Chapter 56
Information Security-Based Nano- and Bio-Cryptography

W. K. Hamoudi
University of Technology, Iraq

Nadia M. G. Al-Saidi
University of Technology, Iraq

ABSTRACT

Information security can provide confidentiality, integrity, and availability for society to benefit efficiently from data storage and open networks. Free space communication networks suffer from adversaries who interfere with data on networked computers. Inventing new protection techniques has arisen to ensure integrity and authenticity of digital information. This chapter introduces Nano and Bio techniques in cryptography to enhance the information security systems. Tasks unfeasible on a classical computer can now be performed by quantum computers, yielding a big impact on online security. Threats of exponentially fast quantum algorithms on business transactions could be overcome by this new technology. Based on biological observations, the exploration of biometric cryptography and authentication to determine individuals' authenticity can be done through numeric measurements. This provides very reliable automated verification and strong protection against biometric system attacks.

INTRODUCTION

There is an increasing need for a multidisciplinary, the system-oriented approach to manufacturing Micro/Nano-devices that function reliably (Bharat, 2007). This can be achieved through the intermixing of ideas from different disciplines and the systematic flow of information (Ahmad, Amri, Zuriati & Elissa, 2009). Cryptography is the science of protecting the privacy of information during communication under hostile conditions. With this information era that is full of various information and knowledge, and the increasing use of digital devices, many applications such as, electronic mail, electronic fund transfer, classified files, etc., are easily transmitted and suitable for communicating over the insecure communication channels. However, the security and authentication is still a challenging problem, and there

DOI: 10.4018/978-1-5225-3158-6.ch056

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

is always a growing demand of cryptographic techniques, which has spurred a great deal of intensive research activities in the study of cryptography (Ganesan, Ishan, & Mansi 2008).

Quantum key distribution (QKD) is a very advanced encryption method of Quantum Cryptography (QC) for distributing a secret key. It allows the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of quantum physics. QKD can be used in conjunction with existing network services for businesses communication services when a higher degree of confidentiality and protection are needed. Practical realization of QKD technology relies on availability of systems providing production, propagation, and detection of single photons. Single photon sources based on; Nano quantum dots, carbon nanotubes and diamond nanowires have enabled the development and recent demonstration of a number of commercial products.

Bio-cryptography is an emerging multidiscipline technology which combines biometrics with cryptography. It inherits the advantages of both and provides strong means to protect against biometric system attacks. Biometric is the science or technology which analyzes and measure the biological data. It is first used for recognition and identification, while it is used now for automatic identification and authentication. The characteristic features of the individual's is stored in a database using input devices, which then compared with the features extracted from the traits of the individual need to be identified. This type of schemes provides an essential security requirement. The biometric data have many advantages over traditional systems, they cannot be guessed, forgotten, stolen or lost. There is nothing to remember or carry, and are more users friendly, where their efficiency makes it easily to be applied alone or hybrid with other security and authentication methods (Al-Saidi, Said & Othman, 2012). Authentication is the first step of information security. It refers to the process used to identify and confirm the validity of the user. It is a mechanism used to authenticate user identity over insecure communication network. Traditional alphanumeric passwords are widely used for authentication. They have memorability problem for secure passwords and their security is based on the password only. It is always threatened due to the availability of simple, rapid and perfect duplication and distribution means using simple dictionary attacks.

The material of this chapter is arranged into 6 sections, and as follows:

1. Introduction
2. Nano and bio-assemblies.
3. Cryptography and Information security.
4. Nano-technology applications in information systems.
5. Quantum dots in cryptography.
6. Authentication based on Nano and Biometric techniques.
7. Nano and Bio in cryptanalysis (from Bio to Nano: how to defeat attacks).
8. Conclusion.

NANO AND BIO-ASSEMBLIES

Nanotechnology is a multidisciplinary use of materials and processes that refer to the control, manipulation, and applications of Nano-scale devices. Materials in a scale below 100 nm have different characteristics from their bulk counterpart; then new size and shape properties appear; see Figure 1. Nanotechnology has proved its success in consumer products, chemistry, environmental science, security, mathematics, medicine, physics, and many other fields. Manipulating molecules and atoms directly was suggested by

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/information-security-based-nano--and-bio-cryptography/186729

Related Content

Automated Screening of Fetal Heart Chambers from 2-D Ultrasound Cine-Loop Sequences
N. Sriraam, S.Vijayalakshmiand S.Suresh (2012). *International Journal of Biomedical and Clinical Engineering (pp. 24-33).*
www.irma-international.org/article/automated-screening-of-fetal-heart-chambers-from-2-d-ultrasound-cine-loop-sequences/86049

Feature Evaluation and Classification for Content-Based Medical Image Retrieval System
Ivica Dimitrovskiand Suzana Loskovska (2010). *Ubiquitous Health and Medical Informatics: The Ubiquity 2.0 Trend and Beyond (pp. 509-531).*
www.irma-international.org/chapter/feature-evaluation-classification-content-based/42948

Ontology-Based Spelling Correction for Searching Medical Information
Jane Moon (2009). *Medical Informatics: Concepts, Methodologies, Tools, and Applications (pp. 2244-2258).*
www.irma-international.org/chapter/ontology-based-spelling-correction-searching/26370

Gait Event Detection System for the Control of Lower Limb Exoskeleton: Review and Future Requirements
Mohanavelu Kalathe, Sakshi Agarwal, Vinutha Sampaathand Jayanth Daniel (2021). *International Journal of Biomedical and Clinical Engineering (pp. 14-28).*
www.irma-international.org/article/gait-event-detection-system-for-the-control-of-lower-limb-exoskeleton/282492

Basic Principles and Benefits of Various Classification Systems in Health
Dimitra Petroudiand Athanasios Zekios (2006). *Handbook of Research on Informatics in Healthcare and Biomedicine (pp. 51-58).*
www.irma-international.org/chapter/basic-principles-benefits-various-classification/20562