Απλή μέθοδος κρυπτογράφησης

Μάθημα: Γλώσσες Περιγραφής Υλικού Ι (CST304 / 2010-2011)
Διδάσκων: Νικόλαος Καββαδίας
nkavv@uop.gr
20/04/2011

Αντικείμενο της εργασίας

Αντικείμενο αυτής της εργασίας είναι η περιγραφή σε Verilog HDL ενός κυκλώματος κρυπτογράφησης και αποκρυπτογράφησης αποθηκευμένου μηνύματος. Ο αλγόριθμος χρησιμοποιεί κλειδί key των 8-bit το οποίο εφαρμόζει σε όλα τα αποθηκευμένα δεδομένα. Τα κρυπτογραφημένα δεδομένα αποθηκεύονται στις ίδιες θέσεις (in-place computation) με τα αρχικά δεδομένα. Η διαδικασία συνεχίζεται μέχρις ότου να κρυπτογραφηθεί όλος ο πίνακας οπότε και valid = 1. Η θεωρούμενη μνήμη ζητείται να υλοποιηθεί ως RAM ασύγχρονης ανάγνωσης διαστάσεων 128x5-bit. Θεωρείστε ότι κάθε θέση μνήμης των 5-bit μπορεί να χρησιμοποιηθεί για ένα αλφάβητο 32 χαρακτήρων όπως το εξής: **`#abcdefghijklmnopqrstuvwxyz ?!.,`**

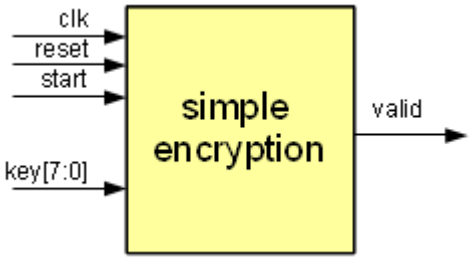
Τα αρχικά δεδομένα της μνήμης μπορούν να δοθούν με ένα μπλοκ λογικής **`initial`** το οποίο θα δίνει τα αρχικά περιεχόμενα της μνήμης (δώστε όποιες τιμές επιθυμείτε αρκεί να είναι από 5'b00000 ως 5'b11111). Η μνήμη μπορεί να υλοποιηθεί είτε ως συνθέσιμη μνήμη σε ξεχωριστό αρχείο ram.v είτε ως μη-συνθέσιμη μνήμη δηλωμένη ως reg κατάλληλου τύπου μέσα στο ίδιο module. Για τον έλεγχο ορθής λειτουργίας να χρησιμοποιηθεί κλειδί key = 8'd11 και key = 8'd31.

Η διαδικασία της κρυπτογράφησης δίνεται στο Σχήμα 1 με τη μορφή κώδικα ANSI C χαμηλού επιπέδου. Η ίδια διαδικασία μπορεί να χρησιμοποιηθεί και για την αποκρυπτογράφηση κρυπτογραφημένου μηνύματος.

```
STATE_1:
  i = 0; goto STATE_2;
STATE_2:
  if (i < 128) {goto STATE_3;} else {goto STATE_8;}
STATE_3:
  c = mem[i]; goto STATE_4;
STATE_4:
  c = c ^ k; goto STATE_5;
STATE_5:
  mem[i] = c; goto STATE_6;
STATE_6:
  k = k + c; goto STATE_7;
STATE_7:
  k = k & 31; i = i + 1; goto STATE_2;
STATE_8:
  valid = 1;
}
```

Σχήμα 1: Ψευδοκώδικας για τον αλγόριθμο κρυπτογράφησης.

Ενδεικτική διεπαφή του κυκλώματος δίνεται στο Σχήμα 2, και οι θύρες εισόδου και εξόδου περιγράφονται αναλυτικά στον Πίνακα 1.



Σχήμα 2: Η διεπαφή του κυκλώματος κρυπτογράφησης.

Πίνακας 1: Θύρες εισόδου και εξόδου για το κύκλωμα.

Θύρα	Εύρος bit	Κατευθυντικότητα	Περιγραφή
clk	1	Είσοδος	Είσοδος ρολογιού
reset	1	Είσοδος	Επανατοποθέτηση
start	1	Είσοδος	Σήμα ενεργοποίησης
key	8	Είσοδος	Κρυπτογραφικό κλειδί
valid	1	Έξοδος	Επιβεβαίωση εγκυρότητας της εξόδου

Παράδοση και βαθμολόγηση της εργασίας

Στην εργασία του μαθήματος, ο φοιτητής καλείται

- να παραδώσει την περιγραφή του κυκλώματος που σχεδίασε σε Verilog HDL
- να αναπτύξει σε κείμενο την περιγραφή της λειτουργίας του κυκλώματος
- να παρουσιάσει αποτελέσματα (π.χ. κυματομορφές, αρχεία εισόδου/εξόδου) τα οποία να αποδεικνύουν τη σωστή λειτουργία του κυκλώματος

Η εργασία παραδίδεται σε τυπωμένη μορφή (με το συνολικό κώδικα Verilog HDL) και υποβάλλεται σε ηλεκτρονική μορφή (PDF της εργασίας + αρχεία κώδικα) στο email του διδάσκοντα. Οι φοιτητές μπορούν να παραδώσουν τις εργασίες τους το αργότερο μέχρι και την ημέρα των εξετάσεων της περιόδου Ιουνίου-Ιουλίου 2011. Εργασία η οποία θα παραδοθεί μετά το πέρας αυτής της ημερομηνίας, δεν θα βαθμολογηθεί ώστε να ληφθεί υπόψη για τις εξετάσεις της περιόδου Ιουνίου-Ιουλίου.

Μια εργασία βαθμολογείται με άριστα το 10. Μη εμπρόθεσμη παράδοση εργασίας συνεπάγεται το βαθμό μηδέν (0).

Η εργασία του μαθήματος είναι υποχρεωτική.