Statistical Zaps and New Oblivious Transfer Protocols

Vipul Goyal
Carnegie Mellon University

Abhishek Jain
Johns Hopkins University

Zhengzhong Jin
Johns Hopkins University

Giulio Malavolta
Carnegie Mellon University
University of California, Berkeley

Statistical Security in 2-party Protocols

Statistical Security in 2-party Protocols

- **Everlasting security** Computational unbounded adversary can't break.

- **Hard to achieve**
  - Impossible for *both* parties to achieve for general functionalities

- **Focus of this work:** One-side Statistical Security
  - Interactive Proof Systems: Statistical Privacy for Prover
  - Oblivious Transfer: Statistical Privacy for Receiver

Statistical Security in 2-party Protocols

- **Everlasting security** Computational unbounded adversary can't break.

- **Hard to achieve**
  - Impossible for *both* parties to achieve for general functionalities

- **Focus of this work:** One-side Statistical Security
  - Interactive Proof Systems: Statistical Privacy for Prover
  - Oblivious Transfer: Statistical Privacy for Receiver

Interactive Proof System

Prover

ω : witness

$x \in L$

Verifier

Interactive Proof System

Prover

$x \in L$

Verifier

ω : witness

Interactive Proof System

Prover

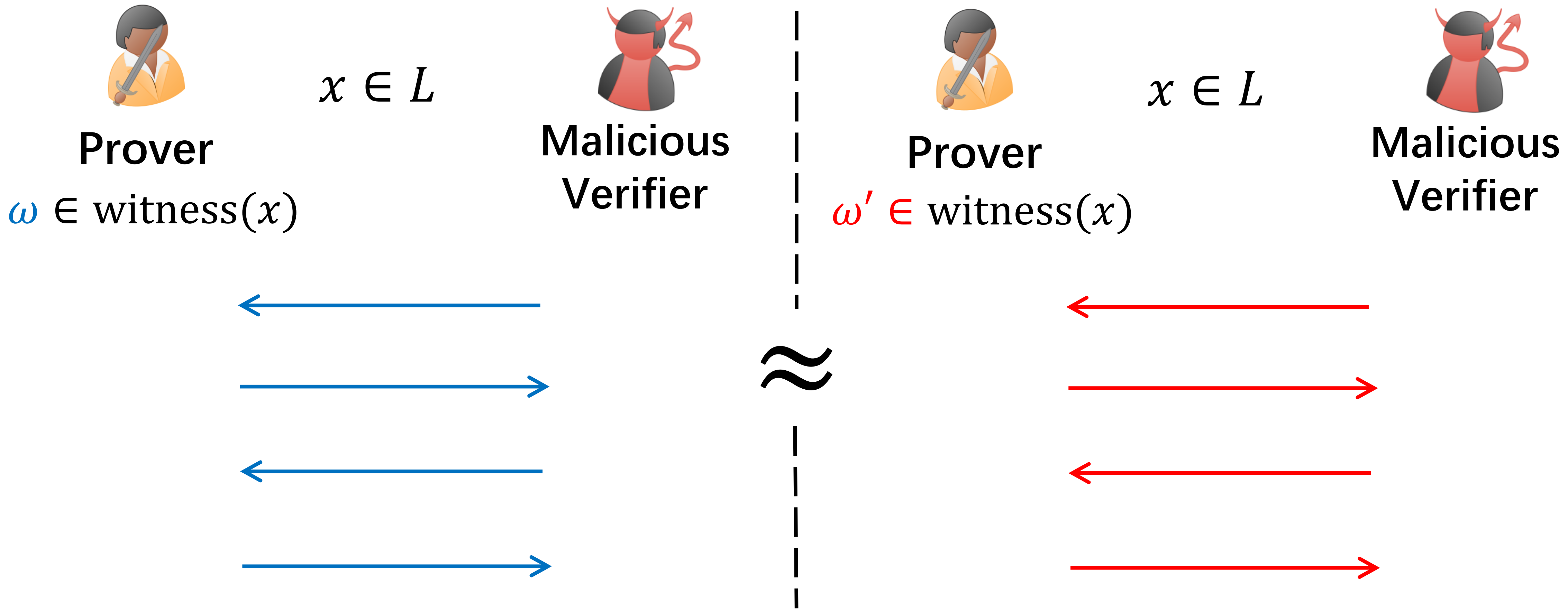
ω : witness

$x \in L$

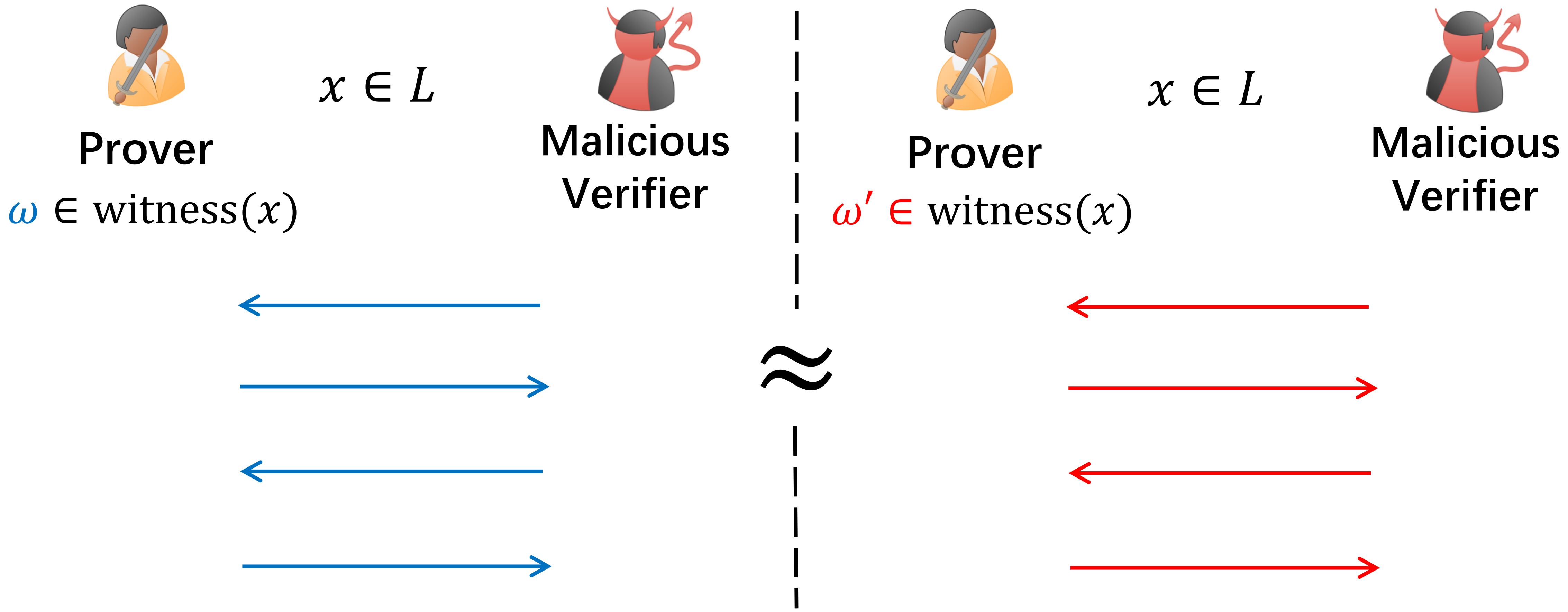
Verifier

Accept/Reject

Witness Indistinguishability (WI)



Witness Indistinguishability (WI)



- Unlike zero-knowledge, WI can be achieved in 2-round

Zaps: 2-round Public-Coin WI [DN00]

Prover

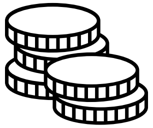
$x \in L$

Verifier

Zaps: 2-round Public-Coin WI [DN00]

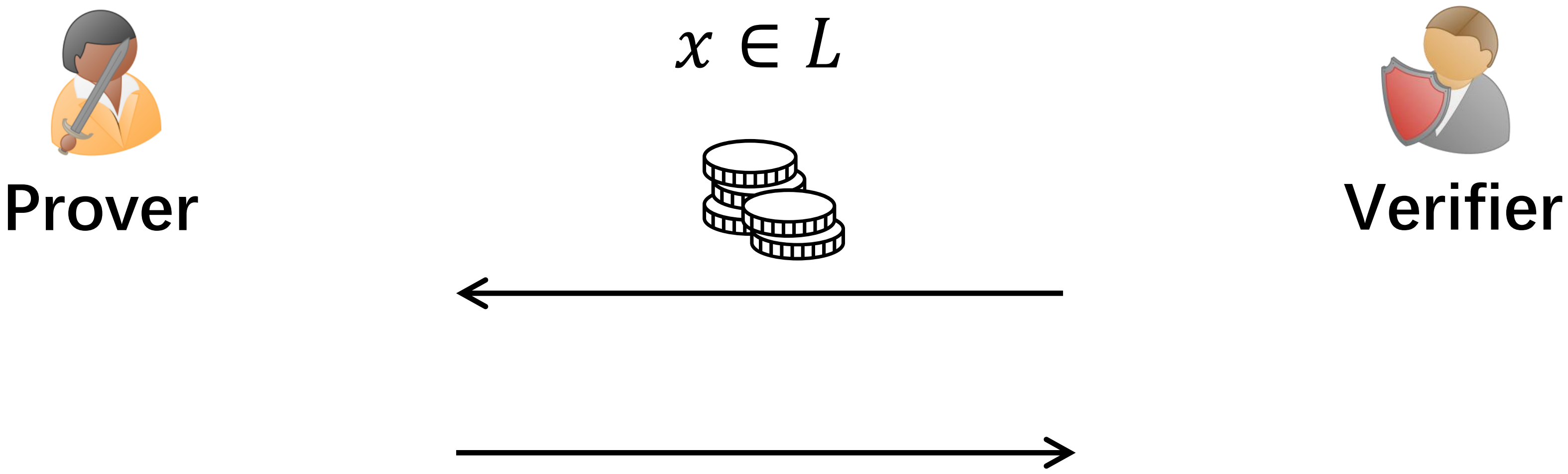
Prover

$x \in L$

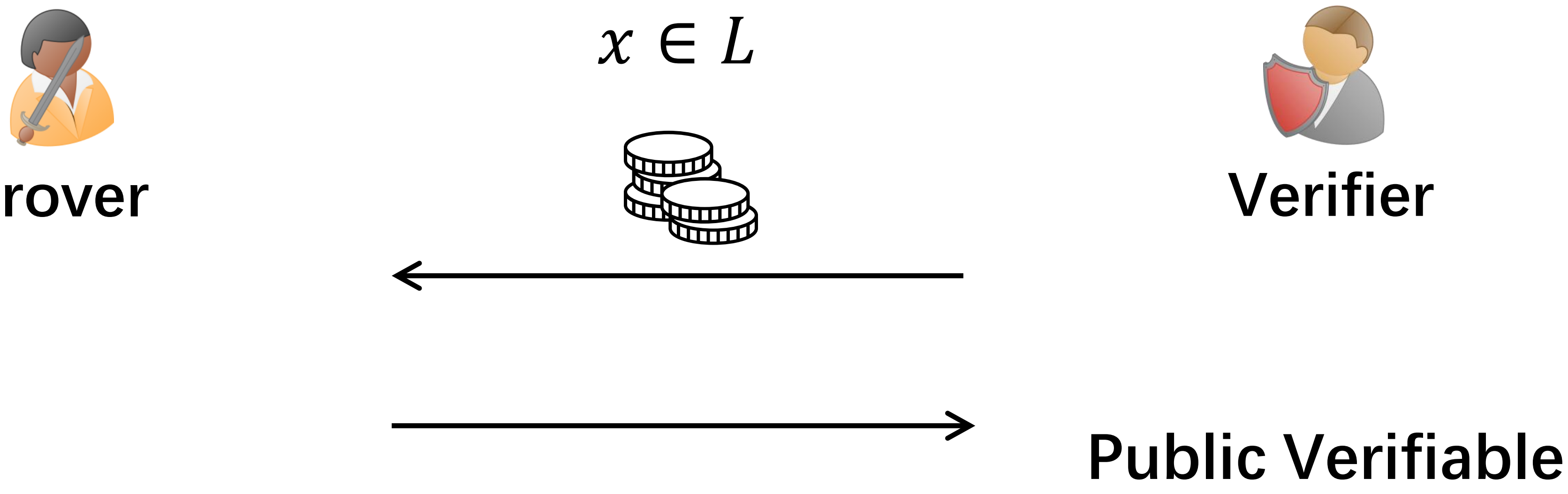


Verifier

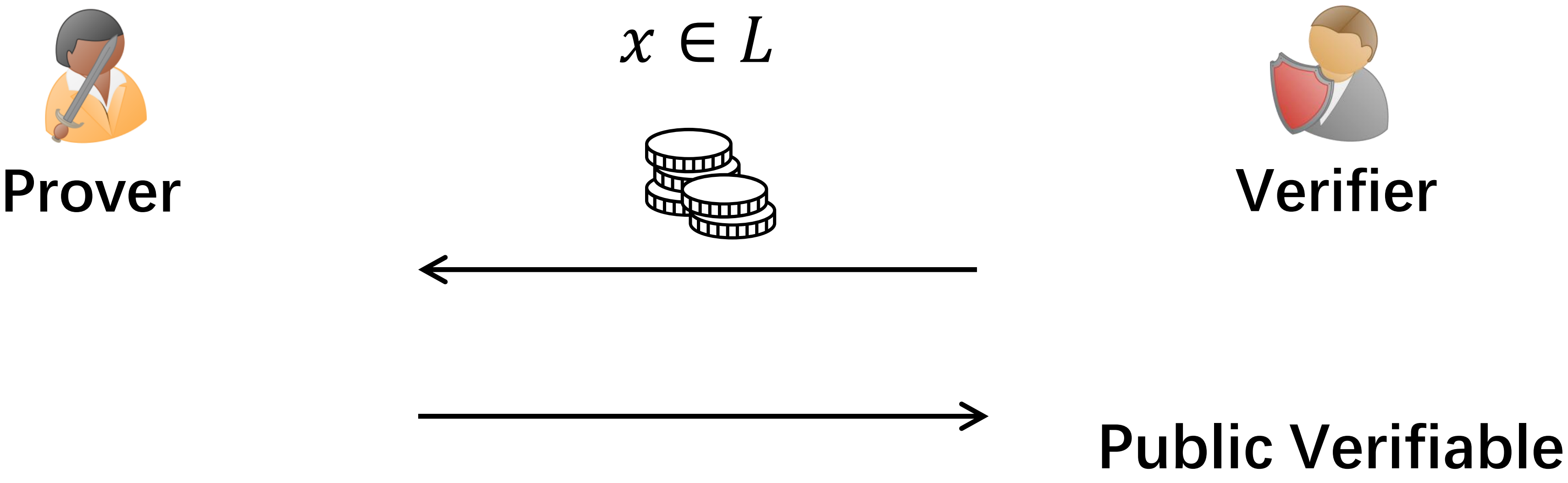
Zaps: 2-round Public-Coin WI [DN00]



Zaps: 2-round Public-Coin WI [DN00]

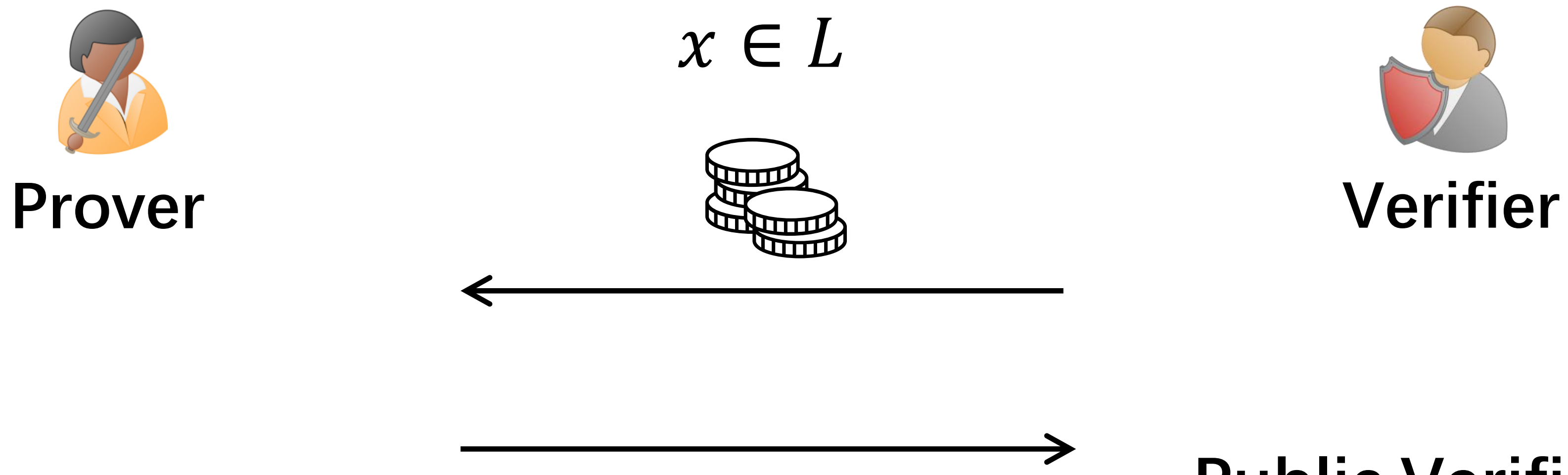


Zaps: 2-round Public-Coin WI [DN00]



Public Coin: Verifier only uses public random coins

Zaps: 2-round Public-Coin WI [DN00]



Public Verifiable

Public Coin: Verifier only uses public random coins

Many Applications:

- Round-efficient secure multiparty computation [HHPV18]
- Resettable-secure protocols [DGS09]

……

Previous Works

[DN00] Zaps and NIZK proofs in common random string model are equivalent.

Previous Works

[DN00] Zaps and NIZK proofs in common random string model are equivalent.

NIZKs

- Quadratic Residuosity Assumption [DMP88]
- Trapdoor permutation [FLS90]
- Decisional Linear Assumption [GOS06]

Previous Works

[DN00] Zaps and NIZK proofs in common random string model are equivalent.

NIZKs

- Quadratic Residuosity Assumption [DMP88]
- Trapdoor permutation [FLS90]
- Decisional Linear Assumption [GOS06]

Previous Works

[DN00] Zaps and NIZK proofs in common random string model are equivalent.

NIZKs

- Quadratic Residuosity Assumption [DMP88]
- Trapdoor permutation [FLS90]
- Decisional Linear Assumption [GOS06]

→ **Zaps**

Previous Works

[DN00] Zaps and NIZK proofs in common random string model are equivalent.

NIZKs

- Quadratic Residuosity Assumption [DMP88]
- Trapdoor permutation [FLS90]
- Decisional Linear Assumption [GOS06]

→ **Zaps**

- [BP15] Zaps from Indistinguishability Obfuscation
- Above works are ***computational*** Zap proofs

Previous Works

[DN00] Zaps and NIZK proofs in common random string model are equivalent.

NIZKs

- Quadratic Residuosity Assumption [DMP88]
- Trapdoor permutation [FLS90]
- Decisional Linear Assumption [GOS06]

Zaps

- [BP15] Zaps from Indistinguishability Obfuscation
- Above works are ***computational*** Zap proofs

Question (1): Does there exist statistical Zaps?

Question (1): Does there exist statistical Zaps?

Result (1): Statistical Zaps from quasi-poly hard Learning with Errors

Question (1): Does there exist statistical Zaps?

Result (1): Statistical Zaps from quasi-poly hard Learning with Errors

[KKS18] achieves statistical *private-coin* WI.

Oblivious Transfer (OT)

Sender

m_0	m_1

Receiver

$\beta \in \{0,1\}$

Oblivious Transfer (OT)

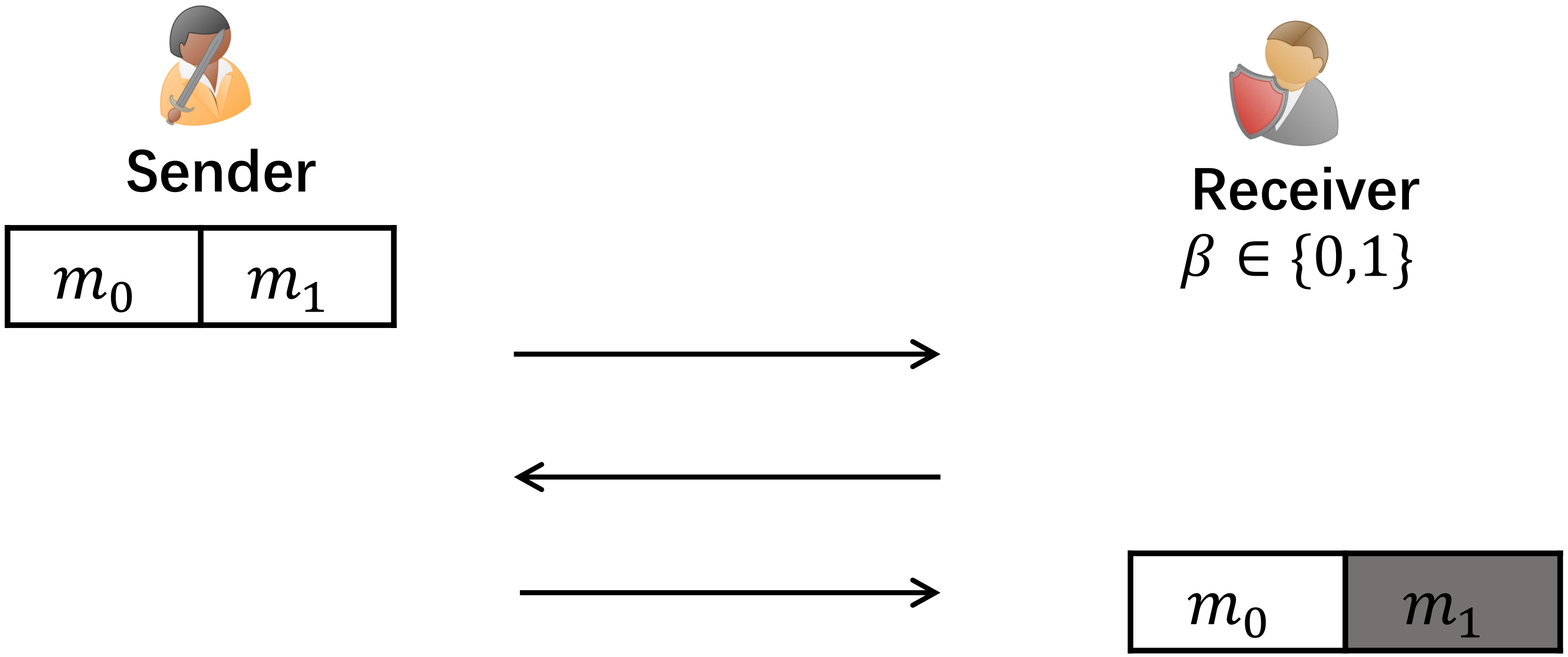
Sender

m_0	m_1

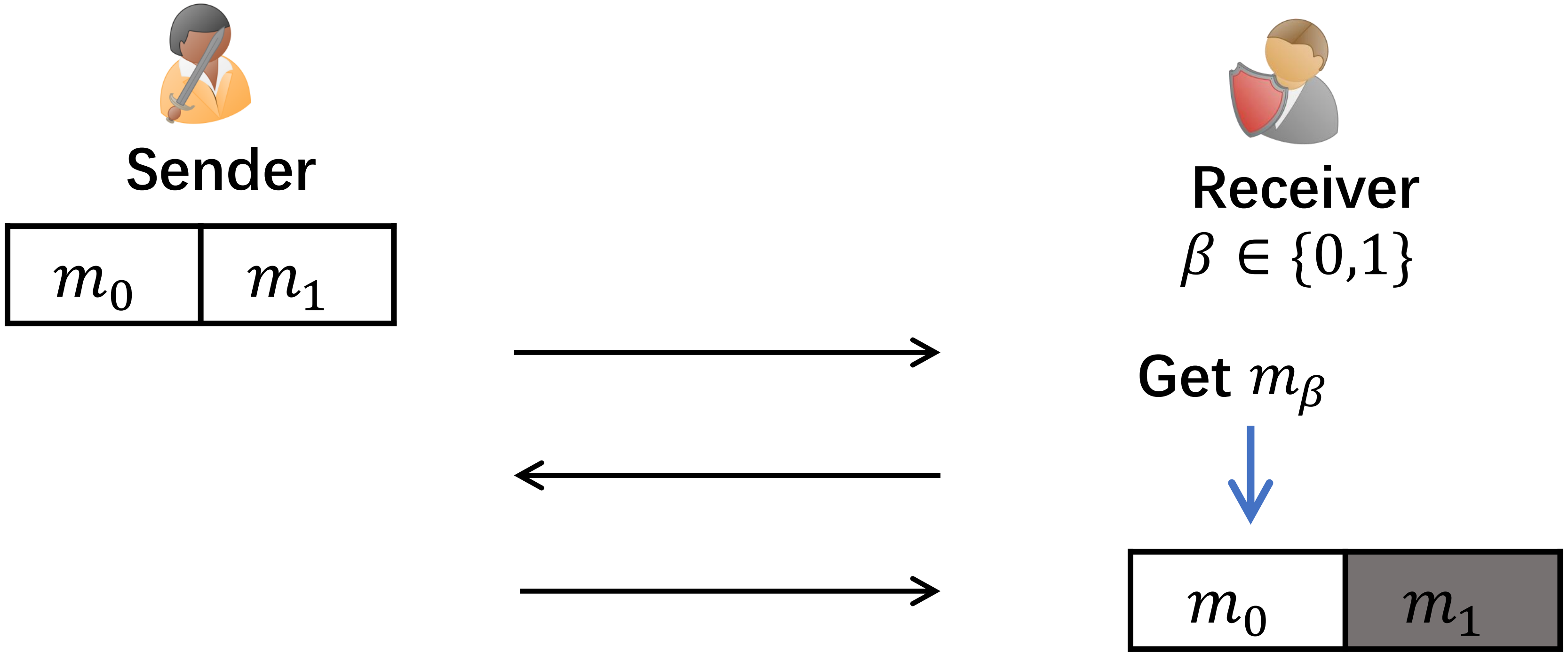
Receiver

$\beta \in \{0,1\}$

Oblivious Transfer (OT)



