Concurrently Secure Identification Schemes based on the Worst-Case Hardness of Lattice Problems

ASIACRYPT 2008
Dec. 10

Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa
(Tokyo Institute of Technology)

Agenda

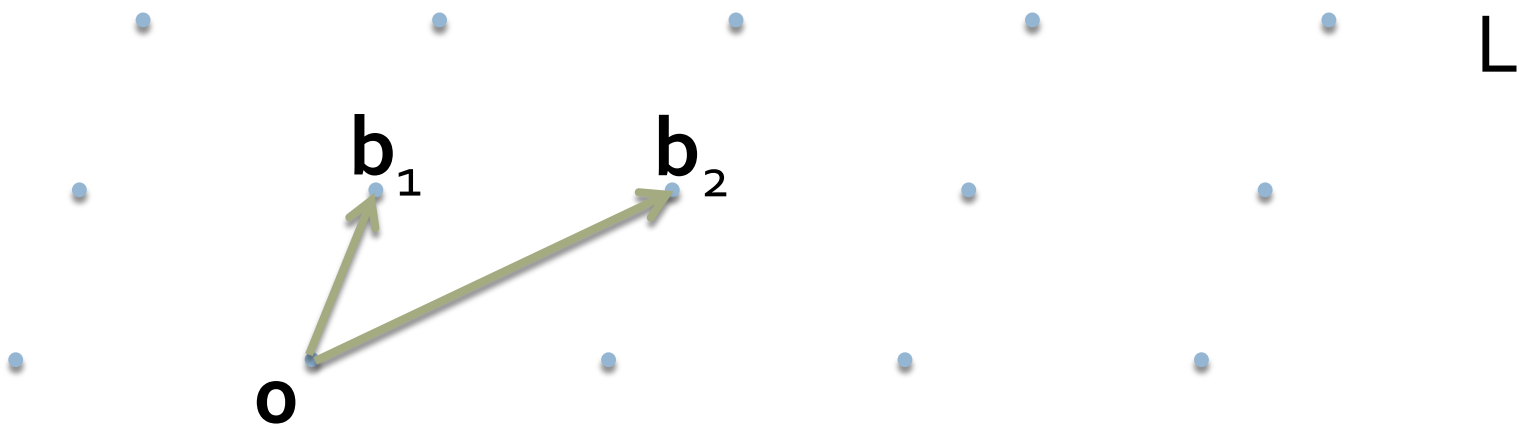
- Background
- Strategy for C-ID
- Lyubashevsky's ID
- Ours (or Stern's ID)

Agenda

- Background
  - Lattices
  - Lattice Problems
  - Schemes and Their Bases
- Strategy for C-ID
- Lyubashevsky's ID
- Ours (or Stern's ID)

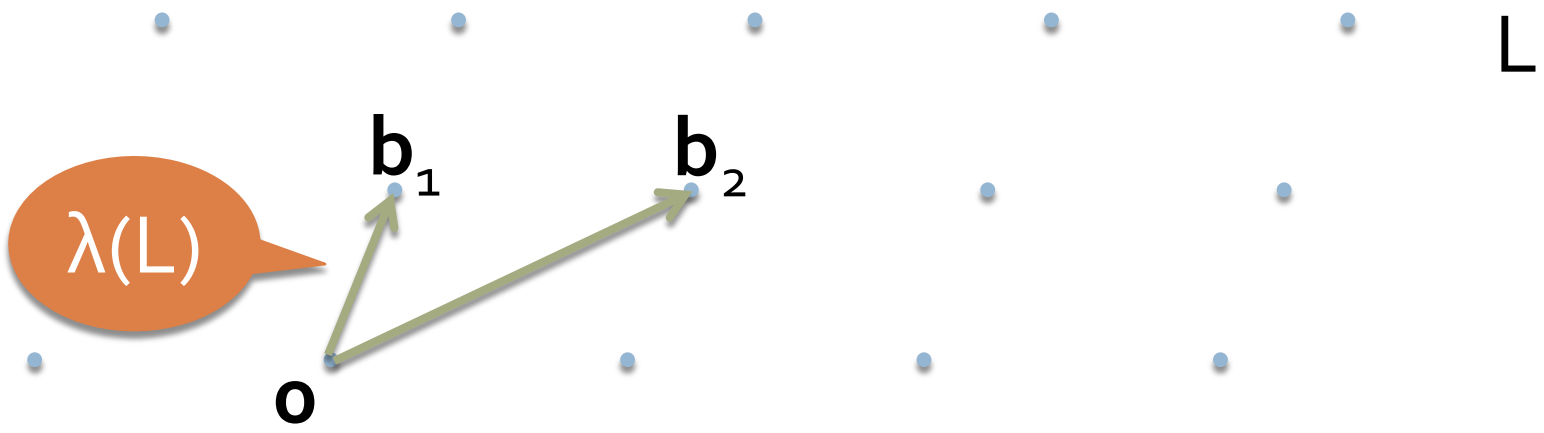
Lattices

- Given: $\mathbf{B}=[\mathbf{b}_1,\ldots,\mathbf{b}_n]$
- $L(\mathbf{B}) := \{\Sigma_i \alpha_i \mathbf{b}_i \mid \alpha_i \in \mathbb{Z} \text{ for all } i\}$



Lattices

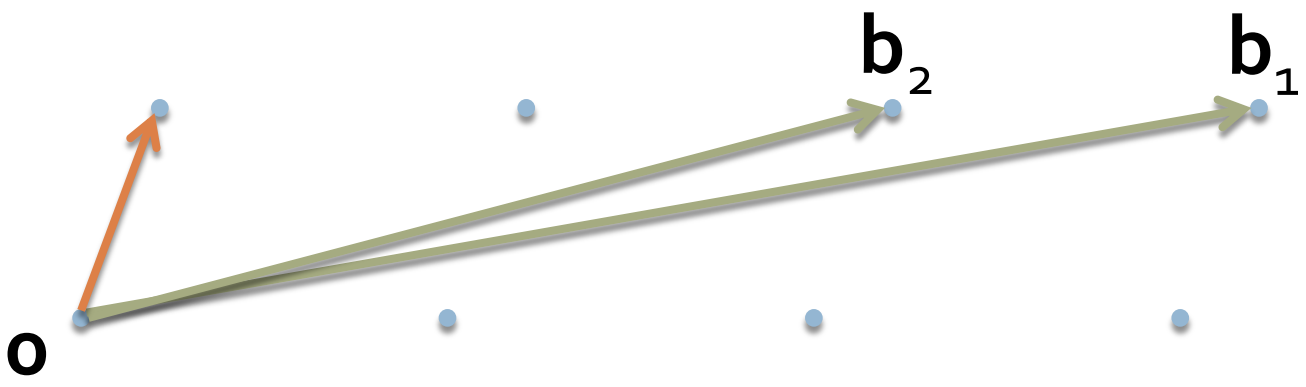
- Given: $\mathbf{B}=[\mathbf{b}_1,\ldots,\mathbf{b}_n]$
- $L(\mathbf{B}) := \{\Sigma_i \alpha_i \mathbf{b}_i \mid \alpha_i \in \mathbb{Z} \text{ for all } i\}$
- $\lambda(L)$: the length of the shortest vector in L



Approx. ver. of SVP

SVP_γ

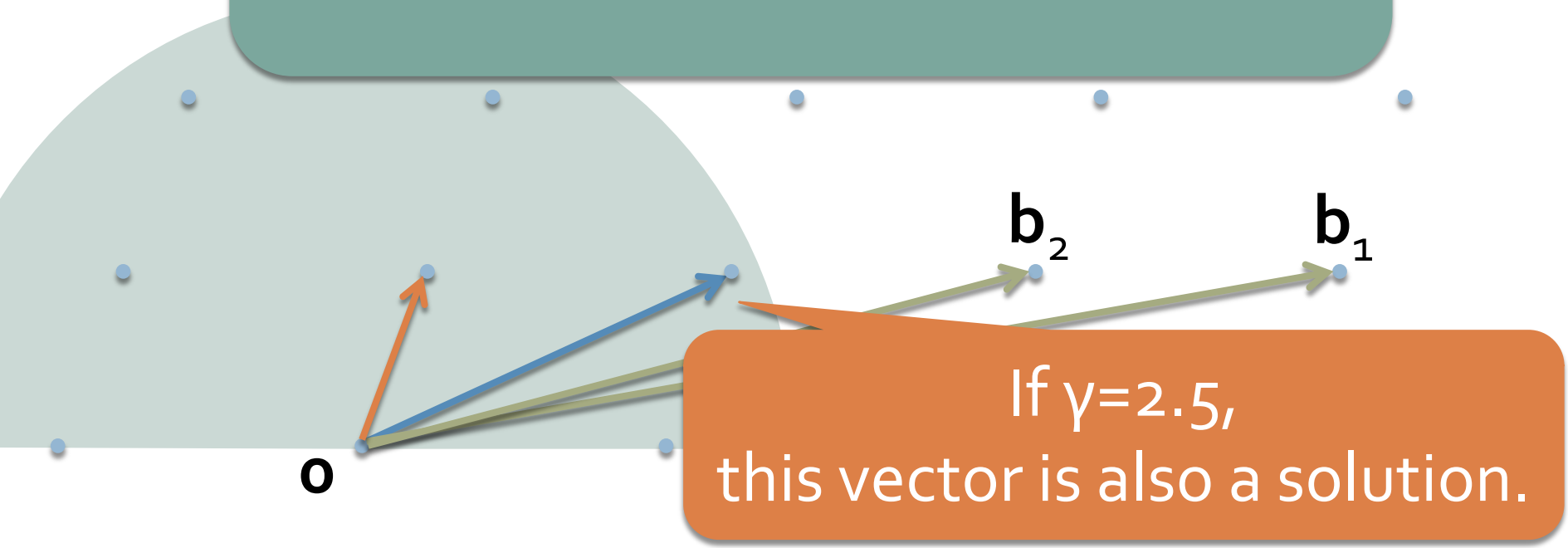
Given a basis **B** of a lattice L,
find $\mathbf{v} \in L - \{\mathbf{o}\}$ s.t. $\|\mathbf{v}\| \leqq \gamma\, \lambda(L)$



Approx. ver. of SVP

SVP_γ

Given a basis **B** of a lattice L,
find $\mathbf{v} \in L - \{\mathbf{o}\}$ s.t. $\|\mathbf{v}\| \leqq \gamma\, \lambda(L)$



If $\gamma = 2.5$,
this vector is also a solution.

