Module sui::vdf

Hash an arbitrary binary message to a class group element to be used as input for vdf_verify .

This function is currently only enabled on Devnet.

The internal functions for hash_to_input .

Verify the output and proof of a VDF with the given number of iterations. The input, output and proof are all class group elements represented by triples (a,b,c) such that b^2 - 4ac = discriminant. The are expected to be encoded as a BCS encoding of a triple of byte arrays, each being the big-endian twos-complement encoding of a, b and c in that order.

This uses Wesolowski's VDF construction over imaginary class groups as described in Wesolowski (2020), 'Efficient Verifiable Delay Functions.', J. Cryptol. 33, and is compatible with the VDF implementation in fastcrypto.

The discriminant for the class group is pre-computed and fixed. See how this was generated in the fastcrypto-vdf crate. The final selection of the discriminant for Mainnet will be computed and announced under a nothing-up-my-sleeve process.

This function is currently only enabled on Devnet.

The internal functions for vdf_verify_internal .

Constants

```bash

```

Hash an arbitrary binary message to a class group element to be used as input for vdf_verify .

This function is currently only enabled on Devnet.

```bash

```

```bash

```

The internal functions for hash_to_input .

```bash

```

```bash

```

Verify the output and proof of a VDF with the given number of iterations. The input, output and proof are all class group elements represented by triples (a,b,c) such that b^2 - 4ac = discriminant. The are expected to be encoded as a BCS encoding of a triple of byte arrays, each being the big-endian twos-complement encoding of a, b and c in that order.

This uses Wesolowski's VDF construction over imaginary class groups as described in Wesolowski (2020), 'Efficient Verifiable Delay Functions.', J. Cryptol. 33, and is compatible with the VDF implementation in fastcrypto.

The discriminant for the class group is pre-computed and fixed. See how this was generated in the fastcrypto-vdf crate. The final selection of the discriminant for Mainnet will be computed and announced under a nothing-up-my-sleeve process.

This function is currently only enabled on Devnet.

```bash

```

```bash
```

The internal functions for vdf_verify_internal .

```bash
```

```bash
```

Function

Hash an arbitrary binary message to a class group element to be used as input for vdf_verify .

This function is currently only enabled on Devnet.

```bash
```

```bash
```

The internal functions for hash_to_input .

```bash
```

```bash
```

Verify the output and proof of a VDF with the given number of iterations. The input, output and proof are all class group elements represented by triples (a,b,c) such that b^2 - 4ac = discriminant. The are expected to be encoded as a BCS encoding of a triple of byte arrays, each being the big-endian twos-complement encoding of a, b and c in that order.

This uses Wesolowski's VDF construction over imaginary class groups as described in Wesolowski (2020), 'Efficient Verifiable Delay Functions.', J. Cryptol. 33, and is compatible with the VDF implementation in fastcrypto.

The discriminant for the class group is pre-computed and fixed. See how this was generated in the fastcrypto-vdf crate. The final selection of the discriminant for Mainnet will be computed and announced under a nothing-up-my-sleeve process.

This function is currently only enabled on Devnet.

```bash
```

```bash
```

The internal functions for vdf_verify_internal .

```bash
```

```bash
```

```

## Function

The internal functions for hash_to_input .

```bash

```

```bash

```

Verify the output and proof of a VDF with the given number of iterations. The input, output and proof are all class group elements represented by triples (a,b,c) such that b^2 - 4ac = discriminant. The are expected to be encoded as a BCS encoding of a triple of byte arrays, each being the big-endian twos-complement encoding of a, b and c in that order.

This uses Wesolowski's VDF construction over imaginary class groups as described in Wesolowski (2020), 'Efficient Verifiable Delay Functions.', J. Cryptol. 33, and is compatible with the VDF implementation in fastcrypto.

The discriminant for the class group is pre-computed and fixed. See how this was generated in the fastcrypto-vdf crate. The final selection of the discriminant for Mainnet will be computed and announced under a nothing-up-my-sleeve process.

This function is currently only enabled on Devnet.

```bash

```

```bash

```

The internal functions for vdf_verify_internal .

```bash

```

```bash

```

Function

Verify the output and proof of a VDF with the given number of iterations. The input, output and proof are all class group elements represented by triples (a,b,c) such that b^2 - 4ac = discriminant. The are expected to be encoded as a BCS encoding of a triple of byte arrays, each being the big-endian twos-complement encoding of a, b and c in that order.

This uses Wesolowski's VDF construction over imaginary class groups as described in Wesolowski (2020), 'Efficient Verifiable Delay Functions.', J. Cryptol. 33, and is compatible with the VDF implementation in fastcrypto.

The discriminant for the class group is pre-computed and fixed. See how this was generated in the fastcrypto-vdf crate. The final selection of the discriminant for Mainnet will be computed and announced under a nothing-up-my-sleeve process.

This function is currently only enabled on Devnet.

```bash

```

```bash

```
```

The internal functions for vdf_verify_internal .

```bash
```

```bash
```

Function

The internal functions for vdf_verify_internal .

```bash
```

```bash
```