成果名称：高性能小面积AES密码电路设计方法

委托方名称：安徽工程大学

项目简介：

1.创新性：本成果提出的基于合成矩阵的AES密码电路结构，采用常数矩阵合并与组合运算技术减少电路面积和缩短关键路径，与运算单元单独实现方式相比，具有更小的电路面积和更高的电路性能。

2.成熟度：本成果已获得授权专利5项，整体电路的Verilog代码，Xilinx FPGA、Synopsis DC电路综合报告。

3.所属行业和应用领域：本成果属于信息安全行业，具体属于密码芯片优化设计技术领域。

4.市场前景：加密技术是信息安全的重要手段之一，AES加密算法是目前国际上最流行的分组密码算法，绝大多数国内外密码芯片中都集成了AES加密算法硬件电路。本发明中的AES解密普通轮变换电路结构可以进一步减少AES密码电路面积，提高电路性能，从而拓宽密码芯片应用范围，提高密码芯片性能，特别是可以进一步扩大密码芯片在资源受限应用领域中应用范围。

转让底价（万元）：10

项目图片：（如有）无

交易机构：安徽联合技术产权交易所；

交易机构联系人：沈工 管工 0551-65909080 65909081；

地址：安徽创新馆3号馆1楼。