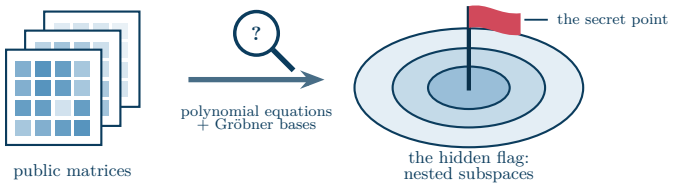
Capture the Flag: Algebraic Attacks on Multi-Party DPFs



an attacker sees only the matrices on the left and must find the flag on the right

A distributed point function (DPF) splits a function that is zero everywhere except at one secret point into keys for several parties. Each key alone reveals nothing, yet the parties can evaluate their keys locally and add up the results to obtain the function value. DPFs are a workhorse of private information retrieval, private statistics, and the preprocessing of multi-party computation (MPC). For two parties the key size is tiny (logarithmic in the domain size); for three or more parties, all constructions from standard assumptions have keys that grow with a root of the domain size.

A recent construction [1] escapes this barrier with an elegant algebraic idea: the secret point is encoded in public matrices that respect a hidden chain of nested subspaces, a so-called *flag*. Security rests on a new assumption: in essence, that nobody can recover that flag from the public matrices. Part of the confidence in it comes from the arithmetic: the scheme works modulo a large composite number whose factorization is secret, as in RSA, so an attacker who gets close still faces a factoring problem. Over a prime modulus, that safety net is gone — and a prime is exactly what would shrink the key size by an order of magnitude and make the scheme usable in the preprocessing above. So how hard is it for an attacker to capture the flag?

The goal of this thesis is to answer this question experimentally. You will (i) study DPFs and the construction of [1] and state the flag-recovery problem precisely; (ii) generate instances with a planted flag (e.g., in SageMath) and turn flag recovery into polynomial equations, borrowing modellings from MinRank cryptanalysis [2]; and (iii) solve small instances with Gröbner-basis tools such as msolve, measuring how time, memory and solving degree grow, in order to extrapolate safe parameters. Ambitious students can hunt for shortcuts: better modellings, or attacks that use the extra public information of the real scheme.

The topic suits a student who enjoys linear algebra and experiments; no prior knowledge of Gröbner bases is required. More information can be found by contacting Feiyang Qiu (email below).

[1] T. Krips and P. Pullonen-Raudvere, "Multi-party distributed point functions with polylogarithmic key size from invariants of matrices," Cryptology ePrint Archive, Paper 2025/978, 2025.

[2] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J.-P. Tillich, and J. Verbel, "Improvements of algebraic attacks for solving the rank decoding and MinRank problems," in *Advances in Cryptology – ASIACRYPT 2020*, Springer, 2020, pp. 507–536.

Practicalities

Promotor:	Bart Preneel
Daily supervisor:	Feiyang Qiu feiyang.qiu@esat.kuleuven.be office B01.34
Nature of the work:	20% literature, 40% theoretical work, 40% software/experiments
Number of students:	1