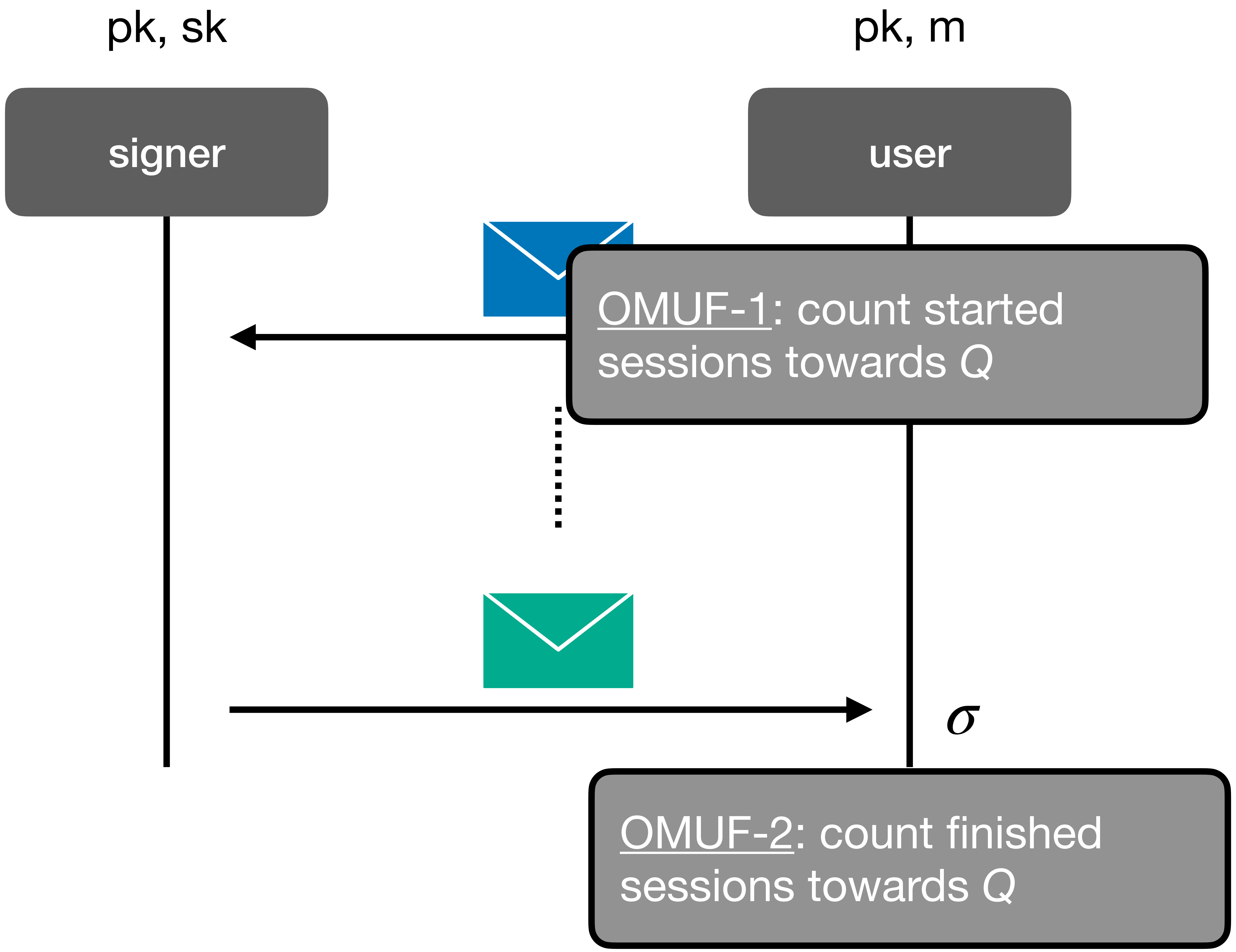
Practical Blind Signatures in Pairing-free Groups

