Magic Adversaries *VS* Individual Reduction
--- " Science Wins Either Way "

Yi Deng

deng@iie.ac.cn

State Key Lab. of Information security, CAS

An annoying situation in crypto: for lots of earlier simple and elegant constructions:

An annoying situation in crypto: for lots of earlier simple and elegant constructions:

- No concrete attack;

An annoying situation in crypto: for lots of earlier simple and elegant constructions:

- No concrete attack;
- No security proof（under standard assumption）;

An annoying situation in crypto: for lots of earlier simple and elegant constructions:

- No concrete attack;
- No security proof（under standard assumption）;
- But black-box lower bounds

Impagliazzo and Rudich make us feel less embarrassed

An annoying situation in crypto: for lots of earlier simple and elegant constructions:

- No concrete attack;
- No security proof（under standard assumption）;
- But black-box lower bounds

Impagliazzo and Rudich make us feel less embarrassed

A few black box barriers have been bypassed (e.g., Barak's public coin arguments)

An annoying situation in crypto: for lots of earlier simple and elegant constructions:

- No concrete attack;
- No security proof（under standard assumption）;
- But black-box lower bounds

Impagliazzo and Rudich make us feel less embarrassed

A few black box barriers have been bypassed (e.g., Barak's public coin arguments)

But for most of them, it is unclear whether the BB lower bounds are fundamental barriers.

An annoying situation in crypto: for lots of earlier simple and elegant constructions:

- No concrete attack;
- No security proof（under standard assumption）;
- But black-box lower bounds

Impagliazzo and Rudich make us feel less embarrassed

A few black box barriers have been bypassed (e.g., Barak's public coin arguments)

But for most of them, it is unclear whether the BB lower bounds are fundamental barriers.

We show that there must be a new way to get around some of known BB lower bounds.

Specifically, we prove:

Specifically, we prove:

if $\exists$ injective OWF f, then one of the following statements must be true:

1. (infinitely-often) public key encryption/KE exist.

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR-NP statements with small indist. gap.

Specifically, we prove:

if $\exists$ injective OWF f, then one of the following statements must be true:

1. (infinitely-often) public key encryption/KE exist.

   - ➢ Impossible for BB construction [IR 89]
   - ➢ All known results are negative [DS16…]

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR-NP statements with small indist. gap.

Specifically, we prove:

if ∃ injective OWF f, then one of the following statements must be true:

1. (infinitely-often) public key encryption/KE exist.

   - Impossible for BB construction [IR 89]
   - All known results are negative [DS16…]

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR-NP statements with small indist. gap.

   - [DNS90] observed that FS may not be bbCZK;

Specifically, we prove:

if $\exists$ injective OWF f, then one of the following statements must be true:

1. (infinitely-often) public key encryption/KE exist.

   - Impossible for BB construction [IR 89]
   - All known results are negative [DS16…]

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR-NP statements with small indist. gap.

   - [DNS90] observed that FS may not be bbCZK;
   - Impossible for BB simulation [CKPR01];

Specifically, we prove:

if $\exists$ injective OWF f, then one of the following statements must be true:

1. (infinitely-often) public key encryption/KE exist.

   - Impossible for BB construction [IR 89]
   - All known results are negative [DS16…]

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR-NP statements with small indist. gap.

   - [DNS90] observed that FS may not be bbCZK;
   - Impossible for BB simulation [CKPR01];
   - Generate a lone line of research [CLOS02, PR03, Lin03b, PR05, Pas04, Lin08, GGJ13, GGJS12, GGS15, GLP+15…];

Specifically, we prove:

if ∃ injective OWF f, then one of the following statements must be true:

1. (infinitely-often) public key encryption/KE exist.

- Impossible for BB construction [IR 89]
- All known results are negative [DS16…]

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR-NP statements with small indist. gap.

- [DNS90] observed that FS may not be bbCZK;
- Impossible for BB simulation [CKPR01];
- Generate a lone line of research [CLOS02, PR03, Lin03b, PR05, Pas04, Lin08, GGJ13, GGJS12, GGS15, GLP+15…];
- Known constant-round CZK protocols rely on much stronger assumption [CLP15,PPS15]

Specifically, we prove:

if $\exists$ injective OWF f, then one of the following statements must be true:

1. (infinitely-often) PKE/KE exists.

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR-NP statements with small indist. gap.

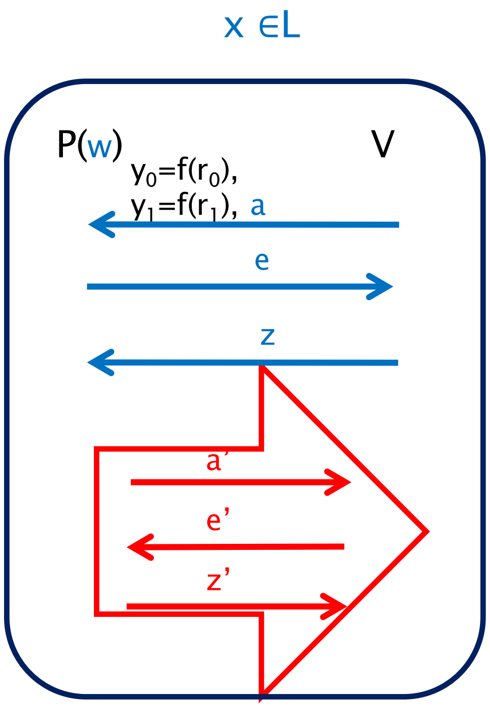
Proof idea.

Given a magic adv V^* that breaks the dist. CZK of Feige-Shamir, we construct PKE/KE from V^* (based on injective OWF).

The classic Feige-Shamir Argument

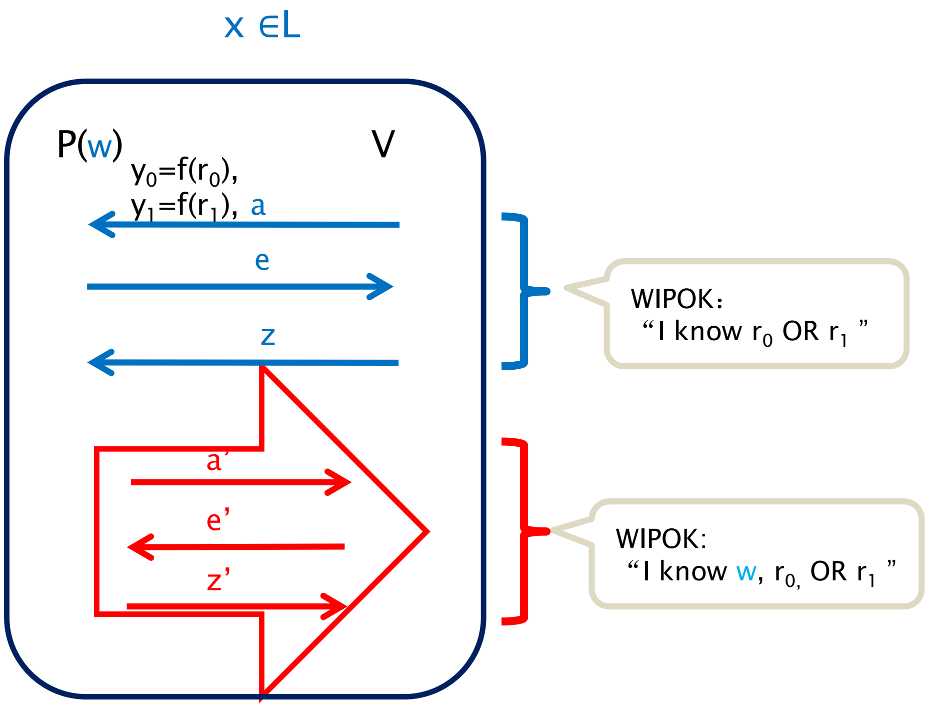
The classic Feige-Shamir Argument

In Standalone setting



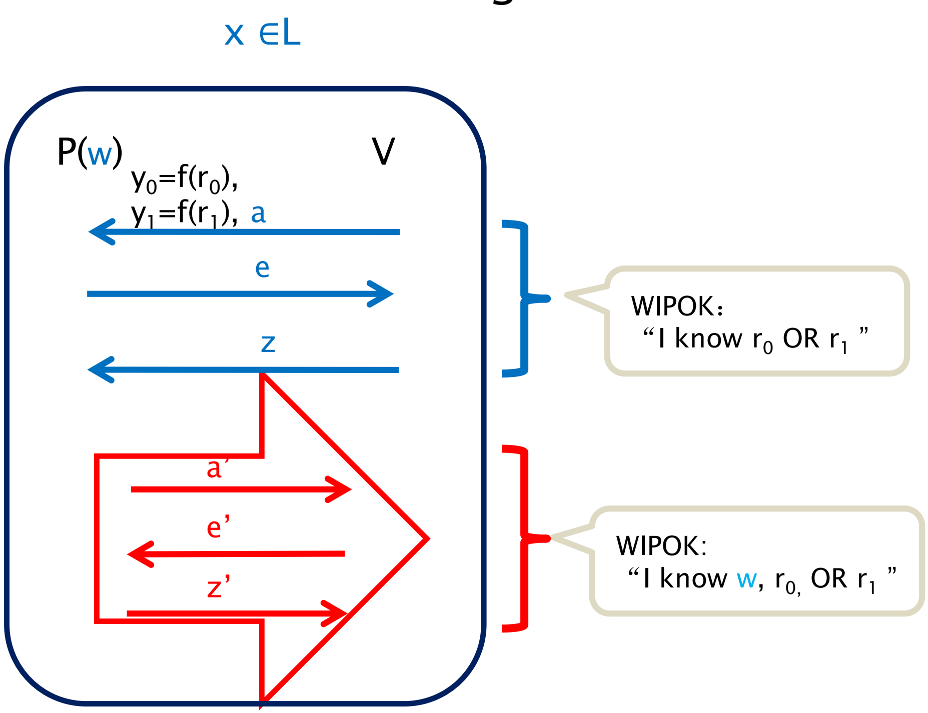
The classic Feige-Shamir Argument

In Standalone setting



The classic Feige-Shamir Argument

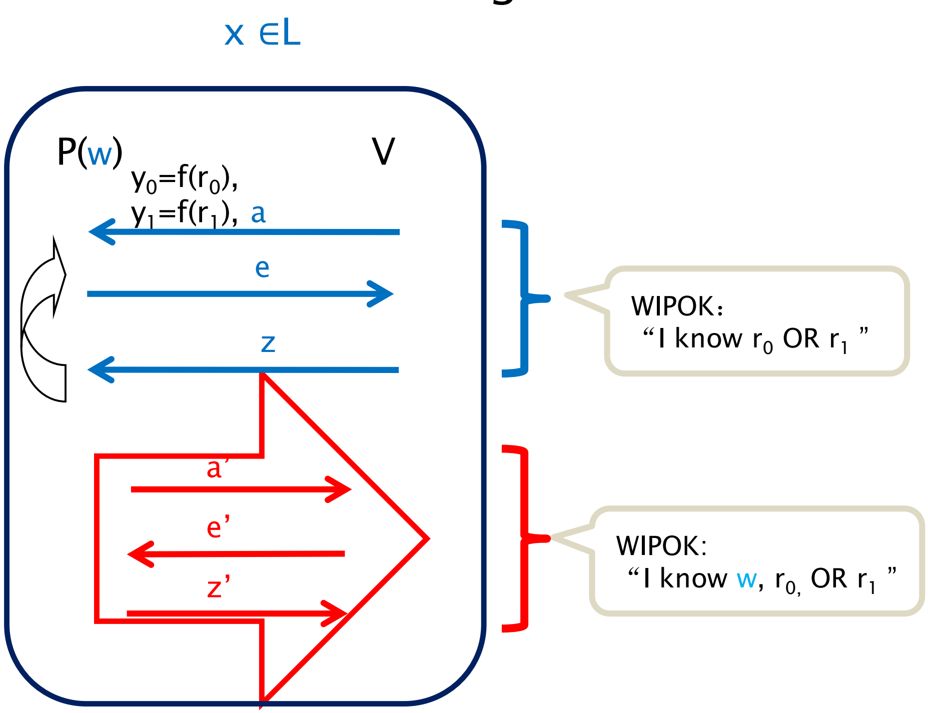
In Standalone setting



- Completeness;
- Soundness;

