Homomorphic Secret Sharing with Verifiable Evaluation

TCC 2024

Arka Rai Choudhuri
Nexus

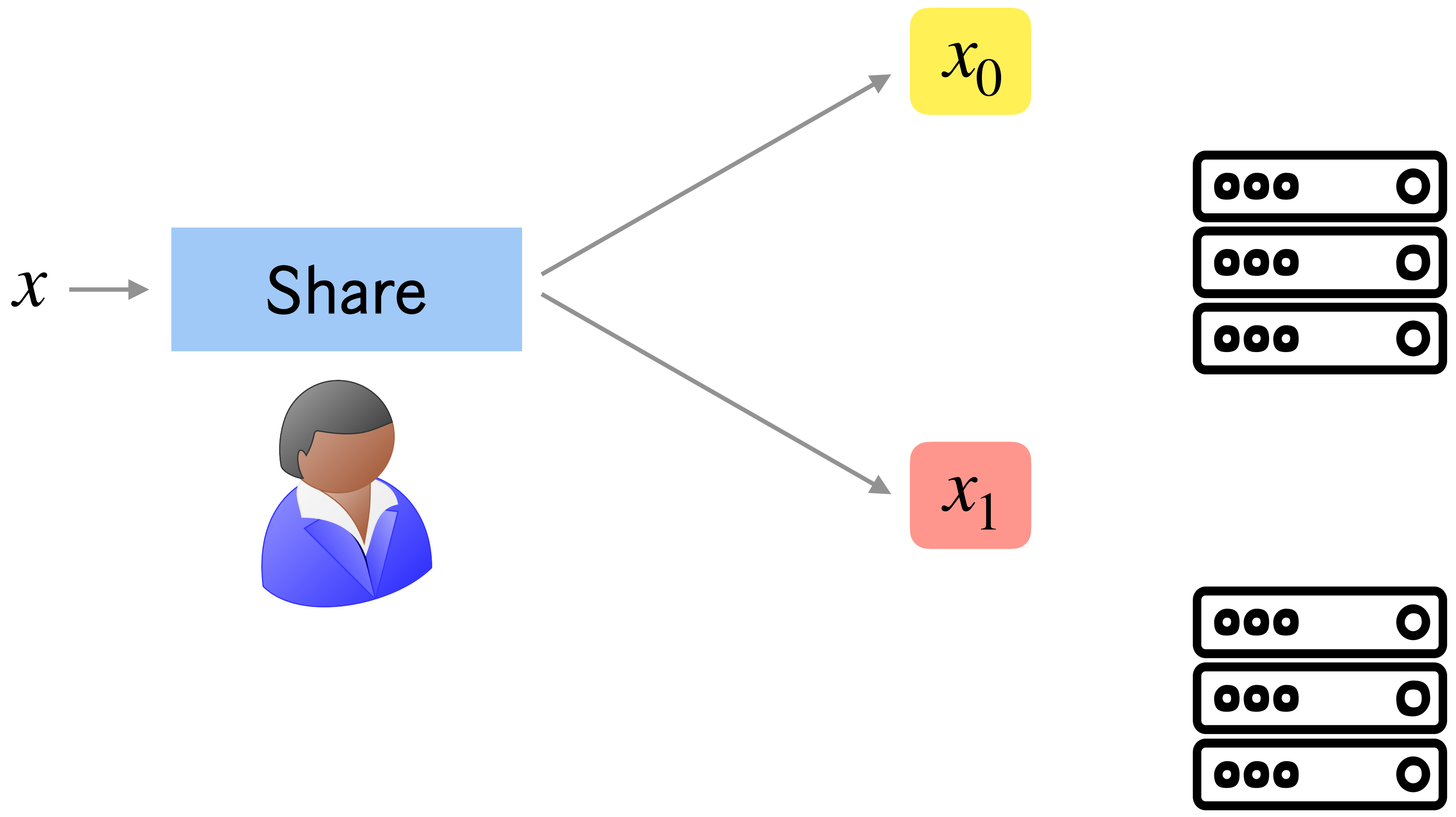
Aarushi Goel
Purdue University

Aditya Hegde
Johns Hopkins University

Abhishek Jain
NTT Research
Johns Hopkins University

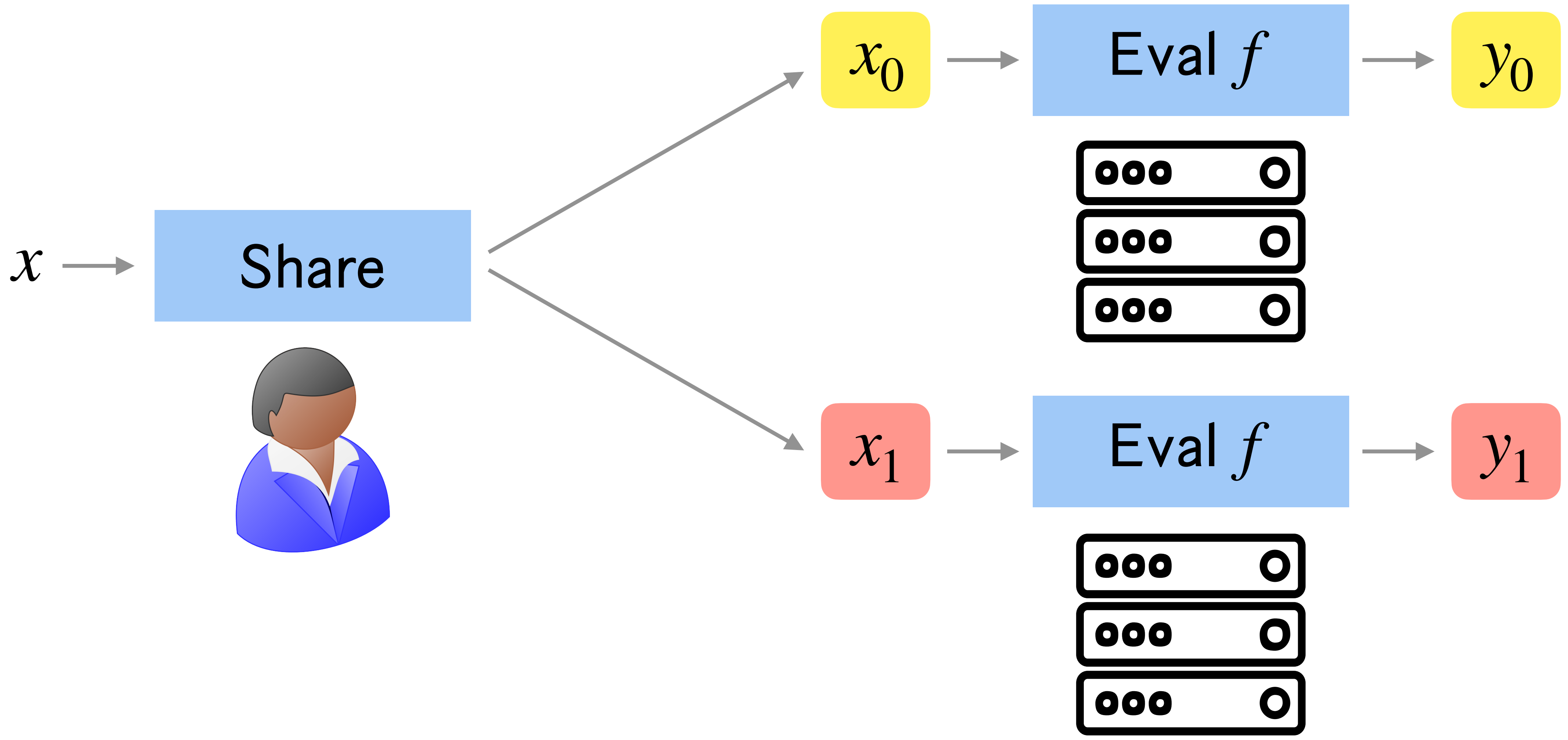
Homomorphic Secret Sharing

[Boyle-Gilboa-Ishai 16]



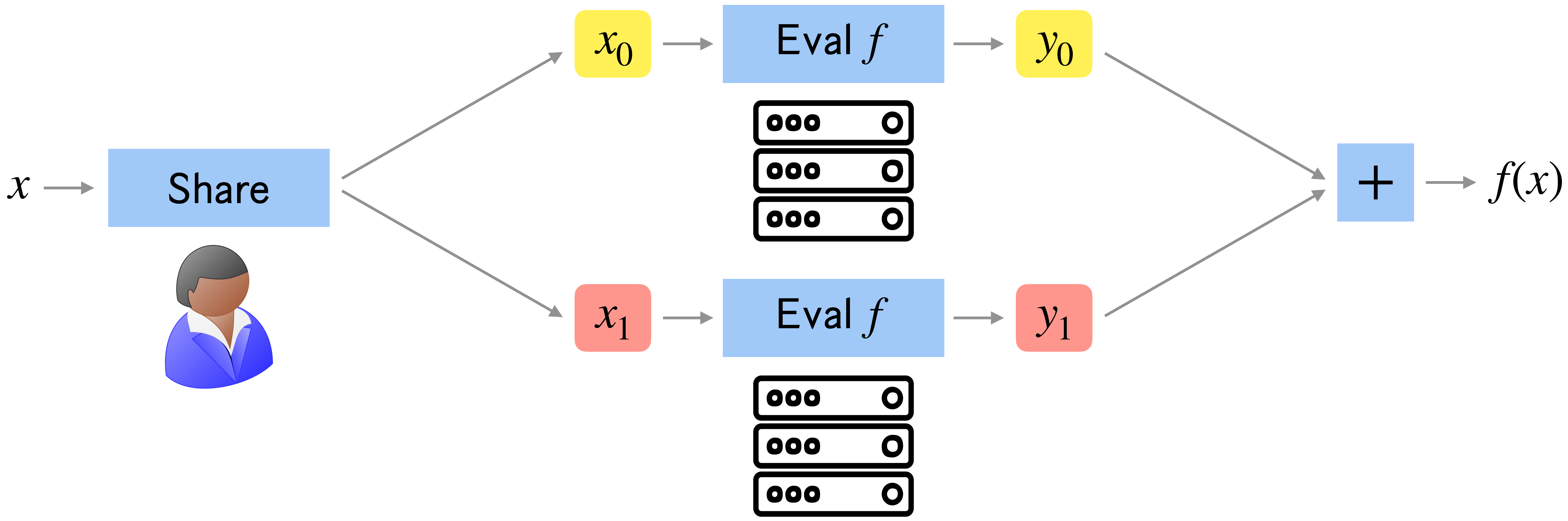
Homomorphic Secret Sharing

[Boyle-Gilboa-Ishai 16]



Homomorphic Secret Sharing

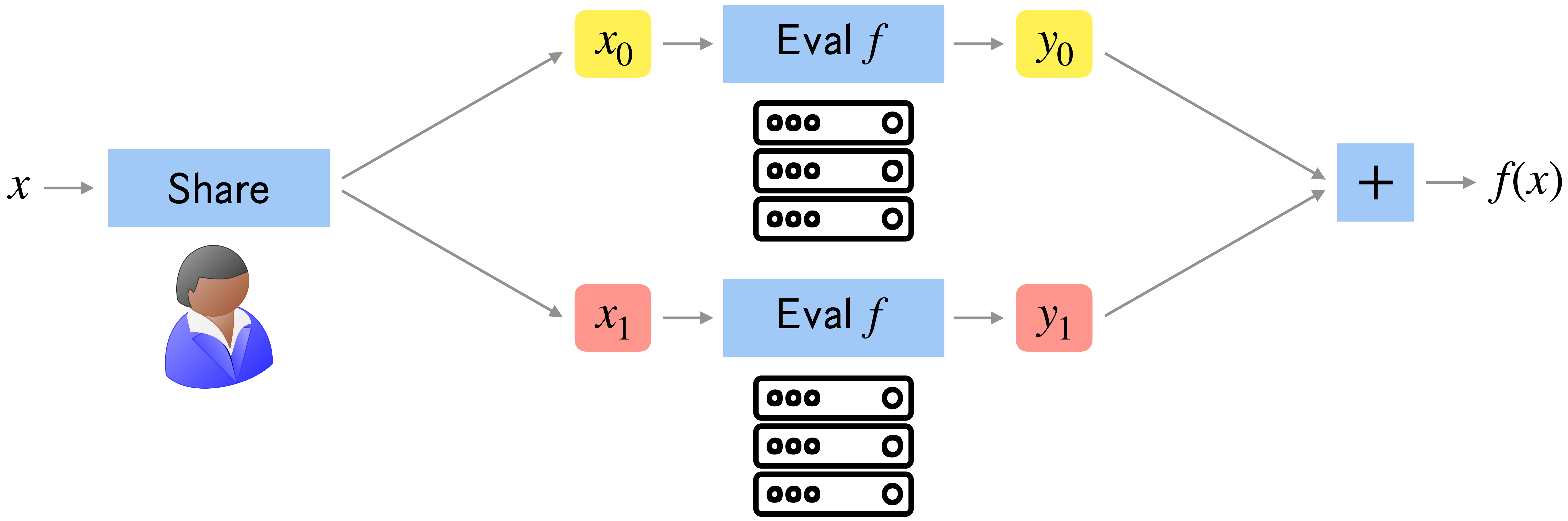
[Boyle-Gilboa-Ishai 16]



Correctness $y_0 + y_1 = f(x)$

Homomorphic Secret Sharing

[Boyle-Gilboa-Ishai 16]

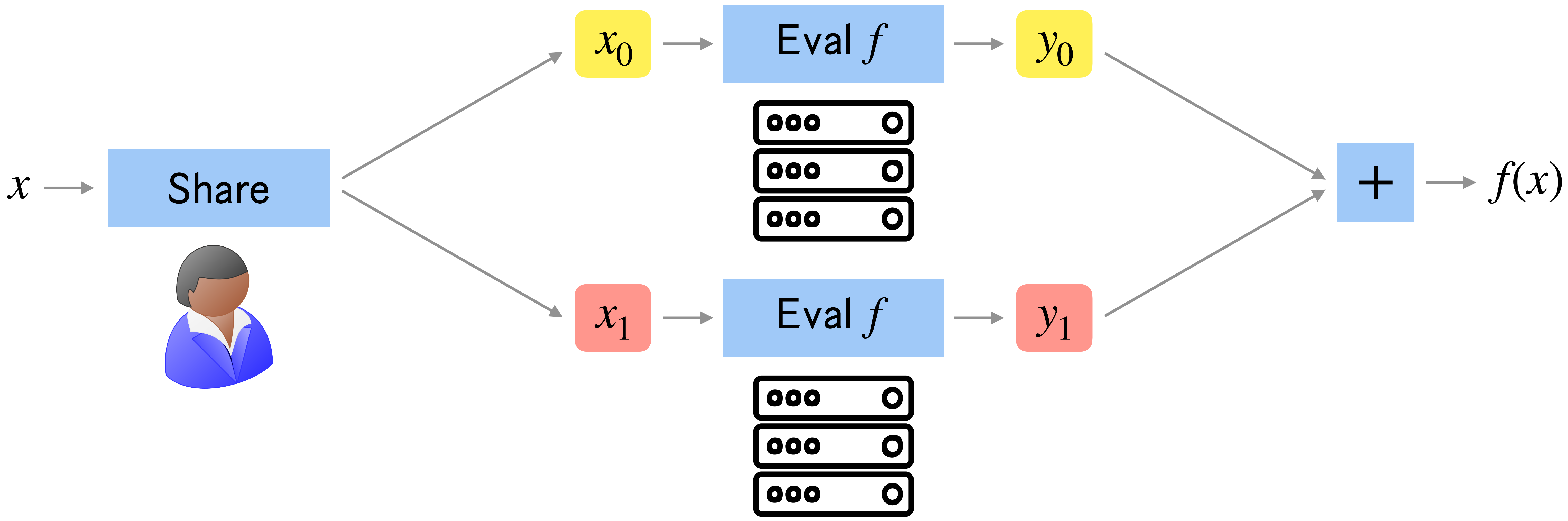


Correctness $y_0 + y_1 = f(x)$

Security x_0 and x_1 hide x

Homomorphic Secret Sharing

[Boyle-Gilboa-Ishai 16]



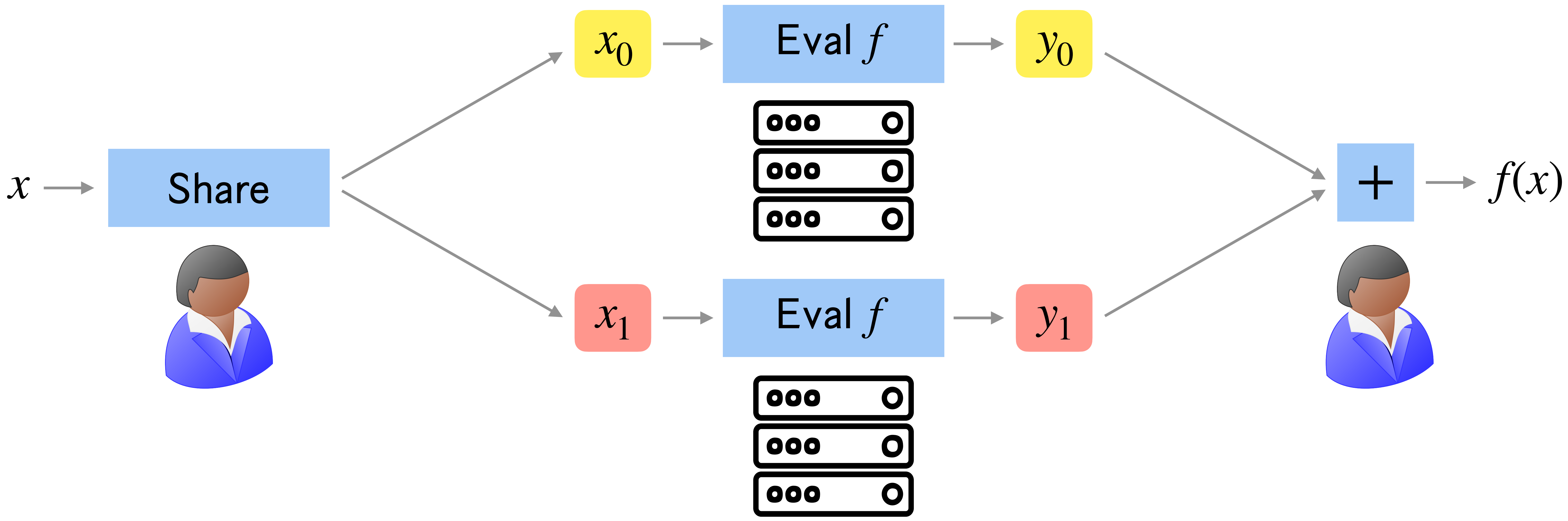
Correctness $y_0 + y_1 = f(x)$

Security x_0 and x_1 hide x

Succinctness y_0 , y_1 same size as $f(x)$

Homomorphic Secret Sharing

[Boyle-Gilboa-Ishai 16]



Enables private delegation of computation

Prior Works

Low degree polynomials

LPN

[Boyle-Couteau-Gilboa-Ishai-Kohl-Scholl 19]
[Couteau-Meyer 21]

Sparse LPN

[Dao-Ishai-Jain-Lin 23]

NC^1

DDH

[Boyle-Gilboa-Ishai 16]
[Boyle-Gilboa-Ishai 17]
[Boyle-Couteau-Gilboa-Ishai-Orrù 17]

DCR

[Fazio-Gennaro-Jafarikhah-Skeith 17]
[Orlandi-Scholl-Yakoubov 21]
[Roy-Singh 21]

Class Groups

[Abram-Damgård-Orlandi-Scholl 22]

LWE

[Boyle-Kohl-Scholl 19]

P/poly

FHE

[Dodis-Halevi-Rothblum-Wichs 16]
[Chilloti-Orsini-Scholl-Smart-Leeuwen 22]

iO + OWF

[Boyle-Gilboa-Ishai 15]

Prior Works

Low degree polynomials

LPN

[Boyle-Couteau-Gilboa-Ishai-Kohl-Scholl 19]

[Couteau-Meyer 21]

Sparse LPN

[Dao-Ishai-Jain-Lin 23]

NC^1

DDH

[Boyle-Gilboa-Ishai 16]

[Boyle-Gilboa-Ishai 17]

[Boyle-Couteau-Gilboa-Ishai-Orrù 17]

DCR

[Fazio-Gennaro-Jafarikhah-Skeith 17]

[Orlandi-Scholl-Yakoubov 21]

[Roy-Singh 21]

Class Groups

[Abram-Damgård-Orlandi-Scholl 22]*

LWE

[Boyle-Kohl-Scholl 19]

P/poly

FHE

[Dodis-Halevi-Rothblum-Wichs 16]

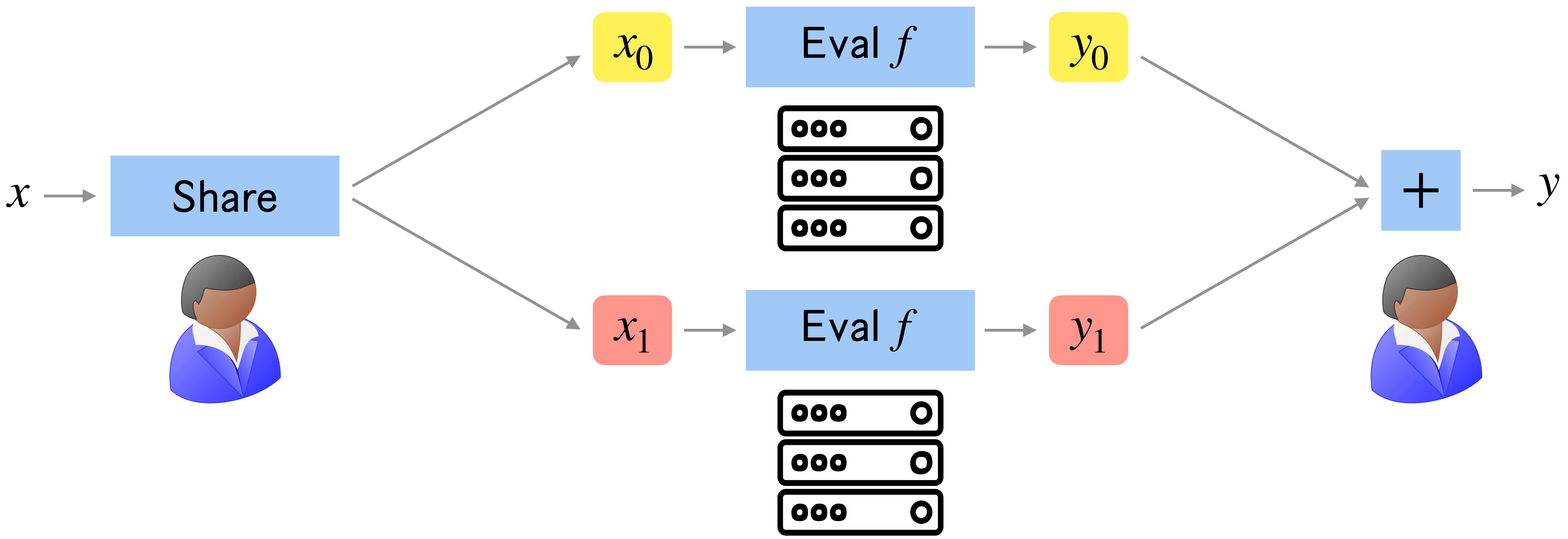
[Chilloti-Orsini-Scholl-Smart-Leeuwen 22]

iO + OWF

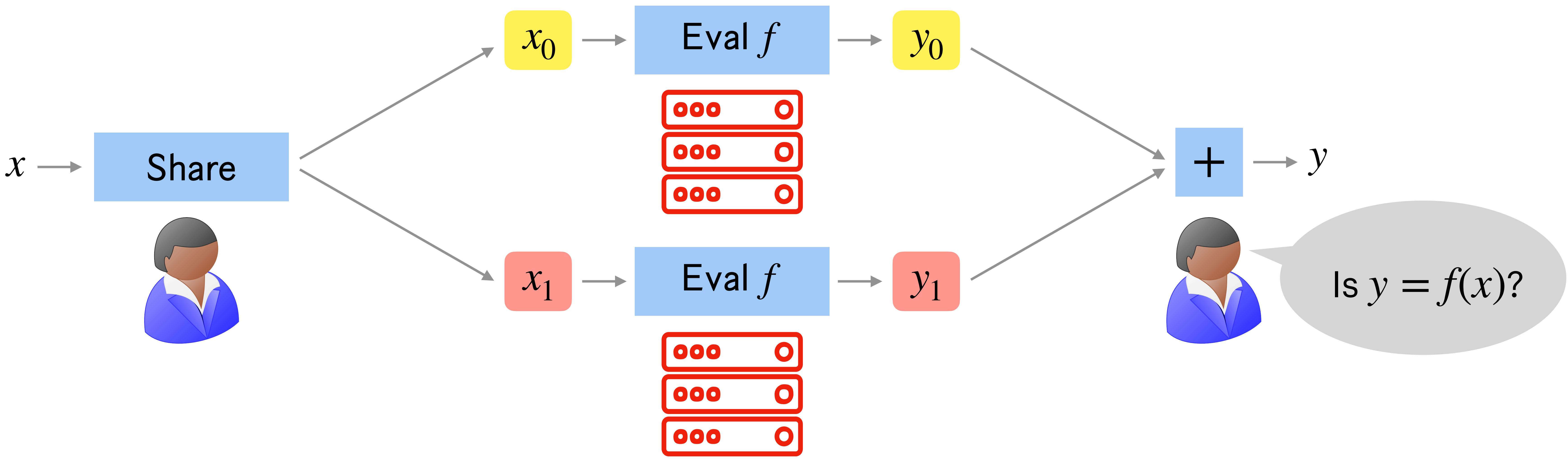
[Boyle-Gilboa-Ishai 15]

Assume semi-honest servers

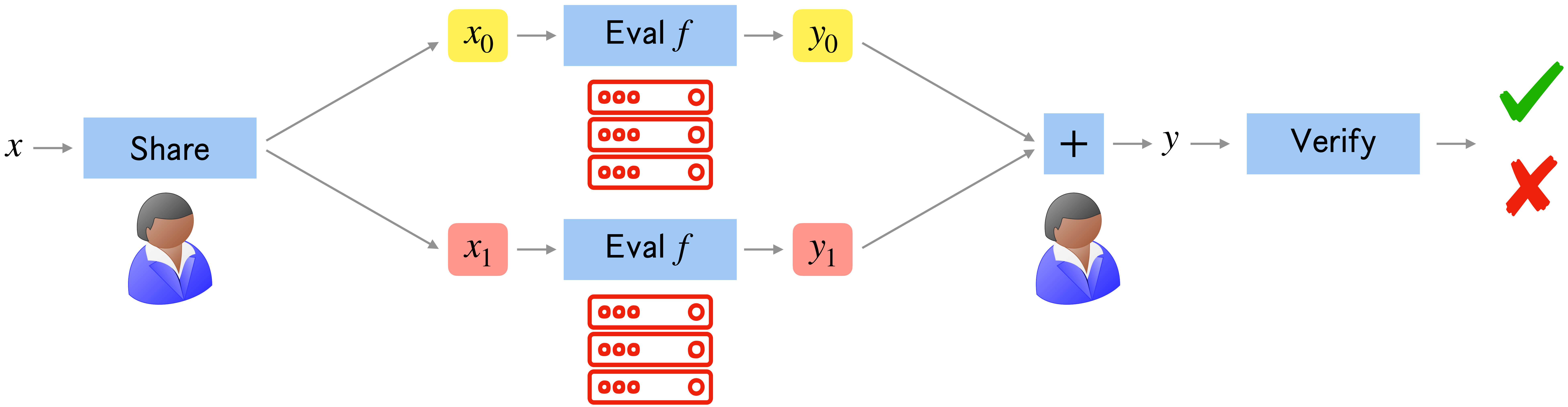
HSS with Verifiable Evaluation (ve-HSS)



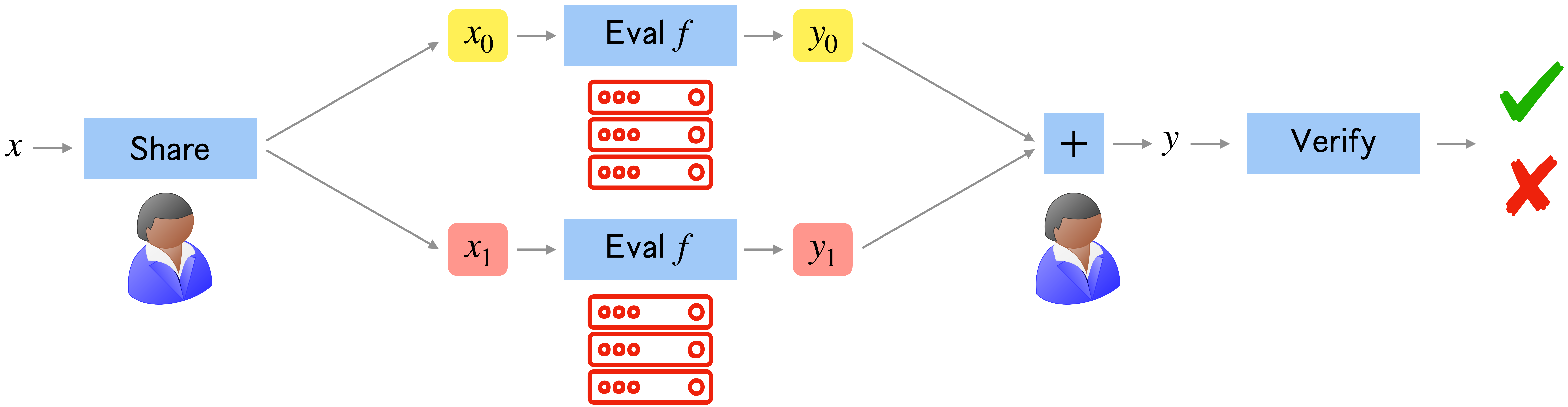
HSS with Verifiable Evaluation (ve-HSS)

