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

V. Kalos
MATTR
G. Bernstein
Grotto Networking

3 March 2025

Blind BBS Signatures
draft-irtf-cfrg-bbs-blind-signatures-01

Abstract

This document defines an extension to the BBS Signature scheme that supports blind digital signatures, i.e., signatures over messages not known to the Signer.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Crypto Forum Research Group mailing list (cfrg@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/cfrg.

Source for this draft and an issue tracker can be found at https://github.com/cfrg/draft-irtf-cfrg-bbs-blind-signatures.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The BBS digital signature scheme, as defined in [I-D.irtf-cfrg-bbs-signatures], can be extended to support blind signatures functionality. In a blind signatures setting, the user (called the Prover in the context of the BBS scheme) will request a signature on a list of messages, without revealing those messages to the Signer (who can optionally also include messages of their choosing to the signature).

By allowing the Prover to acquire a valid signature over messages not known to the Signer, blind signatures address some limitations of their plain digital signature counterparts. In the BBS scheme, knowledge of a valid signature allows generation of BBS proofs. As a result, a signature compromise (by an eavesdropper, a phishing attack, a leakage of the Signer's logs etc.,) can lead to impersonation of the Prover by malicious actors (especially in cases involving "long-lived" signatures, as in digital credentials applications etc.,). Using Blind BBS Signatures on the other hand, the Prover can commit to a secret message (for example, a private key) before issuance, guaranteeing that no one will be able to generate a valid proof without knowledge of their secret.

Furthermore, applications like Privacy Pass ([I-D.ietf-privacypass-protocol]) may require a signature to be "scoped" to a specific audience or session (as to require "fresh" signatures for different sessions etc.,). However, simply sending an audience or session identifier to the Signer (to be included in the signature), will compromise the privacy guarantees that these applications try to enforce. Using blind signing, the Prover will be able to require signatures bound to those values, without having to reveal them to the Signer.

The presented protocol, compared to the scheme defined in [I-D.irtf-cfrg-bbs-signatures], introduces an additional communication step between the Prover and the Signer. The Prover will start by constructing a "hiding" commitment to the messages they

want to get a signature on (i.e., a commitment which reveals no information about the committed values), together with a proof of correctness of that commitment. They will send the (commitment, proof) pair to the Signer, who, upon receiving the pair, will attempt to verify the commitment's proof of correctness. If successful, they will use it in generating a BBS signature over the messages committed by the Prover, including their own messages if any.

This document, in addition to defining the operation for creating and verifying a commitment, also details a core signature generation operation, different from the one presented in [I-D.irtf-cfrg-bbs-signatures], meant to handle the computation of the blind signature. The document will also define a new BBS Interface, which is needed to handle the different inputs, i.e., messages committed by the Prover or chosen by the Signer etc... The signature verification and proof generation core cryptographic operations however, will work as described in [I-D.irtf-cfrg-bbs-signatures]. To further facilitate deployment, both the exposed interface as well as the core cryptographic operation of proof verification will be the same as the one detailed in [I-D.irtf-cfrg-bbs-signatures].

Below is a basic diagram describing the main entities involved in the scheme.

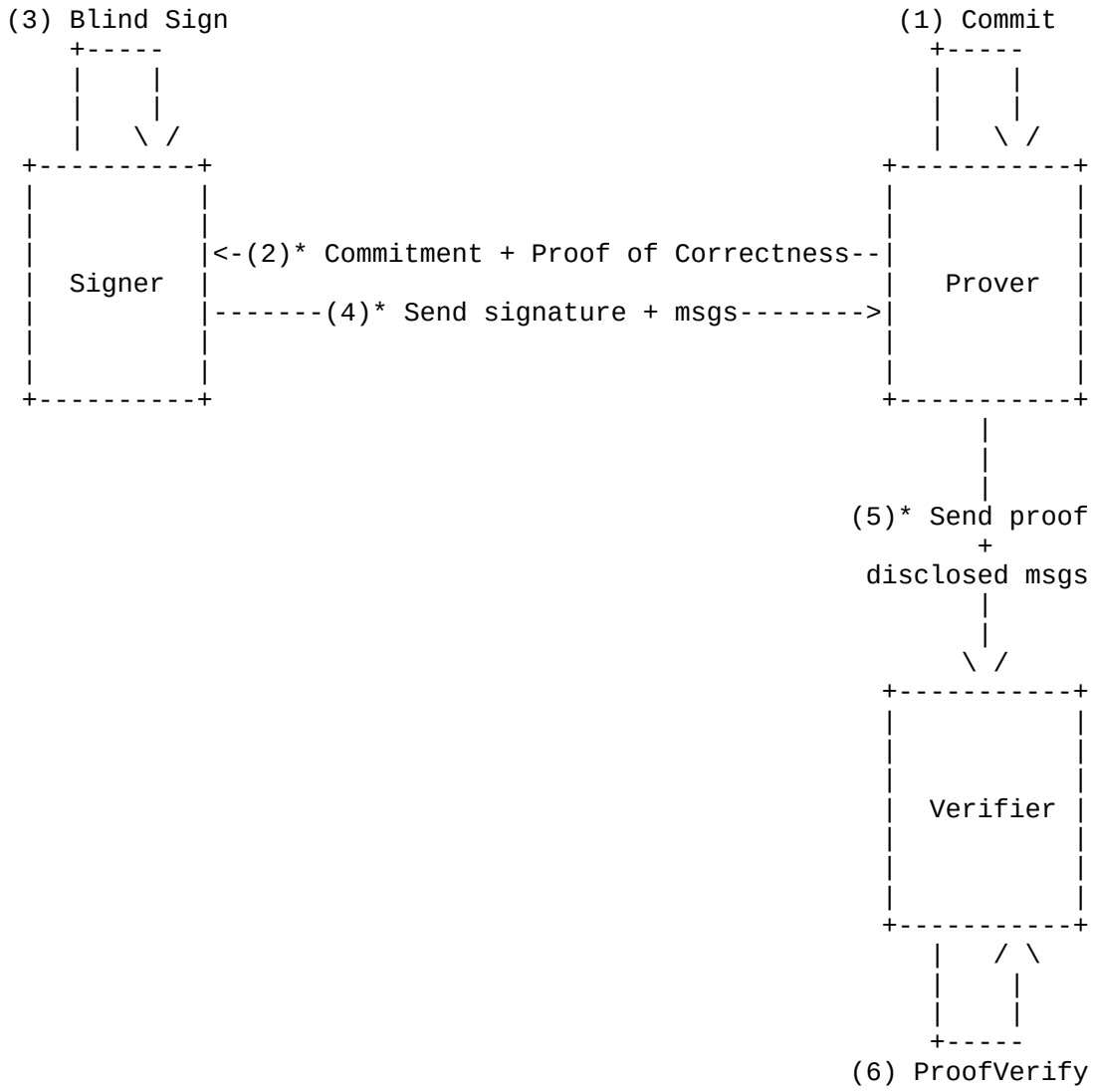

Figure 1: Basic diagram capturing the main entities involved in using the scheme.

Note The protocols implied by the items annotated by an asterisk are out of scope for this specification

1.1. Terminology

Terminology defined by [I-D.irtf-cfrg-bbs-signatures] applies to this draft.

Additionally, the following terminology is used throughout this document:

blind_signature The blind digital signature output.
commitment A point of G1, representing a Pedersen commitment ([P91]) constructed over a vector of messages, as described e.g., in [BG18].
committed_messages A list of messages committed by the Prover to a commitment.
commitment_proof A zero knowledge proof of correctness of a commitment, consisting of a scalar value, a possibly empty set of scalars (of length equal to the number of committed_messages, see above) and another scalar, in that order.
secret_prover_blind A random scalar used to blind (i.e., randomize) the commitment constructed by the prover.
signer_blind A random scalar used by the signer to optionally re-blind the received commitment.
NONE An empty function input indicator, used to specify that one of the OPTIONAL inputs of a procedure is not provided by the calling operation.

1.2. Notation

Notation defined by [I-D.irtf-cfrg-bbs-signatures] applies to this draft.

Additionally, the following notation and primitives are used:

list.append(elements) Append either a single element or a list of elements to the end of a list, maintaining the same order of the list’s elements as well as the appended elements. For example, given list = [a, b, c] and elements = [d, a], the result of list.append(elements) will be [a, b, c, d, a].

2. Conventions

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. BBS Signature Scheme Operations

This document makes use of various operations defined by the BBS Signature Scheme document [I-D.irtf-cfrg-bbs-signatures]. For clarity, whenever an operation will be used defined in [I-D.irtf-cfrg-bbs-signatures], it will be prefixed by "BBS." (e.g., "BBS.CoreProofGen" etc.). More specifically, the operations used are the following:

* BBS.CoreVerify: Refers to the CoreVerify operation defined in Section 3.6.2 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-coreverify) of [I-D.irtf-cfrg-bbs-signatures].
* BBS.CoreProofGen: Refers to the CoreProofGen operation defined in Section 3.6.3 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-coreproofgen) of [I-D.irtf-cfrg-bbs-signatures].
* BBS.create_generators: Refers to the create_generators operation defined in Section 4.1.1 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-generators-calculation) of [I-D.irtf-cfrg-bbs-signatures].
* BBS.messages_to_scalars: Refers to the messages_to_scalars operation defined in Section 4.1.2 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-messages-to-scalars) of [I-D.irtf-cfrg-bbs-signatures].
* BBS.get_random_scalars: Refers to the get_random_scalars operation defined in Section 4.2.1 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-random-scalars) of [I-D.irtf-cfrg-bbs-signatures].
* BBS.hash_to_scalar: Refers to the hash_to_scalar operation defined in Section 4.2.2 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-hash-to-scalar) of [I-D.irtf-cfrg-bbs-signatures].
* BBS.calculate_domain: Refers to the calculate_domain operation defined in Section 4.2.3 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-07.html#domain-calculation) of [I-D.irtf-cfrg-bbs-signatures].

4. Scheme Definition

4.1. Commitment Operations

4.1.1. Commitment Computation

This operation is used by the Prover to create a commitment to a set of messages (committed_messages), that they intend to include in the blind signature. Note that this operation returns both the serialized combination of the commitment and its proof of correctness (commitment_with_proof), as well as the random scalar used to blind the commitment (secret_prover_blind).

```
(commitment_with_proof, secret_prover_blind) = Commit(
                                                  committed_messages,
                                                  api_id)
```

Inputs:

- committed_messages (OPTIONAL), a vector of octet strings. If not supplied it defaults to the empty array ("()").
- 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. blind_generators = BBS.create_generators(
                                  length(committed_message_scalars) + 1,
                                  "BLIND_" || api_id)

3. return CoreCommit(committed_message_scalars,
                             blind_generators, api_id)
```

4.1.2. Commitment Validation and Deserialization

The following is a helper operation used by the BlindSign procedure (Section 4.2.1) to validate an optional commitment. If a commitment is not supplied, or if it is the Identity_G1, the following operation will return the Identity_G1 as the "default" commitment point, which will be ignored by all computations during BlindSign.

```
commit = deserialize_and_validate_commit(commitment_with_proof,
                                         blind_generators, api_id)
```

Inputs:

- commitment_with_proof (OPTIONAL), octet string. If it is not supplied it defaults to the empty octet string ("").
- blind_generators (OPTIONAL), vector of points of G1. If it is not supplied it defaults to the empty set ("()").
- api_id (OPTIONAL), octet string. If not supplied it defaults to the empty octet string ("").

Outputs:

- commit, a point of G1; or INVALID.

Procedure:

```
1. if commitment_with_proof is the empty string (""), return Identity_G1

2. com_res = octets_to_commitment_with_proof(commitment_with_proof)
3. if com_res is INVALID, return INVALID

4. (commit, commit_proof) = com_res
5. if length(commit_proof[1]) + 1 != length(blind_generators),
                                                    return INVALID

6. validation_res = CoreCommitVerify(commit, commit_proof,
                                         blind_generators, api_id)
7. if validation_res is INVALID, return INVALID
8. commitment
```

4.2. Blind BBS Signatures Interface

The following section defines a BBS Interface for blind BBS signatures. The identifier of the Interface is defined as ciphersuite_id || BLIND_H2G_HM2S_, 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]). Each BBS Interface MUST define operations to map the input messages to scalar values and to create the generator set, required by the core operations. The input messages to the defined Interface will be mapped to scalars using the messages_to_scalars operation defined in Section 4.1.2 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-messages-to-scalars) of

[I-D.irtf-cfrg-bbs-signatures]. The generators will be created using the create_generators operation defined in Section 4.1.1 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-generators-calculation) of [I-D.irtf-cfrg-bbs-signatures].

Other than the BlindSign operation defined in Section 4.2.1, which uses the FinalizeBlindSign procedure, defined in Section 4.3.3, all other interface operations defined in this section use the core operations defined in Section 3.6 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-core-operations) of [I-D.irtf-cfrg-bbs-signatures].

4.2.1. Blind Signature Generation

This operation returns a BBS blind signature from a secret key (SK), over a header, a set of messages and optionally a commitment value (see Section 1.1). If supplied, the commitment value must be accompanied by its proof of correctness (commitment_with_proof, as outputted by the Commit operation defined in Section 4.1.1).

The BlindSign operation makes use of the FinalizeBlindSign procedure defined in Section 4.3.3 and the B_calculate procedure defined in Section 5.2. The B_calculate is defined to return an array of elements, to establish extendability of the scheme by allowing the B_calculate operation to return more elements than just the point to be signed.

```
blind_signature = BlindSign(SK, PK, commitment_with_proof, 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 Commit operation. If not supplied, it defaults to the empty string ("").
- 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 ("()").

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.
- (octet_point_length, octet_scalar_length), defined by the ciphersuite.

Outputs:

- blind_signature, a blind signature encoded as an octet string; or
  INVALID.

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 + 1, "BLIND_" || api_id)

3.  commit = 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(generators, commit, message_scalars)
7.  if res is INVALID, return INVALID
8.  (B) = res

9.  blind_sig = FinalizeBlindSign(SK,
                                  PK,
                                  B,
                                  generators,
                                  blind_generators,
                                  header,
                                  api_id)
10. if blind_sig is INVALID, return INVALID
11. return blind_sig
```

4.2.2. Blind Signature Verification

This operation validates a blind BBS signature (signature), given the Signer’s public key (PK), a header (header), a set of, known to the Signer, messages (messages) and if used, a set of committed messages (committed_messages) and the secret_prover_blind as returned by the Commit operation (Section 4.1.1).

This operation makes use of the CoreVerify operation as defined in Section 3.6.2 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-coreverify) of [I-D.irtf-cfrg-bbs-signatures].

```
result = VerifyBlindSign(PK, signature, header, messages, committed_messages,
                                                    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 "()".
- 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:

- result: either VALID or INVALID

Procedure:

```
1. (message_scalars, generators) = prepare_parameters(
                                        messages,
                                        committed_messages,
                                        length(messages) + 1,
                                        length(committed_messages) + 1,
                                        secret_prover_blind,
                                        api_id)

2. res = BBS.CoreVerify(PK, signature, generators, header,
                                                message_scalars, api_id)
3. return res
```

4.2.3. Proof Generation

This operation creates a BBS proof, which is a zero-knowledge, proof-of-knowledge, of a BBS signature, while optionally disclosing any subset of the signed messages. Note that in contrast to the ProofGen operation of [I-D.irtf-cfrg-bbs-signatures] (see Section 3.5.3 (https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html#name-proof-generation-proofgen)), the ProofGen operation defined in this section accepts 2 different lists of messages and disclosed indexes, one for the messages known to the Signer (messages) and the corresponding disclosed indexes (disclosed_indexes) and one for the messages committed by the Prover (committed_messages) and the corresponding disclosed indexes (disclosed_commitment_indexes).

Furthermore, the operation also expects the secret_prover_blind (as returned from the Commit operation defined in Section 4.1.1) value. If the BBS signature is generated using a commitment value, then the secret_prover_blind returned by the Commit operation used to generate the commitment should be provided to the ProofGen operation (otherwise the resulting proof will be invalid).

This operation makes use of the CoreProofGen operation as defined in Section 3.6.3 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-coreproofgen) of [I-D.irtf-cfrg-bbs-signatures].

```
proof = BlindProofGen(PK,
                      signature,
                      header,
                      ph,
                      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) = prepare_parameters(
   messages,
   committed_messages,
   length(messages) + 1,
   length(committed_messages) + 1,
   secret_prover_blind,
   api_id)

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

5. proof = BBS.CoreProofGen(
                    PK,
                    signature,
                    generators,
                    header,
                    ph,
                    message_scalars,
                    indexes,
                    api_id)
6. return proof
```

4.2.4. Proof Verification

The ProofVerify operation validates a BBS proof, given the Signer's public key (PK), a header and presentation header values, two arrays of disclosed messages (the ones known to the Signer and the ones committed by the prover) and two corresponding arrays of indexes those messages had in the original vectors of signed messages. In addition, the BlindProofVerify operation defined in this section accepts the integer L, representing the total number of signed messages known by the Signer.