The classic Feige-Shamir Argument

In Standalone setting

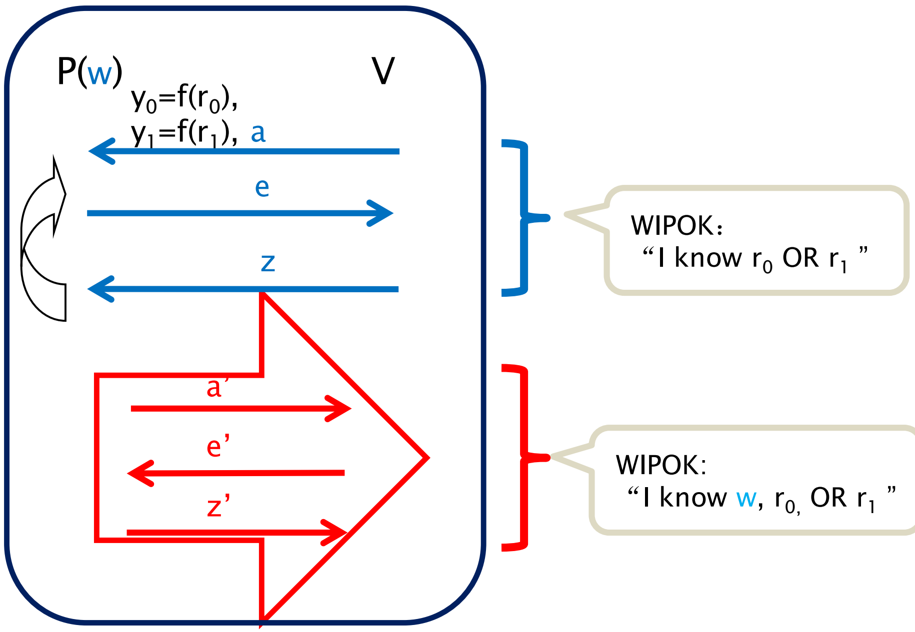


- Completeness;
- Soundness;
- Standalone ZK

The classic Feige-Shamir Argument

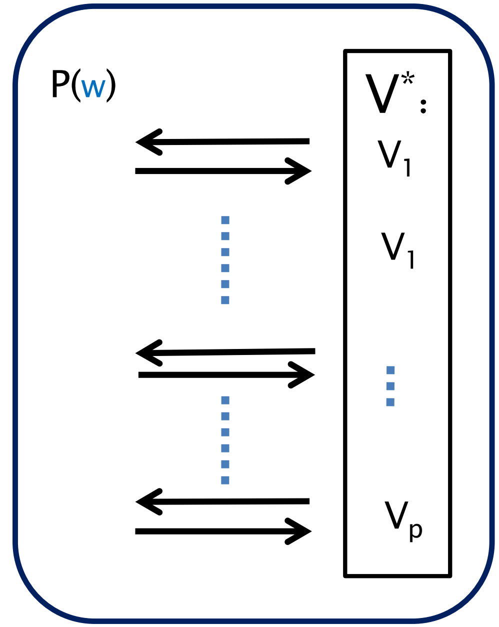
In Standalone setting

$x \in L$



- Completeness;
- Soundness;
- Standalone ZK

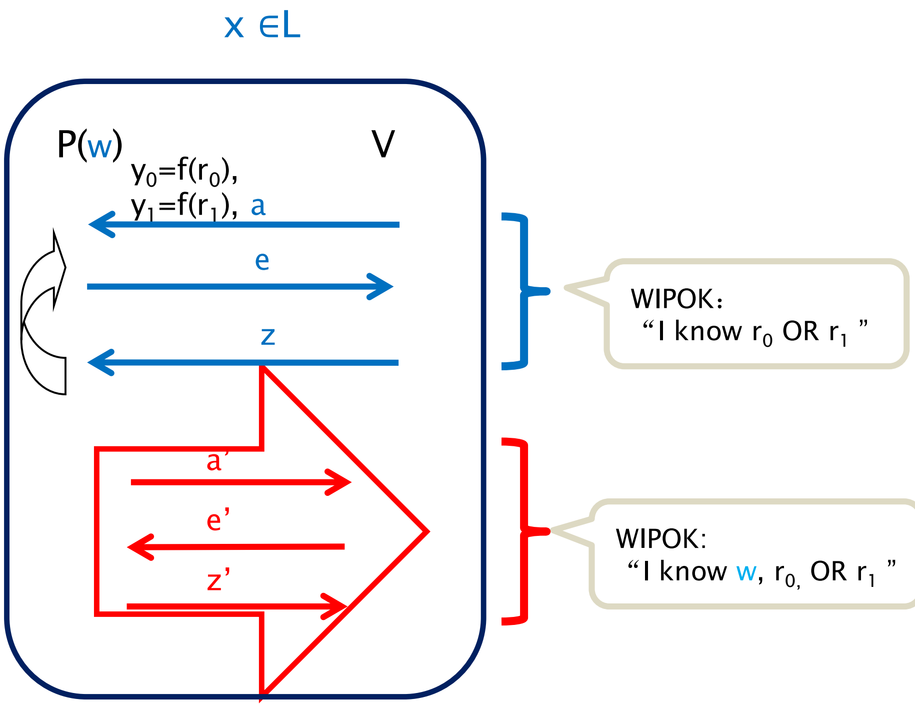
In concurrent setting



V^*controls all msgs scheduling.

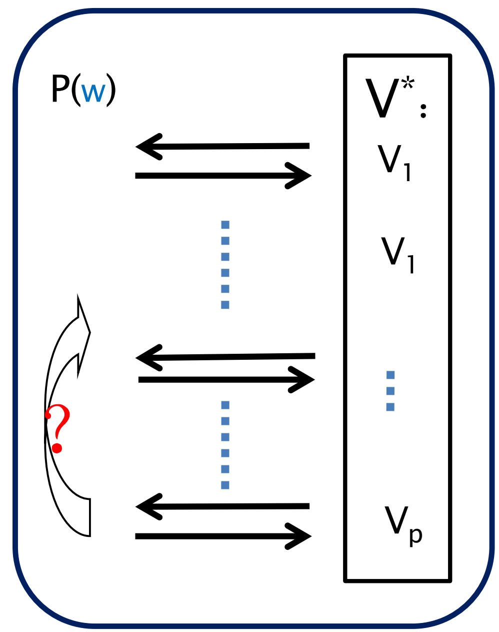
The classic Feige-Shamir Argument

In Standalone setting



- Completeness;
- Soundness;
- Standalone ZK

In concurrent setting

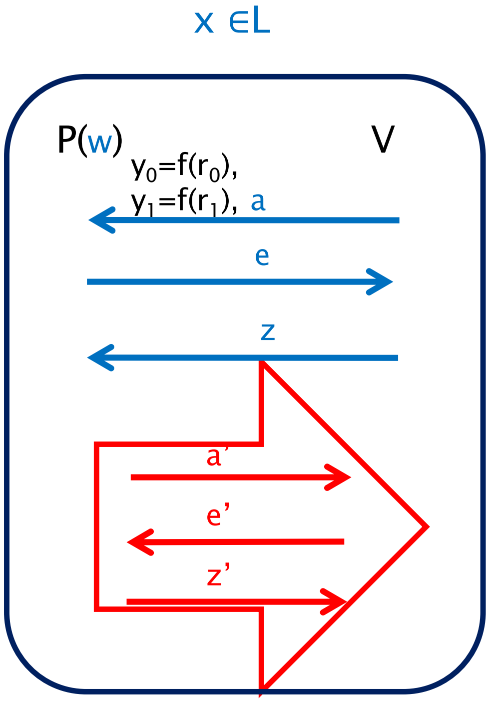


V^*controls all msgs scheduling.

BB simulator fails: Nesting effect

In fact

F-S in Standalone setting

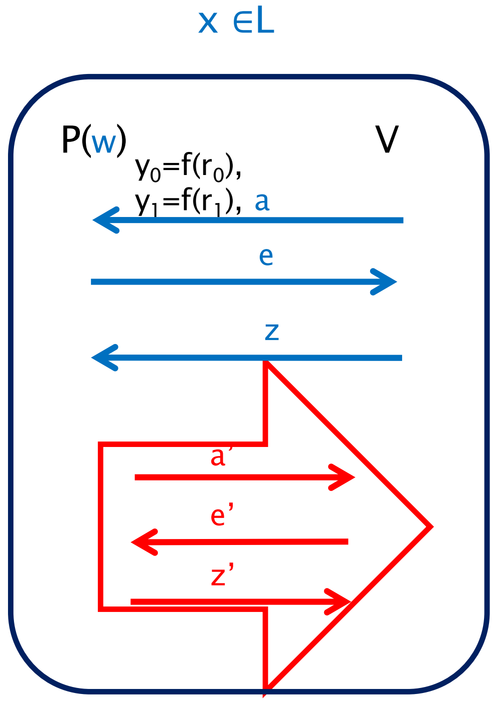


In fact

- For any $o(\log n/\log\log n)$-round protocol (e.g. Feige-Shamir) , there is a class C of concurrent verifiers for which BB simulator fails [CKPR01]:

$$\nexists \text{ (bb) S } \forall \ \mathcal{V} \in C$$

F-S in Standalone setting



In fact

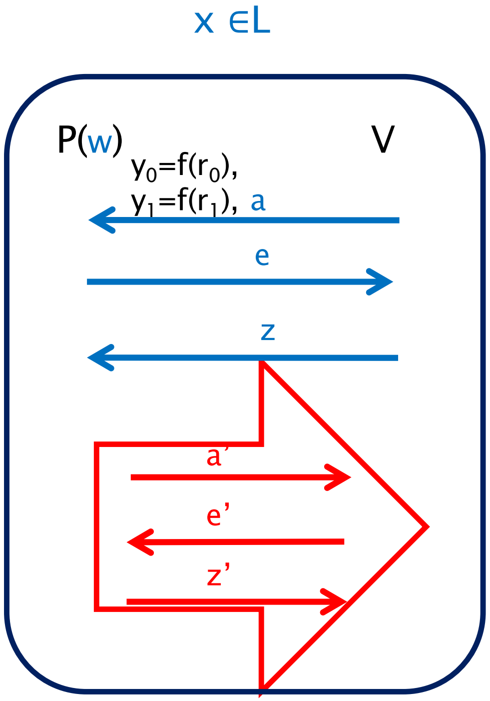
- For any $o(\log n/\log\log n)$-round protocol (e.g. Feige-Shamir)， there is a class $\mathcal{C}$ of concurrent verifiers for which BB simulator fails [CKPR01]:

$$\nexists \text{ (bb) S } \forall\ \mathcal{V} \in \mathcal{C}$$

- We observe that for every $\mathcal{V} \in \mathcal{C}$, there is a simulator that works well:

$$\forall\ \mathcal{V} \in \mathcal{C}\ \ \exists\ \text{S}_{\mathcal{V}}$$

F-S in Standalone setting



In fact

- For any $o(\log n/\log\log n)$-round protocol (e.g. Feige-Shamir)， there is a class C of concurrent verifiers for which BB simulator fails [CKPR01]:

$$\nexists \text{ (bb) S } \forall\ \mathcal{V} \in C$$

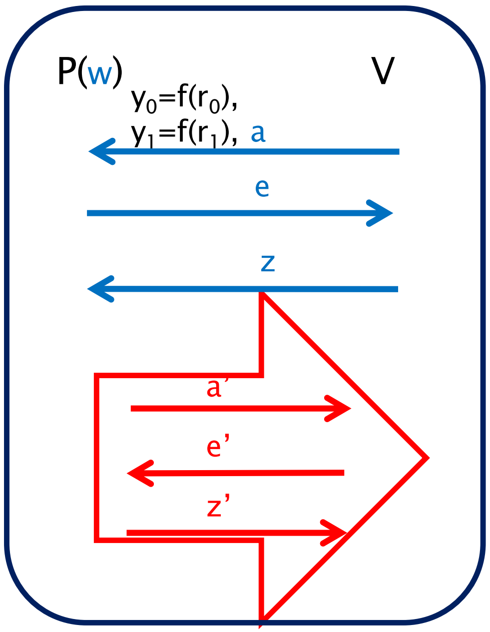
- We observe that for every $\mathcal{V} \in C$, there is a simulator that works well:

$$\forall\ \mathcal{V} \in C \quad \exists\ \text{S}_{\mathcal{V}}$$

$\text{S}_{\mathcal{V}}$ takes the randomness and functionality of $\mathcal{V}$ as input.

F-S in Standalone setting

x ∈L



In fact

- For any $o(\log n/\log\log n)$-round protocol (e.g. Feige-Shamir)， there is a class C of concurrent verifiers for which BB simulator fails [CKPR01]:

$$\not\exists \text{ (bb) S } \forall\ \mathcal{V} \in C$$

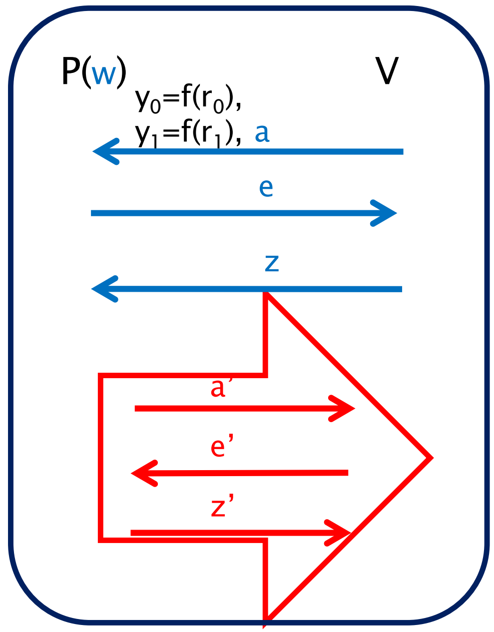
- We observe that for every $\mathcal{V} \in C$, there is a

Natural security definitions only require the *existence* of reduction/simulation.

$$\forall\ \mathcal{V} \in C \quad \exists \quad S_{\mathcal{V}}$$

F-S in Standalone setting

$x \in L$



In fact

- For any $o(\log n/\log\log n)$-round protoco (e.g. Feige-Shamir)， there is a class C concurrent verifiers for which BB simul fails [CKPR01]:

$$\nexists \text{ (bb) S } \forall\ \mathcal{V} \in C$$

This reveals a gap between the *universal* simulation

$$\exists \text{ S } \forall\ \mathcal{V}$$

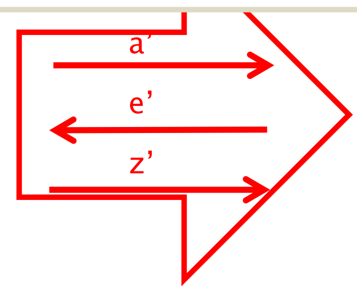
and *individual* simulation

$$\forall\ \mathcal{V}\ \exists \text{ S}$$

- We observe that for every $\mathcal{V} \in C$, there is a

Natural security definitions only require the *existence* of reduction/simulation.

$$\forall\ \mathcal{V} \in C\ \ \exists\ \text{S}_{\mathcal{V}}$$



In fact

- For any $o(\log n/\log\log n)$-round protocol (e.g. Feige-Shamir) , there is a class C of concurrent verifiers for which BB simulator fails [CKPR01]:

$$\nexists \text{ (bb) S } \forall\ \mathcal{V} \in C$$

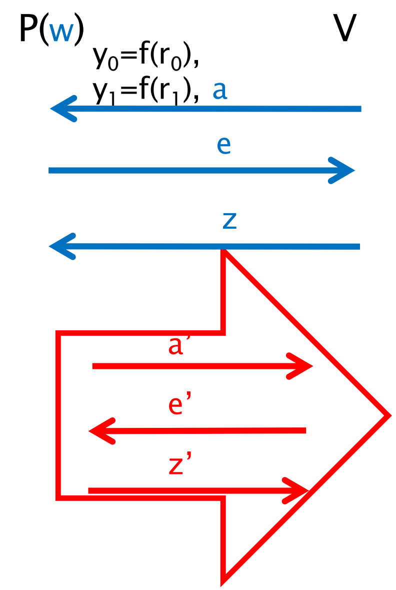
- We observe that for every $\mathcal{V} \in C$, there is a simulator that works well:

$$\forall\ \mathcal{V} \in C \quad \exists\ S_{\mathcal{V}}$$

Any magic adv V* (not in C) that breaks CZK of Feige-Shamir (i.e., no efficient alg can simulate its view) ?

