electrical signals, the said series having a plurality of contacts at each end thereof, another switch adapted to make successive circuits between said sources of current and a predetermined number of selected contacts at one end of said series, and means for varying the paths through said multiple-contact switches.

5. In a device of the character described, a source of current, a series of cryptographic rotors or the like adapted to provide a plurality of variable paths for electrical signals, the said series having a plurality of contacts at each end thereof, another switch for selecting a contact at one end of said series, a signaling device associated with each of the contacts at the other end of said series, and an additional switch adapted, when closed, to provide a signal to said series of rotors, and, when opened, to actuate said rotor stepping device.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

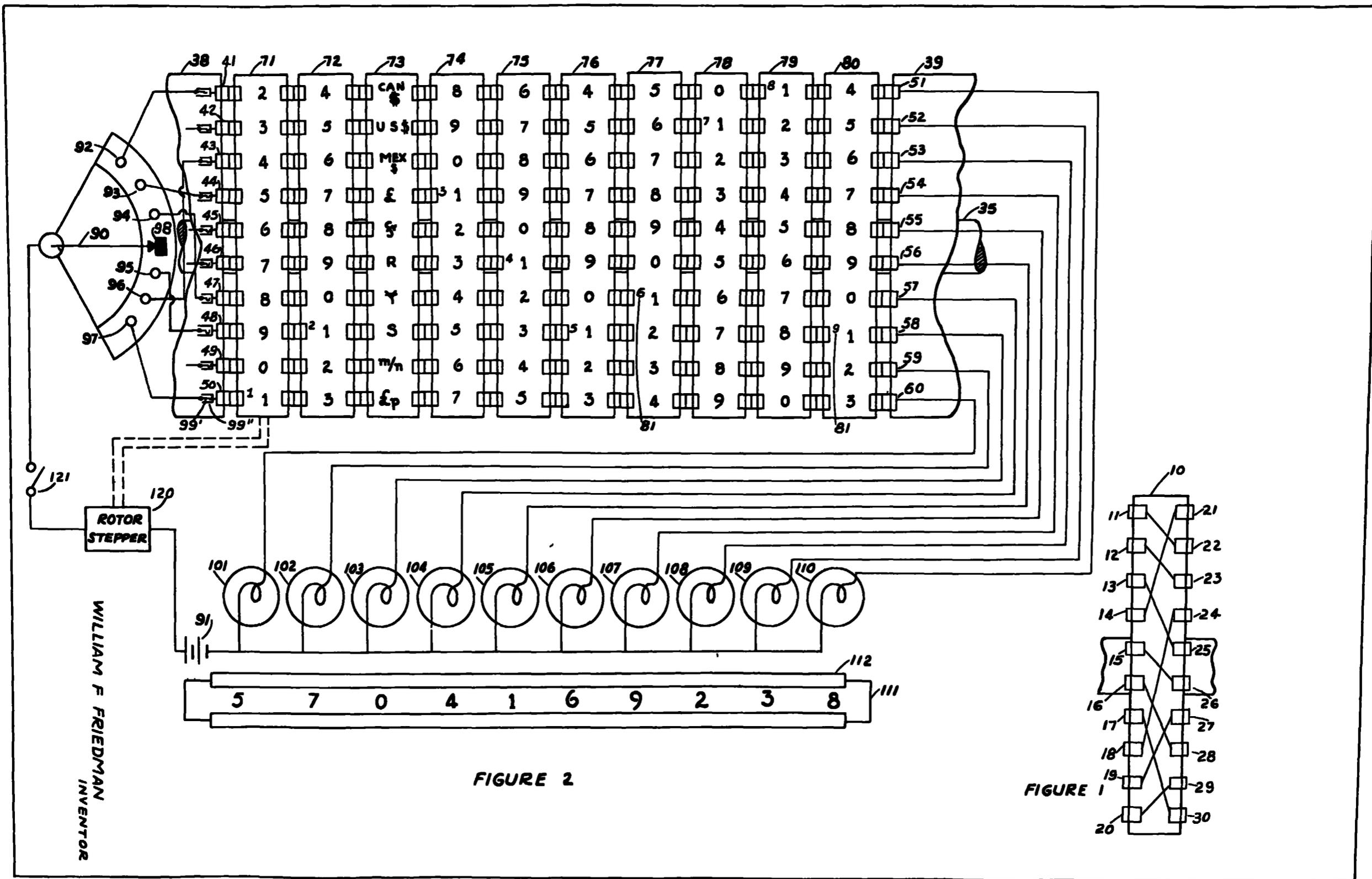
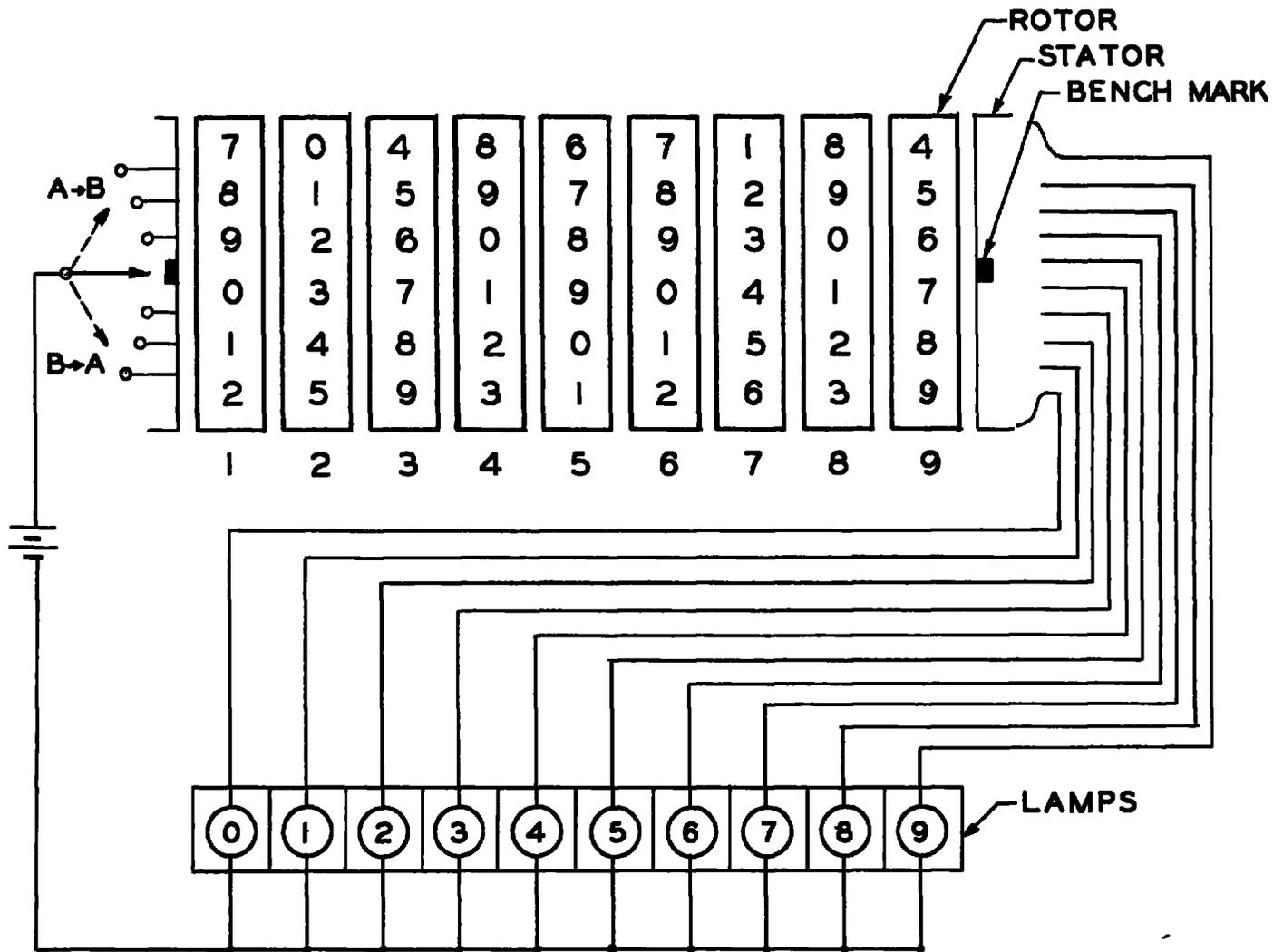


FIGURE 2

FIGURE 1

~~CONFIDENTIAL~~

Wm. Friedman



REF ID: A620
Belgian are the same as the ones shown here in.