This operation makes use of the CoreProofVerify operation as defined in Section 3.6.4 (https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html#name-coreproofverify) of [I-D.irtf-cfrg-bbs-signatures].

```
result = BlindProofVerify(PK,
                          proof,
                          header,
                          ph,
                          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 = 2 * octet_point_length + 3 * 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
5. M = total_no_messages - L

Procedure:

1. (message_scalars, generators) = prepare_parameters(
   disclosed_messages,
   disclosed_committed_messages,
   L + 1,
   M,
   NONE,
   api_id)

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

```
5. result = BBS.CoreProofVerify(PK,
                                proof,
                                generators,
                                header,
                                ph,
                                message_scalars,
                                indexes,
                                api_id)
6. return result
```

4.3. Core Operations

4.3.1. Core Commitment Computation

```
(commit_with_proof, secret_prover_blind) = CoreCommit(blind_generators,
                                                      committed_messages, api_id)
```

Inputs:

- blind_generators (REQUIRED), vector of pseudo-random points in G1.
- committed_messages (OPTIONAL), a vector of scalars. 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 ("").

Deserialization:

```
1. M = length(committed_messages)
2. if length(blind_generators) != M + 1, return INVALID
3. (Q_2, J_1, ..., J_M) = blind_generators
```

Procedure:

```
1. (secret_prover_blind, s~, m~_1, ..., m~_M)
                                          = BBS.get_random_scalars(M + 2)
2. C = Q_2 * secret_prover_blind + J_1 * msg_1 + ... + J_M * msg_M
3. Cbar = Q_2 * s~ + J_1 * m~_1 + ... + J_M * m~_M

4. challenge = calculate_blind_challenge(C, Cbar, blind_generators,
                                                                 api_id)

5. s^ = s~ + secret_prover_blind * challenge
6. for m in (1, 2, ..., M): m^_i = m~_1 + msg_i * challenge

7. proof = (s^, (m^_1, ..., m^_M), challenge)
8. commit_with_proof = commitment_with_proof_to_octets(C, proof)
9. return (commit_with_proof, secret_prover_blind)
```

4.3.2. Core Commitment Verification

This operation is used by the Signer to verify the correctness of a commitment_proof for a supplied commitment, over a list of points of G1 called the blind_generators, used to compute that commitment.

```
result = CoreCommitVerify(commitment, commitment_proof,
                                                blind_generators, api_id)
```

Inputs:

- commitment (REQUIRED), a commitment (see (#terminology)).
- commitment_proof (REQUIRED), a commitment_proof (see (#terminology)).
- blind_generators (REQUIRED), vector of pseudo-random points in G1.
- api_id (OPTIONAL), octet string. If not supplied it defaults to the empty octet string ("").

Outputs:

- result: either VALID or INVALID

Deserialization:

```
1. (s^, commitments, cp) = commitment_proof

2. M = length(commitments)
3. (m^_1, ..., m^_M) = commitments

4. if length(blind_generators) != M + 1, return INVALID
5. (Q_2, J_1, ..., J_M) = blind_generators
```

Procedure:

```
1. Cbar = Q_2 * s^ + J_1 * m^_1 + ... + J_M * m^_M + commitment * (-cp)
2. cv = calculate_blind_challenge(commitment, Cbar, blind_generators,
                                                                  api_id)
3. if cv != cp, return INVALID
4. return VALID
```

4.3.3. Finalize Blind Sign

This operation computes a blind BBS signature, from a secret key (SK), a set of generators (points of G1), a supplied commitment with its proof of correctness (commitment_with_proof), a header (header) and a set of messages (messages). The operation also accepts the identifier of the BBS Interface, calling this core operation.

```
blind_signature = FinalizeBlindSign(SK,
                                    PK,
                                    B,
                                    generators,
                                    blind_generators,
                                    header,
                                    api_id)
```

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.
- B (REQUIRED), a point of G1, different than Identity_G1.
- generators (REQUIRED), vector of pseudo-random points in G1.
- blind_generators (OPTIONAL), vector of pseudo-random points in G1. If not supplied it defaults to the empty array.
- header (OPTIONAL), an octet string containing context and application specific information. If not supplied, it defaults to an empty string.
- api_id (OPTIONAL), an octet string. If not supplied it defaults to the empty octet string ("").

Outputs:

- blind_signature, a blind signature encoded as an octet string; or INVALID.

Definitions:

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

Deserialization:

1. L = length(generators) - 1
2. M = length(blind_generators) - 1

3. if L <= 0 or M <=0, return INVALID
4. (Q_1, H_1, ..., H_L) = generators
5. (Q_2, J_1, ..., J_M) = blind_generators

Procedure:

1. domain = BBS.calculate_domain(PK, Q_1, (H_1, ..., H_L, J_1, ..., J_M),

header, api_id)
2. e_octs = BBS.serialize((SK, B, domain))
3. e = BBS.hash_to_scalar(e_octs, signature_dst)
4. A = B * (1 / (SK + e))
5. return BBS.signature_to_octets((A, e))

5. Utilities

5.1. Prepare Parameters

```
(message_scalars, generators) = prepare_parameters(
                                                messages,
                                                committed_messages,
                                                generators_number,
                                                blind_generators_number,
                                                secret_prover_blind,
                                                api_id)
```

Inputs:

- 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 "()".
- secret_prover_blind (OPTIONAL), a scalar value or NONE. If not supplied it defaults to zero "0".
- api_id (OPTIONAL), an octet string. If not supplied it defaults to the empty octet string ("").

Outputs:

- (message_scalars, generators), A vector message_scalars of scalar values and a vector generators of points from the G1 subgroup; or INVALID

Procedure:

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

2. committed_message_scalars = ()

3. if secret_prover_blind != NONE;
committed_message_scalars.append(secret_prover_blind)
4. committed_message_scalars.append(BBS.messages_to_scalars(
committed_messages, api_id))

5. generators = BBS.create_generators(generators_number, api_id)
6. blind_generators = BBS.create_generators(
blind_generators_number, "BLIND_" || api_id)

7. return (message_scalars.append(committed_message_scalars),
generators.append(blind_generators))

5.2. Calculate B value

```
res  = B_calculate(generators, commitment, message_scalars)

Inputs:

- generators (REQUIRED), an array of at least one point from the
                         G1 group.
- commitment (OPTIONAL), a point from the G1 group. If not supplied it
                         defaults to the Identity_G1 point.
- message_scalars (OPTIONAL), an array of scalar values. If not
                              supplied, it defaults to the empty
                              array ("()").

Outputs:

- res, an array of a single element from the G1 subgroup, or INVALID.

Deserialization:

1. L = length(messages)
2. if length(generators) != L + 1, return INVALID
3. (Q_1, H_1, ..., H_L) = generators
4. (msg_1, ..., msg_L) = messages

Procedure:

1. B = Q_1 + H_1 * msg_1 + ... + H_L * msg_L + commitment
2. if B is Identity_G1, return INVALID
3. return B
```

5.3. Blind Challenge Calculation

challenge = calculate_blind_challenge(C, Cbar, generators, api_id)

Inputs:

- C (REQUIRED), a point of G1.
- Cbar (REQUIRED), a point of G1.
- generators (REQUIRED), an array of points from G1, of length at least 1.
- api_id (OPTIONAL), octet string. If not supplied it defaults to the empty octet string ("").

Definition:

- blind_challenge_dst, an octet string representing the domain separation tag: api_id || "H2S_" where ciphersuite_id is defined by the ciphersuite and "H2S_" is an ASCII string composed of 4 bytes.

Deserialization:

1. if length(generators) == 0, return INVALID
2. M = length(generators) - 1

Procedure:

1. c_arr = (M)
2. c_arr.append(generators)
3. c_octs = BBS.serialize(c_arr.append(C, Cbar))
4. return BBS.hash_to_scalar(c_octs, blind_challenge_dst)

5.4. Serialize

5.4.1. Commitment with Proof to Octets

commitment_octets = commitment_with_proof_to_octets(commitment, proof)

Inputs:

- commitment (REQUIRED), a point of G1.
- proof (REQUIRED), a vector comprising of a scalar, a possibly empty vector of scalars and another scalar in that order.

Outputs:

- commitment_octets, an octet string or INVALID.

Procedure:

1. commitment_octs = BBS.serialize(commitment)
2. if commitment_octs is INVALID, return INVALID
3. proof_octs = BBS.serialize(proof)
4. if proof_octs is INVALID, return INVALID
5. return commitment_octs || proof_octs

5.4.2. Octet to Commitment with Proof

```
commitment = octets_to_commitment_with_proof(commitment_octs)

Inputs:

- commitment_octs (REQUIRED), an octet string in the form outputted from
                              the commitment_to_octets operation.

Parameters:

- (octet_point_length, octet_scalar_length), defined by the ciphersuite.

Outputs:

- commitment, a commitment in the form (C, proof), where C a point of G1
              and a proof vector comprising of a scalar, a possibly
              empty vector of scalars and another scalar in that order.

Procedure:

1.  commit_len_floor = octet_point_length + 2 * octet_scalar_length
2.  if length(commitment_octs) < commit_len_floor, return INVALID

3.  C_octets = commitment_octs[0..(octet_point_length - 1)]
4.  C = octets_to_point_g1(C_octets)
5.  if C is INVALID, return INVALID
6.  if C == Identity_G1, return INVALID

7.  j = 0
8.  index = octet_point_length
9.  while index < length(commitment_octs):
10.     end_index = index + octet_scalar_length - 1
11.     s_j = OS2IP(commitment_octets[index..end_index])
12.     if s_j = 0 or if s_j >= r, return INVALID
13.     index += octet_scalar_length
14.     j += 1

15. if index != length(commitment_octs), return INVALID
16. if j < 2, return INVALID
17. msg_commitment = ()
18. if j >= 3, set msg_commitment = (s_2, ..., s_(j-1))
19. return (C, (s_0, msg_commitments, s_j))
```

6. Security Considerations

Security considerations detailed in Section 6 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-security-considerations) of [I-D.irtf-cfrg-bbs-signatures] apply to this draft as well.

6.1. Prover Blind Factor

The random scalar value secret_prover_blind calculated and returned by the Commit operation is responsible for "hiding" the committed messages (otherwise, in many practical applications, the Signer may be able to retrieve them). Furthermore, it guarantees that the entity generating the BBS proof (see BlindProofGen defined in Section 4.2.3) has knowledge of that factor. As a result, the secret_prover_blind MUST remain private by the Prover and it MUST be generated using a cryptographically secure pseudo-random number generator. See Section 6.7 (https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html#name-randomness-requirements) of [I-D.irtf-cfrg-bbs-signatures] on recommendations and requirements for implementing the BBS.get_random_scalars operation (which is used to calculate the secret_prover_blind value).

6.2. Key Binding

One natural use case for the blind signatures extension of the BBS scheme is key binding. In the context of BBS Signatures, key binding guarantees that only entities in control of a specific private key can compute BBS proofs. This can be achieved by committing to the private key prior to issuance, resulting in a BBS signature that includes that key as one of the signed messages. Creating a BBS proof from that signature will then require knowledge of that key (similar to any signed message). The Prover MUST NOT disclose that key as part of a proof generation procedure. Note also that the secret_prover_blind value returned by the Commit operation defined in Section 4.1.1 (see Section 6.1), has a similar property, i.e., it’s knowledge is required to generate a proof from a blind signature. Many applications however, requiring key binding, mandate that the same private key is used among multiple signatures, whereas the secret_prover_blind is uniquely generated for each blind signature issuance request. In those cases, a commitment to a private key must be used, as described above.

7. Ciphersuites

This document uses the BBS_BLS12381G1_XOF:SHAKE-256_SSWU_RO_ and BBS_BLS12381G1_XMD:SHA-256_SSWU_RO_ defined in Section 7.2.1 (https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html#name-bls12-381-shake-256) and Section 7.2.2 (https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html#name-bls12-381-sha-256) correspondingly, of [I-D.irtf-cfrg-bbs-signatures].

8. Test Vectors

8.1. BLS12-381-SHA-256

8.1.1. Generators

```
api_id = "BBS_BLS12381G1_XMD:SHA-256_SSWU_RO_BLIND_H2G_HM2S_"

P1 = "a8ce256102840821a3e94ea9025e4662b205762f9776b3a766c872b948f1fd225e
      7c59698588e70d11406d161b4e28c9"
Q1 = "8aa0382ea3cd294680e3425bb0bb9293210a4d3e94d8ba59096fcb24eb9b565466
      45bea83e170b078ff3cc5aeac18c49"

Generators = {

H_0 = "8065ec88f9bbee345b44e7825b2d602c91b0398b7c885d722450459c26efb1619
       eb4249428644b9e3d8d11d469d0c62b"
H_1 = "b96f3af9abcd3ee2228fbe97d4e5a0ef10aaf655c6889e284f27a732492ecdb64
       a91f92dbaa93f2a7fb550659935985f"
H_2 = "a99d1b53cc51738a46a7e1fe9b9d89a57977154dcccb7ce741eb779bf69ff655b
       110f0e97c4715616401e5a47d2c373a"
H_3 = "9791c624fec3d688975f9c9143f066404115e0dcc1e318ef4f5290c0103ee4a28
       57dbf9347d997ee507ab629216797f6"
H_4 = "8a472740d4968c831a3ad3d3c55ada8aca8478e4d0698ece52eff445d15aec1a4
       79332e34562e80831b9593c85b435ec"
H_5 = "b5102a6529b39de47c136de78a8697395e11013f8aa91f695f158009b52985ade
       e67a63fc354846b7f4b944349295c95"
H_6 = "845df3031a580f6c58b6d324f42f2158088a924dab9e77151851408a8bda31c26
       6000c10bc47cc38aa3ac24dad22462c"
H_7 = "b4296c820736cafb7c9229cf499788314a4578de69e88832ca39babe36c48073e
       61968ae320f9bae61079724a5271eac"
H_8 = "9253f55dacd9e144f6da37f4adb420773325d142d900a6ae7de851c2643532e0b
       9181ae3ee02fe8c123b10dd12822876"
H_9 = "979a52e753c367e3baa8826e7b74a23856abca5468ba5ce5719b4c57eb7e9ee87
       9935f98fbd6959661d3e866477063b2"

}
```

8.1.2. Blind Generators

```
api_id = "BLIND_BBS_BLS12381G1_XMD:SHA-256_SSWU_RO_BLIND_H2G_HM2S_"

P1 = "a8ce256102840821a3e94ea9025e4662b205762f9776b3a766c872b948f1fd225e
      7c59698588e70d11406d161b4e28c9"
Q1 = "a347532dc0ba9b83e4f15f3eeb7dffd934f5fa4668d927fbcb68096d5a26f6e59f
      66681201be1c263af1a25b6749759c"

Blind Generators = {

J_0 = "af590ba56aa0e526a0763ae6926347dce988ffb9cc1a0b4510ada06fe08816f5c
       36a6c7007cc8558e5793f9a2cbae462"
J_1 = "a9a6e5f3093823745734a2195d80886f47185be6a3e4d00df2bd5996aa9d664e3
       4244ea15e9ad4c41d8825331fcfd5a3"
J_2 = "a6c1a8fd251a338e25d3ea4e09334ea250f0257783f2be4ce4406798ea9acbce4
       1e7648c7fb1409fcd822396f652c4e7"
J_3 = "80d1232ee4a5623d7ac5a3912c555f9f6f34716edfe156ae40b6ac19afba58dd1
       8556e49529e39da91aa806c9c55d493"
J_4 = "b8775d3d2f58cafd808d135de79367f34c9ad22a6a878631fd0b1383541999b16
       b6f3bae96ab51bb4ab25caf69462473"

}
```

8.1.3. Commitment

Mocked random scalar parameters

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

8.1.3.1. valid no committed messages commitment with proof

```
committedMessages = "[  ]"
proverBlind = "1b6f406b17aaf92dc7deb911c7cae49756a6623b5c385b5ae6214d7e3
               d9597f7"

Trace:

s_tilde = "0b71f3e3fc1517bd763b180dc4f6d269da8c96fb5307653b77205c31e40c5
           21e"
m_tildes = "[  ]"

commitmentWithProof = "849d3cc626720202cbc1610fc01ab41ce32099af602def0c5
                       79f37dd18b485ef60719275a036bdd8120e7e938c8e1a3d4d
                       0322587441ccc5caf186001b45dd09ee159713c3e3ea0f411
                       f94a5d6665546562d09c093b687a129e464a57e18cdbf5306
                       bcabf3e7cc95f5ba98cdd9bf3768"
```

8.1.3.2. valid multiple committed messages commitment with proof

```
committedMessages = "[ 5982967821da3c5983496214df36aa5e58de6fa25314af4cf
                       4c00400779f08c3, a75d8b634891af92282cc81a675972d192
                       9d3149863c1fc0, 835889a40744813a892eff9deb1edaeb, e
                       1ca9729410dc6ba,  ]"
proverBlind = "4fba5396baa36b2fde81d46a9b9ee89c425dbc5e1ffd65c20249afb4a
               bd37589"

