Arithmetic for Crypto in FPGA: HDL or HLS?

Arnaud Tisserand*[1]

[1]CNRS, Lab-STICC – CNRS : UMR6285 – France

Résumé

When implementing arithmetic for cryptographic circuits, choosing an appropriate design method among HDL and HLS is key for short research projects. Hardware description languages (HDL), such as VHDL or Verilog, and related synthesis tools allow to master low level details but require important efforts. High-level synthesis (HLS) uses "higher" level languages, such as C, and specific tools to quickly produce circuits but with a much reduced control in implementation details. Only very basic arithmetic support is available in HDL and HLS. Based on research work done in recent years, we will illustrate some of their pros and cons.

*Intervenant