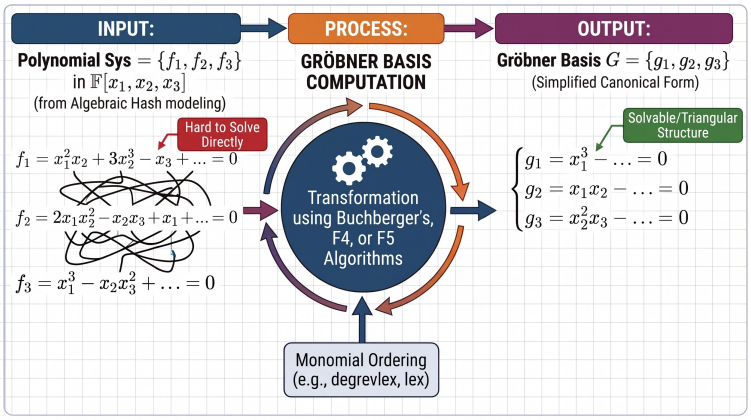
The Impact of Algebraic Modelling Strategies on Gröbner Bases Computation



Algebraic hash functions (such as Poseidon or Rescue) are modern cryptographic primitives built using simple, low-degree polynomials over finite fields, making them highly efficient for Zero-Knowledge Proofs (ZKPs). To evaluate their security against preimage or collision-based attacks, researchers translate the hash mapping into a multivariate polynomial system and attempt to solve it using Gröbner bases.

However, the computational feasibility of this attack depends entirely on how the equations are mathematically modelled. This thesis focuses exclusively on resolving the core *degree versus variable* trade-off in algebraic modelling. When building the multivariate polynomial ideal, one must choose between composing the hash rounds into a single dense equation (yielding very few variables but exponentially high polynomial degrees) or introducing intermediate variables for each round (maintaining low degrees but creating a massive system of equations).

The objective of this project is to systematically benchmark how these two competing representations dictate the execution time and peak memory usage of Gröbner basis algorithms. By analyzing this specific trade-off on a reduced-round algebraic hash function, the thesis will identify the optimal equation structure for practical algebraic cryptanalysis.

Theoretical Framework and Student Profile. This research relies heavily on abstract algebra, specifically the theory of rings, finite fields, and Gröbner bases. The ideal candidate should have a combined background in Mathematics and Engineering to effectively bridge advanced algebraic theory with computational performance benchmarking.

Practicalities

Promotor:	Prof. Dr. Ir. Vincent Rijmen		
Daily supervisor:	Sundas Tariq	sundas.tariq@esat.kuleuven.be	office B01.34
	Dr. Amit Singh Bhati	amitsingh.bhati@3milabs.tech	office B01.17

Nature of the work:	20% literature, 30% theoretical work, 50% software
Number of students:	1 or 2