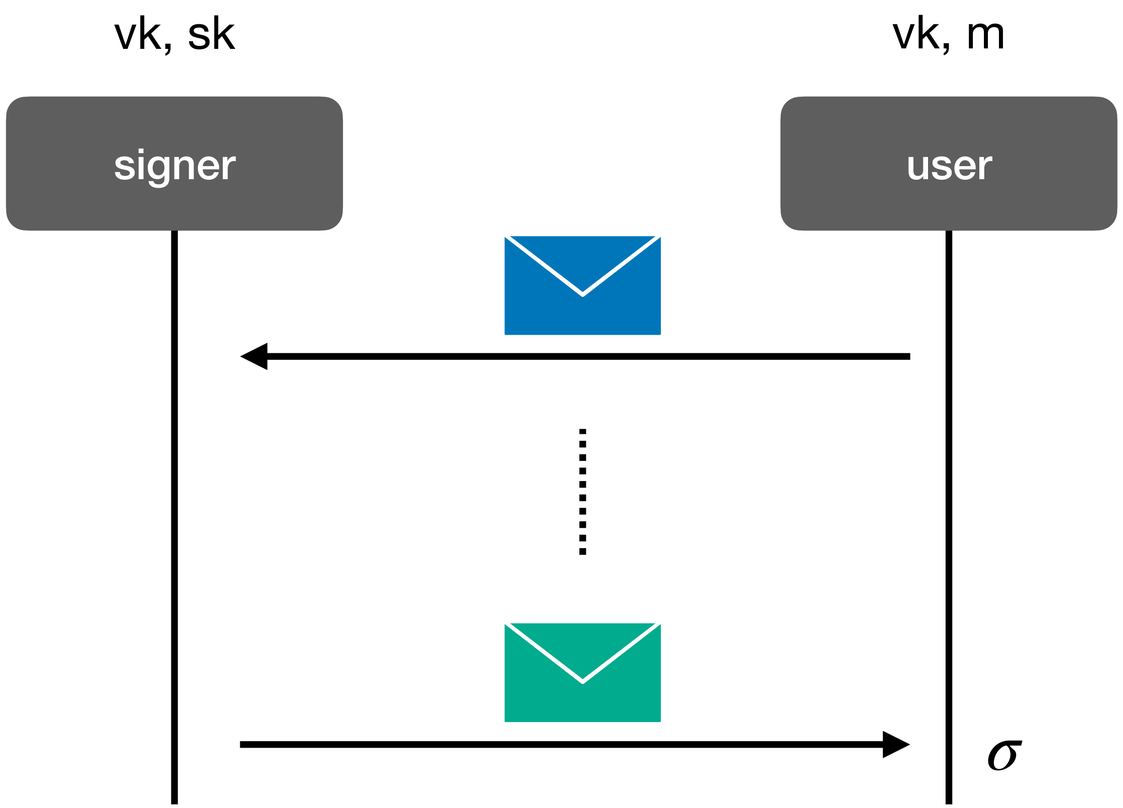
# Tightly-Secure Blind Signatures in Pairing-Free Groups


| | |
|---|---|
| Nicholas Brandt | ETH Zurich |
| Dennis Hofheinz | ETH Zurich |
| Michael Klooß | KIT |
| Michael Reichle | ETH Zurich |

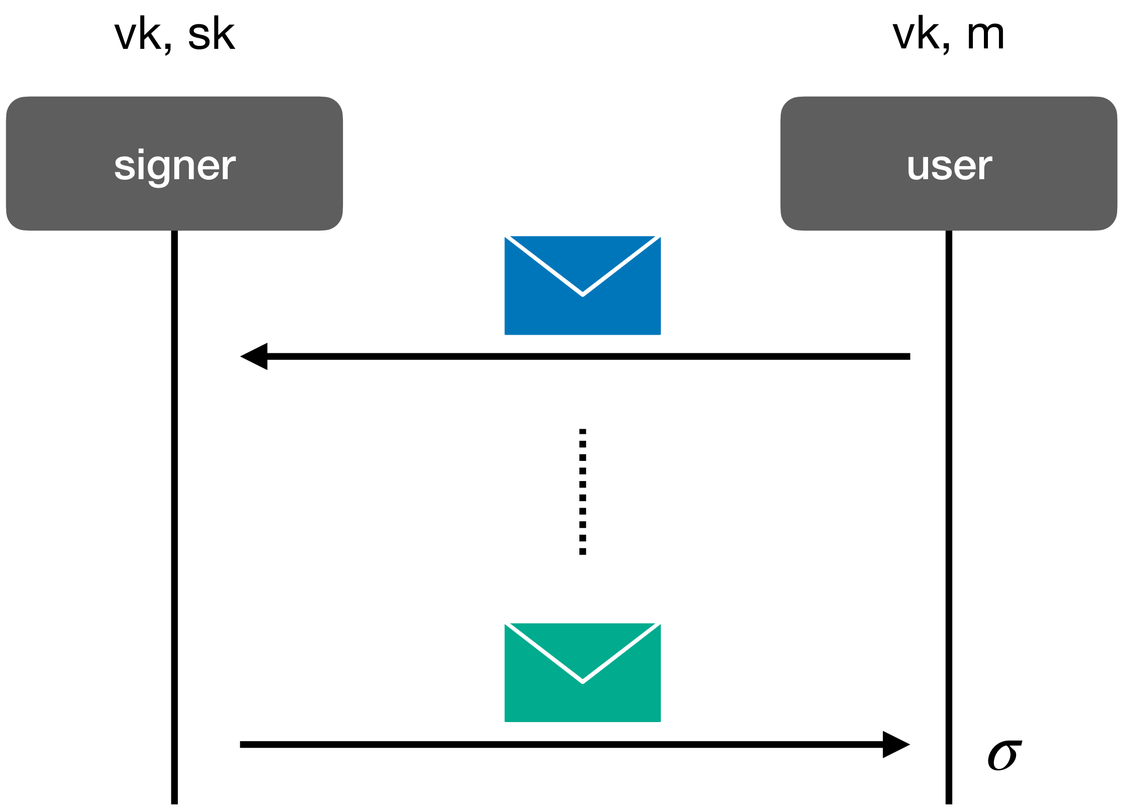
# Blind Signatures




Correctness:

- honest signatures verify

# Blind Signatures



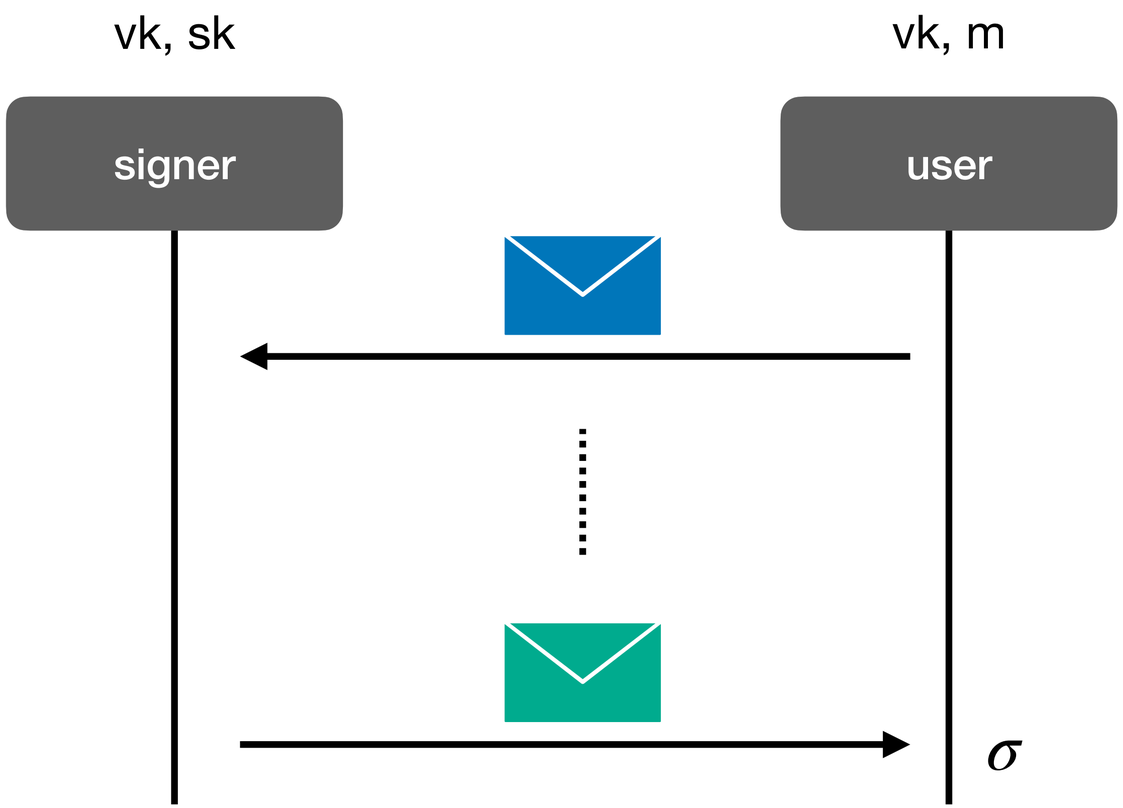

Correctness:

- 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 $Q_S$ signatures from $Q_S$ sessions with distinct messages

