



**ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ**  
**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**  
**ΤΜΗΜΑ ΦΥΣΙΚΗΣ**  
**ΕΡΓΑΣΤΗΡΙΟ ΜΗ-ΓΡΑΜΜΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ,**  
**ΚΥΚΛΩΜΑΤΩΝ & ΠΟΛΥΠΛΟΚΟΤΗΤΑΣ**



**ΠΑΡΟΥΣΙΑΣΗ ΜΕΤΑΔΙΔΑΚΤΟΡΙΚΗΣ ΕΡΕΥΝΑΣ**

Την Τετάρτη 17 Ιουλίου 2024 και ώρα 10:00  
ο μεταδιδακτορικός ερευνητής του Τμήματος Φυσικής

**Δρ. Ιωάννης Καφετζής**

θα παρουσιάσει δημόσια τα αποτελέσματα της μεταδιδακτορικής του έρευνας με αντικείμενο:

**"Σχεδίαση Χαοτικών Συστημάτων και Κβαντικών Εκδοχών τους για Ανάπτυξη  
Μεθόδων Κρυπτογραφίας και Ασφαλούς Μετάδοσης Σημάτων"**

**Επιβλέπων: Χρήστος Βόλος, Αναπληρωτής Καθηγητής**

Η παρουσίαση θα πραγματοποιηθεί με το ψηφιακό λογισμικό ZOOM, μέσω του συνδέσμου:  
<https://authgr.zoom.us/j/4957807556?pwd=MUYwenFGVVJDSC9ybIRjWHVrYkUwUT09>

Ο αυξανόμενος όγκος πληροφορίας που μεταφέρεται κατά τη σύγχρονη επικοινωνία, ιδίως μέσω του διαδικτύου, καθιστά την ασφαλή μετάδοση σημάτων επιτακτική ανάγκη. Η χασοτική κρυπτογραφία είναι μια πολλά υποσχόμενη προσέγγιση στο κομμάτι αυτό, λόγω του εν δυνάμει χαμηλού υπολογιστικού κόστους και της μεγάλης ταχύτητας κρυπτογράφησης, χωρίς την υπονόμευση της ασφάλειας του συστήματος.

Η παρούσα μεταδιδακτορική έρευνα μελέτησε το πρόβλημα της χρήσης διακριτών χασοτικών χαρτών στην κατασκευή κρυπτογραφικών συστημάτων για την ασφαλή μετάδοση σήματος, εφαρμόσιμων σε πραγματικές συνθήκες. Πυλώνες της έρευνας αποτέλεσαν ο σχεδιασμός νέων χασοτικών χαρτών καθώς και κβαντικές εκδοχές τους, η αυτοματοποίηση της δυναμικής ανάλυσης χασοτικών χαρτών, η χρήση τους στο σχεδιασμό γεννητριών ψευδοτυχαίων αριθμών, ο σχεδιασμός σχημάτων κρυπτογράφησης και η επαλήθευση της κρυπτογραφικής ισχύος τους, καθώς και ο σχεδιασμός πρωτοτύπων που επιβεβαιώνουν την εφαρμοσιμότητα των μεθόδων σε πραγματικές συνθήκες.

Επιπλέον, στα πλαίσια του μεταδιδακτορικού αναπτύχθηκαν υπολογιστικά πλαίσια (frameworks) ανοικτού κώδικα που απλοποιούν την δυναμική ανάλυση χασοτικών συστημάτων, την επιτάχυνση σχημάτων χασοτικής κρυπτογραφίας, υφιστάμενων και νέων, μέσω παράλληλης επεξεργασίας σήματος, καθώς και τον αυτοματοποιημένο σχεδιασμό ηλεκτρονικών κυκλωμάτων που εξομοιώνουν χασοτικά δυναμικά συστήματα συνεχούς χρόνου.