

**Προκήρυξη Διπλωματικών Εργασιών Ακαδημαϊκού Έτους 2011-2012**  
**Επιβλέπων Καθηγητής Παύλος Σπυράκης**

<b>1. Παιχνίδια, ψυχαγωγικές και εκπαιδευτικές διαδραστικές εγκαταστάσεις με τη χρήση "διάχυτων" υπολογιστικών συστημάτων (Pervasive Gaming/Installations)</b>	
<b>Άτομα</b>	2
<b>Περιγραφή</b>	<p>Οι τομείς των ασύρματων δικτύων αισθητήρων, των ενσωματωμένων συσκευών αλλά και των κινητών τηλεφώνων τα τελευταία χρόνια συγκλίνουν, συνδυάζονται και αλληλοκαλύπτονται δημιουργώντας αυτό που ονομάζεται Internet of Things.</p> <p>Στο πεδίο αυτό, οι εφαρμογές ψυχαγωγίας αξιοποιούν τις δυνατότητες που προσφέρονται για να δημιουργηθούν νέες, μη συμβατικές εφαρμογές παιχνιδιών που λαμβάνουν χώρα στο φυσικό περιβάλλον των χρηστών, με σενάρια που εξελίσσονται σε απομακρυσμένες περιοχές και περιλαμβάνουν φυσικούς τρόπους αλληλεπίδρασης.</p> <p><b>A) Υλοποίηση συνεργατικών παιχνιδιών με χρήση φορητών δικτυωμένων συσκευών</b></p> <p>Στόχος της εργασίας είναι η ανάπτυξη παιχνιδιών που θα περιλαμβάνουν πολλούς παίχτες και θα βασίζονται στην έντονη φυσική δραστηριότητα στο χώρο. Χαρακτηριστικό παράδειγμα τέτοιων παιχνιδιών είναι αυτά που βασίζονται στην πλατφόρμα Fun in Numbers (<a href="http://www.funinnumbers.eu">www.funinnumbers.eu</a>). Βασικό χαρακτηριστικό είναι η χρήση αισθητήρων και άλλων εισόδων στο σύστημα (π.χ., θέση, απόσταση) ως ενεργειών κατά τη διάρκεια των "παιχνιδιών". Δυνητικά το σύστημα θα μπορούσε να υλοποιηθεί έχοντας κατά νου συγκεκριμένο χώρο και "εκπαιδευτικό" ρόλο, π.χ. μια διαδραστική εμπειρία μέσα στο πλαίσιο μιας επίσκεψης σε ένα μουσείο.</p> <p><b>B) Εφαρμογή μηχανής γυμναστικής με πτήση/περιήγηση μέσω Google Earth ή Street View</b></p> <p>Στόχος της εργασίας είναι η υλοποίησης συστήματος που να συνδέει τη φυσική μας δραστηριότητα π.χ., στο χώρο ενός γυμναστηρίου, και παίρνοντας ως input τη δραστηριότητά μας σε ένα διάδρομο γυμναστικής ή ένα ποδήλατο, να δίνεται στον χρήστη οπτικό feedback προκειμένου να κάνει την όλη εμπειρία περισσότερο ευχάριστη, ενδεχομένως μαζί με περισσότερη πληροφορία (π.χ., σύγκριση δραστηριότητας με άλλους χρήστες, κτλ). Θα βασιστούμε σε κάποια ενσωματωμένη πλατφόρμα υλικού όπως Arduino ή Sun Spot για τη διασύνδεση σε επίπεδο υλικού ενώ σε επίπεδο λογισμικού σε τεχνολογίες HTML5 και τα συστήματα της Google.</p>
<b>Προαπαιτούμενα</b>	
<b>Συνεπίβλεψη</b>	Δρ. Ιωάννης Χατζηγιαννάκης, Δρ. Γεώργιος Μυλωνάς, Δρ. Ευάγγελος Θεοδωρίδης

