MSc thesis defense presentation

Ελ■νη Παρταλ■δου **defends her MSc thesis.**

Date:	Τετ■ρτη, 22 Νο■ 2017
■ρα:	16:00
Location:	Σχολ■ Ηλεκτρολ■γων Μηχανικ■ν και Μηχανικ■ν Υπολογιστ■ν, ΕΜΠ (παλαι■ κτ■ρια), 1.1.31
Thesis title:	Μια αναδρομ■ στην Μη-Μεταθετικ■ Κρυπτογραφ■α
Committee:	• Αριστε■δης Παγουρτζ■ς • Ευ■γγελος Ρ■πτης • Ευστ■θιος Ζ■χος

Thesis abstract

Non-commutative cryptography is considered to be the art of designing systems

and methods that use algebraic structures, like groups, that are non- commutative.

There are plenty of examples that could be used for this cause. These groups are going be called platform groups and will share a few common characteristics. Considering a few appropriate options we pick among these and explore specific properties that are useful. We use these properties in the Shpilrain-Zapata protocol in order to demonstrate the level of security that can be achieved by picking the correct group. We, of course, show the importance of the relationship between what we study and a specific decision problem, called the word problem, in terms of taking advantage of the computational complexity of it and its ability to be solved efficiently in our choice of algebraic structure. Later on we will discuss a variety of attacks for the Shpilrain-Zapata protocol and the attacks that we think were more efficient .