Περίληψη

Βασικό αντικείμενο, αυτής της εργασίας, όπως μαρτυρά και ο τίτλος της είναι η ανάλυση διαφόρων υλοποιήσεων του αλγορίθμου κρυπτογράφησης AES , που προκύπτουν από την χρήση του εργαλείου Xilinx Vivado HLS. Πιο συγκεκριμένα, γίνεται ανάλυση της επίδοσης ενός αλγορίθμου κρυπτογράφησης, καθώς χρησιμοποιούμε τρείς διαφορετικές υλοποιήσεις. Εφόσον, φτιάξαμε τις υλοποιήσεις ώστε να είναι συνθέσιμες για το εργαλείο που χρησιμοποιούμε, τις κάνουμε σύνθεση. Μετά την σύνθεση, μπορέσαμε να βρούμε τις αποδόσεις των τριών διαφορετικών υλοποιήσεων. Εφόσον, λάβαμε γνώση τις αποδόσεις, εντοπίσαμε τις διαφορές των υλοποιήσεων αυτών. Στην συνέχεια, εφόσον έχουμε εντοπίσει τις διαφορές μπορέσαμε πιο εύκολα να δούμε τον λόγο για την διαφορά των αποδόσεων που υπάρχουν. Έπειτα, χάρις κάποιες παραμετροποιήσεις που κάναμε στην πιο αργή υλοποίηση και κάποιων εργαλείων που μας παρέχει το εργαλείο HLS, μπορέσαμε να μεγαλώσουμε την απόδοση αυτηνής της υλοποίησης, σε ένα πολύ ικανοποιητικό επίπεδο. Στο τέλος, συμπεραίναμε ότι με την σωστή γραφή του κώδικα καθώς με την χρήση των κάποιων εργαλείων που μας προσφέρει το λογισμικό μπορούμε να φτιάξουμε κυκλώματα με υψηλή απόδοση.

Απόδοση στα αγγλικά:

The main object of this work, as evidenced by its title, is the analysis of various implementations of the AES encryption algorithm resulting from the use of the Xilinx Vivado HLS tool. More specifically, the performance of an encryption algorithm was analyzed, as we used three different implementations. Since we've made the implementations to be synthesized for the tool we're using, we're making the synthesis for these implementations. After the synthesis, we were able to find the performances of the three different implementations. Since we learned the odds, we identified the differences from the different three designs. Then, once we have identified the differences, we could more easily see the reason for the difference in yields. Then, thanks to some parameterizations we made to the slower implementation and some of the tools provided by the HLS tool, we were able to increase performance of this implementation to a very satisfactory level. Finally, we concluded that with the correct writing of the code, as with the use of some software tools we can make high performance circuits.