doi:10.11959/j.issn.1000-436x.2015112

T 函数 Walsh 谱值与差分转移概率快速算法

刘燕，胡斌，徐立平
（解放军信息工程大学 密码工程学院，河南 郑州 450001）

摘 要：根据 T 函数自身输入与输出结构特点，结合 T 函数窄度相关定义，研究了 T 函数线性性质和差分性质。通过构造马尔可夫链和概率转移矩阵，给出了其 Walsh 谱值与差分转移概率计算的多项式时间快速算法，时间复杂度为 $O(n)$，并将该算法应用于对 TSC 系列 T 函数的研究，得到任意输入输出线性组合的 Walsh 谱值表达式。
关键词：T 函数；窄度；Walsh 谱值；差分转移概率；马尔可夫链
中图分类号：TN918.1 **文献标识码**：A

Efficient algorithm for computing Walsh spectrum and differential probability

LIU Yan, HU Bin, XU Li-ping
(School of Cryptography Engineering, Information Engineering University, Zhengzhou 450001, China)

Abstract: According to the characteristic of T-functions, along with the definition of narrow T-functions, the linear property and differential property were studied. Markov chain and transition matrices were constructed to propose fast algorithm for computing Walsh spectrum and differential probability, of which the time complexity is $O(n)$. In addition, the algorithm is applied in the T-functions in TSC-family and finally the result expression is given.
Key words: T-function; narrowness; Walsh spectrum; differential probability; Markov chain

1 引言

2002 年，Klimov 和 Shamir 在文献[1]中提出了 T 函数的概念。T 函数是由 6 种基本运算（加、减、乘、逆、异或、与、或）组成的非线性函数，在计算机中具有硬件实现速度快的优点。同时，T 函数基于字的运算，易于软件实现。所以一经提出便受到了密码学界的广泛关注。T 函数可用于序列密码、分组密码和散列函数等设计。特别是在流密码中，T 函数可以代替线性反馈移位寄存器（LFSR），而且克服了 LFSR 生成序列周期无法达到最大的缺陷。2004 年后，大量基于 T 函数设计的密码算法和相应的攻击的研究成果开始涌现。如在 eSTREAM 中提交的密码算法 ABC[2]、TSC[3~5]、Mir[6]的设计均采用了 T 函数。2005 年，Daum 在文献[7]中提出了 T 函数窄度的概念，用于研究 T 函数方程快速求解问题，该方法同样适用于散列函数方程的求解，对提高散列函数攻击效率有重要意义。对 T 函数的研究还有一个重要途径，即代数动力系统理论。2009 年，Anashin[8] 基于该理论，从非阿基米德分析理论的角度，在 2-adic 距离下讨论了 T 函数的性质。2012 年，Anashin[9]等在非阿基米德遍历理论及保测理论的基础上，给出单圈 T 函数判定的新标准，并提出了判定 T 函数的新方法。

在密码分析中，密码算法能否抵抗差分攻击和线性攻击是衡量密码算法安全性的重要指标。2006 年，K. Nyberg 和 J.Wallen[10]提出了模 2^n 加法的 Walsh 谱值多项式时间计算算法，常亚勤[11]在此基础上给出了环 $Z/(2^n)$上的仿射函数 Walsh 谱值快速计算算法。而对于非线性函数的相关研究成果较少，现有计算 T 函数 Walsh 谱值及差分转移概率一般只能遍历输入空间进行计算，计算复杂度为指数

收稿日期：2014-03-23；**修回日期**：2014-09-02
基金项目：国家自然科学基金资助项目（61272041, 61202491, 61272488）
Foundation Item: The National Natural Science Foundation of China (61272041, 61202491, 61272488)

时间。本文在 T 函数窄度概念的基础上，给出了 T 函数 Walsh 谱值和差分转移概率的快速计算算法，其时间复杂度均为 $O(n)$，并将该算法实现运用于 TSC 系列 T 函数的研究，说明了该算法的可行性。

2 预备知识

符号说明：记 F_2 为二元域，$F_2^{m\times n}$ 为 F_2 上 $m\times n$ 维向量空间，$Z/(2^n)$ 为模 2^n 剩余类环。称 $\boldsymbol{x}=([\boldsymbol{x}]_{n-1},\cdots,[\boldsymbol{x}]_1,[\boldsymbol{x}]_0)\in F_2^n$ 为一个 n bit 单字，在 $\boldsymbol{x}\leftrightarrow\sum_{i=0}^{n-1}2^i[\boldsymbol{x}]_i$ 对应规则下，可以自然地将 F_2 中的 n 维向量 $\boldsymbol{x}$ 看作 $Z/(2^n)$中的整数 $\sum_{i=0}^{n-1}2^i[\boldsymbol{x}]_i$，从而按这种对应方式，在 $Z/(2^n)$与 F_2^n 之间建立了一一对应关系。称 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{m-1})^{\mathrm{T}}\in F_2^{m\times n}$ 为 m 个 n bit 字，其中 $x_k=([x_k]_{n-1},\cdots,[x_k]_1,[x_k]_0)$ (k=0,1,⋯, m−1)为一个 n bit 单字。“⊕”表示逐位异或，“·”表示逐位相乘，“||”表示连接运算。

定义 1[1] 设 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{m-1})^{\mathrm{T}}\in F_2^{m\times n}$，其中 $\boldsymbol{x}_i=([x_i]_{n-1},\cdots,[x_i]_0)\in F_2^n$ 为一个 n bit 字，设 f(x)=([f(x)]$_{n-1}$,⋯, [f(x)]$_1$, [f(x)]$_0$) 为 $F_2^{m\times n}\to F_2^{l\times n}$ 上的多输出函数。如果其输出的第 i 位[f(x)]$_i$ 仅与输入的第 0 位到第 i 位，即([$\boldsymbol{x}$]$_i$,⋯,[$\boldsymbol{x}$]$_1$,[$\boldsymbol{x}$]$_0$)有关，则称 f(x)为 T 函数。[$\boldsymbol{x}$]$_i$, [f(x)]$_i$表示 n 维向量 $\boldsymbol{x}$ 和 f(x)的第 i 路分量，i=0,1,⋯,n-1。当 m=l=1 时称为单字 T 函数，否则称为多字 T 函数，如图 1 所示。

$$f:\begin{pmatrix}[\boldsymbol{x}]_0\\[\boldsymbol{x}]_1\\\vdots\\[\boldsymbol{x}]_{n-1}\end{pmatrix}^{\mathrm{T}}\to\begin{pmatrix}f_0([\boldsymbol{x}]_0)\\f_1([\boldsymbol{x}]_1,[\boldsymbol{x}]_0)\\\vdots\\f_{n-1}([\boldsymbol{x}]_{n-1},...,[\boldsymbol{x}]_1,[\boldsymbol{x}]_0)\end{pmatrix}^{\mathrm{T}}$$

