CFRG
Internet-Draft
Intended status: Informational
Expires: 4 September 2025

V. Kalos
MATTR
G. Bernstein
Grotto Networking

3 March 2025

BBS per Verifier Linkability
draft-irtf-cfrg-bbs-per-verifier-linkability-01

Abstract

The BBS Signatures scheme defined in [I-D.irtf-cfrg-bbs-signatures], describes a multi-message digital signature, that supports selectively disclosing the messages through unlinkable presentations, built using zero-knowledge proofs. Each BBS proof reveals no information other than the signed messages that the Prover chooses to disclose in that specific instance. As such, the Verifier (i.e., the recipient) of the BBS proof, may not be able to track those presentations over time. Although in many applications this is desirable, there are use cases that require the Verifier be able to track the BBS proofs they receive from the same Prover. Examples include monitoring the use of access credentials for abnormal activity, monetization etc.. This document presents the use of pseudonyms with BBS proofs.

A pseudonym, is a value that will remain constant each time a Prover presents a BBS proof to the same Verifier, but will be different (and unlinkable), when the Prover interacts with a different Verifier. This provides a way for a recipient (Verifier) to track the presentations intended for them, while also hindering them from tracking the Prover’s interactions with other Verifiers.

This Internet-Draft will expire on 4 September 2025.

Table of Contents

1. Introduction

The BBS Signature Scheme, originally described in the academic work by Dan Boneh, Xavier Boyen, and Hovav Shacham [BBS04], is a signature scheme able to sign multiple messages at once, allowing for selectively disclosing those message while not revealing the signature it self. It does so by creating unlinkable, zero-knowledge proofs-of-knowledge of a signature value on (among other) the disclosed set of messages. More specifically, the BBS Prover, will create a BBS proof that if validated by the Verifier, guarantees that the prover knows a BBS signature on the disclosed messages, guaranteeing the revealed messages authenticity and integrity.

The BBS Proof is by design unlinkable, meaning that given two different BBS proofs, there is no way to tell if they originated from the same BBS signature. This means that if a Prover does not reveal any other identifying information (for example if they are using proxies to hide their IP address etc.), the Verifier of the proof will not be able "track" or "correlate" the different proof presentations or the Provers activity via cryptographic artifacts. This helps enhance user privacy in applications where the Verifier only needs to know that the Prover is in possession of a valid BBS signature over a list of disclosed messages.

In some applications, however, the Verifier needs to track the presentations made by the Prover over time, as to provide security monitoring, monetization services, configuration persistance etc.. To promote privacy reason, the Prover should not reveal or be bound to a unique identifier that would remain constant across proof presentations to different Verifiers and which could be used to link a Provers interactions with different Verifiers.

The goal of this document is to provide a way for a Verifier to track the proof presentations that are intended for them, while at the same time not allowing the tracking of the Prover's activities with other Verifiers. This is done through the use of pseudonyms. A pseudonym as defined by this document, is a value that will be constant when the Prover presents BBS proofs to the same Verifier, but will change when the Prover interacts with different recipients (with no way to link the two distinct pseudonym values together). This is done by constructing the pseudonym value by combining a unique Verifier identifier with a unique Prover identifier.

To avoid forging requests, the Prover's identifier will be signed by the same BBS signature used to generate the BBS proof. This requires extending the BBS proof generation and verification operations with some additional computations that will be used to prove correctness of the pseudonym, i.e., that it was correctly calculated using the Verifier identifier, as well as, the undisclosed and signed Prover identifier. The Prover identifier MUST be considered secret from the point of view of the Prover, since, if it is revealed, any entity will be able to track the Prover's activity across any Verifiers.

This document will define new BBS Interfaces for use with pseudonyms, however it will not define new ciphersuites. Rather it will re-use the ciphersuites defined in Section 6 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-03.html#name-ciphersuites) of [I-D.irtf-cfrg-bbs-signatures]).

Pseudonyms when used appropriately prevent verifiers from linking prover (proof) presentations between them. We call this verifier-verifier collusion. In addition pseudonyms can be used to prevent the signer from linking prover presentations to a verifier. We call this verifier-signer collusion. This second property is not always desirable in all use cases, for example to allow tracking of purchases a controlled substance by a prover by a central authority while preventing tracking by individual shops.

1.1. Terminology

The following terminology is used throughout this document:

SK The secret key for the signature scheme.
PK The public key for the signature scheme.
L The total number of signed messages.
R The number of message indexes that are disclosed (revealed) in a proof-of-knowledge of a signature.
U The number of message indexes that are undisclosed in a proof-of-knowledge of a signature.
scalar An integer between 0 and r-1, where r is the prime order of

the selected groups, defined by each ciphersuite (see also Notation (#notation)).

generator A valid point on the selected subgroup of the curve being used that is employed to commit a value.

signature The digital signature output.

presentation_header (ph) A payload generated and bound to the context of a specific spk.

INVALID, ABORT Error indicators. INVALID refers to an error encountered during the Deserialization or Procedure steps of an operation. An INVALID value can be returned by a subroutine and handled by the calling operation. ABORT indicates that one or more of the initial constraints defined by the operation are not met. In that case, the operation will stop execution. An operation calling a subroutine that aborted must also immediately abort.

1.2. Notation

The following notation and primitives are used:

a || b Denotes the concatenation of octet strings a and b.

I \ J For sets I and J, denotes the difference of the two sets i.e., all the elements of I that do not appear in J, in the same order as they were in I.

X[a..b] Denotes a slice of the array X containing all elements from and including the value at index a until and including the value at index b. Note when this syntax is applied to an octet string, each element in the array X is assumed to be a single byte.

X[-1] Denotes the last element of the array X

range(a, b) For integers a and b, with a <= b, denotes the ascending ordered list of all integers between a and b inclusive (i.e., the integers "i" such that a <= i <= b).

length(input) Takes as input either an array or an octet string. If the input is an array, returns the number of elements of the array. If the input is an octet string, returns the number of bytes of the inputted octet string.

Terms specific to pairing-friendly elliptic curves that are relevant to this document are restated below, originally defined in [I-D.irtf-cfrg-pairing-friendly-curves].

E1, E2 elliptic curve groups defined over finite fields. This document assumes that E1 has a more compact representation than E2, i.e., because E1 is defined over a smaller field than E2. For a pairing-friendly curve, this document denotes operations in E1 and E2 in additive notation, i.e., P + Q denotes point addition and x * P denotes scalar multiplication.

G1, G2 subgroups of E1 and E2 (respectively) having prime order r.

GT a subgroup, of prime order r, of the multiplicative group of a field extension.
e G1 x G2 -> GT: a non-degenerate bilinear map.
r The prime order of the G1 and G2 subgroups.
BP1, BP2 base (constant) points on the G1 and G2 subgroups respectively.
Identity_G1, Identity_G2, Identity_GT The identity element for the G1, G2, and GT subgroups respectively.
hash_to_curve_g1(ostr, dst) -> P A cryptographic hash function that takes an arbitrary octet string as input and returns a point in G1, using the hash_to_curve operation defined in [I-D.irtf-cfrg-hash-to-curve] and the inputted dst as the domain separation tag for that operation (more specifically, the inputted dst will become the DST parameter for the hash_to_field operation, called by hash_to_curve).
point_to_octets_g1(P) -> ostr, point_to_octets_g2(P) -> ostr returns the canonical representation of the point P for the respective subgroup as an octet string. This operation is also known as serialization.
octets_to_point_g1(ostr) -> P, octets_to_point_g2(ostr) -> P returns the point P for the respective subgroup corresponding to the canonical representation ostr, or INVALID if ostr is not a valid output of the respective point_to_octets_g* function. This operation is also known as deserialization.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Key Concepts

A _pseudonym_ will be cryptographically generated for each prover-context of usage pair. Its value is dependent on a pseudonym secret (nym_secret) and a context identifier (context_id).

3.1. Context Identifier

The Context Identifier (context_id) is an octet string that represents a specific context of usage, within which, the pseudonym will have a constant value. Context Identifiers can take the form of unique Verifier Identifiers, Session Identifiers etc., depending on the needs of the application. Verifiers will be able to use the pseudonym values to track the presentations generated by a Prover, using the same signature, for that specific context.

3.2. Pseudonyms

The _pseudonym_ is a cryptographic value computed by the prover based on the nym_secret and the context_id. At a high level this is computed by hashing the context_id to the elliptic curve group G1 and then multiplying it by the nym_secret value. See Section Section 4 for details. The pseudonym is sent to a verifier along with the BBS proof.

This document defines a pseudonym as point of the G1 group different from the Identity (Identity_G1) or the base point (BP1) of G1. A pseudonym remains constant for the same context, when combined with the same signature, but is unique (and unlinkable) across different contexts. In other words, when the Prover presents multiple BBS proofs with a pseudonym to a Verifier, the pseudonym value will be constant across those presentations, if the same context_id value is used. When presenting a BBS proof with a pseudonym to a different context, the pseudonym value will be different. Note that since pseudonyms are group points, their value will necessarily change if a different a ciphersuite with a different curve will be used. Serialization and deserialization of the pseudonym point MUST be done using the point_to_octets_g1 and octets_to_point_g1 defined by the BBS ciphersuite used (see Section 6 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-03.html#name-ciphersuites) of [I-D.irtf-cfrg-bbs-signatures]).

This document specifies pseudonyms to be BBS Interface specific (see Section TBD of [I-D.irtf-cfrg-bbs-signatures] for the definition of the BBS Interface). It is outside the scope of this document to provide a procedure for "linking" the pseudonyms that are used by different Interfaces or that are based on different ciphersuites. An option is for the Prover to present both pseudonyms with the relevant BBS proofs to the Verifier, and upon validation of both, the Verifier to internally link the 2 pseudonyms together.

3.3. Mapping Messages to Scalars

Each BBS Interface defines an operation that will map the inputted messages to scalar values, required by the core BBS operations. Each Interface can use a different mapping procedure, as long as it comforts to the requirements outlined in [I-D.irtf-cfrg-bbs-signatures]. For using BBS with pseudonyms, the mapping operation used by the interface is REQUIRED to additionally adhere the following rule;

For each set of messages and separate message msg',
if C1 = messages_to_scalars(messages.push(msg')),
and msg_prime_scalar = messages_to_scalars((msg')),
and C2 = messages_to_scalars(messages).push(msg_prime_scalar),
it will always hold that C1 == C2.

Informally, the above means that each message is mapped to a scalar independently from all the other messages. For example, if a = messages_to_scalars((msg_1)) and b = messages_to_scalars((msg_2)), then (a, b) = messages_to_scalars((msg_1, msg_2)). Its trivial to see that the messages_to_scalars operation that is defined in Section TBD of [I-D.irtf-cfrg-bbs-signatures], has the required property. That operation will be used by the Interface defined in this document to map the messages to scalars. Note that the above operation (and hence the defined by this document Interface), only accepts messages that are octet strings.

4. Pseudonym Calculation Procedure

The following section describes how to calculate a pseudonym from a secret held by the Prover and the public context unique identifier. The pseudonym will be unique for different contexts (e.g., unique Verifier identifiers) and constant under constant inputs (i.e., the same context_id and nym_secret). The context_id is an octet string representing the unique identifier of the context in which the pseudonym will have the same value. The nym_secret value is a scalar calculated from secret input provided by the Prover and random (but not secret) input provided by the Signer. This will guarantee uniqueness of the nym_secret between different signatures and users.

pseudonym = hash_to_curve_g1(context_id) * nym_secret

Additionally, the nym_secret value will be signed by the BBS Signature. This will bind the pseudonym to a specific signature, held by the Prover. During proof generation, along the normal BBS proof, the Prover will generate a proof of correctness of the pseudonym, i.e., that it has the form described above, and that it was constructed using a nym_secret signed by the BBS signature used to generate that proof.

5. High Level Procedures and Information Flows

To prevent forgeries in all cases all BBS messages are signed with the inclusion of some form of the provider pseudonym secret (nym_secret). In addition the pseudonym is always computed by the prover and sent with the proof to the verifier. While two different variations of signature and proof generation are given below based on the previously discussed unlinkability requirements there MUST be

only one verification algorithm for the verifier to use.

1. The Prover computes their input for the nym_secret (called prover_nym) and retained for use when calculating the nym_secret value.
2. The Prover will wrap up in a cryptographic commitment using the _CommitWithNym_ procedures of Blind BBS the messages they want to include in the signature (committed_messages) and the prover_nym value, generating a commitment_with_proof and a secret_prover_blind.
3. The commitment_with_proof is conveyed to the signer which then uses the signing procedures in Section Section 6.1 to create a BBS signature and their input for the nym_secret value, called signer_nym_entropy. They will convey both to the Prover.
4. On receipt of the signature and the signer_nym_entropy value, the Prover verifies the signature using the procedure of section Section 6.1 and calculates the nym_secret value by adding their prover_nym secret and the provided signer_nym_entropy values.
5. The Prover computes the _pseudonym_ based on the nym_secret and the pseudonym's context identifier context_id.
6. The Prover generates a proof using nym_secret, secret_prover_blind, signature, messages, committed_messages and the indexes of the messages to be reveled from those two lists (i.e., disclosed_indexes and disclosed_committed_indexes) using the procedures of Section Section 6.2.
7. The Prover conveys the proof and pseudonym to the verifier. The verifier uses the procedure of Section Section 6.3 to verify the proof.

6. BBS Pseudonym Interface

The following section defines a BBS Interface that will make use of per-origin pseudonyms where the nym_secret value is only known to the prover. The identifier of the Interface, api_id, is defined as ciphersuite_id || H2G_HM2S_PSEUDONYM_, where ciphersuite_id the unique identifier of the BBS ciphersuite used, as is defined in Section 6 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-03.html#name-ciphersuites) of [I-D.irtf-cfrg-bbs-signatures]).

The prover create a nym_secret value and keeps it secret. Only sending a commitment with the proof of the nym_secret that the signer will used when creating the signature.

6.1. Signature Generation and Verification with Pseudonym

6.1.1. Commitment

This section will describe the steps with which the Signer will generate a blind signature over an array of messages provided (and committed) by the Prover (committed_messages) and a pseudonym secret prover_nym, also chosen by the Prover. During signature generation, the Signer will provide their own randomness into the pseudonym secret. This will ensure that the pseudonym secret will always be unique, among different signature generation events.

This section will provide a high level description of the required operations, by detailing the modifications required in the relevant BBS blind signature operations, to also consider the use of pseudonyms. The full formal description of the operation can be seen at Appendix. We will reference those operations where appropriate in this section.

Initially, the Prover will chose a set of messages committed_messages that they want to be included in the signature, without reveling them to the Signer. They will also choose their part of the pseudonym secret prover_nym as a random scalar value.

```
(commitment_with_proof, secret_prover_blind) = CommitWithNym(
                                                  committed_messages,
                                                  prover_nym,
                                                  api_id)
```

Inputs:

- committed_messages (OPTIONAL), a vector of octet strings. If not supplied it defaults to the empty array ("()").
- prover_nym (OPTIONAL), a random scalar value. If not supplied, it defaults to the zero scalar (0).
- api_id (OPTIONAL), octet string. If not supplied it defaults to the empty octet string ("").

Outputs:

- (commitment_with_proof, secret_prover_blind), a tuple comprising from an octet string and a random scalar in that order.

Procedure:

```
1. committed_message_scalars = BBS.messages_to_scalars(
                                              committed_messages, api_id)
2. committed_message_scalars.append(prover_nym)

3. blind_generators = BBS.create_generators(
                                  length(committed_message_scalars) + 1,
                                  "BLIND_" || api_id)

4. return Blind.CoreCommit(committed_message_scalars,
                           blind_generators, api_id)
```

6.1.2. Blind Issuance

The Signer generate a signature from a secret key (SK), the commitment with proof, the signer_nym_entropy and optionally over a header and vector of messages using the BlindSignWithNym procedure shown below.

Typically the signer_nym_entropy will be a fresh random scalar, however in the case of "reissue" of a signature for a prover who wants to keep their same pseudonymous identity this value can be reused for the same prover if desired.

```
BlindSignWithNym(SK, PK, commitment_with_proof, signer_nym_entropy,
                 header, messages)

Inputs:

- SK (REQUIRED), a secret key in the form outputted by the KeyGen
                 operation.
- PK (REQUIRED), an octet string of the form outputted by SkToPk
                 provided the above SK as input.
- commitment_with_proof (OPTIONAL), an octet string, representing a
                                    serialized commitment and
                                    commitment_proof, as the first
                                    element outputted by the CommitWithNym
                                    operation. If not supplied, it
                                    defaults to the empty string ("").
- signer_nym_entropy (REQUIRED), a scalar value.
- header (OPTIONAL), an octet string containing context and application
                     specific information. If not supplied, it defaults
                     to an empty string ("").
- messages (OPTIONAL), a vector of octet strings. If not supplied, it
                       defaults to the empty array ("()").

Deserialization:

1. L = length(messages)

// calculate the number of blind generators used by the commitment,
// if any.
2. M = length(commitment_with_proof)
3. if M != 0, M = M - octet_point_length - octet_scalar_length
4. M = M / octet_scalar_length
5. if M < 0, return INVALID

Procedure:

1.  generators = BBS.create_generators(L + 1, api_id)
2.  blind_generators = BBS.create_generators(M, "BLIND_" || api_id)

3.  commit = Blind.deserialize_and_validate_commit(commitment_with_proof,
                                                   blind_generators, api_id)
4.  if commit is INVALID, return INVALID

5.  message_scalars = BBS.messages_to_scalars(messages, api_id)

6.  res = B_calculate(signer_nym_entropy, message_scalars,
                      generators, blind_generators[-1])
7.  if res is INVALID, return INVALID
8.  B = res
```

```
9.  blind_sig = Blind.FinalizeBlindSign(SK,
                                        PK,
                                        B,
                                        generators,
                                        blind_generators,
                                        header,
                                        api_id)

10. if blind_sig is INVALID, return INVALID
11. return blind_sig
```

6.1.2.1. Calculate B

The B_calculate_with_nym operation is defined as follows,

```
B = B_calculate_with_nym(signer_nym_entropy, generators,
                                                commitment,
                                                nym_generator,
                                                message_scalars)
```

Inputs:

- signer_nym_entropy (REQUIRED), a scalar.
- generators (REQUIRED), an array of at least one point from the G1 group.
- commitment (REQUIRED), a point from the G1 group
- nym_generator (REQUIRED), a point from the G1 group
- message_scalars (OPTIONAL), an array of scalar values. If not supplied, it defaults to the empty array ("()").

Deserialization:

1. L = length(messages)
2. if length(generators) != L + 1, return INVALID
3. (Q_1, H_1, ..., H_L) = generators

Procedure:

1. B = Q_1 + H_1 * msg_1 + ... + H_L * msg_L + commitment
2. signer_nym_entropy = get_random(1)
3. B = B + nym_generator * signer_nym_entropy
4. If B is Identity_G1, return INVALID
5. return B

6.1.3. Verification and Finalization

The following operation both verifies the generated blind signature, as well as calculating and returning the final nym_secret, used to calculate the pseudonym value during proof generation.

