具有多种优良密码性质的布尔函数的设计：优化和折中

张卫国
（西安电子科技大学）

本文简要介绍作者2014年在密码函数设计这一课题取得的研究成果。

一 提出一种新型密码函数设计方法——GMM构造法

流密码系统的安全性依赖于密码函数的密码学指标是否优良，如何设计同时抵抗所有已知攻击的密码函数是困扰密码学界的难题。为了抵抗BAA攻击、相关攻击、BM攻击、代数攻击、快速代数攻击，要求密码函数具有高非线性度、弹性（平衡且相关免疫）、高代数次数、高代数免疫阶、高快速代数免疫阶等性质指标。把有关流密码安全的多种指标加以综合研究的意义重大，而目前已知的密码函数设计方法在处理多指标折中优化时，总是顾此失彼，比较多的研究是同时兼顾2–3个密码学指标。

Maiorana–McFarland（MM）构造技术是上世纪九十年代初由Camion等人提出[1]。在之后的二十余年里，这种构造技术衍生出许多变种版本，这些构造方法具有以下无法克服的缺陷：a）弹性密码函数非线性度都不高于$2^{n-1}-2^{\lfloor n/2 \rfloor}$；b）代数免疫性质较差；c）不能抵抗快速代数攻击。

我们提出Generalized Maiorana–McFarland（GMM）构造技术[2]，在保持传统MM构造技术优点的前提下，扬长避短，通过对定义在不同向量空间上的线性函数进行广义毗连，得到一系列用已知方法（包括传统MM构造技术）不能得到的密码函数。GMM构造技术可以实现多种密码指标的优化折中，使密码函数同时具有如下优势：

> 严格几乎最优的非线性度（抵抗BAA攻击）；
> 具有弹性（抵抗相关攻击）；
> 最优代数次数（抵抗BM攻击）；
> 最优代数免疫（抵抗代数攻击）；
> 优良快速代数免疫（抵抗快速代数攻击）；
> 便于硬件实现（较少的硬件代价）。

从代数攻击和快速代数攻击提出后，人们对基于LFSR的流密码系统的安全性抱有悲观态度，如何设计同时满足多种密码学指标的密码函数是保证这类流密码系统安全性的核心难题。由GMM构造技术得到的密码函数，可以实现多种密码学指标的折中，又具有硬件实现的简易性。

上世纪九十年代，大量的工作研究了如何设计密码函数使其同时满足弹性和高非线性度；2000年的美国密码学年会上(CRPTO2000)，P. Sarkar和S. Maitra正式提出“弹性函数的非线性度紧上界”这一公开问题[3]。这一难题可通俗地描述为：在弹性阶确定的前提下，布尔函数的非线性度最大可达到多少呢？在2009年我们把t阶弹性函数的非线性度大幅度提高到接近$2^{n-1}-2^{n/2-1}-2^{n/4-t+1}$，并猜想$t$阶弹性函数的非线性度不超过$2^{n-1}-2^{n/2-1}-2^{n/4-t+1}$[4]. 至今，仍然没有新的结果超过这一界限。

利用GMM构造法可得到另外一大类新型t阶弹性函数，其非线性度比我们2009年的结果略有提高，但仍然没有超过$2^{n-1}-2^{n/2-1}-2^{n/4-t+1}$[2].

“弹性布尔函数的非线性度的紧上界”这一科学难题进展缓慢，这一问题的进展对实践中设计更安全的流密码系统有重要指导意义，同时也有着重要的科学意义。

二 利用不相交线性码技术构造出非线性度严格几乎最优的弹性S盒

S盒在对称密码学中具有举足轻重的地位，它不仅可以作为分组密码的核心部件，也可用于流密码系统以提高加解密速度。在流密码中要求所使用的S盒具有弹性和高

作者简介：张卫国，教授，博士生导师，IEEE高级会员。2001年7月和2007年3月分别在西安电子科技大学获学士和博士学位，2007年7月至今在西安电子科技大学通信工程学院任教。张卫国教授长期从事对称密码学基础理论研究，近年来在密码函数的设计和分析方面取得一系列研究成果。

非线性度。但由于S盒是多输出密码函数，这使得S盒的弹性和非线性度之间存在更强的制约。“是否存在非线性度严格几乎最优的弹性S盒”是这一研究方向的公开问题，我们利用不相交线性码构造出非线性度严格几乎最优的弹性S盒，解决了这一难题[5]。

