密码函数的正规性

王维琼[1,2] 肖国镇[1]

(西安电子科技大学ISN国家重点实验室 西安 710071)[1] (长安大学理学院 西安 710064)[2]

摘 要 指出一个好的密码函数除了自身需要具备良好的复杂性外,对其做一个较小的改动后仍需具有良好的复杂性;基于此思想对布尔函数的正规性这一复杂性指标作了改进,定义了扩展的正规性,讨论了扩展正规性和正规性之间的关系以及扩展正规性和代数免疫之间的关系;并从布尔函数代数正规型的角度分析了函数的正规性和代数免疫阶,为正规性和代数免疫的分析提供了一条新的思路。

关键词 密码函数,代数免疫,正规性,代数正规型

中图法分类号 TN918.1 **文献标识码** A

Normality of Cryptographic Boolean Functions

WANG Wei-qiong[1,2] XIAO Guo-zhen[1]

(State Key Laboratory of Integrated Service Network, Xidian University, Xi'an 710071, China)[1]

(College of Science, Chang'an University, Xi'an 710064, China)[2]

Abstract It was pointed out that a good cryptographic Boolean function should also be complex enough after it is changed a little. The generalized normality of Boolean functions based on this theory was introduced. The relation between the normality and generalized normality of Boolean functions, and the relation between the generalized normality and the generalized algebraic immunity were proposed. Finally, the normality and algebraic immunity of Boolean functions from the point of algebraic normal form of Boolean functions were presented, which proposed a new way to analyzing the normality and algebraic immunity of Boolean functions.

Keywords Cryptographic boolean functions, Algebraic immunity, Normality, Algebraic normal form

1 引言

基于Shannon提出混淆及扩散思想,一个好的密码函数必须同时满足平衡性、高非线性性、好的扩散性、高的代数免疫阶、非正规等多个密码学指标。其中正规性这一指标是Dobbertin[1]在1994年构造高非线性的平衡函数时提出的。Carle[2]推广了正规性的概念,指出若一个 n 元布尔函数在某一维 k 子空间或仿射子空间上的限制为常数,则称其为 k 正规的。显然,正规的布尔函数是有缺陷的,而且容易证明若函数为 k 正规,则其必为更低阶的正规,因而我们更关心的是正规阶的上界,希望其越低越好。

与此同时,一个好的密码函数还应满足当给其一个微小的变动时仍然具有良好的复杂性。在本文中仅考虑改变布尔函数在0点处的值。虽然改动前后函数的非线性度只相差1,但代数次数可能相去甚远。其次,函数本身可能具有较复杂的结构,但改动后便是一个很简单的函数。例如:当 $n=3$ 时,设 $f(x)=x_1+x_1x_2+x_1x_3+x_2x_3+x_1x_2x_3$,则改动后函数就变为 $1+x_2+x_3$,从而进行密码分析和攻击时可以从改动后的函数入手,影响了 f 自身的复杂性,所以在考虑密码函数的各项复杂性指标时必须考虑这一因素。文献[3]中指出,在很多情况下改动前后函数的代数免疫阶差1,便会影响函数抗代数攻击的能力。本文正是基于此思想对密码函数的正规性这一复杂性指标进行分析:推广了正规性的定义,讨论了改动前后函数的正规阶上界之间的关系并分析了扩展正规阶上界与扩展代数免疫阶之间的关系。另一方面,对布尔函数正规性的判定一直是个比较困难的问题,因为判定算法要基于寻找所有的 k 维子空间和仿射子空间[4,5],而这需要相当大的计算量。本文提出从布尔函数代数正规型的角度来分析函数的正规性及代数免疫阶,给出了一种新的思路。

2 预备知识

n 元布尔函数 $f(x)$ 定义为映射:$f:F_2^n\to F_2$,其中 $x=(x_1,x_2,\cdots,x_n)\in F_2^n$,并记 B_n 为 F_2^n 上所有 n 元布尔函数的集合。对于 $\forall f(x)\in B_n$,都可以唯一地表达成如下的多项式形式:

$$f(x_1,x_2,\cdots,x_n)=\bigoplus_{a\in F_2^n} g(a_1,a_2,\cdots,a_n)x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \tag{1}$$