This operation uses the BlindBBS.Verify function as defined in Section 4.2.2 (https://www.ietf.org/archive/id/draft-kalos-bbs-blind-signatures-01.html#name-blind-signature-verificatio) of the Blind BBS document [BlindBBS]

```
nym_secret = VerifyFinalizeWithNym(PK,
                      signature,
                      header,
                      messages,
                      committed_messages,
                      prover_nym,
                      signer_nym_entropy,
                      secret_prover_blind)
```

Inputs:

- PK (REQUIRED), an octet string of the form outputted by the SkToPk operation.
- signature (REQUIRED), an octet string of the form outputted by the Sign operation.
- header (OPTIONAL), an octet string containing context and application specific information. If not supplied, it defaults to an empty string.
- messages (OPTIONAL), a vector of octet strings. If not supplied, it defaults to the empty array "()".
- committed_messages (OPTIONAL), a vector of octet strings. If not supplied, it defaults to the empty array "()".
- prover_nym (OPTIONAL), scalar value. If not supplied, it defaults to the zero scalar (0).
- signer_nym_entropy (OPTIONAL), a scalar value. If not supplied, it defaults to the zero scalar (0).
- secret_prover_blind (OPTIONAL), a scalar value. If not supplied it defaults to zero "0".

Outputs:

- nym_secret, a scalar value; or INVALID.

Procedure:

1. (message_scalars, generators) = Blind.prepare_parameters(

```
                                        messages,
                                        committed_messages,
                                        length(messages) + 1,
                                        length(committed_messages) + 2,
                                        secret_prover_blind,
                                        api_id)

2. nym_secret = prover_nym + signer_nym_entropy (modulo r)
3. message_scalars.append(nym_secret)

4. res = BBS.CoreVerify(PK, signature, generators, header,
                                                  message_scalars, api_id)

5. if res is INVALID, return INVALID
6. return nym_secret
```

6.2. Proof Generation with Pseudonym

This section defines the ProofGenWithNym operations, for calculating a BBS proof with a pseudonym. The BBS proof is extended to include a zero-knowledge proof of correctness of the pseudonym value, i.e., that is correctly calculated using the (undisclosed) pseudonym secret (nym_secret), and that is "bound" to the underlying BBS signature (i.e., that the nym_secret value is signed by the Signer).

Validating the proof (see ProofVerifyWithNym defined in Section 6.3), guarantees authenticity and integrity of the header, presentation header and disclosed messages, knowledge of a valid BBS signature as well as correctness and ownership of the pseudonym.

To support pseudonyms, the ProofGenWithNym procedure takes the pseudonym secret nym_secret, as well as the context identifier context_id, which the pseudonym will be bounded to.

```
(proof, pseudonym) = ProofGenWithNym(PK,
                        signature,
                        header,
                        ph,
                        nym_secret,
                        context_id,
                        messages,
                        committed_messages,
                        disclosed_indexes,
                        disclosed_commitment_indexes,
                        secret_prover_blind)
```

Inputs:

- PK (REQUIRED), an octet string of the form outputted by the SkToPk operation.
- signature (REQUIRED), an octet string of the form outputted by the Sign operation.
- header (OPTIONAL), an octet string containing context and application specific information. If not supplied, it defaults to an empty string.
- ph (OPTIONAL), an octet string containing the presentation header. If not supplied, it defaults to an empty string.
- messages (OPTIONAL), a vector of octet strings. If not supplied, it defaults to the empty array "()".
- committed_messages (OPTIONAL), a vector of octet strings. If not supplied, it defaults to the empty array "()".
- disclosed_indexes (OPTIONAL), vector of unsigned integers in ascending order. Indexes of disclosed messages. If not supplied, it defaults to the empty array "()".
- disclosed_commitment_indexes (OPTIONAL), vector of unsigned integers in ascending order. Indexes of disclosed committed messages. If not supplied, it defaults to the empty array "()".
- secret_prover_blind (OPTIONAL), a scalar value. If not supplied it defaults to zero "0".

Parameters:

- api_id, the octet string ciphersuite_id || "BLIND_H2G_HM2S_", where ciphersuite_id is defined by the ciphersuite and "BLIND_H2G_HM2S_"is an ASCII string composed of 15 bytes.

Outputs:

- proof, an octet string; or INVALID.

Deserialization:

1. L = length(messages)
2. M = length(committed_messages)
3. if length(disclosed_indexes) > L, return INVALID
4. for i in disclosed_indexes, if i < 0 or i >= L, return INVALID
5. if length(disclosed_commitment_indexes) > M, return INVALID
6. for j in disclosed_commitment_indexes, if i < 0 or i >= M, return INVALID

Procedure:

```
1. (message_scalars, generators) = Blind.prepare_parameters(
                                        messages,
                                        committed_messages,
                                        L + 1,
                                        M + 2,
                                        secret_prover_blind,
                                        api_id)
2. message_scalars.append(nym_secret)

3. indexes = ()
4. indexes.append(disclosed_indexes)
5. for j in disclosed_commitment_indexes: indexes.append(j + L + 1)

6. (proof, pseudonym) = CoreProofGenWithNym(PK,
                                signature,
                                generators.append(blind_generators),
                                header,
                                ph,
                                context_id,
                                message_scalars.append(committed_message_scalars),
                                indexes,
                                api_id)
7. return (proof, pseudonym)
```

6.3. Proof Verification with Pseudonym

This operation validates a BBS proof with a pseudonym, given the Signer's public key (PK), the proof, the pseudonym, the context identifier that was used to create it, a header and presentation header, the disclosed messages and committed messages as well as the, the indexes those messages had in the original vectors of signed messages. Validating the proof also validates the correctness and ownership by the Prover of the received pseudonym.

```
result = ProofVerifyWithNym(PK,
                                  proof,
                                  header,
                                  ph,
                                  pseudonym,
                                  context_id,
                                  L,
                                  disclosed_messages,
                                  disclosed_committed_messages,
                                  disclosed_indexes,
                                  disclosed_committed_indexes)
```

Inputs:

- PK (REQUIRED), an octet string of the form outputted by the SkToPk operation.
- proof (REQUIRED), an octet string of the form outputted by the ProofGen operation.
- header (OPTIONAL), an optional octet string containing context and application specific information. If not supplied, it defaults to the empty octet string ("").
- ph (OPTIONAL), an octet string containing the presentation header. If not supplied, it defaults to the empty octet string ("").
- L (OPTIONAL), an integer, representing the total number of Signer known messages if not supplied it defaults to 0.
- disclosed_messages (OPTIONAL), a vector of octet strings. If not supplied, it defaults to the empty array ("()").
- disclosed_indexes (OPTIONAL), vector of unsigned integers in ascending order. Indexes of disclosed messages. If not supplied, it defaults to the empty array ("()").

Parameters:

- api_id, the octet string ciphersuite_id || "H2G_HM2S_", where ciphersuite_id is defined by the ciphersuite and "H2G_HM2S_"is an ASCII string comprised of 9 bytes.
- (octet_point_length, octet_scalar_length), defined by the ciphersuite.

Outputs:

- result, either VALID or INVALID.

Deserialization:

1. proof_len_floor = 3 * octet_point_length + 4 * octet_scalar_length
2. if length(proof) < proof_len_floor, return INVALID
3. U = floor((length(proof) - proof_len_floor) / octet_scalar_length)
4. total_no_messages = length(disclosed_indexes) + length(disclosed_committed_indexes) + U - 1
5. M = total_no_messages - L

Procedure:

1. (message_scalars, generators) = Blind.prepare_parameters(
   disclosed_messages,
   disclosed_committed_messages,
   L + 1,

```
                                        M + 1,
                                        NONE,
                                        api_id)

2. indexes = ()
3. indexes.append(disclosed_indexes)
4. for j in disclosed_commitment_indexes: indexes.append(j + L + 1)

5. result = CoreProofVerifyWithNym(PK,
                                   proof,
                                   pseudonym,
                                   context_id,
                                   generators,
                                   header,
                                   ph,
                                   message_scalars,
                                   indexes,
                                   api_id)
6. return result
```

7. Core Operations

7.1. Core Proof Generation

This operations computes a BBS proof and a zero-knowledge proof of correctness of the pseudonym in "parallel" (meaning using common randomness), as to both create a proof that the pseudonym was correctly calculated using an undisclosed value that the Prover knows (i.e., the nym_secret value), but also that this value is "signed" by the BBS signature (the last undisclosed message). As a result, validating the proof guarantees that the pseudonym is correctly computed and that it was computed using the Prover identifier that was included in the BBS signature.

The operation uses the BBS.ProofInit and BBS.ProofFinalize operations defined in Section 3.7.1 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-07.html#name-proof-initialization) and Section 3.7.2 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-07.html#name-proof-finalization) correspondingly of [I-D.irtf-cfrg-bbs-signatures], the PseudonymProofInit operation defined in Section 7.3.1 and the ProofWithPseudonymChallengeCalculate defined in Section 8.1.

```
(proof, pseudonym) = CoreProofGenWithNym(PK,
                                         signature,
                                         pseudonym,
                                         verifier_id,
                                         generators,
                                         header,
                                         ph,
                                         messages,
                                         disclosed_indexes,
                                         api_id)
```

Inputs:

- PK (REQUIRED), an octet string of the form outputted by the SkToPk operation.
- signature (REQUIRED), an octet string of the form outputted by the Sign operation.
- pseudonym (REQUIRED), A point of G1, different from the Identity of G1, as outputted by the CalculatePseudonym operation.
- context_id (REQUIRED), an octet string, representing the unique proof Verifier identifier.
- generators (REQUIRED), vector of points in G1.
- header (OPTIONAL), an octet string containing context and application specific information. If not supplied, it defaults to an empty string.
- ph (OPTIONAL), an octet string containing the presentation header. If not supplied, it defaults to an empty string.
- message_scalars (OPTIONAL), a vector of scalars representing the messages. If not supplied, it defaults to the empty array "()" must include the nym_secret scalar as last element.
- disclosed_indexes (OPTIONAL), vector of unsigned integers in ascending order. Indexes of disclosed messages. If not supplied, it defaults to the empty array "()".
- api_id (OPTIONAL), an octet string. If not supplied it defaults to the empty octet string ("").

Parameters:

- P1, fixed point of G1, defined by the ciphersuite.

Outputs:

- proof, an octet string; or INVALID.

Deserialization:

```
1.  signature_result = octets_to_signature(signature)
2.  if signature_result is INVALID, return INVALID
3.  (A, e) = signature_result
4.  L = length(message_scalars)
5.  R = length(disclosed_indexes)
6.  (i1, ..., iR) = disclosed_indexes
7.  if R > L - 1, return INVALID, Note: we never reveal the nym_secret.
8.  U = L - R

// Note: nym_secret is last message and is not revealed.
9.  undisclosed_indexes = (0, 1, ..., L - 1) \ disclosed_indexes
10. (i1, ..., iR) = disclosed_indexes
11. (j1, ..., jU) = undisclosed_indexes
12. disclosed_messages = (message_scalars[i1], ..., message_scalars[iR])
13. undisclosed_messages = (message_scalars[j1], ...,
                                                    message_scalars[jU])
```

ABORT if:

```
1. for i in disclosed_indexes, i < 0 or i > L - 1, // Note: nym_secret
                                                   // is the Lth message
                                                   // and not revealed.
```

Procedure:

```
1. random_scalars = calculate_random_scalars(5+U)
2. init_res = BBS.ProofInit(PK,
                        signature_res,
                        header,
                        random_scalars,
                        generators,
                        message_scalars,
                        undisclosed_indexes,
                        api_id)
3. if init_res is INVALID, return INVALID

4. pseudonym_init_res = PseudonymProofInit(context_id,
                                           message_scalars[-1],
                                           random_scalars[-1])
5. if pseudonym_init_res is INVALID, return INVALID
6. pseudonym = pseudonym_init_res[0]

7. challenge = ProofWithPseudonymChallengeCalculate(init_res,
                                                    pseudonym_init_res,
                                                    disclosed_indexes,
                                                    disclosed_messages,
                                                    ph,
                                                    api_id)
```

```
8. proof = BBS.ProofFinalize(init_res, challenge, e_value,
                                  random_scalars, undisclosed_messages)
9. return (proof, pseudonym)
```

7.2. Core Proof Verification

This operation validates a BBS proof that also includes a pseudonym. Validating the proof, other than the correctness and integrity of the revealed messages, the header and the presentation header values, also guarantees that the supplied pseudonym was correctly calculated, i.e., that it was produced using the Verifier’s identifier and the signed (but undisclosed) Prover’s identifier, following the operation defined in Section 4.

The operation uses the BBS.ProofVerifyInit operation defined Section 3.7.3 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-07.html#name-proof-verification-initiali) of [I-D.irtf-cfrg-bbs-signatures], the PseudonymProofVerifyInit operation defined in Section 7.3.2 and the ProofWithPseudonymChallengeCalculate operation defined in Section 8.1.

```
result = CoreProofVerifyWithNym(PK,
                                    proof,
                                    pseudonym,
                                    context_id,
                                    generators,
                                    header,
                                    ph,
                                    disclosed_messages,
                                    disclosed_indexes,
                                    api_id)
```

Inputs:

- PK (REQUIRED), an octet string of the form outputted by the SkToPk operation.
- proof (REQUIRED), an octet string of the form outputted by the ProofGen operation.
- pseudonym (REQUIRED), A point of G1, different from the Identity of G1, as outputted by the CalculatePseudonym operation.
- context_id (REQUIRED), an octet string, representing the unique proof Verifier identifier.
- generators (REQUIRED), vector of points in G1.
- header (OPTIONAL), an optional octet string containing context and application specific information. If not supplied, it defaults to an empty string.

- ph (OPTIONAL), an octet string containing the presentation header. If not supplied, it defaults to an empty string.
- disclosed_messages (OPTIONAL), a vector of scalars representing the messages. If not supplied, it defaults to the empty array "()".
- disclosed_indexes (OPTIONAL), vector of unsigned integers in ascending order. Indexes of disclosed messages. If not supplied, it defaults to the empty array "()".
- api_id (OPTIONAL), an octet string. If not supplied it defaults to the empty octet string ("").

Parameters:

- P1, fixed point of G1, defined by the ciphersuite.

Outputs:

- result, either VALID or INVALID.

Deserialization:

1. proof_result = octets_to_proof(proof)
2. if proof_result is INVALID, return INVALID
3. (Abar, Bbar, r2^, r3^, commitments, cp) = proof_result
4. W = octets_to_pubkey(PK)
5. if W is INVALID, return INVALID
6. R = length(disclosed_indexes)
7. (i1, ..., iR) = disclosed_indexes

ABORT if:

1. for i in disclosed_indexes, i < 1 or i > R + length(commitments) - 1

Procedure:

1. init_res = BBS.ProofVerifyInit(PK, proof_result, header, generators, messages, disclosed_indexes, api_id)

2. pseudonym_init_res = PseudonymProofVerifyInit(pseudonym, context_id, commitments[-1], cp)
3. if pseudonym_init_res is INVALID, return INVALID

4. challenge = ProofWithPseudonymChallengeCalculate(init_res, pseudonym_init_res, disclosed_indexes,

```
                                                    messages,
                                                    ph,
                                                    api_id)
5. if cp != challenge, return INVALID
6. if e(Abar, W) * e(Bbar, -BP2) != Identity_GT, return INVALID
7. return VALID
```

7.3. Pseudonym Proof Generation Utilities

7.3.1. Pseudonym Proof Generation Initialization

```
pseudonym_init_res = PseudonymProofInit(context_id,
                                        nym_secret, random_scalar)
```

Inputs:

- context_id (REQUIRED), an octet string
- nym_secret (REQUIRED), a scalar value
- random_scalar (REQUIRED), a scalar value

Outputs:

- a tuple consisting of three elements from the G1 group, or INVALID.

Procedure:

```
1. OP = hash_to_curve_g1(context_id, api_id)
2. pseudonym = OP * nym_secret
3. Ut = OP * random_scalar
4. if pseudonym == Identity_G1 or Ut == Identity_G1, return INVALID
5. return (pseudonym, OP, Ut)
```

7.3.2. Pseudonym Proof Verification Initialization

```
pseudonym_init_res = PseudonymProofVerifyInit(pseudonym,
                                              context_id,
                                              nym_secret_commitment
                                              proof_challenge)
```

Inputs:

- pseudonym (REQUIRED), an element of the G1 group.
- context_id (REQUIRED), an octet string.
- nym_secret_commitment (REQUIRED), a scalar value.
- proof_challenge (REQUIRED), a scalar value.

Outputs:

- a tuple consisting of three elements from the G1 group, or INVALID.

Procedure:

1. OP = hash_to_curve_g1(context_id)
2. Uv = OP * nym_secret_commitment - pseudonym * proof_challenge
3. if Uv == Identity_G1, return INVALID
4. return (pseudonym, OP, Uv)

8. Utility Operations

8.1. Challenge Calculation

```
challenge = ProofWithPseudonymChallengeCalculate(init_res,
                                                 pseudonym_init_res,
                                                 i_array,
                                                 msg_array,
                                                 ph, api_id)
```

Inputs:
- init_res (REQUIRED), vector representing the value returned after initializing the proof generation or verification operations, consisting of 5 points of G1 and a scalar value, in that order.
- pseudonym_init_res (REQUIRED), vector representing the value returned after initializing the pseudonym proof, consisting of 3 points of G1.
- i_array (REQUIRED), array of non-negative integers (the indexes of the disclosed messages).
- msg_array (REQUIRED), array of scalars (the disclosed messages after mapped to scalars).
- ph (OPTIONAL), an octet string. If not supplied, it must default to the empty octet string ("").
- api_id (OPTIONAL), an octet string. If not supplied it defaults to the

empty octet string ("").

Outputs:

- challenge, a scalar.

Definitions:

1. challenge_dst, an octet string representing the domain separation tag: api_id || "H2S_" where "H2S_" is an ASCII string comprised of 4 bytes.

Deserialization:

1. R = length(i_array)
2. (i1, ..., iR) = i_array
3. (msg_i1, ..., msg_iR) = msg_array
4. (Abar, Bbar, D, T1, T2, domain) = init_res
5. (pseudonym, OP, Ut) = pseudonym_init_res

ABORT if:

1. R > 2^64 - 1 or R != length(msg_array)
2. length(ph) > 2^64 - 1

Procedure:
1. c_arr = (R, i1, msg_i1, i2, msg_i2, ..., iR, msg_iR, Abar, Bbar, D, T1, T2, pseudonym, OP, Ut, domain)
2. c_octs = serialize(c_arr) || I2OSP(length(ph), 8) || ph
3. return hash_to_scalar(c_octs, challenge_dst)

9. Security Considerations

TODO Security

10. Ciphersuites

This document does not define new BBS ciphersuites. Its ciphersuite defined in Section 6 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-03.html#name-ciphersuites) of [I-D.irtf-cfrg-bbs-signatures]) can be used to instantiate the operations of the described scheme.

