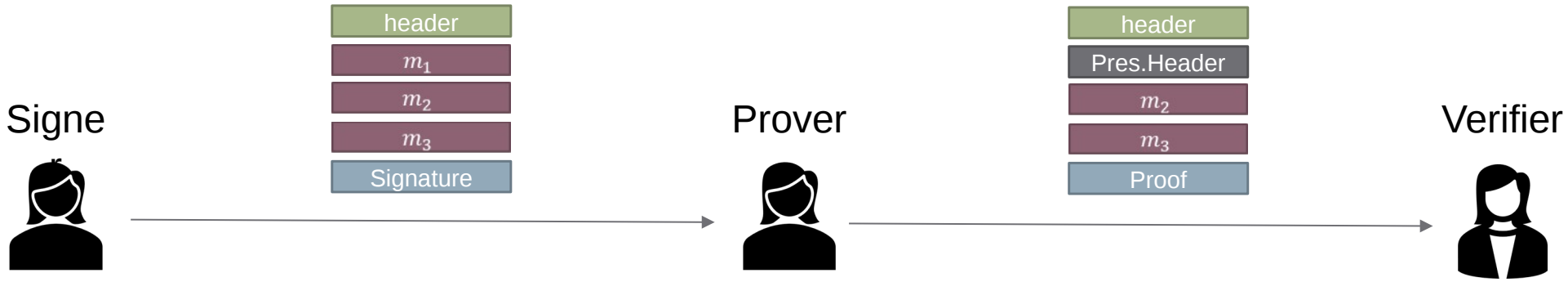
The BBS Signatures Scheme

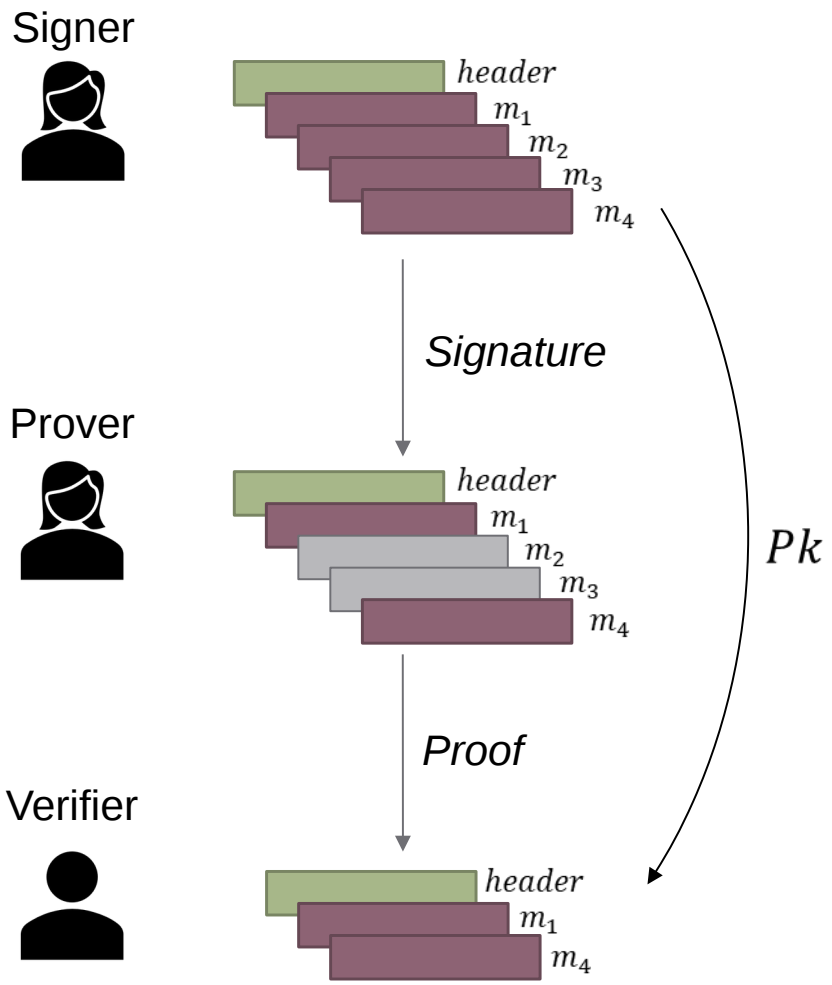
Tobias Looker, Vasilis Kalos, Andrew Whitehead, Mike Lodder

BBS Signatures: An overview

A multi-message digital signature, supporting zero-knowledge proofs of knowledge of the signature and selective disclosure of the signed messages.



