Practical Round-Optimal Blind Signatures in the ROM from Standard Assumptions

- Shuichi Katsumata — PQShield — AIST
- Michael Reichle — ETH Zürich
- Yusuke Sakai — AIST

presented by Brice Minaud — ENS Paris, Inria

Introduction

Introduction

Blind Signature:

- interactive signing protocol
- privacy guarantees

Introduction

Blind Signature:

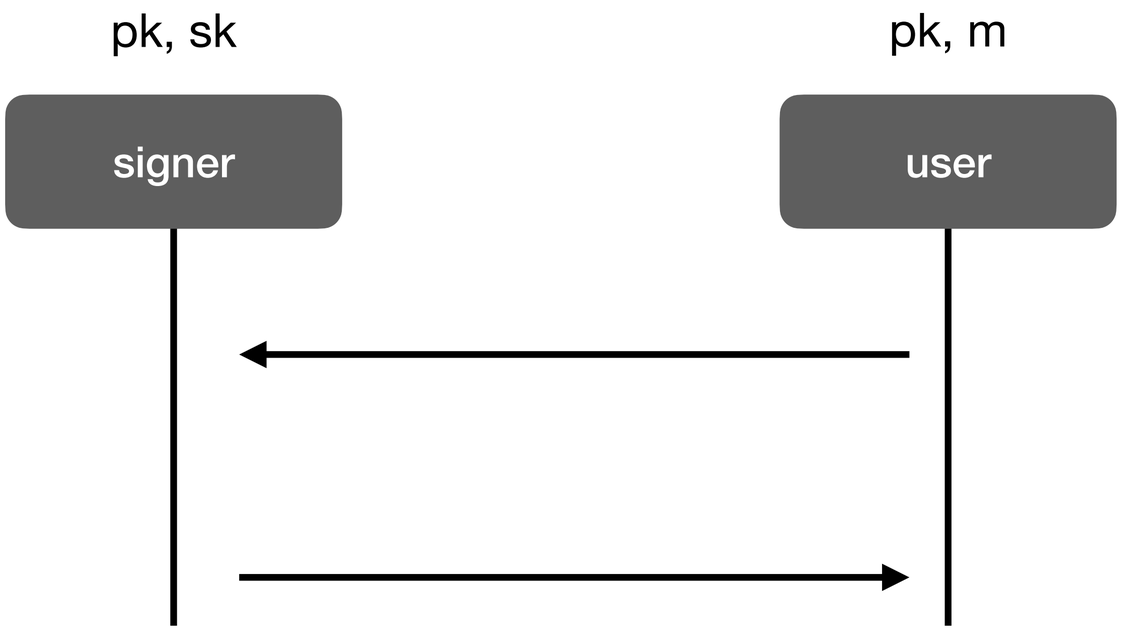
- interactive signing protocol
- privacy guarantees

Applications:

- e-cash, e-voting, anonymous credentials
- authentication tokens, blockchain

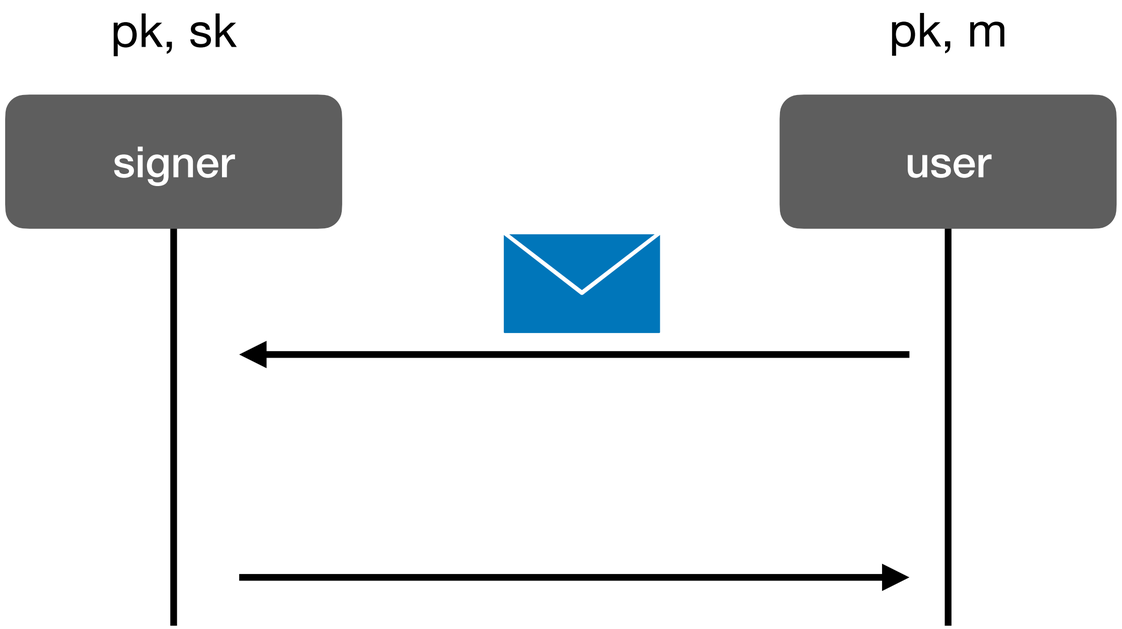
Definition

Round Optimal



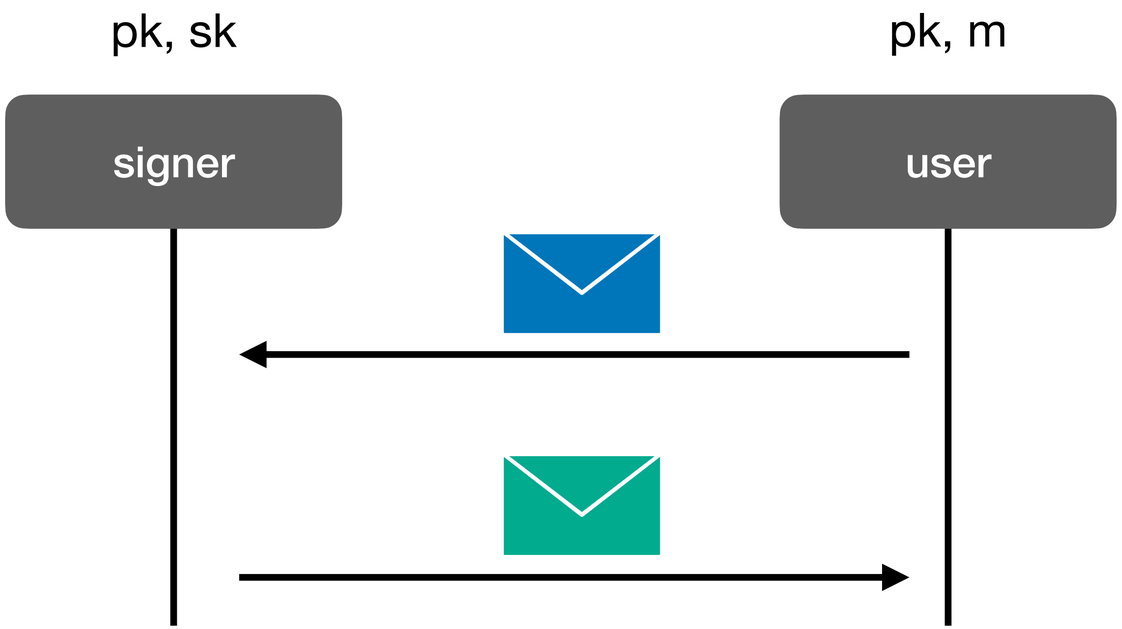
Definition

Round Optimal



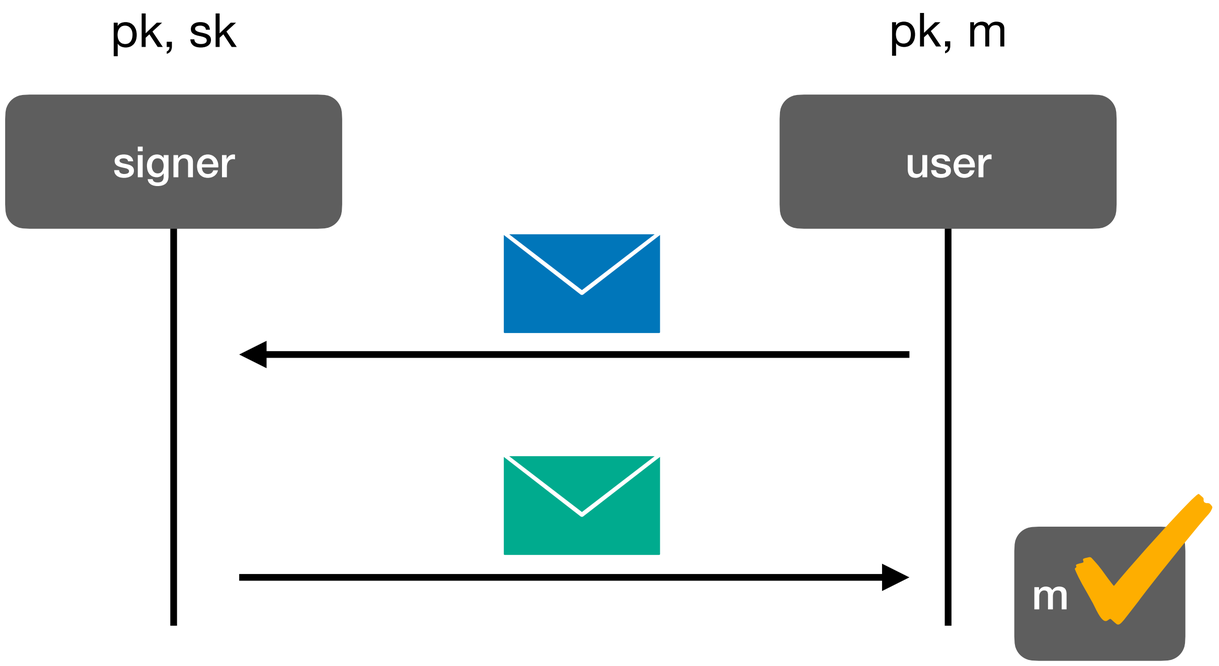
Definition

Round Optimal



Definition

Round Optimal



Security

Correctness:

- honest signatures verify

Security

Correctness:

- honest signatures verify

Blindness:

- signatures unlinkable to signing sessions

Security

Correctness:

- honest signatures verify

Blindness:

- signatures unlinkable to signing sessions

One-more Unforgeability:

- can obtain at most Q signatures from Q sessions

This Work

Goals:

This Work

Goals:

- *number of rounds:* round-optimal

This Work

Goals:

- *number of rounds:* round-optimal
- *signature size:* compact

This Work

Goals:

- *number of rounds:* round-optimal
- *signature size:* compact
- *security assumptions:* standard assumptions + ROM

Related Works

Blind Signatures in the ROM under standard assumptions

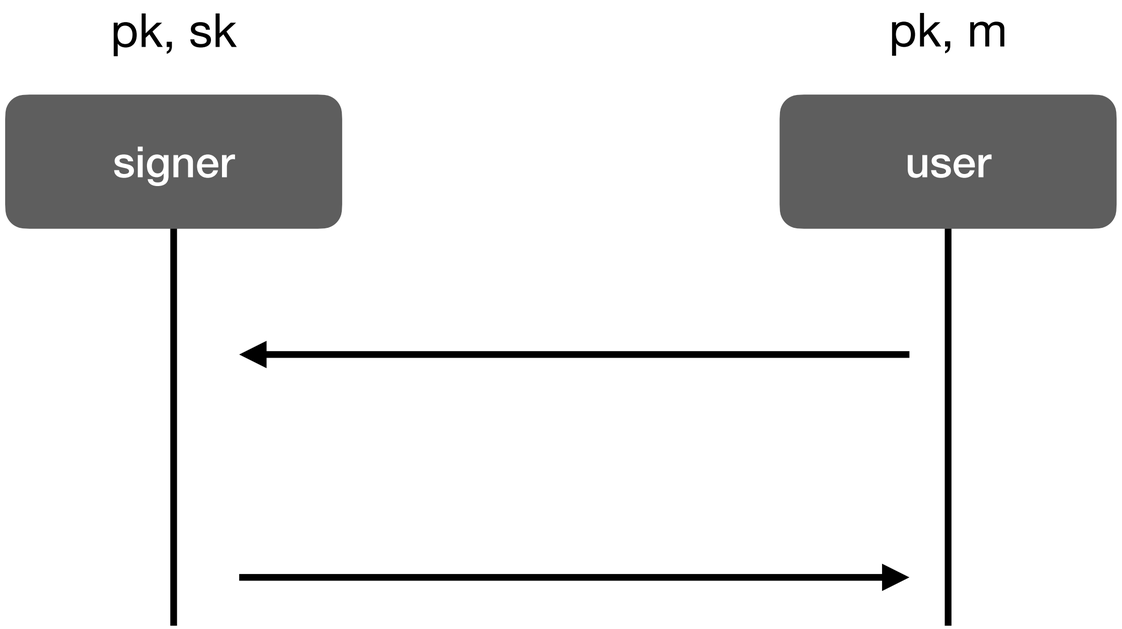
Reference	Signature Size	Communication Size	Assumption
[dK22]	100 KB	850 KB	DSMR, MLWE, MSIS
[BFP13]	96 B	220 KB	SXDH, CDH
[AJOR18]	5.5 KB	1 KB	SXDH
[HLW23]	5 KB 9 KB	72 KB 36 KB	CDH
?	?	?	?

Framework 1:

Fischlin with Rewinding

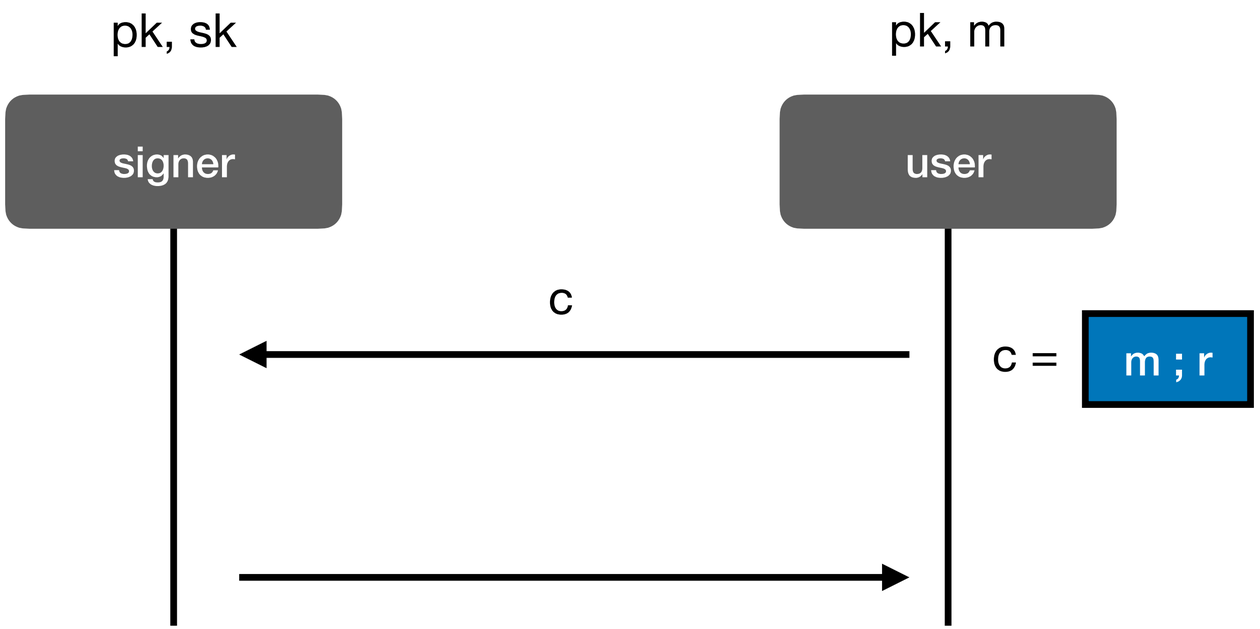
Fischlin

Framework [F06]



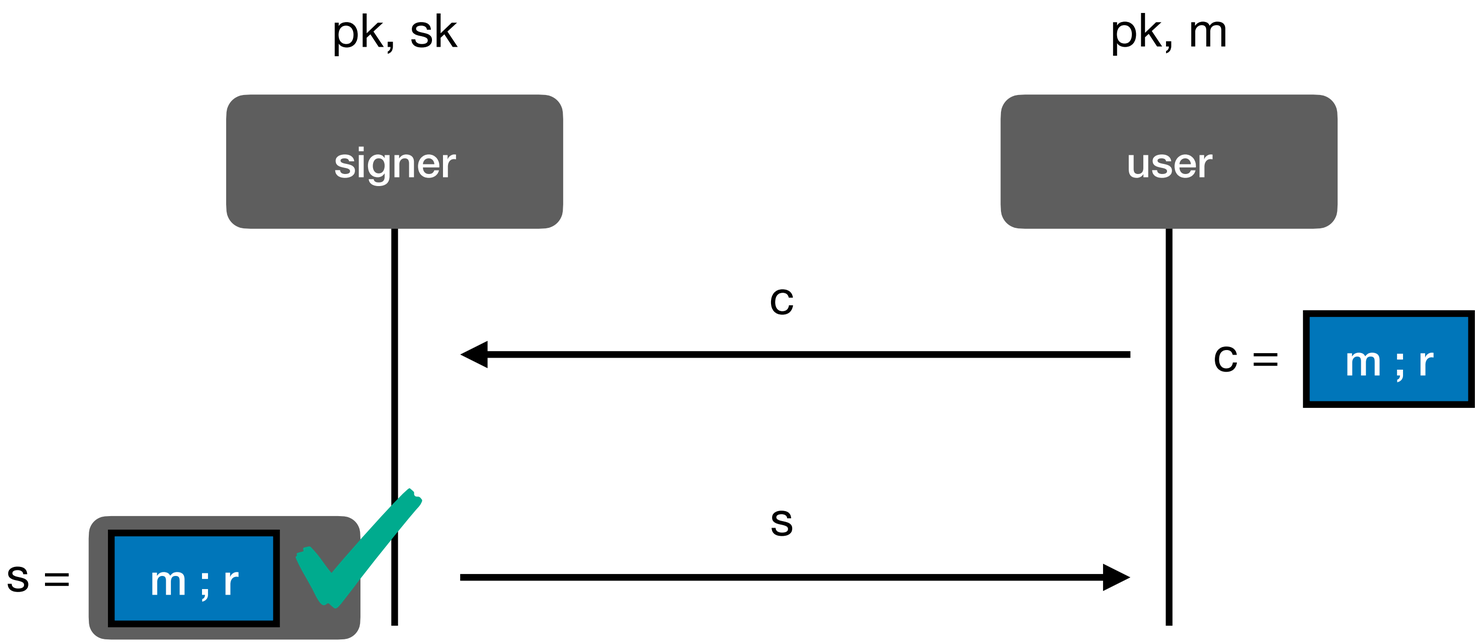
Fischlin

Framework [F06]