Trace:

s_tilde = "2c78a955f6598824fc77bf6cb5a8b58204da0cadb499faf4bbee2d4fceadc
           0d1"
m_tildes = "[ 2b8c33fb06580d8dffdc72212967ae75838859096abeea973cc0d9e80a
            c1946c, 2b9e86176d6a4c5b63fcd4a4ace793316c0f7adccdc888b308b5
            408bd6a21b89, 005c784be3f30d47393996fe596adbbe30aeb1d3a8d888
            b5075aa56d3b2be35c, 6b64079fac7b8d026520647b5764c5dbbe8b5486
            efb7791f5742511129c36a87, 41cbd69ac7603928be8e96d29756fe6763
            e5de8103c68eb484744ebb29bd2a1b ]"

commitmentWithProof = "a2a3e178bcc77f98a3c07f8532134021ab5847326b5b3bfc3
                       089ca73f1bc51cfe2c99163f4919525dd6bedc8a14ee39e30
                       374643902017ca2e6fb8b5647c736e82d1d3c5b05de5c3021
                       fa6f40d9f36dd22fa06e522411aa20377088ca9a15885d7a5
                       044175f0168e927149ee71e2d257079e0100d6d96a7ddf539
                       2dbc64267af8df7b4711cb5eeccb5e8901d0580b9e837f383
                       37cb7260cffcf4f962154fafe5c98beaed7e4d2fc0f8e7eb1
                       ba4eb04086f170aa4924894e2ab63054049c9ef5dfff4f90b
                       48ef0dcf1f50699907301073270e4782d4d7628cfbe1444ce
                       a930928bb45004e41e0ad86a874ea03473845ce42f78ceb6f
                       855ba8326a4d47732c5aed3968b396a07f079b22b5bf2139e51a03"
```

8.1.4. Signature Test Vectors

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

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

header = "11223344556677889900aabbccddeeff"
messages = "[  ]"

commitmentWithProof = "849d3cc626720202cbc1610fc01ab41ce32099af602def0c5
                       79f37dd18b485ef60719275a036bdd8120e7e938c8e1a3d4d
                       0322587441ccc5caf186001b45dd09ee159713c3e3ea0f411
                       f94a5d6665546562d09c093b687a129e464a57e18cdbf5306
                       bcabf3e7cc95f5ba98cdd9bf3768"

committedMessages = "[  ]"

proverBlind = "1b6f406b17aaf92dc7deb911c7cae49756a6623b5c385b5ae6214d7e3
               d9597f7"

Trace:

B = "9964a978251fcc52c918dee3d8f102d2152fa7a805df85b1e91e0c45d4d8d7c02aa
     b78353a240176f6a33899b98b3379"
domain = "0b3a152bc770ff9e21f09ac58f59c99379ca0eeb61990ba666d994014085b3
          32"

signature = "ab54c35fb2af5c75d6368bc5772547e126d60a92205d011bb9ee5d11494
             32e91611fd376fe5b79d6ed7c2ba00a19b7434744945fd77bf02cd4628a
             6e5deeae50768116d55510251bb6a716a38340e184"
```

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

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

header = "11223344556677889900aabbccddeeff"
messages = "[  ]"

commitmentWithProof = "a2a3e178bcc77f98a3c07f8532134021ab5847326b5b3bfc3
                       089ca73f1bc51cfe2c99163f4919525dd6bedc8a14ee39e30
                       374643902017ca2e6fb8b5647c736e82d1d3c5b05de5c3021
                       fa6f40d9f36dd22fa06e522411aa20377088ca9a15885d7a5
                       044175f0168e927149ee71e2d257079e0100d6d96a7ddf539
                       2dbc64267af8df7b4711cb5eeccb5e8901d0580b9e837f383
                       37cb7260cffcf4f962154fafe5c98beaed7e4d2fc0f8e7eb1
                       ba4eb04086f170aa4924894e2ab63054049c9ef5dfff4f90b
                       48ef0dcf1f50699907301073270e4782d4d7628cfbe1444ce
                       a930928bb45004e41e0ad86a874ea03473845ce42f78ceb6f
                       855ba8326a4d47732c5aed3968b396a07f079b22b5bf2139e51a03"

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

proverBlind = "4fba5396baa36b2fde81d46a9b9ee89c425dbc5e1ffd65c20249afb4a
               bd37589"

Trace:

B = "b21004683409ac48cab4ac654761afa96b90d72742c2a3d1c66343df47713737e6b
     2367f1dbf0bd917e6f8bc3fd1440a"
domain = "13c94073eb7dbd279f60d5907c19d83e4a9ae19f99d6b3ca020785730a3f37
          eb"

signature = "b7446e6ae4e8b5707ac0108f3b1049e9ea01bd6b2b4a7dcf06e5ad1c62a
             9c0b1585829f0e30fba6c9761469ed908deca52ba5499cef2827b99527b
             4adf1f30522ce32366385ba87594b8d0e44d156eec"
```

8.1.4.3. 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,  ]"

commitmentWithProof = "849d3cc626720202cbc1610fc01ab41ce32099af602def0c5
                       79f37dd18b485ef60719275a036bdd8120e7e938c8e1a3d4d
                       0322587441ccc5caf186001b45dd09ee159713c3e3ea0f411
                       f94a5d6665546562d09c093b687a129e464a57e18cdbf5306
                       bcabf3e7cc95f5ba98cdd9bf3768"

committedMessages = "[  ]"

proverBlind = "1b6f406b17aaf92dc7deb911c7cae49756a6623b5c385b5ae6214d7e3
               d9597f7"

Trace:

B = "99c95be56780fa694d182ca279de80297eb93fae1c8f398c7bc155b0a3be3abc7c6
     1813cfead8a35a89dc4d7118b266f"
domain = "a2271347c620cd43982d4f53dbdd176db8c87fbec6eb15318355bdb39da7d1
          9933f1bbb1845e7c547f8fb2e9858d1ff9"

signature = "b869cccbe84dce890949db3393c963ead72d044863b2c75bc26c0adfbe0
             8b5bb01db9e4db3313fc660ebb3283634772809d177d191bffde6fe7fbd
             8ca95d7b842e434ae973b7e458325b9eb23b6cf076"
```

8.1.4.4. 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,  ]"

commitmentWithProof = "a2a3e178bcc77f98a3c07f8532134021ab5847326b5b3bfc3
                       089ca73f1bc51cfe2c99163f4919525dd6bedc8a14ee39e30
                       374643902017ca2e6fb8b5647c736e82d1d3c5b05de5c3021
                       fa6f40d9f36dd22fa06e522411aa20377088ca9a15885d7a5
                       044175f0168e927149ee71e2d257079e0100d6d96a7ddf539
                       2dbc64267af8df7b4711cb5eeccb5e8901d0580b9e837f383
                       37cb7260cffcf4f962154fafe5c98beaed7e4d2fc0f8e7eb1
                       ba4eb04086f170aa4924894e2ab63054049c9ef5dfff4f90b
                       48ef0dcf1f50699907301073270e4782d4d7628cfbe1444ce
                       a930928bb45004e41e0ad86a874ea03473845ce42f78ceb6f
                       855ba8326a4d47732c5aed3968b396a07f079b22b5bf2139e51a03"

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

proverBlind = "4fba5396baa36b2fde81d46a9b9ee89c425dbc5e1ffd65c20249afb4a
               bd37589"

Trace:

B = "8e1c3ee4b13e5936f9cb5f87342107ed9ab4417c04d6e5d712143a54bdb476aaf42
     40e8a4f11a67d81feb1398f889889"
domain = "1207ed090723fa7e41c07e970ebb647d1d043079cc2a38c650c32234f18239
          36"

signature = "862eb2fedd0a2b76fb978035cb33952004bdd6136e107bb343cb2c5ea56
             6eb0c3b0ba31b1d022ebf03d0abf050ab293c0afd9c96003331aa13f18a
             7a47e2e1ccaa8feb7f3a236e92b2da38462358c48a"
```

8.1.4.5. valid no commitment 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,  ]"

commitmentWithProof = "null"

committedMessages = "null"

proverBlind = "null"

Trace:

B = "874d657ff2b90023d18c8eb1d2fbc0beb8b9c1ae98a285db1076466edd7c0a3179b
     c572d4f7b0e15b39cbe298d2023cd"
domain = "1430cf0a3d8a0519a9ecf47534b6026a7671935d9854ed5e68b42fdb543d5f
          7a"

signature = "8aa8fdfb190987d1fe1c8e34e69eae25594701958064e4483d74580a4a0
             f51f058a87735d727383b864904aa7b5e4a9b3821a18319df0ccb2e351a
             9bf75bf1f34d8858dde57119bfafd8ff56e0c54fa4"
```

8.1.5. Proof Test Vectors

Mocked random scalar parameters

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

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

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "862eb2fedd0a2b76fb978035cb33952004bdd6136e107bb343cb2c5ea56
             6eb0c3b0ba31b1d022ebf03d0abf050ab293c0afd9c96003331aa13f18a
             7a47e2e1ccaa8feb7f3a236e92b2da38462358c48a"

commitmentWithProof = "a2a3e178bcc77f98a3c07f8532134021ab5847326b5b3bfc3
                       089ca73f1bc51cfe2c99163f4919525dd6bedc8a14ee39e30
                       374643902017ca2e6fb8b5647c736e82d1d3c5b05de5c3021
                       fa6f40d9f36dd22fa06e522411aa20377088ca9a15885d7a5
                       044175f0168e927149ee71e2d257079e0100d6d96a7ddf539
                       2dbc64267af8df7b4711cb5eeccb5e8901d0580b9e837f383
                       37cb7260cffcf4f962154fafe5c98beaed7e4d2fc0f8e7eb1
                       ba4eb04086f170aa4924894e2ab63054049c9ef5dfff4f90b
                       48ef0dcf1f50699907301073270e4782d4d7628cfbe1444ce
                       a930928bb45004e41e0ad86a874ea03473845ce42f78ceb6f
                       855ba8326a4d47732c5aed3968b396a07f079b22b5bf2139e51a03"
proverBlind = "4fba5396baa36b2fde81d46a9b9ee89c425dbc5e1ffd65c20249afb4a
               bd37589"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

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 = "2cf2bd257845b6138247ad87cb387aee347a9104fd1090f92e3b7559e855b068"
r_2 = "14f989abea9c9d0cbae6d72e2eb806ac7dbfcd08a8ed647ad5b8e16a83b94d4a"
e_tilde = "07e5d7e2b504d3e3075617400781df19831fac0763602bc494b3fe40dcdef
           b47"
r1_tilde = "35888226d06bd50f1901008bdf70b1472ad98304664828c6a0fa45b396cc
            a7d9"
r3_tilde = "21e5d2a43d0190ddee9319dab20ad1bfaacf7c12399ac384fe9bf1235c19
            1907"
m_tilde_scalars = "[ 6683a44c7e1b057c7ce5e99dca9d71a091441b6c23ad9bfd45b
                    a23862f610cf7 ]"

domain = "1207ed090723fa7e41c07e970ebb647d1d043079cc2a38c650c32234f18239
          36"
challenge = "5c1dd59fd821e66b06a117d7248b8676e5c15da737cbeb371790a379171
             30e74"


L = "10"

proof = "a80ea73d954433eca5bff121e0ad4b41e91d2b600cc717eff3804f11ef21cc9
         b9b20da25387722ae6b2dd78103a3413484c3a88248f51c9bfe93cbd88dabc6
         19ba8a432814b15f8dfe601c1cac5404986541968307c8d06acf63ab906c411
         77ba9e5e8f4f1ff77426d3e905b7809243e9ae10acd1013c40525c257e3fe6f
         1bec2a5204433d354f3508eb93e24c91e49b60e8c0bd15af07241c43301024d
         5d8701516307a7b1bb381fbc3bfcaefa4d092519b4996840e199e7e2c40d75d
         593a993ea002fe4d411a9ef650cd0416033ff04d1bb51ca8377b789a2747206
         95c86f5e70ecb56c4abcb3b6ff88edf48677c273ca24547a67e10d4deab8b9c
         989c48d9414b1c05bf61b8f8ae73c9d48c37dec55c1dd59fd821e66b06a117d
         7248b8676e5c15da737cbeb371790a37917130e74"
```

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

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "862eb2fedd0a2b76fb978035cb33952004bdd6136e107bb343cb2c5ea56
             6eb0c3b0ba31b1d022ebf03d0abf050ab293c0afd9c96003331aa13f18a
             7a47e2e1ccaa8feb7f3a236e92b2da38462358c48a"

commitmentWithProof = "a2a3e178bcc77f98a3c07f8532134021ab5847326b5b3bfc3
                       089ca73f1bc51cfe2c99163f4919525dd6bedc8a14ee39e30
                       374643902017ca2e6fb8b5647c736e82d1d3c5b05de5c3021
                       fa6f40d9f36dd22fa06e522411aa20377088ca9a15885d7a5
                       044175f0168e927149ee71e2d257079e0100d6d96a7ddf539
```

```
                        2dbc64267af8df7b4711cb5eeccb5e8901d0580b9e837f383
                        37cb7260cffcf4f962154fafe5c98beaed7e4d2fc0f8e7eb1
                        ba4eb04086f170aa4924894e2ab63054049c9ef5dfff4f90b
                        48ef0dcf1f50699907301073270e4782d4d7628cfbe1444ce
                        a930928bb45004e41e0ad86a874ea03473845ce42f78ceb6f
                        855ba8326a4d47732c5aed3968b396a07f079b22b5bf2139e51a03"
proverBlind = "4fba5396baa36b2fde81d46a9b9ee89c425dbc5e1ffd65c20249afb4a
               bd37589"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

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 = "5a113c961c5d21bd78b50c3079ea482f5e861c20be37899d26e2ba565ea67093"
r_2 = "1ce7fcf7fc75bffdf3cd0a284a5cd4acf6be87df552fa937f246a38e8c03af0b"
e_tilde = "286458907bcd8e3fc535ed9575531919d1942a907ef8ed10360e292fca5ad
           0bb"
r1_tilde = "40caa7858d917197f007c87ea7e80f638db1313b0e3d46612bb2e73798bb
            24c8"
r3_tilde = "6d30be5b88e8cb333e4872bdf0c4d7cffe4540eddf03eafaae3d4cb1f3ad
            1cda"
m_tilde_scalars = "[ 342ddc1b4e04cef472c764f5bda8afae4b189e78ffcbb519075
                  a83e640c0100c, 51608282827ece21a8ed20b774e2ff12935341
                  6006317c16e409e1a925540345, 0c1ff555f2b0f53e8859aff29
                  47b22b1ef9d2be2c65621d8f6aa3252340fcaf2 ]"
```

```
domain = "1207ed090723fa7e41c07e970ebb647d1d043079cc2a38c650c32234f18239
          36"
challenge = "6f77fc07c8857b819c764ae92d3779b4bf76f875b4589b37daad83c6bf1
             889ba"

L = "10"

proof = "a1fe94ec24e6d325d2494e10bdc395bd82e613e8dd08ca8f4eeffee294246b9
         321cc0e5997de7ae473a4d4c39f27b9088c815c0ff4f8ff7da0ef6d3338e048
         e2b28d98e148e1e8717b6ff6dfc4c74379aab5f409212986ce667c0b9ae4c48
         c278720d66be792af1a62989ea56f433a17f05af1f761b48b9ae2bb24418208
         111680d75c8b7d781186afedbe7c7f293b644cad32737358fed7adc516ec643
         19298fa4d22e2119db88e846f4d8665858b0930016a56245de910baa76242d3
         b2f48d61e78491695773063178c1f35d392198616b619fb5019a17fd6ec0bbb
         f6820cfe6bf8eb58801049465d86aca537126b759f76d65d2239d71584c85c3
         71ff9bc0fd38ebd6623df2cba477ef0ffb0c0c9f35e8a6b4c2c865f4e1b0e5b
         c543601c0a209816a420bd9a6b71e0cf9bc330cc2078c8d74f7c741b2fc6ce3
         e553fe11d4ee2e02b34e81bd06074dfc892b87046a6f77fc07c8857b819c764
         ae92d3779b4bf76f875b4589b37daad83c6bf1889ba"
```

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

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "862eb2fedd0a2b76fb978035cb33952004bdd6136e107bb343cb2c5ea56
             6eb0c3b0ba31b1d022ebf03d0abf050ab293c0afd9c96003331aa13f18a
             7a47e2e1ccaa8feb7f3a236e92b2da38462358c48a"

commitmentWithProof = "a2a3e178bcc77f98a3c07f8532134021ab5847326b5b3bfc3
                       089ca73f1bc51cfe2c99163f4919525dd6bedc8a14ee39e30
                       374643902017ca2e6fb8b5647c736e82d1d3c5b05de5c3021
                       fa6f40d9f36dd22fa06e522411aa20377088ca9a15885d7a5
                       044175f0168e927149ee71e2d257079e0100d6d96a7ddf539
                       2dbc64267af8df7b4711cb5eeccb5e8901d0580b9e837f383
                       37cb7260cffcf4f962154fafe5c98beaed7e4d2fc0f8e7eb1
                       ba4eb04086f170aa4924894e2ab63054049c9ef5dfff4f90b
                       48ef0dcf1f50699907301073270e4782d4d7628cfbe1444ce
                       a930928bb45004e41e0ad86a874ea03473845ce42f78ceb6f
                       855ba8326a4d47732c5aed3968b396a07f079b22b5bf2139e51a03"
proverBlind = "4fba5396baa36b2fde81d46a9b9ee89c425dbc5e1ffd65c20249afb4a
               bd37589"

