

基于 FPGA 的低开销 RO-PUF 研究

余方计^{1*} 范小娇¹

YU Fangji FAN Xiaojiao

摘要

随着智能信息化时代的到来,硬件克隆设计频发、资源开销过大的问题日益突出,亟需能兼顾安全性与硬件资源优化的有效解决方案。基于此,文章提出了一种基于六输入双输出查找表(LUT6_2)的可选式双轨道双输出 RO PUF(selectable dual-track dual-output RO PUF, SDT-DORO PUF)设计,以降低硬件资源的开销。通过在 Zynq-7000 系列 SoC FPGA 开发板上实现该设计,实验结果表明,SDT-DORO PUF 结构设计在 Zynq-7000 系列 SoC FPGA 开发板中唯一性和可靠性的性能指标分别为 49.44% 和 98.877%,均接近理想值,且成功通过了 NIST 随机性测试。该设计不仅有效降低了硬件资源消耗,同时还展示了作为芯片加密技术的潜力,为集成电路的安全性提供了新的解决方案。

关键词

资源消耗; PUF; FPGA; 硬件安全

doi: 10.3969/j.issn.1672-9528.2025.12.030

0 引言

近年来,随着人工智能与集成电路技术的持续进步,智能电子设备在日常生活中的应用愈发广泛,而防止硬件电路被克隆成为一大难题。利用芯片制造中的随机工艺差异,在硬件电路中嵌入物理不可克隆函数(PUF),从而解决防克隆问题。因此,对两个相同的智能电子设备施加相同的激励,会产生不同的响应位^[1]。PUF 具备低能耗、防复制及无需固定存储的特点,能为设备创造独一无二的数字标识,确保实现可靠且安全的认证^[2-3]。

现有的 PUF 研究主要分为两类:延迟型 PUF 和存储型 PUF。延迟型 PUF 利用信号传播时间差,如环形振荡器 PUF(RO PUF)、可配置 RO PUF(CRO PUF)、占空比 PUF(DC PUF)和仲裁器 PUF(Arbiter PUF)。存储型 PUF 则通过存储单元上电随机状态,如静态随机存储器 PUF(SRAM PUF)依据 SRAM 上电稳定状态生成唯一响应。相同资源下对于延迟型 PUF 来说 CRO PUF 生成的响应位要多。

Suh 等^[4]提出了 RO PUF 结构,通过比较振荡器频率差异生成响应,但易受温度和电压波动影响。而后, Maiti 等^[5]提出 CRO PUF,通过配置不同振荡器组合降低噪声,提高了生成的响应位和降低了硬件开销。Agustin 等^[6]的 DC PUF 通过测量信号占空比变化生成响应,较 RO PUF 更可靠。Lee 等^[7]的 Arbiter PUF 比较对称路径信号延迟确定输出,但是

FPGA 实现困难。Guajardo 等^[8]的 SRAM PUF 利用 SRAM 单元上电随机状态生成响应位,无需额外电路。针对 CRO PUF 资源消耗问题, Pei 等^[9]提出了利用 LUT 设计的 RO 单元,可在单个 CLB 内配置双输出振荡环用来输出频率,从而降低硬件开销和增加响应位的输出。然而,文献[9]中想要每增加一倍的响应位需要额外增加一倍的 CLB 资源。

针对文献[9]中因响应位的增加而导致 CLB 硬件资源开销不断扩大的问题,本文提出了基于六输入双输出查找表(LUT6_2)的可选式双轨道双输出 RO PUF(selectable dual-track dual-output RO PUF, SDT-DORO PUF)。该方案在 Zynq-7000 系列 SoC FPGA 开发板上,通过灵活配置 LUT6_2 单元,构建了 RO 环的使能、双轨切换及延迟模块,从而实现基于 LUT 的低开销 SDT-DORO PUF 设计方案。

