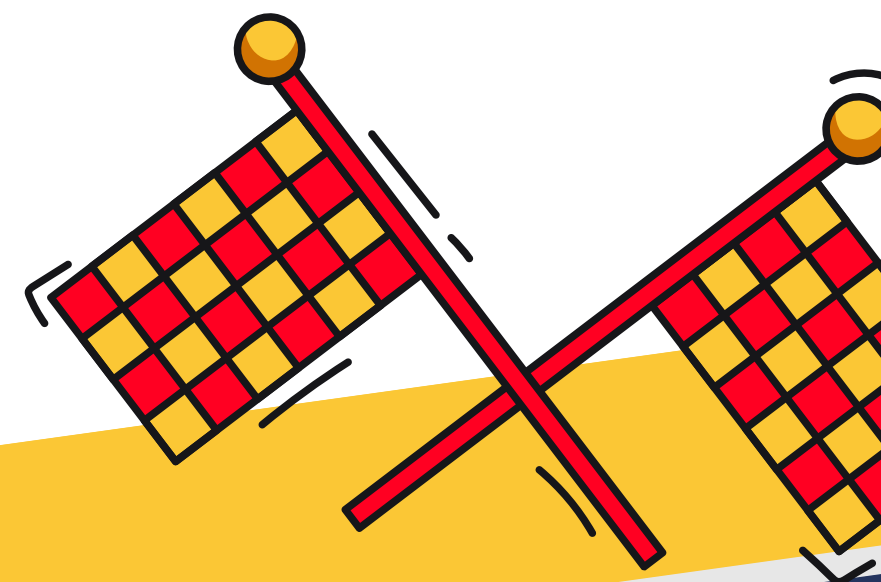
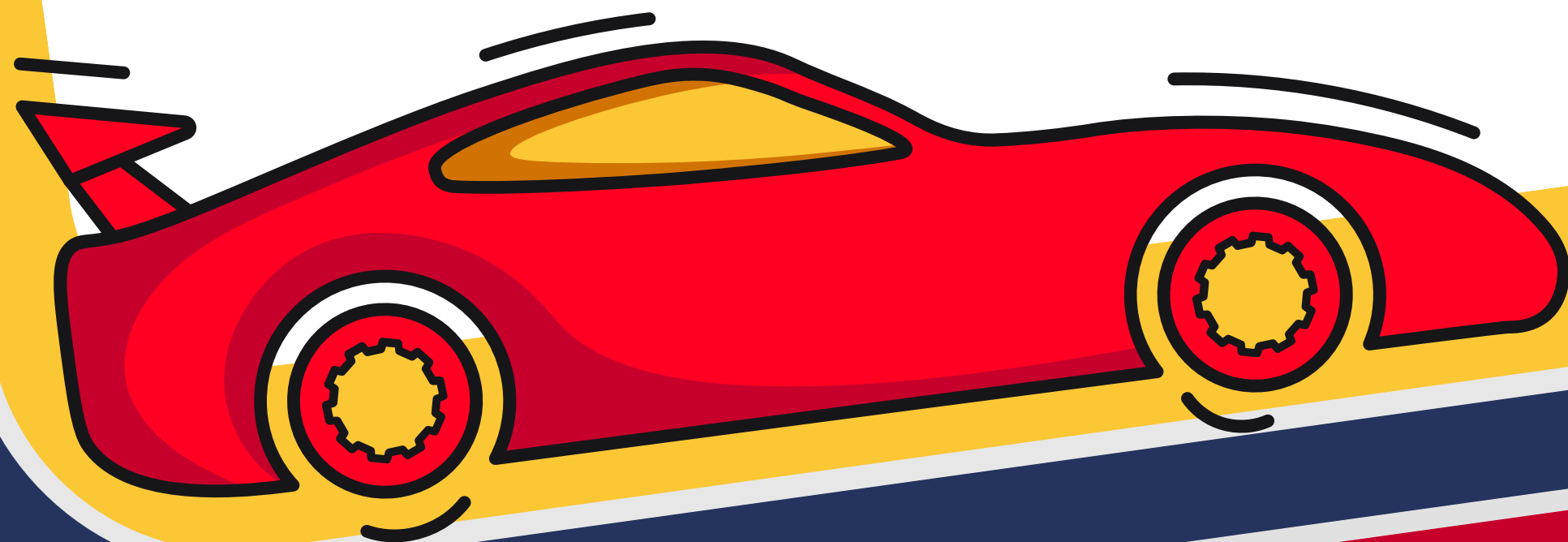