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

```
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 = "034d543fdd164520876e558a77c102d4ad8bc99bf82ebe74590481473df2df56"
r_2 = "4a8334929ba48d36eb4ebc7f8bfa701b4d3f30ef25bc01e2a45ef9611c16037f"
e_tilde = "19726feed8e0e5ff22e4f5de19713977beceb12c3e85c1f3fb41cfe4a7237
           d1a"
r1_tilde = "73012dc2f14039c8de5853b26baab7b51280a3f41425416d78a1a91fbaae
            9bf2"
r3_tilde = "68263029bdc322a3d6460758135205dec58957ff3e5397276a2f0ffdc738
            d5e4"
m_tilde_scalars = "[ 52638b8d190f9fd439188b22c903507cfe5282296c2c9f605f1
                    ef714afc14062, 2cbc33e381cf6ae09dbb6f1d08e3ea93a5aa03
                    c4a6574fd2fa2e879dc4deeca9, 1ec36e6be1c702255d9aa4d59
                    0014b2b5de2f07d290c9551b66977cde157094b, 5491612228a9
                    93693c79c11ae169dad9be4116a704ae9ed333ef96e3986373a0,
                     6f4d920974d33c1e08c86b7f4b6bb7c58a5c0289d8d706a92d48
                    55125ccedb70, 279717a2b1e1d34cccfddfe9c8e3729f6e92e28
                    197a09459c6dcd56e3920a0d7 ]"

domain = "1207ed090723fa7e41c07e970ebb647d1d043079cc2a38c650c32234f18239
          36"
challenge = "03ec71a4d9d89d066763fd6a055e6a9e42a3b6a153732a42a5be5bfd2cf
             85b7d"

L = "10"

proof = "82a7815ebceefbfb5c1728c940b8ec6efe0d64c6c53c5b7e5a01a598f3e904b
         f4eb43f94f3c41c2c73bf86ad6b4d9a6f87b89bb4c08ab7d0aa1afa52de982f
         b5f173b88db16b09a25358489da59d7d8da1f603aa83b55a6664e276e8b2498
```

```
          5de93c5ee7b5fe52c329660f963fa3a26b9316aaddbdb83e764fdb4323be987
          0a9d7fa18c9136ad79d06f6de5e820631cd30a1739ba5dd8f204020cf071e8a
          1a5313e4a3eb1ba058c91f37f397976920eff270ff2bb79bdab9dd006752c91
          5b22e2fff4f362a1dd663b2a178bb7ae08d1a6251e39fb11ff14b24a237ff2d
          8be9fe8d0db493dc019535e53dd31c0608543fb69f9fb31d1483514e65edc9c
          5111281409df08b88d333e4cc76fc41a45e49767523813f5e585c562933a6d7
          fd8b664102bd4822ba062ccee37ea50a3c9e03fc642b84c7d422155b61d69e5
          a832e41169bb08748ac245be18e159be1bb343afc170483a8887fe5b889adc4
          3f410529c7fad530084b1cc90f8854d8bf402def3f90e525e4bc99b5b8b8095
          495651f2cb6844b91a7832744954ca5bbf9a4f9c863c6b3485ad58bdb54fa6c
          71058fe29296eab761ab1a2c4be2db749c40f173f8b2e03ec71a4d9d89d0667
          63fd6a055e6a9e42a3b6a153732a42a5be5bfd2cf85b7d"
```

8.1.5.4. valid half prover committed messages and half signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "862eb2fedd0a2b76fb978035cb33952004bdd6136e107bb343cb2c5ea56
             6eb0c3b0ba31b1d022ebf03d0abf050ab293c0afd9c96003331aa13f18a
             7a47e2e1ccaa8feb7f3a236e92b2da38462358c48a"

commitmentWithProof = "a2a3e178bcc77f98a3c07f8532134021ab5847326b5b3bfc3
                       089ca73f1bc51cfe2c99163f4919525dd6bedc8a14ee39e30
                       374643902017ca2e6fb8b5647c736e82d1d3c5b05de5c3021
                       fa6f40d9f36dd22fa06e522411aa20377088ca9a15885d7a5
                       044175f0168e927149ee71e2d257079e0100d6d96a7ddf539
                       2dbc64267af8df7b4711cb5eeccb5e8901d0580b9e837f383
                       37cb7260cffcf4f962154fafe5c98beaed7e4d2fc0f8e7eb1
                       ba4eb04086f170aa4924894e2ab63054049c9ef5dfff4f90b
                       48ef0dcf1f50699907301073270e4782d4d7628cfbe1444ce
                       a930928bb45004e41e0ad86a874ea03473845ce42f78ceb6f
                       855ba8326a4d47732c5aed3968b396a07f079b22b5bf2139e51a03"
proverBlind = "4fba5396baa36b2fde81d46a9b9ee89c425dbc5e1ffd65c20249afb4a
               bd37589"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

revealedMessages =

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

```
revealedCommittedMessages  =

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


Trace:

random_scalars:

r_1 = "6fe2700deae18571f365d5b549a03eca3a19414532982cdb173e6442f8488a82"
r_2 = "4cc007c238298166e67bcbc8332435b27f39879b75ab00ed5e6863f6296051a4"
e_tilde = "53f3c5e5ff89fb20a89d7fffa1198b13744d1ae78457119e5bb3da42d77bf
           e56"
r1_tilde = "14e6c0d53eba55936c1f1ff11d9775fde7bc366d1859cdbd9ec9f65510a1
            9b02"
r3_tilde = "0a3c38367bd4f42d8b44d988580b40ad1c929a3844fd92e0d2c2a7247962
            18b4"
m_tilde_scalars = "[ 4e27cd534e2d06c2af769760a2651010d8f2495066c4a4bbf33
                   778f558c72b09, 2ea785a49f1b29d7f79323d5e369e3598665c6
                   e6ed1352797dcdd20b249d58fe, 438393d39c51a4efe0bf3b53a
                   cf17a7b26724ad7de58ff8bd5fdf9dea0f5675e, 01d9d79da491
                   8a57bd628cd625cba37cb3a278b419e04f5880c6cbc77c905c2f,
                    525ec7e60016e00e8e1d039d245bd7c44c4dbff8f566deb9e902
                   d10819edc0b5, 1a65097b4ef6145d0ca4c8257e193afe8245c85
                   a3cc934b1a28c876c7d65809f, 5f3a2f4d08763ca6a6685aebb3
                   eeb66a0887c750698b44ac17b7bed8ac3a1fd6, 4c583e5e4fc91
                   3aa71989afc50cfd8c2024d64df96ed12c7ef82d50ed4d8bb1b ]"

domain = "1207ed090723fa7e41c07e970ebb647d1d043079cc2a38c650c32234f18239
          36"
challenge = "5c2e5be0db5131fee3e284bb3bdc98ff34eccb03eb70cac6b8aedef3761
             10de7"


L = "10"

proof = "906a557b649ef5fa3ae1b17f814bbf1e78936daed6ac985416ce97bdaada5e8
         74d60f34074c5f2a8c02b1c33c3cb041294aa3da2e1bb55674a4b94d860f347
         7be7eb1adb763894796b285df22112a153ad13c35e4b9707046de269833e27c
         16d9621b73f05e4c7c543bf995e76ac1013839c6e8a9909b36e979192c5497b
         cc9fc534aa9296ec36ae43c398cdd328d3b606ebb0642786b508eb1d38893cf
         ffe8c9cff3c385644bd3641e0d1cbeda08bf16902d6dfeefa3ac8f8840a5f15
         5c54695b908e729b7f0d06fa9453d28746dfae608580fab158d2966ed54a3b5
         28346d72d49b0d69576b1094b3b14bfcba67af81c4467b424e9ac53fbf9cf8c
         a7c4cd20ac61243d61d91cd937eb82cb1524e38b24bd0ef235886c9f32e139f
         fe0b371bf1a310dd4a81bdda3994f1c2f85bd4b775dd2b716ad1a06e4b60444
```

```
         8a8bad5a75581b8c655652b284b1f727f52fe74ff501990b95918fdac4a00c3
         509bcb978370224b2c38aea21d811f30fcf623aa3f917ca0193ae9fd3ad3f82
         c7e1dd80c5712d280faa027b90d27ffb37fad3ea7bcc5c69885dfe74acfb072
         13d01cd974133e5f6c423d7e3fa118c590cbf5edac814486965aadec1620615
         6c97e37f7ebc837f9482f2b7c97e691bf80d0d4a02ccff38794349ef189ef7e
         7c909dc0c420236abac3be7613c66e41dee0a3246a759225c2e5be0db5131fe
         e3e284bb3bdc98ff34eccb03eb70cac6b8aedef376110de7"
```

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

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "862eb2fedd0a2b76fb978035cb33952004bdd6136e107bb343cb2c5ea56
             6eb0c3b0ba31b1d022ebf03d0abf050ab293c0afd9c96003331aa13f18a
             7a47e2e1ccaa8feb7f3a236e92b2da38462358c48a"

commitmentWithProof = "a2a3e178bcc77f98a3c07f8532134021ab5847326b5b3bfc3
                       089ca73f1bc51cfe2c99163f4919525dd6bedc8a14ee39e30
                       374643902017ca2e6fb8b5647c736e82d1d3c5b05de5c3021
                       fa6f40d9f36dd22fa06e522411aa20377088ca9a15885d7a5
                       044175f0168e927149ee71e2d257079e0100d6d96a7ddf539
                       2dbc64267af8df7b4711cb5eeccb5e8901d0580b9e837f383
                       37cb7260cffcf4f962154fafe5c98beaed7e4d2fc0f8e7eb1
                       ba4eb04086f170aa4924894e2ab63054049c9ef5dfff4f90b
                       48ef0dcf1f50699907301073270e4782d4d7628cfbe1444ce
                       a930928bb45004e41e0ad86a874ea03473845ce42f78ceb6f
                       855ba8326a4d47732c5aed3968b396a07f079b22b5bf2139e51a03s"
proverBlind = "4fba5396baa36b2fde81d46a9b9ee89c425dbc5e1ffd65c20249afb4a
               bd37589"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

revealedMessages =

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

revealedCommittedMessages  = {}

Trace:
```

```
random_scalars:

r_1 = "143f08e576583f264b72129ca9892b9c688e13087ed3d9509f85c43120eb79ad"
r_2 = "0217e712a7b1f6b5e65590f3f440f9d9ed25b76e065294fc728b866dbf4ef148"
e_tilde = "33b25342e7badf42d6b56c2d2db9a20fbd96b87ff39d8cd471142f3209884
           944"
r1_tilde = "097f8d774312e72fd4f29f2d5d9d317b3f12942cdb9b2e9be3d191afe5cb
            8b2b"
r3_tilde = "5a77c4f0644db0007295cf51a6a3145757380080264 0c2b1cdf28e8ec2cf
            6a9e"
m_tilde_scalars = "[ 0766852f1fa8f06c12dd87e3bb6f85162d2fcd7af8e9d14521b
                    521dde5ff8705, 65afb4d1a56075f316f72d2aa86fb9a8379a6e
                    a1d47be68e55eeeb6cd176f0d9, 04a0b83f6d79bb19a9230a7f3
                    cfbe70a81371490dee785cb0a206a462f9441ec, 4168e396ab4d
                    eb71c39e12e10ee26d8c0b8b56b136e78b64abdf0baabdb4aa4f,
                     241cceaf36d43c7f1d56264ac98e7c35fcdfb5d77022334224fa
                    05e43ab72e23, 59f396acf1d81dff23ea10d92dd718a0928fcd4
                    f90585352b9f628df4904808c, 057f3655600aaf1efe069fd15d
                    1a8ed4f6b122fd3a54b9b2d0db6b7edf7cbfac, 2ddb9f0733eef
                    a0c47edbe47f55601711d2a1b3d13c6f07747a4f6a7f9405fb3,
                    30d19e2d1625799e21b7dc2b8cc08376863b7b1370aafac151216
                    ecd56985814, 6f5c1c1071faced0bbdfb5e382ca6a0c62adf679
                    128361ba48f890aca65fb340, 496c5273ff17a2219473e75c203
                    a4ee1210d43a3f31bbf18dbd262862e073bea ]"

domain = "1207ed090723fa7e41c07e970ebb647d1d043079cc2a38c650c32234f18239
          36"
challenge = "2327ce643cc12df227ef05f13ab395a6d318c59e2195d410e768cdf9e7a
             1784c"

L = "10"

proof = "98805466f2fb4858dd9f60cfdc24d73b5192df64fce827b6ce942a6f2c8d5b3
         3f7eb7bf178353cf4bac91a4d6b84b536a89f504e4b46dea57ed2bc29d83993
         d71fb0b5a012d36aa8c3f0ba25220435be5f1b632166228bbb496eaebc1e382
         67eb46b5550d6e4d32d2f5559ada94828f729cac8f192a8fdb7aac7ffcf0102
         fef68314723ded1927965f30096e5f89103a036f32fb9980015f9d7781f86e6
         61e90d7b01f4c4c1bca0f7e0101098d9abcb603c3945c14b8cb298eecda9e7a
         8271dd407e68a45c4d2d4842b7095392873ccb4f2a0136ed04e9410b8c65ece
         d108f5b87b9c5b84c5ff95d3345f410d8a0efd51b5d24978c578859f2183cac
         affc17c031c24dc58ffc29d46922e16672140d1b078b8e7e9f87d31663ee497
         90274b2735bc807562c8e76f3223925ad2c15093e118ed7ec82eb590d8a9227
         408339f4091363da652e68cdf02c0003c94e35a2085d621447c2b0840b22af2
         a5d62fea5e898dba51d93bdd5f23c6b448f722d95d70459fd68f59b617adeb6
         2b0441745b0d69e865e0fc956359e137cf4706286a9764e6b7efd431cde5988
         76b992196c15662ba6c6768ad0ed4291963ac304dfa951c41d7233d6d85d2a9
         ff903468590ea787d413205b56d1892fa666230c93a87756d96fe3832930f01
         826651f8f449a945c0a3a9b50472c2060eceb566ec39961685560f49c36b500
```

```
         31dc8b4339da942e5c25498919a812209bbff527c332a5e50f27a539f805caa
         7c1a774034906d2aae0b6c2db4696d3ed91453ea0f1e42d4129a9812dbddec7
         1d55d3ec1598202db88e15f3ad7f8eef3098102be8f978785e2327ce643cc12
         df227ef05f13ab395a6d318c59e2195d410e768cdf9e7a1784c"
```

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

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "862eb2fedd0a2b76fb978035cb33952004bdd6136e107bb343cb2c5ea56
             6eb0c3b0ba31b1d022ebf03d0abf050ab293c0afd9c96003331aa13f18a
             7a47e2e1ccaa8feb7f3a236e92b2da38462358c48a"

commitmentWithProof = "a2a3e178bcc77f98a3c07f8532134021ab5847326b5b3bfc3
                       089ca73f1bc51cfe2c99163f4919525dd6bedc8a14ee39e30
                       374643902017ca2e6fb8b5647c736e82d1d3c5b05de5c3021
                       fa6f40d9f36dd22fa06e522411aa20377088ca9a15885d7a5
                       044175f0168e927149ee71e2d257079e0100d6d96a7ddf539
                       2dbc64267af8df7b4711cb5eeccb5e8901d0580b9e837f383
                       37cb7260cffcf4f962154fafe5c98beaed7e4d2fc0f8e7eb1
                       ba4eb04086f170aa4924894e2ab63054049c9ef5dfff4f90b
                       48ef0dcf1f50699907301073270e4782d4d7628cfbe1444ce
                       a930928bb45004e41e0ad86a874ea03473845ce42f78ceb6f
                       855ba8326a4d47732c5aed3968b396a07f079b22b5bf2139e51a03"
proverBlind = "4fba5396baa36b2fde81d46a9b9ee89c425dbc5e1ffd65c20249afb4a
               bd37589"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

revealedMessages = {}


revealedCommittedMessages  =

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

Trace:

random_scalars:

r_1 = "23d8b41f82e80a32c4606bf7198b6a85bfdcbb9a87773a54e668aa6cc50f4b60"
r_2 = "259cb8451e183911fd32701689c8da084a351cbc878edabb5c65892f5566cbee"
```

```
e_tilde = "0750d611202174343211411eb9aeb18d6b09057c51e9f9524cf1ec29a845a
           4c9"
r1_tilde = "519d28834203f545ce2e917b1428e59f4ca3e716351c2f03b9884bf3b84e
            e5d9"
r3_tilde = "664fd86f51bd56079f1f58e8f29881ca6881f9022b267a0842eb9bd66d8f
            f116"
m_tilde_scalars = "[ 35c21b4641053b0e351cecc6b4f7aa9687771ea67785ba51ddb
                   13ee3d6616344, 2dec7bd3fcd718500184d41d750642b55d21ea
                   63b494bdf41011dca9d7075b57, 277ca0dcb0183675a981bfa22
                   e2ad09c8a61b23761575078374a9df40cb63237, 3376f31a419e
                   b425ae5375029f0f1caba349467ff477c30aa6a577ffbabc162b,
                    22808132ab0fea4b85a2b6621abc8f2e78b65f3417db2e8350be
                   c0a5d02f12f7, 68b417316ece357d32bd0e94f5211a900abf588
                   8ec25ad7762d40413d45a6ff5, 668d12f5ef2c391c0dc06f1f2c
                   1451d710c743311cd213c268bd7b41085300d5, 1f45ce8d90d44
                   399aafe97bd024636747766b670004c366af6b19dfd211fdae9,
                   304b07fecf8dcc052c29b4d52934a031d4abdad430c4bd3ccc650
                   28d4e26da8f, 02d05a55bcfe243c268154cc03f548ffa461f84c
                   4087c7bbb6284e4e07ffee53, 3e20f9d1709e50cf709530e4e26
                   7f544eda9c4b9e214e4b133c20cda8477ffe9, 6e41035b050e5e
                   a1f97bc975eb5a63447470bc24639a7f63269e8b3f5d8f94a3, 3
                   1dad9cf8ab3482296a766c4c6e2a97b2ad9e83cf8c83755940736
                   235bea6e0e ]"

domain = "1207ed090723fa7e41c07e970ebb647d1d043079cc2a38c650c32234f18239
          36"
challenge = "6f1ee88214bdcd79462a1f7411e0c8ab10a8bba0140c9cddfbcdc88d7ca
             19dfd"

L = "10"

proof = "aff98a4a0bc336e459d47c19816f372de628581bc626fdd20e907db10d2218d
         d47530fbebc78afed77f2557d344d620d9097016e84b0dc7588686bbeacb44f
         c55bb3004bf79e89d82ed37df3e1835975cc63a00b76685eecc4aff51426fb4
         3cb87d8ba852fb786f1cf649271517bcc4bb72af3e3b2fa4ae57bea485b6f98
         86fe33d0e5bd95d21f4ccaa4d80b64692caa23d32c7368ef99f1b9ab1672ecb
         3ae7393a3a4d3efa6f4dc18d8563788f97d8b3fb7427593bdc21aed4332d17b
         94d82b8c20ea1236a756a4ec2cfa5e1050588e04582299196c1f28e04c2349c
         5d9e717ba6a581ed255f20bf4210f852d2cd95844fdaacf4d8339a14fe7982b
         e4f447812616433a3e23990c180ec2540c13f9d467e996cd9a2df2bdd1b0bfe
         3e51c116e13888d21e26ee61d7ca070968bc13e9d3d33dce20dfc52618bfa4d
         340f558660f41d67d11f5af9a1e185f261a2d14eb667987d700ce77ed24e3b7
         0c29e49c188b5963dfb16ab7c2439ec6824f738e3df128865e180a41b06b1db
         ad2eed8a82728fc4dd34046410345c38415d9daaa3076efbbf84b8f3c52c2bf
         527d10ae882b0790a7f3b6b3e2c877fbb5a7d18bda860278598f1a83c855e67
         e3b8f8d807b29514d2420753ace9356a39e70fe49c5f2e29cea65820b57f3b2
         5363685a5559c577ca48046d5eaa35568a935f58dbd9dae2744eb4dfe33cbb6
         6bc2b351f2b634f508fe2e37ae19c89f14b4d6d6f636890d62e0f4ccb9565d4
```

```
         f8786b429188c7351f08538aff7b760da7867683315700ab549b639a59b9025
         fbf67ffb34a834d8b9e893d9d5969e9022813c4529115e682758166b4d2b8af
         72f44b00dff7b769bb985c40bef59e18034febfd7bb5ee847b13160b0da82b2
         8cd400c53ff004038e67b9fd49511f9e8b69df923f3aa73fb1636f1ee88214b
         dcd79462a1f7411e0c8ab10a8bba0140c9cddfbcdc88d7ca19dfd"
```

