Vehicle taxation and subsidies without nation-scale surveillance

Martin Suomalainen[1]

[1]This research has been funded by the Defense Advanced Research Projects Agency (DARPA) under contract HR0011-20-C-0083. The views, opinions, and/or findings expressed are those of the author(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government. This research has also been supported by European Regional Development Fund through the Estonian Centre of Excellence in ICT Research (EXCITE).

Estonian EV Subsidy

2. peatükk
Toetuse andmise alused

§ 4. Toetatav tegevus

(1) Meetme raames toetatakse elektrisõiduki ostmist kasutamiseks peamiselt Eestis.

(2) Elektrisõiduk käesoleva määruse mõistes on ainult elektri jõul liikuv ehk täiselektriline M1 või N1 kategooria sõiduk.

(3) Elektrisõidukiga tuleb nelja aasta jooksul toetuse väljamaksmisest läbida vähemalt 80 000 kilomeetrit.

(4) Elektrisõidukiga tuleb vähemalt 80% lõikes 3 nõutud kilometraažist läbida Eestis.

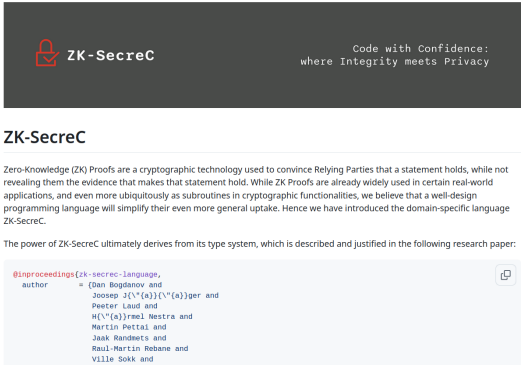
(5) Elektrisõiduki esimese 80 000 kilomeetri läbimiseks kulutatud energiakulu ulatuses tuleb tarbida taastuvenergiat.

Compliance

- Cars were installed with GPS trackers
- Only odometer readings and current country were transmitted once per quarter
- GPS module could be toggled remotely
- Opt-out with periodic reporting and allowing inspection.

ZK-SecreC

- DSL for creating Zero-Knowledge proofs
- Emphasis on real data sizes and interoperability
- Designed to tackle new classes of problems
- Outputs intermedia representation that protocols can ingest



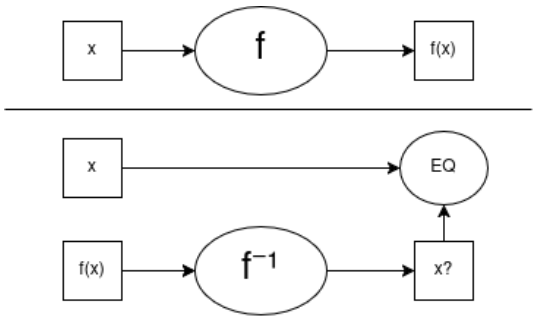
Language Features

```
uint[N] $pre @prover
```

- Three-dimensional type system
  - Stage: mark on/off-circuit
  - Domain: mark data visibility
- Allows branching on Stage and Domain
- Library of highly polymorphic code

Witness expansion

- Reducing the size of the circuit is crucial for performance
- Instead of f, maybe compute f^{-1}
- Care must be taken to not underconstrain
- $10 \cdot 10 \mod 13 = 9$
- Creates need to track on/off circuit computation



