# Bandersnatch VRF-AD Specification

Davide Galassi     Seyed Hosseini

29 Jul 2024 - Draft 13

---

## *Abstract*

This specification delineates the framework for a Verifiable Random Function with Additional Data (VRF-AD), a cryptographic construct that augments a standard VRF by incorporating auxiliary information into its signature. We're going to first provide a specification to extend IETF's ECVRF as outlined in RFC-9381 [1], then we describe a variant of the Pedersen VRF originally introduced by BCHSV23 [2], which serves as a fundamental component for implementing anonymized ring signatures as further elaborated by Vasilyev [3]. This specification provides detailed insights into the usage of these primitives with Bandersnatch, an elliptic curve constructed over the BLS12-381 scalar field specified in MSZ21 [4].

## 1. Preliminaries

**Definition**: A *verifiable random function with additional data (VRF-AD)* can be described with two functions:

- $Prove(sk, in, ad) \mapsto (out, \pi)$ : from secret key $sk$, input $in$, and additional data $ad$ returns a verifiable output $out$ and proof $\pi$.

- $Verify(pk, in, ad, out, \pi) \mapsto (0|1)$ : for public key $pk$, input $in$, additional data $ad$, output $out$ and proof $\pi$ returns either 1 on success or 0 on failure.

### 1.1. VRF Input

An arbitrary length octet-string provided by the user and used to generate some unbiasable verifiable random output.

### 1.2. VRF Input Point

A point in $\langle G \rangle$ generated from VRF input octet-string using the *Elligator 2 hash-to-curve* algorithm as described by section 6.8.2 of RFC-9380 [5].

### 1.3. VRF Output Point

A point in $\langle G \rangle$ generated from VRF input point as: $Output \leftarrow sk \cdot Input$.

### 1.4. VRF Output

A fixed length octet-string generated from VRF output point using the proof-to-hash procedure defined in section 5.2 of RFC-9381.

The first 32 bytes of the hash output are taken.

### 1.5 Additional Data

An arbitrary length octet-string provided by the user to be signed together with the generated VRF output. This data doesn't influence the produced VRF output.

## 2. IETF VRF

Based on IETF RFC-9381 which is extended with the capability to sign additional user data (`ad`).

### 2.1. Configuration

Configuration is given by following the *"cipher suite"* guidelines defined in section 5.5 of RFC-9381.

- `suite_string` = "Bandersnatch_SHA-512_ELL2".

- The EC group $\langle G \rangle$ is the prime subgroup of the Bandersnatch elliptic curve, in Twisted Edwards form, with finite field and curve parameters as specified in MSZ21. For this group, `fLen` = `qLen` = 32 and `cofactor` = 4.

- The prime subgroup generator $G \in \langle G \rangle$ is defined as follows:

$$G.x = \texttt{0x29c132cc2c0b34c5743711777bbe42f32b79c022ad998465e1e71866a252ae18}$$

$$G.y = \texttt{0x2a6c669eda123e0f157d8b50badcd586358cad81eee464605e3167b6cc974166}$$

- `cLen` = 32.

- The public key generation primitive is $pk = sk \cdot G$, with $sk$ the secret key scalar and $G$ the group generator. In this cipher suite, the secret scalar `x` is equal to the secret key `sk`.

- `encode_to_curve_salt` = `pk_string` (i.e. `point_to_string(pk)`).

- The `ECVRF_nonce_generation` function is specified in section 5.4.2.2 of RFC-9381.

- The `int_to_string` function encodes into the 32 bytes little endian representation.

- The `string_to_int` function decodes from the 32 bytes little endian representation eventually reducing modulo the prime field order.

- The `point_to_string` function converts a point in $\langle G \rangle$ to an octet-string using compressed form. The $y$ coordinate is encoded using `int_to_string` function and the most significant bit of the last octet is used to keep track of $x$ sign. This implies that `ptLen = flen = 32`.

- The `string_to_point` function converts an octet-string to a point on $\langle G \rangle$. The string most significant bit is removed to recover the $x$ coordinate as function of $y$, which is first decoded from the rest of the string using `int_to_string` procedure. This function MUST outputs "INVALID" if the octet-string does not decode to a point on the prime subgroup $\langle G \rangle$.

- The hash function `hash` is SHA-512 as specified in RFC-6234 [6], with `hLen` $= 64$.

- The `ECVRF_encode_to_curve` function uses *Elligator2* method described in section 6.8.2 of RFC-9380 and is described in section 5.4.1.2 of RFC-9381, with `h2c_suite_ID_string` $=$ `"Bandersnatch_XMD:SHA-512_ELL2_RO_"` and domain separation tag `DST = "ECVRF_"` ∥ `h2c_suite_ID_string` ∥ `suite_string`.

## 2.2. Prove

**Input**:

- $x \in \mathbb{Z}_r^*$: Secret key
- $I \in \langle G \rangle$: VRF input point
- $ad \in \Sigma^*$: Additional data octet-string.

**Output**:

- $O \in \langle G \rangle$: VRF output point
- $\pi \in (\mathbb{Z}_r^*, \mathbb{Z}_r^*)$: Schnorr-like proof

**Steps**:

1. $O \leftarrow x \cdot I$
2. $Y \leftarrow x \cdot G$
3. $k \leftarrow nonce(x, I)$
4. $c \leftarrow challenge(Y, I, O, k \cdot G, k \cdot I, ad)$
5. $s \leftarrow k + c \cdot x$
6. $\pi \leftarrow (c, s)$

7. **return** $(O, \pi)$

## 2.3. Verify

**Input**:

- $Y \in \langle G \rangle$: Public key

- $I \in \langle G \rangle$: VRF input point

- $ad \in \Sigma^*$: Additional data octet-string.

- $O \in \langle G \rangle$: VRF output point

- $\pi \in (\mathbb{Z}_r^*, \mathbb{Z}_r^*)$: Schnorr-like proof

**Output**:

- True if proof is valid, False otherwise

**Steps**:

1. $(c, s) \leftarrow \pi$

2. $U \leftarrow s \cdot G - c \cdot Y$

3. $V \leftarrow s \cdot I - c \cdot O$

4. $c' \leftarrow challenge(Y, I, O, U, V, ad)$

5. **if** $c \neq c'$ **then return** False

6. **return** True

## 2.4. Challenge

Challenge construction mostly follows the procedure given in section 5.4.3 of RFC-9381 [1] with some tweaks to add additional data.

**Input**:

- $Points \in \langle G \rangle^n$: Sequence of $n$ points.

- $ad \in \Sigma^*$: Additional data octet-string.

**Output**:

- $c \in \mathbb{Z}_r^*$: Challenge scalar.

**Steps**:

1. $str = \texttt{suite\_string} \parallel \texttt{0x02}$

2. **for each** $P$ **in** $Points$: $str = str\parallel \texttt{point\_to\_string}(P)\$$

3. $str = str\|ad\|0x00$

4. $h = \texttt{hash}(str)$

5. $h_t = h[0]\|..\|h[cLen-1]$

6. $c = \texttt{string\_to\_int}(h_t)$

7. **return** $c$

With `point_to_string`, `string_to_int` and `hash` as defined in section 2.1.

# 3. Pedersen VRF

Pedersen VRF resembles IETF EC-VRF but replaces the public key with a Pedersen commitment to the secret key, which makes this VRF useful in anonymized ring proofs.

The scheme proves that the output has been generated with a secret key associated with a blinded public key (instead of the public key). The blinded public key is a cryptographic commitment to the public key, and it can be unblinded to prove that the output of the VRF corresponds to the public key of the signer.

This specification mostly follows the design proposed by BCHSV23 [2] in section 4 with some details about blinding base point value and challenge generation procedure.

## 3.1. Configuration

Pedersen VRF is configured for prime subgroup $\langle G \rangle$ of Bandersnatch elliptic curve $E$ defined in MSZ21 [4] with *blinding base* $B \in \langle G \rangle$ defined as follows:

$$B.x = \texttt{0x2039d9bf2ecb2d4433182d4a940ec78d34f9d19ec0d875703d4d04a168ec241e}$$

$$B.y = \texttt{0x54fa7fd5193611992188139d20221028bf03ee23202d9706a46f12b3f3605faa}$$

For all the other configurable parameters and external functions we adhere as much as possible to the Bandersnatch cipher suite for IETF VRF described in section 2.1 of this specification.