8.1.5.7. valid no prover committed messages and no signer messages revealed proof

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "862eb2fedd0a2b76fb978035cb33952004bdd6136e107bb343cb2c5ea56
             6eb0c3b0ba31b1d022ebf03d0abf050ab293c0afd9c96003331aa13f18a
             7a47e2e1ccaa8feb7f3a236e92b2da38462358c48a"

commitmentWithProof = "a2a3e178bcc77f98a3c07f8532134021ab5847326b5b3bfc3
                       089ca73f1bc51cfe2c99163f4919525dd6bedc8a14ee39e30
                       374643902017ca2e6fb8b5647c736e82d1d3c5b05de5c3021
                       fa6f40d9f36dd22fa06e522411aa20377088ca9a15885d7a5
                       044175f0168e927149ee71e2d257079e0100d6d96a7ddf539
                       2dbc64267af8df7b4711cb5eeccb5e8901d0580b9e837f383
                       37cb7260cffcf4f962154fafe5c98beaed7e4d2fc0f8e7eb1
                       ba4eb04086f170aa4924894e2ab63054049c9ef5dfff4f90b
                       48ef0dcf1f50699907301073270e4782d4d7628cfbe1444ce
                       a930928bb45004e41e0ad86a874ea03473845ce42f78ceb6f
                       855ba8326a4d47732c5aed3968b396a07f079b22b5bf2139e51a03"
proverBlind = "4fba5396baa36b2fde81d46a9b9ee89c425dbc5e1ffd65c20249afb4a
               bd37589"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

revealedMessages = {}

revealedCommittedMessages  = {}

Trace:

random_scalars:

r_1 = "60d345d6f2bf3d7b6734145a0a1c84731771d9fb8f2caa849dc33a3e1ed42906"
r_2 = "5fd44fc64975d153f17a73ce413b86211acf63e62494ae73a0865f068588fb02"
e_tilde = "6e3fdd342aa6c154fd11ba738e191c54f9877522f4648b466eb4ee1d30178
           0bb"
r1_tilde = "3da42b3641758dc3d8bce1ced15d1fd1d291bfd533d11373248082eca6d4
            5d9c"
```

```
r3_tilde = "01be275b265a083b2b8a1ba7110576e28cfcad346717c512c3311ca40316
            8120"
m_tilde_scalars = "[ 67ff540238565851a1f98c6357507be2da16884e44ae26fe4d0
                    a0a8607532fbe, 5de3cb769cc629a9ab21fe29bb7acc06cd5df9
                    79826fabe26b78cc9ab67a32f9, 1a14acb3666d2d123db8d19ec
                    473dd980cb1100532be1abda1b941668b43ff28, 4f03cb50f6a2
                    5f1f7f277682ab5965a772ac0b24e9ad2f1a7b42a047d8d7adc6,
                     11ef78647f2fbdc57f8d29cab816584920596bbd3813d2ee7df7
                    f44b24617f33, 4d7fb091d8f42be6fc0fc0401cc5ffbf0da7aad
                    8951a451f26abf5820eece429, 03b576c0e1b8063af7f9acc917
                    84cb062920820e9b2d4baf11d55777d11e2946, 5c8053e4347ad
                    1c5f600a7d1d5aef448dc0fbbad6204430486c65e7216c18a73,
                    4b81ebb73b19c698f62d0fda7505452e97382b09bbe7821ef40fb
                    1f3b3f26172, 1ab69f6373dcf9d87b75f2e140a34345a92f7952
                    a44436832036bf6bc4fb3b75, 0f0059e68095e5edccc546ac531
                    2234ed1d6b1ca65c4b13f77dc1b7bae4623a2, 1372682d7f0522
                    cf87aa4805f43d493c2beb7784fe9875712480a5bec63a8b69, 3
                    66a39b41f91f2f6faee881f06c1077e9c65257fc75587353880f6
                    406ff828f0, 4eac85d64994ff0b48690a25055eb62f0f0b4a890
                    95c54fc1b08fb7ba0e90eae, 475da477f48d661e2271eefd16d7
                    437a64f6ec7a4cda8deaacdc9c6275489fe2, 3a9be520243abe9
                    76b50d5ad343692ac99e28d3d11e4e9a5cd458316d097ce36 ]"

domain = "1207ed090723fa7e41c07e970ebb647d1d043079cc2a38c650c32234f18239
          36"
challenge = "134eed0aa579badf2131c90aea352b28586cd1dc6663008e9e38866a9f3
             83aeb"

L = "10"

proof = "b27d9bc8c52a582d00db93da283346751c8da54a902703110e511fa39f184ed
         6c464d78c81d4bbcc57b7de1b31c7644184ba8f06266dfa8b2662b756f8c89b
         f3b01f7f66753028dc0ca85a0417a4f6d9dae4b393aaf5c152734f210a790a5
         f96a2ad1aaab7c1f5167484d18bf19570e2fa4d58b481225a1a576286bac7e4
         353aa7cba80939eabc492347fc05f8bd701f5410ecb5faf54d4a617bddf39bc
         b314d750257e99db7f0b03d043f8674668479322dc83c5c1e9e05dd760a4e1b
         5c45a044072bfe4e0f21bea9cc6362a38664532b4e10d0e7c4751452ff30724
         70b6919bded88d3e591e96a4b71603944015ca36594432351d9de6309820d5a
         837e28e690b662a959833fd51faf6b77e7636f206385eee2d3aa1d99758e1ef
         310a914f1a9fa3cd8eb2feb170c13de8e36de2dd2726430e0782cd0d5eaef64
         d11bd871eb27b6b2a9536a4189731b32cd16ee25ba305ee01d99689e66534d5
         8399a514b92813873ed28f377679f3aab6e977d62226dd4fa0eef43f7b69f92
         ca0d69588fb8339ba0b35d1fbc3623fdf2d761fa537d54b0b2cd094a8bf98f1
         117a8f665c5f68f101926f729185a6d830894f4864f606d47b5b5fab349b23b
         9be04443d1d6bef67a1755bcb5ac2d46e8af259bc449ce19edc5a4a20f5d236
         bf6089012df8021ebb68c756aa85528a98aa758a5524cf71ccc9867ec837576
         d092c68844d8ace281fd063343b212399dcd1cc80fd7cbd822e559df5616c81
         eb8e6e7768d8f9819b757d3a1f9211d047bdbb172c26e2e3f0a4541d7e30b05
```

```
d25b6905abba445488543a16729090eb6d0a45cef159f17cea4ebdc307f9191
d76dc52277cda93c0ae75d8021ced39b064229271d673cf28ec645ba56637ec
f0f54982f78773cf3ae8514dfcd4932c41337c766e9d9e6041bd0a01062da4a
d80106520b29888ca5c4893a8b447cf502e6672b038698bf1b7ae0d87c4e546
ae98c7b6c21ad1fb56d54ee930ba9524c55705c00b05c3b6dd0c3f42ca9f9c0
6748cdda8c1ca428122e780a80ae78c66c1d02728ea751dce0ac100134eed0a
a579badf2131c90aea352b28586cd1dc6663008e9e38866a9f383aeb"
```

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

```
signerPublicKey = "a820f230f6ae38503b86c70dc50b61c58a77e45c39ab25c0652bb
                   aa8fa136f2851bd4781c9dcde39fc9d1d52c9e60268061e7d7632
                   171d91aa8d460acee0e96f1e7c4cfb12d3ff9ab5d5dc91c277db7
                   5c845d649ef3c4f63aebc364cd55ded0c"
signature = "8aa8fdfb190987d1fe1c8e34e69eae2559470195806 4e4483d74580a4a0
             f51f058a87735d727383b864904aa7b5e4a9b3821a18319df0ccb2e351a
             9bf75bf1f34d8858dde57119bfafd8ff56e0c54fa4"

commitmentWithProof = "null"
proverBlind = "null"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

revealedMessages =

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


revealedCommittedMessages  = null

L = "10"

proof = "a8c57d443b888815e25ca197a543c3a007c573cea5d2cc3c7aa312dbe4aa33a
         62490ced4d8f5c0a99aeada24f79b2d34b32cb742dab22663402104828af5e0
         85a6019fb073e08374e9be9b1af64140a4d1ce2b8016f85ebca3ebb5aa02847
         b91936d649f19d0e85a19118e5e13e2beabf2d705e1db59f8945adddafc7731
         0b0a02042093a5477d9efd4a98cb2fad4dc535fa9f5e6a96f744ece30bbf1fc
         ca709d5b4fcc8c390b4e2ad755292cc20817141d9348e4a7d7c864493625c8a
         aa455c486afab64ae63f56c10b90047bbfa20825b2cb00f19ee3b54f7c7bdce
         a55f5811803b9cff2c2f2e96495dd12236e17c9581997b7880062715aa7deec
         4ca4b3b4eebba824cbe0adcba83f8e70bc0004ee350b536513829798 3171d9c
         ca33ca2376157f390a724f857b4212fe834898d332a582083b8791969d2a070
         57722a22b44132c5fc2ed0035b3b2e71f9ec08ebc33e019a1fa76bd8d642da2
         1cd0a8b36080203c2c4d5b10411e90b8bebd4540405564805191 75f28f31210
         870454bfad2905d49e9b655b5bea6318955ba210938b279717a2b1e1d34cccf
         ddfe9c8e3729f6e92e28197a09459c6dcd56e3920a0d73954d79b681f1e93f7
         0566a73f42610c389ec3f0d65a4727229df891a61511d2"
```

8.2. BLS12-381-SHAKE-256

8.2.1. Generators

```
api_id = "BBS_BLS12381G1_XOF:SHAKE-256_SSWU_RO_BLIND_H2G_HM2S_"

P1 = "8929dfbc7e6642c4ed9cba0856e493f8b9d7d5fcb0c31ef8fdcd34d50648a56c79
      5e106e9eada6e0bda386b414150755"
Q1 = "98947e7a6283c629cb9721fe0aeb3c32252d307307ff0608a3c97331ca4b5669ab
      d19d90db94c58b446db705c09e7eac"

Generators = {

H_0 = "82999b68b153ad49c9ce47d178be8d82f122cd86c836d75120c3c775a44ba9532
       8a90beac7367c504f54a246f8e3205c"
H_1 = "8c7a5dbe9e899b76154f1c6cccea621b5532b93ce927a73d9ac44ef2d0eb006d9
       1587884ea111bbc0f66770a57a37d8a"
H_2 = "895ce03ec7b8ed0b6f6004d50d52132689793672b35a01d14ea4884796afa7b33
       e4b78d6489ede095cf8c202946da4f6"
H_3 = "b05ce29d4da638e0ea3f26fc673bbea1b343d240328ec278aaca12dcf9654983e
       14614a55407d2afb995f4ce145d9c3a"
H_4 = "a449a514d0e1bed84d2e8951fc7fc1596cf8f79397de06cedd00201412d0a81b6
       32b7f96b42b8323ad97d8fb80395bef"
H_5 = "aac7ea0084b8acef55530990952d3842d990d32512b8ab9e543afa7d46c66fda0
       94cb1bf84e7fc11153211c57e8e15e0"
H_6 = "a26ec4c96335f503aa698c32211c777c0f0df8692e2a107eb3a62901ca96f8e31
       2f5375afd52171ccddf738a09f1eda2"
H_7 = "84206f2773436ea438d308ef90aa2d2a08e3a2555225d9c4013be119d80fc7869
       d0ce6fa4ab7ac7b5371f8b499dd6109"
H_8 = "8ab206f6aa7bd7b96d946f3e87723ab4bd0a4bc42fd4d63e7a139f46e4f793540
       04e33f47e916988082c80e084b0375f"
H_9 = "b88931b5c26e1e6e5566addb734be441b6f4520868a8d8c2bc16b53c8ddda2c0c
       3ca217c5d8245f2b0646b874365d3fc"

}
```

8.2.2. Blind Generators

```
api_id = "BLIND_BBS_BLS12381G1_XOF:SHAKE-256_SSWU_RO_BLIND_H2G_HM2S_"

P1 = "8929dfbc7e6642c4ed9cba0856e493f8b9d7d5fcb0c31ef8fdcd34d50648a56c79
      5e106e9eada6e0bda386b414150755"
Q1 = "a881a2d06ea464af4cf6c1177812f6d9d25f19fd68a3d6af2aadf065deca715d29
      06d1d1a5db76ba4ec843c6ad510f46"

Blind Generators = {

J_0 = "a9b4d7aadbfcab6e63f6d112366226c1e6b9ebac4a99fc015b444cb4768e1db1f
       3710b3088c0d00c74d264a2d07c4e06"
J_1 = "b78ce56f07607521ef84ab56dbc2c2e2fae0948ce91cb4e33af951ae4e9a4c8aa
       1b816b3b99987b2157cd442808222b5"
J_2 = "8f2a392c6fa4066ed4834f95400b2a69e6fc951d899805d5cf8c252379d5d0a9d
       aa9033b2c4e6a7c63ecaa4f236933ce"
J_3 = "83d6efbab354280eab4cf0feb9d064f5525c57a7ba709644df81d45596571147c
       383448bf44466129758dbccb43c4d29"
J_4 = "916d77f038fa7b5d8abc6533ef06c3cce2018677dfe36cc8fbcdcc0bfb471c18b
       b82eddc71e1156bd7740c1402e6be9c"

}
```

8.2.3. Commitment

Mocked random scalar parameters

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

8.2.3.1. valid no committed messages commitment with proof

```
committedMessages = "[  ]"
proverBlind = "30bd5c9bd2b61c44dd169c92cf28bb607830c56073f10e7a800c857cb
               05ec249"

Trace:

s_tilde = "4ead1c3cc9624bf2b82d6ce2dc1e8e7b664521f22faa543a78fc47d86fb04
           df3"
m_tildes = "[  ]"

commitmentWithProof = "b6389b0fdf04b9c35165acb11685e02193c53c3c1bb8ef3a9
                       404dcee1727a365a3ac6ba7fc32654101cc72cc0ee7d32b23
                       d2018bd6dc2f932c71d4401e763d4ed9999ee6c98837aa7db
                       e823050697dd744b05920ad0b6393e94f9b86e92d41940694
                       5f1e79d4be58dbaf9dc95237c951"
```

8.2.3.2. valid multiple committed messages commitment with proof

```
committedMessages = "[ 5982967821da3c5983496214df36aa5e58de6fa25314af4cf
                     4c00400779f08c3, a75d8b634891af92282cc81a675972d192
                     9d3149863c1fc0, 835889a40744813a892eff9deb1edaeb, e
                     1ca9729410dc6ba,  ]"
proverBlind = "41fb2f74c30256398c927a262602b5ac3ebc6f84d9169476f8fcb1525
               c93b649"

Trace:

s_tilde = "4ead1c3cc9624bf2b82d6ce2dc1e8e7b664521f22faa543a78fc47d86fb04
           df3"
m_tildes = "[  ]"

commitmentWithProof = "85d8034b358566ebfd26f921211b257d30def9962ddf80dc7
                       cbdbf96da2bf598a8bbdc03bdc311ff290673ab29edf4a642
                       be726c577a1aaeb11d00d10c5a07c824bbf8e47af13042f57
                       0b6bfc05e42783d70fb3ee76ab7c2565fda74ed6536e14105
                       adf9ae943736a6c96c1102d1dc4424eda4ee1961f0d450736
                       d1cc9f6b3ad2f9f1bcd3b63ef5445798b65ad04806240edee
                       143b5c7c57f61ab7fc9fd8f0b05d984e12cee674541b6a792
                       02931e0ef11bcfc908660861b48cfd4ce0970c9726d9359b4
                       bd0c853da78891e9c9db41f2029195279d92f6831b37b5c6d
                       5ac28840e97c12f7962e65adac6705ae712daa61c0c0bda85
                       a3da6850a8dce296797beff88b1c8e8459dba0730ecace09177f79"
```

8.2.4. Blind Generators

