Pure Mathematics 理论数学, 2026, 16(2), 241-247
Published Online February 2026 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2026.162054

Hans汉斯

一类可逆移位不变函数的构造

丁肇鹏*#，石景琦

青岛大学数学与统计学院，山东 青岛

收稿日期：2026年1月9日；录用日期：2026年2月5日；发布日期：2026年2月13日

摘　要

在面向安全多方计算、全同态加密与零知识证明等的对称密码构件的设计中，人们需在大素数有限域上构造乘法复杂度低且可逆的非线性层。移位不变函数因其良好的非线性结构与实现优势而被广泛采用，Lai-Massey构造是其中具有代表性的一类。本文基于广义的Lai-Massey构造，提出了更一般的可逆移位不变函数的构造方法，为面向算术的非线性层设计提供了更丰富的可逆向量值函数。

关键词

Lai-Massey构造，有限域，置换，移位不变函数，循环矩阵

A Construction of a Class of Invertible Shift-Invariant Functions

Zhaopeng Ding*#, Jingqi Shi

School of Mathematics and Statistics, Qingdao University, Qingdao Shandong

Received: January 9, 2026; accepted: February 5, 2026; published: February 13, 2026

Abstract

In the design of symmetric cryptographic components for secure multi-party computation, fully homomorphic encryption, and zero-knowledge proofs, one needs to construct nonlinear layers over large prime finite fields that are both invertible and of low multiplicative complexity. Shift invariant functions are widely adopted due to their favorable nonlinear structure and implementation advantages, with the Lai-Massey construction being a representative example. Building on generalized Lai-Massey constructions, this paper proposes a more general method for constructing invertible shift-invariant functions, providing a richer collection of invertible vector valued functions for

*第一作者。
#通讯作者。

文章引用: 丁肇鹏, 石景琦. 一类可逆移位不变函数的构造[J]. 理论数学, 2026, 16(2): 241-247.
DOI: 10.12677/pm.2026.162054

arithmetization-oriented nonlinear layer design.

Keywords

Lai-Massey Construction, Finite Fields, Permutations, Shift-Invariant Functions, Circulant Matrices

1. 引言

近些年来，随着安全多方计算(Secure Multi-Party Computation, MPC)、全同态加密(Fully Homomorphic Encryption, FHE)以及零知识证明(Zero-Knowledge proofs, ZK)等广泛的应用，对称密码的基本构件的设计有了新的要求，其设计重心从传统的运算友好转向在大素数域上减少乘法的次数，即减小乘法复杂度。这一趋势在面向算术化的密码方案中表现得尤为明显(参见文献[1]-[7])。由此，构造一个具有低乘法复杂度且可逆的非线性层成为了值得关注的问题：一方面需要非线性层具有可逆性以支撑迭代轮函数的置换性质，另一方面非线性层需保持足够的代数复杂性质以抵抗代数攻击。

众所周知，迭代型对称密码算法通常是对轮函数进行多轮迭代实现加解密的，而轮函数往往可分解为“非线性层 + 线性层”，可写作

$$x \mapsto c + M \cdot S\text{-Box}(x),$$

其中 S-Box 为非线性层， M 为可逆的线性层， c 为轮常数。在面向算术化的对称密码算法中仍使用这种迭代结构，只是底层运算从二元域上的比特运算拓展为素数阶有限域上的运算。Lorenzo Grassi 等在文献[8]中针对非线性层的构造，定义了一类移位不变(shift-invariant)函数 S_F：从一个局部映射 $F:\mathbb{F}_p^m \to \mathbb{F}_p$ 出发，在 $\mathbb{F}_p^n$ 上定义映射

$$S_F(x_0,\cdots,x_{n-1}) = (y_0,\cdots,y_{n-1}), \quad y_i = F(x_i,x_{i+1},\cdots,x_{i+m-1}),$$

其中指标按 n 取模。该函数 S_F 具有移位不变性，即对 $\mathbb{F}_p^n$ 上的任意平移置换 Π 都有 $S_F \circ \Pi = \Pi \circ S_F$，我们把由局部映射 $F:\mathbb{F}_p^m \to \mathbb{F}_p$ 所定义的移位不变函数 S_F 称为由 F 诱导的移位不变 (m,n)-提升函数。上述定义的移位不变函数在二元域上的例子是 Wolfram 在文献[9]中定义的 χ 函数，随后 Daemen 在文献[10]对其进行了系统的分析并证明了 χ 所诱导的移位不变函数在奇数长度上可逆。χ 函数的应用参见文献[11]，[12]等。