# Our Contribution

- ***Tight blind signatures in pairing-free groups***
  - secure under DDH with $\log(Q_S)$ loss
  - *extension:* non-programmable ROM
  - *extension:* predicate blindness

# Our Contribution

## Blind Signatures in Pairing-free Groups

| Scheme | Signature Size | Communication Size | Security | Assumption | Loss |
|---|---|---|---|---|---|
| **[CKMTZ23]** | $3(\mathbb{G}/\mathbb{Z}_p)$ | $6(\mathbb{G}/\mathbb{Z}_p)$ | AGM + ROM | DL | $O(Q_S)$ |
| **[TZ22]** | $4\mathbb{Z}_p$ | $6(\mathbb{G}/\mathbb{Z}_p)$ | AGM + ROM | DL | $O(1)$ |
| **[KR25]** | $6(\mathbb{G}/\mathbb{Z}_p)$ | $19(\mathbb{G}/\mathbb{Z}_p)$ | ROM | DDH | $O(Q_H)$ |

# Our Contribution

## Blind Signatures in Pairing-free Groups

- ***First tight BS without AGM***

| Scheme | Signature Size | Communication Size | Security | Assumption | Loss |
|---|---|---|---|---|---|
| **[CKMTZ23]** | $3(\mathbb{G}/\mathbb{Z}_p)$ | $6(\mathbb{G}/\mathbb{Z}_p)$ | AGM + ROM | DL | $O(Q_S)$ |
| **[TZ22]** | $4\mathbb{Z}_p$ | $6(\mathbb{G}/\mathbb{Z}_p)$ | AGM + ROM | DL | $O(1)$ |
| **[KR25]** | $6(\mathbb{G}/\mathbb{Z}_p)$ | $19(\mathbb{G}/\mathbb{Z}_p)$ | ROM | DDH | $O(Q_H)$ |
| **Our Work** | $41(\mathbb{G}/\mathbb{Z}_p)$ | $83(\mathbb{G}/\mathbb{Z}_p)$ | ROM | DDH | $O(\log Q_S)$ |

# Overview

- **Starting Point:** build on recent progress **[CTZ24,KRW24]**

# Overview

- **Starting Point:** build on recent progress **[CTZ24,KRW24]**
  - rely on blind signature with pairing-based verification (e.g., BLS)

# Overview

- **Starting Point:** build on recent progress **[CTZ24,KRW24]**
  - rely on blind signature with pairing-based verification (e.g., BLS)
  - employ $\sum$-protocol for verification instead of pairing

# Overview

- **Starting Point:** build on recent progress **[CTZ24,KRW24]**
  - rely on blind signature with pairing-based verification (e.g., BLS)
  - employ ∑-protocol for verification instead of pairing
  - issue ∑-protocol à la Schnorr

# Overview

- **Starting Point:** build on recent progress **[CTZ24,KRW24]**
  - rely on blind signature with pairing-based verification (e.g., BLS)
  - employ ∑-protocol for verification instead of pairing
  - issue ∑-protocol à la Schnorr
  - **result:** pairing-free blind signature without AGM

❌ loss is $\Omega(Q)$

# Overview

- **Our Techniques:**

# Overview

- **Our Techniques:**
  - employ tight pairing-based SPS (not blinding-friendly)

# Overview

- **Our Techniques:**
  - employ tight pairing-based SPS (not blinding-friendly)
  - translate SPS **[AHNOP17]** into $\Sigma$-protocol $\Pi_{\mathsf{SPS}}$

# Overview

- **Our Techniques:**
  - employ tight pairing-based SPS (not blinding-friendly)
  - translate SPS **[AHNOP17]** into $\Sigma$-protocol $\Pi_{\mathsf{SPS}}$
  - issue $\Pi_{\mathsf{SPS}}$ interactively à la **[CTZ24]** *homomorphically*

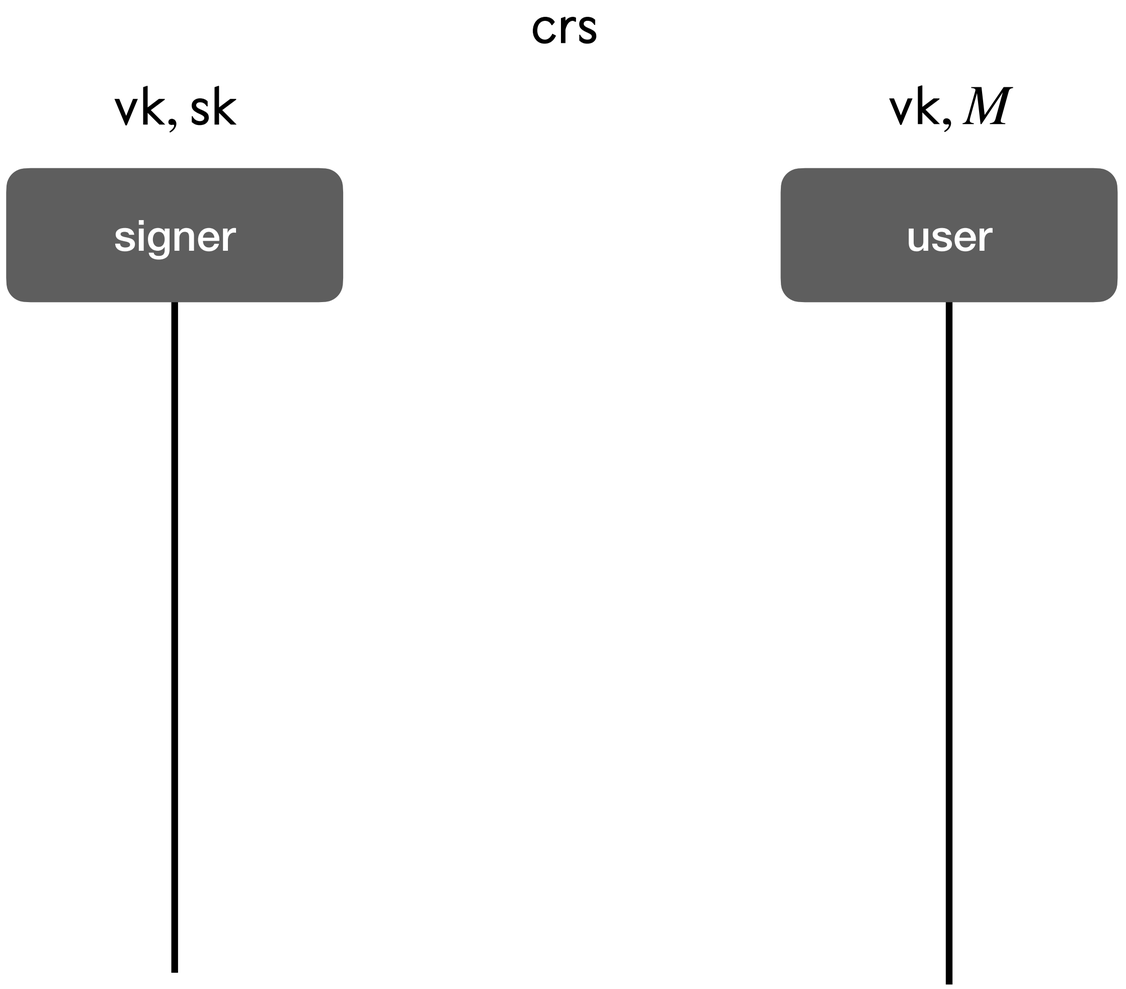
    $\rightarrow$ compile via Fiat-Shamir