ZK-SecreC example

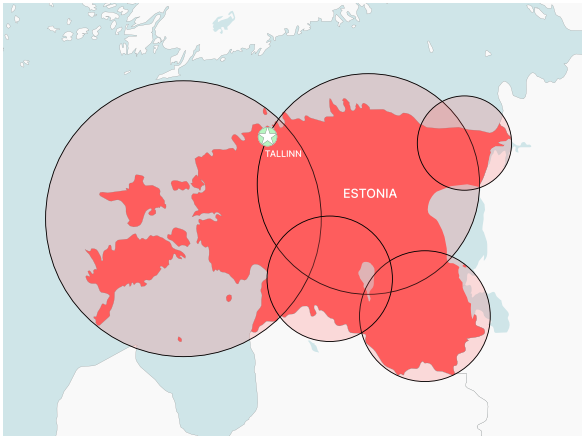
```
pub fn sqrt_fixed[N : Nat, $S, @D](x : Fixed[N, $S, @D]) -> Fixed[N, $S, @D]
  if (post $S) {
    let res = fixed_post(sqrt_fixed_pre(fixed_pre(x)));
    if (@prover <= @D) { check_coef_sqrt(x,res)}
    res
  } else {sqrt_fixed_pre(x)}
}
```

Output

- Outputs IR that integrates with ZK protocols
  - VOLE (Diet Mac'n'Cheese, emp-zk)
  - MPC-in-the-head (ZKB++)
  - VOLE-in-the-head (Schmivitz)
  - Circom
- Function Gates
- Field Switching

Proof statement

- Approximated Estonia with Circles
- Used standard (x,y) coordinate projection for Estonia
- Given a coordinate trace
  - Check validity of inputs
  - Find total path length
  - Find total path length within Estonia
  - Assert that they're within parameters

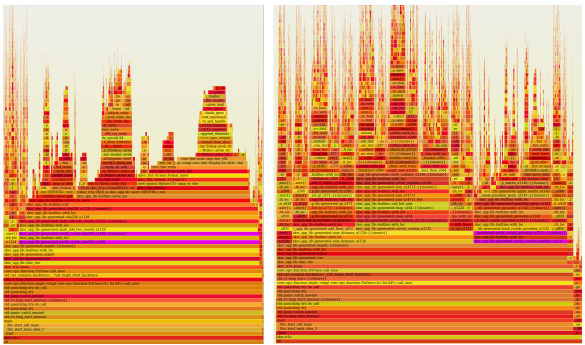


Requirements

- Needed to ensure privacy of
  - Location trails
  - Activity patterns
- 1h/day of driving
- 2 coordinates per minute
- 3600 coordinates/month
- 43200 coordinates/year

Input validation

- Assume coordinates are signed by a trusted source
- Signature check not under ZK
- Poseidon over SHA256 was necessary
- Poseidon implemented in ZK-SecreC

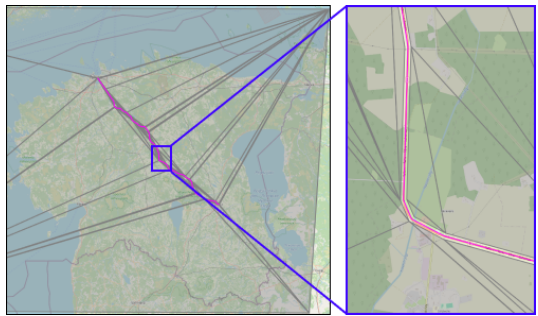


Distance Evaluation

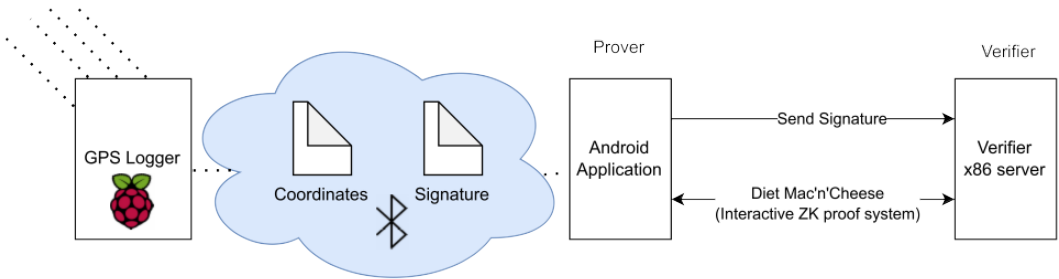
- For each coordinate
  - Compute if it's contained in a circle
  - Compute distance to previous coordinate
- Added support for fractional numbers
- Heavy use of witness expansion tricks for performance
- Verifier challenges for faster inequality checks

