Non-Interactive Zero-Knowledge from Vector Trapdoor Hash

Pedro Branco
Bocconi

Arka Rai Choudhuri
Nexus

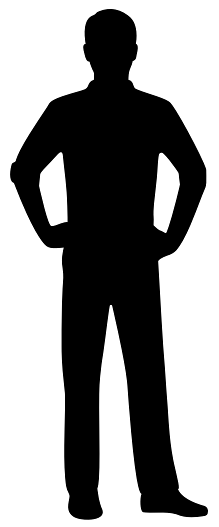
Nico Döttling
CISPA

Abhishek Jain
NTT and JHU

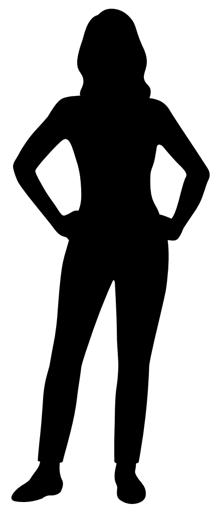
Giulio Malavolta
Bocconi

Akshayaram Srinivasan
University of Toronto

Zero-Knowledge Proofs [GMR85]

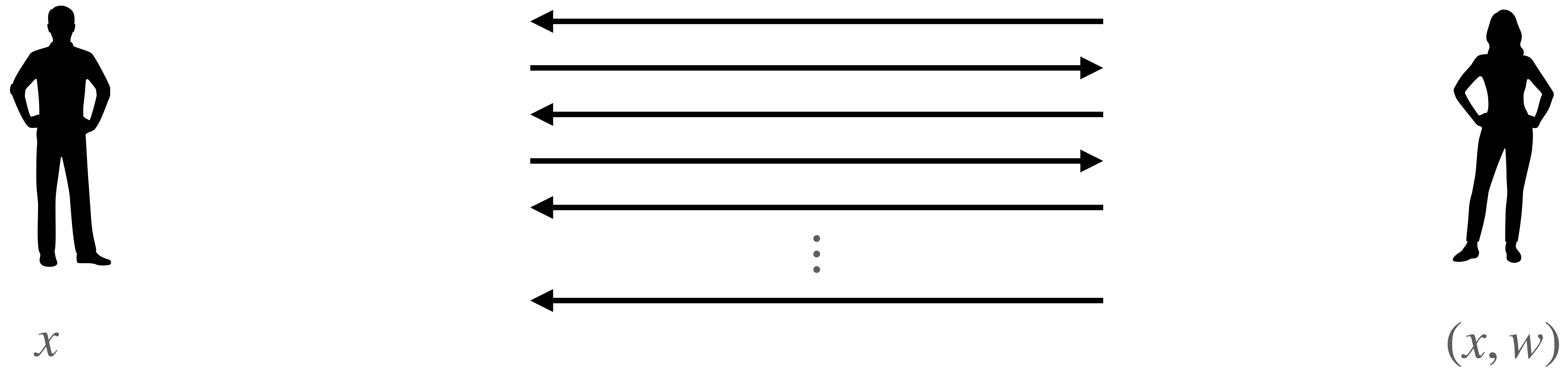


x

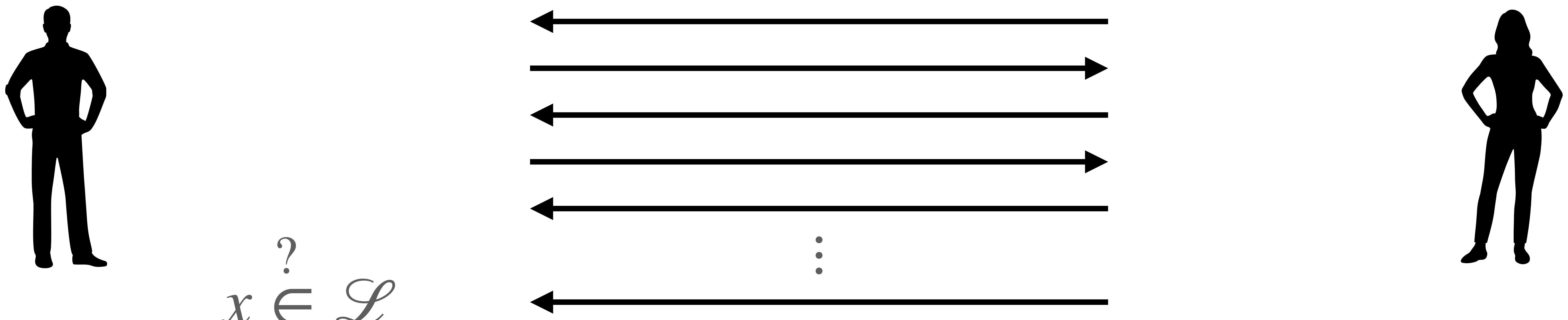


(x, w)

Zero-Knowledge Proofs [GMR85]



Zero-Knowledge Proofs [GMR85]