1 低开销 SDT-DORO PUF 设计

本文利用 LUTs 单元设计的 SDT-DORO PUF 结构已在 Zynq-7000 系列 SoC FPGA 设备上得到了实现。该款 FPGA 中的基本逻辑单元可配置逻辑块(CLB)由切片 L 和切片 M 组成,是设计结构的主要使用资源。两个切片中都包含有用于实现逻辑函数的 4 个 6 输入查找表(单输出 LUT6 和双输出 LUT6_2)、实现路径选择的 3 个多路复用器(MUX)、支持级联算法操作的 1 个进位链和 8 个触发器^[10]。利用 CLB 资源可以实现众多的组合逻辑电路。

1.1 原理设计

如图 1(a)所示,是双输出 AND 门使能单元,其中使能单元的输出 Out5 和 Out6 作为图 1(b)的输入, Enable 端

1. 西京学院计算机学院 陕西西安 710123

[基金项目] 陕西省科技厅重点研发项目(2022GY-052)

口用来控制 RO 环起振。如图 1 (b) 所示, 是双输出可配置反相器单元, 该单元由 2 个选择器和 2 个反相器组成, 其中 A3 端口用于控制选择两个反相器不同的路径走向, A0 和 A1 端口连接前一级使能或相同单元的输出, 为了使图 1 (b) 中 A0 和 A1 的信号流能分别在 Out5 和 Out6 进行输出, 在不配置时 A3 为 0, 在配置 A3 时需要使其中任意偶数个为 1。如图 1 (c) 是实现图 1 (a) 和图 1 (b) 的双输出查找表 LUT6_2, A0-A4 端口是两个查找表的共同输入, 用于图 1 (a) 和图 1 (b) 的输入, A5 端口用于选择控制 Out6 的输出是图 1 (c) 上面的 LUT5 输出还是下面 LUT5 的输出, 当 A5=1 时, Out6 输出图 1 (c) 中上面的输出, 这也是本设计的设置。

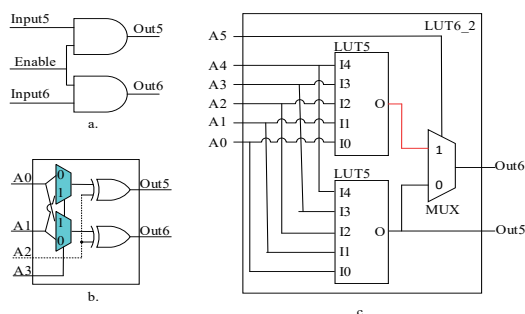


图 1 基于六输入双输出 LUT6_2 使能与延时单元

如图 2 (b) 所示, 是可选式双轨道结构的抽象图, 现有独立线路 IN1、IN2、IN3、IN4。其中, IN1 和 IN2 由实线标注, 是一组双输出 RO 延时通过路径, 通过这一组路径可以实现基本双输出 RO 结构的输出响应串。此外, IN3 和 IN4 是另一组双输出 RO 延时通过路径, 由虚线标注, 同样可以实现相同的响应串输出。其中, Key 用于控制双轨道的切换, 当 Key=0 时, IN1 输出到 Out1, IN2 输出到 Out2, 此时停止 IN3 和 IN4 进行输入, 而 Key=1 时, IN3 输出到 Out1, IN4 输出到 Out2, 停止 IN1 和 IN2 的输入。路径切换的原理是根据具有二选一 MUX 的逻辑进行实现的, 如图 2 (a) 所示。如图 2 (c) 是由 7 阶图 2 (a) 组成, 实现 7 阶双输出可配置反相器单元的路径控制。

