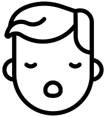
Reusable Non-Interactive Secure Computation

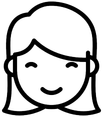
Melissa Chase	(MSR Redmond)
Yevgeniy Dodis	(NYU)
Yuval Ishai	(Technion)
Daniel Kraschewski	(TNG Technology Consulting)
Tianren Liu	(MIT $\rightarrow$ UW)
Rafail Ostrovsky	(UCLA)
Vinod Vaikuntanathan	(MIT)

Aug 22, 2019

Non-Interactive Secure Computation (NISC)

S 

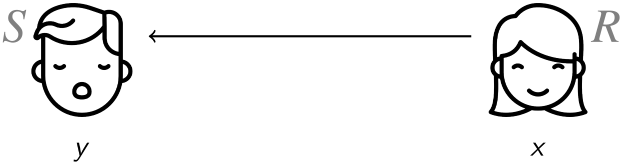
y

 R

x

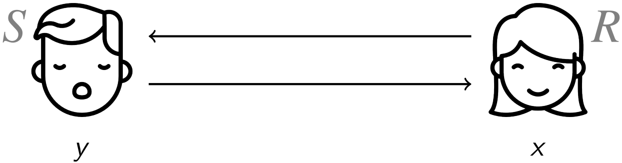
Goal: receiver gets $f(x, y)$ for a public function f.

Non-Interactive Secure Computation (NISC)



Goal: receiver gets $f(x, y)$ for a public function f.

Non-Interactive Secure Computation (NISC)



Goal: receiver gets $f(x, y)$ for a public function f.

Non-Interactive Secure Computation (NISC)

Goal: receiver gets $f(x,y)$ for a public function f.

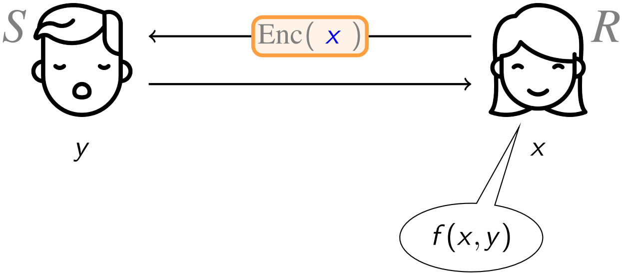
Non-Interactive Secure Computation (NISC)

E.g. FHE $\Longrightarrow$ Semi-honest NISC

Goal: receiver gets $f(x, y)$ for a public function f.

Non-Interactive Secure Computation (NISC)

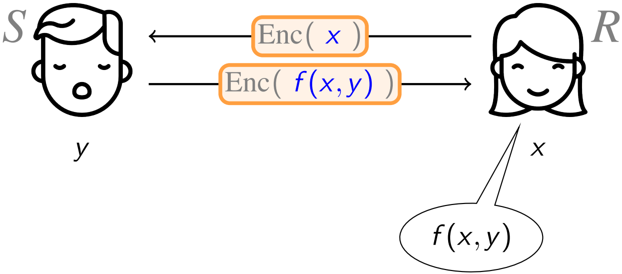
E.g. FHE $\Longrightarrow$ Semi-honest NISC



Goal: receiver gets $f(x, y)$ for a public function f.

Non-Interactive Secure Computation (NISC)

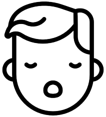
E.g. FHE $\Longrightarrow$ Semi-honest NISC



Goal: receiver gets $f(x,y)$ for a public function f.

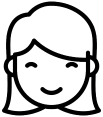
Garbled Circuit + OT $\Longrightarrow$ Semi-honest NISC [Kilian'88]

S



y

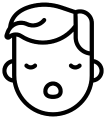
R



x

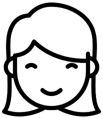
Garbled Circuit + OT $\implies$ Semi-honest NISC [Kilian'88]

S



y

R



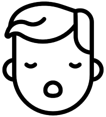
x

$\tilde{C}$ and tags

$w_{1,0}$	$w_{1,1}$
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

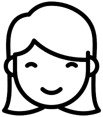
Garbled Circuit + OT $\Longrightarrow$ Semi-honest NISC [Kilian'88]

S



y

R



x

$\tilde{C}$ and tags

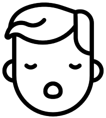
$w_{1,0}$	$w_{1,1}$
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

$x =$

1
0
0
1
$\vdots$
1

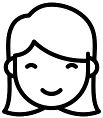
Garbled Circuit + OT $\Longrightarrow$ Semi-honest NISC [Kilian'88]

S



y

R



x

$\tilde{C}$ and tags

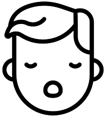
$w_{1,0}$	$w_{1,1}$
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

$x =$

1
0
0
1
$\vdots$
1

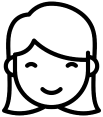
Garbled Circuit + OT $\Longrightarrow$ Semi-honest NISC [Kilian'88]

S



y

R



x

$\tilde{C}$ and tags

$w_{1,0}$	$w_{1,1}$
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

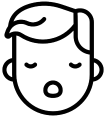
$x =$

1
0
0
1
$\vdots$
1

$\tilde{C}$ and $(w_{i,x_i})_{i=1}^{n}$ reveals $f(x,y)$
and nothing else computationally.

Garbled Circuit + OT $\Longrightarrow$ Semi-honest NISC [Kilian'88]

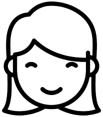
S



y

$\xrightarrow{\quad \tilde{C} \quad}$

R



x

$\tilde{C}$ and tags

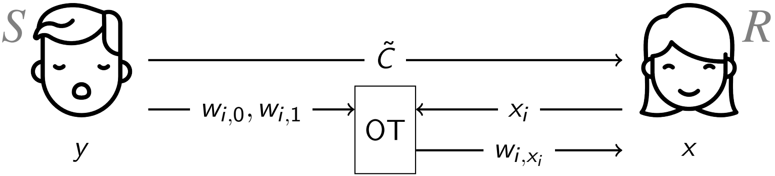
$w_{1,0}$	$w_{1,1}$
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

$x =$

1
0
0
1
$\vdots$
1

$\tilde{C}$ and $(w_{i,x_i})_{i=1}^{n}$ reveals $f(x,y)$
and nothing else computationally.

Garbled Circuit + OT $\implies$ Semi-honest NISC [Kilian'88]



$\tilde{C}$ and tags

$w_{1,0}$	$w_{1,1}$
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

$$x = \begin{array}{|c|}\hline 1 \\ \hline 0 \\ \hline 0 \\ \hline 1 \\ \hline \vdots \\ \hline 1 \\ \hline \end{array}$$

$\tilde{C}$ and $(w_{i,x_i})_{i=1}^{n}$ reveals $f(x, y)$
and nothing else computationally.

NISC in OT-hybrid model

Advantages

- OT realization from various models/assumptions
- Efficiency
- Malicious Security [Ishai-Kushilevitz-Ostrovsky-Prabhakaran-Sahai'88]
  - Information-theoretical NISC for $\mathbf{NC}^0$ in OT-hybrid.
  - NISC in OT-hybrid using black-box PRG.

Disadvantages

- NOT reusable secure.

NISC in OT-hybrid model

Advantages

- OT realization from various models/assumptions
- Efficiency
- Malicious Security [Ishai-Kushilevitz-Ostrovsky-Prabhakaran-Sahai'88]
  - Information-theoretical NISC for $\mathbf{NC}^0$ in OT-hybrid.
  - NISC in OT-hybrid using black-box PRG.

Disadvantages

- NOT reusable secure.

NISC in OT-hybrid model

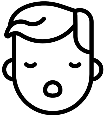
Advantages

- OT realization from various models/assumptions
- Efficiency
- Malicious Security [Ishai-Kushilevitz-Ostrovsky-Prabhakaran-Sahai'88]
  - Information-theoretical NISC for $\mathbf{NC}^0$ in OT-hybrid.
  - NISC in OT-hybrid using black-box PRG.

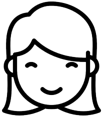
Disadvantages

- NOT reusable secure.

