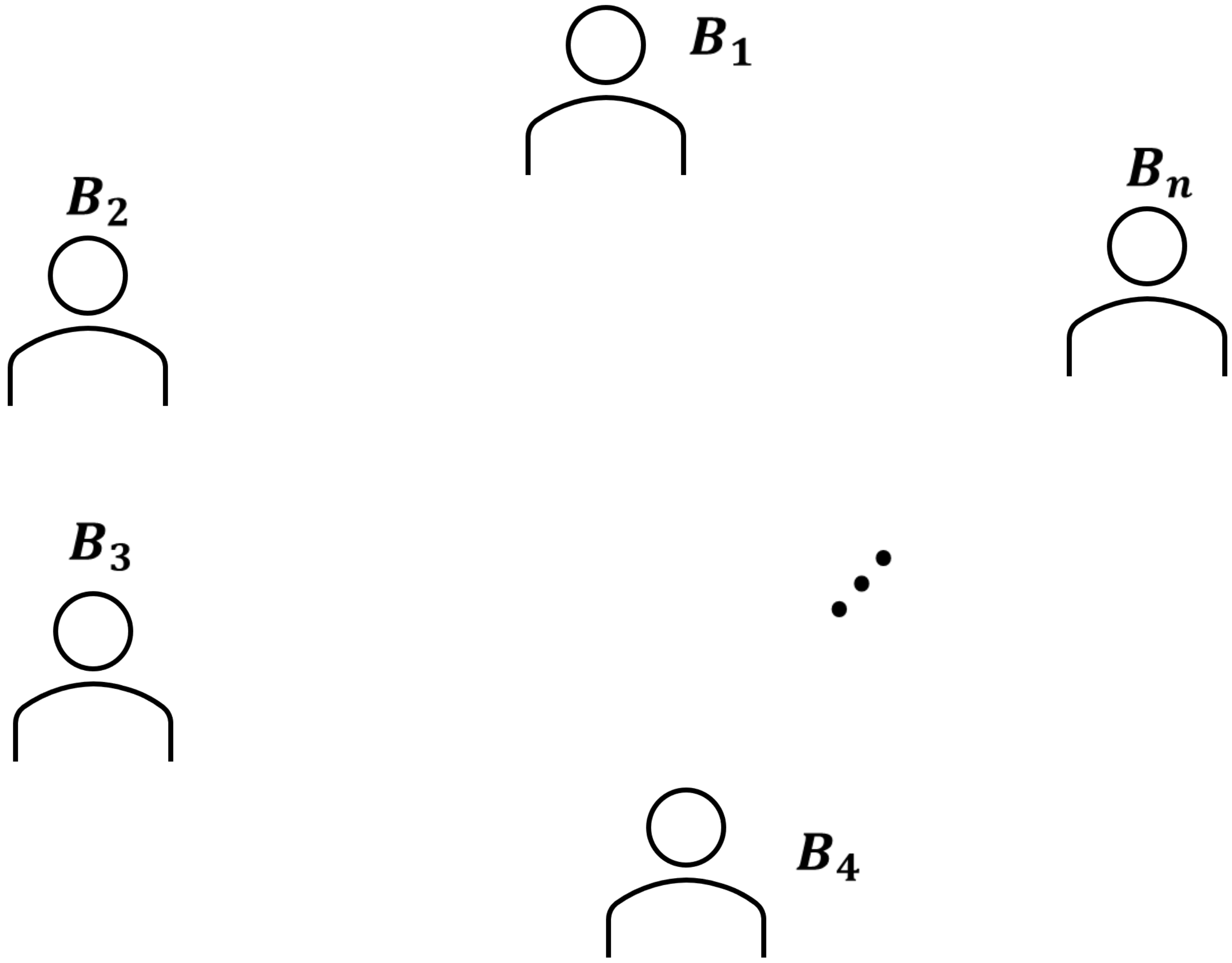
Simple, Fast, Efficient, and Tightly-Secure Non-Malleable Non-Interactive Timed Commitments