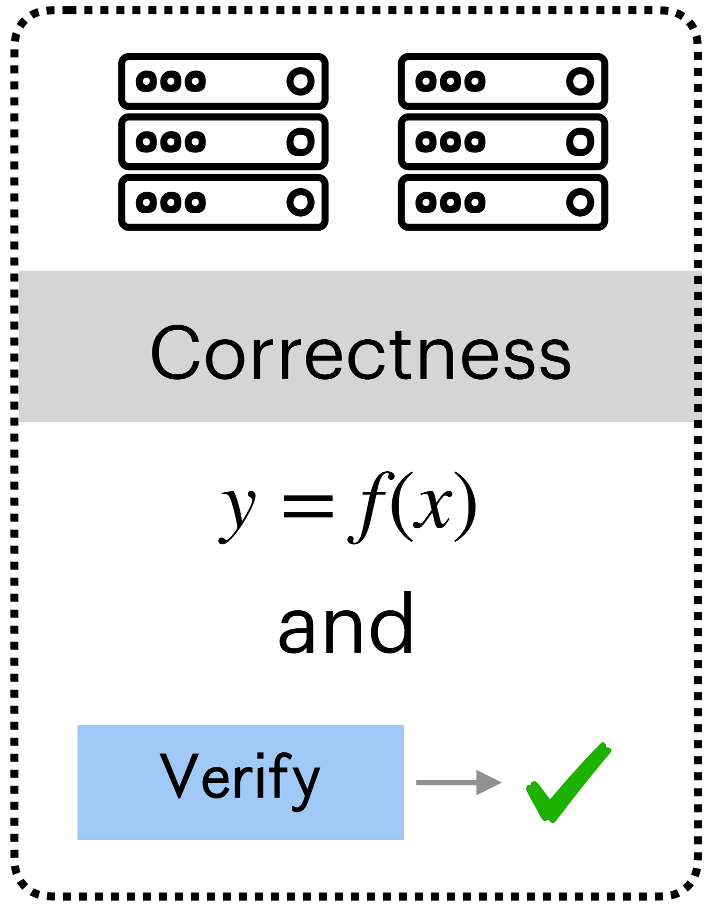


HSS with Verifiable Evaluation (ve-HSS)

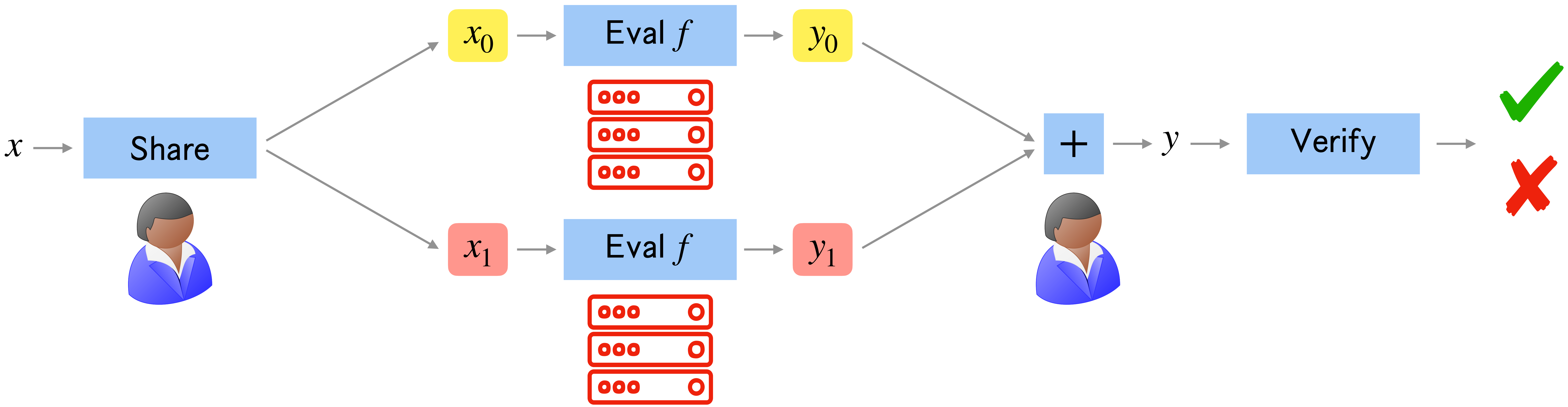


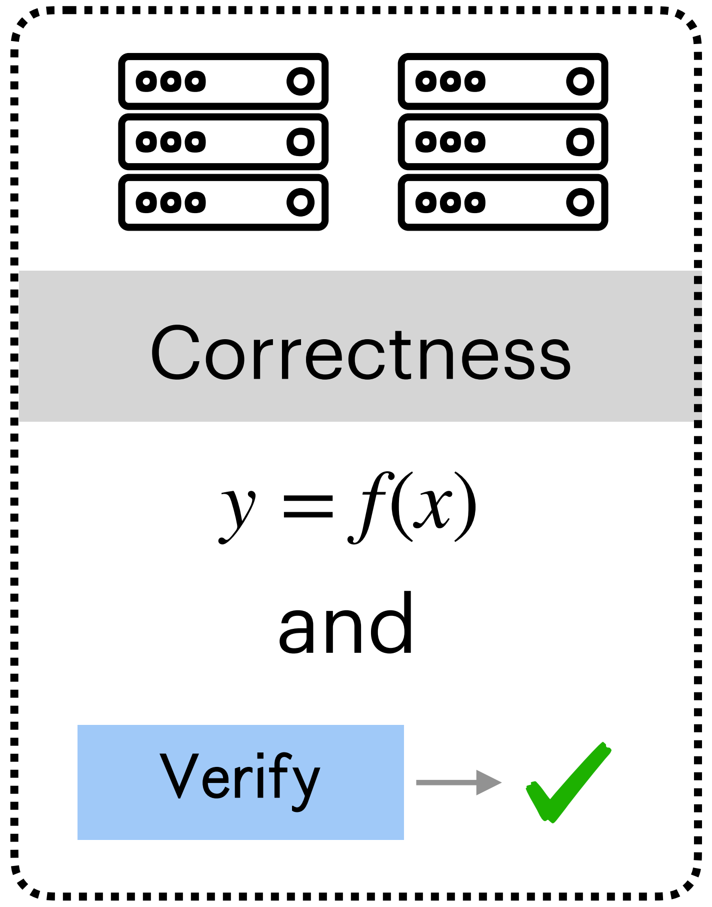
HSS with Verifiable Evaluation (ve-HSS)

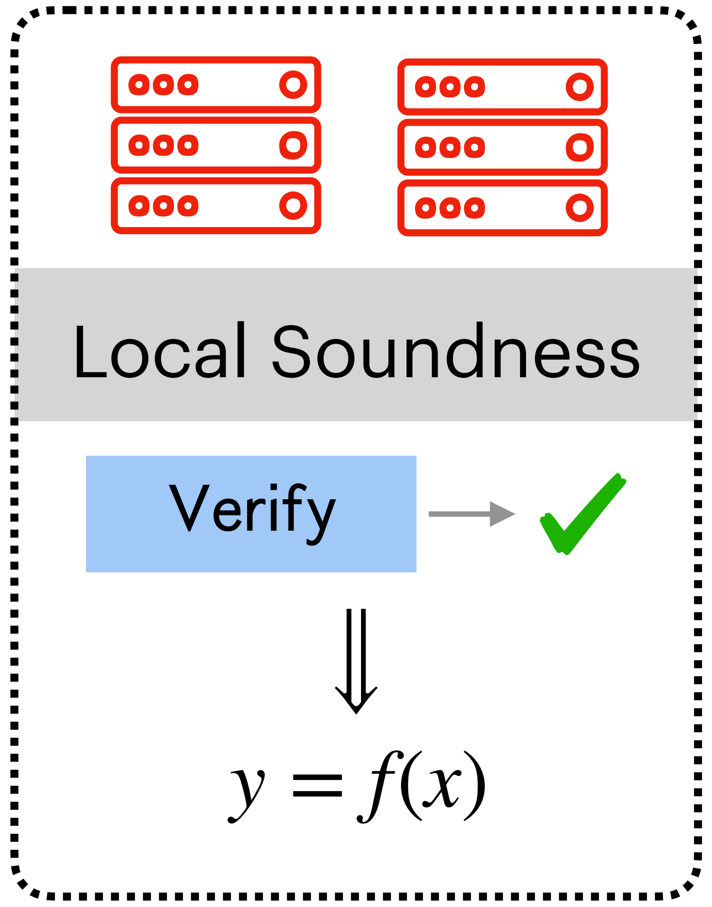




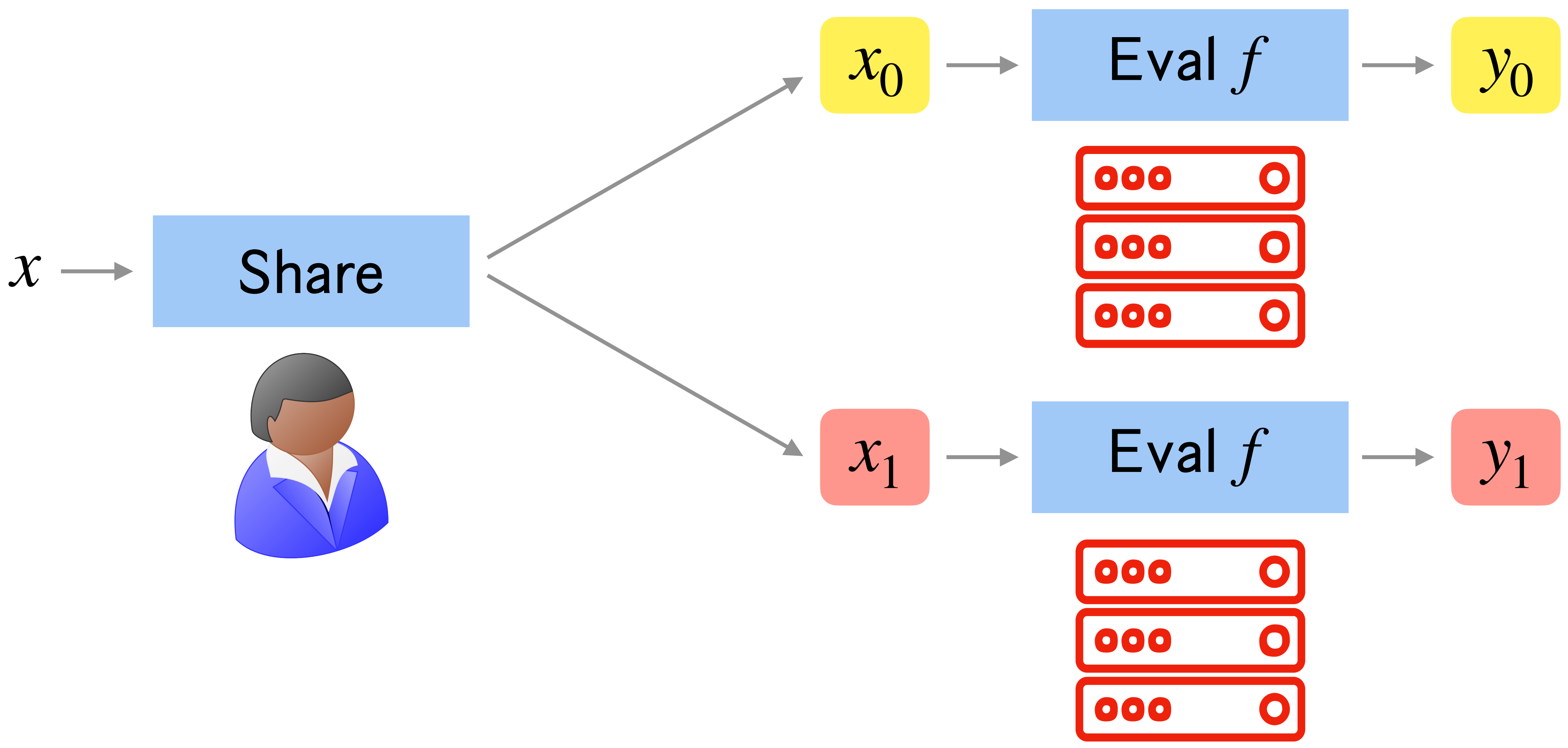
HSS with Verifiable Evaluation (ve-HSS)

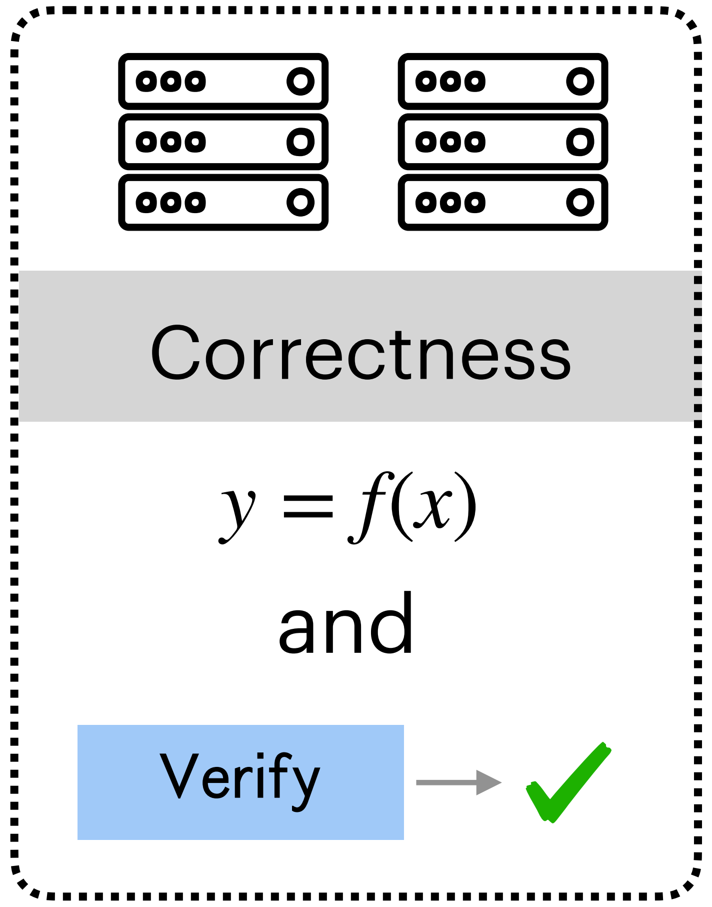


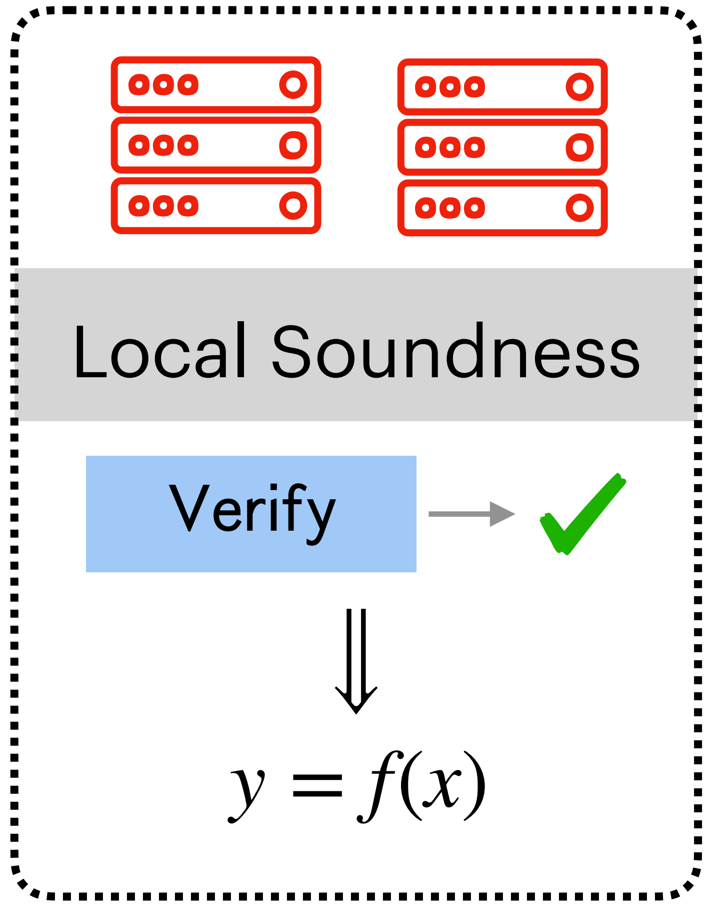




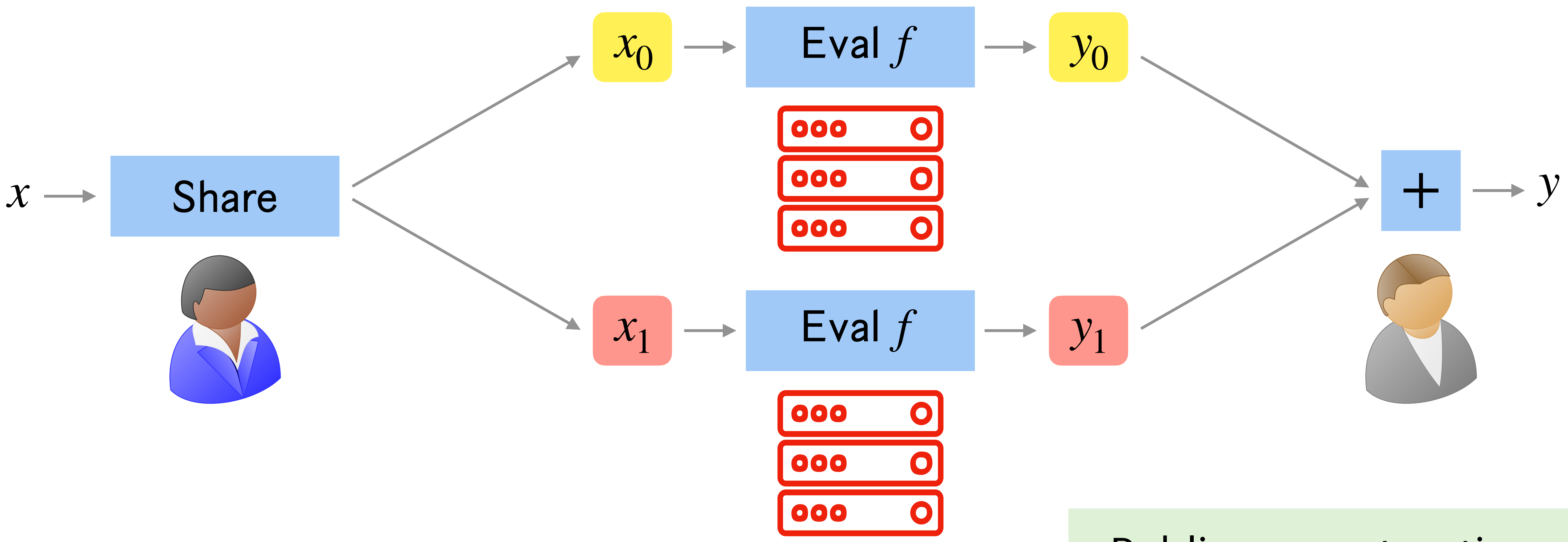
HSS with Verifiable Evaluation (ve-HSS)







HSS with Verifiable Evaluation (ve-HSS)



Public reconstruction of output

Correctness

$y = f(x)$

and

Verify → ✓

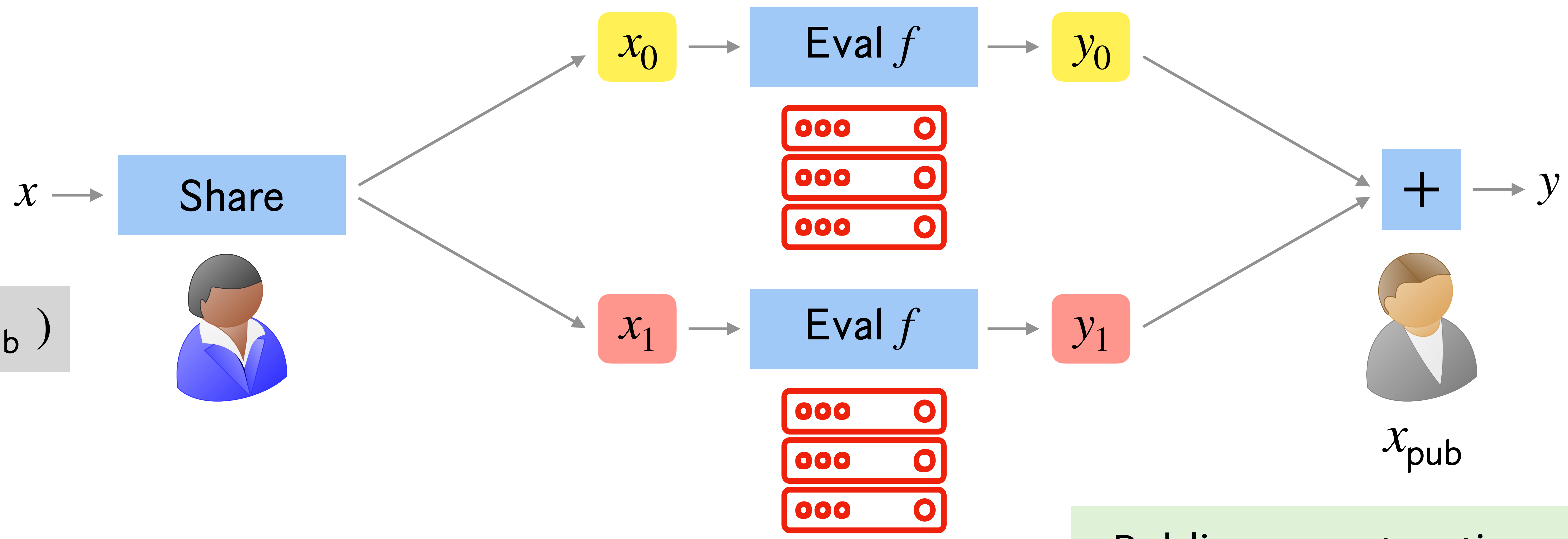
Local Soundness

Verify → ✓

$\Downarrow$

$y = f(x)$

HSS with Verifiable Evaluation (ve-HSS)



$x = (\, x_{\text{priv}} \,,\; x_{\text{pub}} \,)$

Public reconstruction of output

Correctness

$y = f(x)$

and

Verify → ✓

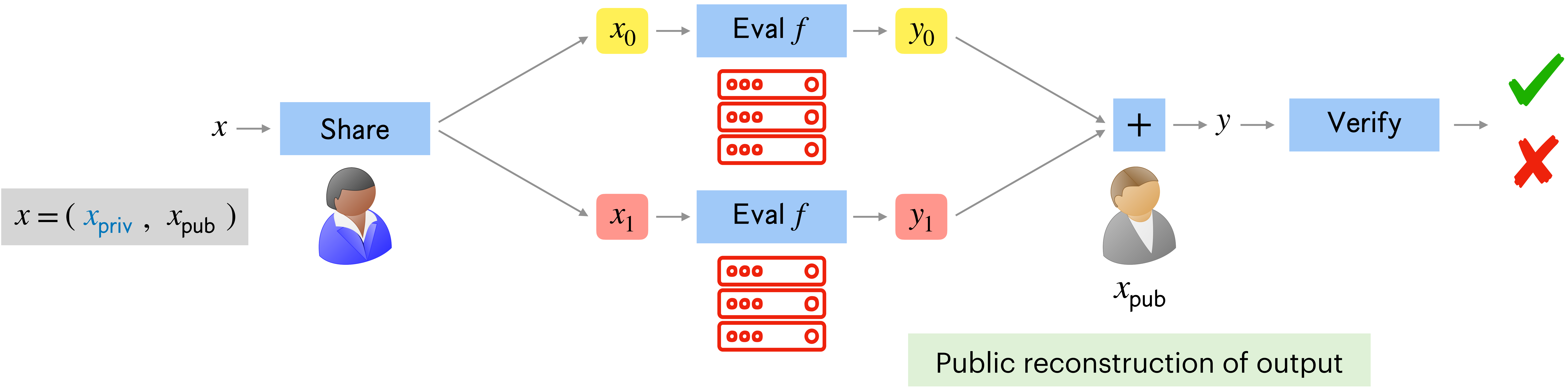
Local Soundness

Verify → ✓

$\Downarrow$

$y = f(x)$

HSS with Verifiable Evaluation (ve-HSS)



$x = (x_{\text{priv}},\ x_{\text{pub}})$

$x \rightarrow$ Share

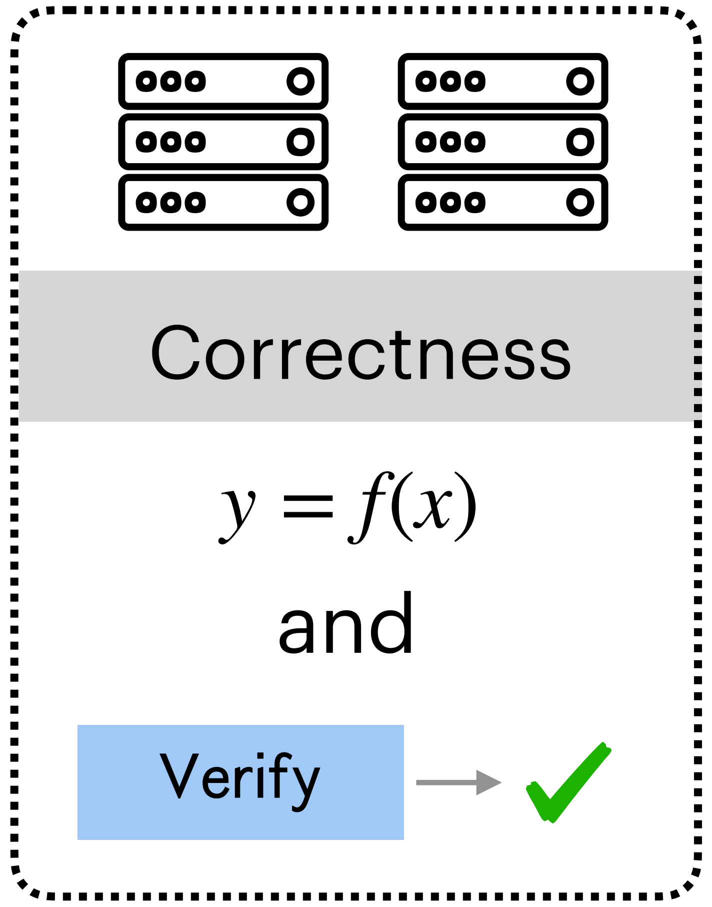
$x_0 \rightarrow$ Eval f $\rightarrow y_0$