F-S in Standalone setting

x ∈L



Consequence of a magic adv V^* *(oversimplified)*

Consequence of a magic adv V^* *(oversimplified)*

Fix n， and assume V^* runs in poly(n) steps in a real interaction.

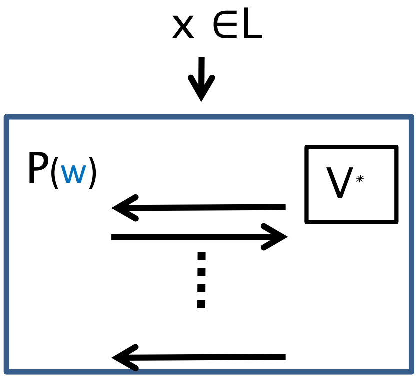
We prove:

Consequence of a magic adv V^* *(oversimplified)*

Fix n, and assume V^* runs in poly(n) steps in a real interaction.

We prove:

$\exists$ V^*' step i:



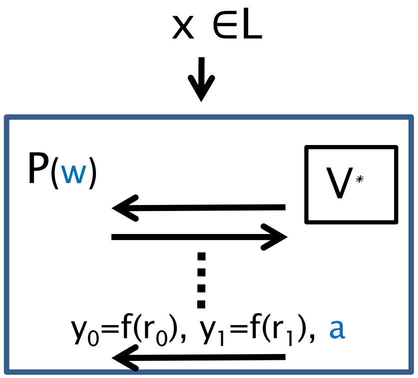
Consequence of a magic adv V^* *(oversimplified)*

Fix n， and assume V^* runs in poly(n) steps in a real interaction.

We prove:

∃ V^*' step i:

1. At step i, V^* outputs the first message （y_0, y_1, a） of a session;



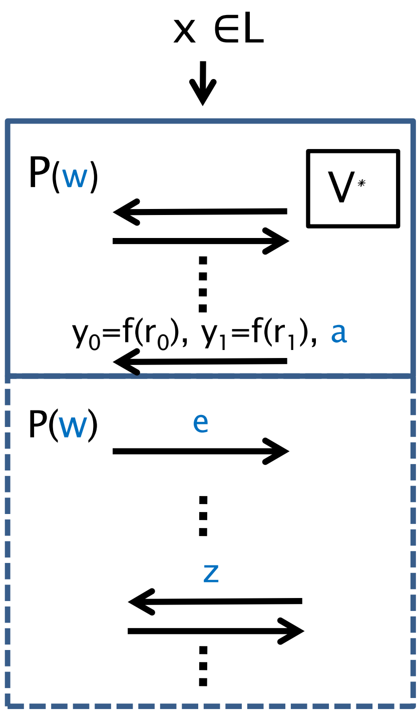
Consequence of a magic adv V^* *(oversimplified)*

Fix n, and assume V^* runs in poly(n) steps in a real interaction.

We prove:

∃ $V^{*'}$ step i:

1. At step i, V^* outputs the first message (y_0, y_1, a) of a session;
2. V^* will complete its proof of "I know one of preimages" at a later time.



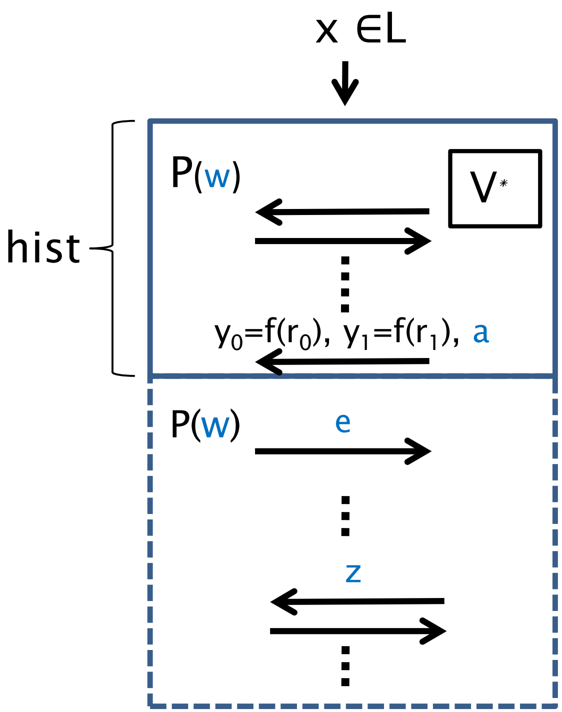
Consequence of a magic adv V^* *(oversimplified)*

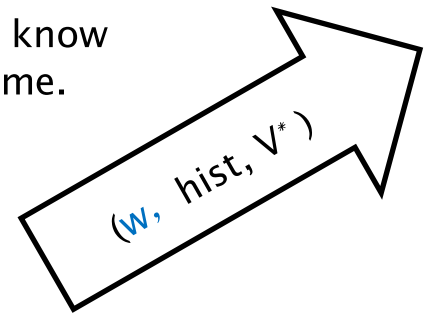
Fix n, and assume V^* runs in poly(n) steps in a real interaction.

We prove:

∃ V^{*}' step i:

1. At step i, V^* outputs the first message (y_0, y_1, a) of a session;
2. V^* will complete its proof of "I know one of preimages" at a later time.





Given the witness w as input, there is a PPT inverting E,

E (w,hist, V^*) → r_b.

(by rewinding)

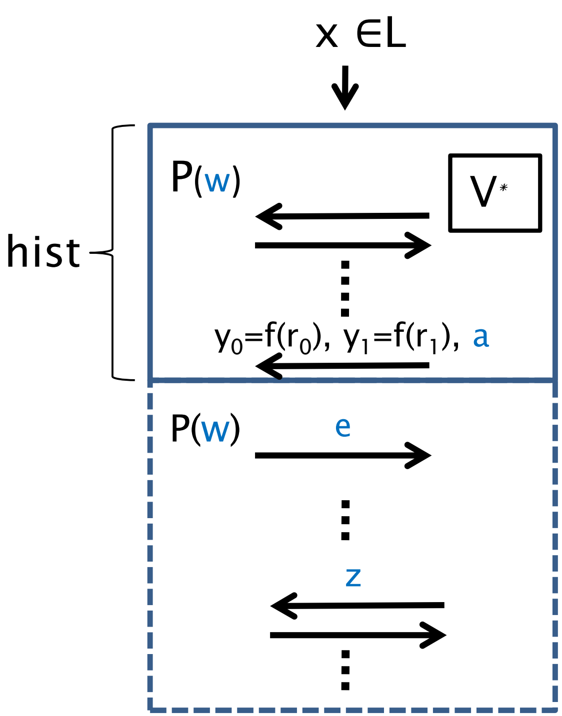
Consequence of a magic adv V^* *(oversimplified)*

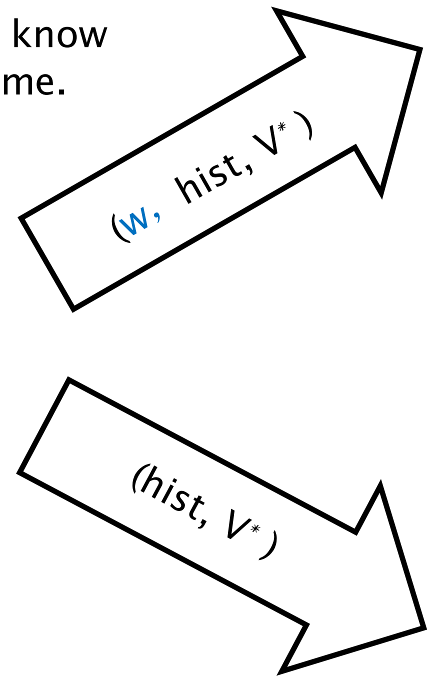
Fix n， and assume V^* runs in poly(n) steps in a real interaction.

We prove:

∃ V^*' step i:

1. At step i, V^* outputs the first message （y_0, y_1, a） of a session;
2. V^* will complete its proof of "I know one of preimages" at a later time.





Given the witness w as input, there is a PPT inverting E,

E (w,hist, V^*) → r_b.

(by rewinding)

Without the witness w, no PPT T(hist,V^*) can invert any images y_0, y_1.

(otherwise we will have a simulator for V^*)

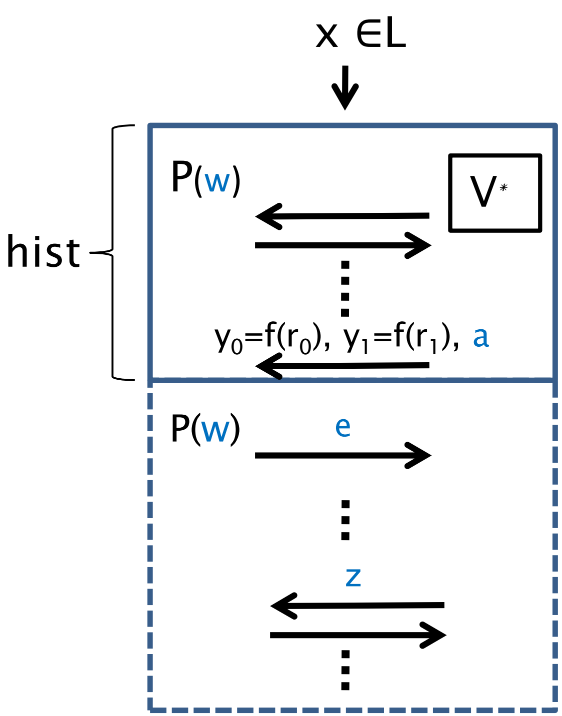
Consequence of a magic adv V^* *(oversimplified)*

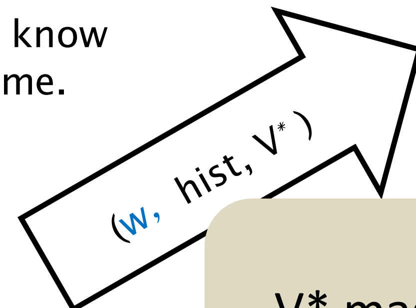
Fix n, and assume V^* runs in poly(n) steps in a real interaction.

We prove:

∃ V^{*}' step i:

1. At step i, V^* outputs the first message (y_0, y_1, a) of a session;
2. V^* will complete its proof of "I know one of preimages" at a later time.



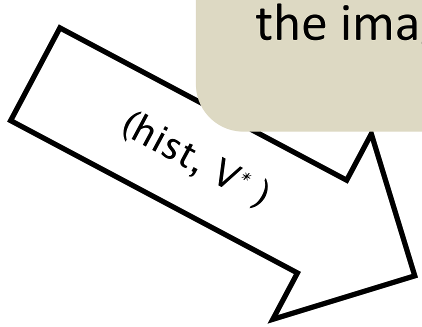


Given the witness w as input, there is a PPT inverting E,

E (w,hist, V^*) → r_b.

(by rewinding)

V* magically creates a trapdoor (w) for the images of f output by V^* at its step i.



Without the witness w, no PPT T(hist,V^*) can invert any images y_0, y_1.

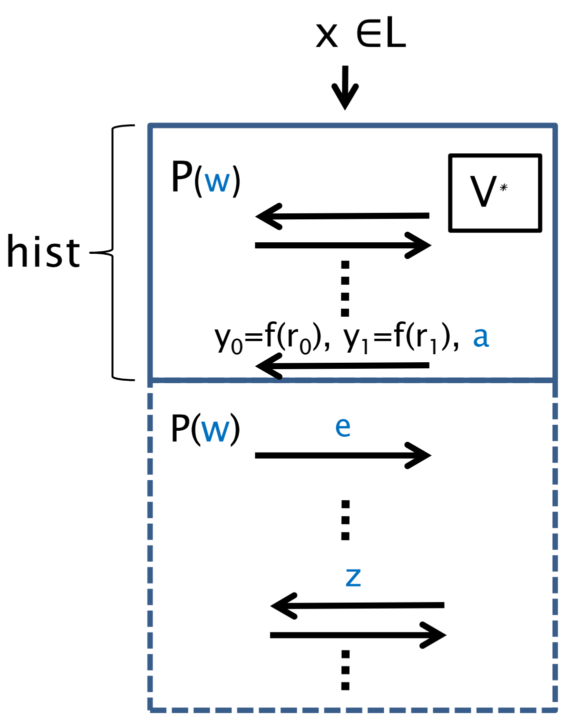
(otherwise we will have a simulator for V^*)

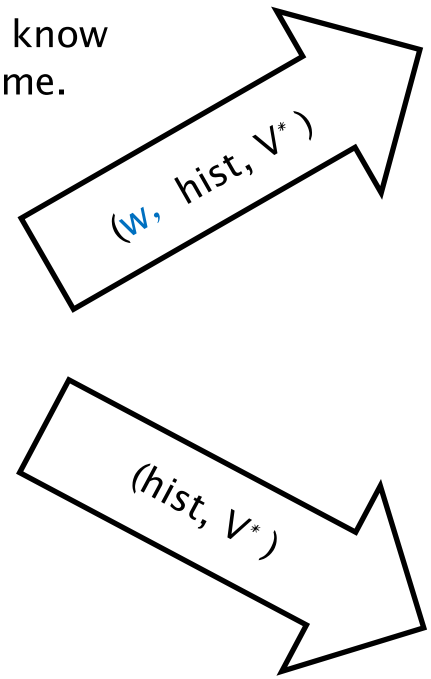
Consequence of a magic adv V^* *(oversimplified)*

Actually, we prove that there are infinitely many n, for each n

$\exists$ V^{*}' step i_n:

1. At step i, V^* outputs the first message （y_0, y_1, a） of a session;
2. V^* will complete its proof of "I know one of preimages" at a later time.

