基于元胞自动机的 S 盒的性质与神经网络实现研究

黄俊君,关 杰
(解放军战略支援部队信息工程大学, 河南郑州 450001)

摘 要: 基于元胞自动机(CA)的 S 盒密码学性质良好且软硬件实现代价低,被用于 Keccak、SIMON 等密码算法. 本文研究了基于 CA 的 S 盒的性质,给出并证明了此类 S 盒的三个重要性质:移位不变性、镜面对称性和互补性;同时研究了基于 CA 的 S 盒的神经网络实现方法,指出相比一般的 S 盒,基于 CA 的 S 盒在进行神经网络实现时可以用更简单的结构、消耗更少的资源来完成,并且给出了一种权重阈值搜索算法可以方便快速地实现基于 CA 的 S 盒的神经网络结构.

关键词: 元胞自动机; S 盒; Keccak; 神经网络; 权重阈值; 搜索算法
中图分类号: TN918.1; TN302 **文献标识码:** A **文章编号:** 0372-2112 (2020)12-2462-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.12.023

Research on Properties and Neural Networks Implementation of Cellular Automata Based S-Boxes

HUANG Jun-jun, GUAN Jie
(*PLA SSF Information Engineering University, Zhengzhou, Henan* 450001, *China*)

Abstract: Cellular automata (CA) based S-boxes are the type of S-boxes with good cryptography and low cost of hardware as well as software implementation, which are used in Keccak, SIMON, and other cryptographic algorithms. This paper studied the properties of CA-based S-boxes, and the three important properties were given and proved, including shift invariance, mirror symmetry and complementarity. Meanwhile, the neural network implementation for CA-based S-boxes was studied, which demonstrated that the CA-based S-boxes could be implemented with simpler structure and less resources than the general one. In addition, a weight threshold search algorithm which could easily and quickly implement the neural network structure of CA-based S-boxes was shown.

Key words: cellular automata; S-boxes; Keccak; neural networks; weight and threshold; search algorithm

1 引言

在设计对称密码时,一般将 Shannon 提出的混乱和扩散[1]作为基本的设计原则,由于 S 盒(Substitution-boxes)可以为对称密码提供有效的混乱作用,因此作为重要部件被许多密码算法所使用.

元胞自动机[2](Cellular Automata, CA)是一种广泛应用在不同领域的用来模拟和分析复杂离散问题的并行运算模型. 在密码学中也被用来设计序列密码、分组密码、杂凑函数等. 同样可以将 CA 构型的变换过程定义为 S 盒的变换,这类 S 盒就是本文研究的基于 CA 的 S 盒,其实现代价低且有较好的安全性能. 因此已被广泛应用到许多密码算法中[3],最典型的如作为 SHA-3[4] 标准之一的 Keccak[5] 杂凑函数的 S 盒.

人工神经网络(Artificial Neural Networks, ANN)是可以用计算机程序或者硬件电路表示的能够模拟生物神经系统的并行互连的非线性自适应系统[6]. 神经网络的并行性、非线性计算、扩散性、混沌分类特性等性质使其应用于密码学领域成为可能. 文献[7]介绍了一种将任意一个 S 盒用 ANN 实现的方法,但是对于一个一般的 n 进 n 出 S 盒需要至少 n 个 ANN 才能将其实现. 而基于 CA 的 S 盒与一般的 S 盒相比仅用其 $1/n$ 的网

收稿日期:2019-10-11;修回日期:2020-07-06;责任编辑:覃怀银
基金项目:国家自然科学基金项目(No. 61572516, No. 61272041, No. 61272488)

络数量便可实现,具有相当的优势.

2　相关工作

2004 年 Mukhopadhyay 等[8]提出了一种自动化设计分组密码轮函数的框架,其中非线性 CA 的使用体现了基于 CA 的 S 盒的思想. 此后对基于 CA 的 S 盒的研究主要解决几个问题:

(1)如何找到性质良好且实现高效的基于 CA 的 S 盒. 文献[9,10]等都尝试将简单的 CA 代入特定结构以构造 S 盒,但这种方式很难找到符合一定要求的 S 盒;而文献[11]通过遗传算法搜索满足特定性质的 S 盒,是更为可行的方案.

(2)研究基于 CA 的 S 盒的密码学性质. 文献[12]研究一类基于 CA 的 S 盒的差分性质;文献[3]证明了基于 CA 的 S 盒的非线性度上界. 然而对这类 S 盒性质的探究并不足够,为了更好的把握其密码学性质,本文将进一步研究其一般性的性质.

(3)基于 CA 的 S 盒相比一般 S 盒的优势. Bitslice 技术是 Biham[13]为加速 DES 的软件实现效率提出的,基于 CA 的 S 盒适用 Bitslice 技术从而在实现效率上具有优势,Keccak 的设计就充分考虑了这一点. 而本文将说明这类 S 盒在神经网络的实现上相比一般的 S 盒也具有相当的优势.

3　基本概念

3.1　S 盒的密码学性质

将 m 进 n 出的 S 盒用映射 $F:Z_2^m\to Z_2^n$ 表示,m、n 都是正整数. 由于满足置换条件的 S 盒可以在许多密码体制中实现数据的唯一替代,是目前主流 S 盒必须满足的性质. 而 $m=n$ 是置换 S 盒的必要条件,因此本文研究的 S 盒限制在 $F:Z_2^n\to Z_2^n$.

除了置换性质,差分性质和线性性质也是 S 盒重要的密码学性质. 下面给出差分、线性和置换的相关定义.