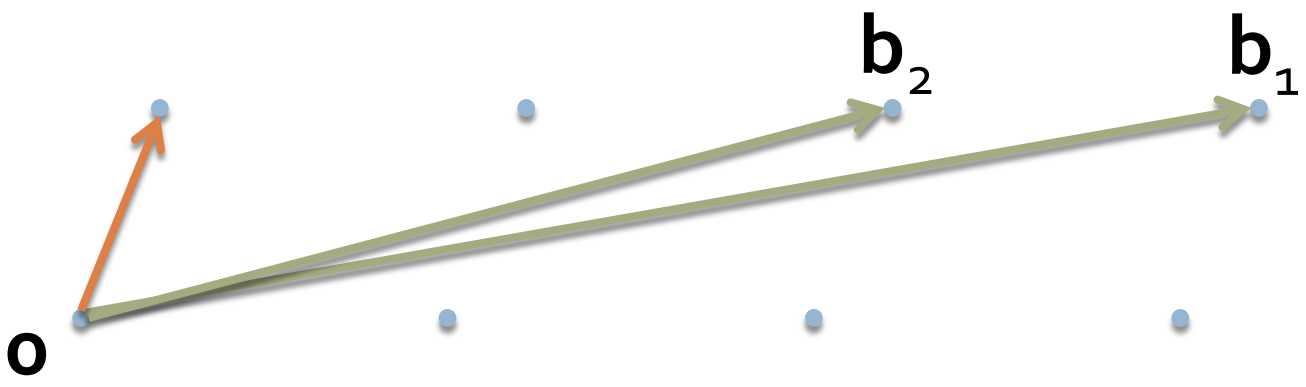
Gap ver. of SVP_γ

$GapSVP_\gamma$

Given a basis **B** and a real d,

YES: $\lambda(L) \leqq d$

NO: $\lambda(L) > \gamma d$



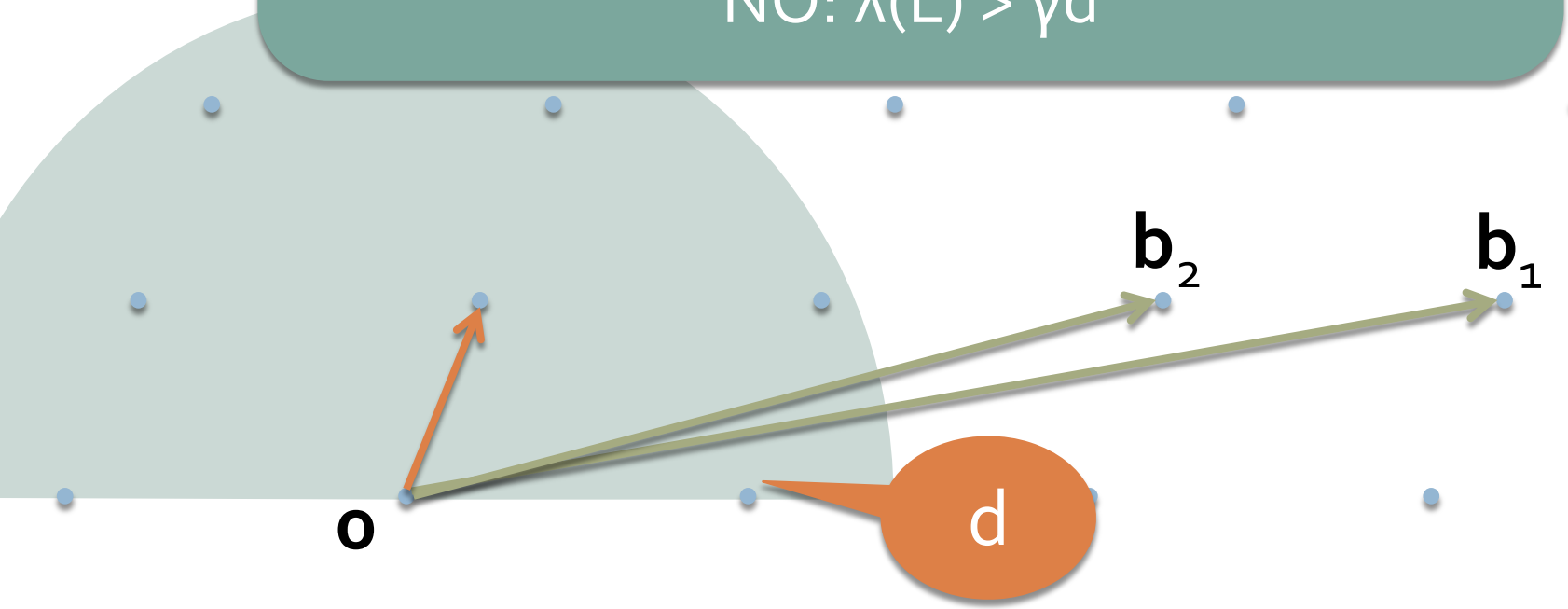
Gap ver. of SVP_γ

$GapSVP_\gamma$

Given a basis **B** and a real d,

YES: $\lambda(L) \leqq d$

NO: $\lambda(L) > \gamma d$



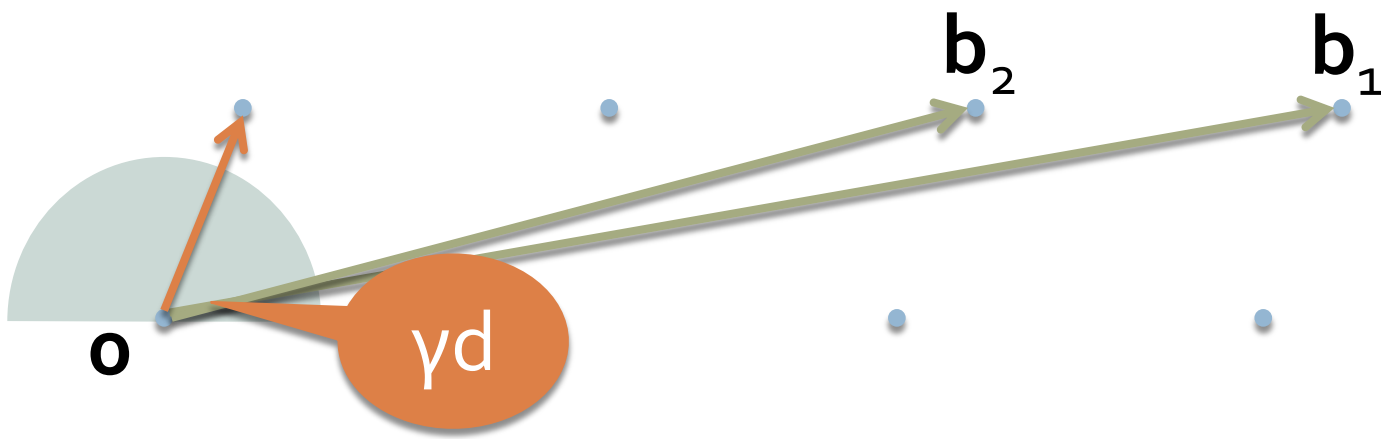
Gap ver. of SVP_γ

$GapSVP_\gamma$

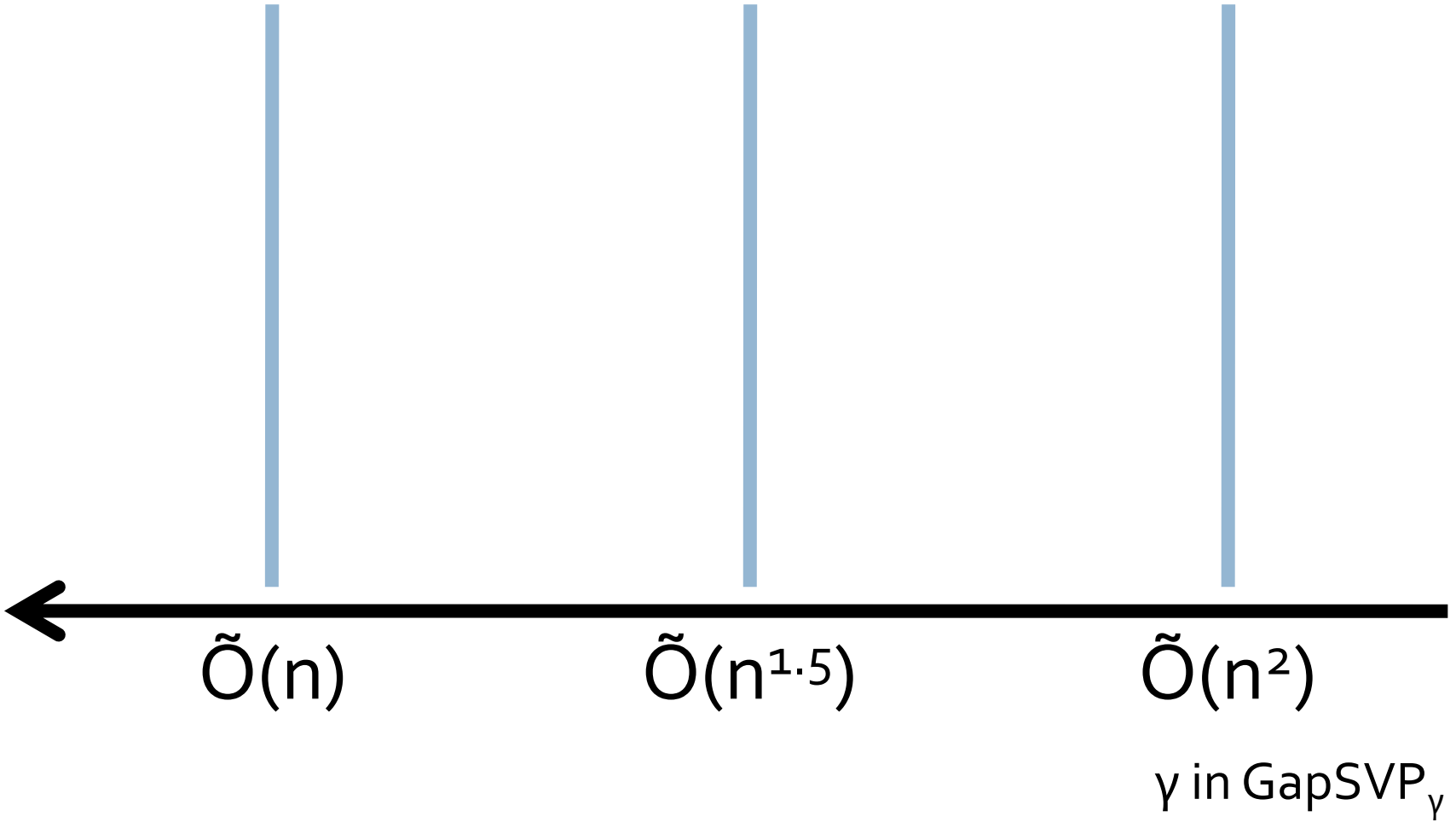
Given a basis **B** and a real d,

YES: $\lambda(L) \leqq d$

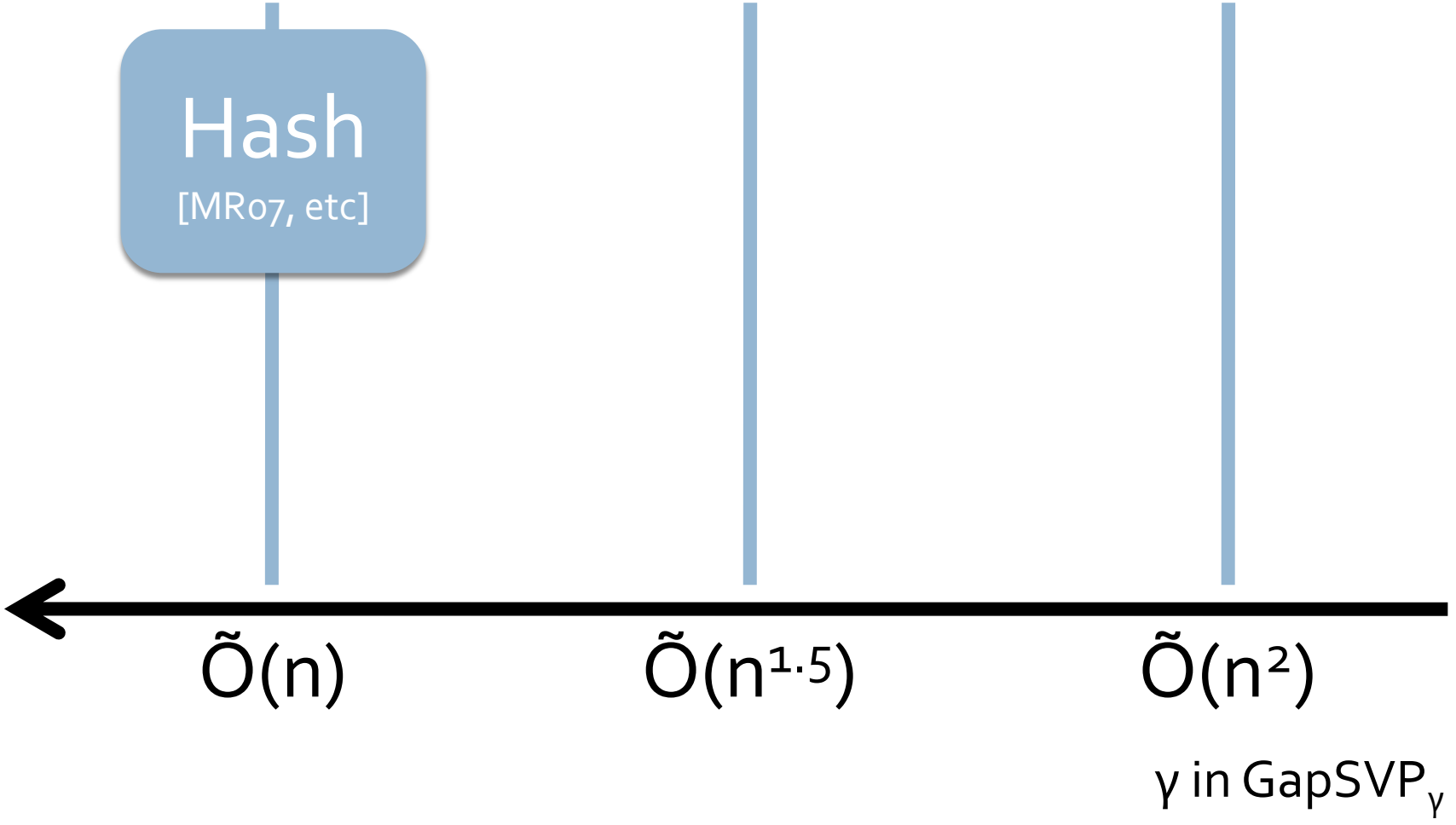
NO: $\lambda(L) > \gamma d$



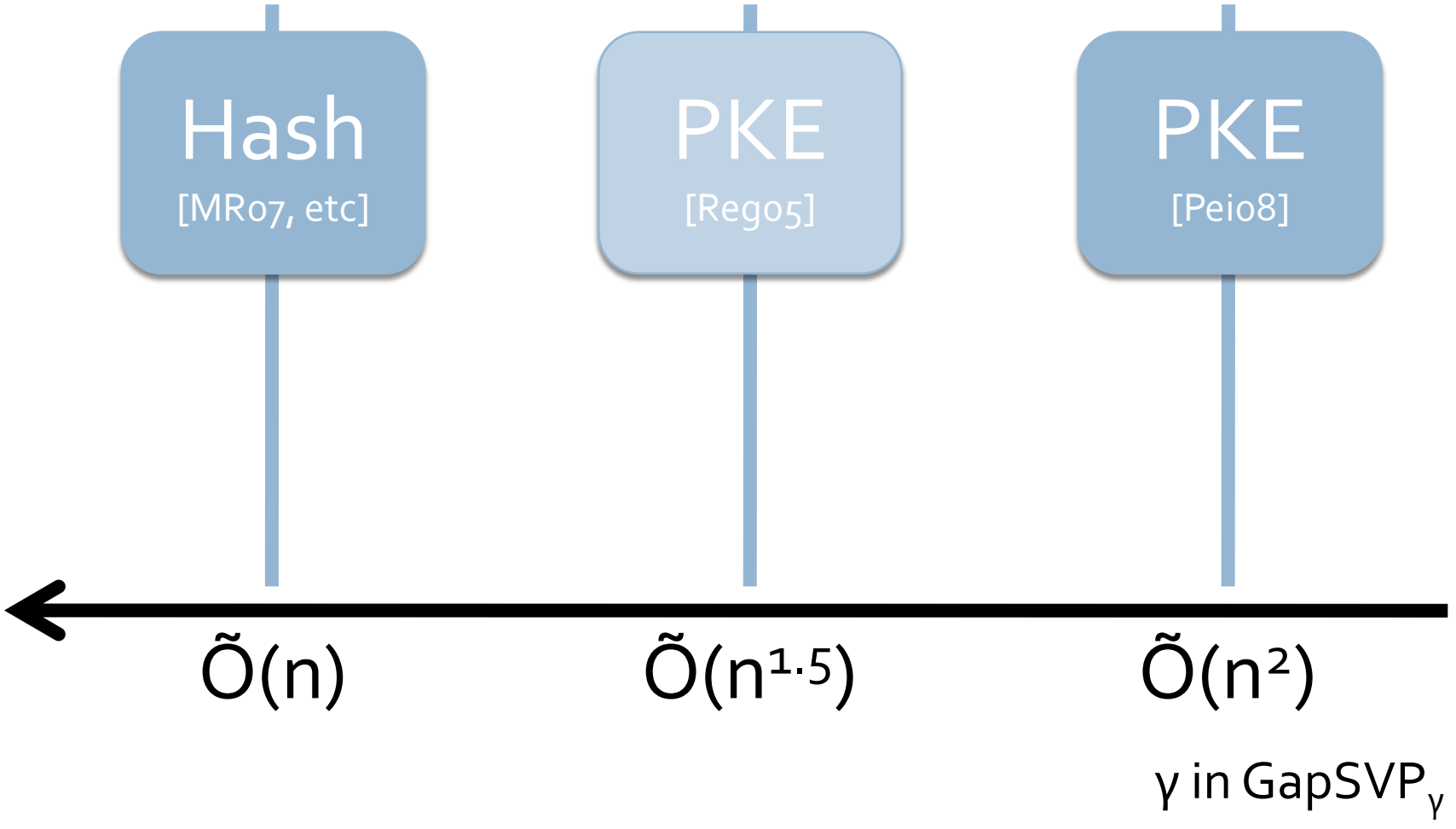
Schemes and Assumptions #1



