Pi-Cut-Choo and Friends

Compact Blind Signatures via Parallel Instance Cut-and-Choose and More

https://ia.cr/2022/007

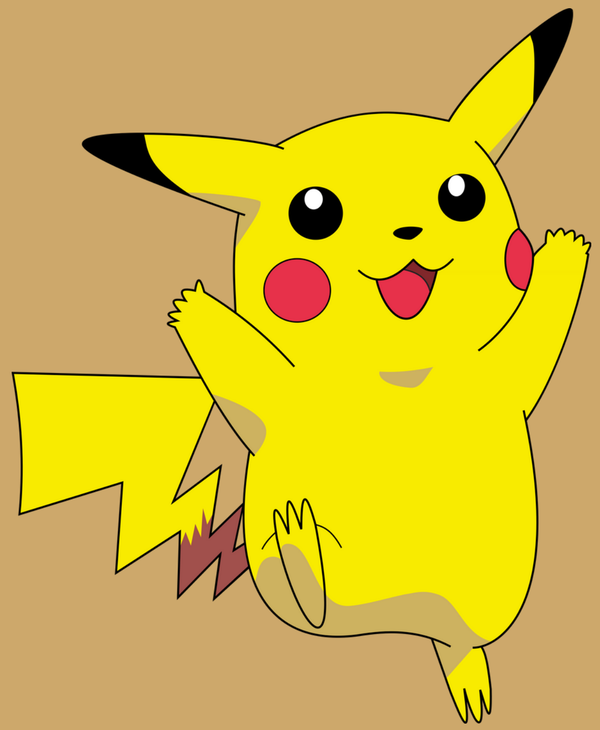


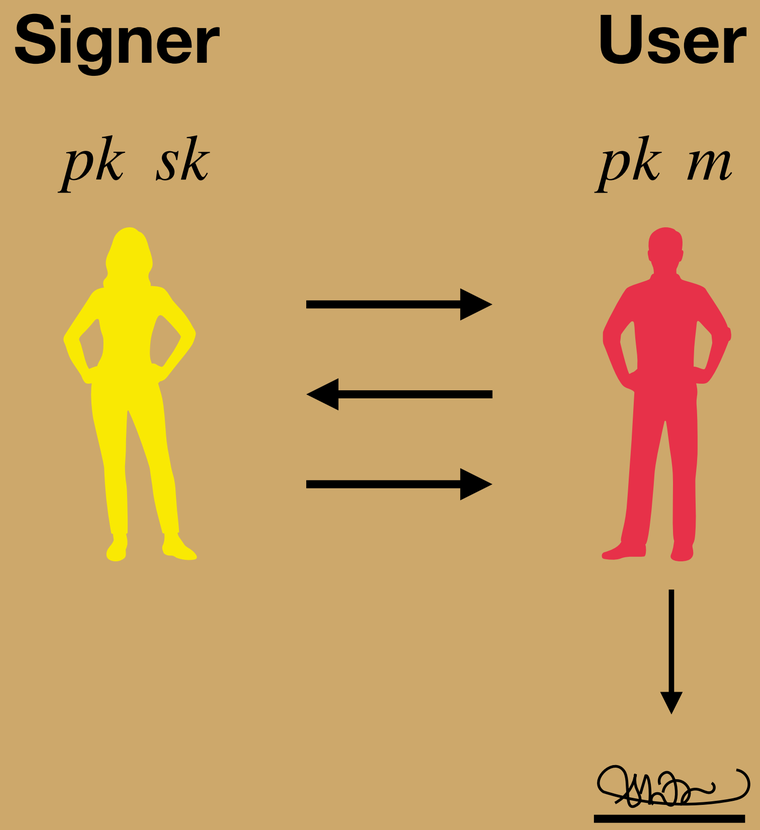
Image Source: shorturl.at/cDZ06

Rutchathon Chairattana-Apirom
Lucjan Hanzlik
Julian Loss
Anna Lysyanskaya
Benedikt Wagner

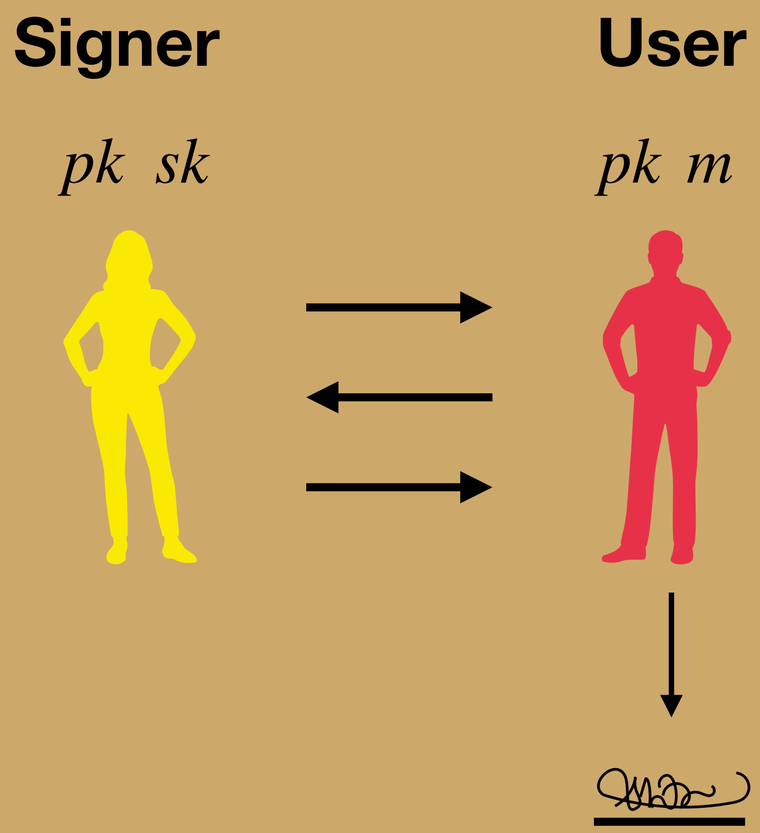
BROWN

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Blind Signatures [Cha82]



Blind Signatures [Cha82]



Applications:

