Secure Distribution Protocol for Restoring Information with Different Accesing Grants

Lidia Ogiela*, Marek R. Ogiela, and Urszula Ogiela
AGH University of Science and Technology
Al. Mickiewicza 30, PL-30-059 Krakow, Poland
{logiela, mogiela, ogiela}@agh.edu.pl

Abstract

In the paper will be presented some advances in procedures used for encryption and division of secret data, as well as modern approaches for management of splitted information. Computer techniques for secret information sharing aim to secure information against disclosure to unauthorized persons. The paper will describe algorithms allowing for information sharing and secret parts distribution with regards to the different accessing grants for particular persons. Presented protocol allows to prevent insider treats and information leakage, while performing secret part distribution, and information restoration.

Keywords: Cryptographic Protocols; Secret Sharing Algorithms; Information Distribution and Management

1 Introduction

Data security, information safety and authorisation have been a subject of research of cryptography, mathematics and informatics, which tries to restrict access to various kinds of data [2, 3, 7]. The diversity of this information was not only due to the contents of the different data sets [4, 5, 6], but also the others features of these sets:

- size of the data sets;
- the form under which data was concealed:
  - numerical sets,
  - visual images,
  - signals and sounds;
  - biometrics, etc.

The main idea of cryptography was the data concealing and authorized. These processes were thus to guard access to data in the best possible way so that these data sets would not be send, transferred, disclosed or used by individuals not authorised to do so. These situation implied creation and use a new solution in those scientific field started promoting where methods of concealing of the data sets: coding it, encrypting it, guarding access to information/data.

Every new solution in cryptography was presented as algorithmically and computationally secure, but only to the time when a new solution were created. For example of algorithms based on the use of cryptographic keys dedicated for encrypting or decrypting processes, security consisted in ensuring that

Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 2 (January 15, 2015)

[*] Corresponding author: AGH University of Science and Technology, Al. Mickiewicza 30, PL-30-059 Krakow, Poland

the key could not be broken and the key could not be taken over by a unauthorized person.
If the cryptographic keys used in cryptographic protocols were taken over, the entire information could be disclosed. Thus a search a new, the better and more secure solutions started. A new solution was data splitting and sharing algorithms and protocols were included in the group of algorithms protecting information sets from disclosure.
Data splitting and sharing algorithms are based on coding data sets into a binary form and then splitting these coded data sets among a selected group of individuals each of whom receives a share of the split parts of secret data. In order to reconstruction the data secret, all parts of the secret must be combined and the information decoded.
Information splitting algorithms require all parts of the secret owners to put together their shares to reproduce the divided information/data. This cryptographic protocol creates a risk, because losing even one share of the secret part will make it impossible to divide the split data. The same situation is if even a single part of the secret trustee objects to reproducing the dividing data sets.

2 Secure Distribution Protocols for Information Management

Cryptographic algorithms of data splitting and sharing divide information between a group of secret trustees. These groups were selected at the processes of definition of the algorithms. In these algorithms, a trustee of secret holds one of n shares of the divided secret data into which secret information I has been divided. The stage of dividing secret information and distributing it among process participants is thus the same in both secret splitting and sharing algorithms.
Secret information I is divided between n process trustee of secret. Every participant of those algorithms receives one of n shares of the divided secret information. Every part of secret information alone is useless. Thus disclosing a single part of the divided secret information poses no threat to the security of the entire secret information I. Trustees of the part of secret information store theirs parts of the global information I until it becomes necessary to reproduce and disclose it. This process differs for information splitting and sharing protocols.
Data splitting protocols require combining all n shares of the split secret information to reproduce this secret data. If shares combined are less then n, the secret information I will not be reproduced.
Information sharing protocols require combining a certain parts of secret information $m < n$ to reproduce secret information I. Thus it's necessary to combine only selected parts of secret shares (m) to reproduce the secret information I. The number of m required to reproduce secret I depends on which one data sharing scheme is chosen. Those solutions are known as (m, n)-threshold schemes [1, 8, 10], where:

- n – the number of shares into which secret information I will be divided,
- m – the number of shares absolutely required to reproduce secret I.

