

LowMC 实例的差分枚举攻击效果分析

葛欣欣^{1,2}, 李智虎³, 王美琴^{1,2}, 胡凯^{1,2}

- (1. 山东大学网络空间安全学院(研究院), 山东 青岛 266237;
2. 山东大学密码技术和信息安全教育部重点实验室, 山东 青岛 266237;
3. 中国电力科学研究院有限公司, 北京 100192)

摘要: LowMC 是具有低乘法复杂度特征的算法。针对低数据量和少量 S 盒参数下的 LowMC 实例, 差分枚举攻击被提出, 理论上可以攻击全轮 LowMC 算法。考虑到这种攻击是在线性层完全随机的条件下给出的, 对 LowMC 算法在真实的线性层下抵抗差分枚举攻击的强度进行了研究。通过对关键起始轮数的研究发现, 差分枚举攻击并非总是可以达到理论攻击轮数。对于某些关键起始轮数比理论值小的 LowMC 实例, 差分枚举攻击甚至会失败。由于 LowMC 算法的轮数设置基于现有攻击的效果, 该分析对 LowMC 算法的轮数设计具有重要意义。

关键词: 分组密码; LowMC 算法; 差分枚举攻击; 关键起始轮数

中图分类号: TN918.1

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021046

Effect of the difference enumeration attack on LowMC instances

GE Xinxin^{1,2}, LI Zhihu³, WANG Meiqin^{1,2}, HU Kai^{1,2}

1. School of Cyber Science and Technology, Shandong University, Qingdao 266237, China
2. Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Qingdao 266237, China
3. China Electric Power Research Institute, Beijing 100192, China

Abstract: The LowMC is an algorithm with low multiplicative complexities. For the parameter with limited data complexities and low number of S-boxes, the difference enumeration attack was proposed, which could theoretically attack all rounds of the LowMC. Considering that the original attack is based on the random linear layer, the strength

收稿日期: 2021-01-10; 修回日期: 2021-03-15

通信作者: 王美琴, mqwang@sdu.edu.cn

基金项目: 国家自然科学基金(62002201, 62032014); 国家重点研发计划(2018YFA0704702); 山东省重大科技创新项目(2019JZZY010133); 山东省自然科学基金重大基础研究项目(ZR202010220025)

Foundation Items: The National Natural Science Foundation of China (62002201, 62032014), The National Key R&D Program of China (2018YFA0704702), The Major Scientific and Technological Innovation Project of Shandong Province (2019JZZY010133), The Major Basic Research Project of Natural Science Foundation of Shandong Province, (ZR202010220025)

论文引用格式: 葛欣欣, 李智虎, 王美琴, 等. LowMC 实例的差分枚举攻击效果分析[J]. 网络与信息安全学报, 2021, 7(3): 149-155.

GE X X, LI Z H, WANG M Q, et al. Effect of the difference enumeration attack on lowMC instances[J]. Chinese Journal of Network and Information Security, 2021, 7(3): 149-155.

of LowMC algorithm against differential enumeration attacks under a specific linear layer deserves more study. The difference enumeration attack cannot reach theoretical rounds through the research on the so-called key initial round. In terms of some LowMC instances, the key initial round is smaller than the theoretical value, which leads to the failure of the difference enumeration attack. Since the number of rounds of the LowMC is completely based on existing attacks, the analysis is of great significance to the rounds design of the LowMC.

Keywords: block cipher, LowMC algorithm, difference enumeration attack, key initial round

1 引言

Albrecht 等^[1]在 2015 年欧密会上提出了 LowMC 算法。LowMC 算法基于 SPN 结构, 采用了部分非线性层和随机线性层的设计, 其乘法复杂度非常低。LowMC 实例是通过改变分组长度、密钥长度、每轮 S 盒的数量和数据复杂度的安全预期得到的。LowMC 算法的低乘法复杂度特点使它在多方计算和全同态加密等场景下效率较高, 自公开以后就受到了广泛关注。

