TECHNISCHE UNIVERSITÄT DARMSTADT

Do You Need a Receipt? Anonymous Credential Revocation at Continental Scale via Private Record Certification

Kasra EdalatNejad, Sebastian Faust, **Jonas Hofmann**,
Philipp-Florens Lehwalder, Thomas Schneider

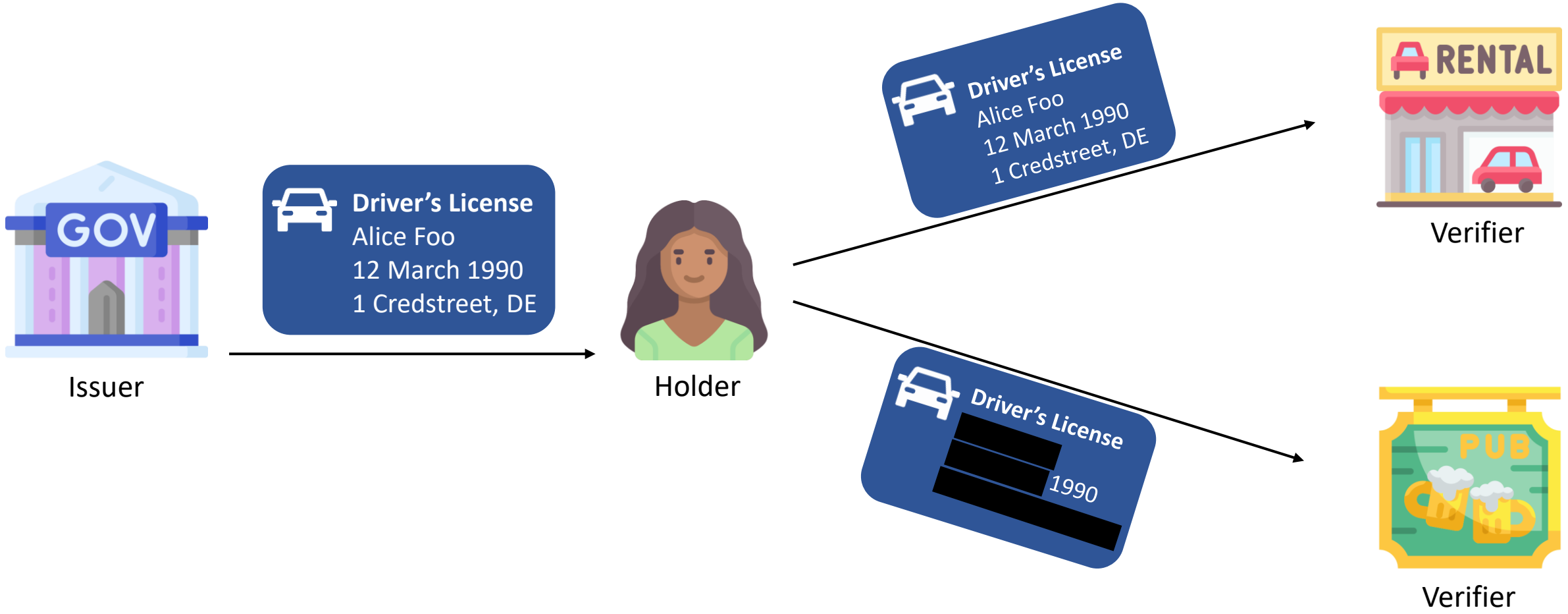
CROSSING

Funded by
DFG Deutsche Forschungsgemeinschaft
German Research Foundation

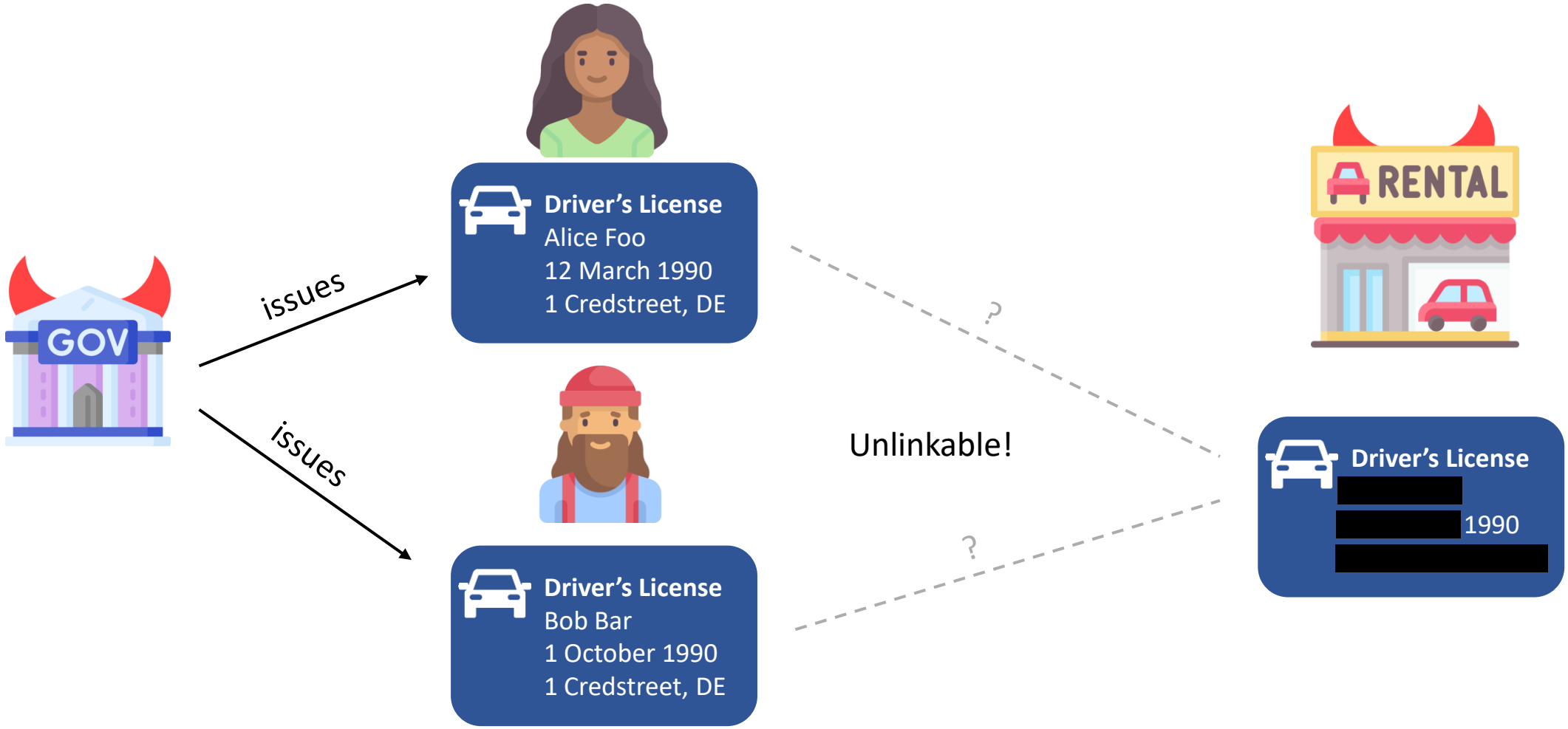
Funded by the European Union

erc
European Research Council
Established by the European Commission

Anonymous Credentials

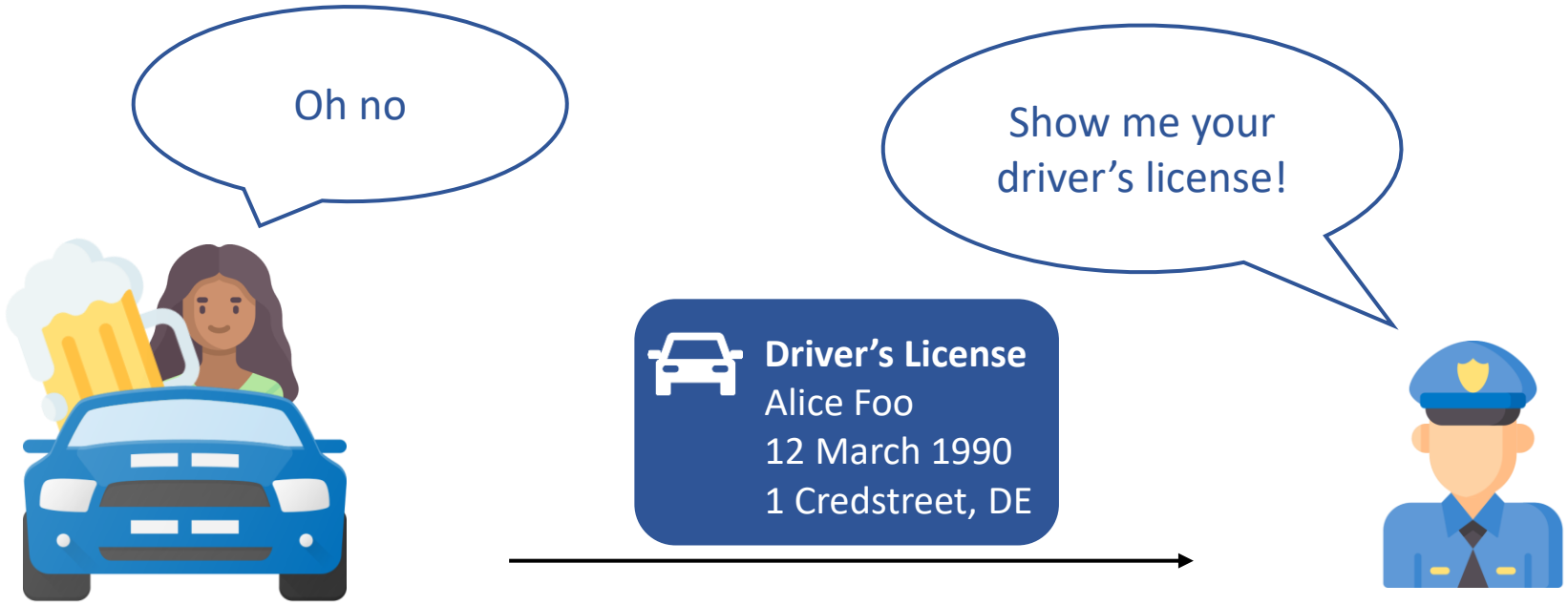


Anonymous Credentials - Unlinkability



How to invalidate a Credential?

How to invalidate a Credential?



Anonymous Credential Revocation



Revocation Authority







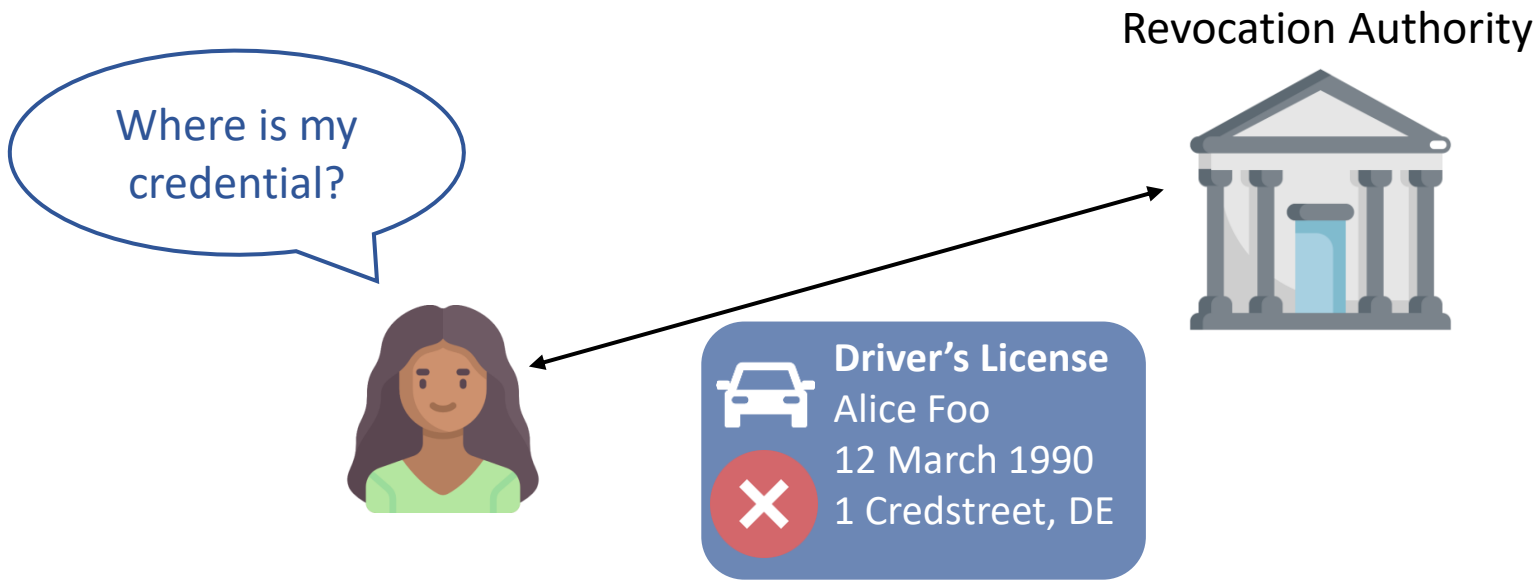
Anonymous Credential Revocation



Anonymous Credential Revocation



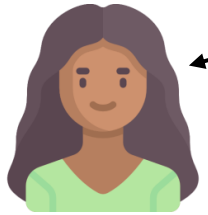
Anonymous Credential Revocation



Anonymous Credential Revocation

Revocation is time-critical!

Revocation Authority







Driver's License
Alice Foo
12 March 1990
1 Credstreet, DE

Driver's License
Alice Foo
12 March 1990
1 Credstreet, DE

Revocation Scheme Wishlist



Unlinkability



Instant Revocation



Scalability



Revocation Privacy

Ideal Revocation Scheme

Property	Unlinkability	Scalability	Instant Revocation	Revocation Privacy
Status List	✗	–	–	✗
Token-Based	–	–	✗	✗
Accumulator	✓	✗	–	✗
Ours	✓	✓	✓	✓

Naïve Approach



Revocation Authority

(sk, pk)

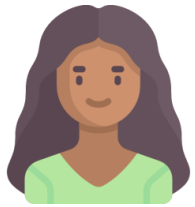