Peter Chvojka, Tibor Jager

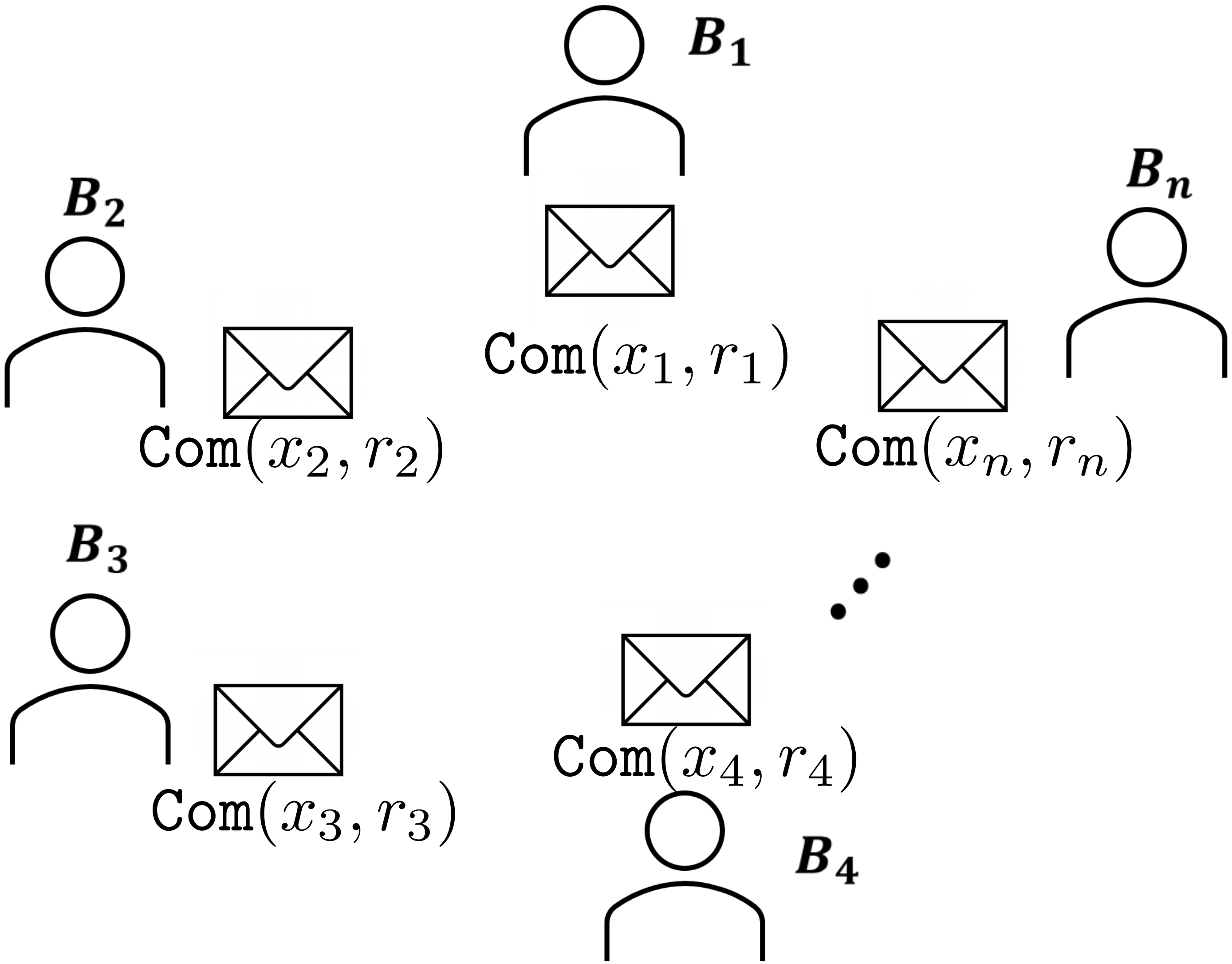
institute IMDEA software

BERGISCHE UNIVERSITÄT WUPPERTAL

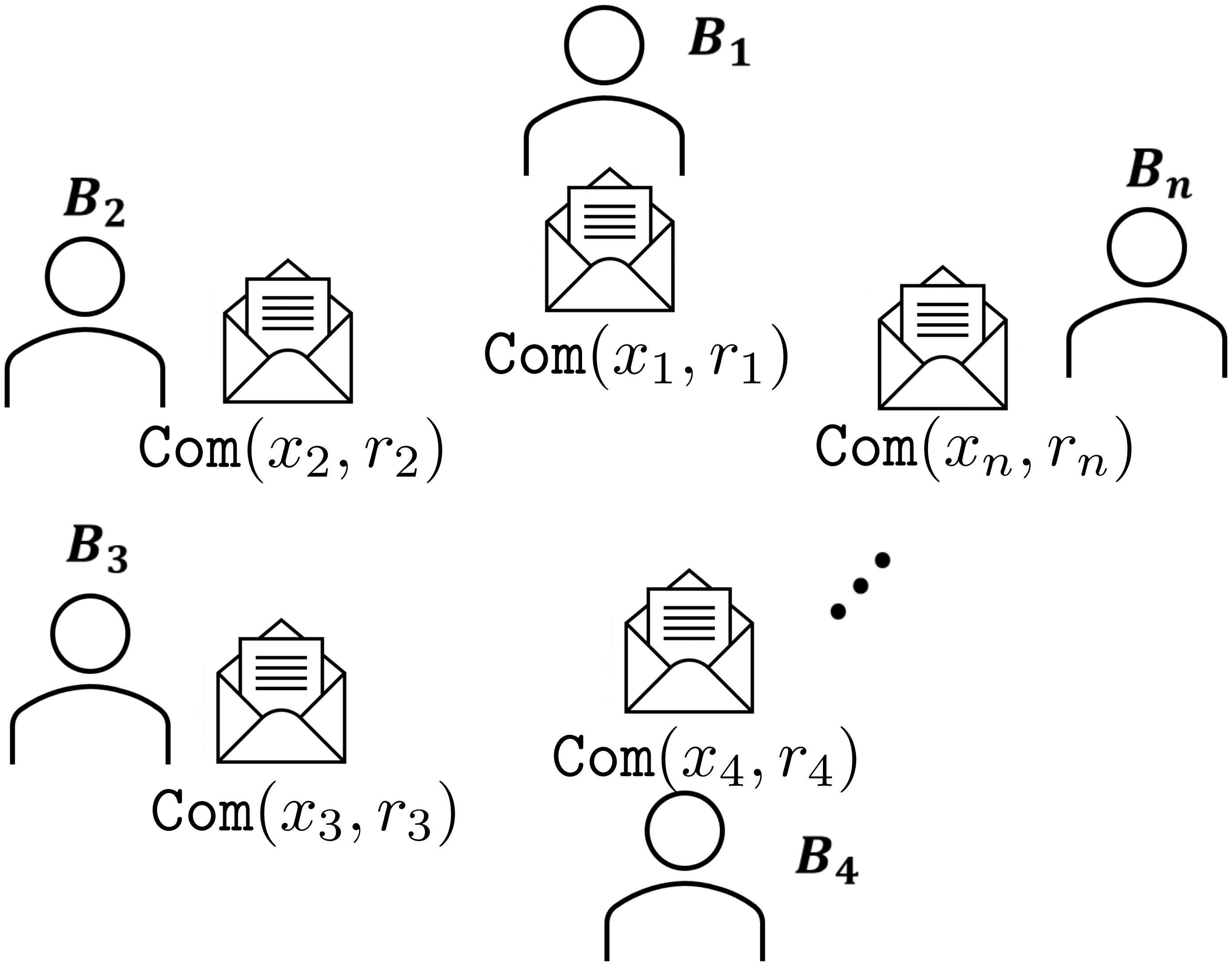
Motivation – Sealed-Bit Auction



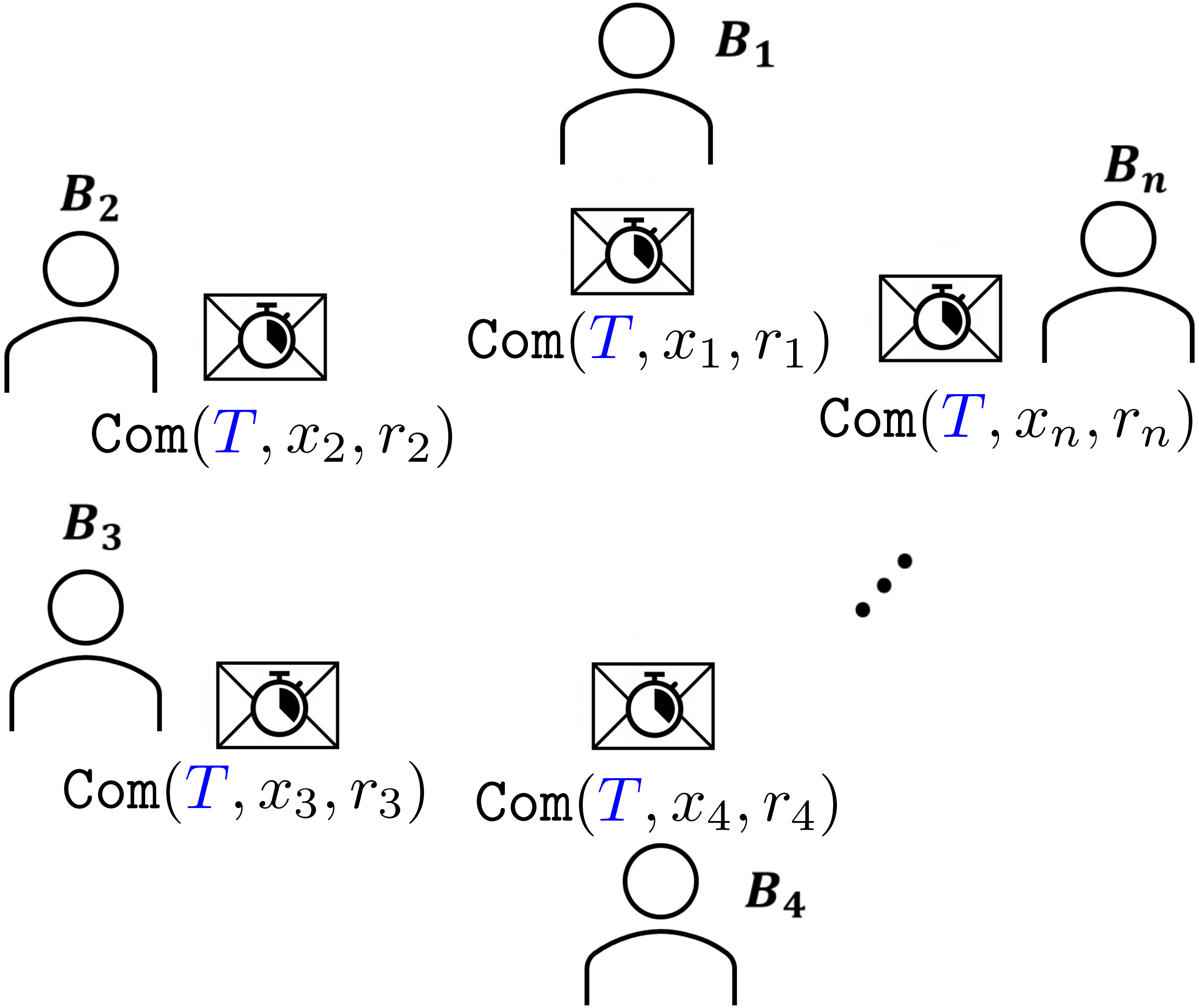
Motivation – Sealed-Bit Auction



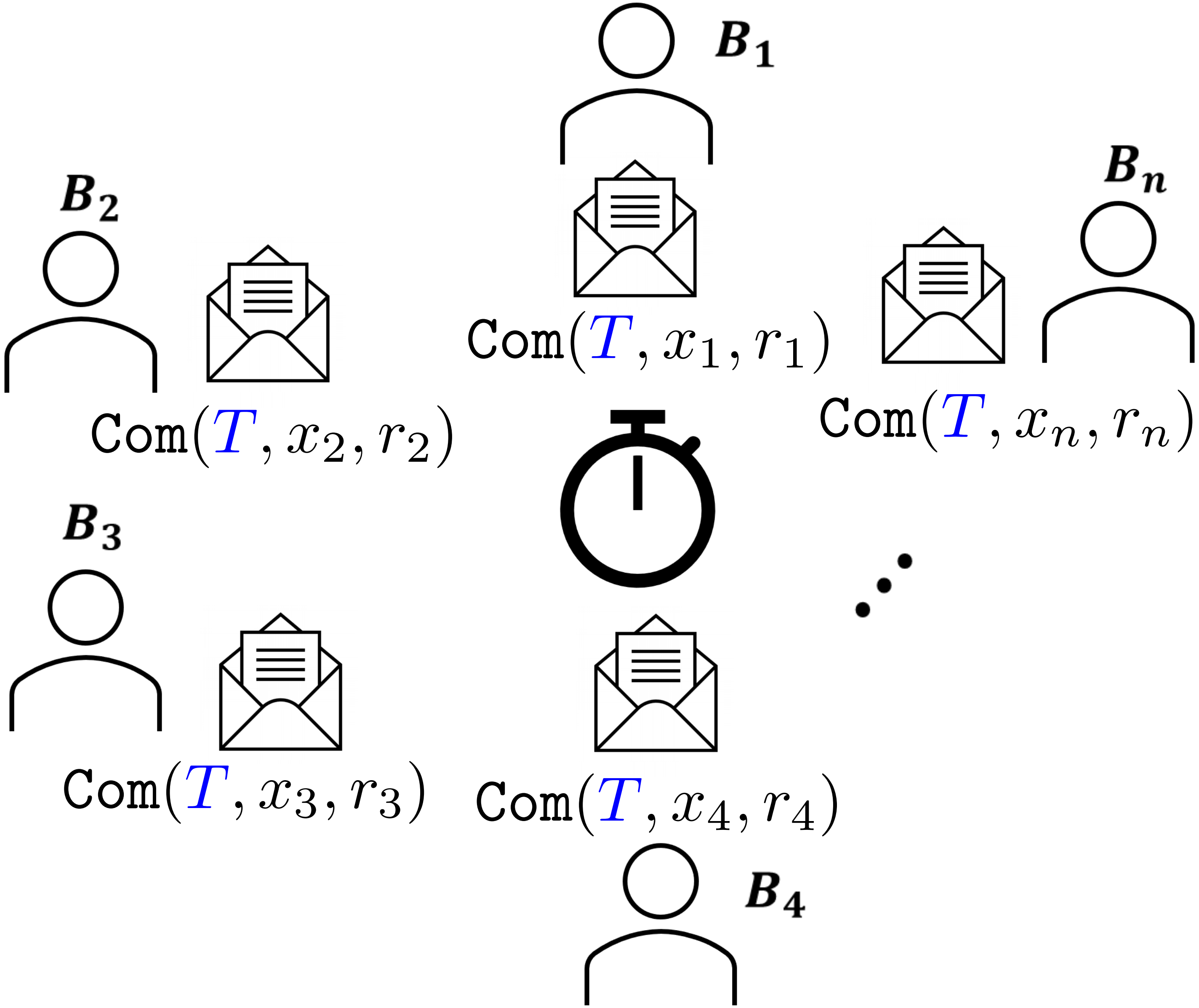
Motivation – Sealed-Bit Auction



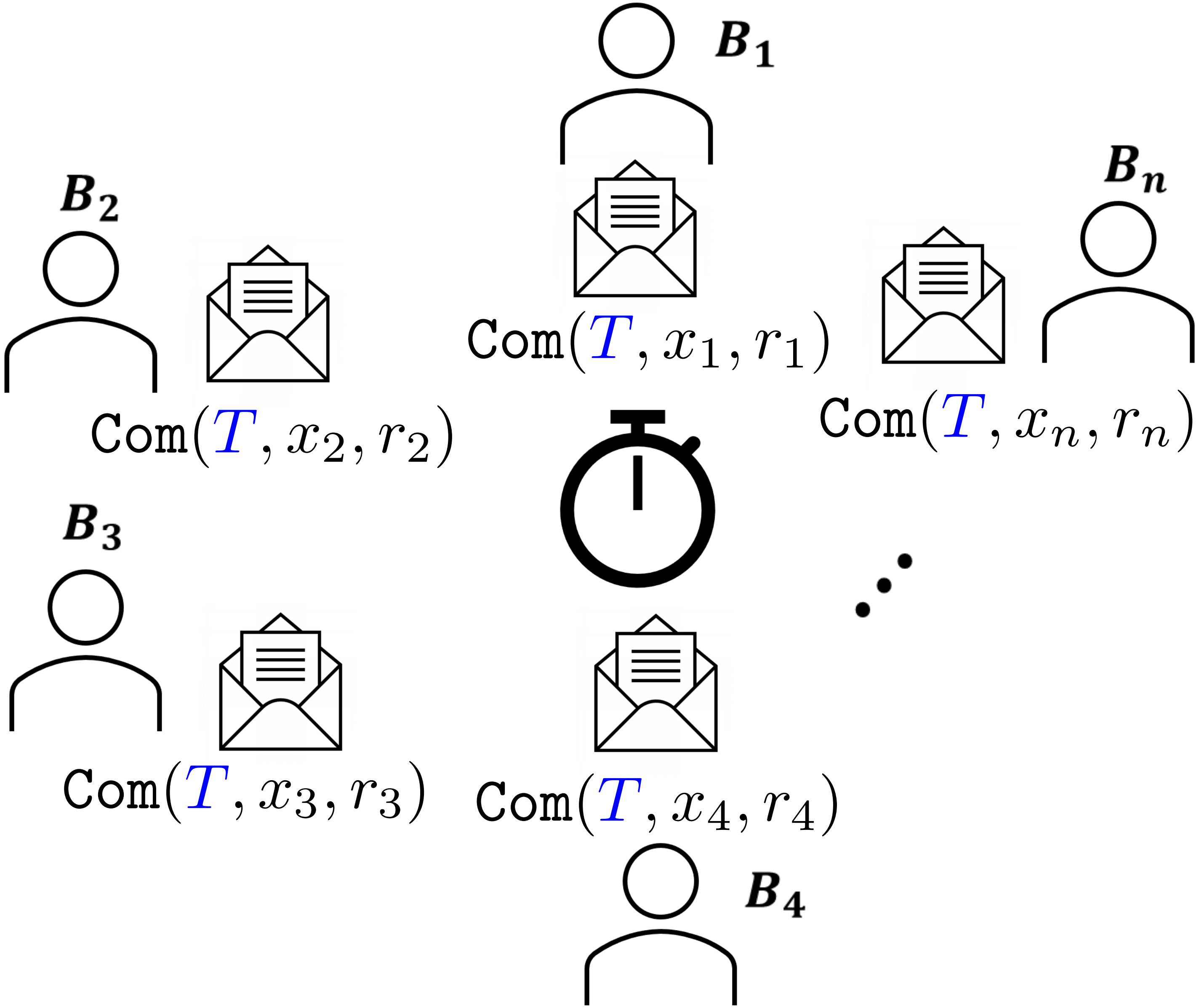
Motivation – Sealed-Bit Auction



Motivation – Sealed-Bit Auction

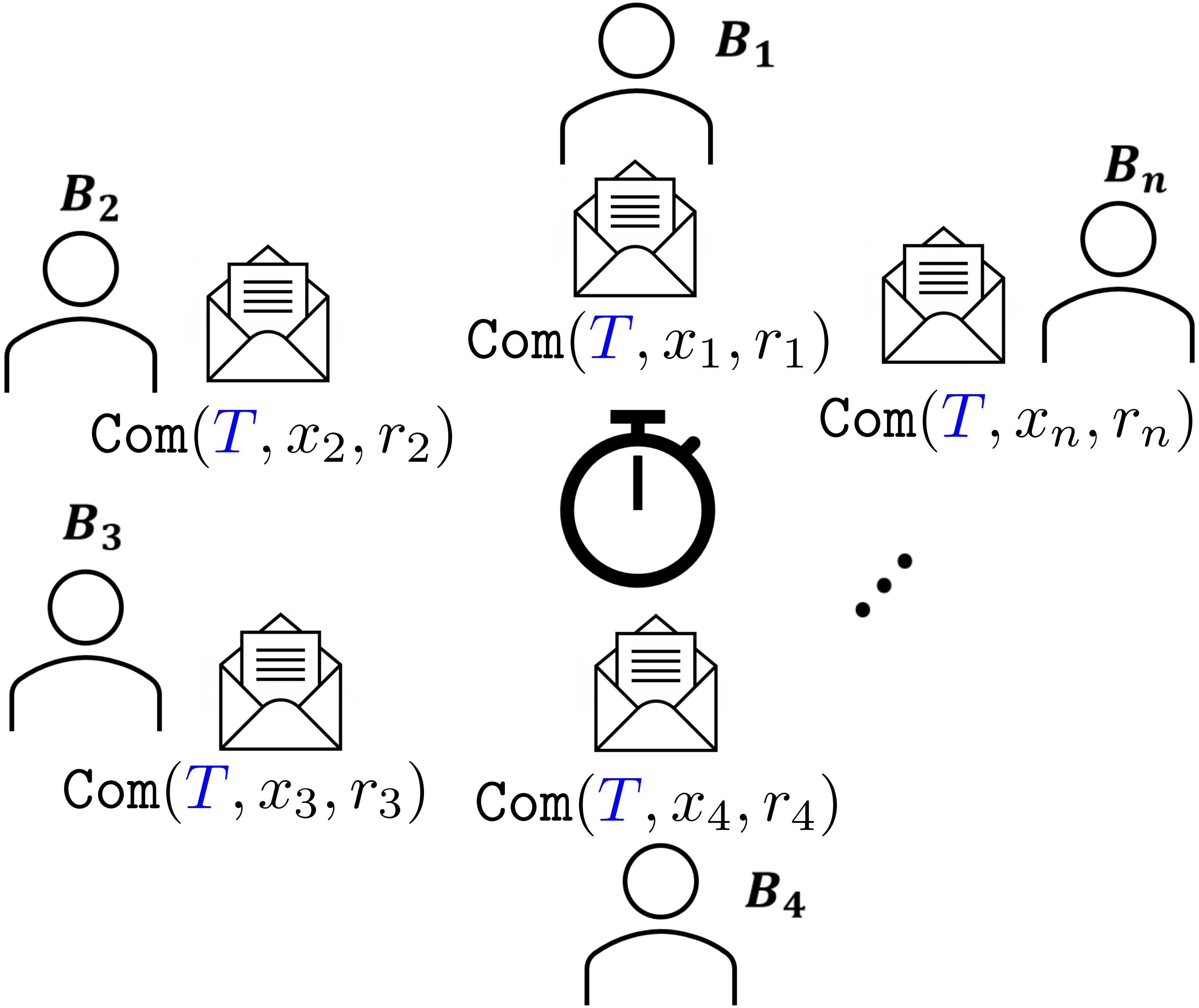


Motivation – Sealed-Bit Auction



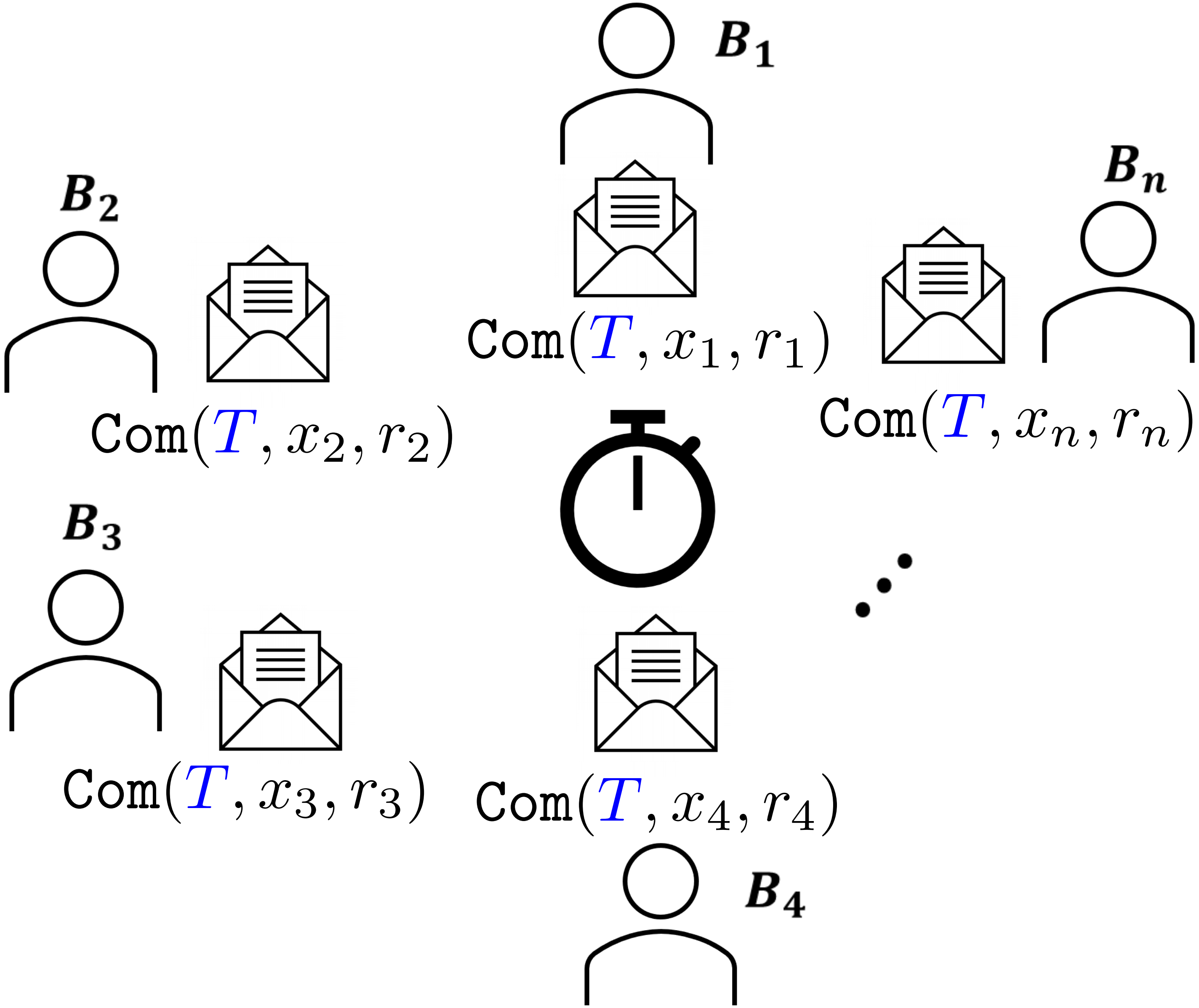
- Public Verifiability of Commitments

Motivation – Sealed-Bit Auction



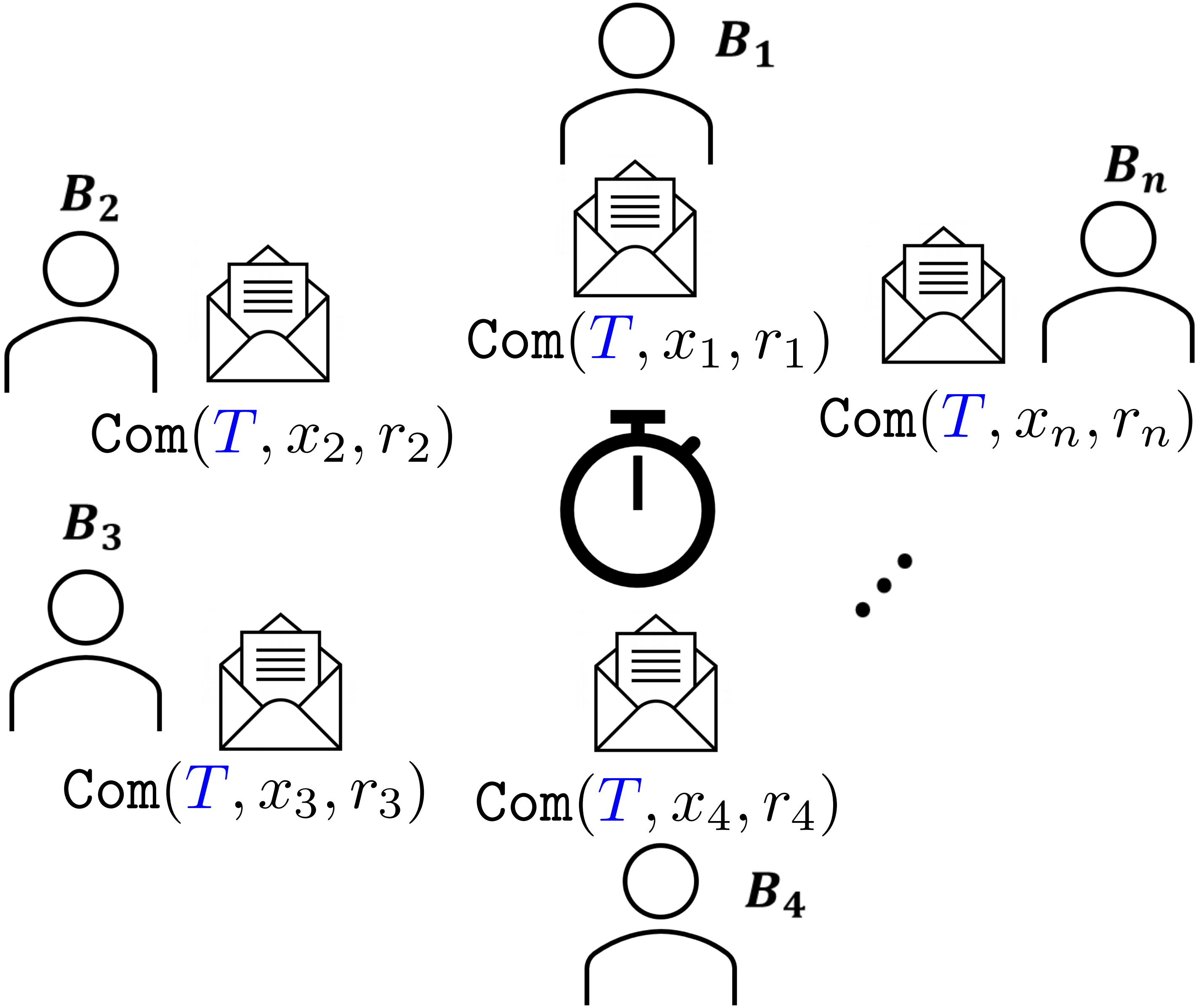
- Public Verifiability of Commitments
- Non-Interactivity

Motivation – Sealed-Bit Auction



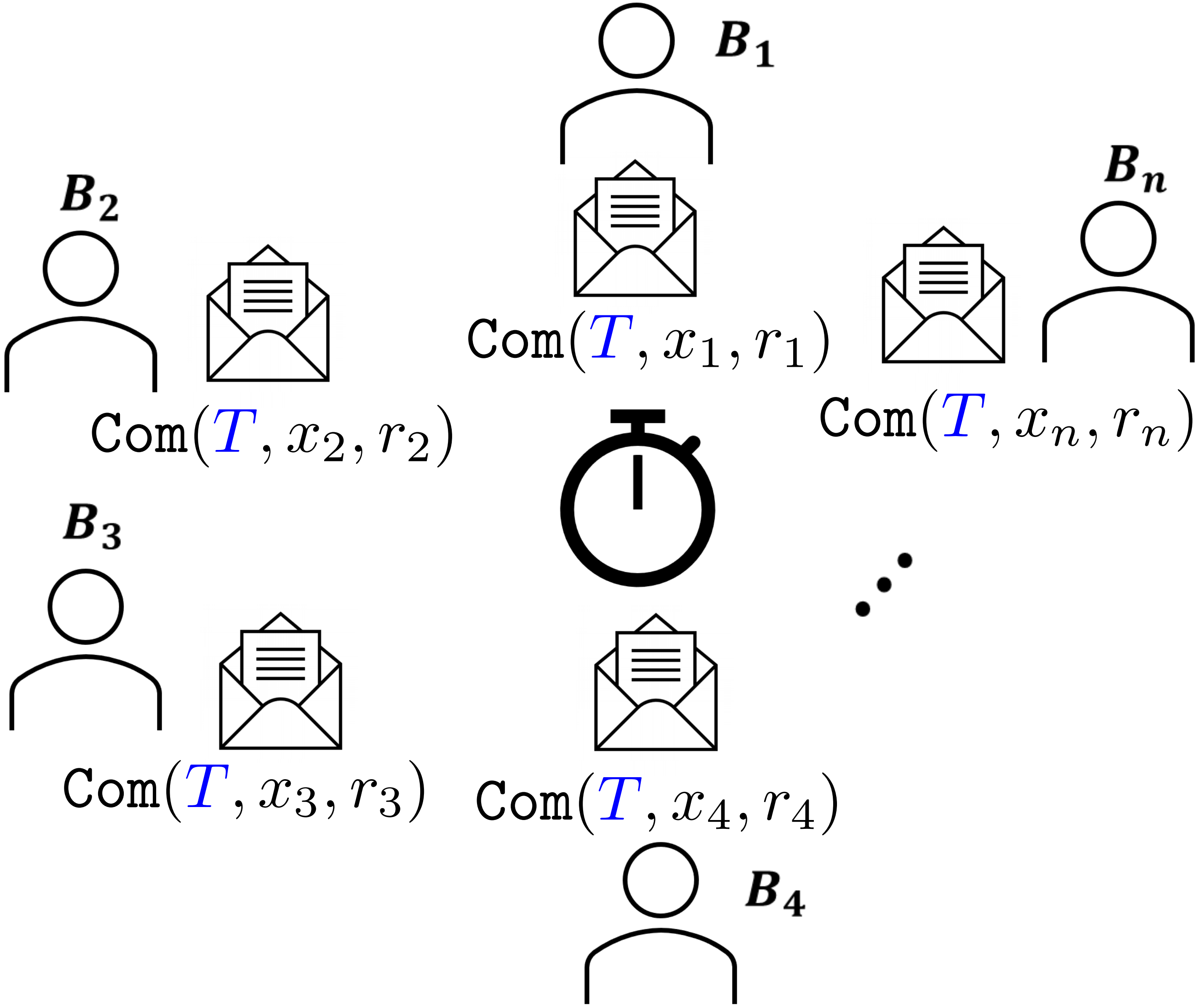
- Public Verifiability of Commitments
- Non-Interactivity
- Non-Malleability/CCA security

Motivation – Sealed-Bit Auction



- Public Verifiability of Commitments
- Non-Interactivity
- Non-Malleability/CCA security
- Homomorphic Properties

Motivation – Sealed-Bit Auction



- Public Verifiability of Commitments
- Non-Interactivity
- Non-Malleability/CCA security
- Homomorphic Properties
- Public Verifiability of Forced Decommitment

Applications

- Unbiased E-voting (MT19)
- Sealed Bid Auctions (MT19)
- Multi-Party Contract Signing (MT19)
- Fairness in Multi-Party Computation – Fair Coin Flipping (MT19)
- Revealing Census Data
- Responsible Disclosure of Security Flaws

Non-Interactive Timed Commitment
(KLX20)

- $\mathsf{crs} \leftarrow \mathsf{PGen}(1^\lambda, T)$
- $(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m)$
- $0/1 \leftarrow \mathsf{ComVrfy}(\mathsf{crs}, c, \pi_{\mathsf{Com}})$
- $0/1 \leftarrow \mathsf{DecVrfy}(\mathsf{crs}, c, m, \pi_{\mathsf{Dec}})$
- $m \leftarrow \mathsf{FDec}(\mathsf{crs}, c)$ - runtime *T*

Non-Interactive Timed Commitment Publicly Verifiable (KLX20)

- $\mathsf{crs} \leftarrow \mathsf{PGen}(1^\lambda, T)$
- $(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m)$
