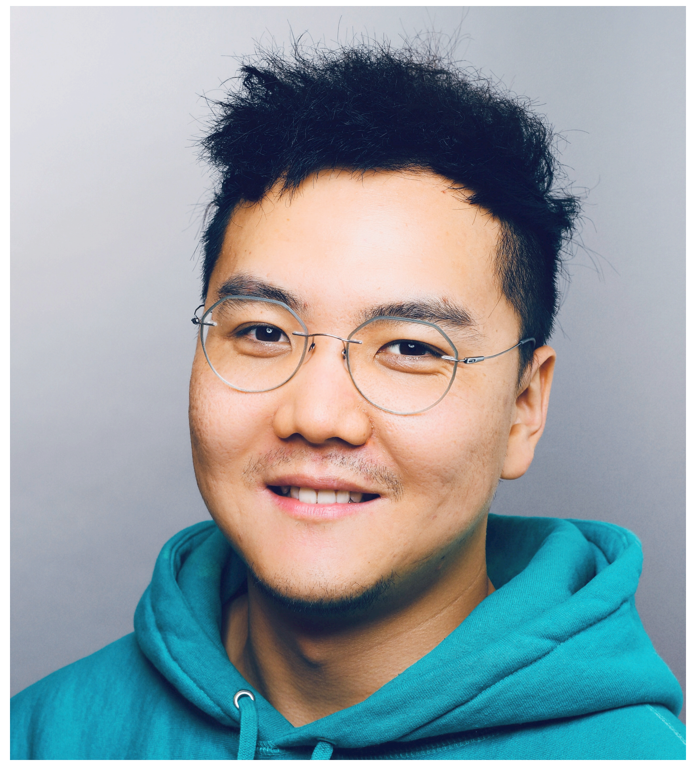
Enhanced Trapdoor Hashing from DDH and DCR

EUROCRYPT 2025



Geoffroy Couteau
CNRS, IRIF
Universitè Paris Citè

Aditya Hegde
JHU

Sihang Pu
CNRS, IRIF
Universitè Paris Citè

Setting: Two-Round Sender-Receiver Computation

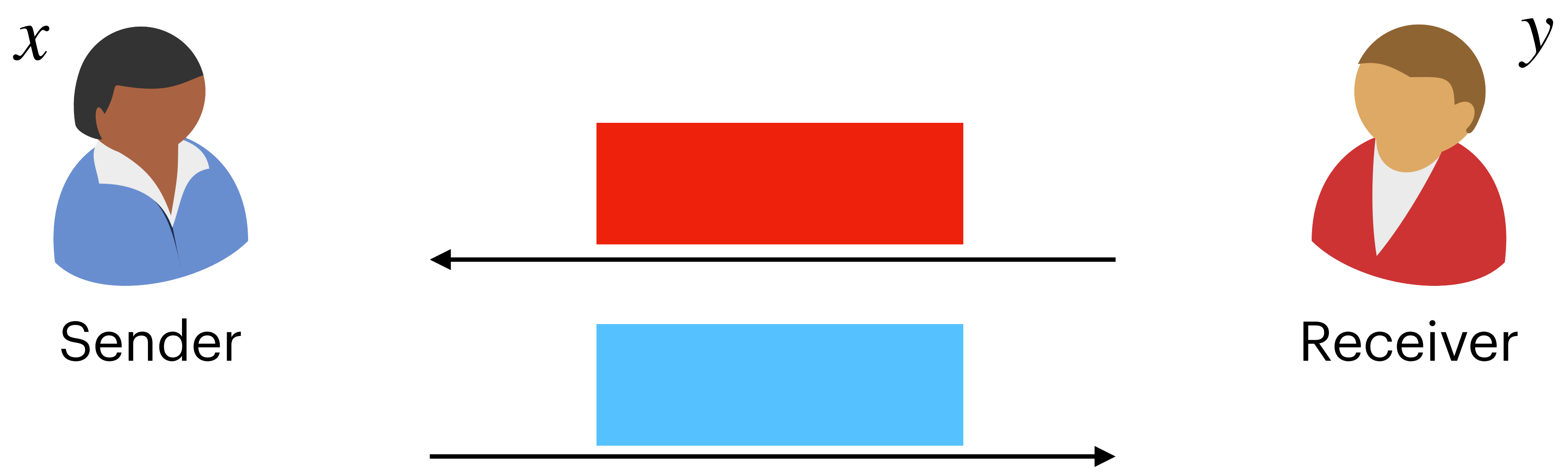
Public function F

Setting: Two-Round Sender-Receiver Computation

Public function F

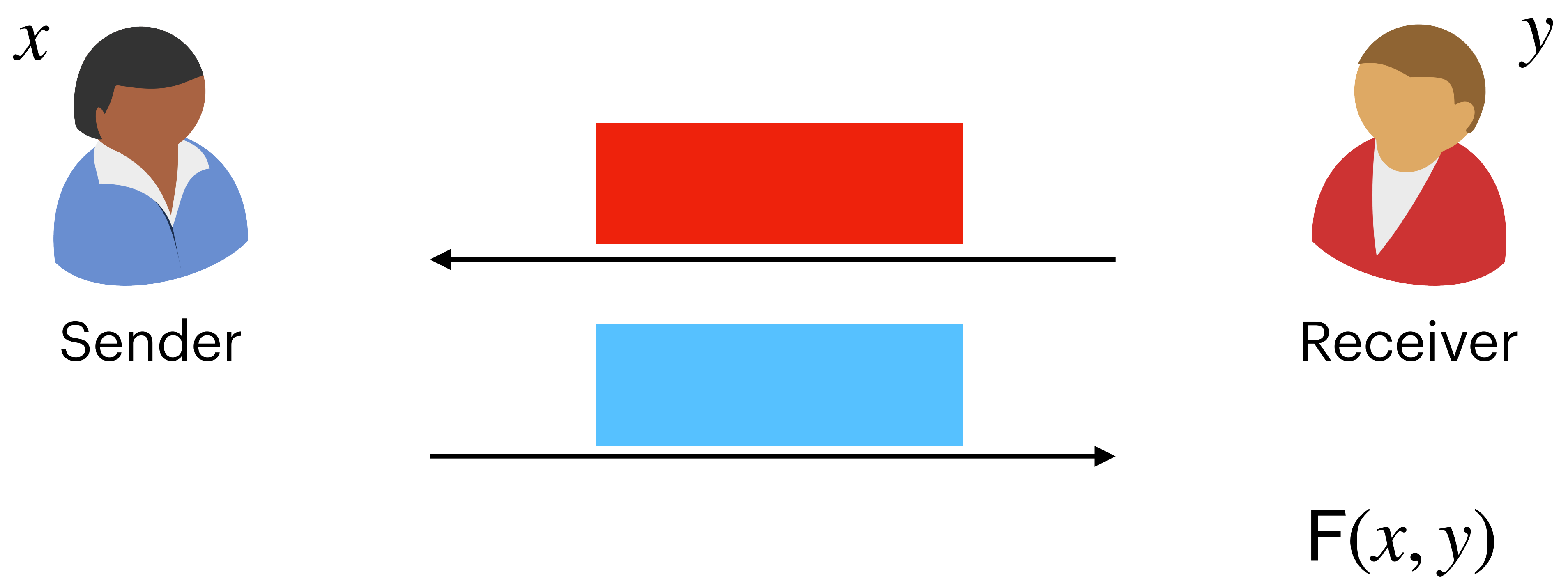
Setting: Two-Round Sender-Receiver Computation

Public function F



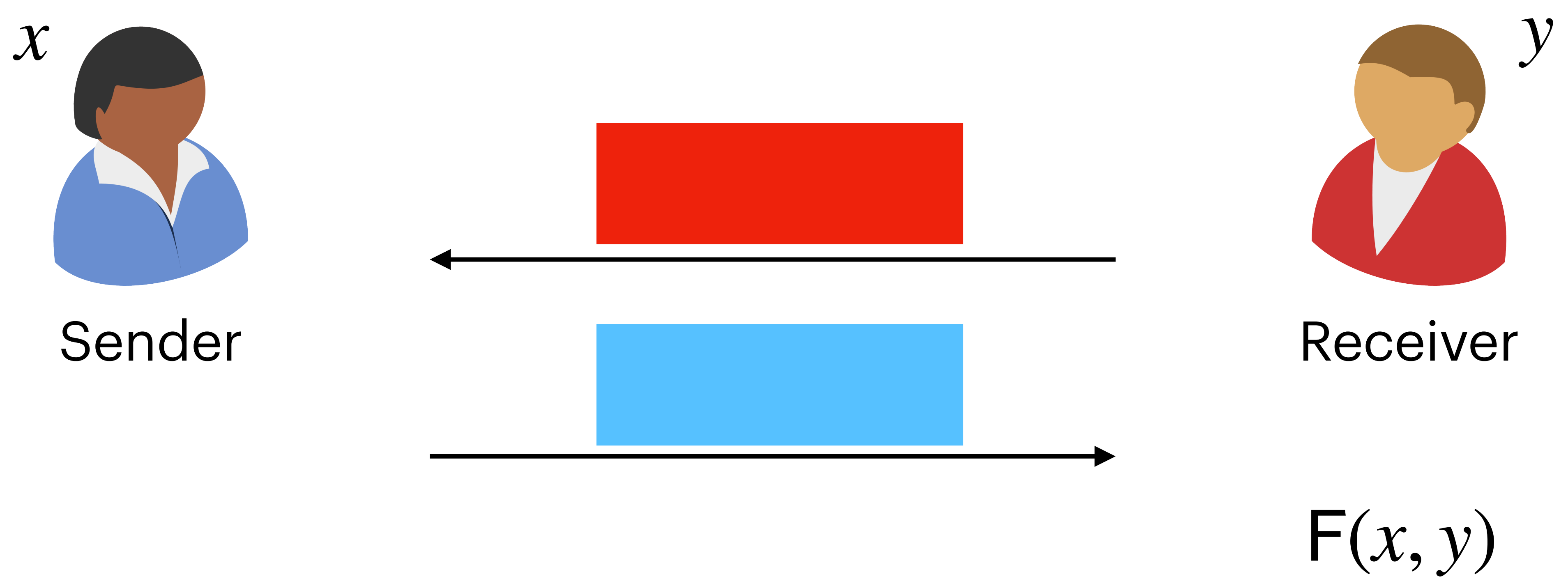
Setting: Two-Round Sender-Receiver Computation

Public function F



Setting: Two-Round Sender-Receiver Computation

Public function F

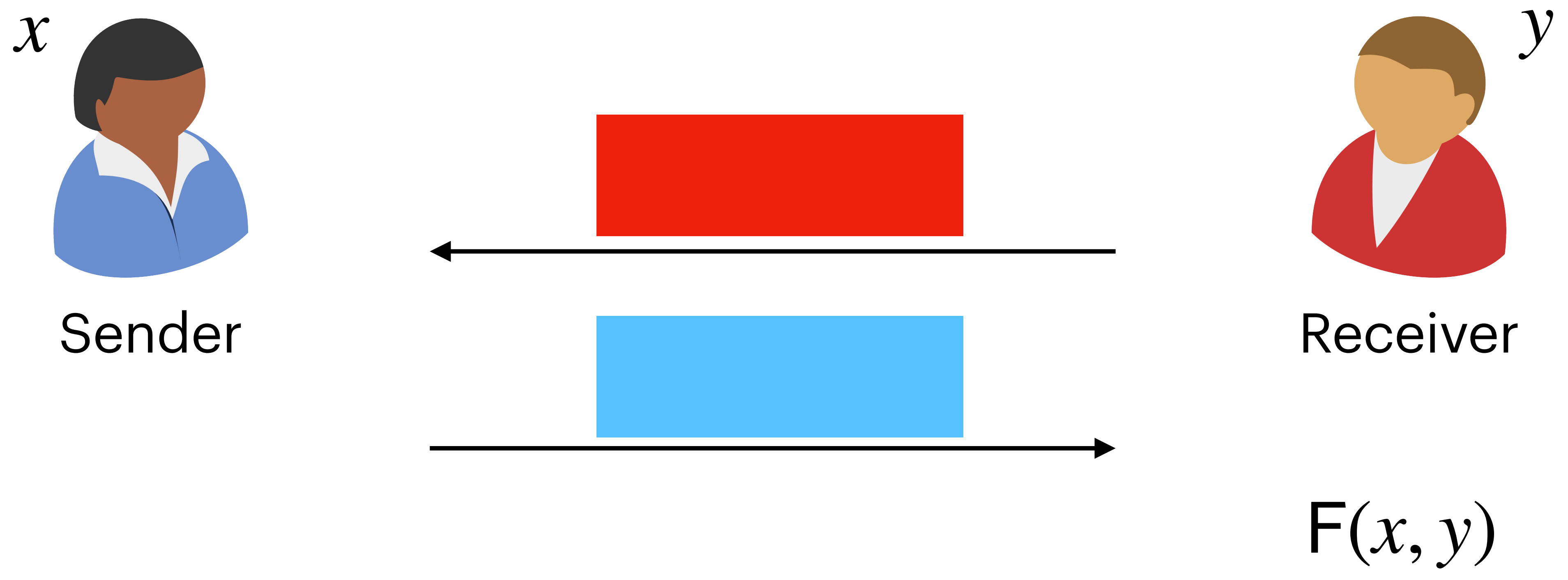


Privacy:  does not learn y

 does not learn x

Setting: Two-Round Sender-Receiver Computation

Public function F

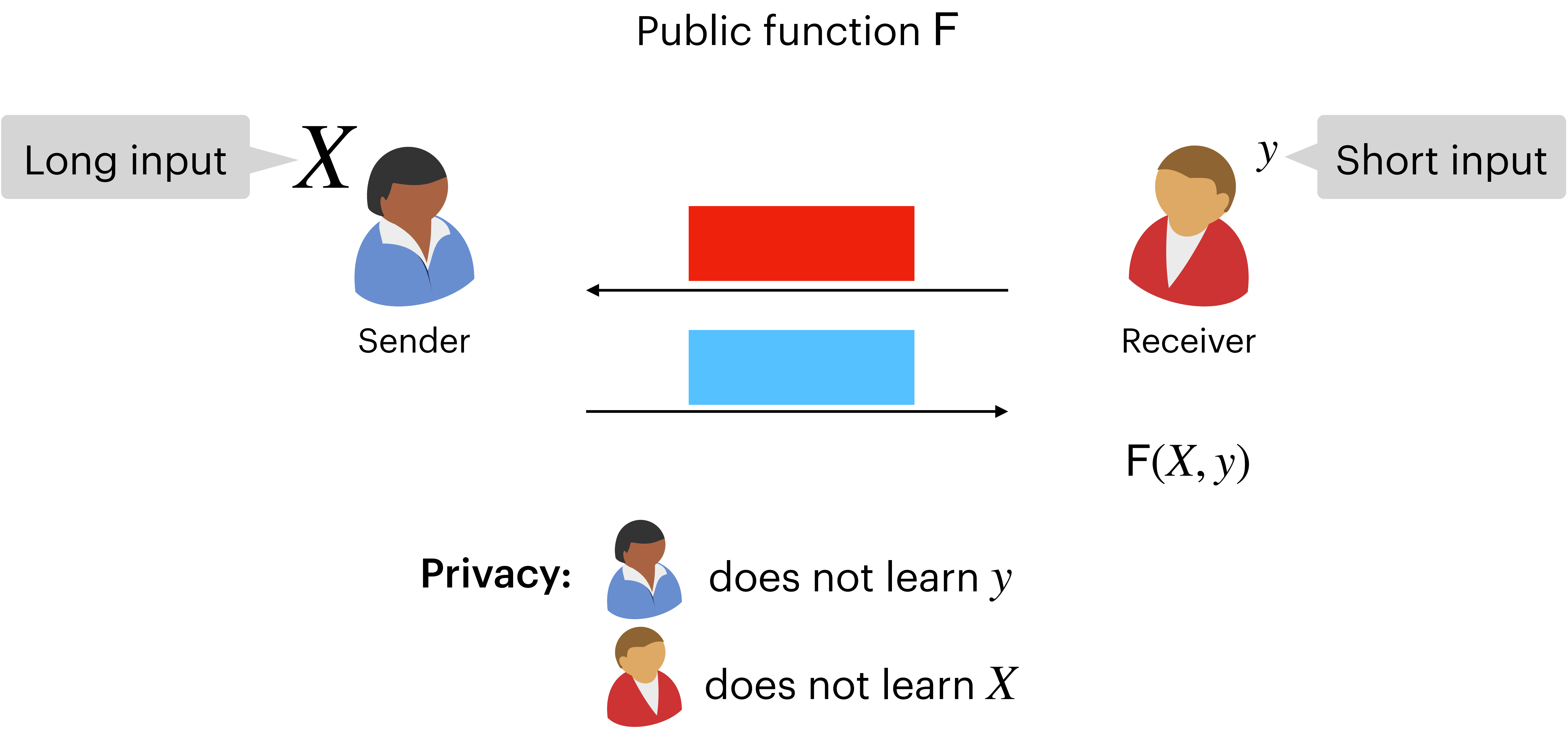


Privacy: does not learn y

does not learn x

What is the **minimum communication** cost of **semi-honest** secure protocols?

Setting: Two-Round Sender-Receiver Computation



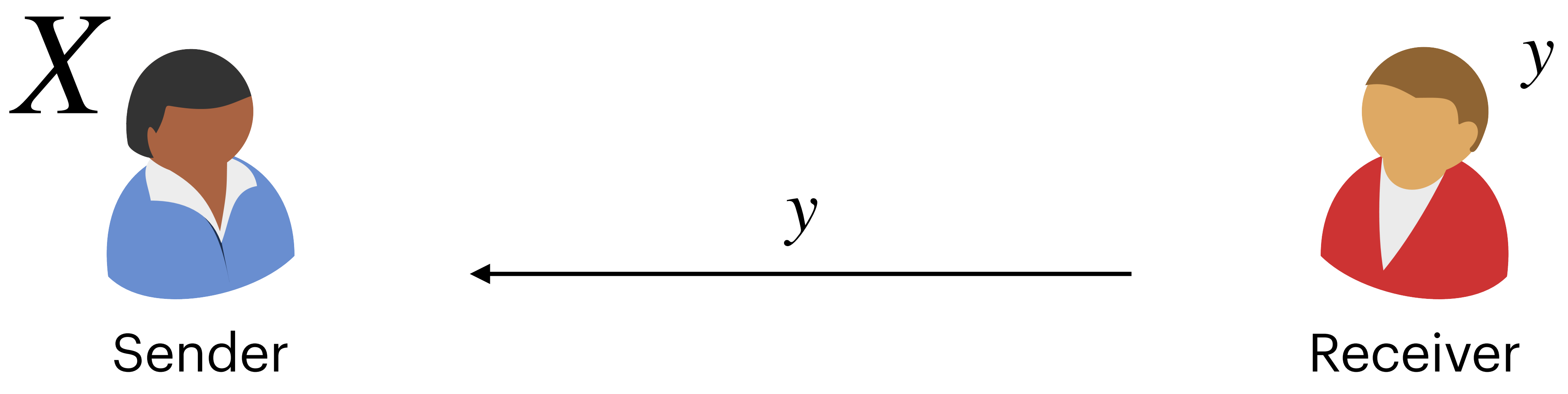
What is the **minimum communication** cost of **semi-honest** secure protocols?

Ideal World Two-Round Sender-Receiver Computation

Public function F

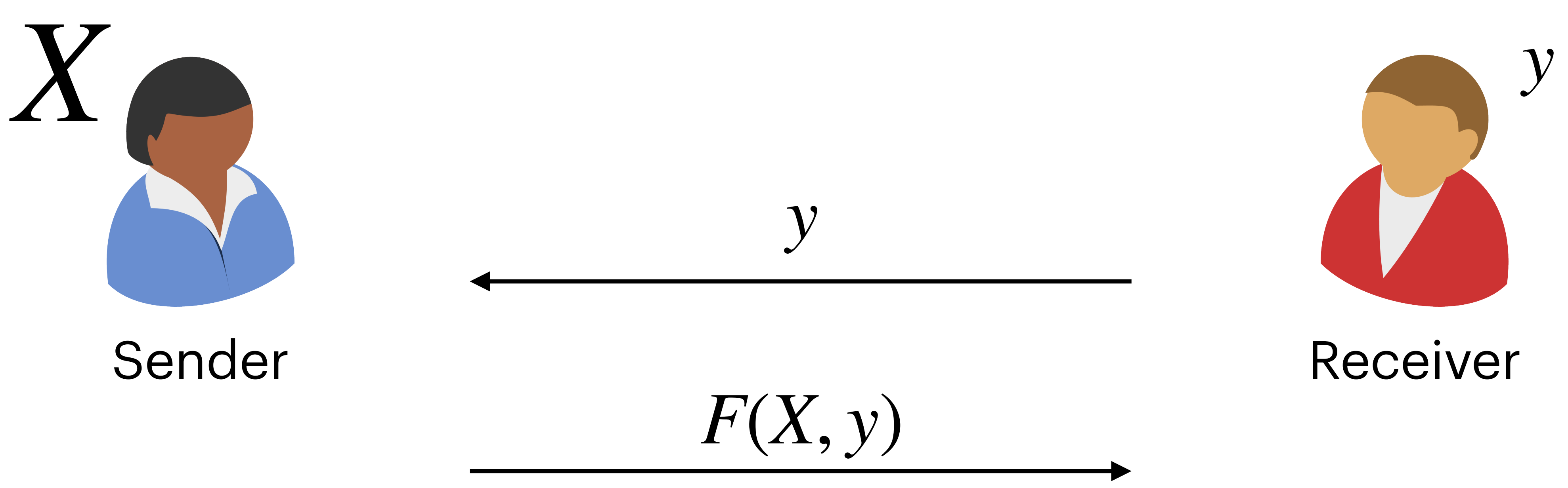
Ideal World Two-Round Sender-Receiver Computation

Public function F



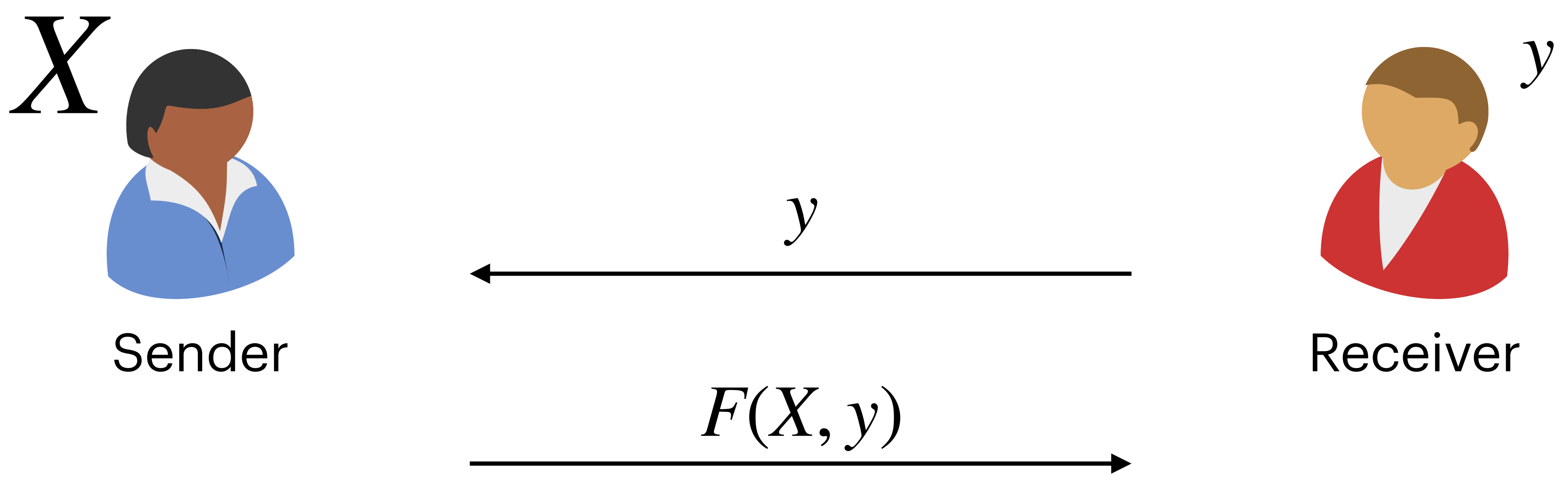
Ideal World Two-Round Sender-Receiver Computation

Public function F



Ideal World Two-Round Sender-Receiver Computation

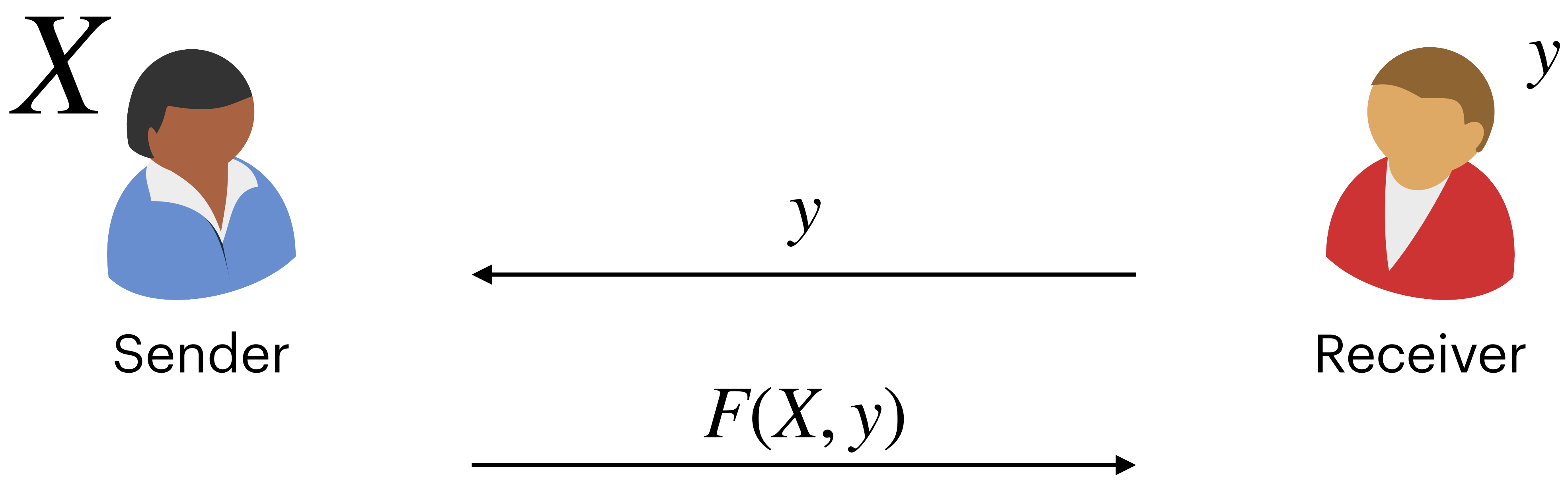
Public function F



Total communication: $|y| + |F(X, y)|$

Ideal World Two-Round Sender-Receiver Computation

Public function F



Total communication: $|y| + |F(X, y)|$

Can secure protocols achieve similar efficiency?