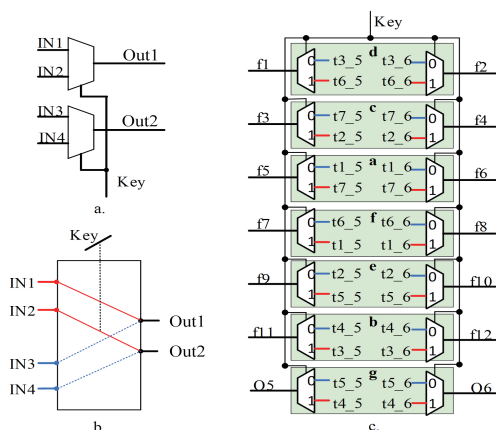


图 2 基于六输入双输出 LUT6_2 可选式双轨道单元

1.2 电路实现

如图 3 所示, 是可选式双轨道双输出 RO PUF 结构设计, 结构中单个 RO 环由 2 个使能单元和 7 个基本延时单元和 7 个基本可选式双轨道单元组成, 而整个 SDT-DORO PUF 结构的组成除两个 RO 环之外, 还有 4 个计数器 Counter 和 2 个比较器 CMP 构成。如图 3 所示, 该 SDT-DORO PUF 设计电路结构通过输入使能信号 (Enable) 和激励信号 Sel, 可以使具体的 SDT-DORO 环路径输出脉冲, 其中 Sel 为 7 位长度的变量, 对于 Sel 在此前提到的 A3 配置方式, 当轨道选择变量 Key=0 时, 起振方式会走红线路径, 此时, 则每个计数器就有 64 种脉冲计数方式, 则 Counter1 的 64 种计数和 Counter3 的 64 种计数输出进行比较得到 128 位响应, 同理 Counter2 和 Counter4 也是如此, 共计输出 128 位响应, 同理当 Key=1 时起振路径会走蓝线, 根据 Sel 的配置会再有 128 位的响应进行输出, 最后通过 Key 和 Sel 的配置总共将有 256 位的响应进行输出。

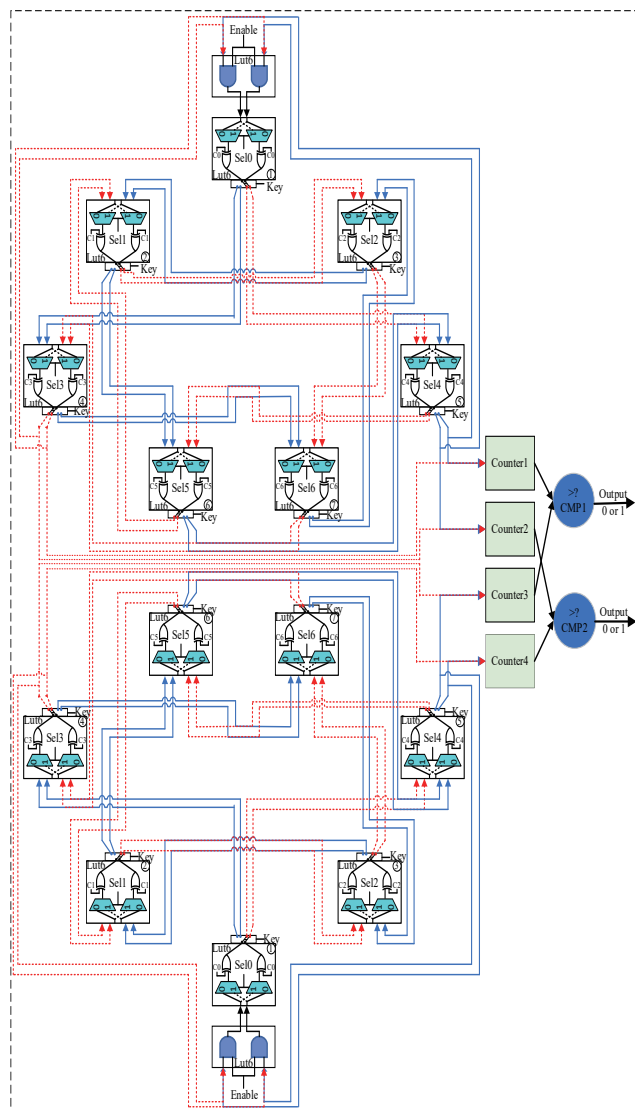


图 3 所提出的 SDT-DORO PUF 结构图

2 实验结果

在本节中, 根据 RO PUF 电路系统性能指标量化方法, 评估所提出的 SDT-DORO PUF 结构在随机性、唯一性、可靠性和硬件资源开销方面的性能。本文实验平台基于 Xilinx 的 Zynq-7000 系列开发板。在该系列开发板上实现了 16 个 PUF, 且每个 PUF 皆具备 256 位的输出响应。

