F. T. Leahy, Jr.
7 September, 1951
AFSA-343

CRYPTANALYTIC SURVEY OF NEW HAGELIN TELETYPE SCRAMBLER

OGA

INTRODUCTION:

The same cryptographic corporation that manufactures Hagelin* machines [redacted] a new machine designed to scramble teletype messages. This device has been examined from the viewpoint of the cryptanalyst with a view toward determining what steps should be followed by a cryptanalytic unit intercepting traffic.

DESCRIPTION OF DEVICE:

The "plain" output of a teletype is enciphered character by character by the addition of an ever-changing key in the standard manner, i.e. modulo 2 addition level by level. (It is assumed that the teletype has a standard 5-level, 32 character output.)

The everchanging key comes from a fixed reading station on some one of four 32-position rotating cylinders. Each of these cylinders, regardless of whether it has just been selected to supply the key or not, steps forward from 1 to 6 positions (independently) after each character is enciphered. Both the selection of the cylinder to be used, and the amount of the stepping to be effected, are brought about by six regularly stepping Hagelin pin-wheels. (These wheels are the same as in the M-209, hence of lengths 26, 25, 23 21, 19, 17.)

---

* The M-209

Three of the six wheels (the cryptographic clerk's key list will state which three) are used to select one of the four cylinders to furnish the key. These three wheels will, at each encipherment, furnish one of eight possible configurations of "dots and crosses" (active or inactive pegs). These eight are broken into 4 groups of two each, and one group assigned to each cylinder. Example:

1	2	3	4
.X.	XX.	...	..X
.XX	XXX	X..	X.X

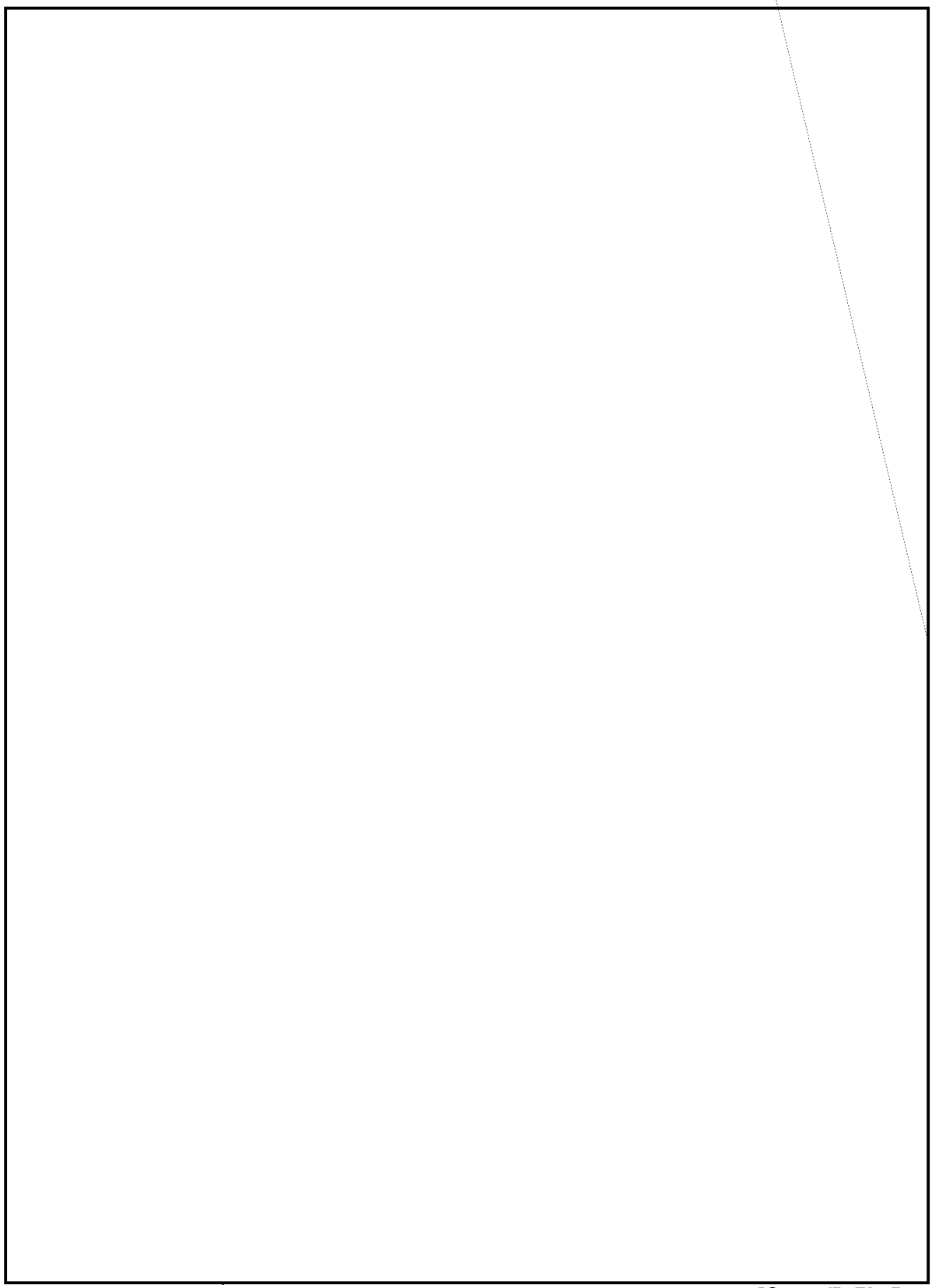
Note that for cylinder 1 and 2, the third wheel's status is immaterial; and for cylinder 3 and 4, the first wheel's status is similarly irrelevant.