2. Εφαρμογές Έξυπνης Πόλης: Σχεδιασμός, Ανάπτυξη και Πειραματική Αξιολόγηση	
Άτομα	2
Περιγραφή	<p>Τα τελευταία χρόνια υπάρχει μια σαφής τάση σε πολλούς εφαρμοσμένους κλάδους της πληροφορικής και των τηλεπικοινωνιών για τη σύνδεση του πραγματικού και του ψηφιακού κόσμου. Χαρακτηριστικό παράδειγμα είναι η ενσωμάτωση αισθητήρων, όπως επιταχυνσιόμετρων (accelerometers) σε διάφορες συσκευές που χρησιμοποιούμε καθημερινά, όπως π.χ., κινητά τηλέφωνα, χειριστήρια παιχνιδιομηχανών, PDA, MP3 players, κτλ. Η παρουσία αισθητήρων στο άμεσο περιβάλλον μας επιτρέπει την ανάπτυξη τεράστιου εύρους κατανεμημένων εφαρμογών, όπως π.χ. οι εφαρμογές "έξυπνων οικολογικών κτηρίων" και το "ζωντανών νηπιαγωγείων", κλπ.</p> <p><b>A) Εφαρμογή portal κοινωνικής δικτύωσης για δεδομένα από αισθητήρες - εστίαση σε ρύπανση και μόλυνση του περιβάλλοντος</b></p> <p>Σκοπός της εργασίας είναι να υλοποιηθεί ένα portal όπου κάθε χρήστης θα μπορεί να εισάγει δεδομένα από αισθητήρες που έχουν σχέση με ρύπανση και μόλυνση του περιβάλλοντος (σκουπίδια, αέριοι ρύποι, γύρη, σκόνη) σε συνδυασμό με γεωγραφικά δεδομένα (gps traces) και αυτά να γίνονται αναπαράσταση στο google maps. Θα χρησιμοποιηθούν κινητά τηλέφωνα και άλλες πλατφόρμες, ενώ θα απαιτηθεί να υλοποιηθεί διεπαφή με αισθητήρες. Ενδεχομένως το σύστημα να εγκατασταθεί σε οχήματα (π.χ., λεωφορεία) για τη συστηματική συλλογή δεδομένων. Το σύστημα εκτός από τις διαφορετικές συνιστώσες λειτουργίας, που μπορούν η καθεμία να είναι ένας διαφορετικός client σε smartphones, μπορεί να χρησιμοποιεί μια κοινή υποδομή για την αποθήκευση και επεξεργασία πληροφορίας. επίσης, μπορεί να υπάρχει μια desktop συνιστώσα. Έμφαση θα δοθεί στο σχεδιασμό της διεπαφής με άλλα συστήματα για την παροχή των δεδομένων που έχουν συλλεγεί.</p> <p><b>B) Σύστημα επίβλεψης και ελέγχου της άρδευσης δημόσιων χώρων και κτιρίων σε μια αστική περιοχή</b></p> <p>Στην εργασία αυτή στόχος είναι η ανάπτυξη συστήματος για την κεντρική επίβλεψη/έλεγχο της άρδευσης των διάφορων "πράσινων" χώρων που βρίσκονται στα όρια ενός δήμου. Λόγω του πλήθους τέτοιων χώρων στην έκταση ενός δήμου, ένα τέτοιο σύστημα θα μπορούσε να συνεισφέρει στην εξοικονόμηση τόσο υδάτινων πόρων αλλά και τη μείωση του σχετικού κόστους. Η υλοποίησή του αφορά στην διασύνδεση μιας υποδομής με μετρητές κατανάλωσης νερού, και της παροχής διεπαφής για την επίβλεψη και τον έλεγχο/χρονοπρογραμματισμό τους. Έμφαση θα δοθεί στο σχεδιασμό της διεπαφής με άλλα συστήματα για την παροχή των δεδομένων που έχουν συλλεγεί.</p>
Προαπαιτούμενα	
Συνεπίβλεψη	Δρ. Ιωάννης Χατζηγιαννάκης, Δρ. Γεώργιος Μυλωνάς, Δρ. Ευάγγελος Θεοδωρίδης