$x_1 \rightarrow$ Eval f $\rightarrow y_1$

$+ \rightarrow y \rightarrow$ Verify $\rightarrow$ ✓ ✗

x_{pub}

Public reconstruction of output

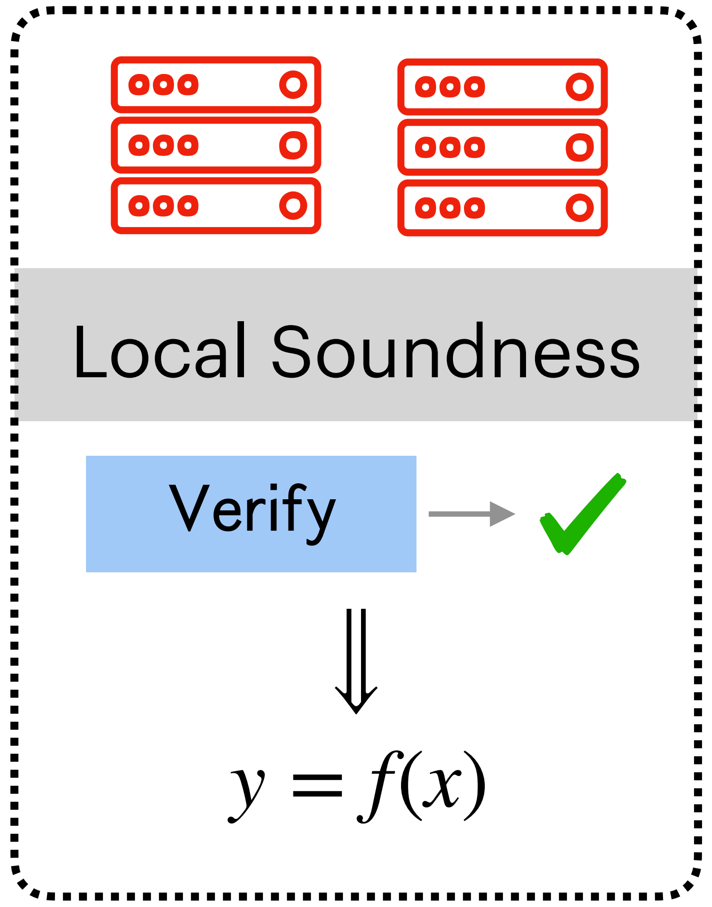


Correctness

$y = f(x)$

and

Verify → ✓

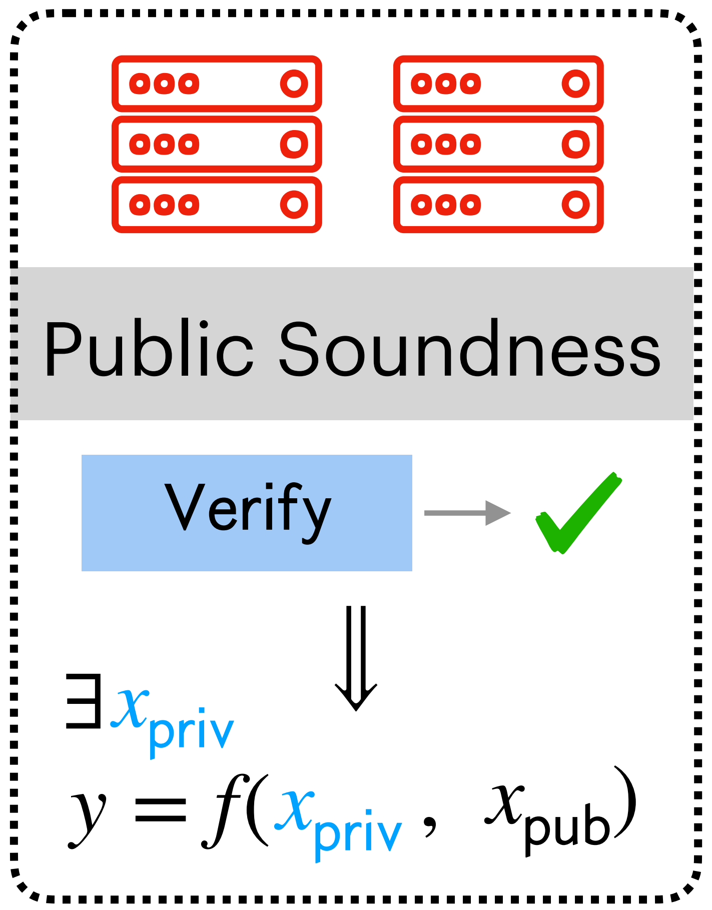


Local Soundness

Verify → ✓

$\Downarrow$

$y = f(x)$



Public Soundness

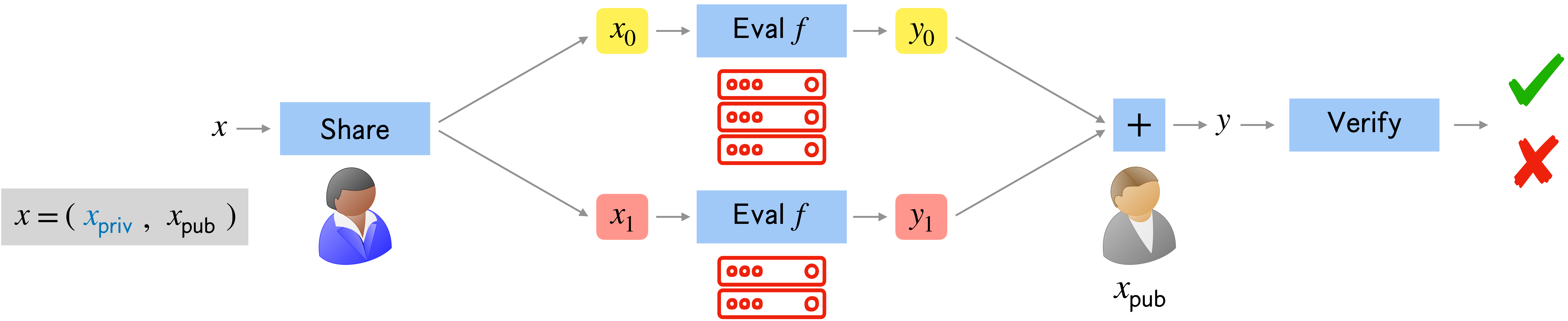
Verify → ✓

$\Downarrow$

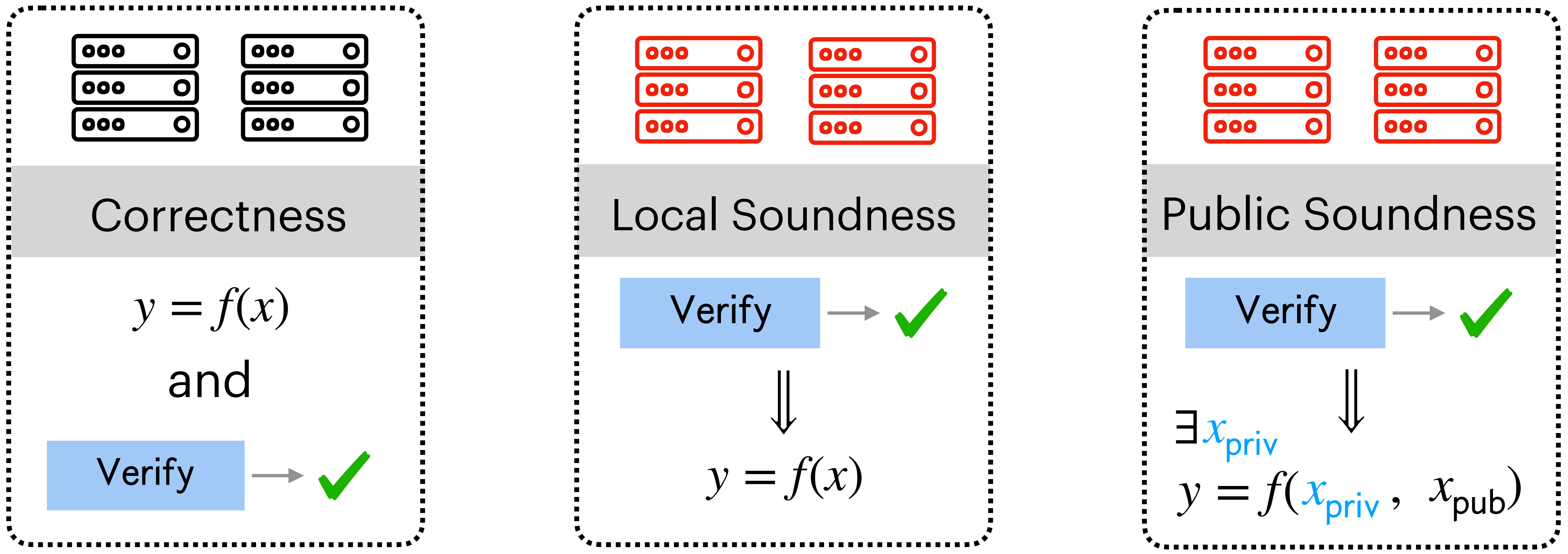
$\exists x_{\text{priv}}$

$y = f(x_{\text{priv}},\ x_{\text{pub}})$

HSS with Verifiable Evaluation (ve-HSS)

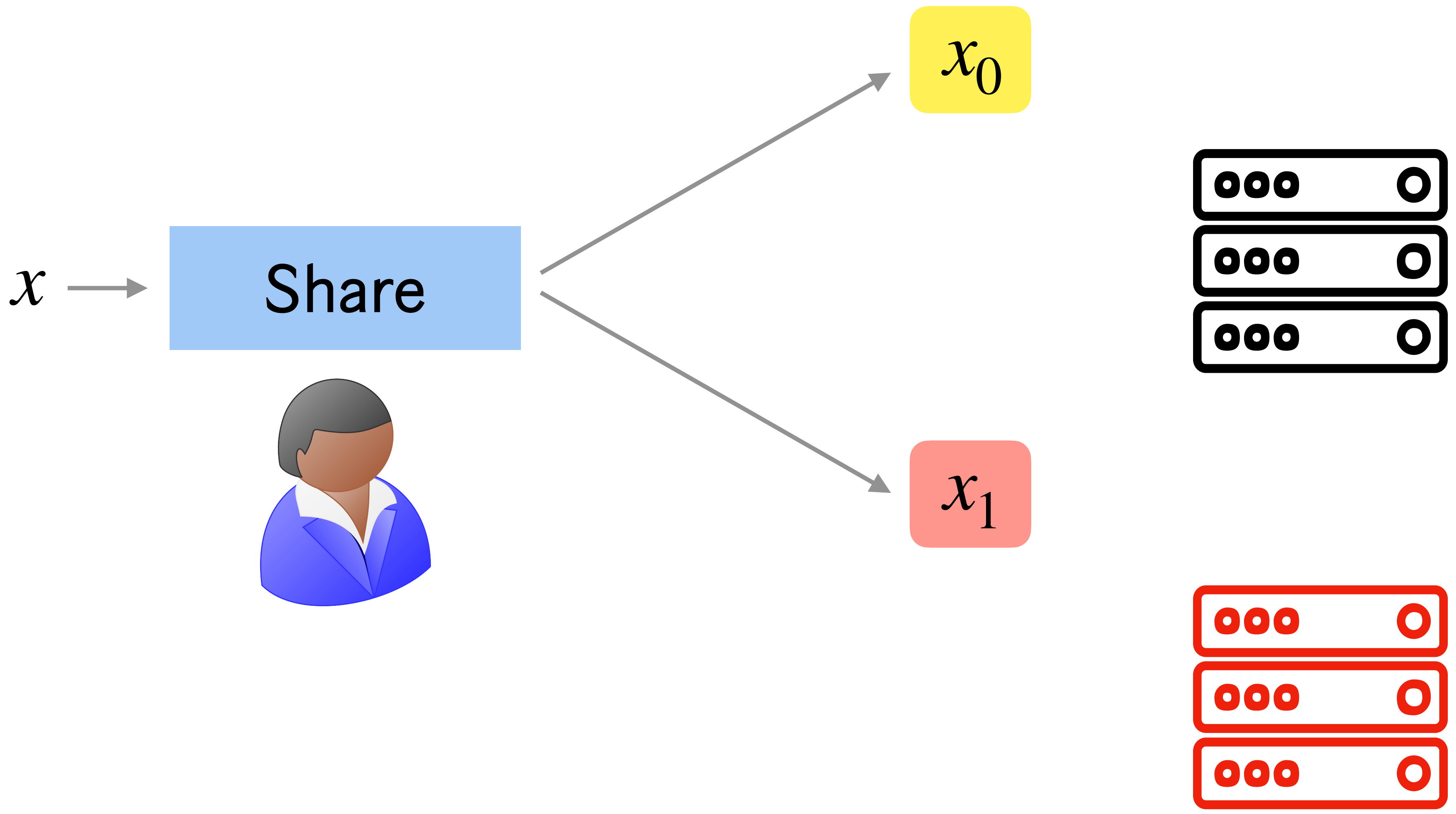


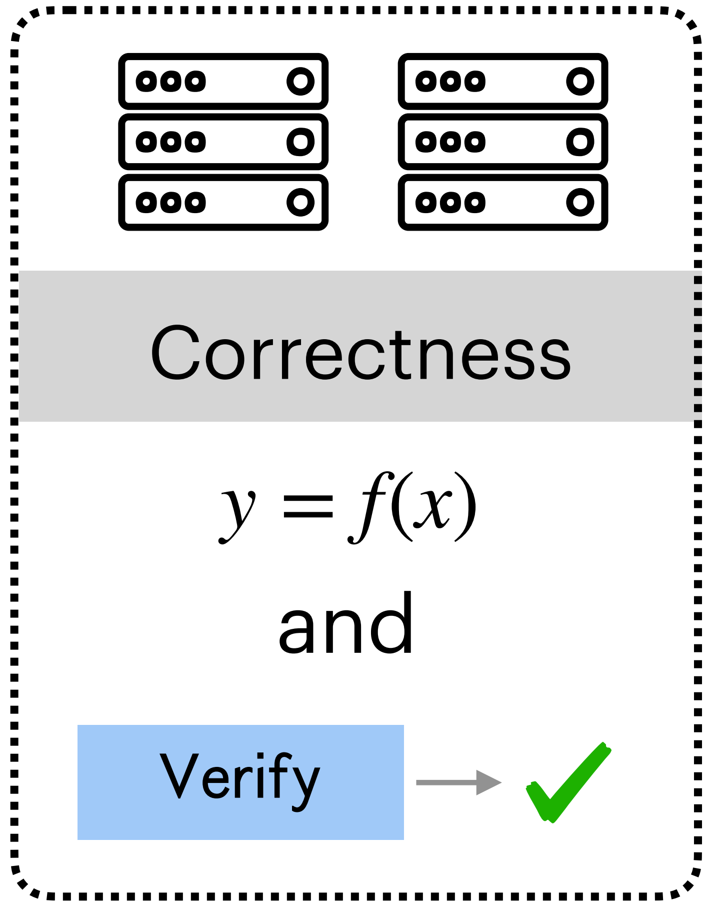
Public reconstruction of output



Privacy requires at least one honest server

HSS with Verifiable Evaluation (ve-HSS)



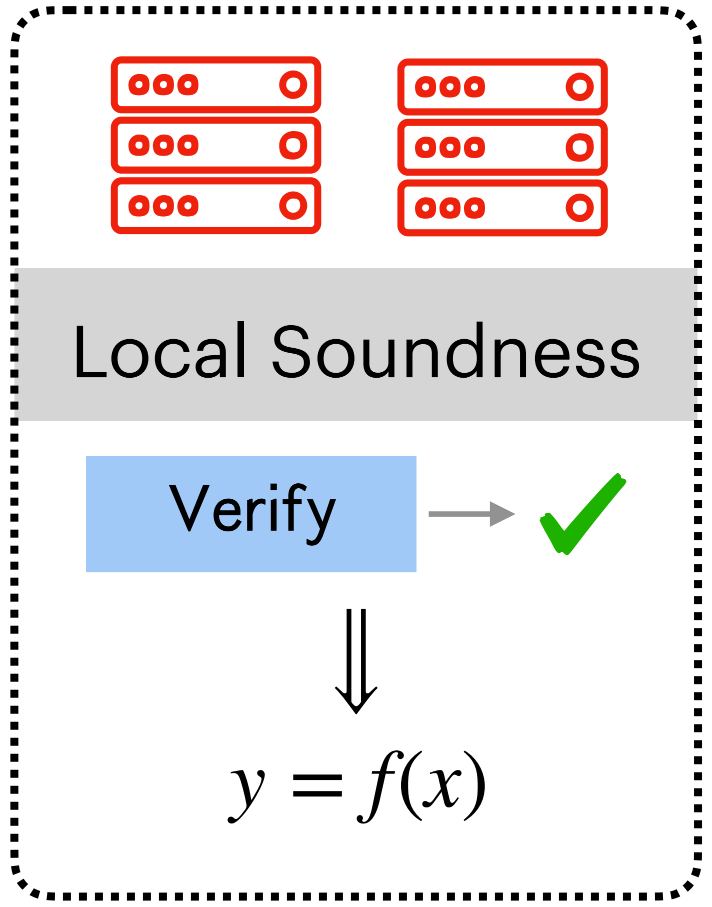


Correctness

$y = f(x)$

and

Verify → ✓

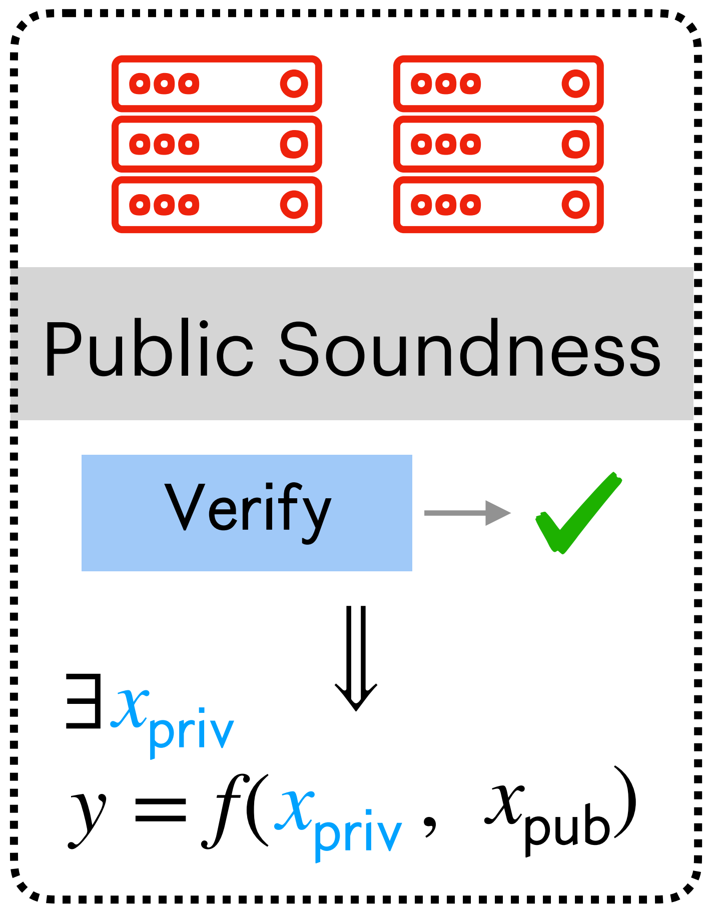


Local Soundness

Verify → ✓

$\Downarrow$

$y = f(x)$

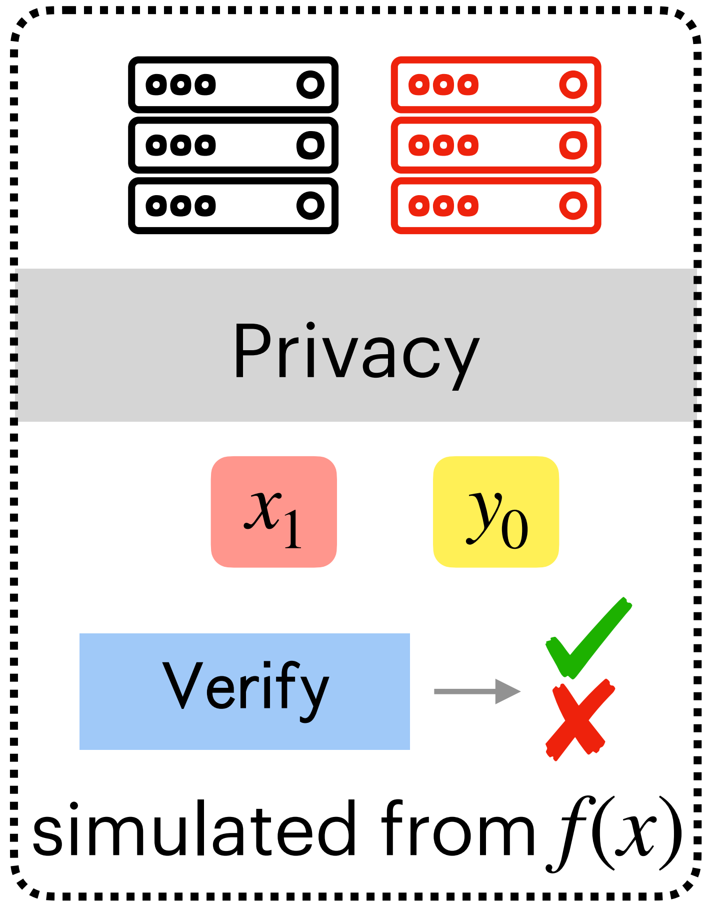


Public Soundness

Verify → ✓

$\exists x_{\text{priv}}$ $\Downarrow$

$y = f(x_{\text{priv}}, x_{\text{pub}})$



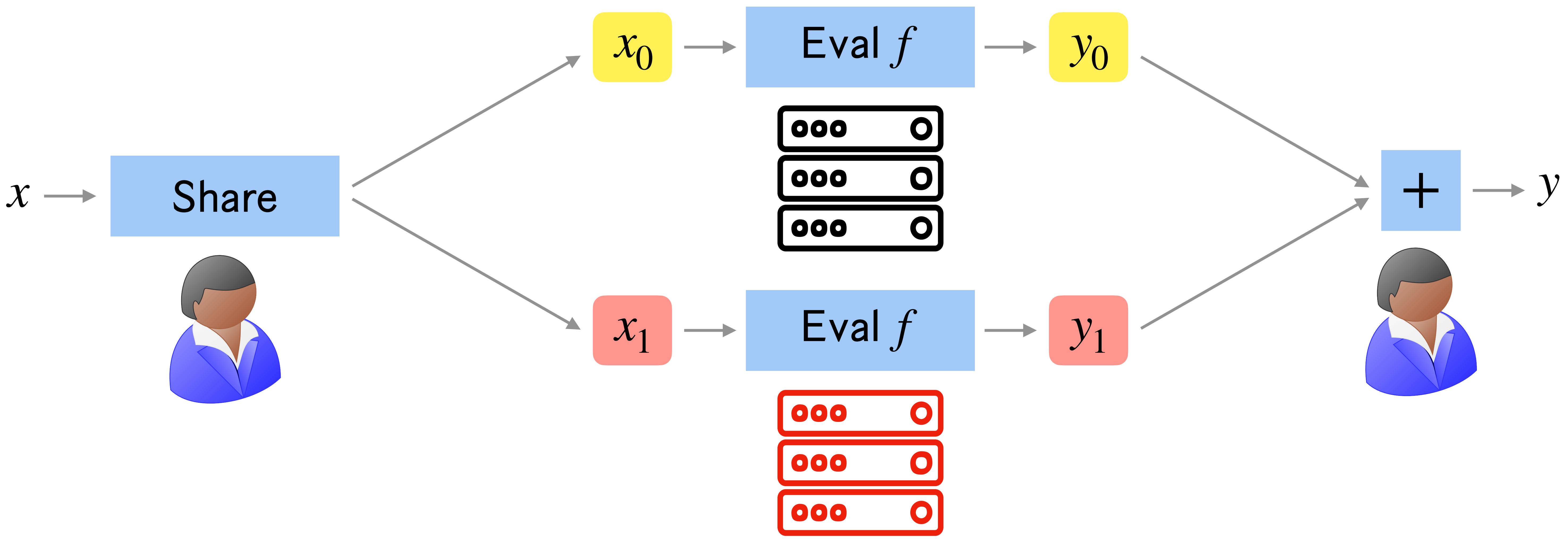
Privacy

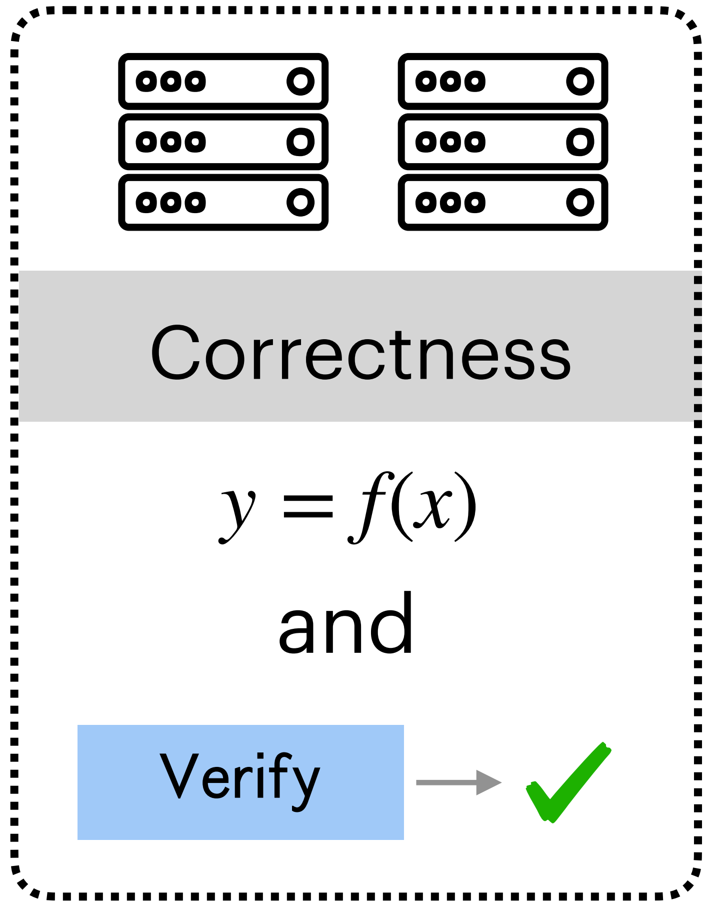
x_1 y_0

Verify → ✓ ✗

simulated from $f(x)$

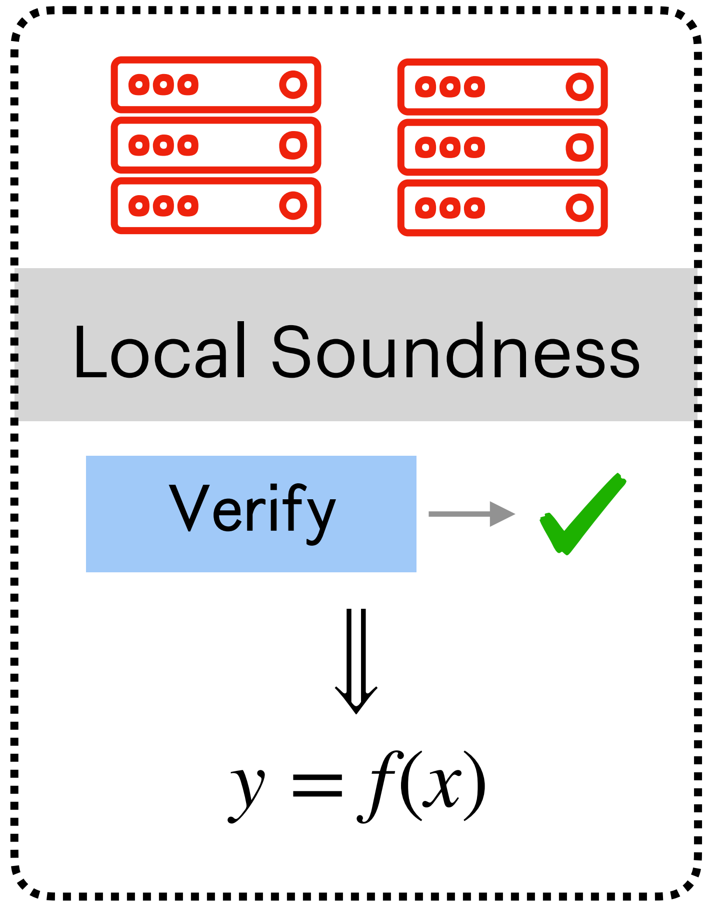
HSS with Verifiable Evaluation (ve-HSS)




Correctness

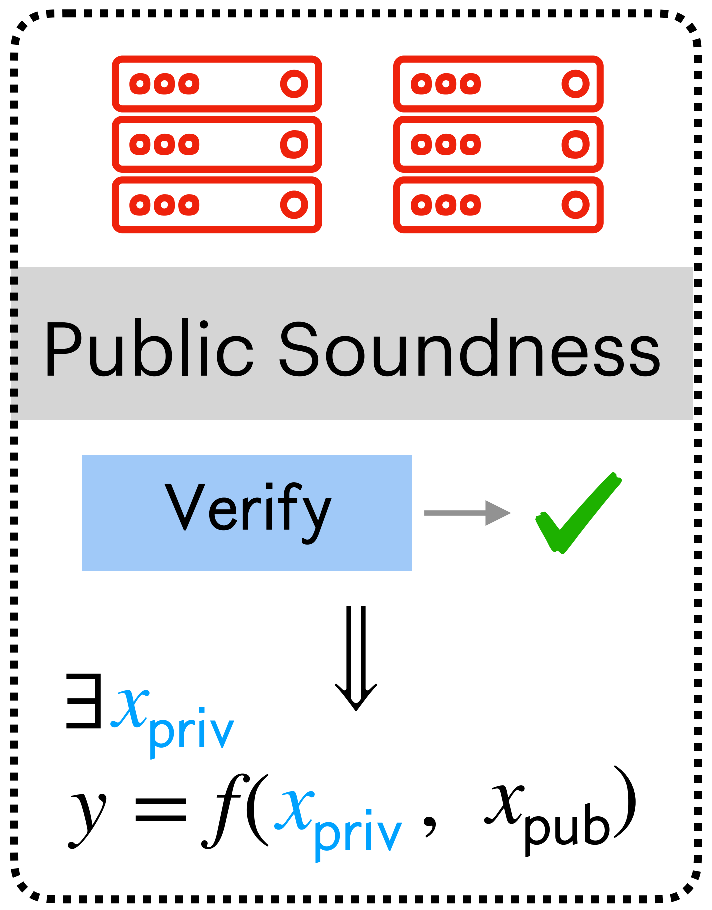
$y = f(x)$

and


Local Soundness

$\Downarrow$

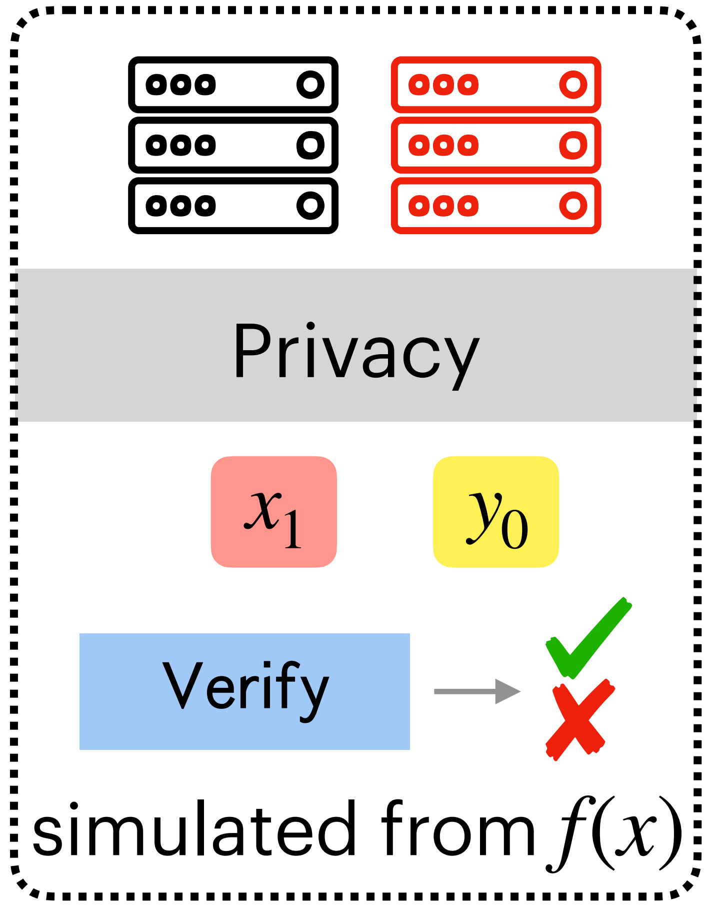
$y = f(x)$


Public Soundness

$\Downarrow$

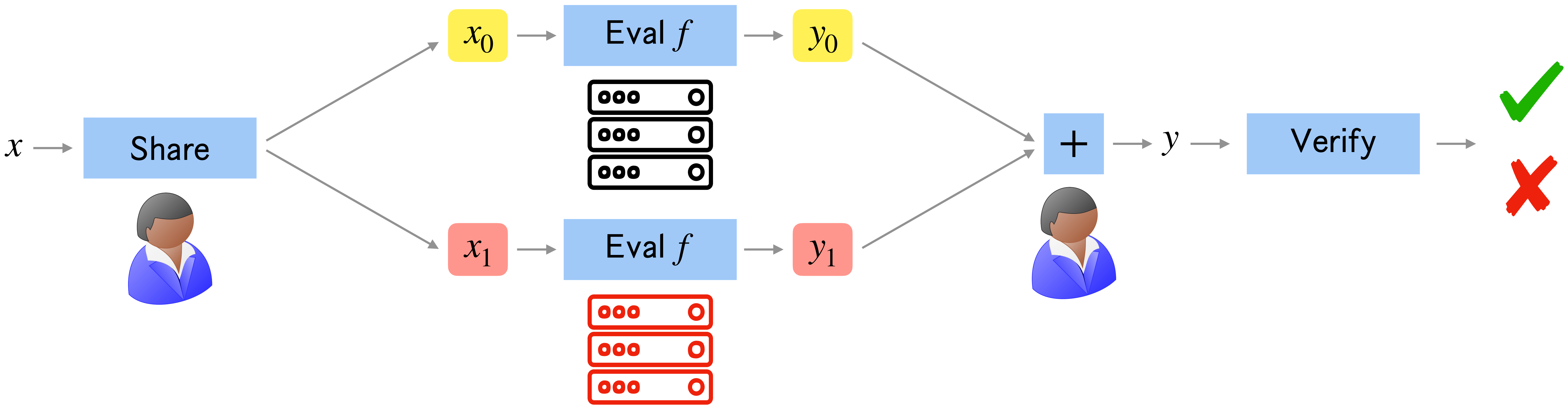
$\exists x_{\text{priv}}$

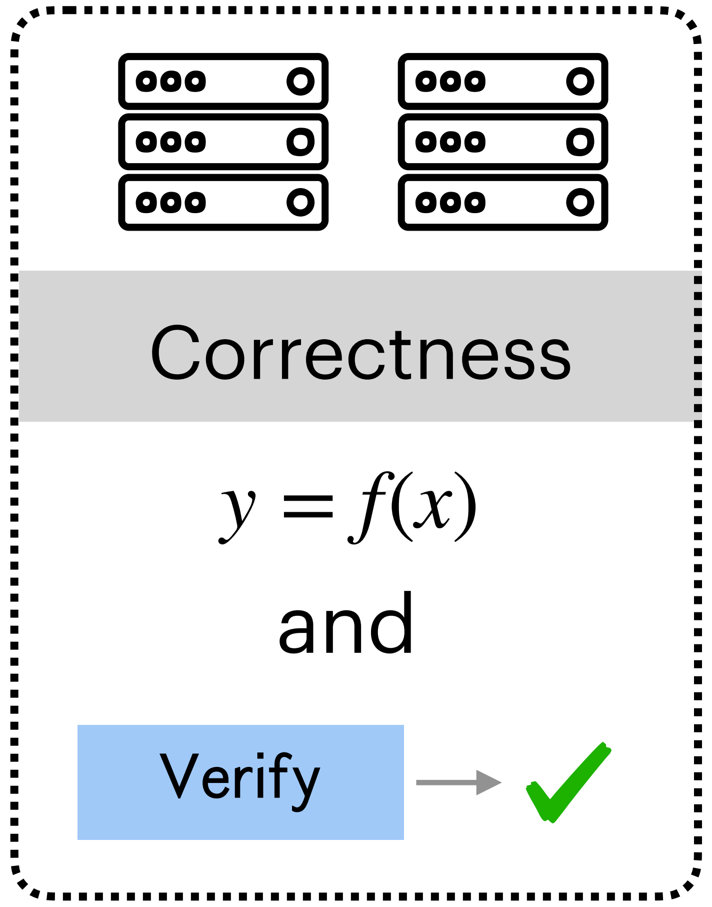
$y = f(x_{\text{priv}}, x_{\text{pub}})$

