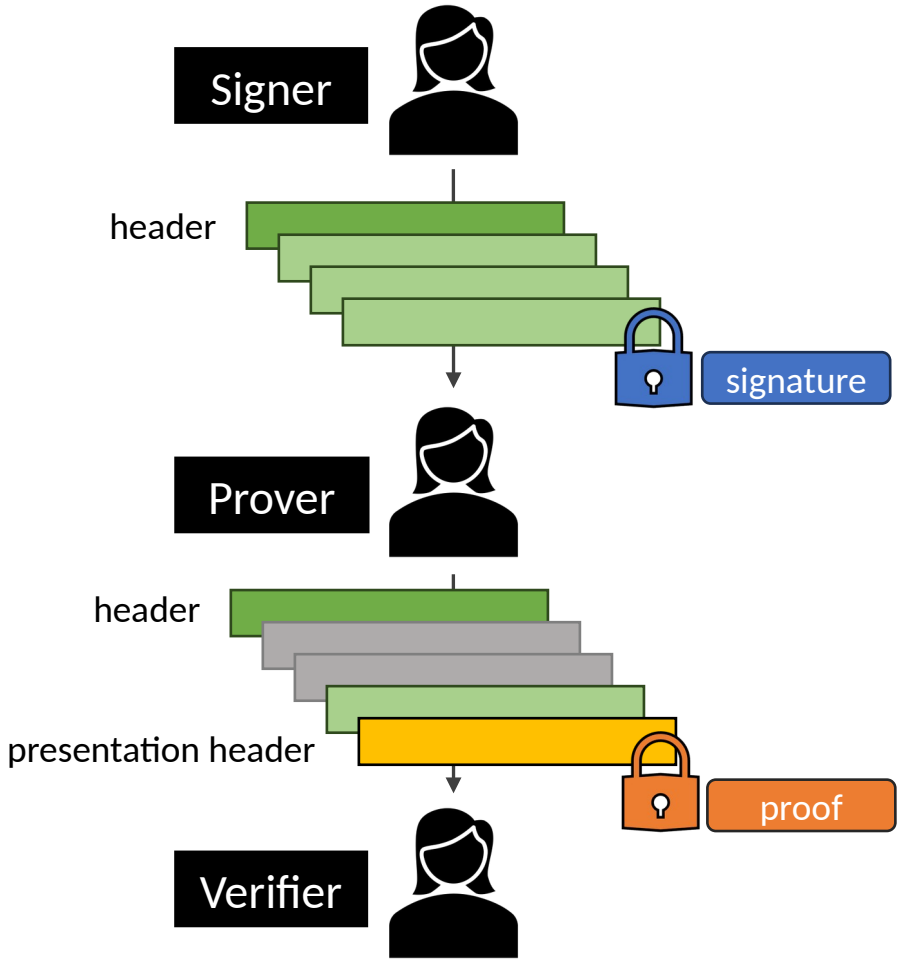
The BBS Signatures Scheme

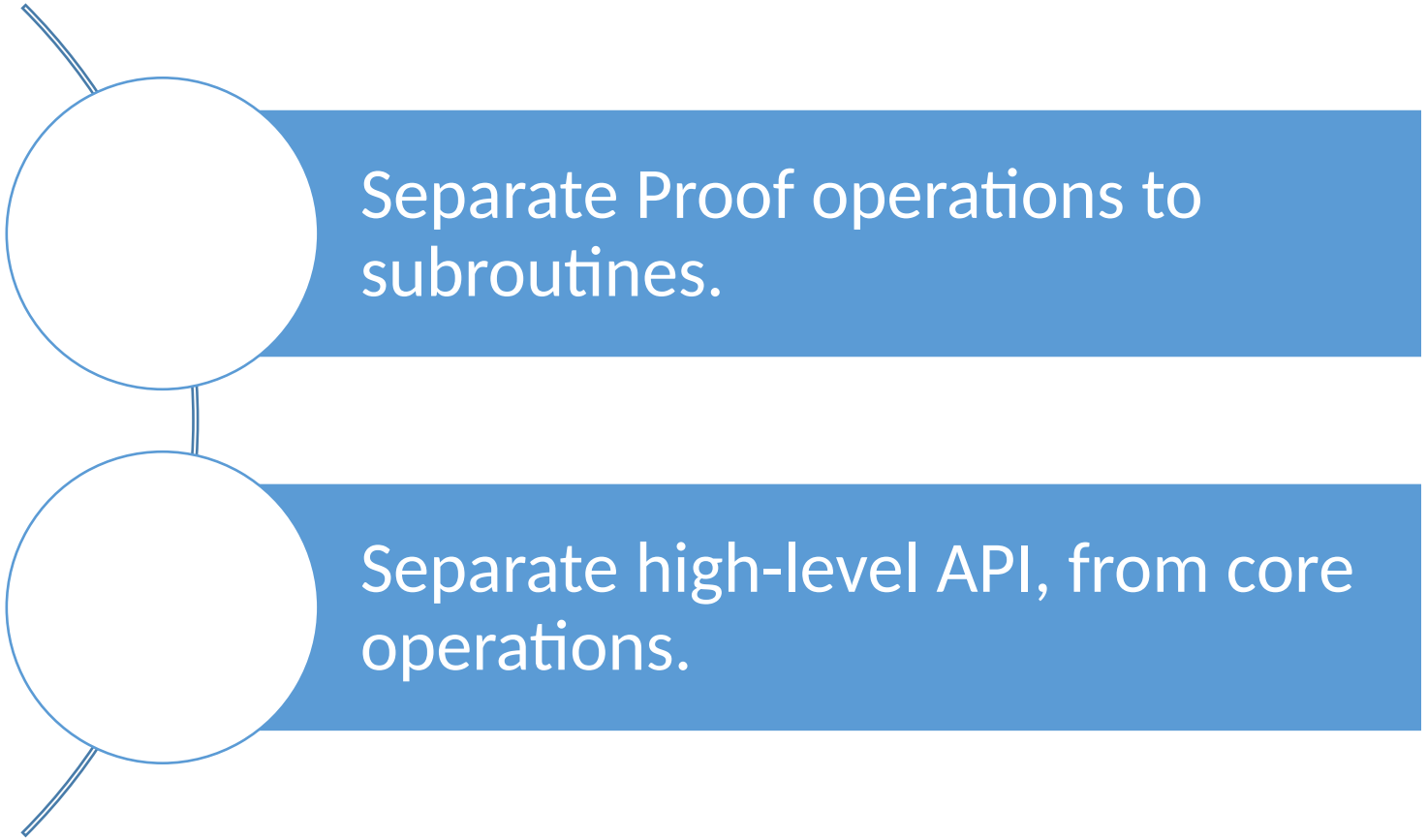
Tobias Looker, Vasilis Kalos, Andrew Whitehead, Mike Lodder

BBS Signatures Recap

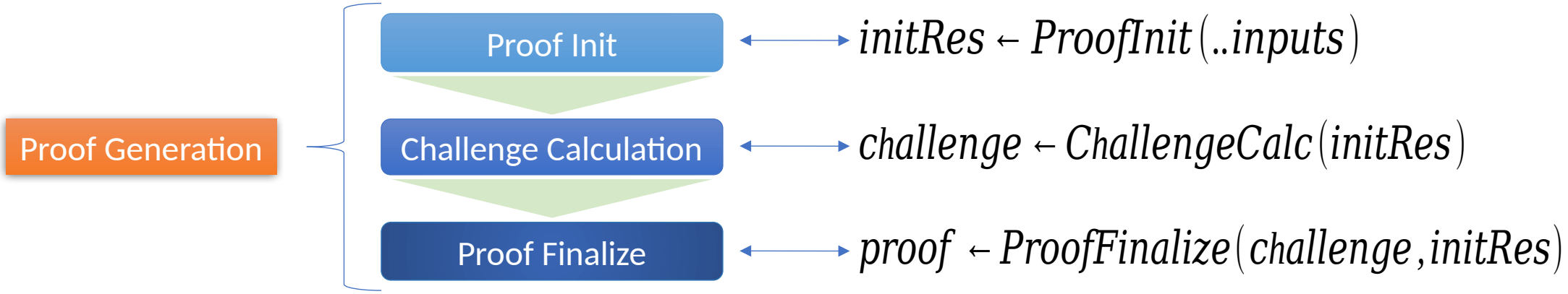


- Deterministic multi message signature.
- Unlikable proofs (zk-proof of knowledge) supporting selective disclosure of messages.
- Header: always revealed value (e.g., alg identifier, token type etc.,).
- Presentation header: value bound to the proof (e.g., random nonce etc.,).