<b>3. Ανίχνευση Ανθρώπινης Δραστηριότητας/Κινητικότητας: Μοντελοποίηση, Ανάλυση, Εφαρμογές</b>	
<b>Άτομα</b>	2
<b>Περιγραφή</b>	<p>Τα τελευταία χρόνια υπάρχει μια σαφής τάση μείωση του μεγέθους των συσκευών (και κατ' επέκταση των υπολογιστικών δυνατοτήτων τους) και η ενσωμάτωση τους στο περιβάλλον που μας περιβάλλει. Η νέα κατεύθυνση είναι η αντικατάσταση του ισχυρού υπολογιστή από ένα μεγάλο πλήθος πολύ μικρότερων συσκευών που βρίσκονται διάχυτα στο περιβάλλον. Σε αυτά τα συστήματα η συνήθης υπόθεση ότι ο κάθε πράκτορας του συστήματος, δηλαδή κάθε ανεξάρτητη υπολογιστική μονάδα, είναι τόσο υπολογιστικά ισχυρή δεν είναι πλέον αποδεκτή.</p> <p><b>A) Μοντελοποίηση της ανθρώπινης δραστηριότητας/κινητικότητας σε αστικές περιοχές</b></p> <p>Η μοντελοποίηση της ανθρώπινης δραστηριότητας/κινητικότητας σε μια αστική περιοχή ή σε έναν κλειστό χώρο είναι ένα ενδιαφέρον θέμα, με εφαρμογές από τη διαχείριση των χρηστών μιας εταιρείας κινητής τηλεφωνίας, ως τον πολεοδομικό σχεδιασμό μιας αστικής περιοχής. Μπορεί να χρησιμοποιηθεί επίσης ως input για εξομοιώσεις λειτουργίας δικτυακών πρωτοκόλλων σε ασύρματες τεχνολογίες.</p> <p><b>B) Στοχευμένες διαφημίσεις κ εμπορικές υπηρεσίες σε αστικά περιβάλλοντα</b></p> <p>Στόχος της διπλωματικής εργασίας είναι η υλοποίηση ενός συστήματος παροχής στοχευμένων διαφημίσεων και εμπορικών υπηρεσιών με χρήση των τεχνολογιών Bluetooth και Wifi των κινητών τηλεφώνων. Το σύστημα θα προωθεί εξατομικευμένο περιεχόμενο προς τους καταναλωτές/επισκέπτες ενός καταστήματος (εμπορικό κέντρο, κλπ) υπό τη μορφή διαφημίσεων, προσφορών (κουπονιών κλπ). Το περιεχόμενο καθορίζεται από τα καταστήματα που έχουν εγγραφεί στο σύστημα, και η επιλογή του περιεχομένου που αποστέλλεται στο κινητό του τελικού χρήστη εξαρτάται τόσο από τα ενδιαφέροντα και δεδομένα που έχει δηλώσει ο ίδιος σε σχετικό δικτυακό τόπο του συστήματος όσο και στην τρέχουσα φυσική θέση του μέσα στο στη πόλη (πχ πεζόδρομος, εμπορικό κέντρο κλπ -π.χ. σε ποιά καταστήματα βρίσκεται πιο κοντά, σε ποιά βιτρίνα παρέμεινε για περισσότερο χρόνο κλπ).</p>
<b>Προαπαιτούμενα</b>	
<b>Συνεπίβλεψη</b>	Δρ. Ιωάννης Χατζηγιαννάκης, Δρ. Γεώργιος Μυλωνάς, Δρ. Ευάγγελος Θεοδωρίδης