在 2015 年亚密会上, Dinur 等^[2]提出了优化差值攻击, 在弱密钥下以 2^{57} 的时间复杂度全轮攻破 LowMC-80。之后 Dobraunig 等^[3]在 2015 年的 ICISC 会议上提出高阶代数攻击, 以 2^{33} 的复杂度全轮攻破 LowMC-80。为此, LowMC 算法的设计者给出了新的轮数计算公式, 称为 LowMCv2。少量 S 盒、低数据量参数版本的 LowMCv2 算法被新提出的基于非交互式零知识证明 (NIZK, non-interactive zero-knowledge) 的公钥签名方案采用作为加密算法^[4]。少量 S 盒和低数据量是指每轮 S 盒数量和数据量都取较小值。随后, 在 2018 年的 FSE 会议上, Rechberger 等^[5]提出了可以攻破全轮 LowMCv2 算法少量 S 盒参数版本的差分枚举攻击。他们在中间相遇攻击^[6-7]的基础上, 考虑 d 差分的传播, 分别从输入差分、输出差分两个方向进行加密和解密, 在中间轮数进行差分集合的碰撞^[8-9], 从而得到 LowMCv2 算法的差分枚举攻击区分器。为了抵抗差分枚举攻击, LowMC 算法的第 3 版 (LowMCv3) 再次修改了轮数。但是, Rechberger 等的攻击是在理想线性层的假设下进行的, 对实例化的 LowMCv2 算法 (即线性层是一组真实的矩阵) 的实际攻击效果依然是未知的。

本文研究了差分枚举攻击对实例化后的 LowMCv2 算法的攻击效果, 发现对于某些参数

的 LowMC 实例, 差分枚举攻击的实际可攻击轮数并不能达到理论计算值。差分枚举攻击的可攻击轮数与 LowMCv2 算法的概率为 1 的差分路线 (这条路线的轮数被称为关键起始轮数) 直接相关。为此, 本文给出一种高效的计算 LowMC 算法概率为 1 的差分路线的方法。本文控制非线性层部分的差分状态, 保证 S 盒部分不引入差分、其他部分引入差分, 建立差分传播的线性方程组。之后通过高斯消元法^[10]解方程组, 可以得到概率为 1 的差分路线。实验发现, 无论是在 LowMC 算法设计者推荐的线性矩阵下, 还是任意随机矩阵下, 关键起始轮数都有很大概率无法达到理论值, 也就是说, 差分枚举攻击并不总是可以达到理论的攻击轮数。对于某些特殊参数下的 LowMC 算法实例, 差分枚举攻击甚至会失败。在 LowMCv3 算法中, 考虑了差分枚举攻击的可攻击轮数, 重新定义 LowMC 算法的轮数。本文对差分枚举攻击的实际攻击效果分析表明, LowMCv3 算法的轮数可以适当降低, 以提升 LowMCv3 算法的实现效率。

2 差分枚举攻击及在 LowMC 算法的应用

2.1 LowMC 算法描述

LowMC 算法^[1]是基于 SPN 结构的部分非线性层分组密码, 其轮函数如图 1 所示。令第 r 轮的输入状态为 x_r , 则输出状态 x_{r+1} 的计算公式为

$$x_{r+1} = \text{KeyAddition}^{(r)} \cdot \text{ConstantAddition}^{(r)} \cdot \text{LinearLayer}^{(r)} \cdot \text{SboxLayer}(x_r) \quad (1)$$

SboxLayer 由 m 个 3 bit S 盒组成。非线性层中采用了具有低代数次数、低乘法复杂度等特点的 S 盒, S 盒为 $S(a, b, c) = (a \oplus bc, a \oplus b \oplus ac, a \oplus b \oplus c \oplus ab)$ 。此时要求 n 和 m 的关系满足 $n \geq 3m$, 当 $n > 3m$ 时, 剩余的 $n - 3m$ 位状态直接进入线性层。