然而，将上述可逆构造直接迁移到大素域 $\mathbb{F}_p$ 并不顺利。我们期望构造的是以低次数(尤其是二次)局部映射 F 作为基本单元，在较大 n 上得到可逆的 S_F，从而在每轮仅用 $O(n)$ 甚至更少的乘法实现非线性层。文献[8]给出了如下结果：当局部映射 F 为二次多项式时，使 S_F 成为可逆映射的 n 存在上界，即对于 $m=2$，若 $n \geq 3$ 则不存在二次多项式 F 使 S_F 成为可逆映射；对于 $m=3$，$n \geq 5$ 同样不存在可逆映射 S_F，并进一步猜想，当局部映射 F 为二次多项式时，对于固定的 m，使 S_F 成为可逆映射的 n 的上界为 $2m-1$。

尽管存在上述结论，但是在某些具备特殊结构且满足一定条件的局部映射族中，可逆是必然存在的。文献[13]给出了一个例子即 Lai-Massey 构造：由 $\mathbb{F}_p^2 \to \mathbb{F}_p$ 的局部映射 $F(x_0,x_1) = x_0 + (x_0 - x_1)^2$ 诱导的移位不变函数

$$S_F(x_0,x_1) = x_0 + (x_0 - x_1)^2 \,\|\, x_1 + (x_1 - x_0)^2,$$

可验证 $S_F\left(x_0,x_1\right)$ 是可逆的。文献[8]给出了对 Lai-Massey 构造的如下两种推广。

命题 1 ([8]) 设 $p\geq 2$ 为素数。令 $n=m\geq 2$，并满足 n 是 p 的倍数(即 $n\equiv 0\ (\mathrm{mod}\ p)$)或 n 是偶数。令局部映射为

$$F\left(x_0,\cdots,x_{n-1}\right)=\sum_{i=0}^{n-1}\mu_i x_i+H\left(\sum_{i=0}^{n-1}\omega_i x_i\right),$$

其中 $\left(\mu_0,\cdots,\mu_{n-1}\right)\in\mathbb{F}_p^n$ 满足其构成的循环矩阵 $\mathrm{circ}\left(\mu_0,\cdots,\mu_{n-1}\right)\in\mathbb{F}_p^{n\times n}$ 可逆，并且 ω_i 与 H 满足：

1) 若 $n\equiv 0\ (\mathrm{mod}\ p)$，则对每个 $i\in\{0,1,\cdots,n-1\}$ 有 $\omega_i=1$；

2) 若 $n\equiv 0\ (\mathrm{mod}\ 2)$，则对每个 $i\in\{0,1,\cdots,n-1\}$ 有 $\omega_i=(-1)^i$，并且 $H:\mathbb{F}_p\to\mathbb{F}_p$ 为偶函数，即对于任意 $t\in\mathbb{F}_p$ 有 $H(-t)=H(t)$。

则由 F 在 $\mathbb{F}_p^n$ 上诱导的移位不变函数 S_F 是可逆的。

命题 2 ([8]) 设 $p\geq 2$ 为素数，令 $n=m\geq 2$。设 $\mu=\left(\mu_0,\cdots,\mu_{n-1}\right)\in\mathbb{F}_p^n$，使得循环矩阵 $C:=\mathrm{circ}\left(\mu_0,\cdots,\mu_{n-1}\right)\in\mathbb{F}_p^{n\times n}$ 可逆，取 $\gamma\in\mathbb{F}_p\setminus\{0\}$。令 $H:\mathbb{F}_p\to\mathbb{F}_p$ 为任意函数，并定义 $F:\mathbb{F}_p^n\to\mathbb{F}_p$ 为

$$F\left(x_0,\cdots,x_{n-1}\right)=\sum_{i=0}^{n-1}\mu_i x_i+\gamma\sum_{i=0}^{n-1}H\left(x_i-x_{i+1}\right),$$