<b>4. Κατανεμημένος Υπολογισμός</b>	
<b>Άτομα</b>	
<b>Περιγραφή</b>	<p>Τα κατανεμημένα συστήματα χρησιμοποιούνται καθημερινά στο χώρο των επιχειρήσεων, της εκπαίδευσης, της δημόσιας διοίκησης αλλά ακόμα και στο σπίτι, ιδιαίτερα στις μέρες μας, όπου ο παγκόσμιος ιστός επιτρέπει την πρόσβαση σε δεδομένα ανεξαρτήτως της γεωγραφικής τους τοποθεσίας. Οι θεμελιώδεις δυσκολίες που πρέπει να αντιμετωπιστούν από ένα κατανεμημένο σύστημα σχετίζονται κυρίως με την ασύγχρονη εκτέλεση των διεργασιών, την περιορισμένη τοπική γνώση και τα σφάλματα που παρουσιάζονται.</p> <p>Η θεωρία του κατανεμημένου υπολογισμού έχει ως βασικό στόχο την επίτευξη ενός πλαισίου εργασίας για τα κατανεμημένα συστήματα μέσω του οποίου θα μπορούσαμε να μελετήσουμε τα θεμελιώδη προβλήματα που εμφανίζονται στην πλειοψηφία των καταστάσεων που αντιμετωπίζουν τα κατανεμημένα συστήματα. Στόχος της διπλωματικής είναι η επιλογή ενός συγκεκριμένου προβλήματος και η μελέτη της βιβλιογραφίας. Στη συνέχεια θα σχεδιαστεί μια νέα αλγοριθμική λύση και θα αναλυθεί η ορθότητα και η απόδοση της λύσης.</p>
<b>Προαπαιτούμενα</b>	Κατανεμημένα Συστήματα
<b>Συνεπίβλεψη</b>	Δρ. Ιωάννης Χατζηγιαννάκης & Δρ. Όθωνα Μιχαήλ

<b>5. Χρονικά Μεταβαλλόμενα Δυναμικά Δίκτυα</b>	
<b>Άτομα</b>	
<b>Περιγραφή</b>	<p>Τα τελευταία χρόνια υπάρχει μια σαφής τάση μείωση του μεγέθους των συσκευών (και κατ' επέκταση των υπολογιστικών δυνατοτήτων τους) και η ενσωμάτωση τους στο περιβάλλον που μας περιβάλλει. Η νέα κατεύθυνση είναι η αντικατάσταση του ισχυρού υπολογιστή από ένα μεγάλο πλήθος πολύ μικρότερων συσκευών που βρίσκονται διάχυτα στο περιβάλλον. Σε αυτά τα συστήματα η συνήθης υπόθεση ότι ο κάθε πράκτορας του συστήματος, δηλαδή κάθε ανεξάρτητη υπολογιστική μονάδα, είναι τόσο υπολογιστικά ισχυρή δεν είναι πλέον αποδεκτή.</p> <p>Πρόσφατα προτάθηκε το μοντέλο των πρωτόκολλων πληθυσμών που βασίζεται στην πρόβλεψη ότι τα μοντέρνα συστήματα θα αποτελούνται από τεράστιο πλήθος φτηνών και μικρών πρακτόρων. Οι πόροι που θα είναι διαθέσιμοι σε κάθε πράκτορα μπορεί να είναι ισχυρά περιορισμένοι. Στο νέο μοντέλο, ο καταναεμημένος υπολογισμός θα διεξάγεται μέσω αλληλεπιδράσεων μεταξύ των πρακτόρων. Μικρές τοπικές αλληλεπιδράσεις συνθέτουν μια καθολική σύνθετη λειτουργία.</p> <p>Στόχος της διπλωματικής είναι η μελέτη και κατανόηση του νέου μοντέλου καταναεμημένου υπολογισμού. Θα εξεταστεί τι υπολογισμούς μπορεί να φέρει σε πέρας ένα συνεργατικό δίκτυο. Ιδιαίτερο ενδιαφέρον έχει η ανάπτυξη ενός ενδιάμεσου λογισμικού για την ανάπτυξη αλγοριθμικών λύσεων. Υπάρχουν στη διάθεσή μας ένα πλήθος από ενσωματωμένα υπολογιστικά συστήματα τα οποία θα χρησιμοποιηθούν για τους σκοπούς της συγκεκριμένης εργασίας.</p>
<b>Προαπαιτούμενα</b>	Καταναεμημένα Συστήματα
<b>Συνεπίβλεψη</b>	Δρ. Ιωάννης Χατζηγιαννάκης, Δρ. Όθωνας Μιχαήλ

