基于 AES 算法的 DSP 安全防护设计实现

张猛华，陈振娇，徐新宇

（中国电子科技集团公司第五十八研究所，江苏 无锡 214035）

摘　要：针对 DSP 系统数据安全防护的应用需求，在不改变 DSP 功能的基础上提出一种基于 AES 算法的新安全应用机制.该机制单独集成 AES 解密模块，通过软件实现数据的传输控制，优化 AES 算法并采用解密密钥预先写入 OTP（One Time Programable）的方式代替密钥扩展模块的设计，降低硬件设计的复杂度，以最优的资源实现数据的安全防护功能.为保证面积的兼容一致性，通过优化布局，将版图密度由原先的 55%提升到 70%，电路一次设计成功，用户使用结果表明，在 100 MHz 工作频率下，电路的安全性能、数据处理速度及电特性参数均满足系统的应用需求.

关键词：　DSP；AES 算法；安全防护；加/解密

Design and implementation of DSP security protection based on AES algorithm

ZHANG Meng-hua，CHEN Zhen-jiao，XU Xin-yu

（China Electronics Technology Group Corporation No.58 Research Institute，Wuxi 214035，China）

Abstract：To meet the application requirement of DSP system data security protection， a new security application mechanism based on AES algorithm is proposed without changing the DSP function. This mechanism integrates AES decryption module separately， and realizes data transmission control through software， optimizes the AES algorithm and replaces the design of the key extension module with the decryption key pre-written into the OTP， reduces the complexity of the hardware design， and realizes the data security protection function with the optimal resources. In order to ensure the compatibility and consistency of the area， the layout density was increased from 55% to 70% by optimizing the layout， and the circuit was successfully designed at the first time. The user's application results showed that the safety performance， data processing speed and electrical characteristic parameters of the circuit all met the application requirements of the system under the working frequency of 100MHz.

Key words：　DSP；AES algorithm；security protection；encrypt/decrypt

作者简介：

张猛华　男，（1979-），硕士，高级工程师.研究方向为数字信号处理器设计、超大规模集成电路设计.

陈振娇（通讯作者）　男，（1987-），硕士，工程师.研究方向为数字信号处理器设计.E-mail:czj_587@163.com.

徐新宇　男，（1979-），硕士，高级工程师.研究方向为数字信号处理器设计、超大规模集成电路设计