$=$

0
1
1
0
1

idx = 3

$\text{Sign}(sk, (3, \text{time}))$





Driver's License
idx = 3

Naïve Approach



Revocation Authority
(sk, pk)

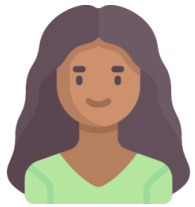


$=$

0
1
1
0
1

idx = 3

$\text{Sign}(sk, (3, \text{time}))$





Driver's License
idx = 3

No privacy!

Naïve Approach



Revocation Authority
(sk, pk)

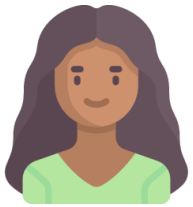


$=$

$\text{Sign}(sk, (1, \text{time}))$
$\perp$
$\text{Sign}(sk, (3, \text{time}))$
$\perp$
$\text{Sign}(sk, (5, \text{time}))$

idx = 3


[3]





Driver's License
idx = 3

Naïve Approach



Revocation Authority
(sk, pk)

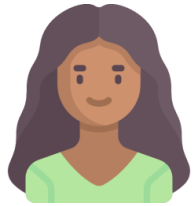
$=$

$\text{Sign}(sk, (1, \text{time}))$
$\perp$
$\text{Sign}(sk, (3, \text{time}))$
$\perp$
$\text{Sign}(sk, (5, \text{time}))$

Private Information Retrieval (PIR)

idx = 3

$[3]$



Driver's License
idx = 3

Naïve Approach

Property	Unlinkability	Scalability	Instant Revocation	Revocation Privacy
Naïve Approach V1	–	✗	–	✗



Revocation Authority
(sk, pk)

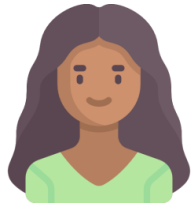
$=$

$\text{Sign}(sk, (1, \text{time}))$
$\perp$
$\text{Sign}(sk, (3, \text{time}))$
$\perp$
$\text{Sign}(sk, (5, \text{time}))$

Private Information Retrieval (PIR)

idx = 3

$[3]$



Driver's License
idx = 3

Naïve Approach



Revocation Authority
(sk, pk)



$=$

$\mathrm{Sign}(sk, co_1), co_1$
$\mathrm{Sign}(sk, co_2), co_2$
$\mathrm{Sign}(sk, co_3), co_3$
$\mathrm{Sign}(sk, co_4), co_4$
$\mathrm{Sign}(sk, co_5), co_5$

