SM3 算法高速 ASIC 设计及实现

于永鹏，严迎建，李　伟

（解放军信息工程大学 密码工程学院，河南 郑州 450001）

摘　要： 详细介绍了 SM3 算法流程，对其控制流和数据流进行相应的硬件设计.控制流硬件设计中，重点分析了消息填充过程中状态机的设计；数据流硬件设计中，提出一种双路并行结构加法器（Two Parallel Road Adder，TPRA）的设计方法，同时结合 CSA 结构的应用，极大地优化了关键路径的时钟延时，最终完成 SM3 算法高速 ASIC 设计.在 65 nm 工艺库下进行综合，数据吞吐率可以达到 3.37 GB/s，能够满足快速、高效地生成消息摘要的需求.

关键词： SM3；控制流；数据流；双路并行；ASIC

High Speed ASIC Design and Implementation of SM3 Algorithm

YU Yong-peng，YAN Ying-jian，LI Wei

(Academy of Cryptography Engineering, PLA Information Engineering University， Zhengzhou 450001, China)

Abstract： The process of SM3 algorithm is introduced in detail, and the hardware of the control flow and the data flow are designed. In the design of the control flow, the design of state-machine is analyzed in this paper emphatically in the process of message filling. In the design of the data flow, a new structure of adder called Two Parallel Road Adder is put forward. Combined the application of CSA structure, the clock delay of the critical path has been optimized greatly and at last this paper finish high speed ASIC design of SM3 algorithm. Compiling under the 65 nm technology library, data throughput can reach 3.37 GB/s. The design proposed in this paper could meet the need of fast and efficient message abstract generating.

Key words： SM3; control flow; data flow; TPRA; ASIC

作者简介：

于永鹏　男，（1991-），硕士研究生.研究方向为安全芯片设计与防护.E-mail：1228964300@qq.com.

严迎建　男，（1973-），博士，教授.研究方向为密码芯片安全防护.

李　伟　男，（1983-），博士研究生，讲师.研究方向为专用集成电路设计.