MSc thesis defense presentation

Γε■ργιος Καρυστιαν■ς defends his MSc thesis

Date:	Δευτ■ρα, 29 Α■γ 2016
■ρα:	13:00
Location:	Εθνικ■ και Καποδιστριακ■ Πανεπιστ■μιο Αθην■ν, Τμ■μα Πληροφορικ■ς και Τηλεπικοινωνι■ν, Β7
Thesis title:	Κρυπτογραφ■α Ελλειπτικ■ν Καμπυλ■ν και το Bitcoin
Committee:	• Ιω■ννης Εμ■ρης • ■γγελος Κιαγι■ς • Αριστε■δης Παγουρτζ■ς

Thesis abstract

Στα πλα■σια αυτ■ς της Διπλωματικ■ς εργασ■ας θα δο■με και θα αναλ■σουμε την Κρυπτογραφ■α Ελλειπτικ■ν Καμπυλ■ν, τους αλγ■ριθμους κρυπτογρ■φησης της και τις ψηφιακ■ς υπογραφ■ς. Στην συν■χεια θα δο■με κ■ποιες βελτι■σεις στην απ■δοση των αριθμητικ■ν πρ■ξεων χρησιμοποι■ντας προβολικ■ς συντεταγμ■νες και θα μελετ■σουμε κ■ποιες μεθ■δους που κ■νουν τα Κρυπτοσυστ■ματα Ελλειπτικ■ν Καμπυλ■ν ανθεκτικ■ σε Side Channel Attacks, οι οπο■ες θεωρο■νται αρκετ■ αποδοτικ■ς κρυπταναλυτικ■ς μεθ■δους και αποτελο■ν παρ■μετρο σχεδιασμο■ εν■ς κρυπτογραφ■ματος μιας και εκμεταλλε■ονται ιδι■τητες του υλικο■ π■νω στο οπο■ο ε■ναι σχεδιασμ■νο και υλοποιημ■νο ■να τ■τοιο σ■στημα. Στην συν■χεια θα μιλ■σουμε για το Bitcoin το οπο■ο ε■ναι ■να Ψηφιακ■ ν■μισμα που αξιοποιε■ τεχνικ■ς κρυπτογρ■φησης για την παραγωγ■ μον■δων αξ■ας και την επαλ■θευση συναλλαγ■ν, χωρ■ς τη διαμεσολ■βηση κεντρικ■ς τρ■πεζας. Θα δο■με το πρ■βλημα της Malleability ιδι■τητας στο Bitcoin και πως αυτ■ μπορε■ να αντιμετωπιστε■. Τ■λος θα δο■με πως μπορο■με να χρησιμοποι■σουμε το Bitcoin για Multiparty Computations πρωτ■κολλα.