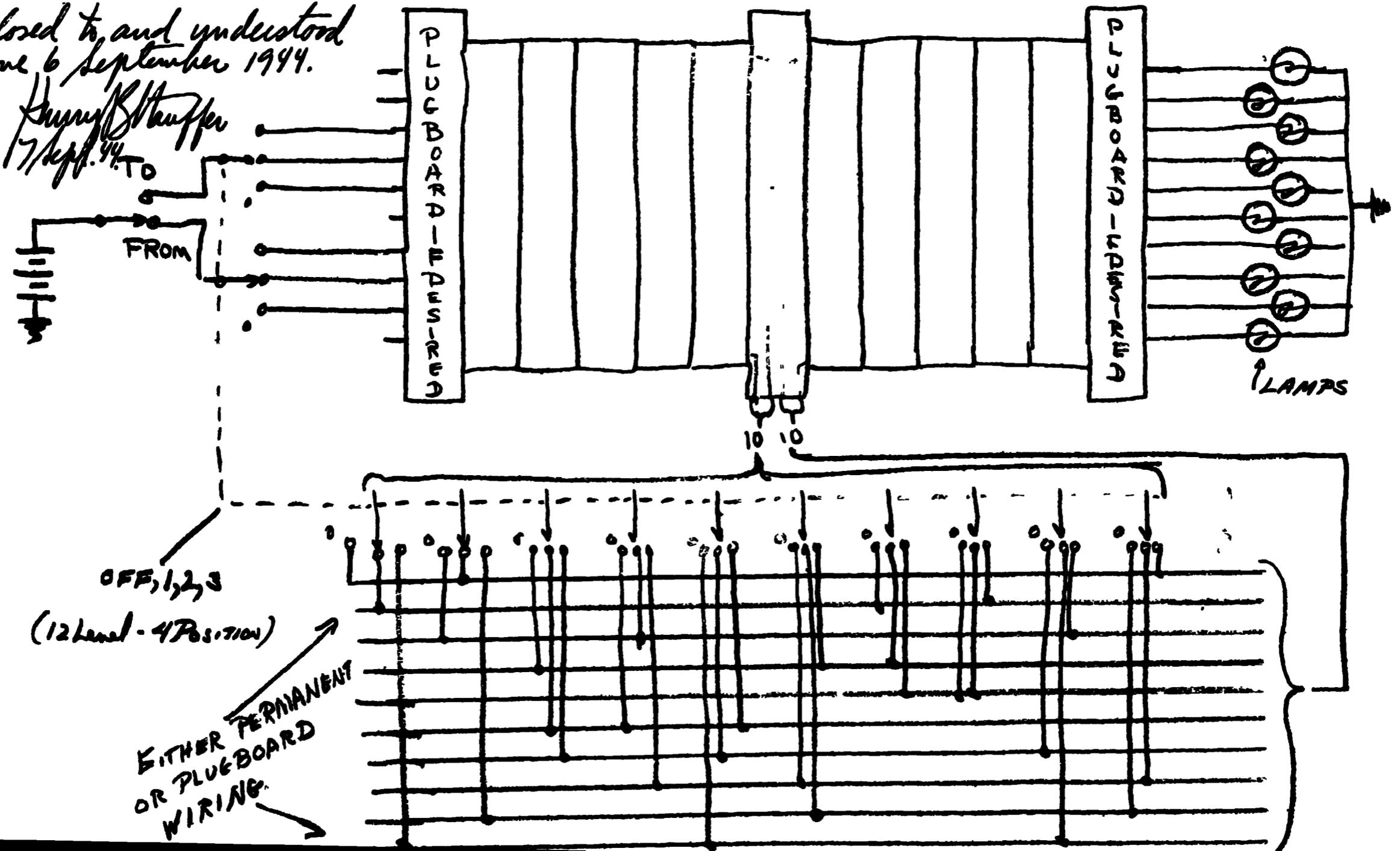
Les Toan William F. Friedman

5 September 1944. IMPROVEMENT IN AUTHENTICATOR DEVICE