Reusable NISC

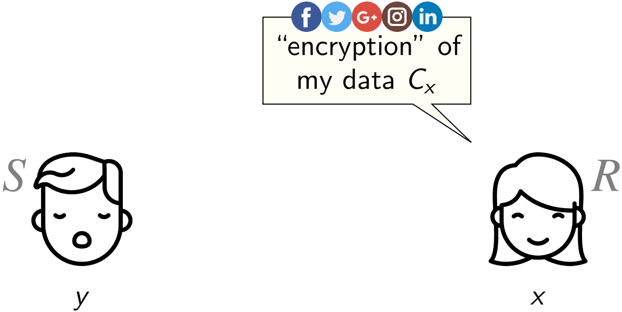
S 

y

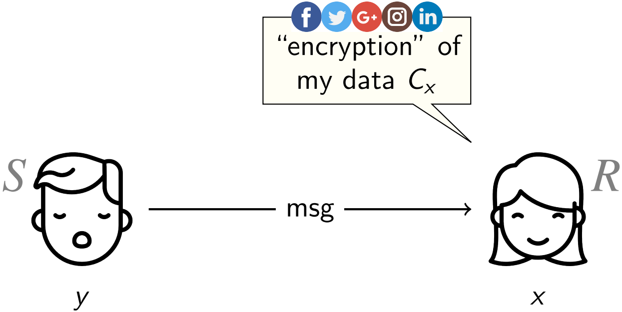
 R

x

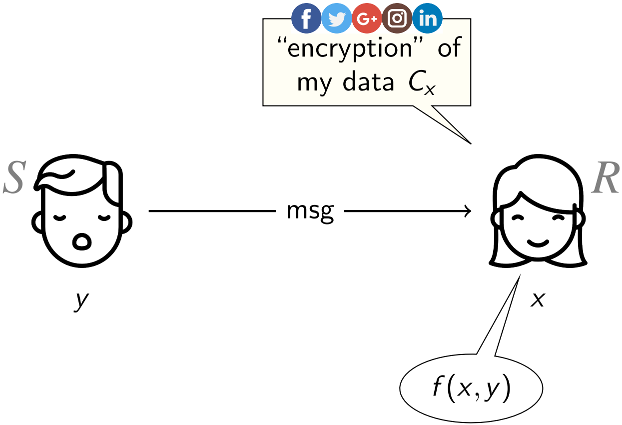
Reusable NISC



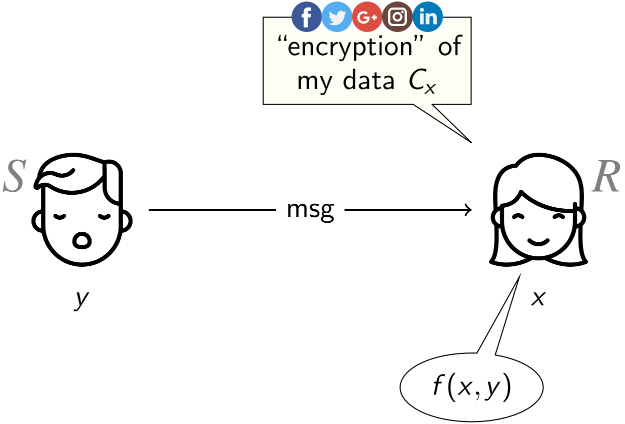
Reusable NISC



Reusable NISC

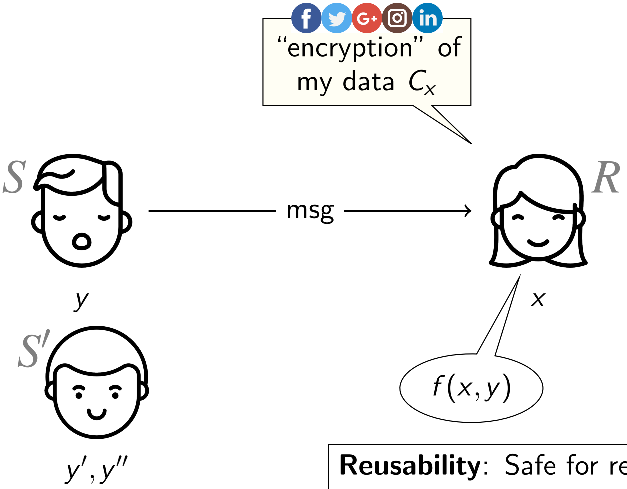


Reusable NISC



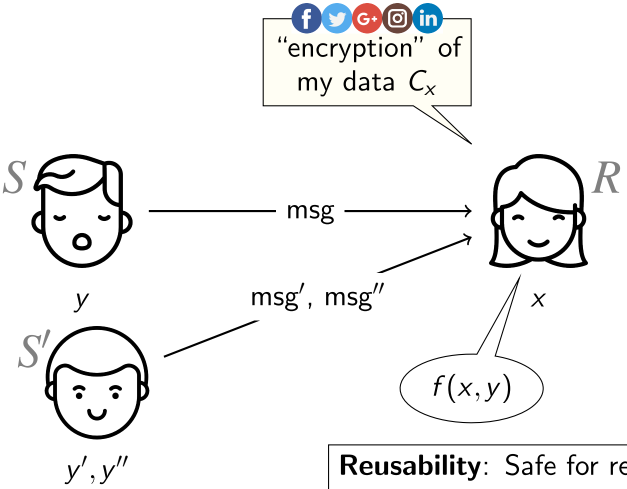
Reusability: Safe for receiver to reuse first msg and randomness

Reusable NISC



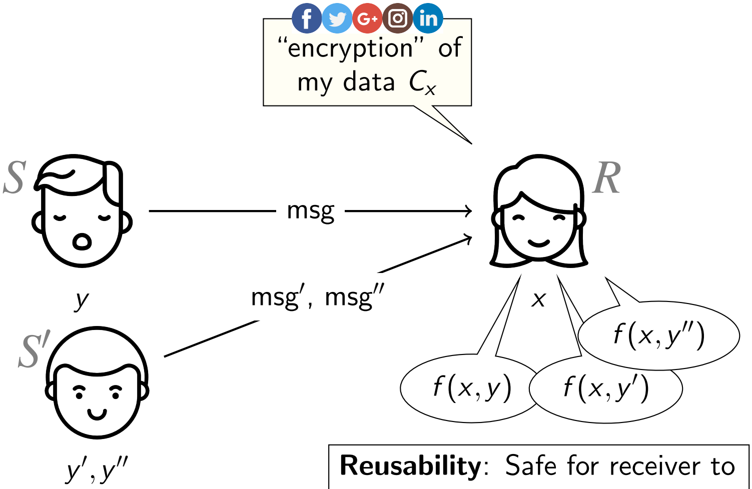
Reusability: Safe for receiver to reuse first msg and randomness

Reusable NISC



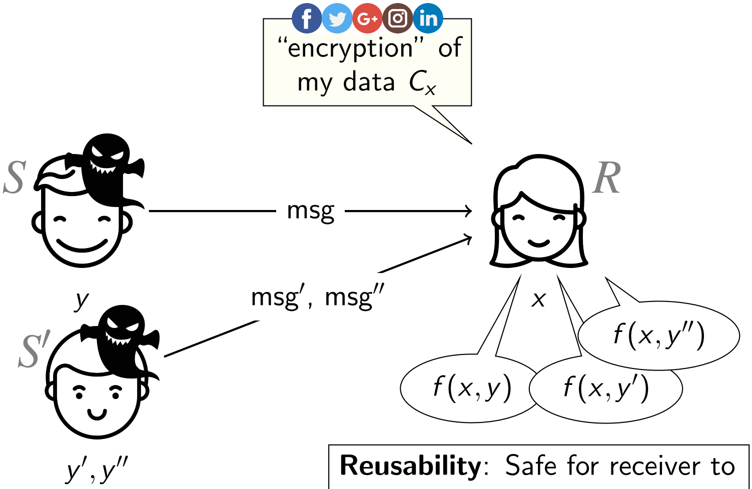
Reusability: Safe for receiver to reuse first msg and randomness

Reusable NISC



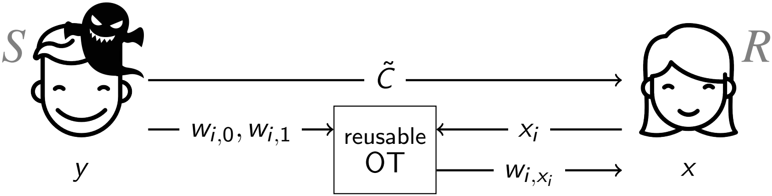
Reusability: Safe for receiver to reuse first msg and randomness

Reusable NISC



Reusability: Safe for receiver to reuse first msg and randomness

NISC in OT-hybrid model



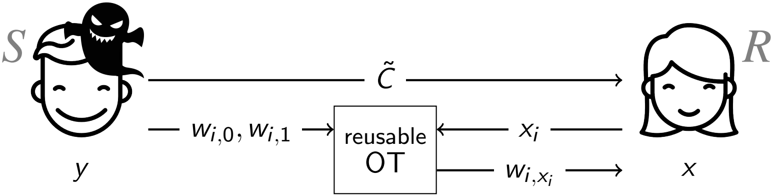
$\tilde{C}$ and tags

$w_{1,0}$	$w_{1,1}$
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

$x =$

1
0
0
1
$\vdots$
1

NISC in OT-hybrid model



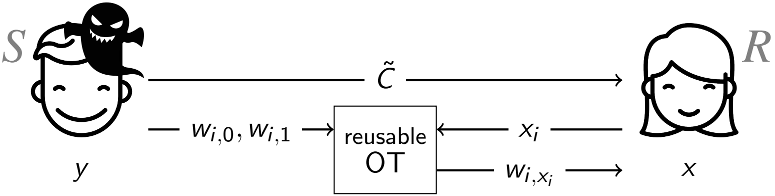
$\tilde{C}$ and tags

$w_{1,0}$	mess
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

$x =$

1
0
0
1
$\vdots$
1

NISC in OT-hybrid model



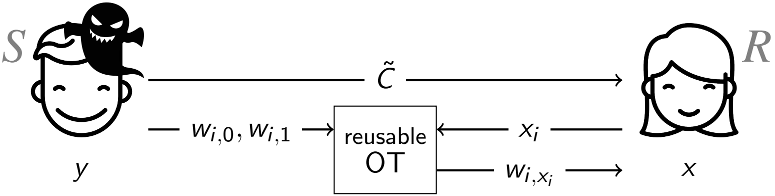
$\tilde{C}$ and tags

$w_{1,0}$	mess
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

$$x = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$$

Replacing $w_{1,1}$ changes 's behaviour $\implies x[1] = 1$
thus **NO security** against malicious sender.

NISC in OT-hybrid model



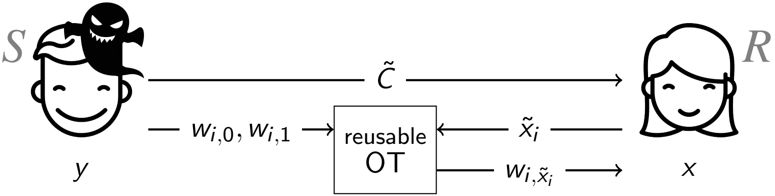
$\tilde{C}$ and tags

$w_{1,0}$	mess
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

$x =$

1
0
0
1
$\vdots$
1

NISC in OT-hybrid model + one-shot UC-security [IKOPS'11]



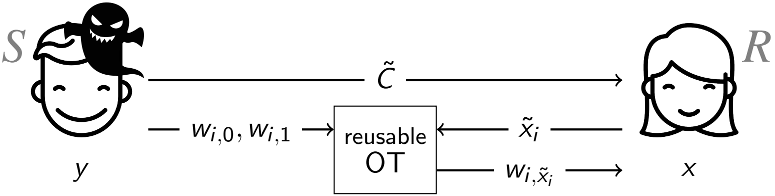
$\tilde{C}$ and tags

$w_{1,0}$	mess
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

let OT input be encoding $\tilde{x} =$

1
0
0
1
$\vdots$
1

NISC in OT-hybrid model + one-shot UC-security [IKOPS'11]



$\tilde{C}$ and tags

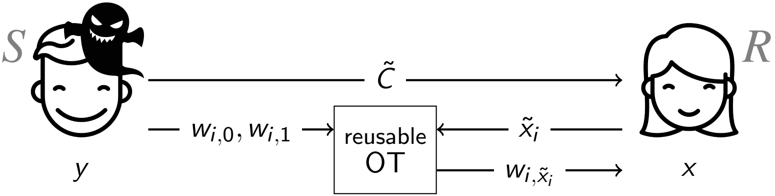
$w_{1,0}$	mess
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

let OT input be encoding $\tilde{x} =$

1
0
0
1
$\vdots$
1

A few bits of $\tilde{x}$ leaks no information about x.

NISC in OT-hybrid model + one-shot UC-security [IKOPS'11]



$\tilde{C}$ and tags

$w_{1,0}$	mess
$w_{2,0}$	$w_{2,1}$
$w_{3,0}$	$w_{3,1}$
$w_{4,0}$	$w_{4,1}$
$\vdots$	
$w_{n,0}$	$w_{n,1}$

let OT input be encoding $\tilde{x} =$

1
0
0
1
$\vdots$
1

Repeat the attack to learn the whole encoding $\tilde{x}$
thus **NO reusable security** against malicious sender.

Our Results

Impossible to patch the protocol against malicious adversaries in reusable settings, as we show...

Theorem 1

There is no information-theoretic reusable NISC in rOT-hybrid model.

Our Results

Impossible to patch the protocol against malicious adversaries in reusable settings, as we show...

Theorem 1

There is no information-theoretic reusable NISC in rOT-hybrid model.

There is no reusable NISC for certain functionalities in rOT-hybrid model with black-box simulation, assuming OWF.

Our Results

Impossible to patch the protocol against malicious adversaries in reusable settings, as we show...

Theorem 1

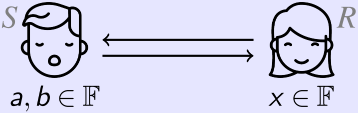
There is no information-theoretic reusable NISC in rOT-hybrid model.

There is no reusable NISC for certain functionalities in rOT-hybrid model with black-box simulation, assuming OWF.

Expansive alternative:
Semi-honest NISC $+$ reusable NIZK $\implies$ reusable NISC.

