Enhanced FPGA Implementation of the Hummingbird Cryptographic Algorithm

http://www.firstlight.cn 2010-11-18

Hummingbird is a novel ultra-lightweight cryptographic algorithm aiming at resource-constrained devices. In this work, an enhanced hardware implementation of the Hummingbird cryptographic algorithm for low-cost Spartan-3 FPGA family is described. The enhancement is due to the introduction of the coprocessor approach. Note that all Virtex and Spartan FPGAs consist of many embedded memory blocks and this work explores the use of these functional blocks. The intrinsic serialism of the algorithm is exploited so that each step performs just one operation on the data. We compare our performance results with other reported FPGA implementations of the lightweight cryptographic algorithms. As far as author's knowledge, this work presents the smallest and the most efficient FPGA implementation of the Hummingbird cryptographic algorithm.

存档文本