其中,$a=(a_1,a_2,\cdots,a_n)$,$g(x)\in B_n$ 为 $f(x)$ 的Mobius变换,$\oplus$表示二元域上的加法。

称表达式(1)为 $f(x)$ 的代数正规型,并称式中的每一项

到稿日期:2009-10-30 返修日期:2009-12-25 本文受国家自然科学基金(60773003)资助。

王维琼(1979-),女,博士生,主要从事信息论与密码理论研究,E-mail:wqwang18@126.com;肖国镇(1934-),男,教授,博士生导师,主要从事密码理论、信息论与编码理论研究。

$x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ 为 $f(x)$ 的一个单项。

定义 1[1,2] 若存在 F_2^n 的一个 $\lceil n/2\rceil$ 维仿射子空间 V，使 $f(x)\in B_n$ 在 V 上的限制为常数(或仿射函数)，则称 $f(x)$ 是(弱)正规的。更一般地，若存在 F_2^n 的一个 $k(1\leqslant k\leqslant n)$ 维仿射子空间 V，使 $f(x)$ 在 V 上的限制为常数(仿射函数)，则称函数 $f(x)$ 为 k-(弱)正规的。

在考虑 $f(x)$ 的正规性这一复杂性指标时，仍需考虑给 $f(x)$ 一个较小的变动后是否仍具有较低的正规阶上界。本文只考虑改变 $f(x)$ 在 0 点处的值以得到一个新的函数 $f^C(x)$。为此先引入函数 $\Delta(x)=(1\oplus x_1)(1\oplus x_2)\cdots(1\oplus x_n)$。显然 $\Delta(\alpha)\neq 0$ 当且仅当 $\alpha=0$，即对于 $\forall x\in F_2^n$，有 $f^C(x)=\Delta(x)+f(x)$，且 $(f^C)^C=f$。又因 $\Delta(x)$ 中包含了关于 $x_1,x_2,\cdots,x_n$ 的所有单项，即 $f^C(x)$ 的代数正规型中包含了所有关于 $x_1,x_2,\cdots,x_n$ 的单项中不在 f 的代数正规型中的项，故称其为 $f(x)$ 的补函数。为区别于许多文献中用 $NL(f)$ 来表示 $f(x)$ 的非线性度，引入了记号 $NN(f)$ 来表示 $f(x)$ 的正规阶上界。

定义 2 设 $f(x)\in B_n$，定义 $f(x)$ 的扩展正规阶上界 $NN^*(f)=\max\{NN(f),NN(f^C)\}$。

定义 3[6,7] 设 $f(x)\in B_n$，若存在 $g(x)\in B_n$，使 $f\cdot g=0$，则称 g 为 f 的一个零化子。记 $AN(f)=\{g\in B_n\mid f\cdot g=0\}$ 为 f 的零化子的集合，称 $AI(f)=\min\limits_{g\neq 0\in AN(f)\cup AN(f+1)}\deg(g)$ 为 f 的代数免疫阶，并定义扩展的代数免疫阶为 $AI^*(f)=\min\{AI(f),AI(f^C)\}$。

3 主要结论

在此，先给出 f 与 f^C 的正规阶上界之间的关系，以及正规阶上界与扩展正规阶上界之间的关系。

定理 1 设 $f(x)\in B_n$，则

(1) $|NN(f)-NN(f^C)|\leqslant 1$；

(2) $0\leqslant NN^*(f)-NN(f)\leqslant 1, 0\leqslant NN^*(f)-NN(f^C)\leqslant 1$。

证明：(1)不妨记 $NN(f)=k$，则有以下两种情形：

1)若存在一 k 维仿射子空间 $a+V$(其中 V 为一 k 维子空间，$a\in F_2^n$)，使得 $f|_{a+V}=\varepsilon_0(\varepsilon_0=0$ 或 1)，则此时仍有 $f^C|_{a+V}=\varepsilon_0$，即 $NN(f^C)\geqslant k$。同时 $NN(f^C)\leqslant k+1$。否则，必存在使得 f^C 为常数的不小于 $k+2$ 维的子空间或仿射子空间，其中包含了一个 $k+1$ 维的仿射子空间 $b+U$，使 $f^C|_{b+U}=\varepsilon_1$，即此时亦有 $f|_{b+U}=\varepsilon_1$，这与 $NN(f)=k$ 矛盾。故 $NN(f^C)\leqslant k+1$，且等式成立当且仅当存在一 k 维子空间 V'，使得 $f|_{(a'+V')\cup V'\setminus\{0\}}=\varepsilon$。