定义 1[14]　设 $F:Z_2^n\to Z_2^n$,$\boldsymbol{X},\boldsymbol{\alpha},\boldsymbol{\beta}\in Z_2^n$,那么 $p_F(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{2^n}\#\{\boldsymbol{X}\mid\boldsymbol{\beta}=F(\boldsymbol{X})\oplus F(\boldsymbol{X}\oplus\boldsymbol{\alpha})\}$ 为 F 在输入差分为 $\boldsymbol{\alpha}$,输出差分为 $\boldsymbol{\beta}$ 下的差分转移概率. 其中,$\#\{\cdot\}$ 代表集合 $\cdot$ 中元素的个数.

定义 2[15]　设 $F:Z_2^n\to Z_2^n$,$\boldsymbol{X},\boldsymbol{\eta},\boldsymbol{\mu}\in Z_2^n$,称

$$\begin{aligned}\rho_F(\boldsymbol{\eta}\to\boldsymbol{\mu}) &= W_{(F)}(\boldsymbol{\eta}\to\boldsymbol{\mu})\\ &=\frac{1}{2^n}\sum_{\boldsymbol{X}\in Z_2^n}(-1)^{\boldsymbol{\eta}\cdot\boldsymbol{X}\oplus\boldsymbol{\mu}\cdot F(\boldsymbol{X})}\end{aligned}\tag{1}$$

为 F 在$(\boldsymbol{\eta},\boldsymbol{\mu})$点的 Walsh 谱. 称 $\boldsymbol{\eta}$ 为输入掩码,$\boldsymbol{\mu}$ 为输出掩码,并称 $\boldsymbol{\eta}\to\boldsymbol{\mu}$ 为 F 的一个线性逼近,ρ_F 为该线性逼近的相关系数.

定义 3[15]　设 $F:Z_2^n\to Z_2^n$,若对任意 $\boldsymbol{X},\boldsymbol{X}^*\in Z_2^n$ 且 $\boldsymbol{X}\neq\boldsymbol{X}^*$,有 $F(\boldsymbol{X})\neq F(\boldsymbol{X}^*)$,称 F 是一个置换.

3.2　基于 CA 的 S 盒

本小节将介绍基于 CA 的 S 盒. 如图 1 所示,通常用来设计 S 盒的 CA 是一维布尔型循环边界 CA,下面给出具体的定义:

定义 4[16]　将映射 $F^n:Z_2^n\to Z_2^n$ 称为一维布尔型循环边界 CA,其中 $n\in\mathbb{N}^*$ 为元胞规模,设 F^n 的局部规则为 $f:Z_2^{r+1}\to Z_2$,那么对 CA 的任意构型 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})$,其下一时刻的构型设为 $\boldsymbol{X}^*$,有:

$$\begin{aligned}\boldsymbol{X}^* &= F^n(\boldsymbol{X})=(f(x_0,\cdots,x_r),f(x_1,\cdots,x_{r+1}),\\ &\quad\cdots,f(x_{n-r},\cdots,x_0),\cdots,f(x_{n-1},\cdots,x_{r-1}))\end{aligned}$$

其中 r 为 CA 的邻域半径且 $r\in\mathbb{N}^*$,映射 F^n 即为 CA 的全局规则.

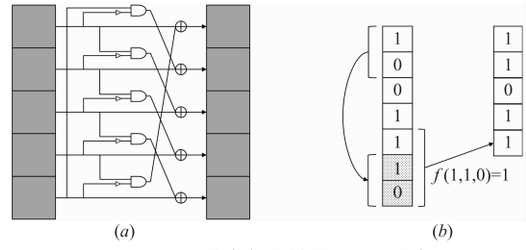


图1　一维布尔型循环边界CA示例

由于全局规则 F^n 可以反映元胞规模的大小,且包含了局部规则、邻域规则等 CA 的信息,所以可以用 CA 的全局规则来表示 CA. 注意在之后的文章中,若不加说明,那么 F^n、CA、基于 CA 的 S 盒均指定义 4 中的一维布尔型循环边界 CA.

4　基于 CA 的 S 盒的性质分析

由基于 CA 的 S 盒的定义不难发现这类 S 盒继承了 CA 的结构,因此可以猜测 CA 的某些性质可以类推至基于 CA 的 S 盒. 所以在本节将通过研究 CA 的性质得到一些基于 CA 的 S 盒的密码学性质.

4.1　循环左移的性质

首先给出循环左移的定义.

定义 5　设 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})\in Z_2^n$,记 $\sigma_k(\boldsymbol{X})$ 为对 $\boldsymbol{X}$ 循环左移 k 位$(k\in Z_n)$,有:

$$\sigma_k(\boldsymbol{X})=(x_k,x_{k+1},\cdots,x_{n-1},x_0,\cdots,x_{k-1})$$

下面给出循环左移变换 σ_k 的几个性质便于后续证明.

