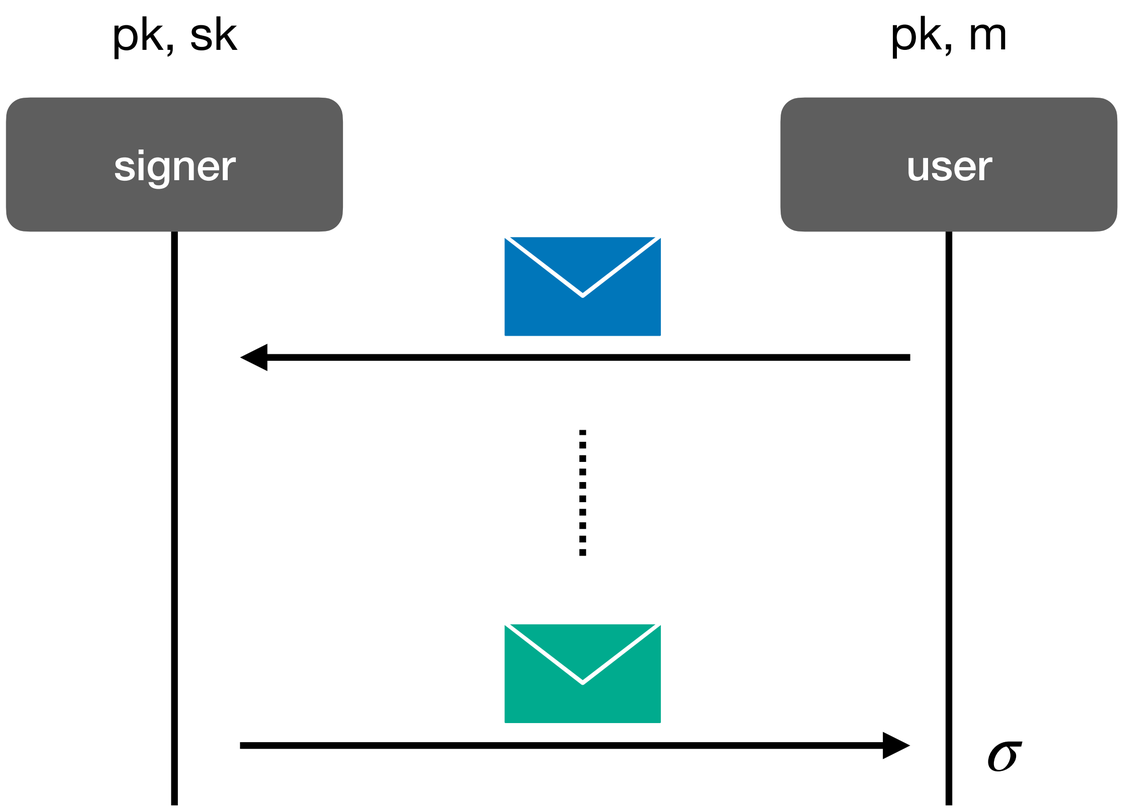
Practical Blind Signatures in Pairing-free Groups

- Michael Klooß — ETH Zurich
- Michael Reichle — ETH Zurich
- Benedikt Wagner — Ethereum Foundation

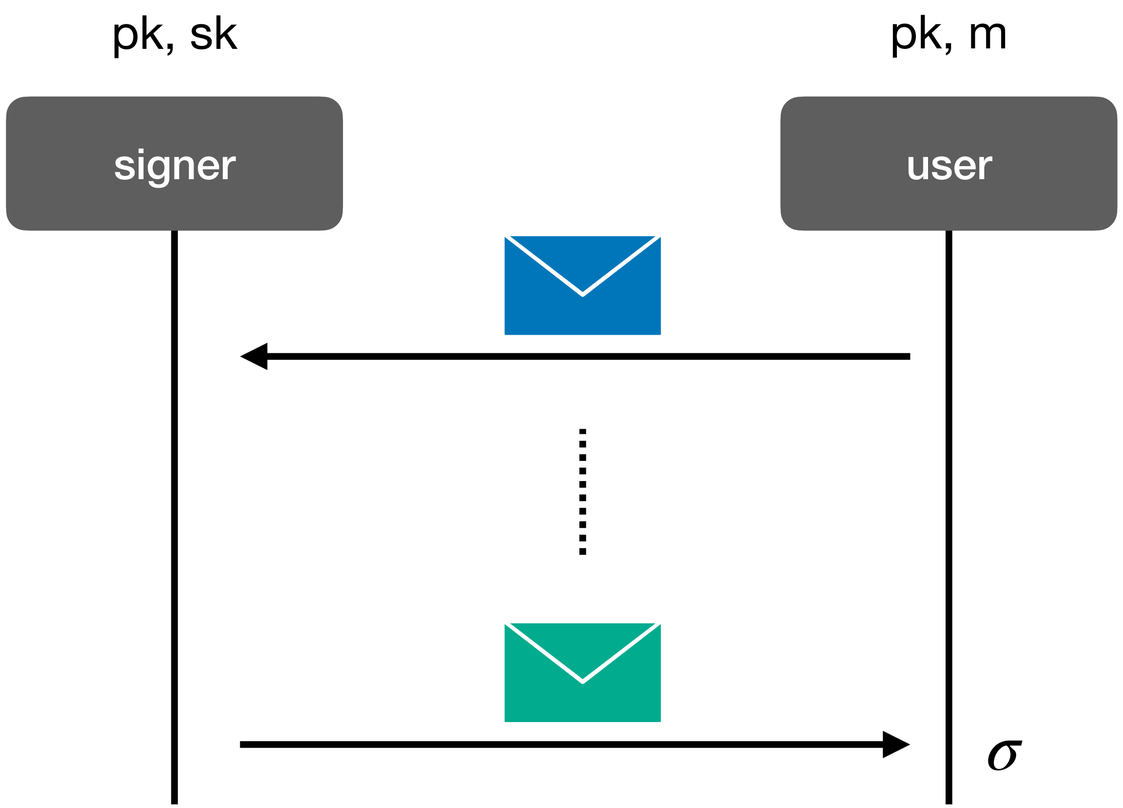
Blind Signatures



Correctness:

- honest signatures verify

Blind Signatures



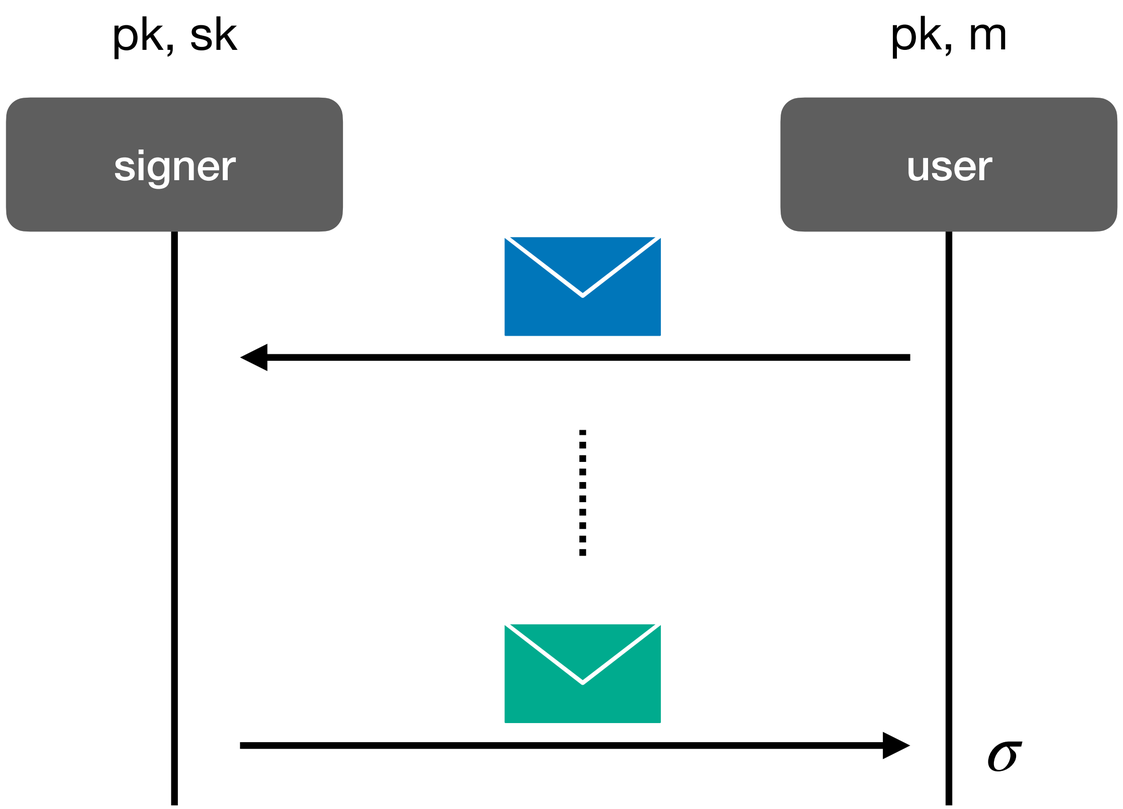
Correctness:

- honest signatures verify

Blindness:

- signatures are *unlinkable* to signing sessions

Blind Signatures



Correctness:

- honest signatures verify

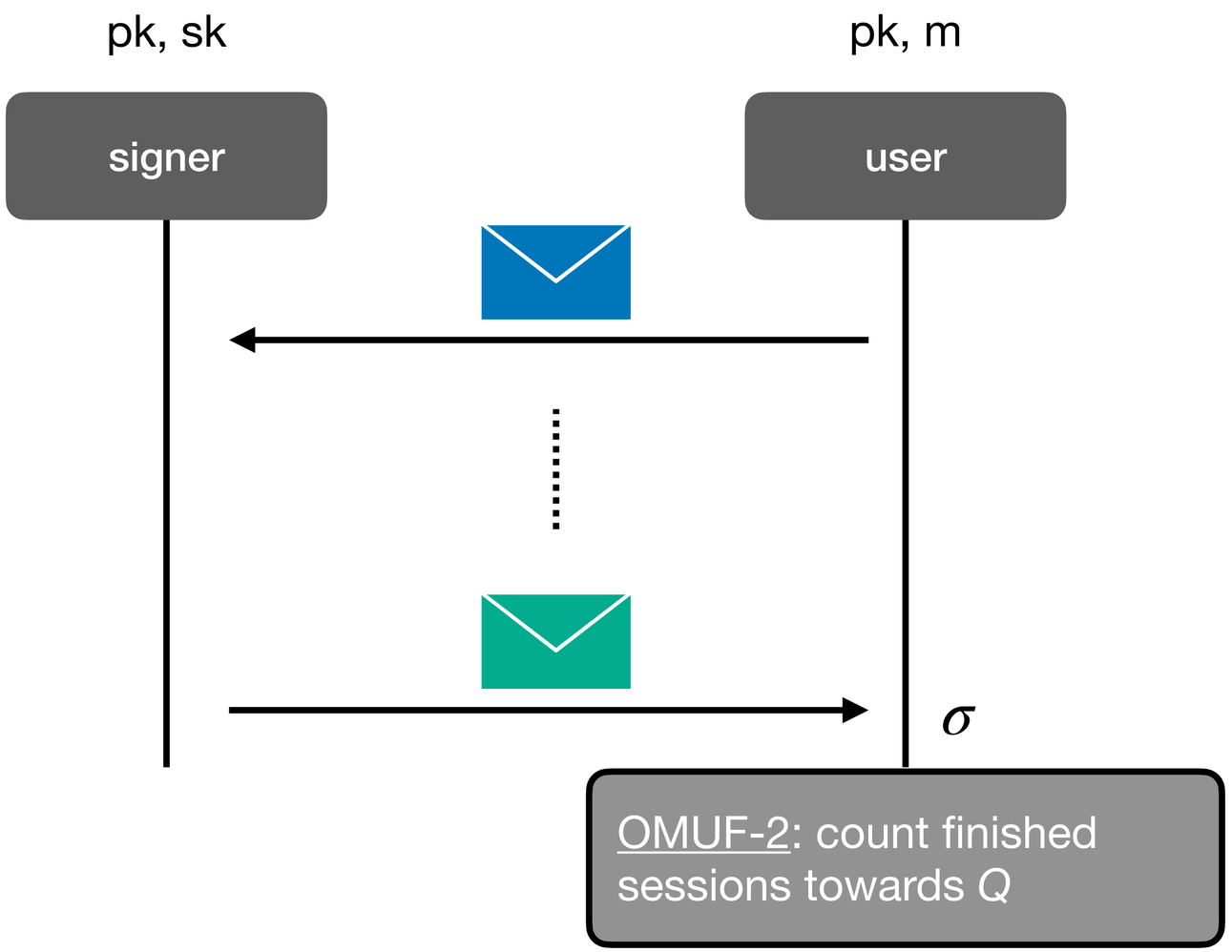
Blindness:

- signatures are *unlinkable* to signing sessions

One-more Unforgeability:

- user can obtain at most Q signatures from Q sessions with distinct messages

Blind Signatures



Correctness:

- honest signatures verify

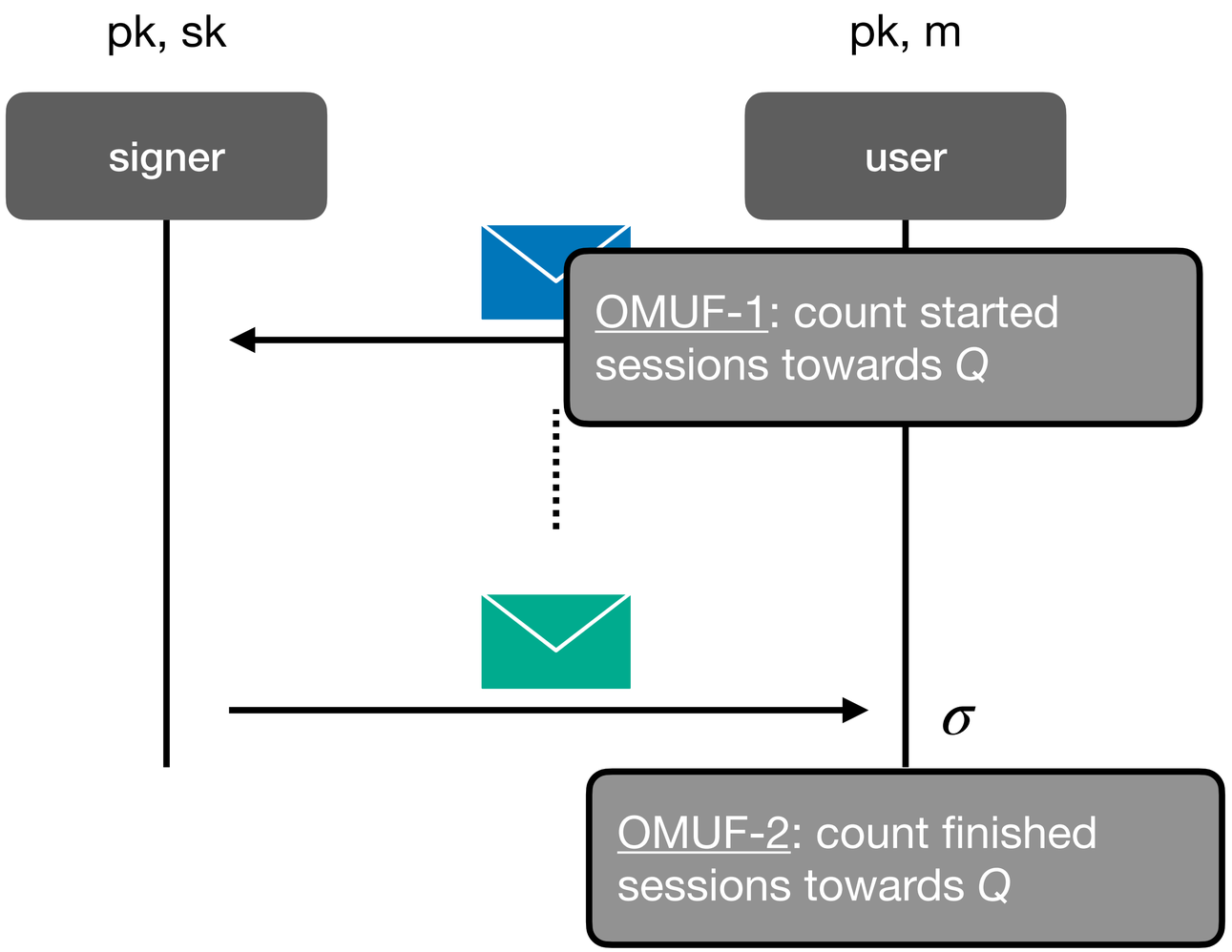
Blindness:

- signatures are *unlinkable* to signing sessions

One-more Unforgeability:

- user can obtain at most *Q* signatures from *Q* sessions with distinct messages

Blind Signatures



Correctness:

- honest signatures verify

Blindness:

- signatures are *unlinkable* to signing sessions

One-more Unforgeability:

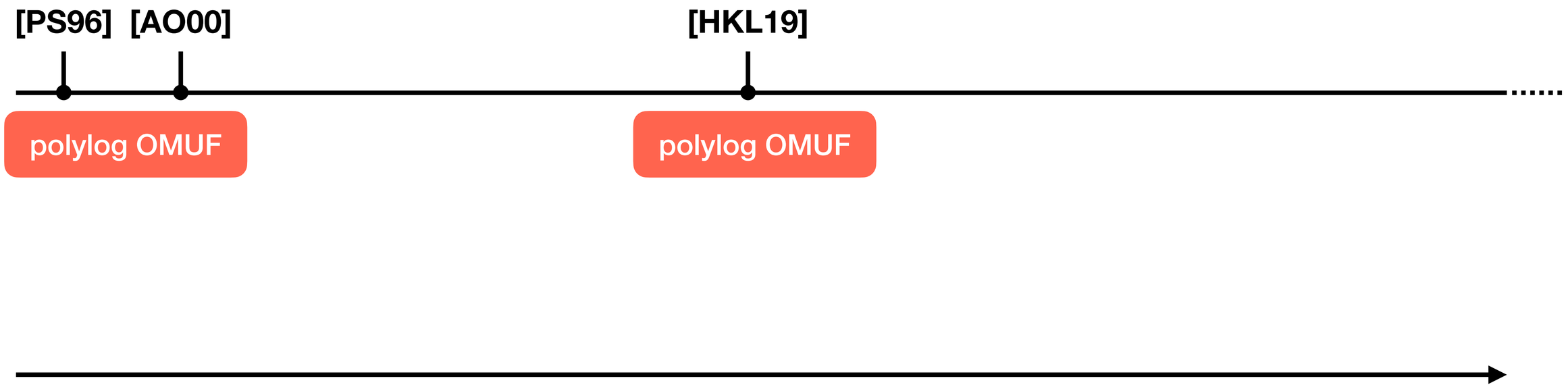
- user can obtain at most Q signatures from Q sessions with distinct messages