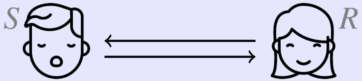
Our Results (continue)

NEW primitive: Oblivious linear function evaluation (OLE)



Our Results (continue)

NEW primitive: Oblivious linear function evaluation (OLE)

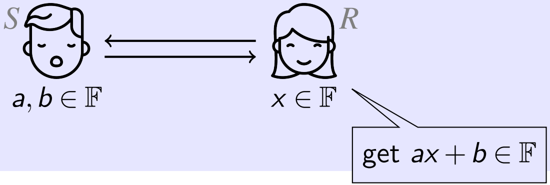


$a, b \in \mathbb{F}$ $\qquad$ $x \in \mathbb{F}$

get $ax + b \in \mathbb{F}$

Our Results (continue)

NEW primitive: Oblivious linear function evaluation (OLE)

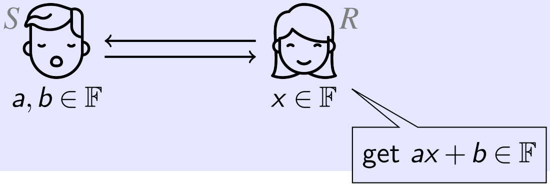


Theorem 2

An information-theoretical UC-secure reusable NISC protocol in rOLE-hybrid model.

Our Results (continue)

NEW primitive: Oblivious linear function evaluation (OLE)



Theorem 2

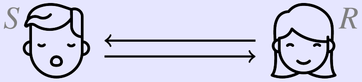
An information-theoretical UC-secure reusable NISC protocol in rOLE-hybrid model.

Theorem 3

An UC-secure 2-msg reusable OLE protocol in the CRS setting, under Paillier assumption.

Our Results (continue)

NEW primitive: Oblivious linear function evaluation (OLE)



$a, b \in \mathbb{F}$ $\quad$ $x \in \mathbb{F}$

get $ax + b \in \mathbb{F}$

Degenerate into OT if $|\mathbb{F}| = 2$.

Theorem 2

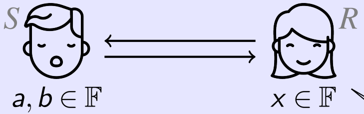
An information-theoretical UC-secure reusable NISC protocol in rOLE-hybrid model.

Theorem 3

An UC-secure 2-msg reusable OLE protocol in the CRS setting, under Paillier assumption.

Our Results (continue)

NEW primitive: Oblivious linear function evaluation (OLE)



get $ax + b \in \mathbb{F}$

Degenerate into OT if $|\mathbb{F}| = 2$.

Theorem 2

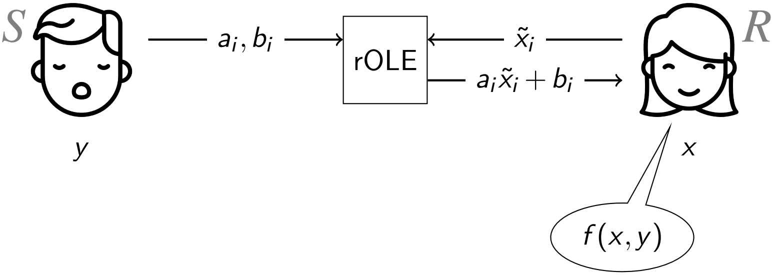
An information-theoretical UC-secure reusable NISC protocol in rOLE-hybrid model.

Security loss $\approx \frac{1}{|\mathbb{F}|}$

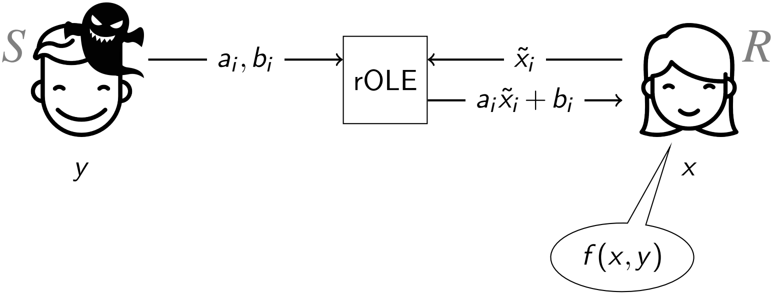
Theorem 3

An UC-secure 2-msg reusable OLE protocol in the CRS setting, under Paillier assumption.

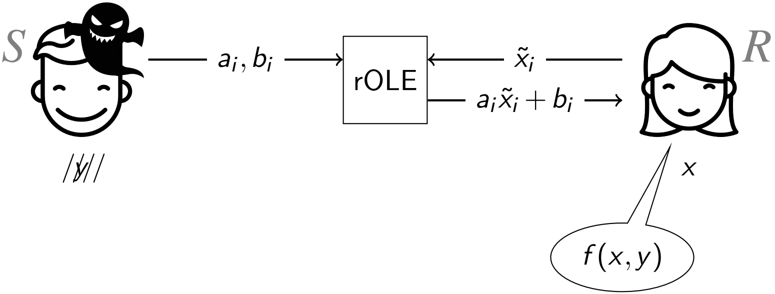
How to Lift One-shot Security to Reusability



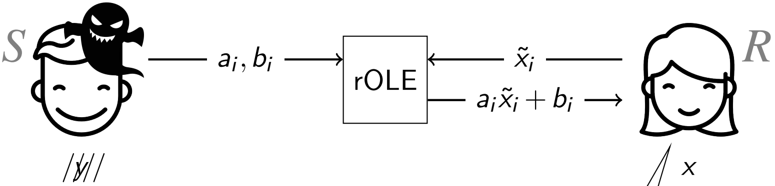
How to Lift One-shot Security to Reusability

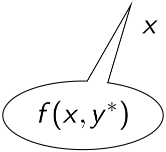


How to Lift One-shot Security to Reusability



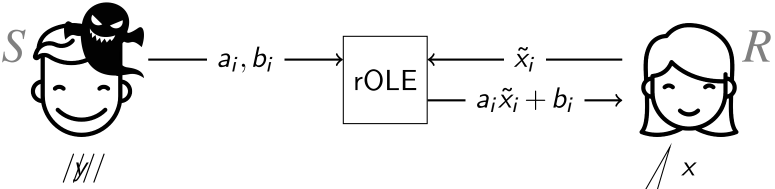
How to Lift One-shot Security to Reusability

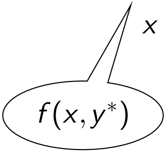




- **UC-security**: $\exists$ an efficient simulator $\mathscr{S}$
  $\mathscr{S}(a_1, b_1, a_2, b_2, \ldots) \to y^*$

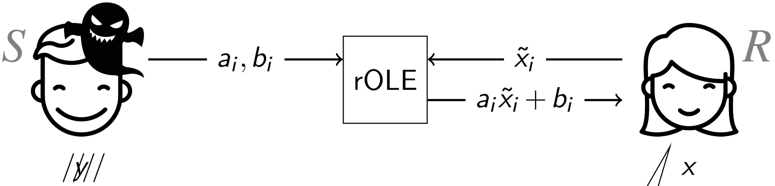
How to Lift One-shot Security to Reusability

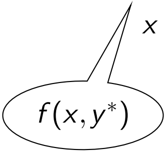




- **UC-security**: $\exists$ an efficient simulator $\mathscr{S}$
  $\mathscr{S}(a_1, b_1, a_2, b_2, \ldots) \to y^*$
- **No Abort** (optional): When abnormal behavior was detected, output $f(x, 0)$

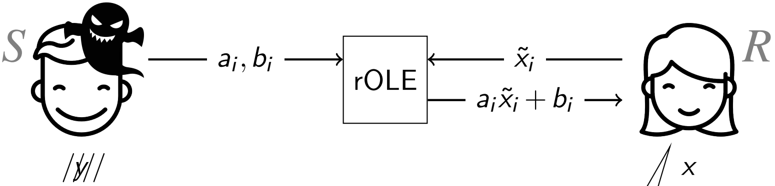
How to Lift One-shot Security to Reusability

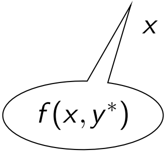




- **UC-security**: $\exists$ an efficient simulator $\mathscr{S}$
  $\mathscr{S}(a_1, b_1, a_2, b_2, \ldots) \to y^*$
- **No Abort** (optional): When abnormal behavior was detected, output $f(x, 0)$
- **Difficulty**: distribution $y^* \implies f(x, y^*)$ has entropy in ideal world
  $\implies$ leak information of receiver's randomness in real world

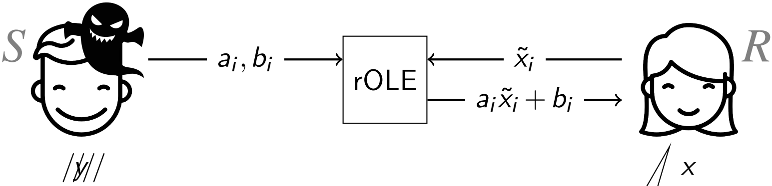
How to Lift One-shot Security to Reusability

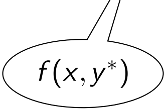




- **UC-security**: $\exists$ an efficient simulator $\mathscr{S}$
  $\mathscr{S}(a_1, b_1, a_2, b_2, \ldots) \rightarrow y^*$
- **No Abort** (optional): When abnormal behavior was detected, output $f(x, 0)$
- **Difficulty**: distribution $y^* \implies f(x, y^*)$ has entropy in ideal world
  $\implies$ leak information of receiver's randomness in real world

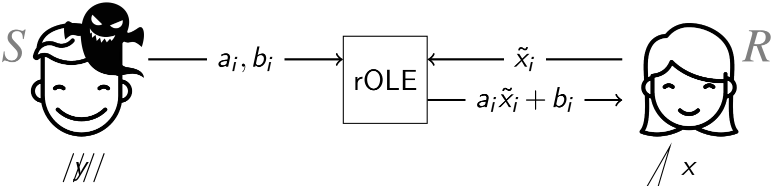
How to Lift One-shot Security to Reusability

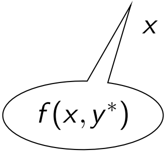




- **UC-security**: $\exists$ an efficient simulator $\mathscr{S}$
  $\mathscr{S}(a_1, b_1, a_2, b_2, \ldots) \to y^*$
- **No Abort** (optional): When abnormal behavior was detected, output $f(x, 0)$
- **Difficulty**: distribution $y^* \implies f(x, y^*)$ has entropy in ideal world
  $\implies$ leak information of receiver's randomness in real world

How to Lift One-shot Security to Reusability

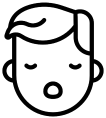




- **UC-security**: $\exists$ an efficient simulator $\mathscr{S}$
  $\mathscr{S}(a_1, b_1, a_2, b_2, \ldots) \to y^*$
- **No Abort** (optional): When abnormal behavior was detected, output $f(x, 0)$
- **Difficulty**: distribution $y^* \implies f(x, y^*)$ has entropy in ideal world $\implies$ leak information of receiver's randomness in real world
- **"Strong" UC-security $\implies$ Reusability**
  The simulator is deterministic

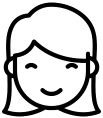
Overview: rNISC in rOLE-hybrid model

S



$y \in \mathbb{F}^n$

R



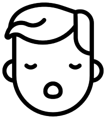
$x \in \mathbb{F}^n$

- Assume f is an arithmetic $\mathbf{NC}^1$ circuit or an arithmetic branching program over $\mathbb{F}$
- [IK'02,AIK'14] encode $y \mapsto (A, b)$ s.t. $Ax + b$ reveals $f(x, y)$ and nothing else
- **Against malicious sender:** detect if (A, b) is honestly generated, i.e. satisfies some simple arithmetic constraints

$$\text{Certified rOLE} \rightarrow \begin{cases} Ax + b, & \text{if } (A, b) \text{ satisfies constraints} \\ \perp, & \text{otherwise} \end{cases}$$