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

Blind Signatures



pk, sk

signer

pk, m

user

σ

<u>OMUF-1</u>: count started sessions towards *Q*

<u>OMUF-2</u>: count finished sessions towards *Q*

<u>Correctness:</u>

- honest signatures verify

<u>Blindness:</u>

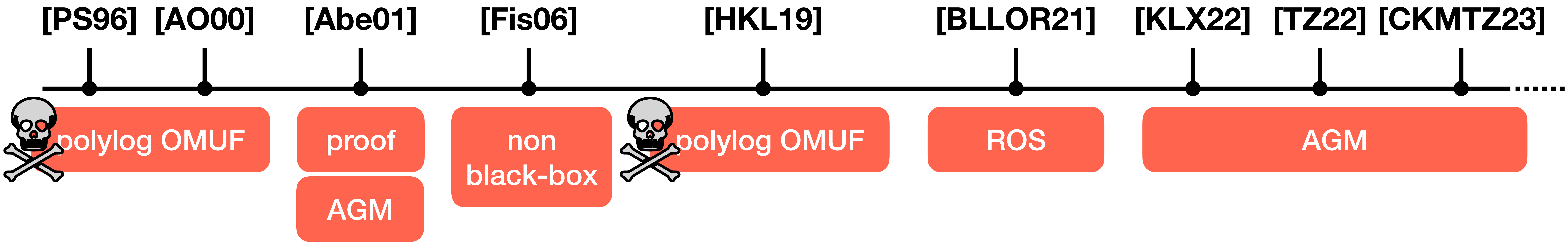
- signatures are *unlinkable* to signing sessions

<u>One-more Unforgeability:</u>

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

Blind Signatures in Pairing-free Curves

Selective Overview



[PS96] [AO00] [Abe01] [Fis06] [HKL19] [BLLOR21] [KLX22] [TZ22] [CKMTZ23] ......

