Innovative cryptographic approaches to computer systems security

OGIELA, Urszula

(出版者 / Publisher)
法政大学大学院理工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学・工学研究科編
(巻 / Volume)
60
(発行年 / Year)
2019-03-31

様式3

論 文 要 旨

理工学 研究科 システム理工学 専攻

創生科学 プログラム ○系 コース 領域

氏 名 Urszula Ogiela Urszula Ogiela 印

論文題目 Innovative cryptographic approaches to computer systems security

論文の要旨

Advanced information security aspects concern to protection and encryption of secure, strategic and important information. These scientific problems and practical solutions are rooted in cryptography, which uses algorithms and protocols for ensuring information confidentiality, and information division techniques, as well methods of reconstructing information.

Innovative approaches, which allow to guarantee information security, focus around data splitting and sharing techniques, as well as its reconstruction. These algorithms are dedicated to information sharing are called threshold schemes.

The main idea discussed in this thesis is to propose such techniques, which allow to create new models of systems security, dedicated to management of shared strategic information. Special emphasis is put on multi-level threshold schemes. What characterizes such a split is the possibility of reconstructing information from sets containing various numbers of shares obtained from divided secret information. This problem has not been fully elaborated yet but seems extremely important from the perspective of the future development of modern systems security.

Hence, in this thesis, the author would like to discuss the development of threshold schemes for information sharing and will demonstrate the ability and the reason for using them to manage secret information in different structures and at different levels. These algorithms are proposed by Author of this dissertation and after theoretical evaluation, will be describe step by step.

The author would like to propose the new methods of information splitting based on new threshold schemes used for secure/strategic/important information division using mathematical linguistic formalisms. Such procedures are described as linguistic threshold schemes. Mathematical linguistic techniques can be used in information splitting procedures and for developing new algorithms for securing data using these techniques. Also, the second class of threshold schemes called biometric threshold

論 文 要 旨

schemes are proposed. Such schemes can use selected personal, or individual data for marking secret parts, splitting secret information and to restore original data.

The basis of proposed innovative approaches to cyber systems security are the new protocols which use of both the linguistic and biometric threshold schemes. Those types of protocols create new secure computing methods oriented on linguistic and biometric (human) aspects of information security processes. The main solution of proposed algorithms is creation of new generation of computer and cyber systems by application of new classes of security protocols described in this thesis.

In addition, an attempt to define new methods that could extend current knowledge and practical solutions, and can contribute to improve decision-making processes, by acquisition, storage and retrieval of secret information in different organizations and knowledge levels.

The interdisciplinary nature of proposed solutions creat the subject of security systems forming part of cryptography and informatics as a new challenge for the research and application work carried out.