# Overview

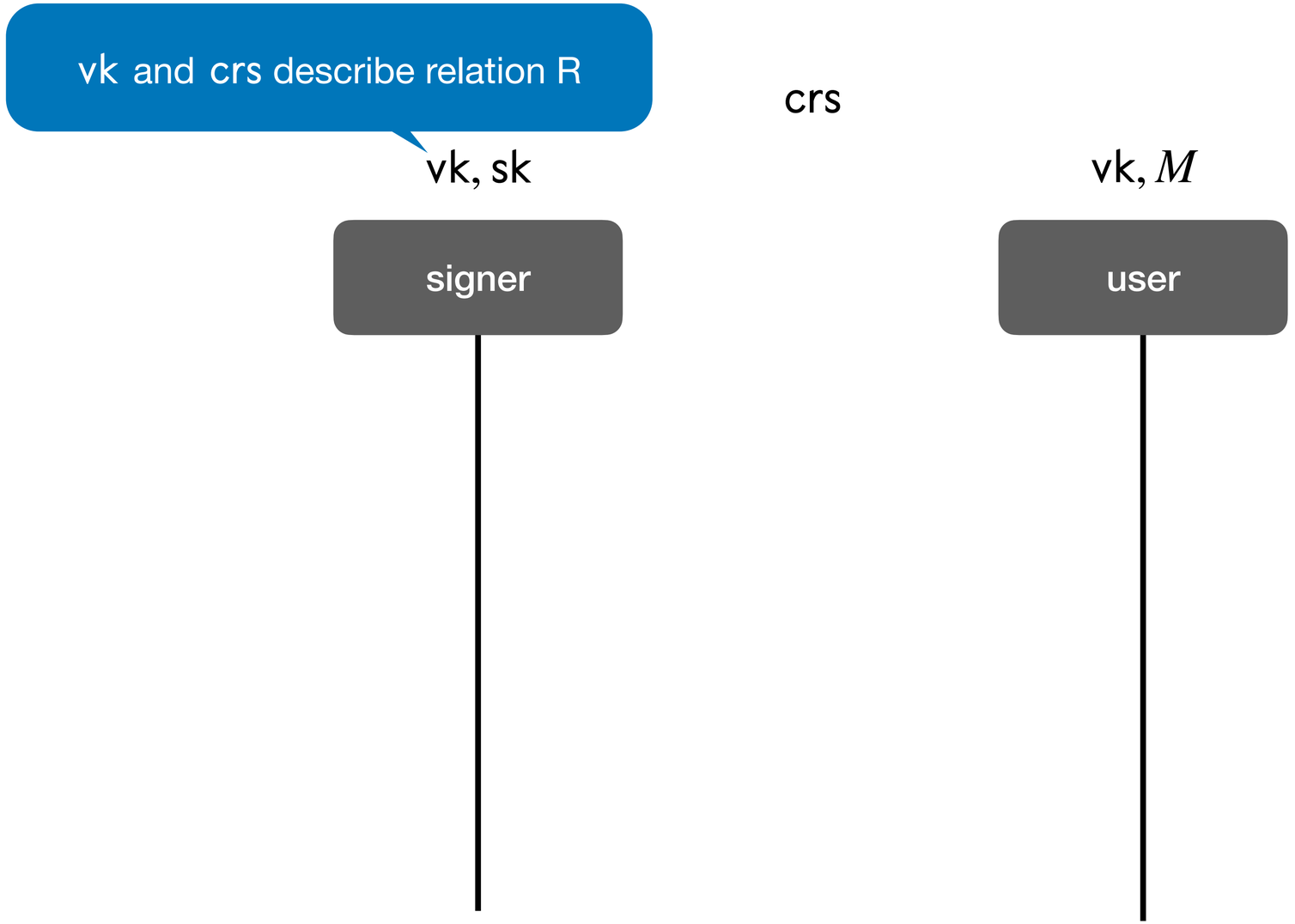
- **Our Techniques:**
  - employ tight pairing-based SPS (not blinding-friendly)
  - translate SPS **[AHNOP17]** into $\Sigma$-protocol $\Pi_{\mathsf{SPS}}$
  - issue $\Pi_{\mathsf{SPS}}$ interactively à la **[CTZ24]** *homomorphically*

    $\rightarrow$ compile via Fiat-Shamir
  - argue security via adaptive partitioning **[Hof17,AHNOP17]**