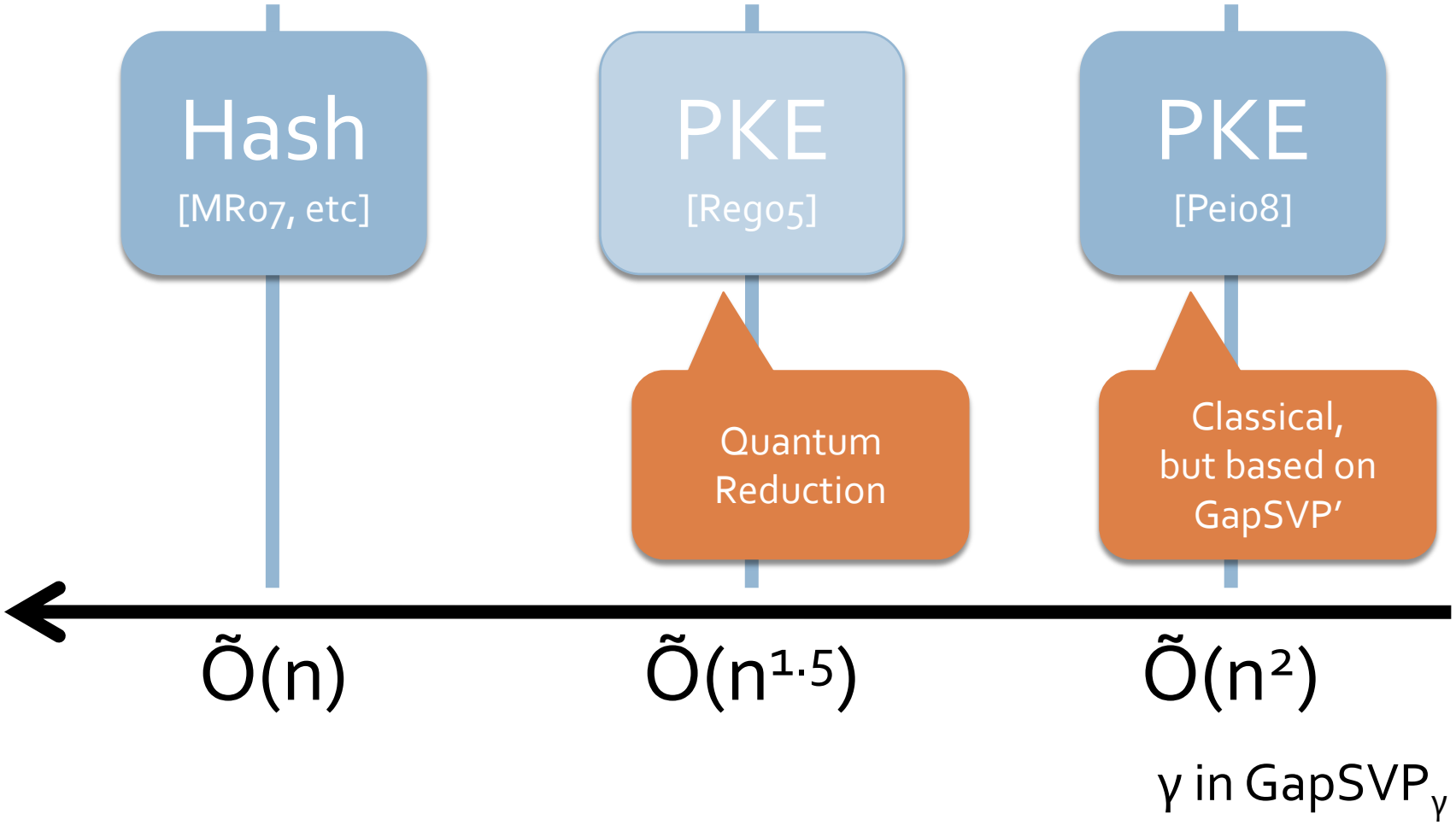
Schemes and Assumptions #1



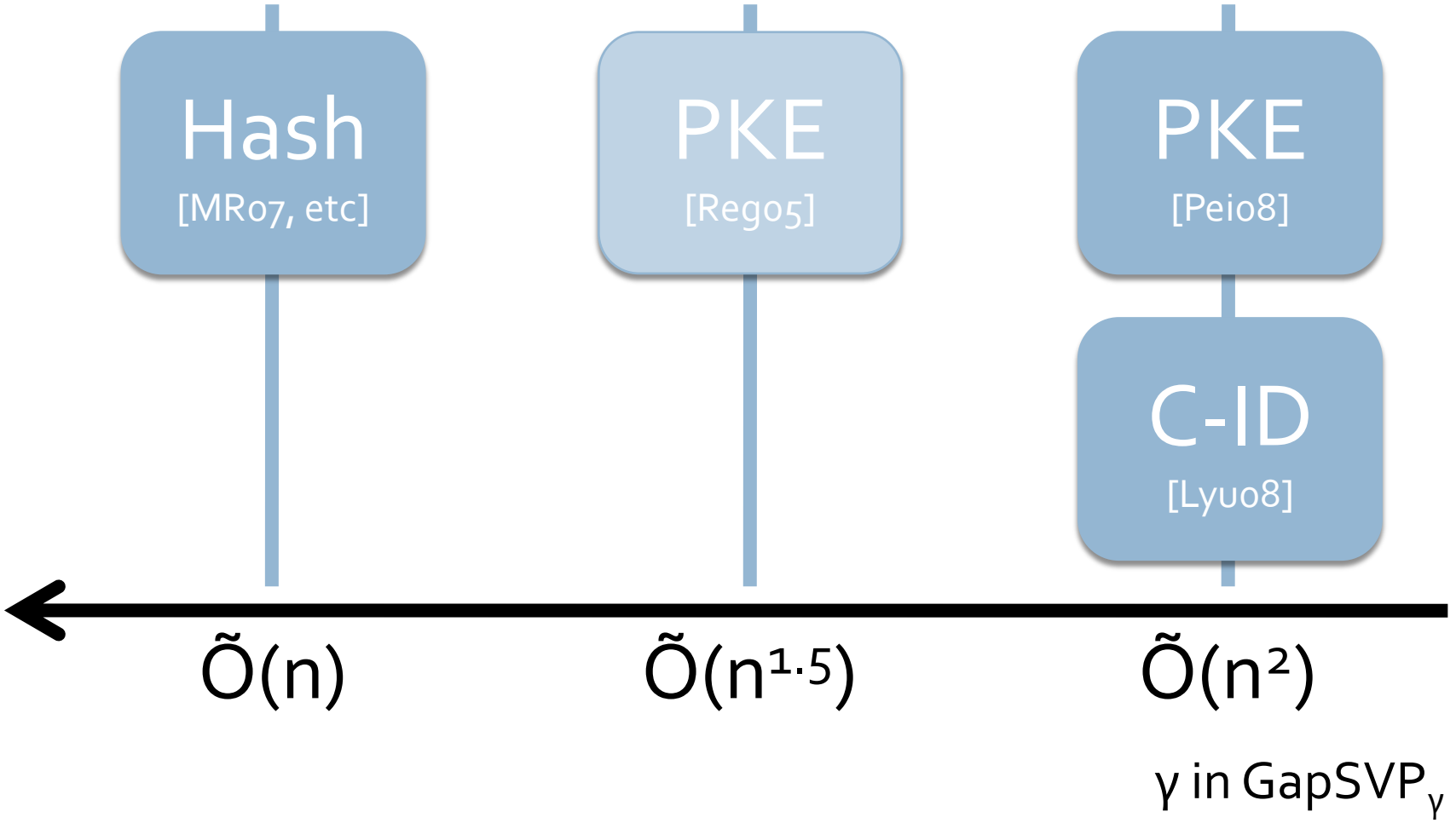
Schemes and Assumptions #1



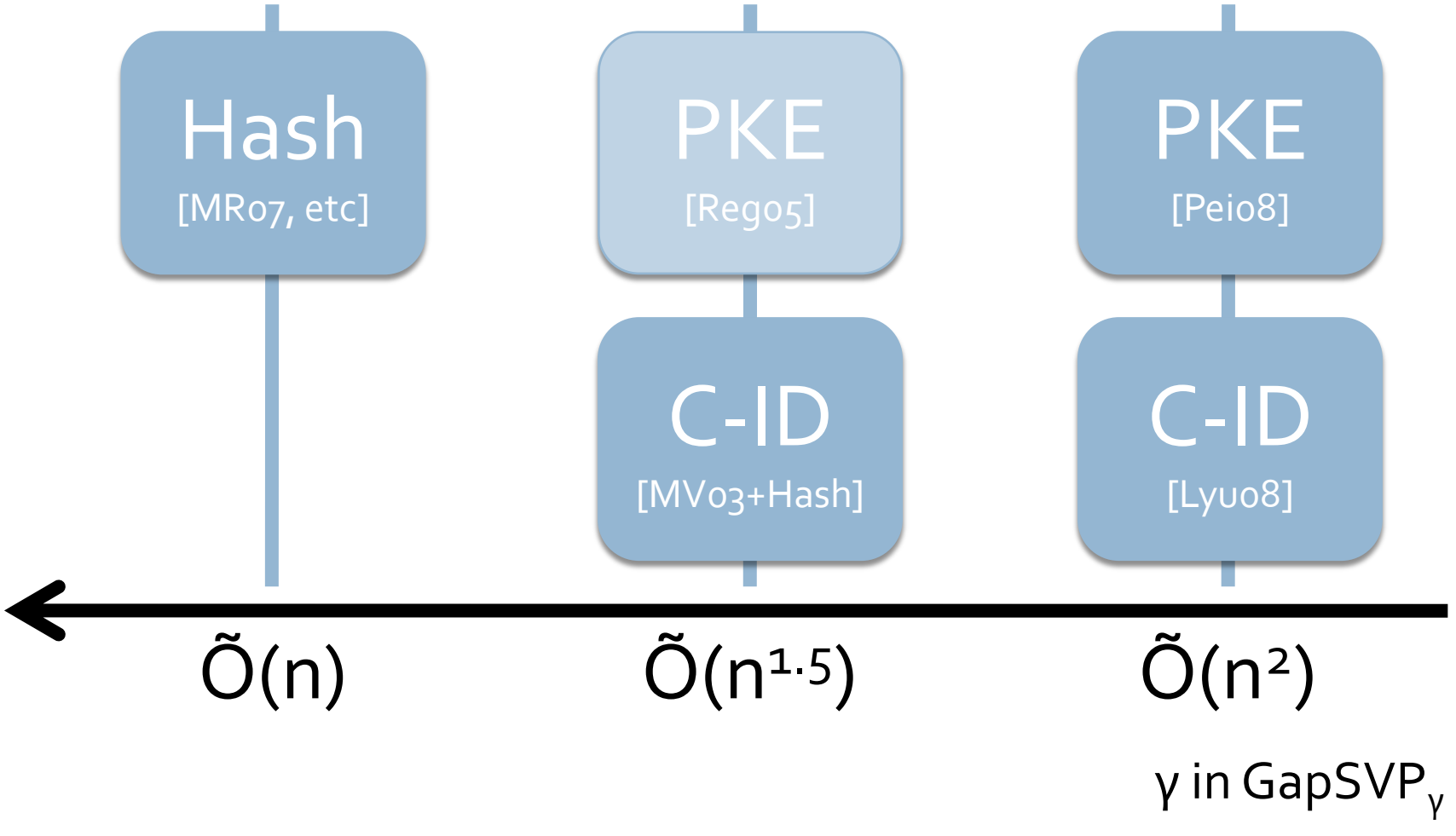
Schemes and Assumptions #1



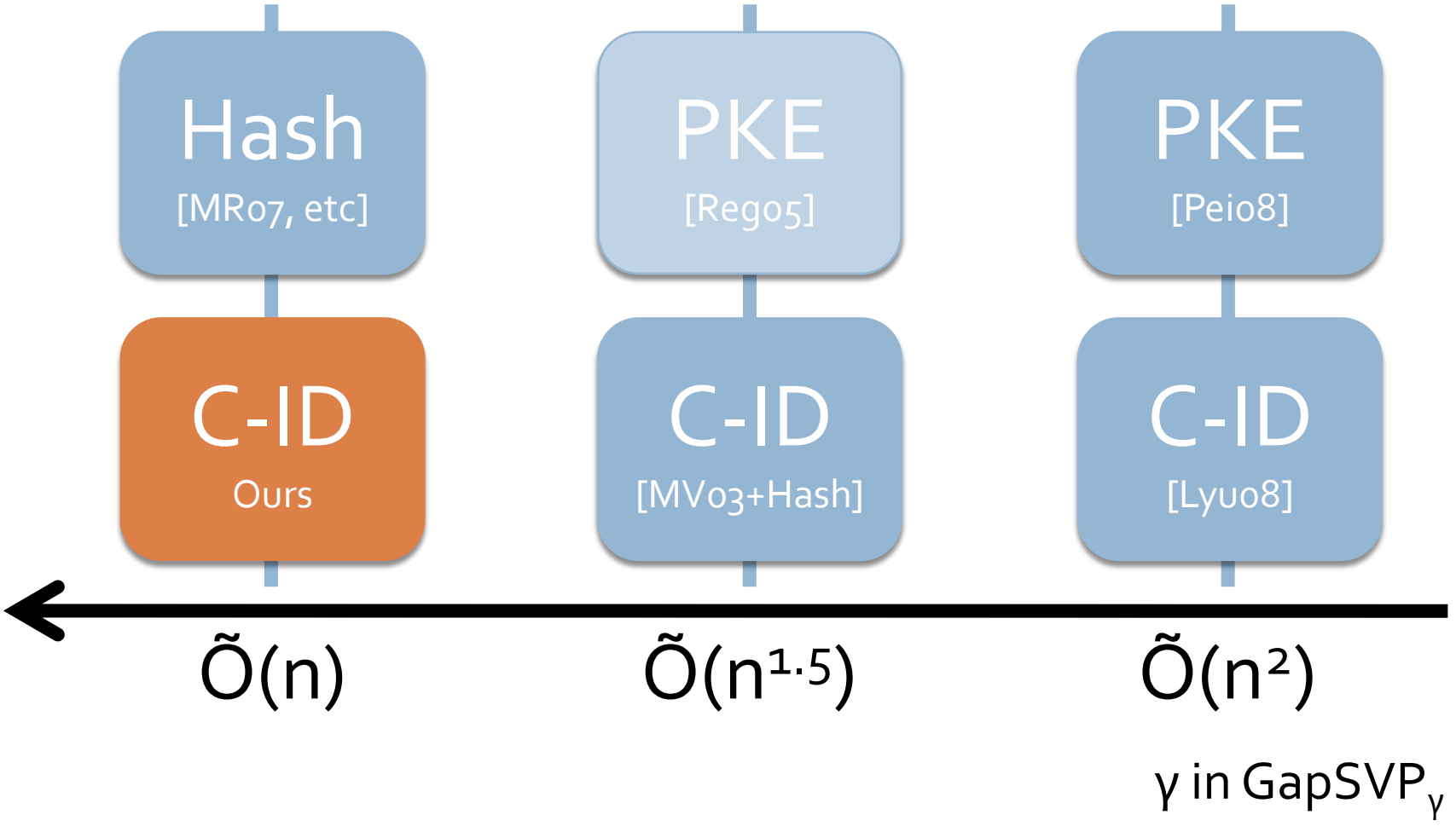
Schemes and Assumptions #1



Schemes and Assumptions #1



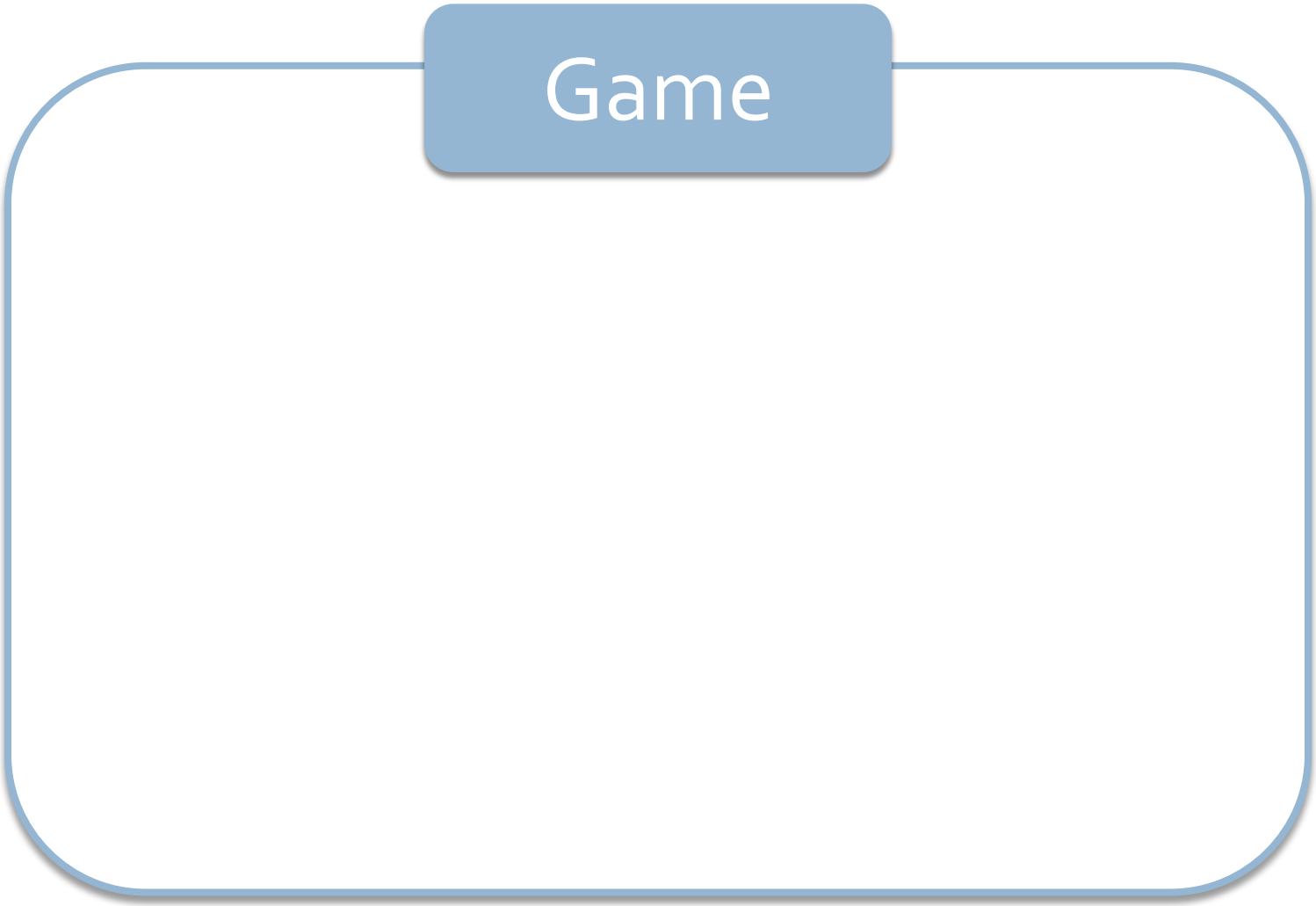
Schemes and Assumptions #1



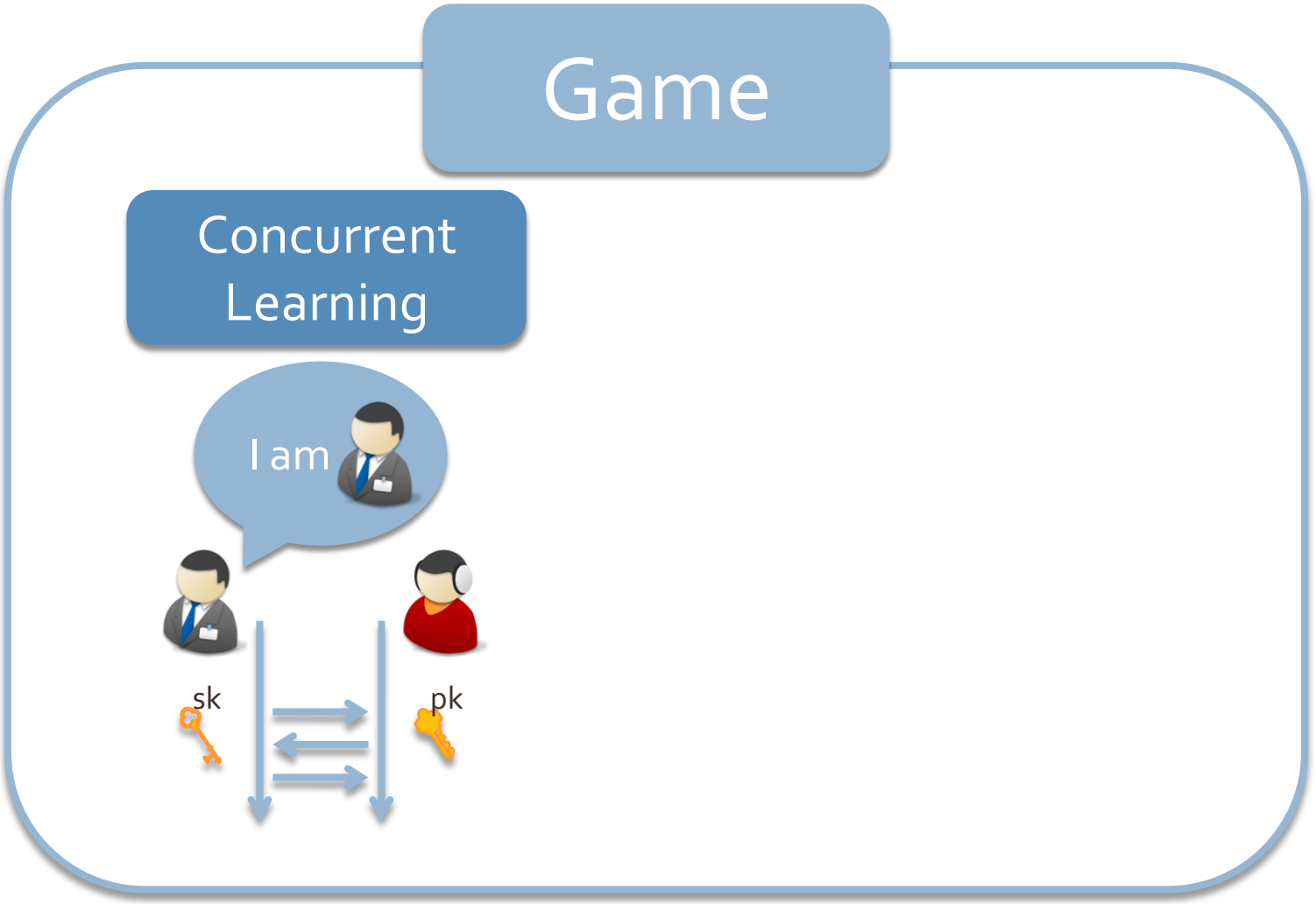
Agenda

- Background
- Strategy for C-ID
  - The Definition of C-ID
  - The Construction Strategy
  - Lattice-based Hash functions
  - A Bare Bone of Lattice-based C-ID
- Lyubashevsky's ID
- Ours (or Stern's ID)