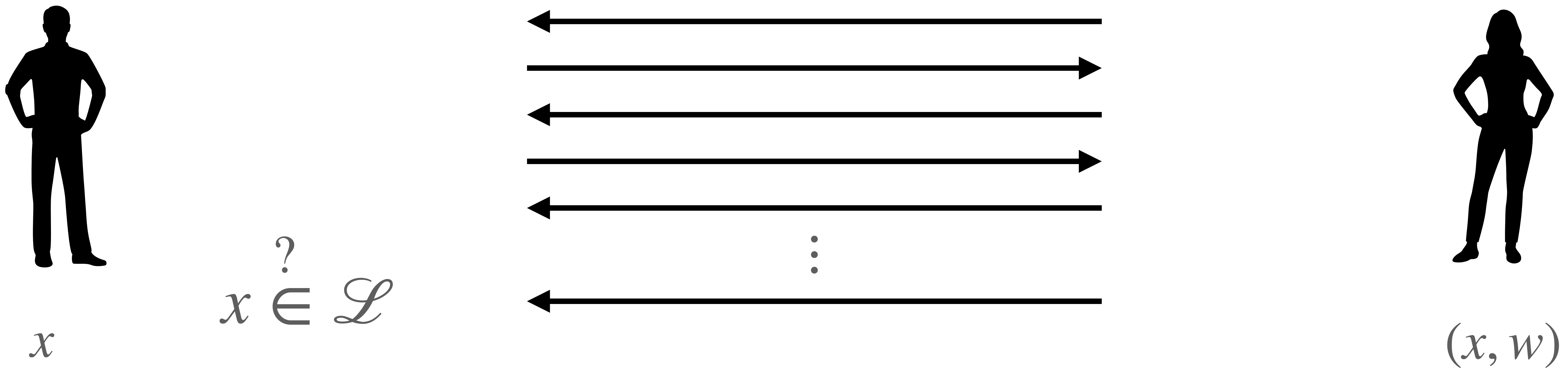


$x \overset{?}{\in} \mathscr{L}$

x

(x, w)

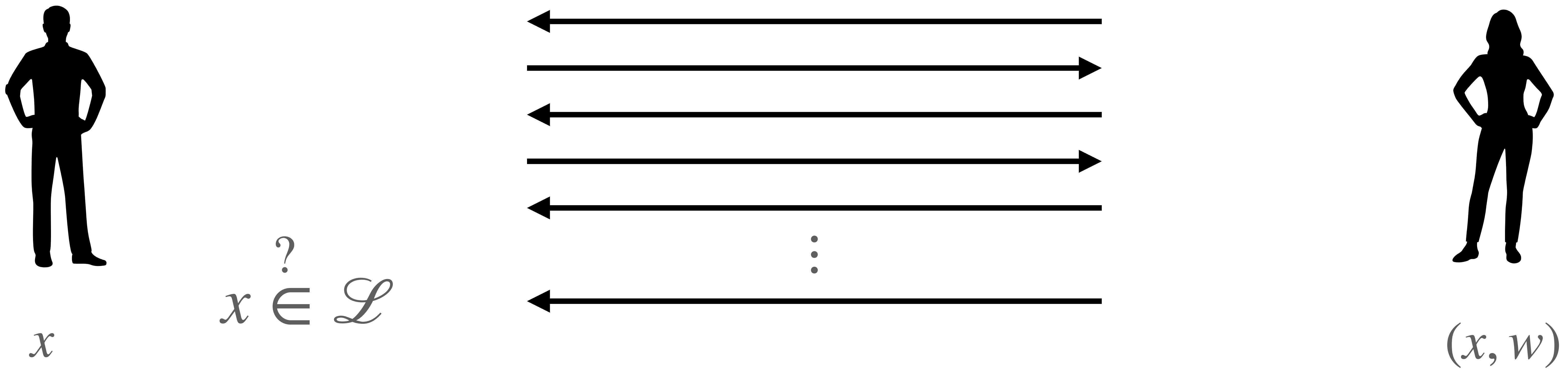
Zero-Knowledge Proofs [GMR85]



Soundness:

$$\Pr\left[x \notin \mathscr{L} \wedge \mathsf{V}\ \text{accepts}\right] = \mathsf{negl}(\lambda)$$

Zero-Knowledge Proofs [GMR85]



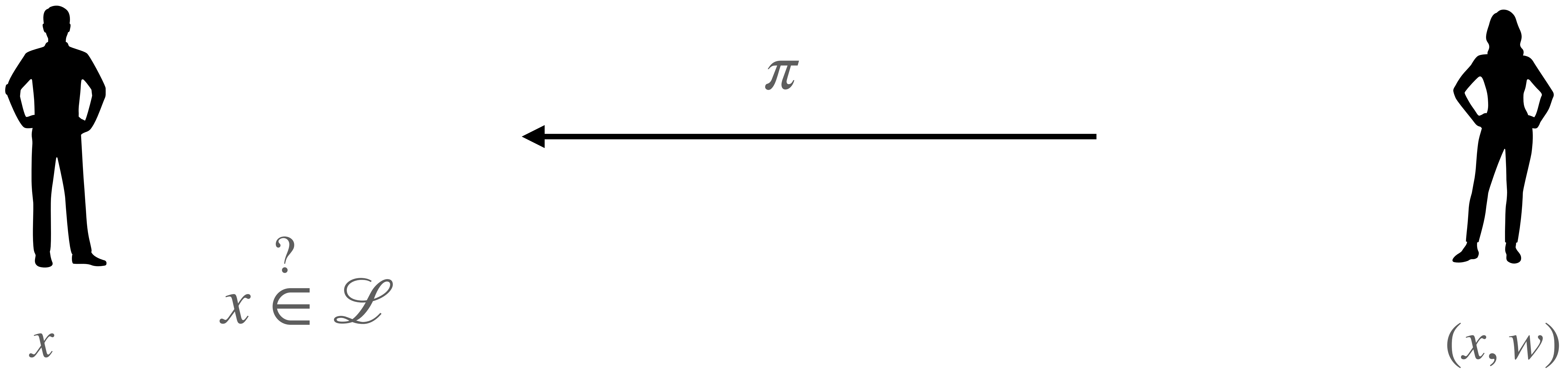
Soundness:

$$\mathsf{Pr}\left[x \notin \mathscr{L} \wedge \mathsf{V} \text{ accepts}\right] = \mathsf{negl}(\lambda)$$

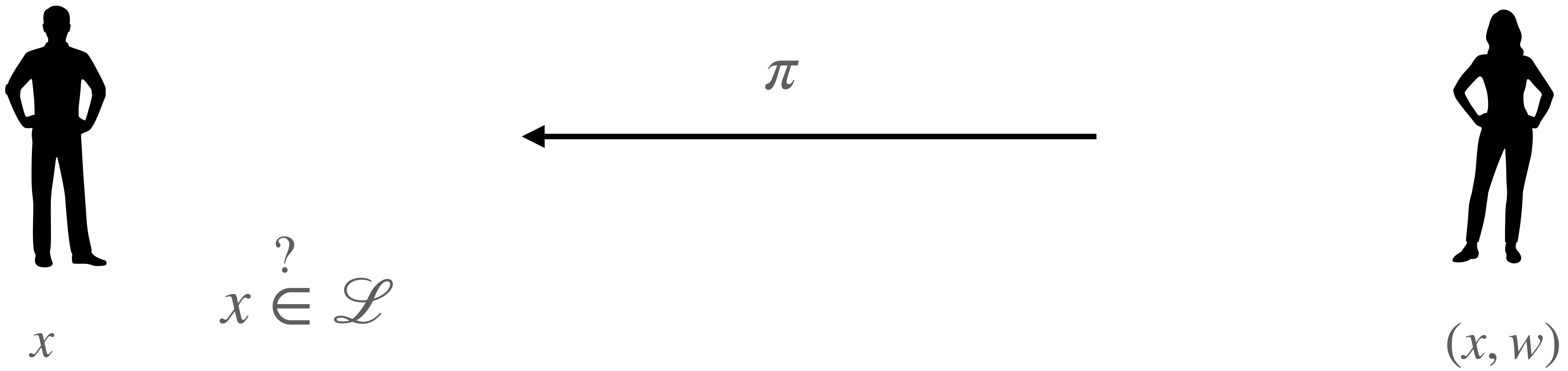
Zero-Knowledge:

$$\{\mathsf{T} \leftarrow \mathsf{Sim}(x)\} \approx \{\mathsf{T} \leftarrow (\mathsf{V}(x) \leftrightarrow \mathsf{P}(x, w))\}$$

Non-Interactive Zero-Knowledge [DMP88]



Non-Interactive Zero-Knowledge [DMP88]



Soundness:

$$\Pr\left[x \notin \mathscr{L} \wedge 1 \leftarrow \mathsf{V}(x, \pi)\right] = \mathsf{negl}(\lambda)$$

Zero-Knowledge:

$$\{\pi \leftarrow \mathsf{Sim}(x)\} \approx \{\pi \leftarrow \mathsf{P}(x, w)\}$$

Why NIZKs?

Theory:

- Minimal round complexity
- Assumptions

Why NIZKs?

Theory:

- Minimal round complexity
- Assumptions

Applications:

- CCA security
- Signatures
- Blockchains

⋮

Random Oracle Vs Standard model

- **Random Oracle:** Don’t exist

Random Oracle Vs Standard model

- **Random Oracle:** Don’t exist
- **Standard Model:** Impossible

Random Oracle Vs Standard model

- **Random Oracle:** Don't exist
- **Standard Model:** Impossible

$\boxed{\text{This talk: NIZK = NIZK for all NP in the CRS model}}$

NIZKs Constructions

Others

- Pairings [GOS'06]
- QR [BDMP91]

NIZKs Constructions

Others

- Pairings [GOS'06]
- QR [BDMP91]

Correlation Intractability Hash

- iO [CCRR18,HL18]
- FHE/LWE [CCH+19,PS19]
- DDH + LPN [BKM20]
- Sub-exp DDH [JJ21]
- MQ + LPN [DJJ24]

NIZKs Constructions

Others

- Pairings [GOS'06]
- QR [BDMP91]

Correlation Intractability Hash

- iO [CCRR18,HL18]
- FHE/LWE [CCH+19,PS19]
- DDH + LPN [BKM20]
- Sub-exp DDH [JJ21]
- MQ + LPN [DJJ24]

Hidden-Bits Generator

- Trapdoor permutations [FLS90]
- LWE (super-poly mod to noise) [Wat24]

