AES 算法作为一种广泛应用的加密算法，一直以来都受到学术界和工业界的高度关注。目前，AES 算法在不同领域不断有新的研究成果涌现。以下是对 AES 算法目前最新研究成果的介绍。

一、FPGA 实现方面的新进展

高效的 FPGA 实现方案：有研究提出了 AES-128 算法的 FPGA 实现作为加速器用于高性能密码学应用[1]。该方案利用 Xilinx Vivado 软件在 Virtex-7 评估套件上对 AES 算法进行编码，实现了资源高效的设计，仅使用 588 个查找表（LUTs）和 353 个触发器。这展示了 FPGA 技术在密码学加速方面的有效性，在算法复杂性和资源利用之间取得了良好的平衡。

改进的 AES 加密算法及 FPGA 实现：为提高数据传输的保密性和加密解密的高效性，有研究利用数字信封技术对传统的 AES 加密算法进行改进，并基于 FPGA 予以实现[3]。将 AES 加密算法和非对称加密中的 RSA 加密算法相结合，利用 RSA 加密算法中陷门单向置换变换的特点，对敏感密钥信息单独进行加密。实验验证结果表明，改进程序完成了数据加解密算法，可实现错误率为零，加解密速度达到 1.62 Mb/s，比文献研究结果提高了近 25.56%。

二、避免使用查找表的方法

提高加密解密速度：有研究描述了在 AES 加密和解密过程中，在 MixColumns 变换中不使用查找表的方法[2]。加密过程包括字节替换、行移位、列混合和轮密钥加。在第 10 轮中不进行列混合变换。解密过程包括逆列混合、逆行移位、逆字节替换和轮密钥加。该研究在 Matlab 软件中使用了两种方法进行 AES 加密和解密，即基于查找表和在 MC/IMC 变换中不使用查找表。实验结果表明，不使用查找表的加密和解密过程比使用查找表的方法更快。例如，在 MC 变换中不使用查找表的加密过程耗时 0.091 秒，而使用查找表则耗时 0.399 秒；在IMC变换中不使用查找表的解密过程耗时0.149秒,而使用查找表则耗时0.206秒[2]。

三、与其他技术结合的创新

DNA 计算增强 AES 算法：有研究提出了一种用 DNA 序列增强的高级加密标准（AES）设计[4]。该算法在混合列步骤中将所有特征（数据、算法操作和使用的函数）都在 DNA 序列上实现，而不是在比特上。这种技术展示了构建基于 DNA 序列的复杂系统的可能性，使其成为在生物环境或 DNA 计算机上使用的合适竞争者。实验结果表明，该算法在不同文本文件大小的破解时间方面有显著改进[4]。

四、基于机器学习的功耗分析

提高分类准确率：针对无掩码防护的 AES 算法实现，有研究将半监督机器学习算法 Tri-Training 应用于功耗分析，有效减少了用机器学习算法进行建模时所需要的有标记能量迹数量[5]。在使用 Tri-Training 算法进行建模时引入了阈值判断操作，提高了分类的准确率，并对比了不同阈值对分类准确率的影响。对在 ATM89S52 单片机上实现的 AES-128 算法进行建模类功耗分析，实验结果表明，在使用 80 条有标记能量迹时，相较于使用有监督学习算法的准确率为 63.49%，本方法的准确率为 74.56%，准确率提升了约 11%[5]。

[1]Siddiqui, A. F., & Sekhar, P. C. (2024). FPGA acceleration of AES algorithm for high-performance cryptographic applications. Computer Science and Engineering, June-July, 3.

[2]Prayitno, R. H., Sudiro, S. A., & Madenda, S. (2021). Avoiding lookup table in AES algorithm. In 2021 Sixth International Conference on Informatics and Computing (ICIC) (pp. 1-6). IEEE.

[3]柴绍杰,张彩珍. "AES加密算法的改进及FPGA实现." 兰州交通大学学报 3(2020).

[4]Omar G. Abood,Saleh Mesbah,Shawkat Guirguis. (2018). Enhancing AES Algorithm with DNA Computing..

[5]王相宾,王永娟,赵远,高光普,袁庆军. (2021). 基于半监督学习的AES算法功耗分析. 《密码学报》(4).