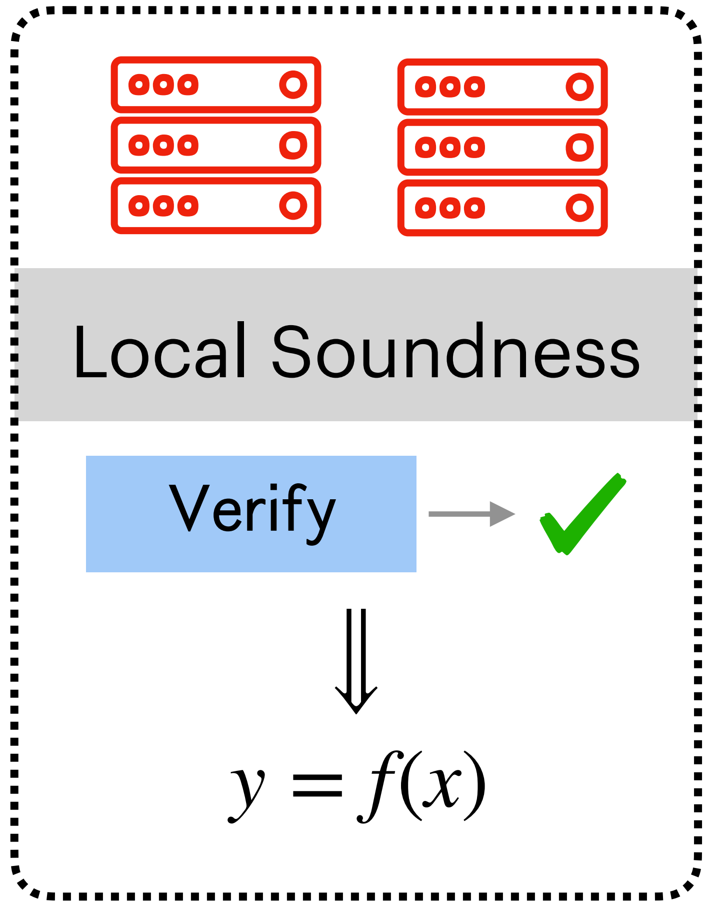

Privacy

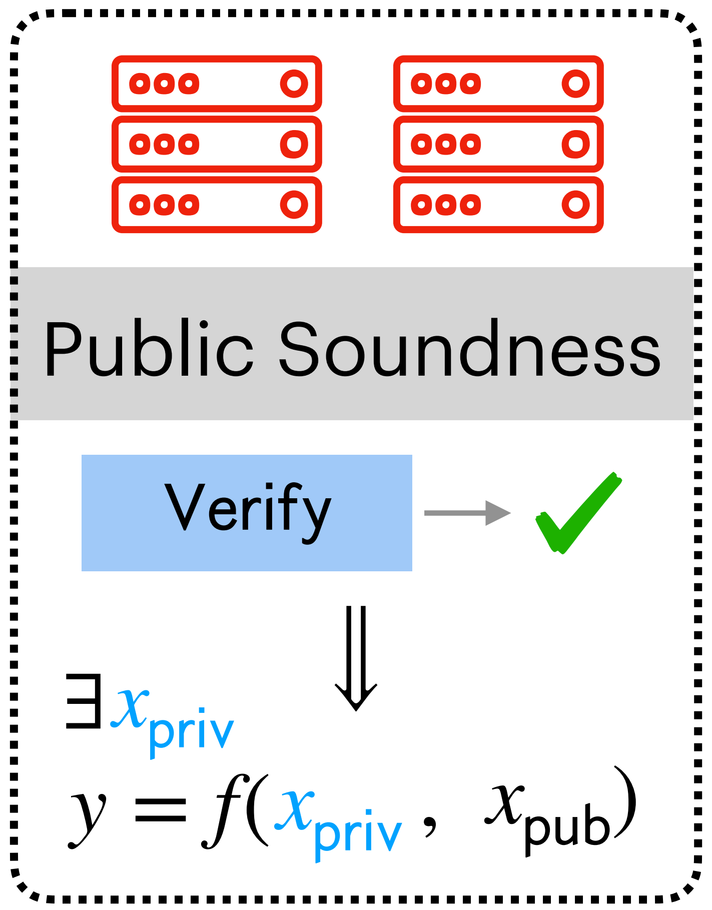
simulated from $f(x)$

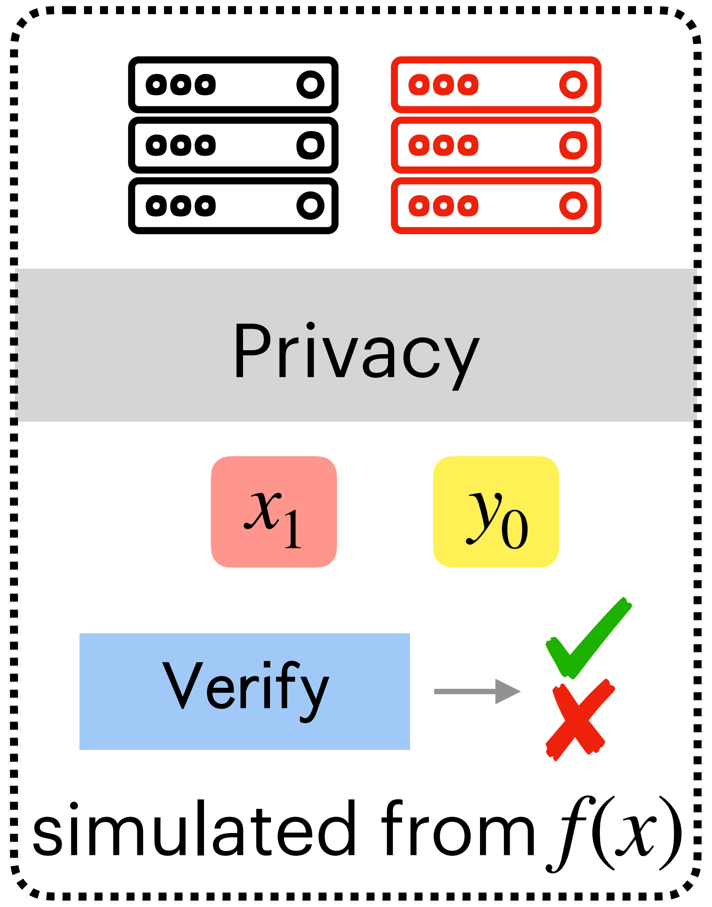
HSS with Verifiable Evaluation (ve-HSS)



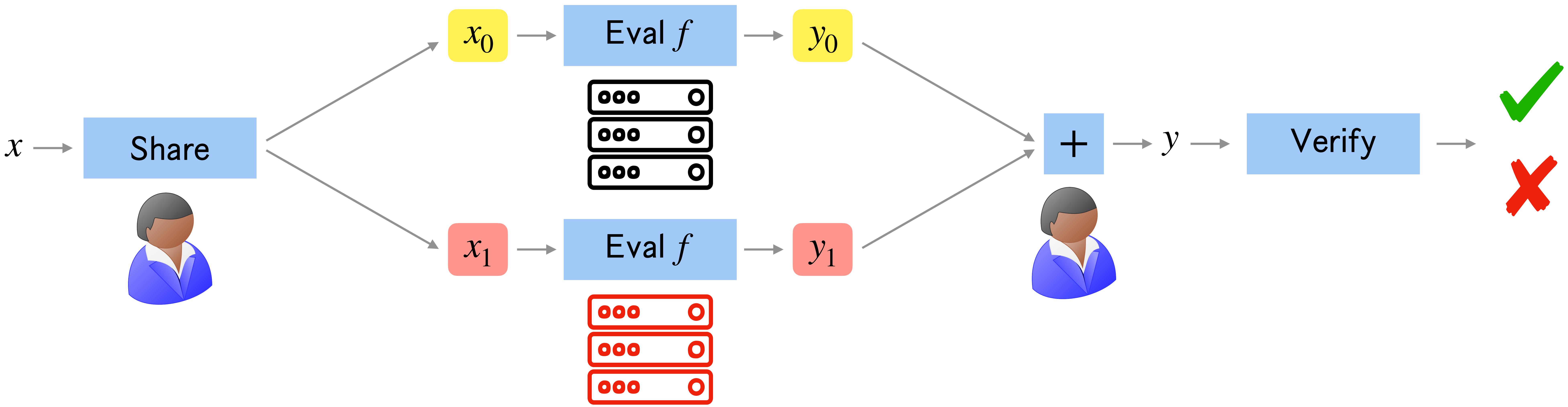


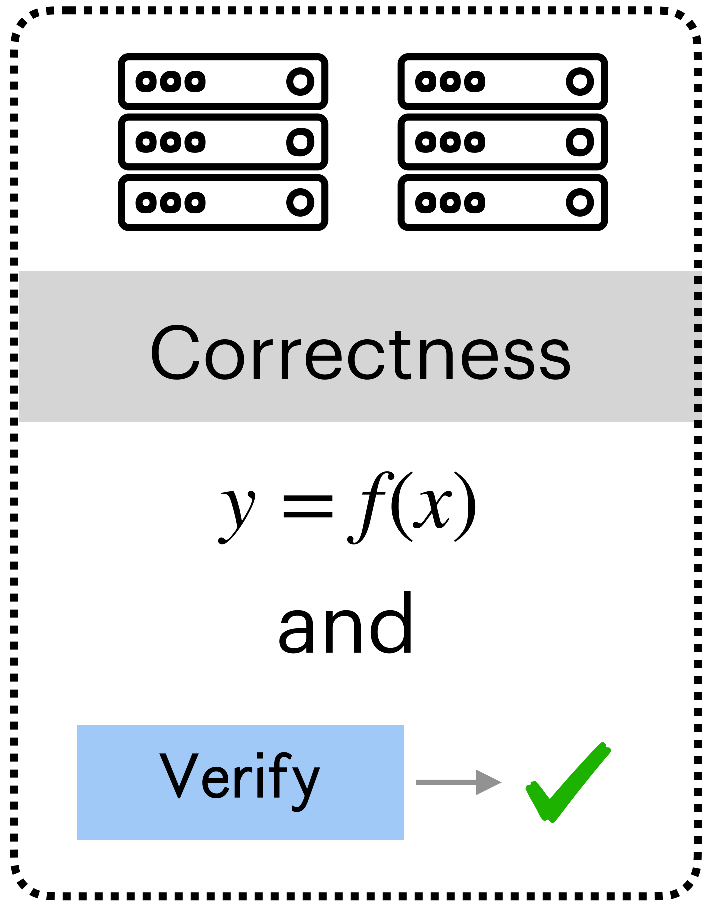



Public Soundness
Verify → ✓
$\exists x_{\text{priv}}$
$\Downarrow$
$y = f(x_{\text{priv}}, x_{\text{pub}})$



HSS with Verifiable Evaluation (ve-HSS)



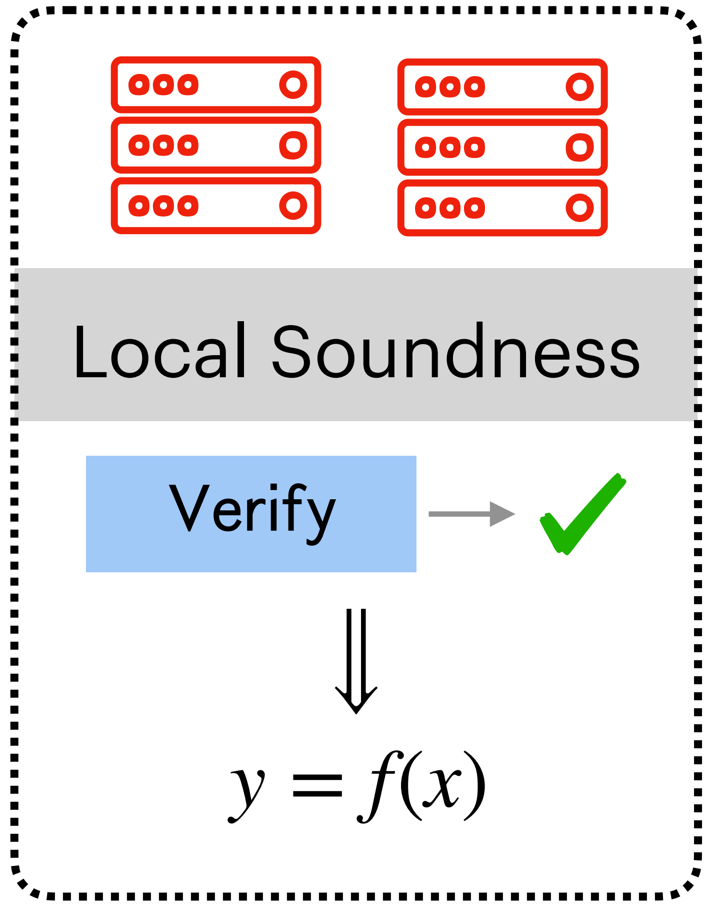


Correctness

$y = f(x)$

and

Verify → ✓

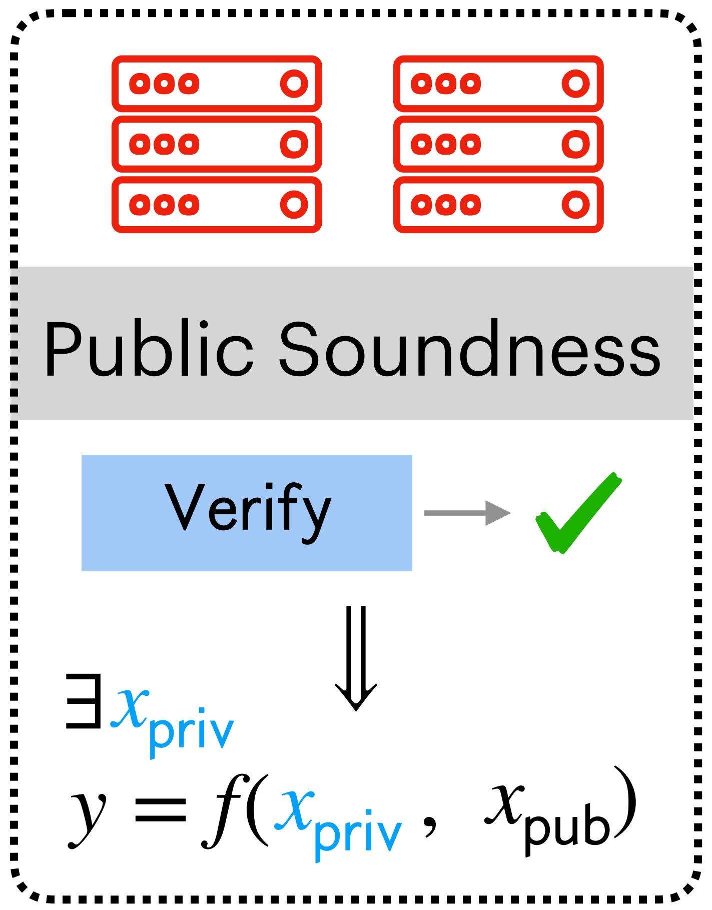


Local Soundness

Verify → ✓

$\Downarrow$

$y = f(x)$

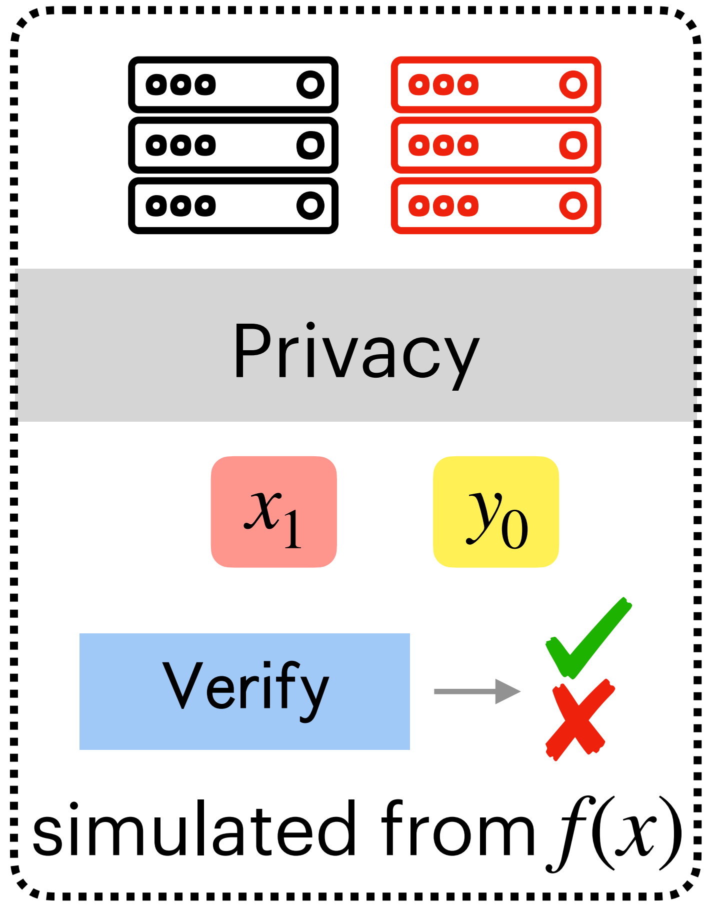


Public Soundness

Verify → ✓

$\exists x_{\text{priv}}$ $\Downarrow$

$y = f(x_{\text{priv}},\ x_{\text{pub}})$

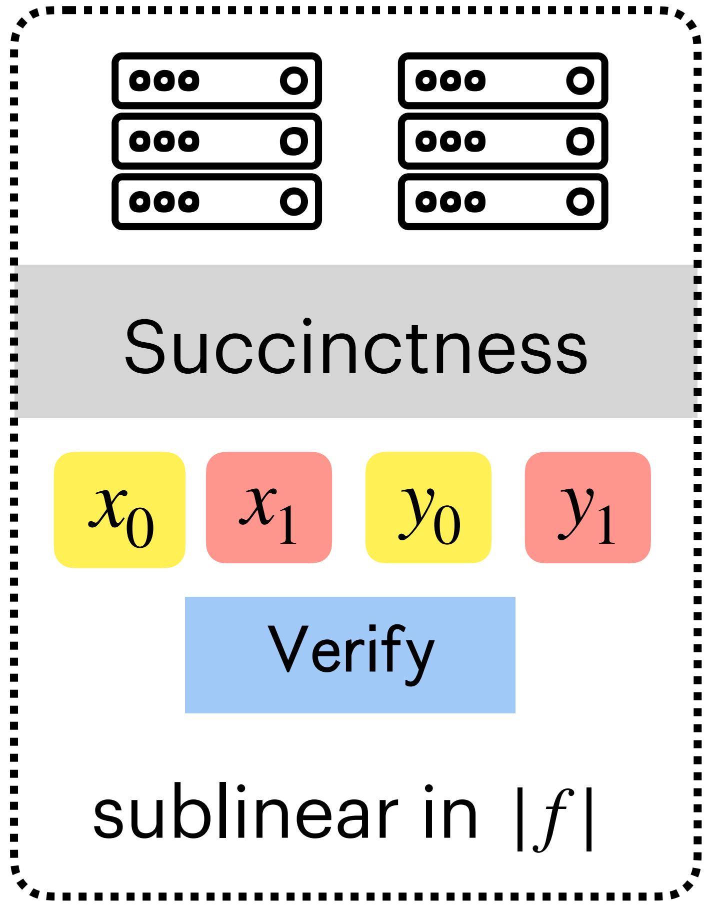


Privacy

x_1 y_0

Verify → ✓ ✗

simulated from $f(x)$



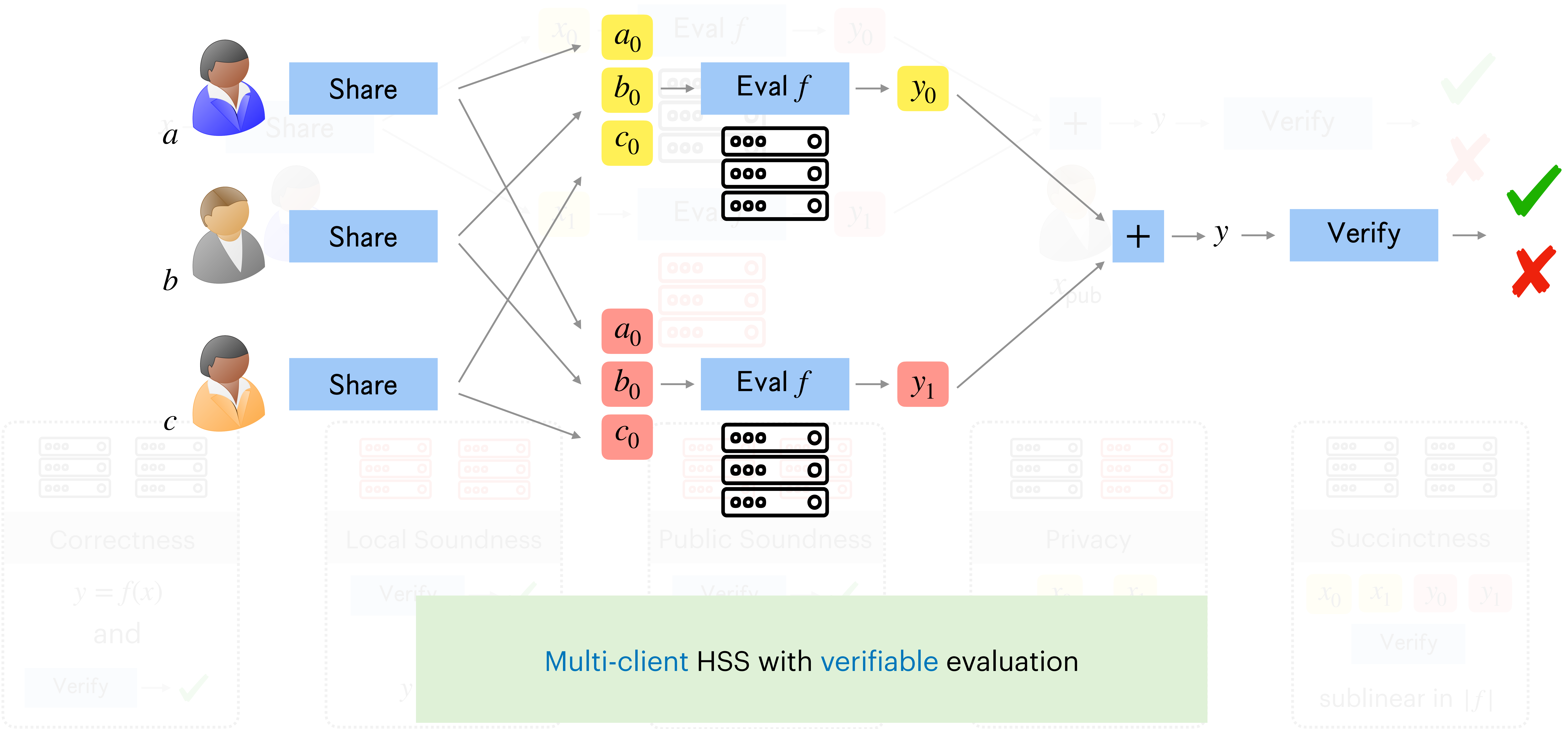
Succinctness

x_0 x_1 y_0 y_1

Verify

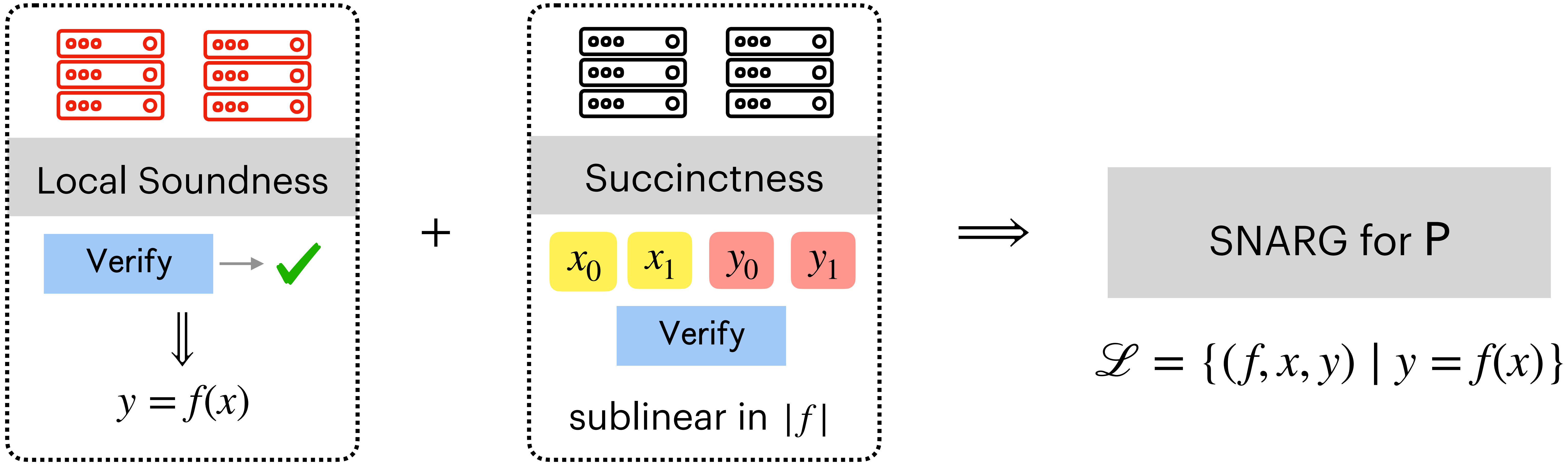
sublinear in $|f|$

HSS with Verifiable Evaluation (ve-HSS)



