

An application of twisted group rings in Cryptography

María D. GÓMEZ OLVERA (University of Almería, Spain)

lolarosenrot@gmail.com

Cryptography is the science of information security. We have used some protocols for a long time to secure our communications, but these protocols could be not enough to preserve our confidentiality anymore. Because of that, new structures and problems are being proposed. In this work, we focus on ring theory, which could provide a setting in order to get secure public key protocols. We give a proposal for a key exchange using a twisted group ring as a platform, and compare it with some currently used protocols.