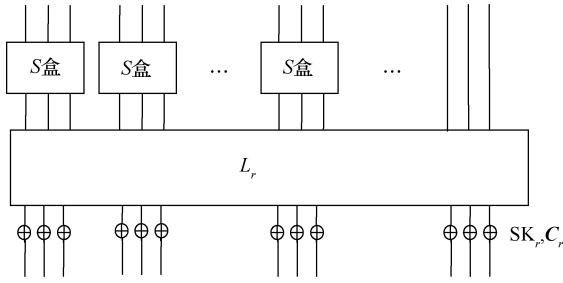


图1 LowMC 算法加密轮函数
Figure 1 The round function of LowMC

$\text{LinearLayer}^{(r)}$ 是第 r 轮的线性层。在这个函数下, 分组状态被 $n \times n$ 的随机矩阵 L_r 乘, 每一轮的随机矩阵是在算法初始化时随机生成的。

$\text{ConstantAddition}^{(r)}$ 是第 r 轮的轮常数加, 是将分组状态与一个 n bit 长度的随机常数向量 C_r 相加, 每一轮的常数向量 C_r 也是随机生成的。

$\text{KeyAddition}^{(r)}$ 是将分组状态与一个 n bit 轮密钥 SK_r 相加, 而轮密钥 SK_r 是由主密钥 K 与一个 $n \times k$ 的随机矩阵 K_r 相乘得到的, 生成的轮密钥 SK_r 具有每一轮独立、随机的特点。

LowMC 算法的分组长度、密钥长度、每轮 S 盒的数量和可承受攻击的数据复杂度是可以根据应用场合改变的参数, 被称为可变参数。为了适用于多种应用场合, 可变参数调整得到不同的实例。对于不同的实例, LowMC 算法轮数是根据可变参数现存的有效攻击计算得到的, 所以正确分析每个攻击的可攻击轮数, 对于 LowMC 算法来说至关重要。LowMC 算法线性层的特点是随机选取且相互独立的。在保证随机性、可靠性、快速生成有效随机位的前提下, 设计者推荐用 Grain 算法中的线性反馈移位寄存器(LFSR, linear feedback shift register)^[11]作为自收缩发生器^[12]生成线性层, 预期这样可以得到尽可能随机化的线性层。考虑到使用 LFSR 生成的线性矩阵存储空间和计算消耗比较大, 将线性层优化为等价线性层^[13]可以在不增加非线性操作和不危及安全性的同时, 减少线性代数复杂度。

2.2 差分枚举攻击在 LowMC 算法上的应用

为了提高差分枚举区分器的长度, Rechberger 等研究了 d 维差分组的传播, 简称 d 差分, 定义如下。

定义 1 d 差分^[14]。

一个 $d+1$ 元组 $(x_0, x_1, \dots, x_d)$ 对应的 d 差分定义为 $(x_0 \oplus x_1, x_0 \oplus x_2, \dots, x_0 \oplus x_d)$, d 差分中的差分个数 d 称为差分维度。

传统的差分枚举攻击的基本思路是对于输入 d 差分 $(\Delta_{\text{in}}^1, \Delta_{\text{in}}^2, \dots, \Delta_{\text{in}}^d), \Delta_{\text{in}}^i \in \Phi_2^n$, 经过正向加密 r_1 轮的差分传播, 得到在 r_1 轮处可达到的差分列表 D_{d_1} , 对于给定的 $r_1 + r_2$ 轮的输出 d 差分 $(\Delta_{\text{out}}^1, \Delta_{\text{out}}^2, \dots, \Delta_{\text{out}}^d), \Delta_{\text{out}}^i \in \Phi_2^n$, 经过反向解密 r_2 轮的差分传播, 得到在 r_1 轮处的可达到差分列表 D_{d_2} 。若 D_{d_1} 和 D_{d_2} 产生碰撞, 则得到一条长度为 $r_1 + r_2$ 的差分路线。结合时间复杂度、避免错误碰撞等条件, r_1 和 r_2 的计算公式如下。

$$r_1 = r_2 < \left\lceil \frac{\frac{1}{2}dn}{\text{lb}\lambda_d^m} \right\rceil, \left\lfloor \frac{k}{\text{lb}\lambda_d^m} \right\rfloor \quad (2)$$

