

# MSc thesis defense presentation

## Γεωργιος Καρυστιανός defends his MSc thesis

<b>Date:</b>	Δευτέρα, 29 Αύγ 2016
<b>Ώρα:</b>	13:00
<b>Location:</b>	Εθνική και Καποδιστριακή Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής και Τηλεπικοινωνιών, B7 <a href="#">Κρυπτογραφία</a> <a href="#">Ελλειπτική</a> <a href="#">Καμπύλη και το</a> <a href="#">Bitcoin</a>
<b>Thesis title:</b>	<a href="#">Ιωάννης Εμμέρης</a> <a href="#">Άγγελος Κιαγιάνης</a> <a href="#">Αριστείδης</a> <a href="#">Παγουρτζής</a>
<b>Committee:</b>	

---

### Thesis abstract

Στα πλαίσια αυτής της Διπλωματικής εργασίας θα δομώ και θα αναλύσω την Κρυπτογραφία Ελλειπτικής Καμπύλης, τους αλγόριθμους κρυπτογράφησης της και τις ψηφιακές υπογραφές. Στην συνέχεια θα δομώ κάποιες βελτιστοποιήσεις στην απόδοση των αριθμητικών πράξεων χρησιμοποιώντας προβολικές συντεταγμένες και θα μελετήσουμε κάποιες μεθόδους που κινούν τα Κρυπτοσυστήματα Ελλειπτικής Καμπύλης ανθεκτικά σε Side Channel Attacks, οι οποίες θεωρούνται αρκετά αποδοτικές κρυπταναλυτικές μεθόδους και αποτελούν παράμετρο σχεδιασμού ενός κρυπτογραφήματος μιας και εκμεταλλεύονται ιδιότητες του υλικού πάνω στο οποίο είναι σχεδιασμένο και υλοποιημένο ένα τέτοιο σύστημα. Στην συνέχεια θα μιλήσουμε για το Bitcoin το οποίο είναι ένα Ψηφιακό νόμισμα που αξιοποιεί τεχνικές κρυπτογράφησης για την παραγωγή μονόδων αξιών και την επαλήθευση συναλλαγών, χωρίς τη διαμεσολάβηση κεντρικής τράπεζας. Θα δομώ το πρόβλημα της Malleability ιδιότητας στο Bitcoin και πώς αυτό μπορεί να αντιμετωπιστεί. Τέλος θα δομώ πώς μπορούμε να χρησιμοποιήσουμε το Bitcoin για Multiparty Computations πρωτόκολλα.