Non-Interactive Batch Arguments for NP from Standard Assumptions

Arka Rai Choudhuri

Johns Hopkins University

Abhishek Jain

Johns Hopkins University

Zhengzhong Jin

Johns Hopkins University

Crypto 2021

Non-Interactive Batch Arguments for NP

CRS

$C, x_1, \cdots, x_k$

$C, x_1, \cdots, x_k$

Non-Interactive Batch Arguments for NP

CRS

$C, x_1, \cdots, x_k$

$C, x_1, \cdots, x_k$

$\text{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \text{SAT}$

Non-Interactive Batch Arguments for NP

CRS

Π

$C, x_1, \cdots, x_k$ $\qquad$ $C, x_1, \cdots, x_k$

$$\mathrm{SAT} = \{(C, x) \mid \exists w\ s.t.\ C(x, w) = 1\}$$

$$\forall i \in [k],\ (C, x_i) \in \mathrm{SAT}$$

Non-Interactive Batch Arguments for NP

CRS

Π

$C, x_1, \cdots, x_k$

$C, x_1, \cdots, x_k$

Π is publicly verifiable

$\mathrm{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Non-Interactive Batch Arguments for NP

CRS

$C, x_1, \cdots, x_k$

Π

$\longrightarrow$

$C, x_1, \cdots, x_k$

Π is publicly verifiable

No PPT  can produce accepting Π if

$\exists i^* \in [k], (C, x_{i^*}) \cancel{\in} \mathrm{SAT}$

$\mathrm{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Non-Interactive Batch Arguments for NP

CRS

Π

$C, x_1, \cdots, x_k$

$C, x_1, \cdots, x_k$

Π is publicly verifiable

$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t.\; C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Non-Interactive Batch Arguments for NP

CRS

$C, x_1, \cdots, x_k$

$w_1, \ldots, w_k$

$C, x_1, \cdots, x_k$

Π is publicly verifiable

$$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$$

$$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$$

Non-Interactive Batch Arguments for NP

CRS

$C, x_1, \cdots, x_k$

$\ll |w| \cdot k$

Π

$C, x_1, \cdots, x_k$

Π is publicly verifiable

$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Non-Interactive Batch Arguments for NP

CRS

$C, x_1, \cdots, x_k$

$\ll |w| \cdot k$

Π

$C, x_1, \cdots, x_k$

Verifier running time:
$k \cdot |x| + |\Pi|$

Π is publicly verifiable

$$\text{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$$

$$\forall i \in [k], (C, x_i) \in \text{SAT}$$

Prior Works

Prior Works

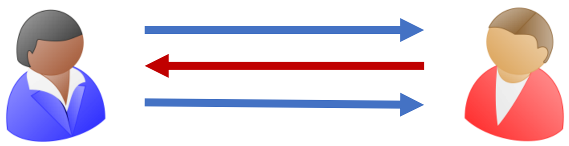
Interactive batch proofs

[Reingold-Rothblum-Rothblum’16, Reingold-Rothblum-Rothblum’18, Rothblum-Rothblum’20]

Prior Works

Interactive batch proofs

[Reingold-Rothblum-Rothblum'16, Reingold-Rothblum-Rothblum'18, Rothblum-Rothblum'20]

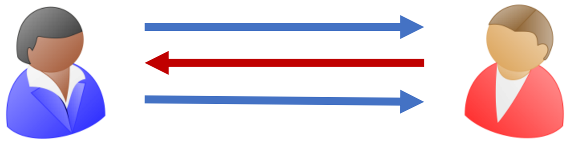


Secure against unbounded cheating prover.

Prior Works

Interactive batch proofs for UP

[Reingold-Rothblum-Rothblum'16, Reingold-Rothblum-Rothblum'18, Rothblum-Rothblum'20]



UP – each statement has a unique witness.

Prior Works

Interactive batch proofs for UP

[Reingold-Rothblum-Rothblum'16, Reingold-Rothblum-Rothblum'18, Rothblum-Rothblum'20]

Succinct Non-interactive Arguments (SNARGs) for NP

[Micali'94, Damgård-Faust-Hazay'12, Bitansky-Canetti-Chiesa-Tromer'13, Bitanksy-Canetti-Chiesa-Goldwasser-Lin-Rubinstein-Tromer'16]

SNARGs

$|\Pi| \ll |w|$

$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Prior Works

Interactive batch proofs for UP

[Reingold-Rothblum-Rothblum'16, Reingold-Rothblum-Rothblum'18, Rothblum-Rothblum'20]

Succinct Non-interactive Arguments (SNARGs) for NP

[Micali'94, Damgård-Faust-Hazay'12, Bitansky-Canetti-Chiesa-Tromer'13, Bitanksy-Canetti-Chiesa-Goldwasser-Lin-Rubinstein-Tromer'16]

SNARGs

$|\Pi| \ll |w|$

$$\mathrm{SAT}^{\otimes k} = \{(C, x_1, \cdots, x_k) \mid \forall i \in [k], (C, x_i) \in \mathrm{SAT}\}$$

$$\mathrm{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$$

$$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$$

Prior Works

Interactive batch proofs for UP

[Reingold-Rothblum-Rothblum'16, Reingold-Rothblum-Rothblum'18, Rothblum-Rothblum'20]

SNARGs for NP from Non-falsifiable assumptions/ Random oracle model

[Micali'94, Damgård-Faust-Hazay'12, Bitansky-Canetti-Chiesa-Tromer'13, Bitanksy-Canetti-Chiesa-Goldwasser-Lin-Rubinstein-Tromer'16]

SNARGs

$|\Pi| \ll |w|$

$$\mathrm{SAT}^{\otimes k} = \{(C, x_1, \cdots, x_k) \mid \forall i \in [k], (C, x_i) \in \mathrm{SAT}\}$$

$$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$$

$$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$$

Prior Works

Interactive batch proofs for UP

[Reingold-Rothblum-Rothblum'16, Reingold-Rothblum-Rothblum'18, Rothblum-Rothblum'20]

SNARGs for NP from Non-falsifiable assumptions/ Random oracle model

[Micali'94, Damgård-Faust-Hazay'12, Bitansky-Canetti-Chiesa-Tromer'13, Bitanksy-Canetti-Chiesa-Goldwasser-Lin-Rubinstein-Tromer'16]

Designated Verifier non-interactive batch arguments for NP

[Brakerski-Holmgren-Kalai'17, Brakerski-Kalai'20]

Prior Works

Interactive batch proofs for UP

[Reingold-Rothblum-Rothblum'16, Reingold-Rothblum-Rothblum'18, Rothblum-Rothblum'20]

SNARGs for NP from Non-falsifiable assumptions/ Random oracle model

[Micali'94, Damgård-Faust-Hazay'12, Bitansky-Canetti-Chiesa-Tromer'13, Bitanksy-Canetti-Chiesa-Goldwasser-Lin-Rubinstein-Tromer'16]

Designated Verifier from standard assumptions

[Brakerski-Holmgren-Kalai'17, Brakerski-Kalai'20]

Prior Works

Interactive batch proofs for UP

[Reingold-Rothblum-Rothblum'16, Reingold-Rothblum-Rothblum'18, Rothblum-Rothblum'20]

SNARGs for NP from Non-falsifiable assumptions/ Random oracle model

[Micali'94, Damgård-Faust-Hazay'12, Bitansky-Canetti-Chiesa-Tromer'13, Bitanksy-Canetti-Chiesa-Goldwasser-Lin-Rubinstein-Tromer'16]

Designated Verifier from standard assumptions

[Brakerski-Holmgren-Kalai'17, Brakerski-Kalai'20]

Non-interactive batch arguments for NP from new non-standard assumption

[Kalai-Paneth-Yang'19]

Falsifiable assumption on groups with bilinear maps.

Do there exists non-interactive batch arguments for NP based on standard assumptions?

Our Result

Theorem

Assuming QR + (LWE/sub-exp DDH) there exists a non-interactive batch argument for NP where

$$|\Pi| = \tilde{O}(|C| + \sqrt{k|C|})$$

QR – Quadratic residuosity, LWE – Learning with Error, DDH – Decisional Diffie-Hellman

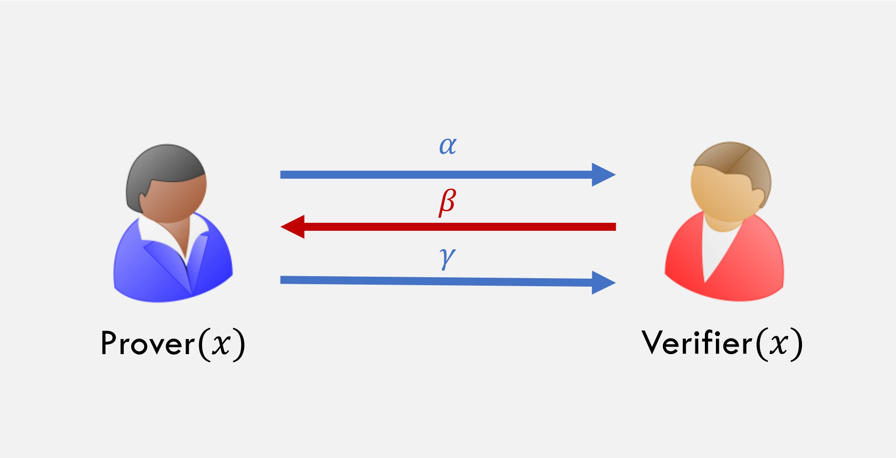
$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t.\; C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Key Insights

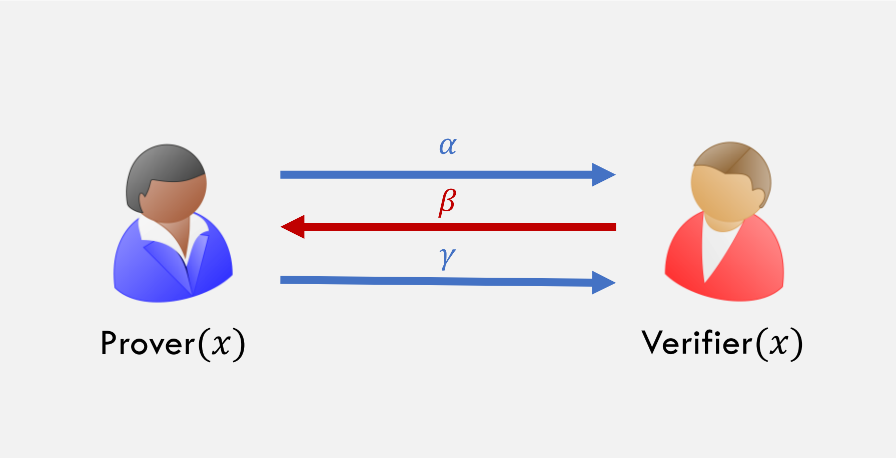
Fiat-Shamir (FS) Methodology

Fiat-Shamir (FS) Methodology



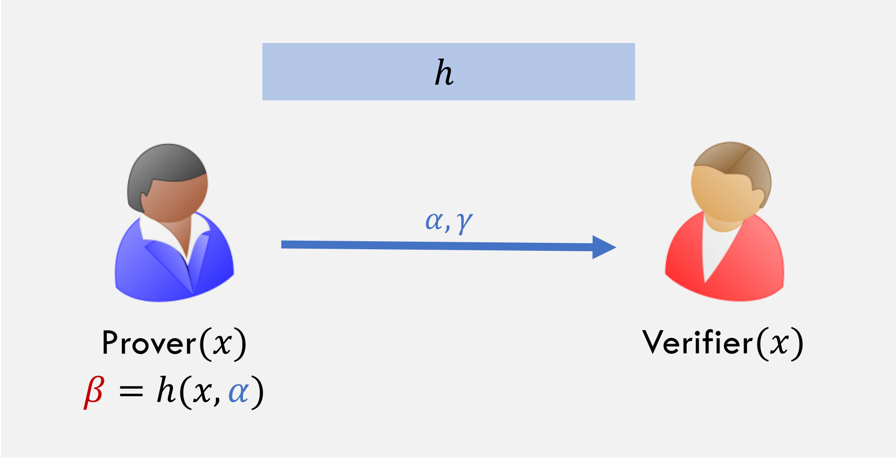
β is a random string

Fiat-Shamir (FS) Methodology

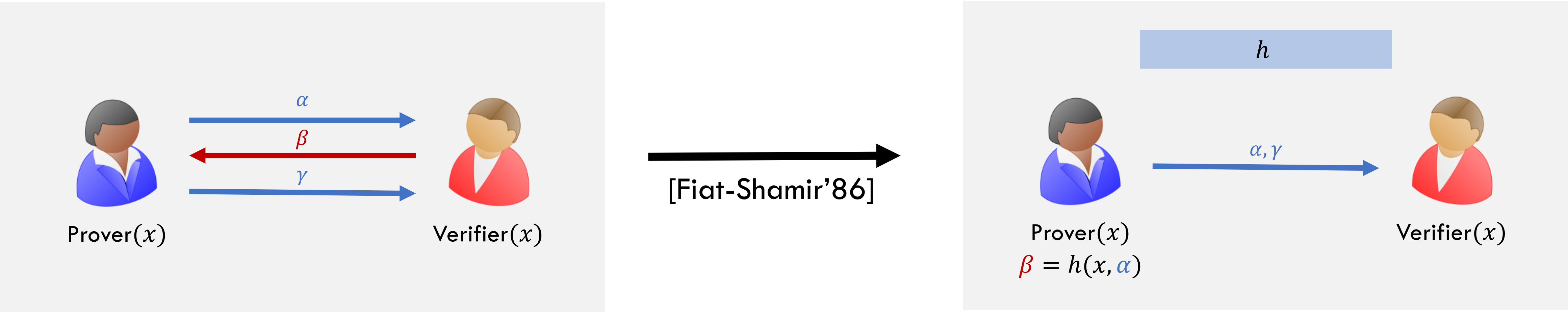


β is a random string

[Fiat-Shamir'86]



Fiat-Shamir (FS) Methodology

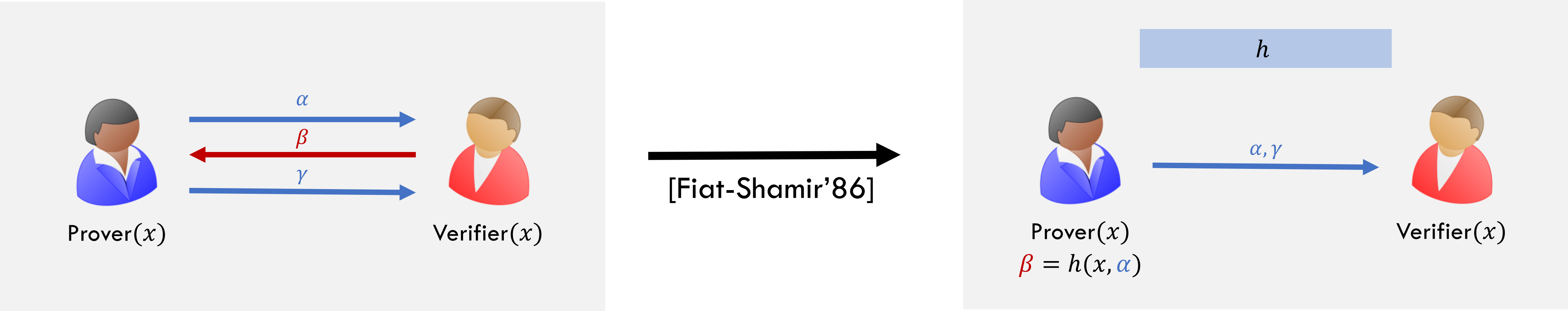


β is a random string

FS methodology is secure for certain protocols under a variety of assumptions (via correlation intractable hash functions)

[Kalai-Rothblum-Rothblum'17, Canetti-Chen-Reyzin-Rothblum'18, Holmgren-Lombardi'18, Canetti-Chen-Holmgren-Lombardi-Rothblum-Rothblum-Wichs'19, Peikert-Sheihian'19, Brakerski-Koppula-Mour'20, Couteau-Katsumata-Ursu'20, Jain-Jin'21, Jawale-Kalai-Khurana-Zhang'21, Holmgren-Lombardi-Rothblum'21]

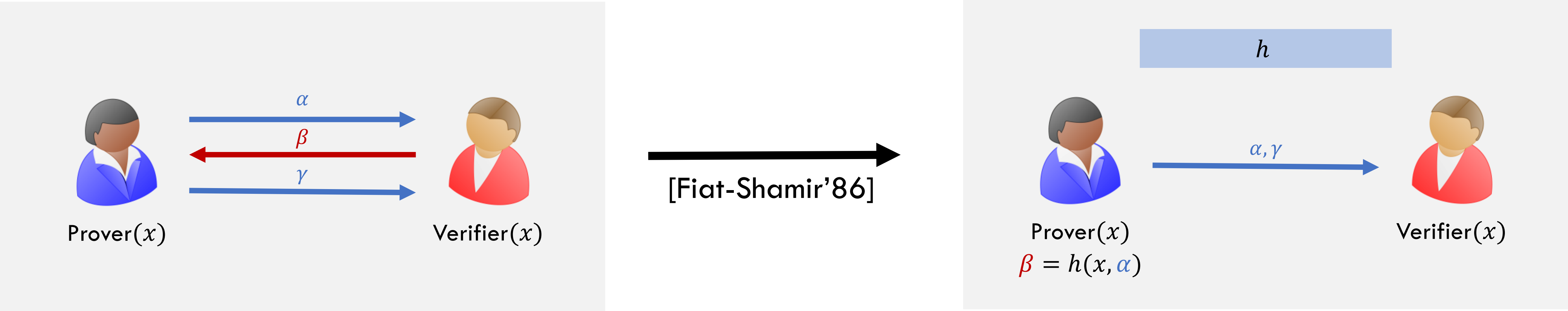
Fiat-Shamir (FS) Methodology



β is a random string

FS methodology is secure for certain protocols under a variety of assumptions (via correlation intractable hash functions)

Fiat-Shamir (FS) Methodology

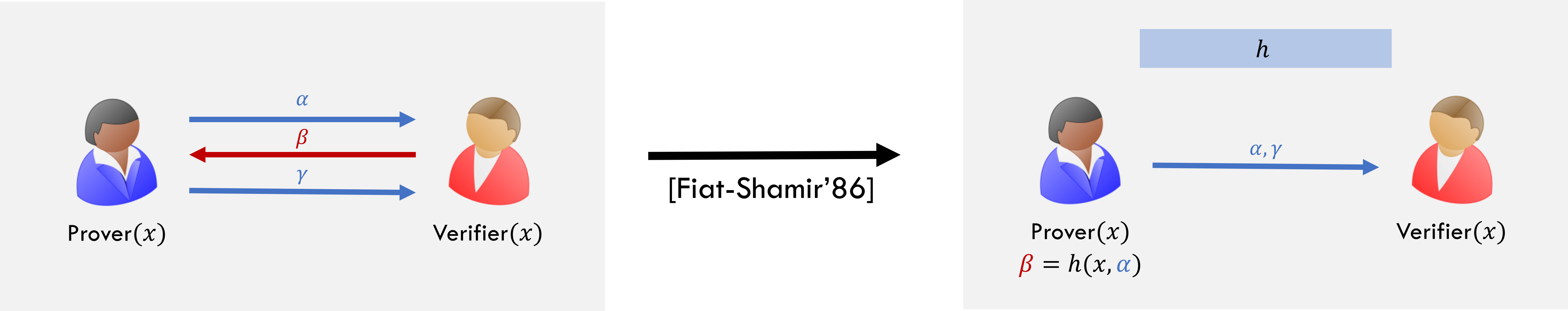


β is a random string

FS methodology is secure for certain protocols under a variety of assumptions (via correlation intractable hash functions)

Proven secure if starting with statistically secure interactive protocols (interactive proofs).