其中, λ_d 为一个随机 d 差分经过 S 盒后平均可达到的输出 d 差分的数量^[15], m 是 LowMC 算法轮函数中的 S 盒个数。由于 LowMC 算法的非线性层中只有部分状态过 S 盒, 对于某些特殊的输入 d 差分, 总是有概率为 1 的 r_0 轮差分路线存在, 差分路线成立概率为 1 的差分路线轮数 r_0 定义如下。

定义 2 关键起始轮数。

关键起始轮数定义为, 在部分非线性层中, 通过选择合适的输入差分, 得到传播概率为 1 的差分路线的长度。

这条概率为 1 的差分路线总是能放在经典的差分枚举攻击之前, 从而延长差分枚举区分器的长度至 $r_0 + r_1 + r_2$ 。对 LowMC 算法的差分枚举攻击如图 2 所示。

对 LowMC 算法来说, 式(2)很好地估计了 r_1 和 r_2 的值。但对于 r_0 的估计, 是建立在 LowMC 算法的线性层为完全随机的假设之上的。在差分枚举攻击过程中, 差分路线每增加一轮, 可能激活的 S 盒个数最多增加 m 个, 过 S 盒的比特数也相应最多增加 $3m$ 个, 那么 r_0 轮后, 经过活跃 S 盒的比特数最多为 $3r_0m$, 有 2^{n-3r_0m} 个差分没有激活任意的 S 盒。为了在 r_0 轮存在概率为 1 的 d 差分特征, 要满足 $2^{n-3r_0m} > d$ 的条件, 于是得到 r_0 的理论最大值为

Δ_x^i : 第 x 轮的第 i 个差分

r_0 : 关键起始轮数

r_1 : 加密方向扩散轮数

r_2 : 解密方向扩散轮数

$$\Pr((\Delta_0^i) \rightarrow (\Delta_m^i)) = 1, i \in (1, \dots, d)$$

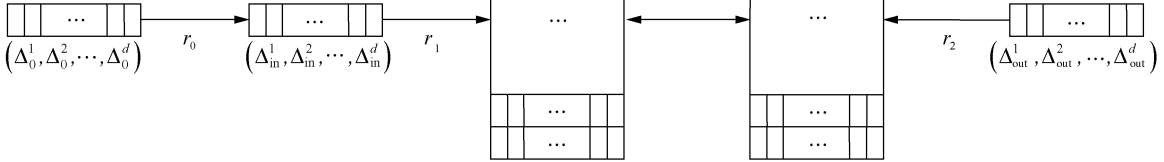


图 2 差分枚举在 LowMC 算法上的应用

Figure 2 Application of difference enumeration in LowMC

$$r_0 = \left\lceil \frac{n - lbd}{3m} \right\rceil \quad (3)$$

记该 r_0 为理论关键起始轮数。当关键起始轮数取到上述值的时候，可以最大化攻击轮数。但是，Rechberger 等的攻击是在理想线性层的假设下进行的，LowMC 实例在差分枚举攻击下的效果仍然未知。下文将通过研究关键起始轮数在实际的线性层下是否可以达到理论值来考察差分枚举攻击对 LowMC 算法的真实攻击效果。

3 差分枚举攻击对线性层实例化后的 LowMC 算法的攻击效果分析

在对 LowMC 算法实施差分枚举攻击时，部分非线性层的特性导致攻击可以分为两部分，第一部分是概率为 1 的关键起始轮数，第二部分是具有差分概率的差分扩散轮数。为了保证可攻击的轮数最大，或者以最小的时间复杂度攻击全轮数，关键起始轮数一定要取到最大值。线性层作为提供扩散性的组件，不仅影响密码算法实现效率，也影响密码算法安全性^[16]。在具体线性层下，实际的关键起始轮数有可能无法达到理论值，因此造成差分枚举攻击达不到理论的攻击轮数。对于某些参数下的 LowMC 算法实例，甚至会攻击失败。

