周报-向嘉豪 (2024-11-11)

向嘉豪

衡阳师范学院

2024 年 11 月 11 日

摘要

本周工作

- 完成了线性层的重构
- 系统性分析了 [LP24] 的线性层优化方法
- 实验结果表明，循环矩阵在 AES 中的应用效果未达预期
- 基于此，我们将研究重点转向线性层中置换操作的优化

线性层优化算法分析

基本概念

- 初始状态：$((x_1), 1)$
- 代价函数：$Cost(x) = weight(x)$，即 x 的汉明权重
- 通过状态转移递归地优化代价函数

基本转移规则

1. $x_i = 1 \lll r : ((x_1, \ldots, x_i, \ldots, x_v), v) \rightarrow ((x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_v), v-1)$
2. $x_i = x_j \lll r : ((x_1, \ldots, x_i, \ldots, x_v), v) \rightarrow ((x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_v), v-1)$

核心转移策略

三种核心策略

1. $x_i = a \oplus (a \ggg r) \oplus b$
   - $a = x_i \wedge (x_i \lll r)$
   - $a \wedge (a \ggg r) = 0$
2. $x_i = x_i \oplus (x_j \lll r), \ i \neq j$
3. $x_i = a \oplus b, \ x_j = (a \ggg r) \oplus c$

AES 线性层结构分析

矩阵结构

- 基于 [AP21] 的研究，分析了切片 AES 线性层 $L = MP$
- M 为 128×128 矩阵，具有显著的分块特征
- P 为 128×128 单位置换矩阵

矩阵表示

$$M = \begin{pmatrix} M_0 & 0 & 0 & 0 \\ 0 & M_0 & 0 & 0 \\ 0 & 0 & M_0 & 0 \\ 0 & 0 & 0 & M_0 \end{pmatrix}, \text{ 其中}$$

$$M_0 = \begin{pmatrix} M_{00} & M_{01} & M_{02} & M_{03} \\ M_{03} & M_{00} & M_{01} & M_{02} \\ M_{02} & M_{03} & M_{00} & M_{01} \\ M_{01} & M_{02} & M_{03} & M_{00} \end{pmatrix}$$

优化效果分析

实验验证

- 对 AES 第一个寄存器的 M 矩阵在交错形式下进行分析
- 可表示为 4×8 矩阵 M_i

矩阵 M_i

$$M_i = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

实验结果

发现

- 向量 $x_i = 01111010$ 可实现最优分解：$x_i = a \oplus (a \ggg r) \oplus b$
- 参数：$a = 0101000$，$r = 3$，$b = 0010000$
- 在交错形式下，$Cost(a) = 2$，可以减少 1 次 XOR
- 然而，转换回标准形式后，仍需 4 次 XOR 操作

结论

揭示了 [LP24] 优化方法的局限性，仅在 XOR 操作次数超过 4 次时体现优势

论文撰写

研究结论

- 循环矩阵在 AES 应用中效果未达预期
- 将研究重心转向线性层中置换操作的优化

主要工作

1. **结构优化**：
   - 重新组织内容结构
   - 提高论文的逻辑性和可读性
2. **算法改进**：
   - 基于切片并行和动态规划的策略，优化 merge 和 split 操作
3. **OPO 算法优化**：
   - 引入贪心递归策略
   - 确保算法收敛性和全局最优解

参考文献 I

Alexandre Adomnicai and Thomas Peyrin.
Fixslicing aes-like ciphers new bitsliced AES speed records on arm-cortex M and RISC-V.
IACR Trans. Cryptogr. Hardw. Embed. Syst., 2021(1):402–425, 2021.

Gaëtan Leurent and Clara Pernot.
Design of a linear layer optimised for bitsliced 32-bit implementation.
IACR Trans. Symmetric Cryptol., 2024(1):441–458, 2024.

老师评语

一、工作报告应明确呈现结果和工作量

本周主要精力投入在理解 [LP24] 的算法，并尝试将其应用于 AES 的线性层优化。由于效果不理想，报告中未详细阐述该部分工作

二、需明确最终完成计划

本周计划，完成 AES 实现、实验数据的整理和论文初稿