

ΕΡΓΑΣΤΗΡΙΟ ΟΠΤΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Θέμα: Χαρακτηρισμός Τυχειότητας Υπερταχέων Γεννητριών Πραγματικά Τυχαίων Αριθμών (ΓΠΤΑ) με το πρότυπο DIEHART (*Randomness Characterization of Ultra-fast True Random Number Generators using DIEHART suite*)

Οι φυσικές πηγές τυχαίων αριθμών βασίζονται σε εγγενώς τυχαίες και μη προβλέψιμες φυσικές διεργασίες. Μια ΓΠΤΑ θα πρέπει να είναι μη προβλέψιμη, μη επαναλήψιμη και στατιστικά αμερόληπτη. Αρχικά, διαδικασίες παραγωγής τυχαίων γεγονότων οι οποίες στηρίζονται σε φυσικές διεργασίες, όπως είναι το ρίξιμο ενός ζαριού, το ανακάτεμα των χαρτιών μιας τράπουλας και η περιστροφή του τροχού της ρουλέτας, χρησιμοποιήθηκαν ευρέως σε τυχερά παιχνίδια. Στη σύγχρονη εποχή, στοχαστικά φυσικά φαινόμενα, όπως ο φωτονικός θόρυβος, ο θερμικός θόρυβος στις αντιστάσεις και η μεταπήδηση συχνότητας σε ταλαντωτές, έχουν χρησιμοποιηθεί ως φυσικές πηγές εντροπίας σε μη ντετερμινιστικές γεννήτριες τυχαίων αριθμών. Αυτές οι φυσικές πηγές τυχειότητας όμως περιορίζονται σε πολύ χαμηλούς ρυθμούς σε σχέση με αυτούς των γεννητριών ψευδοτυχαίων αριθμών (μόλις μερικές δεκάδες Mb/s). Μόλις το 2008 προτάθηκε η αρχή λειτουργίας μιας γεννήτριας πραγματικά τυχαίων αριθμών, στην οποία γίνεται χρήση οπτικών χαοτικών σημάτων που παράγονται από ημιαγωγικά laser στα οποία εφαρμόζεται η τεχνική της οπτικής ανάδρασης. Ο ρυθμός παραγωγής ψηφίων που επιτεύχθηκε από αυτή τη γεννήτρια ήταν 1.7 Gb/s. Το Εργαστήριο Οπτικών Επικοινωνιών του ΕΚΠΑ, έχοντας διαθέσιμα κατάλληλα χαοτικά φωτονικά ολοκληρωμένα κυκλώματα έχει πλέον ανεβάσει το ρυθμό αυτό στα 140 Gb/s:

A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris and D. Syvridis, "Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit", *Optics Express*, vol. 18, n. 18, pp. 18763–18768, August 2010)

Για την αξιολόγηση των στατιστικών ιδιοτήτων των ψηφιακών ακολουθιών και την πιστοποίηση της τυχειότητας των παραγόμενων ακολουθιών χρησιμοποιούνται τεστ αναφοράς τα οποία έχουν υιοθετηθεί παγκοσμίως ως πρότυπα, όπως το Standard Statistical Test Suite του National Institute of Standards and Technology (NIST) και τα τεστ Diehard.

Στην παραπάνω εργασία ο ρυθμός των 140 Gb/s πιστοποιήθηκε με το πρότυπο NIST. Στην παρούσα διπλωματική θα πιστοποιηθεί με το πρότυπο Diehart. Ο υποψήφιος θα έχει ως κύρια ενασχόληση την υλοποίηση του κώδικα των μαθηματικών αλγορίθμων του τέστ Diehart στην πλατφόρμα που χρησιμοποιείται στο εργαστήριο, αλλά και την ενσωμάτωση του στο χαρακτηρισμό της ΓΠΤΑ.

Απαιτήσεις:

- Καλή γνώση γλώσσας προγραμματισμού C ή Matlab.
- Συμμετοχή και σε πειραματικές μετρήσεις στο Εργαστήριο Οπτικών Επικοινωνιών.

Κίνητρα:

- Ενασχόληση με έναν τομέα στον οποίο το Εργαστήριο Οπτικών Επικοινωνιών του τμήματος Πληροφορικής και Τηλεπικοινωνιών του ΕΚΠΑ συγκαταλέγεται μέσα στις κορυφαίες ομάδες παγκοσμίως.
- Εξοικείωση με τηλεπικοινωνιακό εξοπλισμό συστημάτων οπτικών επικοινωνιών.
- Δυνατότητα δημοσιεύσεων.

Επιστημονικός υπεύθυνος:	Καθ. Δημήτριος Συβρίδης
Επιβλέπων:	Δρ. Απόστολος Αργύρης
Πληροφορίες:	Γραφείο Ι5