2.1 随机性

随机性是指制造过程中的工艺偏差和物理特性的不可控性, 使得每个 RO PUF 实例在相同激励下会产生不同且不可预测的响应。随机性越高, 安全性也就越高, 就越不容易遭受攻击。随机性可以通过随机性测试套件 NIST SP800-22 进行质量评估^[11]。

在本文中, 使用 MATLAB 将 Zynq 开发板上实现的 16 组 PUF 结构电路收集的 0 与 1 输出序列以图形化形式展现, 如图 4 所示。图中, 垂直轴代表 FPGA 序列号, 每两行水平轴则代表 256 位的 PUF 输出。通过观察可以看到 PUF 输出呈现出一定的随机特性。为精确量化此随机性, 下面将采用 NIST SP800-22 标准对开发板所产生的随机序列实施测试。



图 4 基于 Xilinx Zynq-7000 的 16 组 256 位 PUF 随机流

本文所采用的 NIST 测试软件, 是依据 SP800-22 测试套件所编写的 Python 程序实现测试^[12]。该测试套件涵盖了 15 个测试项目, 其中 8 项专门用于评估 PUF 的随机性, 具体有近似熵测试、块内频数检验、累积和检验、离散傅里叶变换检验、频数检验、块内最长游程检验、游程检验以及序列检验。每个测试项目完成后, 都会输出一个 p 值, 用于衡量被测序列的随机性水平, p 值越大随机性越好^[11]。针对本文提出的基于 SDT-DORO PUF 实现的测试, 是在 Xilinx Zynq-7000FPGA 开发板上输出的 16 组 256 位的随机序列, 如图 5 所示。

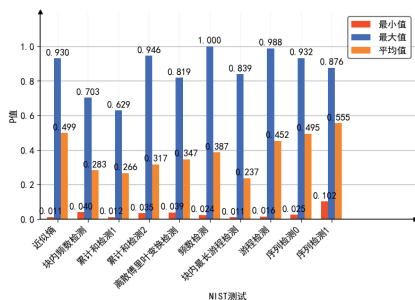


图 5 基于 Xilinx Zynq-7000 的 16×256 位 PUF 输出序列通过了 NIST 测试结果

其中最高值表示 16 组测试的最大值; 最低值表示 16 组测试的最小值; 中间值表示 16 组的平均值。通过这些测试结

果可以看出 p 值均超过了 0.01 的显著性水平阈值, 具有较好的随机性。

2.2 唯一性

唯一性是指两个相同的 PUF 实体在相同激励下产生不同响应的能力。理想情况下, 相同的 PUF 电路在不同 FPGA 芯片上输出的响应应具有 50% 的平均片间汉明距离 (HD_{inter}), 计算公式为:

$$Uniqueness = HD_{inter} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^k \frac{HD(R_i, R_j)}{n} \times 100\% \quad (1)$$

式中: $HD(R_i, R_j)$ 表示响应 R_i 和响应 R_j 的汉明距离; R_i, R_j 表示第 i 个和第 j 个 PUF 实体所产生的响应; k 表示被统计 PUF 实体的个数; Uniqueness 表示芯片的唯一性。

如图 6 所示, 列出了 120 个片间汉明距离在不同区间的概率分布状况, 从中可见 RO PUF 的汉明距离主要聚集在理想值 128 左右。将这 120 个片间汉明距离求平均值为 126.567, 把平均值归一化后就是唯一性的评价指标, 如式 (1)。求得 PUF 的唯一性评价指标为 49.44%。由此可见, 所提出的结构展现出了较好的唯一性。