Fiat-Shamir (FS) Methodology



β is a random string

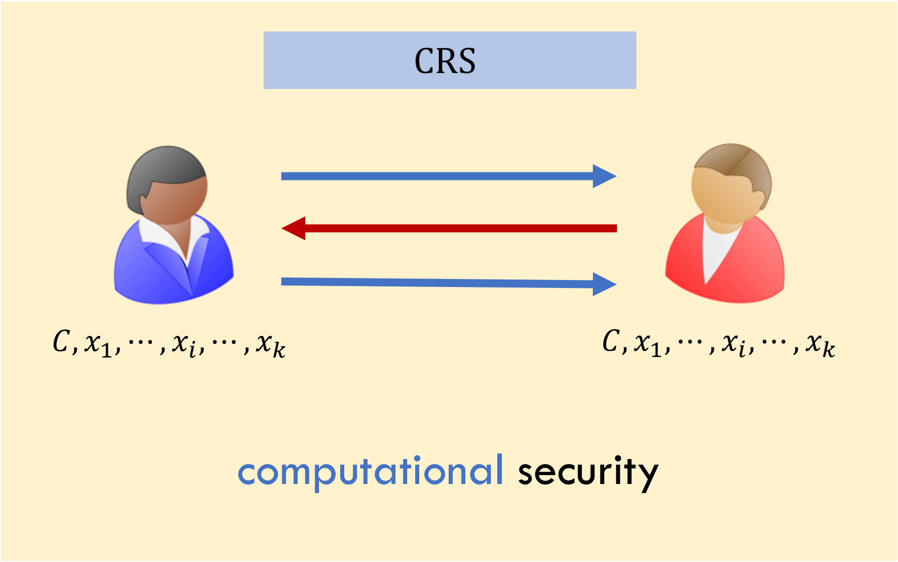
FS methodology is secure for certain protocols under a variety of assumptions (via correlation intractable hash functions)

Proven secure if starting with statistically secure interactive protocols (interactive proofs).

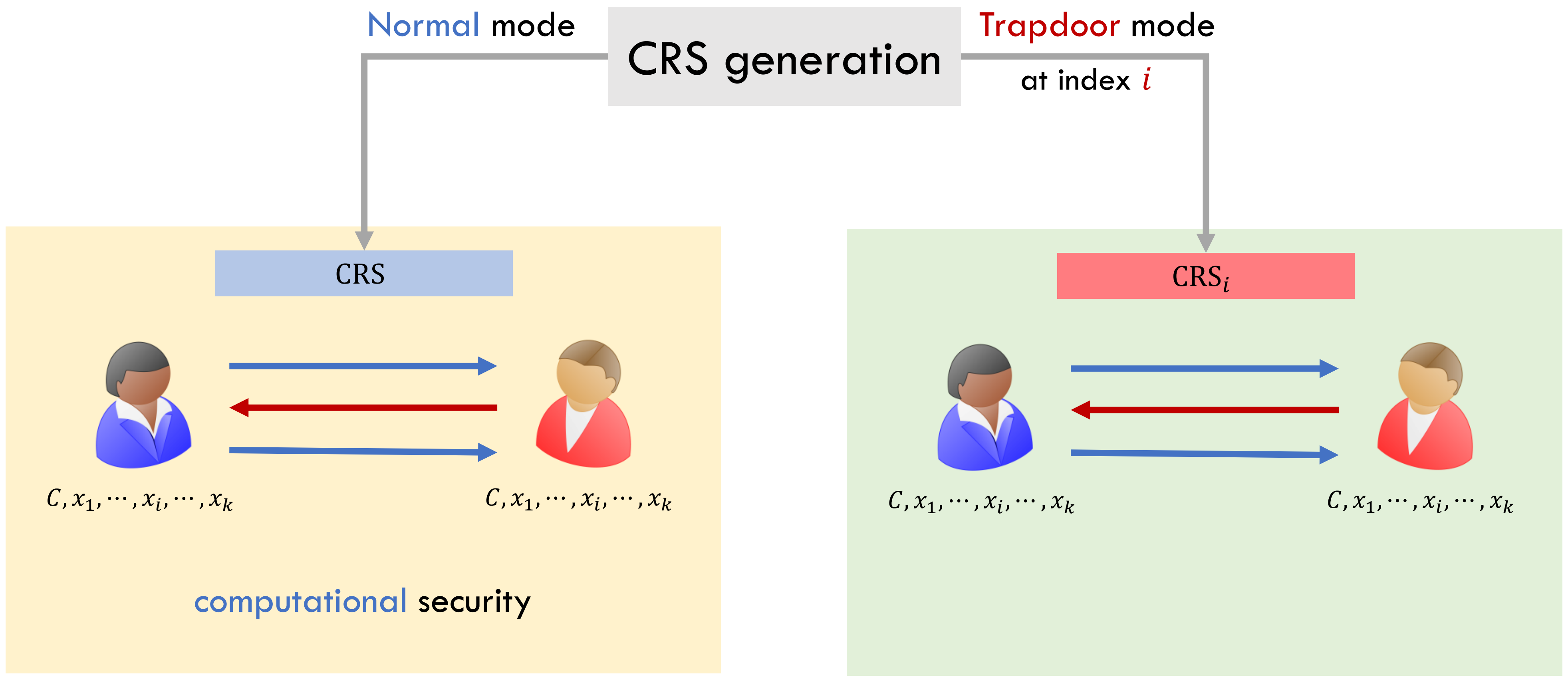
No known interactive proofs for batch NP.