Multi-client HSS with verifiable evaluation

Implications of HSS with Verifiable Evaluation



Local Soundness

Verify → ✓

$\Downarrow$

$y = f(x)$

+

Succinctness

x_0 x_1 y_0 y_1

Verify

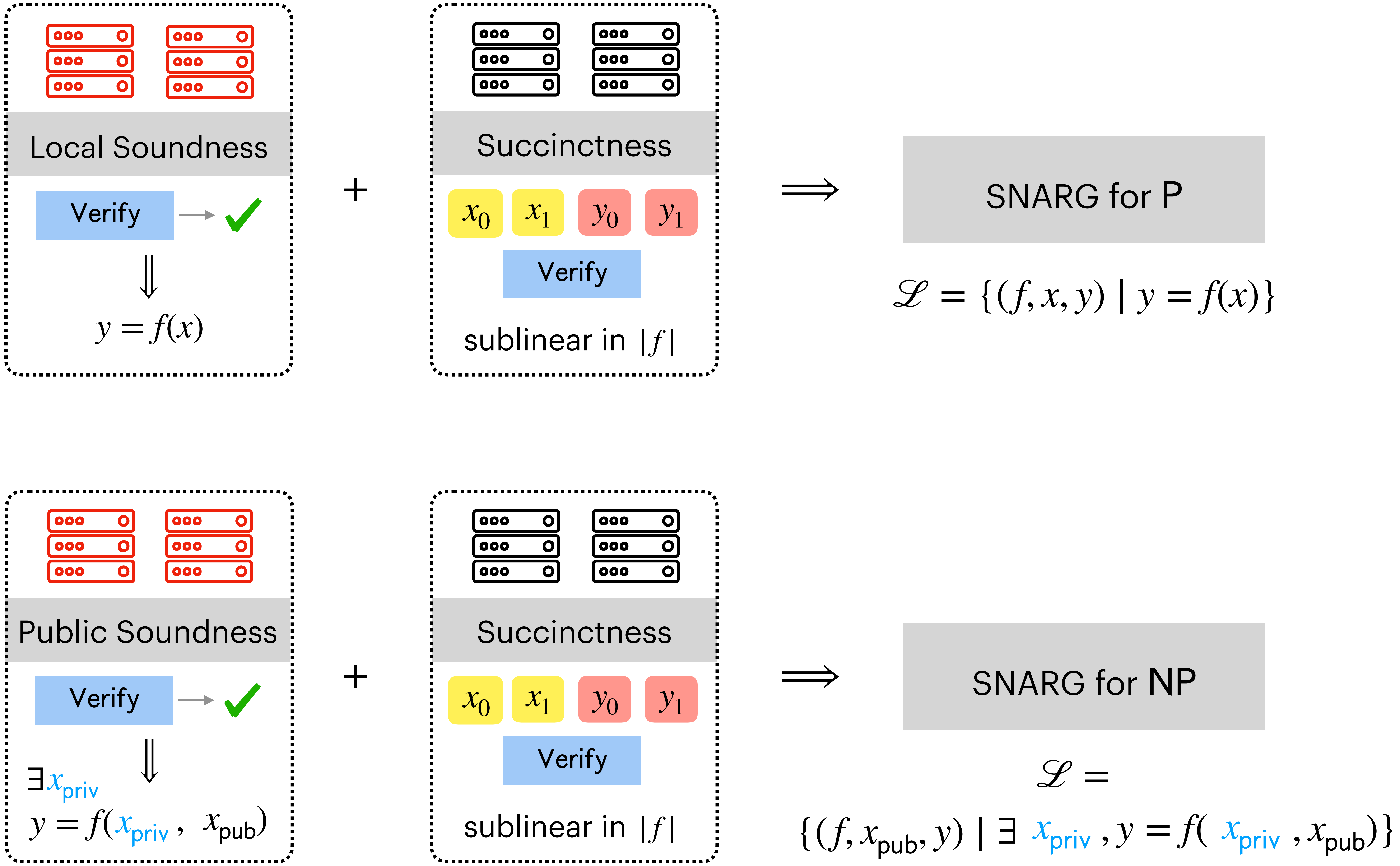
sublinear in $|f|$

$\Longrightarrow$

SNARG for P

$\mathscr{L} = \{(f, x, y) \mid y = f(x)\}$

Implications of HSS with Verifiable Evaluation



Local Soundness

Verify → ✓

$\Downarrow$

$y = f(x)$

+

Succinctness

x_0 x_1 y_0 y_1

Verify

sublinear in $|f|$

$\Longrightarrow$

SNARG for P

$\mathscr{L} = \{(f, x, y) \mid y = f(x)\}$

Public Soundness

Verify → ✓

$\Downarrow$

$\exists x_{\text{priv}}$

$y = f(x_{\text{priv}},\ x_{\text{pub}})$

+

Succinctness

x_0 x_1 y_0 y_1

Verify

sublinear in $|f|$

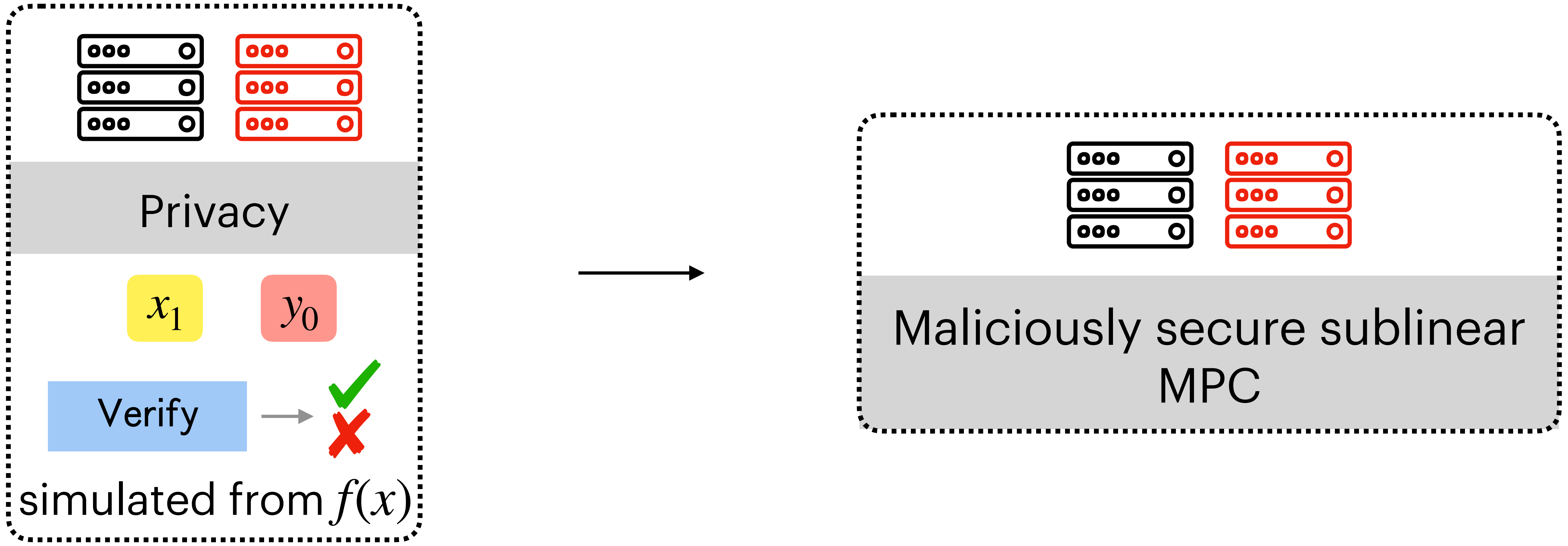
$\Longrightarrow$

SNARG for NP

$\mathscr{L} =$

$\{(f, x_{\text{pub}}, y) \mid \exists\ x_{\text{priv}}\ , y = f(\ x_{\text{priv}}\ , x_{\text{pub}})\}$

Implications of HSS with Verifiable Evaluation



Privacy

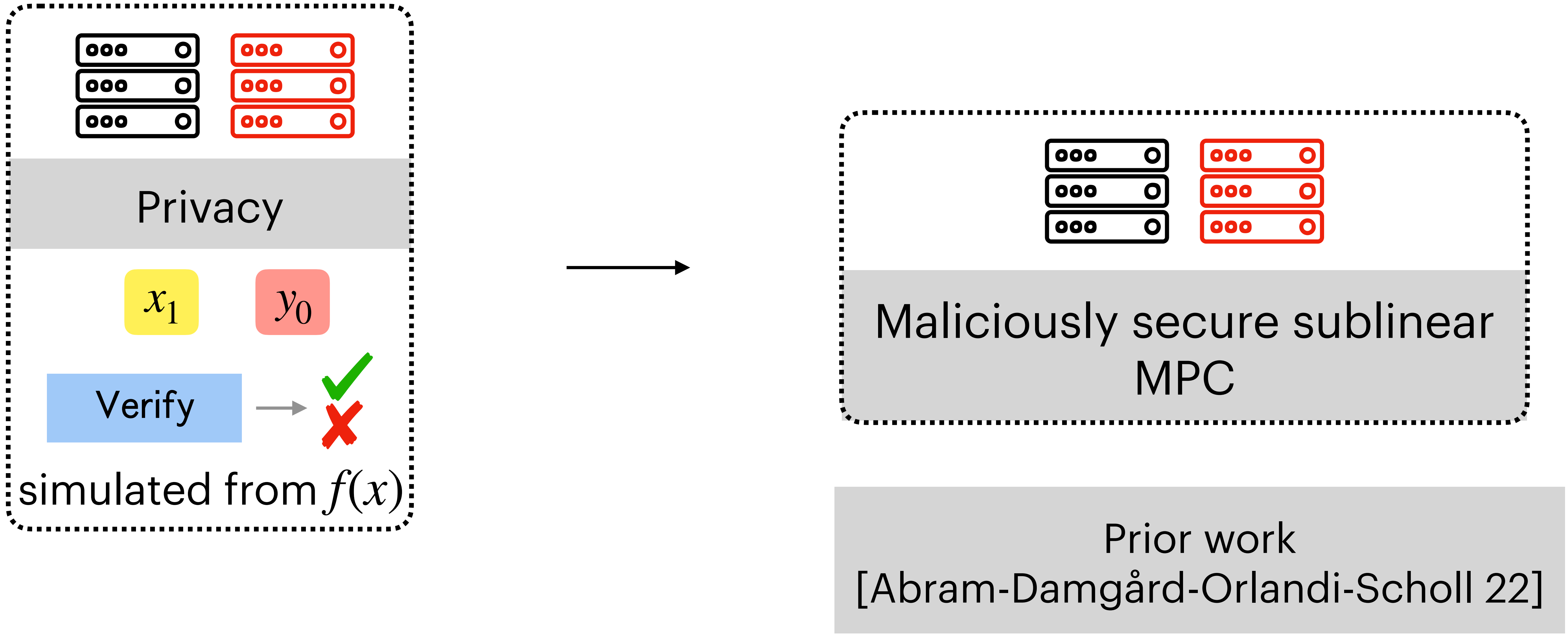
x_1 y_0

Verify → ✓ ✗

simulated from $f(x)$

Maliciously secure sublinear MPC

Implications of HSS with Verifiable Evaluation



Privacy

x_1 y_0

Verify → ✓ ✗

simulated from $f(x)$

Maliciously secure sublinear MPC

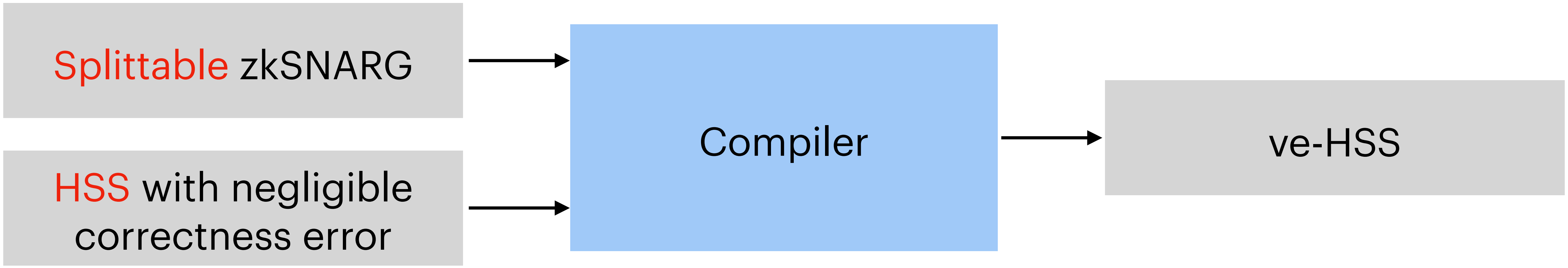
Prior work
[Abram-Damgård-Orlandi-Scholl 22]

Our Results

HSS schemes with verifiable evaluation (ve-HSS) that only make black-box use of cryptography

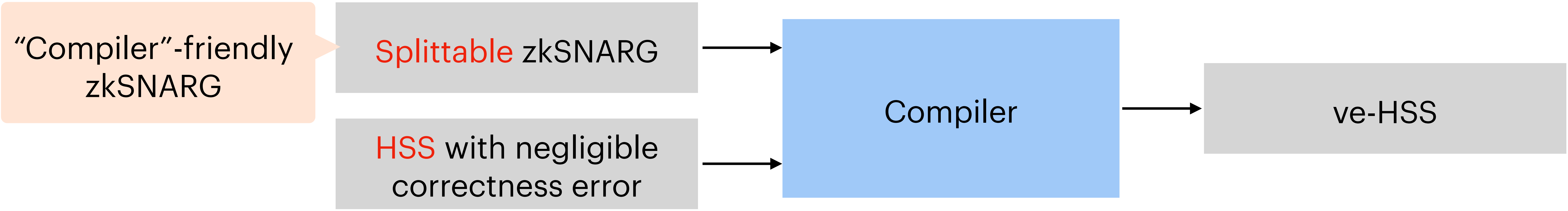
Our Results

HSS schemes with verifiable evaluation (ve-HSS) that only make black-box use of cryptography



Our Results

HSS schemes with verifiable evaluation (ve-HSS) that only make black-box use of cryptography



"Compiler"-friendly zkSNARG

Splittable zkSNARG

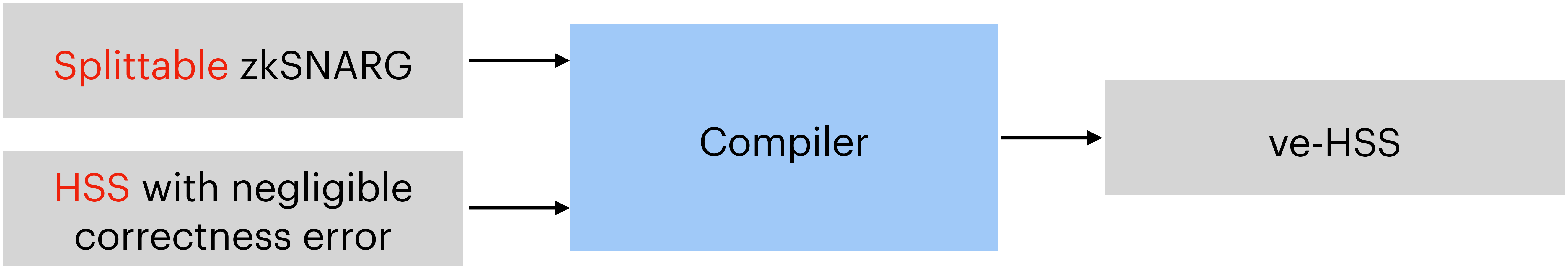
HSS with negligible correctness error

Compiler

ve-HSS

Our Results

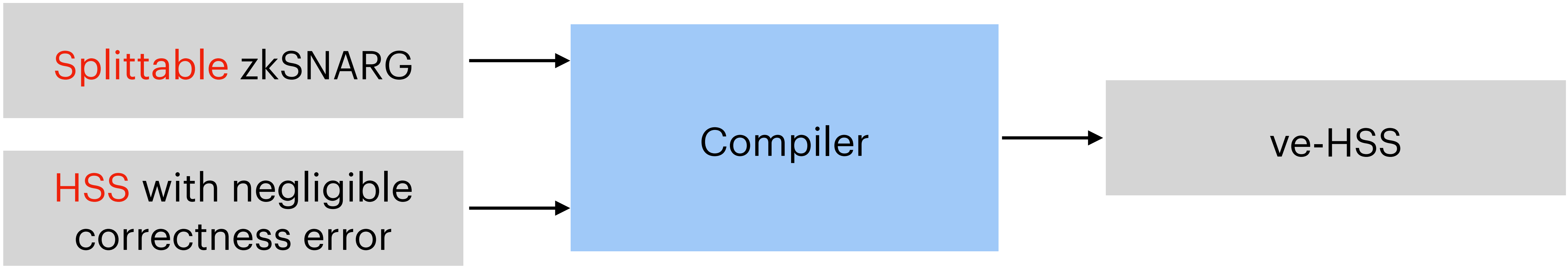
HSS schemes with verifiable evaluation (ve-HSS) that only make black-box use of cryptography



Splittable zkSNARG	HSS	Function Class
Generic Bilinear Group Model [Groth 16]	DCR [Orlandi-Scholl-Yakoubov 21] [Roy-Singh 21] Class Groups [Abram-Damgård-Orlandi-Scholl 22] LWE [Boyle-Kohl-Scholl 19]	NC^1
	FHE [Dodis-Halevi-Rothblum-Wichs 16] [Chilloti-Orsini-Scholl-Smart-Leeuwen 22] iO + OWF [Boyle-Gilboa-Ishai 15]	P/poly

Our Results

HSS schemes with verifiable evaluation (ve-HSS) that only make black-box use of cryptography



HSS	Function Class
DCR [Orlandi-Scholl-Yakoubov 21] [Roy-Singh 21] Class Groups [Abram-Damgård-Orlandi-Scholl 22] LWE [Boyle-Kohl-Scholl 19]	SIMD NC^1
FHE [Dodis-Halevi-Rothblum-Wichs 16] [Chilloti-Orsini-Scholl-Smart-Leeuwen 22] iO + OWF [Boyle-Gilboa-Ishai 15]	SIMD P/poly

Splittable zkSNARG

Subgroup Decision Assumption

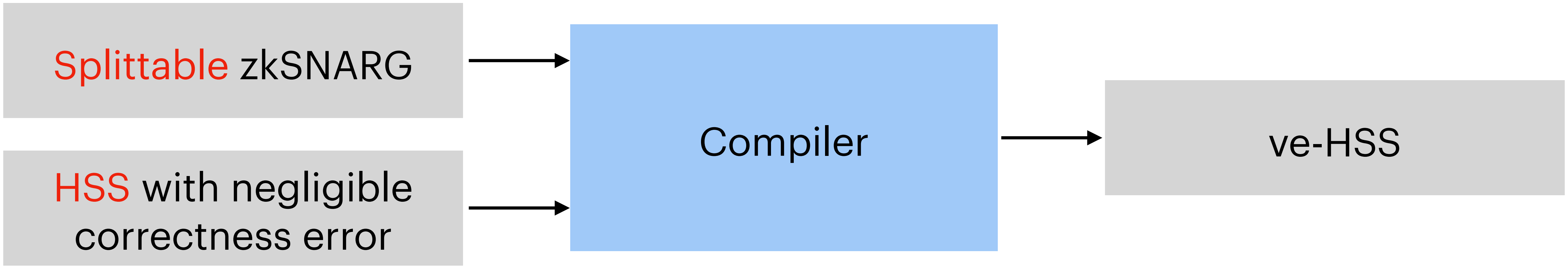
[Waters-Wu 22]

BARG → zkBARG

Black-box in cryptography

Our Results

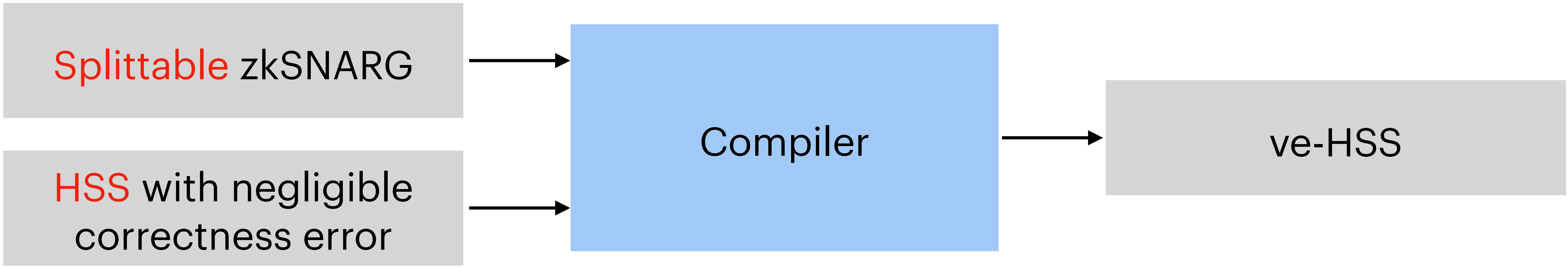
HSS schemes with verifiable evaluation (ve-HSS) that only make black-box use of cryptography



Multi-client HSS schemes with verifiable evaluation that only make black-box use of cryptography

Our Results

HSS schemes with verifiable evaluation (ve-HSS) that only make black-box use of cryptography



Multi-client HSS schemes with verifiable evaluation that only make black-box use of cryptography

Applications

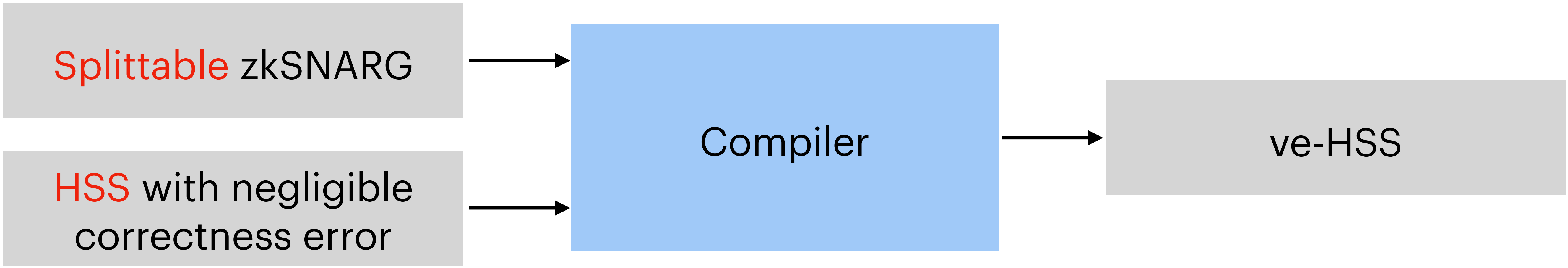
Private and verifiable delegation of computation

Private delegation of zkSNARG computation

Black-box in cryptography!

Our Results

HSS schemes with verifiable evaluation (ve-HSS) that only make black-box use of cryptography



Splittable zkSNARG

HSS with negligible correctness error

Compiler

ve-HSS

Multi-client HSS schemes with verifiable evaluation that only make black-box use of cryptography

Applications

Private and verifiable delegation of computation

Private delegation of zkSNARG computation

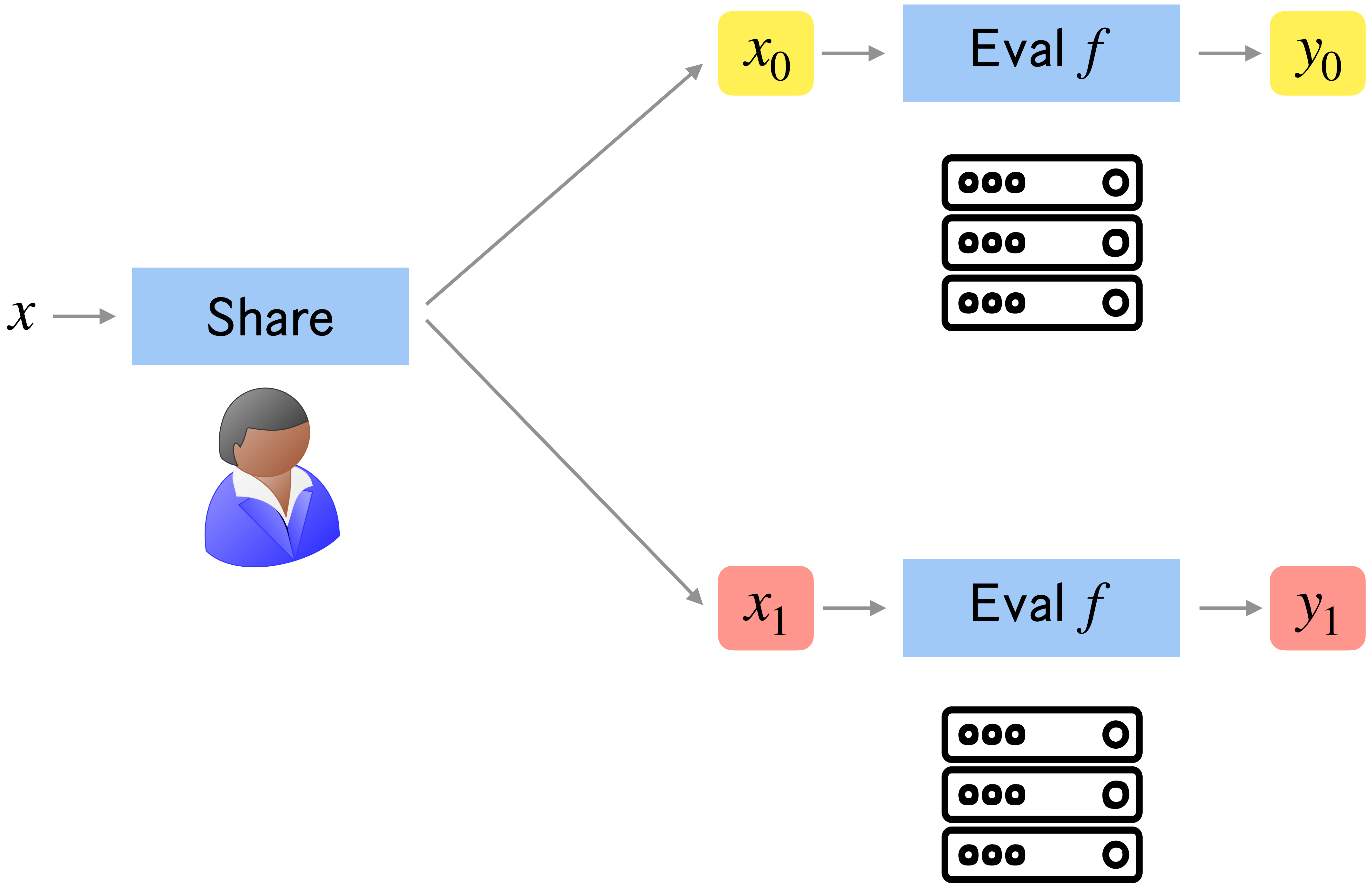
Black-box in cryptography!