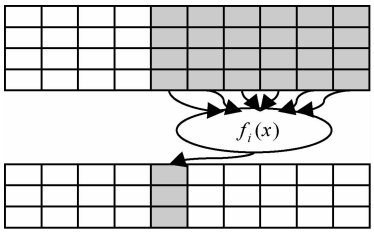


图 1 多字 T 函数

定义 2[1] 设 f(x)是 $F_2^{m\times n}\to F_2^{l\times n}$ 上的多输出函数，记 f(x)=([f(x)]$_{n-1}$, ⋯, [f(x)]$_1$, [f(x)]$_0$)，如果其输出的第 i 位[f(x)]$_i$ 仅与输入的第 0 至第 i−1 位，即([$\boldsymbol{x}$]$_{i-1}$, ⋯, [$\boldsymbol{x}$]$_0$)有关，则称 f(x)为参数。[$\boldsymbol{x}$]$_i$, [f(x)]$_i$表示 n 维向量 $\boldsymbol{x}$ 和 f(x)的第 i 路分量，i = 0,1,⋯,n−1。参数一般用 α,β,γ表示。

定义 3[12] 设$\{X_n,n\geqslant 0\}$为随机序列，其状态空间为 I=$\{i_0, i_1, i_2,\cdots\}$，如果对整数 n 及任意 n+2 个状态 $i_0,i_1,\cdots,i_{n+1}\in I$，有

$$\begin{aligned}&\Pr\{X_{n+1}=i_{n+1}\mid X_0=i_0,X_1=i_1,\cdots,X_n=i_n\}\\&=\Pr\{X_{n+1}=i_{n+1}\mid X_n=i_n\}\end{aligned}$$

则称此随机序列$\{X_n,n\geqslant 0\}$为马尔可夫链。

定义 4[12] 称条件概率 $p_{ij}^{(n)}=\Pr\{X_{m+n}=j|X_m=i\}$, $i,j\in I,m\geqslant 0,n\geqslant 1$为马尔可夫链的 n 步转移概率，并称 $P^{(n)}=(p_{ij}^{(n)})$ 为马尔可夫链的 n 步转移概率矩阵。其中当 n=1 时，$P^{(1)}=P$。

定义 5[13] 设 $f:F_2^n\to F_2^m$ 是多输出函数，$\alpha\in F_2^n,\beta\in F_2^m$，则称 $W_f(\alpha,\beta)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{\alpha x\oplus\beta f(x)}$ 为 f(x)在 (α,β) 点的 Walsh 谱值。

定义 6[13] 设(X,+)是有限交换群，$x_1,x_2\in X$，则称 $\Delta x=x_1-x_2$ 为 x_1 与 x_2 的一个差分。又设(Y,+)也是有限交换群，$f:X\to Y$，则称 $\Delta x=x_1-x_2$ 为 f(x)的一个输入差，$f(x_1)-f(x_2)$ 为与(x_1,x_2)对应的输出差。再设$\alpha\in X,\beta\in Y$，令

$$\begin{aligned}p_f(\alpha\to\beta)&=\Pr\{(x_1,x_2)\in X\times X:f(x_1)-f(x_2)\\&=\beta\mid x_1-x_2=\alpha\}\end{aligned}$$

则称 $p_f(\alpha\to\beta)$ 为 f 在输入差为 α 的条件下，输出差为 β 的差分转移概率。

定义 7[7] 设 f(x)是 $F_2^{m\times n}\to F_2^{l\times n}$ 上的 T 函数，若存在映射：$\lambda_1:F_2^m\to F_2^w$, $\lambda_k:F_2^{m+w}\to F_2^w$ 以及变量 $a_1=\lambda_1([\boldsymbol{x}]_0)$，$a_k=\lambda_k([\boldsymbol{x}]_{k-1},a_{k-1})$，$k$=2,⋯,$n$−1，使函数 f(x)可以表示为

$$\begin{pmatrix}[\boldsymbol{x}]_0\\[\boldsymbol{x}]_1\\[\boldsymbol{x}]_2\\[\boldsymbol{x}]_3\\\vdots\\[\boldsymbol{x}]_{n-1}\end{pmatrix}^{\mathrm{T}}\mapsto\begin{pmatrix}f_0([\boldsymbol{x}]_0)\\f_1([\boldsymbol{x}]_1,a_1)\\f_2([\boldsymbol{x}]_2,a_2)\\f_3([\boldsymbol{x}]_3,a_3)\\\vdots\\f_{n-1}([\boldsymbol{x}]_{n-1},a_{n-1})\end{pmatrix}^{\mathrm{T}}$$

则称非负整数 w 的最小值为 T 函数 f(x)的窄度。

窄度 T 函数是刻画 T 函数的特殊表示方法，由定义知 T 函数 f(x)的第 i 路输出[f(x)]$_i$ 可表示为 f_i([$\boldsymbol{x}$]$_i$,⋯,[$\boldsymbol{x}$]$_1$,[$\boldsymbol{x}$]$_0$)，而窄度定义中的变量 a_i(i=1,⋯, n−1) 可看作蕴含了第 0 路到第 i−1 路输入为第 i 路输出提供的全部信息，这种信息是通过映射 λ_i

(i=1,⋯,n−1)逐路依次传递的。另一方面，变量 a_i(i=1,⋯,n−1)的另一重要性质是当 a_i 取值固定时，T 函数的每一路输出彼此独立，此时对 T 函数性质的研究即可从研究每一路输出函数性质着手。

由于任意 T 函数 $f(x):F_2^{m\times n}\to F_2^{l\times n}$，可表示为 $[f(\boldsymbol{x})]_i=f_i([\boldsymbol{x}]_i,\cdots,[\boldsymbol{x}]_0)$，$i$=0,⋯,$n$−1，则存在映射 $\lambda_1=[\boldsymbol{x}]_0$，$\lambda_i=[\boldsymbol{x}]_{i-1}\|a_{i-1}$，及变量 $a_1=[\boldsymbol{x}]_0$，$a_i=[\boldsymbol{x}]_{i-1}\|a_{i-1}$，$i$=1,⋯，$n$−1 使 $f(x)$可以表示为 $[f(\boldsymbol{x})]_i=f_i([\boldsymbol{x}]_i,\cdots,[\boldsymbol{x}]_0)=f_i([x]_i,a_i)$，$i$=0,⋯,$n$−1，由此可得引理 1。

