The BBS Signature Scheme

BBS Signatures

What are BBS Signatures??

With a few words…

A digital signature scheme supporting:

BBS Signatures

What are BBS Signatures??

With a few words…

A digital signature scheme supporting:

- Selective Disclosure (multi-message signing)

BBS Signatures

What are BBS Signatures??

With a few words…

A digital signature scheme supporting:

- Selective Disclosure (multi-message signing)
- Proof of possession enabled

BBS Signatures

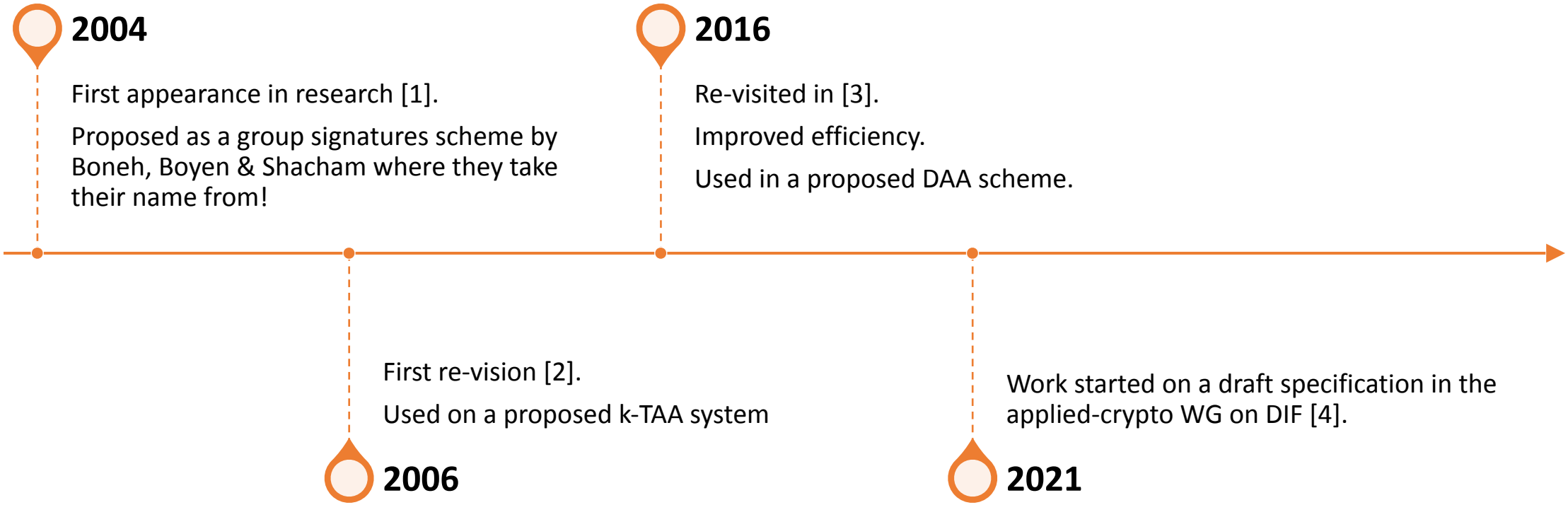
What are BBS Signatures??

With a few words…

A digital signature scheme supporting:

- Selective Disclosure (multi-message signing)
- Proof of possession enabled
- Unlinkable proofs (via a ZKP protocol)