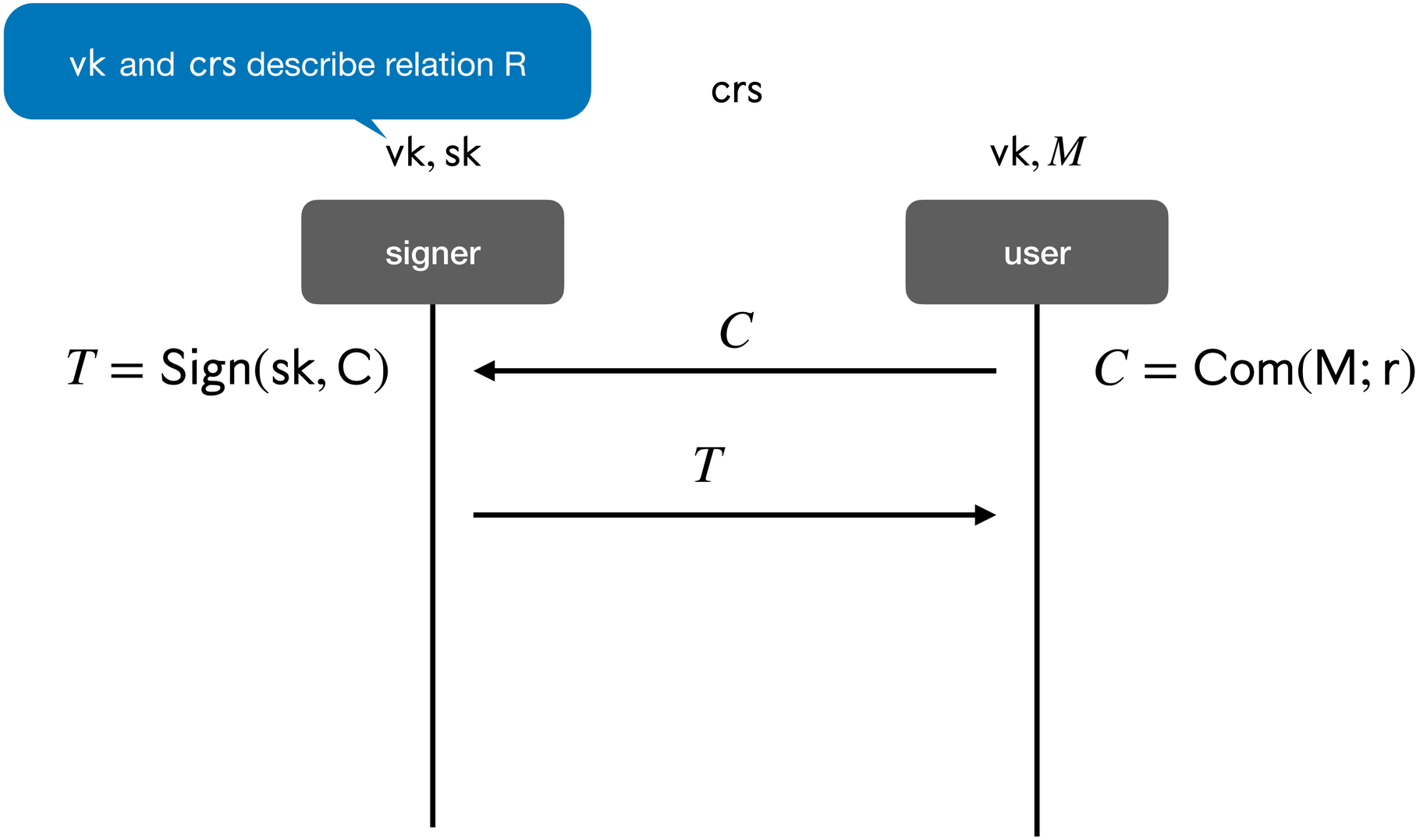
# Blind Signatures without AGM



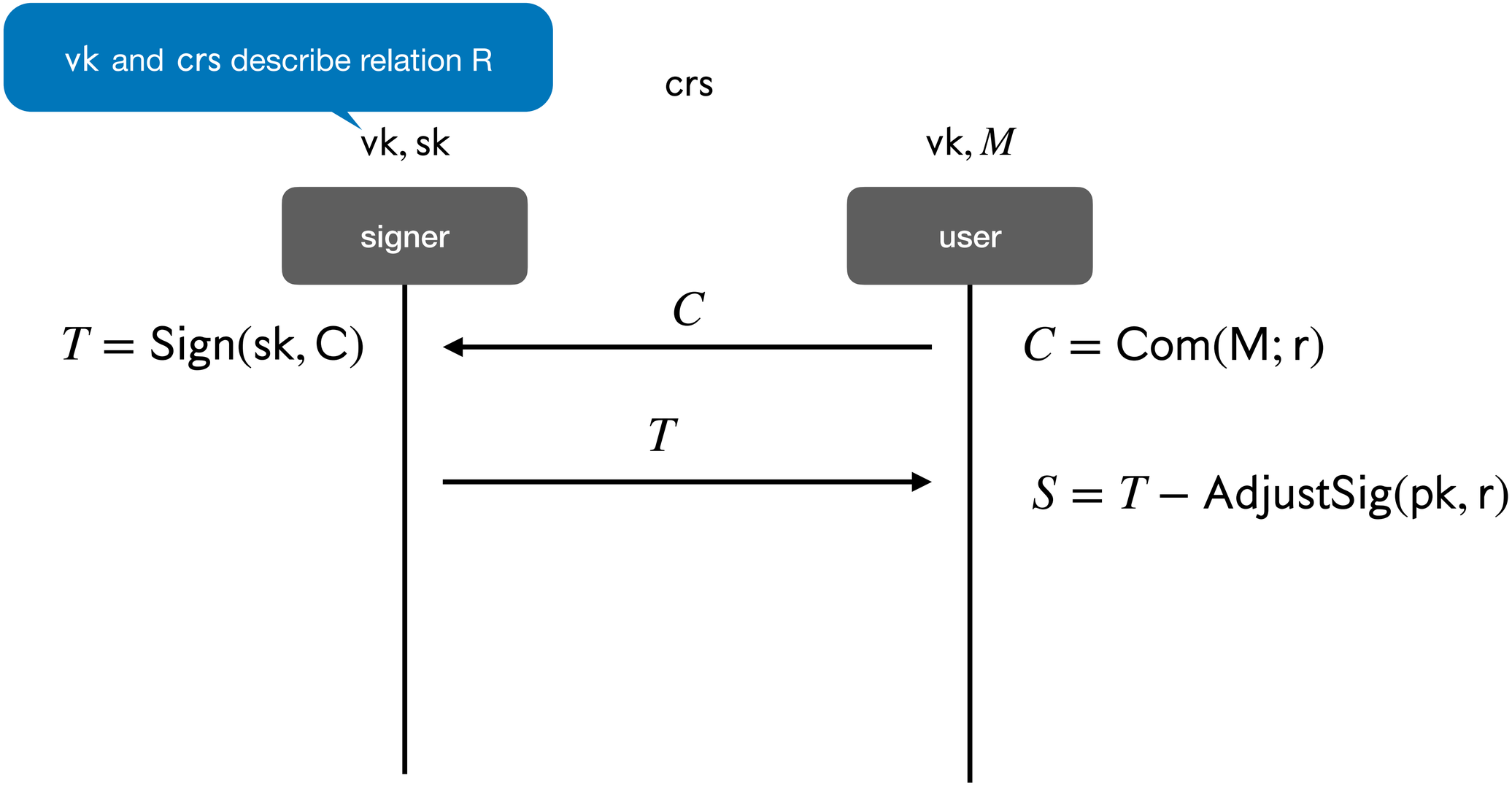
# Blind Signatures without AGM



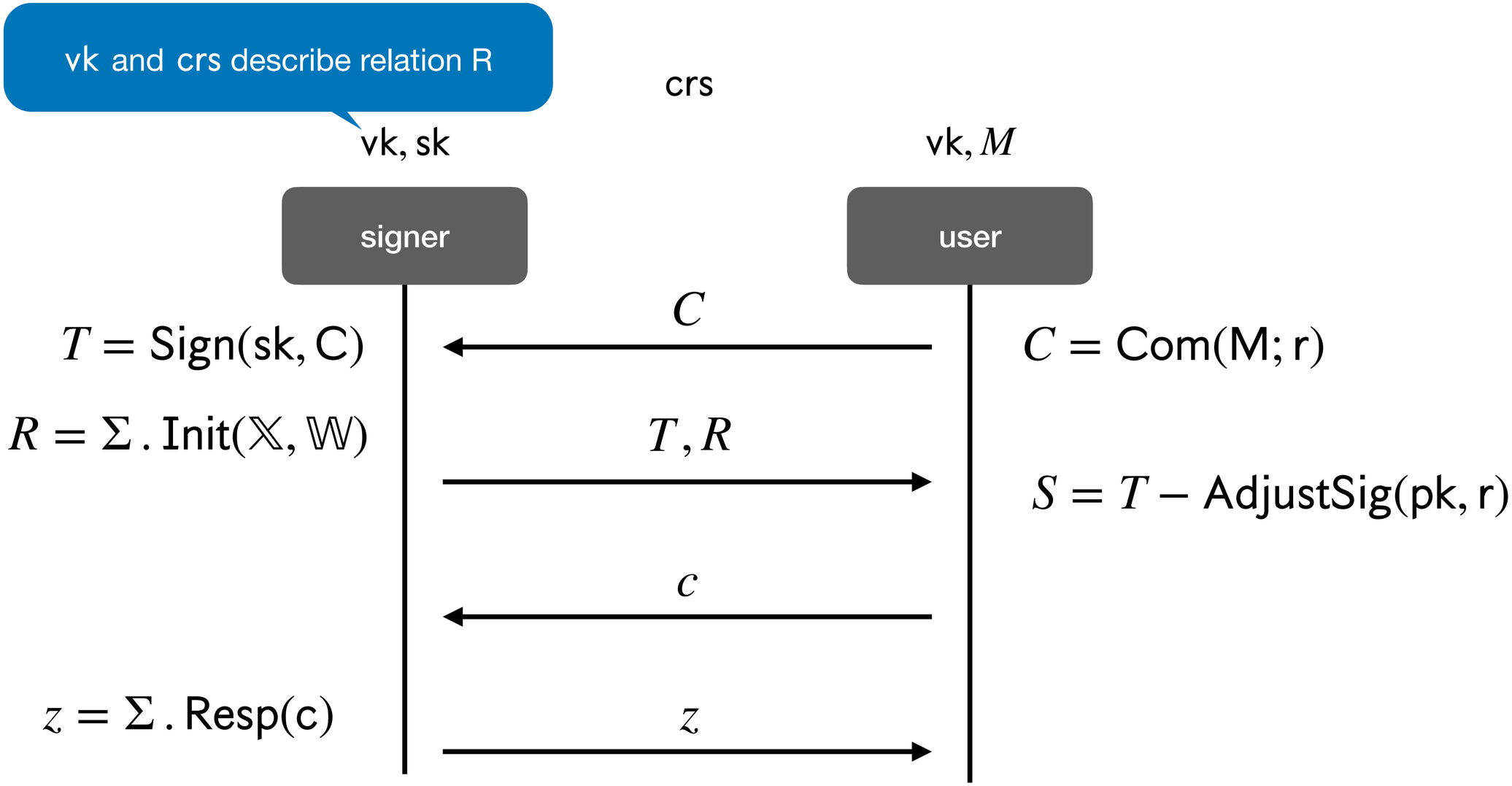
# Blind Signatures without AGM



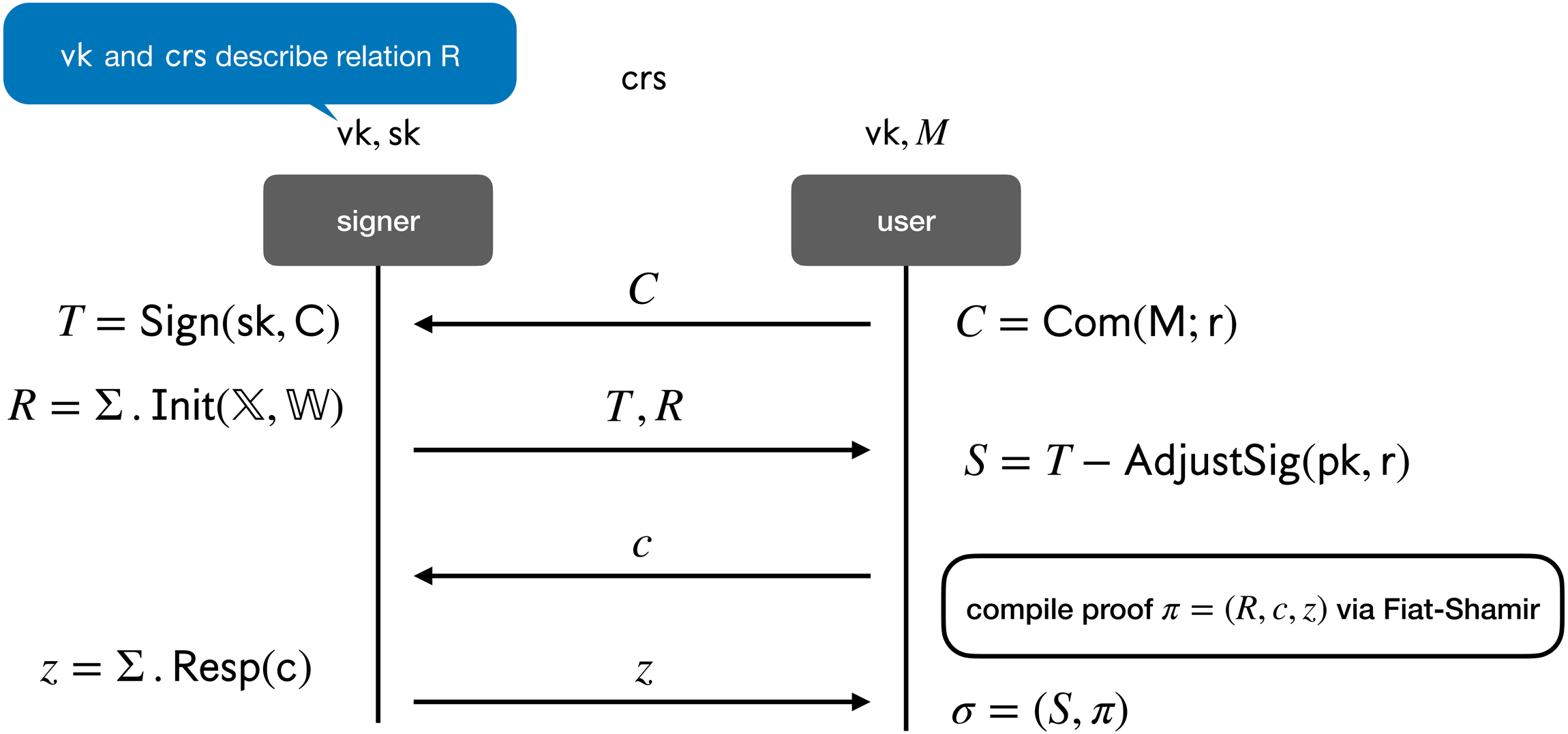
# Blind Signatures without AGM



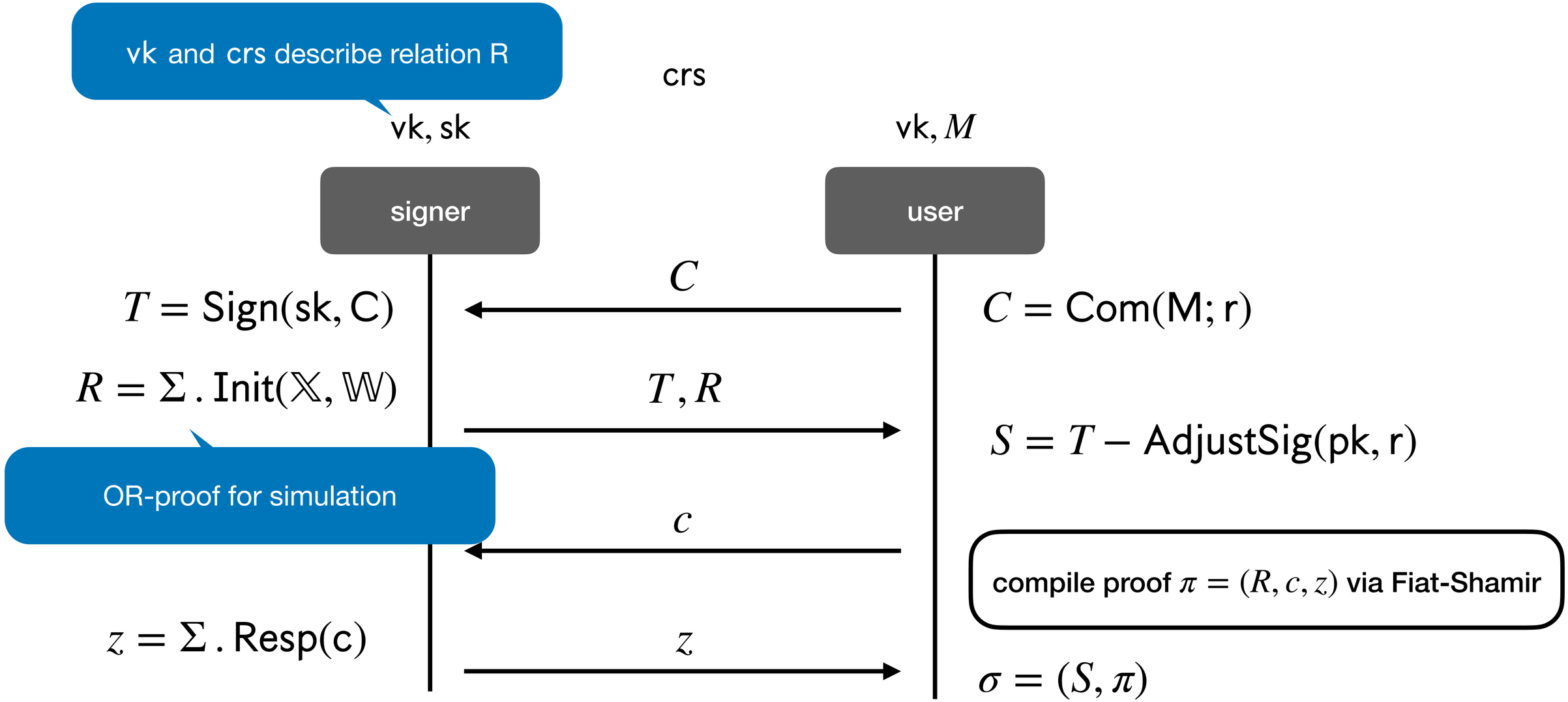
# Blind Signatures without AGM



# Blind Signatures without AGM



# Blind Signatures without AGM



# [AHNOP17] via Fiat-Shamir

## Adaptive partitioning

- vk = CMX

# [AHNOP17] via Fiat-Shamir

## Adaptive partitioning

- vk = CMX
  - $\mathsf{CMX} = (\mathsf{CMX}_0, \mathsf{CMX}_1, \mathsf{CMX}_2)$ // dual-mode commitments to $x_i$

# [AHNOP17] via Fiat-Shamir

## Adaptive partitioning

- $\mathsf{vk} = \mathsf{CMX}$
  - $\mathsf{CMX} = (\mathsf{CMX}_0, \mathsf{CMX}_1, \mathsf{CMX}_2)$ // dual-mode commitments to $x_i$
- $\mathsf{crs} = \left(D_i, \mathsf{pp}_i, \mathsf{pk}_i\right)_{i \in \{0,1,2\}}$ // DDH tuple $\mathbf{D}$

# [AHNOP17] via Fiat-Shamir

## Adaptive partitioning

- $\mathsf{vk} = \mathsf{CMX}$
  - $\mathsf{CMX} = (\mathsf{CMX}_0, \mathsf{CMX}_1, \mathsf{CMX}_2)$ // dual-mode commitments to $x_i$
- $\mathsf{crs} = \left(D_i, \mathsf{pp}_i, \mathsf{pk}_i\right)_{i \in \{0,1,2\}}$ // DDH tuple $\mathbf{D}$
- $\sigma = (\mathsf{CT}, \pi)$
  - $\mathsf{CT} = (\mathsf{CT}_0, \mathsf{CT}_1, \mathsf{CT}_2)$ // encryptions of $Z_i$
  - $\pi = (\pi_0, \pi_1)$ for relations $R_0, R_1$ // compiled via Fiat-Shamir