<b>6. Μελέτη Παιγνίων Συμφόρησης σε Δίκτυα με Ατελή Πληροφόρηση</b>	
<b>Άτομα</b>	
<b>Περιγραφή</b>	<p>Τα παίγνια συμφόρησης σε δίκτυα (network congestion games) έχουν μελετηθεί εκτενώς ως προς τις ισορροπίες Nash και το κόστος της αναρχίας (price of anarchy). Ωστόσο, οι μέχρι τώρα αναλύσεις στηρίζονται στην υπόθεση ότι είναι γνωστά εκ των προτέρων τόσο το συνολικό πλήθος των χρηστών όσο και το βάρος (δηλαδή το φορτίο) κάθε χρήστη.</p> <p>Αντικείμενο της διπλωματικής είναι η θεωρητική και πειραματική μελέτη των ισορροπιών Nash και του κόστους της αναρχίας σε on-line παίγνια συμφόρησης, όπου οι χρήστες φτάνουν σε διαφορετικές χρονικές στιγμές και ο καθένας πρέπει να αποφασίσει για το μονοπάτι από το οποίο θα δρομολογήσει το φορτίο του, γνωρίζοντας μόνο τις αντίστοιχες επιλογές των χρηστών που έχουν προηγηθεί και έχοντας κάποια στατιστική εκτίμηση για τα φορτία των χρηστών που ακολουθούν. Στόχος είναι να βρεθούν οι κατάλληλες στρατηγικές που πρέπει να ακολουθήσουν οι χρήστες ώστε στο τέλος (αφού δρομολογηθούν όλα τα φορτία), το κόστος της αναρχίας (ορισμένο κατάλληλα για την on-line περίπτωση που εξετάζεται) να είναι όσο το δυνατό πιο μικρό.</p>
<b>Προαπαιτούμενα</b>	Οικονομική Θεωρία και Αλγόριθμοι
<b>Συνεπιβλεψη</b>	Δρ. Παναγιώτα Παναγοπούλου

<b>7. Ανάπτυξη και Ανάλυση Κατανεμημένων Αλγορίθμων Χρωματισμού Γραφημάτων με βάση τη Θεωρία Παιγνίων</b>	
<b>Άτομα</b>	
<b>Περιγραφή</b>	<p>Το πρόβλημα χρωματισμού των κορυφών ενός γραφήματος χρησιμοποιώντας όσο το δυνατό λιγότερα χρώματα (Minimum Vertex Coloring) αποτελεί ένα από τα πλέον θεμελιώδη προβλήματα της Θεωρίας Υπολογισμού και της Θεωρίας Γραφημάτων: ζητείται να ανατεθεί ένα χρώμα σε κάθε κορυφή του γραφήματος έτσι ώστε γειτονικές κορυφές να έχουν διαφορετικά χρώματα και το συνολικό πλήθος των χρωμάτων που χρησιμοποιούνται να ελαχιστοποιείται. Σχετικά πρόσφατα, το πρόβλημα μοντελοποιήθηκε ως ένα στρατηγικό παίγνιο μεταξύ των κορυφών του γραφήματος. Η ανάλυση του παιγνίου οδήγησε σε έναν πολυωνυμικό αλγόριθμο για την εύρεση ισορροπιών Nash. Οι ισορροπίες αυτές αποδείχθηκε ότι αντιστοιχούν σε αποδοτικούς χρωματισμούς των κορυφών του γραφήματος, με την έννοια ότι χρησιμοποιούν ένα συνολικό αριθμό χρωμάτων ο οποίος ικανοποιεί μια σειρά από γνωστά άνω φράγματα στο χρωματικό αριθμό του γραφήματος (δηλαδή στο ελάχιστο πλήθος χρωμάτων που απαιτούνται ώστε να χρωματιστούν ορθά οι κορυφές).</p> <p>Αντικείμενο της διπλωματικής είναι να χρησιμοποιηθούν ανάλογες παιγνιοθεωρητικές τεχνικές για την ανάπτυξη και τη θεωρητική και πειραματική μελέτη κατανεμημένων αλγορίθμων χρωματισμού γραφημάτων. Στόχος είναι να μελετηθούν κατανεμημένοι αλγόριθμοι που χρησιμοποιούν ανταγωνιστικό αριθμό χρωμάτων σε σχέση με γνωστούς κατανεμημένους αλγορίθμους που έχουν προταθεί στη βιβλιογραφία.</p>
<b>Προαπαιτούμενα</b>	Οικονομική Θεωρία και Αλγόριθμοι & Κατανεμημένα Συστήματα I & II
<b>Συνεπιβλεψη</b>	Δρ. Παναγιώτα Παναγοπούλου & Δρ. Ιωάννης Χατζηγιαννάκης

