<table>
<tr><td>论文题目</td><td colspan="3">3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound</td></tr>
<tr><td>申请人</td><td colspan="3">张立廷</td></tr>
<tr><td>论文作者</td><td>（请全体作者签名）</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">ASIACRYPT 2012, LNCS 7658, pp. 296－312, 2012.</td></tr>
<tr><td>申请人自述</td><td colspan="3">分组密码链接模式 CBC（Cipher Block Chaining）以最直接的方式调用分组密码算法，串联它们的输入输出，结构简单、效率最优，是密码方案设计中最常用的基本结构之一。人们对 CBC 结构的研究也由来已久，在此基础上设计了诸多方案（CMAC、CCM 等）并被大量标准化推广。但受限于 CBC 结构自身的特点，目前以此为基础的密码方案，在没有随机量、状态值的帮助下，都无法抵抗生日攻击，这一问题在轻量级应用环境中尤为突出。本文中我们率先证明了，只需对 CBC 结构做简单的修改，并在其末端增加两个不同的分组密码调用，就可以使得 CBC 结构突破生日攻击的限制。由此设计的 3kf9 认证模式是第一个串行的且效率比为 1 的超越生日界模式，不仅具备高安全性，也具备堪比原始 CBC 结构的高效率，为轻量级分组密码的现实应用提供了可靠的选择，也为以后此类工作模式的分析与设计找到了突破口。</td></tr>
</table>