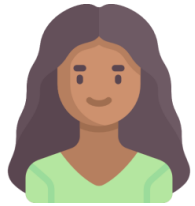


Private Information Retrieval (PIR)

idx = 3



$[3]$





Driver's License
idx = 3

r_i

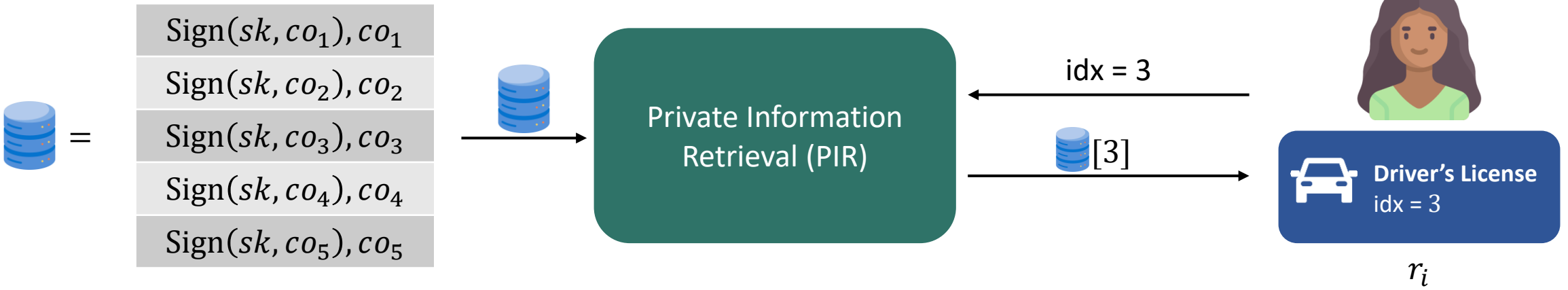
if i is revoked: $\mathrm{co_i} \leftarrow \mathrm{Commit}(\perp; r_i)$
valid: $\mathrm{co_i} \leftarrow \mathrm{Commit}(i, \mathrm{time}; r_i)$

Naïve Approach

Property	Unlinkability	Scalability	Instant Revocation	Revocation Privacy
Naïve Approach V2	✓	✗	–	✓



Revocation Authority
(sk, pk)

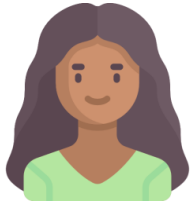


r_i

if i is revoked: $\mathrm{co_i} \leftarrow \mathrm{Commit}(\perp; r_i)$
valid: $\mathrm{co_i} \leftarrow \mathrm{Commit}(i, \mathrm{time}; r_i)$

Naïvely revoking Credentials

Driver's License
Alice Foo
12 March 1990
idx = 3



Holder



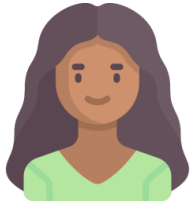
Revocation Authority



Verifier

Naïvely revoking Credentials

Driver's License
Alice Foo
12 March 1990
idx = 3



Holder



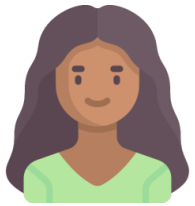
Revocation Authorities



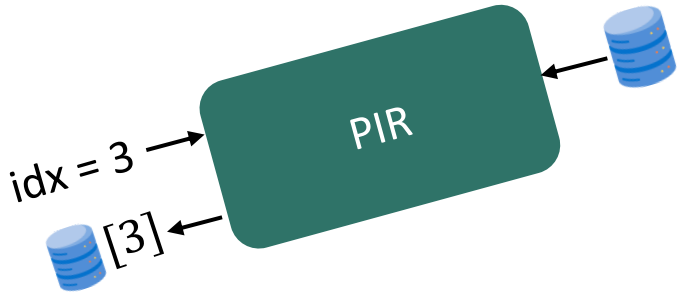
Verifier

Naïvely revoking Credentials





Holder



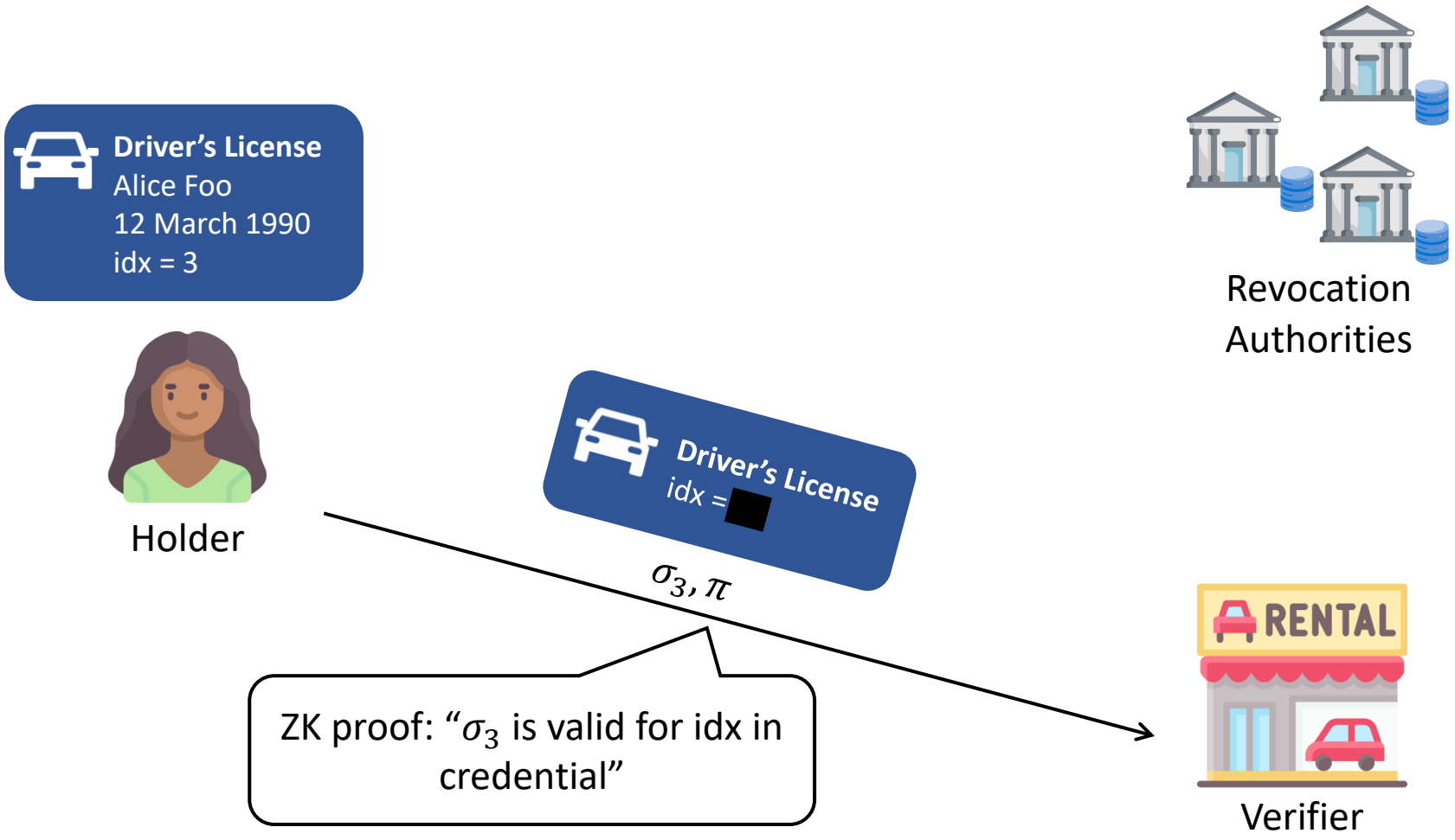


Revocation Authorities



Verifier

Naïvely revoking Credentials

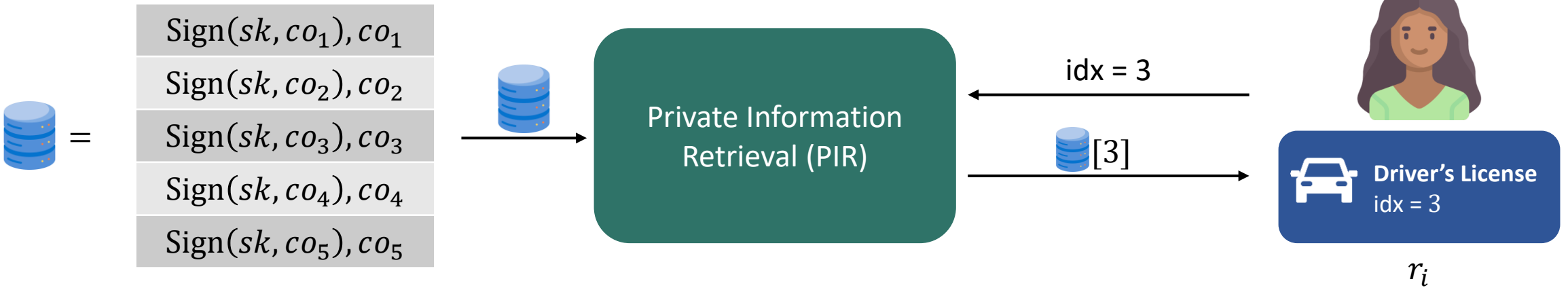


Naïve Approach

Property	Unlinkability	Scalability	Instant Revocation	Revocation Privacy
Naïve Approach V2	✓	✗	–	✓



Revocation Authorities



if i is revoked: $\text{co}_\text{i} \leftarrow \text{Commit}(\perp; r_i)$

valid: $\text{co}_\text{i} \leftarrow \text{Commit}(i, \text{time}; r_i)$

Naïve Approach



Revocation Authorities

Property	Unlinkability	Scalability	Instant Revocation	Revocation Privacy
Naïve Approach V2	✓	✗	–	✓

size: $96B \cdot 1$ billion $= 96\ GB$!