3.1 差分枚举攻击在特定线性层下的关键起始轮数

在 LowMC 的算法中，线性层、轮常数加和密钥生成算法中的矩阵都是随机生成的，对于随机生成的线性矩阵，使用式(3)可以计算理论关键起始轮数。然而，对于 LowMC 算法的某些实例，

差分枚举攻击的实际关键起始轮数可能达不到关键起始轮数的理论值。将初始实际关键起始轮数 r_0 的值设置为理论关键起始轮数，通过以下步骤可以得到最终实际关键起始轮数。

步骤 1 根据 LowMC 算法描述，通过初始化解得到 r_0 轮线性层矩阵，并构建线性方程组。构建的线性方程组要满足两个条件：一是满足每一轮的输入和输出状态之间的线性关系；二是 r_0 轮中所有经过 S 盒的差分比特都为 0，以此保证差分传播概率为 1，于是构造出未知数个数为 $n(r_0 + 1)$ 个、方程数为 $nr_0 + 3mr_0$ 个的线性方程组。

步骤 2 利用高斯消元法求解线性方程组，并对自由变量进行遍历，得到符合条件的非零差分路线。

步骤 3 差分路线的个数若不小于差分枚举攻击所选取的维度 d ，则轮数可以达到 r_0 ，否则不可达到。

步骤 4 若由步骤 3 判断出不可达到 r_0 ，则 r_0 减 1，重复上述步骤 1~步骤 3 并进行判断；若由步骤 3 判断出可达到，则 r_0 加 1，重复上述步骤 1~步骤 3 并进行判断。最终得到 d 差分下实际可达到的最大 r_0 值。

下面对 LowMC 算法的实际关键起始轮数进行分析。以分组长度 128 bit、密钥长度 256 bit、每轮 1 个 S 盒、可允许数据复杂度为 16 个明文作为 LowMC 算法的可变参数为例，分析过程如下。差分维度 d 取 4，根据步骤 1~步骤 4 提出的获得实际关键起始轮数方法，利用式(3)计算得到相应参数的理论关键起始轮数的值为 42 轮。根据步骤 1，

可构建一个未知数为 5 504 个、方程数为 5 502 个的线性方程组。根据步骤 2, 利用高斯消元法求解线性方程组, 得到至少 2 个自由变量, 由此遍历至少 2^2 个自由变量的差分, 可以得到至少 3 条非零差分路线。将得到具体的非零差分路线数量和差分枚举攻击所选取的差分维度 4 进行比较, 当非零差分路线为 3 条时, 不可达到 42 轮的关键起始轮数, 当非零差分路线大于等于 4 条时, 可达到 42 轮的关键起始轮数。对是否可达到当前设置的关键起始轮数进行判断后, 根据步骤 4 进一步得到实际关键起始轮数。若当前关键起始轮数不可达到 42 轮, 则减小 r_0 的值, 将 r_0 取为 41 轮, 重复步骤 1~步骤 3, 判断是否可达到 r_0 , 若仍不可达到 r_0 , 继续减小 r_0 的值进行判断, 直到得到可达到的 r_0 值, 那么该 r_0 为实际关键起始轮数; 同样, 若当前关键起始轮数可达到 42 轮, 则增大 r_0 的值, 将 r_0 取为 43 轮, 重复步骤 1~步骤 3, 判断是否可达到 r_0 , 直到得到不可到达的 r_0 值, 那么 $r_0 - 1$ 为实际关键起始轮数。接下来, 根据真实线性层分析上述参数下 LowMC 实例的关键起始轮数的规律和线性层特性。

