

# S 盒的密码学性质检测工具调研

## 一、为什么要做一个 S 盒检测工具

S 盒( Substitution Box )作为许多密码算法的核心模块,其安全强度至关重要。 $n \times m$ 的 S 盒本质上可以看作一个映射<sup>[1]</sup>:  $S(X) = (f(X), \dots, f(X)): \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ , 相当于  $m$ 个  $n$ 元布尔函数的线性组合。当  $n$ 和  $m$ 均很大时,几乎所有 S 盒都是非线性的,但这会带来存储和运算上的困难。我们希望在较小的存储量下获得好的 S 盒,同时具备必要的安全性,因此有必要通过一系列代数性质,全面准确地度量 S 盒的密码强度。

对 S 盒的深入研究不仅有助于迭代分组密码的设计,而且对于以非线性变换为核心的密码算法的分析有相当价值。同时,对密码学性质进行检测也可以直观地给出各项指标,有助于密码设计者快速找到满足某些特定密码需求的新的密码函数。这些指标主要来源于 S 盒的设计准则和构造方法,工具的检测中会对如下性质进行研究:非线性度、差分均匀度、鲁棒性、平衡性、雪崩效应、扩散准则、代数次数以及轮换对称性等性质。这些性质分别对应着抵抗不同攻击方法的强度。例如,非线性度决定着对应密码算法抵抗线性分析攻击的能力。而 S 盒的安全要求取决于整个原语的设计策略,每一种安全要求对应着抵抗不同的攻击,因此,设计者需要考虑对各个性质抵抗攻击的优势进行权衡,以达到总体设计的优越。S 盒的性质检测可以为设计者提供各个优势的参考,全面准确地度量 S 盒的密码学强度。

另一方面,基于工具的易用性考虑,需要更简单通用的方法检测 S 盒各个密码学性质。尽管已有平台例如 SageMath<sup>[2]</sup>,能够计算 S 盒的部分密码学性质,但评估并不全面,而且对于用户而言操作繁琐,使用困难。目前市面上仍然缺乏国产化、轻量级、评估全面的 S 盒分析检测工具。因此,设计一个简单通用的 S 盒密码学性质检测软件是十分必要的。

## 二、目前的工具分析

S 盒首次出现在 Lucifer 算法中,之后因 DES 的使用而广为流行<sup>[1]</sup>。S 盒是许多分组密码算法中的唯一非线性部件,因此,它的密码强度决定了整个分组密码算法的安全强度。但如何全面准确地度量 S 盒的密码学强度,用更简单通用的方

法检测 S 盒各个密码学性质，一直以来是密码设计与分析的研究难题。

国内外现有的对称密码算法设计仍沿用香农 1949 年提出的“混淆”、“扩散”思想<sup>[3]</sup>，是指通过对称密码算法中的“混淆”和“扩散”部件使得明文、密文和密钥之间的关系异常复杂，使得攻击者无法从密文得到明文的任何信息或者从明文密文对得到密钥的任何信息。而 S 盒主要提供了分组密码算法所必须的混淆作用。许多分组加密算法都是基于 S 盒的密码强度，例如美国高级加密标准 AES 算法、韩国对称加密标准 SEED 算法、欧洲对称加密标准 Camellia 算法和中国商用密码标准 SMS4 算法等。因此，对于上述密码算法中 S 盒分析的研究较多。例如，文献[5]就对上述四种密码算法进行了研究探讨，分别检测了代数性质和布尔函数性质，分析各种算法抵抗差分密码分析和线性密码分析等攻击的能力。

但是，现阶段国内外关于 S 盒密码学性质的研究往往只局限于某一具体的密码算法，缺乏普遍的统计分析。同时，现有的测试方法或工具通常只能完成部分密码学性质的计算，评估并不全面。