Trapdoor Hash Functions (TDH)

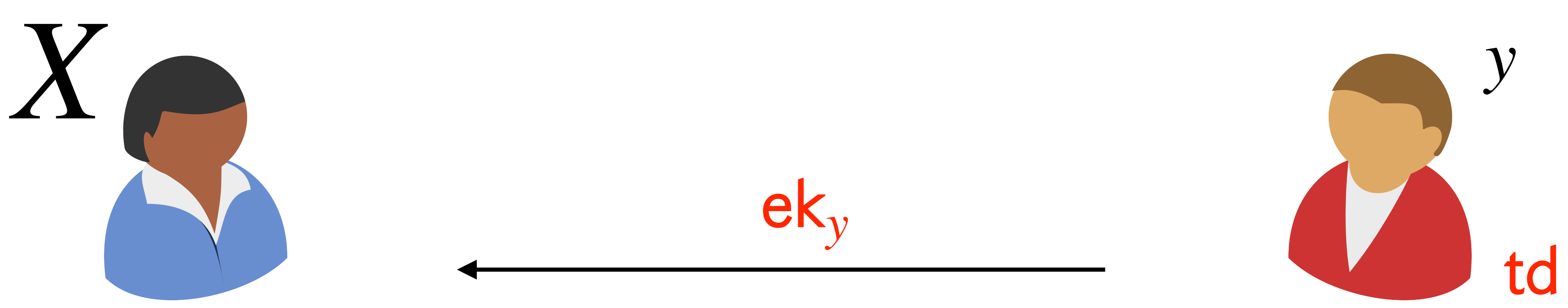
[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

Public function F

Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

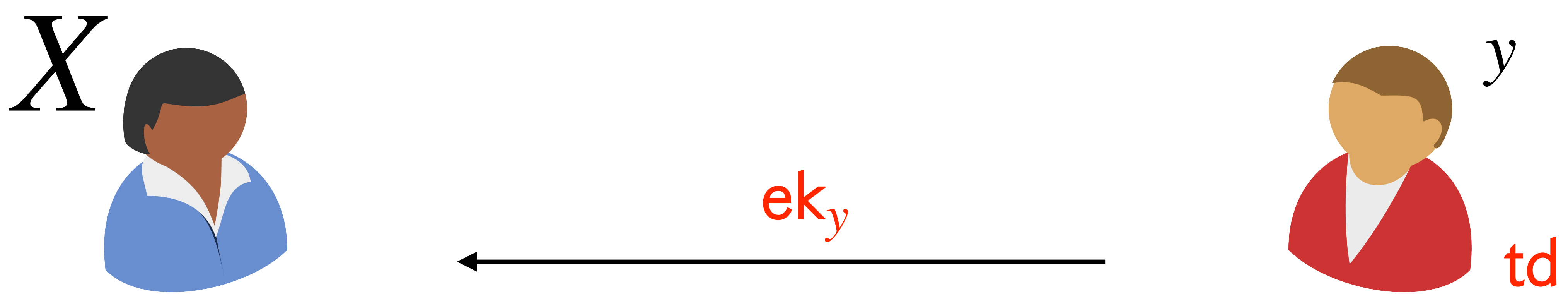
Public function F



Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

Public function F

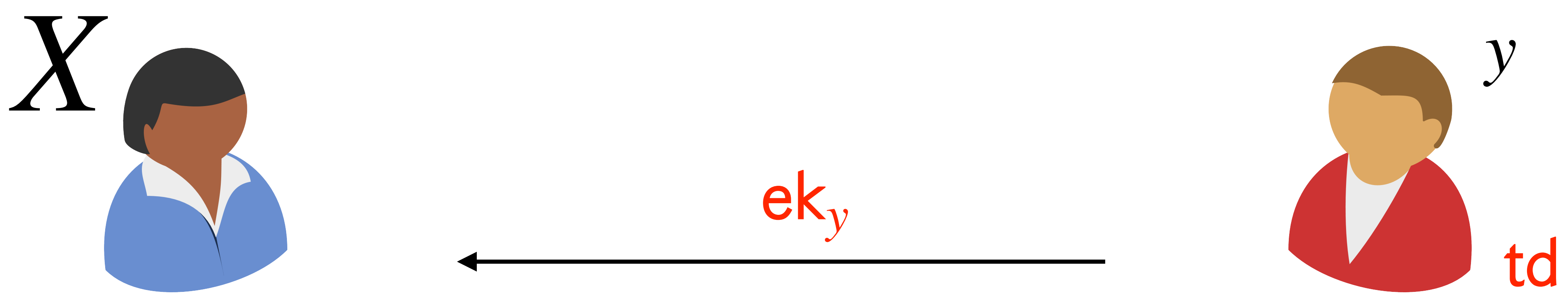


$h \leftarrow \mathsf{Hash}(X)$

Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

Public function F



$h \leftarrow \mathsf{Hash}(X)$

$e \leftarrow \mathsf{Encode}(\mathsf{ek}_y, X)$

Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

Public function F

X 

 y

td

$\xleftarrow{\mathsf{ek}_y}$

$h \leftarrow \mathsf{Hash}(X)$

$e \leftarrow \mathsf{Encode}(\mathsf{ek}_y, X)$

$\xrightarrow{h,\ e}$

$F(X, y) \leftarrow \mathsf{Decode}(\mathsf{td}, h, e)$

Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

Public function F

X 

 y

td

$\xleftarrow{\mathsf{ek}_y}$

$h \leftarrow \text{Hash}(X)$

$e \leftarrow \text{Encode}(\mathsf{ek}_y, X)$

$\xrightarrow{h,\ e}$

$F(X, y) \leftarrow \text{Decode}(\mathsf{td}, h, e)$

Privacy: ek_y hides y

(h, e) hides X

Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

Public function F

X 

ek_y $\longleftarrow$

 y td

$h \leftarrow \mathsf{Hash}(X)$

$e \leftarrow \mathsf{Encode}(\mathsf{ek}_y, X)$

h, e $\longrightarrow$

$F(X, y) \leftarrow \mathsf{Decode}(\mathsf{td}, h, e)$

Privacy: ek_y hides y

(h, e) hides X

Efficiency: h is small i.e., $|h| = o(|X|) \cdot \mathsf{poly}(\lambda)$

Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

Public function F

X

ek_y

$\longleftarrow$

y

td

$h \leftarrow \mathsf{Hash}(X)$

$e \leftarrow \mathsf{Encode}(\mathsf{ek}_y, X)$

h, e

$\longrightarrow$

$F(X, y) \leftarrow \mathsf{Decode}(\mathsf{td}, h, e)$

Privacy: ek_y hides y

(h, e) hides X

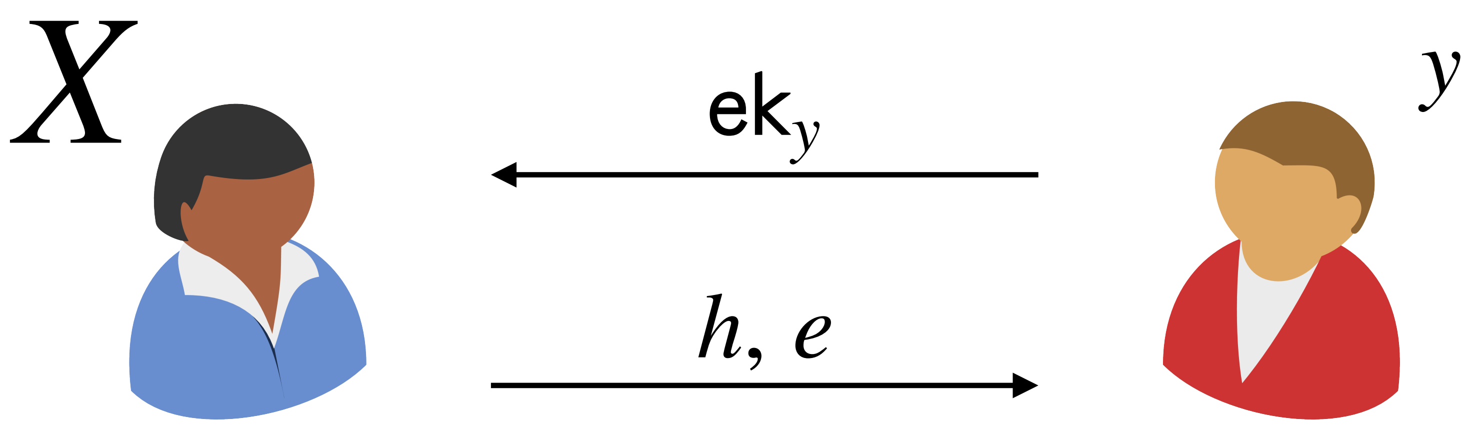
Efficiency: h is small i.e., $|h| = o(|X|) \cdot \mathsf{poly}(\lambda)$

e has high rate i.e., $|e| \approx |F(X, y)|$

Rate: $\dfrac{|F(X, y)|}{|e|}$

Trapdoor Hash Functions (TDH)

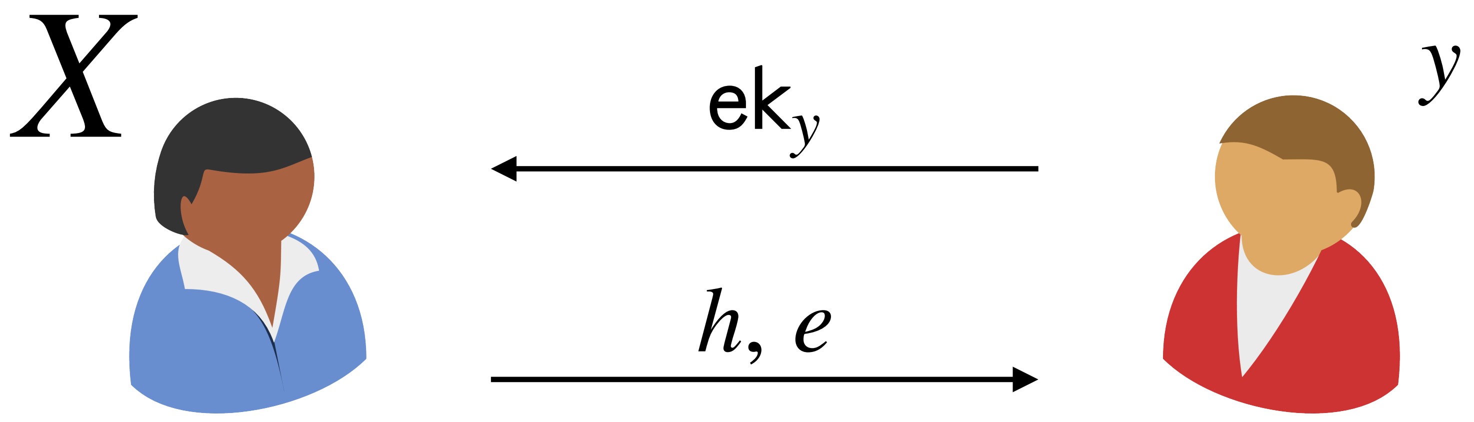
[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]



Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

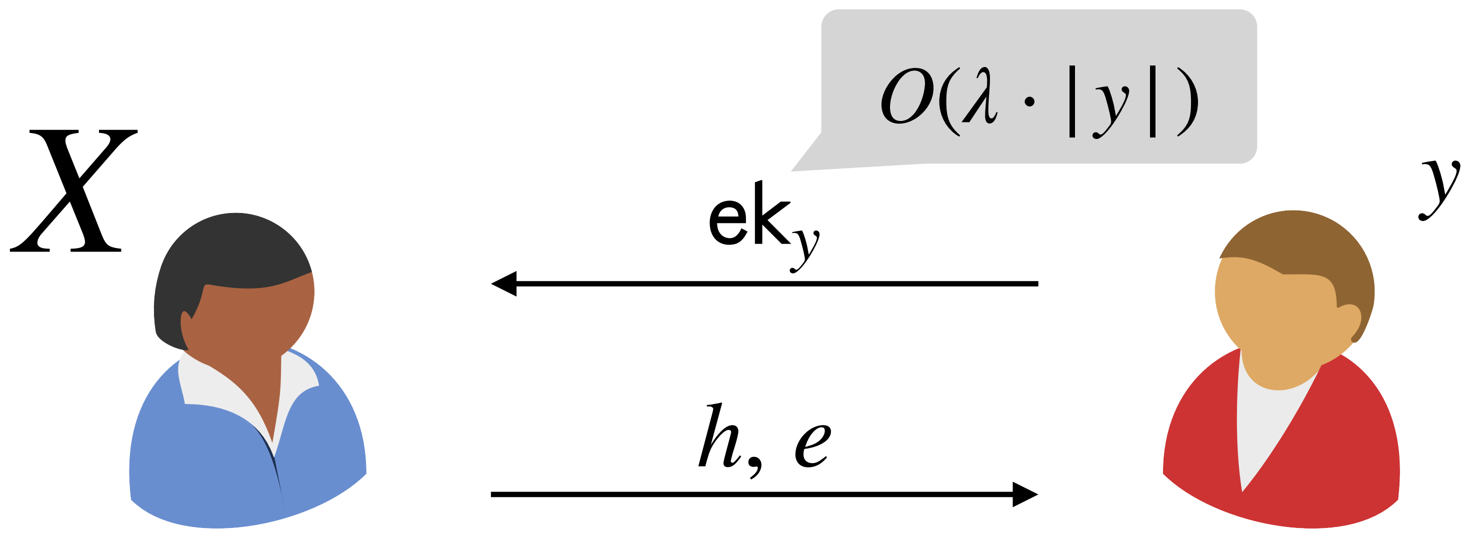
$$F(X, y) = \sum_i x_i \cdot y_i$$



Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

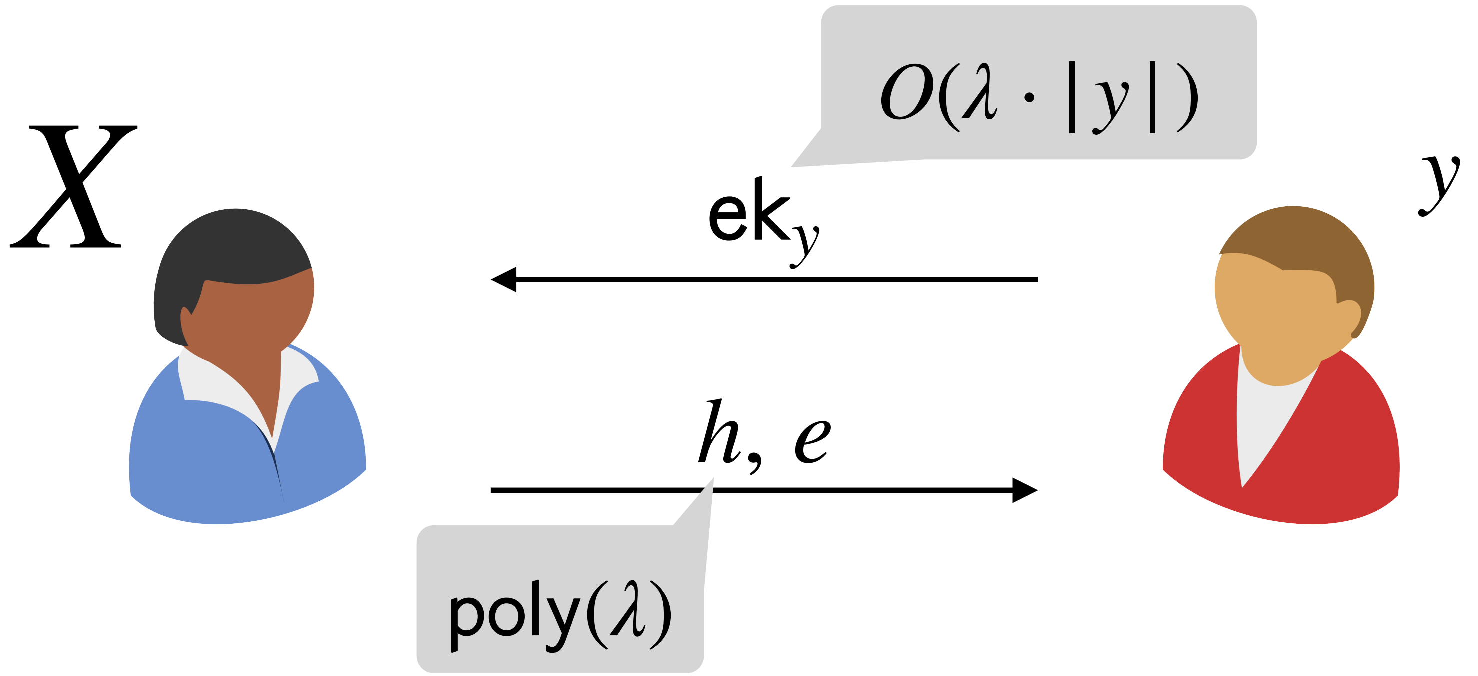
$$F(X, y) = \sum_i x_i \cdot y_i$$



Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

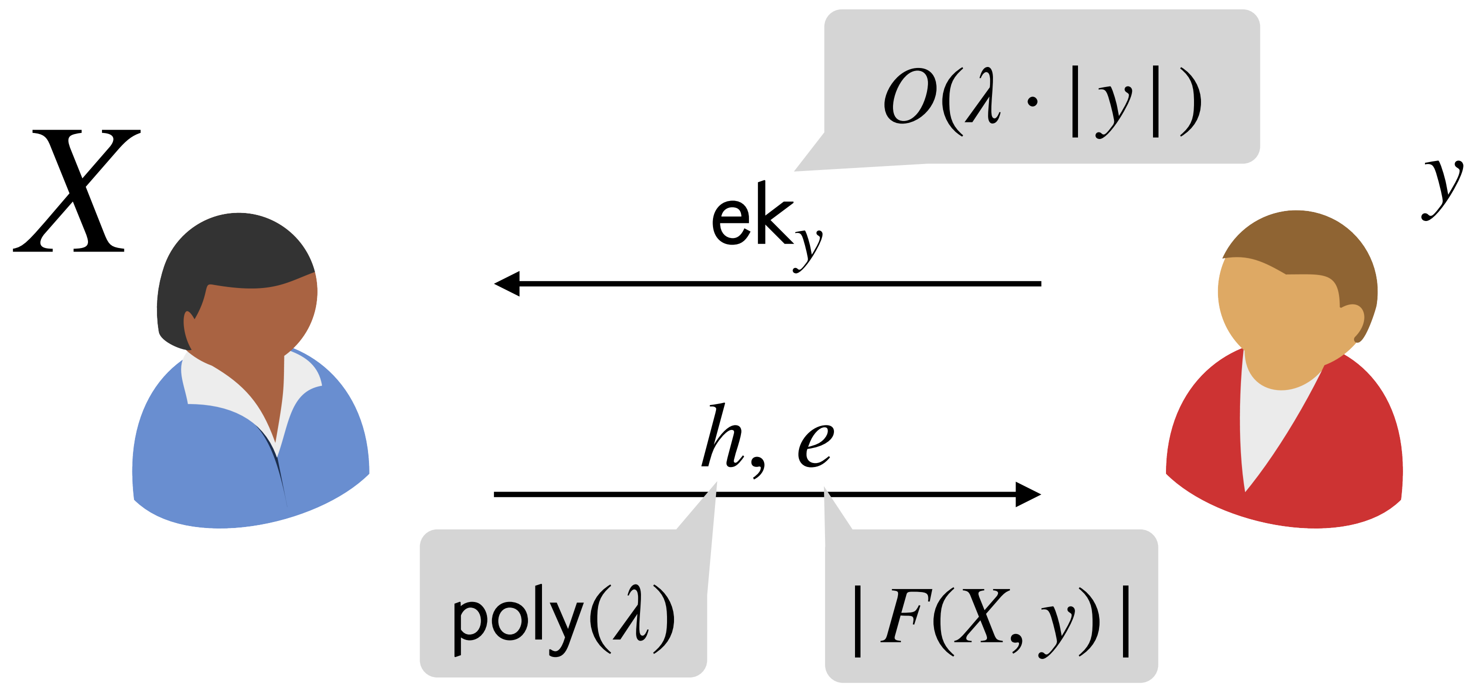
$$F(X, y) = \sum_i x_i \cdot y_i$$



Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

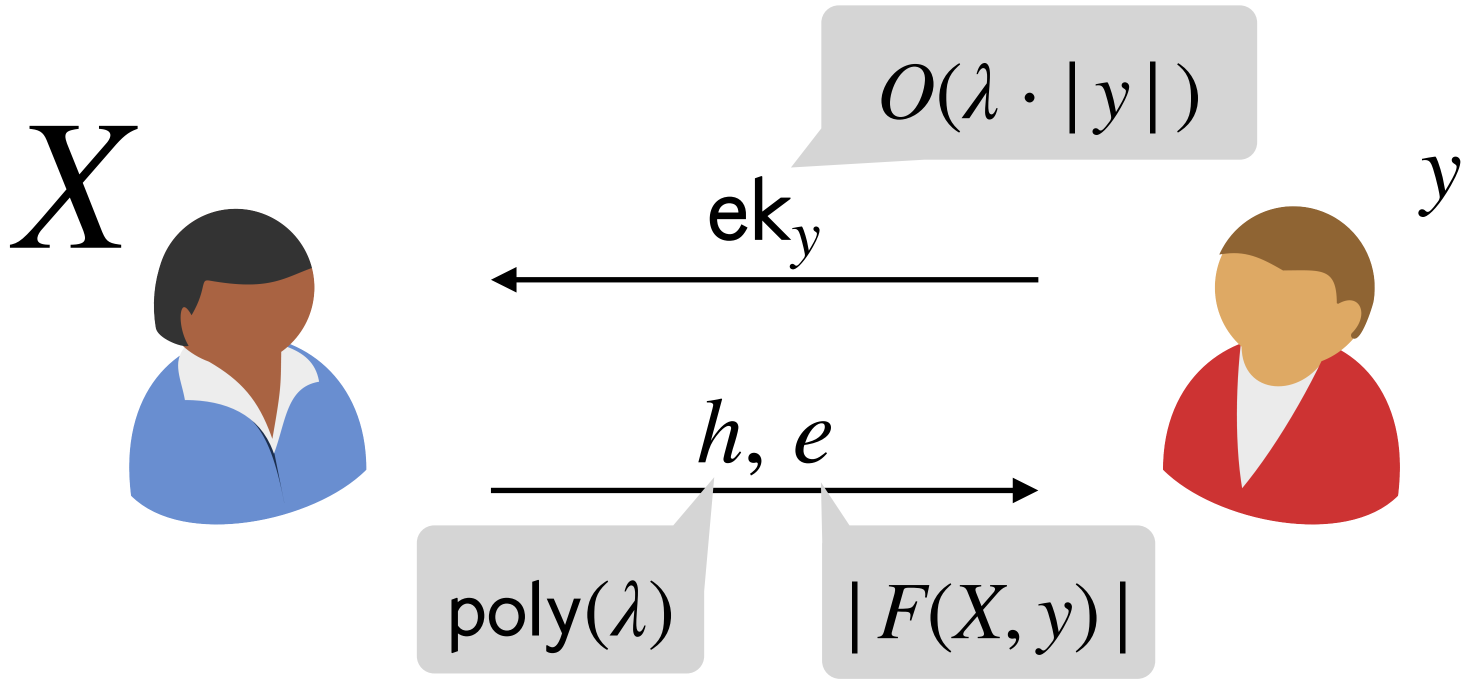
$$F(X, y) = \sum_i x_i \cdot y_i$$



Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

$$F(X, y) = \sum_i x_i \cdot y_i$$

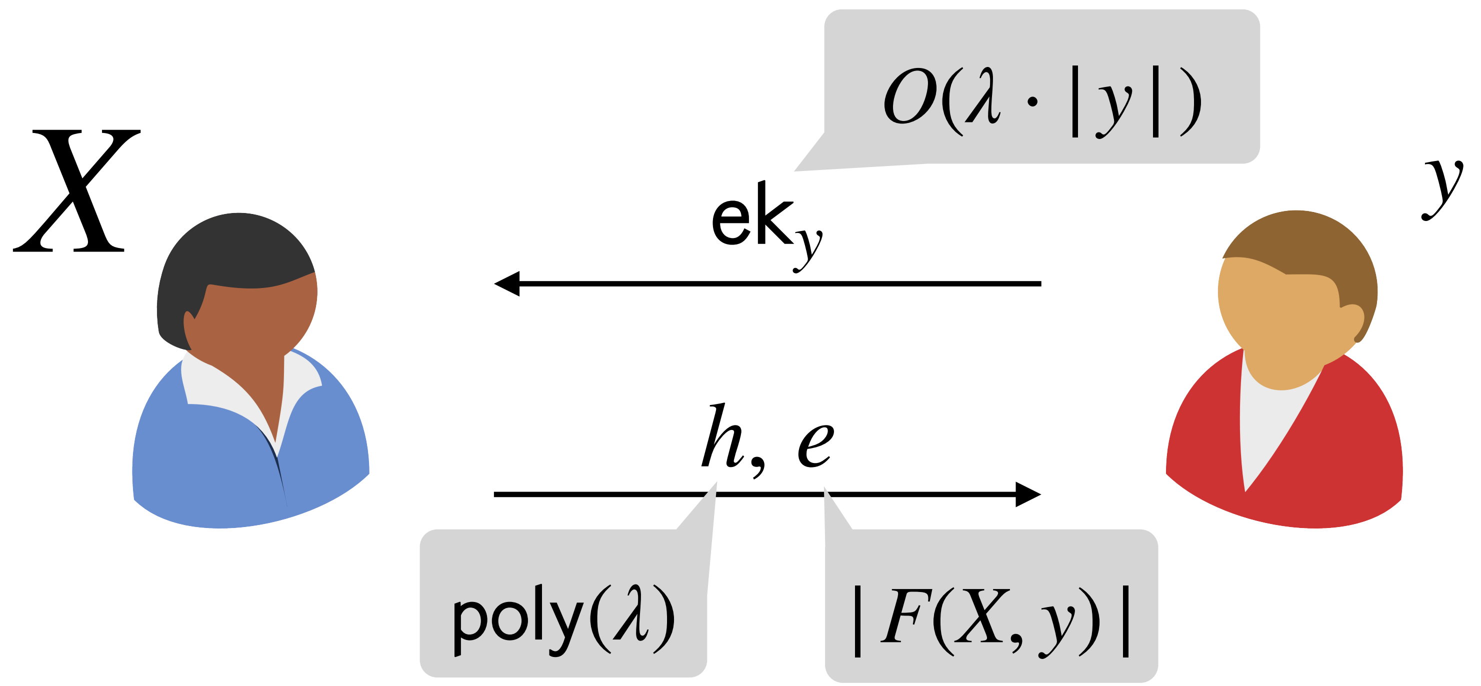


Assumptions: DCR, DDH, QR, LWE

Trapdoor Hash Functions (TDH)

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

$$F(X, y) = \sum_i x_i \cdot y_i$$



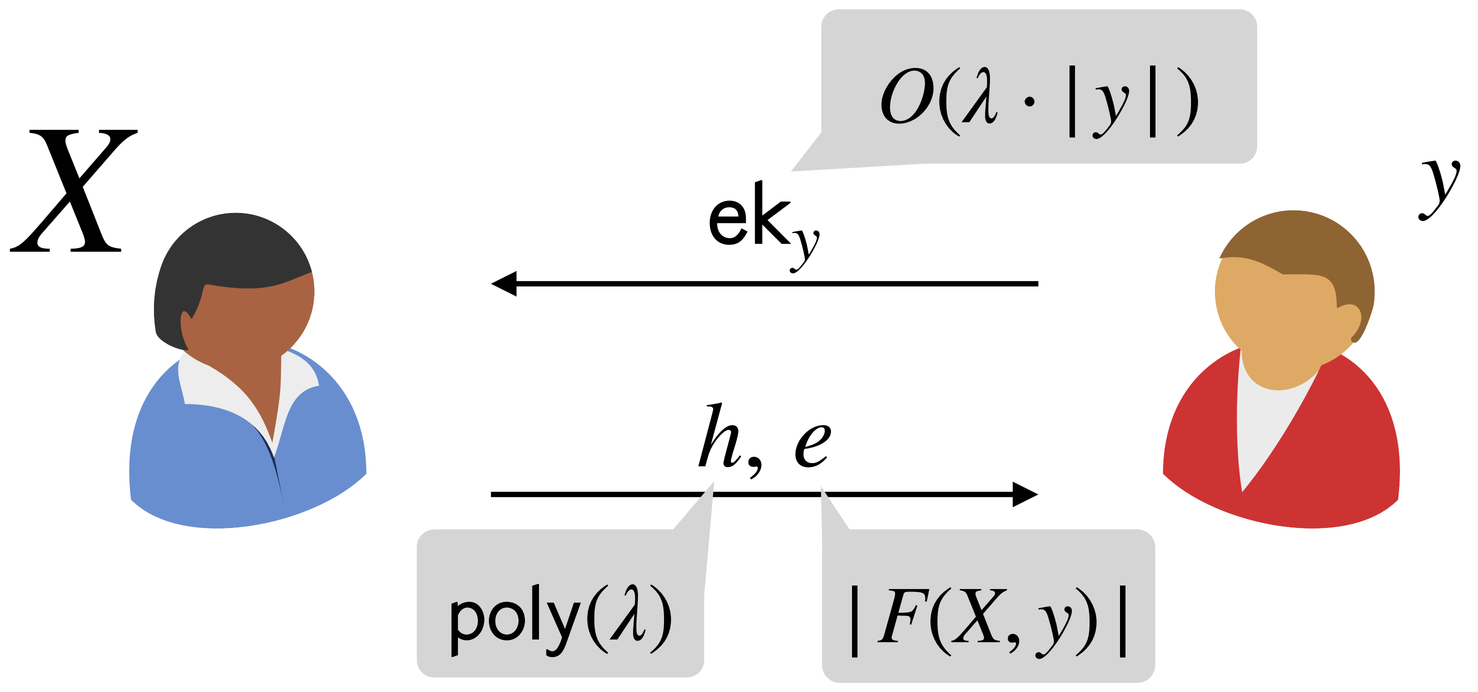
Assumptions: DCR, DDH, QR, LWE

Can we improve the functionality of TDH from group-based assumptions?