实例 1 Grain 算法中的 LFSR 作为自收缩发生器生成线性层。

以 Grain 算法中 LFSR 作为自收缩发生器生成的线性层矩阵, 对线性层矩阵进行分析。利用步骤 1~步骤 4 计算实际的关键起始轮数, 在 4 差分枚举攻击下, 实际关键起始轮数仅能达到 41 轮。在这种线性层矩阵的选择下, LowMC 算法的关键起始轮数无法达到理论值。可以选择减少 r_0 轮数或者减少差分路线维度 d 作为解决方法来解决这一问题, 通常情况下会选择适当减少 r_0 轮数, 这样对攻击轮数的影响比较小。如果减少了差分路线的维度 d , 会在差分枚举的过程中大幅减少可到达差分个数的上限, 进而缩短 r_1 和 r_2 。所以在 Grain 算法中 LFSR 作为随机矩阵生成器时, r_0 取 41 轮可以得到最大攻击轮数。

实例 2 2019 年欧密会提出的 LowMC 算法的线性层。

LowMC 算法为了减少乘法复杂度, 采用了部分非线性层的设计, 同时为了弥补部分非线性层带来的混淆不充分, 采用了高代数次数的随机

矩阵为线性层增强扩散度, 这给 LowMC 算法的实现带来了负担。Dinur 等^[13]在 2019 年欧密会上提出在每个 LowMC 实例等价类中存在线性等价性, 可以在每个实例类中得到一个最优线性层, 并伴随着加解密算法的优化。针对这种优化下的线性层, 本文进行了 4 差分下的关键起始轮数是否可达到理论值的判断, 结果是在 4 差分下不可达到理论的 42 轮关键起始轮数, 实际关键起始轮数为 41 轮。等价线性层在 4 差分下不可达到理论关键起始轮数的这一结果和对 Grain 算法中 LFSR 生成的线性层测试得到的结果一致。

实例 3 真随机数生成的 LowMC 算法线性层。

本文使用 C++ 语言中的 random_device 真随机数生成库, 验证随机生成的线性矩阵的实际关键起始轮数是否和其他特定选取算法下生成的线性矩阵的实际关键起始轮数相同。利用随机数生成器生成 20 000 组 LowMC 实例的 42 轮线性矩阵, 计算关键起始轮数可以达到 42 轮的差分路线个数, 实验结果见表 1。由表 1 可知, 使差分路线个数达到 7 条的线性矩阵有 4 416 组, 占总数的 22.08%; 使差分路线个数达到 15 条以上的线性矩阵有 233 组, 占总数的 1.17%; 剩余的线性矩阵使差分路线个数为 3 条, 占总数的 76.75%, 即随机选取线性矩阵只有 23.25% 的概率可达到 4 差分理论关键起始轮数 42 轮。

利用上述计算实际关键起始轮数的步骤 1~步骤 4, 可以计算实际关键起始轮数, 从而确定非零差分路线个数和实际关键起始轮数的联系。随机选取 3 000 次 LowMC 线性矩阵, 计算 4 差分下的最长关键起始轮数, 实验结果见表 2。实际关键起始轮数等于理论关键起始轮数的线性矩阵有 721 次, 概率为 24.03%, 所占比例与上面 7 条差分路线个数的比例基本相同; 不可达到理论关键起始轮数的线性矩阵有 2 277 次, 所占比例为 75.9%, 此外, 实际关键起始轮数大于理论关键起始轮数的线性矩阵有 2 次, 所占比例可忽略不计。由此, 可以认为在线性矩阵下, 实际关键起始轮数的差分路线个数为 7 条及以上时, 可攻击轮数与理论关键起始轮数相等; 小于 7 条时, 不可达到理论关键起始轮数。

综合考虑对上述随机数生成器生成的具体线

表 1 随机线性矩阵下的满足理论关键起始轮数的差分路线数量^{注 1}
Table 1 The number of differential trails satisfying key initial round in random linear matrices

矩阵组数	满足理论关键起始轮数的差分路线数量	满足理论关键起始轮数的矩阵所占比例
20 000	3 条	76.75%
20 000	7 条	22.08%
20 000	15 条及以上	1.17%

注 1: 线性矩阵由 random_device 库生成, 分组长度为 128 bit, 每轮 1 个 S 盒, 差分维度为 4, 理论关键起始轮数为 42 轮。