Blind Signatures in Pairing-free Curves

Selective Overview

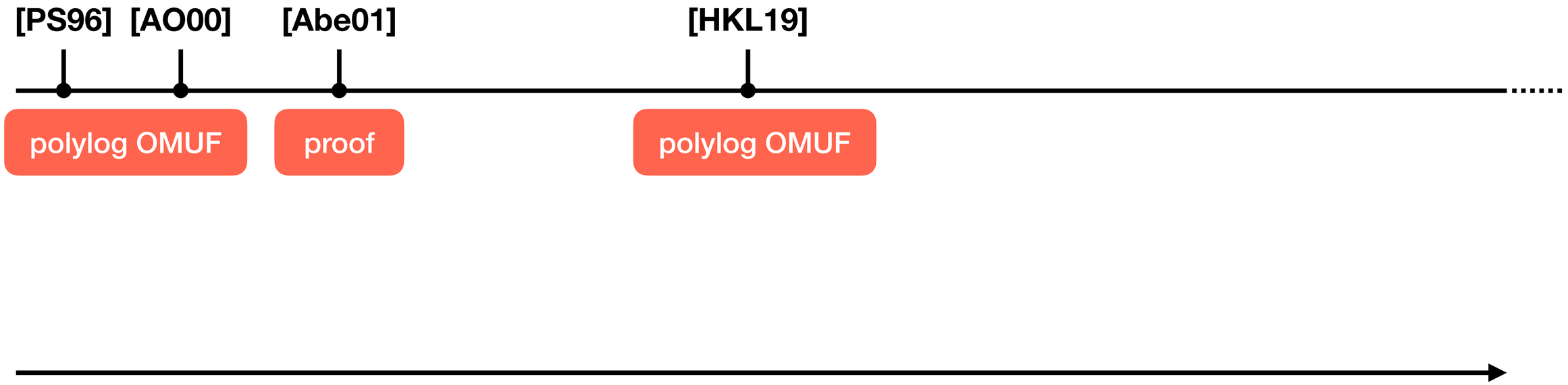
Blind Signatures in Pairing-free Curves

Selective Overview



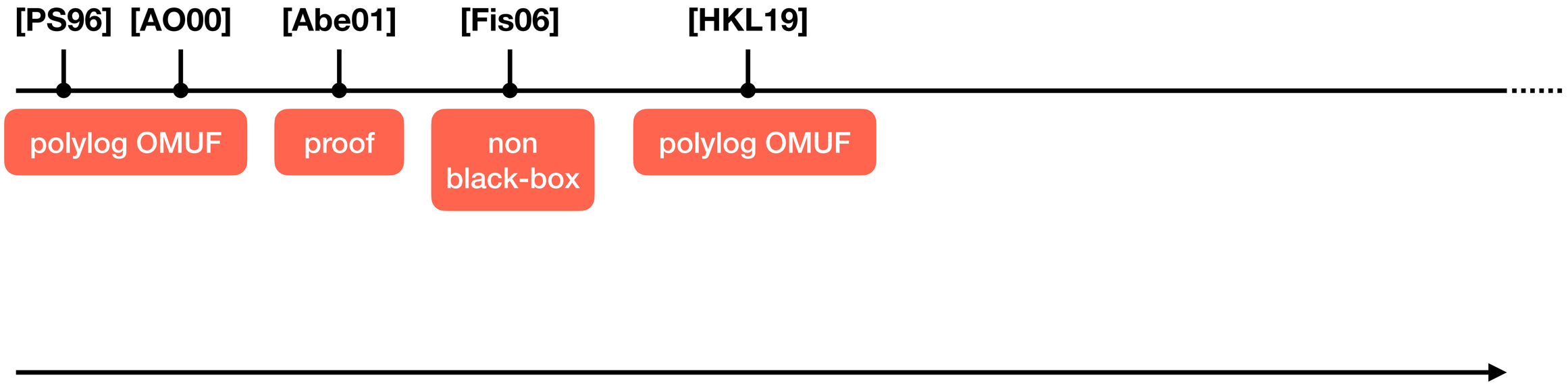
Blind Signatures in Pairing-free Curves

Selective Overview



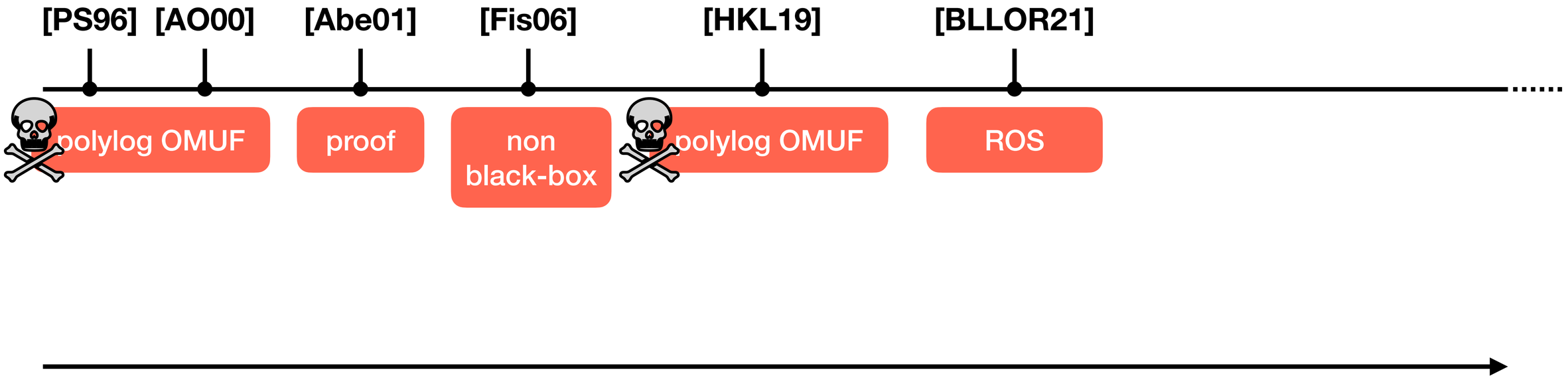
Blind Signatures in Pairing-free Curves

Selective Overview



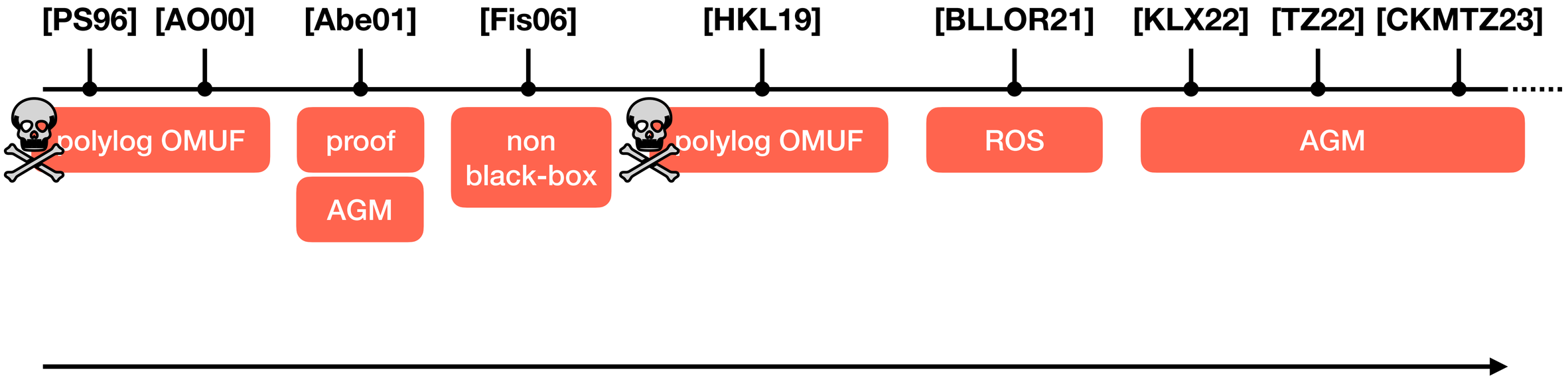
Blind Signatures in Pairing-free Curves

Selective Overview



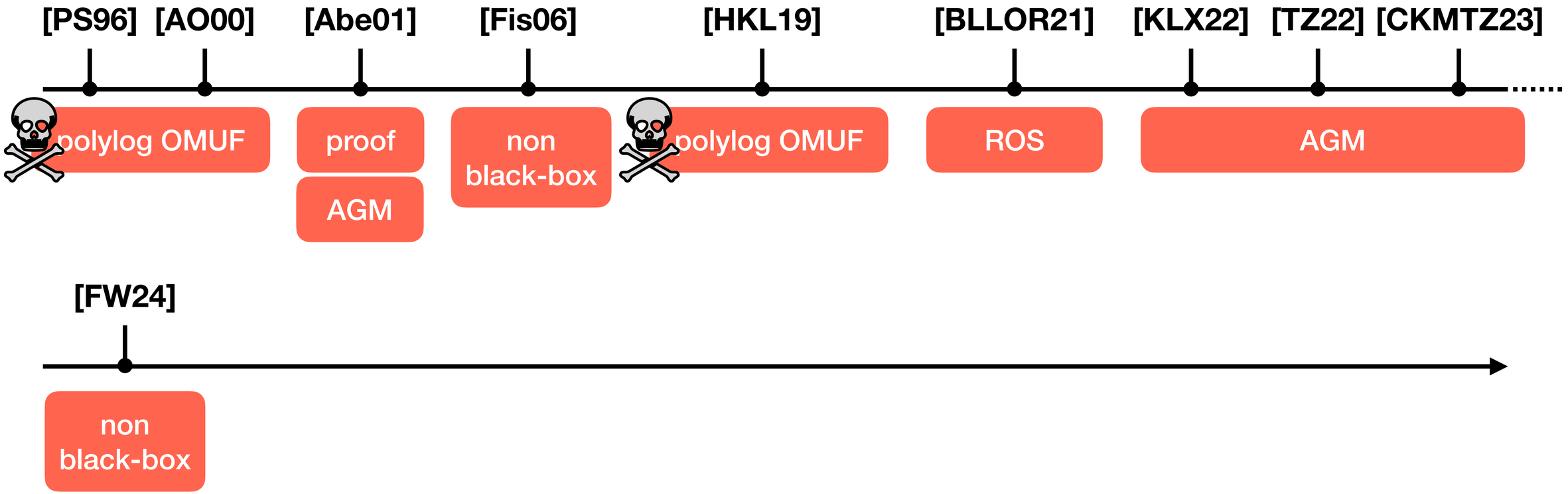
Blind Signatures in Pairing-free Curves

Selective Overview



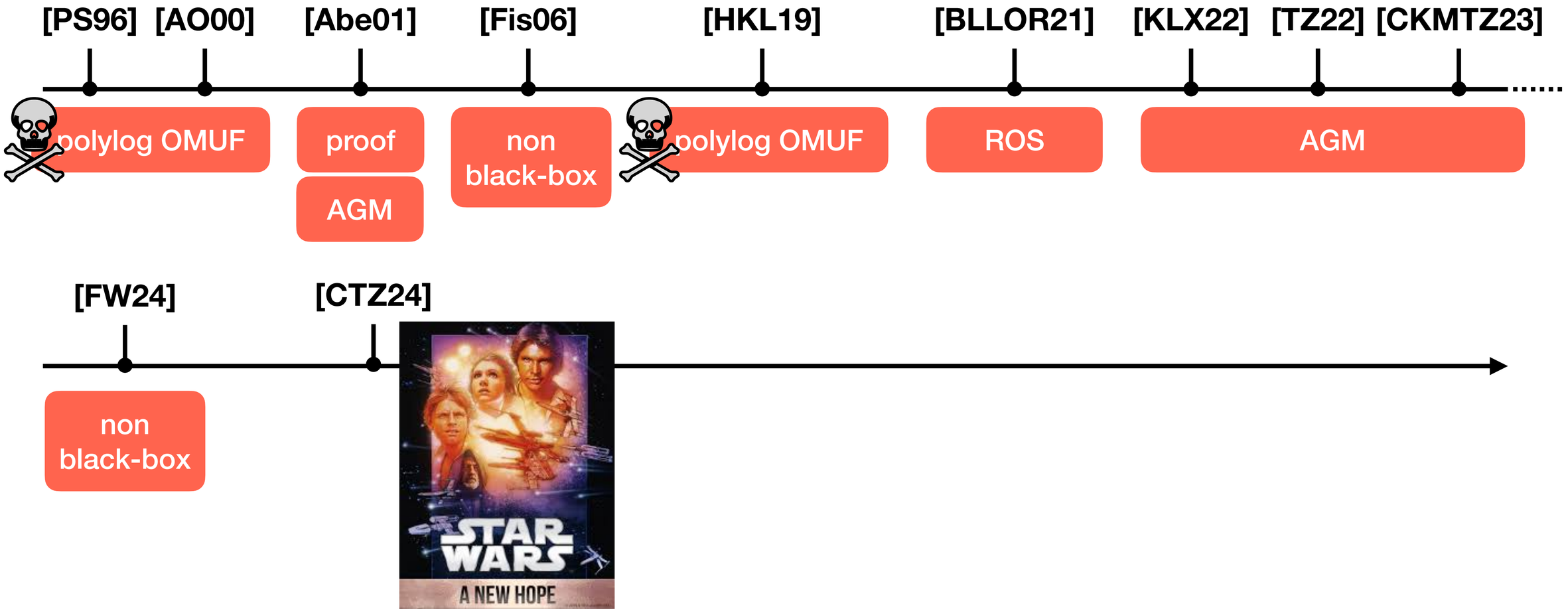
Blind Signatures in Pairing-free Curves

Selective Overview



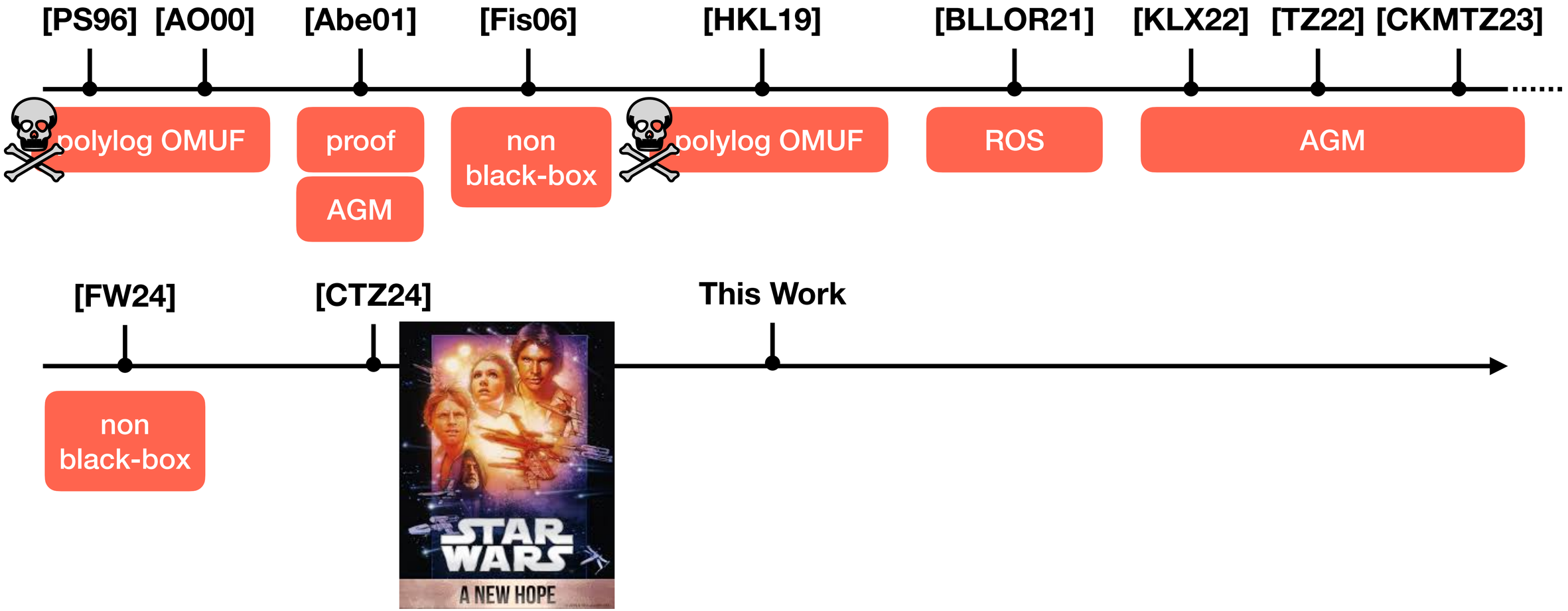
Blind Signatures in Pairing-free Curves

Selective Overview



Blind Signatures in Pairing-free Curves

Selective Overview



Efficiency

Pairing-free blind signature without the AGM

Scheme	Signature Size	Communication Size	Security	Assumption
BS_1 + BS_2 [CTZ24]	$1\mathbb{G} + 4\mathbb{Z}_p$	$5\mathbb{G} + 5\mathbb{Z}_p$	OMUF-1	OMCDH
BS_3 [CTZ24]	$\text{poly}(\lambda)$	$\text{poly}(\lambda)$	OMUF-2	CDH

