<table>
<tr><td>论文题目</td><td colspan="3">The Nonexistence of Permutations EA-Equivalent to Certain AB Functions</td></tr>
<tr><td>申请人</td><td colspan="3">李永强</td></tr>
<tr><td rowspan="3">论文作者</td><td rowspan="3"></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">IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 59, NO. 1, 672-679, JANUARY 2013。
期刊为信工所推荐学术刊物列表A类。</td></tr>
<tr><td>申请人自述</td><td colspan="3">GF(2^n)上的置换多项式在密码学中有着重要的应用，如对称算法中的S盒。当 n 奇数时，GF(2^n)上非线性度最高的函数称为AB函数。由于AB函数是GF(2^n)上多项式中具有最佳抵抗线性攻击能力的函数，因此是密码函数中一类重要的研究对象。

1998年，密码学家C.Carlet, P.Charpin和V.Zinoviev在“Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems” (DCC, 15, 125-156，1998)一文中提出如下猜想：“任何一个AB函数都EA等价于置换”。

2005年，L.Budagyhan, C.Carlet和A.Pott在“New classes of almost bent and almost perfect nonlinear polynomials” (IEEE Trans. Inf. Theory, 52(3), 1141–1152, 2006) 中证明了$x^{2^i+1}+(x^{2^i}+x)\mathrm{Tr}(x^{2^i+1}+x)$是AB函数。并且在GF($2^5$)上，通过计算机搜索验证了该函数是上述猜想的一个反例。

在本文中，我们证明了该反例在一般的情况下都成立，从而完全否证了前述猜想。此外，论文深入研究了GF(2^n)上形如$L(x^{2^i+1})+x$的置换多项式。当 $\dim(\mathrm{Ker}(L))\le n-2$ 时，给出了使得上述多项式为置换的$L(x)$的完全刻画。

论文中的结果被审稿人评价为：“The paper presents very interesting results”；“Proving this theoretically and in general is an important progress”。</td></tr>
</table>