性矩阵测试, 可以认为在分组长度 128 bit、密钥长度 256 bit、每轮 1 个 S 盒、可允许数据复杂度为 16 个明文的参数下, 且攻击所用的 d 差分取为 4 差分时, 实际关键起始轮数可到达理论关键起始轮数的概率仅为 23.25%。

表 2 随机线性矩阵下的实际关键起始轮数^{注 1}
Table 2 Actual key initial rounds in random linear matrices

矩阵组数	实际可攻击轮数	所占比例
3 000	41 轮	75.9%
3 000	42 轮	24.03%
3 000	43 轮	0.07%

3.2 LowMC 算法轮数设置分析

为了确定保证 LowMC 算法安全性下的最低轮数, 对大部分标准攻击进行评估, 得到第二版建议轮数。

$$r \geq \max(r_{\text{stat}}, r_{\text{bmrg}}, r_{\text{deg}} + r_{\text{diff}}) + r_{\text{outer}} \quad (4)$$

其中, r_{stat} 代表统计方法攻击下的轮数, r_{bmrg} 代表飞去来器攻击可攻击轮数, r_{deg} 代表保证有足够代数次数需要的轮数, r_{diff} 代表完全扩散需要的轮数, r_{outer} 代表插值攻击轮数。

LowMC 算法的分组长度、密钥长度、每轮 S 盒数量等参数是可变的, 不同参数的加密算法特征和适用范围有所不同。特别地, 令每轮 S 盒数量和数据量都取较小值, 这种少量 S 盒、低数据量参数下的 LowMC 实例可用于非交互式零知识证明的公钥签名方案的加密算法。针对这种参数下的 LowMC 实例提出的差分枚举攻击影响了第三版轮数的计算。经过 LowMCv2 算法轮数和差分枚举攻击轮数计算, 由 Grain 算法的 LFSR 生成线性矩阵, 以 128 bit 分组长度、1 个 S 盒、差分维度取 4 为例, 得到理论上不可抵抗差分枚举攻击, 而实际可抵抗差分枚举攻击的参数见表 3。由此实例可见, 在实际的差分枚举攻击下, 差分枚举攻击可能会失败。为了抵抗差分枚举攻击, 第三版 LowMC 算法 (LowMCv3) 更改了轮数计算方法。LowMCv3 算法的轮数为差分攻击、线性攻击、飞去来器攻击、插值攻击、差分枚举攻击等一系列攻击的最大轮数。由上述分析结果可知, 在特定参数类型的部分 LowMC 实例下, 差分枚举攻击并不总是可以达到理论攻击轮数, 因此, 针对此类参数, LowMCv3 算法的轮数可以适当降低, 进一步提升实现效率。

表 3 理论与实际差分枚举攻击对比^{注 2}
Table 3 Comparison of theoretical and practical difference enumeration attacks

数据量	密钥长度/bit	LowMCv2 轮数	差分枚举理论可攻击轮数	差分枚举实际可攻击轮数
2^4	168, 169	158	158	157
2^5	168, 169	158	158	157
2^6	168, 169	158	158	157
2^7	168, 169	158	158	157
2^{12}	179	166	166	165
2^{13}	179, 180, 181	166	166	165
2^{14}	179, 180, 181	166	166	165
2^{15}	179, 180	166	166	165

注 2: 线性矩阵由 Grain 算法的 LFSR 生成, 分组长度为 128 bit, 1 个 S 盒, 差分维度为 4。

4 结束语

本文主要对少量 S 盒、低数据量参数下的 LowMC 实例的差分枚举攻击效果进行分析, 利用高斯消元法对加密过程中构建的线性方程组进行求解, 得到差分枚举攻击的实际关键起始轮数。实验结果表明, 对于某些 LowMC 算法实例, 实际关键起始轮数往往小于其理论值。实际和理论的关键起始轮数的差异导致差分枚举攻击的实际攻击效果达不到预期, 通过改变 LowMC 算法的线性层, 可以得到多个 LowMC 算法的实例。这些实例中, 仅有 23.25% 的实例可以被差分枚举攻击成功攻破。对于剩余的 LowMC 实例, 差分枚举攻击必须通过减少差分维度或关键起始轮数来保证攻击可行性。由于 LowMCv3 部分实例的轮数主要考虑了差分枚举攻击的效果, 这部分 LowMCv3 算法的实例可以适当减少轮数以提升实现效率。