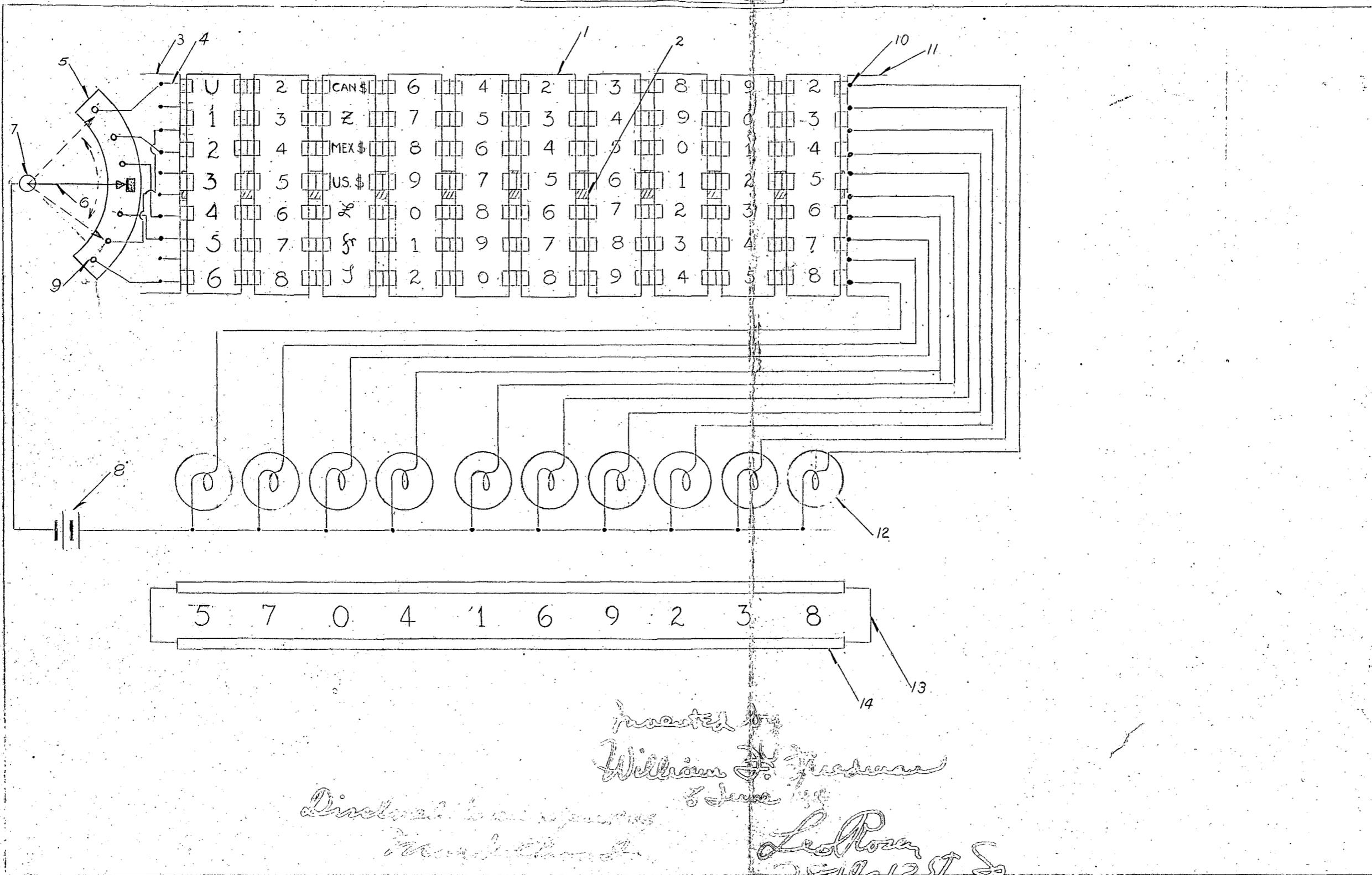
Disclosed to, and understood
by me 6 September 1944.

