PAULO MATEUS

A Matemática da Criptografia, Codificação e Tecnologias da Informação: Desafios e Problemas em Aberto

Nesta apresentação será explorado o papel essencial da Matemática como base das tecnologias da informação, nomeadamente nas áreas da criptografia e da teoria de códigos. Começando pelos contributos fundamentais do século XX, serão destacados os trabalhos pioneiros de Kurt Gödel na lógica matemática, de Alan Turing na formalização dos conceitos de computabilidade e Inteligência Artificial, e de John von Neumann na criação dos princípios fundamentais que sustentam a arquitectura computacional moderna. Será analisado o impacto destes conceitos na actual teoria da computabilidade e complexidade computacional, destacando-se em particular o célebre problema em aberto "P versus NP", cuja resolução terá implicações profundas no futuro da segurança informática, no desenvolvimento de algoritmos eficientes e no tratamento eficaz de grandes volumes de dados. Será igualmente sublinhada a importância dos corpos finitos (campos finitos) para a construção de sistemas criptográficos e códigos corretores de erros, ferramentas indispensáveis para garantir a integridade e segurança das actuais comunicações digitais. Neste contexto, será discutido o surgimento da computação quântica e a forma como esta inovação poderá comprometer a segurança dos métodos criptográficos tradicionais, incentivando a investigação urgente em soluções pós-quânticas mais robustas e seguras. Adicionalmente, será estabelecida uma ligação à área da Inteligência Artificial (IA), analisando-se os desafios relacionados com a privacidade e segurança decorrentes do uso crescente da IA, bem como a classificação em termos de complexidade computacional dos problemas fundamentais desta área. Por fim, serão identificados os principais desafios actuais e problemas em aberto nestas áreas interdisciplinares, salientando-se a importância contínua da investigação matemática para o avanço seguro das tecnologias do futuro.

The Mathematics of Cryptography, Coding and Information Technologies: Challenges and Open Problems

This presentation will explore the essential role of Mathematics as a foundation for information technologies, particularly in the areas of cryptography and coding theory. Starting from fundamental contributions of the 20th century, we will highlight the pioneering work of Kurt Gödel in mathematical logic, Alan Turing in formalizing computability and artificial intelligence, and John von Neumann in creating fundamental principles underlying modern computer architecture. We will discuss the impact of these concepts on current computability theory and computational complexity, emphasising in particular the famous open problem "P versus NP", whose resolution would profoundly influence the future of information security, the development of efficient algorithms, and the effective handling of large volumes of data. The importance of finite fields for the development of cryptographic systems and error-correcting codes—essential tools to ensure the integrity and security of today's digital communications—will also be highlighted. Within this context, we will address the emergence of quantum computing and how this technological innovation may compromise traditional cryptographic methods, motivating urgent research efforts towards more robust and secure post-quantum solutions. Additionally, connections will be drawn to Artificial Intelligence (AI), examining challenges related to privacy and security arising from the increased use of AI, as well as characterizing key computational complexity classes associated with fundamental problems in this field. Finally, the presentation will identify current challenges and major open problems within these interdisciplinary areas, emphasising the continued importance of mathematical research for safely advancing future technologies.

Academia das Ciências de Lisboa, 22 de maio de 2025