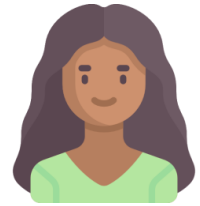
$=$

$\mathrm{Sign}(sk, co_1), co_1$
$\mathrm{Sign}(sk, co_2), co_2$
$\mathrm{Sign}(sk, co_3), co_3$
$\mathrm{Sign}(sk, co_4), co_4$
$\mathrm{Sign}(sk, co_5), co_5$

Private Information Retrieval (PIR)

idx = 3

[3]



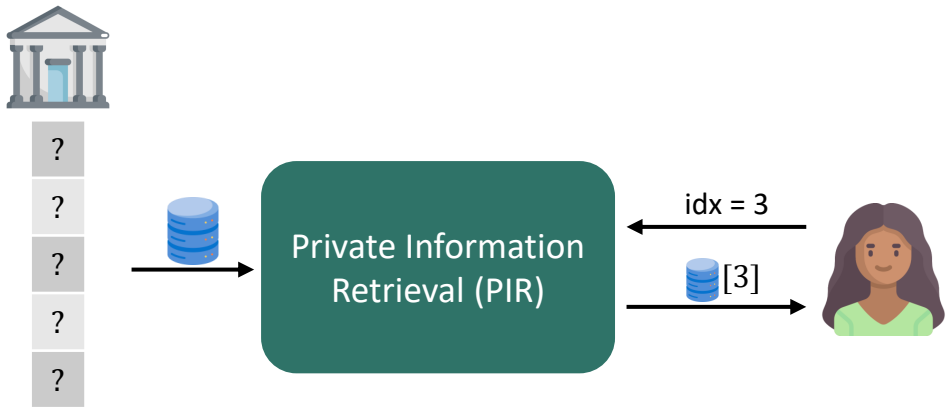
Driver's License
idx = 3

r_i

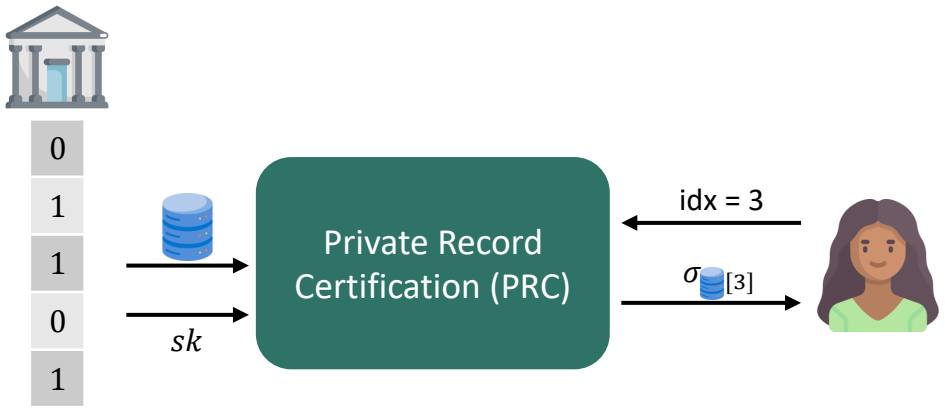
if i is revoked: $\mathrm{co_i} \leftarrow \mathrm{Commit}(\perp; r_i)$
valid: $\mathrm{co_i} \leftarrow \mathrm{Commit}(i, \mathrm{time}; r_i)$

Private Record Certification (PRC)

PIR



PRC



Naïve Approach



Revocation Authority
(sk, pk)

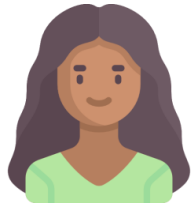
$=$

$\mathrm{Sign}(sk, co_1), co_1$
$\mathrm{Sign}(sk, co_2), co_2$
$\mathrm{Sign}(sk, co_3), co_3$
$\mathrm{Sign}(sk, co_4), co_4$
$\mathrm{Sign}(sk, co_5), co_5$

Private Information Retrieval (PIR)

idx = 3

$[3]$



Driver's License
idx = 3

r_i

PRC for Revocation



Revocation Authority

(sk, pk)

size: $1b \cdot 1$ billion $= 125\ MB$!

$=$

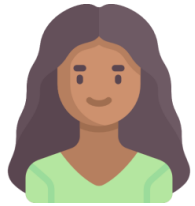
0
1
1
0
1

sk

Private Record Certification (PRC)

idx = 3

$\sigma_{[3]}$



Driver's License
idx = 3

PRC for Revocation



Revocation Authority

(sk, pk)



$=$

0
1
1
0
1

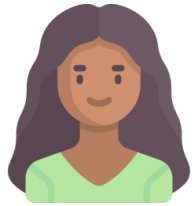


sk

Private Record Certification (PRC)