引理 1[7]　设 $f(x)$是 $F_2^{m\times n}\to F_2^{l\times n}$ 上的 T 函数，则 $f(x)$窄度的上界为 $m(n-1)$。

引理 2[7]　设 $g_i(1\leqslant i\leqslant r)$ 是 $F_2^{m\times n}\to F_2^{l_i\times n}$ 上窄度分别为 w_{g_i} 的 T 函数，f 是 $F_2^{t\times n}\to F_2^{l\times n}$ 上窄度为 w_f 的 T 函数，其中 $t=\sum_{i=1}^{r}l_i$，则 T 函数 $h(x)=f(g_1(x),\cdots,g_r(x))$ 窄度不超过 $(w_f+w_{g_1}+\cdots+w_{g_r})$。

由于文献[7]中并未给出此结论的详细证明，下面给出其证明过程。

证明　由 $f,g_1,\cdots,g_r$ 的窄度分别为 $w_f,w_{g_1},\cdots,w_{g_r}$，则存在映射及变量

$$\lambda_{i_1}:F_2^{m}\to F_2^{w_{g_i}},\lambda_{i_k}:F_2^{m+w_{g_i}}\to F_2^{w_{g_i}};a_{i_1}=\lambda_{i_1}([\boldsymbol{x}]_0),$$
$$a_{i_k}=\lambda_{i_k}([\boldsymbol{x}]_{k-1},a_{i_{k-1}}),i=1,\cdots,r,k=2,\cdots,n-1$$
$$\gamma_1:F_2^{t}\to F_2^{w_f},\gamma_k:F_2^{t+w_f}\to F_2^{w_f};b_1=\gamma_1([\boldsymbol{x}]_0),$$
$$b_k=\gamma_k([\boldsymbol{x}]_{k-1},b_{k-1}),\ k=2,\cdots,n-1$$

使 $f,g_1,\cdots,g_r$ 可表示为

$$g_i(1\leqslant i\leqslant r):\begin{pmatrix}[\boldsymbol{x}]_0\\[\boldsymbol{x}]_1\\\vdots\\[\boldsymbol{x}]_{n-1}\end{pmatrix}^{\mathrm{T}}\mapsto\begin{pmatrix}g_{i_0}([\boldsymbol{x}]_0)\\g_{i_1}([\boldsymbol{x}]_1,a_{i_1})\\\vdots\\g_{i_{n-1}}([\boldsymbol{x}]_{n-1},a_{i_{n-1}})\end{pmatrix}^{\mathrm{T}},$$

$$f:\begin{pmatrix}[\boldsymbol{x}]_0\\[\boldsymbol{x}]_1\\\vdots\\[\boldsymbol{x}]_{n-1}\end{pmatrix}^{\mathrm{T}}\mapsto\begin{pmatrix}f_0([\boldsymbol{x}]_0)\\f_1([\boldsymbol{x}]_1,b_1)\\\vdots\\f_{n-1}([\boldsymbol{x}]_{n-1},b_{n-1})\end{pmatrix}^{\mathrm{T}}$$

令 $s=\sum_{i=1}^{r}w_{g_i}$，现构造如下映射及变量

$$\eta_1:F_2^{m}\to F_2^{s+w_f}:\gamma_1\|\lambda_{1_1}\|\cdots\|\lambda_{1_r},$$
$$\eta_k:F_2^{m+s+w_f}\to F_2^{s+w_f}:\gamma_k\|\lambda_{k_1}\|\cdots\|\lambda_{k_r},k=2,\cdots,n-1$$
$$c_1=b_1\|a_{1_1}\|\cdots\|a_{1_r};\ \ c_k=b_k\|a_{k_1}\|\cdots\|a_{k_r},k=2,\cdots,n-1$$

则通过 η_k 及 c_k (k=0,⋯n−1)，$h(x)=f(g_1(x),\cdots,g_r(x))$可以表示为

$$\begin{pmatrix}f_0(g_1([\boldsymbol{x}]_0),\ldots,g_r([\boldsymbol{x}]_0))\\f_1(g_1([\boldsymbol{x}]_1),\ldots,g_r([\boldsymbol{x}]_1),b_1)\\\vdots\\f_{n-1}(g_1([\boldsymbol{x}]_{n-1}),\ldots,g_r([\boldsymbol{x}]_{n-1}),b_{n-1})\end{pmatrix}^{\mathrm{T}}$$
$$=\begin{pmatrix}f_0(g_{1_0}([\boldsymbol{x}]_0),\ldots,g_{r_0}([\boldsymbol{x}]_0))\\f_1(g_{1_1}([\boldsymbol{x}]_1,a_{1_1}),\ldots,g_r([\boldsymbol{x}]_1,a_{r_1}),b_1)\\\vdots\\f_{n-1}(g_{1_{n-1}}([\boldsymbol{x}]_{n-1},a_{1_{n-1}}),\ldots,g_{r_{n-1}}([\boldsymbol{x}]_{n-1},a_{r_{n-1}}),b_{n-1})\end{pmatrix}^{\mathrm{T}}$$
$$=\begin{pmatrix}f_0(g_{1_0}([\boldsymbol{x}]_0),\ldots,g_{r_0}([\boldsymbol{x}]_0))\\f_1'(g_{1_1}'([\boldsymbol{x}]_1,c_1),\ldots,g_r'([\boldsymbol{x}]_1,c_1),c_1)\\\vdots\\f_{n-1}'(g_{1_{n-1}}'([\boldsymbol{x}]_{n-1},c_{n-1}),\ldots,g_{r_{n-1}}'([\boldsymbol{x}]_{n-1},c_{n-1}),c_{n-1})\end{pmatrix}^{\mathrm{T}}$$
$$\triangleq\begin{pmatrix}h_0([\boldsymbol{x}]_0)\\h_1([\boldsymbol{x}]_1,c_1)\\\vdots\\h_{n-1}([\boldsymbol{x}]_{n-1},c_{n-1})\end{pmatrix}^{\mathrm{T}}$$

由于映射 $\eta_k:F_2^{m+s+w_f}\to F_2^{s+w_f}$，$k=2,\cdots,n-1$，根据 T 函数窄度定义，函数 $h(x)$的窄度不超过 $(w_f+w_{g_1}+\ldots+w_{g_r})$。