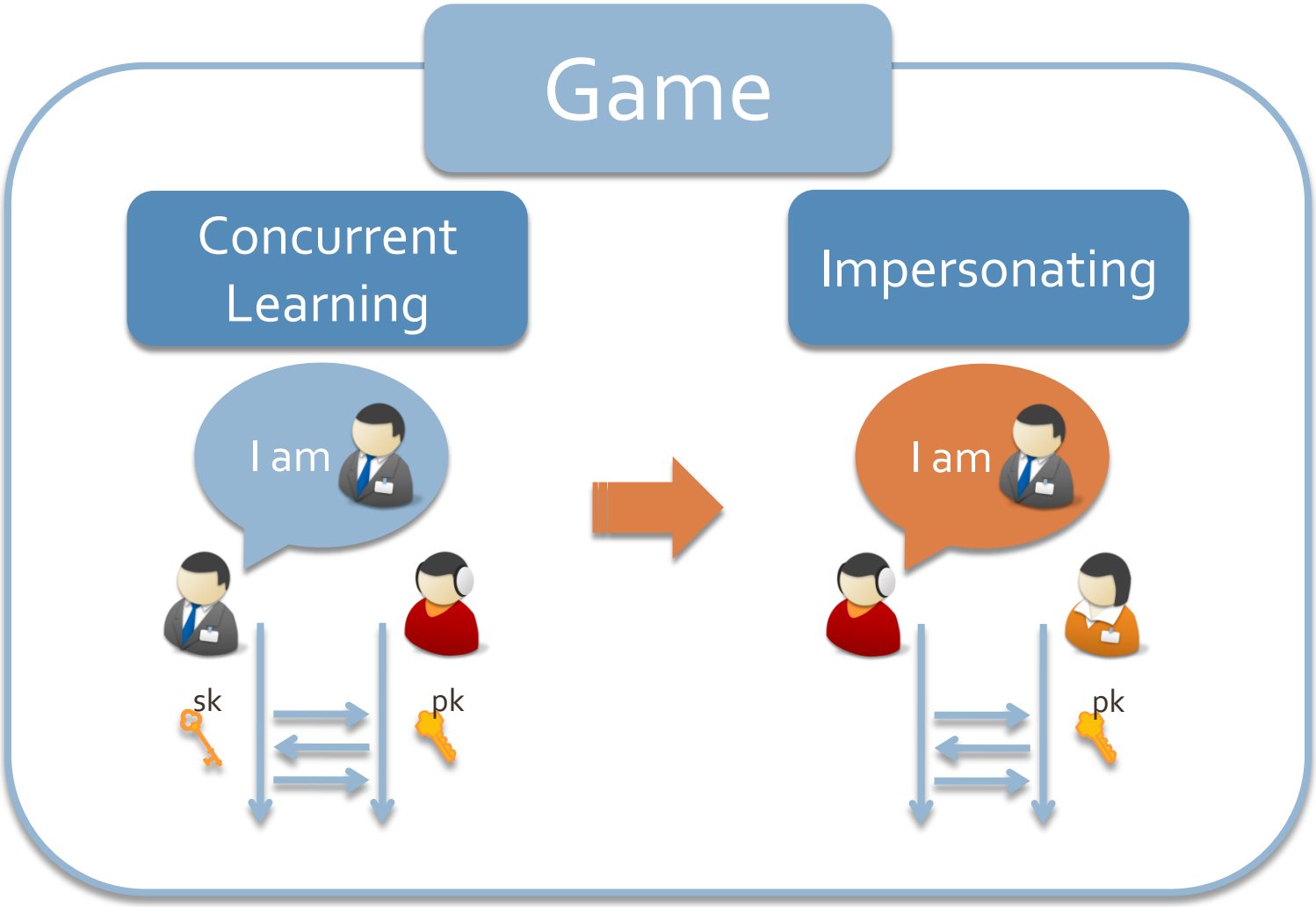
Definition of C-ID



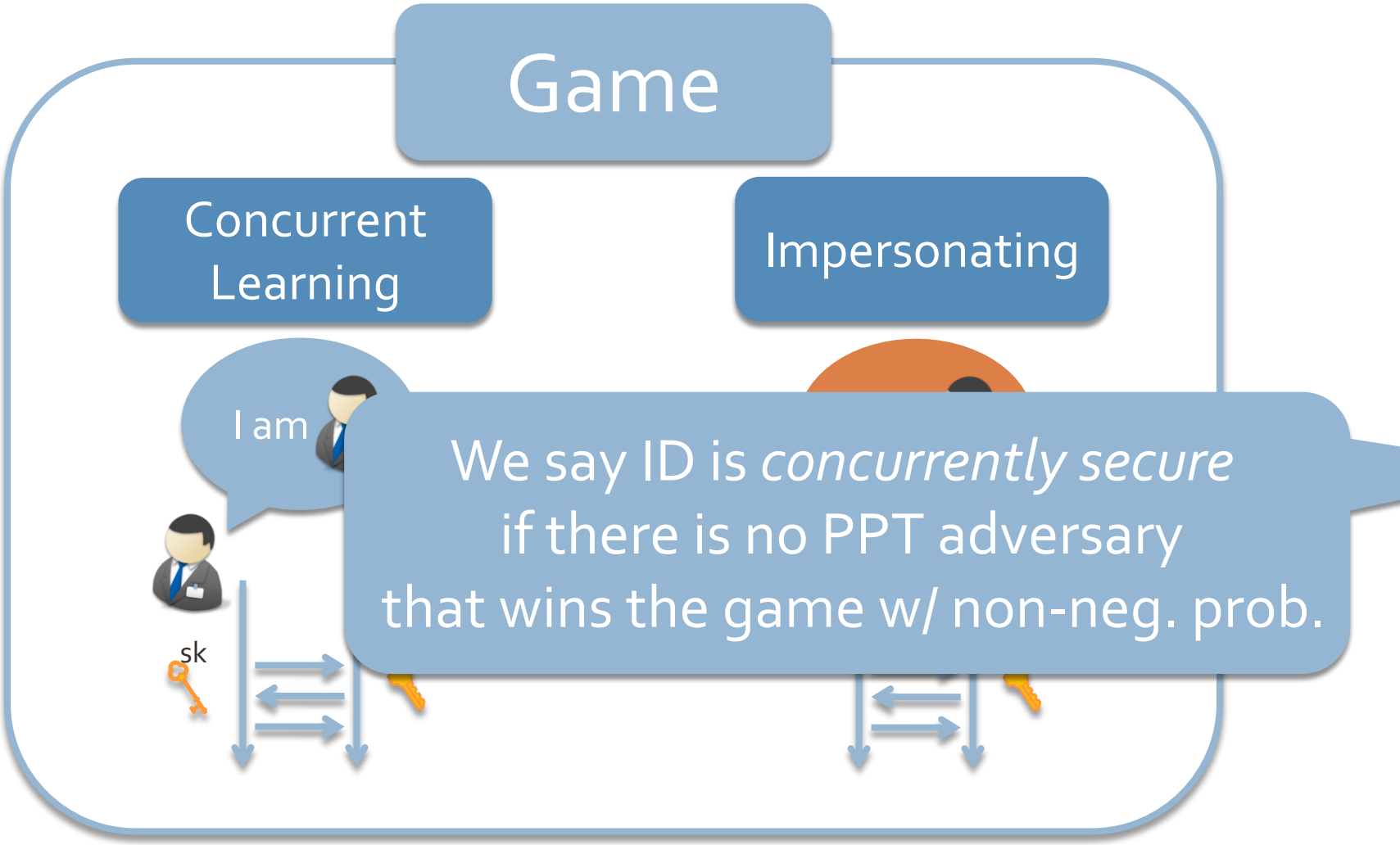
Definition of C-ID



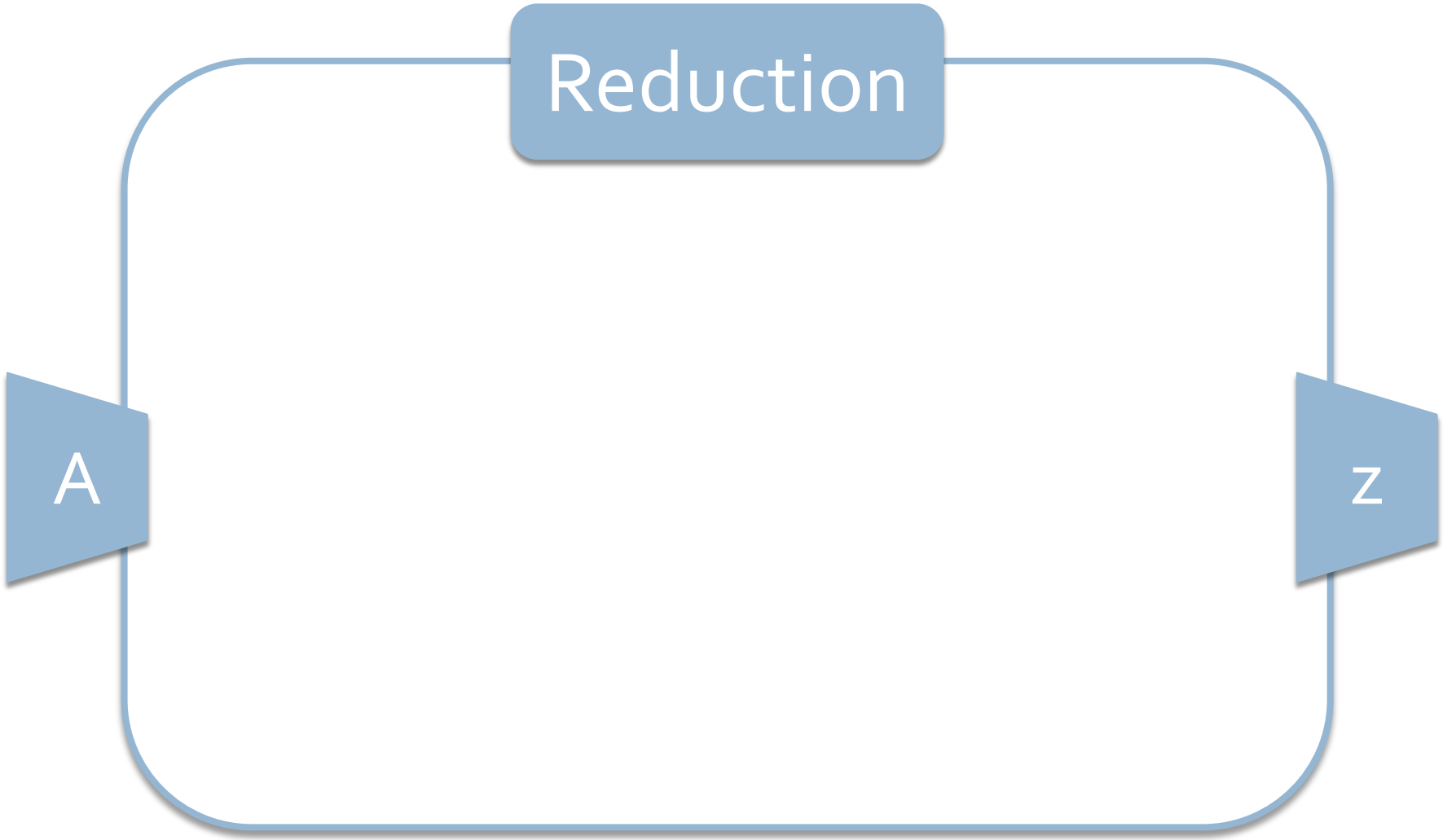
Definition of C-ID



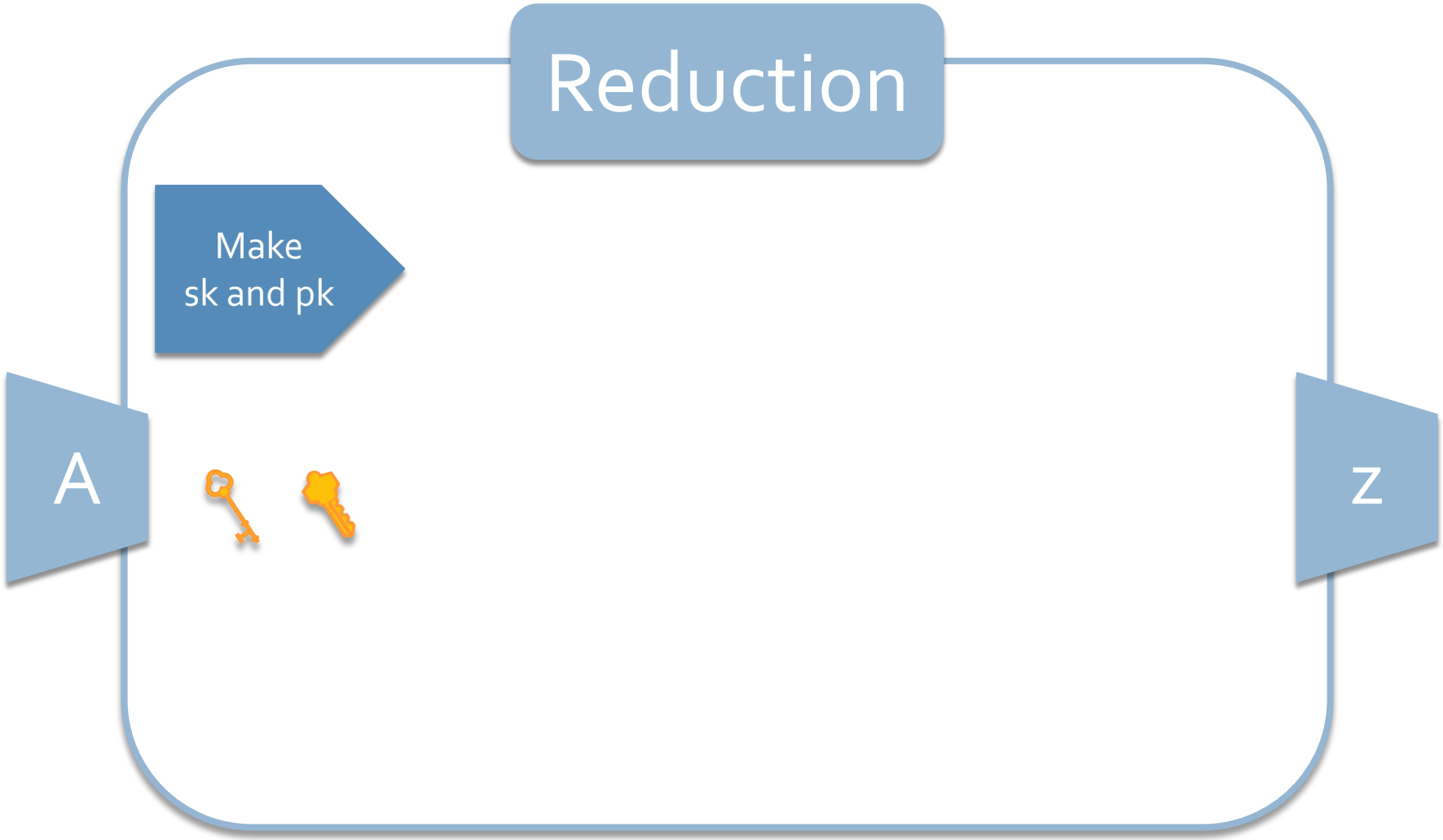
Definition of C-ID



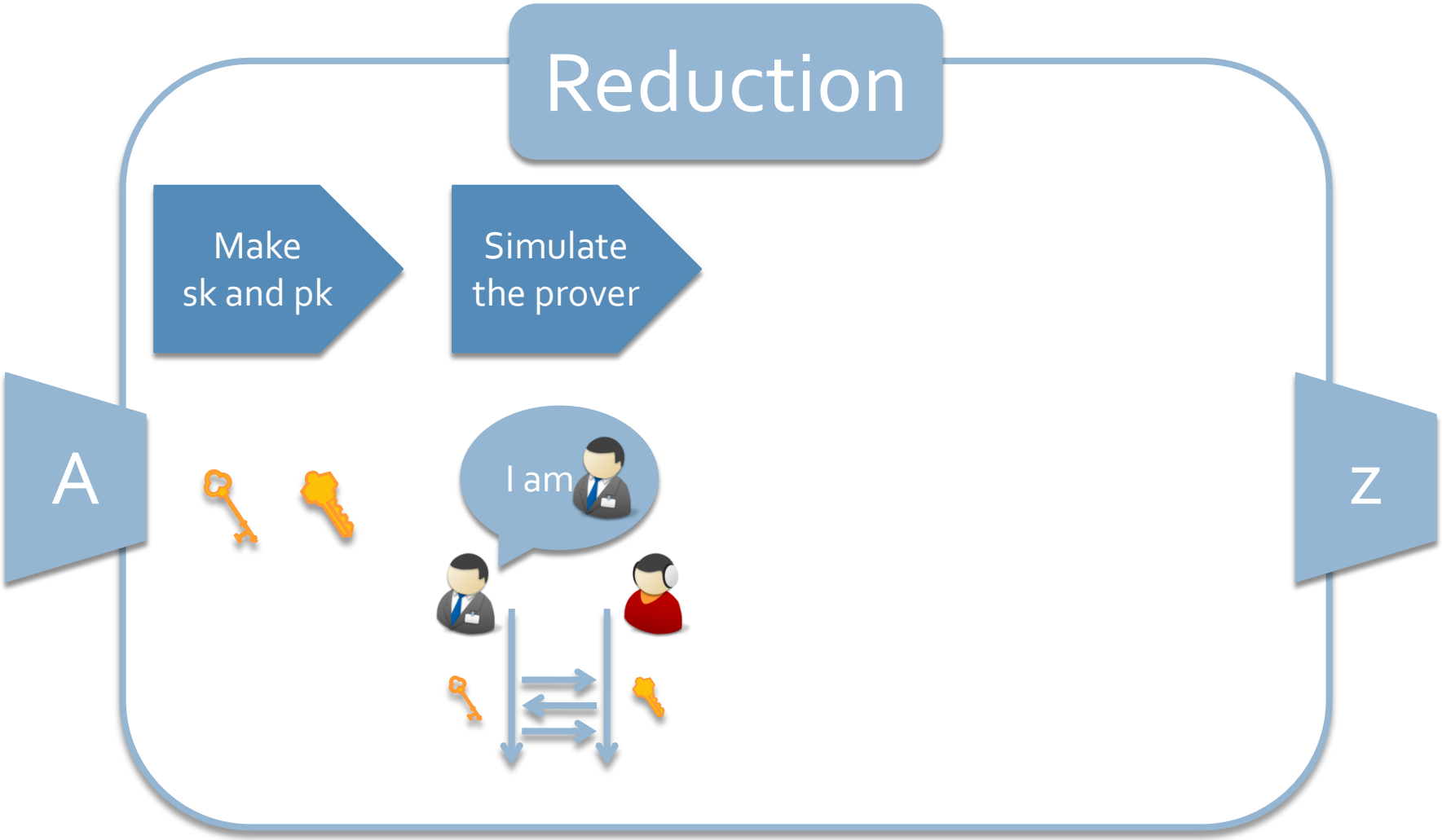
Main Strategy for C-IDs



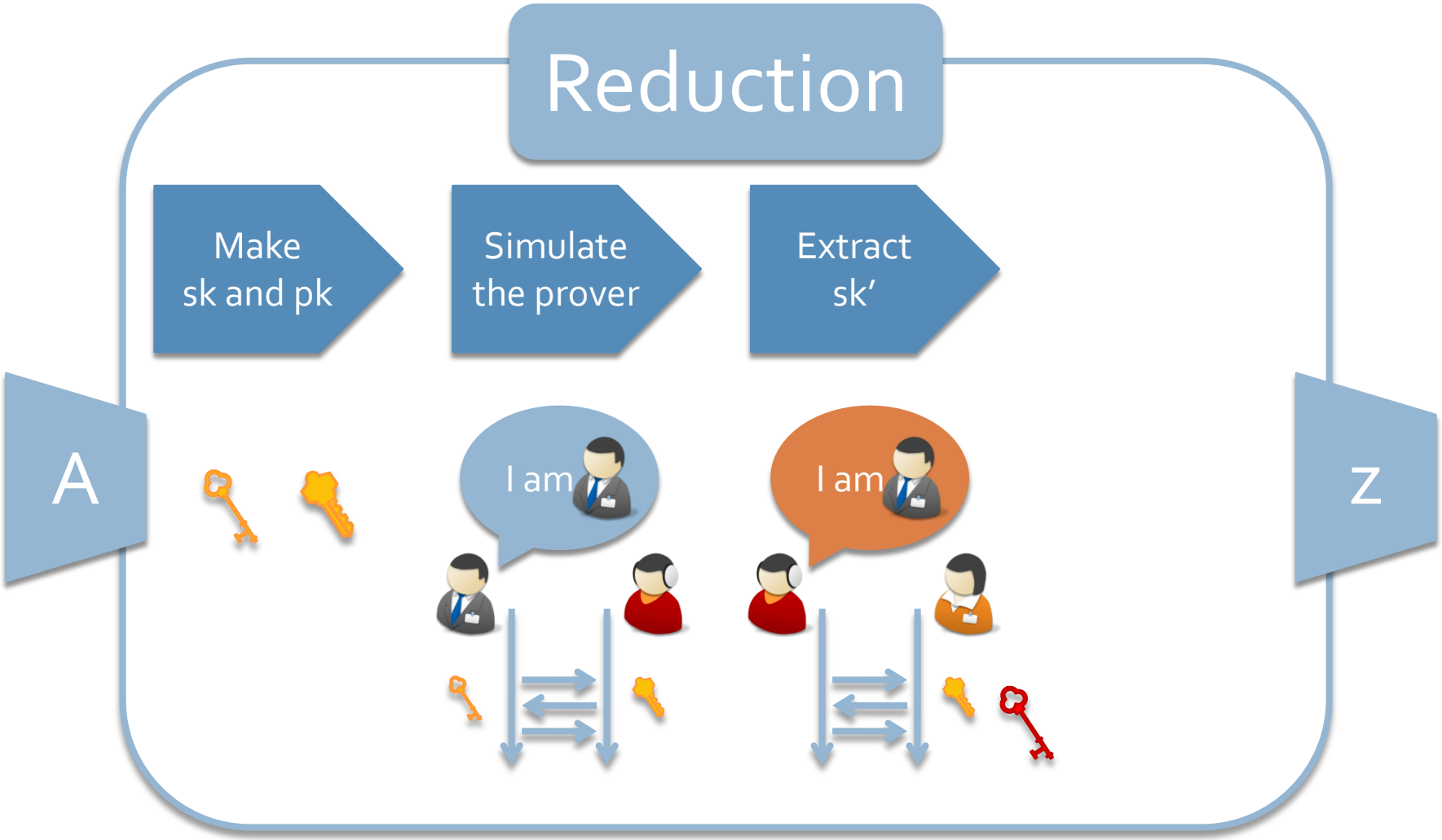
Main Strategy for C-IDs



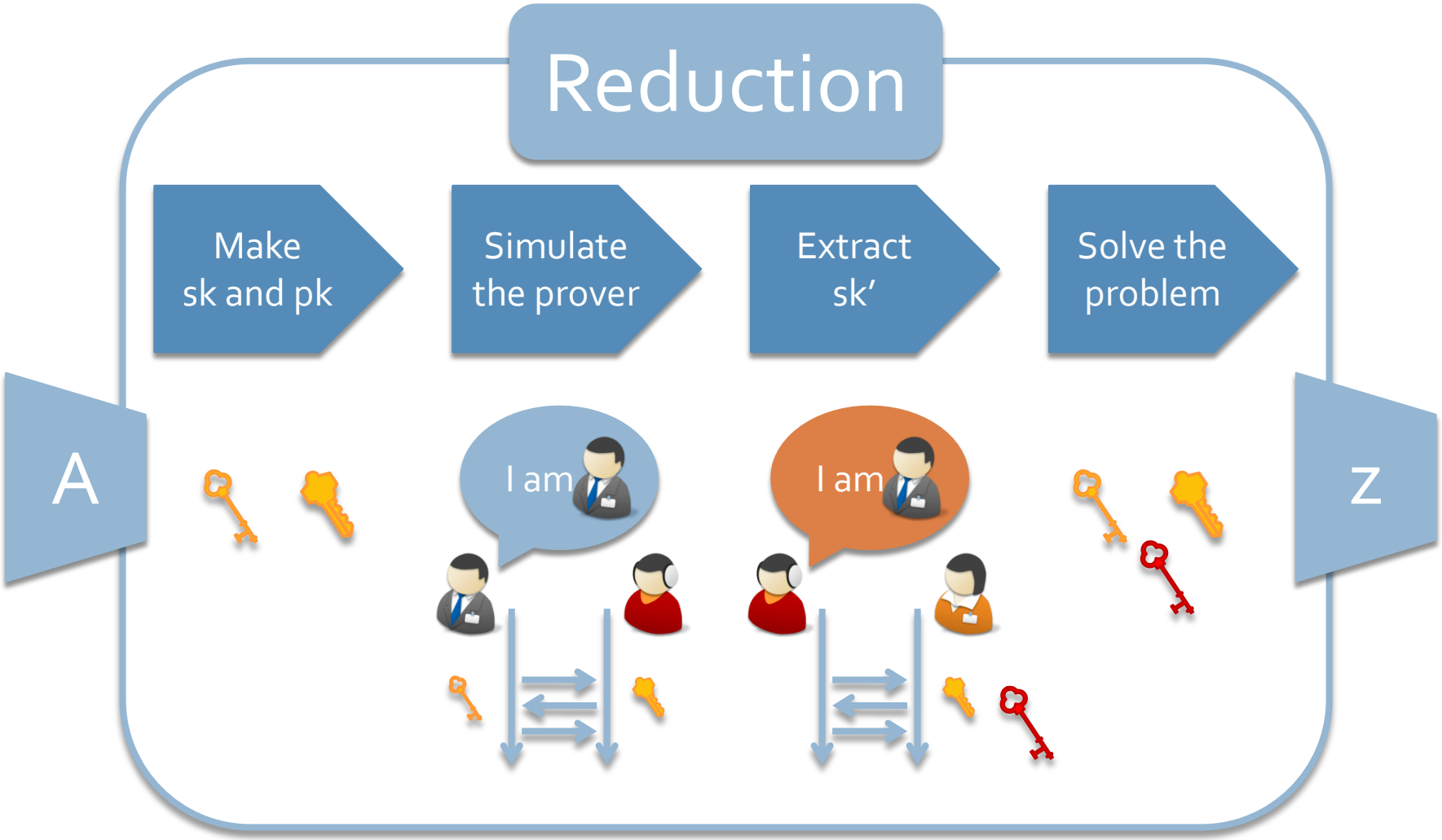
Main Strategy for C-IDs



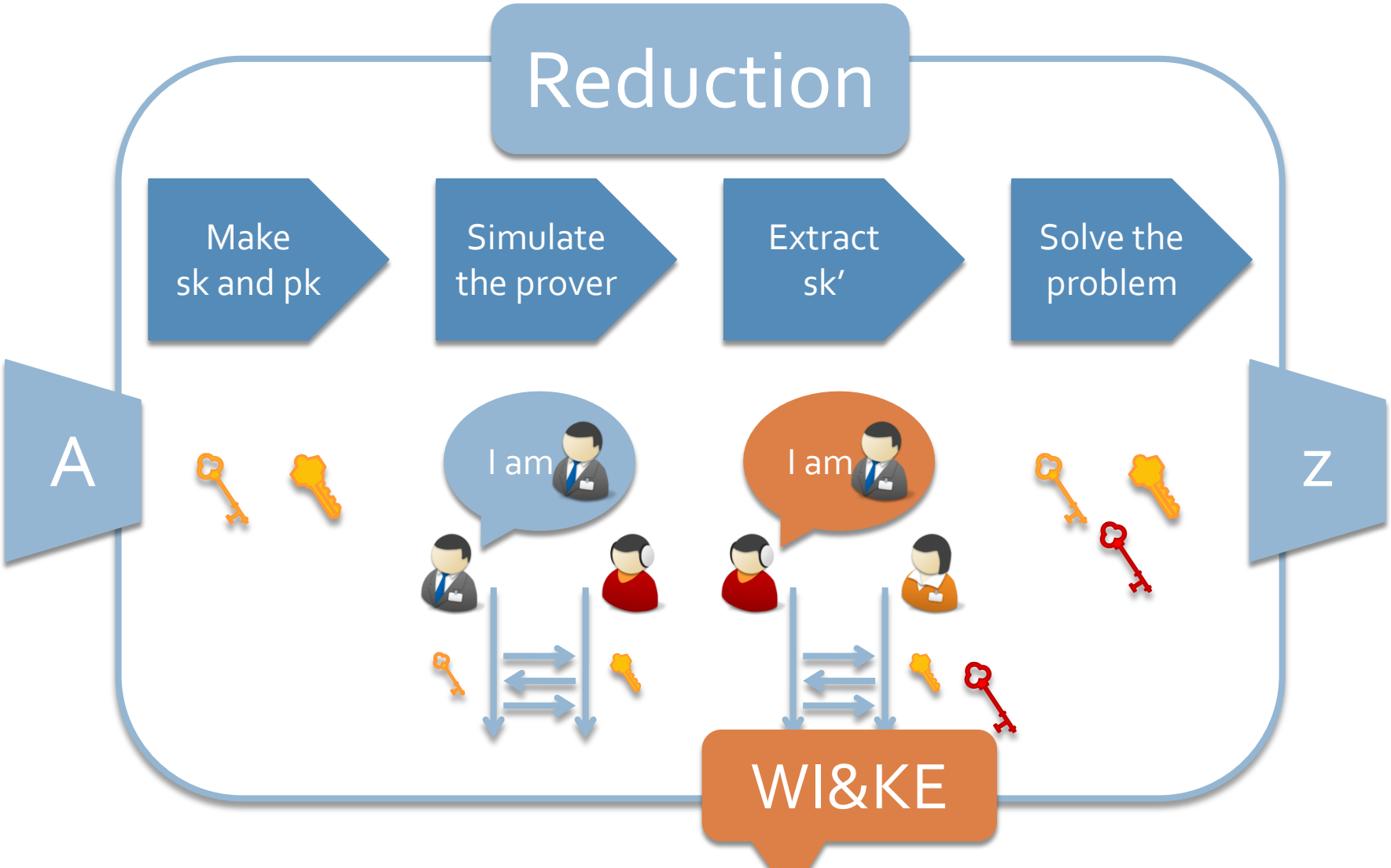
Main Strategy for C-IDs



Main Strategy for C-IDs



Main Strategy for C-IDs



Main Tool in IDs #1

Hash
[Ajt96,GGH96,…]