idx = 3

$\sigma_{[3]}$



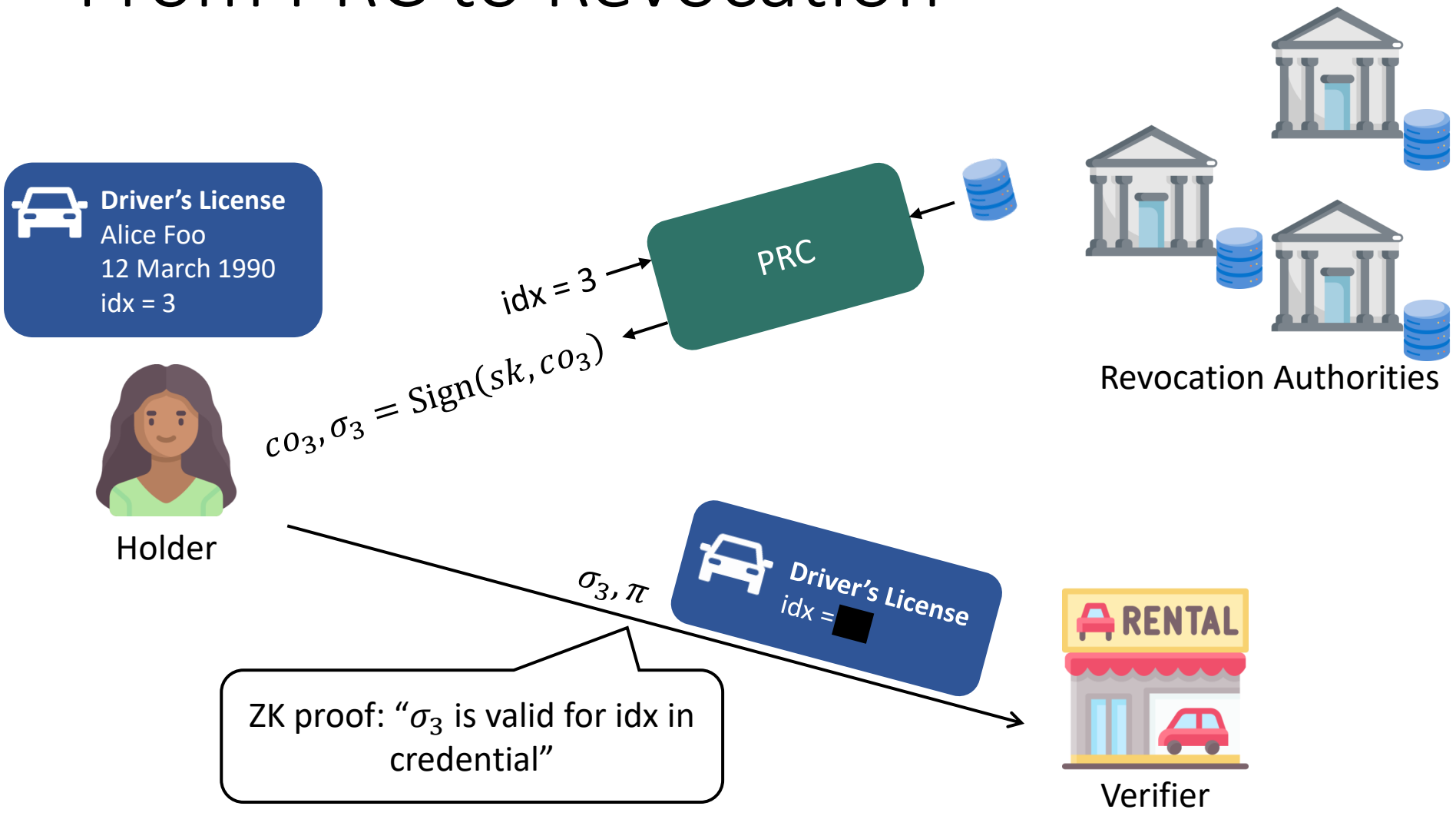


Driver's License
idx = 3

r_i

Design this to be $(\text{Sign}(sk, co_3), co_3)$

From PRC to Revocation



Ingredients 



Secure MPC





Secret Sharing

here: GMW



Commitment Scheme

here: Pedersen

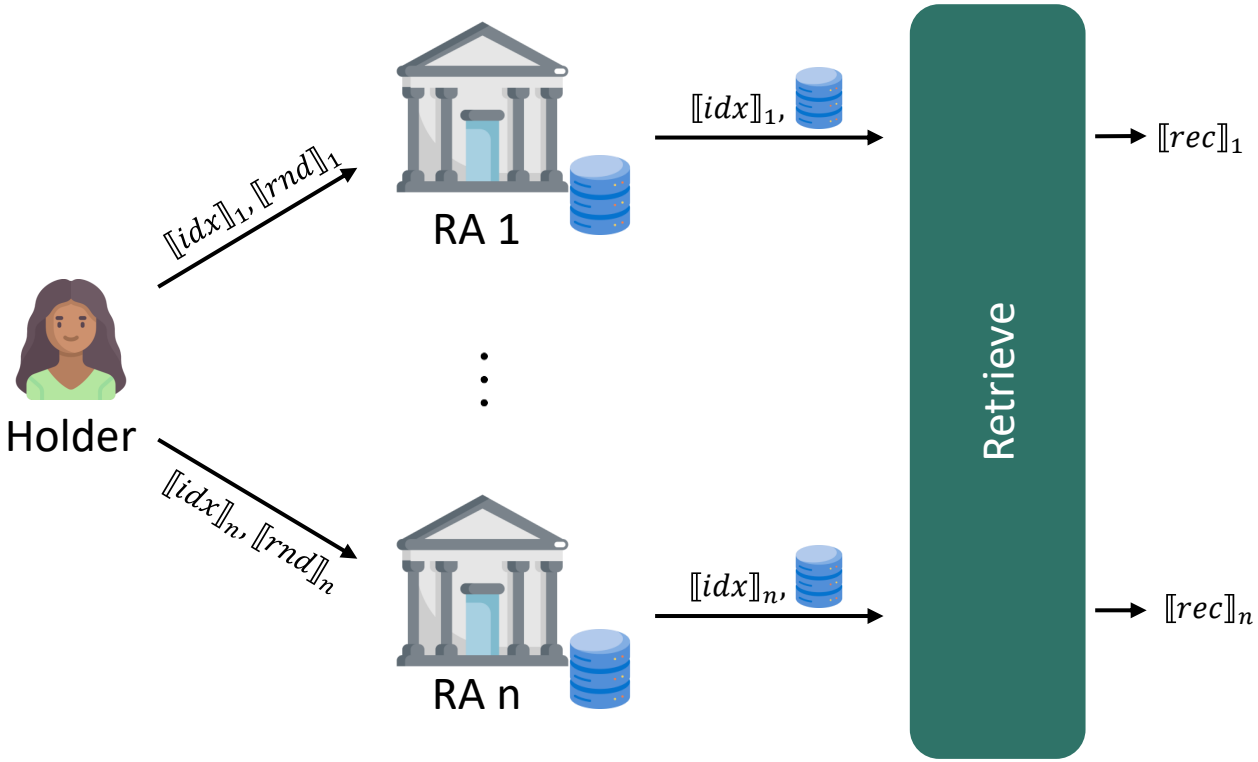


Threshold Signature

here: Threshold EdDSA

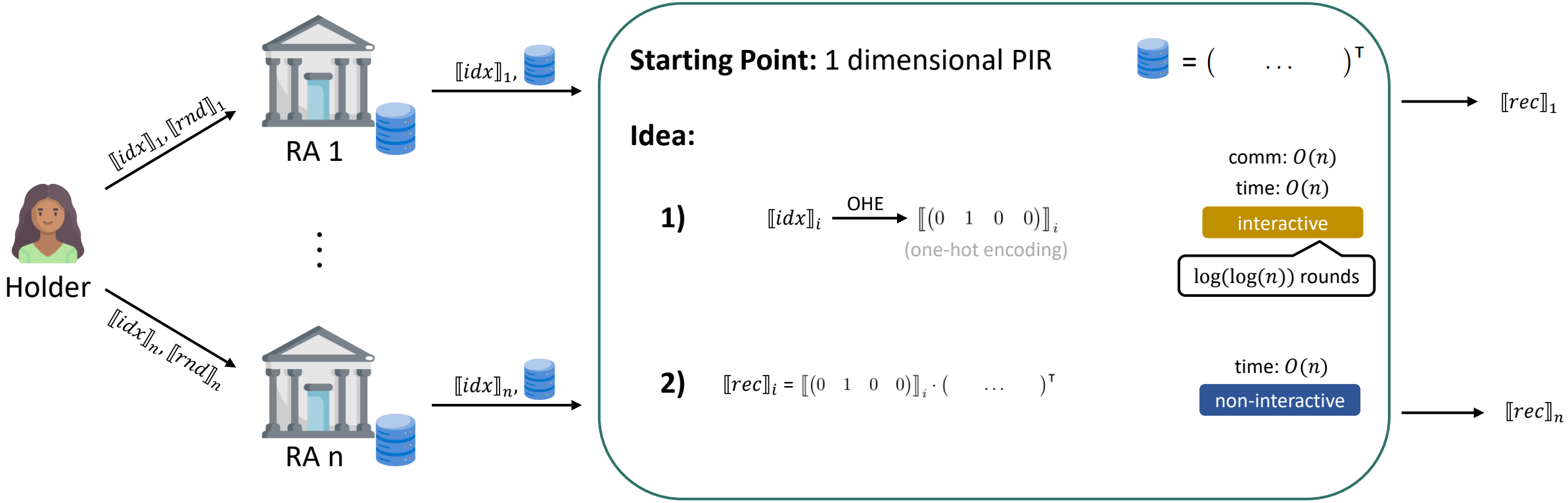
Constructing PRC

$[\![\cdot]\!]$	secret share