Oblivious Transfer (OT)



Oblivious Transfer (OT)

Sender

m_0	m_1

Receiver

$\beta \in \{0,1\}$

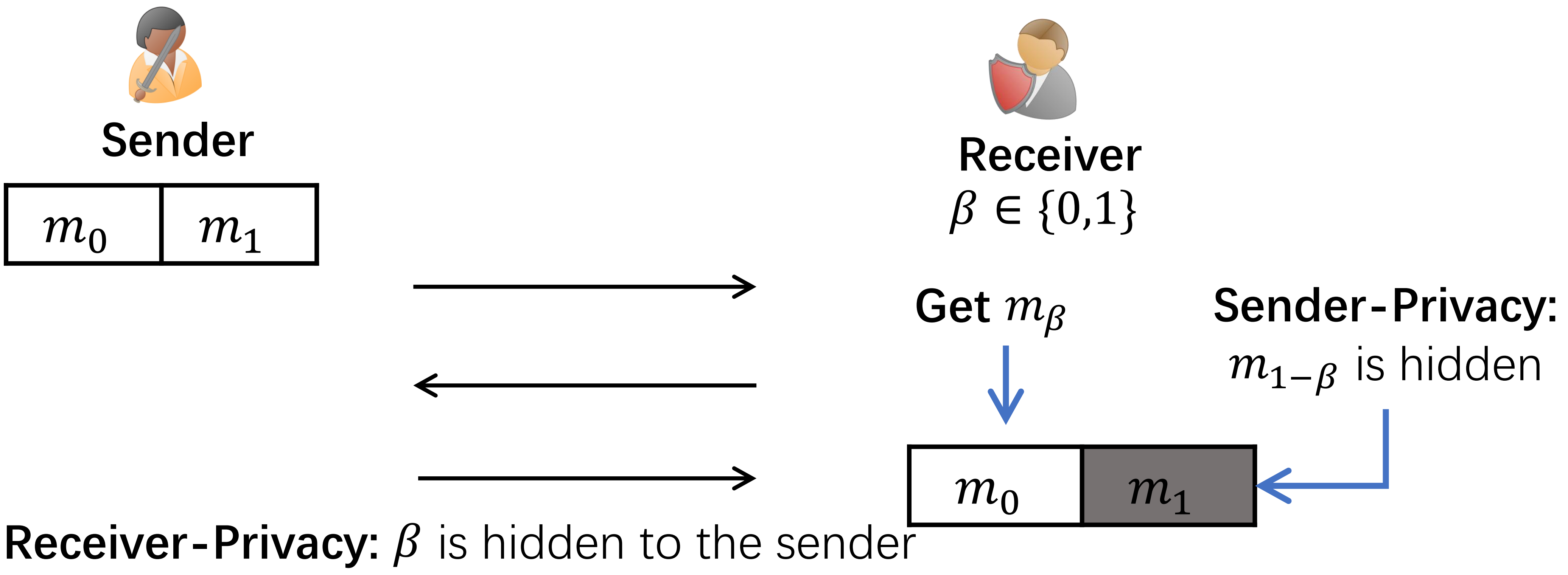
Get m_β

Sender-Privacy:

$m_{1-\beta}$ is hidden

m_0	m_1

Oblivious Transfer (OT)



Oblivious Transfer (OT)

Sender

m_0	m_1

Receiver

$\beta \in \{0,1\}$

Get m_β

Sender-Privacy:
$m_{1-\beta}$ is hidden

m_0	m_1

Receiver-Privacy: β is hidden to the sender

Many Applications:

- Secure multiparty computation [Yao86, GMW87]
- 2-round WI [JKKR17, BGI+17, KKS18]
- Non-malleable commitment [KS17]

Natural Question

2-round statistical sender-private OT in plain model

[NP01, AIR01, Kal05, HK12, BD18]

Natural Question

2-round statistical sender-private OT in plain model

[NP01, AIR01, Kal05, HK12, BD18]

Can we construct **2-round statistical receiver-private** OT?

Natural Question

2-round statistical sender-private OT in plain model

[NP01, AIR01, Kal05, HK12, BD18]

Can we construct **2-round statistical receiver-private** OT? **Impossible!**

Natural Question

2-round statistical sender-private OT in plain model

[NP01, AIR01, Kal05, HK12, BD18]

Can we construct **2-round statistical receiver-private** OT? Impossible!

Sender

Non-uniform Malicious Receiver

Natural Question

2-round statistical sender-private OT in plain model

[NP01, AIR01, Kal05, HK12, BD18]

Can we construct **2-round statistical receiver-private** OT? **Impossible!**

Sender

$$\mathrm{ot}_1 \begin{cases} = \mathrm{OT}_1(\beta = 0; r_0) \\ = \mathrm{OT}_1(\beta = 1; r_1) \end{cases}$$

Non-uniform Malicious Receiver

Natural Question

2-round statistical sender-private OT in plain model

[NP01, AIR01, Kal05, HK12, BD18]

Can we construct **2-round statistical receiver-private** OT? **Impossible!**

Sender

Non-uniform Malicious Receiver

$$\mathrm{ot}_1 = \mathrm{OT}_1(\beta = 0; r_0)$$
$$\mathrm{ot}_1 = \mathrm{OT}_1(\beta = 1; r_1)$$

$\longleftarrow$

m_0	m_1

$\longrightarrow$

Natural Question

2-round statistical sender-private OT in plain model

[NP01, AIR01, Kal05, HK12, BD18]

Can we construct **2-round statistical receiver-private** OT? **Impossible!**

Sender

$$\mathrm{ot}_1 = \mathrm{OT}_1(\beta = 0; r_0)$$
$$\mathrm{ot}_1 = \mathrm{OT}_1(\beta = 1; r_1)$$

Non-uniform Malicious Receiver

m_0	m_1

Compromise sender-privacy

m_0	m_1

Natural Question

2-round statistical sender-private OT in plain model

[NP01, AIR01, Kal05, HK12, BD18]

Can we construct **2-round statistical receiver-private** OT? **Impossible!**

Sender

$$\mathrm{ot}_1 = \mathrm{OT}_1(\beta = 0; r_0)$$
$$\mathrm{ot}_1 = \mathrm{OT}_1(\beta = 1; r_1)$$

Non-uniform Malicious Receiver

m_0	m_1

Compromise sender-privacy

m_0	m_1

- [KKS18] 3-round protocol from *super-poly* hardness assumptions

Question (2): Based on *polynomial hardness* assumptions, does there exist 3-round statistical receiver-private OT in the plain model?

Question (2): Based on *polynomial hardness* assumptions, does there exist 3-round statistical receiver-private OT in the plain model?

Result (2): 3-round statistical receiver-private OT from poly-hardness

Construction (1): 2-round statistical sender-private OT

Construction (2): Computational Diffie-Hellman assumption

Question (2): Based on *polynomial hardness* assumptions, does there exist 3-round statistical receiver-private OT in the plain model?

Result (2): 3-round statistical receiver-private OT from poly-hardness

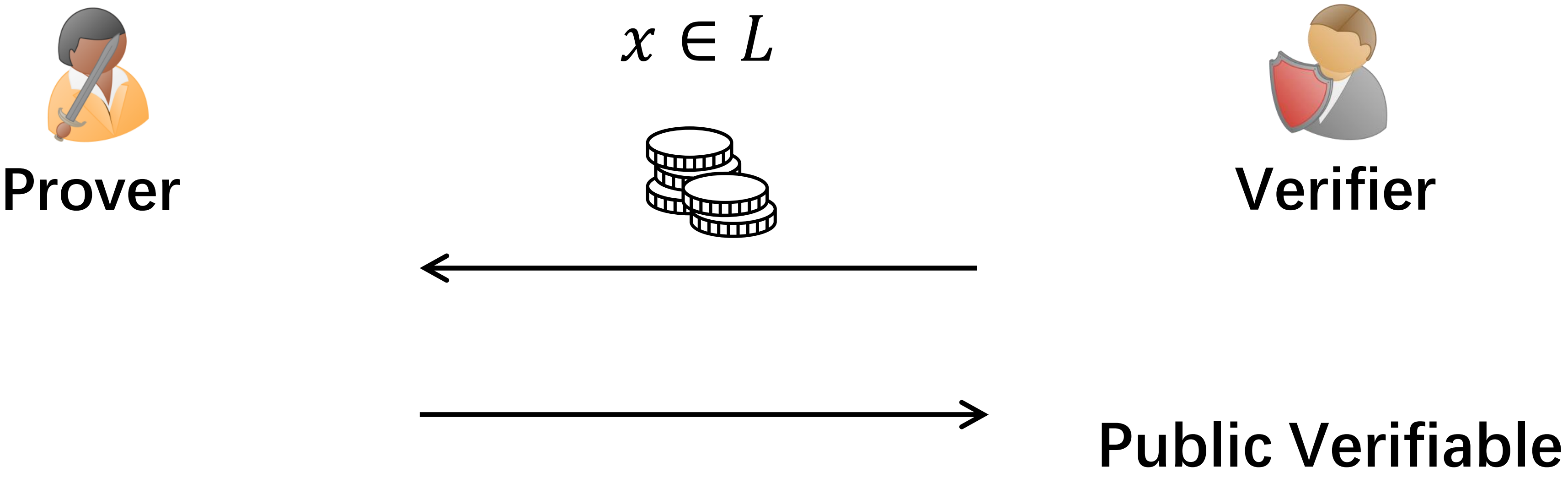
Construction (1): 2-round statistical sender-private OT

OT reversal

Construction (2): Computational Diffie-Hellman assumption

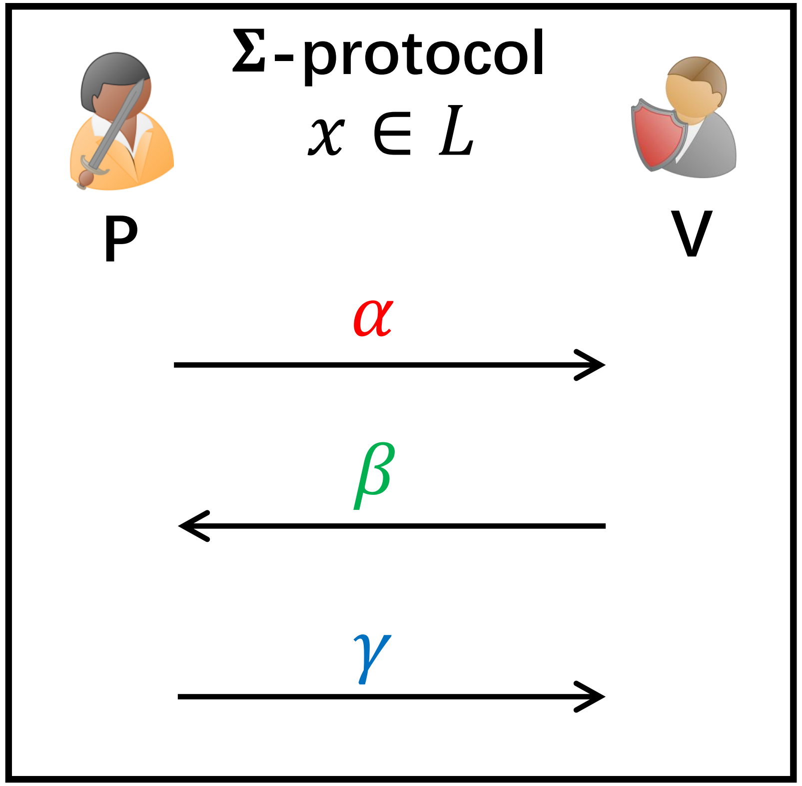
Technical Details
Part I: Statistical Zaps

Statistical Zaps



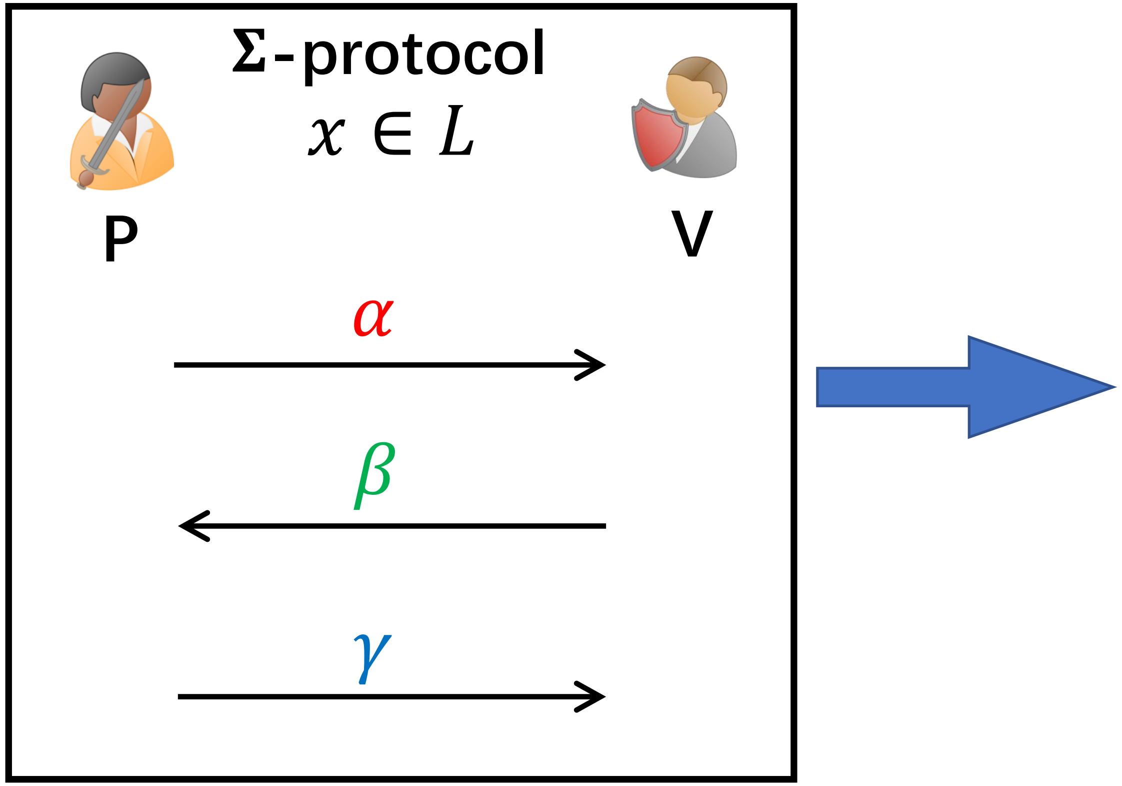
Starting Idea

- Compress a Σ-protocol via a **C**orrelation **I**ntractable **H**ash (CIH) $\{\mathrm{H}_k(\cdot)\}_k$ [CGH98, KRR17, CCRR18, HL18, CCH+19, PS19]



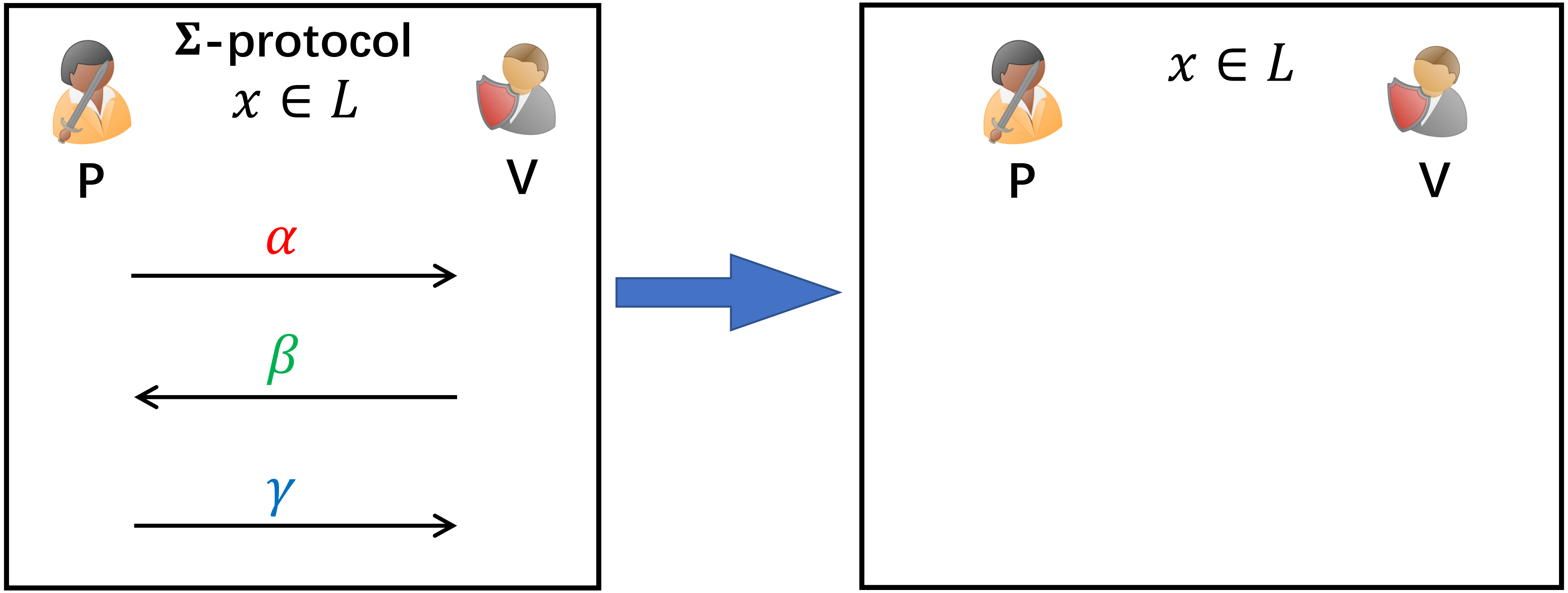
Starting Idea

- Compress a Σ-protocol via a **C**orrelation **I**ntractable **H**ash (CIH) $\{\mathrm{H}_k(\cdot)\}_k$ [CGH98, KRR17, CCRR18, HL18, CCH+19, PS19]



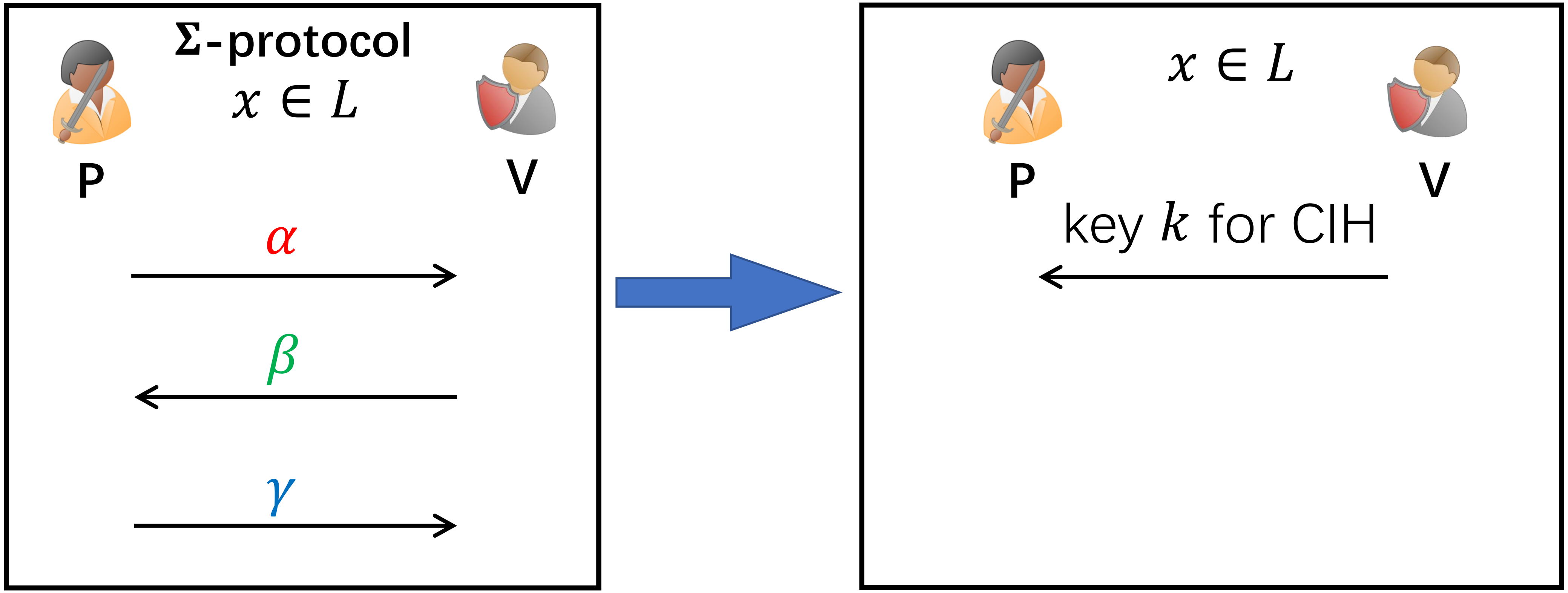
Starting Idea

- Compress a Σ-protocol via a **C**orrelation **I**ntractable **H**ash (CIH) $\{\mathrm{H}_k(\cdot)\}_k$ [CGH98, KRR17, CCRR18, HL18, CCH+19, PS19]