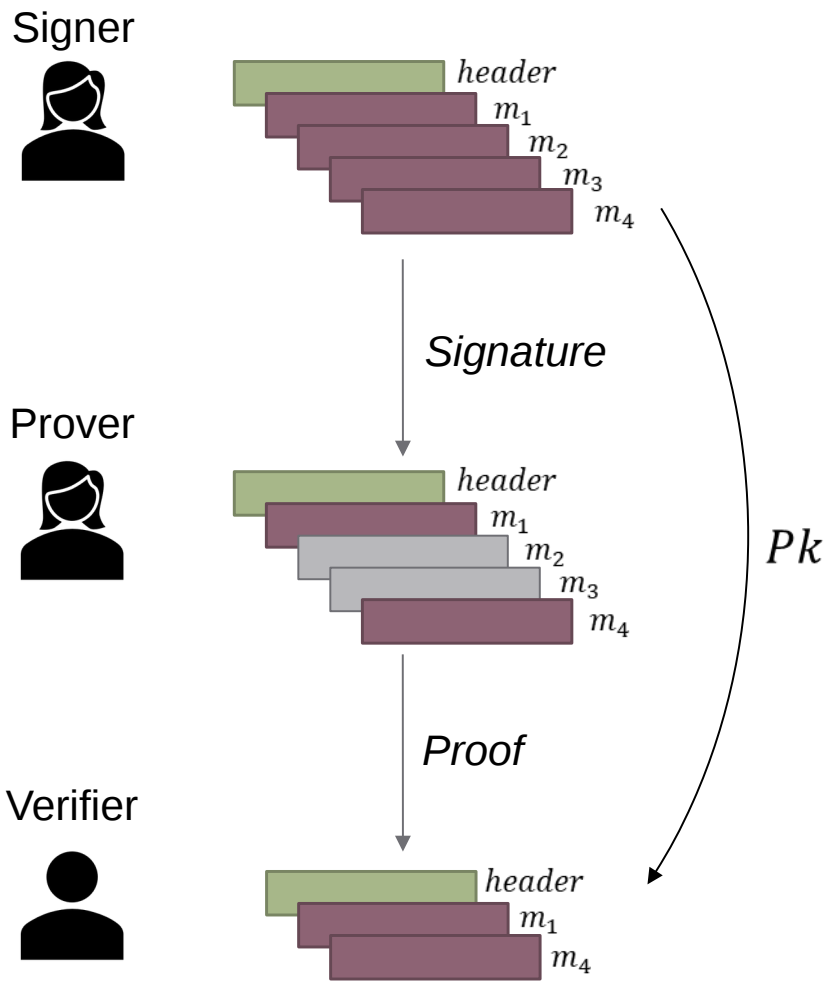
BBS Signatures: A recap



The scheme:

- The Signer can sign multiple messages and a header with a constant size signature.
- The prover can generate a (randomized) proof on a subset of those messages.
- The verifier can validate that proof on those messages and header.
- The header must always be disclosed by the Prover.