Efficiency

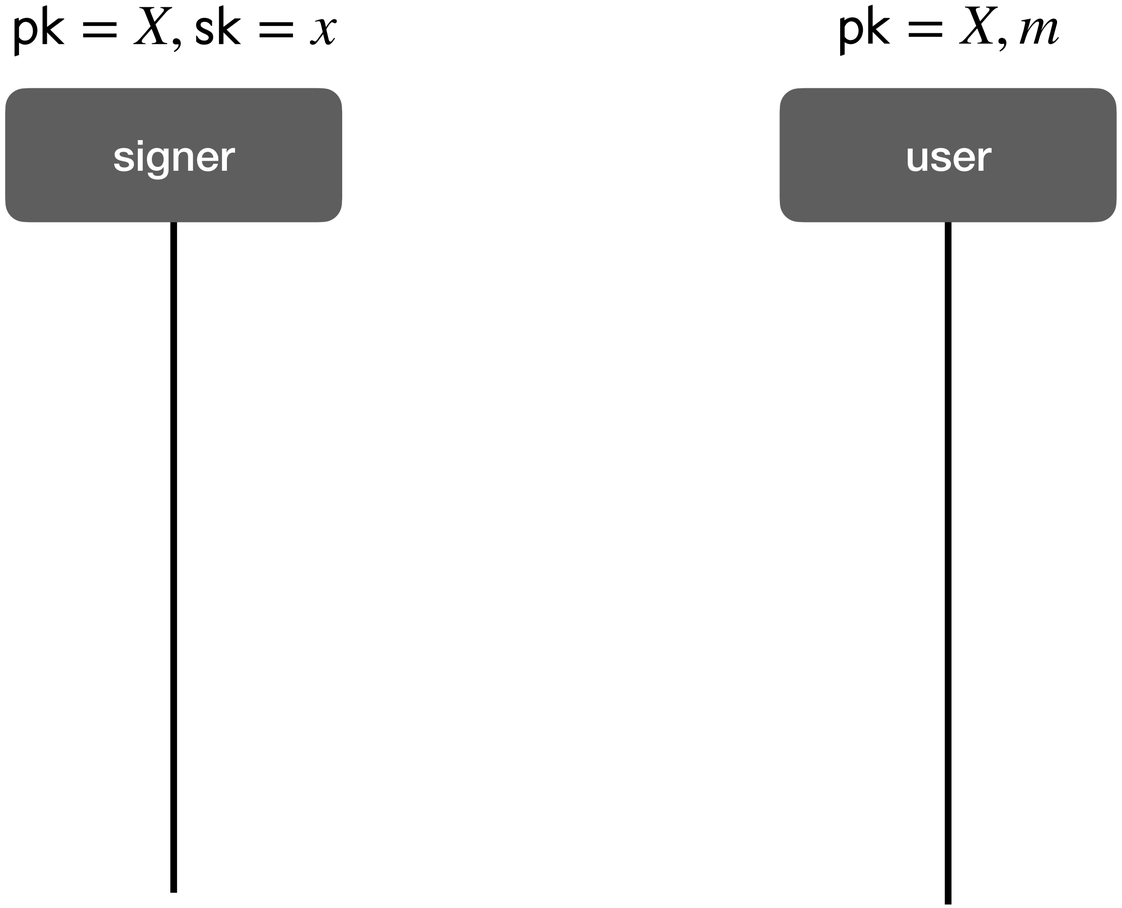
Pairing-free blind signature without the AGM

Scheme	Signature Size	Communication Size	Security	Assumption
BS_1 + BS_2 [CTZ24]	$1\mathbb{G} + 4\mathbb{Z}_p$	$5\mathbb{G} + 5\mathbb{Z}_p$	OMUF-1	OMCDH
BS_3 [CTZ24]	$\text{poly}(\lambda)$	$\text{poly}(\lambda)$	OMUF-2	CDH
Our Work	$2\mathbb{G} + 5\mathbb{Z}_p$	$\text{poly}(\lambda)$	OMUF-2	DDH

