4th International Conference on

Atomic and Nuclear Physics

October 26-27, 2018 | Boston, USA

Encryption algorithms based on bio molecular information

Mohamed Hamdi
University of Carthage, Tunisia

Nowadays, most of the applications using on the Internet are based on the idea that smart sensors can be embedded on a wide variety of objects and devices. New communication schemes are being deployed between these devices so as to develop pervasive computing and ambient intelligence contexts. Due to the security risks that are associated to these communication channels, new protection techniques are being investigated to cover the specific requirements of the future Internet. Cryptosystems based on molecular biology are among the most promising techniques to implement security policies on a large amount of data. This talk provides a review of the recent advances that have been made in the context of encryption using molecular biology information. These information have interesting properties including high-storage capacity, rapid parallelism, and energy-efficiency. One of the most important problems in this field is the Hamiltonian Path Problem which consists in determining the shortest path traversing each node of a directed graph exactly once and returning to the last node. The DNA molecule - as a carrier of data - has a large capacity. One trillion bits of binary data can be stored in one cubic decimeter of a DNA solution. DNA cryptography is built on DNA - which is an information carrier - and modern biotechnology for its tools, and it achieves the encryption process by the use of the characteristics of DNA of massive parallelism and high storage density. In addition, the reason why we can combine cryptography and molecular biology is the encoded plaintext, which can combine the computer and the use of molecular biological techniques, such as polymerase chain reactions, polymerization overlapping amplification, affinity chromatography, cloning, mutagenesis, molecular purification, electrophoresis, magnetic bead separation and other techniques of molecular biology, and then obtain the final cipher text. Most importantly, DNA code abandons that traditional cryptography which uses the intractable mathematical problem of the security guarantee, instead using the limited nature of the learning of biology.

mmh@supcom.tn