11. Test Vectors

11.1. BLS12-381-SHA-256

11.1.1. Generators

```
api_id = "BBS_BLS12381G1_XMD:SHA-256_SSWU_RO_H2G_HM2S_PSEUDONYM_"

P1 = "a8ce256102840821a3e94ea9025e4662b205762f9776b3a766c872b948f1fd225e
      7c59698588e70d11406d161b4e28c9"
Q1 = "a87fa55cfc29d0d0ef43b7816018c6162b9c4a5ddd5239ed24d9799f8e105c267d
      81ccb22f6379853c4070c28c71f13c"

Generators = {

H_0 = "8c6de69580b83b7c6d773857ae64b4495955eb06e67ebc5855af89c72cd8d9bea
       9fd7f71eca20c6a3388dfa67b1e7ccf"
H_1 = "aed1785c1c00d00893413e5011ecdc98706958a2ccf175be8a42afa56ef19c86c
       a6c14afe7e74a72596704fe34b6611d"
H_2 = "b5b5142c6314a918882439b634adb926cf42a55da2962865bcf09fe746554851a
       e075d9a4a03add64a0bec997eb708a8"
H_3 = "b54f25df3ba79539da4ceb375522625518590eebd52211d40cf1083f8a9e8c1bb
       19212f1f31711fd333678002a362830"
H_4 = "8fcb548cd1e5cddba514a7f90e3b0ebd00bd82bd66158f70cc7fffdb09f14ac8f
       c56ef9587cc41a826145334444 94e75"
H_5 = "94a1d50478150c469711ccd09fa4544a590a1903f16445a4a5bc0ab639f1a4085
       80f2464972198d128f1bb4a4fa41b0b"
H_6 = "b36ceb6c0cc0850fd3a2e64fa534a1c15566f99688ec6134c5223a33de83ce553
       4d43c0973a2769ce887d5bac8481519"
H_7 = "a4e6dff6038ab2e8265d9c177d110c742bc97f3a32bd70123ecd67176181b2068
       a0ae8323db6e061e4d8e62db6f283ad"
H_8 = "90977c482711c97318d1e4c4205308847727ca7dbf3ca7d1c55f1906aeca21aae
       22b7f43e73feae41c9a9be75319015d"
H_9 = "a435ee46442dd320426a1eb163176154bb144a7f829900d0e14ec7c28d882572a
       cc1b4f670ef7cf5b41a4bea2efae6c6"

}
```

11.1.2. Blind Generators

```
api_id = "BLIND_BBS_BLS12381G1_XMD:SHA-256_SSWU_RO_H2G_HM2S_PSEUDONYM_"

P1 = "a8ce256102840821a3e94ea9025e4662b205762f9776b3a766c872b948f1fd225e
      7c59698588e70d11406d161b4e28c9"
Q1 = "a264ef107598f1caaeb323b65164bcea80e88814810efc61ea27412e879c7cb934
      4b1b513118d3cf5c79bfa81268ef36"

Blind Generators = {

J_0 = "8af923aaeaad46bf889049b2e5de19ff17778343114e589d716cde6eaa553c9e5
       4fd6805afb244e445be2939ac789b35"
J_1 = "aa6c94da21fafb4cd604029cf599df139aa88ca1cf3676fb7da1e12ec6a8dc83c
       3d7fdbf33a79e760d810c4fbac37f6a"
J_2 = "8f65ebef29b60b81447821ea2d5a201d339b0c092021bd71eeee2d1f39d4972d3
       688c98c21831490583285c12f6da579"
J_3 = "b94e4549a9ecbec9b83c004d86649f0aa6510ba292a2e68d982e79ad4de0e5bd2
       972313a95170f4c5881d7a5b790c205"
J_4 = "a1d1d4460ee7475aa66fcd4c803b11cef74a75b9d4bfe9924de20434e01f35707
       855299c9d4ead6af5b93f57d9392d56"
J_5 = "8852ab63577b0a382df12320c5fc900bce57680d47e371ced873399bd9c5adc79
       3ee890a919fb9c293e55acb4ab0312b"

}
```

11.1.3. Commit

Mocked random scalar parameters

```
seed = "3.14159265358979323846264338327 9"
dst = "BBS_BLS12381G1_XMD:SHA-256_SSWU_RO_H2G_HM2S_COMMIT_MOCK_RANDOM_SC
       ALARS_DST_"
```

11.1.3.1. valid no committed messages commitment with proof

```
committedMessages = "[  ]"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
proverBlind = "3ba0a2583bc7229fa9f2ae3a6697091032947c3a48f302b7fd2b08ca9
              d193041"

Trace:

s_tilde = "3a3b481c984f4396a13b1f65368aa393d08455fbfd351ab80f593aa5de8b4
           b1d"
m_tildes = "[ 5e82a40ae25e65fb04d7722f36ecd62fa4f07c8815e74f0a14a7e0a654
            7a36ce ]"

commitmentWithProof = "b989fc492e2047f602504eb3e236c0acb04224c77ad0d4cbd
                       31c887b9eb05a1f27d7acfb266fe0ae062914bfa060984c5c
                       2ac3247080eb71fefc7e9622ffae372425a699a298ba991a0
                       bc5c6a3d9211347d0ce98d5c0550667269df1fb81f8fa30c0
                       7d4917c7c0786411ee5c05b00b9d501d3f8e244b860b7b111
                       40cddc9787a3ab54ec7fd0a8950dae339f396f2641b"
```

11.1.3.2. valid multiple committed messages commitment with proof

```
committedMessages = "[ 5982967821da3c5983496214df36aa5e58de6fa25314af4cf
                     4c00400779f08c3, a75d8b634891af92282cc81a675972d192
                     9d3149863c1fc0, 835889a40744813a892eff9deb1edaeb, e
                     1ca9729410dc6ba,  ]"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
proverBlind = "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147
               ebf22b8"


Trace:

s_tilde = "691b0c56dff95cd15fc221a7d66ec71742fa8161a435ac51ffaa0f593b059
           89a"
m_tildes = "[ 2df678f035e3b5c2628d40645c3b53d30b77b992b4d1663aa313892d08
            a78e85, 2c0add8de9779bf9e3ba6ef2a863cec5e0375b66c44d326f3019
            14eb73cabb46, 57ea3273104c990cba7c65f88c766b013c326857be408a
            55fefea46c71f51a48, 4ffdcbebe564f0aeac3e40c58cc42964b1948b58
            1671070f85bf003ba61caafe, 19fbc9539129d0fe065c6a19d2df158820
            7232d163e098f127b270c3ad25fa08, 682afdc2c093d95b88e5e1455147
            44d9a254cace1ecd92f20cde388da9adc20f ]"

commitmentWithProof = "99efccc0ccd91efabb8821ee33edacb823b1dd999682aaa54
                       f38a9c4585e7e7aa746357b2842d38c008f6d732dd501c70e
                       ed41caf3eafdd4bb6151ce2c0289401c7d13381e7db90137d
                       7aa2a64224aa2499a4548b2654481a2f0dd16d799116fe41d
                       b7b7a5c3ae8b1c64bef6a89a46f5040a5178d2e1126f7f351
                       89f0f6cea3803e679ce92eff73856b164425ac4ff8405a934
                       f65ada8ccbe21558ab66db113662ea17ce0c9aa0280db20dc
                       f79301c61269ddfdbdcc22025b85f7089c4ebebc224a938b7
                       45daae833ac4698d9d32bfa8382b4bbb2679ae232d2f6e8e1
                       9239e6ea919665ea736b45a61bbd0e4f4d7431f3038c3db25
                       833b9a0cc1a7709419ac241fb6f02ee13e51101743f1983d3
                       fa69b5d344b984c48a265ee6a7b0df8450004ceec7c1997b8
                       59be16af624e3da2cf44"
```

11.1.4. Signature

11.1.4.1. valid no prover committed messages, no signer messages signature

```
secretKey = "60e55110f76883a13d030b2f6bd11883422d5abde717569fc0731f51237
             169fc"
publicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bbaa8fa1
             36f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632171d91aa8d46
             0acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db75c845d649ef3c4f63a
             ebc364cd55ded0c"

header = "11223344556677889900aabbccddeeff"

messages = "[  ]"

committedMessages = "[  ]"

commitmentWithProof = "b989fc492e2047f602504eb3e236c0acb04224c77ad0d4cbd
                       31c887b9eb05a1f27d7acfb266fe0ae062914bfa060984c5c
                       2ac3247080eb71fefc7e9622ffae372425a699a298ba991a0
                       bc5c6a3d9211347d0ce98d5c0550667269df1fb81f8fa30c0
                       7d4917c7c0786411ee5c05b00b9d501d3f8e244b860b7b111
                       40cddc9787a3ab54ec7fd0a8950dae339f396f2641b"

signer_nym_entropy = "3d40961fce6c09eec24a371322732932503b458d7a4cf7891b
                      daa765b30027c5"

proverBlind = "3ba0a2583bc7229fa9f2ae3a6697091032947c3a48f302b7fd2b08ca9
               d193041"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
nym_secret = "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa02
              69bbdc"

Trace:

B = "806cd9006d8c4426821c51b6620b1bac7bb33bb349338883b1cf945d192c1013b36
     60641a777ee67adc14f04d568b761"
domain = "728c2ba4c6e6a7b42c3e17c95bdf6ac83eacddd27a57dc681fbca0601c9fb3
          17"

signature = "8e0595c93044ff2da97c466418ea0eb8648f1ed5cb040f90decb338810c
             5db168a464eacba02eb9dec7659920e59409a1faff9a30512ac66886db4
             38787b463125e08e5aeaf4f4467a066dbd1520a984"
```

11.1.4.2. valid multi prover committed messages, no signer messages signature

```
secretKey = "60e55110f76883a13d030b2f6bd11883422d5abde717569fc0731f51237
             169fc"
publicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bbaa8fa1
             36f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632171d91aa8d46
             0acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db75c845d649ef3c4f63a
             ebc364cd55ded0c"

header = "11223344556677889900aabbccddeeff"

messages = "[  ]"

committedMessages = "[ 5982967821da3c5983496214df36aa5e58de6fa25314af4cf
                     4c00400779f08c3, a75d8b634891af92282cc81a675972d192
                     9d3149863c1fc0, 835889a40744813a892eff9deb1edaeb, e
                     1ca9729410dc6ba,  ]"

commitmentWithProof = "99efccc0ccd91efabb8821ee33edacb823b1dd999682aaa54
                       f38a9c4585e7e7aa746357b2842d38c008f6d732dd501c70e
                       ed41caf3eafdd4bb6151ce2c0289401c7d13381e7db90137d
                       7aa2a64224aa2499a4548b2654481a2f0dd16d799116fe41d
                       b7b7a5c3ae8b1c64bef6a89a46f5040a5178d2e1126f7f351
                       89f0f6cea3803e679ce92eff73856b164425ac4ff8405a934
                       f65ada8ccbe21558ab66db113662ea17ce0c9aa0280db20dc
                       f79301c61269ddfdbdcc22025b85f7089c4ebebc224a938b7
                       45daae833ac4698d9d32bfa8382b4bbb2679ae232d2f6e8e1
                       9239e6ea919665ea736b45a61bbd0e4f4d7431f3038c3db25
                       833b9a0cc1a7709419ac241fb6f02ee13e51101743f1983d3
                       fa69b5d344b984c48a265ee6a7b0df8450004ceec7c1997b8
                       59be16af624e3da2cf44"

signer_nym_entropy = "3d40961fce6c09eec24a371322732932503b458d7a4cf7891b
                      daa765b30027c5"

proverBlind = "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147
               ebf22b8"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
nym_secret = "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa02
              69bbdc"

Trace:

B = "b8a96f809bf8bd7081461e4ce151e4951e68e2d3210a6f59a998ef84df0f6bfdf09
     ab0fd0015f72378549bb53b82c38e"
domain = "1c63c8a9f1c732382f4803e13188d2e433a67afcd59913eeddb4082a3a832d
          ad"

signature = "b30fcb3c30a7eb5a864fadc88e2cdbce2b42bb9400b844a21e5d7ff0713
```

f3cbdf1a082572247d447fb3848bc41dfc6d73840c7e56d0f869c4bee08
aebc411e8b93b396734c96f26a4b7a708a403ff2c9"

11.1.4.3. valid no prover committed messages, multiple signer messages signature

```
secretKey = "60e55110f76883a13d030b2f6bd11883422d5abde717569fc0731f51237
             169fc"
publicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bbaa8fa1
             36f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632171d91aa8d46
             0acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db75c845d649ef3c4f63a
             ebc364cd55ded0c"

header = "11223344556677889900aabbccddeeff"

messages = "[ 9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4
            a45f02, c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811
            f5fb075f9b80, 7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932a
            a348e07b73, 77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c
            , 496694774c5604ab1b2544eababcf0f53278ff50, 515ae153e22aae04
            ad16f759e07237b4, d183ddc6e2665aa4e2f088af, ac55fb33a75909ed
            , 96012096,  ]"

committedMessages = "[  ]"

commitmentWithProof = "b989fc492e2047f602504eb3e236c0acb04224c77ad0d4cbd
                       31c887b9eb05a1f27d7acfb266fe0ae062914bfa060984c5c
                       2ac3247080eb71fefc7e9622ffae372425a699a298ba991a0
                       bc5c6a3d9211347d0ce98d5c0550667269df1fb81f8fa30c0
                       7d4917c7c0786411ee5c05b00b9d501d3f8e244b860b7b111
                       40cddc9787a3ab54ec7fd0a8950dae339f396f2641b"

signer_nym_entropy = "3d40961fce6c09eec24a371322732932503b458d7a4cf7891b
                      daa765b30027c5"

proverBlind = "3ba0a2583bc7229fa9f2ae3a6697091032947c3a48f302b7fd2b08ca9
               d193041"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
nym_secret = "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa02
              69bbdc"

Trace:

B = "a1abe3d14bd71b236c003fc1b69930dfa1cbe4f44db047bfddb5fd5c3b5a40b15c0
     ad364afce854089faa407a8cf8170"
domain = "1336f81ac1181906aa77be751b7be985adb49616287ef2f1e4b8ac7771bb61
          95"

signature = "a8c362043de23de5331483e510aafca643d7d1ace1b50003f4cc0eb2508
             68531d401e0d3af8a35dc596ef209f41b4f6f28f5c63f8a096e2a307263
             3fa624872c3f6f41fb5121b354ad7d0c0ea07e0f2f"
```

11.1.4.4. valid multiple signer and prover committed messages signature

```
secretKey = "60e55110f76883a13d030b2f6bd11883422d5abde717569fc0731f51237
             169fc"
publicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bbaa8fa1
             36f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632171d91aa8d46
             0acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db75c845d649ef3c4f63a
             ebc364cd55ded0c"

header = "11223344556677889900aabbccddeeff"

messages = "[ 9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4
            a45f02, c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811
            f5fb075f9b80, 7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932a
            a348e07b73, 77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c
            , 496694774c5604ab1b2544eababcf0f53278ff50, 515ae153e22aae04
            ad16f759e07237b4, d183ddc6e2665aa4e2f088af, ac55fb33a75909ed
            , 96012096,  ]"

committedMessages = "[ 5982967821da3c5983496214df36aa5e58de6fa25314af4cf
                     4c00400779f08c3, a75d8b634891af92282cc81a675972d192
                     9d3149863c1fc0, 835889a40744813a892eff9deb1edaeb, e
                     1ca9729410dc6ba,  ]"

commitmentWithProof = "99efccc0ccd91efabb8821ee33edacb823b1dd999682aaa54
                       f38a9c4585e7e7aa746357b2842d38c008f6d732dd501c70e
                       ed41caf3eafdd4bb6151ce2c0289401c7d13381e7db90137d
                       7aa2a64224aa2499a4548b2654481a2f0dd16d799116fe41d
                       b7b7a5c3ae8b1c64bef6a89a46f5040a5178d2e1126f7f351
                       89f0f6cea3803e679ce92eff73856b164425ac4ff8405a934
                       f65ada8ccbe21558ab66db113662ea17ce0c9aa0280db20dc
                       f79301c61269ddfdbdcc22025b85f7089c4ebebc224a938b7
                       45daae833ac4698d9d32bfa8382b4bbb2679ae232d2f6e8e1
                       9239e6ea919665ea736b45a61bbd0e4f4d7431f3038c3db25
                       833b9a0cc1a7709419ac241fb6f02ee13e51101743f1983d3
                       fa69b5d344b984c48a265ee6a7b0df8450004ceec7c1997b8
                       59be16af624e3da2cf44"

signer_nym_entropy = "3d40961fce6c09eec24a371322732932503b458d7a4cf7891b
                      daa765b30027c5"

proverBlind = "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147
               ebf22b8"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
nym_secret = "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa02
              69bbdc"
```

Trace:

```
B = "91437a9b859b8623ef0990ea1b07fc6951338042565dd4f9c59f46d95eec8cf72db
     31aacba6b1b2c958c22c47ee238ae"
domain = "4508e372d4ede742110dbcbc3e0c0d286f6d7388827b98805f7b62ad17678d
          93"

signature = "99f409633ab1140121a94508a25d3ef7fe9d7da3559408502e81331f80c
             bddb621a99c02b6bab14c44aaf35b19006a1d0a91f0ac5a47b9c0a99a29
             0c3f36debe34c00ca333a9006e769b4930e39210c8"
```

11.1.5. Proof

Mocked random scalar parameters

```
seed = "3.14159265358979323846264338327 9"
dst = "BBS_BLS12381G1_XMD:SHA-256_SSWU_RO_H2G_HM2S_PROOF_MOCK_RANDOM_SCA
       LARS_DST_"
```

11.1.5.1. valid all prover committed messages and signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "99f409633ab1140121a94508a25d3ef7fe9d7da3559408502e81331f80c
             bddb621a99c02b6bab14c44aaf35b19006a1d0a91f0ac5a47b9c0a99a29
             0c3f36debe34c00ca333a9006e769b4930e39210c8"

commitmentWithProof = "99efccc0ccd91efabb8821ee33edacb823b1dd999682aaa54
                       f38a9c4585e7e7aa746357b2842d38c008f6d732dd501c70e
                       ed41caf3eafdd4bb6151ce2c0289401c7d13381e7db90137d
                       7aa2a64224aa2499a4548b2654481a2f0dd16d799116fe41d
                       b7b7a5c3ae8b1c64bef6a89a46f5040a5178d2e1126f7f351
                       89f0f6cea3803e679ce92eff73856b164425ac4ff8405a934
                       f65ada8ccbe21558ab66db113662ea17ce0c9aa0280db20dc
                       f79301c61269ddfdbdcc22025b85f7089c4ebebc224a938b7
                       45daae833ac4698d9d32bfa8382b4bbb2679ae232d2f6e8e1
                       9239e6ea919665ea736b45a61bbd0e4f4d7431f3038c3db25
                       833b9a0cc1a7709419ac241fb6f02ee13e51101743f1983d3
                       fa69b5d344b984c48a265ee6a7b0df8450004ceec7c1997b8
                       59be16af624e3da2cf44"
proverBlind = "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147
               ebf22b8"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"
```