2)若不存在满足条件的 k 维仿射子空间，则必存在一 k 维子空间 V，使得 $f|_V=\varepsilon_0$。此时，V 中必包含一个 $k-1$ 维的仿射子空间 V'，使得 $f|_{V'}=\varepsilon_0$，从而 $f^C|_{V'}=\varepsilon_0$，即 $NN(f^C)\geqslant k-1$。与此同时，$NN(f^C)\leqslant k$。否则，也必存在一 k 维仿射子空间，使 f 在其上为常数，与假设矛盾。且等式成立当且仅当存在另一 k 维的子空间 U，使 $f|_{U\setminus\{0\}}=\varepsilon_1$，且 $\varepsilon_1\neq f(0)$。

综上可知，$|NN(f)-NN(f^C)|\leqslant 1$。

关于结论(2)的证明容易从结论(1)及 $NN^*(f)$ 的定义中得到。证毕。

例 1 当 $n=3$ 时，设 $f(x)=1+x_1+x_2+x_3+x_2x_3$，则 $f^C(x)=x_1x_2+x_1x_3+x_1x_2x_3$，此时有 $NN(f)=2$，而 $NN(f^C)=1$，即 $NN^*(f)=2$。

从定理 1 的证明过程中可以看出，有一大类的函数均满足 $NN^*(f)\neq NN(f)$，因而在考虑正规性时不可忽略 f^C。

文献[8]中指出，k 正规布尔函数的代数免疫阶不超过 $n-k$。类似地可以得到扩展的正规阶与扩展的代数免疫阶之间的如下关系，这里采用不同于文献[8]中的证明方法。

定理 2 设 $f\in B_n$，若 $NN^*(f)=k$，则 $AI^*(f)\leqslant\min\{n-k,\lceil n/2\rceil,\deg(f),\deg(f^C)\}$。

证明：若 $NN(f)=k$，则存在一 k 维的仿射子空间 $a+V$，使得 $f|_{a+V}=\varepsilon(\varepsilon=0$ 或 1)。若 $\varepsilon=0$，则 $a+V$ 的特征函数 $1_{a+V}(x)=\begin{cases}1 & x\in a+V\\ 0 & \text{else}\end{cases}$ 便为 f 的一个零化子，而 $1_{a+V}(x)$ 仿射等价于 $\prod\limits_{i=1}^{n-k}x_i$。另一方面，因代数次数具有仿射不变性，故 $\deg(1_{a+V})=n-k$，即 $AI(f)\leqslant n-k$。当 $\varepsilon=1$ 时，类似可知 1_{a+V} 为 $f+1$ 的零化子。从而由代数免疫的定义可知 $AI(f)\leqslant n-k$。

当 $NN(f^C)=k$ 时，同理可证 $AI(f^C)\leqslant n-k$。

综上可知，$AI^*(f)\leqslant n-k$。另一方面，因 $f+1$ 为 f 的一个零化子，且已知[9]代数免疫阶的上界为 $\lceil n/2\rceil$。故有 $AI^*(f)\leqslant\min\{n-k,\lceil n/2\rceil,\deg(f),\deg(f^C)\}$。证毕。

如在上面的例 1 中，便有 $AI^*(f)\leqslant\min\{3-2,\lceil 3/2\rceil,3,2\}=1$。

在对布尔函数正规性进行判定时，需要寻找所有的 k 维子空间和仿射子空间，这会造成相当大的计算量。而且只知道[10]当 $n\leqslant 7$ 时所有的布尔函数都是 $\lfloor n/2\rfloor$ 正规的，对 $n>7$ 的布尔函数的正规性却没有更好更快的方法。下面从布尔函数的代数正规型的角度对其正规性进行分析，可以得到一个比较简单易行的结论。

引理 1[11] 设 $f(x),g(x)\in B_n$，则下面命题等价：

(1)对于 $\forall\alpha\in F_2^n$，有 $f(\alpha)=\bigoplus\limits_{\beta\leqslant\alpha}g(\beta)$；

(2)对于 $\forall\alpha\in F_2^n$，有 $g(\alpha)=\bigoplus\limits_{\beta\leqslant\alpha}f(\beta)$；

(3) $f(x_1,x_2,\cdots,x_n)=\bigoplus\limits_{a\in {F_2}^n}g(a_1,a_2,\cdots,a_n)x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$；

(4) $g(x_1,x_2,\cdots,x_n)=\bigoplus\limits_{a\in {F_2}^n}f(a_1,a_2,\cdots,a_n)x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$。

