

MSc thesis defense presentation

Georgios Karistianos defends his MSc thesis

Date:	Monday, 29 Aug 2016
Time:	13:00
Location:	Univeristy of Athens, Department of Informatics and Telecommunications, B7 Κρυπτογραφία Ελλειπτικόν Καμπυλόν και το Bitcoin
Thesis title:	Ioannis Emiris Aggelos Kiayias Aristeidis T. Pagourtzis
Committee:	

Thesis abstract

Στα πλαίσια αυτής της Διπλωματικής εργασίας θα δοµε και θα αναλσοµε την Κρυπτογραφία Ελλειπτικόν Καμπυλόν, τους αλριθµους κρυπτογράφησης της και τις ψηφιακές υπογραφές. Στην συνέχεια θα δοµε κποιες βελτισεις στην απδοση των αριθμητικόν προξων χρησιμοποιντας προβολικς συντεταγµνες και θα µελετσοµε κποιες µεθδους που κνουν τα Κρυπτοσυσµατα Ελλειπτικόν Καμπυλόν ανθεκτικ σε Side Channel Attacks, οι οποες θεωρονται αρκετ αποδοτικς κρυπταναλυτικς µεθδους και αποτελον παρµετρο σχεδιασµο ενς κρυπτογραφµατος µιας και εκµεταλλεονται ιδιτητες του υλικοπνω στο οποο εναι σχεδιασµνο και υλοποιηµνο να ττοιο σστηµα. Στην συνέχεια θα µιλσοµε για το Bitcoin το οποο εναι να Ψηφιακνµισµα που αξιοποιε τεχνικς κρυπτογράφησης για την παραγωγµονδων αξιας και την επαλθευση συναλλαγν, χωρς τη διαµεσολβηση κεντρικς τρεπεζας. Θα δοµε το προβληµα της Malleability ιδιτητας στο Bitcoin και πως αυτµπορε να αντιμετωπιστε. Τλος θα δοµε πως µποροµε να χρησιμοποισοµε το Bitcoin για Multiparty Computations πρωτκολλα.