性质 1　$\forall\boldsymbol{X}\in Z_2^n,\forall k_1,k_2\in Z_n$,有

$$\sigma_{k_1}\cdot\sigma_{k_2}(\boldsymbol{X})=\sigma_{k_1+k_2}(\boldsymbol{X})$$

证明　根据循环左移的定义即有:

$$\begin{aligned}\sigma_{k_1}\cdot\sigma_{k_2}(\boldsymbol{X}) &= \sigma_{k_1}(x_{k_2},x_{k_2+1},\cdots,x_{n-1},x_0,\cdots,x_{k_2-1})\\ &=(x_{k_2+k_1},x_{k_2+k_1+1},\cdots,x_{n-1},x_0,\cdots,x_{k_2+k_1-1})\\ &=\sigma_{k_1+k_2}(\boldsymbol{X})\end{aligned}$$

证毕

性质 2 $\forall \boldsymbol{X},\boldsymbol{X}' \in Z_2^n, \forall k \in Z_n$,有

$$\sigma_k(\boldsymbol{X} \oplus \boldsymbol{X}') = \sigma_k(\boldsymbol{X}) \oplus \sigma_k(\boldsymbol{X}')$$

性质 3 设 $F: Z_2^n \to Z_2^n, \forall k \in Z_n$,则

$$\sum_{X \in Z_2^n} F(\boldsymbol{X}) = \sum_{X \in Z_2^n} F(\sigma_k(\boldsymbol{X}))$$

性质 4 $\forall \boldsymbol{\eta},\boldsymbol{X} \in Z_2^n$,都有

$$\sigma_k(\boldsymbol{\eta}) \cdot \sigma_k(\boldsymbol{X}) = \sigma_k(\boldsymbol{\eta} \cdot \boldsymbol{X}) = \boldsymbol{\eta} \cdot \boldsymbol{X}$$

其中 · 为点积运算.

性质 2、性质 3、性质 4 也可以很容易地根据循环左移的定义证明.

4.2 移位不变性

本小节将给出 CA 的移位不变性:将 CA 的任意输入循环左移 k 位后,相对应地,其输出也将循环左移 k 位. 移位不变性中蕴含了一维 CA 的结构特性,也反映了 CA 的边界条件.

定理 1[10] 设 $F^n: Z_2^n \to Z_2^n$ 为一个 CA,其局部规则为 $f: Z_2^{r+1} \to Z_2$,其中 $n \in \mathbb{N}^*$,$r>0$ 且 $n>r$,那么 $\forall X \in Z_2^n$, $\forall k \in Z_n$ 均有

$$F(\sigma_k(\boldsymbol{X})) = \sigma_k(F(\boldsymbol{X}))$$

定理 1 由循环左移及基于 CA 的 S 盒的定义易证. 通过 CA 的移位不变性可进一步证得 CA 的差分移位不变性和线性移位不变性,具体见推论 1 和推论 2.

推论 1 设 $F^n: Z_2^n \to Z_2^n$ 为一个 CA,对任意输入差分和输出差分 $\boldsymbol{\alpha},\boldsymbol{\beta} \in Z_2^n$,有:

$$p_{F^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = p_{F^n}(\sigma_k(\boldsymbol{\alpha}) \to \sigma_k(\boldsymbol{\beta})), \forall k \in Z_n$$

证明 对 $\forall k \in Z_n$,由定理 1 及差分转移概率的定义和循环左移 σ_k 的性质即有:

$$\begin{aligned} & p_{F^n}(\sigma_k(\boldsymbol{\alpha}) \to \sigma_k(\boldsymbol{\beta})) \\ &= \frac{1}{2^n}\#\{\boldsymbol{X} \mid \sigma_k(\boldsymbol{\beta}) = F(\boldsymbol{X}) \oplus F(\boldsymbol{X} \oplus \sigma_k(\boldsymbol{\alpha}))\} \\ &= \frac{1}{2^n}\#\{\boldsymbol{X} \mid \boldsymbol{\beta} = (F(\sigma_{-k}(\boldsymbol{X})) \oplus F(\sigma_{-k}(\boldsymbol{X}) \oplus \boldsymbol{\alpha}))\} \end{aligned}$$

又有:

$$p_{F^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = \frac{1}{2^n}\#\{\boldsymbol{X} \mid \boldsymbol{\beta} = F(\boldsymbol{X}) \oplus F(\boldsymbol{X} \oplus \boldsymbol{\alpha})\}$$

记集合 $\{\boldsymbol{X} \mid \boldsymbol{\beta} = F(\boldsymbol{X}) \oplus F(\boldsymbol{X} \oplus \boldsymbol{\alpha})\}$ 为 A,记集合 $\{\boldsymbol{X} \mid \boldsymbol{\beta} = (F(\sigma_{-k}(\boldsymbol{X})) \oplus F(\sigma_{-k}(\boldsymbol{X}) \oplus \boldsymbol{\alpha}))\}$ 为 B,构造映射 $\varphi: \boldsymbol{X} \to \sigma_k(\boldsymbol{X})$,下面证明 φ 是 A 到 B 的双射:

首先,对任意 $\boldsymbol{X} \in A$,$\boldsymbol{X}$ 满足 $\boldsymbol{\beta} = F(\boldsymbol{X}) \oplus F(\boldsymbol{X} \oplus \boldsymbol{\alpha})$,则 $\varphi(\boldsymbol{X}) = \sigma_k(\boldsymbol{X})$ 满足:

$$\begin{aligned} \boldsymbol{\beta} &= F(\sigma_{-k} \cdot \sigma_k(\boldsymbol{X})) \oplus F(\sigma_{-k} \cdot \sigma_k(\boldsymbol{X}) \oplus \boldsymbol{\alpha}) \\ &= F(\sigma_{-k}(\varphi(\boldsymbol{X}))) \oplus F(\sigma_{-k}(\varphi(\boldsymbol{X})) \oplus \boldsymbol{\alpha}) \end{aligned}$$