其中，$\alpha=(a_1,a_2,\cdots,a_n)$，$\beta=(b_1,b_2,\cdots,b_n)$，$\beta\leqslant\alpha$ 表示 β 被 α 覆盖，即 $\forall 1\leqslant i\leqslant n, b_i\leqslant a_i$。

定理 3 设 $f(x)\in B_n$，I 为 $\{1,2,\cdots,n\}$ 的一个子集。对任意 $i_1,i_2,\cdots,i_t\in I(t>1)$，若 f 的代数正规型中不含有形如 $x_{i_1}x_{i_2}\cdots x_{i_t}$ 的项，则 $NN(f)\geqslant k$，其中 $k=\#I$。

证明：设 $f(x)=\bigoplus\limits_{a\in F_2^n}g(\alpha)x^a$，$b=(b_1,b_2,\cdots,b_n)$，其中 $b_i=\begin{cases}1 & i\in I\\ 0 & i\notin I\end{cases}$，并记 $V=\{\alpha\mid\alpha\leqslant b\}$，则 V 为一 k 维子空间。因 f 的代数正规型中不含有任意形如 $x_{i_1}x_{i_2}\cdots x_{i_t}$ 的项，即对于 $\forall\alpha\in V$，有 $g(\alpha)=0$。又由引理 1 有 $f(\alpha)=\bigoplus\limits_{\beta\leqslant\alpha}g(\beta)$，即对 $\forall\alpha\in V$，有 $f(\alpha)=0$，从而 $NN(f)\geqslant k$。证毕。

例 2 当 $n=12$ 时，对于 $f(x)=x_1+x_{11}+x_2x_3+x_1x_3x_7+x_5x_8x_{10}+x_4x_5x_9x_{11}+x_3x_7x_8x_{10}x_{12}+x_1x_3x_4x_5x_8x_9x_{10}x_{11}x_{12}$，就可取 $I=\{1,2,4,6,7,8,9,10,11,12\}$，则 $NN(f)\geqslant\#I=10$。

将定理 3 的结论应用于 f^C，便得到了下面的推论。

推论 1 设 $f(x)\in B_n$，若 f 的代数正规型中含有所有形如 $x_{i_1}x_{i_2}\cdots x_{i_t}$ $(t>1)$ 的项，其中 $i_1,i_2,\cdots,i_t\in I\subset\{1,2,\cdots,n\}$，则 $NN(f^C)\geqslant k$，其中 $k=^{\#}I$。

事实上，在寻找具体的 I 时，可以利用下面推论的结论。

推论 2 设 $f(x)\in B_n$，$J\subset\{1,2,\cdots,n\}$，且对 f 的代数正规型中任意项 $x_{i_1}x_{i_2}\cdots x_{i_t}$，都有 $\{i_1,i_2,\cdots,i_t\}\cap J\neq\phi$，则 $NN(f)\geqslant n-k$，其中 $k=^{\#}J$。

其实只需取定理 3 中的 $I=\{1,2,\cdots,n\}-J$ 即可。比如在上例中就可取 $J=\{3,5\}$。

从上面的定理及推论可以看出，只需从函数代数正规型的每一个单项中取一个下标就可构成 J，且 J 越小越有利于取得正规阶上界。

结合定理 2 与定理 3，可得到代数正规型与代数免疫阶之间的如下关系。

推论 3 设 $f(x)\in B_n$，若 f 的代数正规型中不含有任意形如 $x_{i_1}x_{i_2}\cdots x_{i_t}$ $(t>1)$ 的项，其中 $i_1,i_2,\cdots,i_t\in I\subset\{1,2,\cdots,n\}$，则 $AI(f)\leqslant n-k$，其中 $k=^{\#}I$。

如在上面的例 2 中，就有 $AI(f)\leqslant 2$。类似地还可以得到代数正规型与扩展的正规性及扩展代数免疫阶之间的关系。显然，据此结论在计算正规阶上界以及代数免疫阶时可以节省大量的计算。比如在上面的例子中，用我们的方法只需简单计算就可以得出函数的正规阶上界不小于 10 的结论，而采用常规的正规性判定方法仅寻找所有的 10 维子空间和仿射子空间就有约 2^{23} 个。对代数免疫的计算量可类似分析，但本文的方法可能对某些函数不能取得较好的结果。

