Assistant Professorship of Coding for Communications and Data Storage
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis

Efficiency of Gibson's Attack in the GPT Cryptosystem Based on Twisted Gabidulin Codes

The student should first understand the GPT cryptosystem based on twisted Gabidulin codes and Gibson's attack on the original GPT system. Then he/she should apply the attack to the GPT system based on twisted Gabidulin codes.

Advisors

Julian Renner, Sven Puchinger