```
api_id = "BLIND_BBS_BLS12381G1_XOF:SHAKE-256_SSWU_RO_BLIND_H2G_HM2S_"

P1 = "8929dfbc7e6642c4ed9cba0856e493f8b9d7d5fcb0c31ef8fdcd34d50648a56c79
      5e106e9eada6e0bda386b414150755"
Q1 = "a881a2d06ea464af4cf6c1177812f6d9d25f19fd68a3d6af2aadf065deca715d29
      06d1d1a5db76ba4ec843c6ad510f46"

Blind Generators = {

J_0 = "a9b4d7aadbfcab6e63f6d112366226c1e6b9ebac4a99fc015b444cb4768e1db1f
       3710b3088c0d00c74d264a2d07c4e06"
J_1 = "b78ce56f07607521ef84ab56dbc2c2e2fae0948ce91cb4e33af951ae4e9a4c8aa
       1b816b3b99987b2157cd442808222b5"
J_2 = "8f2a392c6fa4066ed4834f95400b2a69e6fc951d899805d5cf8c252379d5d0a9d
       aa9033b2c4e6a7c63ecaa4f236933ce"
J_3 = "83d6efbab354280eab4cf0feb9d064f5525c57a7ba709644df81d45596571147c
       383448bf44466129758dbccb43c4d29"
J_4 = "916d77f038fa7b5d8abc6533ef06c3cce2018677dfe36cc8fbcdcc0bfb471c18b
       b82eddc71e1156bd7740c1402e6be9c"

}
```

8.2.5. Signature Test Vectors

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

```
secretKey = "2eee0f60a8a3a8bec0ee942bfd46cbdae9a0738ee68f5a64e7238311cf0
             9a079"
publicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62bd45949
             cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddbd619e419b99c
             2c41b38179eb001963bc3decaae0d9f702c7a8c004f207f46c734a5eae2
             e8e82833f3e7ea5"

header = "11223344556677889900aabbccddeeff"
messages = "[  ]"

commitmentWithProof = "b6389b0fdf04b9c35165acb11685e02193c53c3c1bb8ef3a9
                       404dcee1727a365a3ac6ba7fc32654101cc72cc0ee7d32b23
                       d2018bd6dc2f932c71d4401e763d4ed9999ee6c98837aa7db
                       e823050697dd744b05920ad0b6393e94f9b86e92d41940694
                       5f1e79d4be58dbaf9dc95237c951"

committedMessages = "[  ]"

proverBlind = "30bd5c9bd2b61c44dd169c92cf28bb607830c56073f10e7a800c857cb
               05ec249"

B = "a44e7c8b4969cb821e48fc8ce3e295ed6a47923155edc19ff783993944863cd2e87
     12b72005f20bf51d7395c15832fc8"
domain = "48d64a62d7dbc8d88d643f15b3c8a1eed78afe3a80bc3e41bc2f92257b25f6
          d8"

signature = "94403c30badaccf53c4d5f6a15e66c98fe021c149254a5b54b75f15fe67
             4978897284db9fb6a8716fa17e69c80acfef45e56e7199abc42be2ba46c
             dfef5b30b3cc1ed12802225733183f02fc535a2127"
```

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

```
secretKey = "2eee0f60a8a3a8bec0ee942bfd46cbdae9a0738ee68f5a64e7238311cf0
             9a079"
publicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62bd45949
             cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddbd619e419b99c
             2c41b38179eb001963bc3decaae0d9f702c7a8c004f207f46c734a5eae2
             e8e82833f3e7ea5"

header = "11223344556677889900aabbccddeeff"
messages = "[  ]"

commitmentWithProof = "85d8034b358566ebfd26f921211b257d30def9962ddf80dc7
                       cbdbf96da2bf598a8bbdc03bdc311ff290673ab29edf4a642
                       be726c577a1aaeb11d00d10c5a07c824bbf8e47af13042f57
                       0b6bfc05e42783d70fb3ee76ab7c2565fda74ed6536e14105
                       adf9ae943736a6c96c1102d1dc4424eda4ee1961f0d450736
                       d1cc9f6b3ad2f9f1bcd3b63ef5445798b65ad04806240edee
                       143b5c7c57f61ab7fc9fd8f0b05d984e12cee674541b6a792
                       02931e0ef11bcfc908660861b48cfd4ce0970c9726d9359b4
                       bd0c853da78891e9c9db41f2029195279d92f6831b37b5c6d
                       5ac28840e97c12f7962e65adac6705ae712daa61c0c0bda85
                       a3da6850a8dce296797beff88b1c8e8459dba0730ecace09177f79"

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

proverBlind = "41fb2f74c30256398c927a262602b5ac3ebc6f84d9169476f8fcb1525
               c93b649"

B = "b2f39ad3749d91fae9e6b5e7326902b970c0bc0ee85fe5c4de82702faff072c923e
     75e2e3af19395b8a978a80b1a887a"
domain = "3600988bb64779f01c57bfb0524521bc241aa0fdfc92e1b892ac2066edccee
          f1"

signature = "82f5137b728baea7d23bc610888e7dbabdae8b6ce404d5e591608bc0d55
             0f246194cbab590eda33dd2a8aafc0f107f0f3158d330459681d5156d65
             f6dbdc7b3bfd003212a89052d668935b53895e70d2"
```

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

```
secretKey = "2eee0f60a8a3a8bec0ee942bfd46cbdae9a0738ee68f5a64e7238311cf0
             9a079"
publicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62bd45949
             cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddbd619e419b99c
             2c41b38179eb001963bc3decaae0d9f702c7a8c004f207f46c734a5eae2
             e8e82833f3e7ea5"

header = "11223344556677889900aabbccddeeff"
messages = "[ 9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4
            a45f02, c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811
            f5fb075f9b80, 7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932a
            a348e07b73, 77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c
            , 496694774c5604ab1b2544eababcf0f53278ff50, 515ae153e22aae04
            ad16f759e07237b4, d183ddc6e2665aa4e2f088af, ac55fb33a75909ed
            , 96012096,  ]"

commitmentWithProof = "b6389b0fdf04b9c35165acb11685e02193c53c3c1bb8ef3a9
                       404dcee1727a365a3ac6ba7fc32654101cc72cc0ee7d32b23
                       d2018bd6dc2f932c71d4401e763d4ed9999ee6c98837aa7db
                       e823050697dd744b05920ad0b6393e94f9b86e92d41940694
                       5f1e79d4be58dbaf9dc95237c951"

committedMessages = "[  ]"

proverBlind = "30bd5c9bd2b61c44dd169c92cf28bb607830c56073f10e7a800c857cb
               05ec249"

B = "8c1c6937d6c059c330f3d4c89ddea956b18c6e7a4d5b16fa85ac9a6f6f6a815008c
     fd3af0fc1a012728ba3ae62c4ac51"
domain = "62638964b2b8eb67c2635a8b87731e2f876e7e84fc4f051903022a731c5fe3
          b8"

signature = "a4999abd5d20fd706cabeb2a44e6dd42b76d6ccfc29ac83d947351a1980
             7e57b0d951d4b79d03250e0e84cc1204a143336c4decbbc7417060f1fc4
             4159192e23e437fe0aaee3971ce89e901f99405b90"
```

8.2.5.4. valid multiple signer and prover committed messages signature

```
secretKey = "2eee0f60a8a3a8bec0ee942bfd46cbdae9a0738ee68f5a64e7238311cf0
             9a079"
publicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62bd45949
             cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddbd619e419b99c
             2c41b38179eb001963bc3decaae0d9f702c7a8c004f207f46c734a5eae2
             e8e82833f3e7ea5"

header = "11223344556677889900aabbccddeeff"
messages = "[ 9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4
            a45f02, c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811
            f5fb075f9b80, 7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932a
            a348e07b73, 77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c
            , 496694774c5604ab1b2544eababcf0f53278ff50, 515ae153e22aae04
            ad16f759e07237b4, d183ddc6e2665aa4e2f088af, ac55fb33a75909ed
            , 96012096,  ]"

commitmentWithProof = "85d8034b358566ebfd26f921211b257d30def9962ddf80dc7
                       cbdbf96da2bf598a8bbdc03bdc311ff290673ab29edf4a642
                       be726c577a1aaeb11d00d10c5a07c824bbf8e47af13042f57
                       0b6bfc05e42783d70fb3ee76ab7c2565fda74ed6536e14105
                       adf9ae943736a6c96c1102d1dc4424eda4ee1961f0d450736
                       d1cc9f6b3ad2f9f1bcd3b63ef5445798b65ad04806240edee
                       143b5c7c57f61ab7fc9fd8f0b05d984e12cee674541b6a792
                       02931e0ef11bcfc908660861b48cfd4ce0970c9726d9359b4
                       bd0c853da78891e9c9db41f2029195279d92f6831b37b5c6d
                       5ac28840e97c12f7962e65adac6705ae712daa61c0c0bda85
                       a3da6850a8dce296797beff88b1c8e8459dba0730ecace09177f79"

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

proverBlind = "41fb2f74c30256398c927a262602b5ac3ebc6f84d9169476f8fcb1525
               c93b649"

B = "95e018b5b7fe84bff803e829231870d1dec64608083a6a7b4b8f5be66ee9a6e25a6
     d067f528e48712528205ae9cdf340"
domain = "04ad1197bffbb54ae41c1d43c61dc29325c2dc771d5cc7dba67907b17f564a
          04"

signature = "80b1195ea9e11a639e11e2dc653ccca0461055edb4f48a6e80b676636e4
             2dd61fae3e52c04e192d5053d60e73f3dec5048d423579dcb96cde6969f
             8048ce53f15ab02449b8d375f869a8df15db78eb02"
```

8.2.5.5. valid no commitment signature

```
secretKey = "2eee0f60a8a3a8bec0ee942bfd46cbdae9a0738ee68f5a64e7238311cf0
             9a079"
publicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62bd45949
             cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddbd619e419b99c
             2c41b38179eb001963bc3decaae0d9f702c7a8c004f207f46c734a5eae2
             e8e82833f3e7ea5"

header = "11223344556677889900aabbccddeeff"
messages = "[ 9872ad089e452c7b6e283dfac2a80d58e8d0ff71cc4d5e310a1debdda4
            a45f02, c344136d9ab02da4dd5908bbba913ae6f58c2cc844b802a6f811
            f5fb075f9b80, 7372e9daa5ed31e6cd5c825eac1b855e84476a1d94932a
            a348e07b73, 77fe97eb97a1ebe2e81e4e3597a3ee740a66e9ef2412472c
            , 496694774c5604ab1b2544eababcf0f53278ff50, 515ae153e22aae04
            ad16f759e07237b4, d183ddc6e2665aa4e2f088af, ac55fb33a75909ed
            , 96012096,  ]"

commitmentWithProof = "null"

committedMessages = "null"

proverBlind = "null"

B = "8ce18ec220f427e23eced9bc5d6a90bf242941676569b406a179e7fe8a3d1c3ba7f
     d0271ce37817876e55fe1fdf598e5"
domain = "62638964b2b8eb67c2635a8b87731e2f876e7e84fc4f051903022a731c5fe3
          b8"

signature = "b80f73e22cf6c050159018539af4fd2c8ed75a7dfa247feadbdecd983e1
             6ddb33ac5c61bfd7f17b4063a7957456ddc0b71d46e6a05b1a464df601a
             abf480edf17ff1d6052089c294577fcfb7b851baad"
```

8.2.6. Proof Test Vectors

Mocked random scalar parameters

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

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

```
signerPublicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62b
                   d45949cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddb
                   d619e419b99c2c41b38179eb001963bc3decaae0d9f702c7a8c00
                   4f207f46c734a5eae2e8e82833f3e7ea5"
signature = "80b1195ea9e11a639e11e2dc653ccca0461055edb4f48a6e80b676636e4
             2dd61fae3e52c04e192d5053d60e73f3dec5048d423579dcb96cde6969f
```

```
             8048ce53f15ab02449b8d375f869a8df15db78eb02"

commitmentWithProof = "85d8034b358566ebfd26f921211b257d30def9962ddf80dc7
                       cbdbf96da2bf598a8bbdc03bdc311ff290673ab29edf4a642
                       be726c577a1aaeb11d00d10c5a07c824bbf8e47af13042f57
                       0b6bfc05e42783d70fb3ee76ab7c2565fda74ed6536e14105
                       adf9ae943736a6c96c1102d1dc4424eda4ee1961f0d450736
                       d1cc9f6b3ad2f9f1bcd3b63ef5445798b65ad04806240edee
                       143b5c7c57f61ab7fc9fd8f0b05d984e12cee674541b6a792
                       02931e0ef11bcfc908660861b48cfd4ce0970c9726d9359b4
                       bd0c853da78891e9c9db41f2029195279d92f6831b37b5c6d
                       5ac28840e97c12f7962e65adac6705ae712daa61c0c0bda85
                       a3da6850a8dce296797beff88b1c8e8459dba0730ecace09177f79"
proverBlind = "41fb2f74c30256398c927a262602b5ac3ebc6f84d9169476f8fcb1525
               c93b649"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

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 = "49269fc9884182a1591f959e813384df71ffb220660cb2a4aa3956e27936d4d8"
r_2 = "66b80c544ba7563a7de236678d228a36195f2b483daec4c49470b63c7231cb11"
e_tilde = "6714fe17c1529464fd269b37dda00e6cdd2b82b592a497cc52e78f24930ef
```

```
           fda"
r1_tilde = "1da4b2f8fe1790bbff2efabd71c8ed624f9fedd10d62dc7a3ca1088657eb
            f220"
r3_tilde = "2354f9de39e2689b893f357e14cead4e405ab3486f188a0b5a503e733d00
            7588"
m_tilde_scalars = "[ 42510c348487be3c19994565911729eafcd4804dacf25a7cb7b
                     7a634ddefc3b5 ]"

domain = "04ad1197bffbb54ae41c1d43c61dc29325c2dc771d5cc7dba67907b17f564a
          04"
challenge = "45526dc44104c6e23c16279daf102b68742a1430eeae18b7e256143d173
             69128"

L = "10"

proof = "8f5edaeeba071bee79350cc4727893732842e80d936448974ea9e1628aa9470
         3adb1c0795d1b2ec66d4b750bdb1a4409ac7e95178c30d0ca84275783688186
         19102571c1862b51abc7560fe1271d86a49439b172709ef7012f527f8cbaac7
         58ab803cab84c7c19d5d4e28241da72c141f2518df44d42846ca7b5802a903b
         ec757c83352a5789ba2d57e3686b49f41b7a1803b642118ed8acc19bdb90bcb
         4fbac1fc16213d557e3ffb13184c908a1b5375072cd58c4773bc9e84f65f5fb
         845cd4318636f91ed2c6fa619ea193be77b18e46a7760242df2ff117ba27a38
         574fb8ca2904423d92cfc3420f58a063703ff71170ffd1e323f667b46197f43
         2aa9d11608ff06b0d4aae0669e0dab0599372f9645526dc44104c6e23c16279
         daf102b68742a1430eeae18b7e256143d17369128"
```

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

```
signerPublicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62b
                   d45949cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddb
                   d619e419b99c2c41b38179eb001963bc3decaae0d9f702c7a8c00
                   4f207f46c734a5eae2e8e82833f3e7ea5"
signature = "80b1195ea9e11a639e11e2dc653ccca0461055edb4f48a6e80b676636e4
             2dd61fae3e52c04e192d5053d60e73f3dec5048d423579dcb96cde6969f
             8048ce53f15ab02449b8d375f869a8df15db78eb02"

commitmentWithProof = "85d8034b358566ebfd26f921211b257d30def9962ddf80dc7
                       cbdbf96da2bf598a8bbdc03bdc311ff290673ab29edf4a642
                       be726c577a1aaeb11d00d10c5a07c824bbf8e47af13042f57
                       0b6bfc05e42783d70fb3ee76ab7c2565fda74ed6536e14105
                       adf9ae943736a6c96c1102d1dc4424eda4ee1961f0d450736
                       d1cc9f6b3ad2f9f1bcd3b63ef5445798b65ad04806240edee
                       143b5c7c57f61ab7fc9fd8f0b05d984e12cee674541b6a792
                       02931e0ef11bcfc908660861b48cfd4ce0970c9726d9359b4
                       bd0c853da78891e9c9db41f2029195279d92f6831b37b5c6d
                       5ac28840e97c12f7962e65adac6705ae712daa61c0c0bda85
                       a3da6850a8dce296797beff88b1c8e8459dba0730ecace09177f79"
```

```
proverBlind = "41fb2f74c30256398c927a262602b5ac3ebc6f84d9169476f8fcb1525
               c93b649"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

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 = "11119e21b175fb9fc7c17cbbaf9f5193ff29018deab299e0179517f518c887ca"
r_2 = "293d6d461a4cfd449607b211dcc500540c49cc73d6c77b1ec62eb982be4935b4"
e_tilde = "3bc9fe82bbca21200fbbff238cf666d79270bbfc9293ea3fed177ac128cff
           30e"
r1_tilde = "5224e6c760e66d54dae6fac6adee3edca19df9f12f84416980b5c2820b64
            7ffd"
r3_tilde = "723457f7d95dfeb89077f16f58f343b1d53b44d474004564a8cc9be5c5cd
            3244"
m_tilde_scalars = "[ 107b5b89bc2574eed71a48bf869b094351bcb2a32fe4ed0f5c6
                     2b9063a086d4b, 6c757b1e66cc101e9e69c2a7c665d68ce19193
                     f11a28ac1efc0a41b5292a1a87, 635ef91197c84f74b14ef14ed
                     7b74ea6a2c4770a1f665cd545854330e3550221 ]"

domain = "04ad1197bffbb54ae41c1d43c61dc29325c2dc771d5cc7dba67907b17f564a
          04"
challenge = "4699df8ccebe97b807f5912144014bea421cc7e53b82acf1188f7420a59
             bcad5"
```