BBS Signatures: A recap

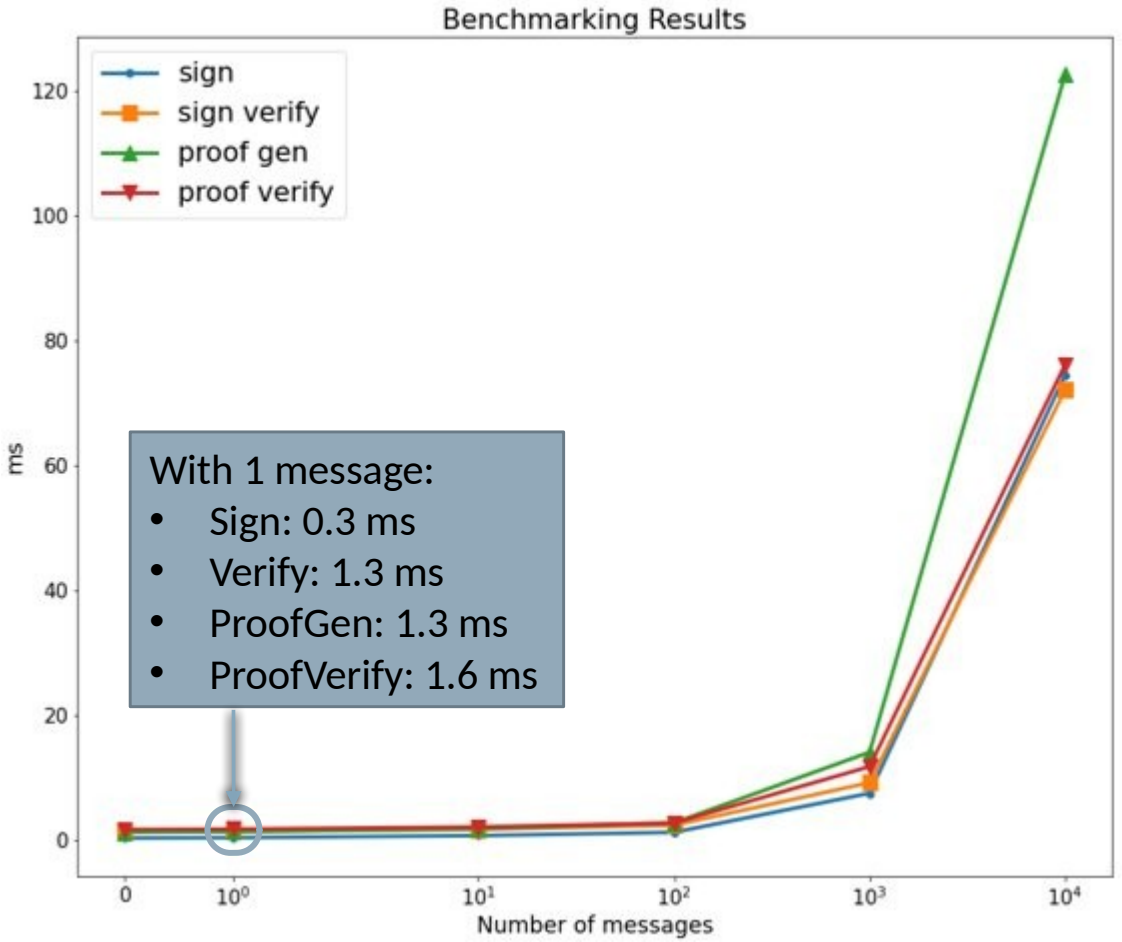


BBS proof properties:

- Validating the proof, means that the prover is in possession of a valid (secret) signature on the disclosed messages.
- No other information is revealed by the proof.
- Unlinkability: using the proof, an adversary cannot link together different proofs coming from the same prover.
- In other words, the proof will be indistinguishable from random.

BBS Signatures: Performance

- Benchmarks of all the operations for 0, 1, 10, 100, 1000 and 10000 messages.
- When messages are involved 50% of the messages were disclosed in the generated proofs.
- Benchmarks run on a MacBook Pro 2.4 GHz 8-Core Intel Core i9, 32 Gb RAM

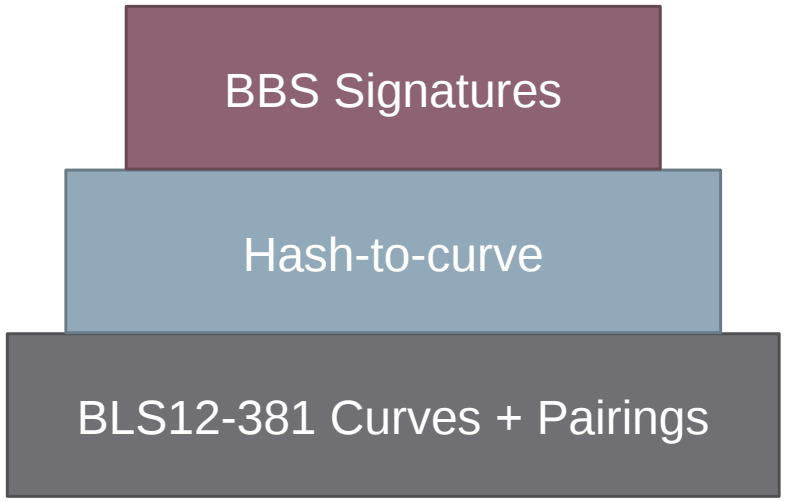


Status Update

Updates:

- Now a CFRG draft.
- Multiple reference implementations, up-to-date with the draft.
- New academic papers looking into the security properties of the scheme and improving its efficiency.