**3.2. Prove**

**Input**:

- $x \in \mathbb{Z}_r^*$: Secret key
- $b \in \mathbb{Z}_r^*$: Secret blinding factor
- $I \in \langle G \rangle$: VRF input point
- $ad \in \Sigma^*$: Additional data octet-string.

**Output**:

- $O \in \langle G \rangle$: VRF output point
- $\pi \in (\langle G \rangle, \langle G \rangle, \langle G \rangle, \mathbb{Z}_r^*, \mathbb{Z}_r^*)$: Pedersen proof

**Steps**:

1. $O \leftarrow x \cdot I$
2. $k \leftarrow nonce(x, I)$
3. $k_b \leftarrow nonce(b, I)$
4. $\bar{Y} \leftarrow x \cdot G + b \cdot B$
5. $R \leftarrow k \cdot G + k_b \cdot B$
6. $O_k \leftarrow k \cdot I$
7. $c \leftarrow challenge(\bar{Y}, I, O, R, O_k, ad)$
8. $s \leftarrow k + c \cdot x$
9. $s_b \leftarrow k_b + c \cdot b$
10. $\pi \leftarrow (\bar{Y}, R, O_k, s, s_b)$
11. **return** $(O, \pi)$

## 3.3. Verify

**Input**:

- $I \in \langle G \rangle$: VRF input point
- $ad \in \Sigma^*$: Additional data octet-string.
- $O \in \langle G \rangle$: VRF output point
- $\pi \in (\langle G \rangle, \langle G \rangle, \langle G \rangle, \mathbb{Z}_r^*, \mathbb{Z}_r^*)$: Pedersen proof

**Output**:

- True if proof is valid, False otherwise

**Steps**:

1. $(\bar{Y}, R, O_k, s, s_b) \leftarrow \pi$

2. $c \leftarrow challenge(\bar{Y}, I, O, R, O_k, ad)$

3. **if** $O_k + c \cdot O \neq I \cdot s$ **then return** False

4. **if** $R + c \cdot \bar{Y} \neq s \cdot G + s_b \cdot B$ **then return** False

5. **return** True

# 4. Ring VRF

Anonymized ring VRF based of [Pedersen VRF] and Ring Proof as proposed by Vasilyev.

## 4.1. Configuration

Setup for plain [Pedersen VRF] applies.

Ring proof configuration:

- KZG PCS uses Zcash SRS and a domain of 2048 entries.

- $G_1$: BLS12-381 $G_1$

- $G_2$: BLS12-381 $G_2$

- TODO: . . .

## 4.2. Prove

**Input**:

- $x \in \mathbb{Z}_r^*$: Secret key

- $P \in TODO$: Ring prover

- $b \in \mathbb{Z}_r^*$: Secret blinding factor

- $I \in \langle G \rangle$: VRF input point

- $ad \in \Sigma^*$: Additional data octet-string.

**Output**:

- $O \in \langle G \rangle$: VRF output point

- $\pi_p \in (\langle G \rangle, \langle G \rangle, \langle G \rangle, \mathbb{Z}_r^*, \mathbb{Z}_r^*)$: Pedersen proof

- $\pi_r \in ((G_1)^4, (\mathbb{Z}_r^*)^7, G_1, \mathbb{Z}_r^*, G_1, G_1)$: Ring proof

**Steps**:

1. $(O, \pi_p) \leftarrow Pedersen.prove(x, b, I, ad)$

2. $\pi_r \leftarrow Ring.prove(P, b)$ (TODO)

3. **return** $(O, \pi_p, \pi_r)$

## 4.3. Verify

**Input**:

- $V \in (G_1)^3$: Ring verifier.
- $I \in \langle G \rangle$: VRF input point.
- $O \in G$: VRF Output point.
- $ad \in \Sigma^*$: Additional data octet-string.
- $\pi_p \in (\langle G \rangle, \langle G \rangle, \langle G \rangle, \mathbb{Z}_r^*, \mathbb{Z}_r^*)$: Pedersen proof
- $\pi_r \in ((G_1)^4, (\mathbb{Z}_r^*)^7, G_1, \mathbb{Z}_r^*, G_1, G_1)$: Ring proof

**Output**:

- True if proof is valid, False otherwise

**Steps**:

1. $rp = Pedersen.verify(I, ad, O, \pi_p)$
2. **if** $rp \neq True$ **return** False
3. $(\bar{Y}, R, O_k, s, s_b) \leftarrow \pi_p$
4. $rr = Ring.verify(V, \pi_r, \bar{Y})$
5. **if** $rr \neq True$ **return** False
6. **return** True

# Appendix A

The test vectors in this section were generated using code provided at https://github.com/davxy/ark-ec-vrfs.

## A.1. IETF VRF Test Vectors

Schema:

```
sk (x): Secret key,
pk (Y): Public key,
in (alpha): Input octet-string,
ad: Additional data octet-string,
h (I): VRF input point,
gamma (O): VRF output point,
out (beta): VRF output octet string,
proof_c: Proof 'c' component,
```

proof_s: Proof 's' component,

**Vector 1**

3d6406500d4009fdf2604546093665911e753f2213570a29521fd88bc30ede18,
a1b1da71cc4682e159b7da23050d8b6261eb11a3247c89b07ef56ccd002fd38b,
-,
-,
b923c55b4b7d8c28156c87e005c6d8385a6f26019eee3149aaeb7ee7ce284b38,
208d1eacbedbfb00708a7068c708a565c0bd41c8155010c52e55c6837fecfa52,
96b48404e1df9c738557ccbdfb5bc6f7b8fa3d281aa51742a5928e7a5d77cf5b
..4fc6ed61fc0f7e073dfc3ee8e06b1e5de55e93ecff8ad926cc99a08e8aa6a779,
106f39b9ba10c49df8dfeeea43f8ff02823110fcd8de3ce6110124d29f75881c,
49584112e665526173bfebb6f8949348b1accf72da122c77b501cd395464330c,

**Vector 2**

8b9063872331dda4c3c282f7d813fb3c13e7339b7dc9635fdc764e32cc57cb15,
5ebfe047f421e1a3e1d9bbb163839812657bbb3e4ffe9856a725b2b405844cf3,
0a,
-,
d905aaf894a97094b1d707ea7685fbc4ac501fc01cef25586a9c36288c5c6302,
25c5ab15ce5d973bfec7b6dd428b5b5971958a056d10cc18d5e9ccd0ee4c7b86,
2ae6660f435f733482e4fb6a2c743288fc1d8a6b173b01f490929cd128514c51
..8112bed1659bb8eab1535e279f9b7349fa316ba6f7bd8baa4ae410141bb565d2,
ac8c53d06bb8c0946c479f1732e16800e810810fedda70f37b8a9c4f1016df11,
9a3d82d40e8600276b5fd92cd8d21287abbece6ee357ff5e086126cf912e3d0a,

**Vector 3**

6db187202f69e627e432296ae1d0f166ae6ac3c1222585b6ceae80ea07670b14,
9d97151298a5339866ddd3539d16696e19e6b68ac731562c807fe63a1ca49506,
-,
0b8c,
587f7c01731c52ce4e02405a9642bf39da4b62befa0a0811f00dd1710a975cc4,
002030eb901d08fe85873b46cd5a1bd2a2c9fbce4f15e9e39066c1fe91be1c1f,
5ca9dc5e02e908b5f1de31c85d30a064353420ab930a541db5f518eee07fb059
..323df22d2ce82d36a5bac52aa322f08072cc0b9c555a5e4179e3c11a067de7a2,
2ae1f37e6427ec7f3b71e90b54eac7b0b21425760f46ca78908bc0fd2077ca16,
78c7f35f0b3e8edd83a08a36a70c263cd7dba1ab81a2d6ee60242b4af06f2d03,

**Vector 4**

b56cc204f1b6c2323709012cb16c72f3021035ce935fbe69b600a88d842c7407,
dc2de7312c2850a9f6c103289c64fbd76e2ebd2fa8b5734708eb2c76c0fb2d99,
73616d706c65,
-,

c1cde8432c5bf619b14a403d611140c117a52ba31004574238bd58bf8fc6181f,
5d5a673794b7a0003a1c36f299c4d61055e4b680bb3c2ccd8858dce89c6cd5d3,
0db282523110f629d8c9424afa66f4dfcb9e6dcea5f7891ab2ffc09eeb72a0ac
..11ac36841ec72644a5d24c1fa879872d3091c5e5b81940761f9f8f378f5013ae,
7eb5a8b661e9d93203d7f7aa4b597e695be7c139b457fa5e33a866f4a66f2f12,
cde921089ee5ec8d2d940e75819a6347cd8f0ccd215b712f90b278ed186cbb03,