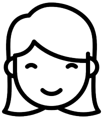
Overview: rNISC in rOLE-hybrid model

S



$y \in \mathbb{F}^n$

R

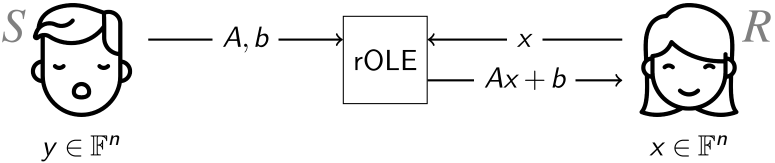


$x \in \mathbb{F}^n$

- Assume f is an arithmetic $\mathbf{NC}^1$ circuit or an arithmetic branching program over $\mathbb{F}$
- [IK'02,AIK'14] encode $y \mapsto (A, b)$ s.t. $Ax + b$ reveals $f(x, y)$ and nothing else
- **Against malicious sender:** detect if (A, b) is honestly generated, i.e. satisfies some simple arithmetic constraints

$$\text{Certified rOLE} \to \begin{cases} Ax + b, & \text{if } (A,b) \text{ satisfies constraints} \\ \perp, & \text{otherwise} \end{cases}$$

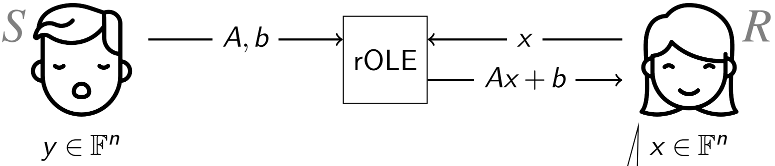
Overview: rNISC in rOLE-hybrid model

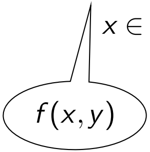


- Assume f is an arithmetic $\mathbf{NC}^1$ circuit or an arithmetic branching program over $\mathbb{F}$
- [IK'02,AIK'14] encode $y \mapsto (A, b)$ s.t. $Ax + b$ reveals $f(x, y)$ and nothing else
- **Against malicious sender:** detect if (A, b) is honestly generated, i.e. satisfies some simple arithmetic constraints

$$\text{Certified rOLE} \to \begin{cases} Ax + b, & \text{if } (A, b) \text{ satisfies constraints} \\ \perp, & \text{otherwise} \end{cases}$$

Overview: rNISC in rOLE-hybrid model

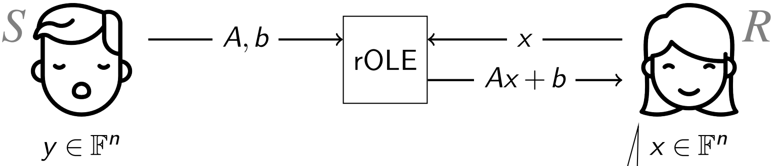


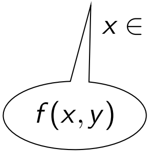


- Assume f is an arithmetic $\mathbf{NC}^1$ circuit or an arithmetic branching program over $\mathbb{F}$
- [IK'02,AIK'14] encode $y \mapsto (A, b)$ s.t. $Ax + b$ reveals $f(x, y)$ and nothing else
- **Against malicious sender:** detect if (A, b) is honestly generated, i.e. satisfies some simple arithmetic constraints

$$\text{Certified rOLE} \to \begin{cases} Ax + b, & \text{if } (A, b) \text{ satisfies constraints} \\ \perp, & \text{otherwise} \end{cases}$$

Overview: rNISC in rOLE-hybrid model

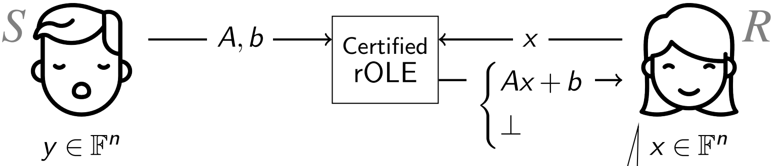


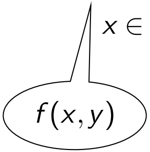


- Assume f is an arithmetic $\mathbf{NC}^1$ circuit or an arithmetic branching program over $\mathbb{F}$
- [IK'02,AIK'14] encode $y \mapsto (A, b)$ s.t. $Ax + b$ reveals $f(x, y)$ and nothing else
- **Against malicious sender:** detect if (A, b) is honestly generated, i.e. satisfies some simple arithmetic constraints

$$\text{Certified rOLE} \rightarrow \begin{cases} Ax + b, & \text{if } (A, b) \text{ satisfies constraints} \\ \perp, & \text{otherwise} \end{cases}$$

Overview: rNISC in rOLE-hybrid model

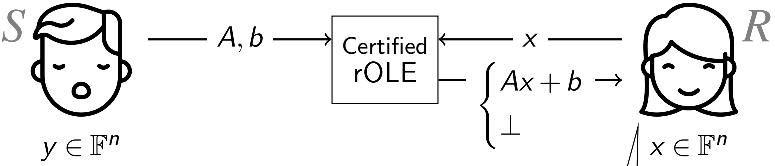


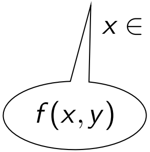


- Assume f is an arithmetic $\mathbf{NC}^1$ circuit or an arithmetic branching program over $\mathbb{F}$
- [IK'02,AIK'14] encode $y \mapsto (A, b)$ s.t. $Ax + b$ reveals $f(x, y)$ and nothing else
- **Against malicious sender:** detect if (A, b) is honestly generated, i.e. satisfies some simple arithmetic constraints

$$\text{Certified rOLE} \to \begin{cases} Ax + b, & \text{if } (A, b) \text{ satisfies constraints} \\ \perp, & \text{otherwise} \end{cases}$$

Overview: rNISC in rOLE-hybrid model



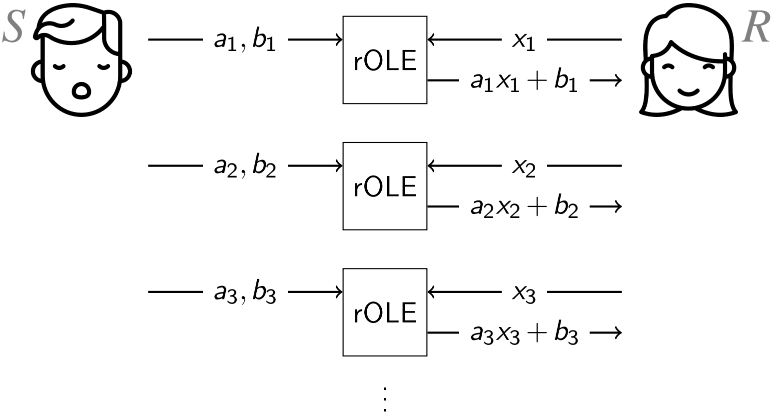


- Assume f is an arithmetic $\mathbf{NC}^1$ circuit or an arithmetic branching program over $\mathbb{F}$
- [IK'02,AIK'14] encode $y \mapsto (A, b)$ s.t. $Ax + b$ reveals $f(x, y)$ and nothing else
- **Against malicious sender:** detect if (A, b) is honestly generated, i.e. satisfies some simple arithmetic constraints

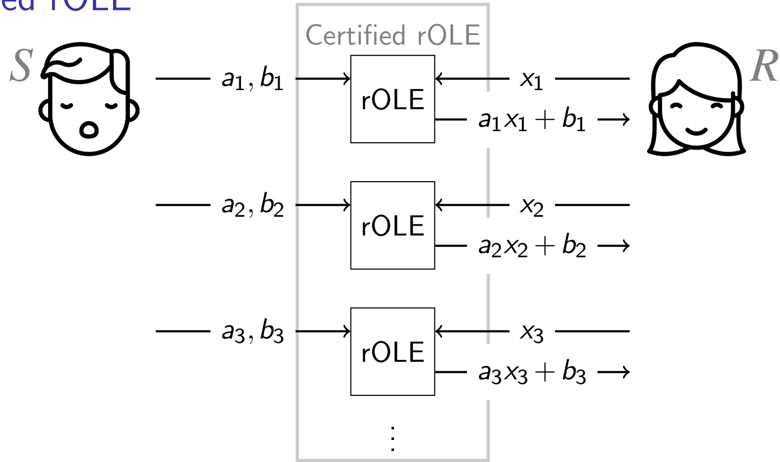
$$\text{Certified rOLE} \to \begin{cases} Ax + b, & \text{if } (A, b) \text{ satisfies constraints} \\ \perp, & \text{otherwise} \end{cases}$$

Certified rOLE

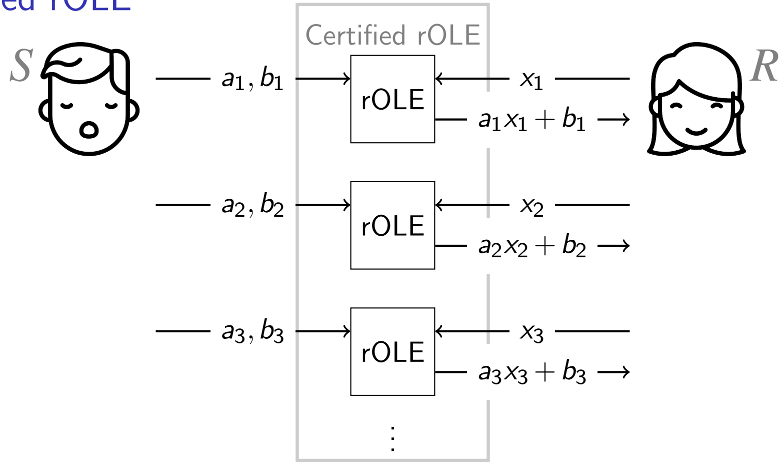
Certified rOLE



Certified rOLE

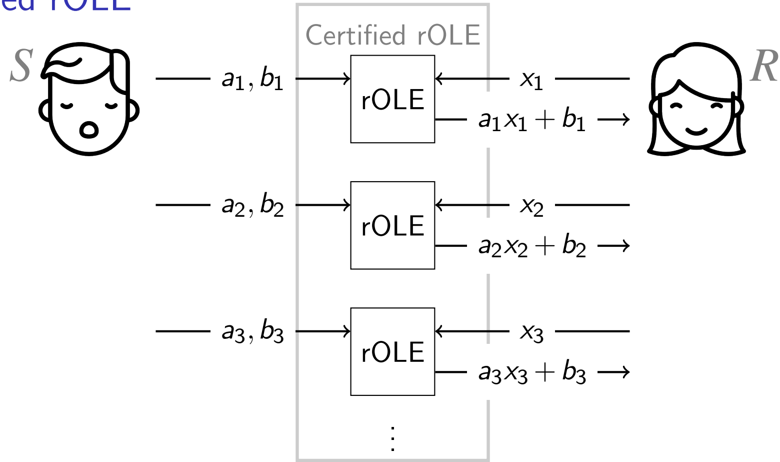


Certified rOLE



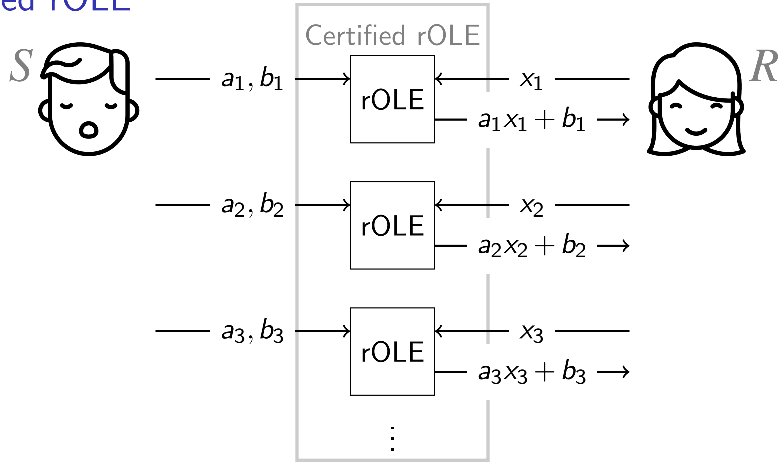
- Sender can prove $(a_1, b_1, a_2, b_2, \ldots)$ satisfies arithmetic constraints