idx	index
rnd	randomness
rec	record value



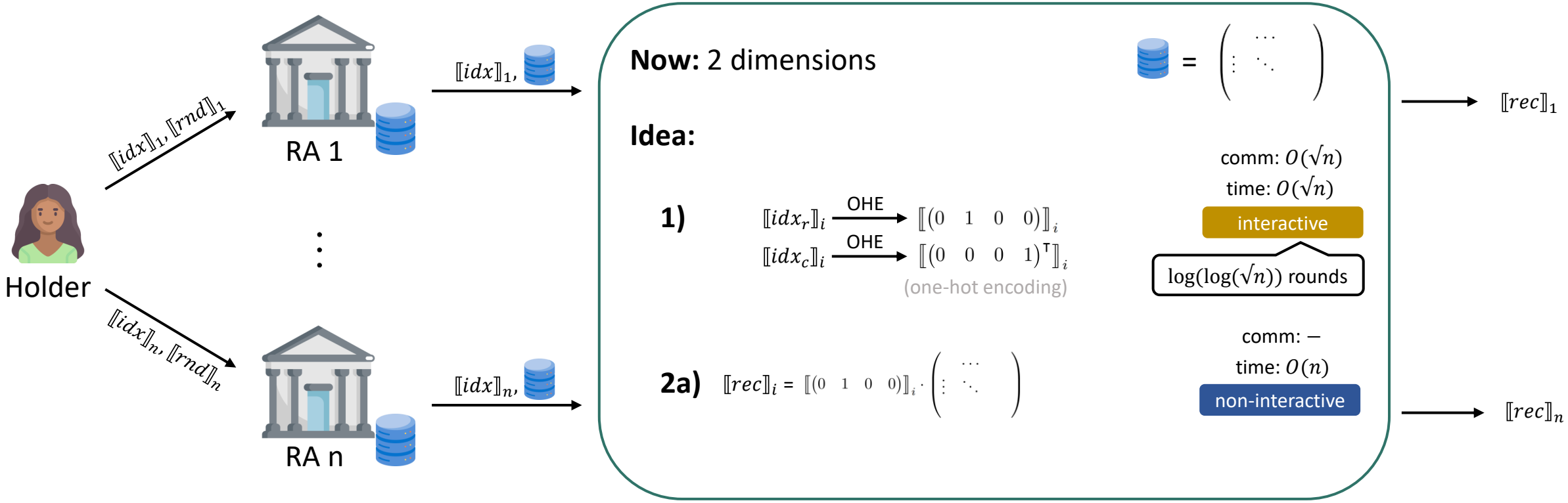
Constructing PRC

$[\![\cdot]\!]$	secret share
idx	index
rnd	randomness
rec	record value



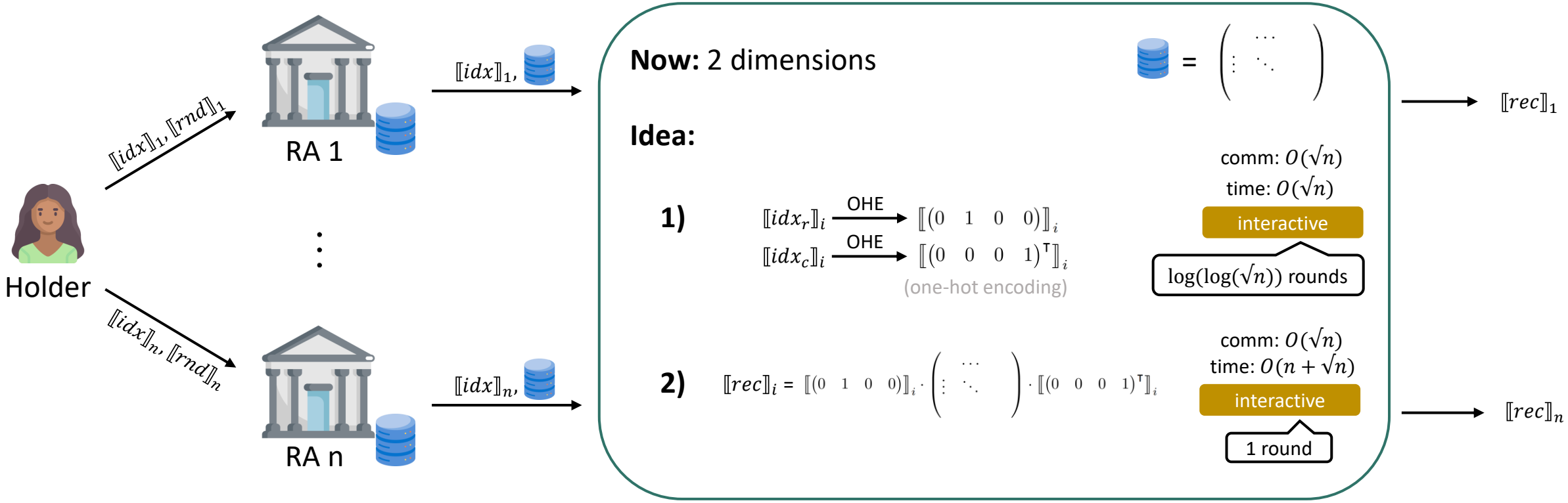
Constructing PRC

$[\![\cdot]\!]$	secret share
idx	index
rnd	randomness
rec	record value



Constructing PRC

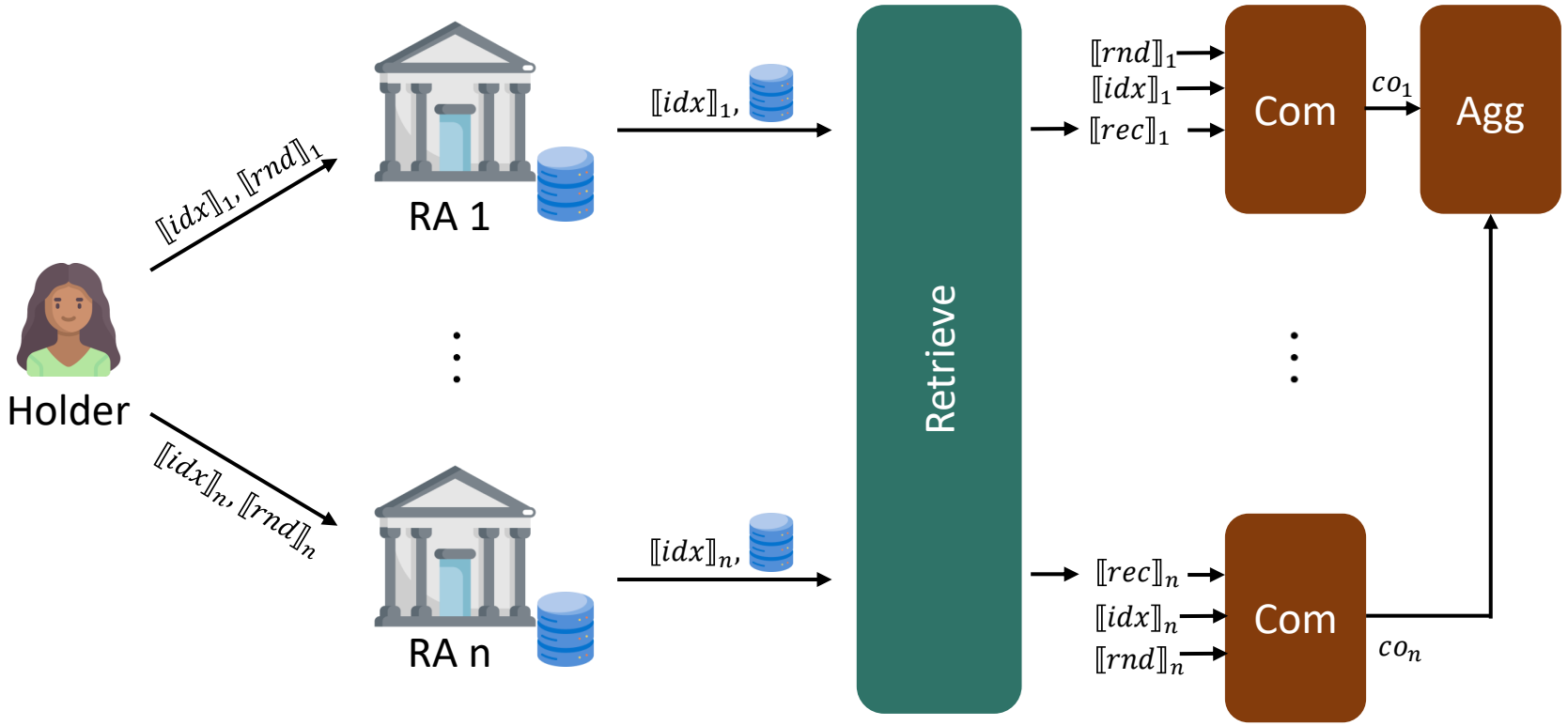
$[\![\cdot]\!]$	secret share
idx	index
rnd	randomness
rec	record value