# [AHNOP17] via Fiat-Shamir

## Adaptive partitioning

- $\mathsf{vk} = \mathsf{CMX}^{x_i}$ $\quad \mathsf{crs} = \left(D_i, \mathsf{pp}_i, \mathsf{pk}_i\right)_{i\in\{0,1,2\}}$ $\quad \sigma = (\mathsf{CT}, \pi)^{Z_i}$
  - $R_0 = \{x_0 G + x_1 M = Z_0\}$ **or** $\{\mathbf{D}$ is DDH tuple$\}$
  - $R_1 = \{Z_0 = Z_1\}$ **or** $x_2 G = Z_2$

# [AHNOP17] via Fiat-Shamir

## Adaptive partitioning

- $\mathsf{vk} = \mathsf{CMX}^{x_i}$ $\quad \mathsf{crs} = \left(D_i, \mathsf{pp}_i, \mathsf{pk}_i\right)_{i\in\{0,1,2\}}$ $\quad \sigma = (\mathsf{CT}, \pi)^{Z_i}$
  - $R_0 = \{x_0 G + x_1 M = Z_0\}$ **or** $\{\mathbf{D}$ is DDH tuple$\}$
  - $R_1 = \{Z_0 = Z_1\}$ **or** $x_2 G = Z_2$
- **adaptive partitioning [Hof17]:**
  - in log(Q) hybrids: enforce conditions on forgery

# [AHNOP17] via Fiat-Shamir

## Adaptive partitioning

- $\mathsf{vk} = \mathsf{CMX}^{x_i}$ $\quad \mathsf{crs} = \left(D_i, \mathsf{pp}_i, \mathsf{pk}_i\right)_{i\in\{0,1,2\}}$ $\quad \sigma = (\mathsf{CT}, \pi)^{Z_i}$
  - $R_0 = \{x_0 G + x_1 M = Z_0\}$ **or** $\{\mathbf{D}$ is DDH tuple$\}$
  - $R_1 = \{Z_0 = Z_1\}$ **or** $x_2 G = Z_2$
- **adaptive partitioning [Hof17]:**
  - <u>in log(Q) hybrids:</u> enforce conditions on forgery
  - <u>in the end:</u> statistically hard to forge

# [AHNOP17] via Fiat-Shamir

## Adaptive partitioning

- $\mathsf{vk} = \mathsf{CMX}^{x_i}$ $\quad \mathsf{crs} = \left(D_i, \mathsf{pp}_i, \mathsf{pk}_i\right)_{i\in\{0,1,2\}}$ $\quad \sigma = (\mathsf{CT}, \pi)^{Z_i}$
  - $R_0 = \{x_0 G + x_1 M = Z_0\}$ **or** $\{\mathbf{D}$ is DDH tuple$\}$
  - $R_1 = \{Z_0 = Z_1\}$ **or** $x_2 G = Z_2$
- **adaptive partiti**
  - in log(Q) hybri
  - in the end: statistically hard to forge