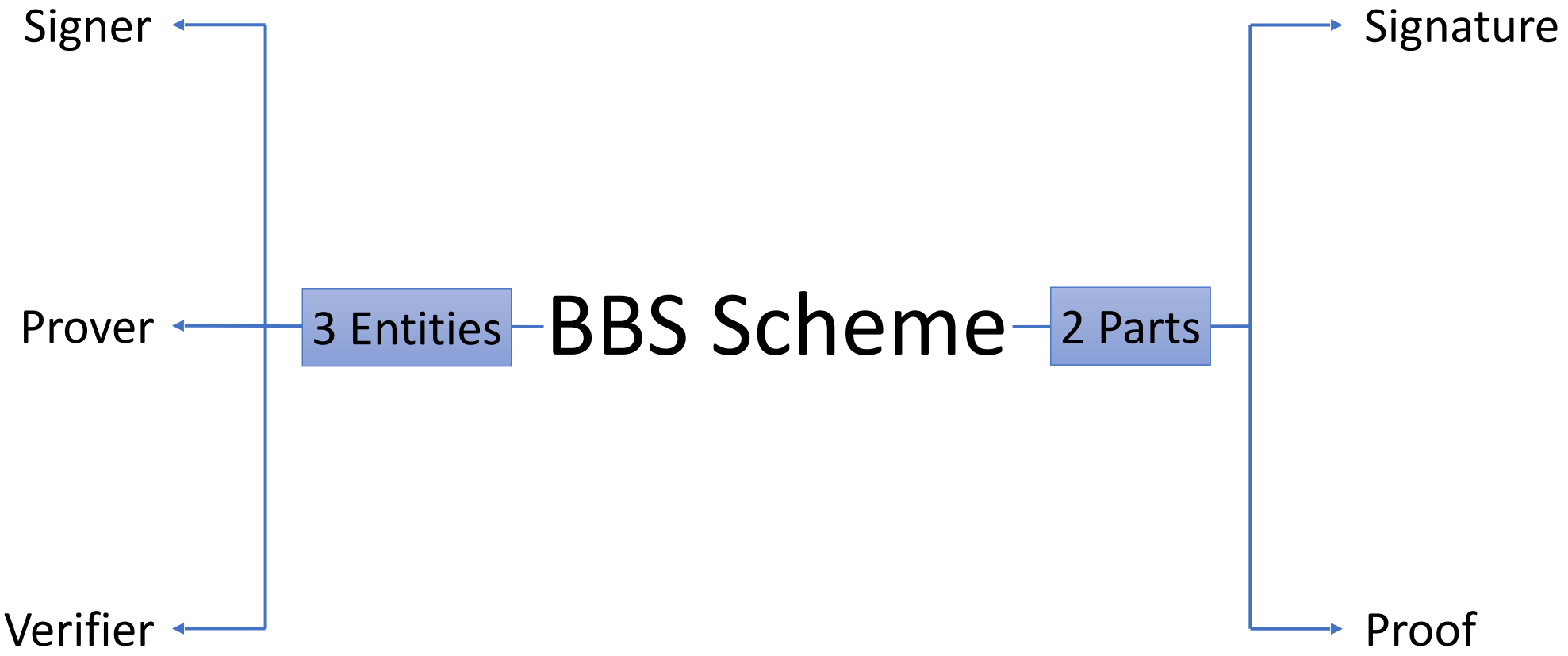
The BBS Main Timeline



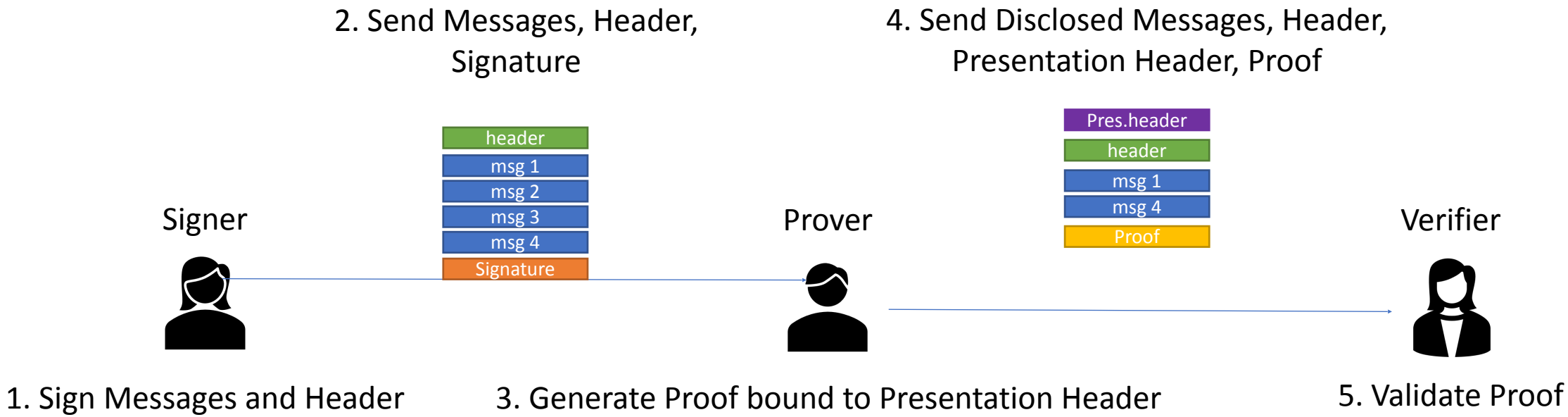
BBS Scheme

Key Information

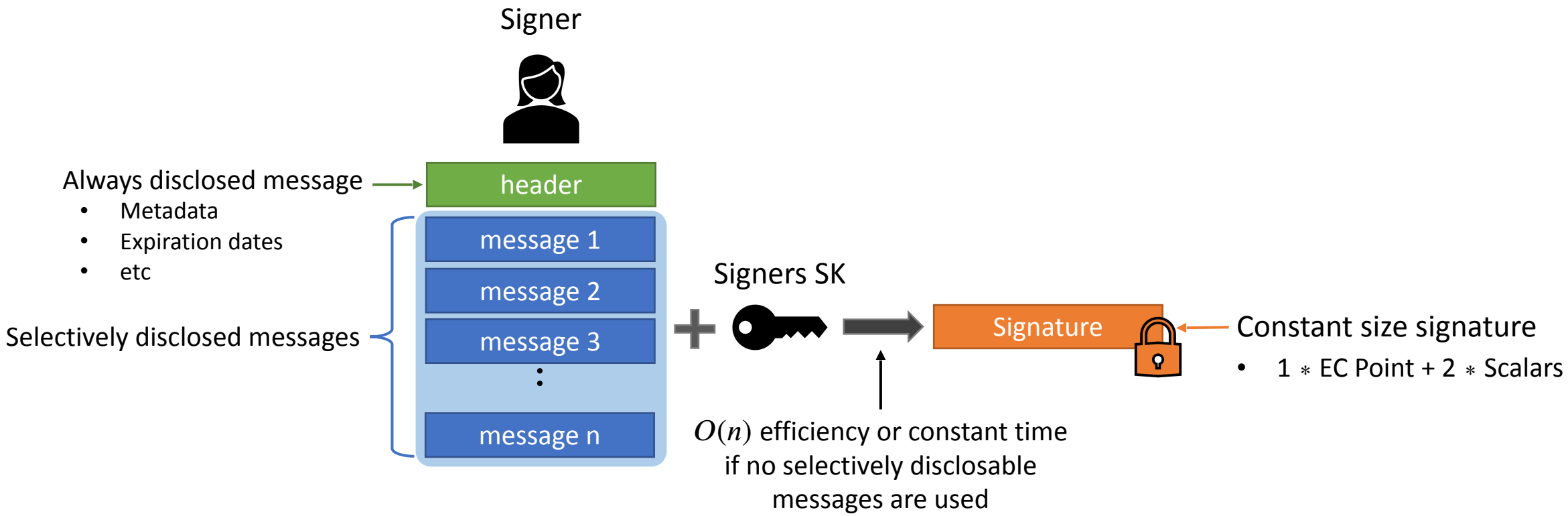
- Pairing based (using type-3 pairings).
- Uses two subgroups G1 and G2, of (known) prime order.
- Current ciphersuite based on the BLS12-381 curves (but any pairing-friendly curve will do).