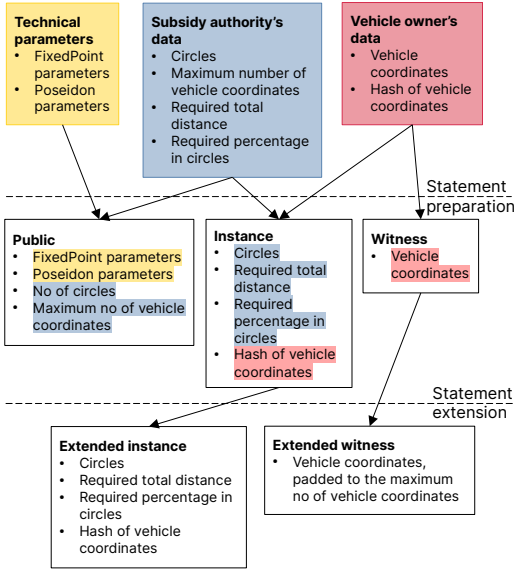
Highway tax

- Prove that a vehicle drove no more than d km along a certain highway
- Represent highway as line segments
- Create polygon for highway + margin
- Create Delaunay triangulation of surrounding area
- Show that L − d km was in triangles, L := total distance



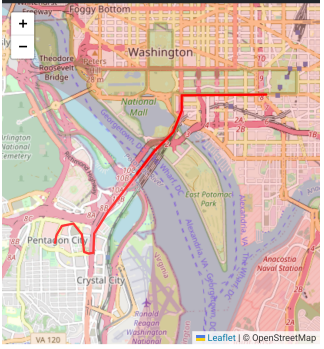
Demonstrator




Technical parameters
• FixedPoint parameters
• Poseidon parameters
Subsidy authority's data
• Circles
• Maximum number of vehicle coordinates
• Required total distance
• Required percentage in circles
Vehicle owner's data
• Vehicle coordinates
• Hash of vehicle coordinates
Statement preparation
Public
• FixedPoint parameters
• Poseidon parameters
• No of circles
• Maximum no of vehicle coordinates
Instance
• Circles
• Required total distance
• Required percentage in circles
• Hash of vehicle coordinates
Witness
• Vehicle coordinates
Statement extension
Extended instance
• Circles
• Required total distance
• Required percentage in circles
• Hash of vehicle coordinates
Extended witness
• Vehicle coordinates, padded to the maximum no of vehicle coordinates

Demonstrator

Distance travelled	4.11 miles
Percentage within bounds	42.96 %



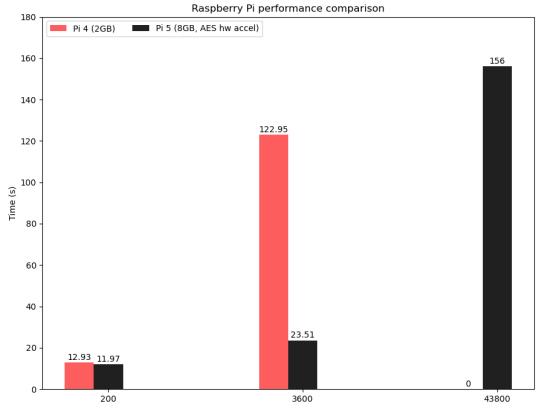
Prove that the path satisfies validation criteria.

Prove

CYBERNETICA

Performance

Prover	Tracking duration	Runtime
Pixel 5a	Trip (400)	13.60s
Pixel 5a	Month (3600)	127s
Pixel 5a	Year (43800)	1724s
Pi 5	Month (3600)	23s
Pi 5	Year (43800)	152s
Pixel 5a	Trip (HW, 400)	36s



Thank you!