СЕКЦИЯ

„АЛГЕБРА И ЛОГИКА”

Драги колеги,
На 25 юни 2021 г. (петък) от 11:00 часа ще се проведе дистанционно заседание на семинара по „Алгебра и логика”.
Доклад на тема

Framing in secret sharing

ще изнесе

Arkadii Slinko (The University of Auckland, New Zealand).

Семинарът ще се проведе посредством платформата **Zoom** и всеки желаещ може да се присъедини като последва линка, зададен на страницата на семинара.

От секция „Алгебра и логика” на ИМИ – БАН

http://www.math.bas.bg/algebra/seminarAiL/

===

Abstract

Secret sharing, a well-known cryptographic technique, introduced 40 years ago as a private and reliable variant of classical storage, has now become a major cryptographic primitive with numerous real-world applications.

In this paper we consider the digital forensics aspects of secret sharing. We investigate the problem of framing which occurs when a coalition of participants is able to calculate the share of a participant who does not belong to it. In the extreme case one authorized coalition can calculate shares of another authorized coalition, obtain the secret and use it in some way blaming another authorized coalition for their action. Our work shows that in an ideal secret sharing scheme an authorized coalition cannot frame participants who are less senior than all members of the coalition and is able to frame a participant who is more senior than at least one member of the coalition.

This is a joint paper with Yvo Desmedt and Songbao Mo. It has just been published in

Desmedt, Y., Mo, S., & Slinko, A. M. (2021). Framing in Secret Sharing. IEEE Transactions on Information Forensics and Security, 16, 2836-2842.