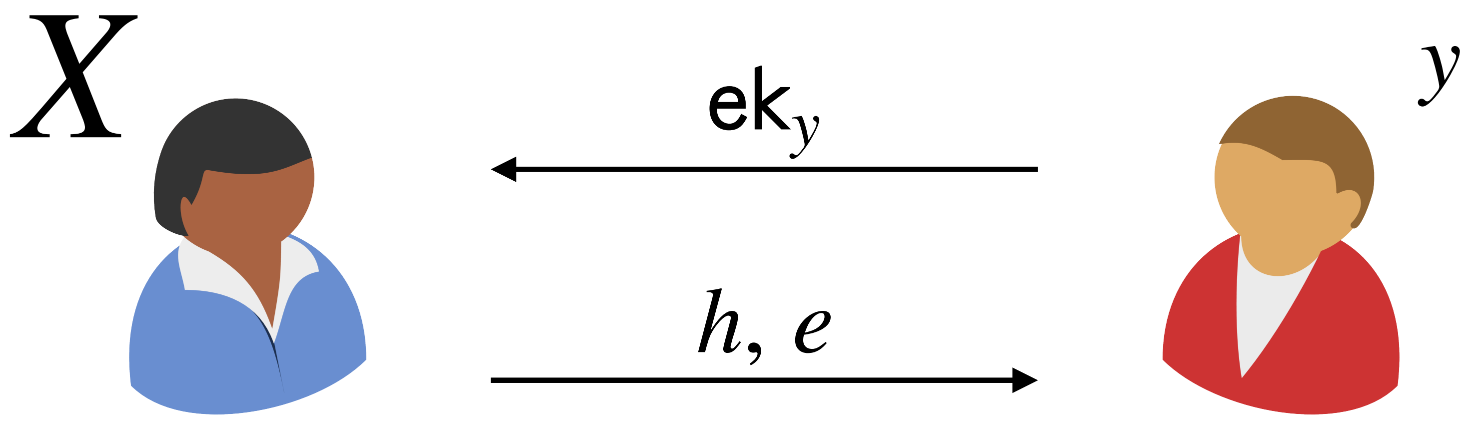
Enhanced Trapdoor Hash Functions from DDH and DCR

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

$$F(X, y) = \sum_i x_i \cdot y_i$$



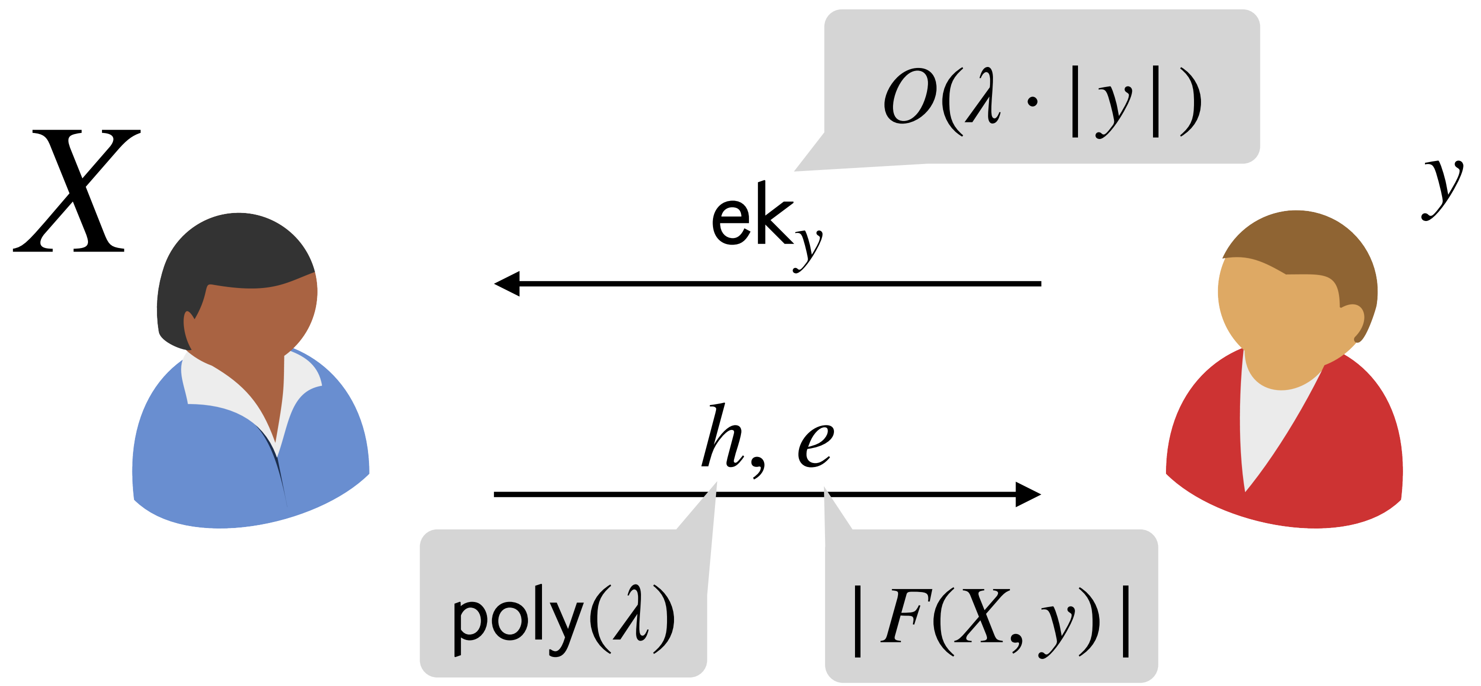
This work



Enhanced Trapdoor Hash Functions from DDH and DCR

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

$$F(X, y) = \sum_i x_i \cdot y_i$$



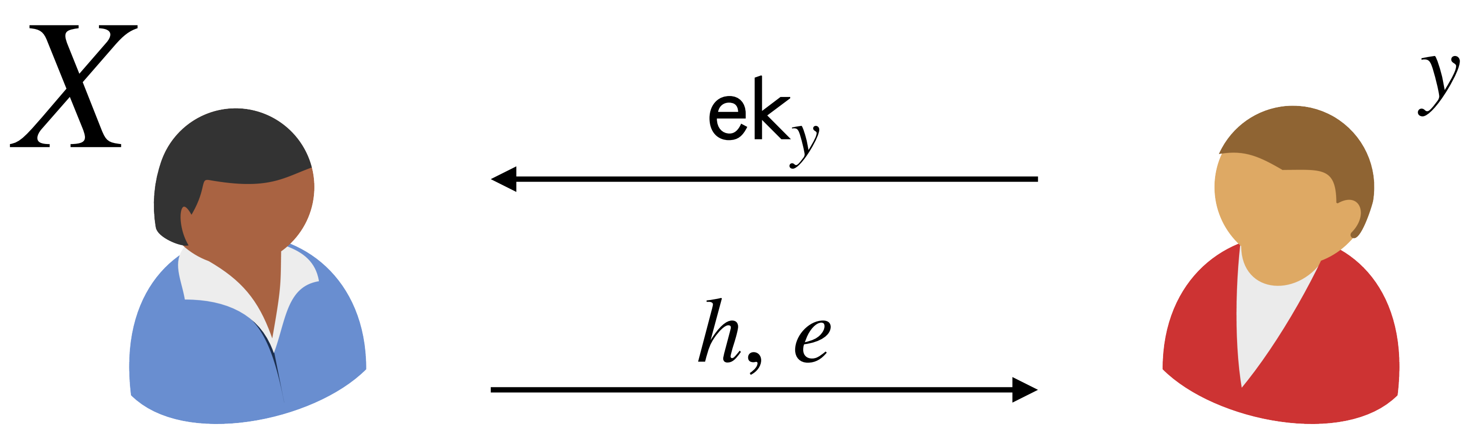
Expressivity

Supports computing Bilinear-NC^1 programs

This work

$$F(X, y) = \sum_{i=1}^{n} f_i(X) \cdot g_i(y)$$

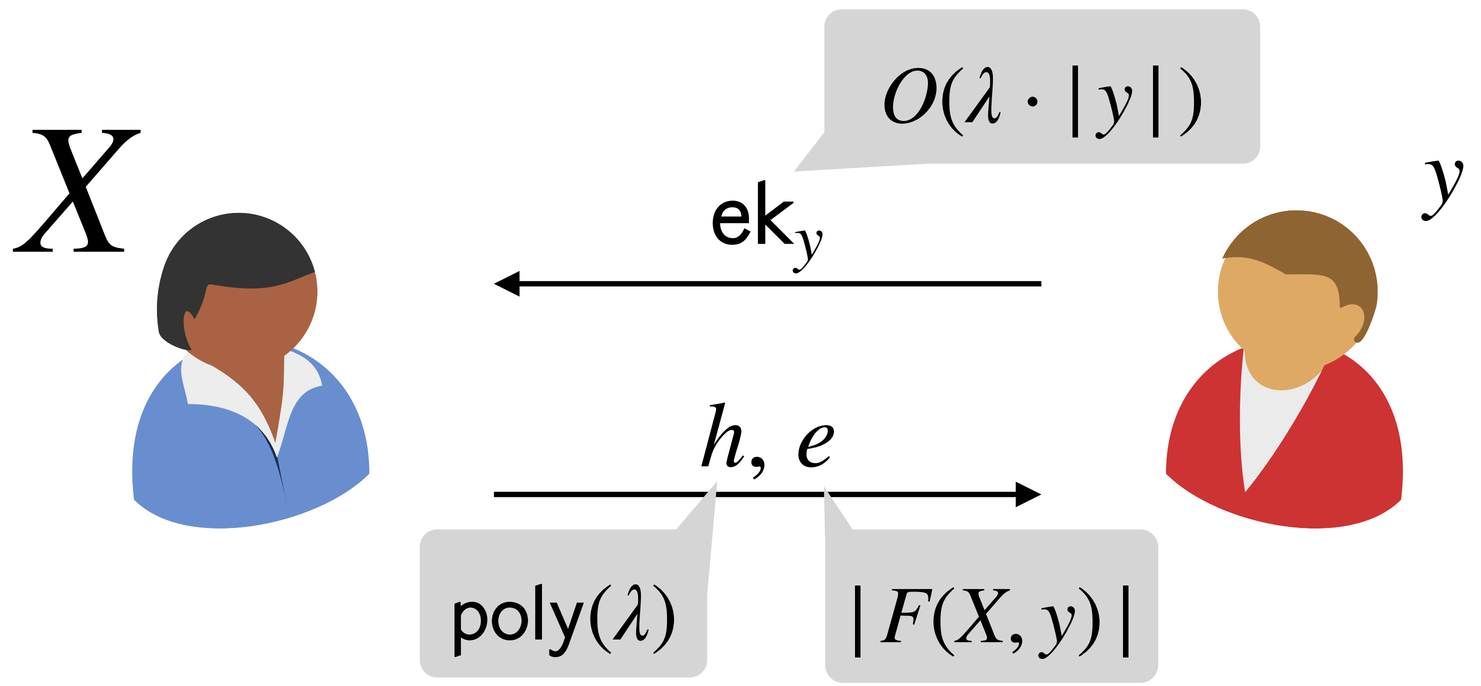
NC^1



Enhanced Trapdoor Hash Functions from DDH and DCR

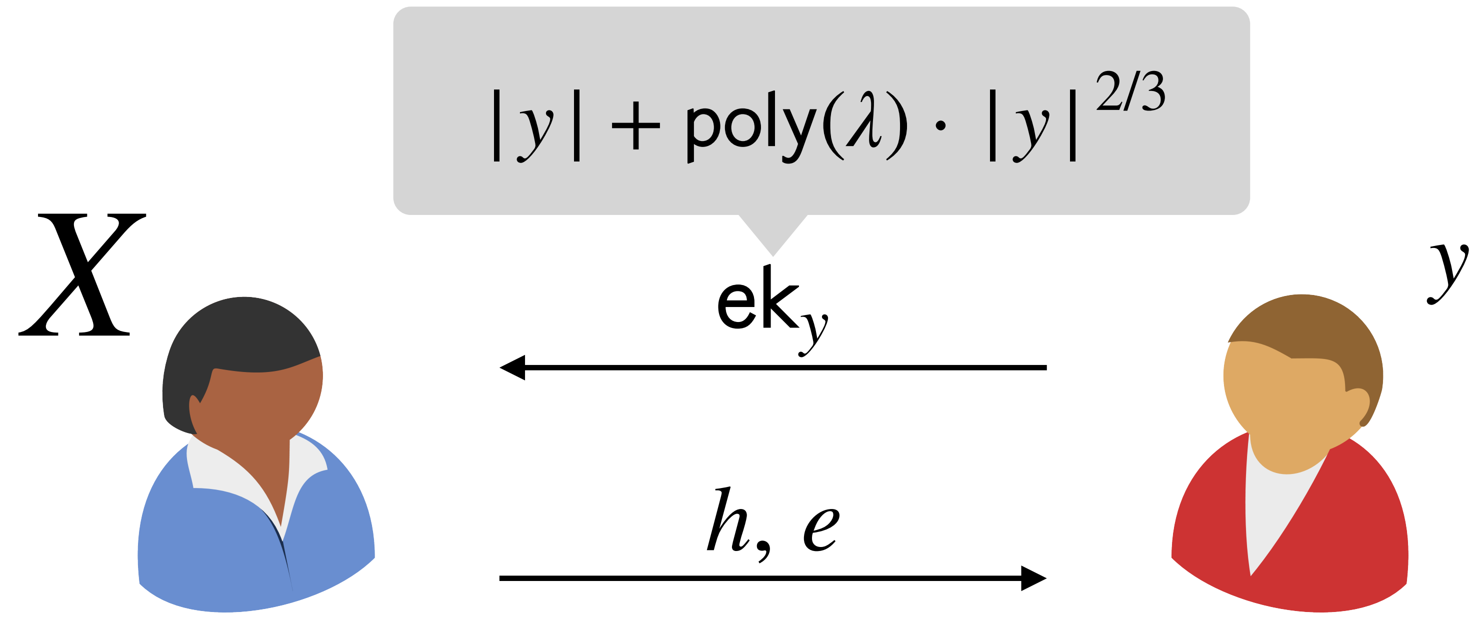
[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

$$F(X, y) = \sum_i x_i \cdot y_i$$



This work

$$F(X, y) = \sum_{i=1}^{n} f_i(X) \cdot g_i(y)$$



Expressivity

Supports computing Bilinear-NC^1 programs

Compactness

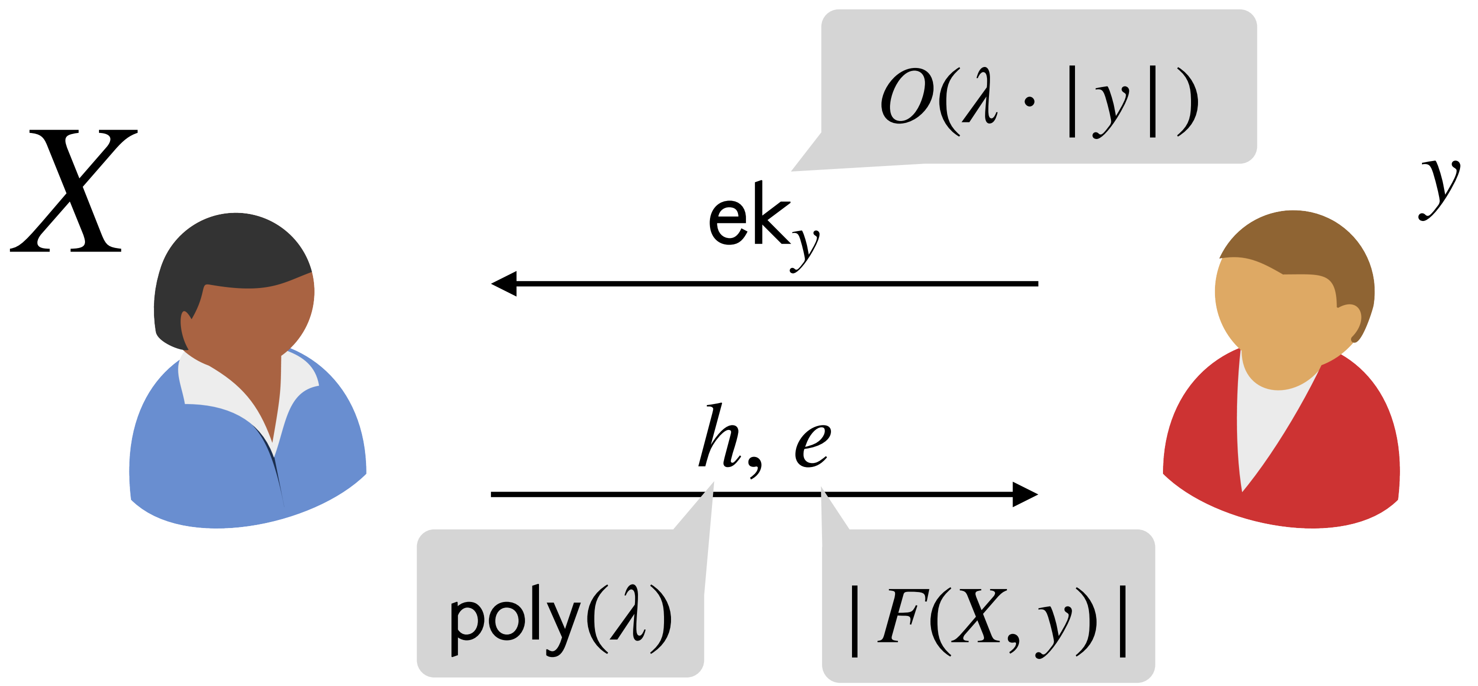
Encoding keys of size $|y|(1 + o(1))$

Enhanced Trapdoor Hash Functions from DDH and DCR

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

This work

$$F(X, y) = \sum_i x_i \cdot y_i$$



Expressivity

Supports computing Bilinear-NC^1 programs

Compactness

Encoding keys of size $|y|(1 + o(1))$

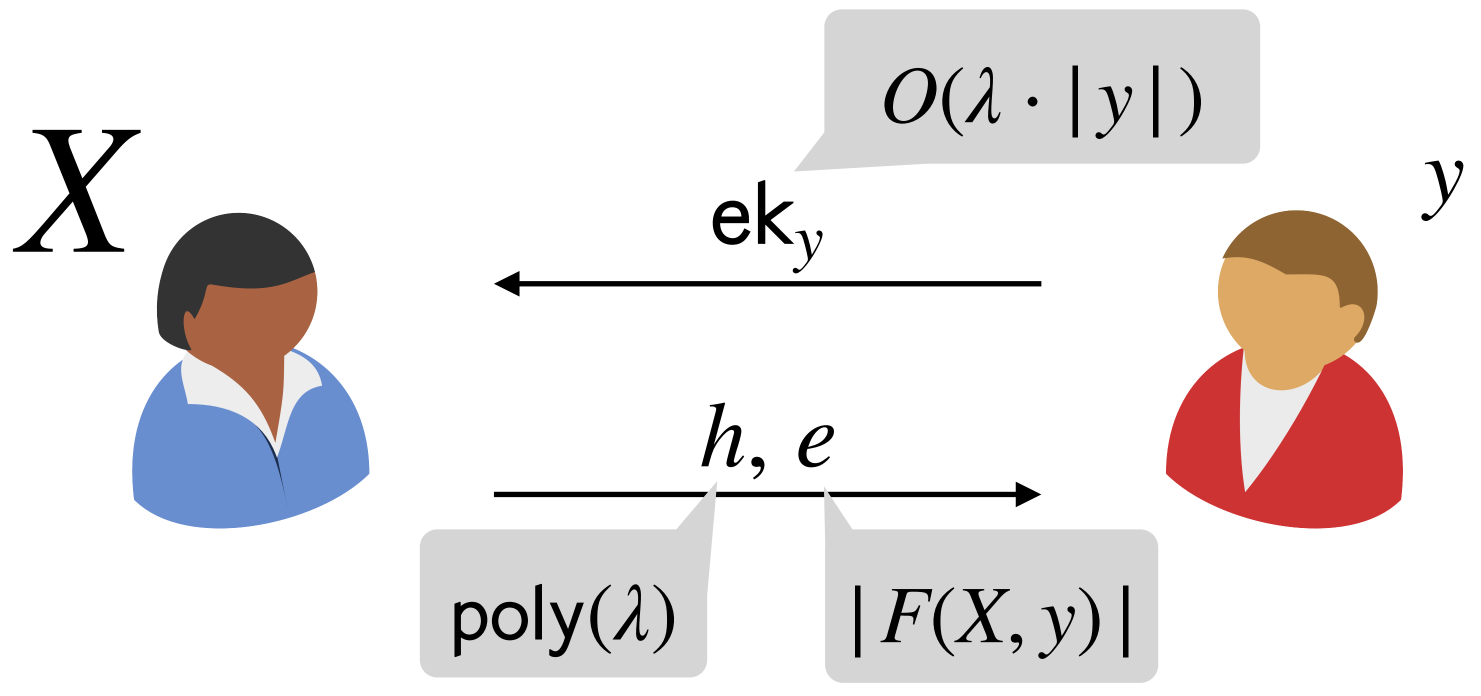
Reusability

Reusable encoding key with functions chosen on-the-fly

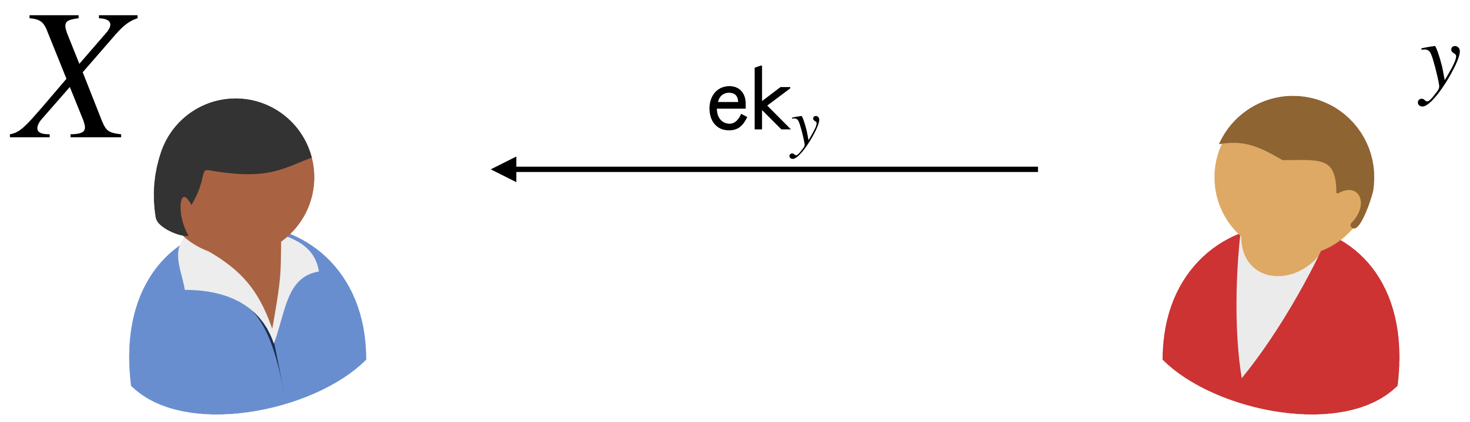
Enhanced Trapdoor Hash Functions from DDH and DCR