Certified rOLE



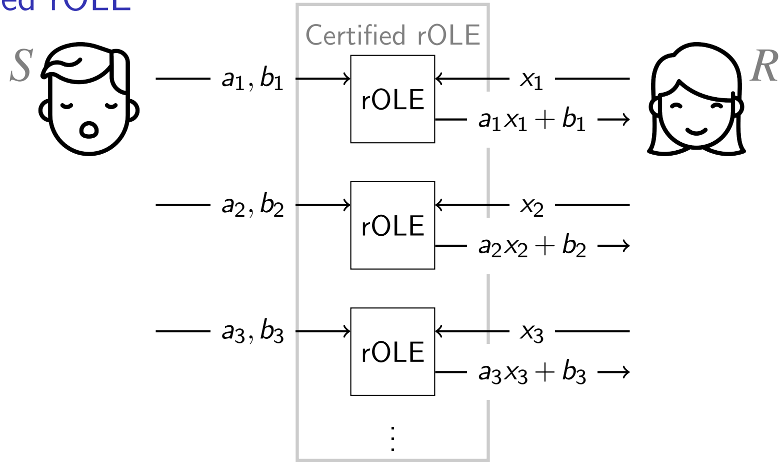
- Sender can prove $(a_1, b_1, a_2, b_2, \ldots)$ satisfies arithmetic constraints
- Side product: reusable DV-NIZK in rOLE-hybrid model.

Certified rOLE



- Sender can prove $(a_1, b_1, a_2, b_2, \ldots)$ satisfies ~~arithmetic constraints~~
- Side product: reusable DV-NIZK in rOLE-hybrid model.

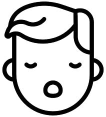
Certified rOLE



- Sender can prove $(a_1, b_1, a_2, b_2, \ldots)$ satisfies ~~arithmetic constraints~~ $a_i = a_j$ for some (i, j)

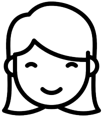
  for general constraints $\rightarrow$ see eprint
- Side product: reusable DV-NIZK in rOLE-hybrid model.