```
signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147ebf22b8"

context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "b04bd002c85e31d2735ee2e6b36aea85147cbf197934f99ae26a7da73b98ebc34561848
 426aded0967e07fb333f79487"

revealedMessages =

0: "9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4a45f02"
1: "c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811f5fb075f9b80"
2: "7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932aa348e07b73"
3: "77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c"
4: "496694774c5604ab1b2544eababcf0f53278ff50"
5: "515ae153e22aae04ad16f759e07237b4"
6: "d183ddc6e2665aa4e2f088af"
7: "ac55fb33a75909ed"
8: "96012096"
9: ""


revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
1: "a75d8b634891af92282cc81a675972d1929d3149863c1fc0"
2: "835889a40744813a892eff9deb1edaeb"
3: "e1ca9729410dc6ba"
4: ""

Trace:

random_scalars:

r_1 = "57af863d7be8df38f5431df51734fcc8b070d4fff721eab0737be707a0479747"
r_2 = "64e66eecfa127d5942a5f80e2482bb283080fa337eee066d9b4ee79e6e3c3fa2"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 177e9bc4a3681ab187a037fc218fb5a401a2f253c1e7a76f095
                    32a8f9be75508, 398d3a444831eeb55b89946106c9f35b7296c7
                    ce0e2e2fa66a4318c10bbb98cc ]"

domain = "4508e372d4ede742110dbcbc3e0c0d286f6d7388827b98805f7b62ad17678d
          93"
challenge = "617597a06f858d771f98e38f1a708718b838e0e50fa5ad9ca8ef61284de
             b2b3c"
```

```
L = "10"

proof = "80c5bbf18019cab0605884177 25e00cb1b21aa86d79100af2c2cf90d6f2b8a0
         42196bba6e686adaceebaad41a15ead368fbf593c7170044f4290d90484013c
         224c7104650e8eaa874f8456879988a403295aa6de5c6a00af182e68e5c01ab
         2ce8bbe372d8ec346fdd3c6cd07e857490b46c0169fa367286cda03204ef9a5
         615bfaabb50b47ab8ff77c87b890f400f49e10ada3b9b8add504356e8ec72ac
         512a20aa9b2f05e0dd58f409533d2157d36355d71d3458e86b39df14b591b84
         60f5784f9e7de26bebd3bb68d30a4a7baf55a84eda86f3d04aa375b988e550d
         81face6020808875ed84263f23252545ad66b2c2ea39d49d2fdeb716f67039b
         bb6e6e8899ebe394623be9508f3f850302fe0e530031541ba38a3a0aa195344
         002fbb453e065d22ce32ed9079baa4e553d31d0eb617597a06f858d771f98e3
         8f1a708718b838e0e50fa5ad9ca8ef61284deb2b3c"
```

11.1.5.2. valid half prover committed messages and all signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "99f409633ab1140121a94508a25d3ef7fe9d7da3559408502e81331f80c
             bddb621a99c02b6bab14c44aaf35b19006a1d0a91f0ac5a47b9c0a99a29
             0c3f36debe34c00ca333a9006e769b4930e39210c8"

commitmentWithProof = "99efccc0ccd91efabb8821ee33edacb823b1dd999682aaa54
                       f38a9c4585e7e7aa746357b2842d38c008f6d732dd501c70e
                       ed41caf3eafdd4bb6151ce2c0289401c7d13381e7db90137d
                       7aa2a64224aa2499a4548b2654481a2f0dd16d799116fe41d
                       b7b7a5c3ae8b1c64bef6a89a46f5040a5178d2e1126f7f351
                       89f0f6cea3803e679ce92eff73856b164425ac4ff8405a934
                       f65ada8ccbe21558ab66db113662ea17ce0c9aa0280db20dc
                       f79301c61269ddfdbdcc22025b85f7089c4ebebc224a938b7
                       45daae833ac4698d9d32bfa8382b4bbb2679ae232d2f6e8e1
                       9239e6ea919665ea736b45a61bbd0e4f4d7431f3038c3db25
                       833b9a0cc1a7709419ac241fb6f02ee13e51101743f1983d3
                       fa69b5d344b984c48a265ee6a7b0df8450004ceec7c1997b8
                       59be16af624e3da2cf44"
proverBlind = "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147
               ebf22b8"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147ebf22b8"
```

```
context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "b04bd002c85e31d2735ee2e6b36aea85147cbf197934f99ae26a7da73b98ebc34561848
 426aded0967e07fb333f79487"

revealedMessages =

0: "9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4a45f02"
1: "c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811f5fb075f9b80"
2: "7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932aa348e07b73"
3: "77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c"
4: "496694774c5604ab1b2544eababcf0f53278ff50"
5: "515ae153e22aae04ad16f759e07237b4"
6: "d183ddc6e2665aa4e2f088af"
7: "ac55fb33a75909ed"
8: "96012096"
9: ""


revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
2: "835889a40744813a892eff9deb1edaeb"
4: ""

Trace:

random_scalars:

r_1 = "3f7f8e5116d83e95bcc525249ad54ff216e7c4c15aad548320db23d7a7fd72cb"
r_2 = "423372f6da6b802f861ac89bb679e6725cf996040fe214fb9f98883b853ff541"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 192287eaaa219042b2217fc6fc8d39e8755bee5d61e441912f6
                    a1399cfc12d17, 27de130fd1b0a7e113950fd909bd7ad0ef5285
                    fdc2a5e098f8038018a62af4d3, 464edb5824e1a70d5d493e98b
                    ccd23abf619476e659c5de9ccf37506c48f5e7e, 005f216a7074
                    70dacafc62ac2e5a99bf9fa42373a8c8f7531d667e4ffdd65650 ]"

domain = "4508e372d4ede742110dbcbc3e0c0d286f6d7388827b98805f7b62ad17678d
          93"
challenge = "4635c8a4a27781a120bf80df9db922f9ca1ad13da46a49bb00948476030
             83b63"


L = "10"

proof = "b3609d5604e27ef07ed771fbe781640c4945f65626c1ec447e836ae27914ccc
```

```
          f69c91817af6a29d32d83c895540c9cf1b959e4cc8e689ab3b3f8b2247cd4be
          9e82cc19af253ed1785ca1a34a97267f9d301539d1f7f204816d7b91e8e32ab
          82ea30a03cf553a9c598db24b5a1da8b69aadb79e0a942321c1621035cd6d27
          5b688a5a18fe740d3e1ef58f50819940cb963ce17df31e0f03dc5d326bbbe07
          724468f3d4f693a70a98cb7cbe6bd7596c7bf592b58a7f2bf640a673d33d669
          a528a20475befc50bf69bdf78160cac32a3521419dec99be743e27d975fff70
          77e322cb163d4088be7492c3c7e2104bdaac0a84597622aac2f1c5d85fa9f19
          9fc562c001c01ac9ad614827bbd0b2d43602c2bb6d722fb78212e9d169252f7
          ad85f77e043f6cb9acf117308a7b2e8d03a77ceba4bee9a1fb735ca38048dc9
          a98c54d3bd3413b45223c59e15afb0c26f01ff66f137179d0006e1584323581
          974b75cb78493c87ffe12f432d7ed812fc95424a8c24635c8a4a27781a120bf
          80df9db922f9ca1ad13da46a49bb0094847603083b63"
```

11.1.5.3. valid all prover committed messages and half signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "99f409633ab1140121a94508a25d3ef7fe9d7da3559408502e81331f80c
             bddb621a99c02b6bab14c44aaf35b19006a1d0a91f0ac5a47b9c0a99a29
             0c3f36debe34c00ca333a9006e769b4930e39210c8"

commitmentWithProof = "99efccc0ccd91efabb8821ee33edacb823b1dd999682aaa54
                       f38a9c4585e7e7aa746357b2842d38c008f6d732dd501c70e
                       ed41caf3eafdd4bb6151ce2c0289401c7d13381e7db90137d
                       7aa2a64224aa2499a4548b2654481a2f0dd16d799116fe41d
                       b7b7a5c3ae8b1c64bef6a89a46f5040a5178d2e1126f7f351
                       89f0f6cea3803e679ce92eff73856b164425ac4ff8405a934
                       f65ada8ccbe21558ab66db113662ea17ce0c9aa0280db20dc
                       f79301c61269ddfdbdcc22025b85f7089c4ebebc224a938b7
                       45daae833ac4698d9d32bfa8382b4bbb2679ae232d2f6e8e1
                       9239e6ea919665ea736b45a61bbd0e4f4d7431f3038c3db25
                       833b9a0cc1a7709419ac241fb6f02ee13e51101743f1983d3
                       fa69b5d344b984c48a265ee6a7b0df8450004ceec7c1997b8
                       59be16af624e3da2cf44"
proverBlind = "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147
               ebf22b8"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147ebf22b8"
```

```
context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "b04bd002c85e31d2735ee2e6b36aea85147cbf197934f99ae26a7da73b98ebc34561848
 426aded0967e07fb333f79487"

revealedMessages =

0: "9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4a45f02"
2: "7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932aa348e07b73"
4: "496694774c5604ab1b2544eababcf0f53278ff50"
6: "d183ddc6e2665aa4e2f088af"
8: "96012096"

revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
1: "a75d8b634891af92282cc81a675972d1929d3149863c1fc0"
2: "835889a40744813a892eff9deb1edaeb"
3: "e1ca9729410dc6ba"
4: ""

Trace:

random_scalars:

r_1 = "4b323b402acbd18f2109d611190669d66af7d4edc0ff899d308b77cbf54a1629"
r_2 = "4224bfcae26523b6a34fc37637e74cd83cb9a61f78b6be0b15414993ccc3f057"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 03da9778016b40f396a9f237e56c3ae5cfc6d5001f328f3db98
                    448e5e1115408, 5863a317cec4996d232afdb379aaf96cdb14e1
                    02fe00b1667b1aa68feacc5099, 3f043505ceae96a3db8f12615
                    52bea2053bfd21a872408ba8e19d0fa3201dc74, 726be9c9f6af
                    8407403c731b1a7282955dc1e563ce08b7d5705ed2cb20b04040,
                     0bffdf4cf02093b2473b6d129636b21d70542048989bf92471aa
                    f7a567e5ee0a, 46782785ca90e9b6751e9301a320c5b1b299a20
                    c1989b9ee0706525dfc7ac45a, 71e38b786f98c5c77b1dac4f08
                    8aad694408882745fa24efa020549e81091d1c ]"

domain = "4508e372d4ede742110dbcbc3e0c0d286f6d7388827b98805f7b62ad17678d
          93"
challenge = "31328cfa0e1e39db013c0988dcf4978c866c1e757c67e9a729d308ca22e
             d8f0d"


L = "10"

proof = "9862cf4d03193c24f13781a02394df3f7b9ce04511592f4b8a1ec0e24331397
```

```
          ba967ea5bf1053b99f1c82e6e0351e1d0b7934c1a1d935eb89de7b45c427f0a
          550b9432d0a58f594098ba0f8f470f9f2e4c8b4a50736d3b51d3810fa18d4b3
          43883e607bcc4bdc4e76a5b39161ca96391354facdfa4fa47cc5b0fe1bd9176
          8f20139e599d4ee9bbc231bf3044cf2385d768b0ebf68e5ce4d8cc846fb7c6b
          d8f641e44a68170462ce0d5204045544c60a5183b0116de517928cb1aadb5e5
          9c89c8a77bc0df77de9fb1134d66ca9454f0cf603952748fd41c40dbaa4d9ef
          1b309804ec7f158db099fcd0c7866b6b3336ff3406ea07011efa8af032b60ab
          5e93baa20db28a5b31478ebbd9440f33d69028a23339683c120fdd978369b26
          d05a2a029c76f5277fb058431623a2c9be517ba4b619c942be097ddf277c988
          4aa3fc9faae80f3dafaa2ad535721c247760838a603842da75da3ba276344f4
          cf0713c91b76df021356e667db02b70f714ab71d966664d9e679f1527473a3f
          fa9c930782a8f349b8dceade0fb6b8121a276ab689fe5330cf4e6d5650b13ac
          4a8ab4930da894f94d2dae09fc94e664dd8490fee8a7d5a7dd52f10f88c828d
          7ea137fb95103edd7cc5497ed3e98bc2c6582e34234d2131328cfa0e1e39db0
          13c0988dcf4978c866c1e757c67e9a729d308ca22ed8f0d"
```

11.1.5.4. valid all prover committed messages and signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "99f409633ab1140121a94508a25d3ef7fe9d7da3559408502e81331f80c
             bddb621a99c02b6bab14c44aaf35b19006a1d0a91f0ac5a47b9c0a99a29
             0c3f36debe34c00ca333a9006e769b4930e39210c8"

commitmentWithProof = "99efccc0ccd91efabb8821ee33edacb823b1dd999682aaa54
                       f38a9c4585e7e7aa746357b2842d38c008f6d732dd501c70e
                       ed41caf3eafdd4bb6151ce2c0289401c7d13381e7db90137d
                       7aa2a64224aa2499a4548b2654481a2f0dd16d799116fe41d
                       b7b7a5c3ae8b1c64bef6a89a46f5040a5178d2e1126f7f351
                       89f0f6cea3803e679ce92eff73856b164425ac4ff8405a934
                       f65ada8ccbe21558ab66db113662ea17ce0c9aa0280db20dc
                       f79301c61269ddfdbdcc22025b85f7089c4ebebc224a938b7
                       45daae833ac4698d9d32bfa8382b4bbb2679ae232d2f6e8e1
                       9239e6ea919665ea736b45a61bbd0e4f4d7431f3038c3db25
                       833b9a0cc1a7709419ac241fb6f02ee13e51101743f1983d3
                       fa69b5d344b984c48a265ee6a7b0df8450004ceec7c1997b8
                       59be16af624e3da2cf44"
proverBlind = "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147
               ebf22b8"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
```

```
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147ebf22b8"

context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "b04bd002c85e31d2735ee2e6b36aea85147cbf197934f99ae26a7da73b98ebc34561848
 426aded0967e07fb333f79487"

revealedMessages =

0: "9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4a45f02"
2: "7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932aa348e07b73"
4: "496694774c5604ab1b2544eababcf0f53278ff50"
6: "d183ddc6e2665aa4e2f088af"
8: "96012096"


revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
2: "835889a40744813a892eff9deb1edaeb"
4: ""

Trace:

random_scalars:

r_1 = "54cd5cce27924327e7b102c514e3ef1ba9f1f9baad1117804203ab8825dfec30"
r_2 = "5f24156b67c03f1d3bf0b9c6f465b21768a84b0f08a75545d9cae648647cc5f9"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 1ba2fb229bd500bb65ed4fb9c44eff2a0bfb3b335bb28548e72
                   9ca10fdd34849, 0bc5a2dde5a559d01f61a4b291391e3f238735
                   726a723dd69954649d84a47ed1, 07c41f1b4ea44a3bafab37e42
                   76d7585b17ce82afd1dd099071d63677dd49298, 737db4fb5754
                   1bea9d125581faa7f2ccea4de7c4f101456b8bae7ae6bda72ea7,
                    0d92794b70ef2b6f56cf03192b9a3714df9503629081053f13f8
                   d12d9e7d79a7, 269df3a0585467568b6f88abedaa986297f33f4
                   aa069f13cd392ec49426866b8, 4a6c5ac852ddc2ef9f735647f9
                   59416dd8f2b78c56580dc1d4bf57993611b970, 1f167fd08394e
                   520dba66007180fbec6ea5b88ad87a4bdc21acdd80ccfa3e5e0,
                   3a870cc60dc5b1083cdd510fcfda6d23c8c9bde556584ddc9f703
                   78eb7515b0f ]"

domain = "4508e372d4ede742110dbcbc3e0c0d286f6d7388827b98805f7b62ad17678d
          93"
challenge = "2748906732822a82890eb57f7561c8b5db183574eff0fafc91eb05ca800
             72e1d"
```

```
L = "10"

proof = "8a62e1920818e649ed51e28aacf1eb069dc06817882b6c5018801c3acfff44a
         6d311ec93ba167ad6538de41aa08f8b37970916033aefb249f7d458f9e10f63
         031cb1c45cc64b094d07dd4cac6b2341b31a454581ae68b59eb7fc56cfac702
         ff792abc5535f3fc5db8e0765fb902d648b64d8640d6bb53f09553ba8c1e125
         de902abf7a3aa01b541e0a97c2895fc452570bd08e5b513b1d416c3c43b8817
         688b906b67c7eab1e39bdcd1f72159c657bc15252e9747d127ec276a560cf51
         df9d56d595a27a804dd219dc202afe946a14543f44ef35f10dc02e00264b590
         af5a4dbd2271eaf67d6701aac36f781d7278e321d023d8ef84426176b3aa6b1
         42e18cbe0dd4b66fd1b740d700b38f48714aaa7857bcb869dbc53971c58ae9f
         521005a6d73b4cd6b86a4e75af543477dc16fb9685145d1c847a8912577bbfd
         5367a5d9dce109b5b50e30a58a4ba349afe98183730fdbf9baeeda7efb9c259
         2d33c6a06294b048c9c7ae97f5e53610399c57385aa0afb15864255c6891a72
         c3e668afd970bc832694c6faff88ede68b04932b28914bdfa291bf16a742652
         8b25f4f2df26c2816a341ab3c5473a42ed5d54b91c16a0a4c16b3556a768fe0
         b33de2e06fe4d0d634746d1bed19363c9d1b779e1b39b846d660b16c66baa30
         b377800b3cbecde0a2a96a6672af4dd6178c24e1396ead043bd37eaeb27e027
         c18581a523ad9cc311cab68b972b7143eecaa519c8149940274890673282 2a8
         2890eb57f7561c8b5db183574eff0fafc91eb05ca80072e1d"
```

11.1.5.5. valid all prover committed messages and signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "99f409633ab1140121a94508a25d3ef7fe9d7da3559408502e81331f80c
             bddb621a99c02b6bab14c44aaf35b19006a1d0a91f0ac5a47b9c0a99a29
             0c3f36debe34c00ca333a9006e769b4930e39210c8"

commitmentWithProof = "99efccc0ccd91efabb8821ee33edacb823b1dd999682aaa54
                       f38a9c4585e7e7aa746357b2842d38c008f6d732dd501c70e
                       ed41caf3eafdd4bb6151ce2c0289401c7d13381e7db90137d
                       7aa2a64224aa2499a4548b2654481a2f0dd16d799116fe41d
                       b7b7a5c3ae8b1c64bef6a89a46f5040a5178d2e1126f7f351
                       89f0f6cea3803e679ce92eff73856b164425ac4ff8405a934
                       f65ada8ccbe21558ab66db113662ea17ce0c9aa0280db20dc
                       f79301c61269ddfdbdcc22025b85f7089c4ebebc224a938b7
                       45daae833ac4698d9d32bfa8382b4bbb2679ae232d2f6e8e1
                       9239e6ea919665ea736b45a61bbd0e4f4d7431f3038c3db25
                       833b9a0cc1a7709419ac241fb6f02ee13e51101743f1983d3
                       fa69b5d344b984c48a265ee6a7b0df8450004ceec7c1997b8
                       59be16af624e3da2cf44"
proverBlind = "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147
               ebf22b8"
```