- $0/1 \leftarrow \mathsf{ComVrfy}(\mathsf{crs}, c, \pi_{\mathsf{Com}})$
- $0/1 \leftarrow \mathsf{DecVrfy}(\mathsf{crs}, c, m, \pi_{\mathsf{Dec}})$
- $(m, \pi_{\mathsf{FDec}}) \leftarrow \mathsf{FDec}(\mathsf{crs}, c)$ - runtime T
- $0/1 \leftarrow \mathsf{FDecVrfy}(\mathsf{crs}, c, m, \pi_{\mathsf{FDec}})$

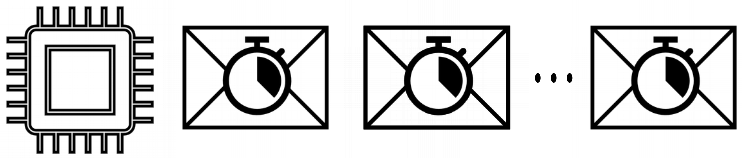
Non-Interactive Timed Commitment Publicly Verifiable Homomorphic (KLX20) (TCLM21)

- crs $\leftarrow \mathsf{PGen}(1^\lambda, T)$
- $(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m)$
- $0/1 \leftarrow \mathsf{ComVrfy}(\mathsf{crs}, c, \pi_{\mathsf{Com}})$
- $0/1 \leftarrow \mathsf{DecVrfy}(\mathsf{crs}, c, m, \pi_{\mathsf{Dec}})$
- $(m, \pi_{\mathsf{FDec}}) \leftarrow \mathsf{FDec}(\mathsf{crs}, c)$ - runtime T
- $0/1 \leftarrow \mathsf{FDecVrfy}(\mathsf{crs}, c, m, \pi_{\mathsf{FDec}})$
- Eval

Non-Interactive Timed Commitment Publicly Verifiable Homomorphic
(KLX20) (TCLM21)

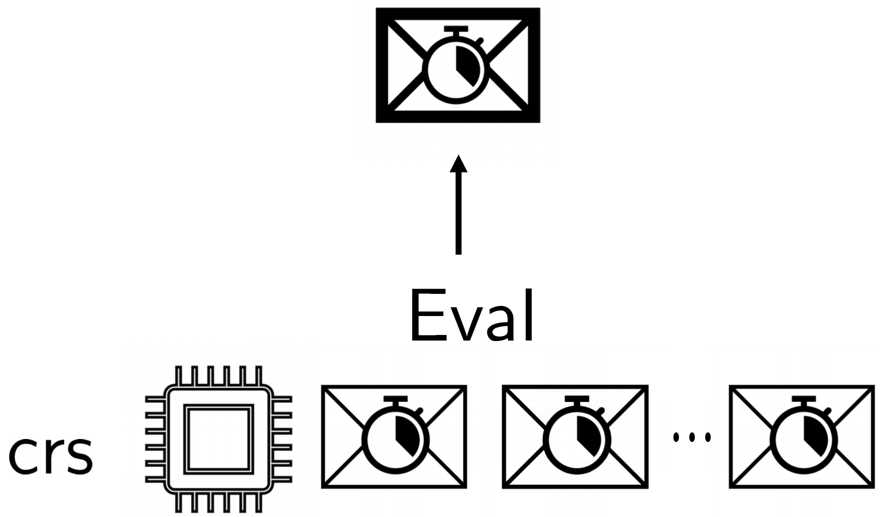
- crs $\leftarrow \mathsf{PGen}(1^\lambda, T)$
- $(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m)$
- $0/1 \leftarrow \mathsf{ComVrfy}(\mathsf{crs}, c, \pi_{\mathsf{Com}})$
- $0/1 \leftarrow \mathsf{DecVrfy}(\mathsf{crs}, c, m, \pi_{\mathsf{Dec}})$
- $(m, \pi_{\mathsf{FDec}}) \leftarrow \mathsf{FDec}(\mathsf{crs}, c)$ - runtime *T*
- $0/1 \leftarrow \mathsf{FDecVrfy}(\mathsf{crs}, c, m, \pi_{\mathsf{FDec}})$
- Eval

Eval

crs 

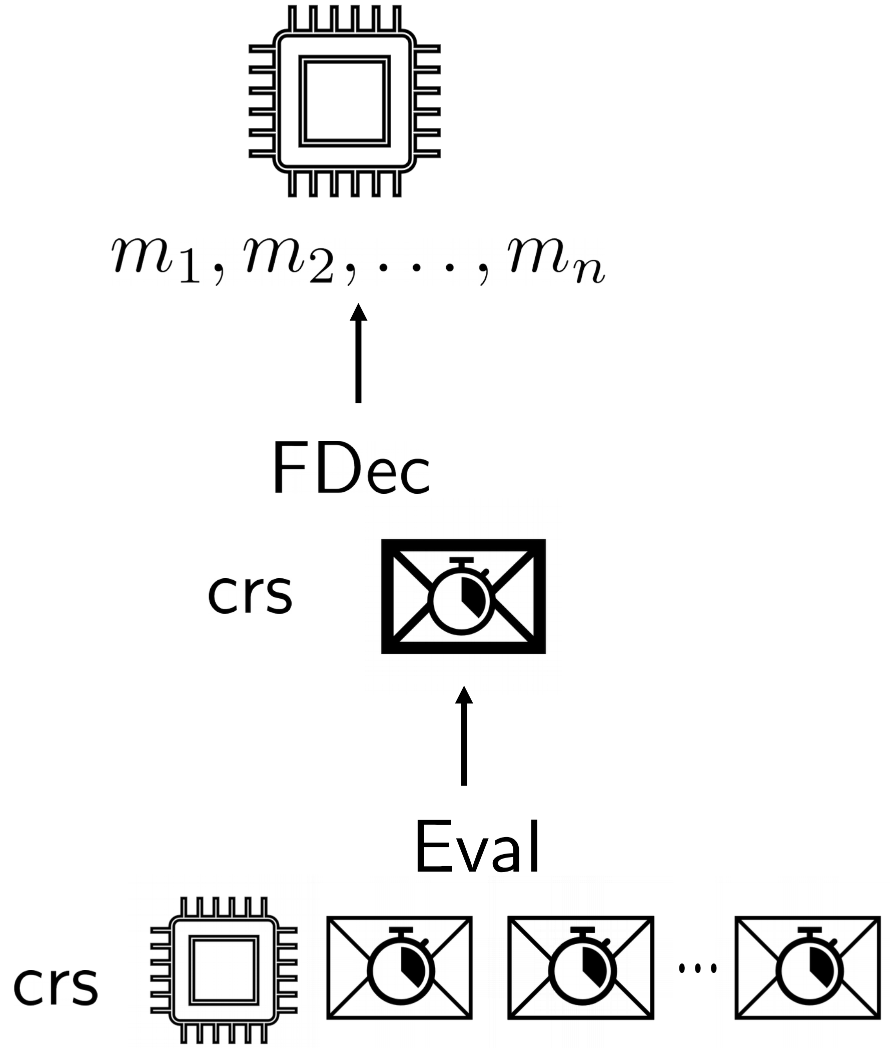
Non-Interactive Timed Commitment (KLX20) Publicly Verifiable Homomorphic (TCLM21)

- crs $\leftarrow$ PGen$(1^\lambda, T)$
- $(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m)$
- $0/1 \leftarrow \mathsf{ComVrfy}(\mathsf{crs}, c, \pi_{\mathsf{Com}})$
- $0/1 \leftarrow \mathsf{DecVrfy}(\mathsf{crs}, c, m, \pi_{\mathsf{Dec}})$
- $(m, \pi_{\mathsf{FDec}}) \leftarrow \mathsf{FDec}(\mathsf{crs}, c)$ - runtime *T*
- $0/1 \leftarrow \mathsf{FDecVrfy}(\mathsf{crs}, c, m, \pi_{\mathsf{FDec}})$
- Eval



Non-Interactive Timed Commitment (KLX20) Publicly Verifiable Homomorphic (TCLM21)