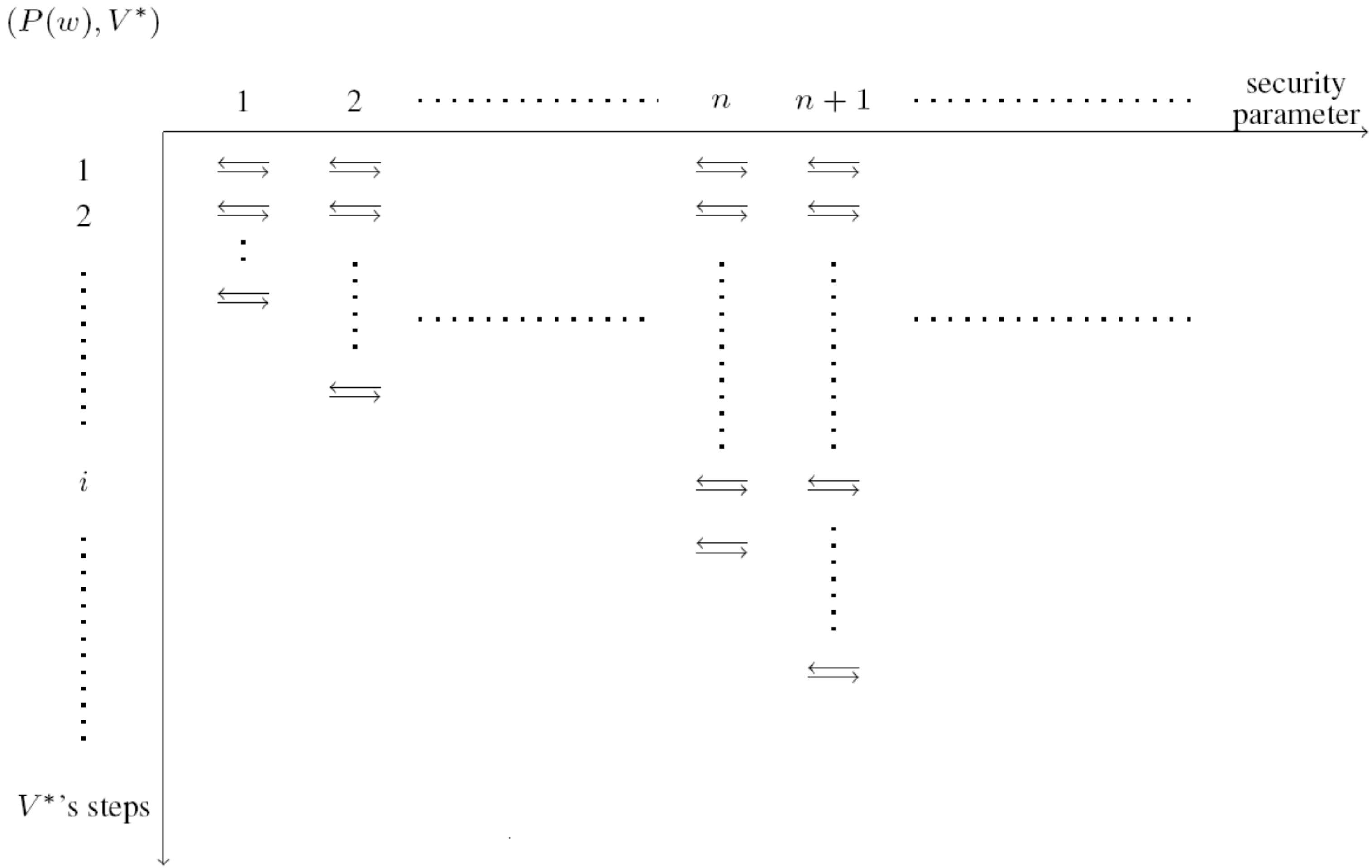




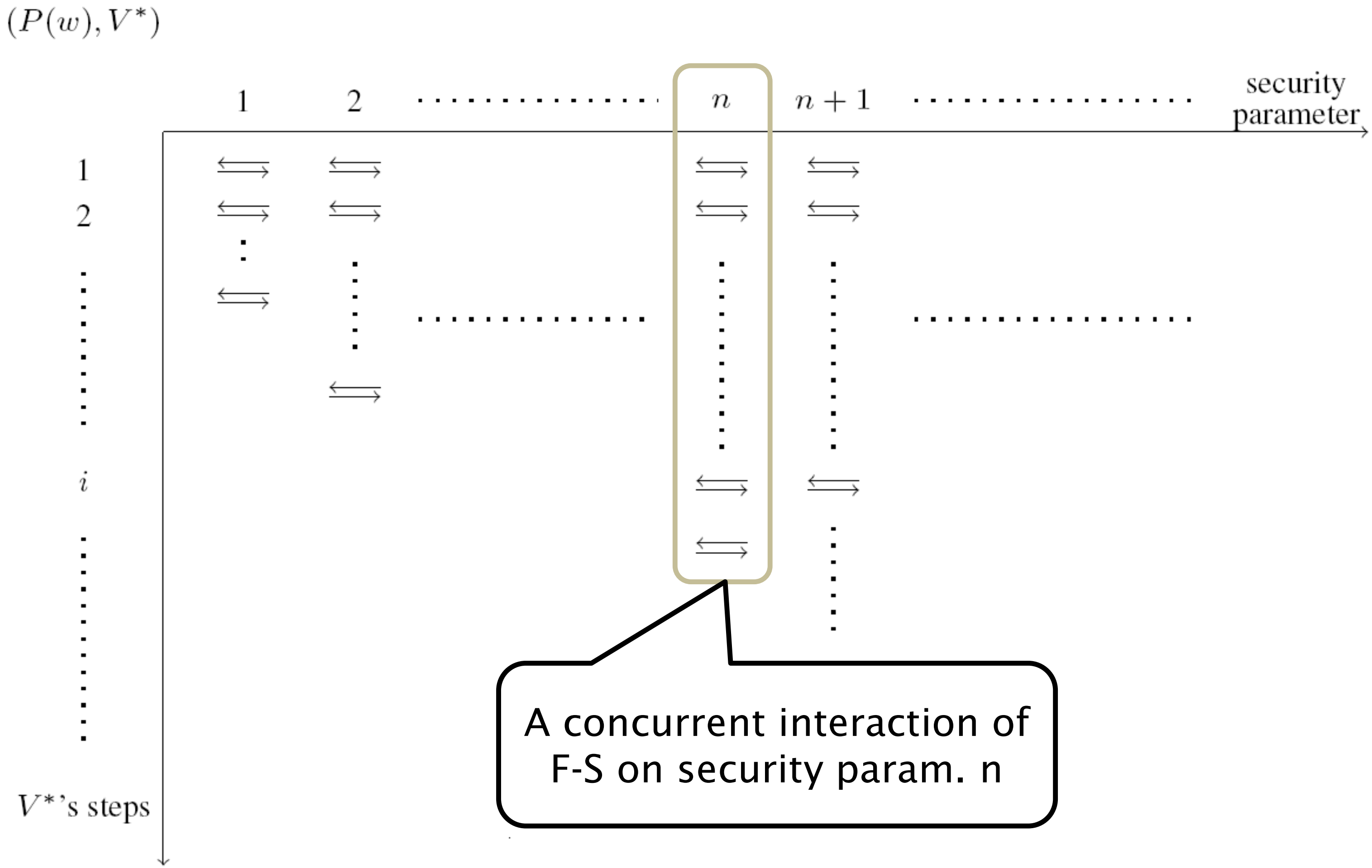
Given the witness w as input, there is a PPT extractor E, E (w,hist, V^*) can extract r_b. (by rewinding)

Without the witness w, no PPT T can extract r_b. (otherwise we will have a simulator for V^*)

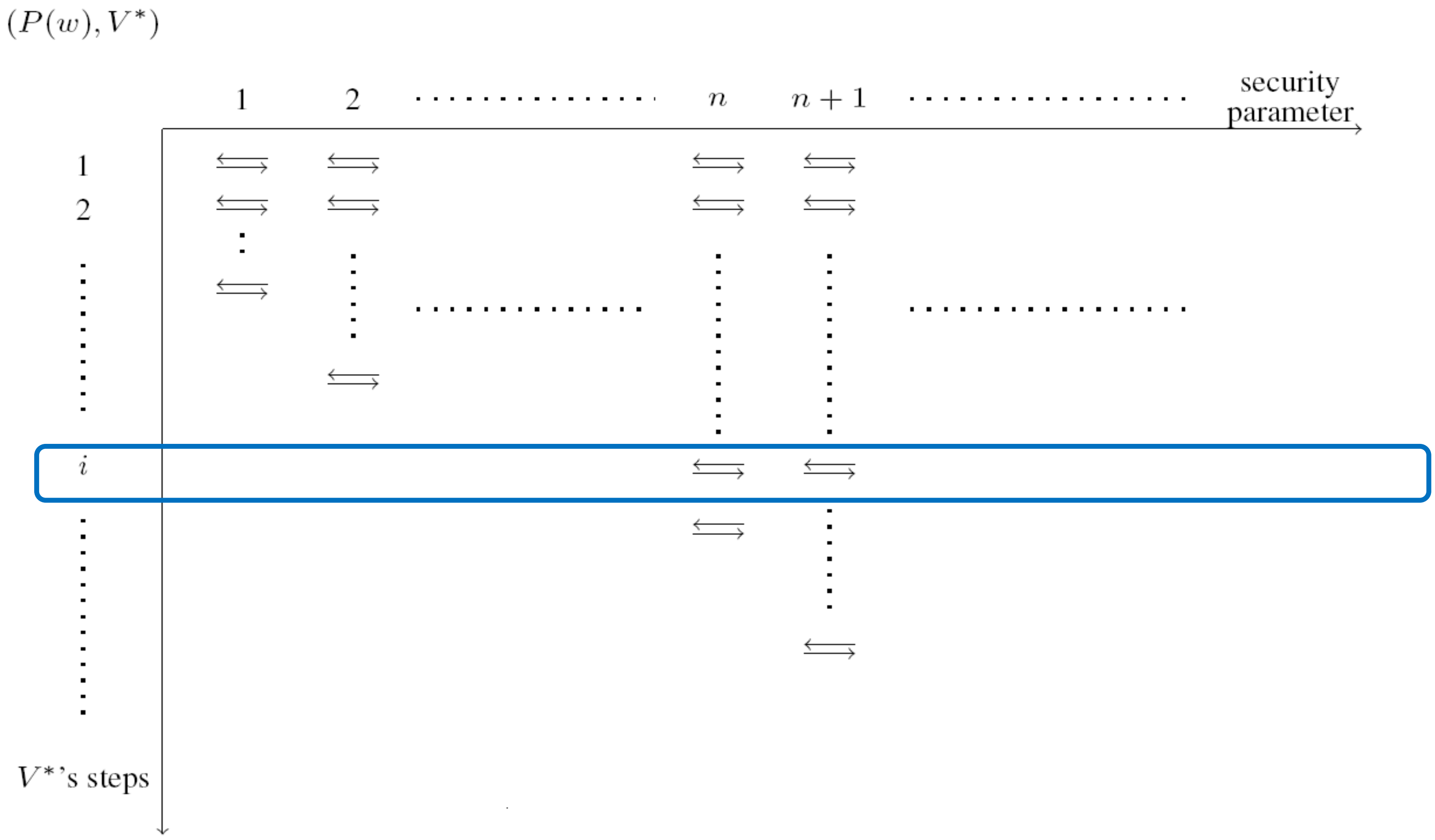
Proof of existence of an infinitely-many set $\{(n, i_n)\}$: A dissection of a magic V



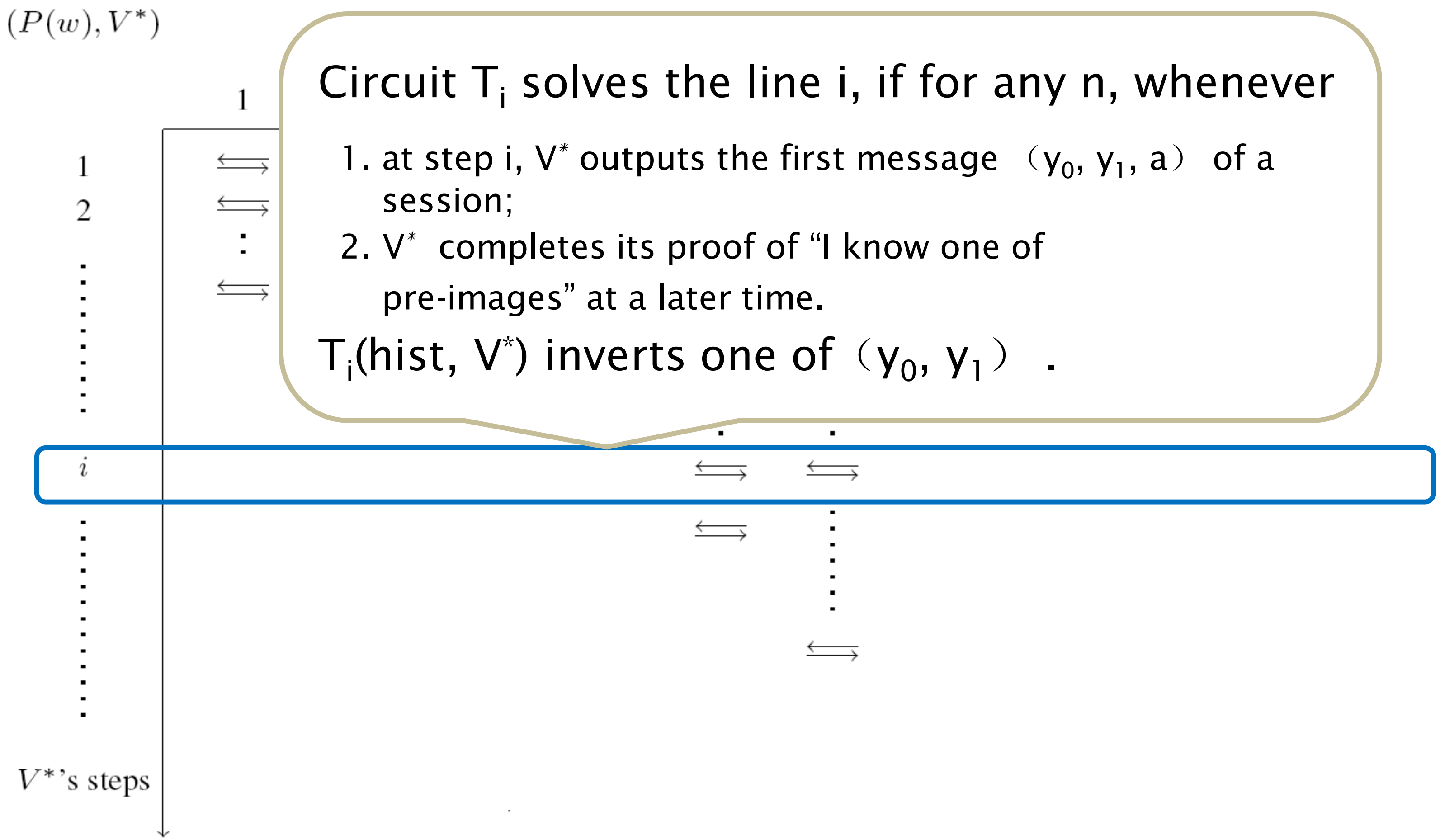
Proof of existence of an infinitely-many set $\{(n, i_n)\}$: A dissection of a magic V