由引理 2，要计算某个 T 函数的窄度，则首先可将其写为多个基本运算（加、减、乘、逆、异或、与、或）复合的形式，再计算每个简单函数的窄度，相加后与引理 1 中给出的上界比较取最小值，即可得到该 T 函数的窄度。

命题 1[11]　设$(X,+)$和$(Y,+)$都是有限交换群，$f:X\to Y$，则 $\forall\alpha\in X,\beta\in Y$，有 $p_f(\alpha\to\beta)=\Pr\{x\in X:f(x+\alpha)-f(x)=\beta\}$。

本文讨论的 $X=F_2^{m\times n},Y=F_2^{l\times n}$，“+”运算为异或。

3　T 函数 Walsh 谱值和差分转移概率快速算法

对于给定的输入输出的线性组合（差分），计算 Walsh 谱值（差分转移概率）一般是遍历输入 x 的取值空间，其计算量为 2^{mn}。当 n 较大时，要计算出具体结果是十分困难的。文献[10]给出了 m 个变量模 2^n 加法，即 $f=(x_1+x_2+\cdots x_m)\bmod 2^n$ Walsh 谱值的快速计算方法，在此基础上，本文研究有效计算 T 函数 Walsh 谱值（差分转移概率）的快速计

算方法。

考虑到 T 函数常可以表示为 $T(x)=f(x) \bmod 2^n$，而定义中 n 的取值根据实际使用需求确定，即定义中 n 可以取任意值，为了有效计算 T 函数（$T(x): F_2^{m\times n} \to F_2^{l\times n}$）$n$ 路输入输出的 Walsh 谱值，首先在 T 函数窄度的定义中假设输入输出规模为 n+1 路，即设函数 $T(x): F_2^{m\times(n+1)} \to F_2^{l\times(n+1)}$ 是窄度为 w 的 T 函数，则存在映射 $\lambda_1: F_2^m \to F_2^w$，$\lambda_i: F_2^{m+w} \to F_2^w$，及变量 $a_1=\lambda_1([\boldsymbol{x}]_0)$，$a_i=\lambda_i([\boldsymbol{x}]_{i-1}, a_{i-1})$，$i$=2,⋯, n，使 $T(x)$ 可以表示为 $[T([\boldsymbol{x}]_0)]_0=f_0([\boldsymbol{x}]_0)$，$[T([\boldsymbol{x}]_0)]_i=f_i([\boldsymbol{x}]_i, a_i)$，$i$=1,⋯,$n$。而在实际计算过程中只取其中的 n 路输入输出 $[\boldsymbol{x}]_i$, $f_i([\boldsymbol{x}]_i, a_i)$, i=0,⋯, n−1，这样做是为了引入映射 λ_n 及变量 a_n，为下文中计算做准备。

显然，此时 $T(x)$窄度的上界为 mn。下文刻画 T 函数均使用窄度的定义描述，即设 $T(x): F_2^{m\times n} \to F_2^{l\times n}$, 是窄度为 w 的 T 函数，则包含了存在映射 λ_i 及变量 a_i，i=0,⋯,n，对此不再赘述。

定理 1 设函数 $T(x): F_2^{m\times n} \to F_2^{l\times n}$, 是窄度为 w 的 T 函数。令变量 $\{a_i, 1\leqslant i\leqslant n\}$ 为随机序列，其状态空间为 $I=F_2^w$，则此随机序列 $\{a_i, 1\leqslant i\leqslant n\}$ 为马尔可夫链。

证明 任意 $2\leqslant k\leqslant n-1$，取 k+1 个状态 $i_1, i_2, \cdots, i_{k+1}\in I$，则

$$\begin{aligned}&\Pr(a_{k+1}=i_{k+1} \mid a_1=i_1, a_2=i_2, \cdots, a_k=i_k)\\&=\Pr(\lambda_{k+1}([\boldsymbol{x}]_i, i_k)=i_{k+1} \mid \lambda_1([\boldsymbol{x}]_0)=i_1, \cdots, \lambda_k([\boldsymbol{x}]_{i-1}, i_{k-1})=i_k)\\&=\Pr(\lambda_{k+1}([\boldsymbol{x}]_i, i_k)=i_{k+1} \mid \lambda_k([\boldsymbol{x}]_{i-1}, i_{k-1})=i_k)\\&=\Pr(a_{k+1}=i_{k+1} \mid a_k=i_k)\end{aligned}$$

因此，$\{a_i, 1\leqslant i\leqslant n\}$为马尔可夫链。

由此，根据 T 函数窄度中变量的定义，构造了关于 T 函数的马尔可夫链。在计算 T 函数的 Walsh 谱值时，为了得到 T 函数 n 路输出的 Walsh 谱值，可以简化为计算每一路输出的 Walsh 谱值，再通过马尔可夫链，构造概率转移矩阵，矩阵相乘即可得到 T 函数 n 路输出的 Walsh 谱值。

定理 2 设函数 $T(x): F_2^{m\times n} \to F_2^{l\times n}$ 是窄度为 w 的 T 函数，设 $\alpha=([\alpha]_{n-1}, \cdots, [\alpha]_1, [\alpha]_0)$，$\beta=([\beta]_{n-1}, \cdots, [\beta]_1, [\beta]_0)$（$0\leqslant i\leqslant n-1$，$[\alpha]_i\in F_2^m$，$[\beta]_i\in F_2^l$）是输入输出的线性组合，则 $T(x)$在 (α, β) 点的 Walsh 谱值为

$$\begin{aligned}W_{T(x)}(\alpha\to\beta)&=\frac{1}{2^{mn}}\sum_{x=0}^{2^{mn}-1}(-1)^{\alpha x\oplus\beta T(x)}\\&=\frac{1}{2^{mn}}\boldsymbol{L}\boldsymbol{A}^{(n-1)}\boldsymbol{A}^{(n-2)}\cdots\boldsymbol{A}^{(1)}\boldsymbol{A}^{(0)}\end{aligned}$$

其中，$\boldsymbol{L}$=(11⋯1) 是 2^w 维行向量，$\boldsymbol{A}^{(0)}$是 2^w 维的列向量, $\boldsymbol{A}^{(0)}$的第 d 行为

$$A_d^{(0)}=|\{x\in F_2^m: [\alpha]_i x\oplus[\beta]_i f_0(x)=0, \lambda_{i+1}(x)=d\}|-|\{x\in F_2^m: [\alpha]_i x\oplus[\beta]_i f_i(x)=1, \lambda_{i+1}(x)=d\}|$$

