

**Cone** is a symmetric cryptosystem based on elementary cellular automata. The key for a Cone machine is an ECA rule. Ternary rules with a neighborhood of 3 require 27 ternary digits, for instance, for  $3^{27}$  possible keys.

Each symbol of plaintext is put at the center of this rule (replacing its central symbol). Then the CA is computed in a triangular fashion, in order to get the apex symbol, which is added mod  $b$  to the plaintext symbol to get the ciphertext symbol. Note that the key therefore serves not only as the rule but also as its own seed (excepting its middle symbol, which is replaced by the plaintext symbol.)

After each ciphertext symbol is computed, this bottom key/seed row is rotated  $p + 1$ , so that the evolution of the machine is a function of the individual plaintext.