

Efficient Round Optimal Blind Signatures

Sanjam Garg

IBM T.J. Watson

Divya Gupta


UCLA

Complexity Leveraging

- Highly **theoretical** tool
- Used to obtain **feasibility** results
- Gives **inefficient** constructions



Main Question



Is there a way to use
complexity leveraging
to get **efficient**
constructions?

Our Application: Blind Signatures

Round Optimal Blind Signatures obtained
using Complexity Leveraging
[Garg-Rao-Sahai-Shröder-Unruh-2011]

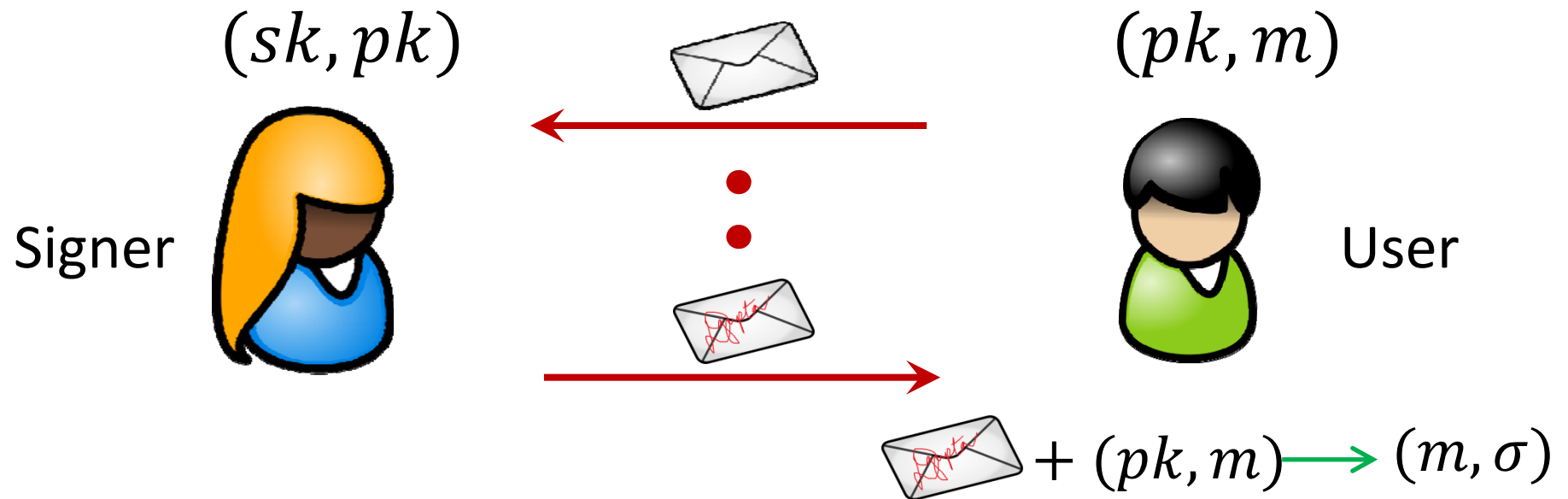


Efficient?