Updates in v4



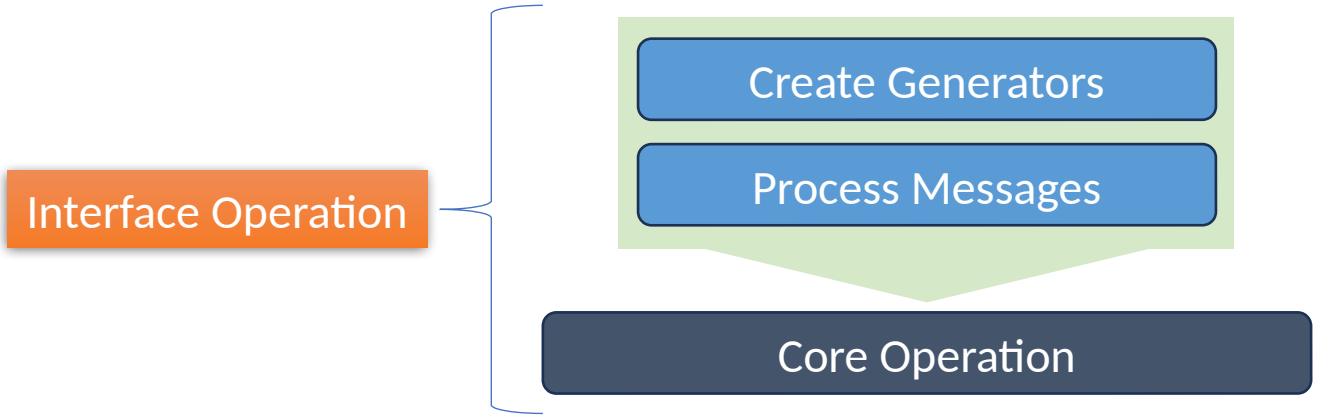
Updates: Separate Proof operations to subroutines.



Examples:

1. Pseudonyms: https://basileioskal.github.io/bbs-per-verifier-id/draft-vasilis-bbs-per-verifier-linkability.html
2. Anonymous revocation with accumulators, e.g., [VB22]

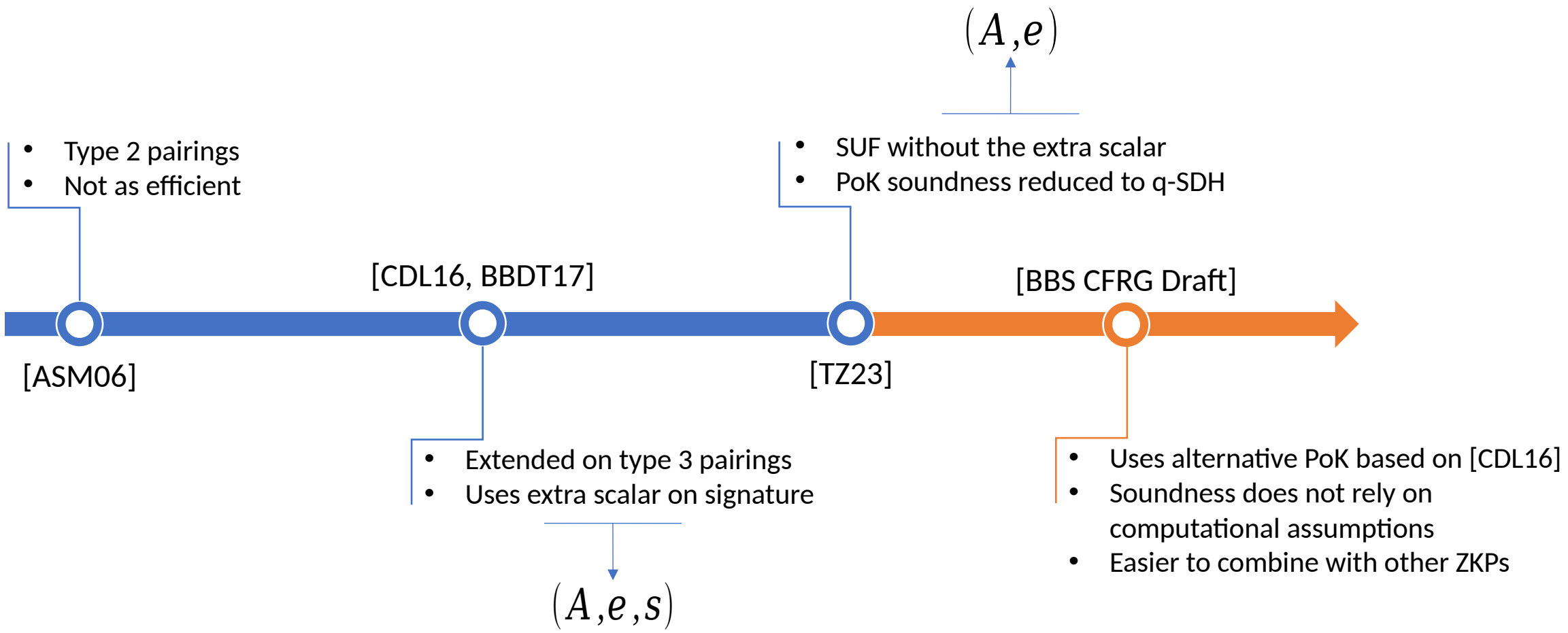
Updates: Separate high-level API, from core operations.