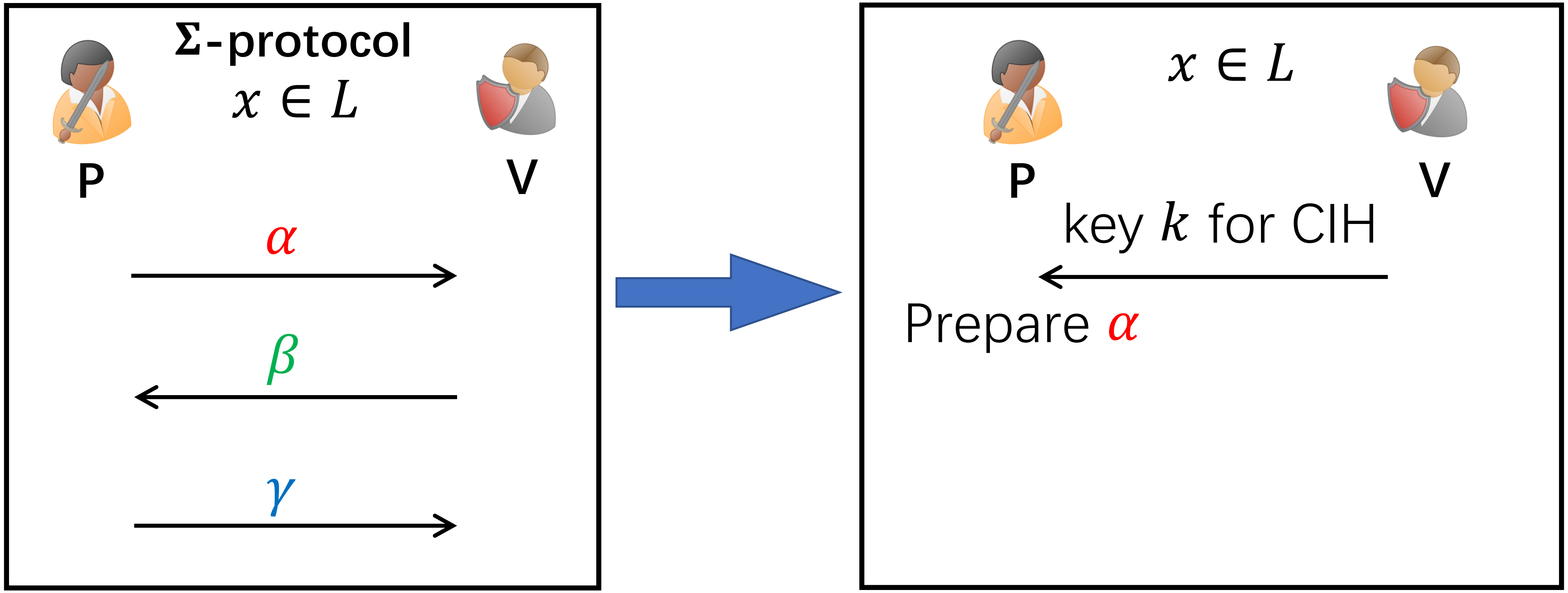
Starting Idea

- Compress a Σ-protocol via a **C**orrelation **I**ntractable **H**ash (CIH) $\{\mathrm{H}_k(\cdot)\}_k$ [CGH98, KRR17, CCRR18, HL18, CCH+19, PS19]



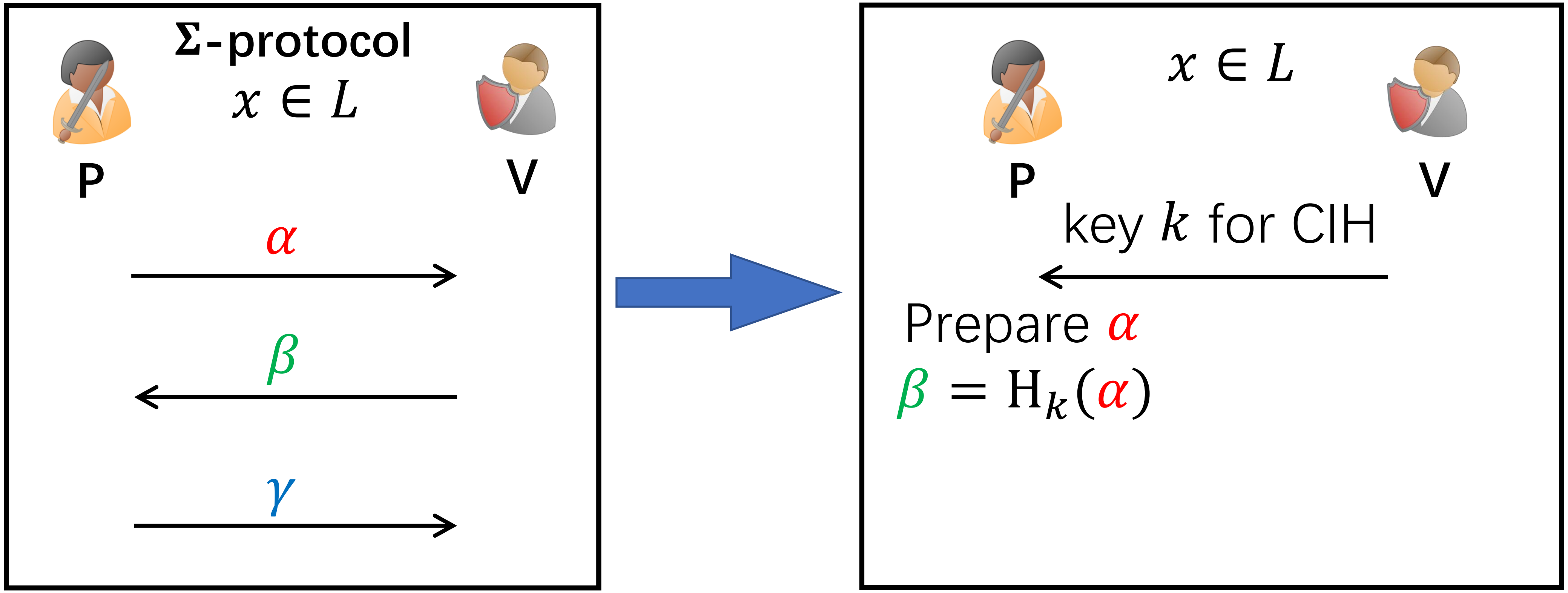
Starting Idea

- Compress a Σ-protocol via a **C**orrelation **I**ntractable **H**ash (CIH) $\{\mathrm{H}_k(\cdot)\}_k$ [CGH98, KRR17, CCRR18, HL18, CCH+19, PS19]



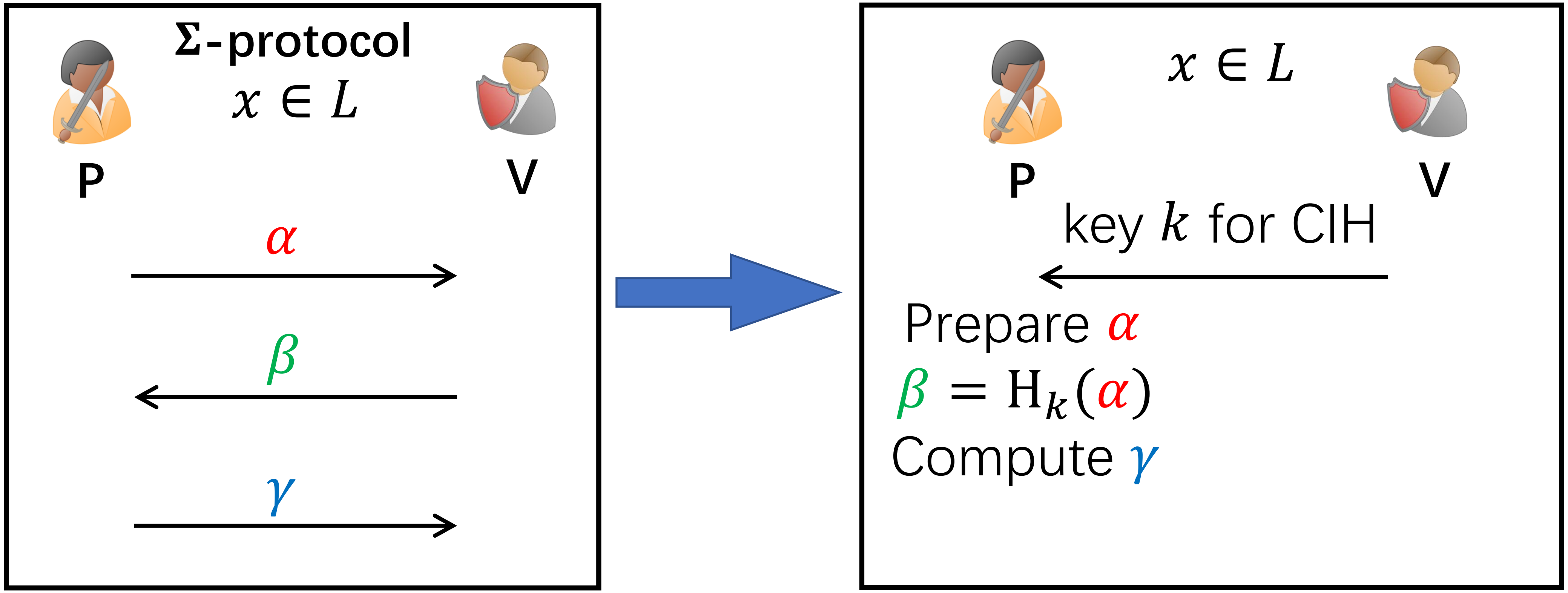
Starting Idea

- Compress a Σ-protocol via a **C**orrelation **I**ntractable **H**ash (CIH) $\{\mathrm{H}_k(\cdot)\}_k$ [CGH98, KRR17, CCRR18, HL18, CCH+19, PS19]



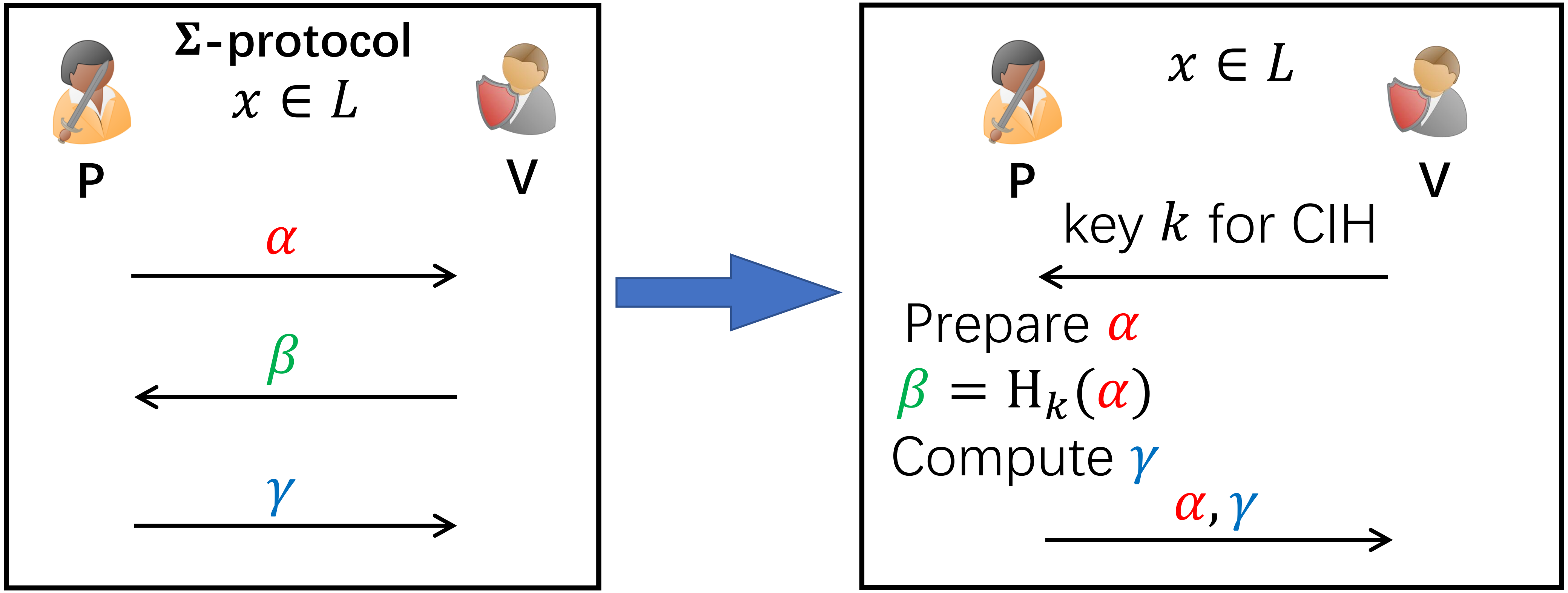
Starting Idea

- Compress a Σ-protocol via a **C**orrelation **I**ntractable **H**ash (CIH) $\{\mathrm{H}_k(\cdot)\}_k$ [CGH98, KRR17, CCRR18, HL18, CCH+19, PS19]



Starting Idea

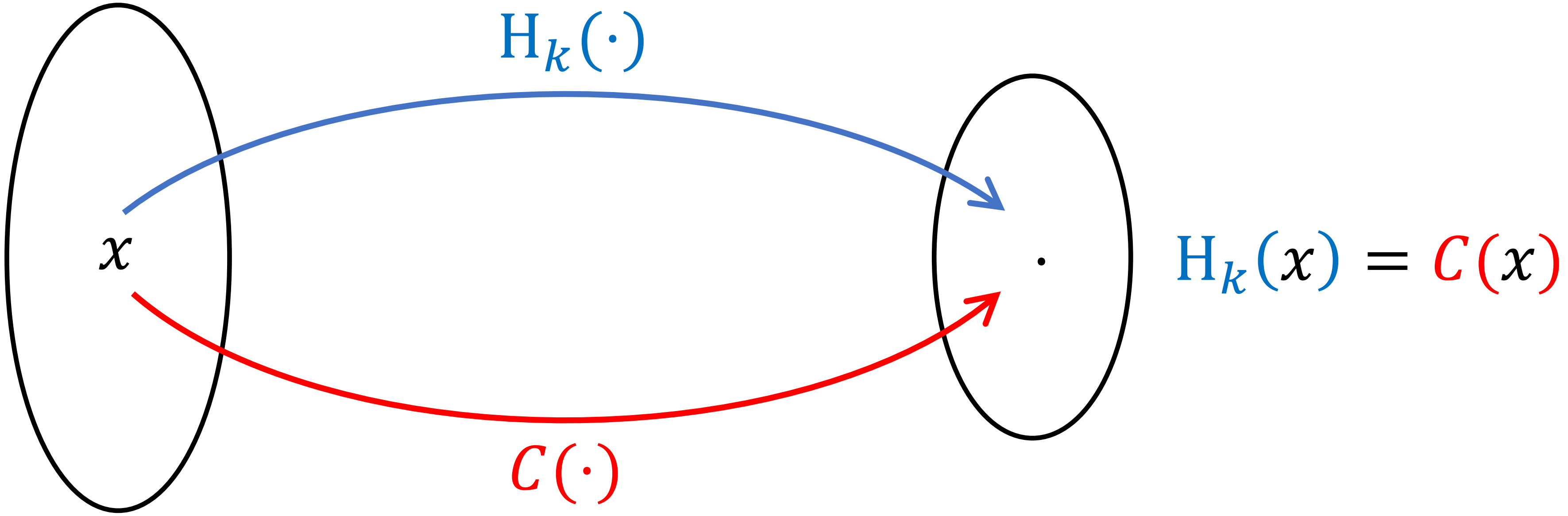
- Compress a Σ-protocol via a **C**orrelation **I**ntractable **H**ash (CIH) $\{\mathrm{H}_k(\cdot)\}_k$ [CGH98, KRR17, CCRR18, HL18, CCH+19, PS19]



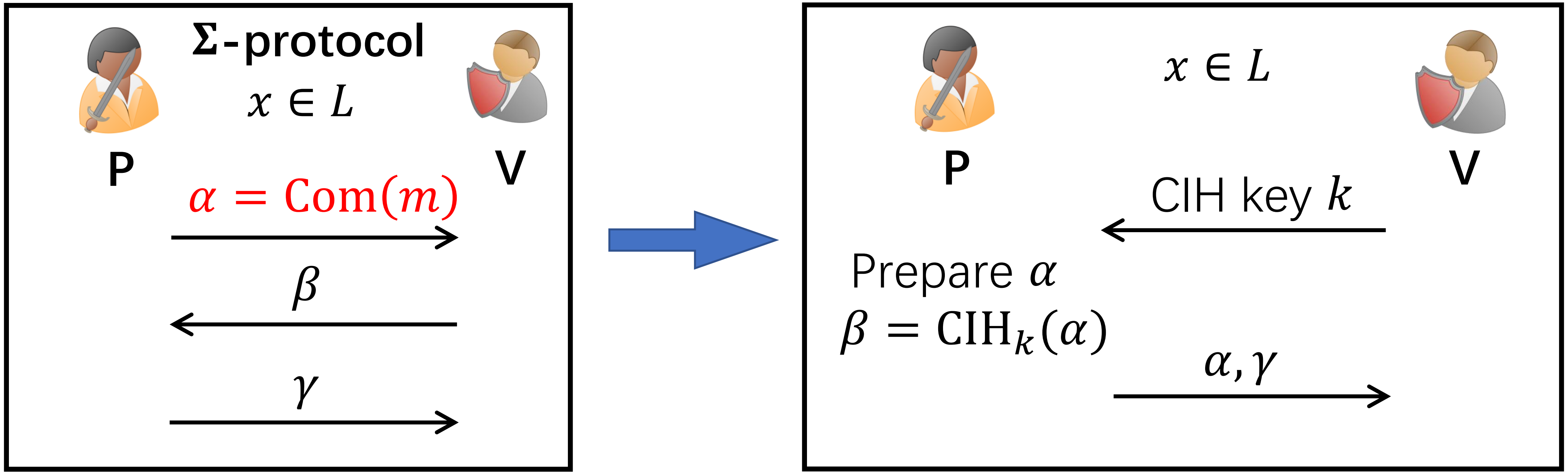
Correlation **I**ntractable **H**ash (CIH)

A CIH is a hash function $\{\mathrm{H}_k(\cdot)\}_k$:

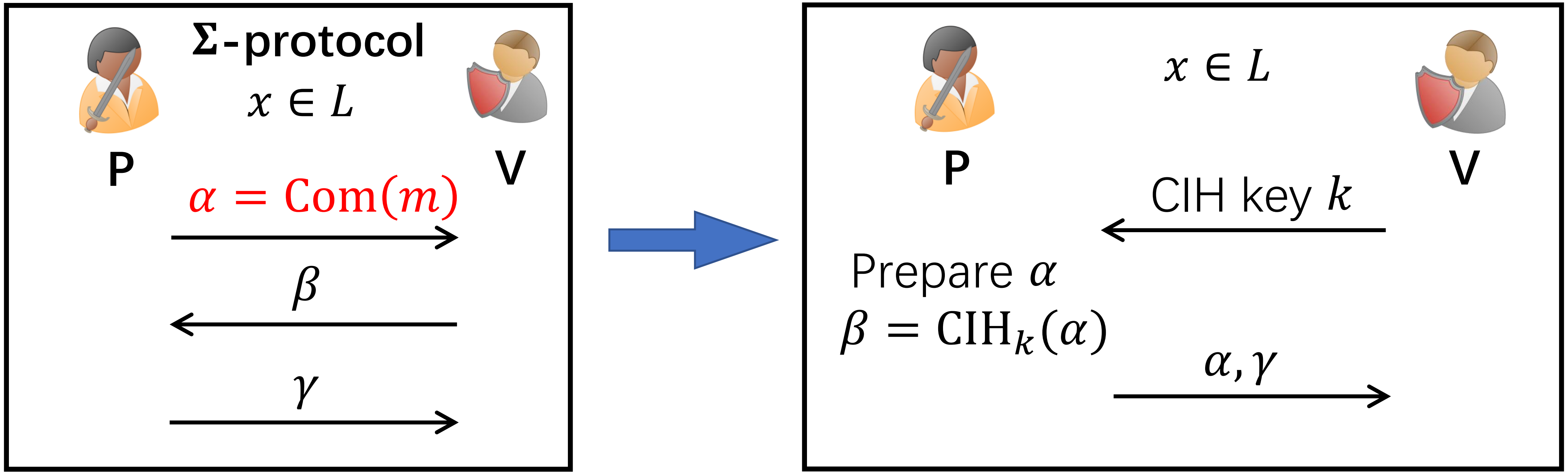
$\forall$ C, let $k \leftarrow \{0,1\}^{\mathrm{poly}(\lambda)}$, it's hard to find an x, such that