☠ polylog OMUF

proof

AGM

non black-box

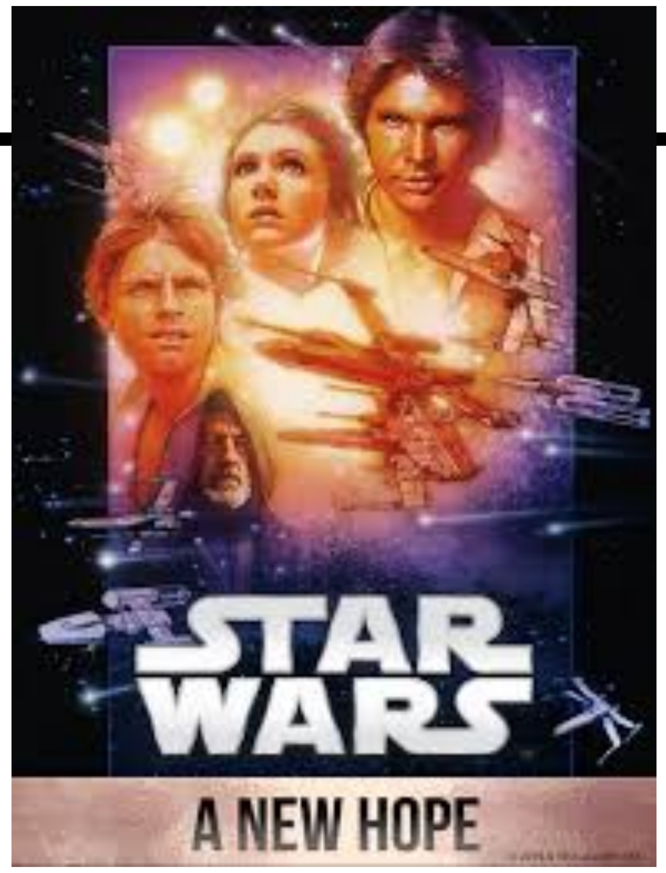
☠ polylog OMUF

ROS

AGM

[FW24] [CTZ24] This Work

non black-box



Efficiency

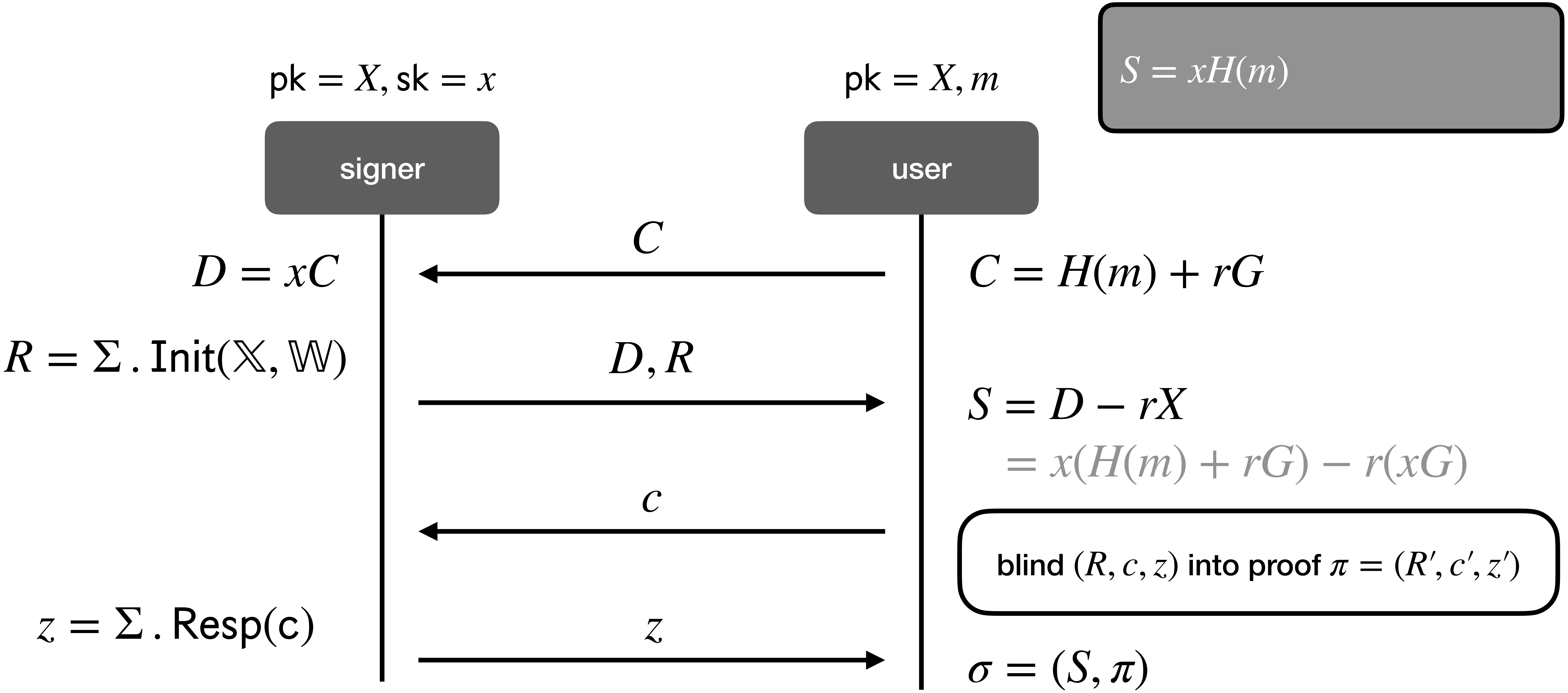
Pairing-free blind signature without the AGM

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]	poly(λ)	poly(λ)	OMUF-2	CDH