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

$$F(X, y) = \sum_i x_i \cdot y_i$$



This work



Expressivity

Supports computing Bilinear-NC^1 programs

Compactness

Encoding keys of size $|y|(1 + o(1))$

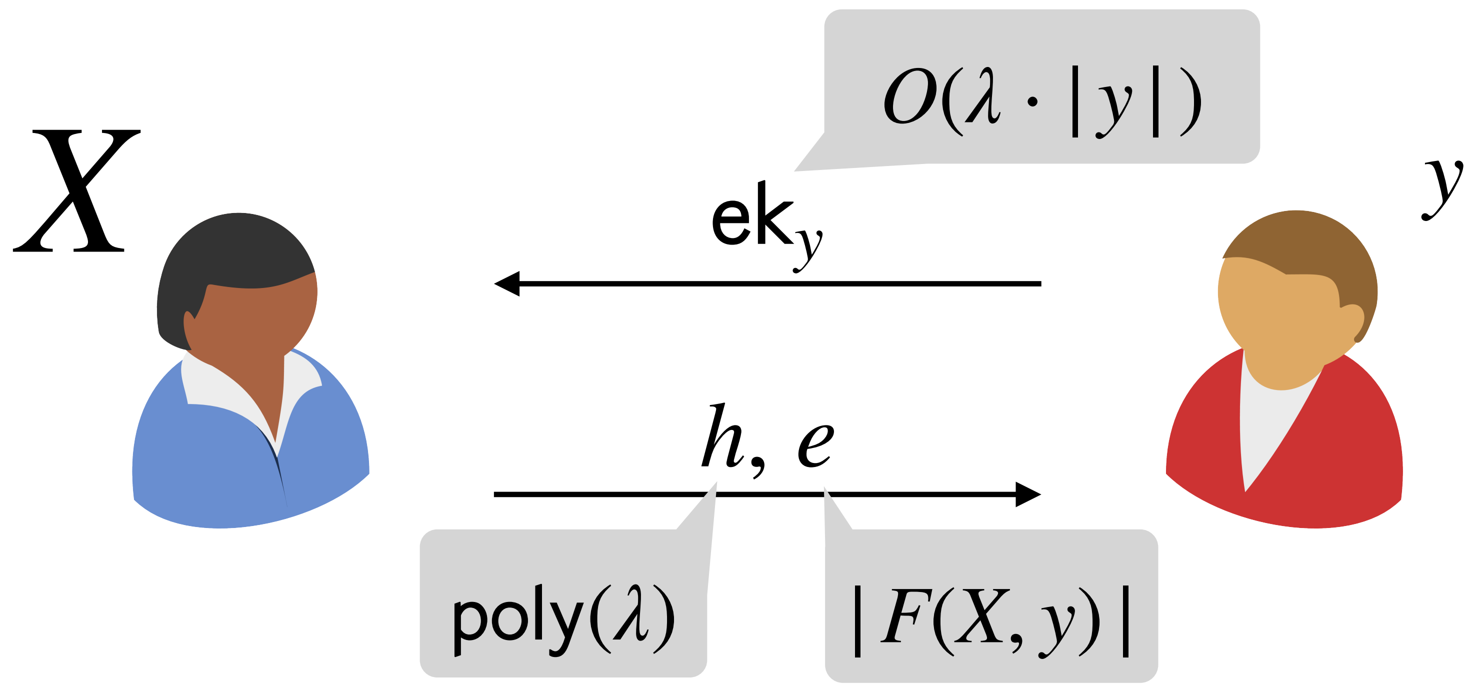
Reusability

Reusable encoding key with functions chosen on-the-fly

Enhanced Trapdoor Hash Functions from DDH and DCR

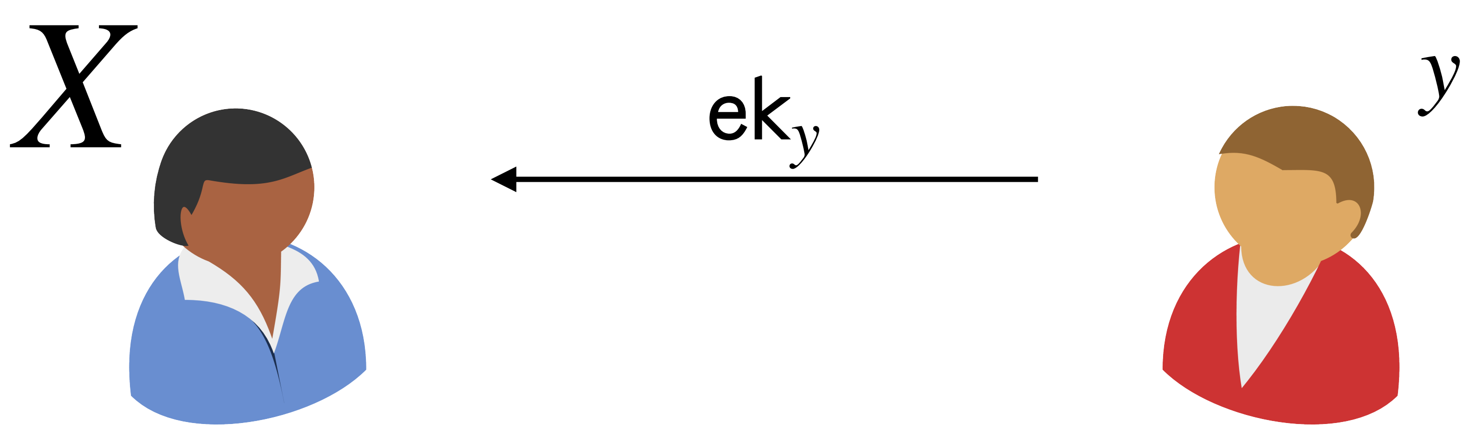
[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

$$F(X, y) = \sum_i x_i \cdot y_i$$



This work

$F_1 \quad F_2 \quad F_3$

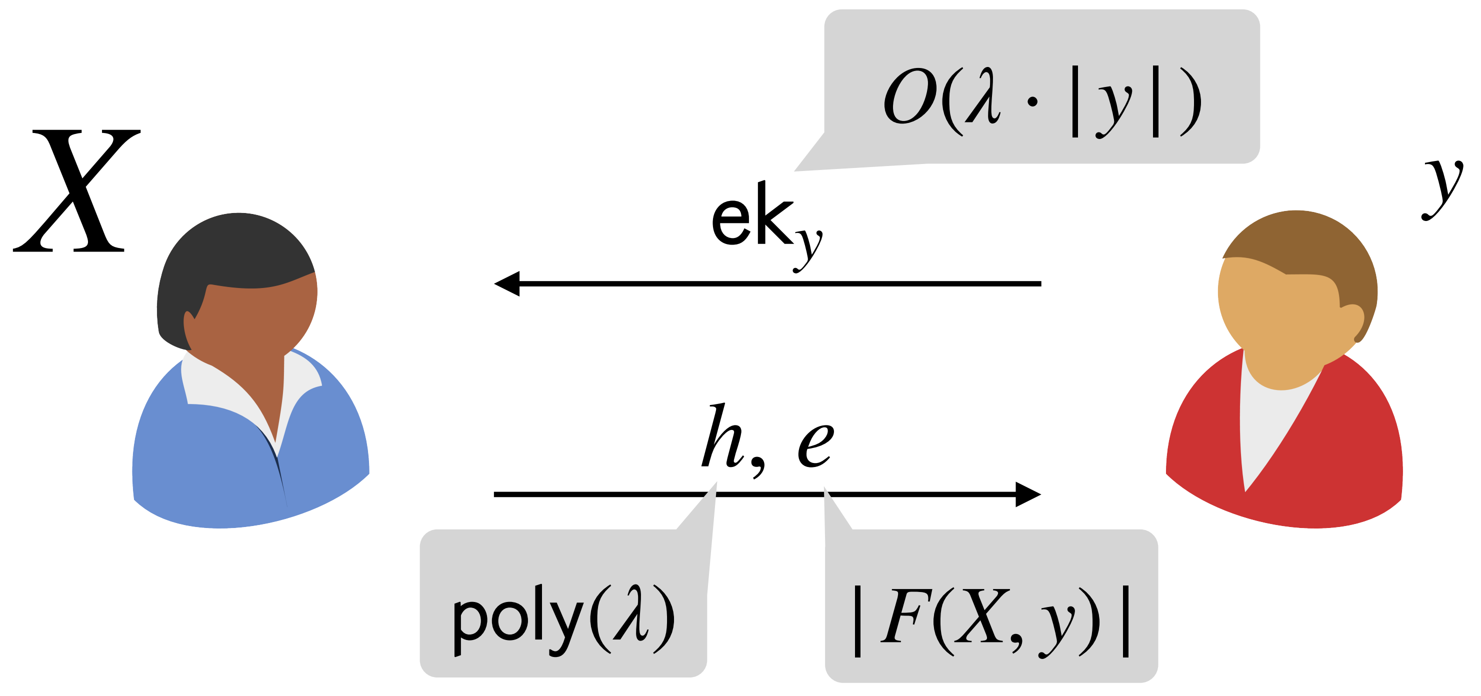


Expressivity	**Compactness**	**Reusability**
Supports computing Bilinear-NC^1 programs	Encoding keys of size $\lvert y \rvert(1 + o(1))$	Reusable encoding key with functions chosen on-the-fly

Enhanced Trapdoor Hash Functions from DDH and DCR

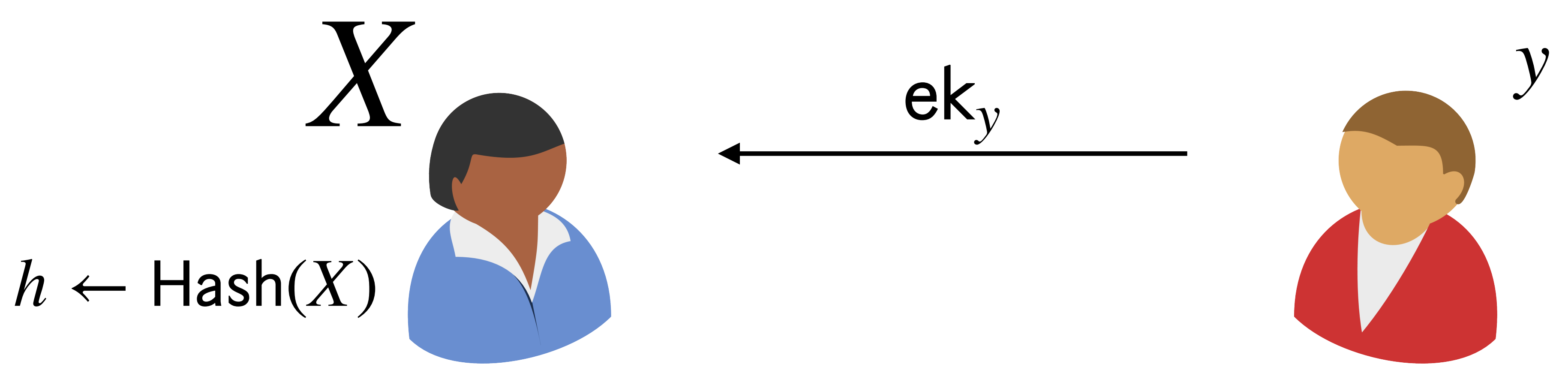
[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

$$F(X, y) = \sum_i x_i \cdot y_i$$



This work

F_1 F_2 F_3

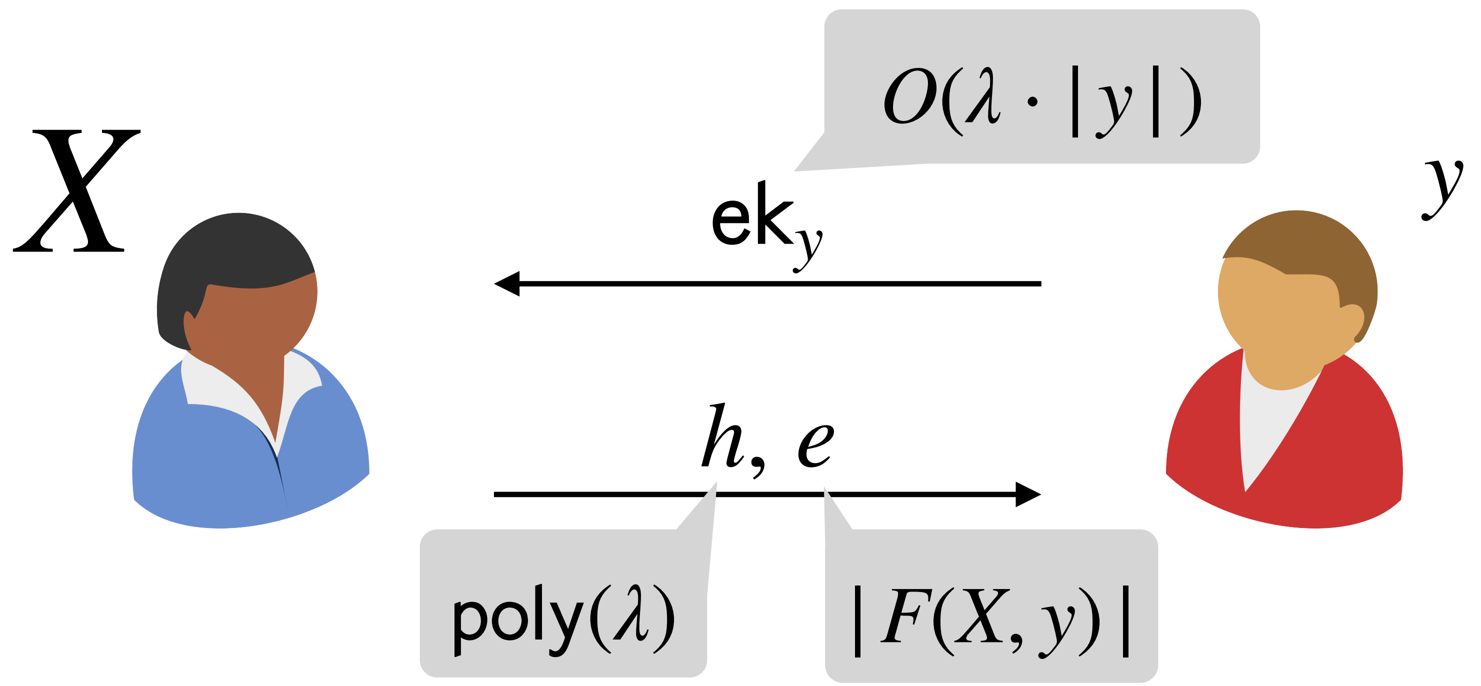


Expressivity	**Compactness**	**Reusability**
Supports computing Bilinear-NC^1 programs	Encoding keys of size $|y|(1 + o(1))$	Reusable encoding key with functions chosen on-the-fly

Enhanced Trapdoor Hash Functions from DDH and DCR

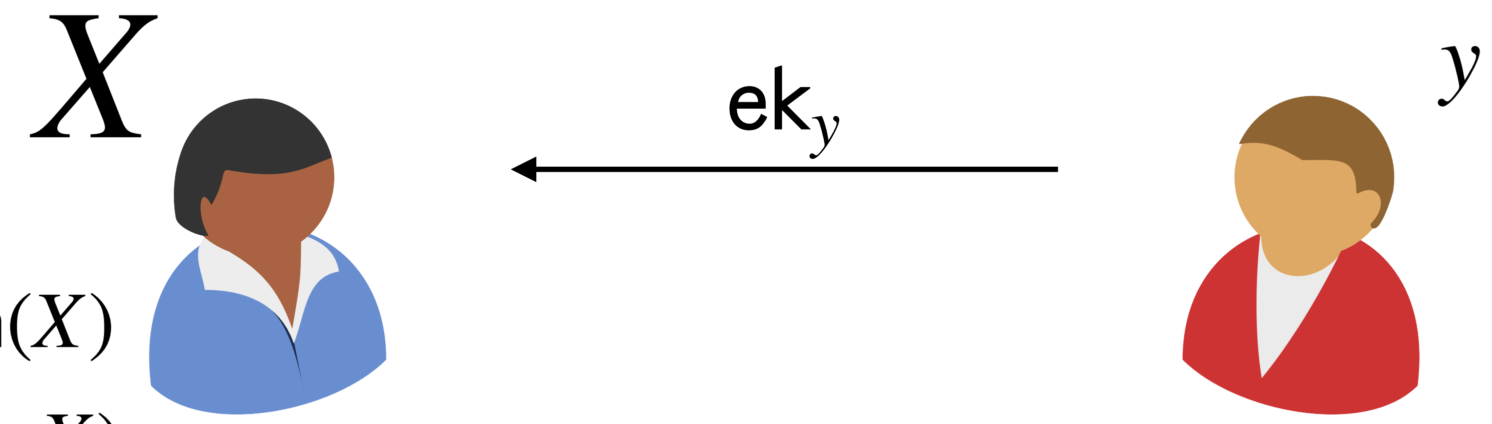
[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

$$F(X, y) = \sum_i x_i \cdot y_i$$



This work

F_1 $\color{blue}{F_2}$ $\color{red}{F_3}$



$h \leftarrow \mathsf{Hash}(X)$

$e_1 \leftarrow \mathsf{Encode}(\mathsf{F}_1, \mathsf{ek}_y, X)$

$\color{blue}{e_2} \leftarrow \mathsf{Encode}(\color{blue}{\mathsf{F}_2}, \mathsf{ek}_y, X)$

$\color{red}{e_2} \leftarrow \mathsf{Encode}(\color{red}{\mathsf{F}_2}, \mathsf{ek}_y, X)$

Expressivity	**Compactness**	**Reusability**
Supports computing Bilinear-NC^1 programs	Encoding keys of size $\lvert y \rvert(1 + o(1))$	Reusable encoding key with functions chosen on-the-fly

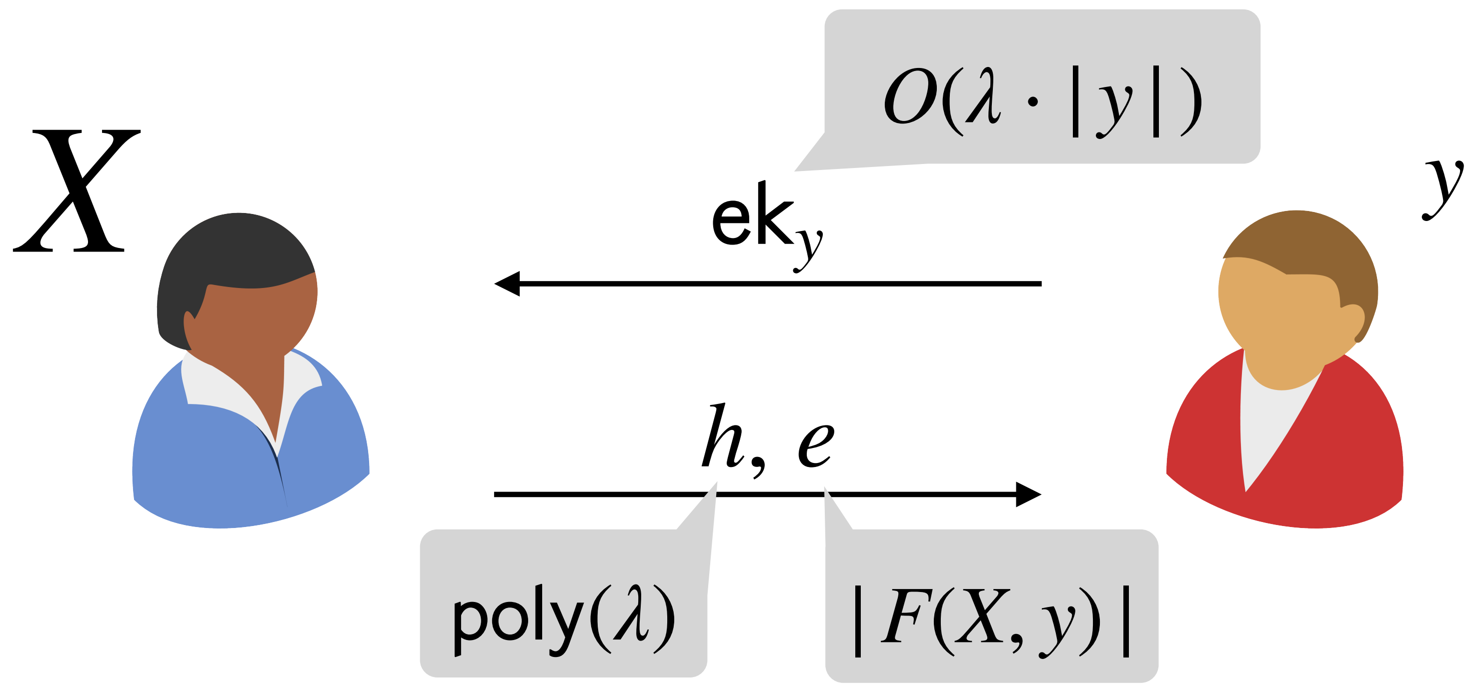
Enhanced Trapdoor Hash Functions from DDH and DCR

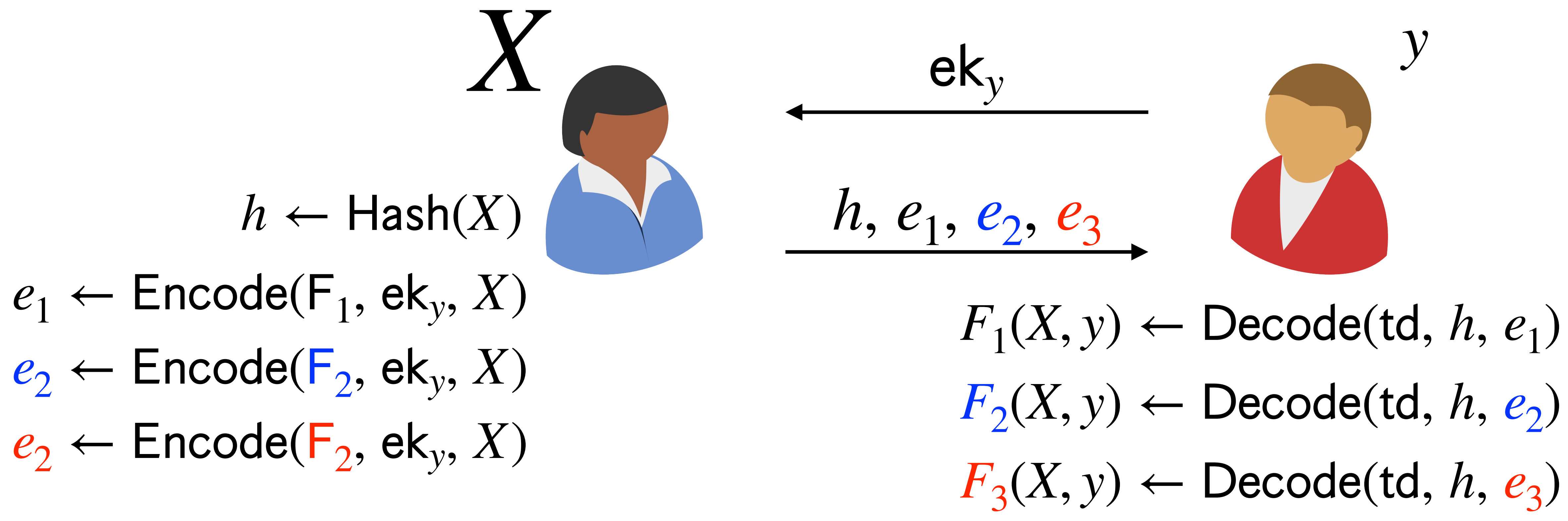
[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

This work

$$F(X, y) = \sum_i x_i \cdot y_i$$

$F_1 \quad F_2 \quad F_3$





Expressivity

Supports computing Bilinear-NC^1 programs

Compactness

Encoding keys of size $|y|(1 + o(1))$

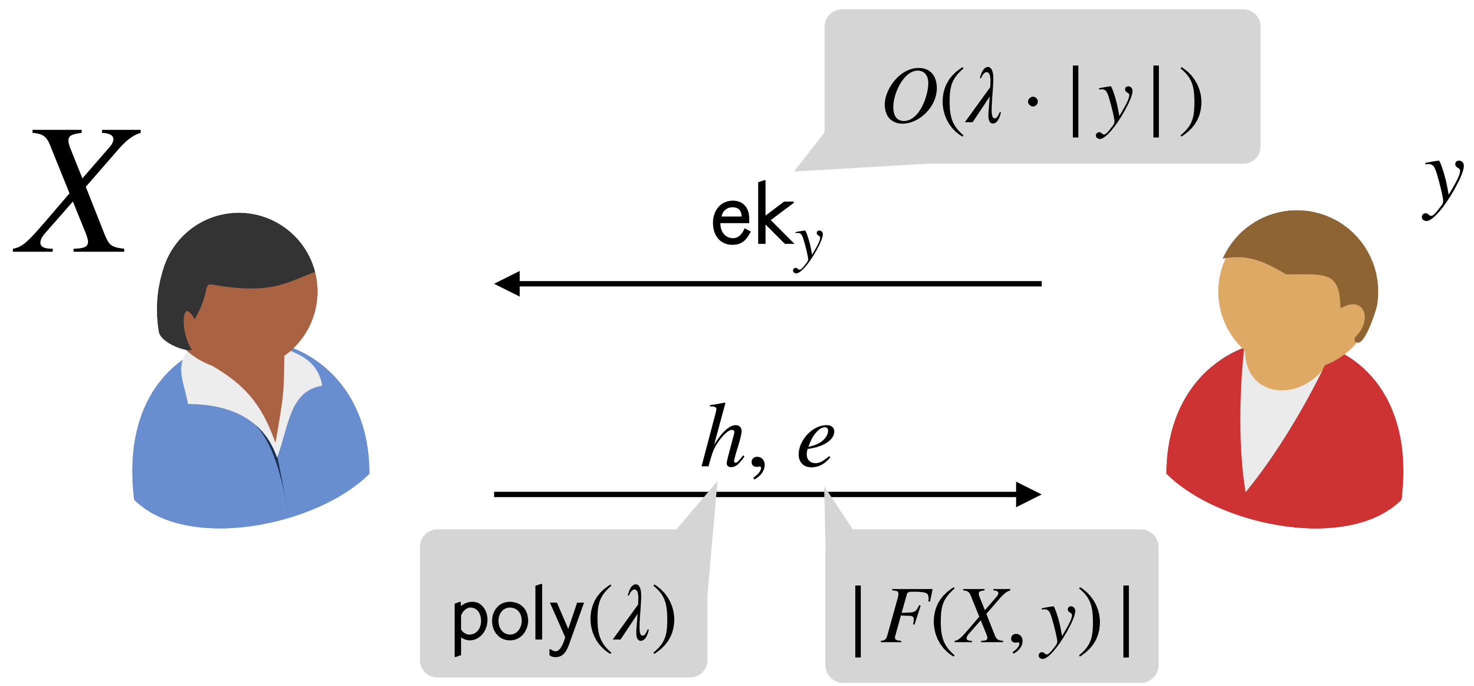
Reusability

Reusable encoding key with functions chosen on-the-fly

Enhanced Trapdoor Hash Functions from DDH and DCR

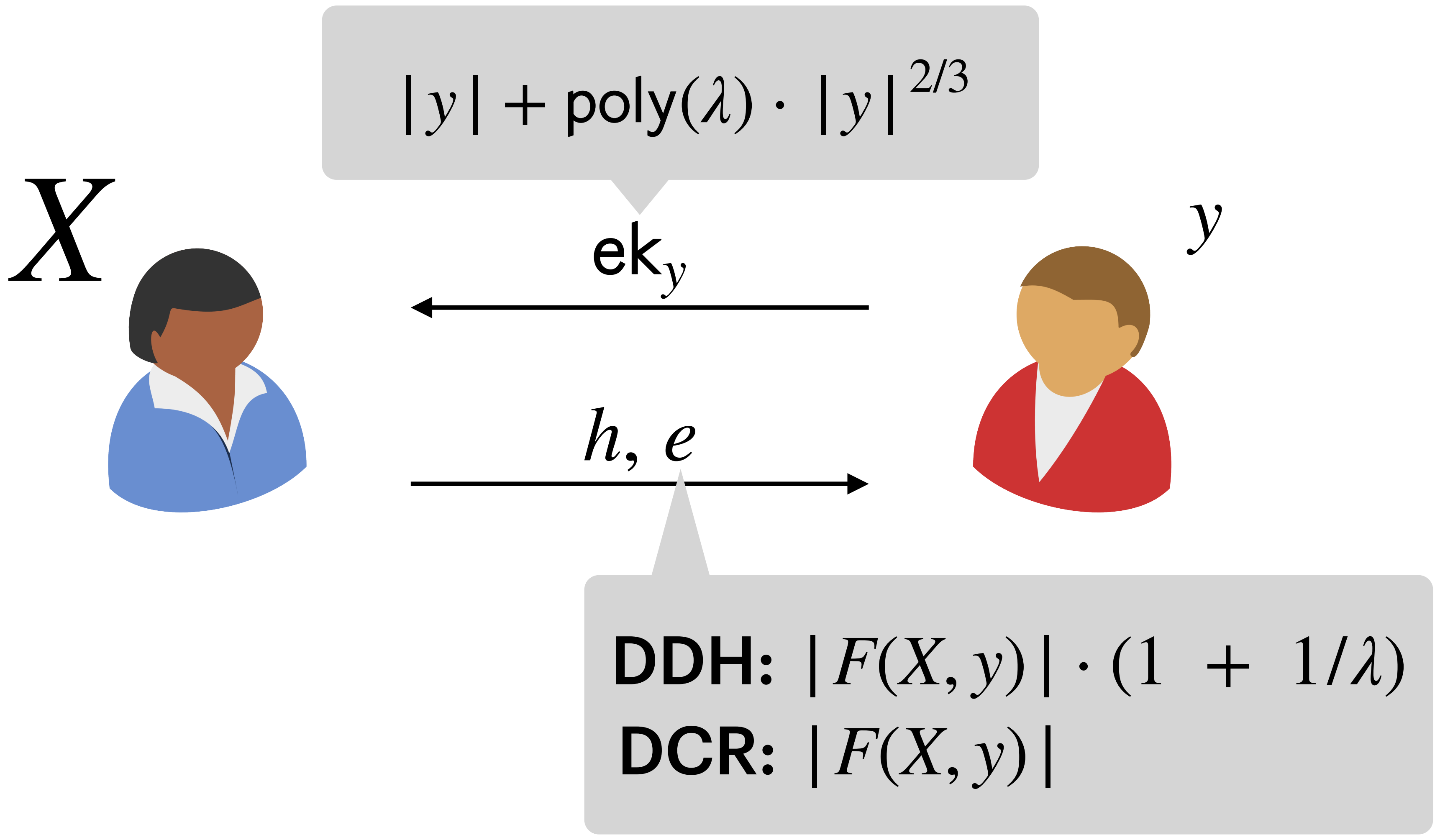
[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

$$F(X, y) = \sum_i x_i \cdot y_i$$



This work

$$F(X, y) = \sum_{i=1}^{n} f_i(X) \cdot g_i(y)$$



Expressivity

Supports computing Bilinear-NC^1 programs

Compactness

Encoding keys of size $|y|(1 + o(1))$

Reusability

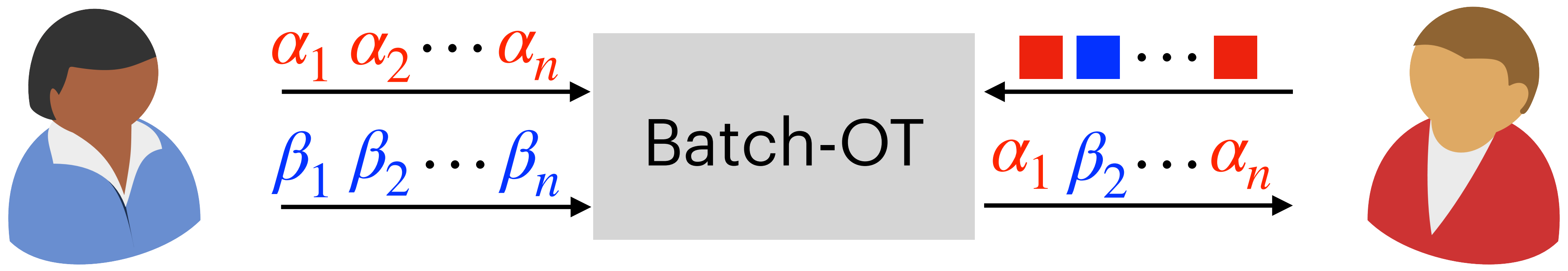
Reusable encoding key with functions chosen on-the-fly