CTZ'24

High-level Overview

replace pairing-based verification of blind BLS via FS-compiled Σ-protocol



CTZ'24

High-level Overview

replace pairing-based verification of blind BLS via FS-compiled Σ-protocol

$S = xH(m)$

$\mathsf{pk} = X, \mathsf{sk} = x$

signer

$\mathsf{pk} = X, m$

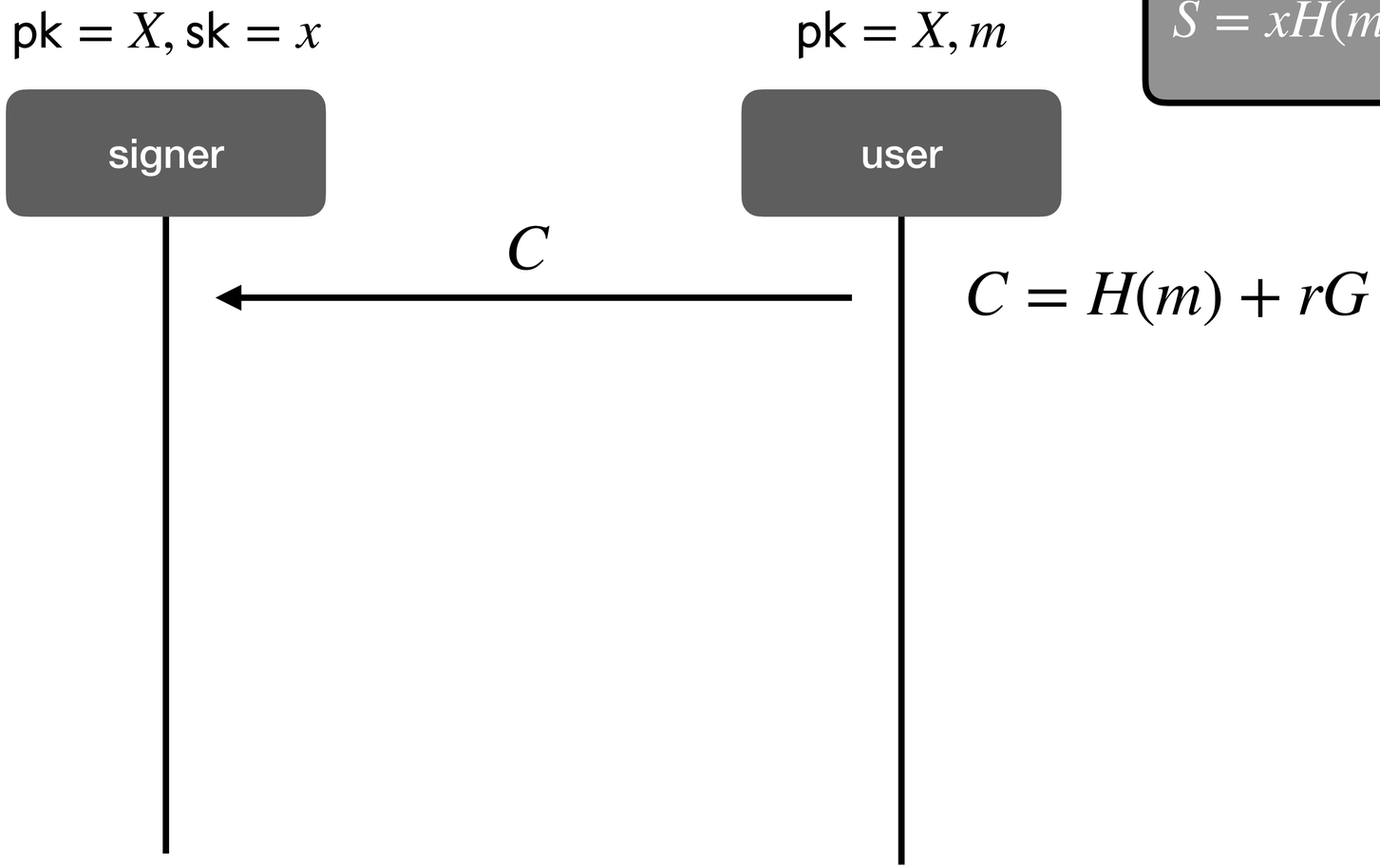
user

CTZ'24

High-level Overview

replace pairing-based verification of blind BLS via FS-compiled Σ-protocol

$S = xH(m)$

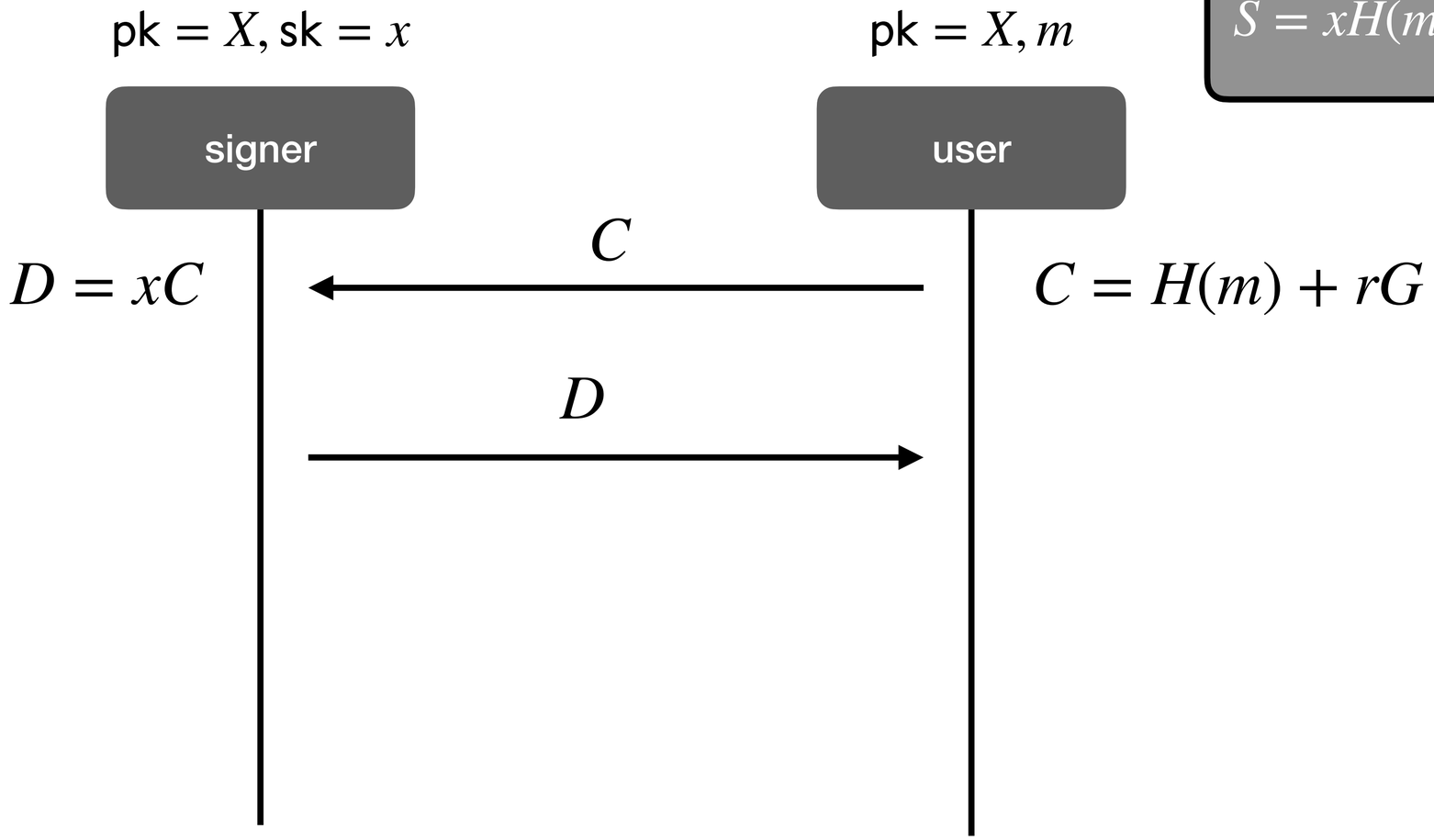


CTZ'24

High-level Overview

replace pairing-based verification of blind BLS via FS-compiled Σ-protocol

$S = xH(m)$

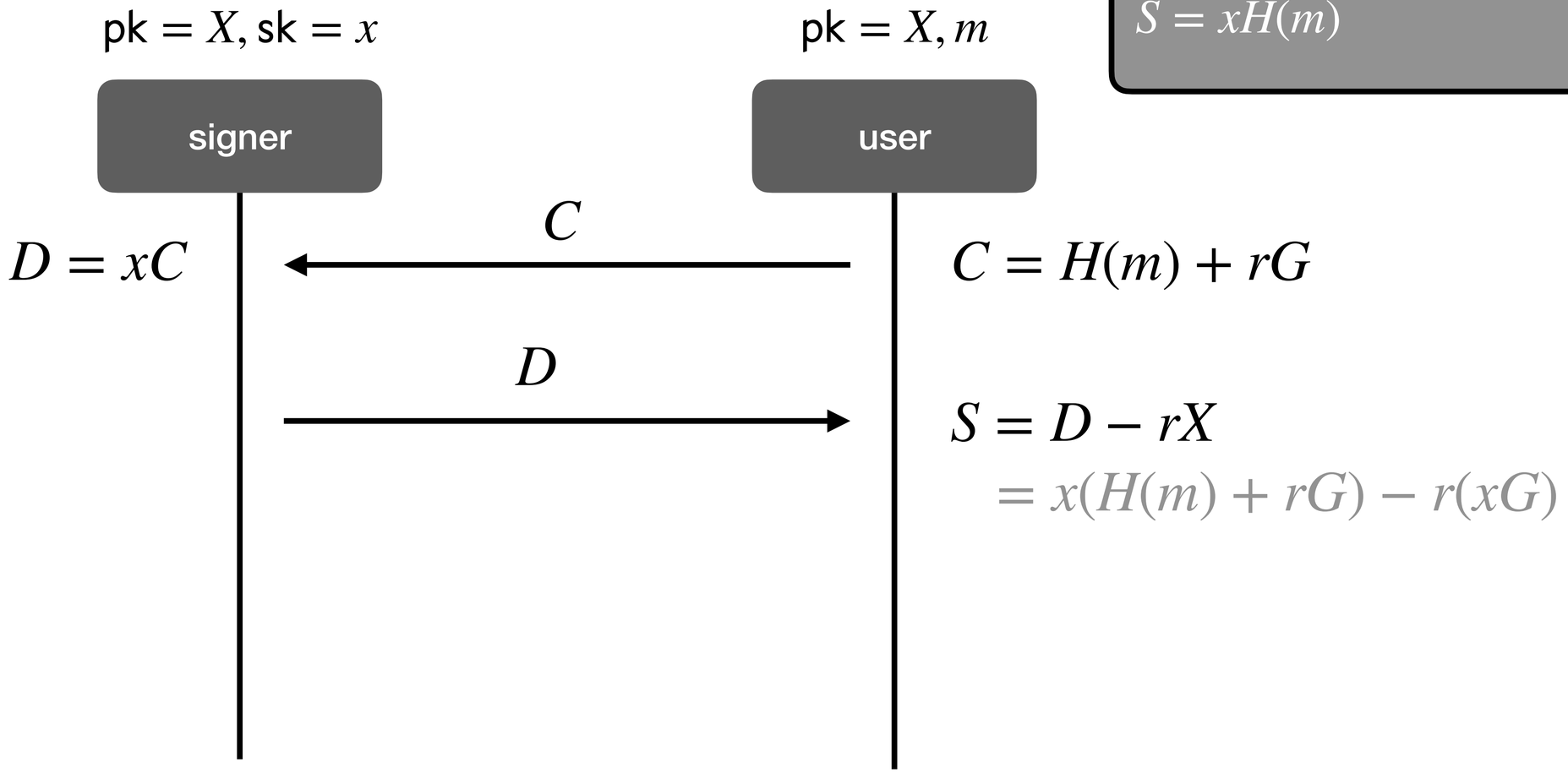


CTZ'24

High-level Overview

replace pairing-based verification of blind BLS via FS-compiled Σ-protocol

$S = xH(m)$

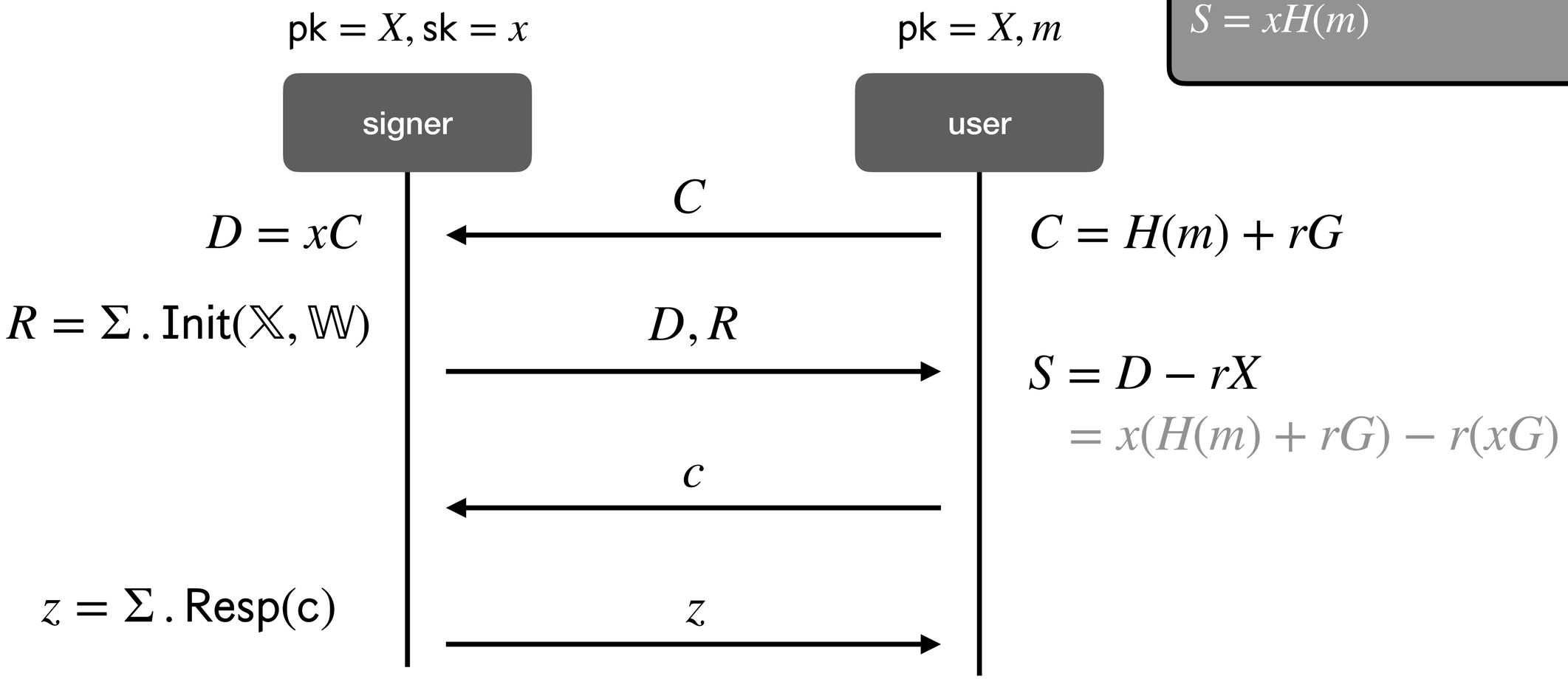


CTZ'24

High-level Overview

replace pairing-based verification of blind BLS via FS-compiled Σ-protocol

$S = xH(m)$

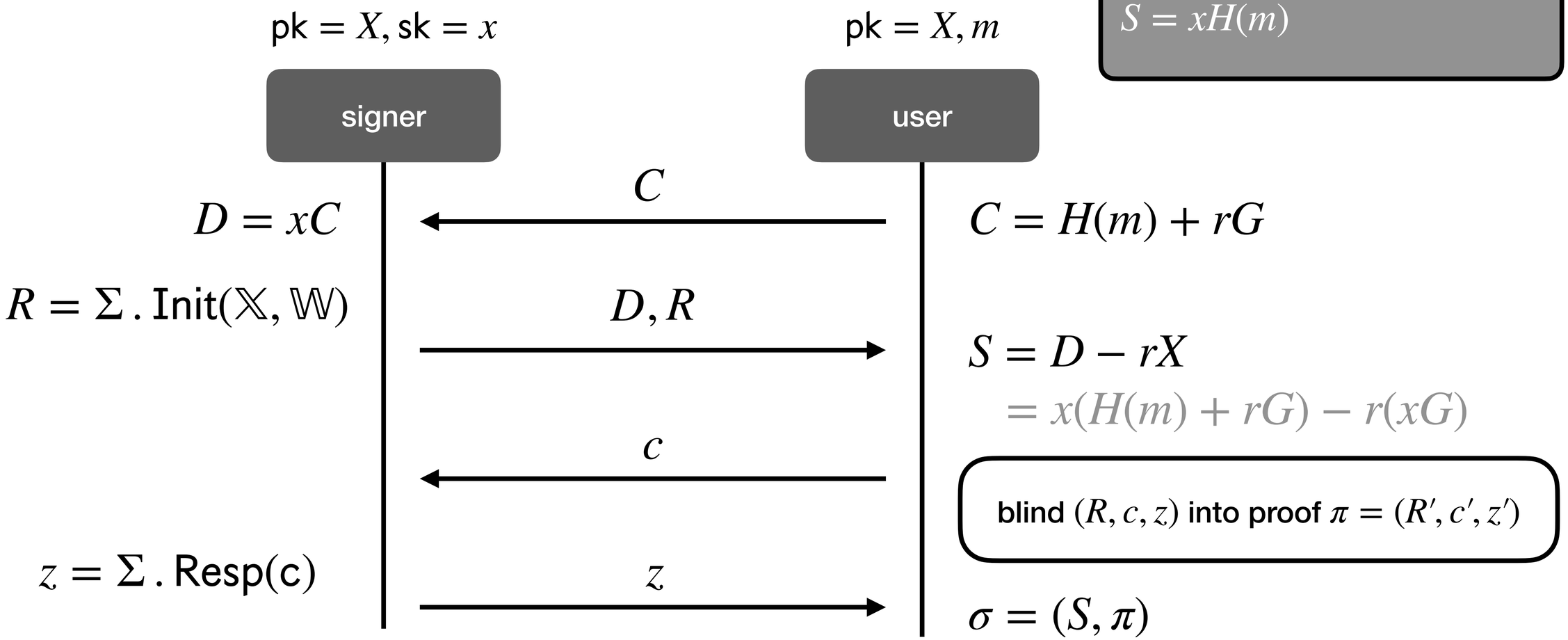


CTZ'24

High-level Overview

replace pairing-based verification of blind BLS via FS-compiled Σ-protocol

$S = xH(m)$



Our Approach

replace pairing-based verification of **[KRS23]** via FS-compiled Σ-protocol

$\mathsf{pk} = (U, V, H), \mathsf{sk} = u$

signer

$\mathsf{pk} = (U, V, H), m$

user

Our Approach

replace pairing-based verification of **[KRS23]** via FS-compiled Σ-protocol

$S_1 = uV + s(H(m)U + H)$