UF argument relies on soundness of the proof systems

# [AHNOP17] via Fiat-Shamir

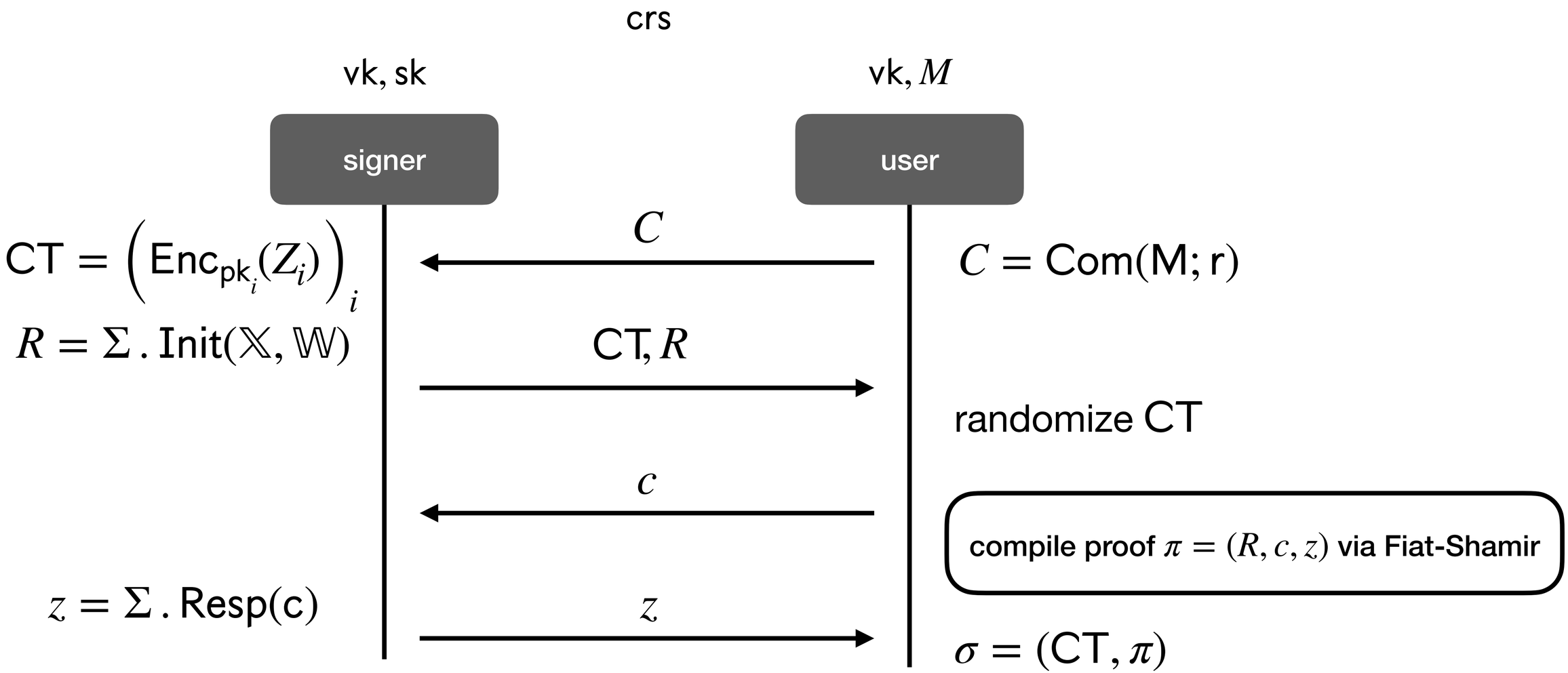
## Adaptive partitioning

- $\mathsf{vk} = \mathsf{CMX}^{x_i}$ $\quad \mathsf{crs} = \left(D_i, \mathsf{pp}_i, \mathsf{pk}_i\right)_{i\in\{0,1,2\}}$ $\quad \sigma = (\mathsf{CT}, \pi)^{Z_i}$
  - $R_0 = \{x_0 G + x_1 M = Z_0\}$ **or** $\{\mathbf{D}$ is DDH tuple$\}$
  - $R_1 = \{Z_0 = Z_1\}$ **or** $x_2 G = Z_2$
- **adaptive partiti**
  - in log(Q) hybri
  - in the end: stat

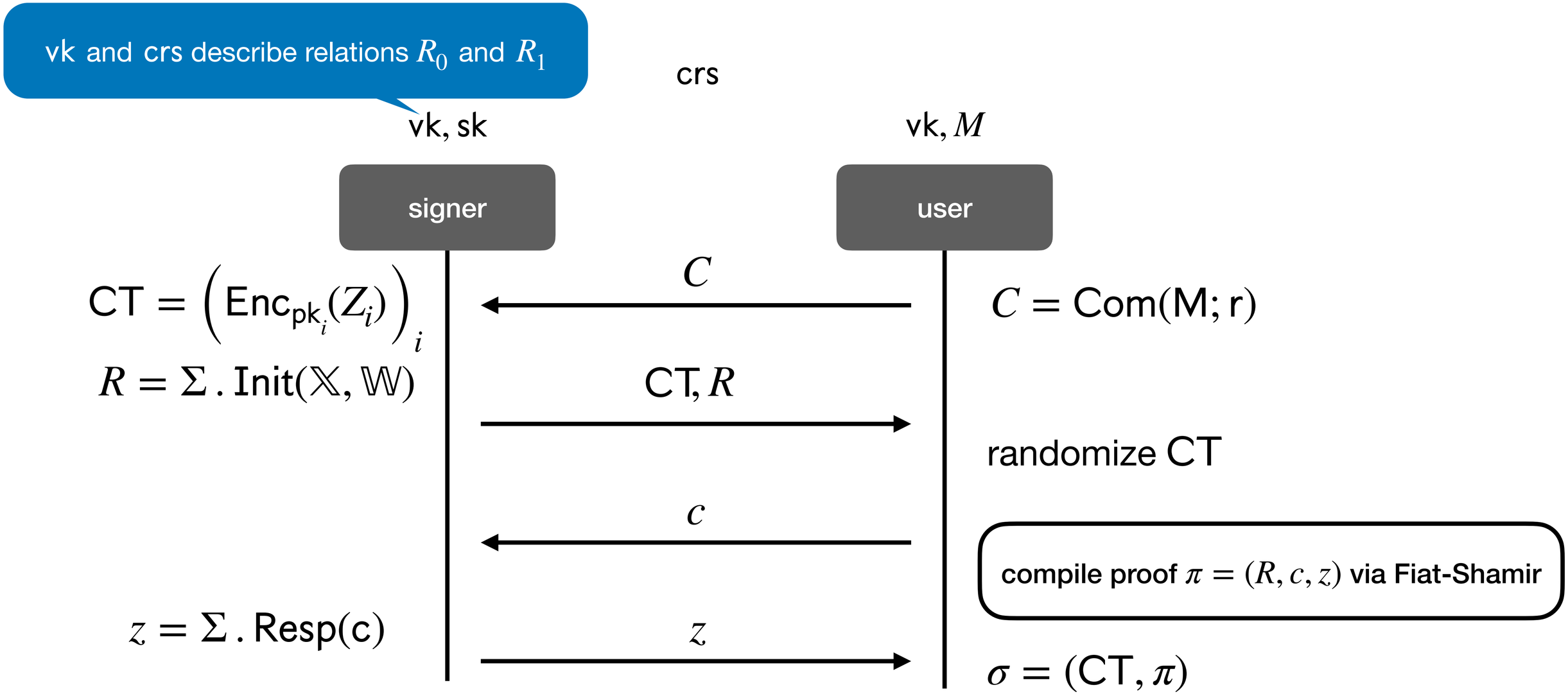
UF argument relies on soundness of the proof systems