NIZKs Constructions

Others

- Pairings [GOS'06]
- QR [BDMP91]

Correlation Intractability Hash

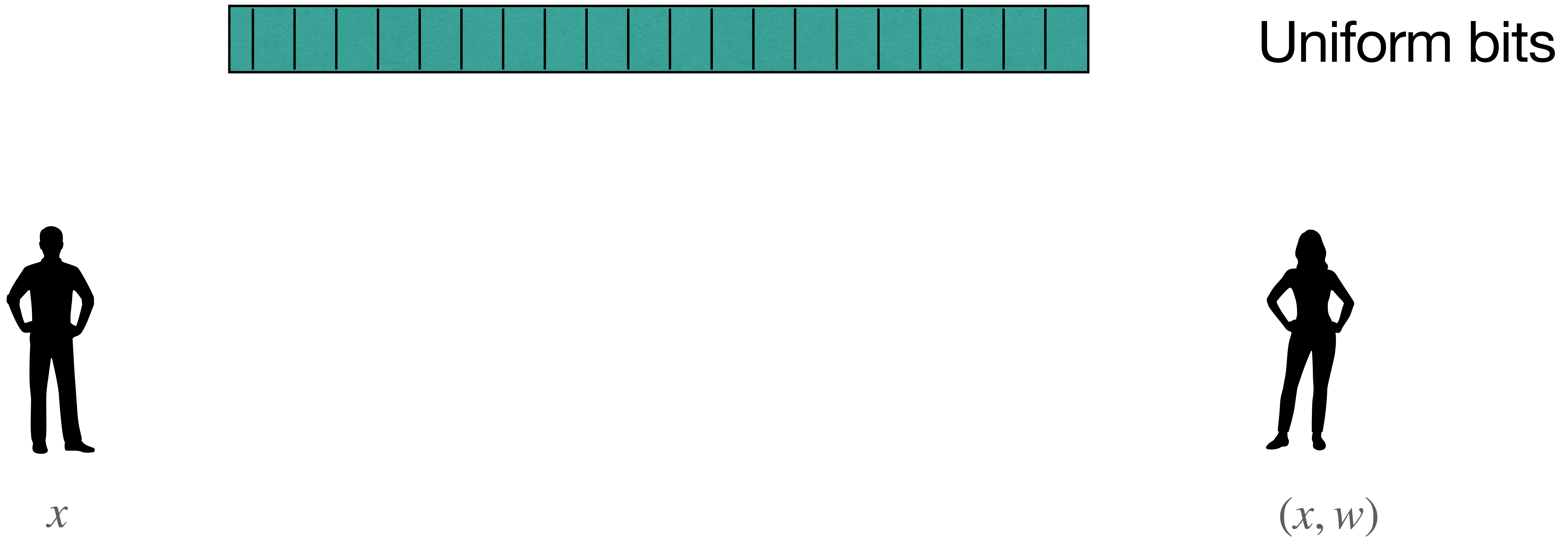
- iO [CCRR18,HL18]
- FHE/LWE [CCH+19,PS19]
- DDH + LPN [BKM20]
- Sub-exp DDH [JJ21]
- MQ + LPN [DJJ24]

Hidden-Bits Generator

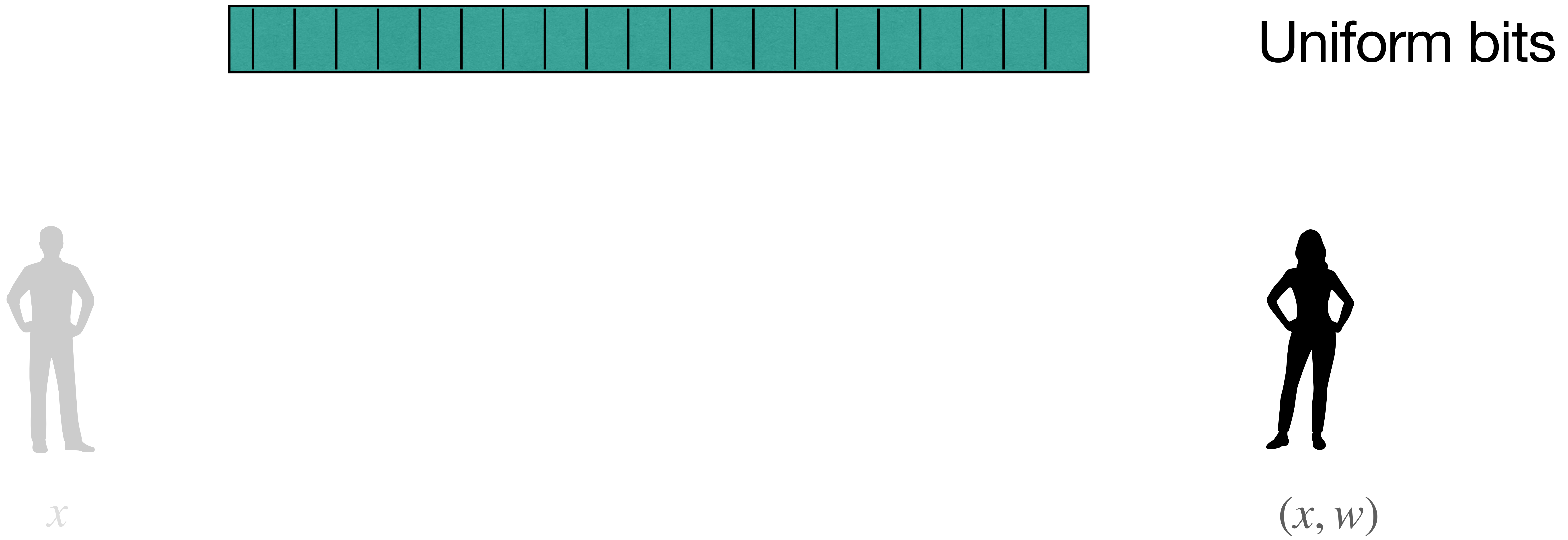
- Trapdoor permutations [FLS90]
- LWE (super-poly mod to noise) [Wat24]

