SM4 算法 CBC 模式的高吞吐率 ASIC 实现

符天枢 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： 由于 SM4 算法在 CBC 模式下存在从电路的输出端到输入端的反馈路径，所以流水线技术难以提高电路的吞吐率.针对这一问题，提出一种逻辑化简方法，使 SM4 加解密算法中每一个轮函数的关键路径减少 1 级异或门延时.基于这种方法，实现了一种 4 轮合 1 的 SM4 电路，在该电路的关键路径中可以减少 4 级异或门延时，且该电路与本文的其他方案相比有更高的单位面积吞吐率.ASIC 实现的综合结果表明，4 轮合 1 的 SM4 电路在 CBC 模式下的吞吐率达到 5.24 Gb/s，高于已发表的同类设计.

关键词： SM4；CBC 模式；高吞吐率；ASIC 实现

A High-Throughput ASIC Implementation of SM4 Algorithm in CBC Mode

FU Tian-shu1,2，LI Shu-guo 1,2

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

Abstract： In CBC mode, pipeline technique does not work on SM4 algorithm to increase throughput, as there is a feedback path from output to input. Over this problem, a logic simplifying method is proposed, which can reduce delay of one stage of XOR gates in each round function of encryption algorithm of SM4. Based on this method, SM4 with a 4-round-in-1 structure is designed, in which, delay of 4 stages of XOR gates can be reduced in the critical path, and this design has a higher throughput per unit area than the other schemes in this paper. Synthesis results show that the ASIC implementation of SM4 with a 4-round-in-1 structure can achieve 5.24 Gb/s in throughput, which is higher than that of reported designs.

Key words： SM4; CBC mode; high-throughput; ASIC implementatio

作者简介：
符天枢　男，（1989-），硕士研究生.研究方向为信息安全算法的数字大规模集成电路设计与实现.
E-mail:fts13@mails.tsinghua.edu.cn.
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.