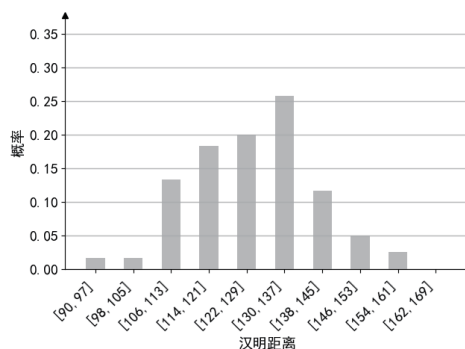


图 6 基于 Xilinx Zynq-7000 的 120 个片间汉明距离概率分布

2.3 可靠性

片内汉明距离用于度量在芯片同一位置部署相同的 PUF 实体, 处于不同时刻或环境情况时, 向该实体施加相同输入激励时, 其两次输出响应序列的差异程度。这一参数是表示 PUF 可靠性的关键指标, 计算公式为:

$$Reliability = 1 - \frac{1}{m} \sum_{i=1}^m \frac{HD(R_i, R_{it})}{n} \times 100\% \quad (2)$$

式中: Reliability 表示 PUF 的可靠性; $HD(R_i, R_{it})$ 表示响应 R_i 与响应 R_{it} 的汉明距离; R_i 表示在开发板老化前条件下 PUF 的输出响应; R_{it} 表示第 t 次在不同老化时间环境条件下 PUF 的输出响应; m 表示测试 PUF 响应的总次数; n 表示生成响应串 $HD(R_i, R_{it})$ 的长度。

在理想状态下, 若测试条件出现变化, 当施加相同激励给 PUF 实体时, 其输出响应在误差允许范围内应保持不变, 此时可靠性的理想取值为 100%。

在本次实验初始阶段, 对 16 组可选式双轨道双输出 RO

PUF 施加一致的激励，并记录开发板老化前的 16 组可选式双轨道双输出 RO PUF 的 256 位输出响应；待开发板静置老化近 3 个月的时间结束后，再次对其输出响应进行测量。得出老化前后的 PUF 实体实验的 16 个片内汉明距离概率分布，如图 7 所示。

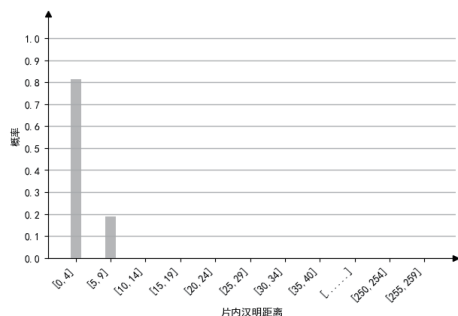


图 7 老化前后的 PUF 实体实验的 16 个片内汉明距离概率分布

图 7 统计了 16 组可选式双轨道双输出 RO PUF 概率分布的片内汉明距离。在图 7 可以看出本文所实现的可选式双轨道双输出 RO PUF 的片内汉明距离最大值为 6，最小值为 0，其片内汉明距离主要集中在 0~4 之间；对于 256 位的可选式双轨道双输出 RO PUF 的平均片内汉明距离为 2.875，平均可靠性为 98.88%，对于可靠性理想值 100% 非常接近。

2.4 相关比较

本文提出的 SDT-DORO PUF 性能与一些现有 RO PUF 结构电路研究进行了对比，主要从随机性、唯一性、可靠性、生成响应位数和硬件开销等方面进行了比较。其中，对于硬件开销的资源消耗比较主要通过一对 RO 环的硬件资源消耗上与其他方案相比。所以，本文仅通过 RO PUF 的延迟电路和选择电路两部分的硬件消耗作为比较，如表 1 所示。

表 1 环形振荡器 PUF 性能指标对比

性能	随机性	唯一性 /%	可靠性 /%	响应 / 位	硬件开销 (Slices)
RO PUF ^[13]	—	47.67	97.88	283	727
CRO PUF ^[14]	—	48.49	99.55	256	210
RO PUF ^[15]	—	47.13	99.16	256	82
MT RO PUF ^[16]	通过	49.17	—	128	16
CRO PUF ^[9]	—	48.80	98.19	248	16
本文	通过	49.44	98.877	256	8