The operating principles of the information splitting (Fig. 1) and sharing (Fig. 2) algorithms are presented below.

To reproduce information, splitting algorithms require that all shares of the split secret be combined, while data sharing algorithms only require a selected number of them. From the point of view of information management, data sharing algorithms are more convenient for efficient management [9, 11]. They make it possible to reproduce the information without all trustees of the secret having to participate. Even if some secret trustees are excluded, the shared message can still be reproduced, which would be impossible in a data splitting algorithm. If a selected share of the secret is accidentally or intentionally obtained in data splitting algorithms and thus poses the threat that the secret information will be revealed to unauthorised individuals, there is the danger that the information may be revealed in an uncertain

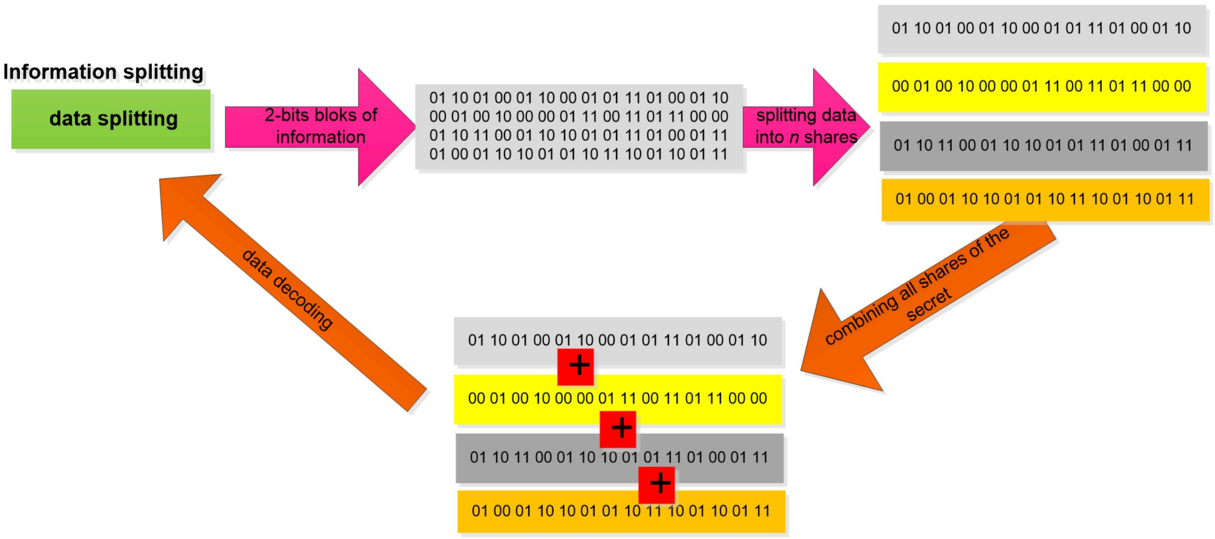

Figure 1: Information splitting algorithm.