```
header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147ebf22b8"

context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "b04bd002c85e31d2735ee2e6b36aea85147cbf197934f99ae26a7da73b98ebc34561848
 426aded0967e07fb333f79487"

revealedMessages =

0: "9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4a45f02"
2: "7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932aa348e07b73"
4: "496694774c5604ab1b2544eababcf0f53278ff50"
6: "d183ddc6e2665aa4e2f088af"
8: "96012096"

revealedCommittedMessages  = {}


Trace:

random_scalars:

r_1 = "3225bff980c15ebad66698a30058f01c7f1dc6c6cc2b959e974c11f2a1aecc15"
r_2 = "57ced773ccd372849c758db968e99c36495478640309379d6cab21383a965ce5"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 60154b04a4c98255e7aef7b9d08452445b613cd407cbe2ae9d4
                    2371e89b9a95b, 70cc1da93eabc0785d2847d89eb73b723e34c3
                    005acd39a41ff1e3954a10fa70, 19521e59845a027b89750643f
                    be7779c70965a624b0be492eef6f9f305442184, 4cce86548146
                    37741ad543a7e8844b6e737b35e7e3c5830cf171fb5bcb8e461e,
                     27b95c59ffe0163b480e802a8d713f5da75a6ead37d5cff34047
                    70777518849b, 3d4295c7724de36f339340e98216e78bfefa4be
                    8172e6c7c3bc024868c8aa8d7, 1e0f8fd41c7562a915cc9069d7
                    7f91afe2a6dea1168e06c53dc2c992f653225b, 3017a9528ac1b
                    f01ee7fcc37477ebc88239be178b953c7165b15bb76998e7653,
                    52b7d08b79d82945295d25de22e7a604c2967c910458eddfbcd9f
                    c60e09169ba, 334ad48e9043501e7c8893ab351f4091b2e7f869
                    25e814a69375d3b9fc6aa520, 2844fcf0fce4ac751997a092e92
                    1aef4c121b3fac72c16213e4f214315279fe6, 365dd49379b57e
                    ddc85c5665b2f4f1115686b4d94674f710d76eeaf91156c6b4 ]"
```

```
domain = "4508e372d4ede742110dbcbc3e0c0d286f6d7388827b98805f7b62ad17678d
          93"
challenge = "373282dd627ee2b2dd2595deb4b502e0d8c319f49a47464ba97e6de55ad
             c99d1"


L = "10"

proof = "add3221aa11a1857cc7a42ca1a92275f4ce564f0914b181751c5a900fd4f899
         5e72ec98b9033758cbc33761549ed0b538e711dc3d91b28d4309648731ad9c7
         4915ffa9c17ded7f4df05ca10c0c44adaa4d5b945f6d008692cd14bdd59ea01
         2ef84460c9e82eaa6b55f48b0a2c3a437e72b96c568716df6fc4dcf9cce56b7
         ddc8fcc7dbcec9090ef6794e861dc8f7fea255707d38665a55aa3b6d177d428
         2b81ed0b93367dd6208700a0207abe13593d1288974c28380354320a1e73fa5
         fb974618d5a852a5e5deb3e06afe3bc82315a73dc4917f064a21eed9f702932
         588254fbed51202cc1fc0a38ca42c243816ca2b6dfefd7c76dcfad9321c1907
         371b78bef1fccd5e42be16d36757f2c0f6ef15f52ac81bd46499410f75bca59
         2b750aa596c07ca4fd6bd244c9d321f9422e8c15d504cd6614df24c75854030
         793c703dafa917e24162a4ca6aef0826597c3ba41c1586b1971334fc632f835
         05fc7dd12641aa603260b1425d896d6f363bd61ef732dc56aaf64ae6d55047d
         c52bf73c138161c16a46f995b20999a53599a48bb1ba734a3be4f4dfe1c9ff8
         1efec2d4970a0b800de0ffcbbf209c83c55c462b756d9200bbf2ccb5d007daa
         a344067037f525c63d5fa8ef51ac2d2fc7f0b380cfbd2c29996b8add5333b46
         7b4505973ba289a5d10efa4bc8ca51933ba48b16d82977f43c19bda9aff9a96
         3d12e6a1bf07357590d49d23de780ce9486c5103d25682f32931aaaa162ed80
         b9066eb60125c33e191793c910f1557f9790ffddbaea850d42e510b4661b303
         8ed606e59452ec83187b88af9488ebf83797ace665449acd054471790c1fe9a
         37bc23aa50b3dde7fe24c2de1955fda7ddcb8dfb62baf91db20373282dd627e
         e2b2dd2595deb4b502e0d8c319f49a47464ba97e6de55adc99d1"
```

11.1.5.6. valid half prover committed messages and no signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "99f409633ab1140121a94508a25d3ef7fe9d7da3559408502e81331f80c
             bddb621a99c02b6bab14c44aaf35b19006a1d0a91f0ac5a47b9c0a99a29
             0c3f36debe34c00ca333a9006e769b4930e39210c8"

commitmentWithProof = "99efccc0ccd91efabb8821ee33edacb823b1dd999682aaa54
                       f38a9c4585e7e7aa746357b2842d38c008f6d732dd501c70e
                       ed41caf3eafdd4bb6151ce2c0289401c7d13381e7db90137d
                       7aa2a64224aa2499a4548b2654481a2f0dd16d799116fe41d
                       b7b7a5c3ae8b1c64bef6a89a46f5040a5178d2e1126f7f351
                       89f0f6cea3803e679ce92eff73856b164425ac4ff8405a934
                       f65ada8ccbe21558ab66db113662ea17ce0c9aa0280db20dc
```

```
                        f79301c61269ddfdbdcc22025b85f7089c4ebebc224a938b7
                        45daae833ac4698d9d32bfa8382b4bbb2679ae232d2f6e8e1
                        9239e6ea919665ea736b45a61bbd0e4f4d7431f3038c3db25
                        833b9a0cc1a7709419ac241fb6f02ee13e51101743f1983d3
                        fa69b5d344b984c48a265ee6a7b0df8450004ceec7c1997b8
                        59be16af624e3da2cf44"
proverBlind = "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147
               ebf22b8"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147ebf22b8"

context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "b04bd002c85e31d2735ee2e6b36aea85147cbf197934f99ae26a7da73b98ebc34561848
 426aded0967e07fb333f79487"

revealedMessages = {}

revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
2: "835889a40744813a892eff9deb1edaeb"
4: ""

Trace:

random_scalars:

r_1 = "13c56cabf679ffcd59c41f3fe18ee4993ac4accba74037e01aafc5c0e79d8524"
r_2 = "2ad00067178fed38af012a1db49065e0135f7514acb184b15adc2f3bb3439c68"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 55cd78757fab58eb75a8260d4a990233ab996a1be803cfec107
                    1981b037fbfa8, 5f22ca14b29e8217c2d80bffadba8fbe0e9a72
                    b08676d8805f494b01ee0a322d, 18916a46f8255442283f13390
                    2d5f16f4cd583f6b8e68b4f2651ae52792485af, 39c6828e74bc
                    304f475a70831781de4be5e876fd5a34a34df553666c14c1b600,
                     54715e8092608f37043d85c2829eab964d0c8332ee8c0e1d3199
                    1394e367adab, 377db8d23e45a90c39b57b9042584b87e0e870d
                    00002aabd2e2b7432b1ee81fe, 456503806bf43b0766c629e5fe
                    e11956ed46232049e7a4fd29ec9f50212ceb88, 1c79c4fc9e4f6
                    96101ae41ba5728a14a54fef180e92c71471e964c8dfc1813ab,
```

```
                  4c7fe9d2f777bfcd1cc185d8c252f75c4512c3ad796a665d8737c
                  1fbccdf5246, 58e4f89934eca37018857c9967661294a68cfb43
                  12214696a9e060d96a6ce3e3, 64b1632f96a49fb49f00d928e84
                  0709b24f33706bab1d72a9243b6ea011d3fd6, 649304c1378ee2
                  0264a7b95c230b85bac9d18fd379b4e51dec087120e7e53201, 2
                  79980776234a84dba380ae7e83241754b68e55c1fd9ba31b75156
                  f8fcc6cb2d, 2d11b81789c8bfaeb419a1f436dc6b7ebc82e6cff
                  7994973ae549ee014c715e5 ]"

domain = "4508e372d4ede742110dbcbc3e0c0d286f6d7388827b98805f7b62ad17678d
          93"
challenge = "32469e79368ded96f86056d48fdd9850ae1dcf7de039024b8940750c8f6
             8d593"


L = "10"

proof = "a95d0c2f1e89fa4f4049f45ecc89fa8a82589f296657ae2f1b50b73af04e251
         d97b4822566f24c04b52bdb3c230b540ea55f4db83a932a5803a29573e1a377
         05a1fa5a8bc59d3bc4e2f2e2bb39471ae191acf4e6738c3d962171dcb16d810
         63b88b4b9f2b517d1b428806e01b1fd245631e668cbabbe4d4a7d6ca7b6b60f
         dbc7f234e4b158e41ce72702c8586e260ee42f92cafb6f46f584b11d9ac0cc1
         2d6e03727ea8f9ef0cdfc6c9d179ce0a8d1042d403a80bd935645cfceb09c45
         5d1c27e1e563489f501482c969710077e49a2e4096157ba62f966f3314d4cdc
         23f67758a9e6e302e4dda34a6900067415e05f626644cd91fa518243deafe3e
         a3dd113413729b66f3a3aadd7f6a417428609847077a7495d2fb0bd5c54b873
         3bf735d876e3f70e46db442c6307829ea4f7229360de17e0ab31c82491cba75
         560a2bc16859f70f48647f28c3805240924f256b4e7234c8e83b8c569f3fbac
         04e6157effa690240f38d611ecb61354e2d7ec0870a36da985dabad7847f893
         9cb91f7dedb3601cec88af2169ff03668f0f381a20bd0e9dbe69cda97561279
         731e2b04d8fc0d48c9a92ad1f2b857b1bbf6d50ae8a6441ba5eb50c85ed05a3
         c6eaf00af0f8a8ce2b9f4d4a06d3cff8a243fd11652dd94176236d55d2d3909
         36b15f676f819181cc2d73f77682db9cc06b9b14a411ce0375c56eb49ef7524
         59c02dc8c065c3f5a8d795497e93a1ab59ae55a5505caec8515efb86c055331
         b1d8a31ec0fc181085c1e1ba1ee6df93c32af3f6930814a2552602f381fc247
         54beb43c9ca9c931ecc7a4c31220970ec805f604c01ed651f1166a583823774
         ccd6088d1be3b6af9f42b63178c7d1a5b70196421fbbdc5fb36238c8bbd6bd4
         cf886036d95abb86e4e7158e87813a5f9ba95df0e853964f4e040c663fcd0c7
         45e54e0c939b8de61176d6d474fca6952dc0fd3720600e525038f32469e7936
         8ded96f86056d48fdd9850ae1dcf7de039024b8940750c8f68d593"
```

11.1.5.7. valid all prover committed messages and signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "99f409633ab1140121a94508a25d3ef7fe9d7da3559408502e81331f80c
             bddb621a99c02b6bab14c44aaf35b19006a1d0a91f0ac5a47b9c0a99a29
             0c3f36debe34c00ca333a9006e769b4930e39210c8"

commitmentWithProof = "99efccc0ccd91efabb8821ee33edacb823b1dd999682aaa54
                       f38a9c4585e7e7aa746357b2842d38c008f6d732dd501c70e
                       ed41caf3eafdd4bb6151ce2c0289401c7d13381e7db90137d
                       7aa2a64224aa2499a4548b2654481a2f0dd16d799116fe41d
                       b7b7a5c3ae8b1c64bef6a89a46f5040a5178d2e1126f7f351
                       89f0f6cea3803e679ce92eff73856b164425ac4ff8405a934
                       f65ada8ccbe21558ab66db113662ea17ce0c9aa0280db20dc
                       f79301c61269ddfdbdcc22025b85f7089c4ebebc224a938b7
                       45daae833ac4698d9d32bfa8382b4bbb2679ae232d2f6e8e1
                       9239e6ea919665ea736b45a61bbd0e4f4d7431f3038c3db25
                       833b9a0cc1a7709419ac241fb6f02ee13e51101743f1983d3
                       fa69b5d344b984c48a265ee6a7b0df8450004ceec7c1997b8
                       59be16af624e3da2cf44"
proverBlind = "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147
               ebf22b8"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "15494ae70742a6a4f420106c79ee405c138557385f3f6f7256449d147ebf22b8"

context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "b04bd002c85e31d2735ee2e6b36aea85147cbf197934f99ae26a7da73b98ebc34561848
 426aded0967e07fb333f79487"

revealedMessages = {}

revealedCommittedMessages  = {}

Trace:

random_scalars:

r_1 = "3073243f29432d46e7f2c4d2a7d87bb15310d624809af1b84187d93d30835bf1"
r_2 = "3bfe24fd593ffdf3d01853eeda787901f8a40b01180d93c3ab47034d74582c4c"
e_tilde = "undefined"
r1_tilde = "undefined"
```

```
r3_tilde = "undefined"
m_tilde_scalars = "[ 167266e78b1e98792faa161d1004860d9513390c951eaa0c38b
                    fdd8139ded981, 11b2f012310127e20e2ba5ccdd795832dae26f
                    337a2ac917246597c51ba0e814, 2a02495eb38ba3648b47a5401
                    07223ec68c8adc407495286e158391bb71830cd, 359e618bf603
                    979957ab4eb1d8a15f3dfad16d2131f74104023a58aa4824668e,
                     0d9a9076dd68a89f31587dcf07975ec95e38f54dcee6a8031020
                    10ef2b7ecfc9, 19762e5c3b76312bca412852d98967d5ec31ad4
                    83db5c4dc54301a48c35e12b5, 0f86ce1283a3b533eb7067a4f3
                    7e3d4f119e56ef94eeec42ca18eed0d84d611e, 29f8e06dfe2c1
                    173c14aa396065573168c89b177d8a2d7ca174ee5d9289760a2,
                    279f39de04874cc0abffe26fedbce6a940fa84f6d66b0ce7ad097
                    6797139b26a, 62ec7df765cd26dec3cdee13c42e24f0f8f8f46e
                    5606c598e82cfe20a46847c4, 40eaf6a1bacfd7d2c9dfd2b5d89
                    f661bfdc5d6a81b381aaf474997312a03fd61, 135e144adc59c8
                    7a6bfea6e571e7c91af3cdc15a97ed12a1171e168f2e2b9bf7, 0
                    844c5e30518175069417b37ff58748e96dcf5e9405d385be3ca27
                    6a331e38ee, 73c0dd04f96c6539deadb2ca61c272bcd154566aa
                    8bcb4ecddf6388f575c6db8, 25fe71c44d29832409b116262738
                    66d4372df93669e76af3d3e284bade276ac8, 22b7f7c40ded108
                    e6678604d3d937c53c7c4cf81e36ff51a89dbf4af573306d1, 07
                    3b68cea44ee1fe91040d61af84e9e665200ed34be657147171c71
                    31db53a78 ]"

domain = "4508e372d4ede742110dbcbc3e0c0d286f6d7388827b98805f7b62ad17678d
          93"
challenge = "24d132773d7773051b9d594aa059a4793902948cf5ef5743e8865bf7cb3
             20ada"


L = "10"

proof = "8a088a3619f2be6061e47e93048b0ea5391e54a8e551e6064f8065e0f09db7b
         e36dacfb2349797d889b9c456a07d0df5b93e0792af6d74293aac66b6be0902
         cddab66c1fce327d2690323d6083a80153969a46c2c3f3462fecb3d47fb6c9b
         909aea8b5cfbebe68f0b88f4e5718ea1a307eb84887e8a28b07cc1ab76f3ba3
         4a9c81a9fa1ad7c2a59dff8b9fd993270ed63cc4723517f556b1657220c7b7e
         3946d88aaaccd7620eaeb0d52fa272bd2cd871c74d9a5a2ea52d2c4cb309fb2
         67a8315eecb02a37906ae71cf47c50267f198806700d239566921e7b2ae7461
         fb6f2c1028702469ada2358c769ac5bbe79d3762adcc226be4f743984d8c2df
         fb27d7eac58fca920dead9129da6b4ced872e60d5d83b93c38a0d2b51b58967
         ffb8fa0cb904346755f84969e583ec69d697806d0492180385da37acf864016
         0c60f82d283ea0bd23f47362af5eeb1bbbc0c8d8d942a1647d78d787105d49b
         9493d912522d384e1ddd71ba917cf8eda4a8f2651fe33e9466d024a9771a428
         8bd0690e07d8dda9dce39b81ebca66509fc4a5990d4639f6d1f8cfd949d2090
         eda44d55e43563a33ff0371d4ed7ca039c65064f2b5d957d60baf654f6c2afa
         f8b49d1933d607d667b77e896ffdfeb1f6572dc6999f1a1ea753e05445a1600
         0c237f762e9cfecba5f43fc65f126e1ed0d31c7855115540ab6c54ad8f321bc
```

```
          0428b998e52eb77eb5ddcd363a7eb4846d8ca820673d0e40447a71b207badeb
          394d7037fbce0c30eb50c6d2cde0f5fc1212fb6be8ed392e4448c278d7afc69
          92a4cbab933429a5f87e372b0ef6d11439862796fb130cc1d1621785848ae55
          12894ed4e97f87a1a1a85c0fe5ea8ed7e6ceabedc26c935266106cf619410fe
          a374f4ba9604d01ce60ef4dfd25962b3174d007d997b9ef7c8120111a9a040d
          7cf4ef178da51d74627cda2cfb52ee6c33c3584bc37e7d89d727a02fbb2ab16
          39e5c5355c2233112d49bc48ef30e09f11a9933feeb936d26635af0445eb7ea
          fdac863378175b936461a7183d848406b788f42c2dead4d419e51f150a7dc72
          cb46987b2444321a0ce9bc090fd936aa1f27dd3dffe3a8c5d490e96924d1327
          73d7773051b9d594aa059a4793902948cf5ef5743e8865bf7cb320ada"
```

11.2. BLS12-381-SHAKE-256

11.2.1. Generators

```
api_id = "BBS_BLS12381G1_XOF:SHAKE-256_SSWU_RO_H2G_HM2S_PSEUDONYM_"

P1 = "8929dfbc7e6642c4ed9cba0856e493f8b9d7d5fcb0c31ef8fdcd34d50648a56c79
      5e106e9eada6e0bda386b414150755"
Q1 = "8c6f8b5efd544cb72ffc140a4585031ebbb8f25acb881ff559c42b94b8ba867be2
      3b183069032ea18c50910c9b7d3fcf"