Certified rOLE

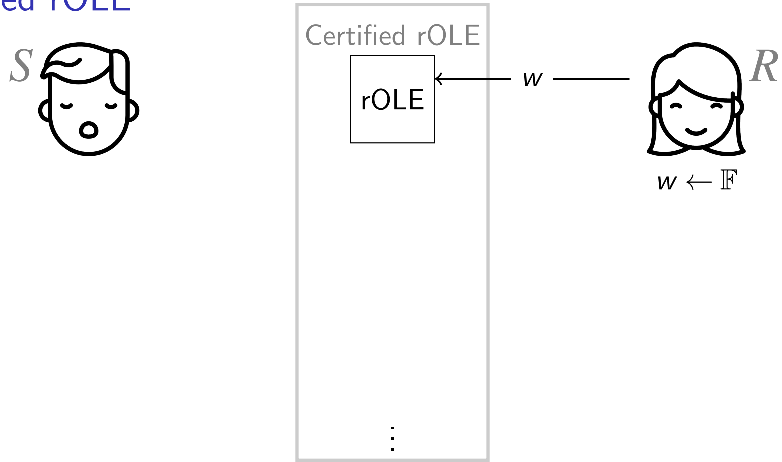
S 

Certified rOLE

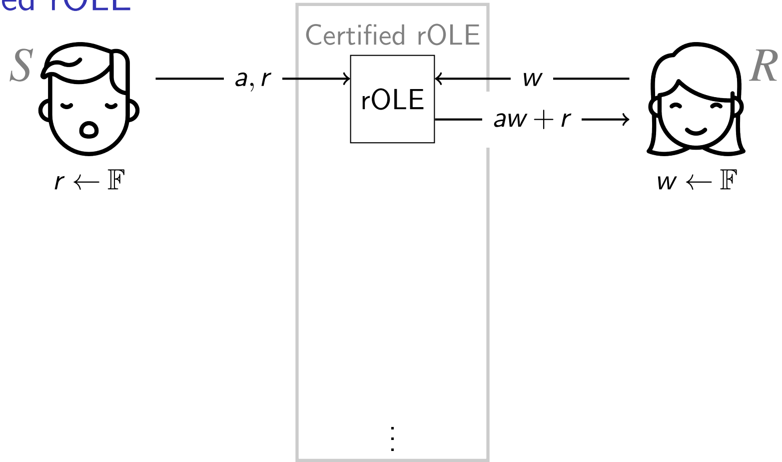
$\vdots$

 R

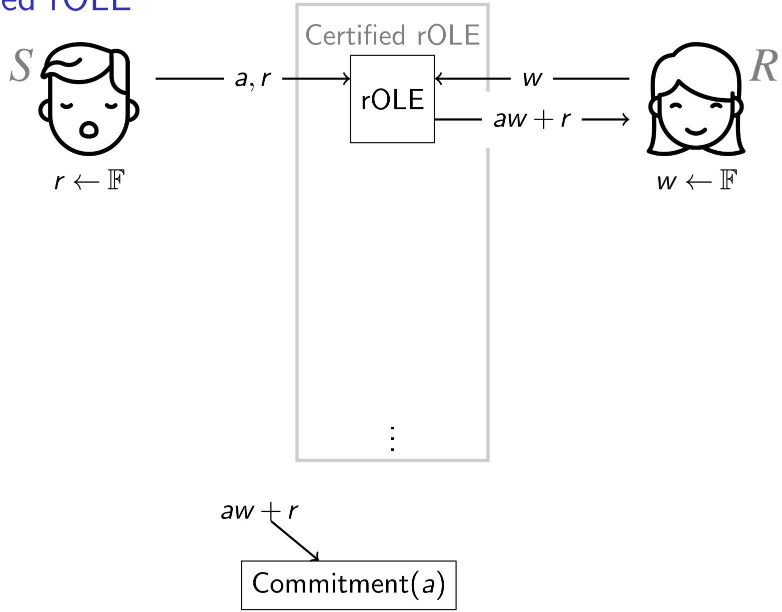
Certified rOLE



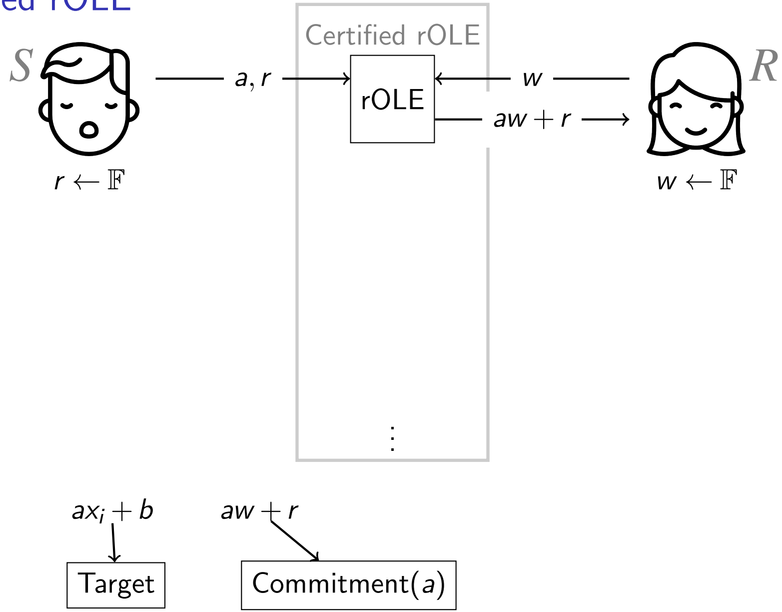
Certified rOLE



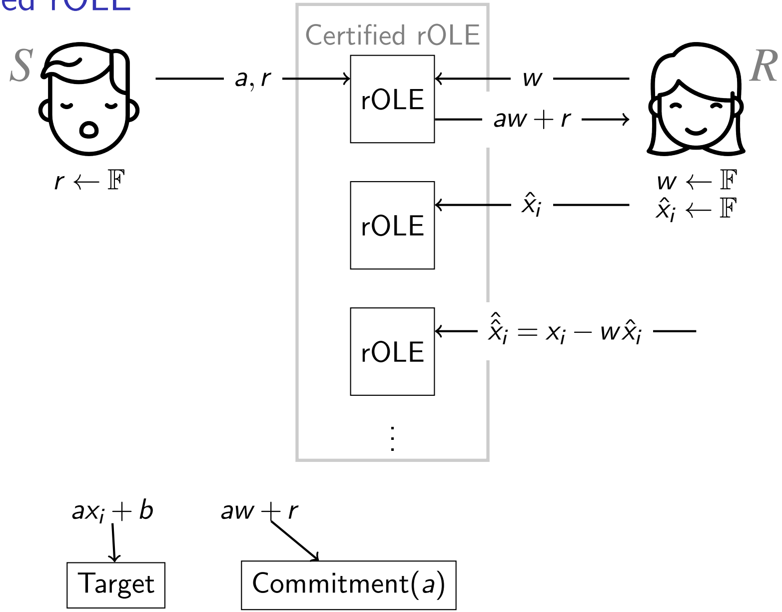
Certified rOLE



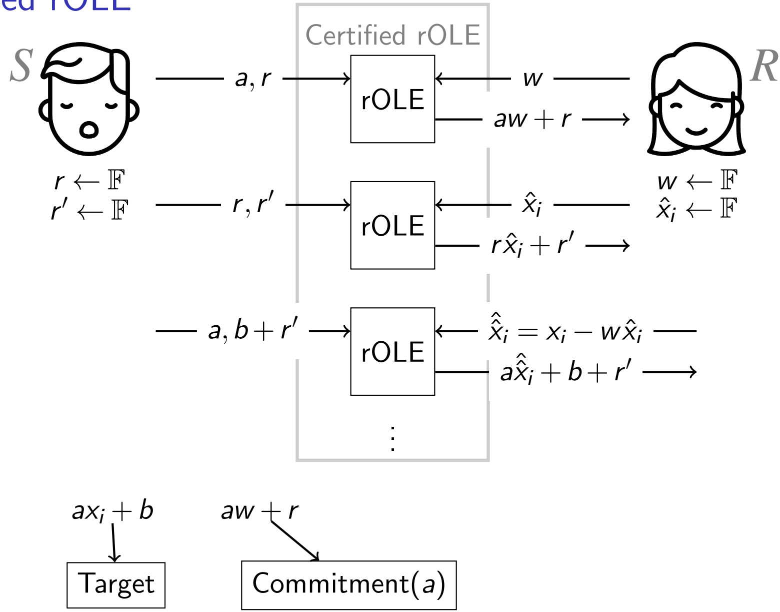
Certified rOLE



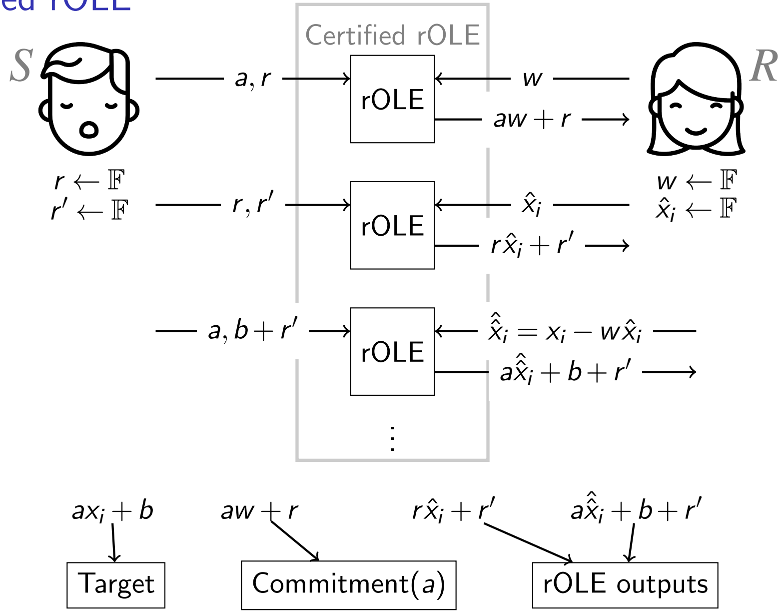
Certified rOLE



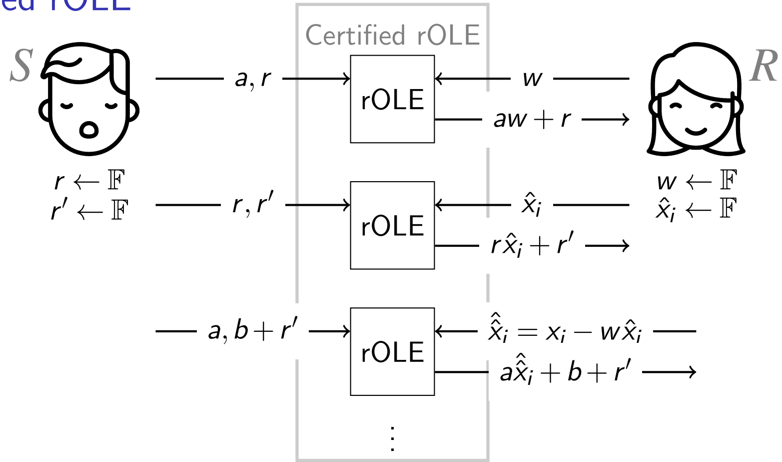
Certified rOLE



Certified rOLE



Certified rOLE



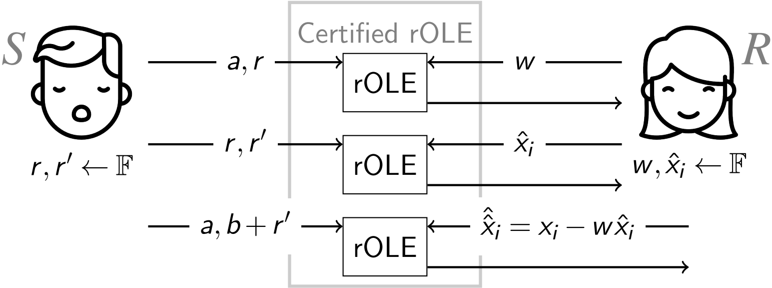
$$ax_i + b \;=\; (aw + r)\cdot \hat{x}_i \;-\; (r\hat{x}_i + r') \;+\; (a\hat{\hat{x}}_i + b + r')$$

Target

Commitment(a)

rOLE outputs

Certified rOLE



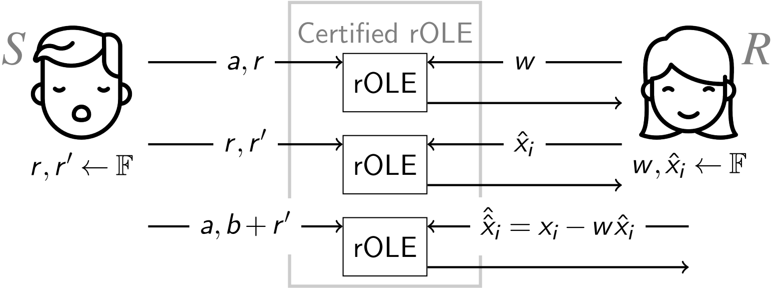
$$ax_i + b = (aw + r)\cdot\hat{x}_i - (r\hat{x}_i + r') + e(a\hat{\hat{x}}_i + b + r')$$

Target

Commitment(a)

rOLE outputs

Certified rOLE

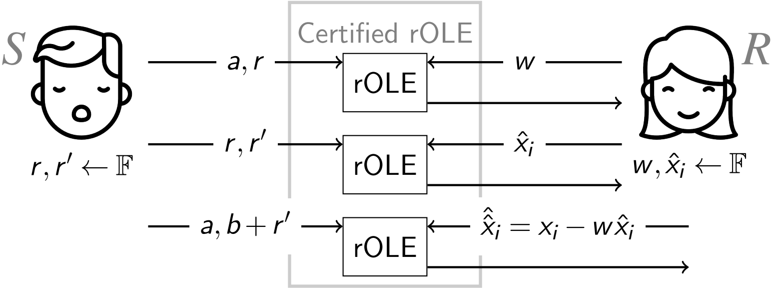


$$ax_i + b \;=\; (aw + r) \cdot \hat{x}_i \;-\; (r\hat{x}_i + r') \;+\; e(a\hat{\hat{x}}_i + b + r')$$

Target | Commitment(a) | rOLE outputs

- Correctness: Above equation.

Certified rOLE

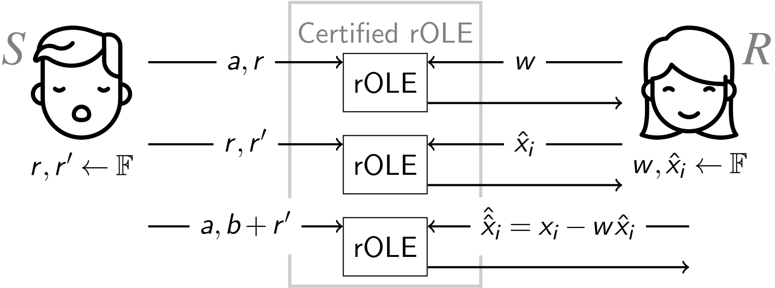


$$ax_i + b \;=\; (aw + r)\cdot \hat{x}_i \;-\; (r\hat{x}_i + r') \;+\; e(a\hat{\hat{x}}_i + b + r')$$

Target | Commitment(a) | rOLE outputs

- Correctness: Above equation.
- UC-secure against Receiver: $x_i := w\hat{x}_i + \hat{\hat{x}}_i$.

Certified rOLE



$$ax_i + b \;=\; (aw + r)\cdot \hat{x}_i \;-\; (r\hat{x}_i + r') \;+\; e(a\hat{\hat{x}}_i + b + r')$$

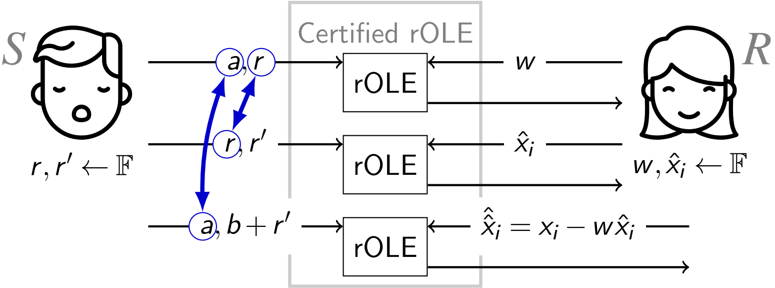
Target

Commitment(a)

rOLE outputs

- Correctness: Above equation.
- UC-secure against Receiver: $x_i := w\hat{x}_i + \hat{\hat{x}}_i$.
- "Strong" UC-secure against Sender:

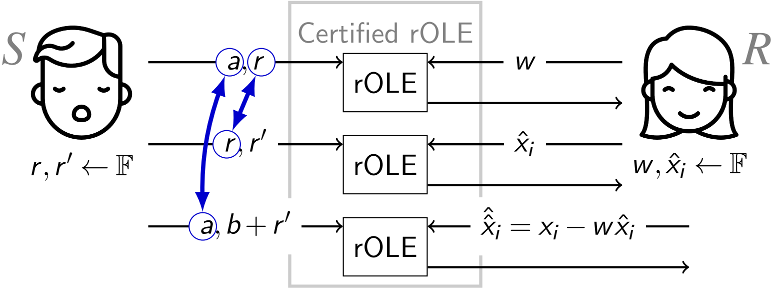
Certified rOLE



$$\underbrace{ax_i + b}_{\boxed{\text{Target}}} \;=\; \underbrace{(aw + r)}_{\boxed{\text{Commitment}(a)}} \cdot \hat{x}_i \;-\; \underbrace{(r\hat{x}_i + r') \;+\; e(a\hat{\hat{x}}_i + b + r')}_{\boxed{\text{rOLE outputs}}}$$

- Correctness: Above equation.
- UC-secure against Receiver: $x_i := w\hat{x}_i + \hat{\hat{x}}_i$.
- "Strong" UC-secure against Sender:

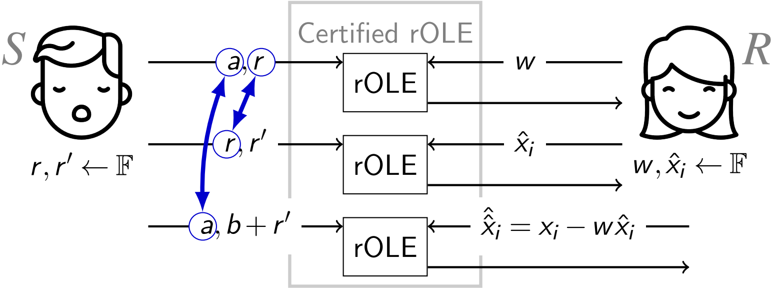
Certified rOLE



$$\underbrace{ax_i + b}_{\boxed{\text{Target}}} \;=\; \underbrace{(aw + r)}_{\boxed{\text{Commitment}(a)}} \cdot \hat{x}_i \;-\; \underbrace{(r\hat{x}_i + r') \;+\; e(a\hat{\hat{x}}_i + b + r')}_{\boxed{\text{rOLE outputs}}}$$

- Correctness: Above equation.
- UC-secure against Receiver: $x_i := w\hat{x}_i + \hat{\hat{x}}_i$.
- "Strong" UC-secure against Sender: Deviate $\implies$ random output

Certified rOLE

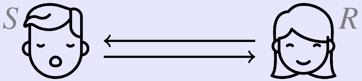


$$\underbrace{ax_i + b}_{\text{Target}} = \underbrace{(aw + r)}_{\text{Commitment}(a)} \cdot \hat{x}_i - \underbrace{(r\hat{x}_i + r') + e(a\hat{\hat{x}}_i + b + r')}_{\text{rOLE outputs}}$$

- Correctness: Above equation.
- UC-secure against Receiver: $x_i := w\hat{x}_i + \hat{\hat{x}}_i$.
- ~~"Strong"~~ UC-secure against Sender: Deviate $\implies$ random output
  not yet

Our Results

NEW primitive: Oblivious linear function evaluation (OLE)



$a, b \in \mathbb{F}$ $x \in \mathbb{F}$

get $ax + b \in \mathbb{F}$

Theorem 2

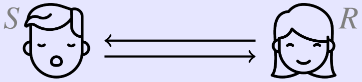
An information-theoretical UC-secure reusable NISC protocol in rOLE-hybrid model.