Constructing PRC

$[\![\cdot]\!]$	secret share
idx	index
rnd	randomness
rec	record value

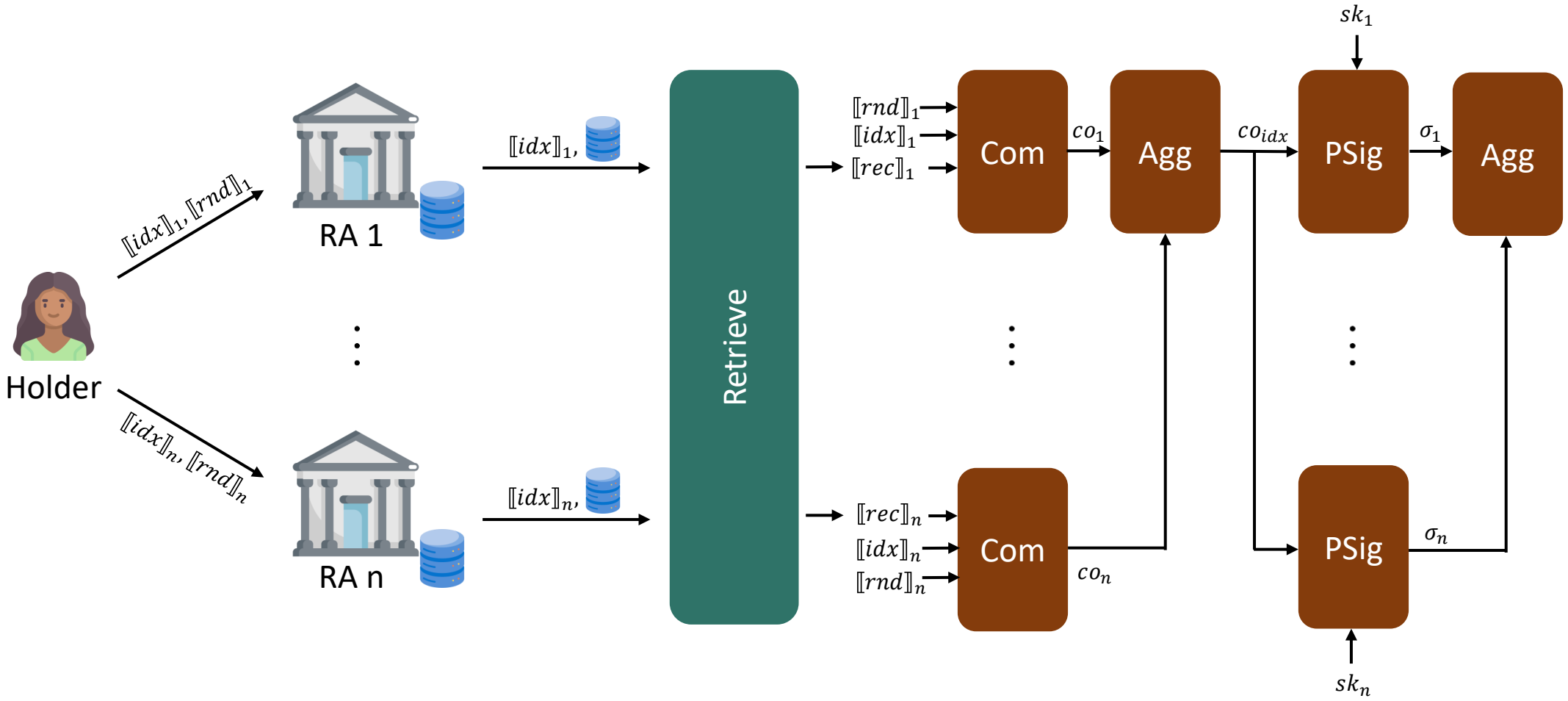
co	commitment



Constructing PRC

$[\![\cdot]\!]$	secret share
idx	index
rnd	randomness
rec	record value

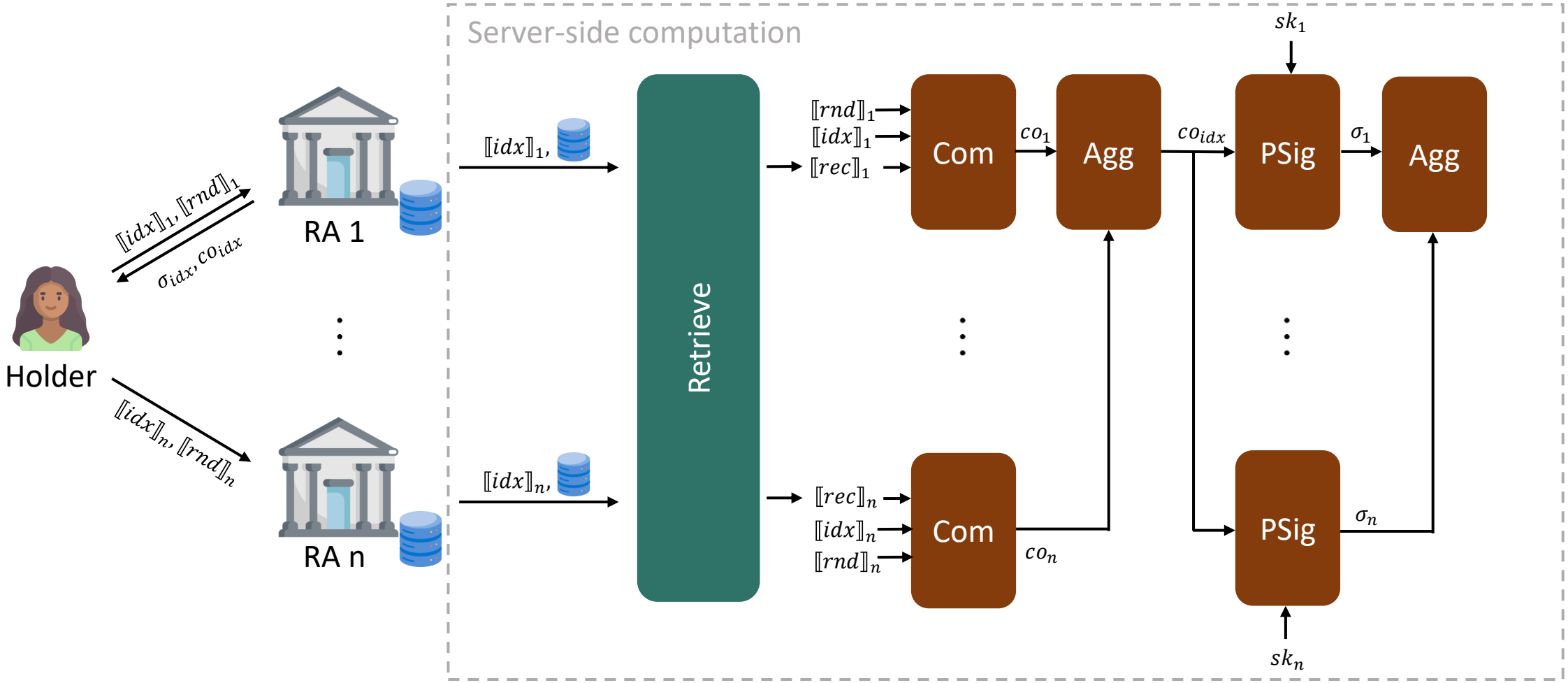
co	commitment
sk	signing key
σ	signature