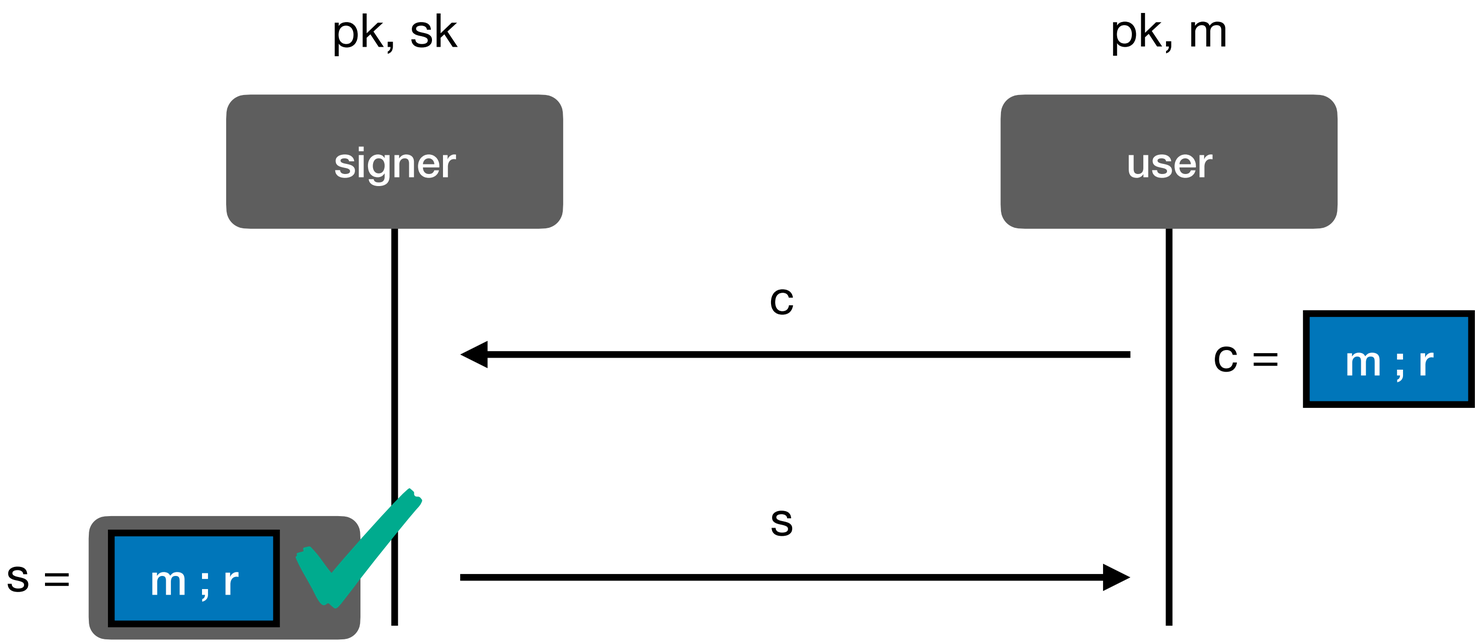
Fischlin

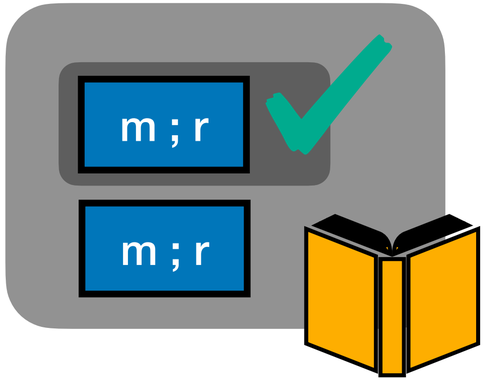
Framework [F06]



Fischlin

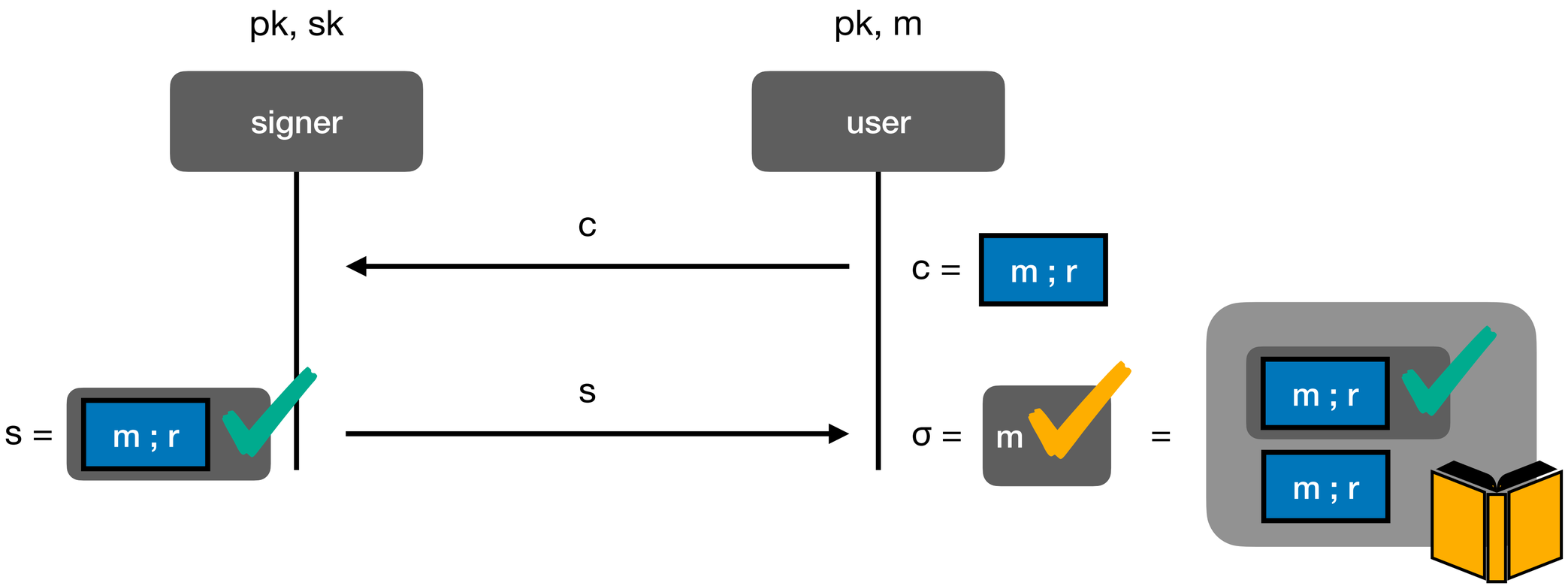
Framework [F06]





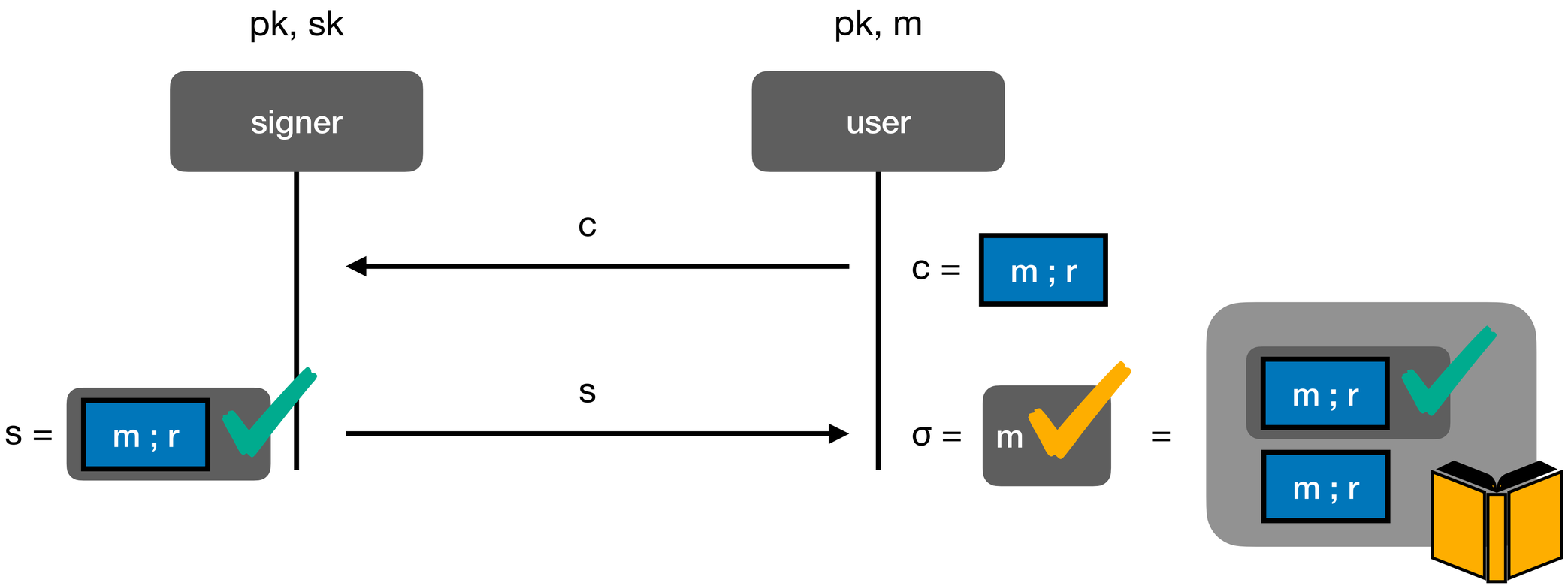
Fischlin

Framework [F06]



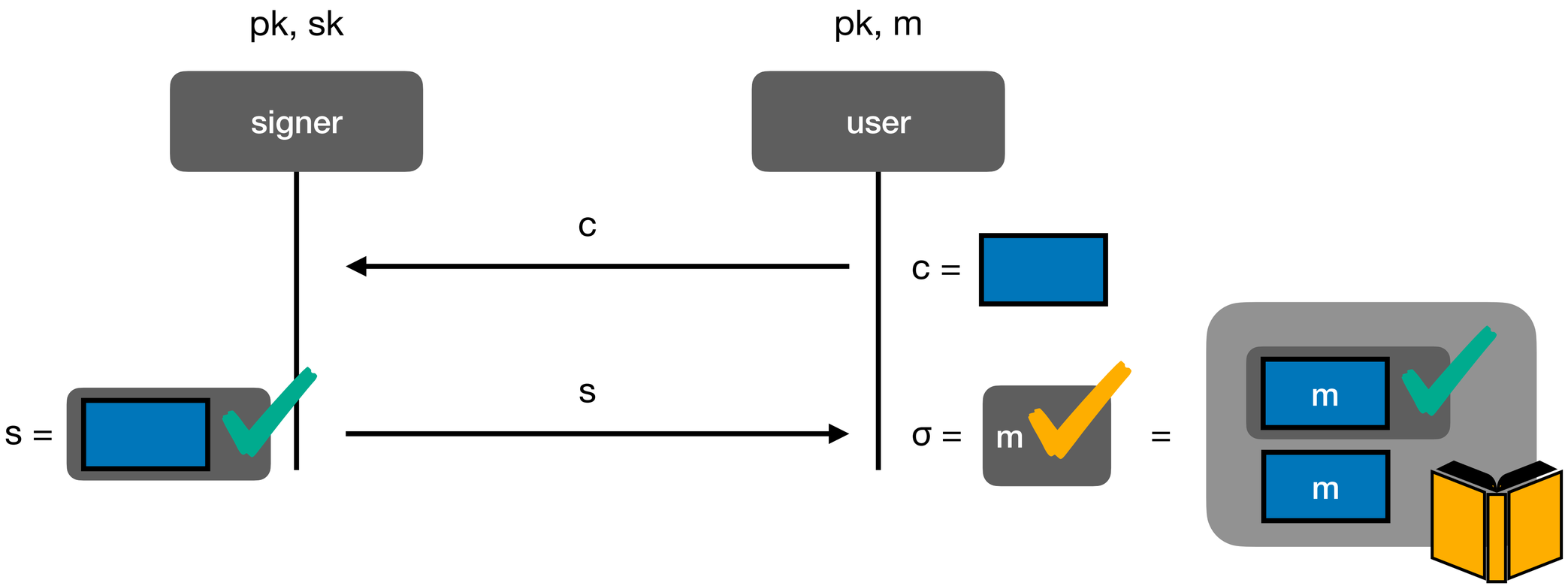
Fischlin

Correctness



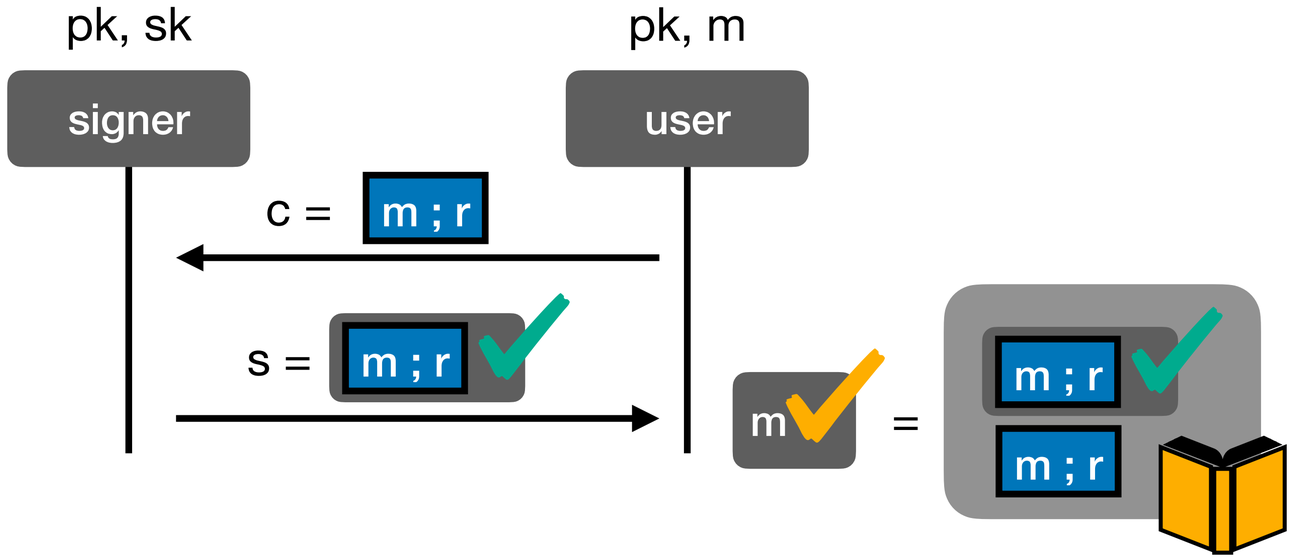
Fischlin

Blindness



Fischlin

One-more Unforgeability

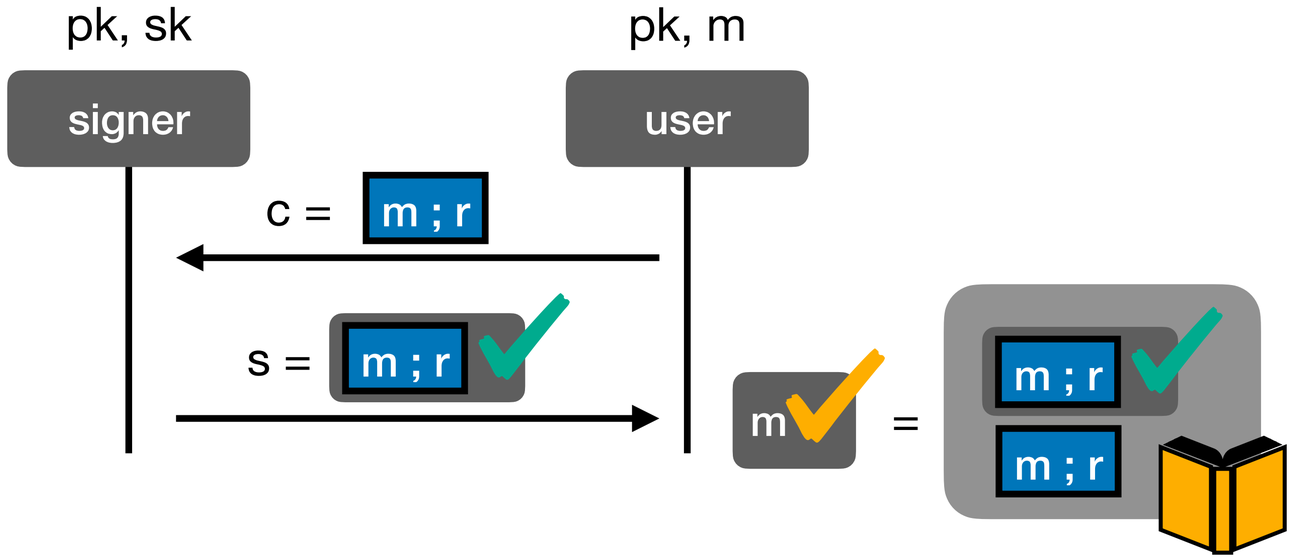


Instantiation:

- NIZK with online-extraction

Fischlin

One-more Unforgeability



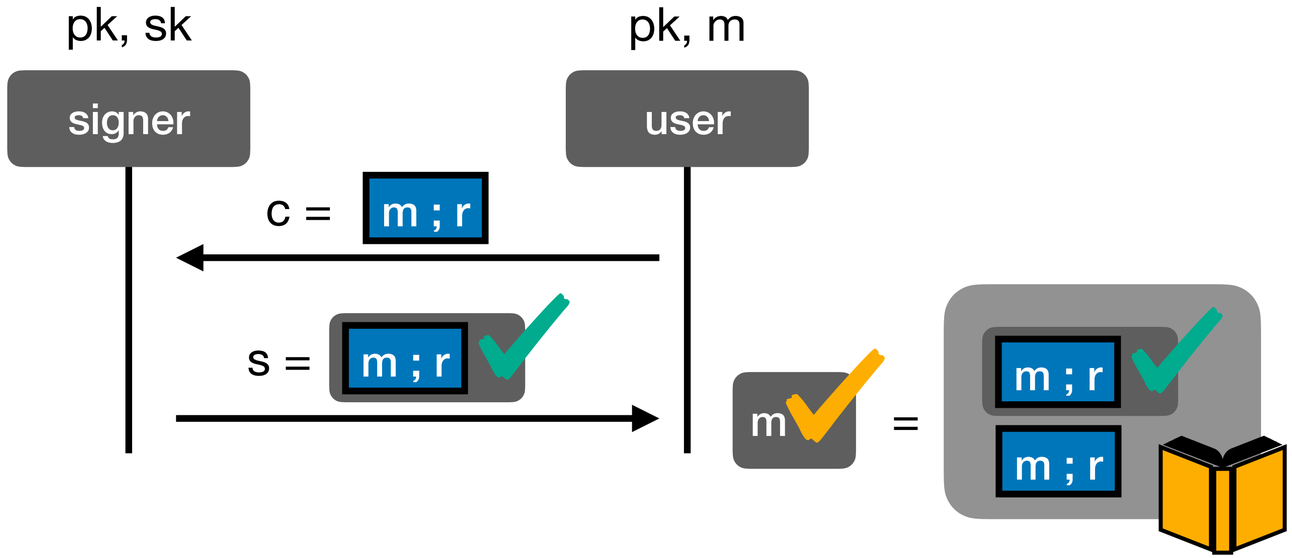
Instantiation:

- NIZK with online-extraction

Proof sketch:

Fischlin

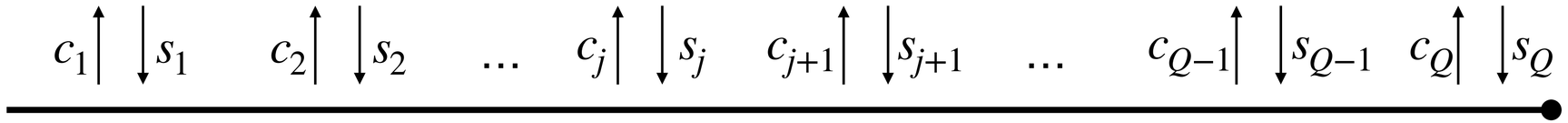
One-more Unforgeability



Instantiation:

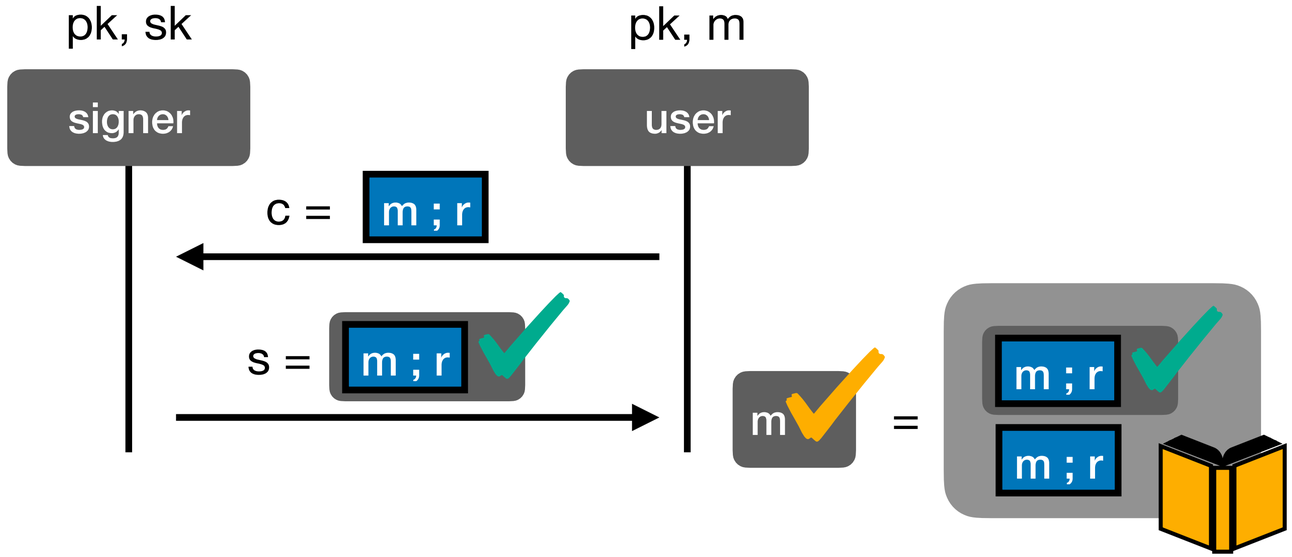
- NIZK with online-extraction

Proof sketch:



Fischlin

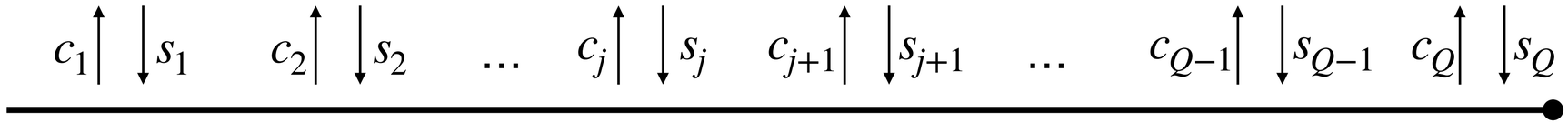
One-more Unforgeability

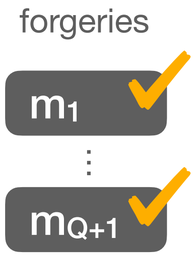


Instantiation:

- NIZK with online-extraction

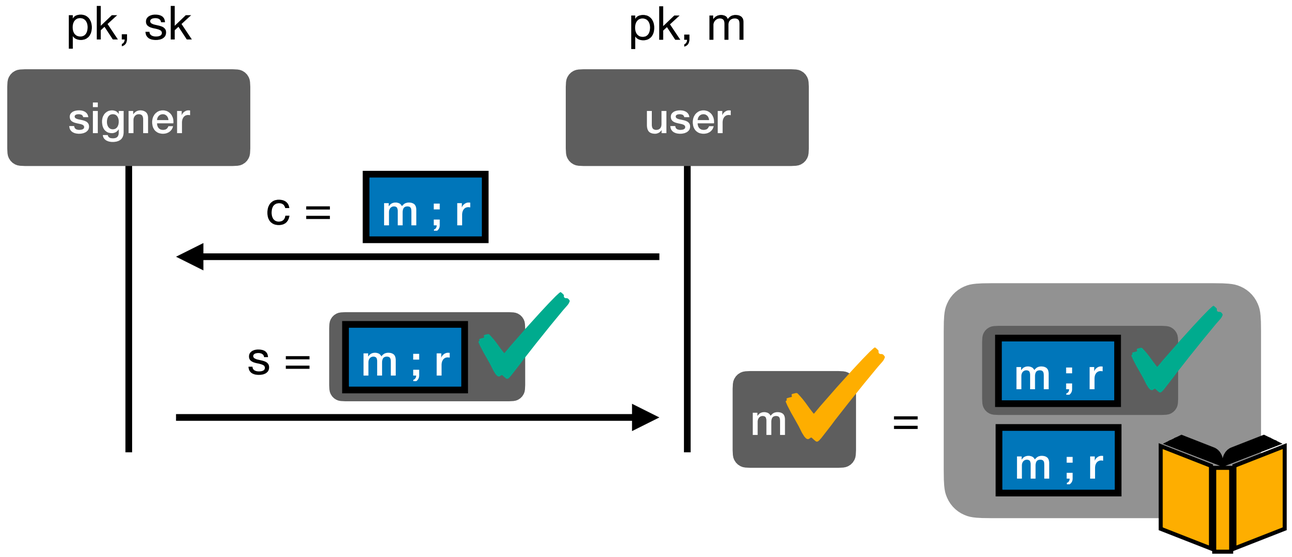
Proof sketch:





Fischlin

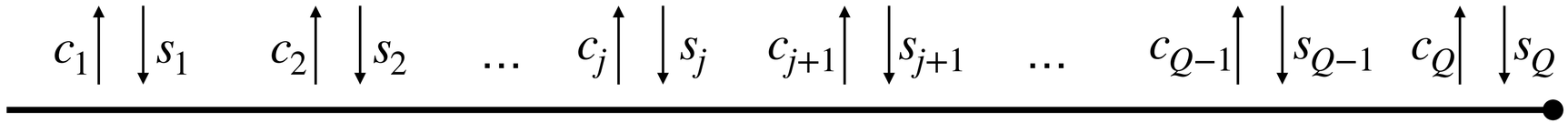
One-more Unforgeability

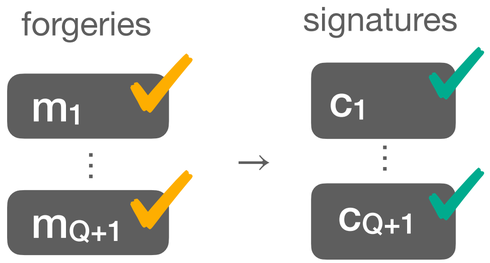


Instantiation:

- NIZK with online-extraction

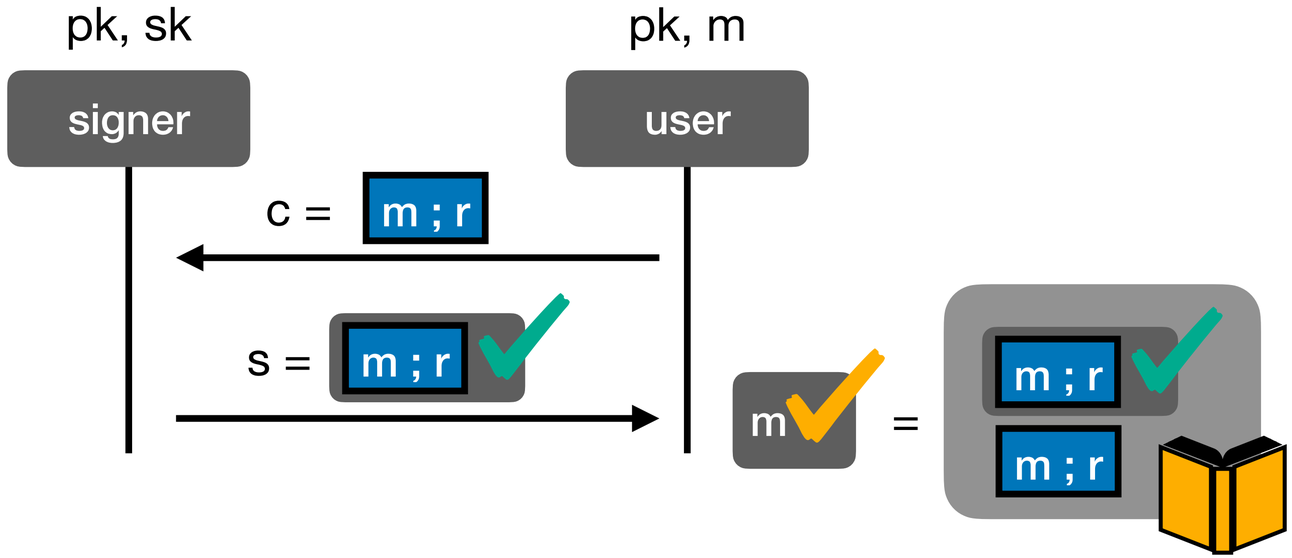
Proof sketch:





Fischlin

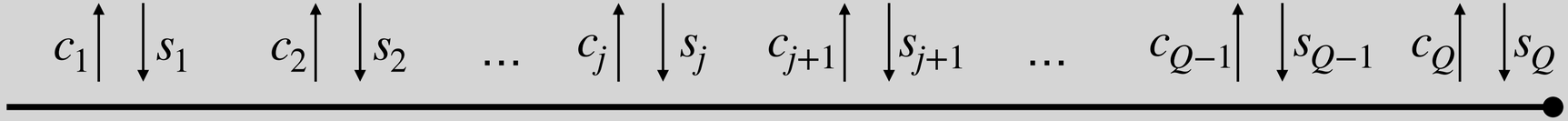
One-more Unforgeability



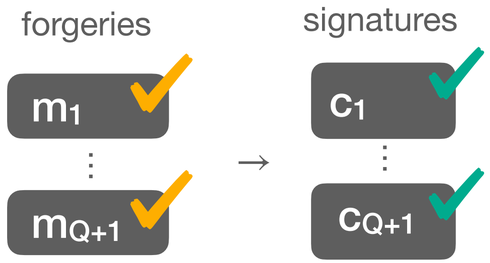
Instantiation:

- NIZK with online-extraction

Proof sketch:

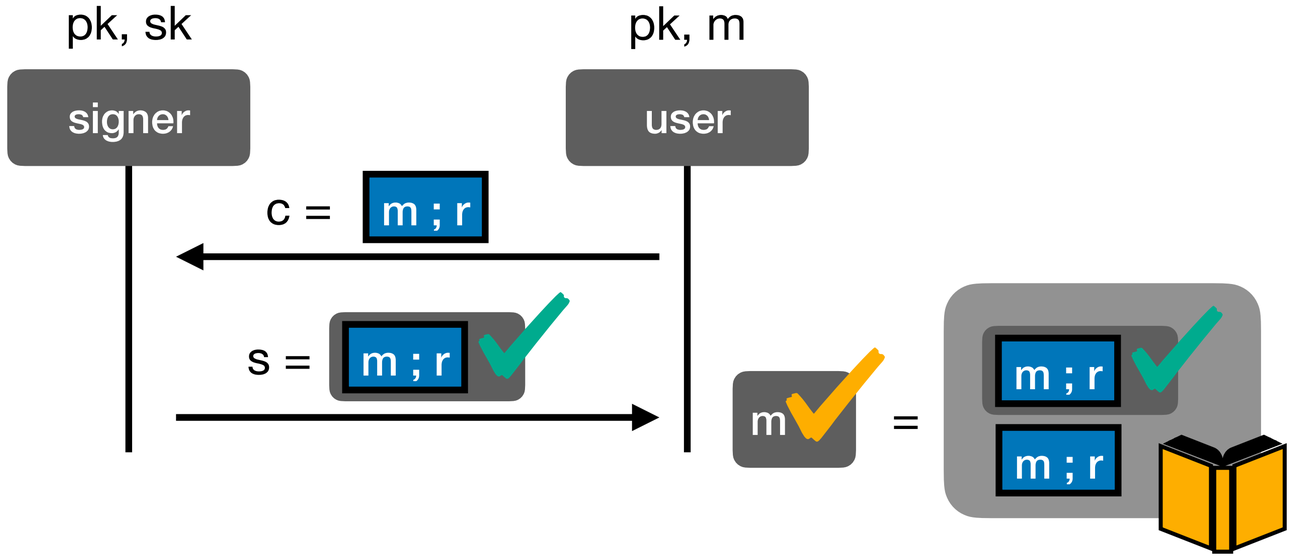


signed at most Q commitments



Fischlin

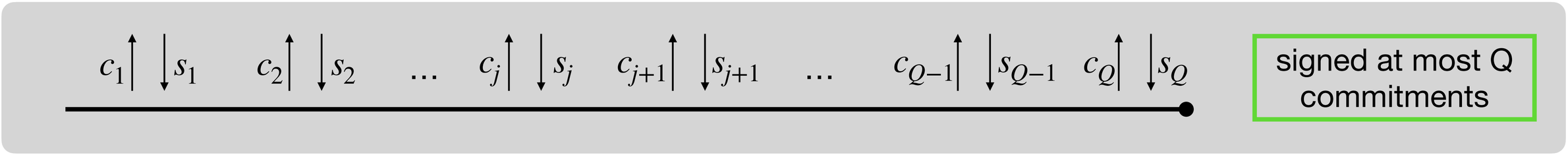
One-more Unforgeability

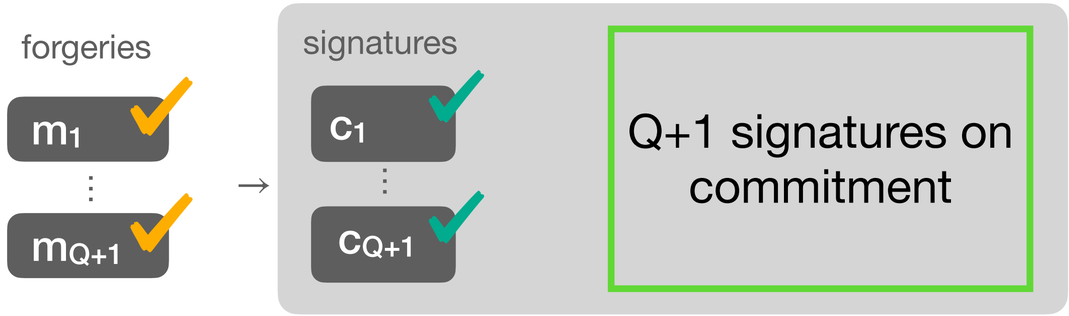


Instantiation:

- NIZK with online-extraction

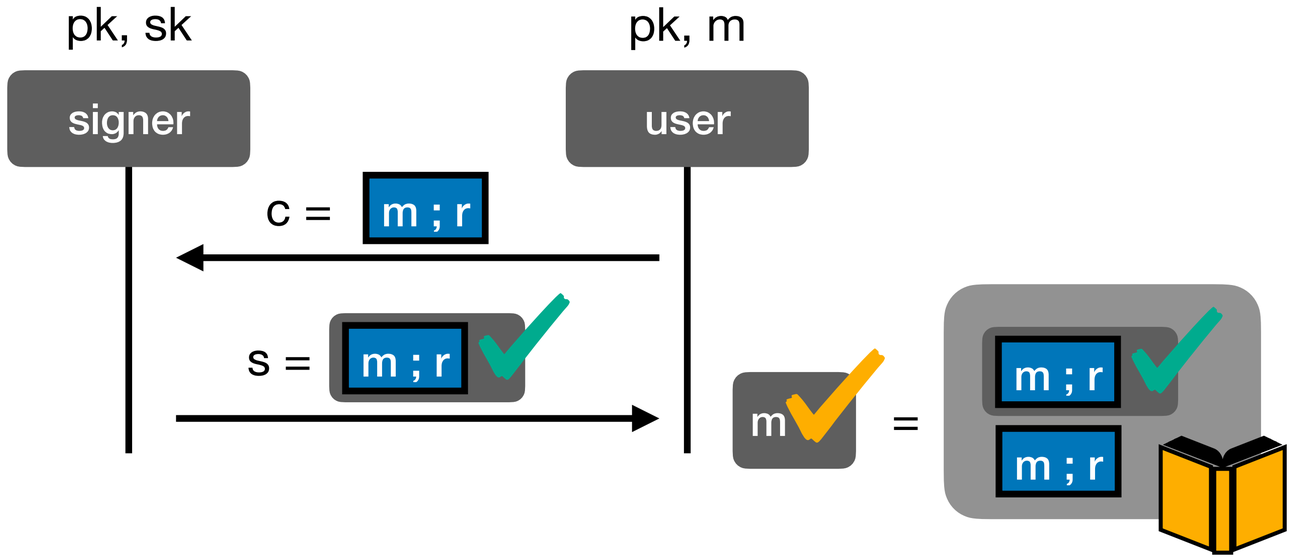
Proof sketch:





Fischlin

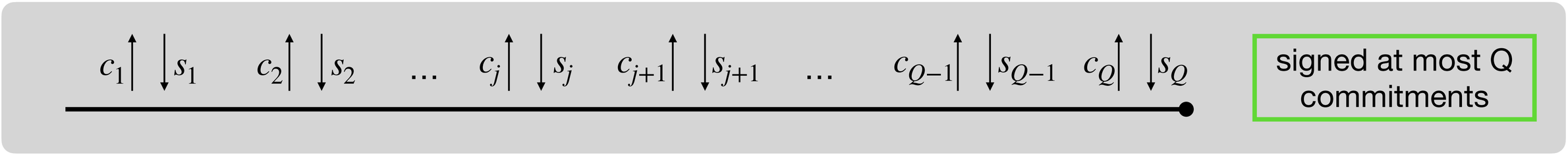
One-more Unforgeability

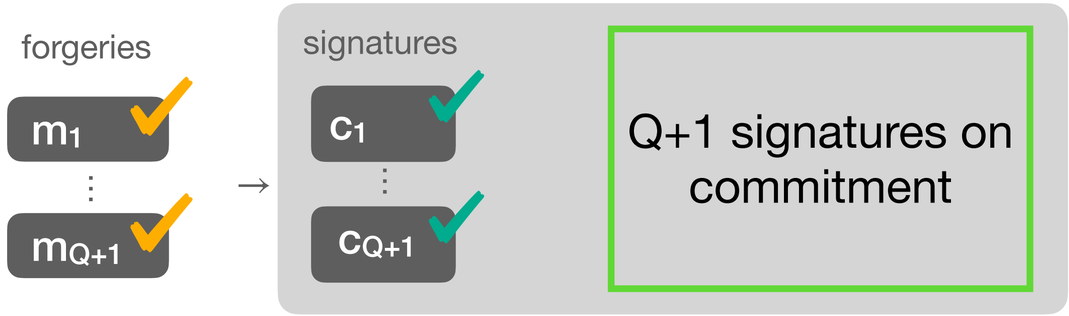


Instantiation:

- NIZK with online-extraction

Proof sketch:



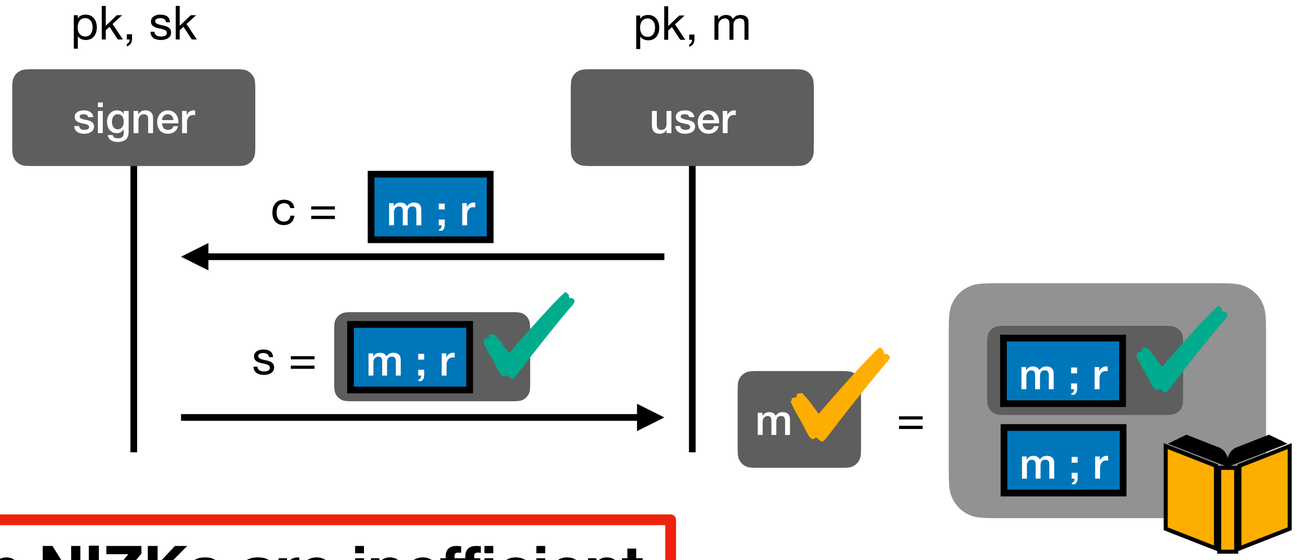


breaks either:

- binding
- unforgeability

Fischlin

One-more Unforgeability

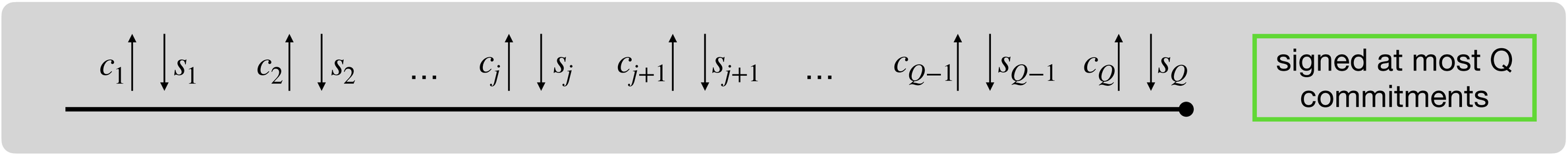


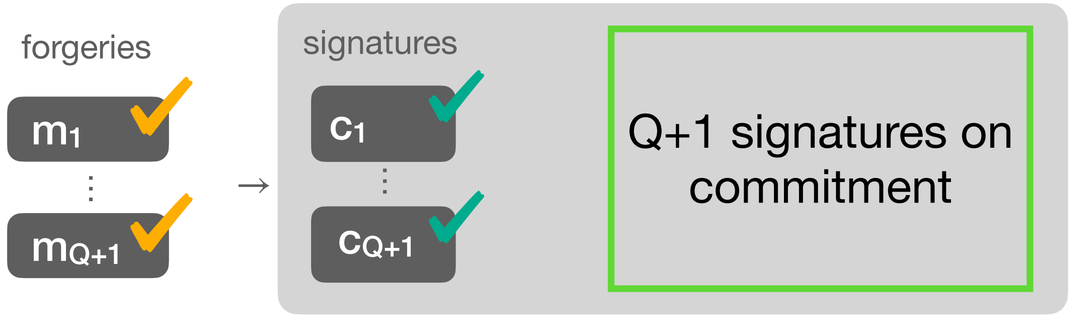
Instantiation:

- NIZK with online-extraction

Known NIZKs are inefficient

Proof sketch:



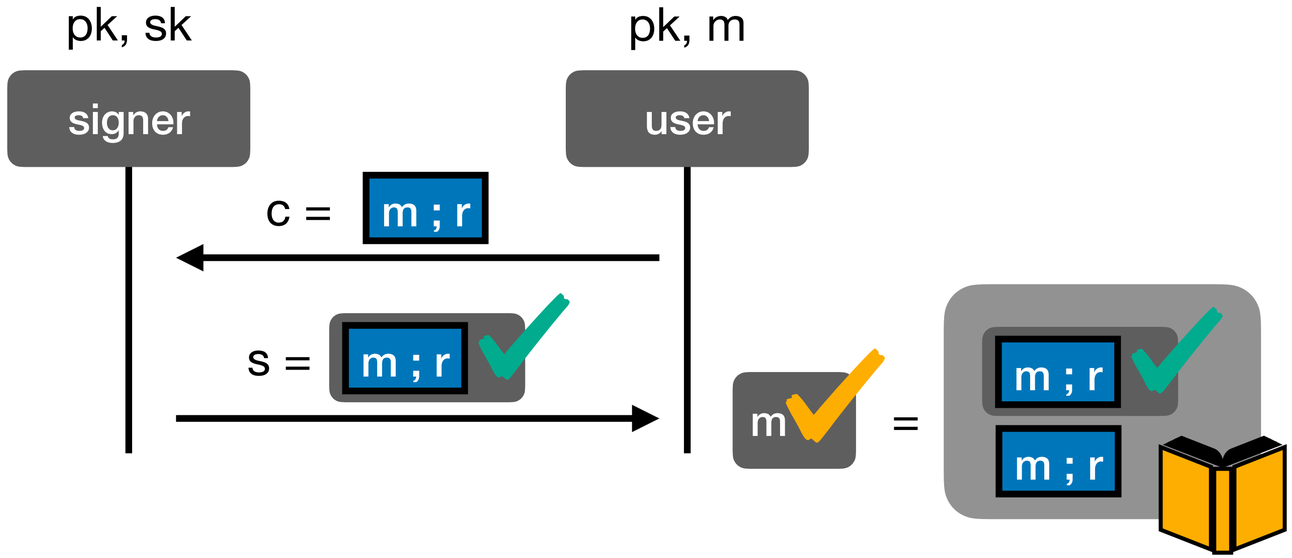


breaks either:

- binding
- unforgeability

Fischlin

One-more Unforgeability

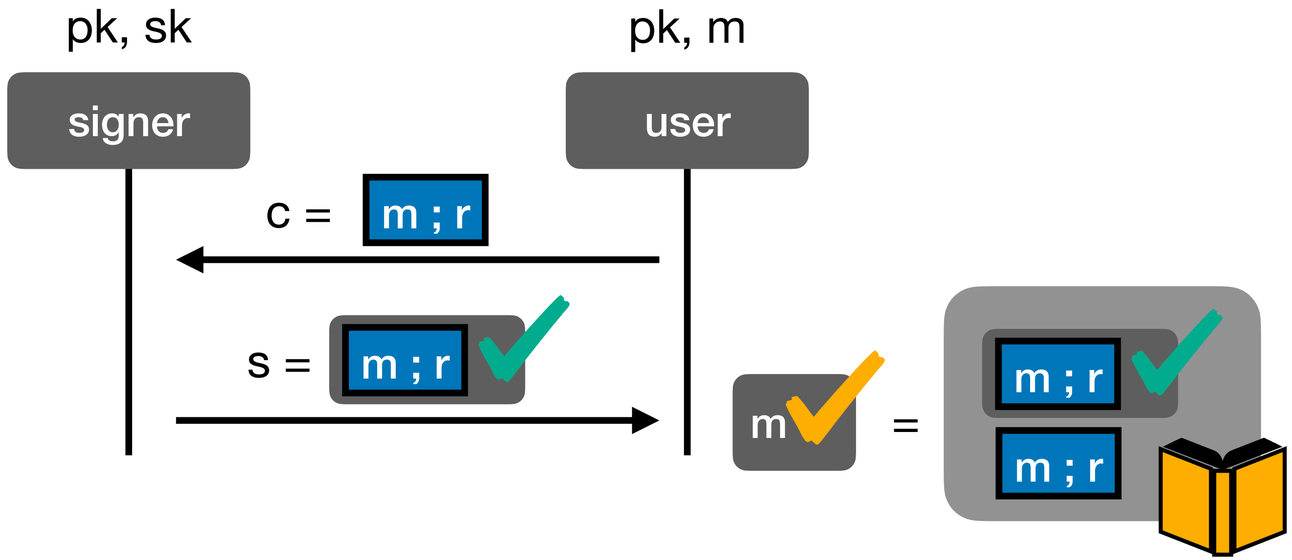


Instantiation:

- Rewinding-based NIZK

Fischlin

One-more Unforgeability



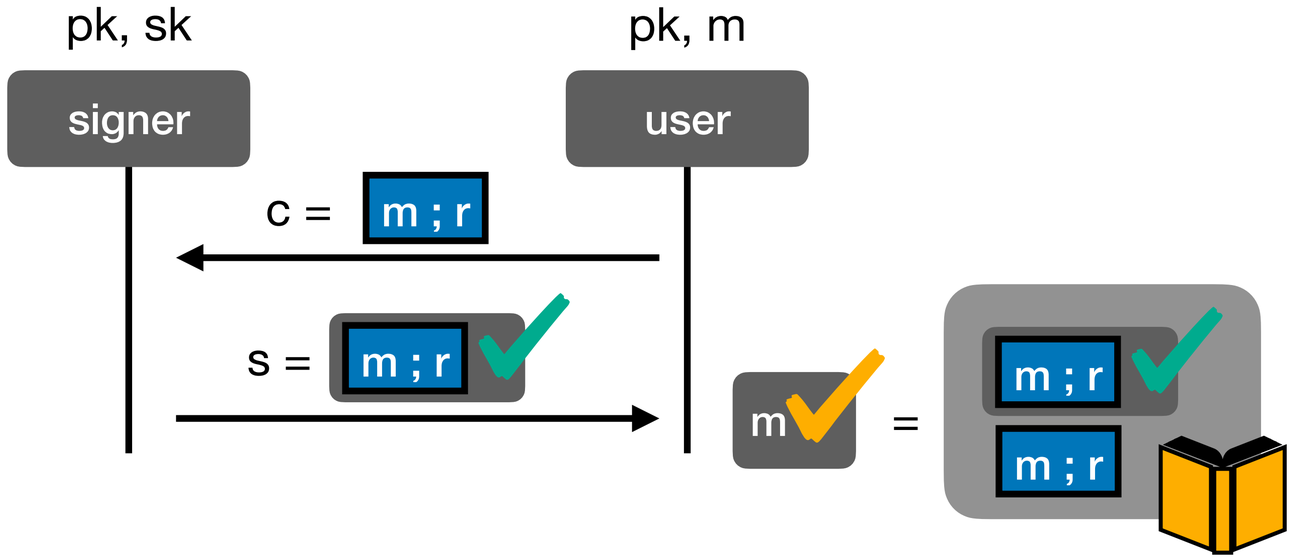
Instantiation:

- Rewinding-based NIZK

Problem:

Fischlin

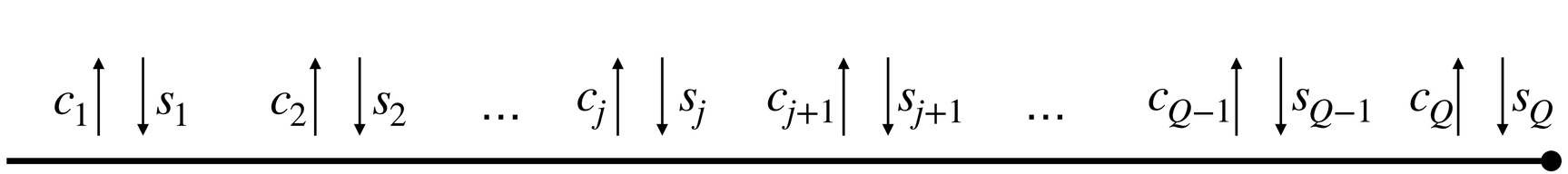
One-more Unforgeability



Instantiation:

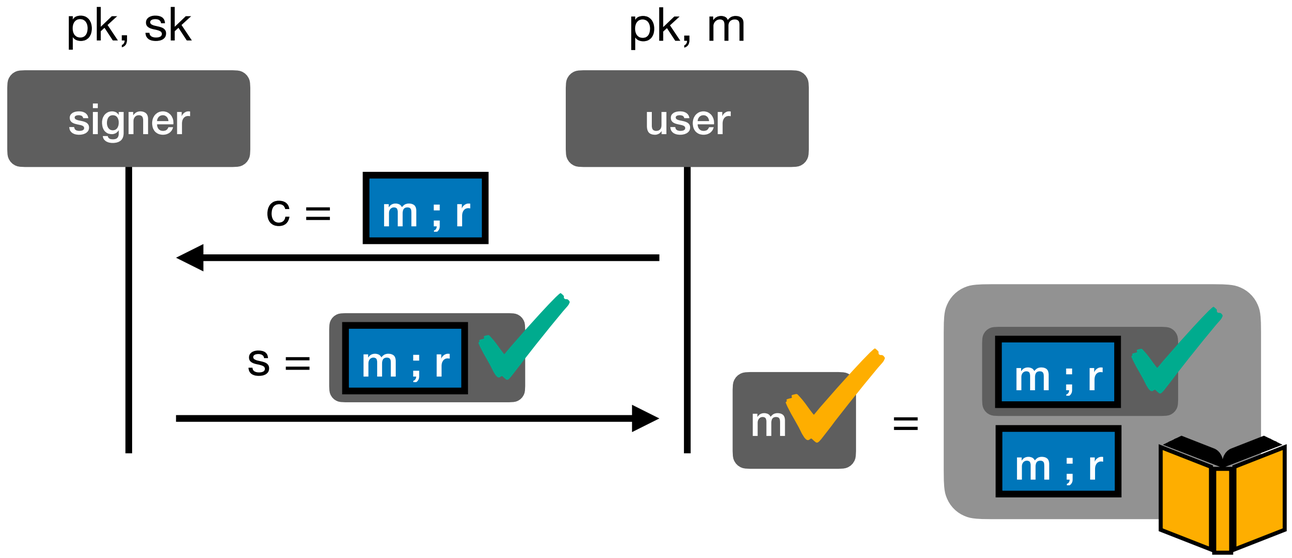
- Rewinding-based NIZK

Problem:



Fischlin

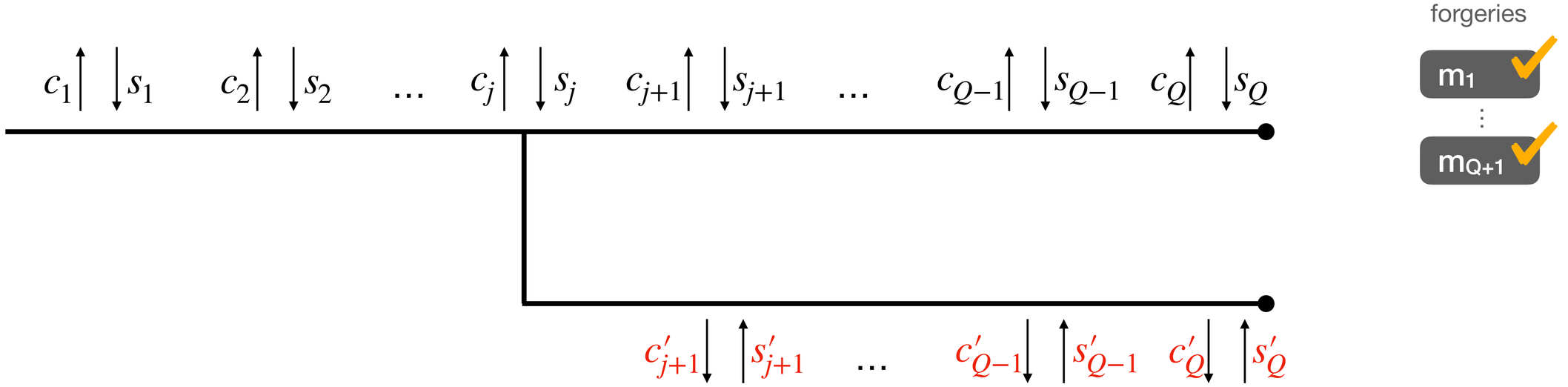
One-more Unforgeability



Instantiation:

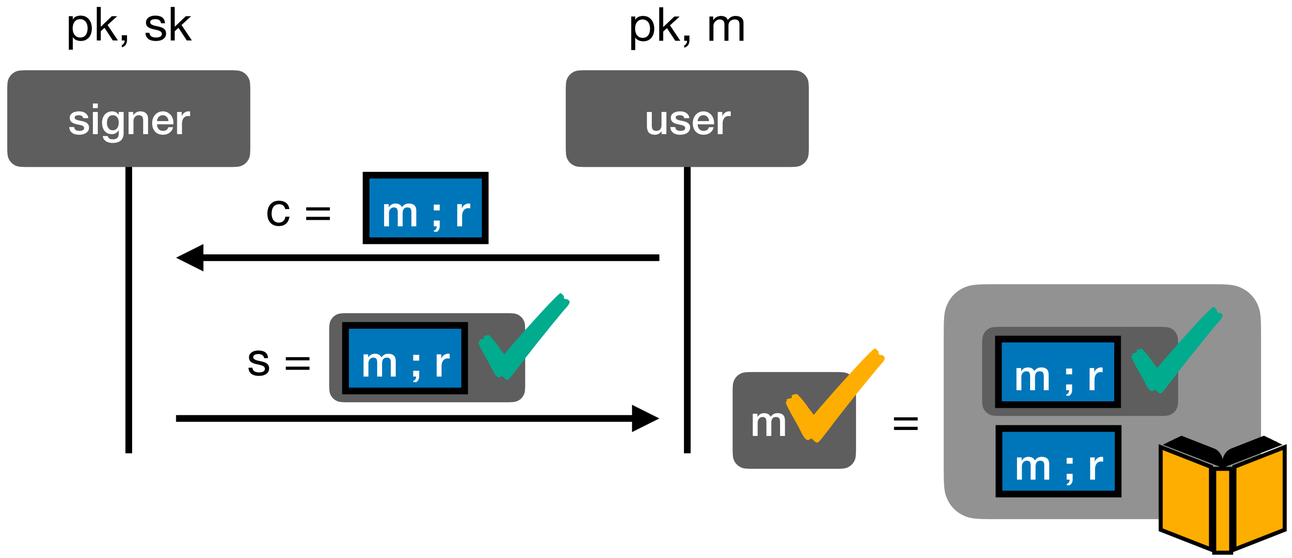
- Rewinding-based NIZK

Problem:



Fischlin

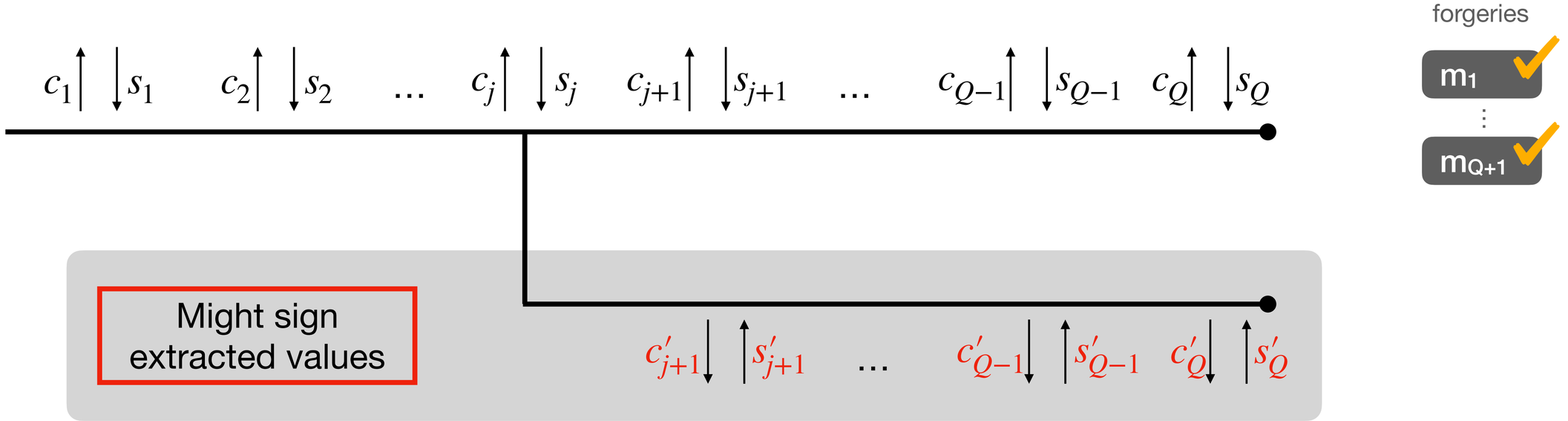
One-more Unforgeability



Instantiation:

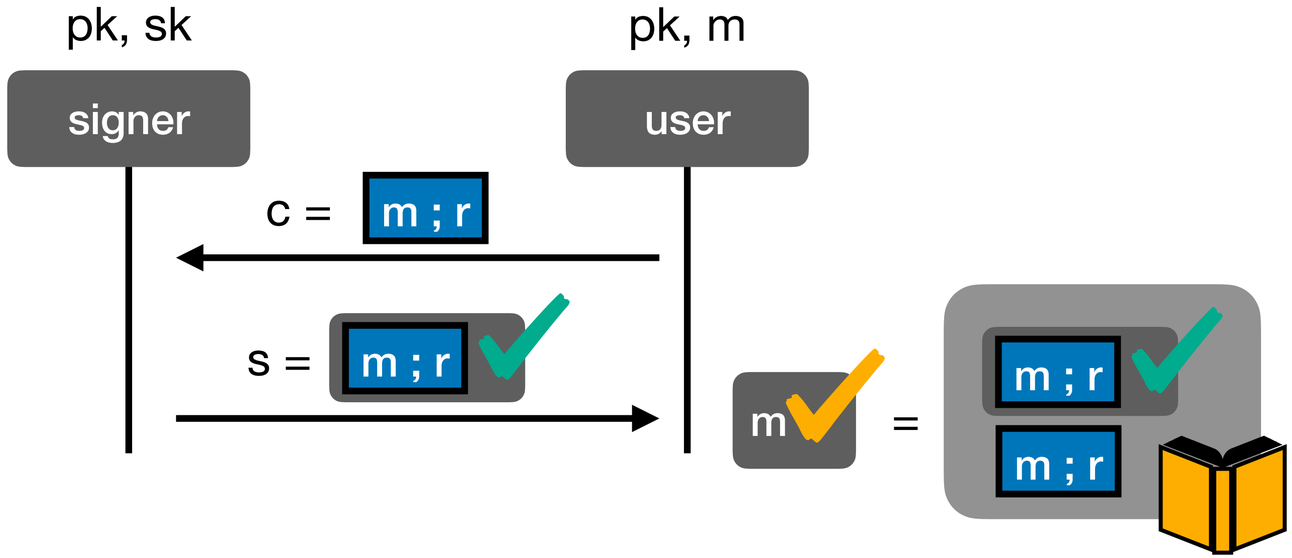
- Rewinding-based NIZK

Problem:



Fischlin

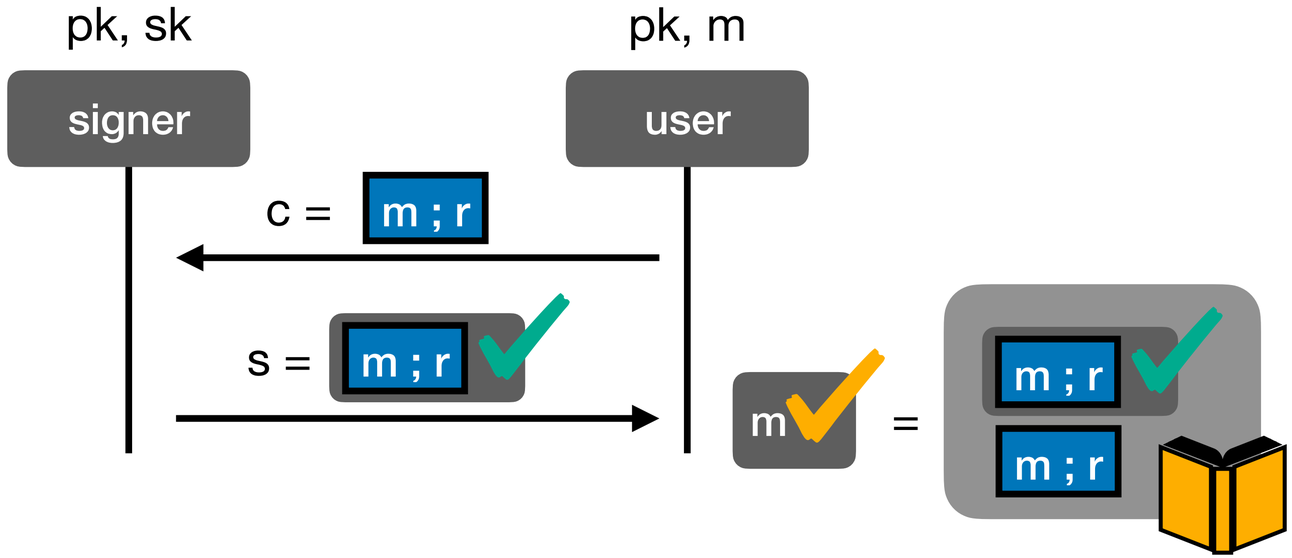
One-more Unforgeability



Fischlin

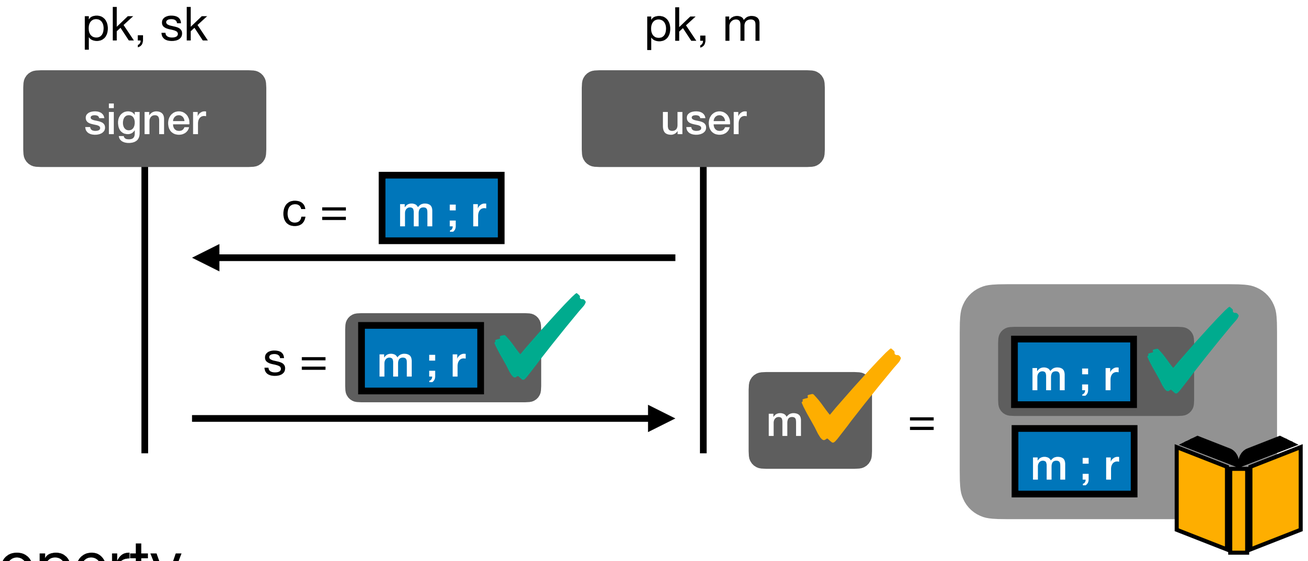
One-more Unforgeability

Idea:



Fischlin

One-more Unforgeability

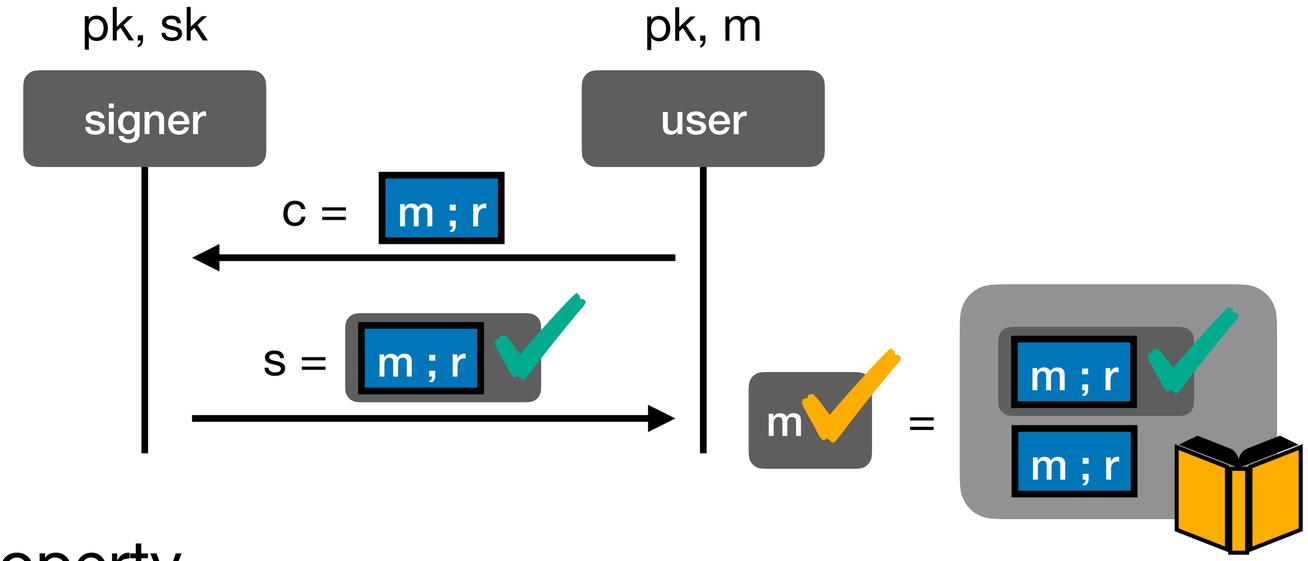


Idea:

1. Use NIZK with *unique* extraction property

Fischlin

One-more Unforgeability



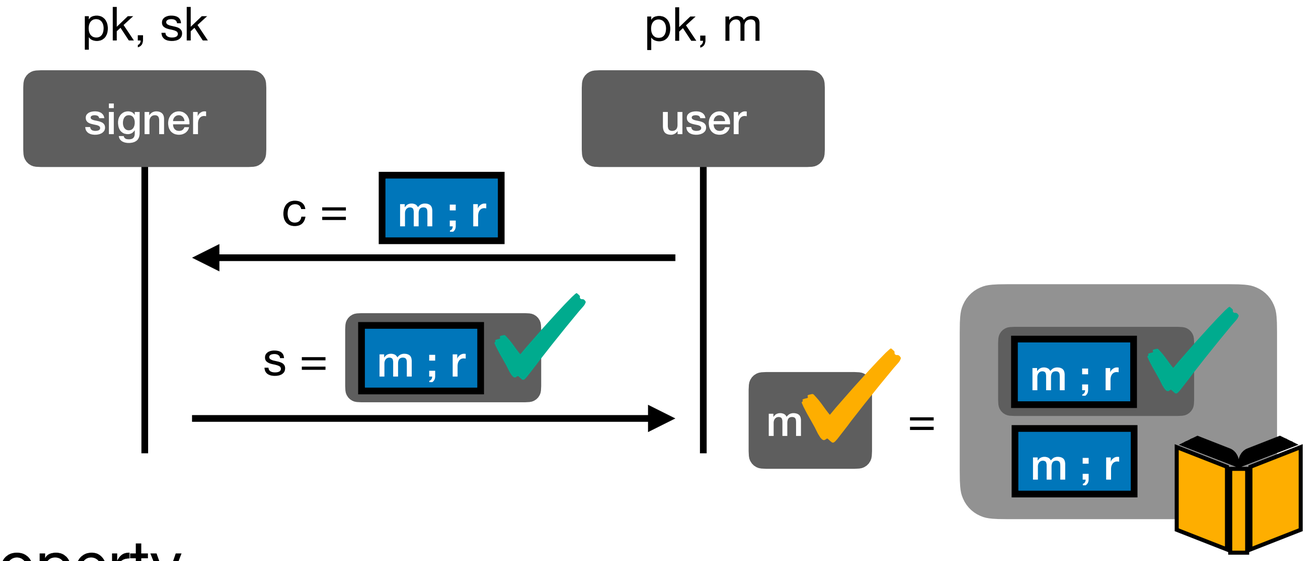
Idea:

1. Use NIZK with *unique* extraction property

➡ NIZK fixes commitments $c_1, \cdots, c_{Q+1}$ statistically

Fischlin

One-more Unforgeability



Idea:

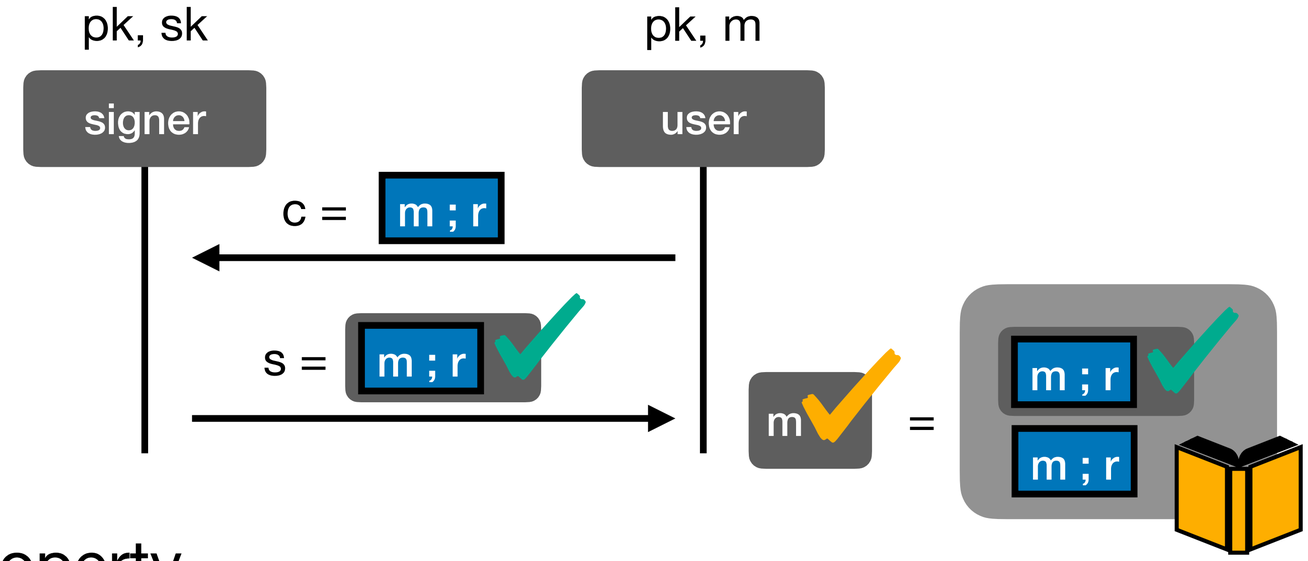
1. Use NIZK with *unique* extraction property

   ➡ NIZK fixes commitments $c_1, \cdots, c_{Q+1}$ statistically

2. Sign pre-randomized commitments Rand(c, rnd) instead

Fischlin

One-more Unforgeability



Idea:

1. Use NIZK with *unique* extraction property

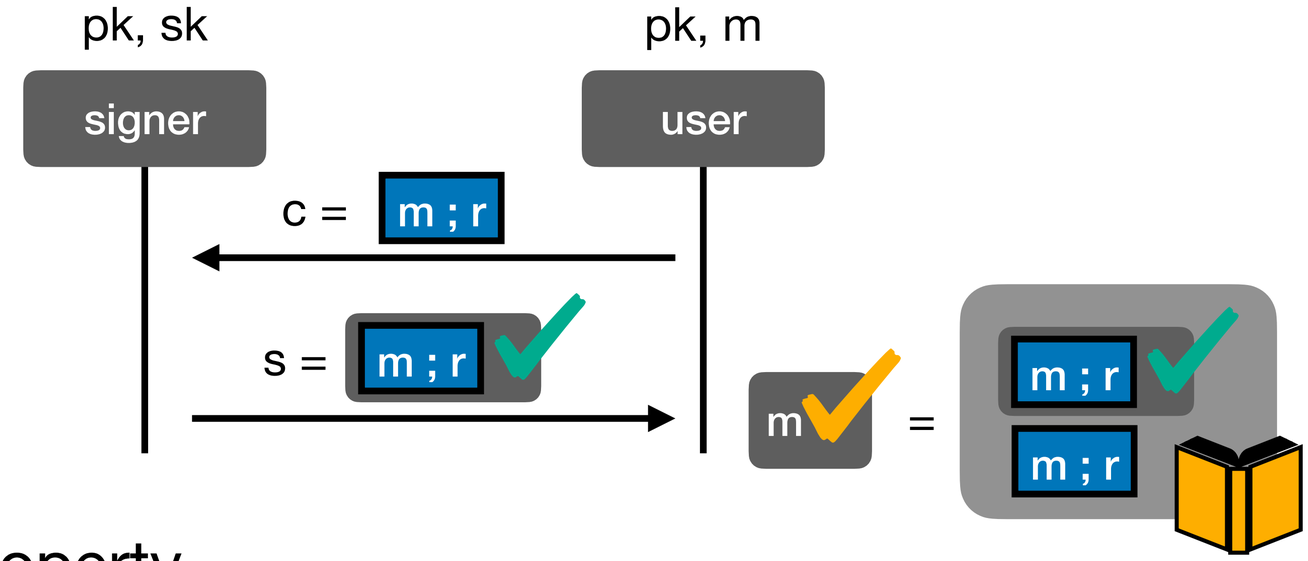
   ➡ NIZK fixes commitments $c_1, \cdots, c_{Q+1}$ statistically

2. Sign pre-randomized commitments Rand(c, rnd) instead

   ➡ unlikely that we sign a fixed value in second run

Fischlin

One-more Unforgeability



Idea:

1. Use NIZK with *unique* extraction property

   ➡ NIZK fixes commitments $c_1, \cdots, c_{Q+1}$ statistically

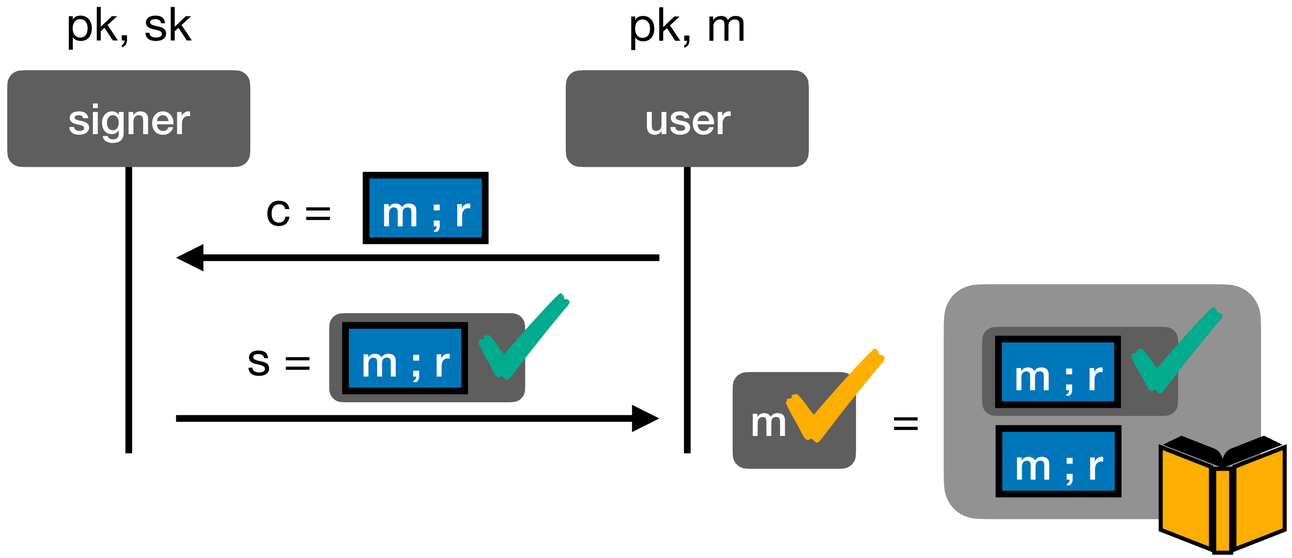
2. Sign pre-randomized commitments Rand(c, rnd) instead

   ➡ unlikely that we sign a fixed value in second run

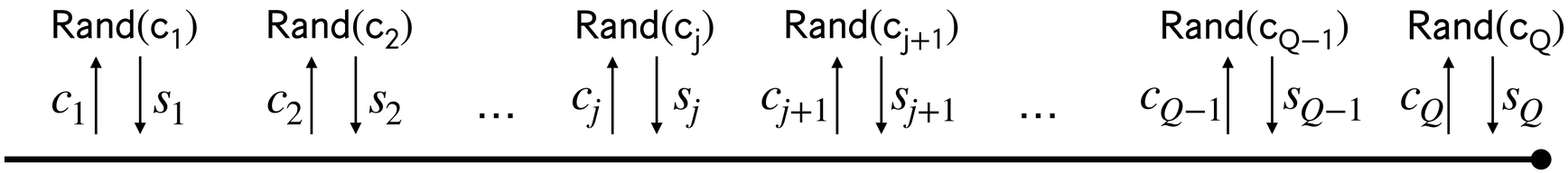
   - alternative: sign c || rnd

Fischlin

One-more Unforgeability

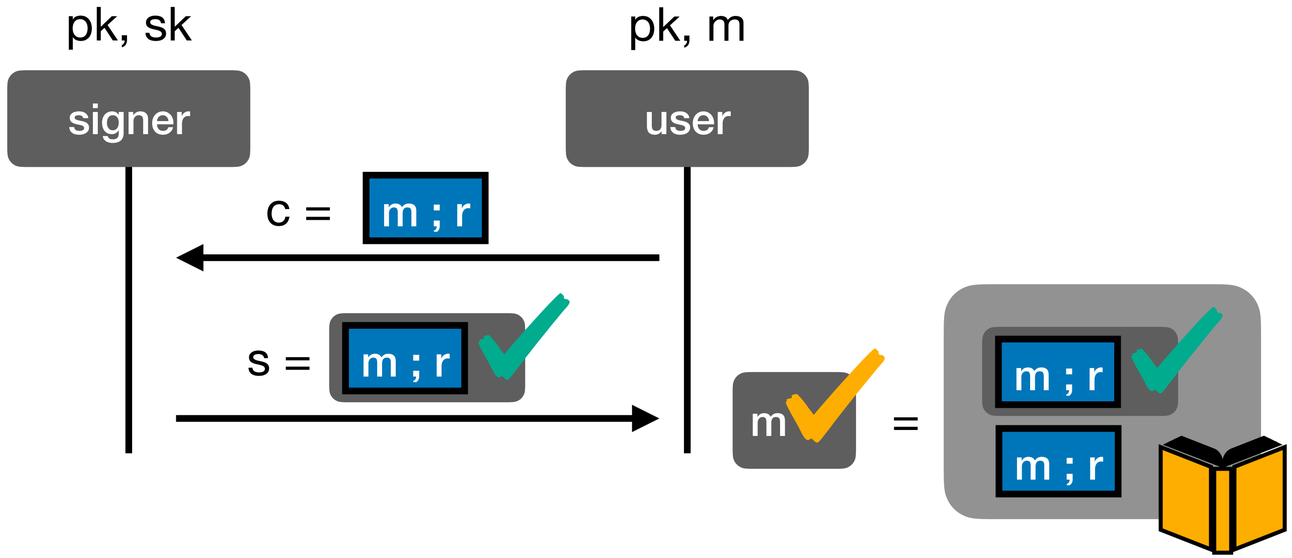


Sketch:

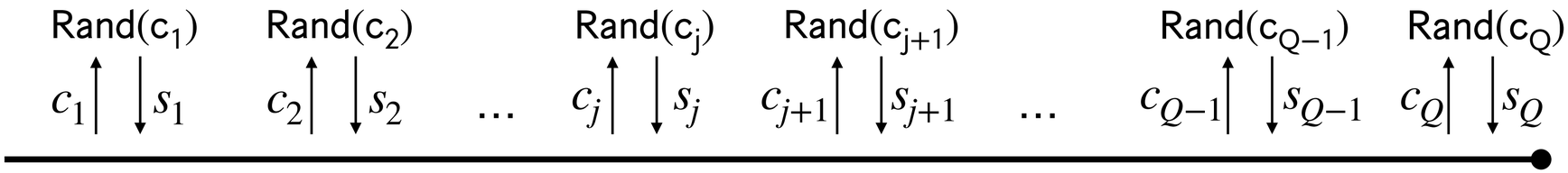


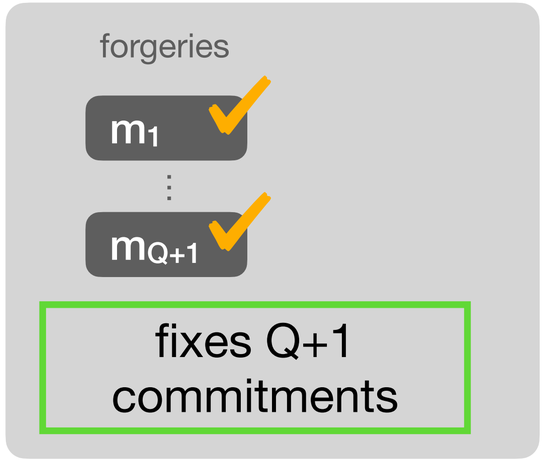
Fischlin

One-more Unforgeability



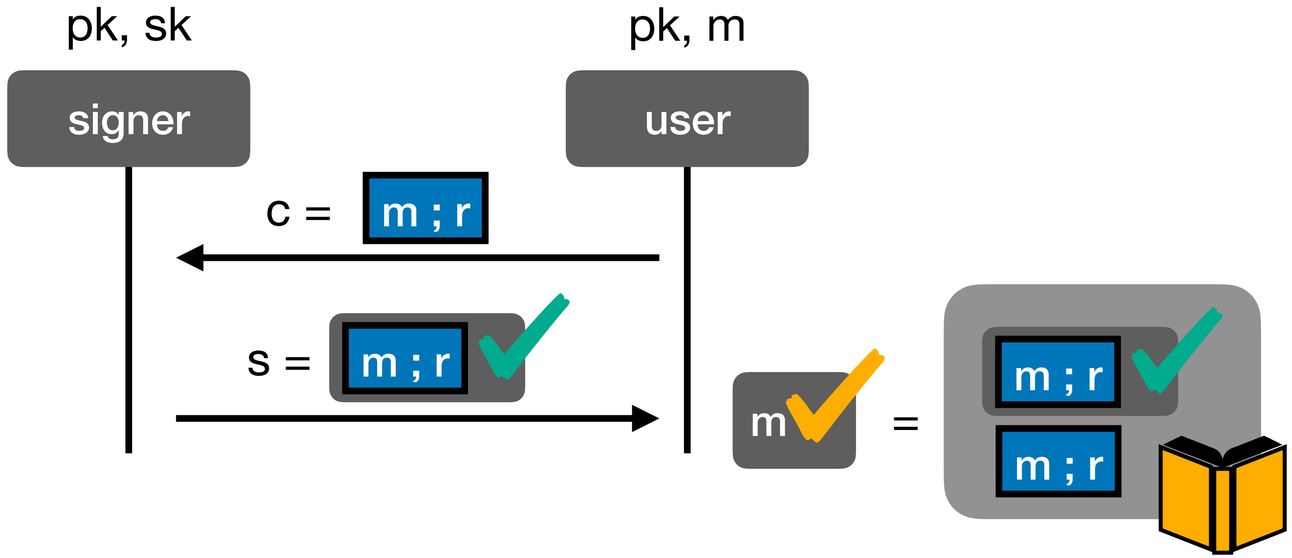
Sketch:



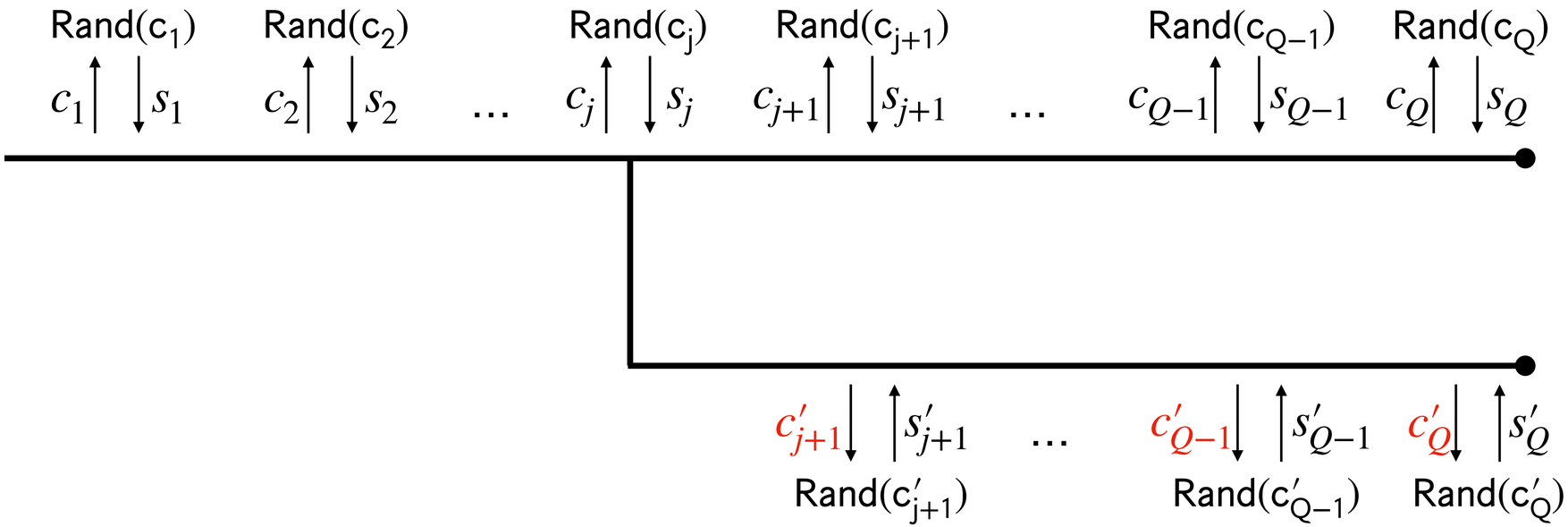


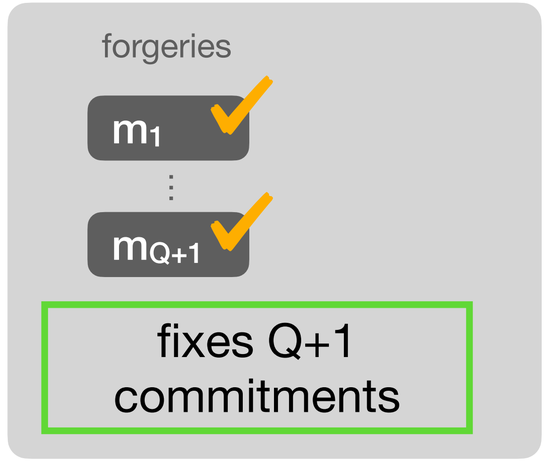
Fischlin

One-more Unforgeability



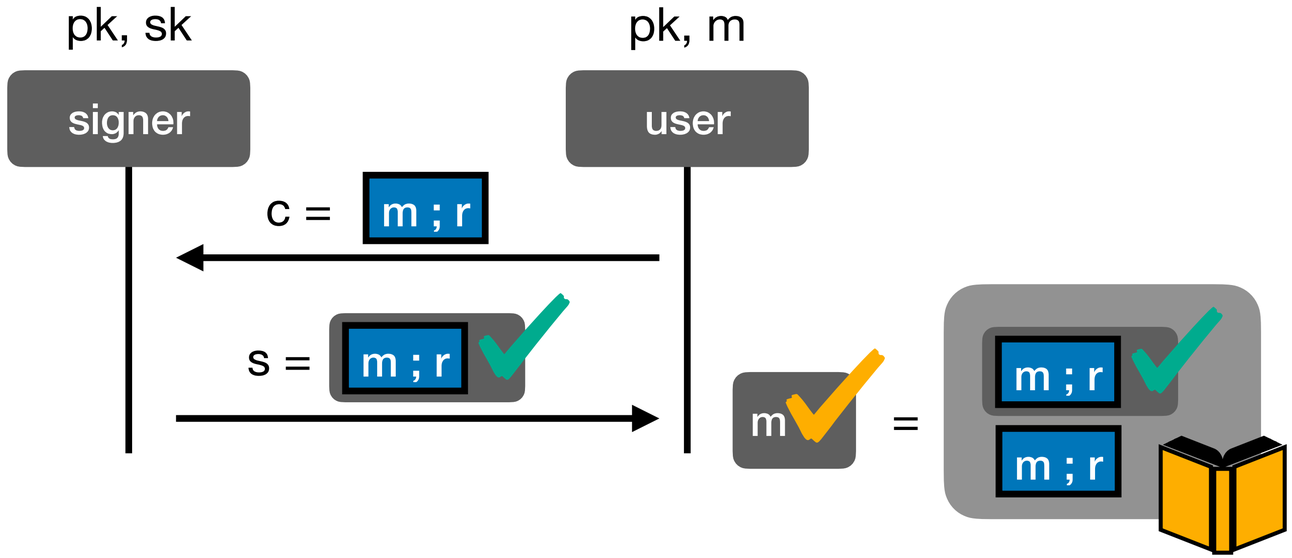
Sketch:



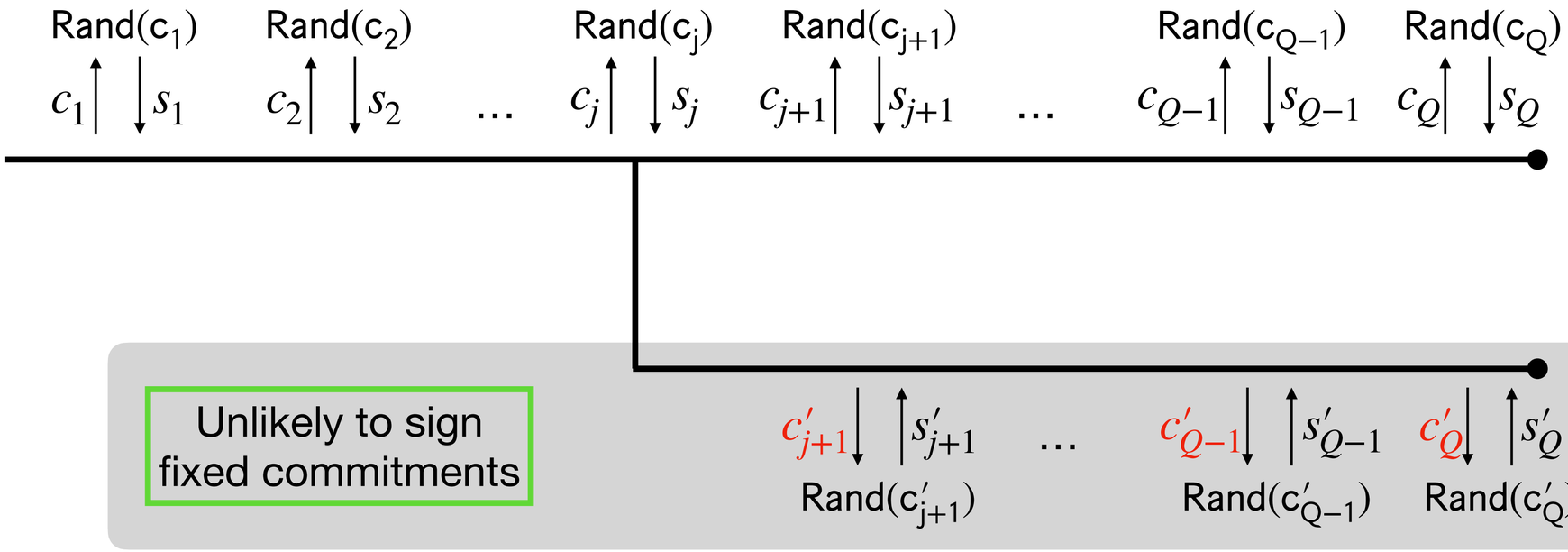


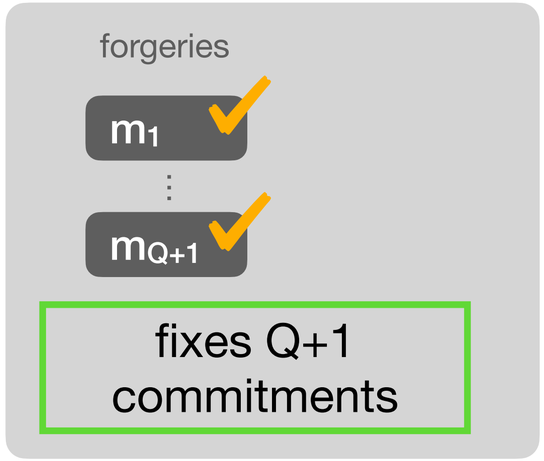
Fischlin

One-more Unforgeability



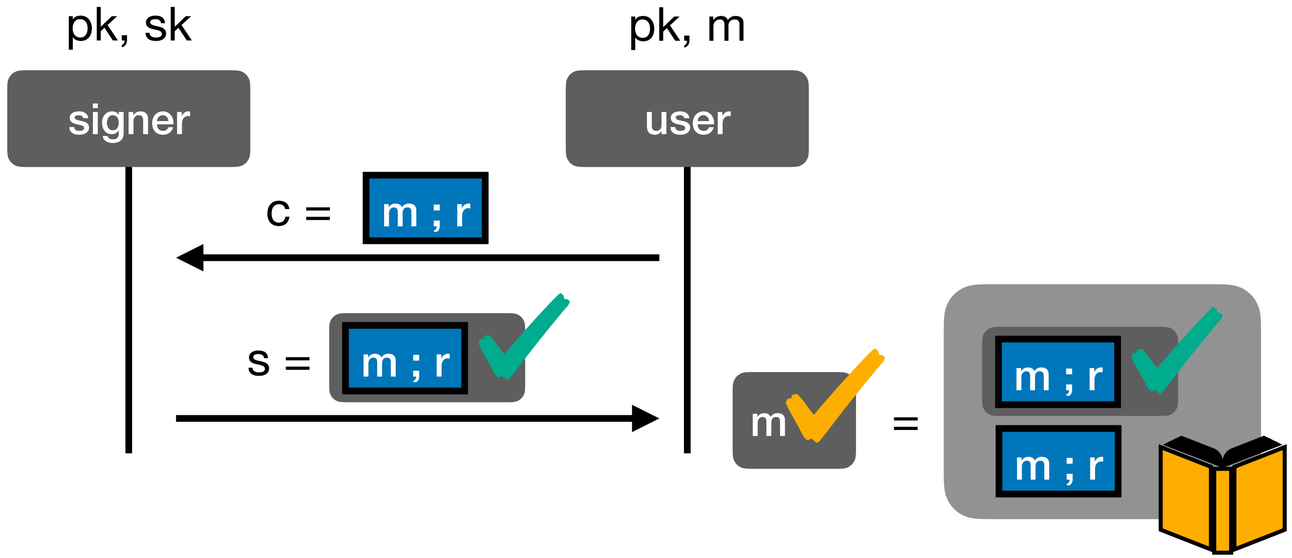
Sketch:



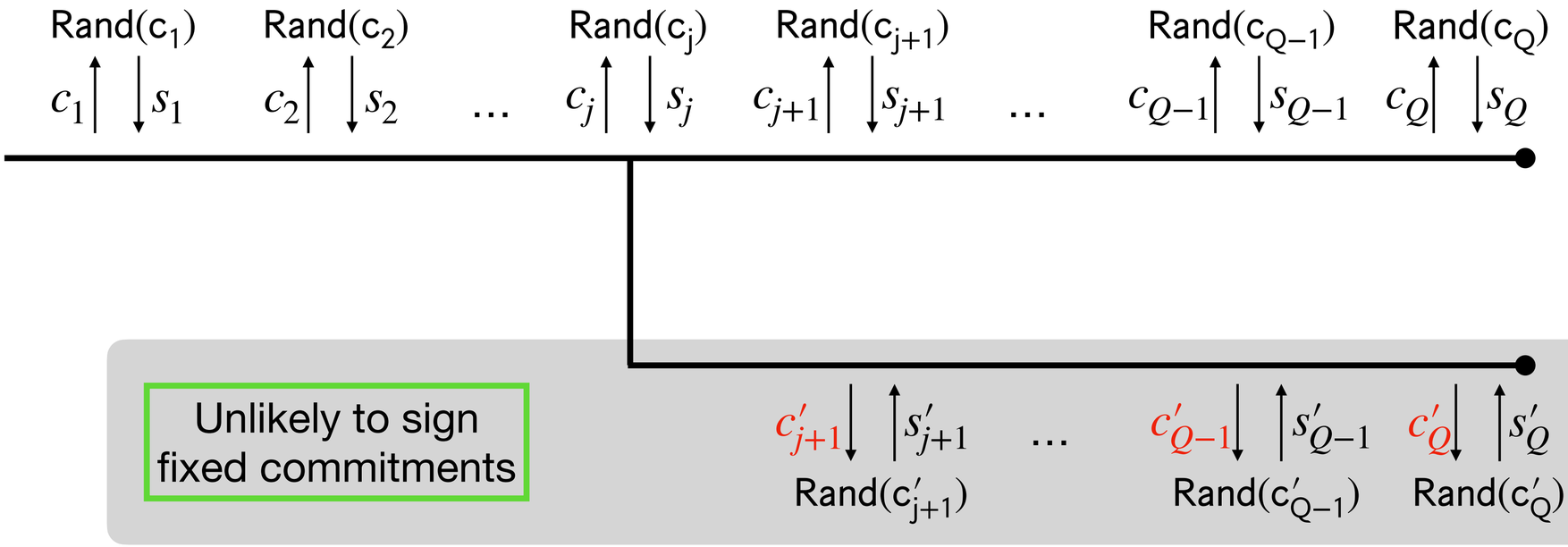


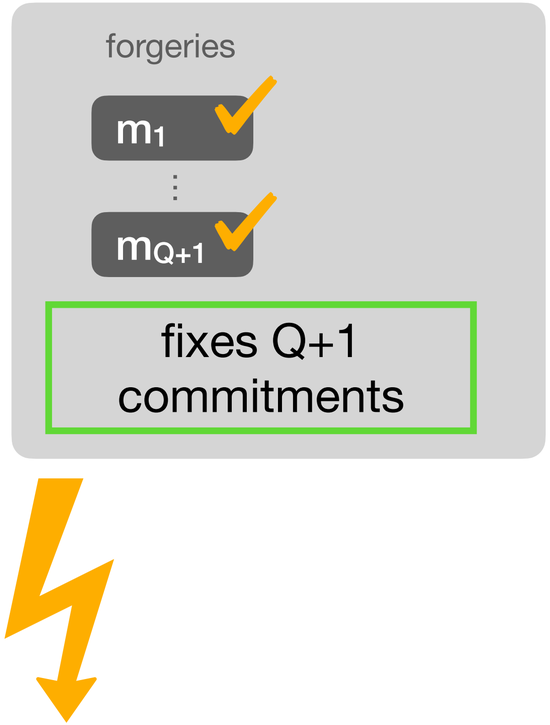
Fischlin

One-more Unforgeability



Sketch:





Instantiation

Pairing-based Blind Signature:

- via **[KPW15]** signatures (SPS) + Fiat-Shamir NIZKs
- signature size, communication: 447 B, 303 B
- partial blindness almost for free

Framework 2

Fischlin with all-but-one Signatures

ABO-based Blind Signatures

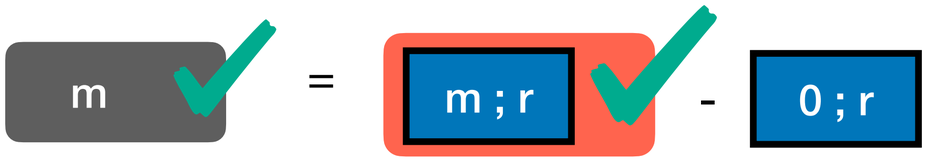
Setup:

- Additive Commitment Scheme

ABO-based Blind Signatures

Setup:

- Signature Scheme

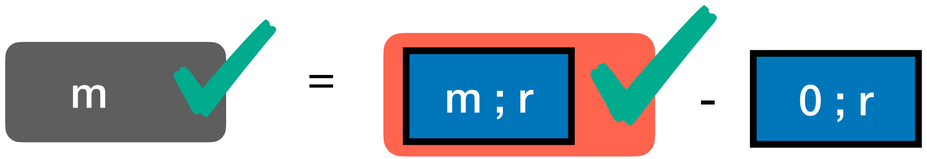


alternative signing algorithm

ABO-based Blind Signatures

Setup:

- Signature Scheme



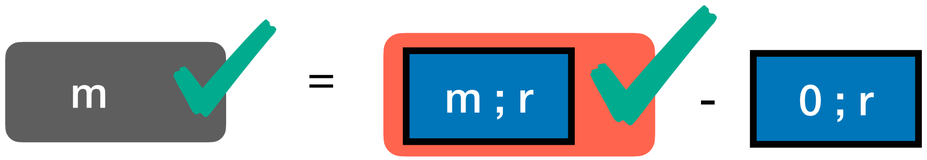
alternative signing algorithm

  - has *all-but-one* reduction

ABO-based Blind Signatures

Setup:

- Signature Scheme



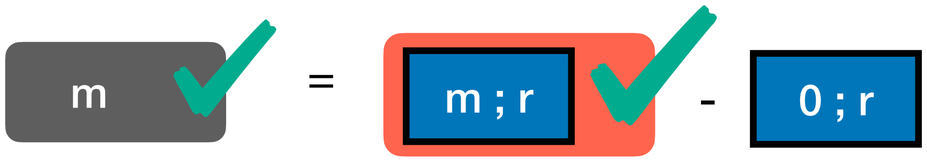
alternative signing algorithm

  - has *all-but-one* reduction
    - puncture *vk* such that reduction can sign all but one message *m**