## Vector 5

da36359bf1bfd1694d3ed359e7340bd02a6a5e54827d94db1384df29f5bdd302,
decb0151cbeb49f76f10419ab6a96242bdc87baac8a474e5161123de4304ac29,
42616e646572736e6174636820766563746f72,
-,
8af6936567d457e80f6715f403e20597c2ca58219974c3996a4e4414c3361635,
022abfa7670d5051a6a0e212467666abb955faafe7fe63446f50eb710383444c,
126296afb914aa1225dfdddfe3bfd185b488801810e18034330b1c07409ccdc4
..f8deccfc30be219cb5186f80a523ae41720031ae39a78f18d3b14df8bb6d8e8a,
4ddb0d1ebe4d7da9e2cca5c85e39b51166c969dfa30bbf69baafa22121b2000e,
2616dff1f59ff7e7bfc25fa0fea37a9c37e93cf1b88a5e73505a195138590c0c,

## Vector 6

da36359bf1bfd1694d3ed359e7340bd02a6a5e54827d94db1384df29f5bdd302,
decb0151cbeb49f76f10419ab6a96242bdc87baac8a474e5161123de4304ac29,
42616e646572736e6174636820766563746f72,
1f42,
8af6936567d457e80f6715f403e20597c2ca58219974c3996a4e4414c3361635,
022abfa7670d5051a6a0e212467666abb955faafe7fe63446f50eb710383444c,
126296afb914aa1225dfdddfe3bfd185b488801810e18034330b1c07409ccdc4
..f8deccfc30be219cb5186f80a523ae41720031ae39a78f18d3b14df8bb6d8e8a,
087914abfd2a59a593384c538bb2f11480d4b196ae2a973ac33cb7dd2cc1541b,
9ad1cdabc97035a05d76c4f4e3c1826deafbc3e4d41df6bf66eaa21d1ba63018,

## Vector 7

35b877a25c394512292b82bdf8468e98eaf03c79c7fc9d53546dadc5fb75b500,
b0e1f208f9d6e5b310b92014ea7ef3011e649dab038804759f3766e01029d623,
42616e646572736e6174636820766563746f72,
1f42,
69dec7fe79f816d095b04cead45e856ff6c7e798f513e09291958e35a5590443,
9adeacd15eacdc651e4db1ea4c0917973eac2000479edf6132f3774601cc6902,
ff5f6324ea18bbb4df92f7d6304bf27a0a44fa80fd40b985de8d43963a7e02c6
..ef6f0947911604155c6fe40f68cc91c96ffd358275b58960554274498a70f144,
50a14bab81a42e118e8c167136db35b731a9194a250ae5e65452592742cbdb0e,
a75b5327d1b921bb72e2e8c525c18d2fce661b365379ae9f1168c75d281d0100,

## A.2. Pedersen VRF Test Vectors

Schema:

```
sk (x): Secret key,
pk (Y): Public key,
in (alpha): Input octet-string,
ad: Additional data octet-string,
h (I): VRF input point,
gamma (O): VRF output point,
out (beta): VRF output octet string,
blinding: Blinding factor,
proof_pk_com (Y^-): Public key commitment,
proof_r: Proof 'R' component,
proof_ok: Proof 'O_k' component,
proof_s: Proof 's' component,
proof_sb: Proof 's_b' component
```

**Vector 1**

```
3d6406500d4009fdf2604546093665911e753f2213570a29521fd88bc30ede18,
a1b1da71cc4682e159b7da23050d8b6261eb11a3247c89b07ef56ccd002fd38b,
-,
-,
b923c55b4b7d8c28156c87e005c6d8385a6f26019eee3149aaeb7ee7ce284b38,
208d1eacbedbfb00708a7068c708a565c0bd41c8155010c52e55c6837fecfa52,
96b48404e1df9c738557ccbdfb5bc6f7b8fa3d281aa51742a5928e7a5d77cf5b
..4fc6ed61fc0f7e073dfc3ee8e06b1e5de55e93ecff8ad926cc99a08e8aa6a779,
a3f1a139943f3dc02c624505a5794dcc1a75651f60ca69081ebf9bdbd7458616,
2882f90320afdcf99680b8662efe846e2fd477cce00a47ac154f996c910b920a,
71d85bb1a0edcf4362ec8137cdef1a856096e4f9995cc3a4db1781d3e9c7b817,
647c218cec9610102b202bcf7d29bdbf91770c326f07586051fa40bee863b63e,
cda38b375717fa7790c18c70dcfcd6ce8f19b13819f088b74688f21dd127c412,
9b52eff1cc2ab908070a1ba89059ae3f6823b43702c60272c5d5943cceb6ac0e,
```

**Vector 2**

```
8b9063872331dda4c3c282f7d813fb3c13e7339b7dc9635fdc764e32cc57cb15,
5ebfe047f421e1a3e1d9bbb163839812657bbb3e4ffe9856a725b2b405844cf3,
0a,
-,
d905aaf894a97094b1d707ea7685fbc4ac501fc01cef25586a9c36288c5c6302,
25c5ab15ce5d973bfec7b6dd428b5b5971958a056d10cc18d5e9ccd0ee4c7b86,
2ae6660f435f733482e4fb6a2c743288fc1d8a6b173b01f490929cd128514c51
..8112bed1659bb8eab1535e279f9b7349fa316ba6f7bd8baa4ae410141bb565d2,
85a94726bcaeaf2db516a6a532ec2450488e7d093374f54de0ba05d2a36bb00a,
b28263558234202119a143c295a3fc5a35a6f830dd0c7018e3f33862d1986c1c,
```

4cb8186c3da92e9be0179f894cdc364aabe1a890340aee9fd886bed45f5017e7,
83a9519edb8ecc4f360eee599c6c1310019c4c3451ca42b4887328e347003bdf,
3e1b408e4ceb5a81e5b71527b01f541d5069438aaa279aa48c39bb7e34f24001,
1dc7b84f188a7fb5bf051464be19e54495f42bd723130992319bad7560023714,

## Vector 3

6db187202f69e627e432296ae1d0f166ae6ac3c1222585b6ceae80ea07670b14,
9d97151298a5339866ddd3539d16696e19e6b68ac731562c807fe63a1ca49506,
-,
0b8c,
587f7c01731c52ce4e02405a9642bf39da4b62befa0a0811f00dd1710a975cc4,
002030eb901d08fe85873b46cd5a1bd2a2c9fbce4f15e9e39066c1fe91be1c1f,
5ca9dc5e02e908b5f1de31c85d30a064353420ab930a541db5f518eee07fb059
..323df22d2ce82d36a5bac52aa322f08072cc0b9c555a5e4179e3c11a067de7a2,
cb3a17d3578d86e2f3b23bb47160327c391c808da28c6be53ed3189d22d78205,
f99d09a38f1a1ead7d9503fd601e2d8a56c09eaeb5fb3130035803e04033b49a,
de58f590cd204247192f5b49d86c81ddc691fd6b55561fb33ccbec24ecbc86db,
d502f832afaddb7bb54e8c28cce458a2a9c3c6c230e4b85539913ec531de168b,
1dd33771a9bfdcf94e6e95fa43e4667adf3279d9c2b22e0877abeb5e99a9e01b,
7863bbac83653e1a48bc0e814e4792c6b2d884522f5556bbb1844c151dcdb700,

## Vector 4

b56cc204f1b6c2323709012cb16c72f3021035ce935fbe69b600a88d842c7407,
dc2de7312c2850a9f6c103289c64fbd76e2ebd2fa8b5734708eb2c76c0fb2d99,
73616d706c65,
-,
c1cde8432c5bf619b14a403d611140c117a52ba31004574238bd58bf8fc6181f,
5d5a673794b7a0003a1c36f299c4d61055e4b680bb3c2ccd8858dce89c6cd5d3,
0db282523110f629d8c9424afa66f4dfcb9e6dcea5f7891ab2ffc09eeb72a0ac
..11ac36841ec72644a5d24c1fa879872d3091c5e5b81940761f9f8f378f5013ae,
141a8a762dff63c7c05b26d022a8027c515e57f067b5546532296f0ca40a1909,
e926e6b3cbca7b66c42cfc603c4ef2dabc3f5e1276b20d2807f007e974675cb1,
29c56732de262411e71908326037f0f961776db2082bf3d88537265af6a57c92,
c59024c715d21f2a08fb0cd8cb24046558222c6753180853f9601d92186c5e3b,
b818a32590aeb6d79d24cdc6cacb6d5cdc58ccb7025b82be1c1ba2cd34c2f005,
e854b63f9c4e0aab3a051885498d42b5ec354e619491ee9ff239bd3fb486b509,