Signer
Prover
Verifier
3 Entities
BBS Scheme
2 Parts
Signature
Proof

BBS Scheme

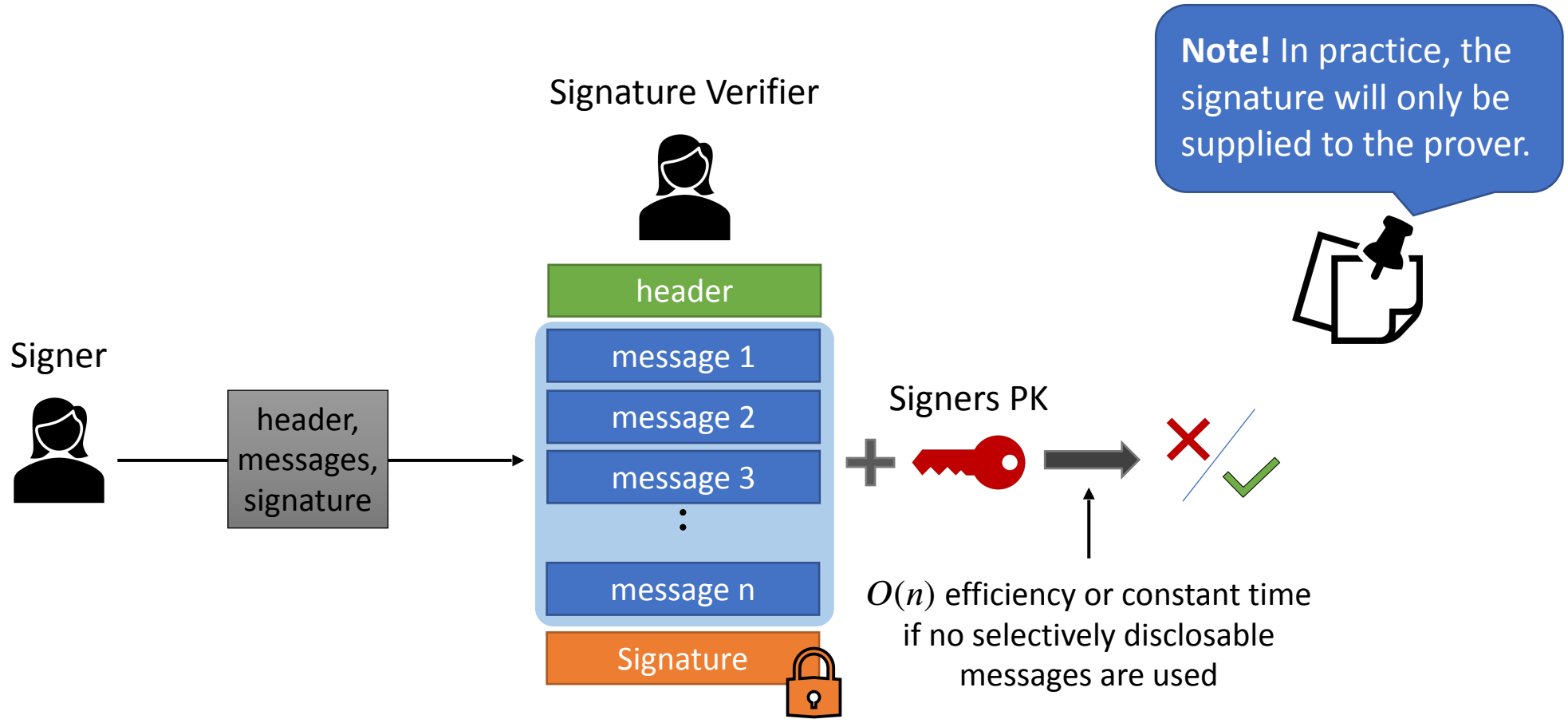

2. Send Messages, Header, Signature
4. Send Disclosed Messages, Header, Presentation Header, Proof
header
msg 1
msg 2
msg 3
msg 4
Signature
Pres.header
header
msg 1
msg 4
Proof
Signer
Prover
Verifier
1. Sign Messages and Header
3. Generate Proof bound to Presentation Header
5. Validate Proof

BBS Signature - Sign

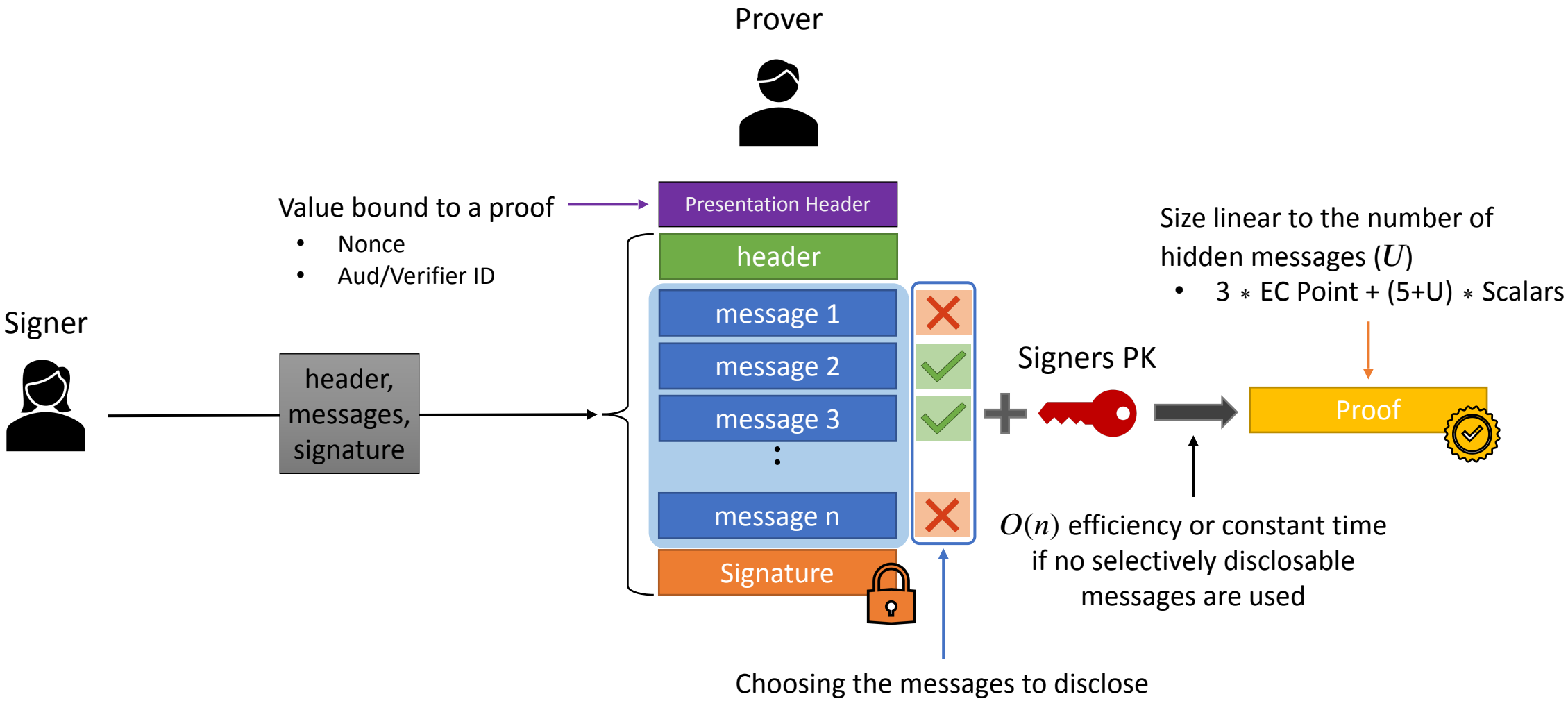


Note: You can generate a signature with either one or both the header and selectively disclosable messages!