?

Hidden-Bits Model [FLS90]



Hidden-Bits Model [FLS90]



Hidden-Bits Model [FLS90]

NIZKs via Hidden Bits Generator

NIZK in Hidden Bits Model
[FLS90]

+

Hidden Bits Generator
[QRW19,KMY20]

=

NIZK

Our Results

Theorem: There exists a HBG assuming either:

1. LWE with polynomial modulus-to-noise ratio
2. DDH + LPN

Our Results

Theorem: There exists a HBG assuming either:

1. LWE with polynomial modulus-to-noise ratio
2. DDH + LPN

Corollary (LWE):

Dual-mode NIZK

1. Stat ZK in the URS
2. Stat Soundness in the CRS

Our Results

Theorem: There exists a HBG assuming either:

1. LWE with polynomial modulus-to-noise ratio
2. DDH + LPN

Corollary (LWE):

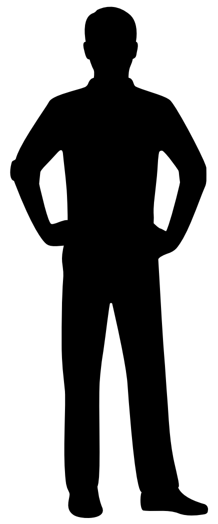
Dual-mode NIZK

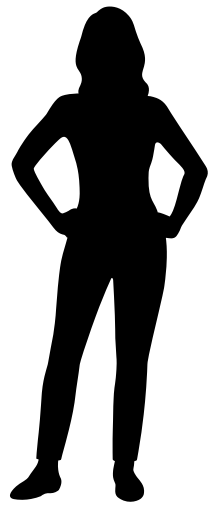
1. Stat ZK in the URS
2. Stat Soundness in the CRS

Corollary (DDH+LPN):

NIZK with statistical soundness

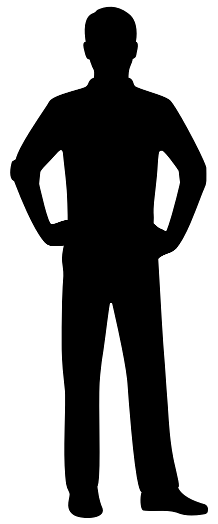
New Primitive: Vector Trapdoor Hash

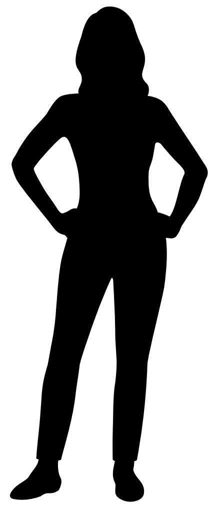




New Primitive: Vector Trapdoor Hash

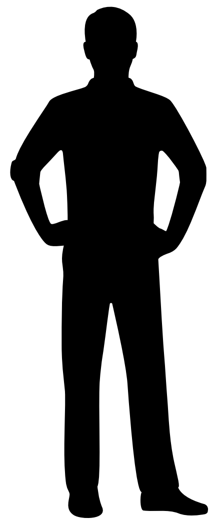
$$\left(\mathsf{hk}, \{\mathsf{ek}_i, \mathsf{td}_i\}_{i\in[k]}\right) \leftarrow \mathsf{Setup}$$





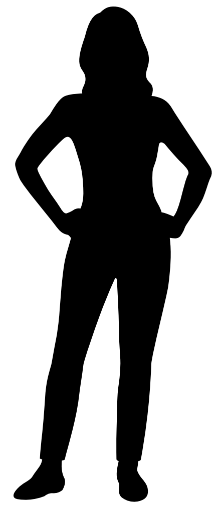
New Primitive: Vector Trapdoor Hash

$$\left(\mathsf{hk}, \{\mathsf{ek}_i, \mathsf{td}_i\}_{i\in[k]}\right) \leftarrow \mathsf{Setup}$$