## Vector 5

da36359bf1bfd1694d3ed359e7340bd02a6a5e54827d94db1384df29f5bdd302,
decb0151cbeb49f76f10419ab6a96242bdc87baac8a474e5161123de4304ac29,
42616e646572736e6174636820766563746f72,
-,
8af6936567d457e80f6715f403e20597c2ca58219974c3996a4e4414c3361635,
022abfa7670d5051a6a0e212467666abb955faafe7fe63446f50eb710383444c,

126296afb914aa1225dfdddfe3bfd185b488801810e18034330b1c07409ccdc4
..f8deccfc30be219cb5186f80a523ae41720031ae39a78f18d3b14df8bb6d8e8a,
4749f32b7aa36158a4fdfb5bc7e63c40b62eb1d7c75036676e093571a3e9cb06,
e159e5494957bb478c4a4d142cde10dadd73a038f8b198c4321dff1271ab61b4,
16a8409cc245978bf55279447d854adca637a58c8c7894a0972b190ad7314492,
3639790d6414b474aa1d53de4e7a896b4e6458c078867acd22200f00f20f280a,
bbfd0996c8937c9aaabad9a254614b75c529f892fdfcfcfbe73486888545b610,
6bce65ffb002c6349213b720115ee1457214796c983618f32b4b79c8c559851b,

**Vector 6**

da36359bf1bfd1694d3ed359e7340bd02a6a5e54827d94db1384df29f5bdd302,
decb0151cbeb49f76f10419ab6a96242bdc87baac8a474e5161123de4304ac29,
42616e646572736e6174636820766563746f72,
1f42,
8af6936567d457e80f6715f403e20597c2ca58219974c3996a4e4414c3361635,
022abfa7670d5051a6a0e212467666abb955faafe7fe63446f50eb710383444c,
126296afb914aa1225dfdddfe3bfd185b488801810e18034330b1c07409ccdc4
..f8deccfc30be219cb5186f80a523ae41720031ae39a78f18d3b14df8bb6d8e8a,
1f64d22282d00a58d17d4fe4dc6e8b9772109b6091e1684649c6084fc842391b,
89e230c832f5c2ee1072d9d110151a2dafa4577d64b7fb0845855ae3d1c12fec,
e3bd5e3a3f07efb256c989f22fcfe8494219dcd37b35419f5f10da68de09f125,
3639790d6414b474aa1d53de4e7a896b4e6458c078867acd22200f00f20f280a,
ceff5ef2315be8be839b1f3c0314b72d976c2e14a2a27c2d1ce8465e90c98607,
0ea7abf79fc1bdebc8b9009cc5744358071c12e82a31565d35a8f91069b55c1b,

**Vector 7**

35b877a25c394512292b82bdf8468e98eaf03c79c7fc9d53546dadc5fb75b500,
b0e1f208f9d6e5b310b92014ea7ef3011e649dab038804759f3766e01029d623,
42616e646572736e6174636820766563746f72,
1f42,
69dec7fe79f816d095b04cead45e856ff6c7e798f513e09291958e35a5590443,
9adeacd15eacdc651e4db1ea4c0917973eac2000479edf6132f3774601cc6902,
ff5f6324ea18bbb4df92f7d6304bf27a0a44fa80fd40b985de8d43963a7e02c6
..ef6f0947911604155c6fe40f68cc91c96ffd358275b58960554274498a70f144,
ea1f922fce5e359d92e0fdcda53a1d2e6b791c7e7a8ffad915f3535c6175f115,
f674ad5f72661aa0c2bc5ca83aee9794c8b8bbc4017abcc00a11a23a0b558e68,
f77eaec55fe36b06f1d1f7eef7db24fdcce74c83fde19b1c322aca288e39948f,
b846dfbceb2a74fe102b3aec94e7b8460f5adcb609c407839ab6cb06d1e3bd38,
35a41d1cb4d22b5c162d319b206db940b6fcef71bbe0c13a6376a89788292519,
c04b177f954d17e7c129ce8d55cb7f148b3957078c96e7229100dc50b7d62b02,

## A.3. Ring VRF Test Vectors

Generated using Zcash BLS12-381 URS.

Schema:

```
sk (x): Secret key,
pk (Y): Public key,
in (alpha): Input octet-string,
ad: Additional data octet-string,
h (I): VRF input point,
gamma (O): VRF output point,
out (beta): VRF output octet string,
blinding: Blinding factor,
proof_pk_com (Y^-): Pedersen proof public key commitment,
proof_r: Pedersen proof 'R' component,
proof_ok: Pedersen proof 'O_k' component,
proof_s: Pedersen proof 's' component,
proof_sb: Pedersen proof 's_b' component,
ring_pks: Ring public keys,
ring_pks_com: Ring public keys commitment,
ring_proof: Ring proof
```

**Vector 1**

3d6406500d4009fdf2604546093665911e753f2213570a29521fd88bc30ede18,
a1b1da71cc4682e159b7da23050d8b6261eb11a3247c89b07ef56ccd002fd38b,
-,
-,
b923c55b4b7d8c28156c87e005c6d8385a6f26019eee3149aaeb7ee7ce284b38,
208d1eacbedbfb00708a7068c708a565c0bd41c8155010c52e55c6837fecfa52,
96b48404e1df9c738557ccbdfb5bc6f7b8fa3d281aa51742a5928e7a5d77cf5b
..4fc6ed61fc0f7e073dfc3ee8e06b1e5de55e93ecff8ad926cc99a08e8aa6a779,
a3f1a139943f3dc02c624505a5794dcc1a75651f60ca69081ebf9bdbd7458616,
2882f90320afdcf99680b8662efe846e2fd477cce00a47ac154f996c910b920a,
71d85bb1a0edcf4362ec8137cdef1a856096e4f9995cc3a4db1781d3e9c7b817,
647c218cec9610102b202bcf7d29bdbf91770c326f07586051fa40bee863b63e,
cda38b375717fa7790c18c70dcfcd6ce8f19b13819f088b74688f21dd127c412,
9b52eff1cc2ab908070a1ba89059ae3f6823b43702c60272c5d5943cceb6ac0e,
7b32d917d5aa771d493c47b0e096886827cd056c82dbdba19e60baa8b2c60313
..d3b1bdb321123449c6e89d310bc6b7f654315eb471c84778353ce08b951ad471
..561fdb0dcfb8bd443718b942f82fe717238cbcf8d12b8d22861c8a09a984a3c5
..a1b1da71cc4682e159b7da23050d8b6261eb11a3247c89b07ef56ccd002fd38b
..4fd11f89c2a1aaefe856bb1c5d4a1fad73f4de5e41804ca2c17ba26d6e10050c
..86d06ee2c70da6cf2da2a828d8a9d8ef755ad6e580e838359a10accb086ae437
..ad6fdeda0dde0a57c51d3226b87e3795e6474393772da46101fd597fbd456c1b
..3f9dc0c4f67f207974123830c2d66988fb3fb44becbbba5a64143f376edc51d9,
89e2e79b6178c12684ac3a6bf9437af3a69dcc529f0021ec40bb006506837ae1
..82bf4b908e46733d3a23507791169fda8ea11b18665fe894ee9f0754c0c3fec7
..0c6b8d1444d9b604ce949cbf130642d89f72b6cb1f08e32a18cdbb00aadfdf1b