$$H = \{f_{\mathbf{A}}:\{0,1\}^m \longrightarrow \mathbb{Z}_q^{\,n} \mid \mathbf{A} \in \mathbb{Z}_q^{\,n \times m}\}$$
$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$$

$SIS_{q,m,\beta}$

Given $\mathbf{A} \in \mathbb{Z}_q^{\,n \times m}$,
find a vector $\mathbf{z} \in \mathbb{Z}^m - \{\mathbf{0}\}$
s.t. $\mathbf{A}\mathbf{z} = \mathbf{0} \bmod q$ and $\|\mathbf{z}\| < \beta$

Main Tool in IDs #1

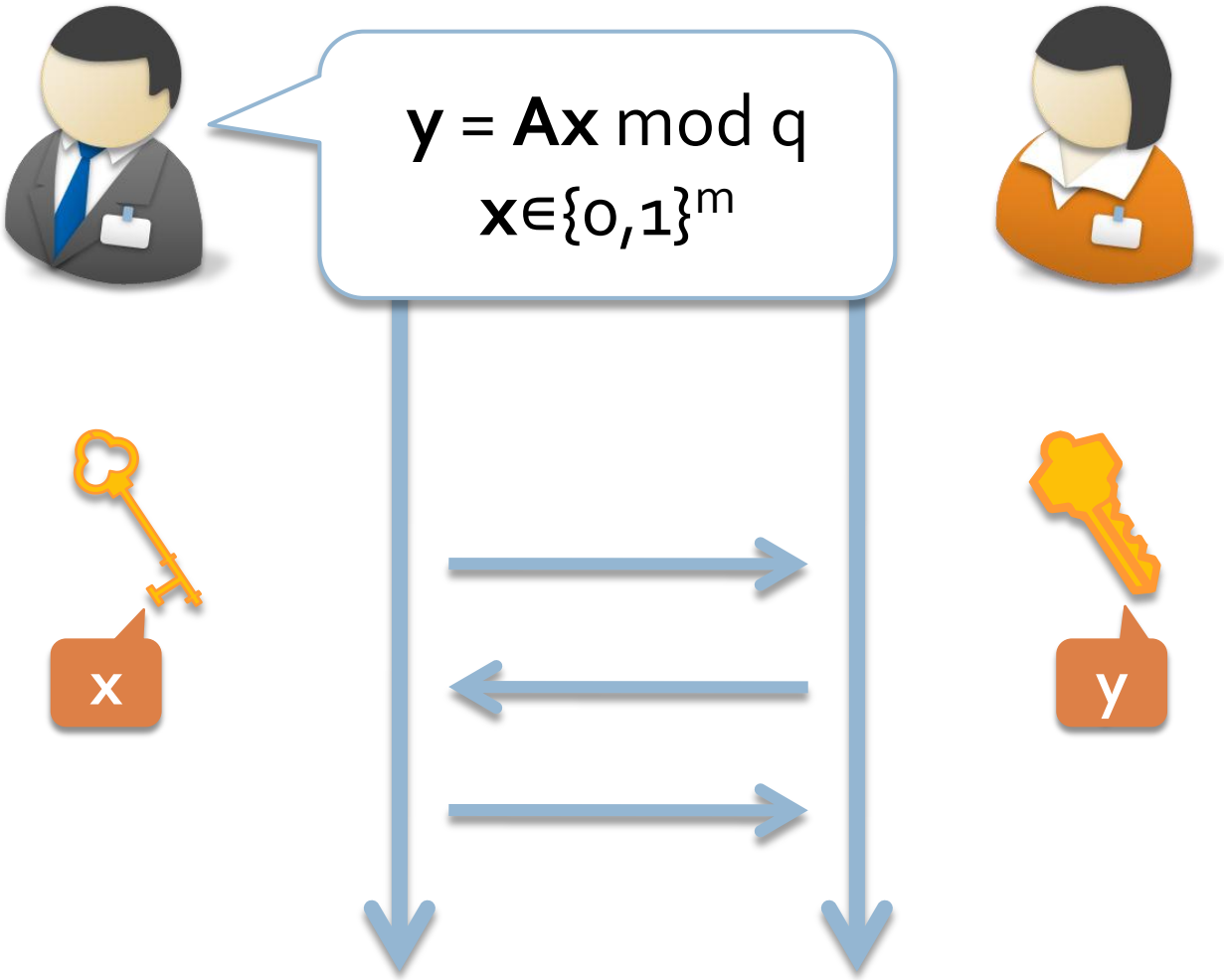
Hash
[Ajt96,GGH96,…]

$$H = \{f_{\mathbf{A}}:\{0,1\}^m \longrightarrow \mathbb{Z}_q^{\,n} \mid \mathbf{A} \in \mathbb{Z}_q^{\,n \times m}\}$$
$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$$

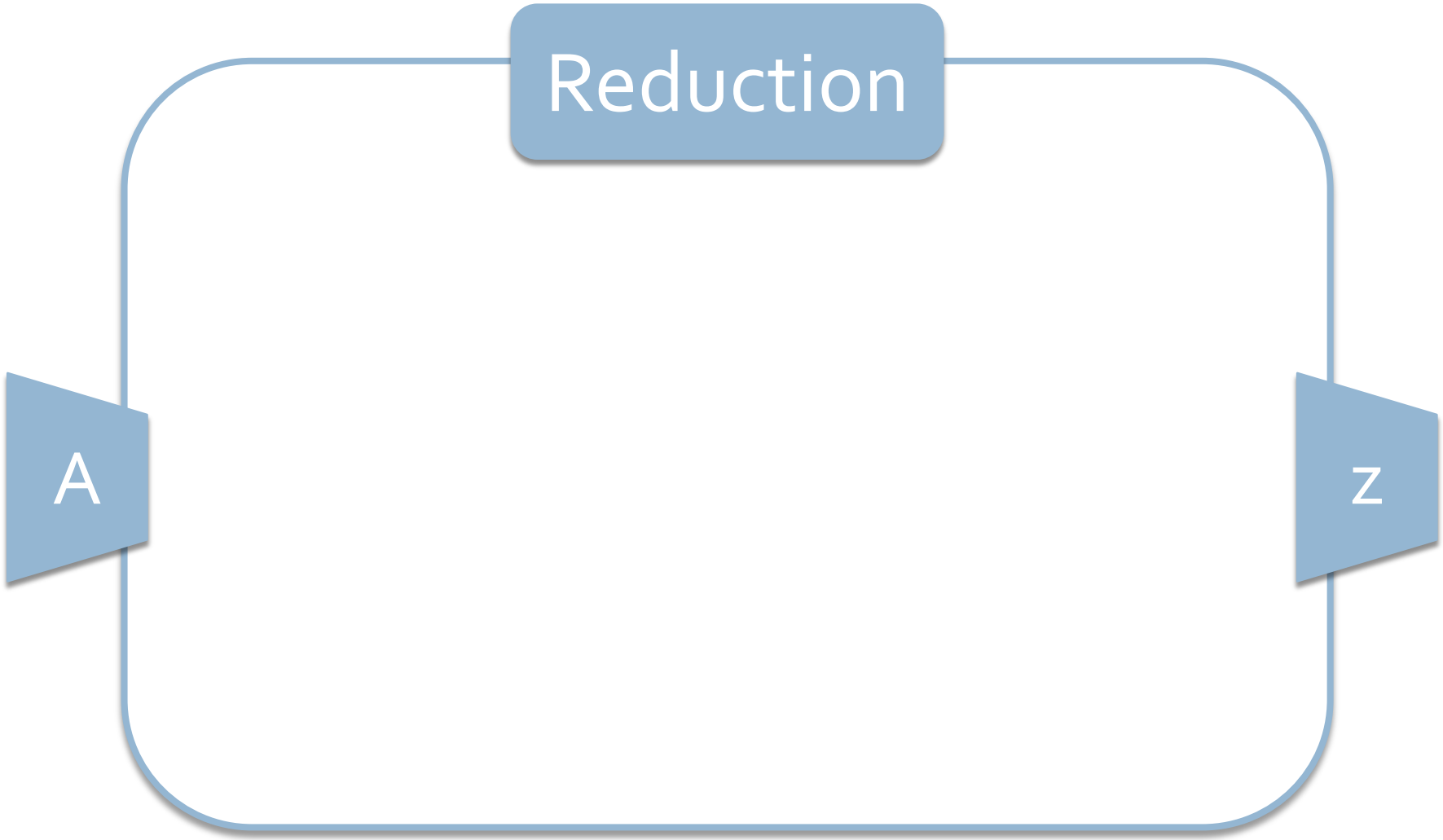
Thm
[Ajt96,MR07,…]