Idea for Security

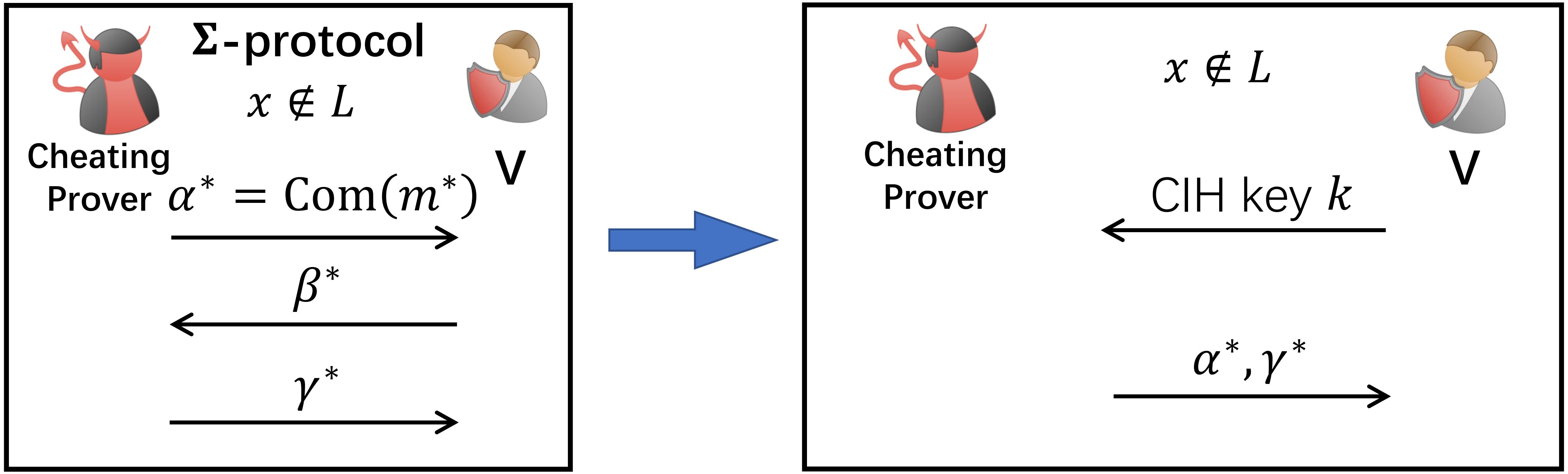


Idea for Security



- **WI:** follows from *hiding property* of the commitment

Idea for Security



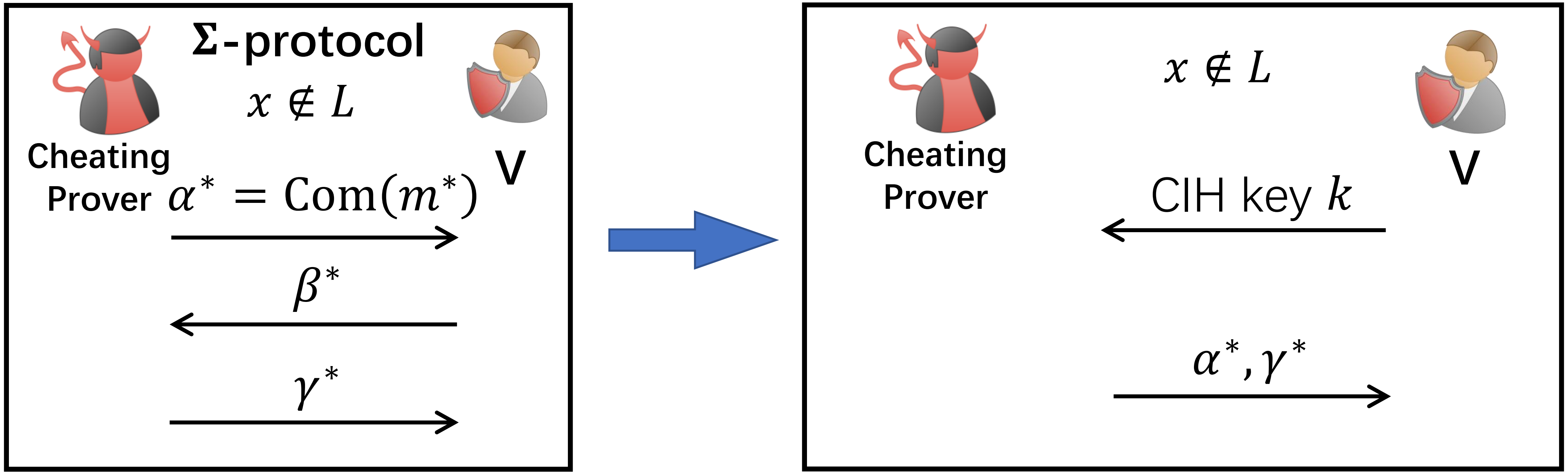
- **Soundness:** *Extract* m^* from α^* using a trapdoor

  Given m^*, the (only) accepting β^* is efficiently computable

  Verifier accepts ⇒ $\beta^* = \mathrm{CIH}_k(\alpha^*) = C(\alpha^*)$
- **Hiding & Extractable commitments** can be built in CRS model

  ⇒ Zaps in CRS model

Idea for Security



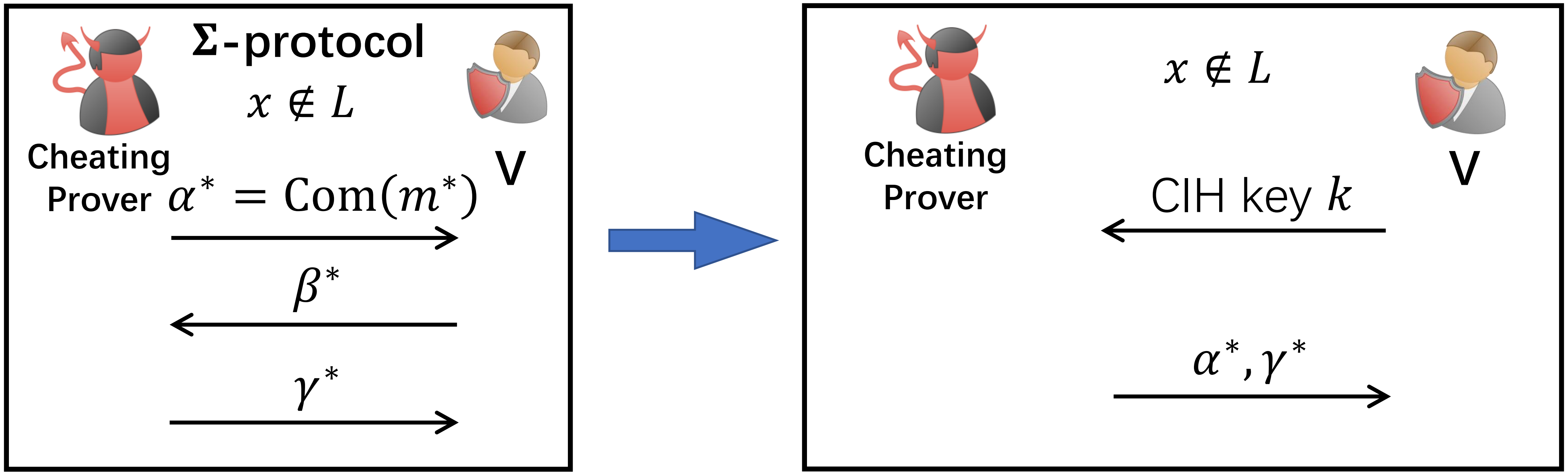
- **Soundness:** <u>*Extract*</u> m^* from α^* using a trapdoor

  Given m^*, the (only) accepting β^* is efficiently computable

  Verifier accepts ⇒ $\beta^* = \mathrm{CIH}_k(\alpha^*) = C(\alpha^*)$
- **Hiding & Extractable commitments** can be built in CRS model

  ⇒ Zaps in CRS model

Idea for Security



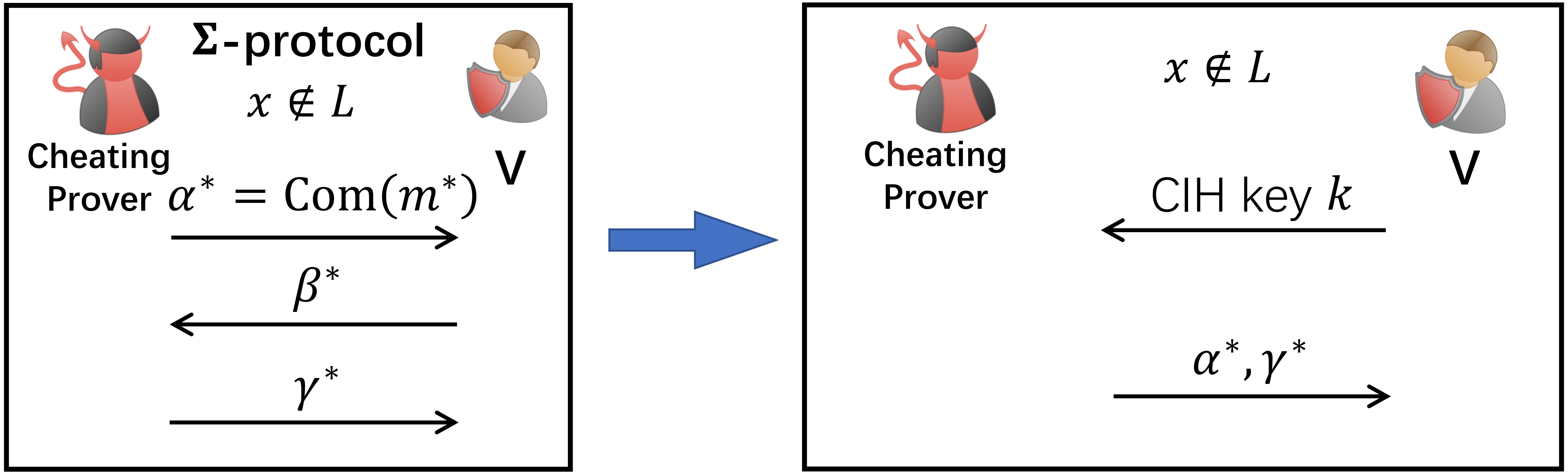
- **Soundness:** <u>*Extract*</u> m^* from α^* using a trapdoor

  Given m^*, the (only) accepting β^* is efficiently computable

  Verifier accepts $\Rightarrow$ $\beta^* = \mathrm{CIH}_k(\alpha^*) = C(\alpha^*)$
- **Hiding & Extractable commitments** can be built in CRS model

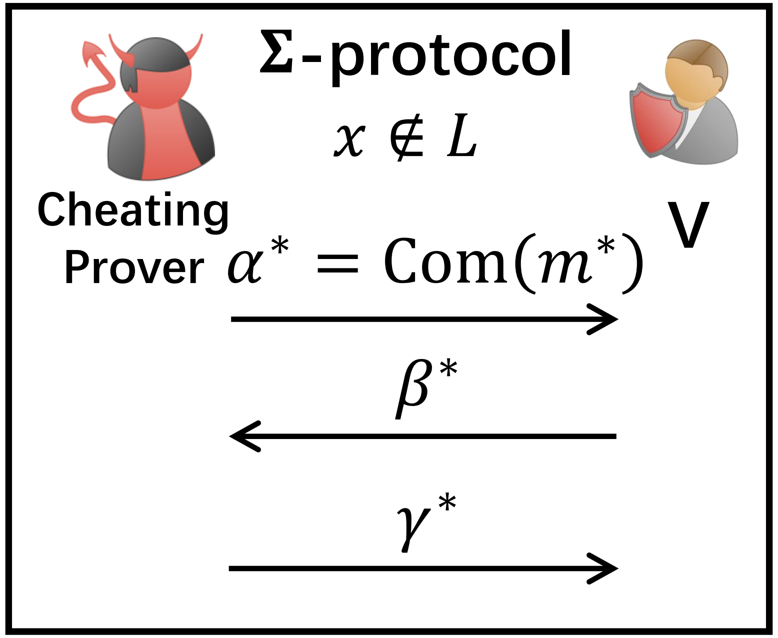
  $\Rightarrow$ Zaps in CRS model

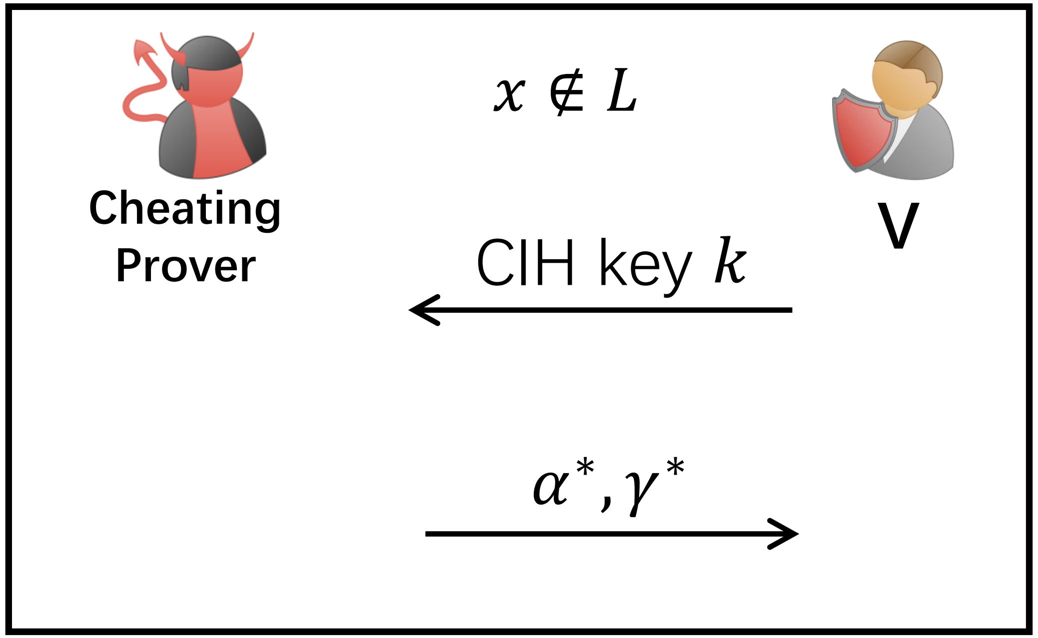
Idea for Security



- **Soundness:** <u>*Extract*</u> m^* from α^* using a trapdoor
  Given m^*, the (only) accepting β^* is efficiently computable $\Big\}$ $\beta^* = C(\alpha^*)$
  Verifier accepts ⇒ $\beta^* = \mathrm{CIH}_k(\alpha^*) = C(\alpha^*)$
- **Hiding & Extractable commitments** can be built in CRS model
  ⇒ Zaps in CRS model

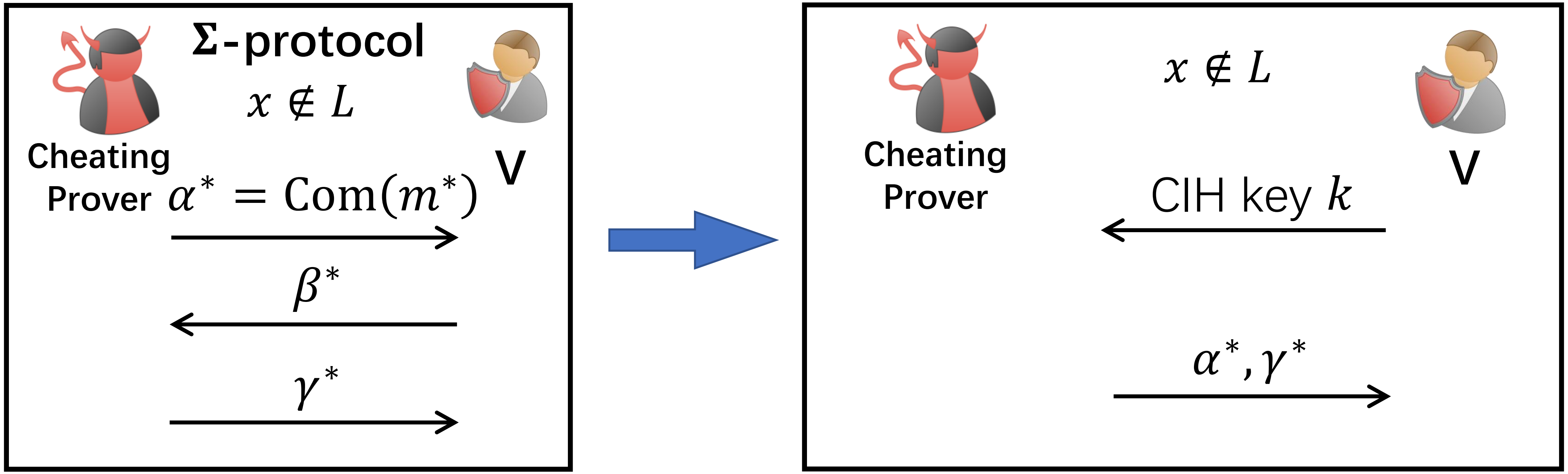
Idea for Security





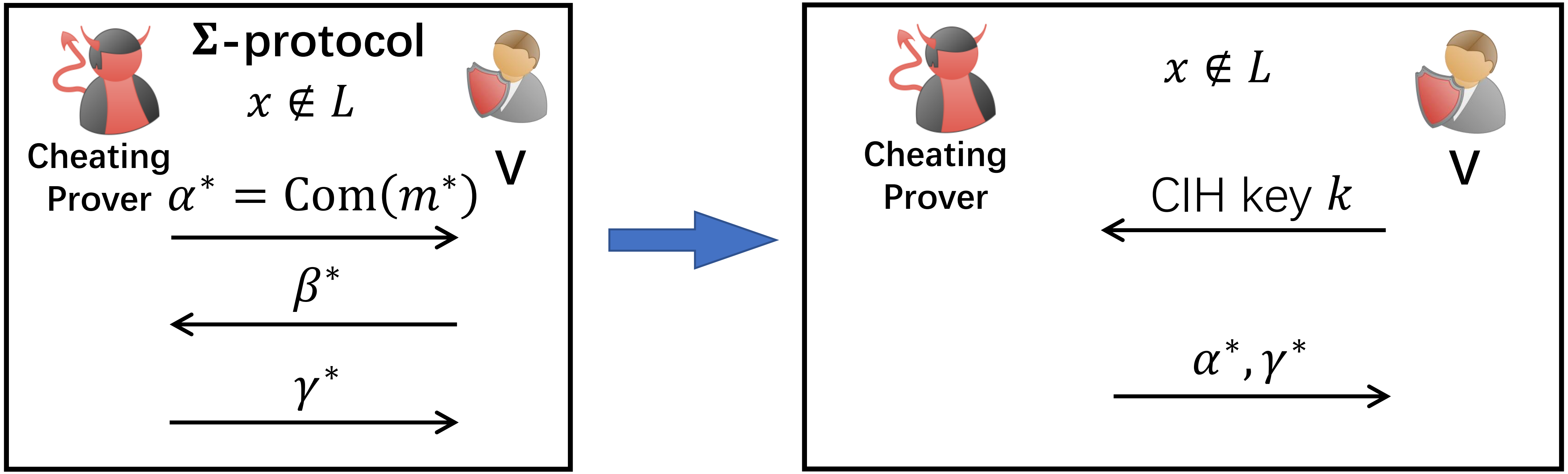
- **Soundness:** <u>*Extract*</u> m^* from α^* using a trapdoor
  Given m^*, the (only) accepting β^* is efficiently computable } $\beta^* = C(\alpha^*)$
  Verifier accepts $\Rightarrow$ $\beta^* = \mathrm{CIH}_k(\alpha^*) = C(\alpha^*)$
- **Hiding & Extractable commitments** can be built in CRS model
  $\Rightarrow$ Zaps in CRS model

Idea for Security



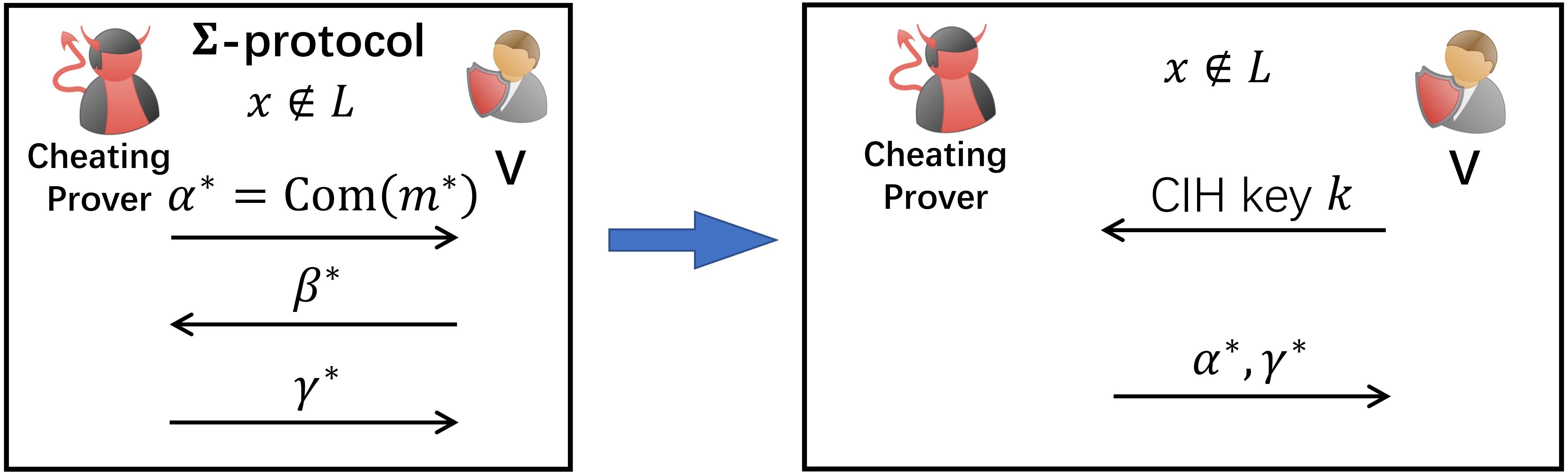
- **Soundness:** *Extract* m^* from α^* using a trapdoor
  Given m^*, the (only) accepting β^* is efficiently computable } $\beta^* = C(\alpha^*)$
  Verifier accepts $\Rightarrow$ $\beta^* = \mathrm{CIH}_k(\alpha^*) = C(\alpha^*)$ **Contradicts CIH!**
- **Hiding & Extractable commitments** can be built in CRS model
  $\Rightarrow$ Zaps in CRS model

Idea for Security



- **Soundness:** <u>*Extract*</u> m^* from α^* using a trapdoor
  Given m^*, the (only) accepting β^* is efficiently computable
  $\beta^* = C(\alpha^*)$
  Verifier accepts ⇒ $\beta^* = \mathrm{CIH}_k(\alpha^*) = C(\alpha^*)$ **Contradicts CIH!**
- **Hiding & Extractable commitments** can be built in CRS model
  ⇒ Zaps in CRS model

Idea for Security



- **Soundness:** <u>*Extract*</u> m^* from α^* using a trapdoor
  Given m^*, the (only) accepting β^* is efficiently computable $\beta^* = C(\alpha^*)$
  Verifier accepts ⇒ $\beta^* = \mathrm{CIH}_k(\alpha^*) = C(\alpha^*)$ **Contradicts CIH!**
- **Hiding & Extractable commitments** can be built in CRS model
  ⇒ Zaps in CRS model

Hiding & Extractability in Plain Model

- Use a 2-round statistical sender-private oblivious transfer

Hiding & Extractability in Plain Model

- Use a 2-round statistical sender-private oblivious transfer

P

V

Hiding & Extractability in Plain Model

- Use a 2-round statistical sender-private oblivious transfer

P

Prepare m, $b' \leftarrow^{\$} \{0,1\}$

V

$b \leftarrow^{\$} \{0,1\}$

Hiding & Extractability in Plain Model

- Use a 2-round statistical sender-private oblivious transfer

P

Prepare m, $b' \leftarrow^{\$} \{0,1\}$

<u>Sender</u>

V

$b \leftarrow^{\$} \{0,1\}$

<u>Receiver</u>(b)

Hiding & Extractability in Plain Model

- Use a 2-round statistical sender-private oblivious transfer

P

Prepare m, $b' \leftarrow^{\$} \{0,1\}$

<u>Sender</u>

V

$b \leftarrow^{\$} \{0,1\}$

<u>Receiver</u>(b)

Hiding & Extractability in Plain Model

- Use a 2-round statistical sender-private oblivious transfer

P

Prepare m, $b' \leftarrow^{\$} \{0,1\}$

Sender

V

$b \leftarrow^{\$} \{0,1\}$

Receiver(b)

$\leftarrow$

m	$\perp$

Put in b'-position

Hiding & Extractability in Plain Model

- Use a 2-round statistical sender-private oblivious transfer

P

Prepare m, $b' \leftarrow^{\$} \{0,1\}$

<u>Sender</u>

V

$b \leftarrow^{\$} \{0,1\}$

<u>Receiver</u>(b)

$\longleftarrow$

m	$\perp$

$\longrightarrow$

Put in b'-position

Hiding & Extractability in Plain Model

- Use a 2-round statistical sender-private oblivious transfer

P

Prepare m, $b' \leftarrow^{\$} \{0,1\}$

<u>Sender</u>

m	$\perp$

Put in b'-position

V

$b \leftarrow^{\$} \{0,1\}$

<u>Receiver</u>(b)