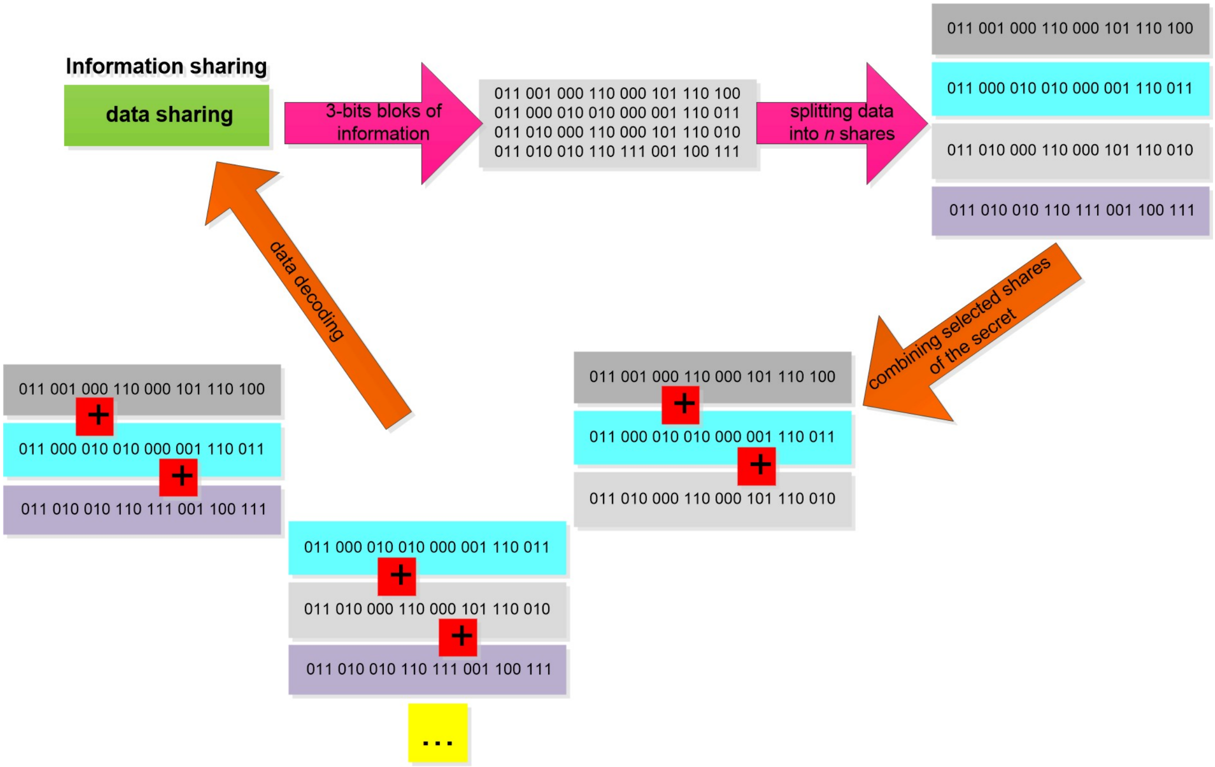

Figure 2: Information sharing algorithm.

situation. In the case of information sharing algorithms, it is possible to exclude a suspected or just unreliable person whose loyalty is in any doubt. Cryptographic protocols on secure data sets the basic data sharing procedures include one of the cryptographic algorithms, for example [10, 12, 13]:

- Shamir's algorithm;

- Tang's algorithm;
- Lagrange's interpolation polynomial algorithm.

3 Managing Secret Shared Strategic Data in Hierarchical and Layered Structures

Managing strategic data is usually equated with important data being managed by persons authorised to access it while ensuring complete security of this data. Strategic data, as a type of secret data, is not disclosed to broad groups of recipients. They are only known to small groups of individuals and their complete confidentiality is reserved. Thus, in managing this type of data, there is always the danger that someone could get hold of this data and disclose it to unauthorised individuals. Data sharing protocols are an effective protection against someone obtaining this data.

The method by which data sharing algorithms work is associated with the operation of (m, n)-threshold schemes which split data sets into n equal shares, of which any m, once combined, allow the shared secret to be reproduced.

The divided secret may have any content, so it is better to share strategic data. Strategic data may comprise economic figures, i.e. the financials of the company, organisation action strategy, intelligence data, design or logistical information.

Economic and financial data stored in the numerical form, which is very easy for unauthorised individuals to steal, has been selected for this analysis. This type of data is known to selected groups of people in individual enterprises, so an efficient process for managing this data has a direct impact on the correct operation and growth of the enterprise. Thus ensuring the security of systems for managing company financial data is the most important job in processes of strategic information management within an enterprise.

The method of dividing data within a selected group of trustees of strategic data depends on the structure of the organisation, enterprise or institution to which it is dedicated [14]. A hierarchical and a layered division are distinguished the most often [11].

The hierarchical division of strategic data is possible in structures which have this nature. The hierarchical nature of the structure within which information is divided can thus be a driver of the method of data sharing (Fig. 3).

In a hierarchical structure, information is shared independently at each hierarchical level, while the shared secret is reproduced by the trustees of the shares of divided information from a higher level.