- Removed Create Generators and Process Messages operations from the ciphersuite.
- Interface operations manage creating the generators and processing the messages.
- Core operations accept generators and processed messages as input.
- Allows application specific generators and pre-processing of messages.

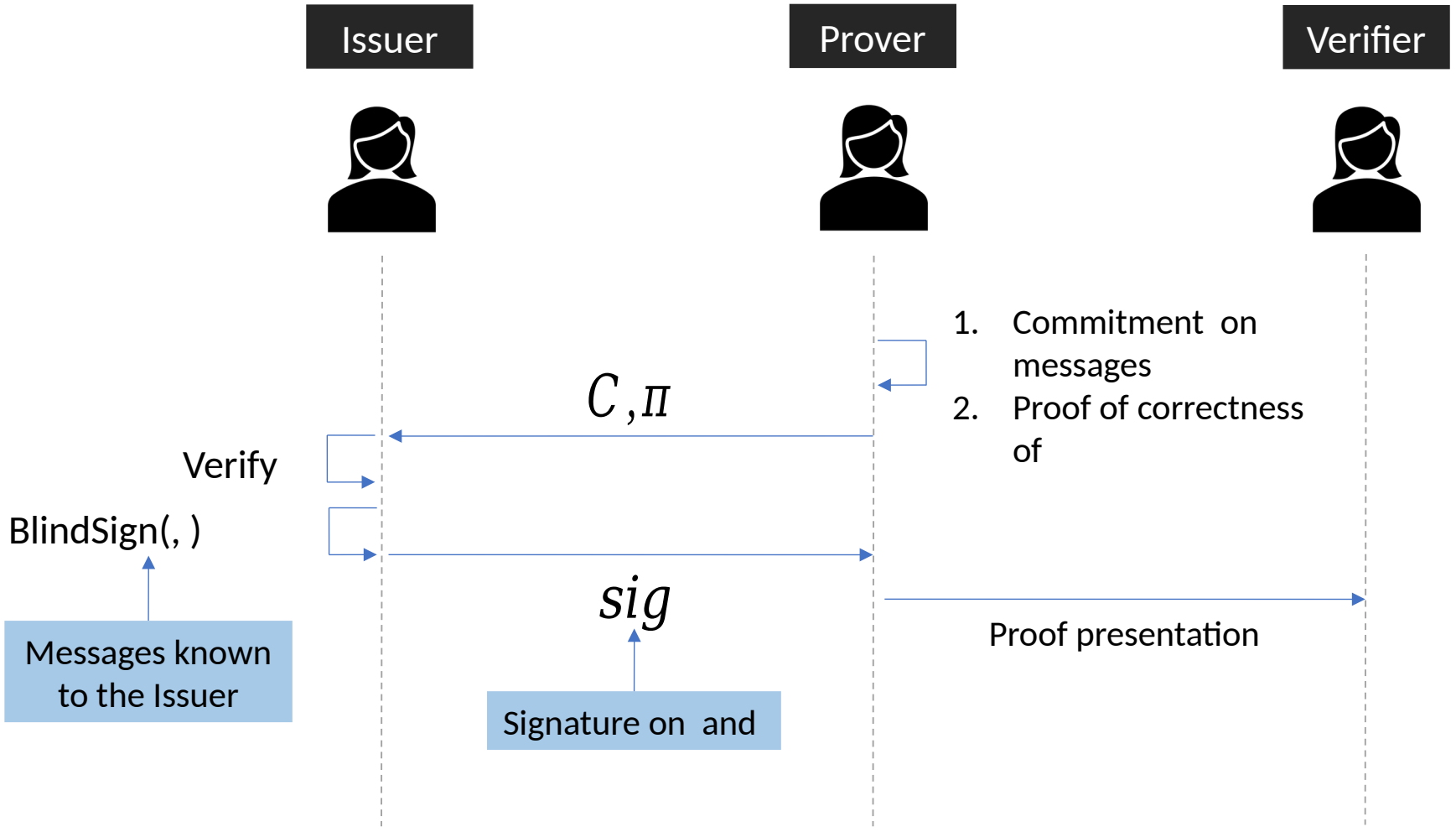
New BBS Proof

BBS Proof Generation Process

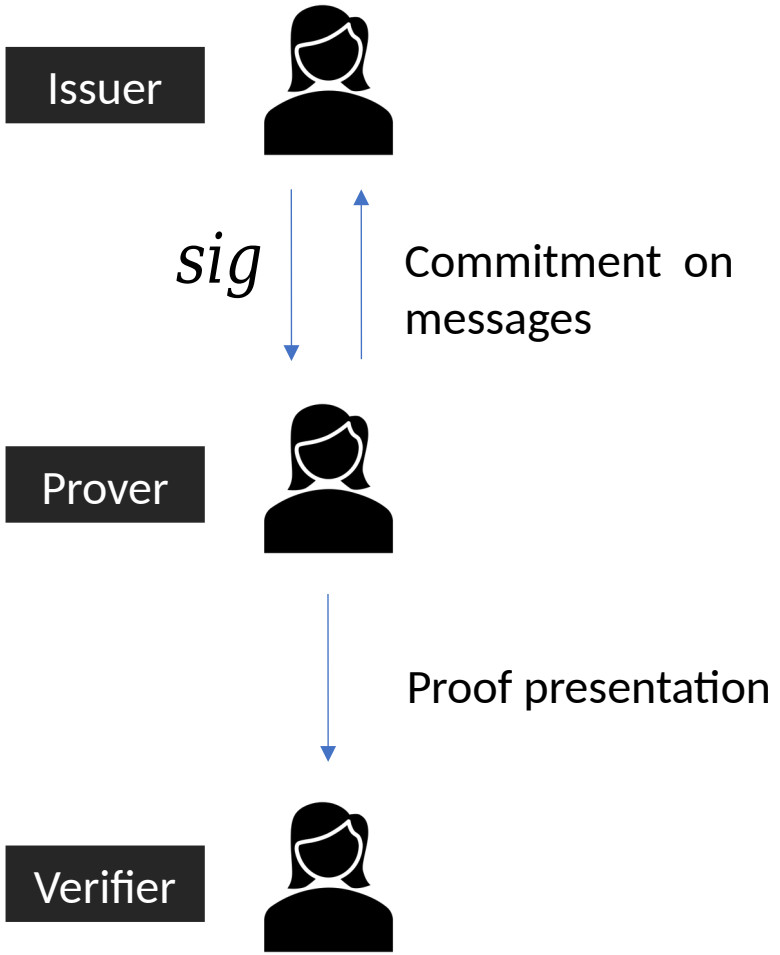


Blind BBS Signatures

BBS Blind Signatures



BBS Blind Signatures



- No “unblinding” needed. The first signed message becomes the commitments “blinding factor” (never disclosed).
- Used for User binding, hiding pseudonyms from the Issuer etc.
- The Verifier should not know if a messages is committed by the Prover or the Issuer.
- Better suited for a different document or should be merged with the “core” draft?

References

[ASM06] Au, M. H., Susilo, W., & Mu, Y. (2006). Constant-Size Dynamic k-TAA. In *Security and Cryptography for Networks: 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006. Proceedings 5* (pp. 111-125). Springer Berlin Heidelberg.

[CDL16] Camenisch, J., Drijvers, M., & Lehmann, A. (2016). Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited. In *Trust and Trustworthy Computing: 9th International Conference, TRUST 2016, Vienna, Austria, August 29-30, 2016, Proceedings 9* (pp. 1-20). Springer International Publishing.

[BBDT17] Barki, A., Brunet, S., Desmoulins, N., & Traoré, J. (2017). Improved Algebraic MACs and Practical Keyed-Verification Anonymous Credentials. In *Selected Areas in Cryptography–SAC 2016: 23rd International Conference, St. John's, NL, Canada, August 10-12, 2016, Revised Selected Papers 23* (pp. 360-380). Springer International Publishing.

[VB22] Vitto, G., & Biryukov, A. (2022). Dynamic Universal Accumulator with Batch Update over Bilinear Groups. In *Cryptographers' Track at the RSA Conference* (pp. 395-426). Cham: Springer International Publishing.

[TZ23] Tessaro, S., & Zhu, C. (2023). Revisiting BBS Signatures. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 691-721). Cham: Springer Nature Switzerland.

[BBS CFRG Draft] Looker, T., Kalos, V., Whitehead, A., & Lodder, M. (2022). The BBS Signature Scheme. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/>

[Editors Draft] Looker, T., Kalos, V., Whitehead, A., & Lodder, M. (2022). The BBS Signature Scheme. Decentralised Identity Foundation. <https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html>

Thank you!

Questions?