Proof of existence of such an infinitely-many set {(n, i_n)}: A dissection of a magic V



Proof of existence of such an infinitely-many set $\{(n, i_n)\}$: A dissection of a magic V

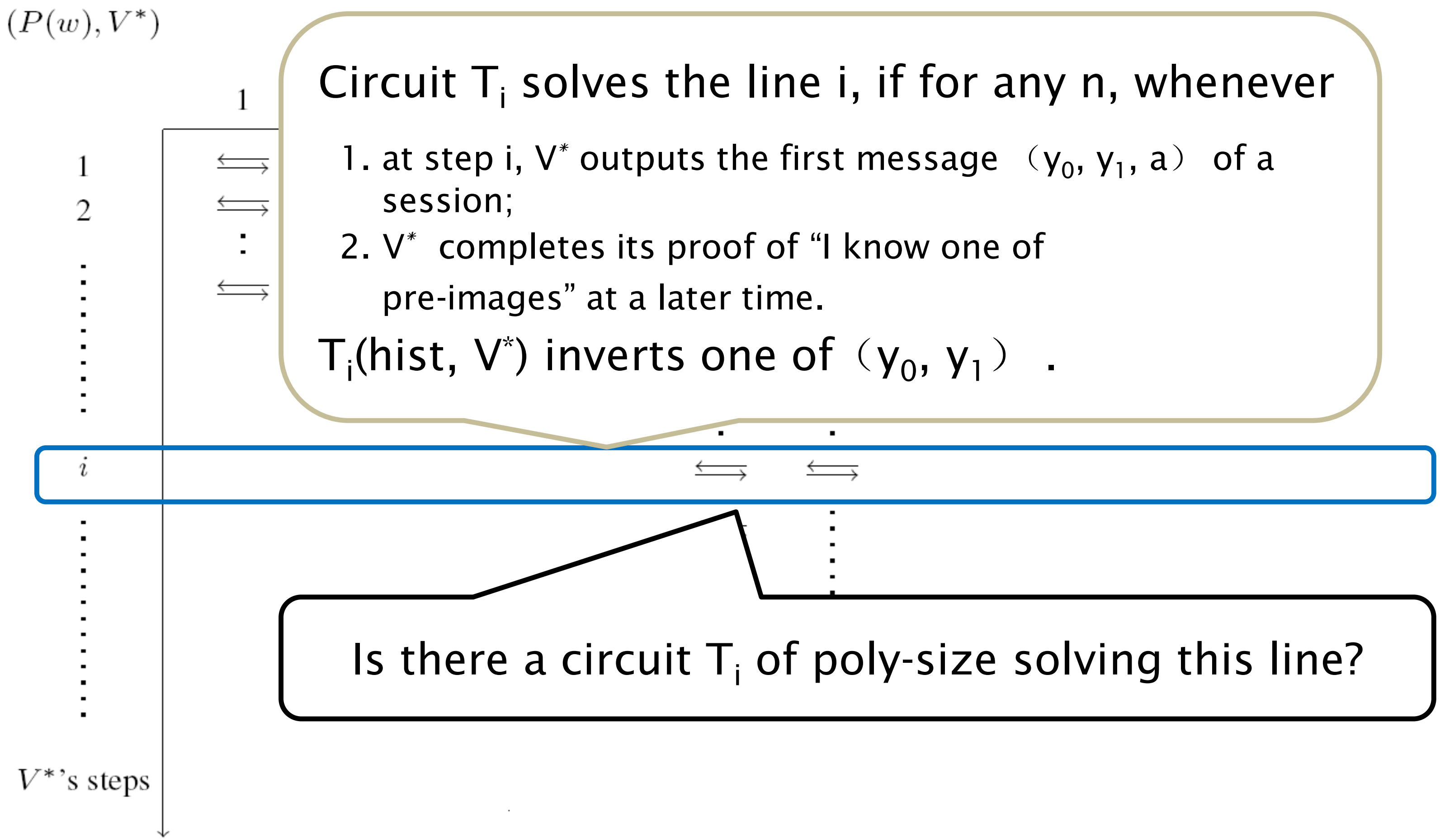


Circuit T_i solves the line i, if for any n, whenever

1. at step i, V^* outputs the first message (y_0, y_1, a) of a session;
2. V^* completes its proof of “I know one of pre-images” at a later time.

$T_i(\text{hist}, V^*)$ inverts one of (y_0, y_1).

Proof of existence of such an infinitely-many set {(n， i_n)}: A dissection of a magic V



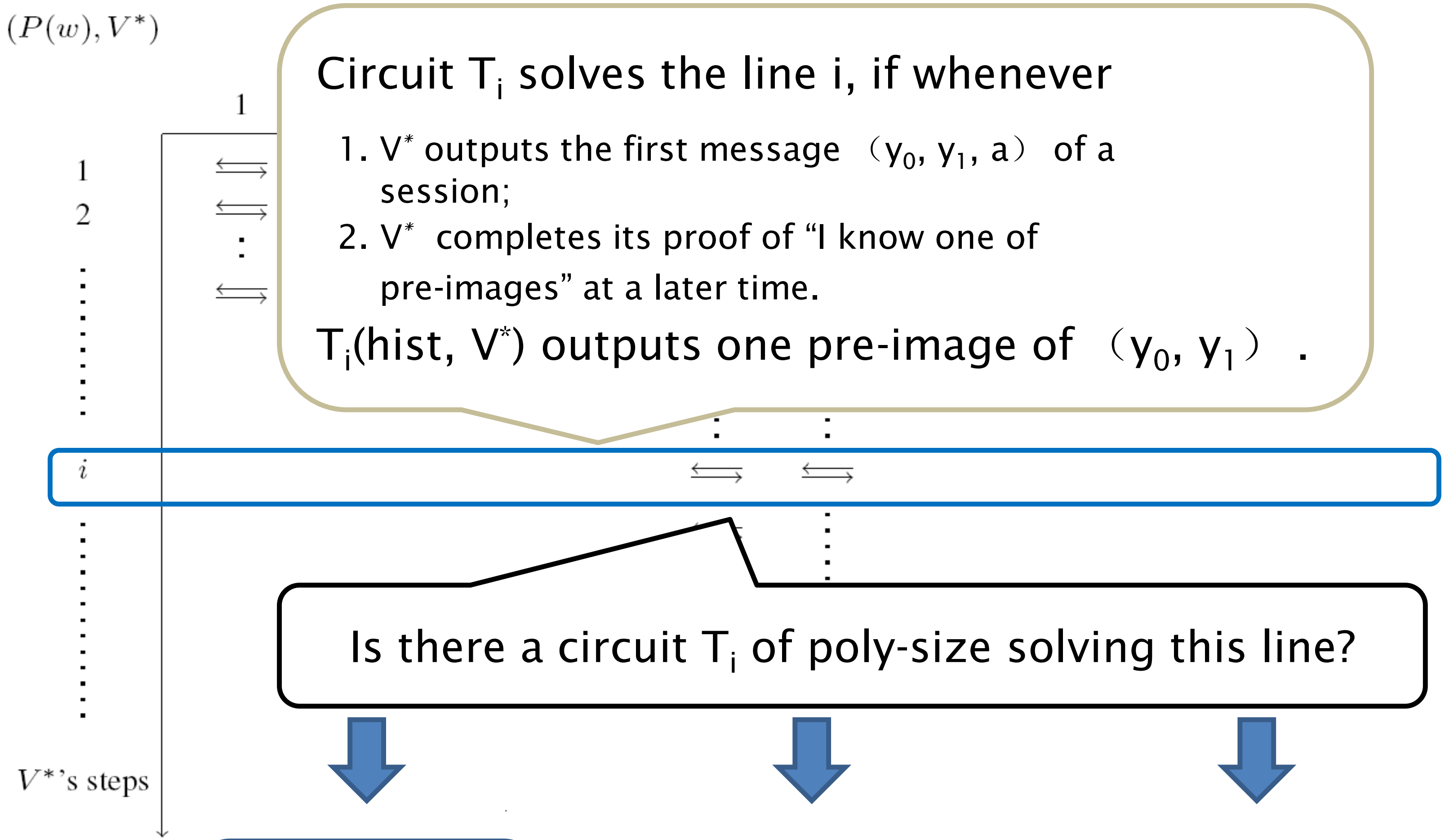
Circuit T_i solves the line i, if for any n, whenever

1. at step i, V^* outputs the first message （y_0, y_1, a） of a session;
2. V^* completes its proof of “I know one of pre-images” at a later time.

T_i(hist, V^*) inverts one of（y_0, y_1）.

Is there a circuit T_i of poly-size solving this line?

Proof of existence of such an infinitely-many set $\{(n, i_n)\}$: A dissection of a magic V



Circuit T_i solves the line i, if whenever

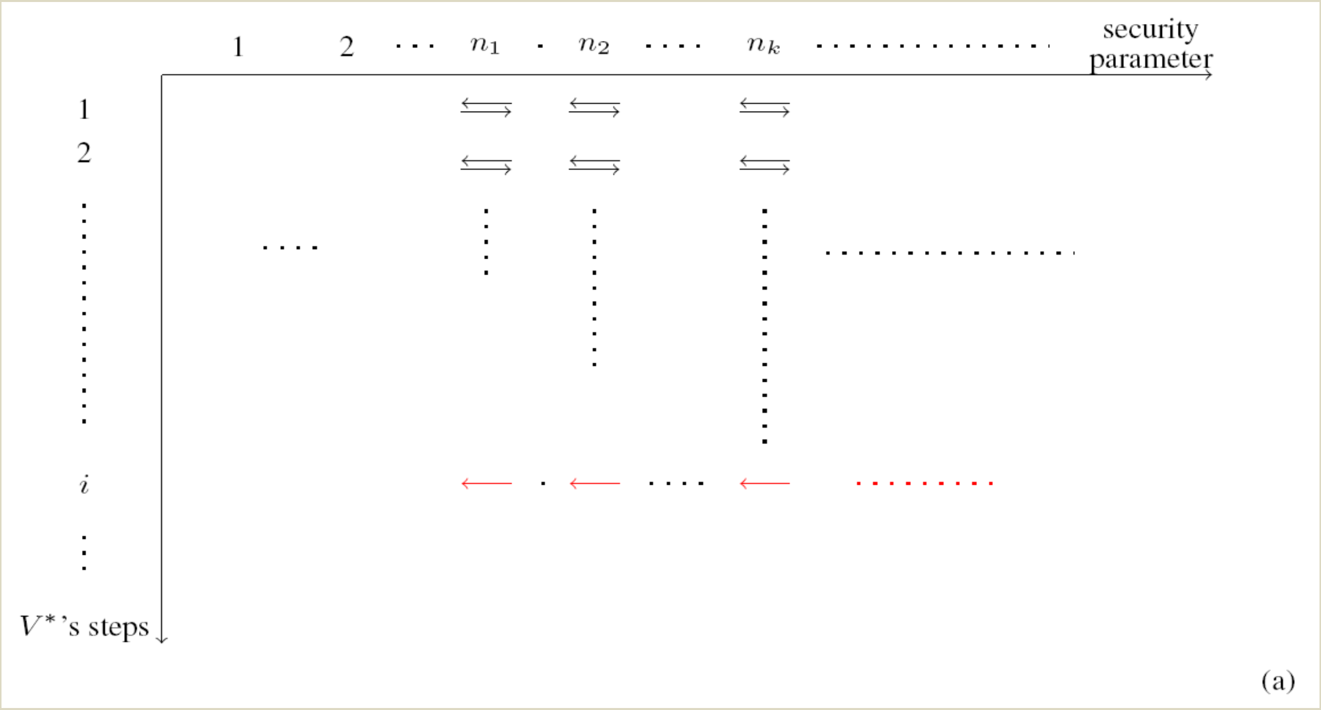
1. V^* outputs the first message (y_0, y_1, a) of a session;
2. V^* completes its proof of “I know one of pre-images” at a later time.

$T_i(\text{hist}, V^*)$ outputs one pre-image of (y_0, y_1).

Is there a circuit T_i of poly-size solving this line?

