MSc thesis defense presentation

Christos Pilichos defends his MSc thesis

Date:	Monday, 13 Nov 2017
Time:	14:00
Location:	Univeristy of Athens, Department of Mathematics, University of Athens, room A11
Thesis title:	Algorithms in Group Theory
Committee:	• Eleftherios Kirousis • Aristeidis T. Pagourtzis • Evangelos Raptis

---

Thesis abstract

Η Μη-Μεταθετικ■ Κρυπτογραφ■α αποτελε■ ■ναν σ■γχρονο κλ■δο των Μαθηματικ■ν που στηρ■ζεται στη δυσκολ■α αλγοριθμικ■ς επιλυσιμ■τητας προβλημ■των απ■ τη Θε- ωρ■α Ομ■δων. ■Ηδη απ■ το 1911 ο Max Dehn κοιν■νησε πως μ■ρος της ■ρευν■ς του αποτελο■ν το πρ■βλημα της λ■ξης, της συζυγ■ας και του ισομορφισμο■ ομ■δων. Τα δυο πρ■τερα προβλ■ματα μαζ■ με εκε■νο της αν■λυσης αποτελο■ν τα θεμ■λια προβλ■ματα των κρυπτοσυστημ■των που εμπερι■χονται στην Εργασ■α. Η περι■γη-

ση στον κ■σμο της Μη-Μεταθετικ■ς Κρυπτογραφ■ας ■χει ως απαρχ■ τους Wagner- Magyarik (ελε■θερες ομ■δες) και Garzon-Zalcstein (ομ■δες Grigorchyk) και δια μ■σ■

των Anshel-Anshel-Goldfeld και Ko-Lee et al. (ομ■δες πλεξ■δων), καταλ■γει στους Shpilrain-Ushakov (ομ■δα Thompson F), Stickel και Kurt. Η κρυπταν■λυση και η προσπ■θεια εν■σχυσης των παραπ■νω πρωτοκ■λλων δ■δει ενδιαφ■ρουσες απ■ρροιες (■πως ■να κρυπτοσ■στημα βασισμενο σε λογικ■ κυκλ■ματα, τη δυναμικ■ εκδοχ■ του πρωτοκ■λλου του Stickel, χρ■ση μονοειδ■ν στο πρωτ■κολλο Wagner-Magyarik, γεν■κευση των πρωτοκ■λλων Anshel-Anshel-Goldfeld και Ko-Lee et al., . . .).