研究报告

For *Two Generalizations of Almost Perfect Nonlinearity*

沈恩祈 PB23151787

论文摘要

本文提出了两种“几乎完美非线性”（APN）函数的数学推广——k-强非正态性和 k 阶和自由性，旨在克服传统 APN 函数在高阶密码分析中的局限。k-强非正态性要求函数在任意 k 维仿射子空间上非仿射，以保证高维非线性，填补了向量函数正态性研究的空白；k 阶和自由性则强制函数在 k 维仿射子空间的求和非零，有效抵御积分攻击中的零和区分器。研究表明，当 k=2 时，以上两种性质退化为传统 APN 条件，确保向下兼容；而当 k>2 时，提供更强的安全性约束，从结构非线性和行为非零和角度加强分析。通过对 AES 核心 S 盒（乘法逆函数）的分析，验证了这两种性质的实际效力。研究发现，AES S 盒在非向量仿射子空间上的求和非零，揭示了其抗积分攻击的机制；同时，S 盒在向量子空间的求和结果与基选择相关，提示高维风险。此外，沃尔什变换推导了性质的频谱特征公式，揭示了代数性质与密码安全性之间的量化关系。k-强非正态性具有单调性和仿射不变性，而 k 阶和自由性则不具单调性和 CCZ 不变性。

关键词

几乎完美非线性（APN）；k-强非正态性；k 阶和自由性；仿射子空间；积分攻击；沃尔什变换；乘法逆函数；高维密码学

研究目标

本文聚焦于密码学与离散数学的交叉研究领域，针对向量函数在抵御密码分析中的核心挑战，系统性地提出并深入探究“几乎完美非线性（APN）”概念的两种数学推广形式——k 强非正态性和 k 阶和自由性。这一研究以提升分组密码核心组件（如 S 盒）的安全性能为导向，旨在解决传统 APN 函数在应对新兴密码分析技术时的理论局限性，具体研究目标逐层展开如下：

（1）理论推广：构建 APN 函数的广义数学框架传统 APN 函数通过“二阶差

分均匀性”抵御差分攻击，但其理论边界难以直接扩展至更高阶攻击场景。本研究从 APN 函数的经典特征出发（如仿射平面上的非仿射性、求和非零性），将“仿射平面”推广至“k 维仿射子空间”，定义两种全新性质：k 强非正态性：要求向量函数在任意 k 维仿射子空间上的限制非仿射，即不存在 k 维仿射子空间使函数退化为仿射映射。这一性质是布尔函数“k 弱正态性”的向量扩展，填补了向量函数在高维子空间上的行为研究空白。k 阶和自由性：要求函数在任意 k 维仿射子空间上的求和结果非零，通过高阶导数的非零性（$(D_{a_1} \setminus dots D_{a_k} F(x) \neq 0)$）刻画，直接关联积分攻击中“仿射子空间求和可预测性”的核心漏洞。

通过上述定义，研究建立了从 k=2（对应传统 APN）到 k≥3 的广义理论框架，揭示了 APN 性质在更高维度的数学本质。

（2）密码学应用：面向高阶攻击的防御机制设计，随着积分攻击、高阶差分攻击等技术的发展，传统 APN 函数的安全局限性凸显。本研究聚焦新性质在密码系统设计中的实际价值：抗积分攻击：积分攻击依赖仿射子空间上的求和规律，k 阶和自由性通过强制求和非零，破坏攻击所需的“零和”条件，提升密码算法对积分区分器的鲁棒性。防御高阶差分攻击：k 强非正态性通过限制函数在高维子空间的线性行为，增加高阶差分攻击中“低代数度分量函数”的存在难度，尤其适用于抵抗基于代数次数的攻击（如猜测确定攻击）。S 盒设计准则扩展：为分组密码核心组件提供新的安全参数（如 k 值选择），允许设计者根据应用场景权衡安全性与实现效率（如轻量级密码可侧重低 k 值优化）