- $\text{crs} \leftarrow \text{PGen}(1^\lambda, T)$
- $(c, \pi_{\text{Com}}, \pi_{\text{Dec}}) \leftarrow \text{Com}(\text{crs}, m)$
- $0/1 \leftarrow \text{ComVrfy}(\text{crs}, c, \pi_{\text{Com}})$
- $0/1 \leftarrow \text{DecVrfy}(\text{crs}, c, m, \pi_{\text{Dec}})$
- $(m, \pi_{\text{FDec}}) \leftarrow \text{FDec}(\text{crs}, c)$ - runtime T
- $0/1 \leftarrow \text{FDecVrfy}(\text{crs}, c, m, \pi_{\text{FDec}})$
- Eval



IND-CCA Security (KLX20)

ExpNITC$_{\mathcal{A}}(\lambda)$

$Challenger$

$\mathcal{A}$

$\mathcal{A}_0$

$\mathcal{A}_1$

IND-CCA Security (KLX20)

$\mathsf{ExpNITC}_{\mathcal{A}}(\lambda)$

$Challenger$

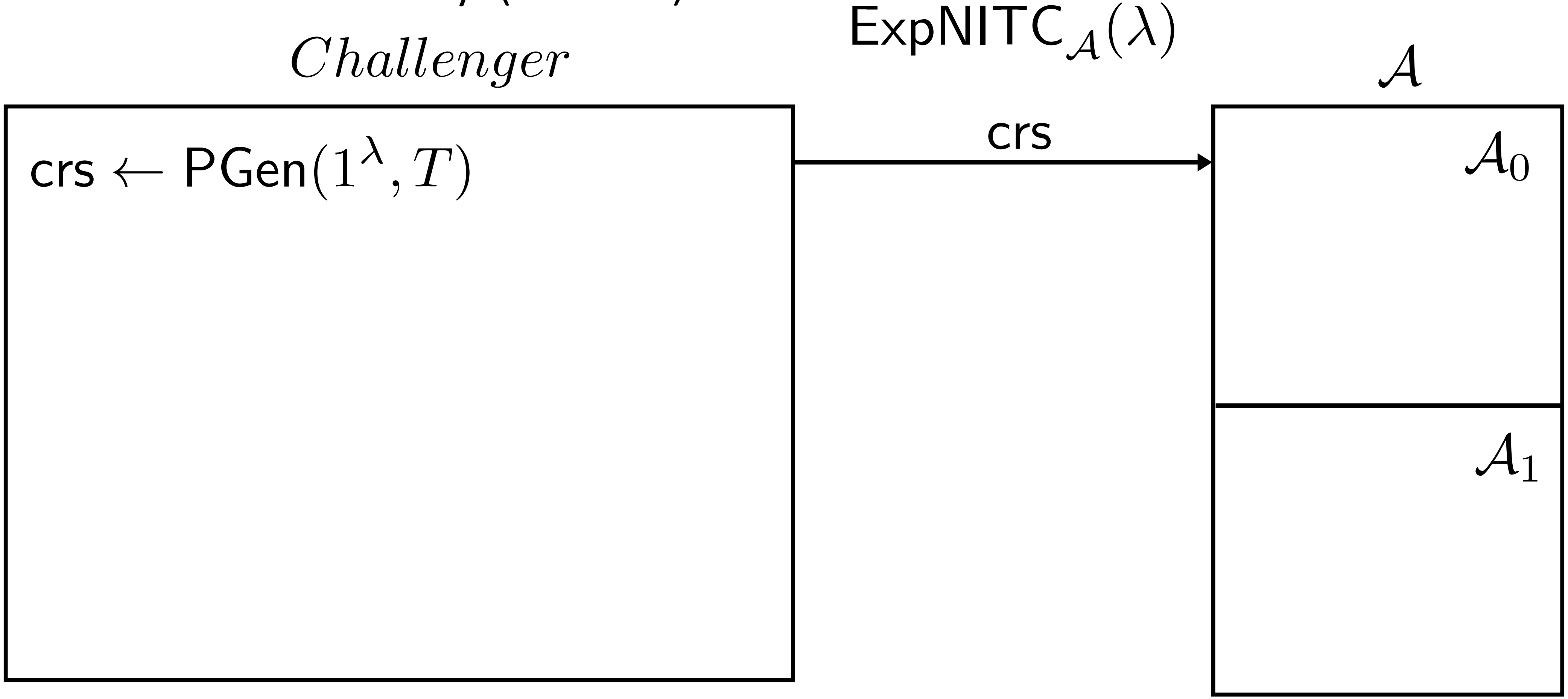
$\mathcal{A}$

$\mathsf{crs} \leftarrow \mathsf{PGen}(1^\lambda, T)$

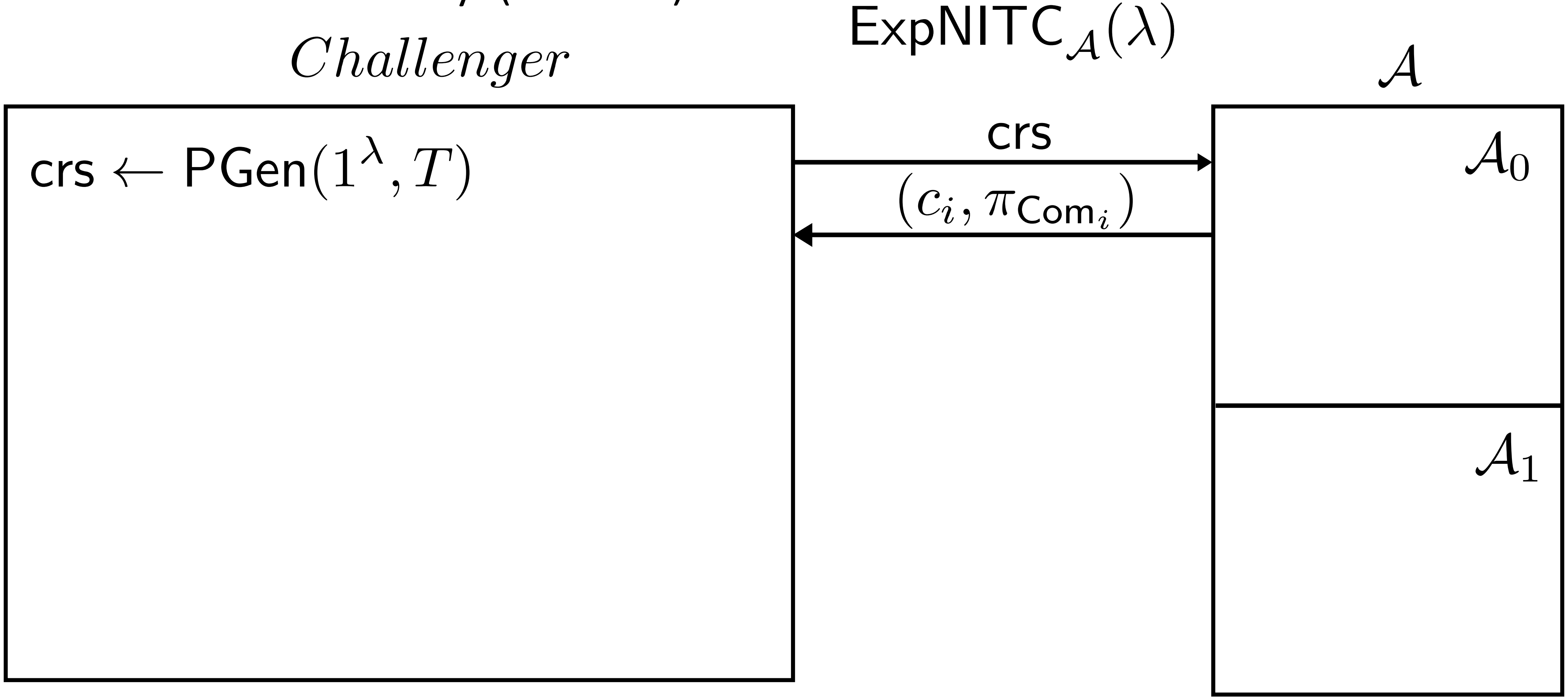
$\mathcal{A}_0$

$\mathcal{A}_1$

IND-CCA Security (KLX20)



IND-CCA Security (KLX20)



IND-CCA Security (KLX20)

$\mathsf{ExpNITC}_{\mathcal{A}}(\lambda)$

$Challenger$

$\mathcal{A}$

$\mathsf{crs} \leftarrow \mathsf{PGen}(1^{\lambda}, T)$

if $\mathsf{ComVrfy}(\mathsf{crs}, c_i, \pi_{\mathsf{Com}_i}) = 1$

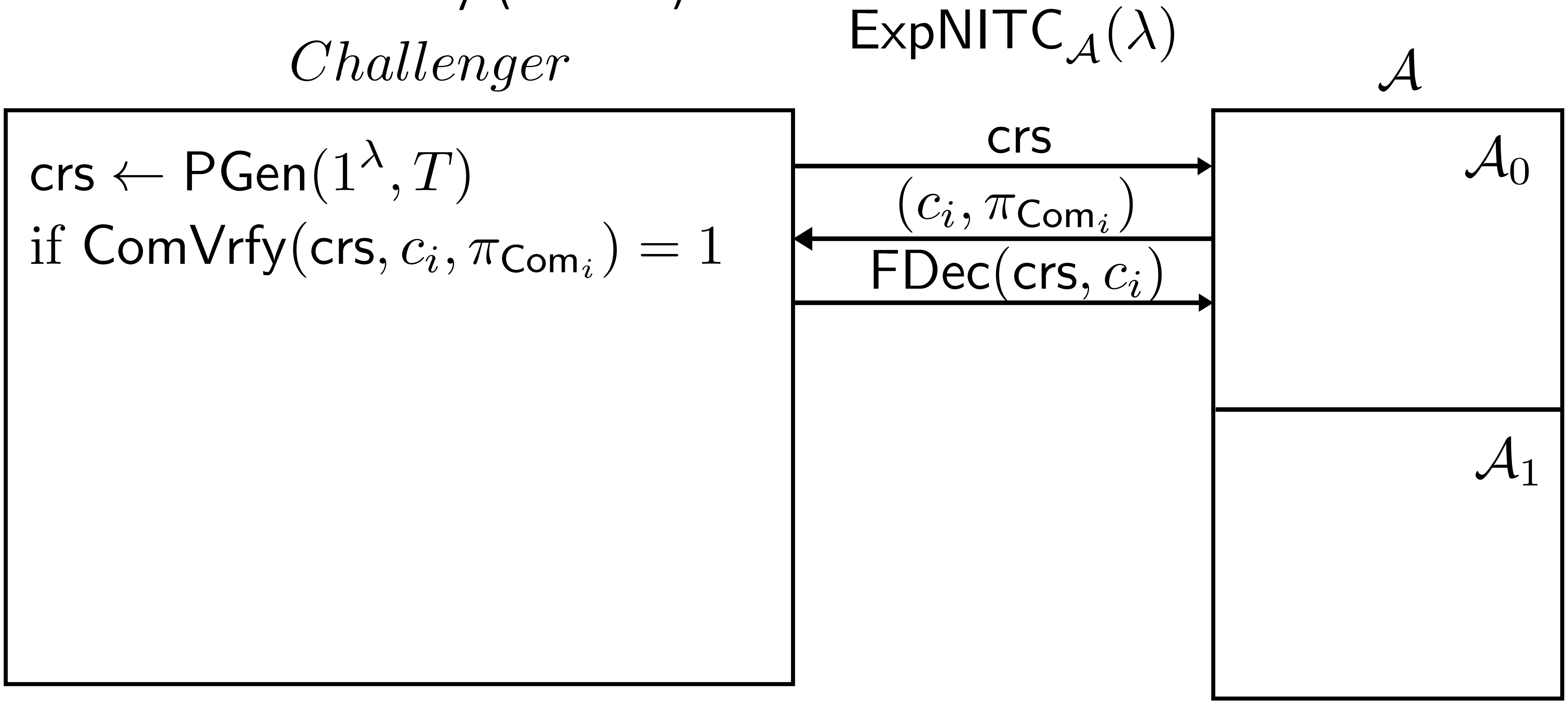
crs

$(c_i, \pi_{\mathsf{Com}_i})$

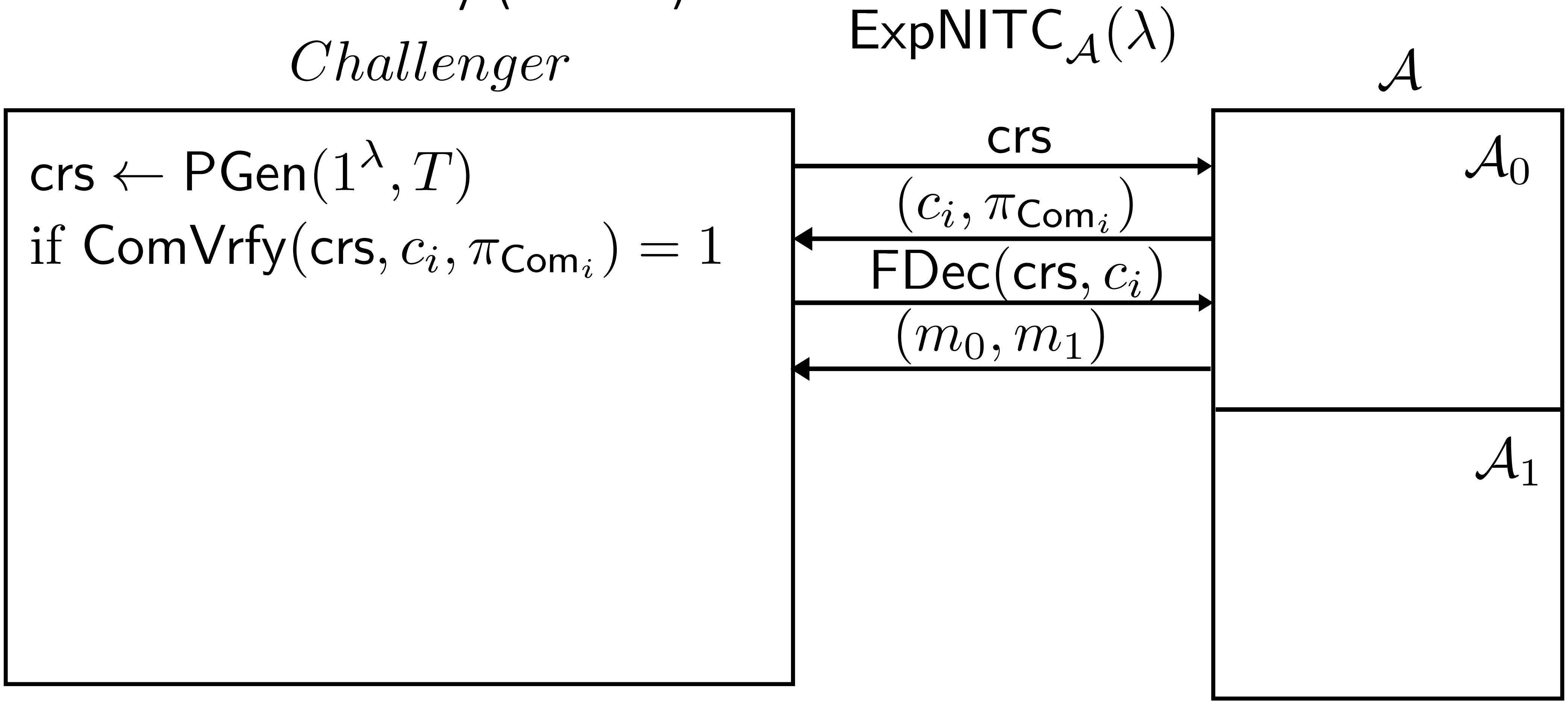
$\mathcal{A}_0$

$\mathcal{A}_1$

IND-CCA Security (KLX20)



IND-CCA Security (KLX20)



IND-CCA Security (KLX20)