Talk Outline

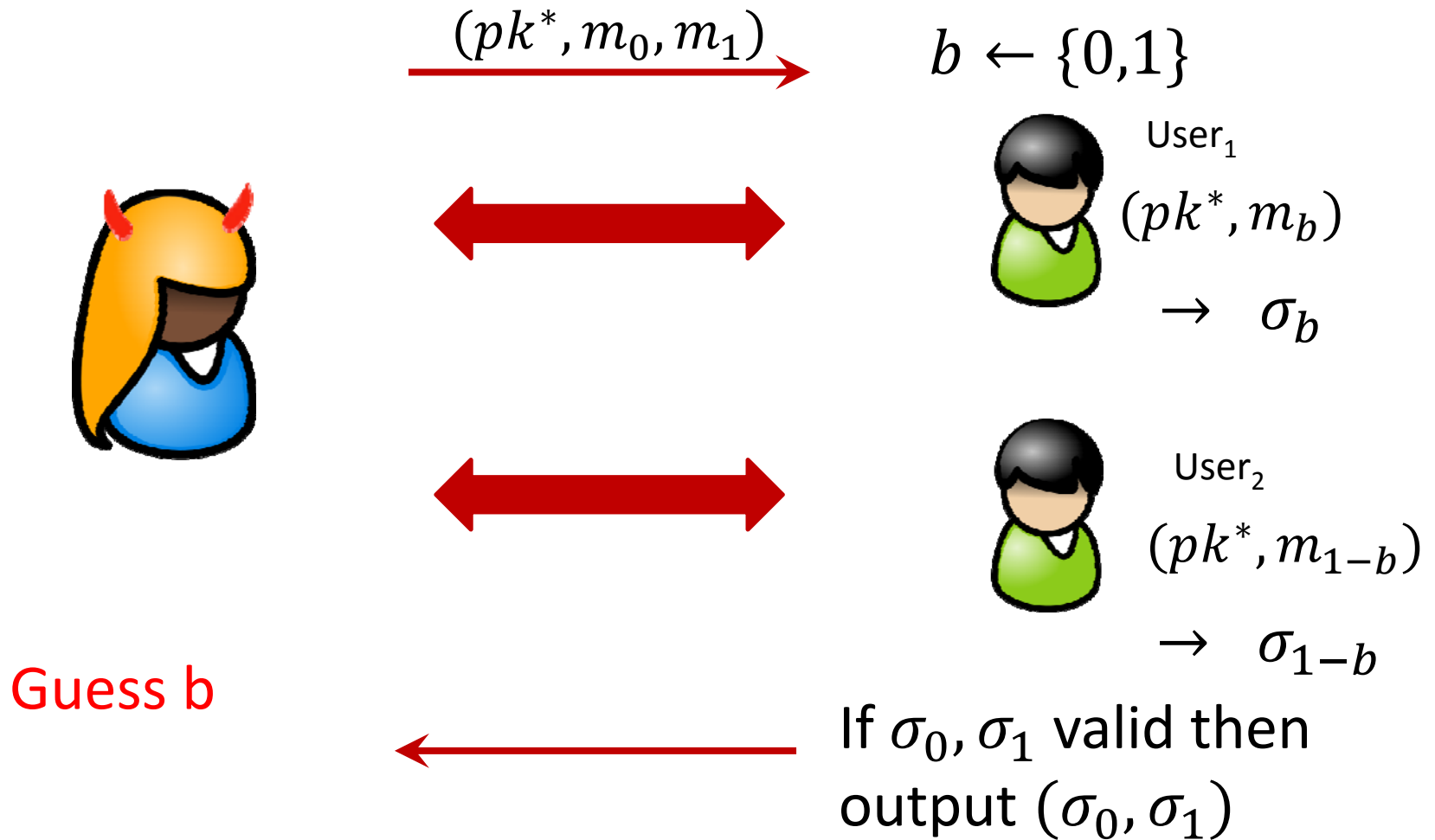
- Define Blind Signatures and their Security Properties
- Previous Work
- Our Result
- Our Construction
 - Construction in CRS model
 - How to remove the CRS

Blind Signatures (Chaum82)