**issue:** statement contains M

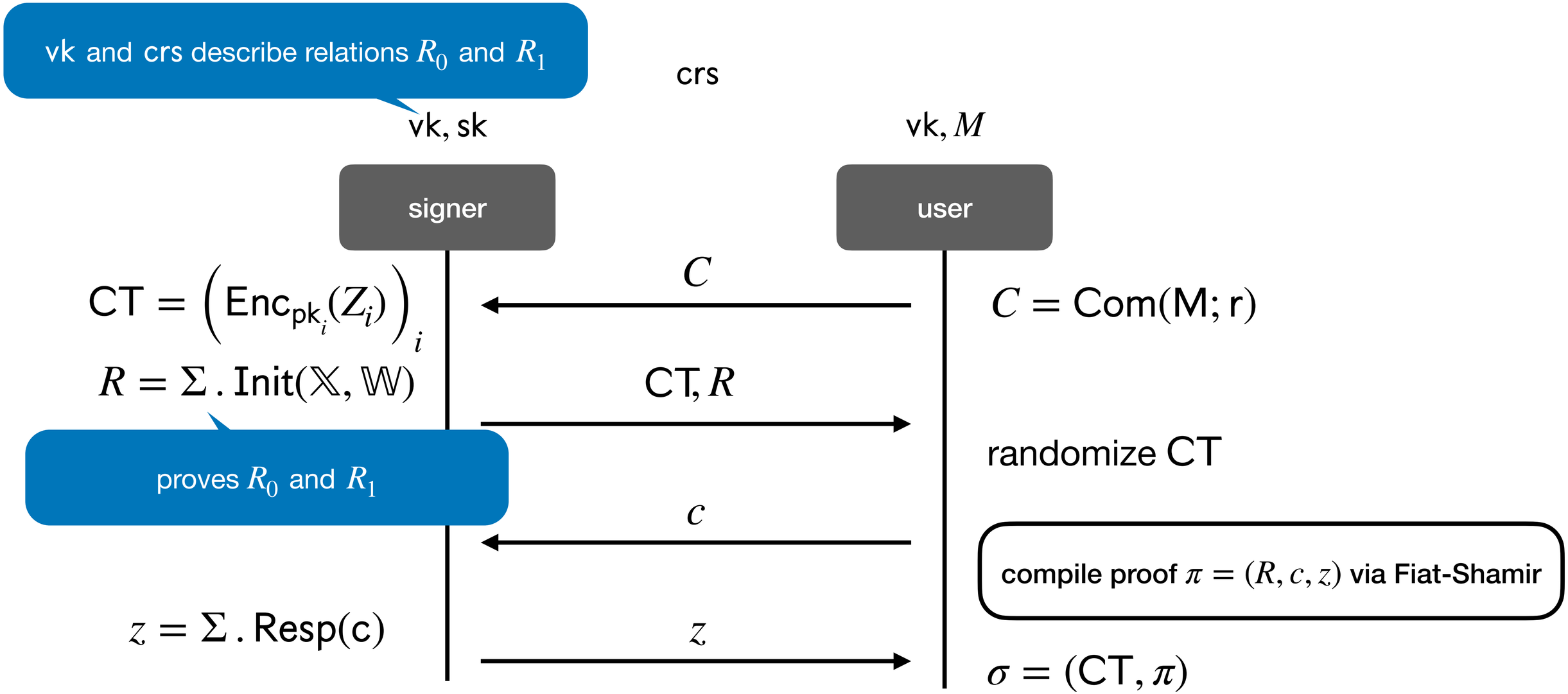
# Blind Signatures from Fiat-Shamir



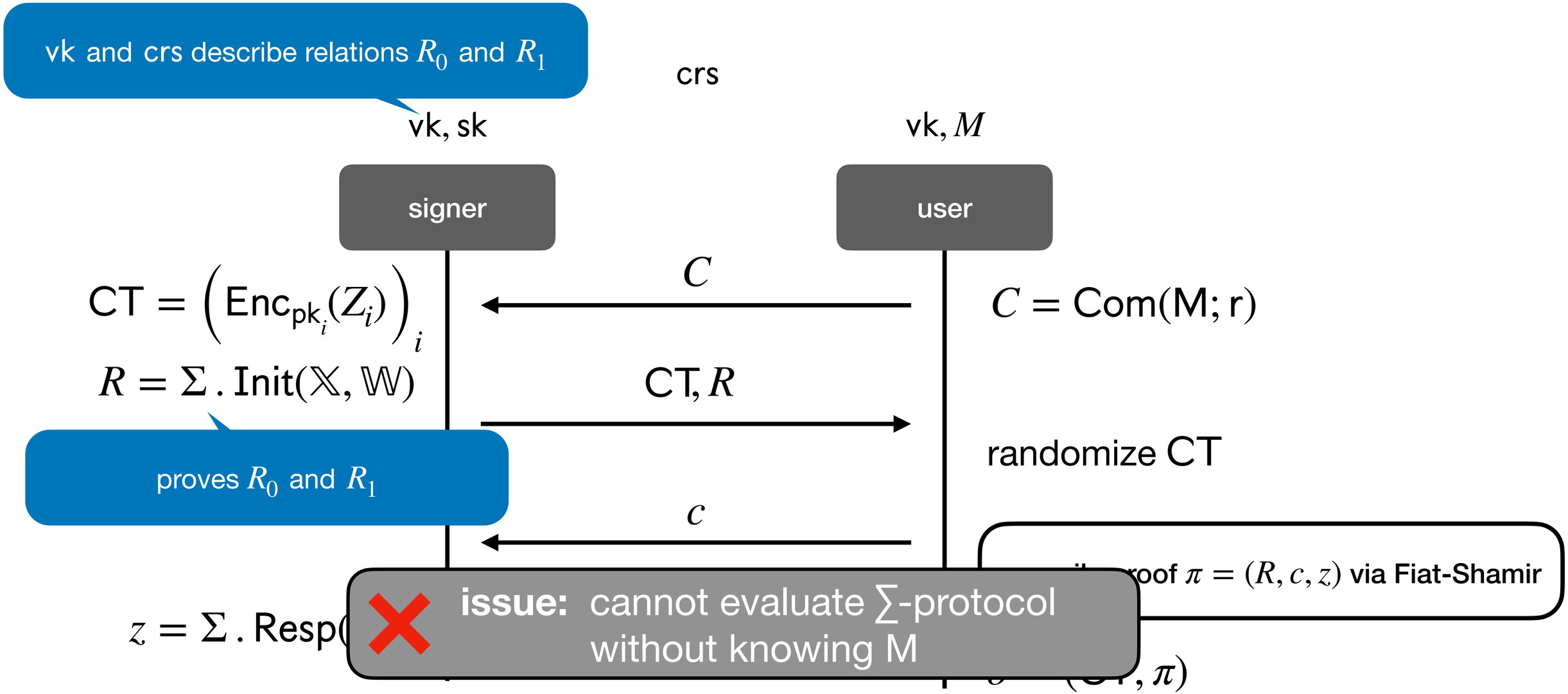
# Blind Signatures from Fiat-Shamir



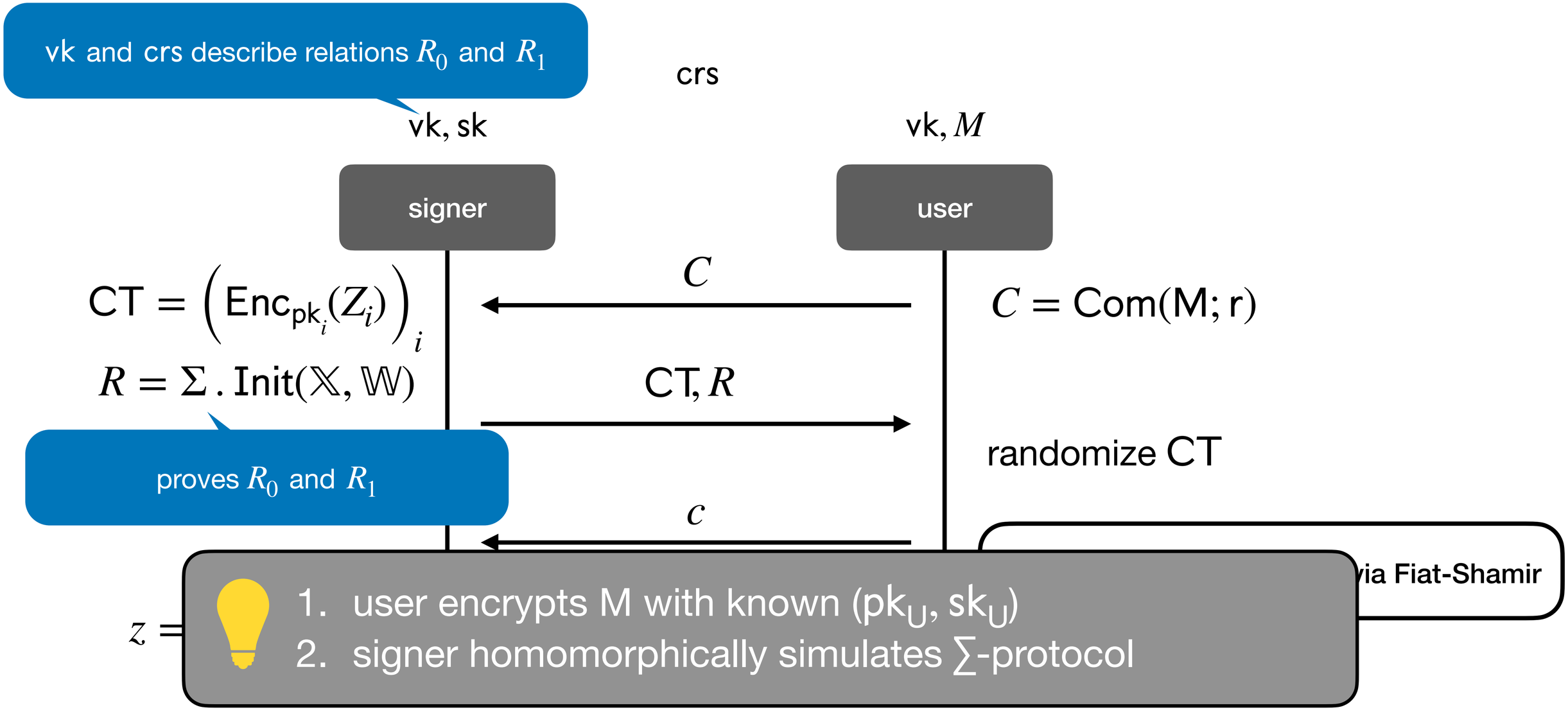
# Blind Signatures from Fiat-Shamir



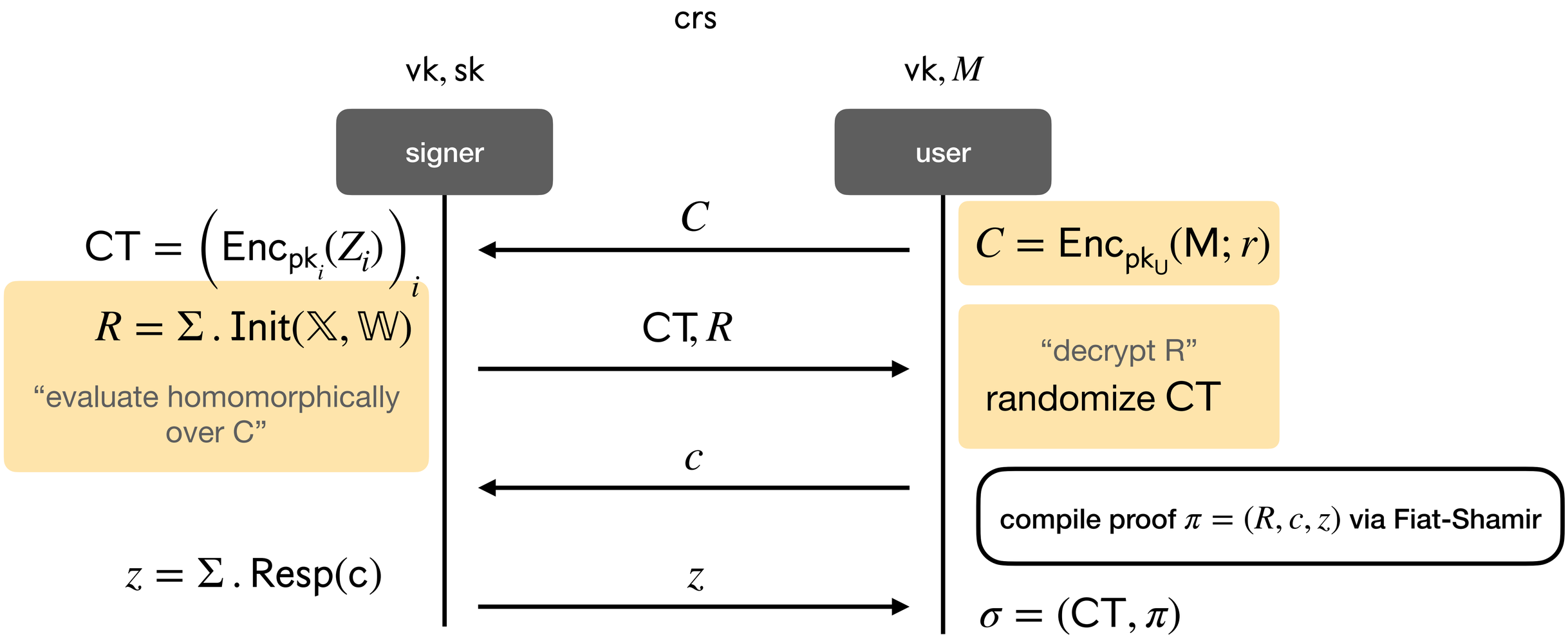
# Blind Signatures from Fiat-Shamir



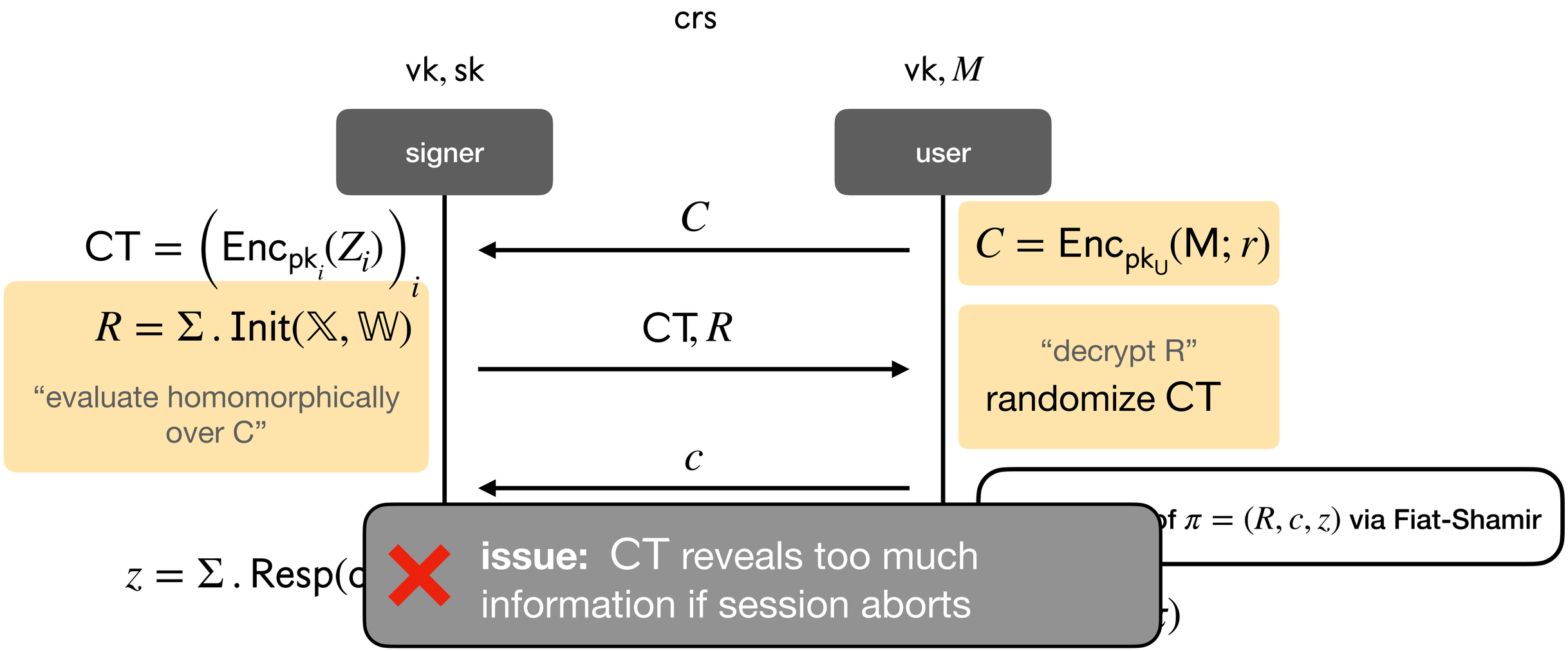
# Blind Signatures from Fiat-Shamir



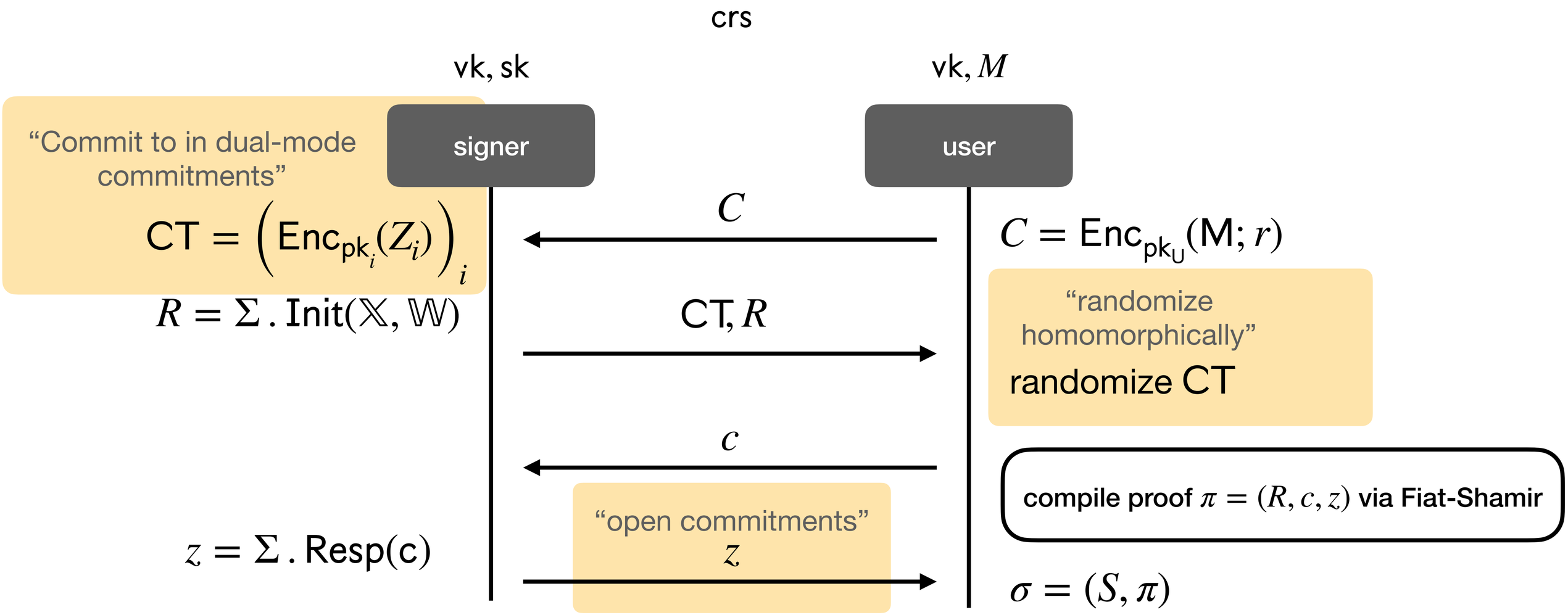
# Blind Signatures from Fiat-Shamir



# Blind Signatures from Fiat-Shamir



# Blind Signatures from Fiat-Shamir



# Summary

- signer issues **[AHNOP17]** signatures via $\sum$-protocol

# Summary

- signer issues **[AHNOP17]** signatures via ∑-protocol
- this happens behind additional homomorphic layers

# Summary

- signer issues **[AHNOP17]** signatures via ∑-protocol
- this happens behind additional homomorphic layers
  - **Blindness:** hide message in encryption → simulate ∑-protocol

# Summary

- signer issues **[AHNOP17]** signatures via $\sum$-protocol