Dual-Mode Interactive Batch Arguments

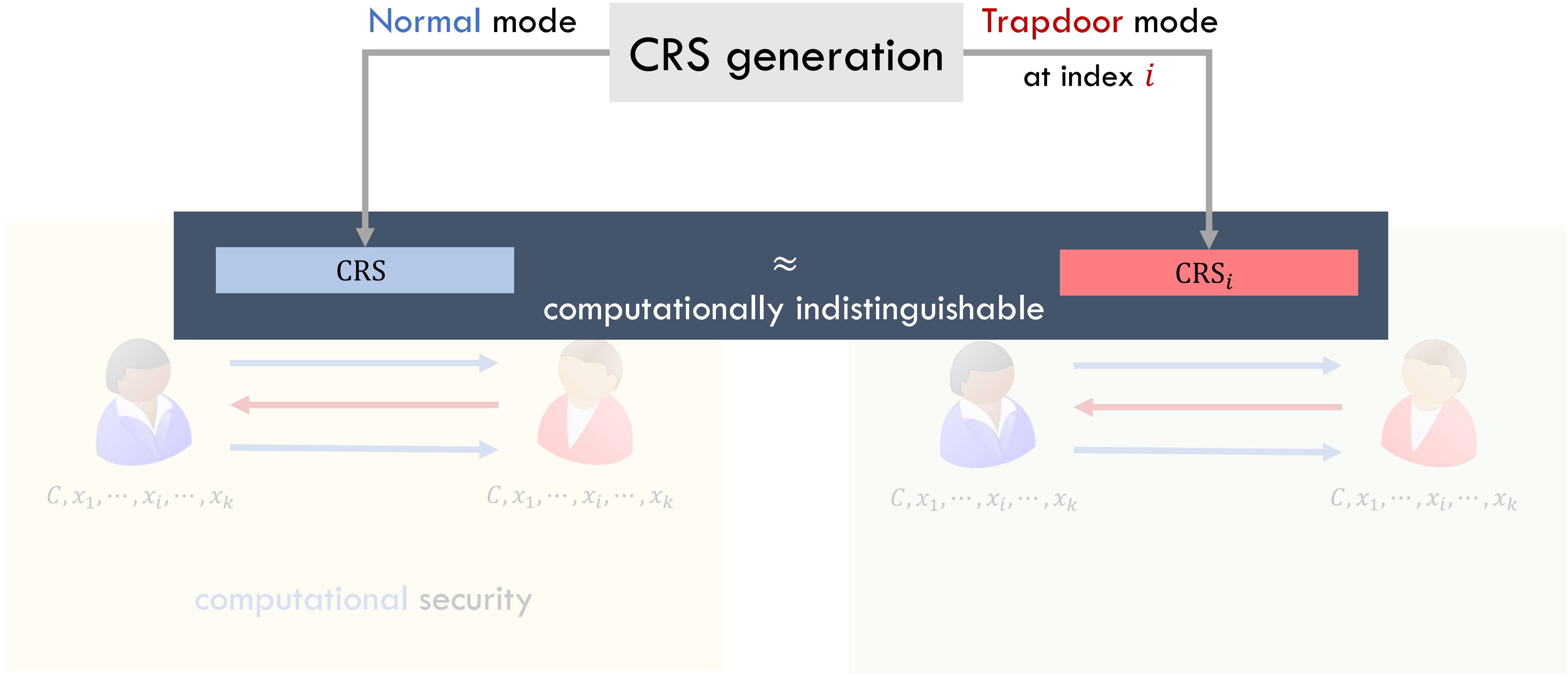
Dual-Mode Interactive Batch Arguments



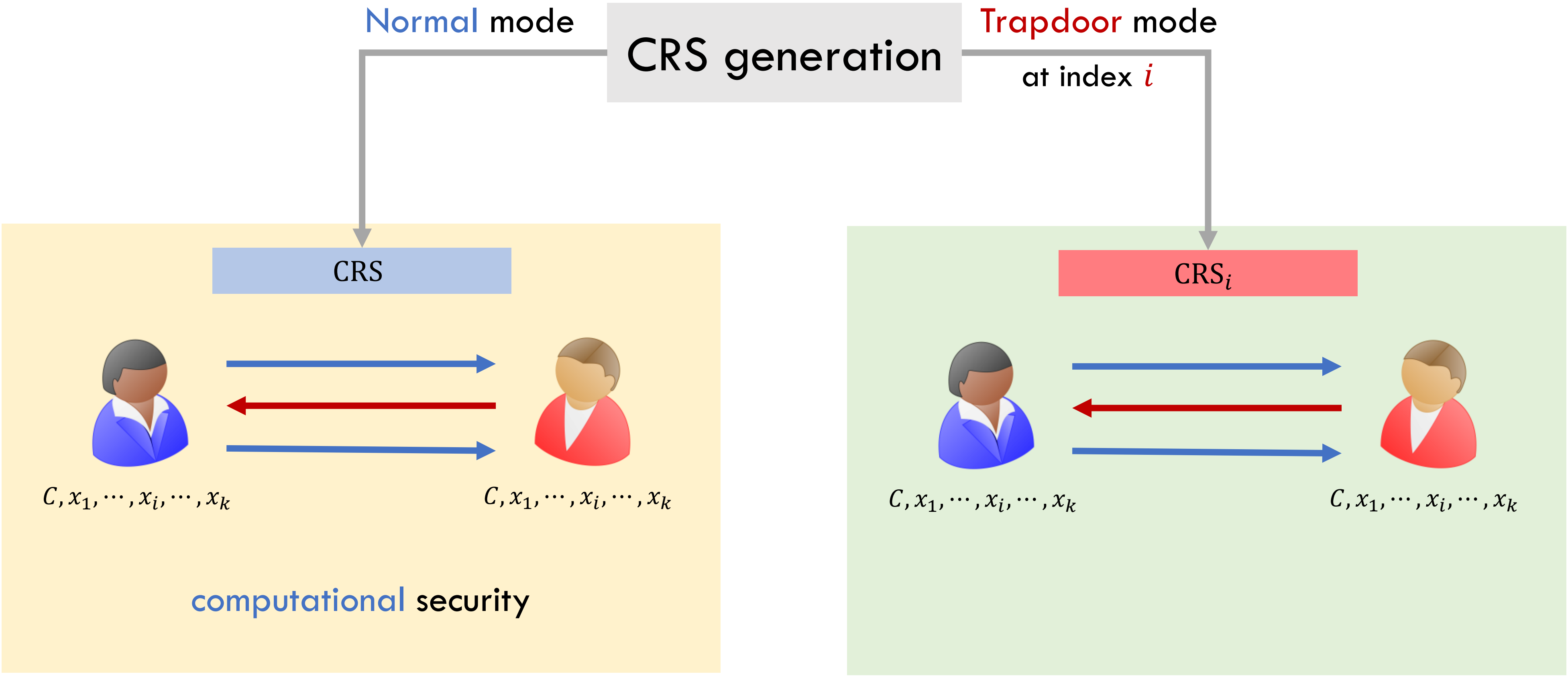
Dual-Mode Interactive Batch Arguments



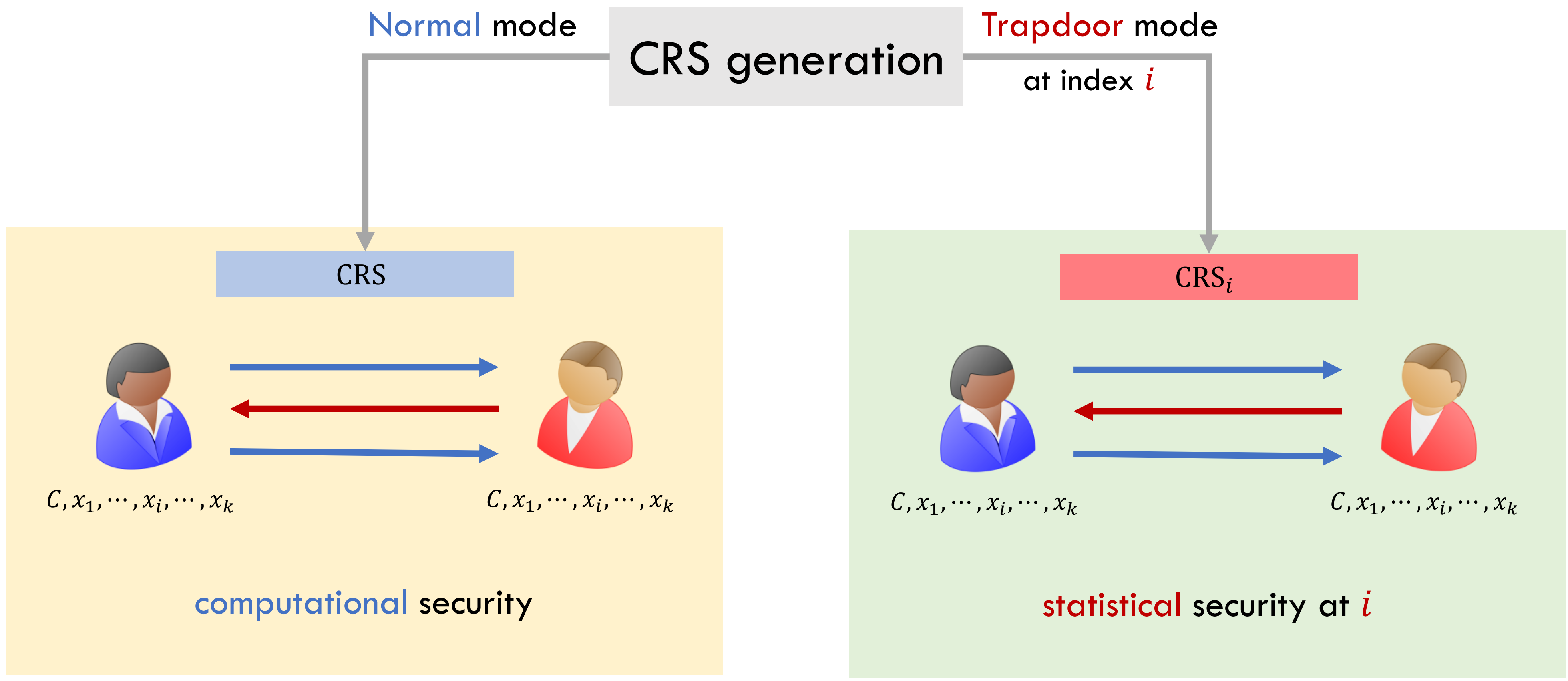
Dual-Mode Interactive Batch Arguments



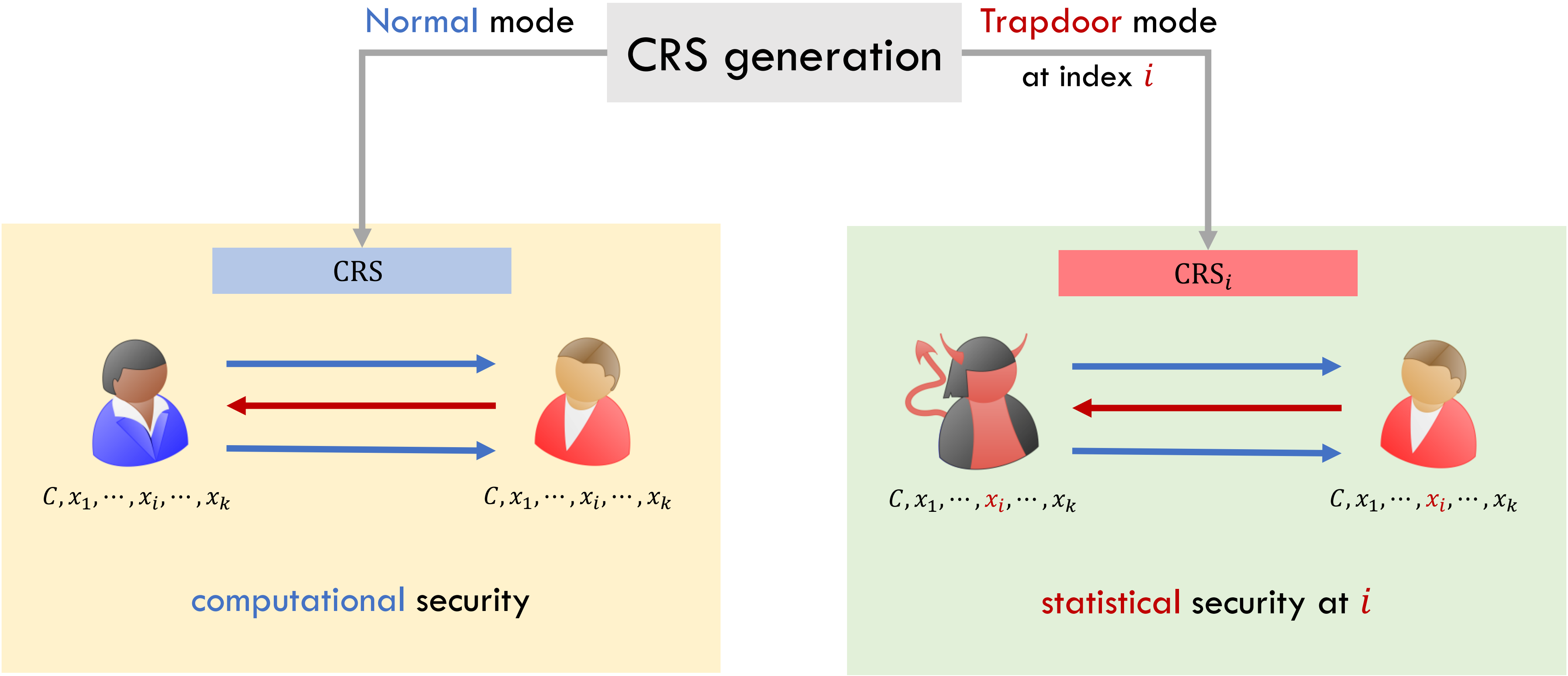
Dual-Mode Interactive Batch Arguments



Dual-Mode Interactive Batch Arguments

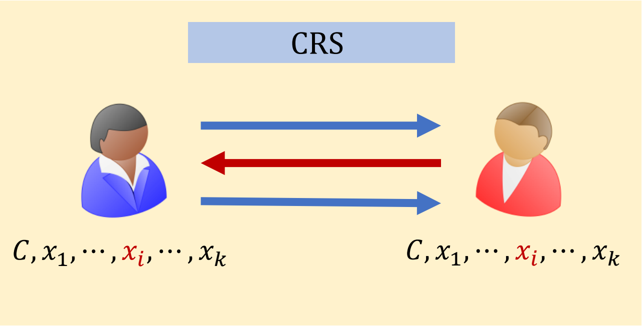


Dual-Mode Interactive Batch Arguments

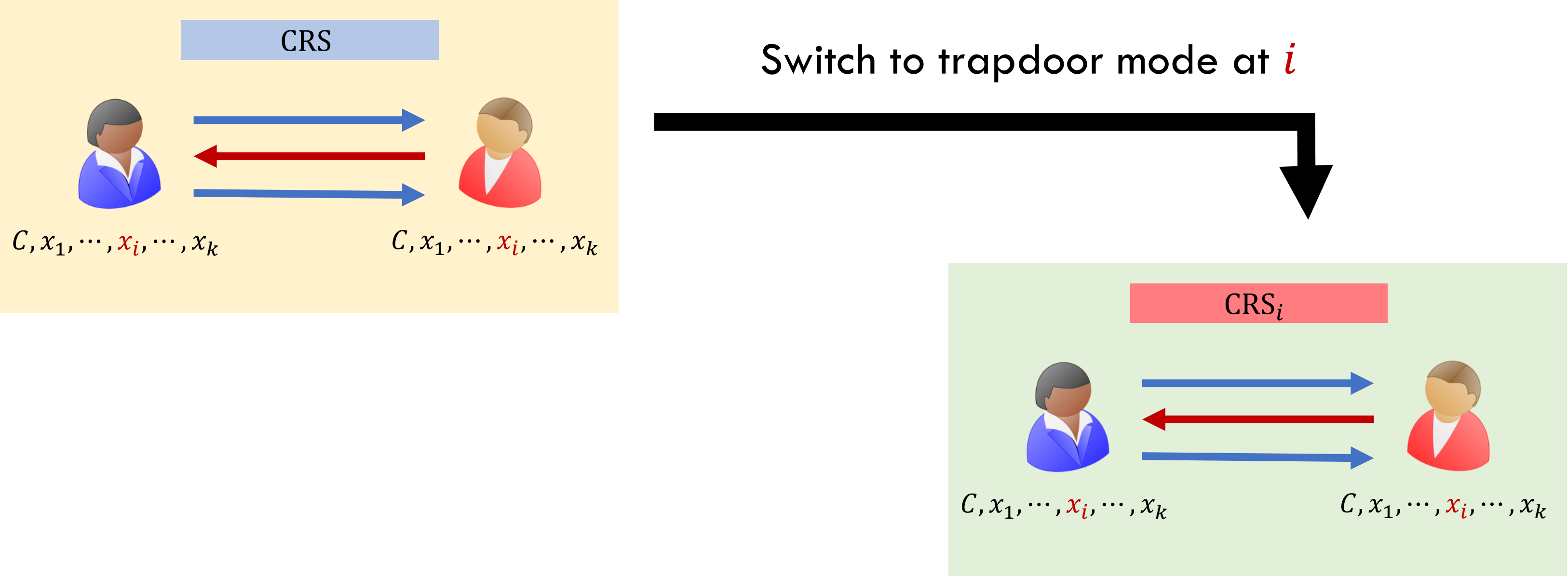


Even unbounded cannot make accept if $(C, x_i) \notin \mathrm{SAT}$

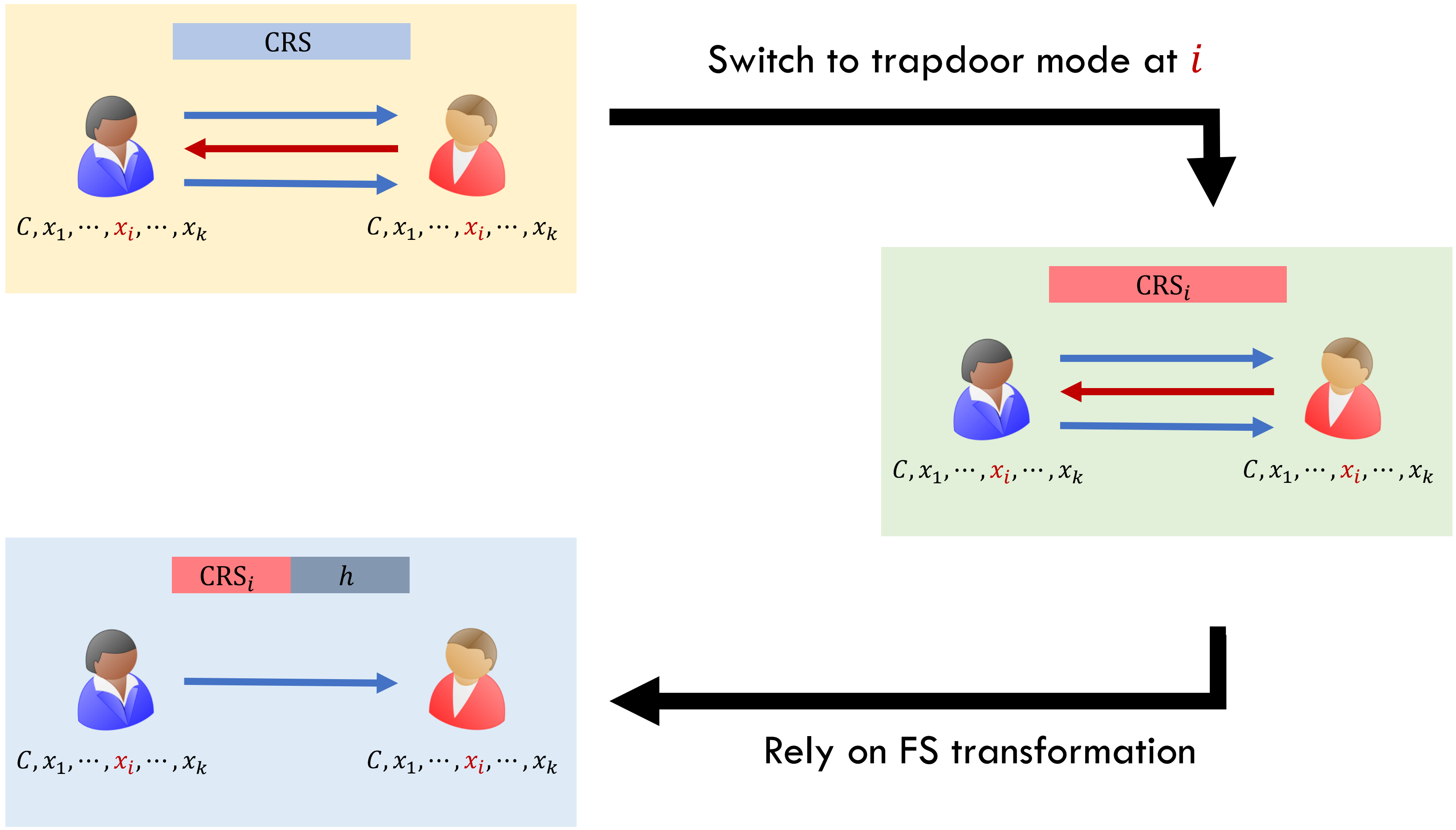
Security Intuition



Security Intuition

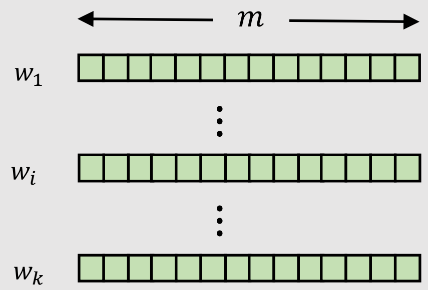


Security Intuition



Dual Mode Batch Argument

Protocol Template

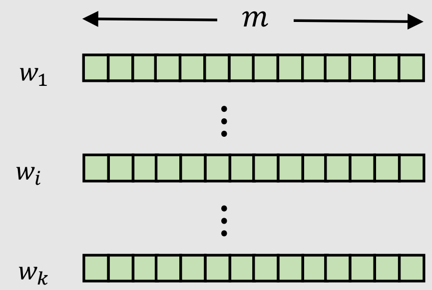


$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Dual Mode Batch Argument

Protocol Template



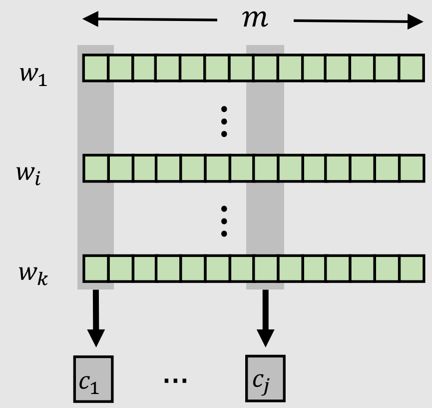
commitment key K

$\text{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \text{SAT}$

Dual Mode Batch Argument

Protocol Template



commitment key K

$\mathrm{SAT} = \{(C, x) \mid \exists w\ s.t.\ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

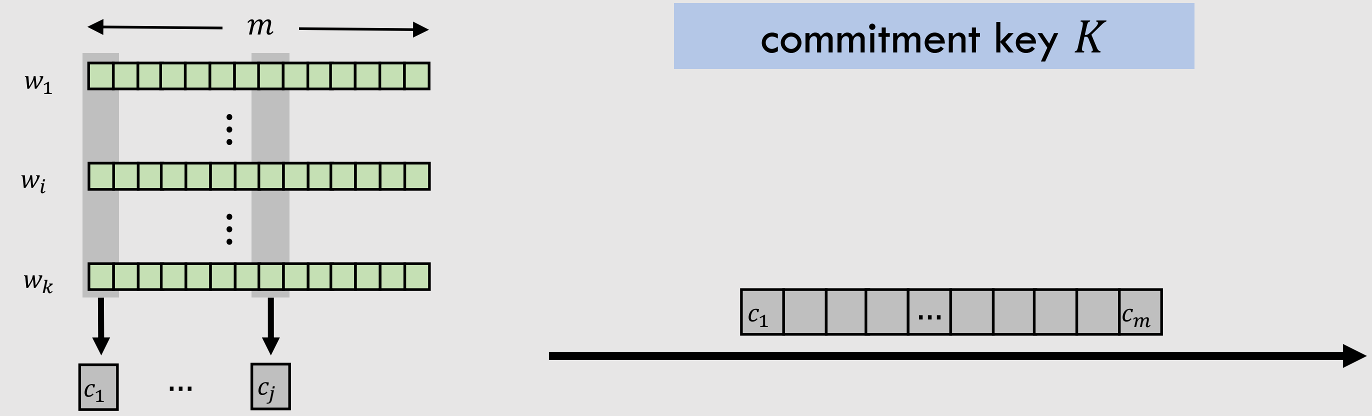
Dual Mode Batch Argument

Protocol Template

SAT $= \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

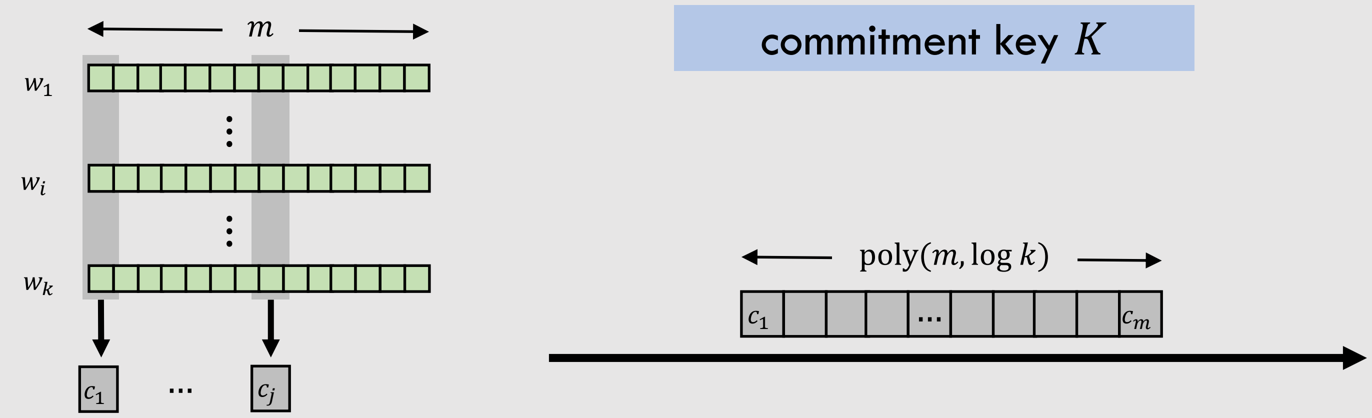
$\forall i \in [k], (C, x_i) \in \text{SAT}$

commitment key K



Dual Mode Batch Argument

Protocol Template

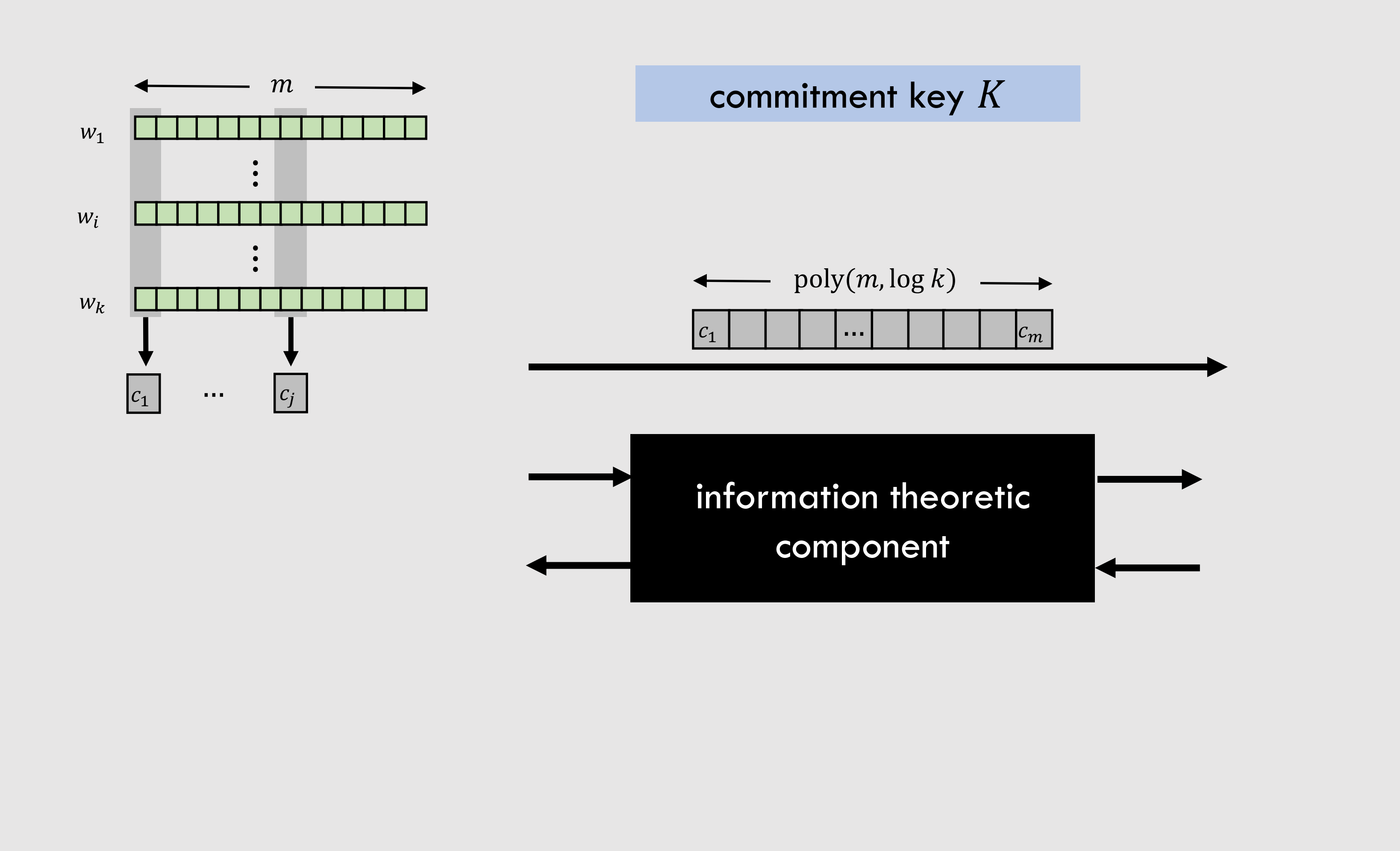


$\mathrm{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Dual Mode Batch Argument

Protocol Template

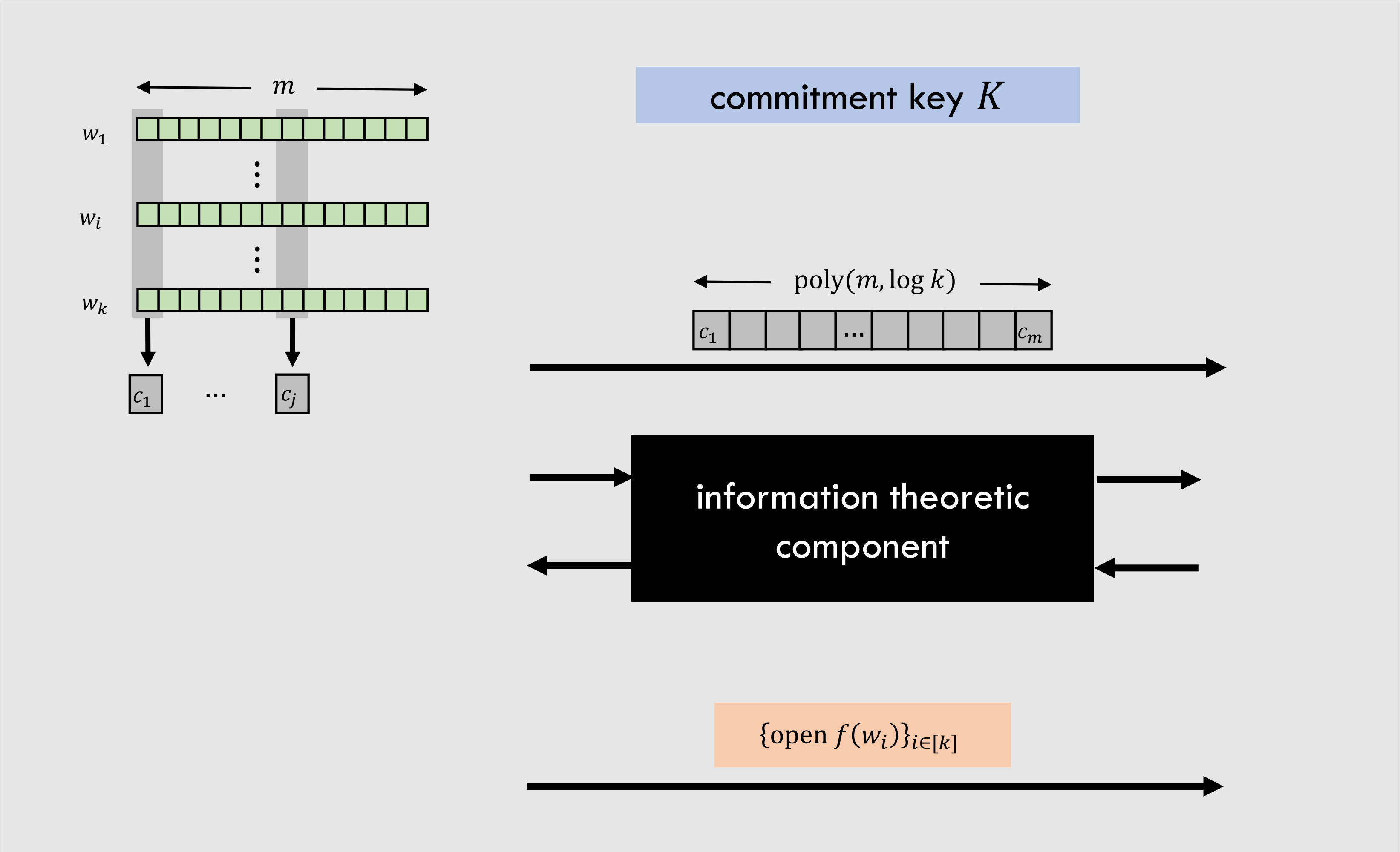


$\text{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \text{SAT}$

Dual Mode Batch Argument

Protocol Template



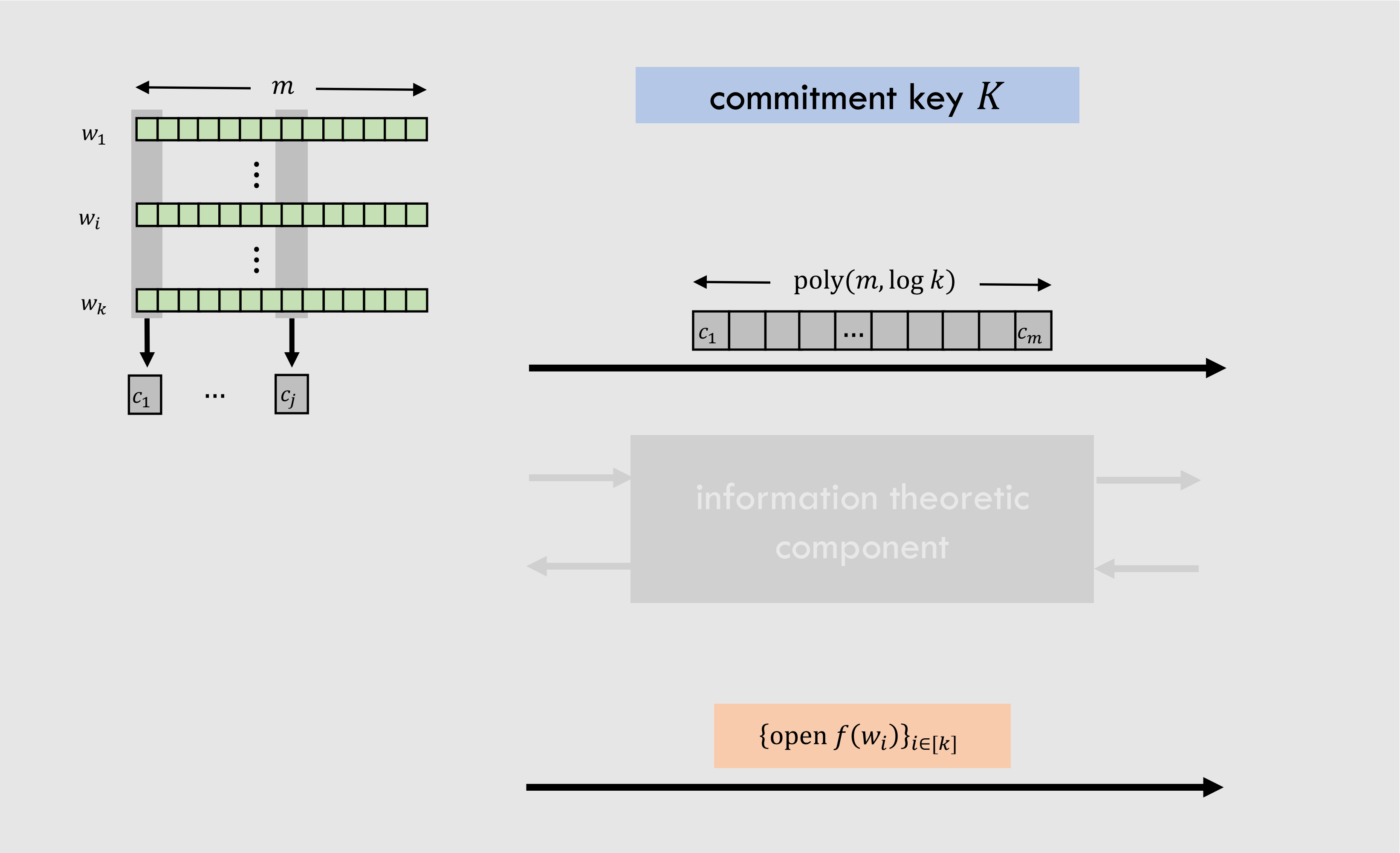
$\mathrm{SAT} = \{(C, x) \mid \exists w\ s.t.\ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

f determined by the information theoretic component.