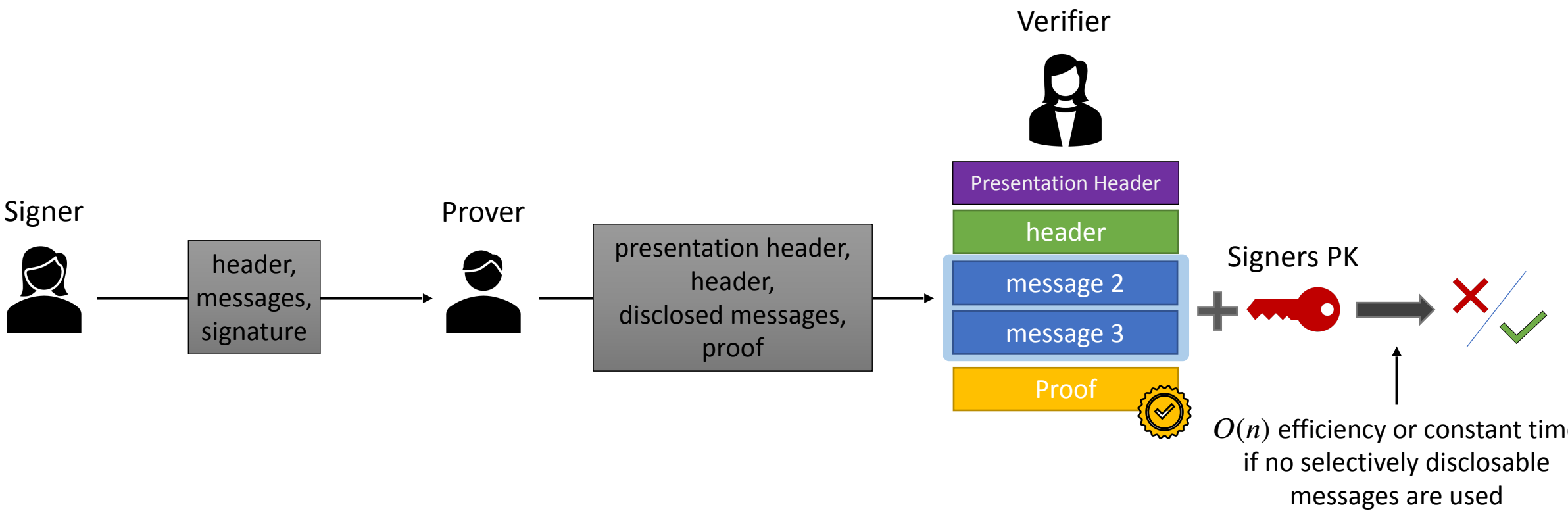
BBS Signature - Verify



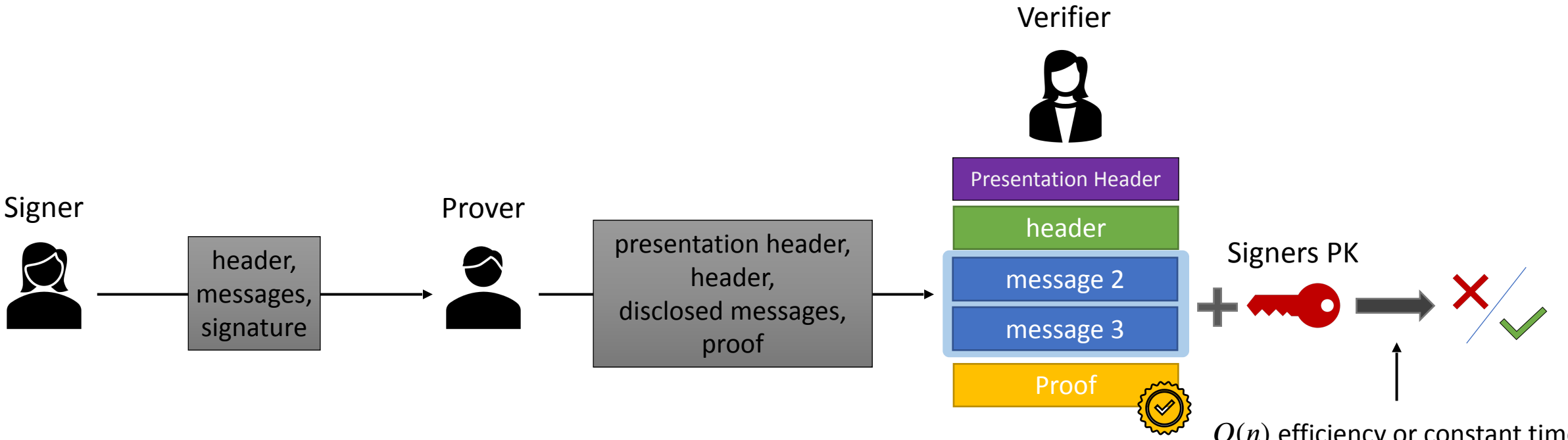
BBS Proof - Generate Proof



BBS Proof - Verify Proof



BBS Proof - Verify Proof

