**Προτεινόμενη Άσκηση για το Μάθημα υλικο-λογισμικού**

Οι φυσικές μη-κλωνοποιήσιμες συναρτήσεις είναι συστήματα υλικού που ή ίδια η δομή τους εμπεριέχει μια εγγενή τυχαιότητα η οποία δεν μπορεί να προβλεφθεί αλλά ούτε και να αναπαραχθεί από τον κατασκευαστή του υλικού. Αυτό το «τυχαίο» χαρακτηριστικό θα πρέπει να είναι εξαιρετικά δύσκολο να το μαντέψει κάποιος ή να το αναπαράγει αλλά ο νόμιμος ιδιοκτήτης (που έχει στη κατοχή του τη διάταξη) θα πρέπει με πολύ εύκολο τρόπο να μπορεί να το υπολογίζει.

Στη βιβλιογραφία έχει προταθεί ότι μια τέτοια διάταξη μπορεί να είναι τα στοιχεία μνήμης. Πιο συγκεκριμένα η SRAM η οποία χρησιμοποιείται σε ενσωματωμένες διατάξεις παρουσιάζει την ιδιαιτερότητα ότι σε κάθε έναρξη της διάταξης (χρήση τροφοδοσίας) τα flip-flop κανονικά δεν θα έπρεπε να έχουν καμία προτίμηση στην αρχική τιμή 0 ή την αρχική τιμή 1. Πιο συγκεκριμένα θα έπρεπε σε κάθε έναρξη της διάταξης οι αρχικές τιμές θα έπρεπε να είναι τυχαία 0-1, παρόλα αυτά λόγω μη προβλέψιμων-τυχαίων διακυμάνσεων κατά την κατασκευή της διάταξης τα flip-flop κλειδώνουν σε σταθερές τιμές οι οποίες παραμένουν σταθερές.

Αυτές οι σταθερές τιμές εξαρτώνται από νανο-μεταβολές στην κατασκευή και άρα είναι μοναδικές για κάθε τσιπάκι μνήμης. Σκοπός της άσκησης είναι η ανάπτυξη κώδικα για τη πλατφόρμα Arduino uno, όπου θα διαβάζει το σύνολο της ελεύθερης SRAM μετά την αρχικοποίηση της διάταξης.

* Θα αποκτά πρόσβαση στην SRAM και θα εντοπίζει τα σταθερά byte (non-radical) όταν το σύστημα γίνεται power-on και θα τα στέλνει μέσω της σειριακής θήρας επικοινωνίας σε ένα αρχείο.
* Eεπεξεργασία των αποτελεσμάτων και μελέτη «τυχαιότητας» σε ένα PC κάνοντας χρήση του πακέτου NIST. ( <https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software> )
* Υλοποίηση πρωτοκόλλου challenge response για αυθεντικοποίηση μέσω της σειριακής (προαιρετικό).

Υλικό που θα χρησιμοποιήσει η ομάδα είναι:

Βιβλίο που περιγράφει αναλυτικά την έννοια των PUF

<https://link.springer.com/book/10.1007/978-3-642-41395-7>

Διπλωματική που περιέχει κώδικα και οδηγίες για Arduino mega

<https://github.com/Tribler/software-based-PUF>

Ενδιαφέρον link

<https://forum.arduino.cc/index.php?topic=277158.0>

Στα πλαίσια της άσκησης θα πρέπει να ετοιμαστεί ένα σύντομο τμήμα βασισμένο σε βιβλιογραφία για τον ορισμό, χρήσεις υλοποιήσεις ακολουθούμενο από την υλοποιήση.