- **Unlinkable Payments**
- **E-Cash**
- **Voting**

Goal: Efficient Parameter

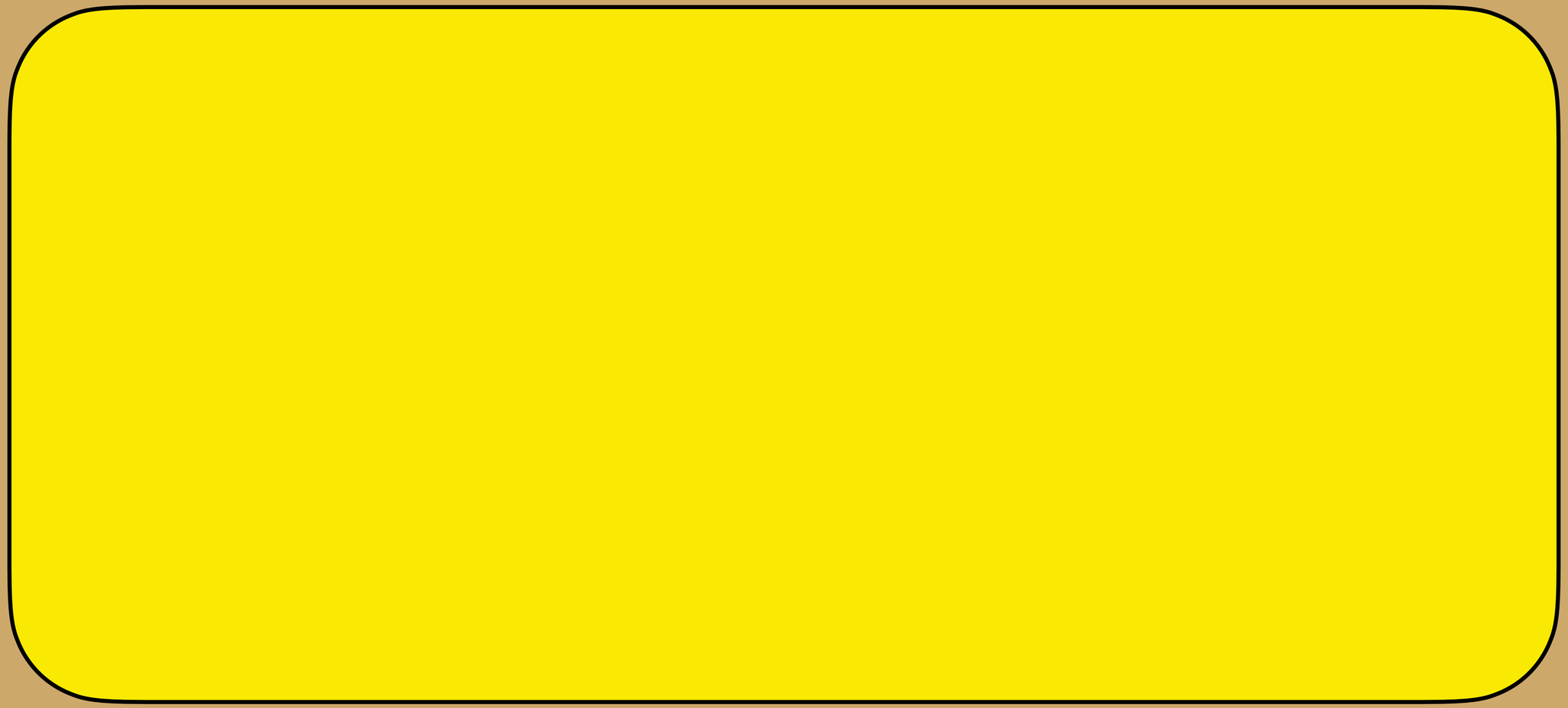
Blind Signatures - Security

Blind Signatures - Security

Blindness

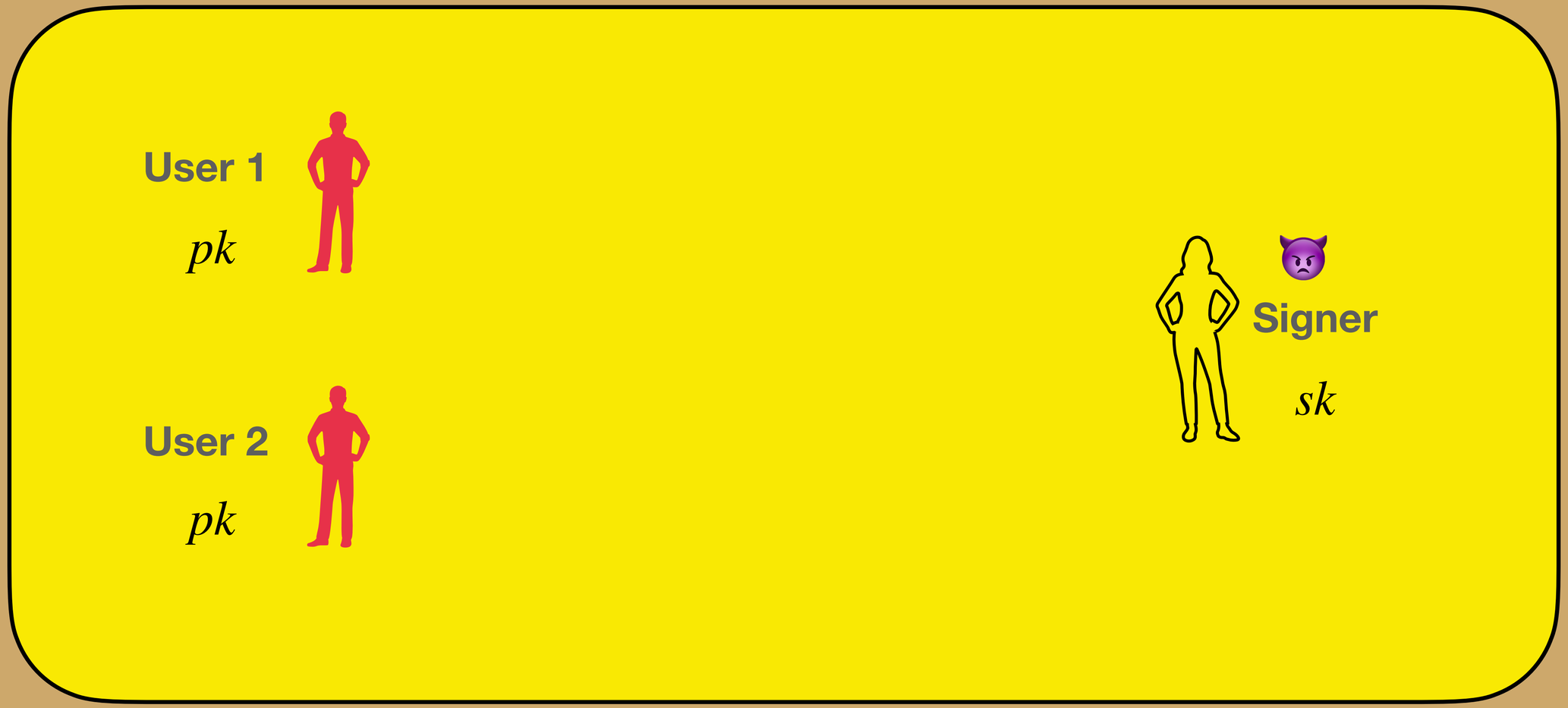
Blind Signatures - Security

Blindness



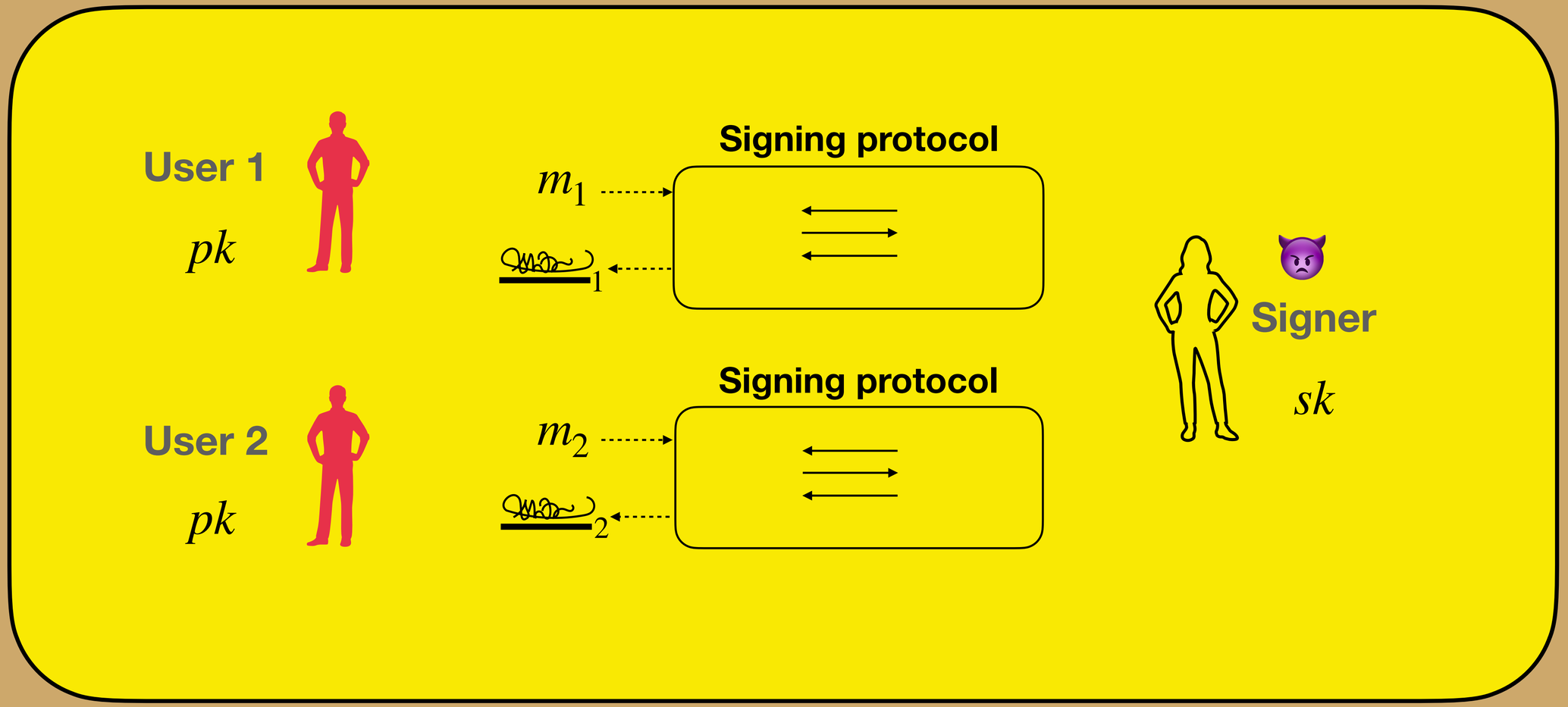
Blind Signatures - Security

Blindness



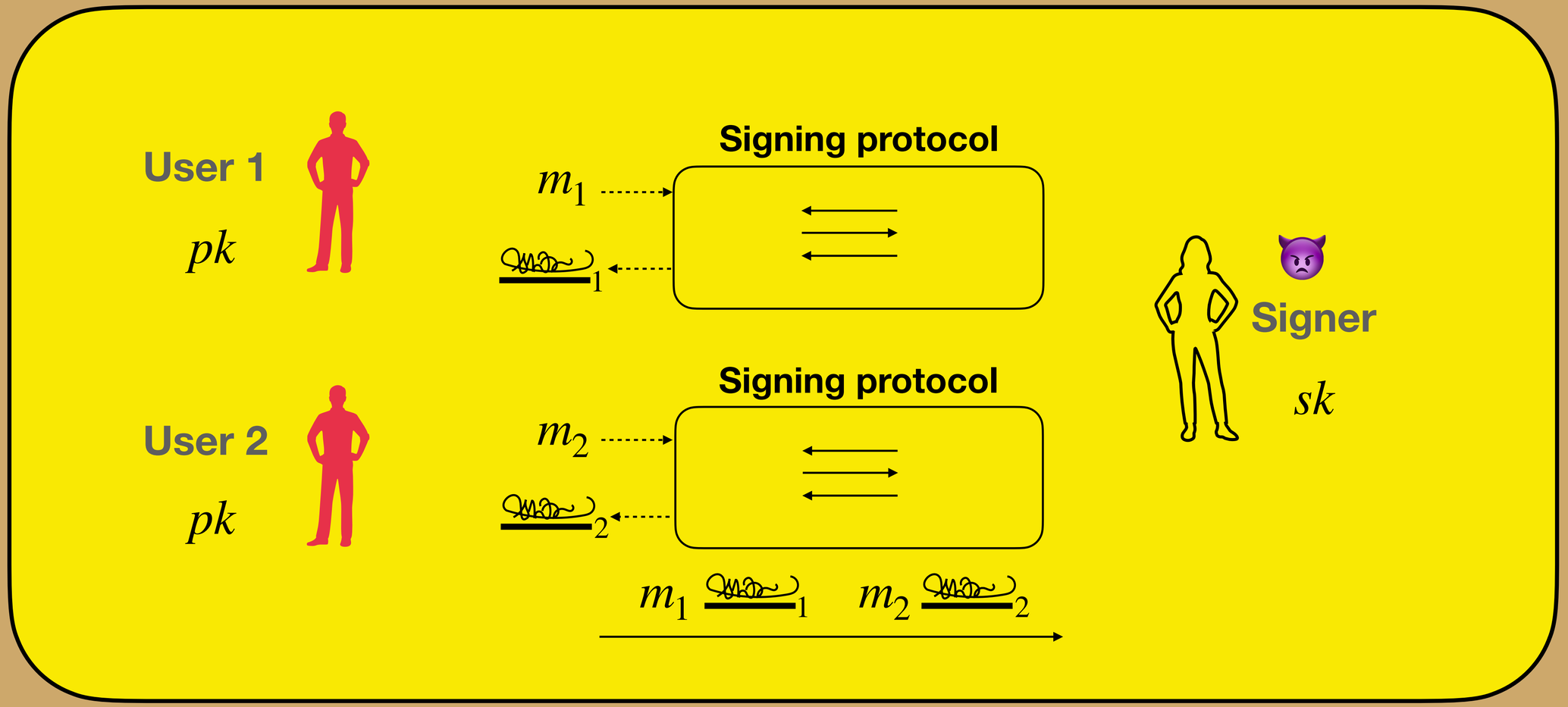
Blind Signatures - Security

Blindness



Blind Signatures - Security

Blindness



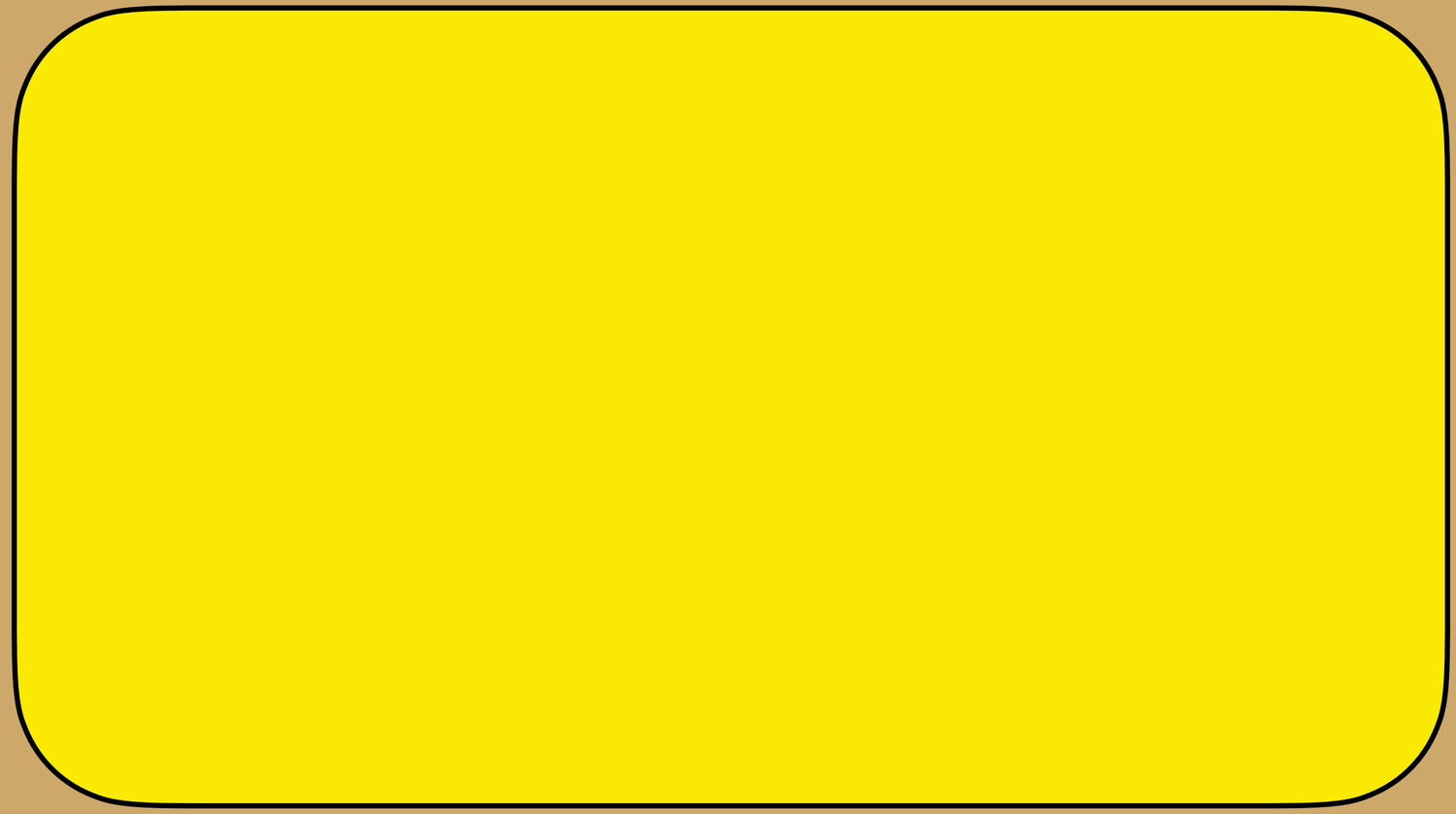
Blind Signatures - Security

Blind Signatures - Security

One-more unforgeability

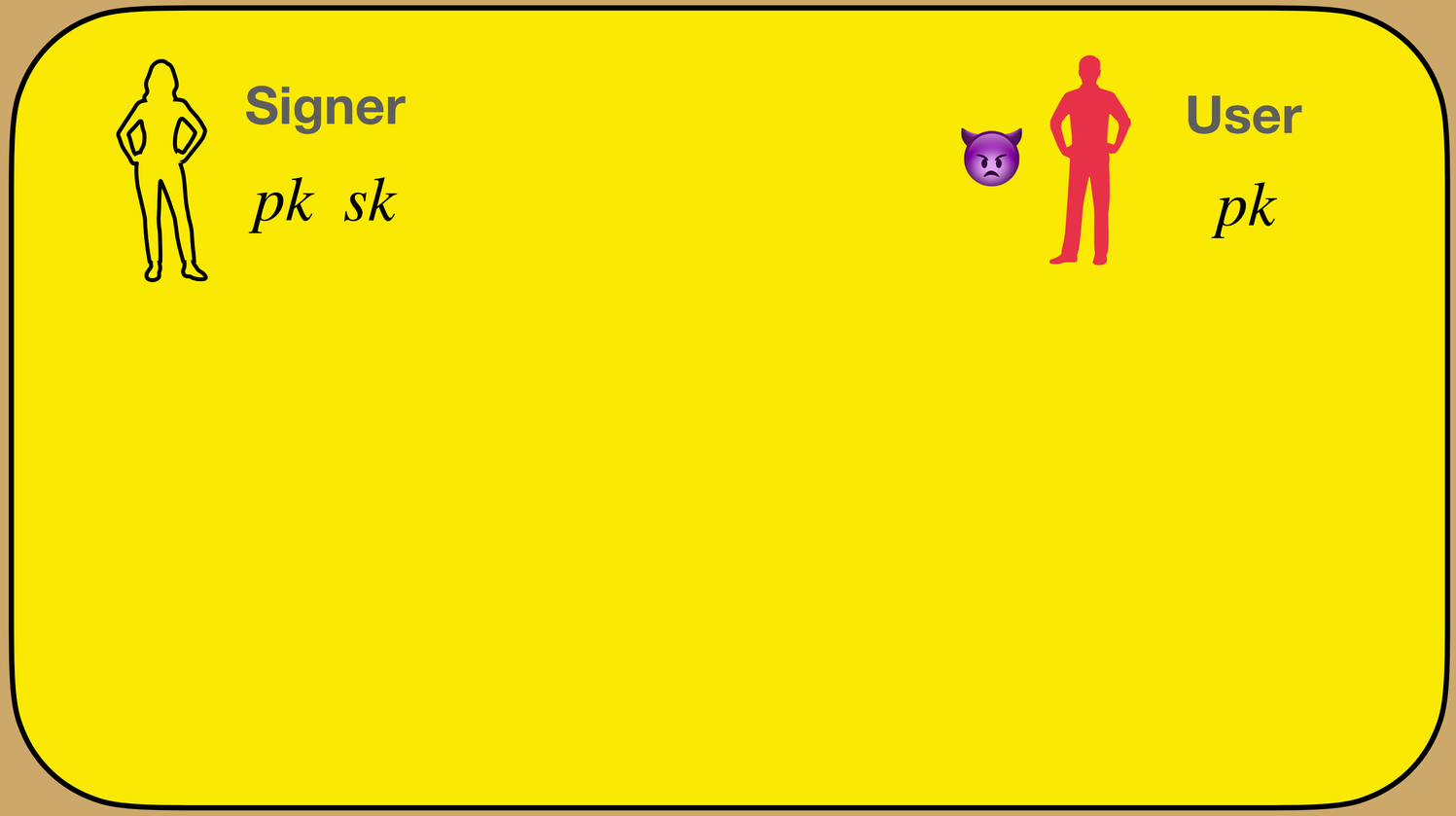
Blind Signatures - Security

One-more unforgeability



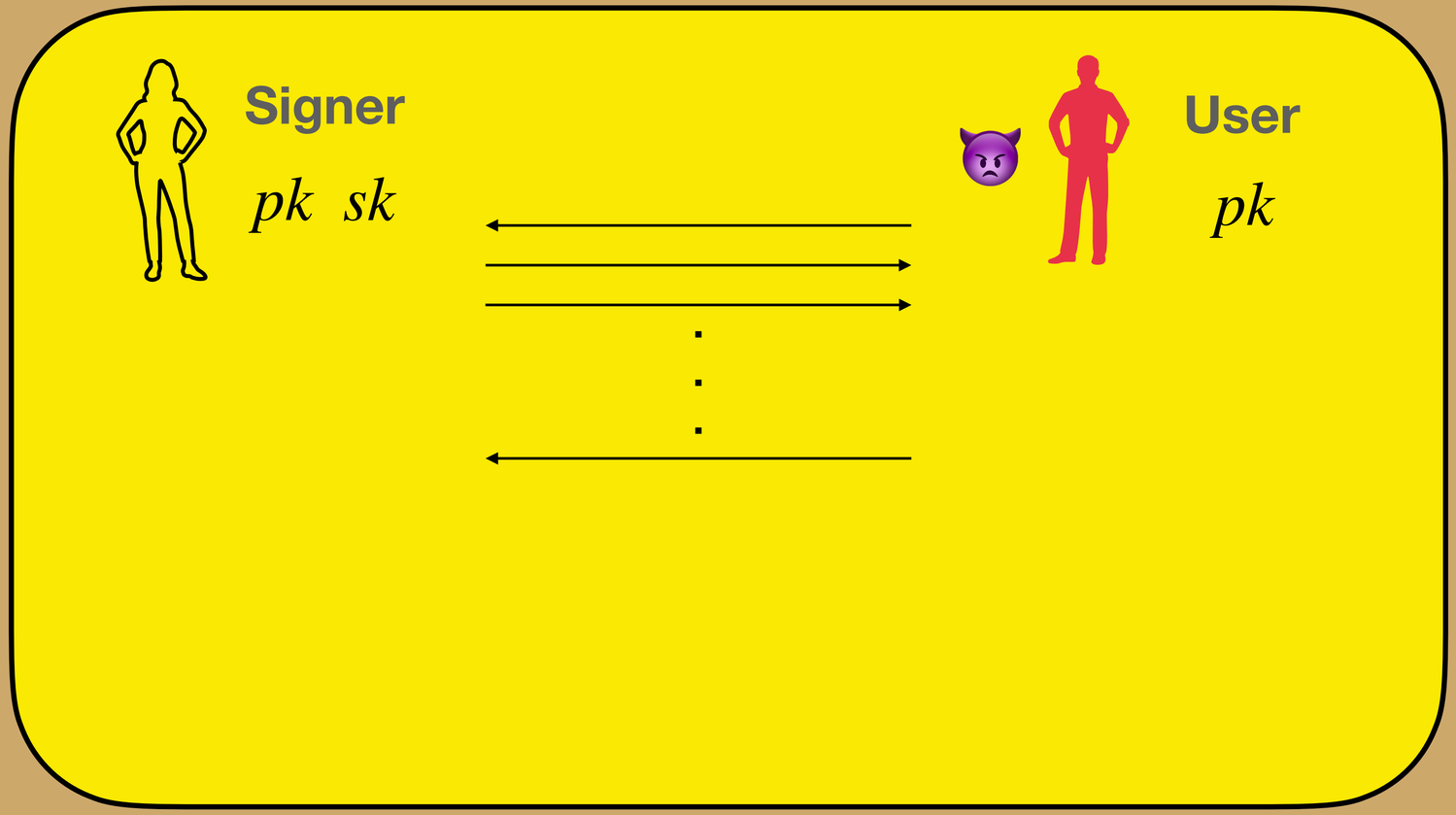
Blind Signatures - Security

One-more unforgeability



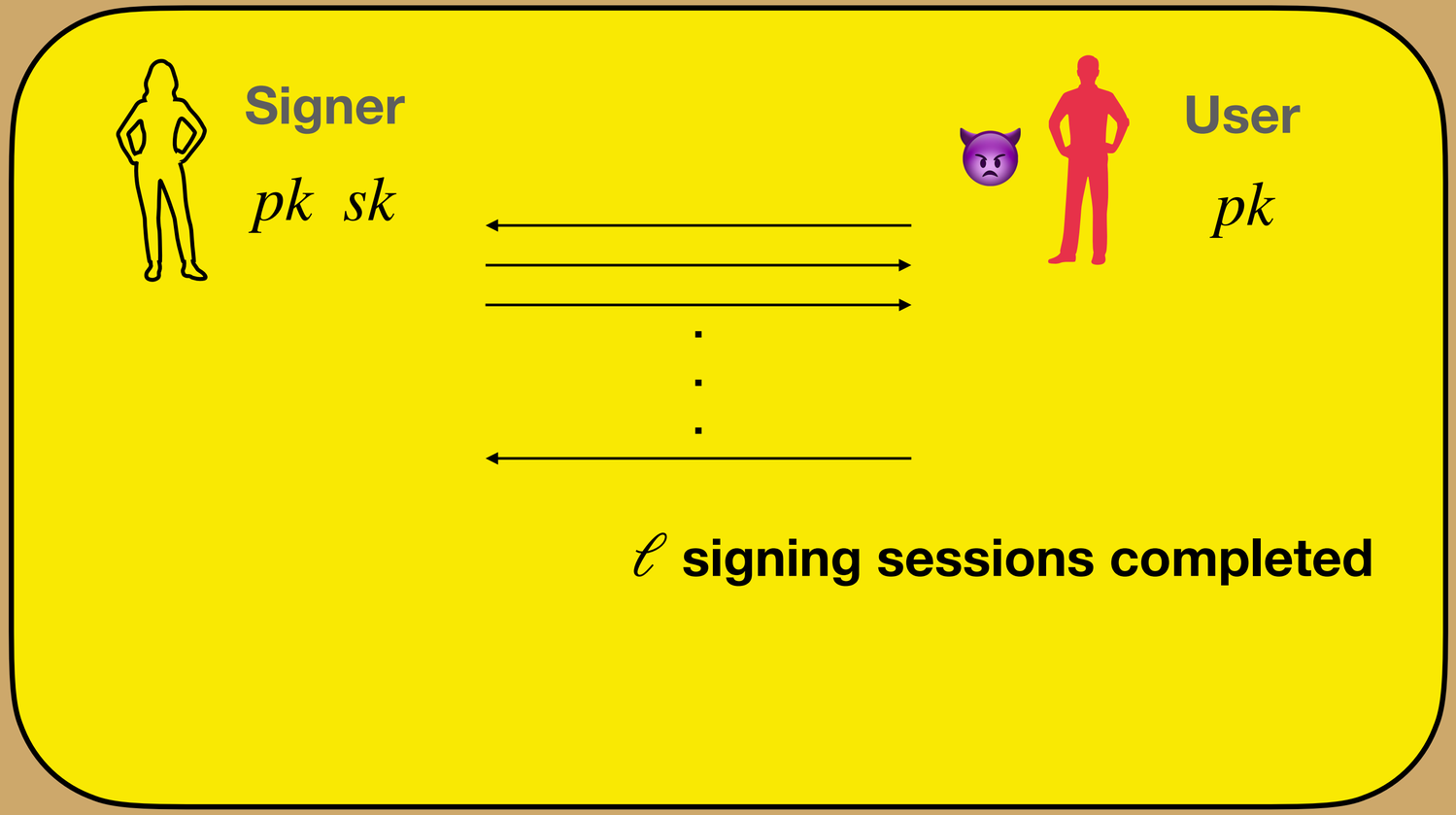
Blind Signatures - Security

One-more unforgeability



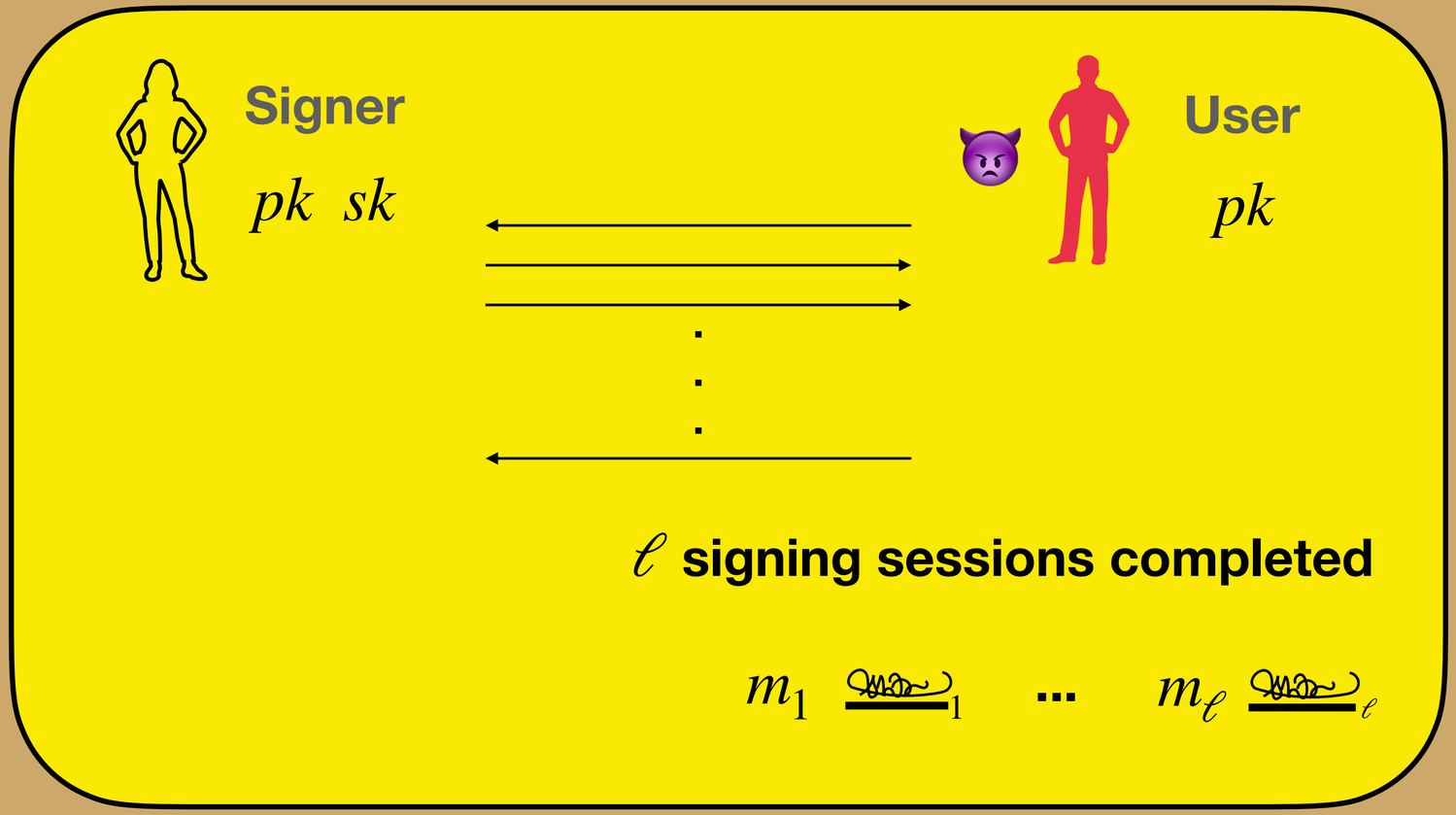
Blind Signatures - Security

One-more unforgeability



Blind Signatures - Security

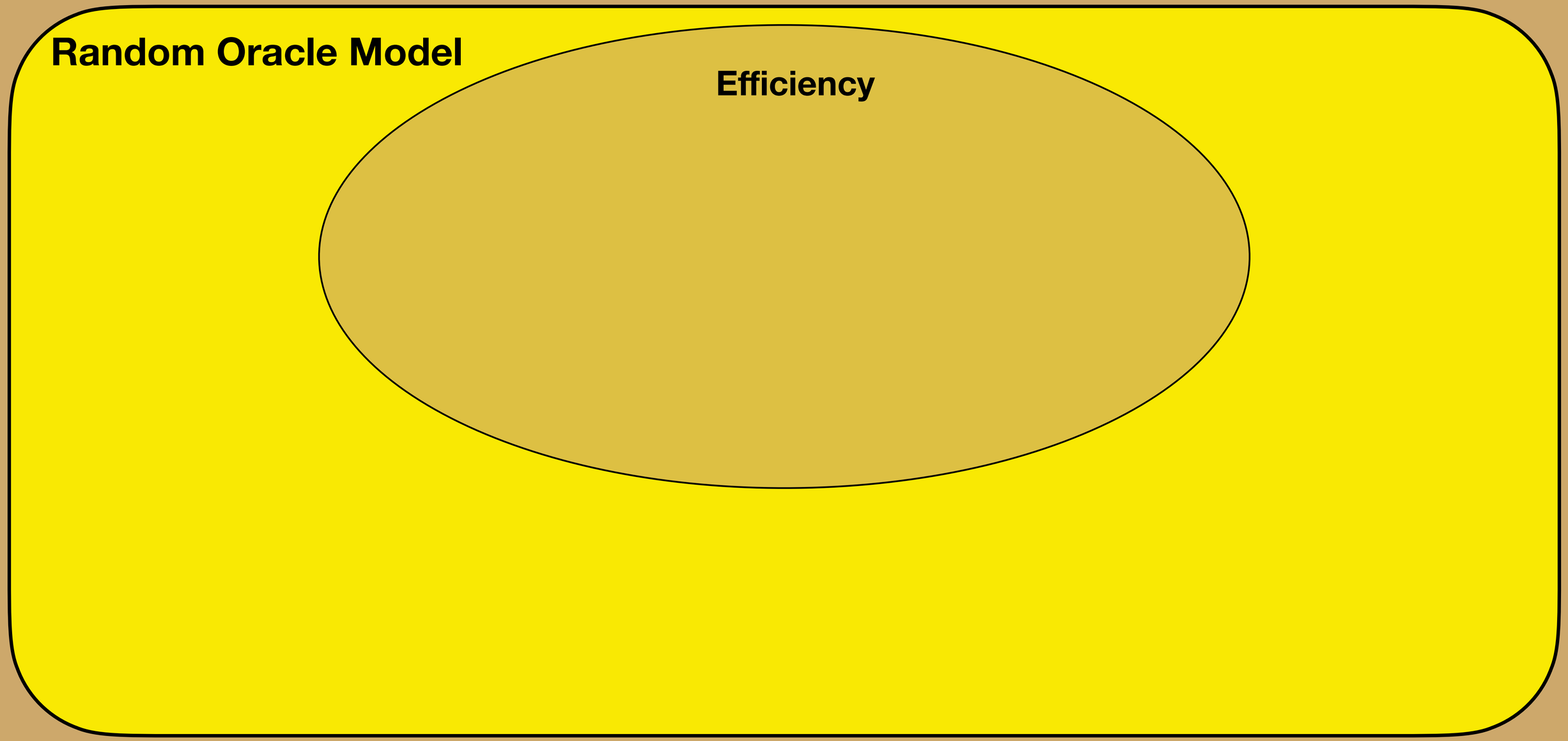
One-more unforgeability



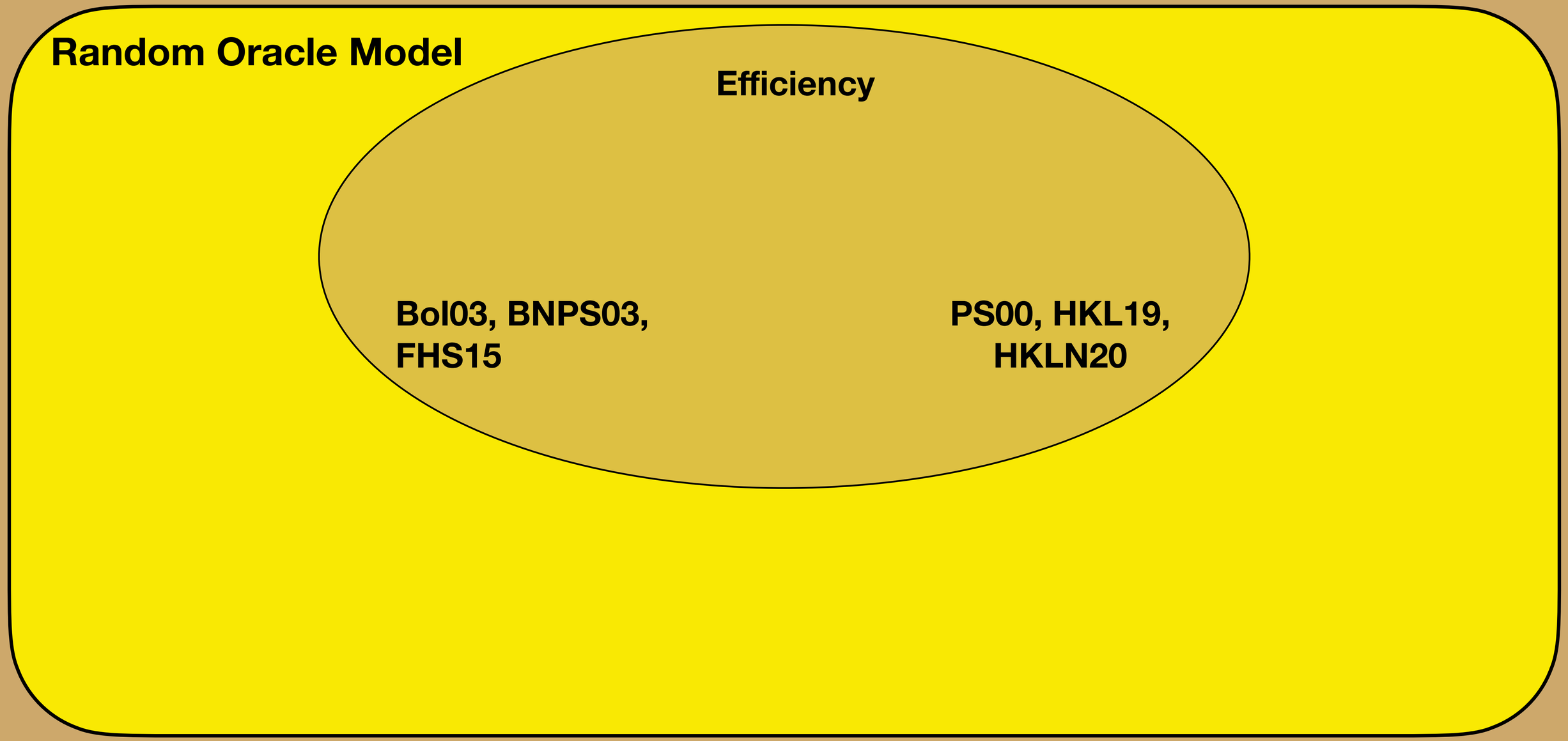
State of The Art

Random Oracle Model

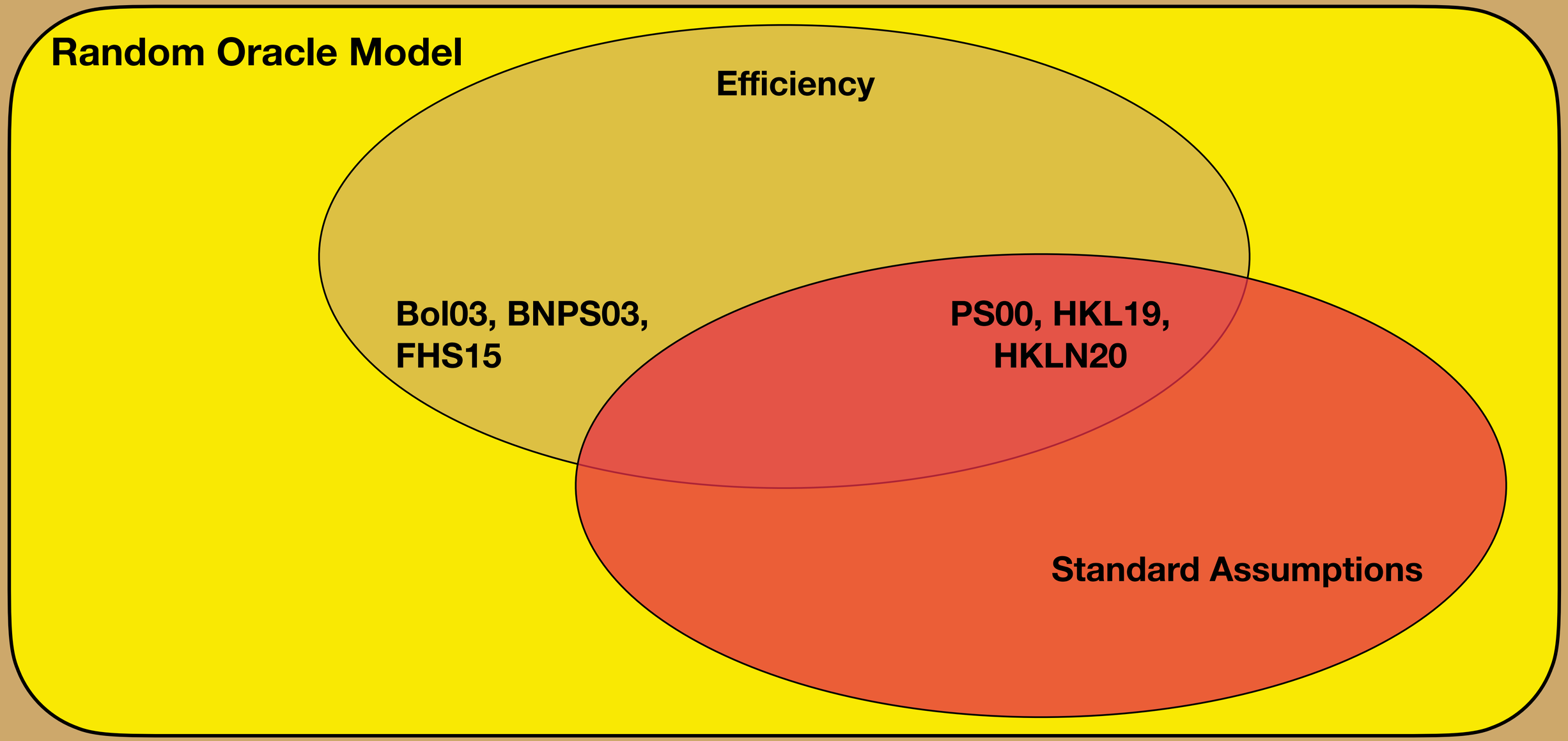
State of The Art



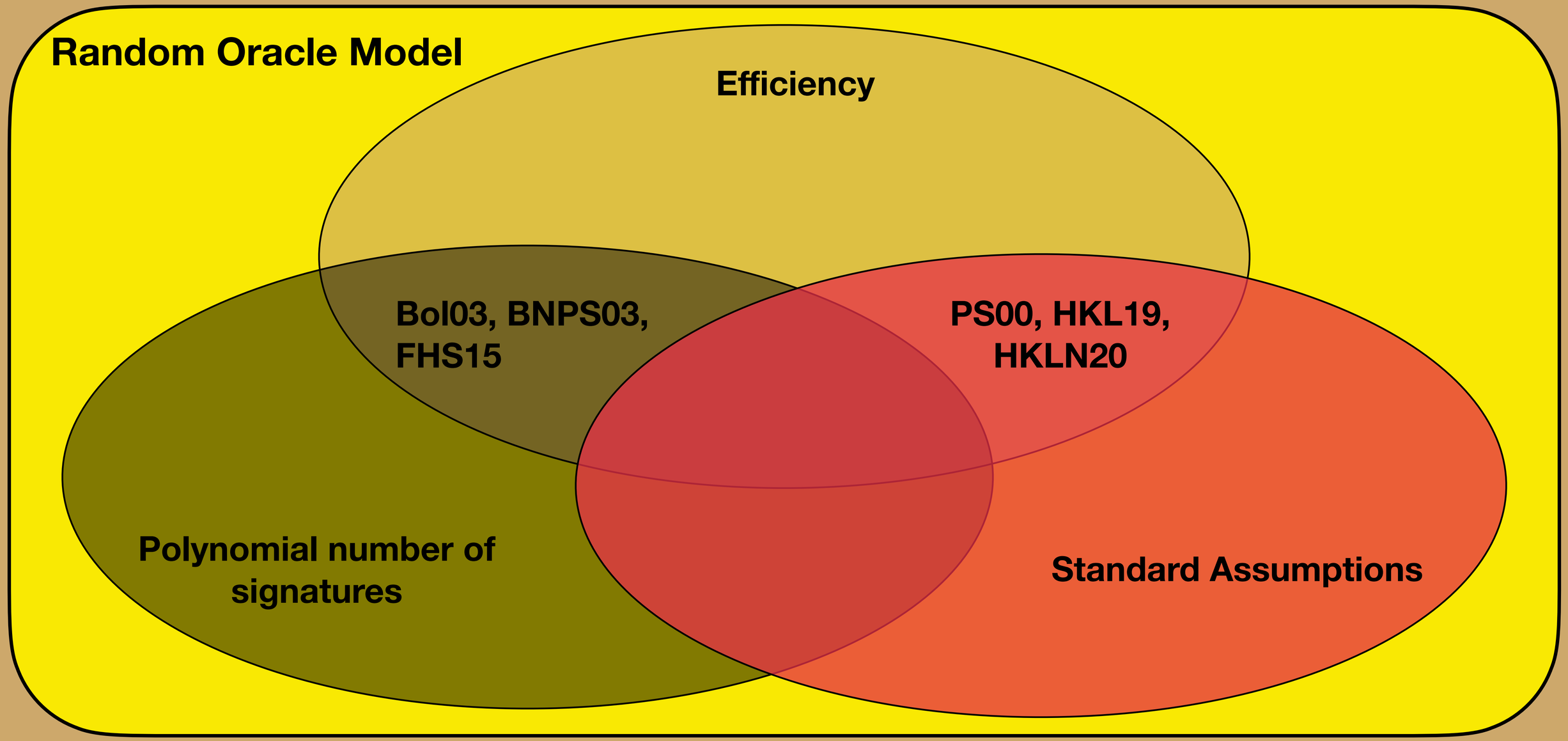
State of The Art