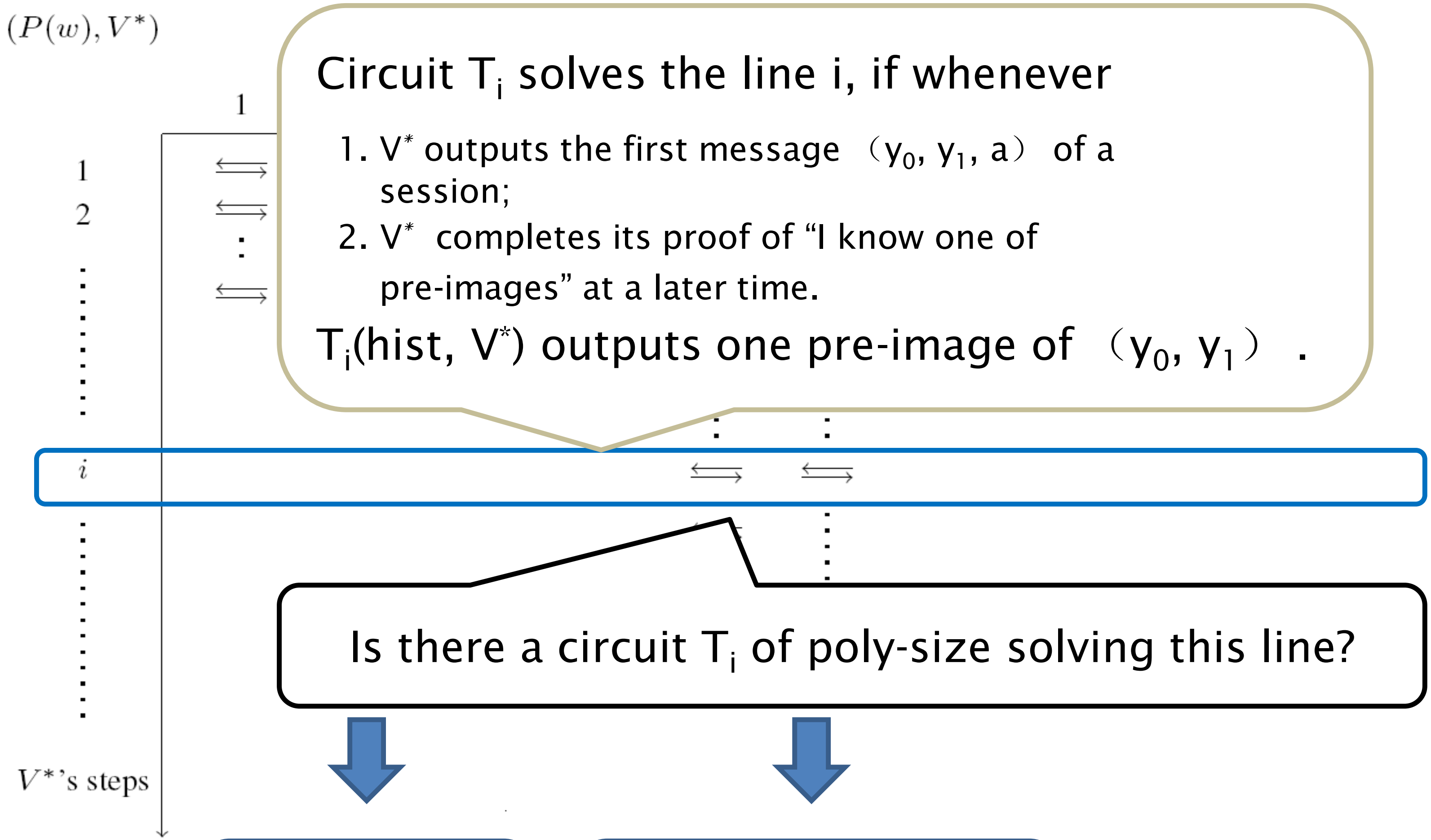
NO.
We are done.

Proof of existence of such an infinitely-many set {(n, i_n)}: A dissection of a magic V



NO.
We are done.

Proof of existence of such an infinitely-many set {(n， i_n)}: A dissection of a magic V



Circuit T_i solves the line i, if whenever

1. V^* outputs the first message （y_0, y_1, a） of a session;
2. V^* completes its proof of "I know one of pre-images" at a later time.

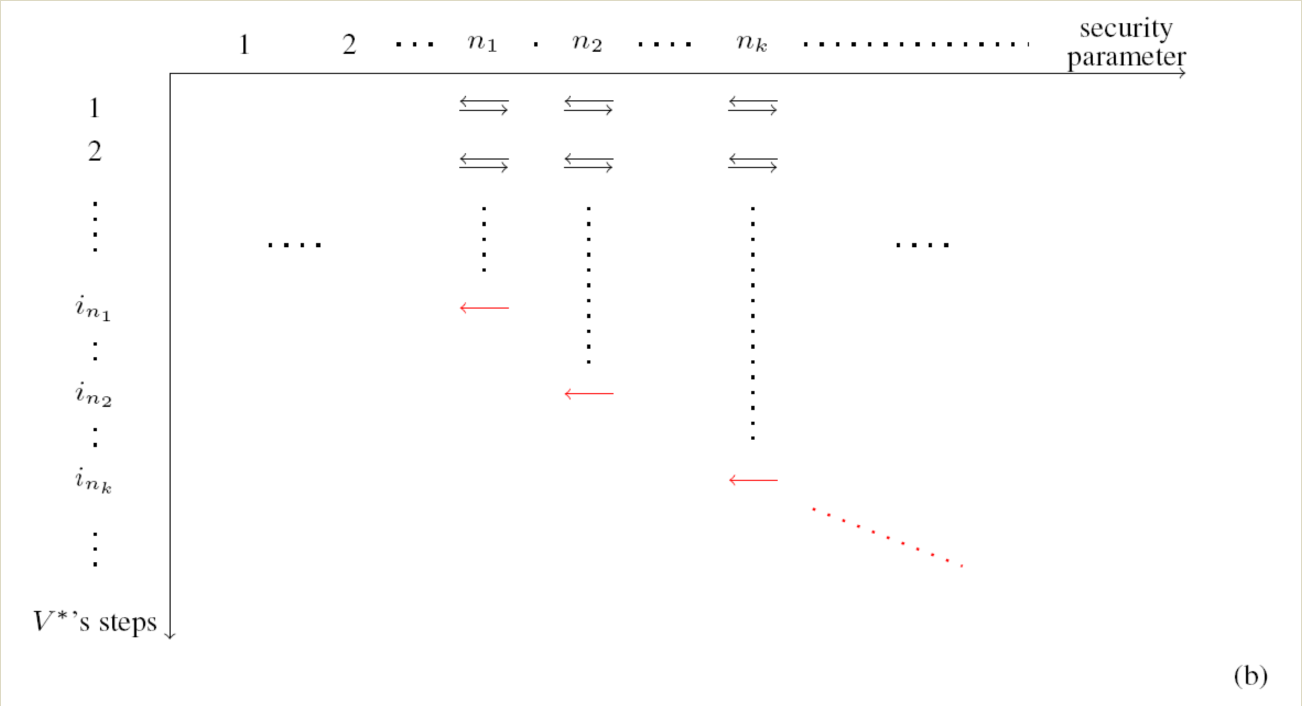
T_i(hist, V^*) outputs one pre-image of （y_0, y_1） .

Is there a circuit T_i of poly-size solving this line?

NO.
We are done.

YES，but requires size P_i，and no poly can upper-bound {P_i}.
We are done.

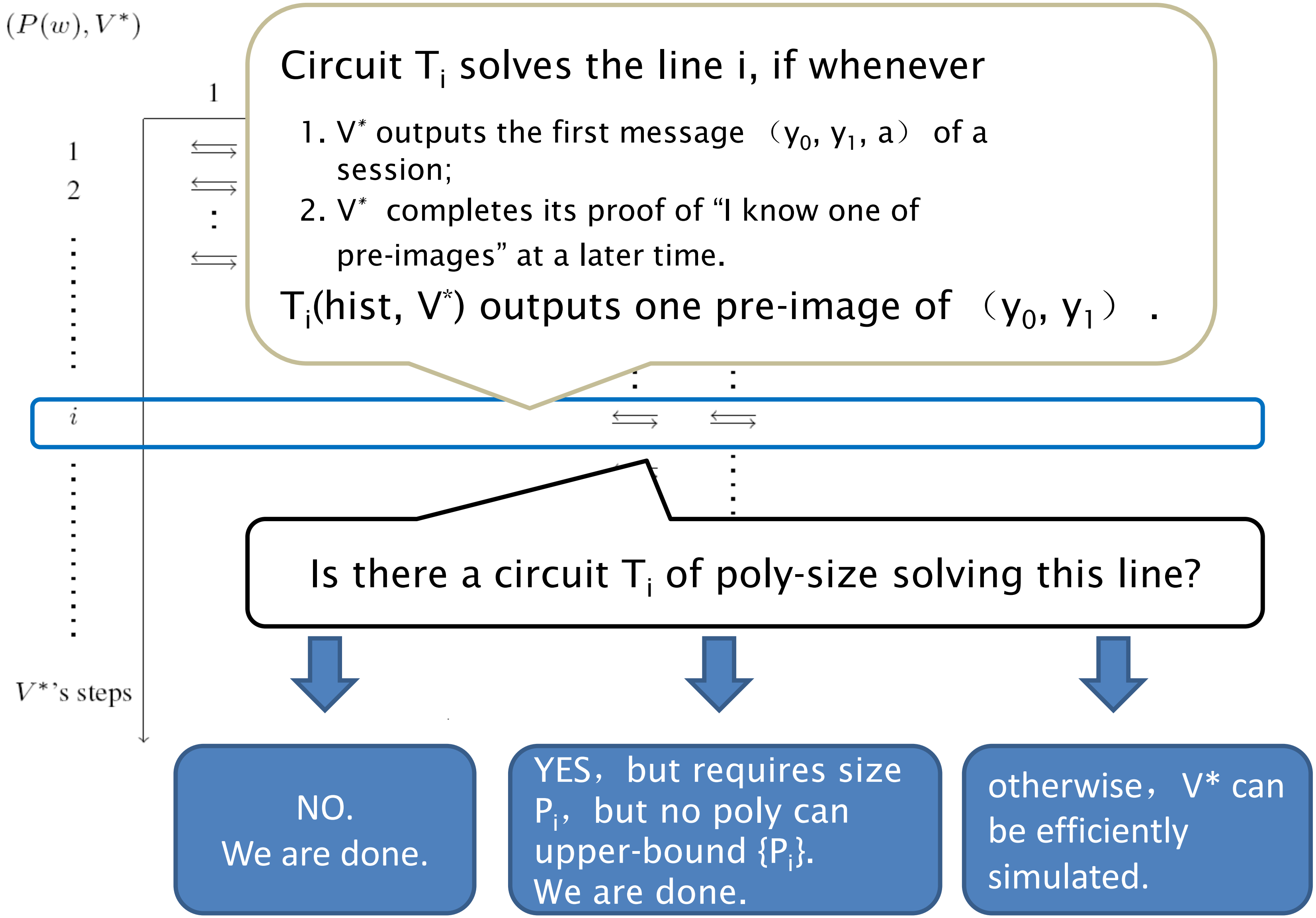
Proof of existence of such an infinitely-many set {(n, i_n)}: A dissection of a magic V



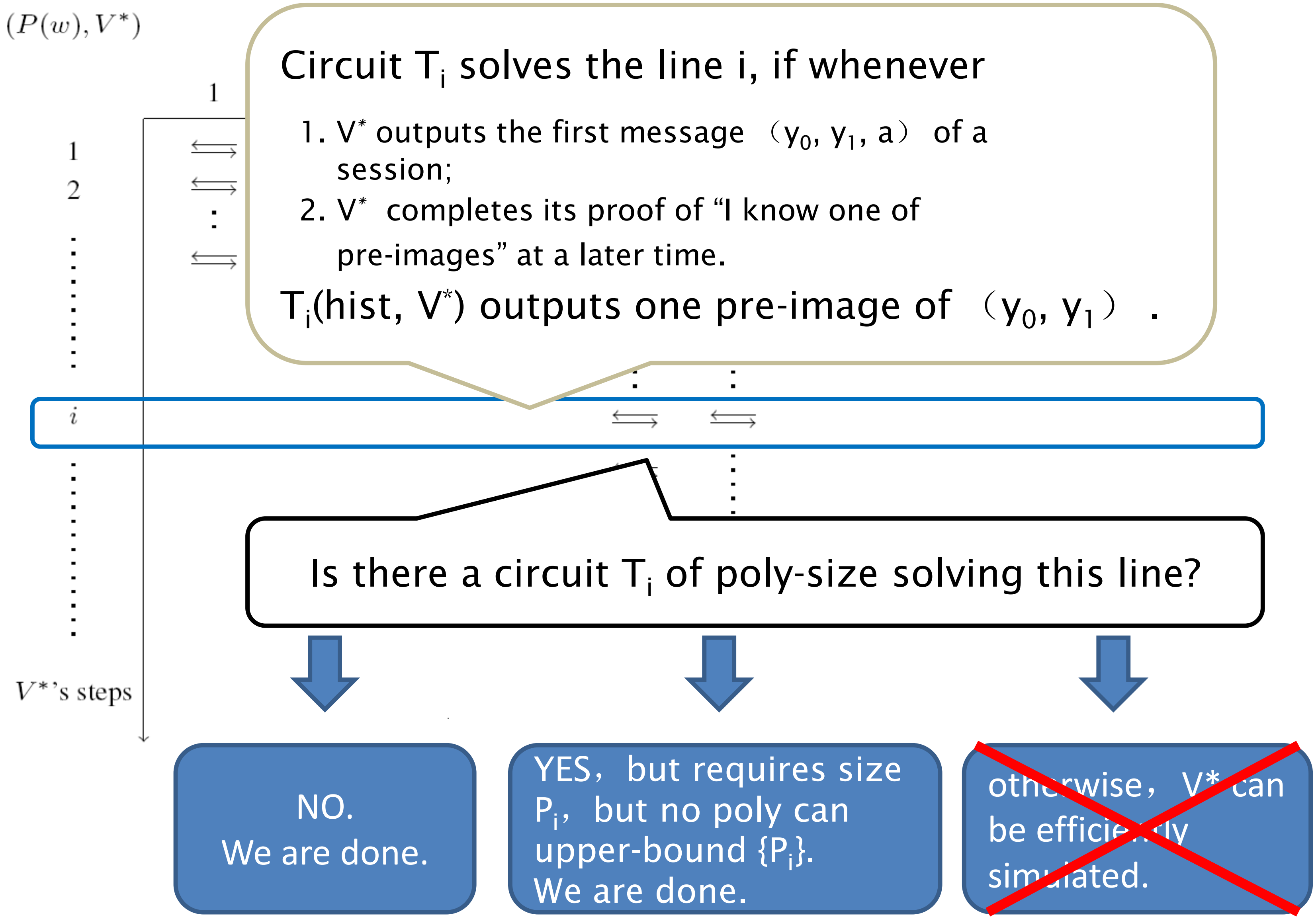
NO.
We are done.