$\mathsf{ExpNITC}_{\mathcal{A}}(\lambda)$

$Challenger$

$\mathsf{crs} \leftarrow \mathsf{PGen}(1^\lambda, T)$

$\text{if } \mathsf{ComVrfy}(\mathsf{crs}, c_i, \pi_{\mathsf{Com}_i}) = 1$

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

$(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m_b)$

$\mathcal{A}$

$\mathcal{A}_0$

$\mathcal{A}_1$

Challenger $\xrightarrow{\mathsf{crs}}$ $\mathcal{A}$

$\mathcal{A}$ $\xrightarrow{(c_i, \pi_{\mathsf{Com}_i})}$ Challenger

Challenger $\xrightarrow{\mathsf{FDec}(\mathsf{crs}, c_i)}$ $\mathcal{A}$

$\mathcal{A}$ $\xrightarrow{(m_0, m_1)}$ Challenger

IND-CCA Security (KLX20)

$\mathsf{ExpNITC}_{\mathcal{A}}(\lambda)$

$Challenger$

$\mathsf{crs} \leftarrow \mathsf{PGen}(1^\lambda, T)$

if $\mathsf{ComVrfy}(\mathsf{crs}, c_i, \pi_{\mathsf{Com}_i}) = 1$

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

$(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m_b)$

$\mathcal{A}$

$\mathcal{A}_0$

$\mathcal{A}_1$

$\xrightarrow{\mathsf{crs}}$

$\xleftarrow{(c_i, \pi_{\mathsf{Com}_i})}$

$\xrightarrow{\mathsf{FDec}(\mathsf{crs}, c_i)}$

$\xleftarrow{(m_0, m_1)}$

$\xrightarrow{(c, \pi_{\mathsf{Com}})}$

IND-CCA Security (KLX20)

$\mathsf{ExpNITC}_{\mathcal{A}}(\lambda)$

$Challenger$

$\mathsf{crs} \leftarrow \mathsf{PGen}(1^{\lambda}, T)$

if $\mathsf{ComVrfy}(\mathsf{crs}, c_i, \pi_{\mathsf{Com}_i}) = 1$

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

$(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m_b)$

$\mathcal{A}$

$\mathcal{A}_0$

$\mathcal{A}_1$

$\xrightarrow{\mathsf{crs}}$

$\xleftarrow{(c_i, \pi_{\mathsf{Com}_i})}$

$\xrightarrow{\mathsf{FDec}(\mathsf{crs}, c_i)}$

$\xleftarrow{(m_0, m_1)}$

$\xrightarrow{(c, \pi_{\mathsf{Com}})}$

$\xleftarrow{(c_i, \pi_{\mathsf{Com}_i})}$

IND-CCA Security (KLX20)

$\mathsf{ExpNITC}_{\mathcal{A}}(\lambda)$

$Challenger$

$\mathsf{crs} \leftarrow \mathsf{PGen}(1^\lambda, T)$

if $\mathsf{ComVrfy}(\mathsf{crs}, c_i, \pi_{\mathsf{Com}_i}) = 1$

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

$(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m_b)$

if $\mathsf{ComVrfy}(\mathsf{crs}, c_i, \pi_{\mathsf{Com}_i}) = 1 \wedge$

$(c, \pi_{\mathsf{Com}}) \neq (c_i, \pi_{\mathsf{Com}_i})$

$\mathcal{A}$

$\mathcal{A}_0$

$\xrightarrow{\mathsf{crs}}$

$\xleftarrow{(c_i, \pi_{\mathsf{Com}_i})}$

$\xrightarrow{\mathsf{FDec}(\mathsf{crs}, c_i)}$

$\xleftarrow{(m_0, m_1)}$

$\mathcal{A}_1$

$\xrightarrow{(c, \pi_{\mathsf{Com}})}$

$\xleftarrow{(c_i, \pi_{\mathsf{Com}_i})}$

IND-CCA Security (KLX20)

$\mathsf{ExpNITC}_{\mathcal{A}}(\lambda)$

$Challenger$

$\mathsf{crs} \leftarrow \mathsf{PGen}(1^\lambda, T)$

if $\mathsf{ComVrfy}(\mathsf{crs}, c_i, \pi_{\mathsf{Com}_i}) = 1$

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

$(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m_b)$

if $\mathsf{ComVrfy}(\mathsf{crs}, c_i, \pi_{\mathsf{Com}_i}) = 1 \wedge$

$(c, \pi_{\mathsf{Com}}) \neq (c_i, \pi_{\mathsf{Com}_i})$

$\mathcal{A}$

$\mathcal{A}_0$

$\xrightarrow{\mathsf{crs}}$

$\xleftarrow{(c_i, \pi_{\mathsf{Com}_i})}$

$\xrightarrow{\mathsf{FDec}(\mathsf{crs}, c_i)}$

$\xleftarrow{(m_0, m_1)}$

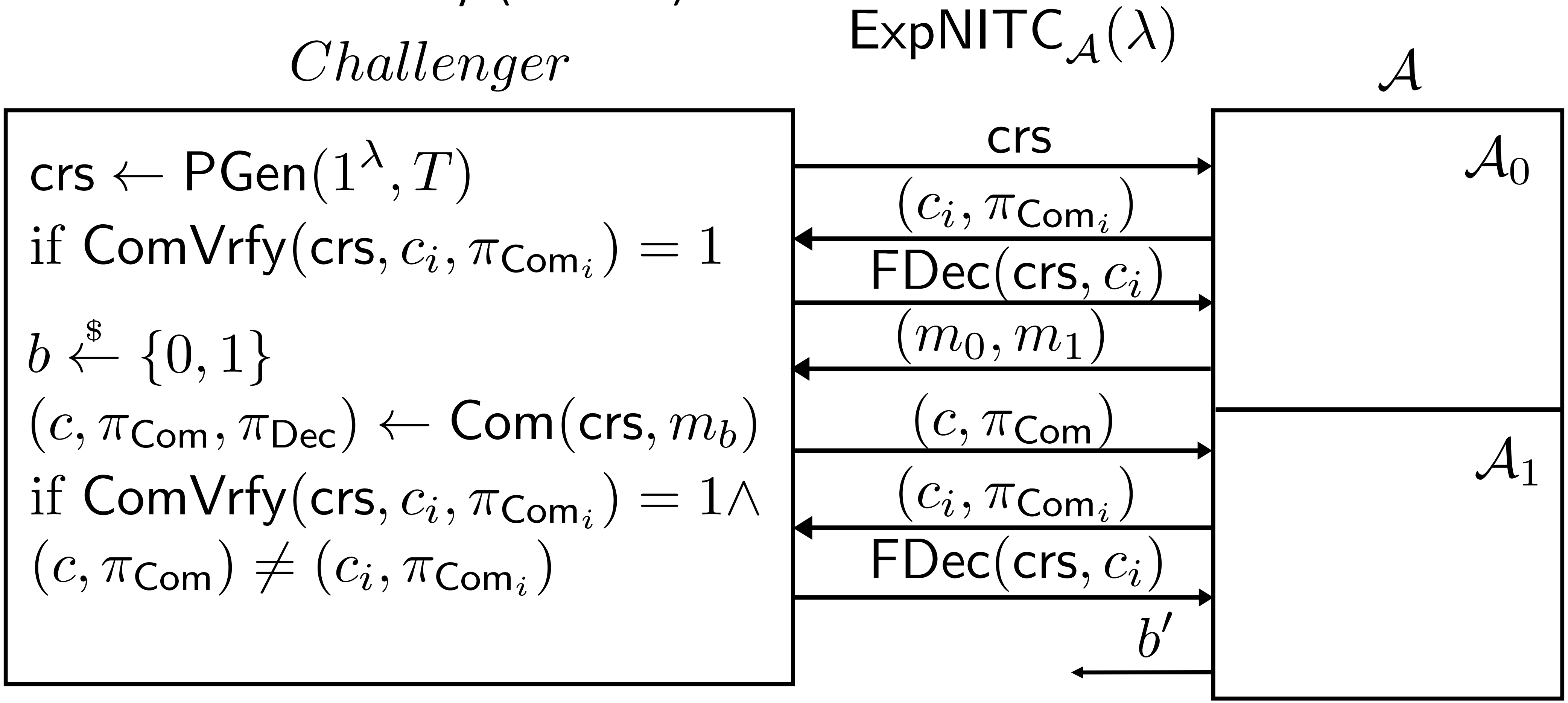
$\mathcal{A}_1$

$\xrightarrow{(c, \pi_{\mathsf{Com}})}$

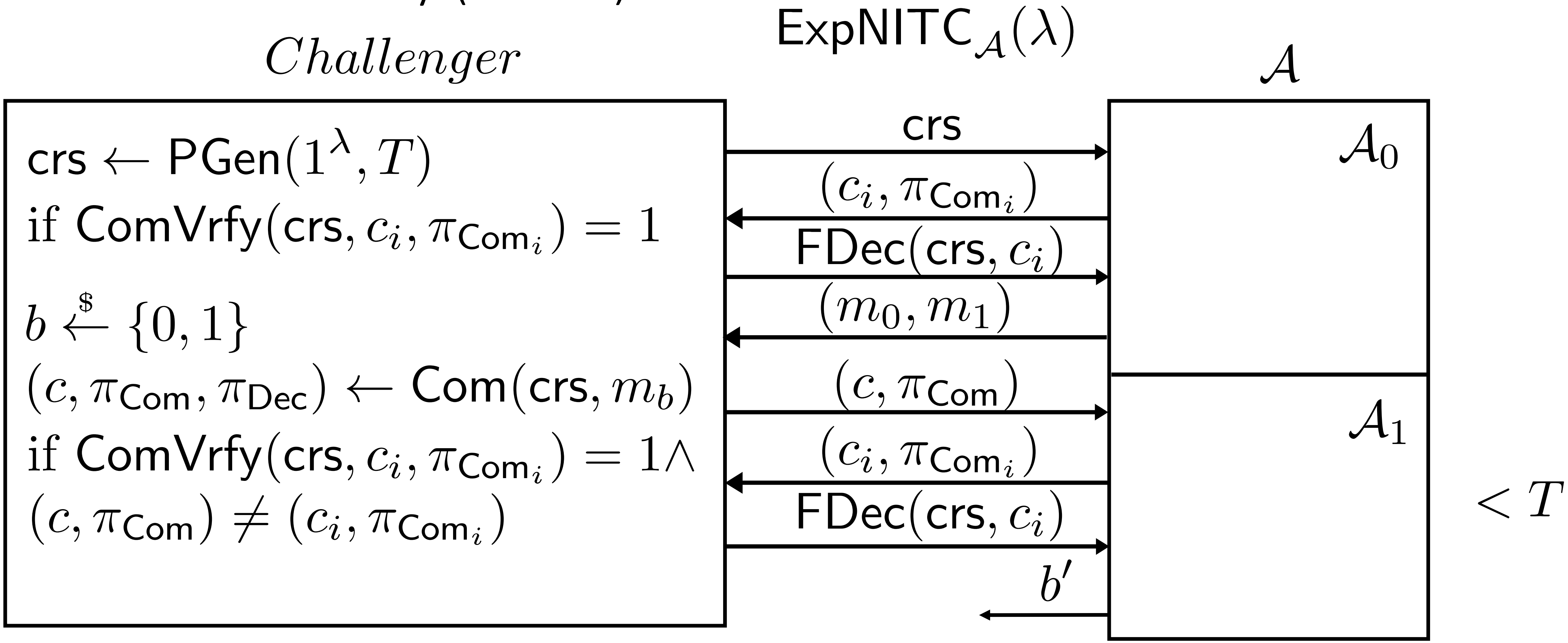
$\xleftarrow{(c_i, \pi_{\mathsf{Com}_i})}$

$\xrightarrow{\mathsf{FDec}(\mathsf{crs}, c_i)}$

IND-CCA Security (KLX20)



IND-CCA Security (KLX20)



IND-CCA Security (KLX20)

$\mathsf{ExpNITC}_{\mathcal{A}}(\lambda)$

$Challenger$

$\mathsf{crs} \leftarrow \mathsf{PGen}(1^{\lambda}, T)$

if $\mathsf{ComVrfy}(\mathsf{crs}, c_i, \pi_{\mathsf{Com}_i}) = 1$

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

$(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}}) \leftarrow \mathsf{Com}(\mathsf{crs}, m_b)$

if $\mathsf{ComVrfy}(\mathsf{crs}, c_i, \pi_{\mathsf{Com}_i}) = 1 \wedge$

$(c, \pi_{\mathsf{Com}}) \neq (c_i, \pi_{\mathsf{Com}_i})$

$\mathcal{A}$

$\mathcal{A}_0$

$\xrightarrow{\mathsf{crs}}$

$\xleftarrow{(c_i, \pi_{\mathsf{Com}_i})}$

$\xrightarrow{\mathsf{FDec}(\mathsf{crs}, c_i)}$

$\xleftarrow{(m_0, m_1)}$

$\mathcal{A}_1$

$\xrightarrow{(c, \pi_{\mathsf{Com}})}$

$\xleftarrow{(c_i, \pi_{\mathsf{Com}_i})}$

$\xrightarrow{\mathsf{FDec}(\mathsf{crs}, c_i)}$

$\xleftarrow{b'}$

$< T$

$$\text{Output of } \mathsf{ExpNITC}_{\mathcal{A}} : b = b'$$

$$\mathbf{Adv}_{\mathcal{A}}^{\mathtt{NITC}} = \left| \Pr[\mathsf{ExpNITC}_{\mathcal{A}}(\lambda) = 1] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda)$$

Publicly Verifiable CCA Secure PKE

Naor-Yung Paradigm (NY90)

- 2x CPA secure PKE and One-Time Simulation Sound NIZK

Publicly Verifiable CCA Secure PKE

Naor-Yung Paradigm (NY90)
- 2x CPA secure PKE and One-Time Simulation Sound NIZK

Efficient OT-SS NIZK

Publicly Verifiable CCA Secure PKE

Naor-Yung Paradigm (NY90)

- 2x CPA secure PKE and One-Time Simulation Sound NIZK

Efficient OT-SS NIZK

- Sigma Protocol

Publicly Verifiable CCA Secure PKE

Naor-Yung Paradigm (NY90)

- 2x CPA secure PKE and One-Time Simulation Sound NIZK

Efficient OT-SS NIZK

- Sigma Protocol
- Only for algebraic languages

Publicly Verifiable CCA Secure PKE

Naor-Yung Paradigm (NY90)
- 2x CPA secure PKE and One-Time Simulation Sound NIZK

Efficient OT-SS NIZK
- Sigma Protocol
- Only for algebraic languages

A challenge: Find a replacement to substitute PKE.