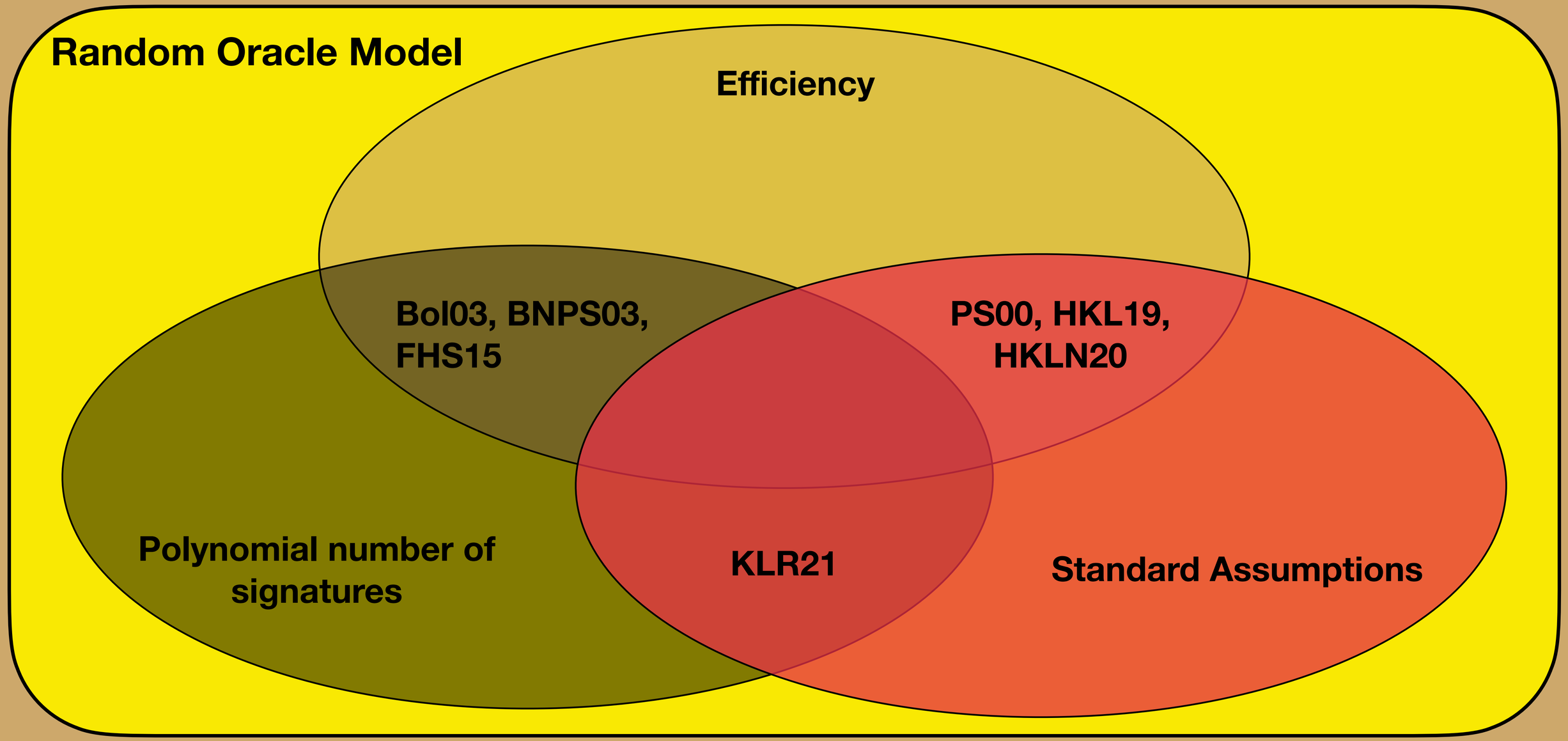
State of The Art



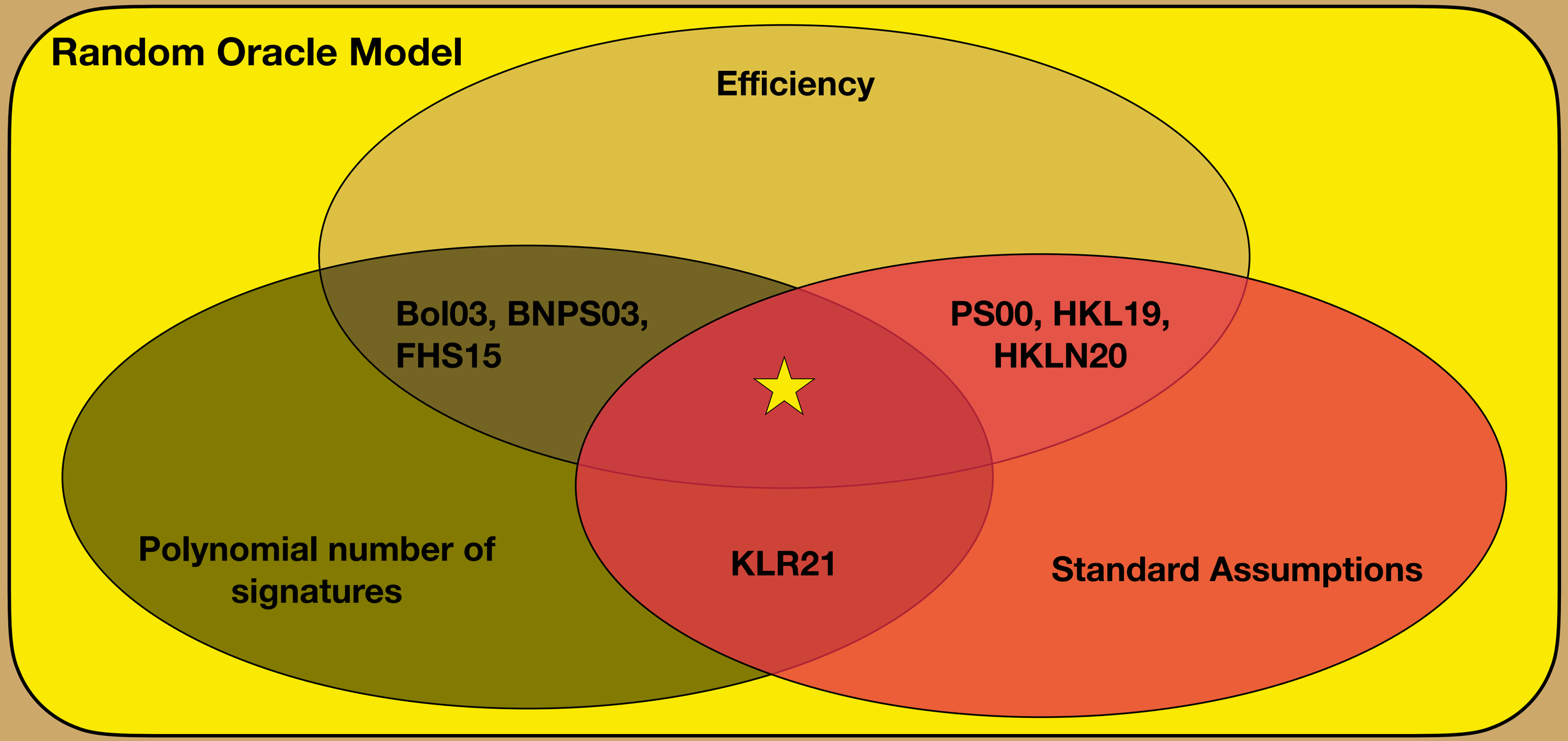
State of The Art

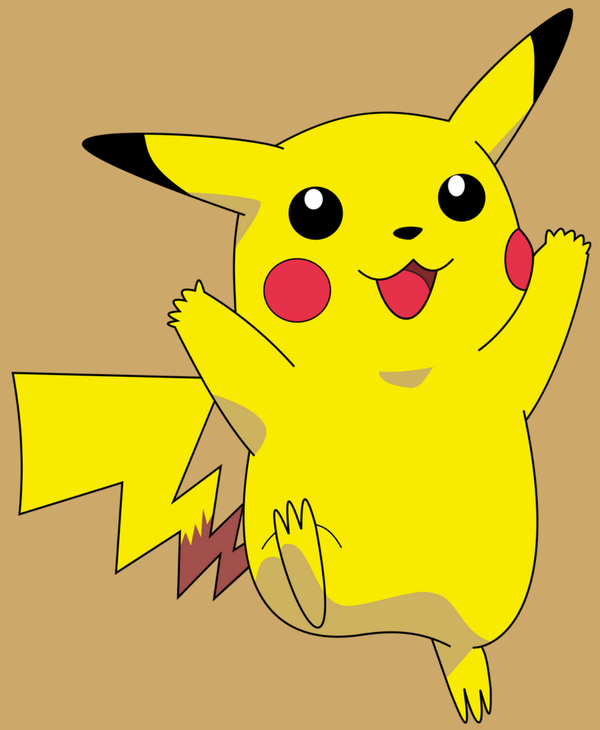


State of The Art



State of The Art





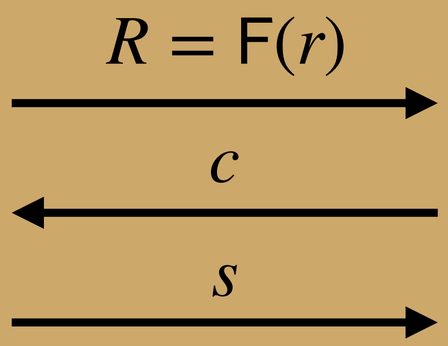
The Boosting Transform

Image Source: shorturl.at/cDZ06

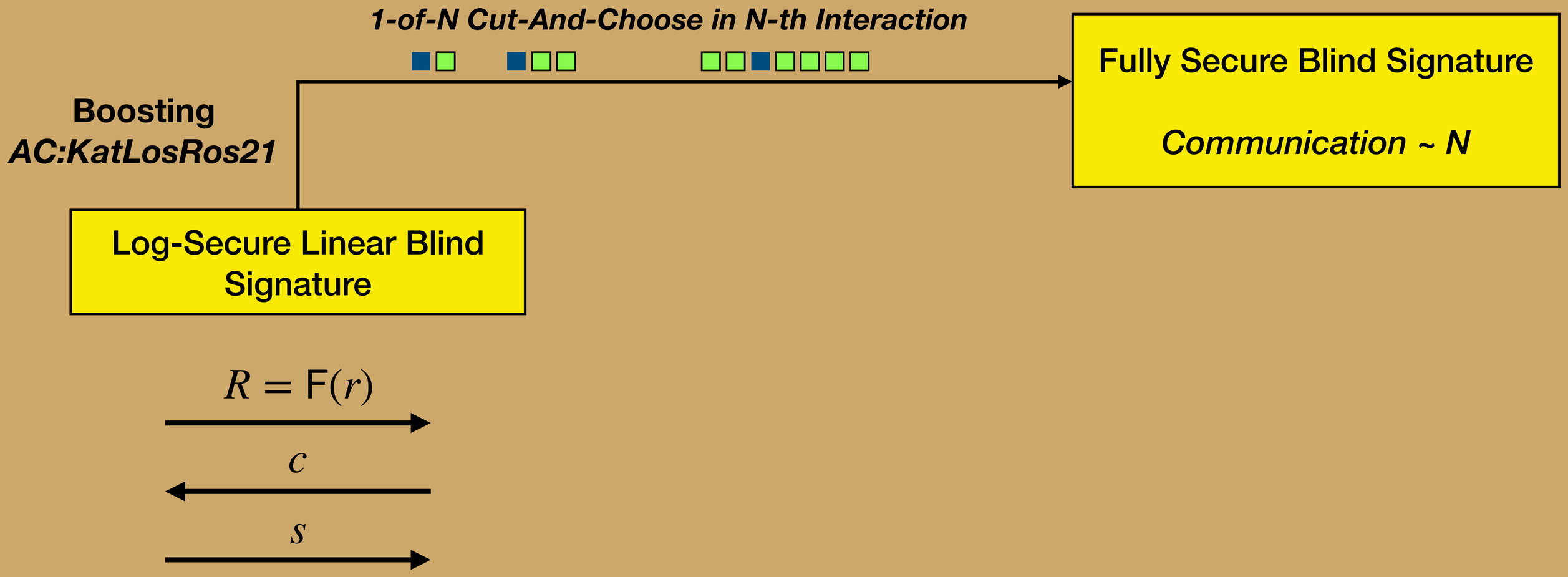
The Boosting Transform

The Boosting Transform

Log-Secure Linear Blind Signature



The Boosting Transform



The Boosting Transform

1-of-N Cut-And-Choose in N-th Interaction

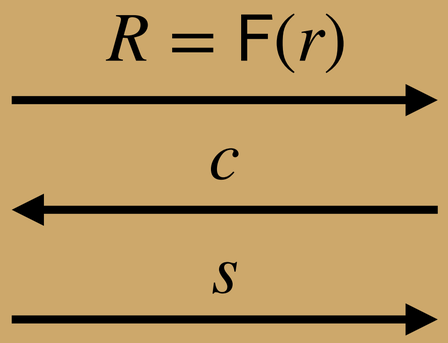
Boosting
AC:KatLosRos21

Fully Secure Blind Signature

Communication ~ N

Log-Secure Linear Blind Signature

★ Simulation knowing Message + Randomness



The Boosting Transform

Signer

$pk \quad sk$

User

$pk \quad m$

The Boosting Transform

In the N-th interaction

Signer

$pk \quad sk$

User

$pk \quad m$

The Boosting Transform

In the N-th interaction

N

Signer

$pk \quad sk$

User

$pk \quad m$

The Boosting Transform

Signer

$pk \quad sk$

In the N-th interaction

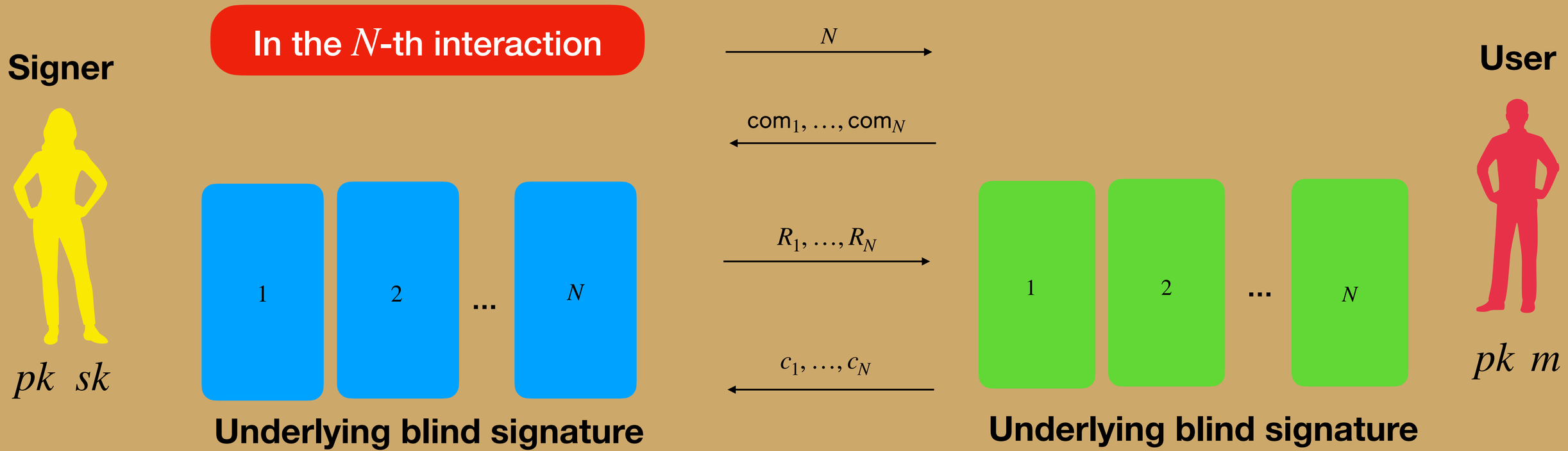
N →

← $\mathsf{com}_1, \ldots, \mathsf{com}_N$

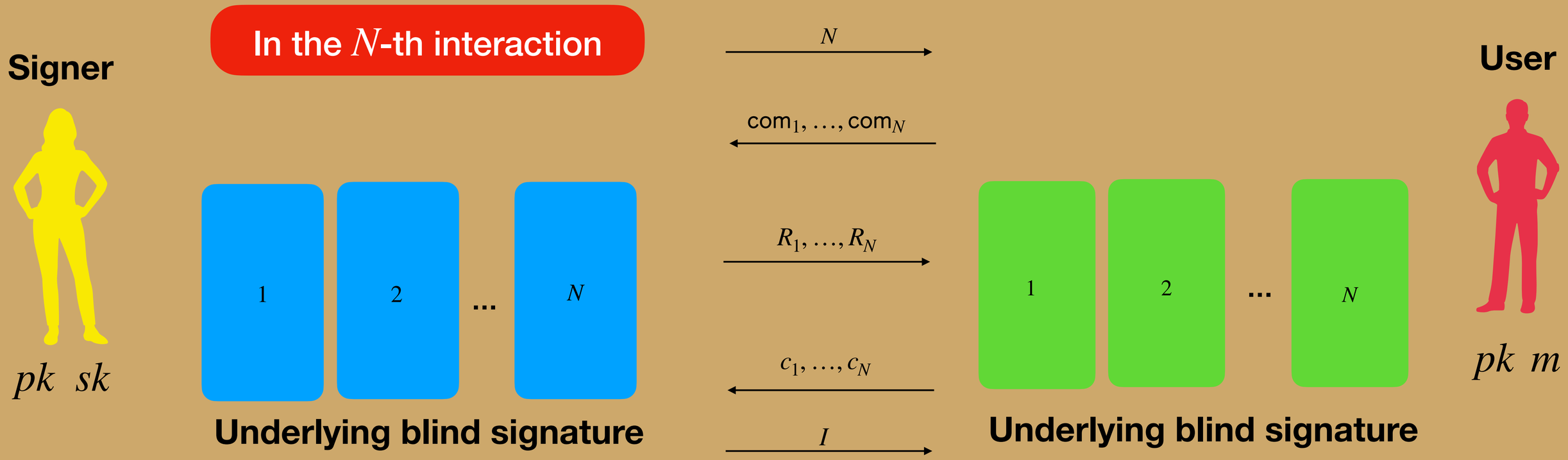
User

$pk \quad m$

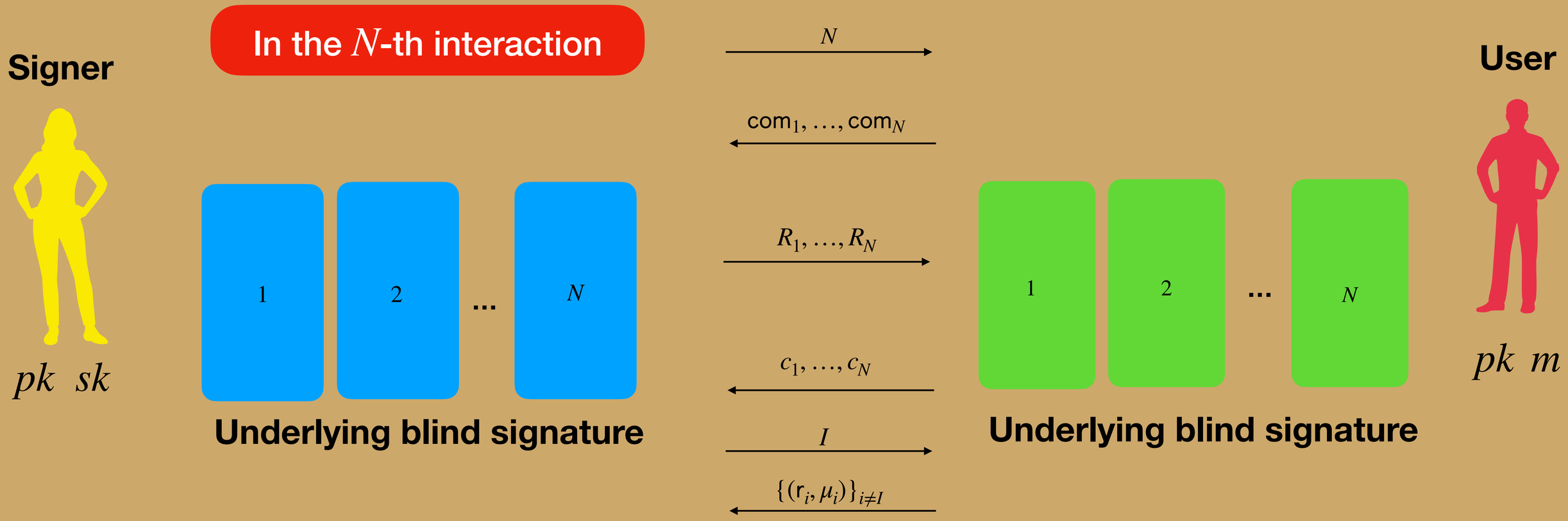
The Boosting Transform



The Boosting Transform



The Boosting Transform