..92e630ae2b14e758ab0960e372172203f4c9a41777dadd529971d7ab9d23ab29
..fe0e9c85ec450505dde7f5ac038274cf,
ae5cf31262305cc0d061a88275a6afeed634e1c7566c79c720812529759a5845
..810a0e88b88aa8ae60f937f1ca4f21da914ad8aba8c1092777dfb212803dfd38
..9c0e3b1678c6e5e0bf02c3c8179537ca205bb3580e43016ccb584c0c08b1114a
..9756566a3bf9085c2669ccf6e6c6fb939a67624a147ebe76112bab427d22edc0
..141fe2828bd0cda558a0b16cf94ad7e4afa58b5c4a914114f7d03572b527346c
..ef906d05c896b820c8ade0122fe727bd262ee283af9b30bb67e8b926f8fa041b
..a9789444ce27e82c0caecb12c94b4a0fcb1514ee4905b644b229b1f7f8734e63
..42ee26310278b91edac541e2d20d28a826f3ee7182acf582e2f1103d90ee3a63
..69b4f91f800eff0bfc83fc9463cc100104de722c78a897f8a5bcac3fa555724d
..3cc17b108fa299caea8a5e14f12bc3da02a51af9ee175c6aea68532d1d7e0c2c
..4a87507258bd695edab7ea8d6f86c47c84c29d7fd237590fae5a2df5280c8601
..684042360445eaf6a6f6b0a38017ce2cf710004662e0a987d87929c15ee74742
..e5e0c83147132513675439c879219b61283005541826556f1700964c3345b62d
..b39e9b2db283d075ef33af3a97344467351ab3b800c29a13c5a02289d0c15868
..e3811debfe757222ea63a0f35bfb91c251ac3e4c74e838af87949b00756a363d
..f0418975ad1b8ca3cc557c6d0896c944adeaf58838f2b8b1bfabf18f05fd4abd
..41a35135149da932e3617bc2ff49f021d9aebe34ca1d3e7fab1ace2b7cfb4fd1
..b2f41416e104129b952a6b9d22d4bb0802668fbc5e2e9735c69b3f44eaff87a4
..bcd6a9a71991feaaa7e7232bc18a4733,

**Vector 2**

8b9063872331dda4c3c282f7d813fb3c13e7339b7dc9635fdc764e32cc57cb15,
5ebfe047f421e1a3e1d9bbb163839812657bbb3e4ffe9856a725b2b405844cf3,
0a,
-,
d905aaf894a97094b1d707ea7685fbc4ac501fc01cef25586a9c36288c5c6302,
25c5ab15ce5d973bfec7b6dd428b5b5971958a056d10cc18d5e9ccd0ee4c7b86,
2ae6660f435f733482e4fb6a2c743288fc1d8a6b173b01f490929cd128514c51
..8112bed1659bb8eab1535e279f9b7349fa316ba6f7bd8baa4ae410141bb565d2,
85a94726bcaeaf2db516a6a532ec2450488e7d093374f54de0ba05d2a36bb00a,
b28263558234202119a143c295a3fc5a35a6f830dd0c7018e3f33862d1986c1c,
4cb8186c3da92e9be0179f894cdc364aabe1a890340aee9fd886bed45f5017e7,
83a9519edb8ecc4f360eee599c6c1310019c4c3451ca42b4887328e347003bdf,
3e1b408e4ceb5a81e5b71527b01f541d5069438aaa279aa48c39bb7e34f24001,
1dc7b84f188a7fb5bf051464be19e54495f42bd723130992319bad7560023714,
7b32d917d5aa771d493c47b0e096886827cd056c82dbdba19e60baa8b2c60313
..d3b1bdb321123449c6e89d310bc6b7f654315eb471c84778353ce08b951ad471
..561fdb0dcfb8bd443718b942f82fe717238cbcf8d12b8d22861c8a09a984a3c5
..5ebfe047f421e1a3e1d9bbb163839812657bbb3e4ffe9856a725b2b405844cf3
..4fd11f89c2a1aaefe856bb1c5d4a1fad73f4de5e41804ca2c17ba26d6e10050c
..86d06ee2c70da6cf2da2a828d8a9d8ef755ad6e580e838359a10accb086ae437
..ad6fdeda0dde0a57c51d3226b87e3795e6474393772da46101fd597fbd456c1b
..3f9dc0c4f67f207974123830c2d66988fb3fb44becbbba5a64143f376edc51d9,

894fd4149cce66e5f39f11c0de38825da7d07c52de1d8e74ed170c6b1a2feec7
..bc158b35068bbcfa9455fd76f699c15cb5e9dfaba7a93cb264c07d9228e8c642
..73e2d5febe689b4b6279f21b1b0b26ec956f6d6d3fd5650edc1e4f7bf8d1663b
..92e630ae2b14e758ab0960e372172203f4c9a41777dadd529971d7ab9d23ab29
..fe0e9c85ec450505dde7f5ac038274cf,
b8cba6c3a415bdb4104a228dc4a431325a8d61b15786a3d7f1450387dbf2b84d
..f1568203e80a81c1293f6b0fbe4f7e6b914ad8aba8c1092777dfb212803dfd38
..9c0e3b1678c6e5e0bf02c3c8179537ca205bb3580e43016ccb584c0c08b1114a
..b758b758807789cc310a41ef5f43cffbab02c806d9cd83d3fe41879b6ee0bbf2
..99179e16cf5f6f76346215dd0ea22525a65893a06327a22dd6c5164285768387
..924e0ca971569a70bbd084fd9dbcc5c8f969fe4e3146a51e8441740b79d2a73d
..5a2eea6ad577933b99821a94b5630a03b55f44cc7c189c76834676c1d5ce492c
..e5ae09a8ecdc7830884a0125b92b38e71ee3b1142da83fd9431c4dac81fef152
..322c5bc6ed916f61e619b10c26b6c05c9fa2ddf3ac6d667bacaa602324b27b25
..cbb4f64138d23da3d647375bd60680b9cd0cc23ecd1d115ae7c4ae5581857143
..e508623ef4d7c3d9a4242309c91ad643cdbd099a451f616ec192fc45e68baa45
..2c31f3b8eb737f70105deb3318fb56f10e56ba042106a3da3c7d743b461d383e
..80f6a56ae688c6e0bcbbfbf760b0067debd79fdc39c3effae076c9133cbb9a6e
..970219c73f080bba8e32bb467f687f124c8986bcd2413f31aa39247c86c6a03e
..18617ea068d6ff5231374b028d621935826b8ae29351a9c006f4ff56e19247a7
..b8fbd55fc31eb427854bad441e3da66096994659ffc40d227668cd2c527fafab
..c92e219e57a9cff6b73532ee8c76225e7aaa402141bc0e9013b5880ee43ba547
..ac4ed2c8deec88414533eca85dc1126386c93e1427999bee8beee14d14a39f06
..3ebaba896479110b7773742af2f24a84,

**Vector 3**

6db187202f69e627e432296ae1d0f166ae6ac3c1222585b6ceae80ea07670b14,
9d97151298a5339866ddd3539d16696e19e6b68ac731562c807fe63a1ca49506,
-,
0b8c,
587f7c01731c52ce4e02405a9642bf39da4b62befa0a0811f00dd1710a975cc4,
002030eb901d08fe85873b46cd5a1bd2a2c9fbce4f15e9e39066c1fe91be1c1f,
5ca9dc5e02e908b5f1de31c85d30a064353420ab930a541db5f518eee07fb059
..323df22d2ce82d36a5bac52aa322f08072cc0b9c555a5e4179e3c11a067de7a2,
cb3a17d3578d86e2f3b23bb47160327c391c808da28c6be53ed3189d22d78205,
f99d09a38f1a1ead7d9503fd601e2d8a56c09eaeb5fb3130035803e04033b49a,
de58f590cd204247192f5b49d86c81ddc691fd6b55561fb33ccbec24ecbc86db,
d502f832afaddb7bb54e8c28cce458a2a9c3c6c230e4b85539913ec531de168b,
1dd33771a9bfdcf94e6e95fa43e4667adf3279d9c2b22e0877abeb5e99a9e01b,
7863bbac83653e1a48bc0e814e4792c6b2d884522f5556bbb1844c151dcdb700,
7b32d917d5aa771d493c47b0e096886827cd056c82dbdba19e60baa8b2c60313
..d3b1bdb321123449c6e89d310bc6b7f654315eb471c84778353ce08b951ad471
..561fdb0dcfb8bd443718b942f82fe717238cbcf8d12b8d22861c8a09a984a3c5
..9d97151298a5339866ddd3539d16696e19e6b68ac731562c807fe63a1ca49506
..4fd11f89c2a1aaefe856bb1c5d4a1fad73f4de5e41804ca2c17ba26d6e10050c