$S_2 = sG$

$\mathsf{pk} = (U, V, H), \mathsf{sk} = u$

signer

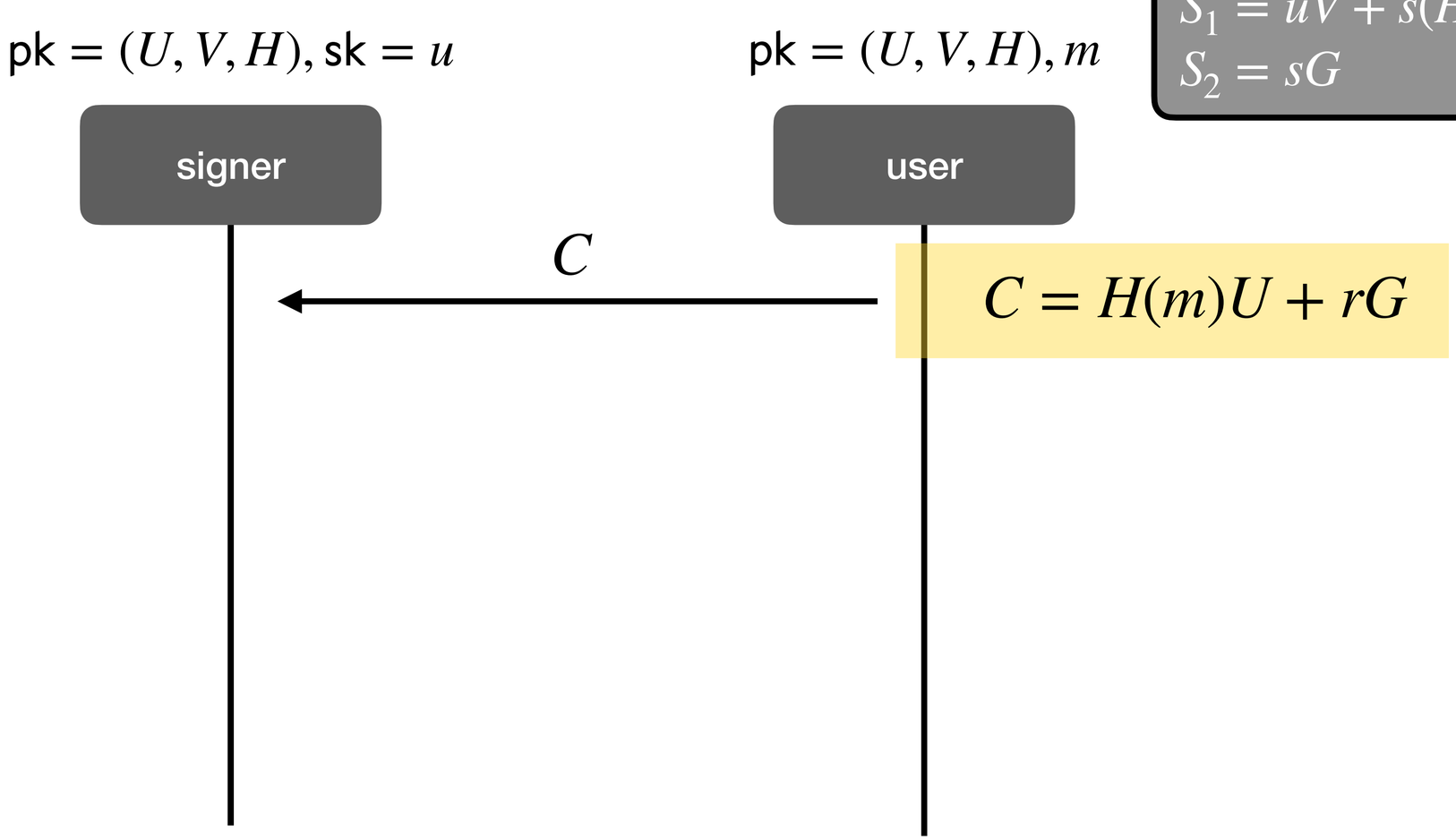
$\mathsf{pk} = (U, V, H), m$

user

Our Approach

replace pairing-based verification of **[KRS23]** via FS-compiled Σ-protocol

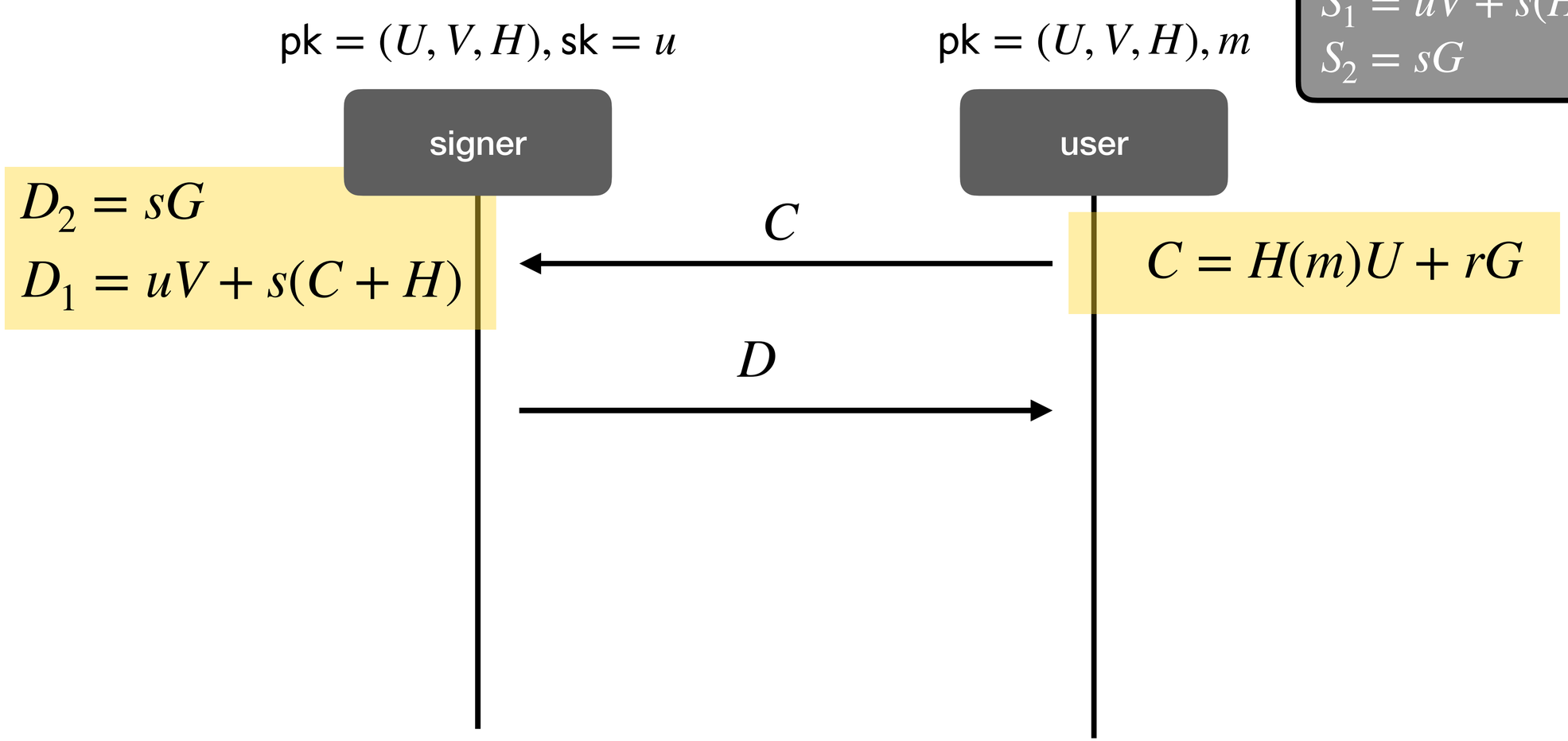
$S_1 = uV + s(H(m)U + H)$
$S_2 = sG$



Our Approach

replace pairing-based verification of **[KRS23]** via FS-compiled Σ-protocol

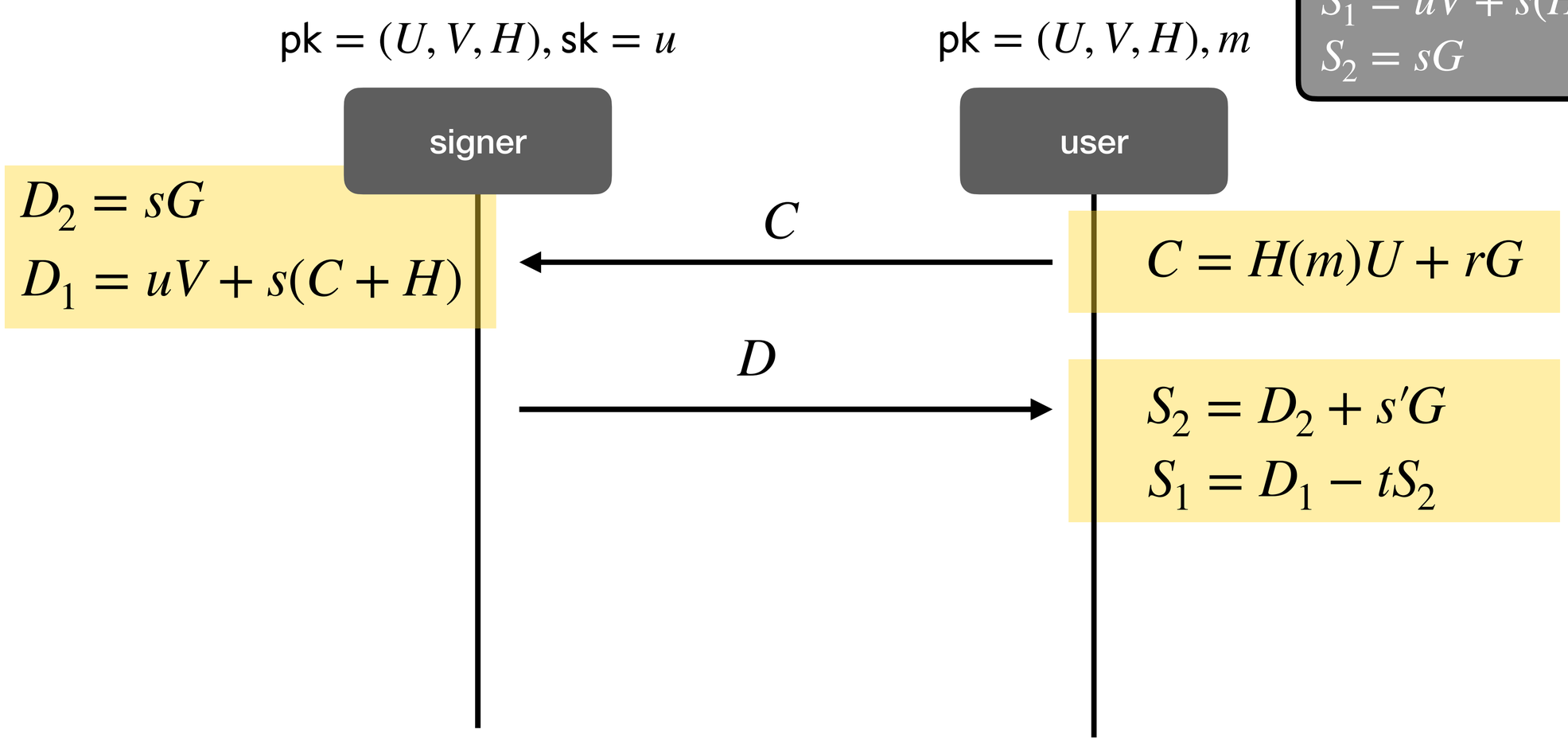
$S_1 = uV + s(H(m)U + H)$
$S_2 = sG$



Our Approach

replace pairing-based verification of **[KRS23]** via FS-compiled Σ-protocol

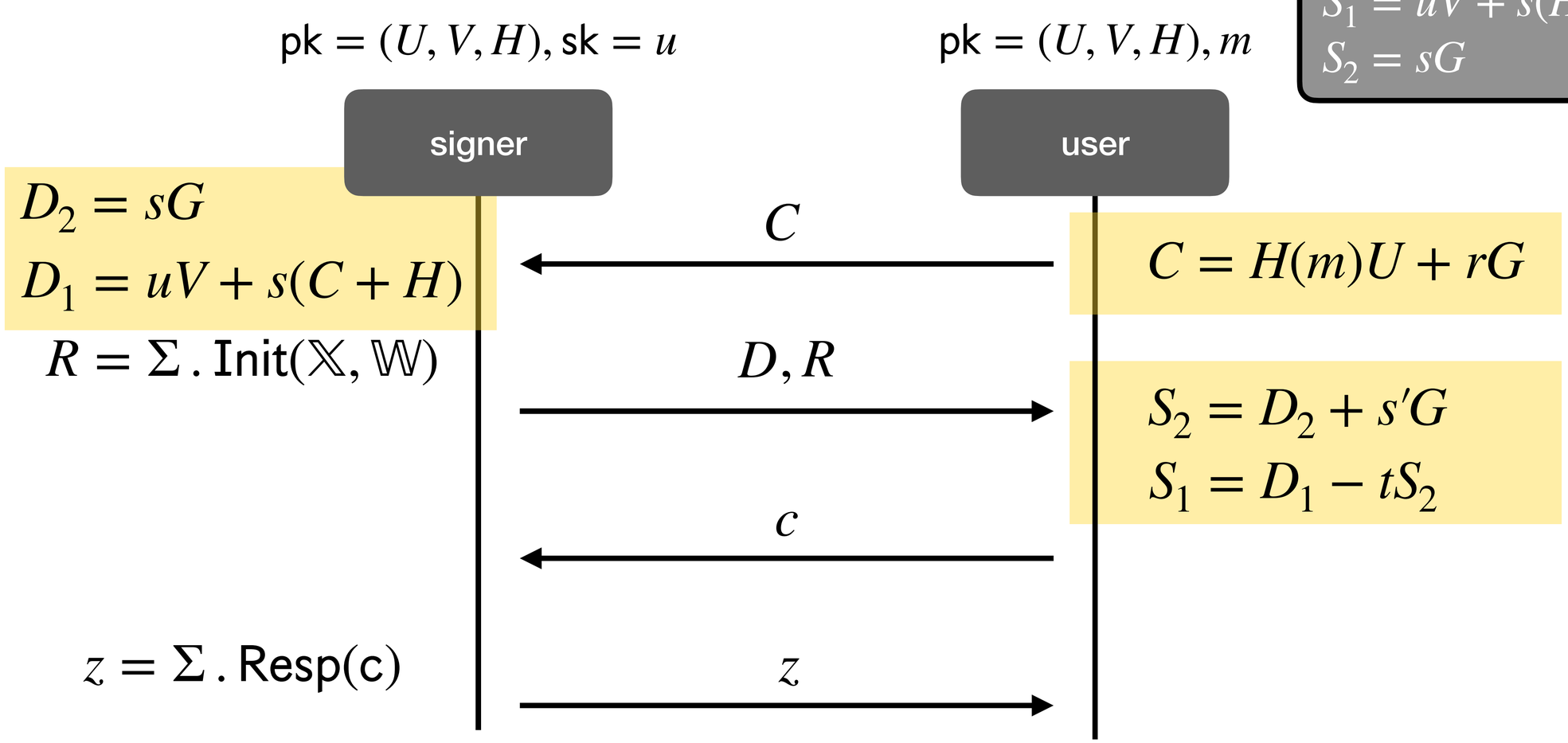
$S_1 = uV + s(H(m)U + H)$
$S_2 = sG$



Our Approach

replace pairing-based verification of **[KRS23]** via FS-compiled Σ-protocol

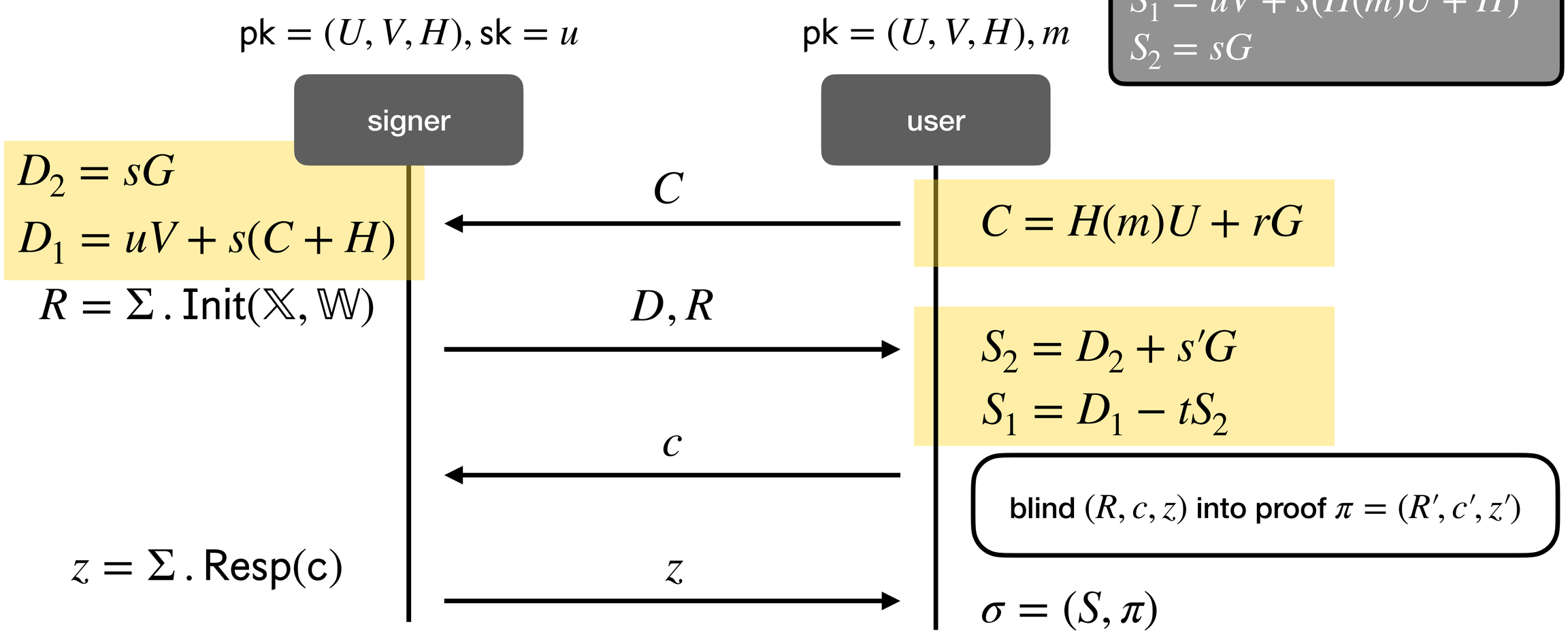
$S_1 = uV + s(H(m)U + H)$
$S_2 = sG$



Our Approach

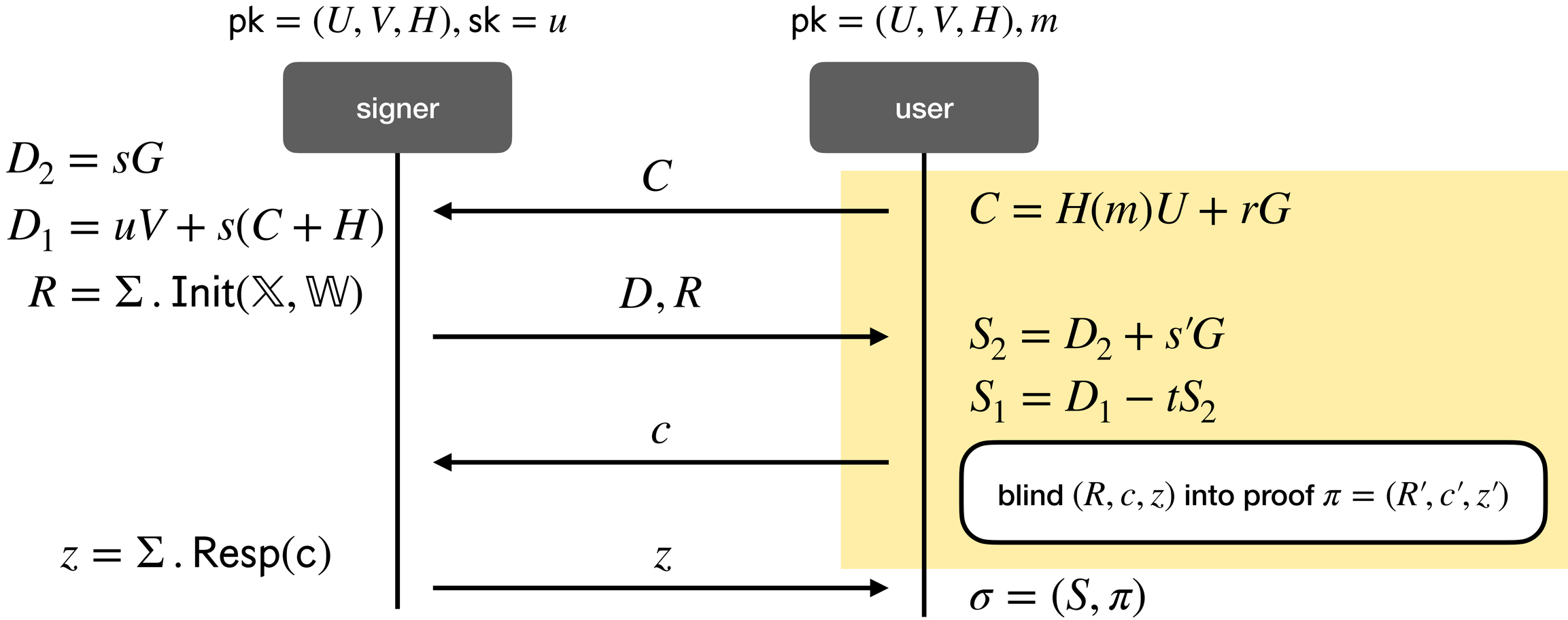
replace pairing-based verification of **[KRS23]** via FS-compiled Σ-protocol

$S_1 = uV + s(H(m)U + H)$
$S_2 = sG$



Blindness

Similar to [CTZ24] and [KRS23]



One-more Unforgeability

Approach of [CTZ24]

- Instantiate FS-compiled NIZK π with an OR-proof:
  - **either** signature S is well-formed
  - **or** know DLog of $Y = H(0)$

One-more Unforgeability

Approach of [CTZ24]

- Instantiate FS-compiled NIZK π with an OR-proof:
  - **either** signature S is well-formed