我们首先解决了“如何把一个线性空间分解成尽可能多的两两互不相交的线性码（线性子空间）”这一瓶颈难题，得到数量极多$[n,k,d]$的不相交码。例如，Niederreiter 2004年发表论文[6]，只找到24个[18,4,6]不相交码，而采用我们的方法可以找到12882个。

我们进一步把上述不相交码技术用于弹性S盒的构造，首次得到非线性度严格几乎最优的弹性S盒，所构造S盒的非线性度远远优于前人结果，有力地证明了这类密码函数的存在性，即非线性度$>2^{n-1}-2^{(n-1)/2}$的弹性S盒是存在并可以构造的。此外，构造的S盒还可以具有较高的代数次数和较好的代数免疫等密码学性质。

三 差分攻击和线性攻击是针对分组密码的主流攻击方式，我们给出两种用于Feistel型分组密码的低差分均匀度、高非线性平衡S盒的设计方案，可有效地抵抗针对分组密码的差分攻击和线性攻击

如何设计具有高非线性度和低差分均匀度的平衡S盒是分组密码设计中的核心问题。我们利用m序列优良的相关性质，结合MM构造技术，设计出非线性度为$2^{n-1}-2^{n/2-1}-2^{\lfloor n/4 \rfloor}$的平衡$(n,m)$S盒[7]。这是平衡$(n,m)$S盒目前所能达到的最高非线性度。以$n$=8为例，$F_{2^8}$上的逆函数$x \to x^{-1}$是AES中采用的核心部件，其非线性度是112；用我们的方法得到的S盒，其非线性度可达到116.

我们还引入差分分布的标准偏差$SD(F)$来度量S盒的差分性质。以n=8为例，我们所设计的函数$SD(F)$=2.203，而AES中的逆函数其标准偏差是3.940.

四 近期其他成果

采用计算机搜索技术，在变元个数较小时，也可以实现各种密码学指标的折中。下面的函数是前人未曾得到过的[8]：(8,1,6,116,4,7); (9,1,7,236,4,8); (10,1,8,484,5,9); (11,1,9,984,5,10); (12,1,10,1988,6,11); (13,1,11,4012,6,12); (14,1,12,8072,7,13)。上述函数的7个指标分别是，变元个数，弹性阶，代数次数，非线性度，代数免疫阶，抵抗快速代数攻击的能力。

参考文献：

[1] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, On correlation immune functions, in Advances in Cryptology – CRYPTO'91, Springer, LNCS 547, pp. 86–100, 1991.P. Sarkar, S. Maitra, Nonlinearity bounds and constructions of resilient Boolean functions, in Advances in Cryptology – CRYPT 2000, LNCS 1880, pp. 515–532, 2000.

[2] WeiGuo Zhang(张卫国),Enes Pasalic,Generalized Maiorana–McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties,IEEE Transactions on Information Theory, vol. 60, no. 10, pp. 6681–6695, 2014.

[3] P. Sarkar and S. Maitra, Construction of nonlinear Boolean functions with important cryptographic properties, in Advances in Cryptology – EUROCRYPT 2000, Springer, LNCS 1807, vol. 1807, pp. 485–506, 2000.

[4] WeiGuo Zhang (张卫国), GuoZhen Xiao (肖国镇), Constructions of almost optimal resilient Boolean functions on large even number of variables, IEEE Transactions on Information Theory, vol. 55, no. 12, pp. 5822–5831, 2009.

[5] WeiGuo Zhang (张卫国), Enes Pasalic, Constructions of resilient S–boxes with strictly almost optimal nonlinearity through disjoint linear codes, IEEE Transactions on Information Theory, vol. 60, no. 3, pp. 1638–1651, 2014.

[6] H. Niederreite, C. Xing, Disjoint linear codes from algebraic function fields, IEEE Transactions on Information Theory, vol. 50, no. 9, pp. 2174–2177, 2004.

[7] WeiGuo Zhang (张卫国), Enes Pasalic,Highly nonlinear balanced S–boxes with good differential properties,IEEE Transactions on Information Theory, vol. 60, no. 12, pp. 7970–7979, 2014.

[8] Jun–Po Yang (杨俊坡), Wei–Guo Zhang (张卫国), Generating highly nonlinear resilient Boolean functions resistance against algebraic and fast algebraic attacks, Security and Communication Networks, vol. 8, pp. 1256 – 1264, 2015.