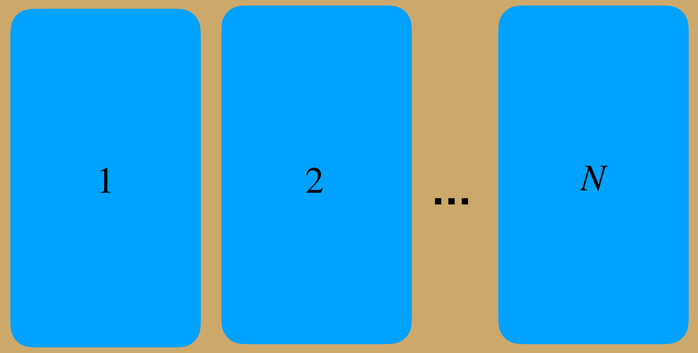


The Boosting Transform

Signer

$pk \quad sk$

In the N-th interaction



Underlying blind signature

N

$\mathsf{com}_1, \ldots, \mathsf{com}_N$

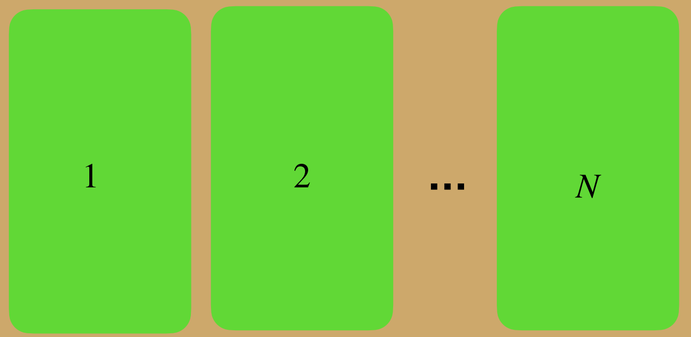
$R_1, \ldots, R_N$

$c_1, \ldots, c_N$

I

$\{(\mathsf{r}_i, \mu_i)\}_{i \neq I}$

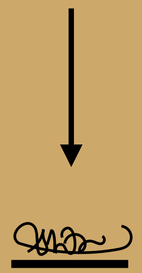
s_I



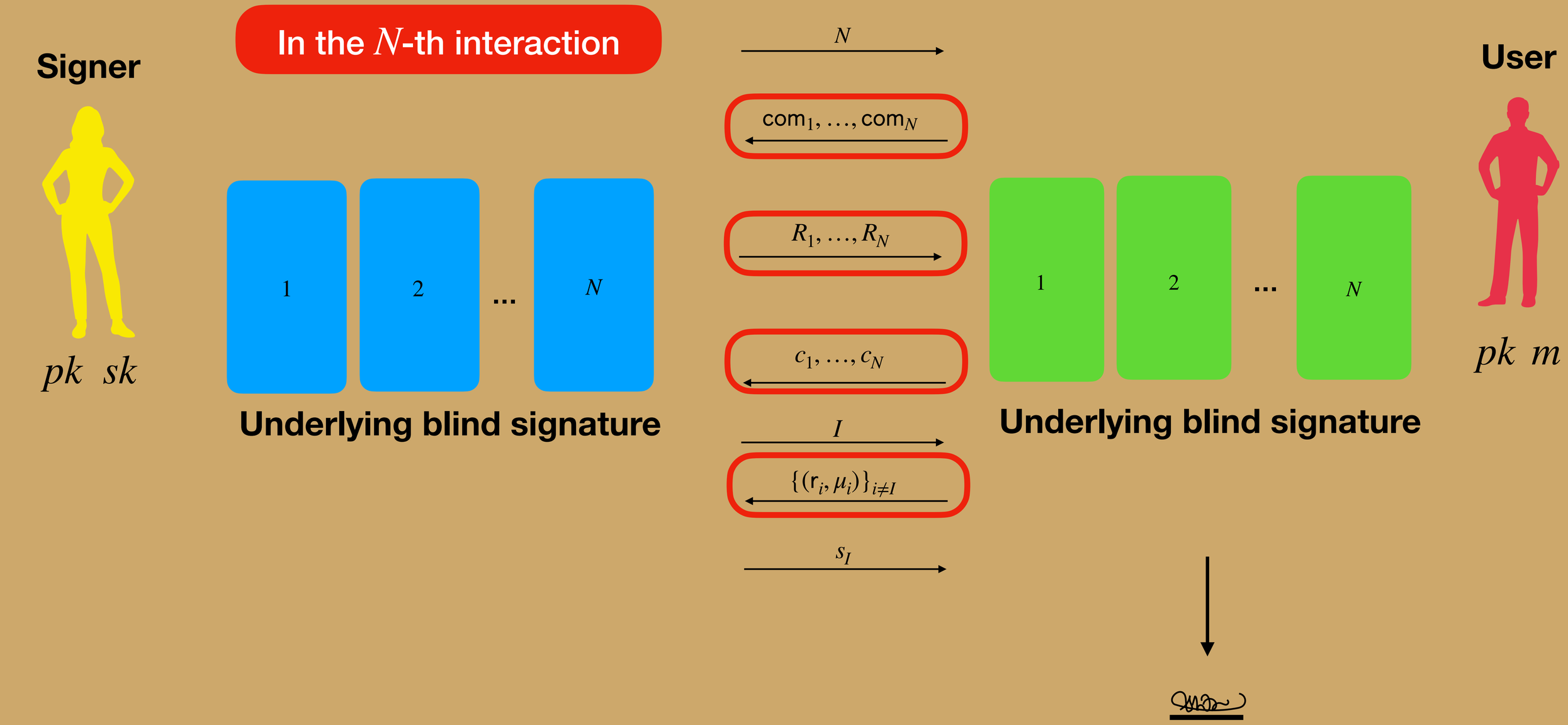
Underlying blind signature

User

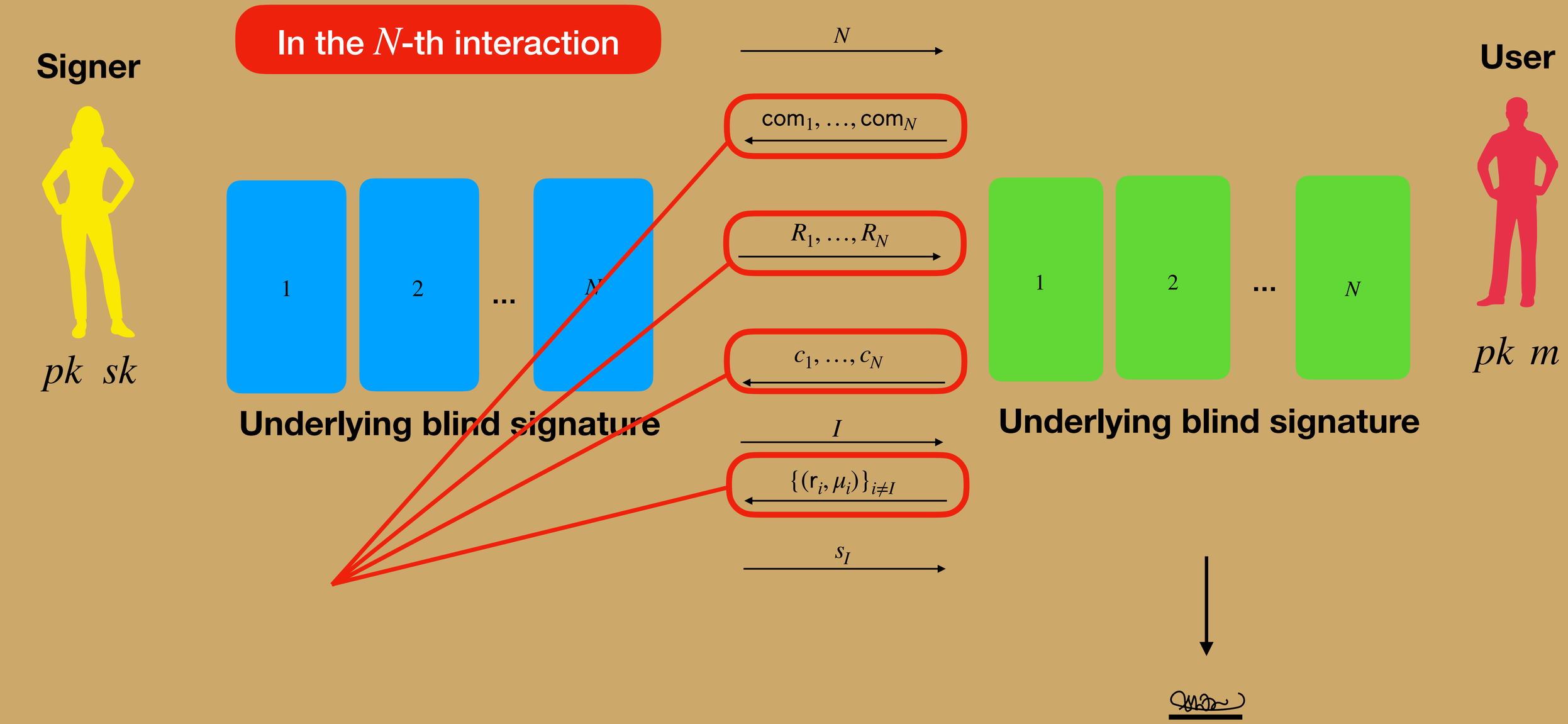
$pk \quad m$



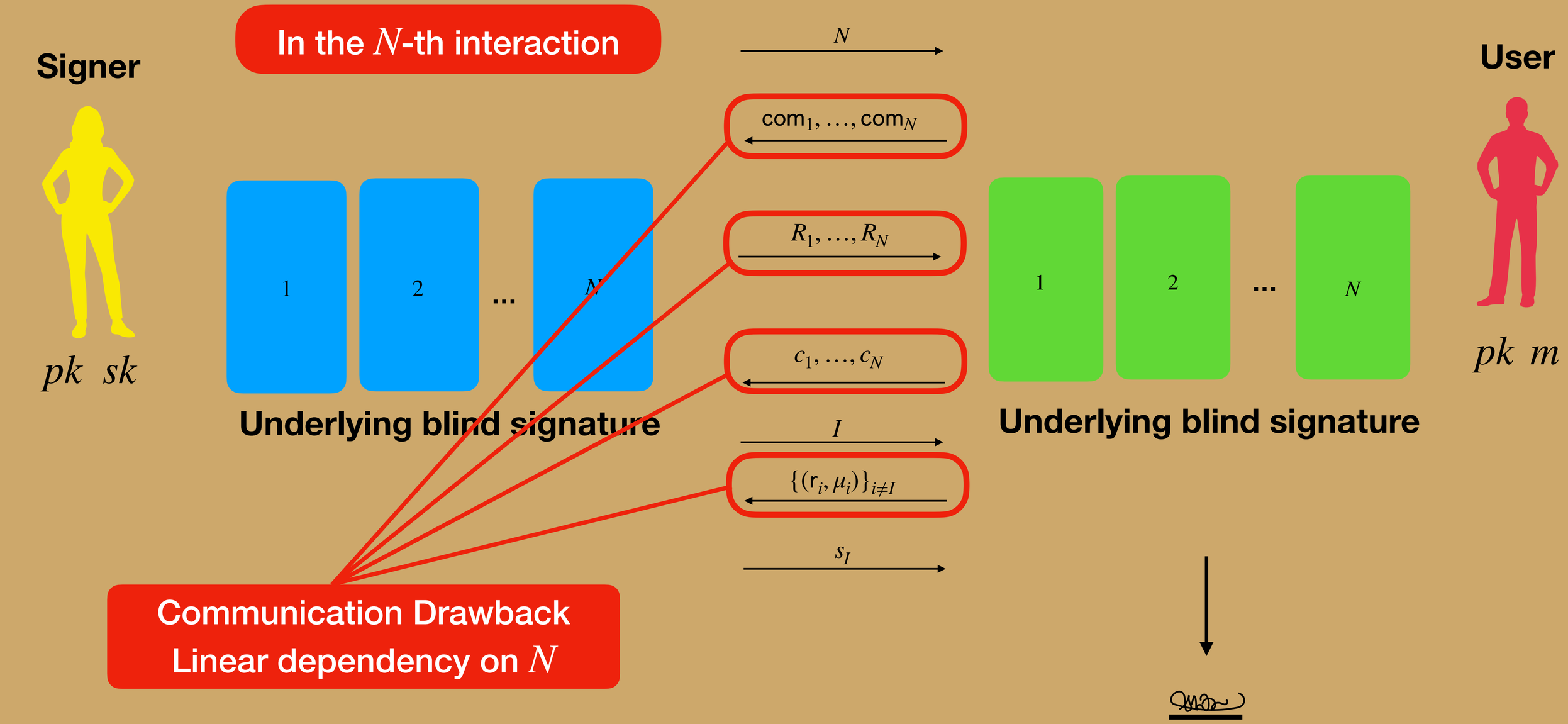
The Boosting Transform



The Boosting Transform



The Boosting Transform



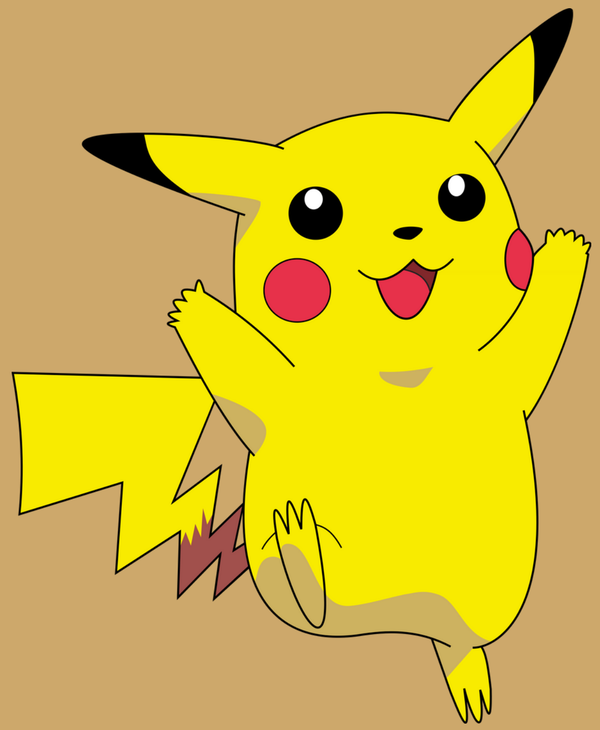
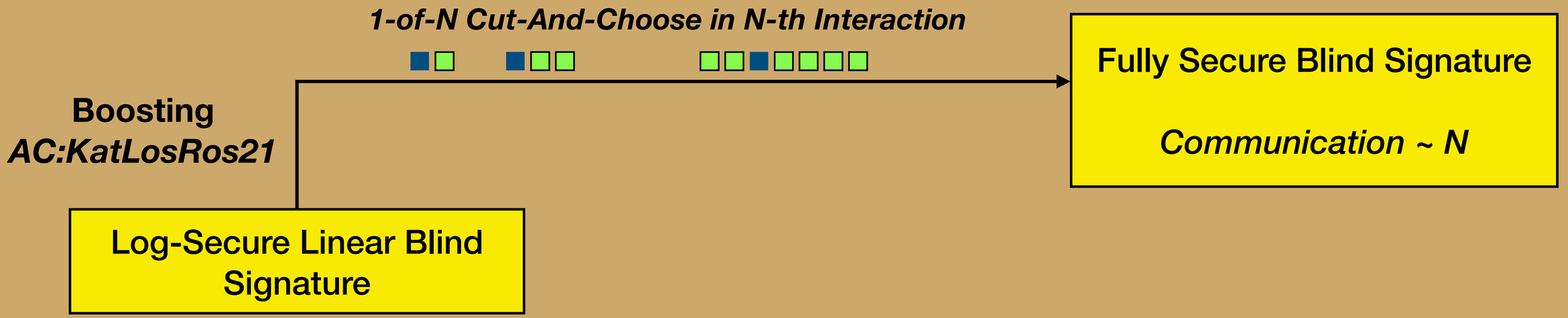


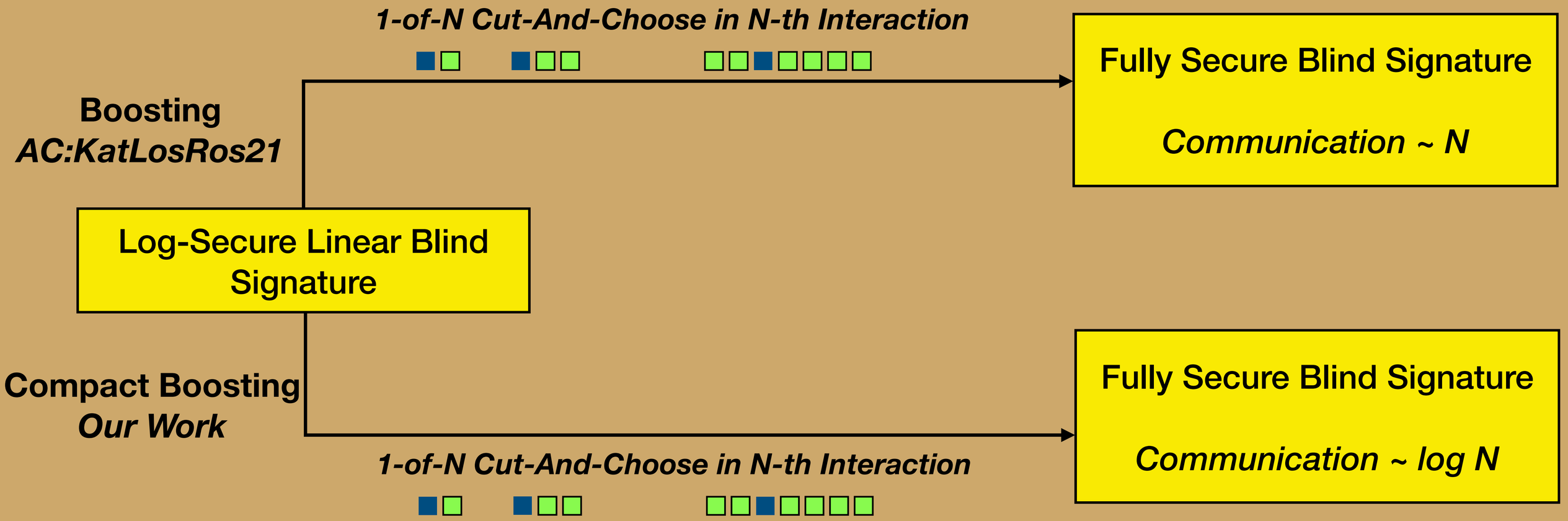
Image Source: shorturl.at/cDZ06

Our Results

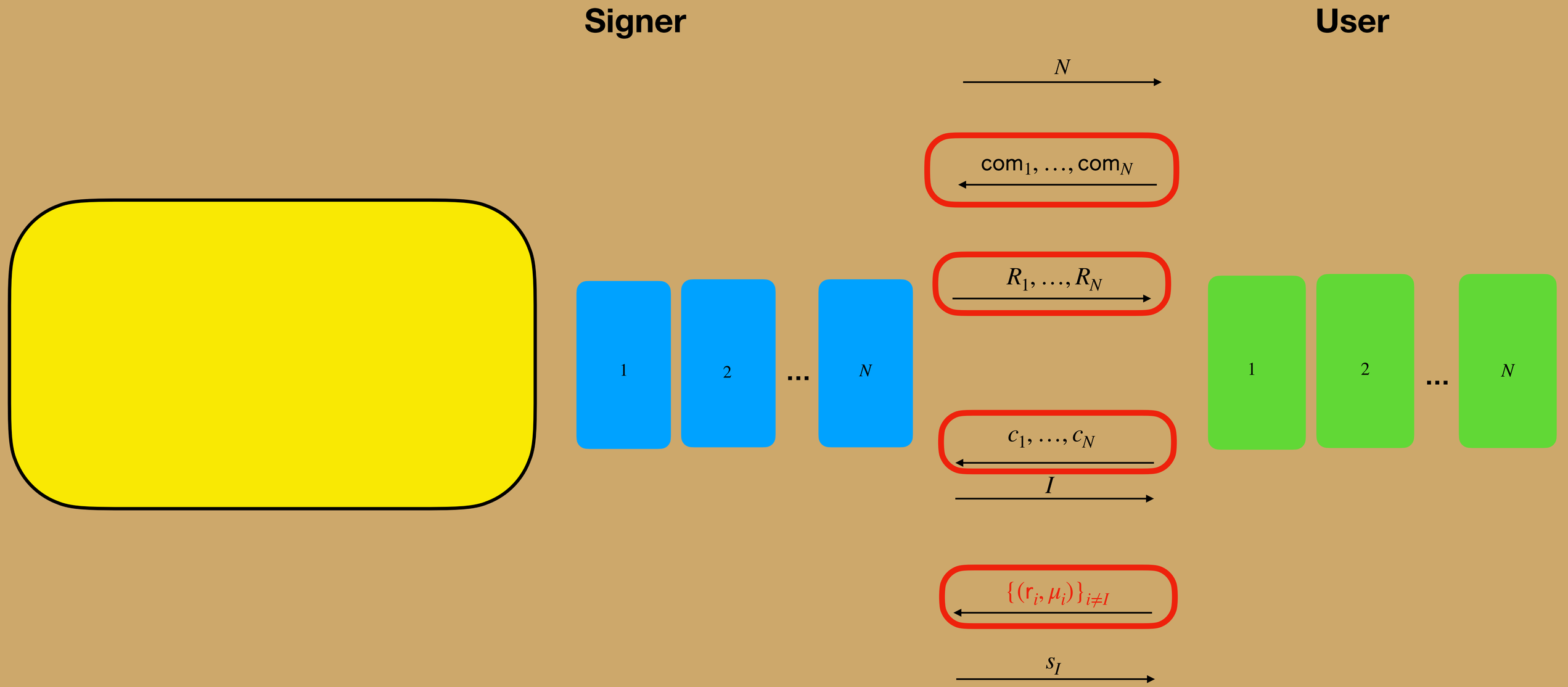
Our Results


1-of-N Cut-And-Choose in N-th Interaction
Boosting
AC:KatLosRos21
Log-Secure Linear Blind Signature
Fully Secure Blind Signature
Communication ~ N

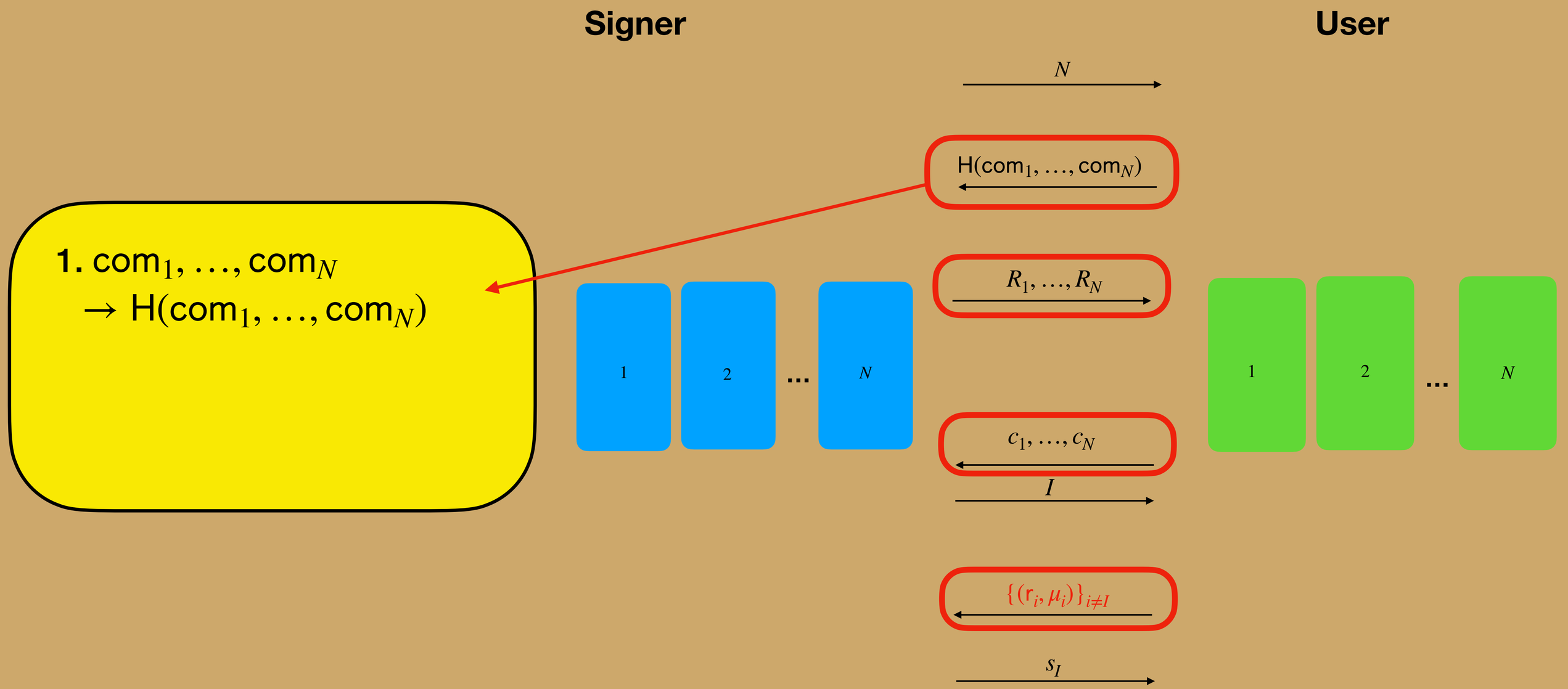
Our Results


1-of-N Cut-And-Choose in N-th Interaction
Boosting
AC:KatLosRos21
Log-Secure Linear Blind Signature
Compact Boosting
Our Work
1-of-N Cut-And-Choose in N-th Interaction
Fully Secure Blind Signature
Communication ~ N
Fully Secure Blind Signature
Communication ~ log N