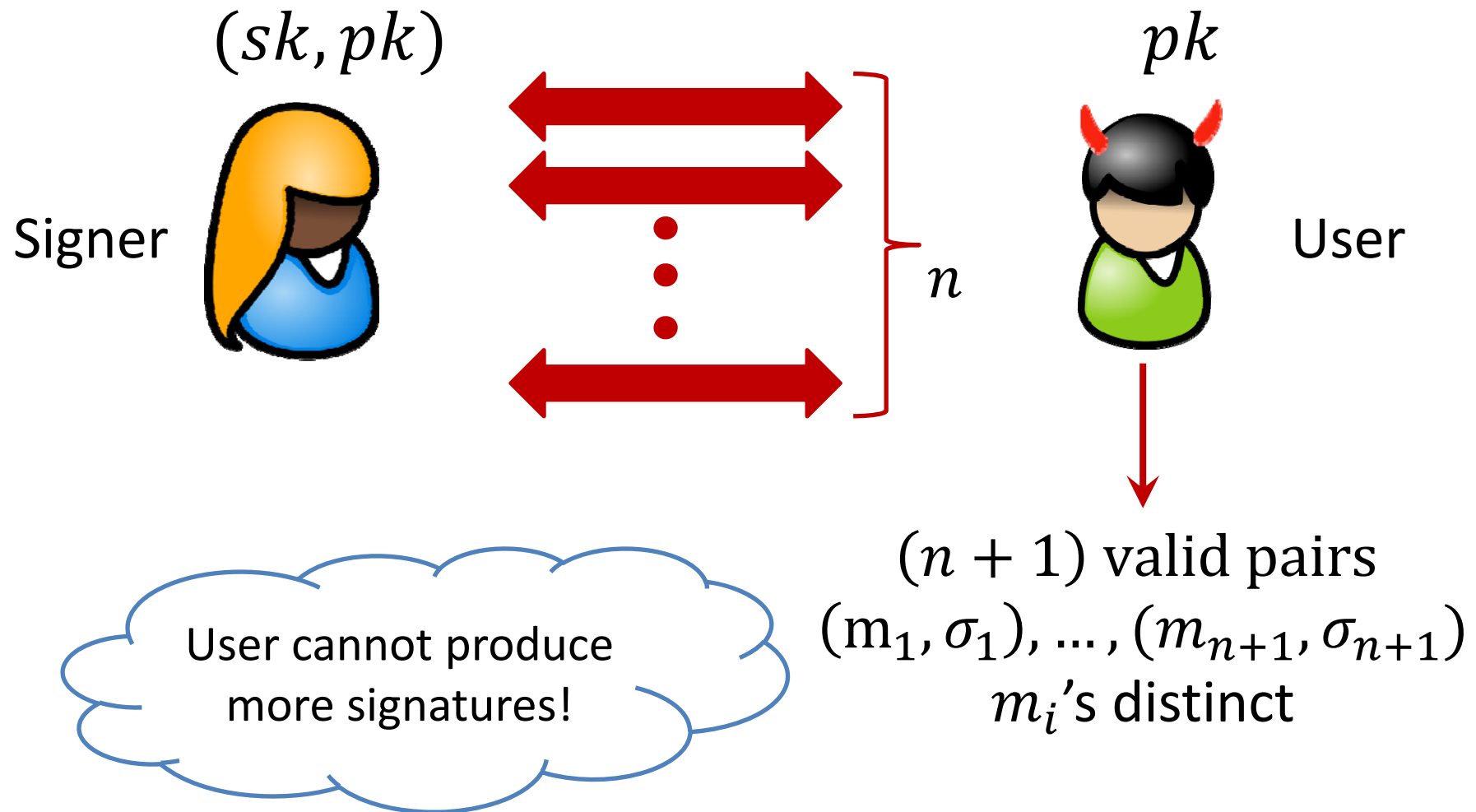
Should satisfy **Blindness** and **Unforgeability**
Round Optimal: 2 Rounds

Blindness Property



Signer is oblivious of the message being signed.

Unforgeability Property



Talk Outline

- Define Blind Signatures and its Security Properties
- **Previous Work**
- Our Result
- Our Construction
 - Construction in CRS model
 - How to remove the CRS

Previous Results

Large amount of work on Blind Signatures.

CRS or Random Oracle or Interactive Assumptions
(Fischlin06, AHO10, Chaum83, Boldyreva03.....)

- Round Optimal and Efficient

Standard Model without complexity leveraging
(JLO97, CKW04, Okamoto06, HKKL07.....)