Generators = {

H_0 = "896962df2851d1b83640182052fc49d07e9492347aee5ba8cbbf6414249367a17
       5d3e09f812dc2ff7d22618e7f0cb630"
H_1 = "80562c843a305661c2588da3ae2e3b96a5faab147fe6a58ff456648b42407af5b
       eddc2009b4078288e2a8e6a73d4ae4b"
H_2 = "896dabeba9bb98ef48d665cfaa894857cac7ed41f2c4b55bb64fd318dde0a8b03
       50578d9c37010dd266629d6bc9f8e70"
H_3 = "b3941ebfc0a011c442c8902d1e654b19d184385691aba1aeec60d87bfbedbcbf5
       d23ea3075126842522638613921240c"
H_4 = "8619d28414b303bc8accde9989b3caf9c9036303c9b8178d25a6fcd738b74c779
       b0a27c867e1a7f0e9b80c5cae3f4e7a"
H_5 = "85d6077858f8ad500df7e928a25cd0e5dbfc43aff4d761852d42feea68123212f
       f7d41978280be66e56724e98f776c9c"
H_6 = "adc477c6cf52b8aaaf055734c12dca89305937001e10e34e9007accb374d16d54
       0c97fa3ba026d6020f64319ce8d52c2"
H_7 = "ad24e98787eb7318cf04fd58793e77d41707e95fb5ab357237f88e2c9566400cb
       085748a3593e2f838caaf3a5223a7ac"
H_8 = "879db6d14a3ead2a81763f4909a6c4633cbd4e20c602e344e1f7d9891b517a329
       f72df0b516c4bbfa4f05c6204c242af"
H_9 = "8f01fc380b30f177090dba078af493e76c51e867f9f5f8f23b1ac162149d58264
       b1e262fbeaaa2f26624de592cc1ae4c"

}
```

11.2.2. Blind Generators

```
api_id = "BLIND_BBS_BLS12381G1_XOF:SHAKE-256_SSWU_RO_H2G_HM2S_PSEUDONYM_
         "

P1 = "8929dfbc7e6642c4ed9cba0856e493f8b9d7d5fcb0c31ef8fdcd34d50648a56c79
      5e106e9eada6e0bda386b414150755"
Q1 = "986e83f847c8c3fe1ad9d3efd0265b66268fc80f4add90b3e96192616364016bfe
      73a4005d2d86f841806a3132a0f544"

Blind Generators = {

J_0 = "9536711b4ff6e1038102b1473bd1be23b77ac6e85684662c7f340ca522f4e5fb5
       c02d7cb2c31c712324b29c540c9d7dc"
J_1 = "91611180da0248d8f7279a962c32472fb1e57b21fc41c09e6ab8aad61fcab5bbb
       51a4095aee80b070d8ca1e80f725339"
J_2 = "ac4f5344e62eafd1e96fc95539db6f568a3cd3dfd8c5cdafdc0bd2f95572c1083
       800f0f4538449051dd3aa362d33b718"
J_3 = "b823809960dafeb4d405c95d44b38cf868efe320b3c1d995daee411507e672a45
       a050f0b3a73c0175fa521f549dfac04"
J_4 = "9319ad949d6c5a368ed996732f0a665551604ee4a57cbadcbdd3f538ef2391f44
       ceef6f3509ead912cf64623da7e12ad"
J_5 = "b755da890d37cb97fc623b228dec163a6138489ff382292f608ac7adabe15856b
       74a5bed22364744d076b39cfda85faa"

}
```

11.2.3. Commit

Mocked random scalar parameters

```
seed = "3.14159265358979323846264338327 9"
dst = "BBS_BLS12381G1_XOF:SHAKE-256_SSWU_RO_H2G_HM2S_COMMIT_MOCK_RANDOM_
       SCALARS_DST_"
```

11.2.3.1. valid no committed messages commitment with proof

```
committedMessages = "[  ]"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
proverBlind = "643a0c0bc86a50e0d8c00bfe6c8debd85373597e1aef6cc912838bf7d
              c376e48"

Trace:

s_tilde = "40e7b7bc3a17cbd4fa61f81728b6f1224a934a34f8cd57000c360f1b30169
           0b8"
m_tildes = "[ 43a77228890e6cf2c297292b8989751a6e0c9713caa592f39e61e23a99
            7321cb ]"

commitmentWithProof = "990c1837a8af86843213e5b12fbfc962efcaf8fd0e5812a62
                       37b91b00a47b5a34714a60b4c365f72b47a4d9b656dde4753
                       a18a8286aca2bf58e8bb9a3d77a3e0052aefc427e5e47b666
                       255e53cfcaa7d34d36adc13da01798b8eb041652a57c3b595
                       ace54ed5eee43370c1697eb5ce996020d88ca5d811c011cde
                       10c6c07dc2f4acbc89bd5652414d5b8823a250ed40b"
```

11.2.3.2. valid multiple committed messages commitment with proof

```
committedMessages = "[ 5982967821da3c5983496214df36aa5e58de6fa25314af4cf
                     4c00400779f08c3, a75d8b634891af92282cc81a675972d192
                     9d3149863c1fc0, 835889a40744813a892eff9deb1edaeb, e
                     1ca9729410dc6ba,  ]"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
proverBlind = "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06
               fea89c3"


Trace:

s_tilde = "4cdc5d3fdbe932953dd181851ebf6c134103666761013ff3db4e6dbe47d39
           92a"
m_tildes = "[ 3aca8b66d624ae8974e93fd1f654ddc5f071c9b026eb6eb116401a4cce
            87d699, 0eb04c03f3571cc6cfaf29f19126d032b85bc1e9ac0af917ec5d
            c8ba61ce2d28, 0824fe0cfae8bdb1d2c88cd0d8a4c1b432a48f7f12e35a
            fe5494400a3caaa974, 05faf4555ddc6450e9f4b26ac7ed56ae57998c52
            9d3a898f93f72406d9c63990, 253782ab563a180dcdb220d0b75ad1499c
            70c8e7da183c2720f313368cf001a3, 58ca8d9150a51f432c32e41bbfc4
            b630333ccd19fd8daa6d581ff651392dbece ]"

commitmentWithProof = "a9577c3e2f15081c03d2e86789c1d9208bc04409b1ca33c25
                       d06017c8fef5d139aee028ac96b9c09636a45846e9a5ee51f
                       83bfd55f12193061e3f707d11d9993d6e08293de7f3dd0a29
                       8c21f369208b43b7b401706a9a0a5dcfa12d28d5a59b09da3
                       37b435cf4aa2a869842c8e1409004865ce6ff78d345e5c814
                       2c9c440b677824ce06a8f70c50bbbb01838a91eb0041fd853
                       c2005109d3aec272dd03346f37fc90828490fbedc4fc88e73
                       07662b785653aba1a28a45bca913b7dd778e8bd141652e6f0
                       507c3f836c8852b8ddbf2c62659dbd7b83f096e7b351f2f0d
                       c6046bce3c8d0c5bb892a7a3d76d6bac899b3d356b099f882
                       87ac25e6879d5808f832927c8e28acae41ab3699b5c0f9da4
                       f58bf67d7e87c5ddb6dadd80fe281e158cc7a24bc398f8402
                       2dc0dc3a123971f7546c"
```

11.2.4. Signature

11.2.4.1. valid no prover committed messages, no signer messages signature

```
secretKey = "60e55110f76883a13d030b2f6bd11883422d5abde717569fc0731f51237
             169fc"
publicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bbaa8fa1
             36f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632171d91aa8d46
             0acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db75c845d649ef3c4f63a
             ebc364cd55ded0c"

header = "11223344556677889900aabbccddeeff"

messages = "[  ]"

committedMessages = "[  ]"

commitmentWithProof = "990c1837a8af86843213e5b12fbfc962efcaf8fd0e5812a62
                       37b91b00a47b5a34714a60b4c365f72b47a4d9b656dde4753
                       a18a8286aca2bf58e8bb9a3d77a3e0052aefc427e5e47b666
                       255e53cfcaa7d34d36adc13da01798b8eb041652a57c3b595
                       ace54ed5eee43370c1697eb5ce996020d88ca5d811c011cde
                       10c6c07dc2f4acbc89bd5652414d5b8823a250ed40b"

signer_nym_entropy = "3d40961fce6c09eec24a371322732932503b458d7a4cf7891b
                      daa765b30027c5"

proverBlind = "643a0c0bc86a50e0d8c00bfe6c8debd85373597e1aef6cc912838bf7d
               c376e48"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
nym_secret = "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa02
              69bbdc"

Trace:

B = "b7d828d9db6412e186b9fca6300f23cd5ac9710fdb4349cf37fa58c97b83fc56c2f
     b3cf320b23ef595e1b7fc26fed722"
domain = "66727320f5282cba4bb93d7dcc20a35237652b6f56722b75faeee18905a44d
          95"

signature = "b75c2aeb0b79506a85fe900efb954ecdc591e5492c90204221371756226
             b3b0a30e39ee578354b7566fd1766bf1d9212424fea257ef8c483c879ff
             a3c2f5c9d7a64cea4770e391ca7b3a305a3306496b"
```

11.2.4.2. valid multi prover committed messages, no signer messages signature

```
secretKey = "60e55110f76883a13d030b2f6bd11883422d5abde717569fc0731f51237
             169fc"
publicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bbaa8fa1
             36f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632171d91aa8d46
             0acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db75c845d649ef3c4f63a
             ebc364cd55ded0c"

header = "11223344556677889900aabbccddeeff"

messages = "[  ]"

committedMessages = "[ 5982967821da3c5983496214df36aa5e58de6fa25314af4cf
                     4c00400779f08c3, a75d8b634891af92282cc81a675972d192
                     9d3149863c1fc0, 835889a40744813a892eff9deb1edaeb, e
                     1ca9729410dc6ba,  ]"

commitmentWithProof = "a9577c3e2f15081c03d2e86789c1d9208bc04409b1ca33c25
                       d06017c8fef5d139aee028ac96b9c09636a45846e9a5ee51f
                       83bfd55f12193061e3f707d11d9993d6e08293de7f3dd0a29
                       8c21f369208b43b7b401706a9a0a5dcfa12d28d5a59b09da3
                       37b435cf4aa2a869842c8e1409004865ce6ff78d345e5c814
                       2c9c440b677824ce06a8f70c50bbbb01838a91eb0041fd853
                       c2005109d3aec272dd03346f37fc90828490fbedc4fc88e73
                       07662b785653aba1a28a45bca913b7dd778e8bd141652e6f0
                       507c3f836c8852b8ddbf2c62659dbd7b83f096e7b351f2f0d
                       c6046bce3c8d0c5bb892a7a3d76d6bac899b3d356b099f882
                       87ac25e6879d5808f832927c8e28acae41ab3699b5c0f9da4
                       f58bf67d7e87c5ddb6dadd80fe281e158cc7a24bc398f8402
                       2dc0dc3a123971f7546c"

signer_nym_entropy = "3d40961fce6c09eec24a371322732932503b458d7a4cf7891b
                      daa765b30027c5"

proverBlind = "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06
               fea89c3"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
nym_secret = "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa02
              69bbdc"

Trace:

B = "8cf62aa99eda2b16a2fd5b324e09cfa7c52680feab7a3e98de0501d1990869ec019
     8e215ada434abbcd13f2f92ce1c6c"
domain = "739e8f67d6fea2dca1ebd844bc6f00b245e0085bc4b4bffc10e02e7e45a1ba
          f8"

signature = "b4b026980b38e88dd7d89c953f8c6750352aa9235865bab030999850e83
```

```
              2578a374fcbeb3882dedc72f50d1fc8e2083932227a61a93ba23f7fac72
              f587b40de4bf36bdb5567ef4721d0615b91ecf1811"
```

11.2.4.3. valid no prover committed messages, multiple signer messages signature

```
secretKey = "60e55110f76883a13d030b2f6bd11883422d5abde717569fc0731f51237
             169fc"
publicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bbaa8fa1
             36f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632171d91aa8d46
             0acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db75c845d649ef3c4f63a
             ebc364cd55ded0c"

header = "11223344556677889900aabbccddeeff"

messages = "[ 9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4
            a45f02, c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811
            f5fb075f9b80, 7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932a
            a348e07b73, 77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c
            , 496694774c5604ab1b2544eababcf0f53278ff50, 515ae153e22aae04
            ad16f759e07237b4, d183ddc6e2665aa4e2f088af, ac55fb33a75909ed
            , 96012096,  ]"

committedMessages = "[  ]"

commitmentWithProof = "990c1837a8af86843213e5b12fbfc962efcaf8fd0e5812a62
                       37b91b00a47b5a34714a60b4c365f72b47a4d9b656dde4753
                       a18a8286aca2bf58e8bb9a3d77a3e0052aefc427e5e47b666
                       255e53cfcaa7d34d36adc13da01798b8eb041652a57c3b595
                       ace54ed5eee43370c1697eb5ce996020d88ca5d811c011cde
                       10c6c07dc2f4acbc89bd5652414d5b8823a250ed40b"

signer_nym_entropy = "3d40961fce6c09eec24a371322732932503b458d7a4cf7891b
                      daa765b30027c5"

proverBlind = "643a0c0bc86a50e0d8c00bfe6c8debd85373597e1aef6cc912838bf7d
               c376e48"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
nym_secret = "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa02
              69bbdc"

Trace:

B = "91e63f20b87851ce9da85f7994a003f23e2e56b2f308cdda62da3160dcc6b5f41b6
     0b40220f4cbeffbcc900ef457a6ef"
domain = "4174ed9aa096e4535ea500d80b77858fb5de8d8ff39f2c409a496a0797eff8
          ba"

signature = "92a8e449a715421cd49fe58433e5ed2300a67d36d589eac87536bcaab61
             6cc846785e17449a9baa83826ee177f79445d27bdd783b7730048f7dfd3
             55fb7494d150f15fb203f4d0aad2a65aa436ffb208"
```

11.2.4.4. valid multiple signer and prover committed messages signature

```
secretKey = "60e55110f76883a13d030b2f6bd11883422d5abde717569fc0731f51237
             169fc"
publicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bbaa8fa1
             36f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632171d91aa8d46
             0acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db75c845d649ef3c4f63a
             ebc364cd55ded0c"

header = "11223344556677889900aabbccddeeff"

messages = "[ 9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4
            a45f02, c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811
            f5fb075f9b80, 7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932a
            a348e07b73, 77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c
            , 496694774c5604ab1b2544eababcf0f53278ff50, 515ae153e22aae04
            ad16f759e07237b4, d183ddc6e2665aa4e2f088af, ac55fb33a75909ed
            , 96012096,  ]"

committedMessages = "[ 5982967821da3c5983496214df36aa5e58de6fa25314af4cf
                     4c00400779f08c3, a75d8b634891af92282cc81a675972d192
                     9d3149863c1fc0, 835889a40744813a892eff9deb1edaeb, e
                     1ca9729410dc6ba,  ]"

commitmentWithProof = "a9577c3e2f15081c03d2e86789c1d9208bc04409b1ca33c25
                       d06017c8fef5d139aee028ac96b9c09636a45846e9a5ee51f
                       83bfd55f12193061e3f707d11d9993d6e08293de7f3dd0a29
                       8c21f369208b43b7b401706a9a0a5dcfa12d28d5a59b09da3
                       37b435cf4aa2a869842c8e1409004865ce6ff78d345e5c814
                       2c9c440b677824ce06a8f70c50bbbb01838a91eb0041fd853
                       c2005109d3aec272dd03346f37fc90828490fbedc4fc88e73
                       07662b785653aba1a28a45bca913b7dd778e8bd141652e6f0
                       507c3f836c8852b8ddbf2c62659dbd7b83f096e7b351f2f0d
                       c6046bce3c8d0c5bb892a7a3d76d6bac899b3d356b099f882
                       87ac25e6879d5808f832927c8e28acae41ab3699b5c0f9da4
                       f58bf67d7e87c5ddb6dadd80fe281e158cc7a24bc398f8402
                       2dc0dc3a123971f7546c"

signer_nym_entropy = "3d40961fce6c09eec24a371322732932503b458d7a4cf7891b
                      daa765b30027c5"

proverBlind = "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06
               fea89c3"
proverNym = "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f6
             99418"
nym_secret = "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa02
              69bbdc"
```

Trace:

```
B = "b08f8a9b235d125fa60c5f4c324d9f7a10b3a3ae01e1b3ebcf4df28aa8ce4338298
     46ee39fa5b8b77d14ed08f4272351"
domain = "3a0cd3db734c170c2099d9f8527578319753eb50f81425b98ee58ad1ea9cc6
          7e"

signature = "a671299573ec1e179a92e97ebc5927698327c11e2c56608e674fff2aaf2
             e1a4ad9ddffcb412391c447cdf09c30e8e95d1888e3f8cc0f58a170b1a4
             c45e21d1d41a387bcfff7275ae96b00d6f805bb32e"
```

11.2.5. Proof

Mocked random scalar parameters

```
seed = "3.14159265358979323846264338327 9"
dst = "BBS_BLS12381G1_XOF:SHAKE-256_SSWU_RO_H2G_HM2S_PROOF_MOCK_RANDOM_S
       CALARS_DST_"
```

11.2.5.1. valid all prover committed messages and signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "a671299573ec1e179a92e97ebc5927698327c11e2c56608e674fff2aaf2
             e1a4ad9ddffcb412391c447cdf09c30e8e95d1888e3f8cc0f58a170b1a4
             c45e21d1d41a387bcfff7275ae96b00d6f805bb32e"

commitmentWithProof = "a9577c3e2f15081c03d2e86789c1d9208bc04409b1ca33c25
                       d06017c8fef5d139aee028ac96b9c09636a45846e9a5ee51f
                       83bfd55f12193061e3f707d11d9993d6e08293de7f3dd0a29
                       8c21f369208b43b7b401706a9a0a5dcfa12d28d5a59b09da3
                       37b435cf4aa2a869842c8e1409004865ce6ff78d345e5c814
                       2c9c440b677824ce06a8f70c50bbbb01838a91eb0041fd853
                       c2005109d3aec272dd03346f37fc90828490fbedc4fc88e73
                       07662b785653aba1a28a45bca913b7dd778e8bd141652e6f0
                       507c3f836c8852b8ddbf2c62659dbd7b83f096e7b351f2f0d
                       c6046bce3c8d0c5bb892a7a3d76d6bac899b3d356b099f882
                       87ac25e6879d5808f832927c8e28acae41ab3699b5c0f9da4
                       f58bf67d7e87c5ddb6dadd80fe281e158cc7a24bc398f8402
                       2dc0dc3a123971f7546c"
proverBlind = "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06
               fea89c3"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"
```

```
signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06fea89c3"

context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "8ef7b8516387badcdf24eda35553031d01c392b93fb943445ae90979d7285d877ba6509
 cec3a3520f46128e97ecbd136"

revealedMessages =

0: "9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4a45f02"
1: "c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811f5fb075f9b80"
2: "7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932aa348e07b73"
3: "77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c"
4: "496694774c5604ab1b2544eababcf0f53278ff50"
5: "515ae153e22aae04ad16f759e07237b4"
6: "d183ddc6e2665aa4e2f088af"
7: "ac55fb33a75909ed"
8: "96012096"
9: ""


revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
1: "a75d8b634891af92282cc81a675972d1929d3149863c1fc0"
2: "835889a40744813a892eff9deb1edaeb"
3: "e1ca9729410dc6ba"
4: ""

Trace:

random_scalars:

r_1 = "63a03d9b47b688aae279fb7a53bf1e27f3be6c718e5bc7c3388bfc859a3fff92"
r_2 = "00dc935c7b744dd702e49d388a587e7a974336e5392cde39d84a0484c6a0c895"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 516259fc7668cceb1f7e68181daa3697df471f8354cb22ebdab
                    01e00336441b9, 2f5e1e67418fb18d0d7359dac450ca67ce4608
                    defa9c80d7edcf85278a929130 ]"

domain = "3a0cd3db734c170c2099d9f8527578319753eb50f81425b98ee58ad1ea9cc6
          7e"
challenge = "1e2ffc5d9bc0f6c649c460d99b27d52f0c2d6244bf0dc1c1382e73a9782
             d0851"
```

```
L = "10"

proof = "87c87375d670774600975ae2cb67a08d884f1a40a0ed279d49e9f9347758f71
         2a23b60ac21b6b210ec6a4b0e80ad7716a604ee9ef21240f4874fb365a4e7a4
         6cc34d9b681ff02a94335ba5e6d3cedcad0e10e5b5a7e1cb75ed9b4b7c64b34
         0729308f98ceff347fc7632a81bdf1c4a50f95347d6108a018857a90f0fb213
         c4cb36b74c48e120f061d4e725ef3c89f55271ac7b7e303c9d58dac01d03a5e
         fb470f9dabde27d9a0935201f960323826aa27278bfcf22fa6094c9caf7a19e
         263fbfe0a1d2c49ea6db45cb82f0af71b856775a2cb6a9698360cc005b4fccc
         24256a5d628552e8405b082360c5b618076e86619b79d53c20f1ad73db7ceeb
         df80af65f5bdaa099d7ede9c043f234f6fd322364168c1e09a10a9ce1096462
         43c70b39f8a6aa42031ba4594d76e6aadc5b3c1c71e2ffc5d9bc0f6c649c460
         d99b27d52f0c2d6244bf0dc1c1382e73a9782d0851"
```