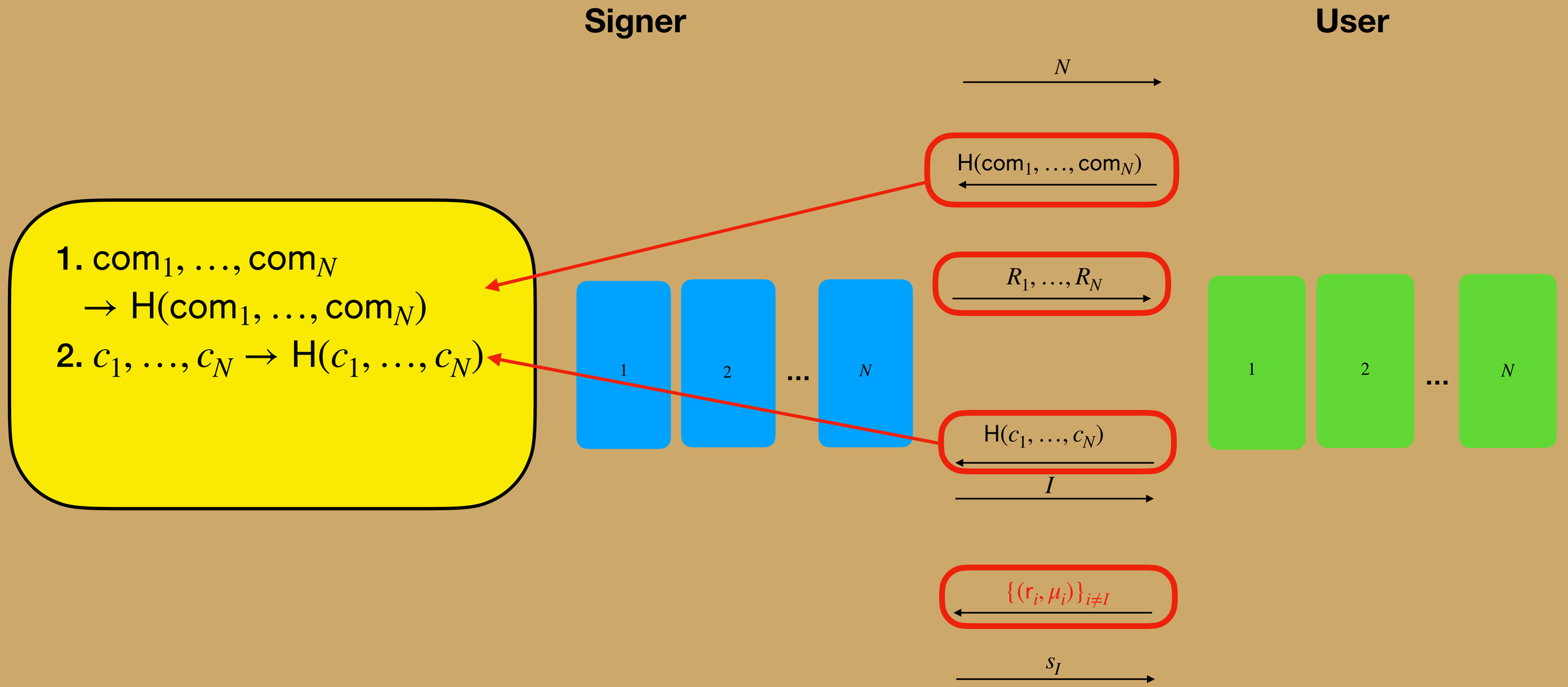
The *Compact* Boosting Transform



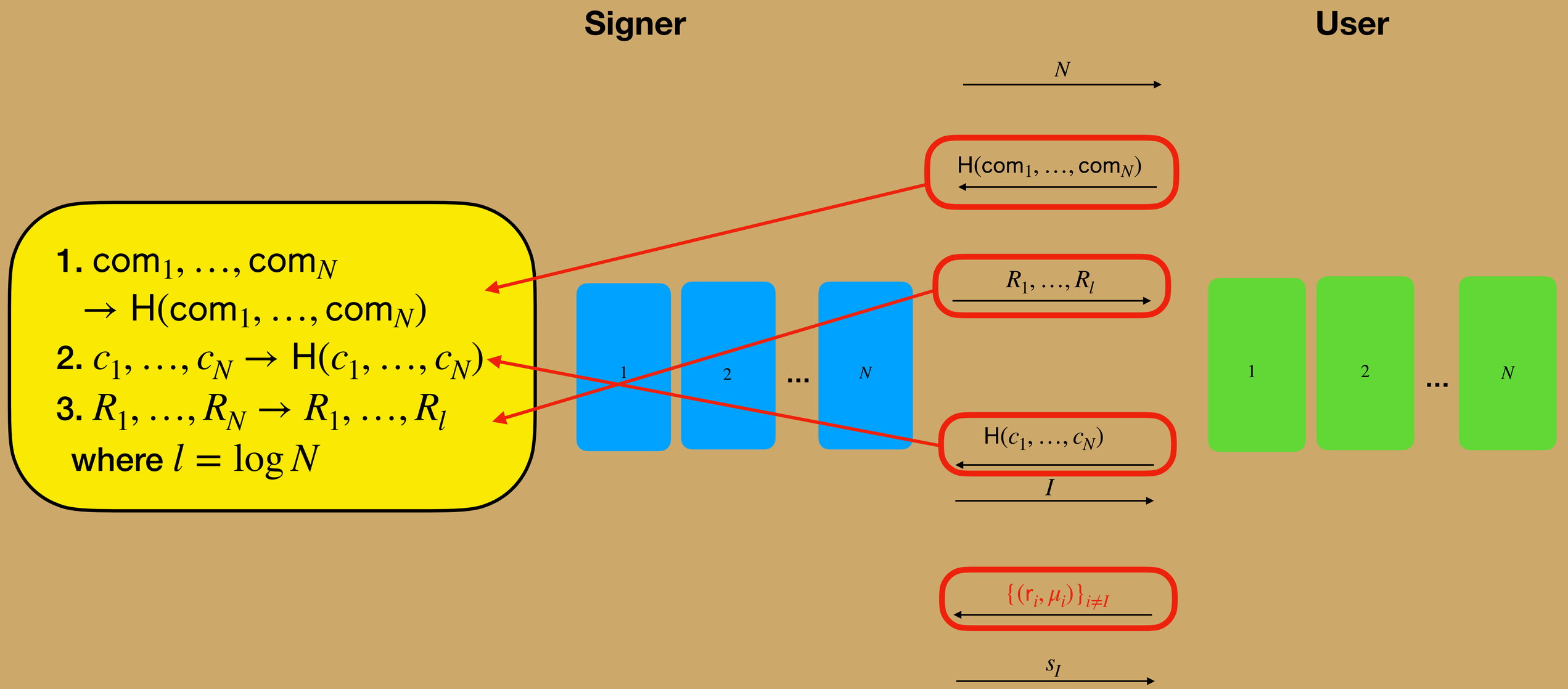
The *Compact* Boosting Transform



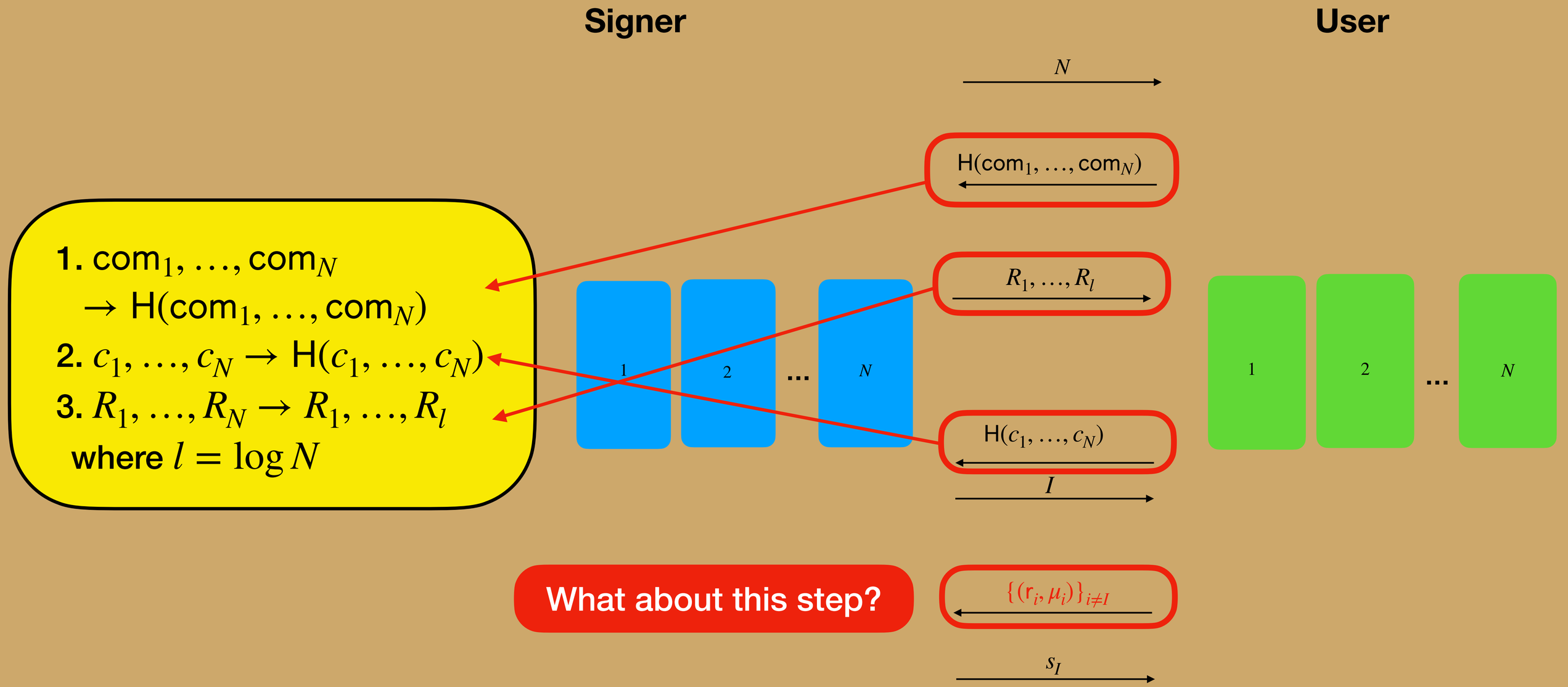
The *Compact* Boosting Transform



The *Compact* Boosting Transform



The *Compact* Boosting Transform



The *Compact* Boosting Transform

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**

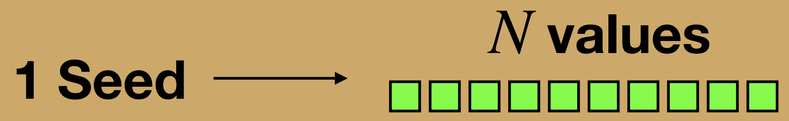
The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**

  1 Seed

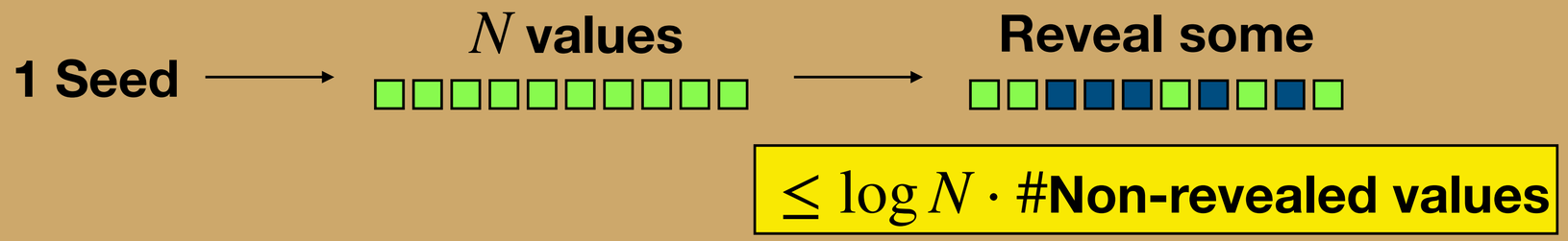
The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



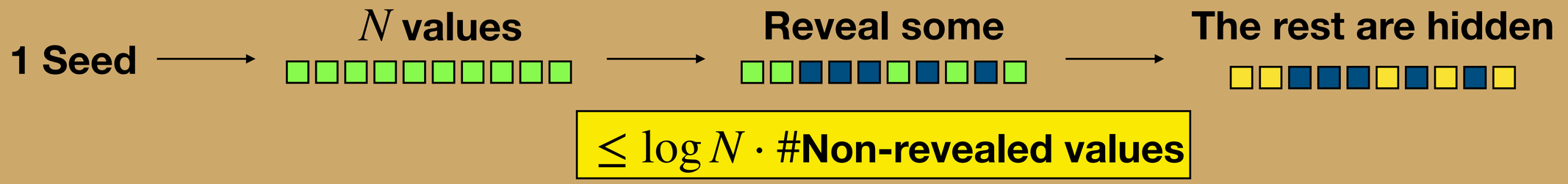
The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



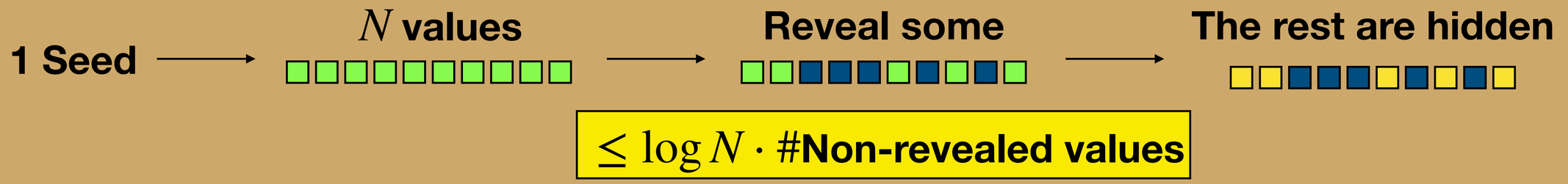
The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



The *Compact* Boosting Transform

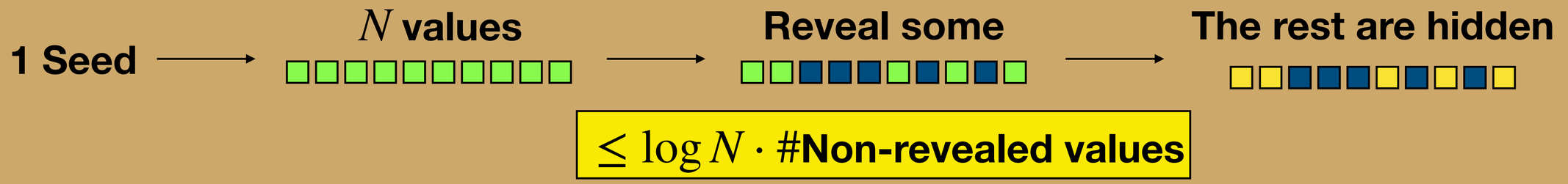
- **Puncturable Pseudorandom Function (PPRF) [SW14]**



- **Applying to Cut-and-Choose Transform**

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**

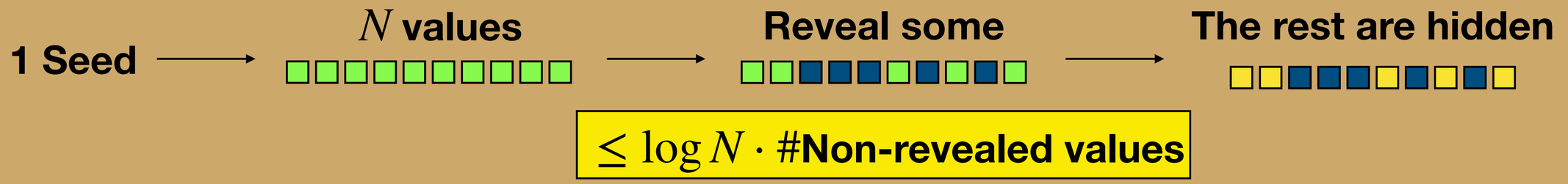


- **Applying to Cut-and-Choose Transform**

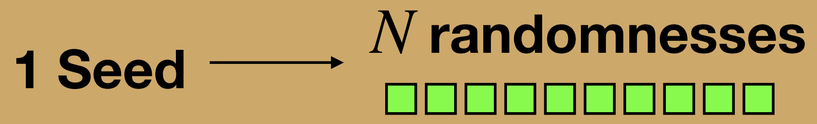
1 Seed

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**

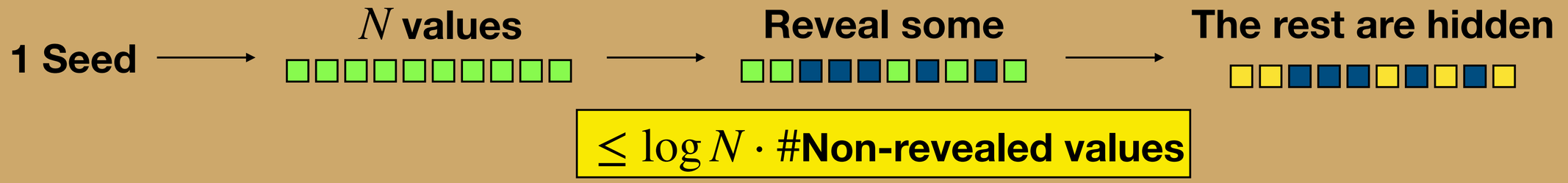


- **Applying to Cut-and-Choose Transform**



The *Compact* Boosting Transform

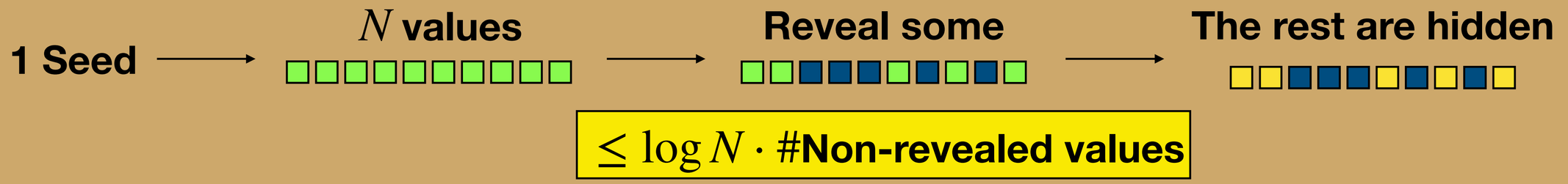
- **Puncturable Pseudorandom Function (PPRF) [SW14]**



- **Applying to Cut-and-Choose Transform**

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



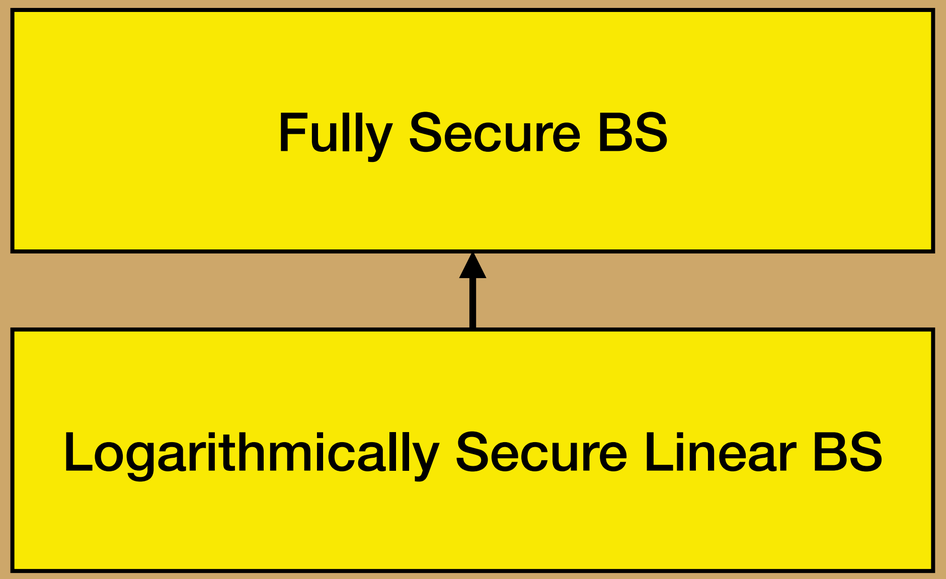
- **Applying to Cut-and-Choose Transform**

Now the protocol is $O(\log N)$ communication!

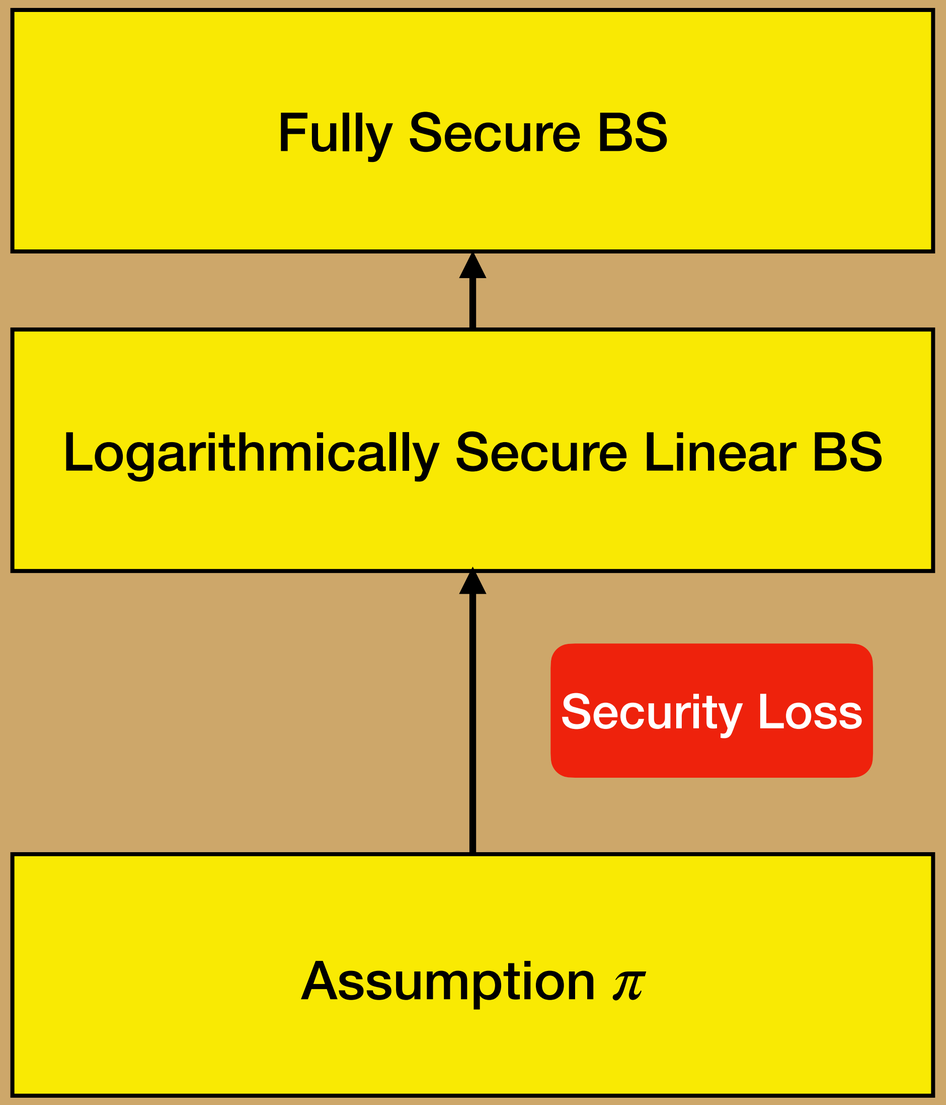
Source: shorturl.at/cDZ06

Remaining Problems

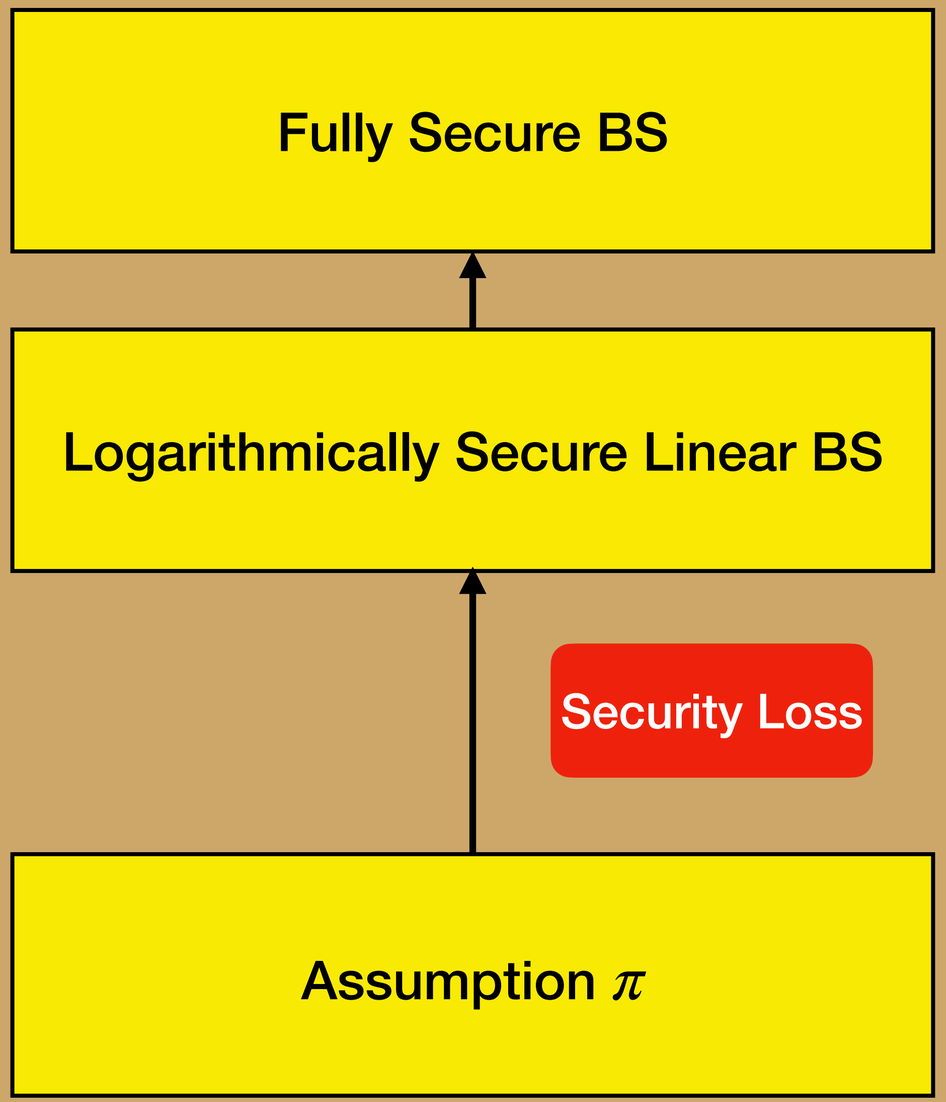
Remaining Problems



Remaining Problems



Remaining Problems



Communication $C_\pi \cdot \log(N) + C$
depends on Assumption!