Applications 1: Compactness

Batch-OT with optimal rate from DDH

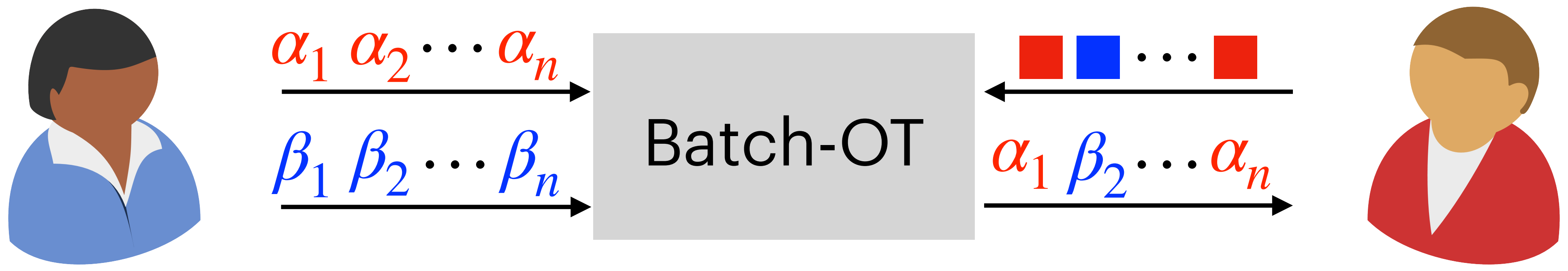
Applications 1: Compactness

Batch-OT with optimal rate from DDH



Applications 1: Compactness

Batch-OT with optimal rate from DDH



Ideal World Communication: $2n$ bits

Applications 1: Compactness

Batch-OT with optimal rate from DDH

Ideal World Communication: $2n$ bits

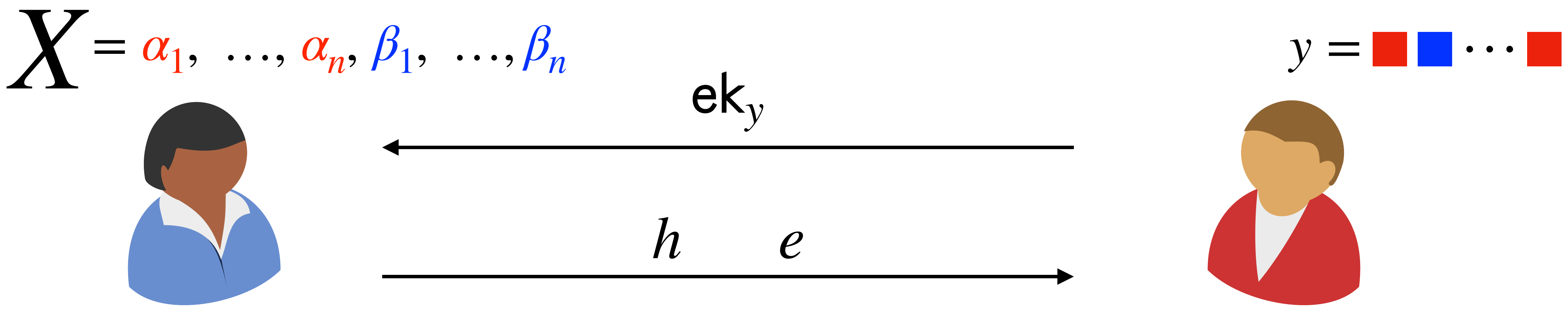
$X = \alpha_1,\ \ldots,\ \alpha_n,\ \beta_1,\ \ldots,\ \beta_n$

$y =$

Applications 1: Compactness

Batch-OT with optimal rate from DDH

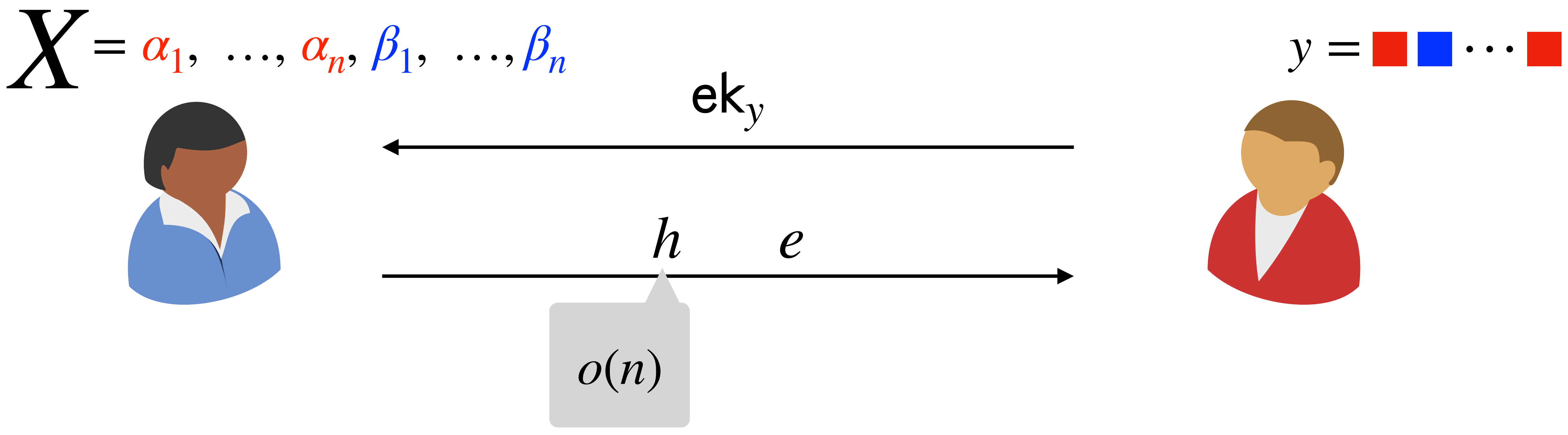
Ideal World Communication: $2n$ bits



Applications 1: Compactness

Batch-OT with optimal rate from DDH

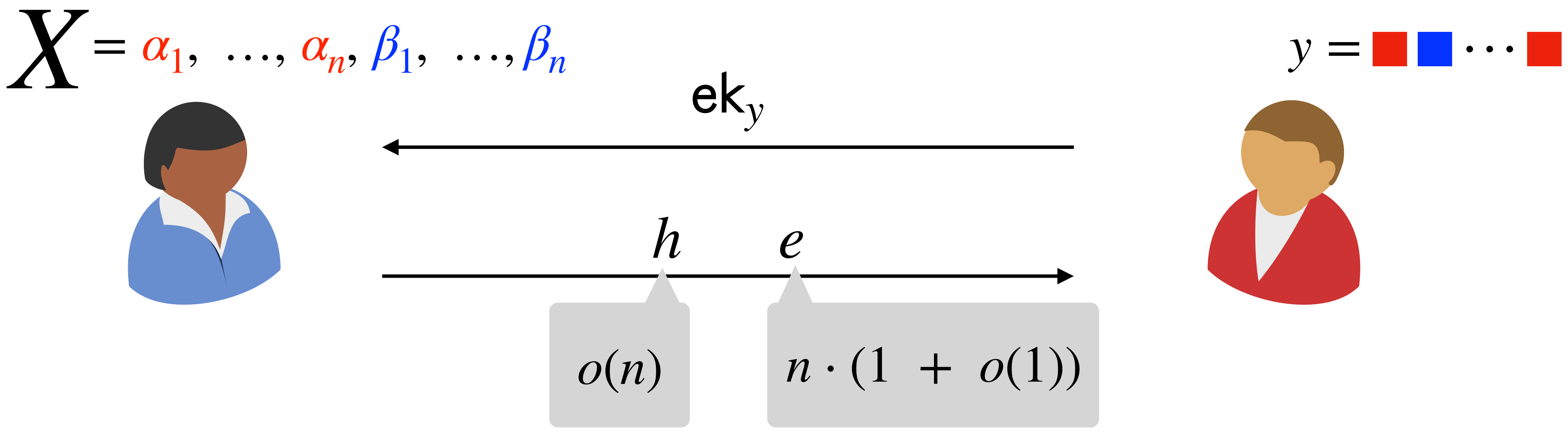
Ideal World Communication: $2n$ bits



Applications 1: Compactness

Batch-OT with optimal rate from DDH

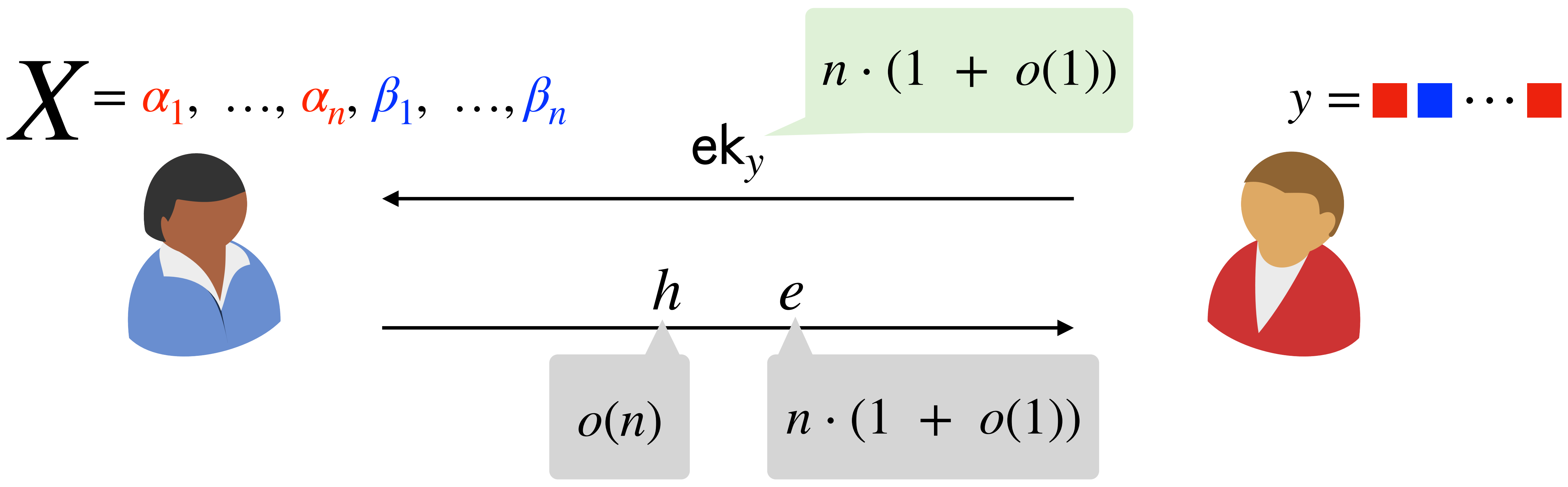
Ideal World Communication: $2n$ bits



Applications 1: Compactness

Batch-OT with optimal rate from DDH

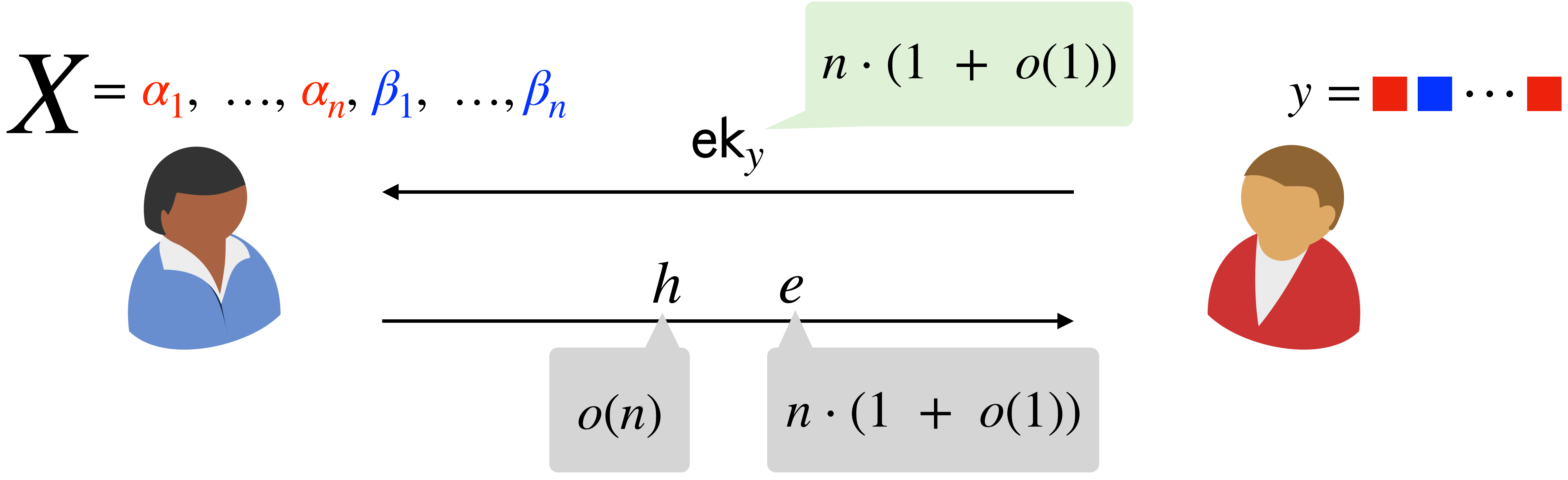
Ideal World Communication: $2n$ bits



Applications 1: **Compactness**

Batch-OT with optimal rate from DDH

Ideal World Communication: $2n$ bits



Communication: $2 \cdot n \cdot (1 + o(1))$ bits

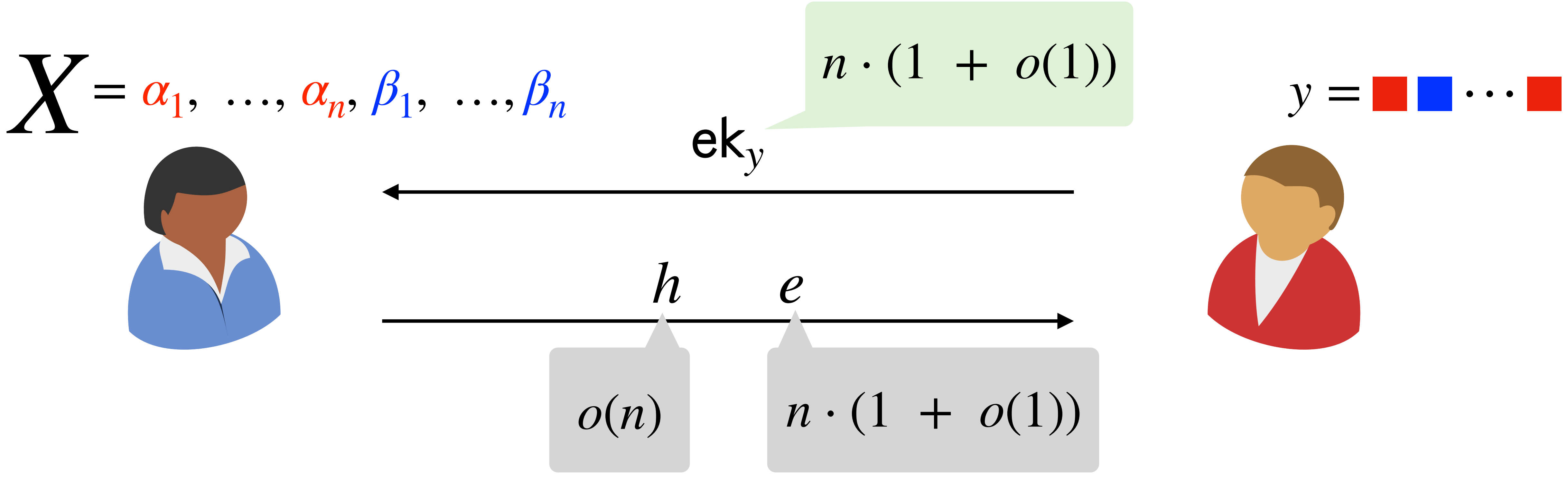
Applications 1: Compactness

Batch-OT with optimal rate from DDH

This Work: $1 + o(1)$ rate

Semi-honest statistical sender privacy

Ideal World Communication: $2n$ bits

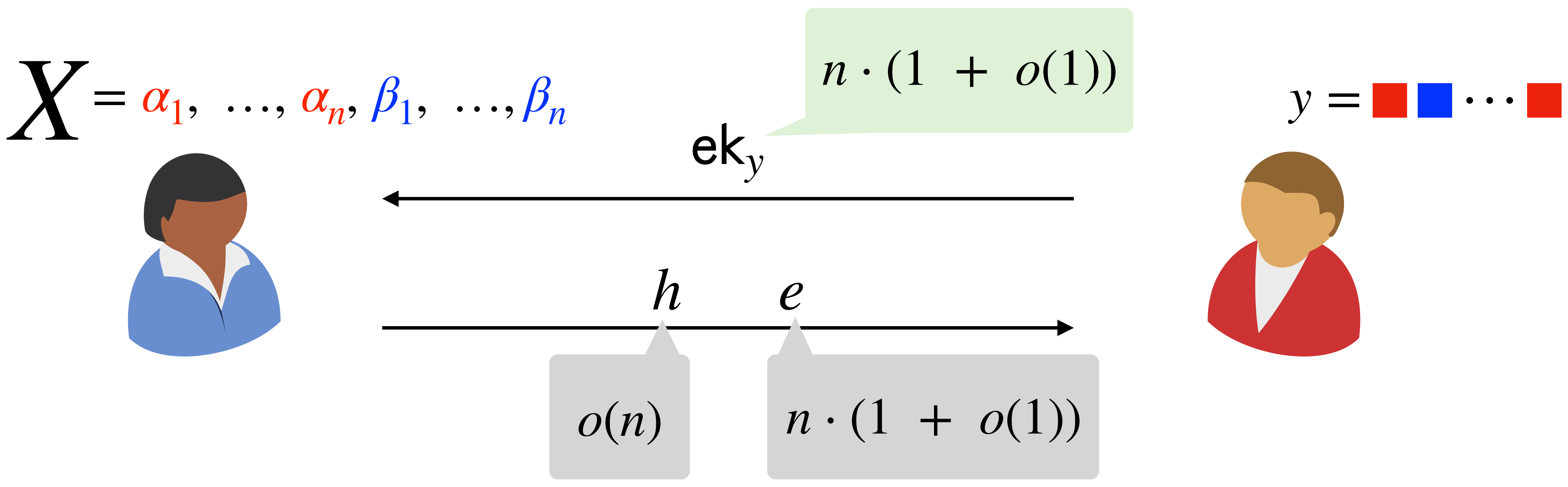


Communication: $2 \cdot n \cdot (1 + o(1))$ bits

Applications 1: Compactness

Batch-OT with optimal rate from DDH

Ideal World Communication: $2n$ bits



Communication: $2 \cdot n \cdot (1 + o(1))$ bits

This Work: $1 + o(1)$ rate

Semi-honest statistical sender privacy

Before:

[Brakerski-Branco-Döttling-Pu'22]:

$1 + o(1)$ rate

DDH + LPN

[Boyle-Giboa-Ishai'17]:

DDH

$n \cdot (4 + o(1))$ bits communication

PKI setup

Applications 1: Compactness

Batch-OT with optimal rate from DDH

This Work: $1 + o(1)$ rate

Semi-honest statistical sender privacy

Before:

[Brakerski-Branco-Döttling-Pu'22]: $1 + o(1)$ rate
DDH + LPN

[Boyle-Giboa-Ishai'17]: DDH
$n \cdot (4 + o(1))$ bits communication
PKI setup

Applications 1: Compactness

Batch-OT with optimal rate from DDH

This Work: $1 + o(1)$ rate

Semi-honest statistical sender privacy

Before:

[Brakerski-Branco-Döttling-Pu'22]: $1 + o(1)$ rate
DDH + LPN

[Boyle-Giboa-Ishai'17]: DDH
$n \cdot (4 + o(1))$ bits communication
PKI setup

Implications of Batch-OT with optimal rate

Applications 1: Compactness

Batch-OT with optimal rate from DDH

This Work: $1 + o(1)$ rate

Semi-honest statistical sender privacy

Before:

[Brakerski-Branco-Döttling-Pu'22]: $1 + o(1)$ rate

DDH + LPN

[Boyle-Giboa-Ishai'17]: DDH

$n \cdot (4 + o(1))$ bits communication

PKI setup

Implications of Batch-OT with optimal rate

String OT: $o(n)$ bits sender-to-receiver communication and $n \cdot (1 + o(1))$ bits receiver-to-sender communication

Applications 1: Compactness

Batch-OT with optimal rate from DDH

This Work: $1 + o(1)$ rate

Semi-honest statistical sender privacy

Before:

[Brakerski-Branco-Döttling-Pu'22]: $1 + o(1)$ rate
DDH + LPN

[Boyle-Giboa-Ishai'17]: DDH
$n \cdot (4 + o(1))$ bits communication
PKI setup

Implications of Batch-OT with optimal rate

String OT: $o(n)$ bits sender-to-receiver communication and $n \cdot (1 + o(1))$ bits receiver-to-sender communication

Lossy Trapdoor Functions (LTDF): Rate-1 LTDF with public key size $n \cdot (1 + o(1))$ bits
Rate-1 LTDF with public key size $o(n)$ bits with CRS

Applications 1: Compactness

Batch-OT with optimal rate from DDH

This Work: $1 + o(1)$ rate

Semi-honest statistical sender privacy

Before:

[Brakerski-Branco-Döttling-Pu'22]: $1 + o(1)$ rate
DDH + LPN

[Boyle-Giboa-Ishai'17]: DDH
$n \cdot (4 + o(1))$ bits communication
PKI setup

Implications of Batch-OT with optimal rate

String OT: $o(n)$ bits sender-to-receiver communication and $n \cdot (1 + o(1))$ bits receiver-to-sender communication

Lossy Trapdoor Functions (LTDF): Rate-1 LTDF with public key size $n \cdot (1 + o(1))$ bits
Rate-1 LTDF with public key size $o(n)$ bits with CRS

Private Information Retrieval: Client computation poly(n, λ)
Database size: 2^n
Upload communication $n +$ poly(λ) bits
Download communication $n \cdot$ poly(λ) bits

Applications 1: Compactness

Batch-OT with optimal rate from DDH

This Work: $1 + o(1)$ rate

Semi-honest statistical sender privacy

Before:

[Brakerski-Branco-Döttling-Pu'22]: $1 + o(1)$ rate
DDH + LPN

[Boyle-Giboa-Ishai'17]: DDH
$n \cdot (4 + o(1))$ bits communication
PKI setup

Implications of Batch-OT with optimal rate

String OT: $o(n)$ bits sender-to-receiver communication and $n \cdot (1 + o(1))$ bits receiver-to-sender communication

Lossy Trapdoor Functions (LTDF): Rate-1 LTDF with public key size $n \cdot (1 + o(1))$ bits
Rate-1 LTDF with public key size $o(n)$ bits with CRS

Private Information Retrieval:
Database size: 2^n

Client computation poly(n, λ)
Upload communication $n +$ poly(λ) bits
Download communication $n \cdot$ poly(λ) bits

Other Implications

Branching programs over encrypted data

Correlated symmetric PIR

Applications 2: Compactness + **Expressivity**

Sublinear 2PC from DCR, with one-sided statistical security for layered circuits

Applications 2: Compactness + **Expressivity**

Sublinear 2PC from DCR, with one-sided statistical security for layered circuits

Bilinear-$\mathsf{NC}^1 \supseteq \log\log$-depth circuits

Applications 2: Compactness + **Expressivity**

Sublinear 2PC from DCR, with one-sided statistical security for layered circuits

Bilinear-$\mathsf{NC}^1 \supseteq \log\log$-depth circuits

This Work: $|x| + (2 + o(1)) \cdot \dfrac{|C|}{\log\log|C|} + |y|^{2/3} \cdot \mathrm{poly}(\lambda)$ bits communication

Applications 2: Compactness + **Expressivity**

Sublinear 2PC from DCR, with one-sided statistical security for layered circuits

Bilinear-$\mathsf{NC}^1 \supseteq \log\log$-depth circuits

Linear communication in **computationally** secure input

Sublinear communication in **statistically** secure input

This Work: $|x| + (2+o(1)) \cdot \dfrac{|C|}{\log\log|C|} + |y|^{2/3} \cdot \mathsf{poly}(\lambda)$ bits communication

Applications 2: Compactness + **Expressivity**

Sublinear 2PC from DCR, with one-sided statistical security for layered circuits

Bilinear-$\mathsf{NC}^1 \supseteq \log\log$-depth circuits

Linear communication in **computationally** secure input

Sublinear communication in **statistically** secure input

This Work: $|x| + (2+o(1)) \cdot \dfrac{|C|}{\log\log|C|} + |y|^{2/3} \cdot \mathrm{poly}(\lambda)$ bits communication

Sublinear in size of circuit

Applications 2: Compactness + **Expressivity**

Sublinear 2PC from DCR, with one-sided statistical security for layered circuits

Bilinear-$\mathsf{NC}^1 \supseteq \log\log$-depth circuits

Linear communication in **computationally** secure input

Sublinear communication in **statistically** secure input

This Work: $|x| + (2 + o(1)) \cdot \dfrac{|C|}{\log\log|C|} + |y|^{2/3} \cdot \mathrm{poly}(\lambda)$ bits communication

Sublinear in size of circuit

Before: Similar results only known from FHE

Applications 2: Compactness + **Expressivity**

Sublinear 2PC from DCR, with one-sided statistical security for layered circuits

Bilinear-$\mathsf{NC}^1 \supseteq \log\log$-depth circuits

Linear communication in **computationally** secure input

Sublinear communication in **statistically** secure input

This Work: $|x| + (2+o(1)) \cdot \dfrac{|C|}{\log\log|C|} + |y|^{2/3} \cdot \mathrm{poly}(\lambda)$ bits communication

Sublinear in size of circuit

Before: Similar results only known from FHE

[Couteau-Meyer-Passelégue-Riahinia'23]: $|x| + |y| + \dfrac{|C|}{\log\log|C|} + \mathrm{poly}(\lambda)$ bits communication

Circular security of Paillier

Layered circuits over $\mathbb{Z}_N$

Applications 3: Compactness + Expressivity + **Reusability**

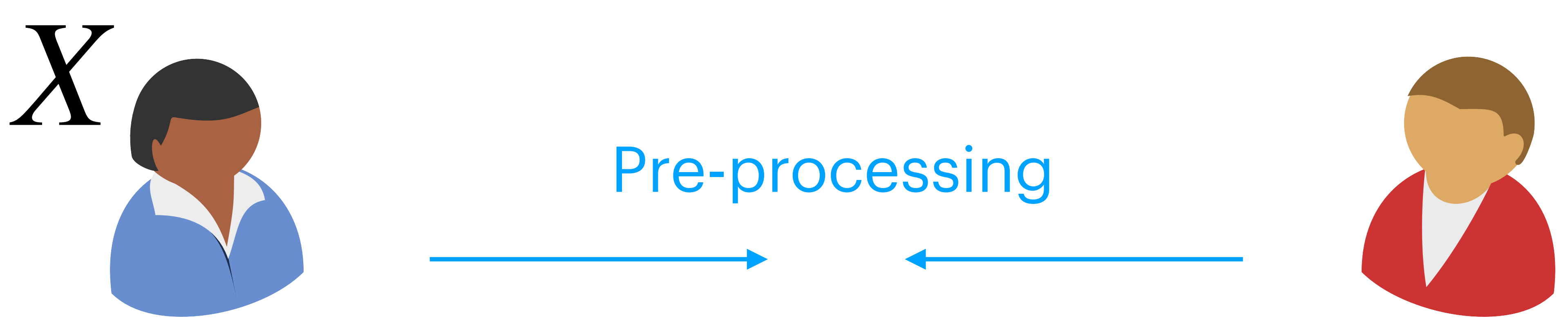
Improving Communication in the Amortized Setting