其中下标均按 n 取模。则由 F 在 $\mathbb{F}_p^n$ 上诱导的移位不变函数 S_F 是可逆的。

上述的命题 1 和命题 2 给出了两类可逆的移位不变函数 S_F 的构造。本文进一步推广了上述结果。首先，对于命题 1，我们考虑了在 n 更一般的情况下，ω_i 与 H 所满足的限制条件，从而给出了更一般的可逆的移位不变函数 S_F；其次对于命题 2，我们将局部映射函数做进一步推广，并证明其诱导的移位不变函数依然可逆。通过对命题 1 和命题 2 的推广，可为密码算法提供更为丰富的可逆移位不变函数的构造。

2. 预备知识

设 $p\geq 2$ 为素数，令 $\mathbb{F}_p$ 表示模 p 的整数域，并令 $\mathbb{F}_p^n$ 表示当 $n\geq 1$ 时相应的向量空间。给定 $x\in\mathbb{F}_p^n$，对每个 $i\in\{0,1,\cdots,n-1\}$，用 x_i 表示它的第 i 个分量，即

$$x=\left(x_0,x_1,\cdots,x_{n-1}\right)\text{ 或 }x=x_0\|x_1\|\cdots\|x_{n-1}.$$

定义 1 令 $p\geq 2$ 为素数。取整数 $1\leq m\leq n$，令 $F:\mathbb{F}_p^m\to\mathbb{F}_p$ 为一个非线性映射。定义 $\mathbb{F}_p^n$ 上的移位不变函数 S_F 为

$$S_F\left(x_0,\cdots,x_{n-1}\right)=y_0\|y_1\|\cdots\|y_{n-1},$$

其中 $y_i=F\left(x_i,x_{i+1},\cdots,x_{i+m-1}\right)$，并且下标按 n 取模。

记 $\mathrm{circ}\left(\mu_0,\cdots,\mu_{n-1}\right)\in\mathbb{F}_p^{n\times n}$ 为如下的循环矩阵：

$$\mathrm{circ}\left(\mu_0,\mu_1,\cdots,\mu_{n-1}\right):=\begin{bmatrix}\mu_0 & \mu_1 & \cdots & \mu_{n-2} & \mu_{n-1}\\ \mu_{n-1} & \mu_0 & \cdots & \mu_{n-3} & \mu_{n-2}\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \mu_1 & \mu_2 & \cdots & \mu_{n-1} & \mu_0\end{bmatrix}.$$

3. 主要结果

在本节中，我们给出命题 1 和命题 2 的进一步推广。

定理 1 设 $p\geq 2$ 为素数。令 $n=m\geq 2$，并满足 n 是 p 的倍数(即 $n\equiv 0\ (\mathrm{mod}\ p)$)或 $\gcd(n,p-1)>1$。令局部映射为

$$F\left(x_0,x_1,\cdots,x_{n-1}\right)=\sum_{i=0}^{n-1}\mu_i x_i+H\left(\omega_0x_0+\omega_1x_1+\cdots+\omega_{n-1}x_{n-1}\right),$$

其中$\left(\mu_0,\cdots,\mu_{n-1}\right)\in\mathbb{F}_p^n$满足其构成的循环矩阵$\operatorname{circ}\left(\mu_0,\cdots,\mu_{n-1}\right)\in\mathbb{F}_p^{n\times n}$可逆，并且$\omega_i$与$H$满足：

1) 若$n\equiv 0\ (\mathrm{mod}\ p)$，则对每个$i\in\{0,1,\cdots,n-1\}$有$\omega_i=1$；

2) 若$\gcd(n,p-1)>1$，则对每个$i\in\{0,1,\cdots,n-1\}$有$\omega_i=\lambda^i$，其中$\lambda\neq 1$为$\mathbb{F}_p$上的n次单位根(即$\lambda^n=1$)，且$H:\mathbb{F}_p\to\mathbb{F}_p$满足对于任意$t\in\mathbb{F}_p$有$H(\lambda t)=H(t)$。

则由F在$\mathbb{F}_p^n$上诱导的移位不变函数S_F是可逆的。

证明 令$x=\left(x_0,\cdots,x_{n-1}\right)^{\mathrm{T}}\in\mathbb{F}_p^n$，$y=S_F(x)=\left(y_0,\cdots,y_{n-1}\right)^{\mathrm{T}}$。并记循环矩阵$C:=\operatorname{circ}\left(\mu_0,\cdots,\mu_{n-1}\right)$。对每个$k\in\{0,1,\cdots,n-1\}$，$S_F$的第$k$个坐标满足

$$y_k=\sum_{i=0}^{n-1}\mu_i x_{k+i}+H\left(\sum_{i=0}^{n-1}\omega_i x_{k+i}\right),$$