With $\Pr = 1/2$,

$b = b'$, extract m √

m	$\perp$

Hiding & Extractability in Plain Model

- Use a 2-round statistical sender-private oblivious transfer

P

Prepare m, $b' \xleftarrow{\$} \{0,1\}$

Sender

V

$b \xleftarrow{\$} \{0,1\}$

Receiver(b)

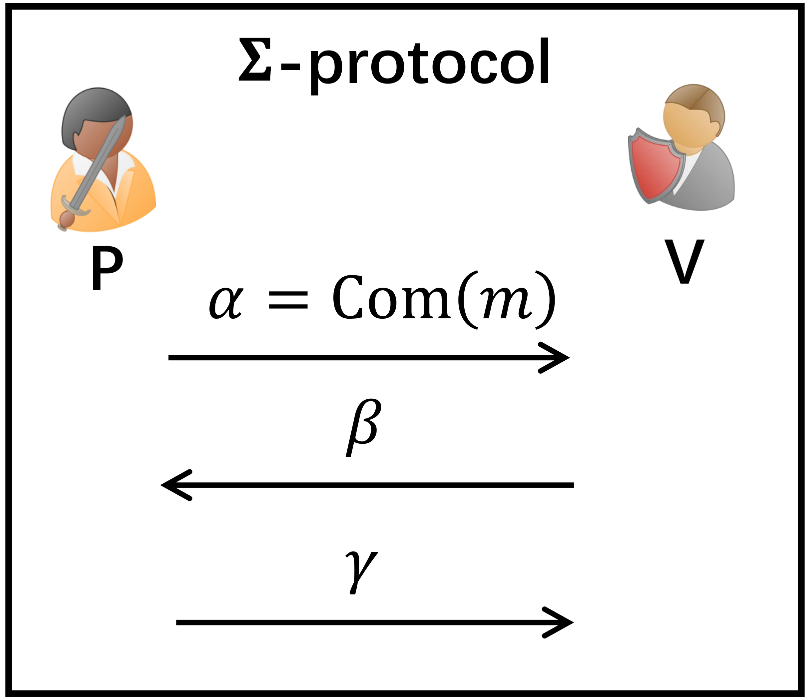
With $\Pr = 1/2$, $b \neq b'$, hide m √

m	$\perp$

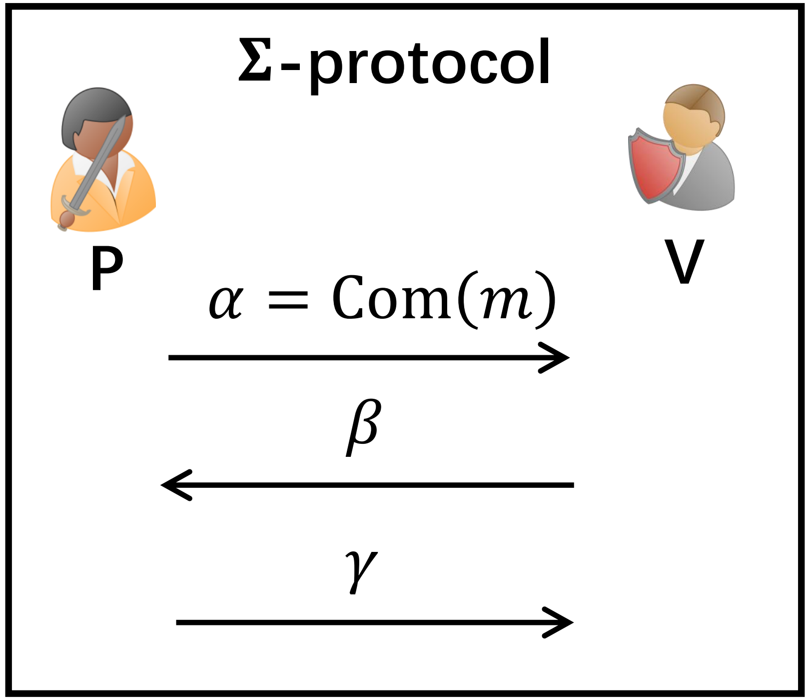
Put in b'-position

m	$\perp$

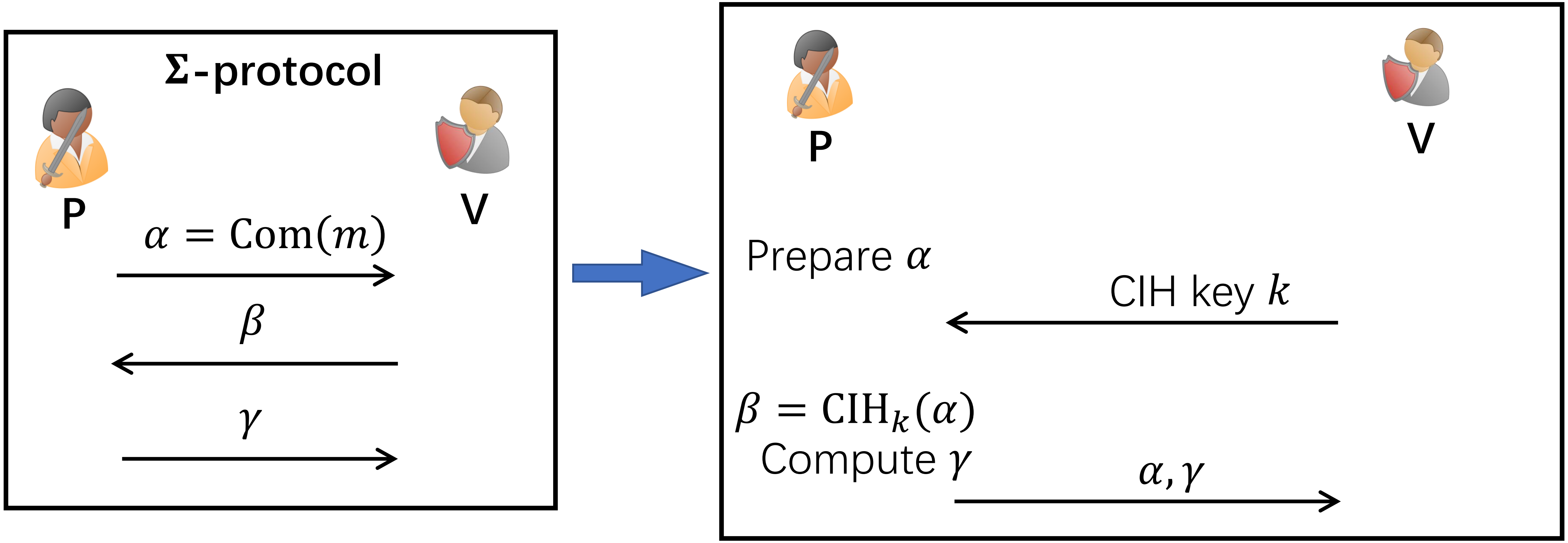
‘Weakly Secure’ Statistical Zaps



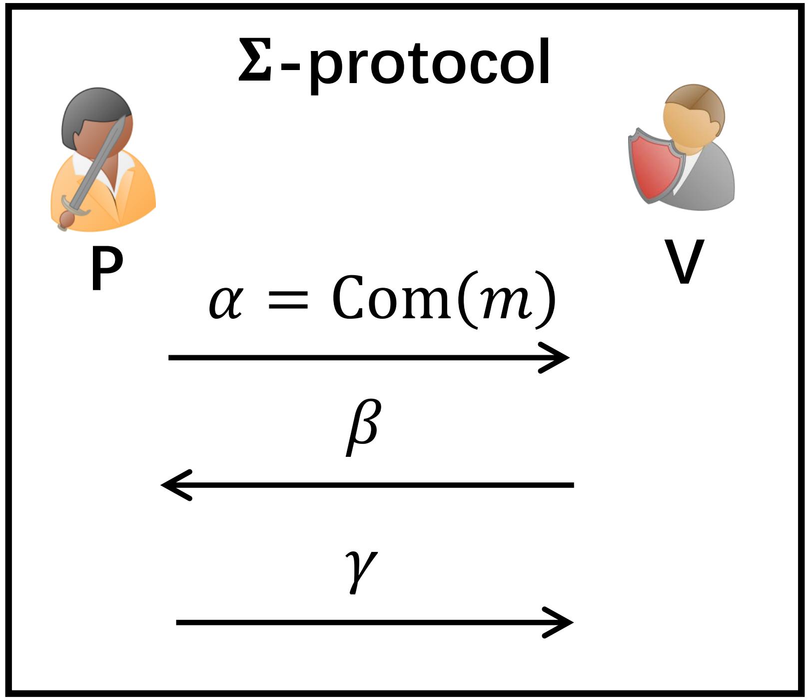
‘Weakly Secure’ Statistical Zaps

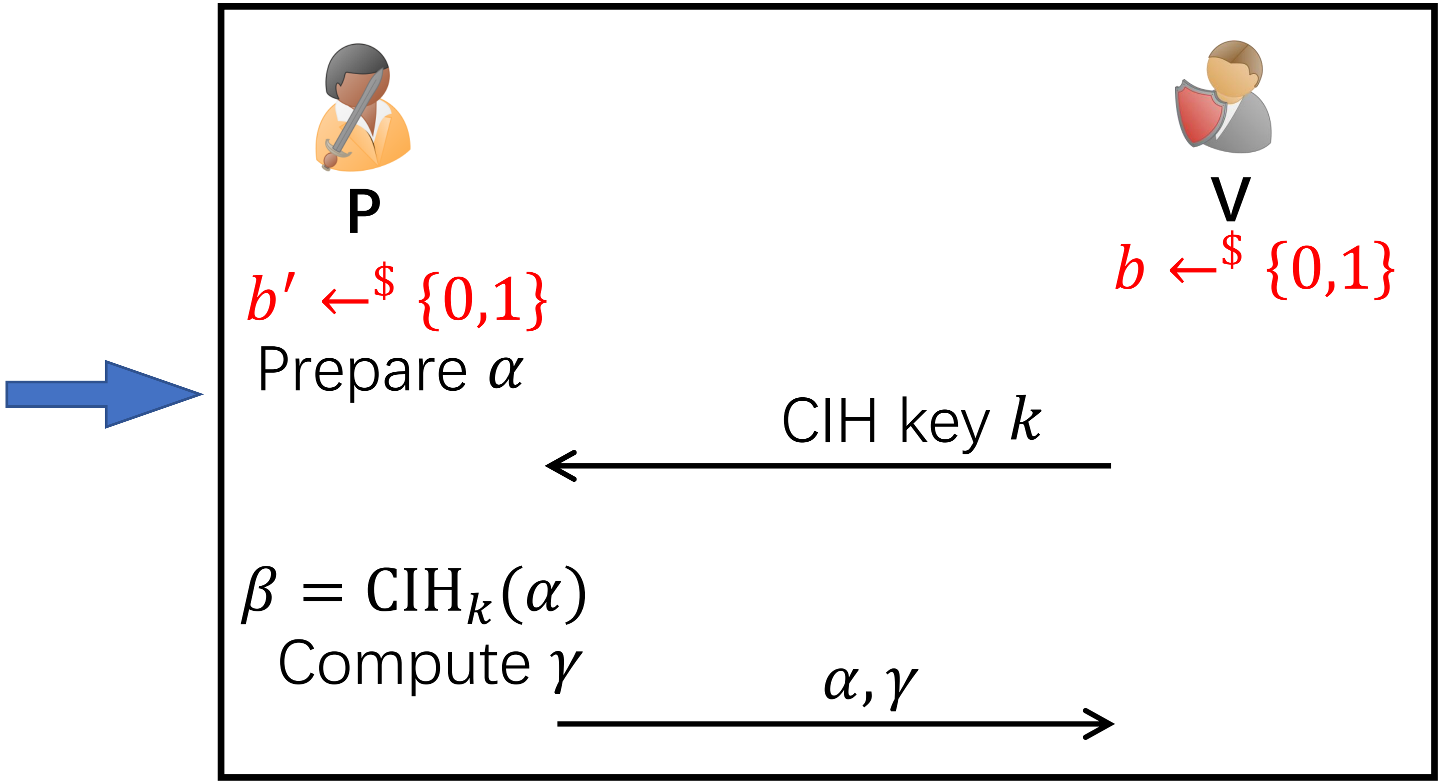


‘Weakly Secure’ Statistical Zaps

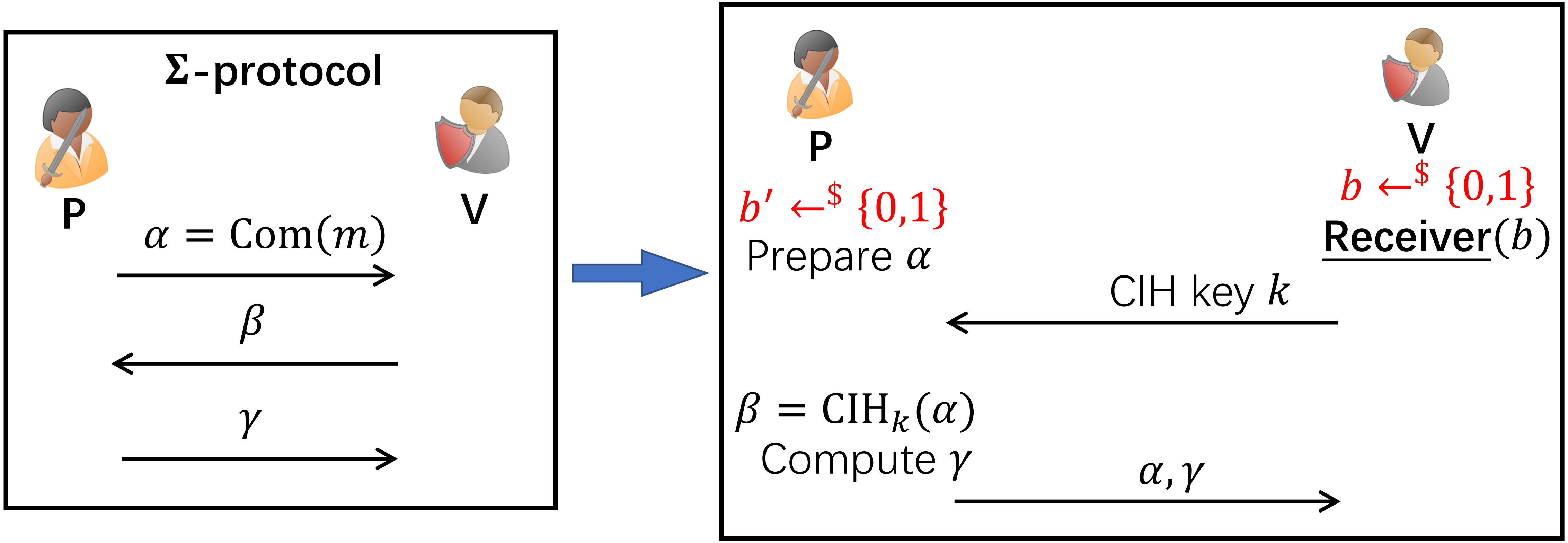


‘Weakly Secure’ Statistical Zaps

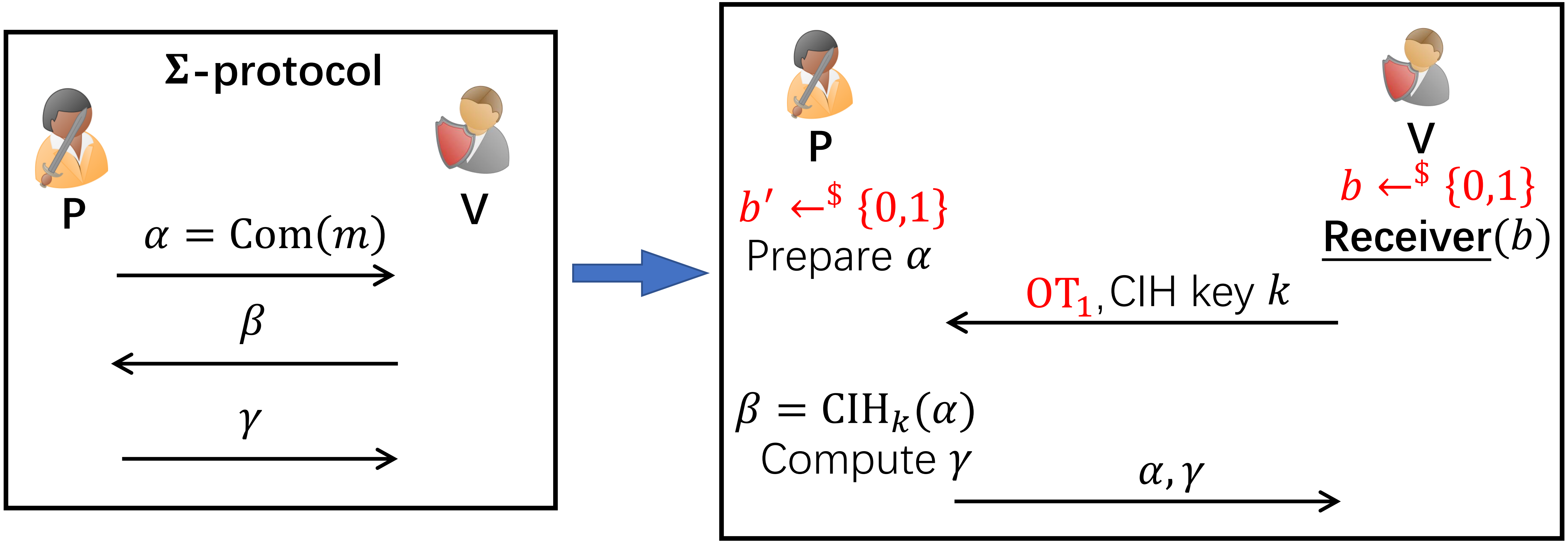




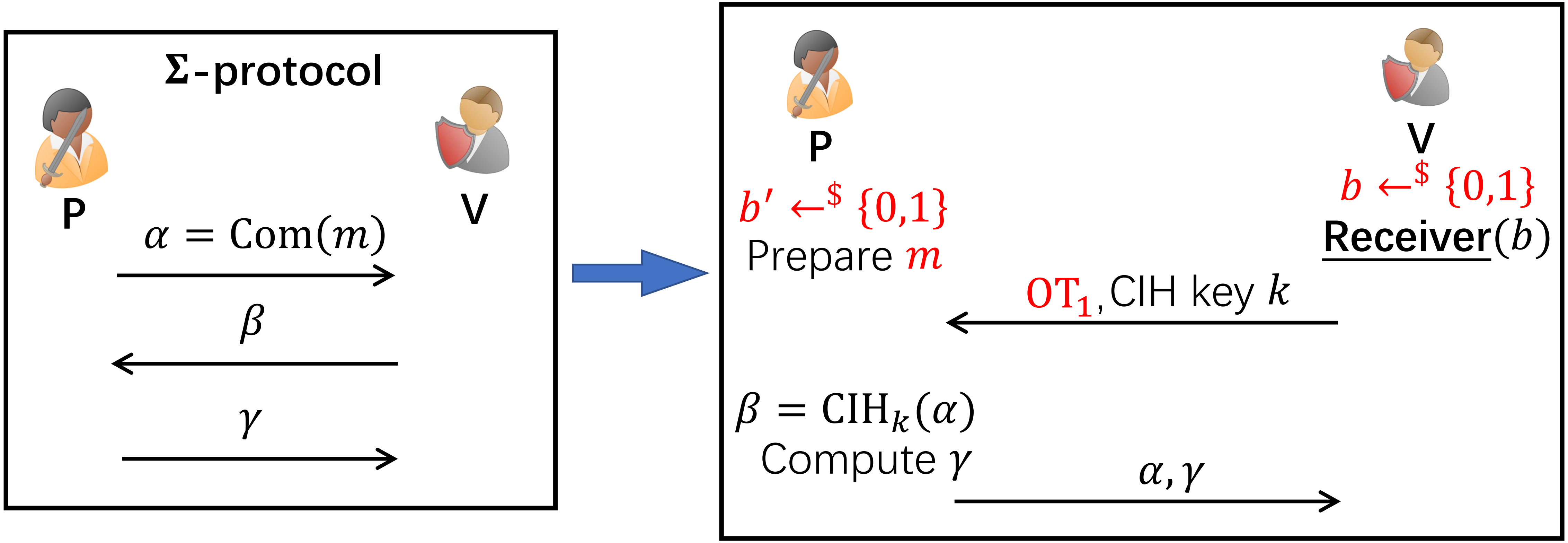
‘Weakly Secure’ Statistical Zaps



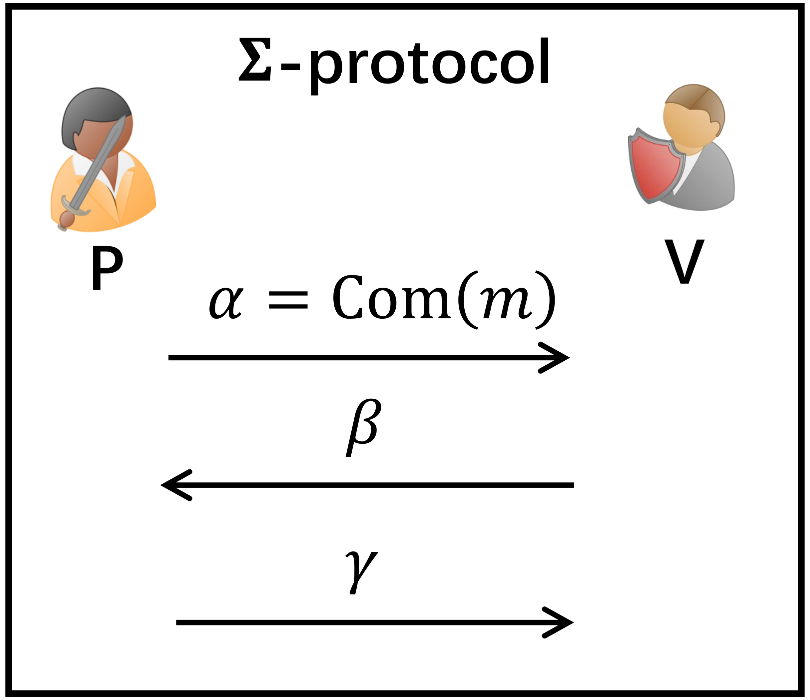