..86d06ee2c70da6cf2da2a828d8a9d8ef755ad6e580e838359a10accb086ae437
..ad6fdeda0dde0a57c51d3226b87e3795e6474393772da46101fd597fbd456c1b
..3f9dc0c4f67f207974123830c2d66988fb3fb44becbbba5a64143f376edc51d9,
a90130fa47aaf758299818bd119e7fecdddb62674541f78c5fa5371b9db62d0f
..8afd73d28225fb1ae60e8959c5f0e929b861ba122a1c8fa45fc9d2b8fb66666e
..f55fdcdfdae22addff823236613fb08b49a694b9f1ec38b72fc0a021857d3026
..92e630ae2b14e758ab0960e372172203f4c9a41777dadd529971d7ab9d23ab29
..fe0e9c85ec450505dde7f5ac038274cf,
a5b1c2890ca37ac292af4f1b736f60fdb463fd46dfc029ec1d490286cad8411d
..bd87f54a692d702c3bf63ef31789e91d914ad8aba8c1092777dfb212803dfd38
..9c0e3b1678c6e5e0bf02c3c8179537ca205bb3580e43016ccb584c0c08b1114a
..b4662ecc45202cdbb759a76aae448f7ee0e0ef12d6d4a49fe9c15a8d5fe432c6
..2073680cb2744396ca33d7c44b90b1f3a6f836fb65712a521a33bacc26103c8b
..aa81afc9a8931a7b5f9e3ea7bc5d30fef146bdfdcab3d7b92ee2bc4a9a29af38
..cb68cb84820f0c4d9c4001b18ab21f80fb4cfec3d079a7d3bed13e32a996362e
..1bf1993a39d4b6a5e75707e61f4e248da6d28fe56d22a6ef7bfe003c5361de35
..693983d2ff6be8002b0278718e4529759ab3e3a275428cdbe6788b92938ef400
..ce55785c59dd2f1f4d510abaa80c3e6655100041da2726288f81ba7a733b856b
..0f62cd45dcd49628e368b2d5fa1c5ca055fcd68a339779f3789d05cb28cf9909
..fa545aa5e98cb68a56f247e387c3cdf5c62c52cb0886d25d77061e67f3d02a4a
..409df07a6ce6e6d42e4ed84b95f2d24b31bbfdc4c10c1c6769e625f2158ff75e
..81a4bb6e4aa3b77f9ba1009ac4337b4a40e1f32f36c9fe2739a908f0961d7842
..420fec2b8ba6a74594873fa68609ba6f6174959ee58fd2823cb582120f5f1f06
..e926e6a0e03ca3041ffa8e5b59c5e549ada411c6eaa4511bc779e4f9923f0fbd
..f74511f723b015c45c77f9621a9280976aab33de095292f8846f9b3bd61b353e
..a71f1d471a3dfc5734b21c2595af996b21946699d864af09663e061afd370aa2
..d61e9b0a1a95f2e97fda089ce75df1d5,

**Vector 4**

b56cc204f1b6c2323709012cb16c72f3021035ce935fbe69b600a88d842c7407,
dc2de7312c2850a9f6c103289c64fbd76e2ebd2fa8b5734708eb2c76c0fb2d99,
73616d706c65,
-,
c1cde8432c5bf619b14a403d611140c117a52ba31004574238bd58bf8fc6181f,
5d5a673794b7a0003a1c36f299c4d61055e4b680bb3c2ccd8858dce89c6cd5d3,
0db282523110f629d8c9424afa66f4dfcb9e6dcea5f7891ab2ffc09eeb72a0ac
..11ac36841ec72644a5d24c1fa879872d3091c5e5b81940761f9f8f378f5013ae,
141a8a762dff63c7c05b26d022a8027c515e57f067b5546532296f0ca40a1909,
e926e6b3cbca7b66c42cfc603c4ef2dabc3f5e1276b20d2807f007e974675cb1,
29c56732de262411e71908326037f0f961776db2082bf3d88537265af6a57c92,
c59024c715d21f2a08fb0cd8cb24046558222c6753180853f9601d92186c5e3b,
b818a32590aeb6d79d24cdc6cacb6d5cdc58ccb7025b82be1c1ba2cd34c2f005,
e854b63f9c4e0aab3a051885498d42b5ec354e619491ee9ff239bd3fb486b509,
7b32d917d5aa771d493c47b0e096886827cd056c82dbdba19e60baa8b2c60313
..d3b1bdb321123449c6e89d310bc6b7f654315eb471c84778353ce08b951ad471

..561fdb0dcfb8bd443718b942f82fe717238cbcf8d12b8d22861c8a09a984a3c5
..dc2de7312c2850a9f6c103289c64fbd76e2ebd2fa8b5734708eb2c76c0fb2d99
..4fd11f89c2a1aaefe856bb1c5d4a1fad73f4de5e41804ca2c17ba26d6e10050c
..86d06ee2c70da6cf2da2a828d8a9d8ef755ad6e580e838359a10accb086ae437
..ad6fdeda0dde0a57c51d3226b87e3795e6474393772da46101fd597fbd456c1b
..3f9dc0c4f67f207974123830c2d66988fb3fb44becbbba5a64143f376edc51d9,
b62f3bf3e83646318894151bb51bb535a2539581773a01956f1874cb64e7a952
..809d40be330de7d34bf01162adb2675e94c21ba7db9087beeb87d536cce326fb
..20a5b816654432c73a772ede266d0d3bbae3f6aa0bcb31b5de62d33863a0098a
..92e630ae2b14e758ab0960e372172203f4c9a41777dadd529971d7ab9d23ab29
..fe0e9c85ec450505dde7f5ac038274cf,
a6e4e910b16cd26a1e1c92b407e8616a521d5640c59129e44d3c5ed3248c9fa9
..0eea775fff48c0f7596d56e321c0013f914ad8aba8c1092777dfb212803dfd38
..9c0e3b1678c6e5e0bf02c3c8179537ca205bb3580e43016ccb584c0c08b1114a
..a1c341fe390f7ef3e45fa49d12fc655ba90805eafd0dee2442ef2618208692e4
..e4931cbbf11ac60aa0384e965036023e85ff0e1317f4a1ce508a40f781596644
..a923d723c0eee4b6acc12e689cd74616ed6d5d38551e5eec82a3c4e6e462de4b
..b95d314c5883fbaa2b101576f5896af8eeb01ec35af191d94371107c79dc345f
..4823f4122a46d5eb06635b11f58e4a93cd59e91e5d7d0b30ce37b11b147f7c08
..661b89b1f0dec5b74602957c6325639cb0f4da1077442441d902799eaef9d92e
..c05d026c4282859350b82be6ee0ec3a484b9252de9522988f42144103a8c8453
..30b002c4f1da7e45b0d6e363141e3097284be9ac846113806e9d2d2123bdae43
..2bf1419d2b6ac8e83fff2bc501938fc9f39ccd8be1ae6c5520419236fc1c791a
..49219e97029ced5760d79eb5c6cb1facab6b83147eb86f6cddaa9990c9fe6f48
..8314bbfc225ed62f9cf14241a49ef9289ad537fa3f36c1fd1fde14ec79ae5eb9
..29ab90ad7d2ea5cfe4b680b8dfe42c408b547cbef65033aadf30aa369984d430
..73b2992b48e2a7e2a22da52f6872fc46afb4f8ac25e80bbd3deeb6e6bed84e9e
..b0d3a832987a1fc58c9739fb772cd89a9c352d8c055f7545735d9b38fb5b9857
..91c4f730c95137aeefb8fb591a95b0624984533b97ac182b390210312b2be0b8
..474d3e230efda6f36f276ea6e8712775,

**Vector 5**

da36359bf1bfd1694d3ed359e7340bd02a6a5e54827d94db1384df29f5bdd302,
decb0151cbeb49f76f10419ab6a96242bdc87baac8a474e5161123de4304ac29,
42616e646572736e6174636820766563746f72,
-,
8af6936567d457e80f6715f403e20597c2ca58219974c3996a4e4414c3361635,
022abfa7670d5051a6a0e212467666abb955faafe7fe63446f50eb710383444c,
126296afb914aa1225dfdddfe3bfd185b488801810e18034330b1c07409ccdc4
..f8deccfc30be219cb5186f80a523ae41720031ae39a78f18d3b14df8bb6d8e8a,
4749f32b7aa36158a4fdfb5bc7e63c40b62eb1d7c75036676e093571a3e9cb06,
e159e5494957bb478c4a4d142cde10dadd73a038f8b198c4321dff1271ab61b4,
16a8409cc245978bf55279447d854adca637a58c8c7894a0972b190ad7314492,
3639790d6414b474aa1d53de4e7a896b4e6458c078867acd22200f00f20f280a,
bbfd0996c8937c9aaabad9a254614b75c529f892fdfcfcfbe73486888545b610,

