SaTC: CORE: Small: Preventing Web Side-channel Attacks via Atomic Determinism
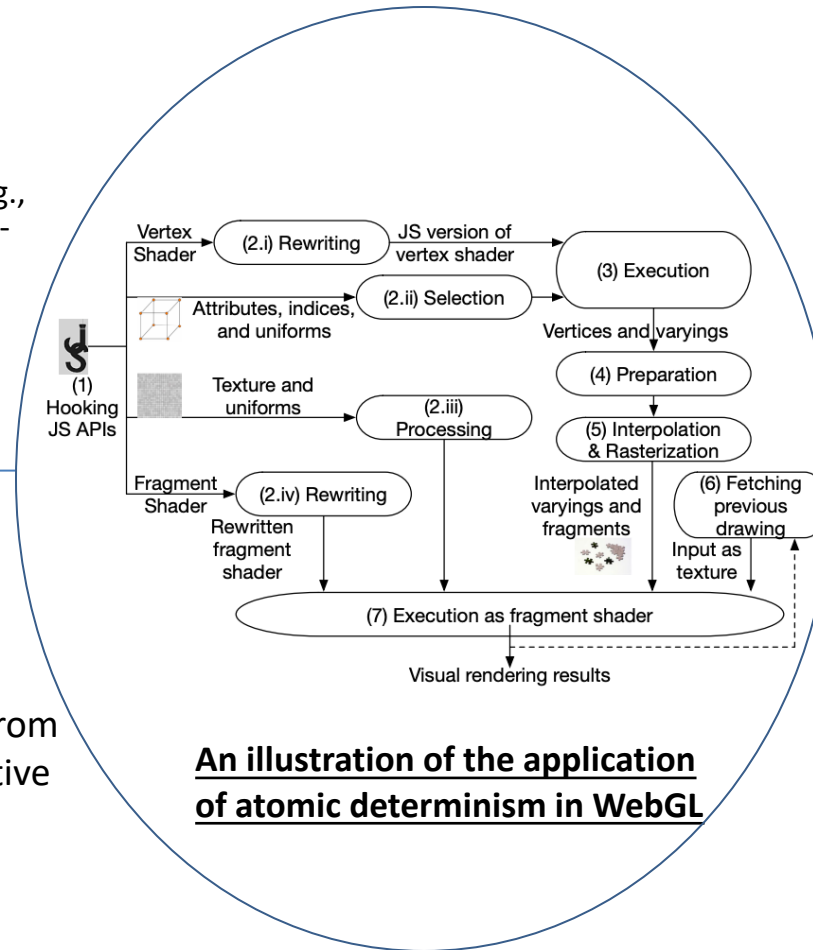
Challenge:

- Web side channels often help low-level attacks, e.g., breaking ASLR, or privacy-related tasks like fingerprinting

Scientific Impact:

- The proposed project will mitigate web side channels without degrading performance.
- It will change people's view that performance and security are enemies.

An illustration of the application of atomic determinism in WebGL

Solution:

- A new concept called atomic determinism
- Borrowing concepts from physics to define relative time between frames

Broader Impact and Broader Participation:

- The proposed project will help web users.
- It can be shipped as part of privacy-preserving browsers.
- The Pis involve the concepts in courses.