Seminário do Grupo de Álgebra e Geometria

A reduced McEliece-type cryptosystem with Reed-Solomon codes.

Paulo Almeida
(CIDMA & DMat UA)

Resumo

Code-based public-key cryptosystems (PKCs) are among the most promising alternatives to classical public-key cryptography, as their security is based on well-established NP-hard problems and they offer efficient encryption and decryption procedures. Moreover, unlike schemes relying on integer factorization or discrete logarithms, code-based cryptosystems currently have no known efficient quantum attacks. This makes them strong candidates for post-quantum cryptography. However, a major drawback of these systems is their typically large key sizes.

I will give an overview of our ongoing work [1-5], and explain in more detail our last proposal based on Reed-Solomon codes that surpasses, in terms of its key sizes, the code-based cryptosystems still in contention or proposed for standardization by NIST for post-quantum cryptography, namely BIKE, HQC and Classic McEliece.

[1] Almeida, P., Beltrá, M., Napp, D.: A reduced McEliece-type cryptosystem with Reed-Solomon codes., submitted to Designs Codes and Cryptography, March 14, 2026.

[2] Almeida, P., Beltrá, M., Napp, D.: A convolutional mask for the McEliece cryptosystem with binary Goppa codes. Applicable Algebra in Engineering, Communication and Computing (2026) https://doi.org/10.1007/s00200-026-00728-7

[3] Almeida, P., Beltrá, M., Napp, D.: A convolutional variant of the Niederreiter cryptosystem with GRS codes. In: 2024 IEEE International Symposium on Information Theory (ISIT), pp. 1818–1823 (2024). https://doi.org/10.1109/ISIT57864.2024.10619550

[4] Almeida, P., Beltrá, M., Napp, D.: A Niederreiter public-key cryptosystem using a convolutional approach. In: The Thirteenth International Workshop on Coding and Cryptography (WCC 2024) (2024).

[5] Almeida, P., Beltrá, M., Napp, D., Sebastião, C.: Smaller keys for the McEliece cryptosystem: a convolutional variant with GRS codes. https://doi.org/10.48550/arXiv.2104.06809

Detalhes do Seminário

- **Data:** 16 de abril de 2026
- **Hora:** 11:00 – 12:00
- **Local:** Sala Sousa Pinto

Este seminário é suportado pelo CIDMA ao abrigo do Programa de Financiamento Plurianual de Unidades de I&D da Fundação para a Ciência e a Tecnologia (FCT, https://ror.org/00snfqn58), referências UID/04106/2025 (https://doi.org/10.54499/UID/04106/2025) e UID/PRR/4106/2025.

CIDMA CENTRO DE I&D EM MATEMÁTICA E APLICAÇÕES
CENTER FOR R&D IN MATHEMATICS AND APPLICATIONS

fct Fundação para a Ciência e a Tecnologia