$\boldsymbol{A}^{(i)}(1\leqslant i\leqslant n-1)$ 是 $2^w\times 2^w$ 维矩阵，$\boldsymbol{A}^{(i)}$的第 d 行第 c 列的值为

$$A_{(d,c)}^{(i)}=|\{x\in F_2^m: [\alpha]_i x\oplus[\beta]_i f_i(x,c)=0, \lambda_{i+1}(x,c)=d\}|-|\{x\in F_2^m: [\alpha]_i x\oplus[\beta]_i f_i(x,c)=1, \lambda_{i+1}(x,c)=d\}|$$

证明 设 $\boldsymbol{P}_i$ (i=1,⋯,n)是 2^w 维列向量，第 c 行 $\boldsymbol{P}_{i,c}$ 的值表示为

$$\begin{aligned}\boldsymbol{P}_{i,c}=&\Pr(\bigoplus_{j=0}^{i-1}([\alpha]_j[x]_j\oplus[\beta]_j[T(x)]_j=0), a_i=c)-\\&\Pr(\bigoplus_{j=0}^{i-1}([\alpha]_j[x]_j\oplus[\beta]_j[T(x)]_j=1), a_i=c)\end{aligned}$$

另设 $\boldsymbol{M}_i$(i=1,⋯,n−1)是 $2^w\times 2^w$ 维矩阵，第 d 行第 c 列 $\boldsymbol{M}_{i(d,c)}$的值表示为

$$\begin{aligned}&\boldsymbol{M}_{i(d,c)}=\Pr([\alpha]_i[x]_i\oplus\beta_i f_i([x]_i, a_i)=0,\\&\lambda_{i+1}([x]_i, a_i)=d \mid a_i=c)\\&-\Pr([\alpha]_i[x]_i\oplus\beta_i f_i([x]_i, a_i)=1, \lambda_{i+1}([x]_i, a_i)=d \mid a_i=c)\end{aligned}$$

则 $\sum_{c\in 2^w}\boldsymbol{M}_{i(d,c)}\boldsymbol{P}_{i,c}$

$$\begin{aligned}&=\sum_{c\in 2^w}\{(\Pr([\alpha]_i[x]_i\oplus[\beta]_i f_i([x]_i, a_i)=0,\\&\lambda_{i+1}([x]_i, a_i)=d \mid a_i=c)-\Pr([\alpha]_i x_i\oplus[\beta]_i f_i([x]_i, a_i)=1,\\&\lambda_{i+1}([x]_i, a_i)=d \mid a_i=c))\\&(\Pr(\bigoplus_{j=0}^{i-1}([\alpha]_j[x]_j\oplus[\beta]_j[T(x)]_j=0), a_i=c)-\\&\Pr(\bigoplus_{j=0}^{i-1}([\alpha]_j[x]_j\oplus[\beta]_j[T(x)]_j=1), a_i=c))\}\\&=\sum_{c\in 2^w}\{(\bigoplus_{j=0}^{j=i}\Pr([\alpha]_j[x]_j\oplus[\beta]_j f_j([x]_j, c)=0, \lambda_{i+1}([x]_i, c)=d)-\\&\Pr(\bigoplus_{j=0}^{j=i}[\alpha]_j[x]_j\oplus[\beta]_j f_j([x]_j, c)=1, \lambda_{i+1}([x]_i, c)=d)\}\\&=\Pr(\bigoplus_{j=0}^{j=i}[\alpha]_j[x]_j\oplus[\beta]_j f_j([x]_j, c)=0, a_{i+1}=d)-\\&\Pr(\bigoplus_{j=0}^{j=i}[\alpha]_j[x]_j\oplus[\beta]_j f_j([x]_j, c)=1, a_{i+1}=d)=\boldsymbol{P}_{i+1,d}\end{aligned}$$

此时，$T(x)$在 (α, β) 点的 Walsh 谱值为

$$W_{T(x)}(\alpha\to\beta)=\sum_{x\in B^m}(-1)^{\alpha x\oplus\beta T(x)}$$
$$=\Pr(\alpha x\oplus\beta T(x)=0)-\Pr(\alpha x\oplus\beta T(x)=1)$$
$$=\sum_{c_{n+1}\in 2^w}\Pr(\alpha x\oplus\beta T(x)=0,a_{n+1}=c_{n+1})-$$
$$\Pr(\alpha x\oplus\beta T(x)=1,a_{n+1}=c_{n+1})$$
$$=\sum_{c_n\in 2^w}\boldsymbol{P}_{n,c_n}=\sum_{c_n\in 2^w}\sum_{c_{n-1}\in 2^w}\boldsymbol{M}_{n-1(c_n,c_{n-1})}P_{n-1,c_{n-1}}$$
$$=\sum_{c_n,\ldots c_0\in 2^w}\boldsymbol{M}_{n-1(c_n,c_{n-1})}\boldsymbol{M}_{n-2(c_{n-1},c_{n-2})}\cdots\boldsymbol{M}_{0(c_1,c_0)}\boldsymbol{P}_{0,c_0}$$
$$=\frac{1}{2^{mn}}\boldsymbol{L}\boldsymbol{A}^{(n-1)}\boldsymbol{A}^{(n-2)}\cdots\boldsymbol{A}^{(1)}\boldsymbol{A}^{(0)}$$

定理 2 利用在变量 $a_i(1\leqslant i\leqslant n)$ 取固定值时，$T(x)$的第 i 路输出$[T(x)]_i$只与第 i 路输入$[\boldsymbol{x}]_i$有关而与低路输入$[x]_{i-1},\cdots\ [x]_0$无关这一特性，结合变量的马尔可夫链，构造了 Walsh 谱的概率转移矩阵。由此，给出任意输入输出线性组合，T 函数 Walsh 谱的计算算法：

算法 1　T 函数 $T(x):F_2^{m\times n}\to F_2^{l\times n}$ Walsh 谱计算算法

Step1　求 T 函数的窄度 w，即找到映射及变量满足定义 7 中的条件。

Step2　构造概率转移矩阵。对每一路输出 $f_i(i=0,\cdots,n-1)$，遍历输入输出线性组合的所有可能值，其数据计算量为 $2^m\times 2^l$。即对任意的输入输出线性组合 $([a]_i,[b]_i)$，其中 $[a]_i=([a_0]_i,\cdots,\ [a_{m-1}]_i)\in F_{2^m}$，$[b]_i=([b_0]_i,\cdots,[b_{l-1}]_i)\in F_{2^l}$，预计算矩阵 $\boldsymbol{A}_s^{(i)}$ 并存储，其中 $s=\sum_{k=0}^{m-1}2^k[a_k]_i+\sum_{k=0}^{l-1}2^{m+k}[b_k]_i$，$i$=0,⋯, n−1。