Any of the six wheels, if active, will contact lugs on the cage, displacing bars to the left, (as in the present M-209). The displacement or lack of displacement of each bar determines which of the four cylinders (one or more) will be stepped one position by this bar. The cage has 24 slide bars, but as it makes only half a revolution (to save time) on each encipherment, only 12 are used per machine cycle.

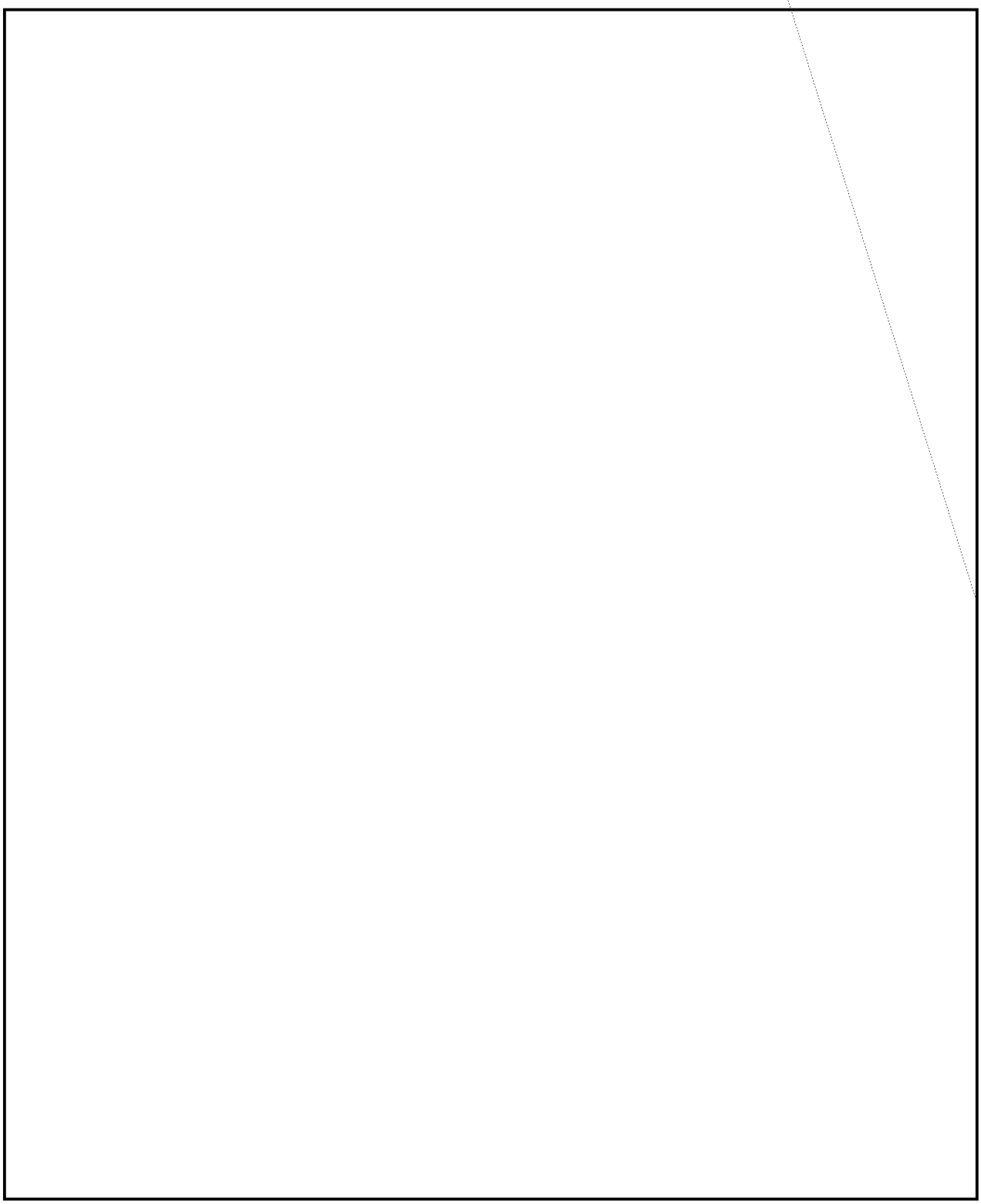
All 32 possible keys in some mixed order appear on the cylinders. The order can be changed as frequently as desired.