Public function F

Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

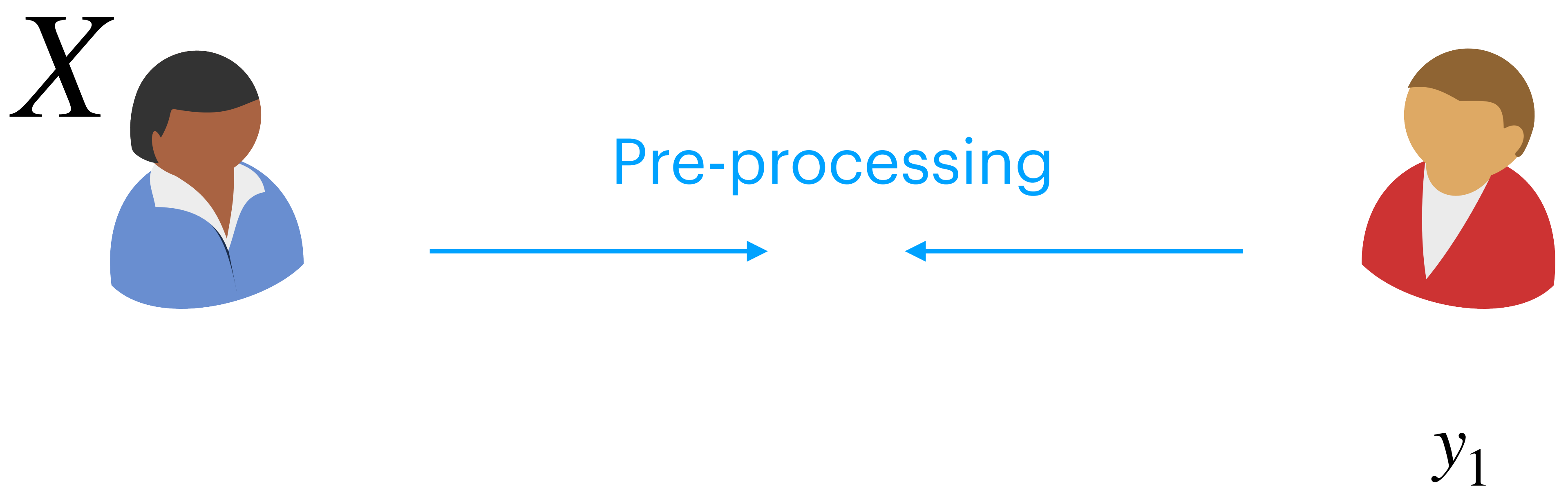
Public function F



Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

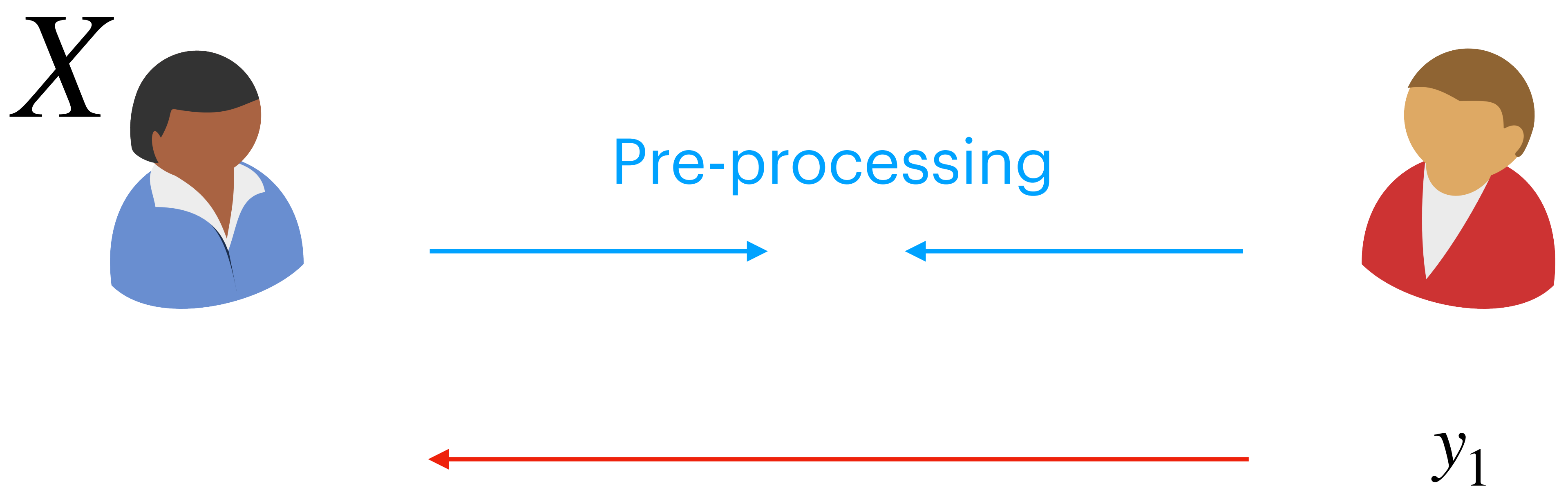
Public function F



Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

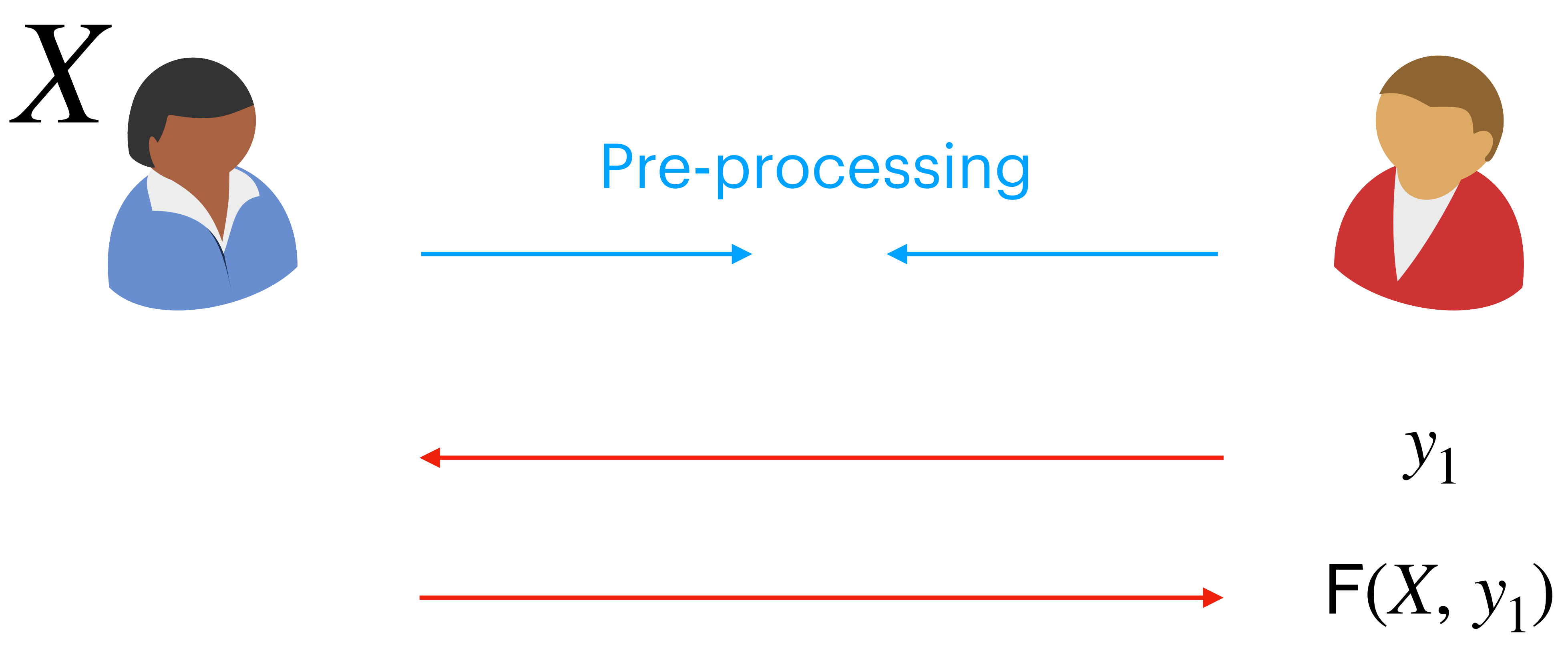
Public function F



Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

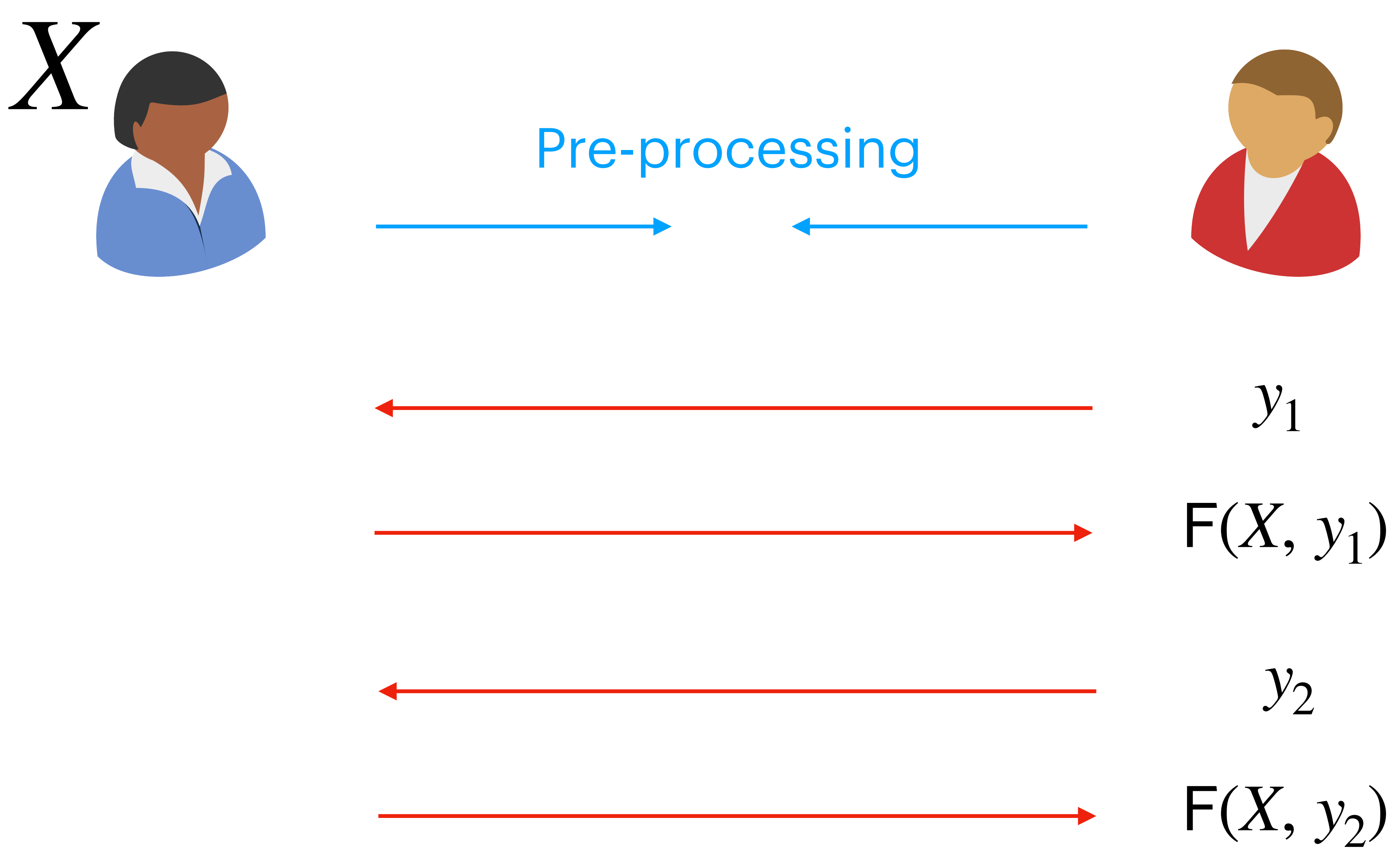
Public function F



Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

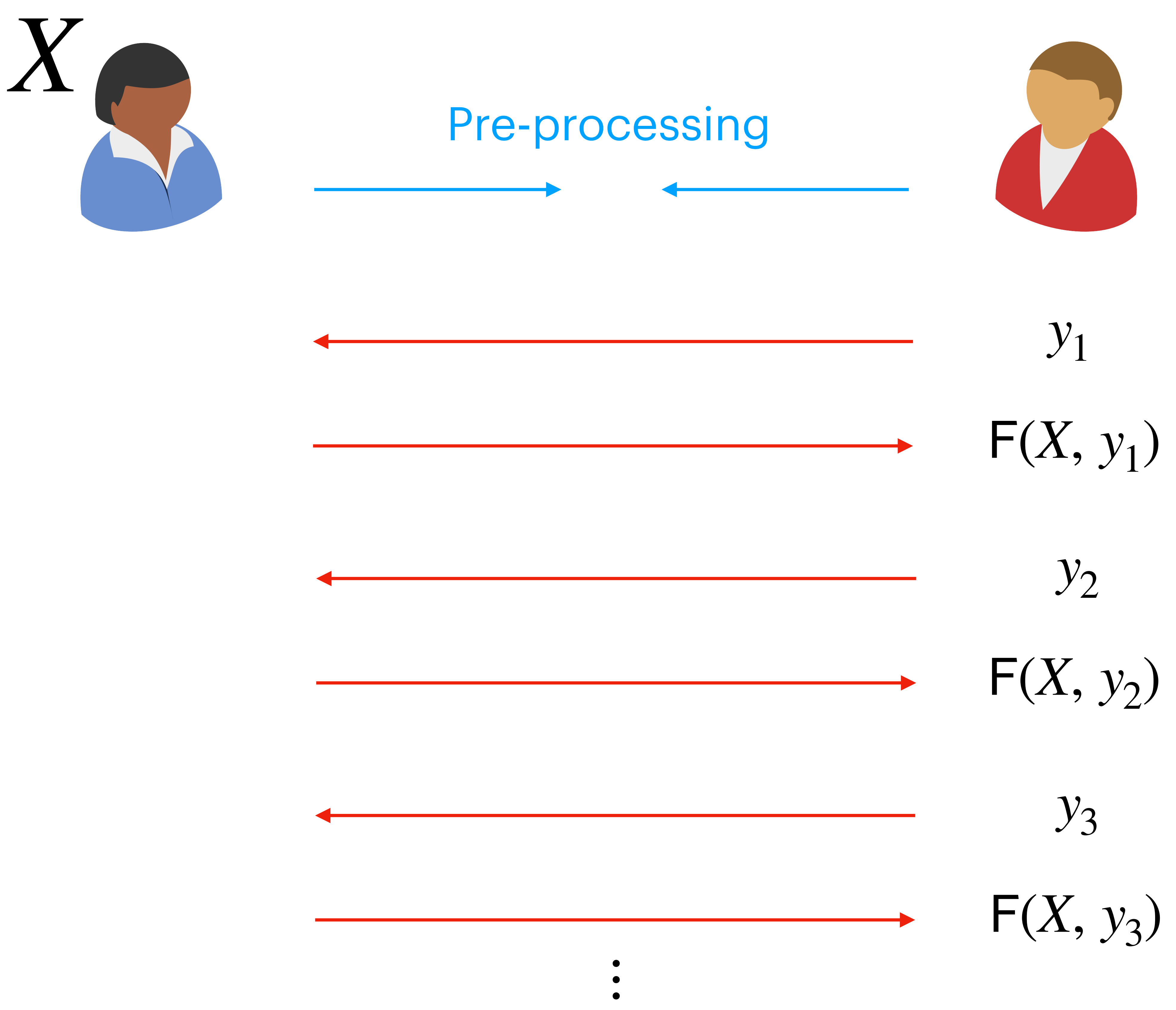
Public function F



Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

Public function F



Applications 3: Compactness + Expressivity + **Reusability**

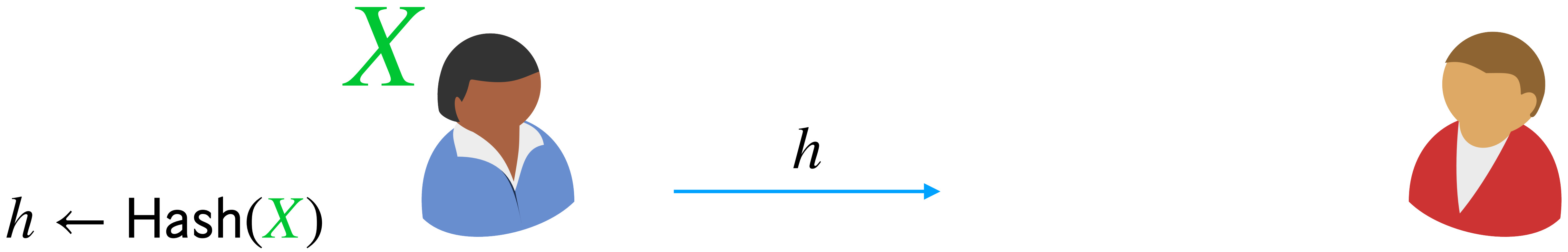
Improving Communication in the Amortized Setting

Public function F

Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

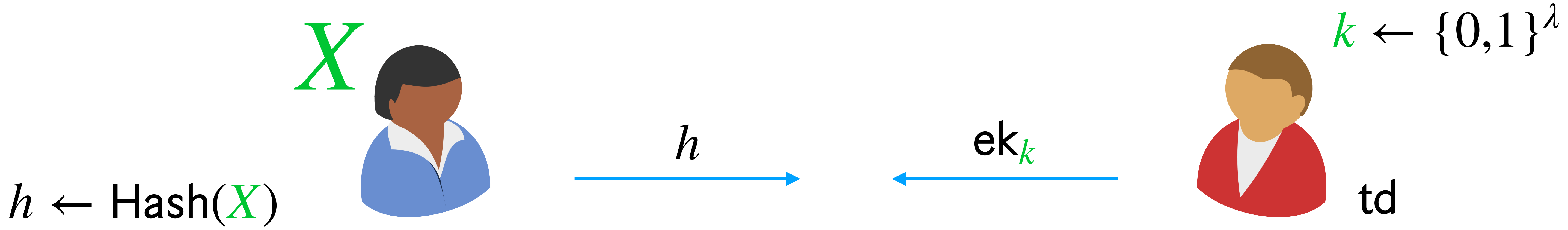
Public function F



Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

Public function F



Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

Public function F

X

$h \leftarrow \text{Hash}(X)$

h →

← ek_k

$k \leftarrow \{0,1\}^\lambda$

td

y_1

$z_1 = y_1 \oplus \text{PRF}(k, 1)$

Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

Public function F

X

$h \leftarrow \text{Hash}(X)$

$\xrightarrow{h}$

$\xleftarrow{\text{ek}_k}$

$k \leftarrow \{0,1\}^\lambda$

td

y_1

$z_1 = y_1 \oplus \text{PRF}(k, 1)$

$\xleftarrow{z_1}$

z_1 ensures privacy of y_1

Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

Public function F

X

$h \leftarrow \text{Hash}(X)$

$\xrightarrow{h}$

$\xleftarrow{\mathsf{ek}_k}$

$k \leftarrow \{0,1\}^\lambda$

td

y_1

$z_1 = y_1 \oplus \text{PRF}(k, 1)$

$\xleftarrow{z_1}$

$\text{F}_1(X, k) = F(X, z_1 \oplus \text{PRF}(k, 1))$

Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

Public function F

X 

$h \leftarrow \mathsf{Hash}(X)$ $\xrightarrow{h}$ $\xleftarrow{\mathsf{ek}_k}$  $k \leftarrow \{0,1\}^\lambda$ td

y_1

$\mathsf{F}_1(X, k) = F(X, z_1 \oplus \mathsf{PRF}(k, 1))$ $\xleftarrow{z_1}$ $z_1 = y_1 \oplus \mathsf{PRF}(k, 1)$

$e_1 \leftarrow \mathsf{Encode}(\mathsf{F}_1, \mathsf{ek}_k, X)$ $\xrightarrow{e_1}$

Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

Public function F

X

$h \leftarrow \mathsf{Hash}(X)$

$\xrightarrow{h}$

$\xleftarrow{\mathsf{ek}_k}$

$k \leftarrow \{0,1\}^{\lambda}$

td

y_1

$\mathsf{F}_1(X, k) = F(X, z_1 \oplus \mathsf{PRF}(k, 1))$ $\xleftarrow{z_1}$ $z_1 = y_1 \oplus \mathsf{PRF}(k, 1)$

$e_1 \leftarrow \mathsf{Encode}(\mathsf{F}_1, \mathsf{ek}_k, X)$ $\xrightarrow{e_1}$ $F(X, y_1) \leftarrow \mathsf{Decode}(\mathsf{td}, e_1, h)$

Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

Public function F

X  $k \leftarrow \{0,1\}^\lambda$ 

$h \leftarrow \text{Hash}(X)$ $\xrightarrow{h}$ $\xleftarrow{\text{ek}_k}$ td

y_1

$\text{F}_1(X, k) = F(X, z_1 \oplus \text{PRF}(k, 1))$ $\xleftarrow{z_1}$ $z_1 = y_1 \oplus \text{PRF}(k, 1)$

$e_1 \leftarrow \text{Encode}(\text{F}_1, \text{ek}_k, X)$ $\xrightarrow{e_1}$ $F(X, y_1) \leftarrow \text{Decode}(\text{td}, e_1, h)$

$\text{F}_2(X, k) = F(X, z_2 \oplus \text{PRF}(k, 2))$ $\xleftarrow{z_2}$ $z_2 = y_2 \oplus \text{PRF}(k, 2)$

$e_2 \leftarrow \text{Encode}(\text{F}_2, \text{ek}_k, X)$ $\xrightarrow{e_2}$ $F(X, y_2) \leftarrow \text{Decode}(\text{td}, e_2, h)$

$\vdots$

Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

Public function F

X  $h \leftarrow \mathsf{Hash}(X)$

$\xrightarrow{h}$ $\xleftarrow{\mathsf{ek}_k}$

 $k \leftarrow \{0,1\}^\lambda$ td

$\mathsf{F}_1(X, k) = F(X, z_1 \oplus \mathsf{PRF}(k, 1))$

$e_1 \leftarrow \mathsf{Encode}(\mathsf{F}_1, \mathsf{ek}_k, X)$

y_1

$\xleftarrow{z_1}$

$z_1 = y_1 \oplus \mathsf{PRF}(k, 1)$

(e_1, h)

Reusability $\Longrightarrow$ Encoding of k can be reused with functions chosen on-the-fly

$\mathsf{F}_2(X, k) = F(X, z_2 \oplus \mathsf{PRF}(k, 2))$

$e_2 \leftarrow \mathsf{Encode}(\mathsf{F}_2, \mathsf{ek}_k, X)$

$\xleftarrow{z_2}$

$z_2 = y_2 \oplus \mathsf{PRF}(k, 2)$

$\xrightarrow{e_2}$

$F(X, y_2) \leftarrow \mathsf{Decode}(\mathsf{td}, e_2, h)$

$\vdots$

Applications 3: Compactness + Expressivity + **Reusability**

Improving Communication in the Amortized Setting

Public function F

X

$k \leftarrow \{0,1\}^\lambda$

$h \leftarrow \mathsf{Hash}(X)$

$\xrightarrow{h}$

$\xleftarrow{\mathsf{ek}_k}$

td

$|z_1| = |y_1|$

y_1

$\mathsf{F}_1(X, k) = F(X, z_1 \oplus \mathsf{PRF}(k, 1))$

$\xleftarrow{z_1}$

$z_1 = y_1 \oplus \mathsf{PRF}(k, 1)$

$e_1 \leftarrow \mathsf{Encode}(\mathsf{F}_1, \mathsf{ek}_k, X)$

$\xrightarrow{e_1}$

$F(X, y_1) \leftarrow \mathsf{Decode}(\mathsf{td}, e_1, h)$

DCR: $|e_1| = |F(X, k)|$

$\mathsf{F}_2(X, k) = F(X, z_2 \oplus \mathsf{PRF}(k, 2))$

$\xleftarrow{z_2}$

$z_2 = y_2 \oplus \mathsf{PRF}(k, 2)$

$e_2 \leftarrow \mathsf{Encode}(\mathsf{F}_2, \mathsf{ek}_k, X$

e_2

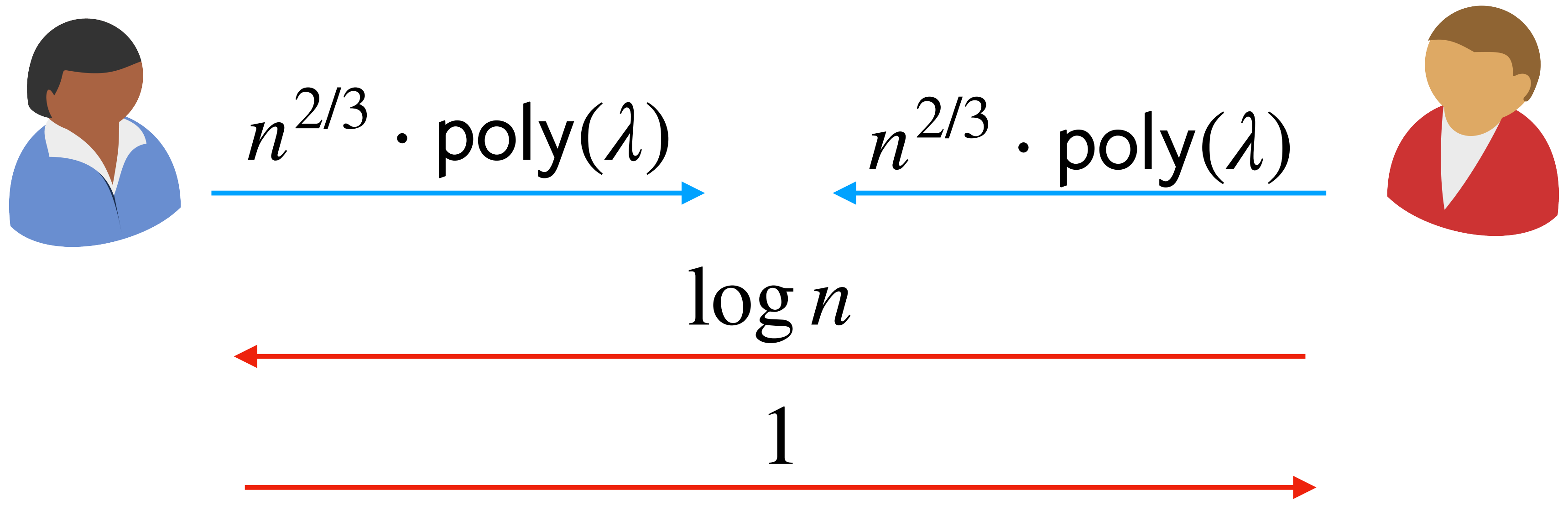
$y_2) \leftarrow \mathsf{Decode}(\mathsf{td}, e_2, h)$

Optimal communication per query from DCR

Applications 3: Compactness + Expressivity + **Reusability**

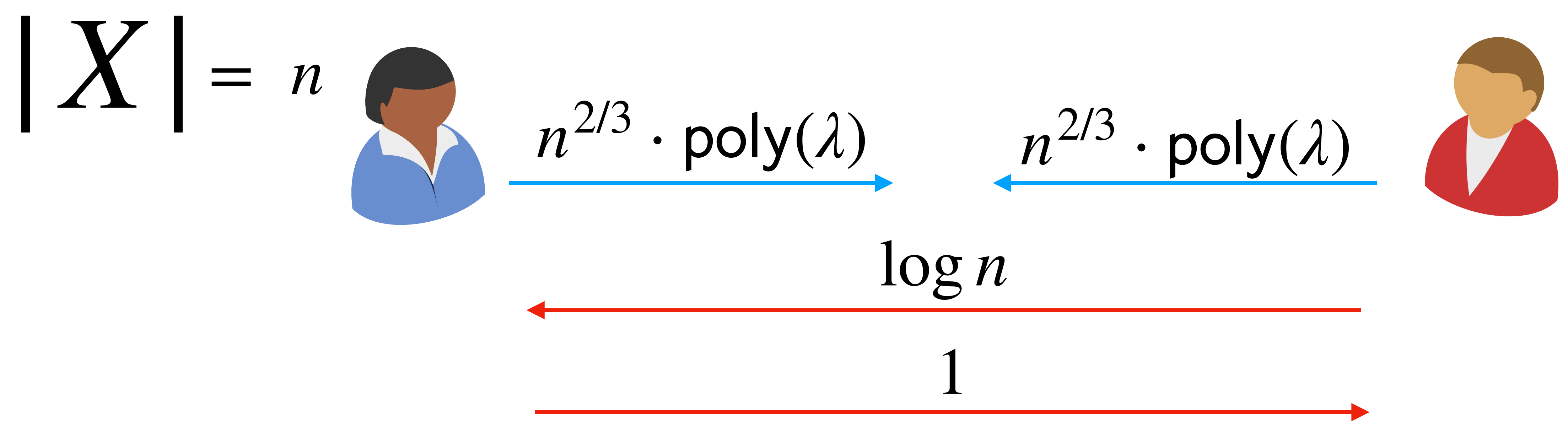
Optimal preprocessing symmetric Private Information Retrieval from DCR