令$T:=\sum_{i=0}^{n-1}\omega_i x_i\in\mathbb{F}_p$，我们先说明对任意$k$都有

$$H\left(\sum_{i=0}^{n-1}\omega_i x_{k+i}\right)=H(T),$$

若$n\equiv 0\ (\mathrm{mod}\ p)$且$\omega_i=1$，此时

$$\sum_{i=0}^{n-1}\omega_i x_{k+i}=\sum_{i=0}^{n-1}x_{k+i}=\sum_{i=0}^{n-1}x_i=T,$$

若$\gcd(n,p-1)>1$且$\omega_i=\lambda^i$、$\lambda\neq 1$、$\lambda^n=1$。则对任意k都有，

$$\sum_{i=0}^{n-1}\omega_i x_{k+i}=\sum_{i=0}^{n-1}\lambda^i x_{k+i}=\lambda^{-k}\sum_{j=0}^{n-1}\lambda^j x_j=\lambda^{-k}T,$$

又因$H(\lambda t)=H(t)$对所有t成立，从而$H\left(\lambda^{-k}T\right)=H(T)$。

因此对所有k都有

$$y_k=\sum_{i=0}^{n-1}\mu_i x_{k+i}+H(T),$$

即向量形式

$$y=Cx+H(T)\boldsymbol{1},\qquad \boldsymbol{1}:=(1,\cdots,1)^{\mathrm{T}}\in\mathbb{F}_p^n.$$

令$\mu':=\sum_{i=0}^{n-1}\mu_i\in\mathbb{F}_p$，注意到$C\boldsymbol{1}=\mu'\boldsymbol{1}$，因此若$\mu'=0$则$C$有非零核向量$\boldsymbol{1}$与$C$可逆矛盾，故$\mu'\neq 0$。于是$C\left(\frac{1}{\mu'}\boldsymbol{1}\right)=\boldsymbol{1}$，从而

$$y=C\left(x+\frac{H(T)}{\mu'}\boldsymbol{1}\right).$$

令$z:=C^{-1}y$，则$z=x+\frac{H(T)}{\mu'}\boldsymbol{1}$。接下来取$\omega$的加权和：

$$\sum_{i=0}^{n-1}\omega_i z_i=\sum_{i=0}^{n-1}\omega_i x_i+\frac{H(T)}{\mu'}\sum_{i=0}^{n-1}\omega_i=T+\frac{H(T)}{\mu'}\sum_{i=0}^{n-1}\omega_i.$$

下面我们说明$\sum_{i=0}^{n-1}\omega_i=0$在两种情形下都成立：

若$\omega_i=1$，则$\sum_{i=0}^{n-1}\omega_i=n\equiv 0\ (\mathrm{mod}\ p)$。

若$\omega_i=\lambda^i$且$\lambda\neq 1$、$\lambda^n=1$，则$\sum_{i=0}^{n-1}\omega_i=\sum_{i=0}^{n-1}\lambda^i=0$。

因此总有$\sum_{i=0}^{n-1}\omega_i z_i=T$。于是$H(T)=H\left(\sum_{i=0}^{n-1}\omega_i z_i\right)$可由$z$唯一确定，并且

$$x=z-\frac{1}{\mu'}H\left(\sum_{i=0}^{n-1}\omega_i z_i\right)\boldsymbol{1}.$$

这给出了从y唯一恢复x的显式逆映射，从而S_F是可逆的。证毕。

注释 1 注意到，由定理 1 的条件 2，我们可以取n为偶数，$\lambda=-1$为$\mathbb{F}_p$上的n次单位根，此时$H:\mathbb{F}_p\to\mathbb{F}_p$为偶函数，由此可见文献[8]中的命题 1 为定理 1 的一个特殊情况。

推论 1 设p为素数，$\lambda\in\mathbb{F}_p\setminus\{0\}$，$H:\mathbb{F}_p\to\mathbb{F}_p$为二次多项式函数$H(t)=at^2+bt+c$，且$a\neq 0$。若对任意$t\in\mathbb{F}_p$都有$H(\lambda t)=H(t)$，则必有$\lambda^2=1$。并且若$\lambda=-1$，则必有$b=0$(即$H(t)=at^2+c$)。