Strawman Approach

[Goldreich-Micali-Wigderson 87] Paradigm

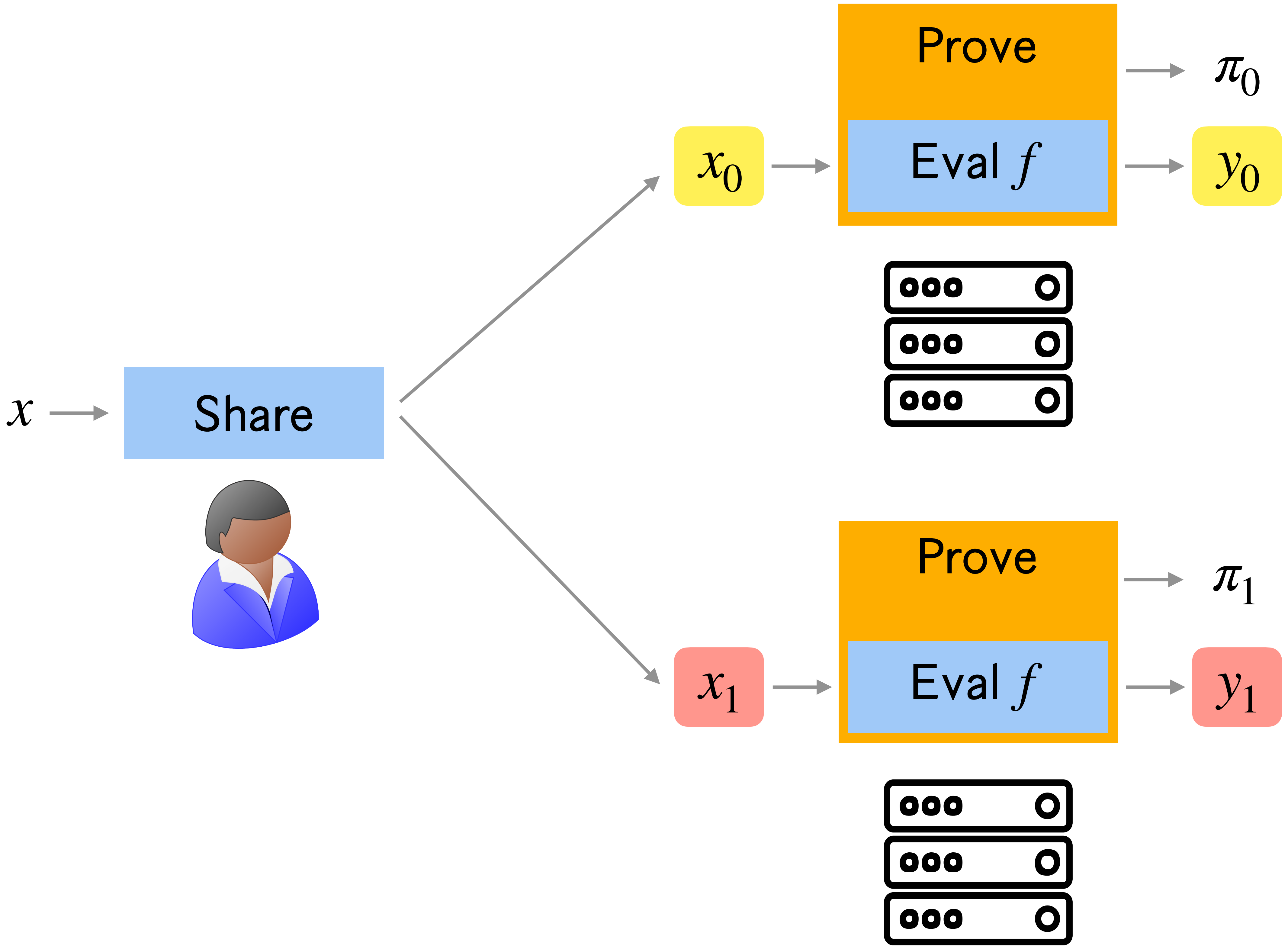
Strawman Approach

[Goldreich-Micali-Wigderson 87] Paradigm



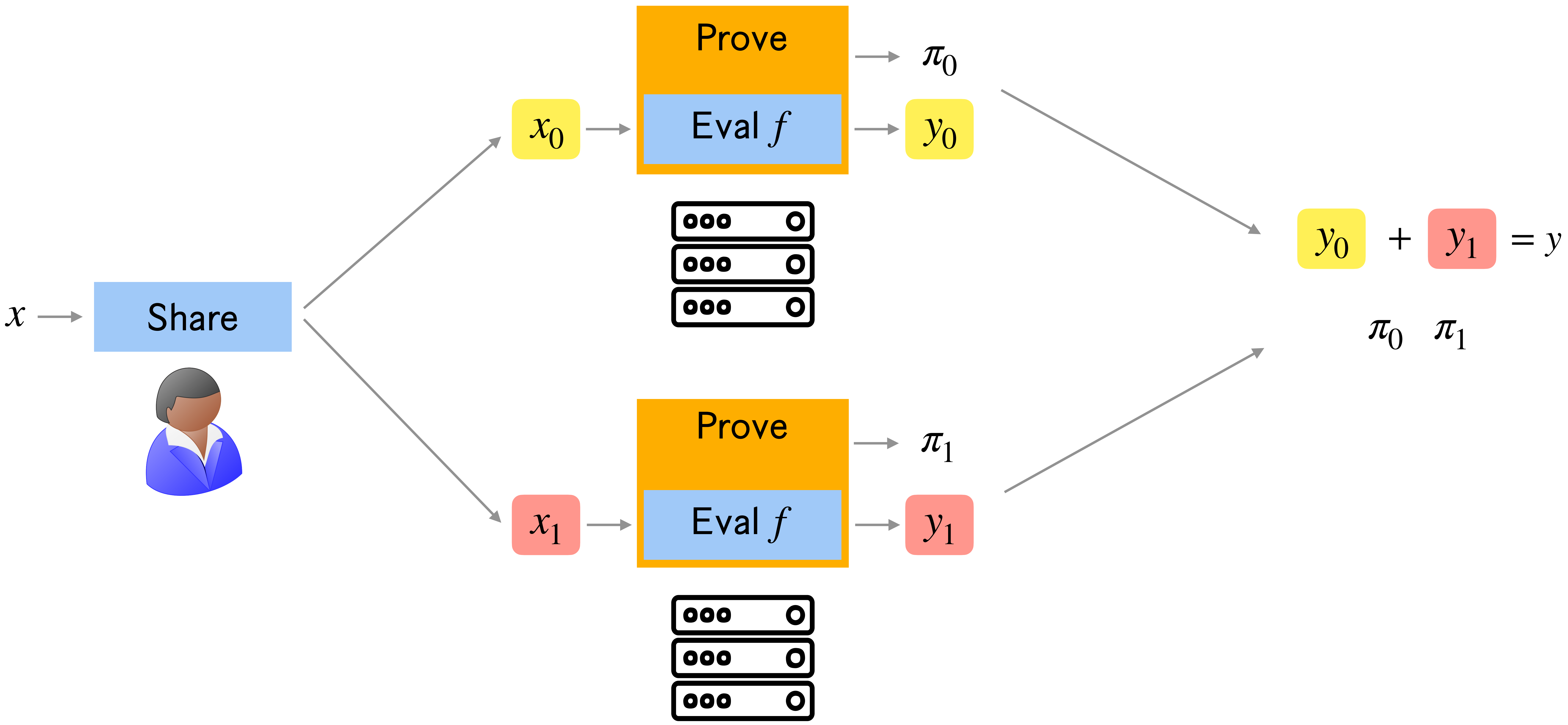
Strawman Approach

[Goldreich-Micali-Wigderson 87] Paradigm



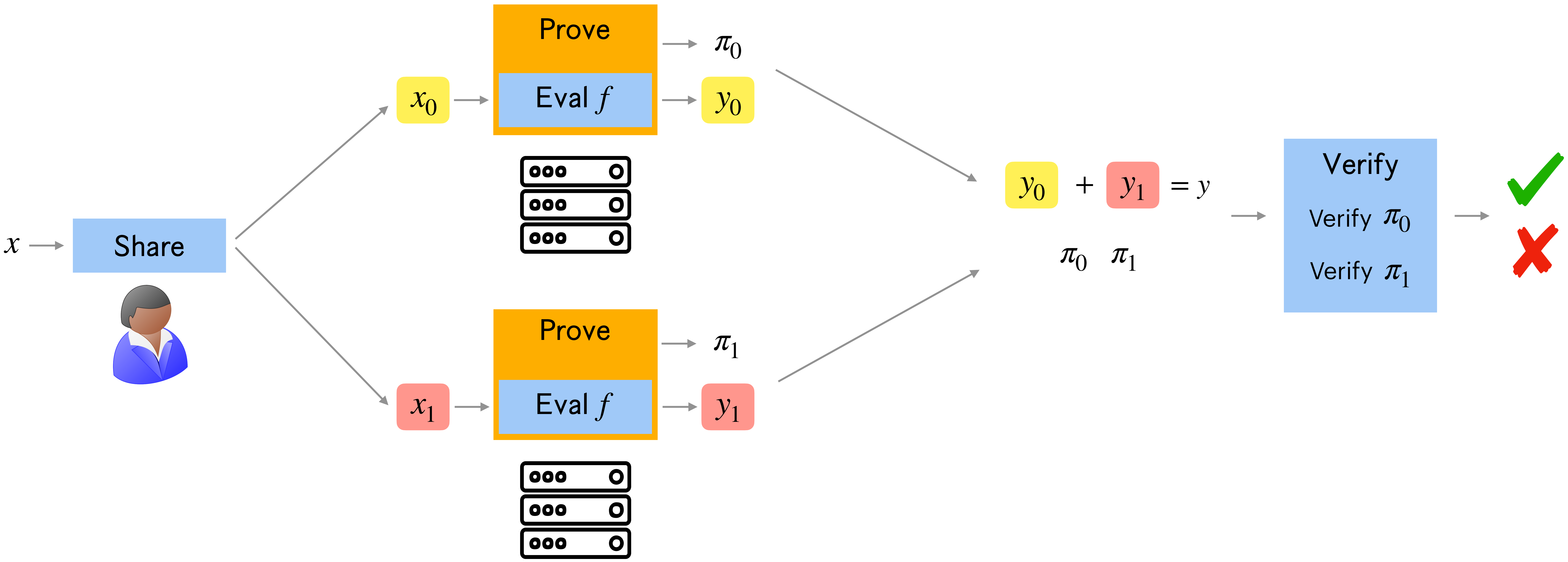
Strawman Approach

[Goldreich-Micali-Wigderson 87] Paradigm



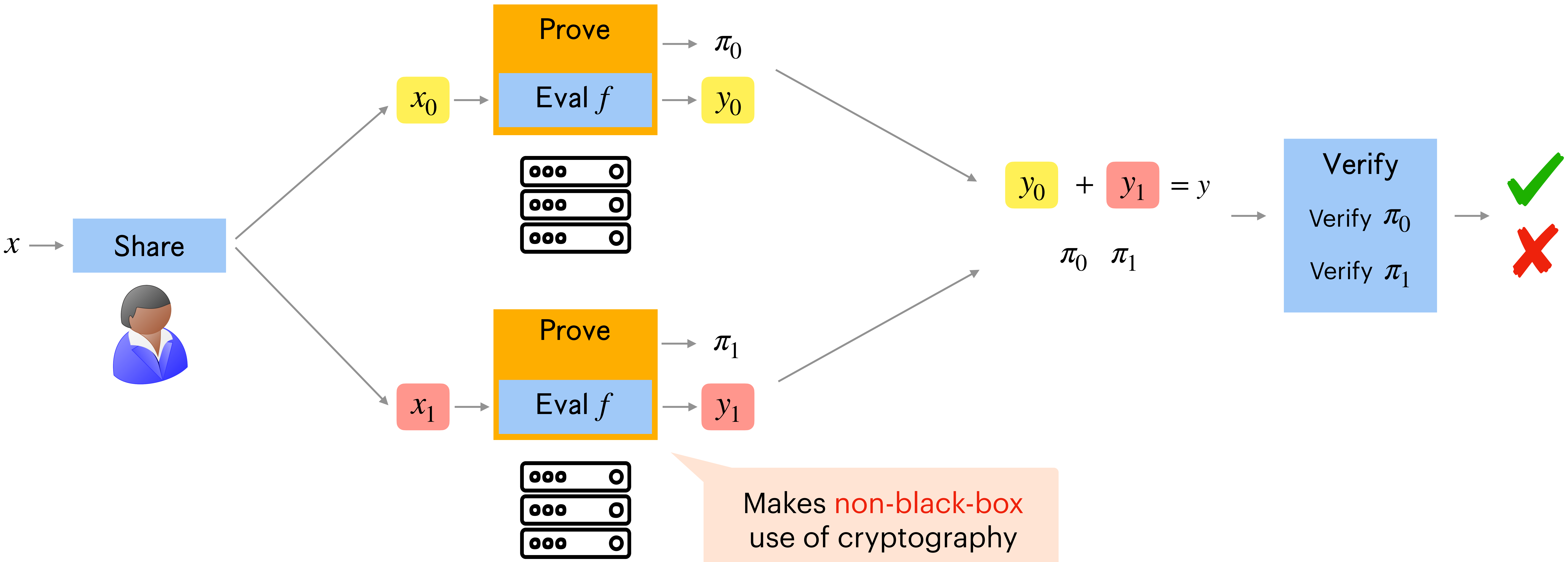
Strawman Approach

[Goldreich-Micali-Wigderson 87] Paradigm



Strawman Approach

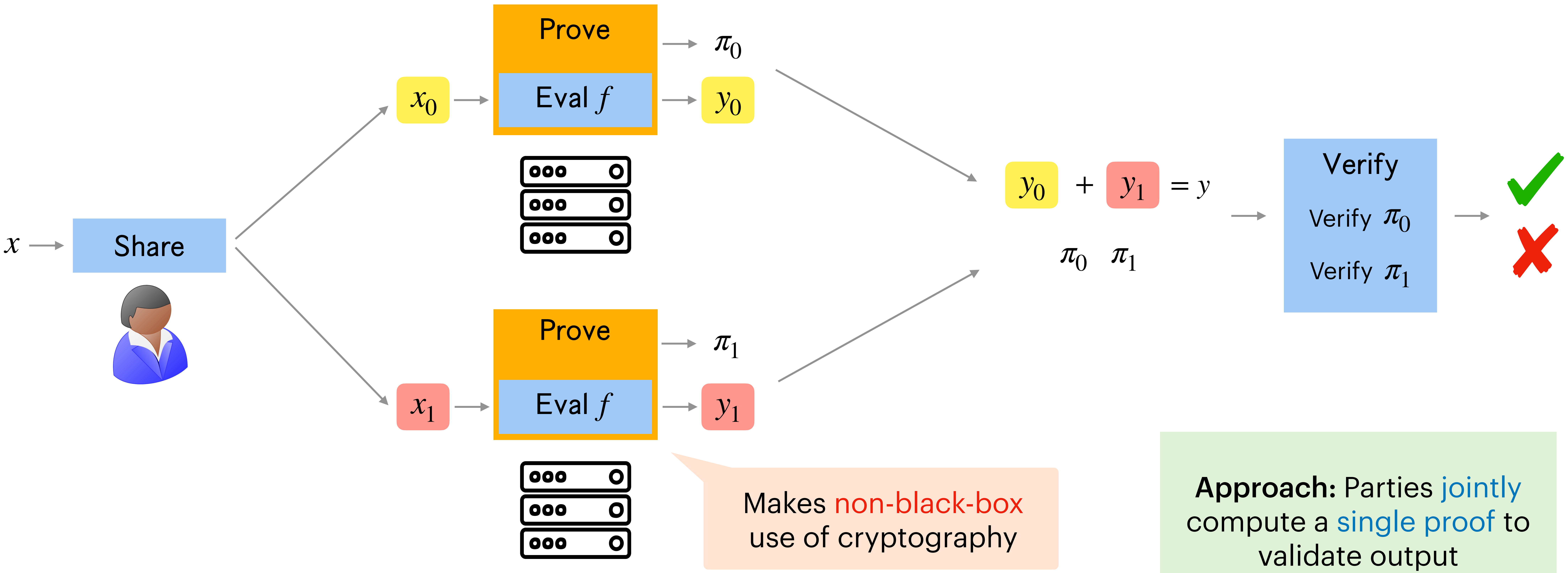
[Goldreich-Micali-Wigderson 87] Paradigm



Makes non-black-box use of cryptography

Strawman Approach

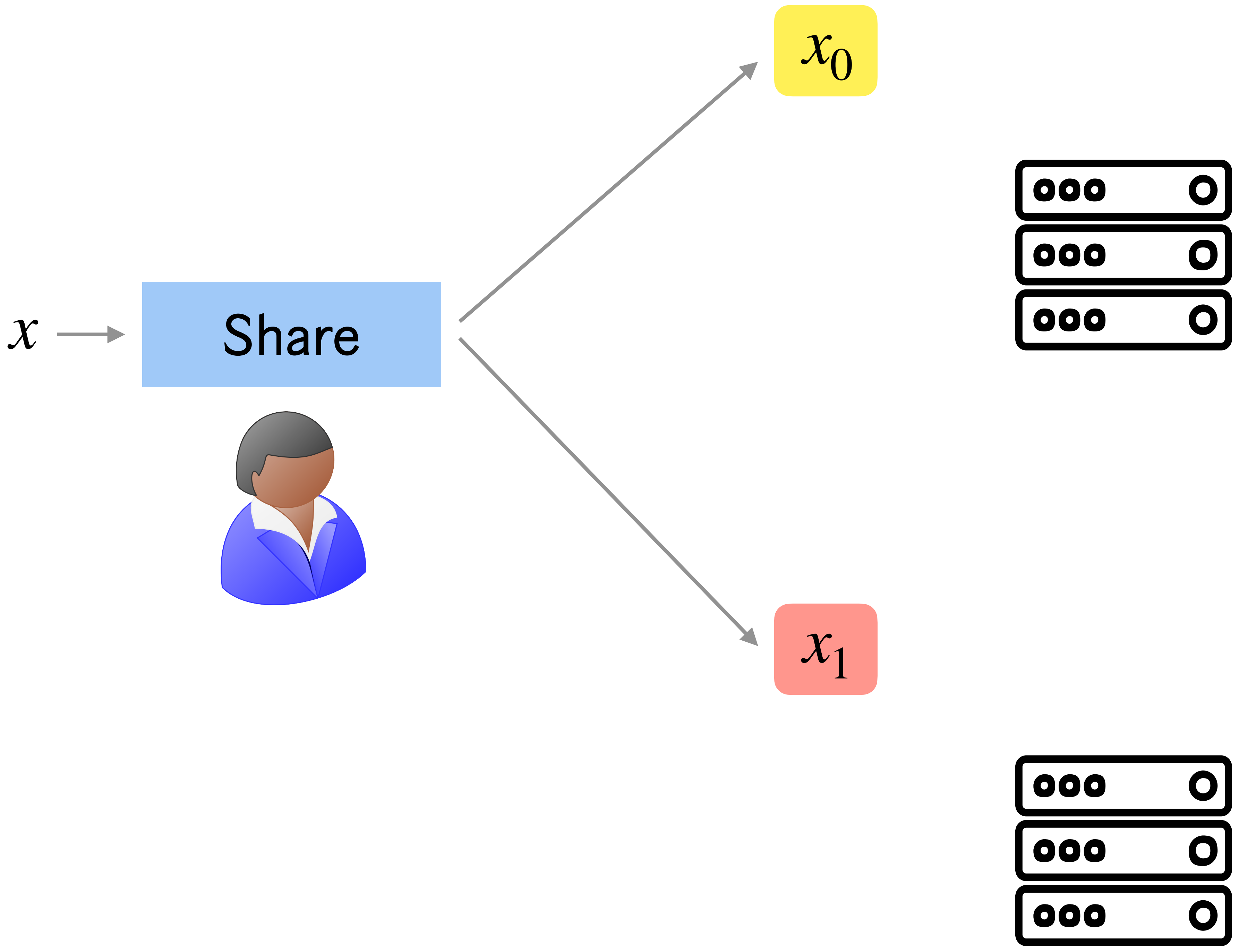
[Goldreich-Micali-Wigderson 87] Paradigm