<b>8. Εφαρμογή αποδείξεων μηδενικής γνώσης για την προστασία της ιδιωτικότητας των σημασιολογικών οντοτήτων στο Internet of Things.</b>	
<b>Άτομα</b>	2
<b>Περιγραφή</b>	<p>Ένα ασύρματο δίκτυο αισθητήρων αποτελείται από χωρικά αυτόνομες συσκευές οι οποίες έχουν τη δυνατότητα παρακολούθησης φυσικών, περιβαλλοντικών, βιολογικών συνθηκών όπως θερμοκρασία, υγρασία, πίεση, ήχο, ρυθμό καρδιάς κτλ. Η εφαρμογή των δικτύων αυτών είναι πλέον διαδεδομένη ευρέως στην καθημερινή ζωή. Κτίρια όπως κατοικίες, εργασιακές εγκαταστάσεις, εργοστάσια και νοσοκομεία αποτελούνται από δίκτυα αισθητήρων π.χ. για την παρακολούθηση ασθενών, χώρων και εγκαταστάσεων, φυσικών συνθηκών. Επιπλέον, η διάδοση του Internet of Things έχει οδηγήσει στην οργάνωση των συσκευών των δικτύων σε σημασιολογικές οντότητες βάσει κάποιας κοινής τους ιδιότητας. Λόγω της ασύρματης φύσης επικοινωνίας των συσκευών που αποτελούν τα δίκτυα αυτά, δημιουργούνται θέματα ασφάλειας και προστασίας της ιδιωτικότητας καθώς σε πολλές περιπτώσεις μεταφέρονται ευαίσθητα δεδομένα.</p> <p>Για την προστασία της ιδιωτικότητας και τη διατήρηση της εμπιστοσύνης η κρυπτογραφία προσφέρει το εργαλείο των αποδείξεων μηδενικής γνώσης. Μια απόδειξη μηδενικής γνώσης είναι ένα διαδραστικό κρυπτογραφικό πρωτόκολλο μεταξύ δύο οντοτήτων, κατά το οποίο η μια οντότητα αποδεικνύει την εγκυρότητα ενός ισχυρισμού χωρίς να αποκαλύπτει πληροφορία η οποία μπορεί να χρησιμοποιηθεί από την άλλη οντότητα. Για την εφαρμογή τέτοιων πρωτοκόλλων σε περιορισμένων πόρων συσκευές, προτείνεται η χρήση της θεωρίας ελλειπτικών καμπυλών. Το πλεονέκτημα αυτού του κρυπτοσυστήματος είναι ότι με χρήση μικρότερου μεγέθους κλειδιών, παρέχει το ίδιο επιπέδου ασφάλειας με άλλα κρυπτοσυστήματα (π.χ. RSA). Σκοπός της διπλωματικής εργασίας αυτής, είναι η εφαρμογή κρυπτογραφικών πρωτοκόλλων για την προστασία της ιδιωτικότητας των σημασιολογικών οντοτήτων που συνθέτουν ασύρματα δίκτυα αισθητήρων.</p>
<b>Προαπαιτούμενα</b>	
<b>Συνεπίβλεψη</b>	Επικ. Καθ. Ιωάννης Σταματίου, Δρ. Ιωάννης Χατζηγιαννάκης, Απόστολος Πυργελής