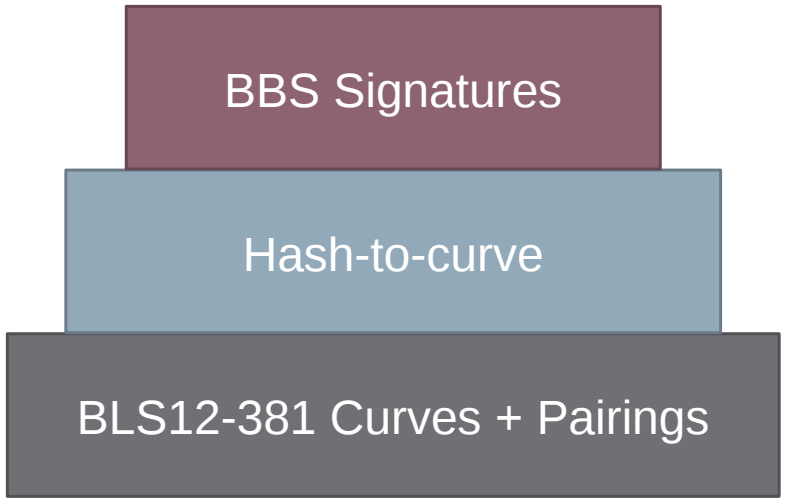
Status Update



The Issue:

- Last time the only supported ciphersuite was based on the BLS12-381 curves, and SHAKE-256.
- In the draft we make heavy use of hash-to-curve.
- There are no many hash-to-curve implementations using SHAKE-256 and BLS12-381.

Status Update



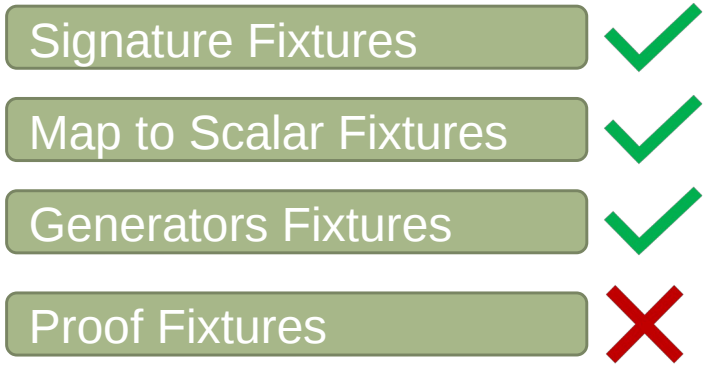
The Issue:

- Last time the only supported ciphersuite was based on the BLS12-381 curves, and SHAKE-256.
- In the draft we make heavy use of hash-to-curve.
- There are no many hash-to-curve implementations using SHAKE-256 and BLS12-381.

New Ciphersuite:

- To avoid using multiple hash functions, we added a second ciphersuite, based again on BLS12-381 and the SHA-256 hash function.
- A BBS ciphersuite can be build using just a hash-to-curve implementation (not directly needing a hash function).

Status Update

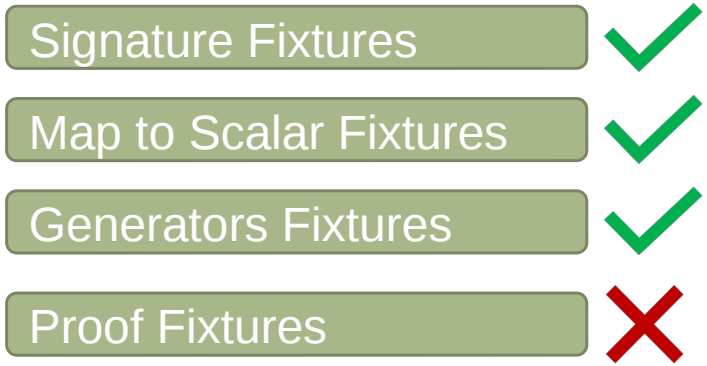


Updated Test Vectors

Signature Fixtures:

- Updated the signature test-vectors to include new features (the header etc.).
- The new signature, map message to scalar and generator fixtures have been validated by multiple, independent implementations.