从表 1 中可以看到，本文设计的可选式双轨道双输出 RO PUF 的唯一性最好，可靠性表现良好，与理想值接近，最小熵值和位混淆值低于相关比较结构值，同时随机性通过了 NIST 测试。与其他方案相比，本设计在降低硬件资源消耗和提高响应位方面具有优异的效果。

3 结论

本文提出的基于查找表的六输入双输出查找表

(LUT6_2) 的可选式双轨道双输出 RO PUF (SDT-DORO PUF) 设计有效降低了硬件资源。实验结果表明，SDT-DORO PUF 在随机性、唯一性和可靠性等性能指标上均表现优异，随机性测试通过了 NIST 标准。该设计不仅降低了硬件开销，还显著提高了响应位的输出，展示了作为芯片加密技术的潜力。未来的研究可进一步优化设计，以提升安全性和不同场景应用下的适用性。

参考文献：

[1]YAO L, LIANG H G, HUANG Z F, et al. A lightweight configurable XOR RO-PUF design based on Xilinx FPGA[C]//2021 IEEE 4th International Conference on Electronics Technology (ICET). Piscataway:IEEE,2021: 83-88.

[2]GU C Y, CHANG C H, LIU W Q, et al. A modeling attack resistant deception technique for securing lightweight-PUF-based authentication[C]//2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST) .Piscataway: IEEE, 2020: 1183-1196.

[3]DELVAUX J, GU D W, SCHELLEKENS D, et al. Helper data algorithms for PUF-based key generation: overview and analysis[J]. IEEE transactions on computeraided design of integrated circuits and systems, 2014, 34(6): 889-902.

[4]EDWARD SUH G, DEVADAS S. Physical unclonable functions for device authentication and secret key generation[C]// Proceedings of the 44th annual design automation conference. Piscataway: IEEE, 2007: 9-14.

[5]MAITI A, SCHAU MONT P. Improved ring oscillator PUF: an FPGA-friendly secure primitive[J]. Journal of cryptology, 2011, 24: 375-397.

[6]AGUSTIN J, LOPEZ-VALLEJO M L. A temperature-independent PUF with a configurable duty cycle of CMOS ring oscillators[C]//2016 IEEE International Symposium on Circuits and Systems (ISCAS). Piscataway: IEEE, 2016: 2471-2474.

[7]LEE J S, CHOI P, KIM S J, et al. Built-in hardware pseudo-random test module for physical unclonable functions[J]. Nonlinear theory and its applications, 2014, 5(2): 101-112.

[8]GUAJARDO J, KUMAR S S, SCHRIJEN G J, et al. FPGA intrinsic PUFs and their use for IP protection[C]//Cryptographic Hardware and Embedded Systems - CHES 2007. Berlin:Springer,2007: 63-80.

[9]PEI S W, ZHANG J D, WANG R N. A low-overhead RO PUF design for Xilinx FPGAs[J]. IEICE electronics express, 2018, 15(5): 20180093.

[10]CROCKETT L H, ELLIOT R A ENOERWITZ M A, et al.

- The Zynq book: embedded processing with the ARM Cortex-A9 on the Xilinx Zynq-7000 all programmable soc[EB/OL]. (2014-07-14)[2025-11-22].<https://dl.acm.org/doi/book/10.5555/2685817>.
- [11]BASSHAM L E, RUKHIN A L, SOTO J, et al. SP 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications[EB/OL].(2010-04-01)[2025-11-22].<https://dl.acm.org/doi/abs/10.5555/2206233>.
- [12]DJ-on-GitHub, sp800_22_tests[EB/OL].[2025-11-02].https://github.com/dj-on-github/sp800_22_tests.
- [13]HABIB B, GAJ K, KAPS J P. FPGA PUF based on programmable LUT delays[C]//2013 Euromicro Conference on Digital System Design. Piscataway:IEEE, 2013: 697-704.
- [14]RABIEI H, KAVEH M, MOSAVI M R, et al. MCRO-PUF: a novel modified crossover RO-PUF with an ultra-expanded CRP space[J].Computers, materials and continua, 2023, 74(3): 4831-4845.