Figure 3 shows information division at three different layers of the organisation. In the highest layer of general management, a single person can reproduce the information. In contrast, in lower layers, the shared secret is reproduced by two out of four protocol participants. This is thus an example of the operation of a (2, 4)-threshold scheme.

The same method of sharing data applies in layered information sharing (Fig. 4).

The method of data reproduction forms a significant difference between information sharing within a hierarchical and a layered structure. In a layered structure, the secret is shared within individual layers in an independent way. Thus, within each layer, data is share independently of any other layer, while the shared information can be reproduced by combining the selected number of secret shares.

Figure 4 shows how, in the superior layer, the information can be individually reproduced by company management. Within the subordinate layer, a (2, 4)-threshold sharing scheme is presented, whereas in the lowest layer, a (3, 5)-threshold sharing is shown. In each layer, the method of operation is similar.

It's also data decoding in interpenetrating structure. If part of the secret data is impossible to obtain, than it's possible to data decoding by the participants of the different level (in hierarchical structure) or layer

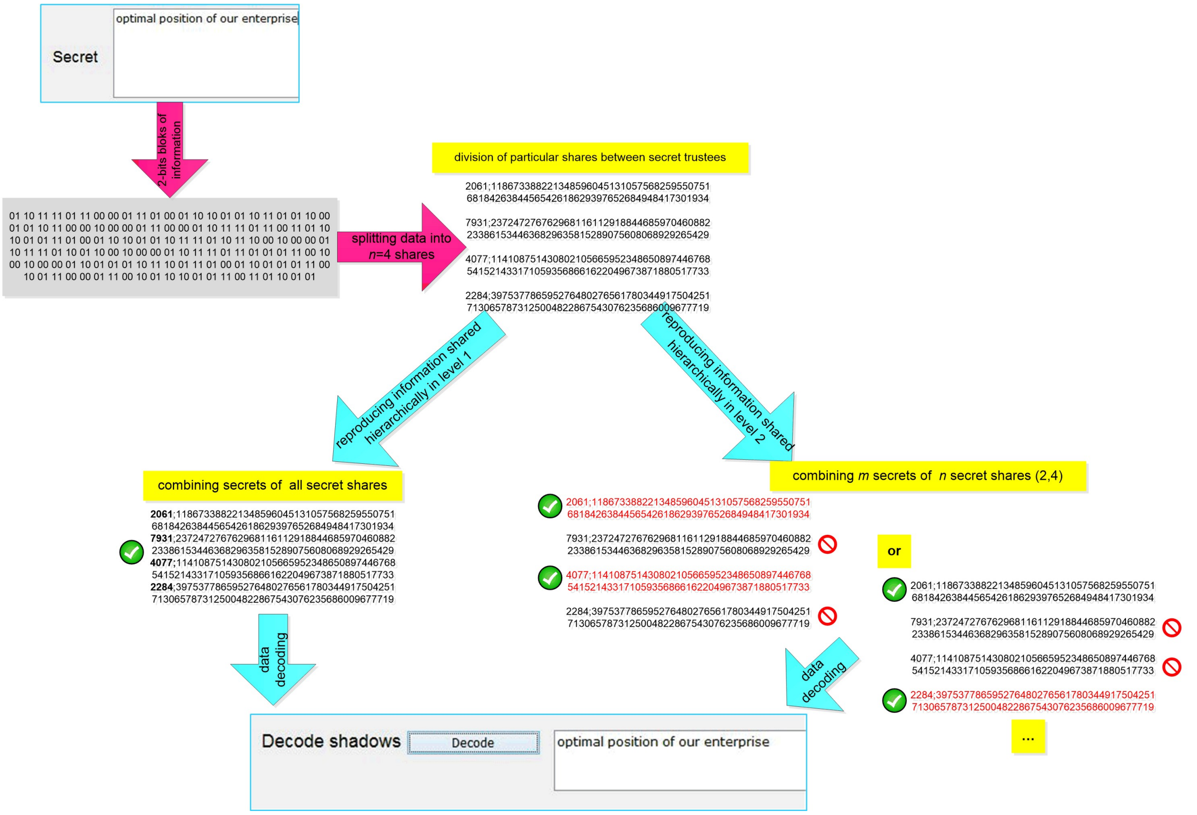

Figure 3: Information sharing in hierarchical structure.