$$SIS_{q,m,\beta} \geqq_{a/w} GapSVP_{\tilde{O}(\beta\sqrt{n})}$$

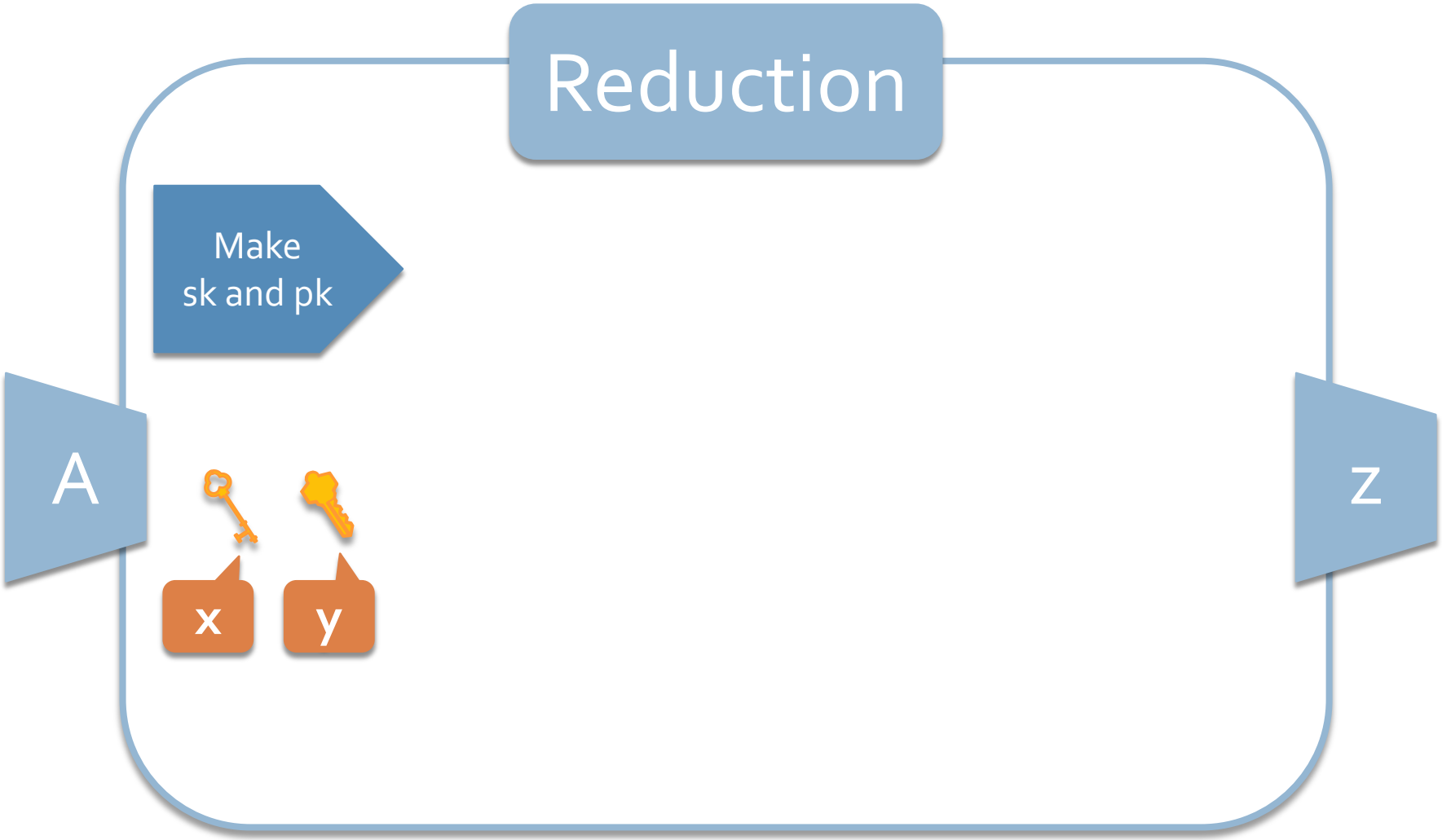
Bare Bone of C-IDs



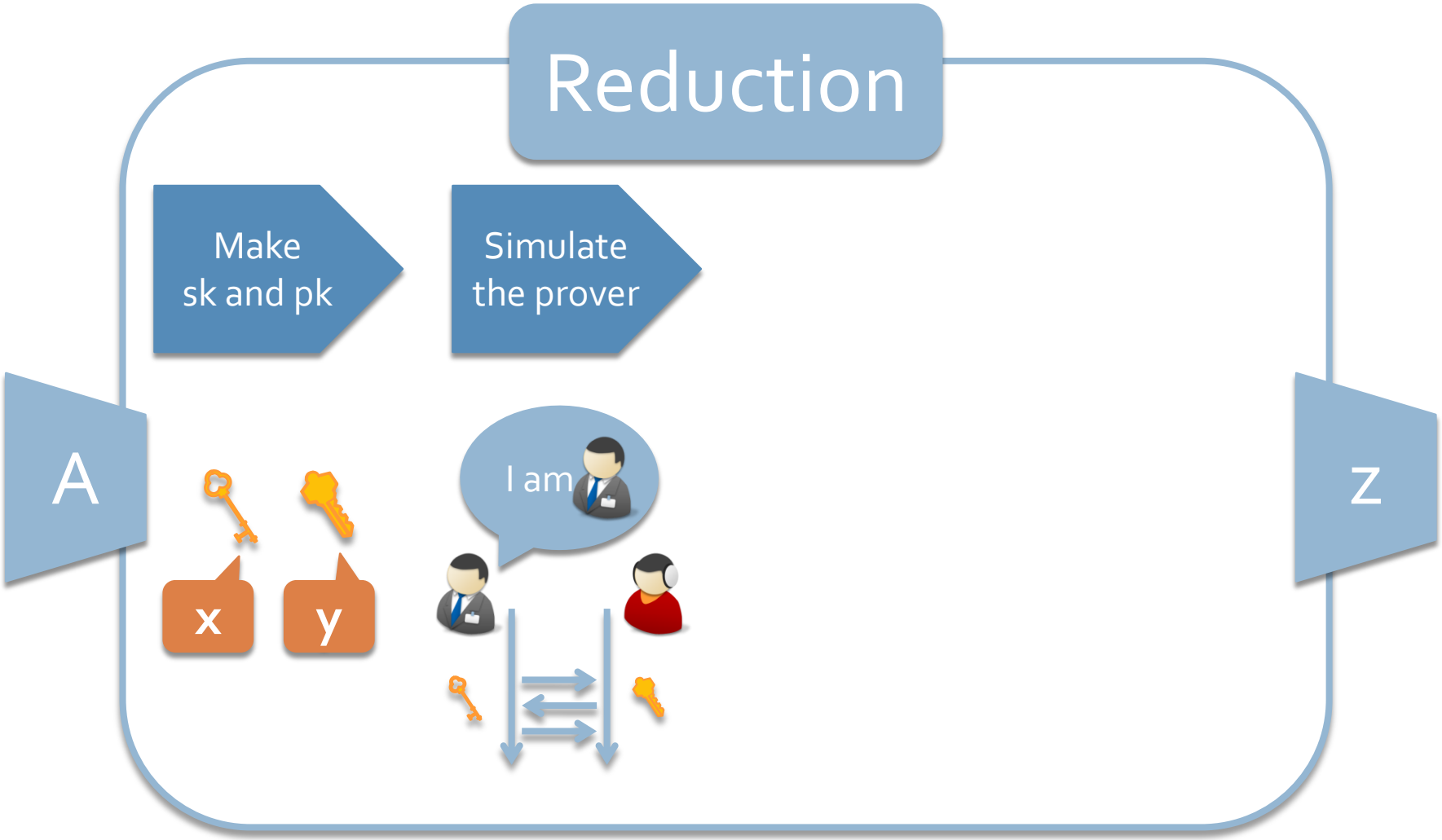
Main Strategy for C-IDs



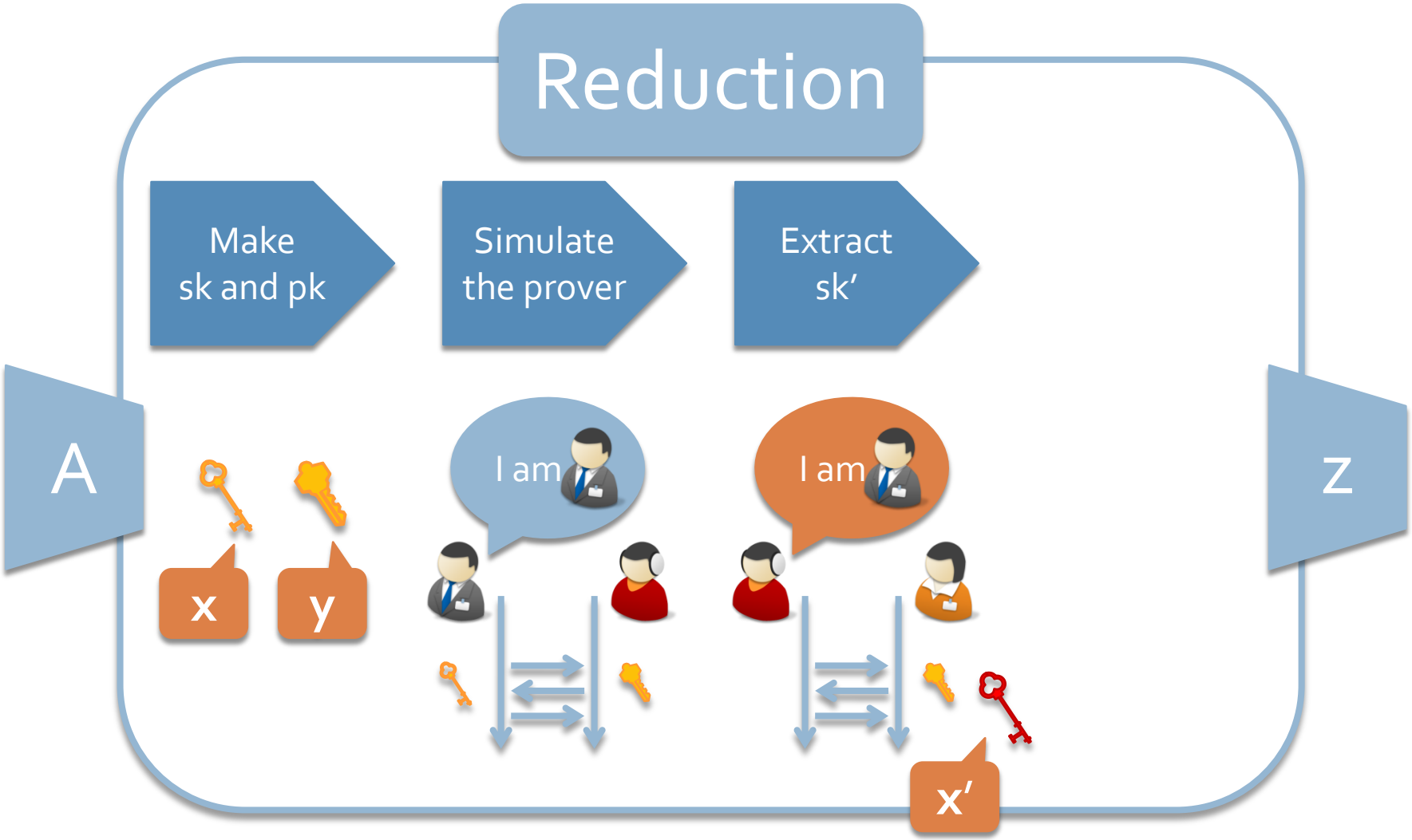
Main Strategy for C-IDs



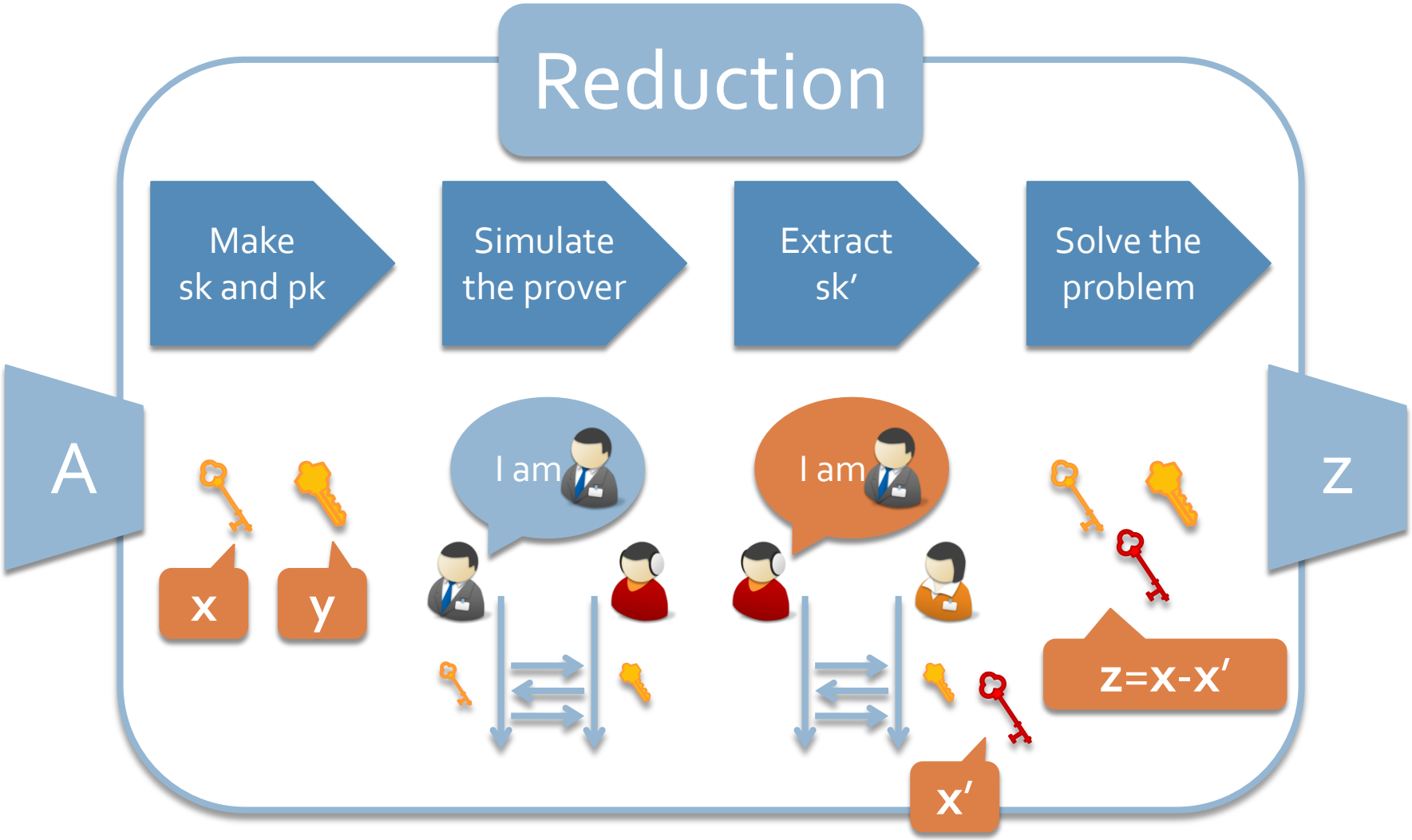
Main Strategy for C-IDs



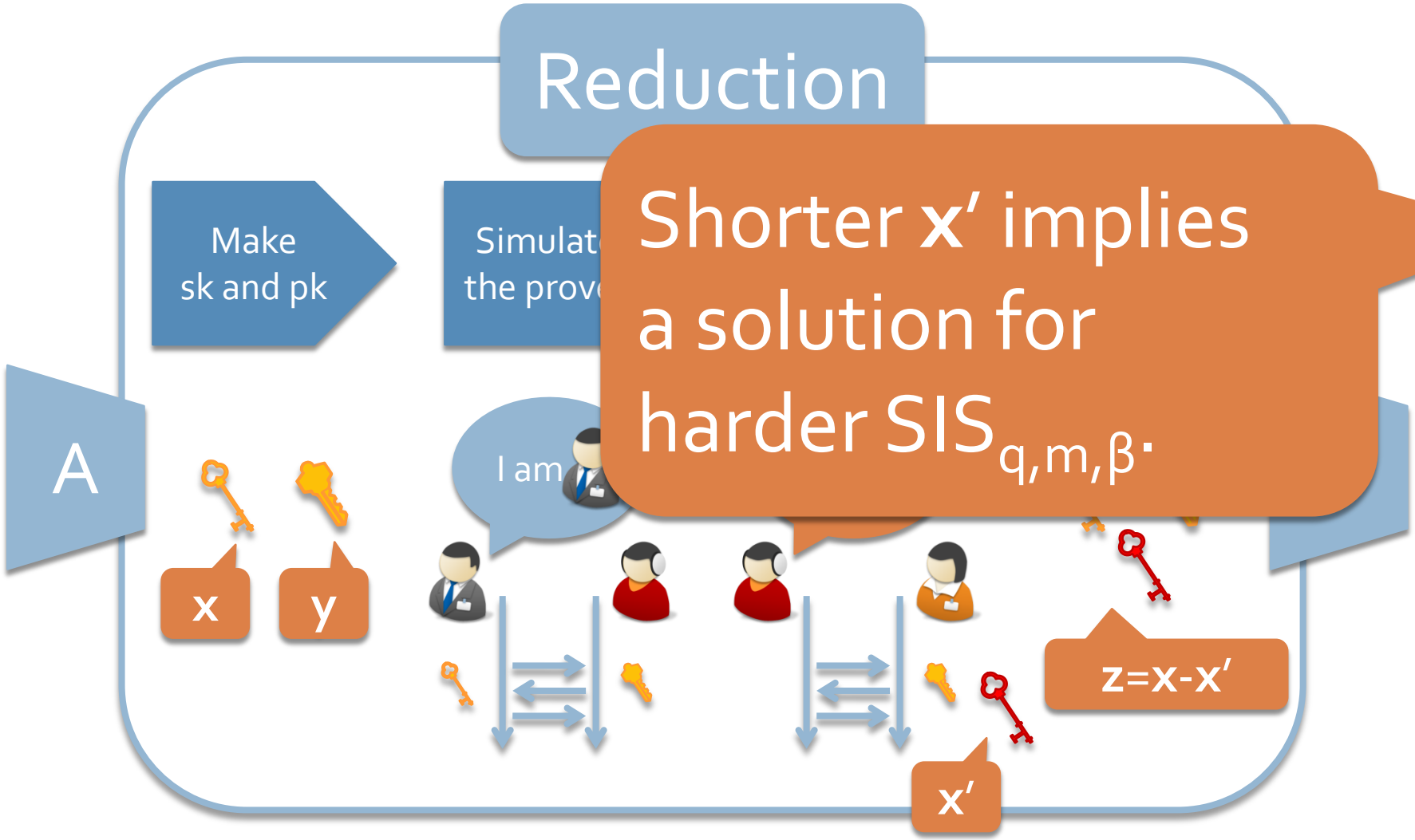
Main Strategy for C-IDs



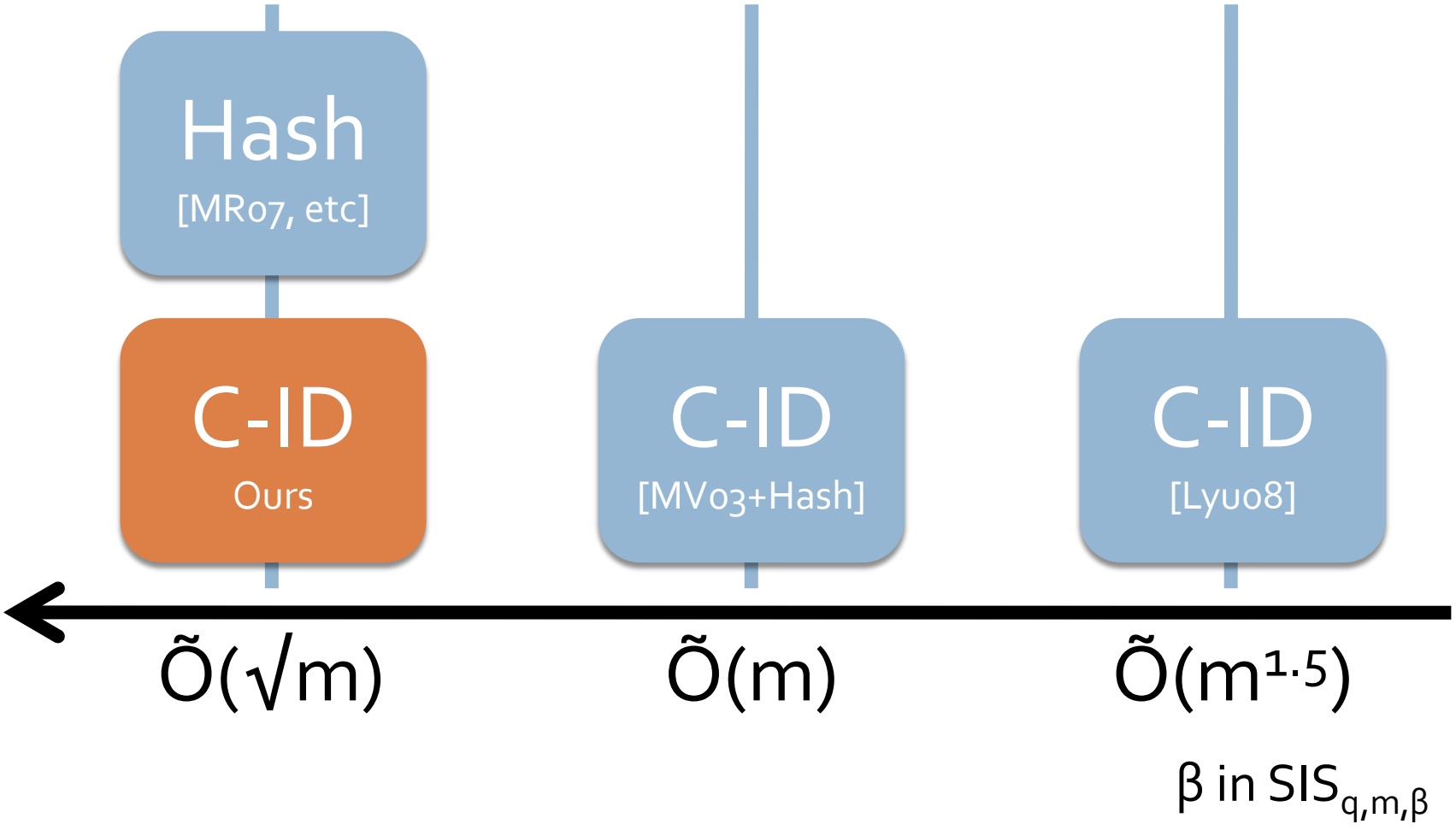
Main Strategy for C-IDs



Main Strategy for C-IDs



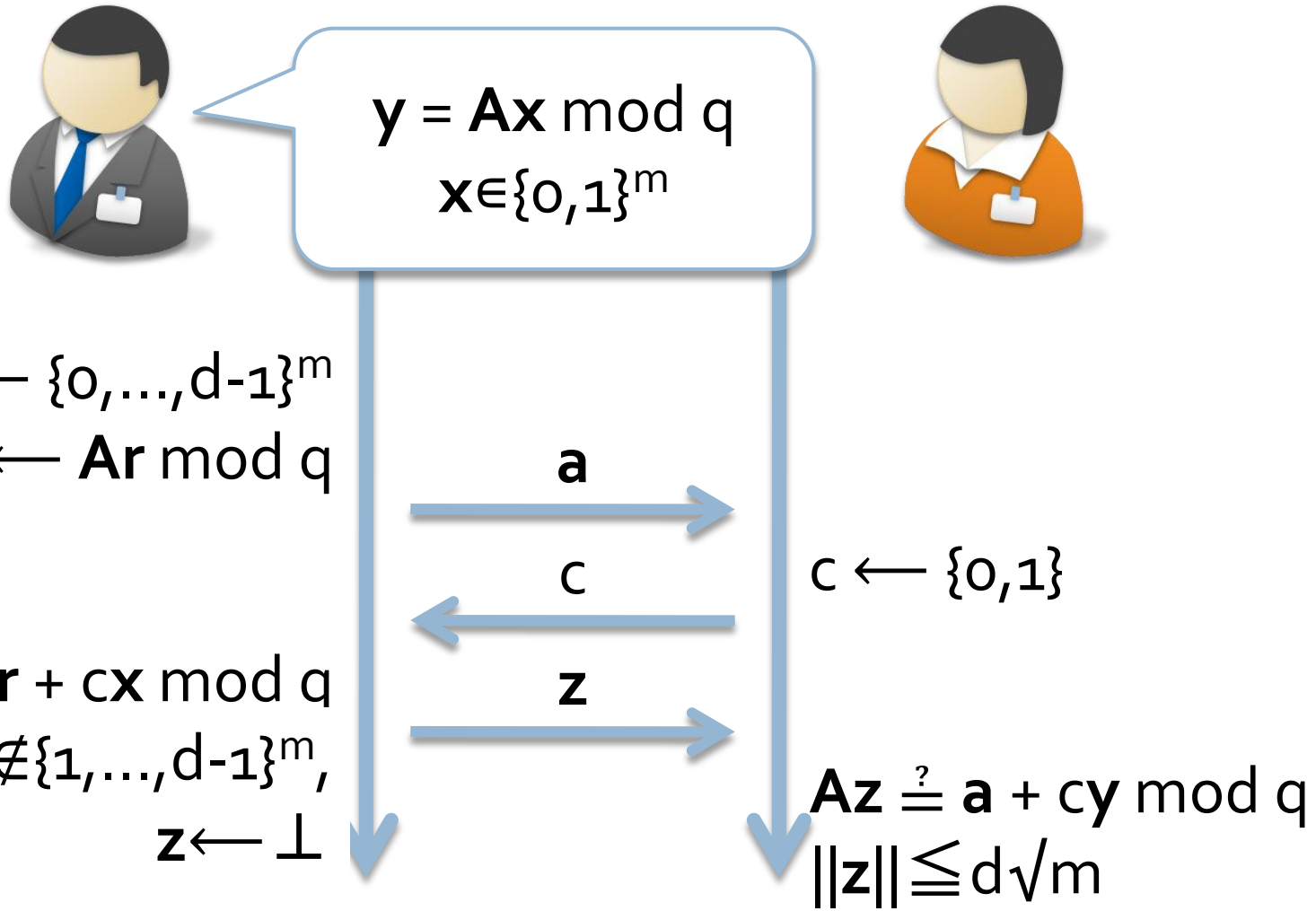
Schemes and Assumptions #2



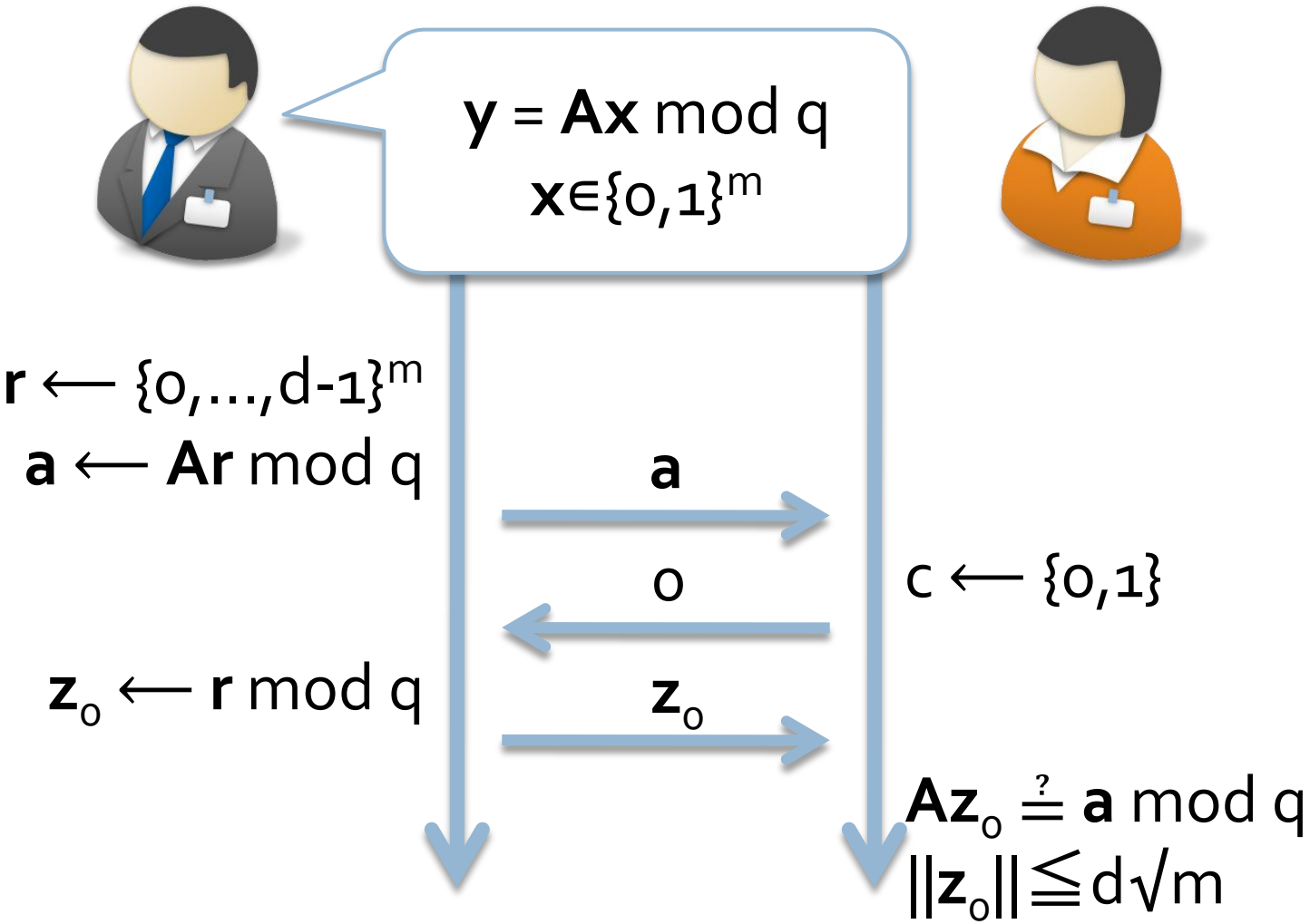
Agenda

- Background
- Strategy for C-ID
- Lyubashevsky's ID
  - Number-Theoretic ID
  - Lyubashevsky's ID
  - The Factor β is Large
- Ours (or Stern's ID)

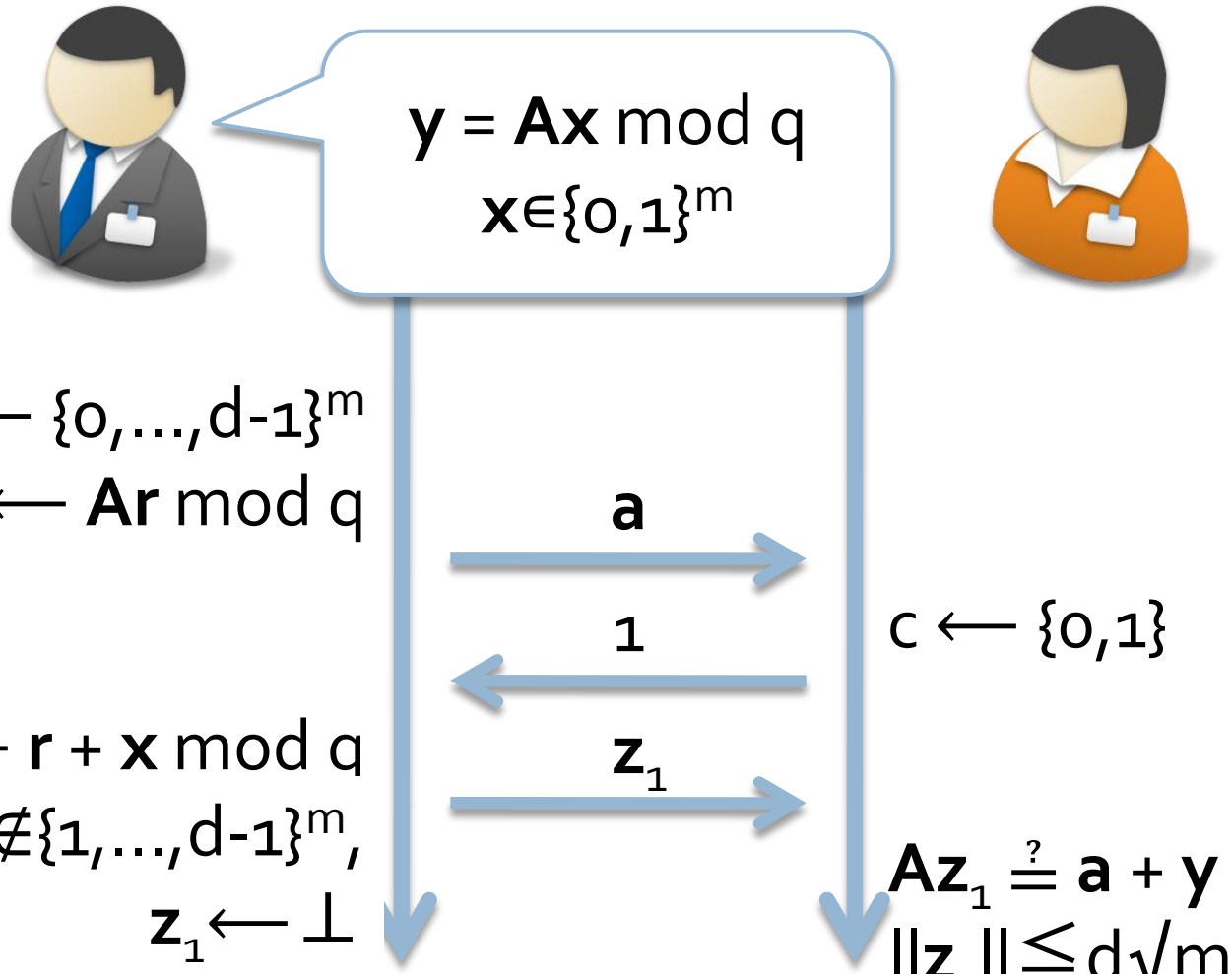
Lyubashevsky's ID [Lyu08]



Lyubashevsky's ID



Lyubashevsky's ID



Lyubashevsky's ID

$\mathbf{y} = \mathbf{A}\mathbf{x} \bmod q$
$\mathbf{x} \in \{0,1\}^m$

$\mathbf{r} \longleftarrow \{0,\ldots,d-1\}^m$
$\mathbf{a} \longleftarrow \mathbf{A}\mathbf{r} \bmod q$

[Lyu08]:
This protocol is WI.
Parallelized ver. works well.

$\mathbf{z} \longleftarrow \mathbf{r} + c\mathbf{x} \bmod q$
if $\mathbf{z} \notin \{1,\ldots,d-1\}^m$,
$\mathbf{z} \longleftarrow \perp$

$\mathbf{z}$

$\mathbf{A}\mathbf{z} \stackrel{?}{=} \mathbf{a} + c\mathbf{y} \bmod q$
$\|\mathbf{z}\| \leqq d\sqrt{m}$

Lyubashevsky's ID

$\mathbf{y} = \mathbf{A}\mathbf{x} \bmod$

$\mathbf{x} \in \{0,1\}^m$

KE outputs $\mathbf{x}'$ s.t.

