

MSc thesis defense presentation

Γεωργιος Καρυστιανός defends his MSc thesis

| | |
|----------------------|--|
| Date: | Δευτέρα, 29 Αύγ 2016 |
| Ώρα: | 13:00 |
| Location: | Εθνική και Καποδιστριακή Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής και Τηλεπικοινωνιών, B7 Κρυπτογραφία Ελλειπτική Καμπύλη και το Bitcoin |
| Thesis title: | Ιωάννης Εμμέρης Γιάννης Κιανής Αριστείδης Παγουρτζής |
| Committee: | |

Thesis abstract

Στα πλαίσια αυτής της Διπλωματικής εργασίας θα δοθεί και θα αναλύσουμε την Κρυπτογραφία Ελλειπτικής Καμπύλης, τους αλγόριθμους κρυπτογράφησης της και τις ψηφιακές υπογραφές. Στην συνέχεια θα δοθεί 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 κρυπτανalyτικές μεθόδους και αποτελούν παράμετρο σχεδιασμού ενός κρυπτογραφικού συστήματος 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 μοναδικών αξιών και την επαλήθευση συναλλαγών, χωρίς τη διαμεσολάβηση κεντρικής τράπεζας. Θα δοθεί το πρόβλημα της Malleability ιδιότητας στο Bitcoin και πώς αυτό μπορεί να αντιμετωπιστεί. Τέλος θα δοθεί πώς μπορούμε να χρησιμοποιήσουμε το Bitcoin για Multiparty Computations πρωτόκολλα.