11.2.5.2. valid half prover committed messages and all signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "a671299573ec1e179a92e97ebc5927698327c11e2c56608e674fff2aaf2
             e1a4ad9ddffcb412391c447cdf09c30e8e95d1888e3f8cc0f58a170b1a4
             c45e21d1d41a387bcfff7275ae96b00d6f805bb32e"

commitmentWithProof = "a9577c3e2f15081c03d2e86789c1d9208bc04409b1ca33c25
                       d06017c8fef5d139aee028ac96b9c09636a45846e9a5ee51f
                       83bfd55f12193061e3f707d11d9993d6e08293de7f3dd0a29
                       8c21f369208b43b7b401706a9a0a5dcfa12d28d5a59b09da3
                       37b435cf4aa2a869842c8e1409004865ce6ff78d345e5c814
                       2c9c440b677824ce06a8f70c50bbbb01838a91eb0041fd853
                       c2005109d3aec272dd03346f37fc90828490fbedc4fc88e73
                       07662b785653aba1a28a45bca913b7dd778e8bd141652e6f0
                       507c3f836c8852b8ddbf2c62659dbd7b83f096e7b351f2f0d
                       c6046bce3c8d0c5bb892a7a3d76d6bac899b3d356b099f882
                       87ac25e6879d5808f832927c8e28acae41ab3699b5c0f9da4
                       f58bf67d7e87c5ddb6dadd80fe281e158cc7a24bc398f8402
                       2dc0dc3a123971f7546c"
proverBlind = "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06
               fea89c3"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06fea89c3"
```

```
context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "8ef7b8516387badcdf24eda35553031d01c392b93fb943445ae90979d7285d877ba6509
 cec3a3520f46128e97ecbd136"

revealedMessages =

0: "9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4a45f02"
1: "c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811f5fb075f9b80"
2: "7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932aa348e07b73"
3: "77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c"
4: "496694774c5604ab1b2544eababcf0f53278ff50"
5: "515ae153e22aae04ad16f759e07237b4"
6: "d183ddc6e2665aa4e2f088af"
7: "ac55fb33a75909ed"
8: "96012096"
9: ""


revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
2: "835889a40744813a892eff9deb1edaeb"
4: ""

Trace:

random_scalars:

r_1 = "37fd1e468e9836a372c056fcc1aaf2a0faf7e3192391d2119525cadd1a21cc84"
r_2 = "3bafe2de79f657cc90b66b65c43af8ab0362841b2b5f1358aad2c861266b12c3"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 5cc47d2ef4f1fd7acacbd9f21708564c024e71d63f0a1dc9cf4
                    2844654777716, 17db681847018b04fbe5cab8c5a3aa6c902961
                    04a0b7af985f8e9ee66300ac7a, 0ad1b39daa6b6abe354992dd2
                    601e8997c23a593c116040800e1e9619d675a7d, 3557de528565
                    c4a0d75aeebf63bfa459becad78d8b2aecdcb289adc047f2b083 ]"

domain = "3a0cd3db734c170c2099d9f8527578319753eb50f81425b98ee58ad1ea9cc6
          7e"
challenge = "3970666b9cdd0f4ab9c4abbc46907422c2538d704a7b8ce1655f76ebb86
             648b4"


L = "10"

proof = "a368748cfab5ea798707998a21db421647144f932990c63dd69fac0b2046f6f
```

```
          4910a806098932ca655ab37f4276a9290b05d44f6755a4f3bb1ee0647d29e81
          e30d9972c22b96c99434b86a9877cd97fb18b923318fa135da8162861ef99c4
          988b264641475a51a0e1ec8a6289db1bb555e3ce8c05a5079011411ca8a9d80
          b671a0df37aabb8b65df3aa2dd5db766f23318665d8086ffdd1b21268ff4f85
          a485be1d05fbb4740a6c9012249924ab956656037629f1ffb6790ff7e9d6fa4
          b62a06585c8246e522b8ffc35b4c830091a7c42b760b6035286156b95246ee1
          77462bafe07e34599b00bb2e161188ea4f19e3f3a890b73ece45df6a71602ca
          3598b0c981f39f3b30104ea893e410a86b6612a90cf576c196ea2a9c31a514d
          bfd90118aef0598714b98d32066185be45e70cab0461715872ec7d7d08374a9
          e2751a99b9222f5b7d5164e039e65ac80e55672f4b42713d94b077f14f2fac7
          4085fe3d300c19802a758d4e4d9a63c1d23bafb54b13970666b9cdd0f4ab9c4
          abbc46907422c2538d704a7b8ce1655f76ebb86648b4"
```

11.2.5.3. valid all prover committed messages and half signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "a671299573ec1e179a92e97ebc5927698327c11e2c56608e674fff2aaf2
             e1a4ad9ddffcb412391c447cdf09c30e8e95d1888e3f8cc0f58a170b1a4
             c45e21d1d41a387bcfff7275ae96b00d6f805bb32e"

commitmentWithProof = "a9577c3e2f15081c03d2e86789c1d9208bc04409b1ca33c25
                       d06017c8fef5d139aee028ac96b9c09636a45846e9a5ee51f
                       83bfd55f12193061e3f707d11d9993d6e08293de7f3dd0a29
                       8c21f369208b43b7b401706a9a0a5dcfa12d28d5a59b09da3
                       37b435cf4aa2a869842c8e1409004865ce6ff78d345e5c814
                       2c9c440b677824ce06a8f70c50bbbb01838a91eb0041fd853
                       c2005109d3aec272dd03346f37fc90828490fbedc4fc88e73
                       07662b785653aba1a28a45bca913b7dd778e8bd141652e6f0
                       507c3f836c8852b8ddbf2c62659dbd7b83f096e7b351f2f0d
                       c6046bce3c8d0c5bb892a7a3d76d6bac899b3d356b099f882
                       87ac25e6879d5808f832927c8e28acae41ab3699b5c0f9da4
                       f58bf67d7e87c5ddb6dadd80fe281e158cc7a24bc398f8402
                       2dc0dc3a123971f7546c"
proverBlind = "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06
               fea89c3"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06fea89c3"
```

```
context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "8ef7b8516387badcdf24eda35553031d01c392b93fb943445ae90979d7285d877ba6509
 cec3a3520f46128e97ecbd136"

revealedMessages =

0: "9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4a45f02"
2: "7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932aa348e07b73"
4: "496694774c5604ab1b2544eababcf0f53278ff50"
6: "d183ddc6e2665aa4e2f088af"
8: "96012096"

revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
1: "a75d8b634891af92282cc81a675972d1929d3149863c1fc0"
2: "835889a40744813a892eff9deb1edaeb"
3: "e1ca9729410dc6ba"
4: ""

Trace:

random_scalars:

r_1 = "7313e18d146909fcb0768f65bc7b40d1470bf6c7eaaf32cabe9d4efef57b4d6c"
r_2 = "43241d9968e2960809d9f4c7b0caad95903aeb236889723182dd66808b1447b9"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 69e1449113b7cccb77270a88081447496f292f3fdaff5063125
                    a2d4a2dfe90d3, 175efe5d253a12dcae58d30b190b421b43eebf
                    c11a1e0a375179712c053bbb5f, 334b6f76a164abfad24247570
                    01a06c32e5780ee1b46dcf641c08753d26731a7, 3d49a5055e25
                    4a8f7bd0559d7f8af12c61e12141c3582b938dbb1dd11bc485fe,
                     4d1d2808c702b371de6834b4e9d3b89ed246c06ded576a9b52b0
                    ba9e969ba4c0, 31e82a5bff25fb098a63b15151a4a4cb0ecbc8b
                    0ea2c2f90d160390600c4998b, 5ec90143423471c547ef946907
                    b2f7d52c2c8aac3444090191eddbde1557c2ba ]"

domain = "3a0cd3db734c170c2099d9f8527578319753eb50f81425b98ee58ad1ea9cc6
          7e"
challenge = "084934b53547e3d7b33807f770c2a6c4fb51d11358bf650ce01b0965a50
             041ce"


L = "10"

proof = "ae0e79f2e30926b255f576949b1f34a4843d061b9279732d20315c1b1e133ee
```

```
          19d54dccae8e1aa90d628e0b4a423e958a4b674599ce231c77c779cf55436be
          406c72296cbef3d46f72702323baab6197223ff60a15e67e9540dcc6875b6fd
          764b27df0665f39469a94270c0433c070598d11deb8692f8db5d06ef2ce323d
          8593d46160a43df880d624e9a64b2935651b638b586d67c809e60e7a0b5affb
          b5a3e6e5d39a6e3dac8d18d7ac31f9b8573e76b6a5579b3d139d1d076a37d30
          0d7fa5bb9f406ef0ee9b23799c78d88209812e1e03306d7648dc4ec8281c772
          22f28522bc98e2dfe93c76e707a23a303cc50f81f3e26d2481661f9a69fff45
          bb93ab27743397092a4b21afb4d7d8fe6f8ca452207e85ea56bdcaa7822f032
          b40ddbdbb0cc4a7a0a49e72939cb60878b0b6075f31dc4f65e1fbdadf8aafcf
          4dcf8b7c1136d00d2eec96fc3c85bb08ceefd4cebb3e81e8c3ae6a868aa7aa3
          88d3baa4846e97698255ceabd698814348c76f99a0673cd718d246c215fed3b
          f658d2eab39d387d56b9165374fd8fb6388d824d30574224b0ccc6927fefff9
          baa7761ee5f084cfb6611a8d39621c77d04f4252b211f0164c4c5c56ffede41
          46709687a52af7380dc12f05081fcb522ec4dcd6218572084934b53547e3d7b
          33807f770c2a6c4fb51d11358bf650ce01b0965a50041ce"
```

11.2.5.4. valid all prover committed messages and signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "a671299573ec1e179a92e97ebc5927698327c11e2c56608e674fff2aaf2
             e1a4ad9ddffcb412391c447cdf09c30e8e95d1888e3f8cc0f58a170b1a4
             c45e21d1d41a387bcfff7275ae96b00d6f805bb32e"

commitmentWithProof = "a9577c3e2f15081c03d2e86789c1d9208bc04409b1ca33c25
                       d06017c8fef5d139aee028ac96b9c09636a45846e9a5ee51f
                       83bfd55f12193061e3f707d11d9993d6e08293de7f3dd0a29
                       8c21f369208b43b7b401706a9a0a5dcfa12d28d5a59b09da3
                       37b435cf4aa2a869842c8e1409004865ce6ff78d345e5c814
                       2c9c440b677824ce06a8f70c50bbbb01838a91eb0041fd853
                       c2005109d3aec272dd03346f37fc90828490fbedc4fc88e73
                       07662b785653aba1a28a45bca913b7dd778e8bd141652e6f0
                       507c3f836c8852b8ddbf2c62659dbd7b83f096e7b351f2f0d
                       c6046bce3c8d0c5bb892a7a3d76d6bac899b3d356b099f882
                       87ac25e6879d5808f832927c8e28acae41ab3699b5c0f9da4
                       f58bf67d7e87c5ddb6dadd80fe281e158cc7a24bc398f8402
                       2dc0dc3a123971f7546c"
proverBlind = "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06
               fea89c3"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
```

```
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06fea89c3"

context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "8ef7b8516387badcdf24eda35553031d01c392b93fb943445ae90979d7285d877ba6509
 cec3a3520f46128e97ecbd136"

revealedMessages =

0: "9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4a45f02"
2: "7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932aa348e07b73"
4: "496694774c5604ab1b2544eababcf0f53278ff50"
6: "d183ddc6e2665aa4e2f088af"
8: "96012096"


revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
2: "835889a40744813a892eff9deb1edaeb"
4: ""

Trace:

random_scalars:

r_1 = "645e79d9cda4c43c9379b57bcf0fd3bf91551d7d3506cdc5ddf0ecd6f1d62ef8"
r_2 = "4651e4a1ca07e8b9027be1593efbe7b3739c689f4fa35f15e08bfd6e1fb403a9"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 19eff867cb51d34a5dcfd09842babd26246fb0f31e9d6495547
                   dfca626ea6218, 4a453094c95378613b7883d8c6134050eac731
                   55047406d9d9bc14c13f1ca43c, 3305b0eb13b29fde6433e5a7e
                   6397973304320e4538d530718865003691fdec1, 20d1e7865a12
                   778a333d5a8629250f552b62a8b5ee72392d8dea199af3d99af4,
                    0fffec53443eee11097ee9f1ca1629f0ada14f58e834027bc519
                   285708978a2a, 1f4bbeb4fa9afd52feae084cc8957cfcaf897b6
                   056b57341fabbd7b2da0bc8dc, 30172f3663cc33948d1f6d290e
                   b86e39ed91feebe4f89578056b627513db4388, 2354405c3a0d0
                   a2836fa077ac742c86fe908c7babacaefc915af6249024442f2,
                   0fc44c488c657f7b3b299769713c611a1b8284750c085334b0334
                   5865912dfff ]"

domain = "3a0cd3db734c170c2099d9f8527578319753eb50f81425b98ee58ad1ea9cc6
          7e"
challenge = "025fa34d8302ee4f998f00214fbc429e2551dfebda5b46b22319ed8f088
             21da0"
```

```
L = "10"

proof = "ad1d728a7fb4b68de8d6ac04842bbe08fe39c4ddcdb6693415efde9565e61af
         a1cd095bacd7830364b5c14f505b4b6cb906de91cf57f482da1ad9dd5d9cb60
         c244568f09f6d30cbee78c09900a1f1c345ee43373d0beb5a4c83659ac3042f
         ab6ac9e660eb2e2b4e11550b27783379deddad2a05528768f0306fbb4e040e4
         ab0402c4b96e34c6adb77c8b37f38db432a74ff95092207821daa45b30115a3
         6d053803a71d0c61be79f9b5c7e465f53df732aba7902a9d67e323989092678
         66e6f3619fa1229c3c0778523f5b7d028ce355272481ca52aa203c049f3890f
         14793e8f744e51bd3f45fc4a7af2a5eadb1427e5b4d7064123101951dd034b7
         23a759228ee439cbed30a4866beb7840663c825303264769801674e6ddf0781
         e54585929b13c4243b4299cdc0292450ea2d74ae328778abb5ac27fc5a7c1f0
         b011751f7e38b6a0033c565b369efa0d49d45889b51c616f1cdcdfd499afe2c
         a256eeb84d215fec570026b18429105dee0451a7682697c045f40d132846f14
         28fb1d4e403e93bd8150a597c6033f84a110dc14da045800e29cc062358ca30
         4b1e382b1251c851cb839e59b5ecfafccc3dedbb6594920c7348026598ffa59
         f7fe3df27d86bb8069c10c5225c8aa8c09ebf23819838663a7474fbda2635b2
         ed3e829870c4fa1208497773650d6d1c315ce5df97b1de16e097279c1eebab2
         39fd37861ff106d575f9bcb01a259aef02cff53f0a3b26e1025fa34d8302ee4
         f998f00214fbc429e2551dfebda5b46b22319ed8f08821da0"
```

11.2.5.5. valid all prover committed messages and signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "a671299573ec1e179a92e97ebc5927698327c11e2c56608e674fff2aaf2
             e1a4ad9ddffcb412391c447cdf09c30e8e95d1888e3f8cc0f58a170b1a4
             c45e21d1d41a387bcfff7275ae96b00d6f805bb32e"

commitmentWithProof = "a9577c3e2f15081c03d2e86789c1d9208bc04409b1ca33c25
                       d06017c8fef5d139aee028ac96b9c09636a45846e9a5ee51f
                       83bfd55f12193061e3f707d11d9993d6e08293de7f3dd0a29
                       8c21f369208b43b7b401706a9a0a5dcfa12d28d5a59b09da3
                       37b435cf4aa2a869842c8e1409004865ce6ff78d345e5c814
                       2c9c440b677824ce06a8f70c50bbbb01838a91eb0041fd853
                       c2005109d3aec272dd03346f37fc90828490fbedc4fc88e73
                       07662b785653aba1a28a45bca913b7dd778e8bd141652e6f0
                       507c3f836c8852b8ddbf2c62659dbd7b83f096e7b351f2f0d
                       c6046bce3c8d0c5bb892a7a3d76d6bac899b3d356b099f882
                       87ac25e6879d5808f832927c8e28acae41ab3699b5c0f9da4
                       f58bf67d7e87c5ddb6dadd80fe281e158cc7a24bc398f8402
                       2dc0dc3a123971f7546c"
proverBlind = "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06
               fea89c3"
```

```
header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06fea89c3"

context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "8ef7b8516387badcdf24eda35553031d01c392b93fb943445ae90979d7285d877ba6509
 cec3a3520f46128e97ecbd136"

revealedMessages =

0: "9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4a45f02"
2: "7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932aa348e07b73"
4: "496694774c5604ab1b2544eababcf0f53278ff50"
6: "d183ddc6e2665aa4e2f088af"
8: "96012096"

revealedCommittedMessages  = {}


Trace:

random_scalars:

r_1 = "04ba5026d055fb29e48748ab435e4b61aa60fc480a826be9cdfa9e2aed3648fb"
r_2 = "1fcac43a8b494879ad671756080583245f11776fbe555bd974fa99b1dc68353"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 637517351b2e91be4cab8d8cba3ce605d6b5bf4709fcec17ab9
                    c7302d188f7e4, 0d2857e8286db4c060f05875b34159b7a3b234
                    2868f4da8e421f1a1362a07030, 40af4c858f59b35c74d2b3353
                    9e29ba7ac642cc90482eca5615b3c915cf9f0f9, 71840e81d029
                    4ac5b3ad0ba9c0b0136f078d8cdac595a64f0d9e63b3fca8a2da,
                     22979e0e072479f80a81fe43c7b5ce6c21c0064b6039d8637950
                    212a7b90c192, 3671cc511ee5093111052d78af04270df346315
                    f6fe3f9a7a32c8f5a92ef6d4c, 1e096373f281d8a87f63a3ff0c
                    925017cd825f2dc97d34f39eff08362e4db6c6, 44ea9cdb9c05e
                    4b5119f2500f4648481fb07d12a1cc75a5b2957e95367b7d681,
                    4da405d28b04edc0adb8043ec95053543d879a067f27b1051dc27
                    e268340d77a, 1ceb3358e8e4617ad361b95563cbf3701a9173ed
                    00b5e303c207879c8f294523, 6d216a3f24966d7baa9049cc320
                    765ef18bfa5162f2d60cac425845ca11f60f0, 2d679ebc3e75c7
                    2b60e7ba485503789542e5d20f923ddf346fea3399269c2e0a ]"
```

```
domain = "3a0cd3db734c170c2099d9f8527578319753eb50f81425b98ee58ad1ea9cc6
          7e"
challenge = "5a08681488a2c99af62a6fff67798ea557b7a3fdb5087904b1ac25e1ea0
             c94b5"


L = "10"

proof = "a07906dab5d5d523a80986c377f6c85618875bdac8bf8bdfd35439051f98762
         c8abdfef2ef08cdc7a6e14beacf7b303b8094057395b26030b2a7450bd5a876
         6487fff98768e705e636916c928adb95a3fd3f80b83f232b18a88396bb9dd11
         12885192a7fa6872221c29a9659f05e7a482e554c6a9b4f5a5571938bb099c2
         bd5f9a29a9fb9495625248d975ebb478758f1bfad60f4750647b1f2f3c33a14
         fa5273c67a0542e2725d911195d9a94d7ec183328166651feaa3ff0ddf7e339
         4426afc1dd26fe2c4a89a2acc8c5ce71f3ca50113e7b1c8a2a8c22fe81505fe
         1cc944b4ea86c4dc9020661e7011231e9db581e037ebe34ae083de76e9a22cc
         100b9304c4796e57cc9d6f5386cc0ef16b66506c43a976dd5a104ee0ce5745c
         b4e61080b3b0aa25777d85c64eade558b63f24edb594ff2add441fb95d9ebb2
         2bd807a6f96f82d10fb77fb6af178b002e81983e9e5396ab8e6c7777398370d
         557a1570cb4a90c3ab9bd9d4b77d475b2b10e2472632590567f0951fe70b7b6
         2645985af9284dc234d91c722d0a730a75df83af042c4f6965f8286ec4479b1
         02e006e463f467e7eccb5bb192bae8e52c1c219edad503d2473de89a67dd872
         0c31e73923914ee8496bd13743192b8b881b0c11b604810249678be3865dfd1
         5e225d264a408f05114a5b1f3634a117a2e7e11ff7571d56847e8ff18edb02d
         0119049b4ccccb7634e4343ade7e788e87da183fd916cfc2111e147a13e2cc1
         667ae18cc5983412b936b0b3ca207134da3febd66368d865f701a22b026c3f1
         f457c471ce02ac90ab44c1d3a3eb65b571bddfd911a93da38a446200e6a0adc
         e64aa23a52ca7a8e5213cfe08c8356f244391d7ad8fc8e352c35a08681488a2
         c99af62a6fff67798ea557b7a3fdb5087904b1ac25e1ea0c94b5"
```