  - **or** know DLog of $Y = H(0)$
- *Knowledge soundness* of NIZK guarantees:

One-more Unforgeability

Approach of [CTZ24]

- Instantiate FS-compiled NIZK π with an OR-proof:
  - **either** signature S is well-formed
  - **or** know DLog of $Y = H(0)$
- *Knowledge soundness* of NIZK guarantees:
  - signature S is of the correct format OR we can learn DLog of Y

One-more Unforgeability

Approach of [CTZ24]

- Instantiate FS-compiled NIZK π with an OR-proof:
  - **either** signature S is well-formed
  - **or** know DLog of $Y = H(0)$
- *Knowledge soundness* of NIZK guarantees:
  - signature S is of the correct format OR we can learn DLog of Y
- Strategy:

One-more Unforgeability

Approach of [CTZ24]

- Instantiate FS-compiled NIZK π with an OR-proof:
  - **either** signature S is well-formed
  - **or** know DLog of $Y = H(0)$
- *Knowledge soundness* of NIZK guarantees:
  - signature S is of the correct format OR we can learn DLog of Y
- Strategy:
    1. under DLog, S is of the correct form

One-more Unforgeability

Approach of [CTZ24]

- Instantiate FS-compiled NIZK π with an OR-proof:
  - **either** signature S is well-formed
  - **or** know DLog of $Y = H(0)$
- *Knowledge soundness* of NIZK guarantees:
  - signature S is of the correct format OR we can learn DLog of Y
- Strategy:
  1. under DLog, S is of the correct form
  2. DLog of Y is used to simulate without knowing sk