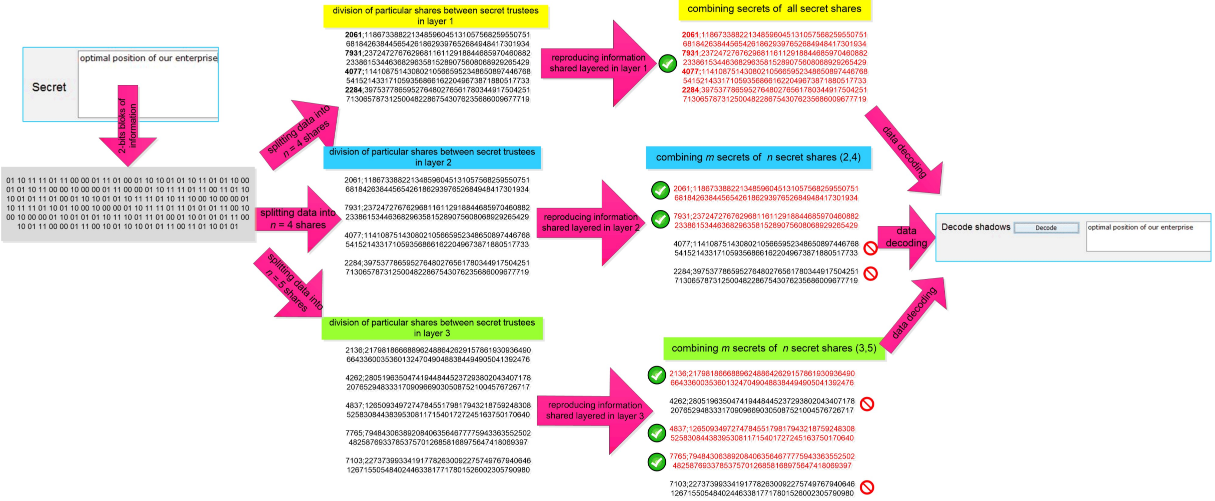
Secret
optimal position of our enterprise
2-bits bloks of information
splitting data into n = 4 shares
splitting data into n = 4 shares
splitting data into n = 5 shares
division of particular shares between secret trustees in layer 1
division of particular shares between secret trustees in layer 2
division of particular shares between secret trustees in layer 3
2136;217981866688962488642629157861930936490 6643360035360132470490488384494905041392476
4262;280519635047419448445237293802043407178 2076529483331709096690305087521004576726717
4837;126509349727478455179817943218759248308 5258308443839530811715401727245163750170640
7765;794843063892084063564677775943363552502 482587693378537570126858168975647418069397
7103;227373993341917782630092275749767940646 1267155054840244633817717801526002305790980
reproducing information shared layered in layer 1
reproducing information shared layered in layer 2
reproducing information shared layered in layer 3
combining secrets of all secret shares
combining m secrets of n secret shares (2,4)
combining m secrets of n secret shares (3,5)
data decoding
data decoding
data decoding
Decode shadows
Decode
optimal position of our enterprise

Figure 4: Information sharing in layered structure.

(in layered structure). This situation presents fig. 5.

The secret information is coded into a binary form in order to protect the contents of data that will be shared. Then, the coded information is divided between protocol participants within different layers according to the selected (m, n)-threshold scheme. In order to reproduce the information, it is necessary to combine m selected secret shares (bearing in mind that m takes different values in different layers).