证明 由$H(\lambda t)=a(\lambda t)^2+b(\lambda t)+c=a\lambda^2t^2+b\lambda t+c$与$H(t)=at^2+bt+c$对所有$t$恒等，得

$$a\left(\lambda^2-1\right)t^2+b(\lambda-1)t=0\quad(\forall t\in\mathbb{F}_p).$$

作为多项式恒等式，其系数必须为零，故$a\left(\lambda^2-1\right)=0$，$b(\lambda-1)=0$。由$a\neq 0$得$\lambda^2=1$。此外若$\lambda=-1\neq 1$，则由$b(\lambda-1)=0$推出$b=0$。证毕。

由推论 1 可知，当局部映射$F:\mathbb{F}_p^m\to\mathbb{F}_p$为二次函数时，非平凡的单位根的取值只能是$\lambda=-1$。

类似推论 1 的证明，可得如下结论。

推论 2 设p为素数且$p>3$，$\lambda\in\mathbb{F}_p$，并令$H(t)=a_st^s+a_{s-1}t^{s-1}+\cdots+a_0$为任意$s$次多项式且$a_s\neq 0$。若对任意$t\in\mathbb{F}_p$都有$H(\lambda t)=H(t)$，则必有

$$\lambda^s=1,\quad a_{s-1}\left(\lambda^{s-1}-1\right)=0,\cdots,a_1(\lambda-1)=0.$$

特别地，当λ为本原s次单位根时，必有$a_{s-1}=\cdots=a_1=0$，从而$H(t)=a_st^s+a_0$。

定理 2 设$p\geq 2$为素数，令$n=m\geq 2$。设$\mu=(\mu_0,\cdots,\mu_{n-1})\in\mathbb{F}_p^n$，使得循环矩阵$C:=\mathrm{circ}(\mu_0,\cdots,\mu_{n-1})\in\mathbb{F}_p^{n\times n}$可逆。取$\gamma\in\mathbb{F}_p\setminus\{0\}$，整数$r$满足$2\leq r\leq n$，并取$a=(a_0,\cdots,a_{r-1})\in\mathbb{F}_p^r$满足$\sum_{j=0}^{r-1}a_j=0$。令$H:\mathbb{F}_p\to\mathbb{F}_p$为任意函数，并定义局部映射$F:\mathbb{F}_p^n\to\mathbb{F}_p$为

$$F(x_0,\cdots,x_{n-1})=\sum_{i=0}^{n-1}\mu_ix_i+\gamma\sum_{i=0}^{n-1}H\left(\sum_{j=0}^{r-1}a_jx_{i+j}\right),$$

其中下标均按n取模。则由F在$\mathbb{F}_p^n$上诱导的移位不变函数S_F是可逆的。

证明令$x=(x_0,\cdots,x_{n-1})^{\mathrm{T}}\in\mathbb{F}_p^n$，并令$y=S_F(x)=(y_0,\cdots,y_{n-1})^{\mathrm{T}}$。记

$$g(x):=\sum_{i=0}^{n-1}H\left(\sum_{j=0}^{r-1}a_jx_{i+j}\right)\in\mathbb{F}_p,$$

则有$F(x)=\sum_{i=0}^{n-1}\mu_ix_i+\gamma g(x)$。令$\sigma$表示循环移位算子，即$\left(\sigma^kx\right)_t=x_{t+k}$(下标按$n$取模)。则对任意$k$，

$$g\left(\sigma^k x\right)=\sum_{i=0}^{n-1}H\left(\sum_{j=0}^{r-1}a_j\left(\sigma^k x\right)_{i+j}\right)=\sum_{i=0}^{n-1}H\left(\sum_{j=0}^{r-1}a_j x_{i+j+k}\right).$$

令 $i'=i+k$，由于外层对 i 的求和是循环的，可得

$$g\left(\sigma^k x\right)=\sum_{i'=0}^{n-1}H\left(\sum_{j=0}^{r-1}a_j x_{i'+j}\right)=g\left(x\right).$$

因此由定义 1，第 k 个输出坐标为

$$y_k=F\left(x_k,x_{k+1},\cdots,x_{k+n-1}\right)=\sum_{i=0}^{n-1}\mu_i x_{k+i}+\gamma g\left(\sigma^k x\right)=\sum_{i=0}^{n-1}\mu_i x_{k+i}+\gamma g\left(x\right).$$

