

FORTEX

Fortex is a conical or triangular “stack of wheels.” Each row is a “wheel” that spins either clockwise or counterclockwise. A center column functions both for the calculation of a modular sum (to an arbitrary but fixed base) and as an “escalator” that increases the number of possible states the machine can be in. Symbols are taken by this vertically rotating central column to new rows.

Earlier versions of Fortex did not use a triangular shape. These earlier versions also lacked a perpendicular rotation (an escalator). On the other hand, something equivalent to the central column was in place. For instance, one can use the first element of each “row” as part of such a virtual column. Then the modular sum of this column can be added to the plaintext symbol.

In all systems, it’s important that the key evolve differently for different plaintexts. Typically the amount of rotation depends directly on the most recent plaintext symbol. This detail is not quite fixed yet, because the latest cipher symbol (which depends on latest plaintext symbol) can also be used.

Note that this system, just like the others, involves rounds of encoding and some version of “autospin.” The encryption function defines this complete process, and the number of rounds is almost always a fixed function of the size of the key (for simplicity and no deeper reason).

The Julia implementation is terser but nevertheless (or for that reason) easier to understand. This system is a bit more complicated than Thorium/Cesium and less complicated than Cone. Fortex and Cone look very much alike in graphical presentations, but Cone uses elementary cellular automata, so they are very different mathematically.