参考文献:

- [1] ALBRECHT M R, RECHBERGER C, SCHNEIDER T, et al. Ciphers for MPC and FHE[C]//EUROCRYPT. 2015: 430-454.
- [2] DINUR I, LIU Y W, MEIER W, et al. Optimized interpolation attacks on LowMC[C]//ASIACRYPT. 2015: 535-560.
- [3] DOBRAUNIG C, EICHLSEDER M, MENDEL F. Higher-order cryptanalysis of LowMC[C]//ICISC. 2015: 87-101.
- [4] CHASE M, DERLER D, GOLDFEDER S, et al. Post-quantum zero-knowledge and signatures from symmetric-key primitives[C]//ACM Conference on Computer and Communications Security. 2017.
- [5] RECHBERGER C, SOLEIMANY H, TIESSEN T. Cryptanalysis of low-data instances of full LowMCv2[C]//IACR Trans Symmetric Cryptol. 2018: 163-181.
- [6] DEMIRCI H, SELÇUK A A. A meet-in-the-middle attack on 8-round AES[C]//FSE. 2008: 116-126.
- [7] DUNKELMAN O, KELLER N, SHAMIR A. Improved single-key attacks on 8-round AES-192 and AES-256[C]//ASIACRYPT. 2010: 158-176.
- [8] 陈少真, 鲁林真. 对 8 轮 ARIA 算法的差分枚举攻击[J]. 电子与信息学报, 2011, 33(7): 1770-1774.
CHEN S Z, LU L Z. Differential enumeration attack on ARIA[J]. Journal of Electronics and Information Technology, 2011, 33(7): 1770-1774.
- [9] 崔竞一. 基于中间相遇思想的攻击方法研究[D]. 郑州: 信息工程大学, 2017.
CUI J Y. Research on cryptanalysis based on meet-in-the-middle[D]. Zhengzhou: Information Engineering University, 2017.
- [10] 王萼芳, 石明生. 高等代数(第三版)[M]. 北京: 高等教育出版社, 2003.
WANG E F, SHI M S. Advanced algebra (third edition)[M]. Beijing:

Higher Education Press, 2003.

- [11] HELL M, OHANSSON T, MAXIMOV A, et al. The grain family of stream ciphers[J]. The eSTREAM Finalists, 2008: 179-190.
- [12] MEIER W, STAFFELBACH O. The self-shrinking generator[C]//EUROCRYPT. 1994: 205-214.
- [13] DINUR I, KALES D, PROMITZER A, et al. Linear equivalence of block ciphers with partial non-linear layers: application to LowMC[C]//EUROCRYPT. 2019: 343-372.
- [14] TIESSEN T. Polytopic cryptanalysis[C]//EUROCRYPT. 2016: 214-239.
- [15] NYBERG K. Differentially uniform mappings for cryptography[C]//EUROCRYPT. 1993: 55-64.
- [16] 李鹏飞. 基于密码结构的扩散层构造[J]. 网络与信息安全学报, 2017, 3(6): 65-76.
LI P F. Construction of diffusion layers based on cipher structures[J]. Chinese Journal of Network and Information Security, 2017, 3(6): 65-76.

[作者简介]



葛欣欣(1997-), 女, 吉林四平人, 山东大学硕士生, 主要研究方向为分组密码分析。



李智虎(1975-), 男, 安徽望江人, 中国电力科学研究院有限公司高级工程师, 主要研究方向为密码理论和密码工程。



王美琴(1974-), 女, 宁夏银川人, 山东大学教授、博士生导师, 主要研究方向为对称密码算法的设计和分析。



胡凯(1992-), 男, 山东临沂人, 山东大学博士生, 主要研究方向为对称密码的分析。