- [15]NALLA ANANDAKUMAR N, HASHMI M S, SANADHYA S K. Compact implementations of FPGA-based PUFs with enhanced performance[C]//2017 30th International Conference on VLSI Design and 2017 16th International Conference on Embedded Systems (VLSID). Piscataway: IEEE, 2017: 161-166.
- [16]ZHANG Y, LIANG H G, YAO L, et al. A high reliability physically unclonable function based on multiple tunable ring oscillator[J].Microelectronics journal, 2021, 117: 105263.

【作者简介】

余方计（1999—），通信作者（email:505272772@qq.com），男，河南商丘人，硕士研究生，研究方向：计算机智能技术与应用。

范小娇（1978—），女，河南焦作人，博士，副教授，研究方向：物联网技术与应用、集成电路新型材料和器件研究。

（收稿日期：2025-07-01 修回日期：2025-12-11）

（上接第 123 页）

5 结语

本研究围绕瞬态电磁干扰下变电站谐振过电压这一问题展开了深入探索，提出了针对性的主动补偿抑制方法。研究结果表明该方法在抑制谐振过电压方面取得了显著成效，高频振荡能量、暂态持续时间、相间不平衡度和能量熵等关键参数均得到大幅优化，电网中的谐波含量显著降低，总谐波畸变率明显下降，有效提高了电网的电能质量和稳定性。同时，与传统的抑制方法相比，所提方法在抑制效果和稳定性等方面均展现出明显优势。未来，将进一步优化主动补偿抑制方法，提高其适应性和智能化水平，以应对更为复杂多变的运行环境，加强与实际工程的结合，为电力系统的安全可靠运行提供更加坚实的保障。

参考文献：

- [1] 向常圆, 宋宝同, 李笑彤, 等. 北京地区 500 kV 变电站 66 kV 侧 PT 间隔故障仿真及铁磁谐振过电压抑制方法研究[J]. 电瓷避雷器, 2024(3):77-84.
- [2] 石小帅, 顾智广, 仲昭峰, 等. 基于 PSCAD 的自耦变空载投运谐振过电压仿真分析[J]. 电工技术, 2023(21):150-151.
- [3] 刘其辉, 吴勇, 闫佳颖, 等. 考虑相位跳变的双馈风电机组低电压穿越特性分析与暂态过电压抑制[J]. 太阳能学报, 2024, 45(5):86-94.

- [4] 董成武, 牛芳, 夏林伟, 等. 两级式单相光伏逆变器并网过电压抑制策略研究[J]. 电网与清洁能源, 2023, 39(11):134-141.
- [5] 杜明珠, 张鹏鹏. 新能源汽车电气系统瞬变过电压抑制技术[J]. 时代汽车, 2024(19):113-115.
- [6] 王蒙, 张文朝, 汪莹, 等. 高比例光伏接入的电力系统暂态过电压控制策略[J]. 太阳能学报, 2023, 44(10):148-155.
- [7] 闫佳颖, 刘其辉, 李开心, 等. 直流换相失败故障下 DFIG 暂态特性分析与过电压抑制[J]. 电网技术, 2024, 48(9): 3912-3920.
- [8] 黄浪尘, 李俊桦, 何东, 等. 一种基于 MOV-RC 缓冲电路的中压直流固态断路器过电压抑制方法研究[J]. 电工电能新技术, 2024, 43(9):51-63.
- [9] 刘杉, 谭开东, 姜喆, 等. 基于可控自恢复消能装置的直流送端暂态过电压抑制方法[J]. 电力系统自动化, 2024, 48(9): 142-150.
- [10] 姚创, 魏菊芳, 崔涵, 等. 基于流敏电阻非有效接地系统 PT 谐振过电压抑制[J]. 电瓷避雷器, 2023(1):191-198.

【作者简介】

代庆超（1983—），男，山东冠县人，本科，高级工程师，研究方向：电力建设、电气设备安装和调试。

（收稿日期：2025-05-28 修回日期：2025-11-28）