Theorem 3

An UC-secure 2-msg reusable OLE protocol in the CRS setting, under Paillier assumption.

Our Results

NEW primitive: Oblivious linear function evaluation (OLE)



$a, b \in \mathbb{F}$ $\quad$ $x \in \mathbb{F}$

get $ax + b \in \mathbb{F}$

Theorem 2

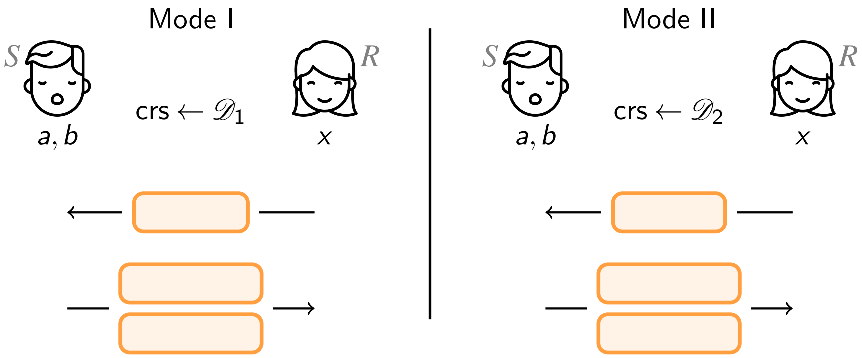
An information-theoretical UC-secure reusable NISC protocol in rOLE-hybrid model.

Theorem 3

An UC-secure 2-msg reusable OLE protocol in the CRS setting, under Paillier assumption.

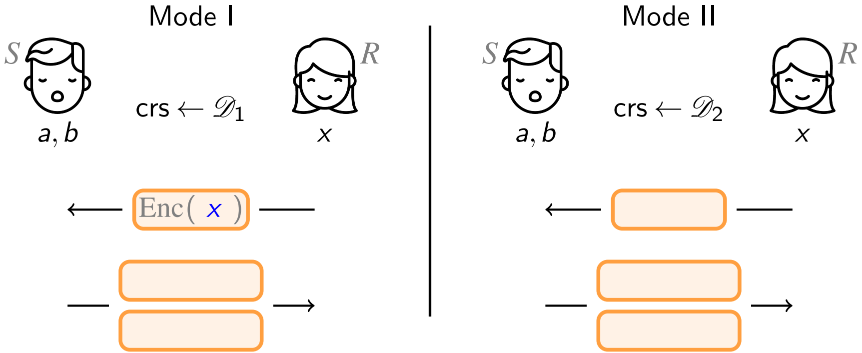
rOLE from Paillier

Dual-mode (similar to OT from [PVW'08])



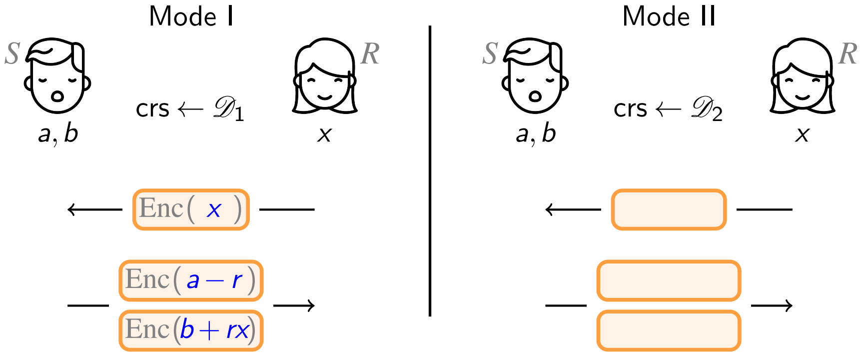
rOLE from Paillier

Dual-mode (similar to OT from [PVW'08])



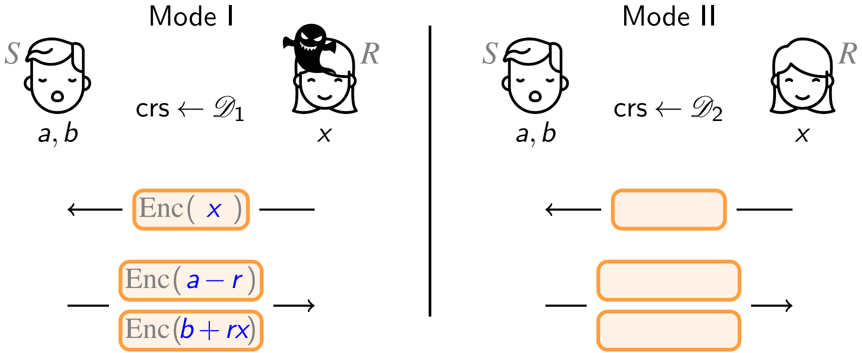
rOLE from Paillier

Dual-mode (similar to OT from [PVW'08])



rOLE from Paillier

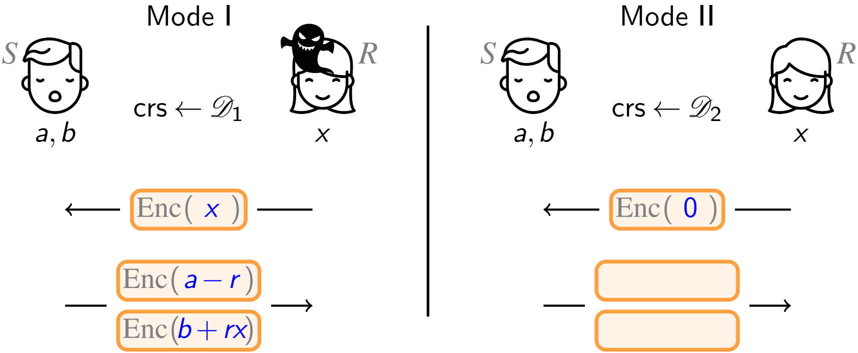
Dual-mode (similar to OT from [PVW'08])



Efficient simulator against
unbounded malicious receiver

rOLE from Paillier

Dual-mode (similar to OT from [PVW'08])



Efficient simulator against
unbounded malicious receiver

rOLE from Paillier

Dual-mode (similar to OT from [PVW'08])

Mode I

S  a, b

$\mathsf{crs} \leftarrow \mathscr{D}_1$

 R x

$\xleftarrow{\quad} \boxed{\mathrm{Enc}(\ x\ )} \xleftarrow{\quad}$

$\xrightarrow{\quad} \boxed{\mathrm{Enc}(a - r)},\ \boxed{\mathrm{Enc}(b + rx)} \xrightarrow{\quad}$

Efficient simulator against
unbounded malicious receiver

Mode II

S  a, b

$\mathsf{crs} \leftarrow \mathscr{D}_2$

 R x

$\xleftarrow{\quad} \boxed{\mathrm{Enc}(\ 0\ )} \xleftarrow{\quad}$

$\xrightarrow{\quad} \boxed{\mathrm{Enc}(\ a\ )},\ \boxed{\mathrm{Enc}(\ b\ )} \xrightarrow{\quad}$

rOLE from Paillier

Dual-mode (similar to OT from [PVW'08])

Mode I

S

a, b

$\mathsf{crs} \leftarrow \mathscr{D}_1$

R

x

$\xleftarrow{\quad \boxed{\mathrm{Enc}(\, x \,)} \quad}$

$\xrightarrow{\quad \boxed{\mathrm{Enc}(a - r)} \quad \boxed{\mathrm{Enc}(b + rx)} \quad}$

Efficient simulator against unbounded malicious receiver

Mode II

S

a, b

$\mathsf{crs} \leftarrow \mathscr{D}_2$

R

x

$\xleftarrow{\quad \boxed{\mathrm{Enc}(\, 0 \,)} \quad}$

$\xrightarrow{\quad \boxed{\mathrm{Enc}(\, a \,)} \quad \boxed{\mathrm{Enc}(\, b \,)} \quad}$

Efficient simulator against unbounded malicious sender

rOLE from Paillier

Dual-mode (similar to OT from [PVW'08])

$\mathscr{D}_1$ is indistinguishable from $\mathscr{D}_2$

Mode I

S  R 

a, b $\qquad$ crs $\leftarrow \mathscr{D}_1$ $\qquad$ x

$\longleftarrow$ $\boxed{\mathrm{Enc}(\ x\ )}$ $\longleftarrow$

$\longrightarrow$ $\boxed{\mathrm{Enc}(a - r)}$, $\boxed{\mathrm{Enc}(b + rx)}$ $\longrightarrow$

Efficient simulator against unbounded malicious receiver

Mode II

S  R 

a, b $\qquad$ crs $\leftarrow \mathscr{D}_2$ $\qquad$ x

$\longleftarrow$ $\boxed{\mathrm{Enc}(\ 0\ )}$ $\longleftarrow$

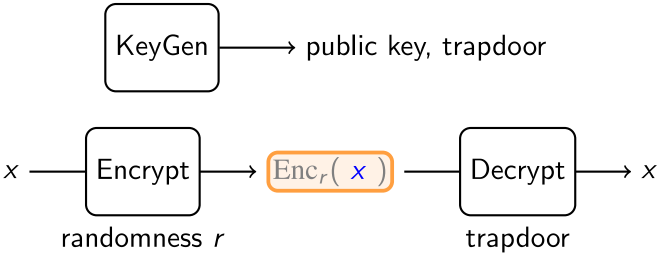
$\longrightarrow$ $\boxed{\mathrm{Enc}(\ a\ )}$, $\boxed{\mathrm{Enc}(\ b\ )}$ $\longrightarrow$

Efficient simulator against unbounded malicious sender

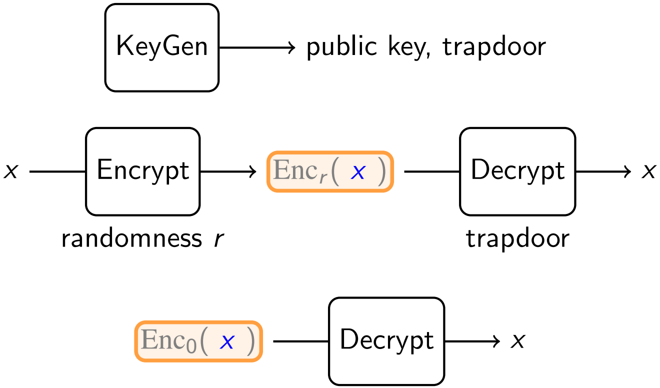
Paillier Encryption Scheme

$\boxed{\text{KeyGen}} \longrightarrow$ public key, trapdoor

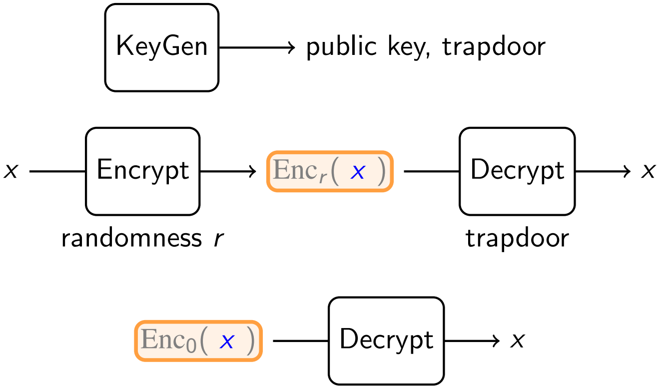
Paillier Encryption Scheme



Paillier Encryption Scheme

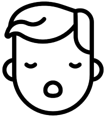


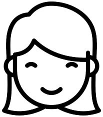
Paillier Encryption Scheme



$$\boxed{\mathrm{Enc}_r(\ x\ )} \cdot \boxed{\mathrm{Enc}_s(\ y\ )} = \boxed{\mathrm{Enc}_{r+s}(\ x+y\ )}$$

