立方攻击：

区分器:

8-round Keccak[r=1152,c=448] 复杂度2^122

[S. Huang, X. Wang, G. Xu, M. Wang and J. Zhao, New Distinguisher on Reduced-Round Keccak Sponge Function, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 2019]

恢复密钥:

1. round Keccak[r=576,1024] 复杂度2^40

7-round Keccak[r,c] c=256,512,768 复杂度2^71

[F. Liu, Z. Cao and G. Wang, Finding Ordinary Cube Variables for Keccak-MAC with Greedy Algorithm, IWSEC, 2019]

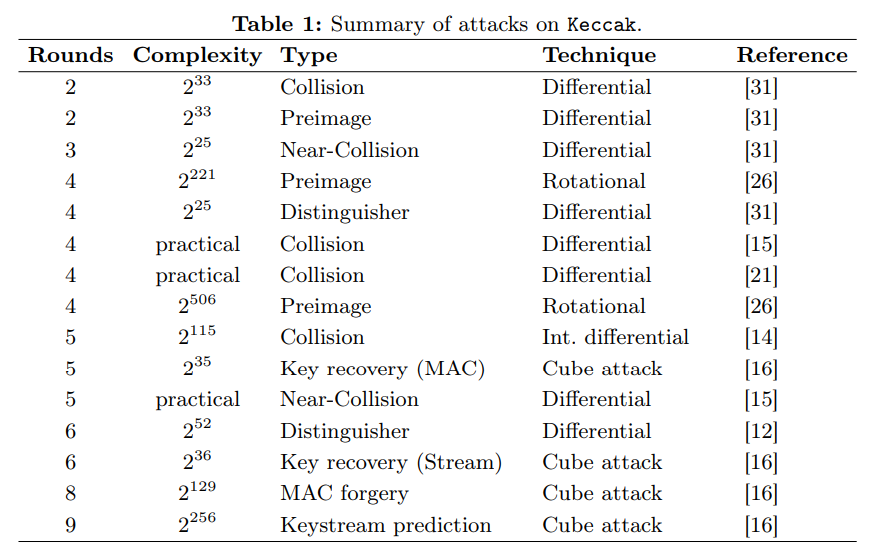
SymSum[Symmetric-Sum]：

区分器:

9-round 复杂度2^511

[D. Saha, S. Kuila and D. R. Chowdhury, SymSum: Symmetric-Sum Distinguishers Against Round Reduced SHA3, IACR Trans. Symmetric Cryptol., 2017]

碰撞攻击和原像攻击：



表格来自[J. Jean and I. Nikolić, Internal Differential Boomerangs: Practical Analysis of the Round-Reduced Keccak-f Permutation, Fast Software Encryption, 2015]

keccak-f[1600]置换：

零和区分器(根据可分性质提出)：

23-round：复杂度2^1546

24-round：复杂度2^1573

[H. Yan, X. Lai, L. Wang, Y. Yu and Y. Xing, New zero-sum distinguishers on full 24-round Keccak-f using the division property, IET Inf. Secur., 2019]

差分分析：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rounds | b=200 | b=400 | b=800 | b=1600 |
| 1 | 2 | 2 | 2 | 2 |
| 2 | 8 | 8 | 8 | 8 |
| 3 | 20 | 24 | 32 | 32 |
| 4 | 46 | [56,63] | [56,104] | [56,134] |
| 5 | [58,89] | [58,147] | [58,247] | [58,372] |
| 6 | [108,142] | [108,278] | [108,556] | [108,1112] |

最优重量的下界是理论下界，上界是最低的已知重量

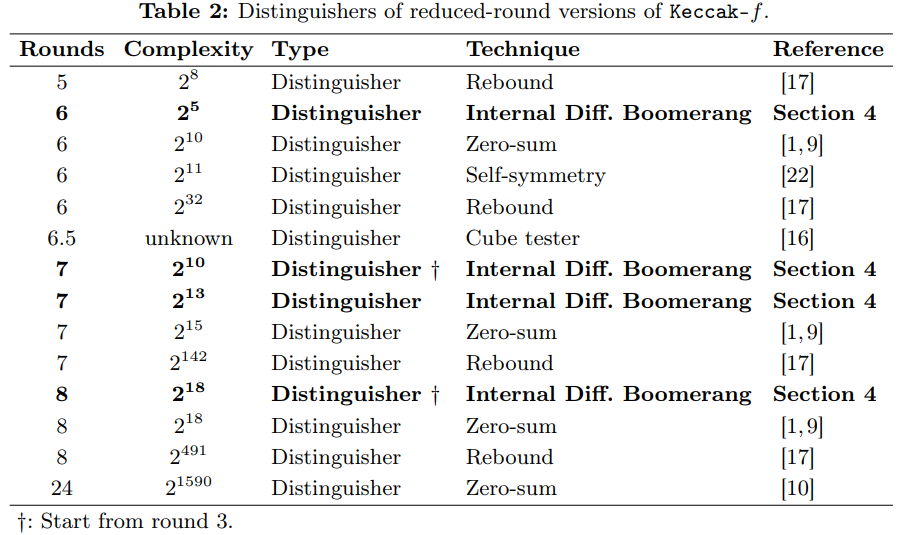
理论下界[G. Liu, W. Qiu and Y. Tu, New Techniques for Searching Differential Trails in Keccak, IACR Trans. Symmetric Cryptol., 2019]

线性分析：b=1600

|  |  |
| --- | --- |
| Round | 最优重量 |
| 1 | 2 |
| 2 | 8 |
| 3 | 13 |
| 4 | 49 |

[C. Dobraunig, M. Eichlseder and F. Mendel, Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates, Asiacrypt, 2015]

Rebound，Boomerang，Self-symmetry：



表格来自[J. Jean and I. Nikolić, Internal Differential Boomerangs: Practical Analysis of the Round-Reduced Keccak-f Permutation, Fast Software Encryption, 2015]

Xoodoo置换[Xoodyak底层置换]：

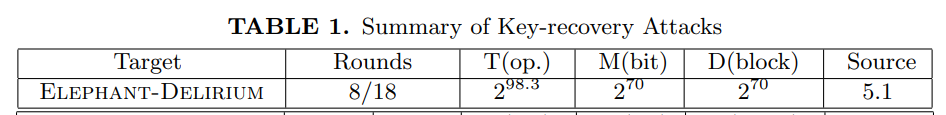
1. round 零和区分器 复杂度2^33
2. Liu, T. Isobe, W. Meier and Z. Yang, Algebraic Attacks on Round-Reduced Keccak/Xoodoo, IACR Cryptol. ePrint Arch., 2020]

6-round 条件立方攻击(Xoodyak) 复杂度 2^43.8

[H. Zhou, Z. Li, X. Dong, K. Jia and W. Meier, Practical Key-recovery Attacks on Round-Reduced Ketje Jr, Xoodoo-AE and Xoodyak, Comput. J., 2020]

Elephant-Delirium：

插值：



[H. Zhou, R. Zong, X. Dong, K. Jia and W. Meier, Interpolation Attacks on Round-Reduced Elephant, Kravatte and Xoofff, IACR Cryptol. ePrint Arch., 2020]