CrypTO Cars

IXH25 - Italian XRPL Hackathon

Group ”PoliTO 1”

Di Felice Francesco, Gasparini Flavio, Savina Matteo

November 8, 2025

Politecnico di Torino

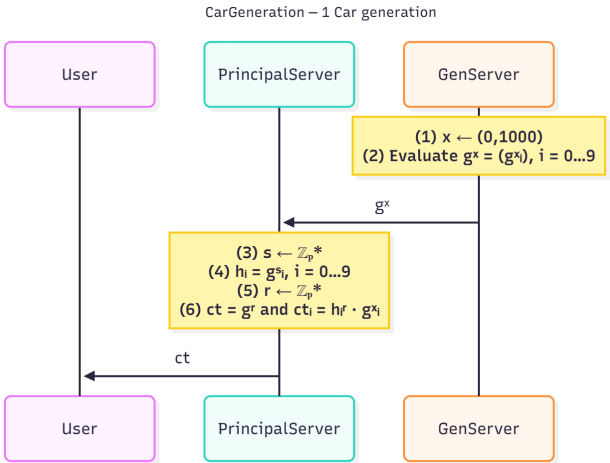
Setting

In our analysis, we modeled four distinct entities involved in the system:

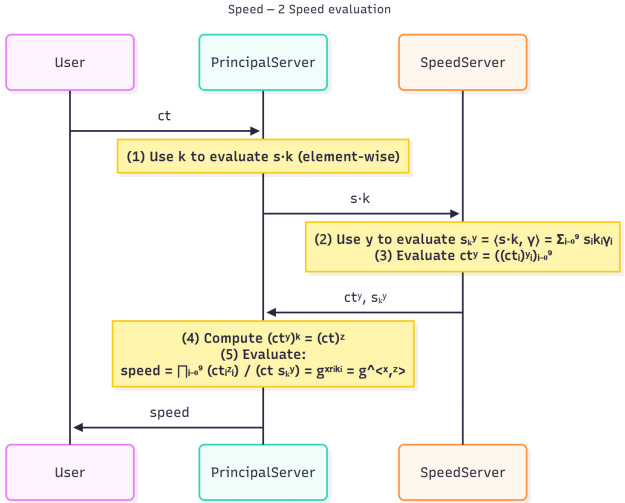
1. User
2. Principal Server
3. Generation Server
4. Speed Server

We employ a **multi-party functional homomorphic encryption scheme**, inspired by the paper *"Simple Functional Encryption Schemes for Inner Products" (2015, École Normale Supérieure)*. The speed function used is defined as $g^{\langle x,z \rangle}$, where $z = k \cdot y$ element-wise. Importantly, the vector z remains individually unknown to each server.
Our security model relies on the **Discrete Logarithm Assumption** and the premise that the **servers do not collude**.

CarGeneration



Speed Computation



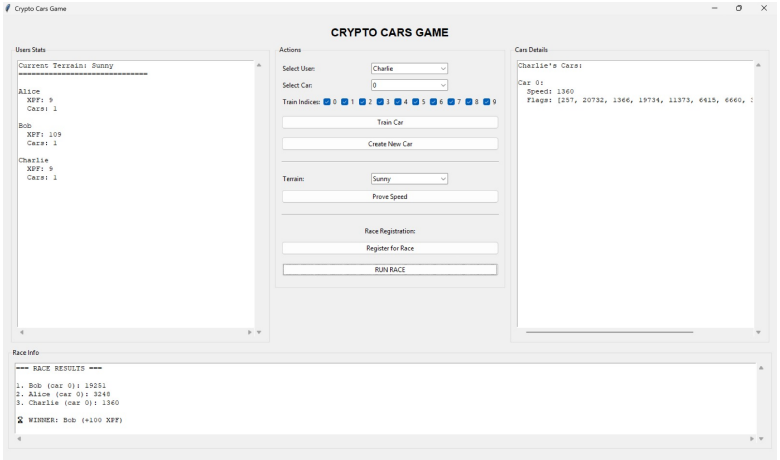
Homomorphic Encryption - Training

At this point the user owns a **car** with a defined **speed**. By spending **1 XPF**, the user can either train the car, or join the next race directly. The user can also input the **weather** on which the race takes place.
The training process is made possible by the use of a **homomorphic encryption scheme**. Thanks to its properties, operations such as adding or subtracting up to 20 from a flag can be performed directly on the encrypted data, without the need for decryption.

Game

Races occur every 10 minutes, following a blockchain-like structure. The winner earns **100 XPF** by adding the new block and other users can verify the result via a **modified version** of the **BLS protocol** on the single $ctx_i^{z_i}$.

Demo


Crypto Cars Game
CRYPTO CARS GAME
Users Stats
Current Terrain: Sunny
Alice
XPF: 9
Cars: 1
Bob
XPF: 109
Cars: 1
Charlie
XPF: 9
Cars: 1
Actions
Select User:
Charlie
Select Car:
0
Train Indices: 0 1 2 3 4 5 6 7 8 9
Train Car
Create New Car
Terrain:
Sunny
Prove Speed
Race Registration:
Register for Race
RUN RACE
Cars Details
Charlie's Cars:
Car 0:
Speed: 1360
Flags: [257, 20732, 1366, 19734, 11373, 6415, 6660,
Race Info
=== RACE RESULTS ===
1. Bob (car 0): 19251
2. Alice (car 0): 3240
3. Charlie (car 0): 1360
WINNER: Bob (+100 XPF)

AI disclaimer

We used Generative AI (ChatGPT-5) to:

- Assist in programming the system's infrastructure, excluding any cryptographic components
- Draft and refine the `README` documentation
- Proofread and improve the presentation slides
- This paragraph! :)

CrypTO Cars

Thank you for listening!
Any questions?