结束语 本文从正规性这一密码函数的复杂性指标出发，考虑到在对密码函数作一个小改动时是否仍然具有良好的复杂性，定义了扩展的正规性。同时研究了扩展正规性这一指标和扩展代数免疫阶之间的关系，并从代数正规型的角度对密码函数的正规性和代数免疫阶进行了分析，提供了一条方便易行的思路。

参 考 文 献

[1] Dobbertin H. Constructions of bent functions and balanced Boolean functions with high nonlinearity [C]// Fast Software Encryption, Lecture Notes in Computer Science. Springer-Verlag, 1994, 1008: 61-74

[2] Carlet C. On the complexity of cryptographic Boolean functions [C]// Sixth International Conference on Finite Fields and Applications, Lecture Notes in Computer Science. Berlin: Springer, 2002: 53-69

[3] Zhang X M, Josef P, Zheng Y. On Algebraic Immunity and Annihilators [C]// ICISC 2006, LNCS 4296. Berlin Heidelberg: Springer-Verlag, 2006: 65-80

[4] Daum M, Dobbertin H, Leander G. An algorithm for checking normality of Boolean functions [C]// Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003). Versailles, France, 2003: 133-142

[5] Braeken A, Wolf C, Preneel B. A randomised algorithm for checking the normality of cryptographic Boolean functions [C]// IFIP TCS. Kluwer, 2004: 51-66

[6] Courtois N, Meier W. Algebraic attacks on stream cipher with linear feedback [C]// Advances in Cryptology-EUROCRYPT 2003, LNCS 2656. Springer Verlag, 2003: 345-359

[7] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions [C]// Advances in Cryptology—EUROCRYPT 2004, LNCS 3027. Springer-Verlag, 2004: 474-491

[8] 张卫国，丁勇，张宁，等. 代数免疫布尔函数的一个特征[J]. 北京邮电大学学报，2007，30(5)：55-57

[9] Dalai D K, Gupta K C, Maitra S. Results on Algebraic immunity for cryptographically significant Boolean functions [C]// INDOCRYPT 2004, LNCS 3348. Springer-Verlag, 2004: 92-106

[10] Dubuc S. Etude des proprie tes de degenerescence et de normalite des fonctions booleennes et construction de fonctions q-aires parfaitement non-line aires [D]. Universite de Caen, 2001

[11] Zheng Y, Zhang X M, Imai H. Restriction, terms and nonlinearity of Boolean functions [J]. Theoretical Computer Science, 1999, 226(1): 207-223

(上接第 40 页)

[6] Huang C, Tseng Y. The coverage problem in a wireless sensor network[J]. Mobile Networks and Applications, 2005, 10(4): 519-528

[7] Li N, Hou J C, Sha L. Design and analysis of an MST-based topology control algorithm[J]. IEEE Transactions on Wireless Communications, 2005, 4(3): 1195-1206

[8] Savarese C, Rabaey J, Langendoen K. Robust positioning algorithms for distributed ad-hoc wireless sensor networks[C]// Proceedings of the USENIX Technical Annual Conference. Monterey, CA, USA, June 2002

[9] Savarese C, Rabaey J M, Beutel J. Locationing in distributed ad-hoc wireless sensor networks[C]// Proceedings of IEEE ICASSP. Salt Lake City, UT, USA, May 2001

[10] Savvides A, Han C C, Strivastava M B. Dynamic fine-grained localization in ad-hoc networks of sensors[C]// Proceedings of ACM MobiCom. Rome, Italy, Jule 2001

[11] Moore D, Leonard J, Rus D, et al. Robust distributed network localization with noisy range measurements[C]// Proceedings of ACM SenSys. Baltimore, MD, USA, Nov. 2004

[12] Zhou Z, Cui J H, Zhou S L. Localization for large-scale underwater sensor networks[R]. UbiNet-TR06-04. Computer Science & Engineering dept, University of Connecticut, 2006

[13] He T, Huang C D, Blum B M, et al. Range-free localization schemes for large scale sensor networks[C]// Proceedings of ACM MobiCom. San Diego, CA, USA, Sep. 2003

[14] Li M, Liu Y H. Rendered path: range-free localization in anisotropic sensor networks with holes[C]// Proceedings of ACM MobiCom. Montreal, Quebec, Canada, Sep. 2007

[15] Golub G. Matrix computations (3rd edition) [M]. The Johns Hopkins University Press, 1996