Remaining Problems

Fully Secure BS

Logarithmically Secure Linear BS

Assumption π

Security Loss

Communication $C_\pi \cdot \log(N) + C$
depends on Assumption!

Inefficient Concrete Parameters

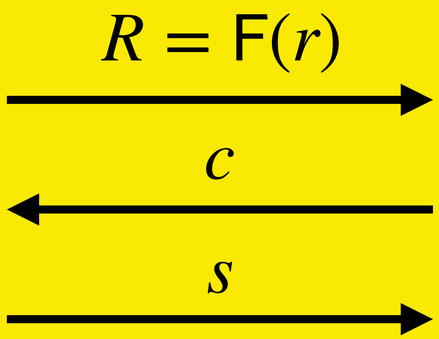
Schnorr:
2^{30} ***Signatures*** $\Longrightarrow$ ***~ 12000 Bit Group***

Source: shorturl.at/drsW5

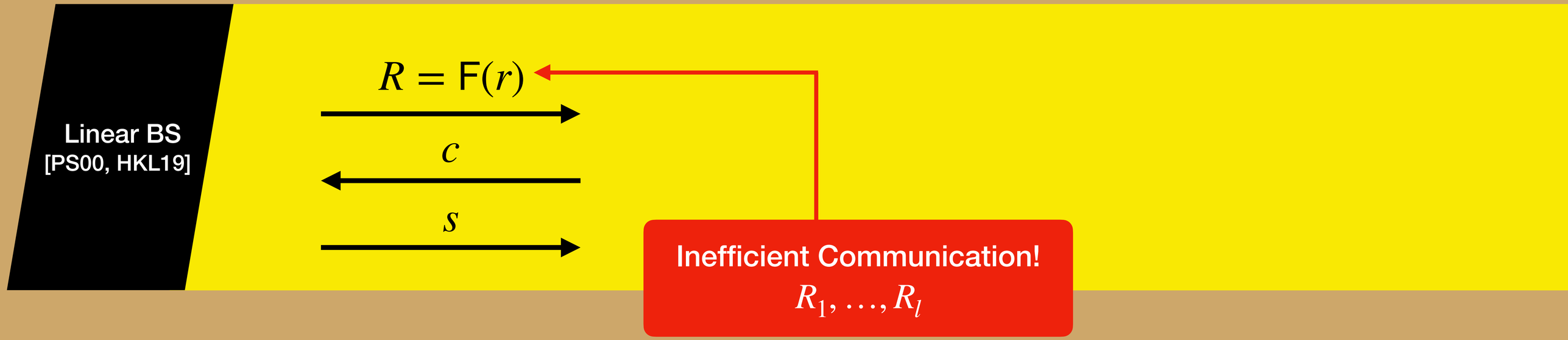
Improving Concrete Parameters

Improving Concrete Parameters

Linear BS
[PS00, HKL19]



Improving Concrete Parameters



Improving Concrete Parameters

Linear BS
[PS00, HKL19]

$R = \mathsf{F}(r)$

c

s

Inefficient Communication!
$R_1, \ldots, R_l$

BLS
[Bol03]

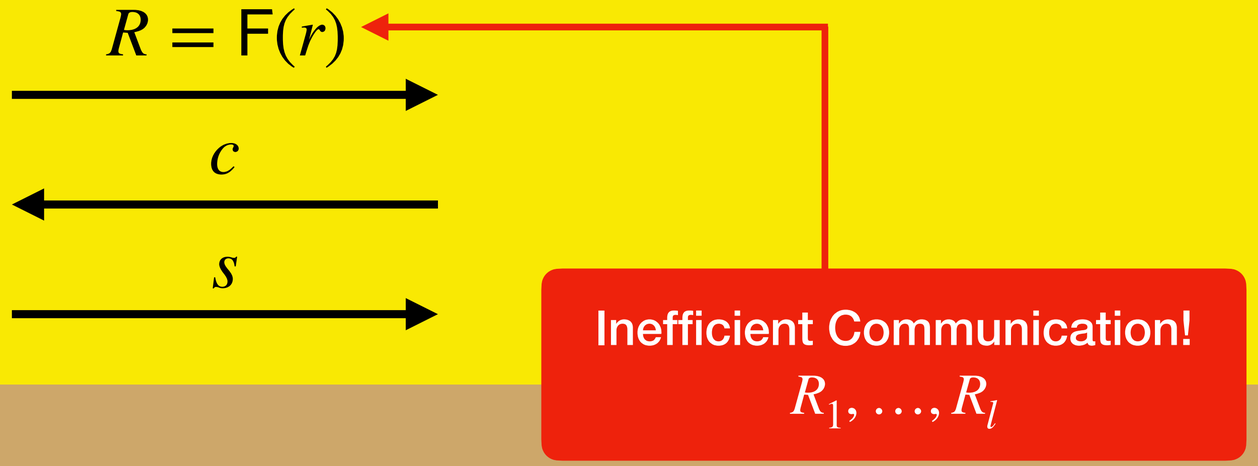
$pk = g^{sk}$

c $\quad c := H(m) \cdot g^{\alpha}$

$s := c^{sk}$ $\quad \sigma := s \cdot pk^{-\alpha}$

Improving Concrete Parameters

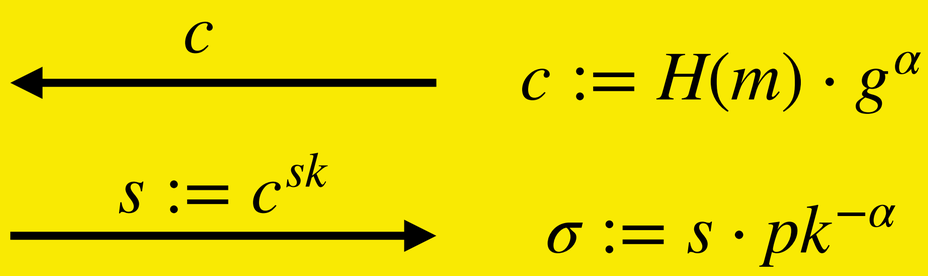
Linear BS
[PS00, HKL19]



★ Simulation knowing Message + Randomness

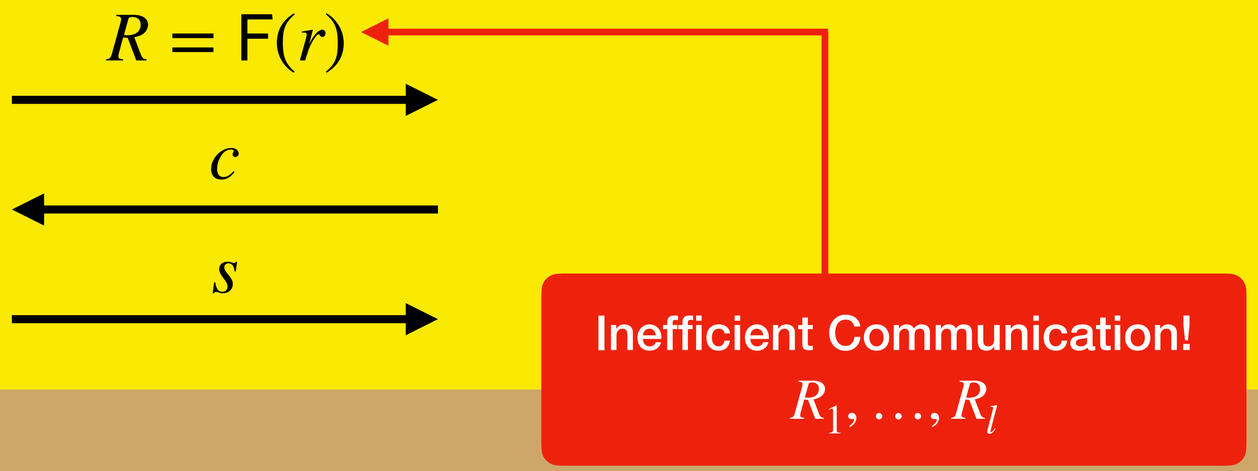
Logarithmic Security

BLS
[Bol03]



Improving Concrete Parameters

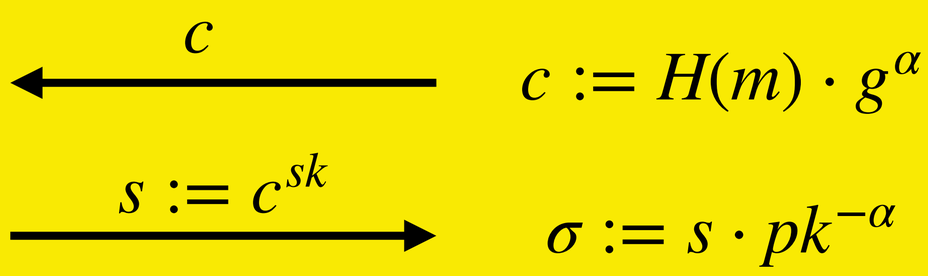
Linear BS
[PS00, HKL19]



★ Simulation knowing Message + Randomness

Logarithmic Security

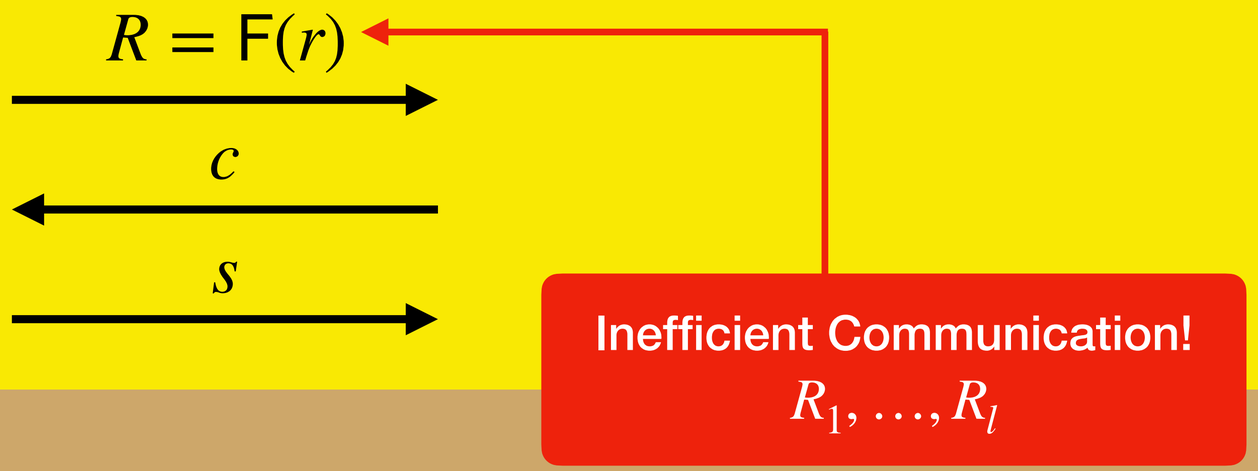
BLS
[Bol03]



★ Simulation knowing Message + Randomness

Improving Concrete Parameters

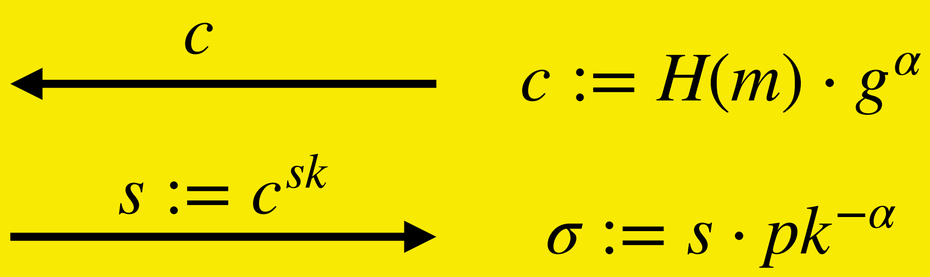
Linear BS
[PS00, HKL19]



★ **Simulation knowing Message + Randomness**

Logarithmic Security

BLS
[Bol03]



★ **Simulation knowing Message + Randomness**

Only Key-Only Security!

Parallel Instance Cut-and-Choose

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

Parallel Instance Cut-and-Choose

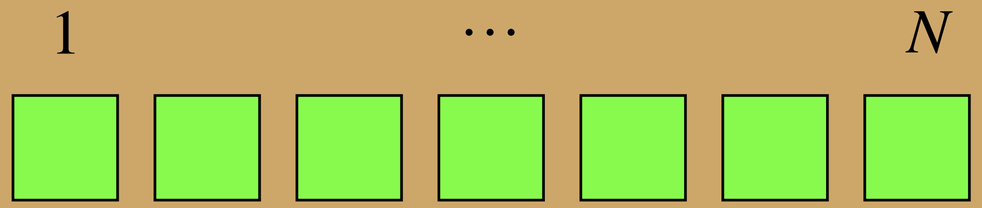
Source: shorturl.at/cDZ06

AC:KLR21 Idea

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

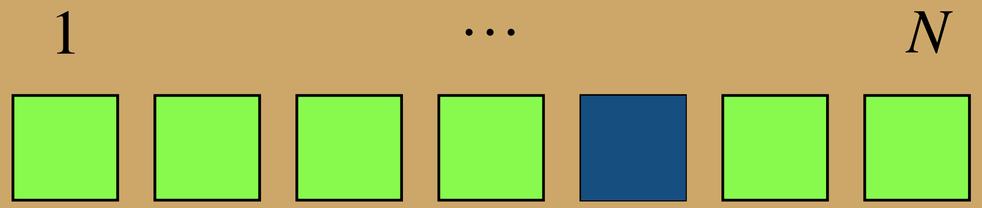
AC:KLR21 Idea



Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

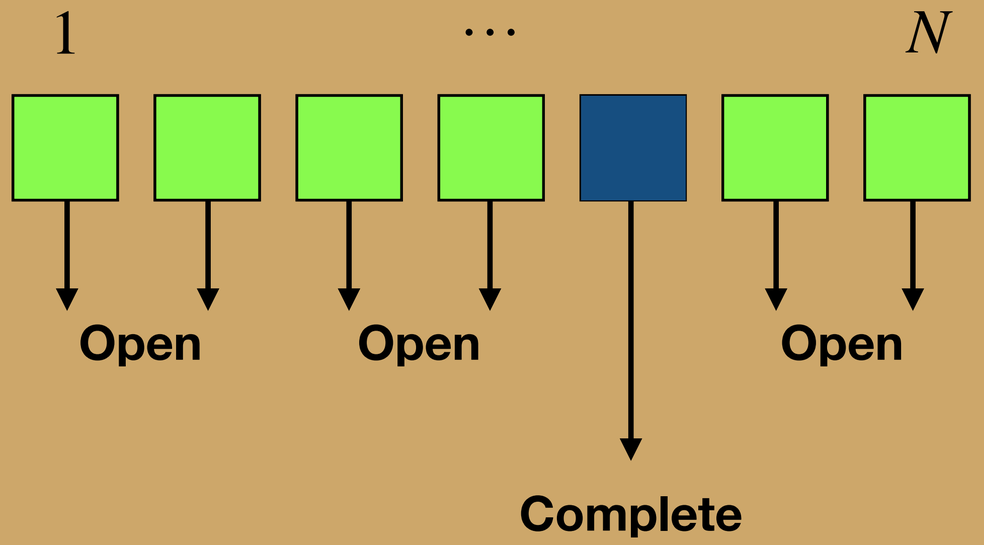
AC:KLR21 Idea



Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

AC:KLR21 Idea



Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

AC:KLR21 Idea

Malformed …

… more than one session

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

AC:KLR21 Idea

Malformed …

… more than one session

No Response Required

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

AC:KLR21 Idea

Malformed …

… more than one session

No Response Required

… no session

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

AC:KLR21 Idea

Malformed …

… more than one session

No Response Required

… no session

Response using ★

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

AC:KLR21 Idea

Malformed …

… more than one session

No Response Required

… no session

Response using ★

… exactly one session

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

AC:KLR21 Idea

Malformed …

… more than one session

No Response Required

… no session

Response using ★

… exactly one session

Need Signer Oracle

$$\Pr[\text{cheat}] = \frac{1}{N}$$

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

AC:KLR21 Idea

Interactions

...

$$\Pr[\text{cheat}] = \frac{1}{2} \qquad \Pr[\text{cheat}] = \frac{1}{3} \qquad \Pr[\text{cheat}] = \frac{1}{q}$$

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

AC:KLR21 Idea

Interactions

$$\Pr[\text{cheat}] = \frac{1}{2} \qquad \Pr[\text{cheat}] = \frac{1}{3} \qquad \Pr[\text{cheat}] = \frac{1}{q}$$

$$\mathbb{E}[\#\text{cheat}] = \sum_{i=2}^{q} \frac{1}{i} \leq \Theta(\log q)$$

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

Our Idea

Interactions →

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

Our Idea

Interactions →

1. Scale

$\mathbb{E}[\#\text{cheat}] < 1$

$\Pr[\#\text{cheat} \geq 1] \leq const$

Source: shorturl.at/kNPR7

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

Our Idea

Interactions →

1. Scale

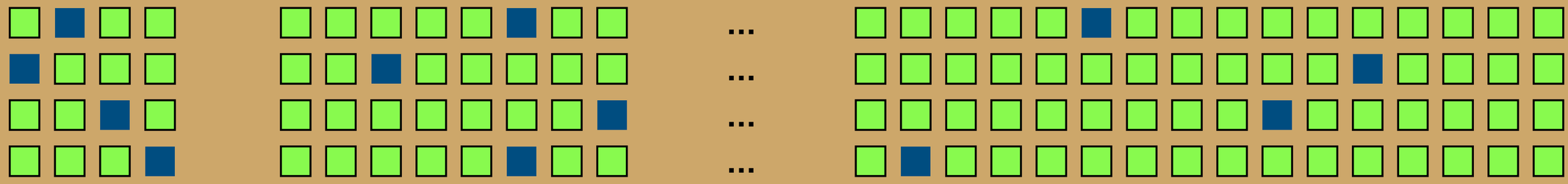
pk 

$\mathbb{E}[\#\text{cheat}] < 1$

$\Pr[\#\text{cheat} \geq 1] \leq const$

Source: shorturl.at/kNPR7

2. Parallel Instance

pk_1 

pk_K

$\Pr[\exists i^* : \#\text{cheat}_{i^*} < 1] \geq 1 - negl$

Parallel Instance Cut-and-Choose

Source: shorturl.at/cDZ06

Our Idea

Interactions →

1. Scale

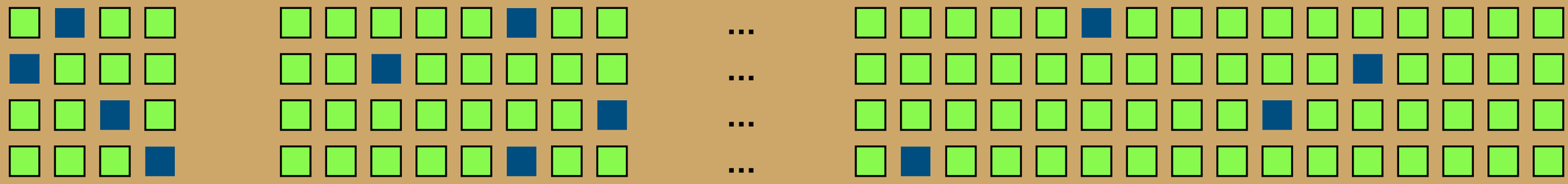
pk 

$\mathbb{E}[\#\text{cheat}] < 1$

$\Pr[\#\text{cheat} \geq 1] \leq const$

Source: shorturl.at/kNPR7

2. Parallel Instance

pk_1 

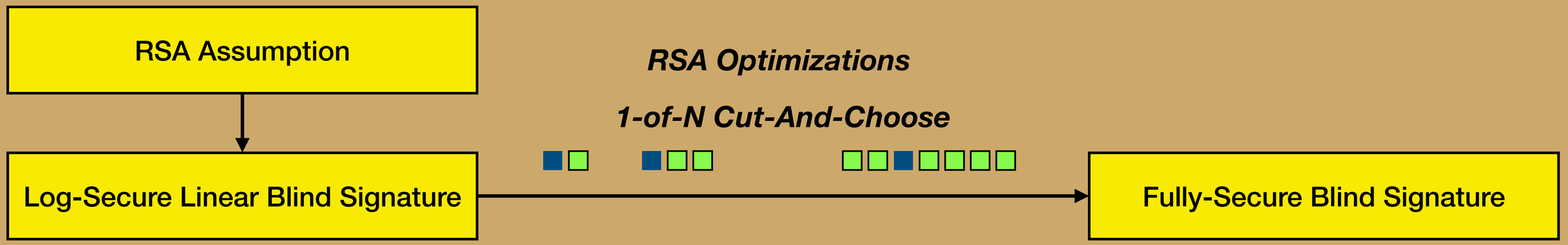
pk_K

$\Pr[\exists i^* : \#\text{cheat}_{i^*} < 1] \geq 1 - negl$

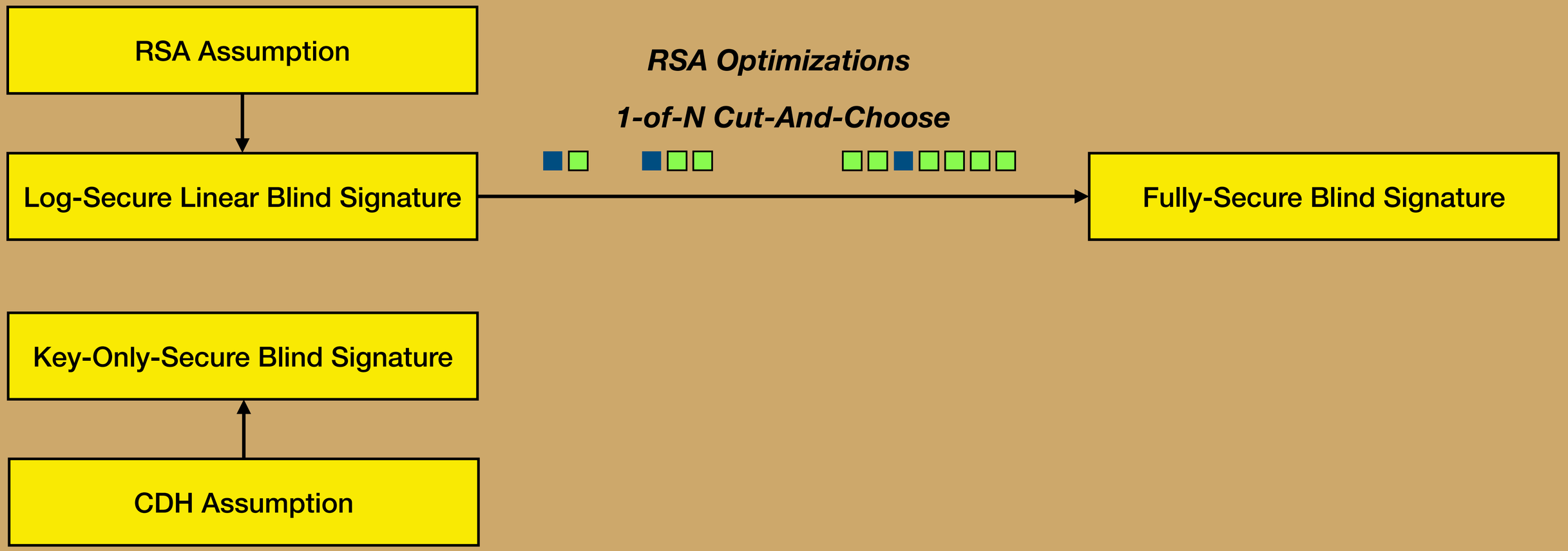
Aggregate: $\sigma_1, \ldots, \sigma_K \Longrightarrow \bar{\sigma}$

Concrete Schemes

Concrete Schemes



Concrete Schemes



Concrete Schemes

RSA Assumption

Log-Secure Linear Blind Signature

RSA Optimizations

1-of-N Cut-And-Choose

Fully-Secure Blind Signature

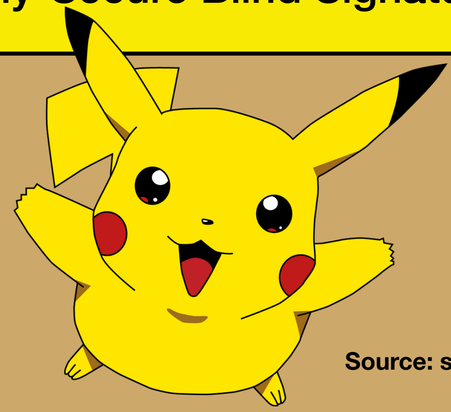
Key-Only-Secure Blind Signature

Parallel Instance 1-of-N Cut-And-Choose

Fully-Secure Blind Signature

CDH Assumption

CDH Optimizations



Source: shorturl.at/EKPQX

Overview

Overview

Generic

Overview


Generic
AC:KatLosRos21
$\Theta(N)$ Communication
Ours
$\Theta(\log N)$ Communication

