Clustering differential trails in Algebraic-Oriented primitives

Two guys from AOdromeda

February 2025

1 Introduction

Many algebraic hash functions argue for statistical security from the fact that any differential trail would pass a certain number of nonlinear components and thus have a low "probability". However, little is known about the possible clustering of such differential trails into differentials or truncated differentials.

In this project, we will study:

- Clustering of trails into differentials in AO primitives. We will attempt to quantify or give bounds on the probability of the differentials.
- Truncated differentials in AO primitives.
- Check if maliciously designed primitives (e.g. carefully crafted round constants) can experience a high level of trail clustering or strong truncated differentials. This might also be related to embedding large invariant subspaces.

1.1 Scope

If time permits, we will focus on (higher priority listed first):

1. Poseidon [Gra+21] and closely related primitives including Neptune [Gra+22] and HadesMiMC [Gra+20].
2. Other primitives based on low degree permutation include (Feistel) MiMC [Alb+16] and GMiMC [Alb+19].
3. Other AO primitives.

1.2 Related works

In [Bey+20; KR21; GRS21], it is shown that a poorly designed linear layer can lead to truncated differential or subspace trails of probability one that survive an infinite number of partial rounds of HadesMiMC instantiations. On the other

hand, a good choice of the linear layer can improve resistance against statistical attacks, which implies that one may reduce the number of full rounds for better efficiency.

[Bey+20] also makes progress on differential attacks against GMiMC-erf. A better differential (compared to the GMiMC designers) was found which leads to a much more efficient distinguisher. In addition, an impossible differential attack that covers more rounds is also introduced. The attack is further improved by a few rounds in [Che+23].

[BL22] improves truncated differential attacks against contracting Feistel ciphers, leading to a distinguisher for GMiMC-crf.

[BCP23] studies propagation of subspaces in primitives with monomial Sboxes applied to Rescue and variants of AES. They show that traditional design principles might not be sufficient in the algebraic setting.

2 Time planning and deliverables

The expected time planning for the project is given in Table 1.

Unit task	**Expected duration**
1. Literature study, identification of target primitives or related toy hash/ciphers	1 month
2. Study of clustering of trails into differentials in AO using Matsui search or similar tools	1 month
3. Study of truncated trails	1 month
4. Study of potential malicious designs	1 month
Total:	4 months

Table 1: Project time planning.

2.1 Deliverables

A written report on the findings, which ideally can lead to a research paper for FSE/ToSC or other relevant venues.

References

[Alb+16] Martin R. Albrecht et al. "MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity". In: *IACR Cryptol. ePrint Arch.* 2016 (2016), p. 492.

[Alb+19] Martin R Albrecht et al. "Feistel structures for MPC, and more". In: *Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part II 24*. Springer. 2019, pp. 151–171.

[BCP23] Aurélien Boeuf, Anne Canteaut, and Léo Perrin. "Propagation of Subspaces in Primitives with Monomial Sboxes: Applications to Rescue and Variants of the AES". In: *IACR Trans. Symmetric Cryptol.* 2023 (2023), pp. 270–298. URL: https://api.semanticscholar.org/CorpusID:266268160.

[Bey+20] Tim Beyne et al. "Out of oddity–new cryptanalytic techniques against symmetric primitives optimized for integrity proof systems". In: *Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part III 40*. Springer. 2020, pp. 299–328.

[BL22] Tim Beyne and Yunwen Liu. "Truncated Differential Attacks on Contracting Feistel Ciphers". In: *IACR Trans. Symmetric Cryptol.* 2022.2 (2022), pp. 141–160. DOI: 10.46586/TOSC.V2022.I2.141-160. URL: https://doi.org/10.46586/tosc.v2022.i2.141-160.

[Che+23] Shiyao Chen et al. "Towards the Links of Cryptanalytic Methods on MPC/FHE/ZK-Friendly Symmetric-Key Primitives". In: *IACR Trans. Symmetric Cryptol.* 2023.2 (2023), pp. 132–175. DOI: 10.46586/TOSC.V2023.I2.132-175. URL: https://doi.org/10.46586/tosc.v2023.i2.132-175.

[Gra+20] Lorenzo Grassi et al. "On a generalization of substitution-permutation networks: The HADES design strategy". In: *Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30*. Springer. 2020, pp. 674–704.

[Gra+21] Lorenzo Grassi et al. "Poseidon: A new hash function for {Zero-Knowledge} proof systems". In: *30th USENIX Security Symposium (USENIX Security 21)*. 2021, pp. 519–535.

[Gra+22] Lorenzo Grassi et al. "Invertible quadratic non-linear layers for MPC-/FHE-/ZK-friendly schemes over Fnp: application to Poseidon". In: *IACR Transactions on Symmetric Cryptology* (2022), pp. 20–72.

[GRS21] Lorenzo Grassi, Christian Rechberger, and Markus Schofnegger. "Proving resistance against infinitely long subspace trails: How to choose the linear layer". In: *IACR Transactions on Symmetric Cryptology* (2021), pp. 314–352.

[KR21] Nathan Keller and Asaf Rosemarin. "Mind the middle layer: the HADES design strategy revisited". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2021, pp. 35–63.