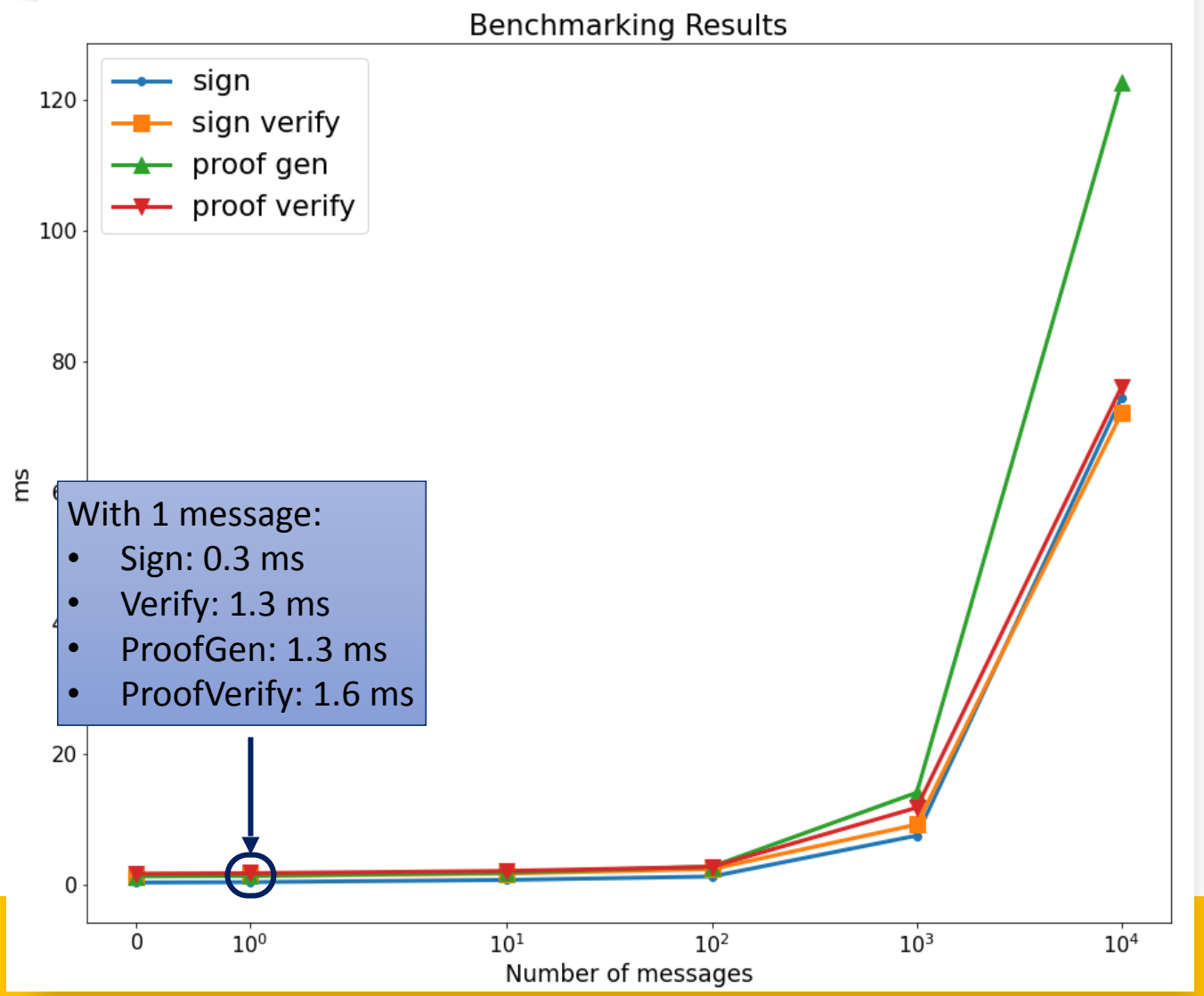


What does Proof provide??

- Proves **integrity/authenticity** of the **revealed messages**.
- Proves **possession** of a **signature**.
- **Un-linkable** Proof.