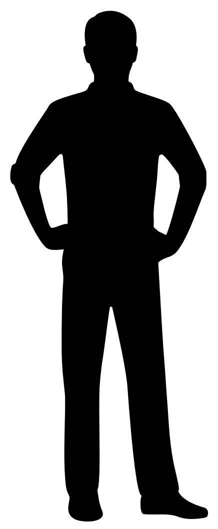
$$\left(\mathbf{h}, \{\pi_i\}_{i\in[k]}\right) \leftarrow \mathsf{Hash}(\mathsf{hk}, \mathbf{x})$$

$$e_i \leftarrow \mathsf{Enc}(\mathsf{ek}_i, \pi_i)$$



New Primitive: Vector Trapdoor Hash

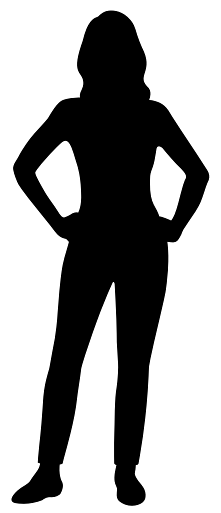
$$\left(\mathsf{hk}, \{\mathsf{ek}_i, \mathsf{td}_i\}_{i\in[k]}\right) \leftarrow \mathsf{Setup}$$



$d_i \leftarrow \mathsf{Dec}(\mathsf{td}_i, \mathbf{h})$

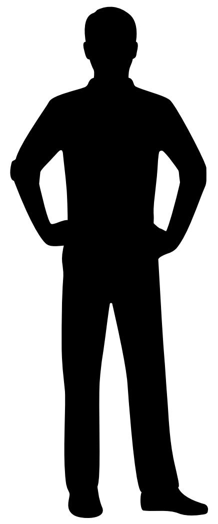
$\left(\mathbf{h}, \{\pi_i\}_{i\in[k]}\right) \leftarrow \mathsf{Hash}(\mathsf{hk}, \mathbf{x})$

$e_i \leftarrow \mathsf{Enc}(\mathsf{ek}_i, \pi_i)$



New Primitive: Vector Trapdoor Hash

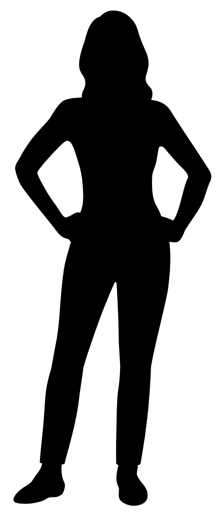
$$\left(\mathsf{hk}, \{\mathsf{ek}_i, \mathsf{td}_i\}_{i\in[k]}\right) \leftarrow \mathsf{Setup}$$



$d_i \leftarrow \mathsf{Dec}(\mathsf{td}_i, \mathbf{h})$

$\left(\mathbf{h}, \{\pi_i\}_{i\in[k]}\right) \leftarrow \mathsf{Hash}(\mathsf{hk}, \mathbf{x})$

$e_i \leftarrow \mathsf{Enc}(\mathsf{ek}_i, \pi_i)$

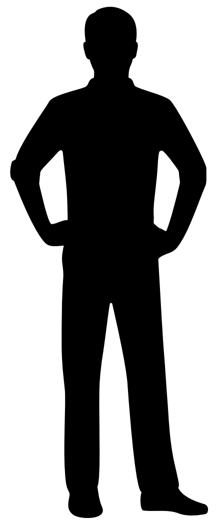


Local opening:

π_i is a local opening for $\mathbf{x}_i$

New Primitive: Vector Trapdoor Hash

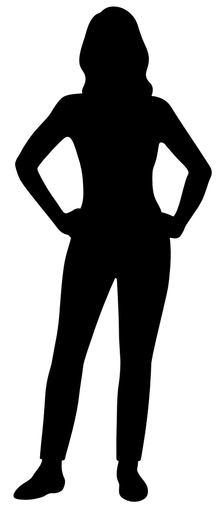
$$\left(\mathsf{hk}, \{\mathsf{ek}_i, \mathsf{td}_i\}_{i\in[k]}\right) \leftarrow \mathsf{Setup}$$



$d_i \leftarrow \mathsf{Dec}(\mathsf{td}_i, \mathbf{h})$

$\left(\mathbf{h}, \{\pi_i\}_{i\in[k]}\right) \leftarrow \mathsf{Hash}(\mathsf{hk}, \mathbf{x})$

$e_i \leftarrow \mathsf{Enc}(\mathsf{ek}_i, \pi_i)$



Local opening:

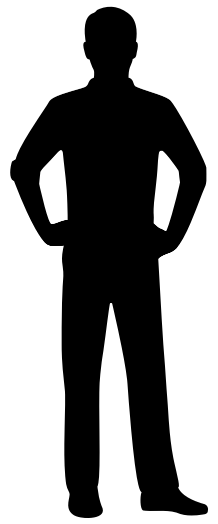
π_i is a local opening for $\mathbf{x}_i$

Statistical binding:

$e_i = d_i$ for almost all $i \in [k]$

New Primitive: Vector Trapdoor Hash

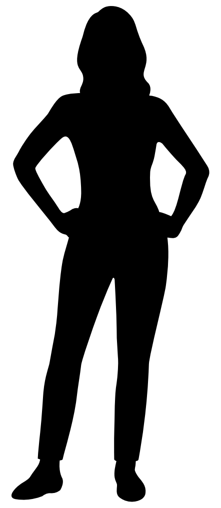
$$\left(\mathsf{hk}, \{\mathsf{ek}_i, \mathsf{td}_i\}_{i\in[k]}\right) \leftarrow \mathsf{Setup}$$