RACING GAME F1-AI

IXH25-Italian XRPL Hackathon

**πve: Emanuele Nardone, Rosa Fera, Gabriele Lozupone,
Sara Marchetti, Emanuele Vita**



CRYPTOGRAPHIC TOOLS

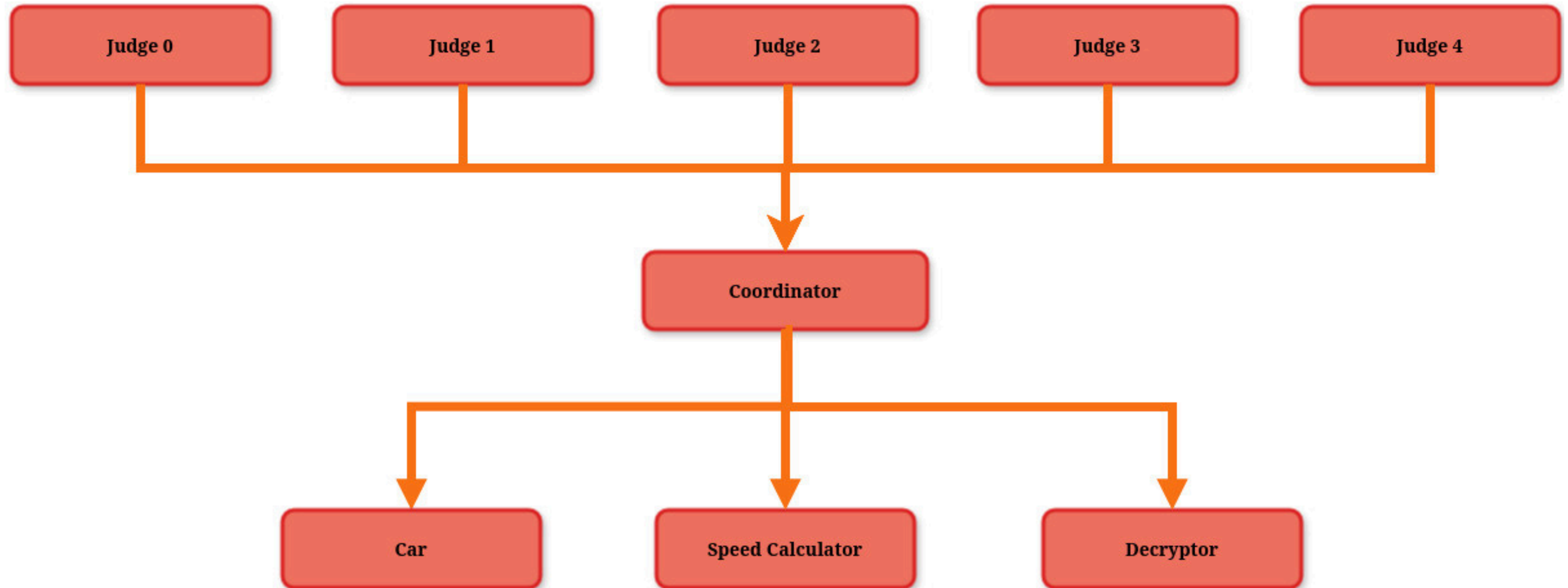
Fully Homomorphic Encryption (FHE) and Distributed Key Generation (DKG)

Compute a machine's speed securely — no one ever learns the secret flags and speed formula.

- Fully Homomorphic Encryption (FHE) → computation on ciphertexts:
BFV scheme based on RLWE.
- Distributed Key Generation (DKG) → no single entity holds the secret.
- Speed and flags could be decrypted only by collaboration.



GENERAL SCHEME



DISTRIBUTED KEY GENERATION

5 Judges collaborate to build one public key:

- Each judge samples a secret share s_k
- Computes a partial public value $b_k = -a \cdot s_k + e_k$
- The system aggregates:

$$b = \sum_{k=0}^4 b_k, s = \sum_{k=0}^4 s_k$$

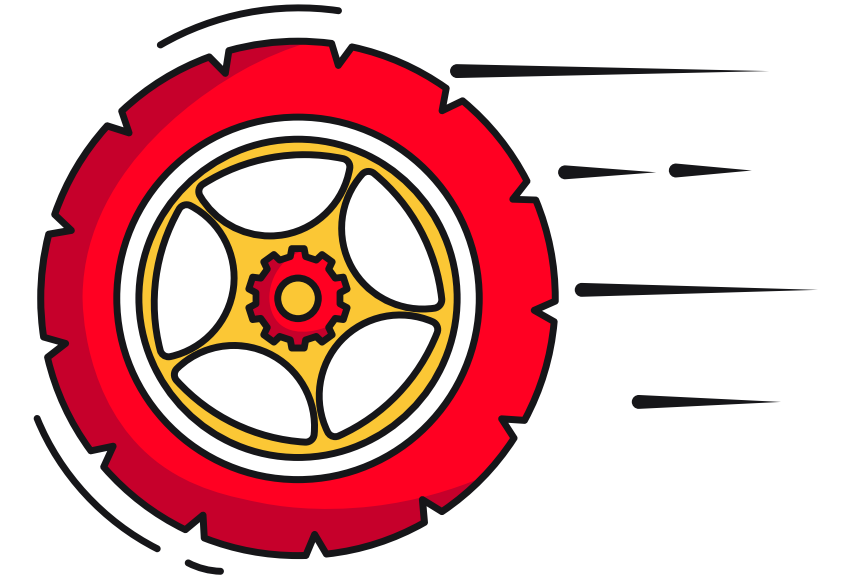
Public key = (a,b) known to all.

Secret key never reconstructed — it's split across judges.

No single party can decrypt alone.



SPEED FORMULA



$$S = t^T W t$$

How W is constructed ?

Each judge generates random $A_k \in \mathbb{Z}^{10 \times 10}$, computes $W_k = A_k^T A_k$ and encrypts it $Enc(W_k)$.

Then:

$$Enc(W) = \sum_{k=0}^4 Enc(W_k)$$

Each $A_k^T A_k$ is positive semi-definite so W is also semi-definite.

SECURE SPEED COMPUTATION

- Each new car $\rightarrow$ vector $t = (t_0, \dots, t_9) \in (0, 1000)^{10}$
- Each judge $k \in \{0, 1, 2, 3, 4\}$ encrypts their part $\rightarrow Enc(t_{0,k})$
- Server computes on ciphertexts:
 - 1) Aggregate vectors: $Enc(t_i) = \sum_{k=0}^4 Enc(t_{i,k})$
 - 2) Compute speed $Enc(S) = Enc(t^T W t)$ using only homomorphic addition and multiplication.

Result = encrypted speed



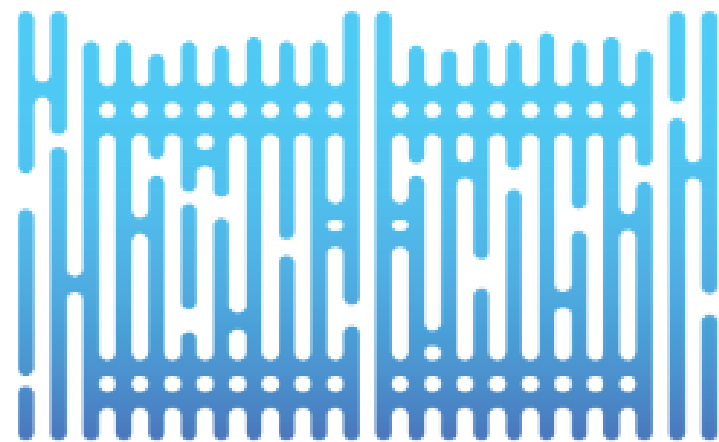
TRAINING WITH FHE

Train your car by tweaking its 10 “flags” (car parameters) —
but keep them secret thanks to Fully Homomorphic Encryption (FHE).

1. Choose which subsets of flags to train $S_{train} \subseteq \{t_0, \dots, t_9\}$
2. For each active flag, generate a random delta $\Delta_i \in (-20, +20)$
3. Encrypt Δ_i
4. $Enc(t_i!) = Enc(t_i) + Enc(\Delta_i)$



The image contains two logos. On the left is the Python logo, which consists of two interlocking snakes, one blue and one yellow. On the right is the NumPy logo, which features a large blue 'N' next to a 3D cube made of smaller blue cubes.