Dual Mode Batch Argument

Protocol Template

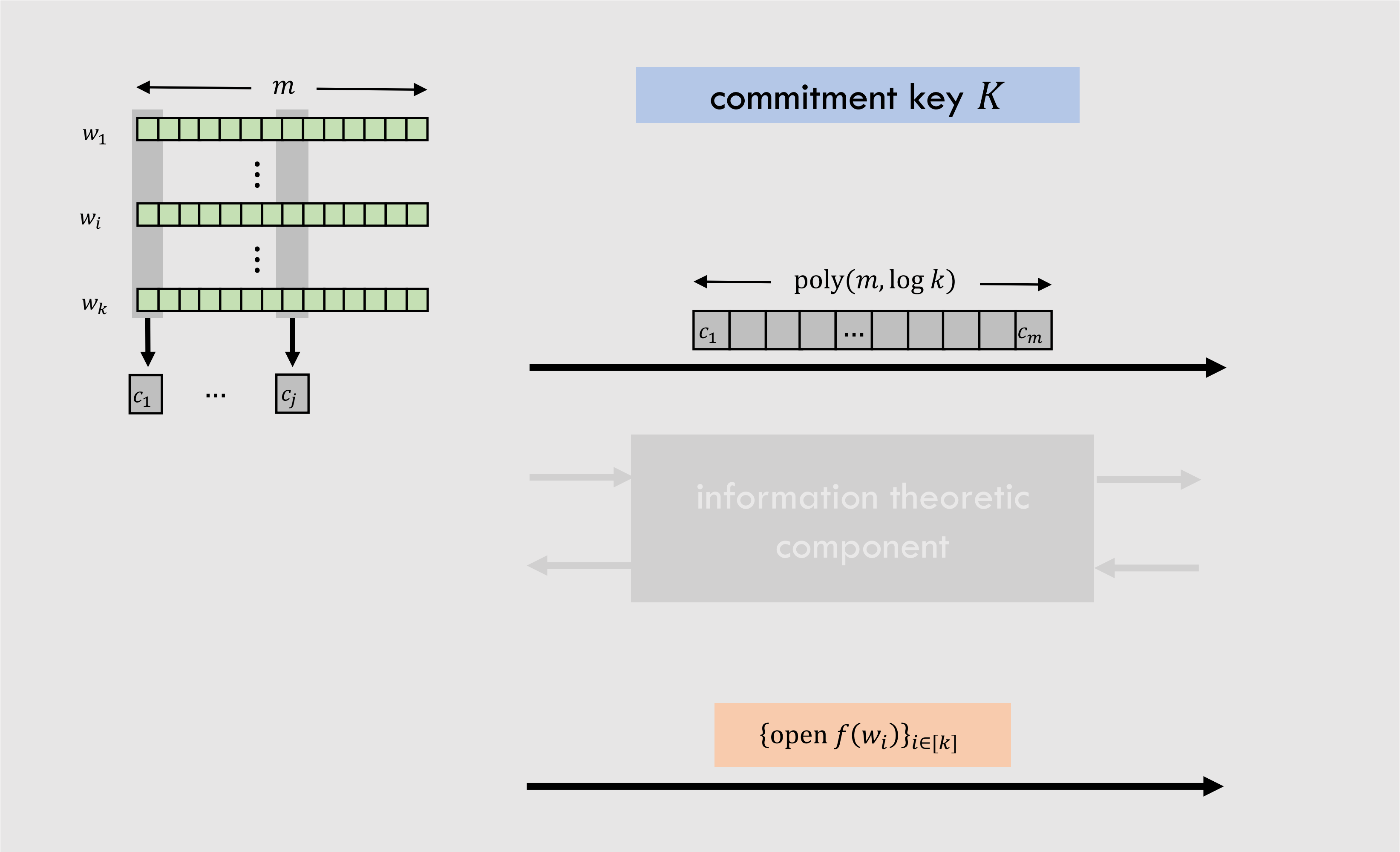


$\mathrm{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Dual Mode Batch Argument

Protocol Template



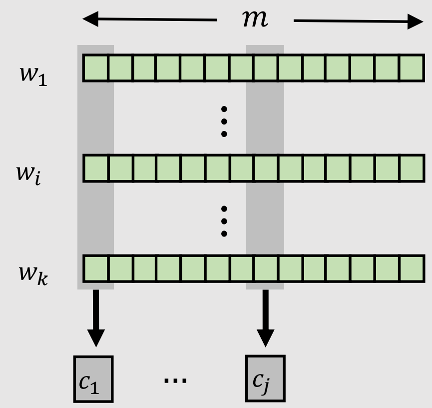
$\mathrm{SAT} = \{(C, x) \mid \exists w\ s.t.\ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Somewhere Statistically Binding (SSB) Commitment Scheme

Dual Mode Batch Argument

Protocol Template



Trapdoor mode

commitment key K_i^*

$\text{poly}(m, \log k)$

c_1 … c_m

information theoretic component

$\{\text{open } f(w_i)\}_{i \in [k]}$

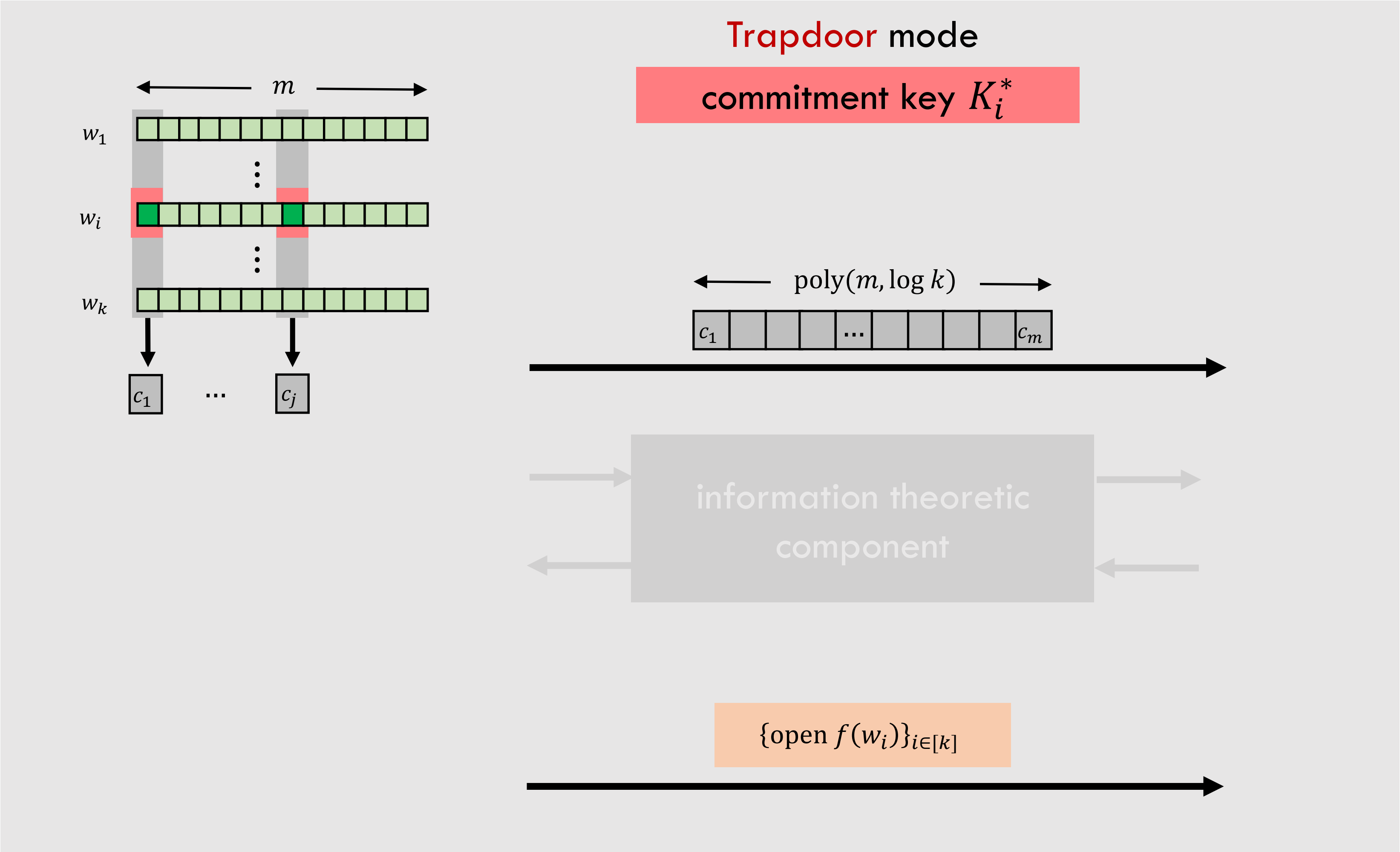
$\text{SAT} = \{(C, x) \mid \exists w \text{ s.t. } C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \text{SAT}$

Somewhere Statistically Binding (SSB) Commitment Scheme

Dual Mode Batch Argument

Protocol Template



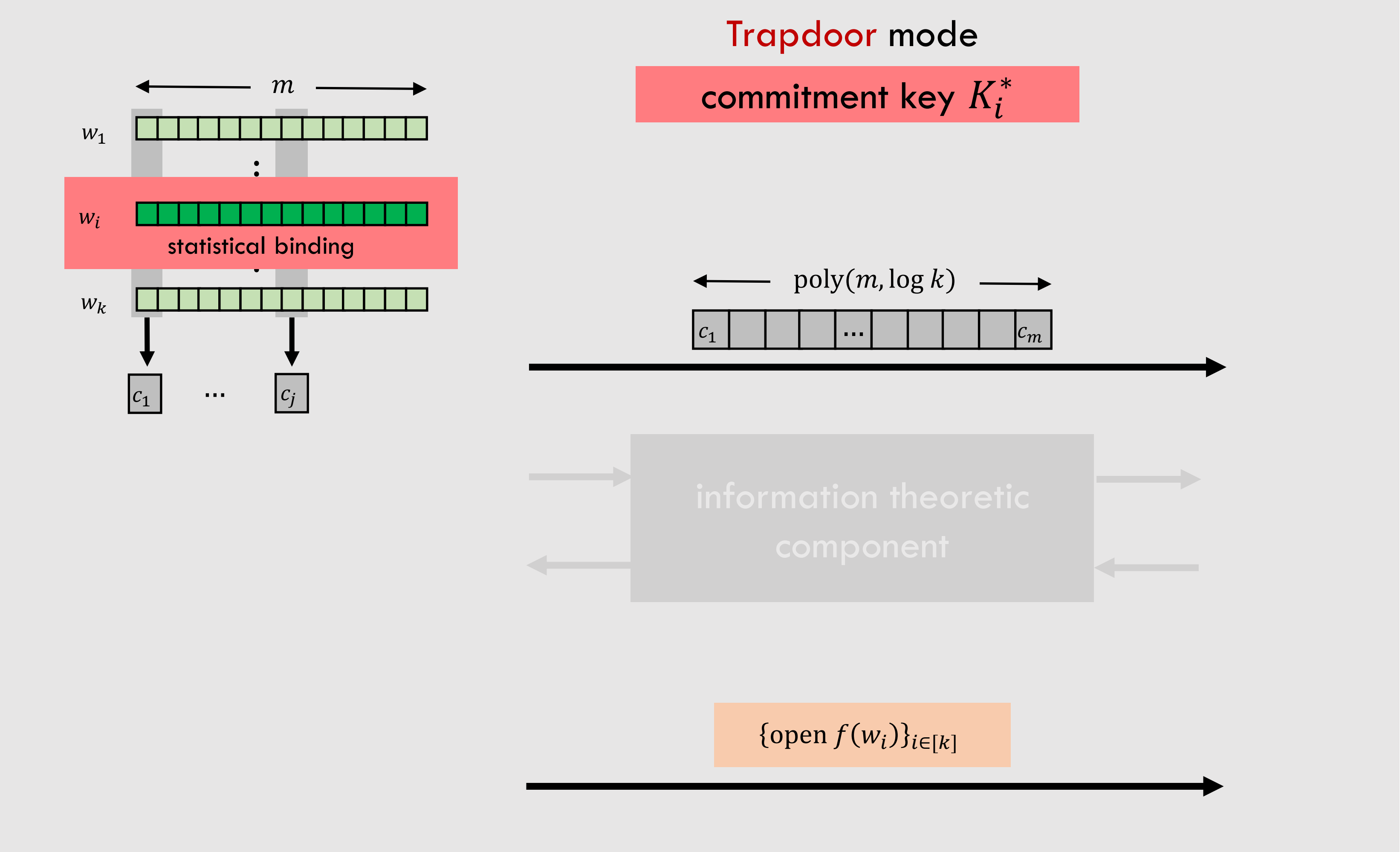
$\mathrm{SAT} = \{(C, x) \mid \exists w \text{ s.t. } C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Somewhere Statistically Binding (SSB) Commitment Scheme

Dual Mode Batch Argument

Protocol Template



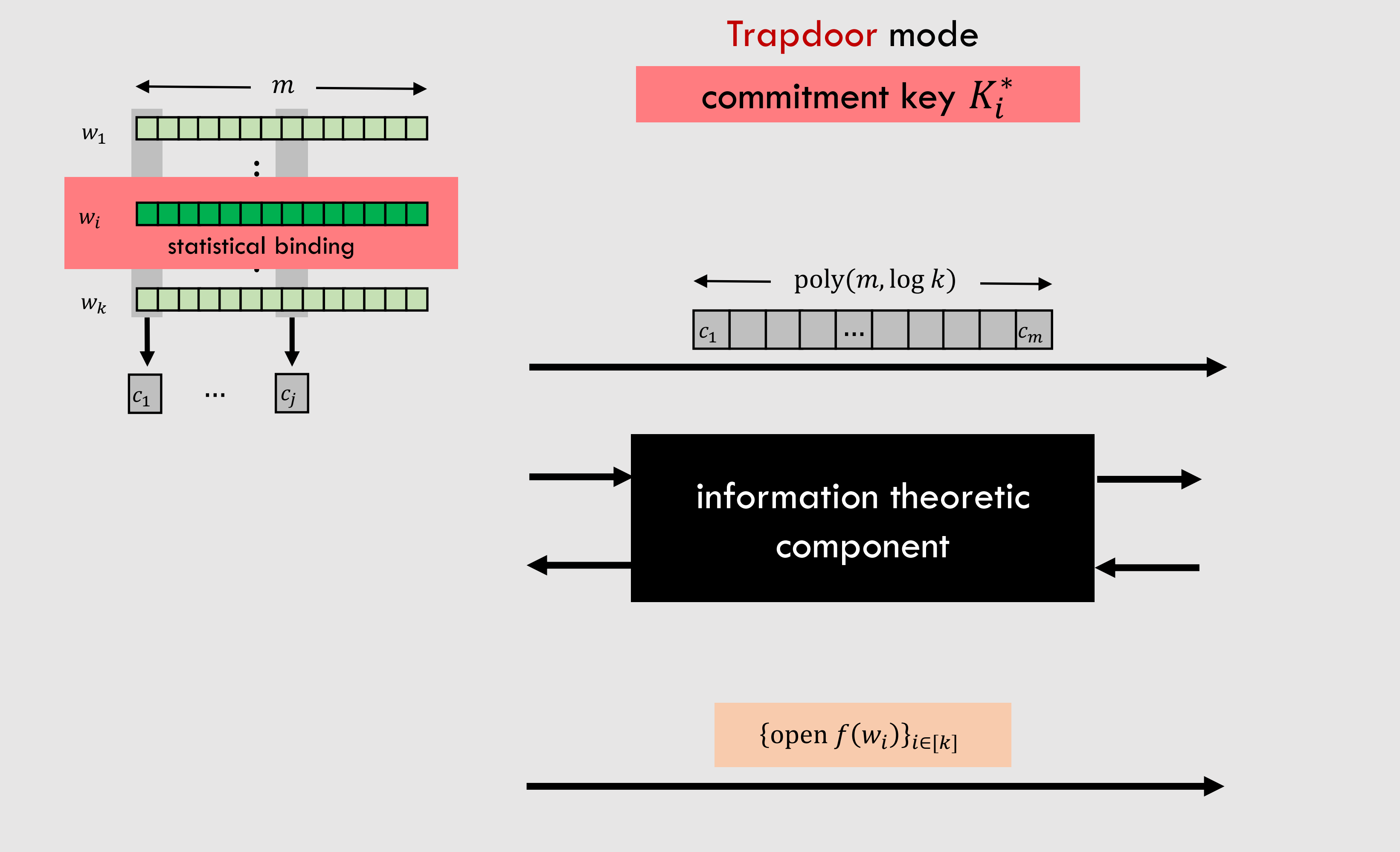
$\text{SAT} = \{(C, x) \mid \exists w \text{ s.t. } C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \text{SAT}$