Overview

Generic

AC:KatLosRos21
$\Theta(N)$ **Communication**

Ours
$\Theta(\log N)$ **Communication**

Concrete

Overview

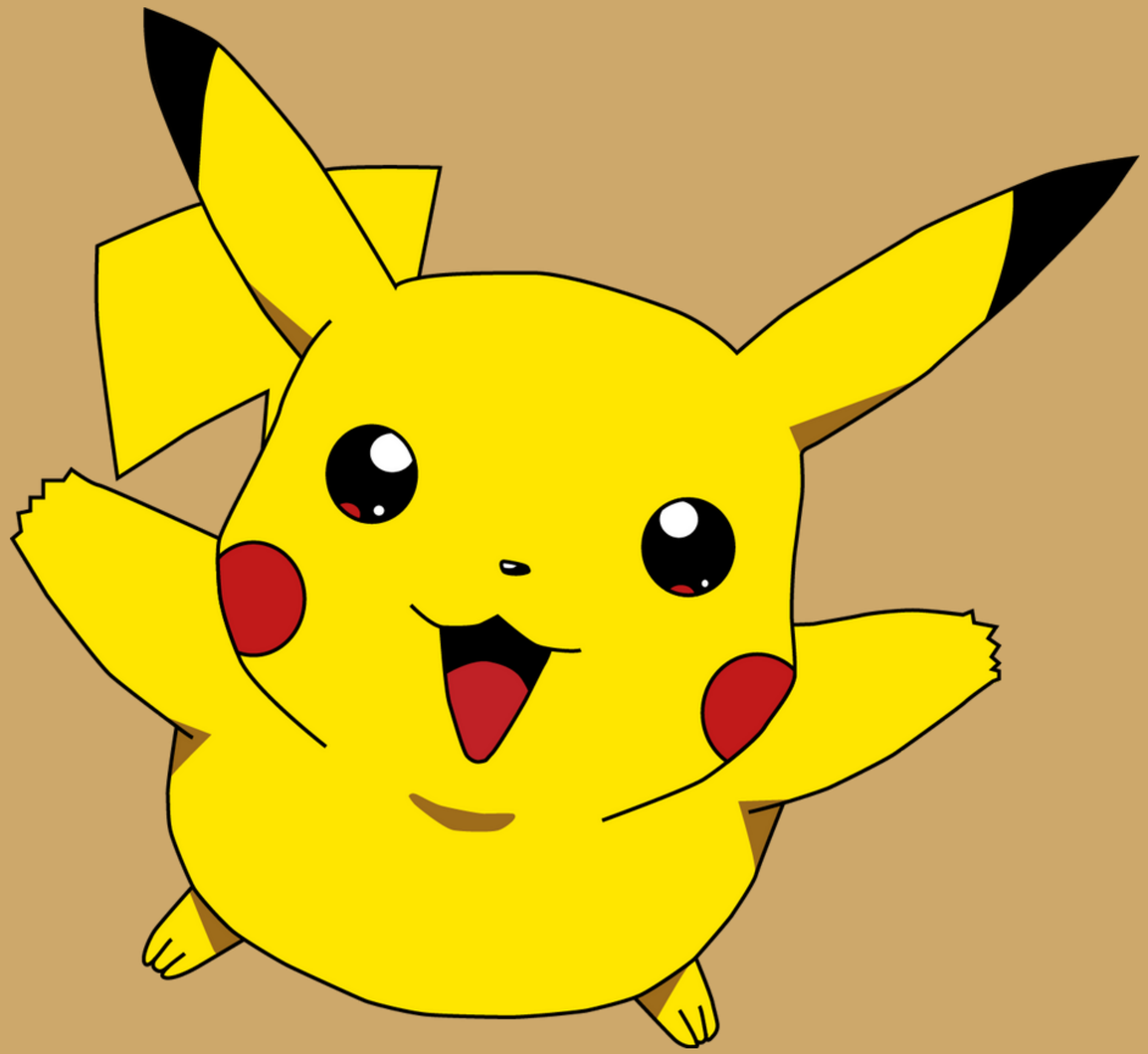
Generic

AC:KatLosRos21
$\Theta(N)$ **Communication**

Ours
$\Theta(\log N)$ **Communication**

Concrete

Assumption	Max. Communication	Signature Size
RSA	8 KB	9 KB
CDH	120 KB	3 KB



https://ia.cr/2022/007

Source: shorturl.at/EKPQX

The Boosting Transform

The Boosting Transform

Signer

User

The Boosting Transform

Signer

In the N-th interaction

User

The Boosting Transform

Signer

In the N-th interaction

N

User

The Boosting Transform

Signer

In the N-th interaction

N

(r_1, μ_1) (r_2, μ_2) ... (r_I, μ_I) ... (r_N, μ_N)

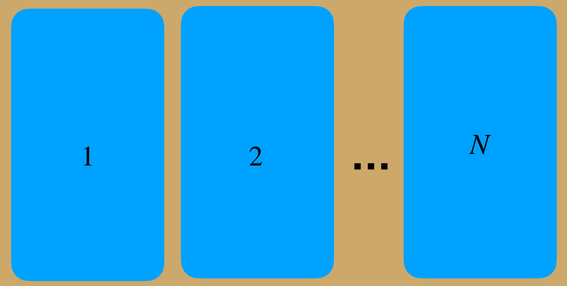
User

The Boosting Transform

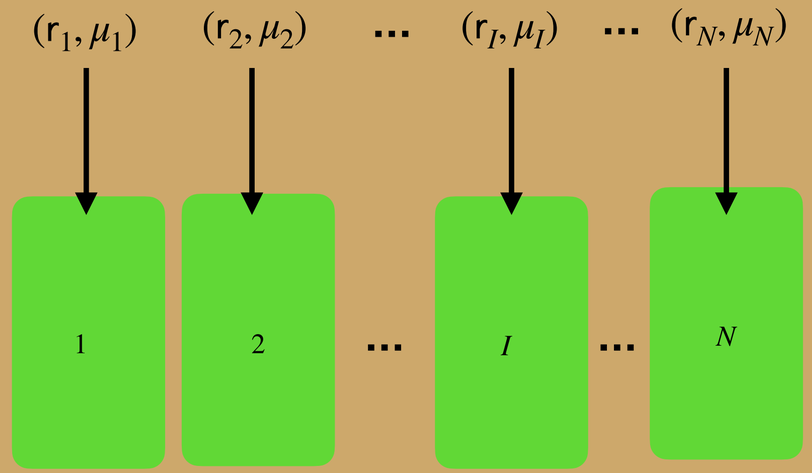
Signer

In the N-th interaction

N



Signer's side of the original blind signature protocol



User

User's side of the original blind signature protocol

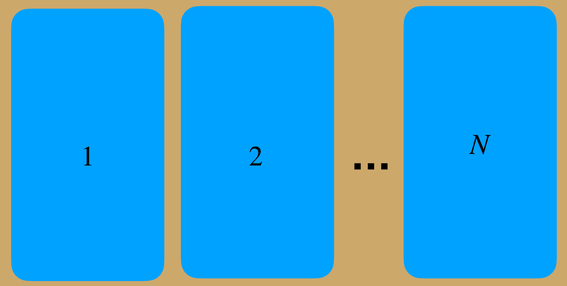
The Boosting Transform

Signer

In the N-th interaction

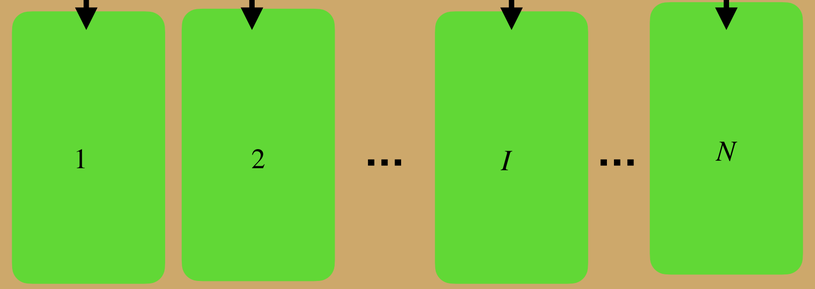
N

$\mathsf{com}_1, \ldots, \mathsf{com}_N$



Signer's side of the original blind signature protocol

(r_1, μ_1) (r_2, μ_2) ... (r_I, μ_I) ... (r_N, μ_N)



User

User's side of the original blind signature protocol

The Boosting Transform

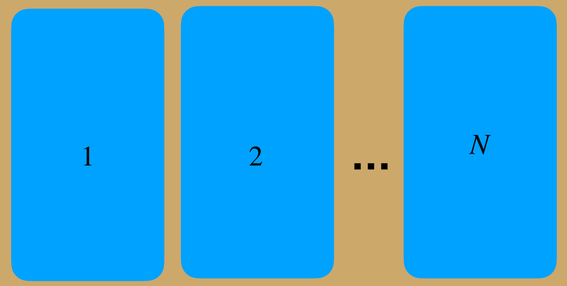
Signer

In the N-th interaction

N

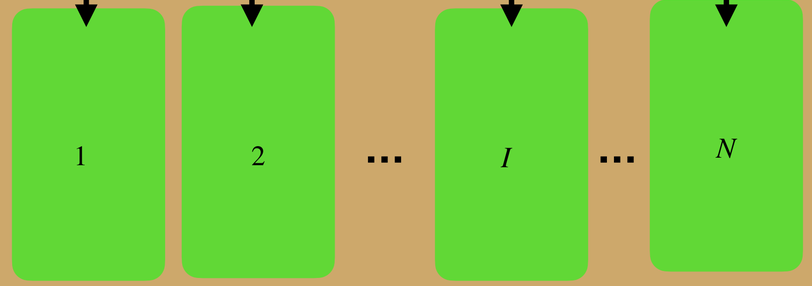
$\mathsf{com}_1, \ldots, \mathsf{com}_N$

$R_1, \ldots, R_N$



Signer's side of the original blind signature protocol

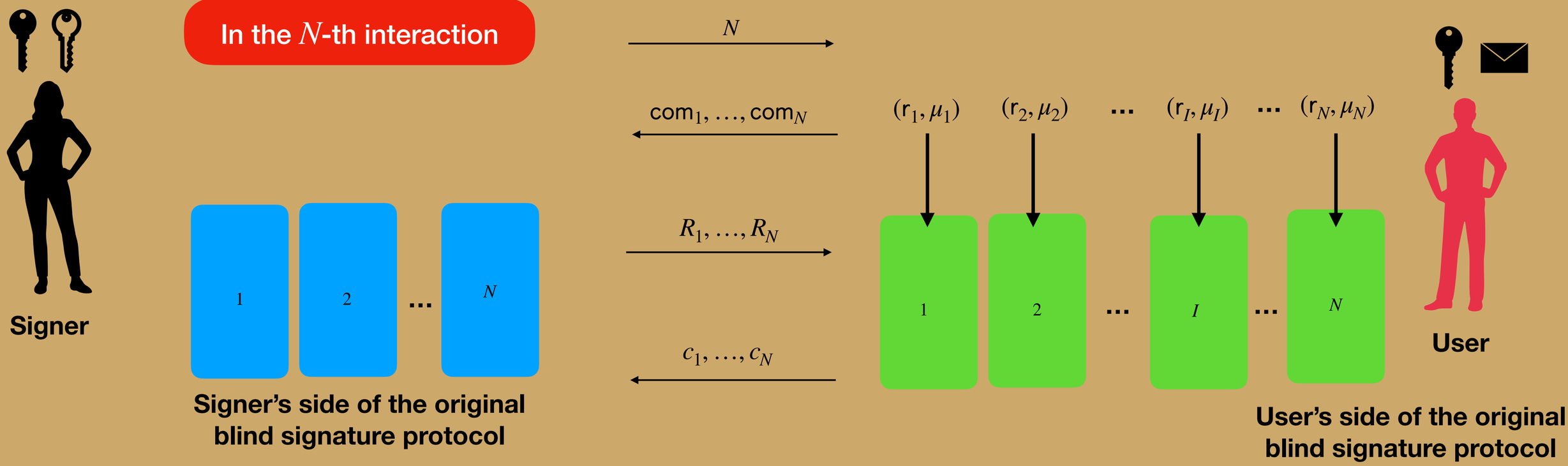
(r_1, μ_1) (r_2, μ_2) ... (r_I, μ_I) ... (r_N, μ_N)



User

User's side of the original blind signature protocol

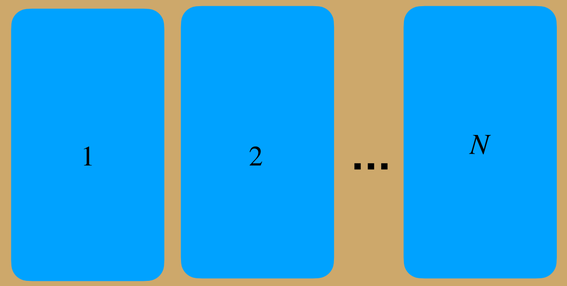
The Boosting Transform



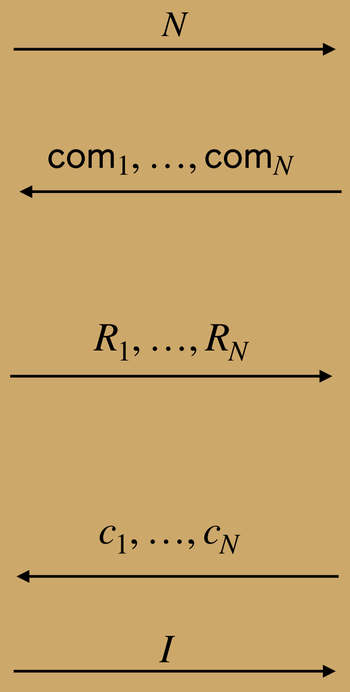
The Boosting Transform

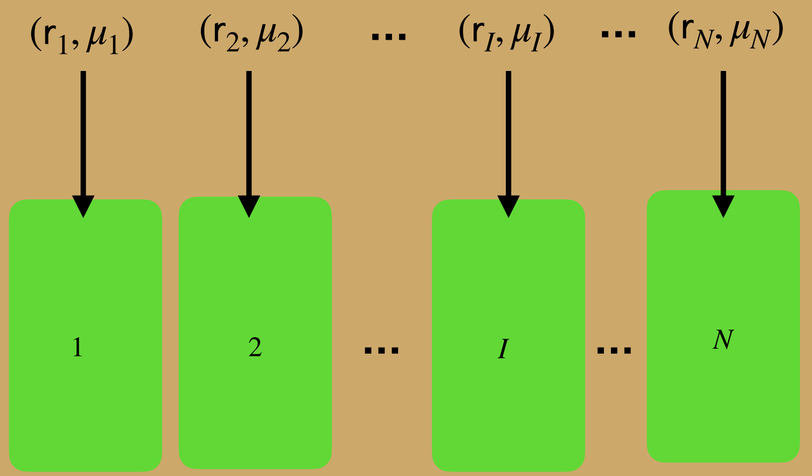
Signer

In the N-th interaction



Signer's side of the original blind signature protocol





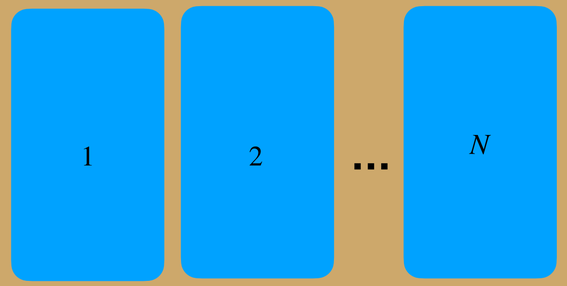
User

User's side of the original blind signature protocol

The Boosting Transform

Signer

In the N-th interaction



Signer's side of the original blind signature protocol

N

$\mathsf{com}_1, \ldots, \mathsf{com}_N$

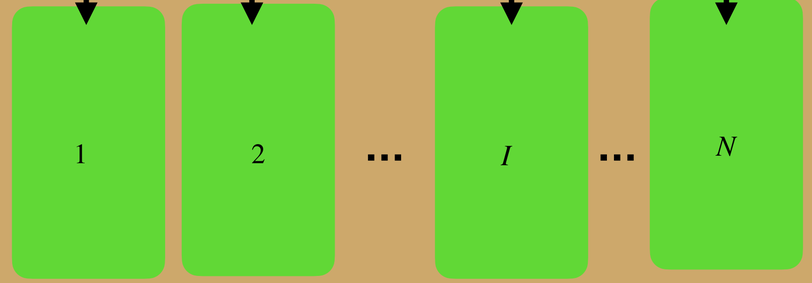
$R_1, \ldots, R_N$

$c_1, \ldots, c_N$

I

$\{(\mathsf{r}_i, \mu_i)\}_{i \neq I}$

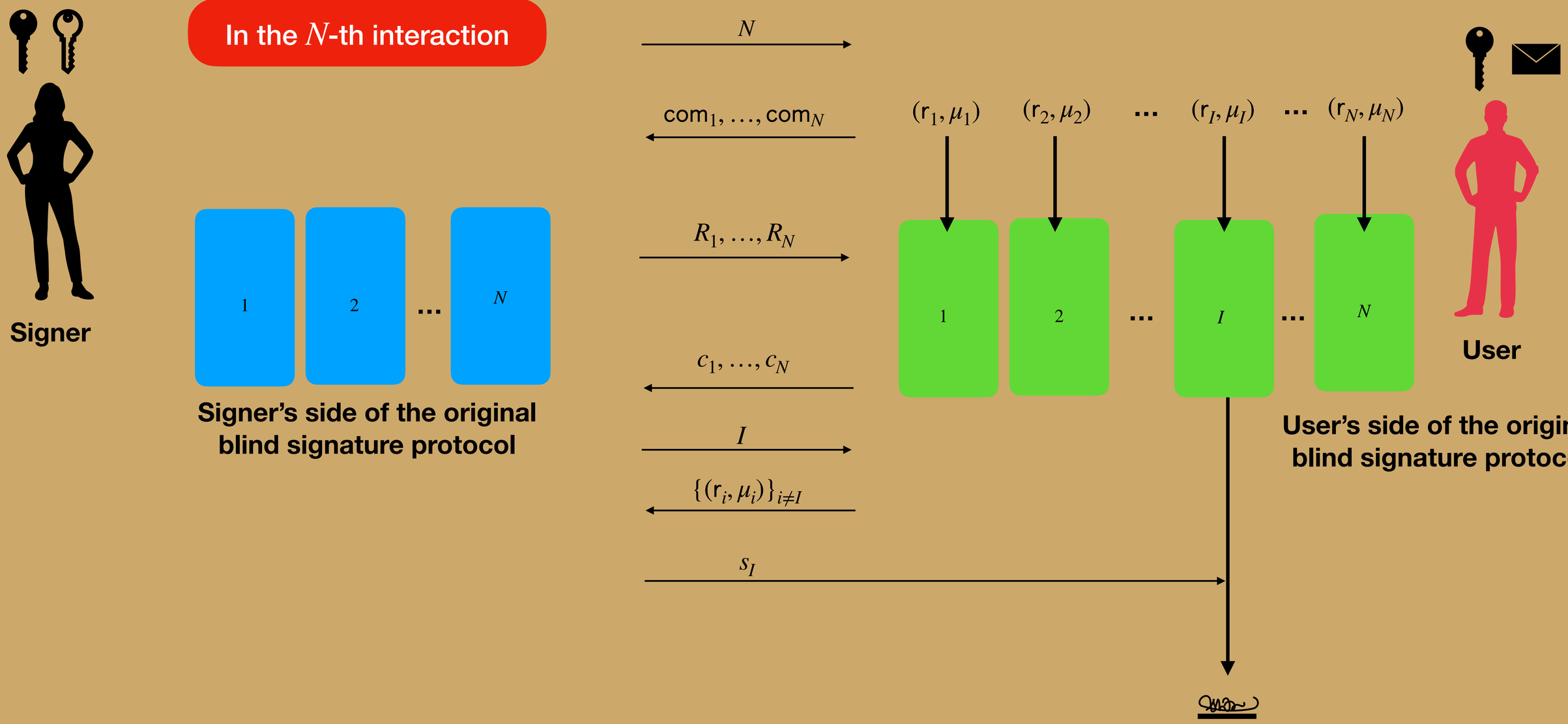
(r_1, μ_1) (r_2, μ_2) ... (r_I, μ_I) ... (r_N, μ_N)



