SMALL KEYS FOR POST-QUANTUM CRYPTOGRAPHY USING CONVOLUTIONAL CODES

PAULO ALMEIDA, MIGUEL BELTRÁ, AND DIEGO NAPP

Abstract. We present a variant of the Nierderreiter code-based cryptosystem that allows to reduce the public key with respect to other alternatives code-based PKC such as the McEliece and the Nierderreiter cryptosystem. As opposed to the classical Nierderreiter cryptosystem, where block codes are used, we propose the use of parity check matrices of convolutional codes to be part of the public key. The secret key is constituted by the parity check of a Generalized Reed-Solomon code and two invertible polynomial matrices. In this scheme the plaintext is divided into a sequence of shorter messages and encrypted sequentially. We analyze ISD and structural attacks and conclude presenting several examples for different security levels.

P. Almeida; CIDMA - Center for Research and Development in Mathematics and Applications, Dept. of Mathematics, University of Aveiro, Portugal
Email address: palmeida@ua.pt

M. Beltrá University of Alicante, Spain
Email address: mbv29@alu.ua.es

D. Napp University of Alicante, Spain
Email address: diego.napp@ua.es

The first author has been partially supported by the Portuguese Foundation for Science and Technology (FCT - Fundac ¸˜ ao para a Ciência e Tecnologia), reference UIDB/04106/2020.

The second author has been partially supported by VIGROB-287 of the Universitat d'Alacant.

The third author has been partially supported by Spanish grants PID2019-108668GB-I00 of the Ministerio de Ciencia e Innovación of the Gobierno de España and VIGROB-287 of the Universitat d'Alacant.

The talk at the 8IMM 2022 has been given by the second author.