<table>
<tr><td>论文题目</td><td colspan="3">Perfect Algebraic Immune Functions</td></tr>
<tr><td>申请人</td><td colspan="3">刘美成</td></tr>
<tr><td rowspan="3">论文作者</td><td rowspan="3">（请全体作者签名）</td><td rowspan="3">索引机构</td><td>☐ SCI</td></tr>
<tr><td>☐ EI</td></tr>
<tr><td>☐ ISTP</td></tr>
<tr><td>期刊/
会议信息</td><td colspan="3">（请给出刊文的期刊或会议的名称，卷、期、页等信息）
ASIACRYPT 2012, LNCS 7658, 172-189.</td></tr>
<tr><td>申请人自述</td><td colspan="3">（请简述论文的目的和意义,解决了什么问题,有何贡献或影响。总字数不超过 500 字）
代数攻击与布尔函数的代数免疫性是密码学领域近十年来的前沿热点研究课题。该论文巧妙地运用矩阵理论，给出了布尔函数的快速代数免疫性上确界，彻底解决了自 2003 年快速代数攻击提出以来悬而未决的难题,从而解决了完全代数免疫函数的存在性问题。同时证明了 Carlet-Feng 函数具有最优快速代数免疫性，解决了 Carlet 和冯克勤在 2008 年亚洲密码学年会提出的猜想。这是首次发现具有最优快速代数免疫性的布尔函数，突破了实验观察的瓶颈，开创了数学证明的先例。</td></tr>
</table>