'Weakly Secure' Statistical Zaps

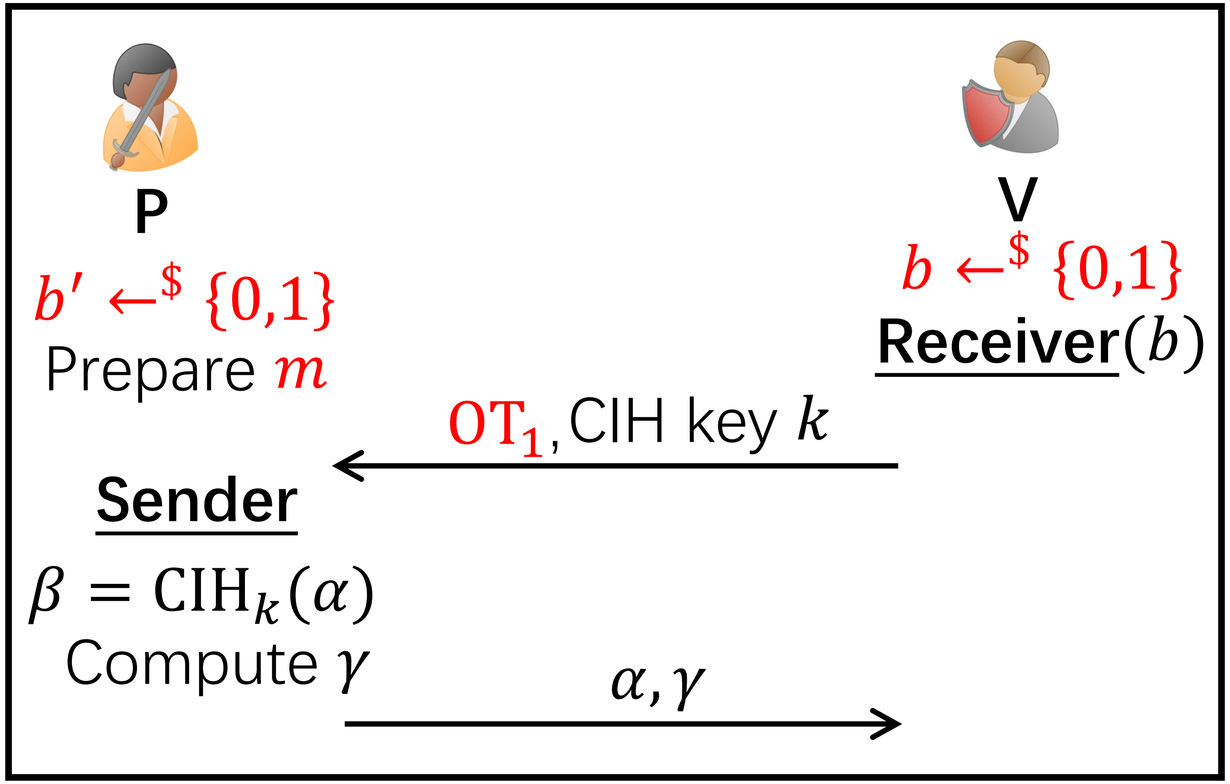


‘Weakly Secure’ Statistical Zaps

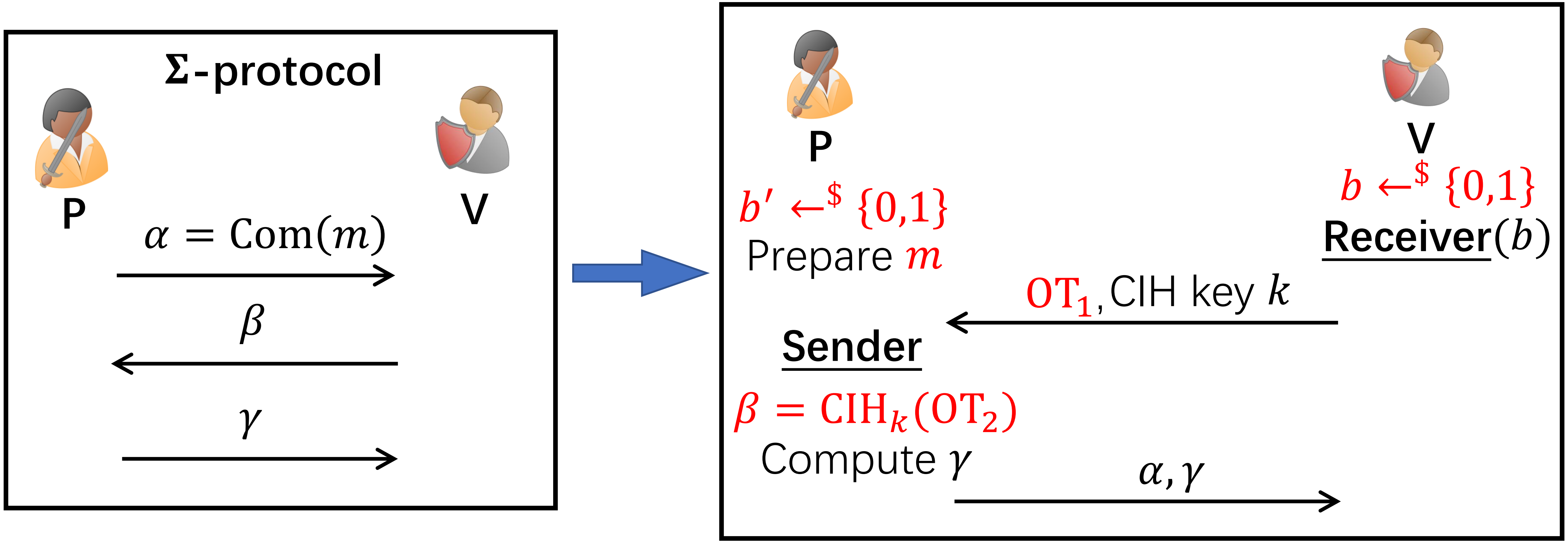


‘Weakly Secure’ Statistical Zaps

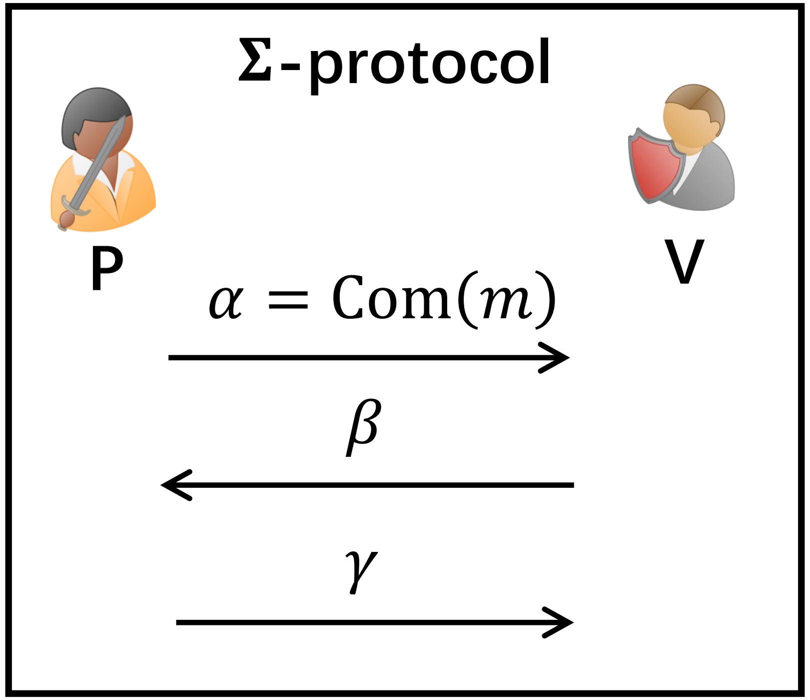


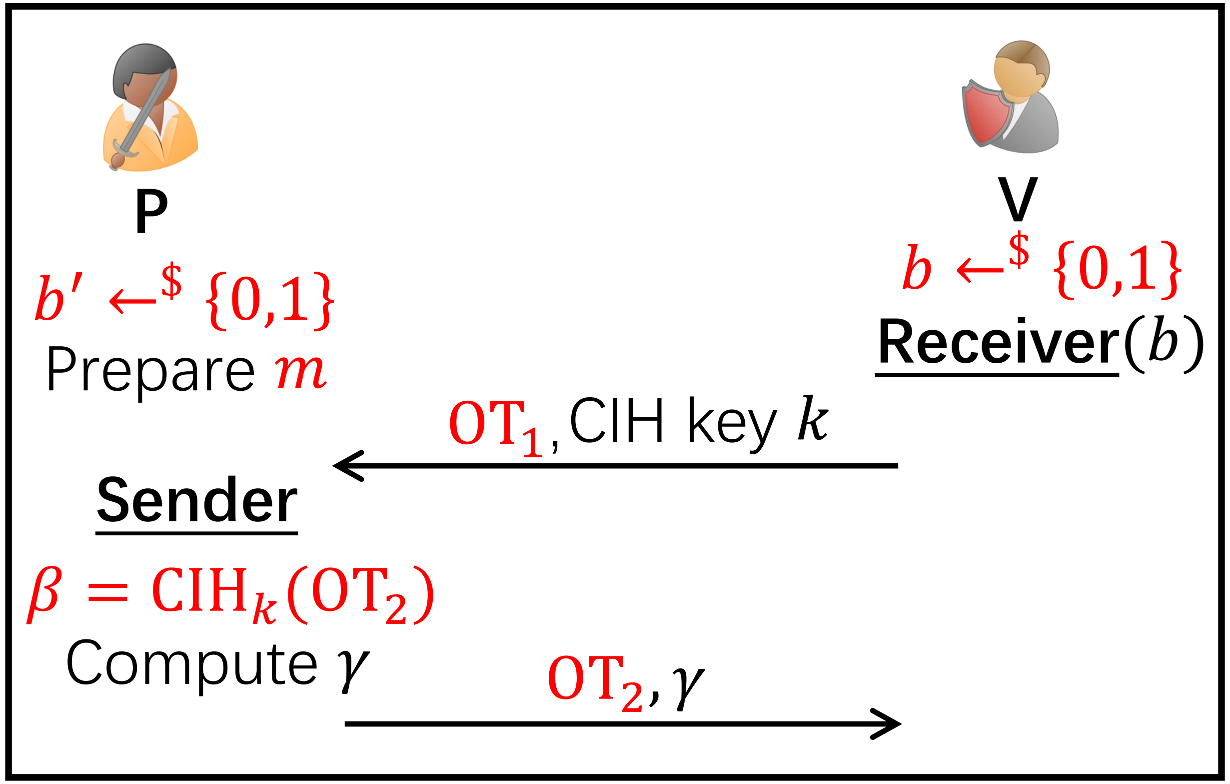


‘Weakly Secure’ Statistical Zaps

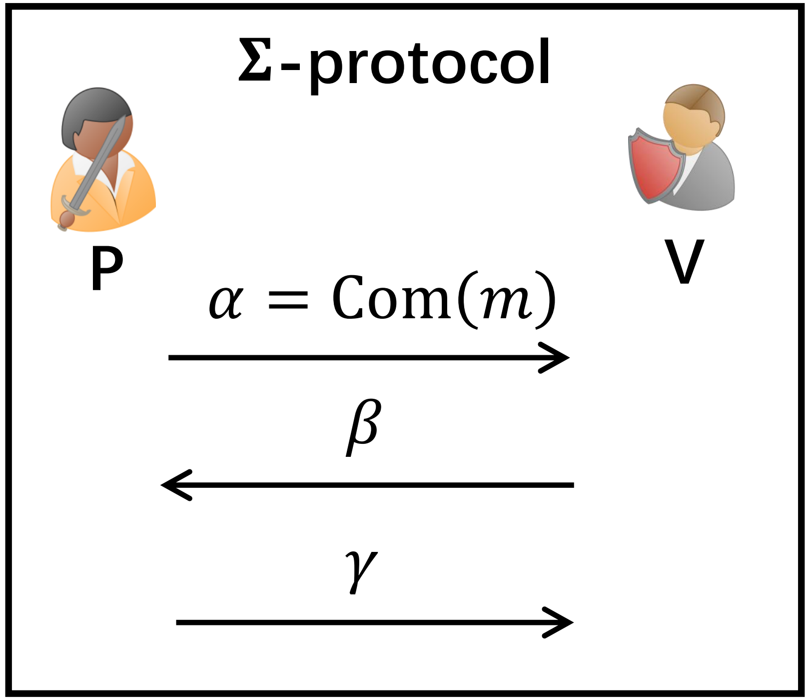


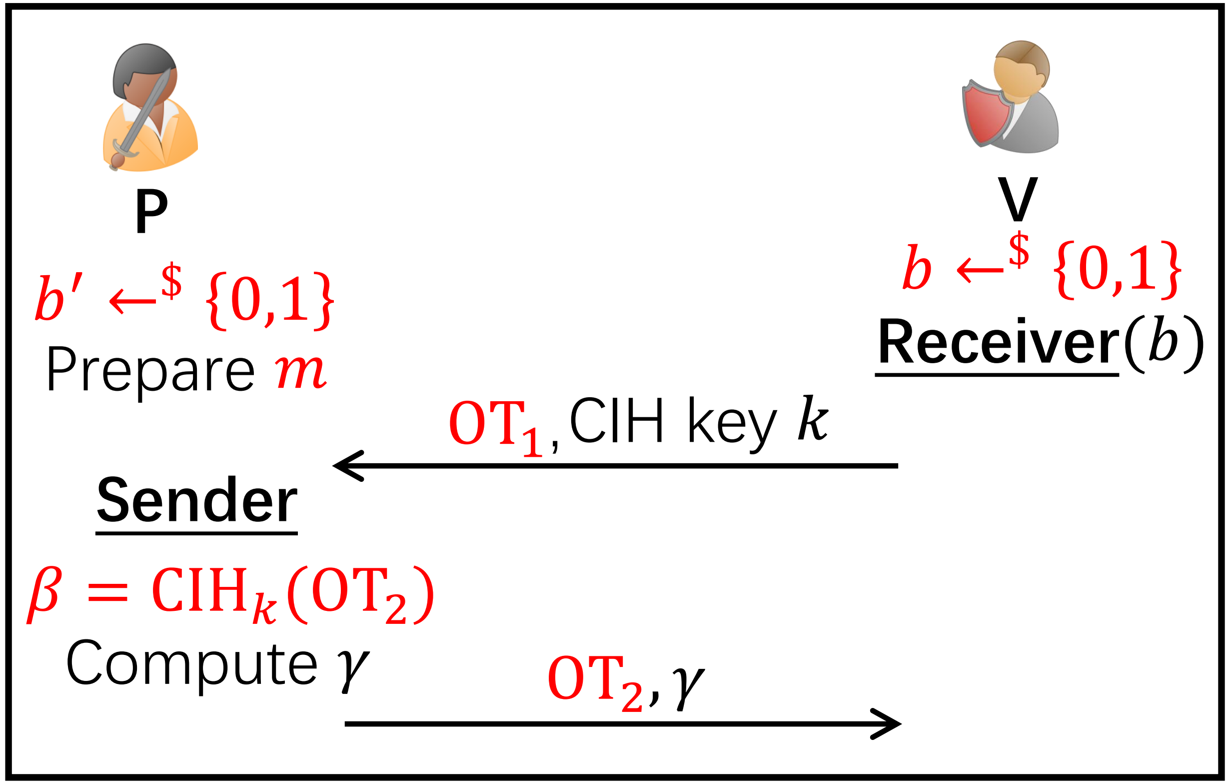
'Weakly Secure' Statistical Zaps





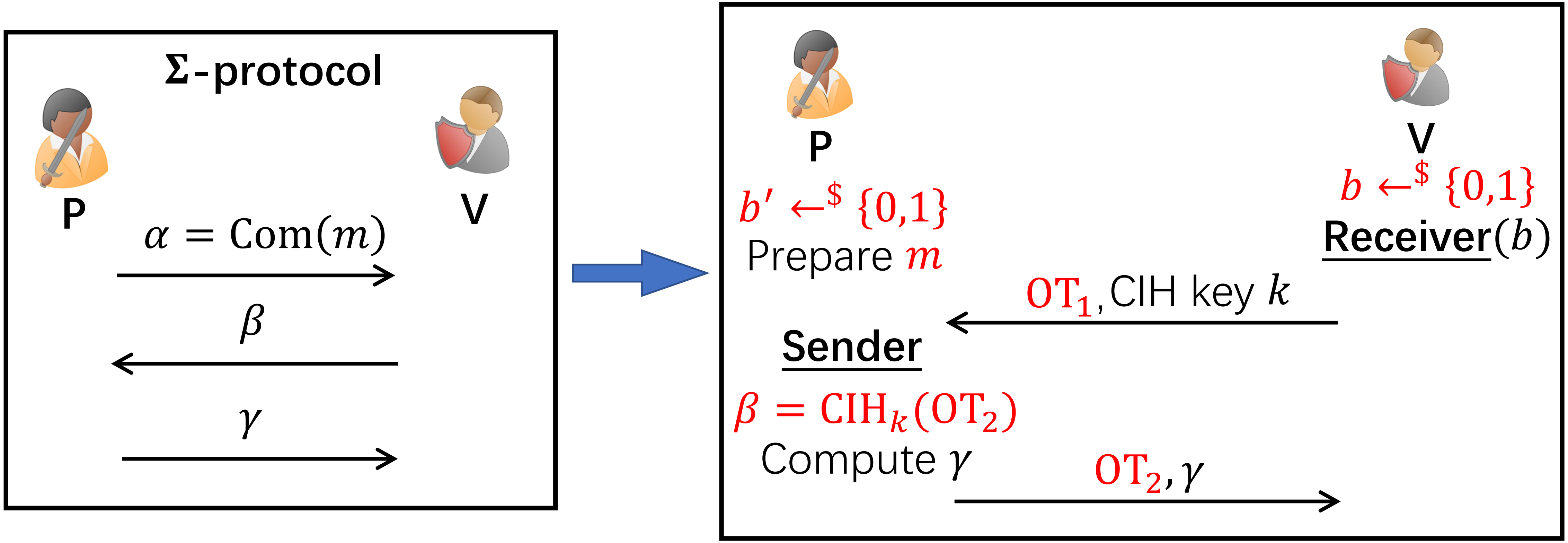
‘Weakly Secure’ Statistical Zaps





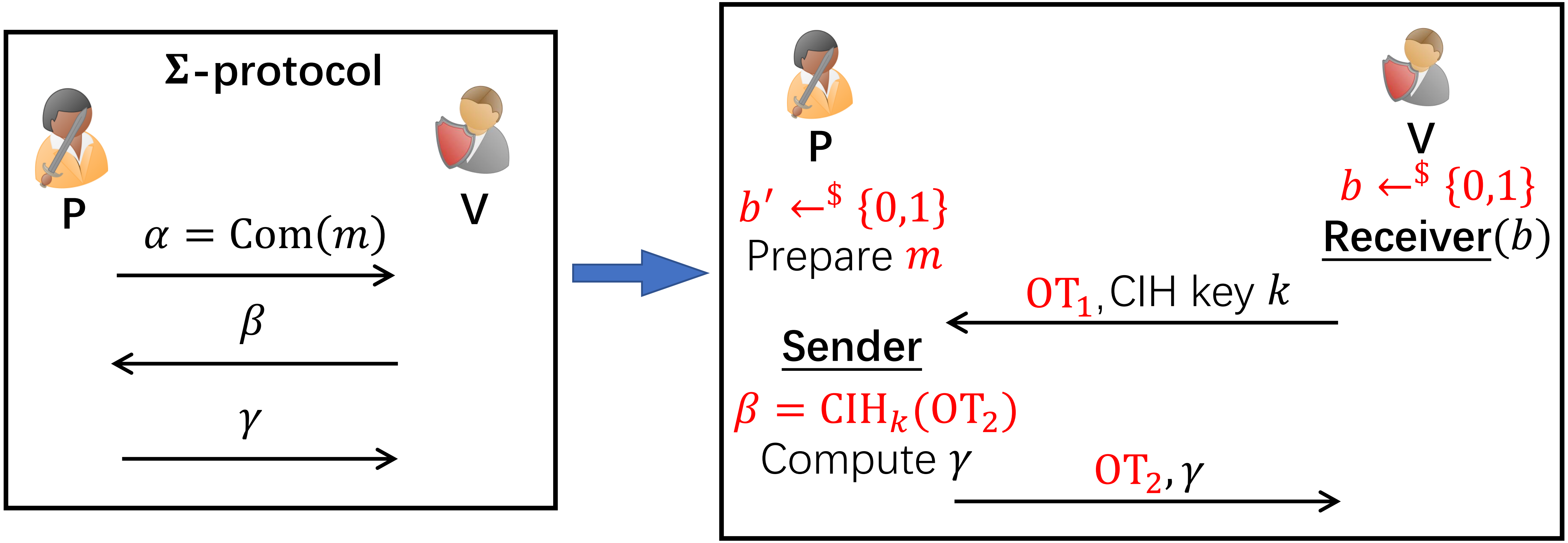
- Statistical WI with $\mathrm{err} \approx 1/2$ (when $b \neq b'$)
- Computational Soundness

‘Weakly Secure’ Statistical Zaps



- Statistical WI with $\mathrm{err} \approx 1/2$ (when $b \neq b'$)
- Computational Soundness

‘Weakly Secure’ Statistical Zaps



- Statistical WI with $\mathrm{err} \approx 1/2$ (when $b \neq b'$)
- Computational Soundness

