Elliptic Curve Verifiable Random Function

A verifiable random function (VRF) is a cryptographic primitive that enables you to generate a random number and provide proof that the number used a secret key for generation. Anyone can verify the proof using the public key corresponding to the secret key, so you can use it as a random number generator (RNG) that generates outputs that anyone can verify. Applications that need verifiable randomness on chain can also benefit from its use.

The VRF used in the Move API in Sui is an elliptic curve VRF (ECVRF) following the CFRG VRF draft specifications version 15 . It uses Ristretto255 elliptic curve group construction with the SHA-512 hash function. The nonce is generated according to RFC6979 .

Any implementation following the same specifications with suite string sui_vrf (see section 5 in the VRF specs) can be used to compute VRF output and generate proofs.

The fastcrypto library provides a CLI tool for such an implementation and is used in the following example.

From the root of the fastcrypto repository, run the following command to generate a key pair:

This outputs a secret key and a public key in hex format. Both the secret and public keys are 32-byte strings:

To compute the VRF output and proof for the input string Hello, world! , which is 48656c6c6f2c20776f726c6421 in hexadecimal, with the key pair generated previously, run the following command:

This should the 80-byte proof and VRF 64-byte output, both in hex format:

You can verify the proof and output in a smart contract using sui::ecvrf::ecvrf_verify from the Sui Move framework:

You can also use the CLI tool for verification:

The preceding command returns the verification:

VRF construction

The VRF used in the Move API in Sui is an elliptic curve VRF (ECVRF) following the CFRG VRF draft specifications version 15 . It uses Ristretto255 elliptic curve group construction with the SHA-512 hash function. The nonce is generated according to RFC6979 .

Any implementation following the same specifications with suite string sui_vrf (see section 5 in the VRF specs) can be used to compute VRF output and generate proofs.

The fastcrypto library provides a CLI tool for such an implementation and is used in the following example.

From the root of the fastcrypto repository, run the following command to generate a key pair:

This outputs a secret key and a public key in hex format. Both the secret and public keys are 32-byte strings:

To compute the VRF output and proof for the input string Hello, world! , which is 48656c6c6f2c20776f726c6421 in hexadecimal, with the key pair generated previously, run the following command:

This should the 80-byte proof and VRF 64-byte output, both in hex format:

You can verify the proof and output in a smart contract using sui::ecvrf::ecvrf_verify from the Sui Move framework:

You can also use the CLI tool for verification:

The preceding command returns the verification: