Degrees of Freedom in Algebraic Attacks on Arithmetization-Oriented Primitives

M2 internship proposal

General information

Location: University of Limoges (Limoges, France)

Team: Cryptis Team, XLIM

Advisor: Pierre Briaud

Duration: 5-6 months

A visit to Simula UiB (Bergen, Norway) is scheduled at the beginning of the internship.

Context

Arithmetization-oriented (AO) primitives encompass a variety of symmetric schemes tailored to advanced cryptographic applications such as secure multiparty computation (MPC) and zero-knowledge (ZK) proofs. The goal is to replace traditional schemes such as AES or SHA-3, which are optimized for conventional hardware, with constructions better suited to the arithmetic computations underlying these applications. To this end, AO designs often rely on simple polynomial structures with low algebraic degree and multiplicative complexity.

At the same time, these features make AO primitives particularly amenable to **algebraic attacks**, which have even been shown to outperform traditional symmetric cryptanalysis in several settings, for instance on several **ZK-friendly permutations**. The tools and techniques used in these attacks, particularly those based on **Gröbner bases**, have long been studied in public-key cryptanalysis, but their application to the AO setting has required significantly revisiting them, leading to new developments.

A first development concerns **solving algorithms for zero-dimensional systems**. While computing an initial Gröbner basis is typically the bottleneck in public-key cryptanalysis, recent work has shown that this is not the case for several AO primitives [5, 2]. This observation has renewed cryptanalytic interest in change-of-order algorithms and, more generally, in methods based on multiplication matrices for obtaining a univariate polynomial. Toward the same goal, elimination approaches using resultants have also been proposed [15, 4, 3].

A complementary development is to **simplify the system given as input to these algorithms**. The point is that the algebraic modeling often leaves degrees of freedom that can be exploited to reduce the number of variables or the degrees of the equations. One early approach in this direction is "**round skipping**" [6], which consists in choosing suitable families of intermediate states to bypass the algebraic complexity of certain rounds. More recently, several extensions of round skipping have been proposed in the context of the Poseidon hash function [11, 12, 13, 14, 7]. While these extensions differ in their specific constructions, they share the idea of carefully choosing constraints and parametrizations of intermediate states to obtain simpler polynomial systems.

Objectives of the internship

Our general goal is to improve algebraic attacks on ZK-friendly permutations by focusing on this second direction, namely, better exploiting the implicit degrees of freedom in their algebraic modelings.

From Poseidon to other primitives. Our starting point will be to investigate whether the extensions of round skipping devised for Poseidon can be applied/adapted to other ZK-friendly permutations. To facilitate the study, we will focus on one particularly promising extension [12]. As for the target primitives, we plan to start with the Griffin permutation [10] and, time permitting, move on to other constructions, such as Anemoi [8], Arion [9], or XHash [1].

More solid grounds for round skips. A longer-term goal is to analyze round-skipping techniques other than [12] and ultimately develop a unified theory of this class of attacks. While this work will likely extend beyond the internship period, we hope that our attempts to adapt these attacks to other ZK-friendly permutations will already help us better distinguish general principles from more primitive-specific considerations.

Student profile

We are looking for an M2 student in cryptography, mathematics, or theoretical computer science, preferably with basic knowledge of symmetric cryptography and algebraic cryptanalysis, as well as good programming skills (Python/SageMath; C is a plus). We also particularly welcome students whose interests lie more in effective algebraic geometry or computer algebra than in cryptography itself.

To apply

Please send a CV, transcripts from the last two years, and details of any prior internships to

pierre.briaud@xlim.fr

References

[1] Ashur, T., Bhati, A.S., Kindi, A., Mahzoun, M., Perrin, L., Tariq, S.: The XHash family for ZK-friendly hash functions. Designs, Codes and Cryptography **94**(6), 132 (2026)

[2] Bak, A., Bariant, A., Boeuf, A., Briaud, P., Øygarden, M., Phanse, A.: The Algebraic CheapLunch: Extending FreeLunch Attacks on Arithmetization-Oriented Primitives Beyond CICO-1. Cryptology ePrint Archive, Paper 2025/2040 (2025)

[3] Bak, A., Bariant, A., Hostettler, M., Neiger, V.: Resultants Meet Resultant: Improving CICO-1 and CICO-2 Attacks on ZK-Friendly Permutations. Cryptology ePrint Archive, Paper 2026/1281 (2026)

[4] Bariant, A., Boeuf, A., Briaud, P., Hostettler, M., Øygarden, M., Raddum, H.: Improved Resultant Attack Against Arithmetization-Oriented Primitives. In: Annual International Cryptology Conference (Crypto). pp. 335–367. Springer (2025)

[5] Bariant, A., Boeuf, A., Lemoine, A., Manterola Ayala, I., Øygarden, M., Perrin, L., Raddum, H.: The Algebraic FreeLunch: Efficient Gröbner Basis Attacks Against Arithmetization-Oriented Primitives. In: Annual International Cryptology Conference (Crypto). pp. 139–173. Springer (2024)

[6] Bariant, A., Bouvier, C., Leurent, G., Perrin, L.: Algebraic Attacks against Some Arithmetization-Oriented Primitives. IACR Transactions on Symmetric Cryptology **2022**(3), 73–101 (Sep 2022)

[7] Bhati, A.S., Tariq, S., Ashur, T.: From Round Skipping to S-Box Skipping: Attacking Poseidon's Partial Layer via Subspace Restriction. Cryptology ePrint Archive, Paper 2026/1692 (2026)

[8] Bouvier, C., Briaud, P., Chaidos, P., Perrin, L., Salen, R., Velichkov, V., Willems, D.: New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode. In: Annual International Cryptology Conference (Crypto). pp. 507–539. Springer (2023)

[9] Campa, L., Roy, A., Steiner, M., Trevisani, S.: Arion: Arithmetization-Oriented Hashing for Zero-Knowledge Proof Systems. IACR Transactions on Symmetric Cryptology **2026**(3) (2026)

[10] Grassi, L., Hao, Y., Rechberger, C., Schofnegger, M., Walch, R., Wang, Q.: Horst meets fluid-SPN: Griffin for zero-knowledge applications. In: Annual international cryptology conference. pp. 573–606. Springer (2023)

[11] Grassi, L., Koschatko, K., Rechberger, C.: Poseidon and Neptune: Gröbner Basis Cryptanalysis Exploiting Subspace Trails. IACR Transactions on Symmetric Cryptology **2025**(2), 34–86 (Jun 2025)

[12] Merz, S.P., García, A.R.: Skipping Class: Algebraic Attacks exploiting weak matrices and operation modes of Poseidon2(b). Cryptology ePrint Archive, Paper 2026/306 (2026)

[13] Sanso, A., Vitto, G.: Top Gun: Degree Annihilation Attacks on Poseidon. Cryptology ePrint Archive, Paper 2026/1254 (2026)

[14] Vitto, G.: Slipway: Accessing Finite Subspace Trails in Poseidon. Cryptology ePrint Archive, Paper 2026/1579 (2026)

[15] Yang, H.S., Zheng, Q.X., Yang, J., Liu, Q.F., Tang, D.: A New Security Evaluation Method Based on Resultant for Arithmetic-Oriented Algorithms. In: International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt). pp. 457–489. Springer (2024)