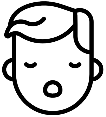
rOLE from Paillier

S

a, b

R

x

rOLE from Paillier

S



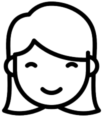
a, b

CRS (Mode I)

$$h = \boxed{\mathrm{Enc}_0(\ 1\ )}$$

$$w = \boxed{\mathrm{Enc}_\alpha(\ 0\ )}$$

$$W_0 = \boxed{\mathrm{Enc}_\beta(\ 1\ )}$$



R

x

rOLE from Paillier

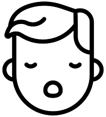
CRS (Mode I)

$h = \boxed{\mathrm{Enc}_0(\ 1\ )}$

$w = \boxed{\mathrm{Enc}_\alpha(\ 0\ )}$

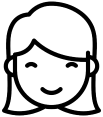
$W_0 = \boxed{\mathrm{Enc}_\beta(\ 1\ )}$

S



a, b

R



x

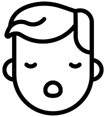
sample sk

$$\longleftarrow W_1 = w^{\mathsf{sk}} W_0^x = \boxed{\mathrm{Enc}_{x\beta+\alpha\cdot\mathsf{sk}}(\ x\ )} \text{———}$$

rOLE from Paillier

CRS (Mode I)

S



a, b

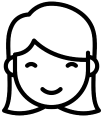
sample r

$$h = \boxed{\mathrm{Enc}_0(\ 1\ )}$$

$$w = \boxed{\mathrm{Enc}_\alpha(\ 0\ )}$$

$$W_0 = \boxed{\mathrm{Enc}_\beta(\ 1\ )}$$

R



x

sample sk

$$\longleftarrow \quad W_1 = w^{\mathsf{sk}} W_0^x = \boxed{\mathrm{Enc}_{x\beta+\alpha\cdot\mathsf{sk}}(\ x\ )} \quad \text{———}$$

$$v = w^r = \boxed{\mathrm{Enc}_{r\alpha}(\ 0\ )}$$

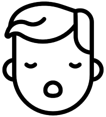
$$\text{———} \quad V_0 = h^a W_0^{-r} = \boxed{\mathrm{Enc}_{-r\beta}(\ a - r\ )} \quad \longrightarrow$$

$$V_1 = h^b W_1^r = \boxed{\mathrm{Enc}_{rx\beta+r\alpha\cdot\mathsf{sk}}(\ b + rx\ )}$$

rOLE from Paillier

CRS (Mode I)

S



a, b

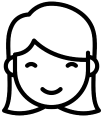
sample r

$$h = \boxed{\mathrm{Enc}_0(\ 1\ )}$$

$$w = \boxed{\mathrm{Enc}_\alpha(\ 0\ )}$$

$$W_0 = \boxed{\mathrm{Enc}_\beta(\ 1\ )}$$

R



x

sample sk

$$\longleftarrow \quad W_1 = w^{\mathsf{sk}} W_0^x = \boxed{\mathrm{Enc}_{x\beta+\alpha\cdot\mathsf{sk}}(\ x\ )} \quad \text{——}$$

$$v = w^r = \boxed{\mathrm{Enc}_{r\alpha}(\ 0\ )}$$

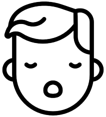
$$\text{——} \quad V_0 = h^a W_0^{-r} = \boxed{\mathrm{Enc}_{-r\beta}(\ a - r\ )} \quad \longrightarrow$$

$$V_1 = h^b W_1^r = \boxed{\mathrm{Enc}_{rx\beta+r\alpha\cdot\mathsf{sk}}(\ b + rx\ )}$$

$$v^{\mathsf{sk}} V_0^x V_1 = \boxed{\mathrm{Enc}_0(\ ax + b\ )}$$

rOLE from Paillier

S



a, b

sample r

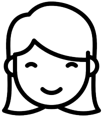
CRS (Mode II)

$$h = \boxed{\mathrm{Enc}_0(\ 1\ )}$$

$$w = \boxed{\mathrm{Enc}_\alpha(\ 0\ )}$$

$$W_0 = \boxed{\mathrm{Enc}_\beta(\ 0\ )}$$

R



x

sample sk

$$\longleftarrow\quad W_1 = w^{\mathsf{sk}} W_0^x = \boxed{\mathrm{Enc}_{x\beta+\alpha\cdot\mathsf{sk}}(\ x\ )}\quad\text{——}$$

$$v = w^r = \boxed{\mathrm{Enc}_{r\alpha}(\ 0\ )}$$

$$\text{——}\quad V_0 = h^a W_0^{-r} = \boxed{\mathrm{Enc}_{-r\beta}(\ a-r\ )}\quad\longrightarrow$$

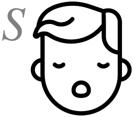
$$V_1 = h^b W_1^r = \boxed{\mathrm{Enc}_{rx\beta+r\alpha\cdot\mathsf{sk}}(\ b+rx\ )}$$

$$v^{\mathsf{sk}} V_0^x V_1 = \boxed{\mathrm{Enc}_0(\ ax+b\ )}$$

rOLE from Paillier

CRS (Mode II)

$$h = \boxed{\mathrm{Enc}_0(\ 1\ )}$$
$$w = \boxed{\mathrm{Enc}_\alpha(\ 0\ )}$$
$$W_0 = \boxed{\mathrm{Enc}_\beta(\ 0\ )}$$



a, b

sample r

x

sample sk

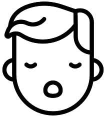
$$\longleftarrow \quad W_1 = w^{\mathsf{sk}} W_0^x = \boxed{\mathrm{Enc}_{x\beta+\alpha\cdot\mathsf{sk}}(\ 0\ )} \quad \text{———}$$

$$v = w^r = \boxed{\mathrm{Enc}_{r\alpha}(\ 0\ )}$$
$$\text{———} \quad V_0 = h^a W_0^{-r} = \boxed{\mathrm{Enc}_{-r\beta}(\ a - r\ )} \quad \longrightarrow$$
$$V_1 = h^b W_1^r = \boxed{\mathrm{Enc}_{rx\beta+r\alpha\cdot\mathsf{sk}}(\ b + rx\ )}$$

$$v^{\mathsf{sk}} V_0^x V_1 = \boxed{\mathrm{Enc}_0(\ ax + b\ )}$$

rOLE from Paillier

S



a, b

sample r

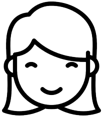
CRS (Mode II)

$$h = \boxed{\mathrm{Enc}_0(\ 1\ )}$$

$$w = \boxed{\mathrm{Enc}_\alpha(\ 0\ )}$$

$$W_0 = \boxed{\mathrm{Enc}_\beta(\ 0\ )}$$

R



x

sample sk

$$W_1 = w^{\mathsf{sk}} W_0^x = \boxed{\mathrm{Enc}_{x\beta+\alpha\cdot\mathsf{sk}}(\ 0\ )}$$

$$v = w^r = \boxed{\mathrm{Enc}_{r\alpha}(\ 0\ )}$$

$$V_0 = h^a W_0^{-r} = \boxed{\mathrm{Enc}_{-r\beta}(\ a\ )}$$

$$V_1 = h^b W_1^r = \boxed{\mathrm{Enc}_{rx\beta+r\alpha\cdot\mathsf{sk}}(\ b\ )}$$

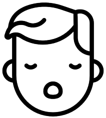
$$v^{\mathsf{sk}} V_0^x V_1 = \boxed{\mathrm{Enc}_0(\ ax+b\ )}$$

rOLE from Paillier

CRS (Mode II)

$$h = \boxed{\mathrm{Enc}_0(\ 1\ )}$$
$$w = \boxed{\mathrm{Enc}_\alpha(\ 0\ )}$$
$$W_0 = \boxed{\mathrm{Enc}_\beta(\ 0\ )}$$

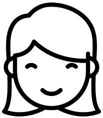
S



a, b

sample r

R



x

sample sk

$$\longleftarrow \quad W_1 = w^{\mathrm{sk}} W_0^x = \boxed{\mathrm{Enc}_{x\beta+\alpha\cdot\mathrm{sk}}(\ 0\ )} \quad \text{———}$$

$$v = w^r = \boxed{\mathrm{Enc}_{r\alpha}(\ 0\ )}$$
$$\text{———} \quad V_0 = h^a W_0^{-r} = \boxed{\mathrm{Enc}_{-r\beta}(\ a\ )} \quad \longrightarrow$$
$$V_1 = h^b W_1^r = \boxed{\mathrm{Enc}_{rx\beta+r\alpha\cdot\mathrm{sk}}(\ b\ )}$$

$$v^{\mathrm{sk}} V_0^x V_1 = \boxed{\mathrm{Enc}_0(\ ax+b\ )}$$

"Strong" UC-security requires a machenism to detect malicious sender

Our Results

- **(!$\exists$ IT rNISC/rOT)** There is no information-theoretical reusable NISC protocol in rOT-hybrid model.
- **(IT rNISC/rOLE for arithmetic $\mathbf{NC}^1$)** Information-theoretical UC-secure reusable NISC protocol for any arithmetic $\mathbf{NC}^1$ circuit or arithmetic branching program in rOLE-hybrid model.
- **(IT rNIZK/rOLE)** Information-theoretical UC-secure reusable NIZK protocol in rOLE-hybrid model; $O(1)$ calls per gate.
- **Previous two + Garbled circuit $\rightarrow$ (rNISC/rOLE)** UC-secure reusable NISC for general circuits; IT secure against sender; poly(λ) calls per gate.
- **(rOLE protocol from Paillier)** UC-secure reusable 2-message OLE protocol in CRS model; one-side IT secure; c.c. $O(1)$ group elements per call.

Our Results

- **rNISC** in CRS model assuming the security of Paillier encryption.
- **rNIZK** in CRS model assuming the security of Paillier encryption. c.c. $O(1)$ group elements per gate.
- **Statistical designated-verifier NIZK argument** for NP in CRS model assuming Paillier.
- Push cryptograph to offline phase.
  In offline phase: prepare random $((a, b), (x, ax + b))$;
  In online phase: consume the prepared randomness.

Our Results

- **rNISC** in CRS model assuming the security of Paillier encryption.
- **rNIZK** in CRS model assuming the security of Paillier encryption. c.c. $O(1)$ group elements per gate.
- **Statistical designated-verifier NIZK argument** for NP in CRS model assuming Paillier.
- Push cryptograph to offline phase. In offline phase: prepare random $((a, b), (x, ax + b))$; In online phase: consume the prepared randomness.

Our Results

- **rNISC** in CRS model assuming the security of Paillier encryption.
- **rNIZK** in CRS model assuming the security of Paillier encryption. c.c. $O(1)$ group elements per gate.
- **Statistical designated-verifier NIZK argument** for NP in CRS model assuming Paillier.
- Push cryptograph to offline phase.
  In offline phase: prepare random $((a, b), (x, ax + b))$;
  In online phase: consume the prepared randomness.