Module sui::ecvrf

@param hash: The hash/output from a ECVRF to be verified. @param alpha_string: Input/seed to the ECVRF used to generate the output. @param public_key: The public key corresponding to the private key used to generate the output. @param proof: The proof of validity of the output. Verify a proof for a Ristretto ECVRF. Returns true if the proof is valid and corresponds to the given output. May abort with EInvalidHashLength , EInvalidPublicKeyEncoding or EInvalidProofEncoding .

Constants

```bash
```

```bash
```

```bash
```

@param hash: The hash/output from a ECVRF to be verified. @param alpha_string: Input/seed to the ECVRF used to generate the output. @param public_key: The public key corresponding to the private key used to generate the output. @param proof: The proof of validity of the output. Verify a proof for a Ristretto ECVRF. Returns true if the proof is valid and corresponds to the given output. May abort with EInvalidHashLength , EInvalidPublicKeyEncoding or EInvalidProofEncoding .

```bash
```

```bash
```

Function

@param hash: The hash/output from a ECVRF to be verified. @param alpha_string: Input/seed to the ECVRF used to generate the output. @param public_key: The public key corresponding to the private key used to generate the output. @param proof: The proof of validity of the output. Verify a proof for a Ristretto ECVRF. Returns true if the proof is valid and corresponds to the given output. May abort with EInvalidHashLength , EInvalidPublicKeyEncoding or EInvalidProofEncoding .

```bash
```

```bash
```