所以 $\varphi(\boldsymbol{X}) \in B$,故 φ 是集合 A 到 B 的一个映射;

任取 $\boldsymbol{X},\boldsymbol{X}' \in A$ 且 $\boldsymbol{X} \neq \boldsymbol{X}'$,必有 $\varphi(\boldsymbol{X}) \neq \varphi(\boldsymbol{X}')$. 否则若 $\varphi(\boldsymbol{X}) = \varphi(\boldsymbol{X}')$,那么 $\sigma_{-k}(\varphi(\boldsymbol{X})) = \sigma_{-k}(\varphi(\boldsymbol{X}'))$,即 $\boldsymbol{X} = \boldsymbol{X}'$,与假设矛盾,所以 φ 是单射;同样不难证 φ 是满射,所以 φ 是 A 到 B 的双射. 因此集合 A 和 B 包含的元素个数相等,即:

$$\begin{aligned} & \#\{\boldsymbol{X} \mid \boldsymbol{\beta} = F(\boldsymbol{X}) \oplus F(\boldsymbol{X} \oplus \boldsymbol{\alpha})\} = \\ & \#\{\boldsymbol{X} \mid \boldsymbol{\beta} = (F(\sigma_{-k}(\boldsymbol{X})) \oplus F(\sigma_{-k}(\boldsymbol{X}) \oplus \boldsymbol{\alpha}))\} \end{aligned}$$

所以 $p_{F^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = p_{F^n}(\sigma_k(\boldsymbol{\alpha}) \to \sigma_k(\boldsymbol{\beta}))$.

证毕

推论 2 设 $F^n: Z_2^n \to Z_2^n$ 为一个 CA,对任意输入掩码和输出掩码 $\boldsymbol{\eta},\boldsymbol{\mu} \in Z_2^n$,有

$$\rho_{F^n}(\boldsymbol{\eta} \to \boldsymbol{\mu}) = \rho_{F^n}(\sigma_k(\boldsymbol{\eta}) \to \sigma_k(\boldsymbol{\mu})), \forall k \in Z_n$$

证明 对 $\forall k \in Z_n$,由定理 1 及 Walsh 谱的定义和循环左移 σ_k 的性质即有:

$$\begin{aligned} & \rho_{F^n}(\sigma_k(\boldsymbol{\eta}) \to \sigma_k(\boldsymbol{\mu})) \\ &= \frac{1}{2^n}\sum_{X \in Z_2^n} (-1)^{\sigma_k(\boldsymbol{\eta}) \cdot \boldsymbol{X} \oplus \sigma_k(\boldsymbol{\mu}) \cdot F(\boldsymbol{X})} \\ &= \frac{1}{2^n}\sum_{X \in Z_2^n} (-1)^{\sigma_k(\boldsymbol{\eta}) \cdot \sigma_k(\boldsymbol{X}) \oplus \sigma_k(\boldsymbol{\mu}) \cdot F(\sigma_k(\boldsymbol{X}))} \\ &= \frac{1}{2^n}\sum_{X \in Z_2^n} (-1)^{\sigma_k(\boldsymbol{\eta}) \cdot \sigma_k(\boldsymbol{X}) \oplus \sigma_k(\boldsymbol{\mu}) \cdot \sigma_k(F(\boldsymbol{X}))} \\ &= \frac{1}{2^n}\sum_{X \in Z_2^n} (-1)^{\boldsymbol{\eta} \cdot \boldsymbol{X} \oplus \boldsymbol{\mu} \cdot F(\boldsymbol{X})} \\ &= \rho_{F^n}(\boldsymbol{\eta} \to \boldsymbol{\mu}) \end{aligned}$$

证毕

推论 2 证明中等式的第一步运用了性质 3,将等式一边连加号内的 $\boldsymbol{X}$ 循环移位 k 位不改变等式的值;第二步利用定理 1,即 CA 的移位不变性;第三步运用的是性质 4.

4.3 镜面对称性和互补性

首先定义 CA 中的运算方向. 对于任一 $F^n: Z_2^n \to Z_2^n$ 及其局部规则 $f: Z_2^{r+1} \to Z_2$,设 $\boldsymbol{X} = (x_0, x_1, \cdots, x_{n-1}) \in Z_2^n$,称该 CA 的运算方向是正向的当:

$$\begin{aligned} F^n(\boldsymbol{X}) = (& f(x_0, x_1, \cdots, x_r), f(x_1, x_2, \cdots, x_{r+1}), \\ & \cdots, f(x_{n-1}, x_0, \cdots, x_{r-1})) \end{aligned}$$

而该 CA 的运算方向是逆向时则有:

$$\begin{aligned} F^n(\boldsymbol{X}) = (& f(x_{n-r-1}, x_{n-r}, \cdots, x_{n-1}), \\ & f(x_{n-r-2}, x_{n-r-1}, \cdots, x_{n-2}), \cdots, \\ & f(x_{n-r}, x_{n-r+1}, \cdots, x_0)) \end{aligned}$$

注意不加说明时 CA 的运算方向均是正向的. 下面给出镜面对称的定义:

定义 6 对任意 $\boldsymbol{X} = (x_0, x_1, \cdots, x_{n-1}) \in Z_2^n$, $f: Z_2^n \to Z_2$,称 $\boldsymbol{X}' = (x_{n-1}, x_{n-2}, \cdots, x_1, x_0) \in Z_2^n$ 为 $\boldsymbol{X}$ 的镜面对称. 若存在 $f': Z_2^n \to Z_2$ 满足 $f'(\boldsymbol{X}') = f(\boldsymbol{X})$,称 f 与 f' 满足镜面对称关系.

