<table>
<tr><td>论文题目</td><td colspan="3">Constructing S-boxes for lightweight cryptography with Feistel structure</td></tr>
<tr><td>申请人</td><td colspan="3">李永强</td></tr>
<tr><td>论文作者</td><td>李永强，王明生</td><td>索引机构</td><td>□ SCI
☑ EI
□ ISTP</td></tr>
<tr><td>期刊/
会议信息</td><td colspan="3">Workshop on Cryptographic Hardware and Embedded Systems 2014 (CHES 2014), LNCS 8731, Page(s) 127-146.
CCF网络与信息安全方向B类国际会议。</td></tr>
<tr><td>申请人自述</td><td colspan="3">轻量级密码算法是对称密码近年的研究热点之一，主要用于资源受限的环境。由于资源受限，要求轻量级密码算法在提供安全保障的同时，具有低的硬件实现代价。如何构造具有高安全强度和低实现代价的部件是设计轻量级密码时的首要问题。

S 盒是对称密码算法的关键部件之一。作为一个非线性部件，S 盒的硬件实现代价通常较高。此外，差分均匀度和非线性度是 S 盒两个最基本的密码学性质，分别衡量了 S 盒抵抗差分攻击和线性攻击的能力。因此，研究如何构造具有最佳差分均匀度和非线性度并且硬件实现代价低的 S 盒，具有十分重要的理论以及实际应用意义。

本文利用 Feistel 结构给出了适用于轻量级分组密码算法的 S 盒的构造。论文分析了此方法构造的 S 盒的密码学性质的界。并通过选取适当的轮函数，给出了一类 $GF(2^{2k})$上具有已知最佳非线性度的差分均匀度为 4 的 S 盒。由于 Feistel 结构的特性，该构造同时具有极低的硬件实现代价。论文同时利用非平衡 Feistel 结构给出了最优 4 比特的 S 盒的构造，相关结果可以直接应用于轻量密码算法的设计。

本文发表在国际会议 CHES2014 上。CHES 是国际密码学会（IACR）主办的学术会议之一，是密码硬件方向的顶级会议。每年会有大量来自各国工业界，学术界以及政府部门的人员参加。14 年参加人员 362 人，接收论文 33 篇，皆为大会报告。

到目前为止，包含本文在内，CHES 收录的中国大陆人员独立完成的论文只有三篇，其中 14 年两篇。本文也是 CHES 历史上首篇以实验室为第一单位的论文。</td></tr>
</table>