$|X| = n$

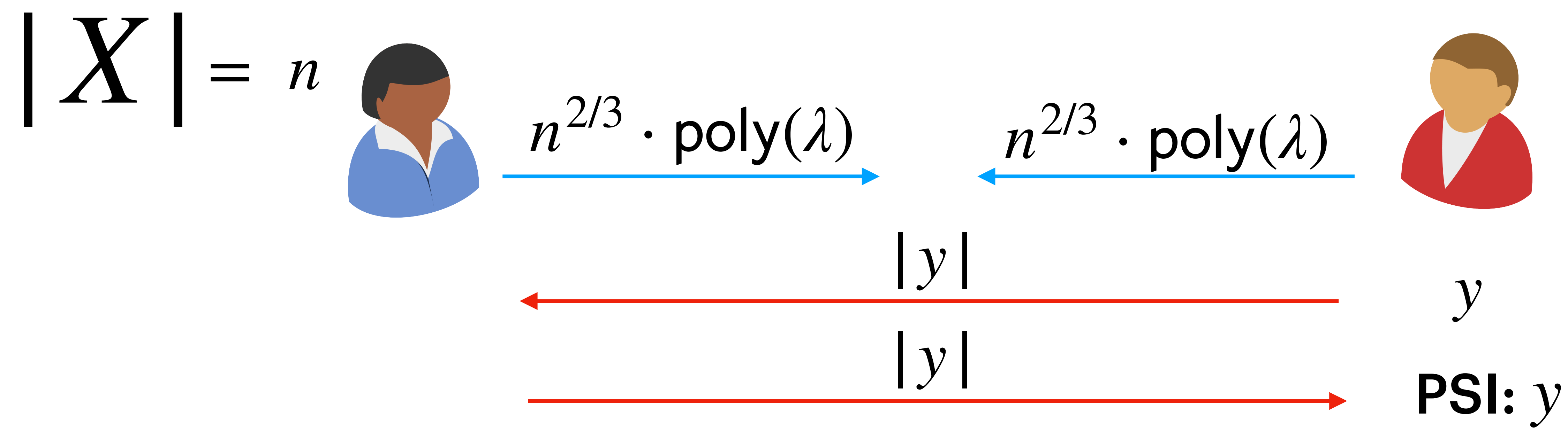


Applications 3: Compactness + Expressivity + **Reusability**

Optimal preprocessing symmetric Private Information Retrieval from DCR



Rate-$\frac{1}{2}$ Private Set Intersection (PSI) and Fuzzy-PSI from DCR



PSI: $y \in X$

Fuzzy-PSI: Is y close to an element in X

Constructing Enhanced TDH

Constructing Enhanced TDH

Staged Homomorphic Secret Sharing

[Couteau-Meyer-Passelégue-Riahinia’23]

+

Trapdoor Hash Functions

[Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

Alternative view: Extending Succinct HSS [Abram-Roy-Scholl’24] using Staged HSS

Staged Homomorphic Secret Sharing

X

y

Staged Homomorphic Secret Sharing

X

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

Staged Homomorphic Secret Sharing

X

$\mathsf{ct}_y \leftarrow \mathsf{Encrypt}(\mathsf{pk}, y)$

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

Staged Homomorphic Secret Sharing

X

$\mathsf{ct}_y \leftarrow \mathsf{Encrypt}(\mathsf{pk}, y)$

$\mathsf{share}_A, \mathsf{share}_B \leftarrow \mathsf{Share}(\mathsf{pk}, X)$

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

Staged Homomorphic Secret Sharing

X

$\mathsf{ct}_y \leftarrow \mathsf{Encrypt}(\mathsf{pk}, y)$

$\mathsf{share}_A, \mathsf{share}_B \leftarrow \mathsf{Share}(\mathsf{pk}, X)$

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

ct_y share_A

StagedEval

out_A

ct_y share_B

StagedEval

out_B

Staged Homomorphic Secret Sharing

X

$\mathsf{ct}_y \leftarrow \mathsf{Encrypt}(\mathsf{pk}, y)$

$\mathsf{share}_A, \mathsf{share}_B \leftarrow \mathsf{Share}(\mathsf{pk}, X)$

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

ct_y share_A

StagedEval

out_A

ct_y share_B

StagedEval

out_B

$\mathsf{out}_A + \mathsf{out}_A = F(X, y)$

Bilinear-NC^1 program

Staged Homomorphic Secret Sharing

X

$\mathsf{ct}_y \leftarrow \mathsf{Encrypt}(\mathsf{pk}, y)$

$\mathsf{share}_A, \mathsf{share}_B \leftarrow \mathsf{Share}(\mathsf{pk}, X)$

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

ct_y share_A

StagedEval

out_A

ct_y share_B

StagedEval

out_B

Key Ingredient: Secure and succinct protocol to distribute input shares

Staged Homomorphic Secret Sharing

X

$\mathsf{ct}_y \leftarrow \mathsf{Encrypt}(\mathsf{pk}, y)$

$\mathsf{share}_A, \mathsf{share}_B \leftarrow \mathsf{Share}(\mathsf{pk}, X)$

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

ct_y share_A

StagedEval

out_A

ct_y share_B

StagedEval

out_B

Key Ingredient: Secure and succinct protocol to distribute input shares

Staged Homomorphic Secret Sharing

X

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$\mathsf{ct}_y \leftarrow \mathsf{Encrypt}(\mathsf{pk}, y)$

$\mathsf{share}_A, \mathsf{share}_B \leftarrow \mathsf{Share}(\mathsf{pk}, X)$

share_A

$\mathsf{ct}_y \quad \mathsf{share}_A$

StagedEval

out_A

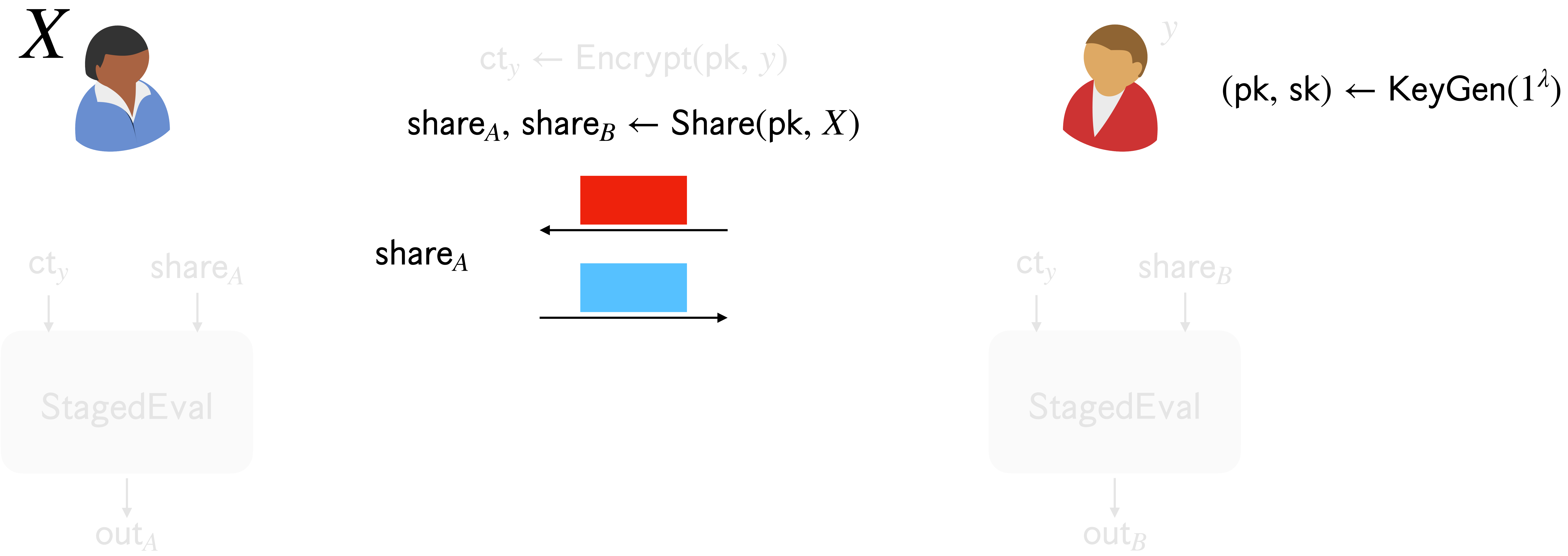
$\mathsf{ct}_y \quad \mathsf{share}_B$

StagedEval

out_B

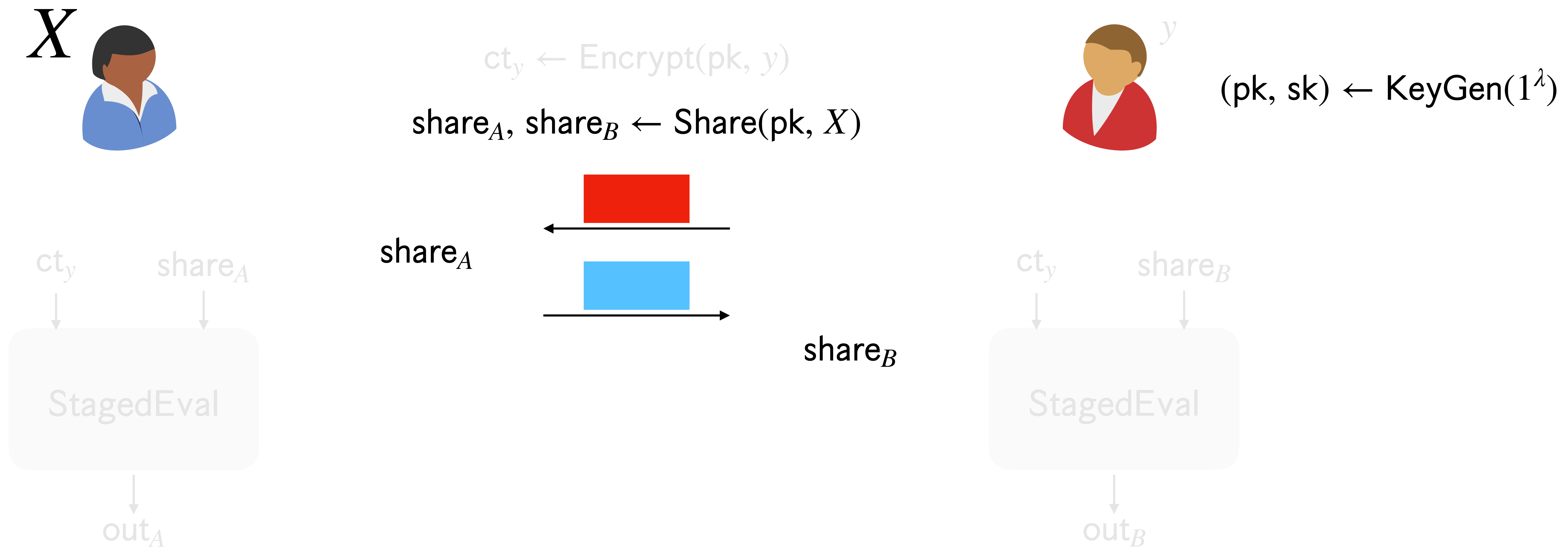
Key Ingredient: Secure and succinct protocol to distribute input shares

Staged Homomorphic Secret Sharing



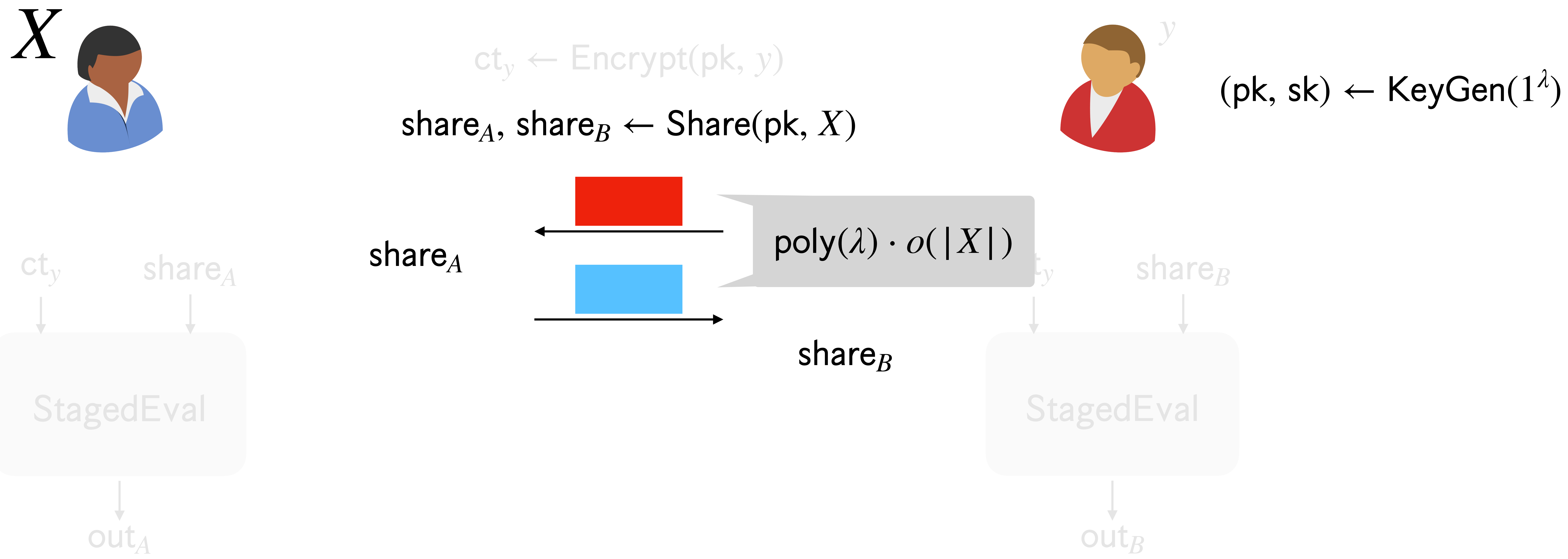
Key Ingredient: Secure and succinct protocol to distribute input shares

Staged Homomorphic Secret Sharing



Key Ingredient: Secure and succinct protocol to distribute input shares

Staged Homomorphic Secret Sharing



Key Ingredient: Secure and succinct protocol to distribute input shares

Enhanced TDH = Staged HSS + Succinct Distribution of Shares

Public function F

Enhanced TDH = Staged HSS + Succinct Distribution of Shares

Public function F

X

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

Enhanced TDH = Staged HSS + Succinct Distribution of Shares

Public function F

X

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$k \leftarrow \{0, 1\}^\lambda$

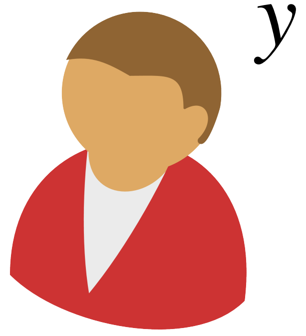
$z = y \oplus \mathsf{PRG}(k)$

$\mathsf{ct}_k \leftarrow \mathsf{Encrypt}(\mathsf{pk}, k)$

Enhanced TDH = Staged HSS + Succinct Distribution of Shares

Public function F

X



y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$k \leftarrow \{0, 1\}^\lambda$

$z = y \oplus \mathsf{PRG}(k)$

$\mathsf{ct}_k \leftarrow \mathsf{Encrypt}(\mathsf{pk}, k)$

$\mathsf{ct}_k, \quad z,$

Enhanced TDH = Staged HSS + Succinct Distribution of Shares

Public function F

X

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$k \leftarrow \{0, 1\}^\lambda$

$z = y \oplus \mathsf{PRG}(k)$

$\mathsf{ct}_k \leftarrow \mathsf{Encrypt}(\mathsf{pk}, k)$

$\mathsf{ct}_k, \quad z,$

Compute share_A from

Enhanced TDH = Staged HSS + Succinct Distribution of Shares

Public function F

X

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$k \leftarrow \{0, 1\}^\lambda$

$z = y \oplus \mathsf{PRG}(k)$

$\mathsf{ct}_k \leftarrow \mathsf{Encrypt}(\mathsf{pk}, k)$

Compute share_A from

$\mathsf{ct}_k, \quad z,$

$\mathsf{share}_A \rightarrow$ StagedEval $\rightarrow \mathsf{out}_A$

$\mathsf{ct}_k \rightarrow$

Evaluate: $\mathsf{F}'(X, k) = F(X, z \oplus \mathsf{PRG}(k))$

Enhanced TDH = Staged HSS + Succinct Distribution of Shares

Public function F

X

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$k \leftarrow \{0, 1\}^\lambda$

$z = y \oplus \mathsf{PRG}(k)$

$\mathsf{ct}_k \leftarrow \mathsf{Encrypt}(\mathsf{pk}, k)$

Compute share_A from

ct_k, z,

$\mathsf{share}_A \rightarrow$ StagedEval $\rightarrow \mathsf{out}_A$

$\mathsf{ct}_k \rightarrow$

Evaluate: $\mathsf{F}'(X, k) = F(X, z \oplus \mathsf{PRG}(k))$

, out_A

Enhanced TDH = Staged HSS + Succinct Distribution of Shares

Public function F

X 

 y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$k \leftarrow \{0, 1\}^\lambda$