令 $\boldsymbol{1}=\left(1,\cdots,1\right)^{\mathrm{T}}\in\mathbb{F}_p^n$，则可写成

$$y=Cx+\gamma g\left(x\right)\boldsymbol{1}.$$

记 $\mu':=\sum_{i=0}^{n-1}\mu_i\in\mathbb{F}_p$。注意到 $C\boldsymbol{1}=\mu'\boldsymbol{1}$。由 C 是可逆矩阵，所以 $\mu'\neq 0$。于是 $C^{-1}\boldsymbol{1}=\frac{1}{\mu'}\boldsymbol{1}$。令 $z:=C^{-1}y$，则

$$z=C^{-1}y=x+\gamma g\left(x\right)C^{-1}\boldsymbol{1}=x+\frac{\gamma}{\mu'}g\left(x\right)\boldsymbol{1}.$$

记 $\alpha:=\frac{\gamma}{\mu'}g\left(x\right)$，则 $z=x+\alpha\boldsymbol{1}$。由 $\sum_{j=0}^{r-1}a_j=0$，对任意 i 有

$$\sum_{j=0}^{r-1}a_j z_{i+j}=\sum_{j=0}^{r-1}a_j\left(x_{i+j}+\alpha\right)=\sum_{j=0}^{r-1}a_j x_{i+j}+\alpha\sum_{j=0}^{r-1}a_j=\sum_{j=0}^{r-1}a_j x_{i+j}.$$

因此

$$g\left(z\right)=\sum_{i=0}^{n-1}H\left(\sum_{j=0}^{r-1}a_j z_{i+j}\right)=\sum_{i=0}^{n-1}H\left(\sum_{j=0}^{r-1}a_j x_{i+j}\right)=g\left(x\right).$$

从而 $\alpha=\frac{\gamma}{\mu'}g\left(x\right)=\frac{\gamma}{\mu'}g\left(z\right)$ 可由 z 唯一确定，并且 $x=z-\frac{\gamma}{\mu'}g\left(z\right)\boldsymbol{1}$。这给出了从任意 y 唯一恢复 x 的逆映射，因此 S_F 可逆。证毕。

注释 2 注意到当 $r=2$，$a=\left(1,-1\right)$，可得到

$$F\left(x\right)=\sum_{i=0}^{n-1}\mu_i x_i+\gamma\sum_{i=0}^{n-1}H\left(x_i-x_{i+1}\right),$$

即文献[8]中命题 2 给出的局部映射。我们可以取更一般的形式，当 $r=4$，$a=\left(1,-1,1,-1\right)$，可得到

$$F\left(x\right)=\sum_{i=0}^{n-1}\mu_i x_i+\gamma\sum_{i=0}^{n-1}H\left(x_i-x_{i+1}+x_{i+2}-x_{i+3}\right).$$

需要强调的是，本文关注的对象是单轮非线性层，其设计目标侧重于在大素数有限域上实现低乘法复杂度与可逆性。因为在 MPC/FHE/Zk 这类算数化场景中，系统开销几乎由乘法门数主导的，因此乘法复杂度决定了非线性层在证明规模、约束数、运行时间上的成本上限。下面我们给出定理 1 和定理 2 两种移位不变函数的乘法复杂度(只统计非线性乘法门数目 $M\left(\cdot\right)$)。对于定理 1 中的可逆移位不变函数，由其构造可知正向计算仅需要对 H 做一次求值。于是

$$M\left(S_F\right)=M\left(H\right),\quad M\left(S_F^{-1}\right)=M\left(H\right)$$

其中 $M(H)$ 为在 $\mathbb{F}_p$ 上计算一次 H 所需的乘法门数。特别地，若取 $H(t)=at^2+b$，则 $M(H)=1$；若取 $H(t)=at^3+b$，则可按 t^2 与 $t^3=t^2\cdot t$ 计算，得到 $M(H)=2$。并且如果 $C\coloneqq \mathrm{circ}(1,0,\cdots,0)$ 且 H 为 2 次多项式计算 S_F 仅需 1 次 $\mathbb{F}_p$ 乘法。对于定理 2，同理可以得到

$$M(S_F)=nM(H),\quad M\left(S_F^{-1}\right)=nM(H)$$

乘法复杂度与状态长度 n 线性相关。

因此定理 1 的乘法复杂度与 n 无关，而定理 2 的乘法复杂度随 n 线性增长。最后我们需要声明的是低乘法复杂度是以更强的代数结构为代价获取的，因此这些构造更适合作为多轮结构中低成本模块，而非单独使用的安全置换。