Somewhere Statistically Binding (SSB) Commitment Scheme

Dual Mode Batch Argument

Protocol Template



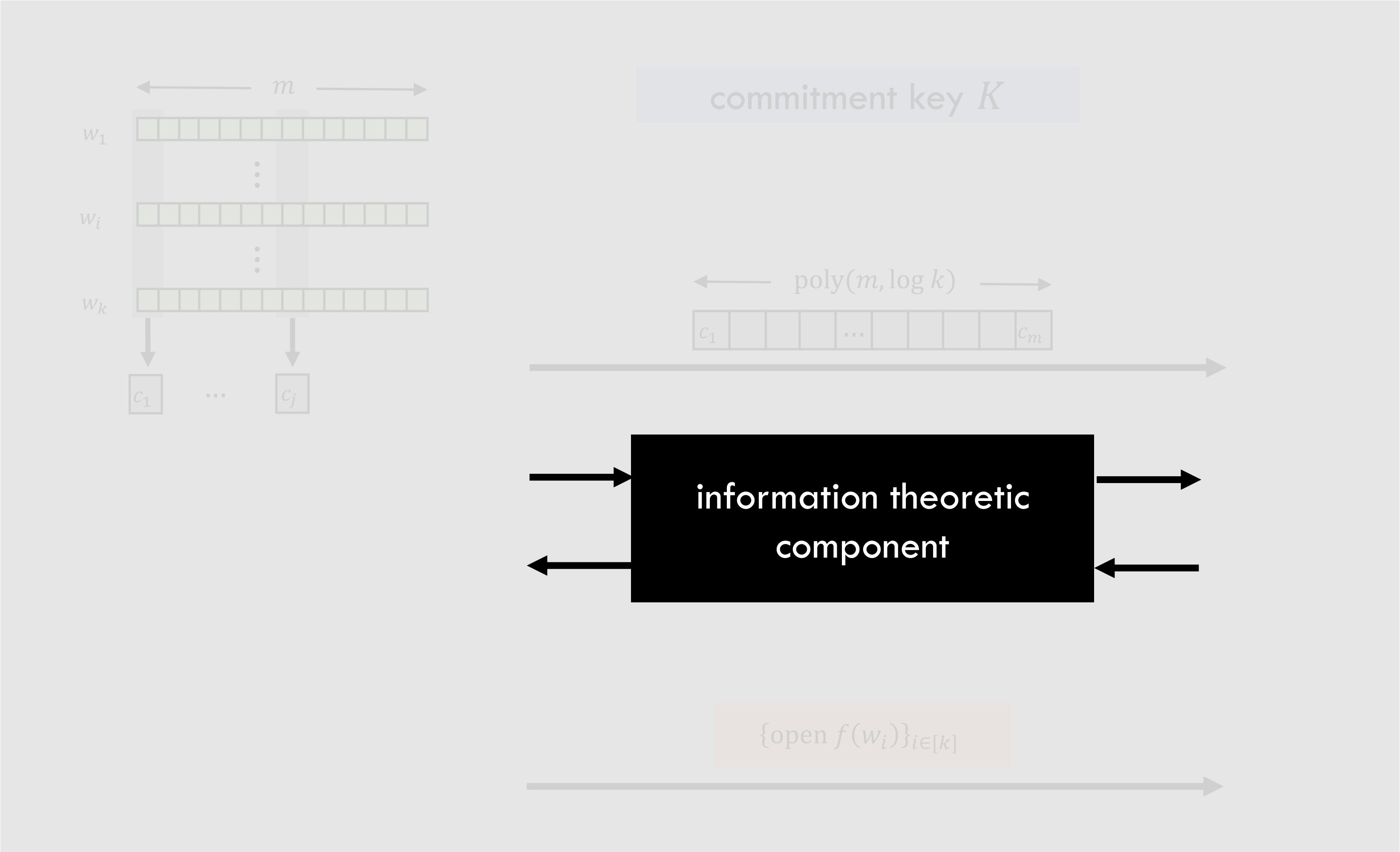
$\mathrm{SAT} = \{(C,x) \mid \exists w \text{ s.t. } C(x,w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

Somewhere Statistically Binding (SSB) Commitment Scheme

Dual Mode Batch Argument

Protocol Template



$\mathrm{SAT} = \{(C, x) \mid \exists w \ s.t.\ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

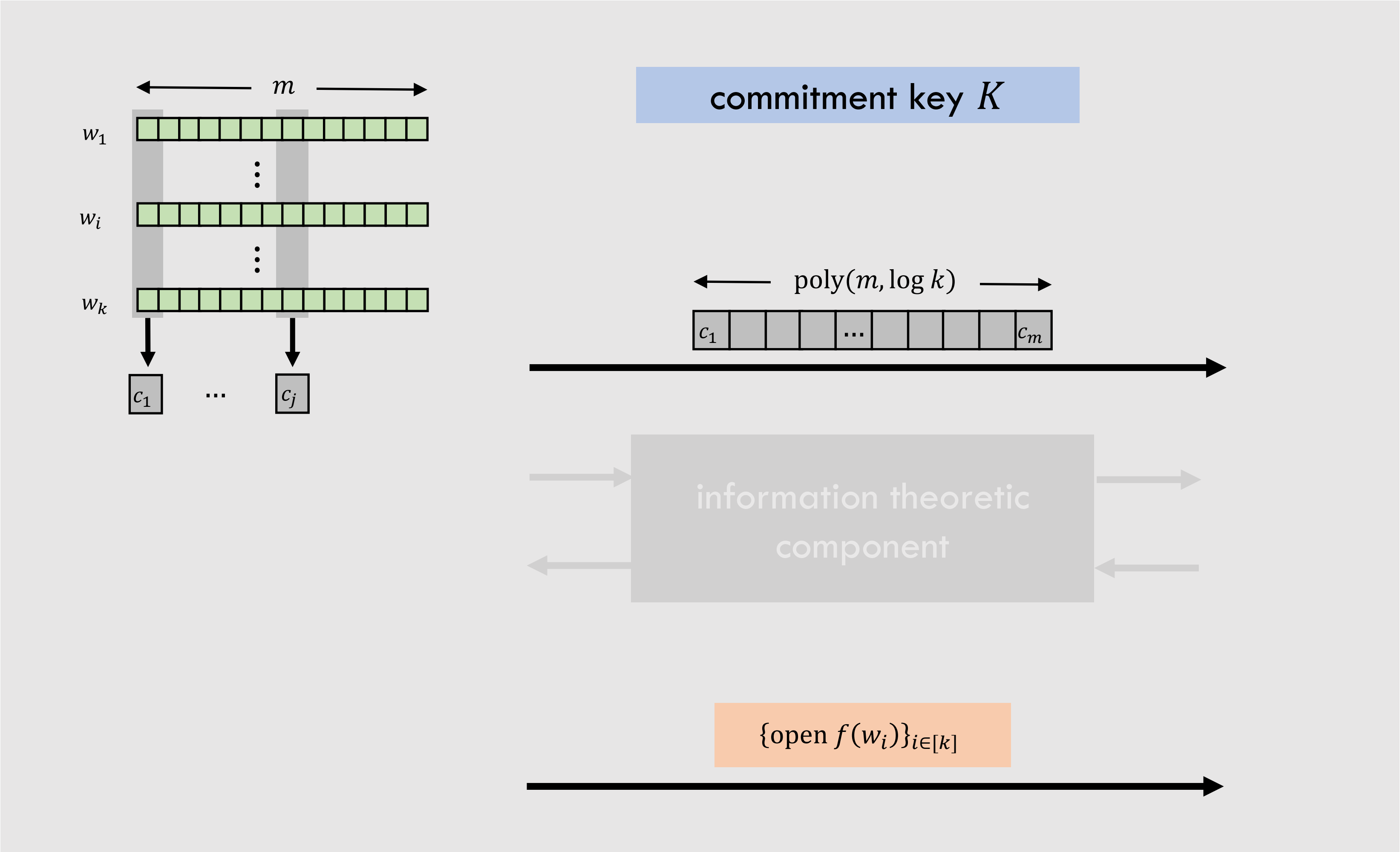
Somewhere Statistically Binding (SSB) Commitment Scheme

Needs to be Fiat-Shamir friendly.

Based on LWE/sub-exp DDH

Dual Mode Batch Argument

Protocol Template



$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

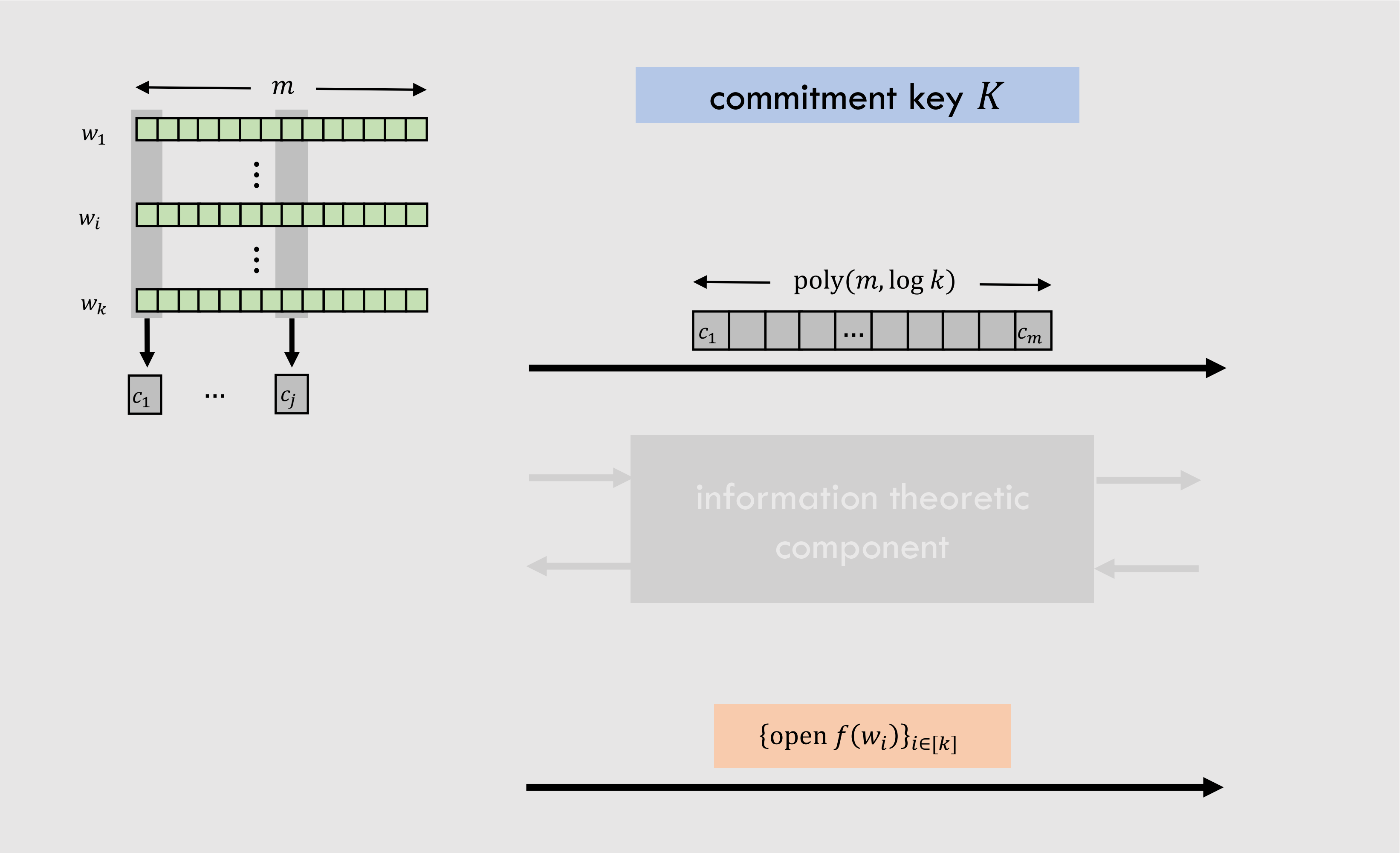
Somewhere Statistically Binding (SSB) Commitment Scheme

Needs to be Fiat-Shamir friendly.

Based on LWE/sub-exp DDH

Dual Mode Batch Argument

Protocol Template



$\text{SAT} = \{(C, x) \mid \exists w \text{ s.t. } C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \text{SAT}$

We construct SSB with appropriate opening to f (with additional properties) based on QR

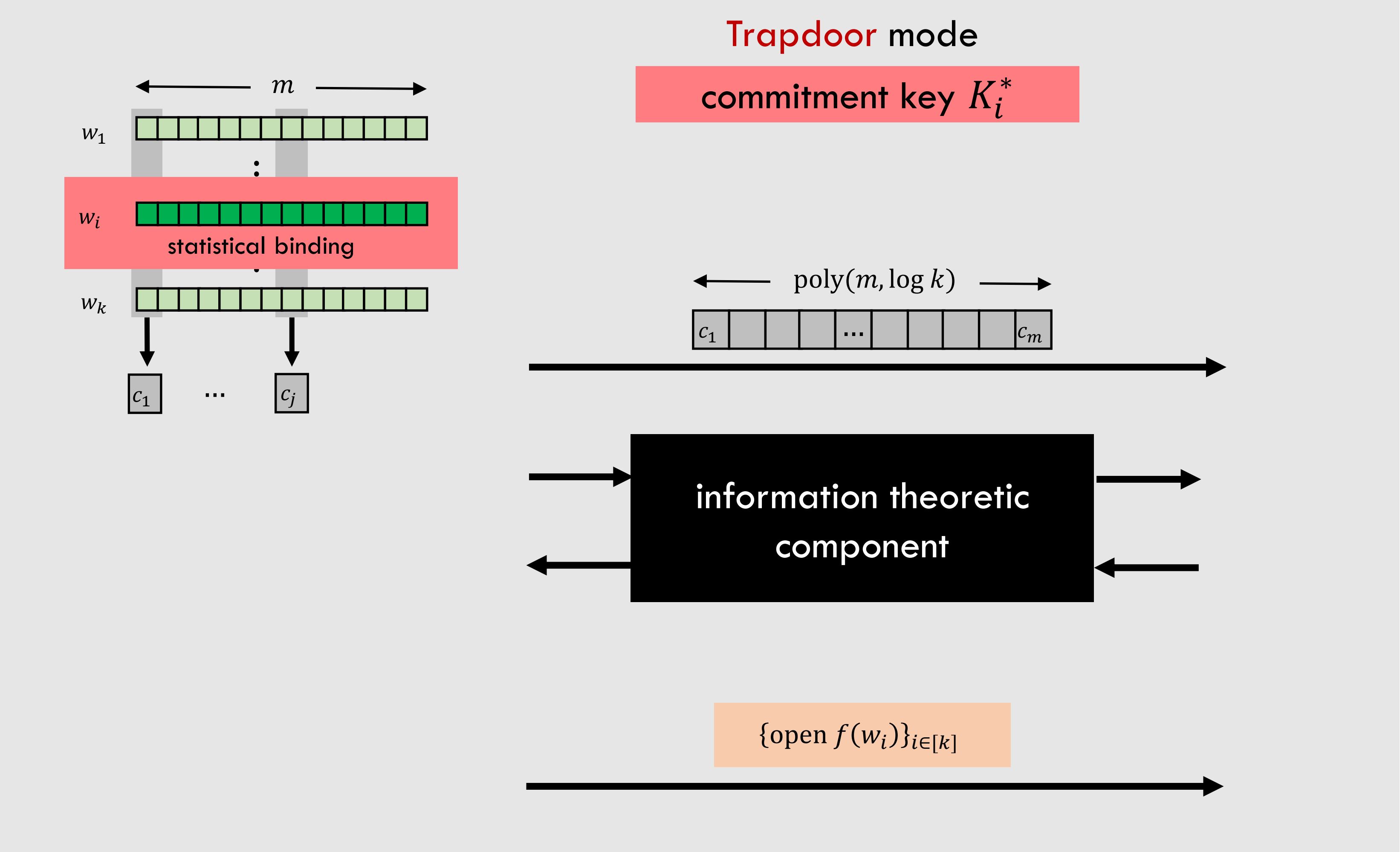
Needs to be Fiat-Shamir friendly.

Based on LWE/sub-exp DDH

(Some) Technical Details

Dual Mode Batch Argument

Protocol Template



$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

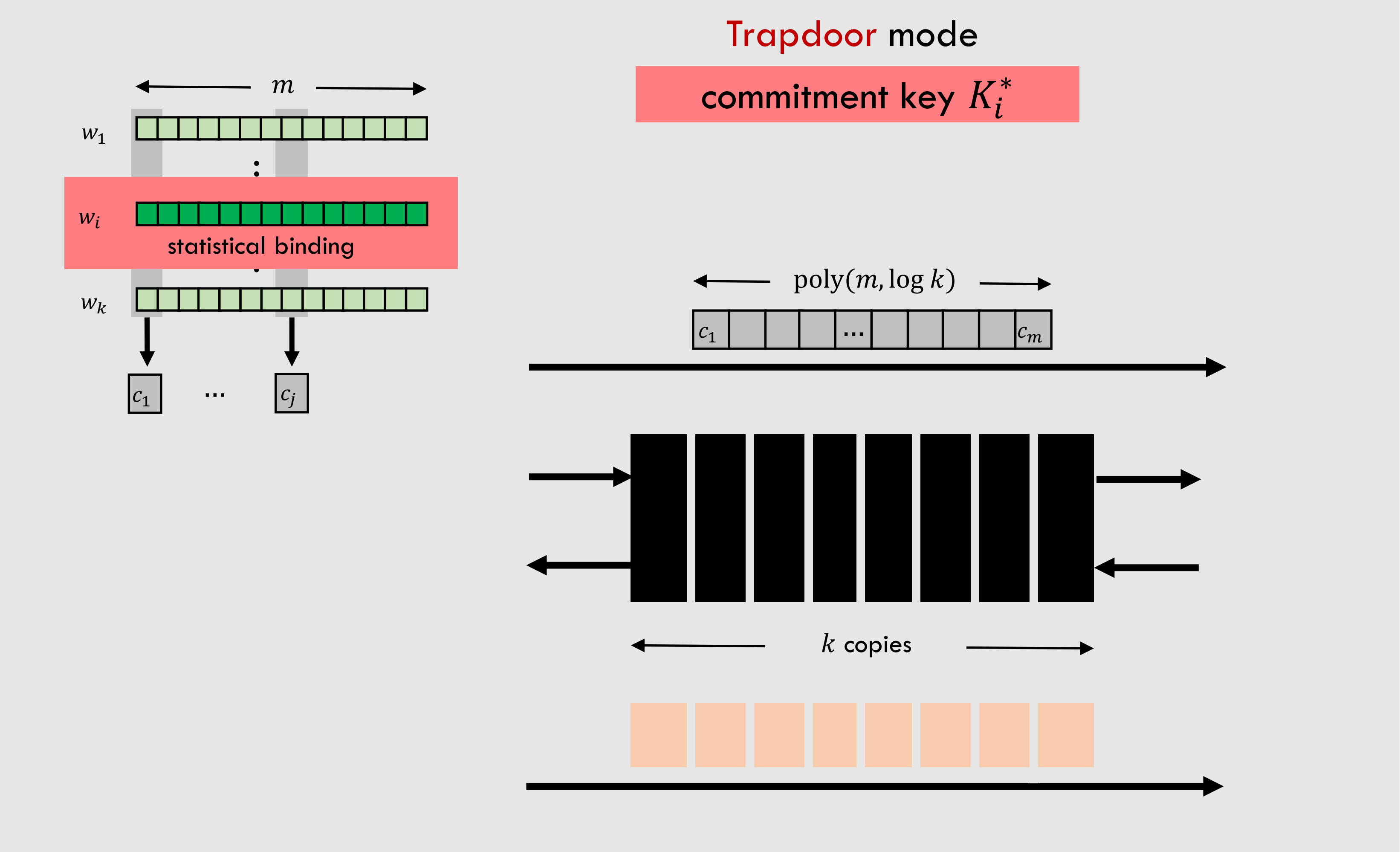
We construct SSB with appropriate opening to f (with additional properties) based on QR

Needs to be Fiat-Shamir friendly.

Based on LWE/sub-exp DDH

Dual Mode Batch Argument

Protocol Template



$\mathrm{SAT} = \{(C, x) \mid \exists w \text{ s.t. } C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

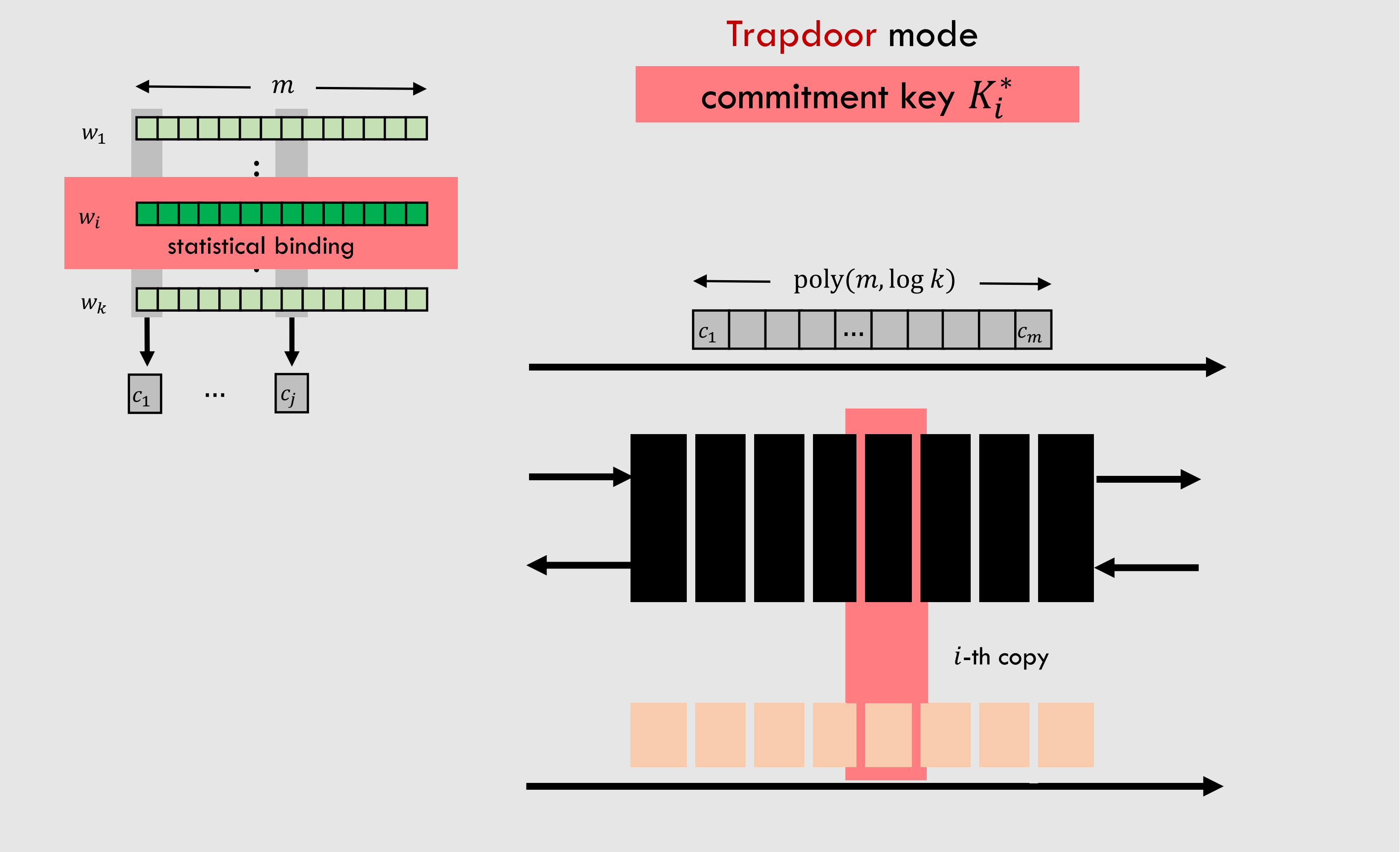
We construct SSB with appropriate opening to f (with additional properties) based on QR

Needs to be Fiat-Shamir friendly.

