Internal o1js audit (Q1 2024)

In March 2024, we spent roughly two person-weeks to conduct an internal audit of parts of the o1js code base. The team member assigned to this task was Gregor Mitscha-Baude.

Scope

The audit scope was formulated as dedicating a certain amount of time, with no precise specification of the code to be covered. Gregor spent the time focusing mainly on reviewing core provable code, in particular (but not exclusively) code which he wasn't already intimately familiar with himself.

The following is a non-exhaustive list of reviewed files:

- Logic which translates high-level snarky constraints into raw Kimchi generic gates:
  - plonk_constraint_system.ml (https://github.com/MinaProtocol/mina/blob/5f668b06164e1951d4bce0594ec40f77c5cdd102/src/lib/crypto/kimchi_backend/common/plonk_constraint_system.ml)
  - gadgets/basic.ts (https://github.com/o1-labs/o1js/blob/ac897b53fa39a493de7576b696156231d2eeacfd/src/lib/provable/gadgets/basic.ts)
  - gadgets/compatible.ts (https://github.com/o1-labs/o1js/blob/main/src/lib/provable/gadgets/compatible.ts)
- General-purpose `Field` and `Bool` gadgets
  - field.ts (https://github.com/o1-labs/o1js/blob/ac897b53fa39a493de7576b696156231d2eeacfd/src/lib/provable/field.ts)
  - bool.ts (https://github.com/o1-labs/o1js/blob/ac897b53fa39a493de7576b696156231d2eeacfd/src/lib/provable/bool.ts)
- Range-check and comparison gadgets
  - gadgets/range-check.ts (https://github.com/o1-labs/o1js/blob/main/src/lib/provable/gadgets/range-check.ts)
  - gadgets/comparison.ts (https://github.com/o1-labs/o1js/blob/ac897b53fa39a493de7576b696156231d2eeacfd/src/lib/provable/gadgets/comparison.ts)
  - int.ts (https://github.com/o1-labs/o1js/blob/ac897b53fa39a493de7576b696156231d2eeacfd/src/lib/provable/int.ts)
- Native curve operations
  - pickles/plonk_curve_ops.ml (https://github.com/MinaProtocol/mina/blob/develop/src/lib/pickles/plonk_curve_ops.ml)

    - gadgets/native-curve.ts (https://github.com/o1-labs/o1js/blob/ac897b53fa39a493de7576b696156231d2eeacfd/src/lib/provable/gadgets/native-curve.ts)
    - group.ts (https://github.com/o1-labs/o1js/blob/ac897b53fa39a493de7576b696156231d2eeacfd/src/lib/provable/group.ts)
    - scalar.ts (https://github.com/o1-labs/o1js/blob/ac897b53fa39a493de7576b696156231d2eeacfd/src/lib/provable/scalar.ts)
- Non-native curve operations
    - gadgets/elliptic-curve.ts (https://github.com/o1-labs/o1js/blob/ac897b53fa39a493de7576b696156231d2eeacfd/src/lib/provable/gadgets/elliptic-curve.ts)

Notably, the audit did not cover any of the (highly critical) zkApp wrapper circuits, because the team had already spent a significant part of the preceding two months on refining those circuits and adding test coverage.

Results

The audit resulted in the following fixes and docs improvements to provable methods.

- https://github.com/MinaProtocol/mina/pull/15296 (https://github.com/MinaProtocol/mina/pull/15296)
    - critical fix of core zkDSL logic
    - also affects Mina and landed in time before the pre-HF devnet release
- https://github.com/o1-labs/o1js/pull/1545 (https://github.com/o1-labs/o1js/pull/1545)
    - make non-native EC add unconditionally sound
    - fixes gap in soundness of of non-native scalar multiplication
- https://github.com/o1-labs/o1js/pull/1507/commits/9f578135f66f4d7a52a794ea9af862d913aa0d5a (https://github.com/o1-labs/o1js/pull/1507/commits/9f578135f66f4d7a52a794ea9af862d913aa0d5a)
    - missing constraint in `isEven()` gadget
    - subsequently reimplemented in https://github.com/o1-labs/o1js/pull/1523 (https://github.com/o1-labs/o1js/pull/1523)
- https://github.com/o1-labs/o1js/pull/1530 (https://github.com/o1-labs/o1js/pull/1530)
    - fix completeness of native scalar multiplication
- https://github.com/o1-labs/o1js/pull/1485 (https://github.com/o1-labs/o1js/pull/1485)
    - fix misleading doccomments
    - remove often-misused `rangeCheckHelper()` API