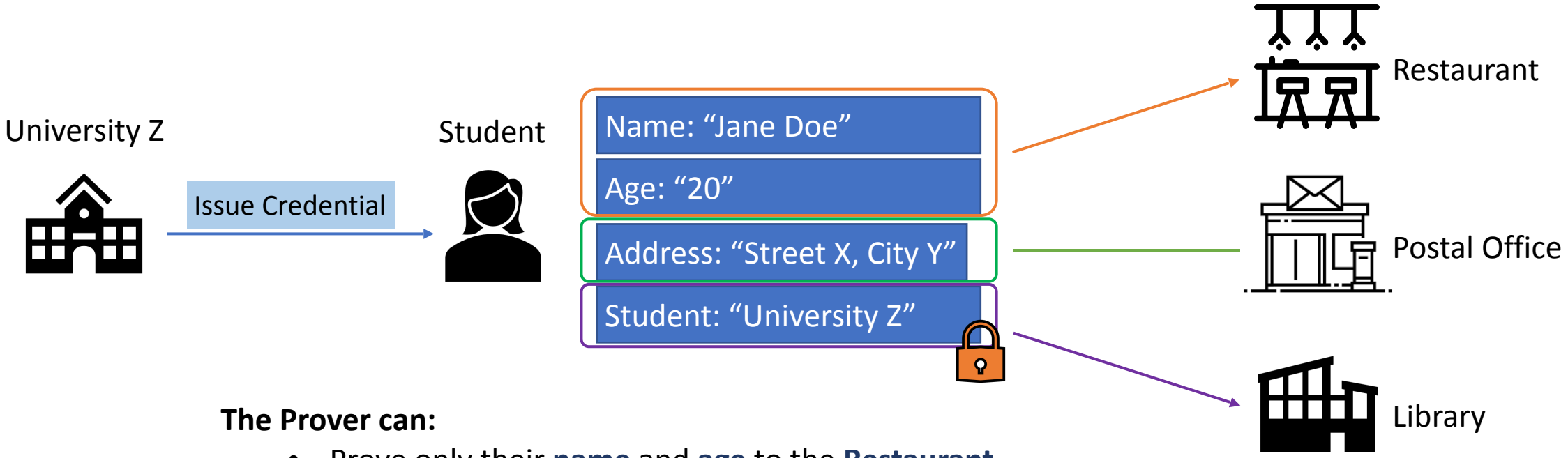
Benchmarks

- 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



Use Cases

Privacy Preserving Anonymous Credentials



The Prover can:

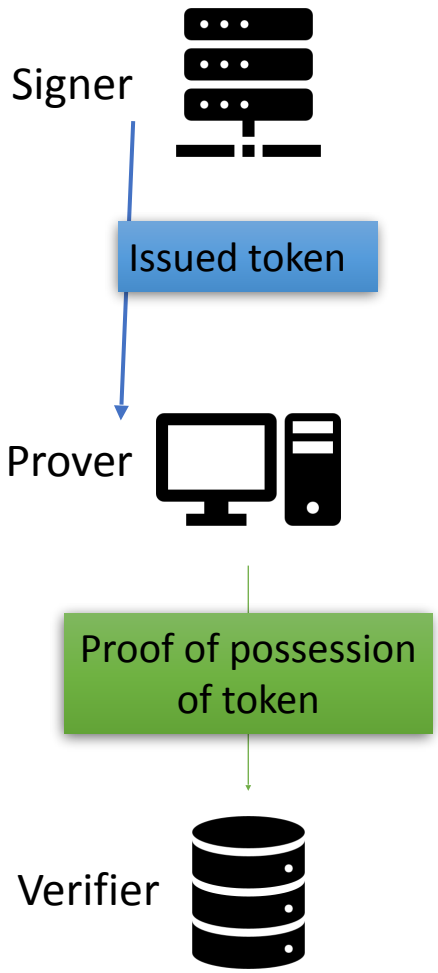
- Prove only their **name** and **age** to the **Restaurant**
- Prove only their **address** to the **Postal Office**.
- Prove only that they **are a student** to the **Library**.

➢ Only send the information that is relative to each Verifier

➢ The Verifiers cannot conspire to discover more information

(each proof is indistinguishable from random)

Proof of Possession enabled Security / Access Tokens



From the signers perspective:

- They can issue a single token that can be used multiple times by the prover.
- Does not require key material supplied by the prover ahead of time to issue.