$d_i \leftarrow \mathsf{Dec}(\mathsf{td}_i, \mathbf{h})$

$\left(\mathbf{h}, \{\pi_i\}_{i\in[k]}\right) \leftarrow \mathsf{Hash}(\mathsf{hk}, \mathbf{x})$

$e_i \leftarrow \mathsf{Enc}(\mathsf{ek}_i, \pi_i)$



Local opening:

π_i is a local opening for $\mathbf{x}_i$

Statistical binding:

$e_i = d_i$ for almost all $i \in [k]$

Hiding:

e_{i*} is uniform, given $\{e_i, \pi_i\}_{i \neq i*}$

VTDH from LWE

1. Hashing and encoding keys
2. Hash and local openings
3. Encoding and decoding

Learning with Errors

$$\left(\boxed{\mathbf{A}}\ ,\ \boxed{\mathbf{s}}\,\boxed{\mathbf{A}} + \boxed{\mathbf{e}} \right)$$

$$\approx_c$$

Expanding

$$\left(\boxed{\mathbf{A}}\ ,\ \boxed{\mathbf{u}} \right)$$

$\mathbf{A} \leftarrow \{0,1\}^{n\times m}$, $\mathbf{s} \leftarrow \{0,1\}^{n}$, $\mathbf{u} \leftarrow \{0,1\}^{m}$ and $\mathbf{e} \leftarrow \mathsf{DG}_\sigma^m$

VTDH from LWE: Hashing and Encoding Keys

$$\mathsf{hk} = \mathbf{A}_1, \ldots, \mathbf{A}_k, \underbrace{\mathbf{W}_1, \ldots, \mathbf{W}_k}_{\text{binary}}$$

VTDH from LWE: Hashing and Encoding Keys

$$\mathsf{hk} = \mathbf{A}_1, \ldots, \mathbf{A}_k, \underbrace{\mathbf{W}_1, \ldots, \mathbf{W}_k}_{\text{binary}} \text{ such that } \mathbf{A}_i \mathbf{W}_i = \mathbf{U}_i$$

VTDH from LWE: Hashing and Encoding Keys

$$\mathsf{hk} = \mathbf{A}_1, \ldots, \mathbf{A}_k, \underbrace{\mathbf{W}_1, \ldots, \mathbf{W}_k}_{\text{binary}} \text{ such that } \mathbf{A}_i \mathbf{W}_i = \mathbf{U}_i$$

$$\mathsf{ek}_i = (\mathbf{s}_i^T \mathbf{A}_1 + \mathbf{e}_1, \ldots, \mathbf{s}_i^T \mathbf{U}_i + \mathbf{e}_i, \ldots, \mathbf{s}_i^T \mathbf{A}_k + \mathbf{e}_k)$$

VTDH from LWE: Hash and Local Proofs

Hash: binary $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k)$ compute $\mathbf{h} = \sum \mathbf{U}_i \mathbf{x}_i$

VTDH from LWE: Hash and Local Proofs

Hash: binary $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k)$ compute $\mathbf{h} = \sum \mathrm{U}_i \mathbf{x}_i$

Local opening: $\pi_i = (\mathbf{W}_1 \mathbf{x}_1, \ldots, \mathbf{x}_i, \ldots, \mathbf{W}_k \mathbf{x}_k)$

VTDH from LWE: Hash and Local Proofs

Hash: binary $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k)$ compute $\mathbf{h} = \sum \mathbf{U}_i \mathbf{x}_i$

Local opening: $\pi_i = (\mathbf{W}_1 \mathbf{x}_1, \ldots, \mathbf{x}_i, \ldots, \mathbf{W}_k \mathbf{x}_k)$

Local Verification:

$(\mathbf{A}_1, \ldots, \mathbf{U}_i, \ldots, , \mathbf{A}_k) \cdot \pi_i$

VTDH from LWE: Hash and Local Proofs

Hash: binary $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k)$ compute $\mathbf{h} = \sum \mathbf{U}_i \mathbf{x}_i$

Local opening: $\pi_i = (\mathbf{W}_1 \mathbf{x}_1, \ldots, \mathbf{x}_i, \ldots, \mathbf{W}_k \mathbf{x}_k)$

Local Verification:

$$(\mathbf{A}_1, \ldots, \mathbf{U}_i, \ldots, , \mathbf{A}_k) \cdot \pi_i = (\mathbf{A}_1, \ldots, \mathbf{U}_i, \ldots, , \mathbf{A}_k)(\mathbf{W}_1 \mathbf{x}_1, \ldots, x_i, \ldots, \mathbf{W}_k \mathbf{x}_k)$$
$$= \sum \mathbf{U}_i \mathbf{x}_i = h$$