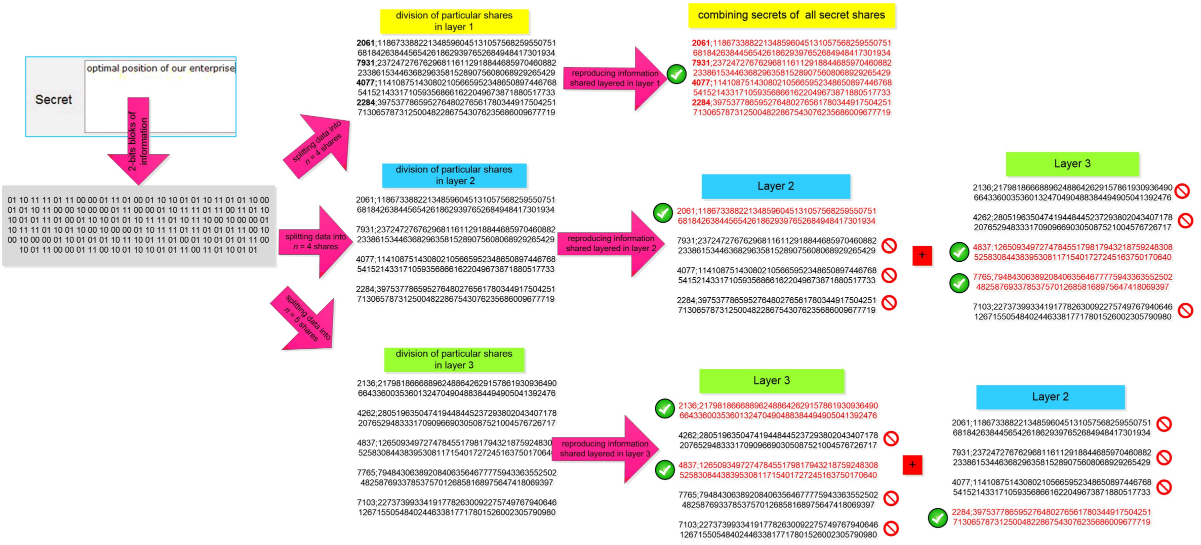

Figure 5: Information sharing in interpenetrating layered structure.

Then, the combined information can be read after it has been decoded. Hence, secret data is protected in the process of information sharing by the following means:

- the process of coding data into a binary form;
- the secret division between trusted trustees (by using the selected algorithms);
- the complete uselessness of a single obtained share of the secret;
- the ability to eliminate an unwanted secret shareholder.

4 Conclusion

Secure distribution protocols used for restoring secret information may use different accessing grants. The main access of these protocols and algorithms are managing strategic enterprise data. This solution implies that the complete confidentiality and security of the data stored, analysed and transferred must be ensured. Such processes are supported by the use of algorithms for data splitting and sharing, which ensure that secret data sets is already secure at the stage of the preliminary strategic information division process. In secret sharing processes we use (m, n)-threshold schemes for sharing secret information ensures the security of the divided secret and its distribution between individual trustees of the secret. That solution significantly improves processes of secret data management.

Dividing secret information between appointed trustees of individual shares of the secret makes it possible to manage data sets in a secure way, enabling this secret to be stored and sent without the risk that the loss of one share would cause the entire secret data to be declassified.

Acknowledgments

This work has been supported by the National Science Centre, Republic of Poland, under project number DEC-2013/09/B/HS4/00501.

References

[1] A. Beime and B. Chor. Universally ideal secret sharing schemes. *IEEE Transactions on Information Theory*, 40:786–794, 1994.

[2] S. Bodzioch and M. Ogiela. New approach to gallbladder ultrasonic images analysis and lesions recognition. *Computerized Medical Imaging and Graphics*, 33(2):154–170, 2009.

[3] T. Hachaj and M. Ogiela. A system for detecting and describing pathological changes using dynamic perfusion computer tomography brain maps. *Computers in Biology and Medicine*, 41(6):402–410, 2011.

[4] L. Ogiela. Syntactic approach to cognitive interpretation of medical patterns. In *Caihua Xiong at all (Eds.). Intelligent Robotics and Applications*, pages 456–462. Berlin Heidelberg Springer-Verlag, 2008.

[5] L. Ogiela. Cognitive informatics in automatic pattern understanding and cognitive information systems. In *Y. Wang, D. Zhang, W. Kinsner (Eds.). Advances in Cognitive Informatics and Cognitive Computing, Studies in Computational Intelligence Vol. 323*, page 209–226. Berlin Heidelberg Springer-Verlag, 2010.