OpenFHE

Player Dashboard

XPF Balance: 203

Your Garage:

Gen	0	113.09 km/h	Player-F1
Gen	1	37.60 km/h	Player-F1
Gen	1	74.93 km/h	Player-F1
Gen	2	84.57 km/h	Player-F1
Gen	1	91.68 km/h	Player-F1

Selected Car:

Gen 0 ID: ...F1-0001

Speed: 113.09 km/h

Training Controls

Select flags to train (0-9):

☒ 10☒ 11☐ 12☐ 13☐ 14
☐ 15☒ 16☒ 17☒ 18☐ 19

Training intensity (delta_max):
20

Train Selected Car (Cost: 1 XPF)

Test Speed

Race Selected Car (Cost: 1 XPF)

Garage: 5 | Races: 3 | Trainings: 4

Game Log & Results

[10:21:24] RACE RESULTS:
[10:21:24] Your car: Player-F1 (Gen 0)
[10:21:24]
[10:21:24] #1: Player-F1 - 113.09 km/h
[10:21:24] #2: Storm-AI - 96.29 km/h
[10:21:24] #3: Blaze-AI - 77.33 km/h
[10:21:24] #4: Rocket-AI - 58.64 km/h
[10:21:24] #5: Lightning-AI - 46.95 km/h
[10:21:24] #6: Thunder-AI - 34.38 km/h
[10:21:24] CONGRATULATIONS! Player-F1 (Gen 0) WON! (+100 XPF)
[10:21:24]
[10:21:24] Training car on flags [1, 6, 7] (delta_max=20)...
[10:22:22] New car created (Gen 1). Speed: 37.60 km/h (-75.48, -66.7%) - slower than parent!
[10:22:25] Your garage now has 2 car(s). Select the fastest for racing!
[10:22:27] Selected: Player-F1 (Gen 0) (Gen 0, 113.09 km/h)
[10:22:30] Training car on flags [1, 6, 7, 8] (delta_max=20)...
[10:22:33] New car created (Gen 1). Speed: 74.93 km/h (-38.16, -33.7%) - slower than parent!
[10:22:33] Your garage now has 3 car(s). Select the fastest for racing!
[10:22:37] Training car on flags [1, 6, 7, 8] (delta_max=20)...
[10:22:40] New car created (Gen 1). Speed: 84.57 km/h
[10:22:40] Your garage now has 4 car(s). Select the fastest for racing!
[10:22:44] Selected: Player-F1 (Gen 0) (Gen 0, 113.09 km/h)
[10:22:49] Training car on flags [0, 1, 6, 7, 8] (delta_max=20)...
[10:22:52] New car created (Gen 1). Speed: 91.68 km/h
[10:22:52] Your garage now has 5 car(s). Select the fastest for racing!
[10:23:02] RACE STARTING!
[10:23:02]
[10:23:02] RACE RESULTS:
[10:23:18] Your car: Player-F1 (Gen 1)
[10:23:18]
[10:23:18] #1: Storm-AI - 96.29 km/h
[10:23:18] #2: Player-F1 - 91.68 km/h
[10:23:18] #3: Blaze-AI - 77.33 km/h
[10:23:18] #4: Rocket-AI - 58.64 km/h
[10:23:18] #5: Lightning-AI - 46.95 km/h
[10:23:18] #6: Thunder-AI - 34.38 km/h
[10:23:18] Player-F1 (Gen 1) didn't win. Try a different flag combination.
[10:23:18] Winner: Storm-AI (96.29 km/h)
[10:23:18]
[10:23:18] Selected: Player-F1 (Gen 0) (Gen 0, 113.09 km/h)
[10:23:39] RACE STARTING!
[10:23:43]
[10:23:43] RACE RESULTS:
[10:23:59] Your car: Player-F1 (Gen 0)
[10:23:59]
[10:23:59] #1: Player-F1 - 113.09 km/h
[10:23:59] #2: Storm-AI - 96.29 km/h
[10:23:59] #3: Blaze-AI - 77.33 km/h
[10:23:59] #4: Rocket-AI - 58.64 km/h
[10:23:59] #5: Lightning-AI - 46.95 km/h
[10:23:59] #6: Thunder-AI - 34.38 km/h
[10:23:59] CONGRATULATIONS! Player-F1 (Gen 0) WON! (+100 XPF)
[10:23:59]

Race Animation

RACE IN PROGRESS

>>> Player-F1
113.1 km/h

Storm-AI
96.3 km/h

Blaze-AI
77.3 km/h

Rocket-AI
58.6 km/h

Lightning-AI
47.0 km/h

Thunder-AI
34.4 km/h

Racing!

Status: Ready to race!

F1-AI WEB APP