- Not Round Optimal; Best known 4 rounds (Okamoto06)

Standard Model using Complexity Leveraging
(GRSUU11)

- Round Optimal but highly inefficient

Talk Outline

- Define Blind Signatures and its Security Properties
- Previous Work
- **Our Result**
- Our Construction
 - Construction in CRS model
 - How to remove the CRS

Our Result

2-Round, Efficient Blind Signature scheme in the **standard model** (without CRS or Random Oracle)

Assumptions: Sub-exponentially Hard DLIN and a variant of DLog

Concrete Efficiency

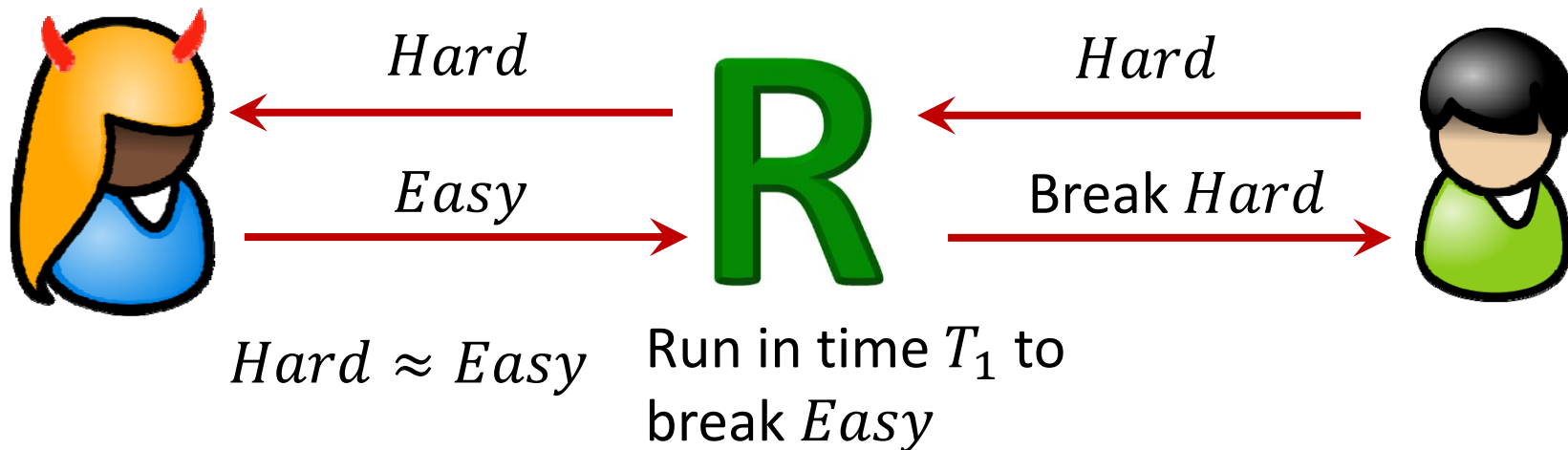
2-Round, Efficient Blind Signature scheme in the **standard model** (without CRS or Random Oracle)

Scheme	Communication Complexity	Signature Size
GRSUU11	> 1GB	small
This Work	100.6KB	6.5KB

Setting of 80 bits of security

Complexity Leveraging

- Consider $T_1 \gg T_2$
- Primitive *Hard* secure against T_1 -adversaries
- Primitive *Easy* secure against T_2 -adversaries such that it can be broken by a T_1 -adversary



Talk Outline

- Define Blind Signatures and its Security Properties
- Previous Work
- Our Result
- **Our Construction**
 - Construction in CRS model
 - How to remove the CRS

Starting Point

(Efficient Scheme in CRS Model)

Common Reference String crs

(sk, pk)



msg_1



msg_2



(pk, m)