Step3　对给定的输入输出的线性组合 (α,β)，其中 $\alpha\in F_2^{m\times n}$，$\beta\in F_2^{l\times n}$ 分别计算 $s_i=\sum_{k=0}^{m-1}2^k[\alpha_k]_i+\sum_{k=0}^{l-1}2^{m+k}[\beta_k]_i$。

Step4　计算得到最终结果 $W_{T(x)}(\alpha\to\beta)=\boldsymbol{L}\boldsymbol{A}_{s_{n-1}}^{(n-1)}\boldsymbol{A}_{s_{n-2}}^{(n-2)}\cdots\boldsymbol{A}_{s_1}^{(1)}\boldsymbol{A}_{s_0}^{(0)}$。

对于一个已知的 T 函数 Step1 和 Step2 可以看作预处理的过程，则该算法的时间复杂性为 n 个矩阵相乘，存储数据量为 $(n-1)2^{m+l}$ 个 $2^w\times 2^w$ 矩阵及 2^{m+l} 个 2^w 维列向量。若仅计算某对特定输入输出线性组合 (α,β) 的 Walsh 谱，则需存储(n-1)个 $2^w\times 2^w$ 矩阵及 1 个 2^w 维列向量。

同样利用 T 函数变量马尔可夫链，给出 T 函数差分转移概率的计算方法，其核心在于构造差分转移概率的概率转移矩阵。此时，根据输入差 α 构造另一条马尔可夫链 $\{a_i',1\leqslant i\leqslant n\,|\,a_1'=\lambda_1([x\oplus\alpha]_i);\ a_k'=\lambda_k([x\oplus\alpha]_{k-1},a_{k-1}'),2\leqslant k\leqslant n\}$，将二者链接 $\{a_i\,\|\,a_i',1\leqslant i\leqslant n\}$ 后仍为马尔可夫链。又利用每一路输出在变量取固定值时相对独立特性，即可构造概率转移矩阵，将差分转移概率转化成概率转移矩阵相乘，具体描述如下。

定理 3　设函数 $T(x):F_2^{m\times n}\to F_2^{l\times n}$ 是窄度为 w 的 T 函数，设 $\alpha=([\alpha]_{n-1},\cdots,[\alpha]_1,[\alpha]_0)$，$\beta=([\beta]_{n-1},\cdots,[\beta]_1,[\beta]_0)$ ($0\leqslant i\leqslant n-1$, $[\alpha]_i\in F_2^m,[\beta]_i\in F_2^l$) 分别为输入差分及输出差分，则此时差分转移概率为

$$P_f(\alpha\to\beta)=\Pr(f(x)\oplus f(x\oplus\alpha)=\beta)$$
$$=\frac{1}{2^{mn}}\boldsymbol{L}\boldsymbol{A}^{(n-1)}\boldsymbol{A}^{(n-2)}\cdots\boldsymbol{A}^{(1)}\boldsymbol{A}^{(0)}$$

其中，$\boldsymbol{L}$=(11⋯1) 是 2^{2w} 维全 1 行向量，$\boldsymbol{A}^{(0)}$是 2^{2w} 维的列向量,第 $d\|d'$行的值为

$$A_{d\|d'}^{(0)}=|\{x\in F_2^m:f_0(x)\oplus f_0(x\oplus[\alpha]_0)$$
$$=\beta_i,\lambda_1(x)=d,\lambda_1(x\oplus[\alpha]_0)=d'\}|$$

$\boldsymbol{A}^{(i)}(1\leqslant i\leqslant n-1)$ 是 $2^{2w}\times 2^{2w}$ 维矩阵，$\boldsymbol{A}^{(i)}$的第 $d\|d'$行第 $c\|c'$列的值为

$$\boldsymbol{A}_{(d\|d',c\|c')}^{(i)}=|\{x\in F_2^m:f_i(x,c)\oplus f_i(x\oplus[\alpha]_i,c')$$
$$=\beta_i,\lambda_{i+1}(x,c)=d,\lambda_{i+1}(x\oplus[\alpha]_i,c')=d'\}|$$

证明过程与定理 1 类似，此处省略。

相应地，给出 T 函数差分转移概率的快速计算方法。

算法 2　T 函数 $T(x):F_2^{m\times n}\to F_2^{l\times n}$ 差分转移概率的快速算法。

Step1　求 T 函数的窄度 w。即找到映射及变量满足定义 7 中的条件。

Step2　构造概率转移矩阵。对每一路输出 $f_i(i=0,\cdots,n-1)$，遍历输入输出线性组合的所有可能值，其数据计算量为 $2^m\times 2^l$。即对任意的输入输出差分 $([a]_i,[b]_i)$，其中，$[a]_i=([a_0]_i,\cdots,[a_{m-1}]_i)\in F_2^m$，$[b]_i=([b_0]_i,\cdots,[b_{l-1}]_i)\in F_2^l$，预计算矩阵 $\boldsymbol{A}_s^{(i)}$ 并存储，其中，$s=\sum_{k=0}^{m-1}2^k[a_k]_i+\sum_{k=0}^{l-1}2^{m+k}[b_k]_i$，$i$=0,⋯,$n$−1。

Step3　对给定的输入输出差分 (α,β)，其中，$\alpha\in F_2^{m\times n}$，$\beta\in F_2^{l\times n}$ 分别计算 $s_i=\sum_{k=0}^{m-1}2^k[\alpha_k]_i+\sum_{k=0}^{l-1}2^{m+k}[\beta_k]_i$。

Step4　计算得到最终结果 $P_T(\alpha\to\beta)=\boldsymbol{L}\boldsymbol{A}_{s_{n-1}}^{(n-1)}\boldsymbol{A}_{s_{n-2}}^{(n-2)}\cdots\boldsymbol{A}_{s_1}^{(1)}\boldsymbol{A}_{s_0}^{(0)}$。

对于一个已知的 T 函数 Step1 和 Step2 可以看作预处理的过程，则该算法的时间复杂度为 $O(n)$，存储数据量为 $(n-1)2^{m+l}$ 个 $2^{2w}\times 2^{2w}$ 矩阵及 2^{m+l} 个 2^{2w} 维列向量。若仅计算某对特定输入输出差分 (α,β) 的差分转移概率，则需存储$(n-1)$个 $2^{2w}\times 2^{2w}$ 矩阵及 1 个 2^{2w} 维列向量。

