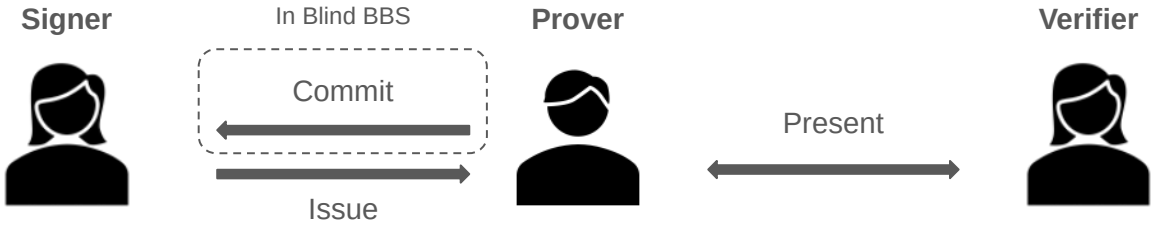
BBS Signature Suite Update

BBS Core, Blind Signing and Pseudonyms

Vasilis Kalos and Greg Bernstein

BBS Core and Blind



Signs an ordered set of messages (statements)

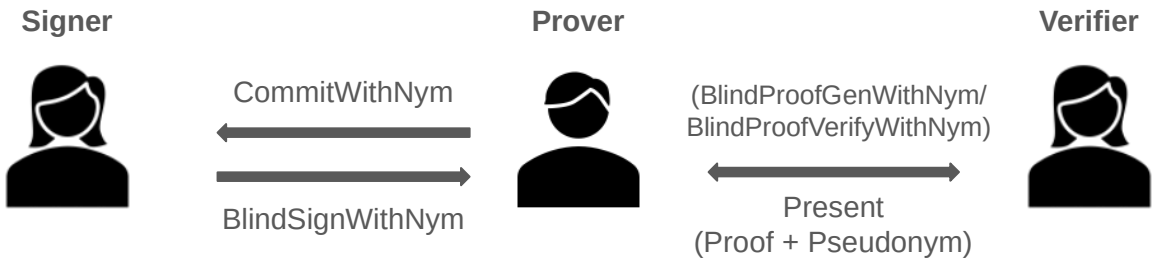
Chooses a subset of messages to disclose and provides a BBS proof.

Verifies disclosed messages against the BBS proof and signers **public** key

- Core BBS:
  - Updates from the crypto panel review - no breaking changes
  - Updates from implementers feedback (clearer test vectors representation, explanatory text etc)
- Blind BBS:
  - No updates

Pseudonyms

Pseudonym: Prover controlled linkability. A value bound to a signature, **constant in a context**, **unlinkable across contexts**



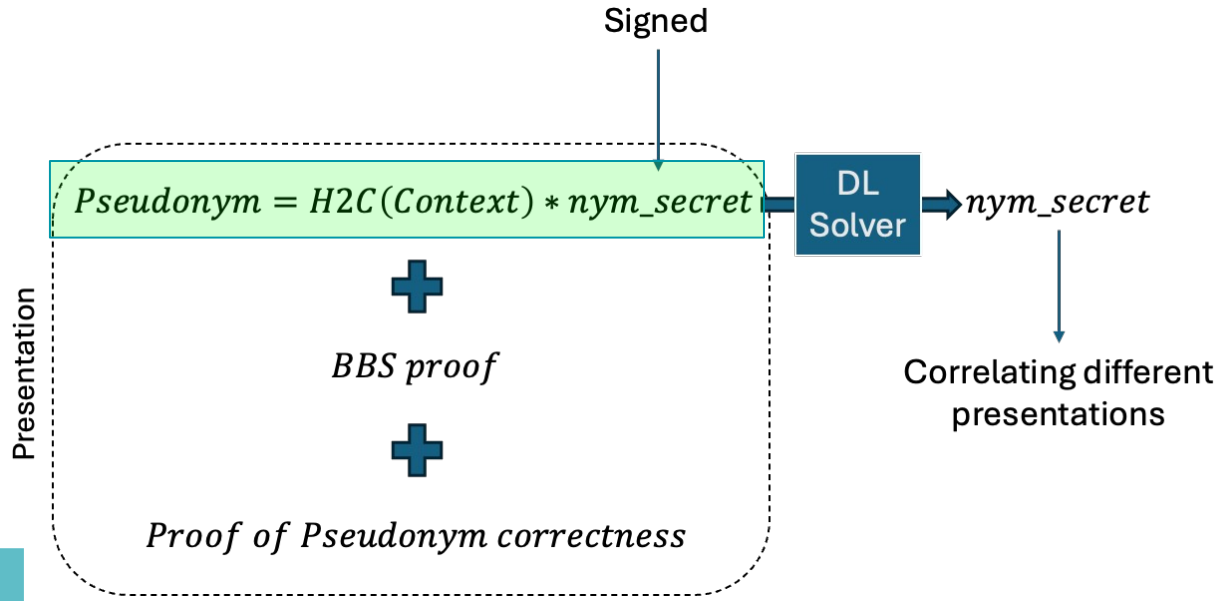
High Level Features

Provides for “controlled/limited” linkability when a **prover** revisits a **verifier** or group of verifiers while maintaining general unlinkability and untraceability.

Provides a general cryptographic pseudonym capability bound to a BBS signature. Such pseudonyms are also useful across multiple verifiers, e.g., “Personhood credentials”

BBS Pseudonyms

- **Core BBS**: Privacy secure against CRPQC
- **BBS Pseudonyms**: Presentations become linkable using a CRPQC



Goal: Secure Pseudonyms against "**store now, link later**" attacks

Proposal

$$Pseudonym = H2C(Context) * nym_secret$$

Use instead

$$Pseudonym = H2C(Context) * (s_0 + s_1 z + s_2 z^2 + \ldots + s_n z^n)$$

Polynomial $\boldsymbol{f}$ of degree $\boldsymbol{n}$, evaluated at $\boldsymbol{z = Hash(Context)}$

Coefficients $s_0, s_1, \ldots, s_n$ are signed

- ➔ Getting the DL of the Pseudonym ⟶ $f(z)$ for a Context-defined $\boldsymbol{z}$
- ➔ Can use the Pseudonym at $\boldsymbol{n}$ different Contexts

Proposal

$$Pseudonym = H2C(Context) * (s_0 + s_1 z + s_2 z^2 + \ ... + s_n z^n)$$

Advantages

- No new/advanced crypto
- Performant

Disadvantages

- Proof size increased by $32 * n$ bytes
- Extra logic to handle reaching maximum usages

Performance (ms) – 10 signed messages – Run on M1/MacBook Pro

	$n = 1$ (not PQ private)	$n = 100$	$n = 1000$	$n = 10000$
Proof Generation	1.9 ms	2.24 ms (~1.2 x increase)	9.2 ms (~4.8 x increase)	69.7 ms (~36 x increase)
Proof Verification	0.19 ms	0.21 ms (~1.1x increase)	0.23 ms (~1.2 x increase)	0.55 ms (~2.3 x increase)

Thank you!

Core BBS draft: https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/09/

Blind Signatures draft: https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-blind-signatures/01/

Pseudonyms draft: https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-per-verifier-linkability/01/

GitHub discussion on proposal

- Issue #10: https://github.com/cfrg/draft-irtf-cfrg-bbs-pseudonyms/issues/10
- Issue #12: https://github.com/cfrg/draft-irtf-cfrg-bbs-pseudonyms/issues/12
- PR #13: https://github.com/cfrg/draft-irtf-cfrg-bbs-pseudonyms/pull/13

Questions?