```
L = "10"

proof = "a52e00a77f6982dcac9fe2ab683073ce3f9bc195a26d721181a3dd621788917
         4379afb78920d43bd28210d535cf7e581ab496573095fa41f0a134705da4037
         ed3099bd386d29087886f746295593c881ef1a5ad19ccbcee4a6041f00172a4
         dfcb18aab20ee55c319e9f76f22ab565da3dc7ddfb797bd1ccf257fdf649742
         fba8f01252fa17bae1a59a419de5412afaf056bac7ab67ffac0ca97ed1916cb
         859d9e9ab5abb1a1fcfe290d19b1660cd7dc7581b3437904023dcdebdff473e
         1147280719c5c65338f62b5bea1d17afc0c778047141ed5dac569b761d59989
         b26f79c175d3cc30e18c8519c2fc755cc4965d6448f96e8dcad1d07f8f93212
         5645570d84b9138897ad9ce402ce6cfe73dcb70554b787a12c1eb61c2a4f3e9
         b6c425f2ae08c5c5eb65359e9e3a7faf08e0c6a486305fc931dda475ccd443a
         16310d618b71d2693d3d6ceed4d6c7d643e06ac04c4699df8ccebe97b807f59
         12144014bea421cc7e53b82acf1188f7420a59bcad5"
```

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

```
signerPublicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62b
                   d45949cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddb
                   d619e419b99c2c41b38179eb001963bc3decaae0d9f702c7a8c00
                   4f207f46c734a5eae2e8e82833f3e7ea5"
signature = "80b1195ea9e11a639e11e2dc653ccca0461055edb4f48a6e80b676636e4
             2dd61fae3e52c04e192d5053d60e73f3dec5048d423579dcb96cde6969f
             8048ce53f15ab02449b8d375f869a8df15db78eb02"

commitmentWithProof = "85d8034b358566ebfd26f921211b257d30def9962ddf80dc7
                       cbdbf96da2bf598a8bbdc03bdc311ff290673ab29edf4a642
                       be726c577a1aaeb11d00d10c5a07c824bbf8e47af13042f57
                       0b6bfc05e42783d70fb3ee76ab7c2565fda74ed6536e14105
                       adf9ae943736a6c96c1102d1dc4424eda4ee1961f0d450736
                       d1cc9f6b3ad2f9f1bcd3b63ef5445798b65ad04806240edee
                       143b5c7c57f61ab7fc9fd8f0b05d984e12cee674541b6a792
                       02931e0ef11bcfc908660861b48cfd4ce0970c9726d9359b4
                       bd0c853da78891e9c9db41f2029195279d92f6831b37b5c6d
                       5ac28840e97c12f7962e65adac6705ae712daa61c0c0bda85
                       a3da6850a8dce296797beff88b1c8e8459dba0730ecace09177f79"
proverBlind = "41fb2f74c30256398c927a262602b5ac3ebc6f84d9169476f8fcb1525
               c93b649"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

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 = "517c6ba25814e7e8a6b1e1e7a1eaefbd13a47b874a249094592b51295c896be6"
r_2 = "17d278dc4ff520d8bcde7c7f35e635c19d9d0e19e0f32e4900e4a69af300b2f6"
e_tilde = "658838c65c01e42cd39fe21885284cef7006630bf8b8ab9183bcc2d212778
           dee"
r1_tilde = "21e2ce874aaef017a9d67f01e432cd16bcf2794299e6594f5065b417d003
            9f42"
r3_tilde = "51a834a77851b6f5b476bd8ce9440019c0ba3b19a1739ae20e0834abca1f
            acd4"
m_tilde_scalars = "[ 586ad615bf1d62d511c8737ebb6a0492e0769faed21e1fb23cb
                   bdf898b25ad55, 441e55f5927fb14f4059f4d4c7aad45b72349b
                   50436cd8d2cd5ae3666ecd64dd, 10292482d9e08dc8d3a14223d
                   fdbe4a14433ddfbff0950732a12f99edd78efd9, 1acd7900624f
                   83027ee6c7700c579d10eaa0060dba6b94322470949717394645,
                    4e525012cc1649cd7a6a4d3a16899e39b9d877243716e6212eff
                   b6320294a382, 65f2bf6e3dcde2dece63dd45ffcdecc8019f046
                   64cb245f45ecdbc945e8a4772 ]"

domain = "04ad1197bffbb54ae41c1d43c61dc29325c2dc771d5cc7dba67907b17f564a
          04"
challenge = "7137f42d2323aae0fce28b89d8188168642178799c25dd6e2e84a8939f1
             1c77a"

L = "10"

proof = "b9b86d89d9e2a9431a8c17b5ea8426448214775d354674b2a0e956c7e10dd7e
         0d5a1034ae733f5591eaa4bec1f3828bba1c5f4f9fa371916a11786c4d249c4
         33f8da8cd3d8134f3539347081d0d59aa63119406e5363beac4104dbdb22959
         a248e1694bd75dd3ff05a40707f9a3bc9f3e1f41ce555ca811d87514e81baa6
         e01923520686eab039a50cb09f9bd4c227084fdb55d2c016f406148575c08b6
         ee6156cb3df0de1662fea2f501ed628a34f4857213f57043ea334a655e17b37
         10b19502d472e7f325d5ef6a64a62c944cb84f2e2500bffdfe1fe9918e78501
         d2fef372cb1373c181394a4ce9adf7e37831c765b0b7ba3fcbe305cf14df858
```

```
         204ecb9217e9eb4f99df376f4be5d5ba43dc608551a87d6b3fcfc435c71923f
         32d3e8bada181269d445453ca4dbccc8a967c90af6d6194f7c3d3f92b7517ef
         67b7c041ae7540ff9299bf5234d6e795c8d186ffdc1c418707616978e67038f
         823a2327f0f12b9c015c4ca56171c4116a13c91a86a732a56e7d0261ab21b38
         218cb8b5701f485424e7fc1e886d021b605c37d047a134563c97d4f51161ddf
         fa6553495fef3220918c436afcb433e82a7606feed6667137f42d2323aae0fc
         e28b89d8188168642178799c25dd6e2e84a8939f11c77a"
```

8.2.6.4. valid half prover committed messages and half signer messages revealed proof

```
signerPublicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62b
                   d45949cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddb
                   d619e419b99c2c41b38179eb001963bc3decaae0d9f702c7a8c00
                   4f207f46c734a5eae2e8e82833f3e7ea5"
signature = "80b1195ea9e11a639e11e2dc653ccca0461055edb4f48a6e80b676636e4
             2dd61fae3e52c04e192d5053d60e73f3dec5048d423579dcb96cde6969f
             8048ce53f15ab02449b8d375f869a8df15db78eb02"

commitmentWithProof = "85d8034b358566ebfd26f921211b257d30def9962ddf80dc7
                       cbdbf96da2bf598a8bbdc03bdc311ff290673ab29edf4a642
                       be726c577a1aaeb11d00d10c5a07c824bbf8e47af13042f57
                       0b6bfc05e42783d70fb3ee76ab7c2565fda74ed6536e14105
                       adf9ae943736a6c96c1102d1dc4424eda4ee1961f0d450736
                       d1cc9f6b3ad2f9f1bcd3b63ef5445798b65ad04806240edee
                       143b5c7c57f61ab7fc9fd8f0b05d984e12cee674541b6a792
                       02931e0ef11bcfc908660861b48cfd4ce0970c9726d9359b4
                       bd0c853da78891e9c9db41f2029195279d92f6831b37b5c6d
                       5ac28840e97c12f7962e65adac6705ae712daa61c0c0bda85
                       a3da6850a8dce296797beff88b1c8e8459dba0730ecace09177f79"
proverBlind = "41fb2f74c30256398c927a262602b5ac3ebc6f84d9169476f8fcb1525
               c93b649"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

revealedMessages =

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


revealedCommittedMessages  =

0: "5982967821da3c5983496214df36aa5e58de6fa25314af4cf4c00400779f08c3"
```

```
2: "835889a40744813a892eff9deb1edaeb"
4: ""

Trace:

random_scalars:

r_1 = "11ac0d86f78a0bcdc7c20417d73522b46d20a8f7e3ac008d2d3bd77730614b34"
r_2 = "2697d76e223bda4ed35e2428030bac7c2ca77122e3bab7b5d6b8bffca307a3d3"
e_tilde = "0fc4a68d61483036dbf45878430cc8382283c481c8c1cd3c9d3fe9aec9263
           be3"
r1_tilde = "1baffa5c4d6187496310d4014bc9f15d0150f215868722186679b8e68d84
            b682"
r3_tilde = "05b85a30f2f49348d34ca44242820c77421979b9b312a05b0fab16690026
            d86a"
m_tilde_scalars = "[ 6f7e7893731097ba853486fea7eb62f66e3e14be47b0565b388
                     c5a9170135b86, 45a4a12e1a7a518a63b66eebbce90605c29f24
                     9f570c85685bc0232c8011fbf3, 2ca1dd61fa58bc6670268750f
                     5acdb19dbeca06ff2eb1a352d69e21318042772, 0c79f4d9a637
                     3202c102adf291522c06e2bf7f0da76f8e6cc3d6762bcc6bee1f,
                      48f8c3fdcdde12d9949c6ba62661e5694363145f140be07d928b
                     4ea9521a838b, 382d6baa8558a7cd49b2fb6ad333114d7d4842c
                     1c29aa2fcb8d6159aa40e84f2, 53ae47dc3e329331a0cc2f4692
                     0d6f8b07f27afc4ad662ddad0e61d5e1b74751, 6165660f8dde9
                     349f501d169e463ddef10b94a248f2de5701966e65ba16b656a ]"

domain = "04ad1197bffbb54ae41c1d43c61dc29325c2dc771d5cc7dba67907b17f564a
          04"
challenge = "66a90c03c8cf53516b6fc592dce852df5bdda6151c17c199d52cca1be06
             6f530"

L = "10"

proof = "86645a1d743284cd08b0659c0f884432de1340f1fb105a7e21ba0cfc34758d7
         56e9e20437e318a4ddff4e1b1d80720138b40b6e3b1b1f9d86aa8ccf51c1bfc
         e10a19b8ac8a6fe4e5256f1e2ee542d44dfacfc6717780b2e4e6601d21e1944
         42db47d0504a29994d88421cdd33950cd46a69b7c31384b17cf98c268c0de5b
         afb02febaae8fbe66e3246311d80d81149e82fe87605c0e233625c108c1c0ba
         d5ba4cce88c6c363f4180f6e18dd252c3b79d06f66513eabcca7f127e2e62c8
         4ab727f167f5732af269619f0f78a279dbe98653a70f99993f65d38fe6f180a
         bf9286cb975b4ce6834467d86c5ec1a1ef4e8c3391f30e14b16a7a6c96e38ee
         f5834785be198207bd5e80213ce626c72ca4222f7281120ee67e850b79b6691
         8863b84ab894cb47cc8729af1300e6c116fa9218c6d7e90119a4964abbddf82
         238bb7d35a5d4390a8879fe56c6b39427623111f391c211571cf5ba209aca01
         9c448aa7524acfeaa7504b8fa3d0e95cc0e99e83ae41b0a8663c8a440ff3b77
         b50808934cb4fef2645f4d000a452e692881274359fb597aaff6f73b0a33134
         c4d7333adc1b501c3bdf1296d5131c497bc556ad0b280409185b1cc65dd2f90
         7e8cb93db88ce4e52c37c02dbbf696b81ecd57a11890796315d19c9bde637d9
```

```
         c1fbaeaa14b092dae8d7e50343e8b5f753bbff7f1944ca366a90c03c8cf5351
         6b6fc592dce852df5bdda6151c17c199d52cca1be066f530"
```

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

```
signerPublicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62b
                   d45949cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddb
                   d619e419b99c2c41b38179eb001963bc3decaae0d9f702c7a8c00
                   4f207f46c734a5eae2e8e82833f3e7ea5"
signature = "80b1195ea9e11a639e11e2dc653ccca0461055edb4f48a6e80b676636e4
             2dd61fae3e52c04e192d5053d60e73f3dec5048d423579dcb96cde6969f
             8048ce53f15ab02449b8d375f869a8df15db78eb02"

commitmentWithProof = "85d8034b358566ebfd26f921211b257d30def9962ddf80dc7
                       cbdbf96da2bf598a8bbdc03bdc311ff290673ab29edf4a642
                       be726c577a1aaeb11d00d10c5a07c824bbf8e47af13042f57
                       0b6bfc05e42783d70fb3ee76ab7c2565fda74ed6536e14105
                       adf9ae943736a6c96c1102d1dc4424eda4ee1961f0d450736
                       d1cc9f6b3ad2f9f1bcd3b63ef5445798b65ad04806240edee
                       143b5c7c57f61ab7fc9fd8f0b05d984e12cee674541b6a792
                       02931e0ef11bcfc908660861b48cfd4ce0970c9726d9359b4
                       bd0c853da78891e9c9db41f2029195279d92f6831b37b5c6d
                       5ac28840e97c12f7962e65adac6705ae712daa61c0c0bda85
                       a3da6850a8dce296797beff88b1c8e8459dba0730ecace09177f79"
proverBlind = "41fb2f74c30256398c927a262602b5ac3ebc6f84d9169476f8fcb1525
               c93b649"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

revealedMessages =

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

revealedCommittedMessages  = {}

Trace:

random_scalars:

r_1 = "211c1037bcd1316e4160817643c34a7bbb83021ddd3b1f22f37ed5253da52e25"
r_2 = "6ca3bb81e84cd13823f2630f90f28084d1409bca3d08983d9901f290450ef52e"
e_tilde = "2a37d3d049c506148362bb3411255f08bd504553caf90b877569b7250ca7f
```

```
           98c"
r1_tilde = "3427333b9226659b999a422946edc23b382d9a355ac03ec8dc45ed57cbe5
            6bc4"
r3_tilde = "633a0ef2d7d6a96a6d273e6984d0dc3a4d8a619fad2be125dd3e4237bfe2
            e53a"
m_tilde_scalars = "[ 5f2b419df907cc204177fb0f60a8865cafc792fec2a5eee3361
                   46ad811cbd483, 03c340104c6b71dd62b77ed31d2b4863e9a692
                   5cb9b78666a0b8c400c4ca31f8, 45f9d520e8682e349a036b876
                   3fd647d2a1cbb81a77f61da5879d563948cffe4, 4010f0d66857
                   c907ebb8f7544e04ff1ba4bdc2baa19f63b4a146f5ccc3853544,
                    4ca37c03d4ab19de664f57d18874d7b86434cff1389cf9865506
                   bcc49f63b4f8, 47965b117a3d83c8133a1f915f858c0b4e1f3d6
                   48af84dadbf722696ab0d62f2, 68bbcf9066fd79d6224a0a8d28
                   9bc38cc7768bca389779edfa29b0fe874b2645, 6185e602029fe
                   3df6f0023323d20d33c67e8e0093e4d603e00506869aa2fa57c,
                   47f3355d90deaa185a76e02fc2bb521714682686569e36f016f51
                   61babdc3006, 461a8b4fc326abf2bc18c43df883fd512d460419
                   c4ee361a45714d8466b5750f, 4da6a68e742b02785c398f1693b
                   856908138fa2376c03546ab2b4168853c255b ]"

domain = "04ad1197bffbb54ae41c1d43c61dc29325c2dc771d5cc7dba67907b17f564a
          04"
challenge = "477a74b3d777518a92fb4ef3b34ba3b63c5282bfc2cd617f19985858425
             bf2b7"

L = "10"

proof = "84de896fc56822074415cda24d66c850e5870365120586dfe07ffbb9d58dd9e
         8b290d72b649b63dfc8bc2473e77ea26dac12380f076960d8416cacba2fe2d5
         cbd3b381ebc7ceb94d7bf966b70122efb7d30d9232a8d33983d94cc8d8792ad
         98c95b9b4cf8007e45767c0d393c4f8366f5f483fffe59a457bcf33e8107853
         61fd4b174d7a477accf0046b5cf0496617d2316579de07be03d310881b640aa
         6cf0b70c23178bfbefd65aa26e33dd28217e9627633d09dba0a6ee70ead27cd
         17c3bb62b92b68d5c434a913ce73e29359dc0d6dd8e735847e809ff1310218b
         a987d39b3a8751ef93e12c8ff3cfa9b1d4edecc10c34cc7d5c4df79a40baeea
         fd1ca1cc5202a8b4e366096d7a14fbc15a103f142ddbb490f422a4ccc277f0b
         0e2f82b0db214bf7b042a6b2f8901710bbc76f73034c4491ee7f652bedb5d75
         362cfeb25508071c8637c2a9fa25f49ea1be0ac97670fde3b36ea07c54a0770
         ceb46eb8913da3781c2537e40a71d99b1725fb85a672d8bec46660b40f5b822
         3492274412a66eda24a3870af56c6ccfde2e54ea37e0307f0439f18fa06e8ab
         46850707dfddeb3c5298df0cfc5fad95ef97d3c05bbef5f534af6366ab5cb7b
         6d54bb5e97afc31517c03165b0666281c67752e0be8d4c46f960bdc4b5bd35c
         f81cba16f3cbdc14eca3d870f8fee8697f17b06c02b76505250be5edde0c39c
         1397bbdec2b16696bd558aedb7efe9b1c3057798bb41b02265aeb737b02e3dc
         747ab2b974d6c79805802ec1a2c4117e9ebba0992c8d454fd2e8f16d1058b29
         8fae0c6bd73287917e8bde4ed5c52e312cc2f462d23ac2a843477a74b3d7775
         18a92fb4ef3b34ba3b63c5282bfc2cd617f19985858425bf2b7"
```

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