Amplify the Security

Sender

Receiver

Amplify the Security

Sender

$\boldsymbol{b}' \leftarrow \{0,1\}^l$

Receiver

$\boldsymbol{b} \leftarrow \{0,1\}^l$

Amplify the Security

Sender

$\boldsymbol{b}' \leftarrow \{0,1\}^l$

Receiver

$\boldsymbol{b} \leftarrow \{0,1\}^l$

Amplify the Security

Sender

$\boldsymbol{b}' \leftarrow \{0,1\}^l$

2^l-positions

$\cdots$	$\perp$	m	$\perp$	$\cdots$

$\boldsymbol{b}'$-th position

Receiver

$\boldsymbol{b} \leftarrow \{0,1\}^l$

Amplify the Security

Sender

Receiver

$\boldsymbol{b}' \leftarrow \{0,1\}^l$

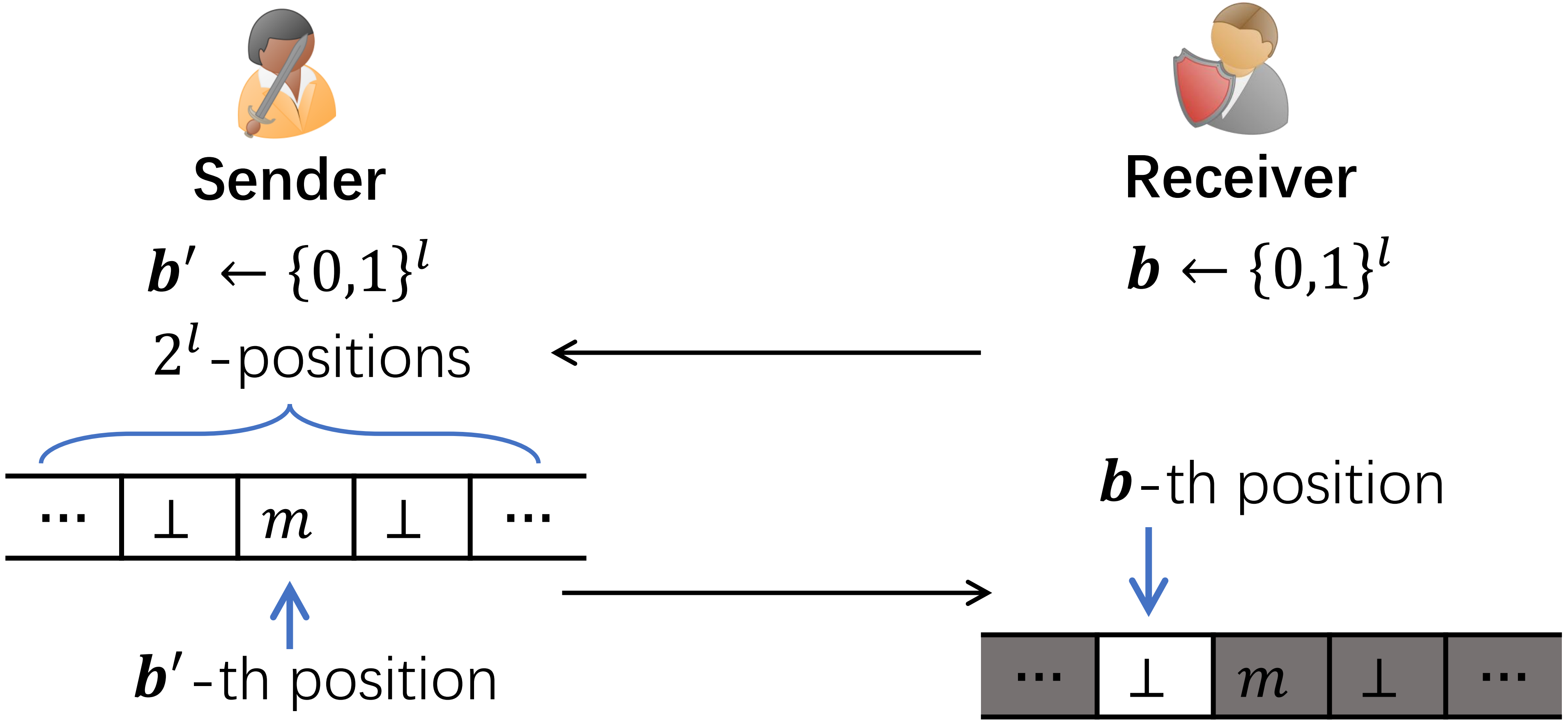
$\boldsymbol{b} \leftarrow \{0,1\}^l$

2^l-positions

$\cdots$	$\perp$	m	$\perp$	$\cdots$

$\boldsymbol{b}'$-th position

Amplify the Security



Amplify the Security

Sender

$\boldsymbol{b'} \leftarrow \{0,1\}^l$

2^l-positions

$\cdots$	$\perp$	m	$\perp$	$\cdots$

$\boldsymbol{b'}$-th position

Receiver

$\boldsymbol{b} \leftarrow \{0,1\}^l$

$\cdots$	$\perp$	m	$\perp$	$\cdots$

Amplify the Security

Sender

$\boldsymbol{b}' \leftarrow \{0,1\}^l$

2^l-positions

$\cdots$	$\perp$	m	$\perp$	$\cdots$

$\boldsymbol{b}'$-th position

Receiver

$\boldsymbol{b} \leftarrow \{0,1\}^l$

With $\Pr = 1 - 2^{-l}$,

$\boldsymbol{b} \neq \boldsymbol{b}'$, hide m √

$\cdots$	$\perp$	m	$\perp$	$\cdots$

Amplify the Security

Sender

$\boldsymbol{b}' \leftarrow \{0,1\}^l$

2^l-positions

⋯	$\perp$	m	$\perp$	⋯

$\boldsymbol{b}'$-th position

Receiver

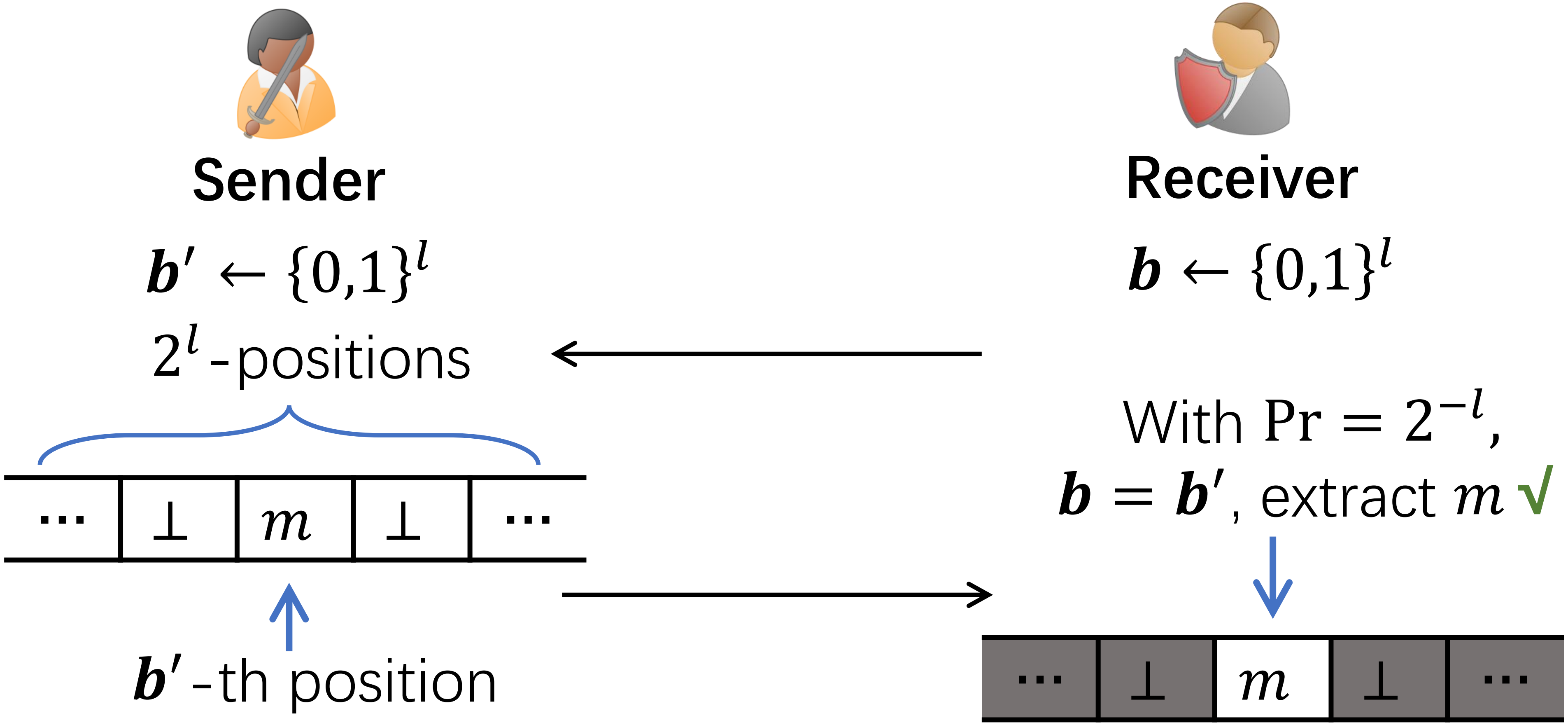
$\boldsymbol{b} \leftarrow \{0,1\}^l$

With $\Pr = 2^{-l}$,

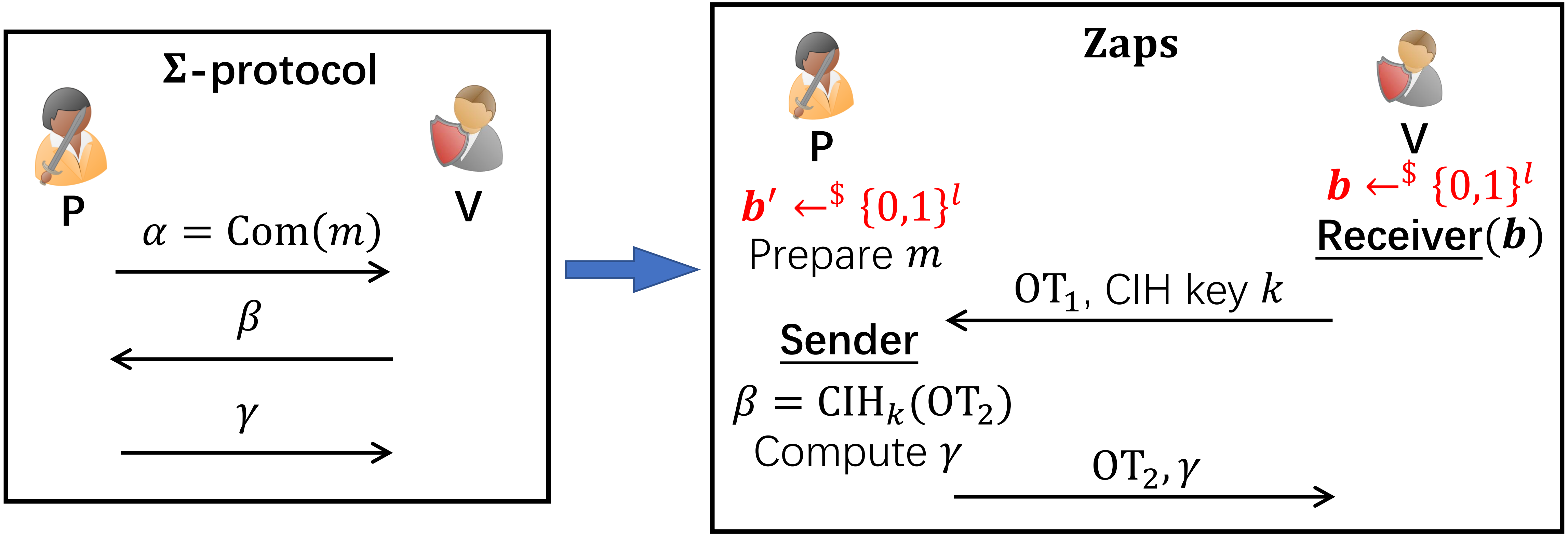
$\boldsymbol{b} = \boldsymbol{b}'$, extract m √

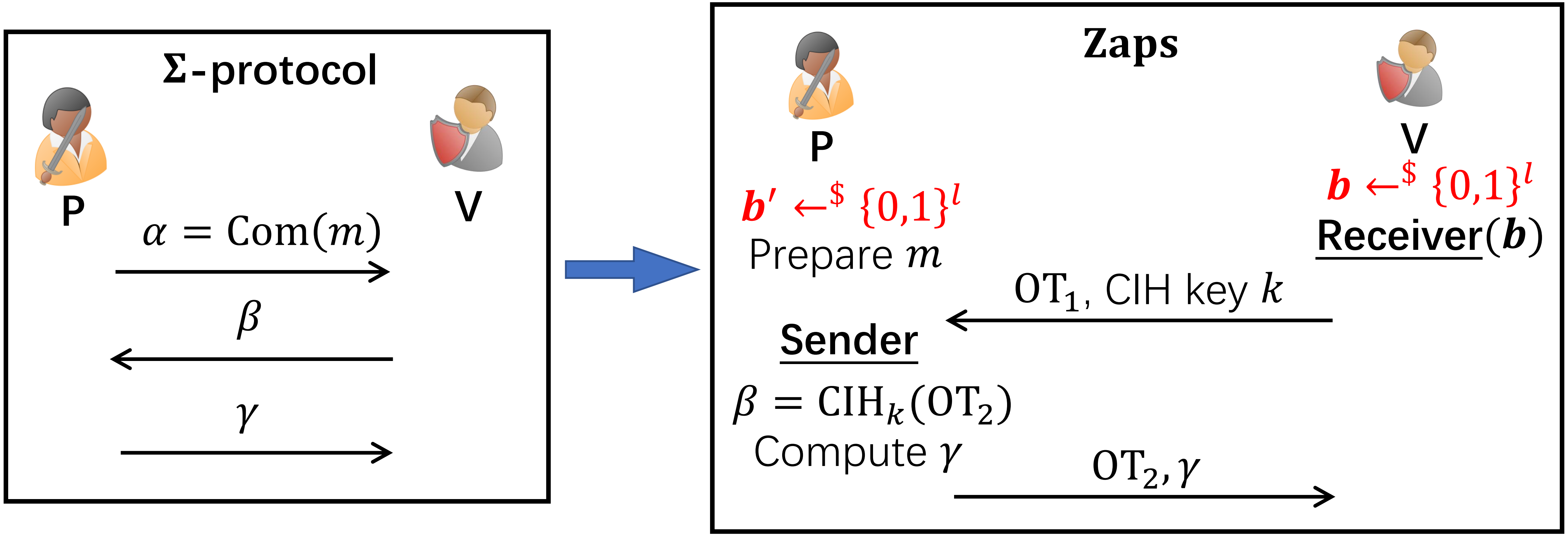
⋯	$\perp$	m	$\perp$	⋯

Amplify the Security

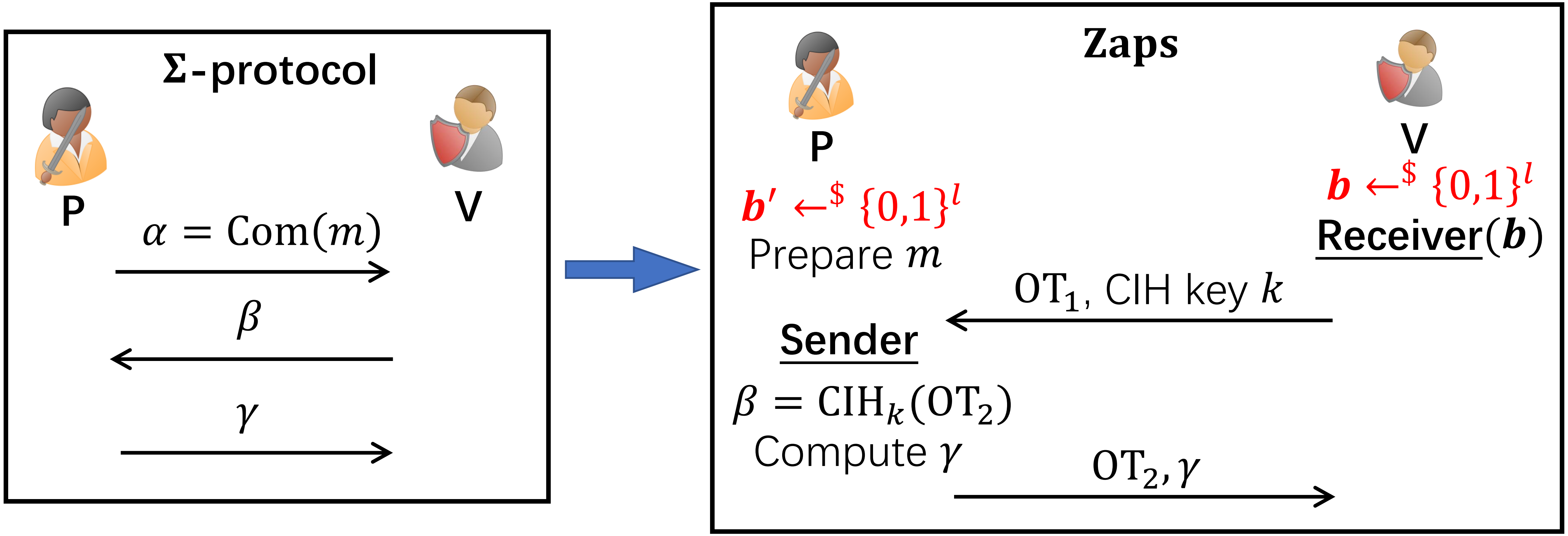


- Can be abstracted as a 2-round statistical hiding extractable commitment [KKS18]

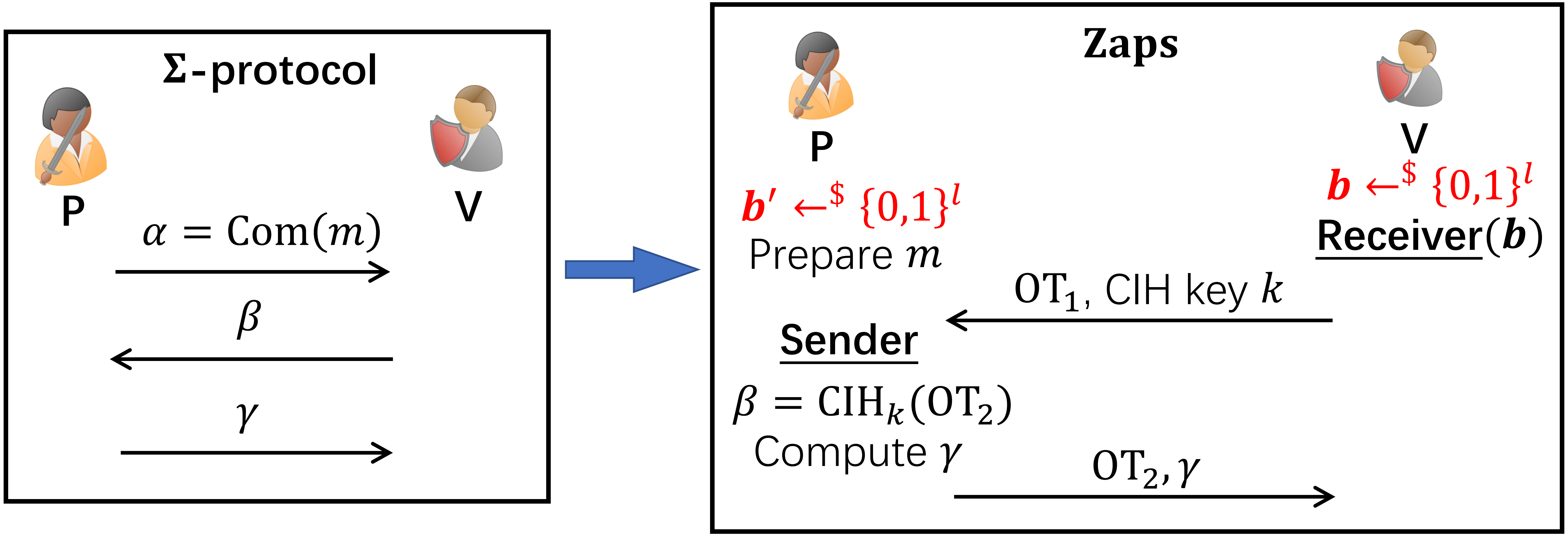

Σ-protocol
P
V
$\alpha = \mathrm{Com}(m)$
β
γ
Zaps
P
V
$b' \leftarrow^{\$} \{0,1\}^l$
$b \leftarrow^{\$} \{0,1\}^l$
Prepare m
Receiver(b)
OT_1, CIH key k
Sender
$\beta = \mathrm{CIH}_k(\mathrm{OT}_2)$
Compute γ
OT_2, γ



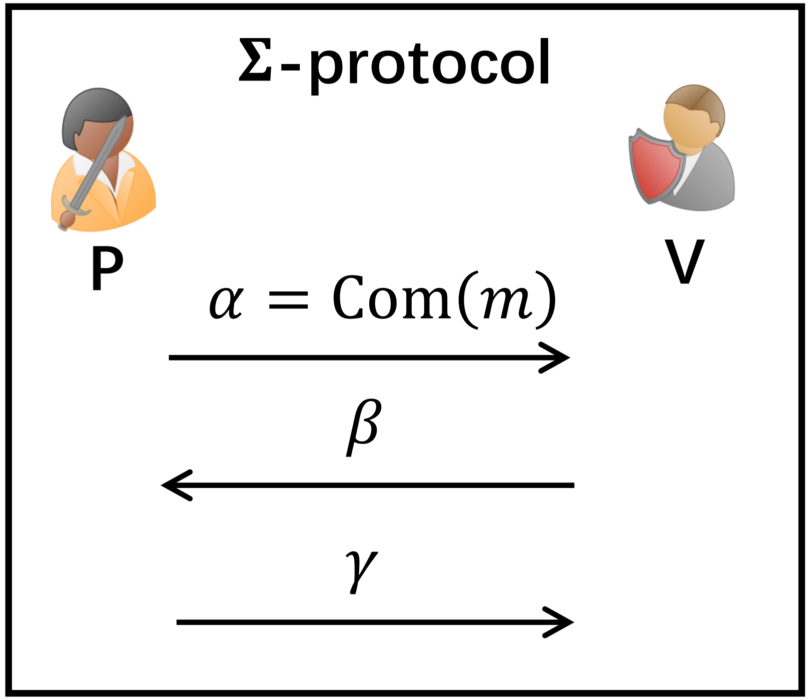
- Statistical WI with $\mathrm{err} \approx 1/2^{l}$ (negligible)
- Computational Soundness via Complexity Leveraging
- Public Coin Property : OT_1 is pseudorandom

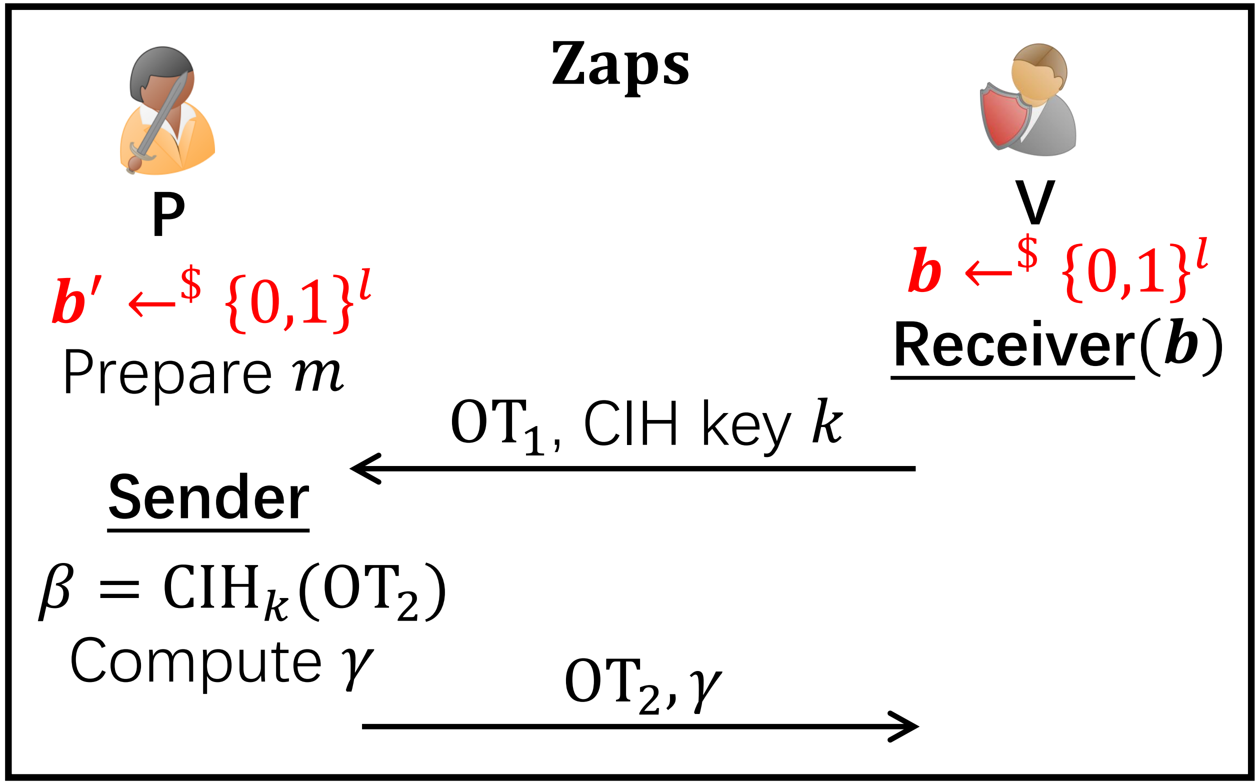


- Statistical WI with $\mathrm{err} \approx 1/2^l$ (negligible)
- Computational Soundness via Complexity Leveraging
- Public Coin Property : OT_1 is pseudorandom



- Statistical WI with $\mathrm{err} \approx 1/2^l$ (negligible)
- Computational Soundness via Complexity Leveraging
- Public Coin Property : OT_1 is pseudorandom