6bce65ffb002c6349213b720115ee1457214796c983618f32b4b79c8c559851b,
7b32d917d5aa771d493c47b0e096886827cd056c82dbdba19e60baa8b2c60313
..d3b1bdb321123449c6e89d310bc6b7f654315eb471c84778353ce08b951ad471
..561fdb0dcfb8bd443718b942f82fe717238cbcf8d12b8d22861c8a09a984a3c5
..decb0151cbeb49f76f10419ab6a96242bdc87baac8a474e5161123de4304ac29
..4fd11f89c2a1aaefe856bb1c5d4a1fad73f4de5e41804ca2c17ba26d6e10050c
..86d06ee2c70da6cf2da2a828d8a9d8ef755ad6e580e838359a10accb086ae437
..ad6fdeda0dde0a57c51d3226b87e3795e6474393772da46101fd597fbd456c1b
..3f9dc0c4f67f207974123830c2d66988fb3fb44becbbba5a64143f376edc51d9,
9436b3535d5dcffd6f15628fb028095f5c0733d067222f8893bb106f2fdac0f6
..3dfcf69a5715522c7318b9b311264ee5a2b499057db5d1211e6b9f4633ad433d
..22dce5f20a95b8a8618b99539bb697791e02b1afcf6e2de8240d067396196b83
..92e630ae2b14e758ab0960e372172203f4c9a41777dadd529971d7ab9d23ab29
..fe0e9c85ec450505dde7f5ac038274cf,
8af467c31da3b5e558a885b12d7ef226df7a8061e67229ab2bf39271d1c5d292
..e9ce57631c8e04d372168d669a39fc5d914ad8aba8c1092777dfb212803dfd38
..9c0e3b1678c6e5e0bf02c3c8179537ca205bb3580e43016ccb584c0c08b1114a
..b16ecd5427ea98b2ae4a7fd8492356cdc3cac256cbca4aa1bf816890794e2f78
..dbebb9a0827679bd8e2e3d4d645d05fd86355b4350c56886912878aeae1626a8
..b7dc38866c27ca62a3824e2286d125907639602f49b36bace5e98e85a0fb0a33
..09560c6efc420851f634642ddafefcc3494e904ac78b68f6a8c4c66cc5c06305
..fc39025d4b2ababf059975eb47ec3e64e93fabc0d11695e6e39cea883b83fc28
..0e13c2df6ba448b21ee03dd938e4a3b1958231255033828a9f1f16fa95768f72
..531ae8df20f04923cc20312641b4a3bc8d4c3f8524392f8ba004a02e4ac9354d
..9cdff871a6cf080db416b89e414d7895e5cb5ebccb6ac8b8c93a215185a78c71
..928cbfe0d635d6625bdde37d110bd1005da656a0b03cfe6372e8fc48f7f31f6c
..eff5c9a971012e038bf10f824bd8c8710da8b10854656e4cf48b32fe4a23de57
..96d770aff3b9a6faac33ad5a9a88f6ed524f5e6faa46bd0375bd2d07211ea2eb
..6d8341fd2e67d5bad6e71ec09ff141df80f8b1507f427d972d2d2bd30e1f1595
..6b7108371df92eafe7b1ccf7b384705d8abb439bffbeea9e9f0d7caa06ef99c0
..e4e4b32776953d16c0c7cea0a6f544d48e4eba06d1d541c51a2ac72f80b905eb
..9742dbba4aff852f64aa519eb65aac2f35b71f94c9263ef3b39a7b815b46a5f6
..d6d28374c8ebe9a6df5103f6e253a8e5,

6bce65ffb002c6349213b720115ee1457214796c983618f32b4b79c8c559851b,
7b32d917d5aa771d493c47b0e096886827cd056c82dbdba19e60baa8b2c60313
..d3b1bdb321123449c6e89d310bc6b7f654315eb471c84778353ce08b951ad471
..561fdb0dcfb8bd443718b942f82fe717238cbcf8d12b8d22861c8a09a984a3c5
..decb0151cbeb49f76f10419ab6a96242bdc87baac8a474e5161123de4304ac29
..4fd11f89c2a1aaefe856bb1c5d4a1fad73f4de5e41804ca2c17ba26d6e10050c
..86d06ee2c70da6cf2da2a828d8a9d8ef755ad6e580e838359a10accb086ae437
..ad6fdeda0dde0a57c51d3226b87e3795e6474393772da46101fd597fbd456c1b
..3f9dc0c4f67f207974123830c2d66988fb3fb44becbbba5a64143f376edc51d9,
9436b3535d5dcffd6f15628fb028095f5c0733d067222f8893bb106f2fdac0f6
..3dfcf69a5715522c7318b9b311264ee5a2b499057db5d1211e6b9f4633ad433d
..22dce5f20a95b8a8618b99539bb697791e02b1afcf6e2de8240d067396196b83
..92e630ae2b14e758ab0960e372172203f4c9a41777dadd529971d7ab9d23ab29
..fe0e9c85ec450505dde7f5ac038274cf,
8af467c31da3b5e558a885b12d7ef226df7a8061e67229ab2bf39271d1c5d292
..e9ce57631c8e04d372168d669a39fc5d914ad8aba8c1092777dfb212803dfd38
..9c0e3b1678c6e5e0bf02c3c8179537ca205bb3580e43016ccb584c0c08b1114a
..b16ecd5427ea98b2ae4a7fd8492356cdc3cac256cbca4aa1bf816890794e2f78
..dbebb9a0827679bd8e2e3d4d645d05fd86355b4350c56886912878aeae1626a8
..b7dc38866c27ca62a3824e2286d125907639602f49b36bace5e98e85a0fb0a33
..09560c6efc420851f634642ddafefcc3494e904ac78b68f6a8c4c66cc5c06305
..fc39025d4b2ababf059975eb47ec3e64e93fabc0d11695e6e39cea883b83fc28
..0e13c2df6ba448b21ee03dd938e4a3b1958231255033828a9f1f16fa95768f72
..531ae8df20f04923cc20312641b4a3bc8d4c3f8524392f8ba004a02e4ac9354d
..9cdff871a6cf080db416b89e414d7895e5cb5ebccb6ac8b8c93a215185a78c71
..928cbfe0d635d6625bdde37d110bd1005da656a0b03cfe6372e8fc48f7f31f6c
..eff5c9a971012e038bf10f824bd8c8710da8b10854656e4cf48b32fe4a23de57
..96d770aff3b9a6faac33ad5a9a88f6ed524f5e6faa46bd0375bd2d07211ea2eb
..6d8341fd2e67d5bad6e71ec09ff141df80f8b1507f427d972d2d2bd30e1f1595
..6b7108371df92eafe7b1ccf7b384705d8abb439bffbeea9e9f0d7caa06ef99c0
..e4e4b32776953d16c0c7cea0a6f544d48e4eba06d1d541c51a2ac72f80b905eb
..9742dbba4aff852f64aa519eb65aac2f35b71f94c9263ef3b39a7b815b46a5f6
..d6d28374c8ebe9a6df5103f6e253a8e5,