研究首次提出一系列待解决的关键问题，为后续研究指明方向：存在性刻画：完全确定(k,n,m)参数空间中两种性质的存在区域，尤其是 m<n 时的可行性。高效验证算法：设计针对高维子空间的性质验证算法，降低计算复杂度（如基于快速沃尔什变换的优化）。多变量扩展：将理论框架从二元域扩展至多元域，探索特征差异对性质的影响。通过上述研究目标的层层递进，本文构建了 APN 函数的广义理论体系，既深化了密码函数的数学基础，又为抗量子密码、轻量级密码等前沿领域提供了新的设计范式。

主要贡献

广义 APN 性质的定义：本研究首次在向量函数层面系统地定义了 APN 性质的两种广义形式，突破了传统 APN 仅针对二阶差分的局限性。提出了“k 强非正态性”和“k 阶和自由性”两个新概念，扩展了 APN 函数的适用范围，并为高维子空间中的函数行为研究提供了新的理论框架：

（1）k 强非正态性：在基于布尔函数“k 弱正态性”的基础上，提出了 k 强非正态性的定义，要求函数在任意 k 维仿射子空间上非仿射。通过该概念，填补了向量函数在高维子空间行为上的研究空白，并证明了当 $k\geq 2$ 时，所有 APN 函数均为 k 强非正态函数，为分析函数的高维非线性提供了新的理论工具。

（2）k 阶和自由性：创新性提出了“k 阶和自由性”的概念，定义了函数在 k 维仿射子空间上求和非零的强约束条件。通过该性质，直接关联了积分攻击中的“仿射子空间零和”漏洞，为抵抗基于求和规律的攻击提供了新的思路。研究进一步揭示了 k 阶和自由性通过避免仿射子空间零和，破坏了积分攻击的核心假设。

单调性与等价不变性：研究发现 k 强非正态性具有单调性，即若函数满足 k 强非正态性，则对于所有 $l\geq k$ 也成立。而 k 阶和自由性不具备单调性，存在函数在 $k=3$ 时满足条件，但在 $k=4$ 时不满足，揭示了两者在高维场景中的本质差异。此外，k 强非正态性和 k 阶自由性在仿射等价下保持一致，但在 CCZ 等价下不恒成立，为函数等价类的安全评估提供了新的依据。

频谱分析与沃尔什变换特征公式：通过频谱分析，推导了两种新性质的沃尔什变换特征公式。例如，k 强非正态性要求沃尔什变换在 k 维子空间的频谱满足特定非零条件，而 k 阶和自由性对应频谱在高阶导数下的正交性约束。这些公式为量化“函数代数性质—频谱特性—密码安全性”的关联提供了可计算的数学工具，并为多维度攻击场景下的 S 盒设计提供了新的评估标准。

AES S 盒分析：研究以 AES 核心 S 盒——乘法逆函数 $F(x)=x^{-1}$ 为研究对象，揭示了其在新理论框架下的独特性质。特别地，发现乘法逆函数在非向量仿射子空间上的求和结果恒非零，进而解释了其在 AES 中抵御积分攻击的表现。研究进一步揭示了乘法逆函数在特定高维子空间中的潜在风险，提出其求和特性与基的选择密切相关，并通过基展开公式，证明其求和结果可表示为高阶行列式。

开放性问题与研究方向：提出了若干具有挑战性的开放性问题，特别是如何完全刻画(k,n,m)参数下两种性质的存在区域，尤其是在 m<n 时的可行性（例如在布尔函数场景下）。此外，设计了针对高维子空间性质验证的高效算法，探索了基于快速沃尔什变换和多项式插值的优化方法。研究还探讨了将理论框架扩展至奇特征域 Fpn，并对已知 APN 函数族（如 Gold 函数、Kasami 函数）进行了高维性质验证。

跨学科研究范式：本研究通过“概念定义—性质分析—实例验证—问题拓展”的完整链条，实现了 APN 函数理论的高维拓展，填补了密码学中抗高阶攻击的理论空白。其核心贡献不仅在于提出两种新性质，还在于建立了连接数学理论、密码分析与算法设计的跨学科研究范式，为后量子密码时代的安全组件设计提供了关键支持。

