SHA-1 算法的高速 ASIC 实现

杜晓婧 1,2,李树国 1,2
（1 清华大学 微电子学研究所，北京 100084；2 清华信息科学与技术国家实验室，北京 100084）

摘　要： SHA-1 算法是一种国际标准的安全杂凑算法.为提高 SHA-1 算法的吞吐率，提出了一种新的五合一架构，该架构使 SHA-1 算法的迭代压缩由原来的 80 轮变为 16 轮，并可使每轮中某些 f 函数和部分加法移到关键路径外，从而缩短了关键路径，提高了吞吐率.在 SMIC 65 nm 的工艺下，吞吐率达到 12.68 Gb/s，高于已发表的同类设计.

关键词： SHA-1 算法；高吞吐率；ASIC 实现；逻辑化简

The High-Throughput ASIC Implementation of SHA-1 Algorithm

DU Xiao-jing1,2，LI Shu-guo1,2

(1 Institute of Microelectronics, Tsinghua University, Beijing 100084, China;
2 Tsinghua National Laboratory for Information Science and Technology, Beijing 100084,China

Abstract： SHA-1 algorithm is one of the national standard for Secure Hash Algorithm. For the sake of accelerating the throughput of SHA-1 algorithm, a new 5-in-1 structure is proposed in this paper. This structure reduces the compression function from original 80 rounds to 16 5-in-1 rounds and in each round some functions f and adders can be moved out of the critical path. Based on this, we can shorten the critical path and increase the throughput. In SMIC 65nm technology, the throughput of SHA-1 can achieve 12.68 Gb/s, which is higher than that of other reported designs and can meet the requirement of high throughput. This design also supports resuming transfer.

Key words： SHA-1 algorithm; high throughput; ASIC implementation; logical simplification

作者简介：
杜晓婧　女，(1990-)，硕士研究生.研究方向为信息安全算法及其大规模集成电路设计与实现.
E-mail:duxiaojing1727@163.com.
李树国　男，(1963-)，教授，博士生导师.研究方向为信息安全算法及其大规模集成电路设计与实现.