Algorand Cryptographic Primitive Specification

September 6, 2019

Abstract

Algorand relies on a set of cryptographic primitives to guarantee the integrity and finality of data. This document describes these primitives.

Contents

1 Representation

As a preliminary for guaranteeing cryptographic data integrity, Algorand represents all inputs to cryptographic functions (i.e., a cryptographic hash, signature, or verifiable random function) via a canonical and domain-separated representation.

1.1 Canonical Msgpack

Algorand uses a version of msgpack to produce canonical encodings of data. Algorand's msgpack encodings are valid msgpack encodings, but the encoding function is deterministic to ensure a canonical representation that can be reproduced to verify signatures. A canonical msgpack encoding in Algorand must follow these rules:

1. Maps must contain keys in lexicographic order;

2. Maps must omit key-value pairs where the value is a zero-value, unless otherwise specified;
3. Positive integer values must be encoded as "unsigned" in msgpack, regardless of whether the value space is semantically signed or unsigned;
4. Integer values must be represented in the shortest possible encoding;
5. Binary arrays must be represented using the "bin" format family (that is, use the most recent version of msgpack rather than the older msgpack version that had no "bin" family).

1.2 Domain Separation

Before an object is input to some cryptographic function, it is prepended with a multi-character domain-separating prefix. The list below specifies each prefix (in quotation marks):

- For cryptographic primitives:
  - "OT1" and "OT2": The first and second layers of keys used for ephemeral signatures.
- In the Algorand Ledger:
  - "BH": A *Block Header*.
  - "BR": A *Balance Record*.
  - "GE": A *Genesis* configuration.
  - "PF": A *Payset* encoded as a flat list.
  - "TX": A *Transaction*.
- In the Algorand Byzantine Fault Tolerance protocol:
  - "AS": An *Agreement Selector*, which is also a VRF input.
  - "CR": A *Credential*.
  - "SD": A *Seed*.
  - "PL": A *Payload*.
  - "PS": A *Proposer Seed*.
  - "VO": A *Vote*.
- In other places:
  - "MX": An arbitrary message used to prove ownership of a cryptographic secret.
  - "NPR": A message which proves a peer's stake in an Algorand networking implementation.
  - "TE": An arbitrary message reserved for testing purposes.
  - In Algorand auctions:
    - "aB": A *Bid*.
    - "aD": A *Deposit*.
    - "aO": An *Outcome*.
    - "aP": Auction parameters.
    - "aS": A *Settlement*.

2 Hash Function

Algorand uses the SHA-512/256 algorithm as its primary cryptographic hash function.

Algorand uses this hash function to (1) commit to data for signing and for the Byzantine Fault Tolerance protocol, and (2) rerandomize its random seed.

3 Digital Signature

Algorand uses the ed25519 digital signature scheme to sign data.

3.1 Ephemeral-key Signature

4 Verifiable Random Function

4.1 Cryptographic Sortition