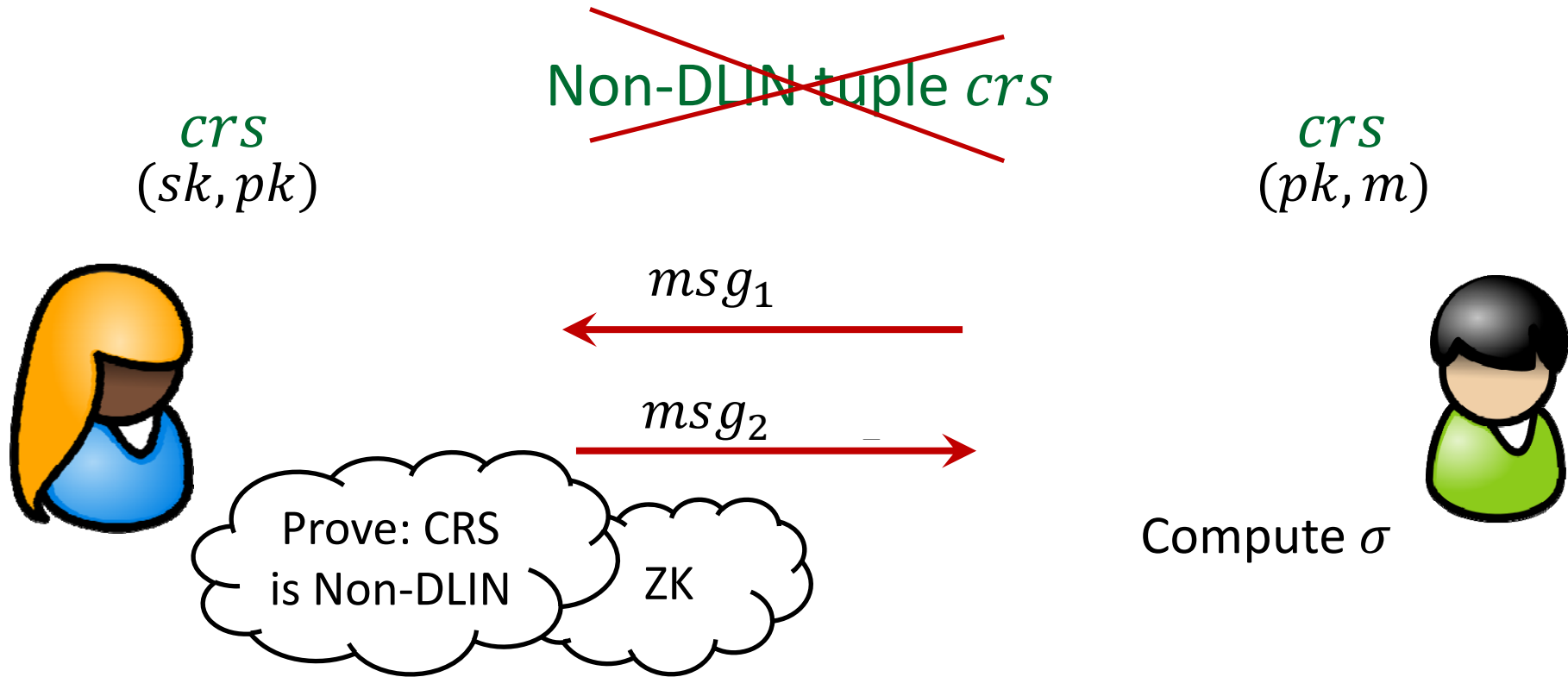
Compute σ

Blindness: crs is non-DLIN tuple

Unforgeability: Under DLIN assumption

Starting Point

(Efficient Scheme in CRS Model)



Blindness: crs is non-DLIN tuple

Unforgeability: Under DLIN assumption

2-Round ZK Argument (Pass 03)

(sk, pk, crs)

(pk, m, crs)



msg_1, ZK_1

msg_2, ZK_2



Reasons for Inefficiency

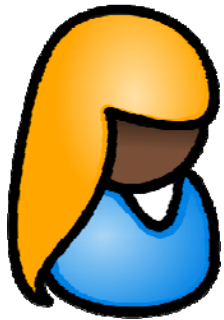
- Soundness: Used Complexity Leveraging → Larger parameters needed!
- Simulation: Used Complexity Leveraging → Public key grows further!

Need 3 levels of security parameters!

Soundness Case: Issue

- Soundness: Used Complexity Leveraging → Larger parameters needed!

(sk, pk, crs)



$Com(B)$
 ZK_2 for either
 crs is non-DLIN
or $A = B$

$Com(A), ZK_1$



(pk, m, crs)

$Com(A)$



$Com(B), ZK_2$



$Com(B)$ is weaker than $Com(A)$

Our Solution

- Soundness: ~~Used Complexity Leveraging~~ → Larger parameters needed!