CTZ'24

High-level Overview

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



$S = xH(m)$

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

$\mathsf{pk} = X, m$

$C = H(m) + rG$

C

$D = xC$

$R = \Sigma.\mathsf{Init}(\mathbb{X}, \mathbb{W})$

D, R

$S = D - rX$

$= x(H(m) + rG) - r(xG)$

c

blind (R, c, z) into proof $\pi = (R', c', z')$

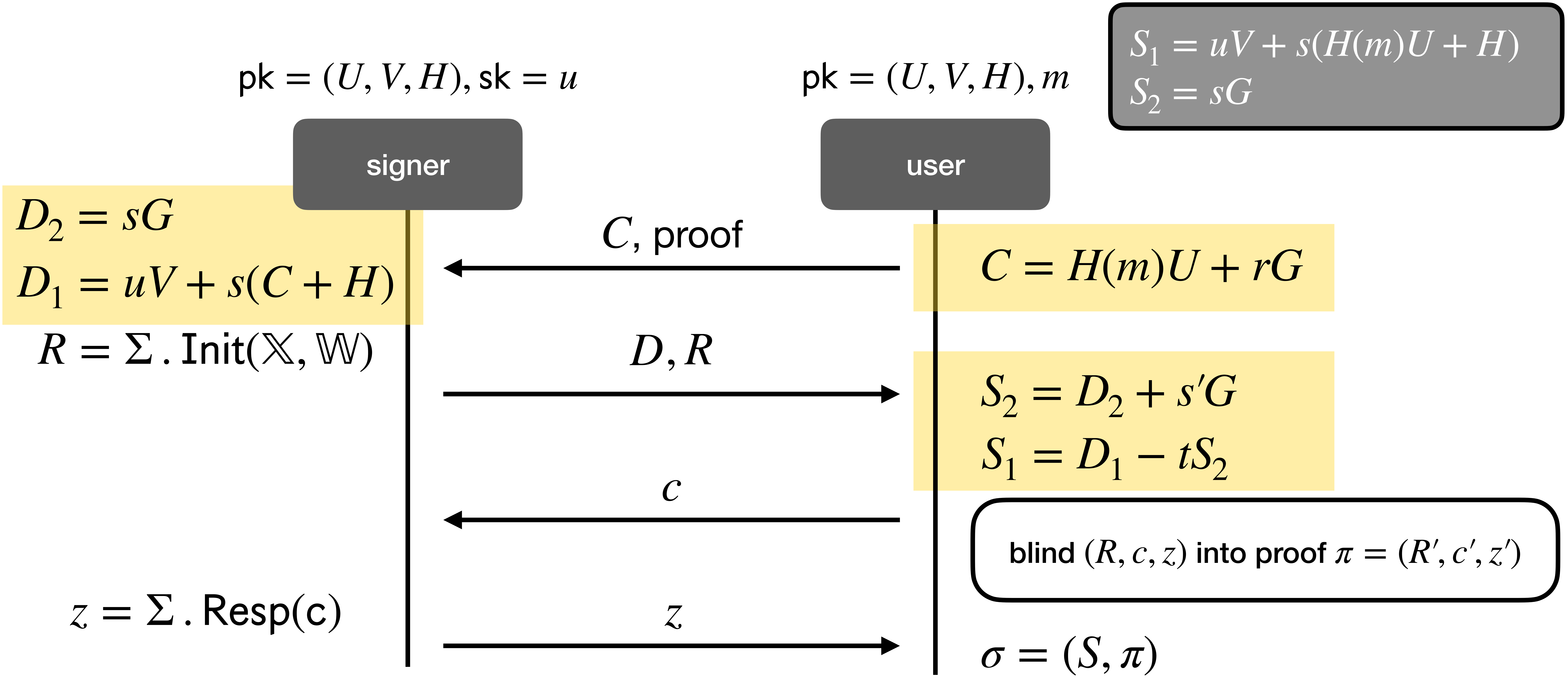
$z = \Sigma.\mathsf{Resp(c)}$

z

$\sigma = (S, \pi)$

Our Approach

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



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

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

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

$C = H(m)U + rG$

C, proof