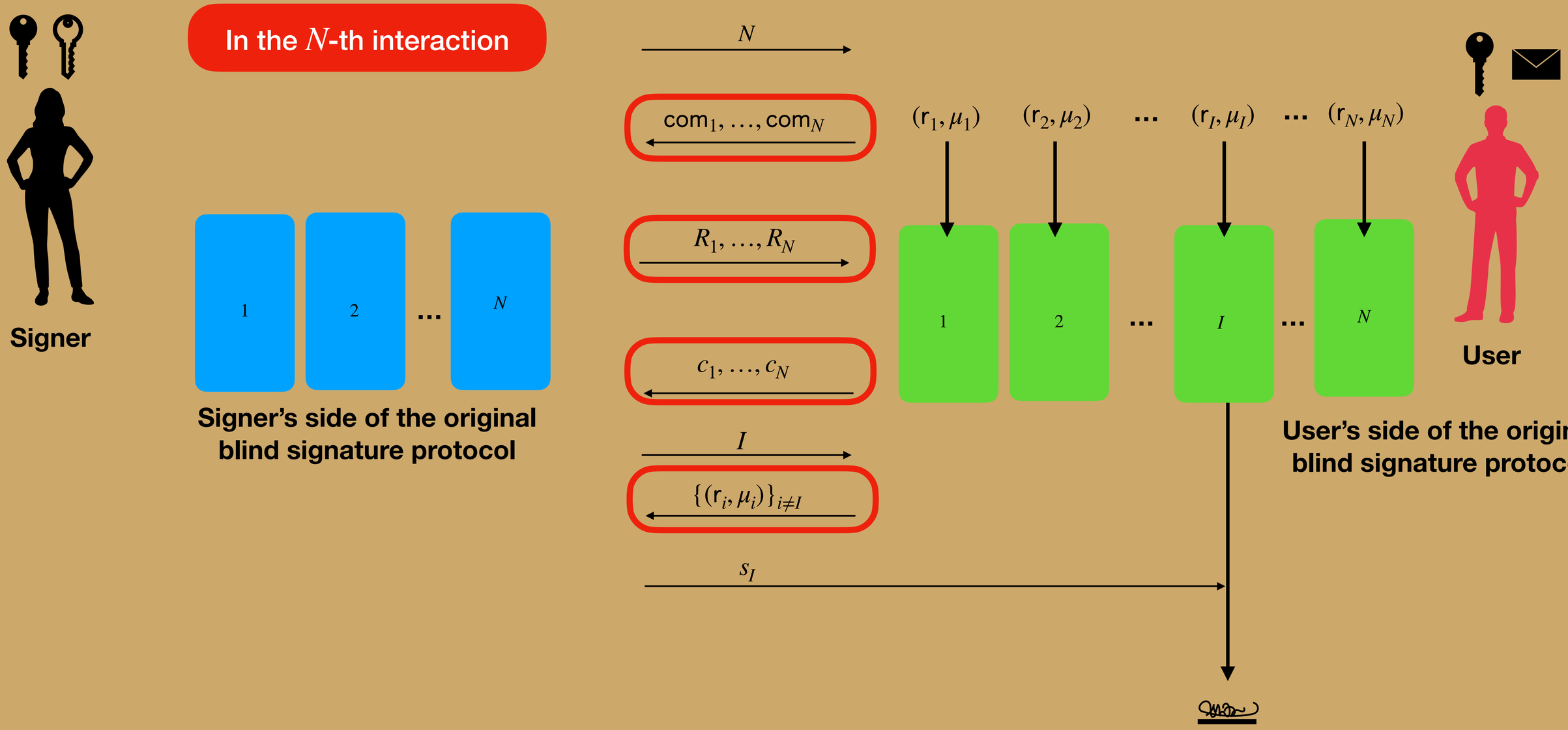
User

User's side of the original blind signature protocol

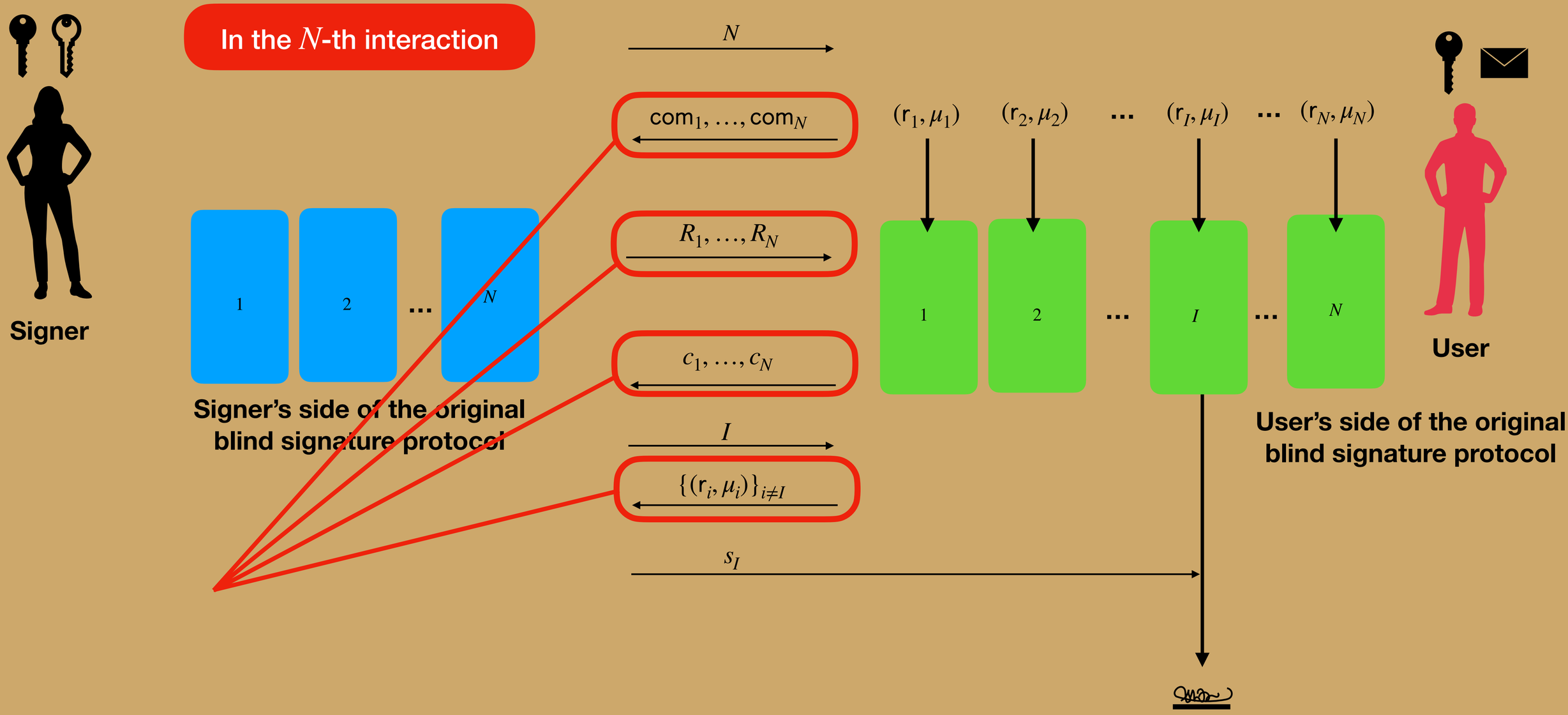
The Boosting Transform



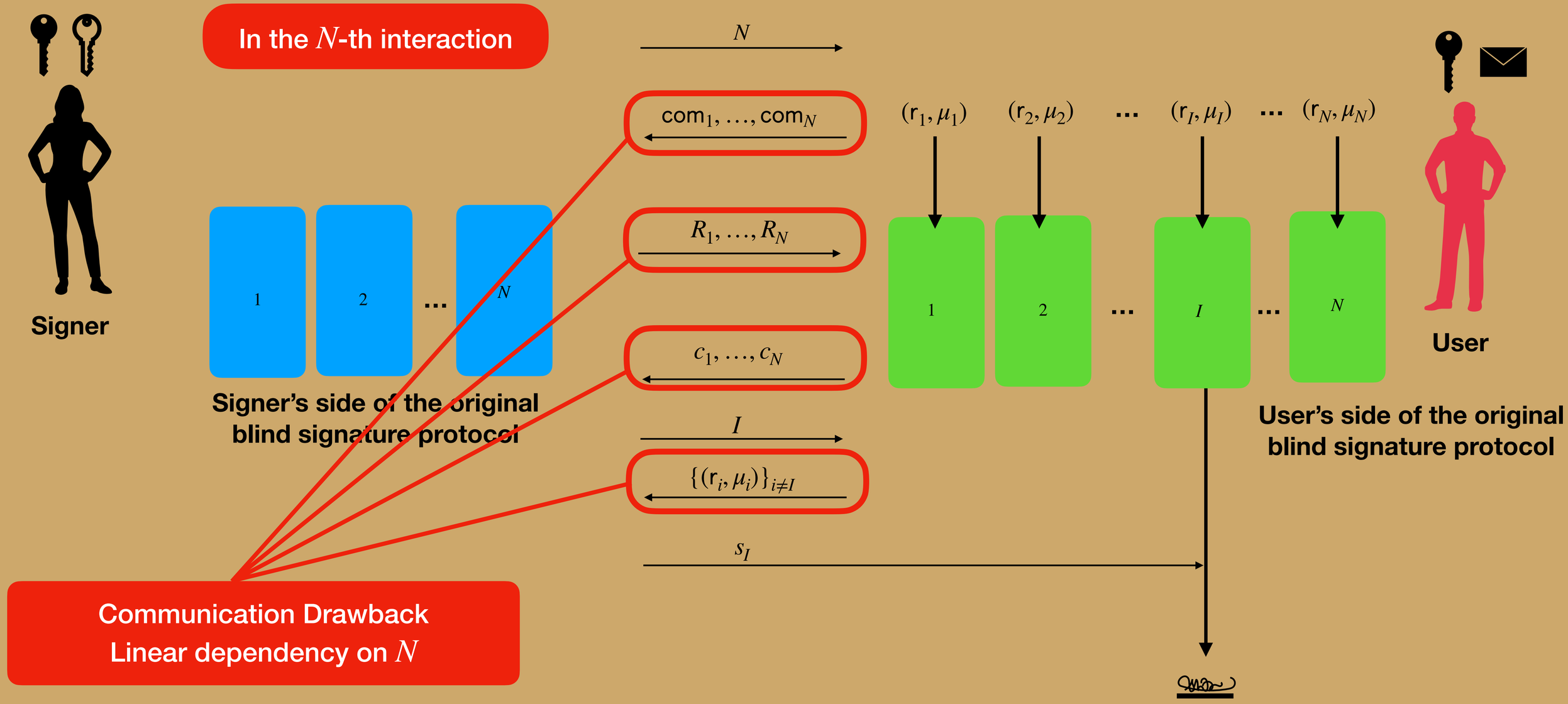
The Boosting Transform



The Boosting Transform



The Boosting Transform



The *Compact* Boosting Transform

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**

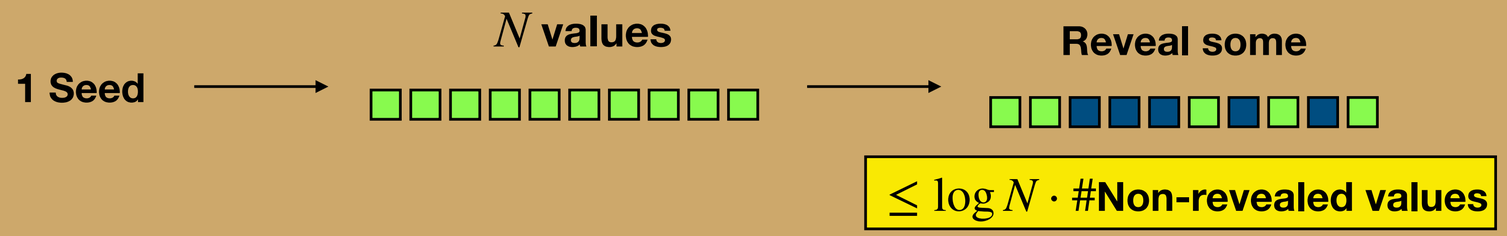
  1 Seed

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**

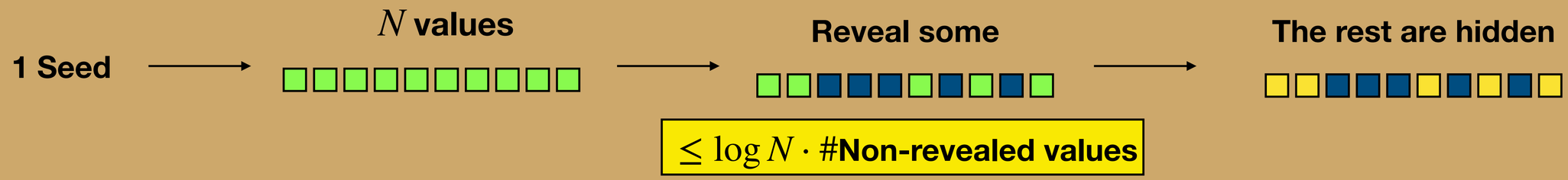
The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



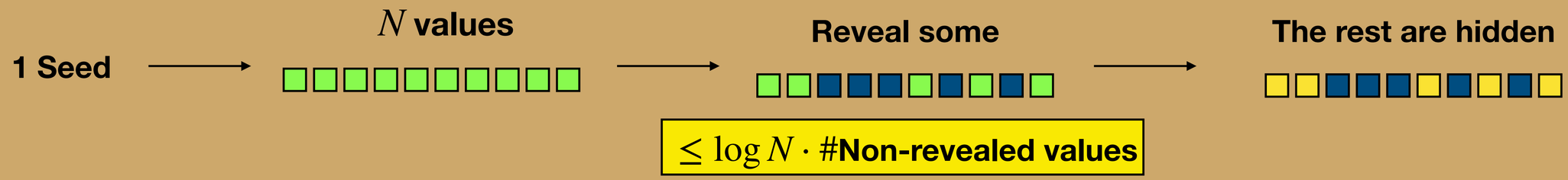
The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



The *Compact* Boosting Transform

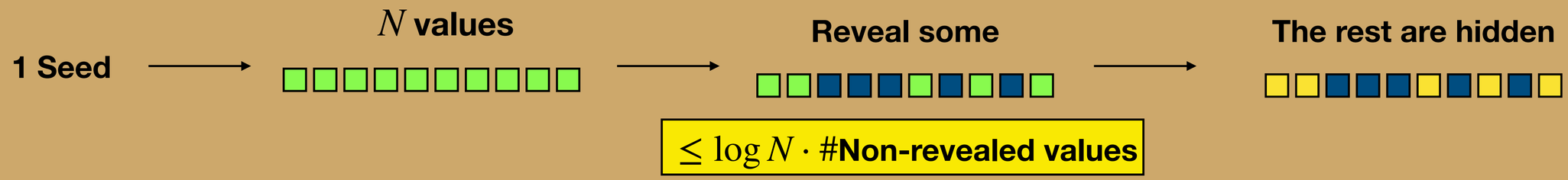
- **Puncturable Pseudorandom Function (PPRF) [SW14]**



- **Randomness Homomorphic Commitment**

The *Compact* Boosting Transform

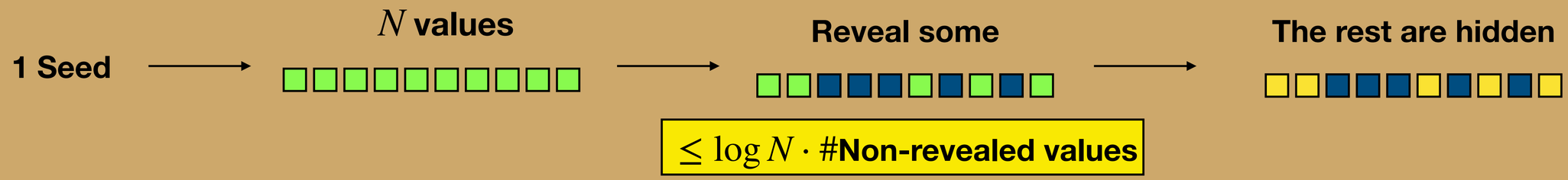
- **Puncturable Pseudorandom Function (PPRF) [SW14]**



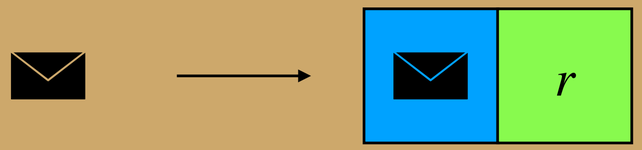
- **Randomness Homomorphic Commitment**

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**

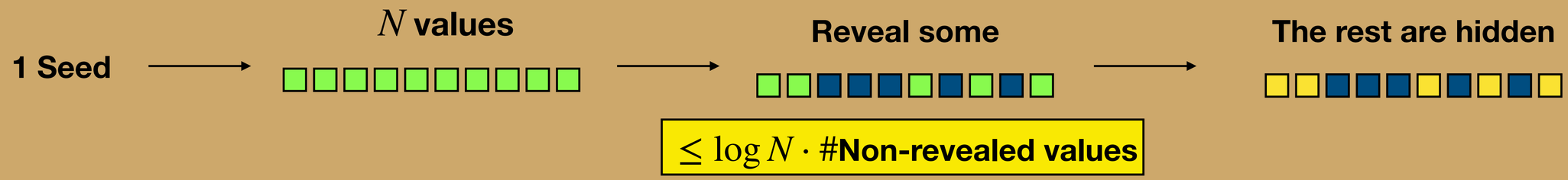


- **Randomness Homomorphic Commitment**

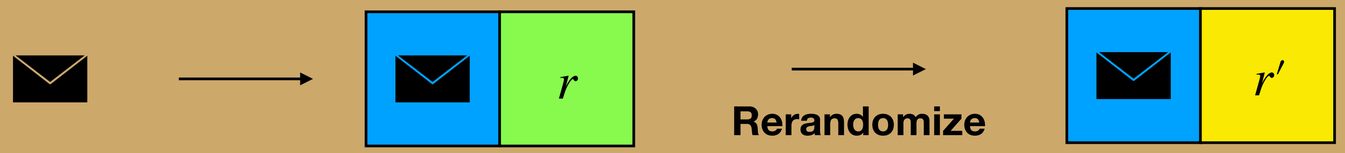


The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**

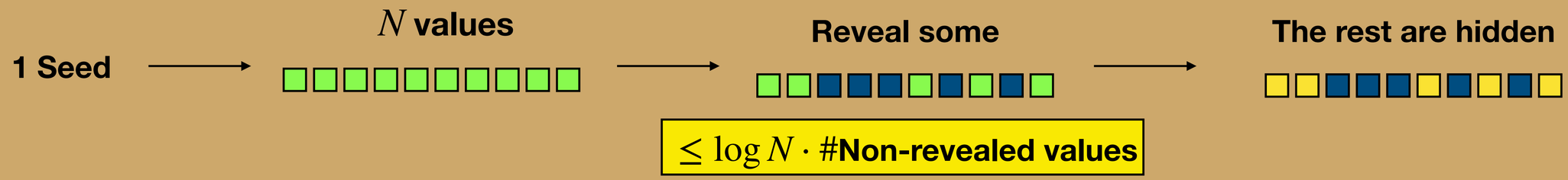


- **Randomness Homomorphic Commitment**

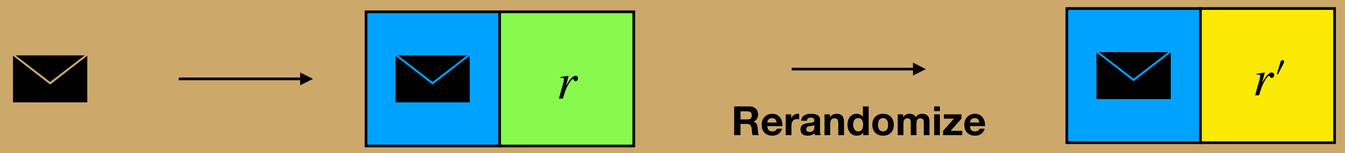


The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



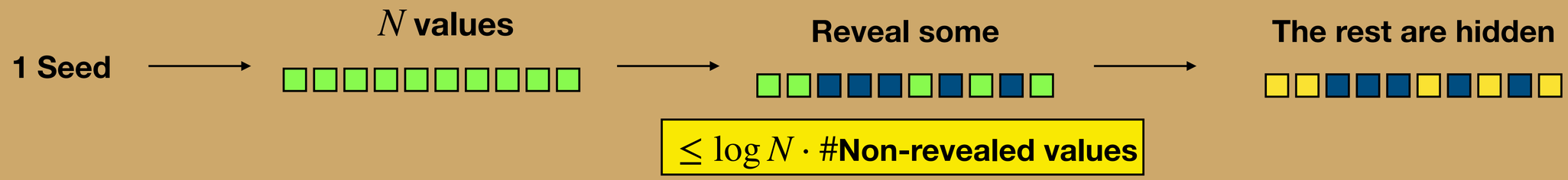
- **Randomness Homomorphic Commitment**



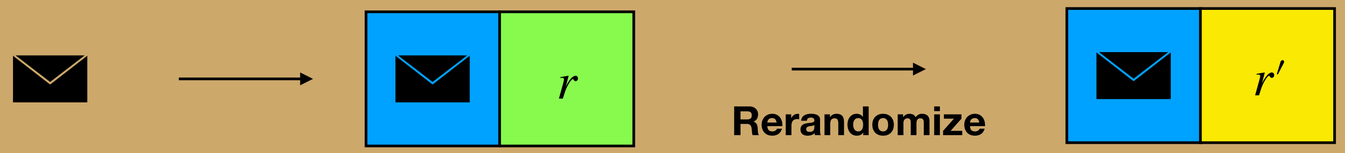
- **Applying to Cut-and-Choose Transform**

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



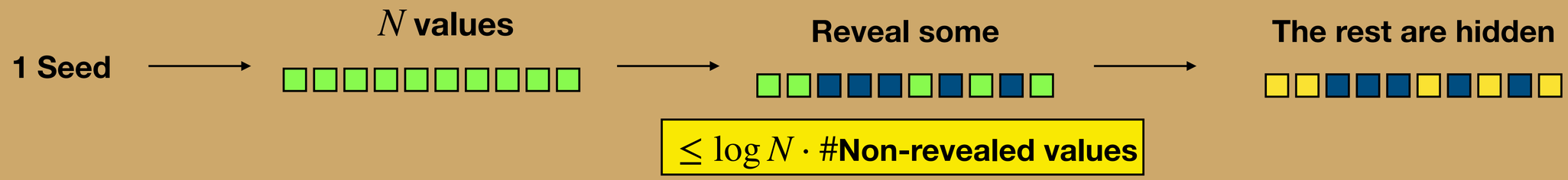
- **Randomness Homomorphic Commitment**



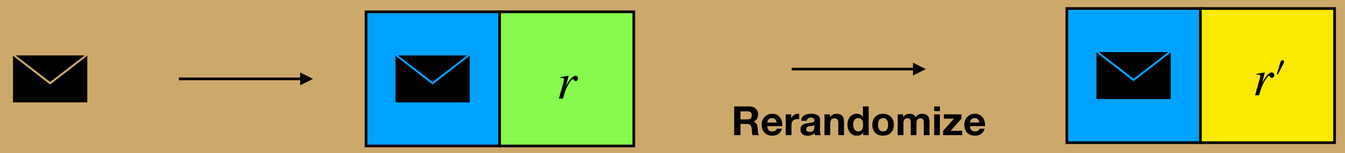
- **Applying to Cut-and-Choose Transform**

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



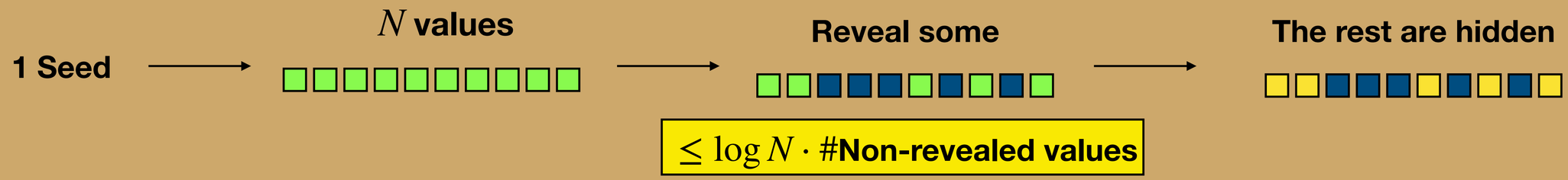
- **Randomness Homomorphic Commitment**



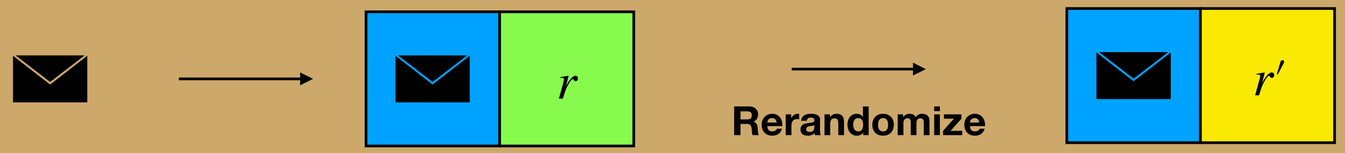
- **Applying to Cut-and-Choose Transform**

The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



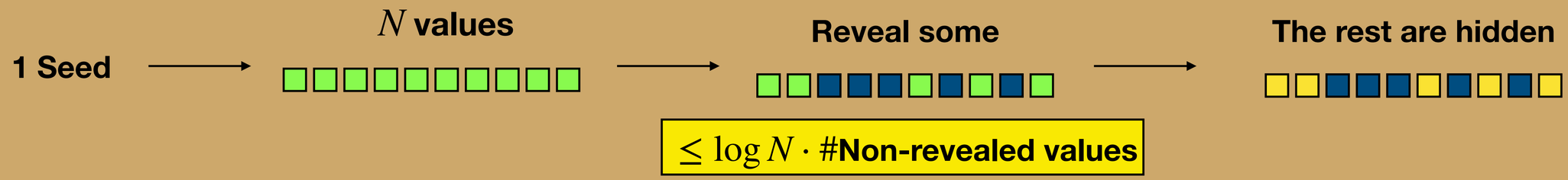
- **Randomness Homomorphic Commitment**



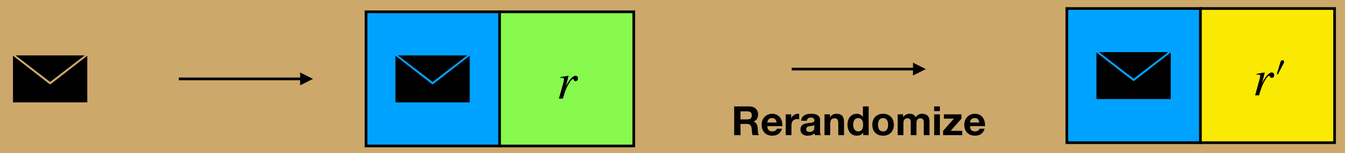
- **Applying to Cut-and-Choose Transform**

The *Compact* Boosting Transform

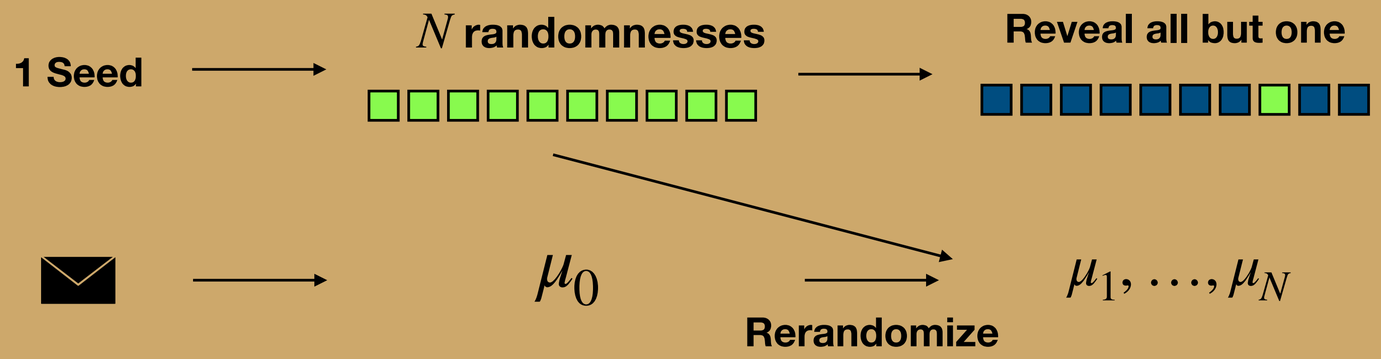
- **Puncturable Pseudorandom Function (PPRF) [SW14]**



- **Randomness Homomorphic Commitment**

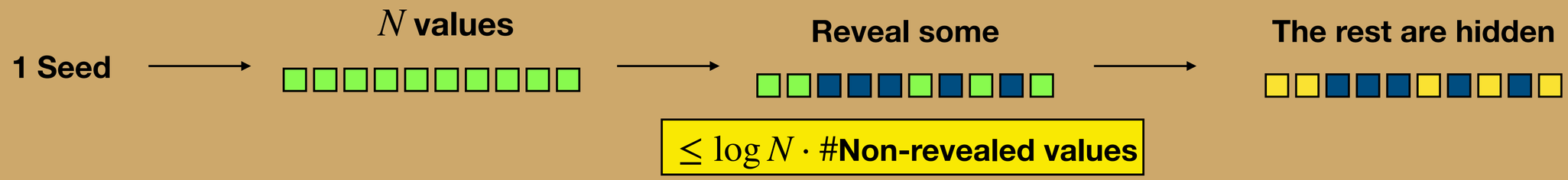


- **Applying to Cut-and-Choose Transform**

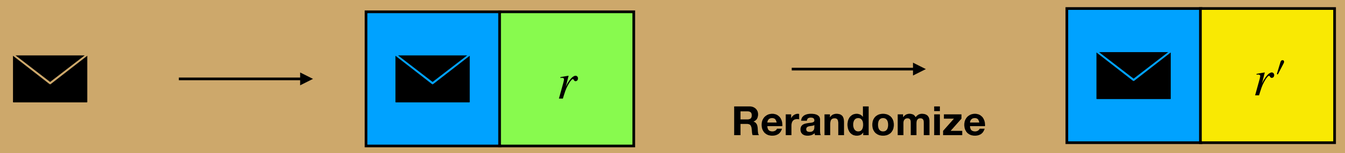


The *Compact* Boosting Transform

- **Puncturable Pseudorandom Function (PPRF) [SW14]**



- **Randomness Homomorphic Commitment**



- **Applying to Cut-and-Choose Transform**