[6] L. Ogiela. Cognitive informatics in image semantics description, identification and automatic pattern understanding. *Neurocomputing*, 122:58–69, 2013.

[7] L. Ogiela. Semantic analysis and biological modeling in selected classes of cognitive information systems. *Mathematical and Computer Modelling*, 58:1405–1414, 2013.

[8] M. Ogiela and U. Ogiela. The use of mathematical linguistic methods in creating secret sharing threshold algorithms. *Computers & Mathematics with Applications*, 60(2):267–271, 2010.

[9] M. Ogiela and U. Ogiela. Dna-like linguistic secret sharing for strategic information systems. *International Journal of Information Management*, 32(2):175–181, 2012.

[10] M. Ogiela and U. Ogiela. Linguistic protocols for secure information management and sharing. *Computers & Mathematics with Applications*, 63(2):564–572, 2012.

[11] M. R. Ogiela and U. Ogiela. *Secure Information Management using Linguistic Threshold Approach. Advanced Information and Knowledge Processing*. Springer-Verlag, London, 2014.

[12] A. Shamir. How to share a secret. *Communications of the ACM*, page 612–613, 1979.

[13] S. Tang. Simple secret sharing and threshold rsa signature schemes. *Journal of Information and Computational Science*, 1:259–262, 2004.

[14] M. van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6:143–169, 1995.

Author Biography

Lidia Ogiela Computer scientist, mathematician, economist. She received Master of Science in mathematics from the Pedagogical University in Krakow, and Master of Business Administration in management and marketing from AGH University of Science and Technology in Krakow, both in 2000. In 2005 she was awarded the title of Doctor of Computer Science and Engineering at the Faculty of Electrical, Automatic Control, Computer Science and Electronic Engineering of the AGH University of Science and Technology, for her thesis and research on cognitive analysis techniques and its application in intelligent information systems. She is an author of more than 100 scientific international publications on information systems, cognitive analysis techniques, biomedical engineering, and computational intelligence methods. She is a member of few prestigious international scientific societies as: SIAM – Society for Industrial and Applied Mathematics, as well as SPIE – The International Society for Optical Engineering, and Cognitive Science Society. Currently she is at the associate professor position, and works in Management Faculty at the AGH University of Science and Technology.

Marek R. Ogiela Professor of Computer Science, cognitive scientist and cryptographer, head of Cryptography and Cognitive Informatics Laboratory. Professor Marek R. Ogiela works at the AGH University of Science and Technology and Pedagogical University in Krakow. In 1992 graduated from the Mathematics and Physics Department at the Jagiellonian University. In 1996 for his honours doctoral thesis on syntactic methods of analysis and image recognition he was awarded the title of Doctor of Control Engineering and Robotics at the Faculty of Electrical, Automatic Control, Computer Science and Electronic Engineering of the AGH University of Science and Technology. In 2001 he was awarded the title of Doctor Habilitated in Computer Science for his research on medical image automatic analysis and understanding. In 2005 he received a professor title in technical sciences.

Member of numerous world scientific associations as well as of the Forecast Committee 'Poland 2000 Plus' of the Polish Academy of Science and member of Interdisciplinary Scientific Committee of the Polish Academy of Arts and Sciences (Bio cybernetics and Biomedical Engineering Section in years 2003-2011). Author of more than 290 scientific international publications on pattern recognition and image understanding, artificial intelligence, IT systems and biocybernetics. Author of recognised monographs in the field of cryptography and IT techniques; author of an innovative approach to cognitive medical image analysis, and linguistic threshold schemes. For his achievements in these fields he was awarded many prestigious scientific honors, including Prof. Takliński's award (twice) and the first winner of Prof. Engel's award.

Urszula Ogiela Economist, and computer scientist. She received Master of Science degree and Master of Business Administration in Information Management from AGH University of Science and Technology in Krakow in 2002. Currently she is a Ph.D. student, and works at the AGH University of Science and Technology, leading her research on linguistic aspect of information data sharing, as well as grammar extensions for secret splitting threshold protocols.