CA 的镜面对称性指的是若两个 S 盒的局部规则满足镜面对称关系,那么对于两个互为镜面对称的输入,如果这两个局部规则的运算方向分别是正向的和逆向

的,那么这两个 S 盒的输出也是互为镜面对称的.

定理 2　设 $F^n:Z_2^n\to Z_2^n$ 为一个 CA,其局部规则为 $f(x_0,x_1,\cdots,x_r):Z_2^{r+1}\to Z_2$,那么将局部规则为 $f_0(x_0,x_1,\cdots,x_r)=f(x_r,x_{r-1},\cdots,x_0)$(即 f_0 和 f 满足镜面对称关系)的 CA 记为 $F_0^n:Z_2^n\to Z_2^n$,从而有

$$F^n(x_0,x_1,\cdots,x_{n-1})=\sigma_{r+1}(F_0^n(x_{n-1},x_{n-2},\cdots,x_0))$$

证明　由基于 CA 的 S 盒的定义即有:

$$\begin{aligned}&F^n(x_0,x_1,\cdots,x_{n-1})\\&=(f(x_0,x_1,\cdots,x_r),\cdots,f(x_{n-1},x_0,\cdots,x_{r-1}))\\&=(f_0(x_r,x_{r-1},\cdots,x_0),\cdots,f_0(x_{r-1},x_{r-2},\cdots,x_{n-1}))\\&=F_0^n(x_r,x_{r-1},\cdots,x_0,x_{n-1},\cdots,x_{r+1})\\&=\sigma_{r+1}(F_0^n(x_{n-1},x_{n-2},\cdots,x_0))\end{aligned}$$

证毕

如图 2 所示,对于局部规则为 $f(x_0,x_1,x_2)$ 的 F^5,(x_0,x_1,x_2,x_3,x_4) 和 (y_0,y_1,y_2,y_3,y_4) 为其输入和输出.那么对局部规则为 $f_0(x_0,x_1,x_2)=f(x_2,x_1,x_0)$ 的 F_0^5,当其输入 (x_4,x_3,x_2,x_1,x_0) 为 F^5 输入的镜面对称且 F^5 和 F_0^5 的运算方向分别是正向和逆向的,那么 F^5 和 F_0^5 的输出将镜面对称.

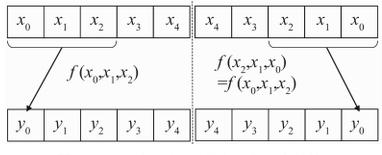


图2　镜面对称的两个局部规则

定理 3 给出的是 CA 的互补性.首先给出变量和向量补的定义.设 $x\in Z_2$,$\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})\in Z_2^n$,称 $\bar{x}=x\oplus 1$ 和 $\overline{\boldsymbol{X}}=(\bar{x}_0,\bar{x}_1,\cdots,\bar{x}_{n-1})$ 为 x 和 $\boldsymbol{X}$ 的补.而 CA 的互补性是指:任意 CA 都对应一个互补的 CA,在任意相同输入下,这两个 CA 的输出必是互补的.

定理 3　设 $F^n:Z_2^n\to Z_2^n$ 为一个 CA,其局部规则为 $f(x_0,x_1,\cdots,x_r):Z_2^{r+1}\to Z_2$,那么 F^n 必存在补 CA,记为 $\overline{F^n}:Z_2^n\to Z_2^n$.对于任意 $(x_0,x_1,\cdots,x_{n-1})\in Z_2^n$,$F^n$ 和 $\overline{F^n}$ 都满足 $F^n(x_0,x_1,\cdots,x_{n-1})=\overline{\overline{F^n}(x_0,x_1,\cdots,x_{n-1})}$.

证明　任意 F^n 都对应了一个局部规则 $\bar{f}(x_0,x_1,\cdots,x_r)$,$\bar{f}$ 在任意 $(x_0,x_1,\cdots,x_r)\in Z_2^{r+1}$ 下都有:

$$\begin{aligned}\bar{f}(x_0,x_1,\cdots,x_r)&=f(x_0,x_1,\cdots,x_r)\oplus 1\\&=\overline{f(x_0,x_1,\cdots,x_r)}\end{aligned}$$

记局部规则 $\bar{f}$ 对应的 n 维 CA 为 $\overline{F^n}:Z_2^n\to Z_2^n$.由向量取补及基于 CA 的 S 盒的定义即有:

$$\begin{aligned}&\overline{\overline{F^n}(x_0,x_1,\cdots,x_{n-1})}\\&=\overline{(\bar{f}(x_0,x_1,\cdots,x_r),\cdots,\bar{f}(x_{n-1},x_0,\cdots,x_{r-1}))}\\&=\overline{(\overline{f(x_0,x_1,\cdots,x_r)},\cdots,\overline{f(x_{n-1},x_0,\cdots,x_{r-1})})}\\&=(f(x_0,x_1,\cdots,x_r),\cdots,f(x_{n-1},x_0,\cdots,x_{r-1}))\\&=F^n(x_0,x_1,\cdots,x_{n-1})\end{aligned}$$

由定义知 $\overline{F^n}$ 就是 F^n 的补 CA,故任意 CA 都存在补 CA.

证毕

注意 $F^n(x_0,x_1,\cdots,x_{n-1})=\overline{\overline{F^n}(x_0,x_1,\cdots,x_{n-1})}$ 在任意 $(x_0,x_1,\cdots,x_{n-1})\in Z_2^n$ 下都满足即说明在相同输入下,F^n 和 $\overline{F^n}$ 的输出互补.

5　基于 CA 的 S 盒的神经网络实现

接下来将继续围绕基于 CA 的 S 盒的结构特点,探索其在神经网络实现上的优势.

5.1　基本概念

若要对一个 n 进 n 出的 S 盒进行神经网络实现,首先要根据 S 盒的输入和每一位输出确定 n 个布尔函数以表示该 S 盒,然后用 n 个单隐层多层感知器(Multiple Layer Perceptron,MLP)表示每一个布尔函数.由基于 CA 的 S 盒的定义知表示这类 S 盒的 n 个布尔函数是一样的,均为局部规则,因此可以将一个单隐层 MLP 复用 n 次,从而减少资源消耗.图 3(a)所示的是实现 Keccak 的 S 盒的神经网络结构,其中 x_0,x_1,x_2,x_3,x_4 和 y_0,y_1,y_2,y_3,y_4 分别表示 S 盒的输入与输出比特.而 P 是表示 Keccak 局部规则的单隐层 MLP,其结构见图 3(b).在该神经网络结构中,每 3 个相邻输入比特进入 P 可以得到 1 个相应的输出位,依次将 5 种 3 个相邻比特输入组合经过 P 的运算就得到了 S 盒的输出,从而实现 S 盒的功能.

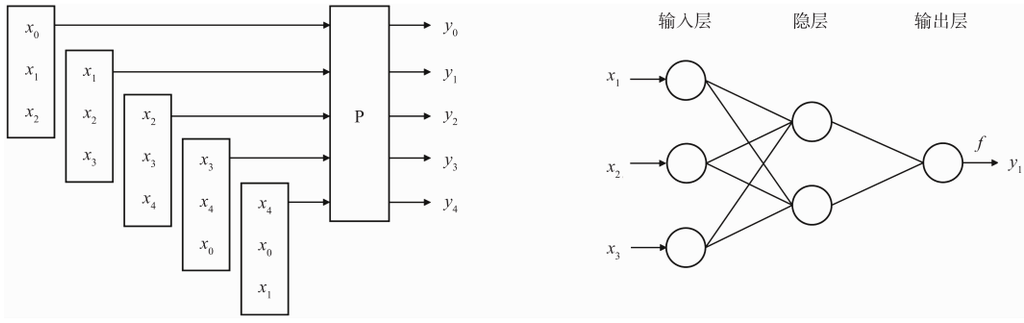
分析图 3(a)的结构可以发现尽管局部规则用神经网络的结构表示,但第 4 节的性质仍然满足.由于 P 完全模拟了局部规则,对任意输入都有与局部规则相同的输出,而第 4 节分析的性质并不对局部规则的内部结构或实现方式有要求,因此基于 CA 的 S 盒的相关性质将保留.

由图 3(b),实现 n 元布尔函数的单隐层 MLP 的输入层和输出层分别有 n 个和 1 个神经元.设 MLP 中隐层神经元数量为 m 个,其输入和输出为 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})$ 和 y,其中 $x_i,y\in Z_2$,$0\leqslant i\leqslant n-1$.隐层中的任一神经元有两个参数,即权重 $\boldsymbol{W}_i=(w_{i,0},w_{i,1},\cdots,w_{i,n-1})^{\mathrm{T}}$ 和阈值 $\boldsymbol{\theta}_i$;输出层神经元的权重和阈值记为 $\overline{\boldsymbol{W}}=(\overline{w_0},\overline{w_1},\cdots,\overline{w_{m-1}})^{\mathrm{T}}$ 和 $\bar{\boldsymbol{\theta}}$.单隐层 MLP 的表达式如下:

$$\begin{cases}y_i=g(\boldsymbol{W}_i\cdot\boldsymbol{X}-\boldsymbol{\theta}_i), & i=0,1,2,\cdots,m-1\\ y=g(\overline{\boldsymbol{W}}\cdot\boldsymbol{Y}-\bar{\boldsymbol{\theta}}), & \boldsymbol{Y}=(y_0,y_1,\cdots,y_{m-1})\end{cases}$$

其中,g 代表可选的激活函数,这里选用的是跃阶函数,因为其更符合 S 盒的输入输出情况且实现简单消耗小,跃阶函数 g 的定义如下:

$$g(x)=\operatorname{sign}(x)=\begin{cases}1, & x>0\\ 0, & x\leqslant 0\end{cases}$$



(*a*)基于CA的S盒的神经网络结构 (*b*)单隐层MLP

图3 Keccak的S盒的神经网络结构

为了使实现 S 盒的神经网络简单且易表示,要选用隐层数量少且参数简单的单隐层 MLP 来表示局部规则,所以本文中权重和阈值的分量均取整数. 表 1 列出的是几个实现 Keccak 局部规则的神经网络参数. 其中 U 表示权重和阈值分量的上界,L 表示权重和阈值分量的下界.