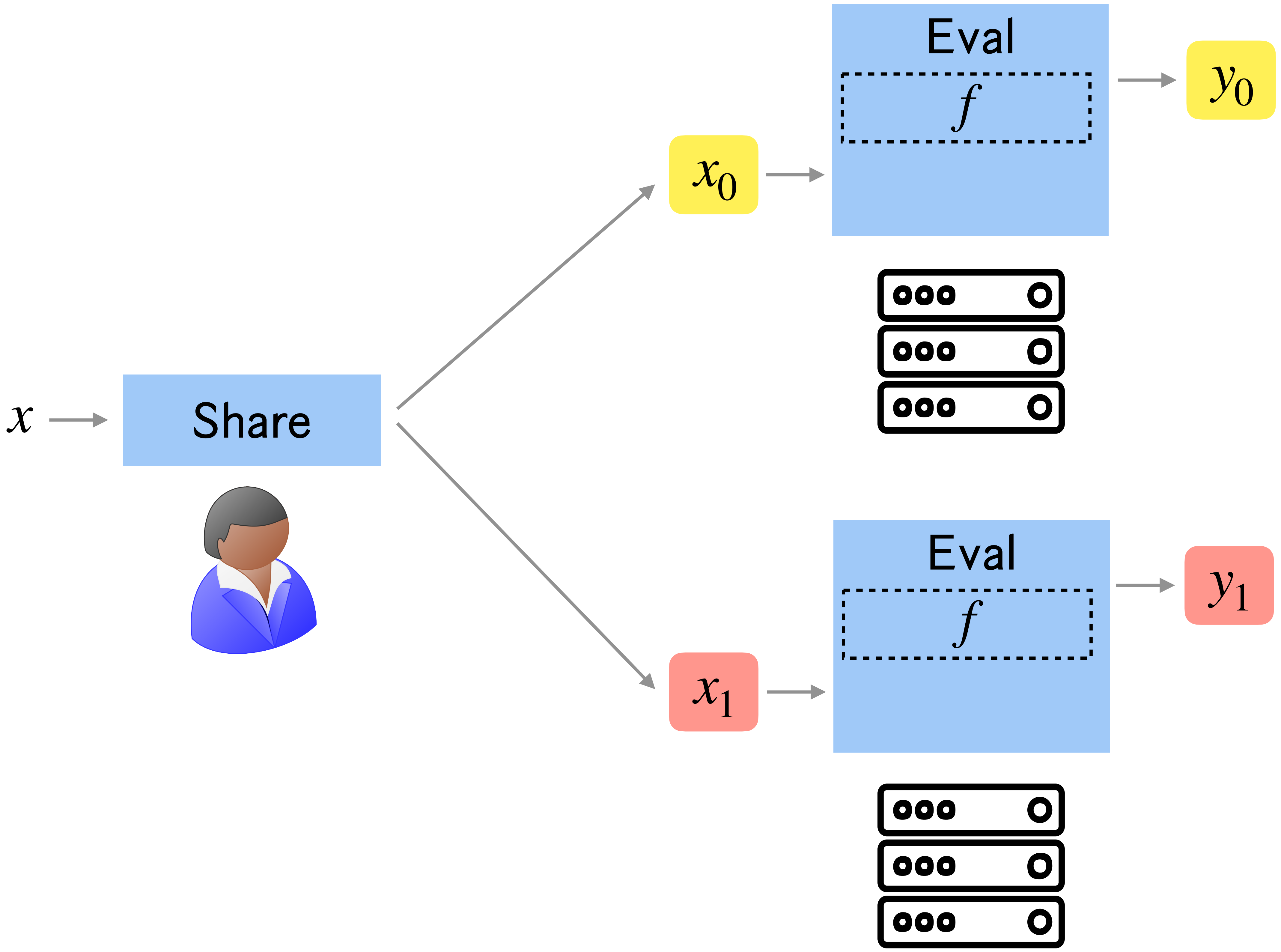
Makes non-black-box use of cryptography

Approach: Parties jointly compute a single proof to validate output

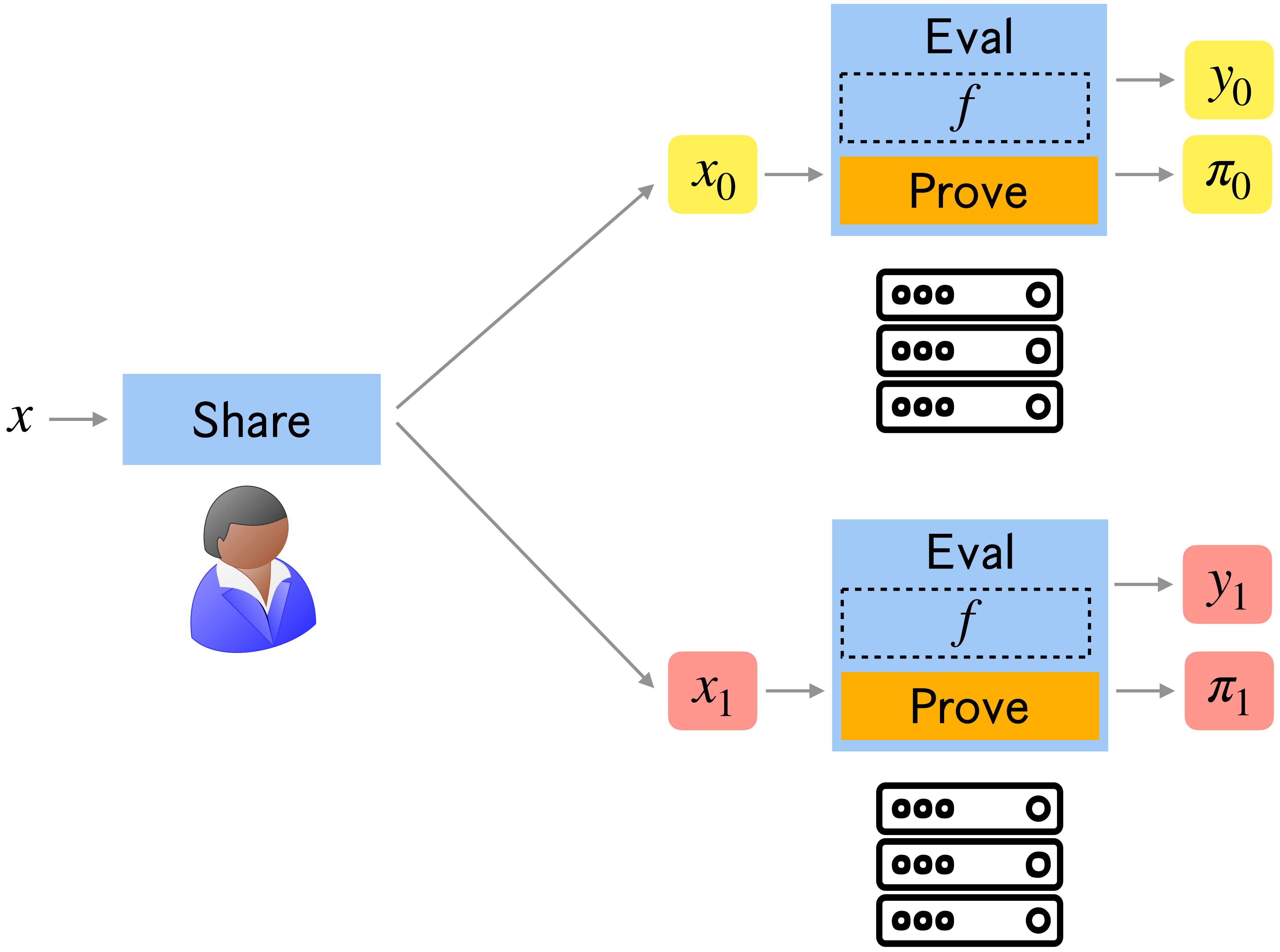
Jointly Computing A Proof



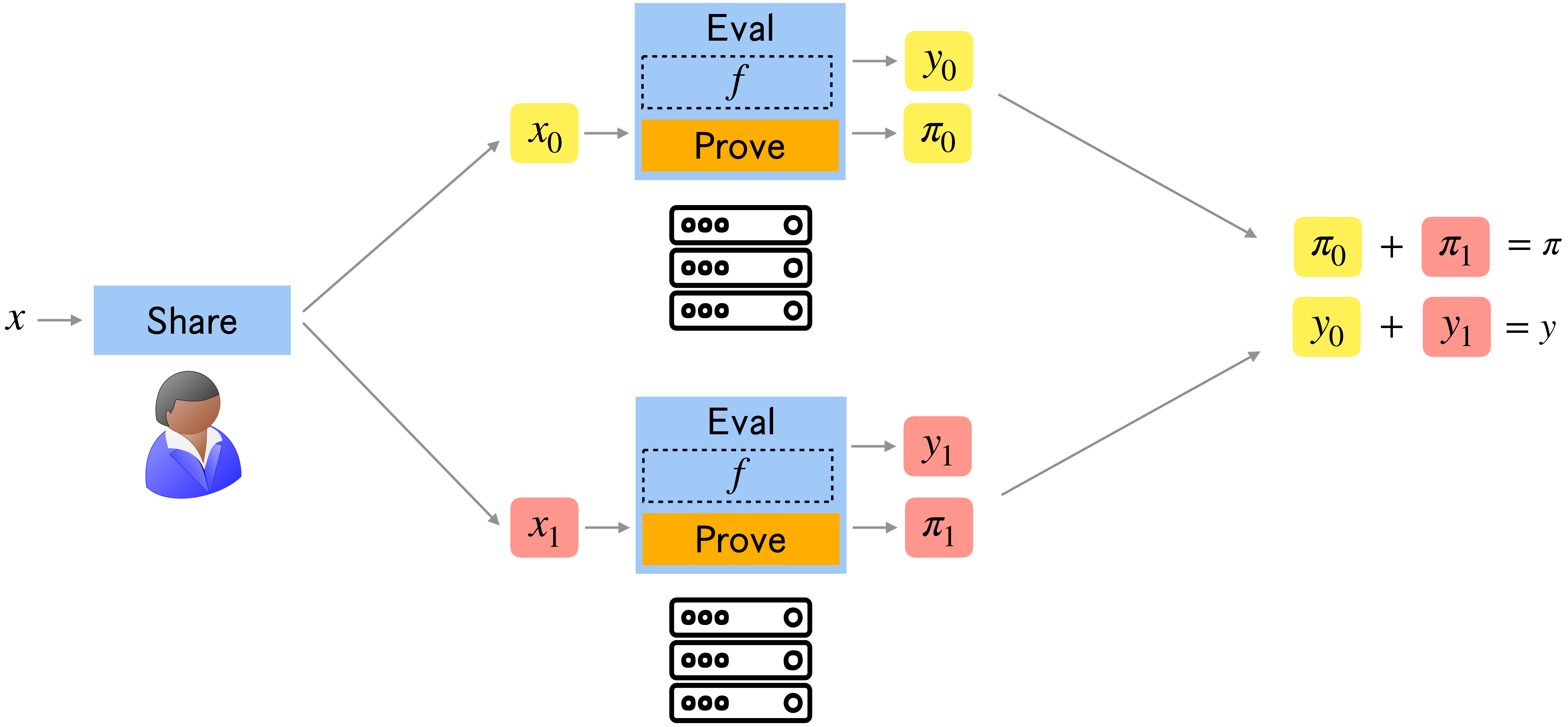
Jointly Computing A Proof



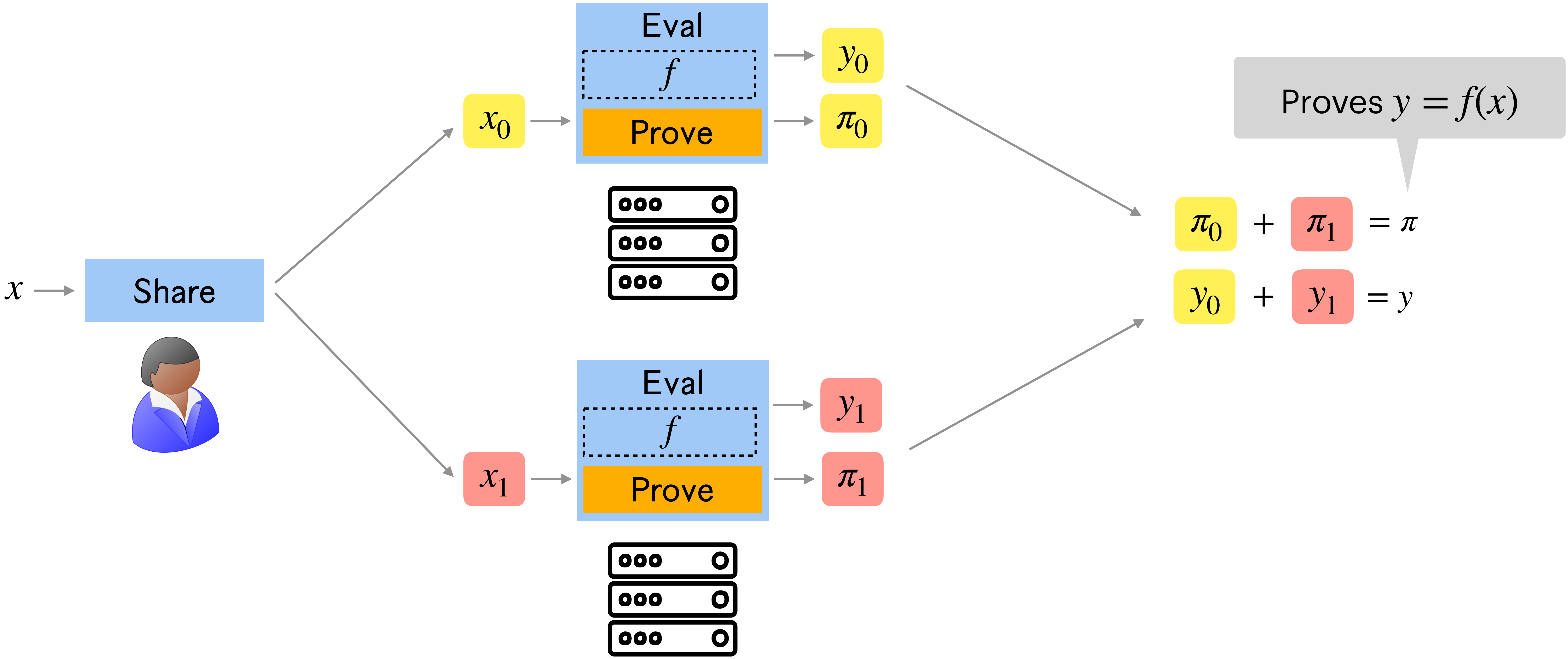
Jointly Computing A Proof



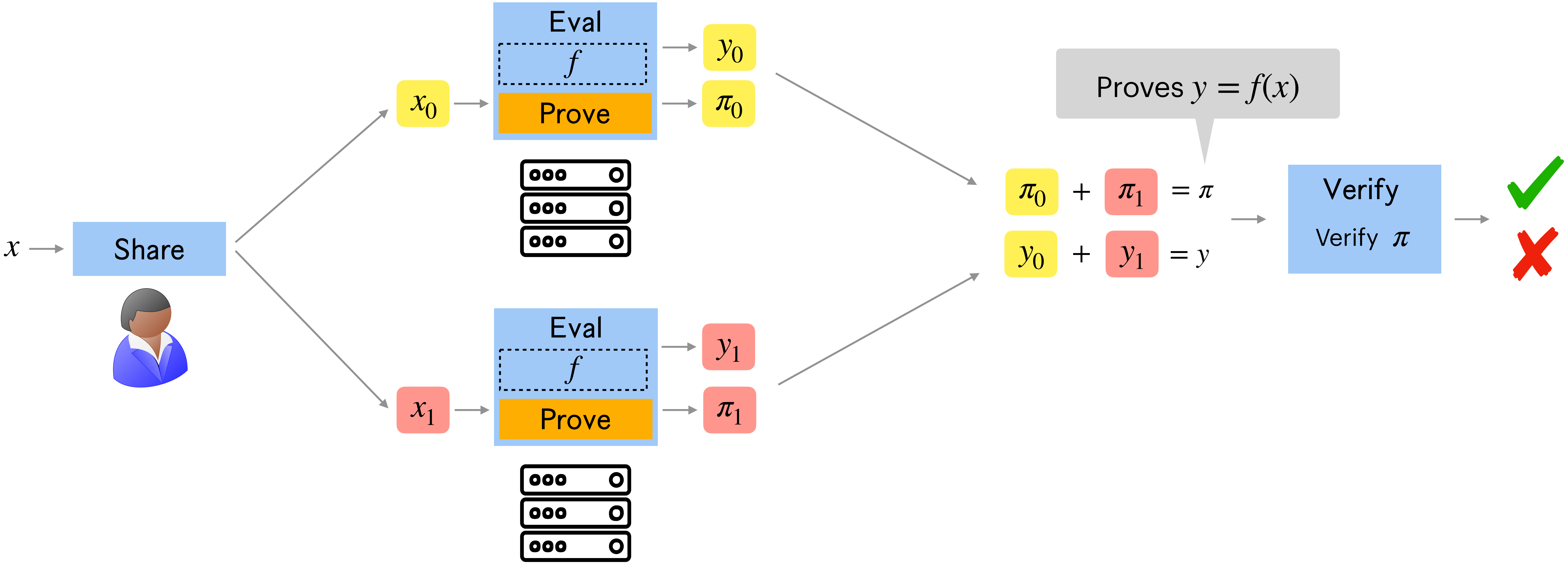
Jointly Computing A Proof



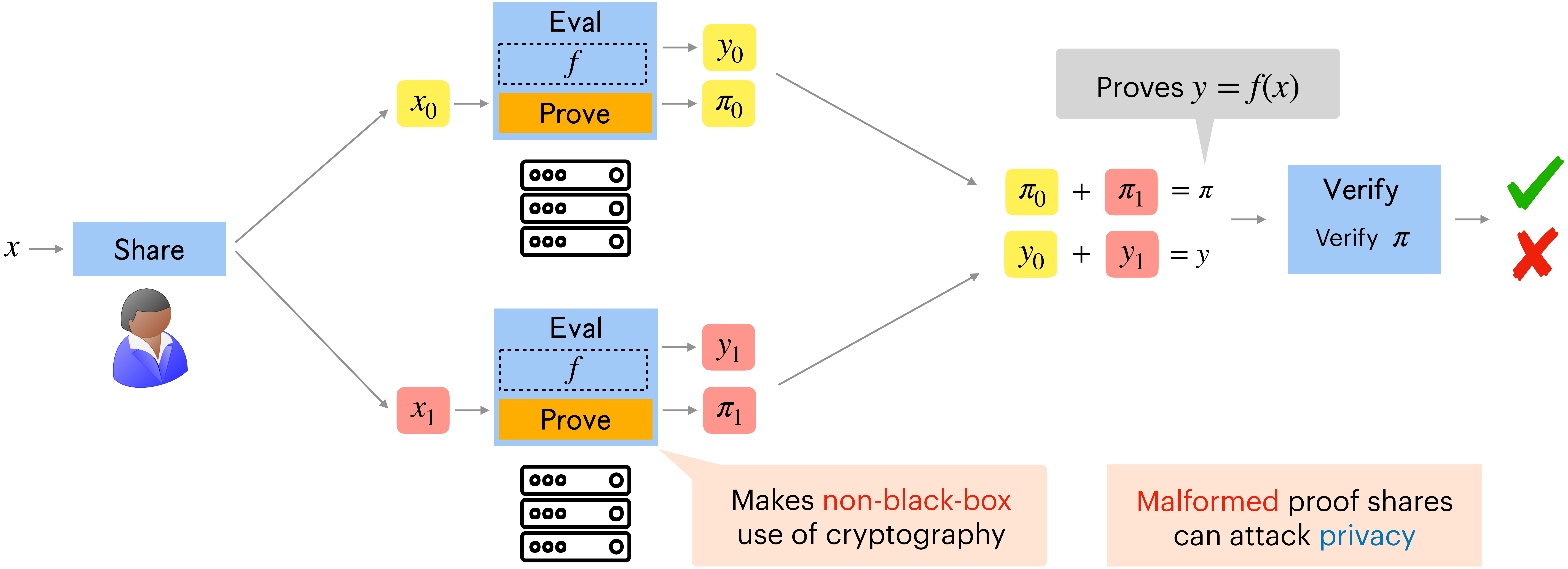
Jointly Computing A Proof



Jointly Computing A Proof



Jointly Computing A Proof

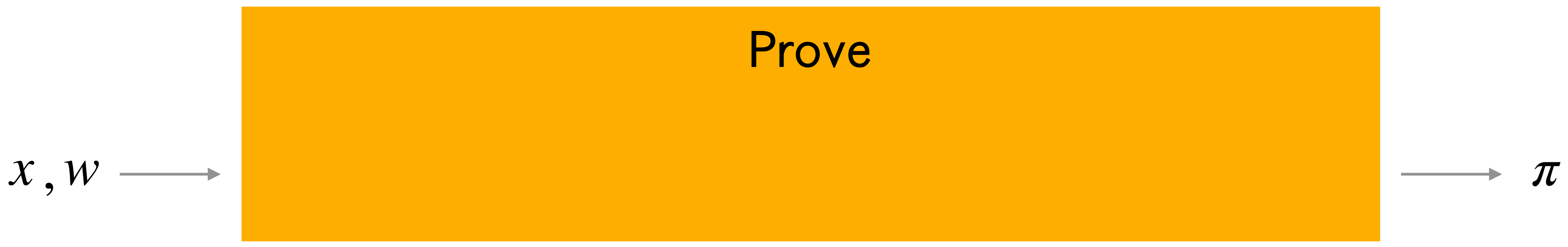


Proves $y = f(x)$

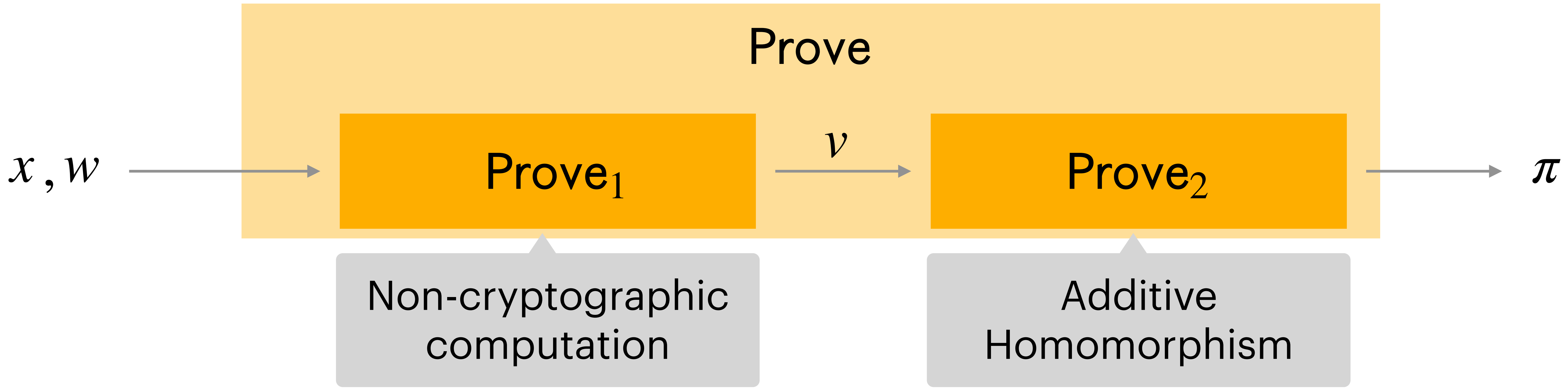
Makes non-black-box use of cryptography

Malformed proof shares can attack privacy

Splittable zkSNARG



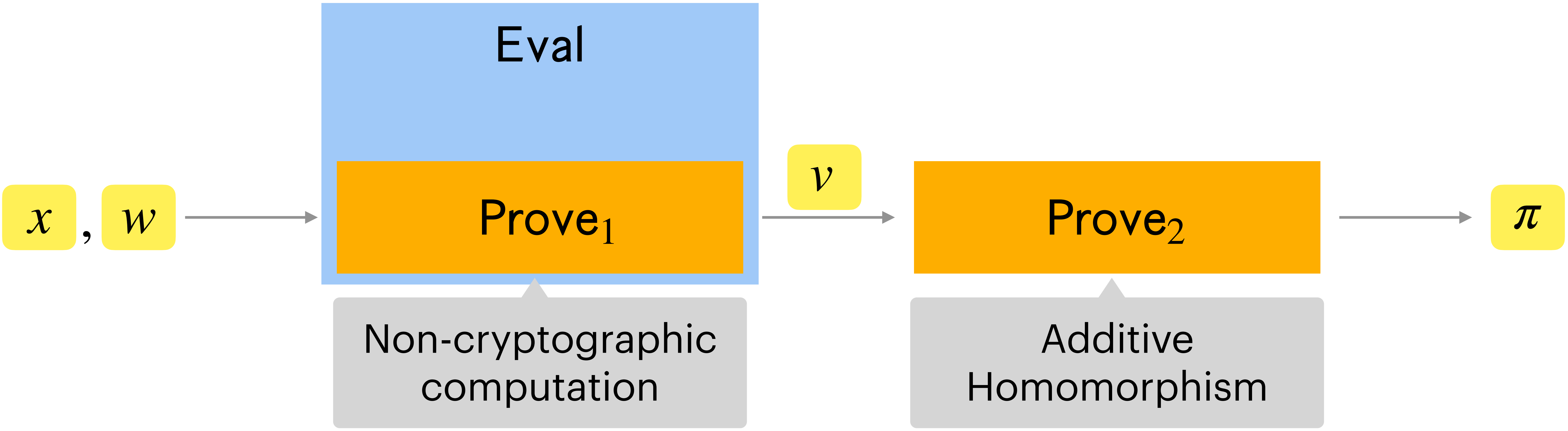
Splittable zkSNARG



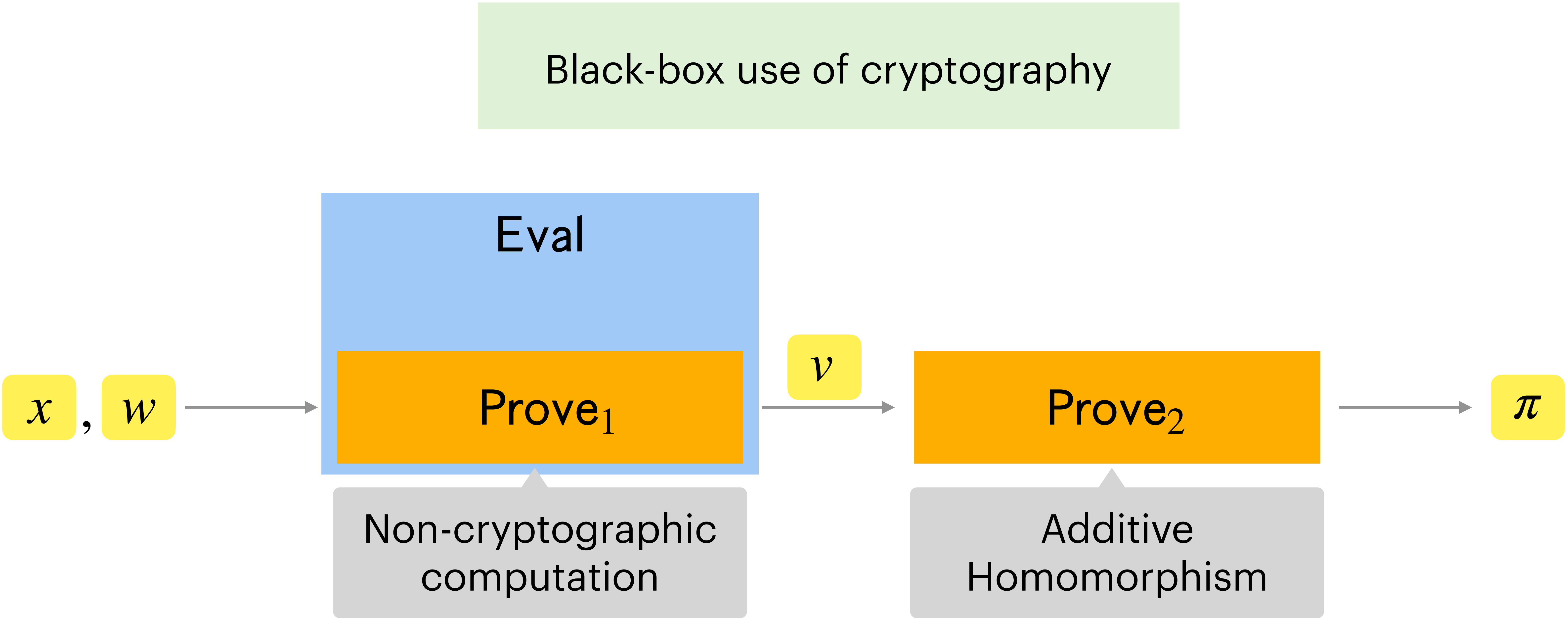
Non-cryptographic computation

Additive Homomorphism

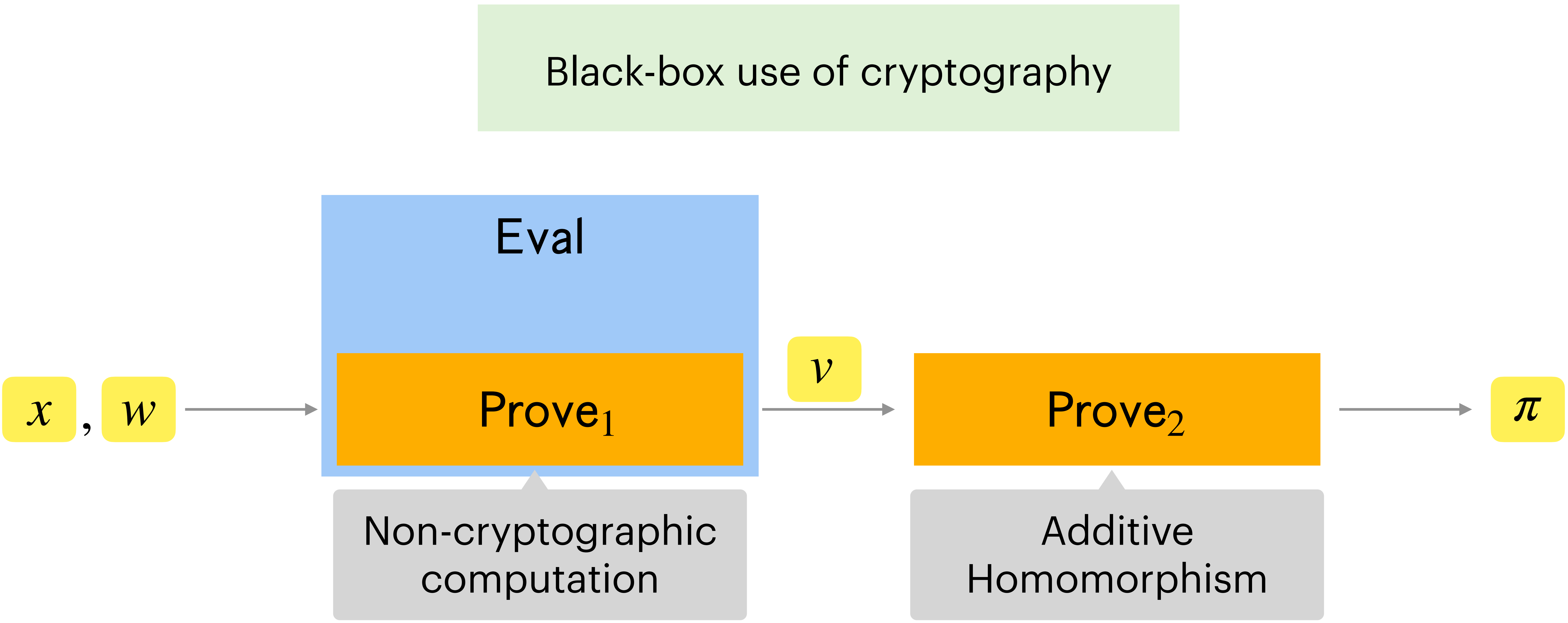
Splittable zkSNARG



Splittable zkSNARG



Splittable zkSNARG



Black-box use of cryptography

Eval

x, w → Prove$_1$ → v → Prove$_2$ → π

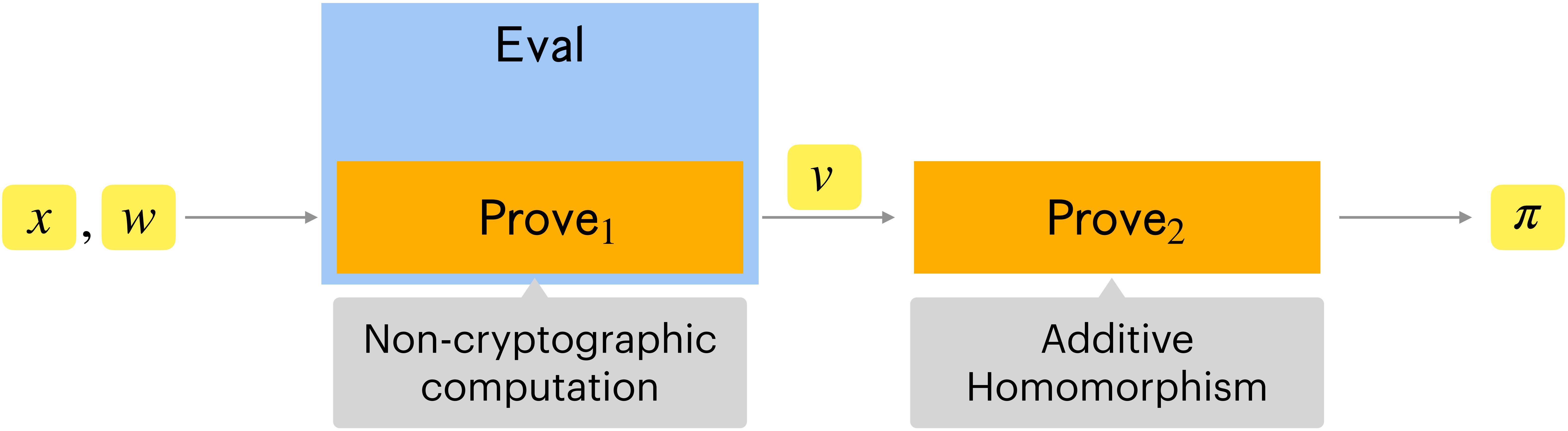
Non-cryptographic computation

Additive Homomorphism

Eval supports a limited class of functions $\Longrightarrow$ Prove$_1$ must be "simple" to compute (low depth circuit)

Splittable zkSNARG

Black-box use of cryptography

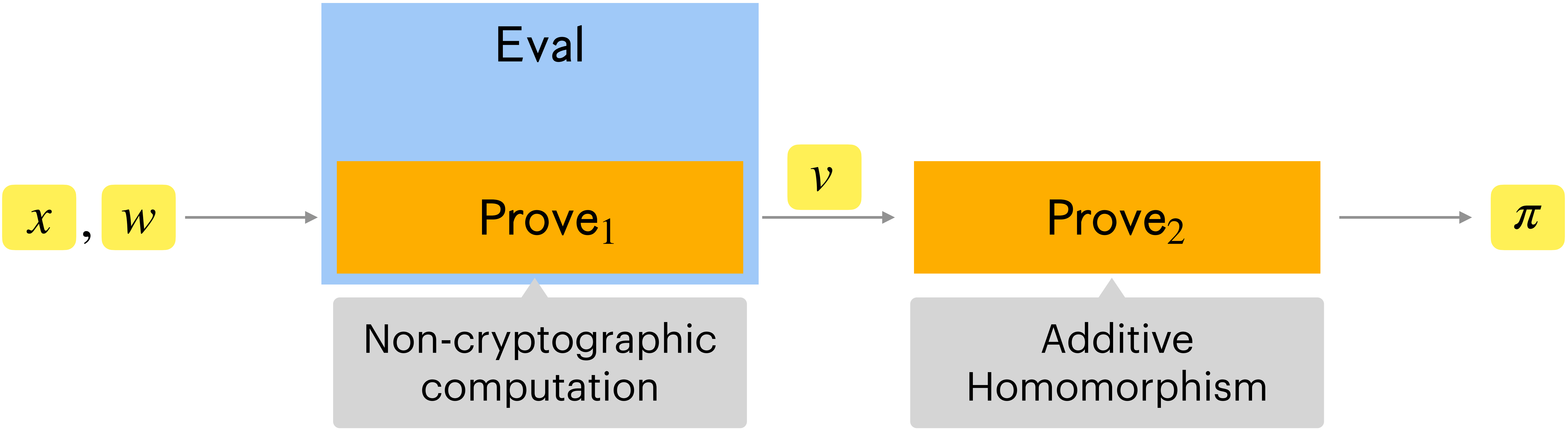


Eval supports a limited class of functions $\implies$ Prove$_1$ must be "simple" to compute (low depth circuit)

Do such zkSNARGs exist?

Splittable zkSNARG

Black-box use of cryptography

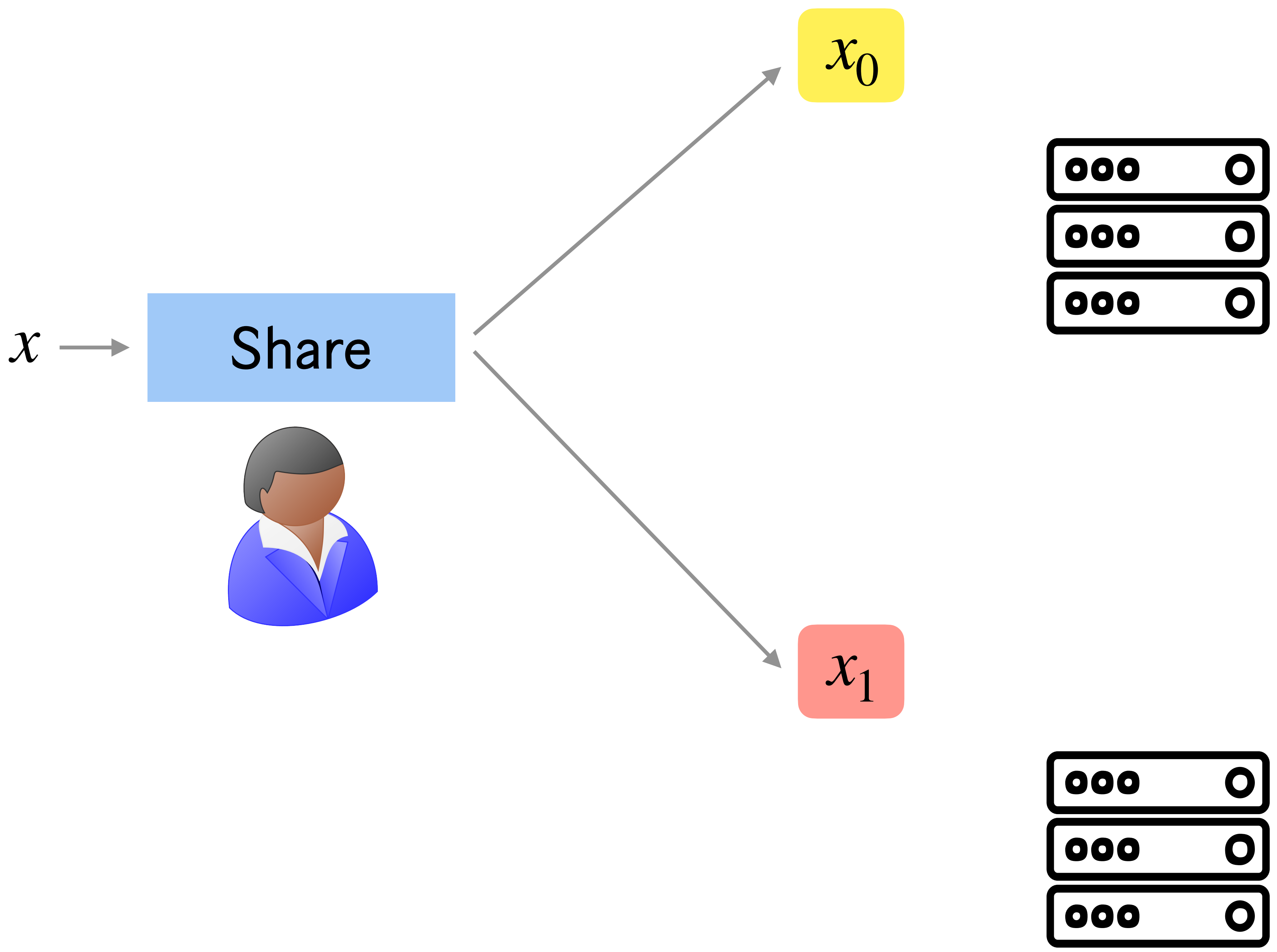


Eval supports a limited class of functions $\Longrightarrow$ Prove$_1$ must be “simple” to compute (low depth circuit)

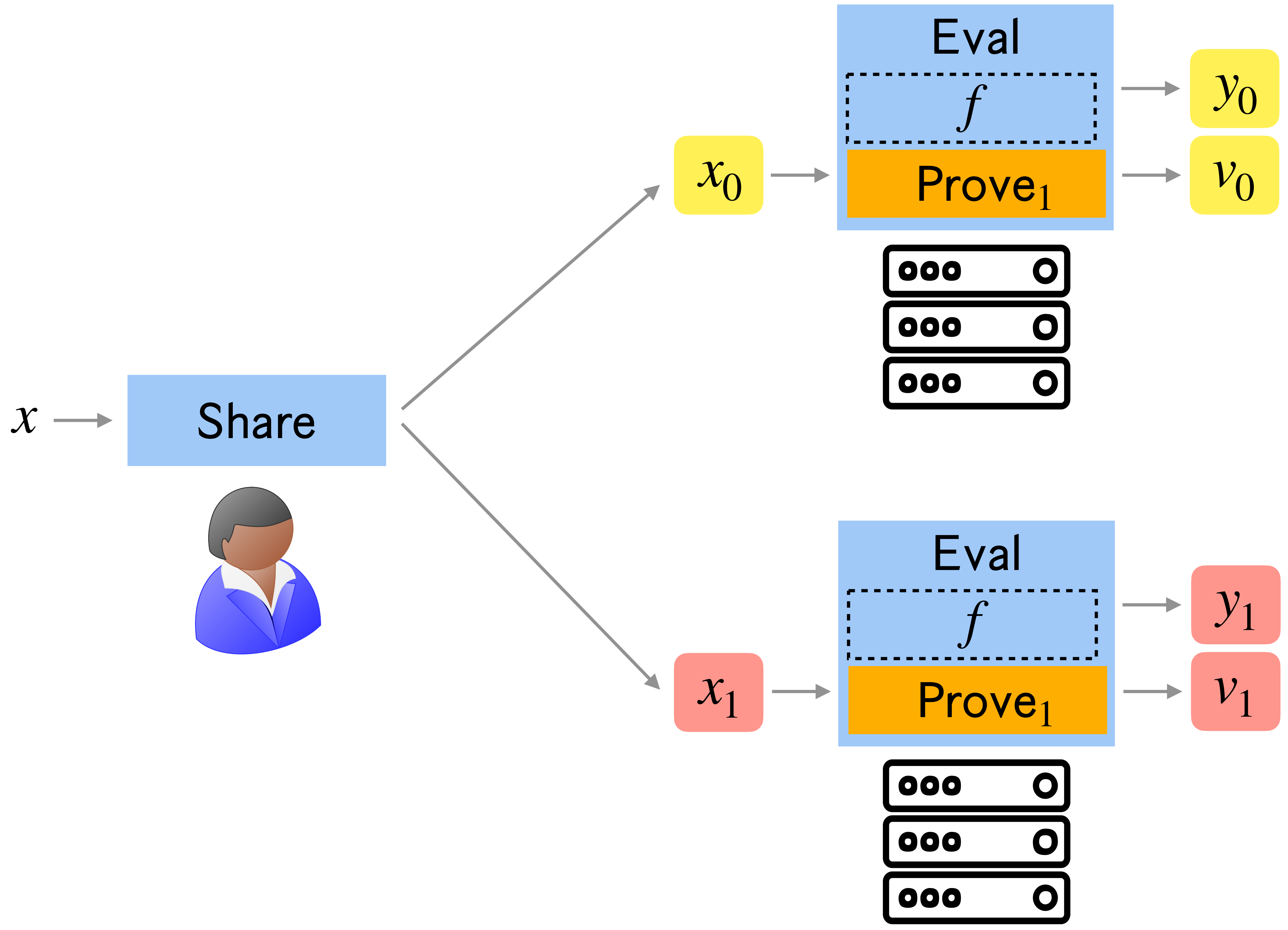
Do such zkSNARGs exist?