VTDH from LWE: Encoding and Decoding

Encoding: $e_i = \mathsf{ek}_i \cdot \pi_i$

VTDH from LWE: Encoding and Decoding

Encoding: $e_i = \mathsf{ek}_i \cdot \pi_i$

$$= (\mathbf{s}_i^T \mathbf{A}_1 + \mathbf{e}_1, \ldots, \mathbf{s}_i^T \mathrm{U}_i + \mathbf{e}_i, \ldots, \mathbf{s}_i^T \mathbf{A}_k + \mathbf{e}_k) \cdot (\mathbf{W}_1 \mathbf{x}_1, \ldots, \mathbf{x}_i, \ldots, \mathbf{W}_k \mathbf{x}_k)$$

$$= \mathbf{s}_i \cdot \Big(\sum \mathrm{U}_i \mathbf{x}_i \Big) + \tilde{e}$$

VTDH from LWE: Encoding and Decoding

Encoding: $e_i = \mathsf{ek}_i \cdot \pi_i$

$$= (\mathbf{s}_i^T\mathbf{A}_1 + \mathbf{e}_1, \ldots, \mathbf{s}_i^T\mathbf{U}_i + \mathbf{e}_i, \ldots, \mathbf{s}_i^T\mathbf{A}_k + \mathbf{e}_k) \cdot (\mathbf{W}_1\mathbf{x}_1, \ldots, \mathbf{x}_i, \ldots, \mathbf{W}_k\mathbf{x}_k)$$

$$= \mathbf{s}_i \cdot \left(\sum \mathbf{U}_i\mathbf{x}_i\right) + \tilde{e}$$

Decoding: $d_i = \mathbf{s}_i \cdot \mathbf{h} = \mathbf{s}_i \cdot \left(\sum \mathbf{U}_i\mathbf{x}_i\right)$

VTDH from LWE: Encoding and Decoding

Encoding: $e_i = \mathsf{ek}_i \cdot \pi_i$

$$= (\mathbf{s}_i^T \mathbf{A}_1 + \mathbf{e}_1, \ldots, \mathbf{s}_i^T \mathbf{U}_i + \mathbf{e}_i, \ldots, \mathbf{s}_i^T \mathbf{A}_k + \mathbf{e}_k) \cdot (\mathbf{W}_1 \mathbf{x}_1, \ldots, \mathbf{x}_i, \ldots, \mathbf{W}_k \mathbf{x}_k)$$

$$= \mathbf{s}_i \cdot \left(\sum \mathbf{U}_i \mathbf{x}_i \right) + \tilde{e}$$

Decoding: $d_i = \mathbf{s}_i \cdot \mathbf{h} = \mathbf{s}_i \cdot \left(\sum \mathbf{U}_i \mathbf{x}_i \right)$

$$\boxed{\mathsf{Round}(e_i) = \mathsf{Round}(d_i)}$$

$$\Downarrow$$

Statistical Binding

VTDH from LWE: Hiding for $i = 1$

To prove: $e_1 = \mathsf{ek}_1 \cdot \pi_1 \approx v \leftarrow \mathsf{Unif}$

VTDH from LWE: Hiding for $i = 1$

To prove: $e_1 = \mathsf{ek}_1 \cdot \pi_1 \approx v \leftarrow \mathsf{Unif}$

1st Step:

$$\boxed{\mathsf{ek}_i = (\mathbf{s}_i^T \mathbf{A}_1 + \mathbf{e}_1, \ldots, \mathbf{s}_i^T \mathbf{U}_i + \mathbf{e}_i, \ldots, \mathbf{s}_i^T \mathbf{A}_k + \mathbf{e}_k)}$$

$$\Big\downarrow \text{ LWE}$$

$$\boxed{\mathsf{ek}_i = (\mathbf{u}_1, \ldots, \mathbf{u}_i, \ldots, \mathbf{u}_k)}$$

VTDH from LWE: Hiding for $i = 1$

To prove: $e_1 = \mathsf{ek}_1 \cdot \pi_1 \approx v \leftarrow \mathsf{Unif}$

1st Step:

$$\boxed{\mathsf{ek}_i = (\mathbf{s}_i^T \mathbf{A}_1 + \mathbf{e}_1, \ldots, \mathbf{s}_i^T \mathbf{U}_i + \mathbf{e}_i, \ldots, \mathbf{s}_i^T \mathbf{A}_k + \mathbf{e}_k)}$$

$$\Big\downarrow \text{LWE}$$

$$\boxed{\mathsf{ek}_i = (\mathbf{u}_1, \ldots, \mathbf{u}_i, \ldots, \mathbf{u}_k)}$$

2nd Step:

$$\boxed{(\mathsf{ek}_1 \pi_1, \mathbf{W}_1 \mathbf{x}_1) \approx_s (v, \mathbf{W}_1 \mathbf{x}_1)}$$

LHL

Recap

- New NIZKs constructions via HBG.

Recap

- New NIZKs constructions via HBG.
- LWE Result: Dual-mode NIZK from LWE.

Recap

- New NIZKs constructions via HBG.
- LWE Result: Dual-mode NIZK from LWE.
- DDH + LPN Result: NIZK from (DDH + LPN) with statistical soundness.

Recap

- New NIZKs constructions via HBG.
- LWE Result: Dual-mode NIZK from LWE.
- DDH + LPN Result: NIZK from (DDH + LPN) with statistical soundness.

Thanks!

Non-Interactive Zero-Knowledge from Vector Trapdoor Hash

Pedro Branco

Bocconi

Arka Rai Choudhuri

Nexus

Nico Döttling

CISPA

Abhishek Jain

NTT and JHU

Giulio Malavolta

Bocconi

Akshayaram Srinivasan

University of Toronto