第 21 卷 第 2 期 电 子 科 学 学 刊 Vol.21 No.2
1999 年 3 月 JOURNAL OF ELECTRONICS Mar. 1999

相关免疫函数的稳定性 [1]

温巧燕 肖国镇

(西安电子科技大学信息保密所 西安 710071)

摘 要 本文讨论了相关免疫函数的稳定性，证明了相关免疫性是不稳定的，但广义相关免疫却具有较好的稳定性.

关键词 相关免疫，稳定性，广义相关免疫

中图号 TN918.1

1 引 言

相关免疫性是流密码系统抗相关分析能力的重要标志，但函数的相关免疫性却与其它密码学性质，如非线性次数和线性复杂度等存在着制约关系，本文进一步分析相关免疫函数的稳定性。

2 定义

定义 1 n 元布尔函数 $f(x)=f(x_1,\cdots,x_n)$ 称为 m 阶相关免疫的，当且仅当对任意 m 个变量 $x_{i_1},\cdots,x_{i_m}$ 和 $a_1,\cdots,a_m\in \mathrm{GF}(2)$，恒有

$$P(f(x)=1)-P(f(x)=1|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)=0,$$

这里 $P(\cdot)$ 和 $P(\cdot|\cdot)$ 分别表示概率和条件概率。

定义 2[1] n 元布尔函数 $f(x)=f(x_1,\cdots,x_n)$ 称为 m 阶 ε-相关免疫的，当且仅当对任意 m 个变量 $x_{i_1},\cdots,x_{i_m}$ 和 $a_1,\cdots,a_m\in \mathrm{GF}(2)$，恒有

$$|P(f(x)=1)-P(f(x)=1|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)|\le\varepsilon.$$

为了便于分析，文献 [2] 中给出如下定义：

定义 3 $f(x)$ 称为 m 阶 ε-相关免疫的，是指对任意线性函数 $l(x)=\omega_1x_1+\cdots+\omega_nx_n$，只要 $1\le\omega(\omega)\le m$, 则下式成立

$$\frac{1}{2^n}|\omega(f(x)+l(x))-2^{n-1}|\le\varepsilon.$$

根据文献 [2] 中推论 5.2.3，若 $f(x)$ 按定义 2 是 ε-相关免疫的，则按定义 3 亦是 ε-相关免疫的。本文采用定义 3 。

当 $\varepsilon=0$ 时，定义 2 和定义 3 就退化为定义 1，将 ε-相关免疫称为广义相关免疫，相应地相关免疫就称为狭义相关免疫。

3 主要结果

引理 设 w 为 $f(x)$ 的重量，当 $f(x)$ m 阶相关免疫时，$2^m|w$，特别地 $m=1$ 时，w 为偶数。

根据此引理可证明相关免疫性是一个极不稳定的性质，有如下结论：

定理 1 设 $f(x)$ 是 n 元 m 阶相关免疫函数，任意改变 $f(x)$ 在某一点的函数值，则 $f(x)$ 不再具有任何阶的相关免疫性。

证明 $f(x)$ 改变一个点的函数值后，重量变为 $w(f)\pm1$，是奇数，所以不是相关免疫函数。

虽然改变一个点的函数值，破坏了相关免疫性，却可能大大提高其非线性次数 (文献 [1] 中定理 17.4.4) 或线性复杂度。

[1] 1997-09-23 收到， 1998-07-01 定稿

定理 2 设 $f(x)$ 是 m 阶相关免疫的，任意改变函数在 r 个点上的函数值，则 $f(x)$ 是 $r/2^n$-相关免疫的。

证明 $f(x)+l(x)$ 最多有 r 个点的值发生变化，设改变 r 个点的值后的函数为 $f_1(x)$，则

$$|w(f(x)+l(x))-w(f_1(x)+l(x))|\le r, \tag{1}$$

故

$$\begin{aligned}&(1/2^n)|w(f_1(x)+l(x))-2^{n-1}|\\&=(1/2^n)|w(f(x)+l(x))-2^{n-1}+w(f_1(x)+l(x))-w(f(x)+l(x))|\\&=(1/2^n)|w(f_1+l)-w(f+l)|\le(r/2^n).\end{aligned} \tag{2}$$

证毕

推论 设 $f(x)$ 是 ε-相关免疫的，任意改变 $f(x)$ 在 r 个点的函数值，则 $f(x)$ 变为 $(\varepsilon+r/2^n)$-相关免疫的。

证明 类似定理 2 的推导过程中的 (1) 式，(2) 式变为

$$\begin{aligned}&(1/2^n)|w(f_1(x)+l(x))-2^{n-1}|\\&=(1/2^n)|w(f(x)+l(x))-2^{n-1}+w(f_1(x)+l(x))-w(f(x)+l(x))|\\&\le(1/2^n)|w(f(x)+l(x))-2^{n-1}|+(1/2^n)|w(f_1(x)+l(x))-w(f(x)+l(x))|\\&\le\varepsilon+(r/2^n).\end{aligned}$$

证毕

当 n 很大，而 r 较小时，$r/2^n$ 很小，也就是说 $f(x)$ 的相关度 [2] 改变很小。所以，广义相关免疫性是一个比较稳定的性质。克服了狭义相关免疫的不稳定性。这是广义相关免疫函数的又一个优势。关于广义相关免疫函数的详细讨论可参考文献 [1,2]。

参 考 文 献

[1] 杨义先，林须端. 编码密码学，北京：人民邮电出版社，1992, 610–617.

[2] 温巧燕. 密码学中的相关免疫函数研究：[博士论文]. 西安：西安电子科技大学，1997.

STABILITY OF CORRELATION-IMMUNE FUNCTIONS

Wen Qiaoyan Xiao Guozhen

(*Institute of Information Security, Xidian University, Xi'an* 710071)

Abstract The stability of correlation-immune functions is discussed in this paper. The correlation-immunity is not stable and generalized Correlation-immunity is stable.

Key words Correlation-immune, Stability, Generalized correlation-immune

温巧燕：女，1959 年生，副教授，博士后，主要从事信息论、编码密码学、信息安全、应用数学等方面的教学与研究.

肖国镇：男，1934 年生，教授，博士生导师，主要从事信息论、编码密码学、信息安全、应用数学等方面的教学与研究.