KASUMI算法的芯片设计与实现

许静雯，李树国
（清华大学 微电子学研究所，北京 100084）

摘 要：KASUMI算法是第三代移动通信系统(3G)使用的一种加密算法.提出一种二合一结构来实现KASUMI算法的芯片设计，依据此二合一结构，KASUMI算法由原始的八轮循环迭代减少为四轮，从而降低了时钟周期数，提高了吞吐率.同时，该设计还实现了f8加密和f9完整性验证两种模式.基于SMIC 0.13 μm CMOS工艺的综合结果表明，KASUMI算法的时钟频率为123.4 MHz，面积为13 979门，吞吐率为1.97 Gb/s，与其他同类方法相比，提高了23%.

关键词：KASUMI；f8；f9；二合一
中图分类号：TN49 **文献标识码**：A **文章编号**：1000－7180(2015)11－0074－04

Design and Implementation of KASUMI Algorithm in Chip

XU Jing-wen, LI Shu-guo
(Institute of Microelectronics, Tsinghua University, Beijing 100084, China)

Abstract: KASUMI algorithm is an encryption algorithm used in the third generation mobile communication system (3G). In this paper, we propose a two-in-one architecture to complete the design of KASUMI algorithm in chip. Based on the architecture, the iteration of the loop in KASUMI algorithm reduces from original 8 rounds to 4 rounds. Therefore, the number of clock cycles of the design is reduced and the throughput is improved. Additionally, the design still implements the encryption of f8 mode and the integrity verification of f9 mode. Using SMIC 0.13 μm CMOS technology, clock frequency of this design and the count of the gates are 123.4 MHz and 13979gates respectively. Most importantly, the throughput achieves 1.97Gbps, which is 23% faster than previous results.

Key words: KASUMI; f8; f9; 2-in-1

作者简介：
许静雯 女，(1990-)，硕士.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: xujingwen_career@163.con.
李树国 男，(1963-)，教授，博士生导师.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.

收稿日期：2014－12－29；**修回日期**：2015－01－30
基金项目：国家"八六三"计划项目(2012AA012402)；清华大学自主研发计划(2011Z05116)