算法 1 和算法 2 从理论上给出了任意 T 函数 Walsh 谱值及差分转移概率的多项式时间算法，该算法的核心在于找到映射及变量将 T 函数表示成分位函数的形式，同时得到该 T 函数的窄度。事实上，在实际应用中，计算 2 个 $t\times t$ 规模矩阵的乘积，目前已知的最好计算时间上界是 Le Gall 和 François 提出的 $O(t^{2.372\ 363\ 9})$[14]。此时，对于窄度为 w 的 T 函数，若计算某对特定输入输出线性组合的 Walsh 谱，实际计算复杂度为 $O(2^{2.372\,363\,9w}n)$，相应地，计算某对特定输入输出差分的差分转移概率，实际计算复杂度为 $O(2^{4.744\,727\,8w}n)$。当 w 的取值与输入规模 n 无关时，可将 $2^{4.744\,727\,8w}$ 视为常数，则计算 Walsh 谱值及差分转移概率的时间复杂性为多项式时间，然而对于 w 取值与 n 有关的 T 函数，该算法将不再为多项式时间。

由于 T 函数是由加法、减法、乘法、与、或、非 6 种基本运算组合而成，考虑到每一种基本运算窄度的大小，该算法实际适用于任意加法、减法、与、或、非及某些数乘（如左移运算）组合而成的 T 函数。在现有基于 T 函数设计的密码算法中，该快速算法能够有效适用于 eSTREAM 中提交的密码算法 ABC、TSC 系列（TSC-1、TSC-2、TSC-3 及 TSC-4）中的 T 函数。但对于乘法运算（如 Klimov 和 Shamir 提出的 T 函数 $f(x)=x+(x^2\vee 5)\bmod 2^n$），由于其分位函数的表达式难以具体给出且窄度大小与 n 的取值有关，该算法对于降低计算此类 T 函数的 Walsh 谱值及差分转移概率的时间复杂性效果并不明显。

4 算法应用实例

下面使用定理 2 及定理 3 的快速算法，研究 TSC 系列中 T 函数的 Walsh 谱值计算及差分转移概率计算。由于 TSC 系列 T 函数构造相似，下面以计算 TSC-2 中 T 函数的 Walsh 谱值为例。

文献[3]给出了 TSC-2 中 T 函数的描述如下。

设 x_0，x_1，x_2，$x_3\in F_2^n$，$\boldsymbol{x}=(x_0,x_1,x_2,x_3)^{\mathrm{T}}$。$F_2^{4n}\to F_2^{4n}$ 上的单圈 T 函数

$$T(x)=x\oplus(\alpha(x)\wedge(x\oplus S(x))) \tag{1}$$

是 TSC-2 序列密码算法中的 T 函数。

下面对其中的符号逐一说明。

$\boldsymbol{x}$ 的第 i 路输出：$[\boldsymbol{x}]_i=([\boldsymbol{x}_0]_i,[\boldsymbol{x}_1]_i,[\boldsymbol{x}_2]_i,[\boldsymbol{x}_3]_i)^{\mathrm{T}}\in F_2^{4n}$，其中 $[\boldsymbol{x}_j]_i\in F_2$，$j=0,1,2,3$，$i=0,1,\cdots,n-1$。

$S(x)$ 是 $F_2^{4n}\to F_2^{4n}$ 上的映射，且 $S(x)=(s([x]_{n-1}),\cdots,s([x]_1),s([x]_0))$。$S(x)$的第 i 路输出为 $[S(x)]_i=s([x]_i)$，其中 $s(y)$是 F_2^4 上的单圈 S 盒，并且 $s(y)$的取值可用数组表示为 s={5,2,11,12,13,4,3,14,15,8,1,6,7,10,9,0}，数组中的值分别表示 $s(y)$在 y 遍历 0,1,⋯,15 时的取值。

$\alpha(x)=(p+1)\oplus p\oplus 2s_1$ 是 $F_2^{4n}\to F_2^n$ 上的参数，其中，$p=x_0\wedge x_1\wedge x_2\wedge x_3$，$s_1=(x_0+x_1+x_2+x_3)\bmod 2^n$。

$\alpha\wedge x=(\alpha\wedge x_0,\alpha\wedge x_1,\alpha\wedge x_2,\alpha\wedge x_3)^{\mathrm{T}}$。

$T(x)$的第 i 路输出为 $[T(x)]_i=\begin{cases}[x]_i, & [\alpha(x)]_i=0\\ s([x]_i), & [\alpha(x)]_i=1\end{cases}$，

其中，$i=0,1,\cdots,n-1$。

由算法 1 的 Step1，首先求 T 函数式(1)的窄度。

定理 4 TSC-2 中 T 函数 $T(x)$的窄度不超过 4。

证明 构造映射 λ_i 及变量 a_i，i=1,⋯,n−1

$$\lambda_1=2([x_0]_0+[x_1]_0+[x_2]_0+[x_3]_0)\|([x_0]_0\wedge[x_1]_0\wedge[x_2]_0\wedge[x_3]_0)$$

$$\lambda_i=([x_0]_{i-1}+[x_1]_{i-1}+[x_2]_{i-1}+[x_3]_{i-1}+[a_{i-1}]_2)\|([x_0]_{i-1}\wedge[x_1]_{i-1}\wedge[x_2]_{i-1}\wedge[x_3]_{i-1}\wedge[a_{i-1}]_0),i=2,\cdots,n$$

$$a_1=\lambda_1([x]_0),\ a_i=\lambda_i([x]_{i-1},a_{i-1}),i=2,\cdots,n$$

此时，$T(x)$可以表示成

$[T(x)]_0=s([x]_0)$，$[T(x)]_i=f_i([x]_i,a_i)=[x]_i\oplus([a_i]_0\oplus[a_i]_1)([x]_i\oplus s([x]_i))(i=1,\cdots,n)$

而 a_i，i=1,⋯,n−1 比特数至多为 4，根据定义 7，T 函数的窄度不超过 4。

下面构造预存矩阵。由定理 2 的证明，$T(x)$的每一路输出函数仅有 2 种表达形式，$[T(x)]_0$和$[T(x)]_i$ (i=1,⋯,n)。所以，此时存储量为 256 个16×16矩阵和 256 个16×1矩阵，共占存储空间 340 kB。