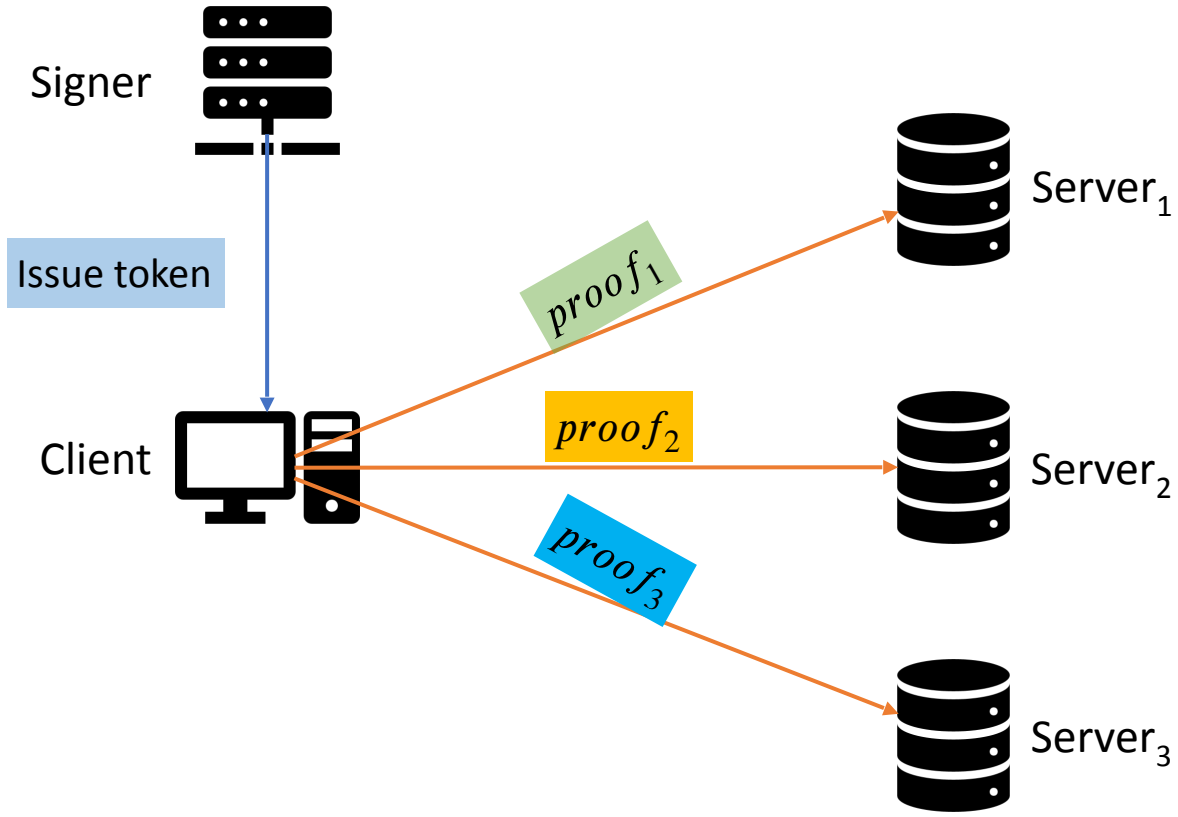
From the provers perspective:

- Can prover possession of the security token multiple times to different parties (verifiers).
- Does not require the prover to manage key material.
- Can scope generated proofs via the presentation header (e.g a generated proof is only valid for a particular verifier or has a TTL etc).

From the verifiers perspective:

- Validates the proof back to the original signer in a way that is inline with existing security tokens (e.g via the signers PK), also provides replay attack detection

Non-Correlating Security Token Proofs



During Proof Presentation:

- Each proof **cannot be correlated** to each other, the token or the client.
- Uncorrelatability holds even against **coalition between RPs** or **RPs and AS**.
- A unique **presentation header is NOT required** for un-correlatability to hold.

Why do this work in the CFRG?

- Fits with numerous existing work items already at the CFRG:
  - Pairing Friendly Curves (including the curve we are using BLS12-381)
  - BLS Signatures
  - Hash to Curve

Call to Action

- Calling for adoption of draft
- We believe it is sufficiently evolved to describe the scheme, however it is incomplete with several outstanding issues to address such as
  - Broader review of the schemes security properties
  - Cipher Suite definition refinement
  - Clarify the extensibility points

Conclusion

- BBS Signatures is an efficient multi messages digital signature supporting **selective disclosure** and **zero-knowledge proofs.**
- It has a **long line of research** backing it up, proving it security properties and improving its efficiency
- There are **multiple use cases** in which that BBS Signatures can be applied
- Current ciphersuite is based on BLS12-381 curves and xof hash functions (shake256) however**, any pairing friendly curve** and **any hash function** can be used
- BBS Signatures are **extendable** to: blind signatures, range proofs, bound signatures

Thank You!!

References

[1] Boneh, D., Boyen, X., & Shacham, H. (2004, August). Short Group Signatures. In Annual International Cryptology Conference (pp. 41-55). Springer, Berlin, Heidelberg.

[2] Au, M. H., Susilo, W., & Mu, Y. (2006, September). Constant-size Dynamic k-TAA. In *International Conference on Security and Cryptography for Networks* (pp. 111-125). Springer, Berlin, Heidelberg.

[3] Camenisch, J., Drijvers, M., & Lehmann, A. (2016, August). Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited. In *International Conference on Trust and Trustworthy Computing* (pp. 1-20). Springer, Cham.

[4] Whitehead, A., Lodder, M., Looker, T., Kalos, V. (2020, October). The BBS Signature Scheme. https://github.com/decentralized-identity/bbs-signature. In Decentralized Identity Foundation. Accessed: 04-06-2022

[5] Pippenger, N. (1980). On the Evaluation of Powers and Monomials. *SIAM Journal on Computing*, *9*(2), 230-250.