阅读感悟

本科生阶段尝试阅读的第一篇纯英文论文，在整个过程中给我的感觉就是味同嚼蜡，在 AI 翻译的辅助下慢慢尝试去理解文章的意思，每一个生涩的词汇都需要去百度查找，过程可谓是困难重重。

所幸一切的努力都是有所回报的。一篇密码学领域的经典论文，探讨了“几乎完美非线性（APN）”函数的高维拓展。在这段一点点解密的日子里，我仿佛置身于一场数学与安全的精妙对话中，见证理论如何抵御现实攻击，又如何引领未来技术的发展方向。阅读完整篇文章后，对于密码学领域，我也初步有了自己的理解。

传统密码就像搭建在二维平面上的堡垒，APN 函数作为堡垒的基石，通过“二阶差分均匀性”抵御差分攻击——就像在平面上设置层层障碍，让攻击者难以找到规律。但随着黑客技术的升级，攻击手段从“平面游走”转向“立体渗透”。积分攻击如同从三维空间俯瞰堡垒，通过分析函数在高维空间上的求和规律，轻松找到堡垒的漏洞。这时候，二维的防御体系显得捉襟见肘，此刻人们不得不思考：如何在更高维度上构建更坚固的堡垒？

此时 APN 函数则应运而生，其核心是在二维仿射平面上保持非线性，就像一个优秀的舞者在舞台上始终保持独特的舞步，不让观众预测下一步动作。当舞

台从二维扩展到三维、四维甚至更高维时，传统 APN 函数的“舞步”则又变得单调，无法应对复杂的攻击节奏。例如，积分攻击利用高维空间的“零和区分器”，如同在舞者周围设置隐形的陷阱，而传统 APN 函数却无法感知这些陷阱的存在。因此 APN 函数急需一套适应高维舞台的“新舞步”-----高维密码的“双重武器”：k-强非正态性与 k 阶和自由性。

而 k-强非正态性的核心思想很简单，无论身处何种环境，都拒绝重复单调的模式。在三维空间中，它要求函数在任何三维仿射子空间上都保持非线性，让攻击者无法通过线性规律破解。这种“叛逆”的性质填补了向量函数在高维空间的研究空白，让密码函数在高维环境中依然保持神秘莫测。

k 阶和自由性则更具攻击性，它直接针对积分攻击的核心——“零和区分器”。在三维仿射子空间中，函数的求和结果始终是一个非零值，如同在陷阱中填入不可预测的变量，让攻击者的计算全盘失效。这种性质通过高阶导数的非零性实现，将积分攻击的基础彻底动摇。

神奇的是，当 k=2 时，这两种性质又完美退化为传统 APN 条件，就像一套兼容不同维度的万能工具，在二维时是坚固的盾牌，在高维时是锋利的长剑。这种“向下兼容，向上拓展”的特性，让理论框架既有传承又有创新，如同将经典建筑的基石与现代摩天大楼的设计理念完美融合，构建出适应未来的密码学体系。

未来展望

目前，验证 k 维性质的计算复杂度极高，如同用手工计算解决天文数字的难题。未来需要开发高效算法，让理论验证从“超级计算机专属”变为“普通开发者可用”。这就像发明计算器，让复杂计算不再是少数人的特权，加速高维密码的普及。

另外，量子计算机的崛起如同一场新的风暴，传统密码体系面临颠覆。高维密码的 k 阶和自由性可能成为抗量子攻击的关键武器，通过格理论与和自由性结合，设计出量子算法难以破解的函数，如同在风暴中建造坚固的量子堡垒。这是密码学应对未来挑战的重要方向，充满未知与机遇。

最后，推动高维安全性质纳入密码标准，开发开源工具链，如同制定建筑规范并提供施工工具，让开发者无需从头搭建安全体系，而是通过成熟的工具快速实现高维防御。这将大大降低应用门槛。