表 1 实现 Keccak 局部规则的神经网络参数表

m	U	L	$\boldsymbol{W}_0$	$\boldsymbol{W}_1$	$\boldsymbol{W}_2$	$\boldsymbol{\theta}$	$\overline{\boldsymbol{W}}$	$\overline{\boldsymbol{\theta}}$
2	2	−2	(−1,−1,1)	(2,−1,1)	/	(0,−2)	(2,−1)	−1
2	2	−1	(0,1,−1)	(2,0,0)	/	(−1,0)	(−1,−1)	−1
2	1	−2	(−2,1,0)	(0,−2,1)	/	(−1,0)	(1,1)	1
3	1	−1	(1,0,0)	(0,−1,1)	(0,0,1)	(0,0,−1)	(−1,1,0)	0

5.2 权重阈值搜索算法

下面介绍将局部规则用单隐层 MLP 表示的权重阈值搜索算法. 注意利用合适的学习算法,单隐层 MLP 可以实现任意的局部规则[17].

算法 1 实现 3 元或 4 元布尔函数神经网络的权重阈值搜索算法

输入:3 元或 4 元布尔函数

输出:实现该布尔函数神经网络结构的参数

Step1:初始化各项数据,count←0,flag←0,m←1,U←8,L←$-U$ 并给权重与阈值一个随机的不超过上下界的初始值,此时得到一个初始的单隐层 MLP 模型;

Step2:将布尔函数的所有输入依次进行当前的单隐层 MLP 模型并判断其输出是否全部与布尔函数的输出一样. 若全部相同,flag←1 并记录此时的权重和阈值,转到 Step5;若存在一个不相同,count←count + 1 并转到 Step3;

Step3:若 count$\leqslant 2^{14+4m}$,在上下界的范围内随机化所有权重阈值并转到 Step2;否则,若 $U=8$,转到 Step4,若 $U\neq 8$,flag←0 并转到 Step5;

Step4:若 $m\leqslant 3$,m←$m+1$,count←0 并转到 Step3;若 $m=4$,搜索失败,算法结束;

Step5:若 flag = 0 且 $U\neq 7$,U←$U+1$,L←$-U$ 并到 Step2;若 flag = 1 且 $U=8$,U←1,L←$-U$ 并到 Step2;若 flag = 1 且 $U\neq 8$ 或 flag = 0 且 $U=7$,输出权重阈值,算法结束.

$n(n\geqslant 5)$元布尔函数则需要先分解成 2^{n-4} 个 4 元布尔函数及 $2^{n-4}-1$ 个 172 号感知器(172P)[7],然后实现每一个 4 元布尔函数并进行组合(组合方式见图 4[7]).

下面解释为何本文及文献[7]中的 DNA-like 算法[18]不考虑直接搜索 5 元以上的布尔函数. 虽然理论上可以找到相应的单隐层 MLP,但是通过大量的实验发现在 5 元以上时,搜索成功率及效率将大大降低(DNA-like 算法在 5 元以上的成功率相对较高,但依旧不可靠,故文献[7]也放弃对 5 元以上布尔函数的搜索),从而需要将参数简单化的搜索策略改变为成功率及效率优先的搜索策略而偏离了目的. 因此,要使搜索的可靠性提高,必须放弃单隐层 MLP 而选用表达能力更强的结构,而用图 4 的方式可以将 5 元以上布尔函数用 4 元布尔函数和 172P 组合的结构来表示,从而本文的算法依旧可以发挥作用.

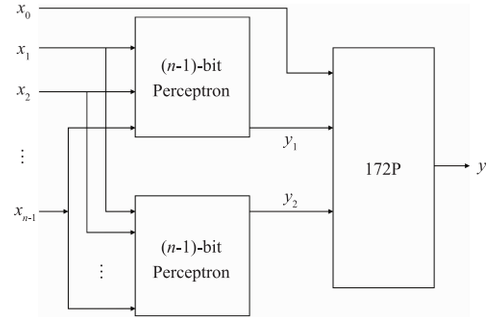


图4 实现n元布尔函数的网络

5.3 结果分析

在个人 PC 上(Intel i5-7200U,4 核,2.50GHz)上执行本文的权重阈值搜索算法,且对全部 256 个 3 元布尔函数及随机 1024 个 4 元布尔函数进行神经网络实现,以分析该算法的成功率及使用该方法得到的单隐层 MLP 的隐层神经元数量分布情况,具体数据见表 2. 注意 3 元布尔函数的搜索结果可以实时得到,而 4 元布尔函数的权重阈值也都可以在数分钟内得到结果. 也就是说该算法对 3 元或 4 元布尔函数的搜索,时间不成为限制因素,可认为该算法是快速的.

由表 2 知实现 4 元布尔函数的单隐层 MLP 时尽管有失败概率,但仅为 0.20%. 另外可知 4 元布尔函数神经网络的隐层神经元数量为 1、2、3、4 的分布分别为 3.32%、27.83%、49.22%、19.43%.

文献[7]通过 DNA-like 算法训练得到权重和阈值,使用该方法的特点是隐层的权重向量都相等,即 $\boldsymbol{W}_0 = \boldsymbol{W}_1 = \boldsymbol{W}_2 = \cdots = \boldsymbol{W}_{m-1}$. 同样 DNA-like 算法可以得到实现 4 元布尔函数的神经网络的参数,而对 $n(n \geqslant 5)$ 元布尔函数也要按图 4 的方法组合实现.

表 2　隐层神经元数量分布表

n	$m=1$	$m=2$	$m=3$	$m=4$	失败	总数
3	104	150	2	0	0	256
4	34	285	504	199	2	1024

表 3 是使用 DNA-like 算法和本文的权重阈值搜索算法实现的部分 4 元布尔函数的神经网络参数对比. 可以看到使用本文方法得到的单隐层 MLP 有更少的隐层神经元,且相对 DNA-like 算法其权重和阈值的 U 更小而 L 更大.