1. $\mathbf{y} = \mathbf{A}\mathbf{x}' \bmod q$
2. $\|\mathbf{x}'\| \leqq 2d\sqrt{m}$

$\mathbf{r} \longleftarrow \{0,\ldots,d-1\}^m$

$\mathbf{a} \longleftarrow \mathbf{A}\mathbf{r} \bmod q$

$\mathbf{a}$

$\mathbf{c}$

$\mathbf{c} \longleftarrow \{0,1\}$

$\mathbf{z} \longleftarrow \mathbf{r} + c\mathbf{x} \bmod q$

if $\mathbf{z} \notin \{1,\ldots,d-1\}^m$,

$\mathbf{z} \longleftarrow \perp$

$\mathbf{z}$

$\mathbf{A}\mathbf{z} \stackrel{?}{=} \mathbf{a} + c\mathbf{y} \bmod q$

$\|\mathbf{z}\| \leqq d\sqrt{m}$

Lyubashevsky's ID

$\mathbf{y} = \mathbf{Ax} \bmod$

$\mathbf{x} \in \{0,1\}^m$

KE outputs $\mathbf{x}'$ s.t.

1. $\mathbf{y}=\mathbf{Ax}' \bmod q$
2. $\|\mathbf{x}'\| \leqq 2d\sqrt{m}$

$\mathbf{r} \longleftarrow \{0,\ldots,d\text{-}1\}^m$

$\mathbf{a} \longleftarrow \mathbf{Ar} \bmod q$

$\mathbf{a}$

$\mathbf{z} \longleftarrow \mathbf{r} + c\mathbf{x} \bmod q$

if $\mathbf{z} \notin \{1,\ldots,d\text{-}1\}^m$,

$\mathbf{z} \longleftarrow \perp$

Since $d=\tilde{O}(m)$, $\beta=\tilde{O}(d\sqrt{m})=\tilde{O}(m^{1.5})$ in $SIS_{q,m,\beta}$

Agenda

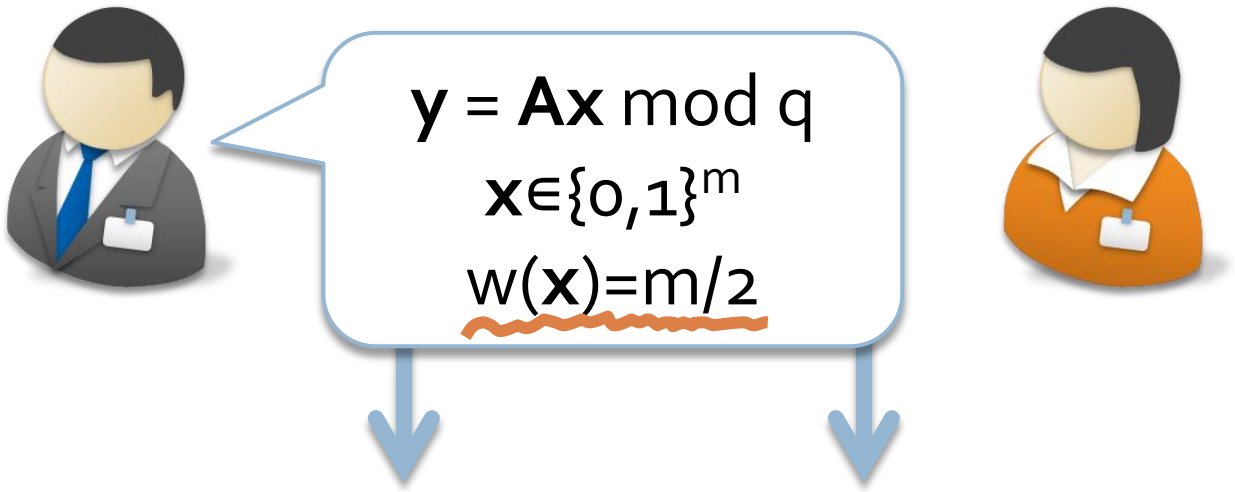
- Background
- Strategy for C-ID
- Lyubashevsky's ID
- Ours (or Stern's ID)
  - Stern's ID
  - Two Problem in Commitment
  - Implementing Commitment

Stern's ID [Ste96]

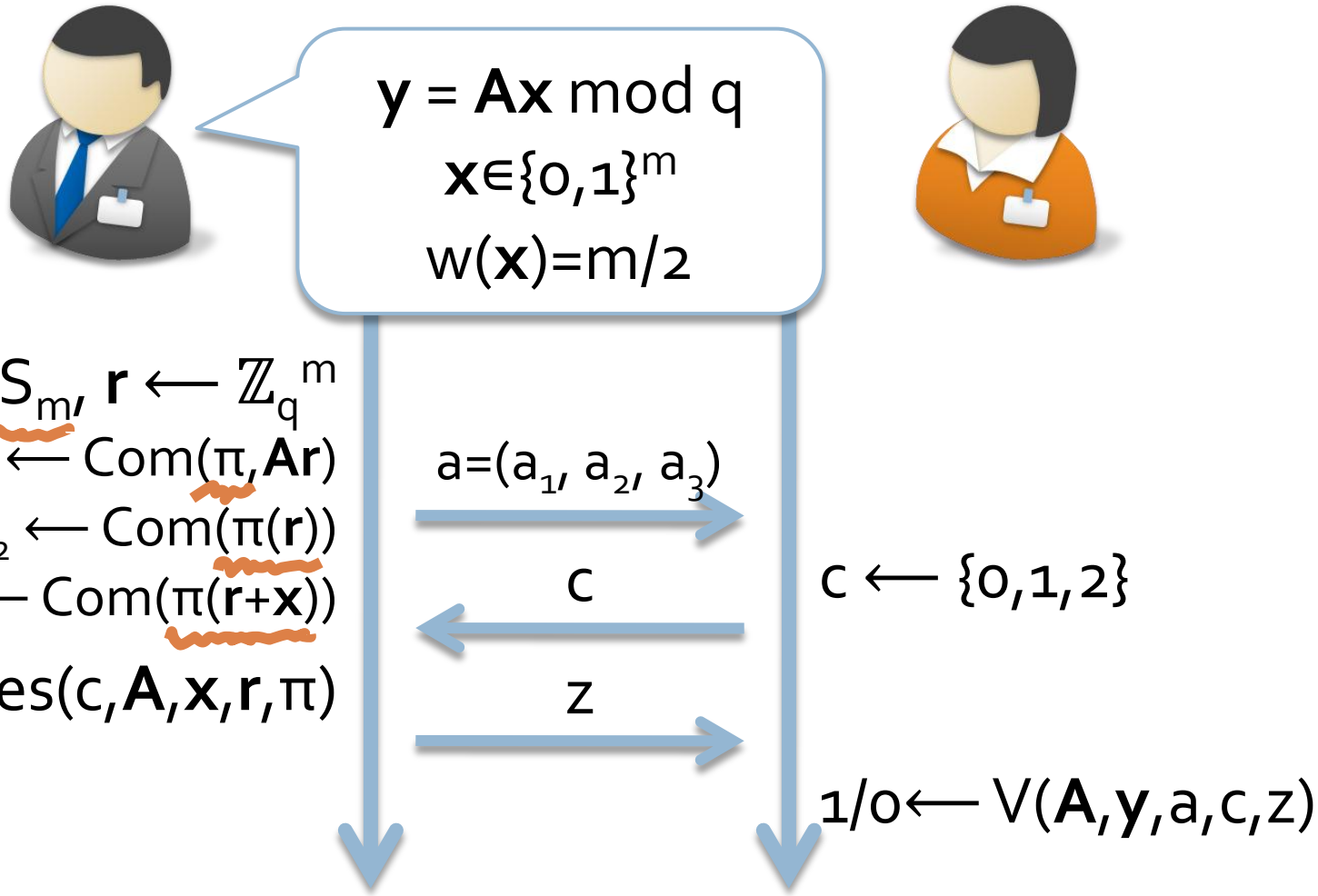
This is a coding-based ID,
but this suits for lattice-based ID

Stern's ID [Ste96]

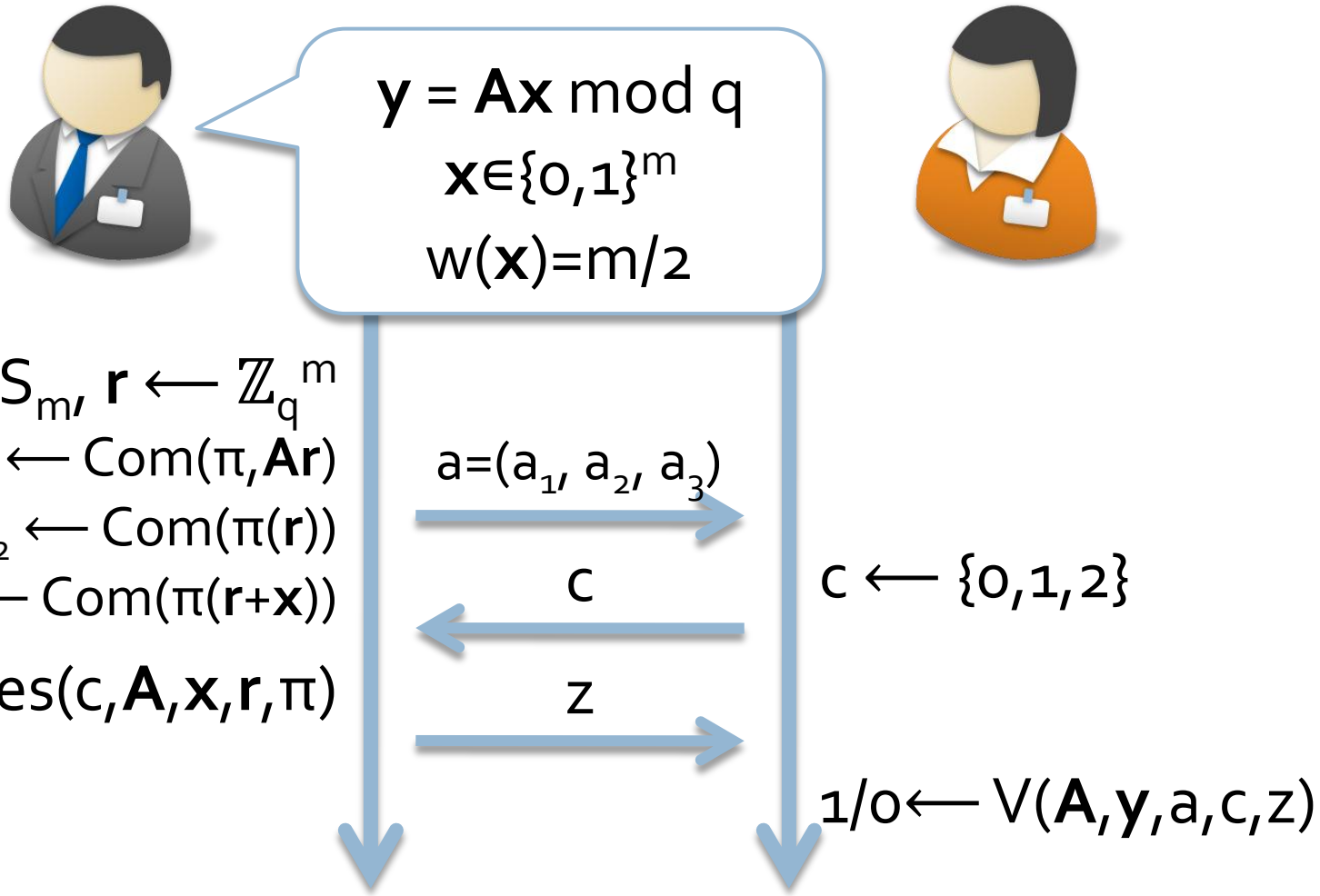
This is a coding-based ID,
but this suits for lattice-based ID.