Homomorphic TLP (MT19)

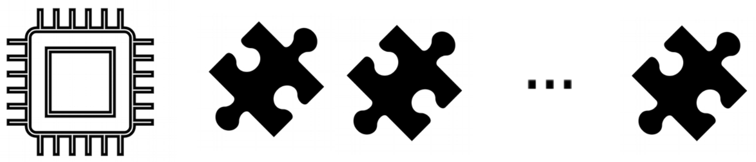
- $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda, T)$
- $Z \leftarrow \mathsf{Gen}(\mathsf{pp}, m)$
- $m \leftarrow \mathsf{Solve}(\mathsf{pp}, Z)$
- Eval

Homomorphic TLP (MT19)

- pp $\leftarrow$ Setup$(1^\lambda, T)$
- $Z \leftarrow$ Gen(pp, m)
- $m \leftarrow$ Solve(pp, Z)
- Eval

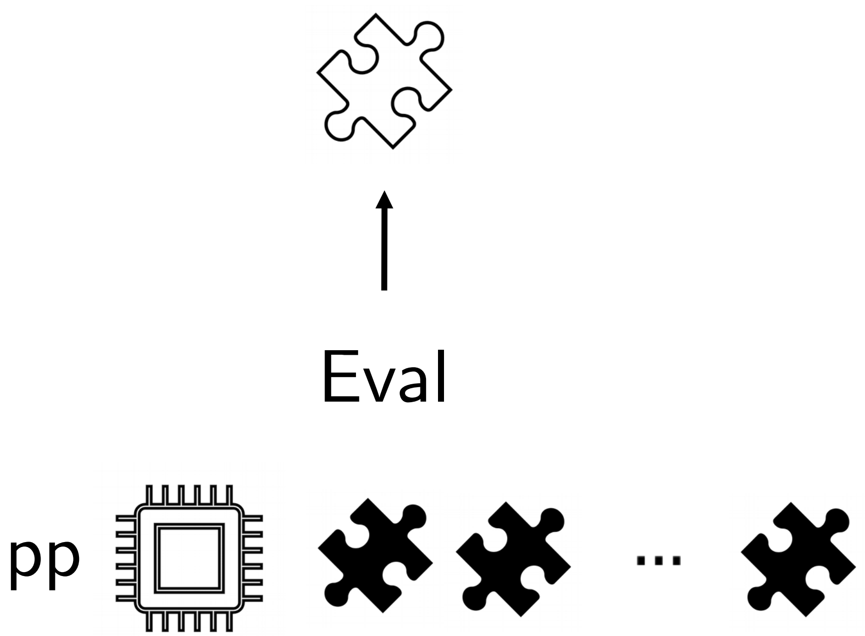
Eval

pp



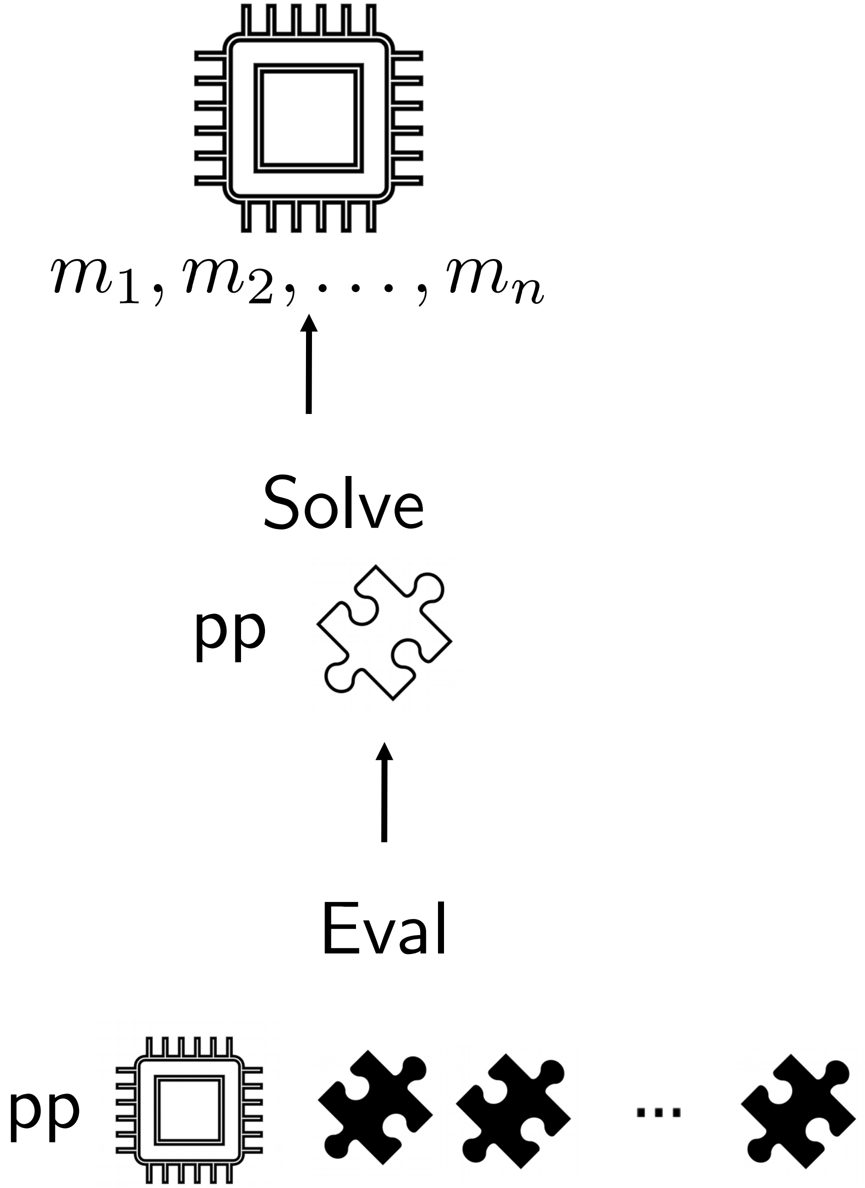
Homomorphic TLP (MT19)

- $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda, T)$
- $Z \leftarrow \mathsf{Gen}(\mathsf{pp}, m)$
- $m \leftarrow \mathsf{Solve}(\mathsf{pp}, Z)$
- Eval



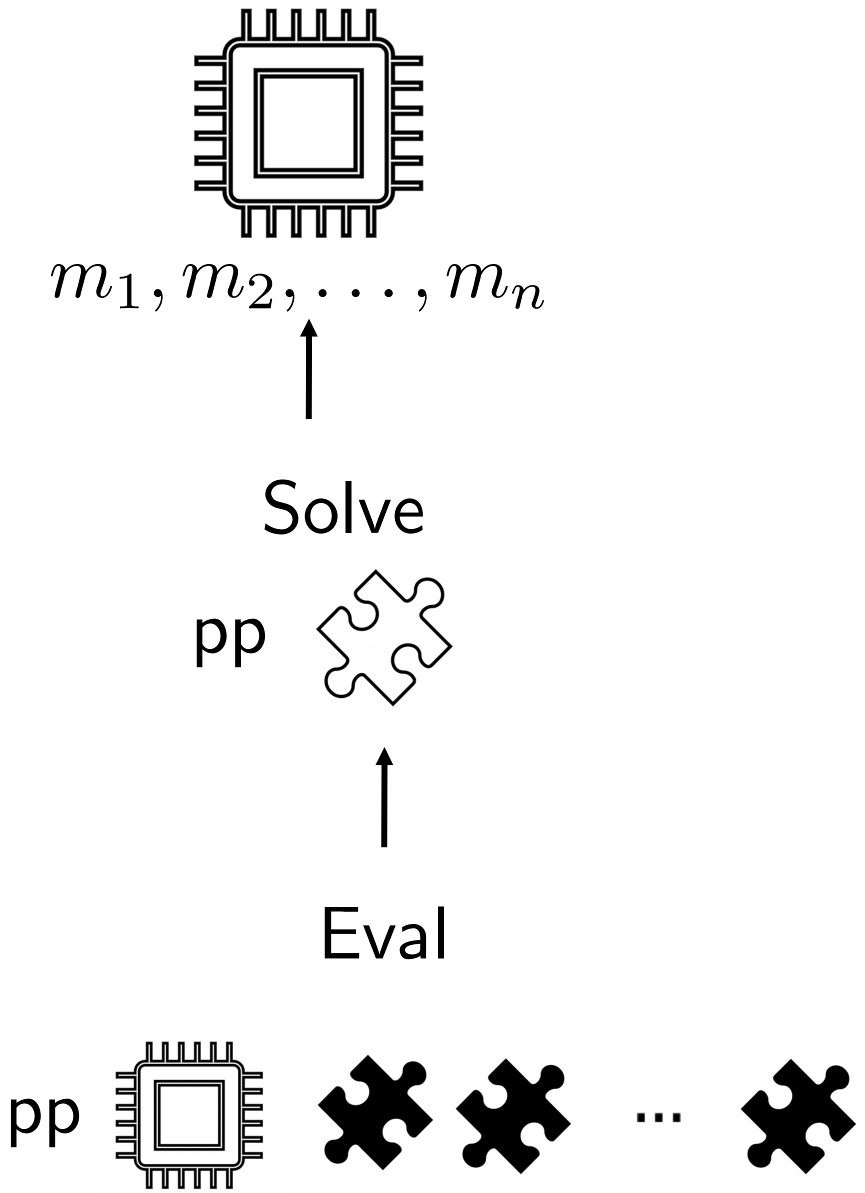
Homomorphic TLP (MT19)

- $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda, T)$
- $Z \leftarrow \mathsf{Gen}(\mathsf{pp}, m)$
- $m \leftarrow \mathsf{Solve}(\mathsf{pp}, Z)$
- Eval



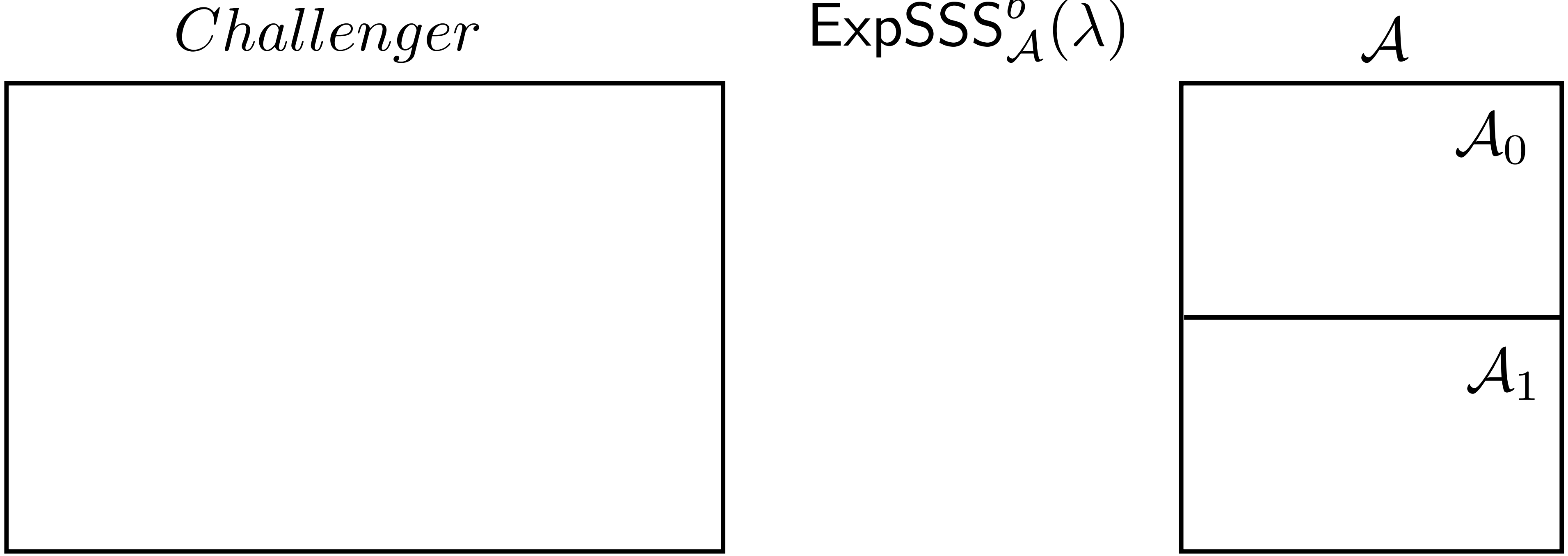
Homomorphic TLP (MT19)

- pp $\leftarrow$ Setup$(1^\lambda, T)$ PGen
- $Z \leftarrow$ Gen(pp, m) Com
- $m \leftarrow$ Solve(pp, Z) FDec
- Eval



Strong Sequential Squaring Assumption (MT19)

$\mathsf{ExpSSS}^{b}_{\mathcal{A}}(\lambda)$



Strong Sequential Squaring Assumption (MT19)

$Challenger$

$\mathsf{ExpSSS}^b_{\mathcal{A}}(\lambda)$

$\mathcal{A}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$\mathcal{A}_0$

$\mathcal{A}_1$

Strong Sequential Squaring Assumption (MT19)

$Challenger$ $\mathsf{ExpSSS}^b_{\mathcal{A}}(\lambda)$ $\mathcal{A}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$ $\xrightarrow{(N, T, g)}$ $\mathcal{A}_0$

$\mathcal{A}_1$

Strong Sequential Squaring Assumption (MT19)

$Challenger$ $\qquad$ $\mathsf{ExpSSS}^b_{\mathcal{A}}(\lambda)$ $\qquad$ $\mathcal{A}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$x \xleftarrow{\$} \mathbb{J}_N$

$y_0 := x^{2^T} \bmod N$

$y_1 \xleftarrow{\$} \mathbb{J}_N$

$\xrightarrow{(N, T, g)}$

$\mathcal{A}_0$

$\mathcal{A}_1$

Strong Sequential Squaring Assumption (MT19)

$Challenger$ $\mathsf{ExpSSS}^b_{\mathcal{A}}(\lambda)$ $\mathcal{A}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$x \xleftarrow{\$} \mathbb{J}_N$

$y_0 := x^{2^T} \bmod N$

$y_1 \xleftarrow{\$} \mathbb{J}_N$

(N, T, g) → $\mathcal{A}_0$

(x, y_b) → $\mathcal{A}_1$

Strong Sequential Squaring Assumption (MT19)

$\mathit{Challenger}$ $\qquad$ $\mathsf{ExpSSS}^{b}_{\mathcal{A}}(\lambda)$ $\qquad$ $\mathcal{A}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^{\lambda})$

$x \xleftarrow{\$} \mathbb{J}_N$

$y_0 := x^{2^T} \bmod N$

$y_1 \xleftarrow{\$} \mathbb{J}_N$

$\xrightarrow{(N, T, g)}$ $\mathcal{A}_0$

$\xrightarrow{(x, y_b)}$ $\mathcal{A}_1$

$\xleftarrow{b'}$

Strong Sequential Squaring Assumption (MT19)

$Challenger$ $\mathsf{ExpSSS}^b_{\mathcal{A}}(\lambda)$ $\mathcal{A}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$x \xleftarrow{\$} \mathbb{J}_N$

$y_0 := x^{2^T} \bmod N$

$y_1 \xleftarrow{\$} \mathbb{J}_N$

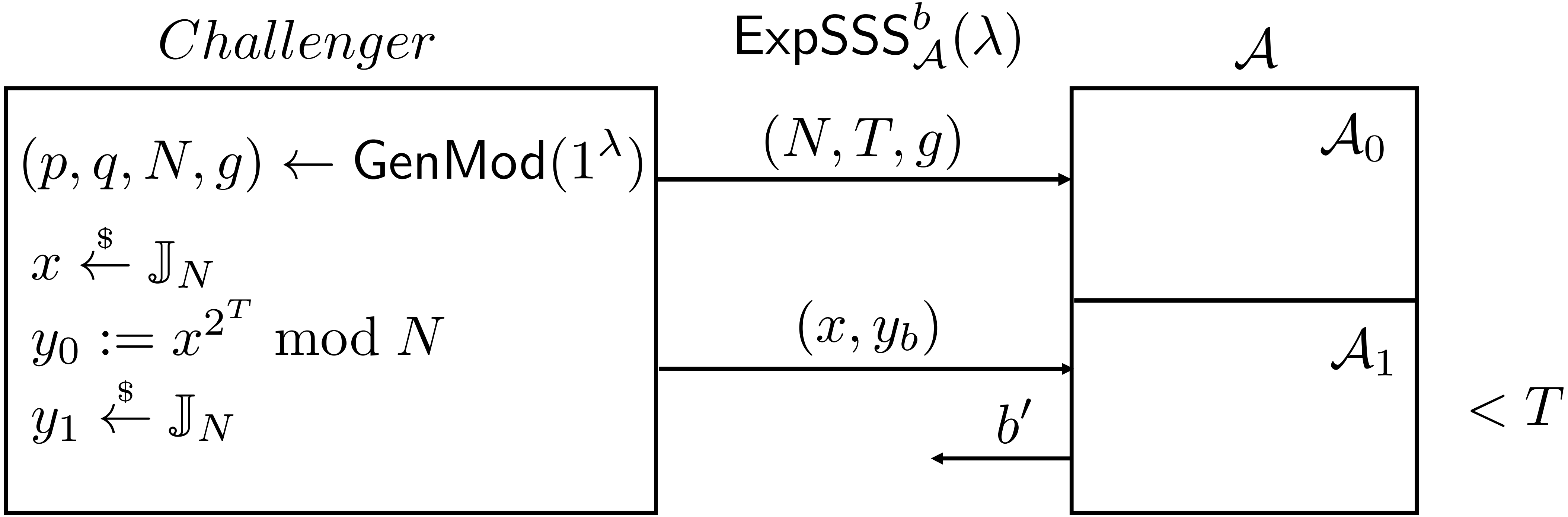
$(N, T, g) \rightarrow \mathcal{A}_0$

$(x, y_b) \rightarrow \mathcal{A}_1$

$\leftarrow b'$

$< T$

Strong Sequential Squaring Assumption (MT19)



$$\mathbf{Adv}^{\mathsf{SSS}}_{\mathcal{A}} = \left|\Pr[\mathsf{ExpSSS}^0_{\mathcal{A}}(\lambda) = 1] - \Pr[\mathsf{ExpSSS}^1_{\mathcal{A}}(\lambda) = 1]\right| \leq \mathsf{negl}(\lambda)$$