Status Update



Updated Test Vectors

Signature Fixtures:

- Updated the signature test-vectors to include new features (the header etc.).
- The new signature, map message to scalar and generator fixtures have been validated by multiple, independent implementations.

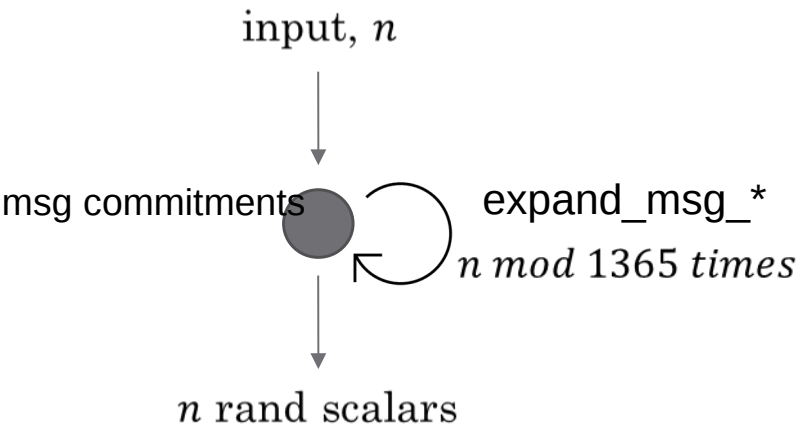
Proof Fixtures:

- The proofs are by their nature randomized, needing random scalars.
- This makes creating fixtures for the proofs challenging.
- Use a ‘deterministic generator’ in place of the PRF?? or list the random components of the proof with the fixture??

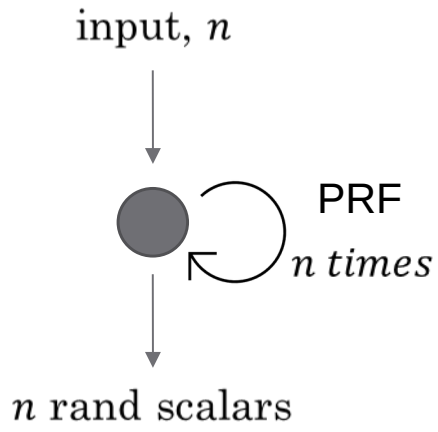
Next Steps

- Because of reliance to hash-to-curve, we have created a small upper limit to the number of messages the prover can create commitments for and hide (1365 messages).
- Different solutions have been proposed with different tradeoffs between efficiency and simplicity.

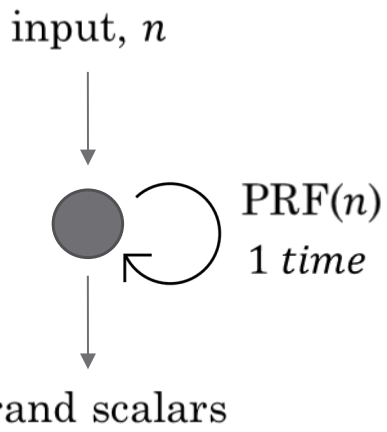
Option 1



Option 2



Option 3



- Big thanks to Riad S. Wahby for helping as with this.
- Options 1: more efficient, Option 2: simpler.
- Next steps are to decide if the performance of option 1 is worth the complexity.

Next Steps

Other immediate next steps:

- Work with the academics reviewing the scheme and apply any potential performance or security improvements.
- Add proof test vectors.
- Apply suggestions made by the implementers of the scheme.
- Refine the scheme and request review.

Questions?

https://github.com/decentralized-identity/bbs-signature

https://datatracker.ietf.org/doc/draft-looker-cfrg-bbs-signatures/