

## The knapsack fuzzy chaos cryptosystem

AIP Conference Proceedings **2398**, 060035 (2022); <https://doi.org/10.1063/5.0093760>

[Bushra Hussien Aliwi<sup>a\)</sup>](#) and [Ruma Kareem K. Ajeena<sup>b\)</sup>](#)

### ABSTRACT

The fuzzy set theory is employed as an influential in mathematics by many researchers. The fuzzy models are used as a fundamental tool to solve several problems in cryptography. This work proposed alternative version of the fuzzy chaotic cryptosystem through employing the Knapsack problem and the chaotic map that uses the Takagi-Sugeno (TS) Fuzzy model. The resulted outputs of the TS Fuzzy chaotic model are used to create the secure ephemeral key. A primitive variable is chosen to add the nonlinearity feature to the chaotic system. The orbit of the points is determined based on the fuzzy chaos system that is unpredictable through the randomly choice of the initial values. On the proposed Knapsack fuzzy chaotic (KFC) cryptosystem, the keys are generated, the masked ciphertext are computed based on the super-increasing sequence which is combined with a secure ephemeral key. One of several experimental results is implemented using the Lorenz map that has a chaotic behavior with two scrolled points. The security considerations of the proposed KFC cryptosystem are determined.