表 3　DNA-like 算法与本文方法得到的神经网络参数比较

4 元布尔函数 $f(x)$	DNA-like 算法			本文方法		
	m	U	L	m	U	L
1,0,0,0,0,0,0,0,1,1,1,0,1,1,1,0	1	12	−8	1	3	−2
1,1,1,0,1,0,0,1,1,1,1,1,1,1,0,1	2	26	−18	2	2	−2
0,0,0,0,1,0,0,1,0,0,0,0,1,1,1,0	3	22	−4	3	1	−1
1,1,1,0,0,0,1,1,0,1,1,1,0,1,0,0	4	12	−10	3	1	−1
1,0,1,1,0,0,0,1,1,0,1,1,1,1,1,0	5	12	−22	3	1	−1

6 结语

本文研究了基于 CA 的 S 盒的性质,给出了移位不变性、镜面对称性及互补性,且通过移位不变性进一步推出差分和线性的移位不变性,为研究这类 S 盒的密码学性质提供了一些有用的结论. 另外也探索了基于 CA 的 S 盒的在神经网络实现上的优势,即实现其的神经网络结构比其他 S 盒的更简单. 本文给出的一种权重阈值搜索算法可以快速给出实现基于 CA 的 S 盒的神经网络结构和参数. 虽然基于 CA 的 S 盒已经被用于许多密码算法中,但大部分都是 Keccak 类 S 盒或其仿射变换. 下一步的工作是找到更多性质优良的基于 CA 的 S 盒以应用在码算法的设计中.

参考文献

[1] SHANNON C E. Communication theory of secrecy systems [J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[2] BURKS A W. Essays on Cellular Automata[M]. Urbana: University of Illinois Press, 1970. 1-2.

[3] MARIOT L, PICEK S, LEPORATI A, et al. Cellular automata based S-boxes[J]. Cryptography and Communications, 2019, 11(1): 41-62.

[4] NIST. Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family [EB/OL]. https://csrc.nist.gov/news/2007/request-for-candidate-algorithm-nominations, 2007-11-02.

[5] BERTONI G, DAEMEN J, PEETERS M, et al. The KECCAK Reference[R/OL]. https://keccak.team/files/Keccak-reference-3.0.pdf, 2011-01-14.

[6] SIMON H. Neural Networks: A Comprehensive Foundation [M]. India: Pearson Education Pte Ltd, 2002. 23-35.

[7] 张霞. S 盒的神经网络实现及其动力学性质[D]. 杭州: 杭州电子科技大学应用数学系, 2015. 7-24.

[8] MUKHOPADHYAY D, ROYCHOWDHURY D. Cellular automata: an ideal candidate for a block cipher[A]. Ghosh R K. International Conference on Distributed Computing and Internet Technology [C]. Bhubaneswar: Springer, 2004. 452-457.

[9] JOSHI P, MUKHOPADHYAY D, ROYCHOWDHURY D. Design and analysis of a robust and efficient block cipher using cellular automata [A]. Watanabe K. International Conference on Advanced Information Networking and Applications[C]. Vienna: IEEE Computer Society, 2006. 67-71.

[10] BHATTACHARYA D, BANSAL N, BANERJEE A, et al. A new optimal S-box design[A]. Gupta S K. International Conference on Information Systems Security[C]. Delhi: Springer, 2007. 77-90.

[11] STJEPAN P, MARIOT L, YANG B, et al. Design of S-boxes defined with cellular automata rules [A]. Valero M. International Conference on Computing Frontiers[C]. Siena: ACM, 2017. 409-414.

[12] 关杰, 黄俊君. 一类新的基于元胞自动机的 S 盒的密码学性质分析[J]. 通信学报, 2019, 40(5): 192-200.
GUAN J, HUANG J J. Research on cryptographic properties of a new S-box based on cellular automaton[J]. Jour-

nal on Communications,2019,40(5):192 – 200. (in Chinese)
[13] BIHAM E. A fast new DES implementation in software [A]. Biham E. 4th International Workshop on Fast Software Encryption[C]. Haifa:Springer,1997. 260 – 271.
[14] 金晨辉,郑浩然,张少武,等. 密码学[M]. 北京:高等教育出版社,2009. 174 – 201.
[15] PIEPRZYK J,FINKELSTEIN G. Towards effective nonlinear cryptosystem design[J]. IEEE Proceedings E-Computers and Digital Techniques,2005,135(6):325 – 335.
[16] 江志松. 元胞自动机的语法复杂性[D]. 苏州:苏州大学数学系,2001. 2 – 4.
[17] CHEN F Y,CHEN G R,HE G,et al. Universal perceptron and DNA-like learning algorithm for binary neural networks:LSBF and PBF Implementations[J]. IEEE Trans on Neural Networks,2009,20(10):1645 – 1658.
[18] CHEN F Y,CHEN G R,HE Q,et al. Universal perceptron and DNA-like learning algorithm for binary neural networks:Non-LSBF implementations[J]. IEEE Trans on Neural Networks,2009,20(8):1293 – 1301.

作者简介

黄俊君 男,1995 年 1 月出生于浙江省绍兴市. 现为解放军战略支援部队信息工程大学研究生. 从事对称密码相关研究.
E-mail:hjj7752@outlook.com

关 杰 女,解放军战略支援部队信息工程大学教授、博士生导师. 1974 年 9 月生于河南郑州. 研究方向为对称密码的设计与分析.
E-mail:guanjie007@163.com