## Vector 6

da36359bf1bfd1694d3ed359e7340bd02a6a5e54827d94db1384df29f5bdd302,
decb0151cbeb49f76f10419ab6a96242bdc87baac8a474e5161123de4304ac29,
42616e646572736e6174636820766563746f72,
1f42,
8af6936567d457e80f6715f403e20597c2ca58219974c3996a4e4414c3361635,
022abfa7670d5051a6a0e212467666abb955faafe7fe63446f50eb710383444c,
126296afb914aa1225dfdddfe3bfd185b488801810e18034330b1c07409ccdc4
..f8deccfc30be219cb5186f80a523ae41720031ae39a78f18d3b14df8bb6d8e8a,
1f64d22282d00a58d17d4fe4dc6e8b9772109b6091e1684649c6084fc842391b,
89e230c832f5c2ee1072d9d110151a2dafa4577d64b7fb0845855ae3d1c12fec,

e3bd5e3a3f07efb256c989f22fcfe8494219dcd37b35419f5f10da68de09f125,
3639790d6414b474aa1d53de4e7a896b4e6458c078867acd22200f00f20f280a,
ceff5ef2315be8be839b1f3c0314b72d976c2e14a2a27c2d1ce8465e90c98607,
0ea7abf79fc1bdebc8b9009cc5744358071c12e82a31565d35a8f91069b55c1b,
7b32d917d5aa771d493c47b0e096886827cd056c82dbdba19e60baa8b2c60313
..d3b1bdb321123449c6e89d310bc6b7f654315eb471c84778353ce08b951ad471
..561fdb0dcfb8bd443718b942f82fe717238cbcf8d12b8d22861c8a09a984a3c5
..decb0151cbeb49f76f10419ab6a96242bdc87baac8a474e5161123de4304ac29
..4fd11f89c2a1aaefe856bb1c5d4a1fad73f4de5e41804ca2c17ba26d6e10050c
..86d06ee2c70da6cf2da2a828d8a9d8ef755ad6e580e838359a10accb086ae437
..ad6fdeda0dde0a57c51d3226b87e3795e6474393772da46101fd597fbd456c1b
..3f9dc0c4f67f207974123830c2d66988fb3fb44becbbba5a64143f376edc51d9,
9436b3535d5dcffd6f15628fb028095f5c0733d067222f8893bb106f2fdac0f6
..3dfcf69a5715522c7318b9b311264ee5a2b499057db5d1211e6b9f4633ad433d
..22dce5f20a95b8a8618b99539bb697791e02b1afcf6e2de8240d067396196b83
..92e630ae2b14e758ab0960e372172203f4c9a41777dadd529971d7ab9d23ab29
..fe0e9c85ec450505dde7f5ac038274cf,
a12e0817ce74eb4ca03e2062e1470d92173eba8d25a931b34856bace49ca0798
..199218268a5cb7eb627c3e7a4c9a37e5914ad8aba8c1092777dfb212803dfd38
..9c0e3b1678c6e5e0bf02c3c8179537ca205bb3580e43016ccb584c0c08b1114a
..a68e0243c11f79b48e15a79e552271053cb87b511a0e07d66557b0e60ff8e8eb
..6b8c00630f6f1f885569fd4de3e0565e9260fcc2be2f62922728c9aa58bc1e57
..5eb3de75aa871f738dc2e86d7cab09ec924ec3eeda5bf7e226104c93df965e46
..5c62365cb0a9d995867bab19da3cecdec967be8db19881c58358c30b778d3b4c
..783af4e70a9e2bb3be8acfb929772e717c0c533585d96ee42f12d21c7deba934
..5e07fdadb158ce200294089daaef01db40361366cb3677bacc07b656e2dd380a
..20de6c88a436bf991a97e7d783e39a71534500af00f59a4d8317735fb38d8628
..7d79a69dadbb9a7c886c125ec3169e4d931ce0aeece7cb704d2191d587210106
..9f5d02c97d44e713d8507b814c5cde061b361e4ec3d7022b2624f15fd0cbdd0f
..33462f57672c9cf12d6d20aeb03c7da7f3f25d0ccb35f295094e034eaa11b154
..8ca4d3ce10b52a176dcbf05f33a574a6e44f99715e8a2f7e8a27f530219fecc8
..994b0e595b715fd4d41027c9eeaa4438523bebdd270c9d8bb4b50baab7710877
..a410431d48e389228b9c8f4abdf6050fa4a3dd6f2204e275b0526c219636266a
..85c7005fed57d50bc53fb758af199ed53e4d4f4c8edff106a208960f52a6c18c
..a3ea8533a3e51719b2041c7769b2c6b070eeec65a24617b1168809358a97b073
..3b852f96cd63e049e7e941b872ee9055,

..ef6f0947911604155c6fe40f68cc91c96ffd358275b58960554274498a70f144,
ea1f922fce5e359d92e0fdcda53a1d2e6b791c7e7a8ffad915f3535c6175f115,
f674ad5f72661aa0c2bc5ca83aee9794c8b8bbc4017abcc00a11a23a0b558e68,
f77eaec55fe36b06f1d1f7eef7db24fdcce74c83fde19b1c322aca288e39948f,
b846dfbceb2a74fe102b3aec94e7b8460f5adcb609c407839ab6cb06d1e3bd38,
35a41d1cb4d22b5c162d319b206db940b6fcef71bbe0c13a6376a89788292519,
c04b177f954d17e7c129ce8d55cb7f148b3957078c96e7229100dc50b7d62b02,
7b32d917d5aa771d493c47b0e096886827cd056c82dbdba19e60baa8b2c60313
..d3b1bdb321123449c6e89d310bc6b7f654315eb471c84778353ce08b951ad471
..561fdb0dcfb8bd443718b942f82fe717238cbcf8d12b8d22861c8a09a984a3c5
..b0e1f208f9d6e5b310b92014ea7ef3011e649dab038804759f3766e01029d623
..4fd11f89c2a1aaefe856bb1c5d4a1fad73f4de5e41804ca2c17ba26d6e10050c
..86d06ee2c70da6cf2da2a828d8a9d8ef755ad6e580e838359a10accb086ae437
..ad6fdeda0dde0a57c51d3226b87e3795e6474393772da46101fd597fbd456c1b
..3f9dc0c4f67f207974123830c2d66988fb3fb44becbbba5a64143f376edc51d9,
b8d97722ccfc97a5cf2cc77aa0bbf5a146dca7762b98e2b6bf4b8e34e04e214b
..28d838eb642749b18ec6b8a0d79d54a3acd644b13615f791f33d648026ed6e16
..9bd516e3413b47ea35c9a8879bc1290d9fea32db7f127ecb33185d102875de50
..92e630ae2b14e758ab0960e372172203f4c9a41777dadd529971d7ab9d23ab29
..fe0e9c85ec450505dde7f5ac038274cf,
98d4f4aa83e7332f2598162283b79c2e09a499623a91dd95bea57ad90cd44bfa
..4bb53ee7c8296272ecfc13821eeab57b914ad8aba8c1092777dfb212803dfd38
..9c0e3b1678c6e5e0bf02c3c8179537ca205bb3580e43016ccb584c0c08b1114a
..83ac15b9d6ebb93fa8dae235893cc41ebd891e1a6dce2ec79ade16223becd3bb
..ec2124a36e035e2f0abf3811c499af3181abdc9cd113da1aa2b8a43c89d7576b
..0570fb7a273d3cde227429acbd034c761f97c0f681a38dc654f90e5c6c983cbd
..0eda1561f831d3fbea4702dcdb4ff16bdc81aadc27338a1858df812ac179f82a
..88acc5774b63f49d8bcde61578ff0c9a7cbda80b5a0f6fb5a80a56f4c403570d
..41cb30835b46489c1d52507e13f639984d783608d6b54335384bd580c57ff10c
..4cc8c86403bcc8d86b67a51cf4a28a571363e17d42ca7f229672ed3a5891ee3a
..a5d0a3a5cf716c8c5fbce739123d2a0965388193ecadd3e9b9d20d390c19e841
..bf85b8b981ae23a36542f3724e13448c8f7f47cd55463b7e450f4ea29c85d615
..1d0cdef59645fd25a2c9ca74341b3d901e4f5a8a850454fb78da2f7c06769659
..8560291b44425e1fecce87f46113967c722675dac020e197ec36e70a6d3957a5
..d29317b23d507eccccf5c4c66c35ed83d29d7cb896109c1868739b7e7abe72d9
..d7d2e777f586efa88c85aed4273d8559984e66b683a66163ba0f30a9ed271322
..04745b711b63fc62319deb6eafd9f784121fa18a529f84422e368e1ffa0b1577
..95bb53f788e75be61241ca4506c96da94dc59ed23c788cb4b385106b9cfac0a5
..16c3be766abb7f3eb1bc3d87d6ff2335,

# References

1.

Internet Engineering Task Force *Verifiable Random Functions*; RFC Editor,

2023;

2.

Burdges, J.; Ciobotaru, O.; Alper, H.K.; Stewart, A.; Vasilyev, S. Ring Verifiable Random Functions and Zero-Knowledge Continuations 2023.

3.

Vasilyev, S. Ring Proof Technical Specification 2024.

4.

Masson, S.; Sanso, A.; Zhang, Z. Bandersnatch: A Fast Elliptic Curve Built over the Bls12-381 Scalar Field 2021.

5.

Internet Engineering Task Force *Hashing to Elliptic Curves*; RFC Editor, 2023;

6.

Internet Engineering Task Force *US Secure Hash Algorithms*; RFC Editor, 2011;