Yes!
[Groth16], zkBARG from [Waters-Wu 22]

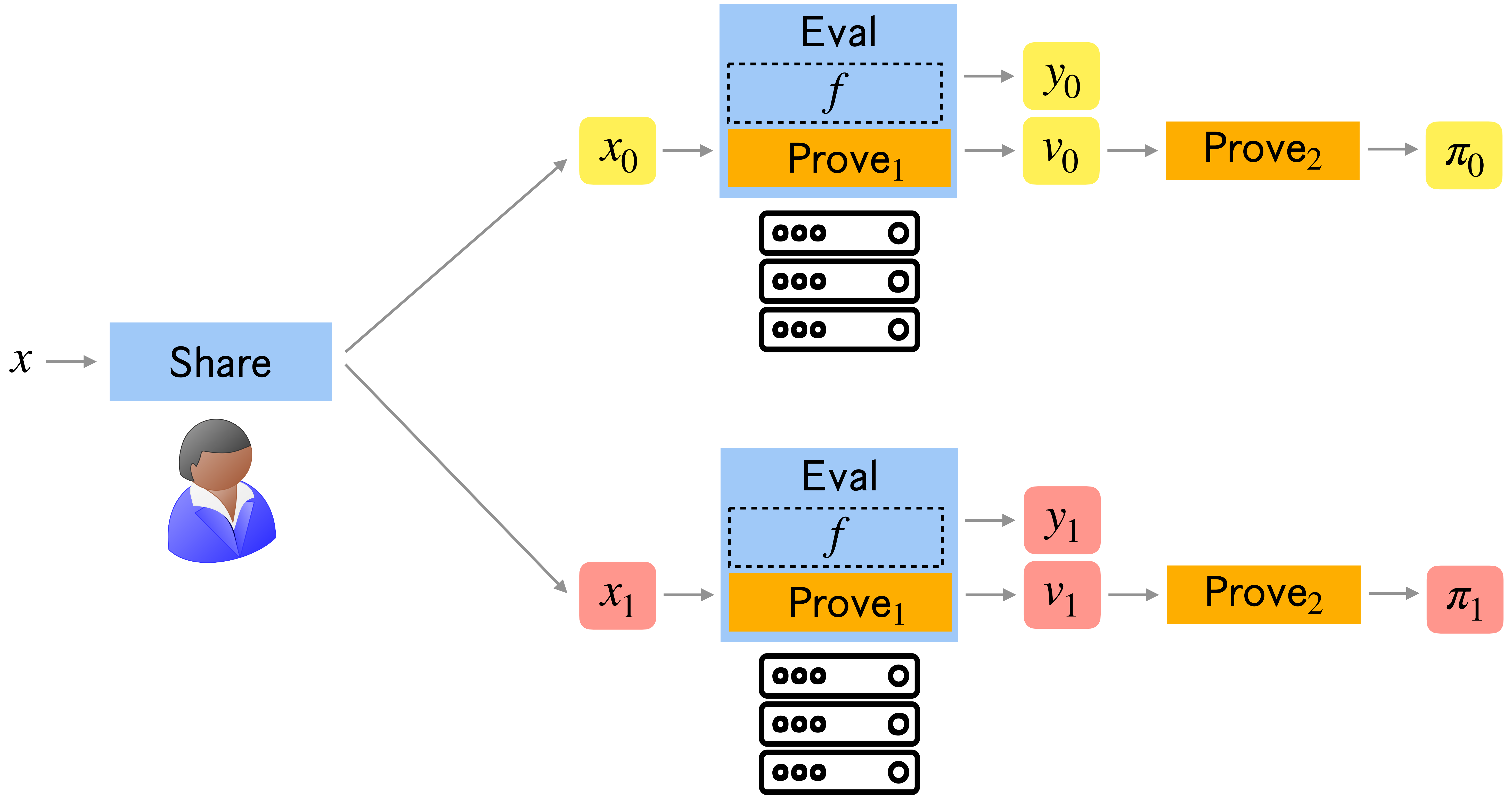
HSS with Verifiable Evaluation From Splittable zkSNARG



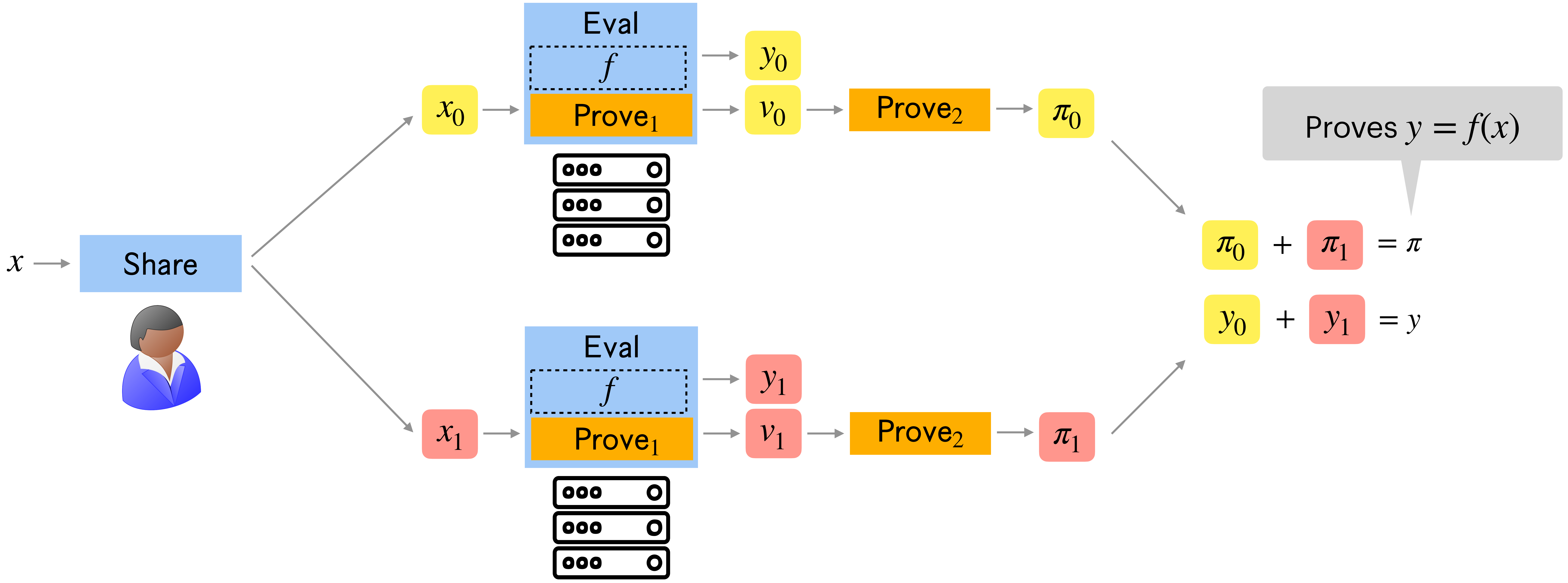
HSS with Verifiable Evaluation From Splittable zkSNARG



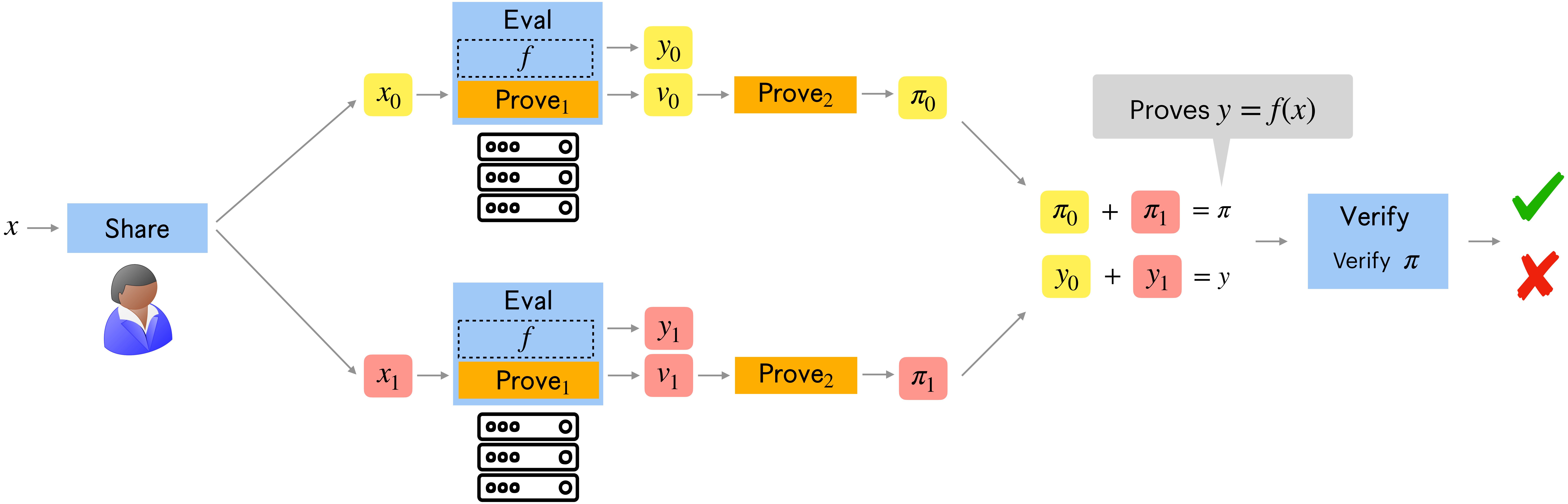
HSS with Verifiable Evaluation From Splittable zkSNARG



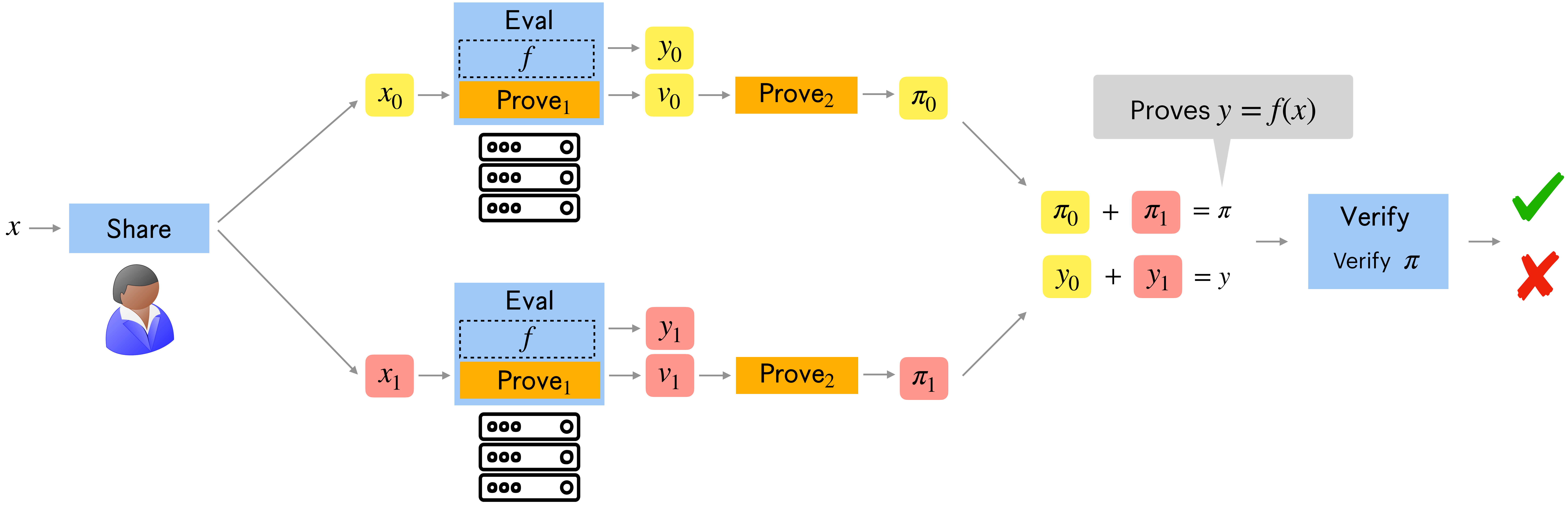
HSS with Verifiable Evaluation From Splittable zkSNARG



HSS with Verifiable Evaluation From Splittable zkSNARG

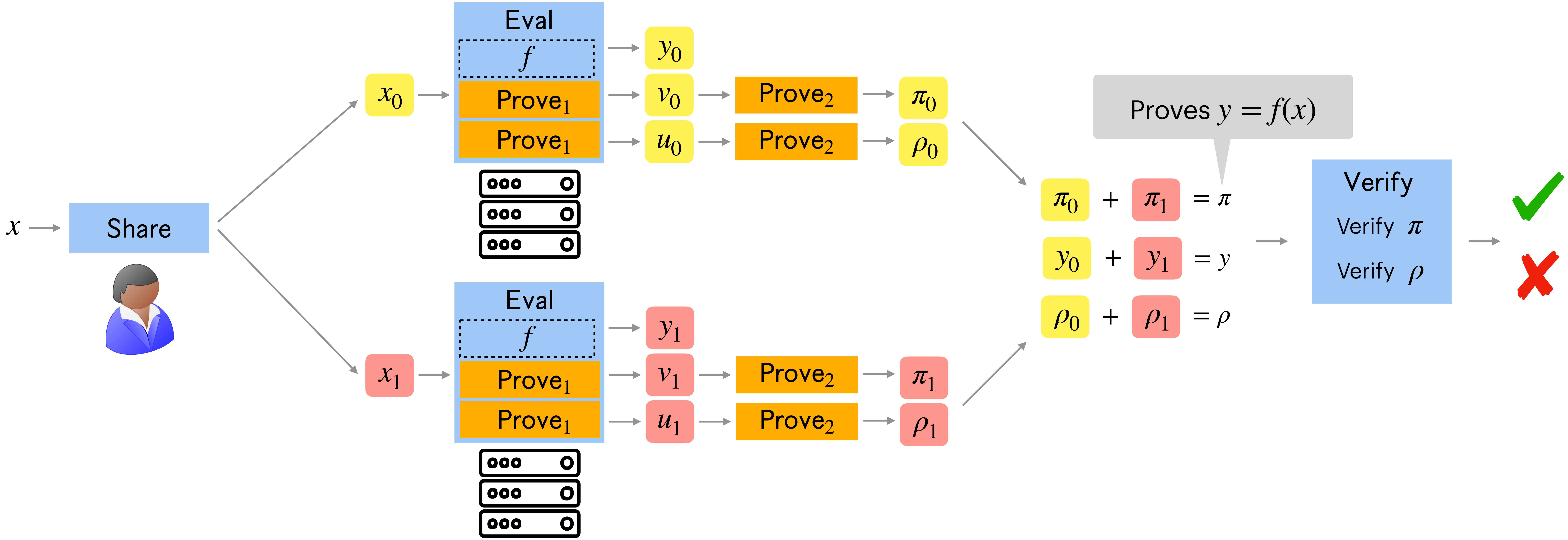


HSS with Verifiable Evaluation From Splittable zkSNARG



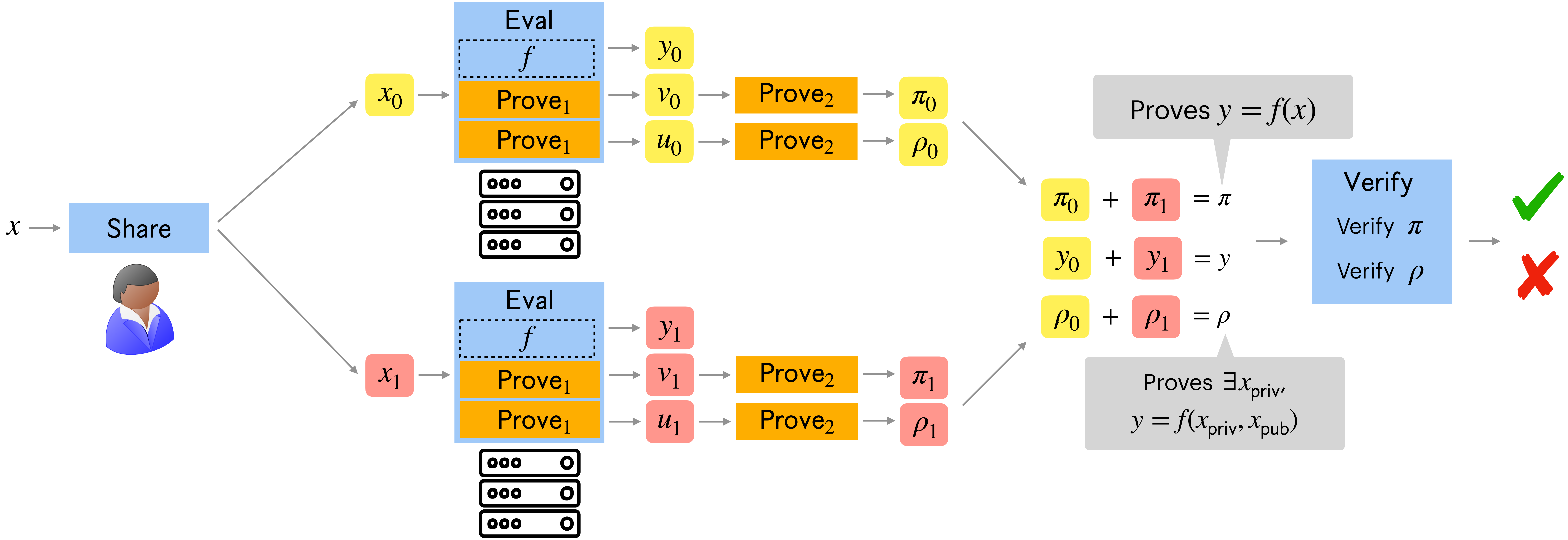
Soundness of $\pi \implies$ Local soundness

HSS with Verifiable Evaluation From Splittable zkSNARG



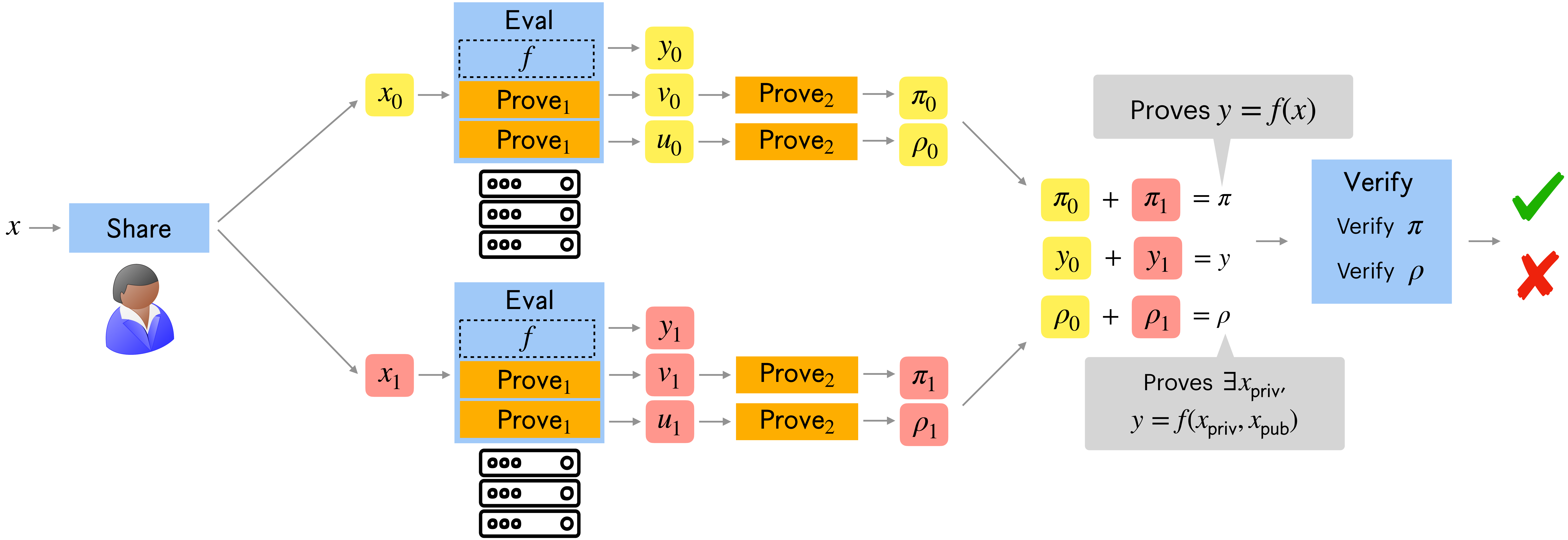
Soundness of $\pi \implies$ Local soundness

HSS with Verifiable Evaluation From Splittable zkSNARG



Soundness of $\pi \implies$ Local soundness

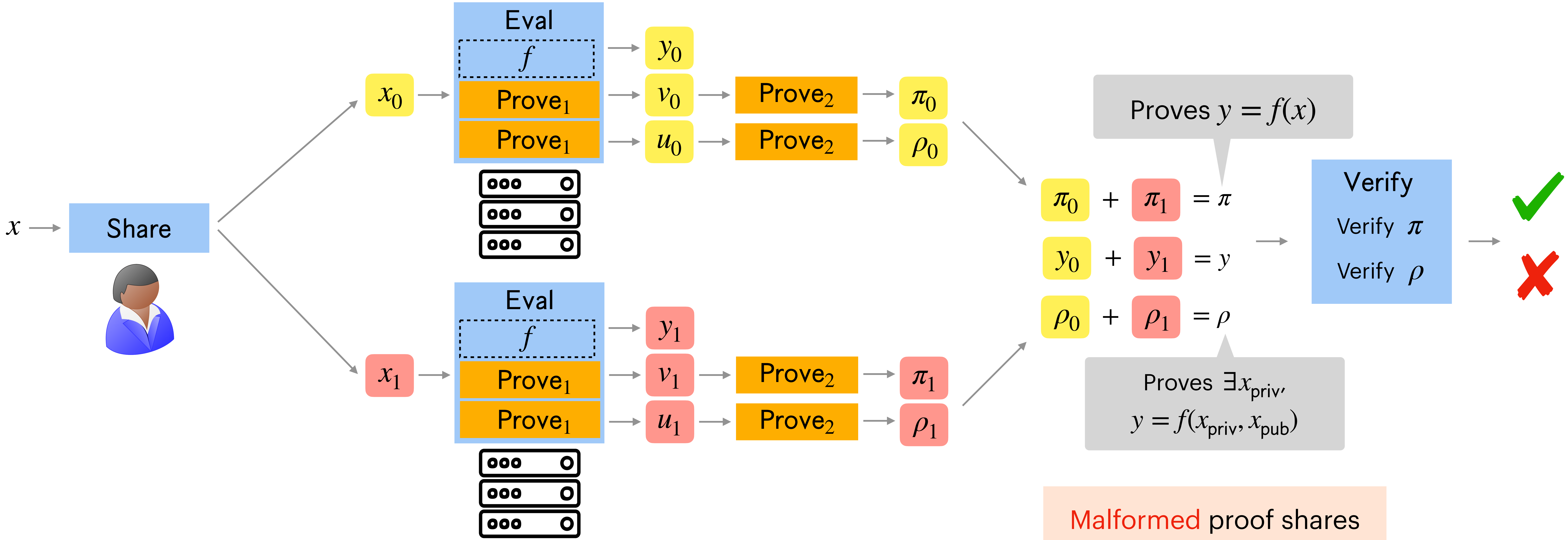
HSS with Verifiable Evaluation From Splittable zkSNARG



Soundness of $\pi \implies$ Local soundness

Soundness of $\rho \implies$ Public soundness

HSS with Verifiable Evaluation From Splittable zkSNARG



x

Share

x_0

Eval

f

Prove$_1$

Prove$_1$

y_0

v_0

u_0

Prove$_2$

Prove$_2$

π_0

ρ_0

x_1

Eval

f

Prove$_1$

Prove$_1$

y_1

v_1

u_1

Prove$_2$

Prove$_2$

π_1

ρ_1

Proves $y = f(x)$

$\pi_0 + \pi_1 = \pi$

$y_0 + y_1 = y$

$\rho_0 + \rho_1 = \rho$

Proves $\exists x_{\text{priv}},$
$y = f(x_{\text{priv}}, x_{\text{pub}})$

Verify

Verify π

Verify ρ

✓

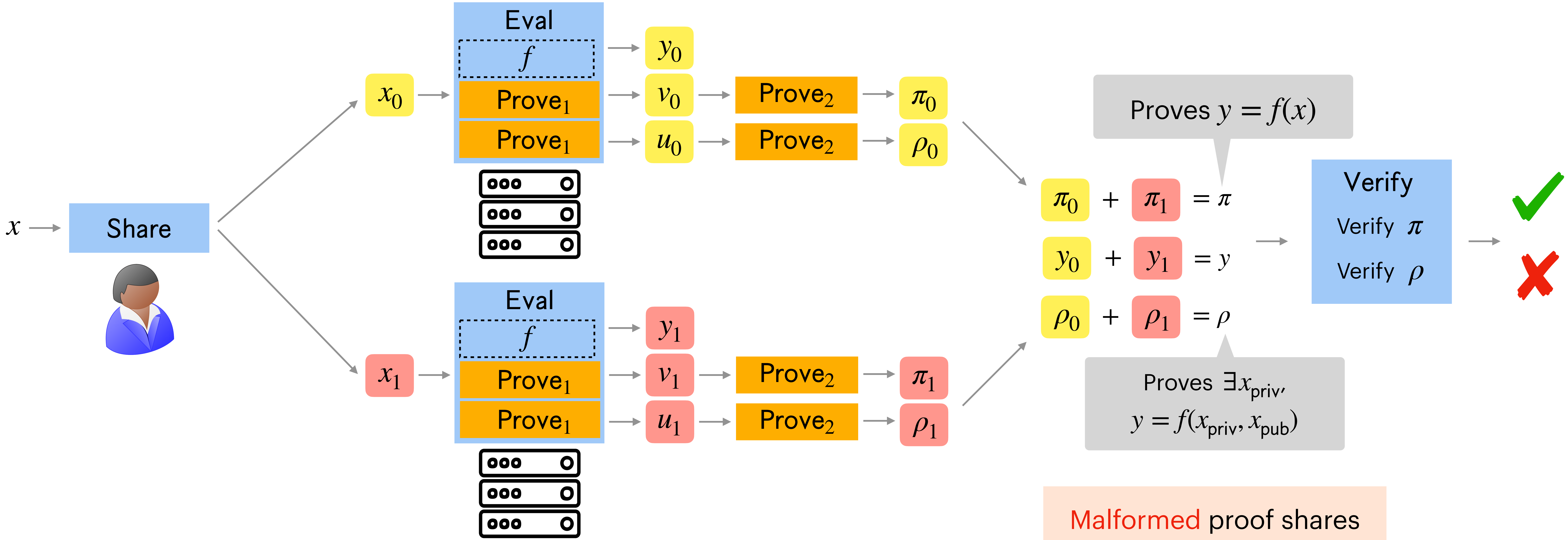
✗

Malformed proof shares can attack privacy

Soundness of $\pi \implies$ Local soundness

Soundness of $\rho \implies$ Public soundness

HSS with Verifiable Evaluation From Splittable zkSNARG



x → Share

x_0 → Eval: f → y_0; Prove$_1$ → v_0 → Prove$_2$ → π_0; Prove$_1$ → u_0 → Prove$_2$ → ρ_0

x_1 → Eval: f → y_1; Prove$_1$ → v_1 → Prove$_2$ → π_1; Prove$_1$ → u_1 → Prove$_2$ → ρ_1

$\pi_0 + \pi_1 = \pi$

$y_0 + y_1 = y$

$\rho_0 + \rho_1 = \rho$

Proves $y = f(x)$

Proves $\exists x_{\text{priv}}$,
$y = f(x_{\text{priv}}, x_{\text{pub}})$

Verify

Verify π

Verify ρ

✓

✗

Malformed proof shares
can attack privacy

Soundness of $\pi \implies$ Local soundness

Soundness of $\rho \implies$ Public soundness

Robust verification: Malformed proof shares always reconstruct to invalid proofs

Thank You