One-more Unforgeability

Approach of [CTZ24]

- The argument is subtle

One-more Unforgeability

Approach of [CTZ24]

- The argument is subtle
- The output signatures S must be well-formed even if S-branch is simulated

One-more Unforgeability

Approach of [CTZ24]

- The argument is subtle
- The output signatures S must be well-formed even if S-branch is simulated
  - BS_1, BS_2: simulation of S via OMCDH

One-more Unforgeability

Approach of [CTZ24]

- The argument is subtle
- The output signatures S must be well-formed even if S-branch is simulated
  - BS_1, BS_2: simulation of S via OMCDH

    → can only argue Q-OMUF for Q opened sessions (OMUF-1)

One-more Unforgeability

Approach of [CTZ24]

- The argument is subtle
- The output signatures S must be well-formed even if S-branch is simulated
  - BS_1, BS_2: simulation of S via OMCDH

    → can only argue Q-OMUF for Q opened sessions (OMUF-1)
  - BS_3: send commitment instead of S

One-more Unforgeability

Approach of [CTZ24]

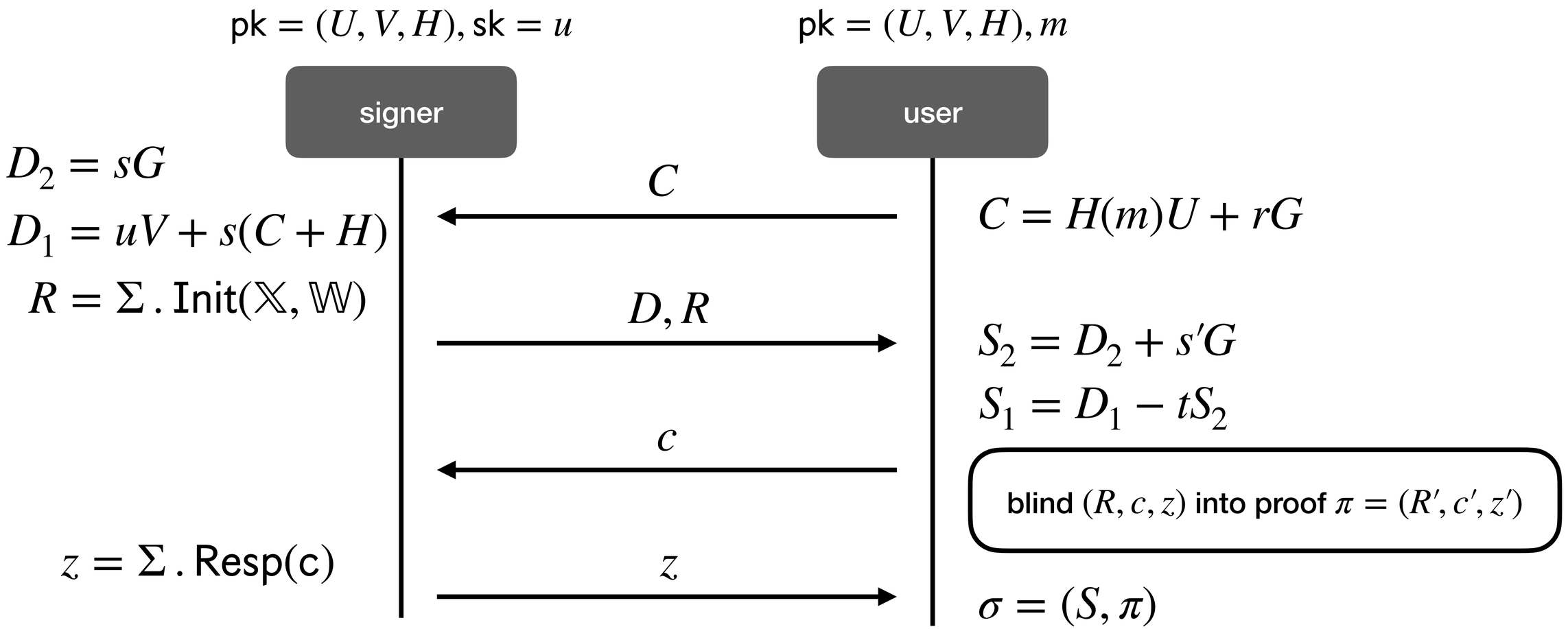
- The argument is subtle
- The output signatures S must be well-formed even if S-branch is simulated
  - BS_1, BS_2: simulation of S via OMCDH

    → can only argue Q-OMUF for Q opened sessions (OMUF-1)
  - BS_3: send commitment instead of S

    → OMUF-2 at cost of signature and communication size

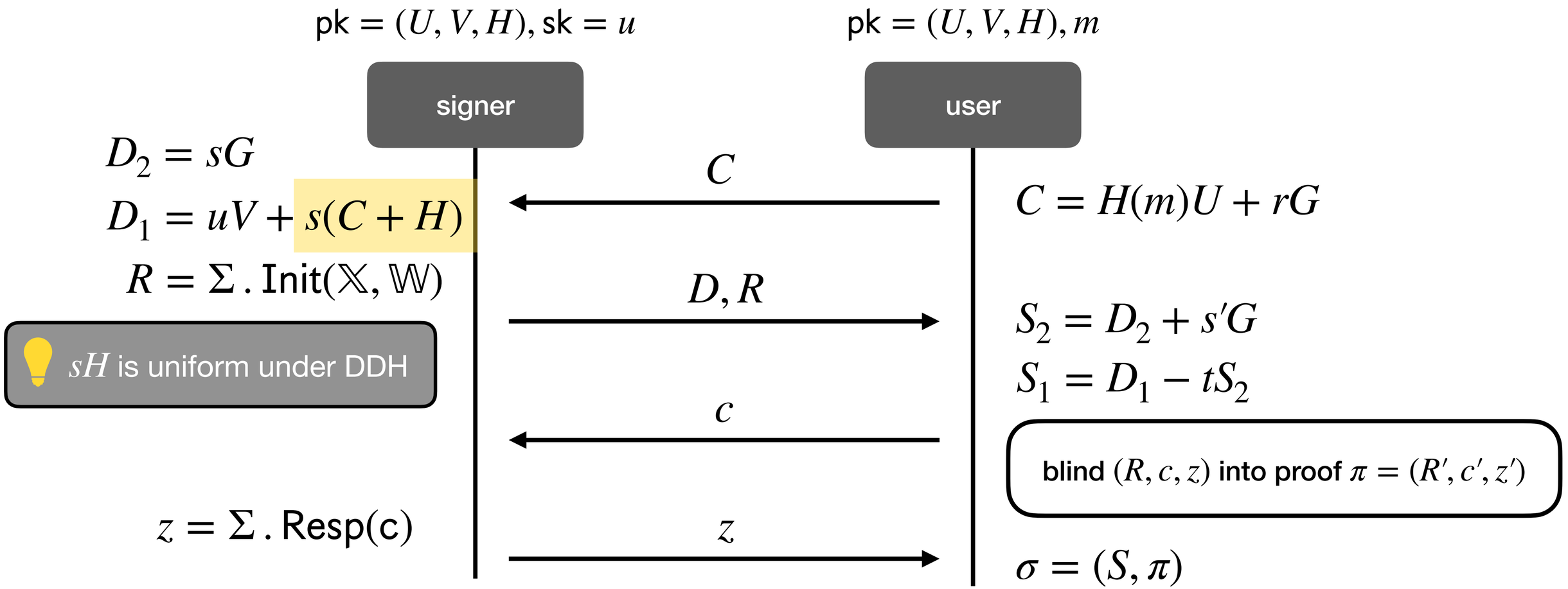
One-more Unforgeability

OMUF-2 for Free



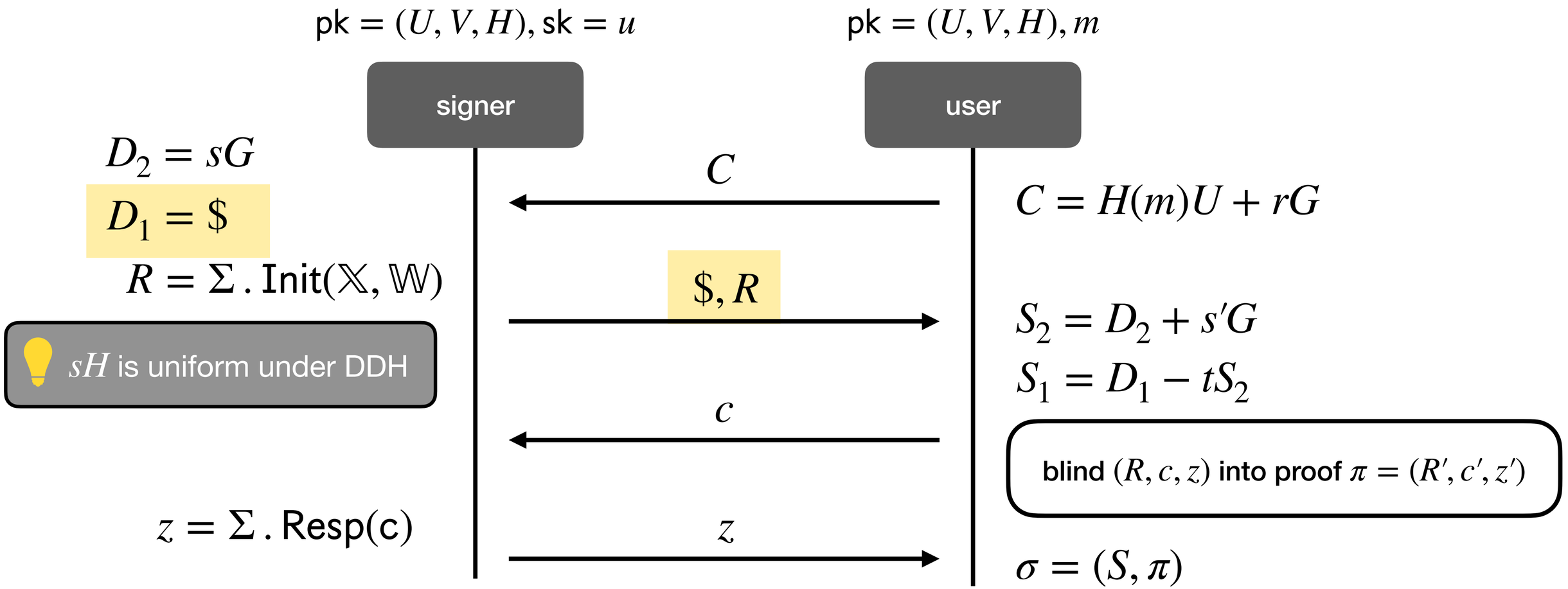
One-more Unforgeability

OMUF-2 for Free



One-more Unforgeability

OMUF-2 for Free



One-more Unforgeability

Avoiding Rewinding

- Instantiate NIZK with an OR-proof:
  - **either** signature S is well-formed
  - **or** know DLog of $Y = H(0)$

One-more Unforgeability

Avoiding Rewinding

- Instantiate NIZK with an OR-proof:
  - **either** signature S is well-formed
  - **or** know DLog of $Y = H(0)$

requires rewinding to argue that S is well-formed

One-more Unforgeability

Avoiding Rewinding

- Instantiate NIZK with an OR-proof:
  - **either** signature S is well-formed
  - **or** $(X, Y, Z) = H(0)$ is a DDH tuple

we can argue that S is well-formed without rewinding

Recap

Pairing-free blind signature without the AGM

Scheme	Signature Size	Communication Size	Security	Assumption
BS_1 + BS_2 [CTZ24]	$1\mathbb{G} + 4\mathbb{Z}_p$	$5\mathbb{G} + 5\mathbb{Z}_p$	OMUF-1	OMCDH
BS_3 [CTZ24]	poly(λ)	poly(λ)	OMUF-2	CDH
Our Work	$2\mathbb{G} + 5\mathbb{Z}_p$	poly(λ)	OMUF-2	DDH

- tighter reduction
- better efficiency
- partial blindness