Fully asynchronous QDI implementation of DES in FPGA

Jan Bělohoubek, Jan Schmidt
Faculty of Information Technology
Czech Technical University in Prague

Abstract

Aim of this work is to probe methodology for asynchronous system prototyping and synthesis on traditional (synchronous) FPGAs. As a demonstration circuit, we have chosen DES cipher for its relatively small complexity. Dual rail logic, which uses two signals to transmit one logic value, was chosen for signalization. Quasi delay intensive model (QDI) was used as main timing model.

By using dual rail logic and asynchronous paradigm, better DPA resistivity was expected as a bonus, because of similarities with *WDDL*. Asynchronous dual rail logic looks similar to WDDL logic, but in asynchronous circuits the dual rail logic is used primarily for synchronization. In WDDL, dual rail logic is used only for masking purposes – it was developed to mask processed values in power traces to reduce DPA attack vulnerability, but it is fully synchronous.

Asynchronous implementation includes additional completion detection circuits, causing additional delays and variable frequency.