Construction of Linearly Homomorphic TLP (MT19)

$\underline{\mathsf{PGen}(1^\lambda, T)}$
$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$
$\varphi(N) := (p-1)(q-1)$
$t := 2^T \bmod \varphi(N)/2$
$h := g^t \bmod N$
return $\mathsf{crs} := (N, T, g, h)$

Construction of Linearly Homomorphic TLP (MT19)

$\underline{\mathsf{PGen}(1^\lambda, T)}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$\varphi(N) := (p-1)(q-1)$

$t := 2^T \bmod \varphi(N)/2$

$h := g^t \bmod N$

$\text{return } \mathsf{crs} := (N, T, g, h)$

Paillier-like encryption

$\underline{\mathsf{Com}(\mathsf{crs}, m)}$

$r \xleftarrow{\$} [N/2]$

$c_0 := g^r \bmod N$

$c_1 := h^{rN}(1+N)^m \bmod N^2$

$\text{return } (c_0, c_1)$

Construction of Linearly Homomorphic TLP (MT19)

$\underline{\mathsf{PGen}(1^\lambda, T)}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$\varphi(N) := (p-1)(q-1)$

$t := 2^T \bmod \varphi(N)/2$

$h := g^t \bmod N$

$\text{return } \mathsf{crs} := (N, T, g, h)$

Paillier-like encryption

$\underline{\mathsf{Com}(\mathsf{crs}, m)}$

$r \xleftarrow{\$} [N/2]$

$c_0 := g^r \bmod N$

$c_1 := h^{rN}(1+N)^m \bmod N^2$

$\text{return } (c_0, c_1)$

$\underline{\mathsf{FDec}(\mathsf{crs}, (c_0, c_1))}$

$y := c_0^{2^T} \bmod N$

$\text{return } \frac{c_1 \cdot y^{-N} (\bmod N^2) - 1}{N}$

Construction of Linearly Homomorphic TLP (MT19)

$\underline{\mathsf{PGen}(1^\lambda, T)}$
$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$
$\varphi(N) := (p-1)(q-1)$
$t := 2^T \bmod \varphi(N)/2$
$h := g^t \bmod N$
return $\mathsf{crs} := (N, T, g, h)$

Paillier-like encryption

$\underline{\mathsf{Com}(\mathsf{crs}, m)}$
$r \xleftarrow{\$} [N/2]$
$c_0 := g^r \bmod N$
$c_1 := h^{rN}(1+N)^m \bmod N^2$
return (c_0, c_1)

$\underline{\mathsf{FDec}(\mathsf{crs}, (c_0, c_1))}$
$y := c_0^{2^T} \bmod N$
return $\frac{c_1 \cdot y^{-N} (\bmod N^2) - 1}{N}$

Paillier-like homomorphism

$\underline{\mathsf{Eval}(\mathsf{crs}, \oplus_N, (c_{i,0}, c_{i,1})_{i\in[n]})}$
$c_0 := \prod_{i=1}^n c_{i,0} \bmod N$
$c_1 := \prod_{i=1}^n c_{i,1} \bmod N^2$
return (c_0, c_1)

Construction of Linearly Homomorphic TLP (MT19)

Paillier-like encryption

$\underline{\mathsf{PGen}(1^\lambda, T)}$
$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$
$\varphi(N) := (p-1)(q-1)$
$t := 2^T \bmod \varphi(N)/2$
$h := g^t \bmod N$
$\text{return } \mathsf{crs} := (N, T, g, h)$

$\underline{\mathsf{Com}(\mathsf{crs}, m)}$
$r \xleftarrow{\$} [N/2]$
$c_0 := g^r \bmod N$
$c_1 := h^{rN}(1+N)^m \bmod N^2$
$\text{return } (c_0, c_1)$

$\underline{\mathsf{FDec}(\mathsf{crs}, (c_0, c_1))}$
$y := c_0^{2^T} \bmod N$
$\text{return } \frac{c_1 \cdot y^{-N} (\bmod N^2) - 1}{N}$

Paillier-like homomorphism

$\underline{\mathsf{Eval}(\mathsf{crs}, \oplus_N, (c_{i,0}, c_{i,1})_{i\in[n]})}$
$c_0 := \prod_{i=1}^{n} c_{i,0} \bmod N$
$c_1 := \prod_{i=1}^{n} c_{i,1} \bmod N^2$
$\text{return } (c_0, c_1)$

$\underline{\mathsf{DecVrfy}(\mathsf{crs}, (c_0, c_1), m, r)}$
$\text{if } c_0 = g^r \bmod N \wedge$
$c_1 = h_1^{rN}(1+N)^m \bmod N^2$
$\quad \text{return } 1$
$\text{return } 0$

Construction of Linearly Homomorphic TLP (MT19)

Paillier-like encryption

$\underline{\mathsf{PGen}(1^\lambda, T)}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$\varphi(N) := (p-1)(q-1)$

$t := 2^T \bmod \varphi(N)/2$

$h := g^t \bmod N$

return $\mathsf{crs} := (N, T, g, h)$

$\underline{\mathsf{Com}(\mathsf{crs}, m)}$

$r \xleftarrow{\$} [N/2]$

$c_0 := g^r \bmod N$

$c_1 := h^{rN}(1+N)^m \bmod N^2$

return (c_0, c_1)

$\underline{\mathsf{FDec}(\mathsf{crs}, (c_0, c_1))}$

$y := c_0^{2^T} \bmod N$

return $\frac{c_1 \cdot y^{-N} (\bmod N^2) - 1}{N}$

Paillier-like homomorphism

$\underline{\mathsf{Eval}(\mathsf{crs}, \oplus_N, (c_{i,0}, c_{i,1})_{i \in [n]})}$

$c_0 := \prod_{i=1}^n c_{i,0} \bmod N$

$c_1 := \prod_{i=1}^n c_{i,1} \bmod N^2$

return (c_0, c_1)

$\underline{\mathsf{DecVrfy}(\mathsf{crs}, (c_0, c_1), m, r)}$

if $c_0 = g^r \bmod N \wedge$

$c_1 = h_1^{rN}(1+N)^m \bmod N^2$

  return 1

return 0

Assumptions:

- Strong Sequential Squaring
- Decisional Composite Residuosity
- Decisional Diffie-Hellman

Naor-Yung (1st Attempt)

$h_1 := g_1^{t_1} \bmod N_1$

$\underline{\mathsf{Com}_1(\mathsf{crs}_1, m)}$

$r_1 \xleftarrow{\$} [N_1/2]$

$c_0 := g_1^{r_1} \bmod N_1$

$c_1 := h_1^{r_1 N_1}(1+N_1)^m \bmod N_1^2$

return (c_0, c_1)

$h_2 := g_2^{t_2} \bmod N_2$

$\underline{\mathsf{Com}_2(\mathsf{crs}_2, m)}$

$r_2 \xleftarrow{\$} [N_2/2]$

$c_0' := g_2^{r_2} \bmod N_2$

$c_1' := h_2^{r_2 N_2}(1+N_2)^m \bmod N_2^2$

return (c_0', c_1')

Naor-Yung (1st Attempt)

$$h_1 := g_1^{t_1} \bmod N_1$$

$$\underline{\mathsf{Com}_1(\mathsf{crs}_1, m)}$$
$$r_1 \xleftarrow{\$} [N_1/2]$$
$$c_0 := g_1^{r_1} \bmod N_1$$
$$c_1 := h_1^{r_1 N_1}(1+N_1)^m \bmod N_1^2$$
$$\text{return } (c_0, c_1)$$

$$h_2 := g_2^{t_2} \bmod N_2$$

$$\underline{\mathsf{Com}_2(\mathsf{crs}_2, m)}$$
$$r_2 \xleftarrow{\$} [N_2/2]$$
$$c_0' := g_2^{r_2} \bmod N_2$$
$$c_1' := h_2^{r_2 N_2}(1+N_2)^m \bmod N_2^2$$
$$\text{return } (c_0', c_1')$$

Proving that commitments contain the same message using the standard Sigma protocol ⇒ $N_1 = N_2$.

Naor-Yung (1st Attempt)

Game	Dec. Queries	Proof	$\texttt{HTLP}_1$	$\texttt{HTLP}_2$	Assumption
0	FDec	Real	m_b	m_b	

Naor-Yung (1st Attempt)

Game	Dec. Queries	Proof	$\texttt{HTLP}_1$	$\texttt{HTLP}_2$	Assumption
0	FDec	Real	m_b	m_b	
1	t_1	Real	m_b	m_b	Snd of NIZK

Naor-Yung (1st Attempt)

Game	Dec. Queries	Proof	$\mathtt{HTLP}_1$	$\mathtt{HTLP}_2$	Assumption
0	FDec	Real	m_b	m_b	
1	t_1	Real	m_b	m_b	Snd of NIZK
2	t_1	Simul	m_b	m_b	ZK of NIZK

Naor-Yung (1^{st} Attempt)

Game	Dec. Queries	Proof	$\mathtt{HTLP}_1$	$\mathtt{HTLP}_2$	Assumption
0	FDec	Real	m_b	m_b	
1	t_1	Real	m_b	m_b	Snd of NIZK
2	t_1	Simul	m_b	m_b	ZK of NIZK
3	t_1	Simul	m_b	m	Sec of HTLP

Naor-Yung (1st Attempt)

Game	Dec. Queries	Proof	$\mathtt{HTLP}_1$	$\mathtt{HTLP}_2$	Assumption
0	FDec	Real	m_b	m_b	
1	t_1	Real	m_b	m_b	Snd of NIZK
2	t_1	Simul	m_b	m_b	ZK of NIZK
3	t_1	Simul	m_b	m	Sec of HTLP

$$t_1 := 2^T \bmod \varphi(N)/2$$

Naor-Yung (1st Attempt)

Game	Dec. Queries	Proof	$\mathtt{HTLP}_1$	$\mathtt{HTLP}_2$	Assumption
0	FDec	Real	m_b	m_b	
1	t_1	Real	m_b	m_b	Snd of NIZK
2	t_1	Simul	m_b	m_b	ZK of NIZK
3	t_1	Simul	m_b	m	Sec of HTLP

$$t_1 := 2^T \bmod \varphi(N)/2$$

SSS
DCR
DDH

Naor-Yung (1st Attempt)

Game	Dec. Queries	Proof	$\mathtt{HTLP}_1$	$\mathtt{HTLP}_2$	Assumption
0	FDec	Real	m_b	m_b	
1	t_1	Real	m_b	m_b	Snd of NIZK
2	t_1	Simul	m_b	m_b	ZK of NIZK
3	t_1	Simul	m_b	m	Sec of HTLP

$$t_1 := 2^T \bmod \varphi(N)/2$$

SSS
DCR
DDH

Naor-Yung (1st Attempt)

Game	Dec. Queries	Proof	$\mathtt{HTLP}_1$	$\mathtt{HTLP}_2$	Assumption
0	FDec	Real	m_b	m_b	
1	t_1	Real	m_b	m_b	Snd of NIZK
2	t_1	Simul	m_b	m_b	ZK of NIZK
3	t_1	Simul	m_b	m	Sec of HTLP

$$t_1 := 2^T \bmod \varphi(N)/2$$

$\boxed{\text{SSS}}$

DCR

DDH

Knowing the factorization of *N* does not allow to reduce to SSS!

Construction of Linearly Homomorphic Encryption

$\underline{\mathsf{PGen}(1^\lambda, T)}$
$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$
$\varphi(N) := (p-1)(q-1)$
$t := 2^T \bmod \varphi(N)/2$
$h = g^t \bmod N$
$\text{return } \mathsf{pp} := (N, T, g, h)$

$\underline{\mathsf{Com}(\mathsf{crs}, m)}$
$r \xleftarrow{\$} [N/2]$
$c_0 := g^r \bmod N$
$\mathrm{c}_1 := h^{rN}(1+N)^m \bmod N^2$
$\text{return } (c_0, c_1)$

$\underline{\mathsf{FDec}(\mathsf{crs}, (c_0, c_1))}$
$y := c_0^{2^T} \bmod N$
$\text{return } \frac{c_1 \cdot y^{-N} (\bmod N^2) - 1}{N}$

$\underline{\mathsf{Eval}(\mathsf{crs}, \oplus_N, (c_{i,0}, c_{i,1})_{i \in [n]})}$
$c_0 := \prod_{i=1}^n c_{i,0} \bmod N$
$c_1 := \prod_{i=1}^n c_{i,1} \bmod N^2$
$\text{return } (c_0, c_1)$

$\underline{\mathsf{DecVrfy}(\mathsf{crs}, (c_0, c_1), m, r)}$
$\text{if } c_0 = g^r \bmod N \wedge$
$c_1 = h_1^{rN}(1+N)^m \bmod N^2$
$\quad \text{return } 1$
$\text{return } 0$

Construction of Linearly Homomorphic Encryption

$\underline{\mathsf{Setup}(1^\lambda)}$
$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$
$\varphi(N) := (p-1)(q-1)$
$t \xleftarrow{\$} [N/2]$
$h = g^t \bmod N$
return $\mathsf{pk} = (N, g, h), \mathsf{sk} := t$

$\underline{\mathsf{Com}(\mathsf{crs}, m)}$
$r \xleftarrow{\$} [N/2]$
$c_0 := g^r \bmod N$
$c_1 := h^{rN}(1+N)^m \bmod N^2$
return (c_0, c_1)

$\underline{\mathsf{FDec}(\mathsf{crs}, (c_0, c_1))}$
$y := c_0^{2^T} \bmod N$
return $\frac{c_1 \cdot y^{-N} (\bmod N^2) - 1}{N}$

$\underline{\mathsf{Eval}(\mathsf{crs}, \oplus_N, (c_{i,0}, c_{i,1})_{i \in [n]})}$
$c_0 := \prod_{i=1}^{n} c_{i,0} \bmod N$
$c_1 := \prod_{i=1}^{n} c_{i,1} \bmod N^2$
return (c_0, c_1)

$\underline{\mathsf{DecVrfy}(\mathsf{crs}, (c_0, c_1), m, r)}$
if $c_0 = g^r \bmod N \wedge$
$c_1 = h_1^{rN}(1+N)^m \bmod N^2$
    return 1
return 0

Construction of Linearly Homomorphic Encryption

$\underline{\mathsf{Setup}(1^\lambda)}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$\varphi(N) := (p-1)(q-1)$

$t \xleftarrow{\$} [N/2]$

$h = g^t \bmod N$

return $\mathsf{pk} = (N, g, h), \mathsf{sk} := t$

$\underline{\mathsf{Enc}(\mathsf{pk}, m)}$

$r \xleftarrow{\$} [N/2]$

$c_0 := g^r \bmod N$

$c_1 := h^{rN}(1+N)^m \bmod N^2$

return (c_0, c_1)

$\underline{\mathsf{FDec}(\mathsf{crs}, (c_0, c_1))}$

$y := c_0^{2^T} \bmod N$

return $\frac{c_1 \cdot y^{-N} (\bmod N^2) - 1}{N}$

$\underline{\mathsf{Eval}(\mathsf{crs}, \oplus_N, (c_{i,0}, c_{i,1})_{i \in [n]})}$

$c_0 := \prod_{i=1}^{n} c_{i,0} \bmod N$

$c_1 := \prod_{i=1}^{n} c_{i,1} \bmod N^2$

return (c_0, c_1)