ABO-based Blind Signatures

Setup:

- Signature Scheme



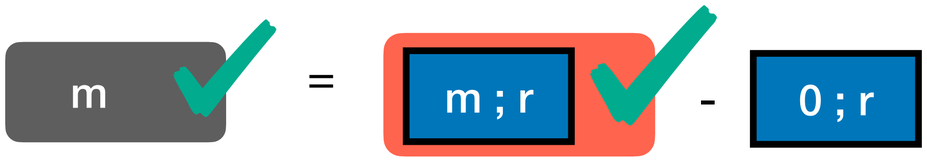
alternative signing algorithm

  - has *all-but-one* reduction
    - puncture *vk* such that reduction can sign all but one message *m**
    - signature on *m** allows to solve hard problem

ABO-based Blind Signatures

Setup:

- Signature Scheme



alternative signing algorithm

  - has *all-but-one* reduction
    - puncture *vk* such that reduction can sign all but one message *m**
    - signature on *m** allows to solve hard problem
  - rerandomizable

ABO-based Blind Signatures

ABO-based Blind Signatures

Example:

ABO-based Blind Signatures

Example:

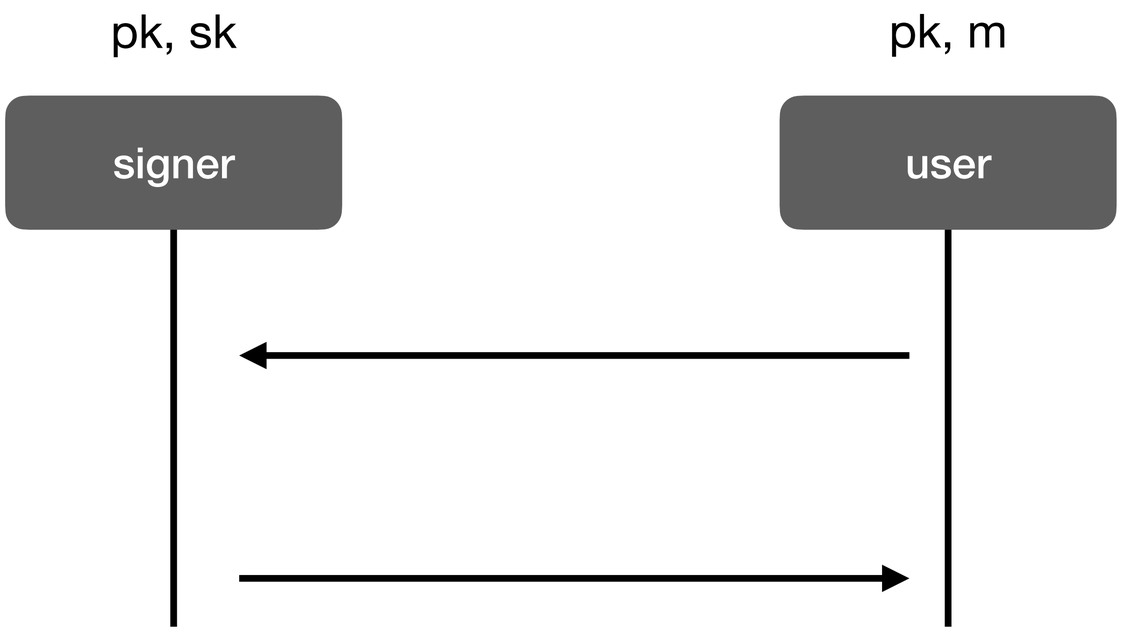
- Pedersen Commitments

ABO-based Blind Signatures

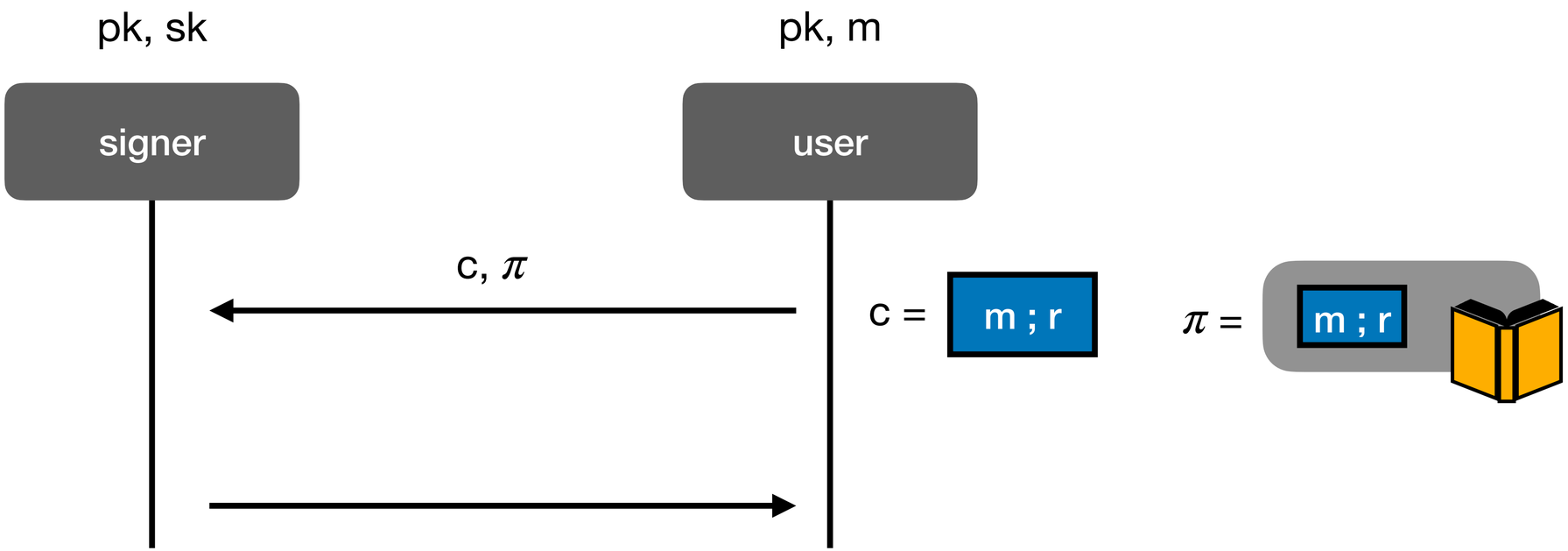
Example:

- Pedersen Commitments
- Boneh-Boyen signatures (based on IBE)

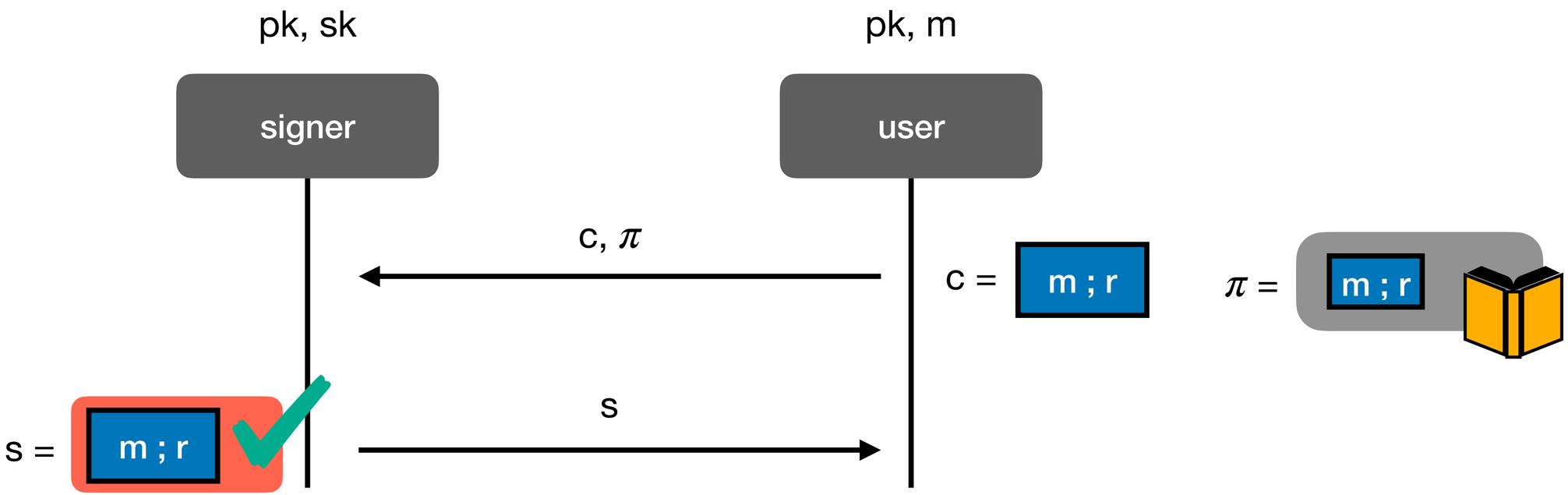
Construction



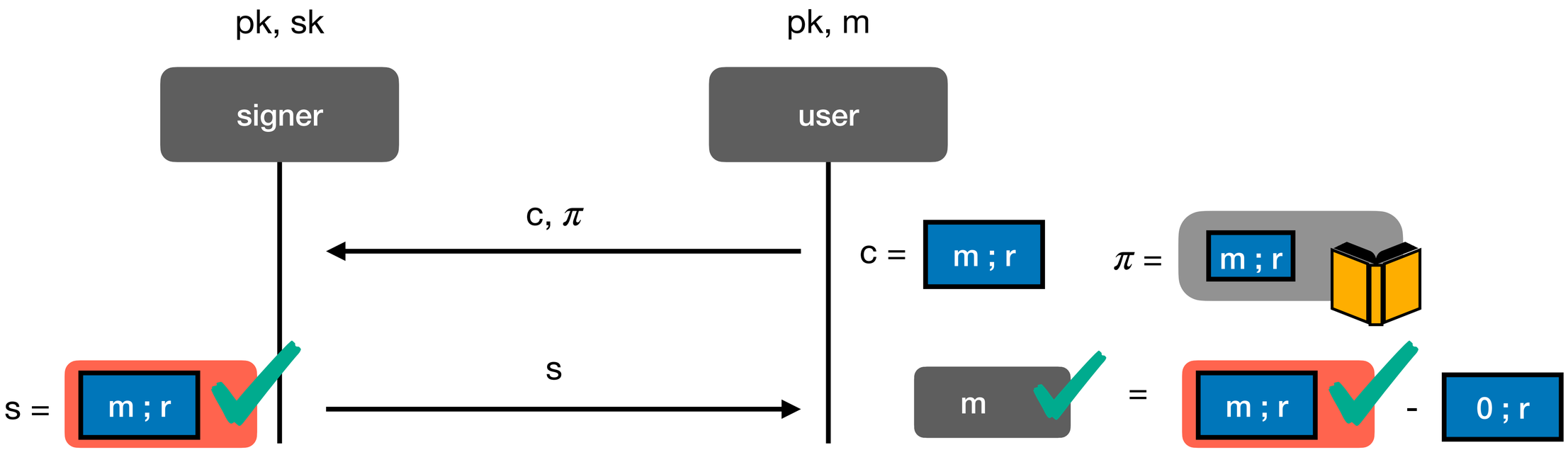
Construction



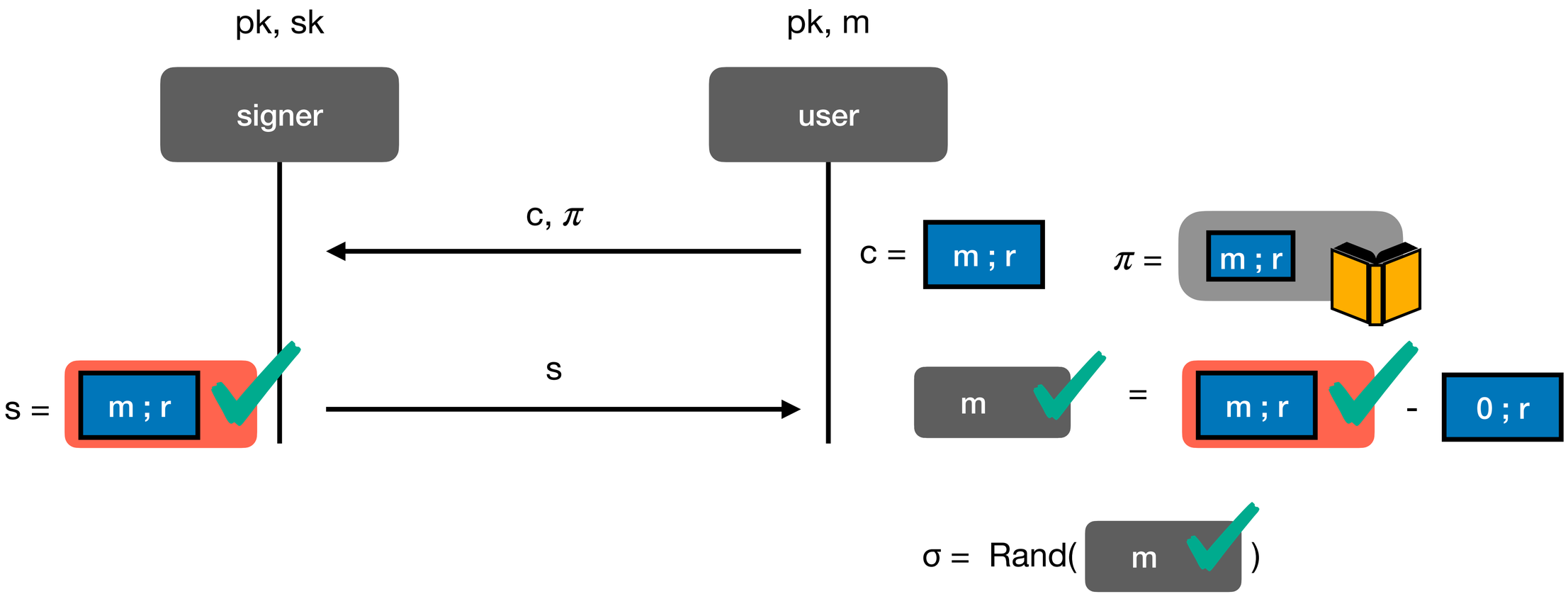
Construction



Construction



Construction



Construction

Proof Sketch (OMUF):

Construction

Proof Sketch (OMUF):

- puncture *vk* *(as in ABO-reduction)*

Construction

Proof Sketch (OMUF):

- puncture *vk* *(as in ABO-reduction)*
- simulate signing oracle:

Construction

Proof Sketch (OMUF):

- puncture *vk* *(as in ABO-reduction)*
- simulate signing oracle:
  - extract message *m* and *r* from π

Construction

Proof Sketch (OMUF):

- puncture *vk* *(as in ABO-reduction)*
- simulate signing oracle:
  - extract message *m* and *r* from π
  - sign *m* with punctured setup:

Construction

Proof Sketch (OMUF):

- puncture *vk* *(as in ABO-reduction)*
- simulate signing oracle:
  - extract message *m* and *r* from π
  - sign *m* with punctured setup: 

Construction

Proof Sketch (OMUF):

- puncture *vk* *(as in ABO-reduction)*
- simulate signing oracle:
  - extract message *m* and *r* from π
  - sign *m* with punctured setup: 

  - compute

Construction

Proof Sketch (OMUF):

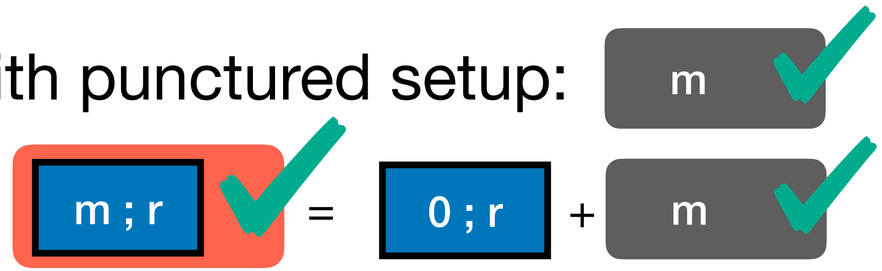
- puncture *vk* *(as in ABO-reduction)*
- simulate signing oracle:
  - extract message *m* and *r* from π
  - sign *m* with punctured setup: 

  - compute 

Construction

Proof Sketch (OMUF):

- puncture *vk* *(as in ABO-reduction)*
- simulate signing oracle:
  - extract message *m* and *r* from π
  - sign *m* with punctured setup:
  - compute
- given forgery:



Construction

Proof Sketch (OMUF):

- puncture *vk* *(as in ABO-reduction)*
- simulate signing oracle:
  - extract message *m* and *r* from π
  - sign *m* with punctured setup: m
  - compute m ; r = 0 ; r + m
- given forgery:
  - if signature is on m*, we can solve a hard problem

Instantiation

Pairing-based Blind Signature:

Instantiation

Pairing-based Blind Signature:

- via Boneh-Boyen Signatures + Pedersen Commitments

Instantiation

Pairing-based Blind Signature:

- via Boneh-Boyen Signatures + Pedersen Commitments
- Bulletproof-based online-extractable NIZK

Instantiation

Pairing-based Blind Signature:

- via Boneh-Boyen Signatures + Pedersen Commitments
- Bulletproof-based online-extractable NIZK
- signature size, communication: 96 B, 2.2 KB

Instantiation

Pairing-based Blind Signature:

- via Boneh-Boyen Signatures + Pedersen Commitments
- Bulletproof-based online-extractable NIZK
- signature size, communication: 96 B, 2.2 KB
- partial blindness almost for free

Results

Efficient Blind Signatures in the ROM under standard assumptions

Reference	Signature Size	Communication Size	Assumption
[dK22]	100 KB	850 KB	DSMR, MLWE, MSIS
[BFP13]	96 B	220 KB	SXDH, CDH
[AJOR18]	5.5 KB	1 KB	SXDH
[HLW23]	5 KB 9 KB	72 KB 36 KB	CDH
this work	447 B	303 B	SXDH
this work	96 B	2.2 KB	DDH, CDH