研究 S 盒密码学性质的平台 SageMath 是较为常见的一个开源数学工具。该工具包含了从线性代数、微积分，到密码学、群论、图论、数论等各种初高等数学的计算功能。而且 SageMath 内置了专门用于密码学计算的模块，其中 sage.crypto 模块可以用于评估 S 盒的许多重要密码学性质。例如，sage.crypto.Sbox 模块<sup>[5]</sup>可以对任意输入的 S 盒进行代数处理和性质评估，比如给出 S 盒的差分分布表(Differential Distribution Tables DDT)，非线性度等；而 sage.crypto.Sboxes 模块<sup>[6]</sup>提供了许多常用的密码算法中的 S 盒及其密码学性质。但是，SageMath 覆盖范围并不全面，暂时还不支持部分重要的密码学性质检测，例如对  $(v, w)$  线性度的检测。同时，在检测大量 S 盒的情况下，该工具的效率并不高，检测时间比较久。除了 SageMath 之外，Magma<sup>[7]</sup>是一款由悉尼大学数学与统计学系计算代数小组开发的功能强大的代数计算程序包，该软件专门解决代数系统中的数论、代数几何和代数组合学的计算问题，也包括密码学模块，对于研究 S 盒非常方便。

另一个 GitHub 的开源项目 libapn<sup>[8]</sup>主要用于研究布尔函数，包括但不限于 APN 函数。它可以用于计算 DDT、差分均匀度、代数次数以及寻找 APN 函数。但是，libapn 只考虑了有关抵抗差分攻击的安全属性，其他的性质并没有覆盖到。

另外，还有一些函数库也可以用于对 S 盒密码学性质的检测。例如，R 是一

个可以用于统计分析的数学编程语言。其中可加载的 `boolfun`<sup>[9]</sup>模块可以用来评估布尔函数的部分密码学属性，例如非线性度，免疫性等，同时也提供了处理布尔多项式的功能。VBF 库(Vector Boolean Fuction Library)是由 Alvarez-Cubero 和 Zufiria 提出的从密码学角度进行布尔函数分析的工具，可用于计算 S 盒的各个密码学性质<sup>[10]</sup>。

文献[11]中提出了一个名为 PEIGEN<sup>[11]</sup>的平台，可以用来评估 S 盒的安全强度，并给出高效的软硬件实现。该平台集成了大部分现有工具的功能特性，检测性质范围比较全面，也使用了效率更高的搜索算法，可以为 S 盒的研究与设计提供系统性的参考。不过该平台主要是对  $n$ -bit S 盒( $3 \leq n \leq 8$ )进行研究，对于更大的 S 盒 ( $n \geq 5$  位)，它仅用于评估安全性，但还不足以完成 S 盒的实现和生成。但是，该平台暂时没有可用的 UI 界面。

而更多的对 S 盒的密码学性质研究则分散在不同的方面，往往只局限于某一具体的密码体系或密码算法，或者只对抵抗某种具体攻击来进行分析。例如，文献[12]主要研究了应用在序列密码中的 S 盒，对欧洲 NESSIE 计划和 eSTREAM 计划进行了关注，特别是对 eSTREAM 计划中所涉及到的利用分组密码部件 S 盒构造流密码的情况进行了统计和分析。但是，现有研究中针对某一个密码学性质的专门研究非常丰富且范围广泛。

随着密码学技术的不断发展，未来会有更多层出不穷的攻击出现。每当新的攻击方式出现，针对抵抗这些攻击的安全属性进行研究与检测是非常有必要的。例如，2011 出现针对轻量级分组密码算法 PRINTcipher 提出的 invariant subspace 攻击<sup>[13]</sup>，引起了人们对于此方面的注意。而在此之前，此类性质并没有被注意到，也缺少相关的研究和检测分析。因此，随着密码学技术的发展，密码分析技术的更新，设计一个安全的密码算法需要考虑的方面会愈加复杂。而一个通用、用户友好且评估全面的 S 盒的密码学检测工具将会为密码学的研究与设计提供系统性的参考和助力。