$D_2 = sG$

$D_1 = uV + s(C + H)$

$R = \Sigma.\mathsf{Init}(\mathbb{X}, \mathbb{W})$

D, R

$S_2 = D_2 + s'G$

$S_1 = D_1 - tS_2$

c

blind (R, c, z) into proof $\pi = (R', c', z')$

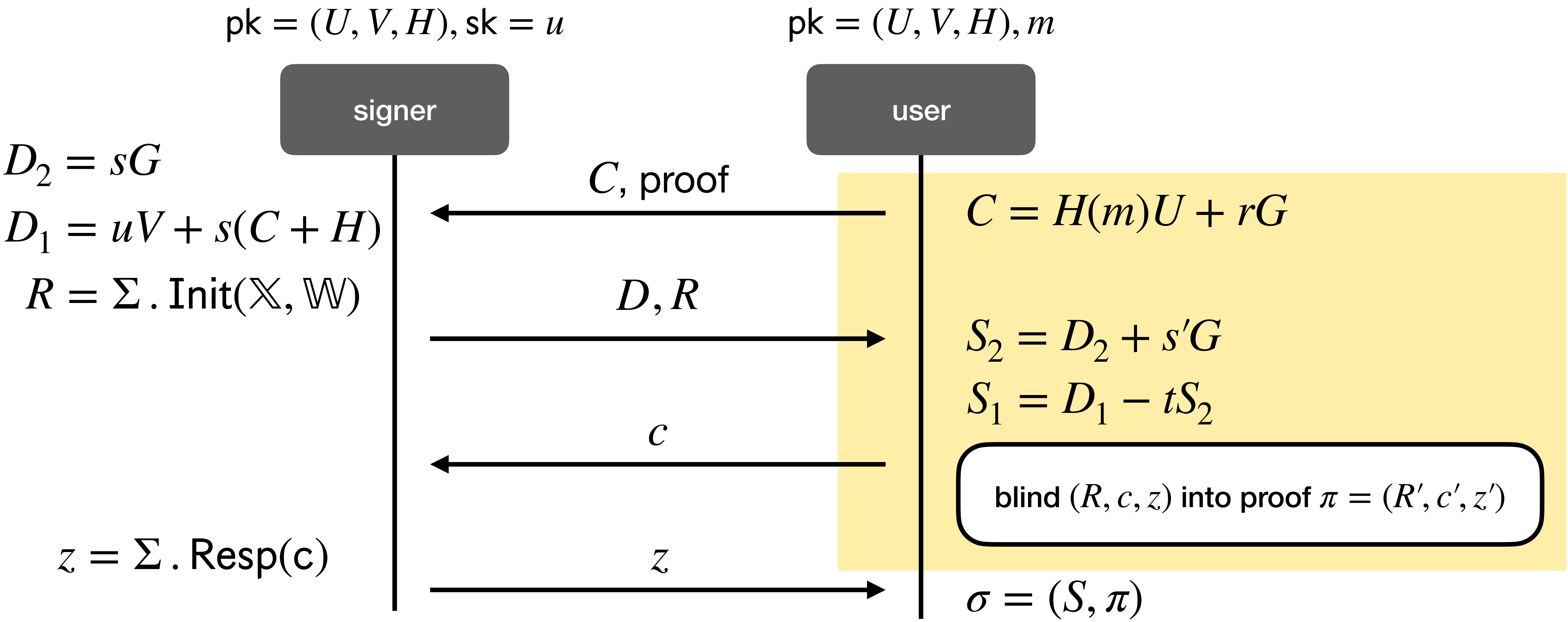
$z = \Sigma.\mathsf{Resp}(c)$

z

$\sigma = (S, \pi)$

Blindness

Similar to [CTZ24] and [KRS23]



pk $= (U, V, H)$, sk $= u$

pk $= (U, V, H), m$

signer

user

$D_2 = sG$

$D_1 = uV + s(C + H)$

$R = \Sigma.\mathsf{Init}(\mathbb{X}, \mathbb{W})$

C, proof

$C = H(m)U + rG$

D, R

$S_2 = D_2 + s'G$

$S_1 = D_1 - tS_2$

c

blind (R, c, z) into proof $\pi = (R', c', z')$

$z = \Sigma.\mathsf{Resp}(c)$

z

$\sigma = (S, \pi)$

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]

