**Security Evaluation of Cryptosystems based on Soft Computing Techniques**

Prof. Sattar B. Sadkhan *SMIEEE* – University of Babylon-IT College- IRAQ.

drengsattar@ieee.org

With advancements in networks, cryptographic technology has become a fundamental technology that sustains the foundations of modern society. It is fair to say that safe and secure communications, business, and transportation are now unthinkable without cryptographic technology (CT). However, CT commonly used in today’s society does not maintain permanent security; even once security is confirmed, advancements in cryptanalysis may bring about rapid security deterioration. Many Researchers are conducting continuous research on security evaluation of cryptographic technology taking into consideration the improvement of ever-advancing cryptanalysis/computing capabilities. The security of a cryptographic algorithm is defined as a number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm with the most efficient algorithm. When evaluating cryptographic security, one should find the most efficient attack algorithm and, with that method, it is estimated how much work should be necessary for the attack.

Soft computing (SC) is an emerging approach to computing which parallels the remarkable ability of the human mind to reason and learn in an environment of certainty and imprecision. SC consists of several computing paradigms, including fuzzy set theory , neural networks, , approximate reasoning , combinatorial optimization methods( such as genetic algorithms). This Talk will introduce the progress in the researches related to security evaluation of cryptosystems based on using different SC techniques.