(sk, pk, crs)

(pk, m, crs)



$Com(B)$
NIZK π under crs :
Either crs is
non-DLIN or
 $A = B$

$Com(A)$

$Com(A)$



$Com(B), \pi$

$Com(B)$ is as hard as $Com(A)$

Use special NIZKs which give
perfect witness extraction under **DLIN crs** .

Soundness Reduction

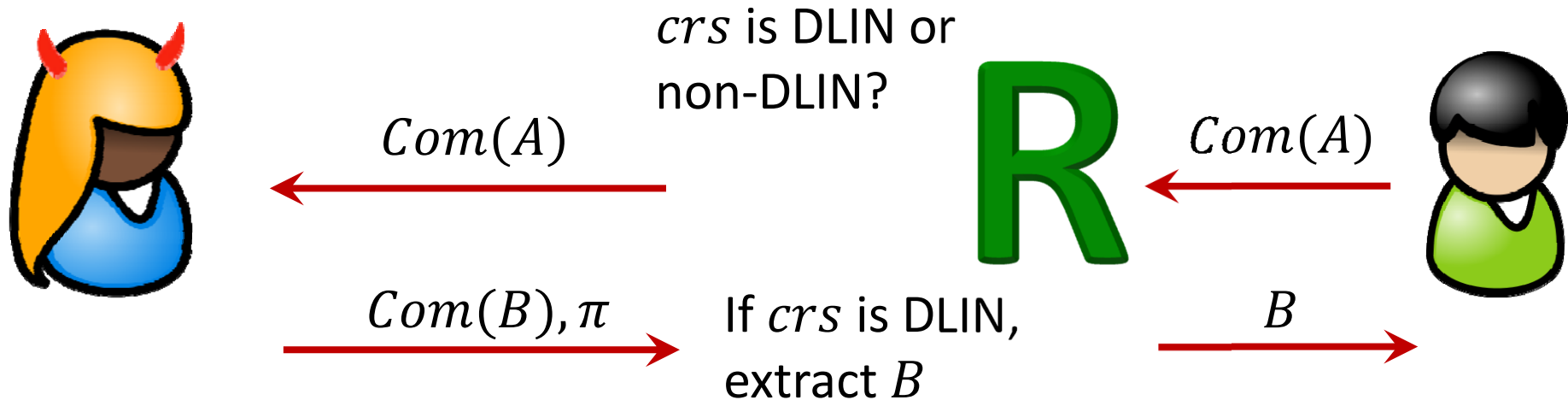
Cheating
Signer

(sk, pk, crs)

Adv for
 Com

(pk, m, crs)

Challenger
for Com



- Used **perfect extraction of π** under **DLIN crs** .
- Need **non-uniform** hiding property of $Com(\cdot)$.
- **Removed** one use of complexity leveraging.

Second Reason for Inefficiency

- Simulation for zero-knowledge uses complexity leveraging
- Cannot get rid of this; Make this more efficient

Second Reason for Inefficiency

(sk, pk, crs)

(pk, m, crs)



$Com(B)$
NIZK π
under crs :
Either crs is
non-DLIN or
 $A = B$

Very inefficient due to
NP reductions for
non-algebraic
statements

$Com(A)$

$Com(A)$

$Com(B), \pi$



Find Com
with nice
properties!

Use efficient
NIZK for
algebraic
statements!

What do we know?

Groth-Sahai NIZK

- A **highly efficient** proof system for **certain** kinds of **algebraic** equations involving elements from **bilinear groups**
- We will try to use these!

Our Solution

$(sk, pk, crs, q \ll 2^k)$

(pk, m, crs, q)



Pick $d < q$
 $D = g^d$

NIZK π
under crs :
Either crs is
non-DLIN or
 $c = d$

C, π'

D, π

Pick $c < q$
 $C = g^c$



Prove:
 $c < q$
Under crs'

Fits GS framework

→ Efficient proof
What if \mathcal{U} picks $c > q$?

If crs is DLIN
then crs' is
non-DLIN

NIZK has **perfect ZK** under **non-DLIN crs** .

Conclusion

1. Complexity leveraging technique is **NOT** a bottleneck in constructing efficient protocols.
2. We obtain **efficient round optimal blind signatures** in the standard model using efficient use of complexity leveraging.