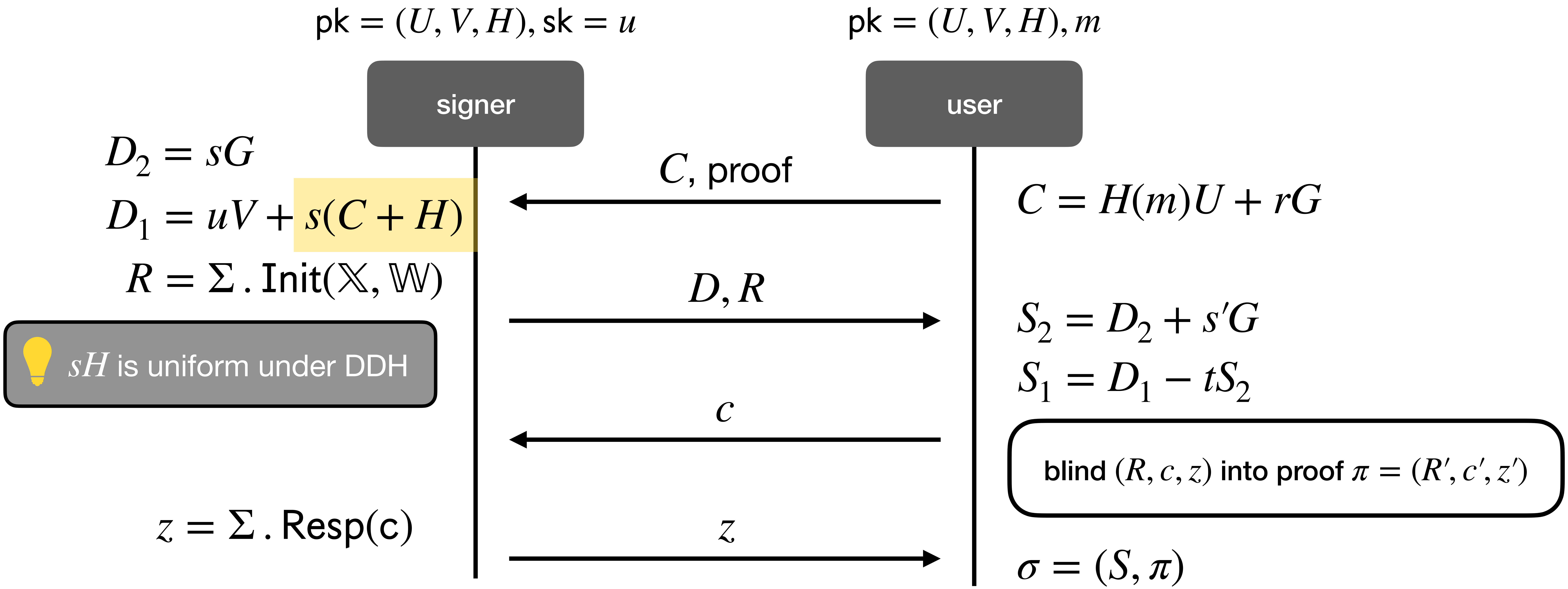
- The argument is subtle
- The output signatures S must be well-formed even if S-branch is simulated
  - BS_1, BS_2: simulation of S via OMCDH