11.2.5.6. valid half prover committed messages and no signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "a671299573ec1e179a92e97ebc5927698327c11e2c56608e674fff2aaf2
             e1a4ad9ddffcb412391c447cdf09c30e8e95d1888e3f8cc0f58a170b1a4
             c45e21d1d41a387bcfff7275ae96b00d6f805bb32e"

commitmentWithProof = "a9577c3e2f15081c03d2e86789c1d9208bc04409b1ca33c25
                       d06017c8fef5d139aee028ac96b9c09636a45846e9a5ee51f
                       83bfd55f12193061e3f707d11d9993d6e08293de7f3dd0a29
                       8c21f369208b43b7b401706a9a0a5dcfa12d28d5a59b09da3
                       37b435cf4aa2a869842c8e1409004865ce6ff78d345e5c814
                       2c9c440b677824ce06a8f70c50bbbb01838a91eb0041fd853
                       c2005109d3aec272dd03346f37fc90828490fbedc4fc88e73
```

```
                        07662b785653aba1a28a45bca913b7dd778e8bd141652e6f0
                        507c3f836c8852b8ddbf2c62659dbd7b83f096e7b351f2f0d
                        c6046bce3c8d0c5bb892a7a3d76d6bac899b3d356b099f882
                        87ac25e6879d5808f832927c8e28acae41ab3699b5c0f9da4
                        f58bf67d7e87c5ddb6dadd80fe281e158cc7a24bc398f8402
                        2dc0dc3a123971f7546c"
proverBlind = "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06
               fea89c3"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06fea89c3"

context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "8ef7b8516387badcdf24eda35553031d01c392b93fb943445ae90979d7285d877ba6509
 cec3a3520f46128e97ecbd136"

revealedMessages = {}

revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
2: "835889a40744813a892eff9deb1edaeb"
4: ""

Trace:

random_scalars:

r_1 = "2782e9be32645456d20a01a8ce5dd233b8049efe8d25eafdb8576f4e8d85826a"
r_2 = "180ea80200b800d1cb672bc1aa52e2e6ecf0acaf794b810f3c16e8b07c413f5e"
e_tilde = "undefined"
r1_tilde = "undefined"
r3_tilde = "undefined"
m_tilde_scalars = "[ 11f580b98813f609f6099d00f35412ae67aa1aa5c35cec654da
                    7fd04eb023616, 3d33bc719b4b5ff24fe54b281a361858912006
                    eff78184deffbf6769ca87b9a4, 2a2fe081ccd47b8a669e86232
                    470b13a5157931bfb3b770dac1080bcccd28d81, 6d0e8353ed62
                    e613e6223334709ad0e146efb9c522633daf44840a2b5424195c,
                     4a1742ed19312608a1095a476a5fc2533b3df79d065c62494f7a
                    0fe9aef2f455, 58d11e68c4ee775d999f69bc33efc83c7557423
                    420b48cf915d772c975c9fcab, 50886691287e055accbec2696c
                    2fb20e9072d704461dc358261d30116f78eca2, 080126141ef0d
                    e78e1454319dc179a72f95d98e8e1c5912d71a09f6113bfd6a9,
```

```
                    3983a595dde792593983b34198422b2d2f13215cb4803b510cd4e
                    59ca0297f0f, 34c8e1e41b5718d9dc82232ea9fd6895601c5366
                    dfdc65a1f58e9b0bc40472cc, 6f9ea2c849ece4b9e6271e0e017
                    75fc358e18b8c0974bbe3fdd7d58a04b6d4dd, 3eb917340ca578
                    8ce9266b29b984756addc2e9d9574e3140ad90ee1a1e668e37, 0
                    5aa05f0dee70e3b5905f5d894be11d37a2e1bf98a838130a5a136
                    968d8c4811, 4e66ec908e4379b5298f7ab5ab8a3690677297690
                    444183674a694ad3a0e5639 ]"

domain = "3a0cd3db734c170c2099d9f8527578319753eb50f81425b98ee58ad1ea9cc6
          7e"
challenge = "10f838acdfd31ccec8b5f53427465e5b715df435647cef473216fe38b70
             7aa8f"


L = "10"

proof = "a8910fb960eaca764593b00202a3f062c53f25d71701531083a72acc34c3e7b
         08642aa58f67f1835d9fd607c93765d35b13e33dc916ccd3582410b9d3b5f0c
         e25b3bb8d2a0954880798251662b0707ed4e09fcaa2a8c5b35b77712ed4f68c
         bfe985bb1ffa92458f9a8b54b19fbba33119e46deada623a3f7e7cfbc9e021f
         eca9bb3273151330a55e7a73a8471e4b4f493856d71fd4c4291e17dc48e75b3
         1bf4e85878efbac859197a31fdd0370dc627454c801ce876590e605acaa176b
         b1900b82d556e7217fcd93ee75970e99ec0d71326a36f02944b36f043c6f93c
         178bd773f3271d7c813e7f8d5fe47cfdf946358401e543e3e8453964a4df416
         17097872c81e622849ea544210174076fea749a25481f060d4f4c8ee179da05
         998e1fee1cf7b2e16fbb47966b96d4f34f18eedea1b91a0f917201c2cb05ccf
         1bbf9330a1adf5ebd6a6a9a3d37bf1cd1f08137bad407d72d185f1a08715292
         ce4cc74585fd9c60c5e0e2b0b37beae01a89f3c3f8e3be9fef9a8c8c9cb04d6
         d6a12bca713387f269684905db470cc88414977aa238651fedfa25521a1a038
         f3aa1f184c062b48170cf2420c626a3f08b81a8a5948e38ebc4798bee33c93c
         984580d73dcc7dc25a54977dfede551d7e2b5e79bdca1b60da532dfd00ae469
         6004bc9d1ecf57cba492145558b7867c721a50556d937c540b5b38313120be5
         5d43c3fb5d9b4a409ec44f62038dda9ac16f0aaf48848d2d646ef4c6cef5de5
         9f969b42ee46d54867833f299582729a06280331e1e77cc2065c5b24ad2d8ee
         2b7e4038384f703a0125fa8e8e2e050885eb20a087c0cf168508b9c68d1f3b7
         2fc7609e3b7096e6dbb7c51bfc85f4726d99e1826a736d02cd245fd76b4800f
         7c313654f21506e0217951fb8417afed7e462e1cc246fe0580a73daadd9e381
         88255ec3a8345fc34bde995bdadf3922d2a380f9c1a2a15d054f710f838acdf
         d31ccec8b5f53427465e5b715df435647cef473216fe38b707aa8f"
```

11.2.5.7. valid all prover committed messages and signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "a671299573ec1e179a92e97ebc5927698327c11e2c56608e674fff2aaf2
             e1a4ad9ddffcb412391c447cdf09c30e8e95d1888e3f8cc0f58a170b1a4
             c45e21d1d41a387bcfff7275ae96b00d6f805bb32e"

commitmentWithProof = "a9577c3e2f15081c03d2e86789c1d9208bc04409b1ca33c25
                       d06017c8fef5d139aee028ac96b9c09636a45846e9a5ee51f
                       83bfd55f12193061e3f707d11d9993d6e08293de7f3dd0a29
                       8c21f369208b43b7b401706a9a0a5dcfa12d28d5a59b09da3
                       37b435cf4aa2a869842c8e1409004865ce6ff78d345e5c814
                       2c9c440b677824ce06a8f70c50bbbb01838a91eb0041fd853
                       c2005109d3aec272dd03346f37fc90828490fbedc4fc88e73
                       07662b785653aba1a28a45bca913b7dd778e8bd141652e6f0
                       507c3f836c8852b8ddbf2c62659dbd7b83f096e7b351f2f0d
                       c6046bce3c8d0c5bb892a7a3d76d6bac899b3d356b099f882
                       87ac25e6879d5808f832927c8e28acae41ab3699b5c0f9da4
                       f58bf67d7e87c5ddb6dadd80fe281e158cc7a24bc398f8402
                       2dc0dc3a123971f7546c"
proverBlind = "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06
               fea89c3"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

signer_nym_entropy =  "3d40961fce6c09eec24a371322732932503b458d7a4cf7891bdaa765b30027c5"
proverNym =  "6830ea571e9fca0194d9ebd5c571369d8b81655afe0bbb9c6f5efe934f699418"
nym_secret =  "3183d923c36e56a823ea4ae0de4287ca87ff06e5785a57268b39a5fa0269bbdc"
proverBlind =  "1ade8b27cccac993dfe3d57be0cd1a200a5cae52d9ea525f106c94f06fea89c3"

context_id =  "bbb4750cdce6d2122bb4c4f039b6ad5a79f028eb448013a38636a95d63af360a"
pseudonym =  "8ef7b8516387badcdf24eda35553031d01c392b93fb943445ae90979d7285d877ba6509
 cec3a3520f46128e97ecbd136"

revealedMessages = {}

revealedCommittedMessages  = {}

Trace:

random_scalars:

r_1 = "326a49e2d8d7913701012fee5c5d928455d70a150535ee83ba8f838289023b1f"
r_2 = "056572994ba90ba03e44b30acc945aca792335b27c5f5ea05a0bf9c4c360603a"
e_tilde = "undefined"
r1_tilde = "undefined"
```

```
r3_tilde = "undefined"
m_tilde_scalars = "[ 19c6e4aacf97f53bff27c7de44179fd91380cdb164405b65189
                    94a92e78a2066, 4aa2ce863a88a4ba2d0d3b7abf4faa42ffa774
                    25d1226f8649855d3b07ab0098, 325d5fdfb63d63a1ed4821521
                    d5e8dd7bdbd3a82d033b0d607f9bc2f263d487c, 4ce828b81b72
                    bed30f74f5f32c6c0e1cd744f03faf0ef901a2bdb1d6952fe523,
                     05601ec295d3a2675f3fbce27e5657d1082f5f1c38c4b6e157d4
                    b66c64846453, 6df288dfa867d51ac44ac185aaa92f7e097a1b4
                    05178d88502066298e2e35e49, 1bf8f8de4f3a15233bb4cf3d9b
                    e23a5e022b0a3b55a492e84dfbbc093a0d0459, 1f501b827c4b1
                    3e3381e26997894aa3f4559062bee1c56d2f79535934c07ffca,
                    46391415dde3df672c839ef8b3d8316d01b8a08265041872f49d2
                    67788851990, 2db4ff5a39bdedfec9bca340748c55b825d9809d
                    d2ab58dec9f27d9b54dde60d, 07ad541e1dad6534c92c5707d16
                    8a5c08dc4cb916b22b63d174b78261fcc0728, 60d1c9f4285a4c
                    69a900d97bd22cc3788272d0dcdec5f9e1e6d64be10a01a0ed, 1
                    d21cf6835ee4d6729c0520135afa68e3125430a97d9502dd86e9d
                    dde148c298, 687c44782b9bdd724a3402d1e929c9f74febc3cf9
                    b91a55431790b3460b6f02b, 09abd129e4fb8d7e3a817bd65f38
                    9d53c3eb8df45d03325461756c5932d32a8c, 2cf3011ae8b91a1
                    4c5a058a43385885324cca7c78da2aaf1b2cc15cc751962f1, 15
                    4099a6f2a3df481fc6bc052b7ece804de2acdbb34b5cc945570a3
                    0416878cb ]"

domain = "3a0cd3db734c170c2099d9f8527578319753eb50f81425b98ee58ad1ea9cc6
          7e"
challenge = "15d12484c7e398e9d97533363068d1b7cc38676e915fbf93264c2209860
             e37c2"


L = "10"

proof = "8d3b51ea093c025a125c461892b18d561dd5205e7c01d5d61dc38278d45fcca
         8241a5fcc42a50558ea24926a6577e37597dfe3f3264cf81a17752c364e0cd3
         55099408f5b37bbc812996533c13c27eb5649082ccadab658253d44f83919a9
         166a92b28c33d426a662fdd57c2ea3f84b89dcad87b7091018ec26234ec12ad
         9a7413cfeeceb7af93be473a95911d2d47f43df6551812412dab2de651d09d2
         c12b6b4536ead479bd7e9201124a963dd94913bf550b84a160073ce170a83ad
         5b841ec384a1316acdd647a07c4d55168105b41489e6e56033f92a57855cc8e
         d2fddc93be3f625490baece8e551be6491f36c145a945a24f4693602e511e03
         647d50b708caaf02f49eaf19cec6c596fe6f79bd18a9da98d1aae28f1bc10d2
         05a16b241c97de75a17ff24bf1e47f063775e219257e7dfad9b87b9127f2942
         10d51e026357a11822e2e4ead4fa1fb2f7615dca5a6bd8ba2094981c377579a
         2442cdfba154f41fc69330a5f0f3f029fcb5ab5ee161edbc12157e33cf37578
         cde84633bba1144de3a61b23886237efd56fdf5576ee3d15e7e4eca557f30c4
         334dbf2921bccf53ac38bf9efe620182a80e49ed9771e63b904eded8388ce34
         fbe47bf5417b0c9ff9dbe489c398c0c93e3778ddaa9b2928dc21e690854e283
         b146ad30d91117e446aeab2a6552cb1e27fa4a9ff976b0705d0b0ef8a24f626
```

```
18724af86b655486a265bfdfc3d920588c74ffedb193821d006253535daaac1
ab794b0033b0f88faed65df6ca145a8478c3d4161136cd72e50c40fc7a2320d
e35238c0c47f3737c246be00932155cfdca71d17cc8e305f6462058dfdc7e87
492e052b221dabb2981621ac4be7a0f075264a4748e8c7b2a58396e193a8ea1
5d7760af0e75339c9e16c0deb36633f082e8831759fd48f28a835960c5846dd
e3b0a7b480d8a6f9c59334b0a844c9553b58ddc849a9b0d785c655dfddbbfd9
d24896f93c2597f3b6dd58126229fda71ed410a6338117cbb41711738dfc673
6435578e6b23d6f03aa939b4016aa995c3b56597516d99133a854130461c8ce
5244caf5b23ffeebfa3b6c8ac8df1194e1a65ed740daf129a325ff3b15d1248
4c7e398e9d97533363068d1b7cc38676e915fbf93264c2209860e37c2"
```

12. IANA Considerations

This document has no IANA actions.

13. Normative References

[I-D.irtf-cfrg-bbs-signatures]
Looker, T., Kalos, V., Whitehead, A., and M. Lodder, "The BBS Signature Scheme", Work in Progress, Internet-Draft, draft-irtf-cfrg-bbs-signatures-08, 3 March 2025, <https://datatracker.ietf.org/api/v1/doc/document/draft-irtf-cfrg-bbs-signatures/>.

[I-D.irtf-cfrg-hash-to-curve]
Faz-Hernandez, A., Scott, S., Sullivan, N., Wahby, R. S., and C. A. Wood, "Hashing to Elliptic Curves", Work in Progress, Internet-Draft, draft-irtf-cfrg-hash-to-curve-16, 15 June 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hash-to-curve-16>.

[I-D.irtf-cfrg-pairing-friendly-curves]
Sakemi, Y., Kobayashi, T., Saito, T., and R. S. Wahby, "Pairing-Friendly Curves", Work in Progress, Internet-Draft, draft-irtf-cfrg-pairing-friendly-curves-11, 6 November 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-pairing-friendly-curves-11>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

14. Informative References

[BBS04] Boneh, D., Boyen, X., and H. Shacham, "Short Group Signatures", In Advances in Cryptology, pages 41-55, 2004, <https://link.springer.com/chapter/10.1007/978-3-540-28628-8_3>.

[BlindBBS] IETF, "Blind BBS Signatures", <https://datatracker.ietf.org/doc/draft-kalos-bbs-blind-signatures/>.

Appendix A. Acknowledgments

TODO acknowledge.

Authors' Addresses

Vasilis Kalos
MATTR
Email: vasilis.kalos@mattr.global

Greg Bernstein
Grotto Networking
Email: gregb@grotto-networking.com