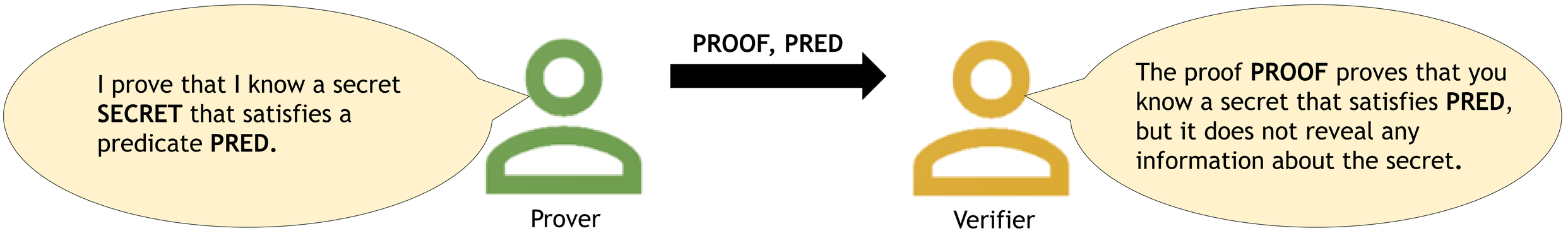
Stateful Zero-Knowledge

Aditya Damodaran, Alfredo Rial, Peter Ryan, SnT, University of Luxembourg

APSIA Research Group

Zero-Knowledge Proofs

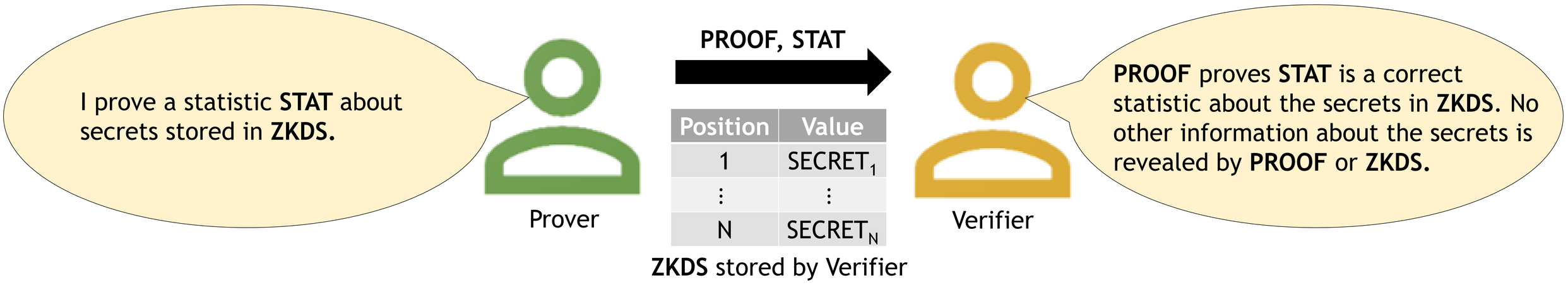
A zero-knowledge proof is a protocol between a prover and a verifier. The prover proves to the verifier knowledge of a secret that satisfies a predicate or condition. The zero-knowledge property ensures that the verifier does not learn any information about the secret.



Stateful Zero-Knowledge (SZK)

We propose stateful zero-knowledge protocols. The secrets used by the prover are stored by the verifier in a zero-knowledge data structure (ZKDS). The ZKDS does not reveal the secrets to the verifier, but allows the prover to prove predicates about secrets stored. Advantages:

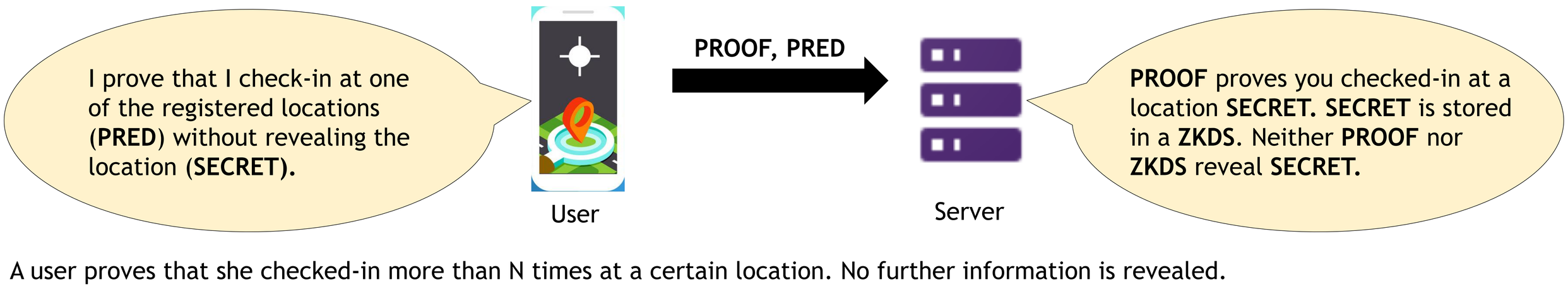
- Efficiency: the prover can reuse a stored secret without reproving predicates about it.
- Functionality: the prover can prove statistics about the stored secrets. For example, the number of times that a secret was used.



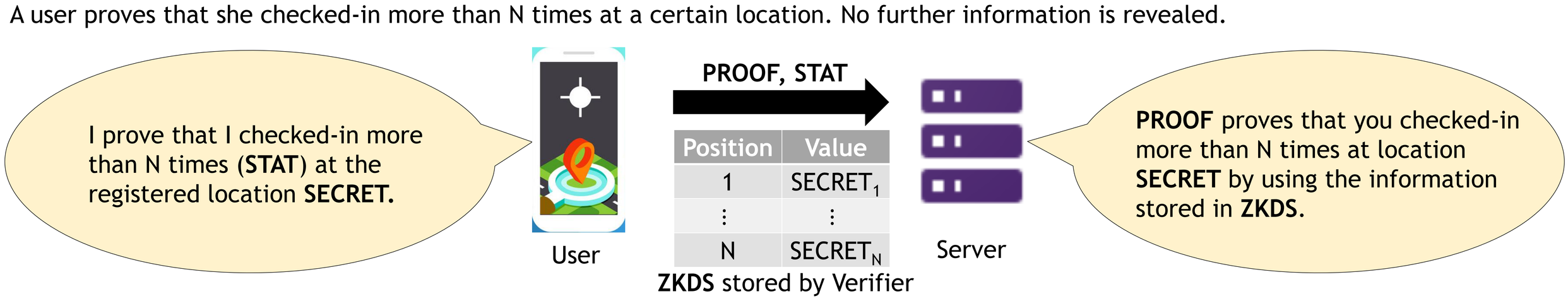
Applications of SZK to Privacy-Preserving Cryptographic Protocols

Example: Privacy-Preserving Location-Based Services

A user proves that she checks-in at a registered location without revealing the location. The location is stored in a ZKDS, along with locations used in previous and future check-ins. Neither the proof nor the ZKDS reveal the locations.



A user proves that she checked-in more than N times at a certain location. No further information is revealed.



Other Examples: Privacy-Preserving E-Commerce, Smart Billing, Access Control

Supported by the Luxembourg National Research Fund (FNR)
CORE Programme. Project code: C17/11650748

Luxembourg National Research Fund