<b>9. Μελέτη και ανάπτυξη κρυπτογραφικών πρωτοκόλλων ανώνυμων πιστοποιητικών σε συσκευές με περιορισμένους πόρους</b>	
<b>Άτομα</b>	
<b>Περιγραφή</b>	<p>Η ανώνυμη πιστοποιητική ήταν σχετικά ανεξερεύνητη μέχρι την εμφάνιση δύο πρωτοκόλλων, idemix και u-prove που εφαρμόστηκαν επίσης για να καλύψουν τις ανάγκες ορισμένων τομέων εφαρμογής, που γίνονται ουσιαστικά προϊόντα και εφαρμόζονται στα πληροφοριακά συστήματα επικοινωνιών. Αυτά τα δύο πρωτόκολλα υποστηρίζονται από δύο από τους ηγέτες στο Διαδίκτυο και την τεχνολογία ICT, για την προστασία των προσωπικών δεδομένων και την πιστοποιημένη και ασφαλή διαχείριση της πληροφορίας στο διαδίκτυο.</p> <p>Αντικείμενο της διπλωματικής είναι ο καθορισμός, η δημιουργία και η διαχείριση ανώνυμων πιστοποιητικών σε συσκευές με περιορισμένους πόρους όπως οι smartcards και οι συσκευές αισθητήρων. Ταυτόχρονα θα ακολουθήσει ανάλυση και προγραμματιστική εφαρμογή των πρωτοκόλλων δημιουργίας ανώνυμων πιστοποιητικών σε υπαρκτές συσκευές χαμηλών πόρων ώστε να αξιολογηθεί η ευχρηστία της τεχνολογίας των ανώνυμων πιστοποιητικών όταν εφαρμόζεται σε συσκευές χαμηλών πόρων.</p>
<b>Προαπαιτούμενα</b>	Διακριτά Μαθηματικά I,II, Θεωρία Υπολογισμού, Υπολογιστική Πολυπλοκότητα, Πιθανότητες, Πιθανοτικές Τεχνικές, Κρυπτογραφία
<b>Συνεπίβλεψη</b>	Επίκουρος Καθηγητής Γιάννης Σταματίου και Δρ. Βάσια Λιάγκου

<b>10. Θεωρία και εφαρμογές των Τοπικά Τυχαίων Αναγωγών (Locally Random Reductions)</b>	
<b>Άτομα</b>	
<b>Περιγραφή</b>	<p>Μία –τοπικά τυχαία αναγωγή (Locally Random Reduction – LRR) απεικονίζει ένα στιγμιότυπο προβλήματος σε ένα σύνολο στιγμιότυπων έτσι ώστε είναι εύκολο να κατασκευαστεί μία απάντηση στο από τις απαντήσεις στα στιγμιότυπα αυτά ενώ, επιπλέον, η κατανομή υποσυνόλων στοιχείων από τα στιγμιότυπα εξαρτάται μόνο από το μέγεθος του (δείτε [1,2]). Οι LRR χρησιμοποιούνται ευρέως στην κρυπτογραφία για τη σχεδίαση αποδοτικών διαδραστικών αποδείξεων μηδενικής γνώσης (Zero Knowledge Interactive Proofs – ZKIPs). Επιπρόσθετα, με χρήση των LRR μπορεί να συνδεθεί η πολυπλοκότητα χειρότερης περίπτωσης υπολογισμού μίας συνάρτησης με την μέση πολυπλοκότητα μιας άλλης, πράγμα που σημαντικό στις αποδείξεις ασφάλειας στη θεωρητική κρυπτογραφία. Στην προτεινόμενη διπλωματική εργασία θα διερευνηθούν οι LRR καθώς και οι χρήσεις τους στη σχεδίαση ισχυρών κρυπτογραφικών συναρτήσεων.</p>
<b>Προαπαιτούμενα</b>	πολύ καλή γνώση θεωρίας πολυπλοκότητας και βασικής θεωρίας πιθανοτήτων.
<b>Συνεπίβλεψη</b>	Χριστόφορος Ραπτόπουλος και Γιάννης Σταματίου