其中设 $\alpha=(\alpha_0,\alpha_1,\alpha_2,\alpha_3)^{\mathrm{T}},\beta=(\beta_0,\beta_1,\beta_2,\beta_3)^{\mathrm{T}}$，$\alpha_k,\beta_k\in F_2(k=0,1,2,3)$，$s=\sum_{k=0}^{3}2^k(\alpha_k+2^4\beta_k)$，则 $\boldsymbol{A}_s^{(0)}$ 的第 d 行与 $\boldsymbol{A}_s$ 的第 d 行第 c 列的值分别为

$$(\boldsymbol{A}_s^{(0)})_d=|\{\boldsymbol{x}\in F_2^4:\alpha\boldsymbol{x}\oplus\beta s(x)=0,\lambda_1(x)=d\}|-|\{\boldsymbol{x}\in F_2^4:\alpha\boldsymbol{x}\oplus\beta s(x)=1,\lambda_1(x)=d\}|$$

$$(\boldsymbol{A}_s)_{(d,c)}=|\{\boldsymbol{x}\in F_2^4:\alpha\boldsymbol{x}\oplus\beta f_i(x,c)=0,\lambda_{i+1}(x,c)$$

$=d\}|-|\{\boldsymbol{x}\in F_2^4:\alpha\boldsymbol{x}\oplus\beta f_i(x,c)=1,\lambda_{i+1}(x,c)=d\}|$

由此，TSC-2 中 T 函数在任意点 (α,β) $(\alpha=(\alpha_0,\alpha_1,\alpha_2,\alpha_3)^{\mathrm{T}}=([\alpha]_{n-1},\cdots,[\alpha]_0),\beta=(\beta_0,\beta_1,\beta_2,\beta_3)^{\mathrm{T}}$，$=([\beta]_{n-1},\cdots,[\beta]_0),[\alpha]_i,[\beta]_i\in F_{2^4},i=n-1,\cdots,0)$ 的 Walsh 谱值均可快速计算，表达式如下。

$$\boldsymbol{W}_{T(x)}(\alpha\to\beta)=\frac{1}{2^{4n}}\sum_{x=0}^{2^{4n}-1}(-1)^{\boldsymbol{\alpha x}\oplus\boldsymbol{\beta}T(x)}$$

$$=\frac{1}{2^{4n}}\boldsymbol{L}\boldsymbol{A}_{s_{n-1}}\boldsymbol{A}_{s_{n-2}}\cdots\boldsymbol{A}_{s_1}\boldsymbol{A}_{s_0}^{(0)}$$

其中，$\boldsymbol{L}$=(11…1) 是 16 维行向量，$s_i=\sum_{k=0}^{3}2^k[\alpha_k]_i+\sum_{k=0}^{3}16[\beta_k]_i,i=n-1,\cdots,0$。

5　结束语

本文基于 T 函数窄度的概念，将 T 函数 Walsh 谱值和差分转移概率的计算转化成 n 个矩阵相乘，提出了 T 函数 Walsh 谱值和差分转移概率快速算法，其时间复杂度均为 $O(n)$。并将该算法实际运用于研究 TSC 系列 T 函数 Walsh 谱值和差分转移概率，给出了计算结果表达式，说明了算法的可行性。该算法适用于任意加法、减法、与、或、非及某些数乘组合而成的 T 函数。而对于乘法，下一步将着重研究其分位函数的具体表示，根据其结构特点，进一步得到适用于乘法的 T 函数 Walsh 谱值和差分转移概率的快速算法。

参考文献：

[1] KLIMOV A, SHAMIR A. A new class of invertible mappings[A]. Workshop on Cryptographic Hardware and Embedded Systems (CHES)[C]. 2003.470-483.

[2] WIRT K. ASC-A stream cipher with built-in Mac functionality[J]. International Journal of Computer Science, 2007, 2(2):131.

[3] HONG, J LEE D, YEOM Y, HAN D. A new class of single cycle T-functions[J]. Fast Software Encryption, Springer,2005, 3557:68-82.

[4] HONG J, LEE D, YEOM Y, HAN D, CHEE S. T-function based stream cipher TSC-3, 2005[EB/OL]. http://www.ecrypt.eu.org/stream/ciphers/tsc3/tsc3.pdf.

[5] MOON D, KWON D, HAN D, *et al*. T-function based stream cipher TSC-4, 2005[EB/OL]. http://www.ecrypt.eu.org/ stream /ciphers /tsc4/tsc4.pdf.

[6] MAXIMOV A. A new stream cipher “Mir-1” [EB/OL]. http://www.ecrypt.eu.org/stream,2008.

[7] DAUM M. Narrow T-function[J]. Fast Software Encryption, Springer, 2005, 3557:50-67.

[8] ANASHIN V, KHRENNILOV A. Applied algebraic dynamics[J]. P-Adic Numbers, Ultrahcetric Analysis, and Application, 2010, 2(4): 360-362.

[9] ANASHIN V, KHRENNILOV A, YUROVA E. T-function revisited: new criteria for bijectivity/transitivity[J]. Designs, Codes and Cryptography, 2014, 71(3): 383-407.

[10] NYBERG K, WALLEN J. Improved linear distinguishers for SNOW2.0[J]. Fast Software Encryption, Springer,2006,4047:144-162.

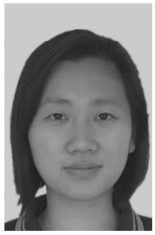
[11] 常亚勤, 金晨辉. 环 $Z/2^n$ 上仿射函数 Walsh 谱的快速算法[J]. 上海交通大学学报,2011,45(3):321-326.
CHANG Y Q, JIN C H. Fast computation of Walsh spectrum of affine function over the ring $Z/2^n$[J]. Journal of shanghai Jiaotong University (Science), 2011, 45(3): 321326.

[12] 方兆本,缪柏其.随机过程第 2 版[M]. 北京: 科学出版社, 2004.
FANG Z B, MIN B Q. Stochastic Process(2nd Edition)[M]. Beijing: Science Press, 2004.

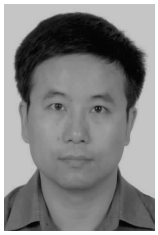
[13] 金晨辉, 郑浩然, 张少武等. 密码学[M].北京：高等教育出版社，2009.
JIN C H, ZHENG H R, ZHANG S W, *et al*. Cryptology[M]. Beijing: Higher Education Press, 2009.

[14] LE G, FRANÇOIS. Powers of tensors and fast matrix multiplication[A]. Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation (ISSAC 2014)[C].2014.

作者简介



刘燕（1990-），女，江苏南通人，解放军信息工程大学硕士生，主要研究方向为密码学与信息安全。



胡斌（1971-），男，河南新县人，解放军信息工程大学教授、博士生导师，主要研究方向为密码学与信息安全。

徐立平（1989-），男，山东济阳人，解放军信息工程大学硕士生，主要研究方向为密码学与信息安全。