

doi:10.1631/FITEE.1601346

**题目：**使用串行外设接口协议的混沌数字加密系统及其 dsPIC 实现

**概要：**当前数字通信的大规模使用需要嵌入式系统（embedded system, ES）和协议级数据加密来实现安全连接。串行外设接口（serial peripheral interface, SPI）协议被 ES 和集成电路制造商广泛应用于有线和无线通信等领域。提出一种应用于 SPI 通信协议的混沌加密和解密算法的设计及其实验实现。混沌加密算法及对应解密算法的设计基于混沌 Hénon 映射和两种模糊和排列方法（结合 DNA 序列）。考虑到对称密钥，SPI 协议采用 16 位配置作为同步发射机和接收机。使用两个低成本 dsPIC 微控制器作为 ES，设计结果得到实验验证。基于其数字信号处理属性，SPI 数模转换器被用于处理、获取和重构机密消息。最后，统计检验证明了加密的安全性。该算法数字处理能力得到 dsPIC 微控制器验证。

**关键词：**混沌系统；统计测试；嵌入式系统；dsPIC 微控制器；串行外设接口（SPI）协议