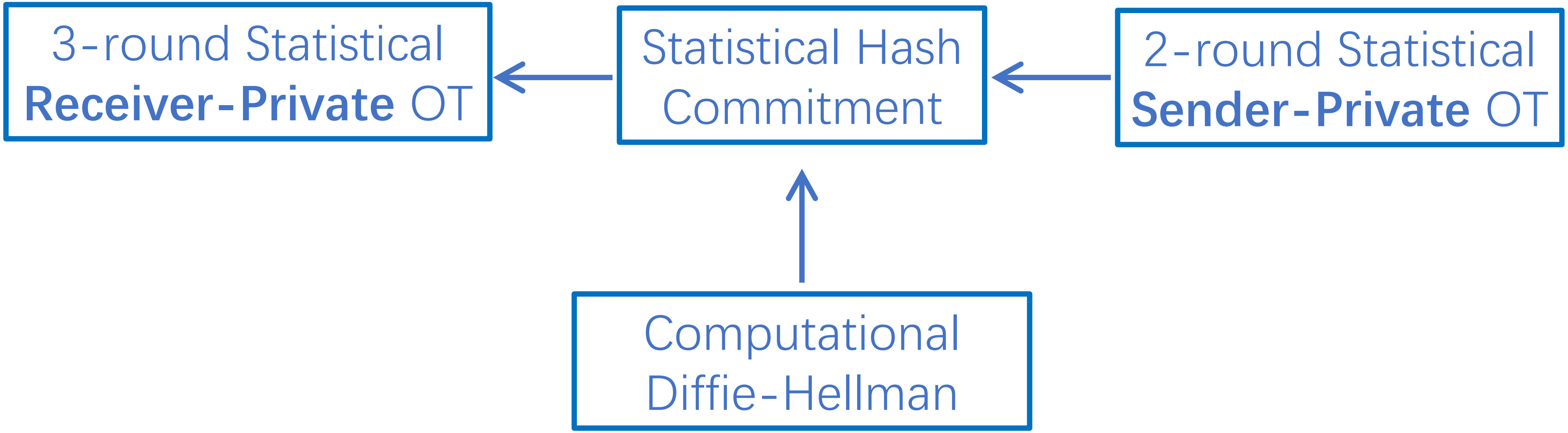


- Statistical WI with $\mathrm{err} \approx 1/2^l$ (negligible)
- Computational Soundness via Complexity Leveraging
- Public Coin Property : OT_1 is pseudorandom

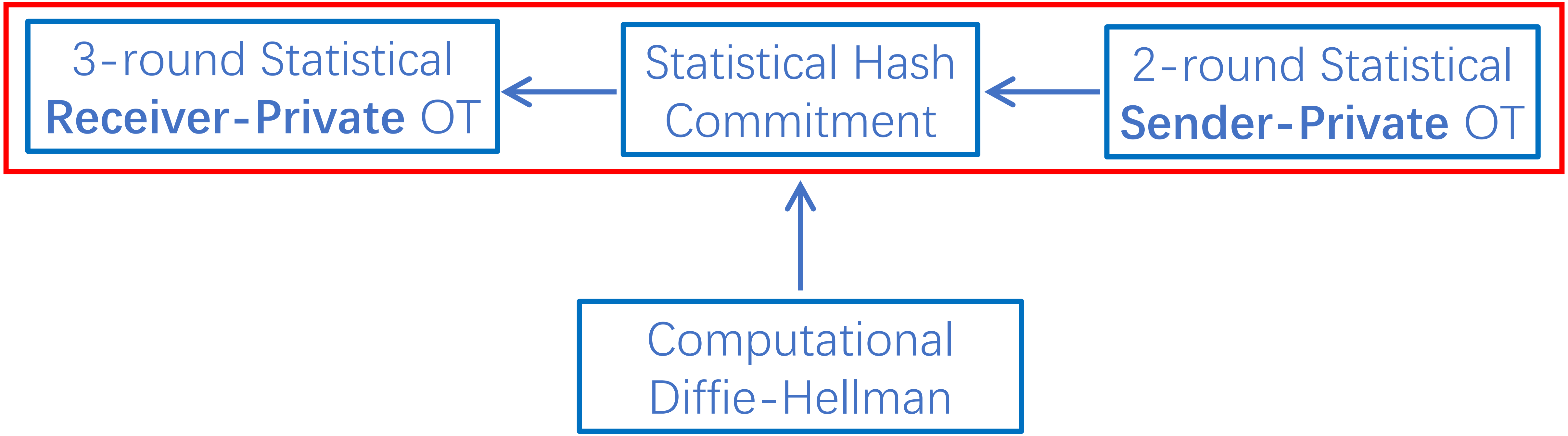
Statistical Zaps

Technical Details
Part II: Oblivious Transfer (OT)

Technical Details
Part II: Oblivious Transfer (OT)



Technical Details
Part II: Oblivious Transfer (OT)



Statistical Receiver-Private OT

Sender

m_0	m_1

Receiver($\beta \in \{0,1\}$)

$\longrightarrow$

$\longleftarrow$

$\longrightarrow$

Get m_β

m_0	m_1

Statistical Receiver-Private OT

Sender

m_0	m_1

Receiver($\beta \in \{0,1\}$)

$\longrightarrow$

$\longleftarrow$

$\longrightarrow$

Get m_β

m_0	m_1

Statistical Receiver-Privacy: β is statistical hidden

Main Tool: Statistical Hash Commitments (SHC)

Main Tool: Statistical Hash Commitments (SHC)

Receiver

Committer$(\beta \in \{0,1\})$

Main Tool: Statistical Hash Commitments (SHC)

Receiver

Committing Phase:

Committer($\beta \in \{0,1\}$)

Main Tool: Statistical Hash Commitments (SHC)

Receiver

Committer$(\beta \in \{0,1\})$

Committing Phase:

Main Tool: Statistical Hash Commitments (SHC)

Receiver

Committer$(\beta \in \{0,1\})$

Committing Phase:

$\longrightarrow$

$\longleftarrow$

Opening Phase:

Main Tool: Statistical Hash Commitments (SHC)

Receiver **Committer**($\beta \in \{0,1\}$)

Committing Phase:

Opening Phase:

Hash value for $\beta = 0$:

Hash value for $\beta = 1$:

Main Tool: Statistical Hash Commitments (SHC)

Receiver

Committer$(\beta \in \{0,1\})$

Committing Phase:

Opening Phase:

Hash value for $\beta = 0$:

Hash value for $\beta = 1$:

β,

Main Tool: Statistical Hash Commitments (SHC)

Receiver

Committer($\beta \in \{0,1\}$)

Committing Phase:

$\longrightarrow$

$\longleftarrow$

Opening Phase:

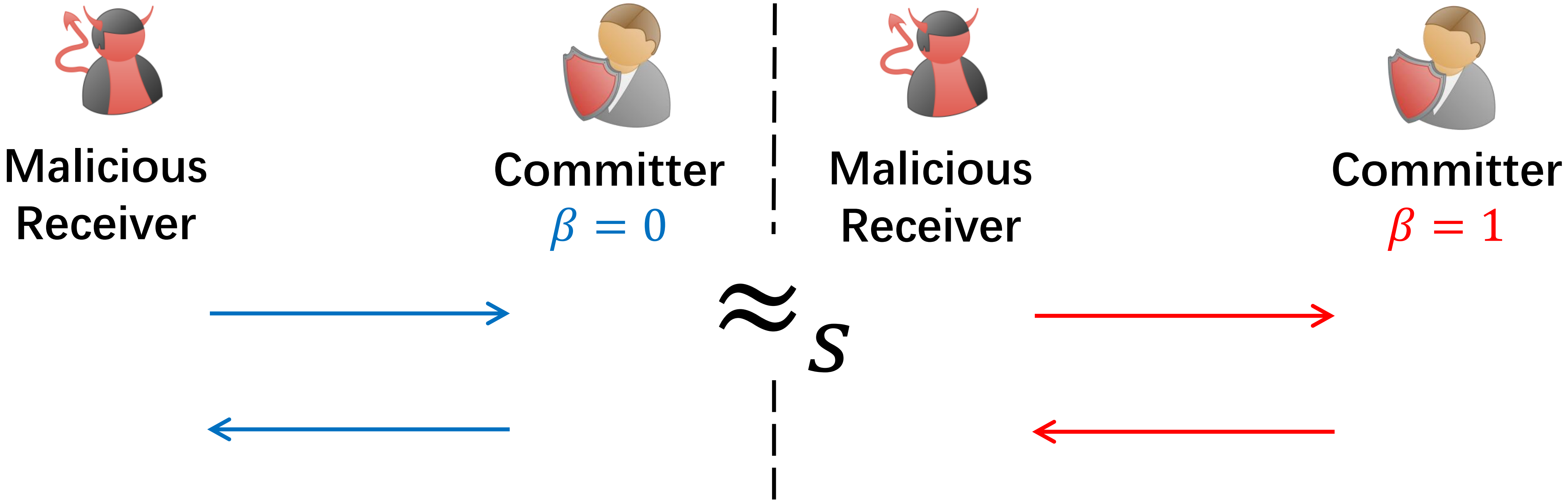
Hash value for $\beta = 0$:

Hash value for $\beta = 1$:

β,

Check $=?$

Statistical **H**ash **C**ommitments (SHC): Statistical Hiding Property



Statistical **H**ash **C**ommitments (SHC): Computational Binding

Receiver

Malicious Committer

Committing Phase:

Hash value for $\beta = 0$:

Hash value for $\beta = 1$:

Statistical **H**ash **C**ommitments (SHC): Computational Binding

Receiver

Malicious Committer

Committing Phase:

Hash value for $\beta = 0$:

Hash value for $\beta = 1$:

Computational Binding:

it's hard for committer to find both

3-round Statistical Receiver-Private OT from SHC

3-round Statistical Receiver-Private OT from SHC

Sender(m_0, m_1)

Receiver$(b \in \{0,1\})$

3-round Statistical Receiver-Private OT from SHC

Sender(m_0, m_1)

Committing Phase

Receiver$(b \in \{0,1\})$

Hash values for opening:

b

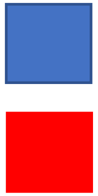
3-round Statistical Receiver-Private OT from SHC

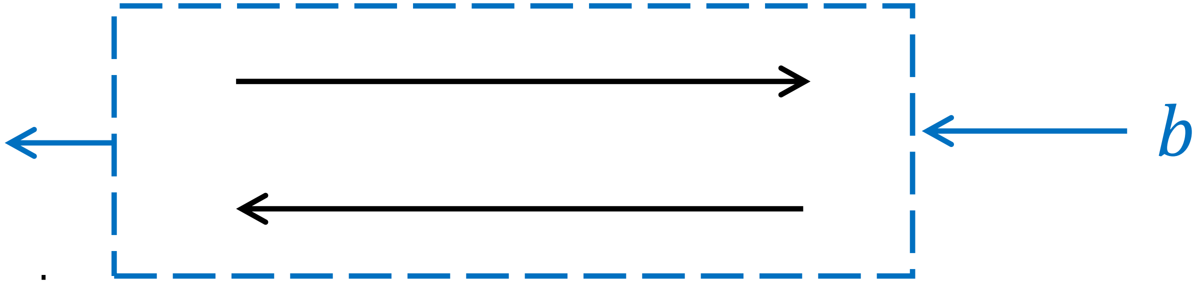
Sender(m_0, m_1)

Committing Phase

Receiver$(b \in \{0,1\})$

Hash values for opening:





$hc(\cdot)$: Goldreich-Levin hardcore predicate

3-round Statistical Receiver-Private OT from SHC

Sender(m_0, m_1)

Committing Phase

Receiver$(b \in \{0,1\})$

b

Hash values for opening:

$hc(\cdot)$: Goldreich-Levin hardcore predicate

$hc(\ ) \oplus m_0$

$hc(\ ) \oplus m_1$

3-round Statistical Receiver-Private OT from SHC

Sender(m_0, m_1) **Committing Phase** **Receiver**$(b \in \{0,1\})$

Hash values for opening: $\boxed{}$ $\boxed{}$

b

$hc(\cdot)$: Goldreich-Levin hardcore predicate

$hc(\boxed{}) \oplus m_0$

$hc(\boxed{}) \oplus m_1$

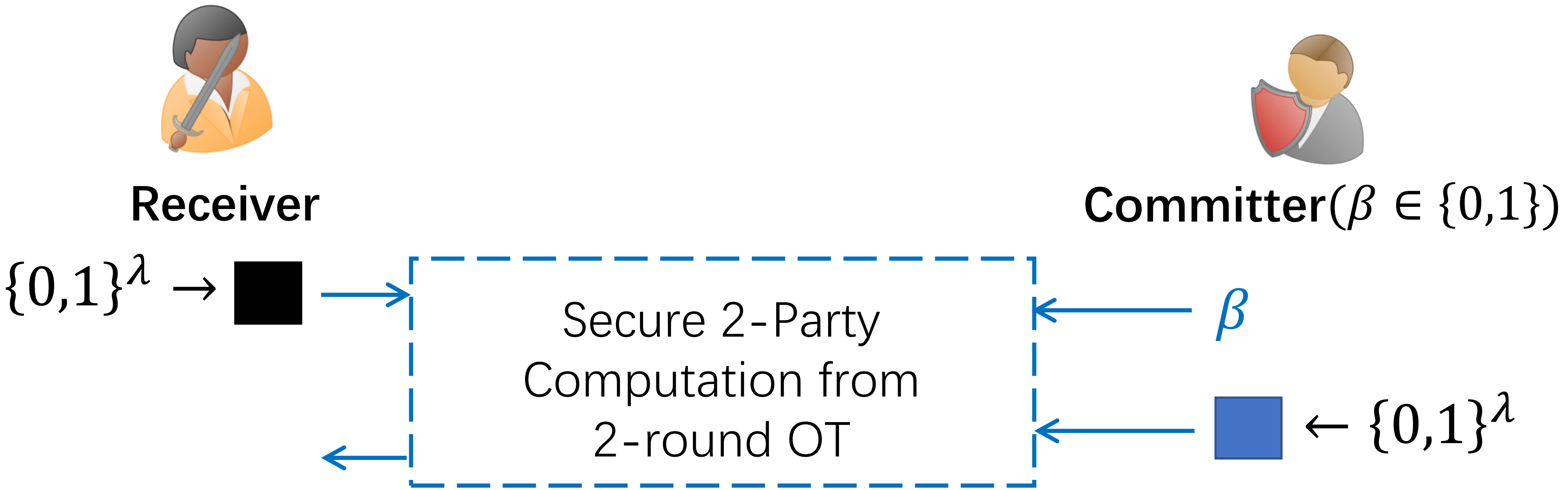
- Statistical Hiding ⇒ Statistical Receiver-Private
- Computational Binding ⇒ Computational Sender-Private

Statistical Hash Commitment from 2-round OT

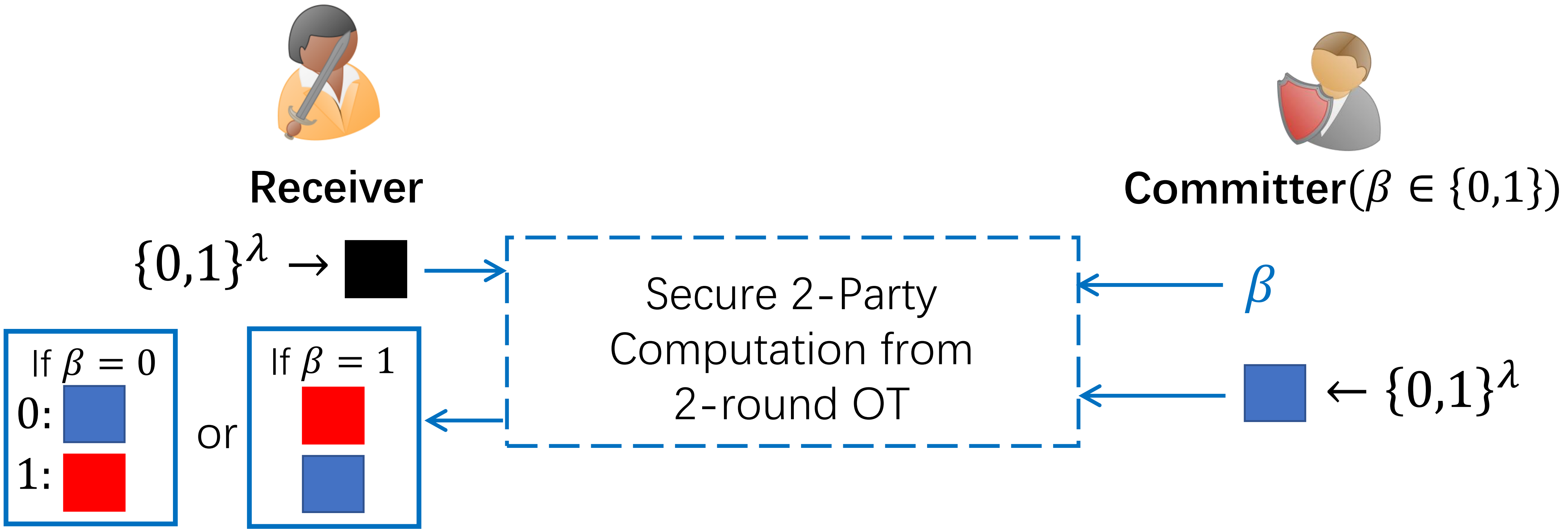
Receiver

Committer$(\beta \in \{0,1\})$

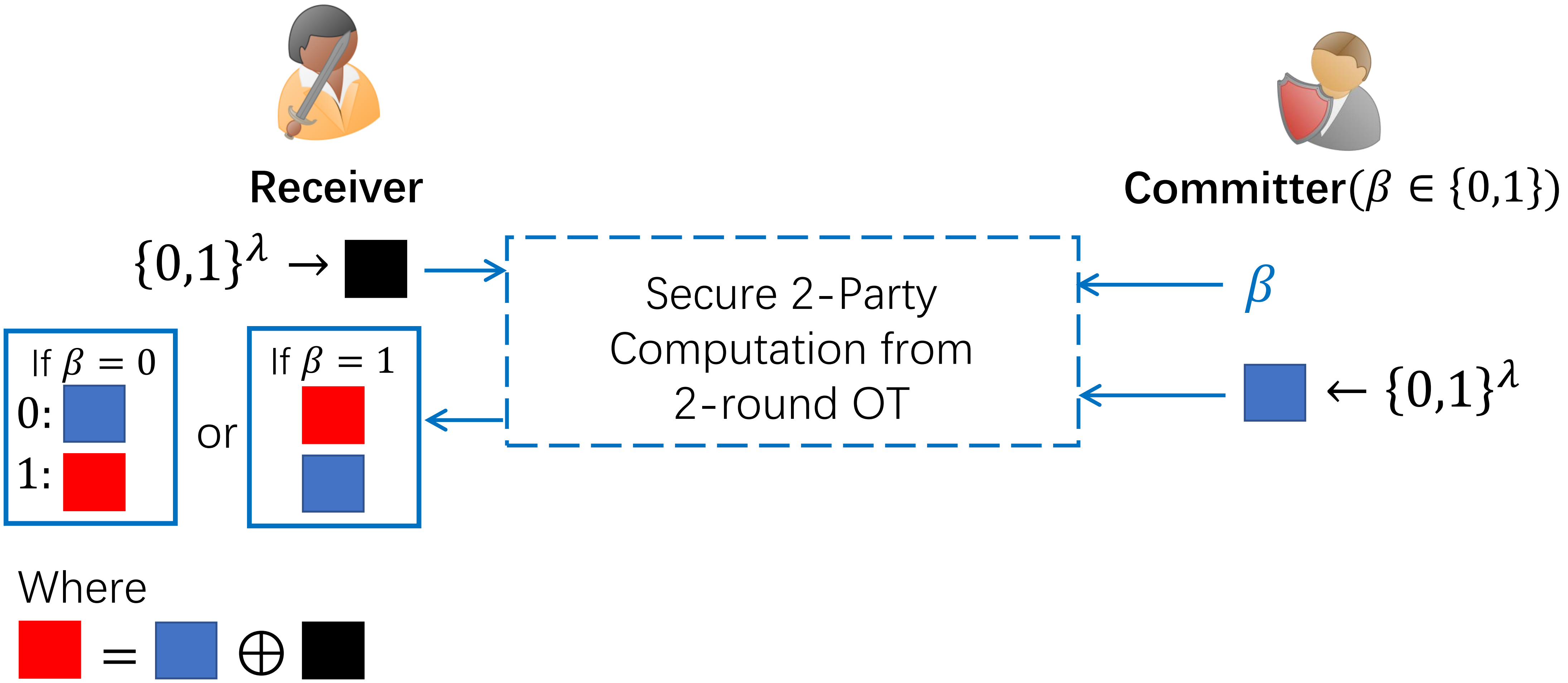
Statistical Hash Commitment from 2-round OT



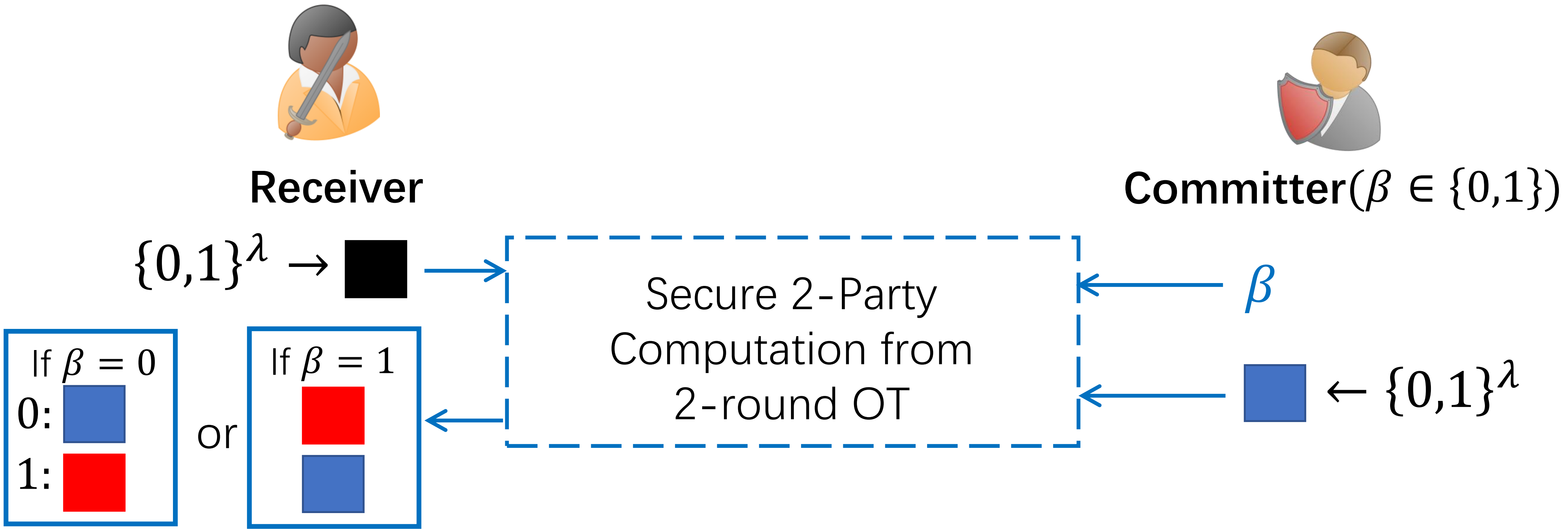
Statistical Hash Commitment from 2-round OT



Statistical Hash Commitment from 2-round OT



Statistical Hash Commitment from 2-round OT



Where

- Statistical Sender-Privacy of OT ⇒ Statistical Hiding
- Computational Hiding of ■ ⇒ Computational Binding

Summary of Results

- Statistical Zaps from quasi-poly hardness Learning with Errors
- 3-round statistical receiver-private oblivious transfer from poly hardness
  - 2-round statistical sender-private oblivious transfer
  - Computational Diffie-Hellman Assumption

Full version : [ia.cr/2020/235](ia.cr/2020/235)

Thank you!