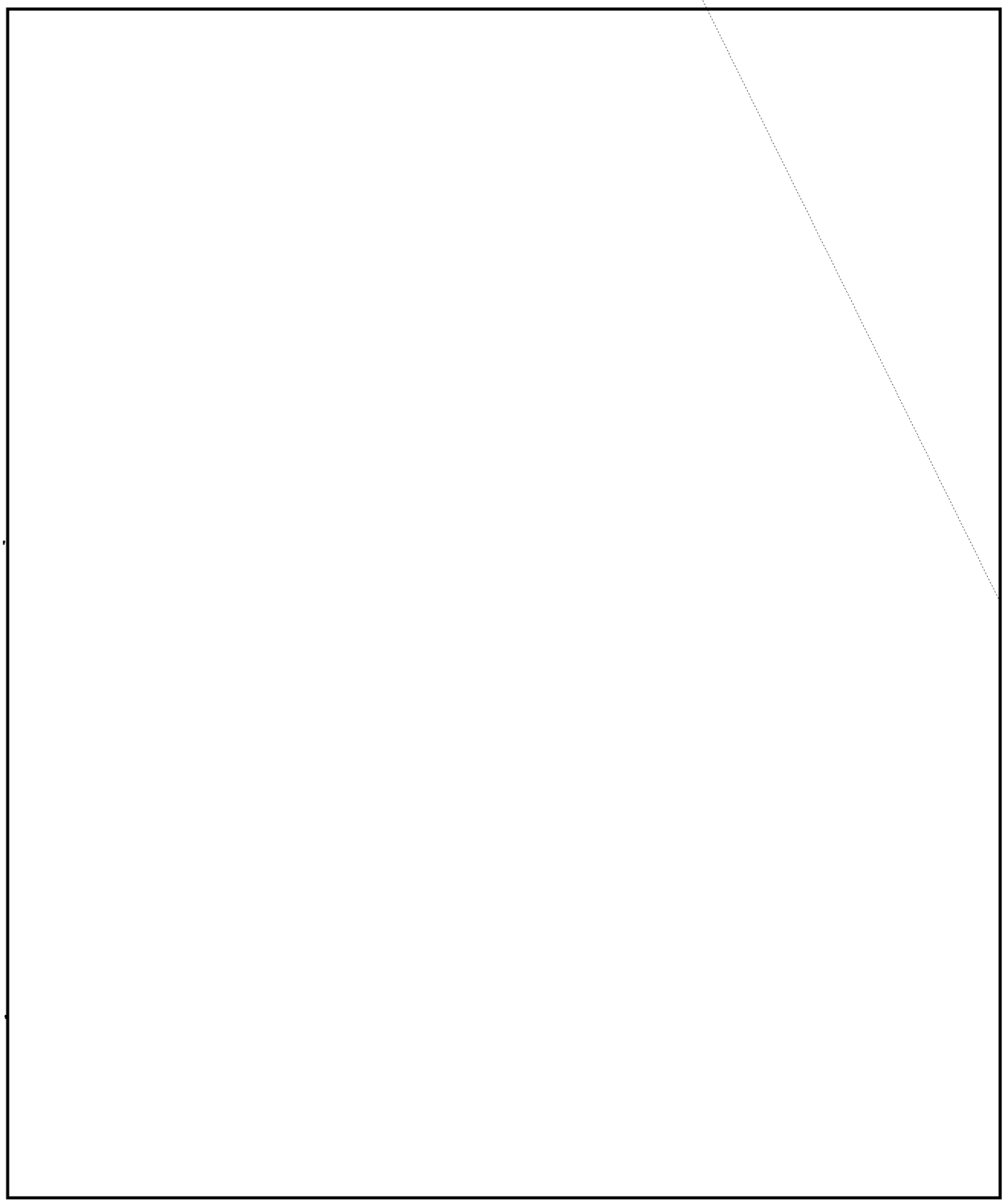
REF ID:A58884

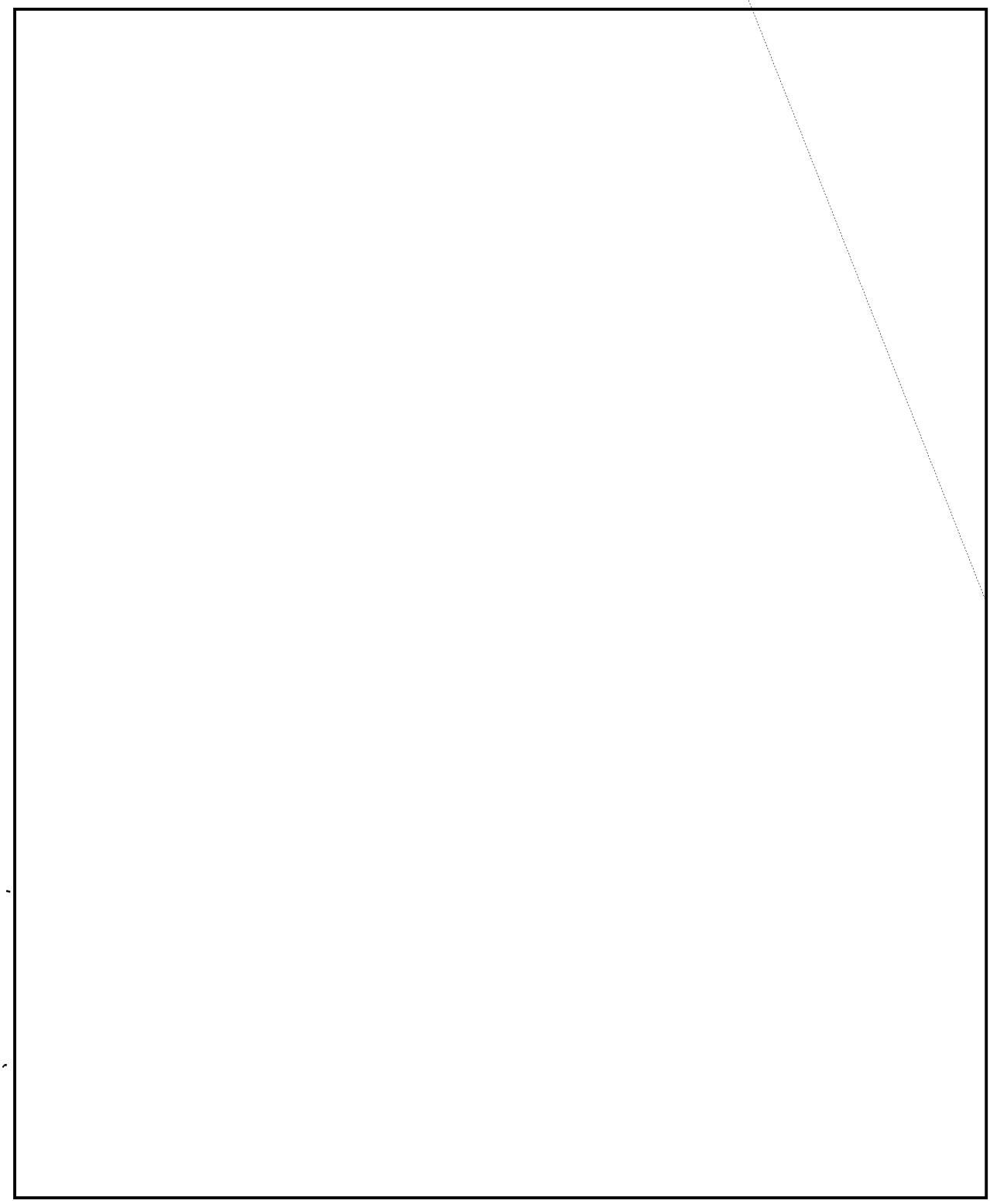
PRINCIPAL DIFFERENCE FROM OTHER SCRAMBLERS:



REF ID:A58884







REF ID:A58884

OGA

REF ID:A58884

OGA