```
signerPublicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62b
                   d45949cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddb
                   d619e419b99c2c41b38179eb001963bc3decaae0d9f702c7a8c00
                   4f207f46c734a5eae2e8e82833f3e7ea5"
signature = "80b1195ea9e11a639e11e2dc653ccca0461055edb4f48a6e80b676636e4
             2dd61fae3e52c04e192d5053d60e73f3dec5048d423579dcb96cde6969f
             8048ce53f15ab02449b8d375f869a8df15db78eb02"

commitmentWithProof = "85d8034b358566ebfd26f921211b257d30def9962ddf80dc7
                       cbdbf96da2bf598a8bbdc03bdc311ff290673ab29edf4a642
                       be726c577a1aaeb11d00d10c5a07c824bbf8e47af13042f57
                       0b6bfc05e42783d70fb3ee76ab7c2565fda74ed6536e14105
                       adf9ae943736a6c96c1102d1dc4424eda4ee1961f0d450736
                       d1cc9f6b3ad2f9f1bcd3b63ef5445798b65ad04806240edee
                       143b5c7c57f61ab7fc9fd8f0b05d984e12cee674541b6a792
                       02931e0ef11bcfc908660861b48cfd4ce0970c9726d9359b4
                       bd0c853da78891e9c9db41f2029195279d92f6831b37b5c6d
                       5ac28840e97c12f7962e65adac6705ae712daa61c0c0bda85
                       a3da6850a8dce296797beff88b1c8e8459dba0730ecace09177f79"
proverBlind = "41fb2f74c30256398c927a262602b5ac3ebc6f84d9169476f8fcb1525
               c93b649"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

revealedMessages = {}


revealedCommittedMessages  =

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

Trace:

random_scalars:

r_1 = "72202656d242b95e869fbcd40581b1924183ac11ac323ebbe011d63536d8287c"
r_2 = "1b6f80e77f00fd46a7ab1e46be33db2582fbadbf8358e7dfb157c69f577b9063"
e_tilde = "48e116be2272e66dac308ec305869640dcc107d3de941659e7dfa80359a3a
           33d"
r1_tilde = "67dbca3425cd03873b9ef9240389de348618c4eb142eb963f03e99f5cc85
            755f"
r3_tilde = "38beeb508bc526d9f70af680eb5e747daf0b0abf9c5dd2da78a795eb082c
```

```
            891e"
m_tilde_scalars = "[ 41e0af39eb876d842a6fa22e739bd8557782d8bc64f1e3e8caa
                    407acf21e9d83, 34318199184c1d1b0088b30f12b59b5be5eaf0
                    a6d4f1bd06cae1844ce79493db, 449a1a27becc2536480469500
                    2bb8671d66119c6b47ca0090a42690f108b8743, 0db0eb8b8579
                    27356955a1e251ad1df40e45427e8dd488b822608565a62a5a31,
                     3030cf9de98a457fdfe9cfbe693e53a2eefbe6590557b04bc5ab
                    cc981b2c5b53, 21e0abb919758a5b8bfd32cc6417b36ca94d091
                    a4ef4b6e9e6840a174ed193d4, 6d46722a4f82d87d5012bab944
                    b18239571c6c20b7133b529d0cd81999251eee, 38af70a2dc939
                    db80ec191f993d38ce477fbf53f0de85c8676e0bd32fb6529b9,
                    39c92b70c8e3635a623da5dfeccb3b2a706e8179f1c94c5185f8c
                    f3a4147f0e4, 1521952789a9f1a2c8e88d102574fc3b11644dcd
                    57e4658bcf37f44ba575a69f, 5ecc4872b50ac3e9159dc3eef11
                    260766090788a864607e669c50ebc489d5a75, 68c917c66ecd82
                    9f333f0f9b12fcaf0c93e6f085fbb0d490e1e1a43ba59d6a94, 6
                    0f3ae300246e53d20ec89d0bce7f4ea8bb2f669f9b972f5e47540
                    1ab9a44ad1 ]"

domain = "04ad1197bffbb54ae41c1d43c61dc29325c2dc771d5cc7dba67907b17f564a
           04"
challenge = "48119c1d708f74bc0949d4c8192562b4dbfd026d123aa296af59e1c64db
              b35b1"

L = "10"

proof = "aaf787d7c259d7acedd1294d0523586acfd5e05c9352ef3ba19147bebba3136
          df55cb7af38abede5736351ad1b7a967c80b662ac990335f89b5202e881770c
          41b6d5da92a2d997f414ccc9e0f5ff07a916eb2262346e19127baa6d63477c4
          0c1adfad4fc36849254eb5baca5da75b5ee3574d0f4b06655b2669ee88ed7d1
          fc76badaf119576cadea140b4441ba3f4ed869ed74d1349b5d625f52879d099
          87f9a37f67b515c1c3ae37ff95887c44641db0562dda674e046d0dd0329498d
          78a4c04525f5f70d46bbeba884f1315d1e0e0a11d64d2d7135ac5247d66dfc7
          55d0ceaaacd435eb379968482f13054121743b2330bd2102da2f876bf6379f7
          f345a6ae731aaeeb63e3a1986c7325ce5707c9c73908d5be9fa555615626dbb
          c3a8893046af612189b39441e42b7433ef181d1423f3df67021fc9de3fbb3a3
          4d69a9bee7cda3db6cfea80f3ef464b9d5abea25db3174abd99e71dc0f396f1
          4d5579556e5c11186156a8c07938cbf860ac0f45b3c235dc8b744baf5656e76
          fcb25020e3069fd5e9a71966118f81246b85a46c62a070a6e66132aca408454
          be0fe2fa4909de71fecad7c85b2869da3787d81fa1d735c72f5479b811bc8c4
          cbc3af332dd7146cd8f933c009ae417a86d8c3ca9f1e5738b6050be9b690422
          a10128428408f1399a628c89f0d2296a4402c0fa529e06729ed80f59c2c8513
          f7b2776b1e5750dd71aaecc0dbf1ed783c35af918099340d614971744f1687c
          bf988438f7f6598a3651be1453ba4491f5c6e6442c973de305c452a8114ff07
          163107dbb65f96fc7ac33ea89db973bfd7e5e4c3a57654b317189220a753c30
          a77902cd969d7e615ec7114795d42a3f3810dadc115ee67e44b29cf35181da3
          903b5219fbef708e73f003e474b1b8dbfc53e1dd7a9134f17b1c48119c1d708
          f74bc0949d4c8192562b4dbfd026d123aa296af59e1c64dbb35b1"
```

8.2.6.7. valid no prover committed messages and no signer messages revealed proof

```
signerPublicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62b
                   d45949cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddb
                   d619e419b99c2c41b38179eb001963bc3decaae0d9f702c7a8c00
                   4f207f46c734a5eae2e8e82833f3e7ea5"
signature = "80b1195ea9e11a639e11e2dc653ccca0461055edb4f48a6e80b676636e4
             2dd61fae3e52c04e192d5053d60e73f3dec5048d423579dcb96cde6969f
             8048ce53f15ab02449b8d375f869a8df15db78eb02"

commitmentWithProof = "85d8034b358566ebfd26f921211b257d30def9962ddf80dc7
                       cbdbf96da2bf598a8bbdc03bdc311ff290673ab29edf4a642
                       be726c577a1aaeb11d00d10c5a07c824bbf8e47af13042f57
                       0b6bfc05e42783d70fb3ee76ab7c2565fda74ed6536e14105
                       adf9ae943736a6c96c1102d1dc4424eda4ee1961f0d450736
                       d1cc9f6b3ad2f9f1bcd3b63ef5445798b65ad04806240edee
                       143b5c7c57f61ab7fc9fd8f0b05d984e12cee674541b6a792
                       02931e0ef11bcfc908660861b48cfd4ce0970c9726d9359b4
                       bd0c853da78891e9c9db41f2029195279d92f6831b37b5c6d
                       5ac28840e97c12f7962e65adac6705ae712daa61c0c0bda85
                       a3da6850a8dce296797beff88b1c8e8459dba0730ecace09177f79"
proverBlind = "41fb2f74c30256398c927a262602b5ac3ebc6f84d9169476f8fcb1525
               c93b649"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

revealedMessages = {}

revealedCommittedMessages  = {}

Trace:

random_scalars:

r_1 = "2aa67d3759b3aa6cdc1e57822f10e4ac850a7f80a82f0967cd5fd21899ca0b69"
r_2 = "1e946e0a41c6a6dcc24894f477899f060f0f6bbe5b913022848d39e356d83cf1"
e_tilde = "6d6c354149a71ca3c43e5657fee3b95652c5978125350c6d317cebc9fb882
           92a"
r1_tilde = "2508a44ef5e20176698f111e2375bfa84661ee27189c300bde8b9d946ceb
            58d7"
r3_tilde = "35632248dc2eea031c09ae0797e1b9974d675d60df32035a5fde566ff71d
            d247"
m_tilde_scalars = "[ 26f66a47894e184b5fe32a2e6568c0786af376d089e2a11e632
                    978c183a6f3fb, 6d3606b3086f0c44c209c5af201d48d20e015f
                    0fc80fd00a10259f7f46ea6eed, 22063ed43999f4ae40a03c4ea
                    9f934b3f946dc167957b20d501a134426695cc0, 29930e487c3e
```

```
                    109322d0f2e097616ece04d87d91649dff92bda1dc438400256f,
                     4b0cff28fe171b5179977f6bed33413ba420e0656e468a579a7f
                    dac983d24314, 6451fce17b93ed5dbf4d2aafbbd6afaa18e6f22
                    2046ac31ed2dc1d6df9a33291, 1f9c3ab790fbad9b71f7478396
                    9fb01a14fc7e1f417a38696b0430a77b68fe94, 480b325408ff5
                    4ddd292d3c3ce8253c540cc8c32ef42308389bc9543c471c2da,
                    5e02607fbd4d0af561e61c377e2b31c2ae1c589ba835f93bd7be3
                    814f65ea450, 6849cc6bf9367386c4189859998d9c4993c84488
                    f9b03d311c197499dda1ee0c, 51b9c711f25213b6a63a9ae2ade
                    5b0d517539992c40bb45297d0709b216db36e, 6be3bcea66b687
                    2421a2572b0c37cfdd0541d226a18fefdd60619217554eb08d, 4
                    8fd2d36c9e119fba1ad5f5fef059838c7b0150f7a4088919ed9bf
                    6934f7c90b, 2c7589a2b29e0be25b1f592ecb84d072fb17659c4
                    bfc6dfc54dba002623f5a0c, 55976175ecac1373e3e27ed645de
                    08514e66d50600363a6de6e791f3358b06f2, 5a4d330bd5d5fe0
                    2528f8c3b2a7d3dcc223d11452f2f772e95cc36b74fc4c60c ]"

domain = "04ad1197bffbb54ae41c1d43c61dc29325c2dc771d5cc7dba67907b17f564a
          04"
challenge = "2fbf52fe4cd4ddc5d94a808edb0ee59f72b54a5a52f2f30b1f43c169b29
             7c741"

L = "10"

proof = "9341832e2e6739548581a238cd563ac3f32749c2e9b3bdfe6b2c92fb72c92ad
         d1e961ce105ff9db40b4e54c4a8fd4567afaa5d76ba043383225573bedbfa79
         02f877a399d4eca9b78b49aa12991f5c875e1a6dcccb7901b203e1865cf27d9
         a75acca75dc526343fe7c0f93f546931ccb77f0e641e0c2201798fe1048163e
         b0f6655b337e37c832ad1ce3715c8084f0211cdf757f4db45e4a5bcabf8490f
         2f3b65246d0e7ee30e475cfef6349de51b637173acf28d05753dd275fc59088
         3eaf1069e362debbb1775ccfb9b35381e21d5d5e06f74bf17819ded6ee4342e
         8bcaaa606363c70bc9f2b7b774edb83614d763a0f84229c99f6a33529c382c2
         fea6d2305ff4acc6d289bb3a576147e96d660b76058eeba1e2f0fbfd877deef
         bf30c218eb2eff9e5dafb65a4f3e0ce00c1ea9c734ef834dea68fd5c7ffc1bf
         3de96818d67a4e4c8640297a405b28285f8a4caae44d6b7b22f7afa1a9f6aeb
         9bb017f0ab1ebdbd894eebf5a1bd56ff3b21a2de642435935e7cb3208ad1543
         a01ed8473ef17ea3635d1743733253b5285a737dbd9000cd2834d27f3029b47
         fdafa389a56c434176f540dc39934e80fe6e1b4c210e00dc7e6b8573106fb2b
         2f8b772b5197c15afeeead937ed5bbd440e29e3ef6db6a60614c8462a497041
         549aa47f0a176caca4dfbbe27320b6f063fa1ef94fa64750f6eb670d1bd14c8
         5bd943c948814f680c3702f5ff1cf35bb7827a43d1e85a8c57afb55285bb9d3
         c4315fa37ee32cf1f98125ffa662919d37426623fb827ddbc2c2da69355a9a9
         2d23ba7aaf4276cba1d333dd96d1124e2753d08b2092a3408c19d6691443c40
         81593c84f05032c26c168086471f09b1906805cda31ce4a49d400679c2c4bf1
         aa06ac44627566a53eddff25095bdde0eb4ea4a47817e5d138fb0053401f5f6
         413d862679c1997439828c055c5a46de460b1eb84d077bf5b4a6f4e54296ea1
         b8e062a944b4678dc961b79928f6f7743d30bdb220365800508f9849b31bf26
         25b27b7d18cee197f2270a226872cb69ba853d0edd9245d2a4ab5bc2fbf52fe
```

```
         4cd4ddc5d94a808edb0ee59f72b54a5a52f2f30b1f43c169b297c741"
```

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

```
signerPublicKey = "92d37d1d6cd38fea3a873953333eab23a4c0377e3e049974eb62b
                   d45949cdeb18fb0490edcd4429adff56e65cbce42cf188b31bddb
                   d619e419b99c2c41b38179eb001963bc3decaae0d9f702c7a8c00
                   4f207f46c734a5eae2e8e82833f3e7ea5"
signature = "b80f73e22cf6c050159018539af4fd2c8ed75a7dfa247feadbdecd983e1
             6ddb33ac5c61bfd7f17b4063a7957456ddc0b71d46e6a05b1a464df601a
             abf480edf17ff1d6052089c294577fcfb7b851baad"

commitmentWithProof = "null"
proverBlind = "null"

header = "11223344556677889900aabbccddeeff"
presentationHeader =  "bed231d880675ed101ead304512e043ade9958dd0241ea70b4b3957fba941501"

revealedMessages =

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


revealedCommittedMessages  = null

L = "10"

proof = "a5de46751c4f2662be4aec33c0a7b869e0d0dd26d4131f1d4c87127058fedb6
         0ad474c387775e8c6209c4e60f6848d91a6f09b4587a5a6ec3e2c7ce0b46ed3
         44630f10554bdef8f92bb0b28086bc6bd77f53f3d769b8be9d0b06a4b11e38e
         e2c90e1a97c1b0d339107ae11f72cc2662b304b2fabc7fc3b3752d85f831873
         cf2ae01919569fa98f68182fa99847e4e71628e9f541ec9f9642af2eb044e33
         930ac345bfb59df26e0cfa02625ec836919eb4ae762b7b9f650cb6c623e51fb
         294cc91a5de51dbf6c6e933ce095432a0a03710af14cd2b2eea0f80bd44d421
         1dc56eb2a2f8482b411a2a7ecfe4e4f2702411f1855a295575288f4915f4d18
         c6f65f31929a22cd838571d986e8483470ace5a248a5ef191deedd241cc5613
         ff865b864ab19b80a600c741bd57842fab0b7284f449731f6a8071d84ebdeb3
         af42cfe10485b6071de72abc2b792ff729783bcea86e9d3797cbb5c6f2a1421
         4e254bece4b797048d2a23bc6509086b4e07dd42f1b30765973fea40fb02702
         dcebec349889c802d8b20d4451e8f8418c9c931acbf865f2bf6e3dcde2dece6
         3dd45ffcdecc8019f04664cb245f45ecdbc945e8a47725e3d58462e7eb65980
         e0253414373959c691e2e039b389beb064cfcdfcf7e3c5"
```

9. IANA Considerations

This document does not make any requests of IANA.

10. 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/>.

[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>.

11. Informative References

[BG18] Bootle, J. and J. Groth, "Efficient Batch Zero-Knowledge Arguments for Low Degree Polynomials", In CRYPTO, 2018, <https://link.springer.com/chapter/10.1007/978-3-319-76581-5_19>.

[I-D.ietf-privacypass-protocol]
Celi, S., Davidson, A., Valdez, S., and C. A. Wood, "Privacy Pass Issuance Protocol", Work in Progress, Internet-Draft, draft-ietf-privacypass-protocol-16, 3 October 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-privacypass-protocol-16>.

[P91] Pedersen, T., "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing", In CRYPTO, 1991, <https://ia.cr/2023/275>.

Authors' Addresses

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

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