Based on LWE/sub-exp DDH

Dual Mode Batch Argument

Protocol Template



$\text{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

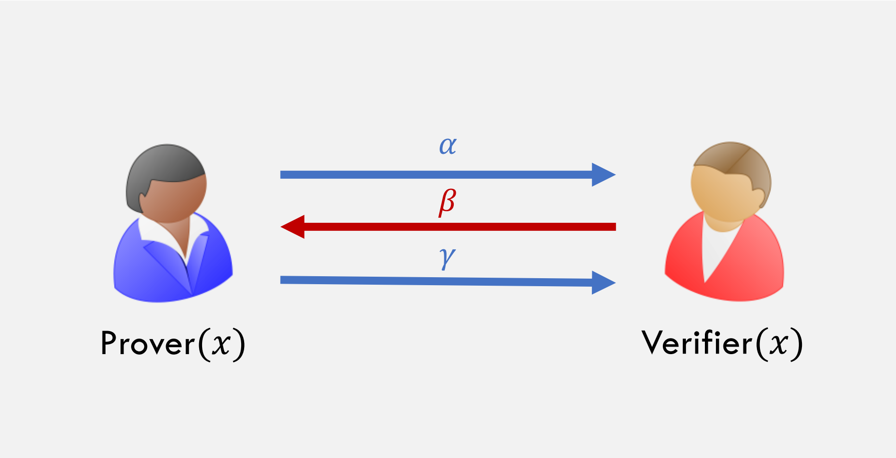
$\forall i \in [k], (C, x_i) \in \text{SAT}$

We construct SSB with appropriate opening to f (with additional properties) based on QR

Needs to be Fiat-Shamir friendly.

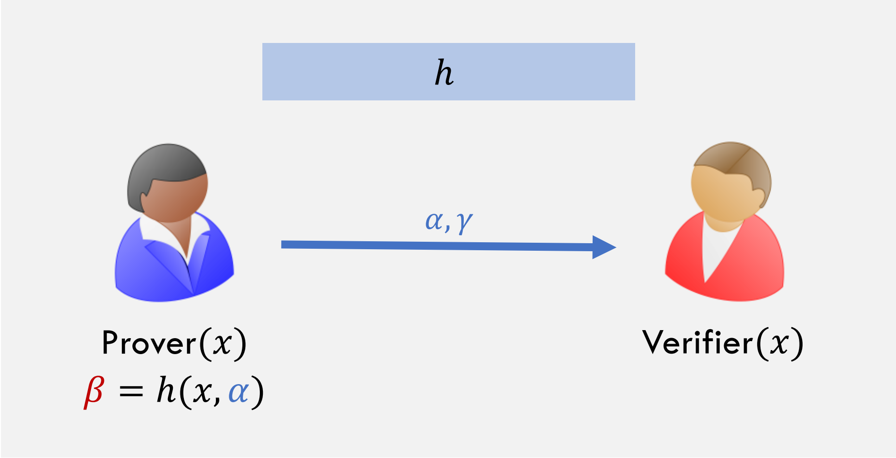
Based on LWE/sub-exp DDH

Fiat-Shamir (FS) Methodology

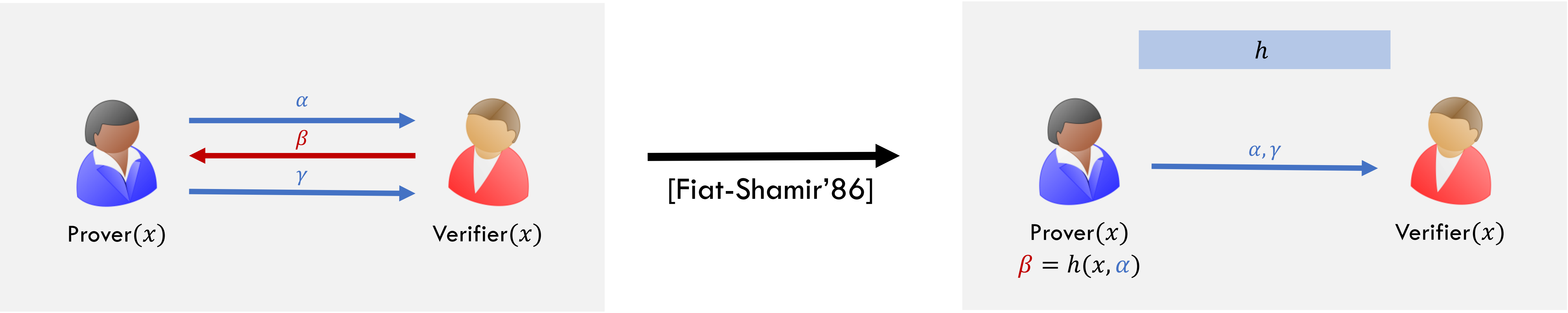


β is a random string

[Fiat-Shamir'86]



Fiat-Shamir (FS) Methodology

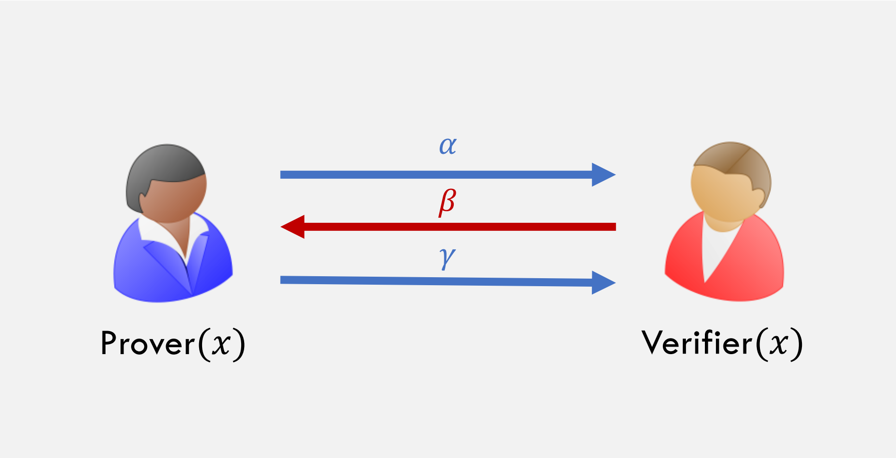


β is a random string

$\forall\, x \notin \mathcal{L}$

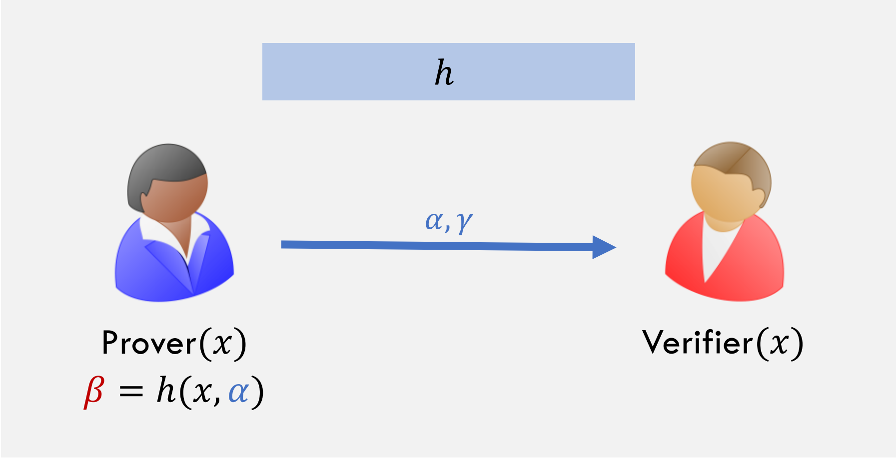
$\mathrm{BAD}_{x,\alpha} = \{\beta \mid \exists \gamma$ s.t. Verifier accepts $(\alpha, \beta, \gamma)\}$

Fiat-Shamir (FS) Methodology



β is a random string

[Fiat-Shamir'86]



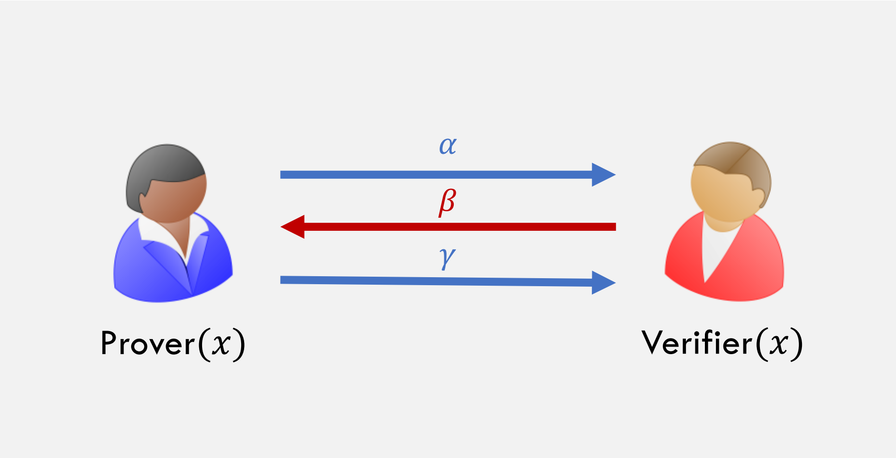
$\forall\, x \notin \mathcal{L}$

$\mathrm{BAD}_{x,\alpha} = \{\beta \mid \exists \gamma$ s.t. Verifier accepts $(\alpha, \beta, \gamma)\}$

If $x \notin \mathcal{L}$, no PPT  can find α such that

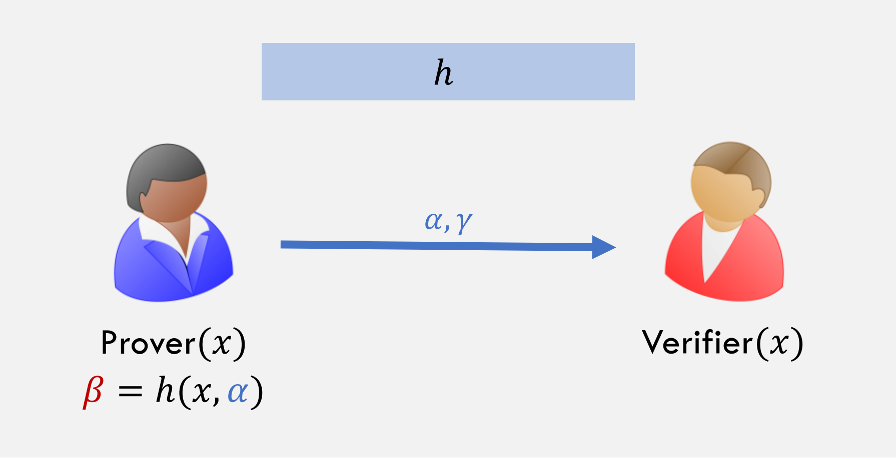
$$h(x, \alpha) \in \mathrm{BAD}_{x,\alpha}$$

Fiat-Shamir (FS) Methodology



β is a random string

[Fiat-Shamir'86]



$\forall\, x \notin \mathcal{L}$

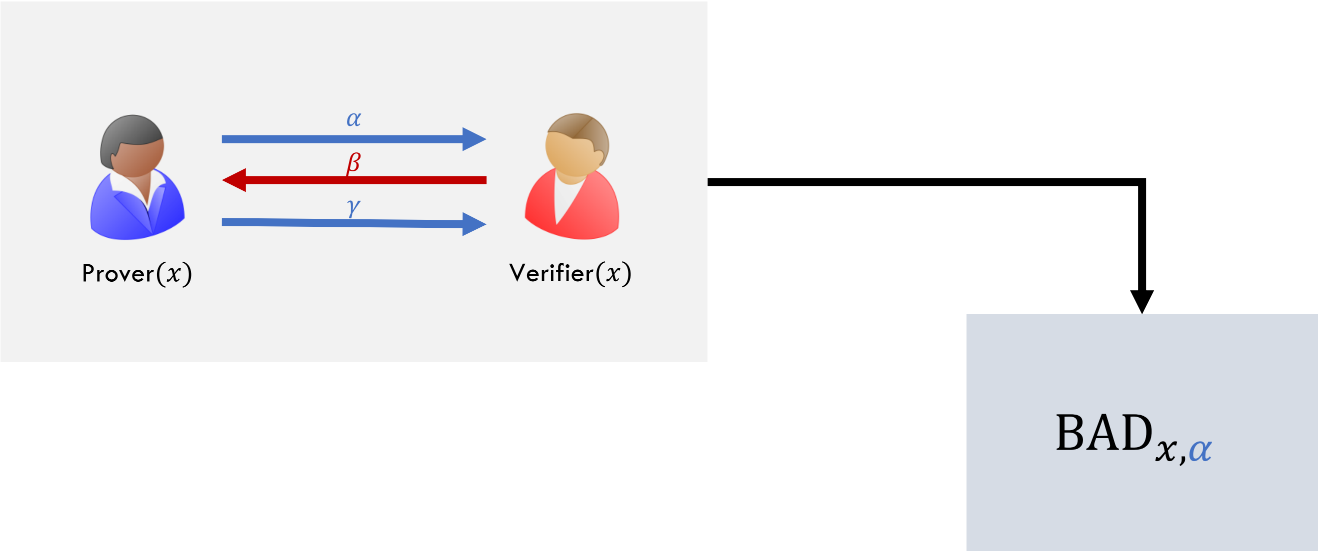
$$\mathrm{BAD}_{x,\alpha} = \{\beta \mid \exists \gamma \text{ s.t. Verifier accepts } (\alpha, \beta, \gamma)\}$$

If $x \notin \mathcal{L}$, no PPT  can find α such that

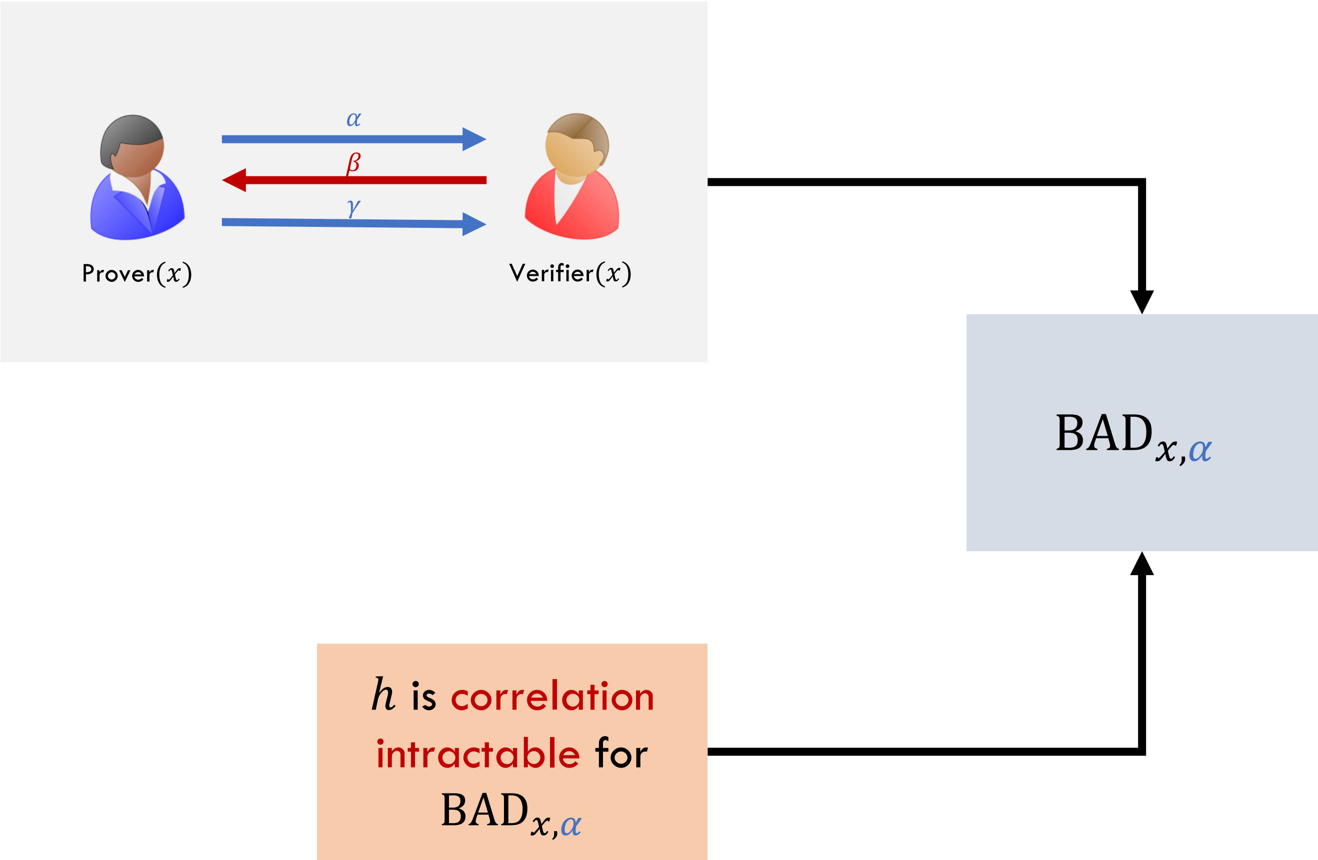
$$h(x, \alpha) \in \mathrm{BAD}_{x,\alpha}$$