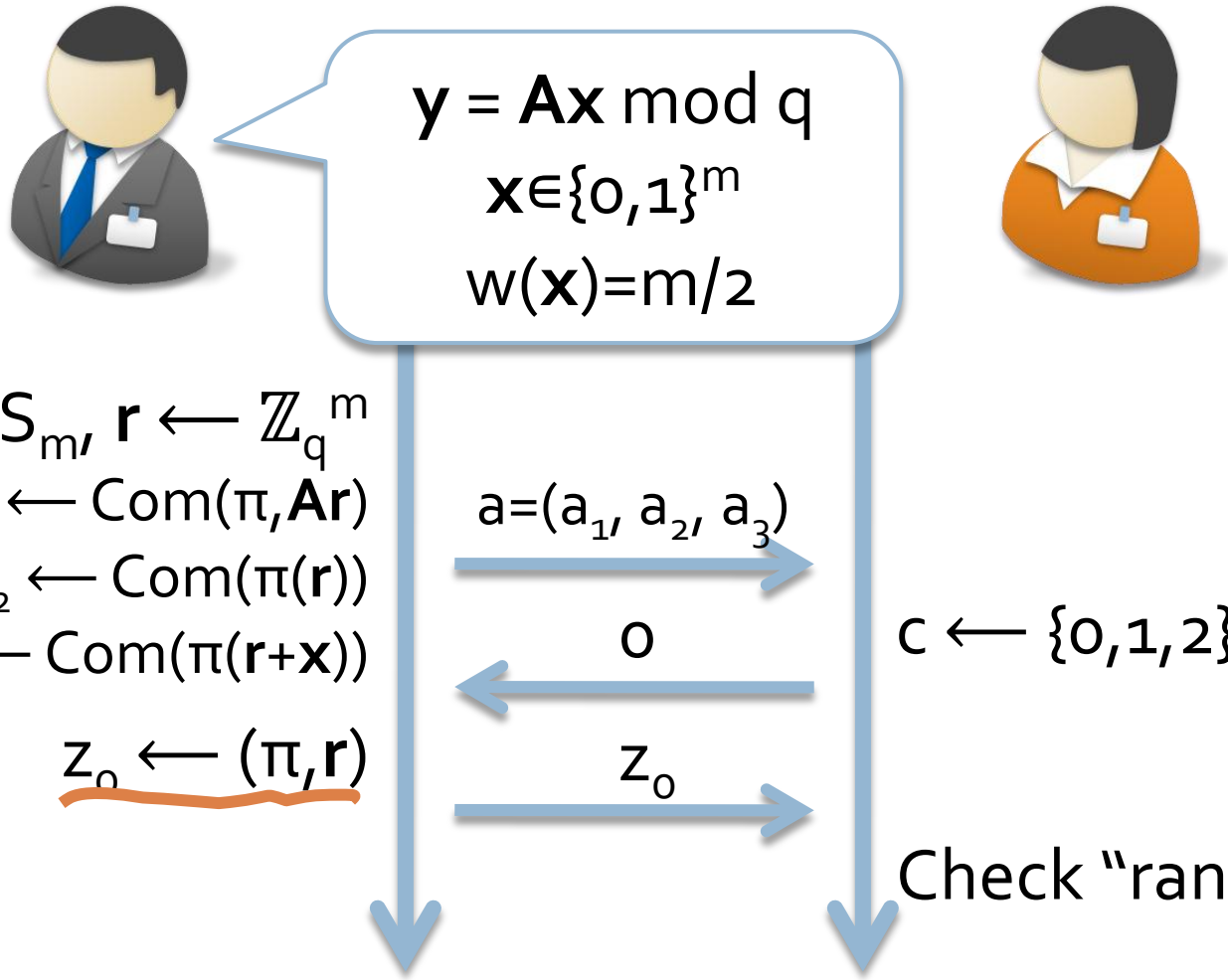
Stern's ID [Ste96]



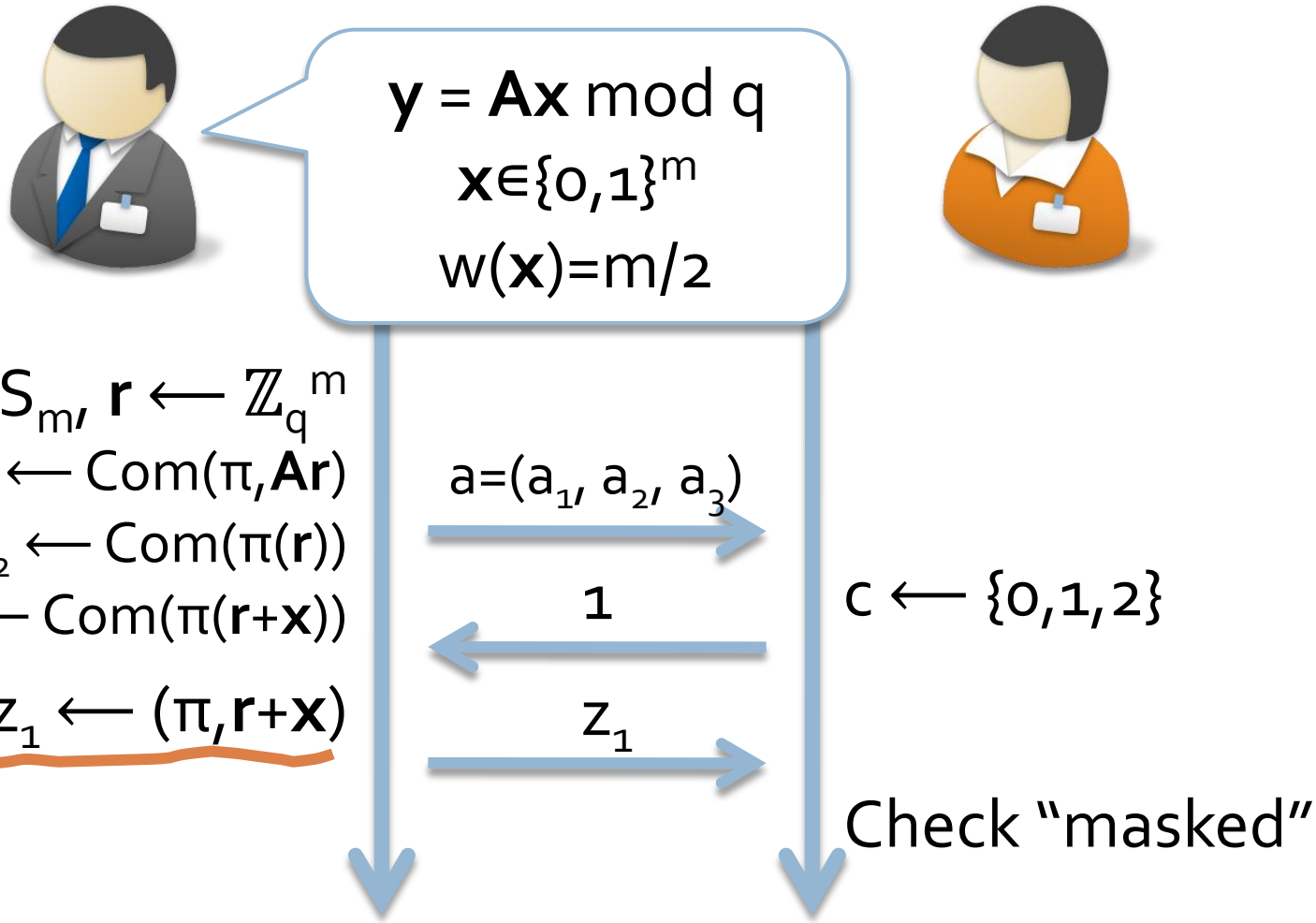
Random/Masked/Permuted



Random/Masked/Permuted



Random/Masked/Permuted



Random/Masked/Permuted

$\mathbf{y} = \mathbf{A}\mathbf{x} \bmod q$

$\mathbf{x} \in \{0,1\}^m$

$w(\mathbf{x}) = m/2$

$\pi \longleftarrow S_m,\ \mathbf{r} \longleftarrow \mathbb{Z}_q^{\,m}$

$a_1 \longleftarrow \mathrm{Com}(\pi, \mathbf{A}\mathbf{r})$

$a_2 \longleftarrow \mathrm{Com}(\pi(\mathbf{r}))$

$a_3 \longleftarrow \mathrm{Com}(\pi(\mathbf{r}+\mathbf{x}))$

$z_2 \longleftarrow (\pi(\mathbf{r}), \pi(\mathbf{r}+\mathbf{x}))$

$a = (a_1, a_2, a_3)$

2

z_2

$c \longleftarrow \{0,1,2\}$

Check "permuted"

Random/Masked/Permuted

$\mathbf{y} = \mathbf{A}\mathbf{x} \bmod q$

$\mathbf{x} \in \{0,1\}^m$

$w(\mathbf{x}) = m/2$

$\pi \longleftarrow S_m,\ \mathbf{r} \longleftarrow \mathbb{Z}_q^{\,m}$

$a_1 \longleftarrow \mathrm{Com}(\pi, \mathbf{A}\mathbf{r})$

$a_2 \longleftarrow \mathrm{Com}(\pi(\mathbf{r}))$

$a_3 \longleftarrow \mathrm{Com}(\pi(\mathbf{r}+\mathbf{x}))$

$z_2 \longleftarrow (\pi(\mathbf{r}), \pi(\mathbf{r}+\mathbf{x}))$

$a = (a_1, a_2, a_3)$

2

z_2

C

$\pi(\mathbf{r}+\mathbf{x}) - \pi(\mathbf{r})$

$= \pi(\mathbf{x}) \stackrel{?}{\in} \{0,1\}^m$

Check "permuted"

Using Stern's ID

$\mathbf{y} = \mathbf{A}\mathbf{x} \bmod q$

$\mathbf{x} \in \{0,1\}^m$

$w(\mathbf{x}) = m/2$

$\pi \longleftarrow S_m$, $\mathbf{r} \longleftarrow \mathbb{Z}_q^m$

$a_1 \longleftarrow \mathrm{Com}(\pi, \mathbf{Ar})$

$a_2 \longleftarrow \mathrm{Com}(\pi(\mathbf{r}))$

$a_3 \longleftarrow \mathrm{Com}(\pi(\mathbf{r}+\mathbf{x}))$

$z \longleftarrow \mathrm{Res}(c, \mathbf{A}, \mathbf{x}, \mathbf{r}, \pi)$

KE outputs $\mathbf{x}'$ or (s_1, s_2) s.t.

1. $\mathbf{y} = \mathbf{A}\mathbf{x}' \bmod q$ and $\mathbf{x}' \in \{0,1\}^m$
2. $\mathrm{Com}(s_1) = \mathrm{Com}(s_2)$

$1/0 \longleftarrow V(\mathbf{A}, \mathbf{y}, a, c, z)$

Two Problems in Stern's ID

Com [Ste96]

$$\mathrm{Com}(m,r) = h(m \oplus r \,\|\, r),$$

where h is a hash function.

Two Problems in Stern's ID

Com [Ste96]

$$\mathrm{Com}(m,r) = h(m \oplus r \,\|\, r),$$

sh function.

1. Is this stat. hiding?

It seems NO.
If it is stat. hiding, the protocol is WI.

Two Problems in Stern's ID

Com [Ste96]

$$\mathrm{Com}(m,r) = h(m \oplus r \,\|\, r),$$

sh function.

1. Is this stat. hiding?

2. Is this based on SIS?

NO.
We implement
Com based on SIS.

Implementing String Com.

Hash
[Ajt97,GGH96,…]

$$H = \{f_{\mathbf{A}}:\{0,1\}^m \longrightarrow \mathbb{Z}_q^{\,n} \mid \mathbf{A} \in \mathbb{Z}_q^{\,n \times m}\}$$
$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$$

Thm
[Ajt97,Reg05,…]

$$\Delta(\mathbf{A}\mathbf{x},\mathbf{r}) \leqq \mathrm{negl}(n),$$
where $\mathbf{x} \longleftarrow \{0,1\}^m$, $\mathbf{r} \longleftarrow \mathbb{Z}_q^{\,n}$

Implementing String Com.

Hash
[Ajt97,GGH96,…]

$$H = \{f_{\mathbf{A}}:\{0,1\}^m \longrightarrow \mathbb{Z}_q^{\,n} \mid \mathbf{A} \in \mathbb{Z}_q^{\,n \times m}\}$$
$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$$

$f_{\mathbf{A}}$ is almost uniform.

Thm
[Ajt97,Reg05,…]

$$\Delta(\mathbf{A}\mathbf{x},\mathbf{r}) \leqq \mathrm{negl}(n),$$
where $\mathbf{x} \leftarrow \{0,1\}^m$, $\mathbf{r} \leftarrow \mathbb{Z}_q^{\,n}$

Implementing String Com.

Com.

$$\mathrm{Com}_A(\mathbf{m},\mathbf{r})=f_A(\mathbf{m}||\mathbf{r})$$

Lemma

A collision implies a solution of $SIS_{q,m,\beta}$ for $\beta=\sqrt{m}$

Implementing String Com.

Com.

$$\mathrm{Com}_A(\mathbf{m},\mathbf{r}) = f_A(\mathbf{m}\|\mathbf{r})$$

Statistical hiding follows from the property of f_A

Lemma

A collision implies a solution of $SIS_{q,m,\beta}$ for $\beta = \sqrt{m}$

S^+-ID

$\pi \longleftarrow S_m$, $\mathbf{r} \longleftarrow \mathbb{Z}_q^m$

$a_1 \longleftarrow \mathrm{Com}_{\mathbf{A}}(\pi, \mathbf{Ar})$

$a_2 \longleftarrow \mathrm{Com}_{\mathbf{A}}(\pi(\mathbf{r}))$

$a_3 \longleftarrow \mathrm{Com}_{\mathbf{A}}(\pi(\mathbf{r}+\mathbf{x}))$

$z \longleftarrow \mathrm{Res}(c, \mathbf{A}, \mathbf{x}, \mathbf{r}, \pi)$

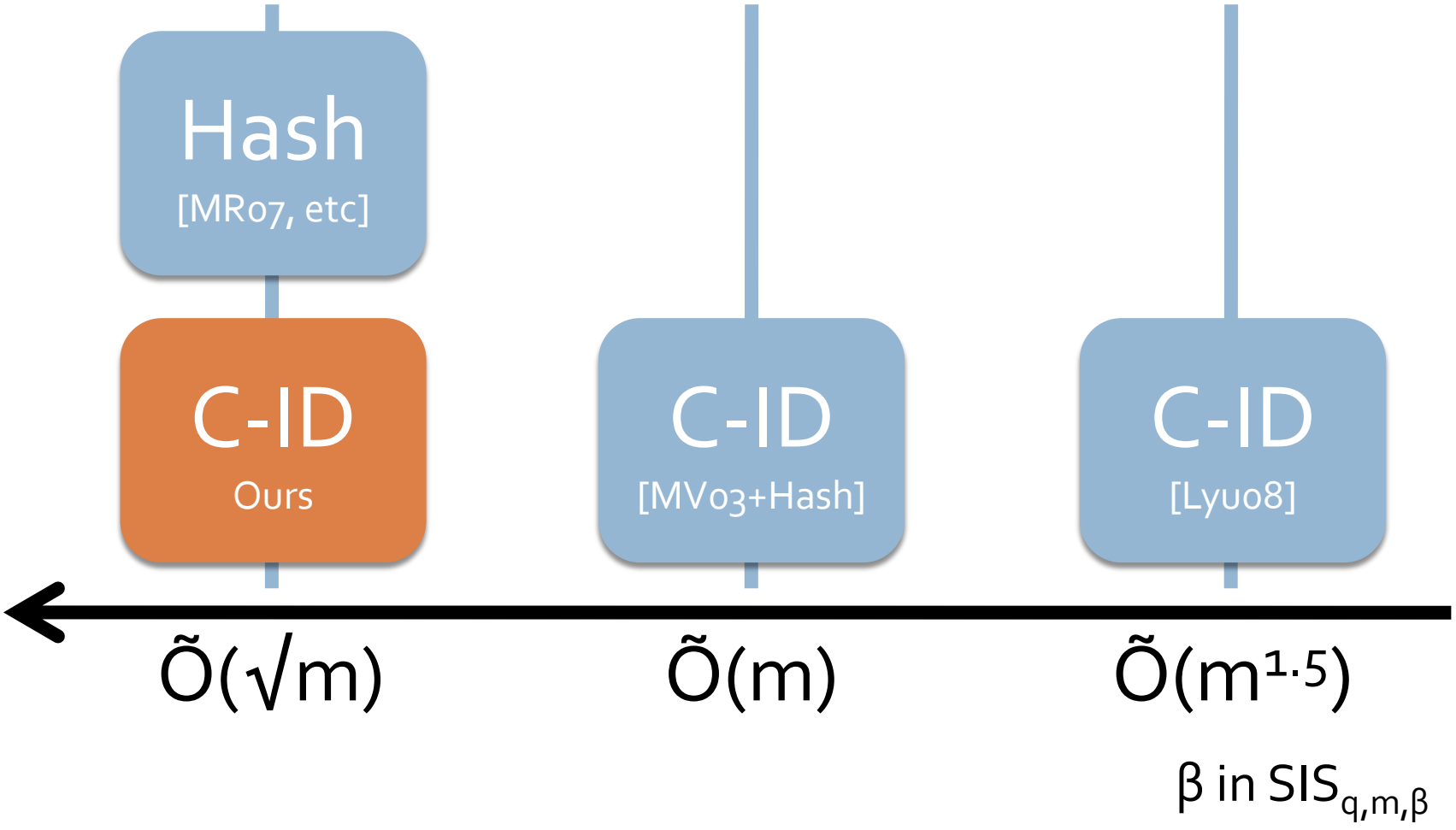
KE outputs $\mathbf{x}'$ or (s_1, s_2) s.t.

1. $\mathbf{y}=\mathbf{A}\mathbf{x}' \bmod q$ and $\mathbf{x}' \in \{0,1\}^m$
2. $\mathrm{Com}_{\mathbf{A}}(s_1)=\mathrm{Com}_{\mathbf{A}}(s_2)$

In the both cases, using KE,
we can solve $\mathrm{SIS}_{q,m,\beta}$ for $\beta=\sqrt{m}$

$1/0 \longleftarrow V(\mathbf{A}, \mathbf{y}, a, c, z)$

Schemes and Assumptions #2



Additional Result

- Ad Hoc Anonymous Identification
  - Identification version of ring sig. [DKNY04]
- Our Idea:
  - $\mathbf{y}_i = \mathbf{A}\,\mathbf{x}_i \bmod q$ for $i = 1,\ldots,k$
  - Using the ID, the prover proves that $\mathbf{Ax} = \mathbf{y}_i \bmod q$
  - Technique: Splitting the permutation

Conclusion

- We modify Stern's ID (S^+-ID)
  - Implement Com by the lattice-based hash functions
- S^+-ID is based on $SIS_{q,m,\tilde{O}(\sqrt{m})}$ (or $GapSVP_{\tilde{O}(n)}$)
- Ad hoc anonymous ID based $SIS_{q,m,\tilde{O}(\sqrt{m})}$

- Using SWIFFT [LMPR08], we have more efficient ones