GPU-Accelerated Cube Attack in Prime Fields

Extending the Kite Framework to target Arithmetization-Oriented Ciphers

Gaetano Bruno

May 10, 2026

Roma Tre University

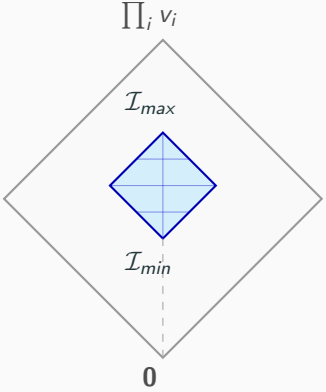
Topological Search via the "Kite" Framework

Problem: Cube attack has complexity $\mathcal{O}(p^d)$.

The Kite-Attack framework[1] proposes a **massively parallel, deterministic topological search**.

- $\mathcal{I}_{min}$: floor of the search space, $|\mathcal{I}_{min}| = \beta$.
- $\mathcal{I}_{max}$: ceiling of the search space, $|\mathcal{I}_{max}| = \alpha$.
- $\mathcal{I}_{free} := \mathcal{I}_{max} \setminus \mathcal{I}_{min}$ free variables set.

$$\mathcal{N}_{\text{config}} = 3^{\alpha-\beta}$$



[1] M. Bernaschi et al., *Kite attack: reshaping the cube attack for a flexible GPU-based maxterm search*, Journal of Cryptographic Engineering, 2019.

GPU Architecture

Kernel 1: Foundational Tensor Generation

To avoid evaluating the cipher $3^{\alpha-\beta}$ times from scratch, we precompute base cube sums over $\mathcal{I}_{min}$[2]. Hardware mapping:

$$1 \text{ Boolean Mask in } \mathcal{I}_{free} \iff 1 \text{ GPU Warp}$$

Kernel 2: Cube Reconstruction & Affine Testing

Cubes of dimension $d \in \{\beta, \ldots, \alpha\}$ are reconstructed from the foundational tensor. An in-register affine test is executed on the superpoly $q(\underline{k})$:

$$e = q(\underline{k}_a) + q(\underline{k}_b) + q(\underline{k}_c) - 2q(\underline{k}_0) - q(\underline{k}_a + \underline{k}_b + \underline{k}_c) \qquad (\text{mod } p)$$

Kernel 3: Formal Superpoly Extraction

The pipeline compute the superpoly coefficients and outputs the linear equation.

[2] A. Agnese, M.Pedicini, *Cube attack in finite fields of higher order*, Australian Computer Society, Inc., 2011.

Use case: small-pSquare

The Context: Prime-Field Masking & SCA

- Boolean masking fails to provide security in **low-noise regimes**.
- *small-pSquare* is a TBC that operates natively in $\mathbb{F}_p$ to enable prime-field masking.
- The non-linear function $x \mapsto x^2$ supports efficient gadgets.
- Total algebraic degree grows exponentially ($\geq 4^r/8$), r number of rounds.

- **Goal:** Search for "weak" monomials in the ANF and exploit them to isolate affine relations in the key elements.

Cryptanalytic Results

The topological search successfully penetrated up to Round 4 and cleanly isolated valid linear superpolys. This enabled the exact algebraic recovery of 3/16 secret key elements.

β	α	Maxterm	Superpoly
6	22	$x_0x_3x_4x_5x_7x_9x_{11}x_{14}t_0t_2t_3t_4$	$10k_2 + 9$
6	22	$x_0x_2x_3x_4x_5x_7x_9x_{11}x_{15}t_0t_2t_4$	$97k_3 + 89$
6	22	$x_0x_3x_4x_5x_7x_9x_{11}x_{14}t_0t_1t_3t_4$	$111k_1 + 124$

Cipher Instance:

- $\mathrm{Enc}_k : \mathbb{F}_{127}^{16} \mapsto \mathbb{F}_{127}^{16}$
- 16 plaintext (x_i), 16 tweak (t_i) variables

Compute Environment:

- **GPU:** NVIDIA A40 (46GB VRAM)

Thank You for Your Attention!