$z = y \oplus \mathsf{PRG}(k)$

$\mathsf{ct}_k \leftarrow \mathsf{Encrypt}(\mathsf{pk}, k)$

Compute share_A from

ct_k, z,

$\mathsf{share}_A \rightarrow$ StagedEval $\rightarrow \mathsf{out}_A$

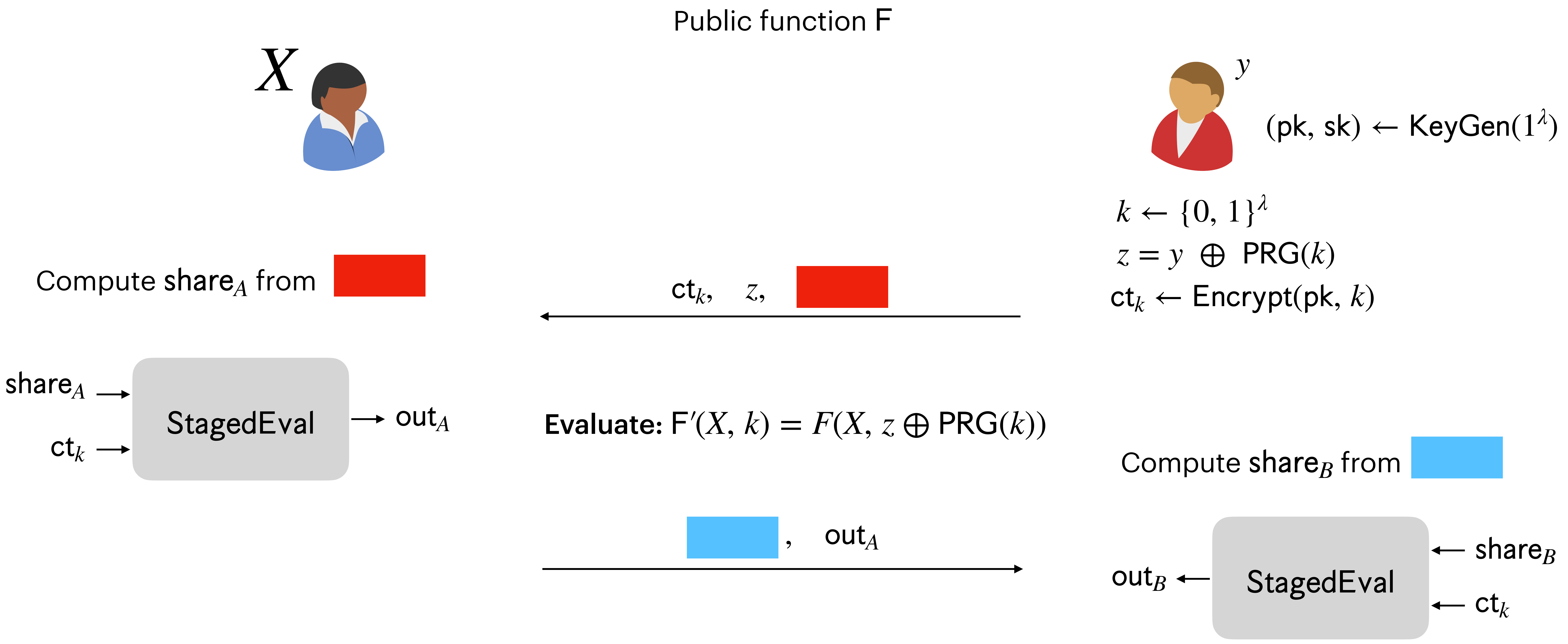
$\mathsf{ct}_k \rightarrow$ StagedEval

Evaluate: $\mathsf{F}'(X, k) = F(X, z \oplus \mathsf{PRG}(k))$

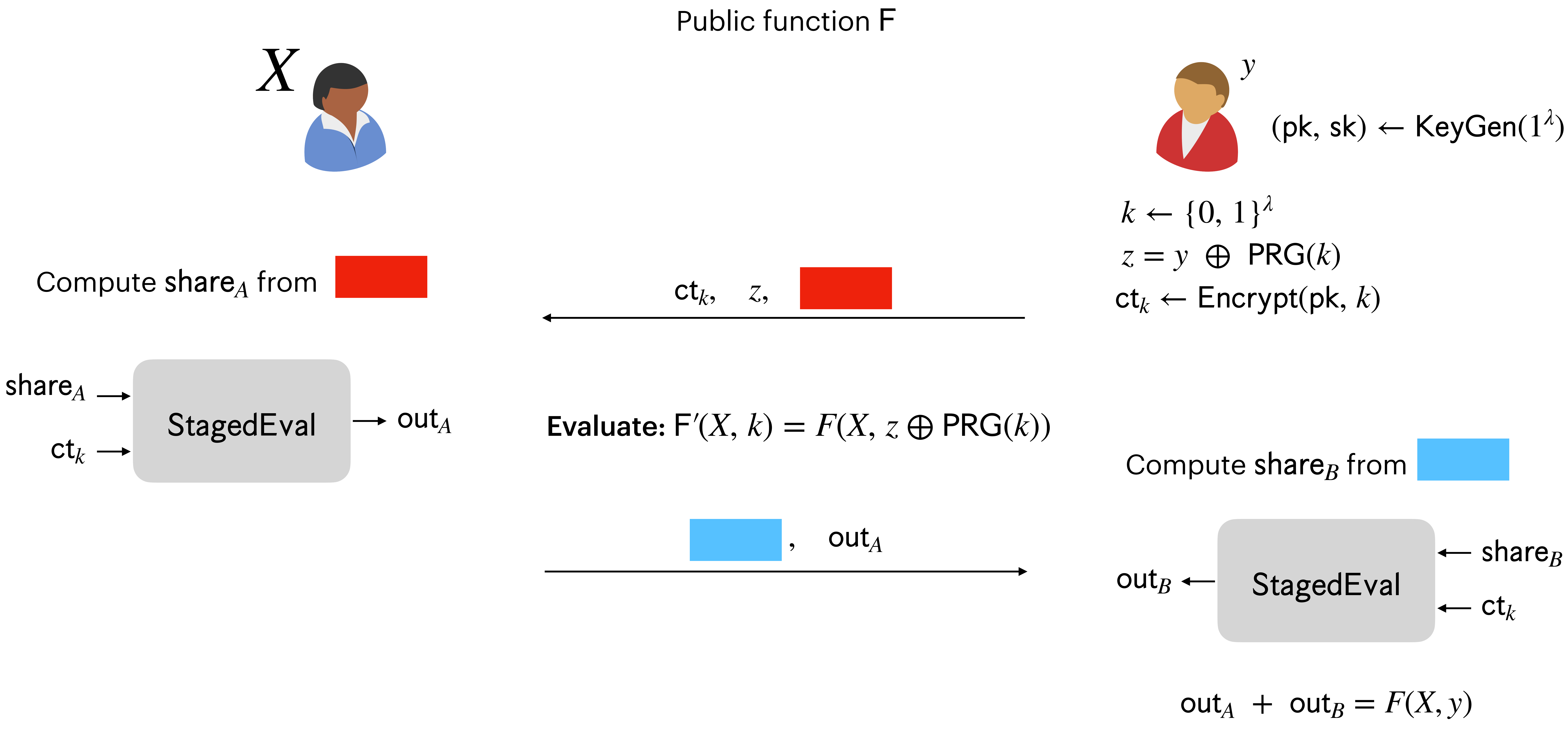
Compute share_B from

, out_A

Enhanced TDH = Staged HSS + Succinct Distribution of Shares



Enhanced TDH = Staged HSS + Succinct Distribution of Shares



Enhanced TDH = Staged HSS + Succinct Distribution of Shares

Public function F

X

y

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

Encoding key ek_y

$|\mathsf{ek}_y| = |y|(1 + o(1))$

$k \leftarrow \{0, 1\}^\lambda$

$z = y \oplus \mathsf{PRG}(k)$

$\mathsf{ct}_k \leftarrow \mathsf{Encrypt}(\mathsf{pk}, k)$

Compute share_A from

ct_k, z,

$\mathsf{share}_A \rightarrow$ StagedEval $\rightarrow \mathsf{out}_A$

$\mathsf{ct}_k \rightarrow$ StagedEval

Evaluate: $\mathsf{F}'(X, k) = F(X, z \oplus \mathsf{PRG}(k))$

Compute share_B from

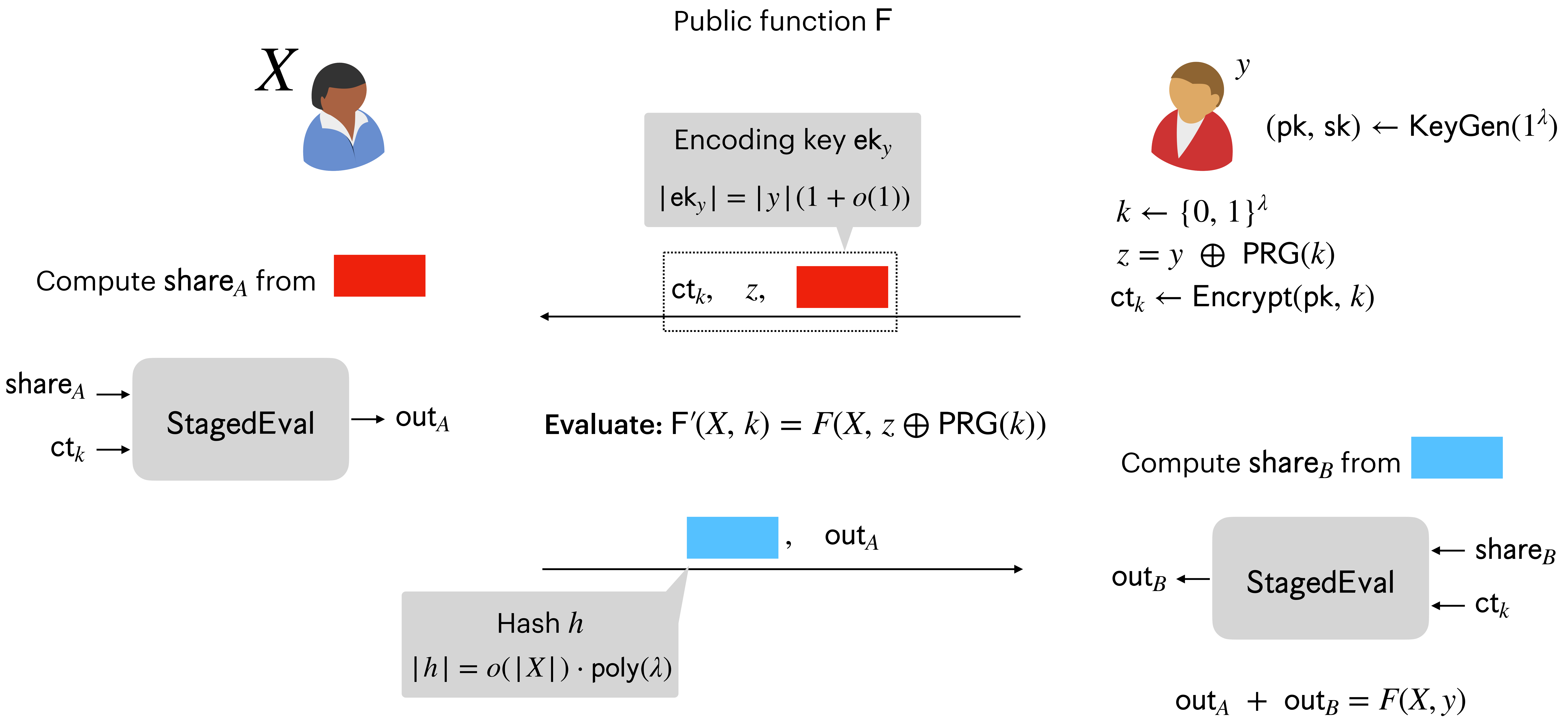
, out_A

$\mathsf{out}_B \leftarrow$ StagedEval $\leftarrow \mathsf{share}_B$

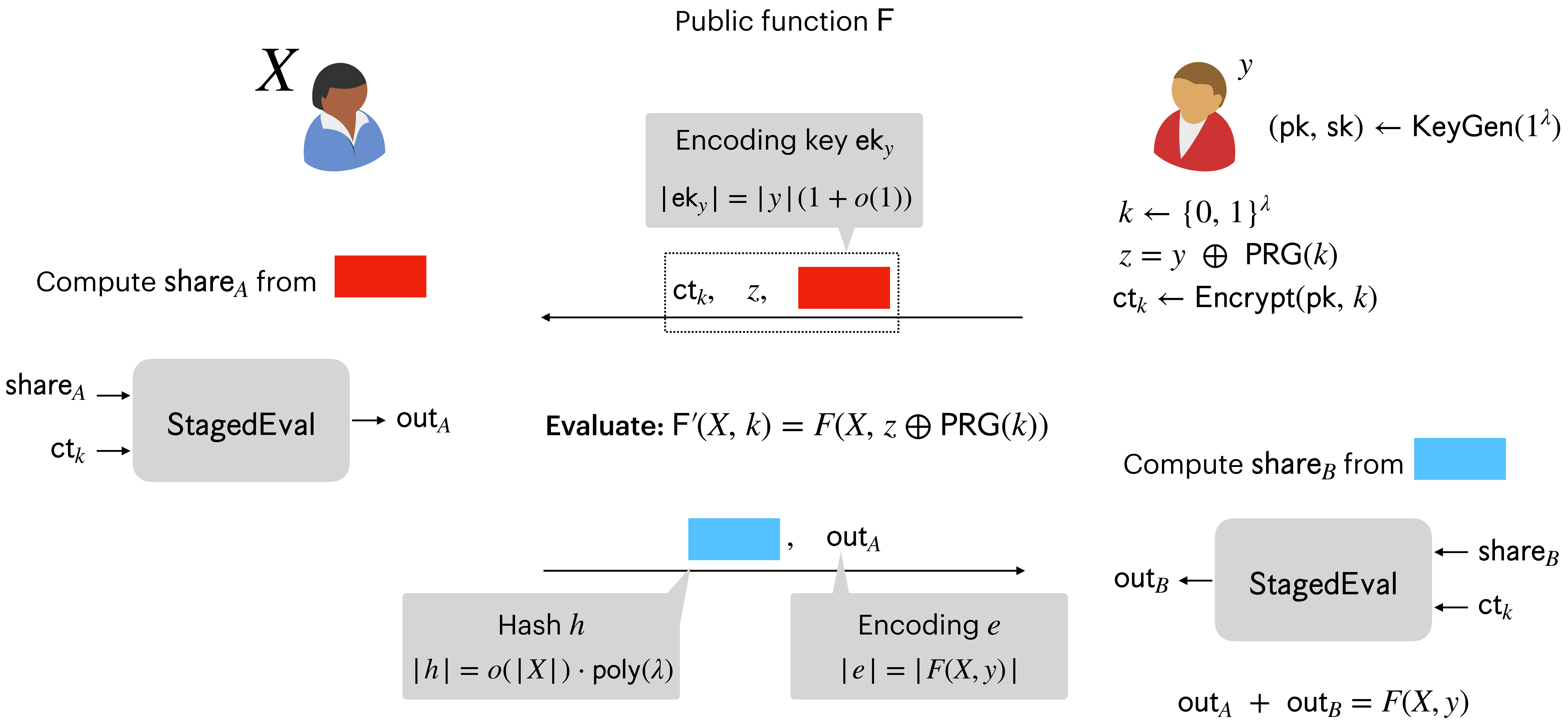
StagedEval $\leftarrow \mathsf{ct}_k$

$\mathsf{out}_A + \mathsf{out}_B = F(X, y)$

Enhanced TDH = Staged HSS + Succinct Distribution of Shares



Enhanced TDH = Staged HSS + Succinct Distribution of Shares



Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

$\text{Share}(\mathsf{pk}, X)$

share_A

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

For each bit b of sk

$\text{ElGamal}(\mathsf{pk}, b \cdot x_1) \quad \cdots \quad \text{ElGamal}(\mathsf{pk}, b \cdot x_n)$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

Share(pk, X)

share_A

For each bit b of sk

$$\mathsf{ElGamal}(\mathsf{pk}, b \cdot x_1) \quad \cdots \quad \mathsf{ElGamal}(\mathsf{pk}, b \cdot x_n)$$

$$=$$

$$(g^{r_1}, g^{\mathsf{sk} \cdot r_1} \cdot g^{b \cdot x_1}) \quad \cdots \quad (g^{r_1}, g^{\mathsf{sk} \cdot r_1} \cdot g^{b \cdot x_n})$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

Share(pk, X)

share_A $\qquad$ share_B

$\mathbb{G}, g$

$\text{sk} \leftarrow \mathbb{Z}_p$

$\text{pk} = g^{\text{sk}}$

For each bit b of sk

ElGamal(pk, $b \cdot x_1$) $\cdots$ ElGamal(pk, $b \cdot x_n$)

$=$

$(g^{r_1}, g^{\text{sk}\cdot r_1} \cdot g^{b \cdot x_1}) \quad \cdots \quad (g^{r_1}, g^{\text{sk}\cdot r_1} \cdot g^{b \cdot x_n})$

$g^{r_1} \ldots g^{r_n}$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

$\mathbb{G}, g$

sk $\leftarrow \mathbb{Z}_p$

pk $= g^{\mathsf{sk}}$

Share(pk, X)

share_A $\qquad$ share_B

For each bit b of sk

$$\mathsf{ElGamal}(\mathsf{pk}, b \cdot x_1) \quad \cdots \quad \mathsf{ElGamal}(\mathsf{pk}, b \cdot x_n)$$

$$=$$

$$(g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_1}) \quad \cdots \quad (g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_n})$$

$$g^{r_1} \ldots g^{r_n}$$

share_B only consists of the random component of the ciphertext

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$$\mathsf{share}_A \xleftarrow{} \mathsf{Share}(\mathsf{pk}, X) \xrightarrow{} \mathsf{share}_B$$

For each bit b of sk

$$\mathsf{ElGamal}(\mathsf{pk}, b \cdot x_1) \quad \cdots \quad \mathsf{ElGamal}(\mathsf{pk}, b \cdot x_n)$$

$$=$$

$$(g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_1}) \quad \cdots \quad (g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_n})$$

$$g^{r_1} \ldots g^{r_n}$$

share_B only consists of the random component of the ciphertext

Attempt:

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \dots, x_n)$

$\text{Share}(\text{pk}, X)$

share_A $\quad$ share_B

$\mathbb{G}, g$

$\text{sk} \leftarrow \mathbb{Z}_p$

$\text{pk} = g^{\text{sk}}$

For each bit b of sk

$\text{ElGamal}(\text{pk}, b \cdot x_1) \quad \cdots \quad \text{ElGamal}(\text{pk}, b \cdot x_n)$

$=$

$(g^{r_1}, g^{\text{sk}\cdot r_1} \cdot g^{b \cdot x_1}) \quad \cdots \quad (g^{r_1}, g^{\text{sk}\cdot r_1} \cdot g^{b \cdot x_n})$

$g^{r_1} \dots \; g^{r_n}$

share_B only consists of the random component of the ciphertext

Attempt:

$k \leftarrow \{0, 1\}^\lambda$

$r_1, \dots, r_n \leftarrow \text{PRG}(k)$

$g^{r_1} \dots \; g^{r_n}$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

$\mathsf{Share}(\mathsf{pk}, X)$

share_A $\quad$ share_B

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

For each bit b of sk

$$\mathsf{ElGamal}(\mathsf{pk}, b \cdot x_1) \quad \cdots \quad \mathsf{ElGamal}(\mathsf{pk}, b \cdot x_n)$$

$$=$$

$$(g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_1}) \quad \cdots \quad (g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_n})$$

$$g^{r_1} \ldots \; g^{r_n}$$

share_B only consists of the random component of the ciphertext

Attempt:

$$k \leftarrow \{0, 1\}^\lambda$$

$$\xleftarrow{\;k,\ \mathsf{pk}\;}$$

$r_1, \ldots, r_n \leftarrow \mathsf{PRG}(k)$

$g^{r_1} \ldots \; g^{r_n}$

$r_1, \ldots, r_n \leftarrow \mathsf{PRG}(k)$

$g^{r_1} \ldots \; g^{r_n}$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

Share(pk, X)

share_A $\quad$ share_B

$\mathbb{G}, g$

$\text{sk} \leftarrow \mathbb{Z}_p$

$\text{pk} = g^{\text{sk}}$

For each bit b of sk

ElGamal(pk, $b \cdot x_1$) $\quad \cdots \quad$ ElGamal(pk, $b \cdot x_n$)

$=$

$(g^{r_1}, g^{\text{sk}\cdot r_1} \cdot g^{b \cdot x_1}) \quad \cdots \quad (g^{r_1}, g^{\text{sk}\cdot r_1} \cdot g^{b \cdot x_n})$

$g^{r_1} \ldots \; g^{r_n}$

share_B only consists of the random component of the ciphertext

Attempt:

$r_1, \ldots, r_n \leftarrow \text{PRG}(k)$

$g^{r_1} \ldots \; g^{r_n}$

$g^{\text{sk}\cdot r_1} \; \ldots \; g^{\text{sk}\cdot r_n}$

$\xleftarrow{\;k,\ \text{pk}\;}$

$k \leftarrow \{0, 1\}^\lambda$

$r_1, \ldots, r_n \leftarrow \text{PRG}(k)$

$g^{r_1} \ldots \; g^{r_n}$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$$\mathsf{share}_A \xleftarrow{} \mathsf{Share}(\mathsf{pk}, X) \xrightarrow{} \mathsf{share}_B$$

For each bit b of sk

$\mathsf{ElGamal}(\mathsf{pk}, b \cdot x_1) \quad \cdots \quad \mathsf{ElGamal}(\mathsf{pk}, b \cdot x_n)$

$=$

$(g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}) \quad \cdots \quad (g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$g^{r_1} \ldots \; g^{r_n}$

share$_B$ only consists of the random component of the ciphertext

Attempt:

$k \leftarrow \{0, 1\}^\lambda$

$r_1, \ldots, r_n \leftarrow \mathsf{PRG}(k)$

$g^{r_1} \ldots \; g^{r_n}$

$\xleftarrow{\;k,\ \mathsf{pk}\;}$

$r_1, \ldots, r_n \leftarrow \mathsf{PRG}(k)$

$g^{r_1} \ldots \; g^{r_n}$

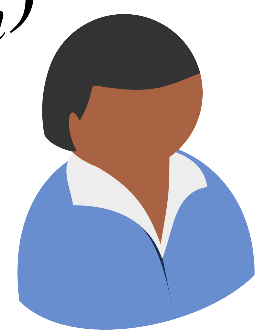
$g^{\mathsf{sk}\cdot r_1} \; \ldots \; g^{\mathsf{sk}\cdot r_n}$

Alice needs g^b to compute $g^{\mathsf{sk}\cdot r_i} \cdot g^{b\cdot x_i}$ but sending this would be insecure

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$



$\mathsf{Share}(\mathsf{pk}, X)$

share_A share_B

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

For each bit b of sk

$\mathsf{ElGamal}(\mathsf{pk}, b \cdot x_1) \quad \cdots \quad \mathsf{ElGamal}(\mathsf{pk}, b \cdot x_n)$

$=$

$(g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}) \quad \cdots \quad (g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$g^{r_1} \ldots \; g^{r_n}$

share_B only consists of the random component of the ciphertext

Observation: Can be computed succinctly using techniques from Trapdoor Hashing [Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$X = (x_1, \ldots, x_n)$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$$(g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$$
$$\vdots$$
$$(g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$$

$g^{r_1} \quad \ldots \quad g^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$$
$$\vdots$$
$$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$$

$g^{r_1} \quad \ldots \quad g^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$$g_1,\ \ldots,\ g_n \leftarrow \mathbb{G}$$
$$r_1 \leftarrow \mathbb{Z}_p$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$

$\vdots$

$(g^{r_1}, g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$g^{r_1} \ \cdots \ g^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1, \ \ldots, \ g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, \ g_n^{\mathsf{sk}\cdot r_1})$

$g_1, \ \ldots, \ g_n \leftarrow \mathbb{G}$

$r_1 \leftarrow \mathbb{Z}_p$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$$
$$\vdots$$
$$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$$

$g^{r_1} \ \ldots \ g^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$$(g_1,\ \ldots,\ g_n)$$
$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \ldots,\ g_n^{\mathsf{sk}\cdot r_1})$$

$g_1,\ \ldots,\ g_n \leftarrow \mathbb{G}$

$r_1 \leftarrow \mathbb{Z}_p$

$$h = (g_1,\ \ldots,\ g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$

$\vdots$

$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$g^{r_1} \ \ldots \ g^{r_n}$

$\mathbb{G},\ g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1,\ \ldots,\ g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \ldots,\ g_n^{\mathsf{sk}\cdot r_1})$

$g_1,\ \ldots,\ g_n \leftarrow \mathbb{G}$

$r_1 \leftarrow \mathbb{Z}_p$

$$h = (g_1,\ \ldots,\ g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \ldots,\ g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$

$\vdots$

$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$g^{r_1} \ \ldots \ g^{r_n}$

$\mathbb{G},\ g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1,\ \ldots,\ g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \ldots,\ g_n^{\mathsf{sk}\cdot r_1})$

$\longleftarrow$

$g_1,\ \ldots,\ g_n \leftarrow \mathbb{G}$

$r_1 \leftarrow \mathbb{Z}_p$

$$h = (g_1,\ \ldots,\ g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \ldots,\ g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T$$

$$= \left(\prod_{i=1}^{n} g_i^{x_i}\right)^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_1})$

$\vdots$

$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_n})$

$g^{r_1} \ \ldots \ g^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$$\xleftarrow[\qquad]{(g_1,\ \ldots,\ g_n) \quad (g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \ldots,\ g_n^{\mathsf{sk}\cdot r_1})}$$

$g_1,\ \ldots,\ g_n \leftarrow \mathbb{G}$

$r_1 \leftarrow \mathbb{Z}_p$

$$h = (g_1,\ \ldots,\ g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \ldots,\ g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T$$

$$= \left(\prod_{i=1}^{n} g_i^{x_i}\right)^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1} = h^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_1}$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \dots, x_n)$

$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$

$\vdots$

$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$g^{r_1}\ \dots\ g^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1,\ \dots,\ g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \dots,\ g_n^{\mathsf{sk}\cdot r_1})$

$g_1,\ \dots,\ g_n \leftarrow \mathbb{G}$

$r_1 \leftarrow \mathbb{Z}_p$

$$h = (g_1,\ \dots,\ g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \dots,\ g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T$$

$$= \left(\prod_{i=1}^{n} g_i^{x_i}\right)^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1} = h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

$$(g^{r_1},\ g^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$$

A change in "base" from $g^{\mathsf{sk}\cdot r_1}$ to $h^{\mathsf{sk}\cdot r_1}$
does not affect staged HSS evaluation

$$= h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$$(h^{r_1},\ h^{\mathsf{sk}\cdot r_1}\cdot g^{b\cdot x_1})$$
$$\vdots$$
$$(h^{r_1},\ h^{\mathsf{sk}\cdot r_1}\cdot g^{b\cdot x_n})$$

$$h^{r_1}\ \ldots\ h^{r_n}$$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1, \ldots, g_n)$

$(g_1^{\mathsf{sk}\cdot r_1}\cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ldots, g_n^{\mathsf{sk}\cdot r_1})$

$g_1, \ldots, g_n \leftarrow \mathbb{G}$

$r_1 \leftarrow \mathbb{Z}_p$

A change in "base" from $g^{\mathsf{sk}\cdot r_1}$ to $h^{\mathsf{sk}\cdot r_1}$
does not affect staged HSS evaluation

$h = (g_1, \ldots$ $\prod_{i=1}$

$$(g_1^{\mathsf{sk}\cdot r_1}\cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ldots, g_n^{\mathsf{sk}\cdot r_1})\cdot X^T$$

$$= \left(\prod_{i=1}^{n} g_i^{x_i}\right)^{\mathsf{sk}\cdot r_1}\cdot g^{b\cdot x_1} = h^{\mathsf{sk}\cdot r_1}\cdot g^{b\cdot x_1}$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \dots, x_n)$

$(h^{r_1},\ h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$

$\vdots$

$(h^{r_1},\ h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$h^{r_1}\ \dots\ h^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1,\ \dots,\ g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \dots,\ g_n^{\mathsf{sk}\cdot r_1})$

$g_1,\ \dots,\ g_n \leftarrow \mathbb{G}$

$r_1 \leftarrow \mathbb{Z}_p$

$$h = (g_1,\ \dots,\ g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b},\ g_2^{\mathsf{sk}\cdot r_1},\ \dots,\ g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$$
$$\vdots$$
$$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$$

$h^{r_1} \ \ldots \ h^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$$(g_1, \ \ldots, g_n)$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1})$$

$$(g_1^{\mathsf{sk}\cdot r_2}, g_2^{\mathsf{sk}\cdot r_2} \cdot g^{b}, \ \ldots, g_n^{\mathsf{sk}\cdot r_2})$$

$g_1, \ \ldots, g_n \leftarrow \mathbb{G}$

$r_1, r_2 \leftarrow \mathbb{Z}_p$

$$h = (g_1, \ \ldots, g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$$

$$(g_1^{\mathsf{sk}\cdot r_2}, g_2^{\mathsf{sk}\cdot r_2} \cdot g^{b}, \ \ldots, g_n^{\mathsf{sk}\cdot r_2}) \cdot X^T = h^{\mathsf{sk}\cdot r_2} \cdot g^{b\cdot x_2}$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

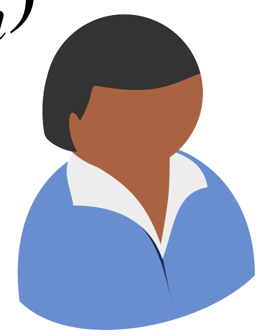
Goal

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$X = (x_1, \ldots, x_n)$



$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_1})$

$\vdots$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_n})$

$h^{r_1} \ \ldots \ h^{r_n}$

$(g_1, \ \ldots, g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1})$

$\vdots$

$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n} \cdot g^{b})$

$g_1, \ \ldots, g_n \leftarrow \mathbb{G}$

$r_1, \ldots r_n \leftarrow \mathbb{Z}_p$

$$h = (g_1, \ \ldots, g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_1}$$

$$\vdots$$

$$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n} \cdot g^{b}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n}) \cdot X^T = h^{\mathsf{sk}\cdot r_n} \cdot g^{b \cdot x_n}$$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_1})$

$\vdots$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_n})$

$h^{r_1} \ \ldots \ h^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1, \ \ldots, g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1})$

$\vdots$

$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n} \cdot g^{b})$

$g_1, \ \ldots, g_n \leftarrow \mathbb{G}$

$r_1, \ldots r_n \leftarrow \mathbb{Z}_p$

$$h = (g_1, \ \ldots, g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$$

$$\vdots$$

$$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n} \cdot g^{b}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n}) \cdot X^T = h^{\mathsf{sk}\cdot r_n} \cdot g^{b\cdot x_n}$$

$h^{r_1}, \ldots, h^{r_n}$ can be computed similarly

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$

$\vdots$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$h^{r_1} \ \ldots \ h^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1, \ \ldots, g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^b, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1})$

$\vdots$

$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n} \cdot g^b)$

$g_1, \ \ldots, g_n \leftarrow \mathbb{G}$

$r_1, \ldots r_n \leftarrow \mathbb{Z}_p$

$$h = (g_1, \ \ldots, g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^b, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$$

$$\vdots$$

$$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n} \cdot g^b, \ \ldots, g_n^{\mathsf{sk}\cdot r_n}) \cdot X^T = h^{\mathsf{sk}\cdot r_n} \cdot g^{b\cdot x_n}$$

h

$h^{r_1}, \ldots, h^{r_n}$ can be computed similarly

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$

$\vdots$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$h^{r_1} \ \ldots \ h^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1, \ \ldots, g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^b, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1})$

$\vdots$

$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n} \cdot g^b)$

$g_1, \ \ldots, g_n \leftarrow \mathbb{G}$

$r_1, \ldots r_n \leftarrow \mathbb{Z}_p$

$$h = (g_1, \ \ldots, g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^b, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$$

$$\vdots$$

$$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n} \cdot g^b, \ \ldots, g_n^{\mathsf{sk}\cdot r_n}) \cdot X^T = h^{\mathsf{sk}\cdot r_n} \cdot g^{b\cdot x_n}$$

$\xrightarrow{h}$

$h^{r_1}, \ldots, h^{r_n}$

$h^{r_1}, \ldots, h^{r_n}$ can be computed similarly

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_1})$

$\vdots$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_n})$

$h^{r_1} \ \ldots \ h^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1, \ \ldots, g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1})$

$\vdots$

$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n} \cdot g^{b})$

$g_1, \ \ldots, g_n \leftarrow \mathbb{G}$

$r_1, \ldots r_n \leftarrow \mathbb{Z}_p$

$$h = (g_1, \ \ldots, g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b \cdot x_1}$$

$$\vdots$$

$$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n} \cdot g^{b}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n}) \cdot X^T = h^{\mathsf{sk}\cdot r_n} \cdot g^{b \cdot x_n}$$

Hash needs to be randomized for security

$\xrightarrow{\quad h \quad}$

$h^{r_1}, \ldots, h^{r_n}$

$h^{r_1}, \ldots, h^{r_n}$ can be computed similarly

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$

$\vdots$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$h^{r_1} \ \ldots \ h^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1, \ \ldots, g_n)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^b, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1})$

$\vdots$

$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n} \cdot g^b)$

$g_1, \ \ldots, g_n \leftarrow \mathbb{G}$

$r_1, \ldots r_n \leftarrow \mathbb{Z}_p$

$h = (g_1, \ \ldots, g_n) \cdot X^T = \prod_{i=1}^{n} g_i^{x_i}$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^b, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$

$\vdots$

$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n} \cdot g^b, \ \ldots, g_n^{\mathsf{sk}\cdot r_n}) \cdot X^T = h^{\mathsf{sk}\cdot r_n} \cdot g^{b\cdot x_n}$

$\xrightarrow{h}$

$h^{r_1}, \ldots, h^{r_n}$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$
$\vdots$
$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$h^{r_1} \ \ldots \ h^{r_n}$

$\mathbb{G}, g$
$\mathsf{sk} \leftarrow \mathbb{Z}_p$
$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1, \ \ldots, \ g_n)$

$g_1, \ \ldots, \ g_n \leftarrow \mathbb{G}$
$r_1, \ldots r_n \leftarrow \mathbb{Z}_p$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, \ g_n^{\mathsf{sk}\cdot r_1})$$
$$\vdots$$
$$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n}, \ \ldots, \ g_n^{\mathsf{sk}\cdot r_n} \cdot g^{b})$$

$h = (g_1, \ \ldots, \ g_n) \cdot X^T$

$O(\lambda \cdot n^2)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, \ g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$
$\vdots$
$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n} \cdot g^{b}, \ \ldots, \ g_n^{\mathsf{sk}\cdot r_n}) \cdot X^T = h^{\mathsf{sk}\cdot r_n} \cdot g^{b\cdot x_n}$

h

$h^{r_1}, \ldots, h^{r_n}$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$
$\vdots$
$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$h^{r_1} \ \ldots \ h^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1, \ldots, g_n)$

$$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ldots, g_n^{\mathsf{sk}\cdot r_1})$$
$$\vdots$$
$$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n}, \ldots, g_n^{\mathsf{sk}\cdot r_n} \cdot g^{b})$$

$g_1, \ldots, g_n \leftarrow \mathbb{G}$

$r_1, \ldots, r_n \leftarrow \mathbb{Z}_p$

$h = (g_1, \ldots, g_n) \cdot X^T$

$O(\lambda \cdot n^2)$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ldots, g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$

$\vdots$

$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n} \cdot g^{b}, \ldots, g_n^{\mathsf{sk}\cdot r_n}) \cdot X^T = h^{\mathsf{sk}\cdot r_n} \cdot g^{b\cdot x_n}$

$O(\lambda)$

h

$h^{r_1}, \ldots, h^{r_n}$

Succinct Distribution of Staged Input Shares

Structure of Staged Input Shares

Goal

$X = (x_1, \ldots, x_n)$

$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1})$
$\vdots$
$(h^{r_1}, h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_n})$

$h^{r_1} \ \ldots \ h^{r_n}$

$\mathbb{G}, g$

$\mathsf{sk} \leftarrow \mathbb{Z}_p$

$\mathsf{pk} = g^{\mathsf{sk}}$

$(g_1, \ \ldots, g_n)$

$g_1, \ldots, g_n \leftarrow \mathbb{G}$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1})$
$\vdots$
$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n} \cdot g^{b})$

$O(\lambda \cdot n^2)$

Can be reused with multiple hashes $\Longrightarrow$ rebalancing gives $O(n^{2/3} \cdot \lambda)$ total communication

$h = (g_1, \ \ldots, g_n) \cdot X^T$

$(g_1^{\mathsf{sk}\cdot r_1} \cdot g^{b}, g_2^{\mathsf{sk}\cdot r_1}, \ \ldots, g_n^{\mathsf{sk}\cdot r_1}) \cdot X^T = h^{\mathsf{sk}\cdot r_1} \cdot g^{b\cdot x_1}$
$\vdots$
$(g_1^{\mathsf{sk}\cdot r_n}, g_2^{\mathsf{sk}\cdot r_n} \cdot g^{b}, \ \ldots, g_n^{\mathsf{sk}\cdot r_n}) \cdot X^T = h^{\mathsf{sk}\cdot r_n} \cdot g^{b\cdot x_n}$

$O(\lambda)$

h

$h^{r_1}, \ldots, h^{r_n}$

Conclusion

- Discussed approach assumes circular security of ElGamal. Constructing from plain DDH and DCR requires extending to circular-secure variants [Boneh-Halevi-Hamburg-Ostrovsky’08] [Brakerski-Goldwasser’10]
- DDH-based Staged HSS evaluation has noticeable error probability which affects privacy. Requires developing new techniques to build trapdoor hash functions

Conclusion

- Discussed approach assumes circular security of ElGamal. Constructing from plain DDH and DCR requires extending to circular-secure variants [Boneh-Halevi-Hamburg-Ostrovsky'08] [Brakerski-Goldwasser'10]
- DDH-based Staged HSS evaluation has noticeable error probability which affects privacy. Requires developing new techniques to build trapdoor hash functions

Thank You