    → 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



pk $= (U, V, H)$, sk $= u$

signer

pk $= (U, V, H), m$

user

$C = H(m)U + rG$

C, proof

$D_2 = sG$

$D_1 = uV + s(C + H)$

$R = \Sigma.\mathrm{Init}(\mathbb{X}, \mathbb{W})$

💡 sH is uniform under DDH

D, R

$S_2 = D_2 + s'G$

$S_1 = D_1 - tS_2$

blind (R, c, z) into proof $\pi = (R', c', z')$

c

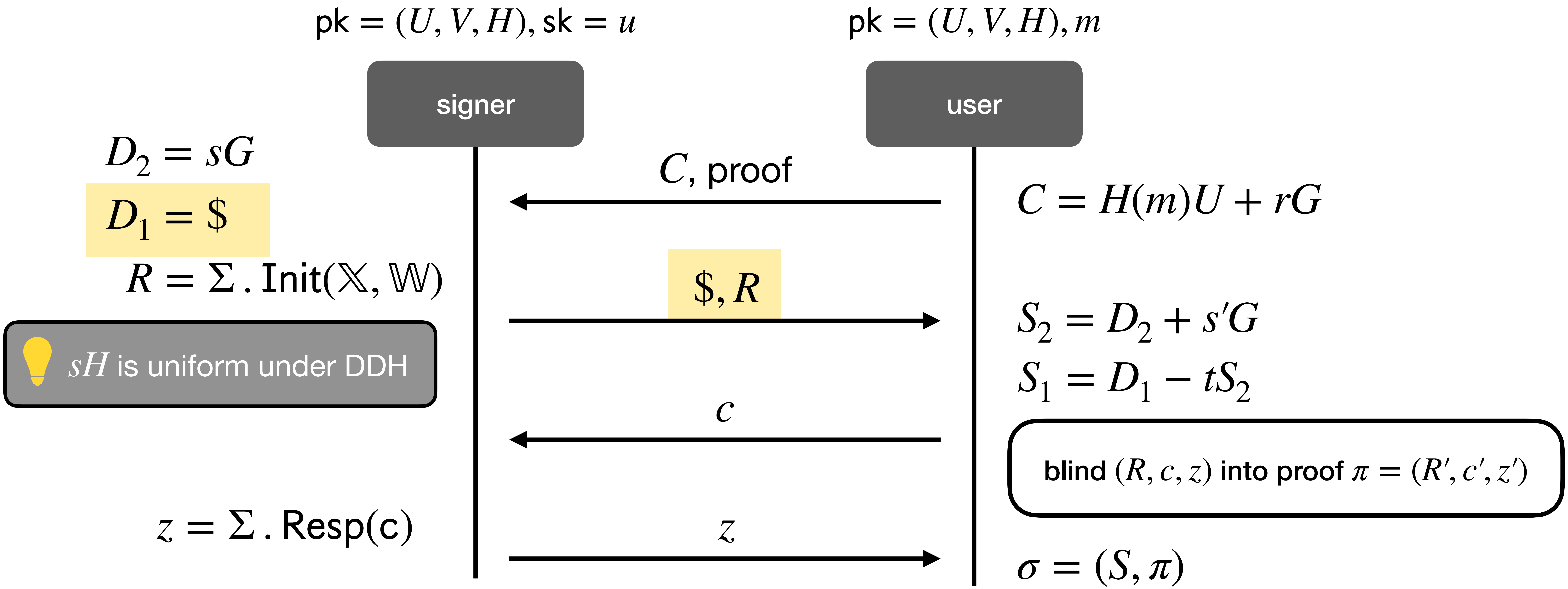
$z = \Sigma.\mathrm{Resp}(\mathrm{c})$

z

$\sigma = (S, \pi)$

One-more Unforgeability

OMUF-2 for Free



pk $= (U, V, H)$, sk $= u$

pk $= (U, V, H), m$

signer

user

$D_2 = sG$

$D_1 = \$$

$R = \Sigma.\text{Init}(\mathbb{X}, \mathbb{W})$

sH is uniform under DDH

$z = \Sigma.\text{Resp(c)}$

C, proof

$\$, R$

c

z

$C = H(m)U + rG$

$S_2 = D_2 + s'G$

$S_1 = D_1 - tS_2$

blind (R, c, z) into proof $\pi = (R', c', z')$

$\sigma = (S, \pi)$

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