<b>11. Πιθανοτικά Μοντέλα για την Εμπιστοσύνη στο Διαδίκτυο</b>	
<b>Άτομα</b>	
<b>Περιγραφή</b>	<p>Στις σημερινές ηλεκτρονικές συναλλαγές, η έννοια της εμπιστοσύνης δεν μπορεί να θεωρηθεί πλέον δεδομένη. Συγκεκριμένα, χρειάζεται να οριστεί ώστε να μπορεί να γίνει αντιληπτή, να εκτιμηθεί, να μετρηθεί και να πιστοποιηθεί. Συνεπώς, ο σχεδιασμός διαφορετικών επιπέδων εμπιστοσύνης για τις διάφορες διαδικτυακές αλληλεπιδράσεις έχει γίνει ένας από τους βασικούς στόχους όσον αφορά στην έρευνα στην διαδικτυακή επιστήμη. Επιπρόσθετα, η εμπιστοσύνη μπορεί να θεωρηθεί ως μια πεποίθηση, η οποία εξελίσσεται στο χρόνο και μπορεί να επηρεάζεται από τις πεποιθήσεις άλλων. Είναι λοιπόν μεγάλης σημασίας ο ορισμός και η ανάλυση μαθηματικών μοντέλων που περιγράφουν την διάδοση πληροφορίας και την εξέλιξη των πεποιθήσεων σε ένα δίκτυο.</p> <p>Ο σκοπός της παρούσας διπλωματικής εργασίας είναι διμερής: (1) η παρουσίαση υπαρχόντων στοχαστικών μοντέλων και (2) η ανακάλυψη νέων στοχαστικών μοντέλων για την αφαιρετικοποίηση της εμπιστοσύνης στο διαδίκτυο.</p>
<b>Προαπαιτούμενα</b>	Πολύ καλή γνώση βασικής Θεωρίας Πιθανοτήτων και Πιθανοτικών Τεχνικών
<b>Συνεπίβλεψη</b>	Επίκουρος Καθηγητής Σωτήρης Νικολετσέας και Δρ. Χριστόφορος Ραπτόπουλος

#### **ΣΗΜΕΙΩΣΗ**

Όσοι θέλουν να υποβάλλουν την υποψηφιότητά τους, να καταθέσουν:

(α) Αίτηση για (2) το πολύ διπλωματικές εργασίες με σειρά προτίμησης

(β) Οι αιτήσεις υποψηφιοτήτων πρέπει να συνοδεύονται από φωτοτυπία Αναλυτικής Βαθμολογίας του φοιτητού όπως κρατείται στη Γραμματεία του Τμήματος.

(γ) Οι αιτήσεις πρέπει να κατατεθούν έως και την Δευτέρα 31 Οκτωβρίου 2011 (μέχρι τις 17:00), για το Καθηγητή Παύλο Σπυράκη, στην Γραμματέα της Διεύθυνσης ΙΤΥΕ, κ. Αγγελική Σταματοπούλου, Κτίριο ΙΤΥΕ, οδός Ν. Καζαντζάκη, Πανεπιστημιούπολη Πατρών. Οι αιτήσεις (με όνομα, τηλέφωνο & email) θα κατατίθενται εγγράφως σε φάκελο (όχι ηλεκτρονικά).