h is correlation intractable (CI) for $\mathrm{BAD}_{x,\alpha}$

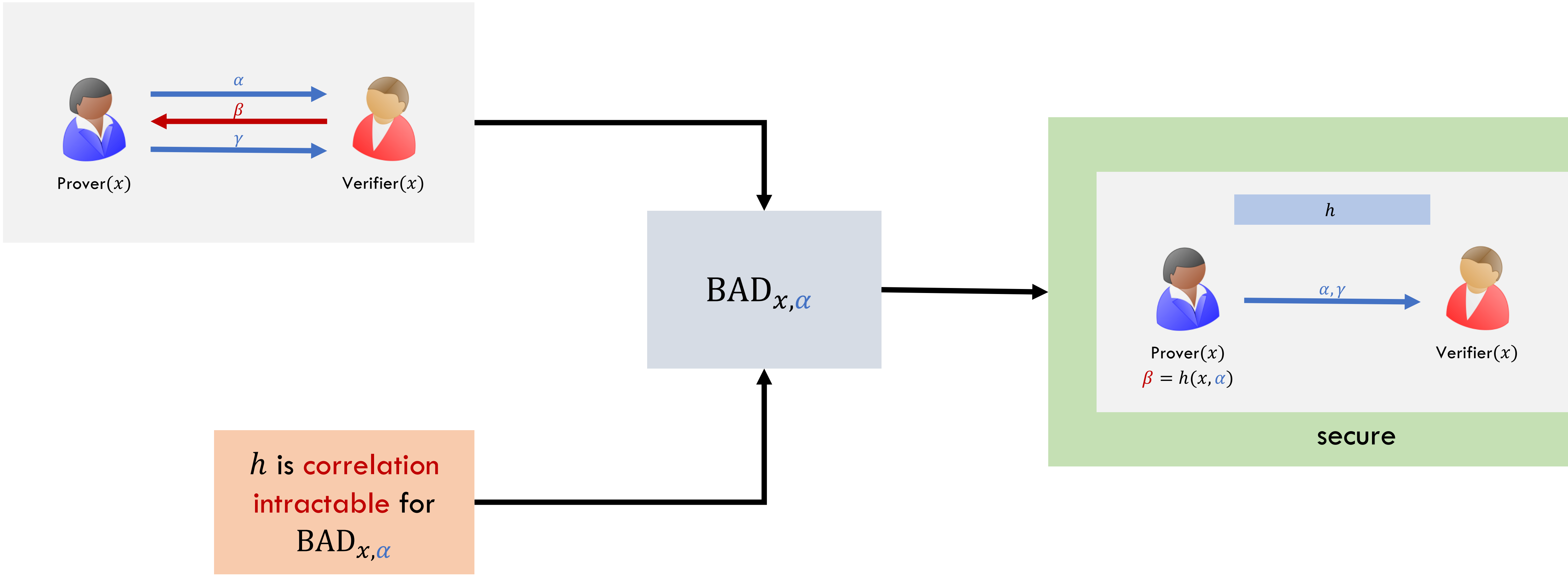
Instantiating the FS Transform



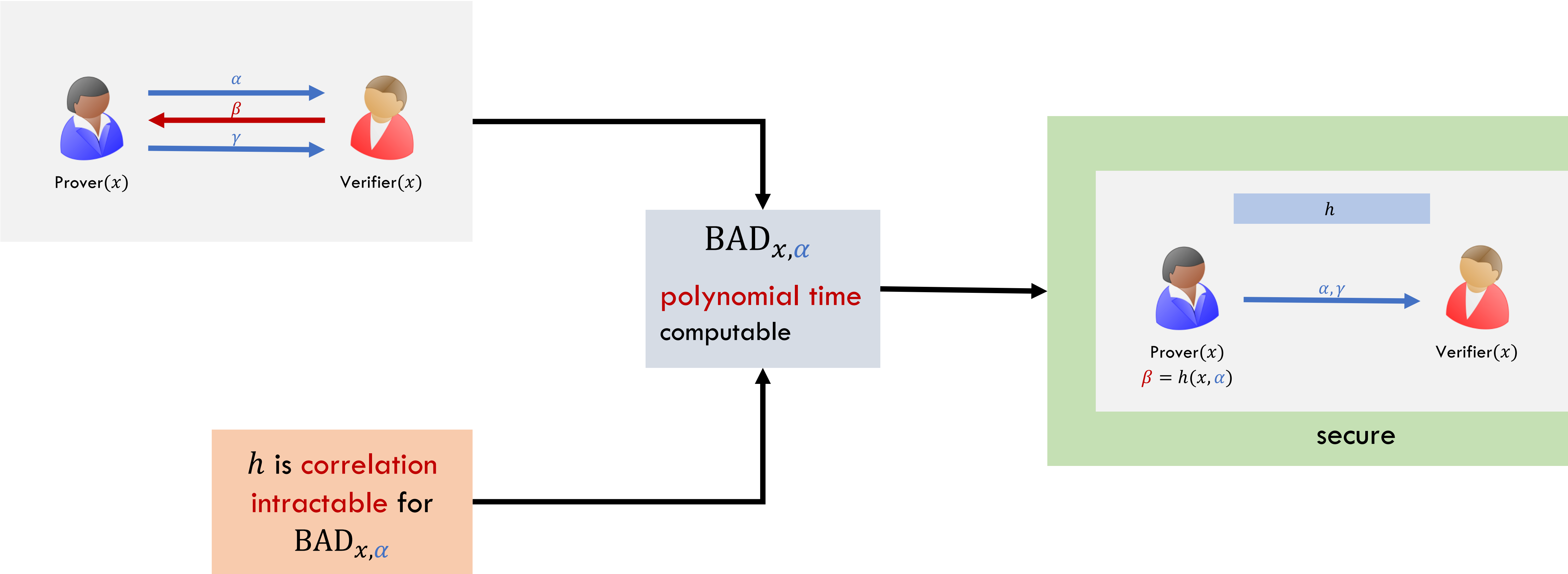
Instantiating the FS Transform



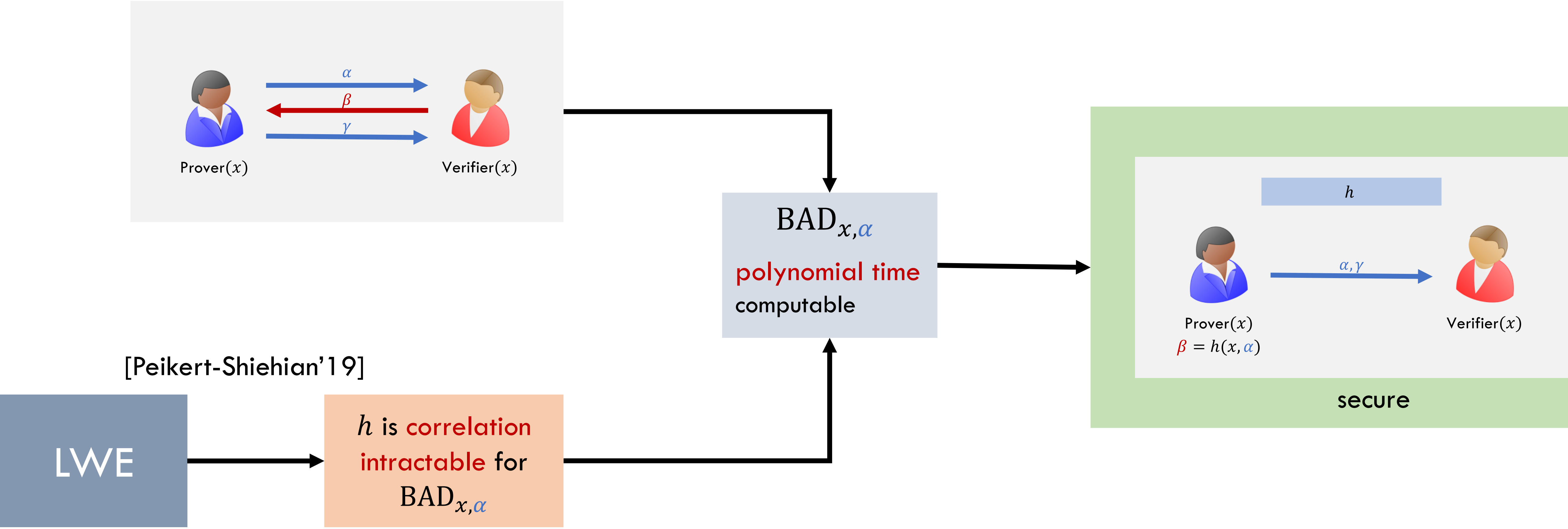
Instantiating the FS Transform



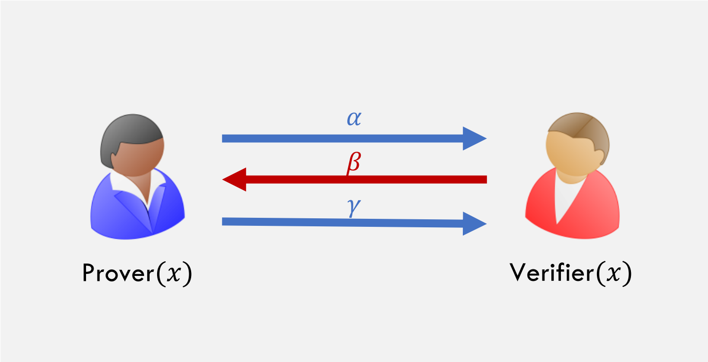
Instantiating the FS Transform



Instantiating the FS Transform



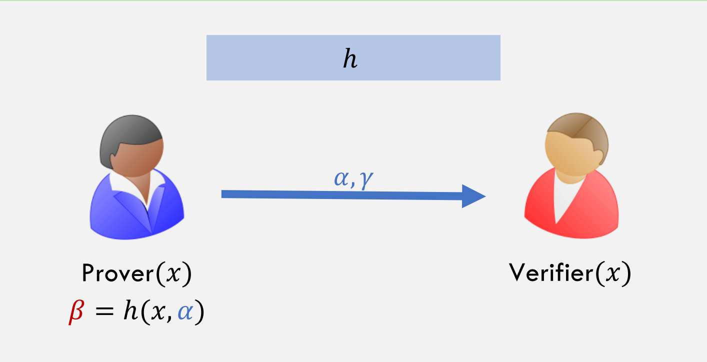
Instantiating the FS Transform



$\mathrm{BAD}_{x,\alpha}$

computable in TC^0

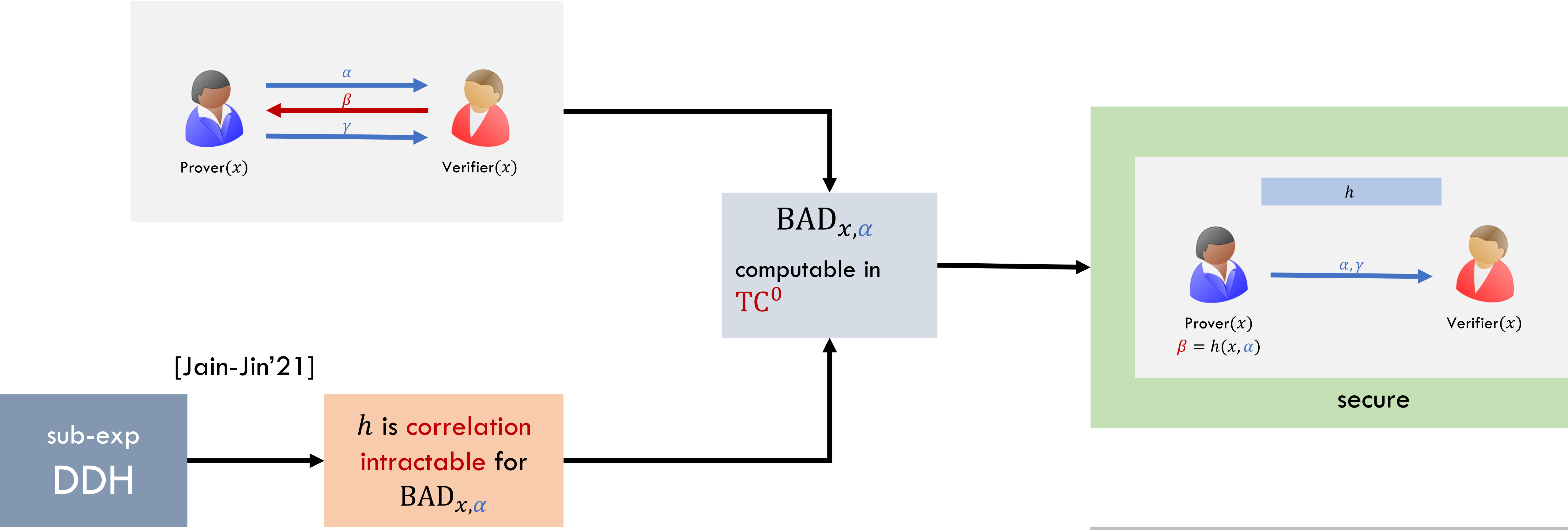
h is correlation intractable for $\mathrm{BAD}_{x,\alpha}$



secure

TC^0 - Constant depth polynomial-size threshold circuits

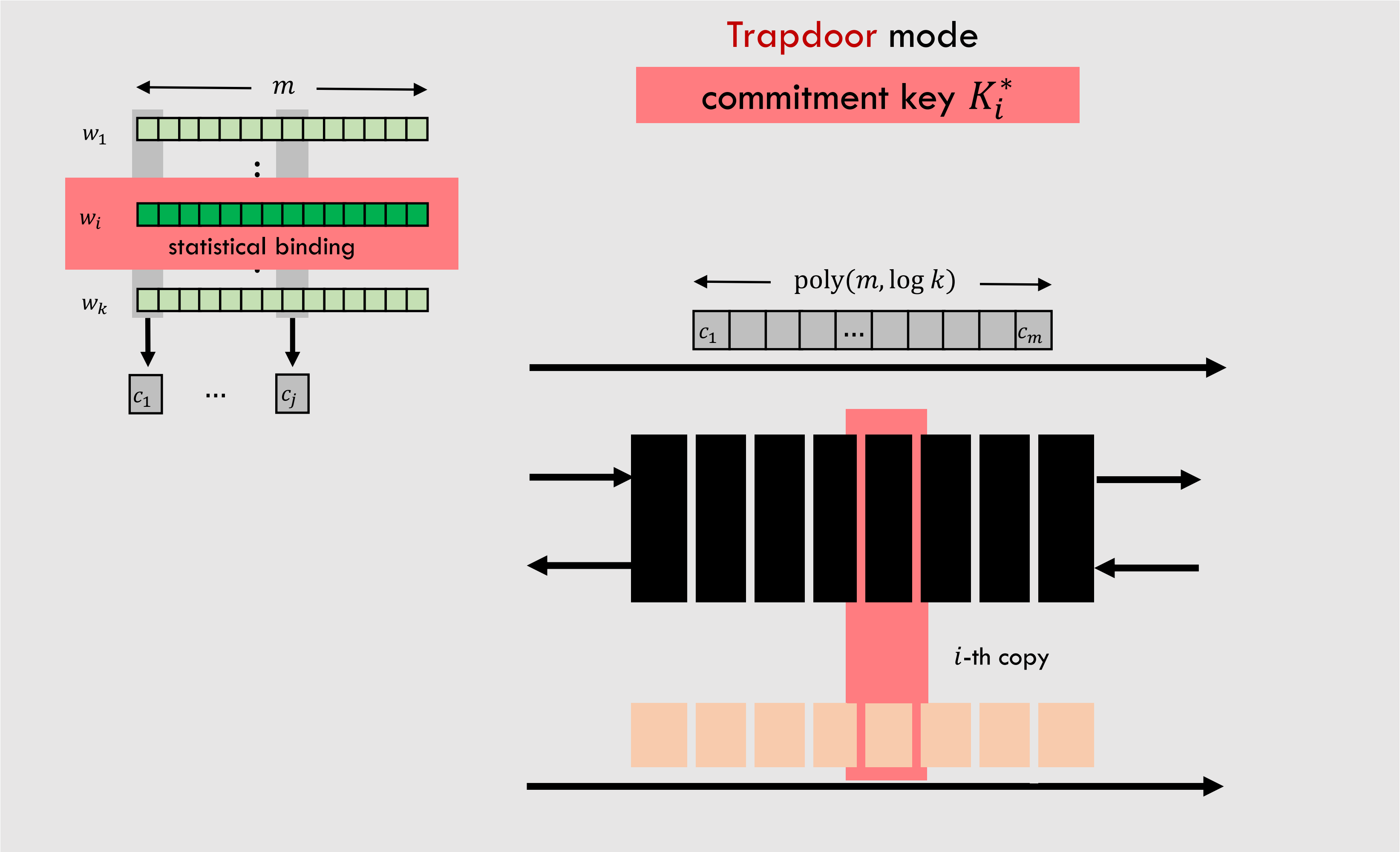
Instantiating the FS Transform



TC^0 - Constant depth polynomial-size threshold circuits

Dual Mode Batch Argument

Protocol Template



$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

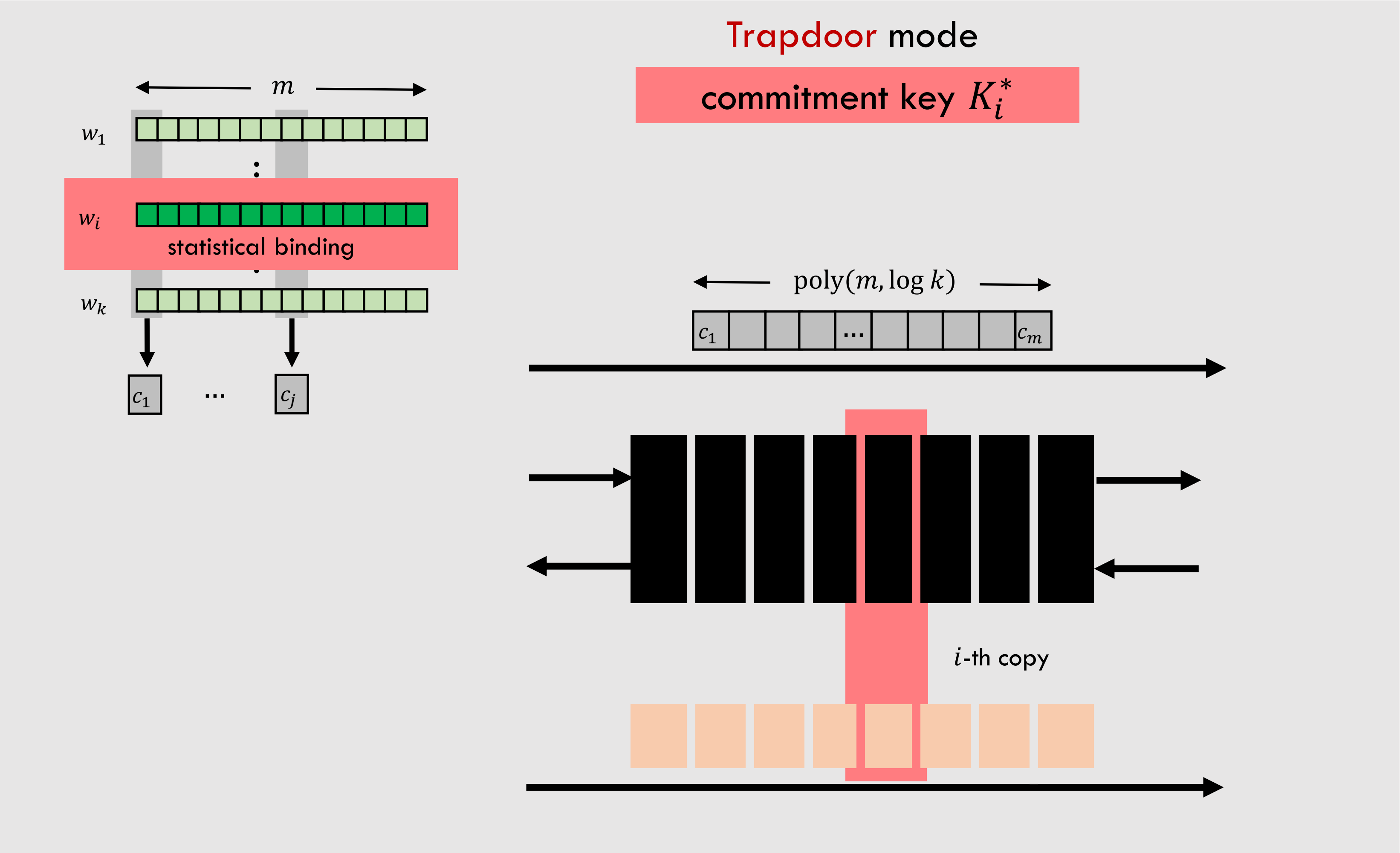
We construct SSB with appropriate opening to f (with additional properties) based on QR

Needs to be Fiat-Shamir friendly.

Based on LWE/sub-exp DDH

Dual Mode Batch Argument

Protocol Template



$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

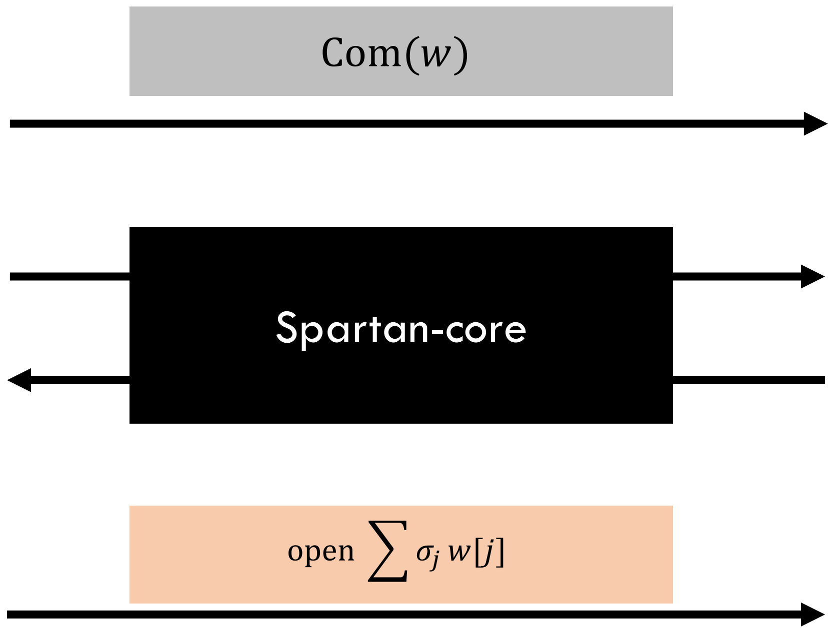
We construct SSB with appropriate opening to f (with additional properties) based on QR

BAD needs to be computable in TC^0.