YES, but requires size P_i, and no poly can upper-bound $\{P_i\}$.
We are done.

Proof of existence of such an infinitely-many set $\{(n, i_n)\}$: A dissection of a magic V



Proof of existence of such an infinitely-many set $\{(n, i_n)\}$: A dissection of a magic V



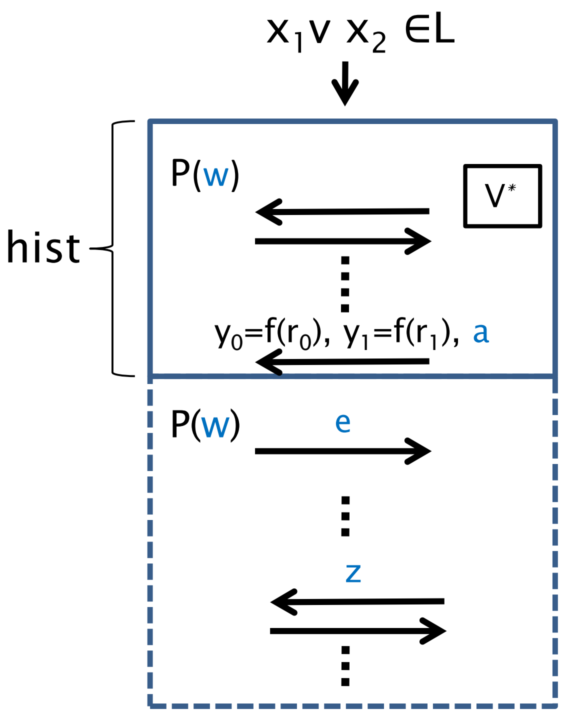
Now suppose that there is a magic V* that breaks the CZK of Feige-Shamir on OR NP-statements $(x_1 v\ x_2)$

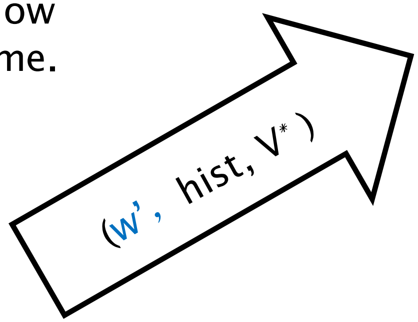
Consequence of a magic adv V^* on $x_1 v\ x_2$ *(oversimplified)*

There are infinitely many n, for each n

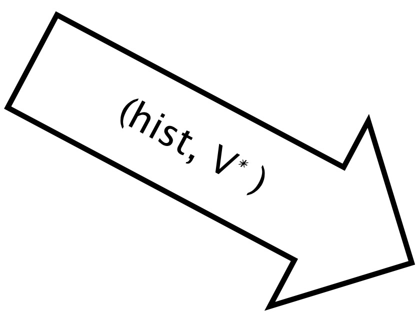
∃ V^*' step i_n

1. At setp i_n, V^* outputs the first message (y_0, y_1, a) of a session;
2. V^* completes its proof of "I know one of preimages" at a later time.





Given the witness w' as input, there is a PPT extractor E, E (w',hist, V^*) can extract r_b.
(by rewinding)



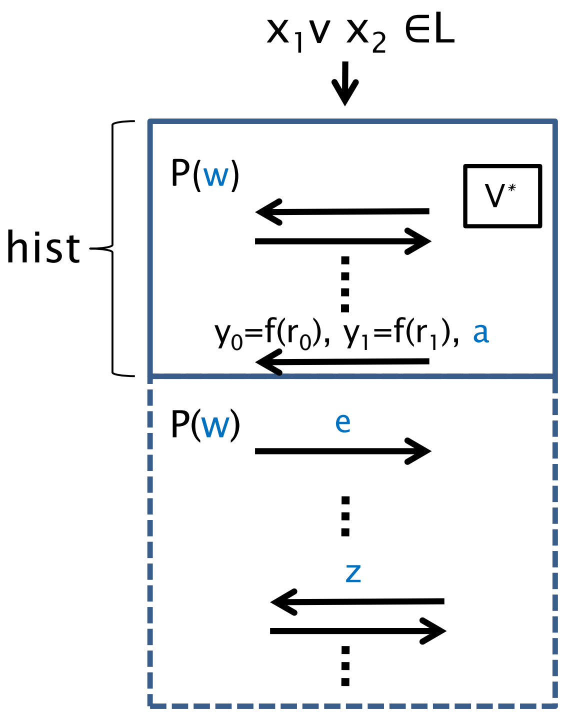
Without knowledge of any witness w, NO PPT T can extract r_b.
(otherwise we will have a simulator for V^*)

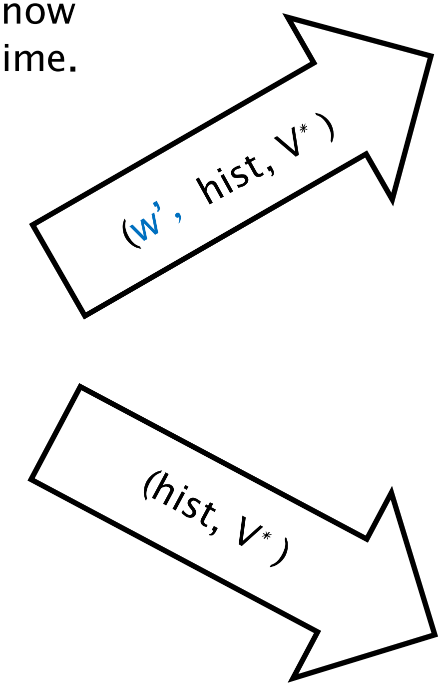
Consequence of a magic adv V^* on $x_1 \vee x_2$ *(oversimplified)*

There are infinitely many n, for each n

$\exists$ V^* ' step i_n

1. At setp i_n, V^* outputs the first message （y_0, y_1, a） of a session;
2. V^* completes its proof of "I know one of preimages" at a later time.





Given the witness w' as input, there is a PPT extractor E, E (w',hist, V^*) can extract r_b. (by rewinding)

Any valid witness to $x_1 \vee x_2$ will work due to concurrent WI of the Feige-Shamir.

Without knowledge of any witness w, NO PPT T can extract r_b.
(otherwise we will have a simulator for V^*)

Consequence of a magic adv V^* on $x_1 v\ x_2$ *(oversimplified)*

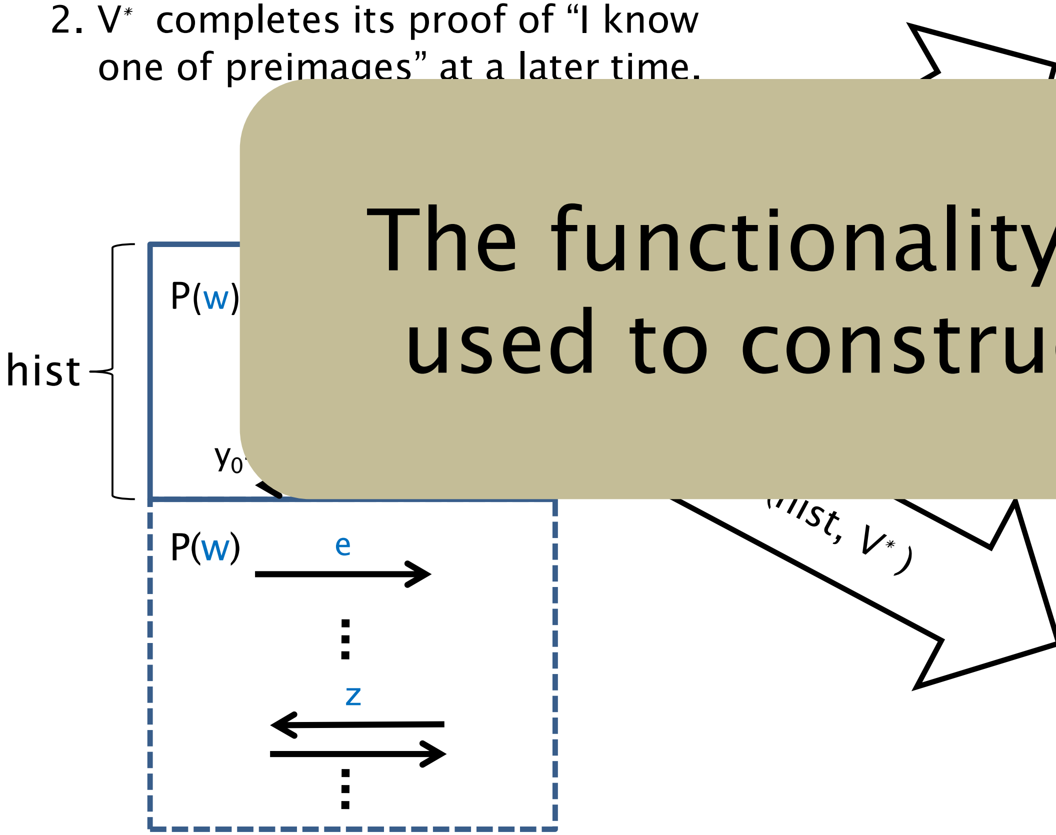
There are infinitely many n, for each n

$\exists$ V^*' step i_n

1. At setp i_n, V^* outputs the first message （y_0, y_1, a） of a session;
2. V^* completes its proof of “I know one of preimages” at a later time.

Given the witness w’ as input, there is a PPT extractor E, E (w’,hist, V^*) can extract r_b.

The functionality of V^* can be used to construct a PKE/KE.



Without knowledge of any witness w, NO PPT T can extract r_b.

(otherwise we will have a simulator for V^*)

PKE/KE from Injective OWF（high-level idea）

Session key k ∈{0,1}

A

B(k)

PKE/KE from Injective OWF（high-level idea）

Session key $k \in \{0,1\}$

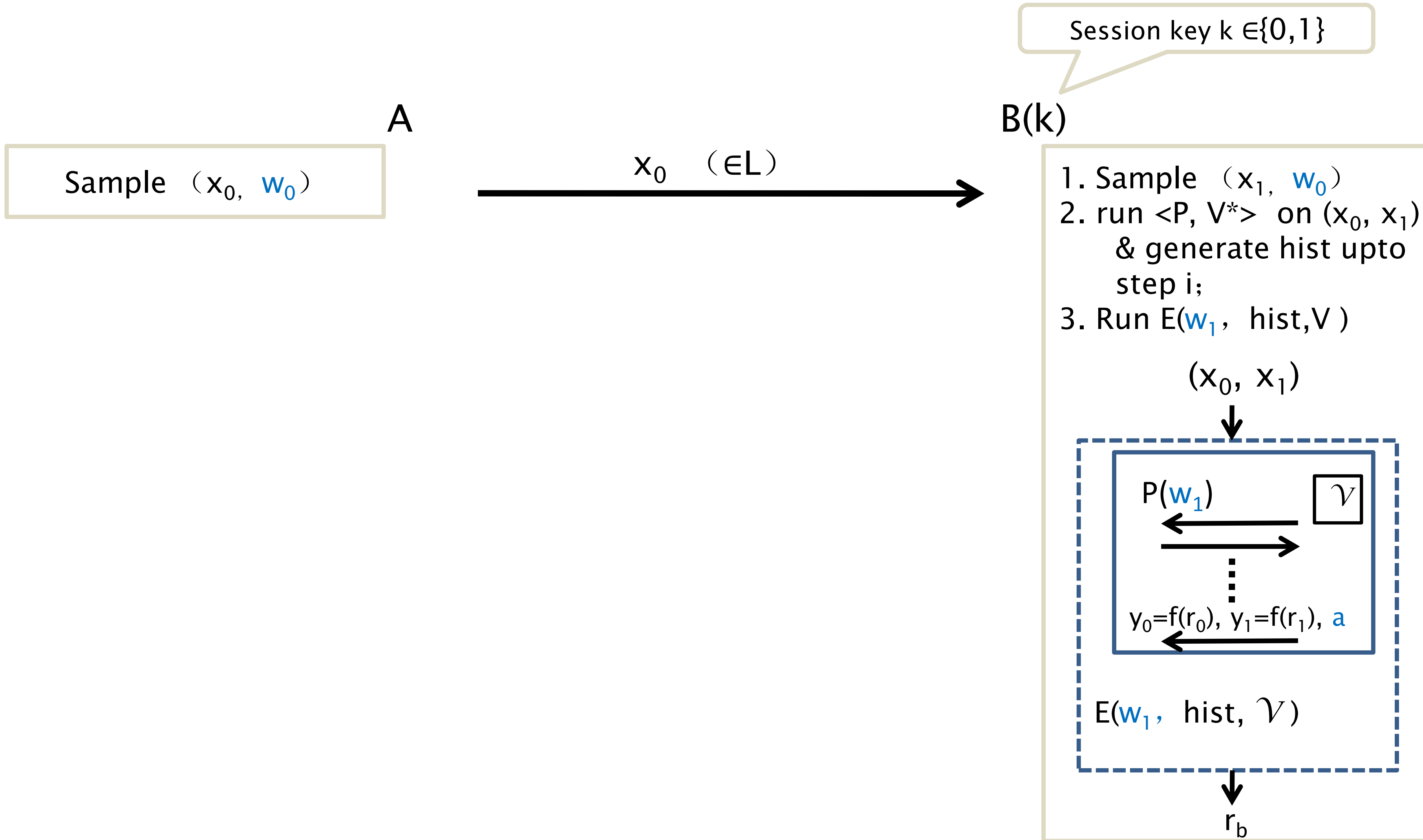
A

B(k)