4. 结论

基于文献[8]中对 Lai-Massey 构造的推广，本文进一步给出了一类更一般的移位不变函数的构造，从而为密码算法提供更为丰富的移位不变函数。

参考文献

[1] Albrecht, M., Grassi, L., Rechberger, C., Roy, A. and Tiessen, T. (2016) MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity. In: Cheon, J. and Takagi, T., Eds., *Advances in Cryptology—ASIACRYPT* 2016, Springer, 191-219. https://doi.org/10.1007/978-3-662-53887-6_7

[2] Albrecht, M.R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., *et al.* (2019) Feistel Structures for MPC, and More. In: Sako, K., Schneider, S. and Ryan, P., Eds., *Computer Security—ESORICS* 2019, Springer, 151-171. https://doi.org/10.1007/978-3-030-29962-0_8

[3] Grassi, L., Lüftenegger, R., Rechberger, C., Rotaru, D. and Schofnegger, M. (2020) On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy. In: Canteaut, A. and Ishai, Y., Eds., *Advances in Cryptology—EUROCRYPT* 2020, Springer, 674-704. https://doi.org/10.1007/978-3-030-45724-2_23

[4] Aly, A., Ashur, T., Ben-Sasson, E., Dhooghe, S. and Szepieniec, A. (2020) Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols. *IACR Transactions on Symmetric Cryptology*, **2020**, 1-45. https://doi.org/10.46586/tosc.v2020.i3.1-45

[5] Grassi, L., Khovratovich, D., Rechberger, C., Roy, A. and Schofnegger, M. (2021) Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. *Proceedings of the* 30*th USENIX Security Symposium* (*USENIX Security* 21), 11-13 August 2021, 519-535. https://www.usenix.org/conference/usenixsecurity21/presentation/grassi

[6] Ha, J., Kim, S., Choi, W., Lee, J., Moon, D., Yoon, H., *et al.* (2020) Masta: An He-Friendly Cipher Using Modular Arithmetic. *IEEE Access*, **8**, 194741-194751. https://doi.org/10.1109/access.2020.3033564

[7] Dobraunig, C., Grassi, L., Guinet, A. and Kuijsters, D. (2021) Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields. In: Canteaut, A. and Standaert, F.X., Eds., *Advances in Cryptology—EUROCRYPT* 2021, Springer, 3-34. https://doi.org/10.1007/978-3-030-77886-6_1

[8] Grassi, L., Onofri, S., Pedicini, M. and Sozzi, L. (2022) Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over Fnp. *IACR Transactions on Symmetric Cryptology*, **2022**, 20-72. https://doi.org/10.46586/tosc.v2022.i3.20-72

[9] Wolfram, S. (1986) Cryptography with Cellular Automata. In: Williams, H.C., Ed., *Advances in Cryptology—CRYPTO*'85 *Proceedings*, Springer, 429-432. https://doi.org/10.1007/3-540-39799-x_32

[10] Daemen, J. (1995) Cipher and Hash Function Design: Strategies Based on Linear and Differential Cryptanalysis. Ph.D. Thesis, Katholieke Universiteit Leuven. https://cs.ru.nl/~joan/

[11] Bertoni, G., Daemen, J., Peeters, M. and Van Assche, G. (2011) The Keccak Reference, Version 3.0. https://keccak.team/files/Keccak-reference-3.0.pdf

[12] Bertoni, G., Daemen, J., Peeters, M. and Van Assche, G. (2013) Keccak. In: Johansson, T. and Nguyen, P.Q., Eds., *Advances in Cryptology—EUROCRYPT* 2013, Springer, 313-314. https://doi.org/10.1007/978-3-642-38348-9_19

[13] Lai, X. and Massey, J.L. (1991) A Proposal for a New Block Encryption Standard. In: Damgård, I.B., Ed., *Advances in Cryptology—EUROCRYPT*'90, Springer, 389-404. https://doi.org/10.1007/3-540-46877-3_35