Based on LWE/sub-exp DDH

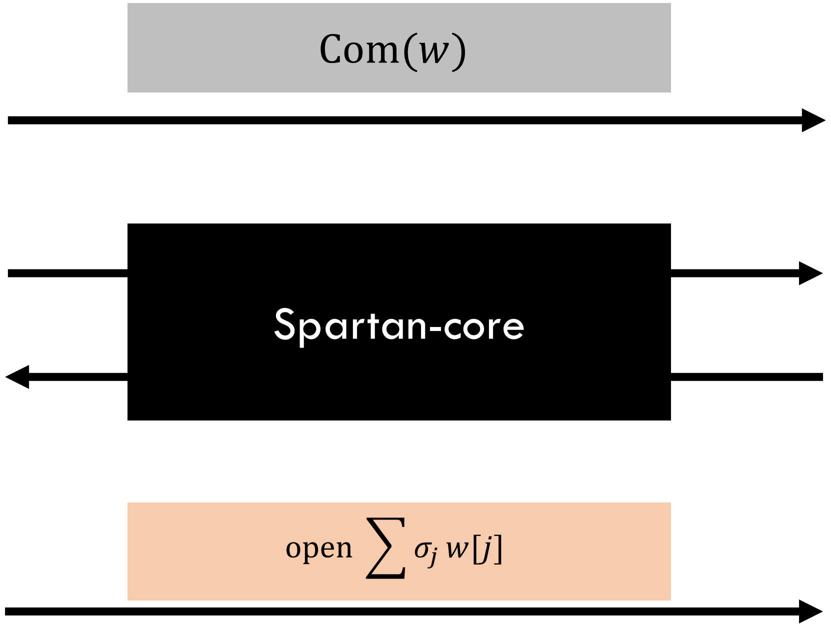
Building Block: Spartan [Setty'20]

$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$



Building Block: Spartan [Setty'20]

SAT $= \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$



Spartan-core primarily consists of the Sumcheck protocol.

Building Block: Spartan [Setty'20]

$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\mathrm{Com}(w)$

$\vdots$

polynomial $g(x)$

$\beta \leftarrow \mathbb{F}$

$\vdots$

open $\sum \sigma_j \, w[j]$

Building Block: Spartan [Setty'20]

$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\mathrm{Com}(w)$

$\vdots$

polynomial $g(x)$

$\beta \leftarrow \mathbb{F}$

$\vdots$

open $\sum \sigma_j \, w[j]$

$\mathrm{BAD} = \{\beta \in \mathbb{F} \mid \beta$ is a root of $g(x) - g_w^*(x)\}$

Building Block: Spartan [Setty'20]

$\text{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\text{Com}(w)$

$\vdots$

polynomial $g(x)$

$\beta \leftarrow \mathbb{F}$

$\vdots$

$\text{open} \sum \sigma_j \, w[j]$

$\text{BAD} = \{\beta \in \mathbb{F} \mid \beta$ is a root of $g(x) - g_w^*(x)\}$

the "true" polynomial an honest prover would have sent

Building Block: Spartan [Setty'20]

$\mathrm{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

$\mathrm{Com}(w)$

⋮

polynomial $g(x)$

$\beta \leftarrow \mathbb{F}$

⋮

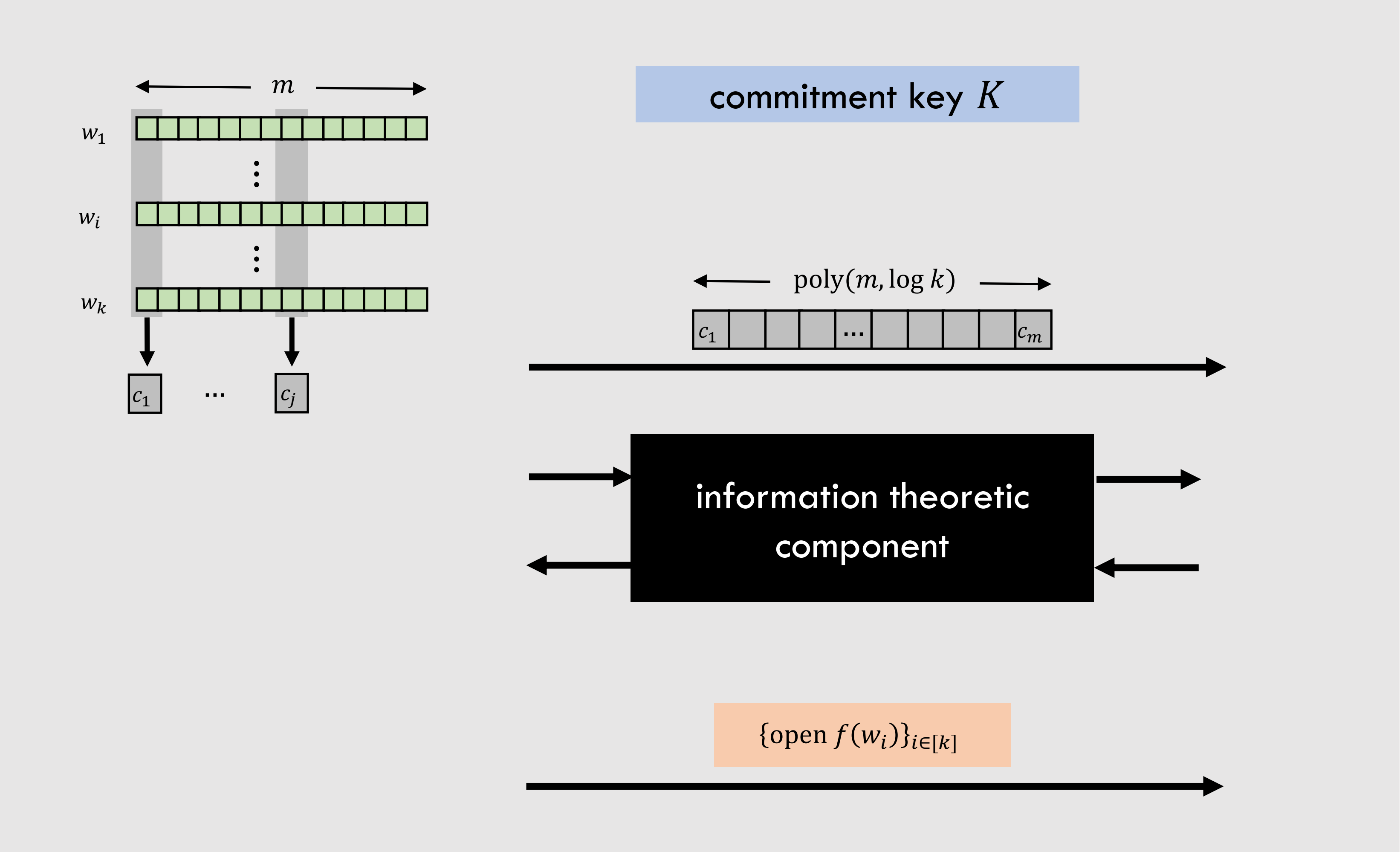
$\mathrm{open} \sum \sigma_j \, w[j]$

$\mathrm{BAD} = \{\beta \in \mathbb{F} \mid \beta$ is a root of $g(x) - g_w^*(x)\}$

Show that appropriate field $\mathbb{F}$, BAD can be computed in TC^0.

Dual Mode Batch Argument

Protocol Template



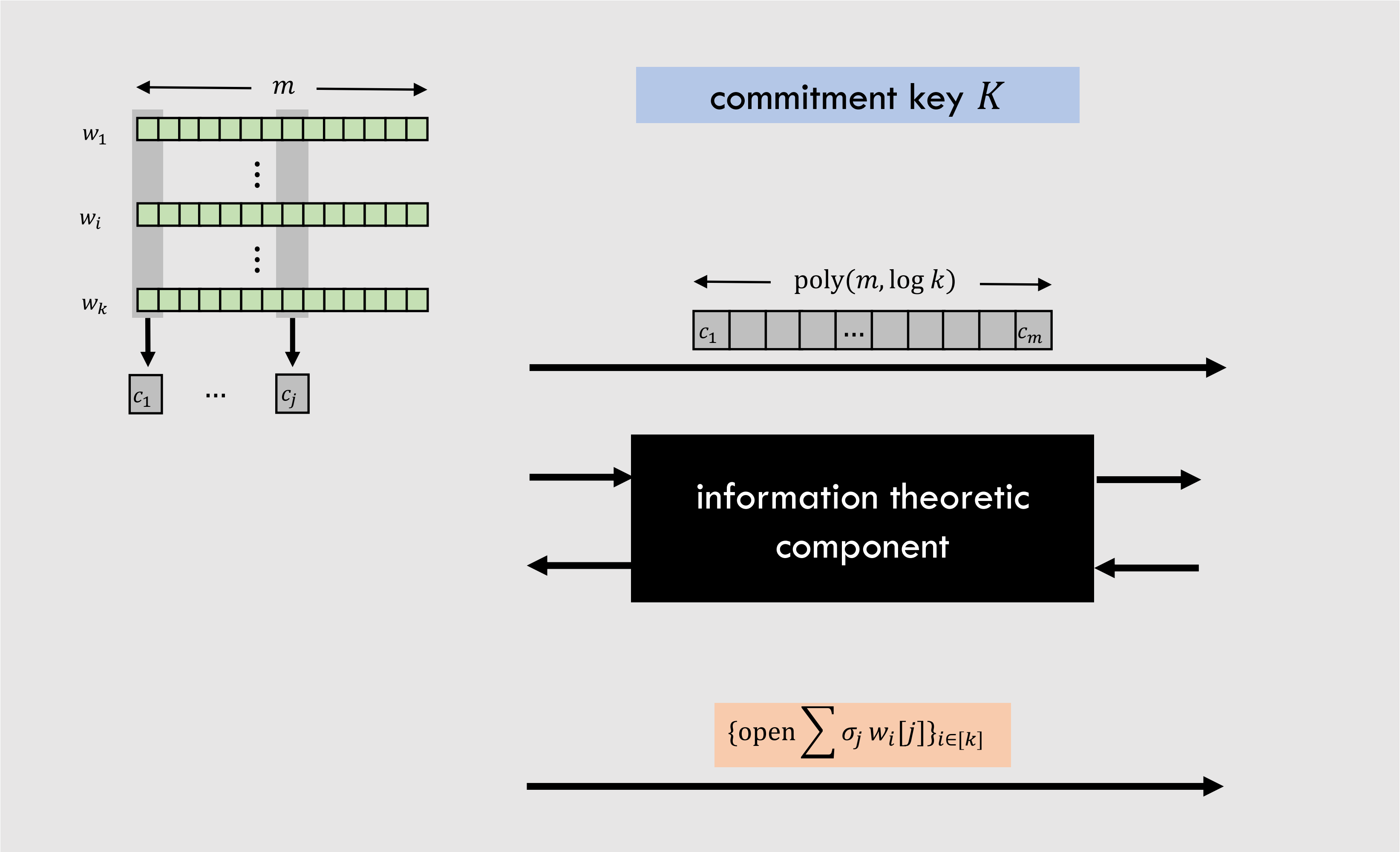
$\mathrm{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

We construct SSB with appropriate opening to f (with additional properties) based on QR

Dual Mode Batch Argument

Protocol Template



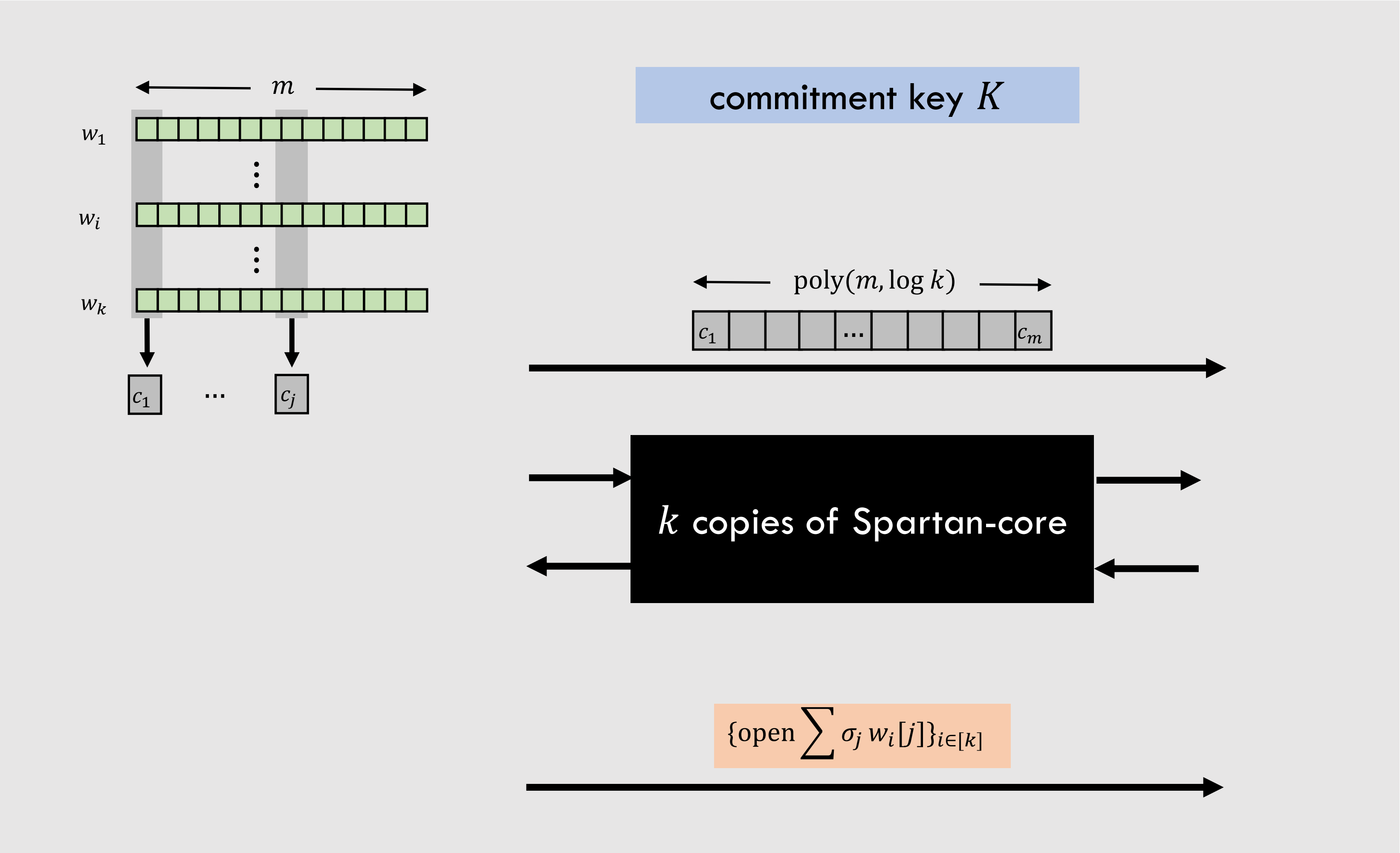
$\mathrm{SAT} = \{(C, x) \mid \exists w \ s.t.\ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

We construct SSB with linear homomorphic opening (with additional properties) based on QR

Dual Mode Batch Argument

Protocol Template



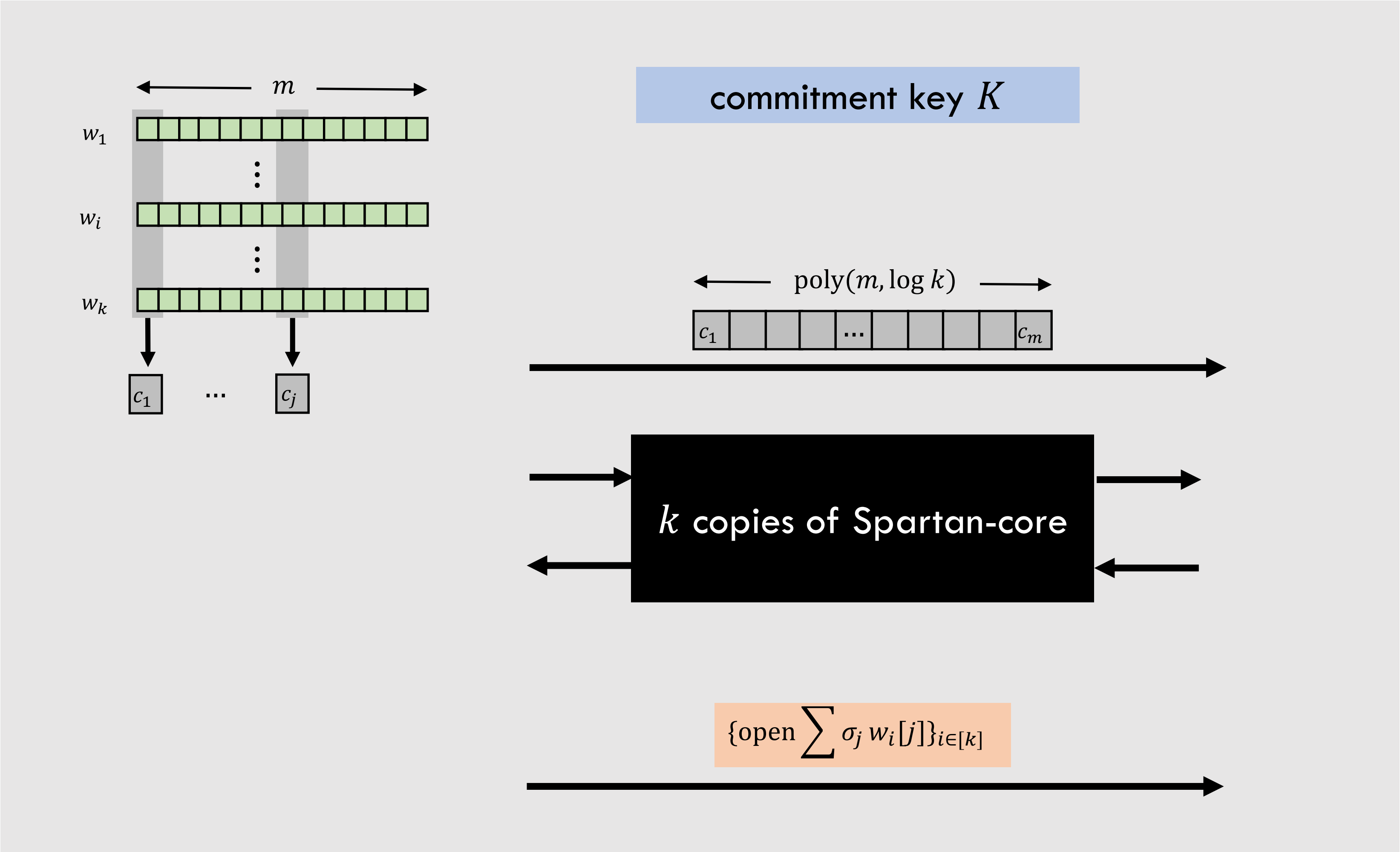
$\text{SAT} = \{(C, x) \mid \exists w \ s.t. \ C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \text{SAT}$

We construct SSB with linear homomorphic opening (with additional properties) based on QR

Dual Mode Batch Argument

Protocol Template



$\mathrm{SAT} = \{(C, x) \mid \exists w \; s.t. \; C(x, w) = 1\}$

$\forall i \in [k], (C, x_i) \in \mathrm{SAT}$

We construct SSB with linear homomorphic opening (with additional properties) based on QR

BAD computable in TC^0.

Concluding Remarks

Theorem

Assuming QR + (LWE/sub-exp DDH) there exists a non-interactive batch argument for NP where

$$|\Pi| = \tilde{O}(|C| + \sqrt{k|C|})$$

Concluding Remarks

Theorem

Assuming QR + (LWE/sub-exp DDH) there exists a non-interactive batch argument for NP where

$$|\Pi| = \tilde{O}(|C| + \sqrt{k|C|})$$

Follow up work [C-Jain-Jin'21b] (ia.cr/2021/808)

- Batch arguments for NP with improved parameters
- Application of batch arguments to construct delegation scheme for $\mathcal{P}$

Thank you. Questions?

Arka Rai Choudhuri

achoud@cs.jhu.edu

ia.cr/2021/807