Constructing PRC

$[\![\cdot]\!]$	secret share
idx	index
rnd	randomness
rec	record value

co	commitment
sk	signing key
σ	signature



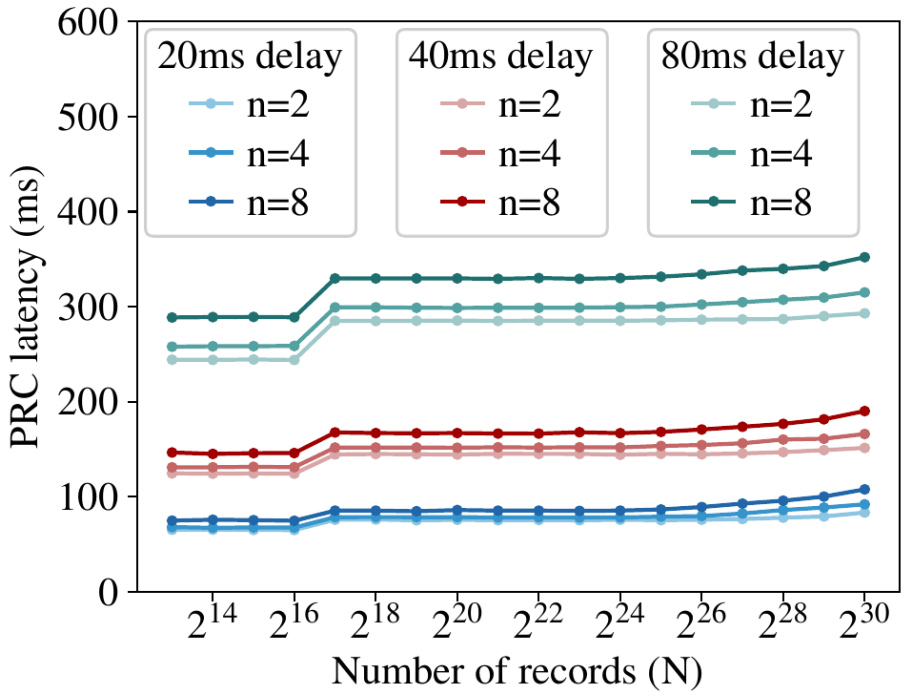
Evaluation

> 1 billion
credentials supported

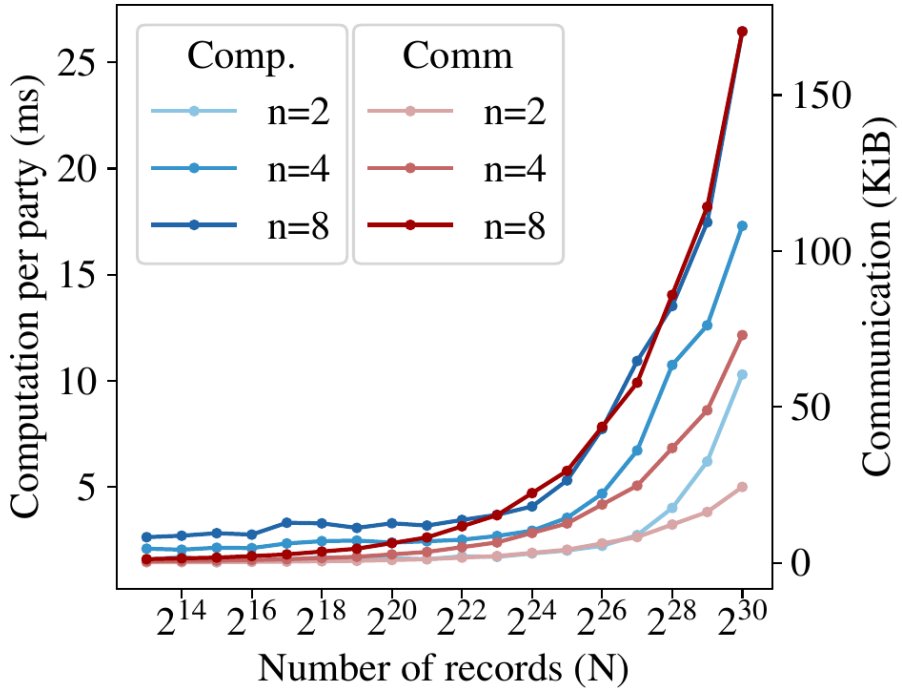
< 400ms
query latency

< 25ms
server compute per query

Latency

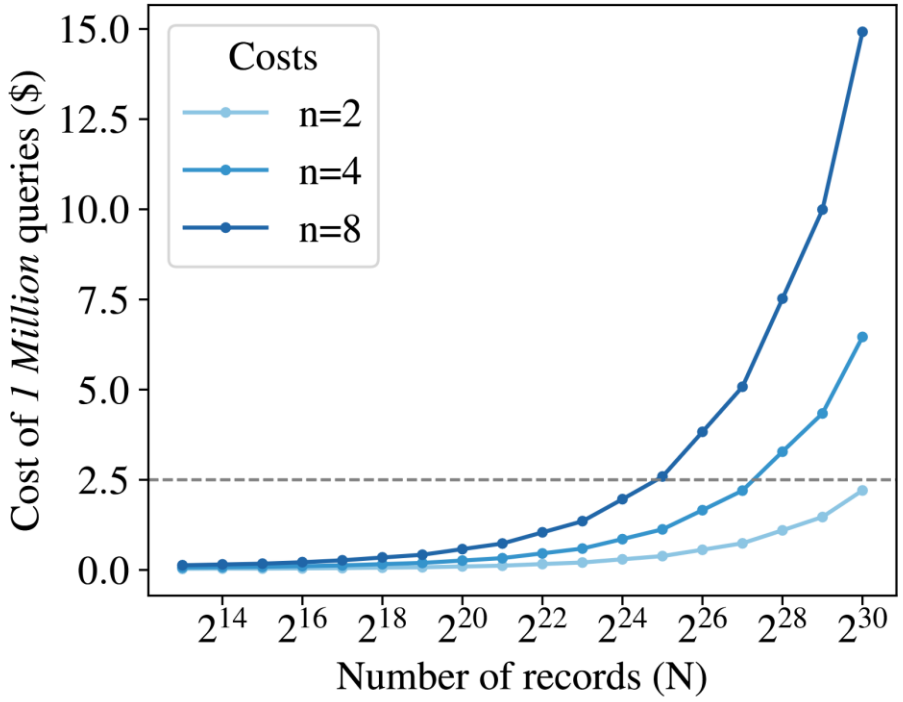


Computation & Communication



Evaluation

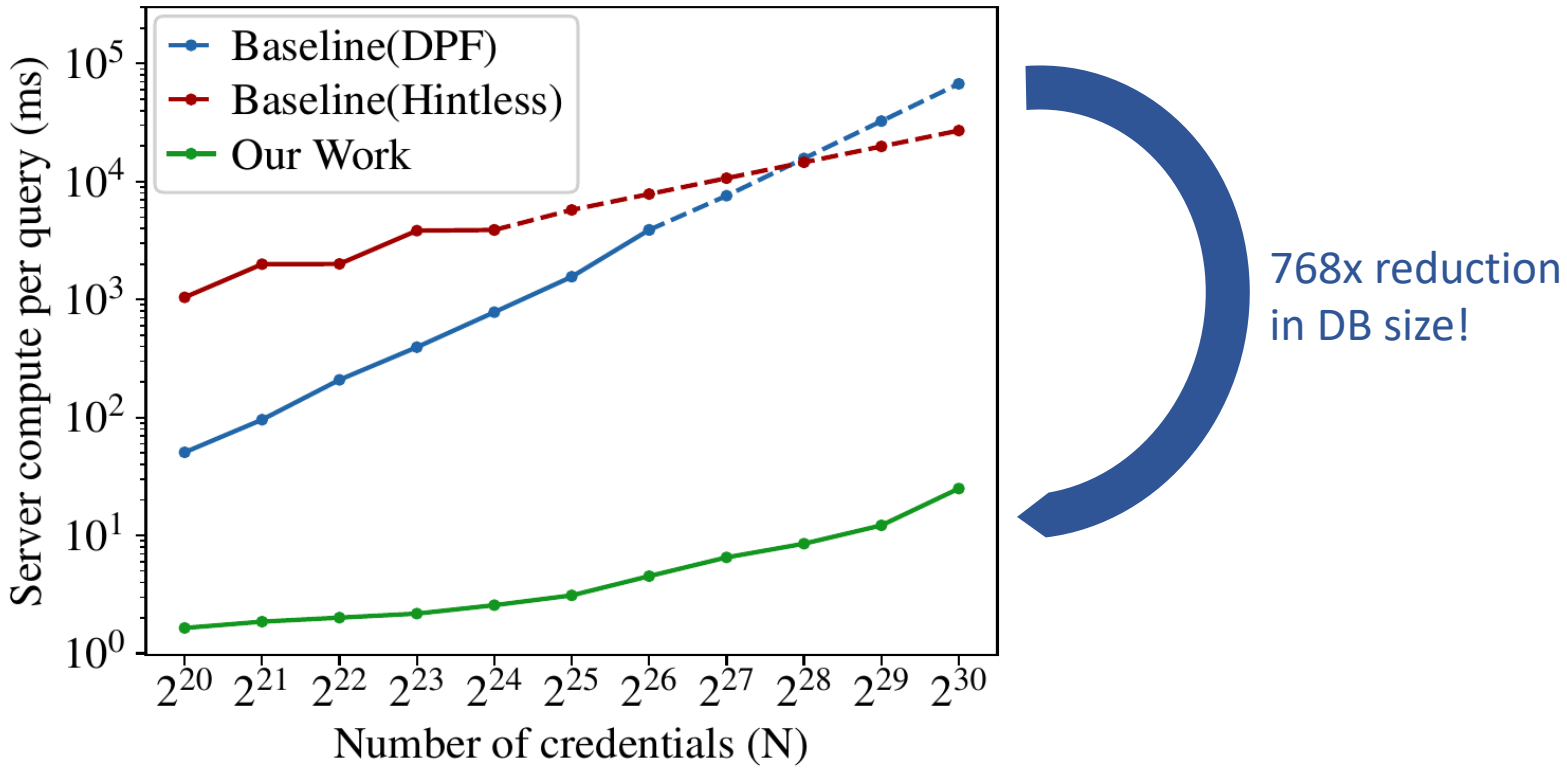
Cost



< $2.50

cost per server
for 1M queries

Comparison with Naïve PIR Approach



= = results extrapolated because code did not run for this DB size

Thank you for your attention!