$\underline{\mathsf{DecVrfy}(\mathsf{crs}, (c_0, c_1), m, r)}$

if $c_0 = g^r \bmod N \wedge$

$c_1 = h_1^{rN}(1+N)^m \bmod N^2$

    return 1

return 0

Construction of Linearly Homomorphic Encryption

$\underline{\mathsf{Setup}(1^\lambda)}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$\varphi(N) := (p-1)(q-1)$

$t \xleftarrow{\$} [N/2]$

$h = g^t \bmod N$

return $\mathsf{pk} = (N, g, h), \mathsf{sk} := t$

$\underline{\mathsf{Enc}(\mathsf{pk}, m)}$

$r \xleftarrow{\$} [N/2]$

$c_0 := g^r \bmod N$

$c_1 := h^{rN}(1+N)^m \bmod N^2$

return (c_0, c_1)

$\underline{\mathsf{Dec}(\mathsf{sk} = t, (c_0, c_1))}$

$y := c_0^t \bmod N$

return $\frac{c_1 \cdot y^{-N} (\bmod N^2) - 1}{N}$

$\underline{\mathsf{Eval}(\mathsf{crs}, \oplus_N, (c_{i,0}, c_{i,1})_{i \in [n]})}$

$c_0 := \prod_{i=1}^n c_{i,0} \bmod N$

$c_1 := \prod_{i=1}^n c_{i,1} \bmod N^2$

return (c_0, c_1)

$\underline{\mathsf{DecVrfy}(\mathsf{crs}, (c_0, c_1), m, r)}$

if $c_0 = g^r \bmod N \wedge$

$c_1 = h_1^{rN}(1+N)^m \bmod N^2$

  return 1

return 0

Construction of Linearly Homomorphic Encryption

Setup(1^λ)

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$
$\varphi(N) := (p-1)(q-1)$
$t \xleftarrow{\$} [N/2]$
$h = g^t \bmod N$
return $\mathsf{pk} = (N, g, h), \mathsf{sk} := t$

Enc(pk, m)

$r \xleftarrow{\$} [N/2]$
$c_0 := g^r \bmod N$
$c_1 := h^{rN}(1+N)^m \bmod N^2$
return (c_0, c_1)

Dec(sk $= t, (c_0, c_1)$)

$y := c_0^t \bmod N$
return $\frac{c_1 \cdot y^{-N} (\bmod N^2) - 1}{N}$

Eval(crs, $\oplus_N, (c_{i,0}, c_{i,1})_{i\in[n]}$)

$c_0 := \prod_{i=1}^n c_{i,0} \bmod N$
$c_1 := \prod_{i=1}^n c_{i,1} \bmod N^2$
return (c_0, c_1)

DecVrfy(crs, $(c_0, c_1), m, r$)

if $c_0 = g^r \bmod N \wedge$
$c_1 = h_1^{rN}(1+N)^m \bmod N^2$
  return 1
return 0

Assumptions:

- Decisional Composite Residuosity
- Decisional Diffie-Hellman

Naor-Yung (2nd Attempt)

$h_1 := g_1^k \bmod N$

$\underline{\mathsf{Enc}(\mathsf{pk}, m)}$

$r_1 \xleftarrow{\$} [N]$

$c_0 := g_1^{r_1} \bmod N$

$c_1 := h_1^{r_1 N}(1+N)^m \bmod N^2$

return (c_0, c_1)

$h_2 := g_2^t \bmod N$

$\underline{\mathsf{Com}(\mathsf{crs}_2, m)}$

$r_2 \xleftarrow{\$} [N/2]$

$c_0' := g_2^{r_2} \bmod N$

$c_1' := h_2^{r_2 N}(1+N)^m \bmod N^2$

return (c_0', c_1')

Naor-Yung (2nd Attempt)

$h_1 := g_1^k \bmod N$

$\underline{\mathsf{Enc}(\mathsf{pk}, m)}$

$r_1 \xleftarrow{\$} [N]$
$c_0 := g_1^{r_1} \bmod N$
$c_1 := h_1^{r_1 N}(1+N)^m \bmod N^2$
$\text{return } (c_0, c_1)$

$h_2 := g_2^t \bmod N$

$\underline{\mathsf{Com}(\mathsf{crs}_2, m)}$

$r_2 \xleftarrow{\$} [N/2]$
$c_0' := g_2^{r_2} \bmod N$
$c_1' := h_2^{r_2 N}(1+N)^m \bmod N^2$
$\text{return } (c_0', c_1')$

$$t := 2^T \bmod \varphi(N)/2$$

Knowing the factorization of *N* does not allow to reduce to DCR!

Triple Naor-Yung

$$h_1 := g_1^{k_1} \bmod N$$

$$\underline{\mathsf{Enc}_1(\mathsf{pk}_1, m)}$$
$$r_1 \xleftarrow{\$} [N]$$
$$c_0 := g_1^{r_1} \bmod N$$
$$c_1 := h_1^{r_1 N}(1+N)^m \bmod N^2$$
$$\text{return } (c_0, c_1)$$

$$h_2 := g_2^{k_2} \bmod N$$

$$\underline{\mathsf{Enc}_2(\mathsf{pk}_2, m)}$$
$$r_2 \xleftarrow{\$} [N]$$
$$c_0' := g_2^{r_2} \bmod N$$
$$c_1' := h_2^{r_2 N}(1+N)^m \bmod N^2$$
$$\text{return } (c_0', c_1')$$

$$h_3 := g_3^{t} \bmod N$$

$$\underline{\mathsf{Com}(\mathsf{crs}, m)}$$
$$r_3 \xleftarrow{\$} [N/2]$$
$$c_0'' := g_3^{r_3} \bmod N$$
$$c_1'' := h_3^{r_3 N}(1+N)^m \bmod N^2$$
$$\text{return } (c_0'', c_1'')$$

Triple Naor-Yung

Game	Dec. Queries	Proof	$\mathtt{PKE}_1$	$\mathtt{PKE}_2$	$\mathtt{HTLP}$	Assumption
0	FDec	Real	m_b	m_b	m_b	
1	k_1	Real	m_b	m_b	m_b	Snd of NIZK
2	k_1	Simul	m_b	m_b	m_b	ZK of NIZK
3	k_1	Simul	m_b	m_b	m	Sec of HTLP
4	k_1	Simul	m_b	m	m	Sec of PKE_2

Triple Naor-Yung

Game	Dec. Queries	Proof	$\texttt{PKE}_1$	$\texttt{PKE}_2$	$\texttt{HTLP}$	Assumption
0	FDec	Real	m_b	m_b	m_b	
1	k_1	Real	m_b	m_b	m_b	Snd of NIZK
2	k_1	Simul	m_b	m_b	m_b	ZK of NIZK
3	k_1	Simul	m_b	m_b	m	Sec of HTLP
4	k_1	Simul	m_b	m	m	Sec of PKE_2
5	k_2	Simul	m_b	m	m	OT-SimSnd
6	k_2	Simul	m	m	m	Sec of PKE_1

Shrinking CRS and Commitment Size - BMV16

crs	Commitment
g_1 $h_1 := g_1^{k_1}$	$g_1^{r_1}$ $h_1^{r_1 N}(1+N)^m$
g_2 $h_2 := g_2^{k_2}$	$g_2^{r_2}$ $h_2^{r_2 N}(1+N)^m$
g_3 $h_3 := g_3^{t}$	$g_3^{r_3}$ $h_3^{r_3 N}(1+N)^m$

Shrinking CRS and Commitment Size - BMV16

crs	Commitment
g_1 $h_1 := g_1^{k_1}$	$g_1^{r_1}$ $h_1^{r_1 N}(1+N)^m$
g_2 $h_2 := g_2^{k_2}$	$g_2^{r_2}$ $h_2^{r_2 N}(1+N)^m$
g_3 $h_3 := g_3^{t}$	$g_3^{r_3}$ $h_3^{r_3 N}(1+N)^m$

$\Rightarrow$

crs	Commitment
g $h_1 := g^{k_1}$ $h_2 := g^{k_2}$ $h_3 := g^{t}$	g^r $h_1^{rN}(1+N)^m$ $h_2^{rN}(1+N)^m$ $h_3^{rN}(1+N)^m$

Shrinking CRS and Commitment Size - BMV16

crs	Commitment
g_1 $h_1 := g_1^{k_1}$	$g_1^{r_1}$ $h_1^{r_1 N}(1+N)^m$
g_2 $h_2 := g_2^{k_2}$	$g_2^{r_2}$ $h_2^{r_2 N}(1+N)^m$
g_3 $h_3 := g_3^{t}$	$g_3^{r_3}$ $h_3^{r_3 N}(1+N)^m$

$\Rightarrow$

crs	Commitment
g $h_1 := g^{k_1}$ $h_2 := g^{k_2}$ $h_3 := g^{t}$	g^r $h_1^{rN}(1+N)^m$ $h_2^{rN}(1+N)^m$ $h_3^{rN}(1+N)^m$

One-Time Simulation Sound NIZK

$$L = \left\{ (c_0, c_1, c_2, c_3) | \exists (m, r) : \begin{array}{r} (\wedge_{i=1}^{3} c_i = h_i^{rN}(1+N)^m \bmod N^2) \wedge \\ c_0 = g^r \bmod N \end{array} \right\}$$

Construction of Linearly Homomorphic PVNITC

$\underline{\mathsf{PGen}(1^\lambda, T)}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$\varphi(N) := (p-1)(q-1)$

$k_1, k_2 \xleftarrow{\$} [N/2]$

$t := 2^T \bmod \varphi(N)/2$

For $i \in [2] : h_i := g^{k_i} \bmod N$

$h_3 := g^t \bmod N$

$\mathsf{crs}_{\mathtt{NIZK}} \leftarrow \mathtt{NIZK}.\mathsf{Setup}(1^\lambda, L)$

return $\mathsf{crs} := (N, T, g, h_1, h_2, h_3, \mathsf{crs}_{\mathtt{NIZK}})$

Construction of Linearly Homomorphic PVNITC

$\underline{\mathsf{PGen}(1^\lambda, T)}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$\varphi(N) := (p-1)(q-1)$

$k_1, k_2 \xleftarrow{\$} [N/2]$

$t := 2^T \bmod \varphi(N)/2$

For $i \in [2] : h_i := g^{k_i} \bmod N$

$h_3 := g^t \bmod N$

$\mathsf{crs}_{\mathtt{NIZK}} \leftarrow \mathtt{NIZK}.\mathsf{Setup}(1^\lambda, L)$

return $\mathsf{crs} := (N, T, g, h_1, h_2, h_3, \mathsf{crs}_{\mathtt{NIZK}})$

$\underline{\mathsf{Com}(\mathsf{crs}, m)}$

$r \xleftarrow{\$} [N/2]$

$c_0 := g^r \bmod N$

For $i \in [3] : c_i := h_i^{rN}(1+N)^m \bmod N^2$

$c := (c_0, c_1, c_2, c_3), w := (m, r)$

$\pi_{\mathsf{Com}} \leftarrow \mathtt{NIZK}.\mathsf{Prove}(\mathsf{crs}_{\mathtt{NIZK}}, c, w)$

$\pi_{\mathsf{Dec}} := r$

return $(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}})$

Construction of Linearly Homomorphic PVNITC

$\underline{\mathsf{PGen}(1^\lambda, T)}$

$(p, q, N, g) \leftarrow \mathsf{GenMod}(1^\lambda)$

$\varphi(N) := (p-1)(q-1)$

$k_1, k_2 \xleftarrow{\$} [N/2]$

$t := 2^T \bmod \varphi(N)/2$

For $i \in [2] : h_i := g^{k_i} \bmod N$

$h_3 := g^t \bmod N$

$\mathsf{crs}_{\mathtt{NIZK}} \leftarrow \mathtt{NIZK}.\mathsf{Setup}(1^\lambda, L)$

return $\mathsf{crs} := (N, T, g, h_1, h_2, h_3, \mathsf{crs}_{\mathtt{NIZK}})$

$\underline{\mathsf{Com}(\mathsf{crs}, m)}$

$r \xleftarrow{\$} [N/2]$

$c_0 := g^r \bmod N$

For $i \in [3] : c_i := h_i^{rN}(1+N)^m \bmod N^2$

$c := (c_0, c_1, c_2, c_3), w := (m, r)$

$\pi_{\mathsf{Com}} \leftarrow \mathtt{NIZK}.\mathsf{Prove}(\mathsf{crs}_{\mathtt{NIZK}}, c, w)$

$\pi_{\mathsf{Dec}} := r$

return $(c, \pi_{\mathsf{Com}}, \pi_{\mathsf{Dec}})$

$\underline{\mathsf{ComVrfy}, \mathsf{DecVrfy}, \mathsf{FDec}, \mathsf{FDecVrfy}, \mathsf{Eval}}$

Conclusion/Comparison to Prior Work

Construction	Hom.	Std.	Setup	Com?	FDec?	|Com|	$\|\pi_{Com}\|$	t_{com}	Tight
EFKP20	-	✘	-	✘	✔	$O(1)$	-	$O(\log T)$	✔
KLX20	-	✔	priv.	✔	✘	$O(1)$	$O(1)$	$O(T)$	✔
TCLM21	lin.	✘	pub.	✔	✘	$O(\lambda)$	$O(\lambda)$	$O(1)$	✘
Our work	lin.	✔	priv.	✔	✔	$O(1)$	$O(\log \lambda)$	$O(1)$	✔
Our work	mult.	✔	priv.	✔	✔	$O(1)$	$O(\log \lambda)$	$O(1)$	✔
Our work	lin.	✘	priv.	✔	✔	$O(1)$	$O(1)$	$O(1)$	✔
Our work	mult.	✘	priv.	✔	✔	$O(1)$	$O(1)$	$O(1)$	✔

Conclusion/Comparison to Prior Work

Construction	Hom.	Std.	Setup	Com?	FDec?	$\lvert\mathsf{Com}\rvert$	$\lvert\pi_{\mathsf{Com}}\rvert$	t_{com}	Tight
EFKP20	-	✘	-	✘	✔	$O(1)$	-	$O(\log T)$	✔
KLX20	-	✔	priv.	✔	✘	$O(1)$	$O(1)$	$O(T)$	✔
TCLM21	lin.	✘	pub.	✔	✘	$O(\lambda)$	$O(\lambda)$	$O(1)$	✘
Our work	lin.	✔	priv.	✔	✔	$O(1)$	$O(\log \lambda)$	$O(1)$	✔
Our work	mult.	✔	priv.	✔	✔	$O(1)$	$O(\log \lambda)$	$O(1)$	✔
Our work	lin.	✘	priv.	✔	✔	$O(1)$	$O(1)$	$O(1)$	✔
Our work	mult.	✘	priv.	✔	✔	$O(1)$	$O(1)$	$O(1)$	✔

- Full paper https://eprint.iacr.org/2022/1498
- Contact: chvojka.p@gmail.com

Conclusion/Comparison to Prior Work

Construction	Hom.	Std.	Setup	Com?	FDec?	$\lvert\mathsf{Com}\rvert$	$\lvert\pi_{\mathsf{Com}}\rvert$	t_{com}	Tight
EFKP20	-	✘	-	✘	✔	$O(1)$	-	$O(\log T)$	✔
KLX20	-	✔	priv.	✔	✘	$O(1)$	$O(1)$	$O(T)$	✔
TCLM21	lin.	✘	pub.	✔	✘	$O(\lambda)$	$O(\lambda)$	$O(1)$	✘
Our work	lin.	✔	priv.	✔	✔	$O(1)$	$O(\log \lambda)$	$O(1)$	✔
Our work	mult.	✔	priv.	✔	✔	$O(1)$	$O(\log \lambda)$	$O(1)$	✔
Our work	lin.	✘	priv.	✔	✔	$O(1)$	$O(1)$	$O(1)$	✔
Our work	mult.	✘	priv.	✔	✔	$O(1)$	$O(1)$	$O(1)$	✔

- Full paper https://eprint.iacr.org/2022/1498
- Contact: chvojka.p@gmail.com

Thank you for your attention.