|  |  |  |  |
| --- | --- | --- | --- |
| Cipher | Rounds | Method | Ref |
| SIMON32/64 | 23 | Linear | [1]&[6]&[11] |
| 22 | DIfferential | [10] |
| **24** | Linear | [11] |
| **24** | Ours (4+14+4+2) | Trail from [7] |
| SIMON48/96 | **25** | Linear | [1]&[6] |
| 24 | DIfferential | [2]&[3]&[10] |
| **25** | Ours (4+15+4+2) | Ours (By CryptoSMT) |
| SIMON64/128 | **32** | Linear | [6] |
| 31 | DIfferential | [3] |
| **32** | Ours (4+22+4+2) | Ours (By CryptoSMT) |
| SIMON128/256 | **56** | Linear | [4] |
| 51 | DIfferential | [3] |
| 54 | Our(4+44+5+1) | Trail from [9] |

[1] Chen H, Wang X. Improved linear hull attack on round-reduced Simon with dynamic key-guessing techniques[C]//Fast Software Encryption: 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers 23. Springer Berlin Heidelberg, 2016: 428-449.

[2] Wang N, Wang X, Jia K, et al. Differential attacks on reduced SIMON versions with dynamic key-guessing techniques[J]. Science China Information Sciences, 2018, 61: 1-3.

[3] Leurent G, Pernot C, Schrottenloher A. Clustering effect in Simon and Simeck[C]//Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part I 27. Springer International Publishing, 2021: 272-302.

[4] Ashur T. Improved linear trails for the block cipher simon[J]. Cryptology ePrint Archive, 2015.

[5] Zhang Y, Lyu L, Qiao K, et al. Automatic key recovery of feistel ciphers: application to SIMON and SIMECK[C]//Information Security Practice and Experience: 16th International Conference, ISPEC 2021, Nanjing, China, December 17–19, 2021, Proceedings 16. Springer International Publishing, 2021: 147-167.

[6] Kölbl S, Leander G, Tiessen T. Observations on the SIMON block cipher family[C]//Advances in Cryptology--CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I 35. Springer Berlin Heidelberg, 2015: 161-185.

[7] Liu Z, Li Y, Wang M. Optimal differential trails in SIMON-like ciphers[J]. Cryptology ePrint Archive, 2017.

[8] 牛开路, 晁佳豪, 王薇. 动态聚集效应及其在 SIMON 算法上的应用[J]. Journal of Cryptologic Research, 2023, 10(4): 737.

[9] Qiao K, Hu L, Sun S. Differential analysis on simeck and simon with dynamic key-guessing techniques[C]//Information Systems Security and Privacy: Second International Conference, ICISSP 2016, Rome, Italy, February 19-21, 2016, Revised Selected Papers 2. Springer International Publishing, 2017: 64-85.

[10] Abdelraheem M A, Alizadeh J, Alkhzaimi H A, et al. Improved linear cryptanalysis of reduced-round SIMON-32 and SIMON-48[C]//Progress in Cryptology--INDOCRYPT 2015: 16th International Conference on Cryptology in India, Bangalore, India, December 6-9, 2015, Proceedings 16. Springer International Publishing, 2015: 153-179.