- this happens behind additional homomorphic layers
  - **Blindness:** hide message in encryption $\rightarrow$ simulate $\sum$-protocol
  - **OMUF:** commit to ciphertexts in dual-mode commitments

# Summary

- signer issues **[AHNOP17]** signatures via ∑-protocol
- this happens behind additional homomorphic layers
  - **Blindness:** hide message in encryption → simulate ∑-protocol
  - **OMUF:** commit to ciphertexts in dual-mode commitments

    → adaptive partitioning

# Our Contribution

## Blind Signatures in Pairing-free Groups

- ***First tight BS without AGM***

| Scheme | Signature Size | Communication Size | Security | Assumption | |
|---|---|---|---|---|---|
| **[CKMTZ23]** | $3(\mathbb{G}/\mathbb{Z}_p)$ | $6(\mathbb{G}/\mathbb{Z}_p)$ | AGM + ROM | DL | $Q_S$ |
| **[TZ22]** | $4\mathbb{Z}_p$ | $6(\mathbb{G}/\mathbb{Z}_p)$ | AGM + ROM | DL | $1$ |
| **[KR25]** | $6(\mathbb{G}/\mathbb{Z}_p)$ | $19(\mathbb{G}/\mathbb{Z}_p)$ | ROM | DDH | $Q_H$ |
| **Our Work** | $41(\mathbb{G}/\mathbb{Z}_p)$ | $83(\mathbb{G}/\mathbb{Z}_p)$ | ROM | DDH | $\log Q_S$ |