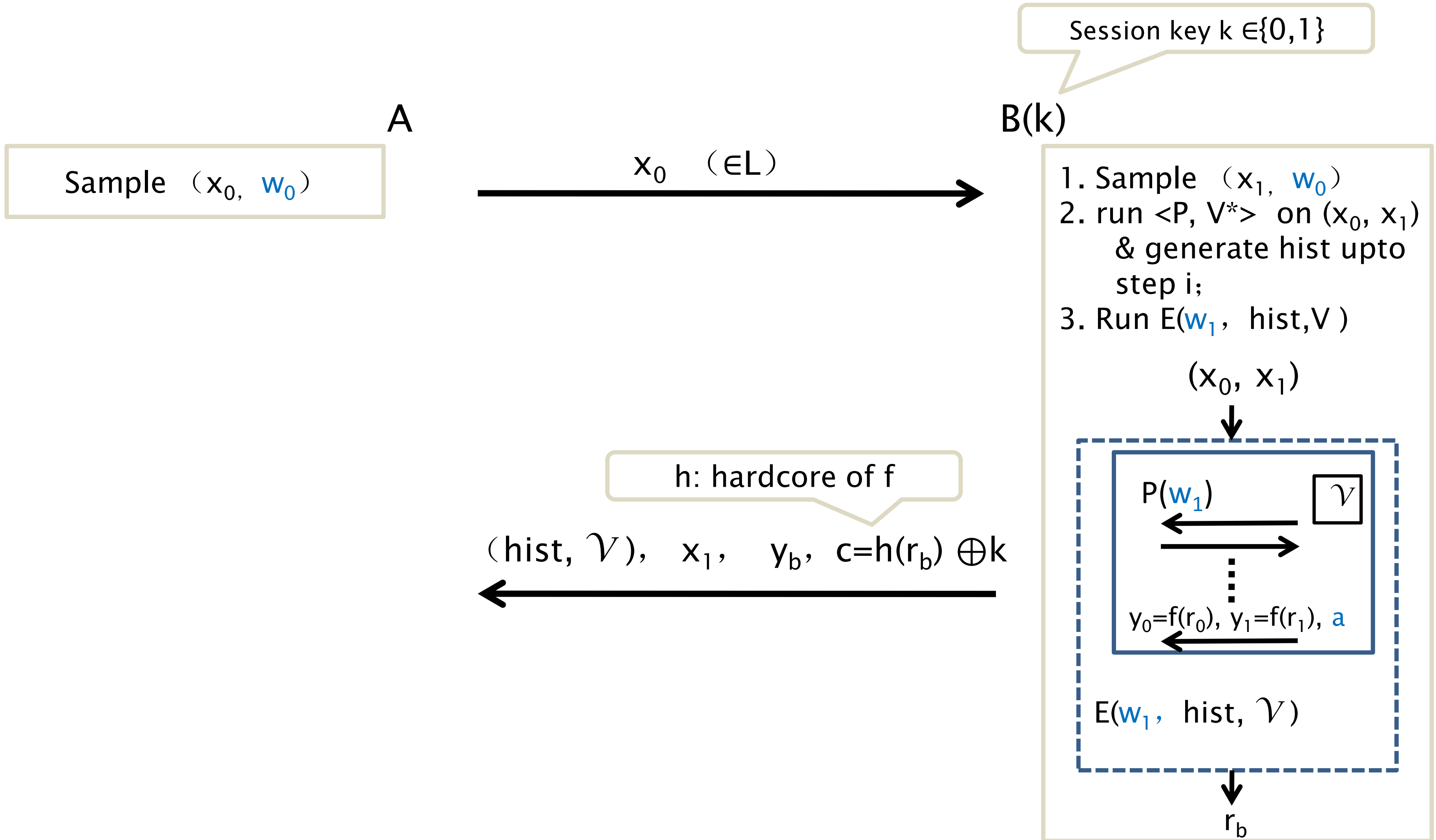
Sample（x_0, w_0）

x_0 （$\in L$）→

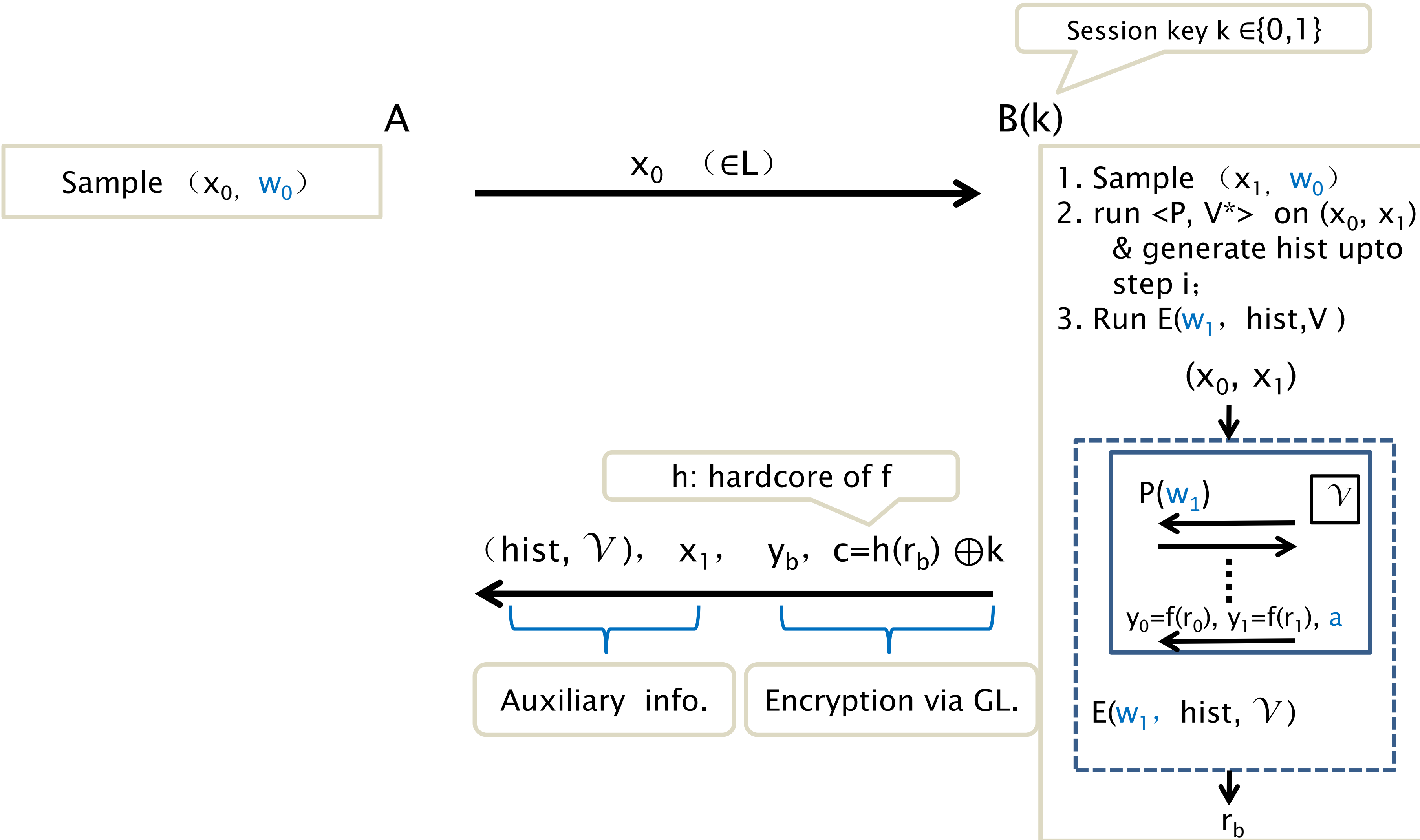
PKE/KE from Injective OWF（high-level idea）



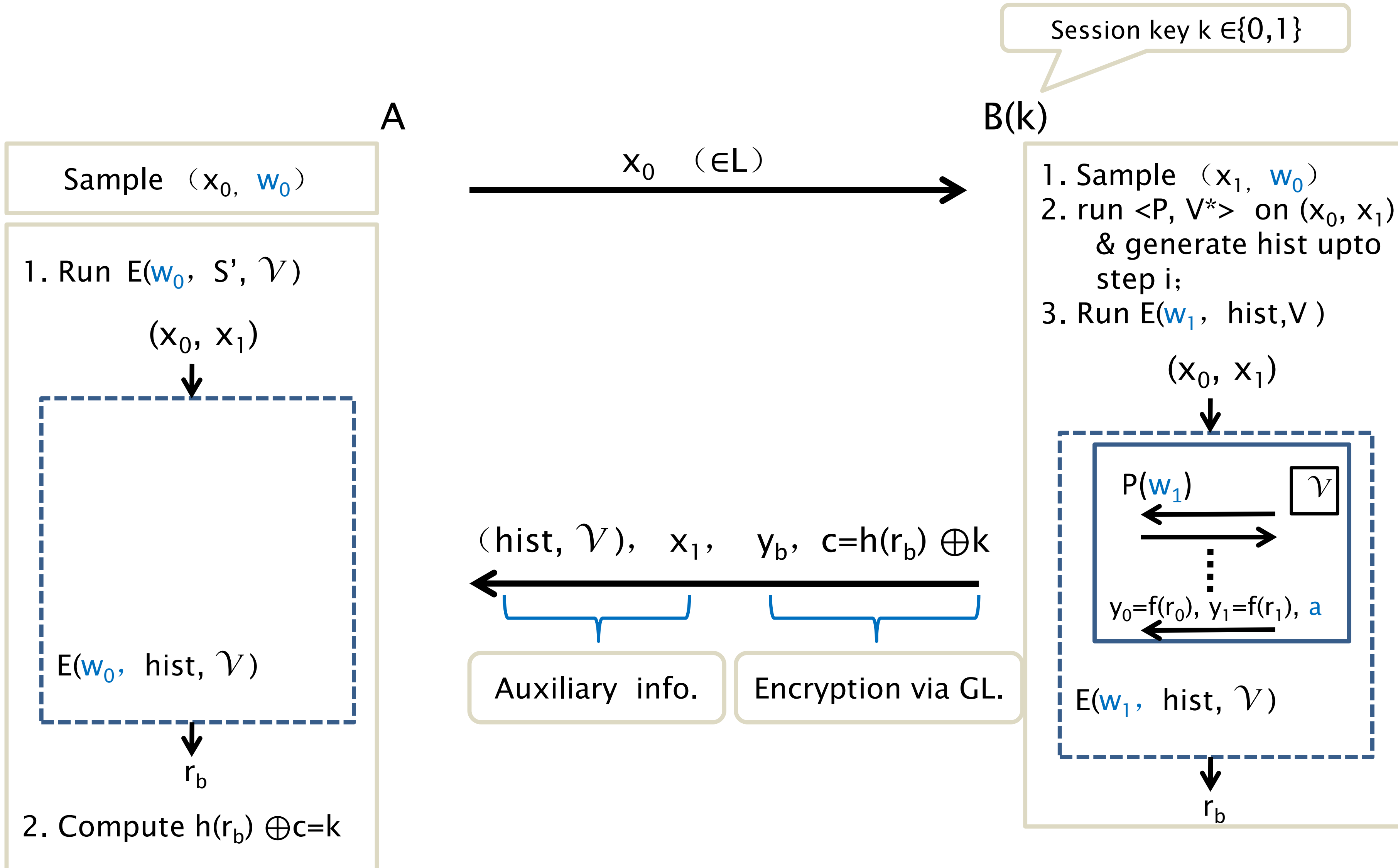
PKE/KE from Injective OWF（high-level idea）



PKE/KE from Injective OWF（high-level idea）



PKE/KE from Injective OWF（high-level idea）



Caveats:

Caveats:

- For the key gen algorithm of our encryption to work, we need a V* that breaks *epsilon-Distributional* concurrent ZK;

Caveats:

- For the key gen algorithm of our encryption to work, we need a V* that breaks *epsilon-Distributional* concurrent ZK;

- V* may output the first msg (a pair of images of f) at its step i (and complete the corresponding WI proof) *with some (non-negl) probability< 1*, which will introduce some error to our encryption and decryption algs.
  We use standard technique （parallel repetition）to reduce this kind of error.

Summary

We prove an ugly theorem:

Assume one-way function exists, then one of the following statements must be true:

1. (infinitely-often) PKE/KE exist.

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR NP-statements with small dist. gap.

$\forall$ V* $\exists$ S

$\exists$ S $\forall$ V*

Thank you!

We prove an ugly theorem:

Assume one-way function exists, then one of the following statements must be true:

1. (infinitely-often) PKE/KE exist.

> If this is true, we don't need trapdoor/algebraic structure for PKE anymore

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR NP-statements with small dist. gap.

$\forall$ V* $\exists$ S

$\exists$ S $\forall$ V*

Thank you!

We prove an ugly theorem:

Assume one-way function exists, then one of the following statements must be true:

1. (infinitely-often) PKE/KE exist.

> If this is true, we don't need trapdoor/algebraic structure for PKE anymore

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR NP-statements with small dist. gap.

> If this is true, then standalone=concurrent (self composition), and we have a new individual reduction (different from the traditional universal reduction)

$\forall V^* \exists S$ $\exists S \forall V^*$

Thank you!

We prove an ugly theorem:

Assume one-way function exists, then one of the following statements must be true:

1. (infinitely-often) PKE/KE exist.

If this is true, we don't need trapdoor/algebraic structure for PKE anymore

2. The 4-round Feige-Shamir protocol is distributional concurrent ZK for OR NP-statements with small dist. gap.

If this is true, then standalone=concurrent (self composition), and we have a new individual reduction (different from the traditional universal reduction)

$\forall V^* \exists S$

$\exists S \forall V^*$

Thank you!