Henry Stuffer
17 Sept. 44

8538



~~CONFIDENTIAL~~



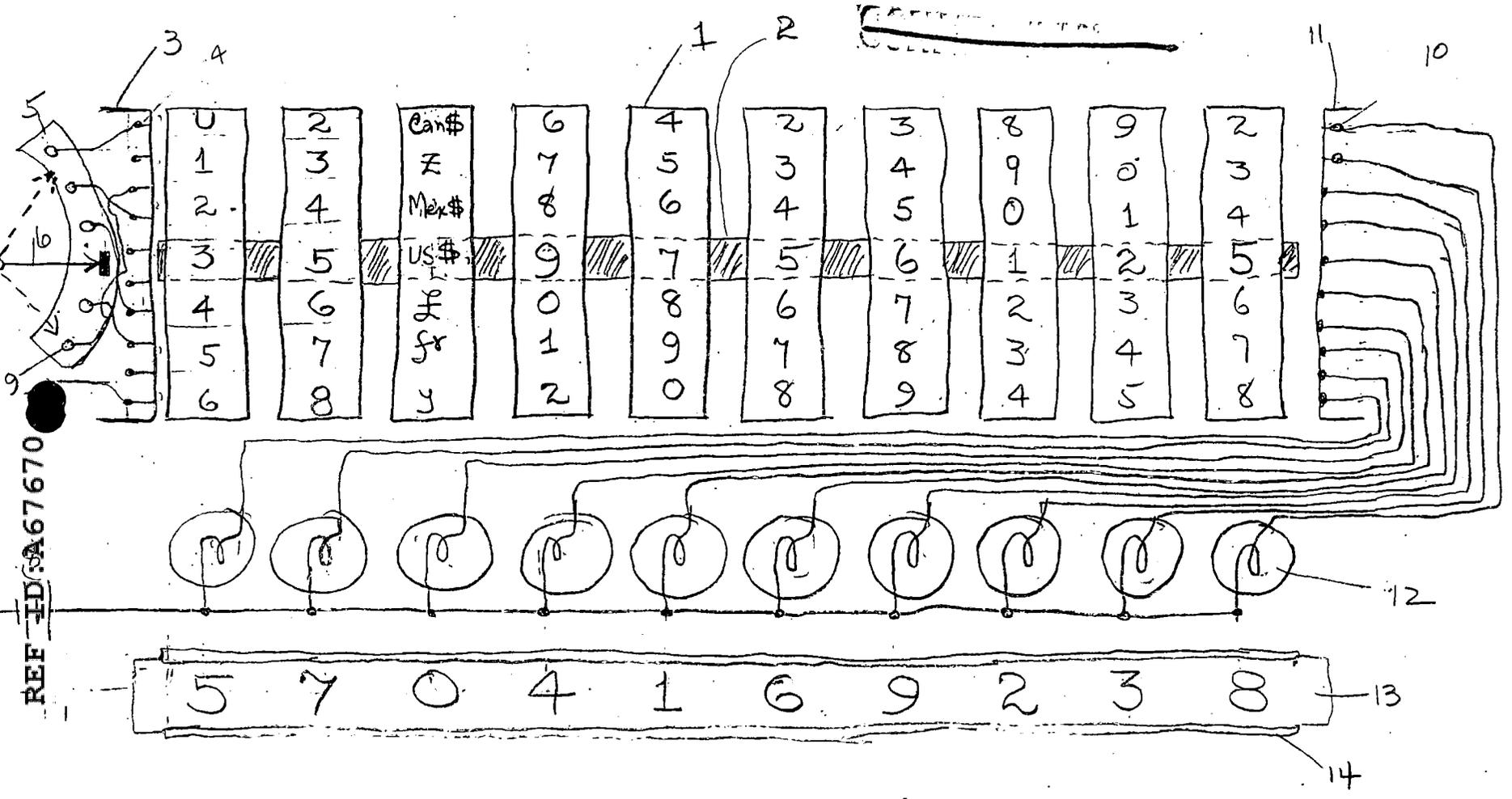
Invented by
William F. Friedman
8 June 1898

Directed by
Frank B. Rowland

Leo Power
279 1/2 St S
Charlottesville Va

~~CONFIDENTIAL~~

REF ID: A67670



Declassified by NSA/CSS

Deputy Associate Director for Policy and Records

On 2013/4/30 by RLP

COMPARISON TABLE

1	1	1	1	1	1	1	1	1	1
38	40	42	47	52	20	25	30	35	36 37
									35 36 37

[Faint, illegible text at the bottom of the page]